

SIEMENS

SIMATIC

Readme

Readme

Validity

1

Improvements in STEP 7

2

Improvements in WinCC

3

Improvements in WinCC
Unified

4

04/2023

A5E52423187-AA

Legal information

Warning notice system

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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

WARNING

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

Trademarks

All names identified by ® are registered trademarks of Siemens AG. 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.

Table of contents

1	Validity	5
2	Improvements in STEP 7	7
2.1	Improvements in Update 1	7
3	Improvements in WinCC	9
3.1	Important notes.....	9
3.2	Improvements in Update 1	10
3.3	Runtime Advanced.....	11
3.3.1	Important notes.....	11
3.3.2	Improvements in Update 1	11
3.4	Runtime Professional	12
3.4.1	Important notes.....	12
3.4.2	Improvements in Update 1	13
3.4.3	WinCC Certificate Manager.....	13
3.4.3.1	Introduction	13
3.4.3.2	Making certificates available.....	14
3.4.3.3	Installing a root certificate manually	16
3.4.3.4	Structure of the user interface	18
3.5	Panels.....	20
3.5.1	Improvements in Update 1	20
4	Improvements in WinCC Unified.....	21
4.1	Important notes.....	21
4.2	Improvements in Engineering and Runtime	24
4.2.1	System functions and scripts	24
4.2.2	User management	25
4.2.3	Diagnostics.....	26
4.2.4	Communication	28
4.3	Unified Engineering	30
4.3.1	General improvements (Unified ES Up1)	30
4.3.2	Improvements in configuring screens (Unified ES).....	31
4.4	Unified PC.....	35
4.4.1	Important notes.....	35
4.4.2	Improvements in Update 1	35
4.4.3	GraphQL.....	36
4.4.4	Improvements in SR1	44
4.5	Unified Comfort Panel	45
4.5.1	Important notes.....	45

Validity

Validity

This update is valid for the following products:

- STEP 7 Basic V18
- STEP 7 Professional V18
- WinCC Basic V18
- WinCC Comfort V18
- WinCC Advanced V18
- WinCC Professional V18
- WinCC Unified V18
- TIA Portal Openness V18

Note

If you modify your system after installing the update with the product DVD, you will have to perform the update again.

Improvements in STEP 7

2.1 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.

Port and service name for TIA Administrator V2

TIA Administrator V2 listens at port "8890".

The service of the TIA Administrator V2 that belongs to the process "node.exe" is "SiemensAwb".

TIA Administrator V1 keeps the previous port "8888" and service name "SiemensTiaAdmin".

Service name for TIA Portal project server

The name of the service associated with the process "Siemens.Automation.Portals.Server(.exe)" has been changed from "V[version number]prjsrv" to "prjsrv".

Improved search function in the information system

The search function has been improved with synonym recognition. When you search for a term, defined synonyms of the term are now also found.

Synonym recognition is available in English, German and Chinese.

Improvements in WinCC

3.1 Important notes

This page contains important information about product properties

Character sets after Windows 10 update

Since Windows 10 Update Version 1809, Windows allows the installation of character sets either with administrator rights for each user (command "Install for all users" in the shortcut menu) or for specific users. In order to use WinCC character sets without restrictions and load them onto an HMI device, the character sets must always be installed with administrator rights.

Note that the "Install" button in the view of a character set only initiates a user-specific installation.

Changing the installation directory

If you had installed the simulation with an earlier version of WinCC, you can no longer change the installation directory during installation.

Access to array variables via OPC UA

If you use WinCC Runtime Advanced as OPC UA server, reading array tags is only supported when the "OPC UA Server Array index range access" setting is activated.

Writing array variables is only possible if the OPC UA client supports the "Write array elements without IndexRange" setting.

Integrated Web server: Communication via OPC UA

If the error message 8010_0000 occurs during the communication of the integrated Web server via OPC UA, check the length of the transmitted arrays. If arrays are to be transmitted via OPC UA, the array may only have a maximum of 20 elements.

PLC code view

The performance of the PLC code view when opening the S7-GRAPH overview depends, among other things, on the number of jumps to be displayed.

3.2 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.

3.3 Runtime Advanced

3.3.1 Important notes

This page contains important information about product properties

Character sets after Windows 10 update

Since Windows 10 Update Version 1809, Windows allows the installation of character sets either with administrator rights for each user (command "Install for all users" in the context menu) or for specific users. In order to use WinCC character sets without restrictions and load them onto an HMI device, the character sets must always be installed with administrator rights.

Note that the "Install" button in the view of a character set only initiates a user-specific installation.

SIMATIC S7-1500 Software Controller V30.0

The update introduces version V30.0 of the SIMATIC S7-1500 Software Controller.

An integrated HMI connection is only possible with Software Controllers up to version 29.1.

As of Software Controller V30.0, integrated HMI connections are not supported and cannot be configured.

When the version of a configured Software Controllers is upgraded to V30.0, an Advanced Runtime existing on the same station is removed.

3.3.2 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.

3.4 Runtime Professional

3.4.1 Important notes

This page contains important information about product properties

Note

If Runtime is operated in kiosk mode with disabled shortcut keys in full-screen, you should disable access to online help in the ActiveX controls, otherwise the operator can gain access to the operating system.

Character sets after Windows 10 update

Since Windows 10 Update Version 1809, Windows allows to install character sets either with Administrator rights for each user (command "Install for all users" in the shortcut menu) or for specific users. In order to use WinCC character sets without restrictions and load them onto an HMI device, the character sets must always be installed with Administrator rights.

Note that the "Install" button regarding a character set only initiates a user-specific installation.

Deactivating NTLMv1 and SMBv1

The NTLMv1 and SMBv1 protocols can be disabled. Deactivating the protocols does not have any effect on the operation of WinCC Runtime Professional.

Note

Security risk from NTLMv1 and SMBv1

Use of the NTLMv1 and SMBv1 protocols is a significant security risk. Communications in the network could be compromised, for example, by man-in-the-middle attacks.

Depending on the operating system, the procedure for deactivating the protocols can be different.

Scripts on the WebUX or WebNavigator server

C or VBS scripts triggered by services such as Global Script, Alarm Logging, or Tag Logging are independent of Graphics Runtime and therefore run only on WebUX or WebNavigator servers.

- Any output of such functions, e.g. via `printf()` or `HMIRuntime.Trace()`, is not visible in the script diagnostics window on a WebUX or WebNavigator client.
- All access to Graphics Runtime from such functions are always made to the local Graphics Runtime of the WinCC server.

Automatic logout on multi-touch devices

To ensure that a configured automatic logout works on devices with a multi-touch screen even when using SIMATIC Logon V1.6 Update 3, configure any function, for example, to set a bit of a tag to the "Touched" event of the screen. This resets the logoff time timer when the screen is touched.

3.4.2 Improvements in Update 1

Contents

This update does not contain any improvements or changes relevant to WinCC Runtime Professional.

3.4.3 WinCC Certificate Manager

3.4.3.1 Introduction

WinCC Runtime Professional supports the use of CA-based HMI certificates (CA = Certificate Authority). You provide these certificates with the "WinCC Certificate Manager" application.

Note**No external certificate authority**

Issuance, distribution and installation of these certificates requires the use of the Certificate Manager.

The use of an external certificate authority or an intermediate certificate authority is not supported.

