SIEMENS

SIMATIC

WinCC
WinCC Professional V13 SP2 – Options

System Manual

WinCC Audit (Panels, Comfort Panels, RT Advanced) 1

WinCC DataMonitor (RT Professional) 2

WinCC Redundancy 3

WinCC Sm@rtServer (Panels, Comfort Panels, RT Advanced) 4

WinCC Server / WinCC Client (RT Professional) 5

WinCC WebNavigator (RT Professional) 6

Online help printout

03/2017
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.

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: Online help printout
℗ 05/2017 Subject to change

Copyright © Siemens AG 2017.
All rights reserved

Table of contents

1 WinCC Audit (Panels, Comfort Panels, RT Advanced) 11

1.1 Basics (Panels, Comfort Panels, RT Advanced) 11
1.1.1 GMP compliance (Panels, Comfort Panels, RT Advanced) 11
1.1.2 GMP-compliant configuration (Panels, Comfort Panels, RT Advanced) 11
1.1.3 Audit option (Panels, Comfort Panels, RT Advanced) 12
1.1.4 Scope of logging (Panels, Comfort Panels, RT Advanced) 13

1.2 Enabling GMP compliant configuration (Panels, Comfort Panels, RT Advanced) 15

1.3 Using the Audit trail (Panels, Comfort Panels, RT Advanced) 16
1.3.1 Audit Trail (Panels, Comfort Panels, RT Advanced) 16
1.3.2 Creating an audit trail (Panels, Comfort Panels, RT Advanced) 18
1.3.3 Parameters for the audit trail (Panels, Comfort Panels, RT Advanced) 20
1.3.4 Setting the audit trail language (Panels, Comfort Panels, RT Advanced) 23
1.3.5 Low free storage space (Panels, Comfort Panels, RT Advanced) 24
1.3.5.1 Low free storage space (Panels, Comfort Panels, RT Advanced) 24
1.3.5.2 Free space critically low (Panels, Comfort Panels, RT Advanced) 24
1.3.5.3 Configuring the "Low free storage space" event (Panels, Comfort Panels, RT Advanced) 25
1.3.6 Logging the audit trail (Panels, Comfort Panels, RT Advanced) 25
1.3.6.1 Reporting an audit trail (Panels, Comfort Panels, RT Advanced) 25
1.3.6.2 Audit Trail reporting (Panels, Comfort Panels, RT Advanced) 26
1.3.6.3 Parameters for the audit trail report (Panels, Comfort Panels, RT Advanced) 27
1.3.6.4 Printing out an audit trail report (Panels, Comfort Panels, RT Advanced) 30
1.3.7 Evaluating an audit trail (Panels, Comfort Panels, RT Advanced) 31
1.3.7.1 Evaluating audit trails (Panels, Comfort Panels, RT Advanced) 31
1.3.7.2 Evaluating Audit Trails in AuditViewer (Panels, Comfort Panels, RT Advanced) 32
1.3.7.3 Evaluating Audit Trails with DOS program (Panels, Comfort Panels, RT Advanced) 33
1.3.8 Audit trail logging concept (Panels, Comfort Panels, RT Advanced) 33
1.3.8.1 Format (Panels, Comfort Panels, RT Advanced) 33
1.3.8.2 Storage location and medium (Panels, Comfort Panels, RT Advanced) 35
1.3.8.3 Protection mechanisms (Panels, Comfort Panels, RT Advanced) 36
1.3.8.4 WinCC upgrade (Panels, Comfort Panels, RT Advanced) 36
1.3.8.5 Audit trail behavior in runtime (Panels, Comfort Panels, RT Advanced) 37

1.4 Configuring audit functions (Panels, Comfort Panels, RT Advanced) 37
1.4.1 Logging tag value changes (Panels, Comfort Panels, RT Advanced) 37
1.4.1.1 Tag value change (Panels, Comfort Panels, RT Advanced) 37
1.4.1.2 Logging tag value changes (Panels, Comfort Panels, RT Advanced) 38
1.4.1.3 Effects of tag change (Panels, Comfort Panels, RT Advanced) 40
1.4.2 Logging recipe data record changes (Panels, Comfort Panels, RT Advanced) 40
1.4.2.1 Recipe data changes (Panels, Comfort Panels, RT Advanced) 40
1.4.2.2 Logging recipe data changes (Panels, Comfort Panels, RT Advanced) 41
1.4.2.3 Effects of recipe data change (Panels, Comfort Panels, RT Advanced) 42
1.4.3 Logging user actions (Panels, Comfort Panels, RT Advanced) 43
1.4.3.1 User actions with GMP-compliant configuration (Panels, Comfort Panels, RT Advanced) 43
1.4.3.2 Logging modes (Panels, Comfort Panels, RT Advanced) 44

1.4.3.3 Configuring the "NotifyUserAction" system function (Panels, Comfort Panels, RT Advanced)....45
1.4.3.4 GMP-compliant user administration (Panels, Comfort Panels, RT Advanced)....46
1.4.4 Logging system functions (Panels, Comfort Panels, RT Advanced)....46

1.5 Performance features of GMP-compliant configuration (Panels, Comfort Panels, RT Advanced)....51
1.5.1 Supported HMI devices (Panels, Comfort Panels, RT Advanced)....51
1.5.2 Restrictions (Panels, Comfort Panels, RT Advanced)....51

2 WinCC DataMonitor (RT Professional)....53

2.1 The basics (RT Professional)....53
2.1.1 DataMonitor (RT Professional)....53
2.1.2 WinCCViewerRT (RT Professional)....54
2.1.3 WebCenter (RT Professional)....54
2.1.4 Trends and Alarms (RT Professional)....57
2.1.5 Excel workbooks (RT Professional)....57
2.1.6 Reports (RT Professional)....58
2.1.7 Access rights (RT Professional)....59
2.1.8 Checking certificates (RT Professional)....59

2.2 Installing DataMonitor (RT Professional)....60
2.2.1 Licensing (RT Professional)....60
2.2.2 Installation of the DataMonitor server (RT Professional)....62
2.2.2.1 Installing DataMonitor server (RT Professional)....62
2.2.2.2 Installing the Internet Information Service (RT Professional)....62
2.2.3 Installation of the DataMonitor client (RT Professional)....64
2.2.3.1 Installation of the DataMonitor client (RT Professional)....64
2.2.3.2 Configuring security settings in Internet Explorer (RT Professional)....65
2.2.3.3 Installing with the installation disk (RT Professional)....67
2.2.3.4 Installing via the Intranet/Internet (RT Professional)....68
2.2.3.5 User rights, user groups and optional installation possibilities (RT Professional)....69

2.3 Configuring the DataMonitor system (RT Professional)....72
2.3.1 Configuring a WinCC project (RT Professional)....73
2.3.1.1 Configuring WinCC screens for Web access (RT Professional)....73
2.3.1.2 WinCC screens as a gadget (RT Professional)....74
2.3.1.3 Configuring runtime settings (DataMonitor) (RT Professional)....75
2.3.1.4 Defining users in WinCC (RT Professional)....77
2.3.2 Transferring a WinCC project (RT Professional)....79
2.3.3 Configuring the DataMonitor Server (RT Professional)....79
2.3.3.1 Setting up the DataMonitor Web page (RT Professional)....79
2.3.3.2 Setting up a firewall (RT Professional)....81
2.3.3.3 Defining users in Windows (RT Professional)....81
2.3.4 Starting the DataMonitor on the DataMonitor client (RT Professional)....83
2.3.4.1 Configuring security settings in Internet Explorer (RT Professional)....83
2.3.4.2 Starting the DataMonitor startup page on the DataMonitor client (RT Professional)....84
2.3.4.3 General Operations of the DataMonitor Client (RT Professional)....86

2.4 Working with WinCCViewerRT (RT Professional)....87
2.4.1 Setting up WinCCViewerRT (RT Professional)....87
2.4.2 Display screens (RT Professional)....89

2.5 Working with the WebCenter (RT Professional)....90
2.5.1 Administration (RT Professional)....90

2.5.1.1 User Groups and Directories (RT Professional)....90
2.5.1.2 Creating Directories (RT Professional)....93
2.5.1.3 Assigning Access Rights (RT Professional)....94
2.5.1.4 Establish a connection to the winCC data (RT Professional)....95
2.5.2 Creating static process screens for the Web Center (RT Professional)....103
2.5.3 Create a layout template for WebCenter pages (RT Professional)....106
2.5.4 Create a WebCenter page (RT Professional)....109
2.5.5 Insert Web parts into the WebCenter page (RT Professional)....112
2.5.6 Configure Web parts within WebCenter pages (RT Professional)....115
2.5.7 Deleting WebCenter Pages and Layout Templates (RT Professional)....117
2.5.8 Exporting and importing WebCenter pages (RT Professional)....119

2.6 Working with Trends and Alarms (RT Professional)....119
2.6.1 Displaying process values in a table (RT Professional)....119
2.6.2 Displaying process values in a diagram (RT Professional)....121
2.6.3 Displaying messages in the alarm table (RT Professional)....123
2.6.4 Alarm Log Column Names (RT Professional)....125
2.6.5 Displaying the hit list of messages (RT Professional)....127
2.6.6 Displaying statistics function for process values (RT Professional)....128

2.7 Working with Excel Workbooks (RT Professional)....130
2.7.1 Configuring an Excel workbook (RT Professional)....130
2.7.1.1 Importing data from a WinCC project (RT Professional)....130
2.7.1.2 Importing data from an xml file (RT Professional)....131
2.7.1.3 Configuring the display of tag values (RT Professional)....132
2.7.1.4 Configuring the display of logging tags (RT Professional)....134
2.7.1.5 Configuring the display of alarms (RT Professional)....135
2.7.1.6 Publishing an Excel workbook (RT Professional)....137
2.7.2 Displaying process data in an Excel Workbook online (RT Professional)....138
2.7.3 Alarm Attributes (RT Professional)....140
2.7.4 VBA Functions of the Excel Workbook (RT Professional)....141

2.8 Working with reports (RT Professional)....141
2.8.1 Preparing an Excel Workbook as a Template (RT Professional)....141
2.8.2 Making an Excel workbook available as a report tool (RT Professional)....142
2.8.3 Making Settings for Reports (RT Professional)....143
2.8.4 Displaying a report with an Excel Workbook (RT Professional)....145
2.8.5 Creating a report with a print job (RT Professional)....148

3 WinCC Redundancy....151

3.1 Basics....151
3.1.1 Overview....151
3.1.2 How Redundancy Works....152
3.1.3 Standard server and preferred server....155
3.1.4 HMI system without redundancy....155
3.1.5 HMI system with redundancy....156
3.1.6 Requirements....157
3.1.7 Setting up the servers....158
3.1.7.1 Structure of a redundant project....158
3.1.7.2 Configuring an Identical Function....159
3.1.7.3 Redundant recipe data....159
3.1.7.4 Online Synchronized Messages....160

3.2 Configuring the redundant system....160

3.2.1 Overview of configuration steps....160
3.2.2 Creating a project....161
3.2.2.1 Creating a server....161
3.2.2.2 Creating clients....162
3.2.2.3 Control....162
3.2.3 Configuring redundant servers....162
3.2.3.1 Configuring master servers....162
3.2.3.2 Configuring the standby server....164
3.2.3.3 Configuring server reaction....164
3.2.4 Configuring clients....166
3.2.5 Loading the project to a device....167
3.2.6 Compiling a project....168

3.3 Migrating a redundant project....169
3.3.1 Migrating a redundant project....169

3.4 System behavior in the event of a fault....170
3.4.1 Failure scenarios....170
3.4.2 Server not in Runtime....171
3.4.3 Connection Fault to Partner Server....172
3.4.4 Faulty network connection to client....174
3.4.5 Faulty Process Connection....174
3.4.6 Software Error....175
3.4.7 Changing the client in case of a process coupling error....176

3.5 Reference....180
3.5.1 System messages WinCC Redundancy....180

4 WinCC Sm@rtServer (Panels, Comfort Panels, RT Advanced)....183

4.1 Basics (Panels, Comfort Panels, RT Advanced)....183
4.1.1 Sm@rt Options (Panels, Comfort Panels, RT Advanced)....183
4.1.2 Application scenarios (Panels, Comfort Panels, RT Advanced)....185
4.1.3 HMI devices suitable for use (Panels, Comfort Panels, RT Advanced)....187
4.1.4 Settings for Sm@rt Options (Panels, Comfort Panels, RT Advanced)....188
4.1.4.1 Configuration in WinCC (Panels, Comfort Panels, RT Advanced)....188
4.1.4.2 Configurations on the HMI device (Panels, Comfort Panels, RT Advanced)....190
4.1.5 Settings for remote control (Panels, Comfort Panels, RT Advanced)....203
4.1.5.1 Session management for remote control (Panels, Comfort Panels, RT Advanced)....203
4.1.5.2 Configuring Sm@rtServer for remote control (Panels, Comfort Panels, RT Advanced)....204
4.1.5.3 Configure Sm@rtClient for remote control (Panels, Comfort Panels, RT Advanced)....208
4.1.5.4 Sm@rtClient-Application (Panels, Comfort Panels, RT Advanced)....209
4.1.5.5 Remote control of key devices (Panels, Comfort Panels, RT Advanced)....213
4.1.6 Use and restrictions of Sm@rt Options (Panels, Comfort Panels, RT Advanced)....214

4.2 Remote control via Sm@rtServer (Panels, Comfort Panels, RT Advanced)....216
4.2.1 Types of the remote control (Panels, Comfort Panels, RT Advanced)....216
4.2.1.1 Remote control and remote monitoring by means of Sm@rtServer (Panels, Comfort Panels, RT Advanced)....216
4.2.1.2 Remote control by means of Internet Explorer (Panels, Comfort Panels, RT Advanced)....217
4.2.1.3 Remote control by means of the Sm@rtClient application (Panels, Comfort Panels, RT Advanced)....218
4.2.1.4 Remote control via the Sm@rtClient display during runtime (Panels, Comfort Panels, RT Advanced)....220
4.2.2 Distributed operator stations (Panels, Comfort Panels, RT Advanced)....222

4.2.2.1 Configuration (Panels, Comfort Panels, RT Advanced)....222
4.2.2.2 Configure distributed operator stations (Panels, Comfort Panels, RT Advanced)....224
4.2.2.3 Configure Sm@rtServer (Panels, Comfort Panels, RT Advanced)....224
4.2.2.4 Project Sm@rtClient (Panels, Comfort Panels, RT Advanced)....226

4.3 E-mail notification from runtime (Panels, Comfort Panels, RT Advanced)....228
4.3.1 Process flow (Panels, Comfort Panels, RT Advanced)....228
4.3.2 Specify trigger for E-Mailing (Panels, Comfort Panels, RT Advanced)....229
4.3.3 Configure secure e-mail notification from Runtime (Panels, Comfort Panels, RT Advanced)....230

4.4 Display integrated Service-Pages (Panels, Comfort Panels, RT Advanced)....232
4.4.1 Integrated Webserver (Panels, Comfort Panels, RT Advanced)....232
4.4.2 Service-pages of the web server (Panels, Comfort Panels, RT Advanced)....234
4.4.3 Installing the client and server certificates for SSL (Panels, Comfort Panels, RT Advanced)....235
4.4.4 Configure access to service-pages (Panels, Comfort Panels, RT Advanced)....236
4.4.4.1 Configure integrated web server (Panels, Comfort Panels, RT Advanced)....236
4.4.4.2 Display and remote-control Service-Pages (Panels, Comfort Panels, RT Advanced)....237
4.4.5 Create own Service-pages (Panels, Comfort Panels, RT Advanced)....239
4.4.5.1 Basics (Panels, Comfort Panels, RT Advanced)....239
4.4.5.2 Create service-page for displaying process values (Panels, Comfort Panels, RT Advanced)....241
4.4.5.3 Transfer Service-pages (Panels, Comfort Panels, RT Advanced)....242

4.5 Access via SIMATIC HMI HTTP Protocol (Panels, Comfort Panels, RT Advanced)....244
4.5.1 Configuration (Panels, Comfort Panels, RT Advanced)....244
4.5.2 Configure access via SIMATIC HTTP Protocol (Panels, Comfort Panels, RT Advanced)....245
4.5.3 Permissible data types (SIMATIC HMI HTTP protocol) (Panels, Comfort Panels, RT Advanced)....245
4.5.4 Configure HTTP server (Panels, Comfort Panels, RT Advanced)....246
4.5.4.1 Configure WinCC-Project (Panels, Comfort Panels, RT Advanced)....246
4.5.4.2 Setting WinCC Runtime Advanced Internet (Panels, Comfort Panels, RT Advanced)....247
4.5.5 Configuring HTTP clients (Panels, Comfort Panels, RT Advanced)....248
4.5.5.1 Configuring HTTP connections in the client (Panels, Comfort Panels, RT Advanced)....248
4.5.5.2 Configure the HTTP-Client tags (Panels, Comfort Panels, RT Advanced)....249
4.5.6 Commissioning an HTTP- connection (Panels, Comfort Panels, RT Advanced)....250

4.6 Connection to the Office-world (Panels, Comfort Panels, RT Advanced)....253
4.6.1 Configuration (Panels, Comfort Panels, RT Advanced)....253
4.6.2 Create VBA-Marko in MS Excel (Panels, Comfort Panels, RT Advanced)....254

5 WinCC Server / WinCC Client (RT Professional)....257

5.1 Guide to client server systems (RT Professional)....257

5.2 Clients and servers (RT Professional)....257

5.3 Plant configurations (RT Professional)....258
5.3.1 Single-user system (RT Professional)....258
5.3.2 Multi-user system (RT Professional)....259

5.4 Configuring a multiple-station system (RT Professional)....261
5.4.1 Requirement (RT Professional)....261
5.4.2 Configuration guidelines (RT Professional)....262
5.4.3 Configuring the server (RT Professional)....262
5.4.4 Configuring the operator authorizations (RT Professional)....263

5.4.5 Configuring clients (RT Professional)....264
5.4.6 Downloading the project to the server (RT Professional)....267

5.5 Characteristics in runtime (RT Professional)....267
5.5.1 Characteristics (overview) (RT Professional)....267
5.5.2 Reaction to system errors (RT Professional)....268
5.5.3 Delta compile in runtime (RT Professional)....268
5.5.4 Characteristics of the server (RT Professional)....269
5.5.4.1 Starting servers (RT Professional)....269
5.5.4.2 Server shutdown (RT Professional)....270
5.5.5 Characteristics of the client (RT Professional)....270
5.5.5.1 Starting the Client (RT Professional)....270
5.5.5.2 Shutting down a client (RT Professional)....270

5.6 WinCC RT Start (RT Professional)....271
5.6.1 Overview of WinCCStart (RT Professional)....271
5.6.2 Activating and deactivating projects on the WinCC server (RT Professional)....271
5.6.3 Activating and deactivating a project from the WinCC client (RT Professional)....273
5.6.4 Enabling time synchronization on the client (Professional) (RT Professional)....274
5.6.5 Additional settings: Autostart and language (RT Professional)....276
5.6.6 Displaying products and components (RT Professional)....277

5.7 SIMATIC Shell (RT Professional)....279
5.7.1 Remote Configuration (RT Professional)....279
5.7.2 Accessing a computer outside a subnet (RT Professional)....280
5.7.3 Activating a project (RT Professional)....281
5.7.4 Deactivating a project (RT Professional)....282

6 WinCC WebNavigator (RT Professional)....285

6.1 Unsupported functions (RT Professional)....285

6.2 The basics (RT Professional)....286
6.2.1 Function Overview (RT Professional)....286
6.2.2 Web Navigator Server on the WinCC server (RT Professional)....287
6.2.3 WebNavigator diagnostics client (RT Professional)....288
6.2.4 WinCCViewerRT (RT Professional)....289
6.2.5 Terminal services and Web Navigator (RT Professional)....290

6.3 Installing WebNavigator (RT Professional)....291
6.3.1 Software and hardware requirements (RT Professional)....291
6.3.2 Licensing (RT Professional)....293
6.3.3 Requirements for the Use of Terminal Services (RT Professional)....294
6.3.4 Installation of WebNavigator server (RT Professional)....295
6.3.4.1 Overview (RT Professional)....295
6.3.4.2 Installing Internet Information Services (IIS) (RT Professional)....296
6.3.4.3 Installing the WebNavigator Server (RT Professional)....297
6.3.5 Installation of WebNavigator client (RT Professional)....299
6.3.5.1 Installing the WebNavigator Client (RT Professional)....299
6.3.5.2 User rights, user groups and optional installation possibilities (RT Professional)....300
6.3.5.3 Internet Explorer Settings (RT Professional)....302
6.3.5.4 Installation from the DVD (RT Professional)....305
6.3.5.5 Installation via the Intranet/Internet (RT Professional)....306
6.3.6 Installing the Web Diagnostics Client (RT Professional)....307

6.4 Configuring the Web Navigator system (RT Professional)....309

6.4.1 Overview of configuration steps (RT Professional)....309
6.4.2 Configuring a WinCC project (RT Professional)....310
6.4.2.1 Configuring WinCC screens for Web access (RT Professional)....310
6.4.2.2 WinCC screens as a gadget (RT Professional)....310
6.4.2.3 Configuring runtime settings (WebNavigator) (RT Professional)....312
6.4.2.4 Managing users for the Web Navigator Client (RT Professional)....313
6.4.2.5 Limitations (RT Professional)....315
6.4.3 Transferring a WinCC project (RT Professional)....316
6.4.4 Configuring the Web Navigator Server (RT Professional)....317
6.4.4.1 Setting up the Web Navigator Web site (RT Professional)....317
6.4.4.2 Setting up a firewall (RT Professional)....323
6.4.4.3 Checking the Activated Web Site (Web) (RT Professional)....324
6.5 Operating a WinCC project (RT Professional)....325
6.5.1 Operating projects using WinCCViewerRT (RT Professional)....325
6.5.1.1 Setting up WinCCViewerRT (RT Professional)....325
6.5.1.2 Operating a WinCC project (RT Professional)....327
6.5.2 Operating projects in Internet Explorer (RT Professional)....328
6.5.2.1 Operating a WinCC project (RT Professional)....328
6.5.2.2 Working with the Web navigation interface (RT Professional)....329
6.5.2.3 Diagnosis of the Connections with "Status.html" (RT Professional)....331
6.5.3 Use the "Hardcopy" function (RT Professional)....333
6.6 Setting up terminal services for Web Navigator (RT Professional)....335
6.6.1 Communication Using Terminal Services (RT Professional)....335
6.6.2 Activating terminal services on the Windows server (RT Professional)....335
6.6.3 Setting Up a User with Access Rights to the Terminal Server (RT Professional)....336
6.6.4 Starting the Terminal Server Application on the Terminal Client (RT Professional)....337
6.7 Troubleshooting (RT Professional)....337
Index....339

WinCC Audit (Panels, Comfort Panels, RT Advanced) 1

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 industrial sectors such as the pharmaceuticals industry, the food and beverage industry. and in the related mechanical engineering sector.

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 use 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 acknowledgement 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 Enabling GMP compliant configuration (Panels, Comfort Panels, RT Advanced)

Introduction

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

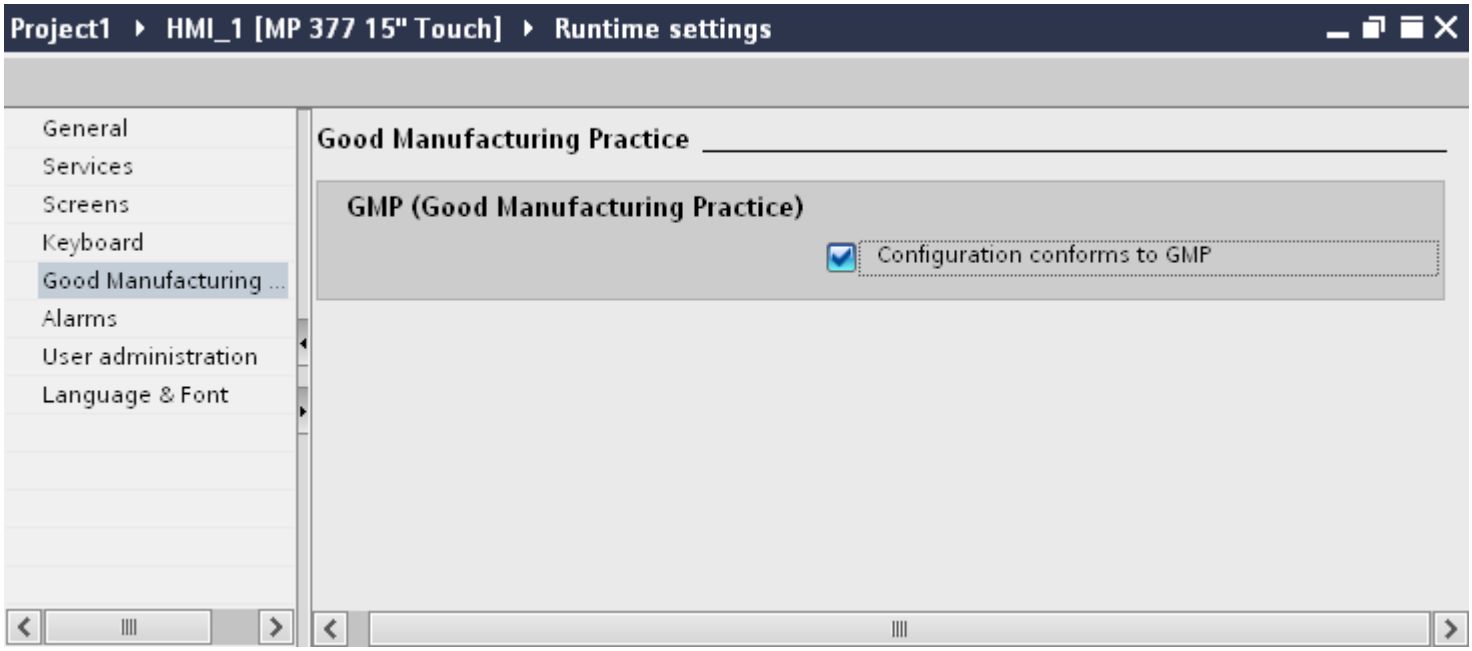
Requirements

- 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

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

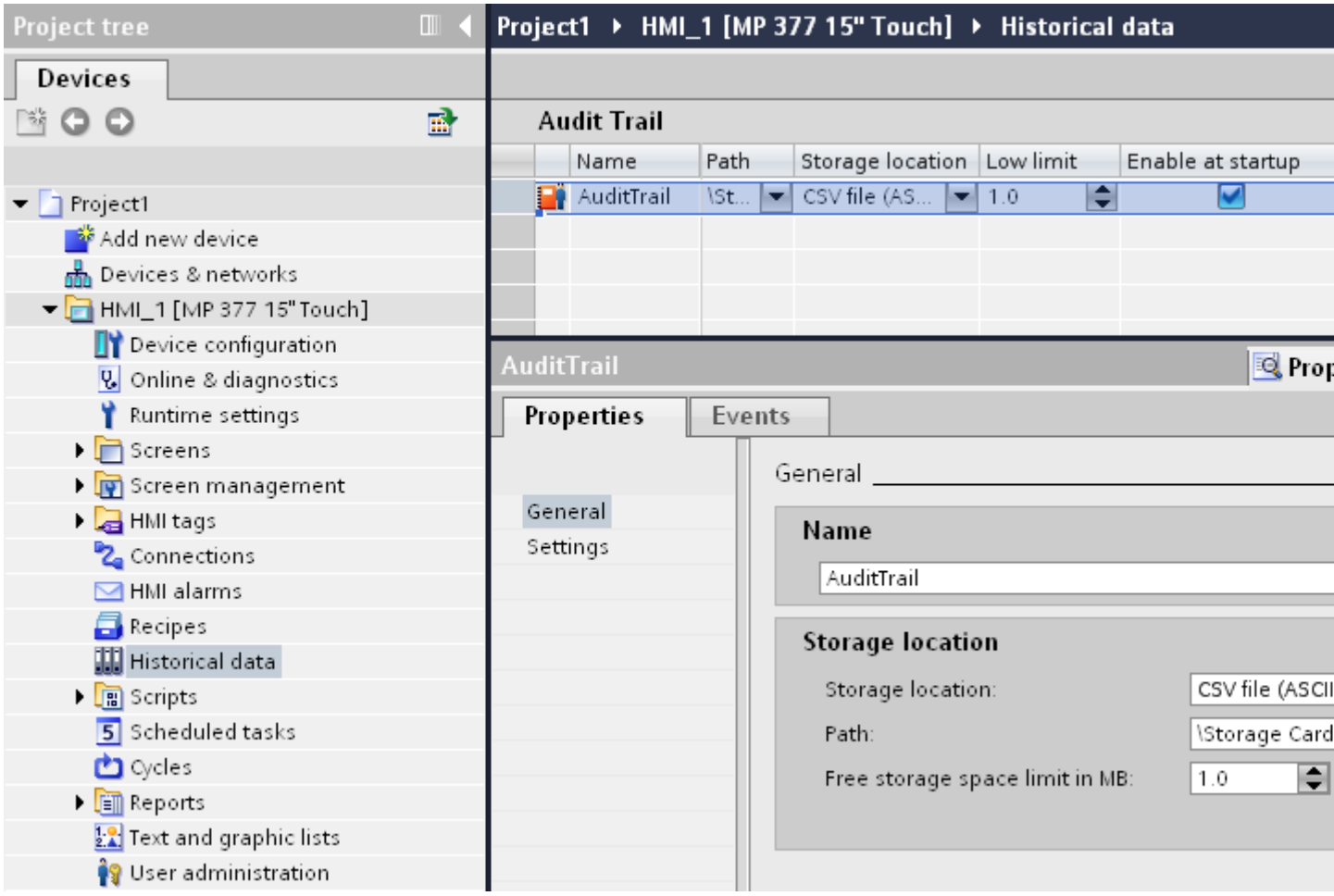
1.3.1 Audit Trail (Panels, Comfort Panels, RT Advanced)

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.

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

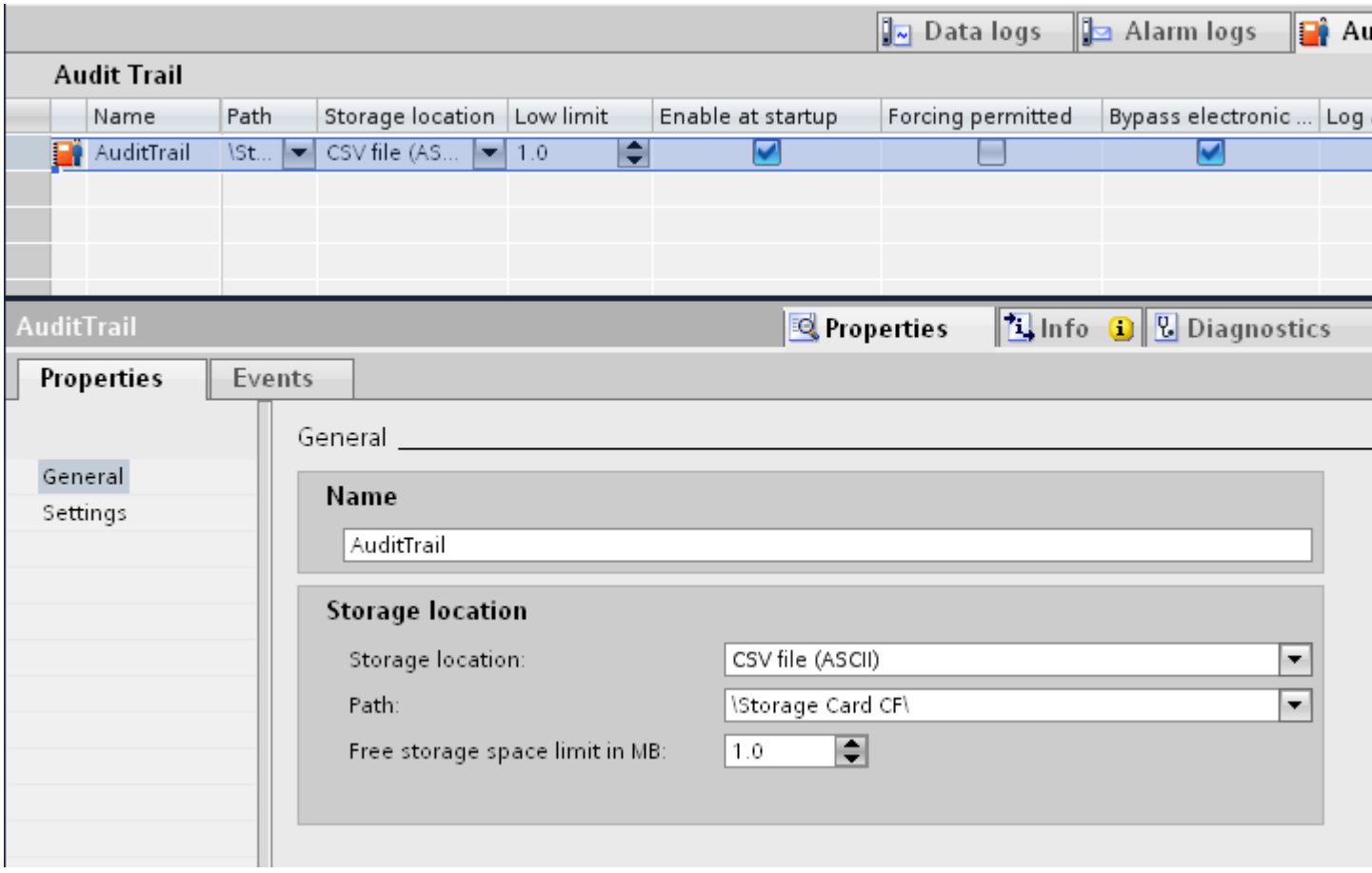
Requirements

"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.

For more information refer to chapter: Low free storage space (Page 24)

Result

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

1.3.3 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.

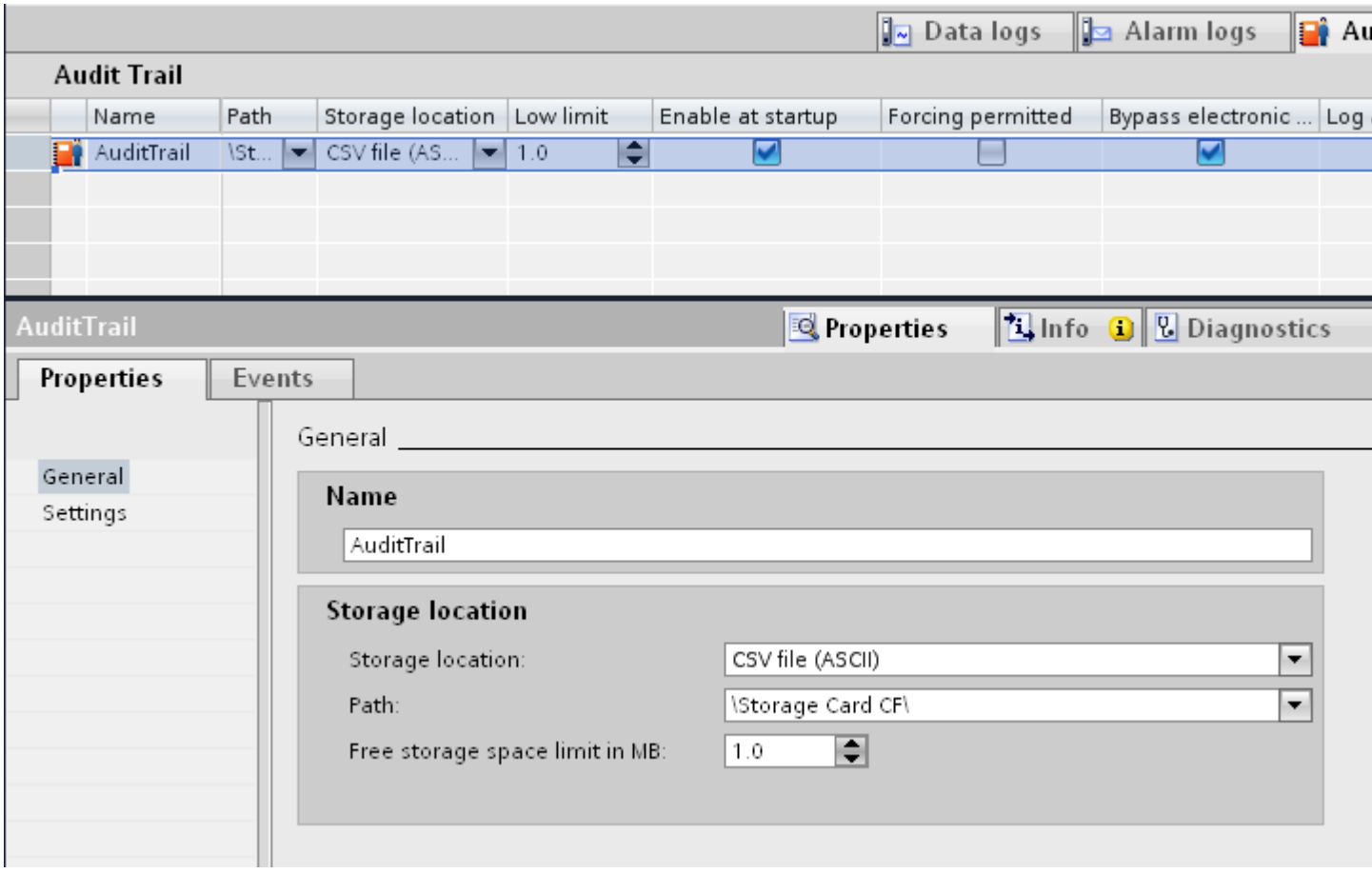
Only one Audit Trail can be created per HMI device.

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)

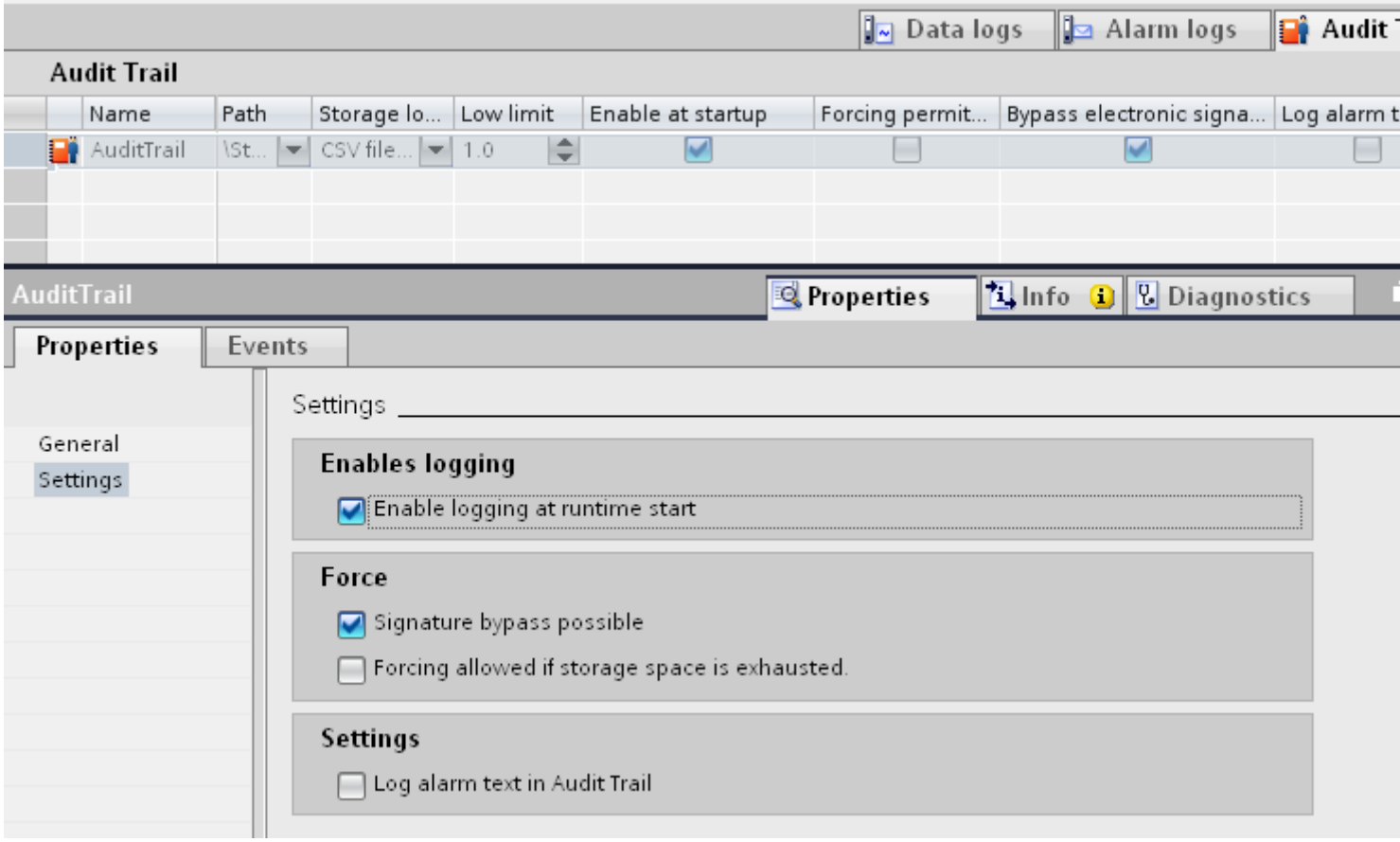
  Note

  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:
  Setting the audit trail language (Page 23)

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

Introduction

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

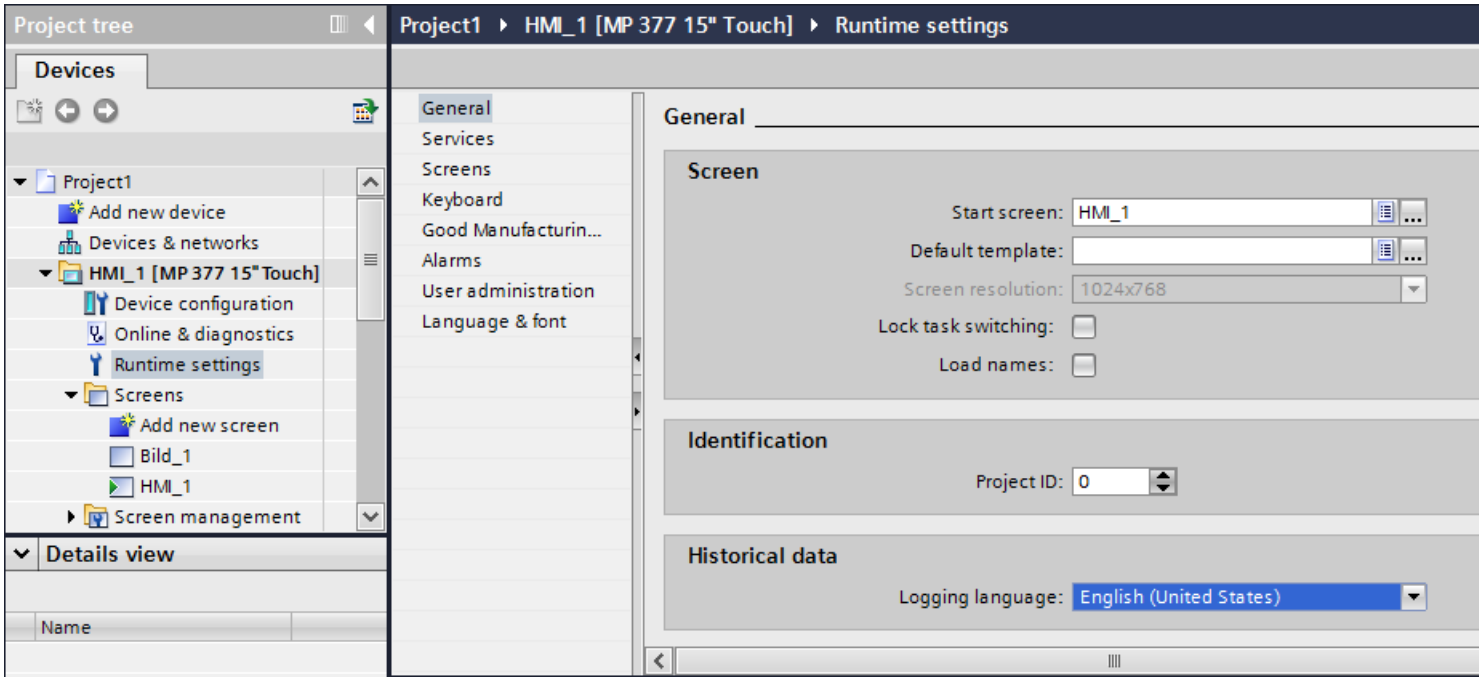
Procedure

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.



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

1.3.5.1 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.

1.3.5.2 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.

1.3.5.3 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.

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

1.3.6.1 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 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.

1.3.6.2 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.

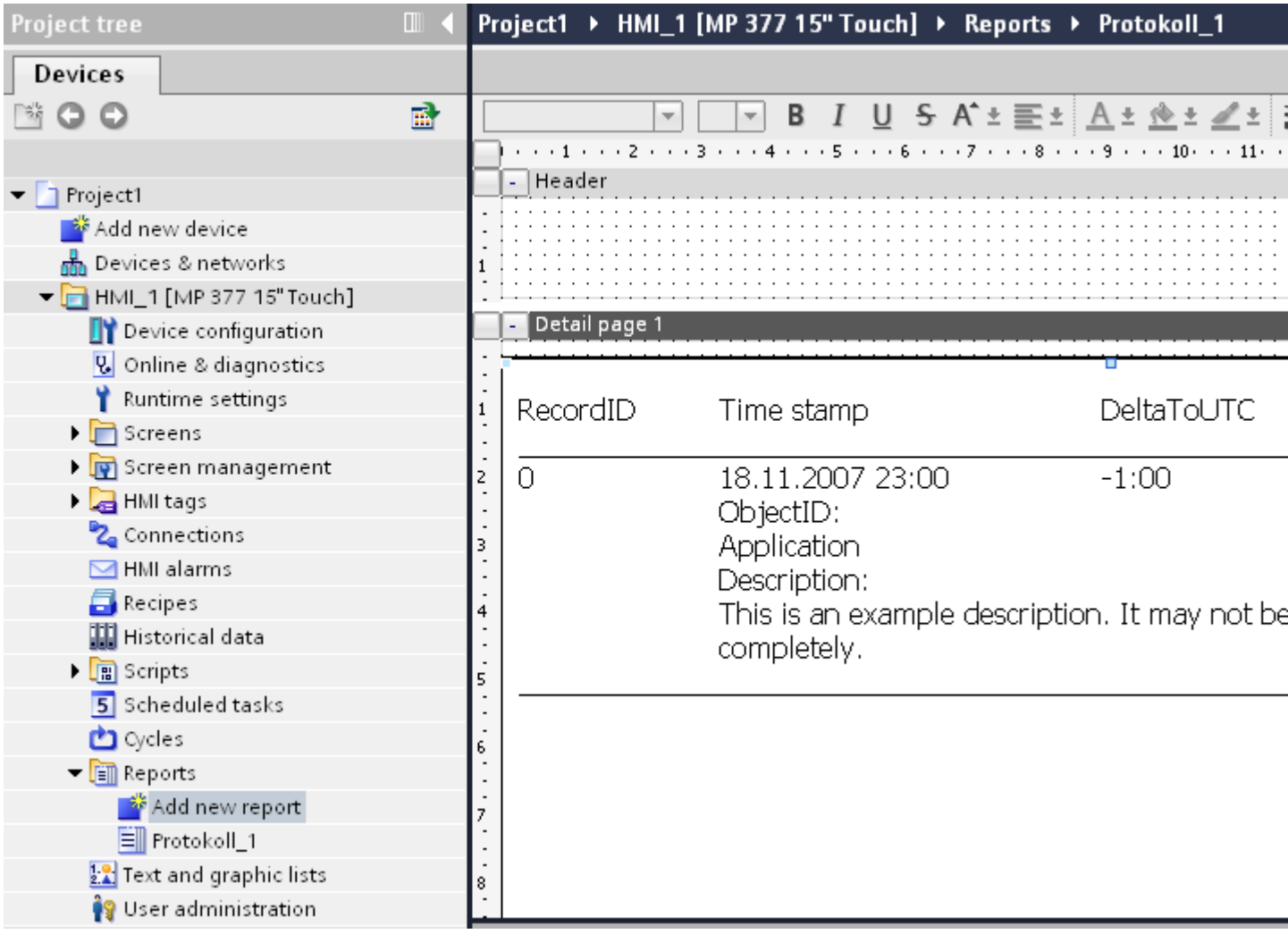
Once the printout is started in runtime, all entries currently contained in the Audit Trail are printed out.

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.

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

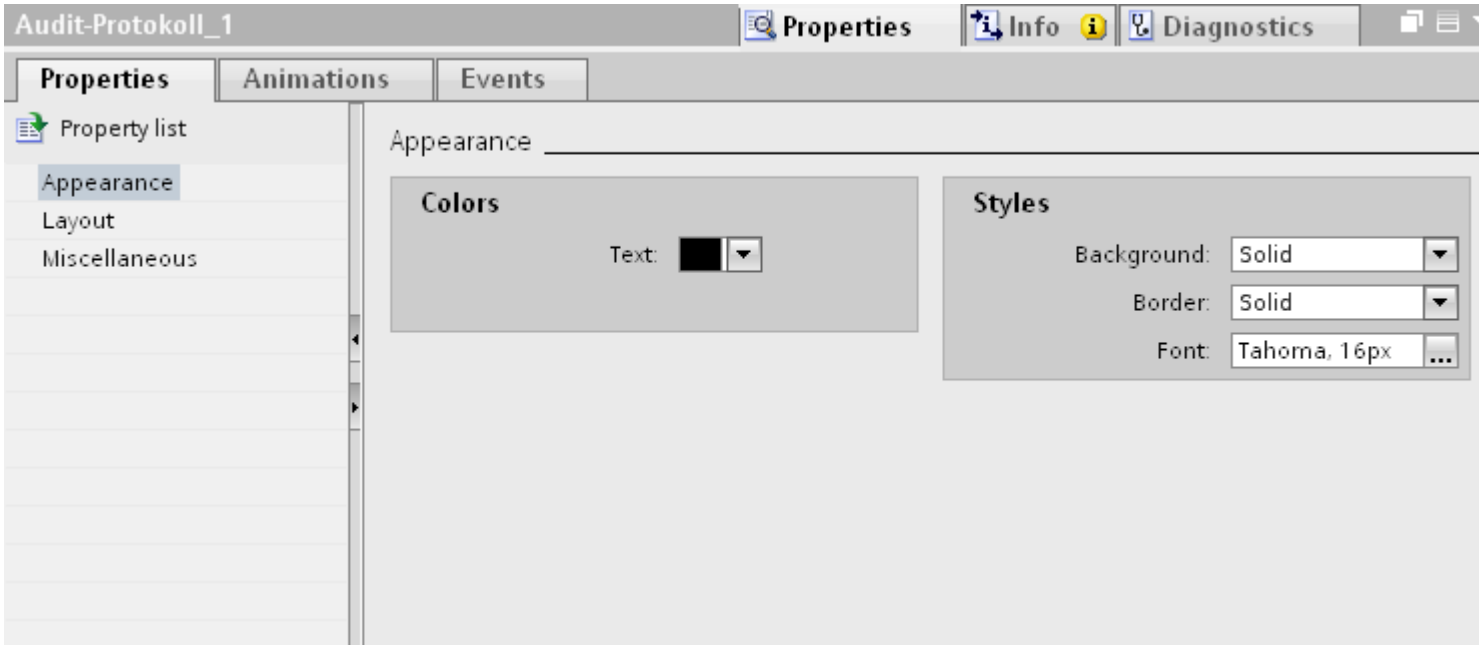
Introduction

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".



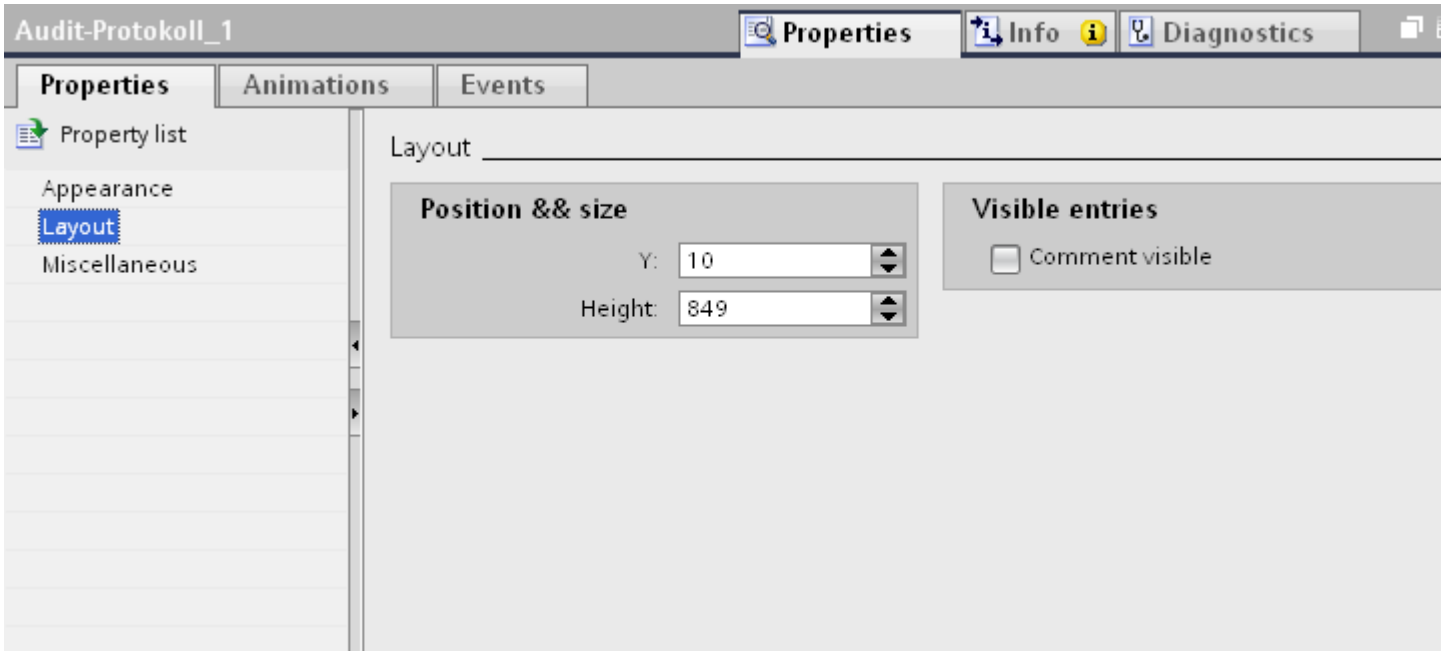
You can configure the foreground color, the background color, the style, and the font settings.

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.

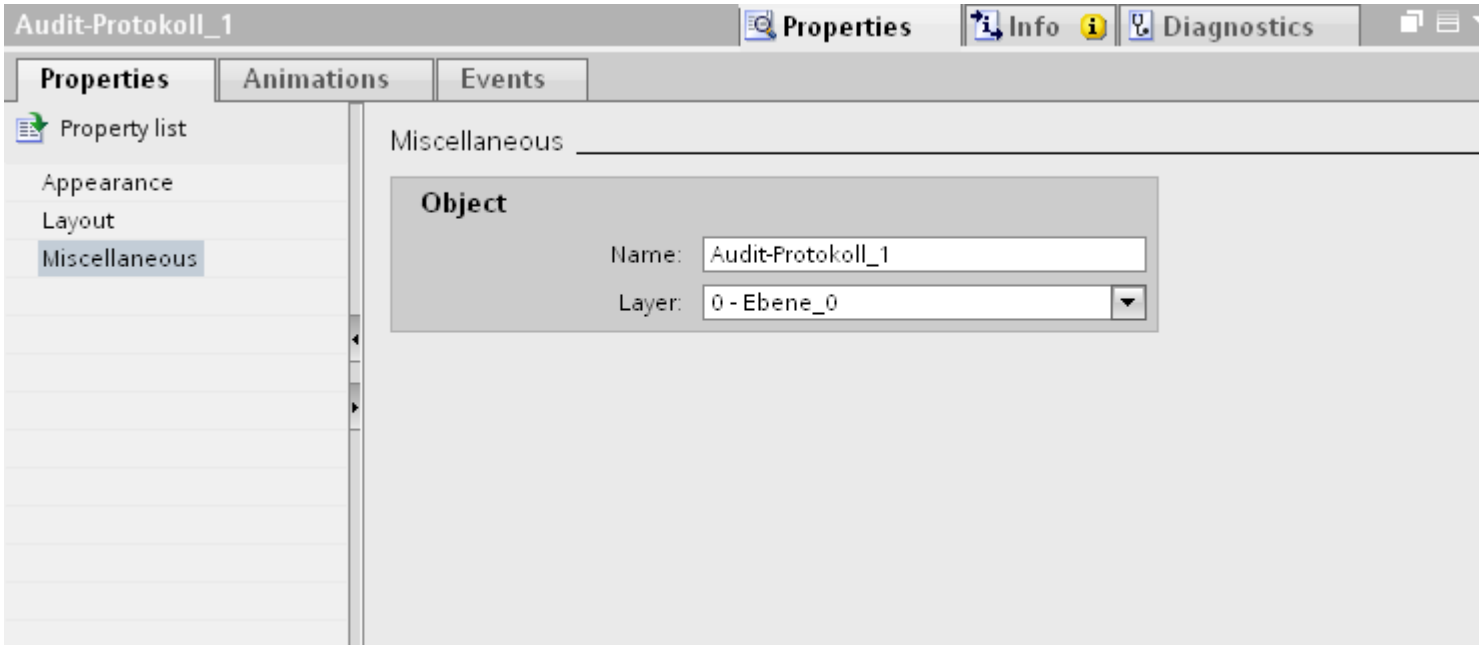
A page break is automatically inserted when the length of the page is exceeded to print out all data.

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".



1.3.6.4 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 system functions "ArchiveLogFile" or "DeleteLog".
- 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.

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.

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

1.3.7.1 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.

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

Introduction

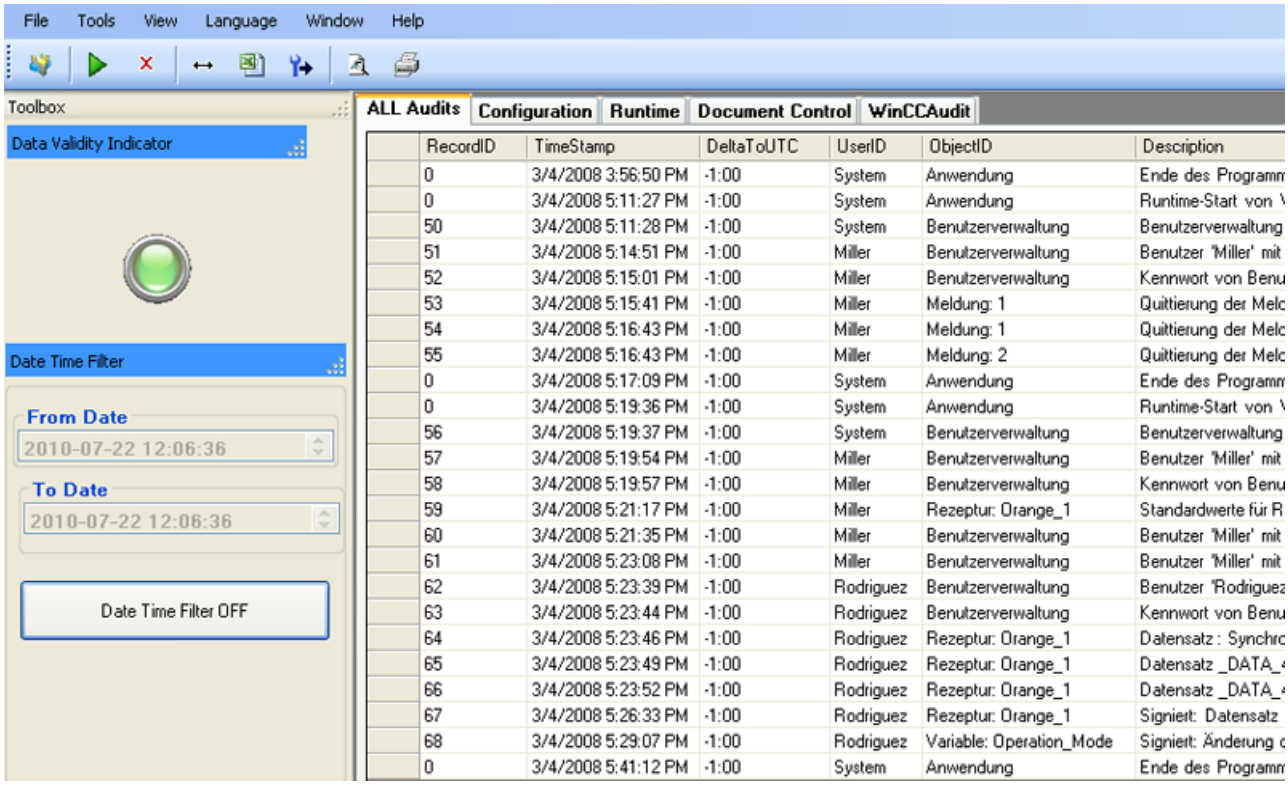
The Audit Viewer allows you to evaluate all Audit Trail data in a table.

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:



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 logon attempts:

1.3.7.3 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.

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"

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

1.3.8.1 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.

1.3.8.2 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 Trai, 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".

1.3.8.3 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:

Evaluating Audit Trails with DOS program (Page 33)

1.3.8.4 WinCC upgrade (Panels, Comfort Panels, RT Advanced)

WinCC upgrade

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.

1.3.8.5 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.

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

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

1.4.1.1 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 will be 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.

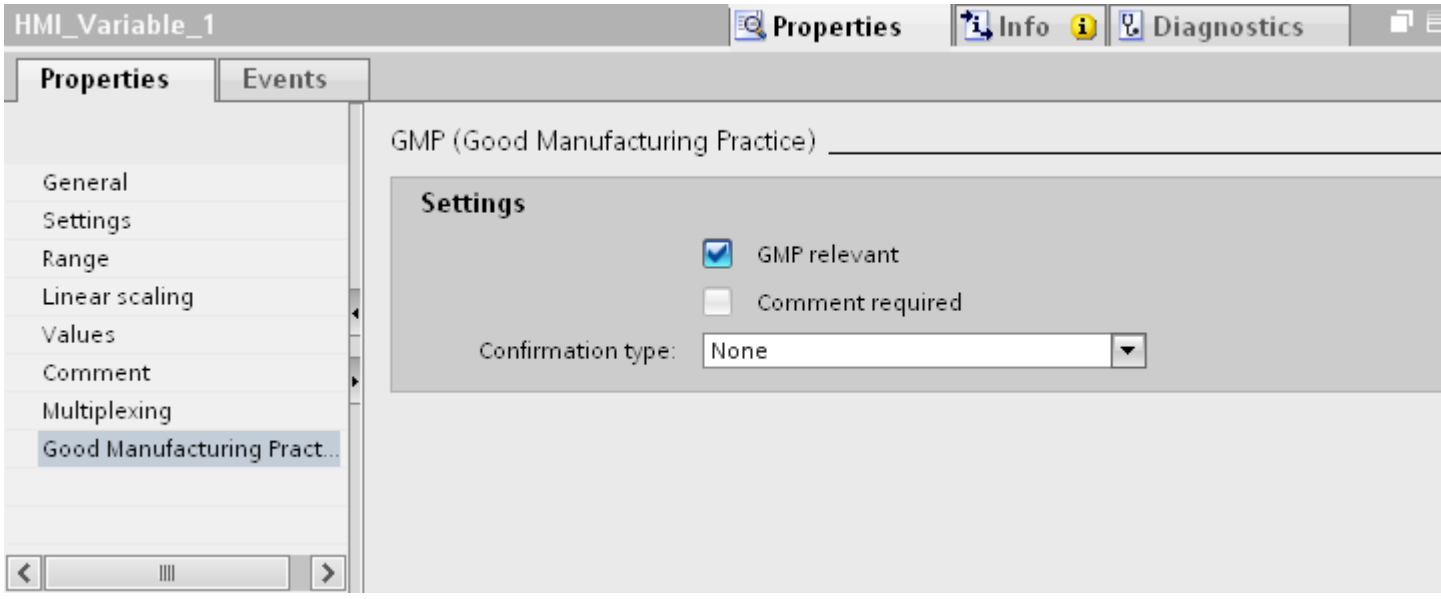
1.4.1.2 Logging tag value changes (Panels, Comfort Panels, RT Advanced)

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.

1.4.1.3 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.

