SIEMENS

SIMATIC

TIA Portal Updates Readme

Readme

Validity 1

Improvements in STEP 7 2

Improvements in WinCC Unified 3

Improvements in WinCC Basic, Advanced, Professional 4

04/2026
A5E55548843-AB

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

A5E55548843-AB
Ⓟ 05/2026 Subject to change

Copyright © Siemens 2025 - 2026.
All rights reserved

Table of contents

1 Validity 5

2 Improvements in STEP 7 7

2.1 Improvements in Update 2 7

2.2 Improvements in Update 1 7

3 Improvements in WinCC Unified 9

3.1 Important notes 9

3.2 Quality codes 14

3.3 Engineering and runtime 19
3.3.1 Improvements in Update 2 19
3.3.2 Improvements in Update 1 21
3.3.2.1 General improvements 21
3.3.2.2 Moving objects 22
3.3.2.3 Setting navigation history 27
3.3.2.4 Show limits of tags 28
3.3.2.5 Configure exclusive GUI operator control enable 30
3.3.2.6 System diagnostics control with script diagnostics functions 35
3.3.2.7 System alarms Runtime 39
3.3.2.8 Configuring user management with domains 39
3.3.2.9 OPC UA support for structures 73

3.4 Unified Engineering 74
3.4.1 Improvements in Update 2 74
3.4.2 Improvements in Update 1 75

3.5 Unified PC 76
3.5.1 Improvements in Update 2 76
3.5.1.1 General improvements in Update 2 76
3.5.1.2 Password protection in WinCC Unified Certificate Manager 76
3.5.2 Improvements in Update 1 79

3.6 Unified Panels 80
3.6.1 Important notes (Unified Comfort Panels) 80
3.6.2 Important notes (Unified Basic Panels) 83
3.6.3 Runtime improvements in Update 2 84
3.6.4 Runtime improvements in Update 1 86

3.7 Redundancy 86
3.7.1 Improvements in Update 2 86
3.7.2 Improvements in Update 1 87

3.8 Audit 87
3.8.1 Entries in the Audit Trail 87
3.8.2 Improvements in Update 2 89
3.8.3 Improvements in Update 1 89

3.9 Reporting Excel add-in 93

3.9.1 Improvements in Reporting Excel add-in V26 Update1 93
3.9.2 Improvements in Reporting Excel add-in V26 93
3.9.3 Checking integrity 94
3.9.3.1 Basic information about the integrity check 94
3.9.3.2 Performing an integrity check 94
3.9.3.3 Error cases during the integrity check 96
3.10 Corporate Designer 96
3.10.1 Improvements in Update 2 96
3.10.2 Improvements in Update 1 97
3.11 WinCC Unified Data Hub 97
3.11.1 Improvements in Update 2 97
3.11.2 Improvements in Update 1 97
4 Improvements in WinCC Basic, Advanced, Professional 99
4.1 Important notes 99
4.2 Improvements in Update 2 (Runtime Professional) 100
4.3 Improvements in Update 1 101
4.4 Removing an SQL instance 101

Validity

1

Validity

This update is valid for the following products:

- STEP 7 Basic V21
- STEP 7 Professional V21
- WinCC Basic V21
- WinCC Comfort V21
- WinCC Advanced V21
- WinCC Professional V21
- WinCC Unified Comfort V21
- WinCC Unified PC V21
- TIA Portal Openness V21

Note

If you modify your system with the installation medium after installing the update, you will need to run the update again.

Improvements in STEP 7

2

2.1 Improvements in Update 2

This update contains the following improvements and changes:

Working with the TIA Portal

Stability when working with the TIA Portal has been improved, partly based on the feedback from returned crash reports.

Advanced online functions of named value data types have been enabled

Named value data types can now be opened via the list of accessible devices (Lifelist) and by a card reader (read-only). Named value data types that are only available online can also be opened directly from the online view of the CPU.

Dependency between project languages and settings for multilingualism of the CPU removed

If you change the editing language and reference language in your project, this will no longer affect the configuration of multilingualism in the properties of the CPU.

2.2 Improvements in Update 1

This update contains the following improvements and changes:

Working with the TIA Portal

Stability when working with the TIA Portal has been improved, partly based on the feedback from returned crash reports.

OPC UA server restart

The need for OPC UA server restarts in certain scenarios has been reduced.

A server restart is no longer required in the following cases:

- When loading non-structural changes to an instance data block.
  This means that adjustments to the content of an instance data block that do not change its structure (such as data types or number of elements) no longer require a restart.
- When loading global data blocks for which the "Data block accessible from OPC UA" attribute is disabled.

Disable the attribute "Data block accessible from OPC UA"

The "Data block accessible from OPC UA" attribute is enabled for all blocks by default. If you want to disable this attribute for a global data block in order to avoid the need for a server restart when loading, follow these steps:

1. Select the "Program blocks" folder in the project tree.
2. Right-click on a block.
3. Select the "Properties" command in the context menu.
   The properties dialog box of the block opens.
4. Click the "Attributes" group in the area navigation.
5. Disable the attribute "Data block accessible from OPC UA".

Exporting blocks with user texts in SIMATIC SD format after upgrading the project

When blocks with user texts are exported in SIMATIC SD format after upgrading a project from V20 to V21, the user texts of the selected block and their assigned MLC IDs (multilingual comment IDs) are lost.

The menu command "Prepare for SIMATIC SD" has been added to the "Options" menu in order to retain the user texts in all project languages and their assigned MLC IDs during export and to ensure that the s7res file is generated.

Improvements in WinCC Unified 3

3.1 Important notes

This page contains important information about product properties.

Licensing: WinCC Unified Clients

SIMATIC HMI Unified Comfort Panels

The following remote accesses (except for local operator control & monitoring) to the Panel Runtime are included license-free:

- 1 x WinCC Unified Client Operate for operator control & monitoring via the Web client
- 1 x WinCC Unified Client Monitor for monitoring via the Web client

Importing S7P files

Importing S7P files is again supported as of V21 Update 2. Simatic Manager 5.7 SP3 is the minimum version that must be installed.

Redundancy

The following subsystems are not yet supported in a redundant system:

- Plant hierarchies
- WinCC Unified Data Hub

User management

When updating the TIA Portal project to device version 21.0.1.0, the user management data must be reloaded during the first download, even if the user has not made any changes to the user configuration. To ensure this, the "Keep current user management data in runtime" option must be disabled in the "Load preview" dialog.

Central user management with shared user domains**:** The central user management of a UMC server can be linked to additional UMC servers and thus expanded. If a UMC Runtime server is used in such a configuration, this server does not provide an "ID provider". When setting up a central domain on the HMI device, the address of the ID provider is generated automatically based on the UMC server address and cannot be changed. This means that UMC servers that do not provide an "ID provider" address (e.g. UMC Runtime servers) cannot be used as UMC servers.

Project download and mapping between central groups and local roles: If you are configuring an OEM domain, you can add a central domain in the Runtime Manager after the project download. The mapping is then created between the central groups and the local roles to which the "Shared role" function right has been assigned. If the user management data is overwritten during a new project download, the mapping is lost. To retain the mapping,

select the option "Keep current user administration data in Runtime" option in the "Load preview" dialog when downloading the project again. Otherwise, the mapping must be repeated.

For HMI devices, the "Radius" authentication method is not supported when adding a user in the "Security settings > Users and roles" editor.

If you want to manage the local users in the "Browser" screen object, enter the IP address or the fully qualified domain name (FQDN) of the device in the "Browser" screen object. The "User login" dialog is displayed.

For shared roles in domain-based user management: The shared-role name must not begin or end with a blank space.

Graphics

If different image formats have been defined for a graphic, an error message is displayed after compiling, advising that mixed image formats are not supported on this device.

I/O field: Configuration and display of tags with time data types

The PLC data types "TIME" and "LTIME" are mapped to the same HMI data type "LTime" in WinCC Unified.

Note that the configuration and display of tags with data type "LTime" in I/O fields is currently not consistent with respect to the base unit. In engineering, the data type "LTime" has the base unit 100 nanoseconds and is configured there accordingly, while in Runtime, I/O fields display the value for numerical output formats in milliseconds. This also pertains to the configured ranges of a tag. The input is processed as a value in milliseconds. If necessary, use a conversion script to adapt the configuration and achieve the desired display in Runtime.

The output format for time specifications {P,s.SSS} is not localized in the I/O field in Runtime and consistently uses a period as decimal separator, regardless of the configured language.

Alarm control

The configuration setting for the "Display options - Configuration" button in the toolbar now works correctly. If this option is set to "None", no alarms are displayed. To make the alarms visible again, the setting must be changed from "None" to another option, for example to "Not suppressed".

Support for automatic multi-line text

Alarm text that exceeds the width of its respective columns is wrapped within the cell. When an alarm line is selected, its height increases automatically to display the wrapped text in full. The heights of all other, unselected alarm rows are also adjusted to ensure a consistent row height across the entire grid. If the text in a line still exceeds the increased height, it is truncated accordingly.

This functionality is supported for the following alarm control columns:

- Information
- Alarm text
- Additional text 1-9

To do this, set the option in Engineering under "Properties > Properties > Alarm control > Selection - Mode" to "Single".

Audit: Mandatory comment for operation

The confirmation for operating actions is always identical for all subsystems. All dialogs use the same workflow, regardless of whether changes are made to alarms, tags, parameter sets, etc.

Trend companion: Indicators at the displayed value

The following indicators are added as a suffix to the values of the trend companion to indicate particular states:

Indicator	Meaning
i.	Indicates that the data was interpolated and does not correspond to an actual tag value. Example: A tag has the value "40" and time stamp "10:00" and the next value "50" and time stamp "10:10". If the ruler of the linked trend view intersects with time stamp "10:05", the "Y-value" column displays the value "45 i." and the "Time stamp" column displays the value "10:05 i.".
b.	Indicates that the tag value has quality code "Bad" at the intersection of the ruler on the PLC side.
u.	Indicates that the tag value has quality code "Uncertain" at the intersection of the ruler on the PLC side.

A combined display of the indicators, i.e., "i. b." or "i. u.," is also possible.

Parameter set control: Restrictions

- The "Filter - allow" property is not supported in the parameter set control.
- 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 display.

Faceplates: "Suspendable" property

The "Suspendable" property of faceplate types only affects scripts for dynamization. Events are excluded from suspension.

- Activating the "Suspendable" property can suspend the scripts for dynamizing non-visible faceplate instances in Runtime.
- The Runtime environment controls which scripts are executed and depends on the performance in Runtime.
- Only scripts that are used for dynamization are suspended. Events are not affected by the "Suspendable" property.

Tags: Thresholds for local session tags

Dynamic thresholds are not supported for local session tags.

Logging

When configuring segmented logs, please note the following additional information:

Size of a log

Note

Memory problems when segmentation is disabled

If you specify "0" for the log period and the maximum log size, segmentation and automatic deletion of segments will be disabled. You cannot create a backup when segmentation is disabled.

Since the log is not limited in size or time period, the hard drive may run out of storage space. To prevent this, the logs can only be deleted via the system functions "ClearAlarmLog" or "ClearTagLog". It is therefore strongly recommended to configure at least the log period or the maximum log size.

Size of a segment

Note

Incorrect configuration when segmentation is disabled

If you have configured "Log time period" and/or "Maximum log size", you must also configure "Segment time period" and/or "Maximum segment size". Otherwise, logging is not possible.

System functions: Parameter description of OpenPLCCodeViewByFCCall changed

The descriptions of the parameters to be transferred for the system function "OpenPLCCodeViewByFCCall" for use in the function list and in the WinCC Unified object model have been adapted:

Parameter	Description
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 that contains the "Called block" block.

Parameter	Description
Called block	Name of the local or global instance of a function 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". 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	Name of the PLC tag or data block tag of a user data type instance connected to "PIN". The parameter is used to limit the display of functions if the function named in "Called block" is called several times. The use of user data type instances requires that the tags of the user data type instance originate from the same data block as the function specified in "Called block".
Screen object path	Path of the screen object "PLC code view".

System functions: Necessity of edit tags for CreateParameterSet

To create parameter sets in Runtime using the "CreateParameterSet" system function, you need to configure the edit tags for the corresponding type of parameter set.

The documentation for the configuration of edit tags has been improved.

"StartProgram" system function

Contrary to the information in the documentation, the value of the parameter "Program name" must not be enclosed in quotation marks, even if the path contains spaces.

Aggregating tag values

The tag values are only aggregated for the following data types and always with the "TimeAverageStepped" aggregation mode: SInt, USInt, Int, UInt, DInt, UDInt, Real, LReal

The tag values are not aggregated for all other data types.

"CreateParamterset" system function

To be able to create a parameter set with the system function "CreateParameterSet" system function, an edit tag must be configured.

System functions for opening/changing a screen with Unified Collaboration

The following system functions cannot be used with Unified Collaboration, because the screen number only allows access to screens from the same device:

- OpenScreenByNumberInPopup
- ChangeScreenAsyncByNumber
- ChangeScreenByNumber

In conjunction with Unified Collaboration, use the following system functions instead:

- OpenScreenInPopup
- OpenScreenInPopupAsync
- ChangeScreen
- ChangeScreenAsync

System function "ChangeUser"

The function is also terminated without an error code if no user change occurs, for example, due to an incorrect password.

3.2 Quality codes

Quality codes

Quality code according to PROFIBUS PA or OPC DA Addition to the quality code tables for the sub-status

Sub-status (bit 5 to bit 2)

Sub-states divide the individual qualities.

- **Sub-Status "BAD"**

BAD: Sub-Status (Bits 5...2)		
0000	Non-specific	There is no specific reason why the value is BAD.
0001	Configuration error	The value is not useful because of some inconsistency regarding the configuration.
0010	Not connected	The value is not reliable because the connection to the provider has been disconnected at consumer-side, e.g. a communication driver actively disconnects from a PLC on user request or by design.
0100	Sensor failure	The value is not useful because it cannot be converted, i.e. a value from the device (PLC) cannot be converted to the corresponding HMI tag.
0101	No communication, with last usable value	The value is not useful because communication to the data source failed, however a last known value is available.
0110	No communication, no usable value	The value is not useful because communication to the data source failed or has never been established since it was last out of service and a last known value is not available.
0111	Out of service	The value is not reliable because the provider side has been disabled or shutdown, e.g. a PLC is in stop mode, or a tag is disabled for maintenance purposes.

- **Sub-Status "UNCERTAIN"**

UNCERTAIN: Sub-Status (Bits 5...2)		
0000	Non-specific	There is no specific reason why the value is UNCERTAIN.
0001	Last usable value	The connection to the data source is still established; however, the data source stopped updating the value for some reason.
0010	Substitute value	A predefined value is used in case of an invalid value due to communication issues with the data source or a range violation. The reason for providing substitute values is configurable.
0011	Initial value	A predefined value intended for the startup of the HMI system (or a sub-ordinate device) is used while not being able provide values from the data source.
0101	Range violation	The value lies outside the range defined by min value and max value. The Limits define which direction (min or max) has been exceeded.
0110	Sub-normal	A value derived from multiple values has less than the required number of good sources. This includes data aggregation by means of data compression algorithms.

- **Sub-Status "GOOD (cascade)"**

GOOD (cascade): Sub-Status (Bits 5...2)		
0000	Non-specific	No error or special condition is associated with this value.
0110	Local override	The value has been overridden by the user or some logic in to continue operation. Typically, the input has been disconnected, and a manually entered value has been 'forced', or a value has been corrected.

Specific information for WinCC Unified Addition to the quality code tables for the sub-status

Extended sub-status (bit 11 to bit 8)

The extended sub-status provides more detailed information about the sub-status. The extended sub-status is relevant for some Quality Codes formed by the HMI system.

- **Extended Sub-Status "BAD"**

Extended Bad Sub-Status (Bits 11...8)		
0000	Non-specific	No HMI specific extended bad sub-status is associated with this value.
0001	Aggregated value	The value has been calculated out of multiple values with less than the required number of good sources. This includes data aggregation by means of data compression algorithms. The corresponding sub-status is set to 'non-specific'.
0011	Unusable value	A (logged) value has been identified to be incorrect, but a respective correction value is not available. The corresponding sub-status is set to 'non-specific'.
0111	Disabled	The provider of the value has been disabled and the previous value was BAD. The corresponding sub-status is taken from the last (previous) sub-status.

- **Extended Sub-Status "UNCERTAIN"**

Extended UNCERTAIN Sub-Status (Bits 11...8)		
0000	Non-specific	No HMI specific extended uncertain sub-status is associated with this value.
0001	Aggregated value	The value has been calculated out of multiple values with less than the required number of good sources to be GOOD as well as less than required number of bad sources to be BAD. This includes data aggregation by means of data compression algorithms. The corresponding sub-status is set to 'sub-normal'.
0111	Disabled	The provider of the value (e.g. logging tag for logged value) has been disabled and the previous value was GOOD or UNCERTAIN. In case of GOOD the corresponding sub- status is set to 'last usable value'. In case of UNCERTAIN the corresponding sub-status is taken from the last (previous) sub-status.

- **Extended Sub-Status "GOOD (cascade)"**

Extended GOOD Sub-Status (Bits 11...8)		
0000	Non-specific	No HMI specific extended good sub-status is associated with this value.
0001	Aggregated value	The value has been calculated out of multiple (good) values. This includes data aggregation by means of data compression algorithms. The corresponding sub-status is set to 'non-specific'.
0010	Manual input	A (logged) value has been created manually. The corresponding sub-status is set to 'non-specific'.

Extended GOOD Sub-Status (Bits 11...8)		
0011	Corrected value	A (logged) value has been corrected. The corresponding sub-status is set to 'non-specific'.
0110	Initial value	The local data source has been initialized with the configured initial value. The corresponding sub-status is set to 'non-specific'. HmiSimpleTag supports the definition of subsets for discrete values via class HmiEnumeration by optional Ref Attribute 'Enumeration'. Only values from the referenced HmiEnumeration are valid values for the HmiSimpleTag. The restriction applies to a single value, or all elements of a dynamic array of values. The datatype of the HmiSimpleTag, or the base datatype in case of a DynArray, must match the datatype of the referenced HmiEnumeration. In case that the value (received from external communications partners such as PLC's) does not match the valid enumeration values of the respective HmiSimpleTag, a configured substitute value is used and the quality code is set to "uncertain; substitute value", if configured; else the null value is used and the quality code is set to "uncertain; substitute value". Additionally, a corresponding trigger event is fired for tags.

Faceplates: "Suspendable" property

The "Suspendable" property of faceplate types only affects scripts for dynamization. Events are excluded from suspension.

- Activating the "Suspendable" property can suspend the scripts for dynamizing non-visible faceplate instances in Runtime.
- The Runtime environment controls which scripts are executed and depends on the performance in Runtime.
- Only scripts that are used for dynamization are suspended. Events are not affected by the "Suspendable" property.

System functions: Parameter description of OpenPLCCodeViewByFCCall changed

The descriptions of the parameters to be transferred for the system function "OpenPLCCodeViewByFCCall" for use in the function list and in the WinCC Unified object model have been adapted:

Parameter	Description
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 that contains the "Called block" block.

Parameter	Description
Called block	Name of the local or global instance of a function 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". 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	Name of the PLC tag or data block tag of a user data type instance connected to "PIN". The parameter is used to limit the display of functions if the function named in "Called block" is called several times. The use of user data type instances requires that the tags of the user data type instance originate from the same data block as the function specified in "Called block".
Screen object path	Path of the screen object "PLC code view".

3.3 Engineering and runtime

3.3.1 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.

Text box

The text in the "Text box" object is displayed correctly in the simulation in WebRH after "Properties > Format > Text trimming > With character ellipsis" is selected.

I/O field

The I/O field correctly displays the default integer value.

Unified Panel: Behavior of the symbolic I/O field during operator actions

The behavior of the symbolic I/O field has been improved for the following operator actions:

Operator action	Starting point	Is the drop-down list of the symbolic I/O field open?	Result
Zoom (touch gesture)	On the symbolic I/O field	Yes	• No zooming takes place. • The drop-down list remains open.
		No	• Zooming takes place.
	Outside the symbolic I/O field	Yes	• The drop-down list is closed. • Zooming takes place.
Zoom (by tag dynamization)	N/A	Yes	• The drop-down list is closed. • Zooming takes place.
Move (using touch gesture or slider on the scrollbar)	On or outside the symbolic I/O field	Yes	• The drop-down list is closed. • Area is moved.
		No	• Area is moved.

Button

The property "Pressed status tags" is consistently and correctly triggered for the button when operated by mouse, touch and keyboard (Enter and Space).

Trend companion

The output of values in date and time format has been improved and now takes the exact configuration into account.

Parameter sets

The error feedback when creating and configuring parameter set types has been improved.

Limit marking in screen objects

Limit marking in screen objects that support thresholds has been improved.

Faceplates

The use of expressions in faceplates has been improved.

The process values are now correctly centered on the bar in the faceplate and displayed with the correct unit.

System functions

If you launch a UI program using the system function "StartProgram", it will run correctly in the foreground.

Alarms

The display of the alarm indicator has been improved and the text alignment is now displayed correctly, i.e. centered.

GRAPH overview

The "GRAPH overview" control has been improved, and the active step is now displayed correctly even after the GRAPH function block has been reinitialized.

View of Things

The "Command fired" event works correctly in View of Things for the "Browser" object.

3.3.2 Improvements in Update 1

3.3.2.1 General improvements

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

The Date Time Picker dialog in Runtime only shows the required fields for the configured output format. The behavior is uniform on Unified Comfort, Unified Basic Panel and PC.



In the "Browser" object, the files in the "UserFiles" directory can be displayed on Unified PC via the URL "https://<IP address or FQDN of the Unified PC>/UserFiles/<file name or file path>". The addressing of the computer should be the same used as for Unified Runtime. The document is opened in Runtime directly in the "Browser" control.

3.3.2.2 Moving objects

Introduction

In WinCC Unified, you can configure the movement of objects in a similar way to WinCC Comfort, without configuring scripts.

The following movement types are supported:

- Linear movement (horizontal, vertical, diagonal) with fixed start and target position.
- Direct movement with tag position based on tag values.

Both movement types can be linked with PLC tags, internal HMI tags and expressions.

When switching between the two movement types, you will be notified if existing dynamizations are overwritten. This prevents unintentional configuration losses.

Linear movements are applied synchronously to both position properties (left and top). Direct movements allow independent configuration of each position property with different dynamization types.

Requirement

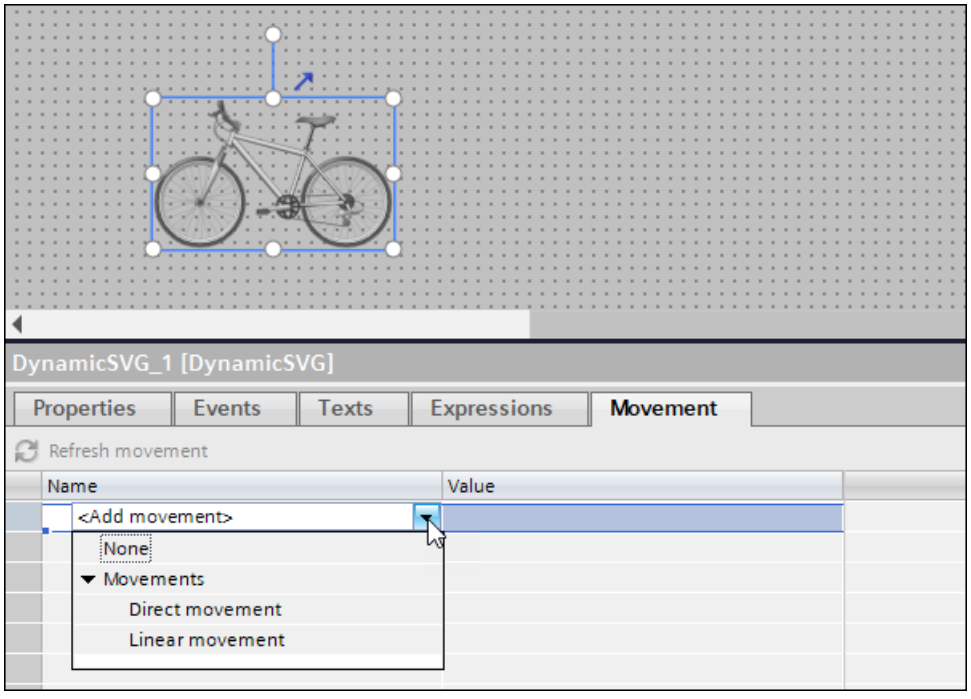
- The HMI screen is open with at least one object.

Initial situation

If you select an object in the screen, the "Movement" tab under "Properties" becomes visible.

The icon is displayed for non-configured objects.

The icon is displayed for objects that have already been configured.

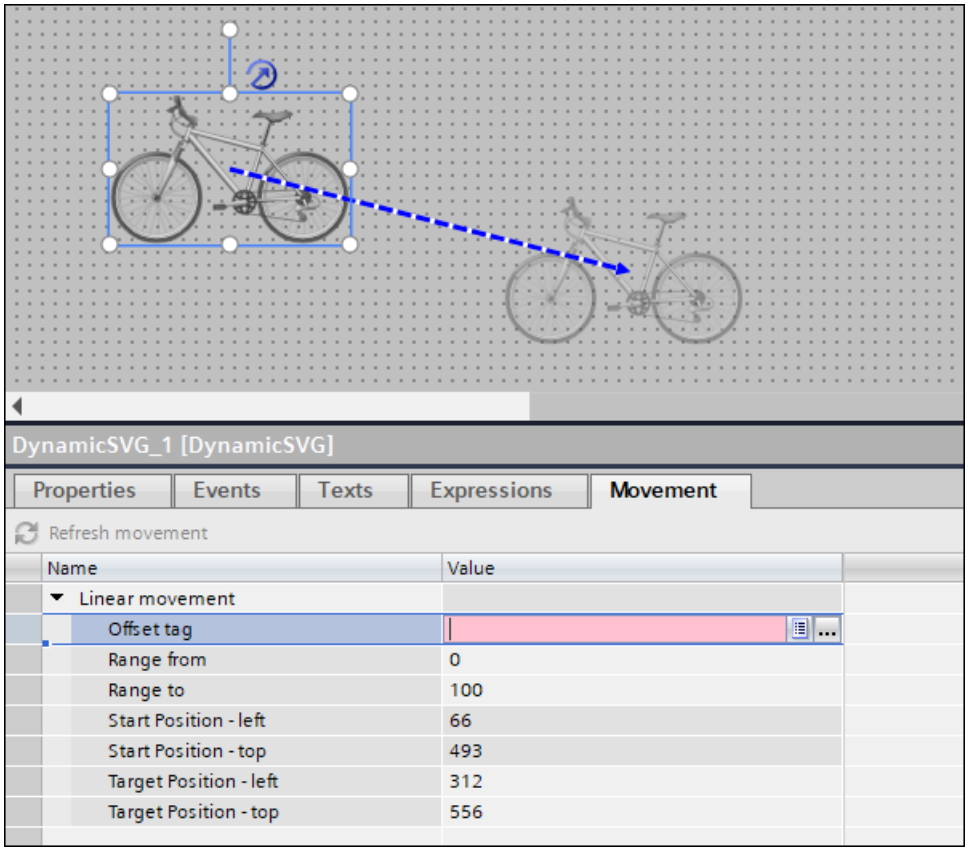


Configuring linear movement

To configure linear movement animation, follow these steps:

1. Click the icon or select "Linear movement" in the Inspector window under "Movement > Name".
2. Under "Movement > Name > Linear movement" in the Inspector window, configure:
   - Offset tag: The tag value determines the current position of the object. The value is between 0 and the range maximum.
   - Range from - to: The value range over which the movement is distributed.
   - Start position left and top is defined in the properties.
   - Target position Left and Top is defined in the properties.

