

SIMATIC

WinCC

WinCC Advanced V14 SP1 - Options

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

| | | |
|----------|--|----------|
| 1 | WinCC Audit (Panels, Comfort Panels, RT Advanced)..... | 7 |
| 1.1 | Basics (Panels, Comfort Panels, RT Advanced)..... | 7 |
| 1.1.1 | GMP compliance (Panels, Comfort Panels, RT Advanced)..... | 7 |
| 1.1.2 | GMP-compliant configuration (Panels, Comfort Panels, RT Advanced)..... | 7 |
| 1.1.3 | Audit option (Panels, Comfort Panels, RT Advanced)..... | 8 |
| 1.1.4 | Scope of logging (Panels, Comfort Panels, RT Advanced)..... | 9 |
| 1.2 | Using the Audit trail (Panels, Comfort Panels, RT Advanced)..... | 11 |
| 1.2.1 | Audit Trail (Panels, Comfort Panels, RT Advanced)..... | 11 |
| 1.2.2 | Creating an audit trail (Panels, Comfort Panels, RT Advanced)..... | 13 |
| 1.2.3 | Parameters for the audit trail (Panels, Comfort Panels, RT Advanced)..... | 15 |
| 1.2.4 | Setting the audit trail language (Panels, Comfort Panels, RT Advanced)..... | 18 |
| 1.2.5 | Low free storage space (Panels, Comfort Panels, RT Advanced)..... | 19 |
| 1.2.5.1 | Low free storage space (Panels, Comfort Panels, RT Advanced)..... | 19 |
| 1.2.5.2 | Free space critically low (Panels, Comfort Panels, RT Advanced)..... | 19 |
| 1.2.5.3 | Configuring the "Low free storage space" event (Panels, Comfort Panels, RT Advanced)..... | 20 |
| 1.2.6 | Logging the audit trail (Panels, Comfort Panels, RT Advanced)..... | 20 |
| 1.2.6.1 | Reporting an audit trail (Panels, Comfort Panels, RT Advanced)..... | 20 |
| 1.2.6.2 | Audit Trail reporting (Panels, Comfort Panels, RT Advanced)..... | 21 |
| 1.2.6.3 | Parameters for the audit trail report (Panels, Comfort Panels, RT Advanced)..... | 22 |
| 1.2.6.4 | Printing out an audit trail report (Panels, Comfort Panels, RT Advanced)..... | 24 |
| 1.2.7 | Evaluating an audit trail (Panels, Comfort Panels, RT Advanced)..... | 25 |
| 1.2.7.1 | Evaluating audit trails (Panels, Comfort Panels, RT Advanced)..... | 25 |
| 1.2.7.2 | Evaluating Audit Trails in AuditViewer (Panels, Comfort Panels, RT Advanced)..... | 26 |
| 1.2.7.3 | Evaluating Audit Trails with DOS program (Panels, Comfort Panels, RT Advanced)..... | 27 |
| 1.2.8 | Audit trail logging concept (Panels, Comfort Panels, RT Advanced)..... | 28 |
| 1.2.8.1 | Format (Panels, Comfort Panels, RT Advanced)..... | 28 |
| 1.2.8.2 | Storage location and medium (Panels, Comfort Panels, RT Advanced)..... | 29 |
| 1.2.8.3 | Protection mechanisms (Panels, Comfort Panels, RT Advanced)..... | 30 |
| 1.2.8.4 | Upgrading WinCC (Panels, Comfort Panels, RT Advanced)..... | 31 |
| 1.2.8.5 | Audit trail behavior in runtime (Panels, Comfort Panels, RT Advanced)..... | 31 |
| 1.3 | Configuring audit functions (Panels, Comfort Panels, RT Advanced)..... | 32 |
| 1.3.1 | Logging tag value changes (Panels, Comfort Panels, RT Advanced)..... | 32 |
| 1.3.1.1 | Tag value change (Panels, Comfort Panels, RT Advanced)..... | 32 |
| 1.3.1.2 | Logging tag value changes (Panels, Comfort Panels, RT Advanced)..... | 32 |
| 1.3.1.3 | Effects of tag change (Panels, Comfort Panels, RT Advanced)..... | 34 |
| 1.3.2 | Logging recipe data record changes (Panels, Comfort Panels, RT Advanced)..... | 34 |
| 1.3.2.1 | Recipe data changes (Panels, Comfort Panels, RT Advanced)..... | 34 |
| 1.3.2.2 | Logging recipe data changes (Panels, Comfort Panels, RT Advanced)..... | 35 |
| 1.3.2.3 | Effects of recipe data change (Panels, Comfort Panels, RT Advanced)..... | 36 |
| 1.3.3 | Logging user actions (Panels, Comfort Panels, RT Advanced)..... | 37 |
| 1.3.3.1 | User actions with GMP-compliant configuration (Panels, Comfort Panels, RT Advanced)..... | 37 |
| 1.3.3.2 | Logging modes (Panels, Comfort Panels, RT Advanced)..... | 38 |
| 1.3.3.3 | Configuring the "NotifyUserAction" system function (Panels, Comfort Panels, RT Advanced)..... | 39 |
| 1.3.3.4 | GMP-compliant user administration (Panels, Comfort Panels, RT Advanced)..... | 40 |

| | | |
|----------|---|-----------|
| 1.3.4 | Logging system functions (Panels, Comfort Panels, RT Advanced)..... | 40 |
| 1.4 | Performance features of GMP relevant configuration (Panels, Comfort Panels, RT Advanced)..... | 45 |
| 1.4.1 | Supported HMI devices (Panels, Comfort Panels, RT Advanced)..... | 45 |
| 1.4.2 | Restrictions (Panels, Comfort Panels, RT Advanced)..... | 46 |
| 1.5 | Enabling GMP compliant configuration (Panels, Comfort Panels, RT Advanced)..... | 46 |
| 2 | WinCC Sm@rtServer (Panels, Comfort Panels, RT Advanced)..... | 49 |
| 2.1 | Basics (Panels, Comfort Panels, RT Advanced)..... | 49 |
| 2.1.1 | Sm@rt Options (Panels, Comfort Panels, RT Advanced)..... | 49 |
| 2.1.2 | Application scenarios (Panels, Comfort Panels, RT Advanced)..... | 51 |
| 2.1.3 | HMI devices suitable for use (Panels, Comfort Panels, RT Advanced)..... | 53 |
| 2.1.4 | Settings for Sm@rt Options (Panels, Comfort Panels, RT Advanced)..... | 54 |
| 2.1.4.1 | Configuration in WinCC (Panels, Comfort Panels, RT Advanced)..... | 54 |
| 2.1.4.2 | Configurations on the HMI device (Panels, Comfort Panels, RT Advanced)..... | 56 |
| 2.1.5 | Settings for remote control (Panels, Comfort Panels, RT Advanced)..... | 69 |
| 2.1.5.1 | Session management for remote control (Panels, Comfort Panels, RT Advanced)..... | 69 |
| 2.1.5.2 | Configuring Sm@rtServer for remote control (Panels, Comfort Panels, RT Advanced)..... | 70 |
| 2.1.5.3 | Configure Sm@rtClient for remote control (Panels, Comfort Panels, RT Advanced)..... | 75 |
| 2.1.5.4 | Sm@rtClient-Application (Panels, Comfort Panels, RT Advanced)..... | 76 |
| 2.1.5.5 | Remote control of key devices (Panels, Comfort Panels, RT Advanced)..... | 80 |
| 2.1.6 | Use and restrictions of Sm@rt Options (Panels, Comfort Panels, RT Advanced)..... | 81 |
| 2.1.7 | Setting up secure communication between WebClient and Sm@rtServer (Panels, Comfort Panels, RT Advanced)..... | 82 |
| 2.1.7.1 | Configuring secure communication for Sm@rtServer (Panels, Comfort Panels, RT Advanced)..... | 82 |
| 2.1.7.2 | Configuring a separate certificate for Sm@rtServer (Panels, Comfort Panels, RT Advanced)..... | 84 |
| 2.1.7.3 | Installing self-signed Sm@rtServer certificates in Internet Explorer (Panels, Comfort Panels, RT Advanced)..... | 84 |
| 2.1.7.4 | Installing self-signed Sm@rtServer certificates in Firefox (Panels, Comfort Panels, RT Advanced)..... | 85 |
| 2.1.7.5 | Configuring secure communication on the WebClient (Panels, Comfort Panels, RT Advanced)..... | 86 |
| 2.2 | Remote control via Sm@rtServer (Panels, Comfort Panels, RT Advanced)..... | 87 |
| 2.2.1 | Types of the remote control (Panels, Comfort Panels, RT Advanced)..... | 87 |
| 2.2.1.1 | Remote control and remote monitoring by means of Sm@rtServer (Panels, Comfort Panels, RT Advanced)..... | 87 |
| 2.2.1.2 | Remote control by means of Internet Explorer (Panels, Comfort Panels, RT Advanced)..... | 88 |
| 2.2.1.3 | Remote control by means of the Sm@rtClient application (Panels, Comfort Panels, RT Advanced)..... | 89 |
| 2.2.1.4 | Remote control via the Sm@rtClient display during runtime (Panels, Comfort Panels, RT Advanced)..... | 91 |
| 2.2.2 | Distributed operator stations (Panels, Comfort Panels, RT Advanced)..... | 93 |
| 2.2.2.1 | Configuration (Panels, Comfort Panels, RT Advanced)..... | 93 |
| 2.2.2.2 | Configure distributed operator stations (Panels, Comfort Panels, RT Advanced)..... | 95 |
| 2.2.2.3 | Configure Sm@rtServer (Panels, Comfort Panels, RT Advanced)..... | 95 |
| 2.2.2.4 | Project Sm@rtClient (Panels, Comfort Panels, RT Advanced)..... | 97 |
| 2.3 | E-mail notification from runtime (Panels, Comfort Panels, RT Advanced)..... | 99 |
| 2.3.1 | Process flow (Panels, Comfort Panels, RT Advanced)..... | 99 |

| | | |
|-------------------|--|------------|
| 2.3.2 | Specify trigger for E-Mailing (Panels, Comfort Panels, RT Advanced)..... | 100 |
| 2.3.3 | Configure secure e-mail notification from Runtime (Panels, Comfort Panels, RT Advanced)..... | 101 |
| 2.4 | Display integrated Service-Pages (Panels, Comfort Panels, RT Advanced)..... | 103 |
| 2.4.1 | Integrated Webserver (Panels, Comfort Panels, RT Advanced)..... | 103 |
| 2.4.2 | Service-pages of the web server (Panels, Comfort Panels, RT Advanced)..... | 105 |
| 2.4.3 | Installing the client and server certificates for SSL (Panels, Comfort Panels, RT Advanced)..... | 106 |
| 2.4.4 | Configure access to service-pages (Panels, Comfort Panels, RT Advanced)..... | 107 |
| 2.4.4.1 | Configure integrated web server (Panels, Comfort Panels, RT Advanced)..... | 107 |
| 2.4.4.2 | Display and remote-control Service-Pages (Panels, Comfort Panels, RT Advanced)..... | 108 |
| 2.4.5 | Create own Service-pages (Panels, Comfort Panels, RT Advanced)..... | 110 |
| 2.4.5.1 | Basics (Panels, Comfort Panels, RT Advanced)..... | 110 |
| 2.4.5.2 | Create service-page for displaying process values (Panels, Comfort Panels, RT Advanced)..... | 112 |
| 2.4.5.3 | Transfer Service-pages (Panels, Comfort Panels, RT Advanced)..... | 113 |
| 2.5 | Access via SIMATIC HMI HTTP Protocol (Panels, Comfort Panels, RT Advanced)..... | 115 |
| 2.5.1 | Configuration (Panels, Comfort Panels, RT Advanced)..... | 115 |
| 2.5.2 | Configure access via SIMATIC HTTP Protocol (Panels, Comfort Panels, RT Advanced).... | 116 |
| 2.5.3 | Permissible data types (SIMATIC HMI HTTP protocol) (Panels, Comfort Panels, RT Advanced)..... | 116 |
| 2.5.4 | Configure HTTP server (Panels, Comfort Panels, RT Advanced)..... | 117 |
| 2.5.4.1 | Configure WinCC-Project (Panels, Comfort Panels, RT Advanced)..... | 117 |
| 2.5.4.2 | Setting WinCC Runtime Advanced Internet (Panels, Comfort Panels, RT Advanced)..... | 118 |
| 2.5.5 | Configuring HTTP clients (Panels, Comfort Panels, RT Advanced)..... | 119 |
| 2.5.5.1 | Configuring HTTP connections in the client (Panels, Comfort Panels, RT Advanced)..... | 119 |
| 2.5.5.2 | Configure the HTTP-Client tags (Panels, Comfort Panels, RT Advanced)..... | 120 |
| 2.5.6 | Commissioning an HTTP- connection (Panels, Comfort Panels, RT Advanced)..... | 121 |
| 2.6 | Connection to the Office-world (Panels, Comfort Panels, RT Advanced)..... | 124 |
| 2.6.1 | Configuration (Panels, Comfort Panels, RT Advanced)..... | 124 |
| 2.6.2 | Creating a VBA macro in MS Excel (Panels, Comfort Panels, RT Advanced)..... | 125 |
| Index..... | | 129 |

WinCC Audit (Panels, Comfort Panels, RT Advanced)

1.1 Basics (Panels, Comfort Panels, RT Advanced)

1.1.1 GMP compliance (Panels, Comfort Panels, RT Advanced)

GMP compliant projects with WinCC

Traceability and therefore the documentation of production data is becoming increasingly important in many sectors such as the pharmaceuticals industry, the food and beverage industry, and the related mechanical engineering industry.

Storage of production data in electronic form offers many advantages compared to paper documents, such as simple acquisition and logging of data.

However, it is also important to ensure that data cannot be falsified and that it can be read at any time.

Industry-specific and general standards for electronic documentation of production data have been developed for this purpose.

The most important set of regulations is the FDA guideline 21 CFR Part 11 for electronic data records and electronic signatures issued by the FDA, the US Food and Drug Administration. The various EU regulations, such as EU 178/2002, also apply for particular industries.

Requirements for production systems in these industries have been developed on the basis of 21 CFR Part 11 and the corresponding layout to comply with GMP (Good Manufacturing Practice). They are also required for other industries.

The following primary requirements are derived from these directives and rules:

- Creation of an Audit Trail or operating trace in runtime
This document can be used to trace a complete log of which user has run what control function on the machine at what time.
- Important process stages must also be traceable to a specific responsibility, for example with an electronic signature.

1.1.2 GMP-compliant configuration (Panels, Comfort Panels, RT Advanced)

Introduction

"GMP compliant configuration" means creating projects in accordance with "Good Manufacturing Practice". The requirements are set out in FDA rules "21 CFR Part 11". The FDA is the U.S. Food and Drug Administration.

GMP-compliant configuration means HMI devices have electronic production data documentation functionalities.

GMP relevant and the audit trail

WinCC offers the "Audit" option for implementing GMP compliance. Using the audit option, the "GMP compliant configuration" function can be enabled.

Enable the "GMP compliant configuration" function directly in the runtime settings of the HMI device. GMP relevant functionalities are then added to WinCC. These functionalities are:

- Audit Trail
- Electronic signature
- Option to label tags as "GMP relevant".
- Option to label tags as "GMP relevant" for recipes.
- NotifyUserAction system function
- Logging of tags using checksum
- Logging of alarms using checksum
- Audit trail record for printing logged changes

A license is required to convert the GMP-relevant functions configured in WinCC in runtime.

Depending on the edition of WinCC, use one of the following licenses:

- WinCC Audit for RT Advanced
- WinCC Audit for SIMATIC Panel

If the labeled objects are executed or changed, then it is saved in a special log, the "Audit Trail".

1.1.3 Audit option (Panels, Comfort Panels, RT Advanced)

Advanced functions

The Audit option adds functions to WinCC to ensure that your project is GMP compliant.

The following functions are added:

- **Audit Trail**
For every HMI device, you can create an Audit Trail .
Operator actions and system processes that are relevant for the FDA-compliance of the process are recorded in an Audit Trail during runtime.
 - User actions such as changes in the values of GMP relevant tags or recipes or the acknowledgment of alarms.
 - Actions by the system, such as starting up runtime or rejection of logon attempts.
- **Electronic signature**
You can set mandatory acknowledgment of important user actions in runtime, such as changing recipe data records or tag values.
All Audit-relevant user actions must be protected by authorization in the user administration. The user will then only be able to run these actions if an electronic signature and, if configured appropriately, a comment have been input. The electronic signature and the comment are logged in the audit trail.

Extension of the WinCC engineering system

For all HMI devices that support "GMP-compliant configuration", the WinCC engineering system is extended to include the following configuration options when GMP is enabled:

- The entry "AuditTrail" is added to the "Logs" editor.
- A "Good Manufacturing Practice Settings" entry is added to "HMI tags" editor in the inspector window of a "Properties > Properties" tag.
- A "Good Manufacturing Practice" entry is added to "Recipes" editor in the inspector window of a "Properties > Properties" recipe.
- "NotifyUserAction" system function

1.1.4 Scope of logging (Panels, Comfort Panels, RT Advanced)

Introduction

It is important to ensure that audit-related processes are always logged in runtime in the audit trail in a project with the option "Audit".

Scope of logging

The following operations are Audit-relevant and are automatically saved in the Audit Trail:

- Runtime sequence
 - Runtime start and runtime stop
 - Project information: Version and project name, of the configuration environment, device, and current runtime configuration
 - Failure of the voltage supply of an active Uninterruptible Power Supply (UPS).
- User administration
 - Logon and logoff of users
 - Invalid logon attempts
 - Import of user administration
 - Changes of user administration
- Alarm system
 - All alarms that are acknowledged by the user.
 - All acknowledgment attempts of the user

Note

Logging alarm text

To log alarm texts, select the "Log alarm text in Audit Trail" option in the Audit Trail editor:
"Audit trail > Properties > Settings" in the "Settings" area

- Log operations
 - Starting, stopping and copying a log
 - Opening and closing all logs
 - Deleting a log
 - Starting a sequence log
 - Long-term logging of a log
- Running specific system functions depending on their functionality and the triggering event

The following audit processes are logged depending on the configuration of the recipes and the tags of the project:

- Change values of GMP-relevant tags by the user
- for GMP-relevant recipes:
 - Storing after changing and creating recipe data records
 - Transfer of recipe data records to the PLC and from the PLC
 - For recipe tags: Changing the setting for the synchronization of the tag values with the PLC ("offline"/"online")
- "NotifyUserAction" system function
You use the system function "NotifyUserAction" to record user actions that are not automatically recorded by the audit trail.
You can configure this system function for screen calls, for example You can also configure function lists containing system functions that do not require signature or acknowledgement.

1.2 Using the Audit trail (Panels, Comfort Panels, RT Advanced)

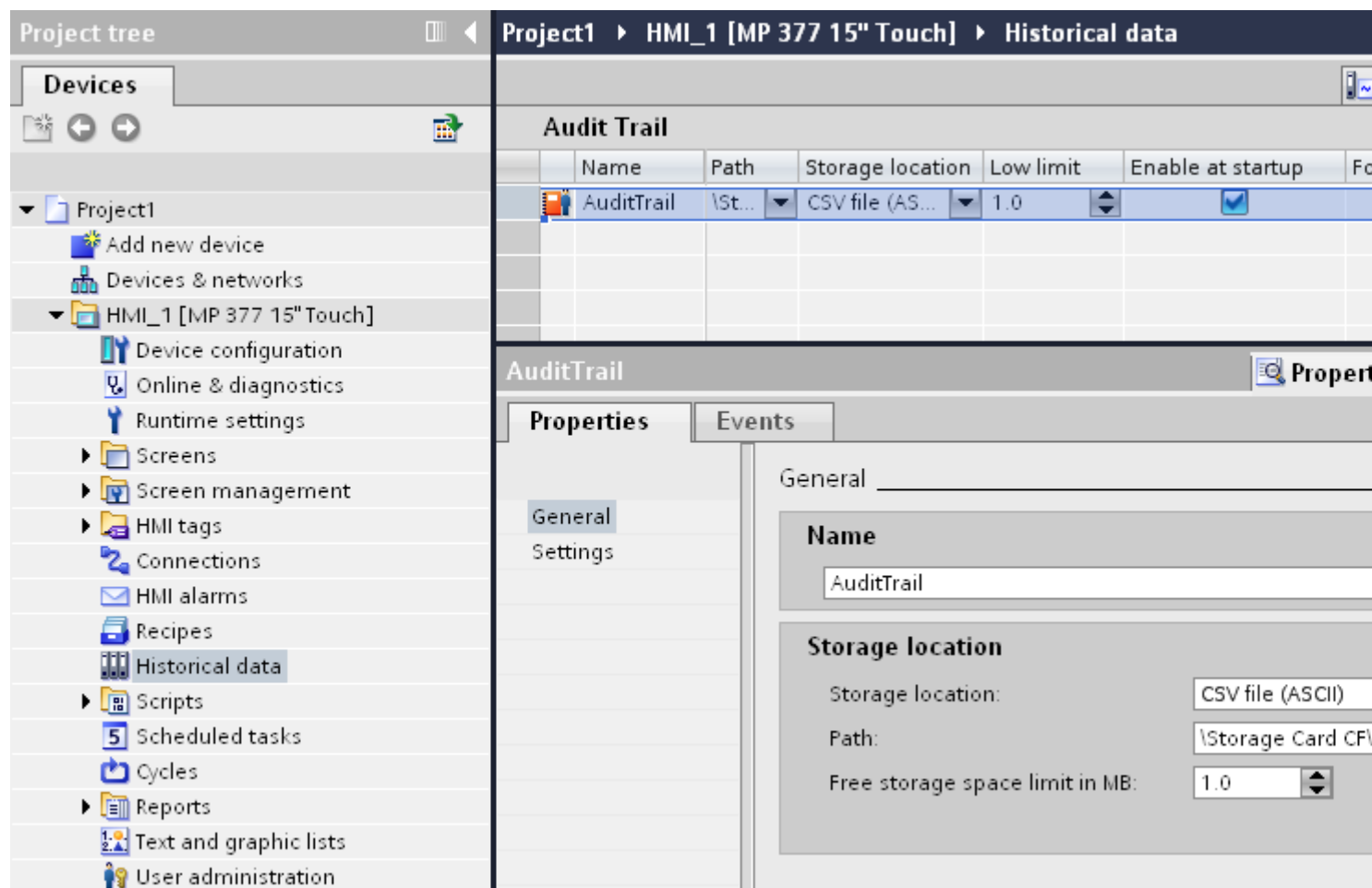
1.2.1 Audit Trail (Panels, Comfort Panels, RT Advanced)

Introduction

Configure a log in the settings for Audit Trail editor. This log is used to store changes in tag or recipe values made by the user and other user actions in runtime.

"Settings for audit trail" editor

1. In the project view, double-click "AuditTrail" in the "Log" group.
2. Click on the "Settings for audit trail" tab.
3. Change the properties of Audit Trail in the inspector window.

**Audit trail work area**

You define the settings for the Audit Trail in the "Properties > Properties" inspector window.

You set the name of the log and the storage location and decide whether logging will begin on startup. Also determine if "Forcing" is permitted.

"Forcing" is a function for administrators. It allows the administrator to continue the process even if the maximum log storage space has been exceeded.

Thus, the Audit Trail switches off and must be rebooted using the "StartLogging" system function.

1.2.2 Creating an audit trail (Panels, Comfort Panels, RT Advanced)

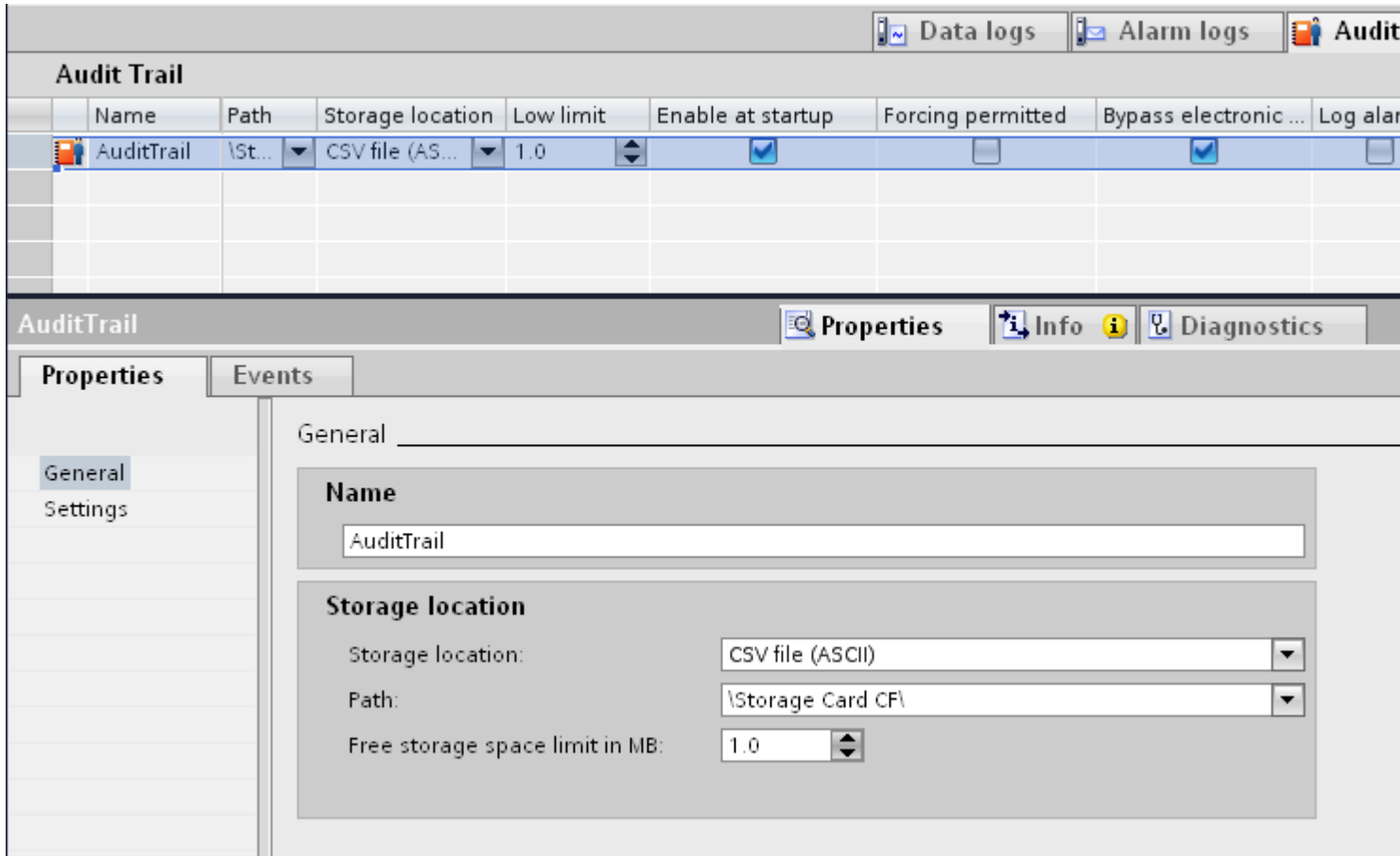
Requirements

"GMP compliant configuration" has been selected on the HMI device.

Procedure

1. Double-click on the HMI device in the project tree.
2. Double-click "Logs".
The "Logs" editor will open.

3. Change to the "Audit Trail" tab.
An audit trail has been created.



4. Define the following in the inspector window:

- Name
- Storage location
- Logging with runtime start-up
- Forcing

Note

No audit-related user actions are permitted in GMP relevant projects if there is insufficient storage space available for the audit trail.

If the check box "Forcing permitted" is activated and, because of the hardware, there is insufficient storage space in runtime, the administrator can interrupt audit trail logging. The administrator can prevent the process from stopping in this way.

If the administrator enables the "Forcing" function, the interruption of the audit trail by the administrator will be entered in the audit trail as the last entry.

At the end of "Forcing" restart the audit trail using the "StartLogging" system function.

Configuring a function list

If necessary, configure a function list for the events "Low free storage space" and "Free space critically low".

The "Low free storage space" event is triggered if the amount of free storage space available for the audit trail in runtime is less than the amount configured in "Minimum storage space in MB".

The "Free space critically low" event is triggered if there is no longer sufficient free storage space for the audit trail in runtime. The value depends on the HMI device.

You can find more detailed information on this in the section: AUTOHOTSPOT

Result

Audit relevant user actions are entered in the configured audit trail in runtime.

1.2.3 Parameters for the audit trail (Panels, Comfort Panels, RT Advanced)

Introduction

Configure Audit Trail in the "Logs" editor if you have enabled "GMP compliant configuration" in the runtime settings.

There are two ways of assigning parameters for the audit trail:

- "Settings for audit trail" editor
- "Audit Trail" inspector window

Editor "Audit Trail"

The "Audit Trail" editor is an overview of the Audit Trail created.

