SIEMENS

SIMATIC HMI

WinCC
WinCC Runtime Professional
Readme

System Manual

Online help printout

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

Security note (Professional)

1

Security information

Siemens offers IT security mechanisms for its automation and drive product portfolio in order to support the safe operation of the plant/machine. Our products are also continuously developed further with regard to IT security. We therefore recommend that you keep yourself informed about updates and upgrades for our products and always use the latest version of each product. You can find information on this at: http://support.automation.siemens.com You can register for a product-specific newsletter here.

For the safe operation of a plant/machine, however, it is also necessary to integrate the automation components into an overall IT security concept for the entire plant/machine, which corresponds to the state-of-the-art IT technology. You can find information on this at:

http://www.siemens.com/industrialsecurity.

Products used from other manufacturers should also be taken into account here.

Passwords

Various passwords are set by default in WinCC. For security reasons, you should change these passwords.

- The default password for the Sm@rtServer and for the integrated Web server is "100".
- For the user "Administrator", the default password is "administrator".

Integrated Web server

It is always possible on a PC to access HTML pages in Runtime, even though the option"HTML pages" is disabled. Setup always installs the standard pages of the Web Server on the PC. Assign an administrator password to prevent unauthorized access to the pages.

Communication via Ethernet

In Ethernet-based communication, end users themselves are responsible for the security of their data network. The proper functioning of the device cannot be guaranteed in all circumstances; targeted attacks, for example, can lead to overload of the device.

Ending Runtime automatically

If automatic transfer is enabled on the HMI device and a transfer is started on the configuration PC, the running project is automatically stopped.

The HMI device then switches autonomously to "Transfer" mode.

After the commissioning phase, disable the automatic transfer function to prevent the HMI device from switching inadvertently to transfer mode.

Transfer mode can cause undesired reactions in the system.

To block access to the transfer settings and thus avoid unauthorized changes, assign a password in the Control Panel.

Network settings

The following tables show the network settings of each product which you need in order to analyze the network security and for the configuration of external firewalls:

WinCC Professional (without simulation)					
Name	Port number	Transport protocol	Direction	Function	Description
ALM	4410*	TCP	Inbound, Outbound	License service	This service provides the complete functionality for software licenses and is used by both the Automation License Manager as well as all license-related software products.
HMI Load	1033	TCP	Outbound	HMI Load (RT Basic)	This service is used to transmit images and configuration data to Basic Panels.
HMI Load	2308	TCP	Outbound	HMI Load (RT Advanced)	This service is used to transmit images and configuration data to Panels.
RPC	**	UDP	Inbound, Outbound	Client / server & ES communication (CCAgent)	This service is used by WinCC Professional and WinCC Runtime Professional.
* Default port that can be changed by user configuration					
** Port is assigned automatically					

WinCC Simulation for Basic Panels					
Name	Port number	Transport protocol	Direction	Function	Description
HMI Load	1033	TCP	Inbound	HMI Load (RT Basic)	This service is used to transmit images and configuration data to Basic Panels.
EtherNet/IP	44818	TCP	Outbound	Ethernet/IP channel	The Ethernet/IP protocol is used for connections to Allen Bradley PLCs.
	2222	UDP	Inbound	Ethernet/IP channel	The Ethernet/IP protocol is used for connections to Allen Bradley PLCs.
Modbus TCP	502	TCP	Outbound	Modbus TCP channel	The Modbus TCP protocol is used for connections to Schneider PLCs.
RFC 1006	102	TCP	Outbound	S7 channel	Communication with the S7 controller via Ethernet/PROFINET
Mitsubishi MC	5002	TCP	Outbound	Mitsubishi MC channel	The Mitsubishi protocol is used for connections to Mitsubishi PLCs.

