SIEMENS

SIMATIC HMI

WinCC Unified
Readme WinCC Unified

System Manual

Validity 1

Important notes 2

Cybersecurity information 3

Engineering and runtime 4

Unified Engineering 5

Unified PC 6

Unified Comfort Panels 7

Unified Basic Panels 8

Redundancy 9

Audit 10

Unified Station Configurator 11

Corporate Designer 12

WinCC Unified Data Hub 13

Online documentation

08/2025
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 persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the application described in the catalog and the associated usage information. 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
Ⓟ 09/2025 Subject to change

Copyright © Siemens 2025.
All rights reserved

Table of contents

1 Validity 7

2 Important notes 9

3 Cybersecurity information 27

4 Engineering and runtime 31

4.1 Improvements in Update 4 31

4.2 Improvements in Update 3 31
4.2.1 Improvements in Update 3 31
4.2.2 Load user files 39
4.2.3 Reading an array as block with handshake procedure 43
4.2.4 Set system time 46

4.3 Improvements in Update 1 48

5 Unified Engineering 49

5.1 Improvements in Update 4 49

5.2 Improvements in Update 3 51
5.2.1 General improvements in Update 3 51
5.2.2 Unified Screen Editor (Next Gen.) 53
5.2.2.1 Unified Screen Editor (Next Gen.) - Introduction 53
5.2.2.2 Select editor 53
5.2.2.3 New functions 54
5.2.2.4 Improvements in Unified Screen Editor (Next Gen.) 54
5.2.3 Screens and screen objects 54
5.2.3.1 Screens and screen objects - Improvements (Unified ES) 54
5.2.3.2 Alarm line 56
5.2.3.3 Centrally defining zooming and panning 57
5.2.3.4 Localized default texts for screen objects 58
5.2.3.5 Searching for an object property in the screen 59
5.2.3.6 Overview of Screen resources 63
5.2.3.7 I/O field: "Shift decimal places" property 64
5.2.4 Faceplates 65
5.2.4.1 Interface tags 65
5.2.4.2 Faceplates: Dynamization via interface properties 65
5.2.4.3 Improved flexibility with use of user data types 68
5.2.5 Libraries 68
5.2.5.1 Use type in type 68
5.2.5.2 Import of text lists 68
5.2.5.3 Scripting: Referencing the default version 69
5.2.5.4 User Tags > Set 'AlwaysDownload' 69
5.2.6 System functions 70
5.2.6.1 System functions for local user management 70
5.2.6.2 System functions for screen navigation 71
5.2.6.3 System functions for backing up and restoring logs 74
5.2.6.4 System functions for PLC code view 75

5.2.7 Using event parameters in the function list ... 77
5.3 Improvements in Update 1 ... 77
6 Unified PC ... 79
6.1 Important information ... 79
6.2 Improvements in Update 4 ... 82
6.3 Improvements in Update 2 ... 85
6.3.1 General improvements in Update 2 ... 85
6.3.2 My WinCC Unified ... 85
6.4 Improvements in Update 1 ... 90
6.5 Improvements in Service Release 1 ... 90
7 Unified Comfort Panels ... 91
7.1 Important information ... 91
7.2 Connecting Unified Comfort Panel with SQL database ... 96
7.3 Improvements in V20 Upd.2 ... 98
7.3.1 General improvements in V20 Upd.2 ... 98
7.3.2 The screen keyboard in runtime ... 100
7.3.3 "Devices and Input" > "Printers" ... 102
8 Unified Basic Panels ... 107
8.1 Important information ... 107
8.2 Improvements in V20 Upd.2 ... 109
8.2.1 General improvements in V20 Upd.2 ... 109
8.2.2 The screen keyboard in runtime ... 110
9 Redundancy ... 115
9.1 Redundancy switchover of the web clients with local user management ... 115
10 Audit ... 117
10.1 General improvements in Update 3 ... 117
10.2 Audit Trail parameters ... 117
11 Unified Station Configurator ... 121
11.1 Important information ... 121
11.2 General improvements in Update 3 ... 122
12 Corporate Designer ... 125
12.1 Improvements in Update 4 ... 125
12.2 Improvements in Update 3 ... 125
12.3 Password for secure transfer of the style ... 125
13 WinCC Unified Data Hub ... 129
13.1 Introduction to Unified Data Hub ... 129
13.2 Installing the WinCC Unified Data Hub ... 130
13.2.1 Software and hardware requirements ... 130

13.2.2 Licenses ... 132
13.2.3 Certificates ... 133
13.2.3.1 Creating certificates ... 133
13.2.3.2 Distributing and installing certificates ... 135
13.2.4 Starting installation ... 138
13.2.5 Adapting the IP address of the UDH server ... 141

13.3 Configuring WinCC Unified Data Hub ... 142
13.3.1 Requirements ... 142
13.3.2 Configuring the device as a Unified Data Hub server ... 142
13.3.3 Configuring the device as a Unified Data Hub client ... 144
13.3.4 Defining logs to be transferred ... 145
13.3.5 Connection diagnostics ... 146

13.4 Central logging and restoring ... 153
13.4.1 Working with GraphQL ... 155
13.4.1.1 Introduction to GraphQL ... 155
13.4.1.2 Creating UDH user roles or user groups ... 156
13.4.1.3 Authorizations in GraphQL ... 159
13.4.1.4 Setting up the GraphQL client ... 159
13.4.1.5 Executing GraphQL operations ... 161
13.4.1.6 Executing a GraphQL operation in standalone mode ... 164
13.4.1.7 Automatic backup and logging of segments ... 165
13.4.1.8 Restoring a backup ... 165
13.4.1.9 Restore intervals ... 168

1 Validity

Validity

This update is valid for the following products:

- TIA Portal V20 (WinCC Unified ES V20)
- SIMATIC WinCC Unified V20 PC Runtime

Note

It is possible that the .NET Framework installed with WinCC Unified PC Runtime Advanced V17 is no longer up to date and could have security vulnerabilities. Since it cannot be brought up-to-date with an update, you yourself have to ensure that the latest version of the .NET Framework is always installed. Instructions on how you can determine the installed version and how to update the .NET Framework are available in the .NET Framework documentation (https://learn.microsoft.com/en-us/dotnet/framework).

Latest Readme version

In the Readme, available as PDF, on the download page of SIMATIC WinCC Unified PC Runtime, you can find contents that could not be included in the Readme delivered with the product.

Example: The Readme files for V19 updates can be found in the SiePortal under Entry ID 109820989 (https://support.industry.siemens.com/cs/document/109820989/updates-for-simatic-wincc-unified-pc-runtime-v19?dti=0&lc=en-WW).

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.

It is the responsibility of the customers to prevent 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 protective 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 that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are outdated or no longer supported may increase the 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)

Important notes

2

This page contains important information about product properties.

Device versions with V20 Update 3

The new device version 20.0.0.2 has been introduced for Unified PC and Unified Panels in order to be able to use the new functions which were introduced with V20 Update 3. Please note the following:

- If you open a project on a computer on which TIA Portal V20 is installed without an update, you cannot edit the devices contained there with device version 20.0.0.2.
- If you switch from a device version 20.0.0.2 to a previous device version, you can no longer use new functions.
- The functions introduced with V20 Update 3 are also supported in higher device versions.

Device versions for Unified PC

- Install Update 3 for WinCC Unified Runtime on the target device before loading a device with device version 20.0.0.2.
- If you load a device with the configured device version 20.0.0.0 into Runtime with a higher device version, warnings are displayed pointing out the different versions. To avoid incompatibilities, the configured device version should correspond to the actual Runtime version.

Images for Unified Panel

- Images can be downloaded from the Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109746530).
- Images are enabled independent of WinCC (TIA Portal).
- Use ProSave to import an image version that does not correspond to the configured device version onto a Panel.
- If a new image only contains improvements for the Runtime of the device, this version is not shown in the Engineering System. In this case, use the latest device version displayed in the Engineering System.
- If the image 20.0.0.0 is installed on the device, install image download version V20.0 Upd.2 or higher before you load a device with the configured device version 20.0.0.2. When loading this device, enable the "Keep aspect ratio" setting in the "Load preview" dialog so that the new image version is transferred to the Panel. Alternatively, use ProSave.
- If you load a device with the configured device version 20.0.0.0, it is not absolutely necessary to update the image on the Panel. If you load a device with the configured device version 20.0.0.0 onto a Panel with a higher device version, warnings are displayed pointing out the different versions. You can ignore them.

Panel: Read and write access to linked S7-300 String tags

String tags of an S7-300 controller can have a maximum of 210 characters. Read and write access to linked HMI tags with String data type is therefore also limited to 210 characters.

Panel: Device name in WinCC Unified Certificate Manager

The device name of a panel is made up of:

- Prefix
  For Unified Comfort Panels: `UCP-`
  For Unified Basic Panels: `UBP-`
- MAC address
  You can find the MAC address:
  - On a UCP:
    Under "Control Panel > System properties > Panel information" in the field of the interface used (field "PN-X1 MAC address" or "PN-X2 MAC address")
  - On a UBP:
    Under "Control Panel > System properties > Panel information" in the "PN-X1 MAC address" field

  The separator character "-" from the MAC address is not part of the device name.

Example of the device name of a UCP: `ucp-3013891244fa`

Note

Read the device name in the Smart Client

The top left corner of a Smart Client shows the panel to which the Smart Client is connected. The displayed string consists of the device name and the postfix `:0`.

Tags

Reading and writing of arrays

For arrays that are not configured as a BlockArray, the Read and Write methods are supported only for individual array elements. Do not call the methods at the higher-level array tags.

If you want to read or write multiple individual array elements, use JavaScript loops or configure the tag as a BlockArray.

The tags are either read from the tag image (cache) or directly from the PLC, or written directly into the PLC. When the tag image is used, the method registers all tags that are not yet registered. You should use the tag image for cyclic reading/writing of tag values. If you do not need the tag value cyclically or the update cycle of the tag is too long, use direct readout (HMIRuntime.Tags.Enums.hmiReadType.hmiReadDirect) or writing (HMIRuntime.Tags.Enums.hmiWriteType.hmiWriteNoWait).

Arrays as block

The following data types are not permitted for read or write access to an array as a block via an external HMI tag in the PLC:

- DateTime
- LTime
- WString

String is not displayed

Affects Unified Basic Panels, Unified Comfort Panels and Unified PCs if they should display a tag of the type String from an S7-300/400 PLC under Unified Runtime.

Long strings from an S7-300/400 PLC cannot be displayed by Unified Runtime.

Divide long strings into multiple tags so that they can be taken from the PLC.

Trigger tags

If you dynamize a property of a screen object using a script triggered by a trigger tag, note the following:

- Writing the tag value within a script of a property dynamization that has this tag as a trigger tag could result in endless loops and thus impaired performance.
- The use of a method to write the tag value of the trigger tag in the same code line in which the tag object is defined results in a corresponding warning on compilation.
  Example:
  ```
  let tag1 = Tag("Tag1").Write(1234);
  ```

If a scheduled task has a tag as trigger condition, note the following:

- Writing the tag value by means of a system function within a scheduled task that has this tag as a trigger condition can result in endless loops and thus impaired performance.

Address multiplexing of tags

Address multiplexing of tags only works with tags that have the quality code "Good". If you use address multiplexing for an array and use an internal HMI tag as the index tag, you must assign a start value for the index tag. Otherwise, the quality code is “Uncertain” when Runtime is started and the respective value of the array is not available.

System tags

The system tag "@SystemActivationState" signals whether Runtime is active and can have the following values:

- System startup in progress (1)
- System started (activated) (2)
- System stopped (3)
- System shutdown in progress (4)
- System restart in progress (5)

In a redundant system, @SystemActivationState_1 signals the state of the active partner and @SystemActivationState_2 signals the state of the passive partner.

The information that Runtime provides for the @SystemActivationState tag for the redundant system is the same as that for the active partner.

Notation for the data type: LTime

LTime has a granularity of 100 ns.
Recommended operators for comparisons with LTime: <=, <, >=, >
Do not use: ==, <>

Logs

Restoring log segments in Runtime

If you restore an archive segment via Runtime Management or the system functions, observe the following notes:

- If you monitor the restored data in a control and display the online data at the same time, a data gap may occur as soon as the oldest segment of online data is automatically deleted in accordance with the configuration. This automatically deleted segment is not included in the restored logging data or in the current online data and is therefore missing from the timeline.
- If you delete an archive segment from the backup, you can still restore the remaining data. In this case, after recovery, an alarm appears that the log segments have only been partially restored.

Database for simulation

The configuration of the storage location is ignored during the simulation. Instead, a new relative folder is used, which is created in the path configured in "WinCC Unified Configuration".

File size of archived projects

The file for an archived project can be unexpectedly large if the "Optimize the size of high-resolution raster graphics" option is activated in the Runtime settings for one of the configured HMI devices under "General > Screen".

Activate the "Discard restorable data" option when archiving the project.

The archive size is considerably smaller. Corresponding data is not lost and can be restored.

Transfer log to another PC

If you are using MSSQL, follow these steps:

1. Use the "TIA Updater Corporate Configuration Tool" to configure the new PC.
2. Make sure that the configuration of the new PC corresponds to the configuration of the replaced PC.
   Make sure that the following settings are identical:
   - Names of the Runtime project
   - Runtime settings
   - Paths to the databases and to the MSSQL server instance.
3. Stop Runtime.
4. Create backups of the databases with the MSSQL Management Studio.

5. Copy the backups to the new PC.
6. Use MSSQL Management Studio to restore each of the databases individually. Make sure that the path to the databases is identical to the path that has been configured on the replaced PC.

Logging cycle for cyclic logging

For cyclic logging, you must select the logging cycle manually. The system notifies you if you select a time that is not supported.

The cycle times 100 ms and 250 ms cannot be configured for cyclic logging.

Select the longest possible logging cycle, as cyclic logging places a heavy load on the system.

The smallest configurable cycle time is 500 ms.

To avoid unnecessary load on the system, we recommend using the "On change" logging mode instead of cyclic logging.

Changing the logging mode

Once you have selected a logging mode, you cannot change it. Instead, create a new logging tag.

Download to device - Internal error due to unsupported path specification

If an unsupported path is specified as the storage location for logs, this can lead to an internal error when loading the project.

Relative path specifications are not supported.

Example

"`.../test`" is not a valid storage path. Runtime attempts to create such a folder with a relative path under "system root", where this is not permitted.

Solution

Enter an absolute path including the storage medium as the storage location.

User management

Two local users whose names differ only in upper/lower case, e.g. "Siemens" and "siemens", are not transferred correctly in UMC. An error message is displayed when loading the project and users cannot be logged in to Runtime. Avoid user names that differ only in upper/lower case.

Redundancy

Restriction for plant objects

Plant objects are not yet supported for redundancy. Using plant objects in a redundant project has the result that Runtime cannot be started completely (partly running).

Restrictions for web client switchover

After a web client switchover, the screen settings of the control, e.g. alarm filters, are reset, even if they were saved before the web client switchover.

Audit

The "Force" settings of the Audit Trail are not supported in WinCC Unified.

The "HmiCheckLogIntegrity" tool for checking changes in the Audit Trail is not supported in WinCC Unified.

Faceplates

Opening a faceplate as a popup from a popup

If you call a faceplate as a popup from within a popup, the popup faceplate will no longer be updated once you close the calling popup.

Style preview

The style for displaying all the faceplate instances in Runtime is specified in the Runtime settings of an HMI device. In the editor, you see a preview of a selected style, but this does not affect the display in Runtime. When a faceplate type is opened, the last style selected as a preview is always used as the style preview.

Faceplate types: Use and visibility of layers

The documentation of the faceplate types has been improved. Observe the following when using layers in faceplate types:

Note

Use and visibility of layers

As in screens, you can use layers in faceplate types to edit the screen objects in a differentiated way.

Note that the visibility of layers in the Engineering System and Runtime is controlled separately. The display in Engineering System has no influence on the display in Runtime. To show or hide a layer in Runtime, adapt the "Runtime visible" property in the Inspector window of the faceplate type under "Properties > Properties > Miscellaneous > Layers".

Parameter set control

Configuration limit parameter set type elements

Unified PC and Unified Comfort Panel support a maximum of 4 000 parameter set type elements.

Filter parameter sets

If you use the filter function to filter parameter sets in Runtime, please note the following information:

Note

Only elements that contain the search term at the beginning of the element name are found.

Example: The "Concentrate" element is found using the "Con" search term; the "onc" search term returns no results.

Use of resource lists

No tags of the "Char", "Bool" or "Real" data type can be used to select a list element.

Create edit tag

If you use edit tags, the procedure differs depending on whether you create the parameter set type using an HMI or a PLC user data type.

To use edit tags when creating the parameter set type using **HMI** user data types, proceed as follows:

1. Duplicate an HMI user data type in the library.
2. For the duplicate, change the connection to "Internal connection".
3. Create a tag that you want to use as an edit tag and change the scope of the tag to "Session local".
4. Assign the duplicated HMI user data type to the edit tag.

To use edit tags when creating the parameter set type using **PLC** user data types, proceed as follows:

1. Manually create an HMI user data type that has the same structure as the PLC user data type and an internal connection.
2. Create a tag that you want to use as an edit tag and change the scope of the tag to "Session local".
3. Assign the HMI user data type to the edit tag.

Note

Structure data types are not supported in HMI user data types and therefore cannot be used for edit tags.

Configure parameter sets: Use all system functions and JavaScript functions for parameter sets

To use all system functions and JavaScript functions for parameter sets (ParameterSet), an edit tag must be created for the corresponding parameter set type (ParameterSetType). The edit tag must then be linked to the parameter set type. The edit tag is used as a buffer for parameter sets. For more details, refer to the respective help for the system functions and JavaScript functions.

Disabled system folders (Linux)

The following system folders are disabled for the export and import of parameter sets and are no longer available for selection:

- /home/industrial
- /home/industrial/.local/share/Trash/files
- /net/mount (if mounted)
- /media/simatic/X51 (if mounted)
- /media/simatic/X61 (if mounted)
- /media/simatic/X62 (if mounted)
- /media/simatic/X63 (if mounted)
- /media/simatic/X64 (if mounted)

System behavior: Importing exported parameter sets again

If you export parameter sets and delete a parameter set in the exported file, this parameter set will still be present after importing the edited file.

By exporting and reimporting parameter sets, you can add new parameter sets or modify existing parameter sets. You cannot delete parameter sets in this way.

Sorting of the columns via the object properties of the parameter set control

The sorting of the columns via the object properties "Sorting order", "Sorting direction - default" and "Allow sorting" under "Properties > Miscellaneous > Parameter set - view > Columns" is not supported by the parameter set control.

Alarm control

To configure the alarm control output, the following setting options can be defined under "Miscellaneous > Alarm statistics - Settings":

- Start time
- Time range - start
- Time range - base
- Time range - factor

The maximum number of alarms is not supported in "Alarm statistics - Settings".

Trend control

Insert a manual break into the label

Under "Properties > Properties > General > Trend areas > Time axes below > [0] Time axis > Output format", you can select a desired time format and edit it manually. You can insert a line break with "`\n`".

You must put the "\n" in single quotes inside the curly brackets "{}": `'\n'`

Examples: `{D,@yyyy-MM-dd'\n'HH:mm:ss}`, `{D,@yyyy-MM-dd}\n{T,@HH:mm:ss}`, `{D}\n{T}`

Button

Transfer format

Use the "Transfer format" function to transfer the "Miscellaneous > Visibility" property from one button to another.

All other properties in the "Miscellaneous" category cannot be transferred.

Process control

The process control is only supported for Runtime on a Unified PC. The control is not available on Panels.

System functions

"EjectStorageMedium()" system function

The "EjectStorageMedium()" system function is available on Unified Comfort Panels and on Unified Basic Panels.

The description of the "Storage device" parameter of the "EjectStorageMedium" system function is as follows:

Parameter	Description
Storage device	Specifies the external storage medium to be ejected: • SD-X51 • USB-X61 • USB-X62

"StartProgram" system function

The "Display mode" parameter of the "StartProgram" system function determines how the program window is displayed on the HMI device. This function has no effect on Linux systems.

This parameter is reserved for future use.

"ExportUserAdministration" system function

- The system function "ExportUserAdministration" internally adds the .udz extension to the specified file name.
  The user management file can be imported in `udz` or `json` format.
  When importing in `json` format, you need to explicitly specify the file extension.
  When importing in `udz` format, you can specify the file extension. However, this is not necessary.
- After the file is exported, renaming or removing the file extension by the user will result in an invalid file. The file can no longer be imported.

The Control Panel can export both `udz` and `json` format. The system function only supports `udz` format.

System functions "IncreaseTag", "SetBitInTag", "ResetBitInTag", "DecreaseTag"

If the value of a GMP-relevant tag is changed using one of the system functions "IncreaseTag", "SetBitInTag", "ResetBitInTag" or "DecreaseTag", the changed bit is recorded in the Audit Trail, not the new value.

System function “StopTagLog”

If you stop logging during Runtime using the "StopTagLog" system function, the affected tags are marked as invalid via the quality code. This signals that no more incoming values are expected. However, the database requires that a value is written each time. The written value depends on the data type and corresponds to the default value of the data type, which means "0" for numeric data types and " " for text data types.

If you visualize an affected logging tag, for example, in a trend control, this default value will be displayed until logging is resumed.

Runtime scripting

Sequence of execution of events and scripts in Runtime

The "Loaded" event occurs when the **static part** of a screen or faceplate container is fully loaded after a screen change or Runtime start.

Dynamizations are only executed in parallel after a screen has been loaded.

"ParameterSetType.GetName" and "ParameterSet.GetName" methods

- If the language ID of the default language is specified, the name is returned.
- The display name is returned for other language IDs. If no display name is configured, the name is returned.
- The return of the methods is not correctly described in the documentation. In case of a successful promise, the name of the parameter set type or the parameter set is returned. In addition, a script example for using the "ParameterSetType.GetName" method:

```
let pstNamePromiseObject = HMIRuntime.ParameterSetTypes
(1).GetName (0);
pstNamePromiseObject.then(function(val){
  HMIRuntime.Trace("ParameterSetType name:" + val);
}).catch(function(errorcode){
 HMIRuntime.Trace ("Exception");
});
```

"hmiReadDirect" method

The "`hmiReadDirect`" method cannot be used in Runtime scripts. Using the method causes Runtime to be aborted.

The "`hmiReadDirect`" method is part of the "`HMIRuntime.Tags.Enums.hmiReadType`" enumeration. The enumeration can be used.

"ParameterSet.ReadAndSave()" method

The correct syntax of the "ParameterSet.ReadAndSave()" method is:

```
ParameterSet.ReadAndSave(OverWrite, OutputStatus)
.then(function() {
    ...
```

```
})
.catch(function(errorCode) {
    ...
})
```

"UserManagement.GetRolesFromUser()" and "UserManagement.HasUserRole()" methods

The UserManagement.GetRolesFromUser() and UserManagement.HasUserRole() methods do not provide a meaningful return value when used in a scheduled task, as no user is assigned to a task.

Do not use the method in scheduled tasks.

"Authorization" property

Reading the "Authorization" property is currently not supported.

"ReadElectronicRecord()" method

When using the system function "ReadElectronicRecord()", transfer the parameters "`dateFrom`" and "`dateTo`" into the Date Time String Format without time zone offset (UTC time): "YYYY-MM-DD HH:mm:ss.ttt"

"SysFct.ExecuteToolbarButton()" method

For the "`systemDiagnosisControlID`" parameter, the control IDs "`Previous (2)`" (previous) and "`Next (3)`" (next) are only supported up to V17 inclusive.

In the current version of WinCC Unified, this information is obsolete because the buttons are no longer supported.

"SysFct.CreateGetAndClearTagCommand" method

The correct syntax is "[HMIRuntime.]Tags.SysFct.CreateGetAndClearTagCommand(TagName);".

"LoggedAlarmStateResult.HostName" property

The data type of the "HostName" property is "String".

"Tag.Write" method

The example has been corrected in the documentation.

The correct syntax is:

```
let tag1 = Tags("MyTag1");
tag1.Write(1234, HMIRuntime.Tags.Enums.hmiWriteType.hmiWriteWait);
```

"DataSet" object

The "DataSet" object can store values of alphanumeric data types, such as "Number", "String" or "Bool" and "DatabaseConnection" objects.

"Label" object

The "Label" object described in the document "WinCC Unified JavaScript Object Model" is not supported.

Reading quality code and time stamp

The quality code and time stamp of a PLC tag can only be read with the help of a script using an internal script tag.

Example:

Realization of the LiveBit functionality for checking the connection status to the PLC

```
HMIRuntime.Tags.SysFct.ResetBitInTag("LiveBit",0);
// This code is suitable
let live = Tags("LiveBit");
live.Read();
HMIRuntime.Trace("LiveBit changed" + "Q-Code:" + live.QualityCode +
"Timestamp:" + live.TimeStamp);
// This code is not suitable
Tags("LiveBit").Read()
HMIRuntime.Trace("LiveBit changes" + "Q-Code:" +
Tags("LiveBit").QualityCode  + "Timestamp:" +
Tags("LiveBit").TimeStamp);
```

Alternatively, use the properties of the "TriggerDataSet" parameter introduced in version 19.2 in tag-triggered scripts.
Using this parameter, it is possible to access the respective properties of the "TriggerTag" directly via "`triggerDataSet("TriggerTag").QualityCode`" or "`triggerDataSet("TriggerTag").TimeStamp`".

"DataGridControl" object

The "DataGridControl" screen object is not implemented in Unified Engineering and has therefore been removed from the WinCC Unified JavaScript object model and the associated documentation.

"RestoreAlarmLog" and "RestoreTagLog"

The types of the "Log" parameter of the JavaScript functions "RestoreAlarmLog" and "RestoreTagLog" are now correctly described as "HMIAlarmLog" and "HMIDataLog".

Adapt screens to a new HMI device - Resize to display

If you replace an HMI device and the screen size is different, you can adapt the existing screens to the new screen size. To do this, use the "Resize to display" function in the context menu of a screen.

When using this function, note:

- The function considers the current dimensions of the screen relative to the screen size of the HMI device at the time the screen was created. The adjustment is made relative to the size ratio between the current dimension of the screen and the dimension of the original device, as well as between the dimension of the original device and the dimension of the new device.
  Example:

Screen size (original HMI device)	800 x 480
Screen size (new HMI device)	1366 x 768
Screen size (original)	800 x 400
Screen size (after fitting to screen size)	1366 x 640

  The system first determines the width and height ratio of the old and new screens:
  - Width: 1366 / 800 = 1.7075
  - Height: 768 / 480 = 1.6

  These values are used to multiply the width and height of the original screen:
  - Width: 800 x 1.7075 = 1366
  - Height: 400 x 1.6 = 640
- The function checks which HMI device the screen was created on and **always** scales it in relation to the new device. If you have already manually adjusted the screen size and then use the function, the screen will be enlarged or reduced by the corresponding scaling factor - regardless of whether, for example, the maximum resolution is exceeded. After using the function, the screen is treated as if it had been created on the new device and can only be resized to screen again after another device change.
  Example:

Screen size (original HMI device)	800 x 480
Screen size (new HMI device)	1366 x 768
Screen size (edited after device change)	1366 x 200
Screen size (after fitting to screen size)	2332 x 320

  - Width: 1366 x 1.7075 = 2332
  - Height: 200 x 1.6 = 320
- Rounding to integers may cause the new dimensions to deviate by ±1 from the desired ratio. This is usually visible in Runtime by scroll bars on the screen window (at +1) or by a background line on the edges of the window (at -1).
  Example:

Screen size (original HMI device)	800 x 480
Screen size (new HMI device)	1366 x 768
Screen size (original)	400 x 214
Screen size (after fitting to screen size)	640 x 342 (unrounded 640 x 342.4)

Runtime settings

Replacement character set

The replacement character set is provided by the system. The character set is used if a configured character set is not available on the system. The default replacement character set is "Siemens Sans". This font may not be able to display certain language-specific characters. When compiling a project, you will receive a warning if the replacement character set is used.

To show texts with different character sets, enable the "Activate language-compatible font families" option in the Runtime settings under "Language & font". When the option is enabled, you can select a language-compatible replacement character set for the Runtime languages. Font families that are suitable for displaying the respective Runtime language are offered.

Alternatively, deactivate the "Use same font for all languages" option under "Settings > Visualization > Screens > General". Assign a separate character set to each screen object in the properties of the object.

Automatic updating of alarms

If the "Automatic update" is deactivated for a connection in the Runtime settings of an HMI device under "Alarms", the alarm system is not initiated for this connection so that no PLC alarms are received.

If the "Automatic update" option is deactivated, no alarms are received from an S7-1200/1500 PLC. In this case, a configured alarm control does not show any alarms.

For the PLC S7-1200 there is no support for "Central alarm management" in the PLC. Therefore the user can disable this option while communication between an HMI device and the PLC is taking place.

Automatic updating of alarms

Under "Tags > Tag notification behavior", you can activate the "Ignore time stamp change" setting. Please note the following information:

Note

Tag logging

The "Ignore time stamp change" setting has no effect on the logging of the tag value.

Connections

Connection without Secure Communication

Note

Deactivating this option increases the security risk.

A connection between Runtime and a PLC without certificate is only possible if the PLC does not support the use of certificates, e.g. PLCs with older firmware or other series.

It is essential to configure a certificate in the PLC for secure communication.

Change with system function "ChangeConnection"

An HMI device has been connected to a PLC using the "ChangeConnection" system function.

Note

The HMI device does not initially trust the PLC certificate after calling the system function. To establish a secure connection, you must trust the certificate manually.

The following scenarios can occur in combination with the system function:

- Source PLC (configured self-signed TLS certificate) ⇒ "ChangeConnection" system function ⇒ Target PLC (configured self-signed certificate)
  You can manually trust the certificate for Unified Comfort Panels and Unified PCs.
  - Unified PC: SIMATIC Runtime Manager > Settings > Certificates
  - Unified Panel: Control Panel > Security > Certificates
- Source PLC (CA-signed certificate) ⇒ "ChangeConnection" system function ⇒ Target PLC (CA-signed certificate from the same CA as the source)
  The new connection to the target PLC is established automatically without any further action. The TLS certificate is not shown in the certificate management and it is not necessary to trust it manually.
- Source PLC (CA-signed certificate) ⇒ "ChangeConnection" system function ⇒ Target PLC (CA-signed certificate from a CA other than the source)
  The new connection to the target PLC cannot be established. The TLS certificate is not shown in the certificate management and cannot be classified as trusted. The manual import of the CA of the target PLC also has no influence.

UaExpert: Free OPC UA client for testing purposes

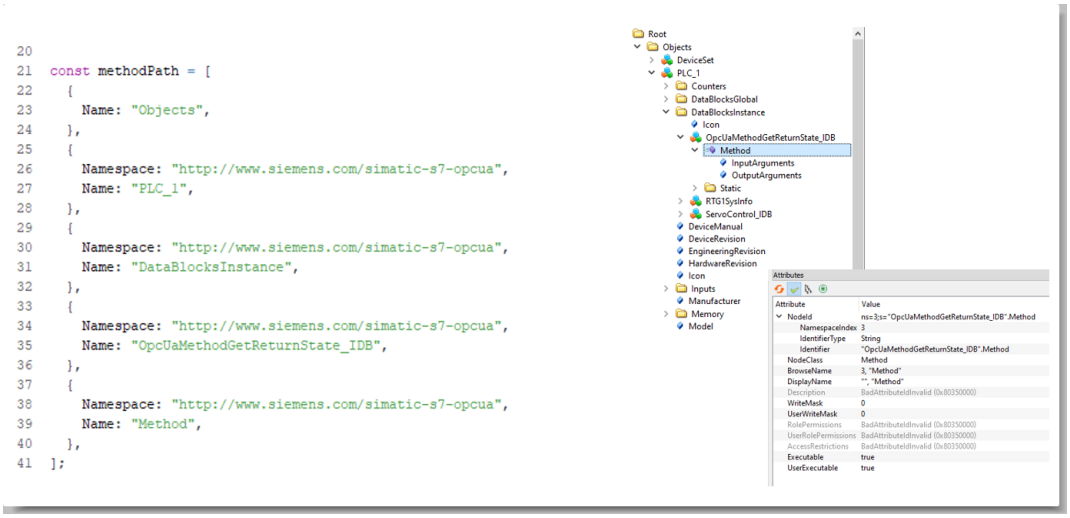
The OPC UA client "UaExpert" communicates directly with the OPC UA server.

"UaExpert" supports the OPC UA functionalities Browse and Read/Write.

Connect UaExpert to an OPC UA server. In the "AddressSpace" of the OPC UA server, you can see the OPC UA nodes that you have configured in the configuration of the OPC UA server interface. In the "DataAccessView" area, you can monitor and edit data.

"UaExpert" is a tool provided by a third-party vendor.

Use UaExpert to determine the correct path to a method.



Runtime does not start after multiple changes to the device version

Under the following conditions, it is possible that a Unified device is compiled and loaded but Runtime cannot be started:

- You use structured PLC tags in the configuration of a Unified device.
- You have upgraded the device to device version 20.0.0.2.
- You have compiled the device and saved the project.
- You change the device version to a lower version, e.g. 20.0.0.0.
  If you have no access to the project before the upgrade, delete the folder with the Runtime IDs of this device in <project folder>\AdditionalFiles\RtIdFiles\. If multiple folders are located in <project folder>\AdditionalFiles\RtIdFiles\, compile the device again and delete the folder with the most recent time stamp in <project folder>\AdditionalFiles\RtIdFiles\.

Runtime call error - HTTP Error 500.19

If you receive the “HTTP Error 500.19” error when you call Unified Runtime, follow these steps:

1. Start the Internet Information Services (IIS) Manager.
2. Select the computer name.
3. Open the entry "Management > Feature Delegation".
4. Ensure that the entry "Modules" has the setting "Read/Write".

You can then use WinCC Unified RT as usual.

Language after starting Runtime

After starting Runtime, the language for which the lowest number has been configured in the Runtime settings is always set.

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 has not been set in the central user management, the language for which the lowest number has been configured in the Runtime settings will be set.

"User profile settings" button

The "User profile settings" button in the toolbar is not supported on Unified Basic Panel and Unified Comfort Panel for the following objects:

- Alarm control
- Trend control
- Function trend control

Updating the search index in a project

The search index in a project is automatically recreated when the project is upgraded from one major version to the next version, e.g. from V19.02 to V20.

If a project is opened after an update, the search index is not updated.

Example: A project created in V20 will open in V20 Update 3.

You manually recreate the search index under "Settings > General > Search in project" with the "Recreate search index" button.

IPI proxy with extended PLC user data type

If you have expanded a PLC software unit with a PLC user data type and then export the PLC proxy and update the existing PLC proxy in another project, you must fully compile first the PLC and then the HMI device after the import.

Data loss when changing PLC user data types

Changes to the elements of a PLC user data type (e.g. name or data type) can cause the configuration of the elements of the user data type (e.g. projected logging tags) to be lost on the HMI device. In this case, even a reconfiguration (for example re-creating a logging tag with the same name) does not lead to a connection to the existing values in Runtime.

To avoid data loss in Runtime, it is recommended to make a copy of the engineering project and a backup of the Runtime project before making any changes to the elements of PLC user data types.

Startdrive V20 SP1

If you want to configure both Startdrive and WinCC in TIA Portal, the use of Startdrive V20 SP1 is recommended for TIA Portal V20 Update 3

Rendering error with OGV videos in the media player

Videos in OGV format that use the Theora codex are not rendered in the media player.

Encode the video with a codex supported by Google, for example vp8 or vp9, and use this video encoding.

Rendering HMI screens

Unified PC Web clients, Panel Web clients and simulations use a different rendering for HMI screens than the Engineering System and Panel Runtime. Therefore, deviations in the rendering of HMI screens are possible in the following cases:

- Fonts with fixed character width can be rendered with deviating line spacing.
- Texts with tabulator characters can be rendered with deviating width.

