SIMATIC HMI

WinCC
WinCC Runtime Advanced readme

System Manual
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  Security information..............................................................................................................................5
2  Installation............................................................................................................................................11
3  Runtime................................................................................................................................................13
   3.1  Notes on operation in Runtime..............................................................................................13
   3.2  Notes on operation of Runtime Advanced.............................................................................15
   3.3  Communication.....................................................................................................................15
Index.....................................................................................................................................................17
Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens’ products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Any third-party products that may be in use must also be taken into account. For more information about industrial security, visit http://www.siemens.com/industrialsecurity (http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx)

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com (http://support.automation.siemens.com)

Passwords

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

- On HMI devices with version V11 or V12, the password "100" is preset for the Sm@rtServer and for the integrated Web server. A default password is not preset for HMI devices with version V13.
- 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 on the HMI device. The HMI device then
switches autonomously to "Transfer" mode. Transfer mode may cause undesired reactions in the system.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Port number</th>
<th>Transport protocol</th>
<th>Direction</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALM</td>
<td>4410*</td>
<td>TCP</td>
<td>Inbound, Outbound</td>
<td>License service</td>
<td>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.</td>
</tr>
<tr>
<td>HMI Load</td>
<td>1033</td>
<td>TCP</td>
<td>Outbound</td>
<td>HMI Load (RT Basic)</td>
<td>This service is used to transmit images and configuration data to Basic Panels.</td>
</tr>
<tr>
<td>HMI Load</td>
<td>2308</td>
<td>TCP</td>
<td>Outbound</td>
<td>HMI Load (RT Advanced)</td>
<td>This service is used to transmit images and configuration data to panels.</td>
</tr>
</tbody>
</table>

* Default port that can be changed by user configuration

### WinCC Simulation for Basic Panels

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

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

* Default port that can be changed by user configuration

## PROFINET protocols for Panels and Runtime Advanced

<table>
<thead>
<tr>
<th>Name</th>
<th>Port number</th>
<th>Transport protocol</th>
<th>Direction</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCP</td>
<td>---</td>
<td>Ethernet</td>
<td>Outbound</td>
<td>Lifelist, PROFINET Discovery and configuration</td>
<td>The DCP protocol (Discovery and basic Configuration Protocol) is used by PROFINET and provides the basic functionality for locating and configuring PROFINET devices.</td>
</tr>
<tr>
<td>LLDP</td>
<td>---</td>
<td>Ethernet</td>
<td>Inbound, Outbound</td>
<td>PROFINET Link Layer Discovery protocol</td>
<td>The LLDP protocol (Link Layer Discover Protocol) is used by PROFINET for topology detection.</td>
</tr>
</tbody>
</table>
## PROFINET protocols for Panels and Runtime Advanced

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Medium</th>
<th>Direction</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRP</td>
<td></td>
<td>Outbound</td>
<td>PROFINET medium redundancy</td>
<td>The MRP protocol (Medium redundancy protocol) enables control of redundant transmission paths using a ring topology.</td>
</tr>
<tr>
<td>PROFINET IO Data</td>
<td></td>
<td>Inbound,</td>
<td>PROFINET Cyclic IO data transfer</td>
<td>Cyclic data exchange is used by panels for direct keys and LEDs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outbound</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NARE</td>
<td></td>
<td>Inbound,</td>
<td>Name Address Resolution</td>
<td>This protocol is used to resolve network names and assign IP addresses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outbound</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROFINET Context</td>
<td>34964</td>
<td>Inbound,</td>
<td>PROFINET connection less RPC</td>
<td>The PROFINET Context Manager provides an endpoint mapper in order to establish an application relation (PROFINET AR).</td>
</tr>
<tr>
<td>Manager</td>
<td></td>
<td>Outbound</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Communication connections for Panels and WinCC Runtime Advanced

<table>
<thead>
<tr>
<th>Name</th>
<th>Port number</th>
<th>Transport protocol</th>
<th>Direction</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>23</td>
<td>TCP</td>
<td>Inbound</td>
<td>Telnet</td>
<td>This service can be used for maintenance.</td>
</tr>
<tr>
<td>SMTP</td>
<td>**</td>
<td>TCP</td>
<td>Outbound</td>
<td>SendEMail</td>
<td>This service is used by Windows CE / PC Runtime to send e-mails.</td>
</tr>
<tr>
<td>HTTP</td>
<td>80*</td>
<td>TCP</td>
<td>Inbound</td>
<td>Hypertext Transfer Protocol</td>
<td>The HTTP protocol is used for communication with the internal Web server.</td>
</tr>
<tr>
<td>RFC 1006</td>
<td>**</td>
<td>TCP</td>
<td>Outbound</td>
<td>S7 channel</td>
<td>Communication with the S7 controller via Ethernet/PROFINET.</td>
</tr>
<tr>
<td>HMI Load</td>
<td>102</td>
<td>TCP</td>
<td>Inbound</td>
<td>Transfer</td>
<td>This service is used to transmit images, Runtime, and configuration data to the panel via PN/IE</td>
</tr>
<tr>
<td>NTP</td>
<td>**</td>
<td>UDP</td>
<td>Outbound</td>
<td>Time synchronization</td>
<td>The NTP protocol (Network Time Protocol) is used for time synchronization in IP-based networks.</td>
</tr>
<tr>
<td>DCOM***</td>
<td>135</td>
<td>TCP</td>
<td>Inbound</td>
<td>OPC server</td>
<td>This service is a component of the Microsoft Windows operating system. Communication via OPC (DA) is based on DCOM. Therefore, this service is required to initialize OPC (DA) connections.</td>
</tr>
<tr>
<td>DCOM***</td>
<td>**</td>
<td>TCP</td>
<td>Outbound</td>
<td>OPC server</td>
<td>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.</td>
</tr>
<tr>
<td>NetBIOS over TCP/IP</td>
<td>**</td>
<td>UDP</td>
<td>Outbound</td>
<td>With the use of Remote File Share</td>
<td>Register / log on to a remote server.</td>
</tr>
<tr>
<td>NetBIOS over TCP/IP</td>
<td>**</td>
<td>UDP</td>
<td>Outbound</td>
<td>With the use of Remote File Share</td>
<td>Register / log on to a remote server.</td>
</tr>
<tr>
<td>SNMP</td>
<td>161</td>
<td>UDP</td>
<td>Inbound</td>
<td>Simple Network Management Protocol</td>
<td>The SNMP client functionality is used by STEP 7 to read status information from PROFINET devices.</td>
</tr>
</tbody>
</table>
## Communication connections for Panels and WinCC Runtime Advanced

