

SIMATIC HMI

WinCC V8.1 WinCC/Connectivity Pack

System Manual

Print of the Online Help

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 Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	WinCC V8.1 Installation / Release Notes	7
1.1	WinCC Installation Notes	7
1.1.1	WinCC installation instructions	7
1.1.2	Scope of delivery	7
1.1.3	SIMATIC WinCC: Product compatibility and supported functions	9
1.1.4	Licenses and Licensing	10
1.1.5	Activating and testing ASIA licenses	13
1.1.6	WinCC installation requirements	16
1.1.6.1	WinCC Installation Requirements	16
1.1.6.2	Hardware requirements for installing WinCC	17
1.1.6.3	Software requirements for installing WinCC	19
1.1.6.4	Microsoft SQL Server for WinCC	23
1.1.6.5	Notes on Data and System Security	25
1.1.6.6	Access rights in the operating system	29
1.1.6.7	How to Adapt the Windows Security Policies	35
1.1.7	Installing WinCC	35
1.1.7.1	Installing WinCC	35
1.1.7.2	How to install WinCC	36
1.1.7.3	How to Install Supplementary Components Later	44
1.1.7.4	How to Install Supplementary Languages	45
1.1.7.5	Configure automatic installation of WinCC	45
1.1.8	Uninstalling WinCC	48
1.1.9	Upgrading WinCC	50
1.1.9.1	Upgrading WinCC	50
1.1.9.2	How to Perform an Upgrade Installation	51
1.1.10	Overview: Notes on operation	53
1.2	WinCC Release Notes	55
1.2.1	Release Notes	55
1.2.2	Notes on operation	55
1.2.2.1	Notes on operation	55
1.2.2.2	Information on the Microsoft Windows operating system	57
1.2.2.3	Information on the database system	62
1.2.2.4	Information on network technology and UPS	63
1.2.3	Notes on WinCC	68
1.2.3.1	General information on WinCC and configurations	68
1.2.3.2	Information on WinCC CS	73
1.2.3.3	Information on WinCC runtime	75
1.2.3.4	Information on Smart tools	77
1.2.3.5	Information on process communication	78
1.2.3.6	Remote access and Remote Desktop Protocol (RDP)	81
1.2.3.7	Ports and protocols	84
1.2.4	Notes on WinCC Redundancy	86
1.2.5	Notes on Process Control Options	87
1.3	WinCC/Connectivity Pack Installation Notes	90
1.3.1	Connectivity Pack licensing	90

1.3.2	Installation of the Connectivity Pack Server	90
1.3.3	Installation of the Connectivity Pack Client	92
1.4	WinCC/Connectivity Pack Release Notes	93
1.4.1	Information on the Connectivity Pack	93
1.5	WinCC/DataMonitor Installation Notes	94
1.5.1	Requirements of installing DataMonitor	94
1.5.2	User rights for installing the DataMonitor client	96
1.5.3	Installing DataMonitor	97
1.5.4	DataMonitor licensing	100
1.5.5	Setting up a secure connection over HTTPS	102
1.6	WinCC/DataMonitor Release Notes	104
1.6.1	Notes about DataMonitor	104
1.7	WinCC/WebNavigator Installation Notes	107
1.7.1	General information on the WebNavigator installation	107
1.7.2	WebNavigator installation requirements	107
1.7.2.1	Hardware and software requirements for WebNavigator	107
1.7.2.2	Licensing WebNavigator	110
1.7.2.3	Requirements for the Use of Terminal Services	112
1.7.3	Installing a WebNavigator server	113
1.7.3.1	Overview: Installing the WebNavigator server	113
1.7.3.2	Installing the WebNavigator server	114
1.7.3.3	Setting up a secure connection over HTTPS	115
1.7.4	Installing the WebNavigator client	117
1.7.4.1	Installing the WebNavigator client	117
1.7.4.2	User rights and user groups for WebNavigator clients	120
1.7.4.3	Settings in the web browser (WebNavigator client)	122
1.7.4.4	Installation from the DVD (WebNavigator client)	123
1.7.4.5	Installation via the Intranet/Internet (WebNavigator client)	123
1.7.5	Installing the WebNavigator diagnostics client	125
1.7.6	WebNavigator Demo Project	126
1.7.7	Uninstalling the WebNavigator	126
1.8	WinCC/WebNavigator Release Notes	128
1.8.1	General information about WebNavigator	128
1.8.2	Notes on WebNavigator installation	131
1.8.3	General notes on WebNavigator client	133
1.8.4	Notes on Internet Explorer for WebNavigator	136
1.9	WinCC/WebUX	138
1.9.1	WebUX licensing	138
1.9.2	Installation of WebUX	140
1.9.3	Configuring the WebUX website	142
1.9.4	Communication: SSL certificate for HTTPS connections	143
1.10	Service and Support	146
1.10.1	Warnings	146
1.10.2	GDPR - General Data Protection Regulations	148
1.10.3	Customer support	150
1.10.4	Support request	152
2	WinCC/Connectivity Pack documentation	155
2.1	WinCC/Connectivity Pack	155

2.2	Overview: WinCC/Connectivity Pack	156
2.3	Applications.....	161
2.3.1	Use Case 1: Local Access to WinCC RT Databases.....	161
2.3.2	Use Case 2: Remote Access to WinCC RT Databases.....	162
2.3.3	Use Case 3: Local Access to WinCC Archive Databases.....	163
2.3.4	Use Case 4: Remote Access to WinCC Archive Databases	164
2.3.5	Use Case 5: Local Access to WinCC User Archive.....	165
2.3.6	Use Case 6: Remote Access to WinCC User Archives	166
2.3.7	Use Case 7: Access Via the WinCC OLE DB Provider	167
2.3.8	Access Using OPC to WinCC Archives, Tags, and Messages.....	168
2.3.9	Transparent access to archived data.....	169
2.3.10	Functions of SQL Servers.....	171
2.4	Access Via the OLE DB Provider.....	173
2.4.1	Access to Archive Data Using OLE DB Provider.....	173
2.4.2	Bases of OLE DB	174
2.4.3	WinCC Archive Connector.....	175
2.4.4	Establishing the Connection to the Archive Database.....	179
2.4.5	Querying the Archive Data	181
2.4.5.1	Displaying Process Value Archives.....	181
2.4.5.2	Querying the Archive Data	183
2.4.5.3	Querying Process Value Archives	184
2.4.5.4	Querying Alarm Message Archives.....	192
2.4.5.5	Displaying Alarm Message Archives	194
2.4.5.6	Query for User Archives.....	196
2.4.5.7	Displaying User Archives	198
2.4.5.8	Configure Access via the Wizard "SQL Server Import/Export"	199
2.4.5.9	Meeting prerequisites for using the Reporting Services	201
2.4.6	Analysis Functions for Messages and Process Values	202
2.4.6.1	Analysis Functions for Messages and Process Values	202
2.4.6.2	Display of Message Archives for Analysis Queries.....	206
2.5	Security Settings During Access to SQL Databases Using MS OLE DB.....	208
2.6	Access via OPC - Open Connectivity	209
2.6.1	OPC Channel.....	209
2.6.1.1	WinCC OPC Channel.....	209
2.6.1.2	OPC Item Manager	210
2.6.1.3	Overview of the Supported WinCC Data Types	213
2.6.1.4	WinCC OPC DA Client	214
2.6.2	OPC - Open Connectivity	230
2.6.2.1	OPC - Open Connectivity	230
2.6.2.2	Functionality of OPC	231
2.6.2.3	OPC specifications and compatibility.....	231
2.6.2.4	Using OPC in WinCC	232
2.6.2.5	How to configure Windows for the use of WinCC OPC	234
2.6.2.6	WinCC OPC DA server.....	235
2.6.2.7	WinCC OPC HDA server	253
2.6.2.8	WinCC OPC A&E Server	266
2.6.2.9	WinCC OPC UA Server	287
2.6.2.10	Diagnostics	317
2.7	Examples for Access Using OLE DB Provider	318

2.7.1	Examples for Access Using OLE DB Provider	318
2.7.2	Example: Configuring the Access to Archive Data Using VB.....	318
2.7.3	Example: Configuring Access to Archive Data Using DataConnector Wizard.....	320
2.7.4	Examples: Analyzing Process Value Archives	326
2.7.4.1	Example: Reading Process Value Archive With WinCC OLE DB Provider and Visual Basic 6 ...	326
2.7.4.2	Example: Reading Process Value Archive With WinCC OLE DB Provider and Visual Basic.NET...	332
2.7.5	Examples: Analyzing Alarm Message Archives.....	336
2.7.5.1	Example: Reading Message Archive Data with the WinCC OLE DB Provider and Visual Basic 6	336
2.7.5.2	Example: Reading Message Archive Data With WinCC OLE DB Provider and Visual Basic.NET.....	340
2.8	Connectivity Station.....	344
2.8.1	Basics of the Connectivity Station	344
2.8.2	Functionality of the Connectivity Station	346
2.8.2.1	Use of OPC interface of the Connectivity Station.....	346
2.8.2.2	Use of OLE DB interface of the Connectivity Station	347
2.8.3	Configuring the Connectivity Station in the S7 project	349
2.8.4	Accessing WinCC data with the Connectivity Station	351
2.9	Connectivity Station for OPC UA	353
2.9.1	Basic information on Connectivity Station for OPC UA.....	353
2.9.2	Using the OPC UA interface of the Connectivity Station.....	355
2.9.3	Configuring Connectivity Station in S7 Project (OPC UA).....	356
2.9.4	Accessing WinCC data with the Connectivity Station (OPC UA)	357
Index		359

WinCC V8.1 Installation / Release Notes

1.1 WinCC Installation Notes

1.1.1 WinCC installation instructions

Contents

This documentation contains important information on the scope of delivery, as well as on the installation and operation of WinCC.

The information contained here takes precedence over the information contained in the manual and online help.

1.1.2 Scope of delivery

Components supplied

WinCC V8.1 is available as a basic package or upgrade package and as a download package "OSD" (Online Software Delivery).

1.1 WinCC Installation Notes

You will receive the following components:

Components ^{1) 2)}	Basic / Upgrade / Download Package
WinCC V8.1 DVD: - WinCC V8.1 - WinCC/WebUX - WinCC/WebNavigator - WinCC/DataMonitor - WinCC/Connectivity Pack - WinCC/Connectivity Station - Microsoft SQL Server 2022 for WinCC V8.1 - SIMATIC Logon V2.0 ^{3) 4)} - Automation License Manager V6.2 Update 2 - AS-OS-Engineering V10.0	X
Additional Content DVD: - SQL Server Management Studio - Visual C++ Redistributable for Visual Studio: 2005 / 2008 / 2010 / 2012 - WinCC V8.1 – Printable online help (PDF files)	X
Required licenses	X
Certificate of License	X

1) Refer to the software requirements in the installation and release notes.

2) If you use the "SIMATIC S7-1200, S7-1500 Channel" with more than 10 connections, you need a SIMATIC NET license, e.g. "SIMATIC NET - SOFTNET-IE S7 Power Pack V19".

3) If you install SIMATIC Logon, a computer restart may be necessary.

4) Use at least SIMATIC Logon V2.0.

Note

Printing installation notes

The installation notes for the respective products are also provided as a PDF file.

You can find the installation and release notes on the WinCC DVD in the "Install_and_Release-Notes" folder.