Runtime API - Connection to a Collaboration device

In C#, the `Connect()` method of the `IRuntime` interface is overloaded. This allows you to connect to a specific Runtime project.

If the Runtime project is a Collaboration project, the Collaboration name of the project must be transferred as parameter when the method is called.

Cybersecurity information

3

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**	**Direction**	**Function**	**Description**
ILScs Manager	20008	TCP	Inbound, Outbound		• Download Runtime projects, including release management checks. • Start and stop Runtime • Performing online backups • Transfer files (from ES to device)
UMC	443	HTTPS	Inbound, Outbound	Centralized user management	The service enables the central management of users and user groups across different software and device platforms.
ILPmon Manager	4999	TCP	Inbound, Outbound	Communication monitoring	The service monitors and manages various processes and communication protocols within a network.
ILEvent Manager	1235	TCP	Inbound, Outbound	Event management	The service is responsible for managing and processing events.
ILDist Manager	4777	TCP	Inbound, Outbound	Data management	The service is responsible for the distribution and management of data between the systems.

WinCC Unified					
ILDataManager	1234 5001	TCP	Inbound, Outbound	Data management	The service is responsible for the management and processing of data within the system.
Node Processes	3103 443 8888	TCP	Inbound, Outbound	Scripting	The service is responsible for the management and execution of Node.js processes within the system. This enables the integration and use of Node.js libraries and scripts.
Graphics Runtime	1339 1345	TCP	Inbound, Outbound	Visualization	The service is responsible for the display and execution of the graphical user interfaces. It ensures that the visualizations and user interfaces are displayed correctly and can be used interactively.
License server	1366	TCP	Inbound, Outbound	License management, license provision	The service is responsible for the management and provision of licenses required for the operation of WinCC Unified software.
Screen debugger	9222	TCP	Inbound, Outbound	Script debugging	Port used for the script debugger for scripts that refer to screens. Can be changed in the Runtime Manager settings.
Job debugger	9224	TCP	Inbound, Outbound	Script debugging	Port used for the script debugger for scripts that refer to jobs. Can be changed in the Runtime Manager settings.

WinCC Unified					
WCCIL Proxy Manager	5678	TCP	Inbound, Outbound	Access management	The service enables access to runtime objects, such as screens, from other HMI devices and their display and operation
WCCILRedu	4410	TCP	Inbound	Monitoring system availability	The service is responsible for redundancy management. It ensures that the system continues to function even if a subsystem fails.
Network Discovery (IS)	34964, 5337	PROFINET	Inbound, Outbound	Network overview	This is used to automatically detect and manage network devices within the industrial network.
UMC AttachAgent	443 Configurable, e.g. 4002	HTTP	Inbound, Outbound	Centralized user management	The service is part of the User Management Component (UMC). It enables the integration and management of users and user groups.
OPC UA Discovery	4840	TCP	Outbound	Automatic discovery, security management	Port reserved by the Local Discovery Server (LDS) for the discovery of OPC UA servers in the network.
RFID	443 configurable, e.g. 5003	HTTPS	Inbound	Access control, process security	The service is mainly used for user identification and administration. RFID (Radio Frequency Identification) allows users to log on to WinCC Unified Panels or PC runtime systems quickly and securely.
GraphQL	4000	TCP	Inbound, Outbound	Reading and writing of process values, management of alarms	Port reserved by the GraphQL server.

Unified Comfort Panel					
Name	**Port number**	**Transport protocol**	**Direction**	**Function**	**Description**
HmiRuntime	1234	TCP	Inbound, Outbound	Visualization of processes	The service provides the user interface on the HMI device and the interaction between the HMI device and the automation system.
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	Inbound, Outbound	Monitoring and management	The service enables the monitoring and management of network devices such as routers, servers, switches and printers from a central station.
FwPnManager	34964	UDP	Inbound, Outbound	Monitoring and management	The service is responsible for managing and monitoring firmware and PROFINET components.

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".

Engineering and runtime

4

4.1 Improvements in Update 4

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Screens and screen objects

Texts with the "Font Awesome 5 Free Solid" font are displayed correctly in the Engineering System and in Runtime.

A selected option is displayed correctly in the option field and in the check box on Unified Control Panels in Runtime.

The "Button" object is displayed correctly when pressed and moved on a Unified Panel, in the simulation and in the SmartClient.

Process diagnostics

The display of ProDiag alarms in Unified Runtime has been improved and the language switchover between Swedish and English now functions correctly.

Importing of STEP 7 Classic projects is possible again

With STEP 7 version V5.7 SP3 installed, the import of STEP 7 Classic projects via the device proxy is possible again.

4.2 Improvements in Update 3

4.2.1 Improvements in Update 3

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Upper/lower case of the user name

When checking the user name, upper/lower case is no longer checked in the following cases:

- During DSSO login to Runtime (DSSO = Desktop Single Sign-On)
- When entering an electronic signature for Audit

Runtime settings: Language-compatible font families

You can use project languages that cannot be displayed with the standard "Siemens Sans" character set.

To centrally configure font families that are compatible with the Runtime languages used, enable the "Activate language-compatible font families" option in the Runtime settings of the HMI device under "Language & Font > Font family settings".

If this option is activated, select one of the font families installed on the device for each Runtime language in the "Replacement character set" column.

True type font families are supported.

Upgrade scenarios for custom styles

If you have a custom style that is based on a V18 template and you upgrade your TIA Portal project to V20 Update 3, the following applies:

- If the MTP device uses device version V18, the use of the existing V18 custom style is not supported. The use of the V18 custom style can lead to a compilation error.
- If the MTP device is upgraded to V20 Update 3, generate a new custom style based on V20 Update 3. Use this new custom style.

Changing styles when a screen is open

Display errors in an open screen that occurred when changing a style in the Runtime settings have been fixed. If you instantiate a faceplate type with a specific style in a screen and then select a different style in the Runtime settings, all screen objects are displayed correctly.

Formula with "Range" evaluation type

If floating point numbers are used in the formula in the "Range" evaluation type, the result is displayed correctly in Runtime.

Position of faceplates in pop-up

The position of pop-ups has been improved.

When you open a faceplate via the "OpenFacePlateInPopUp" method, the pop-up opens at the correct position, depending on the "IndependentWindow" parameter.

Snippets for the dynamization of faceplate types

The "Subscribe to property changes of a faceplate popup window" snippet for the dynamization of faceplate types has been improved. The created code now works without errors.

Dynamic SVGs in faceplates

Color dynamizations for dynamic SVGs in faceplates have been improved. Dynamization now works correctly even when flashing is enabled.

Interface properties of faceplates

An array must not be assigned to an interface property of type WString. An attempt to assign an array is now recognized and rejected by Runtime.

Visibility of nested faceplates

The visibility of nested faceplates has been improved. If the outer faceplates are visible, the inner faceplates are also visible. If the outer faceplate is invisible, so are the inner faceplates.

"ReadAndSaveParameterSet" system function

Successful execution of the "ReadAndSaveParameterSet" system function no longer generates an error message in Trace Viewer.

Runtime scripting - "ReadMaxAge" method

If you call ReadMaxAge for a tag, the current tag value from the PLC is now also always returned in faceplates.

Runtime scripting - "GetSelectedAlarmAttributes" method

Problems with the "GetSelectedArmatAttributes" method have been fixed. The properties of the alarms are returned correctly.

"LeaveFullScreen" and "EnterFullScreen" script functions for kiosk mode

Calling the `HMIRuntime.UI.Kiosk.LeaveFullScreen()` script function in Runtime terminates kiosk mode without simultaneously ending the Runtime display.
The `HMIRuntime.UI.Kiosk.EnterFullScreen()` script function allows the kiosk mode to be started from Runtime.

LeaveFullScreen()

Ends kiosk mode and switches to window mode. As a result:

- Access to the functions of the operating system is possible.
- Runtime is still displayed in a client.
  The client has the following buttons:
  - Minimize: Minimizes the client window.
  - Maximize: Maximizes the client window.

Note

Call Alt+F4

If Alt+F4 has been configured to exit kiosk mode and users press Alt+F4 while the mouse pointer is in the client, the client is closed.

If users press Alt+F4 while the mouse pointer is outside the client, Microsoft Windows is locked.

EnterFullScreen()

If the conditions for starting kiosk mode are met, kiosk mode starts. If the client is in window mode, the client switches to kiosk mode.

Expressions

Performance when loading screen objects with a property dynamized via an expression has been improved. If the expression is not linked to a tag, the screen object is now loaded faster.

Line breaks in Runtime and simulation

The display of line breaks for Unified Panel and Unified PC has been standardized. Line breaks are now displayed the same in simulated projects and in projects with the "RUN" status.

Double line breaks in a text box

In Runtime, duplicate line breaks are displayed correctly in a text box.

Texts from library objects

After a screen change, the text from library objects is displayed correctly.

Text boxes

- The text alignment in text boxes has been improved. The texts are now displayed correctly in the Unified Screen Editor (Next Gen.) and in Runtime.
- Changes to the border width of a text box no longer affect the position of the text in the text box.

"Allow operator control" for grouped screen objects

The behavior of grouped screen objects has been improved. The value of the "Allow operator control" property is now correctly read and applied in Runtime for all objects in a group. This also applies after a change of value during Runtime.

Gauge

The display of the "Gauge" element has been improved.

IO fields

- Line breaks in IO fields
  In the IO field, defined line breaks, e.g. between date and time, are displayed correctly and consistently in Unified PC and Unified Comfort Panel
- Values of the output format {P,DD hh:mm:ss} are correctly displayed in the IO field if a tag of the "Real" data type is connected.
- Scrolling in symbolic IO fields has been improved on touch devices.
- When a custom style is used, IO fields are now correctly displayed in Runtime if the customer creates a new custom style based on a V20 Update 3 template.

Symbolic IO fields with graphics lists

If a symbolic IO field uses a graphics list and users open the corresponding drop-down list in Runtime, the graphics stored in the graphics list are displayed correctly.

Configure parameter sets: Adapting field labels

You can adapt the labels of the "Parameter set type", "Parameter set" and "Number" fields individually and in multiple languages.

To do this, configure under "Properties > General" a static value or a dynamization for the following properties:

- "Number - label": Specifies the label of the "Number" field.
- "Parameter set - label": Specifies the label of the "Parameter set" field.
- "Parameter set type - label": Specifies the label of the "Parameter set type" field.

If you have enabled multiple Runtime languages, adapt the label for additional languages under "Texts".

Editing exported parameter sets

The options for editing parameter sets have been improved. You can open and edit the exported .tsv files in a spreadsheet. When opening, select the tab stop as separator. Make sure that consecutive separators are handled as one separator and no changes are made to the character coding.

Importing parameter sets in Runtime

The import of parameter sets in Runtime has been improved. If you export parameter sets to a TSV file, change a value and re-import the changed file, the import is now also successful if the last value has the data type string and is empty.

Parameter sets: Tracing

After successful execution of the "LoadAndWriteParameterSet" system function, the alarm "Failed to write to PLC" no longer appears in the Trace viewer.

Alarms

- The texts for system alarms relating to redundancy have been improved.
- Scrolling in the alarm control has been improved.
- The display of alarms in the alarm control has been improved. Long or broken alarm texts are displayed correctly and without delay.

Trend control

- The interface for displaying and setting the time has been corrected in the trend control, in the "Time selection" dialog. After a language change in Runtime, the time is displayed correctly and can be configured.
- The trend update can now also be started or stopped by changing the "Switch state" property of the "Start/Stop" button.

Time stamp in value table

The display of time stamps in the control value table has been corrected. Time stamps are never displayed with line breaks.

Trend control: Array as block

A trend control now represents external HMI tags with array as block as a trend with the values via the index. To configure such a trend, follow these steps:

1. Select the type "HMI_Variable" for "Properties > General > Trend areas > Trends > [0] Trend > Data source Y > Source".
2. Select an external HMI tag that accesses a PLC array tag with an array as a block.
3. Select "Index" as the setting of the time axis under "Properties > General > Time axes bottom > Time axis [0]".
4. Select the number of index values to be displayed for "Properties > General > Time axes bottom > Measuring points".

The last read data record of the array as a block from the external HMI tag is displayed in the configured trend control in Runtime.

For correct display of the block data of the array in Runtime, you must observe the following:

- There are two prerequisites for reading in a new data record of the array as a block in Runtime:
  - The trend control is in "Online" mode.
  - A script for manually reading the data record of the external HMI tag with an array as a block is implemented.
    A script can be linked to an event and realized as follows:
    `Tags(<block array tag>).Read(Tags.Enums.hmiReadType.hmiReadDirect)`
- To ensure the consistency of the block data of large arrays to be displayed in the trend control, implement a manual handshake procedure on the HMI and PLC side.

System diagnostics

- The display of tooltips for tiles in various screen styles has been improved.
- If a system diagnostic alarm had a line break, the word "undefined" was displayed.
  This problem has been fixed. Multi-line system diagnostics alarms are now correctly displayed with line breaks.
- The system diagnostics control now shows the complete text of an error description.
- After selecting a device tile in the matrix view, the correct error description is now displayed in the hardware detail view.

PLC code view

- The display of the tooltips within the PLC code view when using Remote Desktop has been improved.
- The slicing of variable values for comparison operations now works correctly.

Reports

Adjustment of the time stamp format in the "Reports" control

In the Engineering System, users have now the option to configure the time stamp format with which the date and time are displayed in the "Reports" control in Runtime. To that end, in the Engineering System, configure the "Time stamp format" property in the properties of the control under "Miscellaneous > Interface > General".

You have the following options:

- Select one of the preconfigured entries under "Date and time" or "Date and time (automatic, language dependent)".
- Enter the desired format manually in the field.
- Add a dynamization and apply the value, for example, from a tag.
  This will make it possible for you to change the time stamp format during Runtime.

Result:

- After the compile and load, all the specifications for date and time are displayed in Runtime in the "Reports" control in the format that you have selected.
  Excluded from this are:
  - Report names that contain the date and time
  - Specifications for the definition of series triggers on the "Task parameters > Triggers" tab in the "Trigger type" area
- If the property is empty or contains an incorrect value, the current Runtime language is evaluated and the standard format of the corresponding region is used.

Note

The configuration of the "Time stamp format" property does not affect the time stamps output in the generated report.

Tracing

The trace messages for faceplate instances have been improved. If the tag linked in the faceplate type in the tag interface is not available in Runtime, the trace message now supplies the name of the faceplate instance.

Panel: Displayed language

If a project language that does not support Runtime has been configured for a Panel in engineering, Runtime displays English instead.

Comfort Panel: Display local files via browser address bar

The display of local files of the UCP via the browser address bar has been improved.

Files stored under "media\SIMATIC_MC" on the UCP can now be viewed in Runtime in a browser, for example in the Control browser.

Example:
To display the file `file:////media/SIMATIC_MC/SDS.pdf`, enter the following URL in the Control browser: `https://localhost/webfile/SDS.pdf`

Comfort Panel: "ExecuteFunctionButton" in alarm controls

The "ExecuteToolbarButton" system function is correctly executed in the alarm control of the Unified Comfort Panel.

Comfort Panel: Trend control

The time range of trend view displays the date and time correctly.

4.2.2 Load user files

Introduction

You have the possibility to load your own files with useful additional information onto a Unified PC, e.g. system manuals, video tutorials or plant and project documentation files.

Files loaded onto the PC can be displayed as follows:

- In a web browser
- In a Runtime client: On an HMI screen in the "Browser" control

To update or delete user files, change the configuration of the user files in the engineering and load the project onto the device.

For changes to user files that have already been loaded, edit the configuration of the user files in the engineering and load the files again.

In Runtime, administrators can delete the folder with the user files.

Restrictions

- The HMI device is a Unified PC.
- The user files are only loaded onto the HMI device when fully loaded.
- The file formats that can be displayed depend on the browser and browser version selected to display them.
- To be able to open user files in Runtime, the following applies to the files and folders in the "UserFiles" folder:
  - The file names and folder names cannot contain a "+" character.
  - All other special characters in file names and folder names must be URL encoded in the address string.

Requirements

- Runtime version configured for the Unified PC and installed Runtime version: V20 Update 3

Workflow

1. Enable access to user files on the Unified PC.
2. In the Engineering System, configure which user files are loaded onto the device.
3. Load the files to Runtime.
4. Open the user files in Runtime.

Activating access to user files

1. Open the WinCC Unified Configuration tool on the Unified PC.
2. Switch to the "Download of projects" step.

3. Enable the "Activate access to user files" option.
4. Switch to the "Apply settings" step and click "Apply".
   The settings are applied.
5. Click "Complete".

Configuring user files in the engineering

In the engineering, you configure in the "HMI files" editor which user files are loaded to Runtime on loading.

You can create folders to improve structuring. Then you save the files in the folders.

NOTICE
Protection from malware Malware can be installed by opening a file, e.g. a PDF file with embedded links. Only upload files from secure locations into the editor. If necessary, scan files with an antivirus program first.

Requirements

- In the engineering, a project is opened with a Unified PC.

Procedure

1. In the project tree, open the "HMI files" editor under "Common data".
2. To add one or more new files, follow these steps:
   – Click "Add new" in the work area of the editor.
   A Windows Explorer opens.
   – In the Explorer, select the desired file(s) and click "Open".

   The files appear in the work area numbered and in alphabetical order.
   On the engineering PC, the files are saved in the file system under "<TIAProjectname>\UserFiles\HMI_globalFiles".

   Note

   If you change the contents of the "HMI_globalFiles" folder directly in the file system, the "HMI files" editor reflects these changes.

3. To store the files in a folder structure, follow these steps:
   – To add a folder, select an empty line in the work area and choose the "Create new folder" command in the context menu.
   In the "Create new folder" dialog, assign the folder name and confirm your entries.
   The folder appears in the work area.
   – To add a subfolder to a folder, select the line with the respective folder and choose the "Create new folder" command in the context menu.
   In the "Create new folder" dialog, assign the folder name and confirm your entries.
   The subfolder appears in the work area under the selected folder.

4. To add files to a folder, follow these steps:
   – Select the folder in the work area.
   – Select "Insert object" from the context menu.
     A Windows Explorer opens.
   – In the Explorer, select the desired file(s) and click "Open".

   The files are added to the folder.
5. To update an added file, follow these steps:
   – Click "Add new" in the work area of the editor or select the "Insert object" command in the context menu of a folder.
     A Windows Explorer opens.
   – In the Explorer, select a file with the same name as the file to be updated.
   – Confirm the prompt.

   The file is overwritten.
6. To delete one or more files, follow these steps:
   – Select the line(s) of the file(s) in the work area
   – Select "Delete" from the context menu.

Result

The files and folders stored in the editor are shown in the "Load preview" dialog and can be loaded onto the Unified PC.

Loading user files to Runtime

Requirements

- At least one file has been added in the "HMI files" editor.

Procedure

To transfer the user files configured in engineering into Runtime, follow these steps:

1. Select the Unified PC in the project tree in engineering.
2. Select "Download to device > Software (all)" in the context menu.
   The "Load preview" dialog is shown after a successful compilation check.
   The "Load" button is inactive.
3. Click the "HMI Runtime" entry.
   The number and total size of the files configured in the "HMI files" editor and a list of the configured files is shown under the entry.

4. Enable the option "Download all user files, including changed or newly added files from the list below".
   The "Load" button becomes active.

NOTICE
Protection from malware Malware can be installed by opening a file, e.g. a PDF file with embedded links. Only enable the option if you trust the files. If necessary, scan the files in the "<TIAProjectname>\UserFiles\HMI_globalFiles" folder with an antivirus program first.

5. Check the remaining default settings and change the settings as necessary.
6. Click "Load".

Result

If access to user files is enabled for Runtime, the contents of the "<TIAProjectname>\UserFiles\HMI_globalFiles" folder are mirrored in the "<Runtime project folder>\UserFiles" folder.

If a file from the "<Runtime project folder>\UserFiles" folder is being used in Runtime, this file is not overwritten. A warning informs you about it.

Opening user files in Runtime

Requirements

- A loaded project has the "RUNNING" status.
- The web browser or Runtime client has access to the web server.
- For opening in a Runtime client:
  The "Browser" control was configured for the displayed HMI screen.

Opening a file directly in the web browser

1. Enter the following URL in the address bar of a web browser:
   "`https://<IP address or FQDN of the Unified PC>/UserFiles/<file name or file path>`"

   Note

   Use the same computer addressing as for Unified Runtime.

2. Authenticate yourself with your UMC user name and password.

Opening a file in the Runtime client in the "Browser" control

1. Enter the following URL in the address field of the "Browser" control:
   "`https://<IP address or FQDN of the Unified PC>/UserFiles/<file name or file path>`"

   Note

   Use the same computer addressing as for Unified Runtime.

Result

The document is opened directly in the web browser or in the "Browser" control.

Deleting user files in Runtime

1. Start SIMATIC Runtime Manager as administrator.
2. Click "Settings".
3. Click on the "Telemetry - User files" tab.
   Under "User file settings", you will see the current storage location and the file size.
4. To delete the folder with the user files, follow these steps:
   - Click "Delete folder".
   - Confirm the prompt.
     The project is stopped and the folder and files are deleted.
   - Close the settings.
5. Start Runtime again.

4.2.3 Reading an array as block with handshake procedure

Introduction

To ensure consistency when reading large data records from arrays as block, implement a manual handshake procedure on the HMI side and PLC side.

The following is an example implementation for read access to an array as a block using a manual handshake procedure, for example to represent rapid changes in the value of a PLC tag in a trend control in an HMI screen:

Read access with handshake procedure

Requirements:

- The "TrendBufferTransfer_ReadRequest" tag is used in the HMI screen as a trigger for the request to read the array as block.
  - For a single request to read: The "TrendBufferTransfer_ReadRequest" tag must be set in script to dynamize a property from the HMI side and reset after the read access from the HMI side is completed.
  - If there is a permanent request to read in a screen: The tag must be set from the HMI side for the "Loaded" event and reset from the HMI side for the "Cleared" event.
- The "TrendBufferTransfer_DataAvailable" tag must be set by the PLC side when the array is ready for data transfer as block and reset by the HMI side as soon as the read access is completed.
- "TrendBufferTransfer_ReadRequest" and "TrendBufferTransfer_DataAvailable" are tags of the type "Int" or "Bool".

Script examples

There are two ways to implement the manual handshake procedure:

- The following script is triggered when a property is dynamized by a change in the value of the trigger tag "TrendBufferTransfer_DataAvailable".
  - In the event that the trigger tag is not set again within at least 200 ms after it has been reset.
  - The reason for this is a minimal query time of the trigger tag "TrendBufferTransfer_DataAvailable".
- The following script is triggered when a property is dynamized by a "Cycle" trigger with a desired cycle time.

Example script for HMI: Handshake procedure for reading an array as a block

Script to dynamize a property (cycle or trigger tag)

```
// Handshake tag to signal from PLC to HMI that block array data is available
let tagRequest_ReadBlock_Available = Tags("HMIData_TrendBufferTransfer_DataAvailable");
if (tagRequest_ReadBlock_Available.Read());
{
  let blockData =
Tags("HMIData_BlockTrendBufferTransfer").Read(HMIRuntime.Tags.Enums.hmiReadType.hmiReadDir
ect);
  // Do something useful with the block array data
  // New data can be transferred into the block array within the PLC as long as requested
  tagRequest_ReadBlock_Available.Write(false);
}
```

Script in screen with trend control for "Loaded" event

```
// Handshake tag to signal from HMI to PLC that the block array data is requested and will
be prepared
  let tagRequest_ReadBlock = Tags("HMIData_TrendBufferTransfer_ReadRequest");
  tagRequest_ReadBlock.Write(true);
```

Script in screen with trend control for "Cleared" event

```
// Block array data in PLC is not needed to be prepared anymore
  let tagRequest_ReadBlock = Tags("HMIData_TrendBufferTransfer_ReadRequest");
  tagRequest_ReadBlock.Write(false);
```

Example script for PLC: Handshake procedure for reading an array as a block

```
// Example for filling two arrays with sine/cosine data
IF "HMIData".simSinCos = TRUE THEN
        // Statement section IF
   FOR #i := 0 TO 179 DO
        "HMIData".TrendBuffer1[#i] := (SIN(INT_TO_REAL(#i) * 2 * "PI" / 180.0))*100;
        "HMIData".TrendBuffer2[#i] := (COS(INT_TO_REAL(#i) * 2 * "PI" / 180.0))*100;
    END_FOR;
END_IF;

// Signal the HMI that the trend can read the block array data
IF ("HMIData".finishedMoveBuffer) THEN
    "HMIData".TrendBufferTransfer_DataAvailable := TRUE;
    "HMIData".finishedMoveBuffer := FALSE;
END_IF;

// Prepare the block array data once if requested by the HMI
IF ( "HMIData".TrendBufferTransfer_ReadRequest AND NOT
"HMIData".TrendBufferTransfer_DataAvailable) THEN
    // Alternately write sine / cosine data into the block array
    IF ("HMIData".currentReadBuffer = 1) THEN
        FOR #i := 0 TO 179 DO
            "HMIData".TrendBufferTransfer[#i] := "HMIData".TrendBuffer1[#i];
        END_FOR;
        "HMIData".finishedMoveBuffer := TRUE;
        "HMIData".currentReadBuffer := 2;
    ELSIF("HMIData".currentReadBuffer = 2) THEN
        FOR #i := 0 TO 179 DO
            "HMIData".TrendBufferTransfer[#i] := "HMIData".TrendBuffer2[#i];
        END_FOR;
        "HMIData".finishedMoveBuffer := TRUE;
        "HMIData".currentReadBuffer := 1;
    END_IF;
END_IF;
```

4.2.4 Set system time

A correctly set and synchronized system time is essential.

- Establish communication with other devices
  The system time is used as the basis for establishing communication between devices and various services. An incorrect system time can cause communication partners to reject connections.
  Some communication protocols also rely on certificate-based security or encryption. If the system time is incorrect (especially if it is set in the future), certificates may be considered expired, leading to connection errors.
- Precise logging of data and events
  Logging and audit trails use a device's system time to time stamp events. An incorrect system time results in data and events being recorded with incorrect time stamps. This will also trigger unexpected alarms.
- Reliability of the overall system
  A correct system time is not only important for Runtime operations but also for operations at operating system level, such as creating and modifying files, which rely on the accurate system time to set time stamps.

When should the system time be set?

- During commissioning of a device
  - Set the system time before commissioning the device.
  - Do not set the system time manually.
    Instead, configure a connection to the NTP server.
- After prolonged storage of the device
  The system time setting for an HMI device or a PLC may be lost if the device is turned off for more than 6 weeks.

Rules for setting the system time

- Never set the system time in a running system, i.e. during production.
  - Sudden jumps in the system time can lead to unpredictable malfunctions.
  - A problem may remain hidden for an extended period, e.g. regular script tasks that are no longer executed.
  - Note: Note that not only the product's own code but also scripts and third-party libraries may rely on the system time to determine, for example, when the "next execution cycle" of a program should run. If the time suddenly jumps back by 8 hours, the next execution cycle will be triggered in 8 hours, not in 100 ms.
- A backward setting of the system time requires re-commissioning (cold restart).
  - Resetting the system time, even when runtime is not active, requires a restart of the project.
- Note the difference between setting the system time and changing the time zone.
  - The system time is based on UTC and is independent of the selected time zone.
  - The software uses UTC time and is therefore not affected by changes in the time zone configuration.
  - If the hardware is moved to a different time zone, change the time zone, not the system time.
  - A change in the time zone has no impact on the UTC system time and therefore does not pose a risk to Runtime.

Time synchronization with NTP

- Configure devices as NTP clients
  - Both HMI panels and PCs can be configured as NTP clients. NTP clients require an NTP server that is synchronized with the NTP server's clock via a radio signal (DCF77), GPS, or the internet.
- Configure an S7 PLC as an NTP server.
  - As an alternative to an internet connection, you can configure an S7 PLC to function as an NTP server.

Avoidable alarms

These alarms can be avoided through consistent time synchronization.

ID	Alarm text	Effect/cause	Solution
537526277 536871427	Computer1 (@2%s@): A time stamp has been corrected.	The alarm is triggered when a value change or a state change from the external source (including via scripting) is timestamped with a value that is not acceptable for the HMI. The following cases are possible: • Too new, default is more than 3 seconds in the future, based on the system time of the HMI system. • Too old, configurable: Values that are so old that they no longer make sense, e.g. an alarm from 1970. • Older than or equal to the last known time stamp of a value/alarm If any of these three conditions are violated, a time correction occurs. The message is information. The system behavior does not change.	Eliminate the cause of the necessary time correction. Ensure that all devices in the system use the same time stamp through time synchronization. You can find information on synchronization under "Basics of communication".

4.3 Improvements in Update 1

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Unified Engineering

5

5.1 Improvements in Update 4

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Screens

In the Unified screen editor (Next Gen.), transparent screens are displayed correctly after changing the background color.

When the zoom level of a screen is less than 100%, objects zoomed with the mouse are displayed correctly.

Faceplates

The deletion of faceplate instances has been improved.

The upgrade of a project with a custom style has been improved. After the upgrade, the screen objects are displayed correctly.

System tags are taken into account when selecting tags for a trigger.

The use of custom styles has been improved in the faceplate editor.

The inheritance of authorizations for nested faceplates has been improved.

Tags

The tags are marked as "subscribed" after they have been completely downloaded to the PLC. Therefore, when switching between popup windows multiple times, no connection interruption is displayed.

Parameter sets and parameter set control

The drop-down menu of the parameter set control is displayed correctly.

Parameter sets with "WString" data type are loaded correctly into the PLC without interrupting the connection.

Scripting

In the "Scripts" editor, formatting changes caused by indentations are correctly recognized as project changes to be saved.

When code is inserted, the cursor stays at the insertion position instead of jumping to the first line.

The "UI.Style" property returns the style consistently in the '<Device name>::<Style name>' format.

If you have created an independent popup with the "OpenFaceplateInPopup" method using the optional "independentWindow" parameter, you can debug scripts within this popup with the VS Code Runtime Debugger.

Simulation

The "Activated" event is triggered correctly on a screen window.

In a text box, the text is displayed correctly even when aligned to the "center".

Compiling and loading

The file names are displayed correctly in the "Load preview" dialog.

User data under "Common data > HMI files" is loaded correctly.

Libraries

In scripts, referencing screens that are master copies from a library works correctly.

Communication

To enable the multiplexing of tags with Allen Bradley ControlLogix or CompactLogix CPUs, the new connection type "Allen-Bradley EtherNet/IP GM" is temporarily available.

Multiplexing requires two tags.

"Tag_1" of the "WString" data type contains a logical address "HMI:Robot5.Block5" as the value.

"Tag_2" uses the connection "Allen-Bradley EtherNet/IP GM" and contains the valid name of an HMI tag in square brackets, for example "[Tag_1]"

Only complete addresses can be multiplexed. The multiplexing of address elements such as "HMI:Robot[Tag_1].Block5" is not possible.

Note

Please note that the "Allen-Bradley EtherNet/IP GM" connection is only available temporarily. With V21, the "Allen-Bradley EtherNet/IP" will be able to multiplex its addresses.

5.2 Improvements in Update 3

5.2.1 General improvements in Update 3

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Colors and color palettes

The local and global search for colors, color palettes and their references has been improved.

- The local search now lists results from the screen editor, faceplate editor, color palette editor and script editor.
- The global search now lists results from the screen editor, faceplate editor, color palette editor and script editor.

Redundancy

Process and system diagnostics is supported for redundancy.

Routed S7 connections

The following scenarios are possible for configuring routed S7 connections between a Unified Basic Panel/Unified Comfort Panel/Unified PC and a PLC.

The source device is always a Unified device with a PROFINET (Ethernet) interface. At least one "Router" is always installed in between.

Scenario	Devices
S7-PLC as a router (PROFINET) ⇔ S7+ PLC as end device (PROFIBUS/PROFINET)	Router: S7-300/400 PLC End device: S7-1500 PLC (PB)
	Router: S7-300/400 PLC End device: S7-1500 PLC (PN)
	Router: S7-300/400 PLC End device: S7-1200 PLC (PN)
S7+ PLC as a router (PROFINET) ⇔ S7+ PLC as end device (PROFIBUS/PROFINET)	Router: S7-1500 PLC End device: S7-1500 PLC (PB)
	Router: S7-1500 PLC End device: S7-1500 PLC (PN)
	Router: S7-1500 PLC End device: S7-1200 PLC (PN)

Scenario	Devices
S7+ PLC as a router (PROFIBUS/PROFINET) ⇔ S7+ PLC as an additional router (PROFIBUS/PROFINET) ⇔ S7+ PLC as end device (PROFINET)	Router: S7-1500 PLC Router: S7-1500 PLC End device: S7-1200 PLC (PN)
IE/PB link (PROFIBUS) ⇔ S7 PLC/S7+ PLC as end device (PROFIBUS)	Router:IE/PB link End device: • S7-300/400 PLC (PB) • S7-1500 PLC (PB)

S7-300/S7-400 PLCs with only one PROFIBUS interface are thus reached via S7 routing from a Unified device with a PROFINET (Ethernet) interface.

Note:

- Information on whether a device supports routing can be found in the respective Equipment Manual. Under the "Asynchronous communication connections - S7 routing" keywords, you will find information on the support of Ethernet, PROFIBUS DB and communications modules.
- Other possible scenarios have not been tested.
- A virtual PLC can only be used as an end device in a routed connection, as it only has one connection.
- Version-dependent restrictions apply to the S7-1500 Software Controller.

Remote access via Web client and Smart Server

After replacing an HMI device or migrating a project, remote access via Web client or Smart Server may no longer be possible. The cause of the problem has been eliminated.

Unified JavaScript properties "ScreenWindow.SupportedNavigation" and "TopLevelScreenWindow.SupportedNavigation"

Together with the listed system functions and methods, the properties enable the creation of navigation between screens in Runtime.

- ClearScreenHistory
- SysFct.ClearScreenHistory()
- ChangeScreenNext
- SysFct.ChangeScreenNext()
- ChangeScreenNextAsync
- SysFct.ChangeScreenNextAsync()
- ChangeScreenPrevious
- SysFct.ChangeScreenPrevious()
- ChangeScreenPreviousAsync
- SysFct.ChangeScreenPreviousAsync()

5.2.2 Unified Screen Editor (Next Gen.)

5.2.2.1 Unified Screen Editor (Next Gen.) - Introduction

"Unified Screen Editor (Next Gen.) " is available as a standard editor as of TIA Portal V21, alongside the existing "Screens" editor.

In the settings in the Engineering System, you can select the editor and switch between the editors. The "Unified Screen Editor (Next Gen.)" option is enabled by default.

In the Unified Screen Editor (Next Gen.), you visualize all screen objects like in the existing "Screens" editor. The Unified Screen Editor (Next Gen.) includes improvements and new functions for working efficiently with screens and screen objects. The next sections contain a description of the new functions and the improvements to existing functions.