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

1.4.2.1 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"

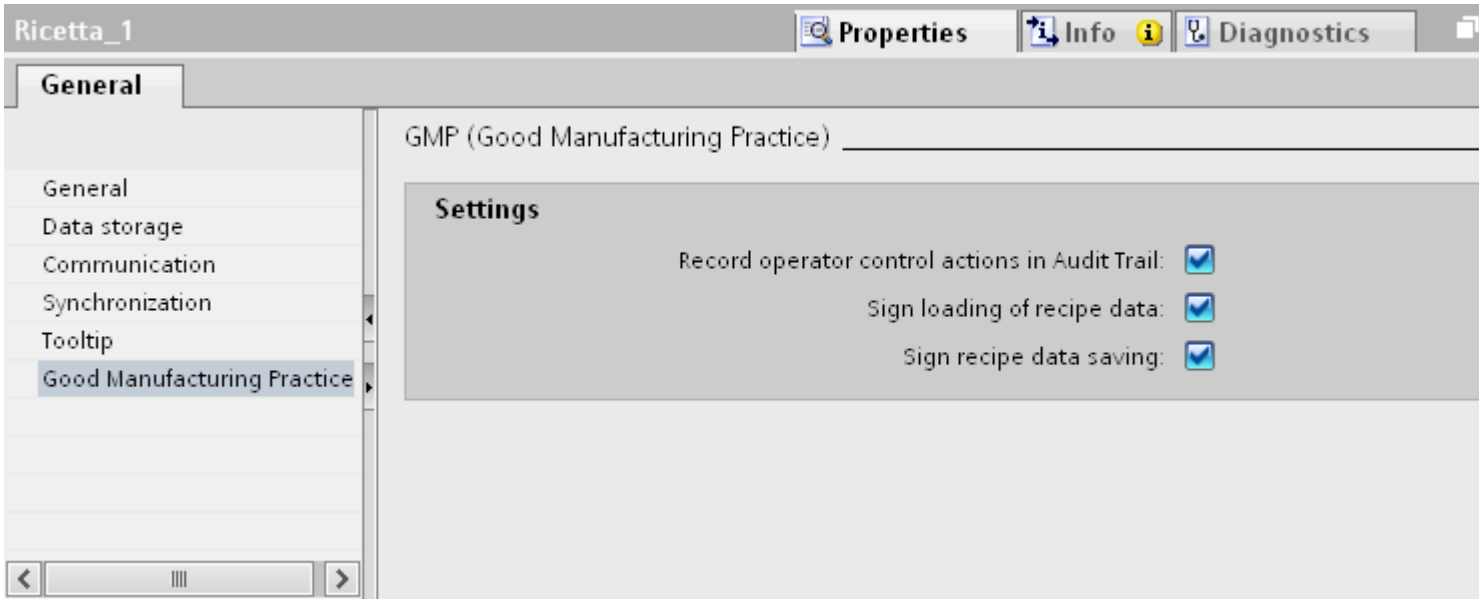
1.4.2.2 Logging recipe data changes (Panels, Comfort Panels, RT Advanced)

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.

1.4.2.3 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.

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

1.4.3.1 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

1.4.3.2 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.

1.4.3.3 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.

1.4.3.4 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

1.4.4 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)	---

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 (ImportDataRecord-sWithChecksum)	entered in Audit Trail if the recipe is GMP-relevant
ExportDataRecords (ExportDataRecords)	---
ExportDataRecordsWithChecksum (ExportDataRecord-sWithChecksum)	---
LoadDataRecord (LoadDataRecord)	entered in Audit Trail if the recipe is GMP-relevant Signing required depending on recipe configuration

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 (---)	---

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 (---)	---

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

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

1.5 Performance features of GMP-compliant configuration (Panels, Comfort Panels, RT Advanced)

1.5.1 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
- Mobile Panels 277
- MP 377
- Comfort Panels
- Panel PCs with WinCC RT Advanced
- WinCC RT Advanced

Note

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

1.5.2 Restrictions (Panels, Comfort Panels, RT Advanced)

Restrictions

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

- "Status/Force" 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 acknowledgement 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.

WinCC DataMonitor (RT Professional) 2

2.1 The basics (RT Professional)

2.1.1 DataMonitor (RT Professional)

Introduction

WinCC DataMonitor consists of a server component and a client component. The DataMonitor Server makes functions for analyzing and displaying data available to the DataMonitor client. Access rights govern access to the functions.

- WinCCViewerRT
  Program for monitoring WinCC projects. The DataMonitor client is therefore a so-called "View Only Client".
- Excel Workbooks
  Display of logged process values in an Excel table for analysis and storage in the Web or as a print template for reports
- Published Reports
  Creation of reports from WinCC print jobs, or from published Excel worksheets. This allows you, for example, to generate statistics and analyses of specific process or history data. The reports are saved in PDF format and can be transferred by e-mail.
- WebCenter
  Central information portal for access to WinCC data via user-specific views, clearly structured WebCenter pages through user groups with individual user rights for reading, writing and creating WebCenter pages.
- Trends & Alarms
  Serves to display logged process values and alarms. The data is displayed in tables and diagrams on predefined WebCenter pages.

Your benefit:

- Display and analysis of current process statuses on office PCs with, for example, MS Internet Explorer or MS Excel
- No additional configuration effort, as screens from the WinCC project are used directly.
- Evaluation via centrally administered templates for detailed analyses of corporate processes, e.g. reports, statistics
- Creation of event-driven or time-driven reports

- Information from the process is individually compiled online in runtime (information portal) and distributed to various people by e-mail.
- User administration with user groups and individual access authorizations, e.g. read, write, and creation of WebCenter pages

2.1.2 WinCCViewerRT (RT Professional)

Overview

The Web Viewer is solely a display program for WinCC projects that is installed using the DataMonitor Client. DataMonitor Client is therefore a so-called "View Only Client".

Don't use Internet Explorer to run the "WinCCViewerRT.exe" application. Run it on the DataMonitor client instead.

The Web Viewer uses its own communication resources to access the DataMonitor server. This prevents Internet users from accessing the system and protects the system against viruses and Trojan horses.

Only the screens which are configured for Web access and published on the DataMonitor server are displayed.

The WinCC user needs the authorization no. 1002 "Web access - view only". The cursor is a "View only cursor" and indicates that process-related operations are not possible. Certain operations are still possible, such as opening the properties dialog of an online trend control.

If the WinCC user is not assigned authorization no. 1002, the DataMonitor Client runs in demo mode after logon.

You can also use the WebViewer as terminal services application. For more information, refer to "Setting up terminal services for WebNavigator servers".

See also

Configuring runtime settings (DataMonitor) (Page 75)

2.1.3 WebCenter (RT Professional)

Overview

The WebCenter is the central information portal for access to WinCC data via Intranet/Internet.

With the help of WebCenter pages and Web parts, the user can arrange and save his view of the WinCC data. WebCenter pages are stored in directories.

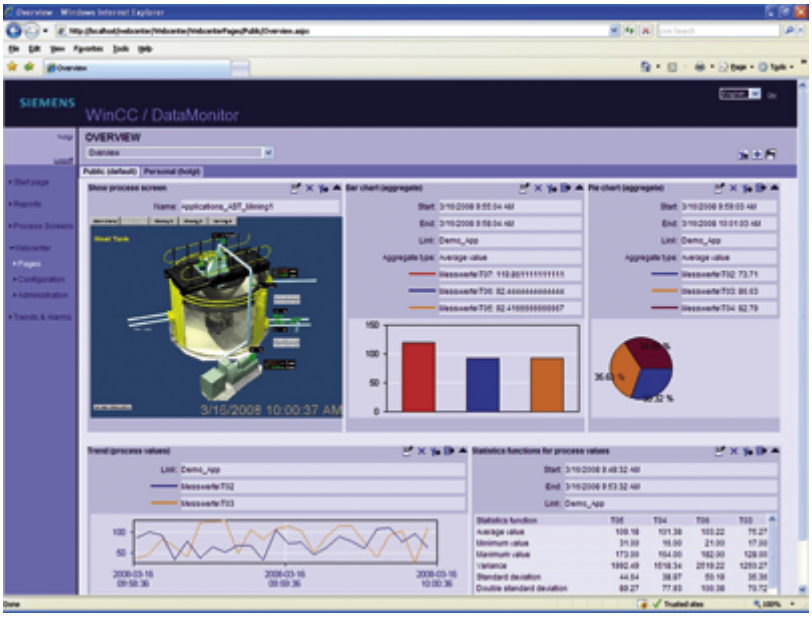
WebCenter pages are like a construction kit. The form of the construction kit is specified by layout master copies. Users can use either the supplied or self-created layout master copies.

Web parts are the individual building blocks that prepare and display data. Within the WebCenter pages, the parameter definitions are stored for the respective Web parts and can

be called up again at any time. A multiple use of the same web part is also possible with different parameter definitions. The WebCenter pages that have been created in this way can be opened by different users with the same parameter definitions depending on the assignment of rights.

To transfer the configuration data to a different computer, copy the corresponding project directory:

- ..\WebCenter\App_Data\Webcenter



Web parts

Up to 15 of the following Web objects can be combined into one screen view:

- Process value table
  The available process values for the specified period are displayed.
- Process values in table (time step)
  The full archive name and the tag name are displayed as a tooltip in the header of the column.
  The process values are summarized beginning with the starting time in the specified time interval.
  The interval result is displayed for the interval depending on the specified aggregate type. For example, a process value was logged every 30 seconds. You have chosen an interval of 60 seconds and "Mean value" as the aggregate type. Now the mean of the two log values is formed and displayed in the table with the first time stamp of the period of calculation.
  If you select a aggregate type without interpolation and no value is available in the interval, no interval result is displayed. If you select a aggregate type with linear interpolation, an interval result is displayed for each interval.
- Statistics functions for process values
  All available process values are used for the specified time period, for example, to calculate and display the mean value.
- Trend process values
  The process values are displayed in trends.

- Trend (time step)
  Concise presentation of precompressed values in trends with aggregate functions, for example, as sums or averages.
- Bar chart (aggregates)
- Pie chart (aggregates)
- Alarm table
  Presentation of the accumulated alarms.
- Alarm hit list
  Presentation of statistical information about the alarms.
- Link to Web Center pages
- Links (external)
  Links to internal Web Center pages and external Internet sites, for example, stock market news.
- Display information
  For example, news reports
- Static process screens
  WinCC screens are integrated into the Web Center with no installation download. A screenshot of the process screen is created as a JPG on the DataMonitor server at regular intervals.
- Display graphic
  JPG images, e.g. company logos.
- The most recent reports
  Display the most recently generated reports. For example, the last ten print jobs generated with "Reports" in PDF format.

Basic procedure

1. Set up a directory for a WebCenter page (Page 93)
2. Assign access rights (Page 94)
3. Establish a connection to the WinCC data (Page 95)
4. Publish screens for the WebCenter (Page 103)
5. Create a layout template for WebCenter pages (Page 106)
6. Create a WebCenter page (Page 109)
7. Insert Web parts into the WebCenter page (Page 112)
8. Configure Web parts within WebCenter pages (Page 115)

See also

Trends and Alarms (Page 57)

2.1.4 Trends and Alarms (RT Professional)

Overview

"Trends & Alarms" are used to display and analyze logged process values and messages in trends and tables and for evaluation with statistics functions.

Predefined Web pages contain the following:

- Display of a process value in a table (Page 119).
- Display of a maximum of three process values in a diagram. (Page 121).
- Statistics functions for process values (Page 128).
- Alarm hit list (Page 127).
- Display of messages in a table (Page 123).

The functions of "Trends & Alarms" are configured with web parts. The same Web parts are used here as are used in the WebCenter pages (Page 54).

2.1.5 Excel workbooks (RT Professional)

Overview

With "Excel Workbooks", it is possible to display process data such as alarms and values of process or logging tags in an Excel table on the DataMonitor client. Data of logging tags of swapped out logs is not displayed.

The data is analyzed using Excel functions or graphically formatted trend view, e.g. mean value calculation, diagram presentation.

You configure the Excel Workbook for displaying the process data using the Excel Add-In "Excel Workbook Wizard". The online display of the process data is performed via the Excel Add-In "Excel Workbook".

The created Excel workbooks can also be configured as templates for the function "Reports".

Note

You need the DataMonitor client to use the "Excel Workbooks" function. The installation file can be found on the DataMonitor start page under "Reports > Download area", on the installation medium, or at the download installations.

Configuring with XML file or online

Simultaneous online access to process data of different WinCC servers is possible using the Excel worksheet. This requires that you either take the data from an XML file or from a local WinCC project during the configuration in the Excel Workbook Wizard.

Separation between process and analysis by configuring with XML file

By using the XML file for the project-relevant data, a separation between the process and the analysis is possible.

You create the XML file on a DataMonitor server. Afterwards, transfer the XML file to a PC with Microsoft Excel, located in operation management for instance. You can configure the process data display in the sheet on the PC.

Afterwards, transfer the workbook to a DataMonitor client where the process data is to be displayed online.

Configuration steps

The configuration of this function is carried out with the following steps:

1. In order to configure using the online data, configure directly on the WinCC server or on a WinCC client with an online connection to the respective WinCC server.
2. You have to create the XML file in order to configure with the data of an XML file. Use the "WinCC DataMonitor Configurator Export" application to create an XML file with the relevant data of the opened WinCC project on the DataMonitor server.
3. Use the Excel add-in "Excel Workbook Wizard" to import the project-relevant data to an Excel workbook.
4. Configure the display of process data such as alarms and tag values.
5. To display process data in the Excel workbook in online mode, use the Excel add-in "Excel Workbook" on a DataMonitor Client. The values can also be further processed in Excel.

Note

If you rename a table in an Excel workbook, the configuration data of the table will be lost.

2.1.6 Reports (RT Professional)

Introduction

Using Reports , you can use WinCC print jobs and published Excel Workbooks to output analysis results and process data. The data is output in PDF or XLS file format

When the reports are created is defined on the DataMonitor Server. The following options are available:

- Manually, for example, by a plant operators.
- Event-driven, for example, when a tag value has changed-
- Time-driven, for example, daily.

You can also transmit a report as e-mail attachment The various directories can only be accessed with the appropriate authorization; including access over an Intranet or the Internet.

Requirement

Output as PDF file (WinCC print jobs)

- PDF Reader The PDF reader can be obtained from www.adobe.com, for example.

Output as XLS file (Excel workbook)

- MS Excel as of Office XP is installed.
  To use the DataMonitor Server for the automatic creation of Excel reports, you must install MS Excel on the server PC.
- The Excel workbook is created at and published as template at the DataMonitor Server. For more information, refer to "Configuring an Excel workbook (Page 130)".

Note

Displaying data on the DataMonitor Client

In the Excel worksheet, the creation time and periods are always displayed in the local time zone of the DataMonitor Server.

See also

Configuring an Excel workbook (Page 130)

2.1.7 Access rights (RT Professional)

Introduction

When using DataMonitor, different authentications are required. You have to define specific users and user rights for this.

- For the functions "Trends and Alarms", "Reports" and "Webcenter", a Windows user.
- For the functions "WinCCViewerRT" and "Excel Workbooks", a WinCC user.

SIMATIC logon allows the central administration of users. To use SIMATIC logon in conjunction with DataMonitor, the DataMonitor user is added to the user group "SIMATIC HMI VIEWER". The user group "SIMATIC HMI VIEWER" is created during the installation of WinCC Runtime Professional.

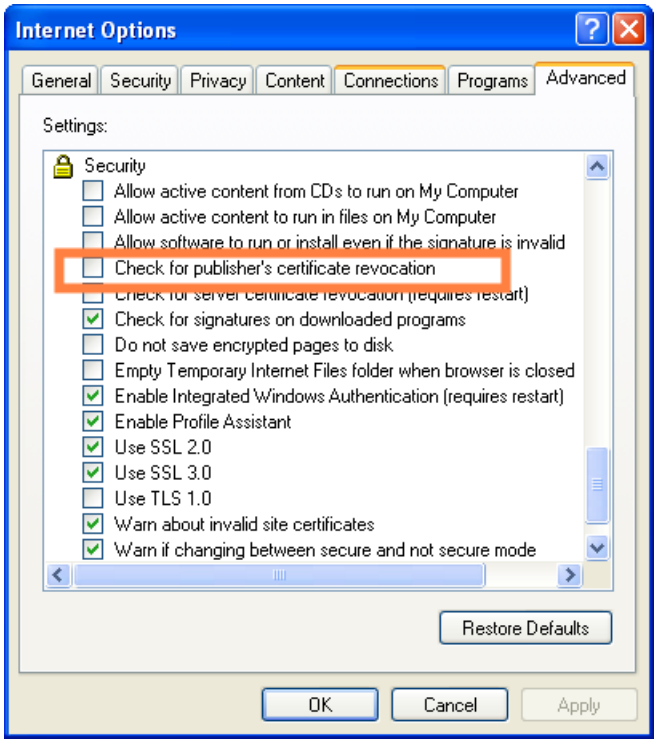
2.1.8 Checking certificates (RT Professional)

Introduction

Before you work with the DataMonitor, you need to adjust the settings in Internet Explorer.

Procedure

1. Open the Internet Explorer.
2. Open the "Internet Options" dialog under:
   "Tools > Internet Options"
3. Select the "Advanced" tab.
4. Deactivate the following option in the "Security" area:
   "Check for publisher's certificate revocation".



2.2 Installing DataMonitor (RT Professional)

2.2.1 Licensing (RT Professional)

DataMonitor client

DataMonitor client does not need a license.

DataMonitor server

Licenses must be installed on the DataMonitor server for the DataMonitor clients. The license check is different for the following function groups.

- "DataMonitor" with the functions:
  "WinCCViewerRT" and "Excel Workbooks"
  A "WinCC DataMonitor" license is required on the server computer for each DataMonitor client.
- "Webcenter" with functions:
  "Webcenter", "Trends and Alarms", "Reports"
  It is not the number of clients but the number of connections that is relevant for the license count with the "Webcenter" function group.

The following table shows the number of possible clients based on the function group and license.

License	"DataMonitor" function group	"WebCenter" function group
1 Client	1	3
3 Clients	3	6
10 Clients	10	20
25 Clients	25	50
50 Clients	50	100

Example

With a "3 Clients" license, the following users can log on simultaneously:

- 3 users of the "DataMonitor" function group
- 6 users of the "WebCenter" function group

Operation without valid license

If no license is available, DataMonitor displays a page requiring acknowledgement indicating the missing license at start-up.

- Click the "OK" button to acknowledge the notice.
  The start page of the DataMonitor is displayed.

Help:

- Check the existing licenses. If necessary, install the required licenses.

Note

If the user does not log out with the "Logout" button and the browser is closed, the connection is maintained and the license remains occupied. The license will only be released again after approximately 20 minutes.

2.2.2 Installation of the DataMonitor server (RT Professional)

2.2.2.1 Installing DataMonitor server (RT Professional)

Requirement

- Administrator rights
- Internet Information Service is installed.
- Installation disk with WinCC RT Professional

Procedure

Proceed as follows to install the DataMonitor server:

1. Place the installation disk in the drive.
   The disk starts automatically if auto-run is enabled in the operating system. If auto-run is not activated, start the Setup.exe program on the disk.
2. Select "User defined" for "Installation mode".
3. Select the "DataMonitor Server" program package.
4. Start the installation.
   You can track the status of the installation in the displayed dialog. Select "Cancel" to cancel the installation.
5. After installing the DataMonitor server, you can transfer the license key for the product. Click on "Transfer License Key" to do this. If you have already transferred the license key or you want to install it subsequently, select "Next".

   Note

   License keys are not transferred automatically. Transfer the missing license keys during or after installation using Automation License Manager.

6. Reboot the PC when prompted by Setup.

Result

The DataMonitor server is installed.

2.2.2.2 Installing the Internet Information Service (RT Professional)

Settings

Before installing the DataMonitor server, you must install the Internet Information Service (IIS). During installation, you specify the settings for the DataMonitor server.

Activate the following settings:

- Web management tools:
  - IIS management service
  - IIS management console
  - IIS management scripts and tools
  - Compatibility with IIS Metabasis and IIS 6 configuration
  - Compatibility with WMI for IIS 6
- WWW services > General HTTP features:
  - Standard document
  - Static content
- WWW services > Application development features:
  - .NET extension capability 3.5 and 4.5
  - ASP
  - ASP.NET 3.5 and 4.5
  - ISAPI extensions
  - ISAPI filters
- WWW services > Security:
  - Requirement filtering
  - Standard authentication
  - Windows authentication

Note

If the logging functions are active with IIS, the log files must be monitored and deleted, if necessary. The event views should be configured in such a way that the log files do not become too large.

Requirements

- Windows user with administrator rights
- Write access for the registry database

Procedure

To install the IIS, follow these steps:

1. Insert the Windows installation disk into the drive.

Open the Control Panel. Click the "Programs and Features" entry.

1. Click the "Turn Windows features on or off" entry.
2. Activate the settings mentioned above.
3. Close the dialog with the "OK" button. The required data is transferred and the IIS is configured accordingly.

Alternative procedure

You can also use the command line "Start > Run > cmd" to install the IIS components located on the installation data carrier:

pkgmgr.exe /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-HttpErrors;IIS-ASPNET;IIS-NetFxExtensibility;IIS-ASP;IIS-ISAPIExtensions;IIS-ISAPIFilter;IIS-BasicAuthentication;IIS-WindowsAuthentication;IIS-ManagementConsole;IIS-ManagementService;IIS-IIS6ManagementCompatibility;IIS-Metabase;IIS-WMICompatibility;IIS-ManagementScriptingTools

2.2.3 Installation of the DataMonitor client (RT Professional)

2.2.3.1 Installation of the DataMonitor client (RT Professional)

Installation Conditions DataMonitor Client

You need not install the DataMonitor client if you only want to use "Webcenter" and "Trends and Alarms".

You can install "Excel Workbook Wizard" on the client PC as an add-on. "Office Excel 2007", "Office Excel 2010" or "Office Excel 2013" are required for the installation of "Excel Workbook" on the client PC, because "Excel Workbook" and "Excel Workbook Wizard" are installed as Excel add-ins.

Note

Installation of the DataMonitor client on the DataMonitor server

To also install DataMonitor client or WebNavigator client on a DataMonitor server, you need to proceed as follows:

1. Switch the start type of the service to manual in the service manager.
2. Reboot the PC.
3. Install the DataMonitor client.
   During the installation, ensure that no WebNavigator clients or DataMonitor clients access the server.
4. When the installation is successfully completed, switch the start type of the "CCArchiveConnMon" service back to automatic.

Requirement

- Software and hardware requirements are met. For more information, refer to "AUTOHOTSPOT".
- Security settings in Internet Explorer are configured.

Installation options

The following options are available for installing the DataMonitor client.

- Installation via the installation disk
  In this case, certain Windows user rights are necessary, depending on the operating system.
- Installation via the Intranet/Internet
  In this case, certain Windows user rights are necessary, depending on the operating system.
- Additional installation options.
  The installation can also be performed without user interaction, under the Windows user rights of the current user or in networks using Group policy-based software distribution.

2.2.3.2 Configuring security settings in Internet Explorer (RT Professional)

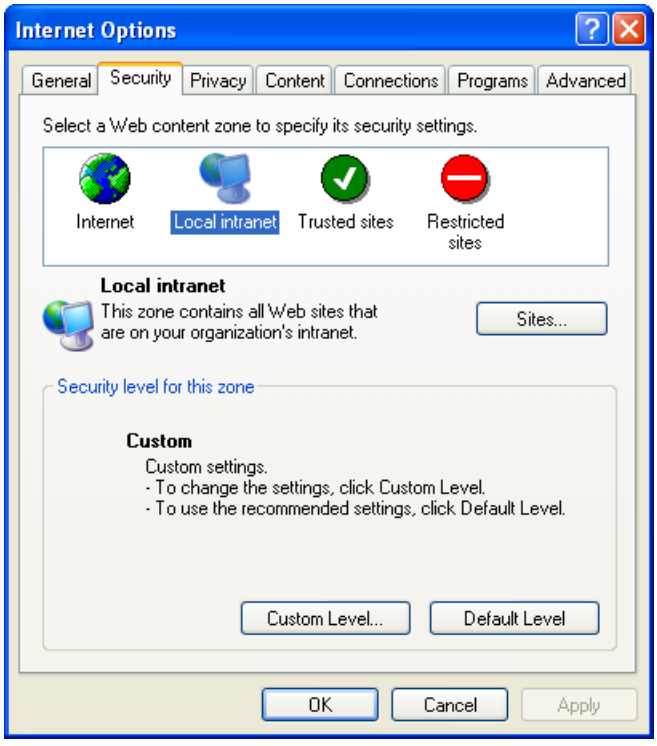
Requirement

Internet Explorer is open.

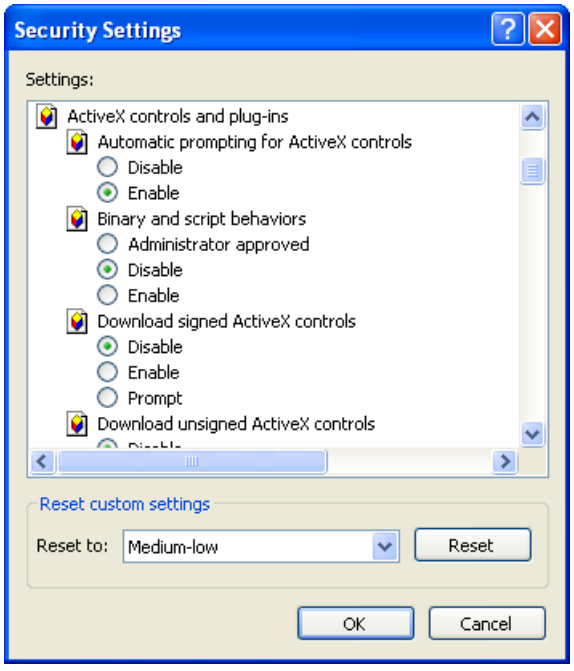
Procedure

To configure the security settings in Internet Explorer, follow these steps:

1. Select the command "Internet Options" from the "Tools" menu in Internet Explorer.
2. Select the "Security" tab. Select the corresponding zone, e.g. "Local Intranet" or "Internet".



3. Click on the "Custom level" button. The "Security settings" dialog opens.



4. Select the "Enable" option for "Script ActiveX controls marked safe for scripting" and "Download signed ActiveX controls".
5. Select the "Enable" option under "Scripting > Active Scripting".
6. Click the "OK" button. Carry out the modifications in the subsequent dialog.
7. Select the "Trusted Sites" icon. Click the "Sites" button. The "Trusted sites" dialog opens.
8. Enter the address of the web server in the field "Add this web site to the zone". Possible formats and placeholders include "*://157.54.100 - 200", "ftp://157.54.23.41", or "http://*.microsoft.com". Deactivate the "Require server verification (https:) for all sites in this zone" check box. Click "Add". Confirm your entries with "OK".
9. Select the "Trusted Sites" icon. Click the "Standard level" button and then the "Custom Level" button. The "Security settings" dialog opens.
10. Select the "Enable" option for "Initialize and script ActiveX controls not marked as safe for scripting". Confirm your entries with "OK".
11. Click on the "General" tab. Click on the "Settings" button in the "Temporary internet files" area . Select the "Automatic" option for "Check for newer versions of stored pages". Confirm the entry using the "OK" button.
12. Click "OK" to close the "Internet Options" dialog.

Result

The security settings in Internet Explorer are configured.

2.2.3.3 Installing with the installation disk (RT Professional)

Requirements

- Security settings in Internet Explorer are configured.
- User possesses the necessary rights for installation.

Procedure

To install the DataMonitor client using the installation disk, follow these steps:

1. Place the installation disk in the drive.
   The disk starts automatically if auto-run is enabled in the operating system. If auto-run is not activated, start the Setup.exe program on the installation disk.
2. Select "User defined" in the "Installation mode" dialog.
3. Select the "DataMonitor Client" program package.

4. Start the installation.
   You can track the status of the installation in the displayed dialog. Select "Cancel" to cancel the installation.
5. Reboot the PC when prompted by Setup.

Result

DataMonitor client is installed. The "WinCCViewerRT" function is activated.

2.2.3.4 Installing via the Intranet/Internet (RT Professional)

Requirements

- Security settings in Internet Explorer are configured.
- User possesses the necessary rights for installation.
- DataMonitor server is installed and configured.
- User is created in user administration.
- The WinCC project is in Runtime on the DataMonitor server.
- The server PC and client PC are interconnected via a TCP/IP-capable network.

Procedure

To install the DataMonitor client via the Intranet/Internet, follow these steps:

1. Enter the address of the DataMonitor server in the address bar.
   - Default web site: "http://www.server_name.de"
   - Web site in the virtual directory: "http://www.server_name.de/DataMonitor"
2. Log on to the DataMonitor server with your user name and password. If you are accessing the DataMonitor server for the first time, you will be prompted to install the DataMonitor client.
3. Click the "Click here to install" link.
4. Click the "Save" button in the "File Download" dialog to store the client setup on the client PC. It is recommended that you save the setup file. Then if the client PC needs to be restarted, it is not necessary to download the setup again.
5. Leave the Internet Explorer open and open Windows Explorer. Navigate to the directory in which you saved the setup file. Double-click the setup file.
6. Follow the instructions on the screen and enter the information and settings necessary. The client-end controls of the DataMonitor are installed. Close the Setup dialog.

Result

After the successful completion of the installation, the DataMonitor client switches to the WinCC project currently in Runtime.

Note

If you have already installed the DataMonitor client and wish to install a current version of the client via the Intranet/Internet, open the Client Setup straight away without saving the installation file on the target PC. If you want to save the new installation file, uninstall the old installation file first or save the new version of the file in different directory than the older version of the file. (necessary)

Note

When downloading the DataMonitor server client software, select the "Save" option to save the client setup on the client PC. It is recommended to save the Setup file because, in the event of a restart of the client computer being necessary, the Setup need not be downloaded again.

If the DataMonitor client was installed previously from the DVD and you want to install an updated version of the client via the Intranet/Internet, the client setup must also be saved on the target PC.

2.2.3.5 User rights, user groups and optional installation possibilities (RT Professional)

User rights, user groups and optional installation possibilities

The following conditions apply for the installation of the DataMonitor client:

- Windows user rights required for installation and first registration of the DataMonitor client
- Installation of the DataMonitor client with restricted windows user rights
- Installation for a configured group of users or PCs
- Group policy based software distribution
- Installation without user interaction

Windows user rights required for installation and first registration of the DataMonitor client

To install the DataMonitor client via Intranet/Internet or from the installation disk, you require certain minimum user rights.

Operating system	Required minimum user rights
Windows Server 2008 R2 SP1/ Windows Server 2012 R2	"Power user"
Windows 7/ Windows 8.1	"Power user"

Use the following for the first logon of the DataMonitor client to the DataMonitor server:

- The user identification of the installation
- A user with equal or higher Windows user rights
  If the first logon was successful, subsequent logons can be performed for a user without "Power user" or "Administrator" rights.

Installation of the DataMonitor client without "Power user" or "Administrator" rights

By using Microsoft Windows Installer technology (MSI), DataMonitor clients can also be installed with limited Windows user rights i.e. without possessing the "Power user" or "Administrator" rights. The add-ons and plug-ins for the DataMonitor client can also be installed this way.

This procedure can be used for the following installations:

- Installation via group policy-based software distribution in networks
- Installation for a configured group of users or PCs.

Installation for a configured group of users or PCs

Using the Microsoft Systems Management server or group policy on a domain controller, it is possible to install a group of users or PCs configured by the administrator.

- The MSI file "WinCCDataMonitorClient.msi" is published on the domain controller and enabled for a user group. The installation is then performed according to the configuration of the group policy based software distribution either during logon of the defined users or when the computer is started.
- When using a Microsoft Systems Management Server, the installation is configured and triggered by the administrator, and executed when the relevant PC boots. Additional information on Microsoft Systems Management server is available on the Microsoft home page.

Group policy based software distribution

The software installation is normally executed with the access rights of the current Windows user. When using MSI technology, the installation is performed by an operating system service with higher rights. This enables installations to be performed for which the Windows user has no permission. Applications which require installations with a higher permission are referred to as "privileged installations" in MSI technology. Installation of these applications is possible when a Windows user is assigned the "Always install with elevated privileges" permission.

To use group policy-based software distribution, a group policy is created on the domain controller. The software to be distributed is assigned or published using the active directory .

- Assignment: The software distribution can be assigned to a user or a PC. The software to be distributed is automatically installed when the user logs on or the PC boots.
- Publication: The software distribution can be published for single users. When the user logs onto the client PC, the software to be distributed appears in a dialog and can be selected for installation.

Installation without user interaction

During installation of the DataMonitor client, the user is normally prompted to enter information, e.g. the target directories, the agreement to the software license conditions or components to be installed.

By implementing a configuration file, installation is possible without user interaction. The required path specification and user information are provided in the "options.ini" configuration file. The INI file must be located in the same directory as the setup file of the DataMonitor client. This installation procedure is advantageous when using the group policy-based software distribution.

Installation from the product DVD occurs with user interaction.

The settings given predefined in the table are used under the following conditions:

- The "options.ini" configuration file is missing and there is no corresponding entry available in the registry of the client PC, e.g. due to another SIMATIC HMI product installed.
- Alternatively, the installation is performed via the group policy-based software distribution with assignment to the PC.

Information	Parameter
Target directory for the DataMonitor client	INSTALLDIR=" <syspath1>\Siemens\WinCC"
Target directory for common components	COMMONDIR=" <syspath2>\Siemens "
User information / user name	USER
User information / organization	COMPANYNAME

The "<syspath?>" parameters result from the settings in the registry under the key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion" :

- "<syspath1>" corresponds to the key "ProgramFilesDir" e.g. "C:\\Program Files"

- "<syspath2>" corresponds to the key "CommonFilesDir", e.g. "C:\\Program Files\\Common Files"

Example of an "options.ini" configuration file

```
[USERINFO]

USER=Integration

COMPANYNAME=Siemens AG

[INSTALLPATH]

COMMONDIR=" C:\Programs\Common files\Siemens "

INSTALLDIR=" C:\Programs\Siemens\WinCC "

[FEATURES]

FUNCTIONTRENDCONTROL=0

HARDCOPY=0

WINCCUSERARCHIVES=0

DEU=0
```

```
FRA=0
ITA=0
ESP=0
```

2.3 Configuring the DataMonitor system (RT Professional)

Introduction

For the use of the WinCC DataMonitor, the data and process screens are made available on the DataMonitor Server to be accessed and displayed on the DataMonitor client.

Requirement

- The server PC and client PC are interconnected.
- On the server PC
  - Internet Information Service is installed.
  - The DataMonitor Server is installed.
  - A license key is installed.
  - WinCC Runtime Professional is installed.
- On the client PC
  - Internet Explorer V 8 or higher is installed.

Configuration steps

The following configuration steps are required to set up a DataMonitor system.

1. Configure the WinCC project.
   - Configuring WinCC screens for Web access
   - For WinCCViewerRT and the "Excel Workbooks" function, define the users and access rights in the "User administration" dialog.
   - Configure Runtime settings
2. Transfer your WinCC project to the server PC. If the configuration PC and the WebNavigator server are interconnected, transfer the WinCC project using the command "Download to device > Software (all)".
3. Configure the DataMonitor Server.
   - Setting up the Web folder
   - Define users and access rights in Windows for the functions "Trend and Alarms", "Reports" and "WebCenter".
4. Start WinCC Runtime on the server PC.

5. Use the DataMonitor functions on the DataMonitor Client.
   - Check the Internet Explorer security settings on the client PC
   - Start Internet Explorer on the client PC and enter the address of the DataMonitor Server.
   - After logging on to the DataMonitor Server you can access the DataMonitor functions.
6. Monitor the WinCC project at the DataMonitor Client.
   - Setting up WinCCViewerRT
   - Displaying screens

2.3.1 Configuring a WinCC project (RT Professional)

2.3.1.1 Configuring WinCC screens for Web access (RT Professional)

Configuring individual WinCC screens for Web access

1. Double-click the desired screen in the project tree. The screen is opened and the screen properties are shown in the Inspector window.
2. In the Inspector window, click "Properties > Properties > Web access".
3. Activate "Web access".

or

1. select the desired screen in the project tree.
2. Select "Web access" command in the shortcut menu.

Configuring several screens for Web access

1. Select "Screens" in the project tree.
2. Select "Web access all" command in the shortcut menu.

Result

The WinCC screens are configured for Web access. During the transfer of the project, the WinCC screens are adapted for access via the Intranet/Internet and published on the DataMonitor Server.

For more information, refer to "Transferring when WinCC projects".

See also

Creating static process screens for the Web Center (Page 103)

2.3.1.2 WinCC screens as a gadget (RT Professional)

Gadget on the Data Monitor Server (RT Professional)

Introduction

Using the "Preview" property, you define which screens to group in a gadget. Gadgets are mini applications for the Windows sidebar. In order to use gadgets, a DataMonitor client must always be installed as well on the DataMonitor server.

The following operating systems support gadgets:

- Windows 7 (Professional, Enterprise, Ultimate, Embedded StdE 7)
- Windows Server 2008 Standard Edition SP2

Procedure

To configure WinCC screens as a gadget, proceed as follows:

1. Double-click the desired screen in the project tree. The screen is opened and the screen properties are shown in the Inspector window.
2. In the Inspector window, click "Properties > Properties > Web access".
3. Activate "Preview" and "Web access".
4. Save the WinCC project.
5. Select the "Compile > Software" command in the shortcut menu of the HMI device.

Result

The screens are assembled for the gadget on the WebNavigator server. As soon as the project is in runtime, the WebNavigator server generates a jpg snapshot image "pdlImage.jpg" of each screen at cyclic intervals and in consecutive order.

The file is stored in the directory "\WinCC\Webnavigator\Server\Web\image_gadget". The gadget accesses this file cyclically in the directory again.

Note that user interactions are not possible in the screens displayed. This includes, for example, calls from login dialogs or notice dialogs via functions.

The following objects are not supported for the display in a gadget:

- GSC diagnostics window
- Media Player

Note

The WinCC project shown in the gadget cannot be operated.

Gadget on the Data Monitor Client (RT Professional)

Introduction

In order to use gadgets, a DataMonitor client must always be installed as well on the DataMonitor server. A preconfigured gadget for displaying WinCC screens is located on the DataMonitor client in the installation directory under ""\WinCC\Webnavigator\GADGET".

The following operating systems support gadgets:

- Windows 7 (Professional, Enterprise, Ultimate, Embedded StdE 7)
- Windows Server 2008 Standard Edition SP2

Requirement

The screens are published on the Data Monitor server and configured as "Preview".

Procedure

To access the gadget with the Data Monitor Client, follow these steps:

1. Double-click on the "_WebNavigator.gadget" gadget in the installation directory under "\WinCC\Webnavigator\GADGET". IN Windows 7 / Windows 2008, the gadget is installed in the sidebar.
2. Define the update cycle in which the gadget loads a screen from the Data Monitor Server, every 17 seconds for example.
3. Enter the address of the Data Monitor Server. The gadget establishes a connection to the Data Monitor Server.
4. If necessary, drag-and-drop the gadget onto the desktop.

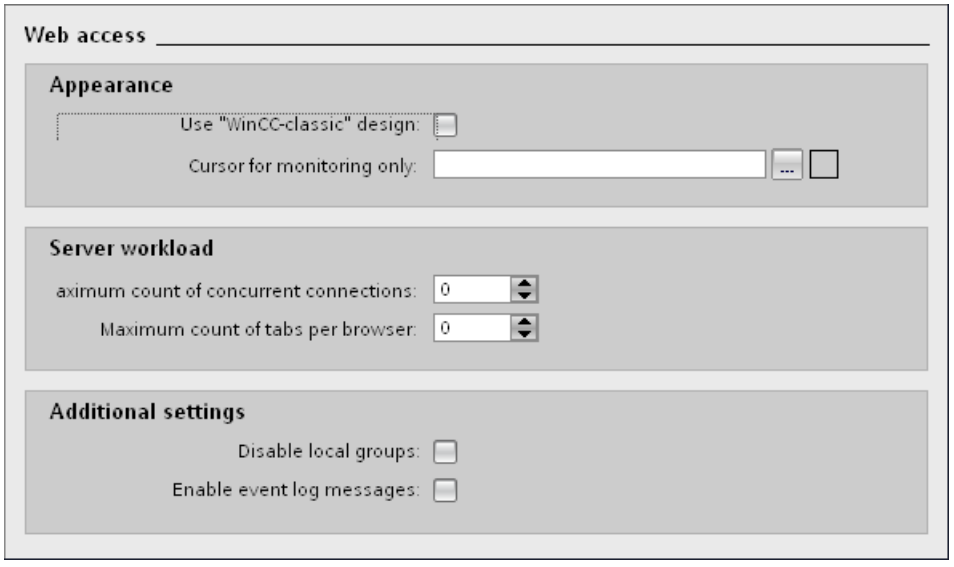
2.3.1.3 Configuring runtime settings (DataMonitor) (RT Professional)

Introduction

You can configure the behavior in runtime in the "Runtime settings" editor.

Procedure

1. Open the "Runtime settings > Web access" editor.



2. To use the "WinCC Classic" design, activate "Use "WinCC-classic" design".
3. To use your own cursor as a "View only cursor", enter the path and file name of the cursor at "Cursor "View only". Alternatively, navigate to the file of the desired cursor using the "…" button.
4. To change the maximum number of concurrent connections, enter the desired number in the "Count of concurrent connections" field.
5. To change the maximum number of open tabs in the browser, enter a suitable value in the "Number of tabs per browser" field. Internet Explorer V7 or higher supports this setting.

   Note

   Server load settings

   Each tab that calls the server homepage uses a license on the server PC. A connection setting of "10" and a tab setting of "2" corresponds to 20 clients. A license for at least 20 clients must be available on the server PC.

6. Define whether the local user group is disabled on the WebNavigator Server.
7. To output an appropriate system message when a WebNavigator logs on and off, activate "Enable event log messages".

Result

The settings for Runtime are configured.

See also

Display screens (Page 89)

2.3.1.4 Defining users in WinCC (RT Professional)

Managing a user group for DataMonitor (RT Professional)

Introduction

A different start screen and the language can be set for each user group. This allows you to make various sections of a project immediately accessible or inaccessible for users.

Note

The name of the user group has to be unique within the project. Otherwise the input is not accepted.

Requirements

- The "User groups" work area is open.
- The "Start" screen has been created and the web access is activate.
- The selected project language is activated.

Procedure

1. Position the mouse cursor on the title of the "Groups" table.
2. Open the shortcut menu with the right mouse button and select the display of the "Start screen" and "Language" columns.
3. Double-click "Add..." in the "Groups" table.
4. Enter "DataMonitor operators" as the name of the user group. Activate at least the "DataMonitor - View only" authorization in the "Authorizations" table.
5. Click the  button in the "Start screen" column. A dialog box for selecting the start screen opens.
6. Select a start screen for Runtime.
7. Close the dialog box by using the  icon.
8. Click the  button in the "Language" column. A dialog box for selecting the language opens.
9. Select the language.

As an alternative, select the user group in the work area; the properties of the user group are then displayed in the Inspector window. In the Inspector window, select "Properties > Properties > Web options". Select the start screen and the language.

Note

The name of the user group is language-dependent. You can specify the name in several languages and switch between languages in runtime.

Managing users for DataMonitor (RT Professional)

Introduction

Create a corresponding user in user administration to enable the use of the "WinCCViewerRT" and "Excel Workbooks" functions.

Requirements

- DataMonitor is installed.
- The "Users" work area is open.
- The "DM_Demo" user is created and assigned view-only rights.
- The "DataMonitor operators" user group has been created.
- The "Start" screen has been created and the web access is activate.
- The selected project language is activated.

Setting the start screen and language

1. Position the mouse cursor on the title of the "Users" table.
2. Open the shortcut menu with the right mouse button and select the display of the "Start screen" and "Language" columns.
3. In the "Start screen" column, click on the button in the row of the "DM_Demo" user. A dialog box for selecting the start screen opens.
4. Select the "Start" screen.
5. Close the dialog box by using the icon.
6. Click the button in the "Language" column. A dialog box for selecting the language opens.
7. Select "Spanish" as the Runtime language.
8. Activate the "DataMonitor operators" user group in the "Groups" table.

As an alternative, select the user in the work area; the properties of the user are then displayed in the Inspector window. In the Inspector window, select "Properties > Properties > Web options". Select the start screen and the language.

Note

The language setting is retained when a user is moved from one group to another. The start screen will be overwritten.

2.3.2 Transferring a WinCC project (RT Professional)

Requirement

- A WinCC project is configured
- DataMonitor Server is installed on the server PC.
- The configuration PC and server PC are interconnected.

Online transfer

Transfer the WinCC project using the command "Load to device > Software (all)". The project is compiled prior to the download. The screens are adapted for access via Intranet/Internet during compilation.

During the download to the server PC, the configured WinCC project is transferred and the screens are published on the DataMonitor Server. For more information, refer to "Compiling and loading".

2.3.3 Configuring the DataMonitor Server (RT Professional)

2.3.3.1 Setting up the DataMonitor Web page (RT Professional)

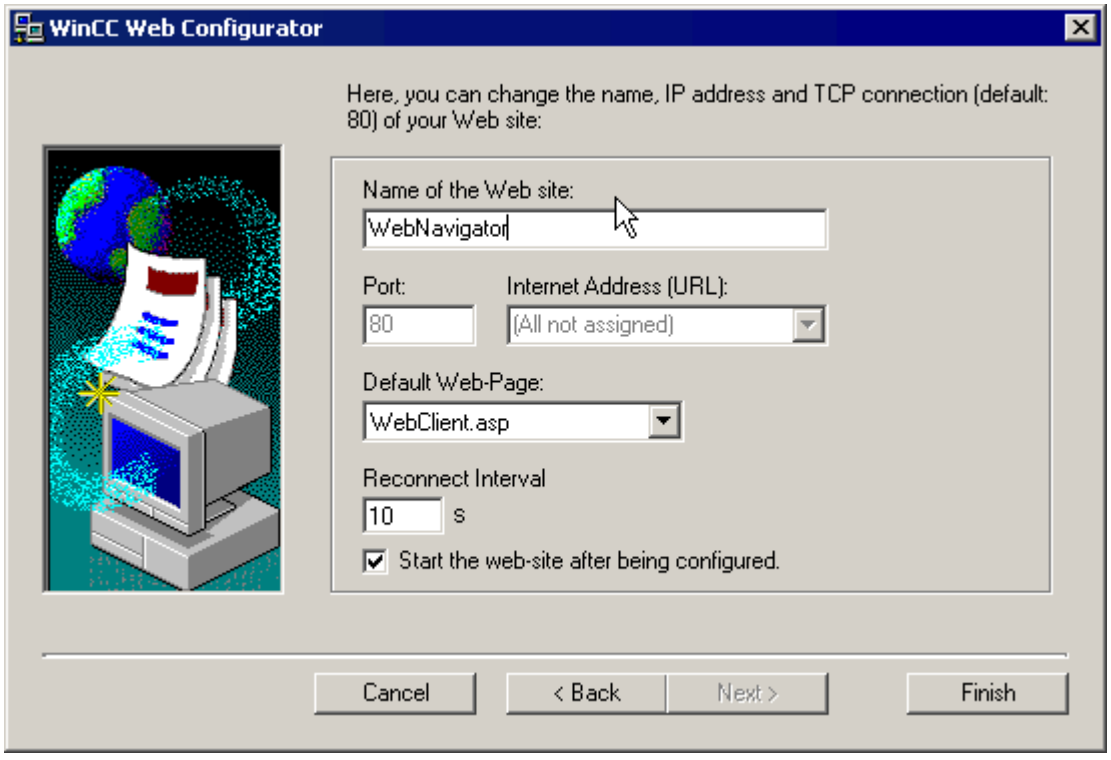
Requirement

- Internet Information Service is installed.
- The WinCC DataMonitor is installed.

Procedure

Set up the DataMonitor Web page as follows:

1. In the Start menu select the command "Start > All Programs > Siemens Automation > Option and Tools > HMI Tools" > WinCC Web Configurator". This starts the Web Configurator.
2. The Web Configurator detects whether a configuration already exists.
   - No configuration available: Select "Create a new standard website (stand-alone)" and click "Next".
   - A configuration exists: Check the configuration
3. Define the desired settings.



4. Enter the name of your Web site in the "Name of the Web site" field.
5. In the "Port" field, enter the port number used for access.
6. In the "IP address" field specify whether the PC is to be reached in the Intranet, Internet or in both networks. Only use addresses from the selection list.
   If you want to make your PC accessible via the Intranet and the Internet, select "All not assigned".
7. Select "DataMonitor.asp" as the standard Web site.
8. Define the time interval after which the Web Navigator Clients automatically start to establish a connection following a connection breakdown. If "0 s" is set, the "Automatic connection establishment" function is disabled.
9. Define the way the Web site is started after configuration.
10. If you have not activated a firewall, click "Finish". If you have installed a firewall, click "Next".

Result

The Web directory has been created and the Web page is activated. If you have activated the firewall, configure the firewall settings with the Web Configurator. See "Setting up a firewall" for additional information.

2.3.3.2 Setting up a firewall (RT Professional)

Introduction

This section describes only the activation of the "HTTP" and "HTTPS" services for port 80 in the respective operating system.

To set up the Windows firewall with advanced security, or for a different port, contact your network administrator.

Requirement

- You have created a standard Web site using the Web Configurator.
- The firewall is activated.
- A logged on Windows user has administrator rights

Procedure

To set up the firewall for a standard port, proceed as follows:

1. Click "Windows Firewall" in the "WinCC Web Configurator".
2. The "Windows Firewall" dialog will open.
3. In Windows 7 or 2008, click "Allow a program or feature through Windows Firewall".
   In Windows 8.1 or 2012, click "Allow an app or feature through Windows Firewall".
4. Activate "Secure WWW Services (HTTPS)" or "WWW Services (HTTP)".
5. Exit the open Windows dialogs with "OK".
6. Click "Finish" in the Web Configurator. The configuration of the server will be completed.

2.3.3.3 Defining users in Windows (RT Professional)

User groups (RT Professional)

User groups in Windows

The following user groups are created automatically in Windows when the DataMonitor server is installed:

"SIMATIC Report Administrators"

The membership in the user group "SIMATIC Report Administrators" is required for extended rights, especially for configuration purposes. You must create at least one user and assign the user group "SIMATIC Report Administrators".

- The following is possible in the "Webcenter" function:
  - Configuration of connections
  - Creation of templates for WebCenter pages
  - Creation and configuration of public and private WebCenter pages
- The following is possible in the "Reports" function:
  - Configuration of reports on the basis of print jobs or Excel workbooks.

"SIMATIC Report Users"

The membership in the user group "SIMATIC Report Users" or in your own user group is required for the functions "Webcenter", "Trends and Alarms" and "Reports".

- The following is possible in the "Webcenter" function:
  - Setting and configuration of WebCenter pages. WebCenter pages are stored in different directories.
  - Opening public pages
- The following is possible in the "Reports" function:
  - Opening reports on the basis of print jobs or Excel workbooks.

Defining Users and Access Rights in Windows (RT Professional)

Requirement

- WinCC Runtime Professional is installed
- DataMonitor Server is installed

Procedure

Proceed as follows to create a user under Windows:

1. Open the Control Panel. Double-click the "Administration" entry.
2. Double-click "Computer Management" in the "Administration" dialog.
   The "Computer Management" dialog opens.
3. Navigate to the directory "System > Local Users and Groups / Groups". Select the "New User..." command in the shortcut menu.
4. Enter the name "DM_Demo" in the "User Name" field in the "New User" dialog. Enter the description "User for DataMonitor" in the "Complete Name" field. Type the desired password into the "Password" field and then repeat it in the "Repeat Password" field. Create the user with "Create". Close the "New user" dialog.
5. In the right part of the table window, click the newly created user. Open the shortcut menu and select the command "Properties". Go to the "Member of" tab. Click "Add".

6. Click the "Advanced >" button in the dialog "Select Groups" and then "Find now".
7. In the dialog below, select the two entries "SIMATIC Report Administrators" and "SIMATIC HMI VIEWER" from the list. To close the dialog, click "OK" twice.
8. The groups "SIMATIC Report Administrators" and "SIMATIC HMI VIEWER" are added to the membership list in the user properties. Click "OK."
9. Close the dialog "Computer Management" with the menu command "File > Exit".
10. Close the dialog "Management" with the menu command "File > Close".

Result

The user "DM_Demo" with membership of the user groups "SIMATIC Report Administrators" and "SIMATIC HMI VIEWER" has been set up.

2.3.4 Starting the DataMonitor on the DataMonitor client (RT Professional)

2.3.4.1 Configuring security settings in Internet Explorer (RT Professional)

Introduction

To have the full functionality available on the DataMonitor client, adapt the security settings in Internet Explorer.

- Internet Explorer V8 or higher

Procedure

To configure the security settings in Internet Explorer, proceed as follows:

1. Click "Tools" > "Internet Options" in the Internet Explorer. The "Internet Options" dialog opens.
2. Click the "Security" tab.
3. Select the "Trusted Sites" icon and click the "Sites..." button. The "Trusted Sites" dialog opens.
4. Enter the address of the DataMonitor Server in the "Add this Website to the zone" field. Possible formats and wildcards include "*://157.54.100 - 200", "ftp://157.54.23.41", or "http://*.microsoft.com".
5. If necessary, clear the "Require server verification for all sites in this zone (https:) check box. Click "Add". Confirm the entry by clicking "OK".
6. Select the "Trusted Sites" icon.

7. Click "Default Level". Click "Customize Level" in the following dialog.
   The "Security settings" dialog box opens.
   - Activate the "Activate" option under "Initialize and script ActiveX controls not marked as safe".
   - Confirm the entry by clicking "OK".
8. Close the "Internet Options" dialog by clicking "OK".

Result

The necessary settings of the DataMonitor client in the Internet Explorer are configured.

2.3.4.2 Starting the DataMonitor startup page on the DataMonitor client (RT Professional)

Introduction

The start page of the DataMonitor summarizes the functions of the DataMonitor.

- "Working with reports (Page 141)":
  Creation and output of the analysis results and process data in print jobs and in published Working with Excel Workbooks (Page 130).
- "Working with the WebCenter (Page 90)"
  Configuration of connections and creation of WebCenter pages for the display of logged data.
- "Working with Trends and Alarms (Page 119)"
  Display of alarms and process values from logs in tables and diagrams.

You start the DataMonitor client on a standalone PC or on a DataMonitor server.

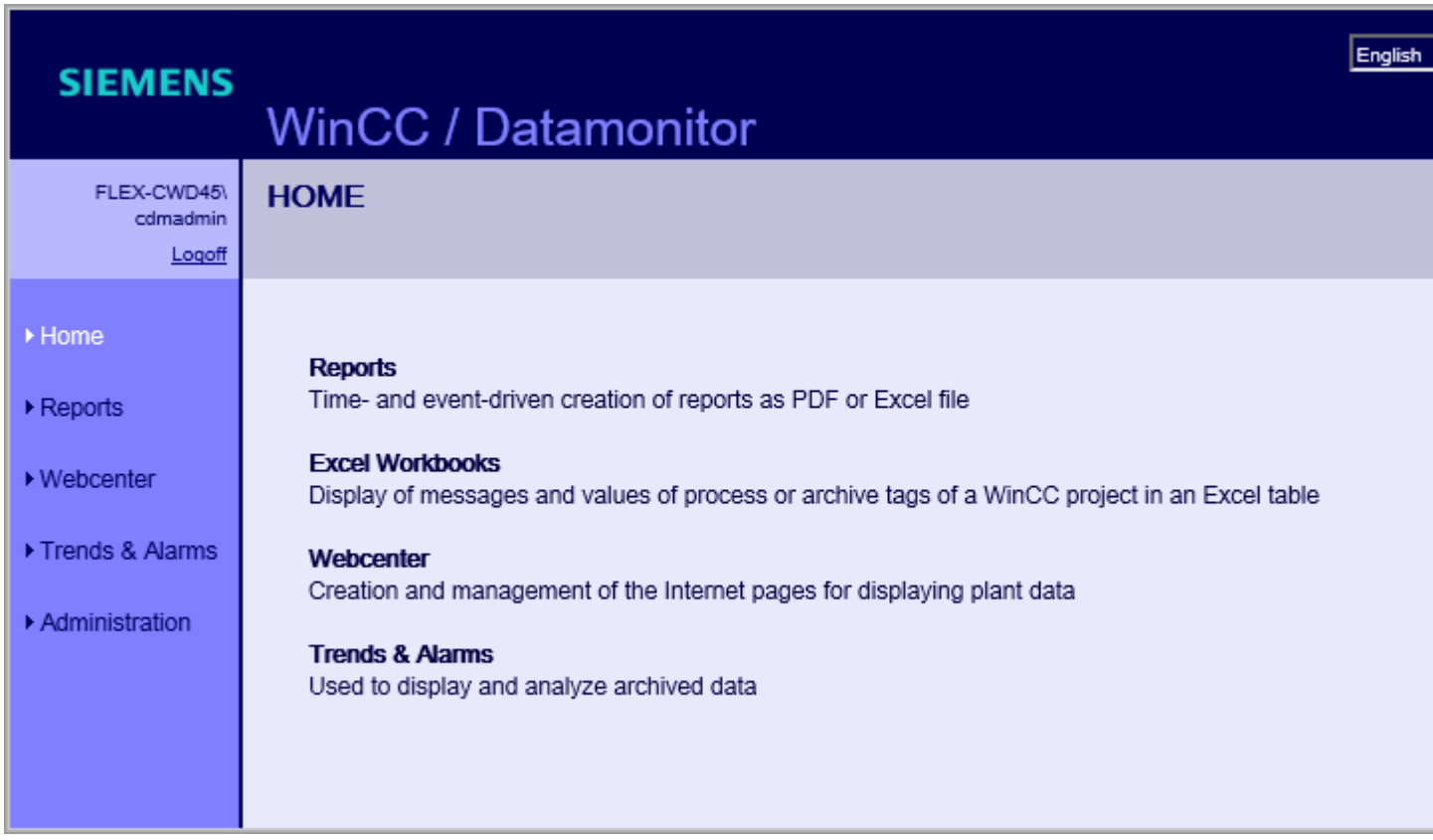
Requirements

- User has been created in the Windows user group "SIMATIC Report Administrators".
- The WinCC project on the DataMonitor Server is in Runtime.
- A user is created in WinCC.

Procedure

To access the Web page of the DataMonitor Server, proceed as follows:

1. Open the MS Internet Explorer on the DataMonitor client.
2. Enter the name of the DataMonitor server in the format "http://<servername>" in the URL. Confirm the entry with "Enter".
3. The logon dialog opens. Enter the name of a Windows user in the "User name" field. Enter the respective password and confirm with "OK".
   The start page with the DataMonitor functions will be displayed.



Result

The start page with the DataMonitor functions will be displayed on the DataMonitor client. The use of the functions depends on the user's access right.

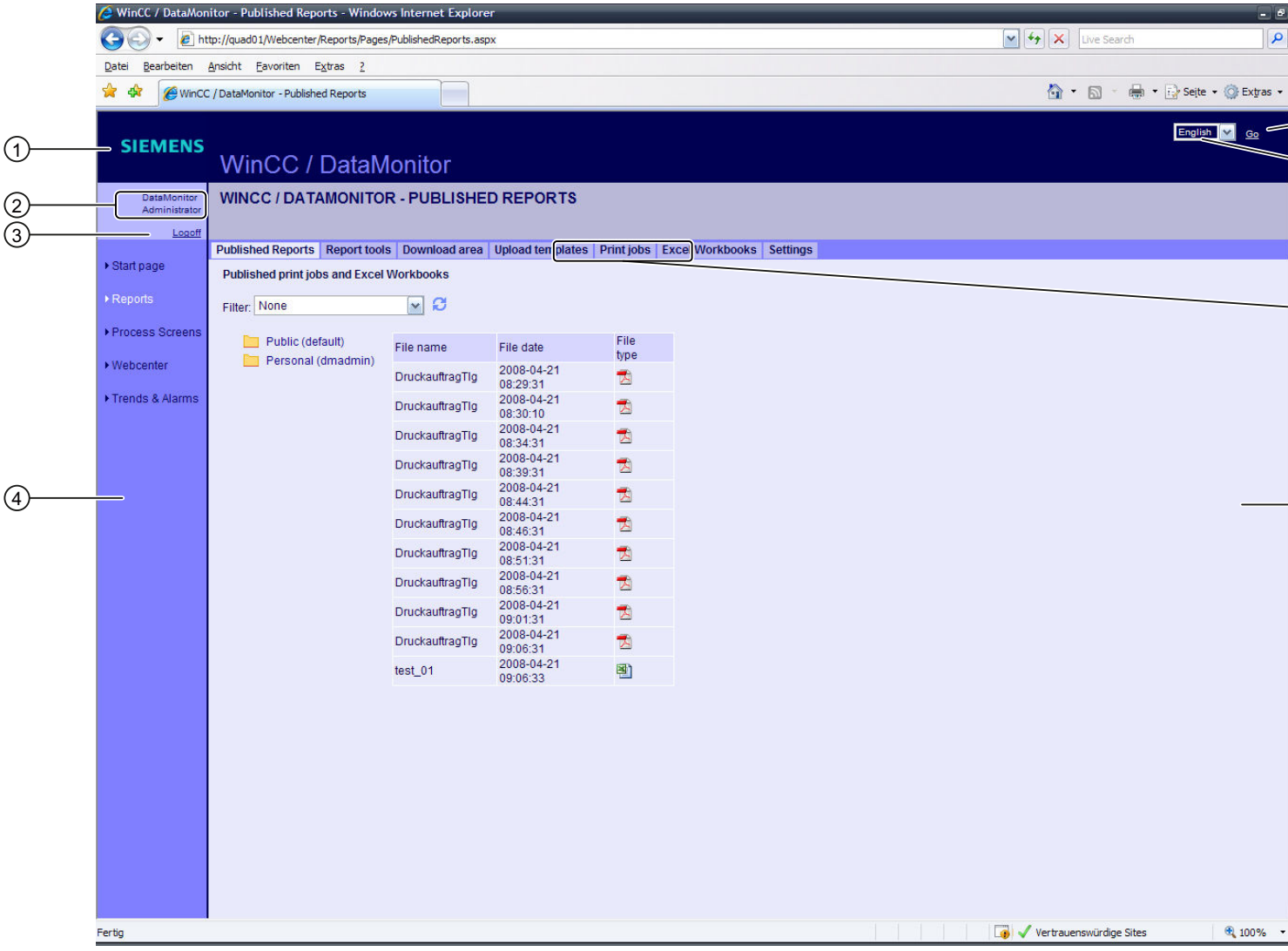
See also

Working with WinCCViewerRT (Page 87)

2.3.4.3 General Operations of the DataMonitor Client (RT Professional)

Introduction

The DataMonitor Web pages have the following structure:



① Header
② Current user
③ Link to logoff
④ Navigation control
⑤ Icon to hide the header
⑥ Interface language selection field
⑦ Tabs depending on the currently displayed contents
⑧ Contents

Switching the user interface language

1. Choose the desired language from the selection field in the header.
   The GUI language is changed.

Hide and show the header

1. To hide the header line, click the symbol .
   This provides more room for displaying the content.
2. To show the header line again, click the symbol .

Logoff

1. To log off from the DataMonitor server, click the "Log off" link.
2. Close Internet Explorer.
   When you close Internet Explorer, the used license will be released immediately.

2.4 Working with WinCCViewerRT (RT Professional)

2.4.1 Setting up WinCCViewerRT (RT Professional)

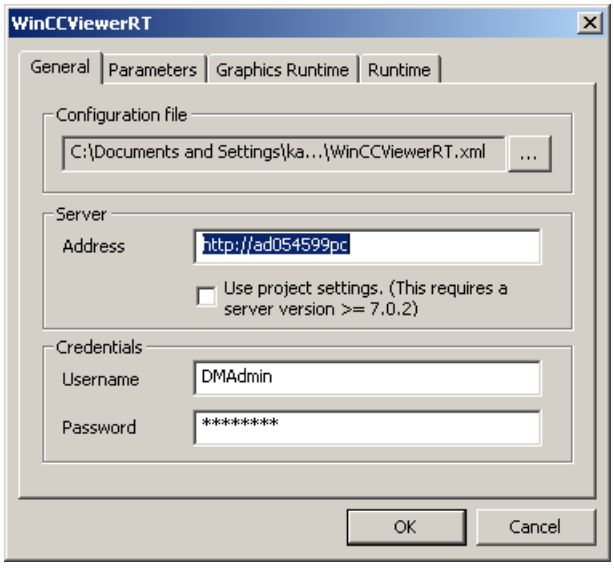
Requirement

- On the server PC
  - The DataMonitor Server is installed.
  - A license key is installed.
  - The WinCC project is in Runtime.
  - The WinCC screens are configured for Web access and published.
- On the client PC
  - DataMonitor Client is installed.

Procedure

Set up WinCCViewerRT as follows:

1. In the Start menu, select "Start > All Programs > Siemens Automation > Option and Tools > HMI Tools" > WinCCViewerRT".
2. Enter the logon data in the "General" tab:



   - Server address: http://<server name>, or http://<IP address>
   - User name and password:
3. In the "Parameters" tab, specify the Runtime language and whether to disable keystrokes that the operator uses to change to other programs.
4. Define the WinCC Runtime Professional properties in the "Graphics Runtime" tab:
   - Start screen
   - Configuration file for screen navigation
   - Window attributes
   - Illegal user actions
5. Define additional user actions in the "Runtime" tab.
   - Automatic logout
   - Enable screen keyboard.
   - Use <Ctrl+Alt+Del> to switch to the Task Manager and to the operating system. This setting is only valid for the on-screen keyboard.
   - Open the "WinCCRTViewer" dialog by means of keystroke.
     You can change the default keystroke <Ctrl+Alt+P>.
6. Close the dialog with "OK".

Result

The WinCCViewerRT is configured. When the dialog is closed, the connection to the DataMonitor server is established. The settings are saved to the configuration file "WinCCViewerRT.xml". The settings in the configuration file are used at the next start of WinCCViewerRT.

The configuration file is stored in the directory "C:\Users\<User name>\Appdata\LocalLow \Siemens\SIMATIC.WinCC\WebNavigator\Client". Under <User name>, enter the name of the user logged-on when the file is created. This allows different configurations to be used, depending on the logged on user. WinCCViewerRT applies the interface language from WinCC.