You need at least Adobe Acrobat Reader V5.0. You can download the Adobe Acrobat Reader free of charge from the following URL:

- <http://www.adobe.com/products/acrobat>

Communication drivers

The communication drivers included in the package do not need an additional license:

- Allen Bradley - Ethernet IP
- Mitsubishi Ethernet

- Modbus TCP/IP
- Omron Ethernet-IP
- OPC
- OPC UA WinCC Channel ¹⁾
- PROFIBUS DP
- SIMATIC 505 TCP/IP
- SIMATIC S5 Ethernet Layer 4
- SIMATIC S5 Profibus FDL
- SIMATIC S5 Programmers Port AS511
- SIMATIC S5 Serial 3964R
- SIMATIC S7 Protocol Suite (SIMATIC S7-400)
- SIMATIC S7-1200, S7-1500 Channel
- SIMATIC TI Ethernet Layer 4
- SIMATIC TI Serial
- Simotion
- SinumerikNC (SINUMERIK, SIMATIC S7-300)
- System Info
- WinCC Unified Channel ¹⁾
- Alarm Channel (Alarm Logging)

1) You need a Connectivity Pack license for the WinCC OPC UA server.

2) You need a Connectivity Pack license for the "WinCC Unified Channel". In WinCC Unified, the station requires a Unified Collaboration license.

See also

Information on WinCC CS (Page 73)

<http://www.adobe.com/products/acrobat> (<http://www.adobe.com/products/acrobat>)

1.1.3 SIMATIC WinCC: Product compatibility and supported functions

To use the software with other SIMATIC products you must ensure that the product versions match and support the required functions.

- You determine the version compatibility with the compatibility tool.
- Note the additional information on the individual products and functions.

WinCC versions in distributed systems

The same WinCC version must be installed on all WinCC stations used in the WinCC system.

1.1 WinCC Installation Notes

These include, for example:

- WinCC servers, redundant servers, archive servers, file servers
- WinCC clients with their own project, WinCC clients without their own project
- PCs on which WinCC options are installed, e.g. WebNavigator server, WebNavigator client, WinCC/Audit, WinCC/Calendar Options

Mixed configurations with different WinCC versions on servers, clients or PCs with WinCC options are not released.

Always install WinCC updates on all PCs in the WinCC system. If different update versions are installed on the clients or servers, no configuration changes are possible in the WinCC project, for example.

SIMATIC Process Historian

Check which functionality is supported by the SIMATIC Process Historian version that is used in each case.

For more information, refer to the documentation for the SIMATIC Process Historian.

Installing PH-Ready / IS-Ready

You install "PH-Ready" and "IS-Ready" from the "Process Historian / Information Server" DVD.

Compatibility tool

With the compatibility tool, Industry Online Support gives you a function you can use to put together a compatible selection of software products or to check existing configurations for compatibility.

In entry 64847781 you can access the compatibility tool and find additional information on how to use the tool:

- SiePortal: Compatibility tool for automation and drives (<https://support.industry.siemens.com/cs/ww/en/view/64847781>)

1.1.4 Licenses and Licensing

Introduction

The WinCC software is protected, and can only be used in its full measure with a valid license.

Each installed software and option used requires a valid license for unrestricted operation of WinCC. The licenses for optional packages must be ordered separately.

You will receive the necessary license keys for installing the licenses as follows:

- As storage medium with license keys
- Via the internet (online software delivery)

When you install a license, it is transferred to a local drive and checked out on the storage medium so that WinCC can use this license.

Note**Microsoft Corporation: License agreement**

The licensee is still required to confirm that the software (SW) contains licensed software by Microsoft Corporation or its subsidiaries.

The licensee hereby agrees to be bound by the terms and conditions of the appended license agreement between Microsoft SQL Server and end user, and to fulfill the same.

Notes on license conditions

Observe the enclosed license conditions, which are also displayed during installation.

You need V8.1 licenses for WinCC V8.1.

The SIMATIC WinCC software is copy-protected against unlicensed use.

More information on licenses and license types:

- "Activating and testing ASIA licenses (Page 13)"
- WinCC Information System:
 - "Licensing > Overview of the licensing"
 - "Licensing > Basic license types and license types in WinCC"

Installed licenses are required to enable proper operation of WinCC. If WinCC is installed without licenses, the program will switch to demo mode at start-up.

Note**Process mode only with a valid license**

It is not allowed to run WinCC in process mode without a valid license.

Cumulating licenses

The cumulation of more than one license per component subject to license is only possible for the following licenses or licenses for the following options:

- WinCC Archive licenses
- WinCC/DataMonitor
- WinCC/WebNavigator
- WinCC/WebUX
- WinCC/IndustrialDataBridge
- WinCC/PerformanceMonitor
- SIMATIC Information Server

Other licenses cannot be cumulated.

1.1 WinCC Installation Notes

Demo mode

If a license is missing for one or multiple components, WinCC will run in demo mode.

WinCC also switches to demo mode when the maximum authorized number of process tags or archive tags is exceeded in a project.

To exit WinCC demo mode, install the required licenses.

Behavior in Runtime

In demo mode, you can use the WinCC software fully for a maximum of one hour. After this period, the operation of WinCC violates the license agreements.

After one hour, the WinCC Explorer and the editors will be closed.

In Runtime, the system will request the acquisition of a valid license. This dialog will appear every 10 minutes.

Details on the demo mode in the WinCC Information System:

- "Licensing > WinCC in the Demo Mode"

Microsoft SQL Server 2022

A license is necessary to use the Microsoft SQL Server database. This license is readily available if WinCC is licensed and properly installed.

The SQL Server licensed with the WinCC installation may only be used in conjunction with WinCC.

Its use for other purposes requires an additional license. These may include:

- Use for internal databases
- Use in third-party applications
- Use of SQL access mechanisms that are not available via WinCC

Uninstalling

After uninstalling WinCC, you must also uninstall the "WinCC" Microsoft SQL Server instance:

Under "Control Panel" > "Software", select the "Microsoft SQL Server 2022" entry to uninstall.

Installing licenses

You can use the Automation License Manager to install licenses.

Licenses can be installed during installation of WinCC or at a later time. You can find the Automation License Manager in the Microsoft Windows Start menu in the "Siemens Automation" program group. After-the-fact installation of a license will take effect upon restart of your computer.

The following requirements must be met for installing licenses:

- The storage medium containing the licenses must not be write-protected.
- You can install the RC licenses on a license server for the configuration. You do not have to install the licenses on the local drive.
- Licenses may only be installed on an uncompressed drive.

Note**Uninstalling WinCC: Licenses remain installed**

After uninstalling WinCC, the licenses remain installed on the system.

Note**Installing licenses before WinCC starts**

Install all required licenses before you start WinCC.

If one of the required licenses is missing, WinCC switches to demo mode when the program starts.

See also

Activating and testing ASIA licenses (Page 13)

1.1.5 Activating and testing ASIA licenses

Overview

The license keys for WinCC Runtime and WinCC RC (Runtime and Configuration) are provided on the supplied license storage medium "License Key USB Hardlock".

The licensed ASIA version is executable in parallel to the European version by switching to Unicode.

The "License Key USB Hardlock" (dongle) checks the following conditions:

- WinCC GUI language
- Runtime language
- The Text Library contains an Asian language.
- Asian characters are used in the WinCC project.
- Operating system settings

You can find more information about installing the license under "Licenses and licensing".

Note

It is not allowed to run WinCC in process mode without a valid license.

Installed Languages

A newly created project receives all installed WinCC languages as project languages.

Delete configuration languages

If you do not have a license for an ASIA version and delete the Asian project languages in the text library, the WinCC project continues to run in demo mode.

To disable Demo mode, close the WinCC project. When reopened it is recognized that the WinCC project no longer requires licenses for an ASIA version.

Testing the validity of the licenses

If you start a correctly licensed WinCC version without a connected dongle, the following error message appears:



The same error message appears after a few minutes if you disconnect the dongle from the computer with a correctly licensed WinCC version.

If this error message does not appear, a non-licensed WinCC version is installed.

No right of usage for WinCC is available in this case. Uninstall this WinCC version and obtain a legally licensed version of WinCC V8.

If necessary, contact WinCC Support and provide the serial number of your software version:

- <http://www.automation.siemens.com/partner/index.asp> (<http://www.automation.siemens.com/partner/index.asp>)

You can find the serial number on the "Certificate of License" (CoL).

Working with the "License Key USB Hardlock"

Please note the following:

- Do not edit data on the "License Key USB Hardlock".
The actions not allowed include:
 - Rename data
 - Delete data
 - Copy data to the "License Key USB Hardlock"
- Do not format the "License Key USB Hardlock".
- Do not remove the "License Key USB Hardlock" from the PC while WinCC is running.

NOTICE
Do not remove the "License Key USB Hardlock" dongle If you remove the dongle from the computer, an error message is generated and WinCC switches to Demo mode. If you re-connect the dongle to the computer, the error message disappears and Demo mode is disabled. WinCC works once again in licensed mode.

See also

Licenses and Licensing (Page 10)

<http://www.automation.siemens.com/partner/index.asp> (<http://www.automation.siemens.com/partner/index.asp>)

1.1.6 WinCC installation requirements

1.1.6.1 WinCC Installation Requirements

Introduction

You will need special hardware and software for the installation of WinCC. The requirements are described in the chapters "Hardware Requirements for Installation" and "Software Requirements for Installation".

Note

Microsoft Windows operating system: Avoid changes in system

Microsoft Windows settings deviating from default can have an effect on operation of WinCC.

Observe this note particularly for the following changes:

- Change of processes and services in Control Panel.
 - Changes in Microsoft Windows Task Manager.
 - Changes in Microsoft Windows registry.
 - Changes in Microsoft Windows security policies.
-

The first check if certain conditions are met is already executed during the installation of WinCC. The following conditions are checked:

- Operating system
- User rights
- Graphic Resolution
- Internet Explorer
- MS Message Queuing
- Due Complete Restart (Cold Restart)

Error Messages

If one these conditions is not met, the WinCC installation will be aborted and an error message will be displayed. For details about the error messages displayed see the table below.

Error Message	Explanation
To execute installation properly, restart the computer	The software installed on your computer requires a restart. Before WinCC can be installed, the computer should be restarted once.
This application requires VGA or any higher resolution	Check the settings of the connected monitor and upgrade the graphic card, if necessary.
You do not have administrator rights. Log on as administrator.	Administrator rights are required for the installation. Log in to Microsoft Windows again as a user with administrator rights.

Error Message	Explanation
Setup has detected that unInstallShield is active. Please close unInstallShield and restart Setup.	Close unInstallShield. This message may also indicate that you are lacking administrator rights for this installation. In this case, log on to Microsoft Windows again as a user with administrator rights.
The Microsoft Message Queuing services are not installed.	Install the Microsoft Message Queuing services. To do this, you will need the Microsoft Windows installation CD.

See also

Defining Access Rights in the Operating System (Page 29)

How to Adapt the Windows Security Policies (Page 35)

Notes on Data and System Security (Page 25)

Software requirements for installing WinCC (Page 19)

Hardware requirements for installing WinCC (Page 17)

Microsoft SQL Server for WinCC (Page 23)

1.1.6.2 Hardware requirements for installing WinCC

Introduction

Certain hardware configuration conditions must be fulfilled for installation.

Hardware requirements

WinCC supports all common IBM/AT-compatible PC platforms.