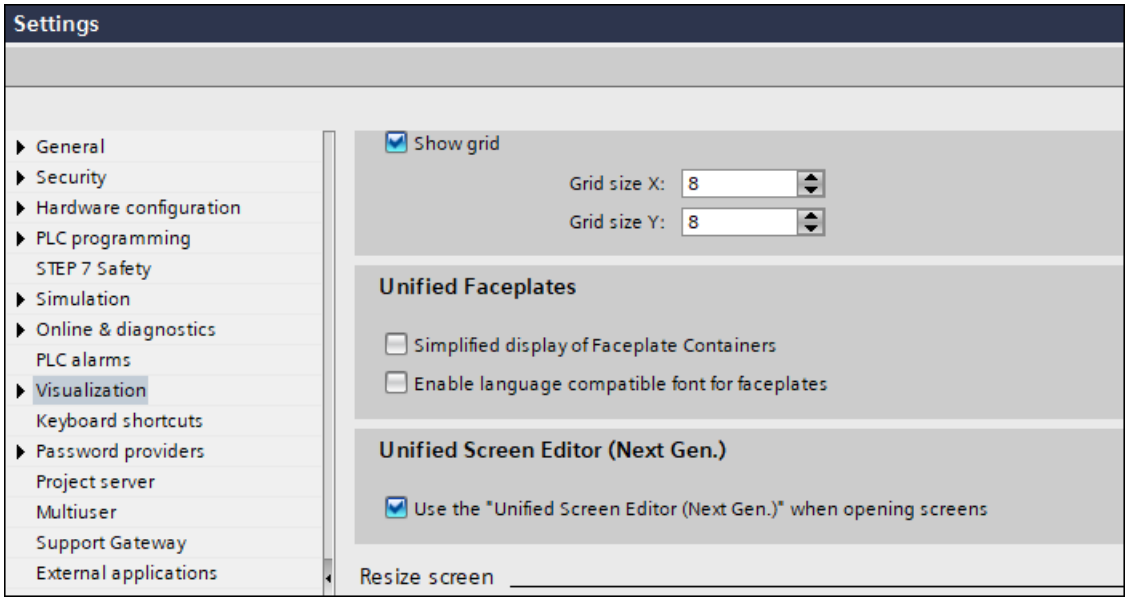
5.2.2.2 Select editor

In the Unified Screen Editor (Next Gen.), you visualize all screen objects like in the existing "Screens" editor. In the settings in the Engineering System, you can select the editor and switch between the editors.

Change editor

If you want to change from the existing "Screens" editor to the Unified Screens Editor (Next Gen.), follow these steps:

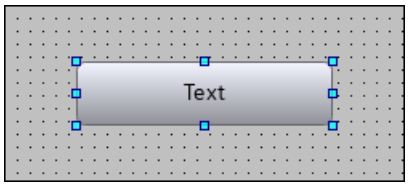
1. Enable the "Unified Screen Editor (Next Gen.)" option under "Options > Settings > Visualization > Screens".
   All open screens in the project are closed when you change the editor.
2. Open the screens again.



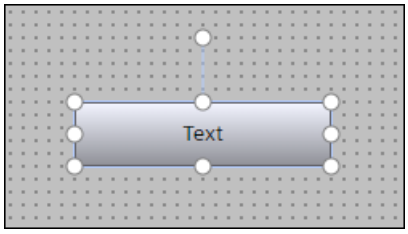
Identify editor

To distinguish between the editors, the grab handles for the objects have a different shape and size.

- In the existing "Screens" editor, the grab handles are blue rectangles.



- In the Unified Screen Editor (Next Gen.), the grab handles are shown as small white circles. The white circle above the object is the rotation handle for rotating the object.



5.2.2.3 New functions

5.2.2.4 Improvements in Unified Screen Editor (Next Gen.)

5.2.3 Screens and screen objects

5.2.3.1 Screens and screen objects - Improvements (Unified ES)

This update contains the following improvements and changes:

Screen objects in layers

If the "Hide layer" option and then "Show layer" is selected in a screen with objects, the objects in the layer are displayed correctly.

Fit to size screen windows

After a device change and automatic adjustment of the screens, the content in image windows is adjusted correctly.

Display of the "Reports" control in the screen editor

If a user interface language which does not have localization for the "Reports" control is active in the engineering, the control is now shown in English in the screen editor.

Determining whether screen objects are contained in a group

The "`LayoutContainer`" property is made available for screen objects with the WinCC Unified JavaScript object model in scripts. The property indicates whether a screen object is part of a group of screen objects.

Return

- If the screen object is part of a group, the property returns the LayoutContainer screen object.
- If the screen object is not part of a group, the property returns "Null".

Example

```
let container = Screen.Items("Rectangle_1").LayoutContainer;
if (container)
{
  HMIRuntime.Trace("Layout container of Rectangle_1:
"+container.Name);
}else
{
  HMIRuntime.Trace("Rectangle_1 is not in a layout container");
}
```

Determining the bounding box of screen objects

The new method "`GetBoundingBoxInScreenCoordinates()`" of the WinCC Unified JavaScript object model in scripts returns an "HMIBox" object for the underlying screen object containing the properties "Left", "Top", "Width" and "Height".

This method is used to determine when a screen object disappears from the visible area if the screen is scrolled when zoomed.

Example

```
let box =
Screen.Items("Rectangle_1").GetBoundingBoxInScreenCoordinates();
if (box)
{
  HMIRuntime.Trace("Bounding box: ("+ box.Left +","+ box.Top +","+
box.Width +","+ box.Height +")");
}
```

5.2.3.2 Alarm line

Use

The alarm line is a write-protected object that displays up to three of the most recent or important active alarms based on configurable criteria. This ensures quick identification of critical alarms, reduces configuration time and increases system efficiency.

The "Alarm line" object is supported as of Version V20 Update 3 and is not compatible with the earlier versions.

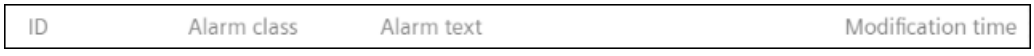
Configuring the alarm line

Requirements

- A screen is open.
- The "Toolbox" task card is open.

Procedure

Drag and drop the "Alarm line" object from the "Toolbox" task card into the screen. The "Alarm line" object is displayed on the screen as a single row with a header text.



Layout

By default, the following columns are displayed in the alarm line:

- ID
- Alarm class
- Alarm text
- Modification time

Properties of the "Alarm line" object

The "Alarm line" object allows the display of up to three alarms, with the "Number of rows" property set to 1 by default and configurable to a maximum of 3 rows.

The standard row height is fixed at 28. The row height depends on the height of the object.

The alarms can be filtered based on the filter criteria configured by the user.

The "Alarm line" object is compatible with screen windows. Compatibility with faceplates is not supported in this version.

The alarm text wrapping is enabled by default, and the multiline text feature is not supported.

Note

The "Alarm line" object is used exclusively for alarm display; alarm selection is not supported.

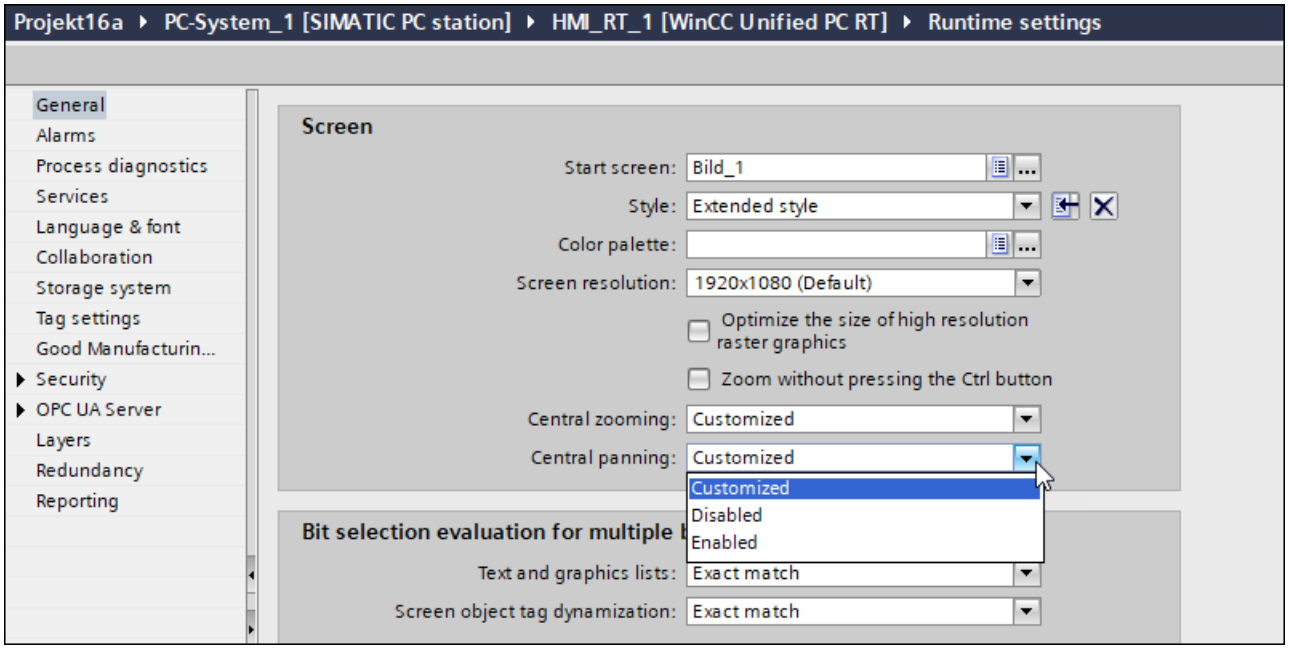
The "Alarm line" object does not support row and column headers, toolbars or vertical and horizontal scroll bars.

5.2.3.3 Centrally defining zooming and panning

In the Runtime settings, you can define the central setting for zooming and panning for the following objects in a Unified device:

- Main screen window
- Screen window
- Popup window
- Faceplate container

Defining zooming and panning



"Central zooming" is the central setting for zooming for the objects in a Unified device.

- If "Custom" is selected, local setting of the "Zoom - allow" object property is supported in Unified Runtime.
- If "Enabled" or "Disabled" is selected, zooming is centrally enabled or disabled in Unified Runtime.

"Central panning" is the central setting for panning for the objects in a Unified device.

- If "Custom" is selected, local setting of the "Pan - allow" object property is supported in Unified Runtime.
- If "Enabled" or "Disabled" is selected, panning is centrally enabled or disabled in Unified Runtime.

5.2.3.4 Localized default texts for screen objects

For screen objects with the default texts, e.g. column headers in the alarm control, the text appears in the installed user interface language that you set as project language when creating the project.

If you select a different language as project language, a secondary, so-called fallback language is used to display the default text.

The localized default texts are only displayed for the objects you created with TIA Portal V20 Update 3. This function is not available for objects created with an earlier version of the TIA Portal.

Overview of the fallback languages

The following table shows the fallback languages for the listed project languages:

Project language	Fallback language
Catalan (Catalonia)	Spanish (Spain)
Basque (Basque country)	Spanish (Spain)
Galician (Galicia)	Spanish (Spain)
Ukrainian (Ukraine)	Russian (Russia)
Belarusian (Belarus)	Russian (Russia)
Georgian (Georgia)	Russian (Russia)
Kazakh (Kazakhstan)	Russian (Russia)
Uzbek (Cyrillic, Uzbekistan)	Russian (Russia)
Azerbaijani (Cyrillic, Azerbaijan)	Russian (Russia)
Swahili (Kenya)	English (United States)
Chinese (Taiwan)	Chinese (simplified)
Chinese (Hong Kong S.A.R.)	Chinese (simplified)
Chinese (Macau S.A.R.)	Chinese (simplified)
Other languages	English (United States)

Display of default texts

The default texts are displayed:

- On the screen:
  In the objects in the screen, the default texts are shown in the language you selected in the "Tasks" task card under "Languages & resources > Editing language".
  If you change the editing language, the default texts are shown in the changed language.
- In the Inspector window:
  Under "Properties > Texts", all default texts of the object are shown in the languages you selected in the project tree under "Languages & resources > Project languages".

If you add another language under "Project languages", this language is first shown in the default texts of a newly added object.

The default text in existing objects is shown in English.

5.2.3.5 Searching for an object property in the screen

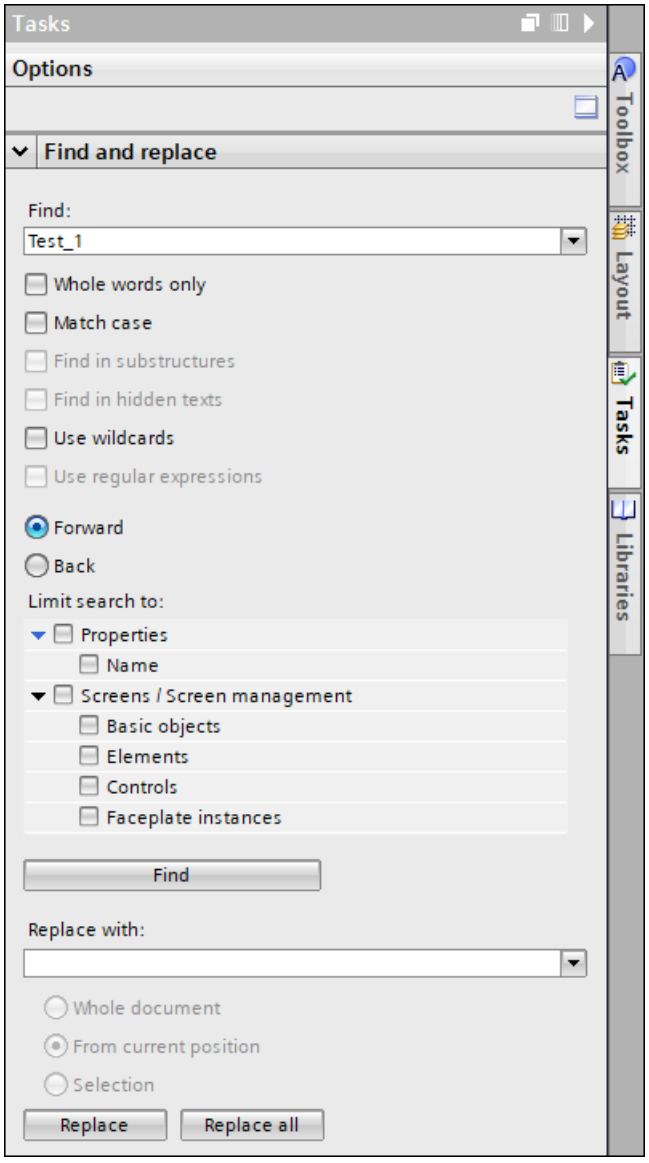
You can search for a static object property without leaving the current screen in the editor.

In the "Find and replace" pane in the "Tasks" task card, you can search for a string in the object properties. After the search:

- The corresponding objects are marked in the screen.
- The hits in the Inspector window are shown under Properties.

You can limit the search to the "Name" property and to selected object types if you enable one or more options under "Limit search to".

The limit is disabled by default.



Limit search

To limit the search to a string, enable the desired option under "Limit search to".

You can search for a string:

- In the "Name" property, when you enable the "Property > Name" option.
- In all properties in the selected object types, when you enable the "Screens / Screen management" option and one or more object types.
- In the "Name" property and in the selected object types, when you enable the "Property > Name" option and one or more object types at the same time.

If you do not enable any option, the string is searched for in all static properties in the screen.

Examples

The following two examples show the search for:

- String in the "Name" property.
- String in the property for the object types.

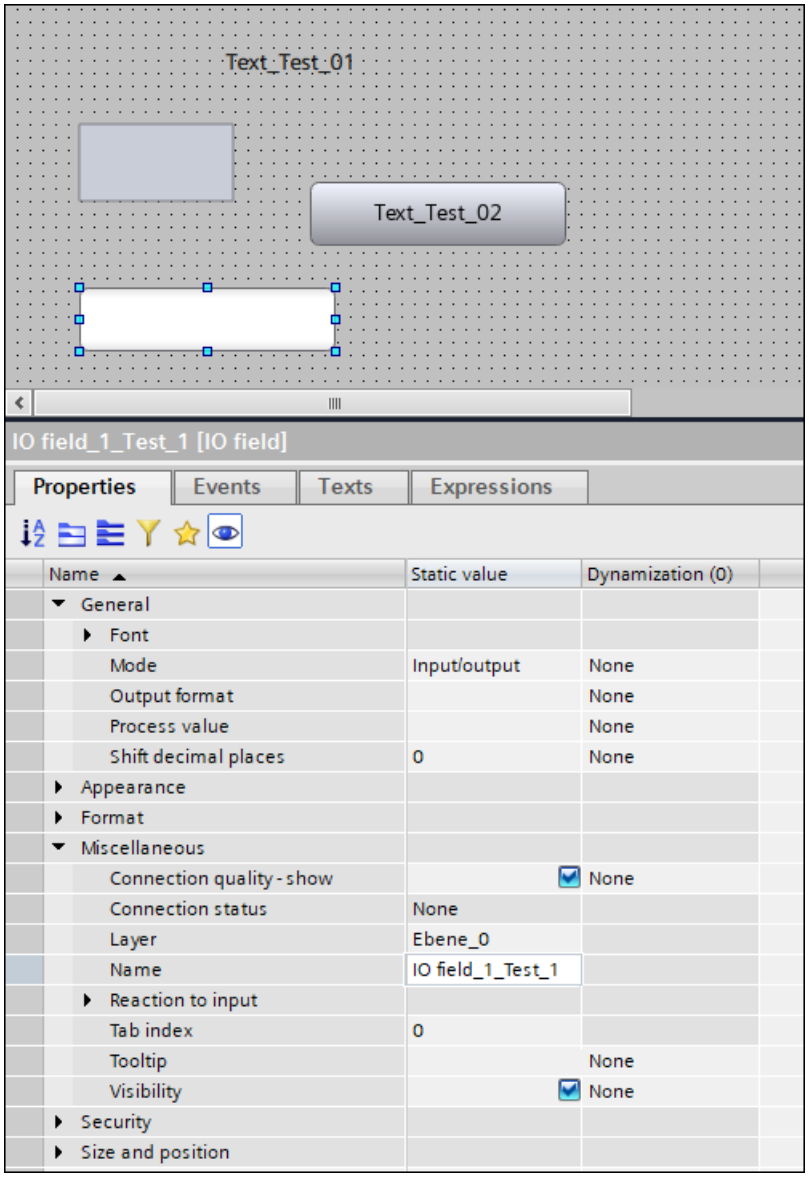
Example: Searching for the string in the "Name" property

You can search for a string in the "Name" property under all objects in the screen.

To search for the string in the "Name" property, follow these steps:

1. Open the "Find and replace" pane in the "Tasks" task card.
2. Enter the string to be searched for in the "Find" drop-down list, e.g. "Test_1".
3. Under "Limit search to", select the "Property > Name" option.
4. Click "Find".
   - The first object with the string that was searched for in the "Name" property is marked in the screen.
   - The name with the string that was searched for is marked in the "Static value" column in the Inspector window.
5. Click "Find" again to display the next hit.
   The next hit is marked.

Repeat this step until you reach the last hit.



Example: Searching for a string in the property for the object type

To search for the string in all properties for the selected object type, follow these steps:

1. Enter the string to be searched for in the "Find" drop-down list, e.g. "Test_1".
2. Enable the "Elements" and "Controls" options, for example, under "Limit search to" under "Screens / Screen management".

3. Click "Find".
   - The first object with the string that was searched for is marked in the screen.
   - The first property with the string that was searched for is marked in the "Static value" column in the Inspector window.
4. Click "Find" again to display the next hit.
   The next hit is marked.

Repeat this step until you reach the last hit in this example in all elements and controls in the screen.

5.2.3.6 Overview of Screen resources

On an HMI device, you can view an overview of all screen objects that you configured in the screens. The screens and the number of all objects contained is shown in a write-protected table.

Opening the "Overview of Screen resources" table

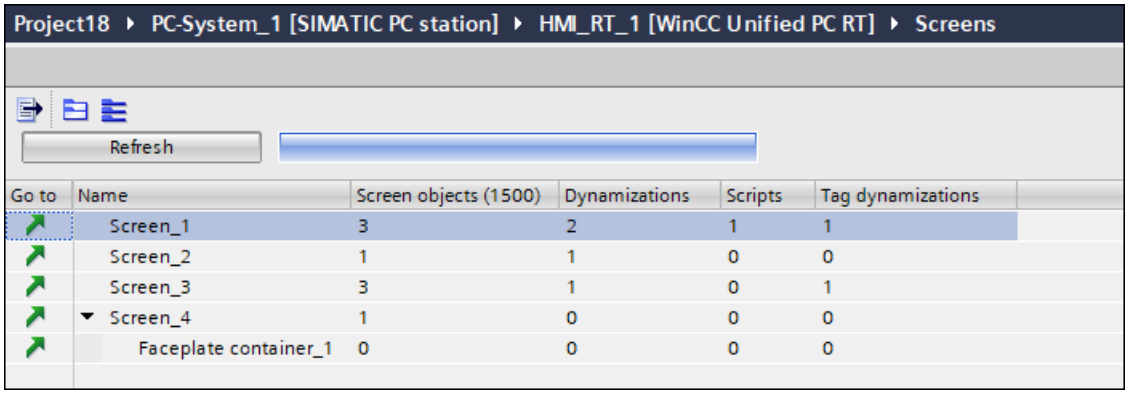
You open the "Overview of Screen resources" table:

- Via the context menu of the "Screens" folder in the project tree.
- Via the "Go to" button in the Resource Monitor of the HMI device.

"Overview of Screen resources" table - Contents

In the "Overview of Screen resources" table, you will find the following columns:

- Go to with the button
- Name
- Screen objects
- Dynamizations
- Scripts
- Tag dynamizations



Functions in the "Overview of Screen resources" table

You go directly to the selected screen with the "Go to" button. You can continue configuring the objects in the screen.

The faceplate container is shown hierarchically. You can expand or collapse the display.

In each column except "Go to", you can sort the entries alphabetically in ascending or descending order.

The number of screen objects in a screen is shown in the "Screen objects" column. The system limit for the number of all screen objects is given in brackets in the column header.

With the button:

- "Export" , you can export the overview as a .csv file.
- "Show all layers" , you can display all layers.
- "Hide all sublevels" , you can hide all sublevels.
- "Update", you can update the table if necessary. The progress of the refresh operation is shown in the progress bar.

5.2.3.7 I/O field: "Shift decimal places" property

The "Shift decimal places" property for the "I/O field" object enables automatic conversion of the integer tags with a power of 10.

The entered value is multiplied according to the number of decimal places and written to the tag. The value is also written into the controller for an external tag.

Conversely, the value from the tag or controller is divided accordingly if the value is shown in the I/O field.

Shifting the decimal places

To shift the decimal place, follow these steps:

1. Dynamize the process value with the tag based on an integer data type, such as SInt, DInt, LInt, Word, DWord, LWord.
2. In the "Shift decimal places" property, enter a value in the "Static value" column, for example, the value 2.
3. Set {F2} as output format.
4. The process value is adjusted in Runtime:
   - If the tag has the value 123, for example, the value 1.23 is shown in the I/O field.
   - If you have entered the value 23.4 in the I/O field, for example, 2340 is written to the tag.

You can dynamize the "Shift decimal places" property using a tag, script or expression.

If the "Shift decimal places" property is enabled, the value of the tag is adapted for the display or the entered value is adapted before it is written into the tag.

Important information

- Ensure that the output format matches the shifted value:
  Select an output format of the "Floating-point numbers" category which matches the value of the "Shift decimal places" property.
  Example:
  With two decimal places, you set {F2} for the output format.
  If you do not set an output format, the value will always be displayed with 2 decimal places, regardless of the value you have configured for the "Shift decimal places" property.
- If you have configured the "Shift decimal places" property and the value is not 0, a warning is displayed under the following conditions:
  - The process value is dynamized with a tag that is not based on an integer data type.
  - The process value is dynamized with an expression or a script.
  - The process value is not dynamized.
  - The assigned tag is processed in a formula.
  - Indirect addressing is activated.

  The warning is displayed:
  - For the "Shift decimal places" property in the "Static value" column.
  - When loading the project.

5.2.4 Faceplates

5.2.4.1 Interface tags

This update contains the following improvements and changes:

Interface tags of "LReal" data type

You can link interface tags of the "LReal" data type on the faceplate container with a tag of any simple data type. This means that you do not have to pay attention to a special data type.

Note

The "WString", "WChar", "ULInt", "LInt", "LWord", "LTime", "DateTime", "Date", "LTime_Of_Day" data types are not supported for linking to an interface tag of the "LReal" data type.

5.2.4.2 Faceplates: Dynamization via interface properties

Object properties can be dynamized with the "Properties interface" option through interface properties via formulas or assignment of evaluation types.

The following property types and interface tag types are supported:

		Interface properties of the faceplate					
		Bool	**LInt**	**ULInt**	**LReal**	**Multilingual Text**	**WString**
Properties of a screen object	**Enum**	x	x	x	x	-	x
	Variant	x	x	x	x	-	x
	Text	x	x	x	x	x	x
	String*	x	x	x	x	-	x

* Formula or evaluation type is not supported for the "Alarm filter" property.

In contrast to the use of scripts, direct dynamization leads to improved performance. Knowledge of scripts is not required.

Dynamization of object properties

1. Select the "Property interface" dynamization type for a property.
   In the Inspector window, the "Properties" of the dynamization are displayed on the right-hand side.
2. Under "Settings", select one of the available interface properties.
   Only properties with a suitable data type are displayed.
3. **Formula**
   To apply a formula, activate the corresponding option in the "Formulas" area.
   The result of the formula must be a numerical value.
4. **Evaluation type**
   If the source property and the target property are of different data types, use the table.
   - Select an evaluation type.
   - In the table, assign the corresponding values to the selected conditions.
     The value of the tag or the result of the formula is assigned to the values.

Note

If you select "None" under "Type", ensure that the source data type and the target data type are the same.

Dynamization of interface properties via the formula

You can dynamize interface properties using formulas with multiple tags and/or interface properties. In a formula, the interface properties are linked by operators. The result of the formula determines the dynamization.

Predefined functions are available in the "Bit by bit" selection list for tags linked bit by bit.

Conversion functions are available to convert values into different reference systems.

The following data types of properties are supported for dynamization via a formula and/or evaluation type:

- Bool
- Color
- LInt (64-bit integer)
- ULInt (unsigned 64-bit integer)
- LReal (floating-point number)
- Multilingual text
- WString (configuration string)

Conditions and restrictions for the evaluation type

You can define the evaluation type of the interface property. The result of the activated formula is the basic value for the evaluation type.

- None
- Area
- Multiple bits
- Single bit

The following conditions and restrictions apply to the evaluation type:

- If the formula is deactivated:
  - The data type of the evaluation type corresponds to the data type of the interface property.
  - Values up to 64 bits are supported for the "single bit" and "multiple bits" evaluation types.
  - Negative values are not allowed.
  - Values up to 32 bits and a maximum of 15 decimal places are supported for the "Area" evaluation type.
- If the formula is activated:
  - The data type of the evaluation type is "LReal".
  - Values up to 32 bits are supported for the "single bit" and "multiple bits" evaluation types.
  - Values up to 32 bits and a maximum of 15 decimal places are supported for the "Area" evaluation type.
- If formula is activated and the data type of the interface property is "color", you can only use the evaluation types in connection with formula.

Validation

Data types and values in the assignment table are validated. Invalid information means that the faceplate type cannot be enabled.

Errors can occur when validating projects migrated from previous versions. If necessary, you have to adjust values or data types.

When compiling a project, invalid values or data types also lead to an error.

5.2.4.3 Improved flexibility with use of user data types

Support of changes to constants in arrays of user data types

User data types that contain arrays defined by constants can be connected to the property interface.

With Unified devices as of device version 20.0.0.2, the user receives warnings instead of errors if the user data type is an array and the number of elements is smaller than the array of the faceplate interface. The faceplate type does not need to be adapted.

In this case, Runtime sends a quality code that shows an access error to the elements, e.g. I/O fields, in the faceplate.

Dynamic access via script (access to interface tag is only established during Runtime) also generates a quality code that indicates an access error. A trace entry is generated.

For devices with a device version up to 20.0.0.2, an error is indicated during compiling as before.

If the constant actually used is larger than the value found in the faceplate type, no error is indicated during compiling as before.

5.2.5 Libraries

5.2.5.1 Use type in type

Faceplate types: Using types in types

If other types, such as faceplate types, text lists or SVGs are referenced in a faceplate type, and the referenced types are changed, the referenced type is only versioned and placed in edit mode when necessary.

In the case of compatible changes on the referenced type, the referencing type is updated. No new version is created. The number of versions and the amount of configuration effort are minimized.

Non-compatible changes lead to versioning of the referencing type.

5.2.5.2 Import of text lists

Incrementing the version number

When importing a text list, the option of "Import library texts and increment version" is now available in the context menu of the types.

This option is offered for the project library and for global libraries.

The version number is only incremented for the text lists that contain new or changed texts.

Imported texts change the version of the library objects from which the export was performed and not the default type. The export is version-specific.

Manual updating is therefore not required.

5.2.5.3 Scripting: Referencing the default version

Simplified access to default version in scripting

The default version of a type in a library can be directly referenced via scripts without the version of the type being specified.

With these methods, you can access the default version of a type in a library directly:

- `HMIRuntime.Resources.FaceplateTypes("MyFacePlate").DefaultName;`
- `HMIRuntime.Resources.GraphicTypes("MyGraphicType").DefaultName;`
- `HMIRuntime.Resources.TextListTypes("MyTextList").DefaultName;`

The methods are available for these library types:

- Faceplate
- Graphic
- Text list

This eliminates the need to adapt a script after a new type version is created.

5.2.5.4 User Tags > Set 'AlwaysDownload'

New option: Always download

For the following library types, you have the option to always use the current version as a default when compiling and loading.

- Faceplates
- Graphics
- Text lists

Via the context menu of a type, you specify in the library under "User Tags > Set 'AlwaysDownload'" that the current version of this type is always loaded when loading. Alternatively, the version used in the project is always loaded if the option is not set.

For selected library types, make sure that the default version is always loaded and is available in Runtime, regardless of whether the default version is used directly in the device or not.

The option is available for types in the project library and in global libraries.

The option can be enabled for multiple types at the same time.

If the option is enabled, this is displayed in the library in the "User Tags" column. The display can be filtered by this option.

When a new type is created, the marking is not set.

Restrictions

This option is not available for HMI devices with a device version lower than 20.0.0.2.

This option is not available for View of Things devices.

5.2.6 System functions

5.2.6.1 System functions for local user management

Note

Support as of V20 Update 3

The system functions for user management are described in the V20 help, but are only supported with V20 Update 3.

Export and import of local user management

The following cases are supported:

- Exchange of users and passwords between different devices to have the same basis on different devices.
- Securing/restoring users and passwords on locked devices to restore the release state.

If all users are locked out, no backup or import can be performed. A user with the "Manage users and roles" permission must be logged in.

There are two new system functions available for this purpose:

- `HMIRuntime.UI.UserManagement.SysFct.ImportUserAdministration(Storagepath, [optional] Password)`
- `HMIRuntime.UI.UserManagement.SysFct.ExportUserAdministration(Storagepath, [optional] Password)`

Parameter:

- `Storagepath (string)`
  Full path and file name for export and import
- `Password`
  Optional, can be provided via a screen object or a tag
  The system function removes the password from the tag or the screen object.
  If a password is used during export, this password must be specified during import. If no password is used during the export, no password is required during the import either.

Note

Indirect addressing

If you pass the parameter via indirect addressing of a tag, the tag must be of the "String" data type. Otherwise, the system function will not be able to delete the value after execution.

Restriction

Since the password is deleted after the system function is executed, it is not possible to execute the system function twice within a function list.

Notes

The data exchange can be made between different devices:

- Between Unified Panels
- Between Unified PCs
- Between Unified Panels and Unified PCs

The Control Panel already offers the option to import/export user data.

The `ImportUserAdministration` system function offers the option of importing exported user data using the Control Panel. Exported user data can be imported via the Control Panel via the `ExportUserAdministration` system function.

The import/export is only possible for local user management.

The system functions can only be executed by users with the "User Administration" right.

5.2.6.2 System functions for screen navigation

Navigation between screen windows in Runtime

The following cases are supported:

- Navigation between screens using Next and Previous buttons.
- Creation of a history with up to 24 entries.

Four new system functions are available for navigation between screen windows:

- `HMIRuntime.UI.SysFct.ChangeScreenNext([optional] string screenWindowPath)`
- `HMIRuntime.UI.SysFct.ChangeScreenPrevious([optional] string screenWindowPath)`

- `HMIRuntime.UI.SysFct.ChangeScreenNextAsync([optional] string screenWindowPath)`
- `HMIRuntime.UI.SysFct.ChangeScreenPreviousAsync([optional] string screenWindowPath)`

Parameter:

- `screenWindowPath (string)`
  Path of the screen window to be changed. If the parameter is empty, the screen window changes from the main screen.

New system function to delete the history:

- `HMIRuntime.UI.SysFct.ClearScreenHistory([optional] string screenWindowPath)`

Parameter:

- `screenWindowPath (string)`
  Object path of the screen window to be deleted from the history, e.g. "~/Screen_window_1". If the parameter is empty, the history of the main screen window is deleted.

This history is deleted in the following cases:

- "`ClearScreenHistory`" system function is executed
- User is switched
- Window is closed or user logs out
- Main screen is switched

In addition, there are two new properties for creating the navigation:

- `ScreenWindow.SupportedNavigation`
- `TopLevelScreenWindow.SupportedNavigation`

These properties indicate which navigation is possible in the screen history. Example: The Previous button is disabled in the first screen window.

SupportedNavigation property

Description

The property is used to dynamize the navigation buttons and describes the direction in which navigation takes place (similar to the navigation buttons of a browser). It is a write-protected property that is only set by the system. It returns a value between 0-3 and has the type Enumeration HmiSupportedNavigation.

Type

Enumeration HmiSupportedNavigation

Possible values:

- `HmiSupportedNavigation.None` (0): Navigation is not possible. Neither forward nor backward navigation can take place.
- `HmiSupportedNavigation.Backward` (1): Only backward navigation can take place.

- `HmiSupportedNavigation.Foreward` (2): Only forward navigation can take place.
- `HmiSupportedNavigation.Backward | HmiSupportedNavigation.Foreward` (3): Both forward and backward navigation can take place.

Access

Read-only

Syntax

`ScreenWindow.SupportedNavigation` or
`TopLevelScreenWindow.SupportedNavigation`

Example script

This example script serves to dynamize the "Previous" and "Next" buttons for script-supported navigation.

Step 1: Disable the previously created buttons with the names "Previous" and "Next" as follows:

```
export function Screen_1_OnLoaded(item) {
            Screen.Items("Previous").Enabled = false;
            Screen.Items("Next").Enabled = false;
}
```

Step 2: Dynamize the "SupportedNavigation" property to change the "value" as follows:

```
export function
Screen_window_1_SupportedNavigation_OnPropertyChanged(item, value) {
            let supportedNavigation =  item.SupportedNavigation;
            HMIRuntime.Trace("Supported Navigation = " +
supportedNavigation);
            if(supportedNavigation ==
UI.Enums.HmiSupportedNavigation.None)
            {
              Screen.Items('Next').Enabled = false;
              Screen.Items('Previous').Enabled = false;
            }
            else
if(supportedNavigation == (UI.Enums.HmiSupportedNavigation.Backward
| UI.Enums.HmiSupportedNavigation.Foreward))
            {
              Screen.Items('Next').Enabled = true;
              Screen.Items('Previous').Enabled = true;
            }
```

```
            else if(supportedNavigation ==
UI.Enums.HmiSupportedNavigation.Backward)
            {
              Screen.Items('Next').Enabled = false;
              Screen.Items('Previous').Enabled = true;
            }
            else if(supportedNavigation ==
UI.Enums.HmiSupportedNavigation.Foreward)
            {
              Screen.Items('Next').Enabled = true;
              Screen.Items('Previous').Enabled = false;
            }
}
```

5.2.6.3 System functions for backing up and restoring logs

Backup and restore of logs

New system functions are available to back up log segments and restore backed up segments using scripts.

- async HMIRuntime.Audit.SysFct.**RestoreAuditLog** (Log[optional], StorageMedium[optional], Filepath[optional], DateFrom [optional], TimeRange[optional], ProcessingStatusTag [optional])
- async HMIRuntime.TagLogging.SysFct.**RestoreTagLog** (Log[optional], StorageMedium[optional], Filepath[optional], DateFrom [optional], TimeRange[optional], ProcessingStatusTag [optional])
- async HMIRuntime.AlarmLogging.SysFct.**RestoreAlarmLog** (Log[optional], StorageMedium[optional], Filepath[optional], DateFrom [optional], TimeRange[optional], ProcessingStatusTag [optional])
- async HMIRuntime.Audit.SysFct.**UnrestoreAuditLog** (ProcessingStatusTag [optional])
- async HMIRuntime.TagLogging.SysFct.**UnrestoreTagLog** (ProcessingStatusTag [optional])
- async HMIRuntime.AlarmLogging.SysFct.**UnrestoreAlarmLog** (ProcessingStatusTag [optional])

These system functions are available on Unified Comfort Panels and Unified PCs.

