SIMATIC HMI

WinCC (TIA Portal) Readme Runtime Professional

Readme

Online documentation

03/2022
Online documentation

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

All names identified by ® are registered trademarks of Siemens 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.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: Online documentation
Ⓟ 04/2022 Subject to change

Table of contents

Validity 1

Validity

This update is valid for the following products:

- WinCC Runtime Professional V17

Note

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

Important notes 2

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.

Improvements in Update 4

3

This update contains the following improvements and changes:

Setting the background color via VB script

The background color property can also be set correctly for the following objects using VB script: Line, polyline, circular arc, ellipse arc, connector

Improvements in Update 3 SR1

4

4.1 Improvements in Update 3 SR1

This update contains the following improvements and changes:

Stability and performance

Improvements including stability and performance have been made based on the feedback received.

Screen keyboard

With the screen keyboard, the response time when opening and the behavior when exiting Runtime have been improved.

Symbolic I/O field

When changing the visibility of object groups, for example, the behavior of the symbolic I/O fields used has been improved.

Screen window in multi-monitor mode

The display of independent screen windows in multi-monitor mode has been improved.

Startup behavior of Runtime

The startup behavior of Runtime has been improved when there is no network connection.

ALARM_DQ alarms

Alarm_DQ alarms are displayed correctly in the alarm control.

Allen-Bradley

If non-configured tags are used, communication via the Allen-Bradley channel is improved.

WebNavigator

WebNavigator Clients V17 can also connect to WebNavigator servers with different versions.

4.2 Secure communication via certificate

Runtime Professional certificate-based communication has been enhanced.

Overview

Supported S7 PLCs

Runtime Professional V17 can now communicate with the following S7 PLCs via certificates:

- S7-1500 PLCs as of firmware 2.9
- S7-1200 PLCs as of firmware 4.5

Note

All of the following statements apply only to S7 PLCs with this firmware.

Expansions

Certificate-based communication between Runtime Professional and S7 PLCs has been enhanced as follows:

- Communication between HMI devices and S7 PLCs with a non-integrated connection now supports self-signed certificates.
- Upgrading S7 PLCs has been simplified. Upgrading in the TIA Portal is no longer mandatory. An S7 PLCs that was only upgraded in the field now communicates with the HMI device via a self-signed certificate. The self-signed certificate is automatically loaded from the PLC into the certificate store of the HMI device.

To use these functions, enable the "ForceSecure" option on the HMI device.

Using self-signed certificates

The following self-signed certificate options are available:

- Use a self-signed certificate generated in the TIA Portal.
  Use the certificate created automatically when adding an S7 PLC or upgrading an existing S7 PLC. Or select certificate settings that differ from the default settings and generate a self-signed certificate yourself.
  When loaded, the certificate is copied to the Runtime project folder.
- Use a self-signed default certificate.
  Do not provide a certificate for the PLC in the TIA Portal and instead enable the "ForceSecure" option on the HMI device for the PLC connection type.
  A self-signed certificate is generated when loading to the PLC. The certificate is copied to the certificate store of the HMI device during the first attempt to make a connection between the PLC and the HMI device. After the certificate is copied to the folder with trusted certificates, it is used for communication.

Enabling or disabling the "ForceSecure" option

Introduction

The "ForceSecure" option ensures that communication between the HMI device and the S7 PLC is protected by a certificate for the following connections:

- Non-integrated connections

- Connections for which no certificate has been configured in the TIA Portal

If the option is enabled and no PLC certificate is found in the Runtime project folder, Runtime searches for a suitable certificate in the "trusted" folder of the HMI device's certificate store.

Note

This option does not affect communication with S7 PLCs that do not support certificates.

Default setting

This option is disabled by default for integrated connections, non-integrated connections and device proxies.

Procedure

Note

It is recommended to enable the option for all connection types.