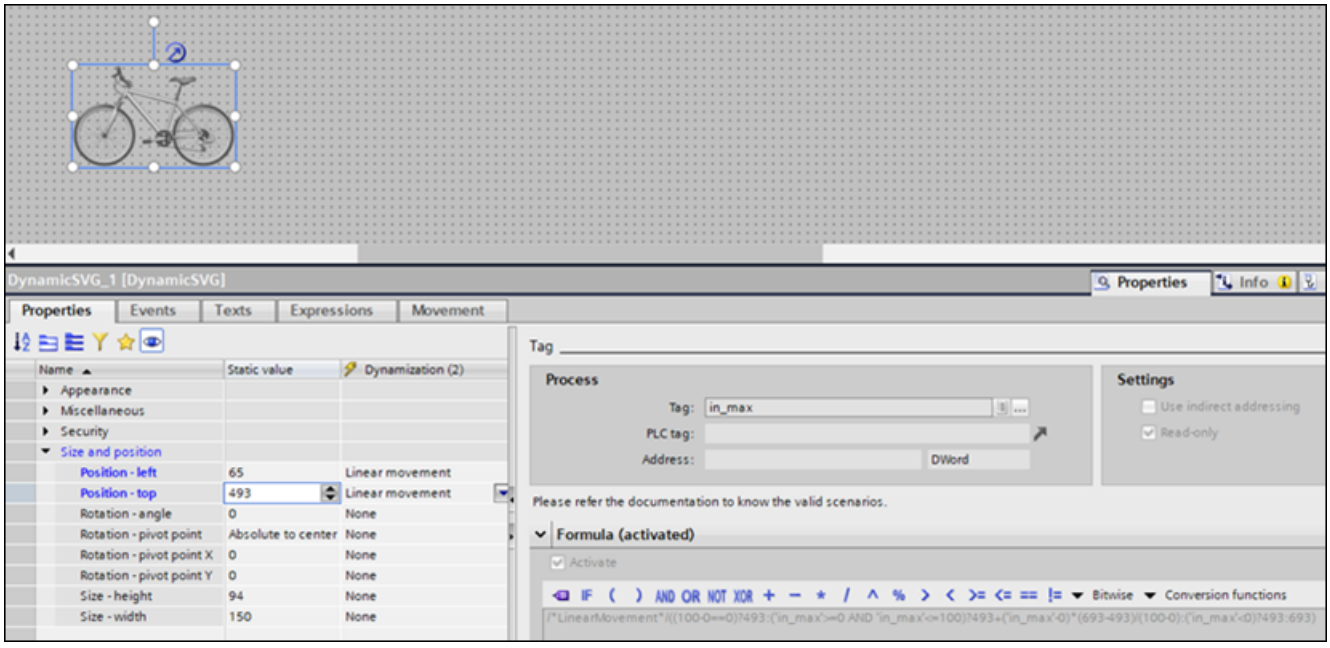
   You can also change the position of the objects directly in the screen by dragging the objects. When dragging, the object coordinates x/y and w/h are displayed on the object.



Note:

- In the Inspector window under "Properties > Size and position > Position - left / Position - top", the values and the "Linear movement" type of dynamics are displayed and updated accordingly.
- If the values in the "Properties" and "Movement" tabs are different, click the "Refresh movement" button. The values are synchronized.

- The target position, the range, the minimum and the maximum are displayed in the formula. The formula is updated accordingly.

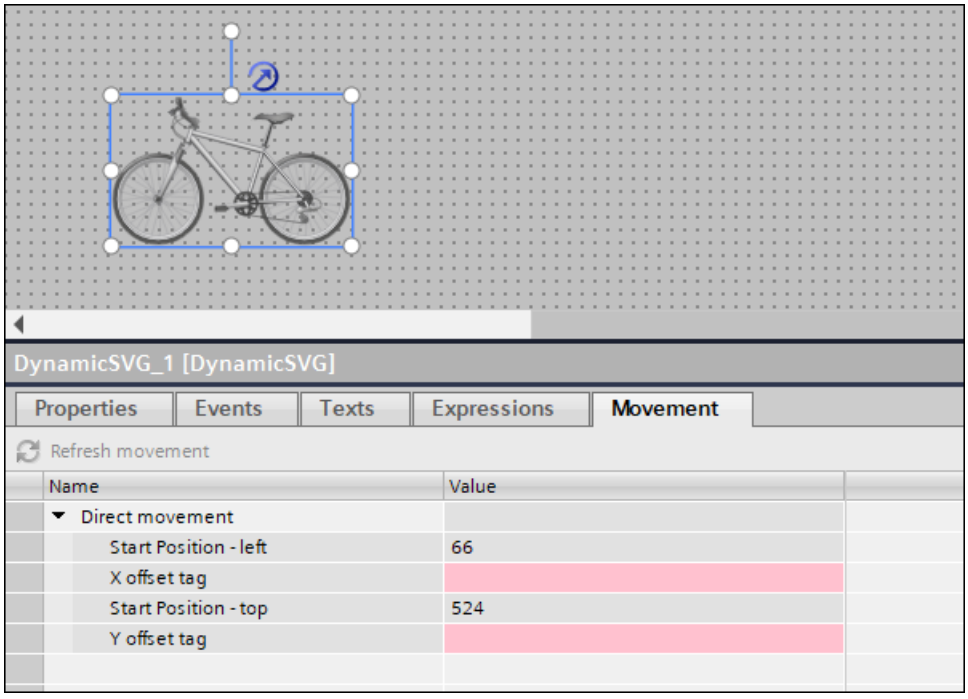


- The preview of object movements is available for relative movement - linear, horizontal, vertical, diagonal.

Configuring direct movement

Proceed as follows to configure direct movement animation:

1. Select in the Inspector window under "Movement > Name" the "Direct movement."
2. Configure:
   - Start position left and top
   - Offset tags X and Y.
     Configure at least one offset tag.



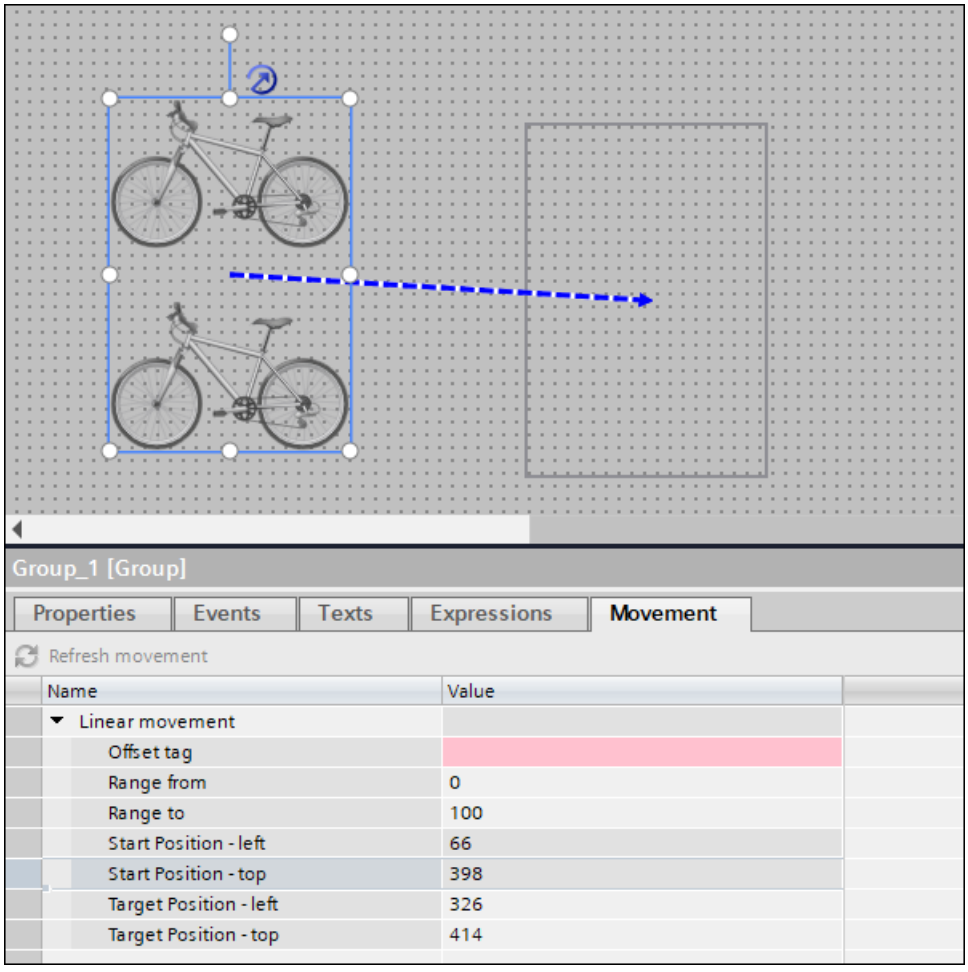
Note:

- In the Inspector window under "Properties > Size and position > Position - left / Position - top", the values and the "Direct movement" dynamization type are displayed and updated accordingly.
- The position is displayed in the formula. The formula is updated accordingly.
- For direct movements, you can configure the "Position - Left" and "Position - Top" independently of each other. While the "Position - Left" can use a direct movement, the "Position - Top" can be dynamized simultaneously with scripts or other dynamization types.
- The preview for direct movement is not displayed in the Engineering System. However, the movement works in Runtime.

Moving object groups

If you want to move several objects at the same time, create an object group.

The bounding box is displayed when the object group is moved linearly.



3.3.2.3 Setting navigation history

Introduction

In the Runtime settings of the device, you can specify how the navigation history is displayed via the screen windows. Two modes - "Flat" and "Nested" - are available.

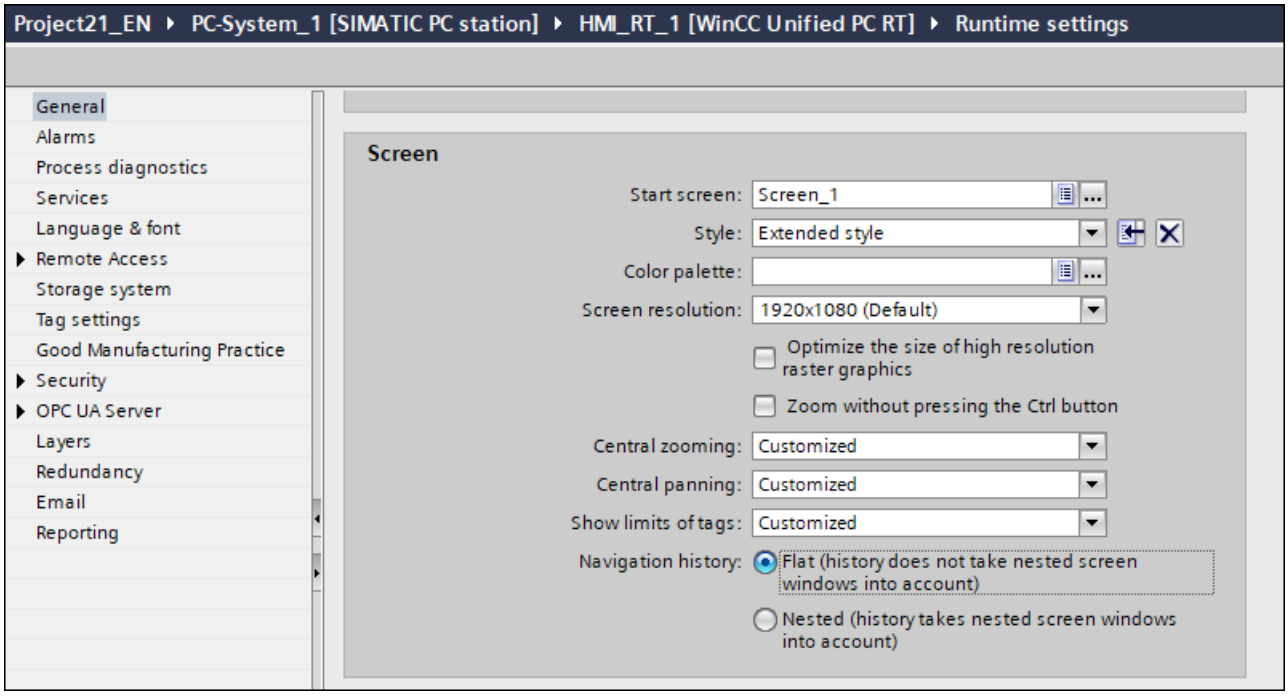
You can use the system functions "ChangeScreenNext" and "ChangeScreenPrevious" for the global navigation concept between screens.

Nested mode is recommended for the navigation concept that spans several screen windows.

Setting navigation history

In the Runtime settings of the device under "General → Screen", you define how the navigation history is displayed via the screen windows:

- Flat:
  The navigation history is limited to one screen window. The screen window is defined via the parameter of the ChangeScreenNext/ChangeScreenPrevious system function. This mode is recommended if you require a separate navigation history for each screen window.
- Nested:
  The navigation history extends to the screen window that is specified as a parameter of the ChangeScreenNext/ChangeScreenPrevious system function and to all lower-level screen windows. With this setting, you can achieve a global navigation history across several screen windows.



The "Flat" option is enabled by default.

Navigation is still possible separately for each screen window.

3.3.2.4 Show limits of tags

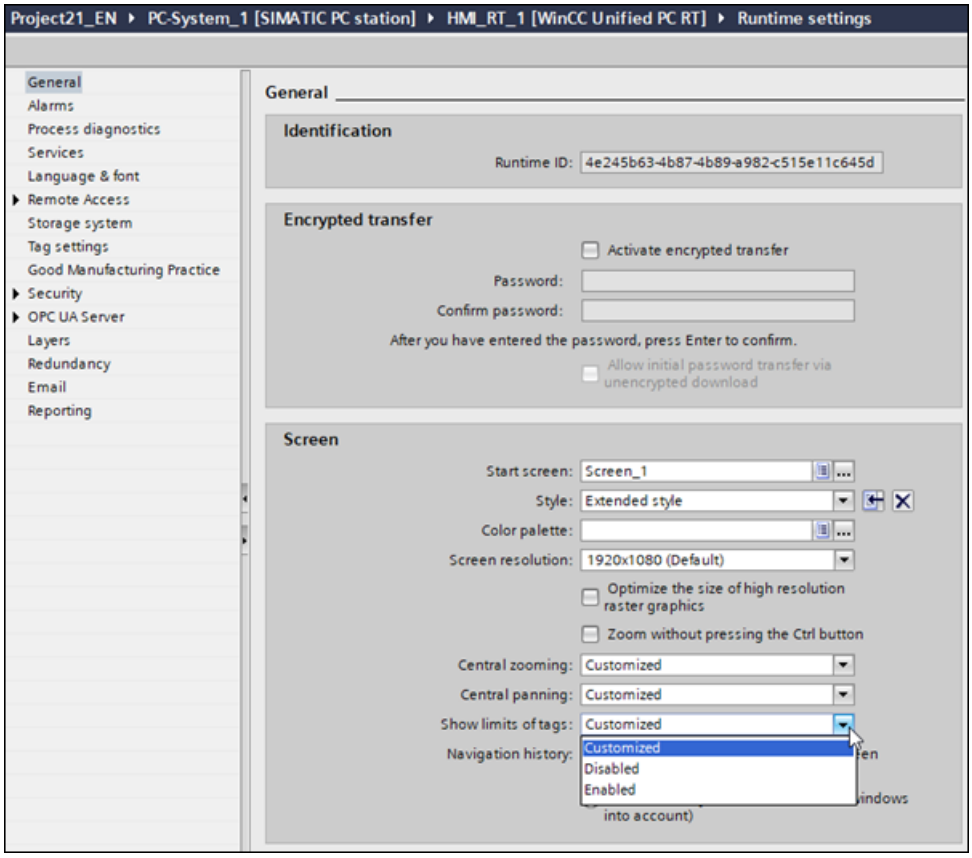
Introduction

In the Runtime settings of the device, you can centrally enable or disable the display of the limits of tags when entering values. The "Show limit" property configured for the individual I/O fields is thus ignored and generally displayed as always enabled or always disabled for all I/O fields.

Enable display of the limits of tags

To enable the display of tag limits, follow these steps:

1. Double-click on "Runtime settings" of the device in the project tree.
2. Select one of the options under "General > Screen > Show limits of tags":
   - Customized: You can enable the display of the tag limits for each I/O field individually. "Customized" is the default setting.
   - Disabled: The display of tag limits is disabled for all I/O fields in the project.
   - Enabled: The display of tag limits is enabled for all I/O fields in the project.

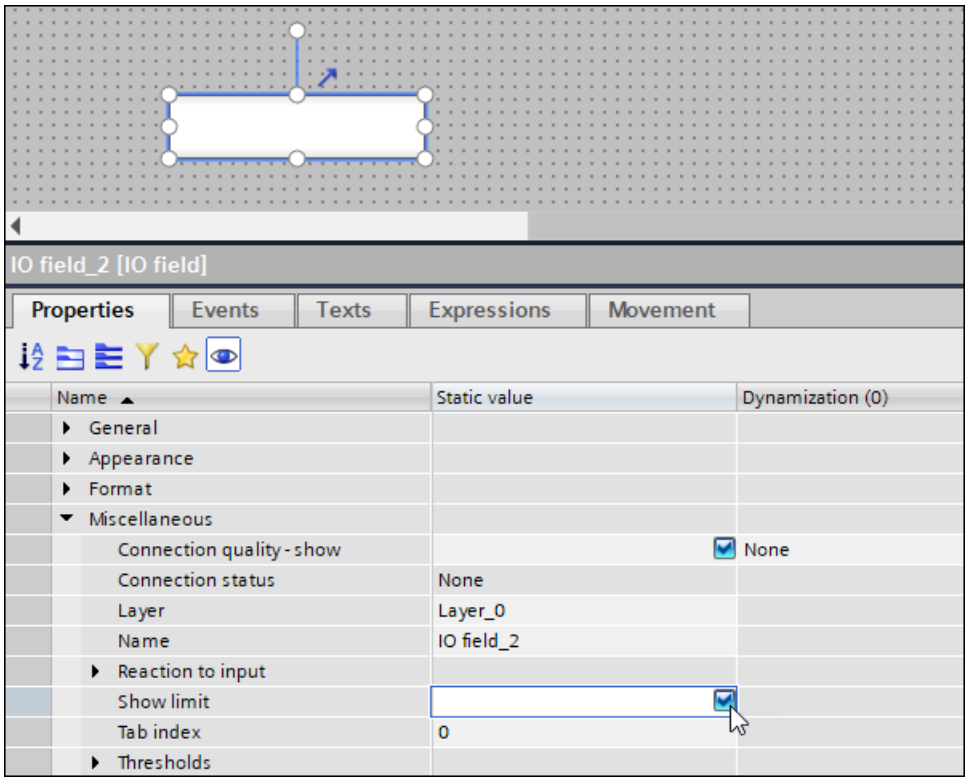


The limits of tags are displayed according to your choice.

Enabling display of limits locally

To enable the display of tag limits for each I/O field individually, follow these steps:

1. Select or clear the check box in the Inspector window under "Properties > Miscellaneous > Show limit".



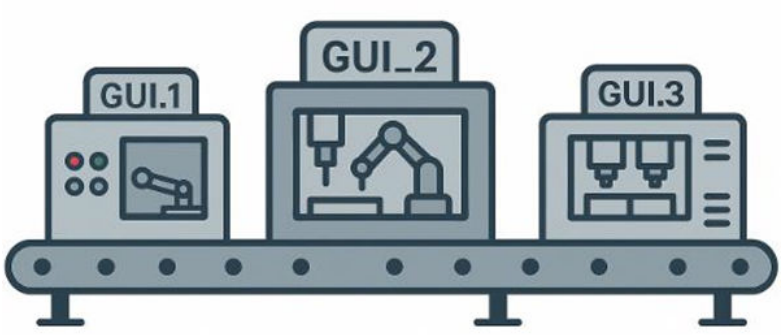
Note: The individual settings cannot override the central enabling or disabling.

3.3.2.5 Configure exclusive GUI operator control enable

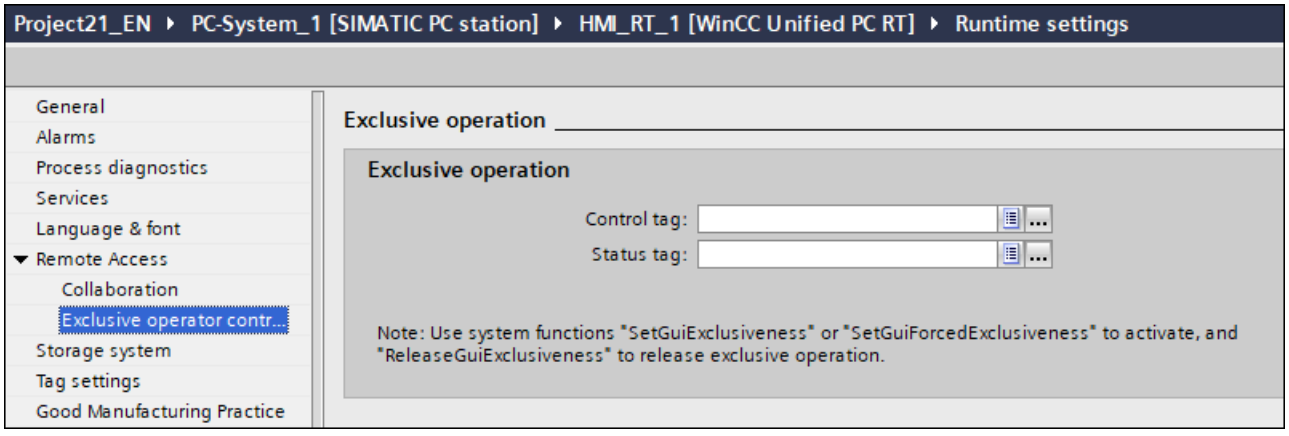
Introduction

The "Exclusive operator control enable" function allows only one operator to operate the machine's Runtime GUI at a time.

With Panel and Unified PC, the function prevents conflicts when several operator stations attempt to access the same machine. The function fulfills the requirements of the Machinery Directive § 197 "More than one control position".



As long as exclusive operator control is active at an operator station, e.g. GUI.1 (Graphical User Interface), all other operator stations are blocked for operation. You configure the buttons for exclusive operator control enable on each user interface.



Tags for exclusive operator control enable

You configure the exclusive operator control enable via the "Control tag" and "Status tag" tags in the Runtime settings of the device.

- You configure the control tag to synchronize the exclusive operator control enable across several clients.
- The status tag contains information about the client that has exclusive access rights.

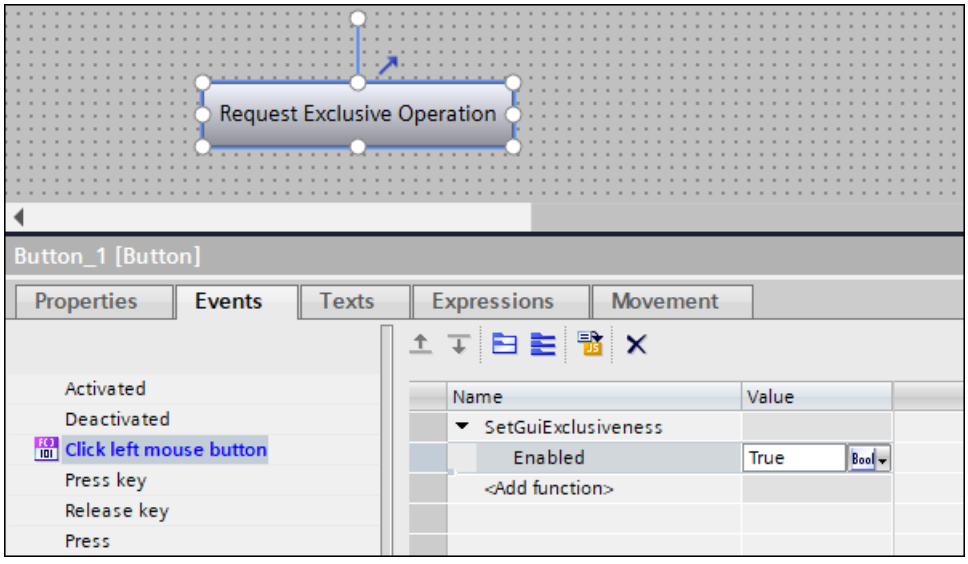
If switching on/off of exclusive operator control enable or the assumption of exclusive operator control is to be audited, you can configure the control tag and the status tag as GMP-relevant.

Configure exclusive operator control enable

To configure the exclusive operator control enable, follow these steps:

1. Click on the Runtime settings of the device in the project tree.
2. Select "Remote access > Exclusive operator control enable".

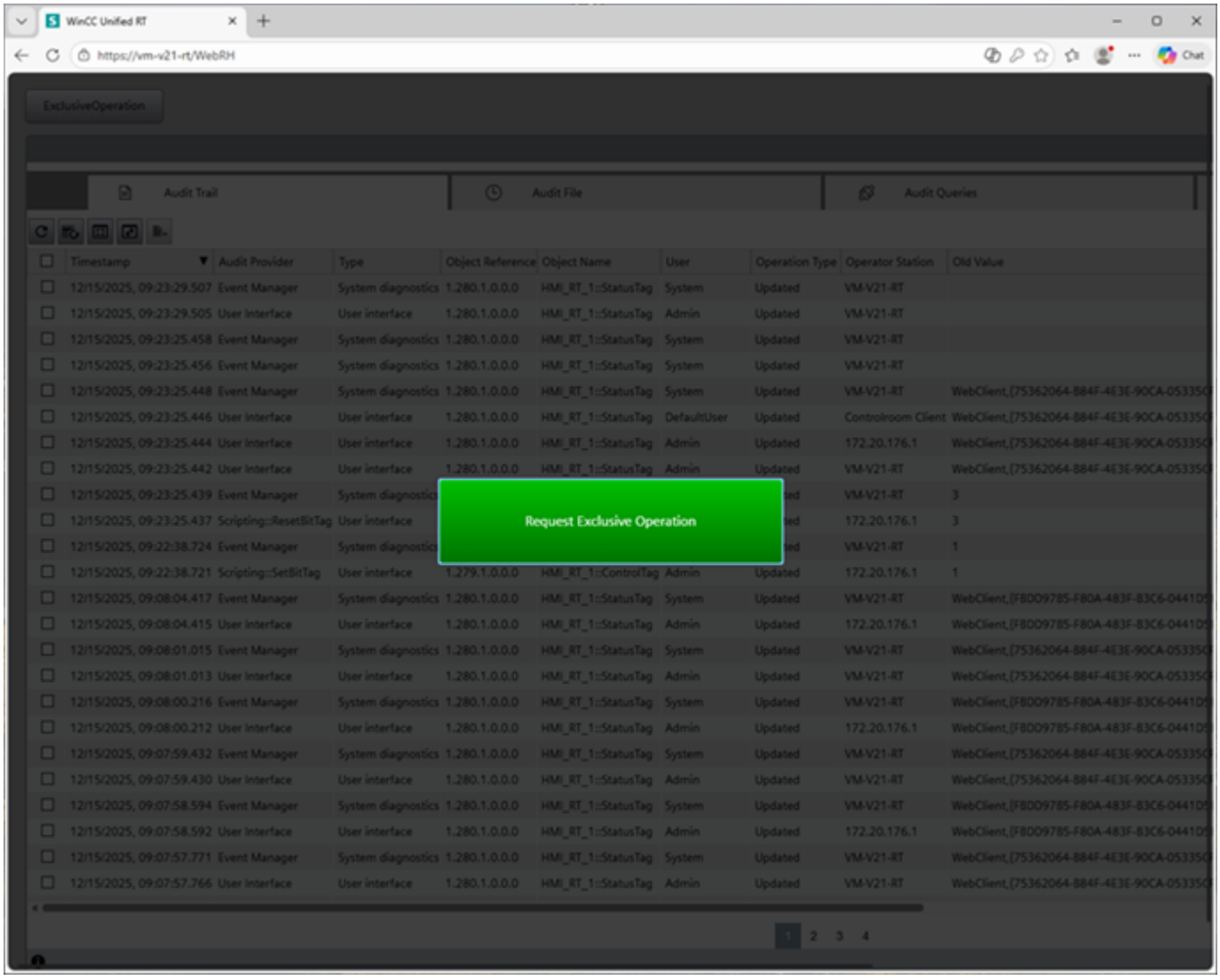
3. Configure the tags:
   - Control tag of the data types DInt, LInt, UDInt, ULInt, DWord or LWord.
   - Status tag of data type String or WString.
4. Configure the buttons for activating and releasing exclusive operator control on the screen.
5. Configure buttons for the system functions:
   - Use the system functions "SetGuiExclusiveness" or "SetGuiForcedExclusiveness" to activate exclusive operator control.
     In forced mode, exclusive operator control is protected against unwanted manipulation.
   - To release exclusive operator control, use the system function "ReleaseGuiExclusiveness".