If a backup or restore process is already active, the system functions cannot be performed.

Errors during execution can be read with the "`GetDetailedErrorDescription`" system function.

Parameters

- `log`
  Log name
  If not specified, all logs of the respective type are included in the restore.
- `StorageMedium/FilePath`
  Path of the restored segments
  If not specified, the backup path as configured in TIA Portal is considered for the restore.
- `DateFrom`
  Start or end date (if the time range is negative)
  If not specified, the entire time range is considered.
- `TimeRange`
  Time span in seconds; can be negative, e.g. NOW - 10 days
- `ProcessingStatusTag`
  Returns the execution status as an integer:
  - 2: Function is currently being executed.
  - 4: Function has been executed successfully.
  - 12: Execution of the function failed.

Note

Parameter DateFrom / TimeRange

Both parameters are optional. Thus, the following combinations can arise during configuration:

- Both parameters are not set: The entire time range is taken into consideration.
- Both parameters are set:
  - `DateFrom` = now: `Time Range` is negative, e.g. now - 10 days.
  - `DateFrom` = [date in the past]>: `TimeRange` is positive: e.g. 01.01.2021 + 10 days
- Only `DateFrom` is set: The time range `DateFrom`. to today is taken into consideration
- Only `TimeRange` is set: Invalid configuration. Errors in Runtime.

Note

Parameter DateFrom

Time is interpreted as UTC (Coordinated Universal Time).

Application example

You configure a button with which log segments that have already been swapped out can be loaded using a script and visualized in a control.

5.2.6.4 System functions for PLC code view

"OpenPLCCodeViewByFCCall" system function

The documentation has been improved.

For the LAD and FBD PLC languages, the function displays the pre-interconnection of a network input of a standard block. The UDT instance is taken into account in the PLC code view.

Note

To display an S7-GRAPH block, use the "OpenGRAPHViewerByBlock" system function.

Use in the function list

OpenPLCCodeViewFromFCCall (String search, PLC name, Containing block, Called block, PIN, User data type instance, Object path to PLC code display)

The "OpenPLCCodeViewFromFCCall" system function has the following parameters:

Parameter	Description
PIN string search	During the search for the PIN name, a substring is searched for, i.e. the PIN name begins with the string passed in the PIN. If this bit is not set, the full PIN name is compared with the PIN.
PLC name	Name of the PLC.
Containing block	Name of the block to be opened and displayed.
Called block	Name of the local or global instance that is called in the code block belonging to the "Containing block" parameter. • For local instances, the hash character # must also be called here, for example "#feeder1". • For global instances, the global name must be specified without the hash character (#), e.g. "feeder3". The use of the name of a function (FC) is not allowed. If "Called block" is called several times within the "Containing block" or its function block (FB), the entry point is always the first call of "Called block".
PIN	Name of the Input PIN of "Called block". The parameter is used to indicate the network that is connected to the Input PIN in the PLC code view.
User data type instance	Limiting the display of multiple called FCs. The display is limited based on the UDT instance connected to any Input Pin or InOut Pin.
Object path to PLC code view	Path of the screen object "PLC code view".

Using scripts

For more information about the "OpenPlcCodeViewByFCCall" system function in JavaScript functions, see the WinCC Unified object model.

5.2.7 Using event parameters in the function list

Assignment of event parameters

The parameters of an event can now be redirected directly to parameters of script functions in global modules.

To do this, a global function can be selected for an event in the function list and the new "Event parameters" value assigned to its parameters. In this way, a call of the global script function with the assigned event parameters is created in the script automatically in the background. Previously, the event parameters could only be used by programming directly in the script.
The parameters of events of the following objects can be assigned:

- Screens and screen objects
- Faceplates (also in connection with interface events of faceplate types)
- Tasks

Restriction

The underlying script of the event parameter assignment is generally downward compatible with TIA Portal V20 and older. However, if you edit the assignment in an older version, the parameters of the script function are converted into strings and the assignment is lost.

5.3 Improvements in Update 1

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Unified PC

6

6.1 Important information

This page contains important information about product properties.

To utilize the functions introduced with WinCC V20 Update 3 in Runtime, you must install WinCC Unified Runtime V20 Update 2.

Previously installed versions of WinCC Unified

If you have V16 installed and want to upgrade to V20 with the latest update, it is recommended that V16 be uninstalled first.

"Control Panel > Set PG/PC interface" no longer available as of V20

If you have only installed WinCC Unified Runtime on a PC, configure the PG/PC interface using the "Communication settings" in the Windows Control Panel.

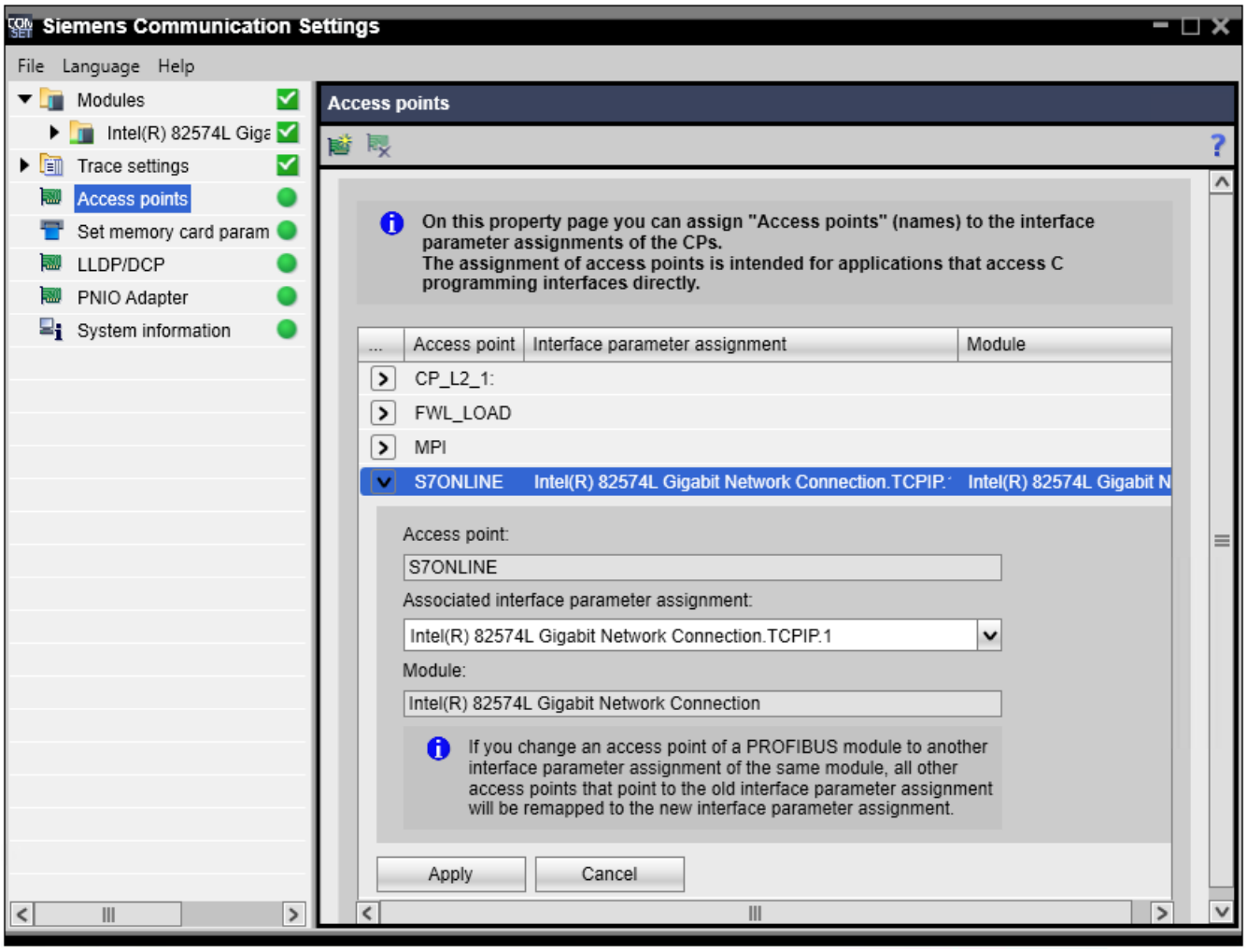
The "Set PG/PC interface" option is no longer available in the Control Panel as of V20.

Under "Communication settings" you can configure all settings in the new interface design.

For example, to establish communication with an S7 PLC, use the "S7Online" option under "Access points" and select the desired TCP/IP adapter under "Assigned interface parameterization".

Note

If you select an option with the extension "TCP.IP.Auto.x" under "Assigned interface parameterization", connection problems may occur.



HTTPS communication via port 443

Unified PC Runtime uses port 443 for the HTTPS communication.

Using this port is mandatory. Before starting the installation, ensure that the port is free. Do not configure a different port.

Alarm control

The "Information" alarm class has the "Active" state machine, which defines an alarm without state. The alarm is therefore triggered immediately and deleted. When the value is evaluated, all bits are evaluated. This means the alarm is triggered for bit [0] and bit [2], although only bit [2] is changed - the entire value is evaluated.

System diagnostics control

The system diagnostics view does not support Soft PLC and 1500 R/H PLC.

My WinCC Unified

- The following applies for logging on to My WinCC Unified:

Logon via ...	Website of the Runtime web server is addressed via ...	
	Device names	**IP address**
Web client	Enter "https://<FQDN or device name>" of the web server in the address line of the browser.	Enter "https://<IP address of the HMI device>" of the web server in the address line of the browser.
Windows tray of a device with SIMATIC WinCC Unified Station Configurator installation	In the Windows system tray, select "SIMATIC WinCC Unified Station Configurator" > "Configure server". Enter the FQDN or device name of the web server under "Server".	In the Windows system tray, select "SIMATIC WinCC Unified Station Configurator" > "Configure server". Enter the IP address of the web server under "Server".

- To configure a client configuration for the local device in My WinCC Unified, enter the IP address of the local device under "Client settings > IP address".
  Do not enter 127.0.0.1 as the IP address.

Disabling Windows shortcuts for kiosk mode

On a device in kiosk mode

If you prevent access to the operating system via shortcuts, the Windows taskbar will no longer be displayed on the kiosk device in the following case. It is no longer possible to operate the device.

Initial situation:

- The device is configured in My WinCC Unified in such a way that the option "Disable shortcut keys for operating system access for operating system access" is deactivated in the kiosk settings.
- The configuration has been saved in My WinCC Unified.
- Kiosk mode has been started on the kiosk device.

Trigger incorrect response:

1. On the kiosk device, press the Windows key+D.
   Kiosk mode is minimized.
2. Open My WinCC Unified on the device.
3. In My WinCC Unified, update the kiosk settings for the kiosk device:
   - Select the option "Disable shortcuts for operating system access".
   - Save your change.

Solution:

You have the following options to block access to the operating system via shortcuts when the device is already in kiosk mode:

Option 1:

1. Terminate kiosk mode.
2. Open My WinCC Unified on the kiosk device.

3. In the kiosk device settings, activate the option "Disable shortcuts for operating system access".
4. Save the change.
5. Restart kiosk mode.

Option 2:

1. Open My WinCC Unified on a device other than the kiosk device.
2. In the kiosk device settings, activate the option "Disable shortcuts for operating system access".
3. Save the change in My WinCC Unified.

Archive databases and backwards compatibility

The method documented under "Using WinCC version compatibility" for replacing a Unified PC with installed Runtime only supports databases that use the "SQLITE" database type.

Trend control

Adding an IO field to a trend area using drag-and-drop

To add a trend in runtime by dragging and dropping an IO field, the following applies as of V19 Update 3:

- The following requirements must be met:
  - A trend control is configured on the HMI screen.
  - An IO field whose data type is not Date or Time is configured on the HMI screen.
  - The IO field does not have the focus.
  - For touch devices: No "Click left mouse button" event is configured on the IO field.
- Procedure on a device with a touch screen:
  - Press the IO field for at least 1 second without moving your finger.
  - Then drag your finger to the trend area.
- Procedure on a device without a touch screen:
  - Left-click on the upper or lower border of the IO field and keep the button pressed.
  - Do not move the mouse for at least 1 second.
  - Keep the left mouse button pressed and drag the IO field onto the trend area.

Adding a trend in runtime is not supported for function trend controls.

6.2 Improvements in Update 4

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Web browser

It is now possible to switch between tabs of the web browser by pressing Ctrl+Tab.

IO field

Negative floating point numbers are displayed correctly in an IO field, even in Unicode languages.

Alarms and alarm control

The sorting of alarms in the alarm control has been improved with regard to prioritized alarms.

The display and function of the scroll bar in the alarm control for specific altitude settings has been improved.

The alarm control is displayed correctly in Runtime even if the visibility changes dynamically.

Screen windows

Screen windows are displayed at the correct position in the screen even when dynamic resizing is performed.

PLC code view

Scrolling when changing the zoom level has been improved.

Faceplates

Symbolic IO fields in faceplates display external text lists correctly.

The use of color palette entries in the properties interface works correctly.

The dynamic font size is correctly transmitted via the properties interface.

Trend control

The trends of the function trend control are displayed correctly.

The display of the first data point in the function trend control in the Unified Panel has been corrected. Distant points can be added with the same X/Y value.

The settings of the trend control are also displayed correctly when opened for the first time after logging in to the web client.

The display of the grid lines when the axis ranges are dynamically changed works correctly.

The display of trend lines on PC Runtime and Unified Comfort Panel is uniform.

The dynamization of the Y axis has been improved.

The display of the trend control and the position of the associated buttons are uniform in simulation and Panel Runtime.

Reporting

Improved robustness in the display of the add-in interface based on the installed MS Excel version and browser version.

User management

When logging in automatically via "Domain Single Sign-On" (DSSO), central users with the "Password must be changed" option activated are shown a message to change their password.

GraphQL

- When calling the following operations, use the `languages` parameter to specify the languages in which the texts are returned:
  - Query "`activeAlarms`"
  - Query "`loggedAlarms`"
  - Subscription "`activeAlarms`"

  The order of the languages now corresponds to the order of the request.
- New behavior for GraphQL language filters
  For languages not configured in the Runtime settings, an empty value is now returned instead of nothing as before.
  This affects the following operations:
  - Query "`activeAlarms`"
  - Query "`loggedAlarms`"
  - Subscription "`activeAlarms`"

My WinCC Unified

If a PIN has been configured in the Kiosk settings, the PIN will now be displayed encrypted to users in the field.

SIMATIC Station Configurator

The setting to enable or disable shortcuts for accessing the operating system now works regardless of how Kiosk mode has been started.

6.3 Improvements in Update 2

6.3.1 General improvements in Update 2

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Licensing of WinCC Unified options

SIMATIC licenses are downward compatible. With a newer License Key from WinCC Unified options, older versions can also be operated.

Storage location of temporary files

The folder for storing temporary or cached files has been changed from "C:\Users\Public\Documents" to "C:\Users\Public\Siemens". As a result of this change, access to the folder works even if the Microsoft Windows security option "Monitored folder access" is enabled.

6.3.2 My WinCC Unified

Stronger PIN for exiting Runtime in kiosk mode

You have the option of increasing the security of the PIN for exiting Runtime in kiosk mode.

When configuring the kiosk mode, you can now activate the use of a 12- to 16-digit PIN. The PIN must contain numbers, special characters as well as upper and lower case letters.

Download the Station Configurator

If you select “Download” in the navigation bar in My WinCC Unified and download Station Configurator, the package with the installation files no longer starts with “_”.

Configuration of RFID login

Users can log into Runtime on local clients via RFID card and a card reader.

As of this update, you have the option of configuring the use of RFID cards in My WinCC Unified. There is no need to install additional software products.

Supported card readers

RFID Reader 10x0R (USB)

Supported functionality

- Maintain the RFID card list:
  - Register cards
  - Deregister cards
  - Edit the display names of the cards
- Manage RFID settings of users added in My WinCC Unified:
  - Assign cards
  - Configure login via PIN
  - Assign default PIN
- Users can view RFID cards assigned to them in My WinCC Unified.
- Users can change the PIN of the RFID cards assigned to them in My WinCC Unified.

Enable RFID

RFID must be activated for Runtime in order to configure login via RFID cards or to log into Runtime via RFID cards.

To activate RFID, you have the following options:

- When installing Unified PC Runtime, in the "User management" step
- After installing Unified PC in "WinCC Unified Configuration" in the "User management" step
- For projects with central user management: In the SIMATIC Runtime Manager settings on the "User management" tab

Maintaining the RFID card list

Introduction

In the RFID card list, you can register cards, deregister cards and edit the display name of the cards.

To register multiple RFID cards, proceed as described here.

To register a new RFID card for an individual user, there is the alternative option of registering a card inserted in the reader during the card assignment to a user. Proceed as described under "Manage user RFID settings".

Requirements

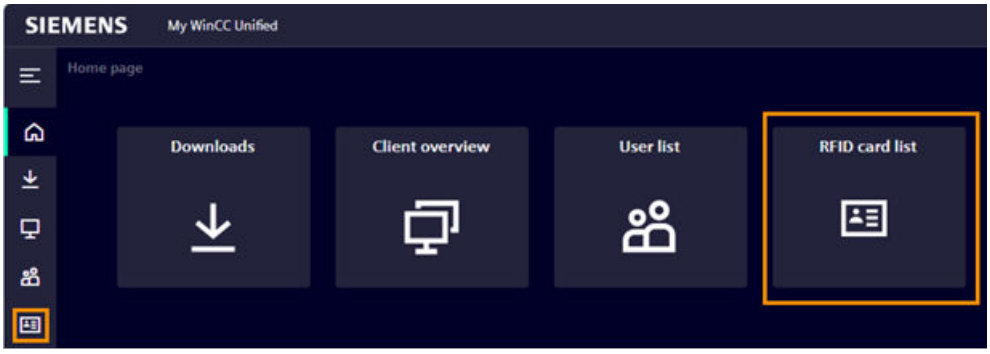
- RFID is activated for Runtime.
- You are logged into My WinCC Unified with a user who has the "User management" function rights.
- The card reader is connected to the HMI device.
- You have access to the reader and the RFID cards.

Restriction

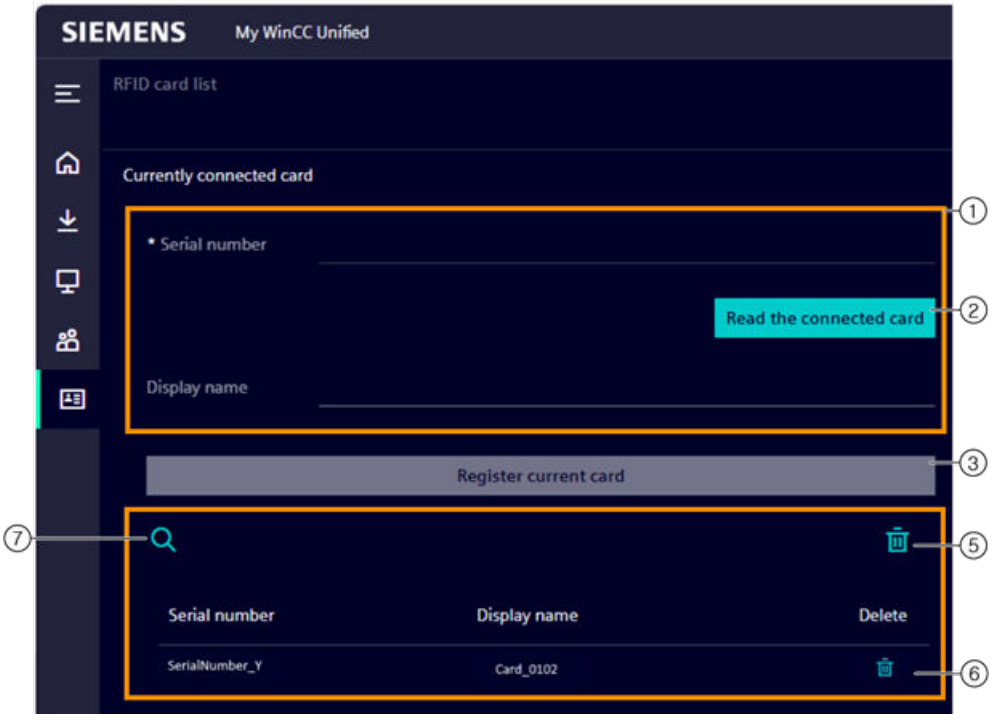
The display name of RFID cards is limited to 128 characters.

Procedure

1. Click on "RFID card list" in the start view of My WinCC Unified or in the navigation bar:



The RFID card list opens in the work area:



① Data of the last card read
② Button for reading the card inserted in the reader
③ Button for registering the last card read
④ List of cards registered for Runtime login
⑤ Button for deregistering all cards registered for Runtime login
⑥ Button for deregistering a single card
⑦ Button for browsing the list

2. To register an RFID card, proceed as follows:
   - Insert the card into the reader.
   - Click "Read connected card".
     The card data is read in and displayed

- (Optional): Enter the display name of the card in the "Display name" field.
- Click "Register current card".

The card is added to the list of registered cards.

3. To edit the display name of a registered card, proceed as follows:
   - Click on a display name in the list of registered cards.
     The field switches to the editing mode.
   - Enter the display name.
4. To deregister a card, click the button in the "Delete" column in the list of registered cards.
5. Save your entries.

Result

The cards from the list are registered for the login to Runtime.

Assign the cards to the users by configuring the RFID settings of the user.

Configure RFID settings of the users

Administrators configure the following for the users added in My WinCC Unified using the "RFID" configuration:

- Which RFID cards are assigned to the user
- Whether Runtime login with one of the assigned cards requires the entry of a PIN
- The standard PIN

Requirements

- RFID is activated for Runtime.
- You are logged into My WinCC Unified with a user who has the following function rights:
  - "User management"
  - "My WinCC Unified - Read and write access to all user settings"
- The user to whom you want to assign an RFID card has been added in My WinCC Unified.
- An alias has been stored for the user in the user management.
- At least one RFID card is registered in My WinCC Unified that is not yet assigned to a user.
  Or, if all cards are already registered:
  - The card reader is connected to the HMI device.
  - You have access to the card reader and an RFID card that has not yet been registered, and the card is inserted in the card reader.

Procedure:

1. Click on "User list" in the navigation bar: 
2. Click on a user in the navigator under "Users".
   The interface for the user configurations is loaded into the work area.

3. If the "RFID" configuration has already been added for the user, click "RFID".
   If the configuration has not yet been added, click "+" and select "RFID".
   The RFID configuration interface is loaded.
   Under "Card" you will see a list of the cards assigned to the user.
4. To assign a new card to the user, proceed as follows:
   - Click "+".
     A new entry is added to the list.
     If all registered cards are already assigned and a card is inserted in the card reader, this card is read in.
   - Open the drop-down list of the new entry.
     You are offered all cards registered in My WinCC Unified that are not yet assigned to a user or the card in the reader if it is not assigned to any user.
   - Select the desired card in the drop-down list.

   The card is added to the list and selected.
5. To link the login with a card to a PIN, proceed as follows:
   - Activate the "PIN required" option in the list for the card.
   - Enter a standard PIN with 8 digits in the "PIN" and "Repeat PIN" fields.
6. Click "Save":

Result:

- The card is assigned to the user.
- If you have selected the card inserted in the reader, the card is simultaneously registered in the RFID card list and assigned to the user.
  The display name is empty. Switch to the RFID card list to set the display name.

Additional options:

- Delete registered cards:
  - All cards: Use the buttons above the list with the registered cards and save.
  - Single card: Use the buttons in the list with the registered cards and save.
- Filter displayed cards:
  Use the search field above the list with the registered cards.

View your own cards

Requirements

- RFID is active for the project running in Runtime.
- You are logged into My WinCC Unified with a user who has one of the following function rights:
  - "My WinCC Unified – Read access to user and device settings"
  - "My WinCC Unified – Read/write access to the user's own settings"

Procedure

In the "User list" under "Users", click on your user and then "RFID".

Change your own PIN

Requirements

- RFID is active for the project running in Runtime.
- You are logged into My WinCC Unified with a user who has the following function right: "My WinCC Unified – Read/write access to the user's own settings"

Procedure

1. In the "User list" under "Users", click on your user and then "RFID".
2. In the "Card" list, click on a card for which the "PIN" option is activated.
3. Enter a new PIN in the "PIN" and "Repeat PIN" fields.
4. Click "Save": 

6.4 Improvements in Update 1

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Redundant systems

PLC alarms are received on both redundant partners.

6.5 Improvements in Service Release 1

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Unified Runtime

After a complete download in RUN, the redundancy switchover is again possible.

If a screen is adapted to the window size and has a solid background, clicking on the background no longer triggers events of elements that are positioned behind the screen.

Unified Comfort Panels

7

7.1 Important information

This section contains important information about product properties.

"System Properties" > "Event Logger"

Only activate the Event Logger for a short period of time as a large amount of data is recorded on the storage medium. If the remaining memory on the storage medium is greatly reduced, this can affect other processes using the storage medium, e.g. alarm logging.

Important information about the X1 and X2 interfaces

DNS is only supported by X2

The use of a DNS server for name resolution is only supported by the interface X2.

Use interface X2 for connections that require DNS name resolution, such as a UMC server for central user management.

Use the interface X2 for connections that require DNS name resolution, such as a UMC server for central user management.

"Network and Internet" > "Network settings" > "PN-X2" > "Ethernet parameters Port"

Note that interface X2 does not support the two "Boundaries" options "End of detection of accessible nodes" and "End of topology discovery".

DCP frames and LLDP frames are therefore always forwarded via interface X2, which enables the recognition of reachable devices and topology discovery for devices that are connected to this interface.

Important notes on storage media

Executing scripts

The execution of scripts from an external storage medium via the "StartProgram" system function is not permitted.

Operating system downgrade and alarm logging

Alarm logs created with a higher HMI device image version cannot be read or updated with a lower HMI device image version.

Example: Alarm logs that have been created with HMI device image V20.0.0.0 cannot be loaded with HMI device image V19.0.0.0.

In this case, the alarm control displays an error message regarding the incompatibility between database version and Runtime version.

After downgrading, use an empty storage medium for alarm logging.

"Backup/Restore" and local user administration

Depending on the HMI device image version, local user administration malfunctions may occur in the following case:

- Restoring a backup from a device running image version ≤19.0.0.2 to a device with image version 20.0.0.0

Solution: Install an image version ≥20.0.0.2 on the target device and then perform the restore.

Updating the operating system and RFID login

Correction to the statement in the Operating Instructions Unified Comfort Panels TIA 20 (12/2024) (https://support.industry.siemens.com/cs/ww/en/view/109977041), PDF file page 115:

The RFID assignments are retained even after updating the operating system if the "Keep current user administration data in runtime" option is **enabled** in the "Load preview" dialog during project transfer.

Notes on the "Edit user" and "Add user" dialogs

Observe the following information regarding the "Edit user" and "Add user" dialogs of the local user administration.

Cancel RFID assignment process

When you assign a user an RFID login via the "Edit user" or "Add user" dialog, the "RFID assignment – Are you sure you want to apply these configurations?" dialog is displayed with the "OK" and "Cancel" buttons. You start the RFID assignment using the "OK" button, you cancel the assignment with "Cancel".

If you select "Cancel", the dialogs "RFID assignment" and "Edit user"/"Add user" are closed and you are back in the user list.

No RFID login is assigned to the selected user.

Adding a PIN

Use the "Edit user" button to assign a PIN to a user who already has an RFID login in the "Edit user" dialog.

Adding a PIN logs the user in

If you assign a PIN to a user who already has an RFID login in the “Edit user” dialog, the user is logged in immediately after the assignment.

Entering PIN immediately with PIN activation

If you select the "PIN required for authentication with RFID card" option for a user, enter a PIN in the "PIN" input field before pressing the "Edit user" or "Add user" button.

Changing a user's RFID PIN

To change a user's PIN, delete the user and create it again.

Resource-intensive SIMATIC Edge apps

The simultaneous operation of a runtime project and resource-intensive Edge apps can lead to performance losses.

Reduce the resource requirements of the apps as much as possible.

NTP server settings

The NTP server settings are deleted when HMI device image version ≤18.0.0.1 is updated to HMI device image version ≥19.0.0.0.

If you use one or several NTP servers, note down - before updating the HMI device image - the NTP server settings and enter them again in the Control Panel under "Language, Region and Formats" > "Date and time" after performing the update.

Notes on the apps under "Add-ons"

Playback quality in the media player

Depending on the load on the HMI device, the playback quality of videos in the "Media Player" app may vary. If the playback quality is inadequate, reduce the load on the HMI device as much as possible, e.g. by closing unnecessary apps.

Supported formats, resolutions and frame rates

Note

The following information also applies to the playback of videos in the Runtime controls "Media player" and "Browser".

The "Media Player" app and the "Media player" and "Browser" Runtime objects support the following video formats:

- mp4
- ogv (VP8/VP9 Codec)
- webm
- mkv

The following table displays recommendations for maximum resolution and frame rate for smooth video playback.

Unified HMI device	Resolution / pixels	Frame rate/ frames per second
MTP700 Unified Comfort	800 x 400	30
MTP1000 Unified Comfort	1280 x 800	30
MTP1200 Unified Comfort	1280 x 800	30
MTP1500 Unified Comfort	1366 x 768	30

Unified HMI device	Resolution / pixels	Frame rate/ frames per second
MTP1900 Unified Comfort	1920 x 1080	30
MTP2200 Unified Comfort	1920 x 1080	30

Notes on the MRP domain names

If you use media redundancy for a Unified Comfort Panel in WinCC (TIA Portal), please take into account the following notes with regard to the name under "MRP domain":

- The MRP domain name must comply with the DNS naming convention and must not contain any special characters. Otherwise, communication errors can occur.
- During configuration, an MRP domain name is automatically generated in accordance with the DNS naming convention.
- To avoid communication errors, use the automatically generated MRP domain name or change the name in accordance with the DNS naming convention.

Output directory for scripts in tasks

It is not permitted to write to the "home/industrial" directory via scripts in Scheduler tasks; use an external storage medium instead.

Important notes on ProDiag

User-defined styles

If user-defined styles (new templates) are configured, the ProDiag controls (GRAPH overview and PLC code view) are displayed in the predefined style of the type "Extended style".

Alarm control

Flashing on range violation

Flashing on range violation is not supported for the alarm control.

Scroll bars

Scroll bars are not available in the alarm control. Use the touchscreen to move the contents of the alarm control horizontally or vertically.

Moving columns

Moving columns within the alarm control is not supported.

Filtering alarms

Multiple selection of filter criteria is not supported in the filter dialog of the alarm control.

Dynamizing visibility of columns

Dynamization of the visibility of columns via a script or a system function is not supported.

System diagnostics control

The system diagnostics control is not supported in conjunction with a Software Controller or S7-1500R/H controller.

Number of connections to LOGO! controllers

Up to and including HMI device image V20.0.0.2, the HMI device supports a maximum of three connections to LOGO! controllers. As of HMI device image V20.0.0.4, this restriction has been eliminated; the information in the operating instructions applies.

SetBrightness

The "SetBrightness" system function and "SetBrightness" method specify the brightness of the screen. The value can be set between 0 and 100. The HMI devices support a brightness setting between 10 and 100%. The brightness settings on the HMI device can be viewed and edited in the Control Panel under "Settings > Display". When the HM I device is restarted, the configuration set in the Control Panel is restored.

- If a value between 0 and 10 is assigned, a brightness of 10% is set for the display.
- If a value between 0 and 100 is assigned, the brightness is set according to this value.

Communication with a third-party OPC UA server

Proceed as follows to enable a panel to connect as an OPC UA client to a third-party OPC UA server whose OPC UA server certificate has been issued by a certification authority (CA):

1. Export the root certificate and the CRL file of the certification authority.
   Proceed as described in the operating instructions for the OPC UA server.
2. (Recommended) Stop Runtime on the panel.
3. Import the root certificate and the CRL file to the panel.
   Proceed as described in TIA Portal in the user help "Certificates in WinCC Unified Runtime".

After the import, the panel trusts the root certificate. It therefore also trusts the OPC UA server certificate when establishing a connection.

To display the root certificate, select "Certificate Authorities" as the "Certificate Store" entry in the "Security > Certificates" control panel. For the CRL file, select "Certificate Revocation List".

Note

Transfer and display of the OPC UA server certificate

When the connection is established, the OPC UA server transmits its application certificate to the panel.

To display the certificate, select "Other Certificates" as the "Certificate Store" entry in the "Security > Certificates" control panel.

This certificate is for information purposes only.

7.2 Connecting Unified Comfort Panel with SQL database

Introduction

You can access MS SQL databases and SQLite databases via JavaScript functions from the Unified Comfort Panel. Note that the resource utilization is directly proportional to the number of the requests to the database and the size of the data to be read or written. This means that frequent access to databases can also affect the performance in Runtime.

The following database options are available for Unified Comfort Panels:

- Microsoft SQL with the driver:

ODBC driver name	Description
{ODBC Driver 18 for SQL Server}	Microsoft ODBC driver for SQL Server version 18.3 Included in this version are: • Azure SQL Database • Azure Synapse Analytics • Azure SQL Managed Instance • SQL Server 2022 • SQL Server 2019 • SQL Server 2017 • SQL Server 2016 • SQL Server 2014

- SQLite with the driver:

ODBC driver name	Description
{SQLite3}	SQLite3 ODBC driver

To create a connection to the database with the "CreateConnection" method, a "connectionString" parameter of type "String" is transferred. The "connectionString" parameter has the form:

MS SQL	`let connectionstring = "DRIVER={ODBC Driver 18 for SQL Server};DATABASE=UCP; UID=userid; PWD=password; trusted_connection=no; SERVER=ipaddress,port_number;TrustServerCertificate=yes";`
	Example:
	`let connectionstring = "DRIVER={ODBC Driver 18 for SQL Server};DATABASE=UCP; UID=TestUser; PWD=test; trusted_connection=no; SERVER=192.168.0.115,1433;TrustServerCertificate=yes";`

SQLite	`let connectionstring = "Driver={SQLite3};Database=PathToDatabase;trusted_connection=yes; ";`
	Example:
	`let connectionstring = "Driver={SQLite3};Database=/media/simatic/X51/MyUCP.db;trusted_connection=yes;";`

Example

The example shows how you can use a button to establish a connection between a Unified Comfort Panel and an SQL server. You create a table there and then close the connection to the server.

1. Configure a button.
2. Specify "Click right mouse button" as event.
3. Convert the event into a script.
4. Insert the sample code into the script.

Result

By clicking the button you establish a connection with an MS SQL database. You create a table and close the connection again.

Sample code

```
//JEx: "CreateConnection"
//SOM_OM_"HMIDatabaseConnection"

(async function() {
try{
HMIRuntime.Trace("Open MS SQL DB");
let connectionstring = "DRIVER={ODBC Driver 18 for SQL Server};
DATABASE=UCP; UID=TestUser; PWD=test; trusted_connection=no;
SERVER=192.168.0.115,1433;";
let conn = await HMIRuntime.Database.CreateConnection(connectionstring);
let query = "Create Table TableMotorData (Name varchar(50), ID char, Temp
float);";
let results = await conn.Execute(query);
conn.Close();
HMIRuntime.Trace("Close MS SQL DB");
}
catch(e)
{
let res = e.Results;
for(let statement in res)
{
let errors = res[statement].Errors;
for (let i in errors)
{
let detailed = errors[i];
HMIRuntime.Trace("Errors state : " + detailed.State);
HMIRuntime.Trace("Errors Message : " + detailed.Message);
}
}
}
})();
```

7.3 Improvements in V20 Upd.2

7.3.1 General improvements in V20 Upd.2

This update contains the HMI device image version 20.0.0.2. To make use of the corresponding Engineering and Runtime improvements, we recommend using WinCC Unified V20 Update 3 for configuring the HMI devices.