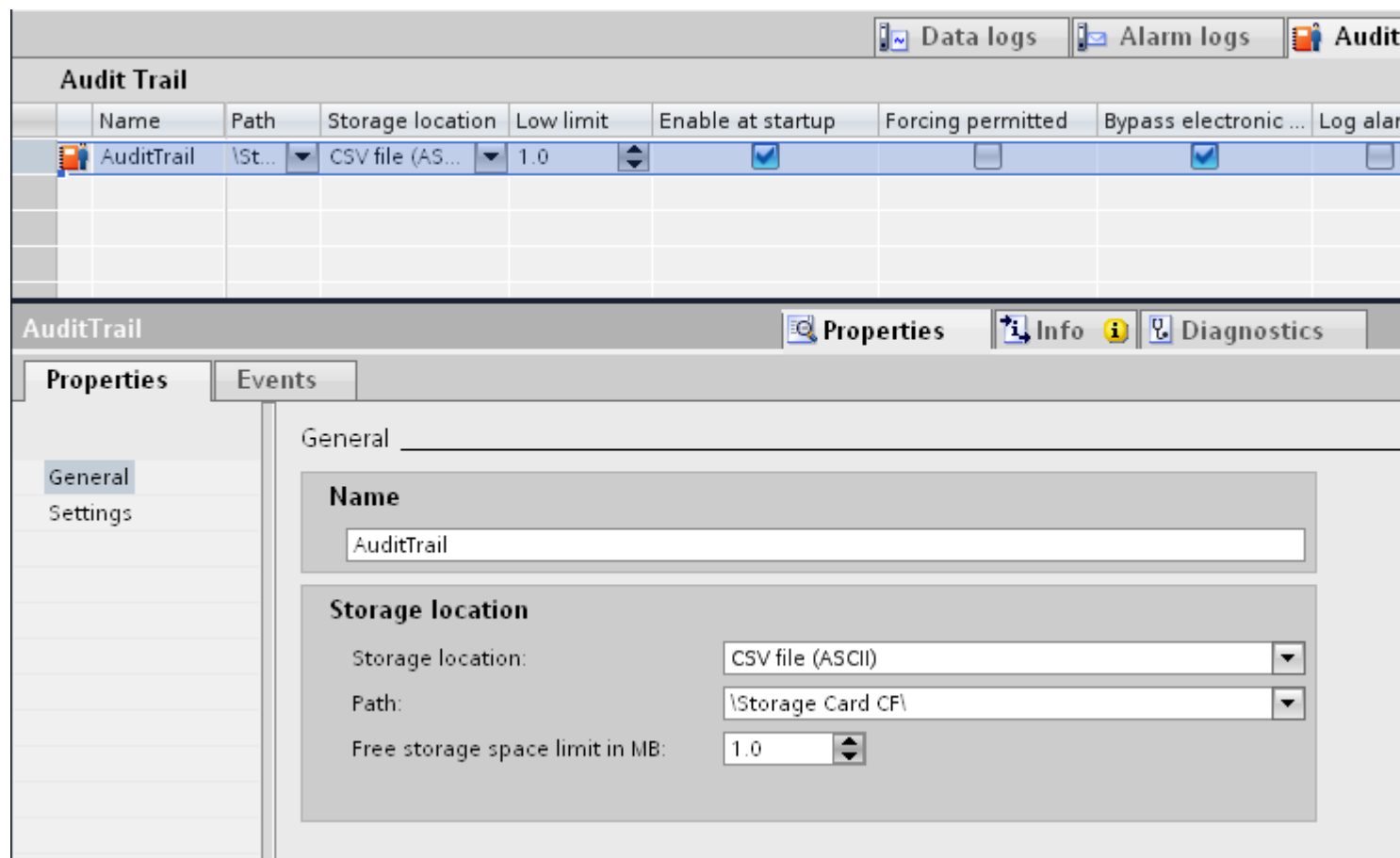
Only one Audit Trail can be created per HMI device.

Parameters that are assigned for the Audit Trail can be seen in the line. You can select or deselect the parameters displayed.

The parameters of an Audit Trail are also displayed and described in more detail in the inspector window.

General inspector window

You can set the following parameters under "Audit trail > Properties > General":



Name

- Under "Name", assign a name for the Audit Trail .
Special characters are not permitted when assigning the name.

Storage location

- Storage location
You can choose between:
 - RDB file
 - a CSV file (ASCII)
 - a TXT file (Unicode)

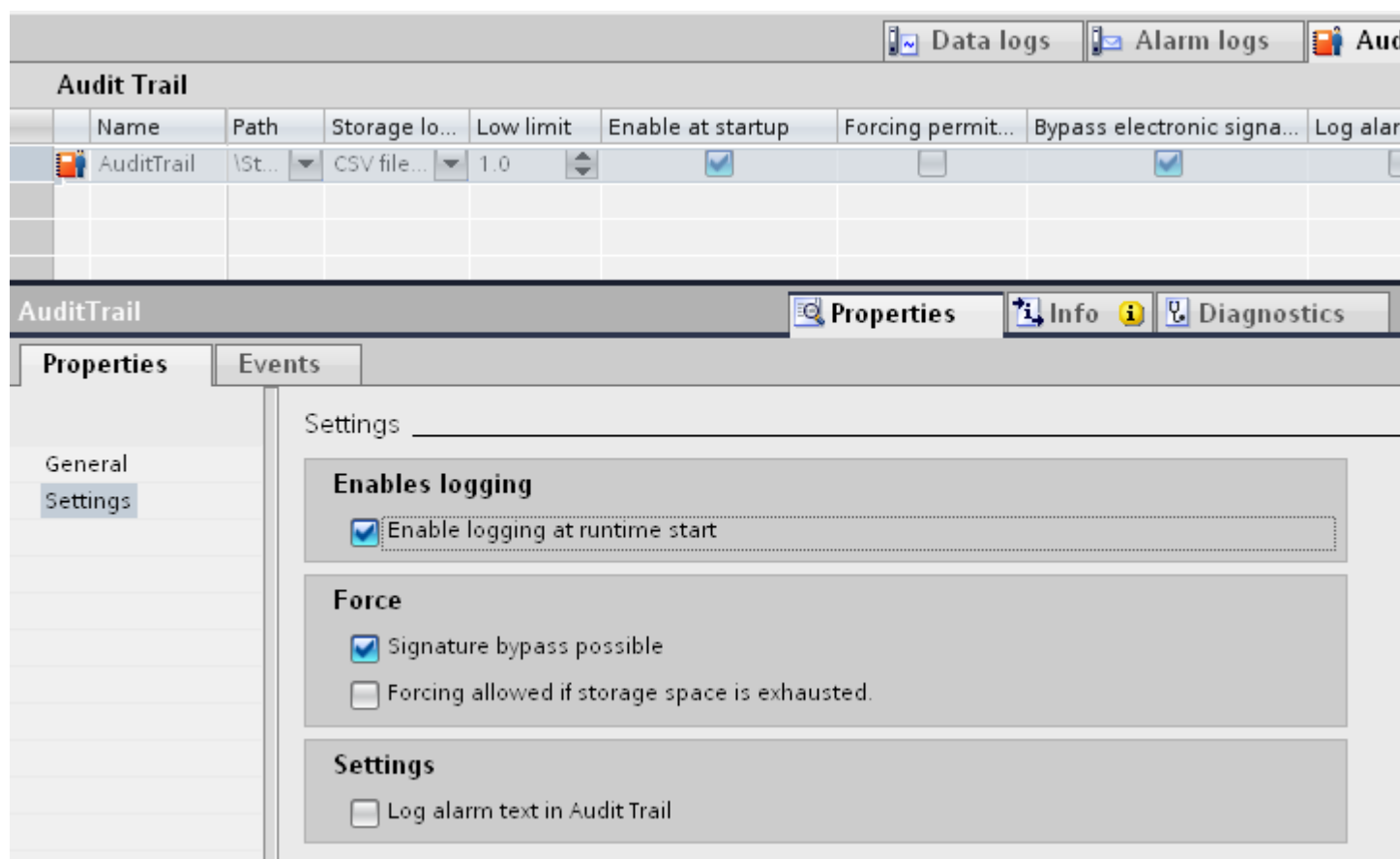
Note

Use "TXT (Unicode)" as storage location for logging Asian languages.

- Path
Depending on the HMI device, enter the storage location of the Audit Trail under "Path".
- Minimum space in MB
Specify the size of remaining storage space that triggers the "Little available memory" event.

Inspector window settings

You can set the following parameters under "Audit trail > Properties > Properties > Settings":



Logging activation

- Enable logging at runtime start

Forcing

- Bypass electronic signature
Specifies whether the administrator is permitted to run operator actions without entering an electronic signature or comments.
- Forcing allowed if storage space is exhausted
This function allows the administrator to interrupt audit trail logging in the following scenarios:
 - There is no free storage space available.
 - The storage medium is missing.
 - Access to required storage medium is not possible.

You can thus prevent the process from stopping.

After Forcing was carried out, the audit trail log switches off.

After the end of "Forcing", the audit trail must be restarted with the system function "StartLogging".

Settings

- Logging alarm texts in the audit trail.

Note

Use "TXT (Unicode)" as storage location for logging Asian languages.

For further details on setting the logging language, refer to the following section:
AUTOHOTSPOT

See also

Format (Page 28)

1.2.4 Setting the audit trail language (Panels, Comfort Panels, RT Advanced)

Introduction

The logging language for an Audit Trail is set in the runtime settings.

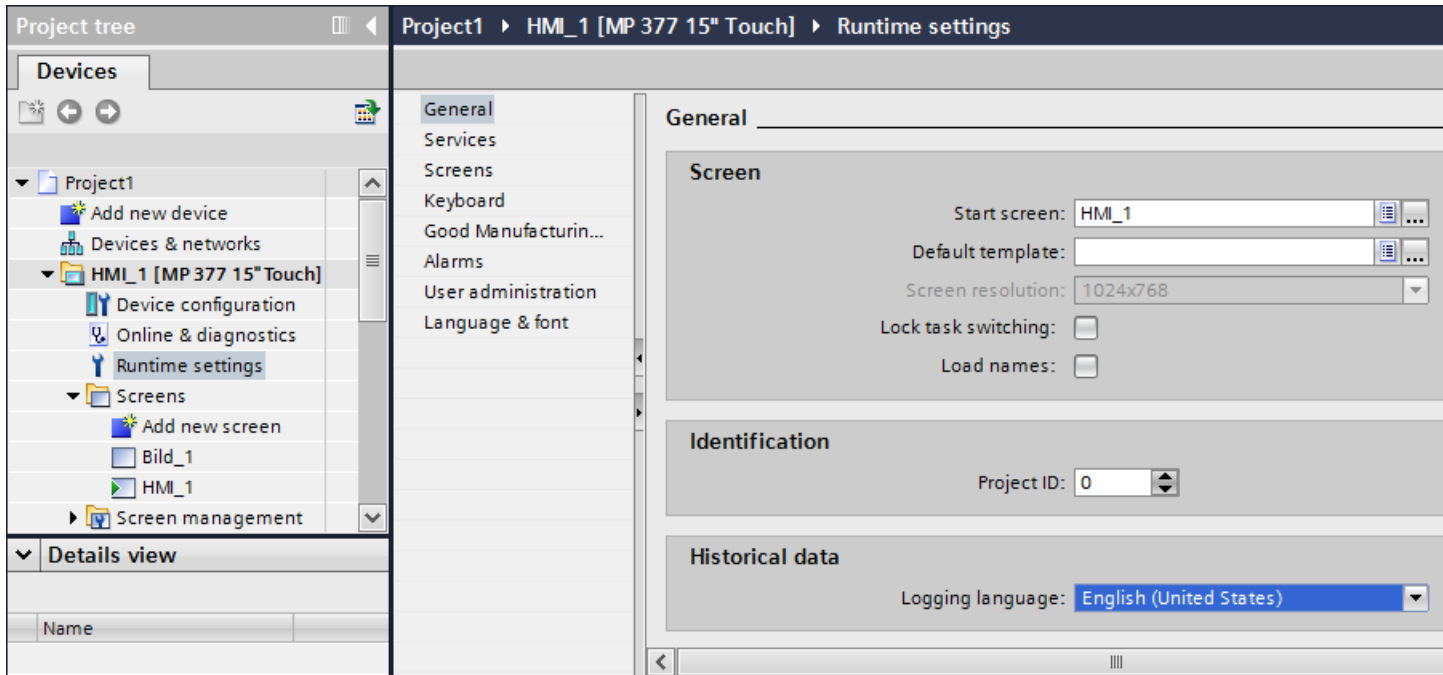
Procedure

1. Double-click on the HMI device in the project tree.
2. Double-click "Runtime settings".

3. Click "General".
4. Select the logging language in the "Logs" area.

Note

If an Asian language was selected, use the "TXT (Unicode)" storage location in the "Audit trail" editor.



1.2.5 Low free storage space (Panels, Comfort Panels, RT Advanced)

1.2.5.1 Low free storage space (Panels, Comfort Panels, RT Advanced)

Description

This event is triggered if the storage space available on the medium to which the Audit Trail is less than the configured minimum.

1.2.5.2 Free space critically low (Panels, Comfort Panels, RT Advanced)

Description

This event is triggered if the storage medium to which an Audit Trail is saved provides insufficient storage space due to hardware restrictions.

1.2.5.3 Configuring the "Low free storage space" event (Panels, Comfort Panels, RT Advanced)

Requirements

- A GMP- compliant configuration is enabled
- An Audit Trail is created

Procedure

1. Click on the Audit Trail in the "Audit Trail" editor.
2. In the Inspector window, click "Properties > General".
3. In the "Free storage space limit in MB" area, select a value that triggers the "Little free space" event.
4. Click on Events in the Inspector window.
5. Click on the "Low free storage space" event.
6. In the function list, specify a system function to execute when an "Overflow" event is triggered.

1.2.6 Logging the audit trail (Panels, Comfort Panels, RT Advanced)

1.2.6.1 Reporting an audit trail (Panels, Comfort Panels, RT Advanced)

Introduction

You can print a report of the operations saved in an Audit Trail. All recorded actions are included in the printout.

Requirements for reporting

The "Audit Trail report" report object is available for the printout of an Audit Trail.

You can configure the report in the "Report" editor. The report object is only available if the "GMP-compliant configuration" option is set in the runtime settings of the HMI device.

If an Audit Trail must be printed in runtime, initially the logging of Audit Trail must be stopped using the "StopLogging" system function.

Whilst an Audit Trail is being printed, no user actions are recorded. Ensure that no GMP-relevant user actions are executed whilst the logging is stopped.

After printing is complete without any errors, restart the Audit Trail using the "StartLogging" system function.

The header of the report is printed in the current runtime language. Change the runtime language to the logging language accordingly.

The logged data from Audit are printed in the configured runtime logging language.

In order to receive a complete report, the report object can also be used in a report in conjunction with the "Print alarm" and "Print recipe" report objects.

1.2.6.2 Audit Trail reporting (Panels, Comfort Panels, RT Advanced)

Introduction

You use the "Audit Trail" report object to configure a report for the output of Audit Trail contents to a printer.

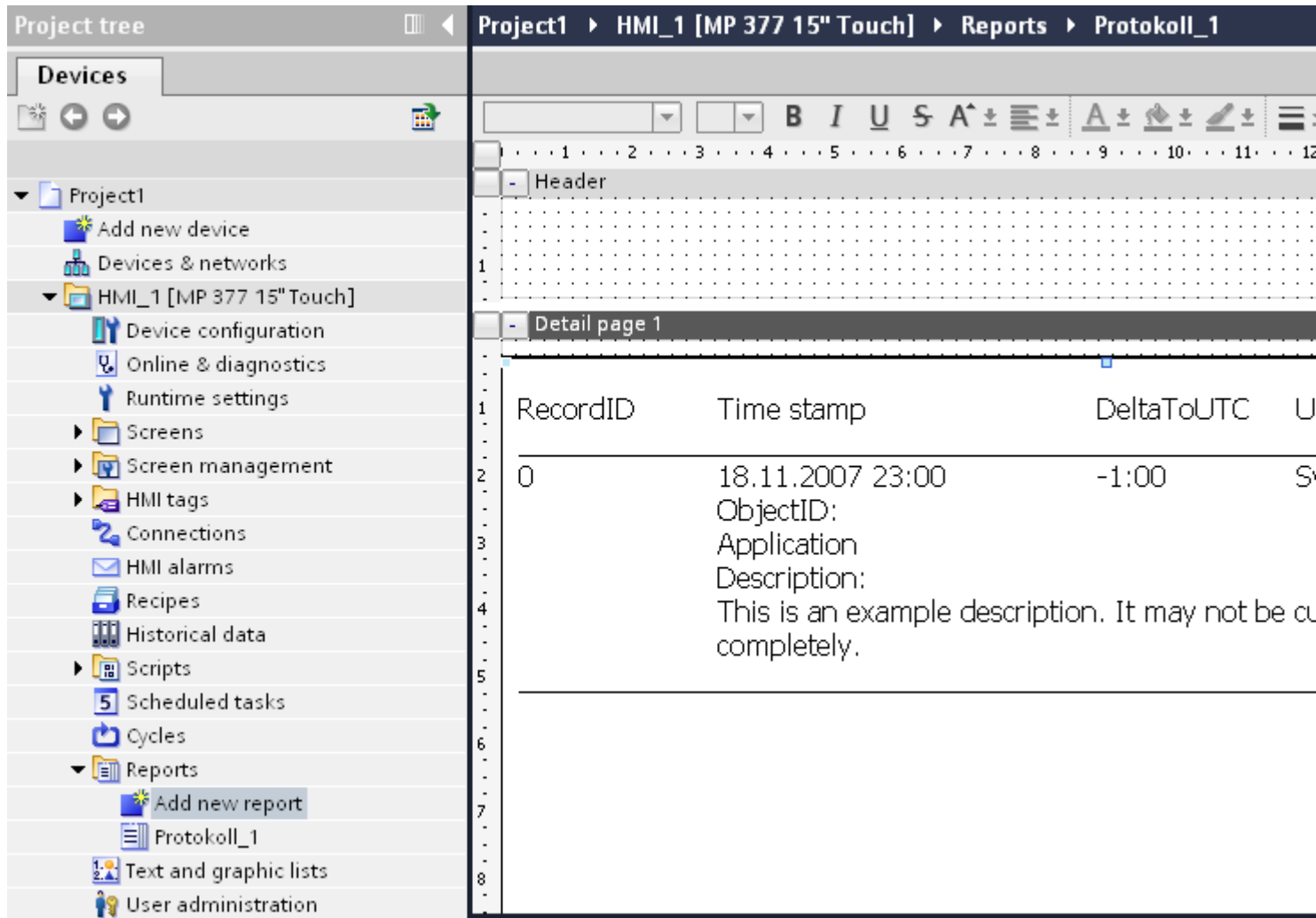
Once the printout is started in runtime, all entries currently contained in the Audit Trail are printed out.

Procedure

To create a report, proceed as follows:

1. Double-click on the "Reports" entry in the project tree.
2. Double-click "Add new report".
A new report is created and opened in the "Report" editor.

3. Drag & drop the "Audit trail report" object under "Tools > Controls" to the report created.



4. Click on the "Audit trail report" object.
5. Change the object properties of the "Audit trail report" object in the inspector window.

Result

You have created a report for the printout Audit Trail.

1.2.6.3 Parameters for the audit trail report (Panels, Comfort Panels, RT Advanced)

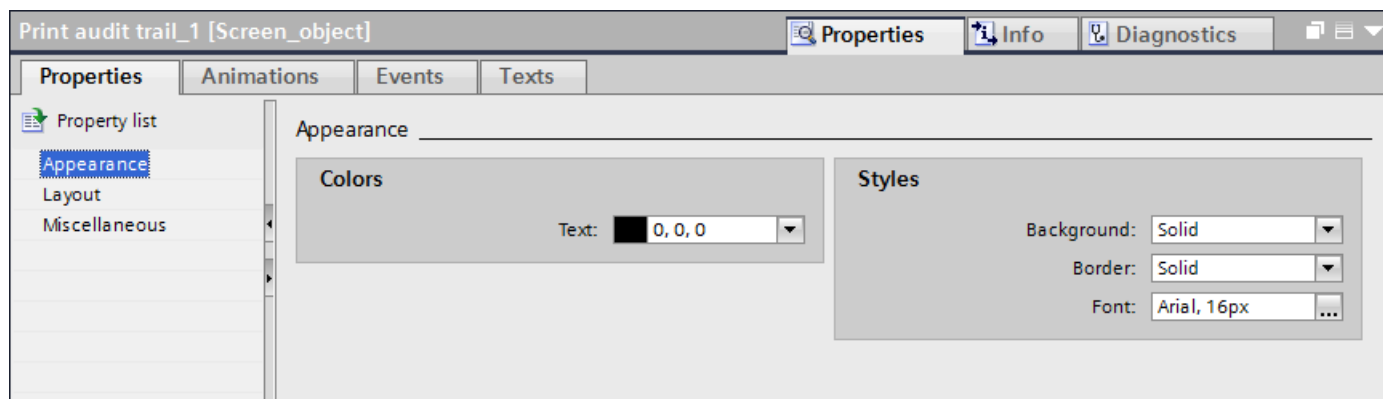
Introduction

The "Audit trail report" parameters can be edited in the inspector window.

Inspector window appearance

Click on the "Audit trail report" object.

Change the appearance of the "Audit trail report" object in the appearance area of the Inspector window under "Properties > Properties > Layout".



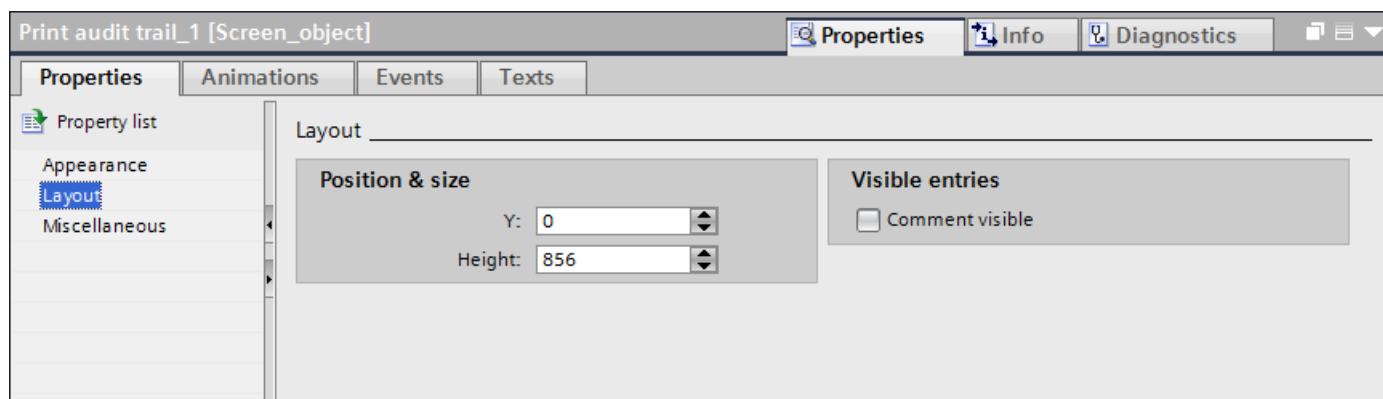
You can configure the foreground color, the background color, the style, and the font settings.

It is recommended to set a font size of 16 px for the output.

Inspector window layout

Click on the "Audit trail report" object.

Change the position and size of the "Audit trail report" object in the appearance area of the Inspector window under "Properties > Properties > Layout".



The "Audit trail report" object always fills the space down to the footer on the report page. If you change the height of the object, then you only change the distance of the object to the header. The report printout can involve a large amount of data.

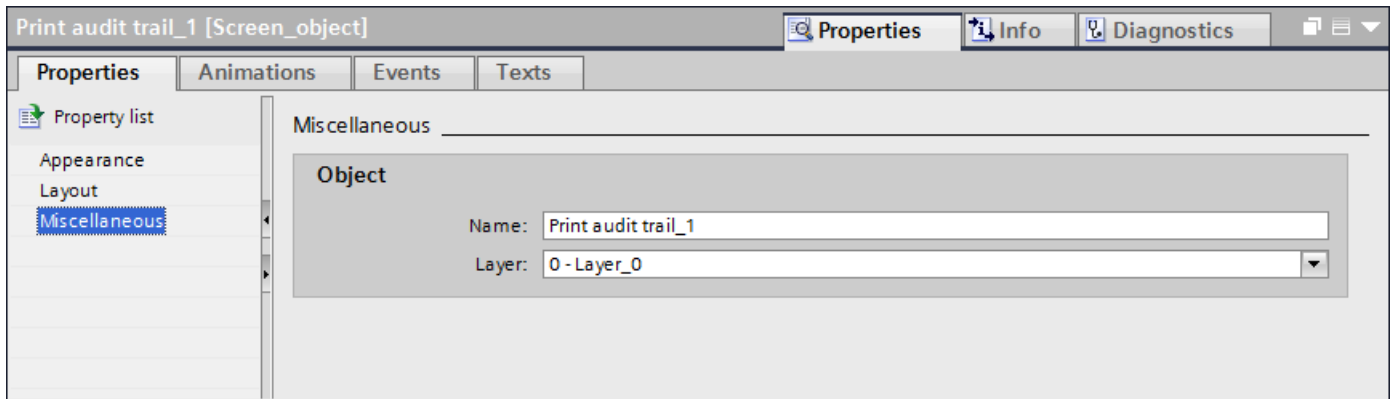
A page break is automatically inserted when the length of the page is exceeded to print out all data.

In the "Visible entries" area, it is determined whether comments are visible on the printed report.

Inspector window miscellaneous

Click on the "Audit trail report" object.

Change the name and layer position of the "Audit trail report" object in the appearance area in the Inspector window under "Properties > Properties > Miscellaneous".



1.2.6.4 Printing out an audit trail report (Panels, Comfort Panels, RT Advanced)

Introduction

Since logging of the Audit must be stopped in order to print out an Audit Trail, a few details regarding this procedure must be noted.

The following steps must be taken to print out an audit trail in a report file on a printer:

- Stop logging using the "StopLogging" system function.
- Start the printout using the "PrintReport" system function.
- Check if the printing is successfully completed.
- If needed, move or delete the Audit Trail using the "ArchiveLogFile" or "ClearLog" system functions.
- Start the logging of Audit by selecting the "StartLogging" system function.

Note

Make sure that the Audit Trail has been printed completely before you delete the Audit Trail.

Requirements

- "GMP compliant configuration" has been enabled.
- A report for the printout of an Audit Trail has been configured.
- The screen for the operator control to be configured is open.

Procedure

1. Add a button to the screen and select "Events > Click" in the Properties window.
2. In the function list, assign the "StopLogging" system function to the "Click" event and select your Audit Trail log.
3. Insert an additional button and assign the "PrintReport" system function to the "Click" event of this button.
4. Configure the "StartLogging" system function in the same function list.
5. Assign unique labels to the buttons.
6. Save the project.

Note

Note the device-specific differences when printing PDFs. You can find additional information at AUTOHOTSPOT.

Result

You have configured the required buttons and system functions. The operator can perform the operating tasks described in the introduction during runtime to print out an Audit Trail report.

Note

You can also insert the report objects for the output of alarms and recipes in the report for the printout of an Audit Trail. However, since GMP-relevant operations and system processes are not recorded while you are printing, you should preferably print the Audit Trail in a separate operation.

1.2.7 Evaluating an audit trail (Panels, Comfort Panels, RT Advanced)

1.2.7.1 Evaluating audit trails (Panels, Comfort Panels, RT Advanced)

Introduction

The Audit Trail has been saved to the memory card of the HMI device and is also read only.

The Audit Trail is protected by a checksum. This checksum ensures that the entry has not been modified at any later time.

There are two possible ways to evaluate the Audit Trail:

- Use the "Audit Viewer":
You can easily evaluate the Audit Viewer for external analysis on an Office PC with the help of the Audit Trail.
- Use the "HmiCheckLogIntegrity" DOS program:
The DOS program makes it possible to carry out an automatic check of the Audit Trail using the return values.

1.2.7.2 Evaluating Audit Trails in AuditViewer (Panels, Comfort Panels, RT Advanced)


Introduction

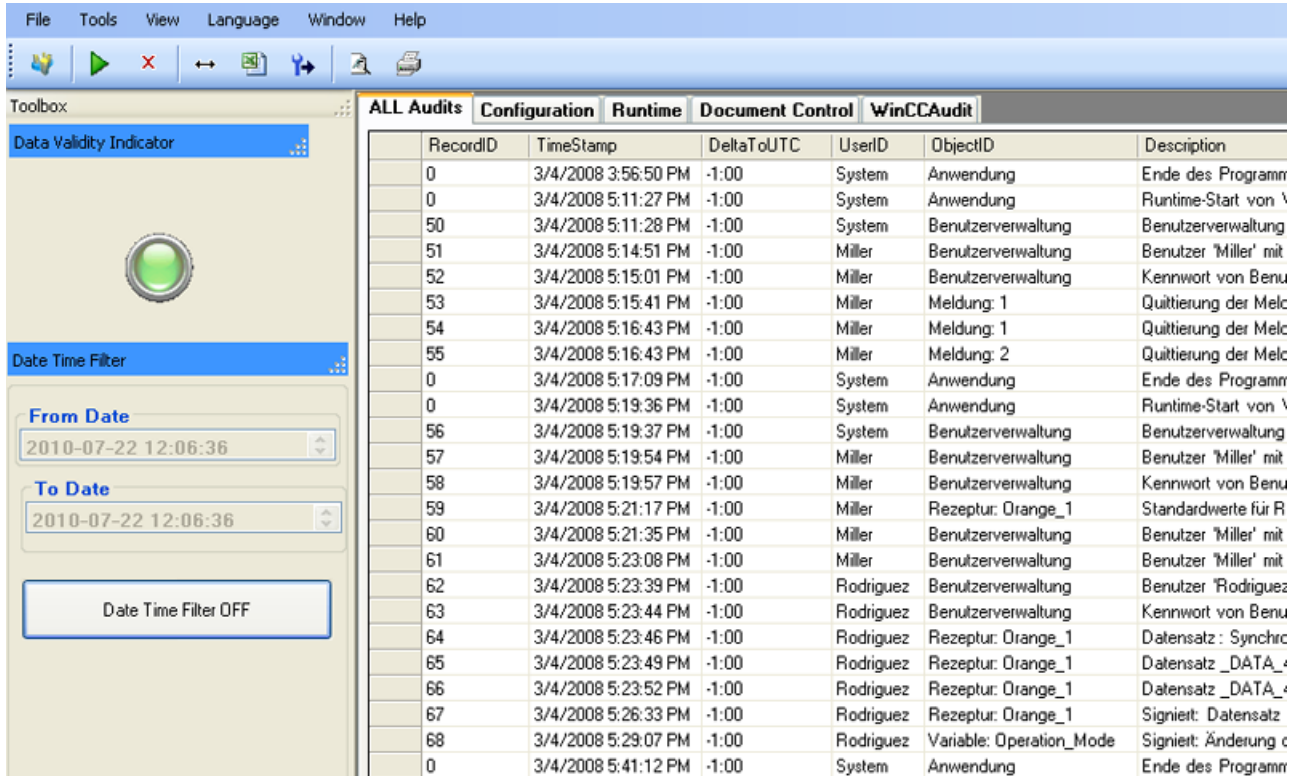
The Audit Viewer allows you to evaluate all Audit Trail data in a table.