Renaming or removing WinCCViewerRT.xml

When you rename or remove the file WinCCViewerRT.xml, the configuration dialog of WinCCViewerRT is opened during the start. Reconfigure WinCCViewerRT, or select a different configuration file.

2.4.2 Display screens (RT Professional)

Requirements

- A license key is installed on the DataMonitor Server.
- The WinCC project on the DataMonitor Server is in Runtime.
- The WinCC screens are configured for Web access and published.
- A WinCC user with the authorization no. 1002 "Web access - view only" is created.

Procedure

To view screens, proceed as follows:

1. In the Start menu, select "Start > All Programs > Siemens Automation > Option and Tools > HMI Tools" > WinCCViewerRT".
2. Log on to the WebNavigator server:
   - If the user and password are configured in "WinCCViewerRT", no logon dialog displayed.
   - If no user and password was configured in "WinCCViewerRT", the logon dialog displayed. Enter the user name and the password of the WinCC user. Click "OK".
3. Press the <Ctrl+Alt+P> keystroke to change the user. The "WinCCViewerRT" dialog opens. Enter the user name and password on the General" tab.
   You can also select the xml file that contains this data.

Result

The Web Viewer connects to the activated WinCC project. The screens of the WinCC project are displayed.

The cursor is a "View only cursor" and indicates that process-related operations are not allowed.



Certain operations are still possible, such as opening the properties dialog of an online trend control.

If necessary, you can use your own cursor symbol as a "View only cursor". See "Configuring runtime settings (DataMonitor) (Page 75)" for more detailed information.

2.5 Working with the WebCenter (RT Professional)

2.5.1 Administration (RT Professional)

2.5.1.1 User Groups and Directories (RT Professional)

Overview

WebCenter pages and reports are stored in directories on the DataMonitor Server.

Its standard complement of directories is as follows:

- "Public"
- "Private"
  Every user has a "Private" directory. Only the respective user has access rights to this directory.

More information on setting up directories can be found in chapter "Creating Directories (Page 93) ".

Windows User Groups

The user groups "SIMATIC Report Administrators" and "SIMATIC Report Users" are created during the installation of the DataMonitor Server. You can create more user groups. More information on setting up user groups and users can be found in chapter "Assigning Access Rights (Page 94) ".

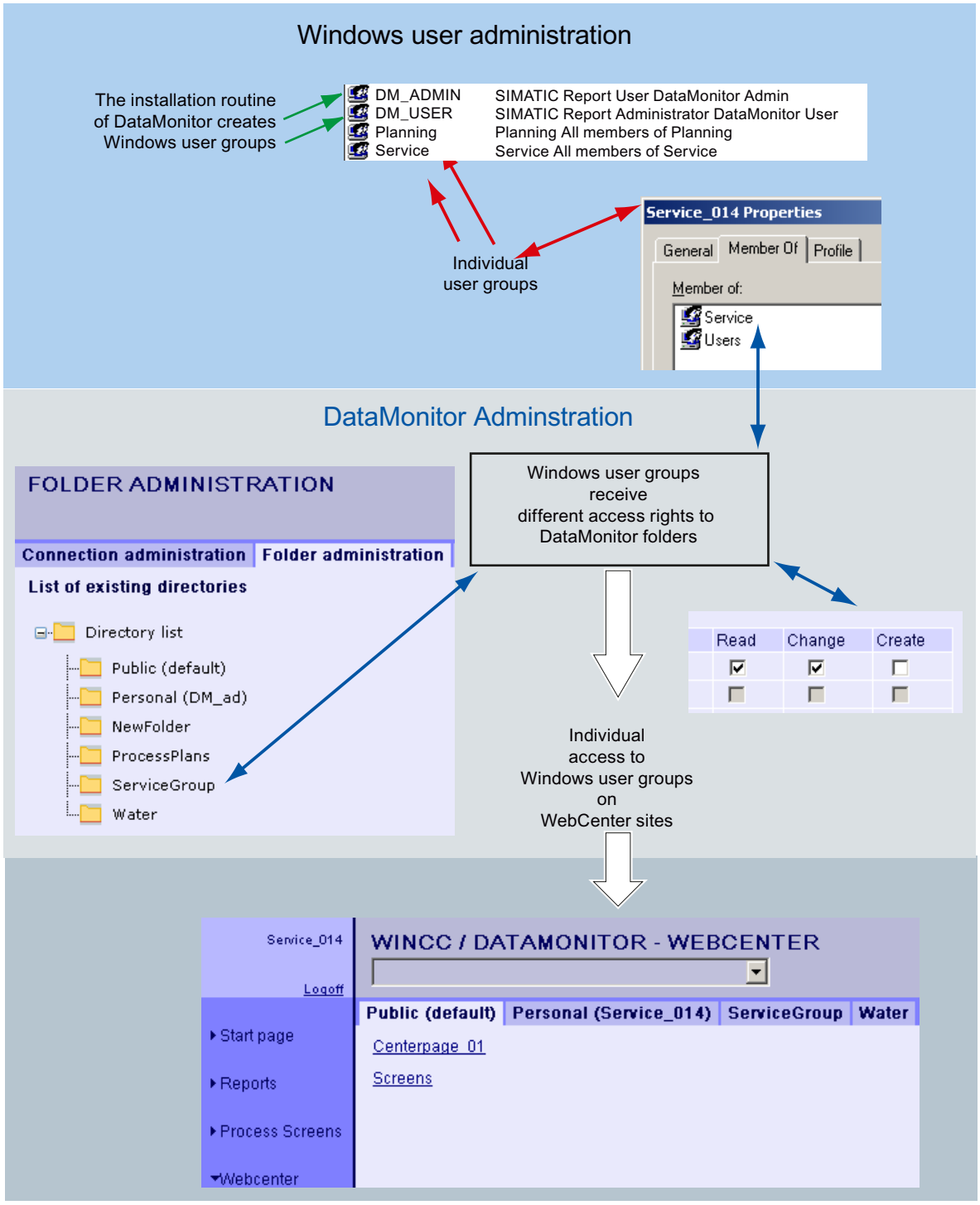
To access the DataMonitor, you can assign all members of a user group with the same access rights to the directory of the DataMonitor server.

The following access authorization is possible:

- Read
- "Change"
- "Create"

A user, as a member of a user group, only has access to a directory if the respective user group has access rights to that directory. This permits user group-specific access. More information on assigning access authorization can be found in chapter "Defining users in Windows (Page 81) ".

The following screen shows the basic user administration for the WebCenter.


Windows user administration
The installation routine of DataMonitor creates Windows user groups
DM_ADMIN SIMATIC Report User DataMonitor Admin
DM_USER SIMATIC Report Administrator DataMonitor User
Planning Planning All members of Planning
Service Service All members of Service
Individual user groups
Service_014 Properties
General
Member Of
Profile
Member of:
Service
Users
DataMonitor Adminstration
FOLDER ADMINISTRATION
Connection administration
Folder administration
List of existing directories
Directory list
Public (default)
Personal (DM_ad)
NewFolder
ProcessPlans
ServiceGroup
Water
Windows user groups receive different access rights to DataMonitor folders
Read
Change
Create
Individual access to Windows user groups on WebCenter sites
Service_014
Logoff
WINCC / DATAMONITOR - WEBCENTER
Public (default)
Personal (Service_014)
ServiceGroup
Water
Start page
Reports
Process Screens
Webcenter
Centerpage_01
Screens

2.5.1.2 Creating Directories (RT Professional)

Introduction

You store WebCenter pages in directories. The following directories exist as defaults:

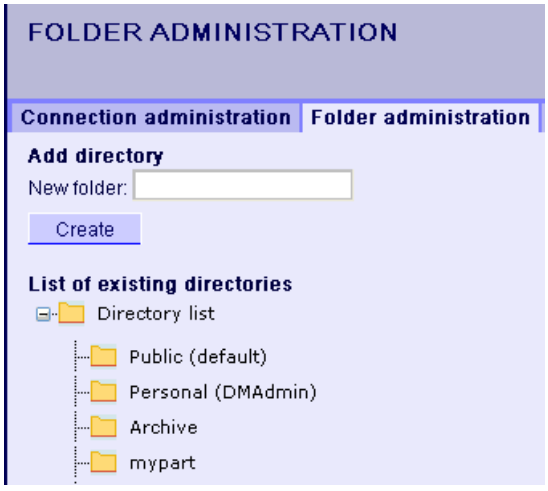
- "Public"
- "Private"
  Every Windows user has their own "Private" directory.

Requirement

- The logged on user is a member of the Windows user group "SIMATIC Report Administrators".
- The DataMonitor start page is open.

Procedure

1. Click in the start page "Webcenter > Administration".
2. Click the "Directory administration" tab.



3. Enter the name "mypart" in the "New directory" field.
4. Click the "Create" button.

Result

You have created the directory "mypart". The user administration is opened automatically. Specify the access rights for the folder. You can also exit the page and configure the access rights at a later time.

2.5.1.3 Assigning Access Rights (RT Professional)

Introduction

In the WebCenter, directories are created in which, for example, the WebCenter pages are stored. You can assign different access rights for the individual directories to Windows user groups.

The following access authorization is possible:

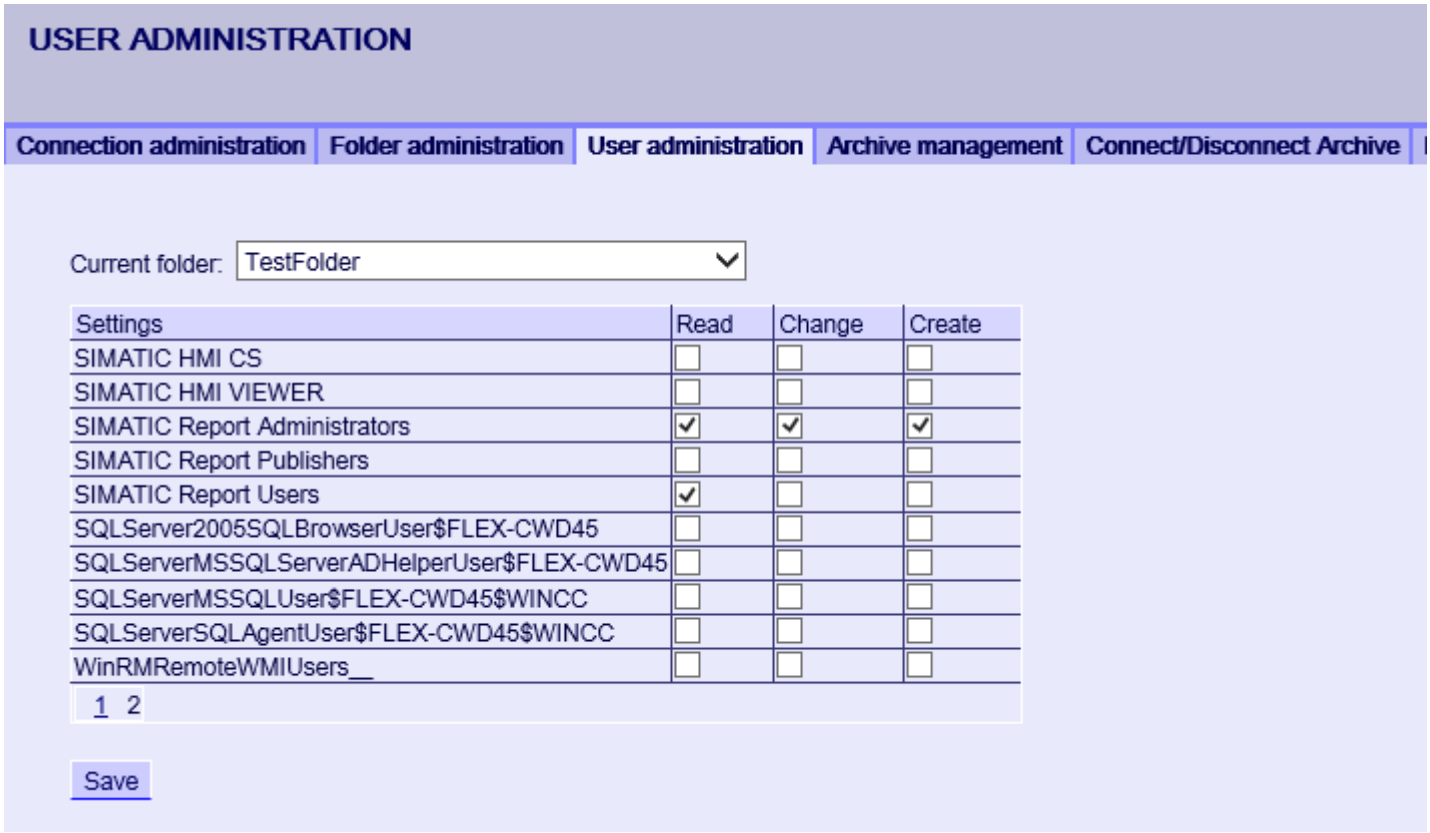
- Read
- "Change"
- "Create"

Requirement

- The logged on user is a member of the Windows user group "SIMATIC Report Administrators".

Procedure

1. Click in the start page "Webcenter > Administration".
2. Click the "User administration" tab.



3. Select the desired directory from the "Current Directory".
   All existing Windows user groups are listed.
4. Activate the access rights in the line of the desired Windows user group.
5. Click "Save".

Result

The access rights have been configured for the desired directory.

2.5.1.4 Establish a connection to the winCC data (RT Professional)

Create connection and set up language (RT Professional)

Introduction

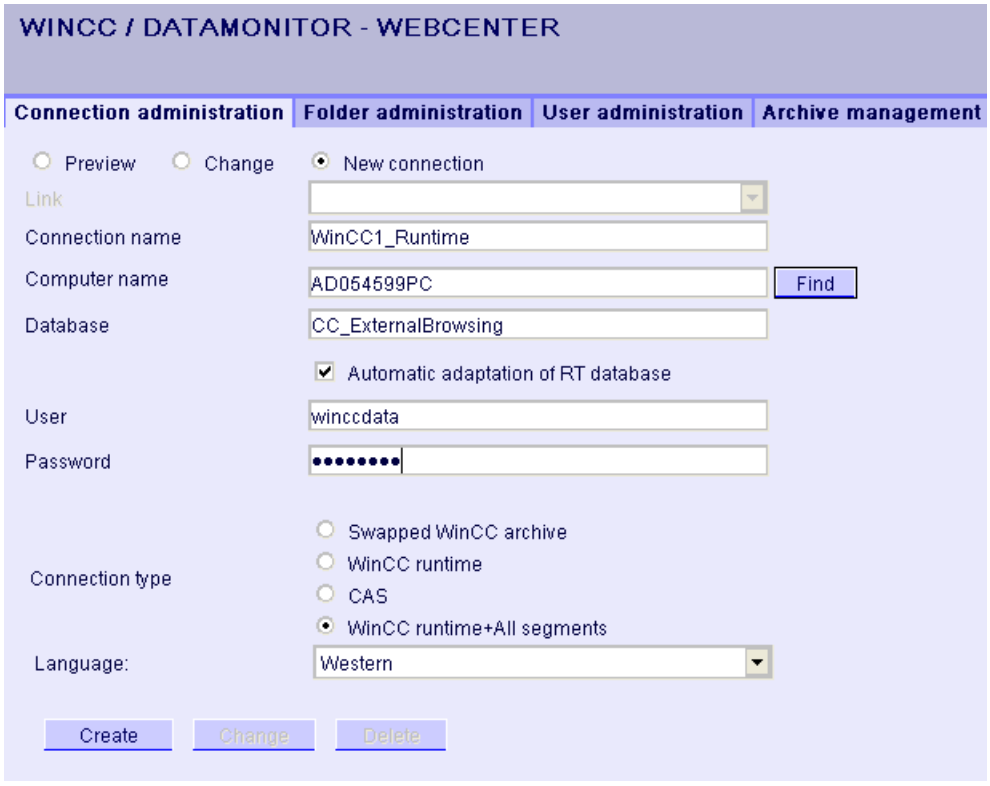
A connection is configured for access to the data in the "Webcenter". A connection is set up for each data source, e.g. WinCC server. The connection is required for example for the function "Trends and Alarms" and the WebCenter page.

Requirement

The logged on user is a member of the Windows user group "SIMATIC Report Administrators".

Procedure

1. Click in the start page "Webcenter > Administration".
2. Click the "Connection administration" tab.



3. Choose the language that corresponds with the linguistic region of the server or log to be linked in "Linguistic region".
   If you do not select the language that corresponds with the respective linguistic region, characters may be displayed incorrectly on the page.
4. Select "New connection".
   After the new installation, no selection is possible in the "Connection" field, as no connections have been configured yet.
5. Enter a name in the field "Connection name", e.g. "WinCC1_ Runtime".
   Any name can be selected. However, it should contain a reference to the selected connection type. Do not use spaces and special characters in the connection name.
6. Enter the name of the PC whose data you would like to access in the "Computer name" field. As an alternative, select the name of the PC using the "Find" button.
7. Enter the desired database in the "Database" field. Alternatively, select the database using the "Find" button.

8. Choose the desired option in the "Connection type" area.
   - "Swapped WinCC Log"
     Further steps are required to access data from logs. For additional information, refer to "Connecting and Disconnecting Swapped Logs (Page 97)".
   - "WinCC Runtime"
     The Runtime database of the selected WinCC project is entered in the "Database" field.
   - CAS
     CAS is not available in this version.
   - WinCC Runtime + all segments
     "CC_ExternalBrowsing" is entered in the "Database" field.
9. Activate "Automatic adaption of RT database". When a segment is changed, the name of the database is adjusted in the connection administration.
10. Click the "Create" button.

Result

The connection to the data source is created and can be selected in "Connections".

Connecting and Disconnecting Swapped Logs (RT Professional)

Configuring a directory (RT Professional)

Introduction

To access data from swapped WinCC logs (log backup file), these logs must be connected to an SQL server again.

You can connect all or individual log backup files of a directory to the SQL server.

Requirement

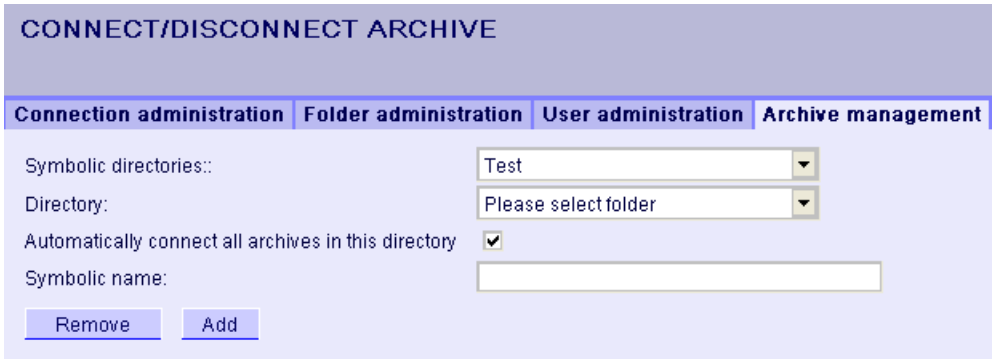
- Write protection of the log backup file has been removed
  Archive backup files are write protected. Create a backup copy of the file before connecting and remove the write protection of the copied log backup file.
- The log backup files are available on the local drive.
- The directories in which the log backup files are set for sharing.
  - The directory must be set for sharing in the Windows Explorer before you start the DataMonitor Server.
  - If you set the directories for sharing later, restart the DataMonitor Server.
- The user group "SIMATIC HMI VIEWER" must have "full access" to the directories.
- The logged on user is a member of the Windows user group "SIMATIC Report Administrators".

- Windows Server 2003 / 2008: "Network service" has been added to the "Print operators" group.
- Windows 7: "Network service" has been added to the "Power user" group.
- Windows XP: "ASPNET" has been added to the "Power user" group.

Procedure

Proceed as follows to create a symbolic directory:

1. Click in the start page "Webcenter > Administration".
2. Click the "Archive administration" tab.



3. Enter a unique symbolic name name in the "Symbolic Name" field.
   The name should only contain the characters permitted in the SQL syntax. You use the symbolic name for access via the DataMonitor client.
4. In "Directory", select the directory in which the log backups are located.
   You can only select directories that have been set for sharing.
5. To connect all existing log backups of the directory, select "Automatically connect all logs in this directory".
   To connect all individual log backup files of the directory, clear "Automatically connect all logs in this directory".
6. Click "Add".

Result

You have created the symbolic directory "Test". If you have cleared "Automatically connect all logs in this directory", define the log backups to be connected on the page "Connect/disconnect logs (Page 99)".

To disconnect logs, clear the desired logs on the page "Connect/disconnect logs"

Note

Connected logs on changeable media

Before changing the media in the drive you need to disconnect the logs on this medium. After changing the medium, check whether the logs are connected on the new medium.

Deleting a symbolic directory

To remove a directory containing logs from the list of symbolic names, disconnect all logs contained in the list. The status of the logs can be seen on the page "Connect/disconnect logs".

Connecting and Disconnecting Logs (RT Professional)

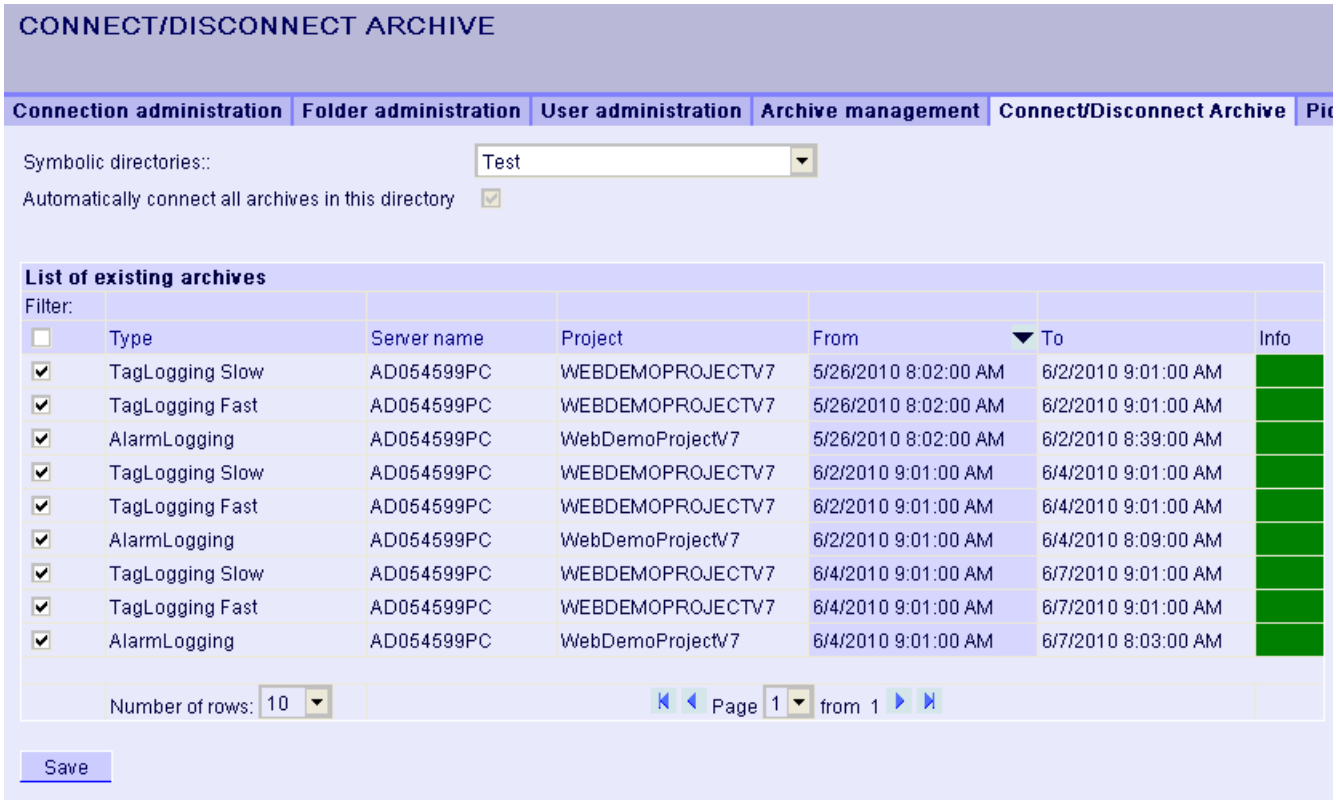
Requirement

- Write protection of the log backup has been removed
  Log backups are write protected. Create a backup copy of the log before connecting and remove the write protection of the copied archive.
- The logged on user is a member of the Windows user group "SIMATIC Report Administrators".
- You have configured the symbolic directory "Test" (Page 97).

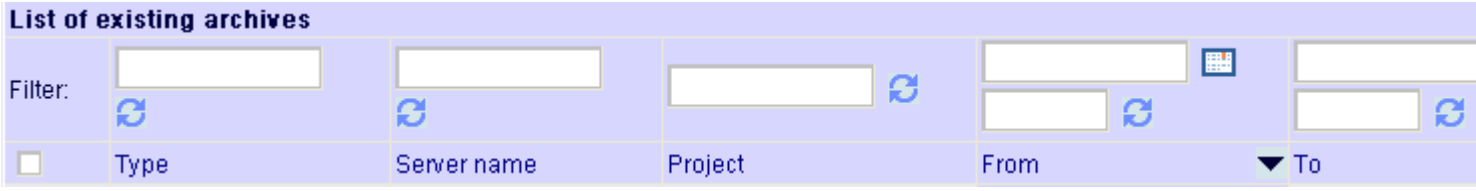
Procedure

To connect or disconnect individual log backups, proceed as follows:

1. Click in the start page "Webcenter > Administration".
2. Click the "Connect/disconnect logs" tab.



3. Select the directory "Test" in "Symbolic directories". Existing logs are displayed in a list. The "Info" column provides information about the status.
   - Green: Connected
   - Red: Disconnected
4. To restrict the display, click "Filter".



5. Enter the desired time period and click "Refresh display".
6. To connect a single archive, select the desired log in the "List of existing logs". Click "Save". The status "Green" indicates that the log is connected.
7. To disconnect a single archive, clear the desired log in the "List of existing logs". Click "Save". The status "Red" indicates that the log is disconnected.

Alternative procedure

Archive backups can be connected in the following ways:

- VB function using the "Restore" method. For detailed information, refer to "Restore".
- Automatic Connection: If you copy the log backups to the "CommonArchiving" folder, the logs are connected to the project in Runtime.
- Using Archive Connector (Page 100).

Result

Logs are connected. If you connect signed logs, which have been changed after the swap, an alarm is output.

Connecting Logs using WinCC Archive Connector (RT Professional)

Introduction

With the Archive Connector, already swapped out WinCC logs can be reconnected to an SQL Server.

Requirement

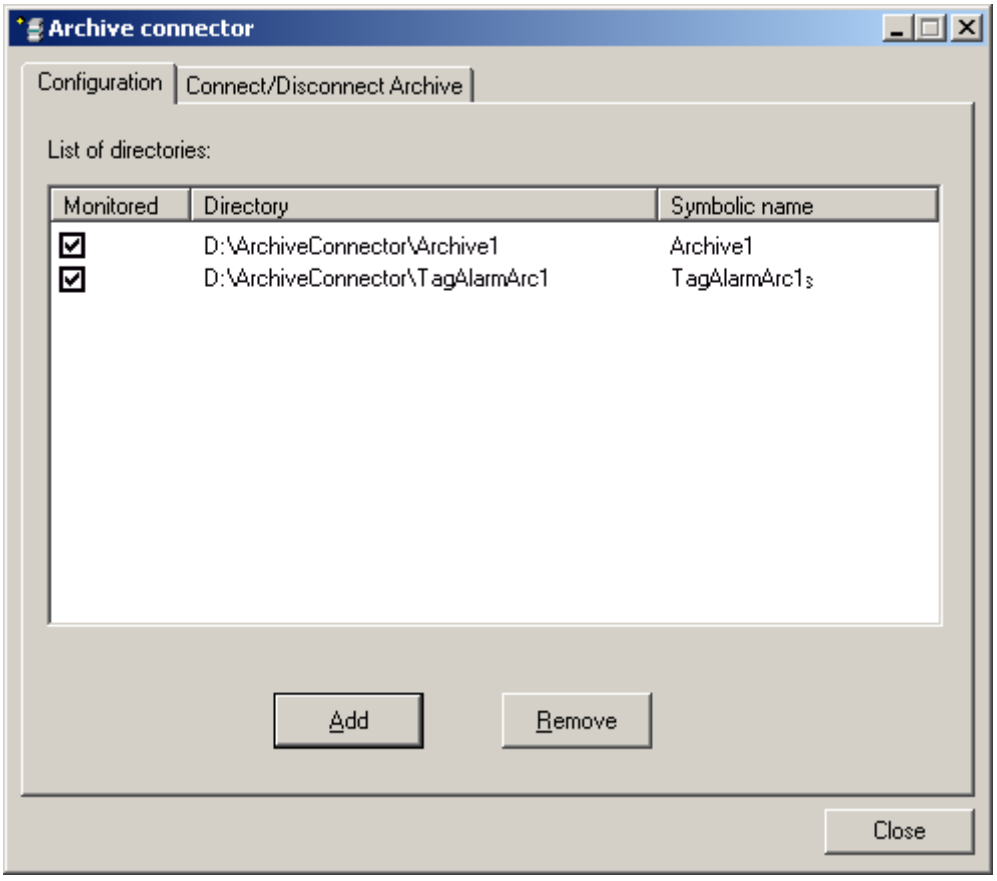
- Write protection of the log backup file has been removed
  Archive backup files are write protected. Create a backup copy of the file before connecting and remove the write protection of the copied log backup file.
- The log backup files are available on the local drive.

- The directories in which the log backup files are set for sharing.
- The user group "SIMATIC HMI VIEWER" must have "full access" to the directories.
- The logged on user is a member of the Windows user group "SIMATIC Report Administrators".

Procedure

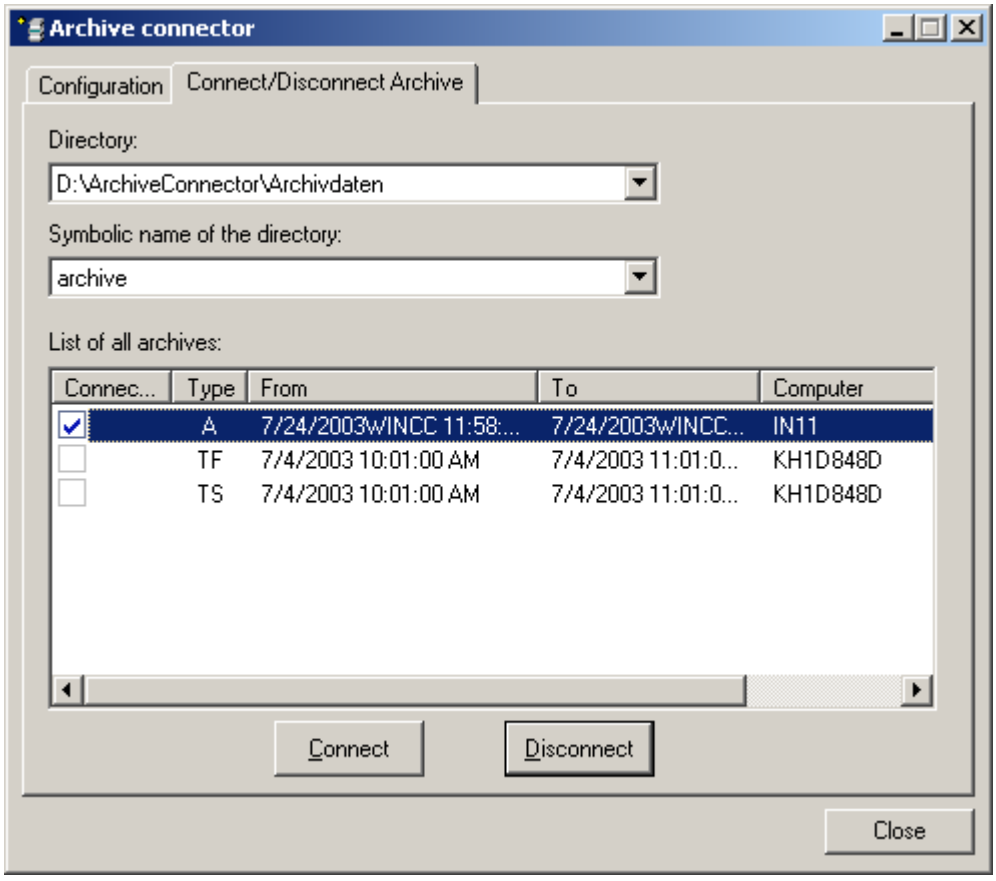
To connect log backup files, proceed as follows:

1. Start the "Archive Connector".



2. Click "Add" in the "Configuration" tab. The "New Directory" dialog is opened.
3. Navigate to the directory in which the log backup files are stored.
4. Enter a symbolic name for the directory. Click "OK." The directory is displayed on the "Configuration" tab.

5. Click the "Connect/Disconnect Logs" tab. All the logs in the selected directory are listed in the "Connect/Disconnect Logs" tab.



6. Select the desired log and click "Connect".

Result

A connection has been created and the desired log backup files are connected to the SQL server.

The connection status of each log is displayed on the "Connect/Disconnect Logs tab". "From" and "To" columns contain the archiving period denoted in the local time zone.

The "Type"column contains the details for log type.

"A"	Alarm logs
"TF"	Fast data log
"TS"	Slow data log

2.5.2 Creating static process screens for the Web Center (RT Professional)

Introduction

In the screen management, specify the screens that you need for the Web element "Static process screens".

The DataMonitor Server generates copies of the screens at configurable cyclic intervals and provides these to the DataMonitor Client and the form of static process screens.

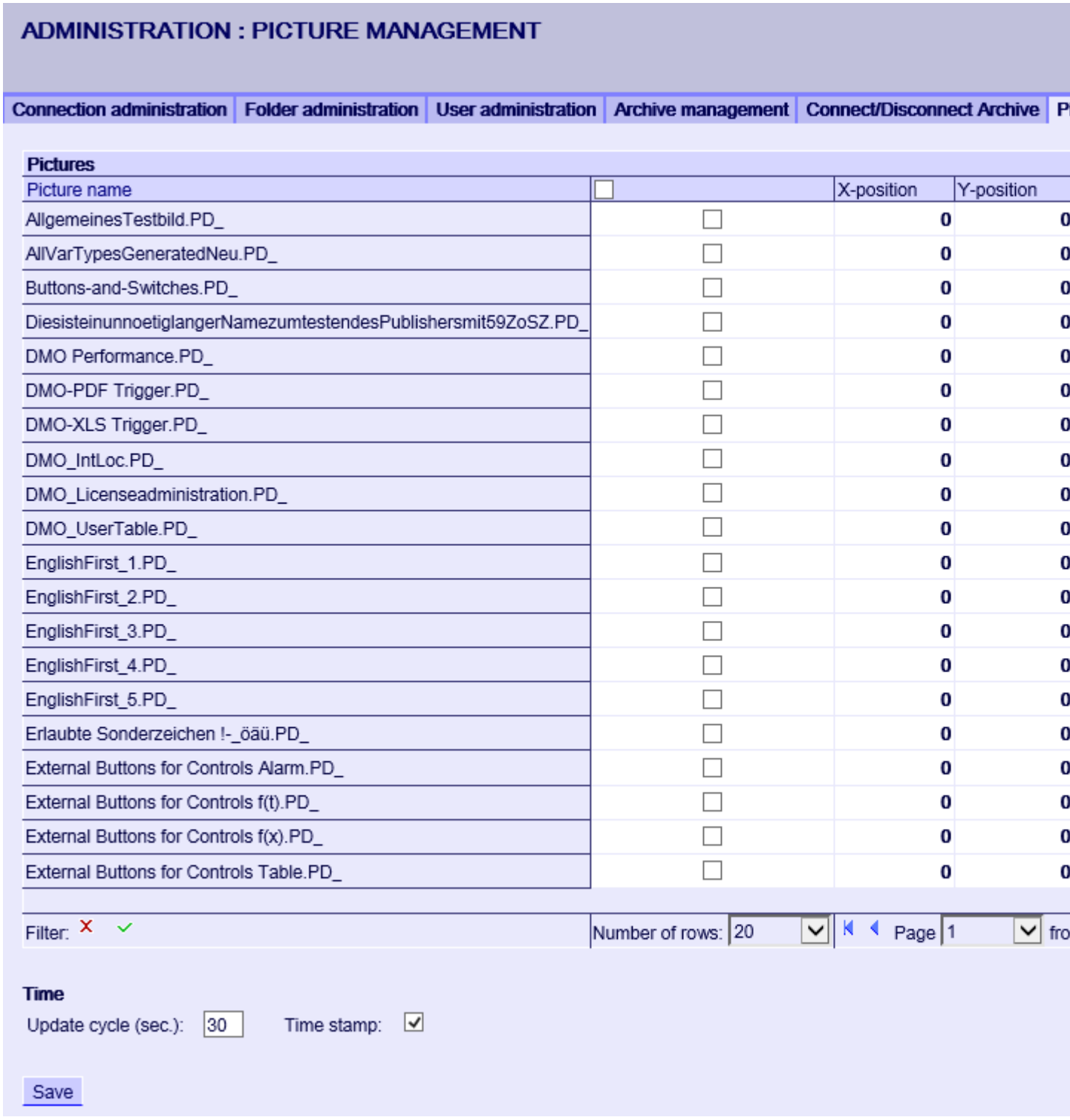
Requirement

- The logged on user is a member of the Windows user group "SIMATIC Report Administrators".
- The WinCC screens are configured for Web access and published. See "Configuring WinCC screens for Web access (Page 73)" for additional information.
- The DataMonitor start page is open.
- The "Screen management" tab is open.

Creating static process screens for the Web Center

1. Select the screens.
   – To select all screens, activate the check box in the column header.

– To select individual screens screens, activate the check box leading the relevant screen.



2. To display only part of the screen, define the following:
   – X position: Start positions in x direction in pixels

- Y position: Start positions in y direction in pixels
- Width: Width of screen in pixels
- Height: Height of screen in pixels

3. To set a language for a process screen, select the required language in the drop-down list.
4. To output the time at which the static process screen screen was created by the DataMonitor Server, activate "Stamp".
   The date time are shown in the static process screen.
5. To change the update cycle, enter the desired value in "Update time interval".
   Select this cycle as large as possible. A cycle that is too small leads to performance problems.
6. Click "Save".

Result

The DataMonitor Server generates the static process screens from the selected screens. The static process screens can be configured in the Web part "Static process screens".

Removing static process screens

To remove static process screens, select the check box at the relevant entry in the "Delete graphic object" column. Click "Save" to remove the static process screen or copy. The deleted static process screens can no longer be configured in the Web part "Static process screens".

Finding screen names or limiting the view

Use a filter to find screen names, or to limit the view to specific screen names.

At the "Filter" entry, click to show the filter above the table. Enter the search term in the text field and then click <Enter>.

To hide the filter, click .

2.5.3 Create a layout template for WebCenter pages (RT Professional)

Introduction

You require a layout template to create a WebCenter page. Many prefabricated layouts have been installed during the installation. Additionally, you can create your own Layout Templates.

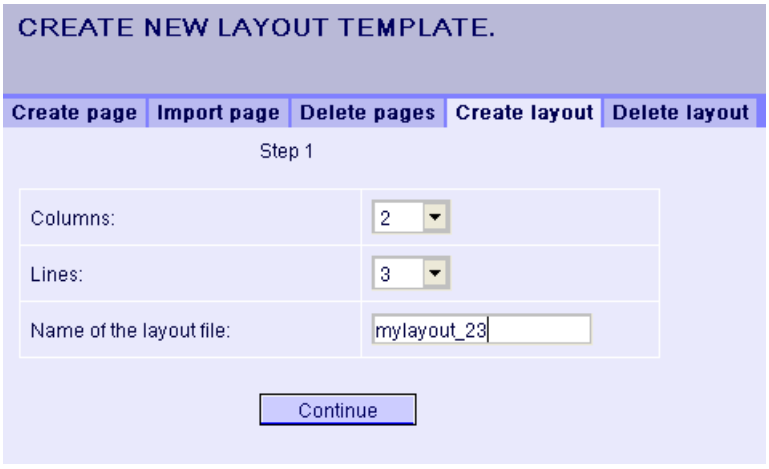
Requirements

- The logged on user is a member of the Windows user group "SIMATIC Report Administrators".
- The DataMonitor start page is open.

Procedure

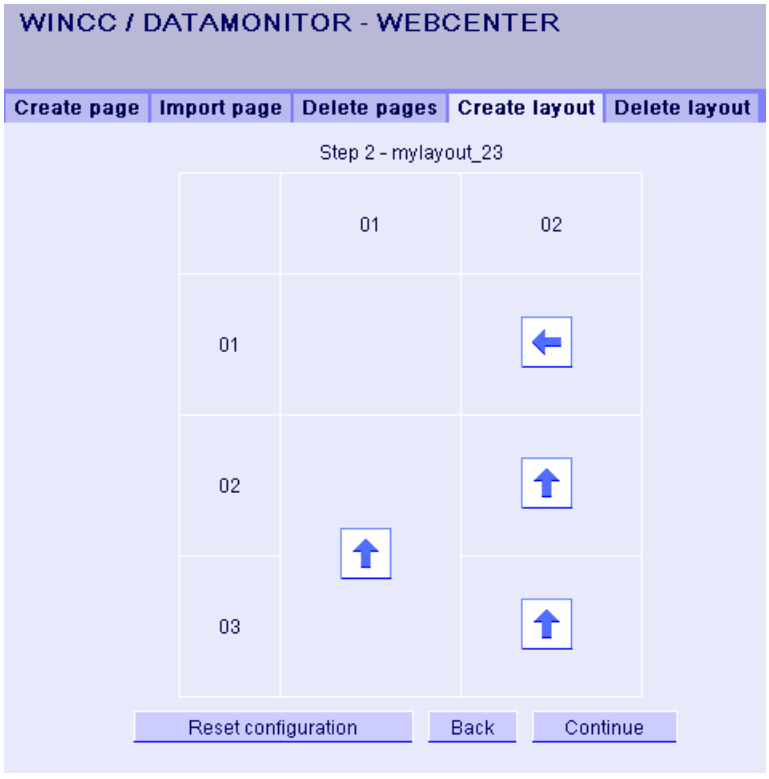
Proceed as follows to create your own layout template:

1. Click "WebCenter > Configuration" in the start page.
2. Click the "Create layout" tab.



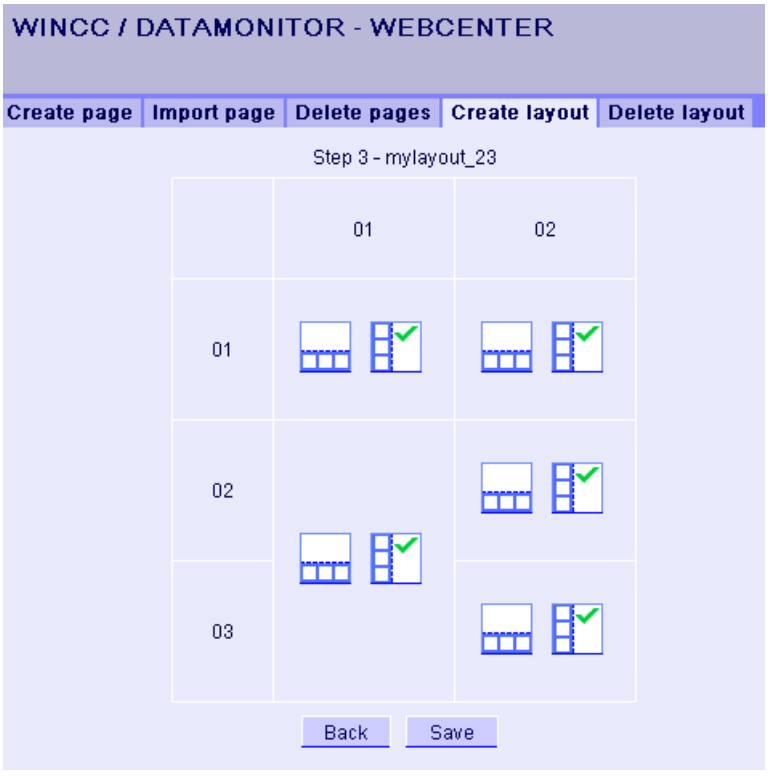
3. Define the number of columns and rows.
4. Enter the name "mylayout_23" in the "Name of the layout file" field. Click "Next."

5. If required, group the table fields. For this, click the appropriate arrow symbol, such as "Arrow up", in the desired field, for example line 3 / column 1.
   The modified view will be displayed.



To restore the original table form, click "Reset configuration".

6. Click "Next."



7. You define the order of the Web parts in the table fields.
   If necessary, select the corresponding symbol in a table field to place the web parts vertically or horizontally.
8. Click "Save".

Result

The layout template "mylayout_23" is created. You can use the layout template as a template for creating a WebCenter page.

2.5.4 Create a WebCenter page (RT Professional)

Introduction

Requirements

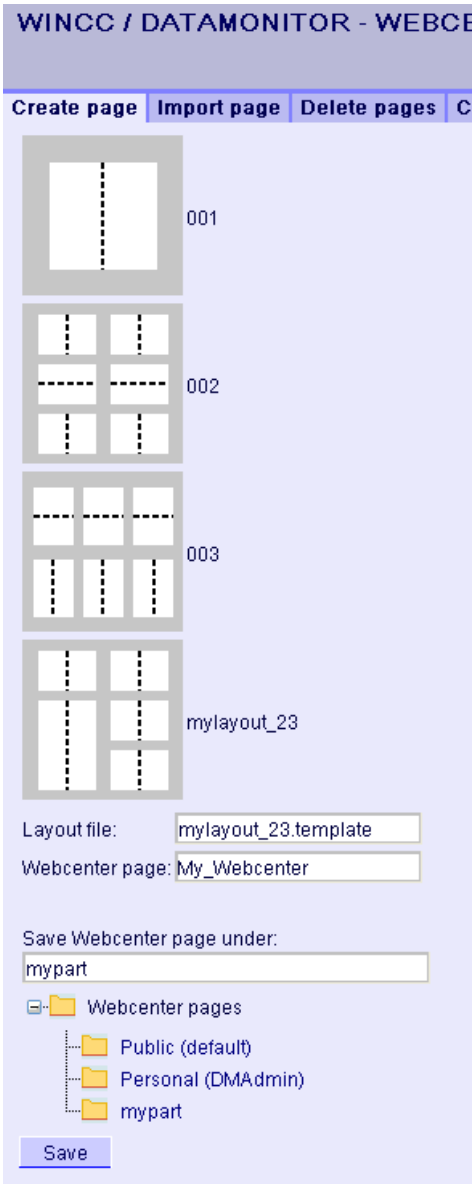
- The directory "myPart" is set up.
- The user logged on is a member of the Windows user group "SIMATIC Report Administrators" or "SIMATIC Report Users".

- The Windows user groups have the "Change" or "Create" access rights to the directory.
- The DataMonitor start page is open.

Procedure

1. Click "WebCenter > Configuration" in the start page.
2. Click the "Create Page" tab.
3. Click the desired layout template. The file name is displayed in the "Layout file" field.
4. Enter a name in the "WebCenter page" field, for example "My_Webcenter".

5. Click the directory in which the WebCenter page is stored. The selected directory is displayed in the field "Save WebCenter page as".



6. Click "Save".

Result

The WebCenter page has been created and saved.

2.5.5 Insert Web parts into the WebCenter page (RT Professional)

Introduction

You combine Web parts to create the contents of the WebCenter pages.

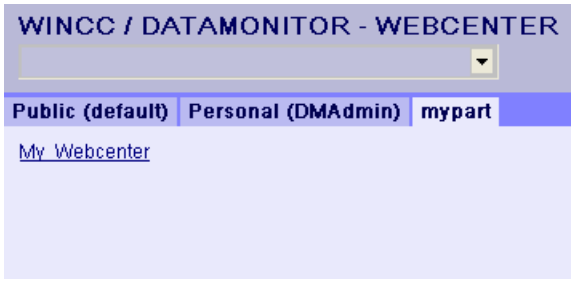
Requirements

- The directory "myPart" is set up.
- The WebCenter page "My_Webcenter" is stored in the directory.
- The user logged on is a member of the Windows user group "SIMATIC Report Administrators" or "SIMATIC Report Users".
- The Windows user groups have the "Change" or "Create" access rights to the directory.
- The DataMonitor start page is open.

Procedure

Proceed as follows to insert Web parts in the WebCenter page:

1. Click "WebCenter > Pages" in the start page.
2. Click the "myPart" tab.



3. Click the "My_Webcenter" entry.

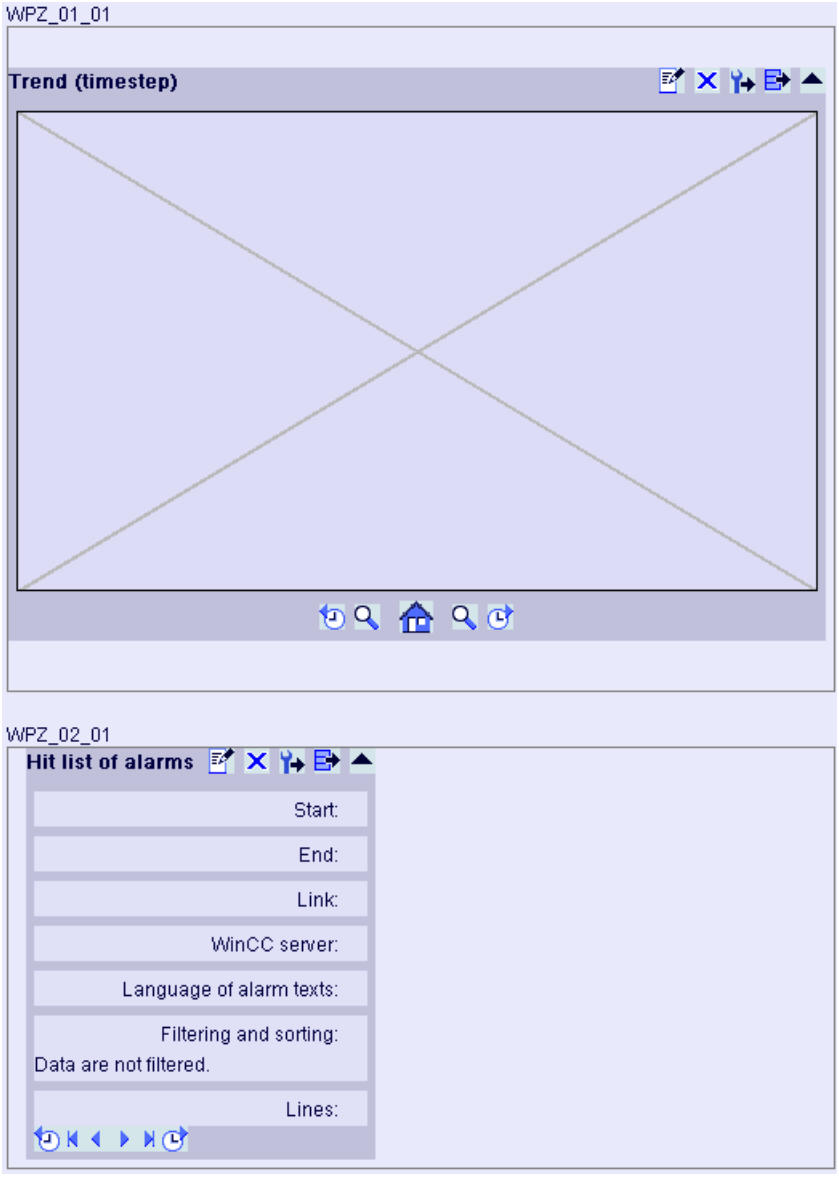
4. To add Web parts, click the symbol on the right side.
   The available Web parts are listed.
   If you have exported web parts that have already been configured, they are listed under "Imported web parts". If necessary, insert these web parts into your WebCenter page.



5. Select "Trend (Timestamp)".
6. Select the entry "WPZ_01_01" and click "Add".
7. Select "Alarm hit list".
   If you insert several Web parts in a spreadsheet field, they are arranged horizontally or vertically. Specify this arrangement when creating the layout template.
8. Select the entry "WPZ_02_01" and click "Add".
9. Click "Close."

Result

Web parts to display data have been inserted into the WebCenter page "My_Webcenter". The current summary of the WebCenter page is displayed.



2.5.6 Configure Web parts within WebCenter pages (RT Professional)

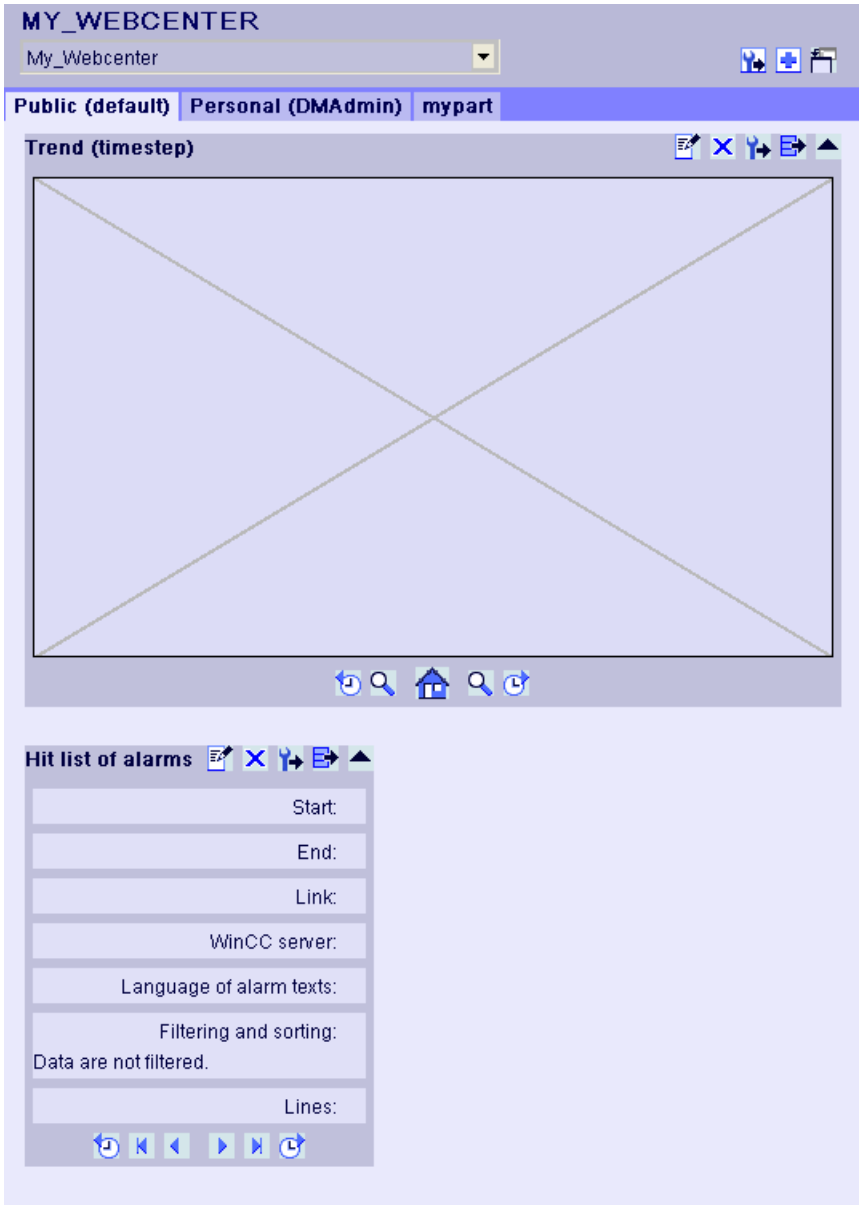
Requirement

- The user logged on is a member of the Windows user group "SIMATIC Report Administrators" or "SIMATIC Report Users".
- The Windows user groups have the "Change" or "Create" access rights to the directory.
- The WebCenter page "My_Webcenter" is open.
- The WinCC project is in Runtime.

Procedure

To configure Web parts within WebCenter pages, proceed as follows:

1. Click the icon in the desired Web part. The configuration dialog opens.



2. Configure the web part.
   - Displaying process values in a table (Page 119)
   - Displaying process values in a diagram (Page 121)
   - Displaying messages in the alarm table (Page 123)
   - Displaying the hit list of messages (Page 127)

– Displaying statistics function for process values (Page 128)

3. To change the position of the web part, move the web part to the desired position with the mouse.

More Operational Capabilities

The following operating options are available:

	Delete Web part
	Minimize Web part
	Maximize Web part
	Export Web part
	Export configuration of the Web part as an XML file

2.5.7 Deleting WebCenter Pages and Layout Templates (RT Professional)

Requirement

Deleting layout templates

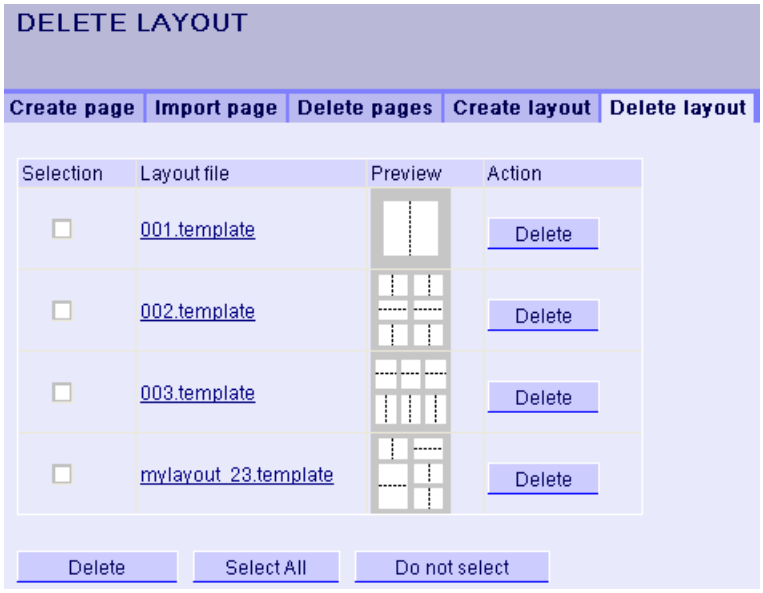
- The user is a member of the Windows user group "SIMATIC Report Administrators".
- The DataMonitor start page is open.

Deleting a WebCenter page

- The logged-in user must have "Create" access rights for the directory in which the page to be deleted is stored.
- The DataMonitor start page is open.

Deleting layout templates

1. Click "WebCenter > Configuration" in the start page.
2. Click the "Delete layout" tab.



3. Delete the selected files.
   - To delete several layout files, select the "Selection" check box for the files to be deleted. Click "Delete".
   - To delete all the layout files, click "Select All". Click "Delete".
   - To delete individual layout files, click the respective "Delete" button in the "Action" column.

Result

The selected layout file is deleted. Note that this also applies to the layout files included in your package.

Existing WebCenter pages which use this layout template are retained. You cannot use this layout to create new WebCenter pages.

Deleting a WebCenter page

1. Click "WebCenter > Configuration" in the start page.
2. Click the "Delete page" tab.
3. Activate the respective check box to mark the pages to be deleted.
4. Click "Delete".

2.5.8 Exporting and importing WebCenter pages (RT Professional)

Requirement

- The logged-on user has access rights.
- The WebCenter page is open.

Exporting a WebCenter page

1. Click 
2. Select if you want to open or save the file as a WebCenter page in the dialog that opens.
   If you save the file, a file is generated with the format "*.Export".
   To open the file, select a program that can display "*.xml" format.

Importing a WebCenter page

1. Click "WebCenter > Configuration" in the start page.
2. Click the "Import page" tab.
3. Enter a file name or click "Browse".
4. To load the file, click "Upload".
5. Enter a name for the WebCenter page.
6. Select the storage location for the WebCenter pages.
7. Click on "Import".

Result

The selected WebCenter page is imported and displayed in the DataMonitor.

2.6 Working with Trends and Alarms (RT Professional)

2.6.1 Displaying process values in a table (RT Professional)

Requirements

- A connection to the WinCC data is established (Page 95)
- The DataMonitor start page is open.

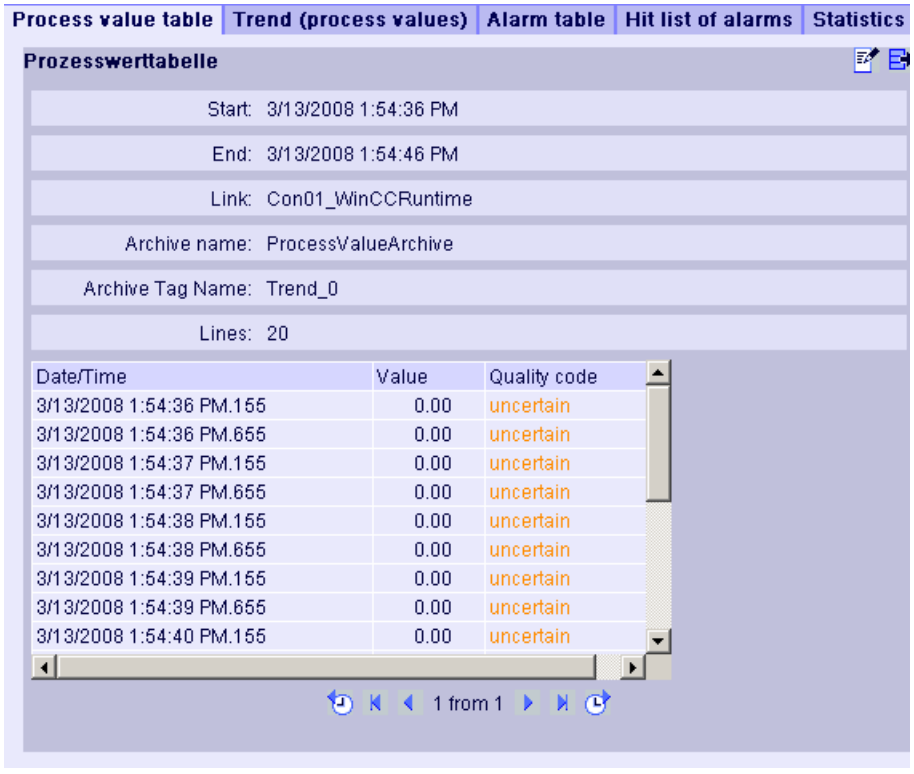
Procedure

Proceed as follows to display process values in a table:

1. Click "Trends & Alarms " in the start page. Click the "Process value table" tab. The Web part "Process Value Table" is displayed.
2. Click . The configuration dialog of the Web part opens.
3. Change the title in the "Header" field. Enter a brief tip in the field "Tooltip".
4. Select the desired connection in the "Connection" field. The logging tags available via this connection will be displayed. You can limit the number of tags using the "Archive selection" and "Tag filter" fields.
5. Click "Add" for the desired logging tags.
6. Define the time range in the "Time period" area.
   With relative times, enter a negative value in the respective field. To obtain additional information on the time specification, click the ? symbol.
   To check the set time range in the column "Preview time frame", click "Preview".
7. Define the number of decimal places in the "Displaying decimal places" section.
8. In the "Table size" area, define the size of the display window. For example, enter a height of "200" and a width of "400".
   If the value "0" is entered into both fields, the size is determined automatically. The size is oriented on spatial requirements of the Web part.
9. The available WebCenter pages are displayed in the "Links to WebCenter Pages" area. To assign the Web part to one or more WebCenter pages, click the × symbol.
10. Confirm your entries.

Result

The values of the logging tags are output in the process value table.



Use the arrow keys to skip backward and forward with multi-page tables. You can export the displayed table in CSV format using the icon. Click the symbol to change your settings.

2.6.2 Displaying process values in a diagram (RT Professional)

Requirements

- A connection to the WinCC data is established (Page 95)
- The DataMonitor start page is open.