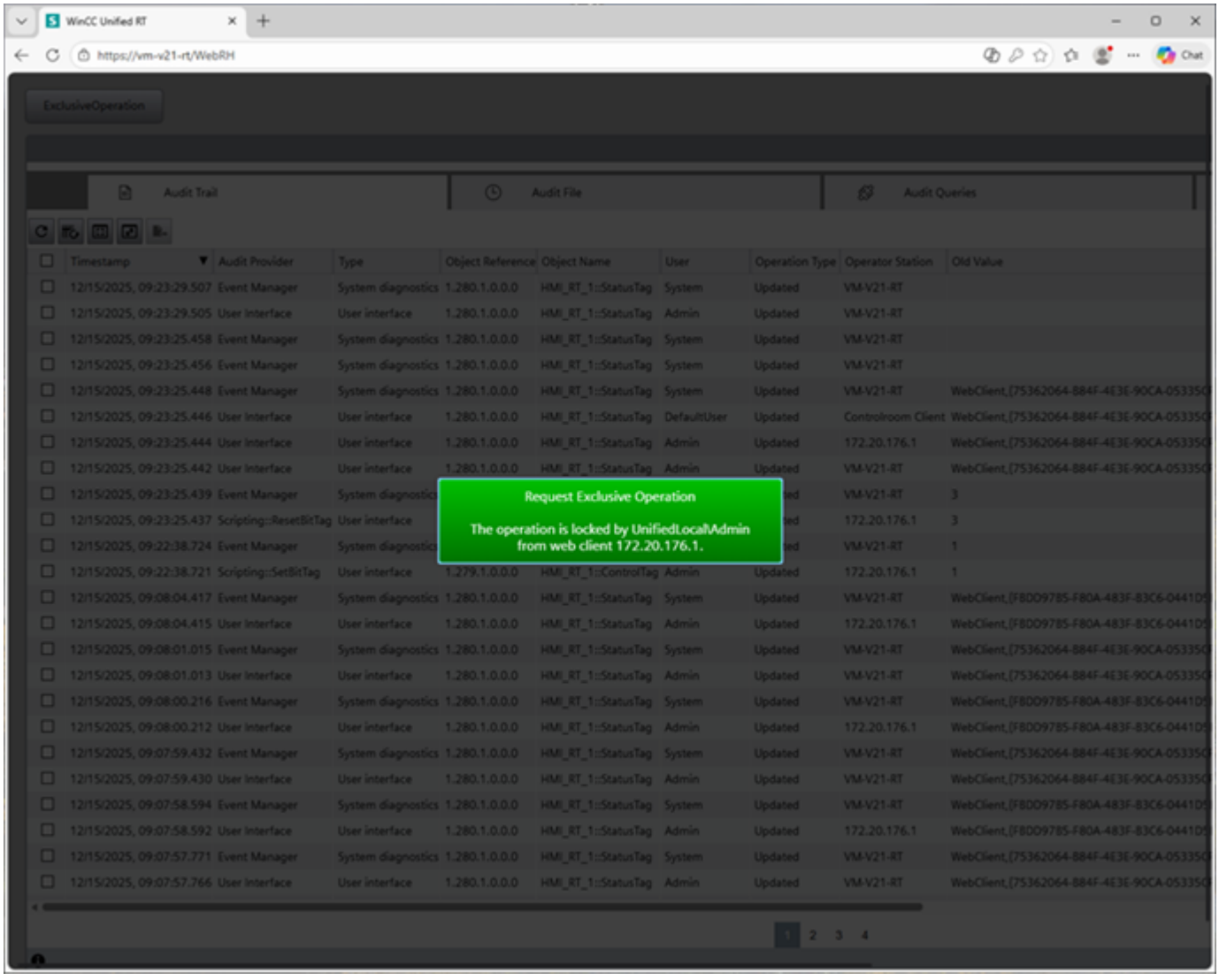
Behavior in Runtime

In Runtime, the following buttons are displayed to the operators after activating the exclusive operator control enable:

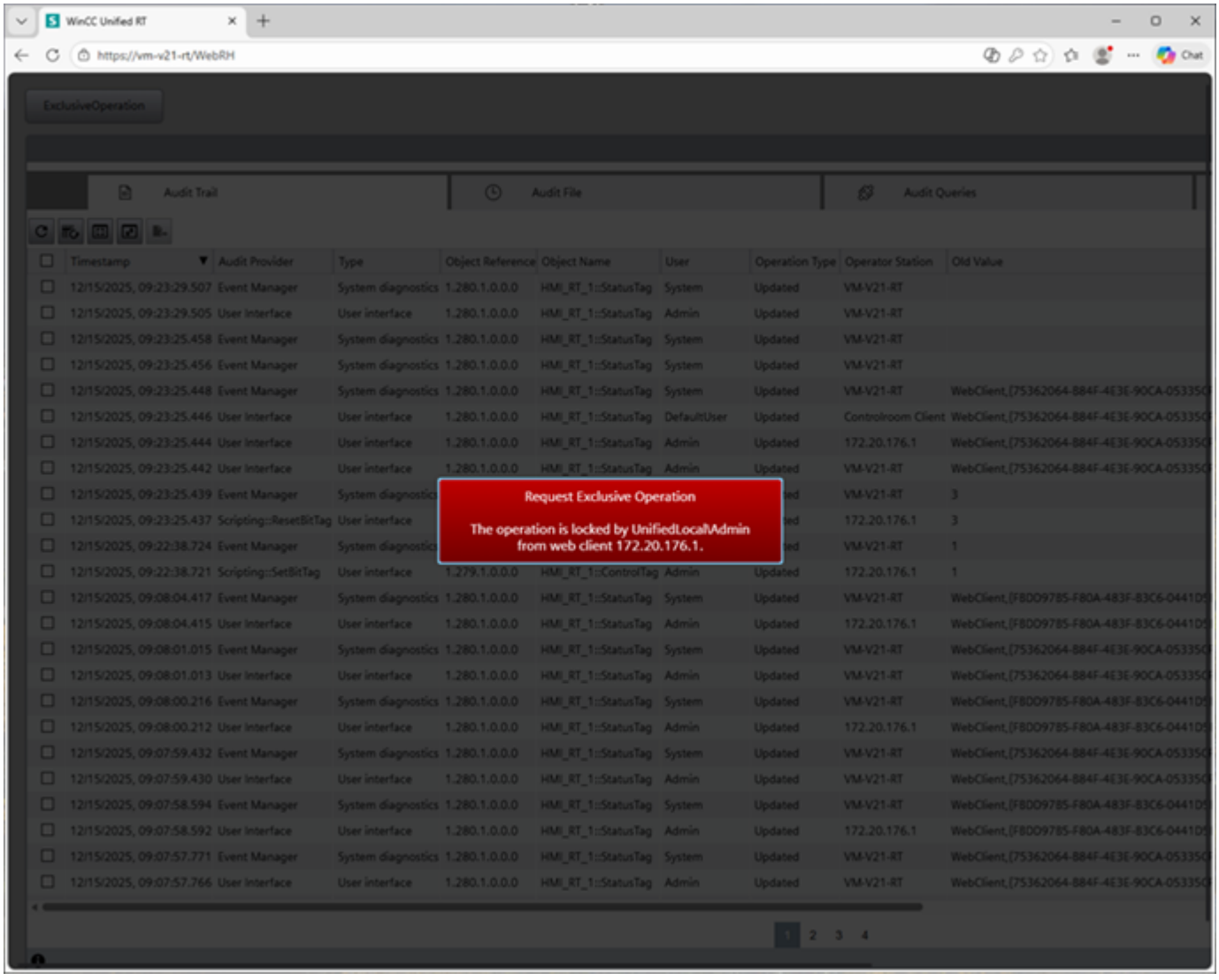
- A green button allows you to assume exclusive operator control.



- If an operator assumes exclusive operator control on a user interface, the green button is no longer displayed on this user interface. On the other GUI operator stations, the button is displayed in green and with the user name and IP address of the active GUI operator station. It is possible to assume exclusive operator control.



- If the "SetGuiForcedExclusiveness" system function has been configured for the button and the button has been activated, the button is displayed in red on all other GUI operator stations. It is not possible to assume exclusive operator control.



Note that an error message is displayed in Runtime if:

- One of the functions is called and the control and status tags are not defined.

3.3.2.6 System diagnostics control with script diagnostics functions

Introduction

The improved system diagnostics control in WinCC Unified Runtime allows you to monitor the execution of scripts. This provides an immediate analysis of script errors, warnings and performance problems without the need for special preparation or debugging tools. This provides comprehensive and integrated script diagnostics.

The new features are in effect as of device version V21 Update 1.

Note

Runtime performance

Activating script diagnostics has an impact on Runtime performance. It is recommended disable script diagnostics in productive operation.

Note

Runtime collaboration and redundancy

Script diagnostics is a local function. Runtime collaboration and redundancy are not supported.

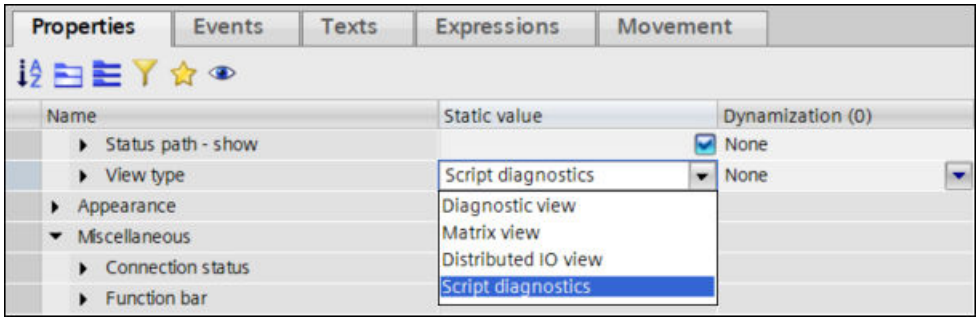
Requirement

1. The "System diagnostics control" object is inserted in the screen.
2. Script diagnostics must be switched on in the Runtime settings. For Unified PC via Runtime Manager, for Unified Panel via Control Panel.
   There are three script diagnostic profiles for this purpose:
   - Off: Script diagnostics is disabled. No messages are displayed in the script diagnostics control.
   - Critical: Messages about script errors and performance are displayed.
   - Full: User-defined traces are also displayed.

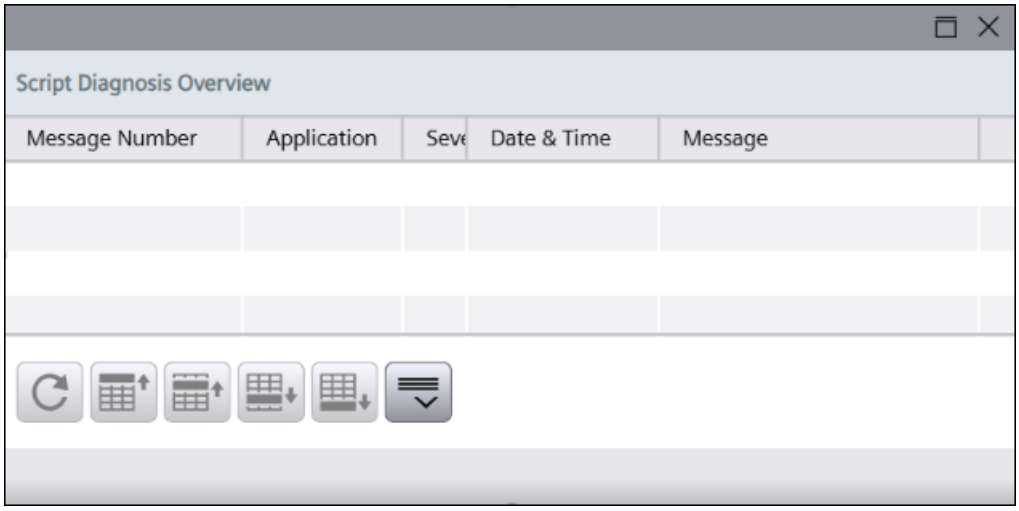
   The default setting is "Off". You can change this setting at any time without restarting Runtime.

Procedure

In the Inspector window under "Properties > General > View type", select the option "Script diagnostics control".



The script diagnostics control opens.



Settings

In the Engineering System, you can customize the properties for the script diagnostics control under "Properties > General", in particular:

- "Script diagnostics control": Defines various properties for the script diagnostics control, such as colors, rows, columns, etc.
- "Information bar": Specifies the representation of the information bar. It shows whether script diagnostics is enabled.
- "Toolbar": Specifies the buttons of the system diagnostics control.

Button		Function
	Reload	Updates the view of the diagnostic event.
	First line	Selects the first of the pending diagnostic events. The visible area of the view is moved.
	Previous line	Selects the previous diagnostic event, starting from the currently selected diagnostics event. The visible area of the view is moved.
	Next line	Selects the next diagnostic event, starting from the currently selected diagnostics event. The visible area of the view is moved.
	Last line	Selects the last of the pending diagnostic events. The visible area of the view is moved.
	Split view	Enables/disables the detail view. In the detailed view, you can see further information on a selected message. In this way, you can investigate the triggering script and the exact cause of the error.

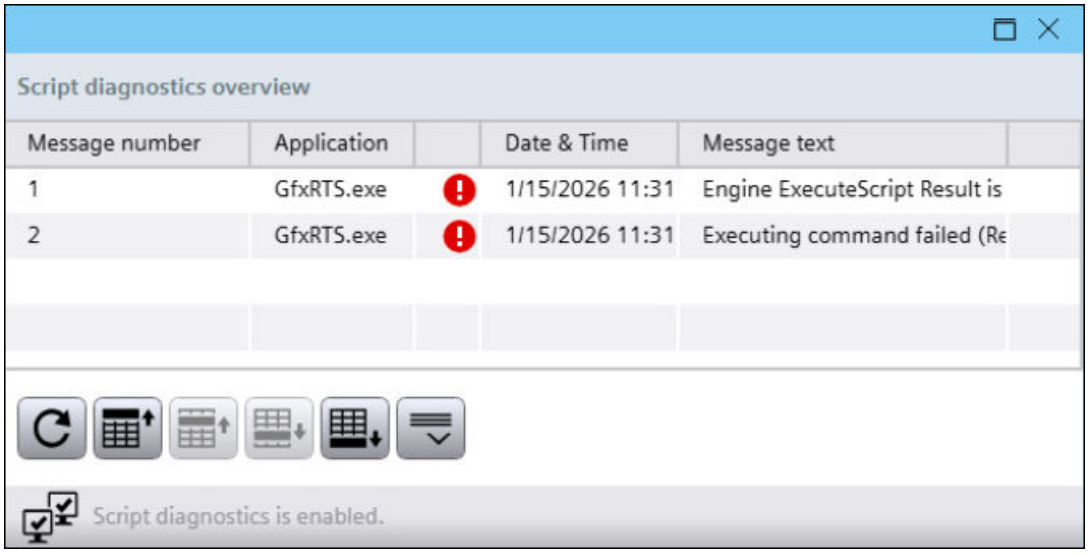
Export script diagnostics

To export the diagnostic data of the active project to a CSV file, use the system function "ExportScriptDiagnosis".

Result

The script diagnostics control is open in the screen and displays script-related messages in Runtime.

The display contains a maximum of 200 entries. If this number is exceeded, the oldest entry is overwritten.



3.3.2.7 System alarms Runtime

Email service

The following system alarms may occur when using the "Email service" functionality:

ID	Alarm text	Effect/causes	Solution
538283015	EmailDeliveryFailed	The email delivery has failed. The alarm can indicate a variety of causes that can occur on the user side. In the second part of the message, the detailed error is displayed in curly brackets. • Internal runtime errors are named, e.g. incorrectly formatted email address. • External error: If the SMTP server reports an error, this original error message is forwarded to the user unchanged.	Check the SMTP configuration.
538283016	EmailServiceNotStarted	The email service could not be started.	Enable reporting to start the email service.
538283017	ReportingConfigurationInconsistent	The deletion of reporting objects was rejected. Deleting objects can lead to an invalid configuration.	Remove the use of the specified objects and restart the download.

Storage capacity

The following alarms refer to the free disk space capacity, whereby "DiskSpaceWarning" is triggered by default at a limit of 90% and "DiskSpaceAlarm" at a limit of 95%.

ID	Message text		
536870949	DiskSpaceWarning	This alarm indicates that the configured limit for free space on the external storage medium has been exceeded. By default, the alarm is triggered at a limit of 90%.	Delete the data that is not required. Expand the external storage medium.
536870950	DiskSpaceAlarm	This alarm warns that the free memory space on the external storage medium is no longer sufficient. By default, the alarm is triggered at a limit of 95%.	Delete the data that is not required. Expand the external storage medium.

3.3.2.8 Configuring user management with domains

Configure separate user management with domains

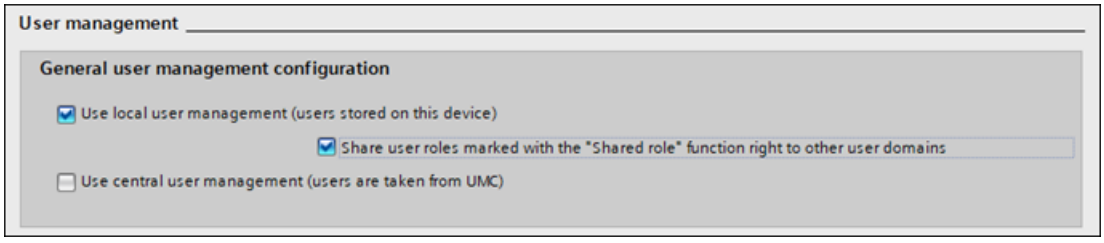
As of V21 Update 1, WinCC Unified offers the option of implementing structured user management for Unified devices.

This enables definition of user roles and users with different visibilities and authorizations – particularly for separation of the OEM (machine supplier) and system user from the end user.

"User roles, ... share with other domains" option

You can use the user roles in several user domains if the specific settings are enabled in the Runtime settings of the device:

- "Local user management" must be selected.
- The option "Share user roles marked with the "Shared role" function right to other user domains" must be selected.



Selecting this option creates the OEM-specific domain:

- This domain contains OEM users that are not visible to the system user.
- Roles without the "Shared role" function right are intended exclusively for the OEM.
- Access to special functions such as maintenance, diagnostics or protected settings can be configured for these users.
- Roles with the "Shared role" function right are visible and available for use in all domains and can be used for the operator.

Additional system user-specific domains can be created in the Runtime Manager or in the Control Panel:

- Domains for central user management
- Domain for local user management
- Domain for central user management + domain for emergency users

Only roles with the "Shared role" function right may be used in these domains. Typical use case: System user roles such as "Operator" or "Maintenance tech".
Each domain has at least one domain administrator who can see and manage the users in the domain.

Definitions

WinCC Unified provides you with six different use cases for structured user management. You will find a general description in this section. The description of the individual use cases and their configuration can be found in the following sections.

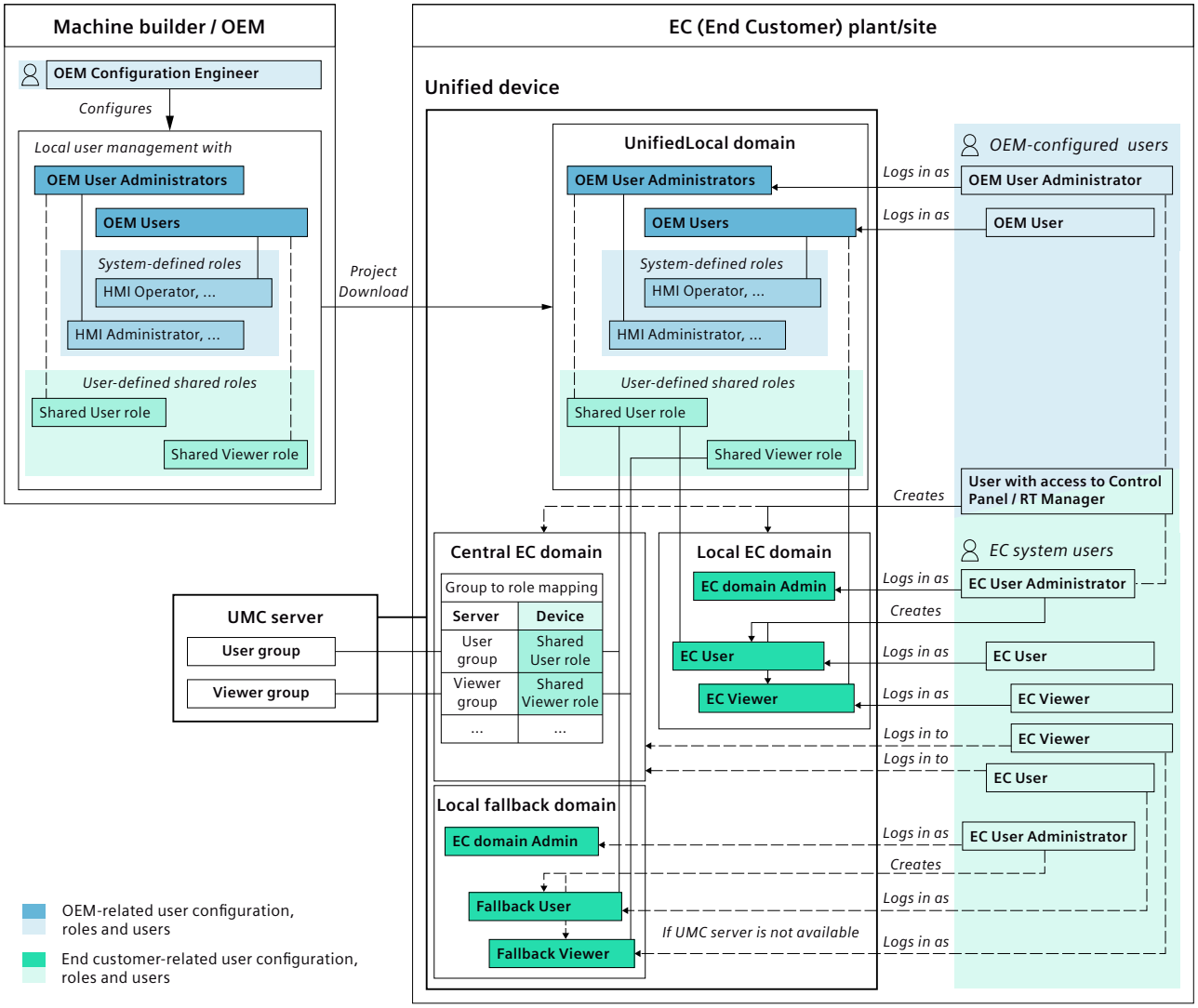
Types of users

The following types of users are defined in the user management:

- Local users: Standard users in Runtime, locally managed.
- Central users: Standard users in Runtime, centrally managed.
- Fallback users: Locally stored users who are available in the event of an interruption in the connection to the central user management system.
- OEM, Original Equipment Manufacturer: Users of the machine manufacturer who may have more rights than the system users.
- System users: User administrator end users, machine operators at the end user site, or other end users.

Structure of the user management

The following example figure shows the basic structure and the possibilities of domain-based user management when an OEM domain is used. Two shared roles, "Shared User role" and "Shared Viewer role", are used in the example.



Functions of the OEM

The OEM (Original Equipment Manufacturer) has the following options:

1. Configure local user management in the Engineering System.
2. Enable the option "Share user roles marked with the "Shared role" function right to other user domains".
3. Create local OEM users.
4. Assign roles to OEM users.

5. Add new roles.
6. Assign the "Shared role" function right to the selected roles. These roles are then available to the end user.

Possible configurations

The following sections describes the individual use cases and their configuration:

1. Local user
2. Central user
3. Central user and fallback user
4. Local users and OEM
5. Central users and OEM
6. Central users, OEM and fallback users

Configurations 1-3 with local or central users are specified in the Engineering System.

Configurations 4-6 with local or central users and OEM are specified in the Engineering System and in SIMATIC Runtime Manager. In Runtime, the system user creates the users and assigns the roles with the "Shared role" function right to them.

Only users who are assigned to the "umcd_global_admin" group in the Computer management under "System > Local users and groups > Users" can create a domain in SIMATIC Runtime Manager.

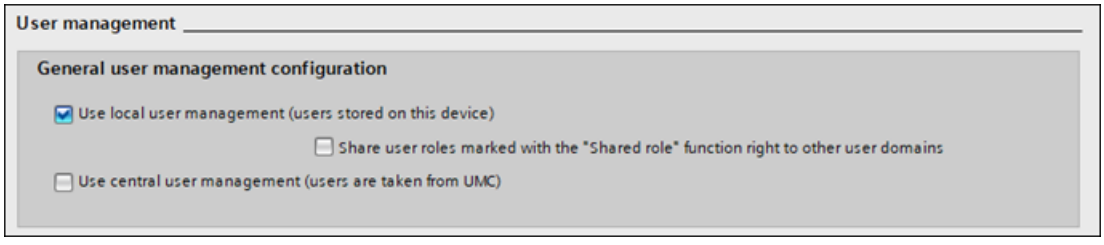
Configuration 1 - Local user

This section describes the following example scenario:

- The user configures the local user management for the user and plant in the Engineering System. A local domain is created.

Engineering System

The users are configured under "Security settings > Users and roles".