Requirements

- Audit Viewer is installed
- The Audit Traillog is located on the computer which has Audit Viewer installed.

Procedure

1. Start the Audit Viewer on the configuration PC:
"Start > SIMATIC > Audit Viewer > Audit Viewer"
This path may be different on your operating system version.
2. Click the  button.
3. Load the Audit Trail:



| RecordID | TimeStamp | DeltaToUTC | UserID | ObjectID | Description |
|----------|---------------------|------------|-----------|--------------------------|-----------------------|
| 0 | 3/4/2008 3:56:50 PM | -1:00 | System | Anwendung | Ende des Programms |
| 0 | 3/4/2008 5:11:27 PM | -1:00 | System | Anwendung | Runtime-Start von \ |
| 50 | 3/4/2008 5:11:28 PM | -1:00 | System | Benutzerverwaltung | Benutzerverwaltung |
| 51 | 3/4/2008 5:14:51 PM | -1:00 | Miller | Benutzerverwaltung | Benutzer 'Miller' mit |
| 52 | 3/4/2008 5:15:01 PM | -1:00 | Miller | Benutzerverwaltung | Kennwort von Benu |
| 53 | 3/4/2008 5:15:41 PM | -1:00 | Miller | Meldung: 1 | Quittierung der Mel |
| 54 | 3/4/2008 5:16:43 PM | -1:00 | Miller | Meldung: 1 | Quittierung der Mel |
| 55 | 3/4/2008 5:16:43 PM | -1:00 | Miller | Meldung: 2 | Quittierung der Mel |
| 0 | 3/4/2008 5:17:09 PM | -1:00 | System | Anwendung | Ende des Programms |
| 0 | 3/4/2008 5:19:36 PM | -1:00 | System | Anwendung | Runtime-Start von \ |
| 56 | 3/4/2008 5:19:37 PM | -1:00 | System | Benutzerverwaltung | Benutzerverwaltung |
| 57 | 3/4/2008 5:19:54 PM | -1:00 | Miller | Benutzerverwaltung | Benutzer 'Miller' mit |
| 58 | 3/4/2008 5:19:57 PM | -1:00 | Miller | Benutzerverwaltung | Kennwort von Benu |
| 59 | 3/4/2008 5:21:17 PM | -1:00 | Miller | Rezeptur: Orange_1 | Standardwerte für R |
| 60 | 3/4/2008 5:21:35 PM | -1:00 | Miller | Benutzerverwaltung | Benutzer 'Miller' mit |
| 61 | 3/4/2008 5:23:08 PM | -1:00 | Miller | Benutzerverwaltung | Benutzer 'Miller' mit |
| 62 | 3/4/2008 5:23:39 PM | -1:00 | Rodriguez | Benutzerverwaltung | Benutzer 'Rodriguez |
| 63 | 3/4/2008 5:23:44 PM | -1:00 | Rodriguez | Benutzerverwaltung | Kennwort von Benu |
| 64 | 3/4/2008 5:23:46 PM | -1:00 | Rodriguez | Rezeptur: Orange_1 | Datensatz: Synchr |
| 65 | 3/4/2008 5:23:49 PM | -1:00 | Rodriguez | Rezeptur: Orange_1 | Datensatz _DATA_ |
| 66 | 3/4/2008 5:23:52 PM | -1:00 | Rodriguez | Rezeptur: Orange_1 | Datensatz _DATA_ |
| 67 | 3/4/2008 5:26:33 PM | -1:00 | Rodriguez | Rezeptur: Orange_1 | Signiert: Datensatz |
| 68 | 3/4/2008 5:29:07 PM | -1:00 | Rodriguez | Variable: Operation_Mode | Signiert: Änderung c |
| 0 | 3/4/2008 5:41:12 PM | -1:00 | System | Anwendung | Ende des Programms |

The "Data Validity Indicator" is lit up in green to indicate that the loaded Audit Trail has not been manipulated.

Each entry in the Audit Trail is time-stamped to allow precise tracking of operator actions. In addition to system events, such as the attempt to import a password list, the system also records failed login attempts:

1.2.7.3 Evaluating Audit Trails with DOS program (Panels, Comfort Panels, RT Advanced)

Introduction

Long-term archiving on a server allows an Audit Trail to be checked automatically using return values in a script.

1.2 Using the Audit trail (Panels, Comfort Panels, RT Advanced)

In addition the programmer can integrate the check using the DOS program "HmiCheckLogIntegrity" into the archiving process. "HmiCheckLogIntegrity" then provides the following return values:

- < 0: Different errors, for example, wrong file format or no file exists.
- 1: The checked Audit Trail is valid.
- > 0: The first line that was manipulated will be returned.

Audit Trail logging is only continued if the return value is "1". In both error cases, the administrator or the shift supervisor can be informed.

HmiCheckLogIntegrity

The "HmiCheckLogIntegrity.exe" DOS program is in the installation directory under:
"SIEMENS > Automation > WinCC Runtime Advanced"

1.2.8 Audit trail logging concept (Panels, Comfort Panels, RT Advanced)

1.2.8.1 Format (Panels, Comfort Panels, RT Advanced)

Format - Audit Trail

On an HMI device with "GMP compliant configuration", all events which are relevant to the audit are recorded at runtime in the Audit Trail. You have several format options.

Selection is dependent on the display program and the runtime language used:

- RDB file
Data is saved with quick access in a proprietary database.
If you require maximum read performance in Runtime, use the "RDB file" storage location.
- CSV file
To view and evaluate a CSV file use, e.g. Microsoft Excel on your PC.

Note

Double quotation marks or several characters are not permitted as list separators for the storage site "File - CSV (ASCII)". You can find the settings for list separators under "Start > Settings > Control Panel > Regional and Language Options".

- TXT file
This file format supports all characters that can be used in WinCC. For editing, you will need software that can save files in Unicode, such as Notepad.

Note

Use "File - TXT (Unicode)" to log Asian languages.

Audit Trail with checksum

The following files are generated under special circumstances:

- *.keep
 - If a log is started without checksum and will be continued with a checksum.
 - If you update WinCC with a service pack or a new version and the Audit Trail or the log is continued with the checksum.
 - The content of the keep file will remain the same when compared with the original log file.

Note

Before you update WinCC with a Service Pack or a new version, exit and save the Audit Trail or the logs using checksum. After WinCC is updated, the audit trail or logs will be continued with new files using checksum.

- *.bak
 - If runtime has determined a serious, irregular problem in the file.

1.2.8.2 Storage location and medium (Panels, Comfort Panels, RT Advanced)

Storage location and medium

Depending on the hardware configuration of the HMI device, the data may be logged locally (on the hard disk of a PC or on the storage card of a panel) or, if present, on a network drive.

Note

Logging on network drives

We do not recommend that you log audit trails directly on a network drive. Power supply can be interrupted at any time. This means there is no guarantee for a reliable operation of logs and audit trails.

We recommend you save the logs on your local hard drive, or on a storage medium of the HMI device. Use the system function "ArchiveLogFile" to save the logs long-term on a network drive.

A "GMP compliant configuration" cannot be operated at runtime to the full extent unless it is possible to save all user actions which are relevant to the audit to the Audit Trail. It must be ensured that sufficient storage space is available for the Audit Trail and that the connection to the storage location for the Audit Trail is not disturbed.

Error-handling with insufficient free storage space

If there is insufficient storage space, your project can be configured so that the administrator has an option of continuing the process without logging in the audit trail (forcing).

Error-handling if there is no storage medium or the connection to the server is interrupted

All audit-relevant user actions are blocked if insufficient storage space is available for the Audit Trail, e.g. due to missing storage medium.

Blocking is canceled as soon as the storage location for the Audit Trail is available again. The block can be skipped by "forcing".

Error-handling with long-term logging

If the audit trail must be moved to a server for long-term logging and the connection to the server is interrupted at this time, the following error-handling is required:

The system closes the audit trail and renames it. The system attempts to send the renamed audit trail to the server again in the background.

If disruption in the connection to the server persists, you receive a system alarm telling you that the connection is down. Then the system attempts to send the renamed audit trail every 300 seconds.

The attempt to transmit the data is repeated until successfully completed. The data is also transmitted after a restart of the HMI device.

"Forcing"

If the storage space for the audit trail is insufficient, for example if there is no storage medium or it is full, all audit-relevant user actions are automatically blocked.

In this case the audit trail logging can be configured to give an administrator the option of continuing to operate the system without logging the audit trail (forcing).

The administrator can also be given the option of running the system quickly out of a critical state in case of emergency. In this case the administrator can operate the system without the requirement to input the required electronic signatures or comments.

If the administrator uses the "forcing" function, this is logged as the last entry in the audit trail.

After the end of forcing, the audit trail must be restarted with the system function "StartLogging".

1.2.8.3 Protection mechanisms (Panels, Comfort Panels, RT Advanced)

Protective mechanisms to prevent changes to audit trail data

The audit trail data are protected against deliberate or accidental changes:

- The directory in which the audit trail is saved can only be accessed with special rights.
- The audit trail files are write-protected.
- Each data record contains a checksum that can be used to detect a change of its contents. This checksum also ensures that the number of lines has not changed in the audit trail file.

Use the "HmiCheckLogIntegrity" tool, included in the audit option, to check whether an audit trail has been changed:

AUTOHOTSPOT

1.2.8.4 Upgrading WinCC (Panels, Comfort Panels, RT Advanced)

Upgrading WinCC

Before you update WinCC with a Service Pack or a new version, you will have to exit and save the Audit Trail or the logs with checksum. After WinCC is updated, the audit trail or logs with checksum will be continued with new files.

Make sure that the logs are started at a defined state with the new version.

1.2.8.5 Audit trail behavior in runtime (Panels, Comfort Panels, RT Advanced)

Effects in runtime

The configuration in Audit Trail has the following effects in runtime, depending on the configuration:

- Audit relevant user actions (such as tag changes and recipe changes) are recorded in an audit trail.
- "Enable logging at runtime start" check box enabled:
The audit trail is started with runtime.
- "Forcing" group, "Allowed if storage space has been exhausted" check box enabled:
A user with administrator rights can use "forcing" to run operations on the plant even though the audit trail can no longer be logged because of storage space limitations. Interrupting the audit trail prevents the process from being stopped.
If the check box "Signing may be bypassed" is enabled, the administrator is not required to input electronic signatures, acknowledgments or comments for operator actions that would normally require signing, acknowledgment or comment.
- If the storage space available for the Audit Trail is less than the configured "Minimum storage space in MB", the function list configured for the "Low free storage space" event will be processed.
- If there is insufficient storage space for the audit trail because of hardware limits, the function list configured for the "Free space critically low" event will be processed.

1.3 Configuring audit functions (Panels, Comfort Panels, RT Advanced)

1.3.1 Logging tag value changes (Panels, Comfort Panels, RT Advanced)

1.3.1.1 Tag value change (Panels, Comfort Panels, RT Advanced)

Changes to tag values

User actions in runtime are recorded in a Audit Trail once "GMP compliant configuration" has been enabled.

When you configure a GMP compliant project, you specify which tags must meet the requirements of Good Manufacturing Practice (GMP).

If the user changes the value of a GMP-relevant tag in runtime, the value change action is logged in the Audit Trail .

Note

The action of changing the value of GMP-relevant tags made by the PLC, or a system function, is not logged in the Audit Trail.

The system functions used to change the values of GMP-relevant tags which are assigned to events that identify a direct user action are logged.

In addition, configure the "NotifyUserAction" system function to make a manual entry in the Audit Trail or to prompt the user for an electronic signature, an acknowledgment, or a comment.

With the "NotifyUserAction" system function only the value changes that are directly triggered by the event to which the system function is configured are entered in the Audit Trail. For example, if additional tags are changed by changing the value of one tag, the additional value changes are not logged in the Audit Trail.

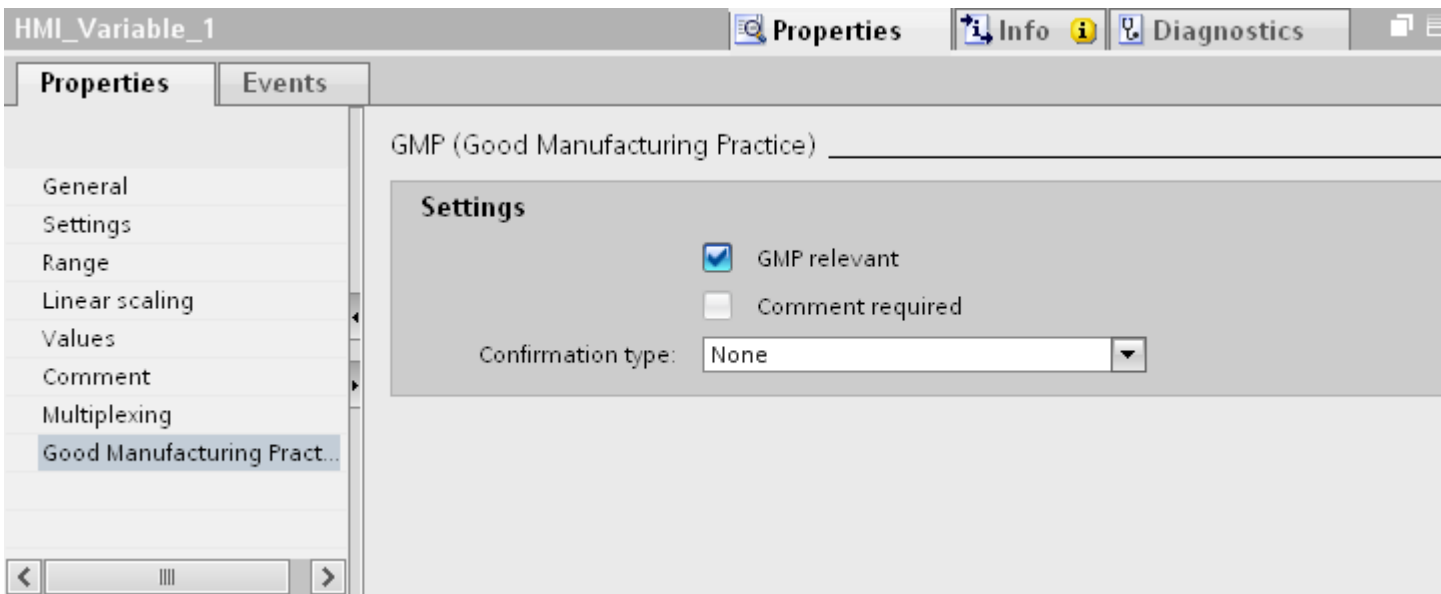
1.3.1.2 Logging tag value changes (Panels, Comfort Panels, RT Advanced)

Requirement

- "GMP compliant configuration" has been enabled.
- The tags for which you want to configure the GMP settings are created.
- The property view is open.

Procedure

1. Open the HMI tags editor and select the tag for which you want to make GMP settings.



2. Click "GMP relevant" under "Properties > Properties > GMP" in the Inspector window.
3. Specify how the user must confirm a value change in the "Confirmation type" selection field:
 - "Electronic signature"
If the user's electronic signature is required.
 - "None"
If the value change is to be logged in the Audit Trail without user confirmation.
 - "Acknowledgment"
If user acknowledgement of the value change is required.
4. Enable the "Comment required" check box if the user is required to input a comment as well as an electronic signature or acknowledgment.
This check box is only enabled if "Electronic signature" or "Acknowledgment" is specified under "Type of confirmation".

Result

If the user changes the value of a GMP-relevant tag in runtime, the value change is entered in the Audit Trail.

1.3.1.3 Effects of tag change (Panels, Comfort Panels, RT Advanced)

Effects in runtime

The configuration has the following effects in runtime depending on the properties of the GMP-relevant tags:

- If the user changes the value of a GMP-relevant tag in runtime, the value change is entered in the Audit Trail.
- Electronic signature
If "Electronic signature" is specified as the "Type of confirmation", the user must log every user-related value change of the tags using an electronic signature. Otherwise the value change will be rejected.
The user name used to sign the change is logged in the audit trail.
- Acknowledgement
If "Acknowledgment" is specified as the "Type of confirmation", the user must acknowledge every user-related value change of the tags. Otherwise the value change will be rejected.
The acknowledgement is logged in the Audit Trail.
- Comments
If the "Comment required" check box is enabled, the user must also comment every user-related value change of the tags, in addition to acknowledgment or input of the electronic signature. Otherwise the value change will be rejected.
The entered comment is logged in the Audit Trail.

1.3.2 Logging recipe data record changes (Panels, Comfort Panels, RT Advanced)

1.3.2.1 Recipe data changes (Panels, Comfort Panels, RT Advanced)

Changes to recipe data

User actions in runtime that are relevant to the quality of the process, such as changes of tag values or recipe values, are recorded in an Audit Trail once "GMP compliant configuration" has been enabled.

You specify during configuration which recipes must meet the requirements of "Good Manufacturing Practice" (GMP).

For GMP-relevant recipes, the following operations during runtime are recorded in the Audit Trail:

- Storing after changing and creating recipe data records
- Transfer of recipe data records to the PLC and from the PLC
- For recipe tags: Changing the setting for the synchronization of the tag values with the PLC ("offline"/"online") if the recipe tags are configured as "GMP-relevant".

Note**Differences in the Audit Trail with recipe display and recipe screen**

If you use a recipe screen to save recipe data, enable the "GMP-relevant" property for the recipe tags. If the user changes the value of a GMP-relevant recipe tag in runtime, the changed value is recorded in the Audit Trail. You can also configure for the tag to require the user to confirm the value change with an electronic signature and enter a comment.

If you use a recipe display to edit data records of a GMP-relevant recipe, the Audit Trail includes a record of which recipe data records were saved or sent to the PLC. The value changes to the recipe tags are not logged in the Audit Trail. Use the "ExportDataRecords" system function to save the value change to data records in a csv file.

If you want to make changes to recipe data records in conformance to the FDA, disable "Enable edit mode" in the recipe view. Use the recipe screen and "GMP relevant" recipe tags.

If you export recipe data records in a regulated project, you can assign the recipe data with a checksum. When you later import the recipe data back, you can use the checksum to determine if the recipe data has changed. The following system functions are available for exporting and importing recipe data with a checksum:

- "ExportDataRecordsWithChecksum"
- "ImportDataRecordsWithChecksum"

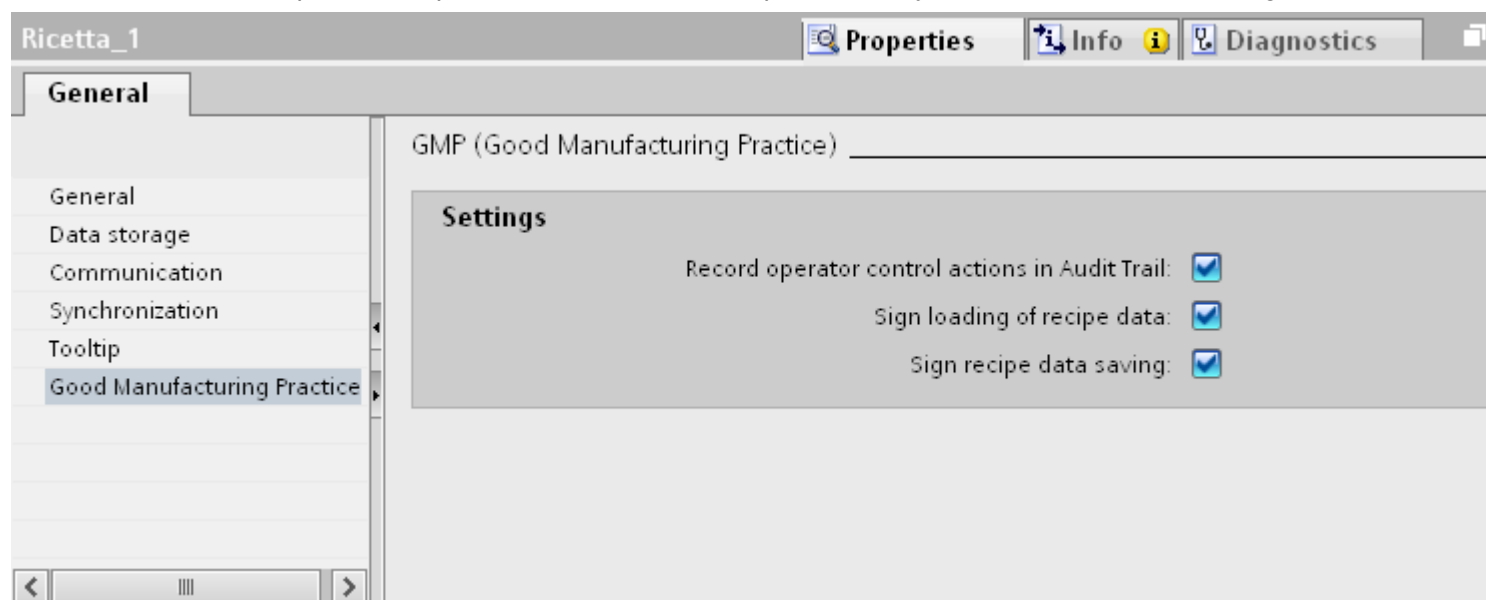
1.3.2.2 Logging recipe data changes (Panels, Comfort Panels, RT Advanced)

Requirement

- "GMP compliant configuration" has been enabled.
- The recipes for which you want to configure the GMP settings are created.
- The property view is open.

Procedure

1. Open the recipe editor and select the recipe for which you want to make GMP settings.



2. Click "GMP relevant" under "Properties > Properties > GMP" in the Inspector window.
3. Under "Settings", select the following:
 - "Record operations in audit trail:"
If all user actions in runtime that affect this recipe are to be recorded in the Audit Trail.
 - "Sign loading of recipe data":
If the user is required to confirm the transfer of recipe data records to or from the PLC using an electronic signature.
 - "Signature for saving recipe data: "
If the user is required to confirm recipe data record saving with an electronic signature.

Result

If the user works with the GMP-relevant recipe in runtime, the change is entered in the Audit Trail.

1.3.2.3 Effects of recipe data change (Panels, Comfort Panels, RT Advanced)

Effects in runtime

The configuration has the following effects in runtime depending on the properties of the GMP-relevant recipes:

Entries in the Audit Trail

Entries are made in the following cases:

- You create and save new recipe data records of a GMP-relevant recipe at runtime.
- You edit recipe data records of a GMP-relevant recipe and save your changes at runtime.
- Recipe data records are transferred to the PLC or recipe data are read from the PLC.
- The "SetRecipeTags" system function is used to change the setting for synchronization of the tag values with the PLC.

This concerns the following changes:

- "offline" to "online"
- "online" to "offline"

Electronic signature

The user must enter an electronic signature in the following cases depending on the configuration:

- The "Sign loading of recipe data" check box is set:
Signature for the transfer of recipe data records to the PLC. Signing is always required if the transfer is triggered with the recipe display functions and even if it is triggered with "SetDataRecordToPLC" system functions.
- The "Sign saving of recipe data" check box is set:
Sign saving of recipe data records. The signature is always required if the save is triggered with the system functions of the recipe display, and even if it is triggered with the "SetDataRecordToPLC" or "SaveDataRecord" system function.
- The user name used to sign the change is logged in the audit trail.

Note

The triggering of the "ImportDataRecords" system function is entered in the Audit Trail but does not require a signature or a comment. In addition, call the "NotifyUserAction" system function to request an electronic signature with or without user comment.

1.3.3 Logging user actions (Panels, Comfort Panels, RT Advanced)

1.3.3.1 User actions with GMP-compliant configuration (Panels, Comfort Panels, RT Advanced)

Introduction

In GMP compliant configuration, user actions and system operations in runtime that are relevant for the quality of the process are recorded in an Audit Trail .

For example, a user logon to the system or the change of a tag value are saved in the log.

In runtime, user actions are saved in an Audit Trail under the following conditions:

- "GMP compliant configuration" has been enabled
- A user is logged on to the system

1.3.3.2 Logging modes (Panels, Comfort Panels, RT Advanced)

Automatic logging of user actions

The following user actions are recorded in runtime without the need for additional configuration steps if "GMP compliant configuration" is enabled:

- User Administration
 - Logon and logoff of users
 - Import of user administration
- Alarm system
 - All alarms that are acknowledged by the user.
If an alarm from an alarm group is acknowledged, an entry is made in the Audit Trail indicating that all other alarms of this group have been acknowledged.
 - All acknowledgment attempts of the user

Note

Logging alarm text

To log alarm texts, select the "Log alarm texts in Audit Trail" option in the Audit Trail editor.

- Log operations
 - Starting and stopping a log
 - Opening and closing all logs
 - Deleting a log
 - Starting a sequence log
 - Copying a log
 - Long-term logging of a log

Configuration-dependent logging

The following processes are logged depending on the configuration of the recipes and the tags of the project:

- Change values of GMP-relevant tags by the user
- for GMP-relevant recipes
 - You create and save new recipe data records of a GMP-relevant recipe at runtime.
 - You edit recipe data records of a GMP-relevant recipe and save your changes at runtime.
 - Transfer of recipe data records to the PLC and from the PLC
 - For recipe tags: Changing the setting for the synchronization of the tag values with the PLC ("offline"/"online")

In addition to logging user actions you can configure tags and recipes to require the user to confirm or acknowledge specific actions with an electronic signature or add a comment to the change.

Manual logging by means of "NotifyUserAction" system function

This system function is used to record actions in the Audit Trail that are not automatically entered in the Audit Trail. This system function is also used to request the user to enter an electronic signature for the action.

1.3.3.3 Configuring the "NotifyUserAction" system function (Panels, Comfort Panels, RT Advanced)

Introduction

This system function is used to log user actions that are not entered automatically entered in the Audit Trail. This system function can also used to request an acknowledgment, or an electronic signature for the user's action.

In this example, the system function is assigned to a button. All operations with this button are logged to the Audit Trail.

Requirements

- "GMP-compliant configuration" has been enabled.
- You created the object that is to be assigned the system function.
A button is used in this example.
- The properties window is open.

Procedure

1. Click the button.
2. Click on "Events" in the Inspector window.
3. Assign the "NotifyUserAction" system function to the "Click" event.

1.3.3.4 GMP-compliant user administration (Panels, Comfort Panels, RT Advanced)**SIMATIC Logon**

To run a central user and user group administration for several applications or HMI devices, activate SIMATIC Logon.

For more information on user administration and SIMATIC Logon, refer to the following chapter:
AUTOHOTSPOT

1.3.4 Logging system functions (Panels, Comfort Panels, RT Advanced)**Introduction**

If system functions are triggered in runtime, this is recorded in the Audit Trail for some system functions. If specific system functions are used on a GMP-relevant object, the user must confirm the triggering.

Some system functions are not supported when using Audit. If you use these system functions in your project, you are solely responsible for them.