WinCC Simulation for Panels and Runtime Advanced					
Name	Port number	Transport protocol	Direction	Function	Description
DCP	---	Ethernet	Outbound	PROFINET	The DCP protocol (Discovery and Basic Configuration Protocol) is used by PROFINET and provides the basic functionality for locating and configuring PROFINET devices.
LLDP	---	Ethernet	Inbound, Outbound	PROFINET	The LLDP protocol (Link Layer Discover Protocol) is used by PROFINET for topology detection.
SMTP	25	TCP	Outbound	SMTP Communication	This service is used by WinCC Runtime Advanced to send e-mails.
HTTP	80*	TCP	Inbound	Sm@rtServer	The Web server is only available when Sm@rtService is activated. The used port may differ depending on automatically selected settings.
RFC 1006	102	TCP	Outbound	S7 channel	Communication with the S7 controller via Ethernet/PROFINET
NTP	123	UDP	Outbound	Time-of-day synchronization	The NTP protocol (Network Time Protocol) is used for time-of-day synchronization in IP-based networks.
SNMP	161	UDP	Outbound	PROFINET	The SNMP client functionality is used by STEP 7 to read status information from PROFINET devices.
HMI Load	2308	TCP	Outbound	HMI Load (RT Advanced)	This service is used to transmit images and configuration data to Panels.
HTTPS	443*	TCP	Inbound	Sm@rtServer	The Web server with HTTPS protocol is only available when Sm@rtService is activated. The used port may differ depending on automatically selected settings.
VNC server	5900*	TCP	Inbound	Sm@rtServer	This service is only available when Sm@rtService is activated.
	5800*	TCP	Inbound	Sm@rtServer	This service is only available when Sm@rtService is activated.
VNC client	5500	TCP	Outbound	Sm@rtServer	This service is only available when Sm@rtService is activated.
* Default port that can be changed by user configuration					

WinCC Simulation for Runtime Professional					
Name	Port number	Transport protocol	Direction	Function	Description
RPC	**	UDP	Inbound, Outbound	Client / server & ES communication (CCAgent)	This service is used by WinCC Professional and WinCC RT Professional.
RPC	**	UDP	Inbound, Outbound	Client / server communication (CCEServer / CCEClient)	This service is used by WinCC Runtime Professional.

WinCC Simulation for Runtime Professional					
HTTP	80	TCP	Inbound, Outbound	Client / server communication (CCEServer / CCEClient)	This service is used by WinCC Runtime Professional.
RFC 1006	102	TCP	Outbound	S7 channel	Communication with the S7 controller via Ethernet/PROFINET
OPC UA	4840	TCP	Inbound	OPC UA server	This service is required for primary communication via OPC UA. It is activated and configured during installation.
OPC UA discovery	52601	TCP	Inbound	OPC UA server	The OPC UA discovery service provides information about installed OPC servers on the same system. This one will be active if installed and configured via the OPC UA server.
DCOM	135	TCP	Inbound	OPC server	This service is part of the Windows operating system. DCOM functionality is part of Microsoft Windows operating system. Because communication via OPC (DA) is based on DCOM, this service is required to initialize OPC (DA) connections.
DCOM	**	TCP	Inbound	OPC server	The communication via OPC (DA) is based on DCOM and uses unspecified ports assigned by the system. This should be taken into consideration when using OPC (DA) and creating rules for the firewall.
HTTP	80	TCP	Inbound	OPC server	This service is required for primary communication via OPC XML. It is activated and configured during installation.
NetBIOS	137	UDP	Inbound	OPC server	This service is part of the Windows operating system. Access to this service is required by OPC-Scout, for example, for browsing.
NetBIOS	138	UDP	Inbound	OPC server	This service is part of the Windows operating system. Access to this service is required by OPC-Scout, for example, for browsing.
SNMP	161	UDP	Outbound	SNMP OPC server	This service is used by the SNMP OPC server to change or query data on network drives, for example.
SNMP Traps	162	UDP	Inbound	SNMP OPC server	This service is used by the SNMP OPC server to query events from network drives, for example.
** Port is assigned automatically					

Special considerations for Windows 7

<div style="text-align: right; font-size: 2em">2</div>

Contents

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

Permission for the starting Runtime

To start WinCC Runtime Professional or WinCC Runtime Advanced, a user must be a member of the automatically created group, "Siemens TIA Engineer".

Working with standard user rights

If you are working with standard user rights in Windows 7, "User Account Control (UAC)" cannot be disabled.

The "User Account Control" is enabled in Windows 7 by default.

For more information on the "User Account Control, refer to the online help for Windows 7.

Slow response from the screen keyboard and SmartServer

The following programs may start and respond very slowly under Windows 7 and Windows 2008 servers:

- Microsoft OSK screen keyboard and HMI TouchInputPC
- SmartServer: <Ctrl+Alt+Del> shortcut in the logon dialog

The delay is caused by the callback for the Internet certificate validation.