Functionality of the WinCC Certificate Manager

- Central creation and management of certificates in the network
- Creation of a certificate authority with:
 - Private key
 - Public key (root certificate)
 - CRL file (CRL = Certificate Revocation List)
- Issuance of the application certificates of the HMI devices
- Renewing existing certificates
- Encrypted export of the application certificates as well as the root certificate for manual distribution to HMI devices
- Encrypted import and installation of the certificates on the HMI devices

- Encrypted export and import of the root certificate, CRL file, and private key, as well as all device certificates for data backup and restore.
- Export of the root certificate and its CRL file for distribution to external communication partners of the HMI device
- Export of an updated CRL file for distribution to the HMI devices and their external communication partners

Available application certificates

With WinCC Certificate Manager you can create the following CA-based application certificates for WinCC Professional HMI devices:

- WebUX | WebNavigator certificate
- OPC UA server certificate
- OPC UA client certificate
- OPC UA tag import certificate

3.4.3.2 Making certificates available

Procedure

The procedure for providing the certificates as well as the operation of the Certificate Manager interface is largely the same for WinCC Professional and WinCC Unified. Follow the steps described in the WinCC Unified Certificate Manager user help.

You can find more information on the WinCC Unified Certificate Manager in Entry ID 109813308 in the Siemens Industry Online Support Portal in the "SIMATIC HMI WinCC Unified Engineering V18" help under "Runtime and Simulation > Certificate Manager".

Restrictions and special features

Deviating from the procedures and facts described in the user help for WinCC Unified Certificate Manager, the following applies to WinCC Professional:

Generation of application certificates

You can only generate the application certificates listed in section AUTOHOTSPOT.

Device binding of the certificates

When adding a device to the certificate authority, you specify what information is used to bind its application certificates to the device.

In the "New device" dialog, you have the option of entering multiple IP addresses in the "IP" field. Use ";" as separator.

Note

Enter the IP address of the device (own IP) as the first IP address.

The IP addresses are added to the Subject Alternative Name of the certificate.

Example: An HMI device is an OPC UA server and has a NAT router. The OPC UA clients communicate with the server via the NAT router. Enter the private IP address of the OPC UA Server HMI device (own IP) and the public IP address in Certificate Manager.

Distribution and installation of the application certificates

To distribute the certificate configuration of the certificate authority to the HMI devices and to install the certificate configuration of an HMI device on the device, follow the steps described in the WinCC Unified Certificate Manager user help for export, import and installation on Unified PCs.

For more information, see Entry ID 109813308 in the Siemens Industry Online Support Portal in the "SIMATIC HMI WinCC Unified Engineering V18" help under "Runtime and Simulation > Certificate Manager > Export, Import and Installation for Unified PCs".

Binding of the WebUX | WebNavigator certificate to the Runtime web page

If the Runtime Server web page has already been set up and you install the WebUX | WebNavigator certificate on the HMI device with Certificate Manager, the installation automatically binds the certificate to the Runtime web page.

If the website has not been set up yet, the binding cannot be performed successfully. Certificate Manager logs this via an entry in the "Output" area.

Installation of the root certificate on the WebUX/WebNavigator clients

To display Runtime in a WebUX/WebNavigator client, the root certificate of the WebUX/ WebNavigator application certificate must be installed as trustworthy on the client. It is not necessary to install the root certificate manually in the following cases:

Runtime access	Display via	Requirement
Local	WinCCViewerRT or Internet Explorer	The WebNavigator certificate has been installed on the HMI device with Certificate Manager.
	Chrome or Edge	The WebUX certificate has been installed on the HMI device with Certificate Manager.
Remote	WinCCViewerRT or Internet Explorer	The WebNavigator client device is also an HMI device. It has the same certificate authority as the HMI device, whose Runtime it displays in WinCCViewerRT or Internet Explorer. The server HMI device has a WebNavigator certificate. On both HMI devices the certificate configuration of the respective device has been installed with Certificate Manager.
	Chrome or Edge	The device of the WebUX client is also an HMI device. It has the same certificate authority as the HMI device, whose Runtime it displays in Chrome or Edge. The server HMI device has a WebUX certificate. On both HMI devices the certificate configuration of the respective device has been installed with Certificate Manager.

In other cases, install the root certificate manually on the WebNavigator clients and WebUX clients. Follow the steps described in section AUTOHOTSPOT.

3.4.3.3 Installing a root certificate manually

This section describes how to install the root certificate in order to display Runtime Professional in a WebUX/WebNavigator client.

Requirements

- On the certificate authority device:
 - A certificate authority has been created with WinCC Certificate Manager.
 - The Runtime Server HMI device has been added to the certificate authority and a WebUX | WebNavigator certificate has been added to the HMI device.
 - The certificate configuration of the HMI device has been exported.
- On the HMI device:

The certificate configuration of the HMI device has been installed with WinCC Certificate Manager.
- On the WebUX/WebNavigator client devices:
 - To display Runtime in a browser, the desired browser must be installed on the WebUX client device.
 - To display Runtime in Internet Explorer, the WebNavigator client must also be installed on the WebUX client device.
 - To display Runtime with WinCCViewerRT, the WebNavigator client must be installed on the WebNavigator client device.

Procedure

1. Export the root certificate on the certificate authority device using Certificate Manager. Follow the steps described in the WinCC Unified Certificate Manager user help.
2. Transfer the exported root certificate file to a storage location that the WebUX/ WebNavigator client device can access, such as a network folder or external storage medium. Follow the steps described in the WinCC Unified Certificate Manager user help. Your further procedure depends on which client you are using.
3. Edge and Chrome as the WebUX client:
 - Double-click the root certificate file on the WebUX client device. The root certificate is opened with the Windows standard form.
 - Select "Install Certificate".
 - In the certificate import wizard, select "Local Machine" as the storage location, "Trusted Root Certification Authority" as the certificate store.
 - Start the import.

4. Browser with its own certificate store as a WebUX client:
Manually install the root certificate on the WebUX client device in the certificate store of the browser. Follow the steps described in the user help of the browser.
For Firefox, for example, follow these steps:
 - In Firefox, click "Display certificates" under "Settings > Privacy & Security" under "Certificates".
 - In the "Certificate Management" window, select the "Certification authorities" tab.
 - Click "Import" and select the root certificate file.
 - In the window that opens, select the option "This certificate can identify websites" and confirm your selection.
5. Internet Explorer or WinCCViewerRT as WebNavigator client:
On the WebNavigator client device, manually copy the root certificate file in the Windows system certificate store to the trusted certificate authorities folder.