The following table shows which system functions are Audit-relevant and whether the user's signature is required:

System functions and Audit

| Function (call in script) | Effect of /Audit |
|---|------------------------|
| StartLogging (StartLogging) | entered in Audit Trail |
| StopLogging (StopLogging) | entered in Audit Trail |
| ClearLog (ClearLog) | entered in Audit Trail |
| StartNextLog (StartNextLog) | entered in Audit Trail |
| CloseAllLogs (CloseAllLogs) | entered in Audit Trail |
| OpenAllLogs (OpenAllLogs) | entered in Audit Trail |
| LogTag (---) | --- |
| CopyLog (CopyLog) | entered in Audit Trail |
| ActivateScreen (ActivateScreen) | --- |
| ActivateScreenByNumber (ActivateScreenByNumber) | --- |
| ActivatePreviousScreen (ActivatePreviousScreen) | --- |

1.3 Configuring audit functions (Panels, Comfort Panels, RT Advanced)

| Function (call in script) | Effect of /Audit |
|---|---|
| SetBitInTag (SetBitInTag) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |
| ResetBitInTag (ResetBitInTag) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |
| InvertBitInTag (InvertBitInTag) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |
| SetBit (SetBit) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |
| ResetBit (ResetBit) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |
| InvertBit (InvertBit) | entered in Audit Trail when tag is GMP-relevant System function must not be applied to tags that require signing or comment. |
| SetBitWhileKeyPressed (---) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |
| SetDataRecordToPLC (SetDataRecordToPLC) | entered in Audit Trail if the recipe is GMP-relevant Signing required depending on recipe configuration |
| GetDataRecordTagsFromPLC (GetDataRecordFromPLC) | entered in Audit Trail if the recipe is GMP-relevant |
| ImportDataRecords (ImportDataRecords) | entered in Audit Trail if the recipe is GMP-relevant |
| ImportDataRecordsWithChecksum (ImportDataRecordsWithChecksum) | entered in Audit Trail if the recipe is GMP-relevant |
| ExportDataRecords (ExportDataRecords) | --- |
| ExportDataRecordsWithChecksum (ExportDataRecordsWithChecksum) | --- |
| LoadDataRecord (LoadDataRecord) | entered in Audit Trail if the recipe is GMP-relevant Signing required depending on recipe configuration |

1.3 Configuring audit functions (Panels, Comfort Panels, RT Advanced)

| Function (call in script) | Effect of /Audit |
|--|--|
| SaveDataRecord (SaveDataRecord) | entered in Audit Trail if the recipe is GMP-relevant Signing required depending on recipe configuration |
| SetDataRecordTagsToPLC (SetDataRecordTagsToPLC) | entered in Audit Trail if the recipe is GMP-relevant Signing required depending on recipe configuration |
| GetDataRecordTagsFromPLC (GetDataRecordTags-FromPLC) | entered in Audit Trail if the recipe is GMP-relevant |
| SetRecipeTags (SetRecipeTags) | entered in Audit Trail if the recipe is GMP-relevant |
| GetDataRecordName (GetDataRecordName) | --- |
| ClearDataRecordMemory (ClearDataRecordMemory) | Not supported |
| ClearDataRecord (ClearDataRecord) | entered in Audit Trail if the recipe is GMP-relevant |
| PrintScreen (PrintScreen) | --- |
| PrintReport (PrintReport) | --- |
| RecipeViewSaveDataRecord (---) | entered in Audit Trail if the recipe is GMP-relevant Signing required depending on recipe configuration |
| RecipeViewSaveAsDataRecord (---) | entered in Audit Trail if the recipe is GMP-relevant Signing required depending on recipe configuration |
| RecipeViewNewDataRecord (---) | --- |
| RecipeViewClearDataRecord (---) | entered in Audit Trail if the recipe is GMP-relevant |
| RecipeViewGetDataRecordFromPLC (---) | entered in Audit Trail if the recipe is GMP-relevant |
| RecipeViewSetDataRecordToPLC (---) | entered in Audit Trail if the recipe is GMP-relevant Signing required depending on recipe configuration |
| RecipeViewSynchronizeDataRecordWithTags (---) | entered in Audit Trail if the recipe is GMP-relevant Signing required depending on recipe configuration |
| RecipeViewRenameDataRecord (---) | entered in Audit Trail if the recipe is GMP-relevant |
| RecipeViewBack (---) | --- |
| RecipeViewOpen (---) | --- |
| RecipeViewMenu (---) | --- |
| TrendViewScrollForward (---) | --- |
| TrendViewScrollBack (---) | --- |
| TrendViewExtend (---) | --- |

1.3 Configuring audit functions (Panels, Comfort Panels, RT Advanced)

| Function (call in script) | Effect of /Audit |
|---|---|
| TrendViewCompress (---) | --- |
| TrendViewBackToBeginning (---) | --- |
| TrendViewStartStop (---) | --- |
| TrendViewSetRulerMode (---) | --- |
| TrendViewBackToBeginning (---) | --- |
| StatusForceGetValues (---) | Not supported |
| StatusForceSetValues (---) | Not supported |
| AlarmViewAcknowledgeAlarm (---) | entered in Audit Trail |
| AlarmViewEditAlarm (---) | --- |
| AlarmViewShowOperatorNotes (---) | --- |
| HTMLBrowserBack (---) | Not supported |
| HTMLBrowserForward (---) | Not supported |
| HTMLBrowserRefresh (---) | Not supported |
| HTMLBrowserStop (---) | Not supported |
| ScreenObjectCursorUp (---) | --- |
| ScreenObjectCursorDown (---) | --- |
| ScreenObjectPageUp (---) | --- |
| ScreenObjectPageDown (---) | --- |
| PressButton (---) | --- |
| ReleaseButton (---) | --- |
| SmartClientViewConnect (---) | Not supported |
| SmartClientViewDisconnect (---) | Not supported |
| SmartClientViewReadOnlyOn (---) | Not supported |
| SmartClientViewReadOnlyOff (---) | Not supported |
| SmartClientViewRefresh (---) | Not supported |
| SmartClientViewLeave (---) | Not supported |
| ShowAlarmWindow (ShowAlarmWindow) | --- |
| ClearAlarmBuffer (ClearAlarmBuffer) | --- |
| ShowSystemAlarm (ShowSystemAlarm) | --- |
| SetAlarmReportMode (SetAlarmReportMode) | --- |
| Logoff (Logoff) | entered in Audit Trail |
| GetPassword (GetPassword) | --- |
| GetGroupNumber (GetGroupNumber) | --- |
| ExportImportUserAdministration (ExportImportUserAdministration) | Import of user administration is entered in Audit Trail Export is not entered in Audit Trail |
| Logon (Logon) | entered in Audit Trail |
| GetUserName (GetUserName) | --- |
| TraceUserChange (---) | --- |
| ShowLogOnDialog (---) | --- |

1.3 Configuring audit functions (Panels, Comfort Panels, RT Advanced)

| Function (call in script) | Effect of /Audit |
|---|---|
| LinearScaling (LinearScaling) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |
| InverseLinearScaling (InverseLinearScaling) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |
| IncreaseFocusedValue (---) | --- |
| DecreaseFocusedValue (---) | --- |
| OpenCommandPrompt (OpenCommandPrompt) | Not supported |
| OpenControlPanel (OpenControlPanel) | Not supported |
| ActivateCleanScreen (---) | --- |
| AdjustContrast (---) | --- |
| CalibrateTouchScreen (CalibrateTouchScreen) | --- |
| OpenScreenKeyboard (OpenScreenKeyboard) | --- |
| OpenTaskManager (OpenTaskManager) | Not supported |
| BackupRAMFileSystem (BackupRAMFileSystem) | Not supported |
| SetAcousticSignal (SetAcousticSignal) | --- |
| ShowOperatorNotes (ShowOperatorNotes) | --- |
| AcknowledgeAlarm (AcknowledgeAlarm) | entered in Audit Trail |
| GoToHome (GoToHome) | --- |
| GoToEnd (GoToEnd) | --- |
| EditAlarm (EditAlarm) | --- |
| DirectKeyScreenNumber (---) | Not supported |
| DirectKey (---) | Not supported |
| SetDeviceMode (SetDeviceMode) | entered in Audit Trail |
| SetDisplayMode (SetDisplayMode) | --- |
| SetConnectionMode (SetConnectionMode) | entered in Audit Trail |
| SetScreenKeyboardMode (SetScreenKeyboardMode) | --- |
| ChangeConnection (ChangeConnection) | Not supported |
| SetLanguage (SetLanguage) | --- |
| SetWebAccess (---) | Not supported |
| StartProgram (StartProgram) | Not supported |
| ShowSoftwareVersion (ShowSoftwareVersion) | --- |
| SimulateTag (---) | Not supported |
| StopRuntime (StopRuntime) | entered in Audit Trail |
| ControlWebServer (ControlWebServer) | Not supported |
| ControlSmartServer (ControlSmartServer) | Not supported |
| OpenInternetExplorer (OpenInternetExplorer) | --- |
| SendEMail (SendEMail) | --- |
| UpdateTag (---) | --- |
| ClearAlarmBufferProTool (ClearAlarmBufferProtoolLegacy) | Not supported |

1.4 Performance features of GMP relevant configuration (Panels, Comfort Panels, RT Advanced)

| Function (call in script) | Effect of /Audit |
|---------------------------|---|
| Encoding(Encode) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |
| EncodeEx(Encode) | entered in Audit Trail when tag is GMP-relevant Signature is mandatory, depending on the tag configuration |

1.4 Performance features of GMP relevant configuration (Panels, Comfort Panels, RT Advanced)

1.4.1 Supported HMI devices (Panels, Comfort Panels, RT Advanced)

Supported HMI devices

The qualification "GMP relevant configuration" can be configured for the following HMI devices:

- TP 277
- OP 277
- MP 277
- MP 377
- Comfort Panel
- Mobile Panel 277
- KTP Mobile Panel
- Panel PC with WinCC RT Advanced
- WinCC RT Advanced

Note

The qualification "GMP" is not supported by WinCC RT Professional.

1.4.2 Restrictions (Panels, Comfort Panels, RT Advanced)

Restrictions

The following functions and configurations cannot be used simultaneously with the qualification "GMP relevant configuration":

- "Watch table" object
- PN direct keys
- DP DirectKey
- Option /Sm@rtServer
- /Sinumerik option
- The functional scope of the HMI devices is only available to a restricted degree in some circumstances because of the limited storage space
- Events of screen objects
You can set mandatory acknowledgment of important user actions in runtime, such as changing tag values. If you assign an event which has to be acknowledged to a screen object, you may not assign any other events to this graphic object.
When the event of a screen object is assigned actions which open a user dialog (such as change of a tag value with mandatory acknowledgement), you may not be able to execute these actions at other events.
- Controlling GMP-relevant tags using a slider
The slider is not suitable for controlling GMP-relevant tags. Any operation of the slider will continuously change the tag value. If this is a GMP-relevant tag, a flood of entries will be generated in the AuditTrail.

1.5 Enabling GMP compliant configuration (Panels, Comfort Panels, RT Advanced)

Introduction

The Audit Trail and "Electronic Signature" functions are qualified as "GMP compliant configuration".

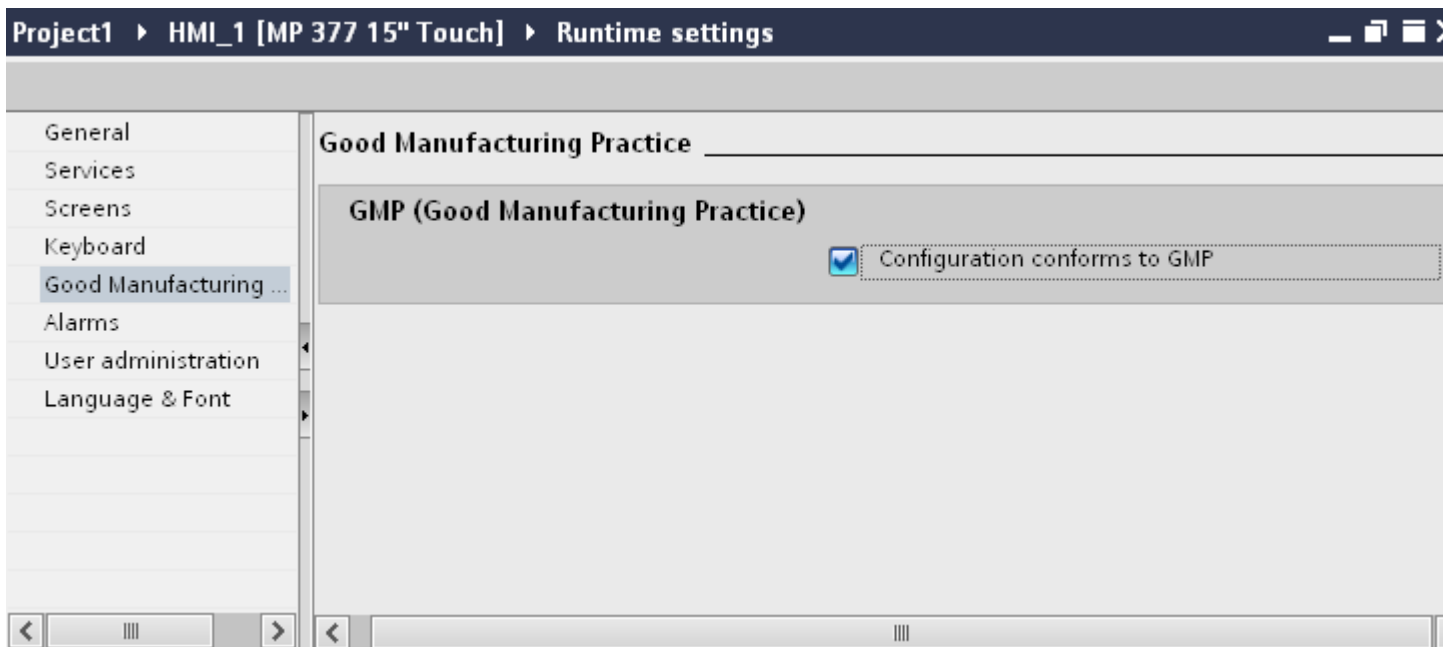
Requirements

- A project is created.
- A GMP compatible HMI device has been created.

Procedure

1. Double-click on the HMI device in the project tree.
2. Double-click "Runtime settings".

3. Click on "GMP".
4. Select "GMP compliant configuration".



Result

The Audit option is now enabled for the HMI device.

The following functions can now be configured:

- Audit Trail log
- "NotifyUserAction" system function
- GMP relevant tags
- GMP relevant recipes

WinCC Sm@rtServer (Panels, Comfort Panels, RT Advanced)

2

2.1 Basics (Panels, Comfort Panels, RT Advanced)

2.1.1 Sm@rt Options (Panels, Comfort Panels, RT Advanced)

Introduction

Using the Sm@rt Options from WinCC, you can communicate between HMI-systems or to an HMI-System by means of TCP/IP-connections (e.g.LAN).

Note

The Sm@rt options are not supported by PCs with multi-touch operation.

Use of the Sm@rt Options

- Distributed operator stations with Sm@rtClients for controlling large machines or machines that are spread out over a large area.
- Operator stations with system-wide access to current process data via the communication driver "SIMATIC HTTP Protocol".
- Local servicing solution for the central archiving, analysis and additional processing of process data.
- Provision of current process data for higher-level systems (SCADA, production management systems, office applications).
- Remote control of an HMI-System by means of Internet, Intranet and LAN.
- Sending of E-Mails on the basis of messages and events
- Provisioning of Standard-HTML-Pages in HMI-system with service-and maintenance information as well as diagnostic functions.
- Easy download of files from the Web browser on the Panel with the "Save as" browser command.

User benefits:

- Flexible solution for access to HMI systems and process data from any location
- Reduction of load on the field bus:
For example, the combination of WinCC Runtime and SIMATIC panels enables a factory control system to have access to process data. No load is placed by the factory level on the sensitive field level with respect to the necessary communication requirements. These requirements are handled by HMI Runtime along with the SIMATIC-panels.
- Expensive on-site service visits to be avoided by using the remote control. Unplanned non-operation periods are reduced and the system productivity is increased.

Note

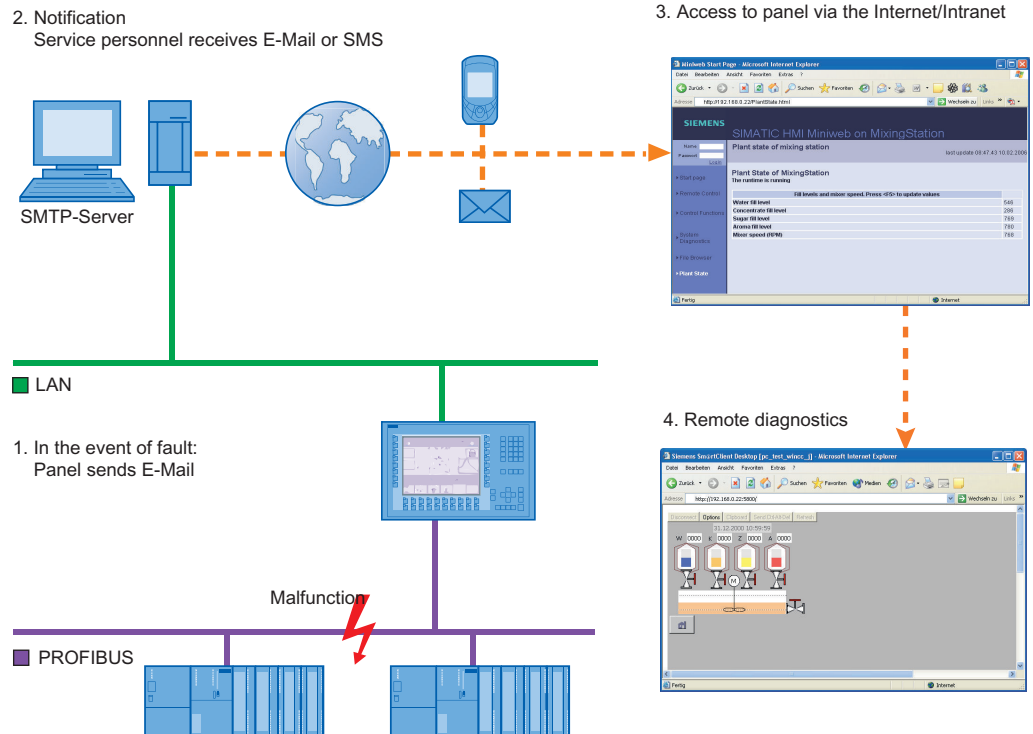
On devices with version V11 or V12, the password "100" is preset for the Sm@rtServer and for the integrated Web server. This password should be changed for security reasons.

On devices with version V13, no passwords are preset.

2.1.2 Application scenarios (Panels, Comfort Panels, RT Advanced)

E-Mailing and remote diagnostics

A factory has a service contract with an external service company. The HMI device and the service technician's PC are linked together over a TCP/IP-ready network. E-mail delivery of certain alarms to the service technician was configured in the project. The service technician accesses the HMI device via the Internet and executes remote diagnostics.



Application example:

Amongst other things, flow rates are measured in the process control of a cooling unit. Contamination in a feed line reduces the flow of coolant. When the flow rate drops below the configured threshold value, the operating device displays a warning. In addition, this warning is also dispatched as an e-mail to the assigned service technician.

The service technician then establishes a connection with the remote device and takes the appropriate actions.

Advantage: An alarm that reaches the service technician in a timely manner helps to minimize unplanned downtime.

Distributed operator stations

Distributed operator systems, the Sm@rtClients are used for controlling large machines or machines that are spread out over a large area.

The Client-HMI device connects to Sm@rtServer via the Sm@rtClient-Display.

The operator can operate and monitor the system from various locations. The operator sees the same image at each operator station, whereby only one station can be operated at one point of time.

The type of operation is also named as a coordinated operation. Then you must change the configuration only at Sm@rtServer.

Access to the tags via SIMATIC HMI HTTP Protocol

Operator stations with system-wide access

For use of the SIMATIC HMI HTTP Protocol, you can provide tags of HMI-device (HTTP-Server) to another device (HTTP-Client).

Thus the local as well as centrally used HMI-systems have access to the tags of other stations. Cell-concepts or line-concepts can be simply implemented. De-centrally obtained information is available centrally.

This concept also permits the setting of cost-effective and small central servicing. There are additional options for archiving, analysis and additional processing of registered process data, if a PC is used for that.

Remote monitoring and remote control- servicing solution

If you connect the use of the SIMATIC HMI HTTP Protocol and the Sm@rtServer with each other, you can implement a complex servicing solution.

For this, display the interested tags of the HMI-devices on the Service-PC. If necessary, use the PC for the remote monitoring and remote control of a specific HMI-device.

The locally used HMI-devices are connected with each other and the total process is controlled comprehensively.

The concept of the remote servicing is possible by using the Sm@rtClient-Display in the servicing HMI-Application. The operator has access to the respectively desired local HMI-device through flexible configuration of the Sm@rtClient-Display.

Connection to the Office-world

The possibility of data exchange exists between HMI-device and office-applications, e.g. MS Excel, with help of VBA-Macro.

For this, the HMI-device must support the Web-Service(SOAP). A script or macro is called in the external application, which has only read or write access to the concerned tags according to provided syntax.

2.1.3 HMI devices suitable for use (Panels, Comfort Panels, RT Advanced)

HMI devices suitable for use

The following table shows the HMI-devices that are suitable for the use of Sm@rt Options.

The number of the connections based on "SIMATIC HMI HTTP Protocol" and the number of maximum connected Sm@rtClients depends on the HMI-device. For additional information see the "Performance features" documentation and in the technical manual of your HMI-device.

Technical data subject to change.

| HMI device | Sm@rt Options |
|--|---------------|
| 270 series | Yes |
| 370 series | Yes |
| OP 177B PN/DP TP 177B PN/DP | Yes |
| Mobile Panel 177 PN Mobile Panel 277 | Yes |
| KTP700 Mobile Panel KTP900 Mobile Panel Mobile Panel 277 IWLAN Mobile Panel 277 IWLAN V2 | Yes |
| In view mode only: <ul style="list-style-type: none"> • KTP400F Mobile Panel • KTP700F Mobile Panel • KTP900F Mobile Panel • Mobile Panel 277F IWLAN (RFID Tag) | Yes |
| Comfort Panels | Yes |
| WinCC Runtime Advanced | Yes |

Combining options on panels

The following table shows which options and functions on the panels can be combined with each other.

Technical data subject to change.

| | SIMATIC HMI HTTP Protocol | Sm@rt Options | HTML browser | WinAC/ MP |
|---------------------------|---------------------------|---------------|--------------|-----------|
| SIMATIC HMI HTTP Protocol | -- | Yes | Yes | Yes |
| Sm@rtServer | Yes | -- | No | No |
| HTML browser | Yes | No | -- | No |
| WinAC/ MP | Yes | No | No | -- |

2.1.4 Settings for Sm@rt Options (Panels, Comfort Panels, RT Advanced)

2.1.4.1 Configuration in WinCC (Panels, Comfort Panels, RT Advanced)

Introduction

In the "Runtime-Settings" Editor, configure the requirements for using the Sm@rt Options.

As an alternative, configure the settings in the Control Panel of the HMI-device.

Note that the settings on the HMI device have a higher priority than the settings in the WinCC project.

Open

Double-click on the "Runtime-settings" entry in the project tree. In the "Runtime-settings" editor, click on the "Services".

The screenshot shows the WinCC Runtime settings editor window. The title bar indicates the path: ...V13_SP1 > RTAdvanced [SIMATIC PC station] > HMI_RT_4 [WinCC RT Advanced] > Runtime settings. The left sidebar contains a tree view with the following items: General, Services (selected), Screens, Keyboard, Good Manufacturing Practice, Alarms, User administration, Language & font, OPC settings, and Tag settings. The main area is titled "Services" and contains four sections:

- Remote control**: A checkbox labeled "Start Sm@rtServer" is present.
- Read/write tags**: Contains several options:
 - ☐ Operate as OPC server
 - ☐ OPC DCOM Server
 - ☒ OPC Unified Architecture Server
 - ☐ HTTP channel server
 - ☒ Web service SOAP
- Diagnostics**: A checkbox labeled "HTML pages" is present.
- SMTP Communication**: Contains several input fields:
 - Server name: [text box]
 - Port: [text box with value 25]
 - Name of sender: [text box]
 - E-mail address: [text box]
 - Login: [text box]
 - Password: [text box with masked characters *****)
 - ☐ Secure connection required (SSL)

"Remote control" Group.

Enter the settings for the selected HMI device in the work area:

- "Remote control" Group.
 - Start Sm@rtServer
Configures the HMI device as Sm@rtServer.

"Read/write tags" group for Panels

- Operate as OPC server
Configures the HMI device as an OPC server.
- HTTP channel server
Configures the HMI device as HTTP server.
- Web service SOAP
Activates tag access via SOAP.

"Read/write tags" group for Comfort Panels

- Operate as OPC UA server
Configures the HMI device as an OPC UA server.
- HTTP channel server
Configures the HMI device as HTTP server.
- Web service SOAP
Activates tag access via SOAP.

"Read/write tags" group for RT Advanced

- Operate as OPC server
 - OPC DCOM server
Configures the HMI device as an OPC DCOM server.
 - OPC UA server
Configures the HMI device as an OPC UA server.
- HTTP channel server
Configures the HMI device as HTTP server.
- Web service SOAP
Activates tag access via SOAP.

"Diagnostics" Group

- HTML pages
Activates service pages of the HMI device.

"SMTP Communication" Group

Activates service pages of the HMI device. "SMTP Communication" Group

- **Server name**
Enter the name of the SMTP server through which you want to send E-mails.
- **Port**
Enter the port number. The SMTP port number depends on the outgoing mail server of your service provider. You can obtain the port number from your service provider.
- **Sender name**
Enter the sender name. The recipient sees in the E-Mail from which device the E-mail originates, e.g. "HMI device Production line 2". If the function is not supported by the SMTP-Server, delete the entry. You can obtain more detailed information for this from your service provider.
- **E-mail address**
If you use an SMTP server that requires a valid e-mail address for authentication, enter it here, for example, "John.Doe@gmx.net."
- **Login**
If you use an SMTP server that requires a user name for authentication, enter it here. You can obtain the user name from your service provider.
- **Password**
If you are using an SMTP server that requires a password for authentication, enter this password. You can obtain the user name from your service provider.
- **The server requires a secure connection (SSL).**
The data are sent via an SSL connection. Your service provider can tell you if your mail server supports an SSL connection.

2.1.4.2 Configurations on the HMI device (Panels, Comfort Panels, RT Advanced)

Settings on the HMI device (Panels, Comfort Panels, RT Advanced)


Introduction

The Sm@rt Options settings in the HMI device are configured in the dialog box "WinCC Runtime Advanced Internet".

Additional tabs may be included in the dialog "WinCC Runtime Advanced Internet". This depends on which options are activated for the network operation in the project.

Note that the settings on the control unit have a higher priority than the settings in the WinCC-project.

Tabs

You have opened the dialog "WinCC Runtime Advanced Internet" with the symbol "WinCC Runtime Advanced Internet" .

The "WinCC Runtime Advanced Internet" dialog of the control panel can contain the following tabs:

- WinCC Runtime Advanced Internet, "Email" tab (Page 57)
- WinCC Runtime Advanced Internet, "Proxy" tab (Page 58)
- WinCC Runtime Advanced Internet, "Web Server" tab (Page 59)
- WinCC Runtime Advanced Internet, "Remote" tab (Page 60)

Input area plan

At Sm@rtServer and Sm@rtClient, the same input area plan must be set.

The Sm@rtServer uses the Standard-Input area plan of the operating system: (Start>Settings>Control Panel> Country settings>Tab "Entry"). These changes become effective after system restart.

At Sm@rtClient, the same input area plan must be set like at Sm@rtServer. No restart is necessary after the switchover of input area plan at Sm@rtClient.

WinCC Runtime Advanced Internet, "Email" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog

Specifies the settings for the E-Mailing.

Settings

- SMTP server
 - Use the default of project file
The SMTP-Server name from the WinCC-Project is used.
 - Enter the name of the SMTP server through which you want to send E-mails.
 - Port
Enter the port number. The SMTP port number depends on the outgoing mail server of your service provider. You can obtain the port number from your service provider.
- Name
 - Name of sender
Enter the sender name. The recipient sees in the E-Mail, from which device the E-mail originates, e.g. "HMI device Production line 2".
If the function is not supported by the SMTP-Server, delete the entry. You can obtain more detailed information for this from your service provider.
 - eMail Address of sender
If you use an SMTP server that requires a valid e-mail address for authentication, enter it here, for example, "John.Doe@gmx.net."

Dialog "Advanced Email Settings"

- Authentication
 - Use the default of project file
The user name and the password from the WinCC-Project are used.
 - Disable authentication
Authentication is not required.
 - Use panel settings for authentication
The settings of the HMI-device are used. Enter the user name under "Login" and the password under "Password". You can obtain the user name and the password from your service provider.
- Encryption
 - Use the default of project file
The setting from the WinCC-Project is used.
 - Enable SSL
The user data and e-mail are encrypted for transmission.
 - Disable SSL
The user data and e-mail are sent un-encrypted.

See also

Settings on the HMI device (Page 56)

WinCC Runtime Advanced Internet, "Proxy" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog box

Settings for utilizing the Proxy-Server.

Note

Enter the Proxy-Server in "Internet Options" at PC.

Settings

- Use proxy server
Activate the "Use Proxy Server" if access is given in your network via Proxy-server.
- Proxy
Enter the name or the address of the proxy-server.
- Port
Enter the port of the proxy-server.

WinCC Runtime Advanced Internet, "Web Server" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog

The following is configured:

- The utilization of the integrated web server and of the HTTP-Server
- User and user web authorizations

Settings

Tag access

Governs the access to tags via the "SIMATIC HMI HTTP protocol":

- "Read/write": Read/write access
- "Read only": read access only

Tag authenticate

Governs the authentication in case of access to variables via the SIMATIC HMI HTTP Protocol":

- "No authentication": No authentication is required for access.
- "Authentication required": An authentication is required for access.
Specify the user name and password when configuring the communication driver "SIMATIC HMI HTTP Protocol".

Enable Remote-Transfer for Projects

This setting enables remote transfer of project files.

Start automatically after booting

(on panel only)

The web server is automatically started after the HMI device boots. As a result, the web server is utilized independent of the runtime.

Note

Start web server automatically on PC

Add a link with the program "Miniweb.exe" in the Autostart-Organizer in order to start the web server automatically after the PC starts. The program is located in the installation index of runtime.

Close with Runtime

The web server is closed along with Runtime.

User Administration

After entering the password, the "UserDatabase-Edit". dialog opens. The "UserDatabase-Edit" dialog is the user administration of the web server.

Start Webserver

Starts the web server.

Close Webserver

Ends the web server.