To work efficiently with WinCC, select a system with the recommended specifications.

Note

Unless noted to the contrary, the same requirements as for servers are applicable to single-user systems.

		Minimum	Recommended
CPU	Microsoft Windows 10 / Microsoft Windows 11 (64-bit)	Dual-core CPU Client/single-user system 2.5 GHz	Multi-core CPU Client: 2.7 GHz Single-user system: 2.7 GHz
	Microsoft Windows Server 2019 / Microsoft Windows Server 2022	Dual-core CPU Client/single-user system server: 2.5 GHz	Multi-core CPU Single-user system/server: 3.5 GHz

1.1 WinCC Installation Notes

		Minimum	Recommended
Work memory	Microsoft Windows 10 / Microsoft Windows 11 (64-bit)	Client: 2 GB Single-user system: 4 GB	8 GB
	Microsoft Windows Server 2019 / Microsoft Windows Server 2022	4 GB	16 GB
Free disc space on the hard drive - For installing WinCC - For working with WinCC ^{1) 2)}		Installation: • Client: 1.5 GB • Server: > 1.5 GB Working with WinCC: • Client: 1.5 GB • Server: 2 GB	Installation: • Client: > 1.5 GB • Server: 2 GB Working with WinCC: • Client: > 1.5 GB • Server: 10 GB Archive databases may require additional disc space.
Virtual work memory ³⁾		The size of the swap file depends on the memory configuration of the PC. Recommended setting: • "Swap file is managed automatically"	
Color depth/ color quality		256	Highest (32-bit)
Resolution		800 * 600	1920 * 1080 (full HD)

1) Depending on project size as well as size of archives and packages.

2) WinCC projects should not be stored on compressed drives or directories.

3) Virtual work memory: Check the applicable Microsoft requirements for the Microsoft Windows edition you are using.

The recommended value in the "Size of swap file for a specific drive" area is a guide for the "Total size of swap file for all drives". Enter the recommended value in both the "Start size" field and the "Maximum size" field.

More information: "SiePortal: Settings for the virtual work memory (FAQ entry 20440472) (<http://support.automation.siemens.com/WW/view/en/20440472>)".

Note

In the case of online configuration, the recommended requirements constitute the minimum requirement.

Virtualization

The following virtualization systems have been tested:

- Microsoft Hyper-V 2019 / 2022
- VMware ESXi 7.0 / 8.0 Update 2

Requirement

The performance data of the virtual computers must meet the minimum requirements for WinCC clients.

You can find more information on virtualized environments with WinCC in the following FAQ:

- SiePortal: Virtualization (FAQ entry 49368181) (<http://support.automation.siemens.com/WW/view/en/49368181>)

See also

Defining Access Rights in the Operating System (Page 29)

Notes on Data and System Security (Page 25)

Software requirements for installing WinCC (Page 19)

1.1.6.3 Software requirements for installing WinCC

Introduction

Certain requirements concerning operating system and software configuration must be met for the installation.

Note

WinCC in a domain or workgroup

WinCC is enabled for operation within a domain or workgroup.

Note however that domain group policies and restrictions in the domains may prevent installation. In this case, remove the computer from the domain before installing Microsoft Message Queuing, Microsoft SQL Server and WinCC. Log on to the computer concerned locally with administrator rights. Carry out the installation. Following successful installation, the WinCC computer can be registered in the domain again. If the domain-group policies and domain restrictions do not impair the installation, the computer must not be removed from the domain during installation.

Note however that domain group policies and restrictions in the domain may also hinder operation. If these restrictions cannot be overcome, operate the WinCC computer in a work group. If necessary, contact the domain administrator.

Operating systems

Operating system languages

WinCC is released for the following operating system languages only:

- German
- English
- French
- Italian
- Spanish
- Chinese (Simplified, PR China)

1.1 WinCC Installation Notes

- Chinese (Traditional, Taiwan)
- Japanese
- Korean
- Multilingual operating system (MUI version)

Configurations

When using more than one server, all servers must be operated with a uniform operating system:

Microsoft Windows Server 2019 or 2022, uniformly Standard or Datacenter edition in each case.

Single-user systems and clients

Operating system	Configuration	Comments
Microsoft Windows 10 ¹⁾	Pro Enterprise	Standard installation 64-bit If you are using SIMATIC NET, please refer to the information in the SIMATIC NET "Readme" file.
Microsoft Windows 10 ¹⁾	Enterprise LTSC (Long-Term Servicing Channel)	Standard installation 64-bit If you are using SIMATIC NET, please refer to the information in the SIMATIC NET "Readme" file.
Microsoft Windows 11 ¹⁾	Pro Enterprise	Standard installation 64-bit If you are using SIMATIC NET, please refer to the information in the SIMATIC NET "Readme" file.

1) The currently released build versions of Windows 10 or Windows 11 are listed in the compatibility tool.

You can also run single-user systems and clients in WinCC multi-user systems on Microsoft Windows Server 2019 / 2022.

WinCC server

Operating system	Configuration	Comments
Microsoft Windows Server 2019	Standard Datacenter	64-bit
Microsoft Windows Server 2022	Standard Datacenter	64-bit

WinCC server with up to three WinCC clients

It is also possible to operate a WinCC Runtime server on Microsoft Windows 10 or Microsoft Windows 11 if you are not running more than three clients.

WinCC ServiceMode is not released for this configuration.

Note**Only enable the terminal server for WinCC/WebNavigator**

WinCC is not suitable for use on a Microsoft terminal server.

You can use the Microsoft terminal server only in connection with the WinCC Web client. Note the installation instructions of the WinCC/WebNavigator.

Virus scanner

You can find information on the use of virus scanners as well as approved virus scanner versions in the WinCC Release Notes under "Notes on operation (Page 55)".

Microsoft Windows Patches / Updates: Compatibility with SIMATIC products

Note the latest information on compatibility of SIMATIC products with Microsoft patches and updates:

- SiePortal: FAQ 18752994 (<https://support.industry.siemens.com/cs/ww/en/view/18752994>)

Microsoft Windows computer name**Do not change the computer name**

Do not change the Windows computer name after installing WinCC installation.

Illegal characters

The following characters are not permitted in the computer name:

- . , ; ! ? " ' ^ ` ~ _
- + = / \ ! @ * # \$ % & § °
- () [] { } < >
- Space character

Note the following:

- Only uppercase relevant
- The first character must be a letter.

Microsoft Message Queuing services

WinCC requires Microsoft Message Queuing services.

During the WinCC installation, the corresponding services are installed and configured.

Internet Explorer - requirements

You can find the browser requirements for WinCC options in the respective installation notes for the option.

1.1 WinCC Installation Notes

You need Microsoft Internet Explorer to open the WinCC online help. Recommended versions:

- Microsoft Internet Explorer V11.0 (32-bit)

If you wish to fully use WinCC's HTML Help, you must permit the use of JavaScript under "Internet Options" in Internet Explorer.

Note

Do not disable Internet Explorer.

Operation with multiple network adapters

When a server is used with several network adapters, read the notes in the WinCC Information System under "Configurations > Distributed Systems > System behavior in Runtime > Special features of communication using a server with several network adapters".

Adapting security policies

The operating system must permit the installation of unsigned drivers and files.

Detailed information is available in the section "Adapting Security Policies under Windows".

Note

Operating system update

An update of the operating system is not permitted if WinCC is started.

Start the computer again after updating the operating system.

Checking the "Path" environment variable

Before starting WinCC, you should check the entries in the "Path" environment variable.

A few programs insert paths containing quotation marks in the environment variable. These paths can prevent WinCC from starting or limit its functionality. The paths with quotation marks can also interfere with the software of other manufacturers.

1. To open the "System properties" dialog, search for "Advanced system settings" in the Windows search window.
2. In the "Advanced" tab, click the "Environment variables" button.
3. Display the value of the "Path" system tag.

If the "Path" system variable contains paths with quotation marks, reorder the entries so that these paths are called last.

Microsoft Internet Information Service (IIS)

During the WinCC installation, the Microsoft Internet Information Service (IIS) is installed for the of the following components or options:

- WinCC/DataMonitor
- WinCC/WebNavigator
- WinCC/WebUX

See also

Notes on Data and System Security (Page 25)

Defining Access Rights in the Operating System (Page 29)

Installing WinCC (Page 35)

How to Adapt the Windows Security Policies (Page 35)

Hardware requirements for installing WinCC (Page 17)

Microsoft SQL Server for WinCC (Page 23)

Notes on operation (Page 55)

SiePortal: FAQ 18752994 (<https://support.industry.siemens.com/cs/ww/en/view/18752994>)

1.1.6.4 Microsoft SQL Server for WinCC

WinCC requires Microsoft SQL Server 2022 in the 64-bit version:

- Microsoft SQL Server 2022 64-bit Standard Edition
- Microsoft SQL Server 2022 64-bit Express Edition

SQL Server is included automatically in the WinCC installation.

Microsoft SQL Server 2022

Licensing

Read the information on licensing Microsoft SQL Server under "Licenses and licensing".

User rights

Appropriate user rights must be set up to access the Microsoft SQL Server data. For more information, refer to the section "Specifying access rights in the operating system (Page 29)".

Encrypted connection

To increase security, use encrypted communication.

1.1 WinCC Installation Notes

You can find information on this in the following Microsoft entries:

- Internet: "Server network configuration" (<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-network-configuration?view=sql-server-ver15>)
- Internet: "Configure SQL Server Database Engine for encrypting connections" (<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-sql-server-encryption?view=sql-server-ver15>)

Regional Settings: Disable "Unicode UTF-8" beta setting

To avoid conflicts when accessing the SQL server, disable the following option in the "Regional Settings" dialog:

- "Beta: Use Unicode UTF-8 for worldwide language support"

WinCC/Connectivity Pack

When you install WinCC/Connectivity Pack, the required connectivity components are installed along with the Microsoft SQL Server.

SQL server instance "WinCC"

During installation, a new "WinCC" instance with the required settings is created with Microsoft SQL Server.

This instance is always installed in English. The language in which existing SQL server instances have been installed has no effect on this. Existing instances are not affected by the Service Pack.

"WinCC" instance after removing WinCC

When WinCC is removed, the "WinCC" SQL server instance remains installed and must be removed manually for licensing reasons.

Installation of Microsoft SQL Server Express

Microsoft SQL Server Express is installed in the following cases:

- Installation of "WinCC client"
- Installation of the WinCC V8 demo version

Requirement for the installation of Microsoft SQL Server Express

The Microsoft Windows user name of the user performing the installation must not contain any space characters.

SQL Server Management Studio (SSMS)

The SQL Server Management Studio is no longer part of the SQL Server installation.

If you want to install SQL Server Management Studio, use the provided "Additional Content" DVD.

SQL Server port number

You can manually configure the port number for the Microsoft SQL Server communication.

You can find more information in the following Microsoft article:

- Internet: "Configure a Server to Listen on a Specific TCP Port" (<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port?view=sql-server-ver15>)

See also

Defining Access Rights in the Operating System (Page 29)

Software requirements for installing WinCC (Page 19)

Notes on Data and System Security (Page 25)

Ports and protocols (Page 84)

Internet: "Server network configuration" (<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-network-configuration?view=sql-server-ver15>)

Access rights in the operating system (Page 29)

Internet: "Configure a Server to Listen on a Specific TCP Port" (<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port?view=sql-server-ver15>)

Internet: "Configure SQL Server Database Engine for encrypting connections" (<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-sql-server-encryption?view=sql-server-ver15>)

1.1.6.5 Notes on Data and System Security

Introduction

System security when using WinCC can be increased by implementing simple measures.