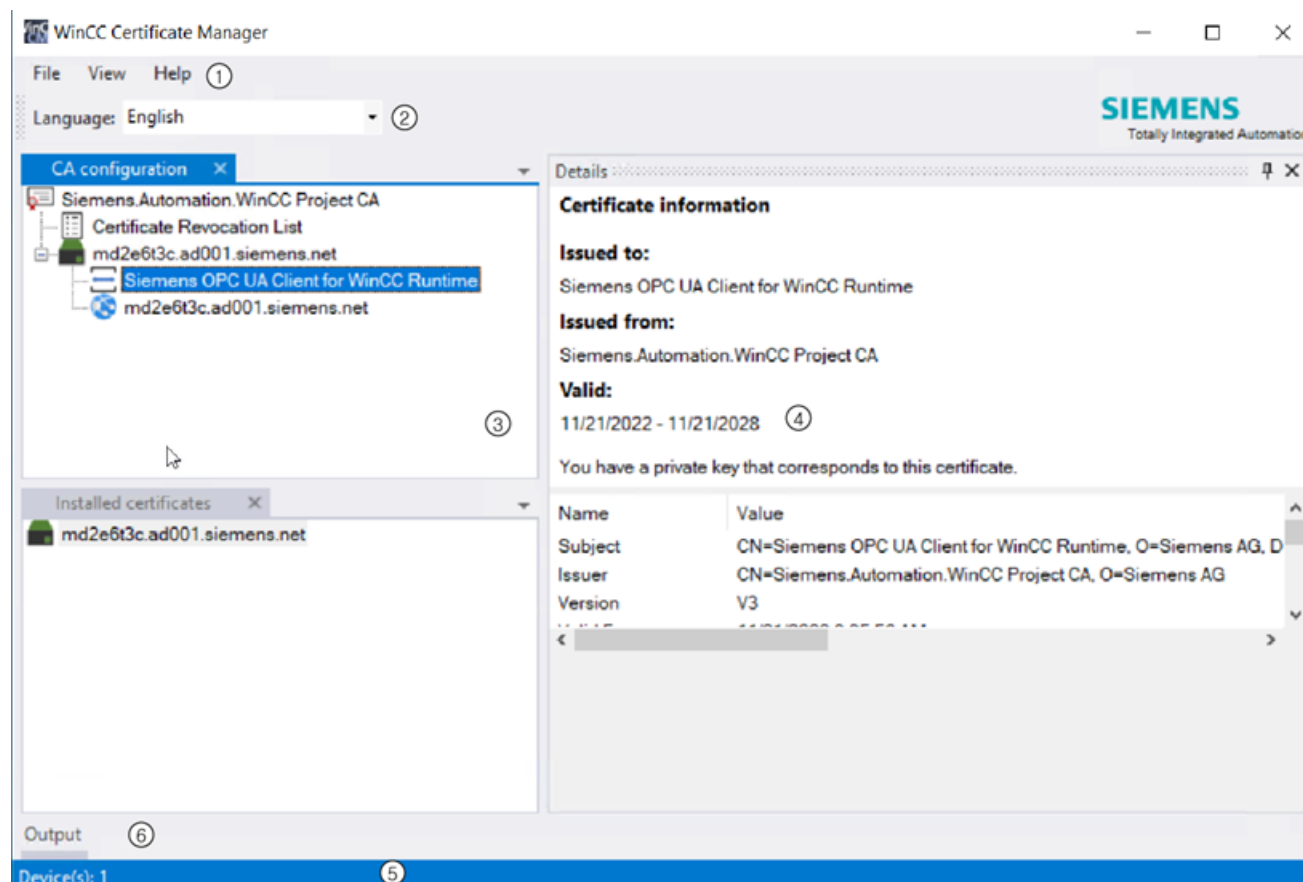
Result

The next time the client tries to connect the WebUX/WebNavigator client with Runtime, the client trusts the root certificate and thus also the WebUX certificate or the WebNavigator certificate from Runtime.

3.4.3.4 Structure of the user interface

Overview

The interface of WinCC Unified Certificate Manager has the following structure:




- ① Menu bar
- ② Toolbar
- ③ Work area with the "CA configuration" and "Installed certificates" tabs
- ④ "Details" area (fixed)
The "Details" area shows you detailed information about the certificate selected in the work area.
- ⑤ Information bar
- ⑥ "Output" area (hidden)
The "Output" area logs operator control actions.

You can customize the display of the interface to suit your needs. Follow the steps described in the WinCC Unified Certificate Manager user help.

Menu bar

Menu	Description
"File > Exit"	Closes Certificate Manager.
"View"	Configure which Certificate Manager interface elements you see. You can open or close the following interface elements: <ul style="list-style-type: none">• "Output" area• "Details" area• "CA configuration" tab• "Installed certificates" tab
"Help"	"About Certificate Manager" Opens a dialog with information about the installed software version.

Toolbar

Button	
	To change the user interface language

3.5 Panels

3.5.1 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 Unified

4.1 Important notes

This page contains important information about product properties.

Device versions with V18 Update 1

The new device version 18.0.0.1 was introduced for Unified PC and Unified Comfort Panels in order to be able to use the new functions which were introduced with V18 Update 1. Please note the following:

- If you open a project on a computer on which TIA Portal V18 is installed without an update, you cannot edit the devices contained there with device version 18.0.0.1.
- If you switch from a device version 18.0.0.1 to a previous device version, you can no longer use new functions such as switching the visibility of layers or the "Authorization" interface property for faceplates.
- The functions are also supported by higher device versions.

Unified PC

- Install Update 1 for WinCC Unified Runtime on the target device before loading a device with device version 18.0.0.1.

Images for Unified Comfort Panel

- Images can be downloaded from the Industry Online Support.
- Images are released independent of WinCC (TIA Portal).
- Use ProSave to import an image version that does not correspond to the configured device version onto a panel.
- If a new image only contains improvements for the runtime of the device, this version is not shown in the engineering system. In this case, use the current device version displayed in the engineering system.
- If the image 18.0.0.0 is installed on the device, install image download version V18.0 Upd.1 or higher before you load a device with the configured device version 18.0.0.1. When loading this device, activate the setting "Keep aspect ratio" in the "Load preview" dialog so that the new image version is transferred to the Panel. Alternatively, use ProSave.
- If you load a device with the configured device version 18.0.0.0, it is not absolutely necessary to update the image on the Panel. If you load a device with the configured device version 18.0.0.0 onto a panel with a higher device version, warnings are displayed pointing out the different versions. You can ignore them.

4.1 Important notes

Processes for WinCC Unified Simulation

Additional processes and services are also installed during the installation of the TIA Portal or components of the TIA Portal. You can find an overview of these processes, the associated services and their respective functions in the information system under "Installation > Overview of Processes and Services of TIA Portal Components".

The following processes for WinCC Unified Simulation are not listed in the information system for TIA Portal V18:

Table 4-1 WinCC Unified Simulation

Process	Corresponding service	Function
UAppStarterHost.exe	UAppStarterHost.exe	System function to jump from the web client to the TIA Portal for ProDiag scenarios.
OpcUAServerRTIL.exe	OpcUAServerRTIL.exe	Provides access to WinCC Unified via OPC UA protocol.
webums.exe	-	Web interface for user management with User Management Component (UMC) to manage UMC objects.
REPDataProviderHost.exe	-	Reporting enables the configuration of templates and the creation of Excel and PDF-based reports on production data.
WCCILgraphQLServer.exe	GraphQL server	GraphQL Web API

Character sets after Microsoft Windows 10 update

Since Windows 10 Update Version 1809, Windows allows the installation of character sets either with administrator rights for each user (command "Install for all users" in the shortcut menu) or for specific users. In order to use WinCC character sets without restrictions and load them onto an HMI device, the character sets must always be installed with administrator rights.

Note that the "Install" button in the view of a character set only initiates a user-specific installation.

Microsoft Edge limitation

If you want to start Runtime in Microsoft Edge and enter the address "https://localhost", the error message "INET_E_RESOURCE_NOT_FOUND" appears. In this case, use the address "https://localhost/WebRH".

Performance features for SIMATIC Unified PC communication

SIMATIC NET is required to use more than 10 connections.

Unified Collaboration

Collaboration devices must be synchronized in time.

Data types of trigger tags for alarms

Trigger tags of alarms must have the following data types:

- Discrete alarms: "Byte", "Word", "DWord", "LWord" or array with "Byte", "Word", "DWord", "LWord"
- Analog alarms: "Int", "Real", "LReal", "SInt", "USInt", "UInt", "UDInt" and "ULInt"

Audit Trail - Format

Depending on the viewer and the runtime language used, you have two options for the format:

File-based logging

File-based logging allows you to record up to 5000 logging tags in an SQL Lite database.