WinCC Runtime Advanced Internet, "Remote" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog

Settings for the Sm@rtServer

Settings

Start automatically after booting

The Sm@rtServer is automatically started after the HMI device boots. Otherwise the Sm@rtServer starts together with the Runtime.

Close with runtime

The Sm@rtServer is closed together with Runtime.

Change settings

Opens the "Sm@rtServer Settings" dialog for specifying the passwords, authorizations, the screen update mechanism and the behavior when connections are terminated.

Note

This dialog is titled "Sm@rtServer: Default Local System Properties" on the panel.

The dialog contains the following tabs:

- "Server" tab (Page 61)
- "Polling" tab (Page 62)
- "Display" tab (Page 64)
- "Query" tab (Page 64)
- "Administration" tab (Page 65)
- "Certificates" tab (Page 67)

Start Remoting

Starts the Sm@rt Server explicitly.

Stop Remoting

Ends the Sm@rt Server explicitly.

"Sm@rtServer Settings" dialog (Panels, Comfort Panels, RT Advanced)

"Server" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog

Specifying passwords, web authorizations and the disconnection.

Incoming connections

Settings for handling an attempt to establish a connection.

- **Accept socket connections**
This setting enables the connection to the HMI device. It is a basic requirement for using the Sm@rtServers from the outside.
If this check box is deactivated, no remote monitoring and no remote control is possible.
- **Encrypt communication**
Allows an encrypted connection between Sm@rtClient and Sm@rtServer.
- **Password 1**
First password for remote access. "View only" is disabled as default.
- **Password 2**
Second password for remote access. "View only" is selected by default.
This password can be provided as a reserve password for third-party users (such as service technicians); it can be modified when necessary without significant effort within the organization.
- **View only**
If this check box is enabled, read access (monitoring mode) is the only access available when the corresponding password is entered.
Default: Enabled

Note

On devices with version V11 or V12, the password "100" is preset for the Sm@rtServer and for the integrated Web server. This password should be changed for security reasons.

On devices with version V13, no passwords are preset.

Enable network packets queuing (slower)

This setting enables splitting of data into multiple data packets, which are sent separately over the network. It is useful when multiple clients are connected.

Display or port numbers to use

Here, you select the TCP/IP port in the network where the Sm@rtServer waits for attempts to establish a connection.

- "Auto": The Sm@rtServer automatically searches for the appropriate port by itself.
- "Display": The server uses port 5900 plus display number. For HTTP, the server utilizes Port 5800 plus display number.
- "Ports": You enter the port numbers for the "main" and "HTTP" yourself.

No local input during client session

The keyboard and mouse on the server-HMI device are disabled as long as connections are active.

For example, this setting is useful when an HMI device is being administered from outside.

Remove desktop wallpaper (on PC only)

This setting removes the screen background on the PC, thus saving transmission effort.

Default: Enabled

When last client disconnects (on PC only)

This setting governs the behavior after disconnection of the last client connection:

- "Do nothing": no response.
- "Lock workstation": Server PC is locked.
- "Logoff workstation": Server PC is logged off.

The latter two settings are only useful if the Sm@rtServer is running as a service.

"Polling" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog

Specifying the screen update and the use of virtual graphics driver.

Polling modes(on PC only)

The settings govern the screen update.

Most changes are recognized automatically by the server. In case of problems, you can enter additional settings here.

The update method cannot be set on the panel. The settings is always "Poll Full Screen".

- Poll foreground window (On PC only)
Updates the current window.
It increases the load on the server.
- Poll window under cursor (On PC only)
Updates the window that is located under the mouse cursor. The window is updated when a change occurs in the operator control element under the mouse cursor.
Default: Enabled
- Poll full screen (On PC only)
This setting specifies an update each time the screen changes. This setting provides you the lowest display error but places a maximum load on the server.
- Polling cycle
Determine the suitable setting for your configuration. Make sure that the selected update cycle is not too short, since it affects the computer load.

Window polling

- Poll console windows Only (On PC only)
This setting specifies an additional update when changes occur in a console window (MS input requirement).
- Poll on event received only (Only on the PC)
This setting specifies an additional update each time an entry is made.
Default: Enabled
- Mirror driver status
(Only on the PC with a mirror driver installed)
Provides information about the status of the virtual graphics driver.

Mirror driver options (only on a PC with installed mirror driver)

Enable direct access to display driver's mirror screen

The shared-memory area of the virtual graphics driver is used for the display. The setting improves the performance.

Troubleshooting (on PC only)

- Don't use VNCHooks.DLL while polling full screen
VNCHooks.dll is used by default for the screen update. If VNCHooks.dll causes problems when using other program, select this setting.
- Don't use mirror display driver even if available
(Only on the PC with a mirror driver installed)
Use this setting only for troubleshooting.

"Display" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog

Setting of the screen display.

Sharing area(on PC only)

- Full desktop
The entire desktop of the server is accessed.
- Primary display
The main screen of the multi-monitor configuration is displayed.

Downscale to(on PC only)

Scales the screen to be transferred according your inputs. Servers with Windows CE ignore this setting.

"Query" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog

Settings for incoming connection attempts.

Note

This dialog is titled "Default Local System Advanced" on the panel.

Query settings

These settings govern acceptance of incoming attempts to establish a connection.

- Query console on incoming connections
The Sm@rtServer registers the incoming attempts to establish a connection and displays a dialog on the screen in which the connection attempt is accepted or rejected.
- Query timeout
Set the waiting time.
- Default action
Select the response to an attempt to establish a connection once the waiting time expires:
 - "Refuse": Reject attempt (operator control mode - single mode)
 - "Accept": Accept attempt (operator control mode – shared mode)

Allow option to accept without authentication

The dialog for handling attempts to establish connections also contains the button "Accept without password". This gives you the option to accept an attempt to establish connection without a password.

"Administration" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog

Specifications for session management.

Note

This dialog is titled "Default Local System Advanced" on the panel.

Administration

- Disable empty passwords
Select this check box in order to allow an empty "Password 1".
Default: Enabled
- Allow loopback connections
This setting allows connections to your own HMI device. It is useful and necessary when security software is used for secure (encoded) connections.
- Allow only loopback
This setting allows only connections to your own HMI device.

Logging

- Log info to SmartServer.log
(On the panel: Log information to file)
This setting writes information to the server logbook.
- Log detailed debugging information
This setting writes expanded information to the server logbook (for locating errors).

With HMI devices operating with Windows CE, the log is only created when the MMC card is inserted. If the MMC card is inserted, the log is created directly on the card.

The log files are created in the following path on a PC: C:\Documents and Settings\All Users\Application Data\Siemens\HmiRTm

Forced write access

This setting governs forced access in an emergency contrary to normal session management.

- Password needed

If this check box is not selected, every operator can force access in emergencies as follows:

- Pressing the <Shift> key four times
- Clicking four times
- Touching the screen four times

If this check box is enabled, to force access an attempt must be made to gain access and a password must also be entered.

In this case, enter the applicable password in the input field underneath. If a password is not entered, it is not possible to force access in an emergency.

Default: Enabled

Note

On the server, access can only be forced by pressing the <Shift> key four times, clicking four times, or touching the screen four times.

HTTP-Server

- Enable built-in HTTP server

If this check box is activated, the Java-Applet is automatically downloaded on the PC when the connection is first established.

The Java applet accesses the Java VM that is installed on the client and enables remote monitoring and remote control using Internet Explorer.

Default: Enabled

- Enable applet params in URLs

Forwards all parameters of the URL to the Sm@rtClient application.

- https

If this check box is selected, the Java applet is downloaded securely.

Default: Enabled

Connection priority

These settings govern handling of attempts to establish a connection by non-shared clients.

- Disconnect existing connections

When an attempt is made to establish a connection by a non-shared client, the attempt is accepted; the existing connections are disconnected (single mode).

- Automatic shared sessions

When an attempt is made to establish a connection by a non-shared client, the attempt is accepted; the prior existing connections are retained. Access is controlled using session management in shared mode.

Default: Enabled

- **Active user timeout**
For shared mode, enter the time that must elapse without any actions on the active HMI device before access can be changed.
Default setting: 10 seconds
- **Refuse concurrent connections**
If a non-shared client is already connected to the server, attempts to establish a connection by other non-shared clients are rejected.

See also

Remote control by means of Internet Explorer (Page 88)

"Certificates" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog

The "Certificate" tab shows you all security certificates and their properties.
You can also import and delete security certificates.

Selection

In the "Selection" list, select a certificate with the properties you want to view.

- You can use the "Delete" button to delete the selected certificate.
- You can use the "Import" button to import the selected certificate.

The "Import" button is active if the entry "Imported Certificate" is selected.

Certificate

You see the following certificate properties in the "Certificate" area:

- **Issued to:** Name of the organizational unit for which the certificate was issued
- **Issued by:** Name of the certificate issuer
- **Valid from... to:** The validity period of the certificate
- **Thumbprint:** The fingerprint of the certificate

See also

Configuring a separate certificate for Sm@rtServer (Page 84)

User administration for web server (Panels, Comfort Panels, RT Advanced)

Introduction

Different web authorizations for the operation and monitoring are allocated to the users in the user administration.

Requirement

- The "WinCC Runtime Advanced Internet" dialog is open.
- The "Web Server" tab is displayed.

Entries and settings

Click "User Administration" in the "Web Server" tab and enter the password.

Note

On devices with version V11 or V12, the password "100" is preset for the Sm@rtServer and for the integrated Web server. This password should be changed for security reasons.

On devices with version V13, no passwords are preset.

The "UserDatabase-Edit" dialog is opened.

The "UserDatabase-Edit" dialog has three tabs:

- Tab "User Manager"
User administration for creation or deletion of users.
Create a new user using "New"; Delete a user using "Remove". The recreation and deletion become effective using "Apply".
- Tab "Description"
You can store a description of or comments on the users selected on the "User Manager" tab.
- Tab "Authorizations"
Specify the web authorizations for the users selected on the "User Manager" tab. You use "Add" to activate a web authorization and "Remove" to deactivate one.
By default, the password is initially preset to "100" and all web authorizations are granted to users with "Administrator" rights.
For read and write access to the file browser, the user must possess the web authorizations "FileBrowserAdministrator" and "FileBrowserUser".

Note

In principle, every user who has access to the control panel can manage users and web authorizations. If necessary, protect the control panel from unwanted access.

List of web authorizations

The following web authorizations exist:

| Web authorization | Authorized for: |
|--------------------------|--|
| UserData | Import and export of recipes |
| UserAdministrator | Import and export of password lists |
| RuntimeAccess | Starting and stopping of runtime |
| Engineering | HTTP transfer from ES to the target device |
| FileBrowserUser | Read access to the file browser |
| FileBrowserAdministrator | Read/write access to the file browser |
| RTCommunication | Utilization of the SIMATIC HMI HTTP server |
| SoapUser | Read/write access via web service (SOAP) |

2.1.5 Settings for remote control (Panels, Comfort Panels, RT Advanced)

2.1.5.1 Session management for remote control (Panels, Comfort Panels, RT Advanced)

Introduction

WinCC enables remote monitoring and remote control of HMI devices over a TCP/IP-ready network such as a LAN or the Internet. Remote monitoring and remote control is implemented in different ways:

- Remote control by means of Internet Explorer
- Remote control by means of the Sm@rtClient-application
- Remote control by means of the Sm@rtClient-display in

Only one device can ever have access to the HMI-device. Which device is permitted access is determined by the session management.

Session management options

Session management is used to control access. The client-server connection can be in one of two modes:

- Monitoring mode
- Control mode

Monitoring mode

If the client accesses the server in monitoring mode, the operator can see the current screen of the HMI device and track all changes. He can monitor the server but cannot operate.

In the monitoring mode, all the keys on the client retain their standard functions.

If remote control was started from the Sm@rtClient display, the operator uses the <Tab> key or the cursor keys to go to the next object in the current screen of the client project.

Control mode

If the client accesses the server in operator control mode, the operator can use the mouse and the keyboard to control the server from the client. If an access attempt is made from another client, the assignment of operating permission depends on the settings at the server and at the clients.

In operator control mode, the client keys act on the server screen. Thus, the operator uses the <Tab> key to go to the next object in the current screen of the project running on the server.

If remote control was started from the Sm@rtClient display, the operator can only go to another object or screen in the project on the client by using an additionally configured function or an additional menu command. The operator to this menu command as follows:

- On the Touch-device, in which he touches the screen longer than 1 sec.
- On the keyboard =device, in which he masks on the menu with <Shift+Control> and operates it with <Alt> and the keyboard.

In both operating modes, the Sm@rtServer is set so that the operator at the remotely controlled device, the server, can be prevented from performing any activities.

In an emergency, the operator can exact the user rights on a remotely controlled HMI device as well as on an inactive HMI device. If no password is specified, he must click the user interface four times consecutively, touch the screen four times consecutively, or press the <Shift> key four times consecutively. If a password is specified, he must click once or press a key on the client and then enter the specified password.

Settings for session management

You make settings for session management on the server and on the client in the Control Panel "WinCC Internet Settings".

2.1.5.2 Configuring Sm@rtServer for remote control (Panels, Comfort Panels, RT Advanced)

Introduction

The Sm@rtServer has an internal security concept based on passwords and special settings for session management.

Security concept for the Sm@rtServer

Remote monitoring and remote control of the Sm@rtServer from the Sm@rtClient is protected by two functions:

- Encrypt encryption of communication to the server
- Passwords

Encrypt communication to the Sm@rtServer

The "Encrypt communication" function provides a secure connection between Sm@rtClient and Sm@rtServer.

After you have activated the "Encrypt communication" function, the Sm@rtServer sends a Sm@rtServer-specific certificate to the Sm@rtClient.

The Sm@rtClient must support the "Encrypt communication" function for encrypted communication.

The certificate sent by the Sm@rtServer must be accepted to establish communication on the Sm@rtClient.

All connections between Sm@rtClient and Sm@rtServer are then only possible on the basis of the exchanged certificate.

Passwords for the Sm@rtServer

Remote monitoring and remote control of the Sm@rtServer at the Sm@rtClient is protected by two passwords.

The second password is used as a further password for additional access, for example, as a service password.

Note

Passwords for the Sm@rtServer

No default passwords are set.

Therefore, assign the passwords before you use the Sm@rtServer.

Settings on the Sm@rtServer

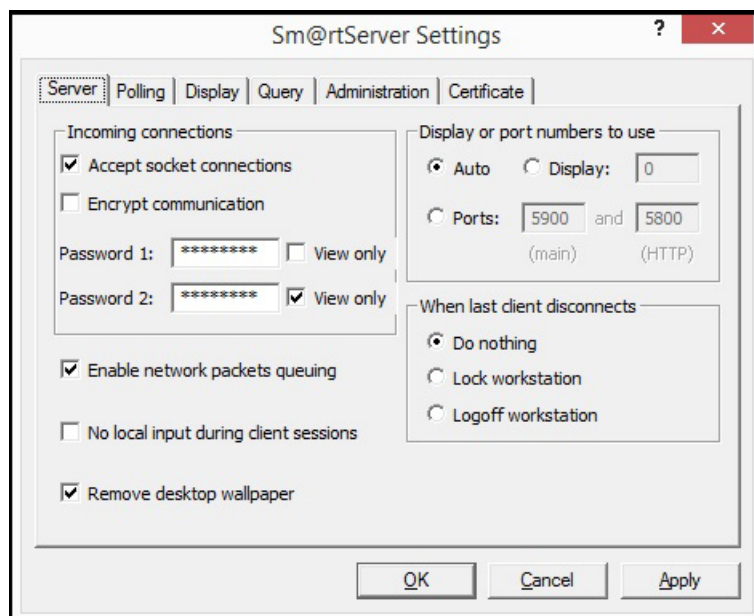
The settings on the server govern which remote operators can access the runtime of the server.

The passwords for access are set on the server. Open "WinCC Runtime Advanced Internet" in the control panel. On the "Remote" tab, click "Change Settings". On the following "Server" tab of the subsequent dialog, enter the passwords of the Sm@rtClient. For both passwords, you can use "View only" to set the monitoring mode and to exclude operator control mode.

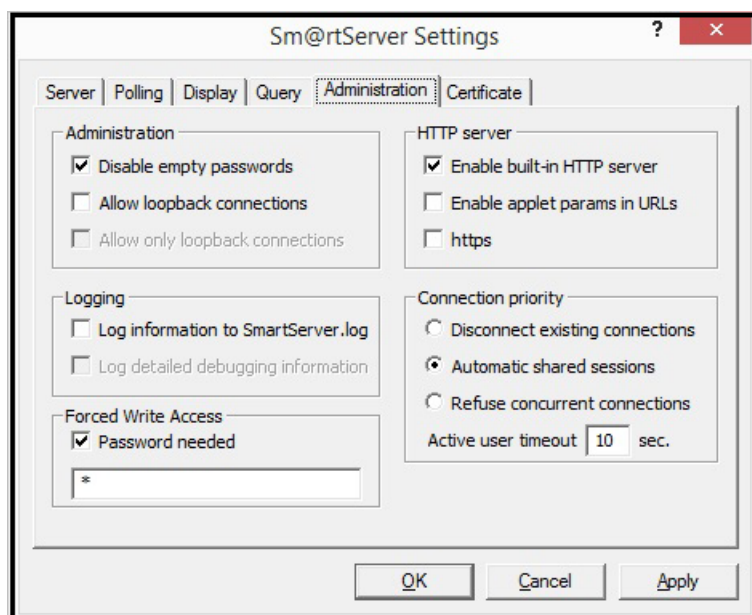
On the panel, this dialog is called "Sm@rtServer: Default Local System Properties" and contains fewer dialog elements than the dialog on the PC.

Control mode

To enable control mode, the "View only" check box must be cleared, at least for "Password 1" (Password 1).



The manner in which the individual remote control station can access the server is set on the "Administration" tab.



- "Disconnect existing connections"
When an access attempt is made by a non-shared client, the previous connection is automatically disconnected and control is transferred to the new client.
When an attempt is made to access by a shared client, the behavior is the same as described for "Automatic shared sessions".
- "Automatic shared sessions"
When an access attempt is made, control is transferred to the new client.
The condition for transferring control is that no action has been undertaken by the previously active client for a period of time (in seconds) as specified in the "Active user timeout" setting.
- "Refuse concurrent connections"
When an attempt is made to access by a non-shared client, this access attempt is rejected so long as the operator station that currently has access is still connected to the server.
When an attempt is made to access by a shared client, the behavior is the same as described for "Automatic shared sessions".

Disabling local operator control of the server

To do so, open the "WinCC Internet Settings" in the Control Panel. On the "Remote" tab, click "Change Settings". On the "Server" tab in the subsequent dialog, select "No local input during client session".

Password for forced access

A password can be specified in "Forced Write Access" for forced access in an emergency.

Sm@rtServer as a service

You can let the Sm@rtServer run as a service. The operator can then also access the service-HMI device from the client-HMI device, for example, the screen saver is active with a password.

Select the check box "Start automatically after booting" in "WinCC Runtime Advanced Internet" on the "Remote" tab.

Sm@rtServer as service in Windows 7

The Sm@rtServer always runs as a service under Windows 7. You cannot stop the Sm@rtServer in Runtime with the Notification Area in the taskbar. You have the following options for stopping the Sm@rtServer:

- Stop using the "ControlSmartServer" system function
Configure the "ControlSmartServer" system function to a button, for example. Select the "Stop" mode at the system function. You can stop the Sm@rtServer in Runtime by clicking the button.
- Stopping the Sm@rtServer in the Control Panel:
Open "WinCC Runtime Advanced Internet" in the Control Panel and select the "Remote" tab. Click on the "Stop" button. Sm@rtServer is stopped.
- Stopping Sm@rtServer by stopping Runtime:
Open "WinCC Runtime Advanced Internet" in the Control Panel and select the "Remote" tab. Activate the "Close with Runtime" option. The Sm@rtServer is stopped at the stop of Runtime.

See also

Configuring secure communication for Sm@rtServer (Page 82)

2.1.5.3 Configure Sm@rtClient for remote control (Panels, Comfort Panels, RT Advanced)

Settings on the client PC

- **Monitoring mode**
At the client-PC you limit the connection to observation mode, if required. This allows you to prevent unintended control operations.
 - If connection is via the Sm@rtClient application
In the following "Sm@rtClient Connection" of Sm@rtClient-application, click "Options..." button.
In the "Sm@rtclient Options" dialog, select the setting "View only (inputs ignored)".
 - If connection is via Internet Explorer
Click on the button "Options..." and select "View only" in the subsequent dialog.
- **Layout**
You can also specify whether or not the HMI-device is to be displayed with the same layout in the Sm@rtClient application. This is useful if you access from a PC on a touch device. In order to suppress the layout, select the "Sm@rtclient Options" setting in the "Suppress Device Layout" dialog.
In addition, you can use "Scale by" to zoom in or out of the layout. To use "Scale by", the Suppress Device Layout setting must be selected or the HMI-device must not supply any layout. Otherwise, the desktop is always displayed with a zoom setting of 100%.

Note

If you scale the display, the performance may be impaired in some situations:

- Strong scaling, for example from 1600 x 1200 px to 640 x 480 px.
 - Scaling with non-matching scaling factors, for example from a 4:3 resolution to 16:10 resolution.
-

Configuring of the Sm@rtClient-display

You can configure the Sm@rtClient display in different ways, and thereby set certain inputs: The server name, the password for accessing Sm@rtServer or the restriction to the monitoring mode.

Encrypted communication

You must enable the "Encrypt communication" function for encrypted communication with the Sm@rtServer.

- Support for the "Encrypt communication" function on the Sm@rtClient
If the Sm@rtClient does not support the "Encrypt communication" function, no communication is possible with a Sm@rtServer which has enabled the "Encrypt communication" function.
Enable the "Encrypt communication" function on the Sm@rtServer.
- Enabling the "Encrypt communication" function on the Sm@rtServer by the Sm@rtClient
You can also enable the "Encrypt communication" function on the Sm@rtServer from the Sm@rtClient:
 - Establish a connection to the server.
 - Enable the "Encrypt communication" function in the "Standard VNC Authentication" dialog.
 - Certificates are exchanged between the Sm@rtServer and Sm@rtClient.
 - The certificate sent by the Sm@rtServer must be accepted by the Sm@rtClient.

2.1.5.4 Sm@rtClient-Application (Panels, Comfort Panels, RT Advanced)

Dialog "New Sm@rtServer: Connection" (Panels, Comfort Panels, RT Advanced)

Introduction

This dialog opens when you click the "Sm@rtClient" button in the taskbar.

Purpose of the dialog box

This dialog is used for selecting the server and the connection method.

Sm@rtServer:

Enter the address of the server to which the connection is to be established. You can find the various options for entering the address under "Remote control by means of the Sm@rtClient application (Page 89)".

Connection profil

Select the type of connection to the server according to the network you are using.

Listening mode

If you enable this function, the Sm@rtClient application is minimized and appears as a button in the Windows taskbar. The Sm@rtClient waits for the Sm@rtServer to establish a connection. To establish the connection, click the "Sm@rtServer" button in the Windows taskbar of the server. Select "Add new client" in the context menu.

Options

The "Sm@rtClient Options" dialog containing the technical settings for the Sm@rtClient-application is displayed.

See also

Remote control by means of the Sm@rtClient application (Page 89)

"Options" dialog, "Globals" tab (Page 79)

"Options" dialog, "Connections" tab (Page 77)

"Options" dialog, "Connections" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog box

Technical settings for the Sm@rtClient-application are specified in this dialog box.

Only change the settings here in special cases.

Note

You can also specify these settings in the Java Applet. Note that some of the dialog elements are named differently there.

Format and encodings

Settings for compressing (encoding) the screen data of the server.

- Use encoding
Preassigned based on the selection under "Connection profile".
Select the desired compression or "Raw" (no compression).
- User 8-bit color
(Only in the Java-Applet): Reduces the color depth at the client to 8 bits (256 colors). The data are then transferred faster. However, incorrect colors may result.
- Custom Compression level
Allows individual customizing of the compression level in the "Level" input field:
1 = least compression (faster); 9 = maximum compression (slower).
- Allow JPEG compression
Allows the use of JPEG compression (involves losses).
Enter the "Screen quality" in the input field underneath:
1 = least compression (faster); 9 = maximum compression (slower).
- Allow CopyRect encoding
(In the Java-Applet: Use CopyRect. Encoding)
Allows compression while using "similar rectangles".

Restrictions

- Viewonly (inputs ignored)
Sets the view mode for this client irrespective of the settings on the server.
- Disable clipboard transfer
Disables the clipboard that is used to transfer data from one PC to another. Applies only to the copying and pasting of texts.
This functionality is not available at a Windows CE server.

Display

Settings for the screen display

- **Scale by**
Zooms in or zooms out the desktop to be displayed. To use "Scale by", the Suppress Device Layout setting must be selected or the HMI-device must not supply any layout. Otherwise, the desktop is displayed with a zoom setting of 100%.
- **Fullscreen Mode**
Displays the desktop to be shown in full-screen mode. If the server screen is larger than the screen of the client, it is scrolled automatically by the mouse movement.
- **Suppress Device Layout**
In the Sm@rtClient application window, the entire layout of remote HMI-device is not shown.
- **Use CTRL + Cursor Key for Scrolling**
The key combinations <CTRL> + cursor key are used to scroll within the local screen. They are no longer transferred to the server.

Mouse

(In the Java-Applet: Mouse buttons 2 and 3)

Settings for the evaluation of mouse actions

- **Emulate 3 Buttons (with 2-button click)**
Emulation of a three-button mouse by a two-button mouse.
- **Swap mouse buttons 2 and 3**
(In the Java-Applet: reversed/normal)
Mouse buttons 2 and 3 are swapped.

Mouse cursor

(In the Java-Applet: Cursor shape updates)

Settings for the display of the cursor

Select the type of transfer of the mouse actions:

- **Track remote cursor locally**
The information on the location of the cursor is transferred separately from the screen information. This speeds up the transfer of the cursor. (JavaApplet: Enabled)
- **Let remote server deal with mouse cursor**
Tracks the server cursor to the client cursor. This allows more accurate cursor positioning. (YES: Ignore)
- **Don't show remote cursor**
The cursor at the server is not included in the transfer. (YES: Disable)

Request shared session

(In the Java-Applet: Share desktop)

Declares this client to be a non-exclusive client.

See also

Dialog "New Sm@rtServer: Connection" (Page 76)

"Options" dialog, "Globals" tab (Panels, Comfort Panels, RT Advanced)

Purpose of the dialog box

Technical settings for the Sm@rtClient-application are carried out in this dialog box.

Only change the settings here in special cases.

Note

You can also carry out these settings in the Java Applet. Note that some of the dialog elements are named differently there.

Interface options

- Show toolbars by default
Displays the toolbar.
- Warn at switching to the full-screen mode
Outputs a message before the full-screen mode is activated.
- Enable Onscreen keyboard
Enables the display of the on-screen keyboard
- Number of connection to remember
The client creates a list of the recently used connections. This setting specifies the number of connections listed.
- Clear the list of saved connections
The list is cleared.

Local cursor shape

Specifies the appearance of the local cursor. This allows you to better differentiate between the local cursor and remote cursor.

Listening mode

- Accept reverse VNC connections on TCP port
Specifies the TCP port number. The Sm@rtClient waits for the Sm@rtServer to establish the connection over this TCP port number.

Logging

- Write log to a file
Writes information in the logbook of the Sm@rtClient-application.
- Verbosity level
Writes expanded information to the server logbook of the Sm@rtClient-application (for locating faults). The amount of detail in the information is dependent on the verbosity level setting.

2.1.5.5 Remote control of key devices (Panels, Comfort Panels, RT Advanced)

Mapping of the function keys

HMI devices are equipped with a variety of function keys.

Example:

From the PC keyboard, you want to remotely control key F20 on the "MP 377 key" of HMI-device.

You can control the F20 key with the PC-keyboard shortcut <SHIFT + F8>.

The table provides you with an overview for controlling the keys.

| xP177/277 | xP377 | PC keyboard shortcut |
|-----------|-------|----------------------|
| F13 | F13 | SHIFT + F1 |
| F14 | F14 | SHIFT + F2 |
| F15 | F15 | SHIFT + F3 |
| F16 | F16 | SHIFT + F4 |
| F17 | F17 | SHIFT + F5 |
| F18 | F18 | SHIFT + F6 |
| F19 | F19 | SHIFT + F7 |
| F20 | F20 | SHIFT + F8 |
| K1 | S1 | SHIFT + F9 |
| K2 | S2 | SHIFT + F10 |
| K3 | S3 | SHIFT + F11 |
| K4 | S4 | SHIFT + F12 |
| K5 | S5 | CTRL + F1 |
| K6 | S6 | CTRL + F2 |
| K7 | S7 | CTRL + F3 |
| K8 | S8 | CTRL + F4 |
| K9 | S9 | CTRL + F5 |
| K10 | S10 | CTRL + F6 |
| K11 | S11 | CTRL + F7 |
| K12 | S12 | CTRL + F8 |
| K13 | S13 | CTRL + F9 |
| K14 | S14 | CTRL + F10 |
| K15 | S15 | CTRL + F11 |
| K16 | S16 | CTRL + F12 |
| HELP | HELP | ALT + H |
| ACK | ACK | ALT + F1 |

2.1.6 Use and restrictions of Sm@rt Options (Panels, Comfort Panels, RT Advanced)

Use restrictions

While using the Sm@rt Options, observe the following instructions:

- HMI devices suitable for use
For additional information, refer to "Usable HMI devices".
- Sm@rtServer and Sm@rtClient
 - If a PC is used as a Sm@rtServer, select the highest-performance platform available.
 - Use only simple projects.
 - Avoid photographs and color gradients in screens.
 - Avoid heavy background loads during operation, for example, those from user-defined functions or logs.
 - The number of the maximum connected Sm@rt Clients depends on the Server-HMI device. For additional information, see the "Performance features" documentation.
 - To improve the performance of the Sm@rtServer, you can disable hardware acceleration of the graphics card .
 - You inevitably loose performance at the HMI when you access the HMI-device using the Sm@rtClient functionality.
- SIMATIC HMI HTTP Protocol
 - Tag exchange via the SIMATIC HMI HTTP Protocol is not suitable for exchanging bulk data.
 - The maximum number of connections depends on the HMI device: For additional information, see the "Performance features" documentation
- Access protection
To protect access to an HMI-device using different passwords, you must use the first password for the protected, and the second password for the unprotected access e.g. remote control with a password, remote monitoring without password.
- Port
The web server connects to the network at the port 80. To run it without problems, make sure port 80 is not in use by any other application, such as IIS World Wide Web Publishing Service.
- Integrated HTML-pages
 - The size of the HTML pages must not exceed 100 Kb in case of Windows CE. In case of exceeding of the given value, these pages are spooled on external storage media.
 - If you display tags on HTML-pages using the entry type "Cyclic on use", it can lead to data-inconsistency.