Procedure

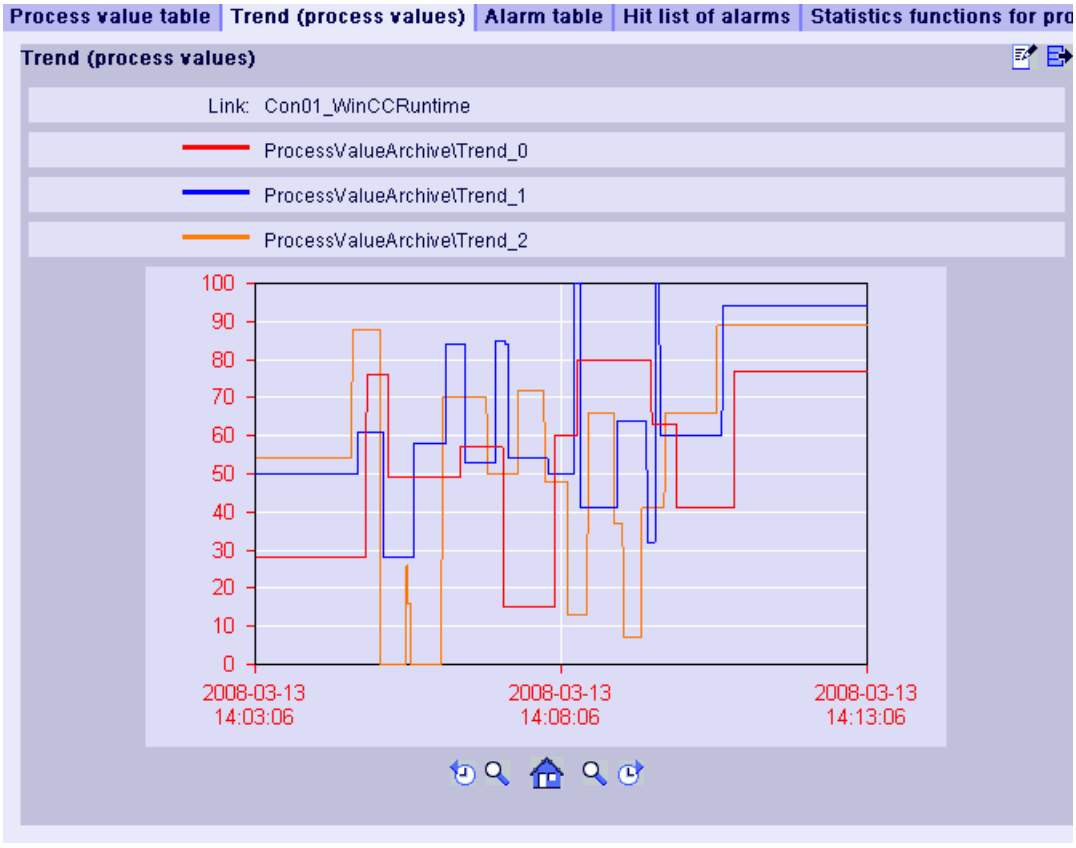
Proceed as follows to display process values in a trend view:

1. Click "Trends & Alarms " in the start page. Click the "Trend (process values)" tab. The Web part "Trend (process values)" is displayed.
2. Click . The configuration dialog of the Web part opens.
3. Change the title in the "Header" field. Enter a brief tip in the field "Tooltip".

4. Select the desired connection in the "Connection" field. The logging tags available via this connection will be displayed. You can limit the number of tags using the "Archive selection" and "Tag filter" fields.
5. Click "Add" for the desired logging tags, e.g. "TREND_1", "TREND_2", "TREND_3. The logging tags are listed in the "Current selection" area.
6. Define the following for the individual logging tags in the "Current selection" area:
   – color of time and value axis
   – form of the trend display
7. In the section "Value axis editor", you can select the automatic scaling for the different value axes or you can assign a minimum and a maximum value to each axis.
8. Define the time range in the "Time period" area.
   With relative times, enter a negative value in the respective field. To obtain additional information on the time specification, click the ? symbol. To check the set time range in the column "Preview time frame", click "Preview".
9. In the section "Diagram settings", define the size of the display window. If the value "0" is entered into both fields, the size is determined automatically. The size is oriented on spatial requirements of the Web part.
10. To display the legend, select "Show legend".
11. The available WebCenter pages are displayed in the "Links to WebCenter Pages" area. To assign the Web part to one or more WebCenter pages, click the x symbol.
12. Confirm your entries.

Result

The selected process values are displayed as trends in a diagram.



The legend shows the assignment of the colors to the logging tags. Skip forward or back by the selected time frame in the absolute time using the and buttons.

Enlarge the display and you can zoom into the diagram area to the left and right of the center line using the "Zoom left" and "Zoom right" buttons. The button is used to restore the original view.

Export the table displayed in CSV format using the icon.

Click the symbol to change your settings.

2.6.3 Displaying messages in the alarm table (RT Professional)

Requirements

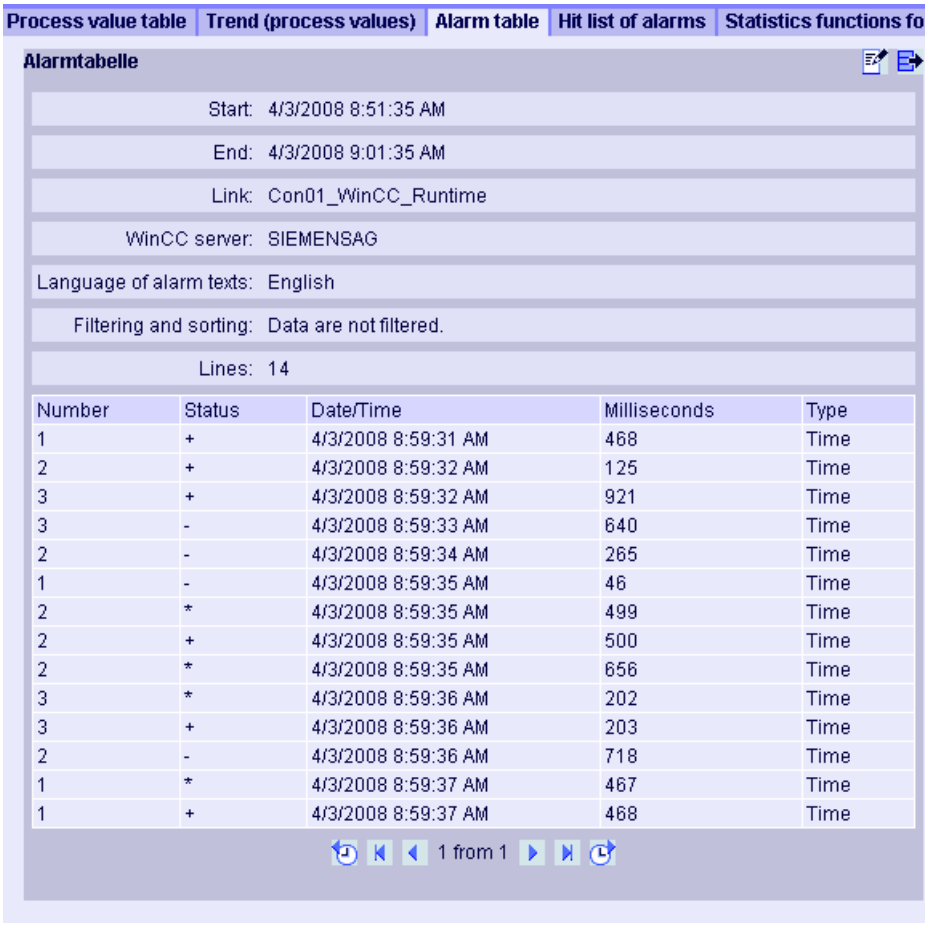
- A connection to the WinCC data is established (Page 95)
- The DataMonitor start page is open.

Procedure

To display alarms in the alarm table, proceed as follows:

1. Click "Trends & Alarms " in the start page. Click the "Alarm table" tab. The Web part "Alarm Table" is displayed.
   Click . The configuration dialog of the Web part opens.
2. Change the title in the "Header" field. Enter a brief tip in the field "Tooltip".
3. Select the connection in the "Connection" field.
4. Select the corresponding WinCC server in the "Selection of WinCC Servers" area.
   You need this setting to be able to select a connection to a swapped out archive that contains log files from several WinCC servers.
5. Define the time range in the "Time period" area. With relative times, enter a negative value in the respective field. To obtain additional information on the time specification, click the ? symbol. To check the set time range in the column "Preview time frame", click "Preview".
6. In the section "Language of the alarm texts", select the language in which the alarms are displayed.
7. In the section "Filter selection", limit the expected search results by means of filter conditions in SQL syntax. To obtain additional information on the filter conditions, click the ? symbol.
8. Define the following for displaying the data:
   - Sorting order: To obtain additional information on sorting, click the ? symbol.
   - Visible columns: To display all the columns, click "Select All". For further information, refer to "Alarm Log Column Names (Page 125)".
   - Number of decimal places
9. In the "Table size" area, define the size of the display window.

10. The available WebCenter pages are displayed in the "Links to WebCenter Pages" area. To assign the Web part to one or more WebCenter pages, click the ? symbol.
11. Confirm your entries.



Result

Use the arrow keys to skip backward and forward with multi-page tables. You can export the displayed table in CSV format using the icon. Click the symbol to change your settings.

2.6.4 Alarm Log Column Names (RT Professional)

Introduction

You can select the alarm log columns while displaying alarms in "Trends and Alarms".

Overview of column names

Position	Name	Type	Comments
1	MsgNo	Integer 4 Bytes	Alarm number
2	State	Small Integer 2 Bytes	Alarm Log Status
3	DateTime	DateTime 8 Bytes	Time stamp of alarm (Date/time without milliseconds)
4	Ms	Small Integer 2 Bytes	Time stamp of alarm (milliseconds)
5	Instance	VarChar (255)	Instance Name of the Alarm Log
6	Flags1	Integer 4 Bytes	(only for internal use)
7	PValueUsed	Integer 4 Bytes	Process Values used
8 to 17	PValue1 to PValue10	Real 8 Bytes	Numerical Process Value 1 to 10
18 to 27	PText1 to PText10	VarChar (255)	Process Value Text 1 to 10
28	Computer name	VarChar (255)	Computer Name
29	Application	VarChar (255)	Application Name
30	Comment	VarChar (255)	Comments
31	UserName	VarChar (255)	User Name
32	Counter	Integer 4 Bytes	Running Alarm Message Counter
33	TimeDiff	Integer 4 Bytes	Time difference to "Incoming" status
34	ClassName	VarChar (255)	Alarm class name
35	Type name	VarChar (255)	Alarm type name
36	Class	Small Integer 2 Bytes	Alarm class ID
37	Type	Small Integer 2 Bytes	Message type ID
38 to 47	Text1 to Text10	VarChar (255)	Alarm Text 1 to 10
48	AG_NR	Small Integer 2 Bytes	Number of the PLC
49	CPU_NR	Small Integer 2 Bytes	Number of the CPU
50	CrComeFore	Integer 4 Bytes	Foreground Color for the "Incoming" Status
51	CrComeBack	Integer 4 Bytes	Background Color for the "Incoming" Status
52	CrGoFore	Integer 4 Bytes	Foreground Color for the "Outgoing" Status
53	CrGoBack	Integer 4 Bytes	Background Color for the "Outgoing" Status
54	CrAckFore	Integer 4 Bytes	Foreground Color for the "Acknowledged" Status
55	CrAckBack	Integer 4 Bytes	Background Color for the "Acknowledged" Status
56	LocalID	Integer 4 Bytes	Location of the Alarm
57	Priority	Integer 4 Bytes	Priority
58	AP_type	Integer 4 Bytes	Loop-in alarm
59	AP_name	VarChar (255)	Loop-in-Alarm Function Name
60	AP_PAR	VarChar (255)	Loop-in-Alarm Screen
61	InfoText	VarChar (255)	Info text
62	TxtCame	VarChar (255)	Incoming text
63	TxtWent	VarChar (255)	Outgoing text
64	TxtCameNWent	VarChar (255)	Text came in and went out
65	TxtAck	VarChar (255)	Text acknowledged
66	AlarmTag	Integer 4 Bytes	Alarm tag
67	AckType	Small Integer 2 Bytes	Acknowledgment Type
68	Params	Integer 4 Bytes	Parameter

See also

Displaying messages in the alarm table (Page 123)

2.6.5 Displaying the hit list of messages (RT Professional)

Requirements

- A connection to the WinCC data is established (Page 95)
- The DataMonitor start page is open.

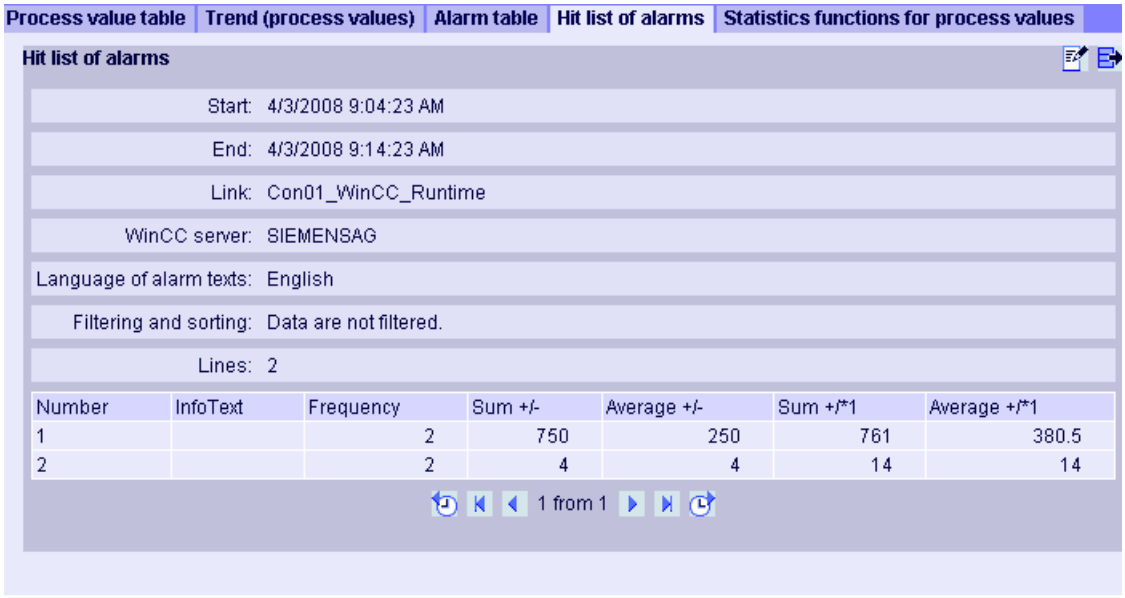
Procedure

To display alarms in a hit list, proceed as follows:

1. Click "Trends & Alarms " in the start page. Click the "Alarm hit list " tab. The web part "Hit list of the alarms" is displayed.
   Click . The configuration dialog of the Web part opens.
2. Change the title in the "Header" field. Enter a brief tip in the field "Tooltip".
3. Select the desired connection in the "Connection" field:
4. Define the time range in the "Time period" area. With relative times, enter a negative value in the respective field. To obtain additional information on the time specification, click the ? symbol. To check the set time range in the column "Preview time frame", click "Preview".
5. In the section "Language of the alarm texts", select the language in which the alarms are displayed.
6. Select the corresponding WinCC server in the "Selection of the WinCC Server" area. You need this setting to be able to select a connection to a swapped out archive that contains log files from several WinCC servers.
7. In the section "Filter selection", limit the expected search results by means of filter conditions in SQL syntax. To obtain additional information on the filter conditions, click the ? symbol.
8. Define the following for displaying the data:
   - Sorting order: To obtain additional information on sorting, click the ? symbol.
   - Visible columns: To display all the columns, click "Select All".
   - Number of decimal places
9. In the "Table size" area, define the size of the display window. If the value "0" is entered into both fields, the size is determined automatically. The size is oriented on spatial requirements of the table.
10. The available WebCenter pages are displayed in the "Links to WebCenter Pages" area. To assign the Web part to one or more WebCenter pages, click the x symbol.
11. Confirm your entries.

Result

The analysis values for the alarms are displayed in a hit list:



The table contains configured data and statistical values, e.g. InfoText, frequency of the alarm.

Explanations for the columns are displayed as a tool tip when the mouse is moved over the respective column header. Use the arrow keys to skip backward and forward with multi-page tables.

With the icon , the displayed analysis values of the alarms can be exported in CSV format. Click the symbol to change your settings.

Note

The display of alarms in the hit list may take some time and may place a strong load on the CPU. A note is displayed in "Trends and Alarms" if the data volume is too high. You may then confirm the alarm and continue without any changes, or you may cancel the process to modify the filter criteria and thus reduce the expected amount of data.

2.6.6 Displaying statistics function for process values (RT Professional)

Requirements

- A connection to the WinCC data is established (Page 95)
- The DataMonitor start page is open.

Procedure

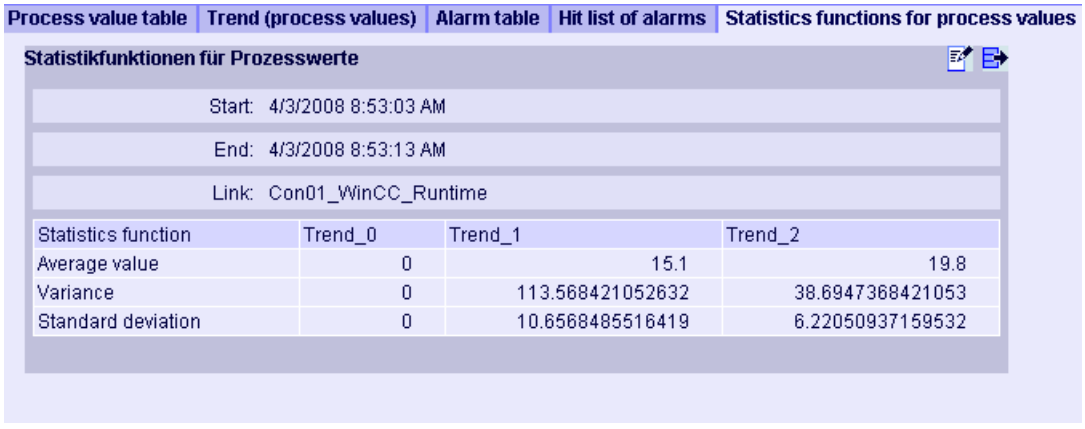
Proceed as follows to display statistics functions for process values:

1. Click "Trends & Alarms " in the start page. Click the "Statistics functions for process values" tab. The Web part "Statistics functions for process values" is displayed.
2. Click . The configuration dialog of the Web part opens.
3. Change the title in the "Header" field. Enter a brief tip in the field "Tooltip".
4. Select the desired connection in the "Connection" field. The logging tags available via this connection will be displayed. You can limit the number of tags using the "Archive selection" and "Tag filter" fields.
5. Click "Add" for the desired logging tags.
6. Define the time range in the "Time period" area.
   With relative times, enter a negative value in the respective field. To obtain additional information on the time specification, click the ? symbol.
   To check the set time range in the column "Preview time frame", click "Preview".
7. Define the following for displaying the data:
   - Number of decimal places
   - Aggregate selection: Define the analysis function for the process values.
8. In the "Table size" area, define the size of the display window. For example, enter a height of "200" and a width of "400". If the value "0" is entered into both fields, the size is determined automatically. The size is oriented on spatial requirements of the table.
9. The available WebCenter pages are displayed in the "Links to WebCenter Pages" area. To assign the Web part to one or more WebCenter pages, click the x symbol.
10. Confirm your entries.

Result

Statistics functions for the selected process values were executed and output in the table.

The log name and tag name are displayed as a tool tip when the mouse is moved over the respective column header.



You can export the displayed table in CSV format using the icon. Click the symbol to change your settings.

2.7 Working with Excel Workbooks (RT Professional)

2.7.1 Configuring an Excel workbook (RT Professional)

2.7.1.1 Importing data from a WinCC project (RT Professional)

Introduction

You need the WinCC configuration data to configure Excel workbooks.

Import this data from a local WinCC project when configuring the workbook using the Excel Workbook Wizard .

Requirement

- Server PC
  - Office 2007, Office 2010 or Office 2013 is installed
  - The Excel add-In "Excel Workbook" is installed.
  - DataMonitor Server is installed.
  - The WinCC project is in Runtime.
  - A user is created in WinCC.
- On the configuration PC
  - Office 2007, Office 2010 or Office 2013 is installed
  - The Excel add-In "Excel Workbook Wizard" is installed.

Procedure

To import data from a WinCC project, proceed as follows on the configuration PC:

1. Open an empty Excel workbook. Select the "Excel Workbook Wizard..." command in the "DataMonitor" menu.
2. Activate the option "Establish connection with WinCC server".
3. The "WinCC Server" field is shown. Enter the name of the server PC and then click "Connect". The log in dialog is displayed.
4. Enter the name and password of a WinCC user.
5. Click "Next >". The "Add / delete tags" dialog opens.

Result

The Excel workbook is configured. Create the view of process data.

2.7.1.2 Importing data from an xml file (RT Professional)

Introduction

You can create the Excel workbook on a PC if, for example, Excel is not installed on the server PC. Create the corresponding xml file on the DataMonitor Server.

Requirement

- Server PC
  - DataMonitor Server is installed.
  - The WinCC project is in Runtime.
  - A user is created in WinCC.
- On the configuration PC
  - Office 2007, Office 2010 or Office 2013 is installed
  - The Excel add-in "Excel Workbook Wizard" is installed.

Creating an XML file on the server PC

1. In the Start menu select the command "Start > All Programs > Siemens Automation > Option and Tools > HMI Tools" > WinCC DataMonitor Configurator Export".
   The function creates an XML file and stores it in subdirectory "Web Navigator\Reports" of the current project. The file name is automatically generated using the format "<projectname>.XML".
2. If no Excel installation exists on the server PC, transfer the XML file to another PC on which MS Excel and the Excel Workbook Wizard are installed.

Configuring data access using an XML file

1. Open an empty Excel workbook. Select the "Excel Workbook Wizard..." command in the "DataMonitor" menu.
2. Activate the option "Load configuration data from file". Click "Next >".
3. Navigate to the required XML file.
4. Click "Next >". The "Add / delete tags" dialog opens.

Result

The Excel workbook is configured. Create the view of process data. Transfer the Excel workbook to the client PC. The DataMonitor Client displays the process data of the server PC.

2.7.1.3 Configuring the display of tag values (RT Professional)

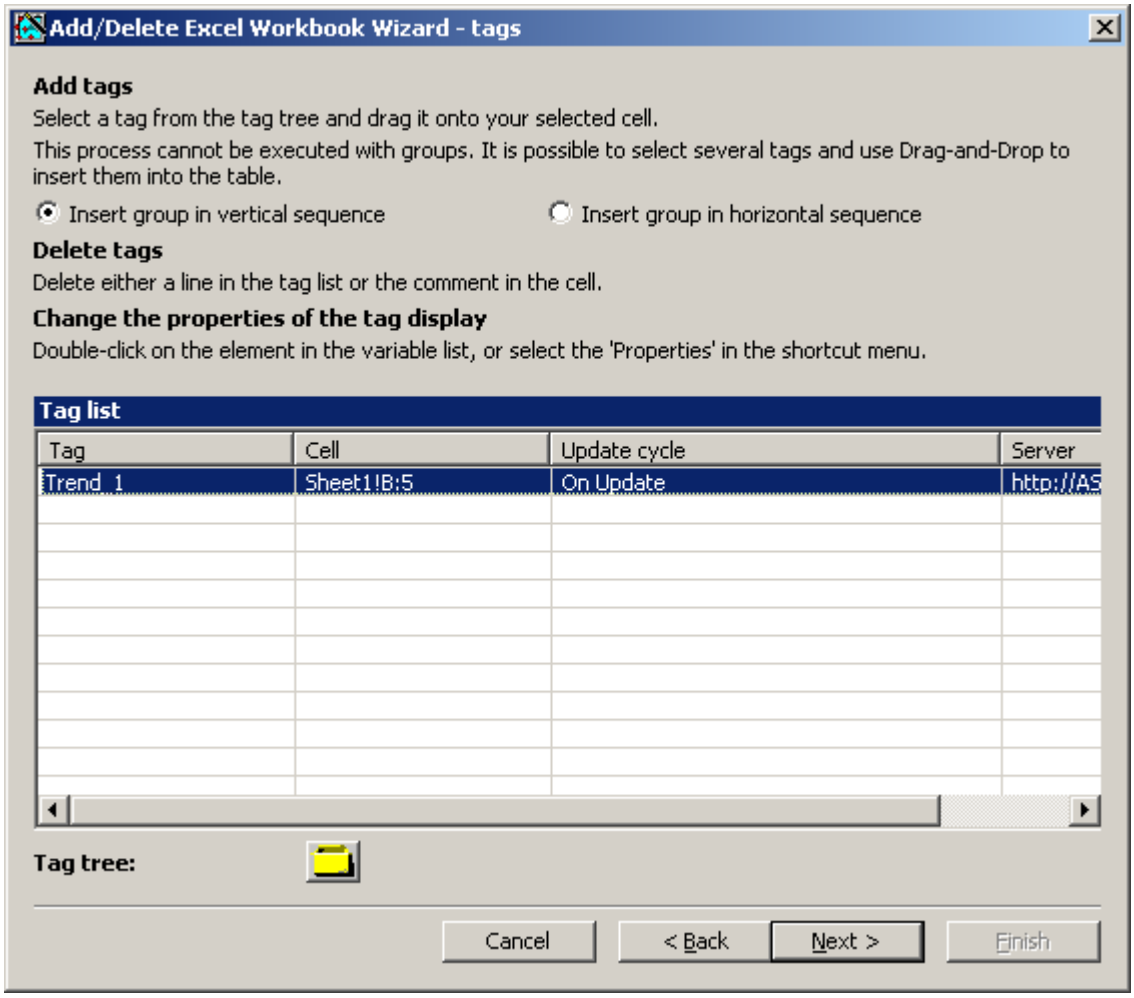
Requirements

- The dialog "Add / delete tags" is open.

Procedure

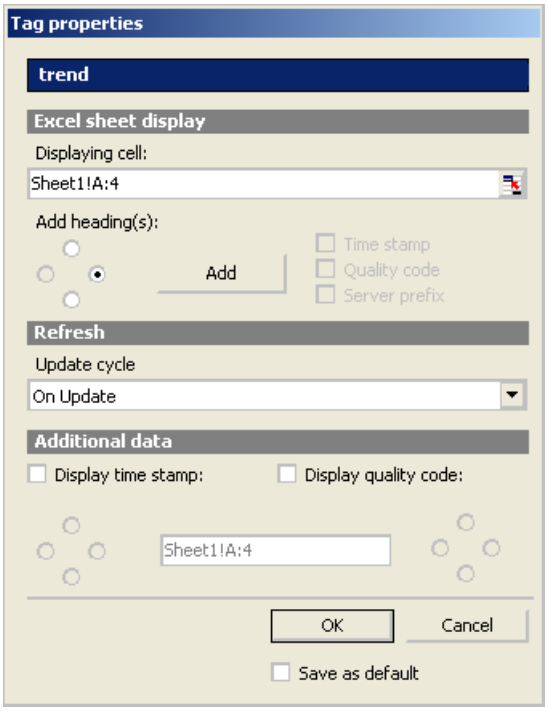
Proceed as follows to display tag values in Excel:

1. Check the option for the insert sequence of tag groups in the "Add tags" area.



2. In the "Tag tree" area, click the directory icon. The object list opens.
3. Select the desired tag in the object list and drag the tag to a field of the Excel table.
4. Close the object list. The tag will be displayed in the window "Tag list".
5. In the "Tag list" window, select the tag and the "Server settings" command from the shortcut menu.
6. In the "Server settings" dialog, enter the name and password of a WinCC user. Activate "Activate automatic login". Confirm your entries.

7. In the window "Tag list", select the tag and select the menu command "Properties" from the shortcut menu. The dialog "Tag properties" will be opened.



8. Define the properties for the view in the table, e.g. the arrangement of headers, time stamps, and quality code.
9. To apply the set update cycle to all tags, select "Save as default".
   Settings in the areas "Display in sheet" and "Additional Data" are not valid for all tags.
10. Confirm your entries. Click the "Next >" button in the dialog "Add tag". The dialog "Add/delete logging tags (Page 134)" is opened.

Result

The display of tag values in an Excel sheet is configured.

In the Excel workbook, each table cell is assigned a short text and a comment which was configured for displaying a tag value.

With tag values, the short text "OV" stands for online tags.

In the comments, the source of the displayed values is shown in the format "WDWx_<number>_<tagname>".
The value for x means:

- O = Online value

Note

After deleting/moving cells filled with configuration data or deleting/inserting new lines/columns in the Excel worksheet, the Excel Workbook Wizard must be executed again. The configuration data is checked and automatically adapted as a result. Confirm the data displayed simply by using the "Next >" button. Save the workbook and close Excel.

2.7.1.4 Configuring the display of logging tags (RT Professional)

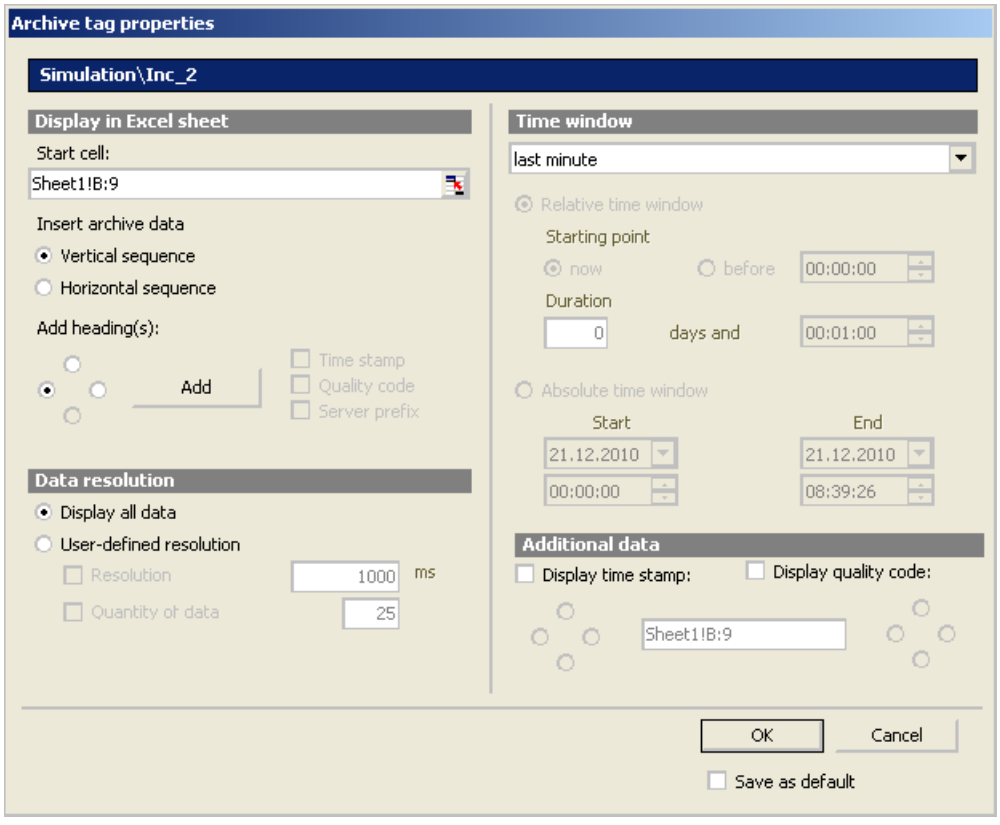
Requirement

- The dialog "Add / delete logging tags" is open.

Procedure

Proceed as follows to display logging tags in Excel:

1. In the "Tag tree" area, click the directory icon. The object list opens.
2. Select the desired logging tag in the object list and drag the logging tag into a field of the Excel table.
3. Close the object list. The logging tag will be displayed in the window "Tag list".
4. In the window "Tag list", select the logging tag and select the menu command "Properties" from the shortcut menu. The dialog "Archive tag properties" will be opened.



5. Define properties for display in the table, e.g. the insert sequence, data resolution, display time window.

6. To save the settings, select "Save as default". The settings in the "Additional data" area are not saved.

   Note

   If you use the option "Number of data" for Data resolution > User-defined resolution", enter an even value in the input box. Even values ensure proper trend display.

7. Confirm your entries. Click the "Next >" button in the dialog "Add logging tag". The dialog "Add/remove alarms (Page 135)" will open.

Result

The display of logging tag values in an Excel sheet is configured.

In the Excel workbook, each table cell is assigned a short text and a comment which was configured for displaying a tag value.

With tag values, the short text "AV" stands for logging tags.

In the comments, the source of the displayed values is shown in the format "WDWx_<number>_<tagname>".
The value for x means:

- A = Archive value

  Note

  After deleting/moving cells filled with configuration data or deleting/inserting new lines/ columns in the Excel worksheet, the Excel Workbook Wizard must be executed again. The configuration data is checked and automatically adapted as a result. Confirm the data displayed simply by using the "Next >" button. Save the workbook and close Excel.

See also

Configuring the display of tag values (Page 132)

2.7.1.5 Configuring the display of alarms (RT Professional)

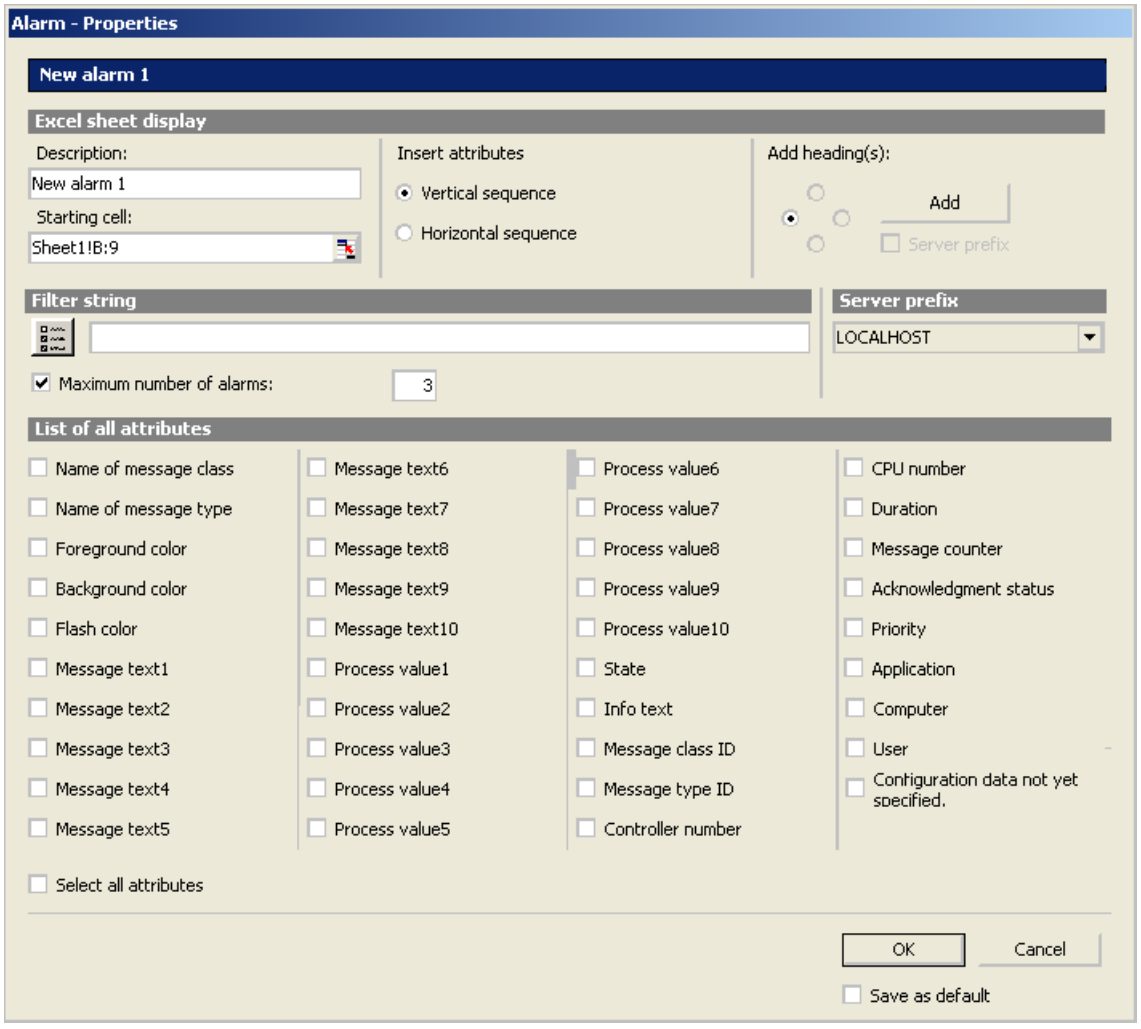
Requirement

The dialog "Add / Delete Alarms" is open.

Procedure

Proceed as follows to display alarms in Excel:

1. Select the required cell in the Excel table. Click "Add alarm".
2. In the "Add alarm" area, click the directory icon. The dialog "Alarm - properties" will be opened.



3. Define the properties for the display of alarms in the Excel table, such as headings and insertion sequence of attributes.
4. Enter a filter condition in the "Filter string" field or use the selection dialog to define specific alarms to be displayed, for example.
5. Use the "Maximum number of alarms" option to limit the number of most recent alarms displayed. You can display maximum 1,000 alarms.
6. Activate the desired attributes in the list. For additional information, refer to "Alarm Attributes (Page 140)".

7. To save the setting, select "Save as default".
8. Confirm your entries. Click the "Next >" button in the dialog "Add logging tag": The "Description" dialog box will open.

Result

The display of alarms in an Excel sheet is configured.

In the Excel workbook, each table cell is assigned a short text and a comment which was configured for displaying an alarm.

With alarms, the short text "AL" and the comment are shown in the format "WDWL_<nummer>_<feldbezeichnung>".

Note

After deleting/moving cells filled with configuration data or deleting/inserting new lines/columns in the Excel worksheet, the Excel Workbook Wizard must be executed again. The configuration data is checked and automatically adapted as a result. Confirm the data displayed simply by using the "Next >" button. Save the workbook and close Excel.

See also

Configuring the display of logging tags (Page 134)

2.7.1.6 Publishing an Excel workbook (RT Professional)

Requirement

The display of tag values, logging tags and alarms is configured.

The "Description" dialog box is open.

Procedure

To access Excel workbooks on the DataMonitor Server, proceed as follows:

1. Click "Publish". The Excel workbook is made available for download on the DataMonitor Server.
2. Use the "Template" button to provide the Excel Workbook for the function "Published Reports".
3. Exit the Excel Workbook Wizard
4. Save the workbook and close Excel.

Alternative procedure

You publish the Excel template on the DataMonitor client. For additional information, refer to "Preparing an Excel Workbook as a Template (Page 141)".

Result

The Excel workbook is made available on the DataMonitor Server. If required, the Excel workbook is downloaded on the DataMonitor clients or opened directly in Internet Explorer.

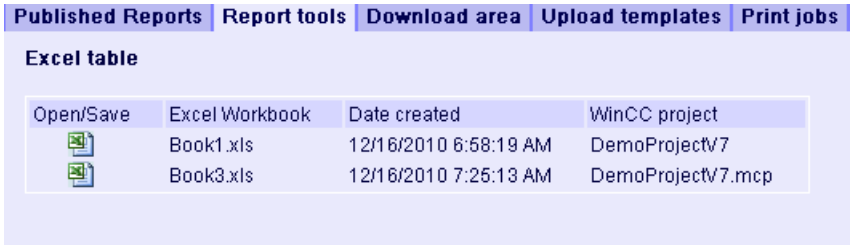
2.7.2 Displaying process data in an Excel Workbook online (RT Professional)

Requirements

- The Excel workbook with the configuration of the process value display must be available on the PC.
- One of the following Excel versions is necessary for online display in the Excel Workbook:
  - Office 2007
  - Office 2010
  - Office 2013
- WinCC Runtime Professional is installed
- DataMonitor Server is installed.
- The WinCC project is in Runtime.
- The DataMonitor start page is open.
- The user "DM_Demo" has been created (Page 77).

Procedure

1. Click "WebCenter > Configuration" in the start page.
2. Click the "Report tools" tab.
   The Excel workbooks that were published in the Excel Workbook Wizard, are shown in an overview.



3. Select a workbook.
4. Click the Excel workbook symbol in the "Open / Save" column.
5. Click "Open >" in the next dialog. The Excel workbook opens.
6. Select the "Excel Workbook" command in the "DataMonitor" menu.

7. The name of one of the servers, whose tags are configured in the Excel table, is displayed in the "WinCC Server" field.
   The following options are available for the server name:
   - Access via domain
     In case of accesses from outside the network domain, the domain is indicated along with the server name.
   - The DataMonitor start page is the standard Web page.
     Only the server name is entered in the "WinCC Server" field.
   - The DataMonitor start page is in the virtual directory:
     The name of the virtual folder needs to be specified after the server name, e.g. "/webnavigator".
8. Activate the "All servers" check box when the tags from several servers are configured in an Excel sheet. The tag values of all the servers are updated in the online display.

   Note

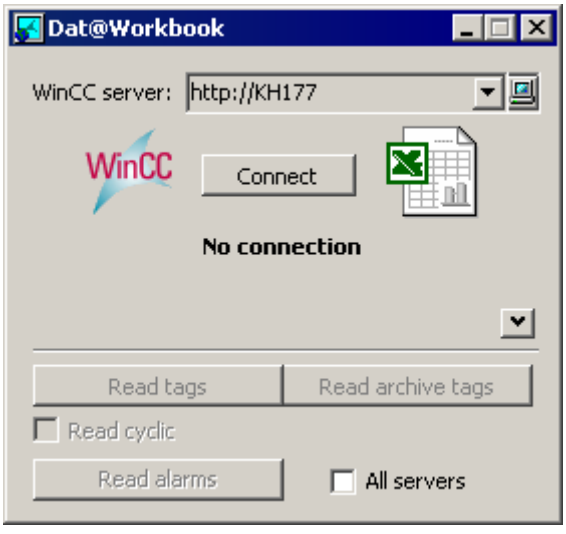
   To establish connections to all the servers, select "All servers" before pressing the "Connect" button to establish the connection.

9. Activate the connection to the WinCC project via the button "Connect". After a successful connection, the log-in dialog will be opened. Enter the user name "DM_Demo" and the respective password. When several servers are used, the logon dialogs of the servers concerned open one after the other.
   If no connection is established, a corresponding message is displayed. Clicking on the dialog will display further information about the error (if available).

   Note

   The Excel Workbook dialog must not be closed as long as the logon dialog for connection establishment to the server persists.

10. The connection status will be displayed in the dialog. Click the buttons "Read tags", "Read logging tags" and "Read alarms" buttons to update the respective values or displays.



   If necessary, select the check box "Read cyclically" to update the tag values in cycles.

11. Close the dialog "Excel Workbook" after ending your calculations in Excel.
12. Save the results in the workbook and close Excel.

Result

The values of an online tag, a logging tag as well as a message window are displayed in the Excel table.

2.7.3 Alarm Attributes (RT Professional)

Introduction

While displaying messages in Excel Workbook you can select the attributes to be displayed in the Excel sheet in the Excel Workbook Wizard .

Overview

Position	Attribute	Type	Comments
1	Alarm class name	VarChar (255)	
2	Alarm type name	VarChar (255)	
3	Foreground color	Integer 4 Bytes	
4	Background color	Integer 4 Bytes	
5	Flashing color	Integer 4 Bytes	
6 to 15	Alarm Text 1 to 10	VarChar (255)	
16 to 25	Process value 1 to 10	Real 8 Bytes	Numerical Process Value 1 to 10
26	State	VarChar (255)	Status text
27	Info text	VarChar (255)	
28	Alarm class ID	Integer 4 Bytes	
29	Message type ID	Integer 4 Bytes	
30	AS Number	Small Integer 2 Bytes	
31	CPU Number	Small Integer 2 Bytes	
32	Duration	Integer 4 Bytes	Time difference to "Incoming" status
33	Alarm counter	Integer 4 Bytes	Consecutive alarm counter
34	Acknowledgment Status	VarChar (255)	Text of the acknowledgement status
35	Priority	Integer 4 Bytes	
36	Application		Application with which the comment was created.
37	Computer	VarChar (255)	Computer on which the comment was created.
38	Users	VarChar (255)	User who created the comment.
39	Comments	VarChar (255)	

See also

Configuring the display of alarms (Page 135)

2.7.4 VBA Functions of the Excel Workbook (RT Professional)

Excel workbooks: VBA functions of the Excel workbook

The following functions are available to you in an Excel workbook if you have generated an instance of the Excel workbook object using the "Application.COMAddIns.Item("ExcelWorkbook.Connect").Object".

- ShowDialog(0): Opens the "Excel Workbook" dialog with a normal size.
- ShowDialog(1): Opens the "Excel Workbook" dialog with a minimized size.
- ShowDialog(2): Opens the "Excel Workbook" dialog hidden.
- CloseDialog: Closes the "Excel Workbook" dialog.
- GetServerID(server name): Gets the ID of the WinCC server with a specified name, for example: "http://Local_PC".
- Connect(ServerID): Connects the specified WinCC server to the Excel workbooks. You can get the "ServerID" using the "GetServerID(server name)" function. The "Excel Workbook" dialog must be opened before establishing a connection.
- ConnectAll: Connects all WinCC servers to Excel workbooks. The "Excel Workbook" dialog must be opened before establishing a connection.
- Disconnect(ServerID): Disconnects the Excel workbook from the specified WinCC server.
- DisconnectAll: Disconnects the Excel workbook from all WinCC servers.
- ReadTags(ServerID): Reads the tags from WinCC server with "ServerID". The connection must be established before tags can be read.
- ReadArchives(ServerID): Reads the logs from WinCC server with "ServerID". The connection must be established before logs can be read.
- ReadAlarms(ServerID): Reads the alarms from WinCC server with "ServerID". The connection must be established before alarms can be read.

As soon as a connection is established or closed, the event "ServerConnected(ServerID)" or "ServerDisconnected(ServerID)" is output by the "ExcelWorkbook.Connect" object. These events can be integrated, for example, using "WithEvents" (VB standard).

2.8 Working with reports (RT Professional)

2.8.1 Preparing an Excel Workbook as a Template (RT Professional)

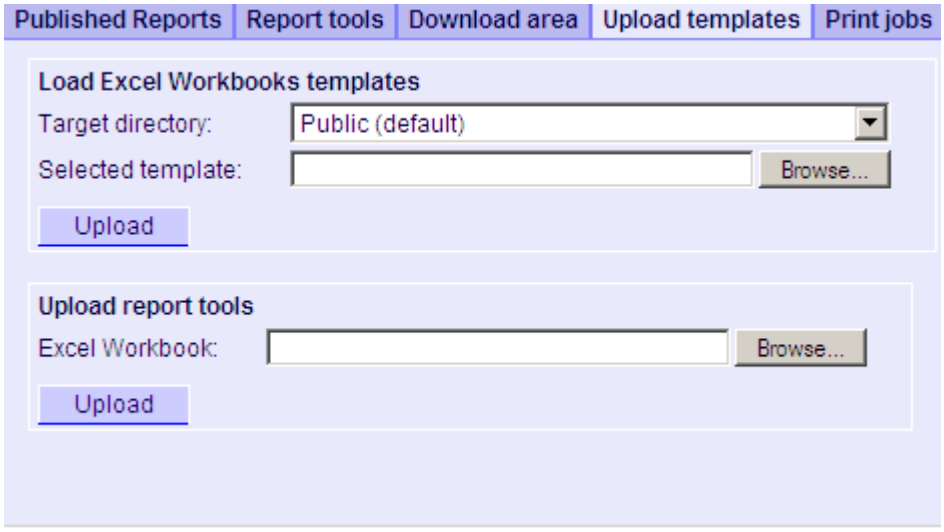
Requirement

- The Excel workbook is created.
- The start page of the DataMonitor is open.

Procedure

Proceed as follows to prepare Excel workbooks as a template:

1. Click "Reports" in the start page.
2. Click the "Upload templates" tag.



3. Select a directory, in which the template will be stored in the "Target directory" field. Only the directories, for which the user that is logged in has "Create" access rights, can be selected.
4. Click the "Browse" button in the "Selected template" field. Navigate to the required Excel workbook.
5. Click the "Upload" button.

Result

The template is prepared for the function "Published Reports".

See also

Publishing an Excel workbook (Page 137)
Configuring an Excel workbook (Page 130)

2.8.2 Making an Excel workbook available as a report tool (RT Professional)

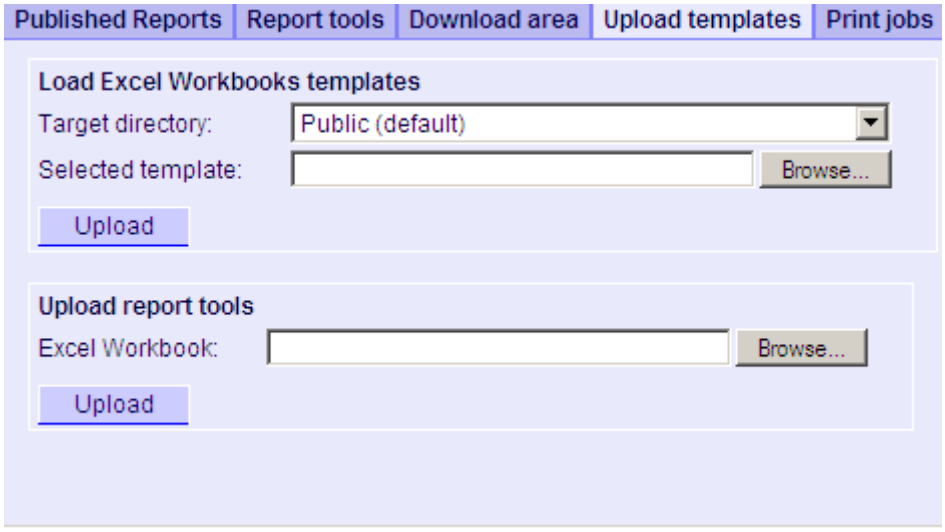
Requirement

- The Excel workbook is created.
- The start page of the DataMonitor is open.

Procedure

Proceed as follows to prepare Excel workbooks as a report tool:

1. Click "Reports" in the start page.
2. Click the "Upload templates" tag.



3. Click the "Browse" button in the "Excel Workbook" field. Navigate to the required Excel workbook
4. Click the "Upload" button.

Result

The Excel workbook is ready in the "Report tools" section.

2.8.3 Making Settings for Reports (RT Professional)

Introduction

Different settings are required for using the function "Reports" from DataMonitor.

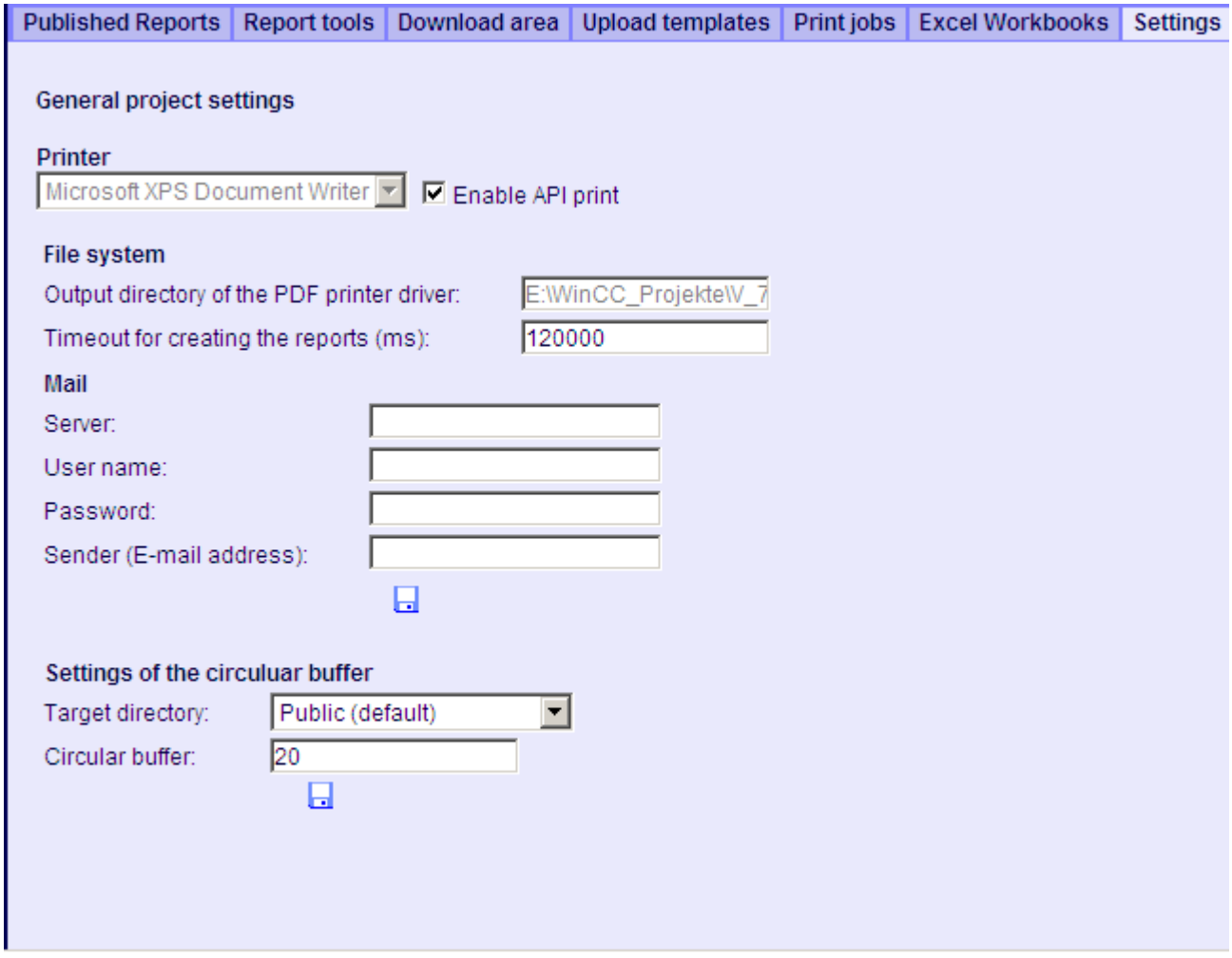
Requirements

- PDF Reader is installed.
- The WinCC project is selected on the DataMonitor server.
- The WinCC project is selected in "Scheduled print jobs in Runtime".
- The DataMonitor start page is open.

Procedure

To configure the reports settings, proceed as follows:

1. Click "Reports " in the start page. Click the "Settings" tab.
   The "Settings" page is displayed.



2. Check the entries in the section "General project settings".
   To enable output to a PDF file, select "Activate API print".
3. Enter the data for sending mail in the "Mail" area:
   - Server
     Outgoing mail server (SMTP)
   - User name
     Name for the sender
   - Password
   - Sender
     Email account, through which you send your Email
4. Click the disk icon in the section "General project settings" to save your settings.

5. In the "Circular buffer" area, you can define how many reports can be stored for the selected target directory. The field has a pre-assigned value of 20.
6. Click the disk icon in this section to save your settings.

Result

The settings for "Reports" have now been made.

2.8.4 Displaying a report with an Excel Workbook (RT Professional)

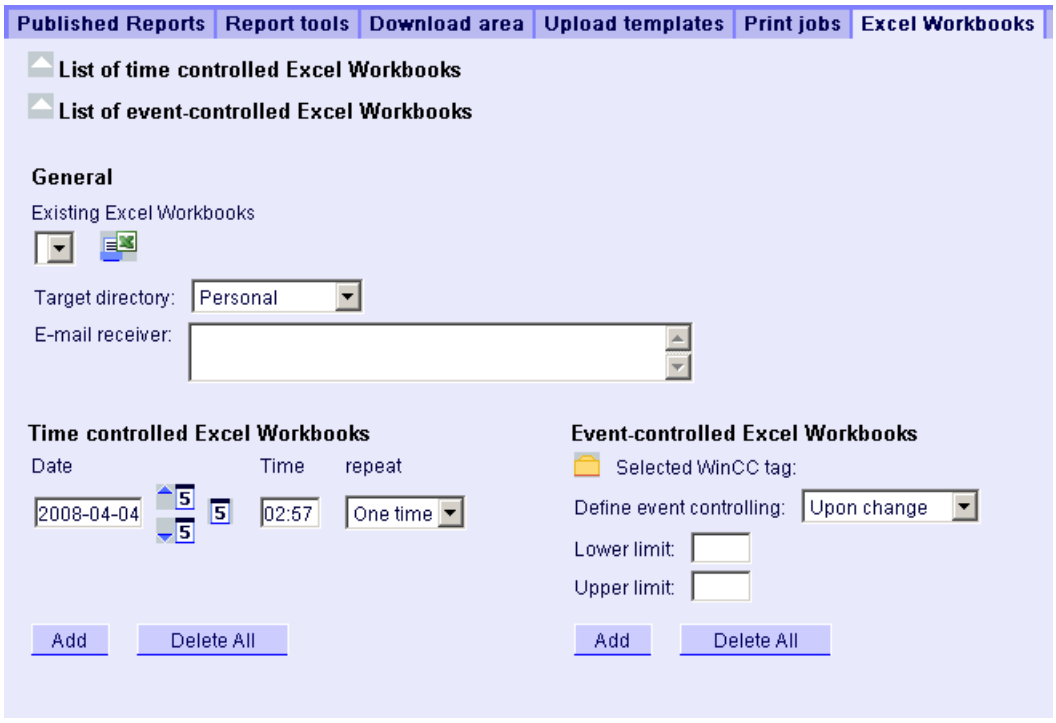
Requirements

- PDF Reader is installed.
- The WinCC project is selected on the DataMonitor server.
- The WinCC project is selected in "Scheduled print jobs in runtime".
- The DataMonitor start page is open.

Procedure

Proceed as follows to create a report with Excel workbooks:

1. Click "Reports" in the start page. Click the "Excel Workbooks" tab.
   The "Excel Workbooks" page is displayed.



   The icons in front of the lists "List of time-controlled Excel Workbooks" and "List of event-controlled Excel Workbooks" are cleared and show that currently, no reports are triggered.

2. Select the desired Excel workbooks, e.g. "My_workbook_1.xls" in the "Existing Excel Workbooks" field.
   This field only shows Excel Workbooks that meet the following conditions:
   - Workbooks that are published as templates in the Excel Workbook Wizard
   - Workbooks in directories for which the current user has the "Read" access right.
3. Select the directory, in which the reports will be stored in the "Target directory" field.
   Only the directories, for which the user that is logged in has "Create" access rights, can be selected.
4. Enter an e-mail address in the field "E-mail recipient". The report is e-mailed to this address.

5. To configure time-controlled triggering, define the following in the "Time-controlled Excel Workbooks" area.
   - Date:
     Enter the date in the field or define the date using the calendar. To open the calendar, click the "calendar" symbol.
   - Time
     Define the triggering time.
   - Repetition
     Define the repetition rate, e.g. "Once" or "Weekly".
6. Click the "Add" button in the "Time-controlled Excel Workbooks" area. The report is displayed in the "List of time-controlled Excel workbooks".
7. To create the report immediately, click the symbol .
8. To configure event-controlled triggering, define the following in the "Event-controlled Excel Workbooks" area.
   - Selected WinCC tag
     Click . The object list opens. Select the desired tag from the object list.
   - Define the event control
     Define the triggering event, e.g. change of the tag value.
     If you selected "Low limit", "High limit", or "Both limits" for event control, you need corresponding limit values.
9. Click the "Add" button in the "Event-controlled Excel Workbooks" area. The report is displayed in the "List of event-controlled Excel workbooks"

Result

A time-controlled or event-controlled report has been triggered with an Excel workbook.

The report is displayed in one of the lists "List of time-controlled Excel workbooks" and "List of event-controlled Excel workbooks". The report can be changed or deleted in the list.

Note

An event-controlled print job will not be initiated if the time, in which the tag changes, is less than one minute.

Note that frequent initiation of the event-controlled print job OR simultaneous initiation of several print jobs over an extended period will lead to heavy load on memory space and resources, e.g. frequent signal changes of a tag.

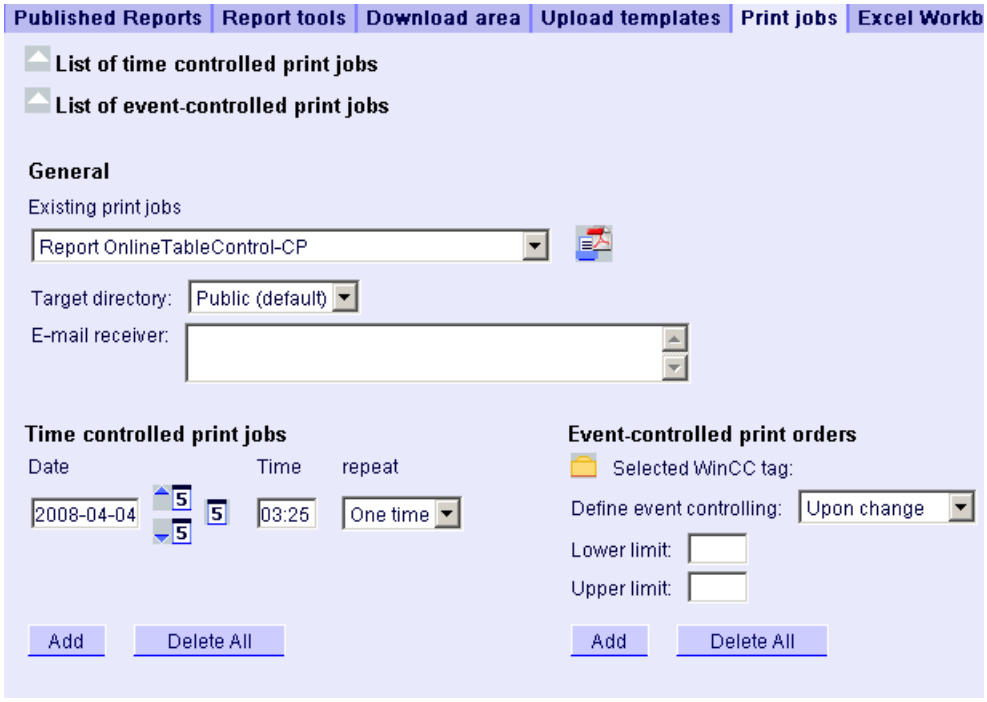
2.8.5 Creating a report with a print job (RT Professional)

Requirements

- PDF Reader is installed.
- The WinCC project is selected on the DataMonitor Server.
- The WinCC project is selected in "Scheduled print jobs in runtime".
- The DataMonitor start page is open.

Procedure

1. Click "Reports" in the start page. Click the "Print jobs" tab.
   The "Print Jobs Configuration" page is displayed.



   The icons in front of the lists "List of time-controlled print jobs" and "List of event-controlled print jobs" are cleared. The icons indicate that no reports are currently triggered.

2. Select the desired print job, such as "Report OnlineTableControl-CP" in the "Existing print jobs" field.
   You can create the report immediately via the  icon.

3. In "Target directory: ", select the directory in which the reports are created.
   Only the directories, for which the user that is logged in has "Create" access rights, can be selected.

4. Enter an e-mail address in the field "E-mail recipient". The report is e-mailed to this address.

5. To configure time-controlled triggering, define the following in the "Time-controlled print jobs" area.
   - Date:
     Enter the date in the field or define the date using the calendar. To open the calendar, click the "calendar" symbol.
   - Time
     Define the triggering time.
   - Repetition
     Define the repetition rate, e.g. "Once" or "Weekly".
6. Click the "Add" button in the "Time-controlled print jobs" area. The report is displayed in the "List of time-controlled print jobs".
7. To configure event-controlled triggering, define the following in the "Event-controlled print jobs" area.
   - Selected WinCC tag
     Click the  icon. The object list opens. Select the desired tag from the object list.
   - Define the event control
     Define the triggering event, when the tag value is changed, for example
   - Low limit and high limit
     If you selected "Only low limit", "Only high limit" or "Both limits" for event control, limits are required.
8. Click the "Add" button in the "Time-controlled print jobs" area. The report is displayed in the "List of event-controlled print jobs".

Result

A time-controlled or event-controlled report with print job in PDF format has been created.

Depending on the type, the report is displayed in one the "List of time-controlled print jobs" or "List of event-controlled print jobs". The report can be changed or deleted in the list.

Note

An event-controlled print job will not be initiated if the time, in which the tag changes, is less than one minute.

Please consider that a frequent triggering of the event-controlled print job over a long time period will use a lot of memory and resources, such as the frequent signal change of a tag.

WinCC Redundancy

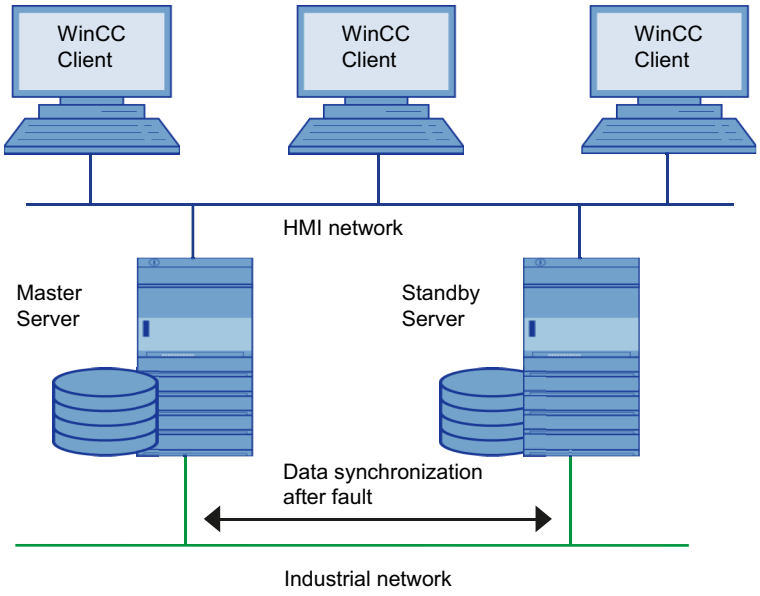
3

3.1 Basics

3.1.1 Overview

Introduction

WinCC Redundancy offers considerably increased availability of WinCC and the plant as a whole with parallel operation of two interconnected servers.



The servers monitor each other in runtime to allow for an early recognition of a failing partner server.

If one server fails, the clients will automatically be switched from the failed server to the still active server. This ensures that all clients will always be available for monitoring and operating the process.

During the failure, the active server will continue to log all alarms and process data of the WinCC project. After the failed server comes back online, the contents of all alarm, process

value and user logs will automatically be copied to the returned server. This will fill the log data gaps of the failed server. This action is also called synchronization after return.