Remedy:

Locate the following files on the product DVD under:
Support\Windows7\CRL_Check or CD_RT\ Support\Windows7\CRL_Check\
:

- DisableCRLCheck_LocalSystem.cmd
- DisableCRLCheck_CurrentUser.cmd

1. Run the "DisableCRLCheck_LocalSystem.cmd" file with administrator rights. Select the command "Run as administrator" from the shortcut menu of the file.
2. Reboot the PC.

If the problem persists, follow these steps:

1. Double-click the file and run the "DisableCRLCheck_CurrentUser.cmd" file with user rights.

2. Reboot the PC.

Note

The callback for the certificate validation is disabled for all users or PCs. To restore the original state, perform the following files:

- RestoreDefaults_LocalSystem.cmd
- RestoreDefaults_CurrentUser.cmd

You can find the files in the following directory of product DVD:

- Support\Windows7\CRL_Check or CD_RT\Support\Windows7\CRL_Check\

Installation

<div style="text-align: right; font-size: 3em;">3</div>

Contents

Information that could not be included in the online help.

Operating system message for SIMATIC USB drivers

An operating system message relating to the SIMATIC USB driver is issued on the operating system Windows Server 2003 R2 StdE SP2.

This message must be acknowledged with "Yes" as soon as possible after the message has been issued. The message may be in the background and therefore not be immediately visible. After a certain period of time, the setup continues with the next component. The SIMATIC USB drivers are then not installed and can not be used.

Installation on a computer with regional setting "Turkish"

If the computer is operated with the regional setting "Turkish" at the time of the installation, WinCC Runtime Professional cannot be started.

Hotfix for SIMATIC NET

Install hotfixes for the following products:

- SIMATIC NET CD V8.0 SP1 for Windows 7: Hotfix 1 for SIMATIC NET CD V8.0 SP1

You can find the hotfixes in the Service & Support area of the Siemens web site under the entry ID 12660737.

Security settings in the Security Controller

You can find the "Securitiy Controller" in the start menu under "Start > Programs > Siemens Automation". You can display and print security settings using the program.

However, do not use "Edit > Make settings" and/or the function "Make setting" in the menu.

Runtime

4

4.1 Notes on operation in Runtime

Contents

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

Special characters in the user view

Special characters, such as / " § $ % & ' ?, are not permitted when entering a name or the password in the user view.

Language behavior - Layout of on-screen keyboard

The layout of the on-screen keyboard is not switched when the runtime language changes.

Tag values exceed the maximum length

You enter a character string in a string tag via an I/O field. If the character string exceeds the configured number of tags, the character string will be shortened to the configured length.

Empty message texts

Runtime is running with a project. The project is saved on a network drive.

In the event of interruptions to the network drive connection, Runtime may attempt to load message texts from the network drive.

In the event of disconnection, the alarm window or the alarm view remains empty.

To avoid this, copy the project to a local drive before the starting the project in Runtime.

Complete download in Service mode

If you need to perform a "complete download" to the OS in Service mode from the engineering station, Runtime automatically stops and then starts again.

The project is then no longer in Service mode.

In this state, the power supply is interrupted and WinCC Runtime no longer starts automatically on the OS.

Remedy:

1. Switch the project manually to Service mode after you have performed the "complete download".

2. Close the project manually.

3. Activate Service mode.

4. Start Runtime again using the surrogate icon in the taskbar.

4.2 Notes on operation of Runtime Professional

Contents

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

User authorizations within the operating system

1. All user must be added to the "SIMATIC HMI" user group. This also applies to users who want to open WinCC projects remotely.

2. The storage folders of the projects must have the NTFS authorizations "SIMATIC HMI" with full access and "SIMATIC HMI Viewer" with read access. The authorizations must be inherited for all subordinate objects.

3. Members of the Windows user group "SIMATIC HMI" should not simultaneously be members of the Windows user group "SQLServer2005MSSQLUser$<Computername> $WINCC". The members of this group have administrator rights to the SQL server. Therefore remove all Windows users from this group for whom restricted access to the WinCC database is sufficient.

Windows 7 / Windows Server 2008: Locking key combinations

If you want to lock key combinations under Windows 7 or Windows Server 2008, you must change the group policies in the administrative tools of the operating system.