You can find additional information in the "WinCC Release Notes > Notes on Operation > Information on the Microsoft Windows operating system (Page 57)".

You can find information on the remote access under "WinCC Release Notes > Notes on WinCC > Remote access and Remote Desktop Protocol (RDP) (Page 81)".

Information on write access for WinCC project folders can be found under "Access rights in the operating system > Defining Access Rights in the Operating System (Page 29)".

Activating WinCC remote communication

On WinCC systems, remote communication is disabled by default in the "SIMATIC Shell" dialog after the installation.

1.1 WinCC Installation Notes

For the following scenarios, you must activate the remote communication of the PCs involved:

- Client-server communication
- Redundant system
- WinCC option "WebNavigator"
If the WebNavigator client is not running on the same PC as the WebNavigator server, remote communication must be enabled.

To enable remote access, proceed as follows:

1. Open the communication settings using the context menu of SIMATIC Shell in Microsoft Windows Explorer.
2. Select the "Remote Communication" option.
3. Configure the encrypted communication in the network: Select the PSK key and the port.
4. Select the network adapter and, if required, the Multicast settings.

Firewall settings

To limit the incoming rule for the CCAgent or CCEServer, you can change the parameter "Remote address" from "Any" to "Local subnet".

You can edit the firewall rules in the "Windows Firewall with Advanced Security" dialog.

Preventing Access to the Operating System Layer in Runtime

If the Microsoft Windows Selection dialog is opened in an activated WinCC project, access to the Microsoft Windows operating system is possible using this function. A Microsoft Windows Selection dialog opens, for example, when data is imported or files are selected.

Protect the corresponding function by executing a Permission Check via the User Administrator to prevent unauthorized access to the operating system.

Preventing access to the Microsoft Windows toolbar

You can use the computer properties to prevent the Microsoft Windows taskbar from being displayed in runtime.

- Activate the "Disable keys" option under "Parameters" in the "Properties - Computer" area of the "Computer" editor.
This disables all shortcut keys for operating system access.
- Deactivate the "Automatically hide the taskbar" setting in Microsoft Windows.

Disabling shortcut keys

If you would like to disable shortcut keys, you must adapt the group policies in the operating system management.

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

- SiePortal: WinCC FAQ 44027453 (<http://support.automation.siemens.com/WW/view/en/44027453>)

Shortcut key <Ctrl+Esc>

If you disable the <Ctrl+Esc> shortcut key, the following shortcut keys are also disabled in runtime:

Shortcut keys	Function
<Windows key+U>	System utility program manager
Press <Shift> five times	Locking function
Press <Shift right> for eight seconds	Impact delay
<Alt left+Shift left+Num>	Keyboard mouse
<Alt left+Shift left+Print>	High contrast

Note**Microsoft Windows Control Panel**

These functions can be configured using the Microsoft Windows Control Panel.

If the functions are activated in the Control Panel before activating WinCC Runtime, they are no longer locked in runtime.

Suppressing Microsoft Windows notifications and alarms in Runtime (kiosk mode)

To prevent the display of Windows notifications and Windows alarms on a PC in Runtime, follow these steps:

1. Enter "Notifications and actions" in the search field of the Windows taskbar.
The settings for Microsoft Windows notifications and actions open.
2. Click "Notification wizard settings".
3. Enable the following settings in the notification wizard:
 - Enable the "Only alarms" option.
 - Under "Automatic rules", disable the "When I'm using an app in full-screen mode/Alarms only" option.

Disabling the Plug&Play services

If the Plug&Play service is enabled, an operating system message may occur in WinCC Runtime when scanning for drivers.

This allows access to the operating system.

Disable the "Plug&Play" service in the Microsoft Windows Services Manager. Activate the service only if you actually need access, for example, to a chip card reader.

Microsoft Windows event display: User administration

You can also find changes in the user administration via the User Administrator or the WinCC UserAdminControl as an entry in Microsoft Windows event display.

Integrity check of the installed WinCC files

With the integrity check tool, you can determine whether the files of your WinCC installation are unchanged and correspond to the delivery state.

The hash value and file signatures are checked, for example.

You can find the "SieSoftIntCheck.exe" tool in the following path:

- <Installation path>\WinCC\SmartTools\SiemensSoftwareIntegrityCheck

Open the tool in the Microsoft Windows window "Command prompt" (CMD).

The WinCC installation files are checked and the result is written into a log file.

Parameters

To display a list of available parameters, enter the following command:

- `SieSoftIntCheck.exe -?`

You can set the following parameters, for example:

- Storage location of the log files "SieSoftIntCheck_YYYY-MM-DD-hh-mm-ss_result.csv" and "SieSoftIntCheck_YYYY-MM-DD-hh-mm-ss_logfile.txt"
- Display of the hash and signature information
- Exception of files with low priority.

Checklist for technical implementation

You can find more information on configuring your system in the following document in the "Industry Online Support":

- WinCC Systems: Checklist for Technical Implementation

See also

Information on the Microsoft Windows operating system (Page 57)

Microsoft SQL Server for WinCC (Page 23)

Ports and protocols (Page 84)

Hardware requirements for installing WinCC (Page 17)

Software requirements for installing WinCC (Page 19)

Defining Access Rights in the Operating System (Page 29)

How to Adapt the Windows Security Policies (Page 35)

How to install WinCC (Page 36)

Notes on operation (Page 55)

Remote access and Remote Desktop Protocol (RDP) (Page 81)

SiePortal: WinCC FAQs (<http://support.automation.siemens.com/WW/view/en/10805583/133000>)

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

1.1.6.6 Access rights in the operating system

Defining Access Rights in the Operating System

Introduction

To support you in protecting your system, WinCC offers a structured user administration:

- Protect your system against unauthorized access.
- Assign each user the required rights.

In order to work with WinCC, certain folders can be enabled for access via the network. For security reasons, you should only assign access rights to these folders to authorized users. You manage access rights via the Microsoft Windows Standard user groups and user groups created by WinCC.

Access rights specified in WinCC

Following WinCC installation, WinCC automatically establishes the following local groups in Microsoft Windows User and Group Administration:

- "SIMATIC HMI"
All users must be members of the "SIMATIC HMI" user group. These members can create local projects, and can process, start, and access these projects remotely. Access to the WinCC database is limited to the minimum rights necessary (read/write). By default, the user who carries out the WinCC installation and the local administrator are members of this group. Additional members must be added manually by an administrator.
- "SIMATIC HMI Viewer"
These members have read access only to configuration and runtime data in the WinCC database. This group is primarily used for accounts for Web publication services, e.g. IIS (Internet Information Services) account for operation of WinCC WebNavigator.
- Access to folder "<Installation Directory>/WinCC/aplib"
Following installation, the directory "Installation Directory/WinCC/aplib" named "SCRIPTFACT" is unlocked for the "SIMATIC HMI" user group. This directory contains central libraries for project script functions.
- "RTIL Tracing User"
The user group is created during the installation of WinCC.
Users in this user group can connect the WinCC project to WinCC Unified via the WinCC Unified channel.

WinCC folder share

With access via folder shares, the folders of a WinCC project are generally read-only.

1.1 WinCC Installation Notes

Access to the WinCC project folders and project data from the network via Microsoft Windows is read-only.

Release project folder for write access

The "SIMATIC HMI" user group needs full access to the project folders of a server in the following cases:

- Access via scripts or open interfaces, e.g. when using WinCC/ODK
- Access via multiuser engineering
- Access of clients with own project
- Integrated projects (SIMATIC Manager)

To enable full access to the WinCC project folders, disable the following option in the "Properties - Project" area of the "Computer" editor:

- Project directory is only shared for write-protected access.

Make sure that full access is restricted to the necessary user groups or users.

You can change the option while runtime is activated.

The change is applied immediately.

User groups and user rights

The following overview contains the tasks of the different user groups with the access rights and instructions required to assign these access rights.

WinCC Installation

- Task: WinCC Installation
- Role: Configuration engineer, Administrator
- Authorization: Microsoft Windows Administrator rights
- Procedure:
Prior to installation, ensure that you have local administrator rights on the computer.
- Explanation:
You need local administrator rights to install WinCC.

Preparation for operation

- Task: Access to WinCC
- Role: Configuration engineer, Administrator
- Authorization: Power user rights, Administrator rights

- Procedure:
After installation, set up the administrative settings as administrator or power user.
- Explanation:
Power user rights are the minimum requirements for administrative settings, e.g. the authorization of file rights or printer driver settings.
To delete a WinCC project completely, you must have power user rights, at a minimum.

Local user rights when operating WinCC

- Task: Operator input in Runtime, configuration
- Role: WinCC user (operator, configuration engineer)
- Authorization:
 - Microsoft Windows "User" group
 - "SIMATIC HMI" user group
- Procedure:
Add the user to the "SIMATIC HMI" user group and, at a minimum, to the Microsoft Windows "User" user group.
- Explanation:
In order to operate WinCC or for remote access to a WinCC project on the client and server, the user must be a member of the "SIMATIC HMI" user group.

Access to distributed systems

- Task: Access to distributed systems
- Role: WinCC user (operator, configuration engineer)
- Authorization: Uniform user groups on all computers
- Procedure:
Enter the WinCC users on all computers in the same group.
Assign the same password to all the users.
- Explanation:
For access to distributed systems, the same user groups must be created on clients and servers.

Access rights for local projects

- Task: Access to projects which were created as follows:
 - Manual copy
 - Duplicate
 - Retrieving
 - Migration
- Role: WinCC user (operator, configuration engineer)
- Authorization: SIMATIC HMI, SIMATIC HMI Viewer

1.1 WinCC Installation Notes

- **Procedure:**
Assign full access rights to the project folder for the "SIMATIC HMI" group.
To do so, open the project following its creation once as administrator or power user.
Alternatively, you can specify access rights in the Microsoft Windows Computer Management.
Even if you want to copy projects with the Project Duplicator you will need the appropriate authorizations. You will either have to grant access to the used folders or duplicate them as main user.
- **Explanation:**
When a local project is newly created, the members of user groups "SIMATIC HMI" and "SIMATIC HMI Viewer" automatically receive the necessary access rights to the project directory.
However, when projects are copied, logged, or migrated, the local authorizations are not transferred but must be reassigned.

Access rights to system information

- **Task:** Access to system information via the "System Info" WinCC channel
- **Role:** Operator
- **Authorization:** System monitor users
- **Procedure:**
Include all those users in the "System monitor users" Microsoft Windows group who require the following system information from the "System Info" WinCC channel:
 - CPU load
 - Status of the export file
- **Explanation:**
Users with Microsoft Windows standard user rights do not have access to certain system information.

See also

Notes on Data and System Security (Page 25)
How to Adapt the Windows Security Policies (Page 35)
How to install WinCC (Page 36)
WinCC Installation Requirements (Page 16)
Installing WinCC (Page 35)
Software requirements for installing WinCC (Page 19)

Including users in the "SIMATIC HMI" user group

Introduction

Include those local users in the "SIMATIC HMI" group whose login permits access to WinCC.

You must first create local users to do so.