The WinCC Redundancy Option offers:

- The automatic synchronization of alarm, process value and user logs after a failed server comes back online.
- The automatic synchronization of alarm, process value and user logs after a process connection error.
- The online synchronization of internal alarms.
- The online synchronization of internal tags (tag synchronization).
- The online synchronization of user logs.
- The automatic switching of clients between the redundant servers if one of the servers fails.
- The automatic switching of clients if the process connection fails.
- The "Application Health Check" function to monitor the WinCC applications.

The "Application Health Check" function

In the WinCC / PCS7 environment the expression "Application Health Check" refers to the cyclic lifebeat monitoring of important applications. The function increases the sensitivity of the redundancy, since the lifebeat monitoring is extended via the servers themselves to the individual applications. All important WinCC applications are automatically monitored.

The lifebeat monitoring detects a software error, sets the server status in the "@RedundantServerState" system tag to "Fault" and switches the linked clients to the redundant server.

A process control message warns the user about the software error.

Note

If a software error was detected by the "Application Health Check" function and client switching was initiated, the relevant server must then be restarted. Only then can the clients be reconnected to the server. The redundant servers must be equipped with Windows 2003 Server or newer and the client PCs with Windows 2000, Windows XP or Windows 7.

3.1.2 How Redundancy Works

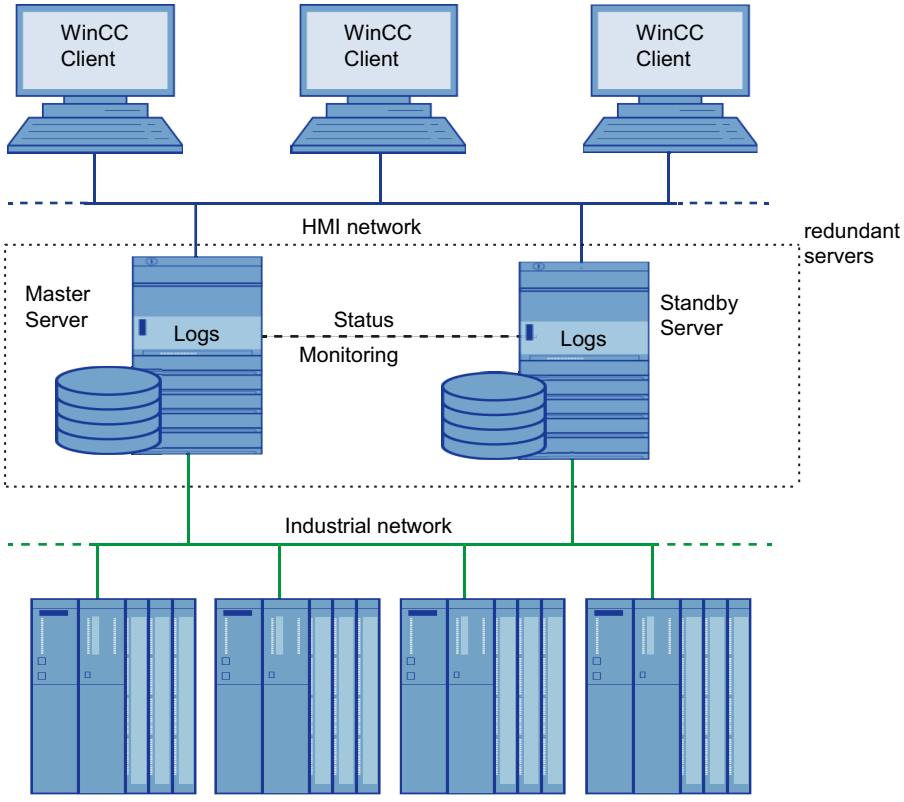
WinCC Logging in Normal Operation

Normally, the master servers run completely in parallel with one another in Runtime. Each server computer has its own process driver connection and has its own data logs. The process data and alarms from the AS are sent to both servers simultaneously where they are processed accordingly.

The servers monitor each other during runtime to allow early recognition of the failure of a partner, which is then indicated by an alarm to the instrumentation and control.

User logs, internal alarms and internal tags can be continuously synchronized online (Online Synchronization).

Both servers have equal rights and work independently of each other. Both are available to the user. Should one server fail, the partner server is always available for equivalent redundancy.



The redundant servers communicate via the terminal bus to monitor the status and synchronize the logs. The network is a PC-LAN network with TCP/IP protocol. If there is an additional connection via a network adapter and/or a serial connection between the servers, this is used to monitor the status but not to synchronize the logs.

Failure of a Server

Server failure refers to the physical failure of a server, for example, due to a power failure or by turning off the server without shutting it down properly.
If one of the servers fails, the server which is still operating receives and logs the process values and alarms from the AS. This guarantees data integrity with no gaps.

The clients will automatically be switched from the failed server to the redundant partner server. All operator stations are thus available again after a short switchover time.

Factors Triggering the Client Switch

The switch of the clients from the default (master) server to the partner server during a server failure is performed automatically by the system. The following factors cause a switch of servers:

- Network connection to server failed
- Server failure
- Process connection error
- The "Application Health Check" function has detected a defective WinCC application and triggers a switchover.
- The project is deactivated.

Factors triggering log synchronization after the server returns

The synchronization of the logs between the servers is initiated after the following errors have been corrected:

- Process connection error. Process connection monitoring may be turned off. For further information see "Configuration".
- Network connection failure to the partner server
- Server failure
- Project is not activated

Synchronization after the server returns

After the failed server comes back online, the redundancy performs a log synchronization for the down time. The gap in the logs caused by the failure is closed by transferring the missing data to the filed server. This action equalizes and makes both servers available again.

The following logs are synchronized:

- Alarm log
- Process value log
- User log
- Internal tags

The failed server receives its data after a slight time delay (caused by the failure). The log synchronization runs in the background, parallel to WinCC process management and logging. This guarantees the operator control and monitoring of the plant at all times.

Comparing internal tags

The internal tags must have the property "Tag synchronization".

Internal tags are compared on partner computers as soon as one of the tags is modified on one of the redundant servers.

The internal tags also include the system tags that start with the "@" character, e.g., @Current_User or @RM_Master. No online comparison should be configured for system tags.

Synchronization after process connection error

If there is a network error during running operation between a server and one or multiple AS, synchronization is automatically started, if this was configured, after the error was handled.

Online Synchronization

A direct server-to-server synchronization (online synchronization) takes place during alarm logging for internal alarms, in user logs and with internal tags with tag synchronization.

3.1.3 Standard server and preferred server

Standard server

In distributed systems, WinCC Controls receive their data with server prefix from specific servers to display alarms and process data.

You configure a standard server to clients in distributed systems so that data without unique server prefix are requested from this standard server. If no standard server is specified, an attempt is made to access the corresponding data locally. If there is no local data (e.g., alarms and archives), access is denied with an error message.

Preferred server

If you are using redundant servers in your multi-user system or distributed system, you can configure a preferred server for the clients.

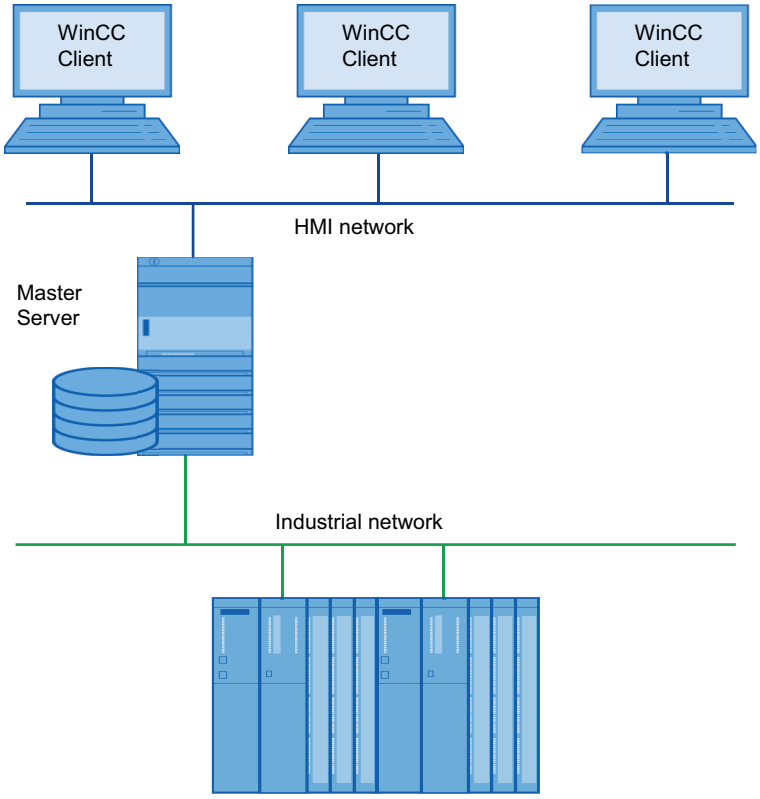
A preferred server is the server of a redundant server pair with which the client in a multi-user system or distributed system primarily interconnects. The preferred server can be selected separately for each client so that the system can be permanently operated.

3.1.4 HMI system without redundancy

WinCC project

A WinCC project consists of a group of automation systems, a server computer and one or more client computers. The project also includes all programs, configuration data and miscellaneous settings.

The tasks of the control level are thus distributed over multiple PCs. The tasks are distributed following to a client server structure.



The above figure shows the typical structure of the WinCC control level, with the corporate level above and the process level below.

Tasks performed by the servers:

- Servers acquire process images and alarms from the automation systems.
- To acquire data, the servers are connected to the automation systems via industrial networks.
- The servers provide the process data to the clients and control the processing states.

Tasks performed by the clients:

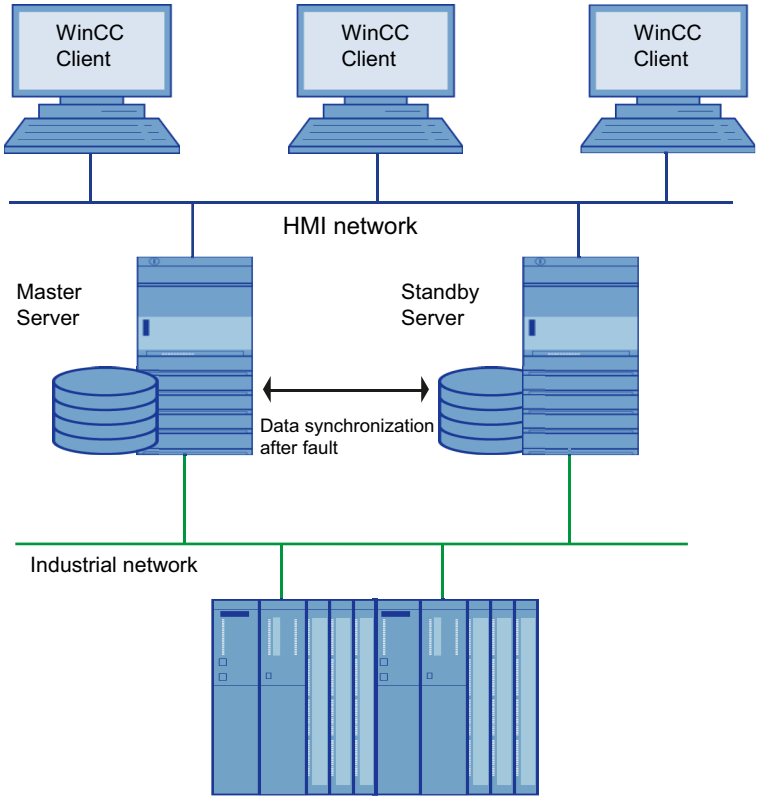
- The client stations operate and monitor the entire plant.
- Clients retrieve the currently needed states from the corresponding server via PC networks.
- In general, all clients are equal and have the same rights.

3.1.5 HMI system with redundancy

WinCC project

A WinCC project consists of a group of automation systems, a server computer and one or more client computers. The project also includes all program data, configuration data and other settings.

Redundant WinCC Project



The above figure shows the typical structure of a redundant WinCC control level, with the corporate level above and the process level below.

A project with a redundant configuration is realized with two configured servers which run in parallel and are functionally identical. The two servers are connected to each other, the AS and the clients. Both servers are configured and displayed as a redundant system in the TIA Portal. The users must make sure that both servers are configured identically.

For further information see "Configuring an identical function".

3.1.6 Requirements

- Only PCs with the following server operating systems can be used for redundant WinCC servers with multi-user mode:
  - Microsoft Windows Server, Version 2008 or higher
- The servers are connected via the network.
- The servers are time-synchronized. We recommend a time synchronization of the entire system (WinCC computer, automation systems, etc.). It can be performed with the "Time synchronization" option in WinCC.
- Alarms and acknowledgments from the AS and clients must always contain a time stamp in the frame to avoid double entries (chronological reporting). A way to achieve this is by using alarm blocks from the ASs.

- Process values, alarms and active alarm blocks from the lower-level automation systems are sent to both servers in parallel.
- The "Redundancy" license is available on each of the two servers.
- The redundancy servers must be configured functionally identical.
- At least one of the following additional connections should exist between the redundant servers:
  - Serial cable
  - Additional network connection via LAN card or via serial connection
    This additional connection ensures a precise definition of the "Master" or "Standby" status. You can also use both connection options at the same time.
    Configure the additional LAN connection via network card or serial connection in the redundancy settings of SIMATIC Shell. Use the TCP/IP protocol with the appropriate IP address or a serial port.

Note

To safely exit WinCC in the event of a power failure, the use of an uninterruptible power supply - UPS - is recommended.

Comparing blocked alarms

When a failed server is restored, currently blocked alarms are searched and compared with the general AS scan in Alarm Logging.

If an alarm is blocked passively, i.e. only on one server, the blocking information is compared.

If an alarm class is blocked on one server, the selection of the block is not compared on the redundant server.

3.1.7 Setting up the servers

3.1.7.1 Structure of a redundant project

Requirement

You must set up and configure two technically identical PCs for a redundant project. You can link up both PCs to each other by means of an additional interface, for example, Ethernet. Configure this link via Simatic Shell on both PCs.

Operating systems

The following operating systems are permitted in a redundant project:

- Single-user system: Windows 7 / 8.1 or Windows Server 2008 / 2012
- Multi-user system: Windows Server 2008 / 2012

Additional information on the necessary user permissions is available in the WinCC information system under "Readme> WinCC Professional> Runtime" under the keyword "Notes on operation of Runtime Professional".

3.1.7.2 Configuring an Identical Function

Tag logs and alarm logs

Archives must be configured with identical function for the redundant servers. Functionally identical means:

- Identical logs, where additions can be made in the form of additional measurement points or logs.

The following logs are synchronized by WinCC:

- Archives held on hard disk, i.e. process value logs, compressed logs and alarm logs.
- On the other hand, no synchronization of main memory logs is performed.

Implementing configuration with identical functions

1. Create a project.
2. Configure this project for redundant servers.
3. Load the project to the redundant server using the "Download to device" function. During this process, the project is compiled and automatically transferred to the master server and the standby server.

This ensures that the project was saved with identical functions on both servers.

3.1.7.3 Redundant recipe data

User logs can be edited by operations, standalone programs, ASs or other functions.

Requirements

The configuration of the logs must be identical on both servers. The projects are always identical when downloaded via the TIA Portal.

Editing user logs in parallel

Note the following when adding data records to redundant user logs in parallel:

- On the server that previously failed, data records can only be added after the server has been restored and the synchronization completed. Otherwise, an error message appears in the script or in the User Archive Control.
- Even during the online synchronization, some time will pass before the data record has been synchronized in the redundant log.

Note

If both servers failed, the computer that was in operation last must be restarted first. Otherwise, changes that have not been saved could be lost.

3.1.7.4 Online Synchronized Messages

All internal alarm tags and alarms without tag connections are synchronized online. This also includes system operator alarms of alarm logging and alarms of Batch-Flexible.

3.2 Configuring the redundant system

3.2.1 Overview of configuration steps

This section describes the configuration of a redundant project using an example. The sample project consists of two identical servers and three clients. In the redundant project, one server is defined as master server and the other as standby server. During the configuration in the TIA Portal, both redundant servers are mapped as one server, symbolic for the redundant system.

Configuration steps

1. Creating a project (Page 161)
   - Configuring master servers (Page 162)
   - Configuring clients (Page 166)
   - Controlling the plant
2. Configuring redundant servers (Page 162)
   - Configuring master servers (Page 162)
   - Configuring the standby server (Page 164)
3. Configuring server reaction (Page 164)
   - Client switchover
   - Synchronization selection
4. Configuring clients (Page 166)
   - Setting up clients
   - Connecting clients with servers
   - Configuring clients
5. Loading the project to a device (Page 167)
6. Compiling a project (Page 168)

See also

Creating a server (Page 161)

Creating clients (Page 162)

Creating a project (Page 161)

3.2.2 Creating a project

Configuration sequence

The TIA Portal is open.

1. Click "Create new project".
   A new project is created.
2. Change to project view.

You have created a project. You can now create devices in the project.

See also

Overview of configuration steps (Page 160)

3.2.2.1 Creating a server

Note

In a redundant project you only map the master server as device in the "Devices & Networks" editor. You perform the division into a redundant system of master server and standby server in the section "Configuring redundant servers".

1. Double-click "Add new device" in the project tree.
   The "Add new device" dialog box opens.
2. Enter the required device name in the text box.
3. Click the "PC systems" selection.
4. In the selection list, click "WinCC RT Professional" under "SIMATIC HMI application".
5. Confirm your selection by clicking "OK".
   The server is created. The work area is opened with the device view and the new device is displayed.
   In the project tree, the new device is created under the selected name.
6. Click in the device view on the newly created station and enter the physical name of the server under "Computer name" in the Inspector window.

See also

Overview of configuration steps (Page 160)

3.2.2.2 Creating clients

Three clients are created to display the various options with the preferred servers:

1. Double-click "Add new device" in the project tree.
   The "Add new device" dialog box opens.
2. Enter the required device name in the text box.
3. In the selection list, click "WinCC RT Client" under "SIMATIC HMI application".
4. Confirm your selection by clicking "OK".
   The client is created. The work area opens in the device view and the new device is displayed.
   In the project tree, the new device is created under the selected name.
5. Click in the device view on the newly created station and enter the physical name of the client under "Computer name" in the Inspector window.
6. Repeat these steps twice, until three clients have been created.

See also

Overview of configuration steps (Page 160)

3.2.2.3 Control

Switch the work area to "Network view". In the work area, you must have four devices displayed next to each other in the order in which they were created.

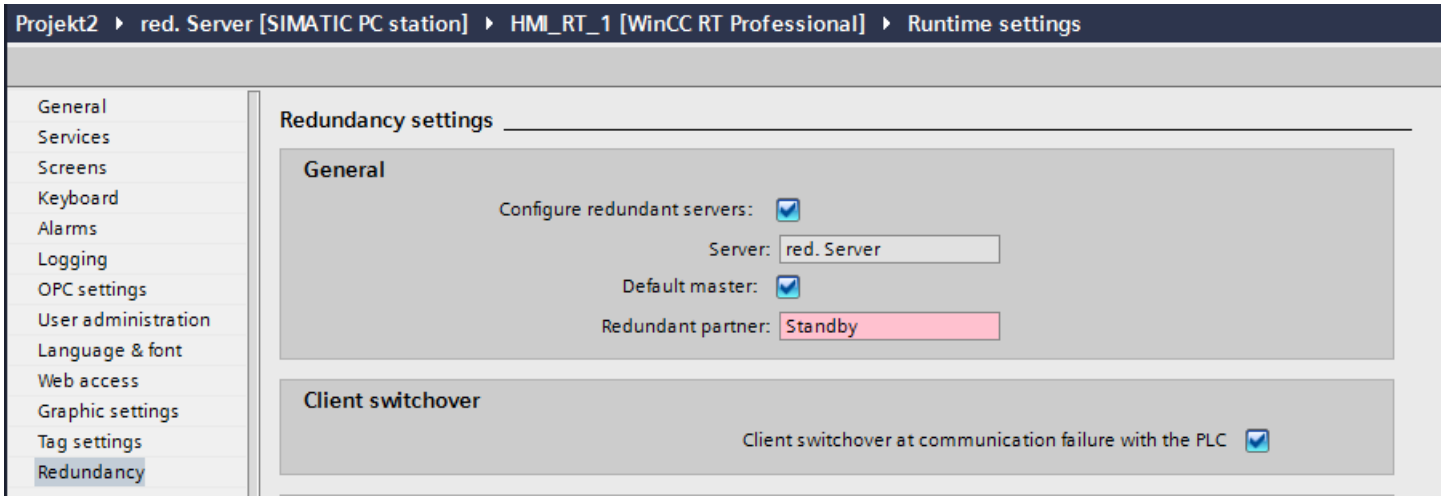
The new devices are displayed one below the other in the project navigation.

3.2.3 Configuring redundant servers

3.2.3.1 Configuring master servers

1. In the network view, click the server that has been created.
   The inspector window opens below the work area.
2. In the inspector window, click the "General" selection under the "General" tab.
   The window shows the server name you have specified.
3. Double-click the name of your server in the project navigation.
   The project navigation offers the following additional options:
   - Device configuration
   - Online & diagnostics
   - HMI_RT_1 [WinCC RT Professional]

4. Double-click "HMI_RT_1 [WinCC RT Professional]".
   The project navigation is expanded by additional setting options.
5. Double-click "Runtime settings".
   The Runtime editor of the server opens in the work area. The "General" setting is opened by default.



6. Click "Redundancy" in the navigator of the Runtime editor.
   The Runtime editor window opens. The name you specified was entered in the "General" box behind the "Server" entry. In this example, "Master" was entered. One of the servers has thus adopted the name "Master" or the name you assigned.
7. Activate redundancy by clicking in the "Configure redundant server" check box.
8. Define the server as "Standard master" by clicking the check box.

Information on configuring the standby server can be found in the next section.

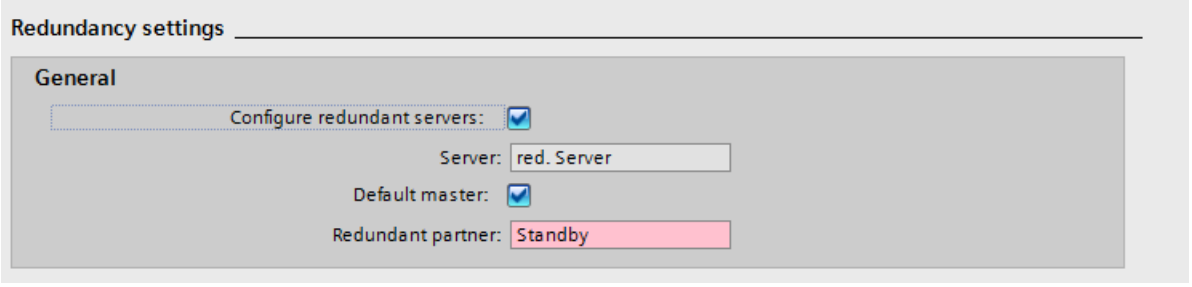
See also

Overview of configuration steps (Page 160)

3.2.3.2 Configuring the standby server

The name you specified was entered in the "General" box behind the "Server" entry. In this example, "Master" was entered. One of the servers has thus adopted the name "Master" or the name you assigned.

1. Enter a name for the redundant partner server in the text box.
   In this example, the second server received the name "Standby".



2. The configuration of the redundant server has now been completed.

Note

Only one device is displayed in the work area. This device includes the redundant server, comprising the master server and standby server.

See also

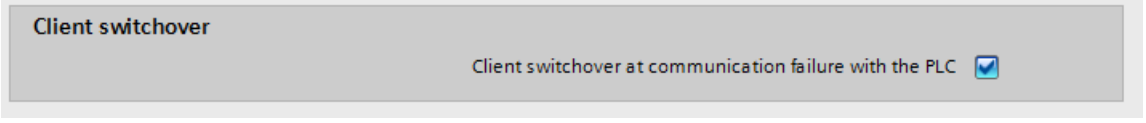
Overview of configuration steps (Page 160)

3.2.3.3 Configuring server reaction

Client switchover

The reaction of the client to communication errors is selected in the "Client switchover" box.

1. By selecting the check box "Automatic client switchover in the case of a PLC error", you activate the automatic switchover of the client to the partner server when communication errors occur in the system.

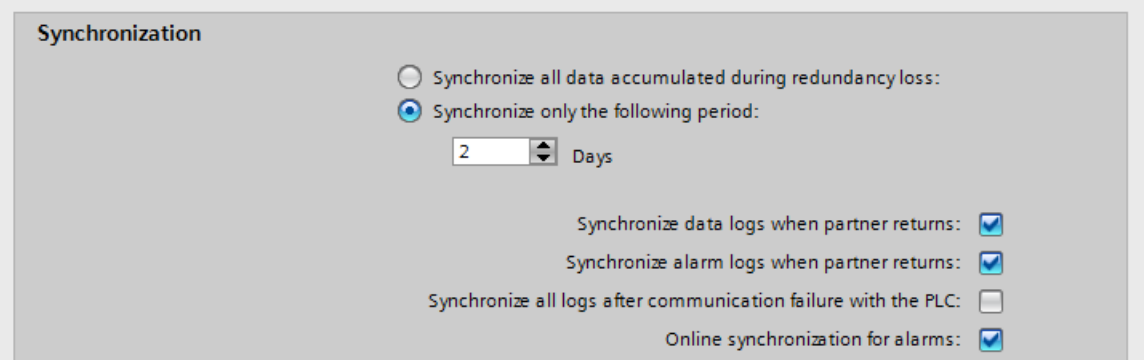


2. Save the project.

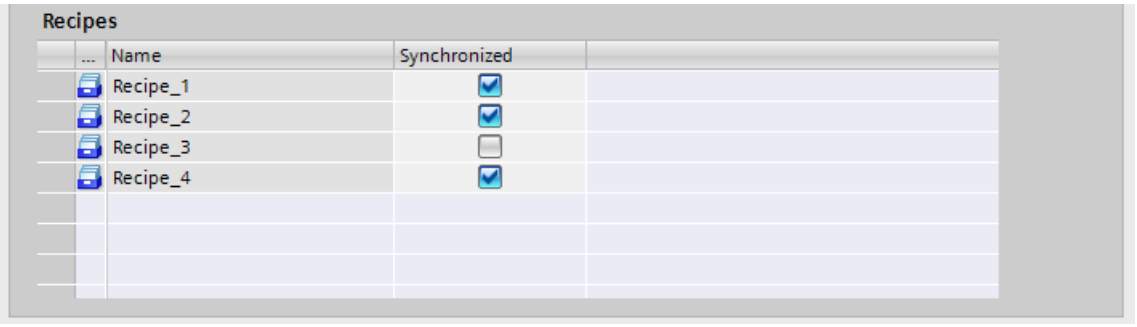
Synchronization

In the "Synchronization" field, you specify which actions are to take place during synchronization of the servers if an error occurs:

1. Click "Synchronize all data in failure time period:".
   All data that was saved during the failure of a server is synchronized when the failed server returns.



2. Click "Synchronize data only for the following time period:"
   In the text box, enter the required time interval for periodic synchronization.
   The data is synchronized periodically independently of server failures.
3. By clicking the four following check boxes, you select the data you want to synchronize after a failure.
4. The recipes used from your recipe log are entered in the "Recipes" list. By selecting the check box in the "Synchronized" column, you select the recipes that you you want to synchronize after a server failure.



5. Save the project.

See also

Overview of configuration steps (Page 160)

3.2.4 Configuring clients

Connecting clients with servers

The work area is in the network view.

1. Connect the redundant server to the Client_1 by clicking on the server connection. Drag the line with the cursor to the connection of Client_1. Keep the left mouse button pressed.
2. Release the left mouse button on the client connection.
   An HMI connection from the server to Client_1 is created and displayed.

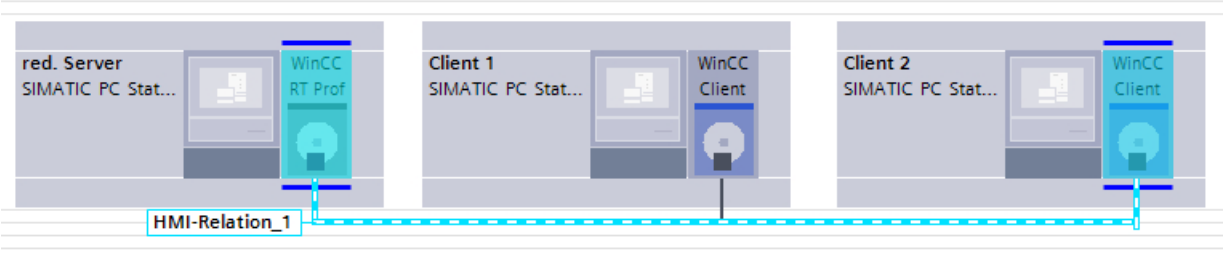


Figure 3-1 Connecting server and client

3. Repeat the process with Client_2 and Client_3.
   You have now connected the servers with the clients.

Configuring clients

1. Click Client_1 in the network view
2. Double-click the name of the client in the project tree.
   The project tree offers the following additional options:
   - Device configuration
   - Online & diagnostics
   - HMI_RT_2 [WinCC RT Professional]
3. Double-click "HMI_RT_2 [WinCC RT Client]".
   The project tree is extended by additional setting options.
4. Double-click "Runtime settings".
   The Runtime editor of the server opens in the work area. The "General" setting is opened by default.
5. Click "Redundancy" in the navigator of the Runtime editor.
   Here you can specify the preferred server of the client.
   - None: The current master is always used. After a change of master because of a failure, the client remains with the must recent current master, also after the return of the failed server.
   - Master: The redundant server set as master is always preferred. After a failure of the master, the client switches back to the master server after its return.
   - Standby: The redundant server set as standby is always preferred. After a failure of the standby, the client switches back to the standby server after its return.

6. Click the appropriate text box to specify the required option of the client.
7. Save the project.

The configuration of the redundant system has now been completed.

An additional activation of the redundant system is not necessary.

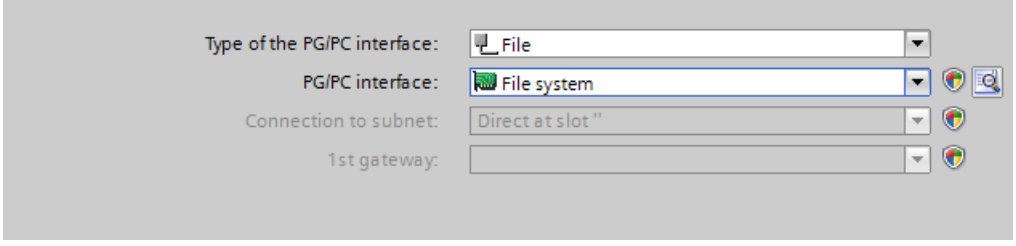
See also

Overview of configuration steps (Page 160)

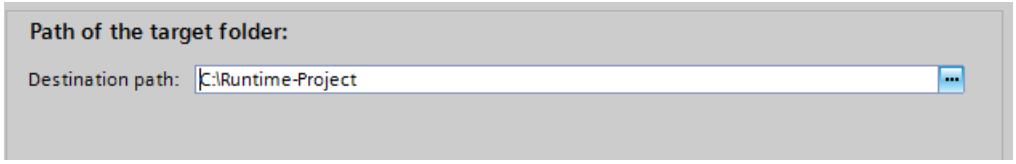
3.2.5 Loading the project to a device

As soon as the "Download to device" function is activated, the project is generally compiled before the actual loading process.

1. For this purpose, open the work area with the devices in the network view.
2. Right-click in the required device to open the shortcut menu.
3. Four options are offered under the menu command "Download to device\":
   - Hardware and software (only changes)
   - Hardware configuration
   - Software (only changes)
   - Software (rebuild all)
     If only the software was changed, the hardware correction options cannot be selected.
4. Click the required action to select it.
   A dialog window opens.
5. Set the type and the PG/PC interface.



6. Set the path of the destination folder. To do this, click the box at the end of the destination path.
   A dialog window opens in which the destination path is set. The destination path is displayed after this:



7. Click the "Load" button.
   The "Load preview" window and a progress window open.
   The project is compiled. The project is transferred to the device after the successful compilation.

An additional reloading of the changes is possible retrospectively, for example, after changes have been made in the hardware or software of the device.

In the case of the first three options, only the changed part is recompiled. In the case of the fourth option, the entire project is recompiled.

See also

Overview of configuration steps (Page 160)

3.2.6 Compiling a project

Compiling data without "Download to device"

Alternatively, the changed data can be compiled using the "Compile" command, without downloading it immediately to the device.

1. Open the work area with the changed devices.
2. Right-click in the required device to open the shortcut menu.
3. Four options are offered under the menu command "Compile\":
   - Hardware and software (only changes)
   - Hardware (only changes)
   - Software (only changes)
   - Software (rebuild all)
4. Click the required action to select it.
   In the bottom window, the result of the compilation is displayed in the "Info" tab.

See also

Overview of configuration steps (Page 160)

3.3 Migrating a redundant project

3.3.1 Migrating a redundant project

Requirements for migration

You can only migrate projects that were created with the software WinCC as of Version 7.2 or Step 7 Plus as of Version 5.5.

Migrating a project

To migrate a project, load it with "Migrate project":

1. Click "Migrate project" in the project view.
   The work area is changed. You are prompted to enter a source path in the text box.
2. Alternatively, click "..." at the end of the text box.
   A dialog window opens.
3. Navigate to your project.
4. Select your project.
5. Click "Open". The source path and the name of your project are entered in the respective boxes.
6. You can use a check box to select whether the data should be copied from WinCC Runtime.
7. Enter the required destination path and, if necessary, another project name in the text boxes of the destination.
   Alternatively: Click the box "..." at the end of the destination path. A navigation window opens in which the destination path can be entered.
   - Click the "Migrate" button.
   - The project is migrated.
   - The project data is then saved.
   - The portal view opens.
   - A window shows the progress of the migration.
   - Finally, a windows indicates that the migration has been successfully completed.
8. Click "OK" to confirm the end of the migration.

The migration of the project was successfully completed. To check, double-click the "Devices & Networks" command in the project navigation. The project opens in the work area in the network view.

3.4 System behavior in the event of a fault

3.4.1 Failure scenarios

Introduction

Some failures that might occur will be used to illustrate how WinCC Redundancy works. The following failures will be discussed:

1. Project is on the redundant AUTOHOTSPOT
2. Connection Fault to Partner Server
3. AUTOHOTSPOT
4. AUTOHOTSPOT
5. AUTOHOTSPOT
6. Changing the client in case of a process coupling error (Page 176)

WinCC Redundancy recognizes the current error itself or reacts to error or fault alarms with the following actions:

- Saving times and events
- Log synchronization
- Changing "Master"/"Standby" identifiers
- Switching clients
- Issuing alarms

Startup of the Server PCs

When the server PCs are starting up, the redundancy component establishes whether the partner server is already active. If the partner server is active, a Standby identifier is set in the server PC. If the partner server is not active during startup, a master identifier is set in the server PC. Upon disruption of the network connection between servers or if the partner server has been turned off, the "Master" code is reset.

In order to identify that the server computer is set as "Master", the system tag @RM_MASTER is set. If the server computer is "Standby", the @RM_MASTER tag is reset. The @RM_MASTER_NAME tag contains the name of the server PC that has the "Master" status, for example, "SERVER1". The tag @RedundantServerState displays on each redundant server its redundancy status, for example, "Standby". These tags can be evaluated by other applications or by scripts. However, the only tag that can be changed is @RM_MASTER.

Redundancy only sets the above tags. Both servers are always completely equal.

If neither a client nor the redundant partner server can be reached for the master server (e.g. project not activated on the PCs, or the network connection between the PCs is interrupted), this then becomes the standby server. This behavior is necessary to ensure that both redundancy servers do not receive the "Master" state.

If there is an additional connection between the two partner servers, the redundancy status is controlled via this connection. This will prevent that redundant partner servers assume the identical status.

Note

Please note that no log synchronization is performed via the serial interface.

3.4.2 Server not in Runtime

Introduction

This scenario discusses the behavior of redundancy, if the project has been deactivated on Server 2.

The following actions will be triggered:

- Server 1 stores the failure time (date and time) of Server 2.
- Server 1 will report the failure of Server 2 through a system alarm.
- If Server 1 is the standby server, this takes over the role of the master by setting the @RM_MASTER tag. Correspondingly the @RM_MASTER_NAME and @RedundantServerState tags are changed.
- The clients connected to Server 2 switch over to Server 1.

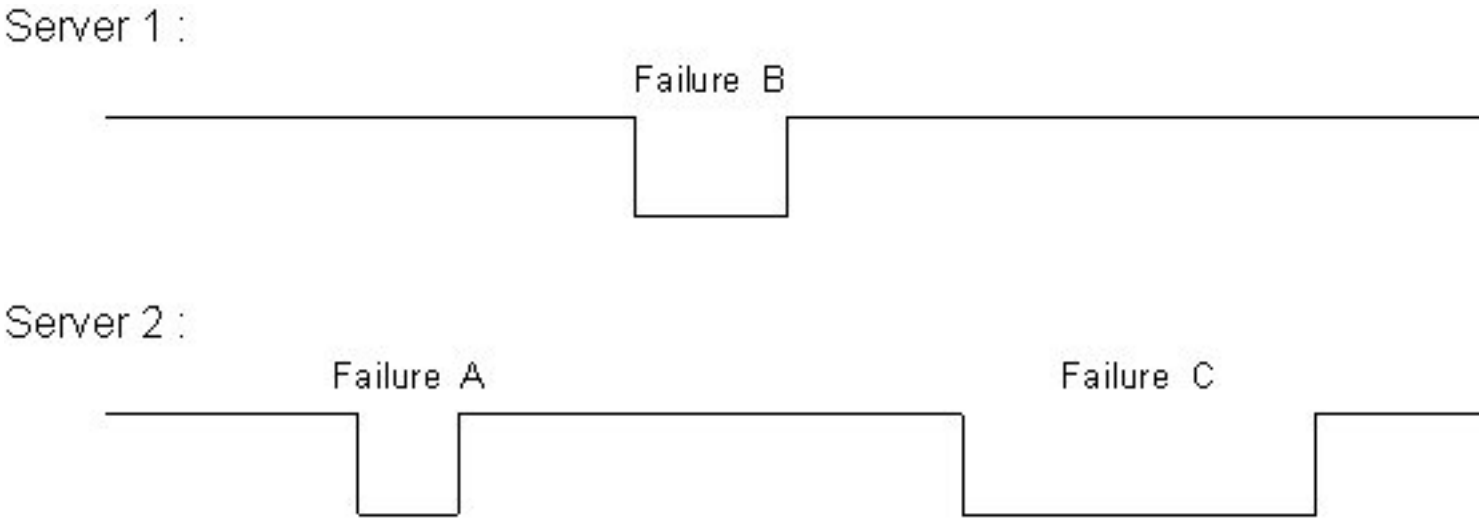
Server 2 Comes Back Online

The downtime means that there is a gap in the logs of Server 2. This gap is filled by the following measures:

- Server 1 stores the return time (date and time) of Server 2.
- Server 1 will report the return of Server 2 through a system alarm.
- A redundancy match is carried out for alarm data, process data and user logs from Server 1 to Server 2.
- The @RM_MASTER tags remain unchanged in both servers, i.e., the @RM_MASTER tag in Server 1 remains set and the @RM_MASTER tag in Server 2 is reset. The @RM_MASTER_NAME and @RedundantServerState tags also remain unchanged.
- Clients which are configured with Server 2 as their preferred server switch back to that server.

Compared to online synchronization, log synchronization following a server failure can take noticeably longer depending on the number of data records to be synchronized and the computer/network loads.

If failures alternate between the two servers (see diagram), they will be synchronized one after the other. After the synchronization, all data will be available in both logs.



In the case above, Server 1 first passes all values to Server 2 for failure A, then Server 1 synchronizes itself from Server 2 for downtime B. Synchronization always occurs on the "Standby" server based on the "Master" server.

All these processes run automatically and in the background, independently of the process value logging and alarm logging from the subordinate automation systems running in parallel.

3.4.3 Connection Fault to Partner Server

Introduction

This scenario discusses the behavior of redundancy in case of connection failures to Server 2. Prior to the occurrence of this event, both servers run in Runtime without failures.

The described connection failure occurs if, for example, the terminal bus at Server 1 is pulled.

Initial Situation 1

Upon connection failure, Server 1 has the "Master" status and Server 2 the "Standby" status.

Connection failure occurs

The following reactions are triggered upon occurrence of the connection failure:

- Server 2 becomes the master server and saves the time of failure (date and time).
- Server 2 indicates by means of a system alarm that the partner server has failed and Server 2 has switched to the "Master" status.
- Server 1 indicates by means of a system alarm that a failure has occurred in redundancy mode and that Server 1 has switched to "Standby" status.
- Tags @RM_MASTER, @RM_MASTER_NAME and @RedundantServerState are reset on both servers according to the switchover.

Connection is restored

During the connection fault, the alarms of Alarm Logging and the user logs could not be synchronized.

This situation is remedied by the following measures:

- Server 2, which is now the master, saves the time of the restoration (date and time).
- Server 2 indicates, by means of a system alarm, the return of the partner server.
- Redundancy synchronization from master server to standby server.
- Through the online synchronization of Alarm Logging, the system alarm concerning the return of the partner server is also displayed on Server 1.
- The @RM_MASTER, @RM_MASTER_NAME and @RedundantServerState tags remain unchanged in both servers.

Initial Situation 2

Upon connection failure, Server 1 has the "Standby" status and Server 2 the "Master" status.

Connection failure occurs

The following reactions are triggered upon occurrence of the connection failure:

- Server 2 becomes the master server and saves the time of failure (date and time).
- Server 2 displays, by means of a system alarm, the failure of the partner server.
- Server 1 indicates, by means of a system alarm, that a failure occurred during redundancy mode and remains the standby server.
- The @RM_MASTER, @RM_MASTER_NAME and @RedundantServerState tags remain unchanged in both servers.

Connection is restored

During the connection fault, the alarms of Alarm Logging and the user logs could not be synchronized.

This situation is remedied by the following measures:

- Server 2 saves the time of return (date and time)
- Server 2 displays, by means of a system alarm, the return of the partner server
- Redundancy synchronization from master server to standby server
- Through the online synchronization of Alarm Logging, the system alarm concerning the return of the partner server is also displayed on Server 1
- The @RM_MASTER, @RM_MASTER_NAME and @RedundantServerState tags remain unchanged in both servers.

3.4.4 Faulty network connection to client

Introduction

In this third scenario, a disturbance occurs in the network connection between Server 2 and the client "CL5" that belongs to Server 2.

The following actions will be triggered:

- Client "CL5" automatically switches over from disturbed Server 2 to running Server 1.

End of the Network Disturbance to the Client

The following reactions are triggered at the end of the network disturbance:

- The @RM_MASTER, @RM_MASTER_NAME and @RedundantServerState tags remain unchanged in both servers.
- If Server 2 is configured as the preferred server for client "CL5", then client "CL5" switches back to that server once more.

3.4.5 Faulty Process Connection

Introduction

In scenario 4, on Server 2 there is a fault on the process link due to an interrupted network connection to the automation systems.

An AS connection error is only recognized by Redundancy as a failure, if the connection is interrupted to only one server. If there is a connection fault from one AS to both servers (e.g. caused by an AS failure), this will not be recognized as a failure by Redundancy.

If WinCC recognizes a failure, the following actions will be triggered:

- The disturbance of the process link is reported on Server 2.
- Server 1 receives a message that partner Server 2 has failed.
- Server 1 stores the failure time (date and time) of Server 2.
- If in the server project "Client change with disturbance in the process link" is configured, the clients linked to this server are changed to the partner server.
- In Server 1, the @RM_MASTER tag is set to Master, in Server 2 to "Standby". Correspondingly the @RM_MASTER_NAME and RedundantServerState tags are adapted. In sever 1, @RedundantServerState is set to "Fault".

Correction of the Process Link Error on Server 2

Provided process connection monitoring has been activated, the gap in the archive of Server 2 will be filled by the following measures:

- Server 1 stores the return time (date and time) of Server 2.
- A redundancy match is carried out from Server 1 to Server 2, since no faults were found for process connection at Server 1. The data of all ASs will be synchronized. This means that the data of ASs that have not failed will also be synchronized.
- On Server 2 the @RedundantServerState tag is changed from "Fault" to "Standby".
- The correction of the process link error on Server 2 is announced by a system message.

3.4.6 Software Error

Introduction

In scenario 5, an error occurs on Server 2 in software that is being monitored. When the error occurs, Server 2 is "Master" and Server 1 is on "Standby" status. There are several clients connected to each server.

If the "Application Health Check“ function detects an error in the WinCC software, the following actions are initiated:

- Application Health Check reports the error to redundancy. The status of Server 2 is set in the @RedundantServerState tag to "Fault". The @RM_Master tag is set to "Standby".
- The @RM_Master tag in Server 1 is set to the "Master". Correspondingly the @RM_MASTER_NAME and RedundantServerState tags are adapted.
- The clients connected to Server 2 switch over to Server 1.
- A process control message warns the user about the software error.

Correction of the Software Error on Server 2

The software error can be cleared by deactivating the server project and restarting server. When the project is activated on Server 2 the archives are automatically synchronized.

- On Server 2 the @RedundantServerState tag is set to "Standby". Server 1 remains at "Master" status.
- Server 1 stores the return time (date and time) of Server 2.
- A redundancy match is carried out for the user archive from Server 1 to Server 2.

Note

When a software error is detected by the "Application Health Check" function resulting in a client switching process and process control message, the server affected must be deactivated and the computer restarted. Only then can the clients be reconnected to the server. An archive synchronization is only performed backdated to the moment a software error is detected by the server.

3.4.7 Changing the client in case of a process coupling error

Introduction

A redundant system consists of two functionally identical servers. One server is the "Master" server and the other is the redundant partner server. In the normal, undisturbed operating state the "Master" server has the status of "Master" and the redundant partner server has the status of "Standby". Clients are connected to the "Master" server unless a preferred server has been configured, in which case they are connected to the preferred server.

As soon as both servers are in Runtime, the processes coupling monitoring is activated. The number of defective logical connections to the "Master" server and the redundant partner server is cyclically determined. If the "Master" server has more defective logical connections than the redundant partner server, the status of the server becomes invalid ("Fault"). The clients are switched over to the redundant partner server, which now has the "Master" status.

Note

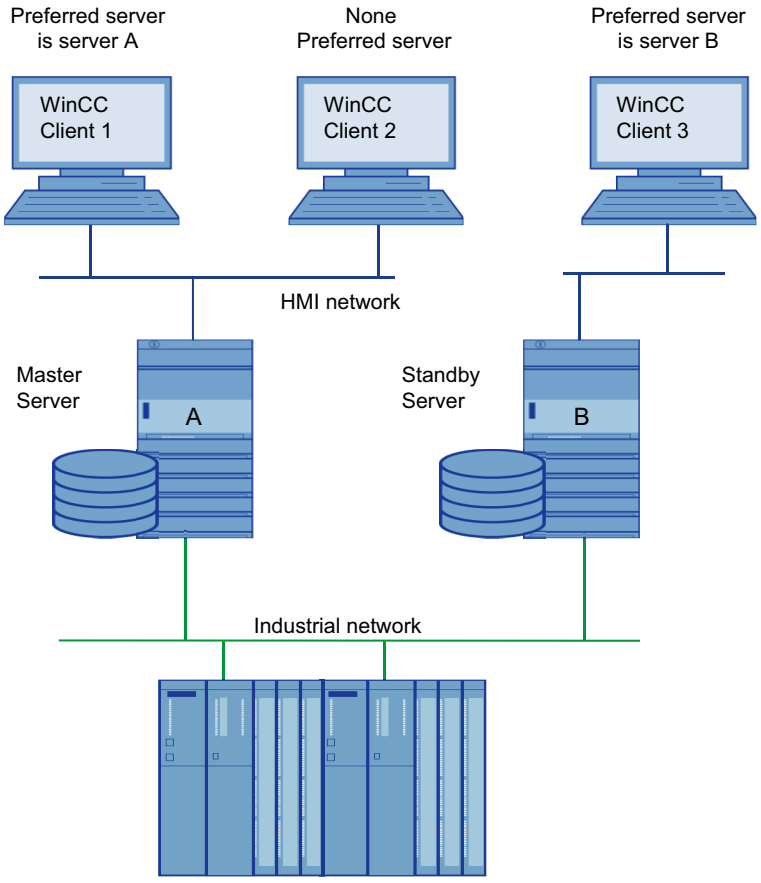
The "Fault" status is not displayed in the "@RM_MASTER" system tag but in the "@RedundantServerState" tag.

Normal operating state

The plant consists of the redundant servers A and B. There are also three clients. Client 1 has entered server A as its preferred server, client 2 has entered no preference and client 3 has entered server B as its preferred server.

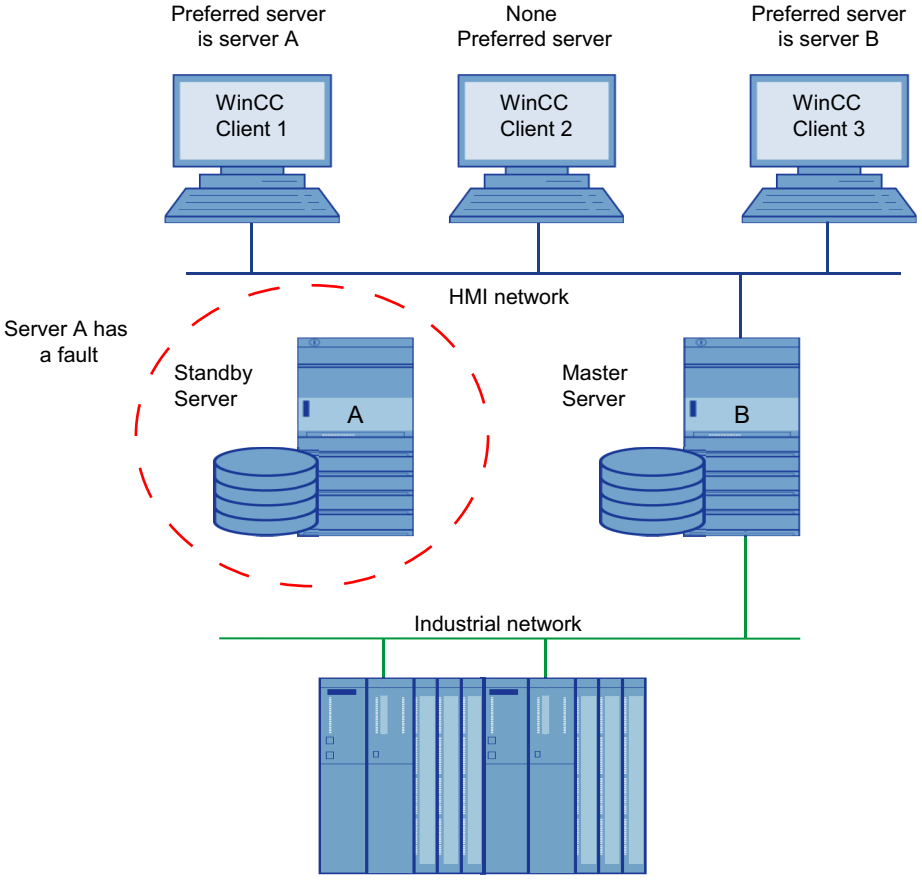
Note

The example below shows the logical connections, not the physical connections. In other words, the connection is shown as separated when the connection is terminated, because the data transfer is interrupted. The physical connection can remain intact at the same time.


Preferred server
is server A
None
Preferred server
Preferred server
is server B
WinCC
Client 1
WinCC
Client 2
WinCC
Client 3
HMI network
Master
Server
A
Standby
Server
B
Industrial network

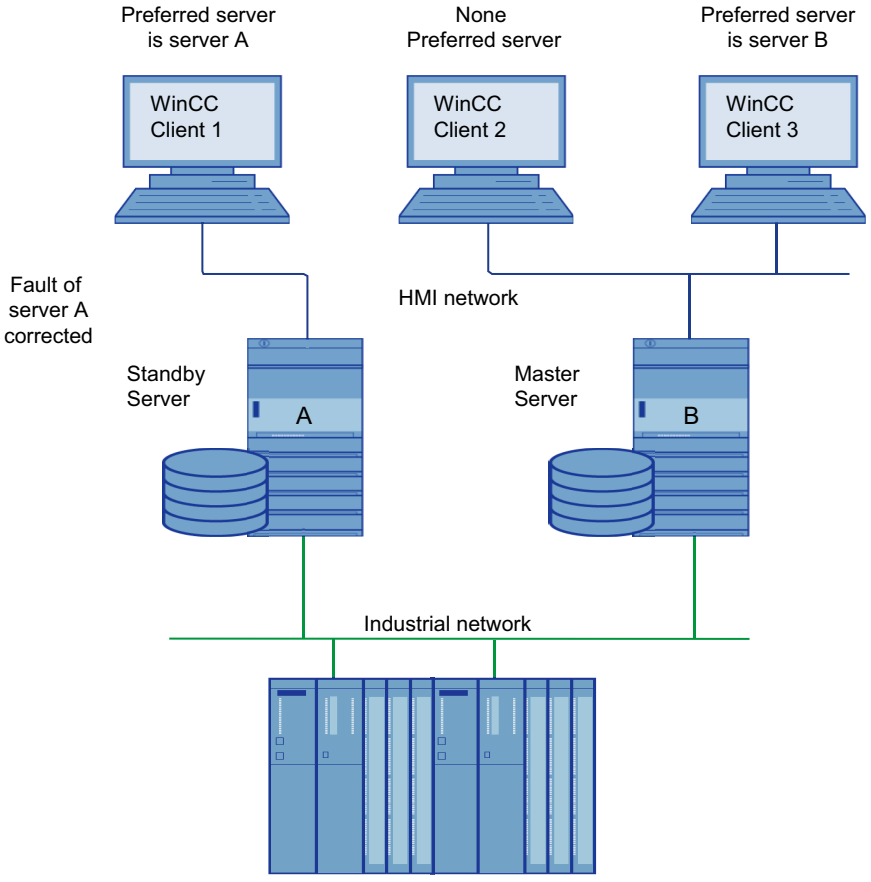
Process connection error on server A

There is a process connection error on server A. The error is not present on server B. The number of defective logical connections on server A is greater than on server B. Server A therefore receives the "Fault" status. As a result, clients 1 and 2 switch over to redundant server B.



End of the process connection error

When the process connection error on server A has been cleared, server A then has the status "Standby". As a result client 1 switches over to server A, since it has indicated this as its preferred server. Client 2 stays connected to server B because this has now become the "Master" server since the Redundancy switchover and client 2 has indicated no preferred server.



Note

The OPC couplers are not monitored. Therefore, there will be no client switching in case of an error in the OPC couplers.

See also

Failure scenarios (Page 170)

3.5 Reference

3.5.1 System messages WinCC Redundancy

Introduction

The "WinCC Redundancy" option provides the following system messages. You can read these system messages on the "System messages" tab in the "HMI Messages" editor.

Message No.	WinCC Message Text
1012200	REDRT:@100%s@:Partner station has failed WinCC was exited on the partner server.
1012201	REDRT:@100%s@: Partner station restarted WinCC was started again on the partner server
1012203	REDRT:@100%s@:Archive synchronization failed
1012204	REDRT:@100%s@:Internal redundancy error
1012205	REDRT:@100%s@:Connection to the partner has been interrupted The connection to the partner server is interrupted
1012206	REDRT:@100%s@:Connection to the partner has been reestablished The connection to the partner server has been reestablished
1012207	REDRT:@100%s@:Partner server - WinCC is not started It was determined at startup that WinCC is not started.
1012208	REDRT:@100%s@:Synchronization launched This message is output at the start of the archive synchronization
1012209	REDRT:@100%s@:Synchronization finished This message is output at the end of the archive synchronization
1012214	REDRT:@100%s@:User archive is being synchonized
1012215	REDRT:@100%s@: User Archive synchronization finished
1012216	REDRT:@100%s@:Archive synchronization canceled Synchronization was canceled by an additional failure
1012217	REDRT:@100%s@:Partner server project has not been activated It was determined at startup that WinCC is not activated on the partner server or is not in runtime
1012220	REDRT:@100%s@: Synchronization is not ready for all User Archives. The synchronization is not ready for all locally configured user archives, because the archive structure of the partner is different for at least one archive or synchronization is not activated on the partner.
1012221	REDRT:@100%s@: Synchronization is ready for all User Archives. The synchronization is ready for the locally configured user archives and the archive structure matches that of the partner.
1012226	REDRT:@100%s@:Partner server project has been activated It was determined at startup that WinCC is active on the partner server.
1012227	REDRT:@100%s@:Error: Partner server is not a server It was determined at startup that the configured partner server is not a server.
1012240	REDRT:@100%s@:RedundancyControl Error @1%s@ in @2%s@ causes state switch
1012241	REDRT:@100%s@:RedundancyControl: Switchover to status @1%s@

Message No.	WinCC Message Text
1012244	REDRT:@100%s@: Overload during Alarm Logging online update Number of messages to be synchronized is too large.
1012247	REDRT:@3%s@:OS server (Master) @1%s@ OS server (Standby) @2%s@ Redundancy error
1012248	REDRT:@3%s@:OS server (Master) @1%s@ OS server (Standby) @2%s@ Redundancy recovered
1012349	REDRT:@1%s@:RedundancyControl: Loss of connection via network card with MAC address @ 2%s@.
1012350	REDRT:@1%s@:RedundancyControl: Connection via network card with MAC address @2%s@ has been reestablished. The connection to the partner server has been reestablished via redundant LAN.
1012351	REDRT:@100%s@:RedundancyControl: System blockage detected. Switch to Fault status.
1012352	REDRT:@100%s@:RedundancyControl: System blockage detected. Restart your computer as soon as possible.
1012353	REDRT:@100%s@:RedundancyControl: Status changed to FAULT. However partner server is not available.
1012354	REDRT:@100%s@:RedundancyControl: Status changed to FAULT. However server isolation is not activated.
1012355	REDRT:@100%s@:RedundancyControl: Status changed to FAULT. However server isolation is locked by @1%s@. Reason: @2%s@
1012356	REDRT:@100%s@:RedundancyControl: Status changed to FAULT => server is isolated
1012357	REDRT:@100%s@:RedundancyControl: Status changed to FAULT. However automatic restart is not activated.
1012358	REDRT:@100%s@:RedundancyControl: Status changed to FAULT. However automatic restart is locked. The network adapter is disconnected and DHCP is released.
1012359	REDRT:@100%s@:RedundancyControl: Reboot of computer disabled by @1%s@. Reason: @2%s@
1012360	REDRT:@100%s@:RedundancyControl: Restart of the computer is canceled. The last restart took place less than @1%s @ s ago.
1012361	REDRT:@100%s@:RedundancyControl: Restart of the computer is canceled. After @1%s@ restarts no further restarts are permitted for @2%s@ s.
1012362	REDRT:@100%s@:RedundancyControl: Rebooting computer in @1%s@ s

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

4

4.1 Basics (Panels, Comfort Panels, RT Advanced)

4.1.1 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).

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.

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

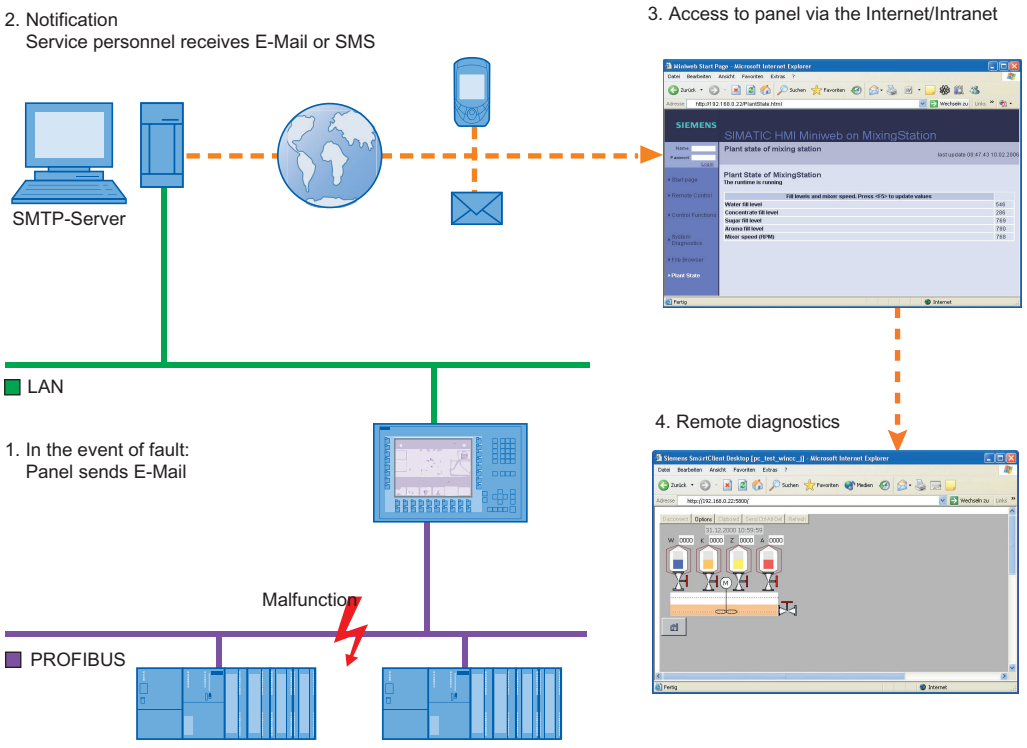
On devices with version V11 or V12, the password "100" is preset for the Sm@rtServer and for the integrated Web server. This password should be changed for security reasons.

On devices with version V13, no passwords are preset.

4.1.2 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.

4.1.3 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
In view mode only: • Mobile Panel 277 IWLAN • Mobile Panel 277 IWLAN V2 • 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	--

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

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

Introduction

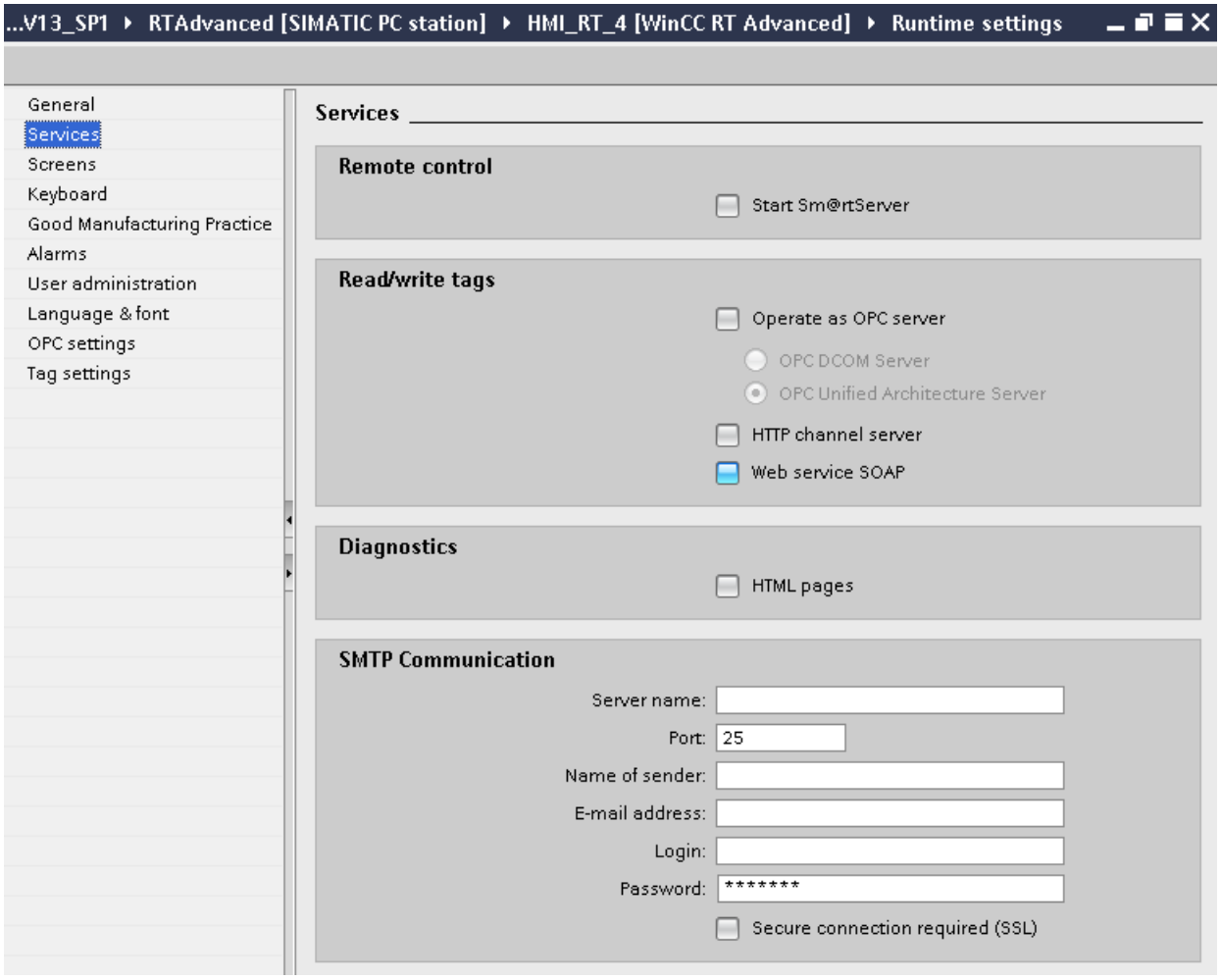
In the "Runtime-Settings" Editor, configure the requirements for using the Sm@rt Options.

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".



"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.