Database-based logging

Database-based logging allows you to record all logging tags up to the high limit in an MS SQL database.

View of Things - Asynchronous operations

In a VoT application, you cannot use asynchronous operations in scripts.

View of Things - Event

A VoT application cannot be compiled if the "Input finished" event is dynamized at an I/O field.

4.2 Improvements in Engineering and Runtime

4.2.1 System functions and scripts

This update contains improvements for:

- System functions

System function for opening the login dialog

The new `"HMIRuntime.UI.UserManagement.SysFct.ShowLoginDialog()"` system function is installed with the update. The `"ShowLogOnDialog"` function is available in the function list. With the system function, you open a login dialog for entering user name and password without leaving the currently displayed screen.

Only local user management supports the `"ShowLogOn Dialog"` system function.

System function for external control of the system diagnostics control

The new `"UI.SysDiag.ExecuteToolBarButton()"` system function is installed with the update. The `"ExecuteToolBarButton"` function (system diagnostics control) is available in the function list. The system function is used to control the buttons of the toolbar in the system diagnostics control.

System function for external control of the parameter set control.

The new `"UI.ParameterControl.SysFct.ExecuteToolBarButton()"` system function is installed with the update. The `"ExecuteToolBarButton"` function (parameter set control) is available in the function list. The system function is used to control the buttons of the toolbar in the parameter set control.

System function for external control of the alarm control

The new `"UI.Alarm.SysFct.ExecuteToolBarButton()"` system function is installed with the update. The `"ExecuteToolBarButton"` function (alarm control) is available in the function list. The system function is used to control the `"Single acknowledgment"` and `"Group acknowledgment"` buttons of the toolbar in the alarm control.

Extension of the `"InsertElectronicRecord"` system function

The `"HMIRuntime.Audit.SysFct.InsertElectronicRecord()"` system function is extended with the update. The `"InsertElectronicRecord"` function is available in the function list.

The `"Confirmation type"` parameter, which specifies how the action must be confirmed, has been extended:

- 0 = (None): No confirmation required, an entry is created in the Audit Trail.
- 2 = (Acknowledgement): Acknowledgment, the user must acknowledge the action; an entry is created in the Audit Trail.

- 3 = (Acknowledgement + Comment): Acknowledgment, the user must acknowledge the action and enter a comment; an entry is created in the Audit Trail.
- 4 = (Digital Signature): Electronic signature; a dialog window opens in which the user must enter the electronic signature; an entry is created in the Audit Trail.
- 5 = (Digital Signature + Comment): Electronic signature; a dialog window opens in which the user must enter the electronic signature and a comment; an entry is created in the Audit Trail.

The "Required function rights (optional)" parameter has been added. If the confirmation type requires an electronic signature, the function right required for the electronic signature can be specified:

- 0 = No function right required.
- 1 = The "First electronic signature" function right is required.
- 2 = The "Second electronic signature" function right is required.
- 3 = The "First electronic signature" and "Second electronic signature" function rights are required.

ActiveScreen property

The "ActiveScreen" property now always returns the screen that has the input focus. If the I/O field in a screen window or a faceplate has the input focus, ActiveScreen thus returns the screen that is displayed in the screen window or faceplate respectively. If you used ActiveScreen to edit the coordinates in the "OpenFaceplateInPopup" script function, for example, this may result in the popup being opened at a different location than it was in previous versions.

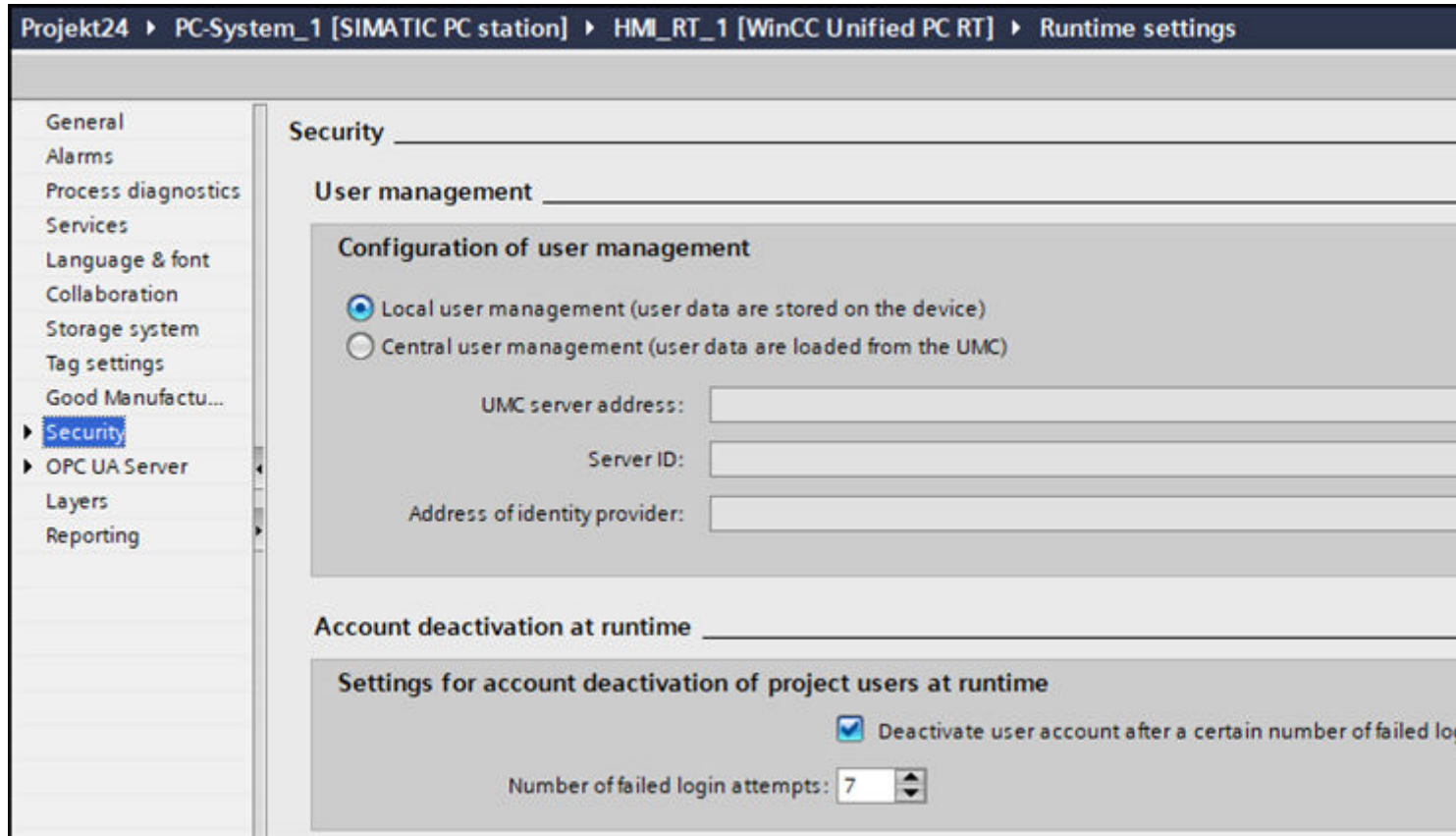
4.2.2 User management

This update contains improvements for:

- Incorrect login attempts

Incorrect login attempts

In the runtime settings, you can specify whether and after how many failed login attempts a user is blocked.