A detailed description of this can be found in the FAQ with the entry ID "44027453" in the SIMATIC Customer Online Support:

Internet: WinCC FAQ 44027453 (http://support.automation.siemens.com/WW/view/en/ 44027453)

Undocked toolbars

If the setting "Always on Top" is used for the Windows taskbar, undocked toolbars can be hidden behind the Windows taskbar in Runtime. Follow the steps below to show the toolbars again:

1. Select the "Properties" command in the shortcut menu of the taskbar.

2. Deselect "Keep taskbar on top of other windows".

Fault in the connection between the server and the client

If the connection between the server and client is faulty, check the settings of the PG/PC interface. TCP/IP(Auto) should not be used for the "Interface Parameter Assignment Used". Used fixed IP addresses instead.

Fault in the connection between the server and the client

If the computer is simultaneously used as a server with the Engineering System and a client cannot establish the connection to the server, you should check the releases set on the server.

1. Exit Runtime on the server.

2. Select the command "Find computer..." in the shortcut menu of the network environment on the desktop of the server.

3. Enter the name of the server as the computer to be found.

4. Open the computer found to see the released directories.

5. Remove all the releases that begin with "WinCC_Project_HMI". Information on this is available in the documentation for the operating system.

This malfunction is caused by the use of the command "Save as..." in conjunction with the startup of the Runtime of this new project. You can make copies of the projects for backup purposes using the "Save as..." command. You should, however, continue to work with the original project.

Language setting for Runtime Professional

With Runtime Professional, illegible texts may occur during runtime if the settings in the operating system for "Language for non-Unicode programs" do not match the selected Runtime language. This setting must also be the same on the client and the server for client/server applications.

Therefore, first check in the Control Panel under "Regional and Language Options > Advanced" whether the setting for "Language for non-Unicode programs" is the same as the Runtime language.

Starting WinCC Runtime Professional

If Engineering System and Runtime are operated on a computer, Runtime or simulation for a project opened in the engineering system should only be started and ended via the TIA portal. Other options, for example, the symbol in the taskbar information area, should not be used.

Setting the services for the SQL server

In order to ensure the full functionality of the SQL server for WinCC and WinCC Runtime, you have to check the SQL server settings.

1. Start "Programme > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager" in the start menu.

2. Click "SQL Server Services" in the tree.

3. Check the services "SQL Server (WinCC)","SQL Server (WINCCPLUSMIG)" and "SQL Server Browser". "Automatic" must be entered for "Start Mode". "LocalSystem" must be entered for "Log On As". Change the settings, if necessary.

4. Click "SQL Server Network Configuration" in the tree.

5. Click "Protocols for WinCC".

6. Check the "TCP/IP" protocol. "Enabled" must be entered for "Status". Change the settings, if necessary.

"Report system error" in WinCC Runtime Professional

The "Report system error" functionality is limited in WinCC Runtime Professional in conjunction with an S7-300 or S7-400. In an alarm view, only one alarm is ever displayed for each diagnostics type. Alarms on other errors of the same diagnostics type are not displayed.

Faceplate instances in a screen

The number of faceplate instances per screen is not limited. However, you should be aware of the fact that the number of faceplate instances used, or the use of scripts in the faceplate instances, will have an impact on performance.

WinCC interface and 64-bit operating system

The open interfaces of WinCC Runtime Professional do not offer native 64-bit support. Runtime API, VBS and the WinCC OleDB provider are primarily affected by this. To be able to use WinCC interfaces with a 64-bit operating system, note the following:
- VB scripts cannot be started by simply double-clicking. You must explicitly use the 32-bit version under "syswow64\wscript.exe".
- .NET applications that use the WinCC API have to be explicitly compiled as 32-bit applications, not with "AnyCPU", but with "x86".
- C++ applications must not be compiled as 64-bit applications.

4.3   Communication

Contents

Information that could not be included in the online help.

Communication via routing

The communication from the connection partners in various subnets can be routed via the following links: PROFINET, PROFIBUS, MPI.

Options

5

5.1 DataMonitor

Contents

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

Approved versions of Microsoft Office

The following versions of Microsoft Office are approved for "Excel Workbooks":

- Office 2003 SP3
- Office 2007 SP2
- Office 2010 SP1 (32-bit version)

The use of the 64-bit version of Office 2010 is not enabled.

Installation on a PC with Microsoft Office 2003 SP2

An error alarm that is output at the end of the setup of "Excel Workbook Wizard" on a computer running Microsoft Office 2003 SP2 indicates that an update for Office 2003 has failed. Proceed as follows:

1. Open the "InstData\KB907417\Media" directory on the medium containing the installation files for WinCC Runtime Professional.
2. Start the update in accordance with the operating system language.
3. Restart the Setup of WinCC Runtime Professional to install the "Excel Workbook Wizard".