The following selection is made for a complete download:

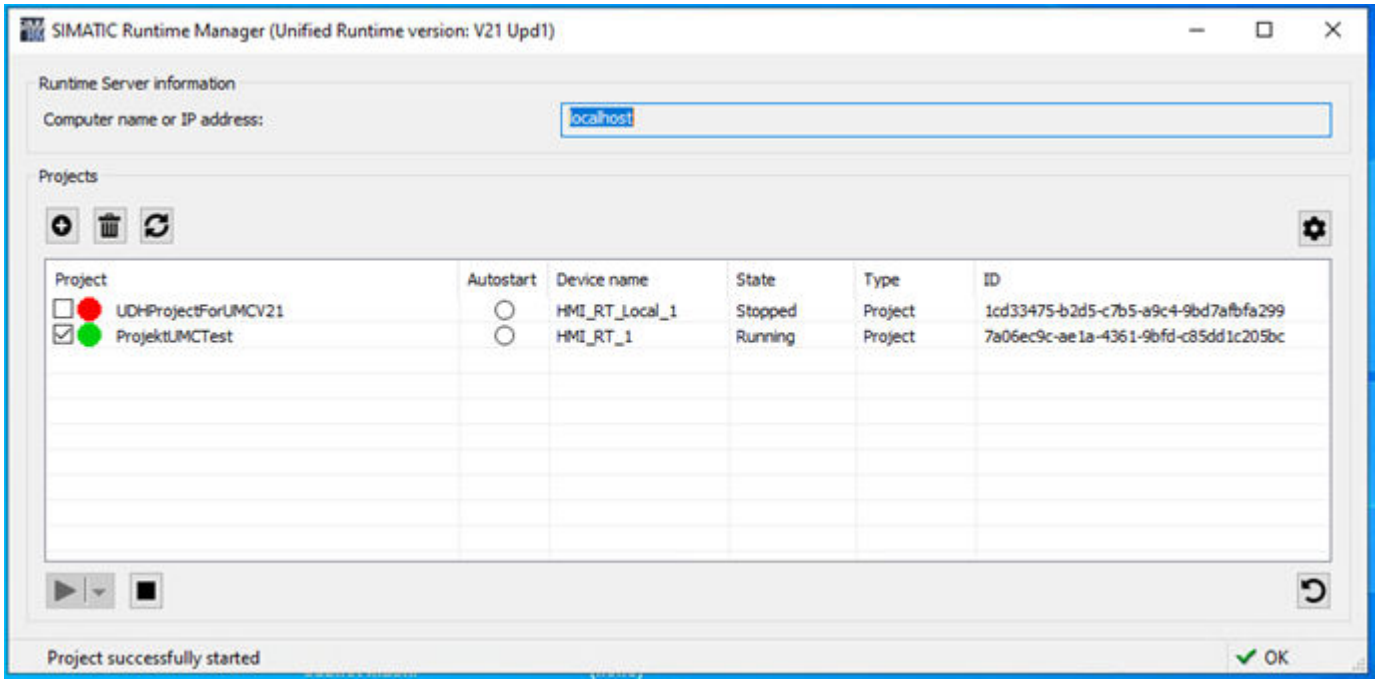
- Enable the "Start Runtime" option.
- Do not enable the "Keep current user administration data in runtime" option. The user management data is overwritten.

Runtime is started after download is complete.

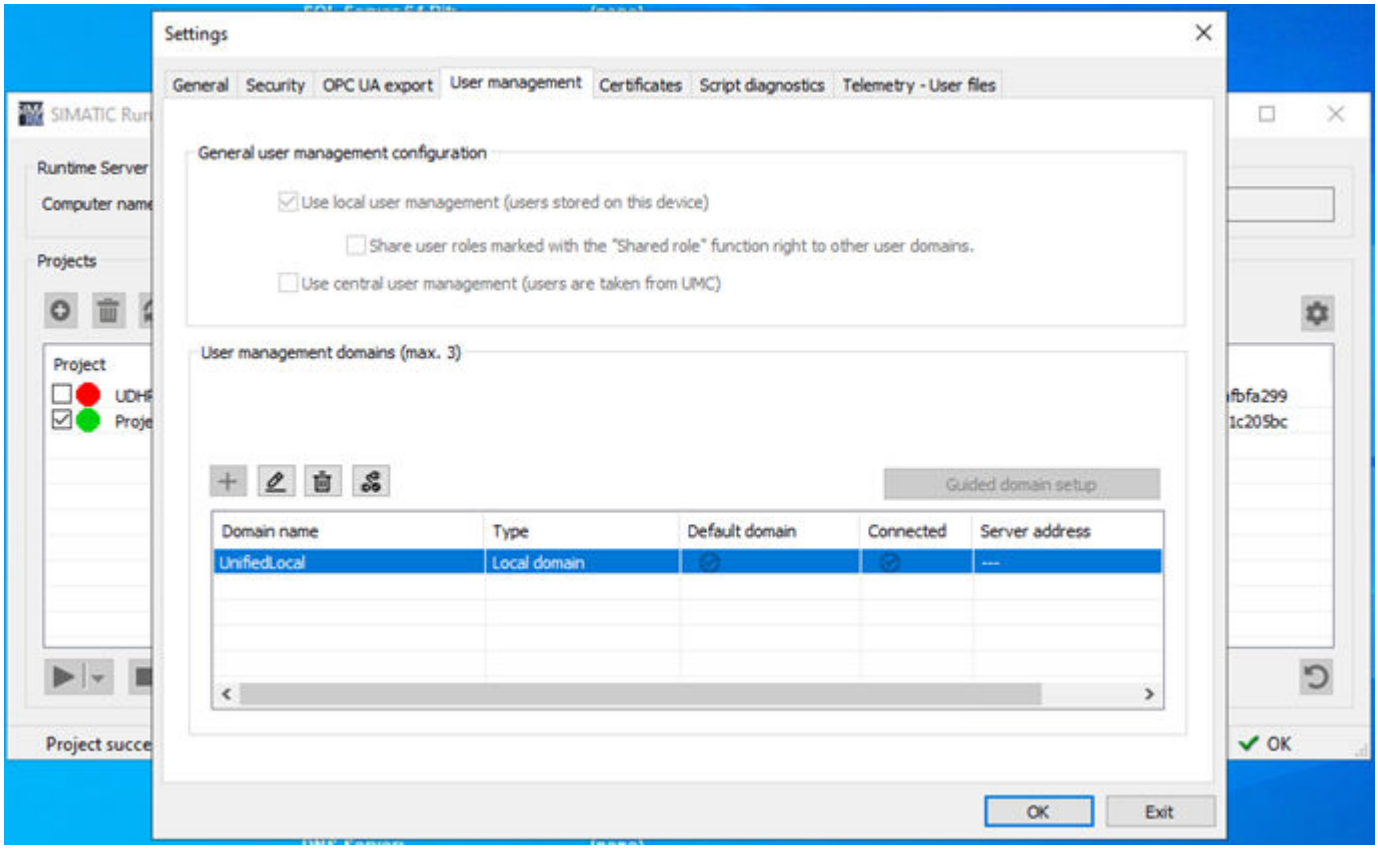
Options in SIMATIC Runtime Manager

The following procedure is a configuration example.

The project is visible in Runtime Manager.



The local domain is visible under "Settings" in the "User management" tab under Domain names.



The "General configuration of user management" dialog is read-only and shows the configuration that was selected in the Engineering System.

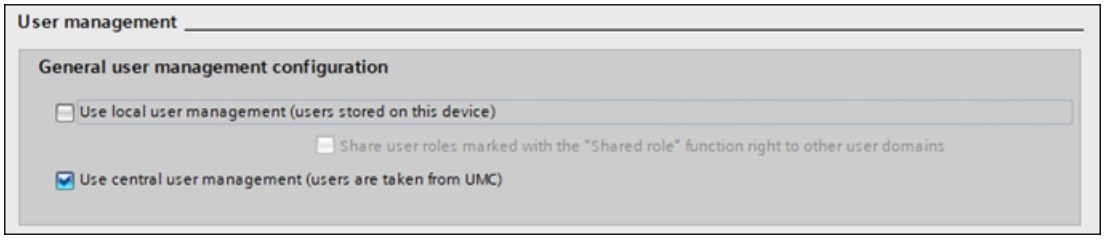
You cannot delete the domain.

You cannot add another domain.

Configuration 2 - Central user

This section describes the following example scenario:

1. The user configures the central user management in the Engineering System. All users have been configured in a central UMC server or imported from an Active Directory.



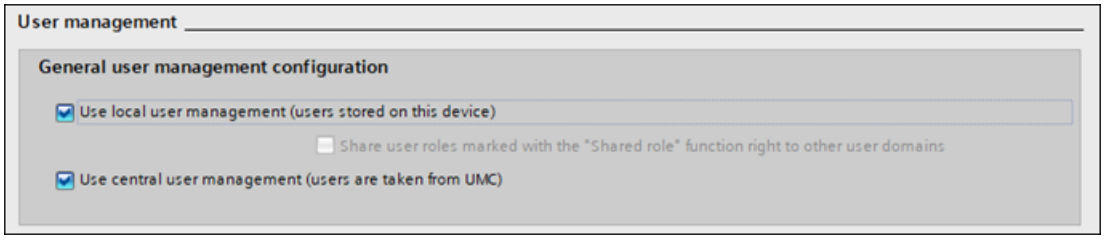
2. The following selection is made for a complete download:
   - Enable the "Start Runtime" option.
   - Do not enable the "Keep current user administration data in runtime" option. The user management data is overwritten.

Runtime is started after download is complete.

Configuration 3 - Central users and fallback users

This section describes the following example scenario:

1. The user configures the central user management in the Engineering System.
2. In addition, the user configures one or more local users as fallback users in case the connection to the central UMC server is interrupted. A locally created fallback user can be used to ensure access to WinCC Unified Runtime during an interruption. The fallback user allows the user to log in and continue working.



3. The following selection is made for a complete download:
   - Enable the "Start Runtime" option.
   - Do not enable the "Keep current user administration data in runtime" option. The user management data is overwritten.

Runtime is started after download is complete.

Note

Enter the domain name as a prefix before the user name in the following cases:

- When logging on automatically in SIMATIC Runtime Manager under "Settings > General > Automatic logon".
- If you use the "ChangeUser" system function, the domain name must be placed in front of the user name separated by "\" if you want to log in with a user who does not belong to the default domain.
- For authentication in the following applications: OPC, GraphQL or My WinCC Unified. If the user belongs to the default domain, it is not necessary to specify the domain name.

Configuration 4 - Local users and OEM

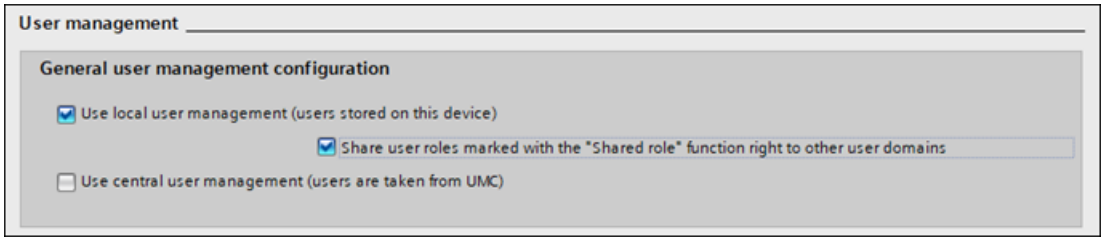
This section describes the following example scenario:

- The OEM configures the local user management and its users in the Engineering System. A local OEM domain is created.
- The end customer user administrator creates an additional local end customer domain on the PC in the SIMATIC Runtime Manager. The end customer user administrator configures their users in this domain.

The users at the end customer are local.

Configuring in the Engineering System

1. The OEM configures the local user management and its users in the Engineering System. A local OEM domain is created.
2. The OEM enables the option "Share user roles marked with the "Shared role" function right to other user domains".



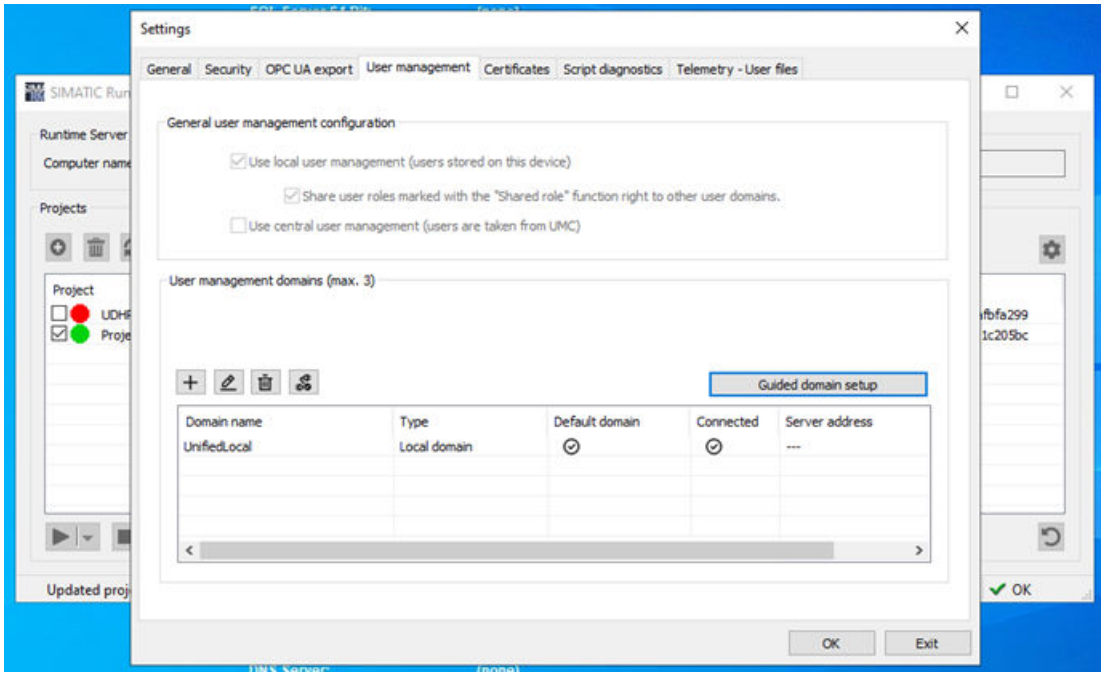
3. The OEM configures the users under "Security settings > Users and roles".
4. The OEM assigns the "Shared role" function right to the roles that are available to the system user. Additional roles with the "Shared role" function right can be created and are available in Runtime.
   These roles can be assigned to the users of the domain newly configured in Runtime. These roles give users function rights in the end customer domain.
5. The following selection is made for a complete download:
   - Enable the "Start Runtime" option.
   - Do not enable the "Keep current user administration data in runtime" option.
     The user management data is overwritten.

Runtime is started after download is complete.

Options in the SIMATIC Runtime Manager

The read-only section "General configuration of user management" is visible in the Runtime Manager under "Settings > User management". The dialog shows the configuration that was selected in the Engineering System.

The following procedure is a configuration example.



The "Add new domain", "Modify selected domain", "Delete selected domain", "Connect UMC server" and "Guided domain setup" buttons are activated.

Note: The domain created in the Engineering System cannot be deleted in Runtime Manager. Only domains created here can be deleted in the Runtime Manager.

To add a new domain, the end customer user administrator has the following options:

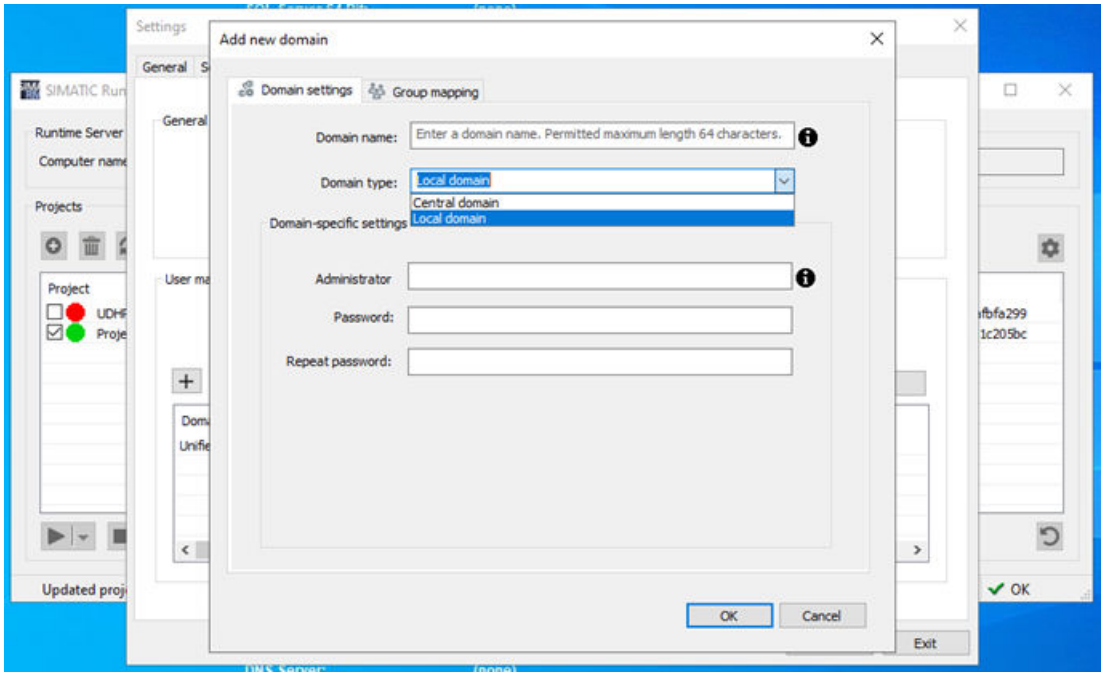
1. Via the "Add new domain" button with the "Plus" symbol.
2. Open "Guided domain setup": A wizard provides support when adding the domain.

Adding a new local domain via the button

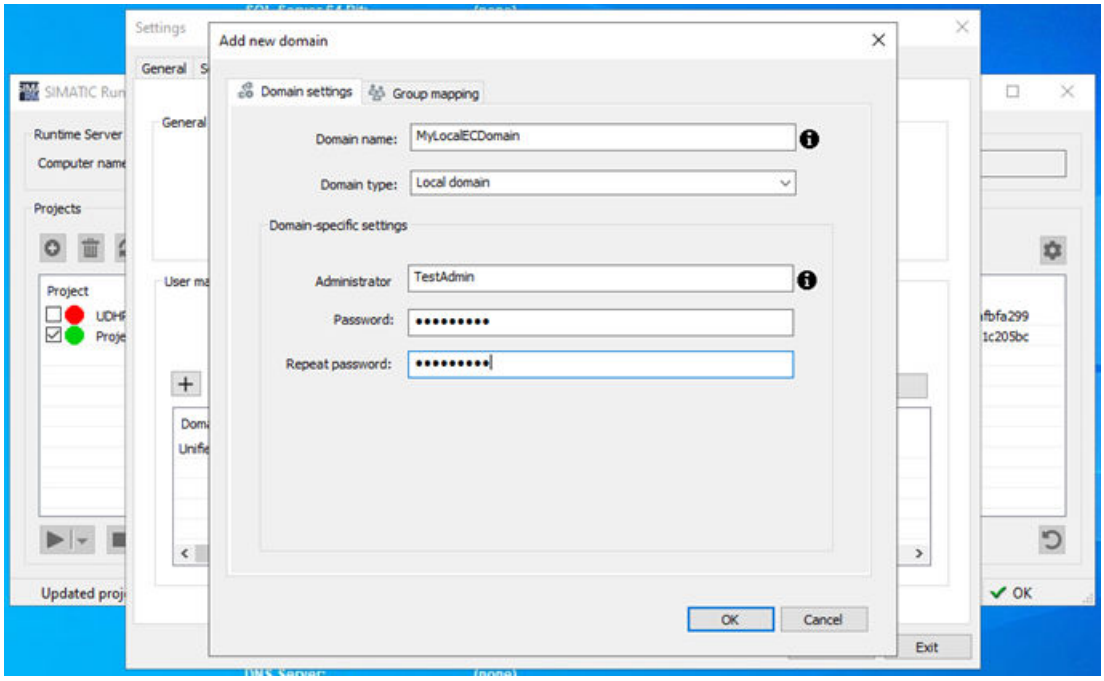
After you click on the "Add new domain" button with the "Plus" symbol, a dialog box is displayed.

To add a local domain, follow these steps:

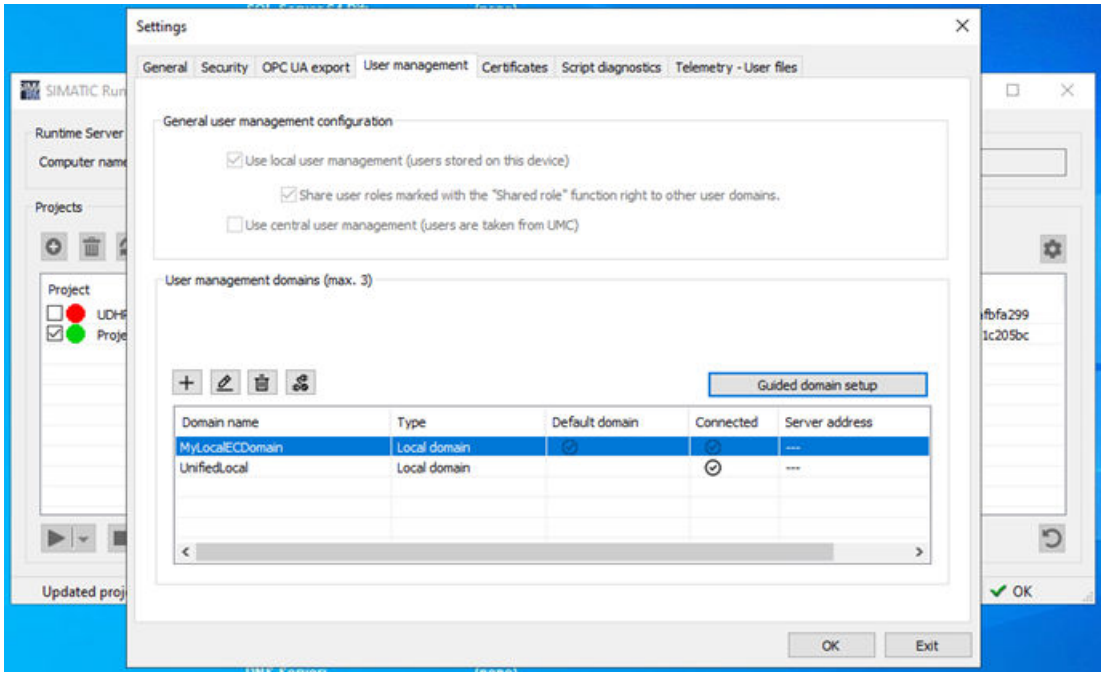
1. Select the local domain under "Domain type".



2. Enter a name under "Domain name", e.g. "MyLocalECDomain".
3. Create a user under "Administrator", e.g. "TestAdmin", who will create and manage the new users in this domain.
4. Enter the password.
5. Click "OK".



A new domain has been added. This end customer domain is defined as the default domain.

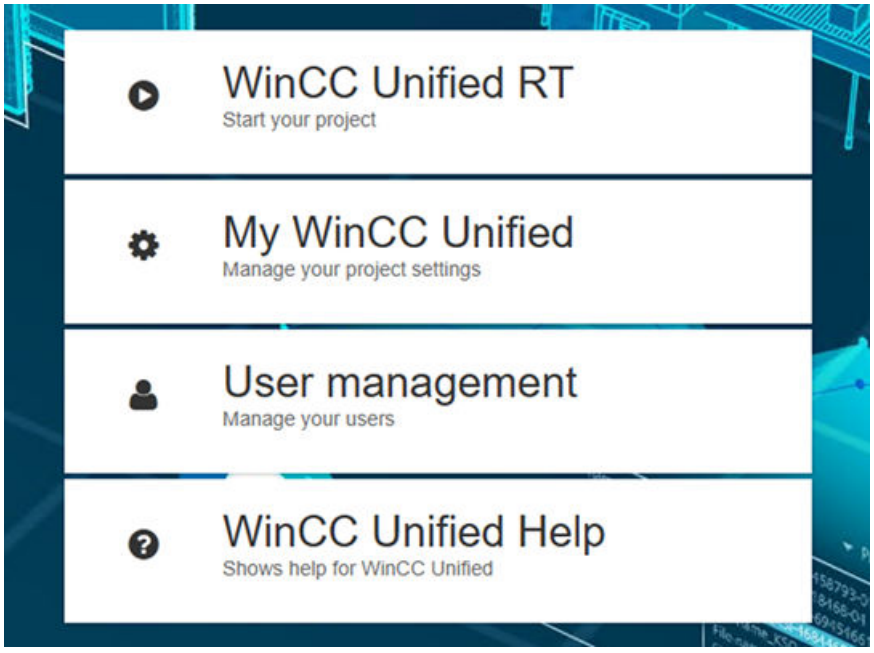


Configuring local users in Runtime

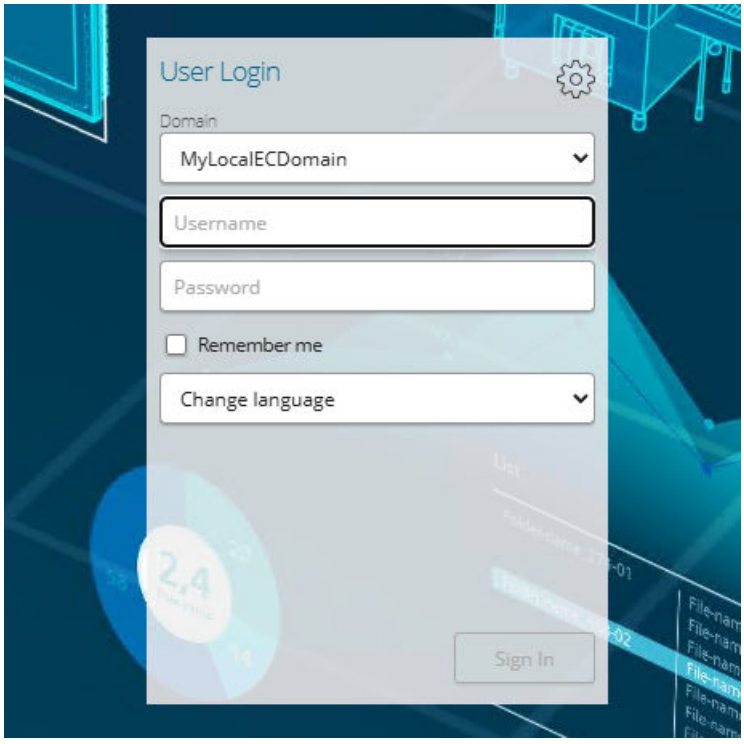
As the "TestAdmin" user, you create the new users and assign them the roles.

To create the users, follow these steps:

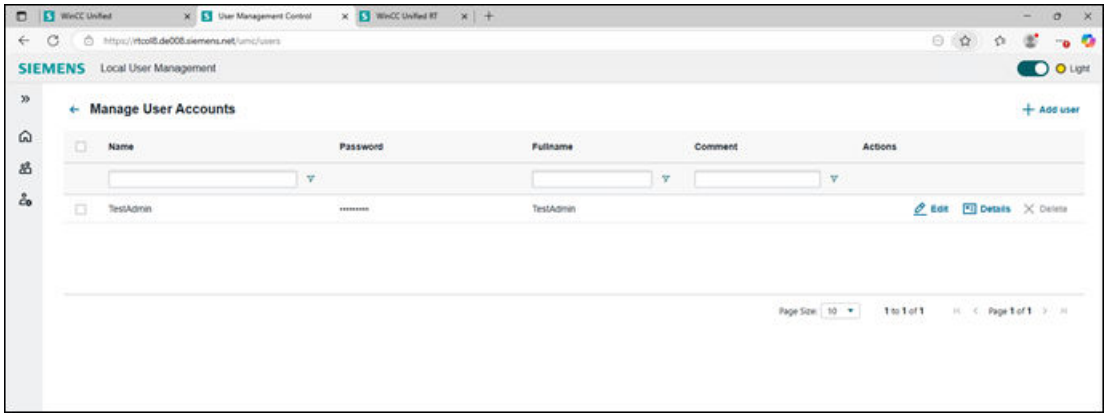
1. In the browser, enter the IP address of the Runtime PC "https://<PC-IP>" or the fully qualified domain name "https://<FQDN>".
   The start page of the Runtime is displayed.