4.2.3 Diagnostics

This update contains improvements for:

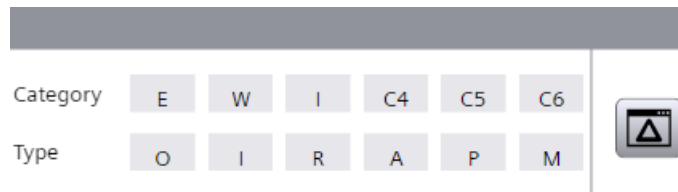
- Process diagnostics
- System diagnostics

Process diagnostics

The stability of process diagnostics objects has been improved.

ProDiag overview

The "ProDiag overview" object provides an overview of the current status of the configured monitoring in Runtime. When an error occurs, the type of error and the error category are determined in the ProDiag overview. You can navigate directly to the alarm control to find the error and you can jump from the corresponding alarm to the PLC code viewer control. You can display the affected program code in the PLC code viewer control.

**Note****Device dependency of the "ProDiag overview" object**

The "ProDiag overview" object is available for PC Runtime.

In the Inspector window, you customize the position, geometry, style, color and font types of the object. You can adjust the following properties in particular:

- Displayed buttons
- Names and colors for categories
- Names and colors for supervision types

You can display a maximum of 8 categories and 6 supervision types in the "ProDiag overview" object. The following pre-defined categories and supervision types are available:

Categories


Name	Categories
E (Error)	Error
W (Warning)	Warning
I (Info)	Information
C4 ... C8	Additional categories

Supervision types

Name	Supervision types
O (Operand)	Operand error
I (Interlock)	Interlock error
R (Reaction)	Reaction error
A (Action)	Action error
P (Position)	Position error
M (Message error)	Alarm

"Jump to Alarm Control" button

The "Jump to Alarm Control" button in the ProDiag overview is activated by default.

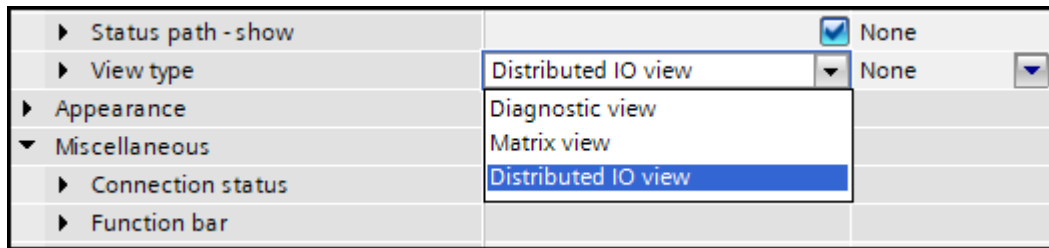
Button	Name	Function
	Jump to Alarm Control	Opens the configured alarm control with the error message after the button has been assigned system functions or scripts.

PLC code view

The "PLC code display" object is used to display the current program status of user programs that have been programmed in the graphical programming languages LAD and FBD as well as GRAPH.

System diagnostics control

The view type for the system diagnostics control object has been extended by the "Distributed IO view".



The "Distributed IO view" shows the distributed devices of the Profinet IO system.

The requirement is that only one PLC is configured with a Profinet IO system. Otherwise, Runtime switches back to the matrix view.

The "Home" button allows you to switch from the distributed IO view to the diagnostics overview. You can also jump to the diagnostics buffer from the distributed IO view.

If the Profinet IO system cannot be accessed, the diagnostics overview is displayed.

If you change the device version from 18.00.01.01 to 18.00.01.00, the matrix view is displayed and the distributed IO view is not visible in the selection field.

4.2.4 Communication

This update contains improvements for:

- Process communication
- OPC UA communication

SIMATIC S7-1500 Software Controller V30.0

Version V30.0 of the SIMATIC S7-1500 Software Controller is introduced with the update.

- Create a direct, integrated connection between a Software Controller and the HMI Runtime of a WinCC Unified PC by dragging and dropping a Unified PC on to Software Controller in the "Devices & Networks" editor.
- Configure the PC/PC interface in Microsoft Windows by assigning the S7ONLINE access point to the RT-VMM virtual network adapter.

- In the "Devices & Networks" editor you create connections to other PLCs, direct or routed. You use the S7ONLINE access point to create a direct connection between the HMI Runtime and an external PLC. You use the VMM Adapter access point to create a connection between the HMI Runtime and an external PLC via the Software Controller. Depending on the number of interfaces on the Software Controller, you can configure several of these connections in different subnets.
- Configure a connection between an HMI Runtime and a Software Controller if both devices are created on different PCs. To do this, assign the VMM Adapter access point to the HMI Runtime.

OPC UA

Unified OPC UA clients can now address OPC UA server tags with an address of up to 256 characters.

Application example: Addressing elements of a nested UDT.

4.3 Unified Engineering

4.3.1 General improvements (Unified ES Up1)

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.

Special characters in the installation path

Even when the installation path contains special characters, objects are always visible when inserted into a screen.

Segment-based backup for SQLite

Segment-based backup is supported as of V18 Update 1 for all archive types of the HMI devices Unified PC and Unified Comfort Panel.

The following requirement must be met:

- The "SQLite" database type must be enabled for the HMI device.

To use segment-based backup for SQLite, follow these steps:

1. Under "Archives", create one of the following archives:
 - Data log
 - Alarm log
 - Audit Trail
2. Under "Backup mode", select the "Path" option and specify a path for the backup.
For Unified Comfort Panel, the fully qualified mountpoint path is required.
Example: To use the "MyBackup" directory, specify the path "/media/simatic/data-storage-1/MyBackup". The mountpoint name is "data-stoarge-1".
A network folder can be configured using the mountpoint name specified in the Control Panel.

Upgrading a device version in the library

The update provides you the possibility to upgrade the device version of faceplate types and script module types in the library.

To upgrade the device version, follow these steps:

1. Select a faceplate type, script module type, or folder in the library.
2. Open the shortcut menu and select "Upgrade device version".
The "Upgrade device version" dialog box opens.

3. Select the required device version under "Lowest device version".
4. Select "OK".

Faceplates

The following improvements have been made for faceplates with V18 Update 1:

- Arrays are not supported when using the HMIUDT, WString, and WChar data types on the "Tag interface" tab of faceplate types. Therefore, the "Array limits" option has been disabled for these data types.
- Faceplates opened as a pop-up that enter the visible area due to changing the display in Runtime, e.g. enlarging the window, are now displayed.

Parameter sets and parameter set control

The following improvements have been made for parameter sets and the parameter set control with V18 Update 1:

- Parameter sets can be created in the parameter set control, even if the parameter set type elements consist of multiple levels.
- If you transfer new parameter sets into the parameter set control with the "Read from PLC" button, the parameter sets are then displayed as selected in the selection menu.

4.3.2 Improvements in configuring screens (Unified ES)

This update contains the following improvements and changes:

Screen management

In the "Devices" area of the project tree, you can find a new "Screen management" folder.

You can create exactly one top-level screen window with screen management. For the top-level screen window, select a screen from the ones available.

You configure all properties of the top-level screen window in the Inspector window.

Zoom&Scroll for top-level screen window

For a top-level screen window, configure the following properties in particular:

- Zoom factor
- Position and visibility of the vertical scroll bar
- Position and visibility of the horizontal scroll bar

You configure the properties:

- In the screen editor of the top-level screen window
- In the Inspector window of the screen, with a screen window under:
 - "Properties > Properties > Format > Zoom - factor".
 - "Properties > Properties > Format > Horizontal scroll bar - position".
 - "Properties > Properties > Format > Vertical scroll bar - position".

In the engineering system, you dynamize the properties using tags or scripts.

You can use the dynamic properties to control the behavior of the screen in runtime.