Removal of WinCC Runtime

If you also want to use DataMonitor after removing WinCC Runtime Professional, you have to perform a repair of the installation as follows:

1. Open the Control Panel.
2. Double-click on "Add/Remove Programs".
3. Select "SIMATIC WinCC/DataMonitor client" in the list of programs installed
4. Click on the "Change/Remove" button.
5. Select the setting "Repair" in the WinCC DataMonitor setup".

Excel Workbooks and Excel Reports

The regional settings of the operating system must match the Office language installed on the computer running Excel Workbooks and Excel Reports. You may also have to adapt the system account settings.

To configure the regional and language settings for system accounts in Windows 7 and Windows 2008(R2), select the "Regions and Language > Administration" dialog in the Control Panel.

Opening Excel workbooks on a computer not connected to the internet

If you want to used the DataMonitor client on a computer not connected to the internet, you must deactivate certificate checking. To do this, follow these steps:

1. Open Internet Explorer.

2. Select the "Internet options" command from the "Tools" menu.

3. Click "Advanced".

4. In the field "Security" deactivate the setting "Check for publisher's certificate revocation".

Opening Excel workbooks with Excel 2010

Due to safety settings, the automatic connection of an Excel workbook with the server does not work in Excel 2010.

If you wish to enable automatic connection, deactivate the "Enable protected view for files originating from the internet" and "Enable Protected View for files located in potential unsafe locations" settings in Excel 2010 under "Files > Options > Trust Center > ProtectedView".

Name of the user groups

The name of the user groups differs at certain locations of the Online Help from the actually created user groups. The following assignment is valid:

SIMATIC Report Administrators corresponds to DM_Admin

SIMATIC Report Users corresponds to DM_User

Connecting archives

If you have connected archives by means of the WinCC objects ""f(x) trend view", f(t) trend view", "table view" or "alarm view", you can no longer connect these archives with the DataMonitor.

If you have connected archives with the DataMonitor, you can no longer connect these archives by means of the WinCC objects ""f(x) trend view", f(t) trend view", "table view" or "alarm view".

Excel-Workbook on a PC with Windows 7

If you operate Excel-Workbook on a PC with Windows 7, you need to deactivate the "Aero Glass" function for the appearance.

Importing configuration data

If you load a project to a device via an external data medium, DataMonitor cannot export a correct XML file on this device.

The exported XML file can then no longer be used for importing configuration data.

Reports in DataMonitor

If the PC with WinCC Runtime Professional performs a restart and then switches back to service mode without Windows login, the following print jobs and Excel workbooks are no longer output:

● Cyclically controlled print jobs and Excel workbooks

● Event-controlled print jobs and Excel workbooks

Remedy:

1. Open the "Reports" area in DataMonitor.

2. Click the "Print jobs" or "Excel Workbooks" tab.

The cyclically and event-controlled print jobs and Excel workbooks are executed again after this selection.

5.2 WebNavigator

Contents

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

Removal of WinCC Runtime

If you also want to use WebNavigator after removing WinCC Runtime Professional, you have to perform a repair of the installation as follows:

1. Open the system controller.

2. Double-click on "Add/Remove Programs".

3. Select "SIMATIC WinCC/WebNavigator client" in the list of programs installed

4. Click on the "Change/Remove" button.

5. Select the setting "Repair" in the WinCC/WebNavigator setup".

Access via Web client

A user can only get access via a Web client if a screen released for Web access has been assigned to him as the start screen in the user administration.

To release a screen for Web access:

1. Select the "Properties" command in the shortcut menu of a screen.

2. Activate the "Web access" option under "Properties > Web access".

To assign a start screen to a user:

1. In the user administration, select the user to whom you would like to assign a start screen.

2. Click "Properties > General" > Web options > Settings in the Inspector window to specify a start screen. You can only select screens which have been released for Web access.

Virus scanner Trend Micro OfficeScan

It is not recommended to use the virus scanner of Trend Micro OfficeScan in combination with WebNavigator, as this virus scanner may have an adverse impact on screen loading times.

Index

L

Language behavior
    On-screen keyboard, 13

M

Maximum length
    Tag, 13

P

Permitted characters
    User view, 13

S

Screen keyboard
    Language behavior, 13
Security Controller, 11
Security settings
    Security Controller, 11

T

Tag
    Maximum length, 13

U

User view
    Permitted characters, 13