2. Click the "User management" button. The "User Login" dialog is displayed.
   The local end customer domain is preset as the default domain in the dialog. To display the domain in which you have logged in, you can configure the "@UserDomain" system tag in the Engineering System, e.g. at the process value of an I/O field.

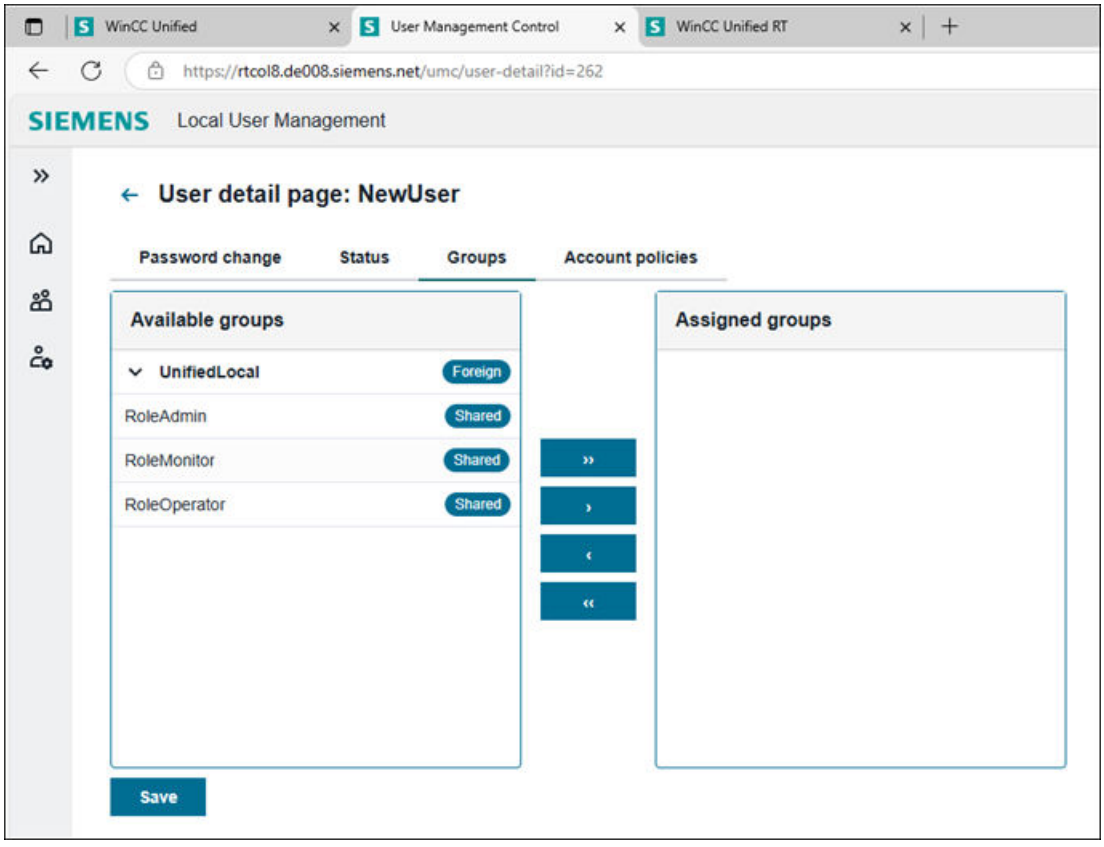


3. Enter the user name "TestAdmin" and password.
4. Select the language in which the user management is displayed. In this example, the interface remains in English.
5. Click "Sign In".
   The user management start page opens in Runtime.
6. Select the "Users" option in the menu.
7. Click the "Add user" button.
8. Create a new user.

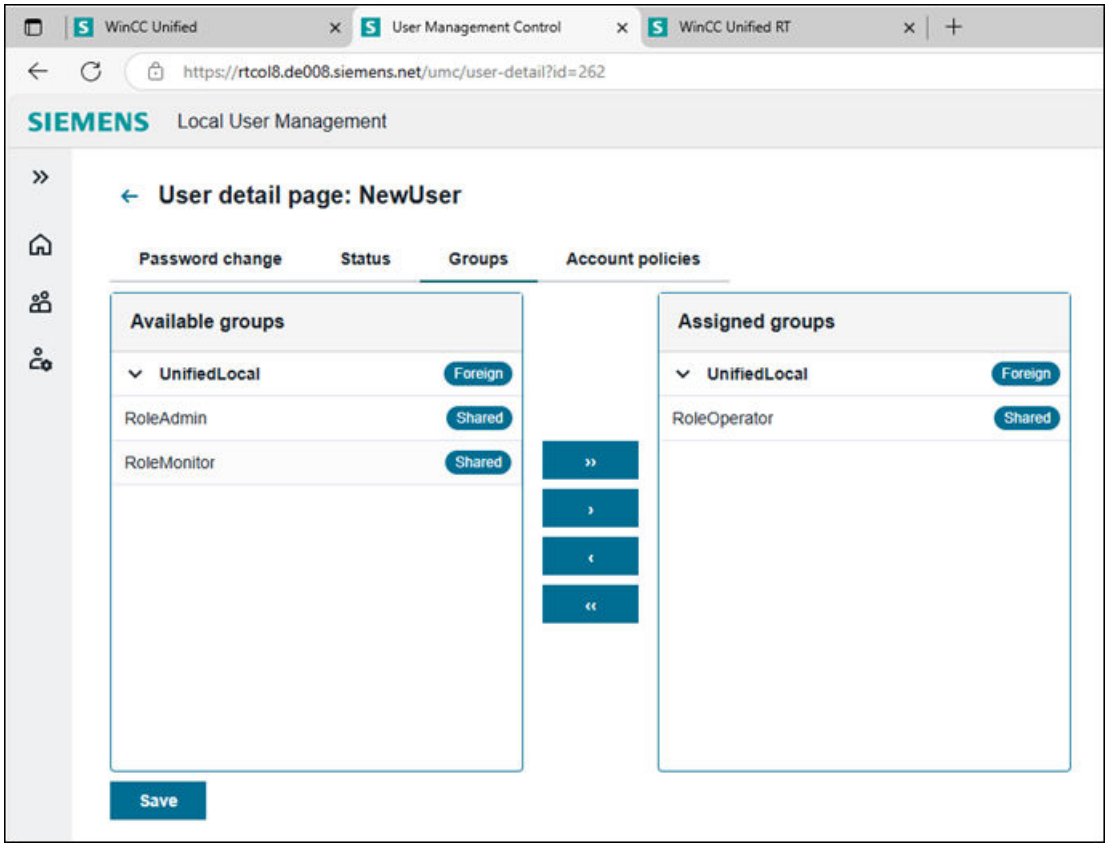


9. Click the "Details" button.

10. Select "Groups". The roles created in the Engineering System are displayed.
    Here, the user from the new domain can use the roles marked with the "Shared role" function right.



11. Assign one or more "Shared roles" to the new user. With the roles, the user has the authorizations that were configured in the Engineering System for the "Shared role".



Note

Enter the domain name as a prefix before the user name in the following cases:

- When logging on automatically in SIMATIC Runtime Manager under "Settings > General > Automatic logon".
- If you use the "ChangeUser" system function, the domain name must be placed in front of the user name separated by "\" if you want to log in with a user who does not belong to the default domain.
- For authentication in the following applications: OPC, GraphQL or My WinCC Unified. If the user belongs to the default domain, it is not necessary to specify the domain name.

Configuration 5 - Central users and OEM

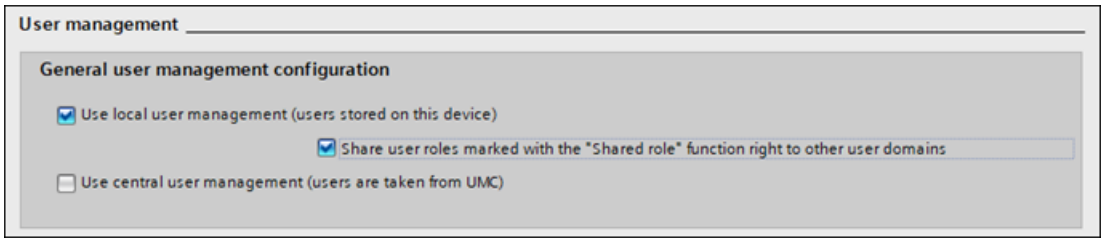
This section describes the following example scenario:

1. The OEM configures the local user management and its users in the Engineering System. A local OEM domain is created.
2. The end customer user administrator creates a central end customer domain on the PC in the SIMATIC Runtime Manager. The end customer user administrator configures their users on this domain.

The users at the end customer are central.

Configuring in the Engineering System

1. The OEM configures the local user management and its users in the Engineering System.
2. The OEM enables the option "Share user roles marked with the "Shared role" function right to other user domains".



3. The OEM assigns the "Shared role" function right to the roles that are available to the system user.
4. The following selection is made for a complete download:
   - Enable the "Start Runtime" option.
   - Do not enable the "Keep current user administration data in runtime" option. The user management data is overwritten.

Runtime is started after download is complete.

Options in the SIMATIC Runtime Manager

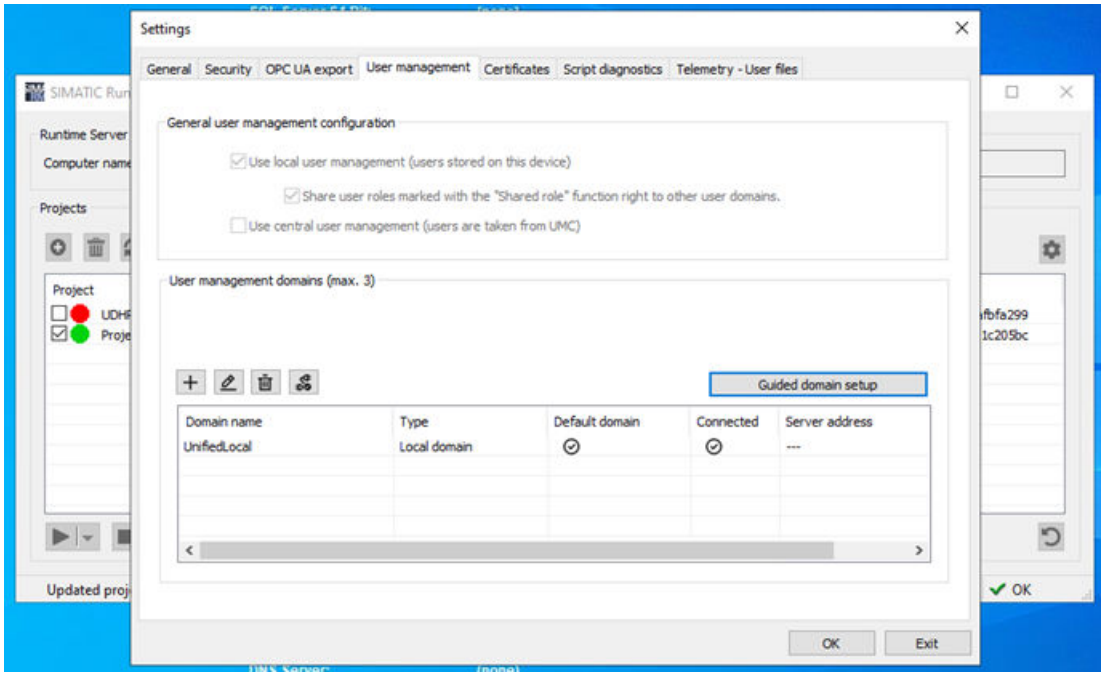
The following procedure is a configuration example.

The end customer user administrator creates a central domain on the PC in the Runtime Manager.

To create this domain, the end customer user administrator configures mapping between the central groups and the local roles to which the "Shared role" function right has been assigned.

The end customer user administrator configures their users in the central user management.

The read-only dialog "General configuration of user management" is visible in the Runtime Manager under "Settings > User management". The dialog shows the configuration that was selected in the Engineering System.



The "Add new domain", "Modify selected domain", "Delete selected domain", "Connect UMC server" and "Guided domain setup" buttons are activated.

Note: The domain created in the Engineering System cannot be deleted in Runtime Manager. Only domains created here can be deleted in Runtime Manager.

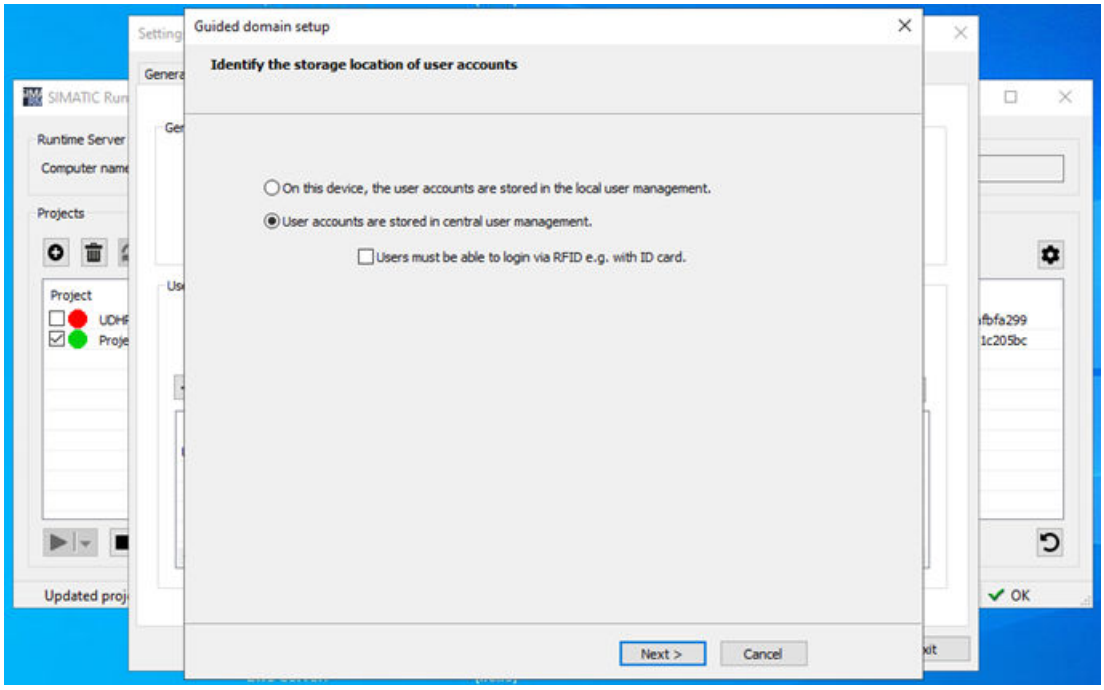
To add a new domain, the end customer user administrator has the following options:

1. Use the "Add new domain" button.
2. Open "Guided domain setup": A wizard provides support when adding the domain.

Add new central domain via "Guided domain setup"

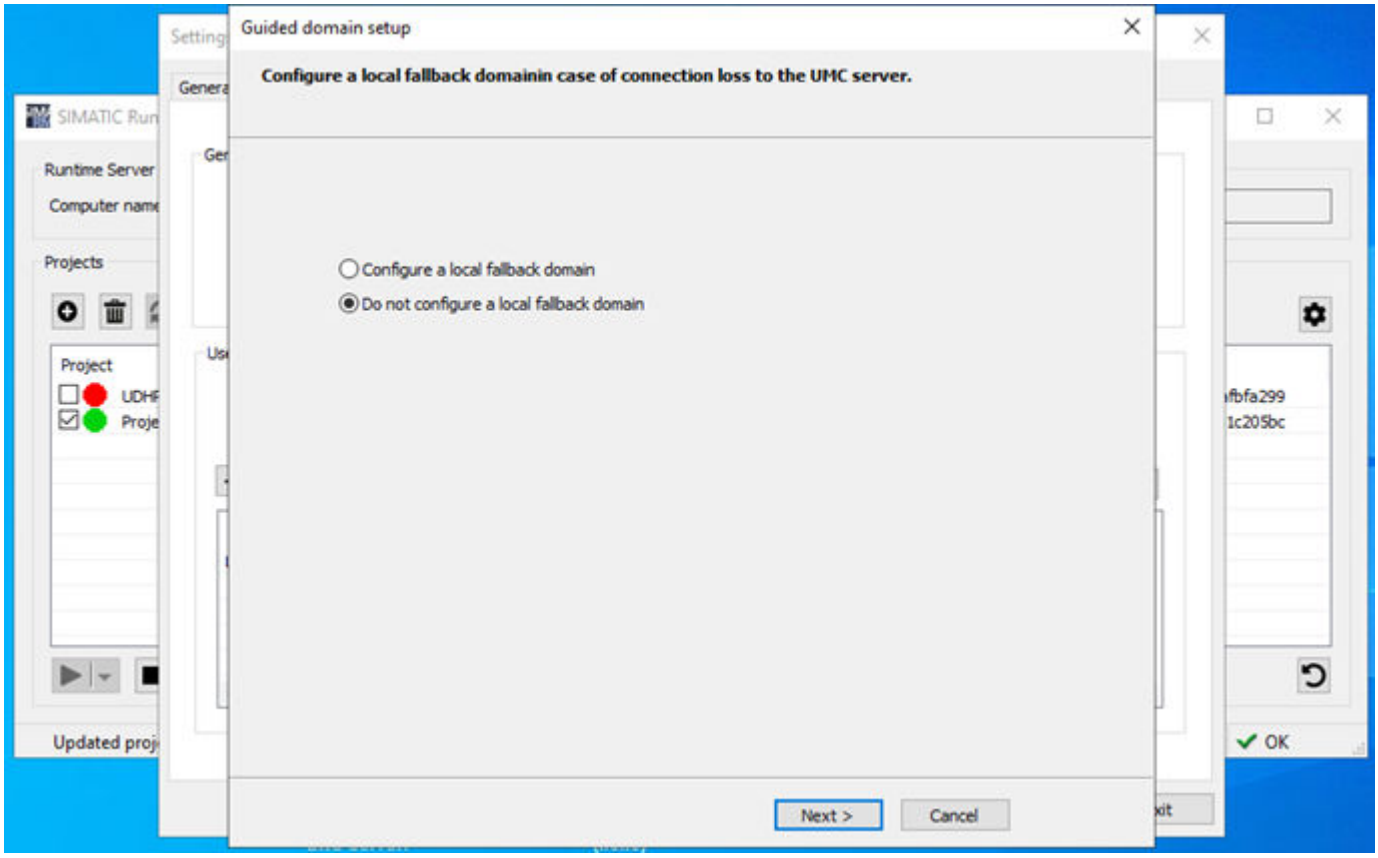
To add a central domain, follow these steps:

1. Click the "Guided domain setup" button.
   A dialog is displayed.
2. Select the option "User accounts are stored in central user management".
   The option "Users must be able to log in via RFID, e.g. with ID card" remains disabled.



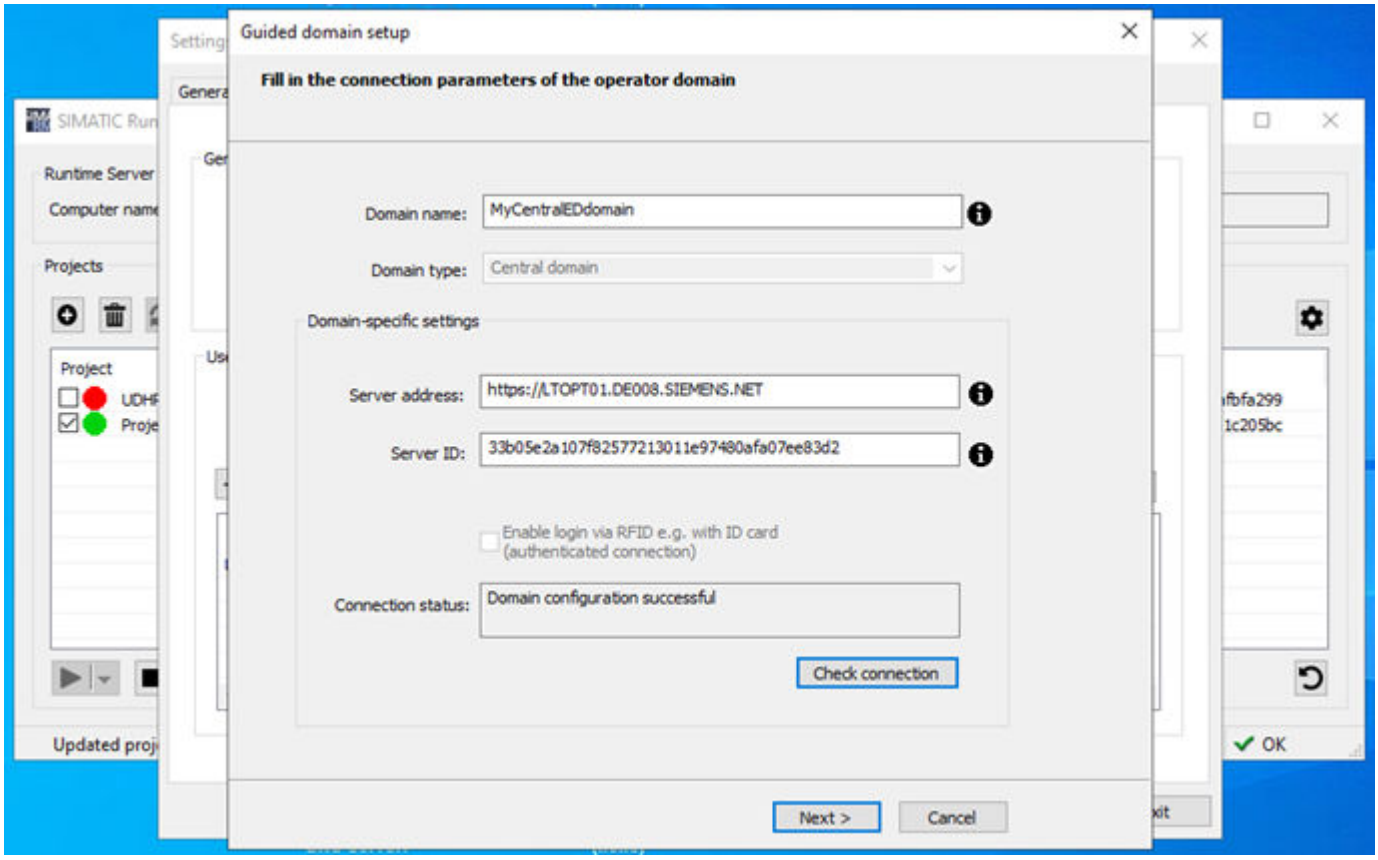
3. Click "Next".

4. Select "Do not configure a local fallback domain".



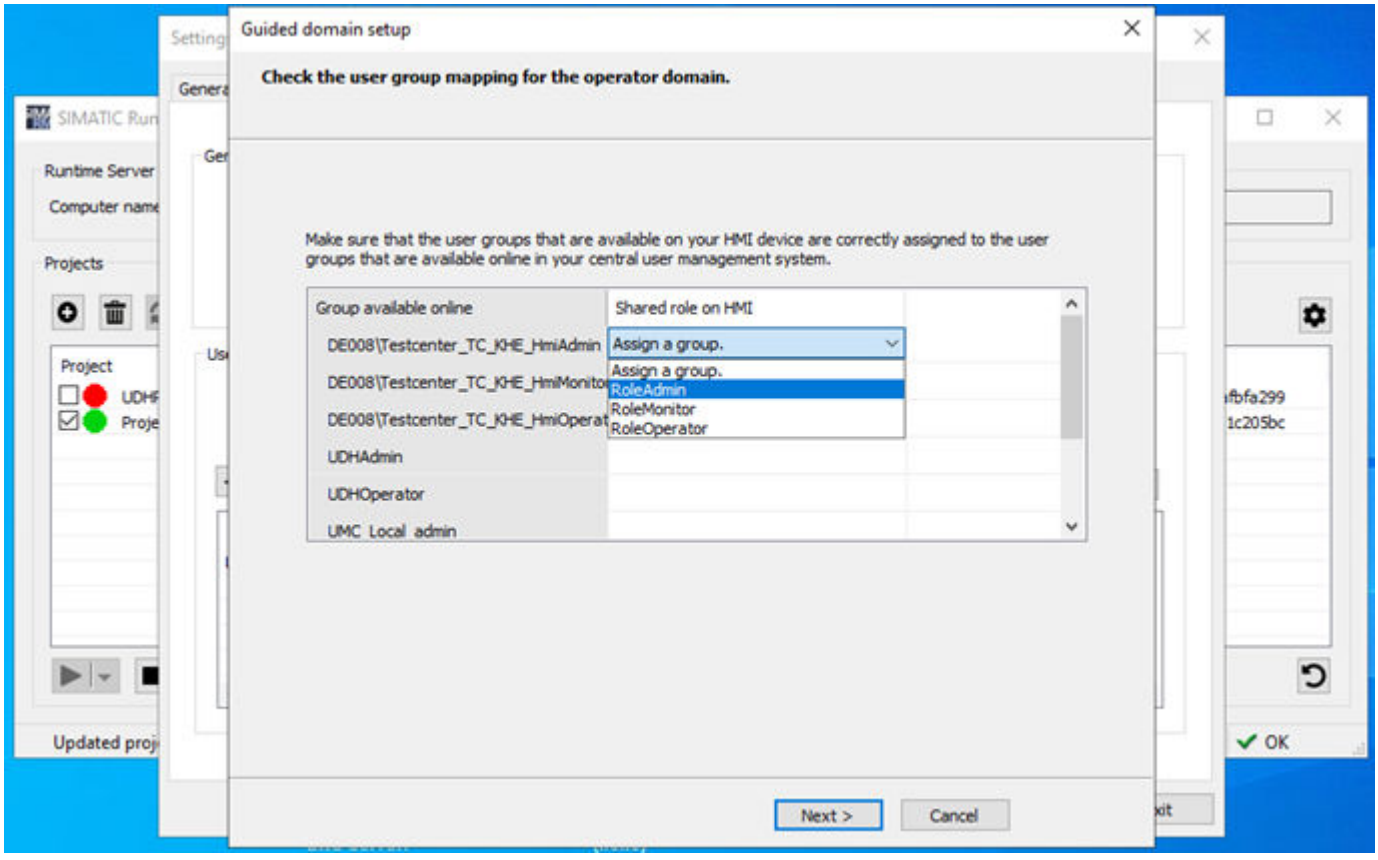
5. Click "Next".
6. Enter the data for the central domain:
   - The domain name, e.g. "MyCentralECDomain".
   - The server address.
   - The server ID (fingerprint).

7. Click "Check connection".
   Connection status is displayed as successful.



8. Click "Next".
9. Assign the authorizations from the local OEM domain to the new central domain. The shared roles created in the Engineering System for the OEM domain are displayed in the right-hand column.

10. In the column on the right, select the shared role that you want to assign to the central groups pre-configured in the UMC server.