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Type</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>443*</td>
<td>TCP</td>
<td>Inbound</td>
<td>The HTTP protocol is used for communication with the panel-internal Web server via Secure Socket Layer (SSL).</td>
</tr>
<tr>
<td>Modbus TCP</td>
<td>**</td>
<td>TCP</td>
<td>Outbound</td>
<td>The Modbus TCP protocol is used for connections to Schneider PLCs.</td>
</tr>
<tr>
<td>Mitsubishi MC</td>
<td>**</td>
<td>TCP</td>
<td>Outbound</td>
<td>The Mitsubishi protocol is used for connections to Mitsubishi PLCs.</td>
</tr>
<tr>
<td>Printing</td>
<td>**</td>
<td>TCP</td>
<td>Outbound</td>
<td>Printing on the control panel (via Ethernet).</td>
</tr>
<tr>
<td>HMI Load</td>
<td>2308</td>
<td>TCP</td>
<td>Inbound</td>
<td>This service is used to transmit images and configuration data to panels. On Comfort Panels, this service is replaced by DeviceManager and SCS in V13 and higher. This service is used to transmit configuration data to WinCC Runtime Advanced.</td>
</tr>
<tr>
<td>HMI Load</td>
<td>50523</td>
<td>TCP</td>
<td>Inbound</td>
<td>This port is used if port 2308 is not available. This service is used to transmit images and configuration data to panels. On Comfort Panels, this service is replaced by DeviceManager and SCS in V13 and higher. This service is used to transmit configuration data to WinCC Runtime Advanced.</td>
</tr>
<tr>
<td>ALM</td>
<td>4410*</td>
<td>TCP</td>
<td>Inbound, Outbound</td>
<td>This service of RT Advanced makes available the complete functionalities for software licenses and is used by the Automation License Manager.</td>
</tr>
<tr>
<td>OPC UA</td>
<td>4870*</td>
<td>TCP</td>
<td>Inbound</td>
<td>This service is required for communication via OPC UA.</td>
</tr>
<tr>
<td>HMI Load</td>
<td>5001</td>
<td>TCP</td>
<td>Inbound</td>
<td>This service is used to transmit images and Runtime to panels.</td>
</tr>
<tr>
<td>HMI Load</td>
<td>5002</td>
<td>TCP</td>
<td>Inbound</td>
<td>This service is used to transmit configuration data to panels.</td>
</tr>
<tr>
<td>VNC client</td>
<td>5500</td>
<td>TCP</td>
<td>Inbound</td>
<td>Reverse VNC server connection. Receive mode is set for the VNC client.</td>
</tr>
<tr>
<td>VNC server</td>
<td>5800*</td>
<td>TCP</td>
<td>Inbound</td>
<td>VNC server connection HTTP</td>
</tr>
<tr>
<td>VNC server</td>
<td>5900*</td>
<td>TCP</td>
<td>Inbound</td>
<td>VNC server connection</td>
</tr>
<tr>
<td>SIMATIC Logon</td>
<td>**</td>
<td>TCP</td>
<td>Outbound</td>
<td>Register / log on to a remote server.</td>
</tr>
<tr>
<td>Allen Bradley Ethernet IP</td>
<td>**</td>
<td>TCP</td>
<td>Outbound</td>
<td>The Ethernet/IP protocol is used for connections to Allen Bradley PLCs.</td>
</tr>
<tr>
<td>Reserved</td>
<td>49152...65535</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Dynamic port range is used, for example, to connect to the remote file sharing.</td>
</tr>
</tbody>
</table>

* Default port that can be changed by user configuration
** Port is assigned automatically.
*** Supported by WinCC Runtime Advanced only.
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.
3.1 Notes on operation in Runtime

Contents

Information that could no longer be included in the online help and important information about product features.

Focus in Runtime

If you have configured a low-contrast combination of focus color and border color in a V12 project, the focus may no longer be identifiable after changing the HMI device version in Runtime. Change one of the two colors.

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. Enable Service mode.
4. Start Runtime again using the surrogate icon in the taskbar.

**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 the product DVD:

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

---

**Starting Runtime**

Only WinCC Runtime V13 can be started in TIA Portal V13. WinCC Runtime V11.02, V12 or V13 can be simulated in TIA Portal V13.
### 3.2 Notes on operation of Runtime Advanced

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

**Permission for starting Runtime**
On a computer running the 32-bit version of Windows 7, WinCC Runtime Professional or WinCC Runtime Advanced can only be started when a user is a member of the automatically created group, "Siemens TIA Engineer".

**.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.

### 3.3 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, 15
  Date/time PLC, 15

D
DTL data type
  Restriction, 15

L
Language behavior
  On-screen keyboard, 13

M
Maximum length
  Tag, 13

S
Screen keyboard
  Language behavior, 13

T
Tag
  Maximum length, 13