Stability and performance

The stability and performance have been improved based, among other things, on the feedback received.

Operating system downgrade and "Alarm persistency"

From now on, when updating the operating system, all data in the message buffer will be deleted, also when you perform an operating system downgrade to a lower major version (e.g. V20 to V19). This means that "Alarm persistency" no longer has to be disabled before an operating system downgrade.

Unified Air

With this update, new functions are available for Unified Air, for example

- Display device information of the HMI device on the mobile device
- Create screenshots in Runtime and download them to the mobile device
- Create and download a summary of device information, device utilization as well as Runtime data to the mobile device.

Detailed information can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109827893).

Secure removal of storage media

The behavior of the device when pressing the "Eject storage media" button in the Control Panel or when calling the "EjectStorageMedium" system function has been improved as follows:

- If Runtime or another application such as "File Browser" or "Trace logger" accesses the storage medium, a dialog is displayed which informs the user that the storage medium cannot be safely removed. Make sure that there is no access to the storage medium when you press the button or call up the system function.
- If the storage medium is not being accessed, a dialog is displayed which informs the user that the storage medium has been successfully ejected.
  The dialog is automatically closed after a timeout of 10 seconds.
  If you missed the timeout, check the status of the storage medium in the Control Panel under "External Devices and Input" > "Connected devices".

Extended printer management

With this update, the additional function "Printers" is available for printer management in the Control Panel under "Devices and Input".

The "Apps" > "Printer Configuration" add-on no longer leads to the local website "CUPS", but also to "Devices and Input" > "Printers".

Under "Printers" you will find all previous and extended features, such as:

- An extensive list of preinstalled printers
- A "PDF" default printer
- Functions to change or copy preinstalled printers or their settings
- Functions to add or delete more printers

The list of supported printers has been extended to include the following models:

- Brightek WH-E89
- Brightek WH-P12
- Brother HL-2260DN
- Brother DCP-L1848W
- HP LaserJet Tank 2606dw
- HP LaserJet MFP 1188w

Under "Printers", you can adjust the settings of preinstalled printers, copy printers or add more printers using the "Add printer" button.

The description of the new "Printers" function is available in the section ""Devices and Input" > "Printers" (Page 102)".

The screen keyboard in Runtime

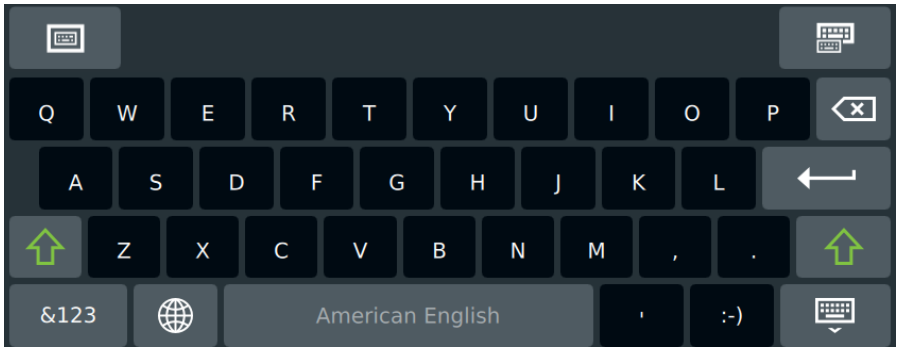
In Runtime, a separate screen keyboard with extended functionality is now available, see the following section "The screen keyboard in runtime (Page 100)".

The following applies with regard to switching the language of the screen keyboard:

- The language of the screen keyboard corresponds to the set Runtime language.
- The English, German, Chinese (simplified and traditional), French, Italian and Spanish languages are supported. The English screen keyboard is used for all other languages.
- To switch the language manually, select the desired language and reopen the screen keyboard.

7.3.2 The screen keyboard in runtime

When you open it for the first time in runtime or after restarting runtime, the screen keyboard is displayed in its default position and in its maximum size.



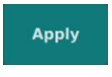
The screen keyboard in runtime has the keyboard layout of the screen keyboard in the Control Panel and has a title bar with additional control keys and functions.

You can use additional control keys to release the screen keyboard from its default position in runtime, move it, scale it and, if necessary, fix it again in its default position.

The last used position and size of the screen keyboard is saved. When reopened, the screen keyboard will be displayed again in the saved position and size.

Additional control keys in runtime

The following additional control keys with the following functions are available in the title bar of the screen keyboard.

	"Undock": Remove the screen keyboard from its default position. The bar for moving the screen keyboard appears. If the screen keyboard has already been moved to a different position, it is displayed in this position.
	"Move": The screen keyboard is removed from its default position and can be moved to another position using the bar.
	"Dock": The screen keyboard will be fixed back to its default position. The bar for moving the screen keyboard is no longer displayed.
	"Scale": The screen keyboard can be scaled and moved using gestures. The "Apply" button for saving size and position appears. Depending on whether the screen keyboard has already been moved or not, the following applies: • If the screen keyboard has already been moved to a different position, it is displayed in this position. • If the screen keyboard was still in the original default position (e.g. after start of runtime), then it will be released from its default position. Note: Scaling screen content in runtime has no influence on the size of the screen keyboard.
	"Apply": The changed scaling and position of the screen keyboard is saved.

Moving the screen keyboard

If the screen keyboard is released from its default position, you can move the screen keyboard.

Moving the screen keyboard via "Undock"

1. Press the "Undock" button in the upper left corner of the screen keyboard.



2. Drag the screen keyboard to the desired position using the "Move" bar.

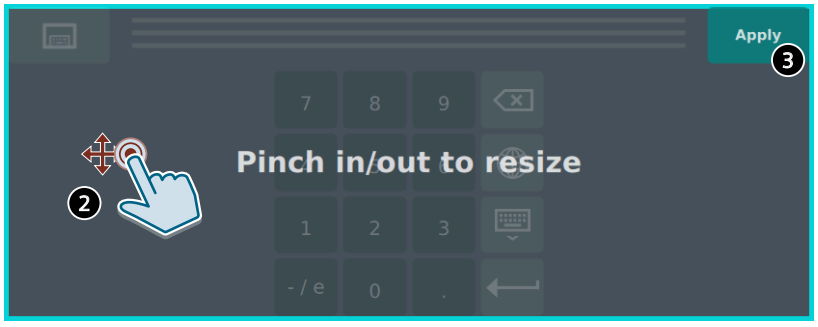


Moving the screen keyboard via "Scale"

1. Press the "Scale" button in the top right corner of the screen keyboard.



2. Drag the screen keyboard to the desired position within its boundary and outside the "Apply" button.



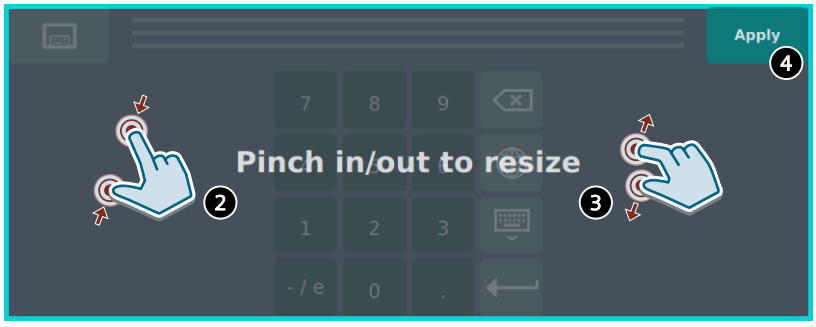
3. Save the setting with "Apply".

Scaling the screen keyboard

1. Press the "Scale" button in the top right corner of the screen keyboard.



2. If desired, reduce the size of the screen keyboard using a "zoom out" gesture.
   When you open it for the first time or after restarting runtime, the screen keyboard is displayed in its maximum size and can only be reduced.



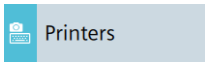
3. If desired, enlarge the screen keyboard using a "zoom in" gesture.
4. Save the setting with "Apply".

7.3.3 "Devices and Input" > "Printers"

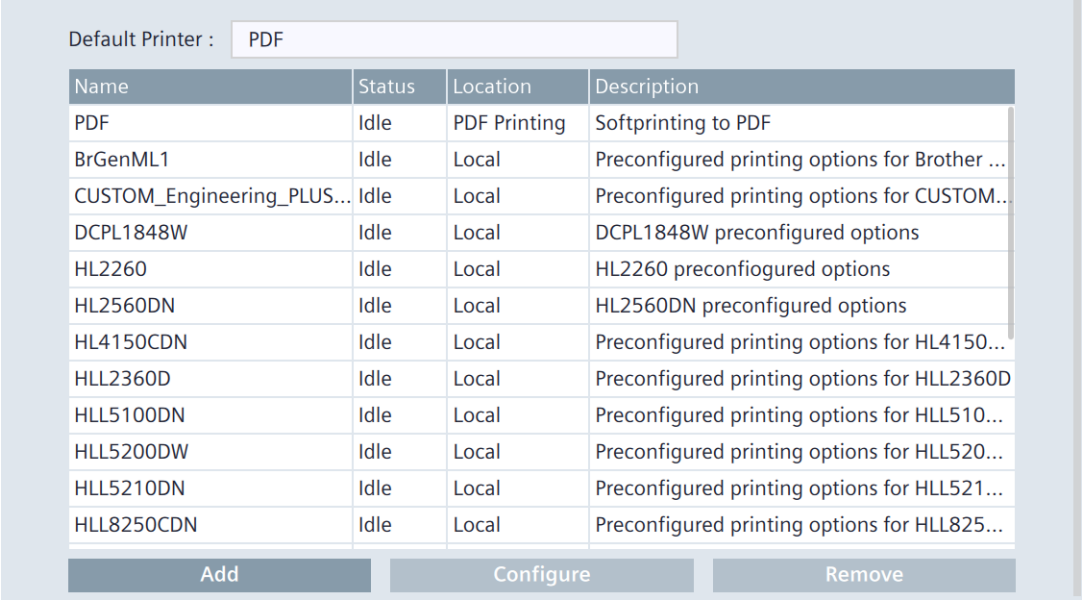
Under "Printers", you manage USB printers for the HMI device. Network printers are not supported.

To add a new printer, you need the associated PostScript Printer Description (PPD) file from the manufacturer.
Maximum allowed PPD file size: 1 MB

The list of the printers is retained even after the operating system has been updated.



Printers



The list displays all available printers.

- "Default Printer": The preferred printer is displayed in this field. The default setting is "PDF". The printer set as "Default Printer" is always displayed in the first line of the printer list. If you add a new printer, select it as "Default Printer" and delete it again later, "PDF" automatically becomes the "Default Printer" again.
- The printer list contains the following columns:
  - "Name": Printer name
  - "Status": Information on the printer activity. Possible values are "Idle", "Printing", "Pause" and "Unknown".
    The status is updated approximately every 3 seconds.
  - "Location" and "Description": Optional comments. You can find more information in the following "Adding a printer" section.

  To sort the entries in the table alphabetically by the content of a column, with the exception of "Default Printer", tap on the header of the corresponding column.
- "Add": Button for adding a further printer.
- "Configure": Button to edit or copy a printer driver, only available in the "Idle" state.
- "Remove": Button to delete printer drivers that were added via "Add". The preinstalled printer drivers cannot be deleted. Removing a printer deletes all pending print jobs from that printer.

The list can have a maximum of 50 entries.

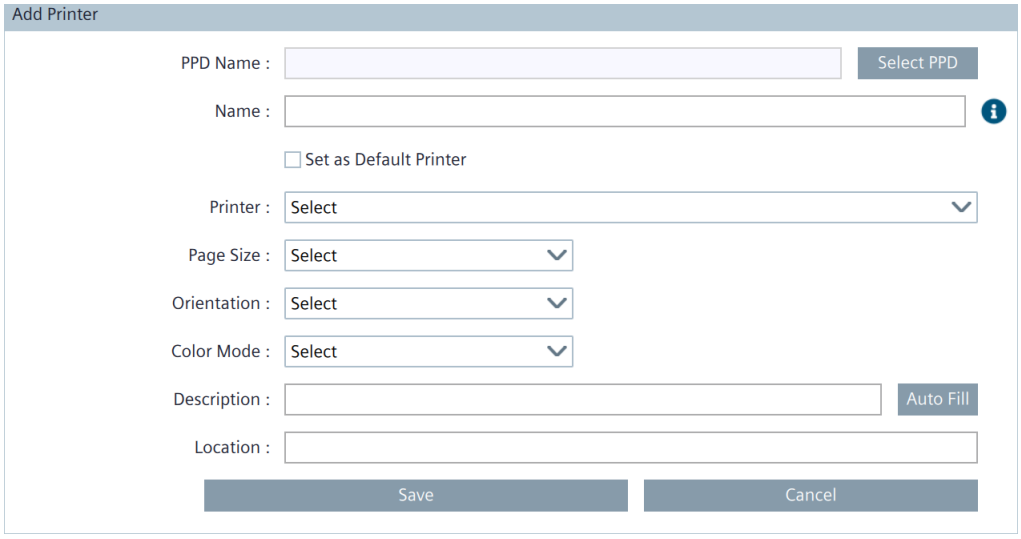
Adding a printer

Requirements

- The new printer supports Linux and CUPS.
- The PPD file for the new printer is available (maximum size 1 MB).

Proceed as follows to add another printer to the list.

1. Select "Add".

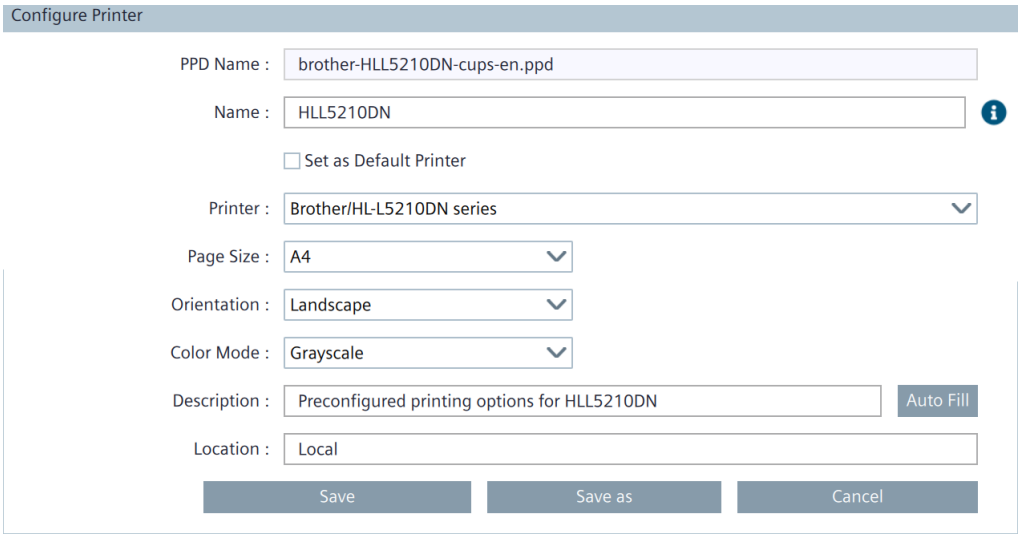


2. Enter the PPD file of the new printer via the "Select PPD" button.
3. Enter a name for the new printer under "Name".
   The name must not contain a space or any of the following special characters:
   ! # $ & ( ) * + , : ; < = > ?' @ [ ] _ { | } ~ ^
4. If desired, enable the "Set as Default Printer" option.
5. If the desired printer is already connected to the HMI device, select the corresponding printer model under "Printer". Otherwise, leave the entry unchanged at "Select" and enter the printer model once the printer is connected to the HMI device. The printer is then fully activated and ready for use.
   The "Printer" entry only needs to be set once for each printer. If you disconnect and reconnect an already activated printer from the HMI device, you do not need to select this printer again under "Printer".
6. Select the default settings for page size, orientation and color mode.
7. Under "Description" you can enter a description for the printer.
   The "Auto Fill" button generates an entry that consists of the values of "Page Size", "Orientation" and "Color Mode".
8. You can add an additional comment under "Location".
9. Select "OK" to add the new printer.

Editing or copying printer settings

Proceed as follows.

1. Select a printer from the list and press "Configure".
   The "Configure Printer" dialog opens. The following figure shows an example.



2. To edit the settings of the selected printer, make the desired changes and select "Save".
3. To copy the printer settings, change the entry under "Name", adjust the other settings, and select "Save as".
   This also allows you to save different settings for a specific printer.

The "Configure Printer" dialog is closed and the settings are saved.

Unified Basic Panels

8

8.1 Important information

This section contains important information about product properties.

Operating system downgrade and alarm logging

Alarm logs created with a higher HMI device image version cannot be read or updated with a lower HMI device image version.

Example: Alarm logs that have been created with HMI device image V20.0.0.0 cannot be loaded with HMI device image V19.0.0.0.

In this case, the alarm control displays an error message regarding the incompatibility between database version and Runtime version.

After downgrading, use an empty storage medium for alarm logging.

"Backup/Restore" and local user administration

Depending on the HMI device image version, local user administration malfunctions may occur in the following case:

- Restoring a backup from a device running image version ≤19.0.0.2 to a device with image version 20.0.0.0

Solution: Install an image version ≥20.0.0.2 on the target device and then perform the restore.

Alarm control

Flashing on range violation

Flashing on range violation is not supported for the alarm control.

Scroll bars

Scroll bars are not available in the alarm control. Use the touchscreen to move the contents of the alarm control horizontally or vertically.

Moving columns

Moving columns within the alarm control is not supported.

Filtering alarms

Multiple selection of filter criteria is not supported in the filter dialog of the alarm control.

Dynamizing visibility of columns

Dynamization of the visibility of columns via a script or a system function is not supported.

System diagnostics control

The system diagnostics control is not supported in conjunction with a Software Controller or S7-1500R/H controller.

Number of connections to LOGO! controllers

Up to and including HMI device image V20.0.0.2, the HMI device supports a maximum of three connections to LOGO! controllers. As of HMI device image V20.0.0.4, this restriction has been eliminated; the information in the operating instructions applies.

Number of connections to LOGO! controllers

The HMI device supports a maximum of 3 connections to LOGO! controllers.

SetBrightness

The "SetBrightness" system function and "SetBrightness" method specify the brightness of the screen. The value can be set between 0 and 100. The HMI devices support a brightness setting between 10 and 100%. The brightness settings on the HMI device can be viewed and edited in the Control Panel under "Settings > Display". When the HM I device is restarted, the configuration set in the Control Panel is restored.

- If a value between 0 and 10 is assigned, a brightness of 10% is set for the display.
- If a value between 0 and 100 is assigned, the brightness is set according to this value.

Create screenshot

The "CreateScreenshot" system function and the "CreateScreenshot" method are also available for WinCC Unified Basic Panels. WinCC Unified Basic Panel only supports the ".png" file format. If a different file format is selected, the screenshot is not created.

Communication with a third-party OPC UA server

Proceed as follows to enable a panel to connect as an OPC UA client to a third-party OPC UA server whose OPC UA server certificate has been issued by a certification authority (CA):

1. Export the root certificate and the CRL file of the certification authority.
   Proceed as described in the operating instructions for the OPC UA server.
2. (Recommended) Stop Runtime on the panel.
3. Import the root certificate and the CRL file to the panel.
   Proceed as described in TIA Portal in the user help "Certificates in WinCC Unified Runtime".

After the import, the panel trusts the root certificate. It therefore also trusts the OPC UA server certificate when establishing a connection.

To display the root certificate, select "Certificate Authorities" as the "Certificate Store" entry in the "Security > Certificates" control panel. For the CRL file, select "Certificate Revocation List".

Note

Transfer and display of the OPC UA server certificate

When the connection is established, the OPC UA server transmits its application certificate to the panel.

To display the certificate, select "Other Certificates" as the "Certificate Store" entry in the "Security > Certificates" control panel.

This certificate is for information purposes only.

8.2 Improvements in V20 Upd.2

8.2.1 General improvements in V20 Upd.2

This update contains the HMI device image version 20.0.0.2. To make use of the corresponding Engineering and Runtime improvements, we recommend using WinCC Unified V20 Update 3 for configuring the HMI devices.

Stability and performance

The stability and performance have been improved based, among other things, on the feedback received.

Operating system downgrade and "Alarm persistency"

From now on, when updating the operating system, all data in the message buffer will be deleted, also when you perform an operating system downgrade to a lower major version (e.g. V20 to V19). This means that "Alarm persistency" no longer has to be disabled before an operating system downgrade.

Secure removal of storage media

The behavior of the device when pressing the "Eject storage media" button in the Control Panel or when calling the "EjectStorageMedium" system function has been improved as follows:

- If Runtime or another application such as "File Browser" or "Trace logger" accesses the storage medium, a dialog is displayed which informs the user that the storage medium cannot be safely removed. Make sure that there is no access to the storage medium when you press the button or call up the system function.
- If the storage medium is not being accessed, a dialog is displayed which informs the user that the storage medium has been successfully ejected.
  The dialog is automatically closed after a timeout of 10 seconds.
  If you missed the timeout, check the status of the storage medium in the Control Panel under "External Devices and Input" > "Connected devices".

The screen keyboard in Runtime

In Runtime, a separate screen keyboard with extended functionality is now available, see the following section "The screen keyboard in runtime (Page 110)".

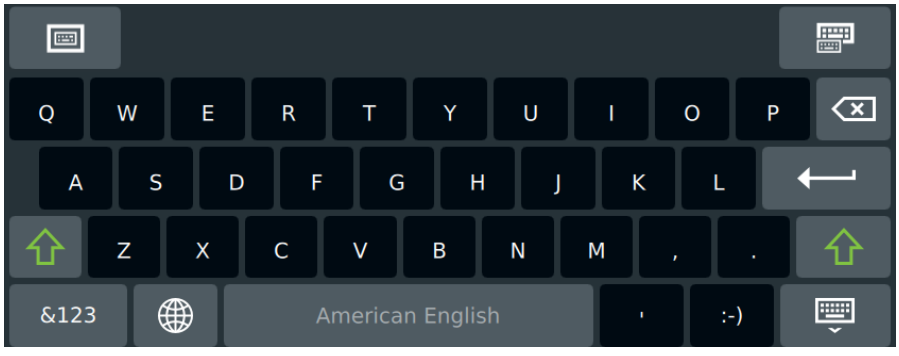
The following applies with regard to switching the language of the screen keyboard:

- The language of the screen keyboard corresponds to the set Runtime language.
- The English, German, Chinese (simplified and traditional), French, Italian and Spanish languages are supported. The English screen keyboard is used for all other languages.
- To switch the language manually, select the desired language and reopen the screen keyboard.

8.2.2 The screen keyboard in runtime

When you open it for the first time in runtime or after restarting runtime, the screen keyboard is displayed in its default position and in its maximum size.

The following figure shows an example for the on-screen keyboard of a device with display diagonal ≥ 7".



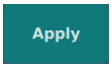
The screen keyboard in runtime has the keyboard layout of the screen keyboard in the Control Panel.

On devices with a display diagonal ≥ 7", the on-screen keyboard has a title bar with additional functions and features:

- You can use additional control keys to release the screen keyboard from its default position in runtime, move it, scale it and, if necessary, fix it again in its default position.
- The last used position and size of the screen keyboard is saved. When reopened, the screen keyboard will be displayed again in the saved position and size.

Additional control keys in runtime (devices with display ≥ 7")

The following additional control keys with the following functions are available in the title bar of the screen keyboard.

	"Undock": Remove the screen keyboard from its default position. The bar for moving the screen keyboard appears. If the screen keyboard has already been moved to a different position, it is displayed in this position.
	"Move": The screen keyboard is removed from its default position and can be moved to another position using the bar.
	"Dock": The screen keyboard will be fixed back to its default position. The bar for moving the screen keyboard is no longer displayed.
	"Scale": The screen keyboard can be scaled and moved using gestures. The "Apply" button for saving size and position appears. Depending on whether the screen keyboard has already been moved or not, the following applies: • If the screen keyboard has already been moved to a different position, it is displayed in this position. • If the screen keyboard was still in the original default position (e.g. after start of runtime), then it will be released from its default position. Note: Scaling screen content in runtime has no influence on the size of the screen keyboard.
	"Apply": The changed scaling and position of the screen keyboard is saved.

Moving the on-screen keyboard (devices with display ≥ 7")

If the screen keyboard is released from its default position, you can move the screen keyboard.

Moving the screen keyboard via "Undock"

1. Press the "Undock" button in the upper left corner of the screen keyboard.



2. Drag the screen keyboard to the desired position using the "Move" bar.

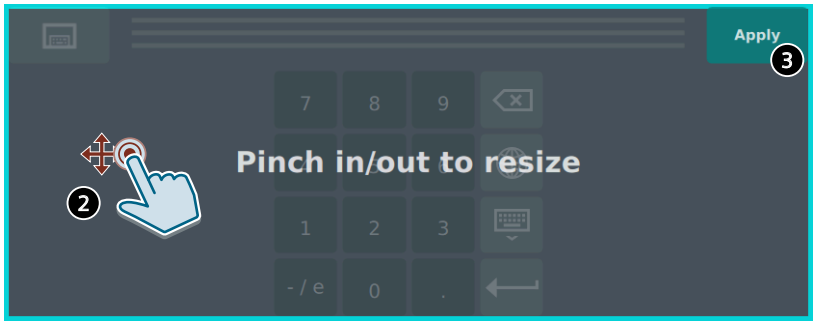


Moving the screen keyboard via "Scale"

1. Press the "Scale" button in the top right corner of the screen keyboard.



2. Drag the screen keyboard to the desired position within its boundary and outside the "Apply" button.



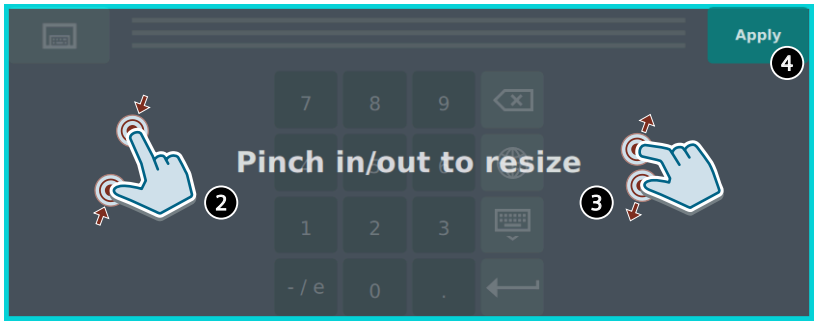
3. Save the setting with "Apply".

Scaling the on-screen keyboard (devices with display ≥ 7")

1. Press the "Scale" button in the top right corner of the screen keyboard.



2. If desired, reduce the size of the screen keyboard using a "zoom out" gesture.
   When you open it for the first time or after restarting runtime, the screen keyboard is displayed in its maximum size and can only be reduced.



3. If desired, enlarge the screen keyboard using a "zoom in" gesture.
4. Save the setting with "Apply".

9 Redundancy

9.1 Redundancy switchover of the web clients with local user management

Redundancy switchover of the web clients is now also possible with local user management.

When a download is performed during which the user data is overwritten, the operator needs to log in again on the first web client redundancy switchover, in contrast to central user management.

Note

When using local user management, it must be ensured that the same users are configured on Unified PC 1 and 2. During a full download in Run to a computer, the modified users are not synchronized with the second computer.

Audit

10

10.1 General improvements in Update 3

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Adjustment of the time stamp format in the "Audit Viewer" control

In the Engineering System, users have now the option to configure the time stamp format with which the date and time are displayed in the "Audit Viewer" control in Runtime.

To that end, in the engineering, configure the "Time stamp format" property in the properties of the control under "Miscellaneous > Interface > General".

You have the following options:

- Select one of the preconfigured entries under "Date and time" or "Date and time (automatic, language dependent)".
- Enter the desired format manually in the field.
- Add a dynamization and apply the value, for example, from a tag.

Result

After the compile and load, all the specifications for date and time are displayed in Runtime in the "Audit Viewer" control in the format that you have selected.

If the property is empty or contains an incorrect value, the current Runtime language is evaluated and the standard format of the corresponding region is used.

Display of checked Audit data records

Checked audit data records are correctly displayed in the Audit Trail as either valid or manipulated.

10.2 Audit Trail parameters

Based on an Audit Trail report, it is possible to determine which operator carried out operator actions at which time. The configuration engineer uses the WinCC Unified Excel add-in to configure a report template with parameters of the Audit Trail. The parameters are relevant for quality assurance in the manufacturing process. You can print out the report either as an Excel file, a PDF file or send it via email.

General information on configuring report templates in the Excel add-in is available in Creating report templates for production protocols.

General functions on the configuration of report jobs in runtime are available in Working with production protocols in runtime.

Audit Trail parameters

The following table contains an overview of the potential values of the individual report columns:

Parameter	Description
Time stamp	Contains the time stamp at which the event occurred.
Object name	Contains the name of the object that triggered the change.
User	Contains the name of the logged-on user. When no user is logged on, the field remains empty.
Operator Station	Contains either the name of the PC or PLC, or the IP address of the web client.
Old value	Contains the tag value before the change.
New value	Contains the tag value after the change.
Reason	Contains the user comment for user actions or the result of the operation for system responses.
Event ID	Contains the internal identifier of the event.
Tracking ID	Contains the internal identifier to link the user action to the system response.
Provider type of the audit	Refers to the internal system component in which the change was made.
	2 - Task scheduler "Scheduler" is entered as provider type in the event of changes in the configured cyclic tasks.
	6 - User interface "UI" is entered as provider type in the event of changes made via the user interface.
	8 - User management On changes to the user management: e.g.: "User management" is entered as provider type on login or logout.
	11 - System diagnostics In the event of changes made by the system in connection with the system response, e.g. "WriteTag", "System diagnostics" is entered as provider type.
Audit provider	Contains the name of the provider, for example, Scheduler, User Interface, Event Manager.
Type of operation	Specifies whether the changed object was created, modified or deleted. 1 - New value 2 - Updated value 3 - Deleted value
Object reference	Contains an identifier of the triggering object. This parameter is reserved for internal purposes.
Integrity	Contains an identifier for proof that data was manipulated later.
Signature	Contains the information on the provided electronic signature (user, role, contract).

Note

Type of operation

Due to the harmonization of the type of operation and to avoid changes to already logged data in the Audit Trail, the description of the type of operation of the previously logged data records differs from the new description.

Unified Station Configurator

11

11.1 Important information

This page contains important information about product properties.

Disabling Windows shortcuts for kiosk mode

On a device in kiosk mode

If you prevent access to the operating system via shortcuts, the Windows taskbar will no longer be displayed on the kiosk device in the following case. It is no longer possible to operate the device.

Initial situation:

- The device is configured in My WinCC Unified in such a way that the option "Disable shortcut keys for operating system access for operating system access" is deactivated in the kiosk settings.
- The configuration has been saved in My WinCC Unified.
- Kiosk mode has been started on the kiosk device.

Trigger incorrect response:

1. On the kiosk device, press the Windows key+D.
   Kiosk mode is minimized.
2. Open My WinCC Unified on the device.
3. In My WinCC Unified, update the kiosk settings for the kiosk device:
   - Select the option "Disable shortcuts for operating system access".
   - Save your change.

Solution:

You have the following options to block access to the operating system via shortcuts when the device is already in kiosk mode:

Option 1:

1. Terminate kiosk mode.
2. Open My WinCC Unified on the kiosk device.
3. In the kiosk device settings, activate the option "Disable shortcuts for operating system access".
4. Save the change.
5. Restart kiosk mode.

Option 2:

1. Open My WinCC Unified on a device other than the kiosk device.
2. In the kiosk device settings, activate the option "Disable shortcuts for operating system access".
3. Save the change in My WinCC Unified.

11.2 General improvements in Update 3

Stability and performance

The stability and performance have been improved based on the feedback received and other factors.

Desktop link to start the kiosk mode

Starting the kiosk mode has been simplified. After installing SIMATIC WinCC Unified Station Configurator, the "Launch Kiosk Mode" link is now available on the desktop:



If the requirements for starting kiosk mode are met, double-clicking on the link starts Runtime in kiosk mode.

Alternatively, you can still start the kiosk mode via the "SIMATIC WinCC Unified Station Configurator" Windows tray.

Stronger PIN for exiting Runtime in kiosk mode

If a strong PIN was configured in the kiosk settings in My WinCC Unified, the PIN for exiting Runtime must now contain 12 to 16 characters, including numbers, special characters as well as upper and lower case letters.

Script function for starting/exiting kiosk mode

Calling the `HMIRuntime.UI.Kiosk.LeaveFullScreen()` script function in Runtime terminates kiosk mode without simultaneously ending the Runtime display.
The `HMIRuntime.UI.Kiosk.EnterFullScreen()` script function allows the kiosk mode to be started from Runtime.

LeaveFullScreen()

Ends kiosk mode and switches to window mode. As a result:

- Access to the functions of the operating system is possible.
- Runtime is still displayed in a client.
  The client has the following buttons:
  - Minimize: Minimizes the client window.
  - Maximize: Maximizes the client window.

Note

Call Alt+F4

If Alt+F4 has been configured to exit kiosk mode and users press Alt+F4 while the mouse pointer is in the client, the client is closed.

If users press Alt+F4 while the mouse pointer is outside the client, Windows is locked.

EnterFullScreen()

If the conditions for starting kiosk mode are met, kiosk mode starts. If the client is in window mode, it switches to kiosk mode.

Access to the operating system in kiosk mode

If the "Disable shortcut keys for operating system access" option has been activated in the kiosk settings of the kiosk device in My WinCC Unified, the Windows Ctrl+Alt+Del screen can no longer be opened in kiosk mode.

Note

Blocking access via screen keyboard

Users can access operating system functions via the Settings page on device with screen keyboard.

To prevent this, enable the setting "Prohibit access to control panel and PC settings" in the Windows group policies. You can find more information on the procedure in the Station Configurator help with the keyword "Blocking access to the operating system for kiosk mode".

Incognito mode

Kiosk mode now starts in Incognito mode. As a result, inputs in I/O fields are no longer suggested with autofill. Cookies and the web cache are deleted at the end of the session.

In earlier versions of Station Configurator, the browser settings had to be adjusted manually on the kiosk device and applied by restarting the browser. (Microsoft Edge: Select "Settings > Privacy, search, and services > Delete browsing data > Choose what to clear every time you close the browser": Enable options "Autofill form data (includes forms and cards)" and "Cookies and other site data")

File selection in custom web controls

If you open an Explorer for file selection from a Custom Web Control, the paths configured in My WinCC Unified are now applied correctly for access to the file system.

Error message after restarting a device in kiosk mode

After restarting a device that is in kiosk mode, the following error message no longer appears: "Device incompatible. The start of the client is supported for device version V19.0.0.0 and higher. The current device version is V0.0.0.0"

Fewer trace alarms

Trace alarms have been improved for kiosk devices. The number of warnings for IP6 addresses has been reduced.

Corporate Designer

12

12.1 Improvements in Update 4

This update contains the following improvements and changes:

Corporate Designer

The export of custom styles has been improved.

When a style with a version different from the device version is imported, a version incompatibility warning is displayed.

An entered font size is displayed correctly in the object, even if the size is not included in the drop-down menu.

The custom template for the "Switch" object has been improved.

The custom template for the "I/O field" object has been improved.

12.2 Improvements in Update 3

Corporate Designer

After a change in the "Documents\WinCC Unified Corporate Designer\LocalWorkspace" folder, all new projects are displayed correctly in the Corporate Designer.

Siemens Style Library

The IO field, which is based on the "style.sslrt.iofield.simple" rendering template, is shown grayed out when user rights are insufficient.