4.1.4.2 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 191)
- WinCC Runtime Advanced Internet, "Proxy" tab (Page 192)
- WinCC Runtime Advanced Internet, "Web Server" tab (Page 193)
- WinCC Runtime Advanced Internet, "Remote" tab (Page 194)

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 receipient 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 Adress 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 190)

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

- "No authentication": No authentification is required for access.
- "Authentication required": An authentification 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 box

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: Current User Properties" dialog for specifying the passwords, authorizations, the screen update mechanism and the behavior when connections are disconnected.

Note

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

The dialog contains the following tabs:

- "Server" tab (Page 195)
- "Polling" tab (Page 196)
- "Display" tab (Page 198)
- "Query" tab (Page 198)
- "Administration" tab (Page 199)

Start Remoting

Starts the Sm@rt Server explicitly.

Stop Remoting

Ends the Sm@rt Server explicitly.

"Sm@rtServer Dialog: Current User Properties" (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.

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 sesssions
  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 217)

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)

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

4.1.5.1 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".

4.1.5.2 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

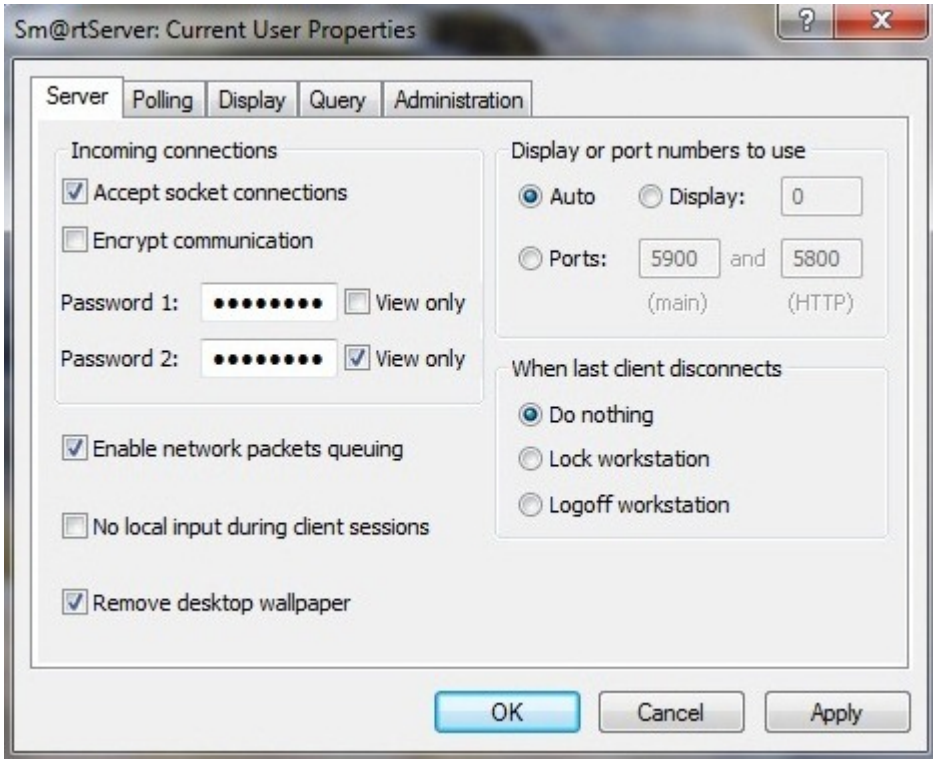
The settings on the server govern which remote operators can access the runtime of the server.

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.

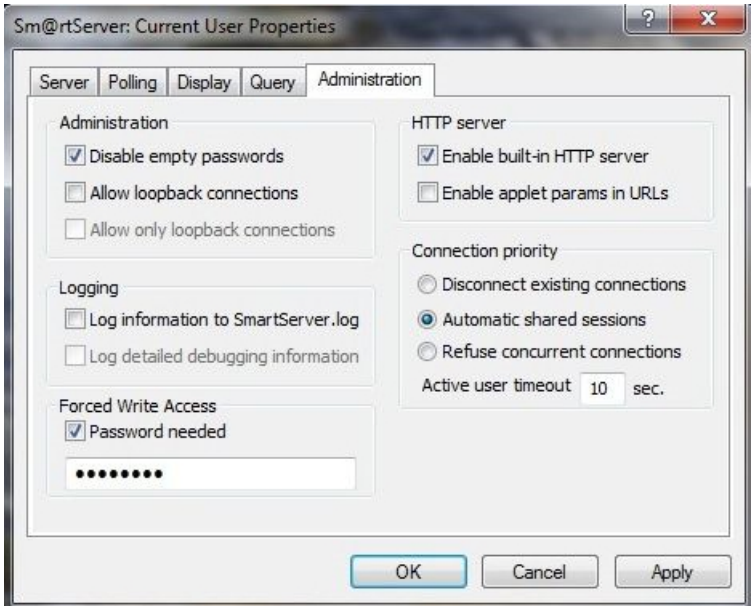
On the panel, this dialog is called "Sm@rtServer: Default Local System Properties" and contains fewer dialog elements than the dialog on the PC.

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 an 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.

4.1.5.3 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.

4.1.5.4 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. The various options for entering the address can be found in "Remote control by means of the Sm@rtClient application (Page 218)".

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

"Options" dialog, "Globals" tab (Page 212)

"Options" dialog, "Connections" tab (Page 210)

"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 ingnored)
  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 209)

"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.

4.1.5.5 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

xP177/277	xP377	PC keyboard shortcut
K16	S16	CTRL + F12
HELP	HELP	ALT + H
ACK	ACK	ALT + F1

4.1.6 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.
- 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".

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

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

4.2.1.1 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.

4.2.1.2 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".

Restrictions

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

See also

"Administration" tab (Page 199)

4.2.1.3 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 Advacned 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 ≤ 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

4.2.1.4 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 detailed instructions on this, refer to "Configure Sm@rtServer (Page 224)".
- The Sm@rtClient-Display in an image is added in the client-HMI device project. For detailed information on this, refer to "Project Sm@rtClient (Page 226)".

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 ≤ 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.

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

4.2.2.1 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).

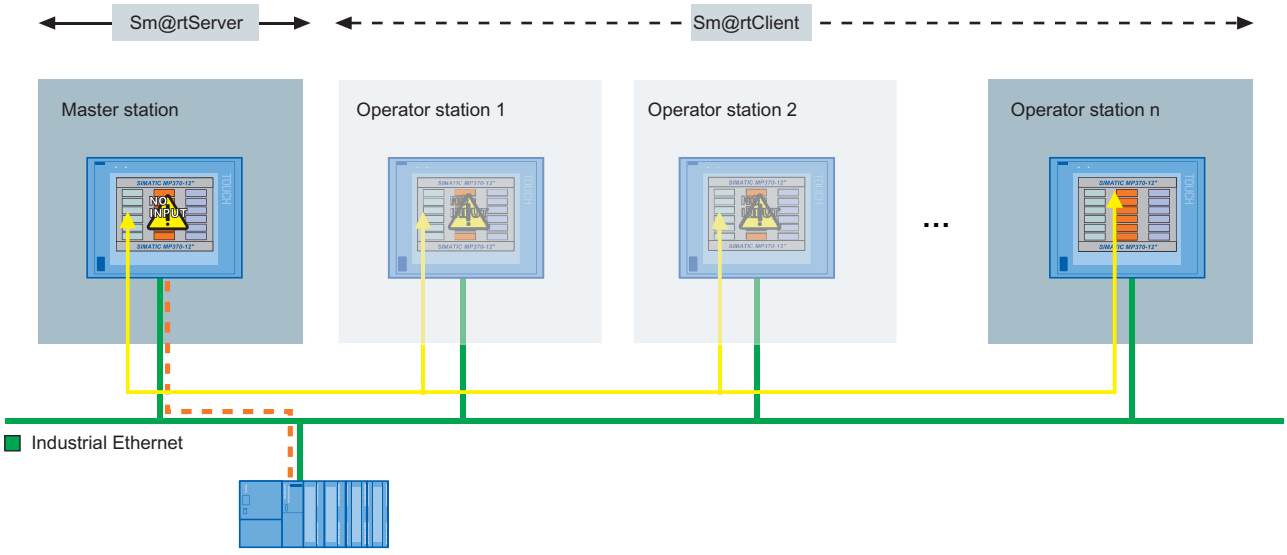


Figure 4-1 Distributed HMI

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.

4.2.2.2 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 224)
2	Setting WinCC Runtime Advanced Internet (Page 225)
3	Project Sm@rtClient (Page 226)

4.2.2.3 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)

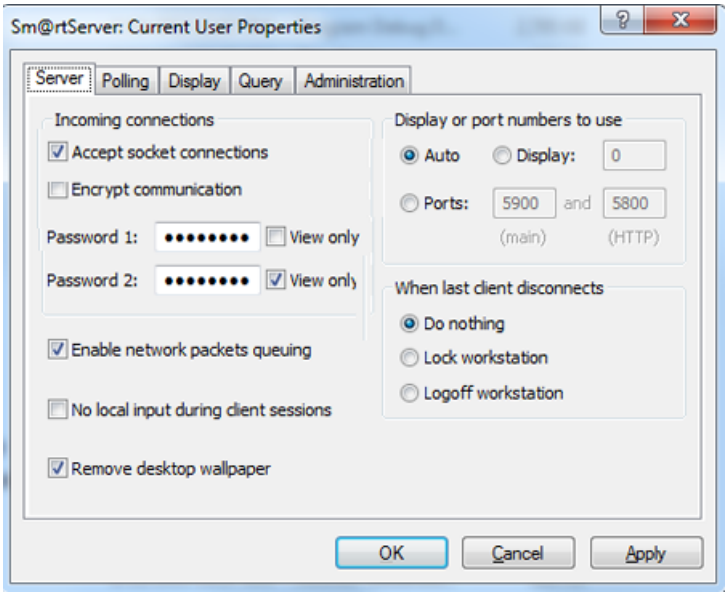
Requirement

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

Procedure

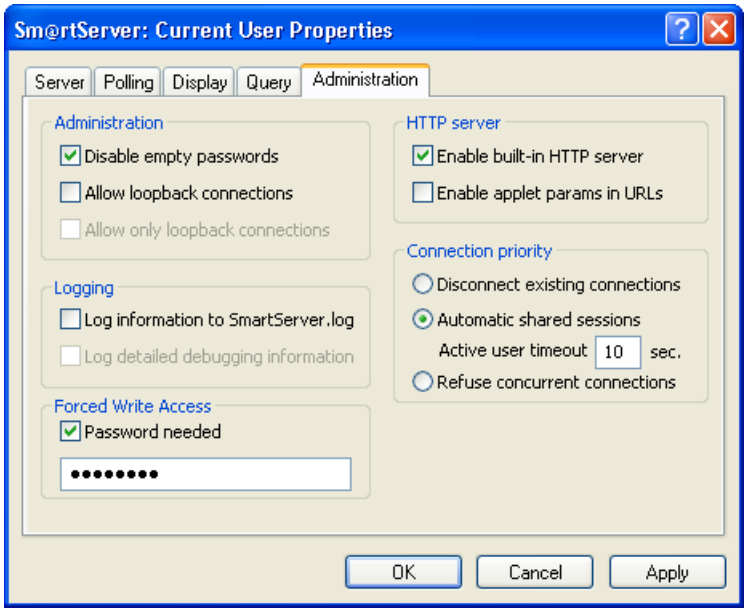
Proceed as follows to change the "WinCC Runtime Advanced Internet" settings on the Sm@rtServer:

1. On the "Remote" tab, select Start automatically after booting".
2. Click on the button "Change settings". The dialogue "Sm@rtServer: Current User Properties" is opened.



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 226)

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

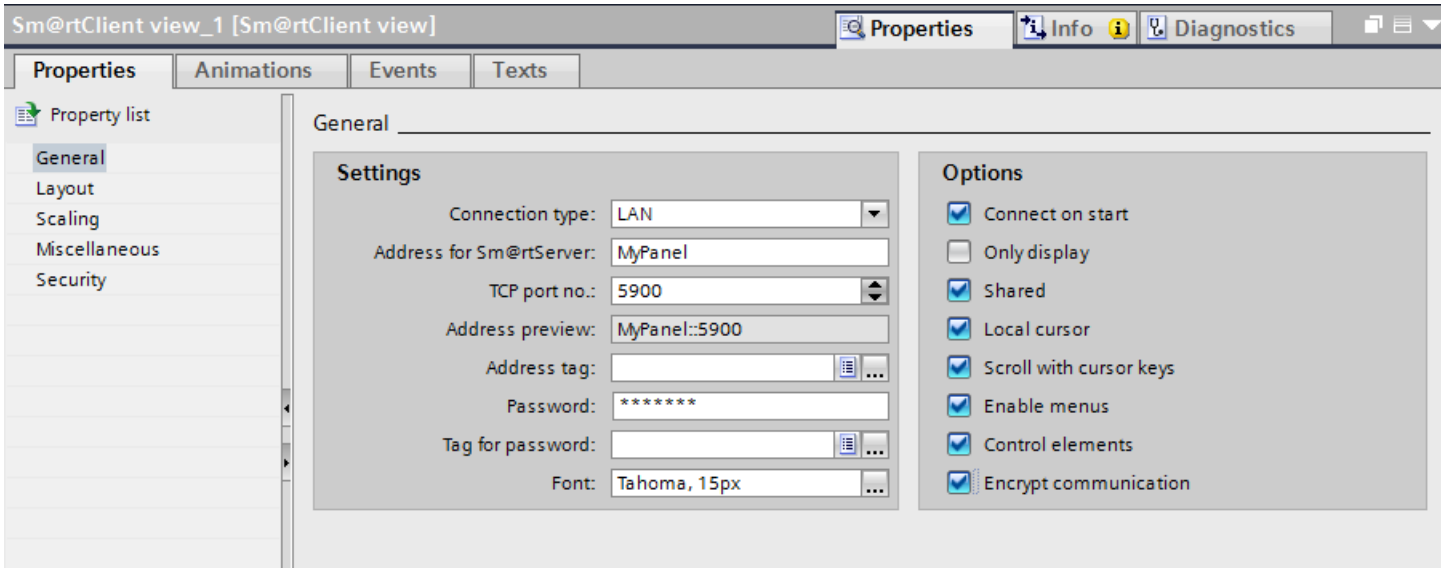
Requirement

- 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 220)

"Server" tab (Page 195)

Setting WinCC Runtime Advanced Internet (Page 225)

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

4.3.1 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.

4.3.2 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.

4.3.3 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 adress 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.

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

4.4.1 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 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.

4.4.2 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.

4.4.3 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.

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

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

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

Requirement

- 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 on "Apply".
6. Click the "Authorizations" tab.

7. Specify on the "Authorizations" tab, which functions can the user carry out on the HTML-pages of an HMI-device. See the section "User administration for web server (Page 201)" for additional details.
8. Close the "UserDatabase-Edit" dialog.
9. On the "Remote" tab, select the "Start automatically after booting" check box.
10. Click "Change settings" and enable in the "Sm@rtServer dialog: Current User Properties", select the checkbox "Enable connections".
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 193)

"Server" tab (Page 195)

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

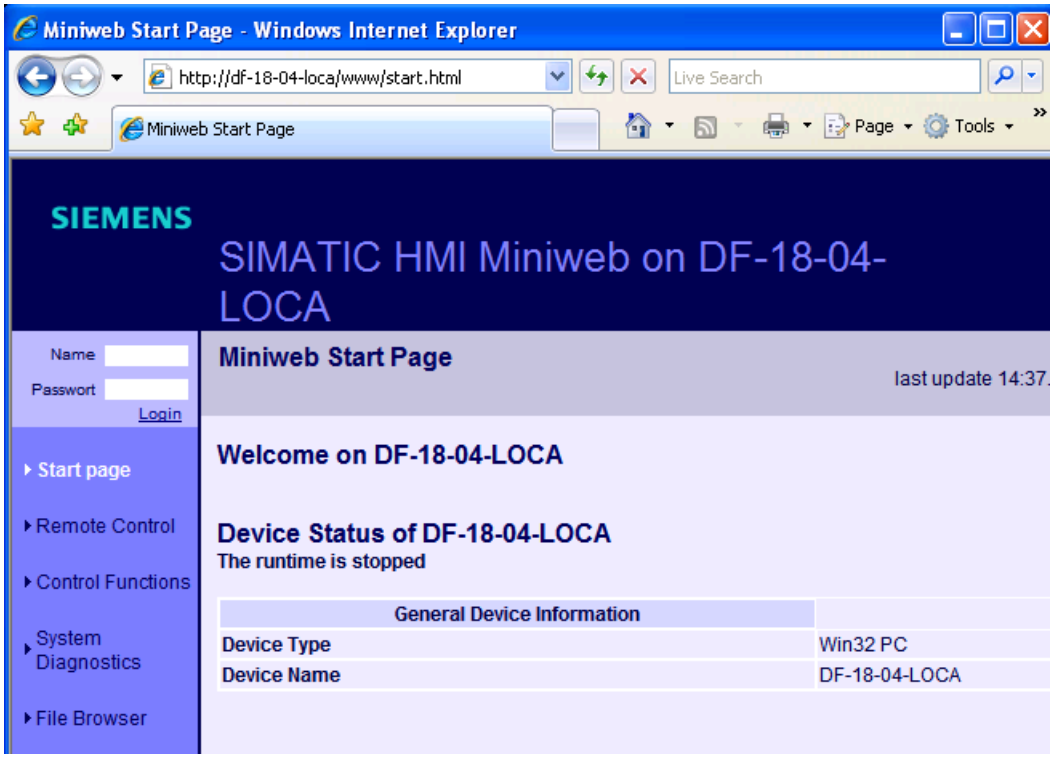
Requirement

- 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"

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

4.4.5.1 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 7: "C.\ProgramData\Siemens\CoRtHmiRTm\MiniWeb11.x.x \WebContent"
- on a PC with Windows XP: "C:\Documents and Settings\All Users\Application Data \Siemens\CoRtHmiRTm\MiniWeb11.x.x\WebContent"
- On xP 177B: "<ES-Installationspath>\Transfer\11.0\XP177B\WebContent.zip"
- On xP 277: "<ES-Installationspath>\Transfer\11.0\XP277\WebContent.zip"
- On MP 177: "<ES-Installationspath>\Transfer\11.0\MP177\WebContent.zip"

- On MP 377: "<ES-Installationspath>\Transfer\11.0\MP377\WebContent.zip"
- on Mobile Panel 177 PN: "<ES-Installationspath>\Transfer\11.0\XP177B\WebContent.zip"
- On Mobile Panel 277: "<ES-Installationspath>\Transfer\11.0\XP277\WebContent.zip"
- On the Mobile Panel 277 (F) IWLAN: "<ES-Installationspath>\Transfer\11.0\XP277_W \WebContent.zip"
- On the Mobile Panel 277 (F) IWLAN V2: "<ES-Installationspath>\Transfer \11.0\XP277_W2\WebContent.zip"

4.4.5.2 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.hml".
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> </td></tr>
<tr><td class="sph_td"><b>"Tags2"</b></td><td class="sph_td"><MWSL><!– write(GetVar("Tag_2")); –></MWSL> </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"><img src="/Images/NaviPfeilblau.gif" alt="" border="0"></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.

4.4.5.3 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:

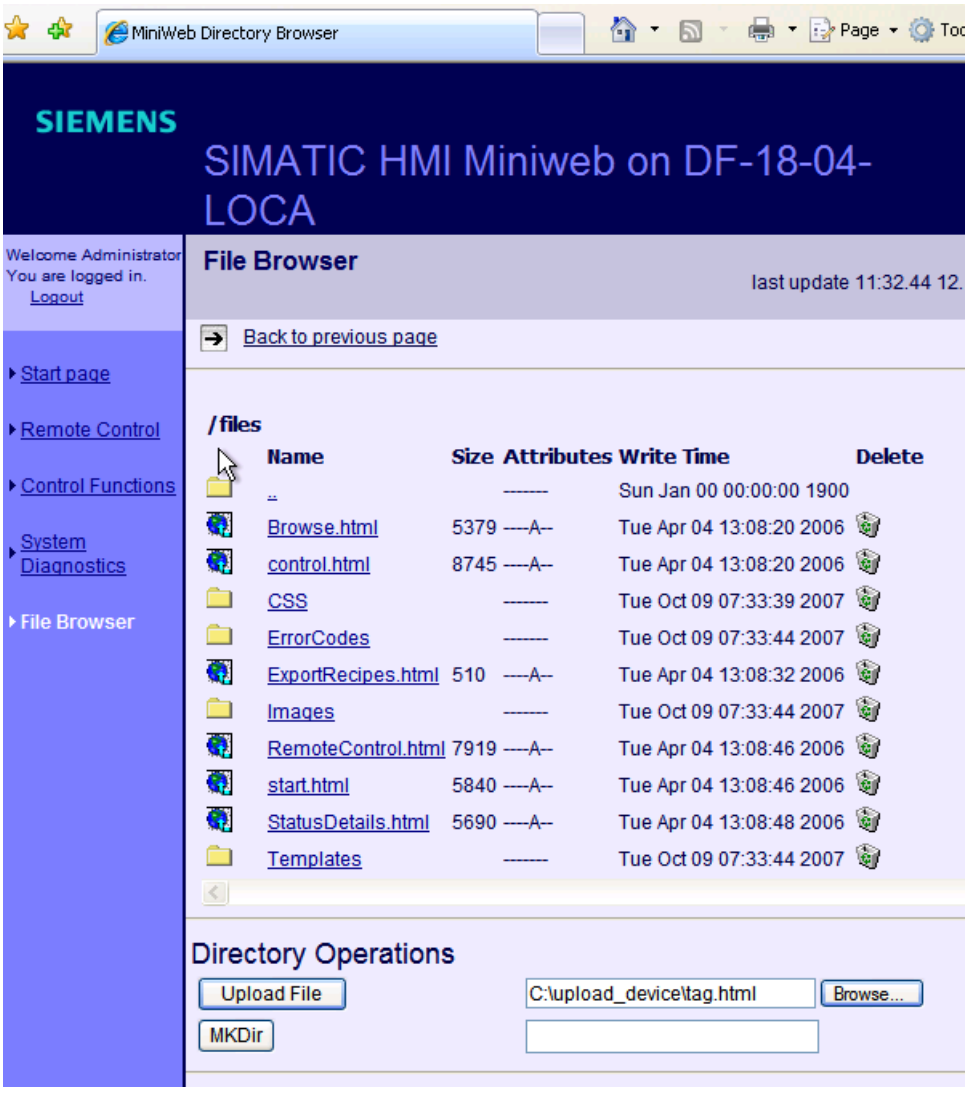
1. Add the changed files to the ZIP-file "WebContents". This file must contain all HTML pages and associated pictures.
   Make sure to provide the correct path information because the files are unpacked in the directories specified in the zip file. Incorrect path information results in errors in direct 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 239)

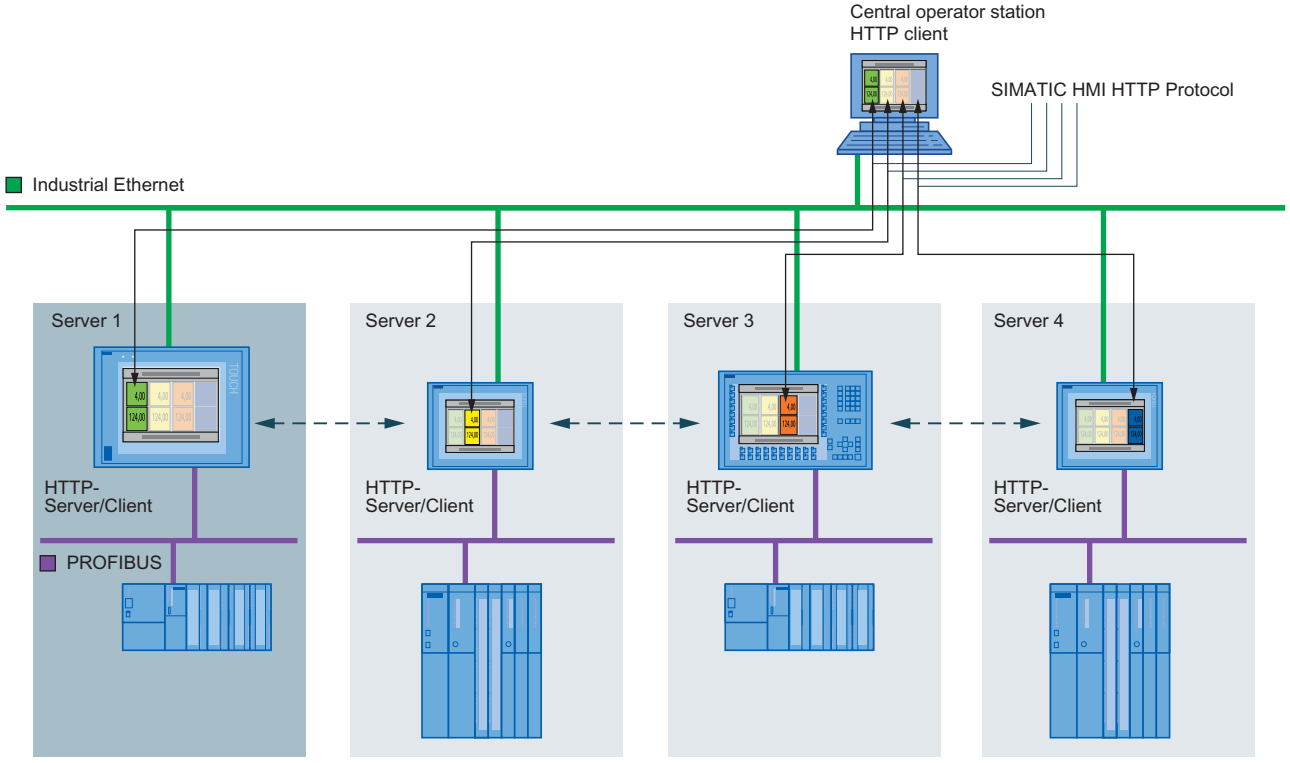
4.5 Access via SIMATIC HMI HTTP Protocol (Panels, Comfort Panels, RT Advanced)

4.5.1 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.



4.5.2 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 246)
2	Setting WinCC Runtime Advanced Internet (Page 247)
3	Configuring HTTP connections in the client (Page 248)
4	Configure the HTTP-Client tags (Page 249)

4.5.3 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 Proto-col	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 246)

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

4.5.4.1 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 245)".
5. Transfer the compiled WinCC-project to the Server-HMI-device.

Result

The HMI-device is HTTP-server configured.

4.5.4.2 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 authentification 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 201) ".
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 190)

WinCC Runtime Advanced Internet, "Web Server" tab (Page 193)

User administration for web server (Page 201)

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

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

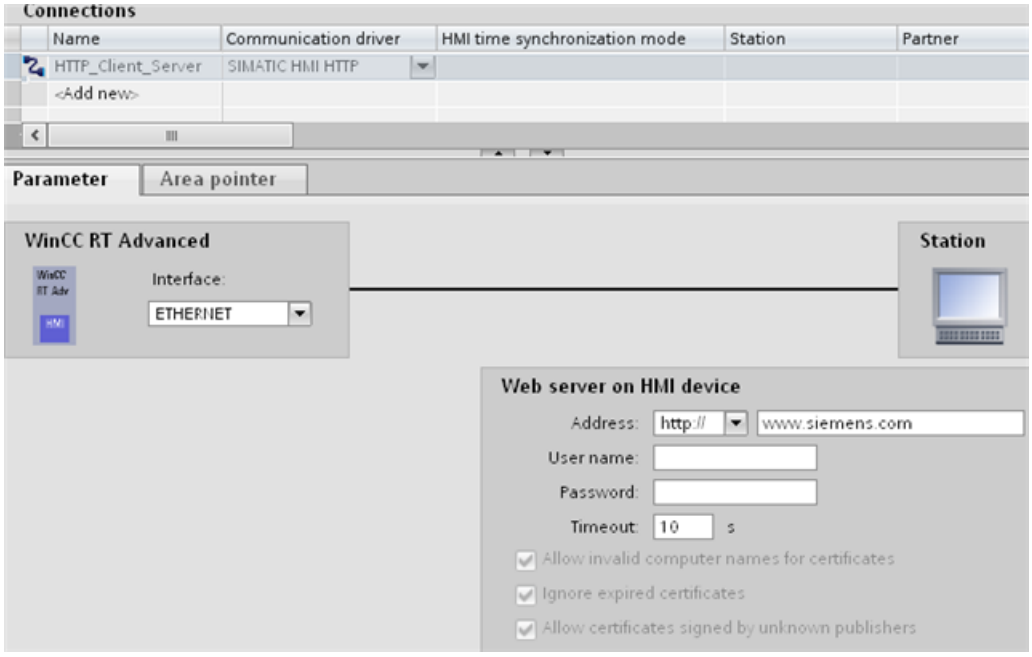
Requirement

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".



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. For detail information for HTTPS-connection, refer to "Commissioning an HTTP- connection (Page 250)".

4.5.5.2 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. For additional information, refer to "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.

4.5.6 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

With the first HTTPS client access, the HTTPS server generates the certificate itself and then saves it in the "Cert.cer" memory. The file is stored in the following directory:

- On a PC / Panel PC (with Windows XP) in the directory "<Runtime-Verzeichnis> \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 XP (PC, Panel PC)	with Windows XP (PC, Panel PC)	• 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, Mobile Panel 277, Comfort Panels)	with Windows XP (PC, Panel PC)	• Memory card • ActiveSync (serial)
with Windows XP (PC, Panel PC)	with Windows CE (xP 277, MP 377, xP 177B, Mobile Panel 177 PN, Mobile Panel 277, Comfort Panels)	
with Windows CE (xP 277, MP 377, xP 177B, Mobile Panel 177 PN, Mobile Panel 277, Comfort Panels)	with Windows CE (xP 277, MP 377, xP 177B, Mobile Panel 177 PN, Mobile Panel 277, Comfort Panels)	• Memory card

Installing a certificate on a client with Windows XP

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.

The "Cert.cer" file generated at the HTTPS server cannot be opened on HMI devices based on Windows CE 5.0 by double-clicking the client.

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.

4.6 Connection to the Office-world (Panels, Comfort Panels, RT Advanced)

4.6.1 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.

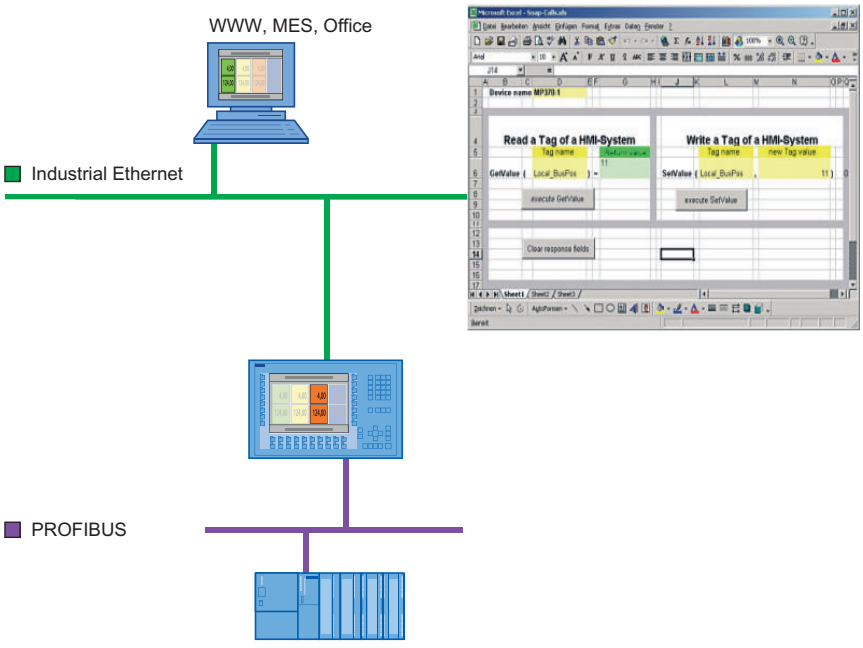


Figure 4-2 Communication with other applications

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. For more information, refer to "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\", z. B. 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 for 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.

4.6.2 Create VBA-Marko 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_1tag 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 188)

WinCC Server / WinCC Client (RT Professional) 5

5.1 Guide to client server systems (RT Professional)

Content

You can efficiently distribute operation and monitoring of your plant to multiple operator stations and servers. A WinCC Server with process connection records process data and logs alarms and process values. Moreover, a WinCC Server performs the following tasks in a WinCC network:

- Providing clients with the configuration data
- Providing clients with data from the process

Moreover, you can precisely map technologically or topologically complex systems.

This section shows you:

- The system configurations you can implement with WinCC.
- How to configure the server and clients in the client/server system.
- How the client/server system reacts in runtime.

5.2 Clients and servers (RT Professional)

Introduction

All process data of a WinCC project, e.g. alarms or trend values, is saved to different Runtime databases. Instead of being stored on each HMI device, these Runtime databases are located on the central WinCC server. The operator stations, i.e. the WinCC clients, access the WinCC server accordingly.

WinCC clients and WinCC servers are independent systems. You can activate WinCC clients at any time. It is also possible to activate and deactivate projects when you work on a WinCC client.

Multiple-station system

You can user the server option to expand a WinCC single-station system to a high-performance multiple-station system with up to 32 coordinated operator control and monitoring stations.

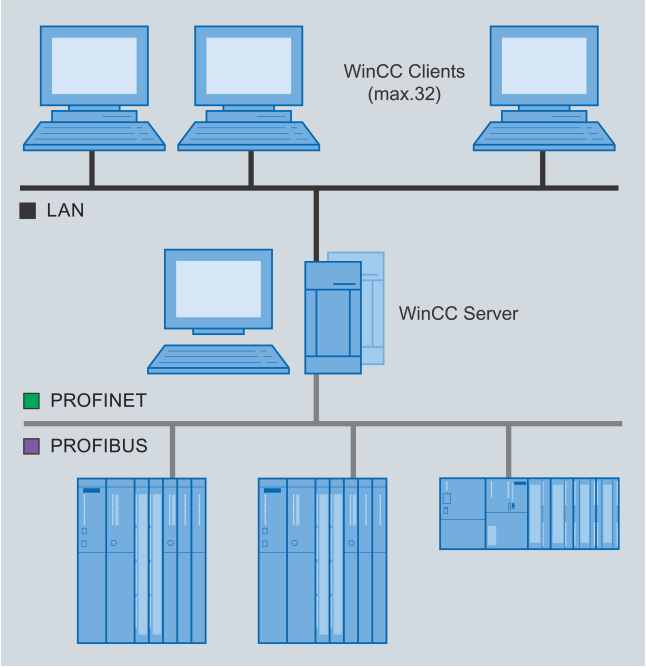


Figure 5-1 Multiple-station system with up to 32 clients on one WinCC server

WinCC clients display the data of precisely one WinCC server with process connection. WinCC clients operating on a multiple-station system do not have an own project ("Client without project"). For this reason, it is not necessary to configure the clients. The WinCC server provides the process and log data, alarms, screens, and reports to its online WinCC clients.

Licenses required

- A WinCC license on the WinCC server.
- On the WinCC server, the " WinCC Server for RT Professional" license.
- On the WinCC clients, the "WinCC Client for RT Professional" license.

5.3 Plant configurations (RT Professional)

5.3.1 Single-user system (RT Professional)

Definition

An operator station has a view of its own project.

Application

Single-station systems are usually operated at the production level. They are used for operator control and monitoring of relatively small applications, but also for independent subprocesses or plant components within larger plants. A single-station system operates autonomously with its own screens and logs: all data are stored locally on one PC.

Structure

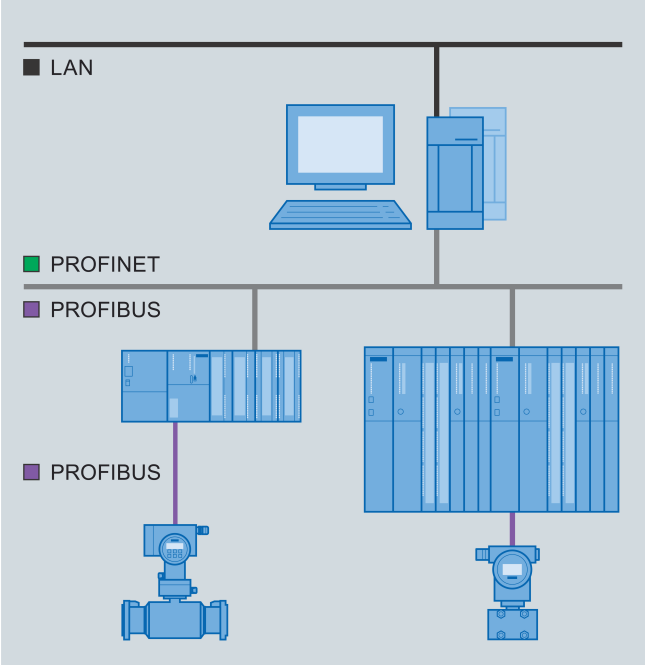


Figure 5-2 Single-station system

Single-station systems are based on the client-server principle:

- Runtime station: The WinCC data is stored in the integrated Microsoft SQL Server database on the operator station.
- The various Runtime components, including third-party components can access the Microsoft SQL Server database.
- Configuration PC: You can choose to use the actual operator station, or a different PC to configure your project.

5.3.2 Multi-user system (RT Professional)

Definition

Up to 32 coordinated operator stations (WinCC clients) have a view of the same server project.

All WinCC data is stored in the integrated Microsoft SQL Server database on the WinCC server. Since the WinCC clients do not have their own WinCC project, they access the WinCC project on the WinCC server.

Application

The same plant processes can be monitored on several operator stations (clients). Any user intervention on an operator station, e.g. value changes, is immediately visible on all other operator stations. A multiple-station system is typically configured for small and mid-sized plants in which distribution of data to several servers is not required.

Distribution of clients

- With different tasks: You operate and monitor different views of the same process, for example, process screens on one operating station and alarms on another operating station.
- With similar tasks: You monitor and control the same view of the process from several locations, for example, along a production line.

You use access rights to specify exactly which functions or plant sections are available to a given user on which operator stations.

Structure

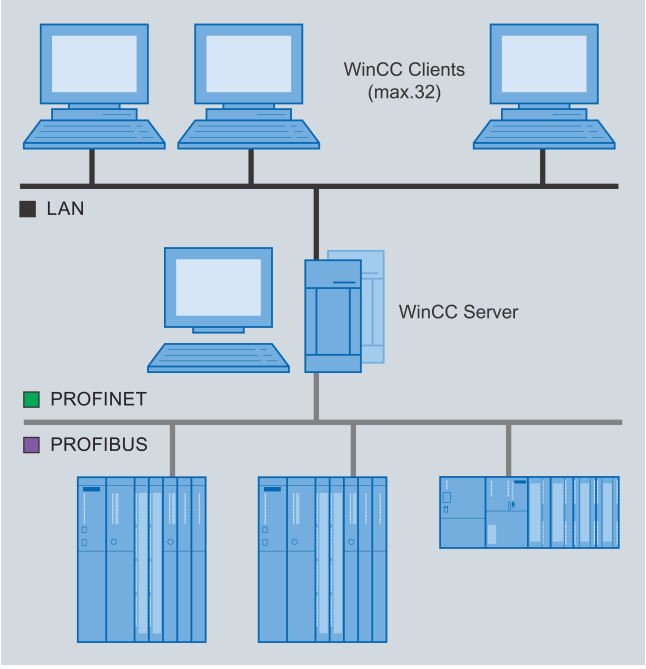


Figure 5-3 Multiple-station system

The client-server technology makes it possible to easily separate WinCC clients from the WinCC server: Configure your project centrally in the TIA Portal on the engineering station

and download it to the WinCC server with process connection. The WinCC clients do not need a project planning, but merely a configuration:

- Networking with the WinCC server using drag-and-drop.
- Separately for each WinCC client:
  - Start screen
    Select a screen configured on the WinCC server as start screen.
  - Runtime language
  - Toolbar
  - Navigation buttons
  - Deactivation of shortcuts
  - Window properties

The WinCC server automatically assumes the task of supplying the WinCC clients:

- Runtime environment
- Screens, process values, alarms, log data, and reports
- Interface with the automation system
- Communication and coordination of clients
- Logging

Process specifications or alarm acknowledgments on one operator station are consistently available to other operator stations.

5.4 Configuring a multiple-station system (RT Professional)

5.4.1 Requirement (RT Professional)

Requirement

- All HMI devices on a client-server system are interconnected via network (LAN) or ISDN and standard TCP/IP protocol.
  You can also log on as client or server with PCs in adjacent subnets that are interconnected via router.

Server PC

- The server PC is connected to the automation systems via process bus.
- WinCC Runtime Professional is installed.

- Operating system on the server PC:
  - Microsoft Windows XP SP3, maximum 3 WinCC clients.
    WinCC ServiceMode is not approved for this configuration.
  - Microsoft Windows 7, maximum 3 WinCC clients
  - Microsoft Windows 2003 SP2 Server, maximum 32 WinCC clients
  - Microsoft Windows 2008 Server, maximum 32 WinCC clients
- Licenses:
  - "WinCC Server for RT Professional" for the WinCC Server
  - "WinCC RT Professional" for the project

Client PC

- A "WinCC Client for RT Professional" license on all WinCC clients.
-
- A WinCC license on the WinCC server.
- The "WinCC Client for RT Professional" license on the WinCC clients.
-

5.4.2 Configuration guidelines (RT Professional)

Introduction

This chapter shows the basic procedure for setting up a multiple-station system. The multiple-station system consists of a WinCC server and two WinCC clients.

Procedure

1. Configuring servers.
2. Configuring clients: Start screen, menus & toolbars, language & font
3. To enable users access to the WinCC server project from a WinCC client: Configure operator authorizations
4. Download the project to the server.

5.4.3 Configuring the server (RT Professional)

Introduction

Set up a project as the WinCC server.

Procedure

1. Create a project.
2. Add "WinCC RT Professional" to the HMI device.
3. Enter "WinCC Server" as the device name.
4. Configure the required screens, logs, tags, alarms, custom toolbars, project languages, etc. for the "WinCC Server".
5. In the Runtime settings under "General", select the start screen, a configuration and design for "Menus & Toolbars".
6. Under "Services", activate the server Runtime services you need for the specific configuration. Example: If the server screen displays recipes, select "Recipes".
7. Go to "Screens" to select the corresponding properties.
8. Under "Language & Font" select the Runtime languages required on the WinCC server.

Result

A project is set up and displayed on the WinCC clients. The project only becomes the server project when you link the "WinCC Server" with the WinCC clients.

5.4.4 Configuring the operator authorizations (RT Professional)

Authorizations in WinCC

To enable access of a WinCC client to a server project, configure the appropriate operator authorizations for this WinCC client in the server project. The WinCC server provides the following operator authorizations:

- "Operate" The WinCC client is granted access to the WinCC server.
- "Enable remote control": A remote WinCC client can activate a server project, i.e. include it in runtime.

The computers on the network are not notified of a change to operator authorizations. This change is activated the next time a WinCC client wants to log on to a WinCC server.

The operator authorization "Enable remote control" is requested from the WinCC client as soon as the WinCC client requests activation of a project on a WinCC sever. If the corresponding operator authorization is not available on the WinCC server, the WinCC client is denied access to the project. Once the server project was closed on the WinCC client, a new logon is necessary at the next request to open the project.

Note

The operator authorizations configured are user-related, not computer-related. An operating authorization assigned is therefore valid for all operating stations with the same login.

Permissions in the operating system

To enable access of the WinCC clients to the server project, the corresponding project folder must be released for network access on the WinCC server. Set up authorizations in the operating system with all rights (write, read, modify) for the users who should have access to the projects.

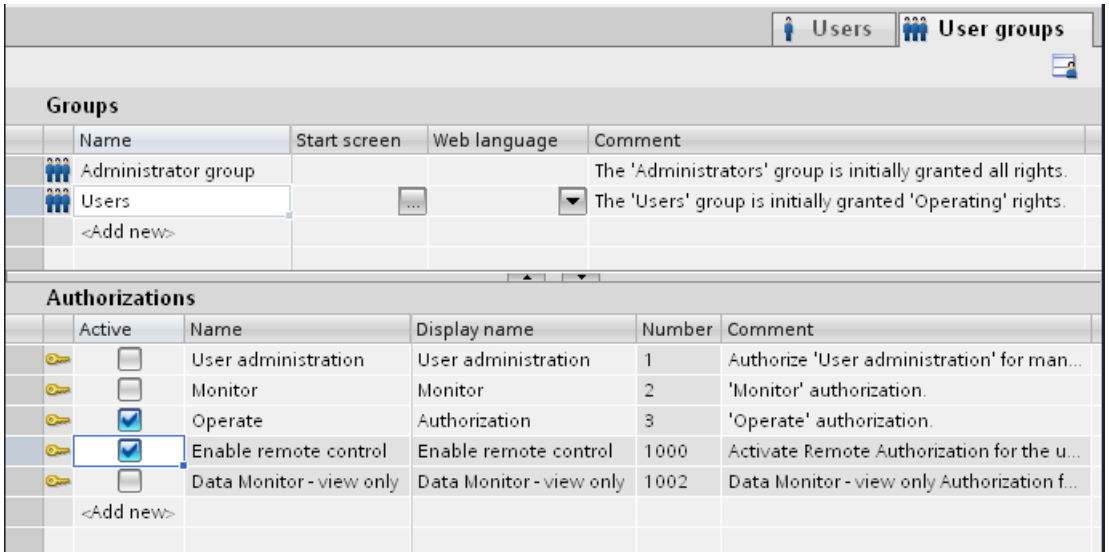
Note

Different Windows permissions can be assigned for the shared project directories to enhance network security.

Detailed information on the assignment of permissions is provided in the Windows documentation.

Procedure

1. Open the WinCC user administration.
2. Select the user group of the user you want to edit.
3. To grant this user full access to the server project, activate the "Operate" and "Enable remote control" operator authorizations.



5.4.5 Configuring clients (RT Professional)

Introduction

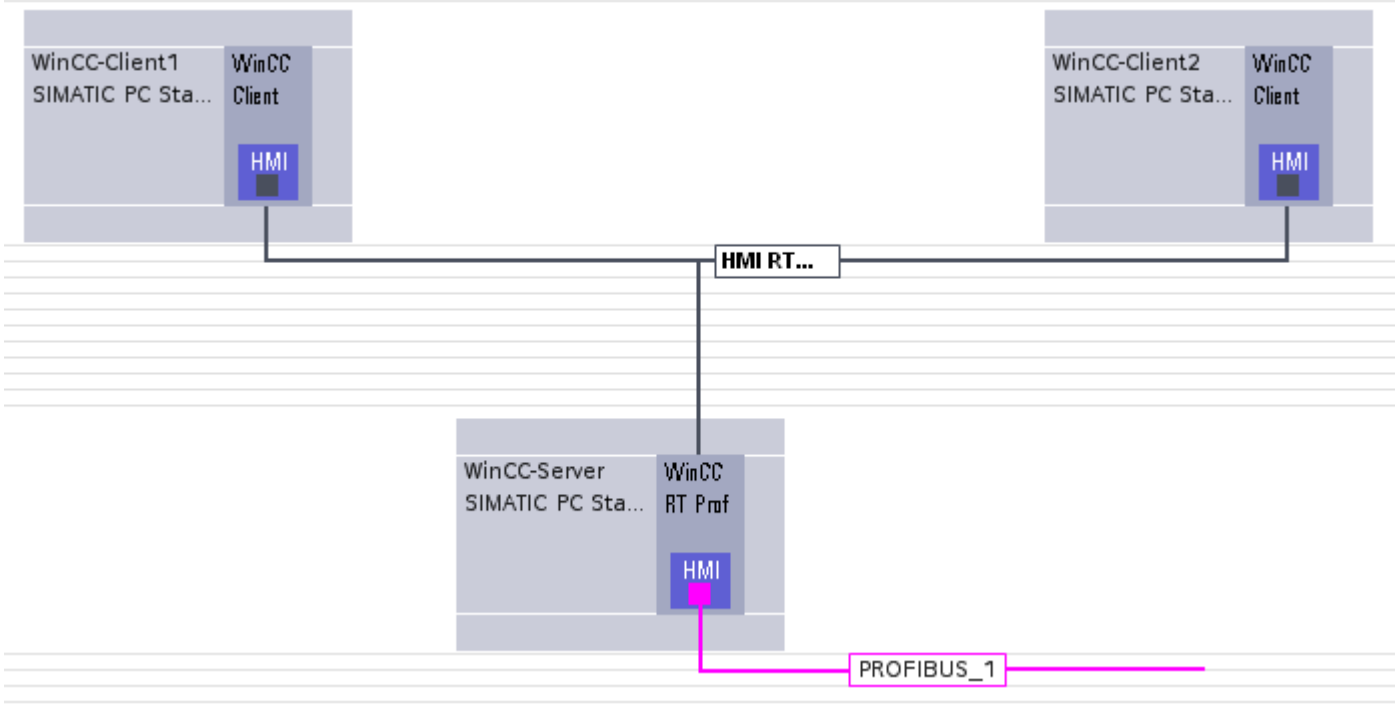
You create two WinCC clients and link them with the WinCC server.

Procedure

1. Add the following HMI devices to the project:
   - WinCC client, device name "WinCC Client1"
   - WinCC client, device name "WinCC Client2"
2. In the "Devices & Networks" editor, "Relations" tab, link the two WinCC clients with the WinCC server by means of drag-and-drop. A multiple-station system will be created.

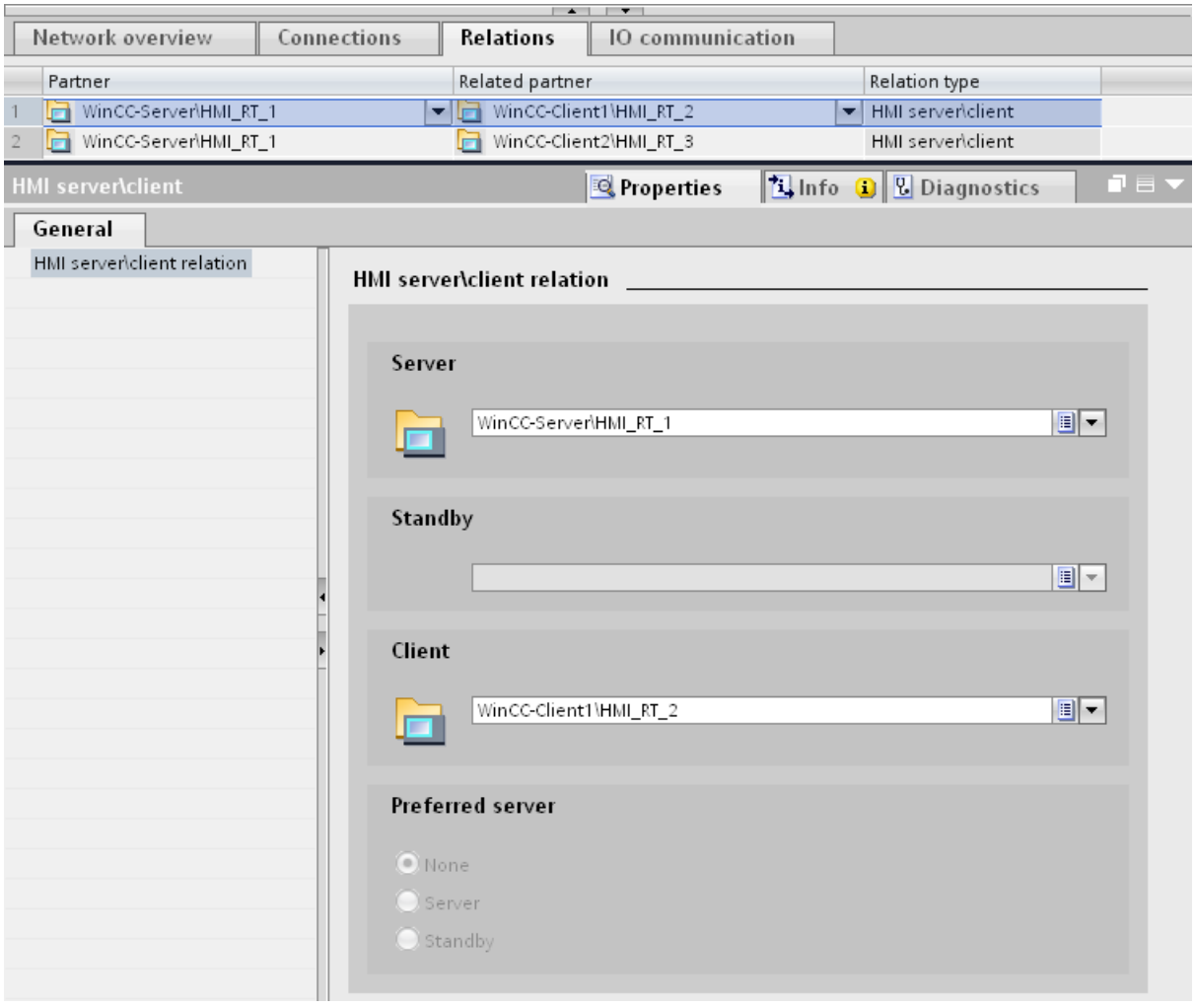
   Note

   In contrast to connections, the physical connection (network) and logic connection (client-server relation) are always created and deleted jointly. When you configure a relation, the devices will be linked automatically.



3. Select "WinCC-Client1".
4. In the inspector window, select Properties > Computer name" and enter the physical computer name of the HMI device.
   The computer name identifies the HMI device in the network.
5. In the Runtime settings, "General" tab, select a screen as the "Start screen" of the WinCC server. In the multiple-station system, the WinCC client then displays this server screen in runtime.
6. Select a "Menus & Toolbars" configuration that was made on the WinCC server.
7. At "Services", activate the client Runtime services you need for the specific configuration, e.g. the scheduler.
8. Select additional design features under "Screens".

9. Select a Runtime language for the WinCC server under "Language & Font". For example, you can configure a separate Runtime language for each WinCC client.
10. Repeat steps 3 to 9 for "WinCC Client2".



"Network data" editor

Using the arrow buttons below the network view, open the "Network data" editor. The "Network data" editor displays the relations you created. You can edit and delete these relations. If you first select a device and then select "Project overview" from the shortcut menu in the "Network data" editor, only the relations of the selected device are displayed.

Result

You have configured a multiple-station system with a WinCC server and two WinCC clients.

5.4.6 Downloading the project to the server (RT Professional)

Procedure

1. Compile the project using the "Compile" icon in the toolbar.
2. Once you successfully compiled your project, select "Project tree > WinCC Server" and then select "Download to device" from the shortcut menu of "WinCC RT Professional".

For the initial transfer, enter the computer's's target address "\\computer name\<shared folder>" in the next dialog and exit the dialog using the "Transfer" button.

A transfer to the WinCC clients is not necessary because the WinCC server provides all necessary data to the WinCC clients.

5.5 Characteristics in runtime (RT Professional)

5.5.1 Characteristics (overview) (RT Professional)

Editor characteristics in runtime

Logs

The Runtime database records and logs the process data on the WinCC server and simultaneously operates as log server. The WinCC clients receive their log data from the log server and display the data as table or graphics. All operations on the WinCC client are forwarded to the WinCC server. Processing results are returned to the WinCC client.

Screens

Data with other subsystems, for example, the log system are always exchanged locally. A screen can be opened and processed by several operating stations in runtime.

Alarms

The "Alarms" Runtime database, which generates alarms on the WinCC server and logs these alarms, functions as an alarm server. The WinCC clients receive their alarms from the alarm server and display them together with log data in the alarm view or alarm window.

When an operating acknowledges an alarm, the acknowledgement is transferred to the alarm server. The alarm server enters the change of status in the log and distributes the notification to all participating WinCC clients. The same process applies to the locking of alarms.

If an alarm server is temporarily unavailable in Runtime, an alarm window will open with a corresponding warning. When the alarm server becomes available again, alarms will be displayed in the alarm window once again.

Reports

The report system includes only print jobs which show log or process data based on Runtime.

The report system is started automatically on all clients during startup. The WinCC server functions as a report server. During startup, the WinCC clients log on to the report server and

obtain the latest information on available print jobs and their status. When a print job is started on a client (always local), it receives the corresponding data from the report server. The report server, on the other hand, receives the status of the print job from the WinCC client. The report server then forwards this information to the other WinCC clients.

Runtime scripts

Project functions and standard functions of the WinCC server are always loaded and executed locally on the WinCC client.

Runtime user administration

The operator authorizations are checked by the Runtime component of the user administration. The Runtime component is automatically started on every computer when WinCC starts. On changes to the login, the current operating rights list is loaded.

Text library (project texts)

The Runtime text library runs on the WinCC server as a text server. The texts are always read from the database on the WinCC server.

5.5.2 Reaction to system errors (RT Professional)

The WinCC clients are not provided any data if no WinCC server is available. All graphic objects that can be operated are grayed out and a connection error is displayed in the controls.

Scripts can be used to configure the display of connection errors on the WinCC client.

Once the WinCC server was recovered, the WinCC client will be reconnected.

5.5.3 Delta compile in runtime (RT Professional)

You create, change and test large, distributed projects with numerous operating stations mostly on a configuration computer. The finished and tested project is then transferred to the respective HMI device. The project is compiled or delta-compiled depending on whether or not the HMI device is in Runtime.

Compiling

The entire project is compiled, downloaded to the HMI device and it will replace the existing project.

Delta-compile (download changes) in Runtime

Instead of downloading the entire project or changing it locally, with a delta download the changes will be applied directly and locally in Runtime.

At any given time during, only the changed or added Runtime objects, e.g. tags, screens, alarms, and logs will be downloaded online to the active runtime of an HMI device, without stopping Runtime on that station.

If you change a screen at runtime and download it to the HMI devices, for example, the modified screen is displayed automatically at the next screen selection in Runtime.

The offline project on the configuration PC and the online project on the HMI device must be consistent.

Field of application

Delta compile (download changes) offers the following options:

- During commissioning, operation, or maintenance, you edit the current project, download it to the HMI devices and immediately test it.
- You edit and download the project online at a central configuration station, instead of taking time-consuming local actions.
- You can first test the proposed changes on the configuration computer offline in a protected environment. Only then do you apply the changes in active operation. This approach helps you eliminate possible configuration errors before they result in downtime.
- Changes can be transferred consistently and take effect at the same time: Configuration changes are often interrelated and mutually dependent: they recalculate a value, create a corresponding tag and add it to a log and a trend display. These changes are completely closed and applied in full during operation. This approach prevents error states and instabilities in Runtime.

5.5.4 Characteristics of the server (RT Professional)

5.5.4.1 Starting servers (RT Professional)

General procedure

The WinCC servers of a client-server system start independently of the WinCC clients. As soon as it has completed its startup, the WinCC makes its services available to the WinCC clients and informs itself about all the nodes on the network.

Communication with the automation system will be started.

If a WinCC server fails in runtime, the data on the WinCC client can no longer be updated. The WinCC clients will be informed of the absent WinCC server.

See also

Reaction to system errors (Page 268)

Activating and deactivating projects on the WinCC server (Page 271)

5.5.4.2 Server shutdown (RT Professional)

General procedure

When you shut down a WinCC server, it will no longer provide process data to the connected WinCC clients. The missing link is, for example, displayed in the alarm window or trend window of the active client projects. All fields with missing process values are displayed in gray in the process screen.

See also

WinCC RT Start (Page 271)

5.5.5 Characteristics of the client (RT Professional)

5.5.5.1 Starting the Client (RT Professional)

General procedure

A WinCC client always remains in runtime, for example, regardless of whether the WinCC server is briefly unavailable. When using WinCCStart to start a WinCC client, the server project is also activated if the WinCC server is not in runtime.

See also

Activating and deactivating a project from the WinCC client (Page 273)

5.5.5.2 Shutting down a client (RT Professional)

General procedure

Runtime is closed on the WinCC client, while runtime of the server project continues.

See also

Activating and deactivating a project from the WinCC client (Page 273)

5.6 WinCC RT Start (RT Professional)

5.6.1 Overview of WinCCStart (RT Professional)

Application area

Using WinCC RT Start, you enable and disable Runtime on the WinCC server and display information about the installed product and components.

Procedure

To open WinCC RT Start, follow these steps:

1. In the Windows Start menu, select "Start > All Programs > Siemens Automation > Runtime Systems > WinCC Runtime Professional V12 SP1 > WinCC RT Start".

Functions

- Activating and deactivating a project
- Autostart of WinCC Runtime
- Displaying installed products and components

5.6.2 Activating and deactivating projects on the WinCC server (RT Professional)

Application area

You activate and deactivate Server Runtime on the WinCC server using WinCC RT Start.

To enable access from a WinCC client to the server project, the server project must be located in a shared folder. The "WinCCProjects" folder is released by default during installation:

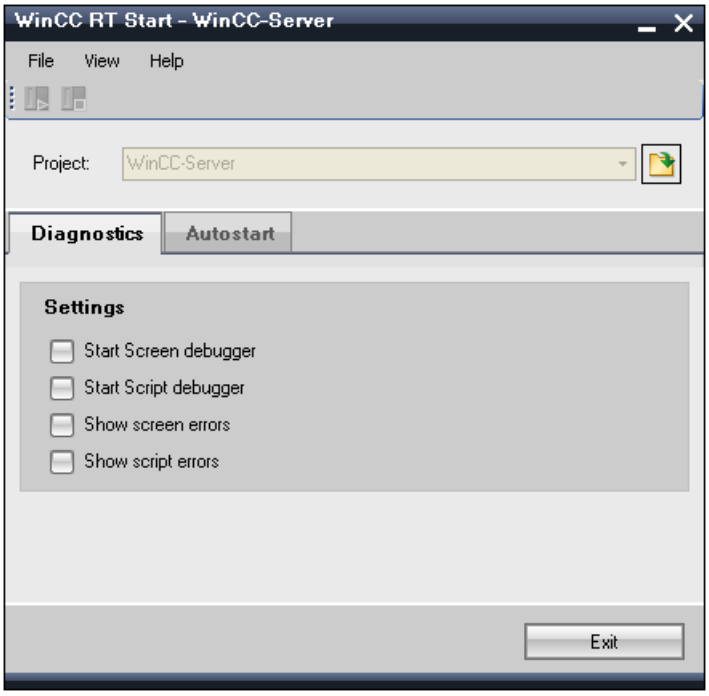
Operating system	Path
Windows 7 English	C:\Users\Public\Public Documents\Siemens\WinCCProjects
Windows XP SP3	C:\Documents and Settings\All Users\Shared Documents\Siemens\WinCC-Projects
Windows Server 2003	C:\Documents and Settings\All Users\Shared Documents\Siemens\WinCC-Projects
Windows Server 2008 English	C:\User\Public\Public Documents\Siemens\WinCCProjects
Windows Server 2008	C:\User\Public\Public Documents\Siemens\WinCCProjects

Note

You can also use your own folders and release these with corresponding authorizations.

Requirement

- The WinCC client and WinCC server are interconnected via network.
- The server project is stored in the "WinCCProjects" folder, or in a different shared folder.
- WinCCStart is opened via the Windows Start menu, "Start > All Programs > Siemens Automation > Runtime Systems > WinCC Runtime Professional V12 SP1 > WinCC RT Start".



Procedure for activating a project

To activate the server project, proceed as follows:

1. Select the "File > Open" menu command. You can also click the file selection button in the "Project" field.
2. Select the server project. The name consists of the project name in the engineering system, e.g. "Project1", and the server name, e.g. "HMI_1".
3. You can select different diagnostic sources in the "Diagnostics" tab.
4. Activate the project using the toolbar icon . You can also activate the project using the "File > Start RT" menu. Activation of runtime is indicated by a checkmark leading the "File > Start RT" menu command.

The WinCC server is started and provides all necessary data to the WinCC clients.

Procedure for deactivating a project

1. Deactivate the current project using the toolbar icon . The checkmark leading the "File > Start RT" menu command is cleared.

The modules for the execution of Runtime will be deactivated. The "WinCC Runtime" program window will be closed.

The WinCC clients are not provided any data if no WinCC server is available. All graphic objects that can be operated are grayed out and a connection error is displayed in the controls. Once the WinCC server was recovered, the WinCC client will be reconnected.

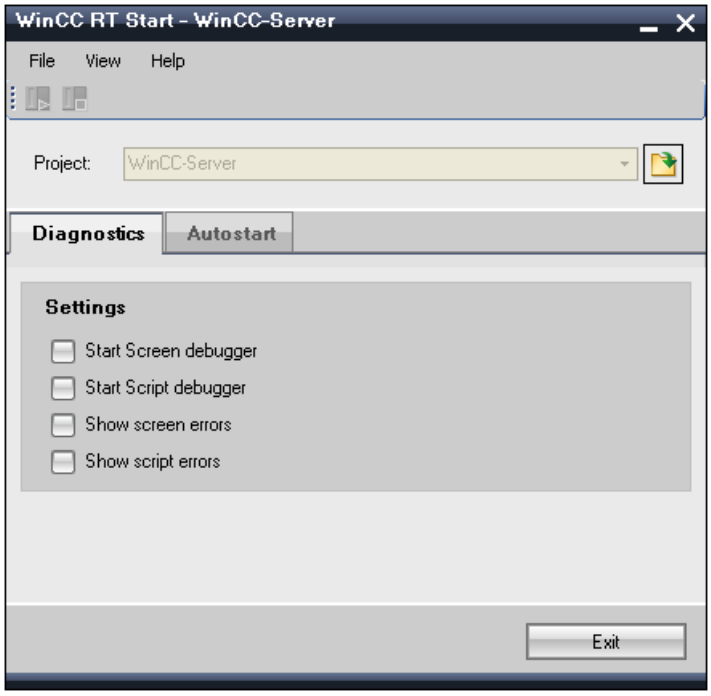
5.6.3 Activating and deactivating a project from the WinCC client (RT Professional)

Application area

Use WinCCStart to activate and deactivate runtime on the WinCC clients.