Resize to display

In the project, you can swap one device for another device with different display size. To adjust the configured screen size to the size of the new target device, use the "Resize to display" function:

1. Select the screen in the project tree.
2. Right-click on the screen. The shortcut menu is opened.
3. Select "Resize to display".

The configured screen size is adapted to the size of the new target device.

Extension of the toolbar in the screen editor

To efficiently configure the frequently used properties, the following functions have been added to the toolbar in the screen editor:



- Font:
 - Font
 - Font size
 - Format bold font
 - Format italic font
 - Underline
 - Strikethrough
 - Increase font size
 - Decrease font size
- Horizontal text alignment:
 - Left
 - Centered
 - Right

- Specify border width or line width
- Line type:
 - Solid
 - Dashed
 - Dotted
 - Dash-dot
 - Dash-dot-dot

The added functions are disabled for grouped objects when a group is selected.

The functions are enabled when a property in one or more objects can be changed.

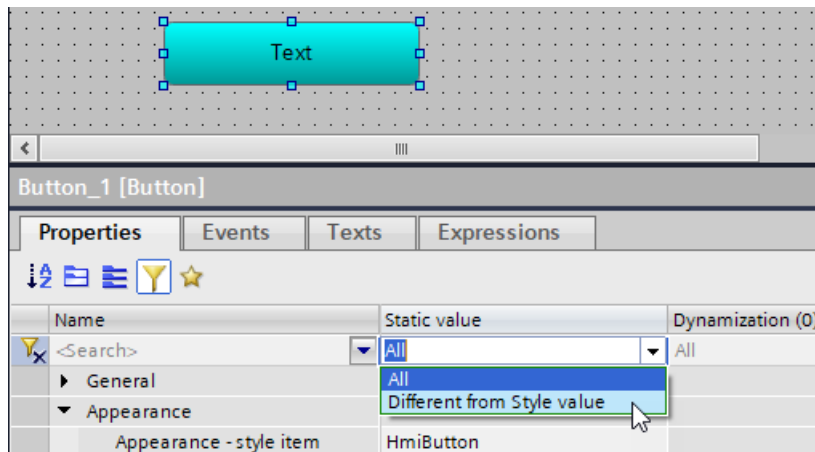
Highlighting and resetting properties of screens and screen objects

You can set one of the three pre-defined styles in the project tree of the project in the runtime settings.

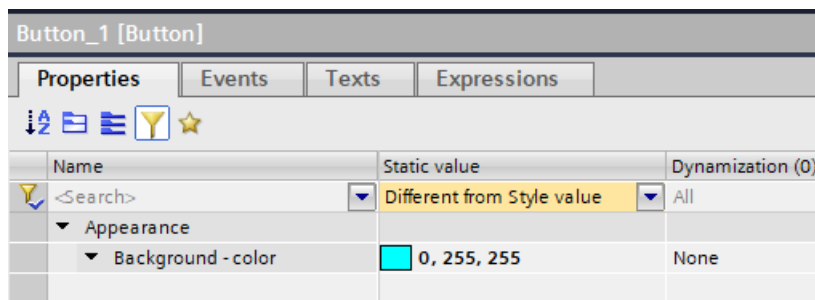
Within the selected style, you can change some properties of screens and screen objects in the Inspector window, for example the background color.

To find the changed properties, follow these steps:

1. Click on the "Filter" icon.
2. In the "Static value" column, select "Different from Style value".

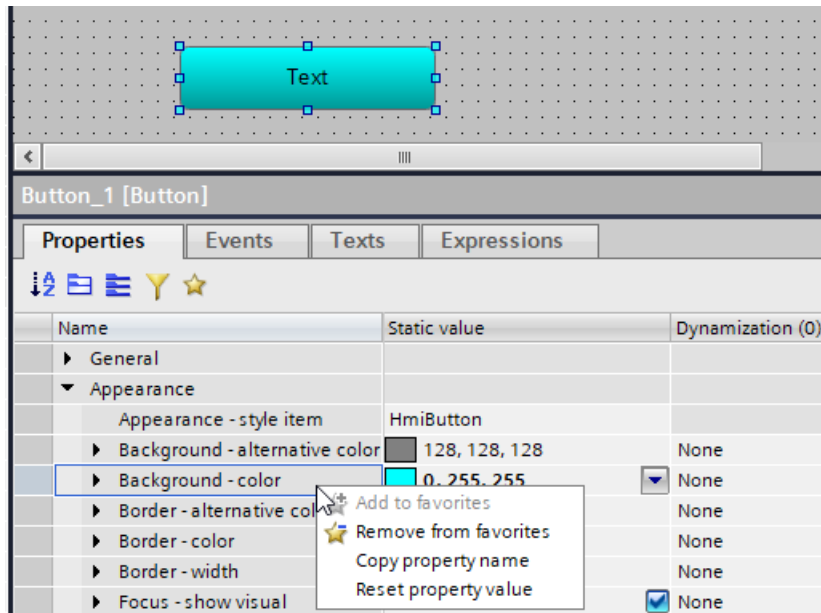


All changed properties are displayed and are formatted bold in the "Static value" column.



To reset the changed property value to the default value of the selected style, follow these steps:

1. Right-click on the property. The shortcut menu is opened.
2. Select "Reset property value".



The property value is reset to the default value of the selected style.

You can reset the following properties:

- Manually set properties.
- Properties that have a corresponding value in the current style.

The properties that do not have a style value are not formatted bolded or displayed in the filter, even when they are set manually.

Optimizing the display of properties

The overview in the Inspector window under "Properties" has been improved with the update. For properties that contain a collection of objects, the following changes have been made for the expandable table:

- Cells without content are displayed in space-saving manner.
- Check boxes and numeric values are displayed centered.
- Modified sorting of the columns is saved across projects.
- Modified visibility of the columns is saved across projects.

The "Selection items" table of the "Check box" element and the "Trend areas" table of the "Trend control" control are affected.

4.4 Unified PC

4.4.1 Important notes

This page contains important information about product properties.

Loading the logon page

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

WinCC Unified Tag Simulator

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

Unified Collaboration

The time of the Collaboration devices must be synchronized.

Project operations

The stability of project operations has been improved. Connection Manager now loads libraries from the correct path.

Microsoft Edge limitation

If you want to start Runtime in Microsoft Edge and enter the address "https://localhost", the error message "INET_E_RESOURCE_NOT_FOUND" appears. In this case, use the address "https://localhost/WebRH".

Activating the script debugger

To activate the script debugger in SIMATIC Runtime Manager, the logged-on user must belong to the Windows user group "SIMATIC HMI".

4.4.2 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.

Trend control

The trend control for curves whose visibility is dynamized in Runtime has been improved.

4.4.3 GraphQL

Escaping

Attribute values and object names, for example of tags or alarms, may contain special characters which are escape sequences in the Runtime system or the programming language of the GraphQL client. Escape sequences do not represent a text but start a special function during the program execution.

To ensure that a special character is interpreted as a normal character, prefix the character in the GraphQL client program code with a masking character (EN: Escaping).

Note

Masking character

Runtime system: \$

Apollo Studio: \

If a special character is an escape sequence in the Runtime system and the programming language, combine the masking characters.

Example

The character " is an escape sequence in the Runtime system and Apollo Studio. To, for example, address a tag with the name MOT1 " enter the following string: MOT1\$\ "

Structure of the server response

The attributes delivered in the server response have the same sequence as in the selection set of the client query.

Subscription of tags during the delta download

If a GraphQL client subscribes to two tags and their tag names are renamed in a delta download such that the tags swap their names, the subscription is now executed further.