Users of a domain may be directly included in the user group "SIMATIC HMI".

WinCC/WebNavigator: Users of the Web client

When you install the WebNavigator client on the WinCC PC, you must also include the users of the Web client in the user group "SIMATIC HMI" or "SIMATIC HMI VIEWER".

Procedure

1. Open the workstation administration under Microsoft Windows.
2. Select the "Local users and groups > Users" entry in the navigation window.
The data window displays all local users.
3. In the context menu, select the "New User" dialog.
Create a user account for each user who is to have access to WinCC.
4. In the navigation window, select the "Local Users and Groups > Groups" entry.
The data window displays all groups.
Select the group "SIMATIC HMI".
5. Using the shortcut menu, open the "Add Member" dialog and include those users as members of the "SIMATIC HMI" user group.

Including domain-global user group in the "SIMATIC HMI" user group

Introduction

During operation of a domain, an additional domain-global user group may be created and included as a member of the "SIMATIC HMI" user group.

Application example

You can find a detailed application example in the Internet under Entry ID 78346833:

- SiePortal: "Installation and operation of WinCC in a Microsoft domain environment" (<https://support.industry.siemens.com/cs/ww/en/view/78346833>)

Requirements

- The domain administrator creates a domain-global user group.
- Within the domain, the domain administrator includes those users in the domain whose login permits access to WinCC.

1.1 WinCC Installation Notes

Procedure

1. Open the workstation administration under Microsoft Windows.
2. In the navigation window, select the "Local Users and Groups > Groups" entry.
The data window displays all groups.
Select the group "SIMATIC HMI".
3. Using the pop-up menu, open the "Add Member" dialog and include domain-global user group as members of the "SIMATIC HMI" user group.

See also

SiePortal: "Installation and operation of WinCC in a Microsoft domain environment" (<https://support.industry.siemens.com/cs/ww/en/view/78346833>)

Release existing project for "SIMATIC HMI" user group

Introduction

You must first remove the existing share of the project directory if the user group "SIMATIC HMI" has to access an existing user group.

The project is then released again while opening WinCC Explorer.

Procedure

1. Open the workstation administration under Microsoft Windows.
2. In the navigation window, select the entry "Shared Folders > Shares".
The data window displays all unlocked directories.
3. Select the respective project directory and remove the share by using the "Cancel Share" context menu.
4. If you now open the project in WinCC, the project directory is automatically unlocked for the "SIMATIC HMI" user group, and all members of the user group are granted access to the project directory.

Note

The enable name of the directory shared by WinCC must not be modified.

1.1.6.7 How to Adapt the Windows Security Policies

Introduction

Before you install WinCC, you must check the operating system settings:

- The system must permit the installation of unsigned drivers and files.

Procedure

1. To open the Microsoft Windows entry field, select the entry "Run" in the "Windows System" program group.
2. Enter "gpedit.msc" in the input box.
The "Local Group Policy Editor" dialog box opens.
3. In the left section of the window under "Policy for local computer", select "Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions".
4. Check the settings of the security policies below:
 - "Display a custom message when installation is prevented by policy (balloon text)"
 - "Display a custom message when installation is prevented by policy (balloon title)""Not configured" must be set for the policy.

See also

Notes on Data and System Security (Page 25)

Defining Access Rights in the Operating System (Page 29)

Software requirements for installing WinCC (Page 19)

WinCC Installation Requirements (Page 16)

1.1.7 Installing WinCC

1.1.7.1 Installing WinCC

Introduction

This section describes the installation of WinCC.

During the WinCC installation, MS Message Queuing and Microsoft Internet Information Service (IIS) are installed and configured if necessary.

Installation of a WinCC file server

If a WinCC server is set up which is to be used for project data archiving only, only the WinCC file server needs to be installed. You can find more information in the WinCC Information System, in the section "Configurations > Fileserver".

Note

Usage only with administrator rights

If you want to use the Fileserver, you need administrator rights.

Fileserver installation requirements

WinCC V8 and WinCC Fileserver V8 cannot be installed at the same time on one computer.

Installation of WinCC Options

The WinCC DVD contains the following options:

- WinCC/Connectivity Pack / Connectivity Station
- WinCC/DataMonitor
- WinCC/WebNavigator
- WinCC/WebUX

These options require their own licenses.

If you purchase a WinCC option at a later date, you will receive the necessary licenses on a license data carrier.

An installation DVD is not supplied. Use the WinCC DVD for installation.

See also

Upgrading WinCC (Page 50)

How to Install Supplementary Components Later (Page 44)

How to install WinCC (Page 36)

Hardware requirements for installing WinCC (Page 17)

WinCC Installation Requirements (Page 16)

Software requirements for installing WinCC (Page 19)

1.1.7.2 How to install WinCC

Introduction

This section describes how to install and run WinCC.

The already installed components are displayed during setup. The following icons are used:

Icon	Meaning
	Current version of program is installed.
	Program is being updated.
	Program setup conditions are not met. Click the icon for details.
	Program can be selected.
	Program selected for installation.
	Program cannot be selected (due to program interdependencies).
	Program selected for installation (cannot be deselected).

Scope of installation

Installing WinCC options

You can install the desired options during the installation of WinCC itself.

For some options, the documentation only becomes available when the corresponding option package is installed.

Package installation

The following components are installed with the selected program package:

WinCC	WinCC installation The package installs the WinCC server with the following components: • WinCC Runtime • WinCC CS (incl. Basic Process Control) • SQL server • OPC server • OPC UA server • OPC UA client • SmartTools • WinCC Unified Collaboration • Automation License Manager WinCC incl. WebUX • Additionally installs WinCC/WebUX
WinCC client	WinCC client installation: When you install the "WinCC client" program package, you need an "RT client" or "RC client" client license. • WinCC Runtime • WinCC CS (incl. Basic Process Control) • SQL Express • OPC server • OPC UA server • OPC UA client • SmartTools • WinCC Unified Collaboration • Automation License Manager WinCC client incl. WebServer • Additionally installs the WebNavigator server
WebNavigator	WebNavigator server • WinCC server with the components of the program package "WinCC installation" • WebNavigator server To install further WebNavigator components, activate the component in the "Programs" view, e.g. "Web Plugin Builder" for the installation of the "WinCC Plug-In Builder". WebNavigator client • Only installs the WebNavigator client

DataMonitor	DataMonitor server If no WebNavigator server is installed yet, it is also installed with the package. • WinCC server with the components of the program package "WinCC installation" • WebNavigator server • DataMonitor server • DataMonitor client To install further DataMonitor components, activate the components in the "Programs" view, e.g. for the installation of "Excel Workbook" and "Excel Workbook Wizard". DataMonitor client • Only installs the DataMonitor client
ConnectivityPack	ConnectivityPack server • WinCC server with the components of the program package "WinCC installation" • ConnectivityPack server To install further Connectivity Pack components, activate the components in the "Programs" view, for example for the installation of the "Connectivity Station". ConnectivityPack client • ConnectivityPack client • SQL Connectivity Components

Custom installation

Select individual components for installation.

The following components are typical examples of additional installations which are not installed with program packages:

- WinCC:
 - WinCC File server (WinCC file server/SQL server)
- WebNavigator:
 - Diagnostics client
 - WinCC Remote Publisher
- Options:
 - SIMATIC Logon
 - AS-OS Engineering

Supplementary installation

You can install or uninstall components and languages at a later stage.

The required disc space depends upon the installed components. An estimated value is shown in the status bar.

1.1 WinCC Installation Notes

More information:

- "How to Install Supplementary Components Later (Page 44)"
- "How to Install Supplementary Languages (Page 45)".

WinCC remote communication

Remote access is disabled by default after installation.

If you use a redundant system or a client-server system, for example, enable the remote communication in the SIMATIC Shell settings.

More information:

- "Notes on Data and System Security (Page 25)"

Requirements

- Make sure that no other setup is running on the PC at the same time, for example, a Microsoft Windows update.
- You need local administrator rights to install WinCC.
Information on the user rights required for operating WinCC:
 - "AUTOHOTSPOT"
- The computer name may only contain permissible characters.
- The security policies must be modified under Microsoft Windows.
- No manually created SQL server instance with the name "WinCC" may be installed.
- Microsoft Message Queuing is installed and configured during WinCC installation.
- The storage medium with the licenses must not yet be connected to the installation PC.
You can transfer the licenses during WinCC installation.
Alternatively, you can install the licenses before installing WinCC using the Automation License Manager.

WinCC is released for the following operating system languages:

- German, English, French, Italian, Spanish
- Chinese (simplified, PRC), Chinese (traditional, Taiwan), Japanese, Korean
- Multilingual operating system

Note

Unfulfilled requirements

An error message is output if you run WinCC Setup without administrator rights, or if other setup conditions are not met.

You can find more information on error messages here: "WinCC Installation Requirements (Page 16)".

Procedure

1. Start the WinCC product DVD.
 - The DVD starts automatically if Autorun is enabled in the operating system.
 - If the Autorun function is not activated, start the Setup.exe program on the DVD.Alternatively, start the downloaded setup.
2. Follow the on-screen instructions.
Read and confirm the License Agreement and the Open Source License Agreement.
3. Select "Install" as the setup type.
4. Select the languages you want to install.
You can also install other languages at a later time.
5. Select the desired type of installation:
 - For Package installation, select the "WinCC installation" or "WinCC incl. WebUX" program package.
If you also want to install WinCC options, select the corresponding program packages.
Select "WinCC client installation" or "WinCC client incl. WebServer" if you only want to install the WinCC client.
 - If you use the user-defined installation, select the desired installation scope.The components to be installed are shown in the "Description" field in each case.
If necessary, change the installation path using the "Browse" button.
6. Check the list of components to be installed in the "Programs" view.
 - If required, activate additional components.
 - Click on "Help" for a description of the displayed icons.
 - When you click on the listed components, information on the installation status of the components may be shown.
 - The content field on the right contains details on the selected component and, at the bottom, the required disc space.
 - You can open the associated documentation for some components with the "Readme" button.
 - The "Storage space" button will show you the available storage space on your PC.
7. Read and confirm the license agreement for the Microsoft SQL Server.
8. Before the installation, the security settings that are adapted for WinCC are displayed in the "System settings" dialog. The firewall is configured automatically.
Confirm the changes to the system settings.
Use the "Save as" button to save the list of changes as a text file "Secon.RTF" in the selected target folder.
9. Start the installation.
You can track the status of the installation in the displayed dialog.
Select "Cancel" to cancel the installation of the current component.

1.1 WinCC Installation Notes

10. You can transfer the product license keys after installing the components.
To do so, click on "Transfer license key".
Select "Next" if you have already transferred the license keys or want to install them at a later time.

Note

Transferring licenses

License keys are not transferred automatically.

Transfer the missing license keys during or after installation with the Automation License Manager.

11. Restart the PC to conclude the installation.

Automatic migration

When you open a project that was created with a previous version of the currently installed WinCC version, the configuration and Runtime data is automatically migrated.

You can convert the pictures and libraries with the Project Migrator or manually via WinCC Explorer.

You can find detailed information on migration in the WinCC Information System:

- "Getting started > Migration"

Entries in the "Siemens Automation" program group

After installing WinCC, you will find new entries in the "Siemens Automation" program group.