12.3 Password for secure transfer of the style

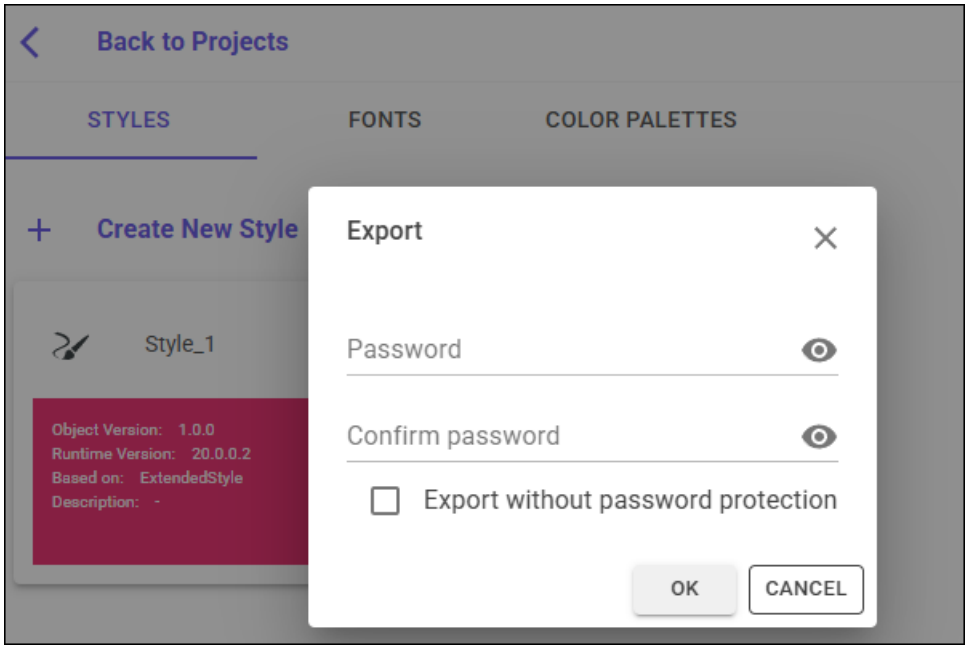
To ensure that your custom style is protected from manipulation during export and import, you can define a password in the Corporate Designer.

The use of this password is optional.

Defining a password for the export

To define a password for the export in the Corporate Designer, follow these steps:

1. Click the three dots in the style card.
2. Click "Export".
   The "Export" dialog opens.



3. Enter a password.
   The password must be at least 8 characters long.
4. Confirm the password.
   You can also export the style without password protection.
5. Select the style file.
   - The file with password protection has the format ".cdx20".
   - The file without password protection has the format ".cd20".
6. Select a local storage location for the style file.

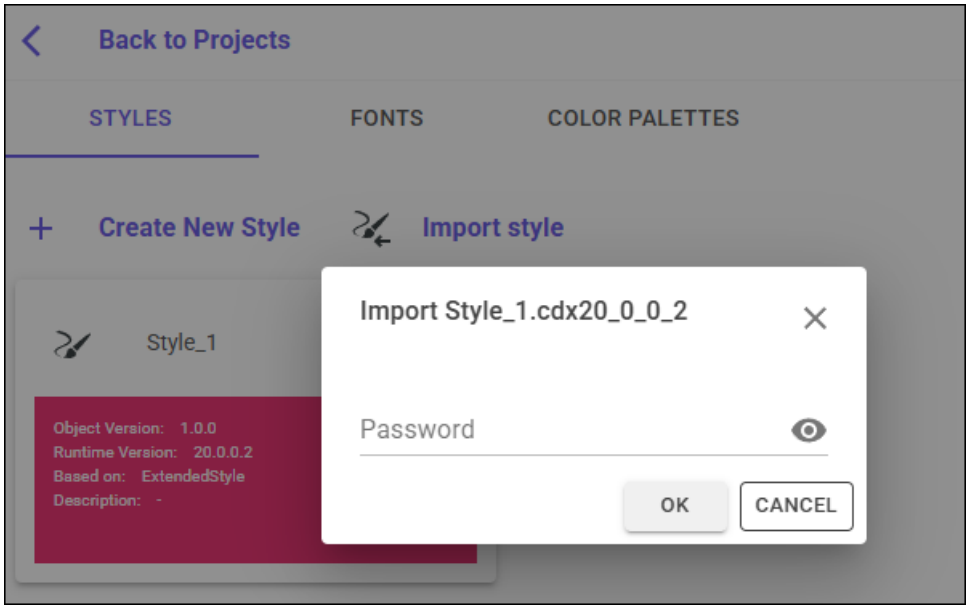
The style file with password protection is exported from the Corporate Designer.

Importing a style file with password protection into the Corporate Designer

To import a style file with password protection into the Corporate Designer, follow these steps:

1. Click the "Import style" icon.
   Your storage location opens.
2. Select a .cdx file that corresponds to the device version in the TIA Portal project.

3. Click "Open".
   The "Export" dialog opens.
4. Enter the password.



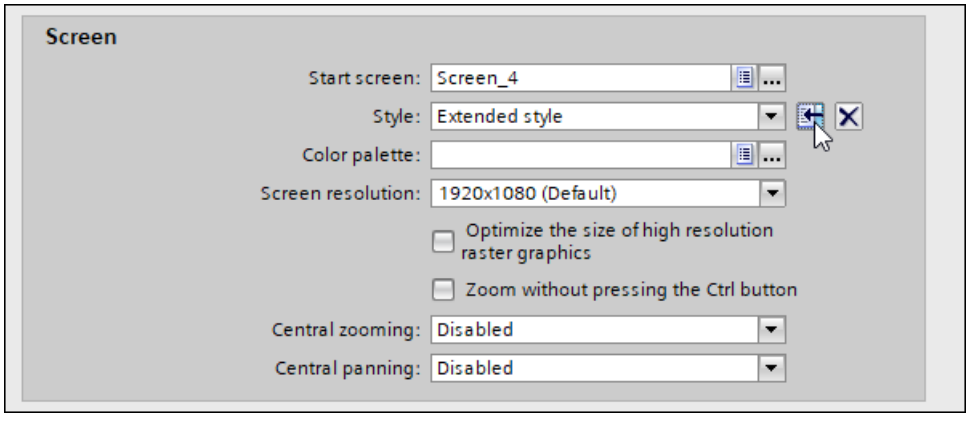
The style file with password protection is imported into the Corporate Designer.

If you select an invalid file or enter an incorrect password, an error message is displayed.

Importing a style file with password protection into the TIA Portal

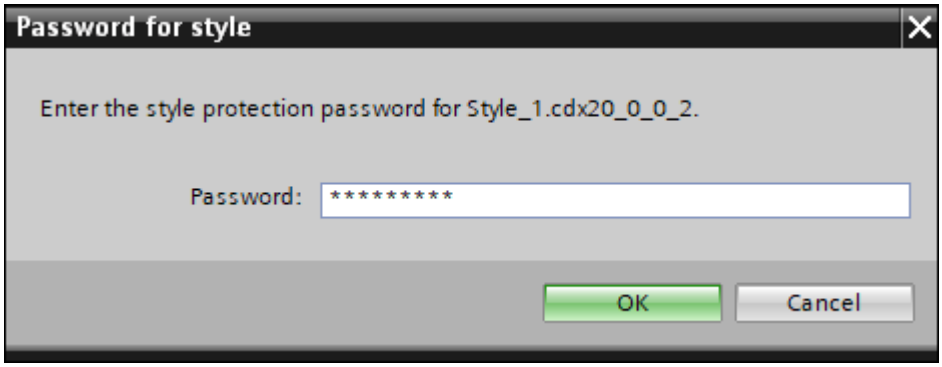
To import the style file with password protection into the TIA Portal, follow these steps:

1. Under "Runtime settings > General > Screen > Style", click the import icon.



   The local storage location opens.
2. Select the style file.

3. Click "Open".
   The "Password for style" dialog opens.



4. Enter the password. Confirm the selection with "OK".

The style is integrated into the TIA Portal project and is available in the "Style" selection list for compatible devices.

WinCC Unified Data Hub

13

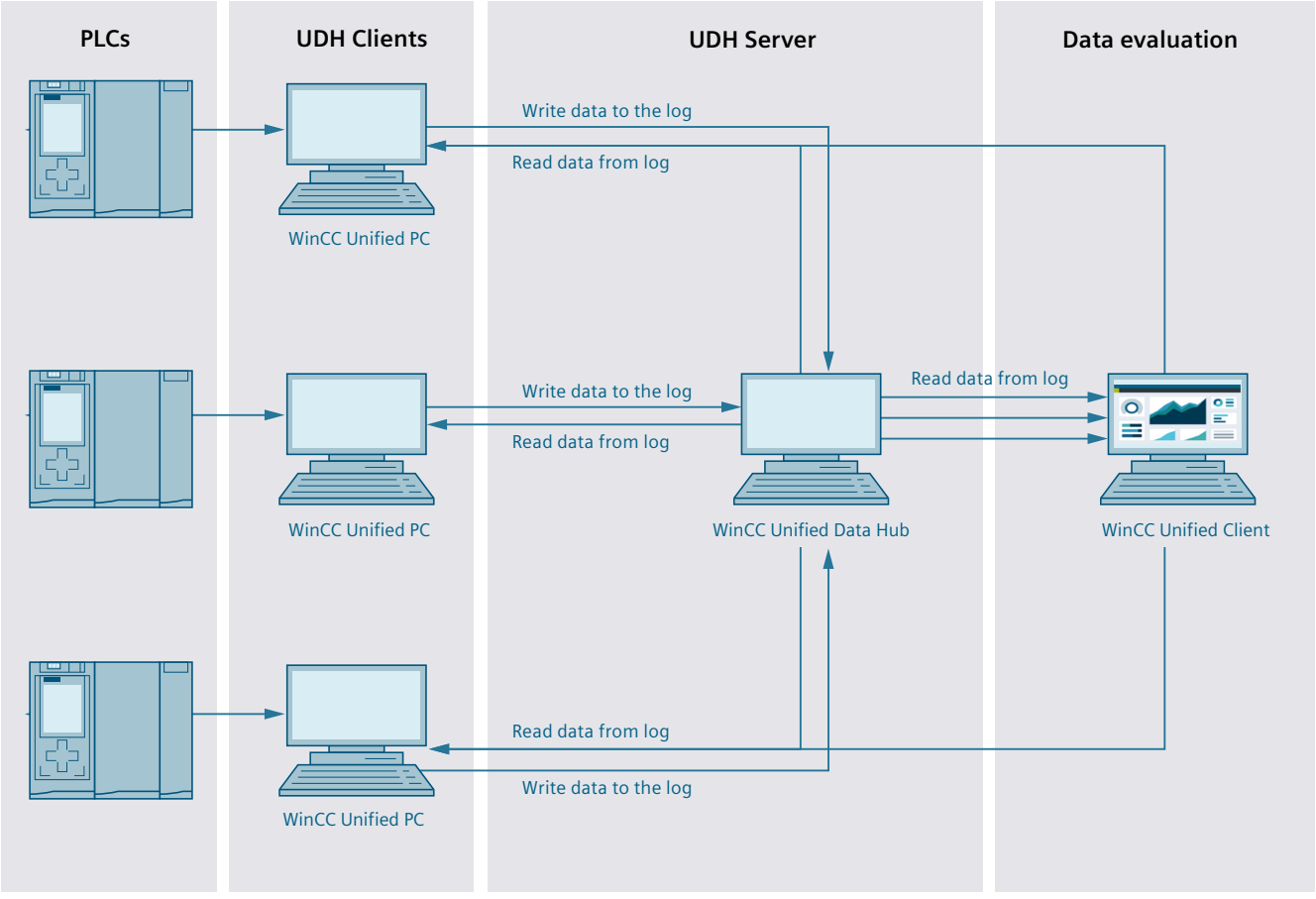
13.1 Introduction to Unified Data Hub

Introduction

SIMATIC WinCC Unified Data Hub is an add-on for WinCC Unified PC.

With WinCC Unified Data Hub you store and process Runtime data in a server-client system. In the process, data from Unified Data Hub Clients is stored in real time on the Unified Data Hub Server for long-term archiving. As a result, all data can be retrieved centrally from one device and can thus be evaluated more easily together.

In this documentation, the term "UDH" is used to refer to "WinCC Unified Data Hub".



Benefits

With WinCC Unified Data Hub, you store and process logging data on a client-server system.

This system offers numerous advantages:

- You store data additionally in a central archive, leaving the local archives untouched.
- You save logging tags, alarms and Audit Trails.
- You retrieve data stored in the central archive on your local HMI device.
- You retrieve data from the central archive even if the Unified Data Hub client is not running.
- A buffer ensures that no data is lost even if the connection to the UDH server is lost.

Functional scope

You create and configure the following functions with WinCC Unified Data Hub:

- You specify which data is to be stored in the central log (Unified Data Hub Server).
- You define which device is to function as the central archive.
- You define which devices should write data to the central log (UDH clients).

13.2 Installing the WinCC Unified Data Hub

13.2.1 Software and hardware requirements

Introduction

With WinCC Unified Data Hub, you store and process Runtime data in a server-client system. You require a license on the configuration device to use this Add-on. Different products are required on the devices used as UDH server and UDH client.

Operating system

WinCC Unified Data Hub supports the same operating systems as WinCC Unified Runtime PC on one PC.

You can find more information in the system manual "WinCC Unified Runtime" under "SIMATIC Unified PC Installation".

User rights

You have administrator rights on the device.

Software requirements

Before you install WinCC Unified Data Hub in the Engineering System and Runtime, you need the following products:

On the UDH server

- WinCC Unified Runtime PC V20 Update 4
- Microsoft SQL Server

On the UDH clients

- WinCC Unified Runtime PC V20 Update 4
- Optional: Microsoft SQL Server, if Microsoft SQL is to be used

On the device for the configuration

- TIA Portal V20 or higher with STEP 7 Professional and WinCC Unified

Hardware requirements

The following points show the recommended hardware requirements.

SSD is recommended for both UDH servers and UDH clients.

UDH server

- Computer: SIMATIC IPC
- Processor: Intel® Core™ i7 / XEON
  At least Intel® Core™ i7 12th generation
- RAM: 128 GB
- 4 separate physical hard disks with the following allocations:
  - Hard disk 1 SSD 500 GB: Operating system and transaction log
  - Hard disk 2 SSD 1TB: Data log
  - Hard disk 3 SSD 1TB: Central alarm log and Audit Trail
  - Hard disk 4 HDD 1TB: Backup

UDH client

- Processor: At least Intel® Core™ i7 12th generation
- Free hard disk space as fallback database for connection losses or UDH server failures. The following hard disk space is reserved by default:
  - Tag Logging: 80 GB
  - Alarm Logging: 80 GB
  - Audit Trail: 10 GB

Bandwidth

- Network bandwidth: 1000 Mbps

Recommendations

- Do not save the local log database and the central log database in the same place.
- Do not store the Runtime project on the hard disk on which the central log database for tags is saved.
- It is not recommended to run a large UDH client on the UDH server PC. If required, a small UDH client can be run on the UDH server PC, specifically on hard disk 3.
  The maximum load for a small UDH client is 12 tag value changes and 2 alarm changes per second.
- The UDH server must be able to trigger alarms that should not be deactivated.
- UDH clients and UDH servers should have the same locale settings.

13.2.2 Licenses

Use Automation License Manager to manage the licenses.

You can find more information in this online help at "Installation > Licensing > Licensing WinCC Unified options > Unified Data Hub".

Required licenses

You need the following licenses to configure and use WinCC Unified Data Hub:

On the UDH server

- WinCC Unified Runtime (RT)
  min.: Unified PC (150) RT
- WinCC Unified Data Hub Server

Note

UDH licenses for UDH servers are version-dependent.

On the UDH clients

- WinCC Unified Runtime (RT)
- WinCC Unified Data Hub Client
  - Unlimited for tags that are logged on the UDH server
  - Unlimited for tags and alarms of a UDH client
- Logging tags
- Data Hub Audit Trail
  For projects that use Audit Trail
- WinCC Unified Database Storage (when using MSSQL)

You are reminded of missing licenses by a pop-up window.

Note

UDH licenses for UDH clients are version-independent.

On the device for the configuration

- WinCC Unified Engineering System (ES)
- WinCC Unified Data Hub (ES)

Note

Collaboration

Licenses for Collaboration are only required if you want to use the full range of Collaboration functions that go beyond UDH. You cannot access log data on the UDH server from UDH clients without a Collaboration license.

13.2.3 Certificates

13.2.3.1 Creating certificates

Introduction

The relevant certificates must be provided in advance. All certificates are issued by a common Certification Authority (CA) to simplify the trust relationship between the communication partners.

The root certificate of the CA is classified as trustworthy on each device for each application. When accessing WinCC Unified Runtime via websites, the root certificate must be configured as trustworthy once in the web browser.

You need a "Runtime Collaboration certificate" for each collaboration device in addition to the root certificate.

You create and manage the certificates with the WinCC Unified Certificate Manager.

Creating a root certificate

1. Select a WinCC Unified PC device in your network that is to serve as the certification authority. The root certificate and the associated key are only available on this device. The configuration of additional application certificates for other devices is only possible on this device.
2. Open WinCC Unified Certificate Manager on this device.
3. Create a new root certificate. Double-click the "Create new certification authority" button.

4. Enter the properties of the root certificate in the "New certification authority" dialog. The fields are freely editable.
   Mandatory fields:
   - "Certification authority"
   - "Password" for the private key

   If necessary, select a different key length and runtime for the certificate.
5. Click "Create".

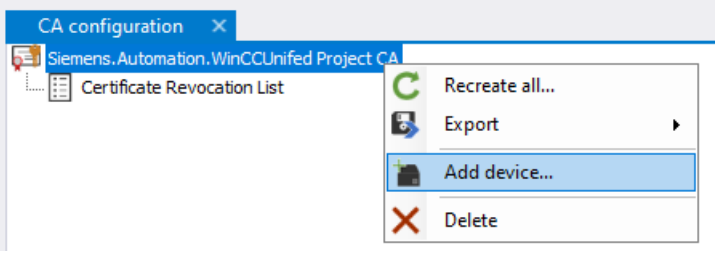
The root certificate and its key are stored on the device and used to generate the device certificates.

Note

If the "WinCC Certificate Manager" is restarted on this device, the root certificate and the device certificates generated with it are loaded automatically.

Adding devices

1. Right-click the root certificate and select "Add device ...".



2. Enter the name and/or IP address of the device in the "New device" dialog box.
   The specification of the IP address is sufficient for Unified Comfort Panel.
   For devices with dynamic IP addresses, enter only the host name.

   Note

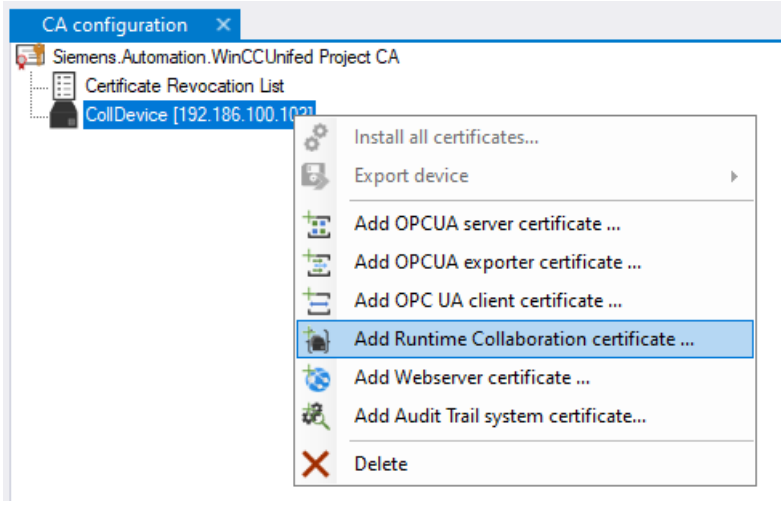
   Permitted names

   Either the host name or the "Fully qualified domain name" can be used as the name. The name is inserted in the certificates created for the device and used for validation. To avoid validation errors when accessing the web pages, the "Fully qualified domain name" must be used within a domain.

   Using the name "localhost" is not permitted and is automatically replaced with the name of the local device by the Certificate Manager.
3. Repeat steps 1 and 2 until all devices have been added.

Adding a "Runtime Collaboration certificate"

1. Right-click on a device and select "Add Runtime Collaboration certificate ..."



2. Enter the properties of the certificate in the dialog.
   If necessary, select a different key length and runtime for the certificate.
3. Create a "Runtime Collaboration certificate" for each collaboration device.
4. If necessary, create additional certificates, e.g. web server certificates.
   You can find additional information in the "WinCC Unified Certificate Manager" operating manual.

Result

- You have created the root certificate.
- You have added all devices.
- You have added a "Runtime Collaboration Certificate" for all devices.
- You have created additional certificates as required.

13.2.3.2 Distributing and installing certificates

Introduction

To distribute the configured certificates to the corresponding devices, the certificates must be exported to a secure storage file. This file must be transferred manually to the respective device and imported there.

Trust communication partners

For successful communication, the device must trust the root certificates of its communication partners and vice versa.

Trust relationship between devices

Devices whose certificate configuration comes from the same certificate authority automatically trust each other after the certificate configuration is installed.

Trust relationship with external communication partners

To establish the trust relationship with an external communication partner, follow these steps:

1. On the certificate authority device:
   Export the root certificate and CRL file to an external data storage medium.
2. On the external communication partners:
   - Connect the external communication partner to the external data storage medium.
   - Copy the files and trust them. To do this, proceed as described in the user help of the device.
   - Import the root certificate of the external communication partner and its CRL file to the external data storage medium.
3. Connect the external data storage medium to the collaboration device.
4. Import the root certificate and the CRL file of the external communication partner into the device and trust it:
   - Unified PC: Use SIMATIC Runtime Manager.

During the next connection attempt, the communication partners mutually accept their application certificates.

Exporting the certificate configuration

After you have completed the certificate configuration of the devices, export the certificate configuration.

Note

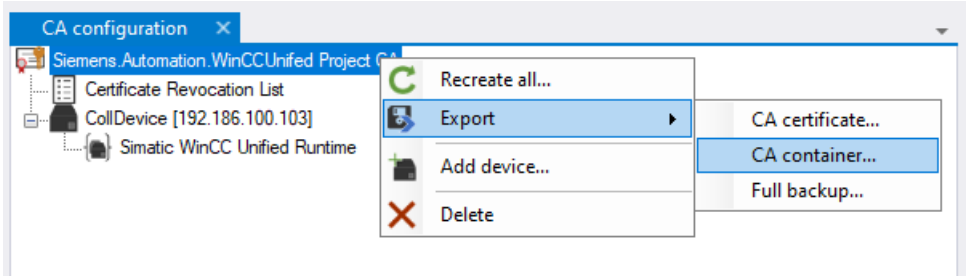
Distribution of root certificate and CRL file

Root certificate and CRL file are part of the certificate configuration of a device. They are exported or imported with the certificate configuration, installed and classified as trusted.

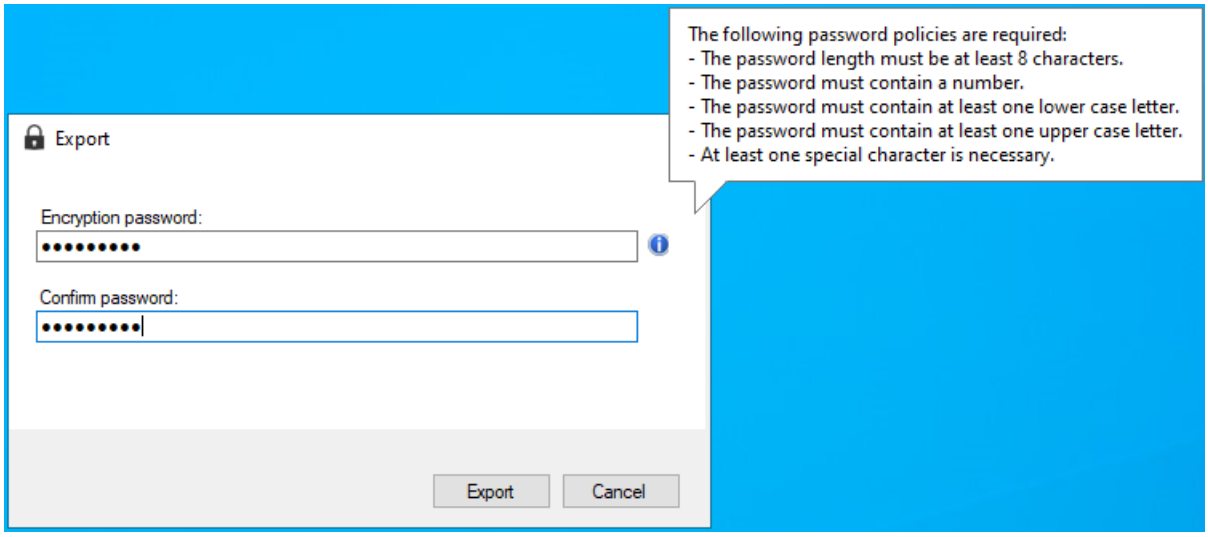
On Unified PCs, you can also export the root certificate and the CRL file via the SIMATIC Runtime Manager.

Exporting all certificates for Unified PC

1. Right-click the root certificate and select "Export..." > "CA container" in the menu.



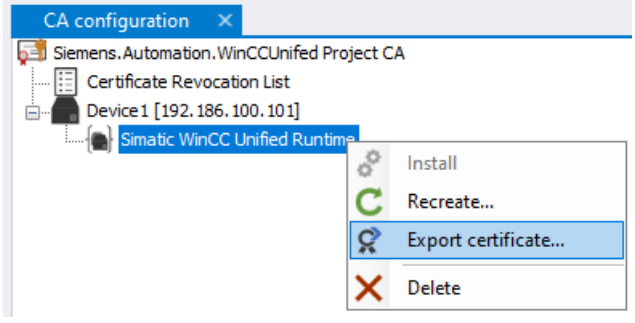
2. Assign a password in the "Export" dialog.



3. Click on "Export" and select the storage location and file name.
   The data is stored encrypted with the specified password.

Exporting the certificate for a device

1. Right-click on the certificate and select "Export certificate" in the menu.



2. Select the format for the exported certificate.
3. Select the storage location.

Making certificates available on Unified devices

To make the certificates of a Unified HMI device available on the Unified PC, follow these steps:

1. Transfer the CA container or the certificates to the Unified PC.
2. Open the Certificate Manager.
3. Open the certificate configuration.



To install an individual certificate of the device:

1. Under the local machine node, right-click the certificate.
2. Select "Install".

Result

You have distributed and installed the required certificates on all collaboration devices.

The Runtime Collaboration certificate only becomes effective after a restart of the WinCC Unified Runtime.

13.2.4 Starting installation

Procedure

Note

Updating an existing installation

If you update an existing installation to a new version, make sure that you always update the UDH server first. Otherwise, the UDH server will not be able to fully process the data generated by the updated client and will have limited functionality.

1. Download the download package for SIMATIC WinCC Unified Data Hub from the Siemens Internet portal to the device and unzip it.
2. Copy the setup files to the UDH server.
3. Double-click the `SIMATIC_WinCC_Unified_Data_Hub_Vxx_xx.exe` file.
4. Follow the installation instructions.
5. Restart the PC.

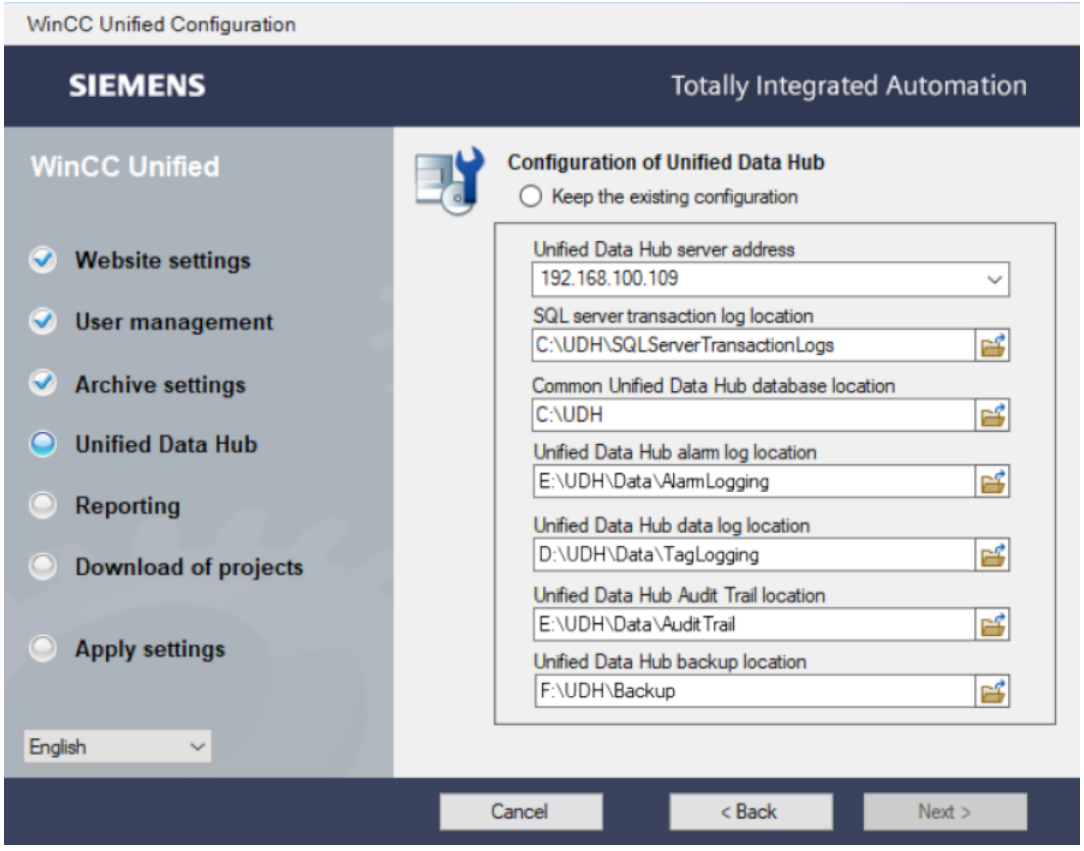
Configuring the UDH server

WinCC Unified Configuration is started automatically during the UDH setup. The UDH server configuration is performed beforehand during the UDH setup.

After the automatic configuration, only the server address and backup storage location can be changed.

To view and modify the configuration, follow these steps:

1. Open WinCC Unified Configuration.
2. If required, modify the configuration of the UDH server:



- Unified Data Hub server address
  TCP/IP address of the UDH server PC
- SQL server transaction log location
  Path of the database transaction log, which should be configured on a dedicated physical hard disk.
- Common Unified Data Hub database location
  Path of the UDH database, can be configured on any non-dedicated hard disk.
- Unified Data Hub alarm log location
  Path of the alarm log; alarm and audit logs should be configured on the same dedicated physical hard disk. SSD is recommended.
- Unified Data Hub data log location
  The storage location of the data log should be configured on a separate physical hard disk. SSD is recommended.
- Unified Data Hub Audit Trail location
  Path of the Audit Trail storage, alarm and audit logs should be configured on the same dedicated hard disk. SSD is recommended.

– Unified Data Hub backup location
  The storage location should be configured on a separate physical hard disk.
  The size should be four times the hard disk capacity of the alarm/audit and data log.

The configuration routine runs even if you do not make any changes. The successful configuration of UDH is displayed in the last step.

If you have made changes, it is recommended that you log out and log back in.

Note

The start times of the central segments for the various logs (alarms, tags, Audit Trails) should be different, as new segments are created on this basis. This prevents all segments from changing at the same time.

Note

Changing the IP address on the server

If the IP address on the UDH server is changed, the UDH server must be reconfigured with WinCC Unified Configuration and the runtime on the UDH clients should be restarted. Otherwise, data synchronization will fail.

13.2.5 Adapting the IP address of the UDH server

The Unified Configuration Tool does not recognize a change to the IP address of the UDH server. In this case, you need to run WinCC Unified Configuration again.

Preferably use fixed IP addresses.

Procedure

1. Configure the desired IP address on the computer to be used as the UDH server.
2. Change the IP address of the UDH server in the TIA Portal project under "Runtime settings > Collaboration".
3. Use the command "Software > Rebuild all" to compile the project that is trying to establish a connection to UDH and the UDH project.
4. Save the project and perform a full download to all affected devices.

   Note

   Do not yet start the UDH project via "Full download".

5. Start the Unified Configuration Tool on the UDH server.
6. Go to the Unified Data Hub section.

7. Click "Next" and run the "Unified Configuration Tool" until it is completed.
   "DONE" is expected as the configuration result.
   The UDH Configuration tool reports contain a warning that the PC must be restarted due to a change of IP address.
8. Start the project now.

13.3 Configuring WinCC Unified Data Hub

13.3.1 Requirements

Introduction

You archive Runtime data with Unified Data Hub. You require a license to configure this option in the TIA Portal and then use it in Runtime. You can find information about the licenses in the Software and hardware requirements (Page 130) section.

Browser

WinCC Unified Data Hub supports the same browsers as WinCC Unified Runtime PC.

For more information, refer to section "Internet browsers WinCC Unified PC" in the "SIMATIC Unified PC readme".

User knowledge

You have the following knowledge:

- General knowledge about TIA Portal

Requirements in TIA Portal

Your TIA Portal project must meet the following requirements:

- The project is open.
- Multiple PLCs and HMI devices (Unified PC) are created on the "Devices" tab.
- The logs to be backed up have been created.

13.3.2 Configuring the device as a Unified Data Hub server

Introduction

The UDH server is used as the receiver of the data of the individual UDH clients and stores this data in the central log on the server.

To store data, you need to set and configure a device as a UDH server.

Requirements

- A Unified PC with device version V20 or higher is configured.
- Microsoft SQL is activated.

Procedure

To configure an HMI device as a Unified Data Hub Server, proceed as follows:

1. In the project tree, click on the HMI device of the PC system that is to be used as the UDH server.
2. Double-click on "Runtime settings" in the project tree.
   The editor for "Runtime settings" opens.
3. Click "Services".
4. Enable "Operate as Unified Data Hub" under "Central archiving system".
5. Click "Storage systems".
6. Under "Database type", select the "Microsoft SQL" type.

   Note

   In order not to impair performance, do not configure any client functionality on the server.

7. Click "Collaboration".
8. Select "Enable collaboration" under "General settings".
9. Assign a system ID for the HMI device under "Identification".
10. Specify the Collaboration name.
11. Enter the IP address or the hostname of the device.

Note

Performance

For optimized performance, do not configure a UDH client on the UDH server PC.

Result

You have configured a Unified PC as a UDH server.

All logging tags, alarms and Audit Trails of a UDH client created in Runtime are automatically stored on the UDH server.

13.3.3 Configuring the device as a Unified Data Hub client

Introduction

The UDH clients receive data from the PLCs. This data is archived locally and additionally sent to the UDH server for long-term logging.

To store data on the UDH server, you need to set and configure one or more devices as UDH client(s).

Requirements

- A Unified PC with device version V20 or higher is configured.

Note

A UDH client can only be installed on a WinCC Unified PC that has been newly integrated into the system. Installation on a running device is not supported.

Procedure

1. Open the Runtime settings of the device that is to be used as the UDH client.
2. Switch to the "Services" area.
3. Disable the option "Operate as Unified Data Hub".
4. Switch to the "Collaboration" area.
5. Select "Enable collaboration" under "General settings".
6. Under "Identification", create the system ID, collaboration name and IP address or host name of the UDH client.
7. Under "Connect actively to", select the device that you have configured as a UDH server.
8. Switch to the "Storage system" area.
9. Select "Microsoft SQL" or "SQLite" as the database type.
10. Under "Central archiving with Unified Data Hub (UDH)", select the data you want to store.
11. Enter the system ID of the UDH server in each case.
12. Click "Good Manufacturing Practice".
13. Enable "Configuration conforms to GMP".
14. Repeat steps 1 to 13 for additional PC systems to be used as clients.