Security through access control

The access of GraphQL clients to Runtime can be restricted as follows:

- Linking access to function rights
An operation of the GraphQL client is only executed if the user who is logged on at the client has the required rights.
Reading rights are required for querying and subscriptions, and writing rights for mutations.
- Controlling access to the object level
The read access and write access of the user logged on at the GraphQL client is defined per object:
 - Read access to an object without authorization: The object is removed from the server response.
 - Write access to an object without authorization: The operation is aborted.

Reading logging alarms

Requirement

- The user who is logged in to Runtime for the GraphQL client has "GraphQL - read access" rights or "GraphQL - read/write access" rights in Runtime.

Description

```
loggedAlarms (
  systemNames: [String]
  filterString: String
  filterLanguage: String
  languages: [String]
  startTime: Timestamp
  endTime: Timestamp
  maxNumberOfResults: Int
): [LoggedAlarm]
```

Operation name	loggedAlarms
Operation type	query
Function	Queries the logged alarms from the server.

4.4 Unified PC

Input parameters	<p>systemNames:</p> <ul style="list-style-type: none"> • Optional • Corresponding to the query <code>activeAlarms</code> <p>filterString, filterLanguage, languages:</p> <ul style="list-style-type: none"> • Optional • Corresponding to the query <code>activeAlarms</code> To filter the logged alarms on the basis of the attributes defined in the type <code>LoggedAlarm</code>. <p>startTime, endTime:</p> <ul style="list-style-type: none"> • Optional • For filtering Restricts the query to logged entries whose alarm status was changed the last time within the time frame defined by <code>startTime</code> and <code>endTime</code>. • Data type: <code>Timestamp</code> <p>maxNumberOfResults</p> <ul style="list-style-type: none"> • Optional • Upper limit for the number of the requested alarm entries • Data type: <code>Int</code>
Selection set	<p>Mandatory specification</p> <p>Specify which attributes the server returns for the queried logged alarms. You can request the attributes defined in the <code>LoggedAlarm</code> type.</p>
Server response	Supplies the attributes requested in the selection set for the queried logged alarms as key-value pairs of a JSON data record.
Error messages (code and description)	<ul style="list-style-type: none"> • 0: Success • 301: Syntax error in query string • 302: At least one of the requested languages is invalid (or not logged) • 303: The provided filter language is invalid (or not logged)

Data type "LoggedAlarm"

The data type `LoggedAlarm` provides the following attribute:

- `hasComments`
Shows whether comments on the logged alarm are pending.
Data type: `boolean`

With exception of the following attributes the data type `LoggedAlarm` also provides the same attributes as the data type `ActiveAlarm`:

- `flashing`
- `connectionName`
- `sourceID`
- `systemSeverity`
- `loopInAlarm`
- `loopInAlarmParameterValues`

- `path`
- `userResponse`

These alarm attributes are not logged.

Acknowledging and resetting alarms

You have the following options:

- Acknowledging or resetting all active alarms of one or more configured alarms.
- Acknowledging or resetting specific alarm instances of one or more configured alarms.

Note

Alarms without group acknowledgment or group reset

The configuration of a configured alarm can prevent a group acknowledgment or group reset. In this case you have to acknowledge or reset each alarm instance in an own operation call.

The execution of `acknowledgeAlarms` and `resetAlarms` aborts when the operation for two or more configured alarms is called and one of the alarms does not allow group acknowledgment or group reset.

Requirement

- The user who is logged in to Runtime for the GraphQL client has the "GraphQL - read/write access" right in Runtime.
- The state machine of the alarms specified in the `input` parameter requires acknowledgement or acknowledgement and confirmation of the alarms.

Description "acknowledgeAlarms" and "resetAlarms"

```

acknowledgeAlarms (
  input: [AlarmIdentifierInput]
): [ActiveAlarm]
resetAlarms (
  input: [AlarmIdentifierInput]
): [ActiveAlarm]
```

Operation name	<code>acknowledgeAlarms</code>	<code>resetAlarms</code>
Operation type	<code>mutation</code>	
Function	Acknowledges the active alarms specified in the input parameter <code>input</code> .	Resets the alarms specified in the input parameter <code>input</code> .
Input parameters	<code>input:</code> <ul style="list-style-type: none"> • Mandatory parameters • Data type: <code>[AlarmIdentifierInput]</code> • Specifies the alarms to be acknowledged or reset 	
Selection set	Mandatory specification Specify which attributes the server returns for the queried alarms. You can request the attributes defined in the <code>ActiveAlarm</code> type.	

Server response	Supplies the attributes requested in the selection set for the alarms as key-value pairs of a JSON data record.
Error messages (code and description)	<ul style="list-style-type: none"> • 0: Success • 2: Cannot resolve provided name • 304: Invalid object state • 305: The alarm cannot be read / acknowledged / reset in current state • x: Alarm instance does not exist

Data type "AlarmIdentifierInput"

The data type has the following attributes:

- name
 - Mandatory specification
 - The fully qualified name of a configured alarm
Alarm of a tag: <System name>::<Tag name>:<Alarm name>
Alarm of an element of a structure tag or array: <System name>::<Tag name>.<Element path>:<Alarm name>
Delimiter for the components of the element path: "."
 - Data type: String
- instanceID
 - Optional
 - The ID of an alarm instance of the configured alarm
 - If "0" is transferred as the instanceID or if no instanceID is transferred, all active alarms of the configured alarm are acknowledged.

Enabling and disabling alarms

You have the following options:

- Disabling one or more configured alarms
The alarm condition of these alarms is no longer checked. No new alarm instances occur.
- Enabling one or more disabled configured alarms
The alarm condition of these alarms is checked again. New alarm instances occur again.

Requirement

- The user who is logged in to Runtime for the GraphQL client has the "GraphQL - read/write access" right in Runtime.

Description "disableAlarms" and "enableAlarms"

```

disableAlarms (
  names: [String]
): [AlarmMutationResult]
enableAlarms (
  names: [String]
): [AlarmMutationResult]
```


Operation name	disableAlarms	enableAlarms
Operation type	mutation	
Function	Disables the alarms specified in the input parameter names.	Enables the alarms specified in the input parameter names.
Input parameters	names: <ul style="list-style-type: none"> • Mandatory parameters • Data type: [String] • The fully qualified name of one or more configured alarms. The alarms are disabled or enabled. Detailed information on how to specify the fully qualified name of a configured alarm, is available further up in the section on acknowledging and resetting of alarms > Data type "AlarmIdentifierInput". 	
Selection set	Mandatory specification Specify which attributes the server returns for the queried alarms. You can request the attributes defined in the AlarmMutationResult type.	
Server response	Supplies the attributes requested in the selection set for the alarms as key-value pairs of a JSON data record.	
Error messages (code and description)	<ul style="list-style-type: none"> • 0: Success • 2: Cannot resolve provided name 	

Data type "AlarmMutationResult"

The data type has the following attributes:

- alarmName
 - The fully qualified name of the configured alarm
Detailed information on how to specify the fully qualified name of a configured alarm, is available further up in the section on acknowledging and resetting of alarms > Data type "AlarmIdentifierInput".
 - Data type: String
- error
 - Feedback on the success of the operation
 - Data type: Error

Shelving alarms and canceling the shelving

Description "shelveAlarms"

```
shelveAlarms (
    names: [String]
    shelveTimeout: Timespan
): [AlarmMutationResult]
unshelveAlarms (
    names: [String]
): [AlarmMutationResult]
```