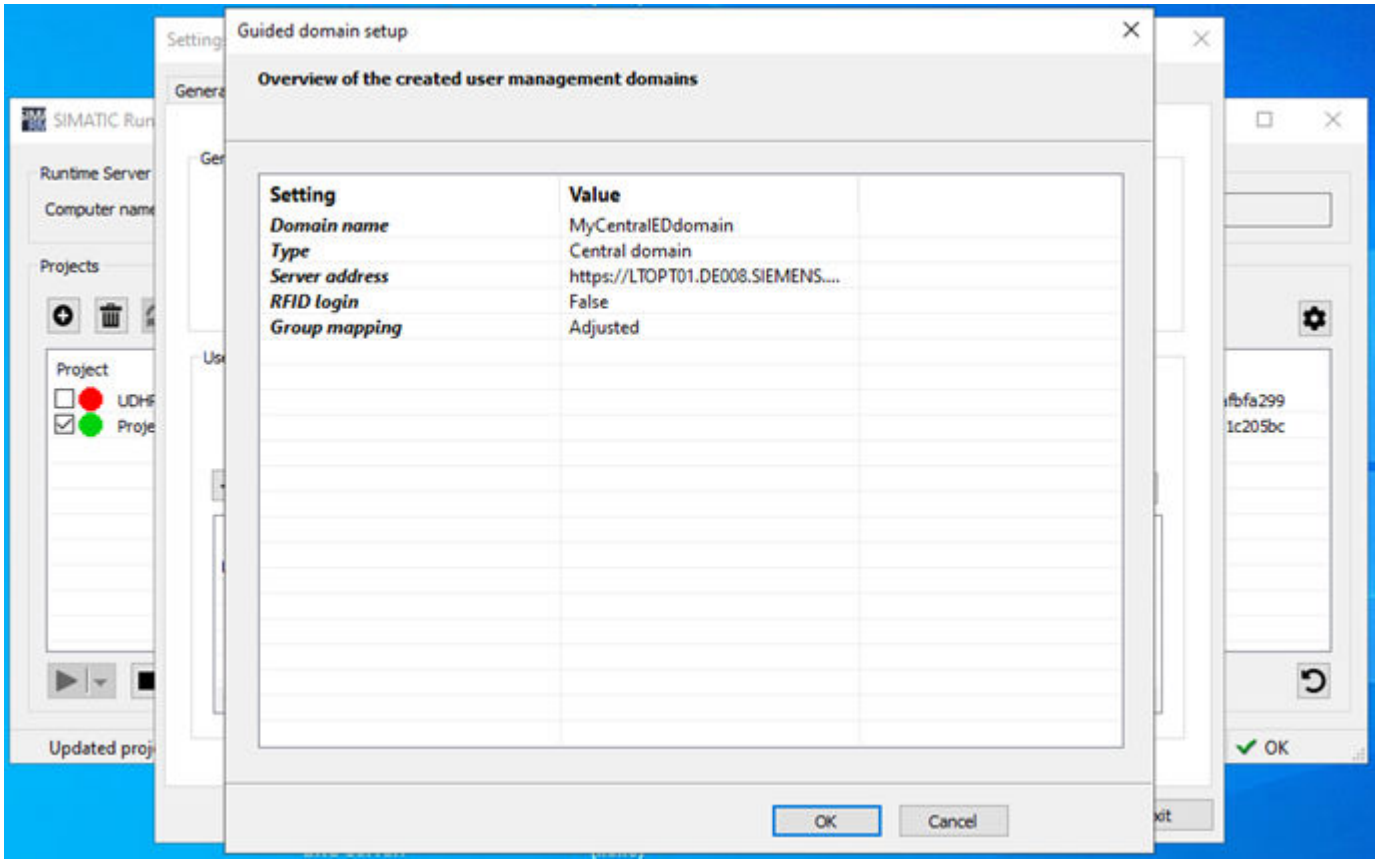
Note

Note:

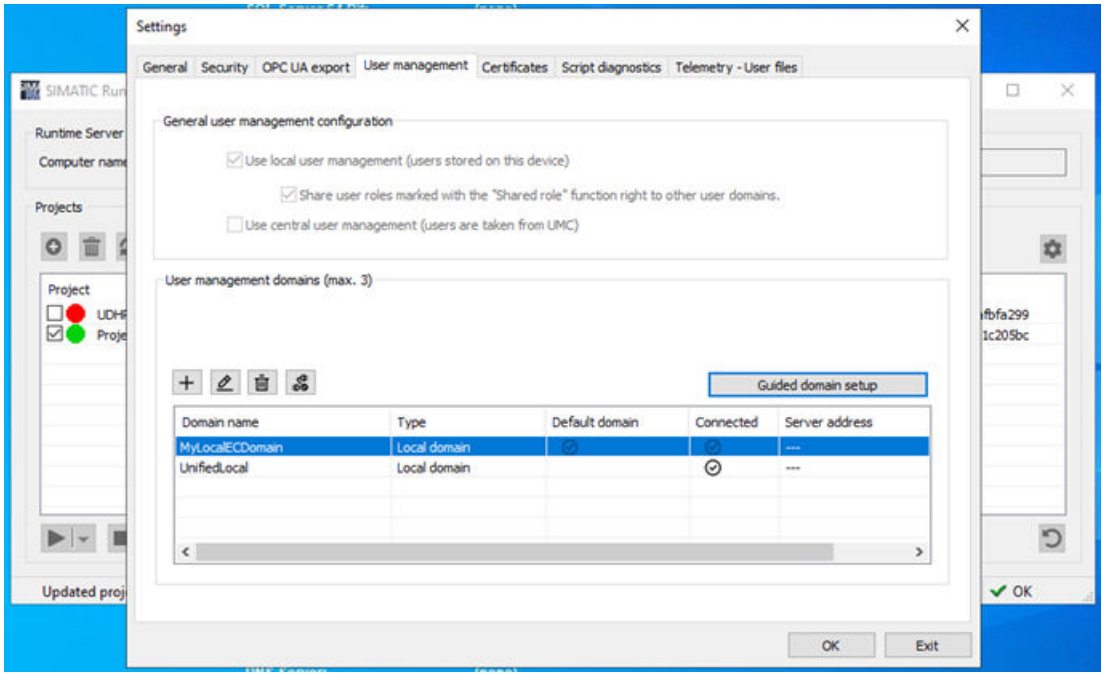
If you configure a "Shared role" function right for a device, you can add a central domain and/or a local domain in the SIMATIC Runtime Manager after downloading the project. The mapping is then created between the central user groups in the central domain and the roles to which the "Shared role" function right is assigned. You can add new users for the local domain and assign the "Shared role" function right.

If the user management data is overwritten during a new project download, the mapping and role assignments are lost. To retain these settings, select the "Keep current user administration data in runtime" option in the "Load preview" dialog when downloading the project again. Otherwise, the mapping and role assignments must be performed again.

11. Click "Next".
    An overview of the created user management domain is displayed.



12. Click "OK".
    The central domain is created and marked as the default domain.



Note

Enter the domain name as a prefix before the user name in the following cases:

- When logging on automatically in SIMATIC Runtime Manager under "Settings > General > Automatic logon".
- If you use the "ChangeUser" system function, the domain name must be placed in front of the user name separated by "\" if you want to log in with a user who does not belong to the default domain.
- For authentication in the following applications: OPC, GraphQL or My WinCC Unified. If the user belongs to the default domain, it is not necessary to specify the domain name.

Configuration 6 - Central users, OEM and fallback users

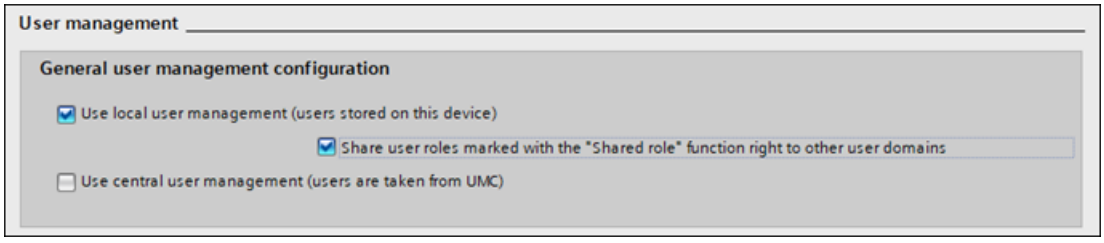
This section describes the following example scenario:

1. The OEM configures the local user management and its users in the Engineering System. A local OEM domain is created.
2. Central end customer domain is created in the SIMATIC Runtime Manager.
3. Local fallback domain is created in the SIMATIC Runtime Manager.

The users at the end customer are central.

Configuring in the Engineering System

1. The OEM configures the local user management and its users in the Engineering System. A local OEM domain is created.
2. The OEM enables the option "Share user roles marked with the "Shared role" function right to other user domains".



3. The OEM assigns the "Shared role" function right to the roles that are available to the system user.
4. The following selection is made for a complete download:
   - Enable the "Start Runtime" option.
   - Do not enable the "Keep current user administration data in runtime" option.
     The user management data is overwritten.

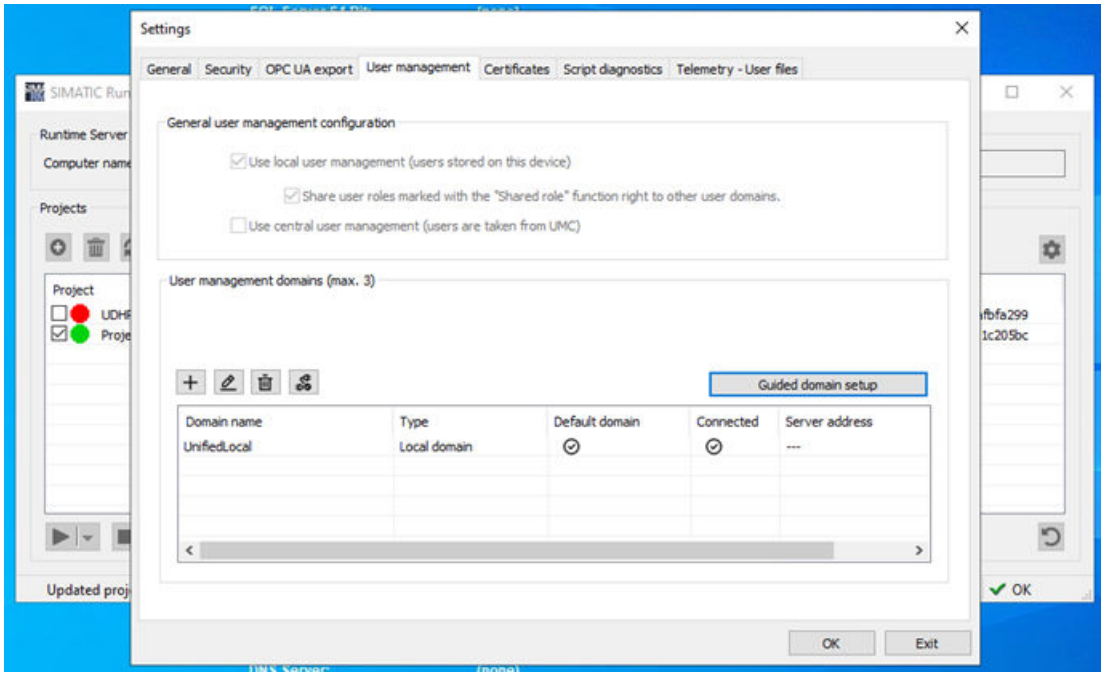
Runtime is started after download is complete.

Options in the SIMATIC Runtime Manager

The following procedure is a configuration example.

1. Create central domain:
   The end customer user administrator creates a central domain on the PC in the Runtime Manager.
   To create this domain, the end customer user administrator configures mapping between the central groups and the local roles to which the "Shared role" function right has been assigned.
   The end customer user administrator configures their users in the central user management.
2. Create additional local fallback domain:
   The end customer user administrator creates an additional local domain on the PC in the Runtime Manager.
   The end customer user administrator configures the fallback users in the additional local domain.

The read-only dialog "General configuration of user management" is visible in the Runtime Manager under "Settings > User management". The dialog shows the configuration that was selected in the Engineering System.



The "Add new domain", "Modify selected domain", "Delete selected domain", "Connect UMC server" and "Guided domain setup" buttons are activated.

Note: The domain created in the Engineering System cannot be deleted in Runtime Manager. Only domains created here can be deleted in the Runtime Manager.

To add a new domain, the end customer user administrator has the following options:

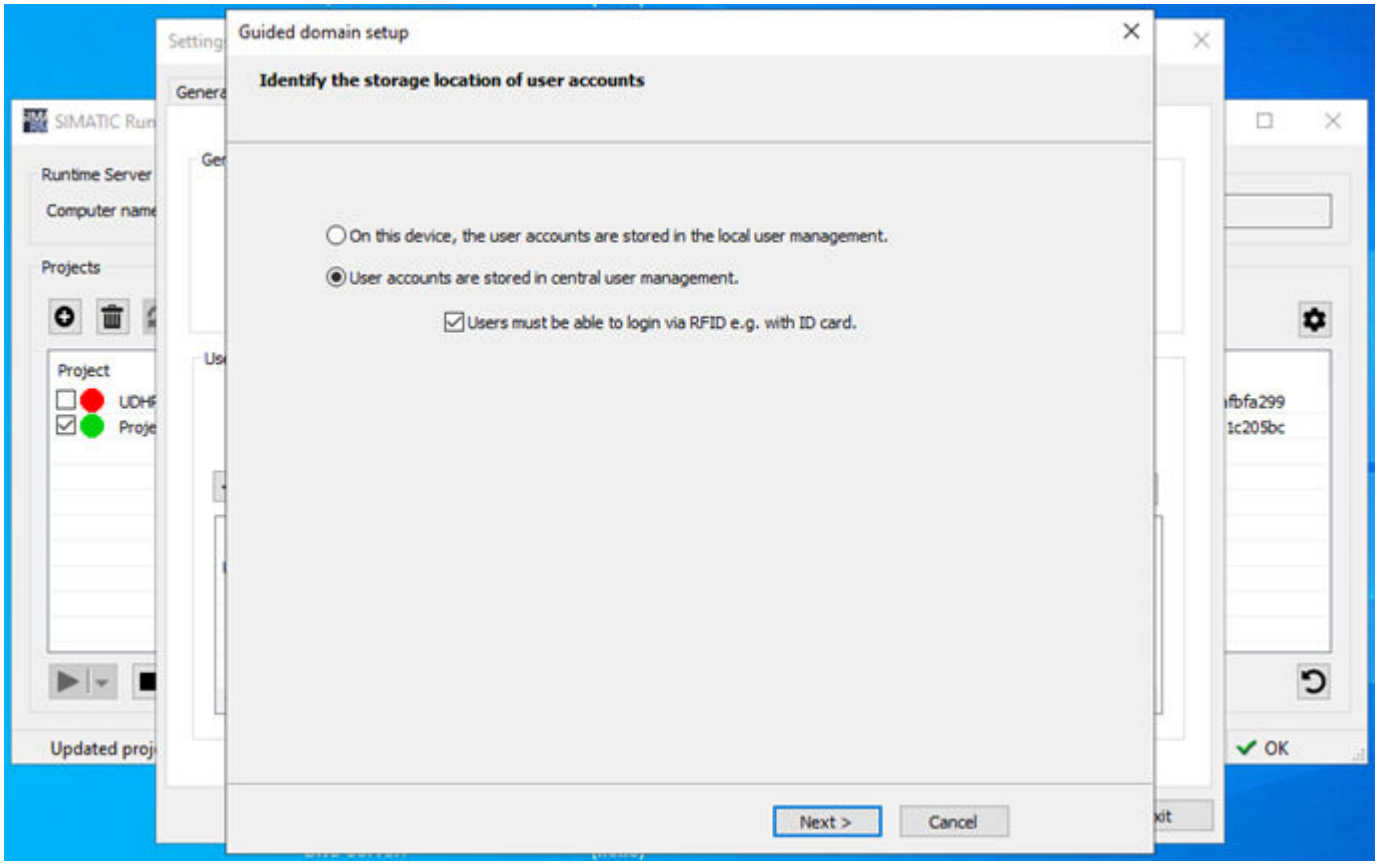
1. Use the "Add new domain" button.
2. Open "Guided domain setup": A wizard provides support when adding the domain.

Adding a central domain and fallback domain via "Guided domain setup"

To add a central domain, follow these steps:

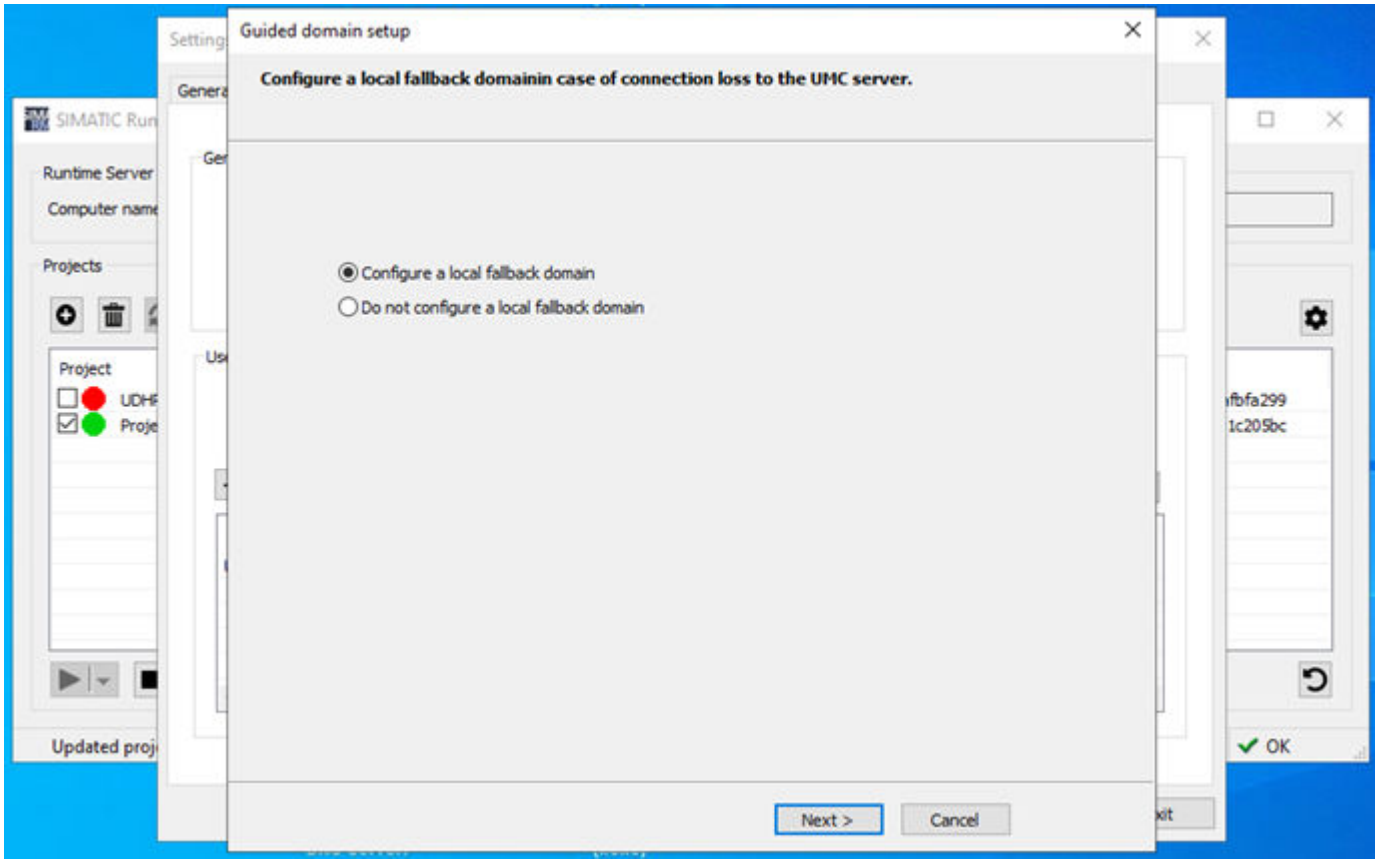
1. Click the "Guided domain setup" button.
   A dialog is displayed.
2. Select the option "User accounts are stored in central user management".

3. Select the option "Users must be able to log in via RFID, e.g. with ID card".



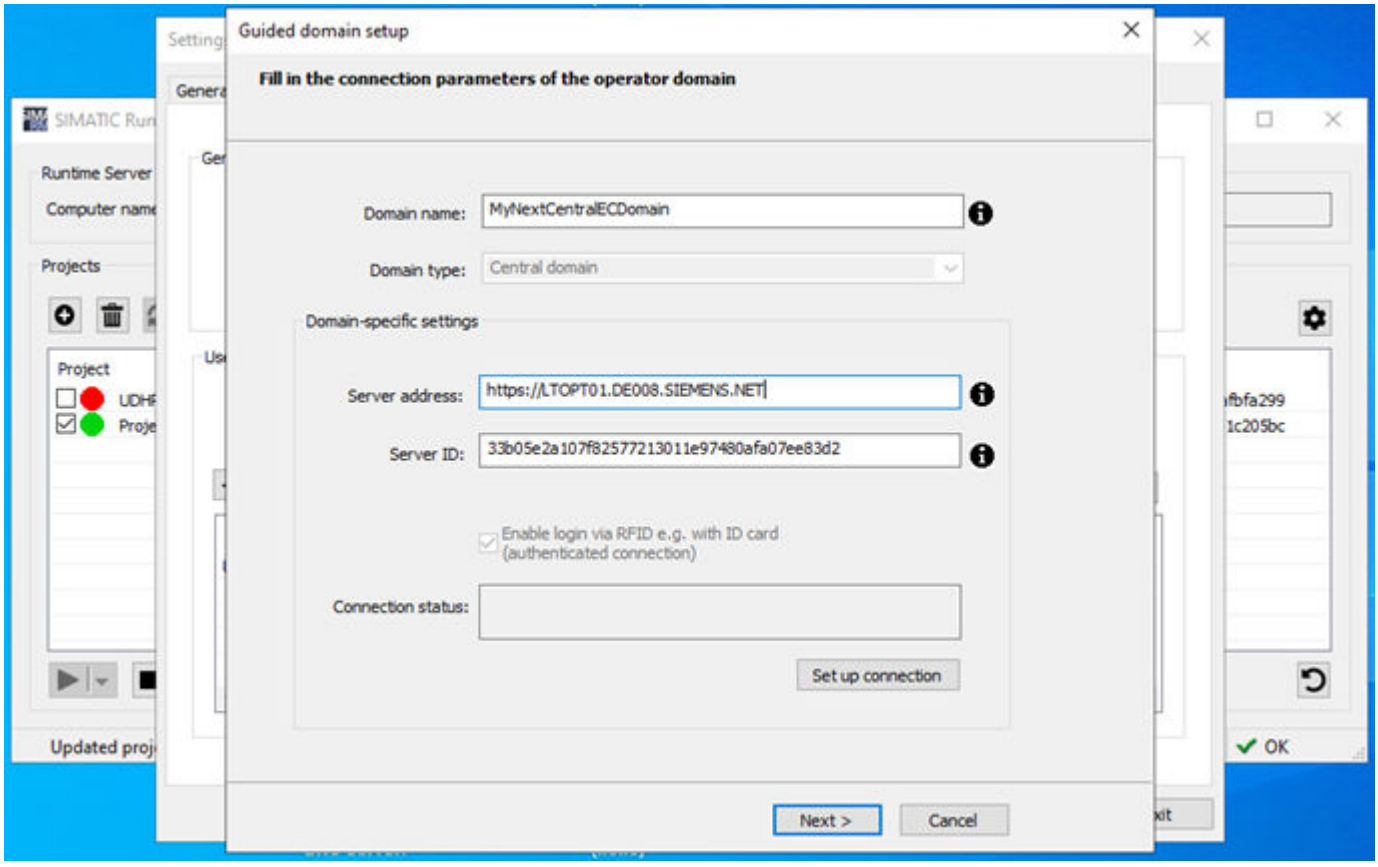
4. Click "Next".

5. Select "Configure a local fallback domain".



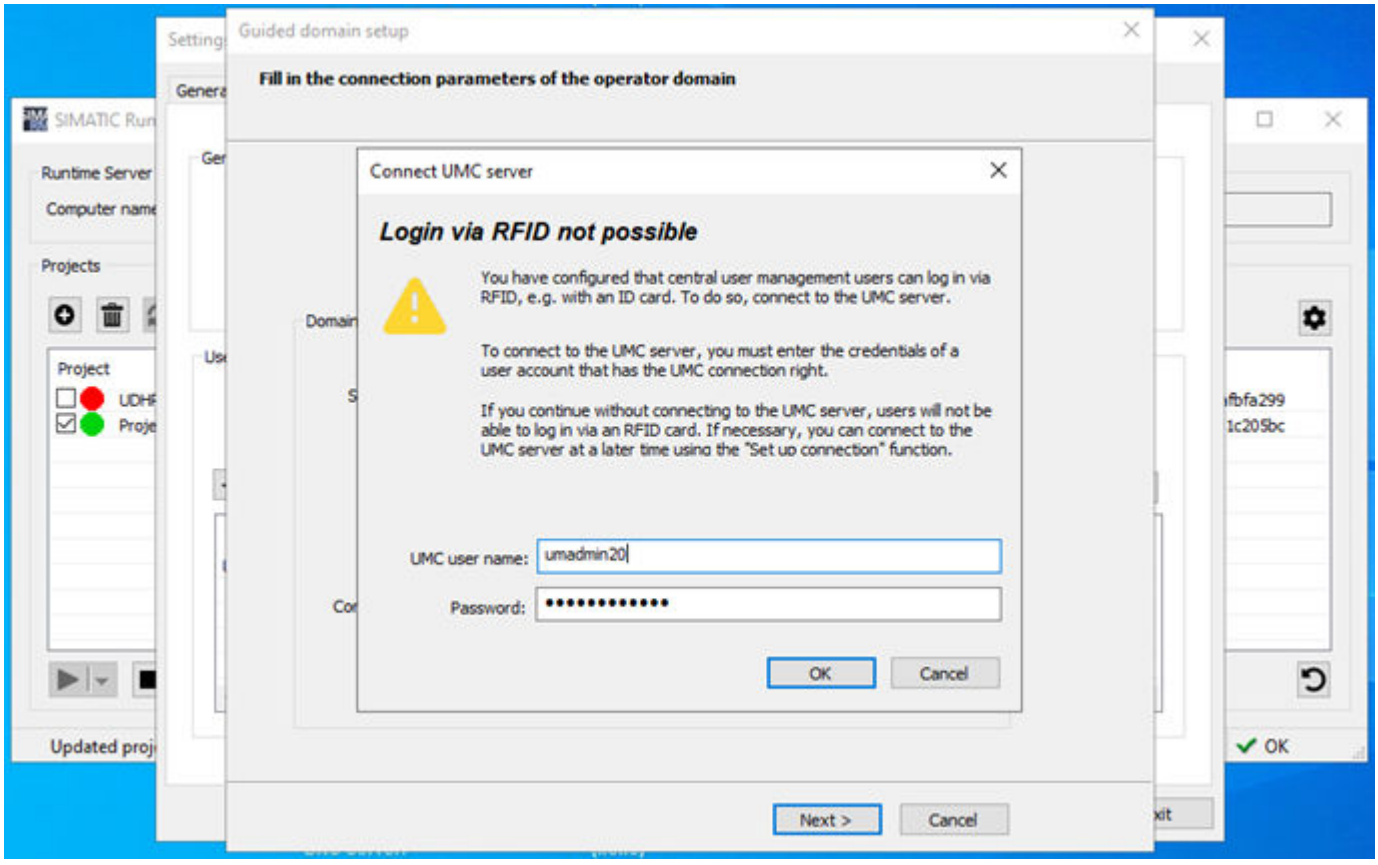
6. Click "Next".