- Starting WinCC Explorer:
 - WinCC Explorer
- Editors and tools for working with WinCC:
 - Autostart
 - Channel Diagnosis
 - Cross Reference Assistant
 - Dynamic Wizard Editor
 - Project Duplicator
 - Project Migrator
 - WinCC Certificate Manager
 - WinCC Documentation Viewer
 - WinCC TAG Simulator

- WinCC documentation:
 - Documentation > Manuals

To open the WinCC Online Help and the installed WinCC options, select the "WinCC Information System" link in the language folder.

Print versions of the WinCC Information System:

 - PDF files in the installation path under "WinCC > Documents"
- License management:
 - Automation License Manager
 - License Analysis
- Security Controller for displaying the customized security settings:
 - Security Controller
- Overview of the installed SIMATIC software and components:
 - Inst. Software
- Editors and tools for working with the supplied WinCC options:
 - PdIPad
 - PublishingWizard
 - Web Navigator Plug-In Builder
 - WinCC Archive Connector
 - WinCC DataMonitor Configurator Export
 - WinCC Web Configuration Center
 - WinCCViewerRT

The entries depend on the installed options.

See also

Upgrading WinCC (Page 50)

Notes on Data and System Security (Page 25)

Defining Access Rights in the Operating System (Page 29)

How to Adapt the Windows Security Policies (Page 35)

How to Install Supplementary Components Later (Page 44)

WinCC Installation Requirements (Page 16)

Hardware requirements for installing WinCC (Page 17)

Software requirements for installing WinCC (Page 19)

Installing WinCC (Page 35)

How to Install Supplementary Languages (Page 45)

1.1.7.3 How to Install Supplementary Components Later

Introduction

Once you have installed WinCC, you can then install further components or options at a later date.

Installation of WinCC Options

The WinCC DVD contains the following WinCC Options:

- WinCC/Connectivity Pack / Connectivity Station
- WinCC/DataMonitor
- WinCC/WebNavigator
- WinCC/WebUX

These options require their own licenses.

If you purchase a WinCC option at a later date, you will receive the necessary licenses on a license data carrier. An installation DVD is not supplied.

Use the WinCC DVD for installation.

Procedure

1. Start the WinCC product DVD.
If the Autorun function is not activated, start the program Setup.exe on the DVD.
2. Specify whether you wish to install individual components or options. The already installed components will be displayed.
3. Follow the on-screen instructions.

Installation path of SmartTools

Run the SmartTools setup from the following path on your WinCC DVD:

- "Instdata\Smarttools\Setup\Setup.exe"

See also

WinCC Installation Requirements (Page 16)

How to install WinCC (Page 36)

Upgrading WinCC (Page 50)

How to Install Supplementary Languages (Page 45)

1.1.7.4 How to Install Supplementary Languages

Introduction

Once you have installed WinCC, you can later install additional languages.

Procedure

1. Open the "Programs and functions" or "Programs and features" entry in the control panel.
2. Select "SIMATIC WinCC Runtime <Version>" and click the "Change" button.
The WinCC Setup program opens.
3. Select your desired languages.
4. When prompted, insert the WinCC product DVD in the DVD drive.
If the home page of the DVD is opened via the Autorun function, close the window with "Exit".
5. Follow the instructions on the screen.
6. If you have installed WinCC CS, select "SIMATIC WinCC Configuration <Version>" and click the "Change" button.
Repeat steps 3 to 5 for WinCC CS.
Repeat this procedure for any additionally installed components and options.

See also

How to Install Supplementary Components Later (Page 44)

How to install WinCC (Page 36)

1.1.7.5 Configure automatic installation of WinCC

The "Central installation" function

Configuring automatic installation

To install WinCC on multiple PCs, use a central installation.

Central setup storage: Note the path length

When you store the setup at a central location and launch it from a network drive, use the shortest possible folder names.

The path length of the drive name, file folder and setup files may be no longer than 255 characters.

Record function

The Record function supports multiple installation on different computers with identical options.

1.1 WinCC Installation Notes

During setup, the Record function records the settings and creates a "Ra_Auto.ini" installation file which supports you during installation.

While in the past you had to navigate through all setup dialogs for each installation, all you have to do now is start setup with the "Ra_Auto.ini" control file.

Conditions for using the record function

- Central installation is only possible for the respective setup version that is available at the time.
A central installation of WinCC has no effect on the subsequent installation of updates or options.
- The "Expert mode" scope of installation cannot be used for automatic installation.
In Expert mode, the installation dialog is opened for each product even when you have saved the installation settings with the Record function.

Overview of the procedure

The following steps are required for a central installation:

1. Call the Record function and create the "Ra_Auto.ini" control file.
2. Start central installation.

WinCC/WebNavigator: Installation without user interaction

For a central installation on a web client start the setup via the following command line:

- Installation with default settings:

```
msiexec /i C:\TEMP\WebnavigatorClient.msi /quiet /log  
C:\temp\installWebNav.log
```
- Installation with reduced user interface:

```
msiexec /i C:\TEMP\WebnavigatorClient.msi /qb /log  
C:\temp\installWebNav.log
```

More information:

- Installing the WebNavigator client (Page 117)

Calling the Record function of the central installation

You use the Record function to create the "Ra_Auto.ini" control file which includes all information for the central installation.

Dependency on operating system

Run the central installation for each operating system version separately.

The control file can only be executed on PCs on which the same operating system version is running. During installation of WinCC, Microsoft updates are installed, for example, which depend on the installed operating system.

Scope of installation for automatic installation

The "Expert mode" scope of installation cannot be used for automatic installation.

Select one of the other available installation methods, e.g. "Standard" or "WinCC Client".

Requirement

- You need administrator rights on your PC.

Procedure

1. To open the Microsoft Windows entry field, select the entry "Run" in the "Windows System" program group.
2. Enter the following command line:

```
- <Path for the installation data>\setup.exe /record
```

Select the DVD drive or a central PC to which the installation data were copied as path for the installation files.
Setup is started.
3. Select the desired language and click "OK".
The "Record function" dialog is displayed.
4. Activate the Record function.
5. Select the path in which you want to create the "Ra_Auto.ini" control file and confirm with "Next".
6. Select the required components and settings for the installation.
Once you have made the settings, the message "Recording completed" is displayed.

Result

The control file "Ra_Auto.ini" is created and saved in the selected path.

The same setup version must be used for central installation and for creation of the "Ra_Auto.ini" file.

Start central installation

For central installation on the PC of your WinCC system, start an automatic installation.

The settings of the "Ra_Auto.ini" control file are applied in the process.

Requirement

- You have created the "Ra_Auto.ini" file using the Record function.
The file "Ra_Auto.ini" must be created with the existing setup version.
- The same operating system version is installed on the PC.

1.1 WinCC Installation Notes

Procedure

1. If required, copy the setup to a central server or PC.
2. Copy the file "Ra_Auto.ini" to the folder "C:\Windows" on the PC to be installed.
3. Start central installation by calling automatic installation:

– <Path for the installation data>\setup.exe /silent

You may receive a message when the central installation was completed successfully.

Note

If an error or inconsistency occurs during installation, you will receive messages that require your acknowledgement.

4. Repeat this process for each required computer.

Alternative procedure

If the file "Ra_Auto.ini" is not located in the "C:\Windows" folder, start central installation with the following call:

- <Path for the installation data>\setup.exe /silent=<storage path>\Ra_Auto.ini

1.1.8 Uninstalling WinCC

Introduction

On your computer, you can remove WinCC completely or simply remove individual components. You cannot remove individual languages.

You can execute the removal via the WinCC product DVD or via the control panel of the operating system.

Procedure: Uninstalling via the WinCC Product DVD

1. Start the WinCC product DVD.
The DVD starts automatically if Autorun is enabled in the operating system.
If the Autorun function is not activated, start the Setup.exe program on the DVD.
2. Follow the on-screen instructions.
3. Select "Remove" as the setup type.
4. Select the components that you want to remove.

Alternative procedure: Uninstalling via the Control Panel

1. Open the "Uninstall or change a program" dialog in the Microsoft Windows Control Panel.
2. Select the desired entry.
The installed WinCC components always start with "SIMATIC WinCC".
3. Choose the "Uninstall" or "Change" option from the shortcut menu.
Remove any WinCC options that may have been installed before you remove the WinCC version.

Microsoft SQL Server

After uninstalling WinCC, you must uninstall the Microsoft SQL Server instance "WinCC":

In the "Uninstall or change programs" dialog, select the entry "Microsoft SQL Server <Version>" to uninstall.

The use of Microsoft SQL Server is only permitted if you have a valid license.

Automation License Manager / MS Update

When WinCC is removed, the following programs remain installed, as they may be needed by other SIMATIC products:

- Automation License Manager
- MS Update V1.0 SP1

If, after removing WinCC, you want to install an earlier version of WinCC, you need to remove both of these programs:

Select the respective entry for removal in the "Uninstall or change a program" dialog.

Removal when the WebNavigator client is installed

If you remove WinCC from a computer on which the WebNavigator client is installed, you must then reinstall the WebNavigator client.

Changing the settings in the Microsoft Windows Event Viewer

When WinCC is installed, the WinCC Setup program changes the settings of the Event Viewer.

- Maximum Log Size (System Log/User Log):
1028 KB
- Log Continuation (System Log/User Log):
"Overwrite events"
(Default setting: Overwrite events that are older than 7 days)

After removing WinCC, these settings are not reset.

You can modify these settings in the Microsoft Windows Event Viewer yourself.

1.1.9 Upgrading WinCC

1.1.9.1 Upgrading WinCC

Introduction

As of version WinCC V7.4 SP1, you can upgrade to the current WinCC version V8.x by means of an upgrade installation. Make sure that the latest WinCC updates for the respective WinCC version have been installed.

Proceed as described in "Upgrading an installation" section.

Note

Restart PC before installing the update

Restart the PC before starting the update installation.

Requirements for the upgrade

If you are upgrading WinCC versions prior to V7.0 SP3, observe the operating system requirements and hardware requirements.

More information on migration of WinCC versions V4 or higher is available under the following URL (entry ID=44029132):

- SiePortal: FAQ Migration V4 > V7 (<https://support.industry.siemens.com/cs/de/en/view/44029132>)
-

Information on migrating projects

WinCC projects > WinCC V7.4 SP1

No migration is required for projects created with WinCC as of V7.4 SP1. You only have to convert the project data.

To convert the project data select the menu command "Tools > Convert Project Data" in the WinCC Explorer.

WinCC projects < WinCC V7.4 SP1

When you open a project of a previous < V7.4 SP1 version with the current WinCC version, you will be prompted to migrate the project. However, you may also use WinCC Project Migrator to migrate several WinCC projects in a single step.

You still have to make some project settings after migration.

For more information about migrating projects see the "Migration" section.

Note

WinCC user no longer needs to be a member of the "SQLServerMSSQLUser\$<COMPUTER NAME>\$WINCC" user group

When you migrate projects created prior to WinCC V7.2, you remove the WinCC users from this group.

In WinCC projects prior to V7.2, you will find the user group under the name "SQLServer2005MSSQLUser\$<COMPUTER NAME>\$WINCC".

Notes on licensing

Licenses from previous WinCC versions must be upgraded to the current version.

You can update the licensing retroactively. Detailed information is available in the WinCC Information System under the topic "Licensing".