2.1 Basics (Panels, Comfort Panels, RT Advanced)

- E-mailing
The E-mailing function is not suitable for the mass dispatch of E-Mails. It is meant for sending important messages.
- Timeout
If the connection between server and client is interrupted, the server will register this disconnection only with a certain delay. The delay is based on the Windows standard configuration of TCP/IP Timeout.

Use-requirements in the company network

In order to implement the mentioned scenario, the accesses to the company network must be enabled. If the company network is protected by a Firewall, the system administrator must release the appropriate ports for that.

- Access to the integrated HTML-pages
The web server connects to the network at the port 80.
- Access to Sm@rtServer for downloading the Java-Applet using the Internet Explorer
The Sm@rtServer is connected to the network at the Port 5800 for downloading the Java-applet.
- Access to the Sm@rtServer using the Internet Explorer for remote monitoring and remote control
The Sm@rtServer is connected to the network at the port 5900.

Note

If you change the ports of the Sm@rtServer you must customize the links in the used Html-pages accordingly. Additional information to modify the Html-pages is provided in "Example: "Configure integrated webserver".

2.1.7 Setting up secure communication between WebClient and Sm@rtServer (Panels, Comfort Panels, RT Advanced)

2.1.7.1 Configuring secure communication for Sm@rtServer (Panels, Comfort Panels, RT Advanced)

Introduction

You can configure secure communication for the communication between Sm@rtServer and WebClient.

Before secure communication can be configured, a number of settings in the "Sm@rtServer Settings" dialog are required and the security certificate needs to be installed in your Web browser.

To open the "Sm@rtServer Settings" dialog, click the "Change settings" button in the "WinCC Runtime Advanced Internet" dialog.

You can use either a self-signed, automatically generated certificate or a separate certificate for secure communication.

The Java applet can also be downloaded to the Sm@rtServer over the WebClient with secure communication.

Principle

The following steps are required to configure secure communication:

- Enable the "Encrypt communication" option on the Sm@rtServer.
Alternatively, you can enable the "Secure" option on the login Website in the WebClient.
- In the "Sm@rtServer Settings" dialog on the "Administration" tab, go to "HTTP-Server" and enable the "https" function.
- Import separate certificate or automatically generated, self-signed certificate.
- Install the self-signed certificate the first time a connection is established.

Note

In V14, "https" is disabled by default and therefore has no impact when older versions are upgraded to V14.

If the "https" check box is cleared, the user can decide in the WebClient whether to upload the Java applet over http or https by specifying "http" or "https" in the URL.

Note

The security certificate for the Sm@rtServer is located in the Windows certificate store. No certificates can be exported on the HMI devices.

The certificate name is as follows: <IP address>.

Note

If you update to Sm@rtServer V14, the Sm@rtClients must confirm the certificates again.

See also

Installing self-signed Sm@rtServer certificates in Internet Explorer (Page 84)

Installing self-signed Sm@rtServer certificates in Firefox (Page 85)

Configuring a separate certificate for Sm@rtServer (Page 84)

Configuring secure communication on the WebClient (Page 86)

2.1.7.2 Configuring a separate certificate for Sm@rtServer (Panels, Comfort Panels, RT Advanced)

Principle

For secure communication between Sm@rtServer and WebClient, you can use either automatically generated, self-signed certificates, or separate certificates.

You save the separate certificates beforehand in the SmartServer.pfx or SmartServer.p12 file. On HMI devices with Windows CE, this file is saved under \flash\simatic; on PCs, it is saved under \ProgramData\Siemens\CoRtHmiRTm\SmartServer.

You then import the certificate to the certificate store using the "Sm@rtServer" dialog and install the corresponding client certificate in your Web browser.

Importing separate certificates

1. Open the "Sm@rtServer" dialog.
2. Enable the "Certificate" tab.
3. Click the "Import" button.
The SmartServer.pfx file is deleted after import. The certificates are stored in the certificate store on the HMI device under My Certificates and on the PC under WinCC Panel RT VNC Service.

Note

In the "Sm@rtServer" dialog on the "Certificate" tab, you can view both automatically generated and imported certificates and their attributes.

See also

"Certificates" tab (Page 67)

Installing self-signed Sm@rtServer certificates in Internet Explorer (Page 84)

Configuring secure communication for Sm@rtServer (Page 82)

Installing self-signed Sm@rtServer certificates in Firefox (Page 85)

2.1.7.3 Installing self-signed Sm@rtServer certificates in Internet Explorer (Panels, Comfort Panels, RT Advanced)

Procedure

The following procedure has been tested and released for Internet Explorer 10.

The first time a connection to Sm@rtServer is established, Internet Explorer reports a problem with the Website's security certificate.

1. Select the "Continue to this website (not recommended)" option.
The "Security Warning" dialog appears.
2. In the "Security Warning" dialog, click "Continue".
3. Click "Certificate error" in the Internet Explorer address bar.
4. Click on the "View certificates" button.
The "Certificate" dialog appears.
5. Click on the "Install Certificate" button.
6. Select the certificate store "Trusted Root Certification Authorities" for installation of the Sm@rtServer certificate.
Once you have installed the certificate, you can export it from the certificate store and install it on other PCs with WebClients for connection to the same Sm@rtServer.

See also

Configuring a separate certificate for Sm@rtServer (Page 84)

Configuring secure communication for Sm@rtServer (Page 82)

2.1.7.4 Installing self-signed Sm@rtServer certificates in Firefox (Panels, Comfort Panels, RT Advanced)

Procedure

The following procedure has been tested and released with Firefox 31.8.

At least Java Version 8 Update 51 must be installed in Firefox for use of the Java applet.

Note

Please note that in some browsers self-signed certificates are classified as untrustworthy. To avoid this, install your own certificate from a recognized certification body.

The first time a connection to Sm@rtServer is established, Firefox reports a problem with the Website's security certificate.

1. In the "This connection is untrusted" dialog, click the "Add exception" button.
The "Add security exception" dialog appears.
2. In the "Add security exception" dialog, click "Get certificate".
3. Then click "View"
The "Certificate Viewer" dialog appears.
4. In the "Certificate Viewer" dialog on the "Details" tab, select the certificate and click "Export".
5. Click "Close".
6. Click on the "Confirm security exception" button.

2.1 Basics (Panels, Comfort Panels, RT Advanced)

7. Open the Java Control Panel using the Control Panel.
8. On the "Security" tab, click the "Manage certificates" button.
The "Certificates" dialog opens.
9. In the "Certificates" dialog, import the exported certificates under certificate type "Secure Site CA".
The import can also be executed on other PCs with WebClients for connection to the same Sm@rtServer.

See also

Configuring secure communication for Sm@rtServer (Page 82)

Configuring a separate certificate for Sm@rtServer (Page 84)

2.1.7.5 Configuring secure communication on the WebClient (Panels, Comfort Panels, RT Advanced)

Basics

You can also configure secure communication with the Sm@rtServer on the login page of the WebClient. When the "Secure" option is enabled, the Sm@rtServer and WebClient communicate securely. The "Secure" option is enabled by default.

Note

When the "Secure" option is enabled, the Sm@rtServer and WebClient communicate securely even if secure communication has not been set for the Sm@rtServer.

Note

Certificate comparison

The result of the certificate comparison between Sm@rtServer and WebClient is displayed in the "Thumbprint" field on the login page.

If the login page has been saved as a Website in htm or html format and is then accessed with a double-click, the fingerprint is checked. The fingerprint of the Sm@rtServer certificate is checked against the fingerprint that is saved in the htm file. The "Thumbprint" field is displayed in green if the two match and in red if they do not.

See also

Configuring secure communication for Sm@rtServer (Page 82)

2.2 Remote control via Sm@rtServer (Panels, Comfort Panels, RT Advanced)

2.2.1 Types of the remote control (Panels, Comfort Panels, RT Advanced)

2.2.1.1 Remote control and remote monitoring by means of Sm@rtServer (Panels, Comfort Panels, RT Advanced)

Introduction

The Sm@rtOptions of WinCC enable the access from HMI device or PC to a remote HMI device via Ethernet.

Requirement

- The License Key "Sm@rtServer" is available at the Server-HMI device.

Note

The 14-day license is not supported by Windows CE devices.

- Both devices are linked via a TCP/IP-ready network, that is via a LAN or the Internet.
- "Sm@rtServer" is activated in the WinCC-Project of the Server-HMI device for the "Services in Runtime".
- Additional requirements must be satisfied according to the type of implementation.

Implementing remote access

The Sm@rtServer supports remote monitoring or remote control on the remote device (server).

Remote monitoring or remote control can be implemented on the local device (client) in various ways:

- By means of Internet Explorer
- By means of the Sm@rtClient-application

Access via HTML pages

The Sm@rt Options enable access for remote control with Microsoft Internet Explorer and by means of integrated HTML pages of the server.



CAUTION

Ethernet communication

In Ethernet-based communication, such as PROFINET IO, HTTP, Sm@rt Options and OPC, it is the end user who is responsible for the security of his data network. The proper functioning of the device cannot be guaranteed in all circumstances; targeted attacks, for example, can lead to an overloading of the device.

2.2.1.2 Remote control by means of Internet Explorer (Panels, Comfort Panels, RT Advanced)

Introduction

On the client HMI device, the connection to the remote HMI device is established by means of Internet Explorer.

The window of the Internet Explorer displays only the screen of the remote HMI device, of the server HMI device. If task switching is not disabled at the server HMI device, you can access the complete desktop.

Requirement

- The Client-HMI device is a PC.
- Internet Explorer from V6.0 SP1 is installed.
- The Client-and Server-certificates are installed to ensure the data security when transferred via internet.
- The Java-Applet is installed. The Java applet accesses the Java runtime environment that is installed on the client.

Note

You achieve the best results in Internet Explorer by installing the current Java Runtime Environment (JRETM) of Sun Microsystems. Go to www.java.com to download this program.

Process flow

Enter the address of the remote device in Internet Explorer. The address consists of the server name and the HTTP port number that is set on the server. The default setting is: 5800.

Examples of addressing: "http://MyPanel:5800" or "http://192.168.168.1:5800".

The following VNC authentication dialog contains the "Thumbprint" and "Password" fields. If there is no "Thumbprint" field, your browser cache still contains the old dialog. In this case, clear your browser cache and try connecting again.

Restrictions

The "Force write access with password" function cannot be implemented using the Java applet.

See also

"Administration" tab (Page 65)

2.2.1.3 Remote control by means of the Sm@rtClient application (Panels, Comfort Panels, RT Advanced)

Introduction

The Sm@rtClient application provides the connection to the remote HMI device on the remote HMI device.

Requirement

- The Client-and Server-certificates are installed to ensure the data security when transferred via internet.
- The Client-HMI device is a PC.

Process flow

The remote control via the Sm@rtClient-application works as follows:

- Start Sm@rtClient application
- Establish connection
- Password input
- Perform operator control or monitoring on the HMI device

Start Sm@rtClient application

You can access the Sm@rtClient application, the program "SmartClient.exe", in various ways:

- By installing WinCC Runtime on the client device you have automatically installed the Sm@rtClient application.
- You have several options if WinCC Runtime is not installed on the client device:
 - Copy the Sm@rtClient application from the WinCC product-DVD from the folder "Support \SmartClient".
 - Copy the Sm@rtClient application from the "...\\Siemens\\Automation\\WinCC RT Advanced" folder of another PC using a floppy disk or the Intranet.

Establish connection

In order to establish the connection to the remote HMI device, call the Sm@rtClient application and enter the IP address of the server.

- IP address or server name:port number
- IP address or server name:display number

Example: "192.168.0.1::5800"

You can also start the Sm@rtClient application with the command line input: "smartclient.exe 192.168.0.1". The logon dialog box opens.

You can include the password in the command line entry to start the Sm@rtClient application: "smartclient.exe 192.168.0.1 /password <password>".

Note

If the Sm@rtServer at the server HMI device does not run as a service, the connection established with the Sm@rtClient application is interrupted automatically as soon as the keyboard shortcut CTRL+ALT+DEL is pressed at the server HMI device or the screen saver is activated. In order for the Sm@rtServer to run as a service, the "Start automatically after booting" check box in the "Remote" tab in the "WinCC Runtime Advanced Internet Settings" dialog must be activated.

Password input

- Password input at the Sm@rtServer
Instead of the on-screen keyboard, the following message is displayed on the Sm@rtClient if you enter the password directly at the Sm@rtServer: "Remote access by Sm@rt Options is in Progress. Please wait until the input of values has been ended." This measure prevents keyboard input for entering the password from being displayed on the Sm@rtClient.
- Password input at the Sm@rtClient
The on-screen keyboard is hidden on the Sm@rtServer due to the actions carried out on the Sm@rtClient. Use the local on-screen keyboard for entries at the Sm@rtClient. The local on-screen keyboard will be displayed automatically on the Sm@rtClient or in the Sm@rtClient view. Close the on-screen keyboard manually. Select "Input > Hide Input Panel" to hide the local on-screen keyboard.

Note

The entries with full-screen keyboard are not protected on HMI devices with a screen size of $\leq 6''$.

Entries in Control Panel Applets which do not use the full-screen keyboard are protected.

Note

Hidden password input is not supported by the on-screen keyboards of third-party products.

Note

You cannot enter special characters with the keyboard shortcut Alt Gr.

Perform operator control or monitoring on the HMI device

In the Sm@rtClient application window, the entire layout of the remote HMI device is shown. Depending on the configuration, you can specify monitoring only or operator control of all keys, including the function keys, with the mouse. In addition, the entire desktop can be accessed in the case of a PC.

For operator control via the keyboard, the following is available:

| Keyboard shortcut | Function |
|--------------------|---|
| <ALT+CTRL+SHIFT+O> | Opens the "Sm@rtClient Options" dialog |
| <ALT+CTRL+SHIFT+F> | Switches over to full screen mode |
| <ALT+CTRL+SHIFT+R> | Updates the display |
| <ALT+CTRL+SHIFT+N> | Opens the "New Sm@rtServer Connection" dialog |
| <ALT+CTRL+SHIFT+S> | Save as |
| <ALT+CTRL+SHIFT+T> | Displays and hides the toolbar |

2.2.1.4 Remote control via the Sm@rtClient display during runtime (Panels, Comfort Panels, RT Advanced)

Introduction

The Sm@rt options of WinCC enables access from the HMI device or PC to a remote HMI device via Ethernet.

Requirement

- The License Key "Sm@rtServer" is available at the Server-HMI device.
- Both devices are linked via a TCP/IP-ready network, that is, via a LAN or the Internet.
- HMI-device is configured as Sm@rtServer. For more information, refer to "Configure Sm@rtServer (Page 95)".
- The Sm@rtClient-Display in an image is added in the client-HMI device project. For more information, refer to "Project Sm@rtClient (Page 97)".

Implementing remote access

The Sm@rtServer supports remote monitoring or remote control on the remote device (server).

On the client HMI device, the connection to the Sm@rtServer is made during runtime by means of the Sm@rtClient display.

On the HMI device only the screen of the server, and not the soft keys, is displayed.

The form of the cursor is not a part of the screen and is therefore not transmitted. Only the coordinates of the cursor are transmitted.

Note

If a soft-key is activated on the client HMI device, then observe the following:

This signal is transferred to the Server-HMI device and becomes effective there, only if no function was configured at the soft-key.

Otherwise, the function projected on the client-HMI device is executed.

Use of direct keys for remote access

You can only operate direct keys locally on the server. Although the key for the direct key can be operated on the Sm@rtClient, no bit is set in the I/O range of the PLC.



CAUTION

Ethernet communication

In Ethernet-based communication, such as PROFINET IO, HTTP, Sm@rt Options and OPC, it is the end user who is responsible for the security of his data network. The proper functioning of the device cannot be guaranteed in all circumstances; targeted attacks, for example, can lead to an overloading of the device.

Password input

Password input at the Sm@rtServer

Instead of the on-screen keyboard, the following message is displayed on the Sm@rtClient if you enter the password directly at the Sm@rtServer: "Remote access by Sm@rt Options is in Progress. Please wait until the input of values has been ended." This measure prevents keyboard input for entering the password from being displayed on the Sm@rtClient.

Password input at the Sm@rtClient

The on-screen keyboard is hidden on the Sm@rtServer due to the actions carried out on the Sm@rtClient. Use the local on-screen keyboard for entries at the Sm@rtClient. The local on-screen keyboard will be displayed automatically on the Sm@rtClient or in the Sm@rtClient view.

Close the local on-screen keyboard manually. Select "Input > Hide Input Panel" to hide the local on-screen keyboard.

Note

The entries with full-screen keyboard are not protected on HMI devices with a screen size of $\leq 6"$.

Entries in Control Panel Applets which do not use the full-screen keyboard are protected.

Note

Hidden password input is not supported by the on-screen keyboards of third-party products.

Note

You cannot enter special characters with the keyboard shortcut Alt Gr.

See also

Project Sm@rtClient (Page 97)

Configure Sm@rtServer (Page 95)

2.2.2 Distributed operator stations (Panels, Comfort Panels, RT Advanced)

2.2.2.1 Configuration (Panels, Comfort Panels, RT Advanced)

Configuration

Multiple HMI devices are used as decentralized, coordinated operator stations that have access to a centralized HMI device connected to the PLC.

The HMI devices are linked via a TCP/IP-network, (LAN or Intranet /Internet).

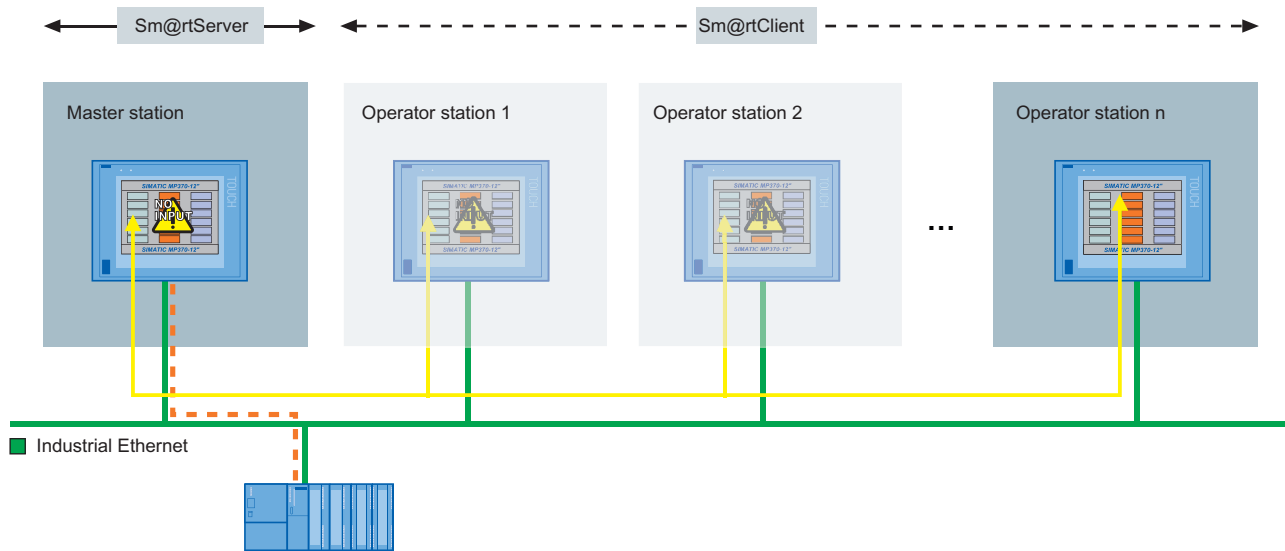


Figure 2-1 Distributed HMI

Only one HMI device, the Sm@rtServer, contains the configuration data. The Sm@rtServer is controlled from the HMI devices.

The decentralized operator stations are the Sm@rtClients. These operator stations display the same process screen of the server. A Sm@rtClient-Display is configured in the process screen for the operation and monitoring.

All devices have the same screen resolution.

The operator stations are in shared mode. As soon as a defined period of time elapses without any action on an operator station, another operator station can become active. If Sm@rtClient display is configured accordingly, the user can also log off directly.

Advantages

- Operator control and monitoring can be performed from various locations without significant efforts.
The project only has to run on one HMI device configured as a server. The same client project runs on all other HMI devices; the Sm@rtClient display object is contained in a screen on these devices. The screen of the server is displayed via the Sm@rtClient display.
- The server is situated remotely from the machine and is thus not exposed to the environmental conditions of the machinery room.
- Coordinated operation is provided by the Sm@rtServer. Additional PLC investments are not required. For example, the load on the field bus is also reduced – the communication load on the bus is removed due to the interlocking mechanisms on the PLC side.

2.2.2.2 Configure distributed operator stations (Panels, Comfort Panels, RT Advanced)

Introduction

Operator control of an extensive printing machine need to have the option to exercise control, when necessary, at multiple locations along the machinery. Depending on his current location, the operator must be able to access the process from an operator station in the vicinity.

Requirement

- The HMI-device with the configuration data is connected with the control.
- The server-HMI device and the Client-HMI devices are networked with each other via TCP/IP-Network.
- The License Key "Sm@rtServer" is available.

Configuration steps

The following basic steps are necessary for configuring the distributed operator stations:

| Step | |
|------|---|
| 1 | Configuring Sm@rtServer (Page 95) |
| 2 | Setting WinCC Runtime Advanced Internet (Page 96) |
| 3 | Project Sm@rtClient (Page 97) |

2.2.2.3 Configure Sm@rtServer (Panels, Comfort Panels, RT Advanced)

Configuring Sm@rtServer (Panels, Comfort Panels, RT Advanced)

Requirement

- The WinCC-Project for the Server-HMI device is configured.

Procedure

Proceed as follows to configure the Sm@rtServer in WinCC:

1. Double-click on the "Runtime-settings" entry in the project tree.
2. In the "Runtime-settings" editor, click on the "Services".
3. Enable "Sm@rtServer" in the group "RemoteControl".
4. Transfer the compiled WinCC-project to the Server-HMI-device.

Result

The Server-HMI device is configured as Sm@rtServer .

Setting WinCC Runtime Advanced Internet (Panels, Comfort Panels, RT Advanced)

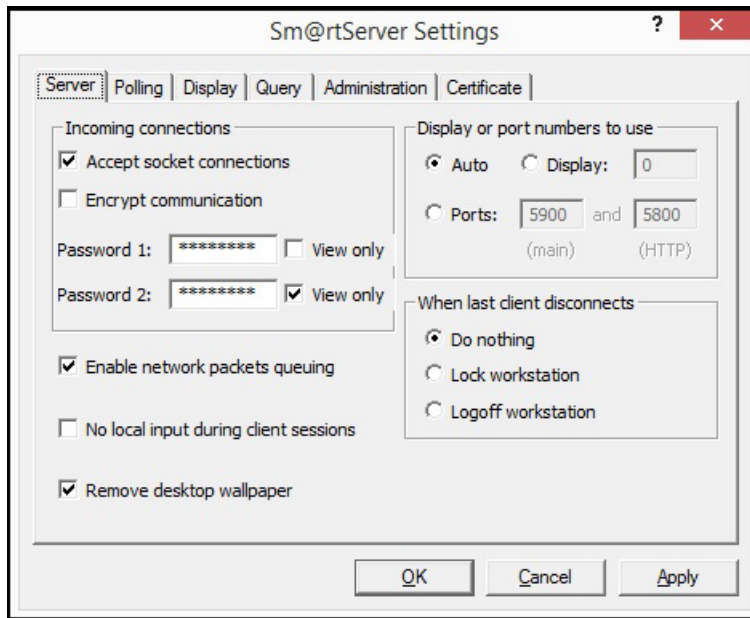
Requirement

- The "Control Panel" opens.
- The "WinCC Runtime Advanced Internet" dialog is open.
- The "Remote" tab is displayed.

Procedure

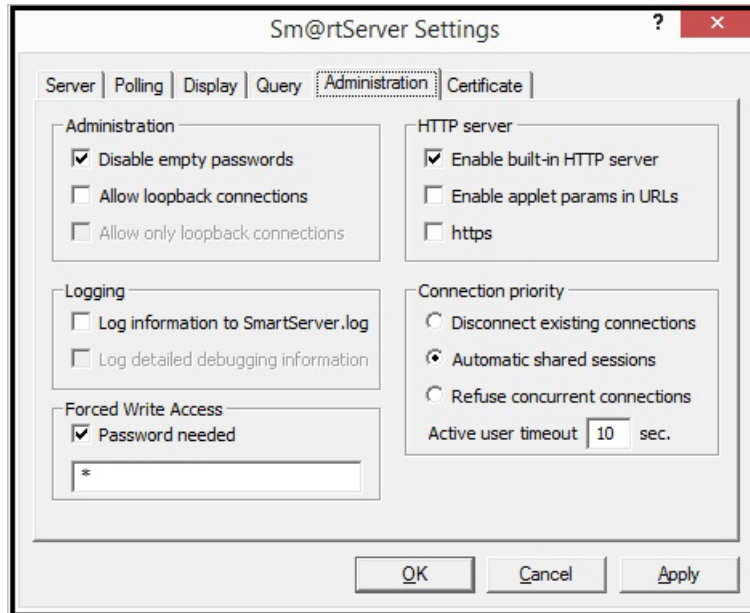
Proceed as follows to change the "WinCC Runtime Advanced Internet" settings on the Sm@rtServer:

1. On the "Remote" tab, select Start automatically after booting".
2. Click on the "Change settings" button. The "Sm@rtServer Settings" dialog opens.



3. On the "Server" tab, select "Accept socket connections".
4. Enable "Encrypt communication" to establish an encrypted connection to the server.
5. Enter a password for "Password 1" and "Password 2". Click "Apply".

6. Click on the "Administration" tab.



7. In the area "Connection priority", select "Automatic shared sessions". For "Active user timeout" enter time that must elapse without any actions on the active HMI device before access can be changed.
8. Under the "Forced write access", clear "Password needed" for the forced access to the HMI device. Click "Apply". Click "OK" to close all opened dialogs.

Result

The settings were changed. The changes will be effective after restarting the Sm@rtServer.

See also

Project Sm@rtClient (Page 97)

2.2.2.4 Project Sm@rtClient (Panels, Comfort Panels, RT Advanced)

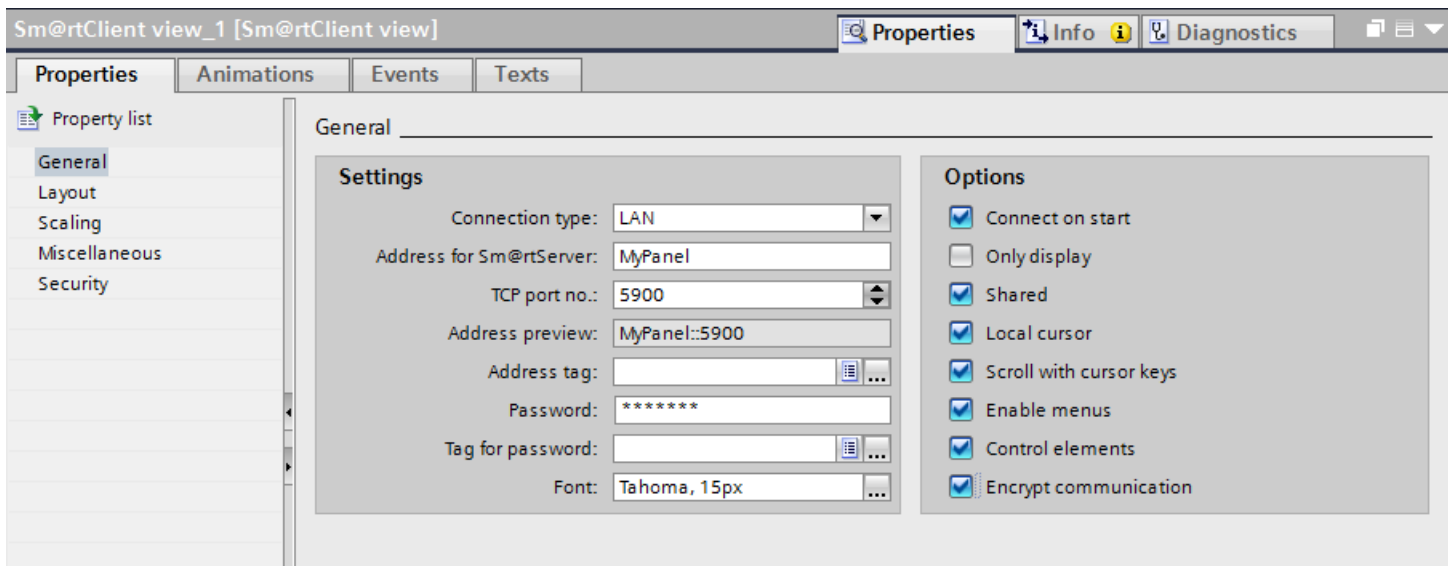
Requirement

- The WinCC project for the client HMI device is configured.
- The "Screens" editor is open.
- The Inspector window is shown.
- The "Tools" task card is open.