7. Enter the data for the central domain:
   - The domain name, e.g. "MyNextCentralECDomain".
   - The server address.
   - The server ID (fingerprint).



8. Click "Configure connection".
   The "Connect UMC server" dialog is displayed.
9. Enter the UMC user with authorization to connect (e.g. UMC admin user) of the UMC ring server.

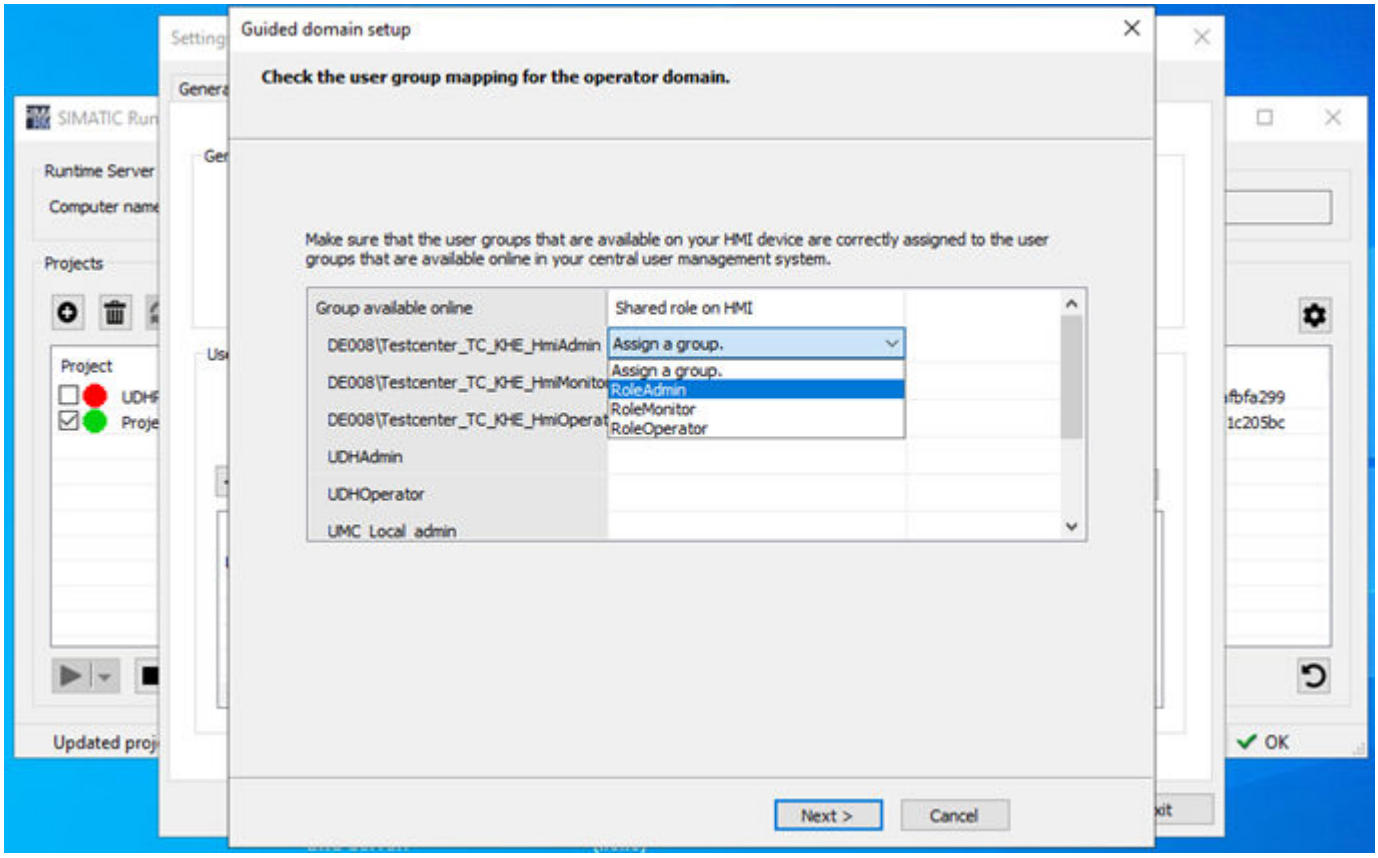
10. Enter the password.



11. Click "OK".
    Connection status is displayed as successful.

12. Assign the authorizations from the local OEM domain to the new central domain. The shared roles created in the Engineering System for the OEM domain are displayed in the right-hand column.

13. In the column on the right, select the shared role that you want to assign to the central groups pre-configured in the UMC server.



Note

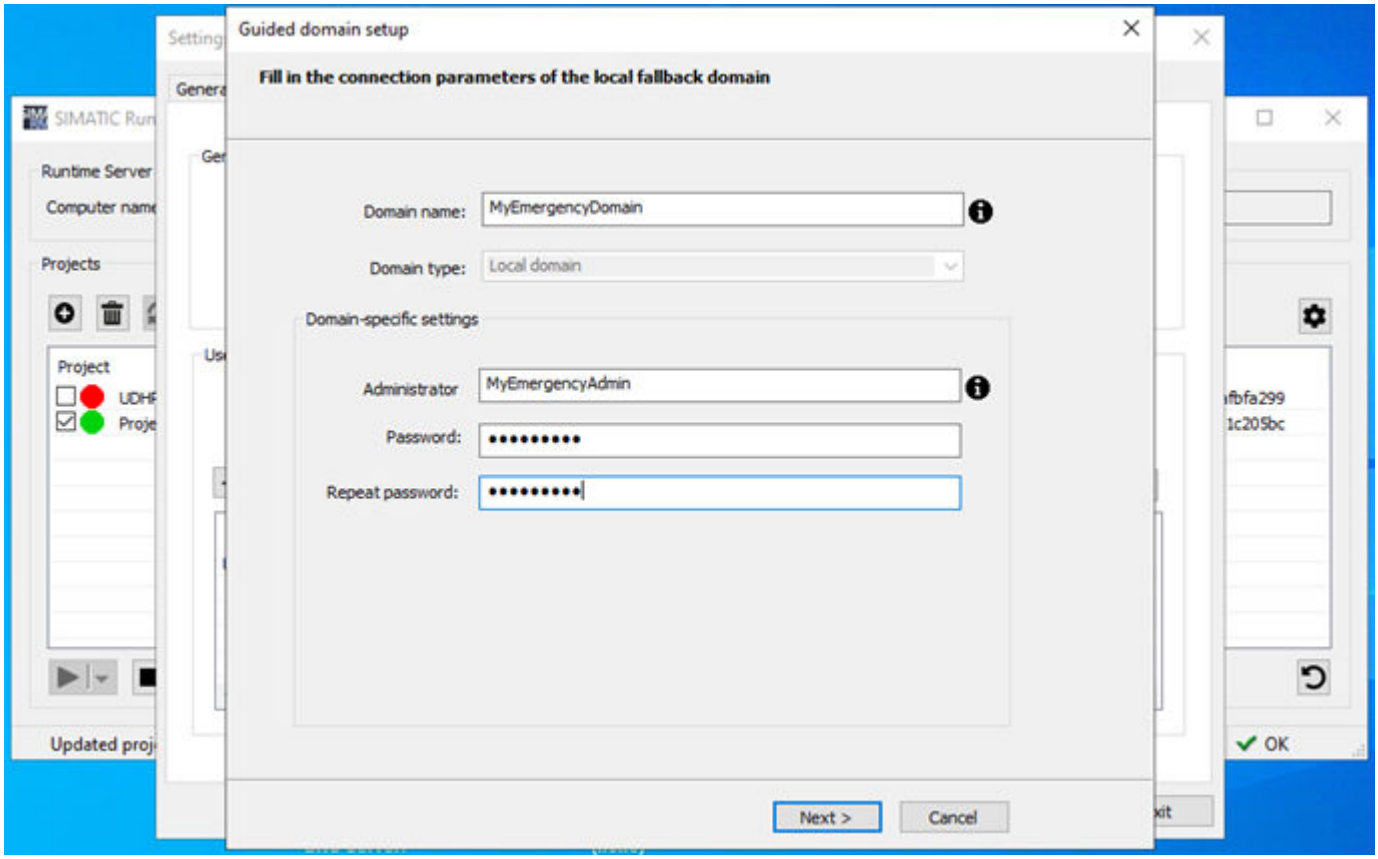
Note:

If you configure a "Shared role" function right for a device, you can add a central domain and/or a local domain in the SIMATIC Runtime Manager after downloading the project. The mapping is then created between the central user groups in the central domain and the roles to which the "Shared role" function right is assigned. You can add new users for the local domain and assign the "Shared role" function right.

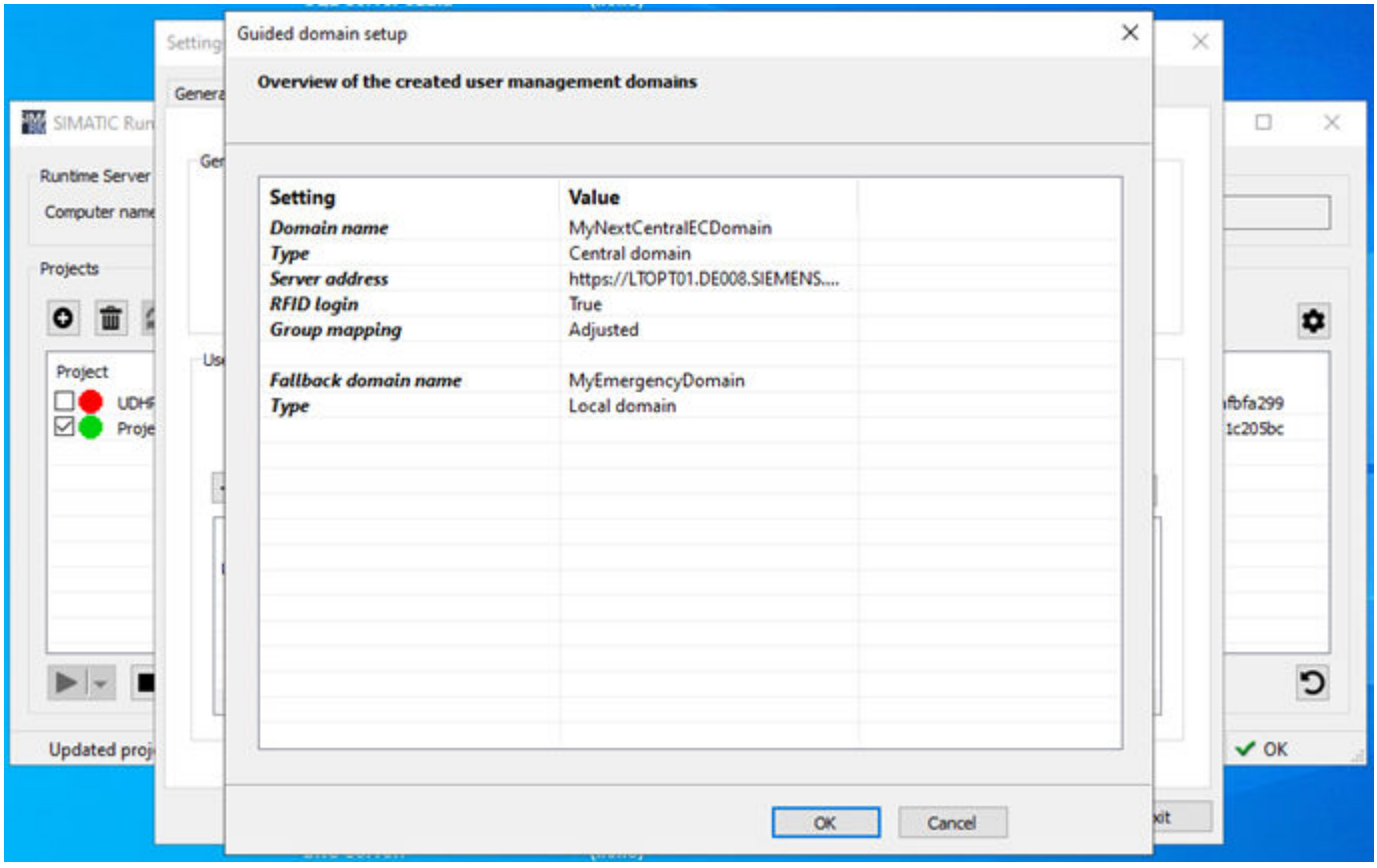
If the user management data is overwritten during a new project download, the mapping and role assignments are lost. To retain these settings, select the "Keep current user administration data in runtime" option in the "Load preview" dialog when downloading the project again. Otherwise, the mapping and role assignments must be performed again.

Click "Next".

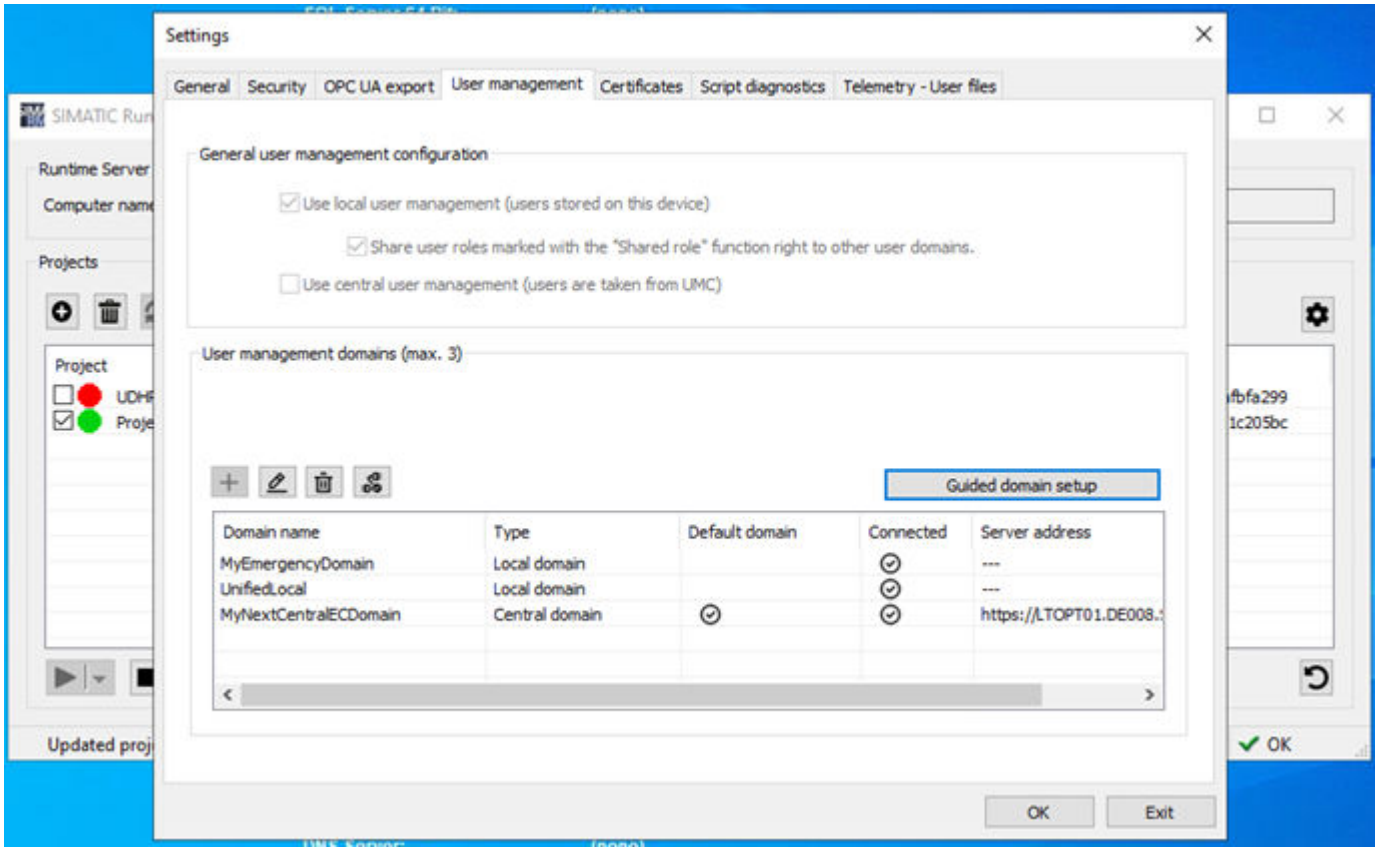
14. Enter the data for the fallback domain:
    - The name of the fallback domain, e.g. "MyEmergencyDomain".
    - The administration user who can add the new users and assign the groups to them.
    - Password.
    - Password repeated.



15. Click "Next".
    An overview of the created user management domain is displayed. Both domains are visible.



16. Click "OK".
    The central and fallback domains have been created.
    The central domain is defined as the default domain.



Configuring local users in Runtime

You can create and manage users in Runtime.

You can learn about the procedure in the section Configuration 4 - Local users and OEM (Page 46).

Note

Enter the domain name as a prefix before the user name in the following cases:

- When logging on automatically in SIMATIC Runtime Manager under "Settings > General > Automatic logon".
- If you use the "ChangeUser" system function, the domain name must be placed in front of the user name separated by "\" if you want to log in with a user who does not belong to the default domain.
- For authentication in the following applications: OPC, GraphQL or My WinCC Unified. If the user belongs to the default domain, it is not necessary to specify the domain name.

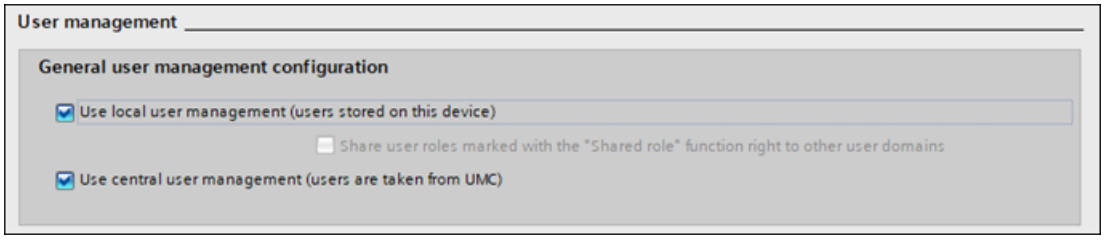
Creating fallback users

The fallback users are created in the local domain. If the connection to the central UMC server is interrupted, a locally created fallback user can be used to ensure access to WinCC Unified Runtime.

Creating fallback users in the Engineering System

To create the fallback users in the Engineering System, proceed as follows:

1. Activate the local user management.
2. Activate the central user management.



3. Create your fallback users as local users in the Engineering System in the user management. You can use any local user with HMI function rights as a fallback user.
4. When logging in with the fallback user, specify the domain name.

Creating a fallback domain in the Runtime Manager

You can also create the fallback domain and the fallback users in the Runtime Manager.

You can learn about the procedure in the section Configuration 6 - Central users, OEM and fallback users (Page 62).

3.3.2.9 OPC UA support for structures

OPC UA: Support of structures

Communication via OPC UA now also supports the use of structures.

To configure a structure for OPC UA communication, follow these steps:

1. Add an HMI user data type.
2. Select "GenericCommunication" as the communication driver in the properties of the HMI user data type.
3. Manually arrange the individual elements within the structure so that the structure to be read by the OPC UA server and the configured HMI user data type are identical.

Note

Note the following:

- The structure and the configured HMI user data type must have the same number of elements, the same data types of the elements and the same order of the elements.
- The data type of an element within the structure of the OPC UA server can be mapped based on an assignment of SIMATIC data types, OPC UA data types and the generic HMI UDT data type.
- Generic HMI user data types can only be used with the OPC UA communication driver in TIA Portal V21.
- Generic HMI user data types can be used with WinCC Unified Faceplates as of device version 21.
- If the configured generic HMI user data type and the structure read by the OPC UA server are different in terms of the number of elements, element sequence and data types of the elements, it is rejected by the WinCC Unified Tag Table.
- Elements of the structure can be used like HMI OPC UA communication tags, which have simple data types, with any screen object or the supported Runtime functions.
- In TIA Portal V21 with WinCC Unified device as of version 21, structures are only supported for simple elements within a structure. Nested structures or complex data types within a structure are not supported.

3.4 Unified Engineering

3.4.1 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.

Installation of SiVArc V21

After SiVArc V21 is installed on a Windows 11 Enterprise 25H2 VM with TIA Portal V21, the projects are displayed correctly in the project view.

Screen objects

After changing the editing language, all objects in the screen are displayed correctly.

When dynamized properties are changed, the dynamization tags of multiple selected objects are correctly maintained.

Text

When transferring the format from one "Text" object to another "Text" object, the alignment is transferred correctly.

Compiling and downloading

Error messages during the compilation of the project have been improved.

Trend control on WinCC clients

The trends on the WinCC clients are now displayed correctly, without the need to manually add the server prefix or adjust the configuration during project migration.

3.4.2 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 Screen Editor (Next Gen.)

The key combination <Ctrl + 0> also works in the Unified Screen Editor (Next Gen.).

Alarms

The compiling now works correctly, even if no status texts are defined for alarms in the Runtime settings.

Tags

The engineering and documentation for BlockArrays has been improved.

Parameter sets

The behavior of the scroll bar when editing parameter set types with the data type "Simple tag" has been improved.

System functions and scripts

Autocomplete has been improved for the PopupScreenWindows function so that a syntax error is no longer displayed.

When creating a script module type in the library, asynchronous functions are always applied correctly.

The occasional incorrect replacement of function parameters with tag definitions has been corrected.

3.5 Unified PC

3.5.1 Improvements in Update 2

3.5.1.1 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 WinCC Unified Runtime Asian

Problems with the detection of the dongle have been resolved.

Recreating the certificate configuration in Certificate Manager

If you recreate the entire configuration of the certificate authority in WinCC Unified Certificate Manager, the newly created certificates will have the same validity period as their predecessors. The calculation of the validity period of the new certificates is now performed correctly.

3.5.1.2 Password protection in WinCC Unified Certificate Manager

Improved password protection for the configuration of the certificate authority

When you create a certificate authority in WinCC Unified Certificate Manager, protect the certificate authority with a password (CA password). The configuration backup of the certificate authority is also protected by a transfer password.

Password protection for certificate authorities has been improved.

New behavior:

- If you start Certificate Manager on a device where a certificate authority has been created, the configuration of the certificate authority is only loaded after entering the CA password.
- When you open a certificate authority backup in Certificate Manager, the configuration of the certificate authority is only loaded after you have entered the transfer password and the CA password.
- After five incorrect CA password entries, Certificate Manager will be deactivated for 3 minutes.
- Certificate authorities created before V21 Update 2, or backups of certificate authorities, must be migrated.

Migrating a certificate authority created before V21 Update 2

If a certificate authority created before V21 Update 2 exists on the device, you must migrate this certificate authority once:

1. Start Certificate Manager.
   You will be prompted to create a new CA password.
2. Enter the password and confirm it.

Note

Password backup

Keep the password in a secure place, such as a certified password manager.

If the CA password is lost, the current configuration of the certificate authority is lost.

The configuration of the certificate authority is loaded into Certificate Manager.

Every future loading of the certificate authority in Certificate Manager requires the entry of this CA password.

Loading a certificate authority that was migrated to V21 Update 2 or created in Update 2

If a certificate authority exists on the device that was created in V21 Update 2 or that was migrated to V21 Update 2, follow these steps:

1. Start Certificate Manager.
2. Enter the CA password and confirm your entry.

The configuration of the certificate authority is loaded into Certificate Manager.

Opening the backup of the certificate authority

NOTICE
Data loss due to opening a backup You can only open the backup file of a certificate authority in Certificate Manager if you reset the current configuration.

Procedure if the backup was created before V21 Update 2

1. Start Certificate Manager.
   A dialog for entering the CA password opens.
2. In the dialog, click "Reset configuration".
3. In Certificate Manager, double-click the "Open configuration..." entry on the "CA configuration" tab.
4. Select the backup file and confirm with "Open".
5. Enter the transfer password set when exporting the backup and confirm with "Open".
   You will be prompted to create a new CA password.
6. Enter the CA password and confirm it.

Note

Password backup

Keep the password in a secure place, such as a certified password manager.

If the CA password is lost, the current configuration of the certificate authority is lost.

Procedure if the backup was created with V21 Update 2

1. Start Certificate Manager.
   The dialog for entering the CA password is displayed.
2. In the dialog, click "Reset configuration".
3. In Certificate Manager, double-click the "Open configuration..." entry on the "CA configuration" tab.
4. Select the backup file and confirm with "Open".
5. Enter the transfer password set when exporting the backup and confirm with "Open".
6. Enter the CA password and confirm your entry.

Result

The CA configuration stored in the backup file is loaded into Certificate Manager.

Procedure in case of loss of CA password

Application 1: Backup created before V21 Update 2 is available

The procedure described here applies in the following case:

- You migrated a certificate authority created before V21 Update 2 to V21 Update 2 and lost the CA password.
- You have access to a backup of the certificate authority created before V21 Update 2.

Open the backup of the certificate authority. To do this, follow the steps described above under "Opening the backup of the certificate authority".

Application 2: No backup created before V21 Update 2 is available

The procedure described here applies in the following cases:

- You have lost the CA password for a certificate authority created with V21 Update 2.
- You have lost the CA password of a certificate authority that was created before V21 Update 2 and migrated after V21 Update 2. You do not have access to a backup of the certificate authority created before V21 Update 2.

Follow these steps:

1. Start Certificate Manager.
   A dialog for entering the CA password opens.
2. In the dialog, click "Reset configuration".

NOTICE
Data loss due to the reset of the configuration
The current configuration of the certificate authority is lost.

3. In the "CA configuration" tab, double-click "Create new certificate authority...".
4. In the "New certificate authority" dialog, set the properties of the new certificate authority. In the "Security" tab, enter the CA password.

   Note

   Password backup

   Keep the password in a secure place, such as a certified password manager.

   If the CA password is lost, the current configuration of the certificate authority is lost.

5. Click "Create".

A new certificate authority is created. The certificate authority is protected by the CA password you entered.

Add the required devices and certificates to the certificate authority.

3.5.2 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.

Graphic display

The dynamization of graphic displays via expressions has been improved.

Alarm control

The display of multi-line texts has been improved.

Trend control

Automatic scaling of the axes of a trend control works correctly, even if the axes are assigned to different trends.

Object groups

The display of objects in a group has been improved so that the objects are displayed correctly even if the "Operator control - allow" property of the group is changed dynamically.

Flashing

The flashing behavior of objects in faceplates has been improved so that the objects also flash correctly when the faceplate is displayed in an screen window and the visibility of the screen window is changed dynamically.

Dynamic change of the Z-order

To prevent borderless screen windows or borderless faceplates from covering other objects by dynamically changing the Z order, the change of the Z order will be prevented for borderless objects in future. This also applies, for example, to the OpenScreen InPopup system function.

3.6 Unified Panels

3.6.1 Important notes (Unified Comfort Panels)

This section contains important information about product properties.

"System Properties" > "Event Logger"

Only enable 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.

"System Properties" > "Screensaver"

If you do not operate the HMI device within the time period specified under "Wait time", the screen saver is activated.

To deactivate the screen saver, touch the touch screen briefly. For security reasons, this touch is not interpreted as an operator action. This means that no unintended functions can be triggered.