See also

How to Perform an Upgrade Installation (Page 51)

SiePortal: FAQ Migration V4 > V7 (<https://support.industry.siemens.com/cs/de/en/view/44029132>)

1.1.9.2 How to Perform an Upgrade Installation

Introduction

If you currently have WinCC V7.4 SP1 or higher installed on your system, you can perform an upgrade installation. Make sure that the latest WinCC updates for the respective WinCC version have been installed.

Before beginning an upgrade installation, the transfer of existing projects must be prepared.

Requirement

The hardware configuration of previous versions is sufficient in most cases to install an upgrade to the current WinCC version V8.x.

However, performance is reduced if the amount of data is increased too much.

If it is expected that the data volume will increase, upgrade the hardware in good time.

Note

Requirements for the upgrade

If you are upgrading WinCC versions prior to V7.0 SP3, observe the operating system requirements and hardware requirements.

More information on migration of WinCC versions V4 or higher is available under the following URL (entry ID=44029132):

- SiePortal: FAQ Migration V4 > V7 (<https://support.industry.siemens.com/cs/de/en/view/44029132>)
-

Upgrade preparation

Note

Backing up a WinCC project

Make a backup copy of your project before upgrading WinCC.

Restart PC before installing the update

Restart the PC before starting the update installation.

Additional steps and adjusting settings

Also read the notes in the WinCC Information System under "Migration".

Check the special characters

Before performing an upgrade installation of WinCC, check the existing projects with regard to special characters used in the archive names, archive tag names, trend names, trend window names, column names and table window names.

You will find a table with the permitted special characters in the section "Working with WinCC > Working with Projects > References".

It is possible that you must use Tag Logging in WinCC V6.2 SP3 or V7.0 to remove certain special characters from the names.

NOTICE
Transferring archives with impermissible special characters
When transferring archives, if they contain impermissible special characters, the runtime archive may be lost.

Modified standard functions (ANSI-C)

If modified standard functions (ANSI-C) are used, make backup copies of the functions prior to the upgrade installation.

During the WinCC installation process, these functions are overwritten by the standard functions supplied.

Procedure

1. Prepare existing WinCC projects for migration.
Check the used names for impermissible special characters.
2. Install the current WinCC version.
Proceed as described in the section "How to install WinCC".
You will need the storage medium that contains the licenses for the current WinCC version.
Upgraded licenses of previous WinCC versions will be lost.
3. Migrate your existing WinCC projects.
Note the corresponding "First Information > Migration" section in the WinCC Information System.

See also

How to install WinCC (Page 36)

WinCC Installation Requirements (Page 16)

Installing WinCC (Page 35)

SiePortal: FAQ Migration V4 > V7 (<https://support.industry.siemens.com/cs/de/en/view/44029132>)

1.1.10 Overview: Notes on operation

Introduction

For trouble-free operation and optimal performance of WinCC, observe the notes on operation under Microsoft Windows and the notes on configuration.

You can find this information in the following sections of the WinCC Information System:

- "Release Notes > Notes on operation (Page 55)"
This section includes information on compatibility and on use of virus scanners.
- "Release Notes > Notes on WinCC > Remote access and Remote Desktop Protocol (RDP) (Page 81)"
The section contains information about remote communication.
- "Working with WinCC > Working with Projects > Making Settings for Runtime > Effect of External Applications at Runtime"
This section contains information on applications that can affect system resources.
- "Working with WinCC > Working with Projects > Making Settings for Runtime > System diagnostics with performance tags"
The section contains information on system tags with which, for example, the time behavior during reading or writing of tags is analyzed.

1.1 WinCC Installation Notes

- "Working with WinCC > Configuration recommendations"
The section contains information on the high-performance configuration of process pictures and on the optimal dynamization of picture objects and controls.
- "Configurations > Multi-User Systems > Quantity structures and performance"
The notes on configuration in this section apply to all project types.

1.2 WinCC Release Notes

1.2.1 Release Notes

Content

These Release Notes contain important information.

The information in these Release Notes has priority over that in the manuals and online help with regard to legal validity.

Please read these Release Notes carefully since it contains information which may prove helpful.

1.2.2 Notes on operation

1.2.2.1 Notes on operation

General information

Avoiding loads from external applications

If several programs are run simultaneously on the same computer, the computer may be exposed to high load levels.

To ensure trouble-free WinCC operations do not run any other applications that can lead to a resource crunch on the PC. Therefore, close any unnecessary programs before starting WinCC. More information is available in the section "Working with Projects > Making Runtime Settings > Impact of External Applications on Runtime".

System diagnostics with performance tags

You can analyze the time behavior, e.g. during reading and writing of data, with the system tags of the "Performance" tag group.

Feedback and user data statistics (telemetry)

WinCC collects and processes license information and statistical usage and diagnostic data like quantity structures or the frequency of use of specific functions in order to keep WinCC safe and up to date, to detect and diagnose problems and to implement product improvements.

The anonymized usage and diagnostic data is initially saved on your local computer in readable form where you can view it.

Storage path:

- ...\\ProgramData\\Siemens\\Automation\\TelemetryConnector\\EventPersistence

The usage and diagnostic data is then also transferred to Siemens via a secure communication channel for the above-mentioned purposes.

You can deactivate this function via the project settings at any time.

Compatibility

You can find information on compatibility on the Internet in FAQ No. 64847781:

- SiePortal: FAQ 64847781 (<https://support.industry.siemens.com/cs/ww/en/view/64847781>)
- Compatibility tool for automation and drive technology: (<https://support.industry.siemens.com/kompatool/index.html?lang=en>)

Using virus scanners

The following virus scanners have been approved for use as of WinCC V8.1:

- Symantec Endpoint Protection V14.3 RU9 (Norton Antivirus)
- McAfee Endpoint Protection Suite V10.7
- Trellix Endpoint Security 10.7 (McAfee)
- Trellix Application Control 8.4 (McAfee)
- TXOne StellarProtect 3.0
- Windows Defender (version contained in the operating system)

You can find updated information on the approved virus scanners in the compatibility tool under "More products > Virus scanners".

Fundamental principle

The use of a virus scanner should not hamper the runtime process in a plant.

Rules for local virus scanners (virus scan clients)

- Integrated firewall of the virus scanners
The used local Windows Firewall is configured in WinCC V8.x using SIMATIC Security Control. You may not install or activate the integrated Firewall of the virus scanners.
- Manual scan
You are not permitted to run a manual scan in Runtime. Run this scan at regular intervals on all system PCs, for example, during a maintenance interval.
- Automatic scan
With an automatic scan it is sufficient to scan the incoming data traffic.
- Time-controlled scan
You are not permitted to run the time-controlled scan in Runtime.
- Pattern update
The pattern update of virus scan clients (system PCs being checked for viruses) is done by the higher-level virus scan server (the system PC that centrally manages the virus scan clients).
- Dialogs
To avoid interfering with the process mode, no dialog messages should be displayed on the virus scan clients.

- Drives
Only the local drives are scanned to prevent overlapping scans on network drives.
- You can deactivate email scan except on the WinCC engineering station that receives email.
Accept all other default settings.

What does this ensure?

The incoming data traffic is checked for viruses. The effect on process mode is kept to a minimum.

Note

When using a virus scanner, make sure that the computer has sufficient system resources.

Screen savers

Using a screen saver costs processor time and can lead to a system overload. Screen savers that do not release portions of the work memory no longer needed continually reduce the usable work memory.

The Microsoft Windows "Logon screen saver" can be used.

See also

Software requirements for installing WinCC (Page 19)

SiePortal: FAQ 64847781 (<https://support.industry.siemens.com/cs/ww/en/view/64847781>)

Compatibility tool for automation and drive technology: (<https://support.industry.siemens.com/kompatool/index.html?lang=en>)

1.2.2.2 Information on the Microsoft Windows operating system**Microsoft security updates and patches**

Make sure that all current patches and security updates from Microsoft are installed on your computer.

For more information, refer to the FAQs in the SIMATIC Customer Online Support:

- SiePortal: FAQ 18752994 (<https://support.industry.siemens.com/cs/ww/en/view/18752994>)
- SiePortal: FAQ search (<https://support.industry.siemens.com/cs/products?search=microsoft&ctp=Faq&mfn=ps&o=DefaultRankingDesc&pnid=14866&lc=en-WW>)

General information

WinCC interface and 64-bit operating system

The public interface of WinCC offer no native 64-bit support. This primarily affects ODK, VBS and the WinCC OLEDB provider.

To use the WinCC interfaces under a 64-bit operating system, the following applies:

- You cannot launch VB scripts simply with a double-click.
You must explicitly use the 32-bit version under "syswow64\wscript.exe".
- .NET applications that use the WinCC API must be explicitly compiled as 32-bit applications.
With "x86" and not with "AnyCPU".
- C++ applications cannot be compiled as 64-bit applications.

Preventing access to Microsoft Windows in runtime

Displaying the online help in runtime

If you wish to ensure that operators have no access to the operating system level of a plant, deactivate online help in all controls. This prevents the Microsoft Windows selection dialog from opening.

For this purpose, deactivate the "Help available in Runtime" option under "Options" in the "Properties - Project" area of the "Computer" editor.

Displaying the Microsoft Windows taskbar in runtime

You can use the computer properties to prevent the Windows taskbar from being displayed in runtime:

- Activate the "Disable keys" option under "Parameters" in the "Properties - Computer" area of the "Computer" editor.
This disables all shortcut keys for operating system access.
- Disable the "Keep the taskbar on top of other windows" setting in Microsoft Windows or enable the options for hiding the taskbar.

If you disable the <CTRL+ESC> shortcut key, the following shortcut keys are also disabled in runtime:

Key combination	Function
<Windows key+U>	System utility program manager
Press <SHIFT> five times	Locking function
Press <SHIFT right> for eight seconds	Impact delay
<ALT left+SHIFT left+NUM>	Keyboard mouse
<ALT left+SHIFT left+PRINT>	High contrast

These functions can be configured using the Microsoft Windows Control Panel.

If the functions are activated in the Windows Control Panel before activating WinCC Runtime, they are no longer locked in runtime.

By activating the option "Disable shortcut keys for operating system access", you are also disabling the shortcut keys for easier operation.

Do not use the "On-screen Keyboard" that can be enabled in Microsoft Windows

Use the virtual keyboard offered by WinCC instead of the "On-Screen Keyboard" enabled by Windows to prevent the display of the Windows taskbar in Runtime.

Keyboard with multimedia keys

Do not use keyboards that support additional multimedia keys (AppKeys).

If you are using a keyboard with multimedia keys for a good reason, disable the corresponding registry keys in the following paths:

- All Microsoft Windows users:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\AppKey\<XX>
- Local Microsoft Windows user:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AppKey\<XX>

Disable the "REG_SZ" entries for multimedia buttons in the numbered folders.

The value of the registry entry must not be set.

NOTICE**Registry change**

Create a backup copy of the registry before you edit the registry.

You can find more information on creating a backup copy, restoring and editing the registry in the Microsoft Knowledge Base under article no. 256986 (<https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users>).

Incorrect use of the Registry Editor can cause serious problems that affect the entire system and require reinstallation.

Use the Registry Editor at your own risk.

Do not specify print to file as standard printing

Do not set print to file as standard printing procedure in the Microsoft Windows operating system.

This prevents the Windows dialog for saving the file from opening when printing from WinCC.

"Hardcopy" function

If the shortcut keys are disabled via the option "Disable shortcut keys for operating system access", the hardcopy function only prints to physically connected printers.

