

# SIEMENS

## SIMATIC HMI

### WinCC WinCC Runtime Advanced readme

#### System Manual

Security information

1

Special considerations for  
Windows 7

2

Installation

3

Runtime

4

Online help printout




07/2013

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.

 <b>DANGER</b>
indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken.
 <b>WARNING</b>
indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.
 <b>CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.
<b>NOTICE</b>
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:

 <b>WARNING</b>
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

<b>1</b>	<b>Security information.....</b>	<b>5</b>
<b>2</b>	<b>Special considerations for Windows 7.....</b>	<b>9</b>
<b>3</b>	<b>Installation.....</b>	<b>11</b>
<b>4</b>	<b>Runtime.....</b>	<b>13</b>
4.1	Notes on operation in Runtime.....	13
4.2	Notes on operation of Runtime Advanced.....	14
4.3	Communication.....	14
	<b>Index.....</b>	<b>17</b>



# Security information

## Security information

Siemens provides automation and drive products with industrial security functions that support the secure operation of plants or machines. They are an important component in a holistic industrial security concept. With this in mind, our products undergo continuous development. We therefore recommend that you keep yourself informed with respect to our product updates. Please find further information and newsletters on this subject at:

<http://support.automation.siemens.com>

To ensure the secure operation of a plant or machine it is also necessary to take suitable preventive action (e.g. cell protection concept) and to integrate the automation and drive components into a state-of-the-art holistic industrial security concept for the entire plant or machine. Any third-party products that may be in use must also be taken into account. Please find further information at:

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

## 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 Advanced (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.

\* Default port that can be changed by user configuration

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.

WinCC Simulation for Panels and Runtime Advanced					
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					





## Special considerations for Windows 7

### 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:

You can find 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\
- 

### **On-screen keyboard**

Once you have opened the TIA Portal, you can no longer call the on-screen keyboard.

To call the on-screen keyboard in Windows, use the following command: "Start > All Programs > Accessories > Ease of access > On-screen keyboard".

# Installation

## 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.



# Runtime

## 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:

### 4.3 Communication

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 Advanced

### Contents

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

### .Net-Controls in Runtime

If you have incorporated a .Net Control in your project as "Specific .Net-Control", you have to copy the files belonging to these controls to the installation directory of WinCC Runtime, e.g. "C:\ProgramFiles\Siemens\Automation\WinCC RT Advanced". Otherwise, the control cannot be loaded in Runtime.

## 4.3 Communication

### Contents

Information that could not be included in the online help.

### Using "DTL" data type for area pointers

Use the "DTL" data type for configuration of area pointers "Date/time" and "Date/time PLC". The "DTL" data type supports time stamp information in the nanosecond range. Because Basic Panels support time stamp information only down to the millisecond range, you will encounter the following restrictions when using the area pointers:

- Area pointer "Date/time"  
For transmission of time information from a Basic Panel to the PLC, the smallest unit of time is 1 millisecond. The value range from microseconds to nanoseconds of the "DTL" data type will be filled with zeros.
- Area pointer "Date/time PLC"  
For transmission of time information from a PLC to a Basic Panel, the area from microseconds to nanoseconds will be ignored. The time information will be processed on the panel down to milliseconds.

### **Communication via routing**

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

### **RT Advanced communication via Station Manager (SIMATIC NET) with a SIMATIC S7 1200**

The following restrictions apply to the PC that communicates with SIMATIC S7 1200 via router using WinCC RT Advanced or RT Professional:

- Windows 7: Only with SIMATIC NET 8.1 installation
- Windows XP: Communication via Station Manager (SIMATIC NET) is not supported.

These restrictions also apply if you are using WinAC MP or Station Manager. Connections with the help of the Station Manager of Runtime Advanced are always treated as routed connections.





# Index

## A

- Area pointer
  - Date/time, 14
  - Date/time PLC, 14

## D

- DTL data type
  - Restriction, 14

## L

- Language behavior
  - On-screen keyboard, 13

## M

- Maximum length
  - Tag, 13

## P

- Permitted characters
  - User view, 13

## S

- Screen keyboard
  - Language behavior, 13

## T

- Tag
  - Maximum length, 13

## U

- User view
  - Permitted characters, 13