Procedure

Proceed as follows to configure the Sm@rtClient:

1. Insert the Sm@rtClient display in the start screen.
2. In the Inspector window, click "Properties > Properties > General".
3. Enter the IP address or the name of the server HMI device in the "Address Sm@rtServer" field.
4. Enter "Password 1" configured on the server in the "Password" field.
5. Activate the "Encrypt communication" function in the "Options" area.
When the "Encrypt communication" function is enabled, the connection to the server is encrypted through the exchange of certificates.
6. Activate the setting "Allow Menu".
This provides the operator with the option of logging off using the menu.



7. Transfer the compiled project to all operator stations.

Result

The Sm@rtClient display was added to the start screen in the WinCC project of the Sm@rtClient.

After the Sm@rtServer and the operator stations are started for the first time, a check is carried out as to whether communication is encrypted.

- If communication is encrypted, save the certificate of the Sm@rtServers on the HMI device. Afterwards, you connect the Sm@rtClient with the Sm@rtServer using encrypted communication.
- If communication is not encrypted, you connect the Sm@rtClient with the Sm@rtServer without a certificate.

In order to control the server from an operator station, the operator must wait a specified amount of time following the last action on another HMI device.

If the operator uses the menu of the Sm@rtClient display to log off at the previously used HMI device, he can immediately control the server at the next HMI device.

See also

Remote control via the Sm@rtClient display during runtime (Page 91)

"Server" tab (Page 61)

Setting WinCC Runtime Advanced Internet (Page 96)

2.3 E-mail notification from runtime (Panels, Comfort Panels, RT Advanced)

2.3.1 Process flow (Panels, Comfort Panels, RT Advanced)

Introduction

WinCC Runtime Advanced with the Sm@rtService offers the option of sending messages automatically via email.

The automatic e-mailing feature ensures that all people affected by the machine status (for example, shift engineer and sales manager) are informed in a timely manner.

Contents and triggers for e-mailing

The following events can trigger an e-mail to be sent:

- Alarm of a certain alarm class
- Event in which a standard function has been configured, such as a tag value change, etc.

Such an e-mail can have the following contents:

- Alarm text with process tags (maximum of 256 characters)
- Date/time
- E-mail address for replies

If you use e-mail gateways or SMS gateways, you receive access to standard networks, which requires external service providers. If configured accordingly, in critical situations the operator station sends an SMS to your mobile phone.

Enabling e-mailing and SMS

The HMI device can send e-mails to an SMTP server only. The server sends the e-mails to the addresses configured in the server.

Nothing else is required to send e-mails to addresses in the company network. However, an external service provider is required to access standard networks.

If an SMS communication is to be sent to service personnel, an SMS gateway is required as well.

Settings on the HMI device

The settings for emailing on the HMI device are made in the "Email" tab under "WinCC Runtime Advanced Internet" on the control panel.

The "Sender" entry field is assigned the default value "Automation HMI device." A change is useful if you want the recipient to be able to identify the device from which the e-mail originated, e.g. "HMI device on production line 2"

You can also use an SMTP server that support authentication to send e-mail.

The following authentication modes can be configured:

- Authentication by means of a valid e-mail address
- Authentication by means of user name and password

Data can also be encrypted and sent via an SSL connection. This means the data cannot be manipulated or read.

2.3.2 Specify trigger for E-Mailing (Panels, Comfort Panels, RT Advanced)

Requirement

- You have to create WinCC project.

Procedure

Proceed as follows to send a message when an alarm is triggered:

1. Double-click on the "HMI-Alarms" entry in the project tree.
2. Click the "Alarm classes" tab in the "HMI-Alarms" editor.
3. Select the alarm class, e.g. "Errors".
4. Enter the E-Mail-Address in the inspector window under "Properties > Properties > General".
5. Create an analog or discrete message with this alarm class.

Result

The trigger to send a message was configured. A message is automatically sent when a message of this alarm class is triggered.

2.3.3 Configure secure e-mail notification from Runtime (Panels, Comfort Panels, RT Advanced)

Introduction

If you send e-mail via the SMTP protocol, the sender is not verified. To ensure secure transmission of e-mails, you can use SMTP servers that support SMTP AUTH (authentication).

You must log on to the SMTP server to send e-mails. The following authentication modes can be configured:

- Authentication by means of a valid e-mail address
- Authentication by means of user name and password

The data can also be sent via an SSL connection. SSL (Secure Socket Layer) encrypts e-mails and user data for transmission. This means the e-mail cannot be manipulated or read during transmission.

Requirement

- The SMTP server supports SMTP AUTH and STARTTLS. You can obtain more detailed information from your service provider.
- User name and password or a valid e-mail address for logon to the SMTP Server. You can obtain this data from your service provider.
- The SMTP server is available.
- The e-mail address of the service technician is entered in the alarm class.
- An analog or discrete alarm has been created for this alarm class.

Procedure in WinCC

1. Double-click on the "Runtime-settings" entry in the project tree.
2. In the "Runtime-settings" editor, click on the "Services".
3. Enter the sender name to be shown in e-mail under "Sender name". If the SMTP server does not support the function, delete the entry.
4. Assign a port number.
Port number 25 is assigned by default.
The port number in WinCC must match the port number in the "WinCC Internet Settings" on the HMI device.

Note

You can only configure the port number with the following HMI devices:

- Comfort Panels
 - RT Advanced
-

5. Enter the authentication data.
 - Authentication by means of a valid e-mail address
Type in the e-mail address required for SMTP authentication in the "E-mail address" input field.
 - Authentication by means of user name and password
Enter the user name and your password. You can obtain the user name and password from your service provider.
6. Enable "The server requires a secure connection (SSL)".

Procedure on the HMI device

Note

Note that the settings on the HMI device have a higher priority than the settings in the WinCC project.

1. Open the "WinCC Runtime Advanced Internet" dialog in the control panel of the HMI device.
2. Click on the "E-mail" tab.
3. Specify the SMTP server.
 - Select "Use the default project file" if you want to use the SMTP server defined in the project.
 - Deactivate "Use the default project file" if you do not want to use the SMTP server defined in the project. Specify the required SMTP server. For HMI devices with Windows CE, specify the computer name or the FQDN (Fully Qualified Domain Name).
4. Assign a port number.
Port number 25 is assigned by default.
The port number must match the port number in the WinCC Internet Settings in the HMI device.

Note

You can only configure the port number with the following HMI devices:

- Comfort Panels
 - RT Advanced
-

5. Enter the sender name given in the e-mail under "Name of the sender". If the SMTP server does not support the function, delete the entry.
6. Enter the authentication data.
7. Enter a valid e-mail address at "eMail address of sender" if required for authentication.
 - Click "Advanced" if you need a user name and password for authentication. The "Advanced Email Settings" dialog opens.

8. Type in the user name and password in the "Advanced Email Settings" dialog.
 - Enable "Use the default of the project file" to use default user data you have defined in the project.
 - Select "Use panel settings for authentication" if you do not want to use the user data defined in the project. Enter the user name and password.
9. Enable transmission via SSL.
 - To use the project settings, enable "Use the default of project file" and SSL in WinCC.

Result

If a tag such as a mixer speed exceeds configured limits, a corresponding alarm is displayed on the HMI device. The data is sent to the SMTP server via SSL connection. The e-mail is sent to the field service technician after successful logon.

2.4 Display integrated Service-Pages (Panels, Comfort Panels, RT Advanced)

2.4.1 Integrated Webserver (Panels, Comfort Panels, RT Advanced)

Introduction

The operator can display and navigate between web pages during runtime using the web server integrated in the HMI device.

The integrated web server displays the integrated service-pages. Depending on the configuration, own configured HTML-pages or Service-pages of a server accessible over Ethernet are be displayed.

Requirement

- "HTML-Pages" is activated in the WinCC-Project of the Server-HMI device for the "Services in Runtime".

Note

It is always possible on a PC to access HTML-pages in runtime, although the option "HTML-pages" is cleared. Setup always installs the standard pages of the Web Server on the PC. Assign an administrator password to prevent unauthorized access to the pages.

Purpose of the web server

The integrated web server permits HTML pages to be displayed during runtime over one of the following routes:

- Internet Explorer
- HTML browser screen object during runtime (not on Windows CE devices)

The following are displayed:

- internal Service-Pages available by default on the HMI-device
- Other pages that you configure
- Other Internet pages

An operator or service technician can access service-critical information via the HTML pages. The standard HTML pages provide the following options:

- Remote control (if the HMI device is configured as a Sm@rtServer)
- Remote control using Microsoft Internet Explorer
- Starting and stopping of runtime
- Remote access to recipe data records and password lists
- Display of system information
- File management using a file browser
- Downloading of configuration data
- A "DATETIME" tag always returns a date within the range from 1.1.1970 00:00:00 to 31.12.2037 23:59:59.
- The "Export recipes" function requires the following authorizations:
 - PC: "UserData"
 - other HMI devices: "UserData" and "FileBrowserUser"

HTML browser for HTML pages

The HTML-pages are also displayed using the configured "HTML browser" screen object (not on Windows-CE devices).

You can also arrange for input or activation of an Internet address. As soon as the operator enters or activates an address, the HTML browser opens the relevant page.

The appearance and functionality of the HTML browser screen object depends on the HMI device type. On PCs, the HTML browser corresponds to the Internet Explorer installed.

Note

Note that the HTML browser options during runtime are restricted due to operating device capacities and options.

2.4.2 Service-pages of the web server (Panels, Comfort Panels, RT Advanced)

Introduction

The operator can use Internet Explorer or the HTML browser screen object during runtime to display service-pages without any additional configuration.

You can also create own service-pages. For detailed information, refer to "Configure In-house service-pages".

Requirement

- "HTML-Pages" is activated in the WinCC-Project of the Server-HMI device for the "Services in Runtime".

Note

It is always possible on a PC to access HTML-pages in runtime, although the option "HTML-pages" is cleared. Setup always installs the standard pages of the Web Server on the PC. Assign an administrator password to prevent unauthorized access to the pages.

Service-pages

WINCC Runtime has the following service-pages:

- start.html: Home page
- RemoteControl.html: Remote control (only for Internet Explorer)
- Control.html: Control functions
- StatusDetails.html: System diagnostics
- Browse.html: File browser (only for Internet Explorer)

Home page: Start.html

The start page contains the links to all other pages and displays current information about the project: Mode, software versions, device data, etc.

"Remote control": RemoteControl.html

The "Remote control" page enables operator control of the HMI device for which a page is to be displayed. This page can only be displayed by using the Internet Explorer.

"Control functions": Control.html

The "Control functions" page enables the following options on the HMI device for which a page is to be displayed:

- Starting and stopping of HMI runtime

Note

The transfer mode must be set in the Loader-menu on the HMI-device.

- Exporting and importing of recipes

Note

After importing recipes with Sm@rtService (HTML pages), restart Runtime. The imported recipes only become active the next time Runtime is started.

- Exporting and importing of password lists

Note

The password list must be named "pdata.pwl." It is exported to the following directory:

On Windows CE-devices: In the "\\Flash\\simatic\\" target directory

On PCs: the folder that was set in the file "HMIloader.exe".

The password list is exported and becomes active the next time Runtime is started.

"System diagnostics": StatusDetails.html

The "System diagnostics" page contains system alarms from the alarm buffer.

"File Browser" – Browse.html

The "File Browser" page is used to administer directories and files on the remote device. This page can be displayed with any Internet browser.

2.4.3 Installing the client and server certificates for SSL (Panels, Comfort Panels, RT Advanced)

Introduction

To ensure data security, data are encoded for transmission over the Internet. Encoding and decoding is performed by appropriate software – the certificates for SSL (Secure Sockets Layer).

- The client certificate for SSL must be installed on devices that are to be used to control a remote device.
- The server certificate for SSL must be installed on HMI devices that are to allow remote control.

2.4.4 Configure access to service-pages (Panels, Comfort Panels, RT Advanced)

2.4.4.1 Configure integrated web server (Panels, Comfort Panels, RT Advanced)

Configure WinCC-Project (Panels, Comfort Panels, RT Advanced)

Requirements

- The WinCC-Project of the server-HMI-device is configured.

Procedure

Proceed as follows to configure the HMI device in such a way that other HMI devices or PCs can be connected to it:

1. Double-click on the "Runtime-settings" entry in the project tree.
2. In the "Runtime-settings" editor, click on the "Services".
3. Enable the "HTML-Pages" in the "Diagnostics" group.
4. Transfer the compiled WinCC-project to the Server-HMI-device.

Result

The Server-HMI-device is configured as web server.

Setting WinCC Runtime Advanced Internet (Panels, Comfort Panels, RT Advanced)

Requirement

- The "WinCC Runtime Advanced Internet" dialog is open.
- The "Web Server" tab is displayed.

Procedure

Proceed as follows to change the "WinCC Runtime Advanced Internet" settings on the HMI device:

1. Click "User Administration" in the "Web Server" tab.
2. Open the "UserDatabase-Edit" dialog.
3. Click "Add" in the "User manager" tab to create a new user.
4. Enter a user name and specify a password.
5. Click "Apply".
6. Click the "Authorizations" tab.

2.4 Display integrated Service-Pages (Panels, Comfort Panels, RT Advanced)

7. Specify on the "Authorizations" tab, which functions can the user carry out on the HTML-pages of an HMI-device. You can find more detailed information on this in the section "User administration for web server (Page 68)".
8. Close the "UserDatabase-Edit" dialog.
9. On the "Remote" tab, select the "Start automatically after booting" check box.
10. Click "Change settings" and select the "Enable connections" check box in the "Sm@rtServer Settings" dialog.
11. Specify a password for "Password2" so that the HMI device can be remotely controlled by the service technician.

Result

A user was created on the HMI device in the user administration of the Web server and configured for the remote control.

The service technician can be connected to the HMI-device by means of the Internet Explorer and the Sm@rtClient Application. After disconnecting the connection, the HMI-device can be operated from his PC.

See also

WinCC Runtime Advanced Internet, "Web Server" tab (Page 59)

User administration for web server (Page 68)

"Server" tab (Page 61)

2.4.4.2 Display and remote-control Service-Pages (Panels, Comfort Panels, RT Advanced)

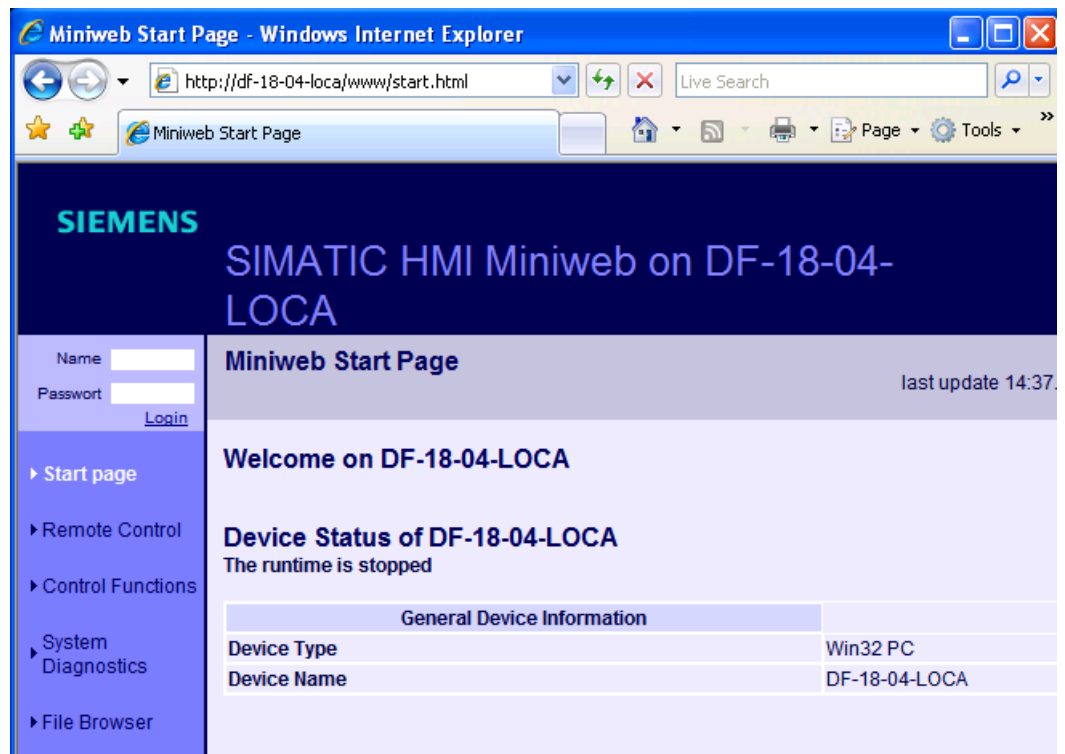
Requirements

- A user is created on the HMI-device in the user administration for the web server.
- The web server is started.
- The Client-and Server-certificates are installed to ensure the data security when transferred via internet.

Procedure

To display and control the service pages, follow these steps:

1. Start the Internet Explorer on the configuration-PC and connect with the "Homepage" of the HMI-device.



2. For "Name" and for "Password", enter the data of the user configured in the user administration of the web server. Click "Login".
3. Click "System Diagnostics". The system alarms from the alarm buffer are displayed on this page.
4. Click "Remote Control" to remotely control the HMI-device.

Result

The service-pages are displayed. The HMI-device can be operated or monitored via the service-pages.

A keyboard units cannot be operated completely in the Internet Explorer, since only the screen content is displayed. Use the Sm@rtClient-Application to remotely control the keys of HMI-device. The Sm@rtClient-Application can be located under "Start > Program > Siemens Automation > Runtime Systems > WinCC Runtime Advanced > Sm@rtClient"

2.4.5 Create own Service-pages (Panels, Comfort Panels, RT Advanced)

2.4.5.1 Basics (Panels, Comfort Panels, RT Advanced)

Introduction

The basic framework of the service-pages corresponds to a normal HTML-file.

- Declaration of the document type
- Header with data for the title
- Body - content to be displayed.

Variable parameters in Service-pages

You can specify variable parameters in HTML documents. As soon as a page with variable parameters is opened, the parameters are replaced by specific values.

```
<BODY > Welcome on <MWSL><!-- write(GetVar("[Parameter]")); --></MWSL></BODY>
```

Available variable parameter

| Parameters | Meaning |
|-----------------------|--|
| ProgramMemoryComplete | CE only: Total program memory |
| ProgramMemoryFree | CE only: Program memory available |
| ProgramMemoryUsed | CE only: Program memory utilized |
| FlashComplete | CE only: Total flash memory |
| ObjStrComplete | CE only: Total available flash memory |
| ObjStrFree | CE only: Volatile memory available |
| ObjStrUsed | CE only: Volatile memory utilized |
| DeviceType | Type of target device as specified in the control panel. |
| BtLdVer | CE only: Bootloader-version, as specified in the control panel. |
| BtLdRelDate | CE only: Bootloader release date |
| ImageVersion | CE only: Image version as it appears on the loader |
| DramSize | CE only: Size of DRAM |
| HostName | The name by which the device is logged on/identified in the network. |
| RtState | Indicates whether Runtime is running on the target device. |
| SystemMessageTable | Outputs a table containing the current system events. |

In the example below, the "HostName" parameter is replaced by the network-name of the device.

```
<BODY > Welcome on <MWSL><!-- write(GetVar("[HostName]")); --></MWSL></BODY>
```

Process tag

Process tag values can also be displayed in HTML pages. The syntax is the same as for device tags. Use the tag name as a placeholder for the tag value, , e.g. Tag_1.

```
<BODY > Welcome on <MWSL><!-- write(GetVar("[Tag_1"]); --></MWSL></BODY>
```



CAUTION

Data inconsistency caused by HTML pages

Note the information below if the "Cyclic in operation" acquisition mode is set at tag:

1. If this tag is not displayed on the HMI device, the HTML page displays the incorrect tag value in the following situations:
 - The HTML page display a "0" value at its first call. The HTML page only displays the correct value after it is called again or updated.
 - The last value is displayed if the connection to the PLC goes down.
2. The HTML page also displays the correct tag value if the tag is displayed on the HMI device.

Situation 1 is based on standard behavior: If a tag is currently not in use currently and its value is not acquired in "Cyclic continuous" mode, the tag is loaded with its initial value in Runtime. Instead of reading the values from the PLC, however, the HTML page receives these from Runtime.

Link own Service-pages

If a user connects to an HMI device, he is automatically forwarded to the start page `http://<Device name>/www/start.html`. This page represents the starting point for the HTML-pages of the web server. Every standard page is accessible from the start page via a link. For this reason, you insert a link for each of your HTML pages in the start page.

Note

When inserting links in the HTML page, you must differentiate between relative and absolute links. Make sure that absolute links start with `"/www"` to ensure that the document will be searched for in the correct directory. Example: `"/www/MyDocument.HTML"`.

Storage location of the service-pages

If files are to be located during a transfer, they must be in a specific directory:

- on a PC with Windows operating system: `"C:\ProgrammData\Siemens\CoRtHmiRTm\MiniWeb14.x.x\WebContent"`
- on xP 177B: `"<ES-InstallationPath>\Transfer\11.0\XP177B\WebContent.zip"`
- on xP 277: `"<ES-InstallationPath>\Transfer\11.0\XP277\WebContent.zip"`
- on MP 177: `"<ES-InstallationPath>\Transfer\11.0\MP177\WebContent.zip"`
- on MP 377: `"<ES-InstallationPath>\Transfer\11.0\MP377\WebContent.zip"`

- on Mobile Panel 177 PN: "<ES-InstallationPath>\Transfer\11.0\XP177B\WebContent.zip"
- on Mobile Panel 277: "<ES-InstallationPath>\Transfer\11.0\XP277\WebContent.zip"
- on Mobile Panel 277 (F) IWLAN: "<ES-InstallationPath>\Transfer\11.0\XP277_W\WebContent.zip"
- one Mobile Panel 277 (F) IWLAN V2: "<ES-InstallationPath>\Transfer\11.0\XP277_W2\WebContent.zip"

2.4.5.2 Create service-page for displaying process values (Panels, Comfort Panels, RT Advanced)

Requirement

The Ta_1 and Tag_2 tags are created in the WinCc-Project.

Procedure

To create an own Service-page, follow these steps:

1. Copy the "WebContents" ZIP-file in a random work directory on your Configuration-PC and un-zip the ZIP-file.
2. Create a copy of start.html and rename the copy in "tag.html".
3. Open the "tag.html" in a text editor, e.g. Notepad.
4. Replace the existing table with a new table, in which the process values of "Tag_1" and "Tag_2" tags are displayed. Save the file "tag.html".

```
<font class="ad_headline2">Device Status of <MWSL><!-- write(GetVar("HostName")); --></MWSL></font><br>
<b>The runtime is <MWSL><!-- write(GetVar("RtState")); --></MWSL></b><br><br>
<table border="1" class="sph_table" cellspacing="0" width="600">
<tr><th class="sph_th"><b>Display of process tags </b></th></tr>
<tr><td class="sph_td"><b> "Tags1" </b></td><td class="sph_td"><MWSL><!-- write(GetVar("Tag_1")); --></MWSL>&nbsp;</td></tr>
<tr><td class="sph_td"><b> "Tags2" </b></td><td class="sph_td"><MWSL><!-- write(GetVar("Tag_2")); --></MWSL>&nbsp;</td></tr>
</table>
```

5. Open the "start.html" file and add a hyperlink to page "tag.html". Expand the available navigation bar, in which you supplement the existing table by an entry.

```
<tr>
<td width="8"></td>
<td width="7"></td>
<td width="101" class="ad_nav_link"><a href="tag.html" class="ad_nav_link">Process value</a></td>
</tr>
```

6. Save start.html.

Result

You have created the service-page "tag.html". You have added a hyperlink on the start page in order to navigate to the service-page from the start-page.

2.4.5.3 Transfer Service-pages (Panels, Comfort Panels, RT Advanced)

Transfer files using the standard-path (Active Sync/CF- card)

Proceed as follows to transfer files via the standard-path:

1. Copy the changed HTML pages and pictures according to "\\Flash\\Simatic\\WebContent". Access then takes place with "http://<device>/www/<HTML page>".

Transfer files via the project transfer

Proceed as follows to transfer the files via the project transfer:

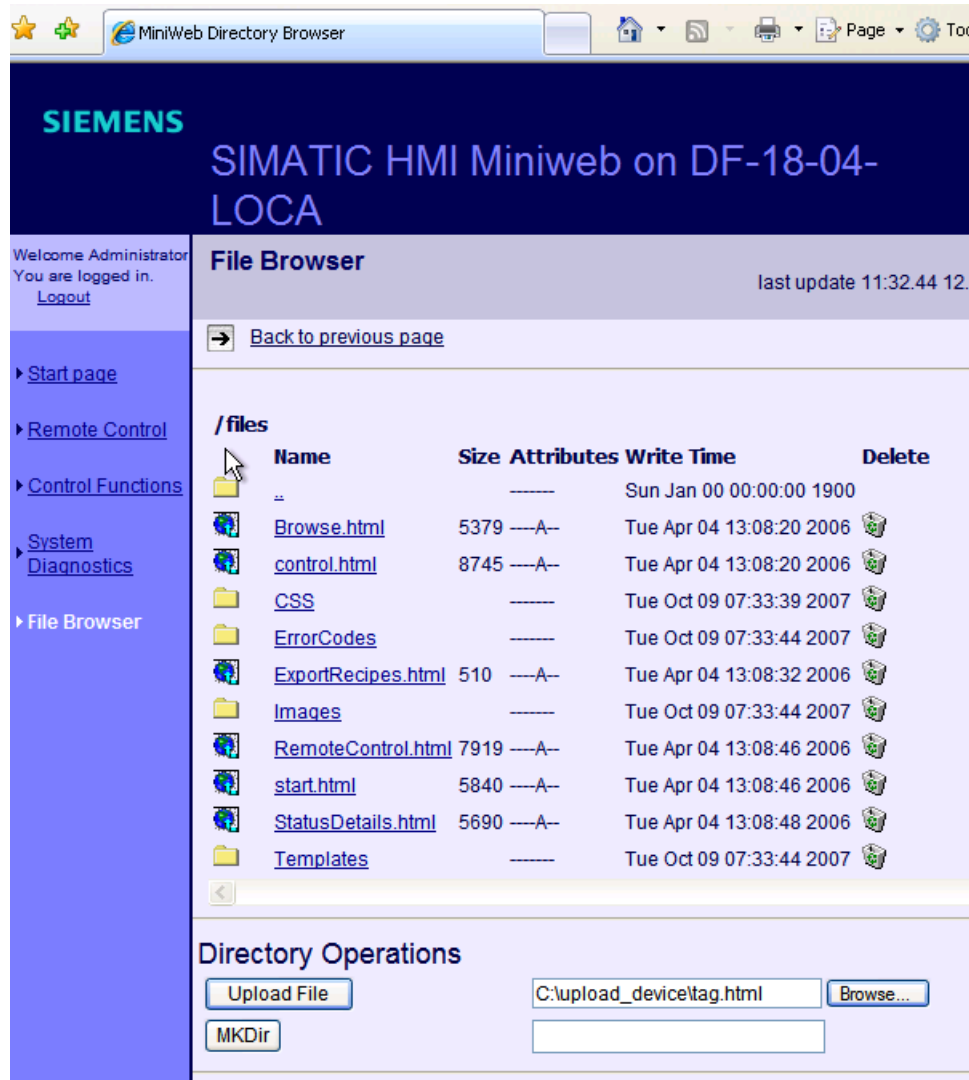
1. Add the changed files to the ZIP-file "WebContents". This file must contain all HTML pages and associated pictures.
Make sure to provide the correct path information because the files are unpacked in the directories specified in the zip file. Incorrect path information results in errors in direct addressing or due to links.
2. In order to transfer the ZIP-file "WebContents", copy this in a certain directory, e.g. for the transfer to an MP377 "<ES-Installationspath>\\Transfer\\1.3\\MP377\\WebContent.zip".
3. Transfer the project to the HMI device.
The ZIP-file "WebContents" is transferred to the Windows CE device where it is unzipped.

Transfer files using the File Browser

Proceed as follows in order to transfer files using the file transfer:

1. Start the Internet Explorer on the configuration-PC and connect with the "Homepage" of the HMI-device.
2. Log-on to the internal Web Server to work with the File Browser.
For read and write access to the file browser, the user must possess the web authorizations "FileBrowserAdministrator" and "FileBrowserUser" .
3. Click on "Browse" in the File Browser . The file selection dialog opens.