Operation name	shelveAlarms	unshelveAlarms
Operation type	mutation	
Function	<p>Shelves the alarms. The attribute <code>suppressionState</code> of the alarms is set to <code>0x2 Shelved</code>.</p> <p>If the GraphQL client has subscribed to one of the shelved alarms, the client receives a notification on the shelving.</p> <p>The shelved alarms are still available and logged in the system. If the GraphQL client has subscribed a shelved alarm, it keeps receiving notifications on changes at the alarm from the Runtime system.</p> <p>The implementation of the GraphQL client controls how the client:</p> <ul style="list-style-type: none"> Deals with notifications about subscribed shelved alarms, for example, whether to suppress them. Deals with operation calls that include shelved alarms, for example whether to disallow read access to these alarms. 	<p>Cancels the shelving of the alarms again. This creates a log entry.</p>
Input parameters	<p>names:</p> <ul style="list-style-type: none"> Mandatory parameters Data type: <code>[String]</code> The fully qualified name of one or more configured alarms. <p>The active alarm instances of these alarms are shelved or their shelving is canceled.</p> <p>Detailed information on how to specify the fully qualified name of a configured alarm, is available further up in the section on acknowledging and resetting of alarms > Data type "AlarmIdentifier-Input".</p>	
	<p>shelveTimeout:</p> <ul style="list-style-type: none"> Optional Time interval after which the shelving of the alarms is automatically canceled. <p>Must not be greater than the timeout configured in Runtime.</p> <p>If no value is transferred, the timeout configured for Runtime is used.</p> <ul style="list-style-type: none"> Data type: <code>Timespan</code> 	-
Selection set	<p>Mandatory specification</p> <p>Specify which attributes the server returns for the queried alarms. You can request the attributes defined in the <code>AlarmMutationResult</code> type. Information on the type can be found further above.</p>	
Server response	<p>Supplies the attributes requested in the selection set for the alarms as key-value pairs of a JSON data record.</p>	
Error messages (code and description)	<ul style="list-style-type: none"> 0: Success 2: Cannot resolve provided name 	

Subscribing to the redundancy status of the host

Requirement

- The user who is logged in to Runtime for the GraphQL client has "GraphQL - read access" rights or "GraphQL - read/write access" rights in Runtime.

Description "reduState"

Operation name	reduState
Operation type	subscription
Function	Subscribes to the redundancy status of the host to which the connected GraphQL server belongs, in a redundant system. Subscribes to the redundancy status of the host connected with the GraphQL client in a redundant system.
Input parameters	-
Selection set	Mandatory specification Specify which attributes the server returns for the queried alarms. You can request the attributes defined in the <code>ReduStateNotification</code> type.
Server response	Supplies the attributes requested in the selection as key-value pairs of a JSON data record.

Note

Passive redundancy status

If the GraphQL client receives a notification that the status is passive, log off the client from the connected GraphQL server. Connect the client with the GraphQL server of the active host.

Type "ReduStateNotification" and "ReduStateValue"

The `ReduStateNotification` type has the following attributes:

value

- Data type: `ReduStateValue`

notificationReason

- Data type: `String`

The `ReduStateValue` type has the following attributes:

- value:
The redundancy status as defined in the enumeration `ReduState`:
 - ACTIVE
The host of the GraphQL server currently connected with the GraphQL client is active.
 - PASSIVE
The host of the GraphQL server currently connected with the GraphQL client is passive.
- timestamp:
 - Data type: `Timestamp`

4.4.4 Improvements in SR1

This update contains the following improvements and changes:

Stability and performance

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

Assigning text lists and graphics lists for reports

In a report template, when you map a text list or graphics list to the column of a data source item, the list values are now read correctly both in the add-in and when the report is generated.

For more information on this, refer to the user help on the Excel add-in under the keyword "Assigning text lists and graphic lists".

Symbolic I/O field in the "Output" mode

If a symbolic I/O field is linked to a resource list in "Output" mode, the applicable list entry is displayed.

Loading from WinCC Unified Online Engineering

Stability of loading from WinCC Unified Online Engineering has been improved.

System tag "@CurrentLanguage"

The value of the system variable ""@CurrentLanguage is changed correctly even after a delta load when changing the Runtime language.

Contexts in the PI Option "Performance Insight"

Stability of archiving of PFI contexts has been improved:

- A memory leak has been corrected.
- Stability of context archiving after loading has been improved:

Error output

Crash in error output when accessing non-existent variables of a faceplate has been corrected.

Updating the browser

Stability on updating the browser has been improved.

4.5 Unified Comfort Panel

4.5.1 Important notes

This section contains important information about product properties.

Configuring connections

For the Unified Comfort Panel in the engineering system, only configure control connections that are also available and used in plant operation.

IP addresses

The IP subnet 172.x.x.x is reserved for SIMATIC Edge communication and must not be used for general network communication.

Notes on the "Edit user" dialog

Cancel RFID assignment process

If you edit the RFID assignment of a user via the "Edit user" dialog and cancel the subsequent assignment process via the "Cancel" button in one of the dialogs, the entries in the user list may not be displayed correctly.

To update the list, select another entry in the navigation area of the Control Panel and then again "Security" > "User management".

RFID activation or PIN change logs the user in

In the following cases, the selected user is logged in to the "Edit user" dialog immediately after the change operation:

- You have switched the "Enable authentication via RFID card" option from "disabled" to "enabled".
- You have switched the "PIN required for authentication with RFID card" option.

PIN dialog

In the following cases, the PIN dialog is displayed again after editing a user via the "Edit user" dialog.

- You have switched the "Enable authentication via RFID card" option from "enabled" to "disabled".
- You have switched the "PIN required for authentication with RFID card" option.

In this case, close the PIN dialog via the "Cancel" button.

Starting Runtime

You can start Runtime directly after loading a project or via the "Start Runtime" button in the Control Panel.

4.5 Unified Comfort Panel

If background processes are running on the HMI device and Runtime is started at the same time, the dialog "Runtime Start" is displayed with the error message "An error occurred while starting project".

Acknowledge the dialog and restart Runtime after some time.

Browser download directory

On a Unified Comfort Panel, the browser download directory is: "/home/industrial/download"

Using the central user management

The following sections contain important information on parameters of the "TIA User Management Component (UMC)".

Auto logoff time

The UMC parameter "Account Policy > Auto logoff time (minutes)" is not supported by Unified Comfort Panels. A user logged on to the Unified Comfort Panel must log off manually.

Must change Password

The UMC parameter "Status > Must change Password" is not supported by Unified Comfort Panels. Make sure that this option is disabled for all users of a Unified Comfort Panel.

Password duration (days)

An expired password cannot be changed on a Unified Comfort Panel. To log on a user whose password has expired, change the password directly in the "TIA User Management Component".

"Plant overview" control for Unified Comfort Panel not supported

With version V18, the "Plant overview" control is supported only for Unified PC. If you use the control under Unified Comfort Panel, an error message is output during compilation. The control must be cleared before compiling.

Alarm view

Flashing on range violation

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

Scroll bars

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

"Show recent" button

The "Show recent" function is only supported in conjunction with ascending sort order.

Moving columns

Moving columns within the alarm view is not supported.

Status bar

If a text was configured for the first element in the status line and an image for the second element, the image may not be displayed immediately after loading. In this case, perform a screen change.

Filter alarms

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

Dynamize visibility of columns

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

Parameter set control

If a parameter set control view was maximized and again reduced, it may happen that the view is not properly displayed. Elements such as parameter set type number or parameter set number may not be visible. Resize the width of the view once to properly display its contents again.