Result

You have configured a Unified PC as a UDH client.

You define the data logs to be backed up separately; see "Defining logs to be transferred (Page 145)".

13.3.4 Defining logs to be transferred

Introduction

You can save the following types of logs:

- Data log
- Alarm log
- Audit Trails

Segmented logs are used for archiving on the UDH server to optimally store the data.

Each log consists of a configurable number of segments. The segments are filled one after the other.

Requirements

- A Unified PC is configured as a UDH client.

Procedure

To activate logging on the UDH server for an individual log, follow these steps:

1. In the project tree, open the "Logs" editor of the UDH client.
2. Select the log that is to be backed up on the UDH server.
3. In the Inspector window, select "Properties > Central".
4. Select the "Activate central logging" check box in the "General" section.
5. Specify the time period and the maximum log size.
6. Repeat steps 1-5 for additional logs and clients.

Result

You have specified which logs are logged on the UDH server.

Resetting logs

You can reset the logs through a complete download in the TIA Portal or through a Runtime start with reset on the UDH client in the Runtime Manager. In this case, the local databases on the UDH client and the databases for the client on the UDH server are reset.

Note on configuring the segments

When new data logs are created, segmenting on the UDH server is configured automatically. The default values should not be changed.

Automatic configuration takes place in accordance with the following recommendations:

- The recommended time period of an individual segment amounts to ≥ 1 week. The time period is set automatically to 1 week.
- The start time of a new segment should lie outside the main production time. The start time of a segment is set automatically to 23:00.
- The start time of a new segment should not intersect within the client. The start time is shifted automatically by one minute for each data log that is added.

13.3.5 Connection diagnostics

Introduction

To run diagnostics for the data flow, use the "Diagnostics Viewer UI".

Diagnostics Viewer UI is started with `RTILdiagnosticsViewer.exe`. The tool can be started on any system and displays the available diagnostics data on this system. To see additional diagnostics data from other systems, enable Trace forwarding and receipt.

Activating diagnostics

1. Start "`RTILtraceTool -mode forwarder -tcp -subsystem "Diagnostics"`" on the system on which the additional diagnostics data is located.
2. Start "`RTILtraceTool -mode receiver -tcp -host <hostnames>`" on the system on which Diagnostics Viewer UI is running.
   `<hostnames>` stand for the IP addresses (or network-resolvable names) of the target computers. All computers must be part of the same network or have suitable routing between them. Multiple IP addresses are separated by commas.
   You can find more information by calling `RTILtraceTool -help` or `RTILtraceTool -mode receiver`.

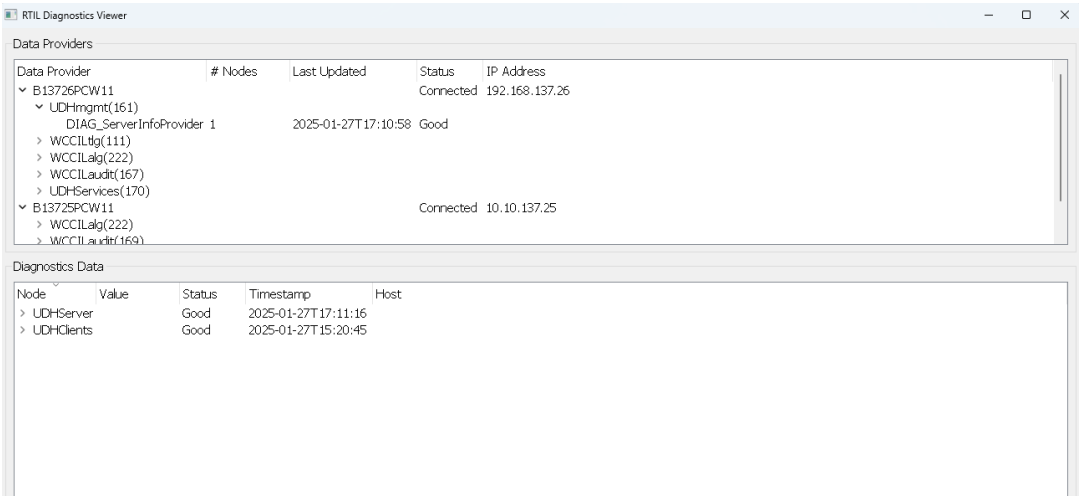
Note

For diagnostics, add a rule for inbound connections in the firewall settings that allows a connection over Port 4725.

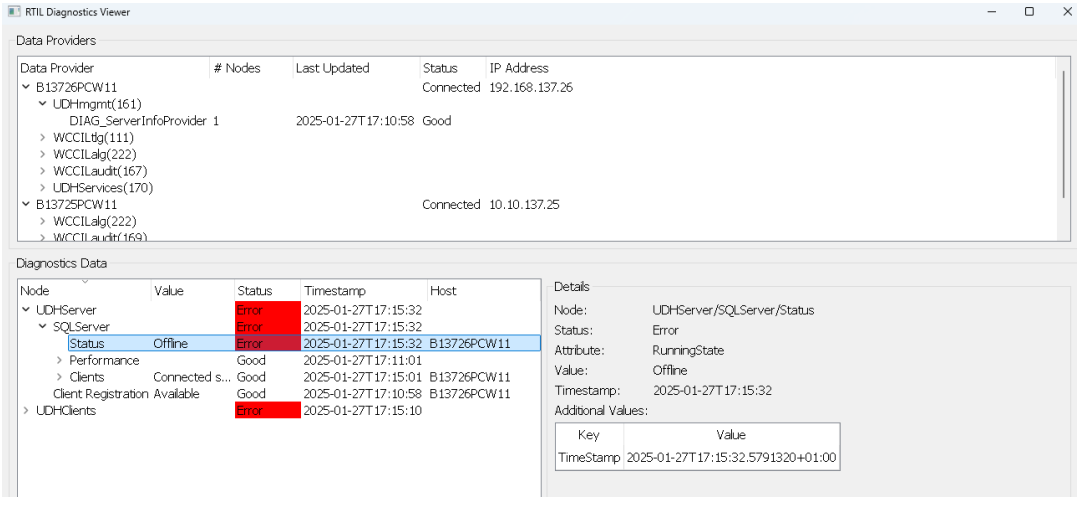
Diagnostics Viewer

Diagnostics Viewer shows the list of data providers, i.e. the systems of the sender, in the upper half. The first node shows the device name, the connection status and the IP address of the device.

1. Click on the device name to display the list of managers that send diagnostics data to the Diagnostics Viewer. The number of nodes, the overall status and the time stamp of the last update are displayed for each manager.



The lower half shows the diagnostics data. Each line represents a node in the tree view. In the structure view, the first node is "UDHServer".

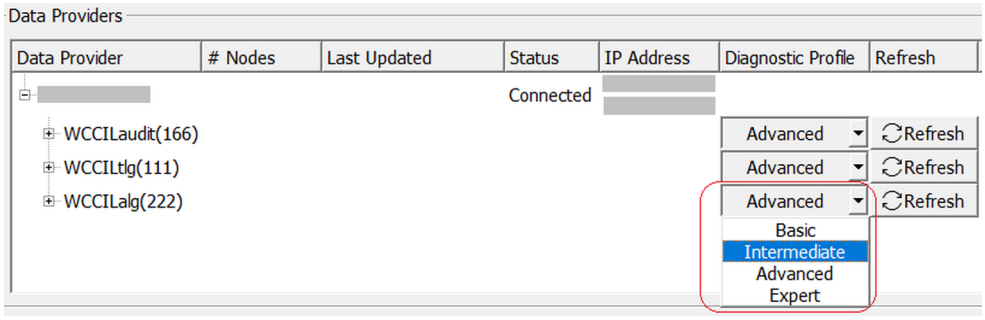


2. Click on a node in the tree view to display the status.
   Each node has a value and a status. The status can be "Good", "Error" (red), "Partially Good" or "Degraded" (yellow). Additional attributes of a node are displayed on the right side.
   There are two types of diagnostics data: server-side and client-side. Server-side diagnostics data shows the attributes of the UDH server, client-side data applies to the respective UDH client.

Standard and extended diagnostics data

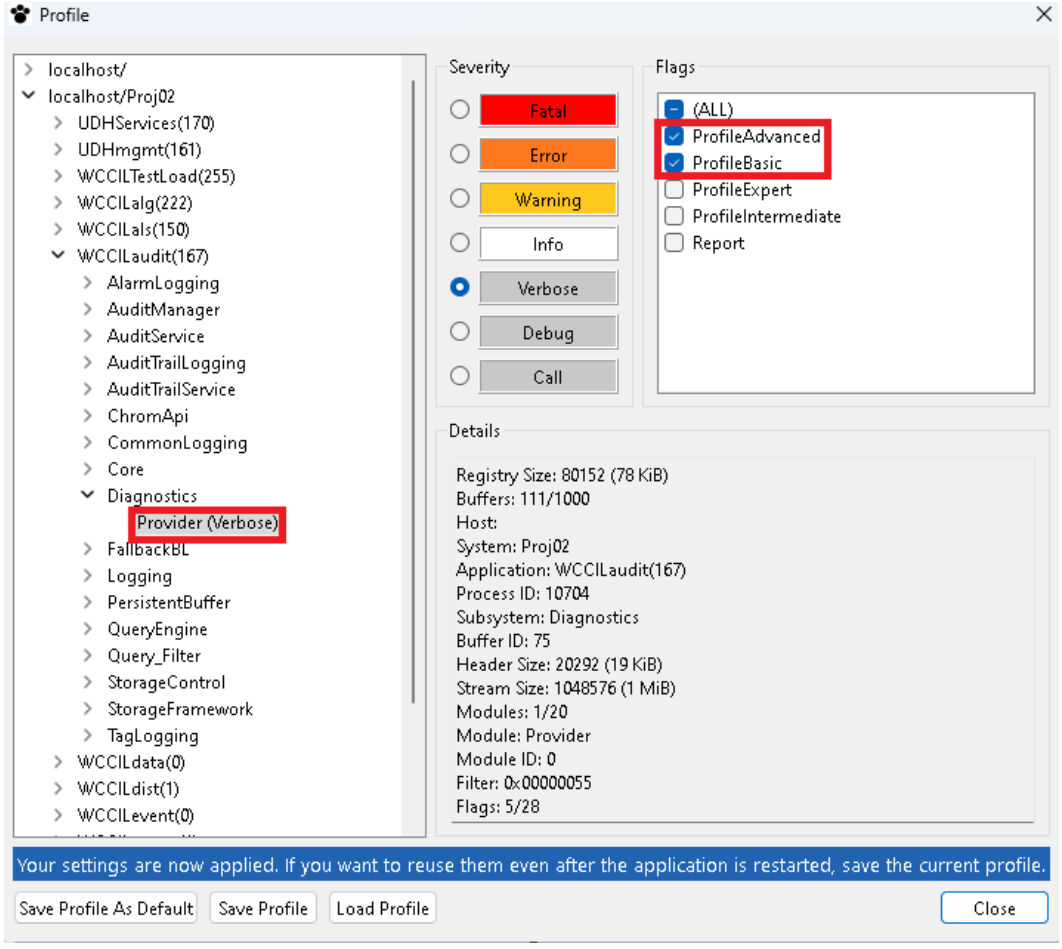
Each node can be displayed as "Basic" or "Advanced". By default, only the "Basic" diagnostic nodes with the essential attributes of the machine are displayed.

1. To show advanced diagnostic data nodes, enable the corresponding diagnostics profile "Advanced" for the corresponding manager:



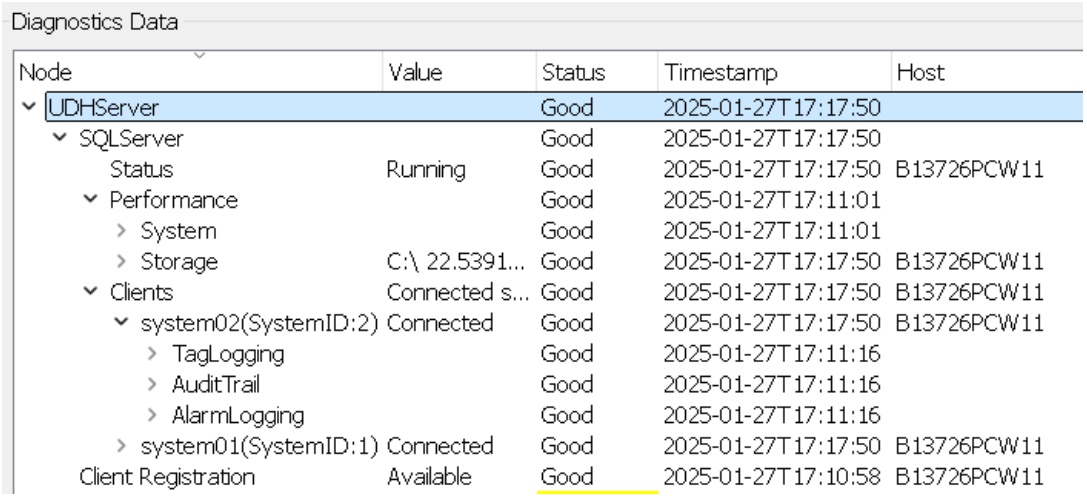
Another way to activate these Trace flags is to use Trace Viewer (`RTILtraceViewer.exe`).

1. Click the icon "Open trace profile dialog" .
2. Under "Diagnostics > Provider", enable the Trace flags.



Server-side diagnostics data

Diagnostics data for the UDH server is displayed under "UDH server".



UDHServer/SQLServer/Status

- Running:
  `SQL Server Services` runs on the same computer on which `UDHmgmt.exe` runs.
- Offline:
  `SQL Server Services` must be started/restarted. While the SQL Server is offline, no data is written to the UDH database, only local logging and buffering (fallback logging) takes place. After restarting the SQL Server, data synchronization from the fallback database to the UDH database begins.

UDHServer/SQLServer/Clients

Returns the list of active UDH clients. This number indicates how many connections are active and sending logging data to the UDH server.

Additional attribute: Registered UDH clients. Displays the total number of registered UDH clients that were connected to the UDH server, even if they are not currently connected.

UDHServer/SQLServer/Clients/<SystemName>

`<SystemName>`: Consists of the configured "Collaboration Name" in the TIA Portal, followed by "SystemID", e.g. `MySystem(SystemID:1)`). These values are set in the TIA Portal under "Runtime settings > Collaboration".

Each system can have several managers with open connections to the UDH server.

Examples:

- Tag Logging: WCCILtlg
- Alarm Logging: WCCILalg
- Audit Trail: WCCILaudit

Status:

- Connected
  All managers are connected.
- Partial connected
  Only some of the managers are connected.
- Not connected
  None of the managers are connected.

UDHServer/SQLServer/Clients/<SystemName>/<Manager>/Connection

- Connected
  The manager (e.g. TagLogging) is connected to the UDH server. This means that logging can take place both in the local database and in the UDH database.
  Additional attributes
  - IP address of the system on which the manager is running
  - Operating time (how long the connection is online)
  - Last connection time
- Not connected
  The manager is not connected to the UDH server. This may mean that the <Manager> must be started or restarted on the system <`System name`>. If a manager is not connected to the UDH server, the "IP address" in the additional attributes is set to zero and the operating time is 0 seconds.

UDHServer/SQLServer/Clients/<SystemName>/<Manager>/Registration

During the registration process, the UDH client establishes a connection to the UDH server for the first time and authenticates itself. The logging process to the UDH server can only be started after successful registration.

- Connect
  The <Manager> is started and registers on the UDH server.
- Successful
  The registration was successful and the logging/synchronization in the UDH database was started.
- Failed
  The registration was not successful. New files cannot be created in the UDH database. This can be caused by an SQL Server error, e.g. if there is already an inconsistent database with the same name.
  The manager and/or the SQL Server must be restarted.

UDHServer/SQLServer/Clients/<SystemName>/<Manager>/Storage

- Size
  Size of the UDH database of the current manager in MB.

UDHServer/SQLServer/Performance/Storage

- Drive
  Returns the most used hard disk and information about how much of it is currently in use.

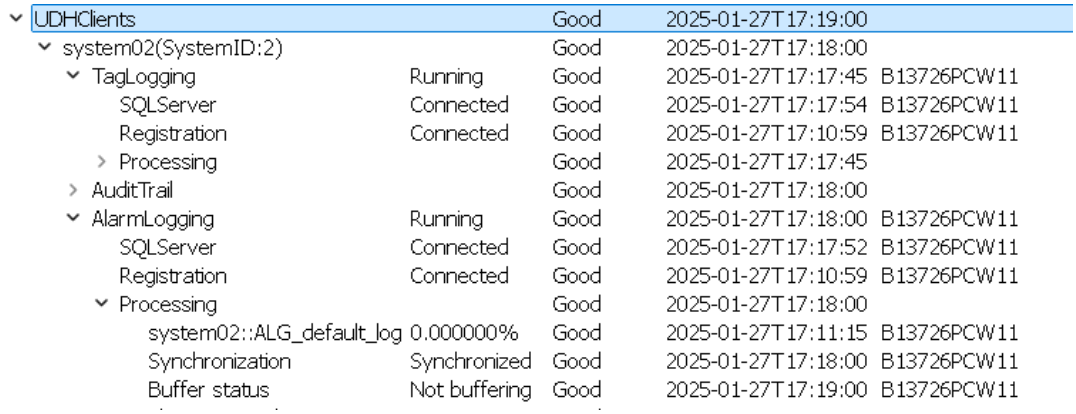
UDHServer/SQLServer/Performance/Storage/<CurrentDisk>

Returns the total capacity of the current data storage medium and how much of it is currently in use.

UDHServer/SQLServer/Performance/System/SQL Server Memory

Returns information about the memory of the SQL Server services.

Client-side diagnostics data



UDHServer/Client registration

- Available
  The UDH server can process incoming connection requests from UDH clients.
- Not available
  The UDH server (`UDHmgmt.exe`) must be restarted. As long as this is not available, no new UDH clients can connect to the UDH server. However, managers with existing connections can continue to write data to the UDH database as this is done via ODBC connections and they are therefore not affected.

UDHClients/<SystemName>/<Manager>: (e.g. UDHClients/System1/TagLogging)

- Running
  The <Manager> runs on <SystemName>.
- Stopped
  The <Manager> is stopped at <System name> and no local or UDH-related logging takes place with this manager.

UDHClients/<SystemName>/<Manager>/SQLServer

- Connected
  The manager is connected to the SQL Server, the health state of the manager is good (e.g. `Healthstate_Good`, `HealthState_Synchronizing`).
  Logging can take place.
- Connected with error
  The health state of the manager is not good, but it also not interrupted (e.g. `HealthState_StorageSpaceExceeded`).
  This indicates that there is a connection to the SQL Server, but there are errors. For example, not enough space on the hard disk.
- Offline
  The manager has no connection to the SQL Server, the HealthState is disconnected (`HealthState_Disconnected`).
  No logging takes place. SQL Server and/or manager must be started/restarted.

UDHClients/<SystemName>/<Manager>/Registration

- Like "UDHServer/SQLServer/Clients/<SystemName>/<Manager>/Registration" but shown by the client page.

UDHClients/<SystemName>/<Manager>/Processing/<LogName>

- Fill level of the WriteQueue in %.
  If the WriteQueue becomes too full (> 75%), it is displayed in yellow. The SQL Server is too slow or the load is too high and the manager's WriteQueue cannot be reduced.
- Additional attribute:
  Bulk mode: Disabled by default, automatically switched on at high load.

UDHClients/<SystemName>/<Manager>/Processing/Buffer status

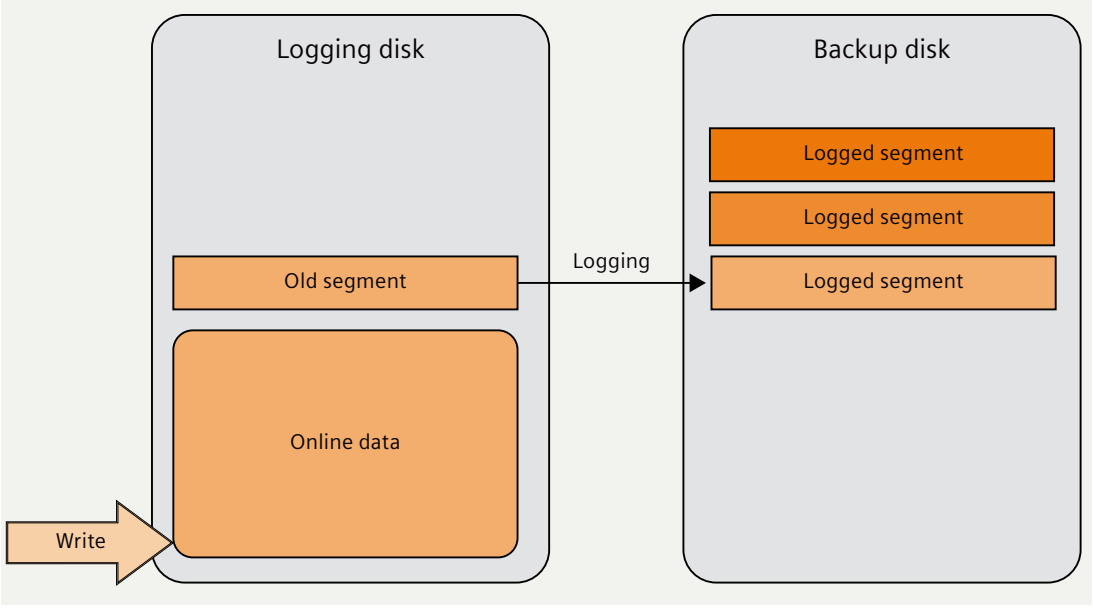
- Buffering
  The manager cannot write to the UDH database. It writes to the fallback database instead.
- Not-buffering
  The manager can write to the UDH database.
- Additional attribute
  BufferSize, the size of the fallback database in MB.
  The "Buffering" status indicates connection problems with the UDH server. As soon as the connection is re-established, the fallback and UDH databases are synchronized so that the fallback database is not overfilled and no data is lost.

UDHClients/<SystemName>/<Manager>/Processing/Synchronization

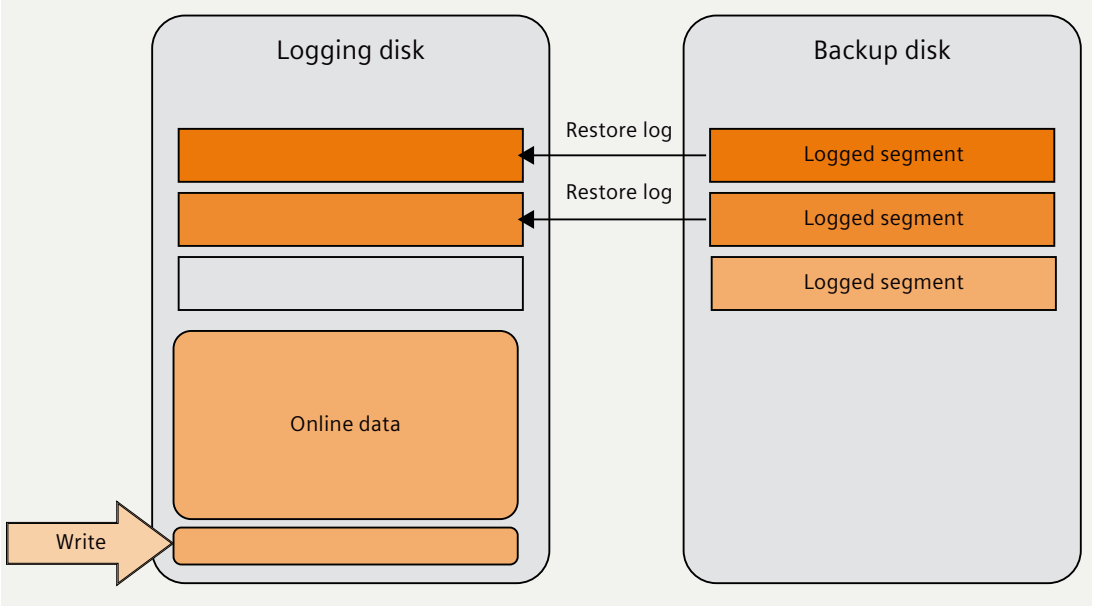
- Synchronized
  The connection to the UDH server is established from the local UDH client, and the same data that is in the local database can be found in the database.
- Synchronizing
  The connection was interrupted but restored. As soon as synchronization is complete, this value automatically changes to "Synchronized". If this is not the case, an error has occurred during synchronization, which is displayed as additional error messages from the manager.
- Out of sync
  The connection to the UDH server is interrupted. There is no logging in the database. The manager writes to the fallback database.

13.4 Central logging and restoring

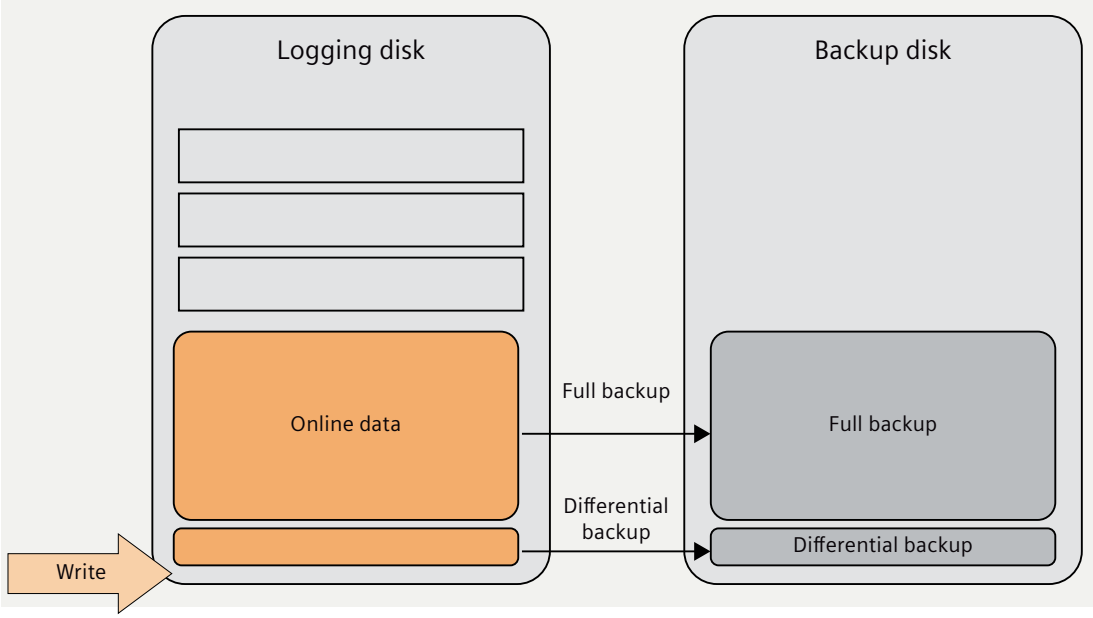
Data is continuously written to a storage medium ("Logging Disk"). This online data can be read. After a configurable time span, data is swapped out to a segment. This swapped-out log segment can no longer be read directly and is swapped out to a further storage medium ("Backup Disk").



Log segments that have been swapped out can be restored with read access on the "Logging Disk". The restoration can be undone (unrestore).



In addition, the online data that has not yet been segmented on the "Backup Disk" is backed up completely and periodic differential backups are created.



If the "Logging Disk" is corrupt, the data from the backup can be restored to a new "Logging Disk".

In this way, data loss is reduced to an unavoidable minimum.

Note

Missing data after the restore

Data may be missing after the restore processes. This is normal behavior during data backup and restore.

The UDH server creates differential backups every hour, which means that, in the event of a failure, the data between the last successful differential backup cycle and the time of the failure cannot be restored.

You cannot read out the data for this period, even if your local backup was active.

Note

Export of archives via system functions

UDH supports the export of archives via the following system functions:

- ExportAuditArchive
- ExportAlarmLog
- ExportTagLog

Further information on how to use it can be found in the respective chapter of the documentation.

See also

Restoring a backup (Page 165)

Restore intervals (Page 168)

13.4.1 Working with GraphQL

13.4.1.1 Introduction to GraphQL

GraphQL API is an easy-to-use, quick-to-integrate Web API with few dependencies and little code. Use GraphQL queries in UDH for specific operations to read and write data in the database.

GraphQL API is provided by the GraphQL Server Manager "UDHServices.exe".

The GraphQL Server Manager is available via IIS at "https://<full device name>/udhlogadmin".

Requirements

- Public Internet connection

What is GraphQL?

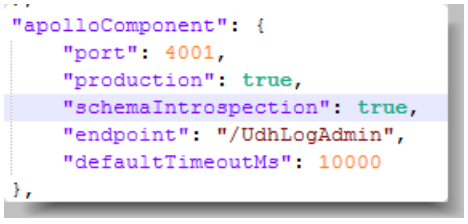
GraphQL is an API concept that defines the following basic properties:

- Transport layer for operations and responses is HTTP and web sockets
- Operations and responses use a JSON-like format
- Operations and responses are described in a standard schema.
- Operations define which response they expect.

Using GraphQL

They use the GraphQL API of any web, mobile, desktop, console and service applications if they have network access via HTTP and web sockets.

1. Log into Apollo Studio:
   Apollo Studio (https://studio.apollographql.com/sandbox/explorer)
   Default for the UDH Services endpoint address: https://<full device name>/UdhLogAdmin
   The endpoint can be configured in `LogAdminConfig.json` if required
   (Default storage location: `WCCIL_CC\config\UDH\LogAdministrator\ Folder`)



Additional documentation

You can find documentation for GraphQL on the Internet:

- SiePortal: SIMATIC HMI WinCC Unified GraphQL (https://support.industry.siemens.com/cs/ww/en/view/109826709)
- GraphQL documentation (https://graphql.org/learn/)
- GraphQL at GitHub (https://docs.github.com/de/graphql/guides/introduction-to-graphql)

13.4.1.2 Creating UDH user roles or user groups

To access the features of GraphQL for UDH, you must manually create two user roles for local user management or two user groups for central user management.

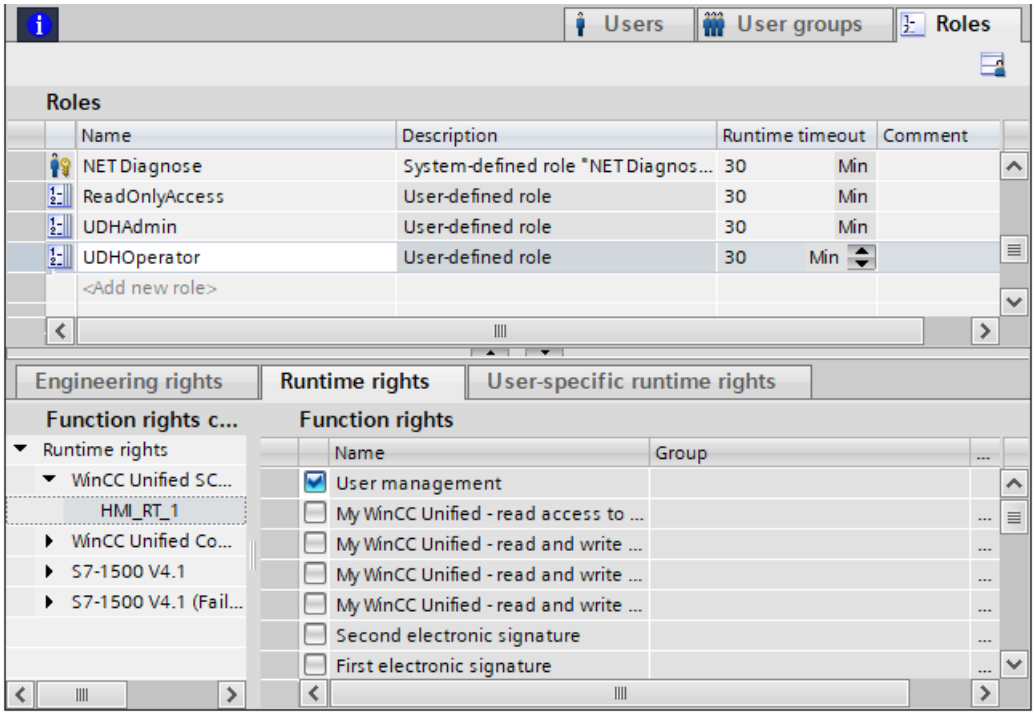
The procedure depends on whether the users are managed locally in the project or whether central user management is configured.

Preferably use local user management.

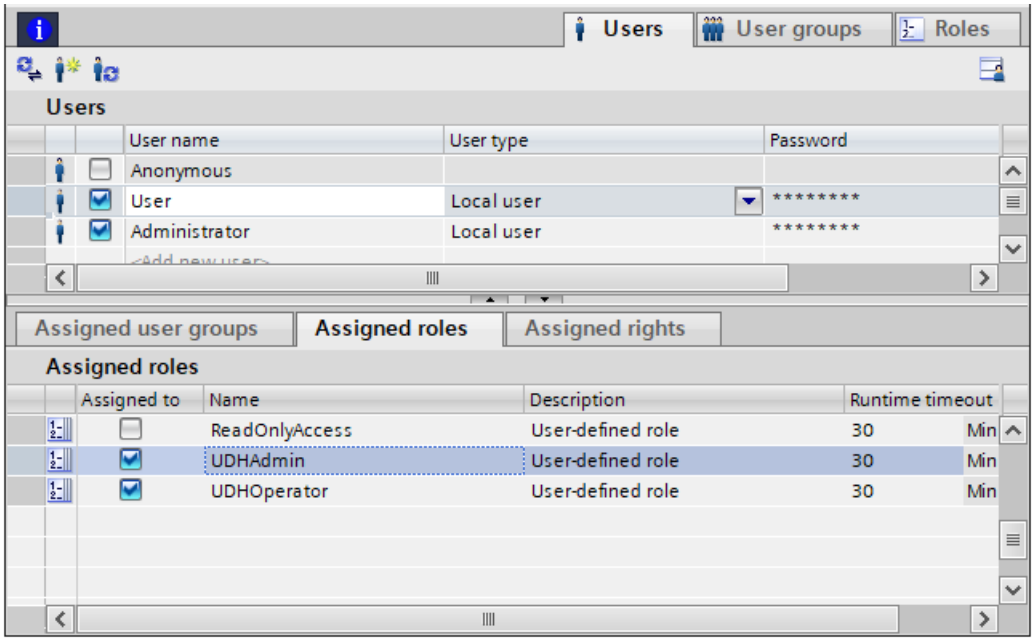
Procedure for local user management

1. In the project tree of the TIA project, select "Security settings > Users and roles".
2. Select the "Roles" tab.

3. Add two new roles:
   - UDHAdmin
   - UDHOperator
4. Select the Runtime of the UDH device under "Runtime rights, Categories of function rights".
5. Assign the "User management" function right to each of the two newly created roles.



6. Assign the newly created roles to the appropriate users under "Users".



7. Load the project completely into the UDH device.
   The newly created roles are displayed in the user management of the UDH server.
   To work with GraphQL, users can log in to Apollo Studio with the newly created authorizations.

Procedure for central user management

Requirement: The UDH server is connected to the central user management server (UMC server).

1. Add two new groups on the UMC server:
   - UDHAdmin
   - UDHOperator
2. Assign the appropriate central users to the newly created user groups.
3. Load the entire project into the UDH device and start the project in Runtime.

The central users with the newly assigned user groups can log into Apollo Studio with the "UDHAdmin" or "UDHOperator" authorization to work with GraphQL.