4. Navigate to the file storage location by means of this dialog. Select the desired file and click "Open."



5. Click "Upload File". The file is copied in the directory of the internal web server.

See also

Basics (Page 110)

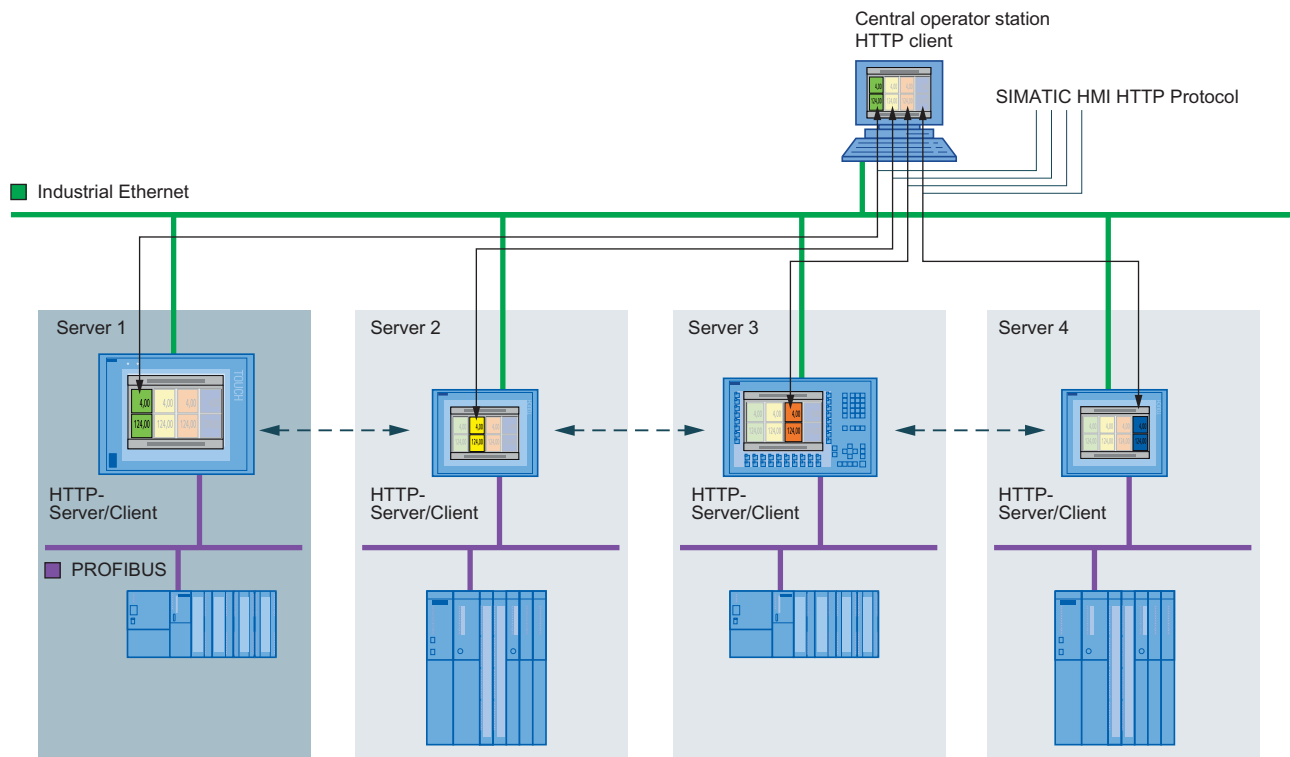
2.5 Access via SIMATIC HMI HTTP Protocol (Panels, Comfort Panels, RT Advanced)

2.5.1 Configuration (Panels, Comfort Panels, RT Advanced)

Configuration

During the communication via SIMATIC HMI HTTP Protocol, an HMI-device accesses the tags of a different HMI-device. The access is "read-only" or "read and write" depending on the configuration of the concerned HMI-device.

The HMI device providing the tags is the HTTP-server; the other HMI-device is the HTTP-client. However, access to tags functions in both directions.



2.5.2 Configure access via SIMATIC HTTP Protocol (Panels, Comfort Panels, RT Advanced)

Introduction

The tags in service-application should be illustrated in an overview for a configuration from multiple HMI-devices.

The panels in the machine level are used as tag server. The service-application illustrating tags of machines in an overview image runs on a PC.

Requirement

- The HMI-devices are networked via a TCP/IP-network with each other.

Configuration steps

The following basic steps are required to configure the access via "SIMATIC HMI Protocol".

| Step | |
|------|---|
| 1 | Configure WinCC-Project (Page 117) |
| 2 | Setting WinCC Runtime Advanced Internet (Page 118) |
| 3 | Configuring HTTP connections in the client (Page 119) |
| 4 | Configure the HTTP-Client tags (Page 120) |

2.5.3 Permissible data types (SIMATIC HMI HTTP protocol) (Panels, Comfort Panels, RT Advanced)

Permitted data types

When configuring tags, the data types listed below can be used.

| Data types in the HTTP Protocol | Length | Signs | Range of values |
|---------------------------------|---------|-------|---|
| Bool | 0 | No | true (-1) or false (0) |
| Char | 1 byte | Yes | -128 to 127 |
| Byte | 1 byte | No | 0 to 255 |
| Int | 2 bytes | Yes | -32768 to 32767 |
| UInt | 2 bytes | No | 0 to 65535 |
| Long | 4 bytes | Yes | -2,147,483,648 to 2,147,483,647 |
| ULong | 4 bytes | No | 0 to 4,294,967,295 |
| Float | 4 bytes | Yes | -3.402823E38 to -1.401298E-45 for negative values and 1.401298E-45 to 3.402823E38 for positive values |

| Data types in the HTTP Protocol | Length | Signs | Range of values |
|---------------------------------|---------------|-------|---|
| Double | 8 bytes | Yes | -1.79769313486231E308 to -4.94065645841247E-324 for negative values and 4.94065645841247E-324 to 1.79769313486232E308 for positive values |
| String | 1 to 255 byte | — | |
| DateTime | 8 bytes | — | 1.1.1970 00:00:00 up to 31.12.2037 23:59:59 |

Please note that data types may be defined in external controllers which have different names in WinCC. To ensure correct assignment, please observe the tag definition in the external controllers.

Note

It is not possible to access array tags from an HTTP client.

See also

Configure WinCC-Project (Page 117)

2.5.4 Configure HTTP server (Panels, Comfort Panels, RT Advanced)

2.5.4.1 Configure WinCC-Project (Panels, Comfort Panels, RT Advanced)

Requirement

- The WinCC-Project for the Server-HMI device is configured.

Procedure

Proceed as follows to configure the HTTP-Server:

1. Double-click on the "Runtime-settings" entry in the project tree.
2. In the "Runtime-settings" editor, click on the "Services".
3. Select "SIMATIC HMI HTTP Server" in the group "Read/write tags".
4. Check the data types of the tags. The HTTP-client can access only those tags, whose data type is supported by communication driver "SIMATIC HMI HTTP Protocol". For additional information, refer to "Permissible data types (SIMATIC HMI HTTP Protocol) (Page 116)".
5. Transfer the compiled WinCC-project to the Server-HMI-device.

Result

The HMI-device is HTTP-server configured.

See also

Permissible data types (SIMATIC HMI HTTP protocol) (Page 116)

2.5.4.2 Setting WinCC Runtime Advanced Internet (Panels, Comfort Panels, RT Advanced)

Requirement

- The "Control Panel" opens.
- The "WinCC Runtime Advanced Internet " dialog is open.
- The "Web Server" tab is displayed.

Procedure

Proceed as follows to change the "WinCC Runtime Advanced Internet" settings on the HTTP server:

1. Specify the access to tags in case of "Tag access".
 - "Read/write": read and write access
 - "Read only": read access
2. Specify the authentication for access in case of "Tag authenticate":
 - "No authentication": No authentication required.
 - "Authentication required": A password is required for the access. Specify the password for configuring the connection via the SIMATIC HMI HTTP Protocol .
3. Click "User Administration" in the "Web Server" tab. Enter your password. The "UserDatabase-Edit" dialog is opened. For detail instructions, refer to "User administration for Webserver (Page 68) ".
4. Click "Add" in the "User manager" tab to create a new user. Enter a user name and specify a password. Click on "Apply".
5. Click the "Authorizations" tab.
6. Specify the web-authorizations on the tab "Authorizations". The user must have the Web-authorization "RTCommunication" for utilizing the SIMATIC HTTP Server.
7. Close all open dialog boxes.

Result

The settings were changed. The changes will be effective after the restart of the WebServer.

See also

Settings on the HMI device (Page 56)
WinCC Runtime Advanced Internet, "Web Server" tab (Page 59)
User administration for web server (Page 68)

2.5.5 Configuring HTTP clients (Panels, Comfort Panels, RT Advanced)

2.5.5.1 Configuring HTTP connections in the client (Panels, Comfort Panels, RT Advanced)

Requirement

The communication driver "SIMATIC HMI HTTP Protocol" is installed.

Procedure

Proceed as follows to create an HTTP-connection:

1. Double-click on the "Connections" entry in the project tree. The "Connections" editor opens.
2. Create a connection. Select "SIMATIC HMI HTTP Protocol" for "Communication driver".

The screenshot displays the WinCC RT Advanced configuration environment. At the top, the 'Connections' table is visible, showing a single entry named 'HTTP_Client_Server' with the 'SIMATIC HMI HTTP' communication driver. Below this, the 'Parameter' tab is active, showing the 'SIMATIC PC station - WinCC RT Advanced' configuration. The 'Interface' is set to 'ETHERNET'. To the right, the 'Estación' (Station) is represented by a computer icon. In the bottom right corner, the 'Web server on HMI device' configuration panel is open, showing fields for 'Address' (http://www.siemens.com), 'User name', 'Password', and 'Timeout' (10 s). Three checkboxes are also present: 'Allow invalid computer names for certificates', 'Ignore expired certificates', and 'Allow certificates signed by unknown publishers', all of which are checked.

| Name | Communication driver | HMI time synchronization mode | Station | Partner | Node | Online | Comment |
|--------------------|----------------------|-------------------------------|---------|---------|------|-------------------------------------|---------|
| HTTP_Client_Server | SIMATIC HMI HTTP | | | | | <input checked="" type="checkbox"/> | |
| <Add new> | | | | | | | |

Parameter | **Area pointer**

SIMATIC PC station - WinCC RT Advanced

WinCC RT Adv

Interface: **ETHERNET**

Estación

Web server on HMI device

Address: **http://** **www.siemens.com**

User name:

Password:

Timeout: **10** s

☒ Allow invalid computer names for certificates

☒ Ignore expired certificates

☒ Allow certificates signed by unknown publishers

3. Select "Ethernet" for "Interface". Select the protocol type "http://" or "https://" for address.
4. Enter the name of the HTTP-server or its IP address.
Ask your network administrator for the specific name or parameters of your network.
If the server has already been commissioned, you can read out the IP address on the server as well:
 - Panel
Click "Start > Programs > Command Prompt" on the server and enter the "ipconfig" command using the screen keyboard. Press <Enter> to display the IP-address.
 - For PC/Panel PC
Click on the server on "Start > Run", enter "Cmd", and press <Enter>. The command interpreter is displayed. Enter the "ipconfig" command. Press <Enter> to display the IP-address.
5. If the "HTTPS" protocol type is selected, you can establish how the HTTPS-client verifies the properties of the server-certificate and how it should react in the event of error:
 - "Allow invalid computer names for certificates"
 - "Allow expired certificates"
 - "Allow certificates signed by unknown publishers"
6. If the "Authentication required" option is selected on the HTTP-server, enter the user name and the password.
7. Enter the time for "Timeout" after which disconnection is identified.

Result

A connection was created in the WinCC-Project of the HTTP-Client. You can find more detailed information on an HTTPS connection under "Commissioning an HTTP- connection (Page 121)".

See also

Commissioning an HTTP- connection (Page 121)

2.5.5.2 Configure the HTTP-Client tags (Panels, Comfort Panels, RT Advanced)

Requirement

- An HTTP-connection was created in the WinCC-Project of the HTTP-Client.
- A tag is created in the WinCC-Project of the HTTP-Server. The data type of the tags is supported by SIMATIC HMI HTTP Protocols .

Procedure

To create tags on the HTTP-client, proceed as follows:

1. Open the "HMI- tags" folder in the project tree and double-click the entry "Standard-tag table". The "Tags" editor opens.
2. Enter a clear tag-name for "Name" in the Inspector window under "Properties > Properties > General".
3. Select the HTTP-connection for "Connection".
4. Select the data type for "data type".
The client does not check any verification of the tag name and the data type. Pay attention that the selected data type here matches the data type of the tags in the HTTP-server. You can find more detailed information on this under "Permissible data types (SIMATIC HMI HTTP Protocol)".
Array tags are not permitted.
5. Enter the exact name of the tag that is to be communicated with on the HTTP-server in the "Address" field.
If the tag to be addressed is in a sub-folder, the complete path along with tag name must be given as address, e.g.[folder name]\[Tag name].

Result

A tag was created in the WinCC-Project of the Client-HMI-device. The tag has access to the HTTP-server tag via an HTTP-connection. You can use an "E/A-Field" in an image to display the process value of this tag.

2.5.6 Commissioning an HTTP- connection (Panels, Comfort Panels, RT Advanced)

Introduction

To establish an HTTP connection, you must perform the following actions:

- In the "Connections" editor of WinCC ES, configure the connection as an "https://" protocol type and define how the HTTPS client should verify the properties of the server certificate and respond to errors.
- Install a valid certificate on the HTTPS client.
Certificates are necessary for server authentication. Using certificates you can ensure that the server with which the connection is to be developed is actually the server for which it is outputting.

Principle of an HTTPS connection

After runtime start, the HTTPS client establishes a connection to the HTTPS server. The HTTPS server presents its certificate, which the client verifies for authenticity. The session code that can only be read by the HTTPS server is then transmitted. The session code is now available on both sides and enables a symmetrical data encryption.

Note

The certificate contains the current time. The current time can lead to problems if the time zones of the server and client are different. For example, a certificate generated on a server with an Asian time zone only becomes valid on a client with European time zone in the future (8 hours).

Preparation for installing a certificate on the client

The HTTPS server generates the certificate itself during the first HTTPS client access. The HTTPS server saves the certificate to the "Cert.cer" file. The file is stored in the following directory:

- On a PC/Panel PC (with Windows) in the directory "<Runtime Directory>\SystemRoot\SSL"
- On Windows CE-based devices in the directory "Flash\Simatic\SystemRoot\SSL"

The certificate must be stored on the HTTPS client on a storage medium from which it can be launched with a double click. You can select from the following transfer options:

| Server | Client | Possible file transfer |
|--|--|---|
| with Windows (PC, Panel PC) | with Windows (PC, Panel PC) | <ul style="list-style-type: none"> • Diskette • USB stick • LAN (Ethernet) • Internet Explorer (via TCP/IP if service is already running) |
| with Windows CE (xP 277, MP 377, xP 177B, Mobile Panel 177 PN, Mo- bile Panel 277, Comfort Pan- els) | with Windows (PC, Panel PC) | <ul style="list-style-type: none"> • Memory card • ActiveSync (serial) |
| with Windows (PC, Panel PC) | with Windows CE (xP 277, MP 377, xP 177B, Mobile Panel 177 PN, Mo- bile Panel 277, Comfort Pan- els) | |
| with Windows CE (xP 277, MP 377, xP 177B, Mobile Panel 177 PN, Mo- bile Panel 277, Comfort Pan- els) | with Windows CE (xP 277, MP 377, xP 177B, Mobile Panel 177 PN, Mo- bile Panel 277, Comfort Pan- els) | <ul style="list-style-type: none"> • Memory card |

Installing a certificate on a client with Windows

Insert the storage medium on which you have saved the "Cert.cer" file into the HTTPS client or open the directory in which the file is located. Double click on the file and follow the instructions in the Windows dialog.

Tip: The Internet Explorer provides an easy way to install a certificate. Connect to this device via HTTPS (e.g.: `https://<my device>`). The browser establishes if a certificate has not yet been imported. In this case, the browser asks if you want to install the certificate. Any faults in the certificate are displayed.

Installing a certificate on a client with Windows CE

Insert the memory card on which you have saved the converted "Cert.cer" file into the HTTPS client. WinCC includes the "InstallCert.exe" tool for importing certificates with Windows CE.

You can implement the installation as follows:

- In Explorer:
Double click the "Cert.cer" file to install the certificate.
- At the command prompt:
Enter "InstallCert [/command parameter] [filename]".
 - command parameters:
Parameter /r must be specified because the certificate used in WinCC Runtime Advanced is a root certificate.
A root certificate is the main certificate and is used to verify the authenticity of all other certificates transferred.
 - filename
You must specify the certificate file with its complete path (e.g. "Storage Card\Cert.cer")

A status alarm is output when you completed the installation. Runtime has to be restarted after the installation of a certificate on Windows CE- HMI devices with HTTPS clients. It is necessary to restart Runtime so that an HTTPS connection can be established.

The file "Cert.cer" cannot be opened.

If the "Cert.cer" file generated on the HTTPS server cannot be opened on HMI devices based on Windows CE 5.0 by double-clicking the client, follow these steps:

1. Open the Control Panel.
2. Select "Certificates > My Certificates".
3. Click the "Import" button.
A dialog box opens.
4. Select the "From a File" menu in the file browser and select the "Cert.cer" file.

2.6 Connection to the Office-world (Panels, Comfort Panels, RT Advanced)

2.6.1 Configuration (Panels, Comfort Panels, RT Advanced)

Data access via web service (SOAP)

WinCC provides options for utilization of web-service (SOAP). Web service (SOAP) is based on the Simple Object Access Protocol. Use of this protocol enables an external application to access tags of an HMI device via Ethernet. If the company network is protected by a Firewall, the system administrator must release the appropriate ports.

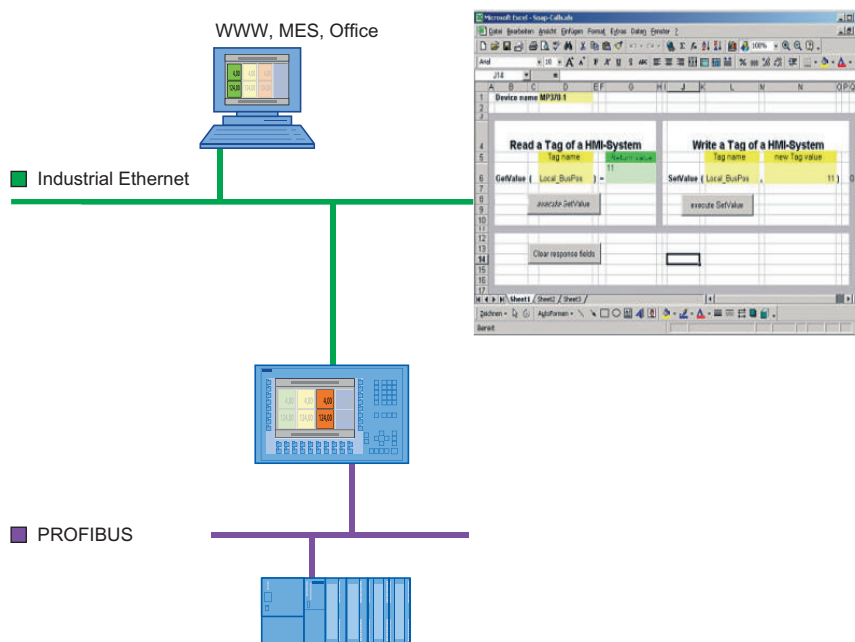


Figure 2-2 Communication with other applications

For example, a device is accessing two HMI devices. The operator sees the values of certain tags and can modify them.

You can use Microsoft Excel, for example, to display tags. You will require the latest version of "MS SOAP Toolkit V2.0" for this purpose. This version is available from Microsoft as a download.

The data access via SOAP is not supported by Windows 7. Use OPC to display the tags in MS Excel. You can find more detailed information on this under "Configuring OPC clients".

Data access to Windows CE HMI-devices

The data access via the Web-service(SOAP) on Windows CE-HMI-devices functions using only the device name and not via the IP-address.

Enter the device name of the HMI-device with the appropriate IP-address in the hosts-file. The hosts file is given in the directory "%windir%\system32\drivers\etc\", e.g. C:\WINNT\system32\drivers\etc.

The device name, e.g.DEVICEMP377, must be set in the control panel on the HMI device under "System > Device Name". Please change the default device name to ensure that the device name is unique within the network.

Example for the entry in the hosts-file:

192.168.56.198 DEVICEMP377

Replace the IP address by the device name in the SOAP client:

objRuntime.mssoapinit http://DEVICEMP377/soap/RuntimeAccess?wsdl

Data access with GetValue, SetValue

Access to a tag in SOAP using GetValue or SetValue functions require a special syntax.

- GetValue: "Sinus_1"
- SetValue: Sinus_1

The tag name must be given in inverted commas for GetValue. The message "Runtime is offline" will otherwise be output when runtime is accessed.

Note

Note that the tag name entry is case-sensitive.

2.6.2 Creating a VBA macro in MS Excel (Panels, Comfort Panels, RT Advanced)

Introduction

Data access over the network via web service (SOAP) is to be used to permit certain tags of an HMI device to be displayed and reset.

For this purpose, macros are written in Excel, which: 1) obtain the relevant tags on the PC over the network and display them, and 2) transfer reset values back to the HMI device.

The task can be solved using VBA macros "ReadTagValue" and "WriteTagValue," which obtain and display the relevant tags in Excel over an appropriate interface and return them to the HMI device over the network. Note that the tag name entry is case-sensitive.

Requirement

- The SOAP toolkit is installed.
- "Web-Service (SOAP)" is selected in the WinCC-Project under "Services in Runtime".

Procedure

1. Insert the "Control element toolbox" toolbar in your workbook in Microsoft Excel.
2. Create a command button. Label the button "ReadTagValue" and name it "Read value".
3. Double-click this command button.
The macro editor is displayed. The "Click" event is already preset.
4. Write the "ReadTagValue" macro ("intVarTag_1" designates the actual tag value):

```
'-----  
Private Sub ReadTagValue_Click()  
  
Dim objRuntime  
Dim intVarTag_1  
Dim objWorksheet  
  
Set objWorksheet = Excel.Worksheets("Sheet1")  
Set objRuntime = CreateObject("MSSOAP.SoapClient")  
objRuntime.mssoapinit "HTTP://servername/soap/RuntimeAccess?wsdl"  
objRuntime.ConnectorProperty("AuthUser") = "Administrator"  
objRuntime.ConnectorProperty("AuthPassword") = "100"  
Var = objWorksheet.Cells(1, 3)  
intVarTag_1 = objRuntime.GetValue(Var)  
objWorksheet.Cells(1, 1) = intVarTag_1  
  
End Sub  
'-----
```

1. Insert a command button. Label the command button "WriteTagValue" and name it "Write value".
2. Double-click this button.
3. Write the "WriteTagValue" macro ("intVarTag_1" designates the return value of the operation):

```

'-----
Private Sub WriteTagValue()

Dim objRuntime
Dim intVarTag_1
Dim objWorksheet

Set objWorksheet = Excel.Worksheets("Sheet1")
Set objRuntime = CreateObject("MSSOAP.SoapClient")
objRuntime.mssoapinit "HTTP://servername/soap/RuntimeAccess?wsdl"
objRuntime.ConnectorProperty("AuthUser") = "Administrator"
objRuntime.ConnectorProperty("AuthPassword") = "100"
Var = objWorksheet.Cells(2,3)
Value = objWorksheet.Cells(2,5)
intVarTag_1 = objRuntime.SetValue(Var,Value)
objWorksheet.Cells(2,8) = intVarTag_1

End Sub
'-----

```

Result

As soon as you call "ReadTagValue_Click" macro by clicking the button "Read-value", the specified intVarTag_1 tag is obtained from the HMI device using the specified device address and displayed in the cell (1,1).

As soon as you call Macro "WriteTagValue" by clicking the "Write value" button, the tag name is read from the cell (2,3), and the tag value is transferred from cell (2,5) to the HMI device.

See also

Configuration in WinCC (Page 54)

Index

A

- Acknowledgement
 - Audit Trail, 34
- Alarm report
 - Configuring, 23
- Audit
 - Configuration, 46
 - Enhancements in the ES, 9
 - Forcing, 30
 - Functional scope, 8
 - Logging concept, 9
 - Scope of logging, 10
 - Screen object, 46
 - Supported HMI devices, 45
- Audit Trail
 - Acknowledgement, 34
 - Checksum, 29
 - Comments, 34
 - CSV file, 28
 - Editor, 11
 - Effects in runtime, 31
 - Electronic signature, 34
 - File format, 28
 - Log tag value change, 32
 - Logging recipe data changes, 34
 - Logging system functions, 40
 - Logging user actions, 37
 - Memory medium, 29
 - Printing, 20
 - Protection against change, 30
 - Reporting, 20
 - Storage location, 29
 - Troubleshooting, 29
- Audit trail editor, 11

C

- Certificate, 121
 - Importing on HTTP client, 121
 - Installing on devices, 121
 - Installing under Windows XP, 121
- Checksum, 30
 - Audit Trail, 29
 - Log, 29

- Comments
 - Audit Trail, 34
 - Electronic signature, 34
- CSV file
 - Audit Trail, 28

D

- Distributed operator stations
 - Configure SmartClient, 95
 - Configure SmartServer, 95
 - configuring, 95

E

- Effects in Runtime
 - Audit Trail,
 - Recipe data change, 36
 - Value changes to GMP-relevant tags, 34
- Electronic signature, 8
- E-Mail
 - Setting at the HMI device, 57
- E-mail notification, 99
 - Configuring, 101
 - Setting up the trigger, 100
- Event
 - Free space critically low, 19
 - Low free storage space, 19

F

- FDA, 7
- File format
 - Audit Trail, 28
- Forcing
 - Audit, 30
- Free space critically low, 19

G

- GetValue, 125
- GMP, 7
- GMP settings, 32, 36
- GMP-relevant tag, 32
- Good Manufacturing Process, 7

H

- Hardware acceleration
 - SmartServer, 81
- HTML page
 - Displaying data type DATETIME, 104
- HTTP client, 119
 - Configure HTTP-Connection, 119
 - Configuring tags, 120
 - Configuring the SIMATIC HMI HTTP protocol, 119
 - Importing certificates, 121
- HTTP server
 - Configure WinCC-Project, 117
 - Setting at the HMI device, 118

I

- Input area plan
 - SmartClient, 57
 - SmartServer, 57
 - SmartService, 57

L

- Log tag value change
 - Audit Trail, 32
- Logging
 - Change to a recipe data record in Audit Trail, 34
 - System functions in Audit Trail, 40
 - Tag value change in Audit Trail, 32
 - User actions in audit trail, 37
- Logging concept
 - Audit, 9
- Logging recipe data changes
 - Audit Trail, 34
- Logging system functions
 - Audit Trail, 40
- Logging user actions
 - Audit Trail, 37
- Low free storage space, 19

M

- Memory medium
 - Audit Trail, 29
- Monitoring mode, 69

N

- NotifyUserAction, 39

P

- Password
 - SmartServer, 81
- Permitted data type
 - SIMATIC HMI HTTP Protocol, 116
- Print alarm
 - Configuring print parameters, 23
- Printing
 - Audit Trail, 20

R

- Recipe
 - GMP settings, 36
- Recipe data record change
 - Effects in Runtime, 36
- Remote control
 - By means of Internet Explorer, 88
 - By means of SmartClient application, 89
 - Configure SmartClient, 75
 - Configure SmartServer, 70
 - Devices with keys,
 - Direct keys, 92
 - Monitoring mode, 69
 - Session Management, 69
 - Smart Options, 87
 - SmartClient display, 91
- Remote monitoring
 - Smart Options, 87
- Reporting
 - Audit Trail, 20
- Runtime settings, 54

S

- Secure communication
 - configuration on the WebClient, 86
 - Sm@rtServer and WebClient, 82
- Service-pages, 105
 - Create own, 112
 - Display, 108
 - remote control, 108
 - Transfer, 113

- Session Management, 69
 - Setting, 70
- Set the services
 - SmartClient, 54
 - SmartServer, 54
- Setting at the HMI device
 - E-Mail, 57
 - HTTP server, 118
- Setting at the HMI-device
 - HTTP server, 59
 - SmartServer, 60
 - Web authorization, 59
 - Web server, 59
- SetValue, 125
- signature
 - electronic, 8
- SIMATIC HMI HTTP Protocol
 - Configuring HTTP clients, 119
 - Configuring the connection, 119
 - Permitted data type, 116
- Smart Options, 87
 - HMI devices suitable for use, 53
 - Remote control, 87
 - Remote control by means of Internet Explorer, 88
 - Remote monitoring, 87
- SmartAccess
 - Distributed operator stations, 95
 - Editing tag values in MS Excel, 125
- SmartClient
 - Monitoring mode, 75
 - Password input, 92
 - SmartClient display, 75
- SmartClient display, 91
- SmartServer
 - As a service, 73
 - Control mode, 70
 - Forced access, 73
 - Hardware acceleration, 81
 - Local operator control, 73
 - Monitoring mode, 70
 - Password, 81
 - Password input, 92
 - Setting at the HMI-device, 60
- SmartService
 - E-mail notification, 99
 - Input area plan, 57
 - Remote control by means of the SmartClient application, 89
- SOAP
 - Access from Excel, 124
 - GetValue, 125
 - SetValue, 125
 - Windows CE, 125
- Storage location
 - Audit Trail, 29
- System function
 - NotifyUserAction, 39
- T**
- Tag
 - GMP settings, 32
 - GMP-relevant tag, 32
- V**
- Value changes to GMP-relevant tags
 - Effects in Runtime, 34
- W**
- Web authorization, 69
 - Setting at the HMI-device, 59
- Web server, 103
 - Configure WinCC project, 107
 - Service-pages, 105
 - User administration, 68
 - Web authorization, 68, 69
- WebClient login page, 86
- WinCC Runtime Advanced Internet, 56