The screen saver is also deactivated in the following cases:

- Remote access to the HMI device takes place, e.g. via Smart Client or the configuration PC.
- The "SetBrightness" system function was called.

Important notes on storage media

Executing scripts

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

Upgrading and downgrading HMI device images

NOTICE
Upgrade to image version V21 Upd.2 only via V21 Upd.1 For security reasons, the signature algorithms for the current HMI device images have been changed. Upgrading to image version V21 Upd.2 or higher is only possible if image version V21 Upd.1 or higher has been installed on the HMI device beforehand. Otherwise, an error message with code 6404 will appear. This intermediate step is only required once. After successful completion, all further updates can be installed without restrictions.

Downgrading to a lower image version is possible without such a restriction.

User management and Unified Air

Unified Air is currently only supported in connection with the previous concept of purely local or purely central user management.

Do not use Unified Air on an HMI device on which there is more than one domain for user management.

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 management.

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.

Resource-intensive SIMATIC Edge apps

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.

Notes on the "Web Browser" app

For security reasons, the "Web Browser" app blocks access to web pages that are on the HMI device.
Instead, use the "Browser" Runtime control, which can be configured for user-specific access to web pages.

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.

Alarm control

Filtering alarms

Alarm filter expressions **cannot** be edited using the screen keyboard or an external keyboard.

System diagnostics view

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

User-specific fonts in faceplates

If you only use a specific character set in faceplates, these characters are displayed in Runtime with a system character set. To ensure that the specific character set is also used in Runtime, use this character set for any other object outside the faceplate.

3.6.2 Important notes (Unified Basic Panels)

This section contains important information about product properties.

"System Properties" > "Event Logger"

Only enable 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.

"System Properties" > "Screensaver"

If you do not operate the HMI device within the time period specified under "Wait time", the screen saver is activated.

To deactivate the screen saver, touch the touch screen briefly. For security reasons, this touch is not interpreted as an operator action. This means that no unintended functions can be triggered.

The screen saver is also deactivated in the following cases:

- Remote access to the HMI device takes place, e.g. via Smart Client or the configuration PC.
- The "SetBrightness" system function was called.

Upgrading and downgrading HMI device images

NOTICE
Upgrade to image version V21 Upd.2 only via V21 Upd.1 For security reasons, the signature algorithms for the current HMI device images have been changed. Upgrading to image version V21 Upd.2 or higher is only possible if image version V21 Upd.1 or higher has been installed on the HMI device beforehand. Otherwise, an error message with code 6404 will appear. This intermediate step is only required once. After successful completion, all further updates can be installed without restrictions.

Downgrading to a lower image version is possible without such a restriction.

Alarm control

Filtering alarms

Alarm filter expressions **cannot** be edited using the screen keyboard or an external keyboard.

System diagnostics view

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

3.6.3 Runtime improvements in Update 2

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved, among others, on account of the feedback received.

Screen window and faceplate

Scrolling in the screen window and in the faceplate works correctly after zooming.

Text lists

The use of array elements as dynamic parameters in text lists now works correctly.

Text box

The text in the "Text box" object is displayed correctly in the simulation on the Unified Panel after "Properties > Format > Text trimming > With character ellipsis" is selected.

Bar

The values are displayed correctly on the bar in the process value indicator mode "Bar with detailed indicator" in all predefined styles.

Trend control

The scaling of the y axis is now consistent in simulation and Panel Runtime.

The behavior when showing and hiding trends has been improved.

The display of the grid lines has been improved.

I/O field

The shifting of decimal places now works correctly and is consistent in simulation and Panel Runtime.

Date and time are displayed uniformly in simulation and Panel.

It is no longer possible to enter negative values into an I/O field that is linked to a PLC tag of data type "Time_of_Day".

The time is displayed in the I/O field in the correct format.

The limit value tooltips are displayed correctly in the I/O field.

Button

If a button is located behind another screen object, no visual feedback is triggered at the button when you touch the object in the foreground on the touchscreen.

The property "Pressed status tags" is consistently and correctly triggered for the button when operated by mouse, touch and keyboard (Enter and Space).

Control Media Player

The "Playback finished" event is triggered correctly.

Tags

Writing tags of PLC data type "DTL" via the HMI works correctly.

Login in Runtime

The unintentional scrolling of the screen during password input has been fixed.

System functions

The positioning of the popup when using the system function "OpenImageInPopup" works correctly.

Scripting

Reading the zoom factor via `ScreenWindow.CurrentZoomFactor` now works correctly on the Panel.

Events

Events of type "Command executed" now work correctly for all screen objects.

Tooltips in faceplates

The display of tooltips in faceplates has been corrected. Tooltips are displayed in full, even if the faceplate width is small.

3.6.4 Runtime improvements in Update 1

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved, among others, on account of the feedback received.

I/O fields

The display of date/time information with the output format {D} has been improved.

Symbolic I/O field

The appearance of texts in symbolic I/O fields has been improved.

Alarm control

The display of multi-line texts has been improved.

Rotated objects

An object can be operated at the visible position, even if the rotation properties have been changed dynamically.

Objects with scroll bar

The scrolling behavior of objects with scroll bars has been improved.

3.7 Redundancy

3.7.1 Improvements in Update 2

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved, among others, on account of the feedback received.

3.7.2 Improvements in Update 1

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved, among others, on account of the feedback received.

Logging tags

The synchronization of logging tags has been improved in redundant systems.

3.8 Audit

3.8.1 Entries in the Audit Trail

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.
Change time stamps	Currently only used for security events. It is the timestamp of the event generation.
Audit provider	Contains the name of the provider, for example, Scheduler, User Interface, Event Manager.
Type	Refers to the internal system component in which the change was made.
	2 - Task scheduler "Scheduler" is entered as type in the event of changes in the configured cyclic tasks.
	6 - User interface "UI" is entered as type in the event of changes made via the user interface.
	8 - User management On changes to the user management: e.g.: Login, logout, "User management" is entered as type.
Object reference	Contains an identifier of the triggering object. This parameter is reserved for internal purposes.
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.
User ID	Reserved for future use.

Parameter	Description
Operator station	Contains either the name of the PC or PLC, or the IP address of the web client.
Operation	Currently used for the parameter set display and security events. The process is saved for the parameter set control (e.g. Create, Save, Rename, Delete, etc.). The event ID of the security event is saved for security events.
Operation type	Specifies whether the changed object was created, modified or removed. 1 - New value 2 - Updated value 3 - Deleted value (this type of operation indicates that the object concerned has been deleted)
Old value	Contains the tag value before the change.
New value	Contains the tag value after the change.
Language	Returns the value of the language code, e.g.: 1033 corresponds to the language code for English (USA).
Reason	Contains the user comment for user actions or the result of the operation for system responses.
Integrity	Contains an identifier to verify whether data was manipulated later or the Audit Trail certificate is not installed or has expired. Example of an integrity entry: • --: Valid event. The entry was not manipulated. The test mode "No verification" in the global settings is not set. • Not verified: An event was not tested for integrity. In this case, the Audit certificate is not installed or has expired. • Invalid Interval**:** Contains two entries of the time interval, one entry for the interval start and one entry for the interval end. The following facts are designated: – Audit Trail certificates are not installed or have expired – One or more entries in the Audit file were deleted. The "Reason" parameter specifies the number of deleted entries • Invalid Event: The entry in the Audit file was manipulated and is marked in red.
Signature	Contains the information on the provided electronic signature (user, role, contract). One entry in the Audit Viewer is for each individual signature and one entry is for the entire operation. Example: Entry for individual signature: • Status 1: Valid signature  • Status 0: Invalid signature  Example: Entry for the entire operation: 

Parameter	Description
Signature status	Reserved for future use.
Display name	Contains the language-dependent display name of the tag.

3.8.2 Improvements in Update 2

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved, among others, on account of the feedback received.

Acknowledging Audit alarms

Audit alarms with electronic signatures can now be acknowledged simultaneously by two different clients.

3.8.3 Improvements in Update 1

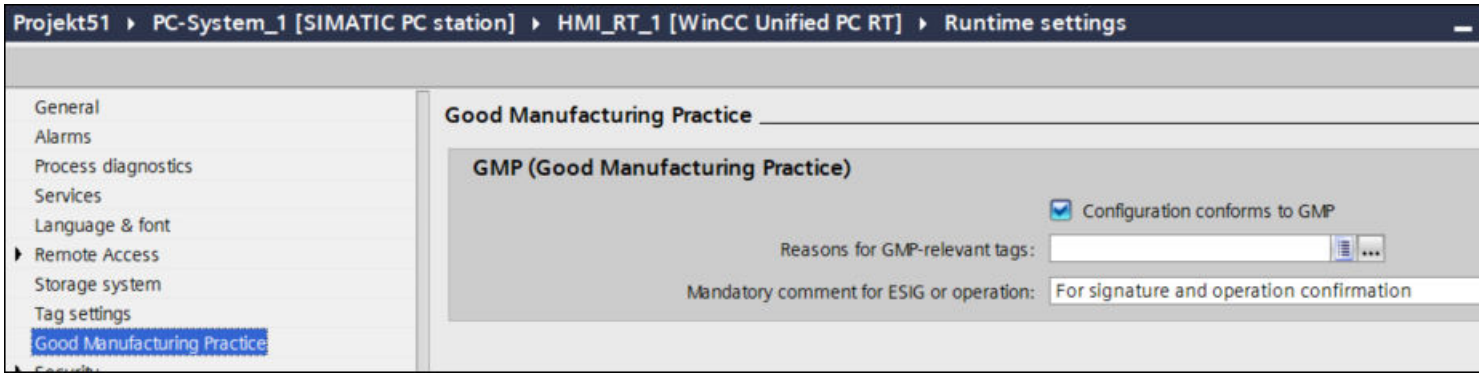
Introduction

The audit class configuration is only applicable for integrated S7 Plus connections and S7 controller alarms in the PLC.

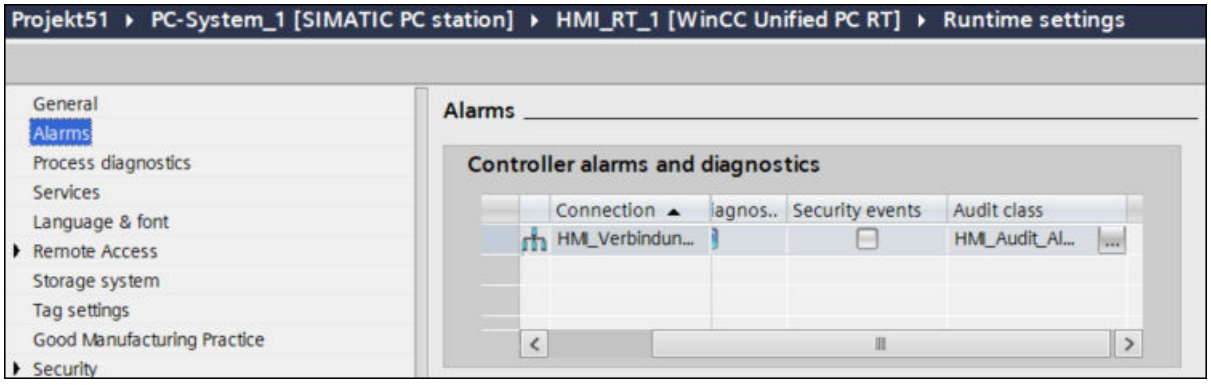
The configuration can be performed for Unified Comfort Panels and Unified PC devices.

Requirement

1. "Configuration conforms to GMP" has been activated in the Runtime settings of the HMI device.

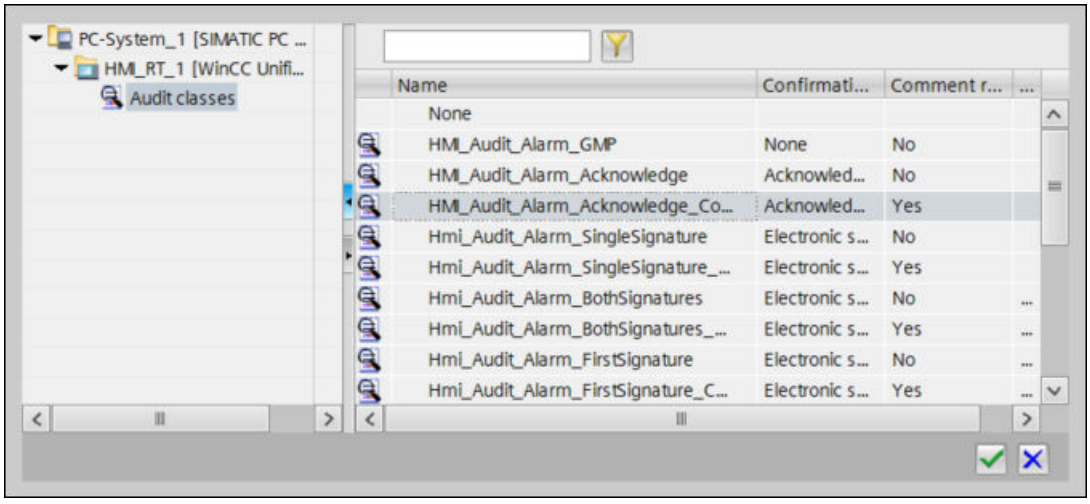


2. An integrated S7 Plus connection is established between the PLC and the HMI device.
3. The "Audit class" column is visible under "Runtime settings > Alarms" in the "Controller alarms and diagnostics" area.



Configuring audit class

1. Click ... in the "Audit class" column. A table with all confirmation combinations opens.
2. For example, select "HMI_Audit_Alarm_Acknowledge_Comment" with comment.

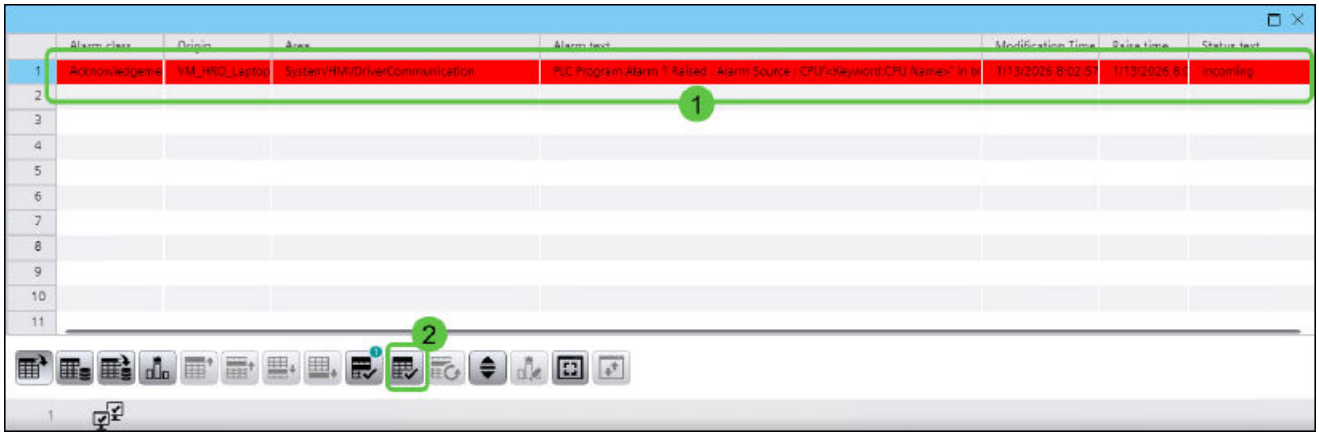


3. Confirm your selection with the green check mark.
4. You can also enter the name of the audit class directly in the field. An invalid audit class configuration is rejected if it has not been entered correctly.

Displaying alarms in Runtime

Download the project to the Unified device.

1. Configure the S7 controller alarms in the PLC. When they are triggered, you can see their value in the alarm control.
2. Select the alarm and acknowledge it.

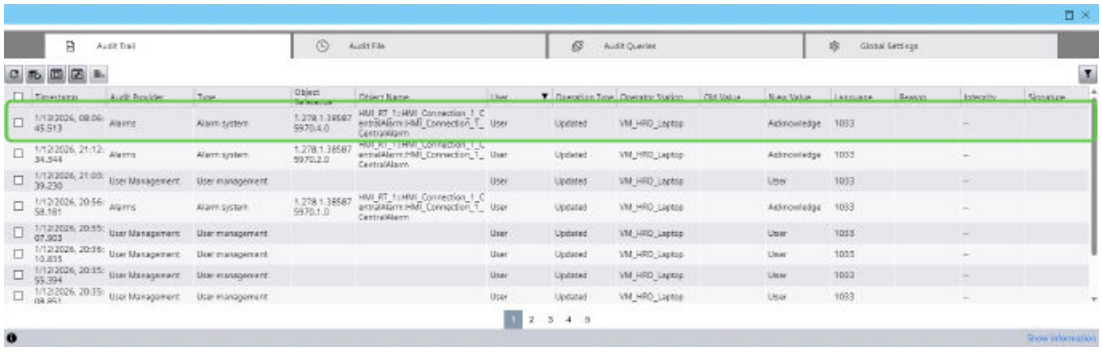


3. An Audit Trail pop-up window is displayed in Runtime where you can make entries such as comment and signature based on the audit class configuration you have selected.



Result

The relevant entries are available in the Audit Trail in the Custom Web Control, provided you have added and configured the "Audit Viewer" object in the Engineering System.



3.9 Reporting Excel add-in

3.9.1 Improvements in Reporting Excel add-in V26 Update1

Stability and performance

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

3.9.2 Improvements in Reporting Excel add-in V26

Stability and performance

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

Logging into the Excel add-in and setting up an online connection

Runtime web servers support the configuration of domains as of V21 Update 1.

If you log on to a Runtime web server with V21 Update in the Reporting Excel add-in V26 or enter an online connection to a Runtime web server with this version, the domains configured for the web server are offered to you. Select the desired domain.

3.9.3 Checking integrity

3.9.3.1 Basic information about the integrity check

Introduction

It is important to check the integrity and authenticity of the installation source and the installed products to ensure that no modified files are present. Siemens supplies the following two validators as command line tools:

- Integrity Validator
  The Integrity Validator is used to check the setup files of an installation source, i.e. an installation medium or downloaded software packages, for modifications. This validator is executed automatically at the beginning of an installation. The Integrity Validator is not installed on your system. You will find it in the installation source in the "IntegrityValidator" directory. From there, you can run it to perform an integrity check manually. You can use the "appsettings.json" configuration file to specify the path to the setup files.
- Installation Integrity Validator
  The Installation Integrity Validator is installed together with every Siemens product bundle that supports the software integrity check. Unlike the Integrity Validator, the Installation Integrity Validator is not executed automatically. You can run it yourself at any time to check the integrity of your system. If your system is connected to the Internet, it is recommended that you repeat this check at a certain time interval.

Both validators create a validation report during validation, in which you can see whether the integrity check was successful or failed. If the integrity check fails, you can see the possible reasons in the report.

You can find more information on the topic of cybersecurity here:

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

3.9.3.2 Performing an integrity check

With the two validators "Integrity Validator" and "Installation Integrity Validator", you can check the integrity of the setup files before installation and of your system at any time after installation. Before you check your system with the Installation Integrity Validator, you should first ensure that it has been installed correctly. With the Integrity Validator, you have the option of customizing the path to the setup files. This is only necessary if you want to place the Integrity Validator outside the installation source.

Both validators have their own help, which you can call up in the command line with "-h" or "--help". This describes, for example, possible commands and the exit codes.

Changing the path to the setup files for the Integrity Validator

To change the path to the setup files, follow these steps:

1. Open Windows Explorer and navigate to the "IntegrityValidator" directory.
2. Open the "appsettings.json" file in a text editor.
3. Enter the desired path for "Path" in "InputDirectory".
4. Save the file.
   The Integrity Validator will now check the setup files that it finds under the specified path during validation.

Checking setup files with the Integrity Validator

To check the setup files with the Integrity Validator, follow these steps:

1. Open the Windows command prompt.
2. Navigate to the "IntegrityValidator" directory. This directory is in the installation source by default. If you have stored it somewhere else, go to that location.
3. To check the setup files, enter the following command:
   `IntegrityValidator.exe validate`
   The validation is performed and the result is displayed together with the exit codes.

Checking the installation of the Installation Integrity Validator

To ensure that the Installation Integrity Validator has been installed correctly on your system, follow these steps:

1. Open the Windows command prompt.
2. Enter the following command:
   `"%COMMONPROGRAMFILES%\Siemens\Automation\Installation Integrity Validator\InstallationIntegrityValidator.exe" --version`
3. Confirm the entry with <Return>.
   If the Installation Integrity Validator is installed correctly, the installed version of the tool will be displayed.

Checking the integrity of the system with the Installation Integrity Validator

To check the integrity of your system with the Installation Integrity Validator, follow these steps:

1. Open the Windows command prompt.
2. To start the validation, enter the following command:
   `"%COMMONPROGRAMFILES%\Siemens\Automation\Installation Integrity Validator\InstallationIntegrityValidator.exe" validate <possibly other options>`
3. Confirm the entry with <Return>.
   The validation is performed and the result is displayed together with the exit codes.
   See also: Error cases during the integrity check (Page 96)

3.9.3.3 Error cases during the integrity check

After the integrity check is performed with the Integrity Validator or the Installation Integrity Validator, the result of the validation is displayed. The colors of the texts have the following meanings:

- Green: Indicates a successful validation.
- Light blue: Displays information.
- Red: Displays validation errors and other error messages.
- Yellow: Displays warnings.

Possible error cases with suggested solutions

The following table shows the possible error cases with suggested solutions:

Error case	Suggested solution
Files missing	Reinstall the setup bundle that provided these files.
Additional files present	Delete the additional files.
Modified files present	Delete the modified files and reinstall the setup bundle that provided these files.
The catalog files for a directory were not found.	Reinstall the setup bundle that provided these files.
The installation directory for a product has not been found.	Contact the Siemens help desk and provide the installation logs.
The installation directory information for a product could not be retrieved.	Contact the Siemens help desk and provide the installation logs.
The self-check/integrity check for the CLI itself has failed for the Installation Integrity Validator. This means that the EXE file or the dependent assembly has been manipulated or is missing.	Reinstall the setup bundle to obtain a correct version of the Installation Integrity Validator.
Incorrect use of the "validate" command. Multiple verbosity modes have been specified.	Only one verbosity mode can be specified together with the "validate" command ("-v" or "-d"). Multiple verbosity modes are not allowed.

3.10 Corporate Designer

3.10.1 Improvements in Update 2

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved, among others, on account of the feedback received.

3.10.2 Improvements in Update 1

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved, among others, on account of the feedback received.

Font weights

The use of different font weights is displayed correctly in the Corporate Designer. Even when using a style created with the Corporate Designer with different font weights, the characters are displayed correctly both in the Engineering System and in Runtime.

3.11 WinCC Unified Data Hub

3.11.1 Improvements in Update 2

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved, among others, on account of the feedback received.

Documentation update

The documentation has been expanded and updated:

Unified Data Hub in the SIMATIC WinCC Unified online documentation

3.11.2 Improvements in Update 1

This update contains the following improvements and changes:

Stability and performance

The stability and performance have been improved, among others, on account of the feedback received.

Improvements in WinCC Basic, Advanced, Professional

4

4.1 Important notes

This page contains important information about product properties.

Installing WinCC Professional without WinCC Professional Runtime

If only WinCC Professional V21 Engineering is installed on a PC and error messages are displayed in the download dialog after installing an update, install at least the simulation from the DVD with WinCC Professional Runtime. It is recommended that you then install the latest WinCC Runtime Professional update.

Power tags that can be configured in the engineering system and the compatibility of licenses and devices

Available License	Devices that can be used						
	Unified devices			Additional devices			
	WinCC Unified PC	Comfort Panels	Basic Panels	Professional	Advanced	Comfort Panels	Basic Panels
WinCC Unified Basic ES	No	No	Yes	No	No	No	Yes
WinCC Unified Comfort ES	No	Yes	Yes	No	No	Yes	Yes
WinCC Unified PC 10k ES	Yes (10k*)	Yes	Yes	No	Yes	Yes	Yes
WinCC Unified PC 100k ES	Yes (100k*)	Yes	Yes	Yes	Yes	Yes	Yes
WinCC Unified PC max ES	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WinCC Basic	No	No	Yes	No	No	No	Yes
WinCC Comfort	No	Yes	Yes	No	No	Yes	Yes
WinCC Advanced	Yes (10k*)	Yes	Yes	No	Yes	Yes	Yes
WinCC Professional 512	Yes (10k*)	Yes	Yes	Yes (512*)	Yes	Yes	Yes
WinCC Professional 4096	Yes (10k*)	Yes	Yes	Yes (4096*)	Yes	Yes	Yes
WinCC Professional max **	Yes (100k*)	Yes	Yes	Yes	Yes	Yes	Yes

* Maximum number of possible PowerTags

** The Information refers to the engineering system. A max license means that there is no limit to the number of power tags in the configuration. However, this does not mean that they are available in unlimited form in Runtime. The licensed number of RT licenses, which is either 250k or 500k applies there.

Example:

The following devices can be configured with the WinCC Professional 4096 license:

- WinCC Unified PC up to 10k PowerTags
- WinCC Unified Comfort
- WinCC Unified Basic
- WinCC Professional up to 4096 PowerTags
- WinCC Basic/Comfort/Advanced

Redundancy

If a user is blocked on one server in a redundant system due to multiple failed login attempts, the information about the block status is not transmitted to the partner server and vice versa.

4.2 Improvements in Update 2 (Runtime Professional)

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.

Logs

The "+" and "-" buttons for expanding and collapsing the log sections are working correctly again and are retained even when inserting a title or back page.

Faceplates

Color properties of SVGHMIs used in the interface now function correctly.

Function trend control

The display of logging data has been improved.

Trend control on WinCC clients

The trends on the WinCC clients are now displayed correctly, without the need to manually add the server prefix or adjust the configuration during project migration.

Monitor keyboard

The monitor keyboard is displayed correctly in WinCC WebNavigator and WinCCViewerRT.

Object color

Changing the color of objects in Runtime works correctly after migrating from WinCC Professional V17 to V20.

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.

Remote communication

WinCC Runtime Professional V21 may experience unexpected behavior related to updated NIC driver and remote communication, such as:

- SIMATIC Shell does not display any other stations except for your own PC.
- The download of the project from the Engineering System does not work.
- Client-server communication cannot be established.

The unexpected behavior is corrected with WinCC Runtime Professional V21 Update 1.

After installing the update, please check the drivers of the network interface card to make sure they are up to date.

4.4 Removing an SQL instance

Contents

A Microsoft SQL Server 2022 instance is installed with the installation of WinCC V21.

If you already had a version of WinCC Runtime Professional installed, the SQL server is updated automatically.

Note

By removing WinCC Runtime Professional or WinCC Professional you do not remove the instance of the SQL server.

Uninstalling an SQL instance

If you want to uninstall an instance of the Microsoft SQL Server, follow these steps:

1. Open the Control Panel.
2. Click "Remove program".
3. From the list of installed programs, select the version of Microsoft SQL Server to remove and click "Remove/change".
4. Click "Remove" in the dialog.
5. In the "Select instance" dialog, select the instance "WINCC" and click "Next".
6. In the "Select functions" dialog, click "Select all" and then "Next".
7. In the "Function rules" dialog, click "Next".
8. In the "Ready to uninstall" dialog, click "Remove".
9. After removal is complete, click "Close" in the "Completed" dialog.