To configure the option for an HMI device, proceed as follows:

1. Create the "ForceSecure.xml" file.
2. Copy the following XML structure into the file:
```
<?xml version="1.0"?>
   <root>
   <NonIntegrated>true</NonIntegrated>
   <Integrated>true</Integrated>
   <IntegratedProxy>true</IntegratedProxy>
   </root>
```
3. To disable certificate store evaluation for one of the connection types, set its node to "false".

   Note

   Certificate-protected communication for non-integrated connections is not possible in this case.

   For integrated connections and device proxy, certificate-protected communication is possible only after upgrading the PLCs in the TIA Portal.

4. Copy the file on the engineering device into the TIA project directory of the project to which the HMI device was added into the following folder:
   "…`\AdditionalFiles\Rdp`"
5. Compile and download the HMI device.
   Your settings will be applied to the communication between the HMI device and its connected S7 PLCs.

To configure the "ForceSecure" option centrally for all projects created in the TIA Portal, proceed as follows:

1. Perform steps 1 to 3 as described above.
2. Copy the file on the engineering device into the program directory "C:\ProgramData\Siemens \Automation\ConfigFiles\RDP".
3. To use a different configuration for individual projects, proceed as described in steps 1 to 4 above.

If the XML file is located in the program directory and in the TIA project directory, the configuration from the project directory takes effect.

Upgrading S7 PLCs

The following options are available when using self-signed certificates.

Upgrading in the field without upgrading the S7 PLC in the TIA Portal

Requirement:
On the HMI device connected to an S7 PLC, the "ForceSecure" option is enabled for the S7 PLC connection type.

Procedure:

1. Upgrade the HMI device in the TIA Portal.
2. Replace the S7 PLC and the HMI device in the field.
3. Download the S7 PLC and the HMI device.
   After the download, the Runtime project folder does not contain a certificate for this S7 PLC.
4. Start Runtime.
   At the first attempt to make a connection, the self-signed certificate is automatically loaded from the S7 PLC. It ends up in the certificate store of the HMI device in the following folder:
   `%PROGRAMDATA%\Siemens\Automation\device-certificate-store \untrusted`
5. Copy the PLC certificate in the certificate store of the HMI device to the folder with the trusted certificates manually or per script:
   `%PROGRAMDATA%\Siemens\Automation\device-certificate-store\trusted \certs`

Upgrading in the field and upgrading in the TIA Portal

Procedure for integrated connections and device proxy:

1. Upgrade the S7 PLC and HMI device in the TIA Portal.
2. Replace the S7 PLC and the HMI device in the field.

3. Download the S7 PLC and the HMI device.
   After the download, the Runtime project folder contains the certificate for this S7 PLC.
4. Start Runtime.
   HMI device and PLC trust each other's certificates. There are no further steps for you.

Procedure for non-integrated connections:

1. Upgrade the S7 PLC and HMI device in the TIA Portal.
2. Enable the option "ForceSecure" for the non-integrated connection type for the HMI device.
3. Replace the PLC and the HMI device in the field.
4. Download the PLC and the HMI device.
   After the download, the Runtime project folder does not contain a certificate for this S7 PLC.
5. Start Runtime.
   At the first attempt to make a connection, the self-signed certificate is automatically loaded from the S7 PLC. It ends up in the certificate store of the HMI device in the following folder:
   `%PROGRAMDATA%\Siemens\Automation\device-certificate-store\untrusted`
6. Copy the PLC certificate in the certificate store of the HMI device to the folder with the trusted certificates manually or per script:
   `%PROGRAMDATA%\Siemens\Automation\device-certificate-store\trusted\certs`
   HMI device and PLC trust each other's certificates.

Alternatively, you can export the PLC certificate from the TIA Portal in advance and copy it to the "`...\trusted\certs`" folder before starting Runtime. The certificate file must have the following name:

"S7PlusChannel_<PLC_IP>.der", e.g. "S7PlusChannel_192.168.0.1.der"

5 Improvements in Update 3

Contents

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

Improvements in Update 2

6

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 Update 1

7

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.