Requirement

- The WinCC client and WinCC server are interconnected via network.
- The is stored in a shared folder on the WinCC server. The "WinCCProjects" folder is released by default and displayed on the network.
- WinCCStart is opened via the Windows Start menu, "Start > All Programs > Siemens Automation > Runtime Systems > WinCC Runtime Professional V12 SP1 > WinCC RT Start".



Procedure for activating a project

To activate the server project, proceed as follows:

1. You can select different diagnostic sources in the "Diagnostics" tab.
2. Select the "File > Open" menu command. You can also click the file selection button in the "Project" field. The WinCC server "\\computer name\<shared folder>" is visible on the network.
3. Select the server project in the shared folder. The name consists of the project name in the engineering system, e.g. "Project1", and the server name, e.g. "HMI_1". A logon dialog opens when you connect to the WinCC server.
4. Enter the user name and password. Once you're successfully connected, the "Activate" toolbar icon is displayed if the WinCC server is not in runtime.
   If the WinCC-Server is in runtime, the runtime of the WinCC client is started automatically. In this case, skip the next step.
5. Activate the server project using the toolbar icon . You can also activate the server project using the "File > Start RT" menu. Activation of runtime is indicated by a checkmark leading the "File > Start RT" menu command.

Runtime of the WinCC server is started. Runtime of the WinCC client then starts automatically. The WinCC server provides all necessary data to the WinCC clients.

Procedure for deactivating a project

1. Deactivate the current runtime of the WinCC client using the toolbar icon . The checkmark leading the "File > Start RT" menu command is cleared.

The modules for the execution of Runtime will be deactivated. The "WinCC Runtime" program window will be closed.

Note

When working on the WinCC client, you can only terminate runtime on the WinCC client, but not the project on the WinCC server.

See also

Shutting down a client (Page 270)

5.6.4 Enabling time synchronization on the client (Professional) (RT Professional)

Introduction

You configure client-server systems with multiple clients and servers as needed in WinCC. You can efficiently operate and monitor large plants in this way.

You have several options to ensure time synchronization in this system.

The following shows how a client without its own project synchronizes the time via the server.

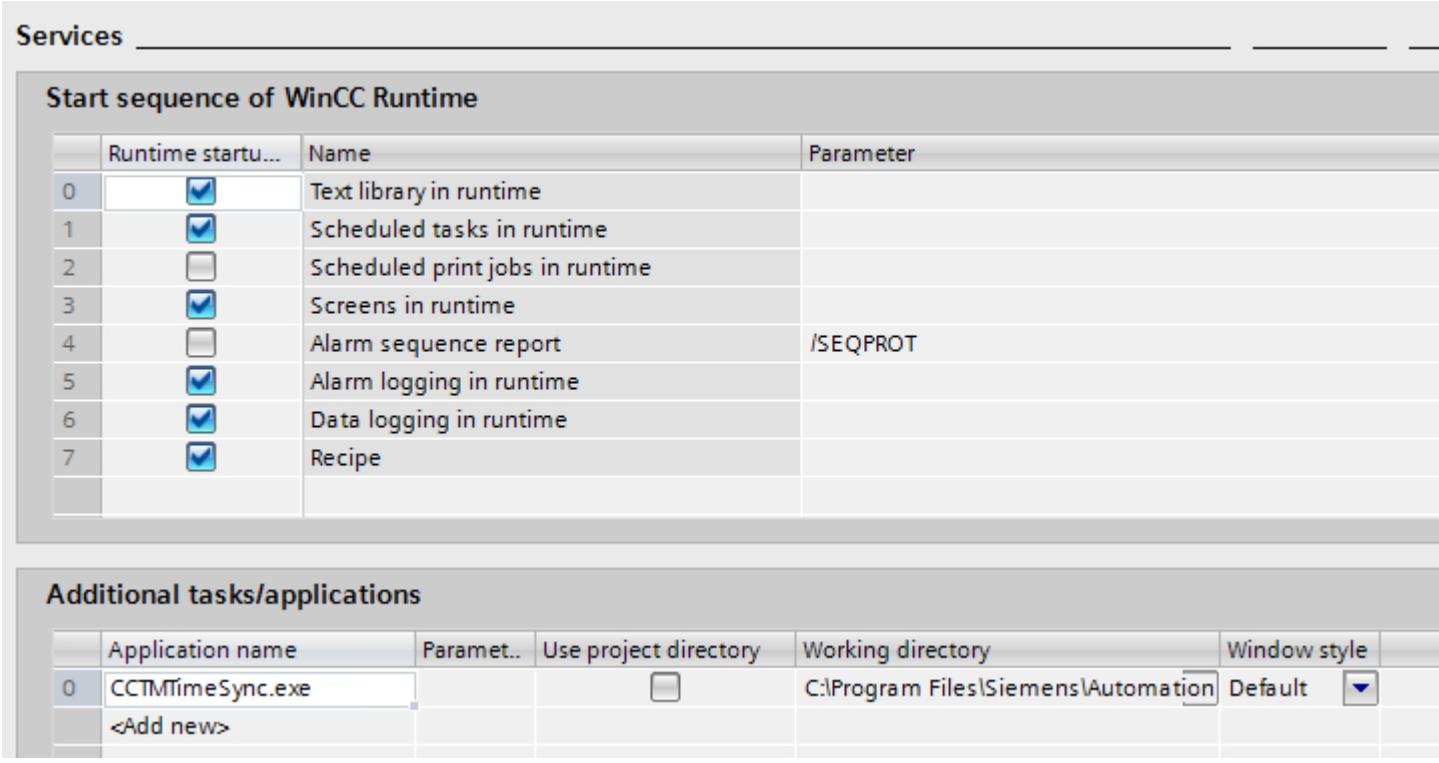
Requirement

- A multi-user system is set up.
- Time synchronization is set up on the server.
- No further time synchronization is enabled on the client.

Procedure

Set up the startup list as follows:

1. Open the "Runtime settings > Services" editor.



2. Under "Additional tasks/applications", enter the "CCTMTimeSync.exe" application and the associated drive path.
   The file is stored in your Siemens installation directory.
3. Disable "Use project directory".
4. Specify the startup size of the task or application window in the "Window style" column, for example, minimized, maximized or standard size.

Result

When you start Runtime, the application is loaded. The time of the client is automatically synchronized with the server.

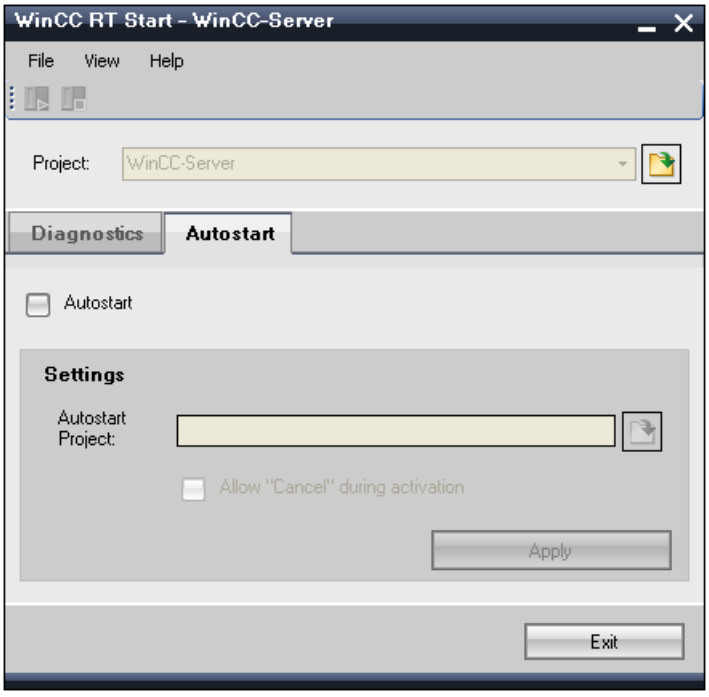
5.6.5 Additional settings: Autostart and language (RT Professional)

Introduction

The "Autostart" function automatically starts the server project at the time the server PC starts. Moreover, you can prevent users from canceling the start of runtime in order to gain unauthorized access to the operating system. To run this setup, you need a corresponding operator authorization in WinCC.

You can change the runtime language.

Procedure for Autostart



1. Go to the "Autostart" tab.
2. Activate "Autostart".
3. Select a server project in the "Settings" area.
   If you restart the computer with a project, the automatic start of runtime is initiated at the end of the load operation. You can prematurely cancel the automatic start and return to the operating system by pressing the "Cancel" button.
4. To prevent an operator from canceling the automatic start, deactivate "Allow cancelling of activation".
5. Click the "Apply" button. A Logon dialog opens.
6. Log on.

After you successfully logged on, server runtime is started automatically at the next restart of the WinCC server.

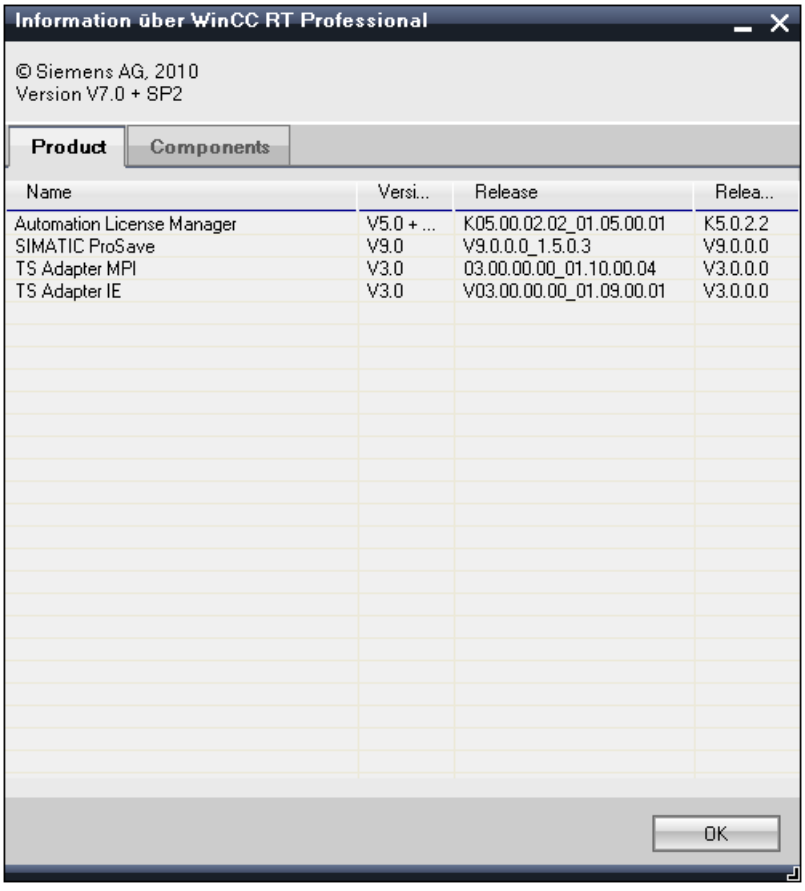
Language change procedure

1. Select the "View > Language" menu command. A dialog that displays all user interface languages available for WinCCStart opens.
2. Select a user interface language.

5.6.6 Displaying products and components (RT Professional)

Introduction

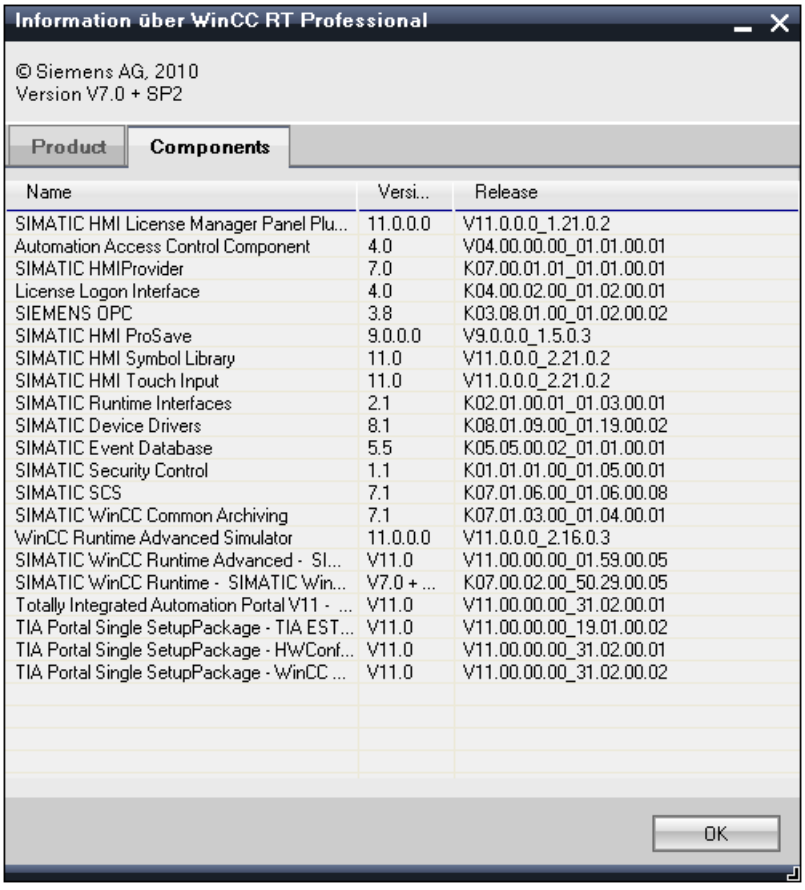
You can view your installed product software and options on the products tab:



The "Component" tab displays the following installed objects:

- Add-on software WinCC tools
- Interfaces
- Drivers

- Databases
- Logs



Procedure

1. Select "Help > About". The "About WinCC SCADA RT" dialog opens.
2. Select a tab.

5.7 SIMATIC Shell (RT Professional)

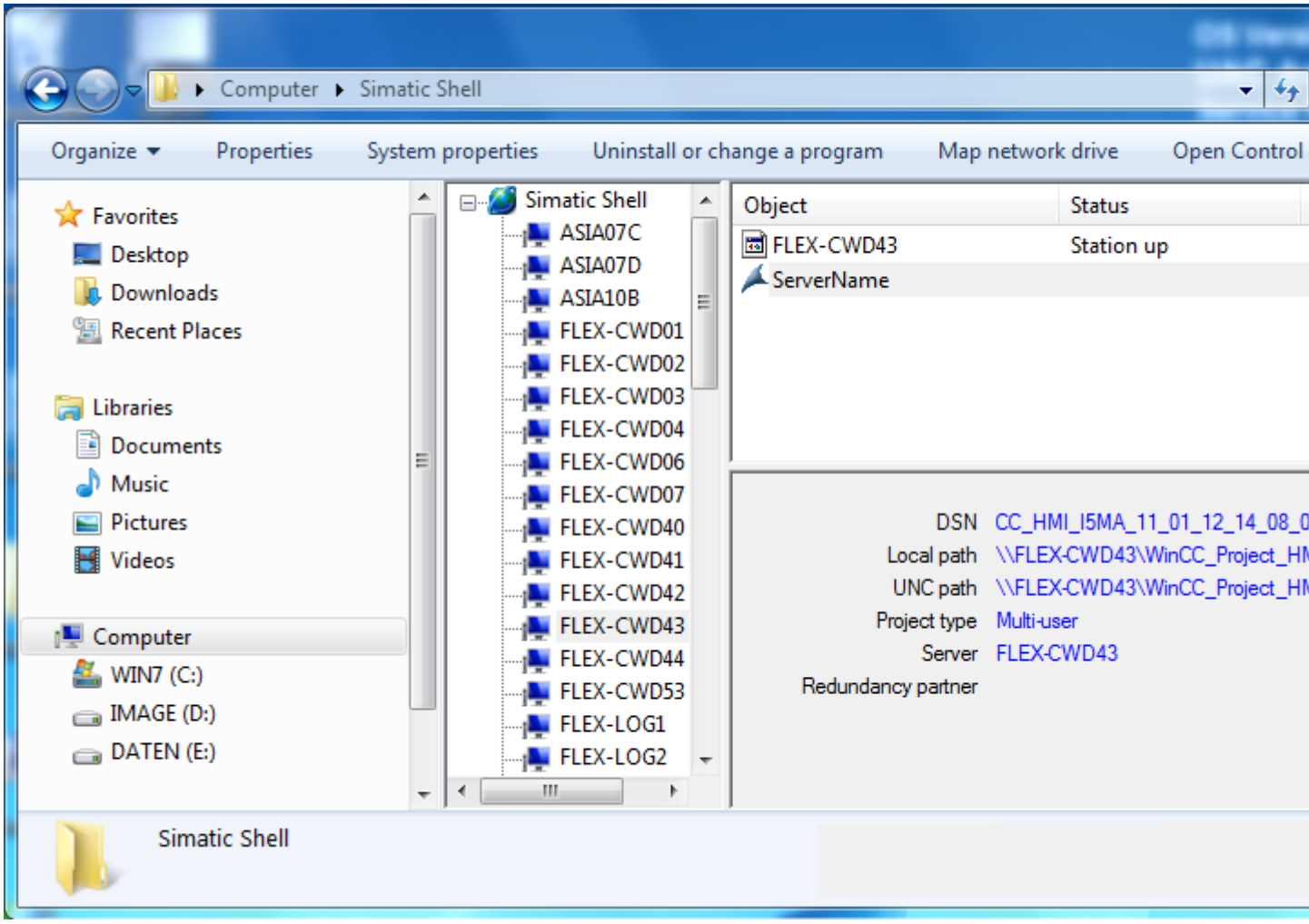
5.7.1 Remote Configuration (RT Professional)

General procedure

Clients provided with the corresponding operator authorizations can operate a server project from a remote station, e.g.:

- Enable a server project
- Disable a server project

For remote configuration, the "Simatic Shell" dialog is available which you access through Windows Explorer.



Function of Simatic Shell

In the "Simatic Shell" dialog you can view the enabled servers and projects of your client-server system available through the network. These include all projects which run under a demo license.

The window can be used to access an enabled server project from a client:

- to enable a project remotely
- to disable a project remotely

Note

Different names with WinCC Start and SIMATIC Shell

When WinCC Start opens, the name of a client-server project is fully displayed with the name of the server PC as the ending, for example, "ClientServerProjectBuild11_1_A-Server_1".

SIMATIC Shell does not show PC names under "Object"; it shows the name of the server PC on which the client-server project is running, for example, "A-Server_1". This means different client-server projects can be referred to with the same object name.

5.7.2 Accessing a computer outside a subnet (RT Professional)

General procedure

Computers located behind a router in a network may be introduced to the system by using the "Simatic Shell" dialog.

Note

You use the "Simatic Shell" dialog for central maintenance and diagnostics of all computers integrated in your client/server system.

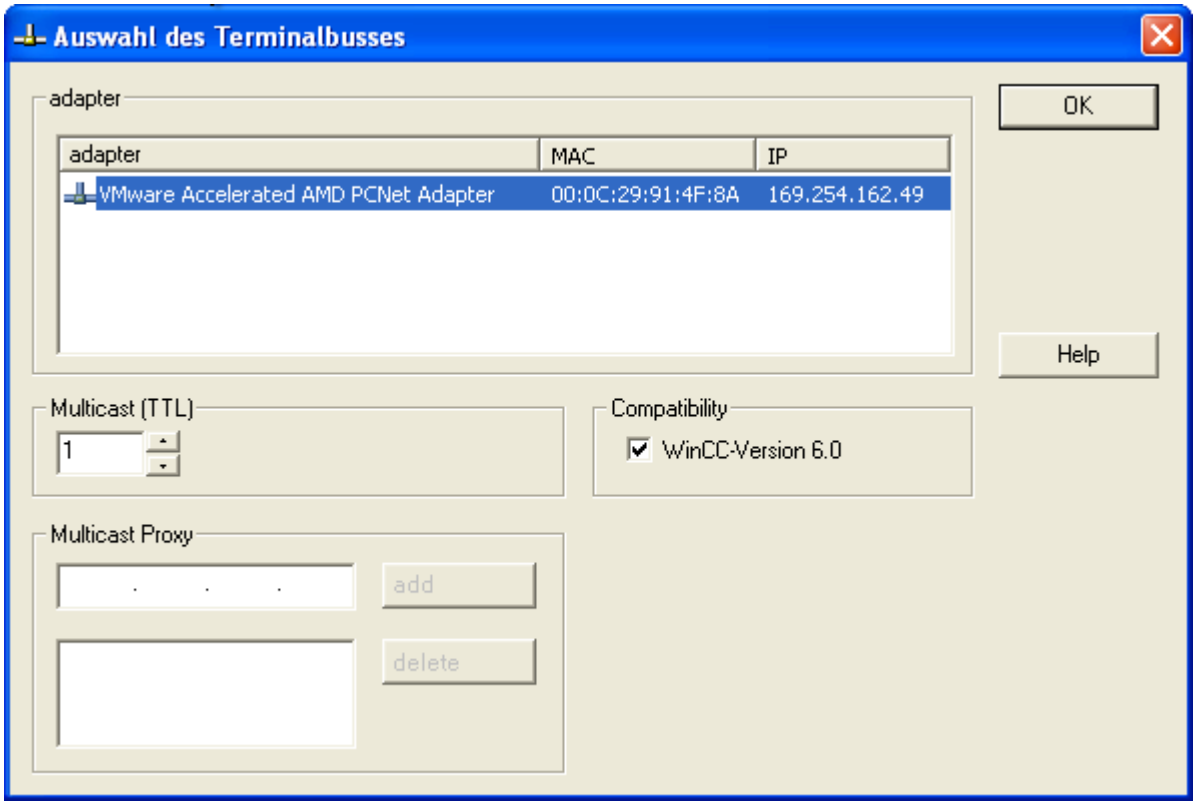
Using the settings in "Simatic Shell", you introduce a computer within your subnet behind your router as an "Agent" who distributes the information from other computers to the computers within the subnet.

After having logged this computer on, all participating computers in the system can communicate even beyond the router limits. Each computer added to an existing group is informed of the current status of all computers, including those beyond the router limits. When the status of a computer changes, a alarm is issued to all participants, e.g.:

- If a computer has enabled a project
- If a computer is shut down.
- If a computer is started up and thus enters the group.

Procedure

1. Click on the folder "My Computer > Simatic Shell" in the Windows Explorer of the client computer. The "Simatic Shell" dialog opens.
2. Select the "Settings" menu command in the shortcut menu of an entry in the navigation window. If no entry is displayed, open the shortcut menu in an empty window. The "Selection of the terminal bus" dialog opens.



3. Check the setting in the field "Multicast Lifetime (TTL)". The value gives the maximum number of route jumps between various subnets (IP Parameters TTL).
4. Under "Multicast Proxy", enter the address of the computer that is the "Agent" for the subnet. This can be any computer of the subnet (client or server).
5. Add the computer to the list of network partners with the "Add" button.
6. Confirm your entry with "OK".

5.7.3 Activating a project (RT Professional)

General procedure

A client/server system makes it possible to enable and disable projects remotely.

If you enable a server project from a client by using the "Simatic Shell" dialog, only the server project is enabled.

Requirements

In order to activate a server project on a client, the following conditions must be fulfilled:

- The user logged onto the client has the operator authorization to "Activate remote" in the WinCC project on the server.
- The project has been enabled for network access

Procedure

1. In Windows Explorer of the client, select the "Simatic Shell" entry. The "My Computer > Simatic Shell" window will be displayed.
   All the servers and projects available in the network with their current status will be displayed.
2. Select the project to be enabled.
3. Select the "Activate remote" command from the shortcut menu.
   A Login dialog appears.
4. Enter the user name and password for the current computer. The project is enabled on the server.

5.7.4 Deactivating a project (RT Professional)

General procedure

A client/server system makes it possible to enable and disable projects remotely.

If you disable a server project from a client by using the "Simatic Shell" dialog, only the server project is disabled.

Requirements

In order to deactivate a server project on a client remotely, the following conditions must be fulfilled:

- The user logged onto the client has the operator authorization to "Activate remote" in the WinCC project on the server.
- The project has been enabled for network access

Procedure

1. In Windows Explorer of the client, select the "My Computer > Simatic Shell". The "Simatic Shell" window is displayed.
   All computers and projects available in the network will be displayed with their current status.
2. Select the project to be enabled.

3. Select the "Deactivate remote" command from the shortcut menu. A Login dialog appears.
4. Enter the user name and password for the current computer. The project is disabled on the server.

WinCC WebNavigator (RT Professional) 6

6.1 Unsupported functions (RT Professional)

The following list is only an excerpt of the unsupported functions. The lists contains the functions which are explicitly declared as unsupported.

Functions

GetHWDiag	OnDeactivateExecute	ReportJob
GetHWDiagLevel	OnErrorExecute	RPTJobPreview
GetKopFupAwl	OnTime	RPTJobPrint
GetKopFupAwlLevel	OpenPrevPicture	RptShowError

VBScript functions

- HMIRuntime.Stop: Terminates Internet Explorer and WinCCViewerRT, however not WinCC Runtime.
- AlarmLogs object
- DataLogs object
- Logging object
- Project object

Functions that are unnecessary:

- DeactivateRTProject: Terminates Internet Explorer and WinCCViewerRT, however not WinCC Runtime.
- ExitWinCC
- FillDiagnoseInTags
- InquireLanguage
- TraceText
- TraceTime

Other functions

These functions are contained in the range of functions in order to guarantee error-free compilation on the WebNavigator client. The functions are not supported by the WebNavigator client.

AXC_OnBtnHornAckn	GetCursorMode	GmsgFunction
AXC_OnBtnPrint	SetCursorMode	MSRTMsgWinCommand
AXC_OnBtnProtocol		TlgTableWindowPressHelpButton

6.2 The basics (RT Professional)

6.2.1 Function Overview (RT Professional)

Introduction

You can use the WinCC WebNavigator option of WinCC Runtime Professional to monitor and control your WinCC project via the Intranet/Internet. This enables you to quickly and easily implement a new type of distribution of controlling and monitoring functions of your automation system. WebNavigator supports current Internet security methods.

The "WebNavigator" add-on package consists of the following components:

- WinCC WebNavigator Server
- WinCC Web Configurator
- WinCC WebNavigator Client
- WinCCViewerRT

WinCC WebNavigator Server

The WebNavigator server is installed on a PC along with WinCC Runtime Professional. The required WinCC screens and functions that are displayed on the WinCC WebNavigator Client are stored on the server PC.

WinCC Web Configurator

The WebNavigator Server needs the Microsoft Internet Information Service (IIS) for communication with the WebNavigator Clients. The IIS is set up and managed with the WinCC Web Configurator. Accesses of the WebNavigator Client are governed via user administration. You can set a different start screen and language for every user. By assigning user authorizations, a scalable access to different project areas and functions is implemented for the various users.

WinCC WebNavigator Client

The WebNavigator Client is started via the MS Internet Explorer with activated ActiveX controls. You control and monitor a running WinCC project without the entire WinCC basic system on the PC.

WinCCViewerRT

Instead of the Internet Explorer, you use the Web viewer "WinCCViewerRT" to visualize the WinCC project.

WebNavigator diagnostics client

You can use the diagnostics client, for example, for the maintenance of several WebNavigator server.

Licensing

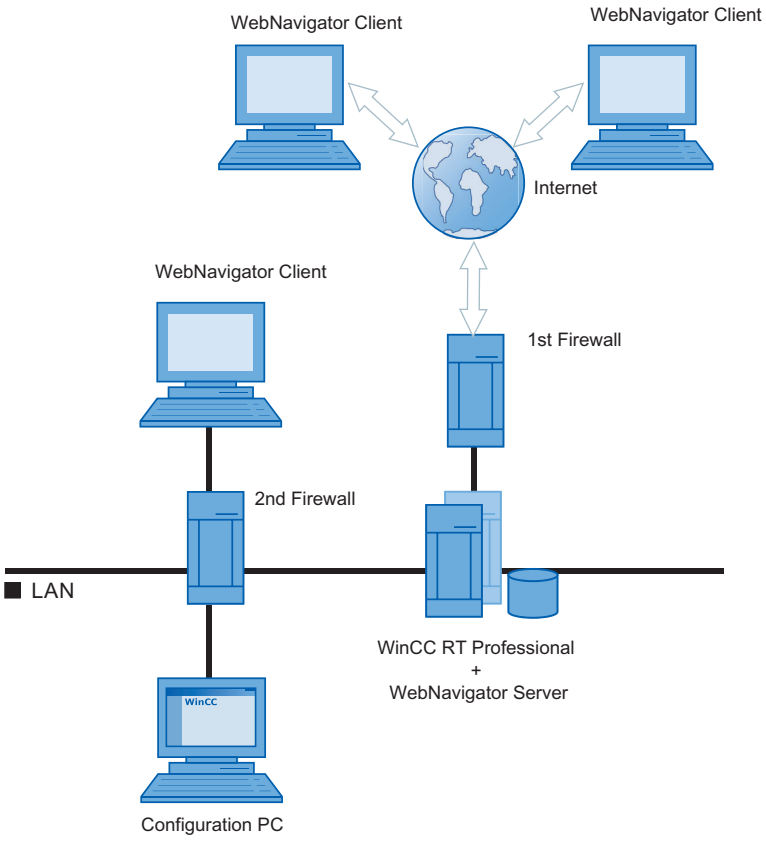
Licensing is managed centrally on the WebNavigator Server in accordance with the number of concurrent accesses of 3, 10, 25, 50, 100 or 150 WebNavigator Clients, for example. A license is not required on the WebNavigator Clients.

6.2.2 Web Navigator Server on the WinCC server (RT Professional)

Structure

WinCC RT Professional and the server components of the WebNavigator are installed on a PC. The WebNavigator client can control and/or monitor the current server project both via the Internet and the Intranet.

To protect against attacks from the Internet, two firewalls are employed. The first firewall protects the WebNavigator Server from Internet attacks. The second firewall provides additional security for the Intranet.



6.2.3 WebNavigator diagnostics client (RT Professional)

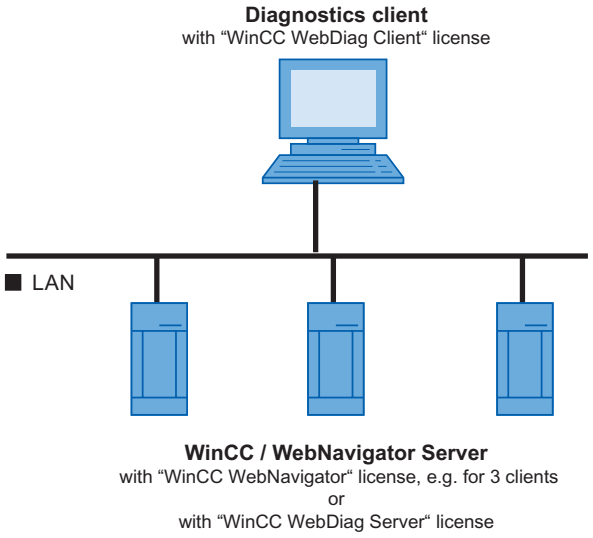
Introduction

The WebNavigator diagnostics client enables cost-effective access to several WebNavigator Servers.

Several diagnostics clients and standard clients can be in operation at the same time. This procedure does not demand an additional license for a WebNavigator Server because licensing is handled on the diagnostics client. The diagnostics client can always access the WebNavigator server, regardless of whether the maximum number of simultaneous accesses has been reached. The diagnostics client always has guaranteed access to the WebNavigator server.

Possible applications:

- Remote maintenance: With the Diagnostics Client, different WinCC systems are accessed for service and maintenance purposes.
- Central Control Room: The diagnostics client is used for simultaneous access to several servers.



6.2.4 WinCCViewerRT (RT Professional)

Overview

Don't use Internet Explorer to run the "WinCCViewerRT.exe" application. Run it on the WebNavigator client instead. The WinCCViewerRT is installed along with the WebNavigator client.

WinCCViewerRT uses its own communication to access the WebNavigator server. This prevents Internet users from accessing the system and protects the system against viruses and Trojan horses.

Only the screens which are configured for Web access and published on the WebNavigator server are displayed. Users can operate and monitor the project, depending on their authorizations.

If the user is assigned the authorization no. 1002 "Web access - view only", he/she can only view the project. The WebNavigator client is therefore a so-called "View Only Client".

The cursor is a "View only cursor" and indicates that process-related operations are not possible. Certain operations are still possible, such as opening the properties dialog of an online trend control.

You can also use WinCCViewerRT as terminal server application. For more information, refer to "Setting up terminal services for WebNavigator servers".

6.2.5 Terminal services and Web Navigator (RT Professional)

Introduction

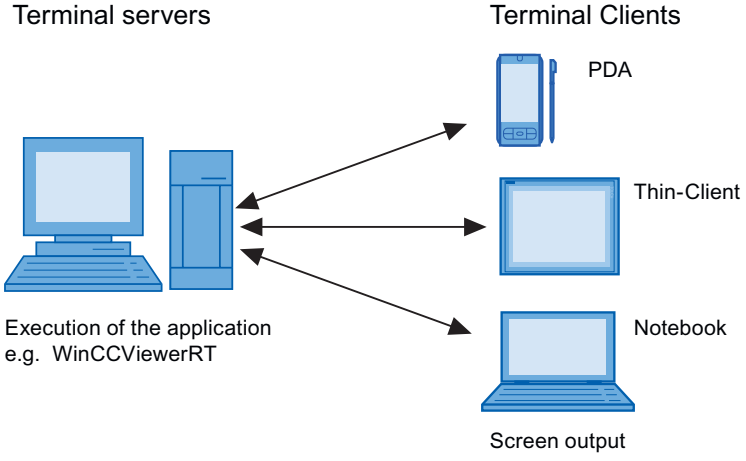
Terminal services in the Windows Server operating systems enable access to the desktop of a Windows server.

The terminal client only handles screen output, while the application runs on the terminal server, for example WinCCViewerRT.

The terminal services transmit only the user interface of the application to the clients. Each client's keyboard inputs and mouse operations are returned back to the server.

This behavior has the following advantages:

- Use of rugged hardware for the clients, for example without fans and hard drives, for application in dusty environments.
- Use of mobile clients with limited power consumption, for example handhelds, palmtops, PDA.
- All applications are located on the server in a secure environment.
- Easy, central administration and system maintenance.
- Support of different operating systems, for example Windows CE, Windows 95.



The WebNavigator client created based on a "THIN²" architecture, i.e. the application running in multiple instances on the terminal server, e.g. WinCCViewerRT, is itself already "thin" with regard to hardware requirements.

For redundant system configurations with terminal services, please consult the corresponding Microsoft documentation.

Note

The terminal client supports only 256 colors.

To reduce the strain on the terminal service, avoid large bitmaps whose size can change ("live video").

6.3 Installing WebNavigator (RT Professional)

6.3.1 Software and hardware requirements (RT Professional)

Introduction

This section describes the hardware and operating system requirements for WinCC WebNavigator.

WebNavigator Server on a WinCC single-user system

Table 6-1 Hardware

	Minimum	Recommended
CPU	Intel Pentium 4; 2.5 GHz	Intel Pentium 4; 3 GHz Dual Core
Working memory	1 GB	2 GB

Table 6-2 Software

Operating system:	Windows 7 Professional, Enterprise, Ultimate, Embedded Standard SP1 (max. 3 clients) Windows 8.1 Professional, Enterprise Windows Server 2008 R2 Standard Edition SP1 Windows Server 2012 R2 Standard Edition
Software:	Internet Explorer as of V8.0 WinCC V13 Runtime
Miscellaneous:	Access to the intranet/Internet or TCP/IP connection to the WebNavigator client

WebNavigator Server on the WinCC server

Table 6-3 Hardware

	Minimum	Recommended
CPU	Dual Core; 2 GHz	Multi Core; 2.4 GHz
Working memory	2 GB	4 GB

Table 6-4 Software

Operating system:	Windows Server 2008 R2 Standard Edition SP1 Windows Server 2012 R2 Standard Edition
Software:	Internet Explorer as of V8.0 WinCC Professional V13
Miscellaneous:	Access to the Intranet / Internet If you publish in the **intranet**, you need a system for name resolution, which can convert computer names into IP addresses. This allows users to use alias name instead of IP addresses when connecting to the server. If you publish on the **Internet**, you need a DNS registry for the IP address. This allows users to use alias name instead of IP addresses when connecting to the server.

WebNavigator Client

Table 6-5 Hardware

	Minimum	**Recommended**
CPU	Intel Pentium 4; 2.5 GHz	Intel Pentium 4; 3 GHz
Working memory	1 GB	2 GB

Table 6-6 Software

Operating system:	Windows 7 (Professional, Enterprise, Ultimate, Embedded Standard) SP1 Windows 8.1 (Professional, Enterprise) Windows Server 2008 R2 Standard Edition SP1 Windows Server 2012 R2 Standard Edition Other operating systems such as WinCE, Win95 via MS Terminal Services Embedded XP in connection with Panel PC 477
Software:	Internet Explorer as of V8.0
Miscellaneous:	Access to the intranet/Internet or TCP/IP connection to the WebNavigator Server

The use of the WebNavigator Client via WLAN is only authorized for the SIMATIC Mobile Panel PC 12".

Web diagnostics client

Table 6-7 Software

Operating system:	Windows 7 (Professional, Enterprise, Ultimate, Embedded Standard) SP1 Windows 8.1 (Professional, Enterprise) Windows Server 2008 R2 Standard Edition SP1 Windows Server 2012 R2 Standard Edition
Software:	Internet Explorer as of V8.0
Miscellaneous:	Access to the Intranet / Internet

6.3.2 Licensing (RT Professional)

WebNavigator Client

No license is required with server-end licensing on the WebNavigator Server on the PC with the WebNavigator Client.

WebNavigator Server

The WebNavigator server runs without a license in Demo mode for 30 days.
A license is required, however, if you want to use the WebNavigator server for a longer period. Licenses are available for 1 / 3 / 5 / 10 / 25 / 50 / 100 / 150 clients that can simultaneously access the WebNavigator server.

If the number of licensed clients is exceeded during a logon attempt of a Web Navigator client, a message appears. No further logon is allowed.

Overview of licenses on the server and client

Server	WebNavigator Client	Diagnostics client
WebNavigator server license + WinCC license	Web Navigator client, no local license required. Maximum number of clients corresponds to the existing license on the server.	Diagnostics client One license per diagnostics client
Web diagnostics server license + WinCC license	WebNavigator client in Demo mode Number unlimited Valid for 30 days	Diagnostics client One license per diagnostics client
No WebNavigator license or no WinCC license	WebNavigator client in Demo mode Number unlimited Valid for 30 days	Diagnostics client in Demo mode Number unlimited Valid for 30 days

Restarting the Web client after changing licenses

If you change the WebNavigator licenses on the Web Navigator server, for example, by transferring a Powerpack, you must restart the Web viewer or Internet Explorer, if it used, on all connected WebNavigator Clients. Otherwise, the WebNavigator Client goes to Demo mode. This also applies to automatic reconnection of the WebNavigator Client.

Web diagnostics client

A diagnostics client license is required on the client PC for the diagnostics client. The diagnostics client can simultaneously access up to 12 WebNavigator Servers.

When a license for WebNavigator Server or Web diagnostics server is installed on the server, the diagnostics client also has access even when the maximum number of clients is exceeded.

Web diagnostics server

This license allows the diagnostics Web client to access the WebNavigator Server when no WebNavigator Server license is installed on the Web Navigator server for the WebNavigator Client.

A total of 50 clients per server is allowed at the most for simultaneous access by diagnostics clients.

Note

Diagnostics client without corresponding license

If you install the diagnostics client without its license, a message appears approximately 1 hour after each start of the PC. Install the diagnostics client license or remove the diagnostics client software.

PC with WinCC Runtime Professional and diagnostics client

If you install a diagnostics client on a PC with WinCC Runtime Professional, you have to reinstall the diagnostics client after removing WinCC.

6.3.3 Requirements for the Use of Terminal Services (RT Professional)

WebNavigator Client is authorized for use with Windows Terminal Services. A maximum of 25 sessions per terminal server are permitted.

Terminal server

Table 6-8 Hardware

	Minimum	Recommended
CPU	Dual Core CPU; 2 GHz	Multi Core; 2.4 GHz
Working memory	2 GB	4 GB

Table 6-9 Software

Operating system	Windows Server 2008 R2 Standard Edition SP2 Windows Server 2012 R2 Standard Edition: It must be possible to open and execute applications that are run on the clients multiple times.
Miscellaneous:	If numerous users want to access the server, you need to use a high performance network adapter.

Note

The memory requirements and processor load increased with each terminal client. You therefore need to ensure that the terminal server has adequate memory and processor load reserves.

Terminal client

Minimum requirement:	Network adapter with TCP/IP Terminal client RDP 5.0 Display or screen Pointing device

Device recommended for use as a client: SIMATIC Mobile Panel PC 12".

Note

As is the case with Windows Server Client Access License CAL, there are two different terminal service CALs:

- The TS Device CAL permits one device user-independent Windows sessions on a Windows server.
- The TS User CAL permits one user device-independent Windows sessions on a Windows server.

A Windows Server Terminal Server "TS CAL" is required for every user or every device.

You can find additional information under "http://www.microsoft.com/licensing/about-licensing/client-access-license.aspx".

6.3.4 Installation of WebNavigator server (RT Professional)

6.3.4.1 Overview (RT Professional)

Requirements

- The software requirements with regard to the Windows operating system apply.
  The following operating systems have been authorized:
  Windows 7 (Professional, Enterprise, Ultimate) SP1
  Windows 8 (Professional, Enterprise)
  Windows Server 2008 R2 Standard Edition SP2
  Windows Server 2012 R2 Standard Edition
- Local administrator rights

Installation sequence for the WebNavigator Server

When you install a WebNavigator Server on a PC, adhere to the following installation sequence:

1. Install the Internet Information Service (IIS).
2. Install the WebNavigator Server.
   To install the WebNavigator Server, you also need to install WinCC Runtime Professional. Microsoft SQL Server is automatically installed.

6.3.4.2 Installing Internet Information Services (IIS) (RT Professional)

Introduction

Before installing the WebNavigator Server, you need to install the Internet Information Service (IIS). You specify the settings for the WebNavigator Server during installation.

Settings under Windows 7 or Windows Server 2008

Activate the following settings under Windows 7 or Windows Server 2008:

- Web management tools:
  - IIS management service
  - IIS management console
  - IIS management scripts and tools
  - IIS compatibility to IIS metabasis and IIS 6 management
  - Compatibility with WMI for IIS 6
- WWW Services > Shared HTTP Features:
  - Standard document
  - Static content
- WWW services > Application development features:
  - ASP
  - ISAPI extensions
  - ISAPI filters
- WWW services > Security:
  - Request filter
  - Standard authentication

Note

If the logging functions are active with IIS, the log files must be monitored and deleted, if necessary. The event views should be configured so that the log files do not become too large.

Settings under Windows 8.1 or Windows Server 2012 R2

Activate the following additional settings under Windows 8.1 or Windows Server 2012 R2:

- WWW services > Application development features:
  - .NET expendability 3.5
  - NET expendability 4.5
  - ASP.NET 3.5
  - ASP.NET 4.5

Requirements

- Administrator rights
- Write access for the registry database

Procedure

1. Open the dialog for the activation of Windows features from the Windows 7 Control Panel. In Windows Server 2008, use the settings for the server manager. For detailed information, refer to the help of the operating system.
2. In the settings for the Internet Information Services, enable the settings described above.
3. Close the dialog with the "OK" button. The required data is transferred and the IIS is configured accordingly.

Alternative procedure

You can also use the command line "Start > Run > cmd" to install the IIS components located on the installation data carrier:

pkgmgr.exe /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-RequestFiltering;IIS-StaticContent;IIS-DefaultDocument;IIS-HttpErrors;IIS-ASPNET;IIS-ASP;IIS-ISAPIExtensions;IIS-ISAPIFilter;IIS-BasicAuthentication;IIS-WindowsAuthentication;IIS-ManagementConsole;IIS-ManagementService;IIS-IIS6ManagementCompatibility;IIS-Metabase;IIS-WMICompatibility;IIS-ManagementScriptingTools

6.3.4.3 Installing the WebNavigator Server (RT Professional)

Requirements

- Local administrator rights
- Internet Information Service is installed.

Procedure

1. Insert the installation disk into the appropriate drive.
   Setup runs automatically unless you have disabled autostart on the PC.
2. If the setup program does not start up automatically, start it manually by double-clicking the "Start.exe" file.
   The dialog to select the setup language opens.
3. Choose the language in which you want the setup program dialogs to be displayed.
4. To read the information on the product and installation, click the "Read Notes" or "Installation Notes" button.
   The corresponding help file opens with instructions.
5. Once you have read the notes, close the help file and click the "Next" button.
   The dialog for the selection of product languages opens.
6. Select the languages for the product user interface, and click the "Next" button. The dialog for selecting the product configuration opens.

   Note

   "English" is always installed as the basic product language.

7. Select the following components for installation:
   - WinCC Runtime Professional
   - WebNavigator Server
8. Choose whether you want a desktop shortcut to be created, and select a different destination directory for the installation if needed. Note that the length of the installation path must not exceed 89 characters.
9. Click the "Next" button.
   The dialog for the licensing conditions opens.
10. To continue the installation, read and accept all license agreements and click "Next".
    In the event that the security and permission settings need to be changed for the installation, the dialog for the security settings opens.
11. To continue the installation, accept the changes to the security and permissions settings, and click the "Next" button.
12. Check the selected installation settings. If you want to make any changes, click the "Back" button until you reach the point in the dialog where you want to make changes. Once you have completed the desired changes, return to the overview by clicking "Next".
13. Click the "Install" button.
    The installation begins.

    Note

    If no license key is found during installation, you have the chance to transfer it to your PC. If you skip the license transfer, you can register it later with the Automation License Manager.

    If the installation was successful, a message to this effect is displayed on the screen. If errors occurred during installation, an error message is displayed informing you of the type of errors.

14. It may be necessary to restart the computer. If this is the case, select the "Yes, restart my computer now." option button. Then click "Restart".
15. If the computer does not reboot, click "Exit".

Result

WinCC Runtime Professional and the WebNavigator Server are installed.

6.3.5 Installation of WebNavigator client (RT Professional)

6.3.5.1 Installing the WebNavigator Client (RT Professional)

Introduction

You can install the WebNavigator Client as follows:

- Installation from the WinCC Runtime Professional Product DVD.
  In this case, certain Windows user rights are necessary, depending on the operating system.
- Installation via Intranet/Internet.
  In this case, certain Windows user rights are necessary, depending on the operating system.
- Installation without user interaction:
  - With the Windows user rights of the current user
  - Or using group policy based software distribution in networks

You can also install the WebNavigator Client additionally on the WebNavigator server . This is useful, for example, if you want to check your WinCC project locally on the server in the Internet Explorer.

WinCCViewerRT

The "WinCCViewerRT" web viewer is installed together with the WebNavigator Client.

Procedure

1. Entry and check of the settings of the client computer in Internet Explorer.
2. Installation of the WebNavigator Client.

Note

When you install from the DVD or through group policy based software distribution, you can upgrade an older version of the WebNavigator Client directly without removal.
If you install Web Navigator Server on a computer after the WebNavigator Client, you need to reinstall the client.

Information on setup and installation of the WebNavigator Client:

- The setup of the WebNavigator Client is interrupted with the error message "WinCC Active" if the local WinCC project is open or has been opened since the PC was last restarted. Restart the computer. Check if WinCC has been entered in the Autostart directory. Remove the item, if required, and then reboot the computer to run the WebNavigator Client installation.
- At least 70 MB free disk space must be available on the local hard drive to install the WebNavigator Client. Otherwise, the installation aborts with a message.
- When installing the WebNavigator Client by downloading it from the Intranet/Internet, you can select between "Open" and "Save" for the Setup file. If you install plug-ins or ActiveX controls at a later time, you need to select the procedure used for installing the WebNavigator Client the first time. Otherwise, the error message "Error 1316" of the "MSI Installer" service appears.
- In the download area of the Web Navigation user interface, the Plug-Ins which can be installed are displayed. At least the same minimum user rights are required as for installation of the WebNavigator Client to install this plug-in. If you select a plug-in in the Web Navigation user interface, the WebNavigator Client Setup starts. You have to confirm the selected plug-in again.

Installing the WebNavigator Client under Windows Server

You cannot install the WebNavigator Client under Windows Server with user rights lower than "Administrator" with the default setting for group policies.
In the group policies, release the installation of WebNavigator Client by

- Assigning and publishing the software
- Or, under "Administrative Templates / Windows Components / Windows Installer", enabling the setting "Always install with elevated privileges". You must activate "Never" for the "Disable Windows Installer" option.

6.3.5.2 User rights, user groups and optional installation possibilities (RT Professional)

Windows user rights required for installation and initial registration of the WebNavigator client

"Administrator" rights are required to install the WebNavigator client via Intranet/Internet or using the WinCC Runtime Professional Product DVD. For the initial registration of the client on the WebNavigator server, you need to use the same name as that used during installation and must log on with the same or higher Windows user rights. The connections must be established successfully. All subsequent logons can then be performed by users with different Windows user rights, which may be more restricted.

Installing the WebNavigator client with restricted user rights

With the employed MSI technology, you can also install the WebNavigator client with restricted Windows user rights. This procedure can be set during the installation using the group policy based software distribution in networks.

The add-ons and plug-ins for the WebNavigator client can also be installed this way.

Installation for a configured group of users or computers

Using the Microsoft Systems Management server or group policy on a Domain Controller, it is possible to install a group of users or computers configured by the Administrator.

- For this the MSI file "WinCCWebNavigatorClient.msi" is published at the Domain Controller and enabled for a user group. Then, depending on the configuration of the group policy based software distribution, you perform the installation either during logon of the specified users or when the computer boots.
- When using a Microsoft Systems Management Server, the installation is configured by the administrator, triggered and executed when the relevant computer boots.

Group policy based software distribution

The software installation is normally executed with the access rights of the current Windows user. When using MSI technology, the installation is performed by an operating system service with a higher level of rights. This enables you to perform installations for which the Windows user is lacking permission. Applications which require installations with a higher-level permission are referred to as "privileged installations" in MSI technology. Installation of these applications is possible when a Windows user is assigned the "Always install with elevated privileges" permission.

To use group policy based software distribution, a group policy is created on the domain controller. The software to be distributed is assigned or published using the active directory .

- Assignment: The software distribution can be assigned to a user or a computer. The software to be distributed is automatically installed when the user logs on or computer boots.
- Publication: The software distribution can be published for single users. When the user logs onto the client computer, the software to be distributed appears in a dialog and can be selected for installation.

Installation without user interaction

During installation of the WebNavigator client, the user is normally prompted to enter information, for examples, about the components to be installed. By implementing a configuration file, installation is possible without user interaction. The required path specification and user information are provided in the "options.ini" configuration file. The file must be in the same folder as the WebNavigator client Setup.
This installation procedure is advantageous when using the group policy based software distribution.

Installation from the product DVD requires user interaction.

The settings given predefined in the table are used under the following conditions:

- The "options.ini" configuration file is missing and there is no corresponding entry available in the client registry, for example, due to another SIMATIC HMI product installed.
- Alternatively, the installation is performed via the group policy based software distribution with assignment to the computer.

Information	Parameters
Target directory for the WebNavigator client	INSTALLDIR=" <syspath1>\Siemens\Automation \SCADA-RT_V11\WinCC\WebNavigator"
Target directory for common components	COMMONDIR=" <syspath2>\Siemens "
User information / user name	USER
User information / organization	COMPANYNAME

The "<syspath?>" parameter is derived from the setting in the registry under the key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion":

- "<syspath1>" corresponds to the key "ProgramFilesDir" e.g. "C:\\Program Files"
- "<syspath2>" corresponds to the key "CommonFilesDir", e.g. "C:\\Program Files\\Common Files"

Example of a "options.ini" configuration file for Windows 7

```
[USERINFO]
USER=Integration
COMPANYNAME=Siemens AG

[INSTALLPATH]
COMMONDIR="C:\Program Files\Common Files\Siemens"
INSTALLDIR="C:\Program Files\Siemens\Automation\SCADA-RT_V11\WinCC
\WebNavigator"

[FEATURES]
FUNCTIONTRENDCONTROL=0
HARDCOPY=0
WINCCUSERARCHIVES=0
DEU=0
FRA=0
ITA=0
ESP=0
```

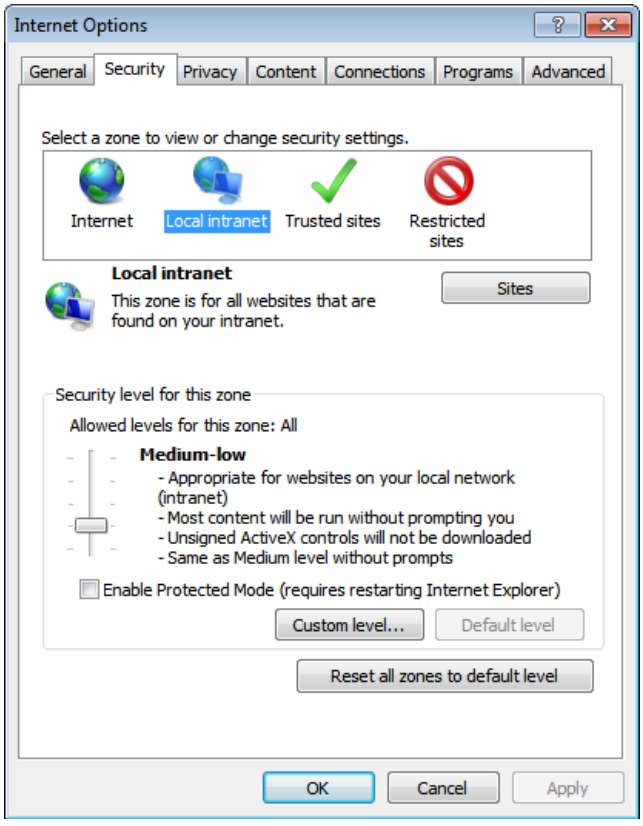
6.3.5.3 Internet Explorer Settings (RT Professional)

Introduction

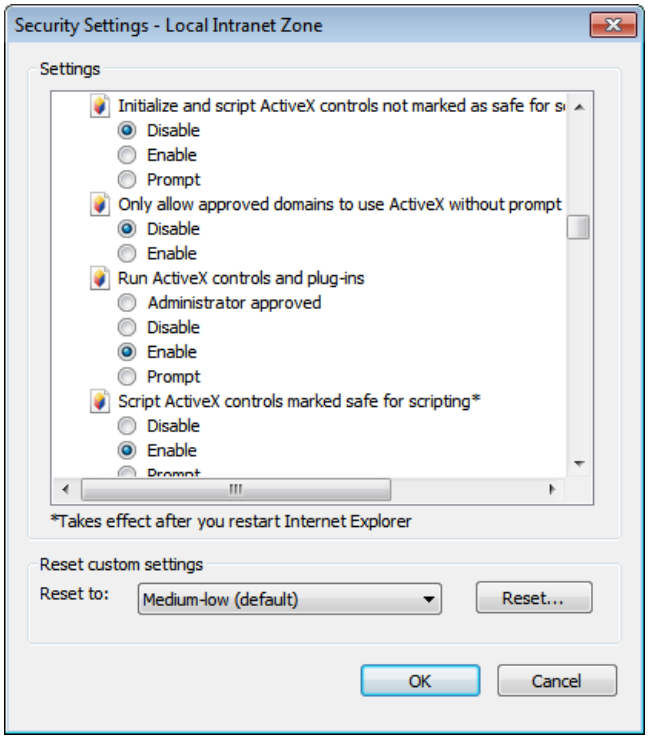
To have the full functionality available on the WebNavigator client, you need to adapt the security settings in Internet Explorer.

Procedure

1. Click "Tools" > "Internet Options" in the Internet Explorer.
2. Select the "Security" tab. Select the corresponding zone, e.g. "Local Intranet" or "Internet".



3. Click "Custom Level".



4. Select the options "Script ActiveX controls marked safe for scripting" and "Download signed ActiveX controls".
5. Select the "Active Scripting" option under "Scripting".
6. Click "OK". Carry out the modifications in the subsequent dialog.
7. Select the "Trusted Sites" icon. Open the "Trusted Sites" with the "Sites" button.
8. Enter the address of the WebNavigator server in the "Add this Website to the zone" field. Possible formats and wildcards include "*://157.54.100 - 200", "ftp://157.54.23.41", or "http://*.microsoft.com". If necessary, clear the "Require server verification for all sites in this zone (https:) check box. Click "Add". Click "Close".
9. Select the "Trusted Sites" icon. Click the "Standard level" button and then the "Custom Level" button. Activate the "Activate" option under "Initialize and script ActiveX controls not marked as safe". Click "OK".
10. Click on the "General" tab. Click on the "Settings" button in the "Browser History" area . Select the "Automatic" option under "Check for newer versions of stored pages". Click "OK".
11. Close the "Internet Options" dialog by clicking "OK".

6.3.5.4 Installation from the DVD (RT Professional)

Requirements

- The information provided in AUTOHOTSPOT applies to the installation and use of the WebNavigator client.
- Minimum user rights are required to install the WebNavigator Client depending on the operating system, see AUTOHOTSPOT.

Procedure

1. Insert the installation disk into the appropriate drive.
   Setup runs automatically unless you have disabled autostart on the PC.
2. If the setup program does not start up automatically, start it manually by double-clicking the "Start.exe" file.
   The dialog to select the setup language opens.
3. Choose the language in which you want the setup program dialogs to be displayed.
4. To read the information on the product and installation, click the "Read Notes" or "Installation Notes" button.
   The corresponding help file opens with instructions.
5. Once you have read the notes, close the help file and click the "Next" button.
   The dialog for the selection of product languages opens.
6. Select the languages for the product user interface, and click the "Next" button. The dialog for selecting the product configuration opens.

   Note

   "English" is always installed as the basic product language.

7. Open the program group "SIMATIC WinCC Web Navigator" and select the "Web Navigator Client" component.
8. Choose whether you want a desktop shortcut to be created, and select a different destination directory for the installation if needed. Note that the length of the installation path must not exceed 89 characters.
9. Click the "Next" button.
   The dialog for the licensing conditions opens.
10. To continue the installation, read and accept all license agreements and click "Next".
    In the event that the security and permission settings need to be changed for the installation, the dialog for the security settings opens.
11. To continue the installation, accept the changes to the security and permissions settings, and click the "Next" button.
12. Check the selected installation settings. If you want to make any changes, click the "Back" button until you reach the point in the dialog where you want to make changes. Once you have completed the desired changes, return to the overview by clicking "Next".

13. Click the "Install" button.
    The installation begins.

    Note

    If no license key is found during installation, you have the chance to transfer it to your PC. If you skip the license transfer, you can register it later with the Automation License Manager.

    If the installation was successful, a message to this effect is displayed on the screen. If errors occurred during installation, an error message is displayed informing you of the type of errors.

14. It may be necessary to restart the computer. If this is the case, select the "Yes, restart my computer now." option button. Then click "Restart".
15. If the computer does not reboot, click "Exit".

Result

The WebNavigator Client is installed and has been added as a function in the navigation window of the WinCC Explorer.

6.3.5.5 Installation via the Intranet/Internet (RT Professional)

Requirements

- The information provided in AUTOHOTSPOT applies to the installation and use of the WebNavigator client.
- Minimum user rights are required to install the WebNavigator Client depending on the operating system, see AUTOHOTSPOT.
- WebNavigator Server must be installed on a computer. The Internet Information Server must be configured with the WinCC Web Configurator. Users must be registered in the WinCC User Administrator. The WinCC project must be in runtime.

Procedure

1. Enter the address "http://www.servername" for the WebNavigator Server in the address bar of Internet Explorer. When installing in a virtual directory, the address can be as follows: "http:// www.servername/WebNavigator/".
2. Enter the user name and the password.

3. If you are accessing the WebNavigator Server for the first time, you will be prompted to install the WebNavigator Client. Click the "Click here to install" link. Click the "Save" button in the "File Download" dialog to store the client setup on the target computer. It is recommended to save the Setup file because, in the event of a restart of the client computer being necessary, the Setup need not be downloaded again.

   Note

   If you want to install a more current version for an existing WebNavigator client via the Intranet/Internet, go directly to the client setup. You do not need to save the installation file on the target computer. If you want to save the new installation file, remove the old installation file. Or save the new version of the file in another directory.

4. Leave the Internet Explorer open and open Windows Explorer. Navigate to the directory in which you saved the setup file. Start Setup by double-clicking the file.
5. Follow the instructions on the screen and enter the information and settings necessary. The client-end controls of the WebNavigator are installed. Close the Setup dialog.

Result

When the installation is completed successfully, the WebNavigator client switches to the WinCC project currently in runtime.

6.3.6 Installing the Web Diagnostics Client (RT Professional)

Introduction

The software for the Web Diagnostics Client is installed from the WinCC Runtime Professional Product DVD on the client computer.

Requirements

- To do this, you must have administrator rights.

Procedure

1. Insert the installation disk into the appropriate drive.
   Setup runs automatically unless you have disabled autostart on the PC.
2. If the setup program does not start up automatically, start it manually by double-clicking the "Start.exe" file.
   The dialog to select the setup language opens.
3. Choose the language in which you want the setup program dialogs to be displayed.
4. To read the information on the product and installation, click the "Read Notes" or "Installation Notes" button.
   The corresponding help file opens with instructions.

5. Once you have read the notes, close the help file and click the "Next" button.
   The dialog for the selection of product languages opens.
6. Select the languages for the product user interface, and click the "Next" button. The dialog for selecting the product configuration opens.

   Note

   "English" is always installed as the basic product language.

7. Open the program group "SIMATIC WinCC Web Navigator" and select the "Diagnostics Client" component.
8. Choose whether you want a desktop shortcut to be created, and select a different destination directory for the installation if needed. Note that the length of the installation path must not exceed 89 characters.
9. Click the "Next" button.
   The dialog for the licensing conditions opens.
10. To continue the installation, read and accept all license agreements and click "Next".
    In the event that the security and permission settings need to be changed for the installation, the dialog for the security settings opens.
11. To continue the installation, accept the changes to the security and permissions settings, and click the "Next" button.
12. Check the selected installation settings. If you want to make any changes, click the "Back" button until you reach the point in the dialog where you want to make changes. Once you have completed the desired changes, return to the overview by clicking "Next".
13. Click the "Install" button.
    The installation begins.

    Note

    If no license key is found during installation, you have the chance to transfer it to your PC. If you skip the license transfer, you can register it later with the Automation License Manager.

    If the installation was successful, a message to this effect is displayed on the screen. If errors occurred during installation, an error message is displayed informing you of the type of errors.

14. It may be necessary to restart the computer. If this is the case, select the "Yes, restart my computer now." option button. Then click "Restart".
15. If the computer does not reboot, click "Exit".

Result

1. The Web Diagnostics Client is installed.

6.4 Configuring the Web Navigator system (RT Professional)

6.4.1 Overview of configuration steps (RT Professional)

Requirements

- The server PC and client PC are interconnected via TCP/IP.
- On the server PC
  - Internet Information Service is installed.
  - The WebNavigator server is installed.
  - A license key is installed.
  - WinCC Runtime Professional is installed.
- On the client PC
  - Internet Explorer V8.0 or higher is installed.

  or
  - WinCCViewerRT is installed.

Basic procedure

The following configurations are required to set up a WebNavigator system:

1. Configure the WinCC project in the TIA Portal. For more information about the TIA Portal, refer to "Getting started with the TIA Portal"
   - Configure WinCC screens for Web access.
   - Create users for WebNavigator client access
   - Observe restrictions
   - Compiling a project
2. Transfer your WinCC project to the server PC. If the configuration PC and the WebNavigator server are interconnected, transfer the WinCC project using the command "Load to device > Software (all)".
3. Configure the WebNavigator Web page on the WebNavigator server.
4. Operate the WinCC project.
   - Using WinCCViewerRT
   - Using Internet Explorer

6.4.2 Configuring a WinCC project (RT Professional)

6.4.2.1 Configuring WinCC screens for Web access (RT Professional)

Configuring individual WinCC screens for Web access

1. Double-click the desired screen in the project tree. The screen is opened and the screen properties are shown in the Inspector window.
2. In the Inspector window, click "Properties > Properties > Web access".
3. Activate "Web access".

or

1. select the desired screen in the project tree.
2. Select "Web access" command in the shortcut menu.

Configuring several screens for Web access

1. Select "Screens" in the project tree.
2. Select the "Web access for all" command in the shortcut menu.

Result

The WinCC screens are configured for Web access. During compilation of the project, the WinCC screens are adapted for access via the Intranet/Internet and published on the WebNavigator server.

For more information, refer to "Transferring a WinCC project (Page 316)".

See also

Transferring a WinCC project (Page 316)

6.4.2.2 WinCC screens as a gadget (RT Professional)

Gadget on the Web Navigator Server (RT Professional)

Introduction

Using the "Preview" property, you define which screens to group in a gadget. Gadgets are mini applications for the Windows sidebar. In order to use gadgets, a WebNavigator client must always be installed as well on the WebNavigator server.