See also

Working with GraphQL (Page 155)

13.4.1.3 Authorizations in GraphQL

Query Mutation	UDHAdmin	UDHOperator	Each authenticated user	Unauthenticated users
Authentication				
session	✓	✓	✓	-
nonce	✓	✓	✓	✓
identityProviderUrl	✓	✓	✓	✓
login*	✓	✓	✓	✓
loginSWAC*	✓	✓	✓	✓
extendSession	✓	✓	✓	-
logout	✓	✓	✓	-
Core				
QueryDatabases	✓	✓	-	-
Read				
QueryAlarms	✓	✓	-	-
QueryAuditRecords	✓	✓	-	-
QueryTags	✓	✓	-	-
Database operations				
QueryArchivedIntervals	✓	-	-	-
QueryRestoredIntervals	✓	-	-	-
QueryBackupInfo	✓	-	-	-
RestoreInterval	✓	-	-	-
UnrestoreInterval	✓	-	-	-
UnrestoreAllIntervals	✓	-	-	-
RestoreDatabase	✓	-	-	-

* Remove the authorization header before logging in, because if the token has expired, the login request will be rejected before a login attempt can be made.

13.4.1.4 Setting up the GraphQL client

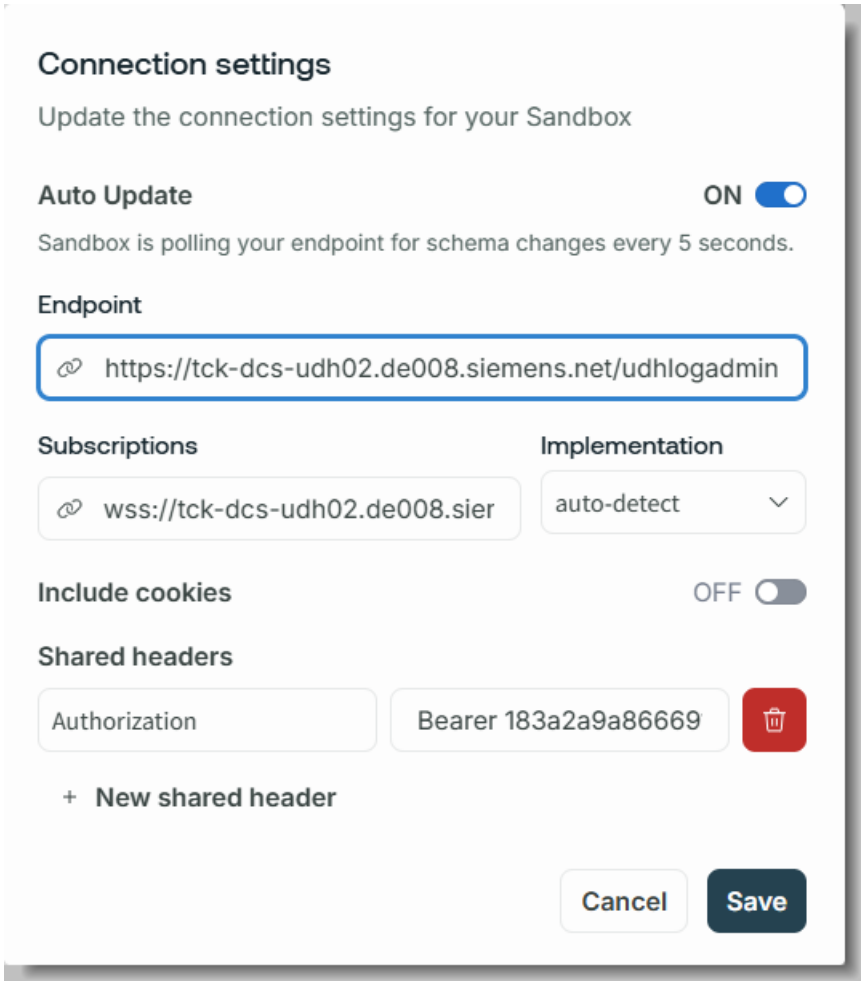
To access the GraphQL server on the UDH server, set up a GraphQL client on any PC.

The certificate authority (CA) is required on the PC to connect to the UDH server.

Procedure

1. Open Apollo Studio in your browser:
   https://studio.apollographql.com/ (https://studio.apollographql.com)
2. Log in.
3. To open the configuration panel of the GraphQL client, click on the gear wheel icon.

4. Configure how the GraphQL client accesses your GraphQL server.



5. Enter the token "Bearer <received token>" under "Shared headers".
   The token can be found in the response to the login operation performed earlier.



After successful setup, a green symbol is displayed in the top left corner.

The GraphQL server provides the GraphQL client with the queries required to work with UDH.

The documentation for the GraphQL API is available.

13.4.1.5 Executing GraphQL operations

In Apollo Studio, you can enter GraphQL operations in the Operations panel. Operations can be entered manually or created semi-automatically using the plus symbols in the documentation view.

You define the parameters of the operation directly in the operation or in the Tags panel at the bottom.

In the Header area, you define additional HTTP header values, e.g. the mandatory authorization token for access to tags and active alarms.

Once the operation, parameters and header have been set up, click on the blue button to run the operation.

The response from the GraphQL server is displayed in the Response panel.

Logging in

To access Runtime data, you need to log in to the GraphQL server.

To do this, use the mutation "`login`".

Note

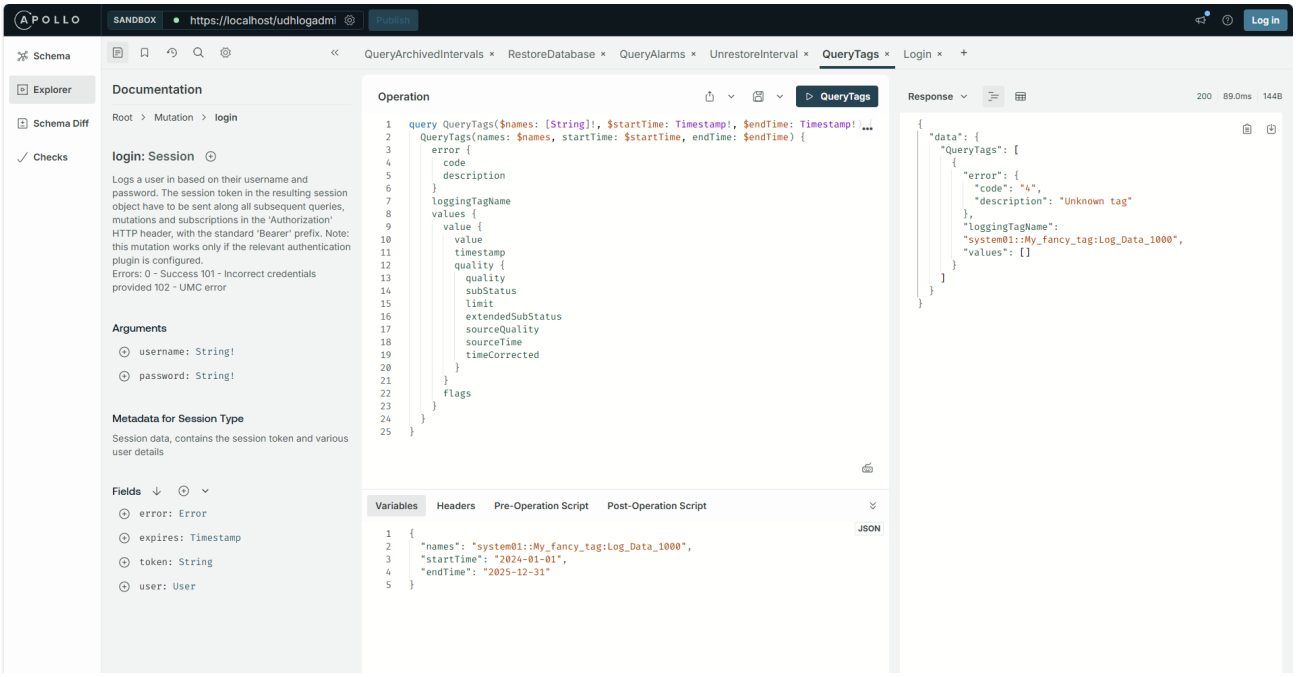
You must use your own UMC-based username/password combination that you use to log into TIA Portal.

The generated token must be specified as the authorization header for all subsequent GraphQL operations. After a certain period of inactivity, your token may expire. In this case, a new registration is required.

GraphQL operations

Query

Query operations read data that corresponds to a specific filter, e.g. the value of a tag or active alarms. The query operations send a one-off HTTPS request to the GraphQL server.



If a domain user is used, the user name for login must be specified as follows: "domain\ \username".

Note

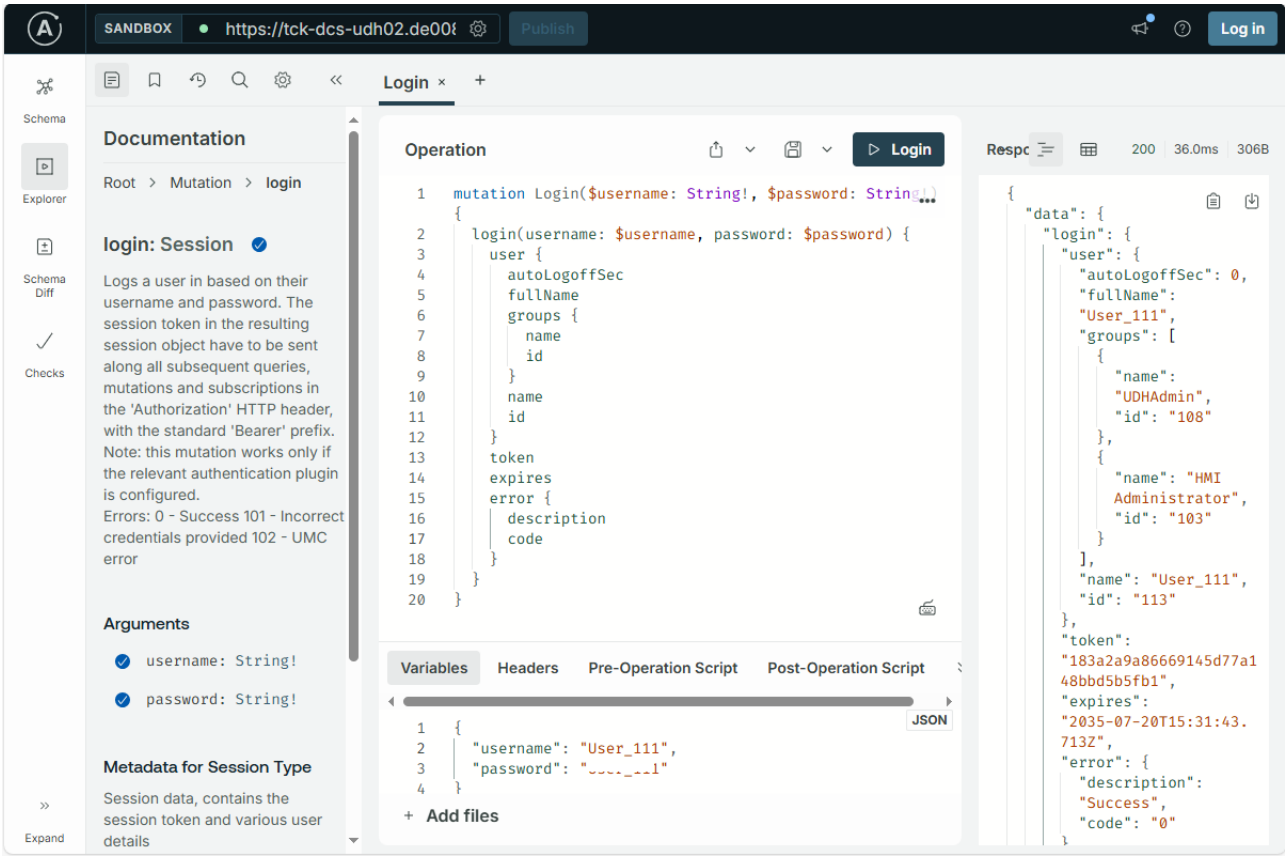
Ensure that you have configured the HTTP header authorization correctly and that you are using a tag name that is available in your product.

Mutation

Mutation operations write data, e.g. changing the value and quality code of a tag. The mutation operations send a one-off HTTPS request to the GraphQL server.

Query

You can read data for the specific logging services with different queries. Each query has its own parameters. A query send a one-off HTTPS request to the GraphQL server.



Note

Ensure that you have configured the HTTP header authorization correctly and that you are using a tag name that is available in your product.

If you query the tag again after performing this mutation, you will find that the value has changed.

Note

The following error or warning messages can occur during the restore process. This is regular behavior in this specific system state and does not cause any problems. After the restore is complete and the system has returned to the normal state, these messages are deleted.

ReadNamedProperty was ended with the following error

Error: [Microsoft][ODBC Driver 18 for SQL Server][SQL Server]Login for user 'NT Service\UDH' to database UDH_Proj01_Target01_AuditTrail_Database failed.'

DatabaseExplorer could not retrieve the protocol inventory for the database UDH_Proj01_Target01_TagLogging_Database

Error: [Microsoft][ODBC Driver 18 for SQL Server][SQL Server]Database 'UDH_Proj01_Target01_TagLogging_Database' is in transition. Try the instruction again later.

DatabaseExplorer could not retrieve the protocol inventory for the database UDH_Proj01_Target01_TagLogging_Database

Error: [Microsoft][ODBC Driver 18 for SQL Server][SQL Server]Database 'UDH_Proj01_Target01_TagLogging_Database' cannot be opened. You are in the middle of a restore.

13.4.1.6 Executing a GraphQL operation in standalone mode

Introduction

Standalone mode allows the UDH server to be disconnected when clients cannot establish a connection.

If a UDH client fails and the UDH data of the client is affected, initiate a backup recovery process in standalone mode.

Without this standalone possibility, UDH clients try continuously to log into the UDH server. This can lead to data loss during the restore process.

Restore process with standalone mode

1. Stop the Runtime project on the UDH server.
2. Restart the Runtime project on the affected UDH client.
3. Start the UDH server in standalone mode using the following steps:
   - Open a command prompt in the directory where the GraphQL Server Manager "UDHServices.exe" is located.
     Example: `C:\Program Files\Siemens\Automation\WinCCUnified\bin`
   - Enter `StartUDHServicesStandalone.bat <install-path> <project-root>`.
     `<install_path>` is the configuration directory of the shared components,
     e.g. `C:\Program Files\Siemens\Automation\WinCCUnified\WCCIL_CC\config`
     `<project_root>` is the path to the downloaded project,
     e.g. `C:\ProgramData\SCADAProjects\Proj02_Central`.
     With these examples, the command looks like this:
     ```
     StartUDHServicesStandalone.bat
     "C:\Program Files\Siemens\Automation\WinCCUnified\WCCIL_CC\config"
     C:\ProgramData\SCADAProjects\Proj02_Central
     ```

4. Restore the backup of the UDH client.
5. Stop the UDH server in standalone mode by running "`StopUDHServicesStandalone.bat`" in the directory where the GraphQL Server Manager "UDHServices.exe" is located.
6. Start the Runtime project on the UDH server.

13.4.1.7 Automatic backup and logging of segments

Segments are logged and backups are created automatically. If the system does not find a full backup, a full backup will be created. If a backup is available, differential backups are created periodically.

Settings

The backup is saved in the same folder as the log. The frequency of differential or full backups is defined in a configuration file. Use the default settings.

Enabling or disabling automatic backup is also managed via the configuration.

The time interval for differential backups should be configured to be shorter than the time interval for full backups. Both time spans can be configured separately via the logging applications.

Default values:

- Differential backup: 1 hour
- Full backup: 1 day

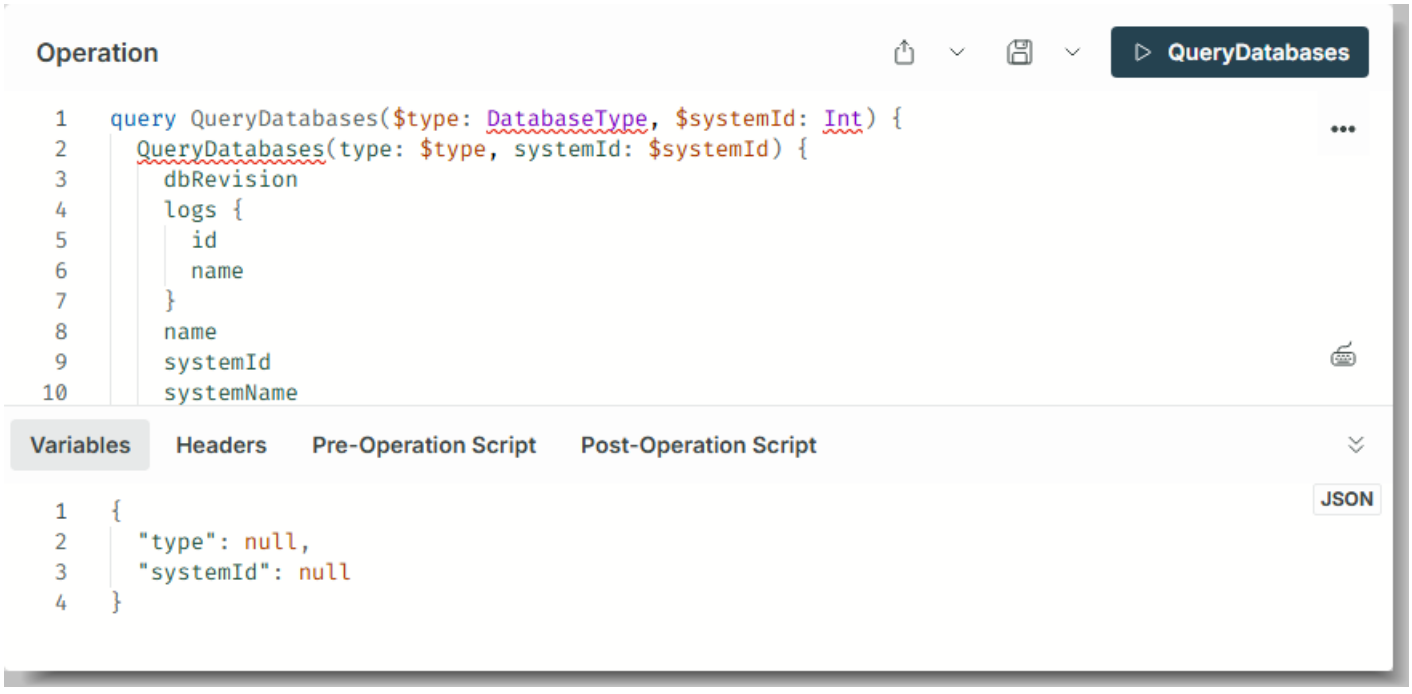
13.4.1.8 Restoring a backup

Requirement

- Public Internet connection

Procedure

1. Log into Apollo Studio:
   Apollo Studio (https://studio.apollographql.com/)
   See also "Setting up the GraphQL client (Page 159)".
   Available queries are displayed on the left side.
2. Perform the query `QueryDatabases`.



   - `type` is an optional parameter that specifies the type of database to be queried. If it is not specified, all databases are returned.
   - `systemId` is an optional parameter that specifies the system ID of the database to be queried. If it is not specified, all databases are returned.

   The response provides the system name, which is required for the next steps.

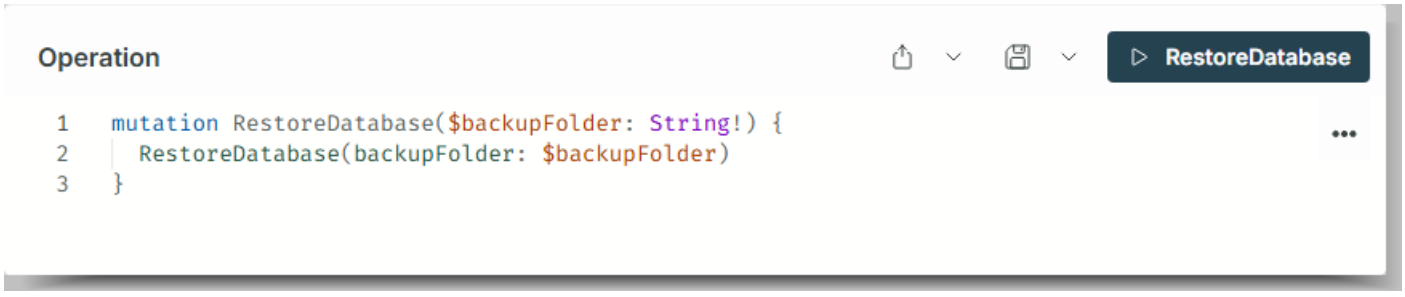
3. Perform the query `QueryBackupInfo`.



   - To list the available backups, click on the + sign next to `QueryBackupInfo` in the left pane.
     The operation is displayed in the middle area.
   - Select the files you want to retrieve in the left area.
   - Fill in the "Tags" arean below.
     `type` and `systemName` are mandatory parameters for the execution of `QueryBackupInfo`.
   - Click "Query".
     The result is shown on the right.

   The response contains `systemName` and `type` which are required for the next step.

4. Perform the query `QueryBackupInfo`.
   The response contains the `backupFolder` which is required for the next step.
5. Perform the mutation `RestoreDatabase`.



   You use this function to restore a database.
   The entry is the `backupFolder` in which the backups are saved

   - Fill in the "Variables" section.
   - Click "RestoreDatabase" to complete the database.
     The system searches for the available backup files and selects them automatically.
     The response contains the time stamp of the restoration process or an error message if an error has occurred.

13.4.1.9 Restore intervals

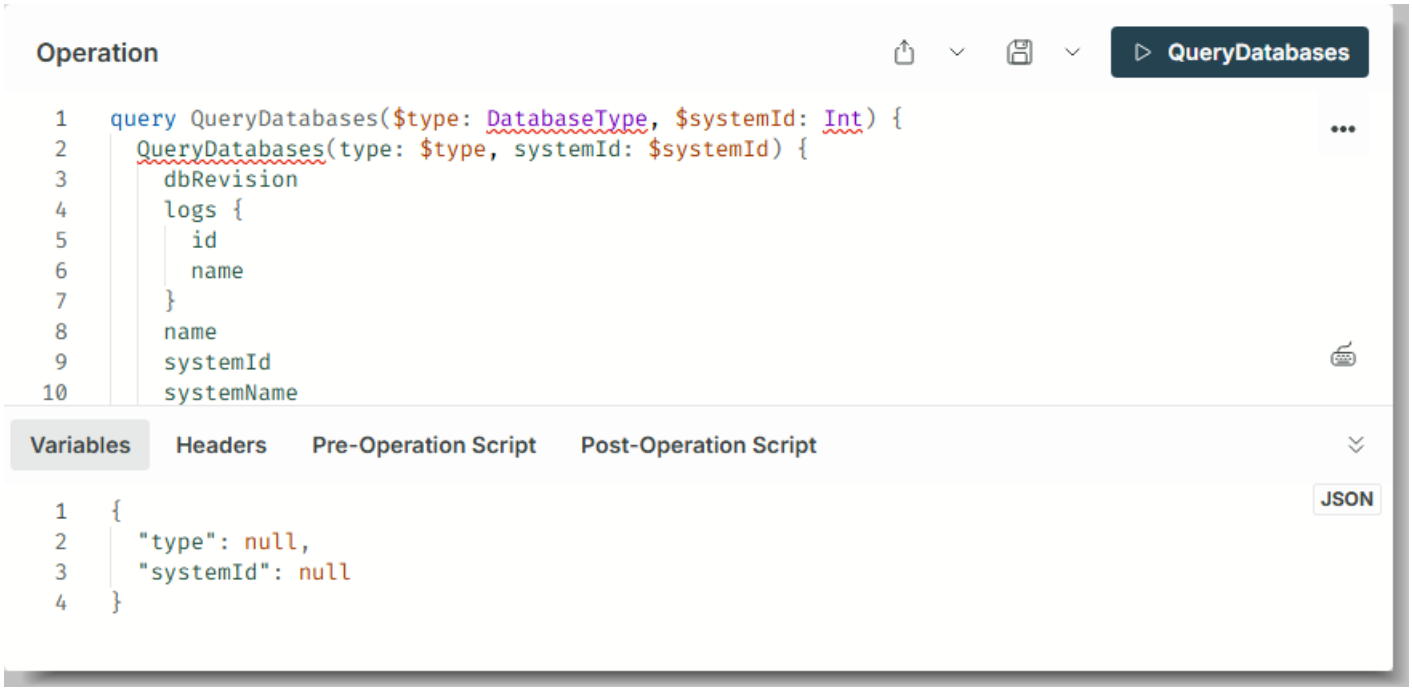
An interval corresponds to a segment that is characterized by the start time and end time of the data acquisition. Segments are periodically swapped out.

You restore intervals in order to be able to read the data they contain.

You undo the restore to free up disk space and prevent unnecessary read access to the data.

Restore interval

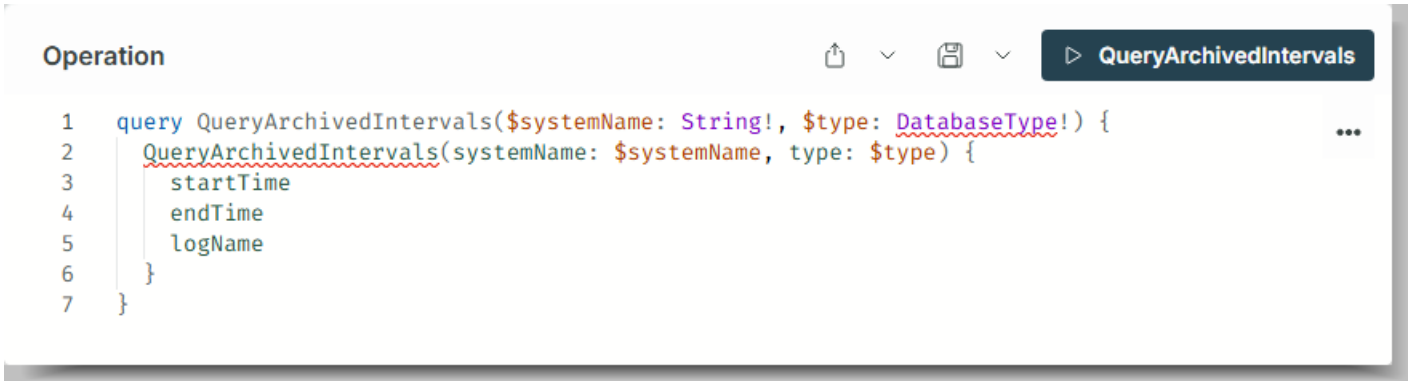
1. Log into Apollo Studio.
2. Perform the query `QueryDatabases`.



   - `type` is an optional parameter that specifies the type of database to be queried. If it is not specified, all databases are returned.
   - `systemId` is an optional parameter that specifies the system ID of the database to be queried. If it is not specified, all databases are returned.

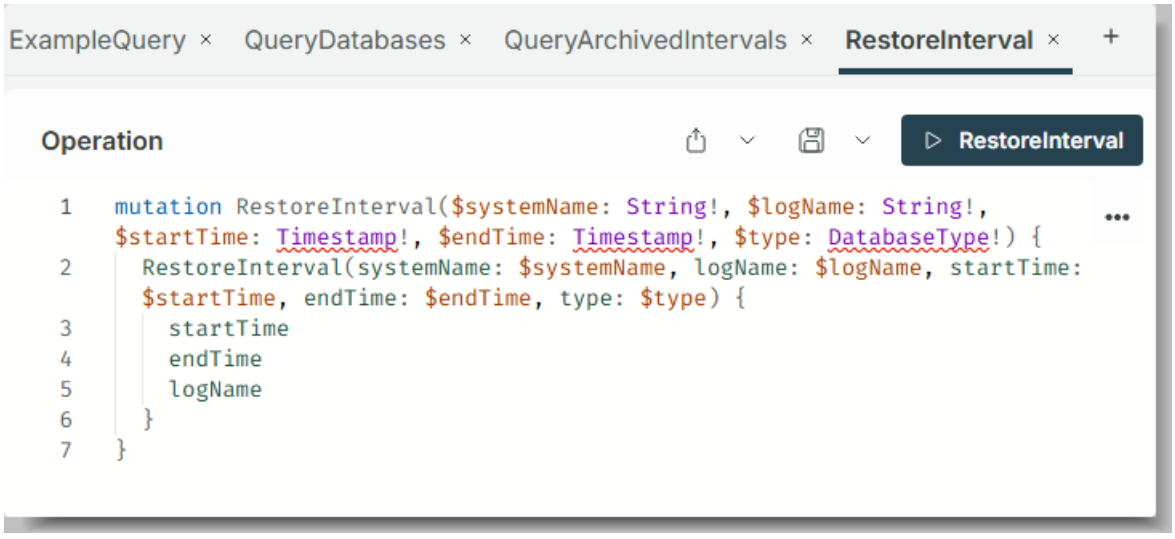
   The response provides the `systemName`, which is required for the next steps.

3. Perform the query `QueryArchivedIntervals`.



The response provides the archive intervals that can be restored in the next step.

4. Perform the mutation `RestoreInterval`.



Restored intervals are available again.

Note

Execution timeout

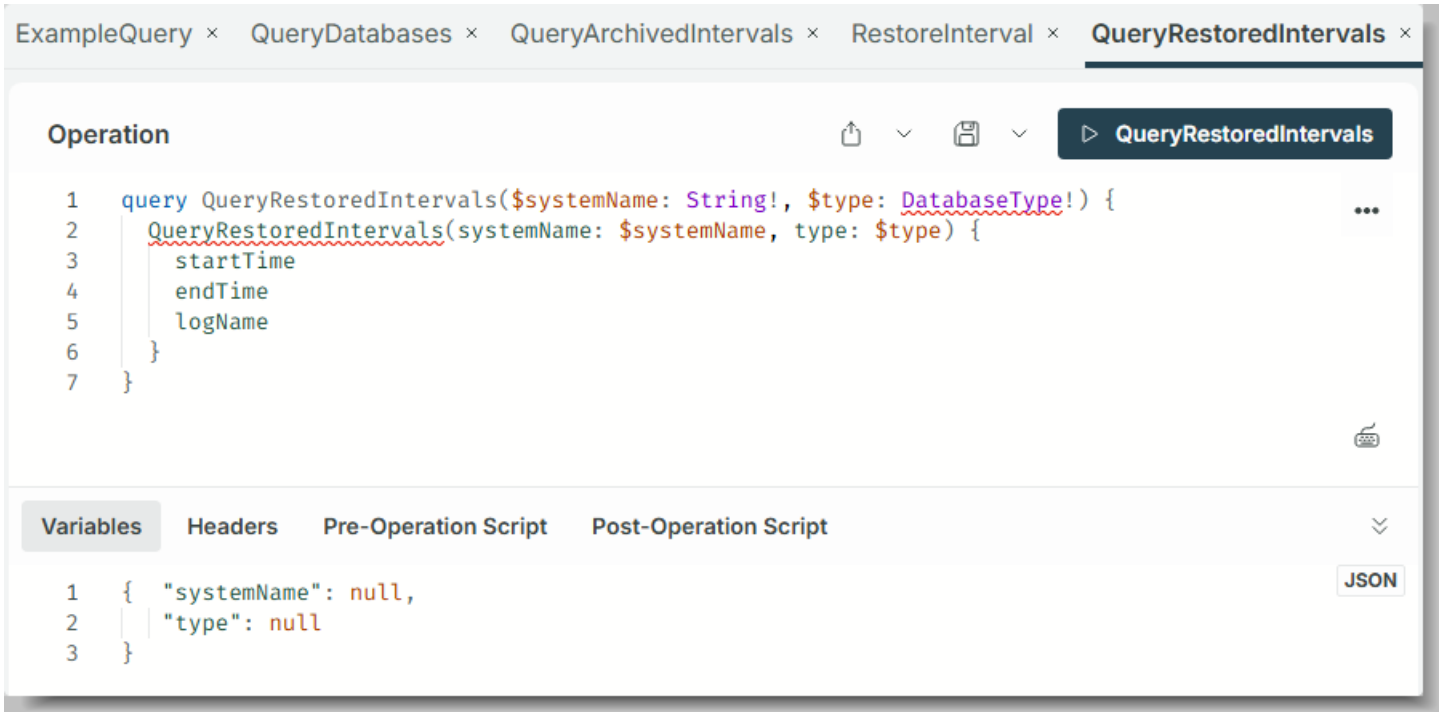
If the execution returns a "NetworkError" as a response, run the corresponding query "QueryRestoredIntervals" again. If the error persists, reduce the configured time interval.

5. Log out of Apollo Studio.

Undoing the restoration of an interval

1. Log into Apollo Studio.
2. Perform the query `QueryDatabases`.
   The response provides the `systemName`, which is required for the next steps.

3. Perform the query `QueryRestoredIntervals`.



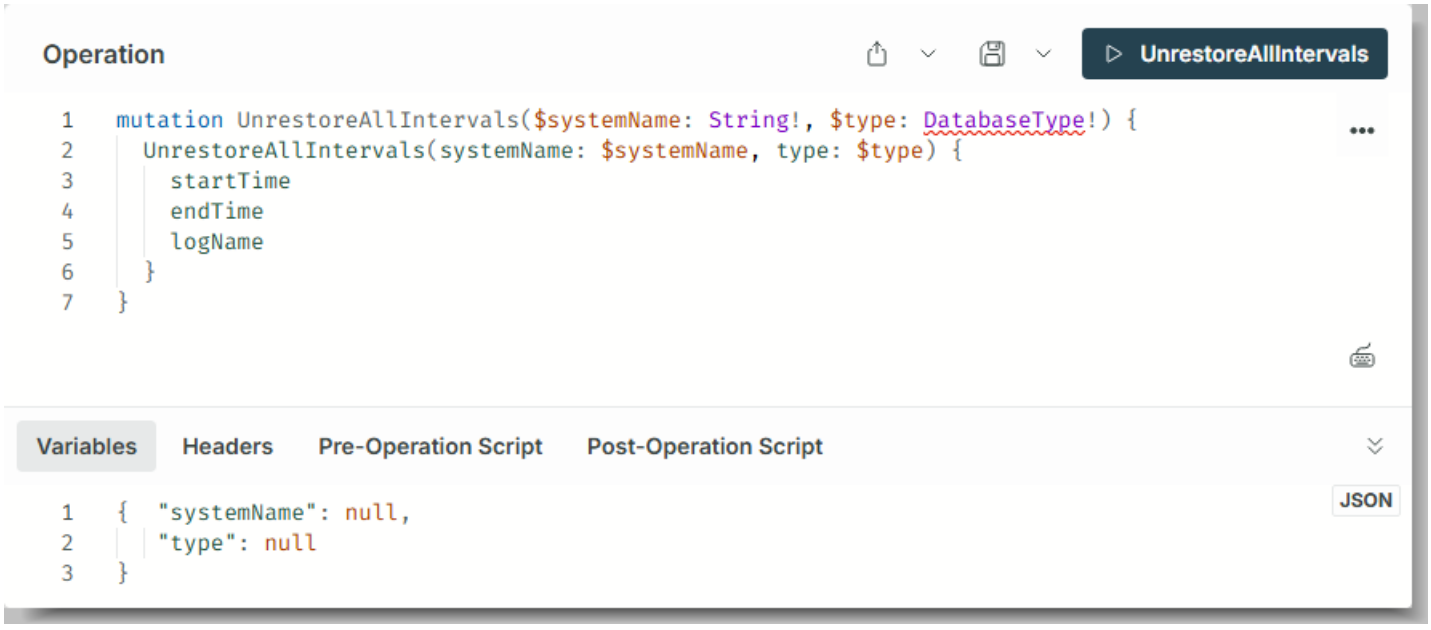
   The response provides the intervals whose restoration can be undone.

4. Perform the mutation `UnrestoreInterval`.
   The restoration of the selected interval is undone.
5. Log out of Apollo Studio.

Undoing the restoration of all intervals

1. Log into Apollo Studio.
2. Perform the query `QueryDatabases`.
   The response provides the `systemName`, which is required for the next steps.

3. Perform the mutation `UnrestoreAllIntervals`.



The restoration of all intervals is undone.

4. Log out of Apollo Studio.

See also

Setting up the GraphQL client (Page 159)