The following operating systems support gadgets:

- Windows 7 (Professional, Enterprise, Ultimate, Embedded StdE 7)
- Windows Server 2008 Standard Edition SP2

Procedure

To configure WinCC screens as a gadget, proceed as follows:

1. Double-click the desired screen in the project tree. The screen is opened and the screen properties are shown in the Inspector window.
2. In the Inspector window, click "Properties > Properties > Web Access".
3. Activate "Preview" and "Web access".
4. Save the WinCC project.
5. Select the "Compile > Software" command in the shortcut menu of the HMI device.

Result

The screens are assembled for the gadget on the WebNavigator server. As soon as the project is in runtime, the WebNavigator server generates a jpg snapshot image "pdlImage.jpg" of each screen at cyclic intervals and in consecutive order.

The file is stored in the directory "\WinCC\Webnavigator\Server\Web\image_gadget". The gadget accesses this file cyclically.

Note that user interactions are not possible in the screens displayed. This includes, for example, calls from login dialogs or notice dialogs via functions.

The following objects are not supported for the display in a gadget:

- GSC diagnostics window
- Media Player

Note

The WinCC project shown in the gadget cannot be operated.

Gadget on the Web Navigator Client (RT Professional)

Introduction

In order to use gadgets, a WebNavigator client must always be installed as well on the WebNavigator server. A preconfigured gadget for displaying WinCC screens is located on the WebNavigator client in the installation directory under "\WinCC\Webnavigator\GADGET".

The following operating systems support gadgets:

- Windows 7 (Professional, Enterprise, Ultimate, Embedded StdE 7)
- Windows Server 2008 Standard Edition SP2

Requirement

The screens are published on the WebNavigator server and configured as "Preview".

Procedure

To access the gadget with the WebNavigator client, proceed as follows:

1. Double-click on the "_WebNavigator.gadget" gadget in the installation directory under "\WinCC\Webnavigator\GADGET". IN Windows 7 / Windows 2008, the gadget is installed in the sidebar.
2. Define the update cycle in which the gadget loads a screen from the WebNavigator server, every 17 seconds for example.
3. Enter the address of the WebNavigator server. The gadget establishes a connection to the WebNavigator server.
4. If necessary, drag-and-drop the gadget onto the desktop.

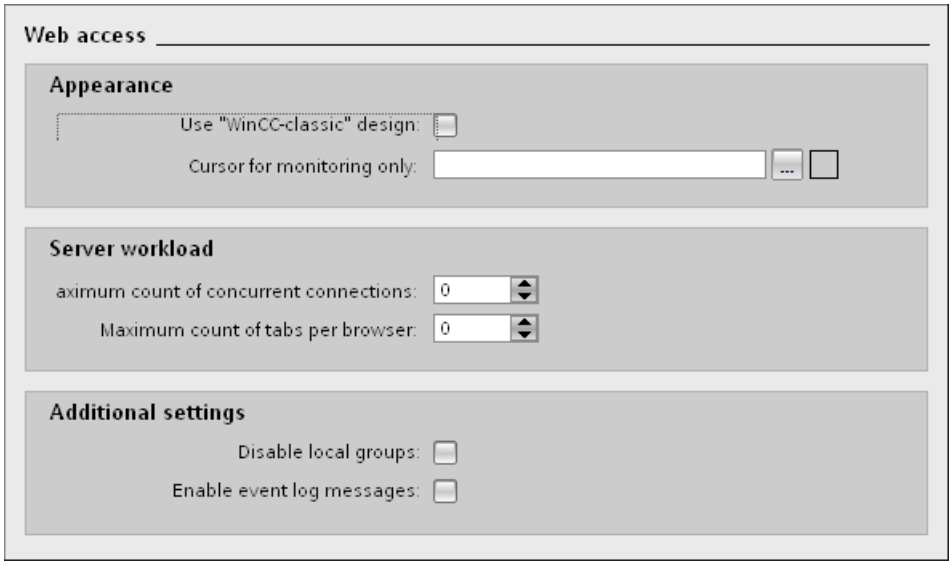
6.4.2.3 Configuring runtime settings (WebNavigator) (RT Professional)

Introduction

You can configure the behavior in runtime in the "Runtime settings" editor.

Procedure

1. Open the "Runtime settings > Web access" editor.



2. To use the "WinCC Classic" design, activate "Use "WinCC-classic" design".
3. To use your own cursor as a "View only cursor", enter the path and file name of the cursor at "Cursor "View only". Alternatively, navigate to the file of the desired cursor using the "…" button.

4. To change the maximum number of concurrent connections, enter the desired number in the "Count of concurrent connections" field.
5. To change the maximum number of open tabs in the browser, enter a suitable value in the "Number of tabs per browser" field. Internet Explorer V7 or higher supports this setting.

   Note

   Server load settings

   Each tab that calls the server homepage uses a license on the server PC. A connection setting of "10" and a tab setting of "2" corresponds to 20 clients. A license for at least 20 clients must be available on the server PC.

6. Define whether the local user group is disabled on the WebNavigator Server.
7. To output an appropriate system message when a WebNavigator logs on and off, activate "Enable event log messages".

Result

The settings for Runtime are configured.

See also

Operating a WinCC project (Page 327)

Setting up WinCCViewerRT (Page 325)

6.4.2.4 Managing users for the Web Navigator Client (RT Professional)

Administration of users for the WebNavigator client (RT Professional)

Introduction

For each user to be logged onto the web client, you must configure the following:

- A start screen of your choice enabled for web access
- A language of your choice

This allows you to make various sections of a project immediately accessible or inaccessible for users.

Requirements

- The "Users" work area is open.
- The user "Foreman" has been created.
- The "Start" screen has been created and the web access is activate.
- The selected project language is activated.

Setting the start screen and language

1. Position the mouse cursor on the title of the "Users" table.
2. Open the shortcut menu by right-clicking and activate the display of the "Web start screen" and "Web language" columns.
3. Click the ... button in the "Master" user row in the "Start screen" column. A dialog box for selecting the start screen opens.
4. Select the "Start" screen.
5. Close the dialog box by using the  icon.
6. Click the  button in the "Web language" column. A dialog box for selecting the language opens.
7. Select the desired language as the runtime language of the web user.

As an alternative, select the user in the work area; the properties of the user are then displayed in the Inspector window. In the Inspector window, select "Properties > Properties > Web options". Select the start screen and the language.

Note

The language setting is retained when a user is moved from one group to another one. The start screen will be overwritten.

Administration of user groups for the WebNavigator client (RT Professional)

Introduction

For each user group to be administered for web clients, you must configure the following:

- A start screen of your choice enabled for web access
- A language of your choice

This allows you to make various sections of a project immediately accessible or inaccessible for users.

Note

The name of the user group has to be unique within the project. Otherwise the input is not accepted.

Requirements

- The "User groups" work area is open.
- The "Start" screen has been created and the web access is activate.
- The selected project language is activated.

Procedure

1. Position the mouse cursor on the title bar of the "Groups" table.
2. Open the shortcut menu by right-clicking and activate the display of the "Web start screen" and "Web language" columns.
3. Double-click "Add..." in the "Groups" table.
4. Enter "Web operators" as the name of the user group.
5. Click the ... button in the "Web start screen" column. A dialog box for selecting the start screen opens.
6. Select a start screen for Runtime.
7. Close the dialog box by using the  icon.
8. Click the  button in the "Web language" column. A dialog box for selecting the language opens.
9. Select the runtime language.
   As an alternative, select the user group in the work area; the properties of the user group are then displayed in the Inspector window.
10. In the Inspector window, select "Properties > Properties > Web options".
11. Select the start screen and the language.

Note

The name of the user group is language-dependent. You can specify the name in several languages and switch between languages in runtime.

6.4.2.5 Limitations (RT Professional)

Introduction

You can use your projects already created with WinCC to also make them available via the Internet/ Intranet.

Essentially, the step consists in publishing the already created WinCC screens and using user administration to set up Web users.

The current version of the Web Navigator has a number of restrictions with regard to functionality, and as a "thin client" solution does not support all the functions offered by a standard WinCC basic system.

You may therefore have to check your existing WinCC projects for these restrictions and if applicable, adapt them.

Functionality restrictions

When using non-supported functions, the user will be informed of this in Runtime with plain text messages.

- The Web Navigator Client only offers the view of a running WinCC project. A configuration of the WinCC Server projects via the Web Navigator Client is not possible.
- Only those WinCC option packages/add-ons can run on the Web Navigator Client, whose documentation expressly states that.
- Not all Runtime API functions are supported on the Web Navigator Client. A list of the functions supported is provided in the Appendix.
- Nearly all the PCS7 options are supported. A list of the options that are not supported is provided in the Appendix.
- The "Reports" editor is an integrated reporting system of WinCC for the time-triggered or event-triggered documentation of alarm messages, operations and log contents. This reporting system is not supported via the Intranet/Internet. Thus, the output of reports is, for example, only possible on the Web Navigator Server and WinCC client.
- No separate logging system is running on the Web Navigator Client. The message log and message system can only be operated and monitored.
- C functions are created and executed in the project of the WinCC server. Functions cannot run on the Web Navigator Client.
- If VB functions are used, there are only minor restrictions due to non-supported functions. If non-supported functions are used in a VB function, an alarm is output.

6.4.3 Transferring a WinCC project (RT Professional)

Requirement

- A WinCC project is configured
- WebNavigator server is installed on the server PC.
- The configuration PC and server PC are interconnected.

Online transfer

Transfer the WinCC project using the command "Load to device > Software (all)". The project is compiled prior to the download. The screens are adapted for access via Intranet/Internet during compilation.

During the download to the server PC, the configured WinCC project is transferred and the screens are published on the WebNavigator server. For more information, refer to "Compiling and loading".

See also

Configuring WinCC screens for Web access (Page 310)

6.4.4 Configuring the Web Navigator Server (RT Professional)

6.4.4.1 Setting up the Web Navigator Web site (RT Professional)

WinCC Web Configurator (RT Professional)

Introduction

The Internet Information Service (IIS) is set up and managed with the WinCC Web Configurator.

Requirement

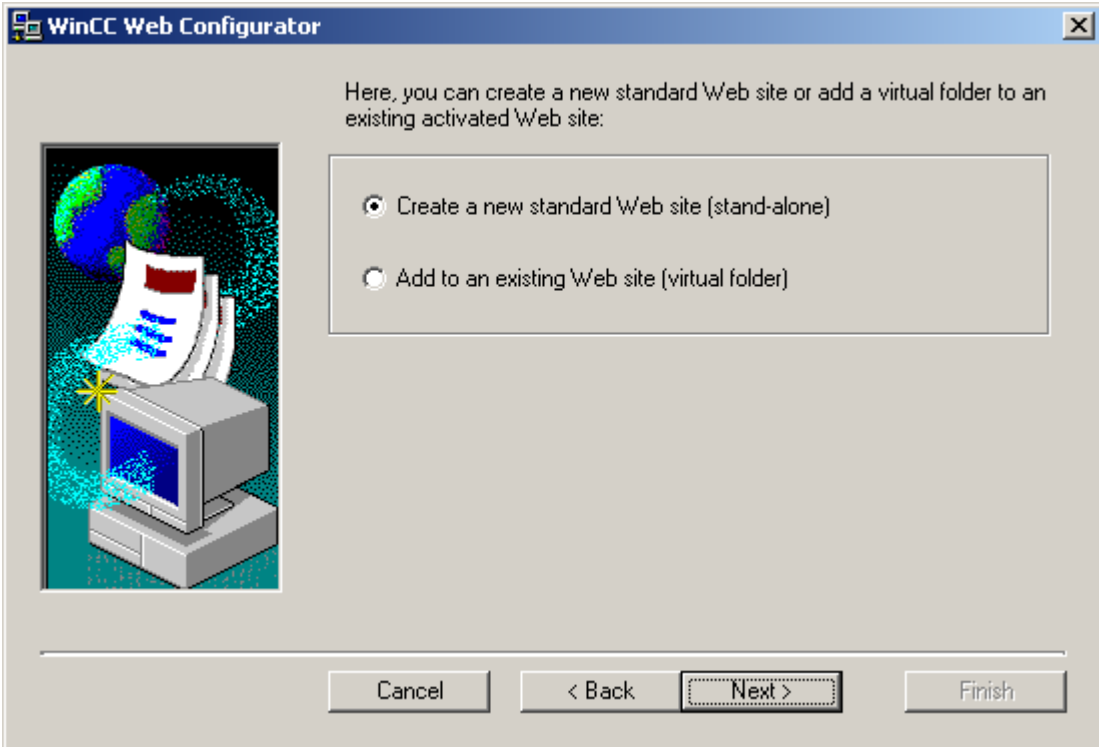
- WebNavigator Server is installed.
- Internet Information Service is installed.

Starting WinCC Web Configurator:

In the Start menu, select "Start > All Programs > Siemens Automation > Option and Tools > HMI Tools" > WinCC Web Configurator".

Initial configuration with the WinCC Web Configurator

During the initial configuration, you specify whether you want to create a new default Web site or a new virtual folder.



- If you only wish to operate the WinCC WebNavigator Web site on your server, activate the option "Create a new standard Web site (stand-alone)".
- If the WinCC WebNavigator Web site is to be added as a subdirectory to your existing Web, activate the option "Add to an existing Web site (virtual folder)".
  This option is necessary if the previous default Web site must remain active or if the operating system supports only the operation of one website.

Configuration management with the WinCC Web Configurator

If the IIS is already configured, change the settings of the existing Web server or virtual directory with the WinCC Web Configurator.

The Web Configurator automatically detects whether a configuration already exists. If a configuration already exists, the dialog for changing the configuration opens.

Note

When you delete the Web directory, restart the PC before creating a new Web directory with the WinCC Web Configurator.

Note the following:

When you change the Web directory and your Web communication is then no longer established, the Web Configurator attempts to automatically adjust the settings correctly.

If this does not work, delete the Web directory from the IIS. Restart the PC and create a new Web directory with the Web Configurator.

Creating a New Standard Web site (Stand-Alone) (RT Professional)

Requirement

- WinCC WebNavigator is installed.
- Internet Information Service is installed
- WinCC Web Configurator is started

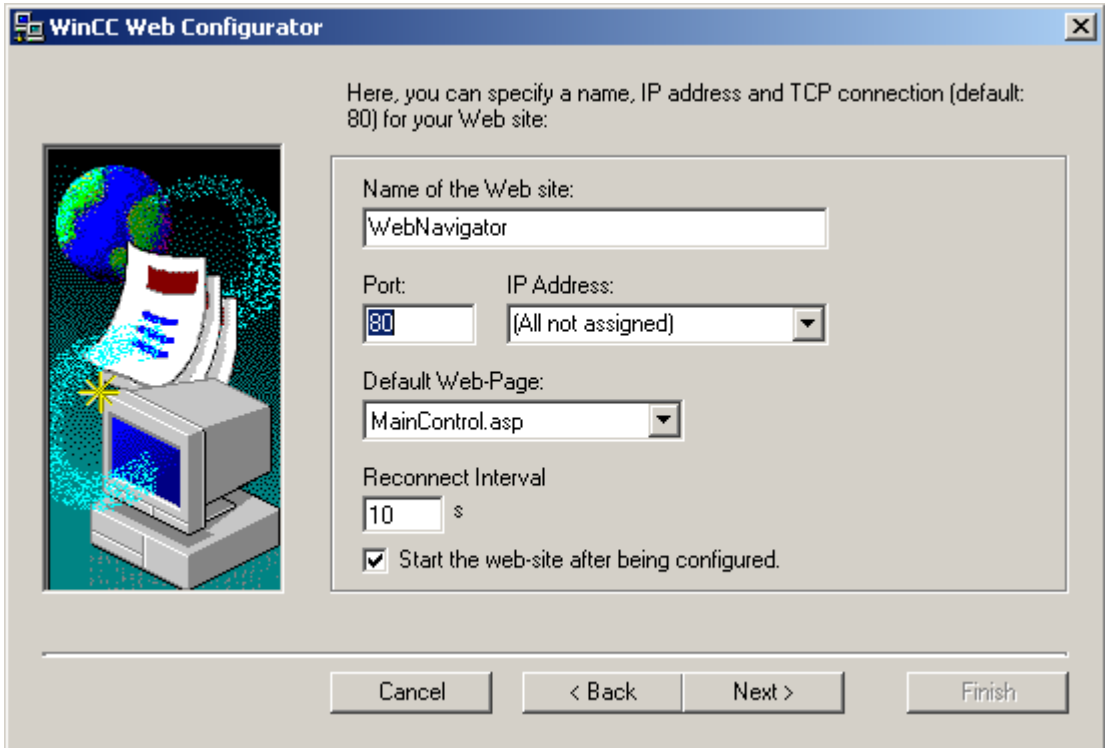
Note

If you have any questions or experience problems with the following settings, contact your Intranet/Internet administrator.

Procedure

Proceed as follows to create a standard Web site:

1. Select "Create a new standard Web site (stand-alone)" and click "Next".



2. Enter the name of your Web site in the "Name of the Web site" field.
3. In the "Port" field, enter the port number used for access.
4. In the "IP address" field specify whether the PC is to be reached in the Intranet, Internet or in both networks. Only use addresses from the selection list.
   If you want to make your PC accessible via the Intranet and the Internet, select "All not assigned".
5. Define the standard Web site that is displayed after selecting the Web server on the WebNavigator Client
   - MainControl.asp
     Starts the WinCC Navigation interface. You need the navigation interface, for example, for download installation.
   - WebClient.asp
     Opens the start screen configured in user administration after login.
6. Define the time interval after which the WebNavigator Clients automatically start to establish a connection following a connection breakdown. If "0 s" is set, the "Automatic connection establishment" function is disabled.
7. Define the way the Web site is started after configuration.
8. If you have not activated a firewall, click "Finish". If you have installed a firewall, click "Next".

Result

The Web directory has been created and the Web page is activated. If you have activated the firewall, configure the firewall settings with the Web Configurator. For further information, refer to "AUTOHOTSPOT".

Creating a virtual folder (RT Professional)

Requirement

- Internet Information Service is installed
- WinCC WebNavigator is installed.
- WinCC Web Configurator is started

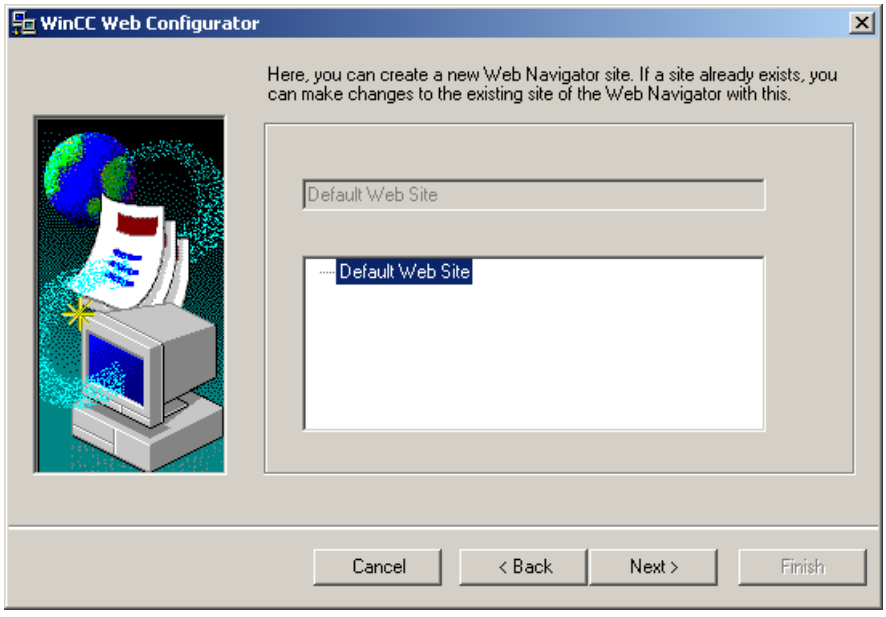
Note

If you have any questions or experience problems with the following settings, contact your Intranet/Internet administrator.

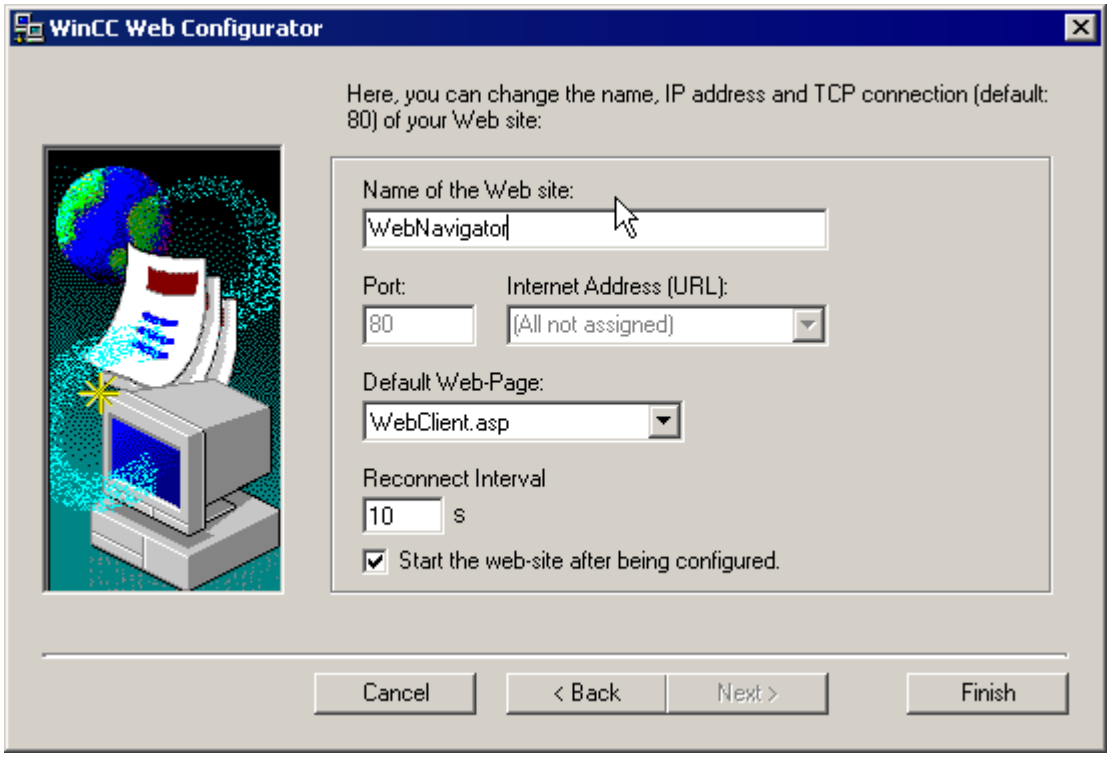
Procedure

Proceed as follows to create a virtual directory:

1. Select "Add to an existing Web site (virtual folder)". Click "Browse."
2. In the following dialog, select the active Web site to which the virtual directory is to be added.



3. Click "OK" to close the dialog box. Click the "Next" button in the following dialog.



4. Enter the name of your Web site in the "Name of the Web site" field.
5. The WinCC Web Configurator takes the IIS settings for the port number and IP address.
6. Define the standard Web site that is displayed after selecting the Web server on the WebNavigator Client.
   - MainControl.asp
     Starts the WinCC Navigation interface. You need the navigation interface, for example, for download installation.
   - WebClient.asp
     Opens the start screen configured in user administration after logon.
7. Define the time interval after which the WebNavigator Clients automatically start to establish a connection following a connection breakdown. If "0 s" is set, the "Automatic connection establishment" function is disabled.
8. Define the way the Web site is started after configuration.
9. Click "Finish" to complete the configuration.

Result

The virtual Web directory has been created and the Web site is activated. To access the Web site, with the WebNavigator Client, add the name of the virtual Web directory to the URL, for example http://WebServer/WebNavigator.

No Active Website

If no active Web is found, the WinCC Web Configurator terminates with a message.



Click "OK" to close the dialog box.

To execute the Web Configurator again, first activate a Web site. For additional information, refer to "Checking of Activated Web site".

6.4.4.2 Setting up a firewall (RT Professional)

Introduction

This section describes only the activation of the "HTTP" and "HTTPS" services for port 80 in the respective operating system.

To set up the Windows firewall with advanced security, or for a different port, contact your network administrator.

Requirement

- You have created a standard Web site using the Web Configurator.
- The firewall is activated.
- A logged on Windows user has administrator rights

Procedure

To set up the firewall for a standard port, proceed as follows:

1. Click "Windows Firewall" in the "WinCC Web Configurator".
2. The "Windows Firewall" dialog will open.
3. In Windows 7 or 2008, click "Allow a program or feature through Windows Firewall".
   In Windows 8.1 or 2012, click "Allow an app or feature through Windows Firewall".
4. Activate "Secure WWW Services (HTTPS)" or "WWW Services (HTTP)".
5. Exit the open Windows dialogs with "OK".
6. Click "Finish" in the Web Configurator. The configuration of the server will be completed.

6.4.4.3 Checking the Activated Web Site (Web) (RT Professional)

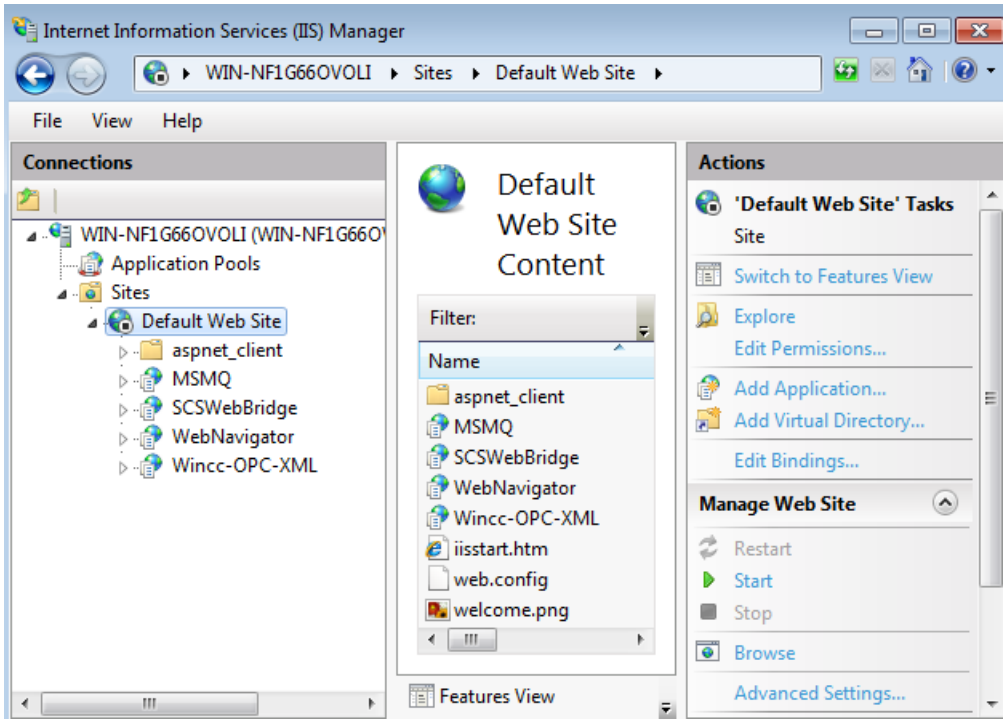
Note

Note that the operating system settings shown depend on the language set for the operating system.

Procedure

Proceed as follows to check the activated website:

1. In the Start menu, select "Programs" > "Administrative Tools" > "Internet Services Manager".



2. Click the name of the PC in the "Connections" area.
3. Click "Default Web Site".
4. Check the information displayed for the websites. If "Stopped" is displayed next to the desired Web site, e.g. "WebNavigator", start the Web site.
5. To start the Web site, select the "Start" command in the shortcut menu.

6.5 Operating a WinCC project (RT Professional)

6.5.1 Operating projects using WinCCViewerRT (RT Professional)

6.5.1.1 Setting up WinCCViewerRT (RT Professional)

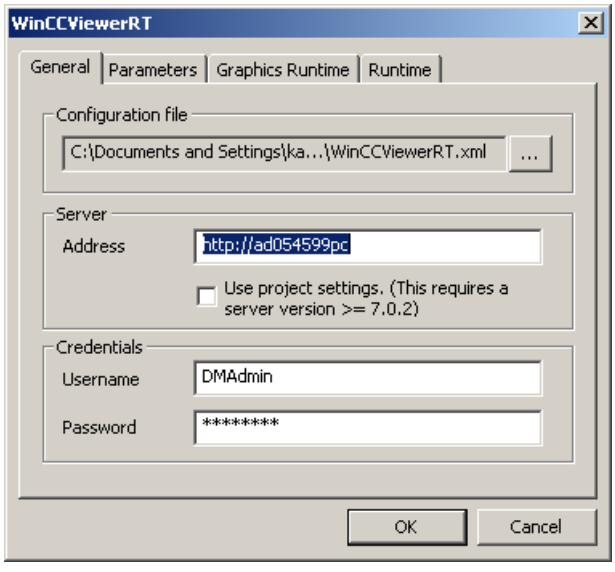
Requirement

- On the server PC
  - The WebNavigator server is installed.
  - A license key is installed.
  - The WinCC project is in Runtime.
  - The WinCC screens are configured for Web access and published.
- On the client PC
  - WebNavigator client is installed.

Procedure

Set up WinCCViewerRT as follows:

1. In the Start menu, select "Start > All Programs > Siemens Automation > Option and Tools > HMI Tools" > WinCCViewerRT".
2. Enter the logon data in the "General" tab:



   - Server address: http://<server name>, or http://<IP address>
   - User name and password

3. In the "Parameters" tab, specify the Runtime language and whether to disable keystrokes that the operator uses to change to other programs.
4. Define the WinCC Runtime Professional properties in the "Graphics Runtime" tab:
   - Start screen
   - Configuration file for screen navigation
   - Window attributes
   - Illegal user actions
5. Specify additional user actions on the "Runtime" tab:
   - Automatic logout
   - Enable screen keyboard.
   - Use <Ctrl+Alt+Del> to switch to the Task Manager and to the operating system. This setting is only valid for the on-screen keyboard.
   - Open the "WinCCRTViewer" by means of keystroke.
     You can change the default keystroke <Ctrl+Alt+P>.
6. Close the dialog with "OK".

Result

WinCCViewerRT is configured. When the dialog is closed, the connection to the WebNavigator server is established. The settings are saved to the configuration file "WinCCViewerRT.xml". The settings in the configuration file are used at the next start of WinCCViewerRT.

The configuration file is stored in the directory "C:\Users\<User name>\Appdata\LocalLow \Siemens\SIMATIC.WinCC\WebNavigator\Client" . Under <User name>, enter the name of the user logged-on when the file is created. This allows different configurations to be used, depending on the logged on user. WinCCViewerRT applies the interface language from WinCC.

WinCCViewerRT.xml Renaming or removing

When you rename or remove the file WinCCViewerRT.xml, the configuration dialog of WinCCViewerRT is opened during the start. Reconfigure WinCCViewerRT, or select a different configuration file.

See also

Configuring runtime settings (WebNavigator) (Page 312)

6.5.1.2 Operating a WinCC project (RT Professional)

Requirement

- On the server PC:
  - The "WinCC WebNavigator license is installed.
  - The WinCC project is in Runtime.
  - The WinCC screens are configured for Web access and published.
  - A user is created in WinCC.
- On the client PC
  - WinCCViewerRT is configured.

Procedure

To view screens, proceed as follows:

1. In the Start menu, select "Start > All Programs > Siemens Automation > Option and Tools > HMI Tools" > WinCCViewerRT".
2. Log on to the WebNavigator server:
   - If the user and password are configured in "WinCCViewerRT", no logon dialog displayed.
   - If no user and password was configured in "WinCCViewerRT", the logon dialog displayed. Enter the user name and the password of the WinCC user. Click "OK".
3. Press the <Ctrl+Alt+P> keystroke to change the user. The "WinCCViewerRT" dialog opens. Enter the user name and password on the General" tab.
   You can also select the xml file that contains this data.

Result

WinCCViewerRT connects to the selected WinCC project. The start screen configured for the user is displayed. Users can operate and monitor the project, depending on their authorizations.

If the user is assigned the authorization no. 1002 "Web access - view only", he/she can only view the project.

The cursor is a "View only cursor" and indicates that process-related operations are not allowed.



Certain operations are still possible, such as opening the properties dialog of an online trend control.

If necessary, you can use your own cursor symbol as a "View only cursor". See "Configuring runtime settings (WebNavigator) (Page 312)" for more detailed information.

6.5.2 Operating projects in Internet Explorer (RT Professional)

6.5.2.1 Operating a WinCC project (RT Professional)

Requirement

- WebNavigator client is installed.
- A user for the WebNavigator Client has been created.
- Internet Explorer as of V8.0

Procedure

To operate the WinCC project, proceed as follows:

1. Enter the address of the WebNavigator Server in the address bar of Internet Explorer:
   - Standard Web site: "http://servername"
   - Web site in the virtual directory: "http://servername"
2. Confirm your entry
3. Enter the user name and the password. Confirm your entry.

Result

The standard Web site is displayed. The appearance depends on the configuration.

If "WebClient.asp" is set, the WebNavigator Client starts with the start screen defined in user administration. For more information, refer to "Managing users for the Web Navigator Client (Page 313)".

If "MainControl.asp" is set, the WebNavigator client starts with the Web navigation interface. For more information, refer to "Working with the Web navigation interface (Page 329)".

See also

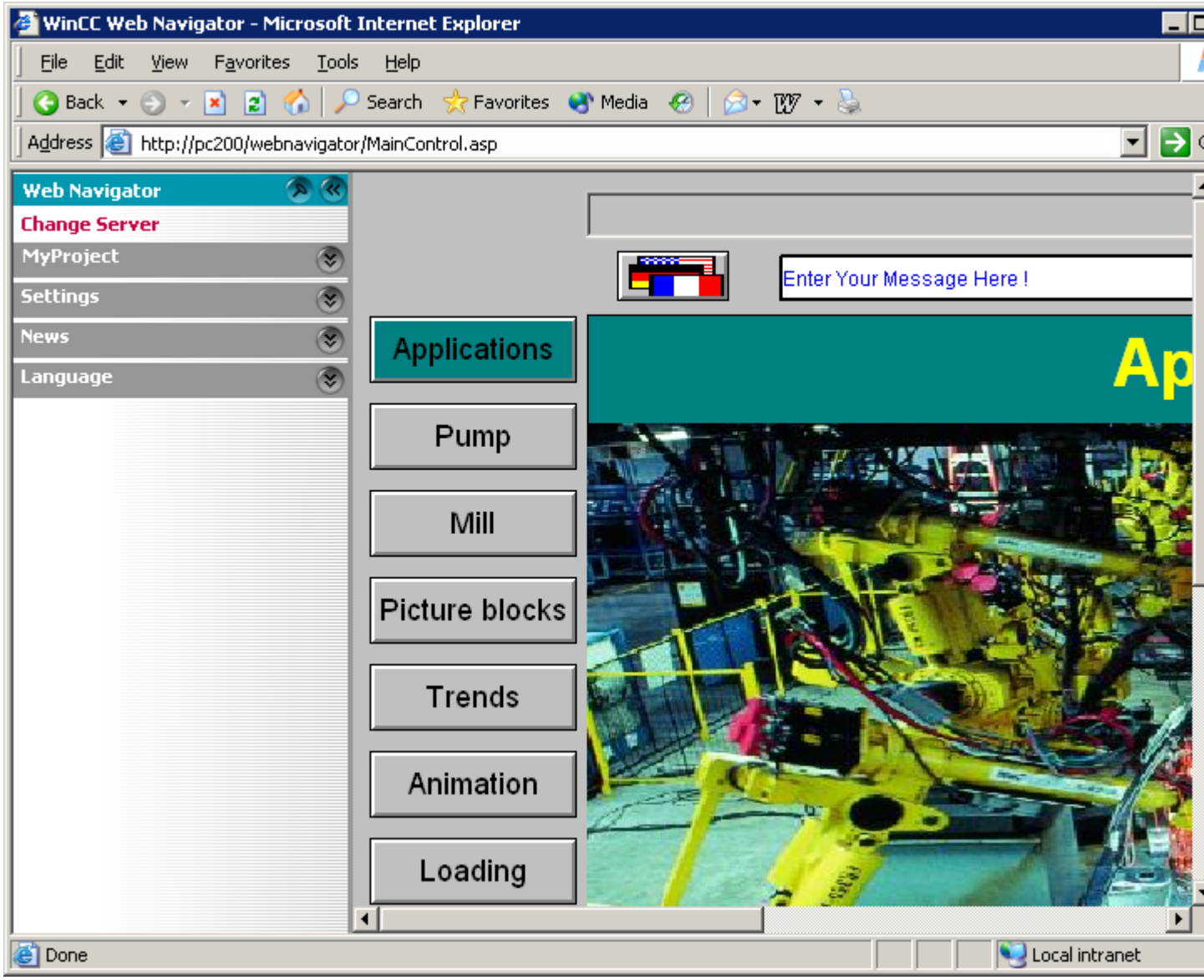
Working with the Web navigation interface (Page 329)

6.5.2.2 Working with the Web navigation interface (RT Professional)

Structure (RT Professional)

Navigation interface menu

The Web Navigation interface combines various Web functions. The various functions are grouped in menus.



- "Change Server" menu:
  Switch to a different WebNavigator server or Sm@rtServer.
- Menu of the current server:
  - Screens: Display or screen navigation of the current WebNavigator Server.
  - Report tools: Installed tools such as "DataWorkbook" for the display and analysis of current process values and historic data.
  - Analysis tools: Installed tools such as "Dat@View" for the display of log data in tables and trends.
  - Diagnostics tools: Status.html for diagnosing the WinCC project and the connection to the Web Navigation server.
  - Additional tools: This can be expanded by the user.
  - Download area:
    The plug-ins which are stored on the WebNavigator Server in the directory "Install / Customize" are available, e.g download of add-ons for WebNavigator.
- "Settings" menu:
  Settings for the WebNavigator Client e.g. adaptation of size of screens
- "Current" menu:
  Links to Web pages, such as "SIMATIC HMI", "WinCC" or "WinCC flexible".

  Note

  The contents of the websites under "News" can be displayed based on the settings both in a new window as well as in an window already open in Internet Explorer. You can make the settings for opening new pages in the Internet Explorer or in your operating system.

- "Language" menu:
  Changing the language of the navigation interface. The standard version of the program includes five languages.

Functions (RT Professional)

User logon

When logging onto the WebNavigator server, the user can determine - through the address entered in Internet Explorer - whether he logs on via the Web navigation interface or the start page configured in the WinCC project.

- The address "http://<server_name>/webnavigator" opens the start page configured in the User Administrator following the logon.
- The address "http://<server_name>/webnavigator/maincontrol.asp" starts the Web navigation interface.

Change of the Server

A different server can be selected via the menu command "Change Server". Enter the address of the new WebNavigator server in the upper input box. Examples of possible input formats are described under "User Logon".
In the lower field, a symbolic name can be entered, which is shown in the menu as the current WebNavigator server. If the name is not specified, the address of the WebNavigator server is displayed.

Expansion Options

Menu

The menu of the navigation interface can be expanded by additional menu entries and functions, for example, depending on the operational area. An expansion is configured in an XML file. The XML file is saved on the WebNavigator server in the subdirectory "_custom_data". Further information is available in the topic "Extending the Web Navigation User Interface".

Tools

The menu command "Additional tools" can be expanded by the user to provide additional tools on the WebNavigator client.

Plug-Ins

The "Download Plug-Ins" menu command provides plug-ins that have been stored on the WebNavigator server in the folder "Install/Customize". In order to display the version name of a plug-in, it must have been assigned the format "Vxx.xx.xx.xx" or "xx.xx.xx.xx".

Languages

Adjustment of language options may be facilitated by adjusting the "Menu.xml" file. The languages are stored as CSV files on the WebNavigator server in the folder "_languages / <language_identifier>". When adding, these language files have to be referenced in the file "maincontrol.asp".

6.5.2.3 Diagnosis of the Connections with "Status.html" (RT Professional)

Introduction

You can call up status information via the WebNavigator server and the WebNavigator clients from a WebNavigator server or any WebNavigator client. The status information will provide information about which users access the WebNavigator server by which Web Navigator clients.

Access to this page is restricted to the users created in the "User Management" by WinCC.

Requirement

User is created in user administration.

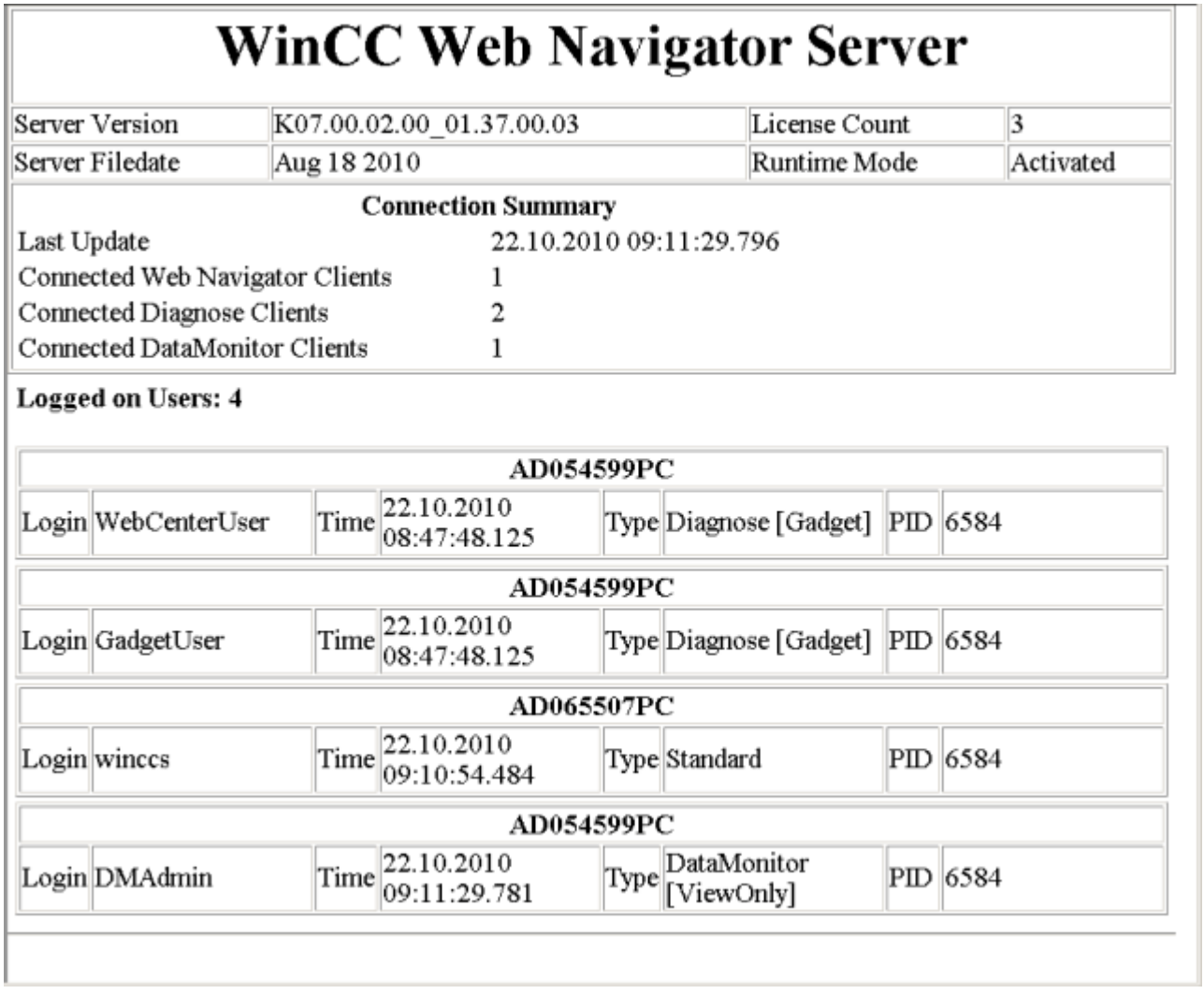
Display "Status.html"

To view the "Status.html" diagnostic site, enter the appropriate address of the WinCC server on which WinCC Runtime runs in the address line:

- Standard Web site: "http://www.server_name.de/status.html"
- Web site in the virtual directory: "http://www.server_name.de/WebNavigator/status.html"
- Log in with your WinCC user name and password.

Status information

The status information is displayed in blocks within the HTML page. There is one information block for the WebNavigator server and one information block for each connected WebNavigator client. The information is only displayed in English.



WinCC Web Navigator Server

Server Version	K07.00.02.00_01.37.00.03	License Count	3
Server Filedate	Aug 18 2010	Runtime Mode	Activated

Connection Summary

Last Update	22.10.2010 09:11:29.796
Connected Web Navigator Clients	1
Connected Diagnose Clients	2
Connected DataMonitor Clients	1

Logged on Users: 4

AD054599PC							
Login	WebCenterUser	Time	22.10.2010 08:47:48.125	Type	Diagnose [Gadget]	PID	6584

AD054599PC							
Login	GadgetUser	Time	22.10.2010 08:47:48.125	Type	Diagnose [Gadget]	PID	6584

AD065507PC							
Login	winccs	Time	22.10.2010 09:10:54.484	Type	Standard	PID	6584

AD054599PC							
Login	DMAdmin	Time	22.10.2010 09:11:29.781	Type	DataMonitor [ViewOnly]	PID	6584

Time specification is in UTC (i.e. minus one hour to CET; minus 2 hours to CEST).

Structure of the Information Block of the WebNavigator server

Field	Description
Server Version	Displays the version number of the WebNavigator server (build no.)
Server File Date	reserved
License Count	Displays the number of licenses
Runtime Mode	Displays the status of Runtime, e.g. activated
Last Update	Date and time of the last refresh of the display
Connected WebNavigator client	Number of connected WebNavigator clients
Connected diagnostic clients	Number of connected diagnostic clients
Connected DataMonitor clients	Number of connected DataMonitor clients

Structure of the information blocks of the Web Navigator clients

Below the caption "Logged on Users:", the information blocks of the connected clients are listed. Each block has the name of the client as a header.

Field	Description
Login	Login name of the current user
Time	Login time of the current user or also time of the most recent automatic reconnect.
Type	Type of WebNavigator client, such as Default, Demo, View Only
PID	Process ID of instance of WebNavigatorRT.exe on the WebNavigator server communicating with this WebNavigator client.

Save status information

The displayed status information can be saved. To do this, use the "Save As" menu command in Internet Explorer and select "(*.txt)" as the file type.

If "(*.htm, *.html)" are selected, the contents displayed are not saved.

6.5.3 Use the "Hardcopy" function (RT Professional)

Introduction

On the WebNavigator client it is possible to generate a hardcopy of the entire screen, of a section, or of the active window.

The hardcopy is output to the default printer by executing the "PrtScr.exe" application.

Requirement

- WebNavigator client is installed.

Starting the hardcopy application

The program is started on the WebNavigator client, for example, using the command input line, or a user-defined function.

The application is saved to the folder "...\Common Files\Siemens\BIN\". The hardcopy is triggered depending on the parameters used.

Examples of the command line

"C:\Program Files\Common Files\Siemens\BIN\PrtScr.exe" –infinit –hotkey="<ALT>+p"

Starts PrtScr.exe and waits for the <ALT>+p keystroke. The entire screen is printed when you press the keystroke.

Parameters

Parameters	Function
-infinit	Used as parameter for launching PrtScr.exe on a system without WinCC. Always use the parameter in combination with "hotkey". The print keystroke and output parameters are not determined in the WinCC project. They are transferred instead via command line input. The PrtScr.exe application is started and waits for the input of the print keystroke. The parameters were transferred once during startup. To edit these parameters close the PrtScr.exe application. Change the parameters and then restart PrtScr.exe .
-end	terminates an active instance of PrtScr.exe
-hardcopy	Starts PrtScr.exe, directly initiates a hard copy, and then waits for the keystroke. Always use the parameters in combination with "infinit" and "hotkey".
-nomcp	Starts PrtScr.exe , creates the hardcopy, and closes PrtScr.exe.
/C= left;top;right;bottom	Starts PrtScr, directly triggers a hardcopy of the specified screen area, and then ends PrtScr.exe (
-l	Prints in landscape format.
-hotkey="x"	Specifies the keystroke. Valid characters and combinations: <ALT>, <SHIFT>,<CTRL> + {0-9, A-Z, 0xXX} The hexadecimal notation "0xXX" can be used to specify the "Virtual Key Code". For more information on "Virtual-Key Codes", refer to the MSDN Library.

6.6 Setting up terminal services for Web Navigator (RT Professional)

6.6.1 Communication Using Terminal Services (RT Professional)

Communication by means of terminal services

To use the WebNavigator Client as a terminal client, do not use a proxy server between the terminal server and WebNavigator Server.

If the terminal server and WebNavigator Server are not installed on the same PC, the WebNavigator Client cannot access the Web Navigation server via the terminal services.

This problem can be solved in various ways:

- A minimal installation of WinCC without licenses is installed on the terminal server.
- After installing the WebNavigator Client, the file "CCEClient_service.vbs" is executed once on the terminal server. The file is located on the WebNavigator product DVD in the "\WebNavigator" directory. The Windows user right "Administrators" is required to execute the VBS file.

Access from the WebNavigator Client and WinCC clients to the WebNavigator Server

If a WebNavigator Client and a WinCC client access the WebNavigator Server, via terminal services in the former case, the WebNavigator Client, as a terminal client, may not open a Windows Desktop in its session.

The following options are available to ensure the Windows desktop is not opened on the WebNavigator Client when beginning a session:

- Direct entry in the terminal services configuration for all users.
- Enter Internet Explorer as the start program in computer management for individual users.

For more information, refer to the FAQs on the Internet, contribution ID 17498344.

6.6.2 Activating terminal services on the Windows server (RT Professional)

Requirement

- Windows user with administrator rights
- Windows 2008 Server, Windows Server 2012

Procedure

Proceed as follows to activate terminal services:

1. Open Control Panel and double-click "Software".
2. Open the "Add or Remove Programs" dialog and click "Add or Remove Windows Components". The "Windows Components Wizard" opens.
3. Activate "Terminal server" and "Terminal server licensing".
4. Click "Next". Follow the instructions.

Note

Activate the terminal services on the server PC before you install the actual applications. Install the applications on the server PC via the "Add or Remove Programs" dialog of the Control Panel. If you install the application via the Control Panel, the application can be configured for all users. Otherwise, the application can only be used for the user who installed the application.

6.6.3 Setting Up a User with Access Rights to the Terminal Server (RT Professional)

Requirements

The terminal server is installed.

Procedure

To set up a user for access to the terminal server, proceed as follows:

1. Go to "Control Panel > Administrative Tools > Computer Management > Local Users and Groups".
2. Select "New User" from the "Users" shortcut menu. The "New User" dialog is opened.
3. Click the "User" icon. Double-click the corresponding user. The user properties dialog opens.
4. Click the "Member of" tab. Click "Add". The "Select Group" dialog opens.
5. Add the group "Remote Desktop Users". Click "OK" to close all the open dialogs.
6. Check the membership of the new user in other groups. If required, add the user to a corresponding group to ensure that the user is assigned the necessary user rights.
7. Close "Computer Management".

6.6.4 Starting the Terminal Server Application on the Terminal Client (RT Professional)

Requirement

- The terminal service on the Windows server is started.
- A user is set up for access to the terminal server.

Procedure

To start an application on the terminal server from the terminal client, proceed as follows:

1. On the terminal client, from the Start menu select the menu command "Programs" > Accessories > Communication > Remote Desktop Connection". The "Remote Desktop Connection" dialog opens.
2. Enter the name of the terminal server.
3. Click the "Connect" button. Log on as the user who was created for access to the terminal server.

Result

The connection is now established. The desktop of the terminal server is displayed. On the terminal server, start an application, e.g. the Web Navigator Client via Internet Explorer.

6.7 Troubleshooting (RT Professional)

No Communication Between Web Navigator Server and Client

If a provider (participating proxy, firewall) has activated Content Filtering for an Internet connection, Web Navigator communication is no longer possible. With content filtering, only certain contents of HTML pages are permitted. The communication is directed via a defined port to a certain IP address, e.g. of the WinCC server.

- You have to deactivate Smart Filtering for the IP address of the Web Navigator Server - as there are no viruses or HTML contents on the WinCC Server, filtering is not useful in this case.
- If the customer uses SSL technology, the data is transferred in encrypted form. Smart Filtering for content is therefore not possible.

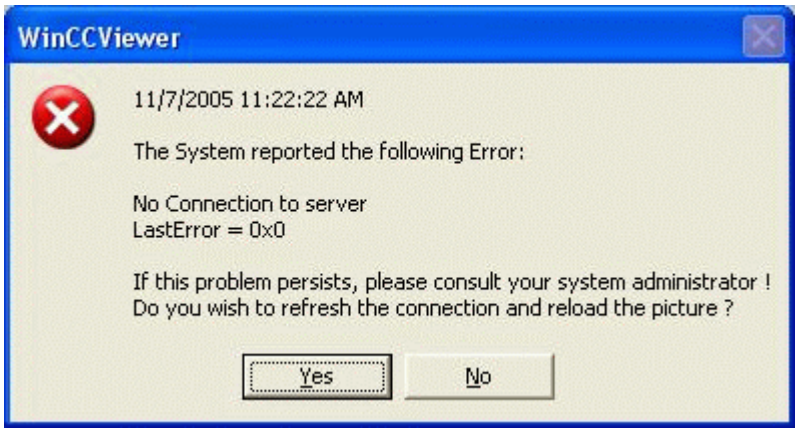
Connection Abort

In an Internet environment, aborted connections, delays and communication fluctuations may occur.

If the communication between the Web Navigator Client and Web Navigator Server is defect, the user receives an alarm on the Web Navigator Client.

The Web Navigator Client then automatically tries to establish a connection in order to restore the connection.

The delay between attempts to establish a connection can be configured with the Web Configurator. If the value "0" is set, the Web Navigator Client does not attempt to reconnect automatically. In this case a message appears on the web client asking you whether the connection is to be reestablished.



Confirm this query to reestablish the connection.

No Screens are Displayed

Make sure the correct Web site is activated on the PC running the Web Navigator Server.

Wrong Start Screen

You have edited a new screen in the "Screens" editor.

- Compile and load the screen on the server PC.
- Delete the temporary Internet files in the Internet Explorer via "Tools" > "Internet Options".

Index

A

Acknowledgement
  Audit Trail, 40
Activating, 281
  Project, 281
Additional tasks
  Runtime settings, 274
Alarm report
  Configuring, 28
Alarm Table
  Display Alarms, 123
Alarms
  Column names, 125
  Display in the alarm table, 123
  Hit list, 127
Alarms and Trends
  Displaying values in a table, 119
  Displaying values in a trend view, 121
Application Health Check, 151, 175
Audit
  Configuration, 51
  Enhancements in the ES, 13
  Forcing, 36
  Functional scope, 12
  Logging concept, 13
  Scope of logging, 14
  Screen object, 52
  Supported HMI devices, 51
Audit Trail
  Acknowledgement, 40
  Checksum, 34
  Comments, 40
  CSV file, 33
  Editor, 16
  Effects in runtime, 37
  Electronic signature, 40
  File format, 33
  Log tag value change, 37
  Logging recipe data changes, 40
  Logging system functions, 46
  Logging user actions, 43
  Memory medium, 35
  Printing, 25
  Protection against change, 36
  Reporting, 25
  Storage location, 35
  Troubleshooting, 35
Audit trail editor, 16

C

CCTMTimeSync.exe, 274
  Startup list, 274
Certificate, 250
  Importing on HTTP client, 250
  Installing on devices, 250
  Installing under Windows XP, 250
Checksum, 36
  Audit Trail, 34
  Log, 34
Client
  Deactivating a server project, 282
  Enabled remote server project, 281
  Shutdown, 270
  Startup, 270
Client/server
  Runtime settings, 263, 265
Client/server system
  Characteristics in Runtime, 267
  Response in Runtime, 268
  Shutting down the client, 270
  Shutting down the server, 270
  Starting up the client, 270
  Starting up the server, 269
Clients, 156
Comments
  Audit Trail, 40
  Electronic signature, 40
Company level, 156
Configuration, 156, 159
  Remote, 279
  WebNavigator, 287
Connection
  Connecting to server, 95
  Establishing connection to the server, 95
CSV file
  Audit Trail, 33

D

Data Monitor
  Runtime settings, 76, 312
DataMonitor, 53
  General operation, 86
  Log off from server, 87

Start Page, 84
Starting the Client, 84
WebCenter, 54
DataMonitor client
Installing, 64
License, 60
Start, 84
DataMonitor server
Installing, 62
License, 60
Logging off from,
Distributed operator stations
Configure SmartClient, 224
Configure SmartServer, 224
configuring, 224
Distributed system
Remote configuration, 279

E

Effects in runtime
Audit Trail, 37
Recipe data change,
Value changes to GMP-relevant tags,
Electronic signature, 12
E-Mail
Setting at the HMI device, 191
E-mail attachment
Report, 143
E-mail notification, 228
Configuring, 230
Setting up the trigger, 229
Event
Free space critically low, 24
Low free storage space, 24
Excel Workbook Assistant, 130
Excel Workbook Wizard, 130, 140
Excel Workbooks, 57
Alarm Attributes,
VBA functions,

F

FDA, 11
File format
Audit Trail, 33
Firewall
Under Windows, 81, 323
Forcing
Audit, 36
Free space critically low, 24
Function
Unsupported functions, 285

G

Gadget, 74, 75, 310, 311
GetValue, 254
GMP, 11
GMP settings, 38, 42
GMP-relevant tag, 38
Good Manufacturing Process, 11

H

Hardware
Requirement, 291
Hardware acceleration
SmartServer, 214
Header
Hide, 87
Show, 87
Hit List of Alarms, 127
HTML page
Displaying data type DATETIME, 233
HTTP client, 248
Configure HTTP-Connection, 248
Configuring tags, 249
Configuring the SIMATIC HMI HTTP protocol, 248
Importing certificates, 250
HTTP server
Configure WinCC-Project, 246
Setting at the HMI device, 247

I

IIS, (See Internet Information Service)
Input area plan
SmartClient, 191
SmartServer, 191
SmartService, 191
Installation
Internet Information Service, 296, 297
Requirement, 291, 294
Security settings, 302
Web diagnostics client, 307
WebNavigator Client, 299, 302, 305, 306
WebNavigator Server, 297
Installing
DataMonitor client, 64
DataMonitor server, 62

Internet Explorer
Security settings, 83, 302
Internet Information Service, 296, 297

L

Layout template
Create, 106
License, 293
DataMonitor client, 60
DataMonitor server, 60
Invalid, 61
Web diagnostics client, 293
Web diagnostics server, 293
Log memory, 171, 172
Log tag value change
Audit Trail, 37
Logging
Change to a recipe data record in Audit Trail, 40
System functions in Audit Trail, 46
Tag value change in Audit Trail, 37
User actions in audit trail, 43
Logging concept
Audit, 13
Logging recipe data changes
Audit Trail, 40
Logging system functions
Audit Trail, 46
Logging user actions
Audit Trail, 43
Low free storage space, 24

M

Memory medium
Audit Trail, 35
Monitoring mode, 203

N

Navigation interface
Extending menus, 330
Server change, 330
Structure, 329
User logon, 330
Network, 280
Access to subnetworks, 280
Router, 280
NotifyUserAction, 45

P

Password
SmartServer, 214
PDF file, 58
Permitted data type
SIMATIC HMI HTTP Protocol, 245
Port
Setting, 319, 321
Print alarm
Configuring print parameters, 28
Printing
Audit Trail, 25
Process control level, 156
Process level, 156
Process value
Displaying Statistics Function, 128
Project, 156
Activating, 281
Deactivating, 282
Operating with WinCC WebNavigator client, 328

R

Recipe
GMP settings, 42
Recipe data record change
Effects in Runtime, 42
Redundancy, 151, 156
Application Health Check, 151, 175
Log synchronization, 154
Principle of operation, 152
Recipe data, 159
Serial connection between servers, 170
System alarms, 171
Remote configuration, 279
Activating a project, 281
Deactivating a project, 282
Remote control
By means of Internet Explorer, 217
By means of SmartClient application, 218
Configure SmartClient, 208
Configure SmartServer, 204
Devices with keys,
Direct keys, 221
Monitoring mode, 203
Session Management, 203
Smart Options, 216
SmartClient display, 220

Remote monitoring
Smart Options, 216
Reporting
Audit Trail, 25
Reports, 58, 143, 145, 148
As e-mail, 143
Excel workbook, 145
PDF file, 58
PDF Report, 143
Print job, 148
Settings, 143
XLS file, 58
Requirement
Hardware, 291
Installation, 291
Operating system, 291
Software, 291
Rights
Access rights, 59
Access rights to directories, 94
User Rights, 59
Router, 280
Runtime, 267, 268
Alarms, 267
Graphics, 267
Logs, 267
Reaction to system errors, 267
Reports, 267
Response to system errors, 268
Scripts, 267, 268
System characteristics, 267
Text library, 267
User administration, 267
Runtime Professional
Setting up the startup list, 274
Runtime settings, 188
Additional tasks, 274
Client/server, 263, 265
Data Monitor, 76, 312
Start sequence, 274

S

Scenario, 170
Screen
Configuring, 310
Preview, 74, 75, 310, 311
Web access, 73, 310
Security settings
Internet Explorer, 83
Server, 156
Activating a project from client, 281
Deactivating a project from client, 282
Shutdown, 270
Startup, 269
Service-pages, 234
Create own, 241
Display, 237
remote control, 237
Transfer, 242
Session
Closing, 87
Session Management, 203
Setting, 204
Set the services
SmartClient, 188
SmartServer, 188
Setting at the HMI device
E-Mail, 191
HTTP server, 247
Setting at the HMI-device
HTTP server, 193
SmartServer, 194
Web authorization, 193
Web server, 193
SetValue, 254
Shutdown, 270
Of the client, 270
Of the server, 270
Shutting down, 270
Of the client, 270
Of the server, 270
signature
electronic, 12
SIMATIC HMI HTTP Protocol
Configuring HTTP clients, 248
Configuring the connection, 248
Permitted data type, 245
SIMATIC Shell, 279, 280
Smart Options, 216
HMI devices suitable for use, 187
Remote control, 216
Remote control by means of Internet Explorer, 217
Remote monitoring, 216
SmartAccess
Distributed operator stations, 224
Editing tag values in MS Excel, 254
SmartClient
Monitoring mode, 208
Password input, 221
SmartClient display, 208
SmartClient display, 220

SmartServer
As a service, 207
Control mode, 204
Forced access, 207
Hardware acceleration, 214
Local operator control, 207
Monitoring mode, 204
Password, 214
Password input, 221
Setting at the HMI-device, 194
SmartService
E-mail notification, 228
Input area plan, 191
Remote control by means of the SmartClient application, 218
SOAP
Access from Excel, 253
GetValue, 254
SetValue, 254
Windows CE, 254
Software
Requirement, 291
Standard Web site, 319, 321
Start sequence
Runtime settings, 274
Startup, 269, 270
Of the client, 270
Of the server, 269
Start-up behavior, 270
Start-up characteristics, 269
Of the client, 270
Of the server, 269
Startup list, 274
Statistics function
Displaying for process values, 128
Storage location
Audit Trail, 35
Synchronization of variables, 154
System characteristics, 267
System error, 268
System errors, 267
System function
NotifyUserAction, 45
System messages, 180
System response, 268

T

Tag
GMP settings, 38
GMP-relevant tag, 38
Terminal service, 294
Terminal services, 335
activate, 335
Creating users, 336
WebNavigator Client, 335
Time synchronization, 274
Trends and Alarms, 57, (See Trends and Alarms)
Alarm Table, 123
Analysis function, 127, 128
Display Alarms, 123
Hit List of Alarms, 127
Message Column Names, 125

U

User administration
WebCenter, 90
User group, 90
Individual groups, 82
User interface language
Switching, 87

V

Value changes to GMP-relevant tags
Effects in Runtime, 40

W

Web access
WebNavigator, 75, 312
Web authorization, 202
Setting at the HMI-device, 193
Web Client, (See WebNavigator Client)
Web Configurator
Creating a standard Web site, 319, 321
Setting a firewall, 81, 323
Setting a port, 319, 321
Web diagnostics client
Installation, 307
Web Part, 112
Delete, 117
Export, 117
insert in WebCenter page,
Minimize, 117
Moving, 117
Web server, 232
Configure WinCC-Project, 236
Service-pages, 234
User administration, 201
Web authorization, 201, 202

WebCenter, 54
Access rights to directories, 94
Create a WebCenter page, 109
Layout template, 106
Static process screens, 103
Template file, 106
User administration, 90
WebCenter page
Create, 109
Creating directory, 93
Inserting web parts, 112
Template file, 106
WebNavigator
Configuring, 309
Functions, 285
Installation requirements, 291
Licenses, 293
Publishing screens, 79, 316
Runtime settings, 75, 312
Terminal services, 290
Transferring the project, 79, 316
WebNavigator Client, 291, 305, 306
Installation, 299
Installation under the Windows Server, 299
Licenses, 293
Navigation interface,
Operating projects, 328
WebNavigator diagnostics client, 291
WebNavigator Server, 291
Installation, 297
Licenses, 293
WinCC DataMonitor, (See DataMonitor)
WinCC projects, 279
Activating remote, 281
Calling, 269
Remote deactivating, 282
WinCC Runtime Advanced Internet, 190
WinCC tag @RM_MASTER, 170
WinCC tag @RM_MASTER_NAME, 170
WinCCViewerRT, 54, 289
Displaying screens, 54, 89, 289
Monitoring projects, 327
Setting up, 87, 325

X

XML file
Create, 131
Storage location, 131