No printout is possible on printers with the "Print to file" function, e.g. save as PDF file. The hardcopy function is not performed for these printers.

If several printers are connected and the configured default printer enables the "Print to file" function, the next physically connected printer in the printer list is used instead of the default printer.

Suppressing Microsoft Windows notifications and alarms in Runtime

To prevent the display of Windows notifications and Windows alarms on a PC in Runtime, follow these steps:

1. Enter "Notifications and actions" in the search field of the Windows taskbar.
The settings for Microsoft Windows notifications and actions open.
2. Click "Notification wizard settings".
3. Select the following settings in the notification wizard:
 - Select the "Alarms only" option.
 - Under "Automatic rules", disable the "When I'm using an app in full-screen mode/Alarms only" option.

WinCC WebBrowser Control: Disabling the shortcut menu

You can restrict the shortcut menu of the WinCC WebBrowser Control in runtime:

- To reduce the shortcut menu to "Forward" and "Backward" navigation, activate the object property "UseSimpleContextMenu" in the Graphics Designer.
- To suppress the shortcut menu completely, disable the Microsoft Windows Group Policy: To open the Microsoft "Group Policy Object Editor", enter "Gpedit.msc" in the search field. Disable the shortcut menu in the Group Policy "User configuration\Administrative templates\Windows components\Internet Explorer\Browser menus".

Warnings with the DCOM configuration

When the "Dcomcnfg.exe" program starts, there may be warnings about unregistered AppIDs of WinCC components.

This reaction has no effect on the functional capability of the software. The warnings can be ignored.

Changing the screen settings

Changing the color palette

If you change the color palette via the Microsoft Windows Control Panel, you should expect color changes and poorer legibility of the text.

When creating the project, therefore, be sure use the same color palette that will be used in runtime.

Changing the resolution

In order to use a different resolution in the destination system, use the "Adapt Picture" or "Adapt Size" functions for pictures and windows.

These settings can lead to blurred displays in runtime and increased system loads.

Operating system with multilanguage installation: wrong language in message boxes

In message boxes in which the user must respond with Yes/No, OK/Cancel, etc., the buttons are always labeled in English in both CS and RT.

This characteristic is independent of both the operating system language set and the WinCC language.

Novell Netware clients

WinCC should not be installed on a system together with the Novell client software.

The installation of WinCC can have the effect that it is no longer possible to log on to the Novell system or the lock the keyboard during runtime.

We recommend you not use the Netware client software or use the Microsoft client for Netware.

Notes on Internet Explorer

Web client: Display of ActiveX controls in Internet Explorer

ActiveX controls are disabled in Internet Explorer by default. For this reason, the WinCC controls are not displayed correctly in Internet Explorer on a Web client.

To display the WinCC controls correctly, add the Web server as a trusted website and enable the ActiveX controls only for the "Trusted sites" zone.

To continue protecting Internet Explorer from foreign ActiveX controls, check that the restricted security settings still apply to the other zones after making the changes.

For more information, refer to the following documentation:

- WinCC/WebNavigator: "WinCC/WebNavigator Installation Notes > Installation of WebNavigator Client > Settings in Internet Explorer"
- WinCC/DataMonitor: "WinCC/DataMonitor Documentation > Configuring the DataMonitor System > Working with the DataMonitor Client > Configuring Security Settings in Internet Explorer"

Internet Explorer: Setting for WinCC without Internet connection

Disable the option "Check for publisher's certificate revocation" on the "Advanced" tab in the Internet Options if you operate WinCC on PCs that do not have an Internet connection.

See also

Notes on Data and System Security (Page 25)

SiePortal: FAQ 18752994 (<https://support.industry.siemens.com/cs/ww/en/view/18752994>)

SiePortal: FAQ search (<https://support.industry.siemens.com/cs/products?search=microsoft&ctp=FAQ&mfn=ps&o=DefaultRankingDesc&pnid=14866&lc=en-WW>)

SiePortal: WinCC FAQs (<http://support.automation.siemens.com/WW/view/en/10805583/133000>)

1.2.2.3 Information on the database system

Information on DB.dll

DB.dll is an ODK component for accessing databases via C API functions.

This functionality is no longer supported when using WinCC. Do not develop any new applications with the WinCC database access layer DB.dll.

Instead, use the following functions offered by Microsoft:

- Use ADO.NET for .NET-based applications.
The database interface of the .NET Framework is object-oriented and designed for scalable applications. The interface is also well suited for data communication through firewalls.
- You can use OLE DB for C++ based applications.
Microsoft provides templates with Visual Studio for this. They make it easier to use the OLE DB database technology with classes, which implement many commonly used OLE DB interfaces.
- You can also use ODBC C++ based applications.
Microsoft provides classes for this, which facilitate programming.

You can find more detailed information and examples on the Microsoft website.

Notes on Microsoft SQL Server

Error accessing the SQL master database after switching off the server while the system is running

If a server fails unexpectedly in runtime (power failure, disconnection of power plug), the WinCC installation may be corrupted as a result and the SQL server will no longer be able to access the SQL master database following a restart.

Access is only possible after reinstalling the WinCC instance.

To reinstall the WinCC instance, you must uninstall and reinstall both WinCC and the Microsoft SQL Server.

Improved access protection for the WinCC databases

For the purposes of improved access protection, the user names "WinCCAdmin" and "WinCCConnect" have been removed from the WinCC database.

Access to the WinCC database is no longer possible using these user names. Applications which use their own SQL user names with password are not affected.

The user "SA" (system administrator) of the SQL server is deactivated during the installation.

Stability of the SQL server: Configuring the MemToLeave parameter

If the SQL server goes offline sporadically, configure the MemToLeave parameter:

1. Close WinCC.
2. Open the SQL server configuration manager.
3. Under "SQL server services" select the entry "SQL server (WinCC)".
4. To open the property dialog, select the "Properties" option from the context menu.
5. Add the following entry on the "Start parameters" tab:
 - -g1024
6. Start WinCC.

Manual detachment of WinCC project databases

Due to a system property in Microsoft SQL Server, the NTFS authorizations may be changed when detaching from the WinCC project databases.

If a WinCC database remains attached after you have closed a WinCC project or if you have manually attached the WinCC database, it is necessary to use the CCCleaner to detach the database.

The "CCCleaner" program is located in the "bin" folder of the WinCC installation directory and must be started as administrator.

1.2.2.4 Information on network technology and UPS

Information on networks

WinCC only supports the TCP/IP network protocol on the terminal bus.

Operation on network servers

It is not permitted to operate WinCC on network servers (e.g. domain controllers, file and name utility servers, routers, software firewalls, media servers, exchange servers, etc.).

Operation on systems with Microsoft Windows cluster technology

WinCC cannot be operated on systems with Microsoft Windows Cluster technology.

Use of redundant servers

When redundant pairs of servers are implemented, the master and standby server must be operated in the same IP/subnet band.

Network adapters with energy-saving mode

When using network adapters provided with energy-saving mode, the energy-saving mode must not be activated.

Operation with multiple network adapters

If WinCC is used on a PC with more than one network adapter, observe the following:

Select the IP addresses which WinCC should use for communication with other WinCC stations. In Microsoft Windows Explorer, select the "Simatic Shell" directory. Click into the navigation window of the dialog "Simatic Shell" and select "Settings..." in the shortcut menu. In the "Settings" dialog that follows, select the IP address to be used.

If problems occur with the configuration and project management despite this setting, it could be due to the assignment of the IP address by the DHCP server to the WinCC station being too slow. In this case, the network administrator must define the IP address for each network adapter on the WinCC station causing the problem.

To do this, press the Microsoft Windows "Start" button and select "Settings" > "Control Panel". Open the "Network Connections" folder and then the "LAN Connection" dialog. Click "Properties" in the "General" tab. Open the "LAN Connection Properties" dialog and select the "Internet Protocol (TCP/IP)" element from the list in the "General" tab by double-clicking it. Use the "Use the following IP address" option button in the properties of Internet Protocol (TCP/IP) to define the IP addresses.

Observe the information in the following chapter: "Special features for communication with a server with multiple network adapters"

Network environment and network drives

Ensure that there are no unnecessary network drive connections.

In order to prevent delays following a restart of a distributed system, start the multi-user projects first. The reason for this is the reaction of the master browser service (responsible for displaying the network environment in the operating system) and administration of the domains and working groups.

Operation with TCP/IP protocol

If the TCP/IP protocol is installed, the IP address must be valid and must not change in runtime operation.

Observe the following here:

1. The IP address becomes invalid when the network adapter is removed or deactivated after installation of the TCP/IP protocol.
2. The IP address may not be initialized yet. This occurs, for example, when the TCP/IP protocol is installed with the IP address derived from a DHCP server. When the computer is connected to the network, the computer undergoes a basic initialization during which an IP address is transferred. This IP address then remains valid even after the computer is disconnected from the network. After the period of the lease has expired, however, it can become invalid or changed in another way.

If the computer is not connected to the network, the user must log on via a user configured locally on this computer. This user should have local power user rights for runtime operation and for the configuration.

Leading zeros in IP addresses

When multi-user mode is used with name derivation via "hosts" and "lmhosts", no preceding zeros may be entered in the "hosts" file. IP addresses with leading zeros are interpreted as OCTAL instead of DECIMAL.

Example:

- Computer_1 199.99.99.020 is interpreted as 199.99.99.16 (decimal)
- Computer_2 199.99.99.026 is interpreted as 199.99.99.22 (decimal)

The specification can also be made hexadecimal:

- 199.99.99.0x10 for Computer_1

Using WinCC in multiple domains

The correct functioning of WinCC can only be guaranteed when all the computers in a multi-user system are located in a common domain or working group. When WinCC is used in different domains or working groups, complications may arise if the access rights and/or name utility are configured incorrectly.

When the user administration is realized in a working group, all the WinCC users must be set up on all the computers in the multi-user system and have the necessary access authorization.

Application example

You can find a detailed application example in the Internet under Entry ID 78346833:

- SiePortal: "Installation and operation of WinCC in a Microsoft domain environment" (<https://support.industry.siemens.com/cs/ww/en/view/78346833>)

Use of WinCC within a domain

If problems occur in accessing the Microsoft Windows domains, it cannot be guaranteed that WinCC functions correctly. Therefore, in addition to a "server-stored user profile", a local user profile and local user with necessary rights for WinCC must be set up. If access problems occur with a domain logon, exit WinCC and log on again using the local user profile.

Application example

You can find a detailed application example in the Internet under Entry ID 78346833:

- SiePortal: "Installation and operation of WinCC in a Microsoft domain environment" (<https://support.industry.siemens.com/cs/ww/en/view/78346833>)

Operation in domains with deactivated NTLM protocol

If the NTLM protocol is deactivated for the domains, you can operate WinCC through the use of the Kerberos protocol.

Information for using routers and firewalls

Using routers

With WinCC V7/V8, it is also possible to connect WinCC clients to WinCC servers via routers.

WinCC clients without their own project cannot be used for configuration with the routers, only for WinCC Runtime. There are no restrictions for WinCC clients with their own project.

The following is required when using routers:

- WinCC must use the correct IP address of the WinCC stations.
- The WinCC stations must be capable of resolving the physical computer name (NETBIOS name) of the other computers in the WinCC project.
- The WinCC stations must be capable of reaching each other via TCP/IP and ICMP without any problems. When testing the connection using Ping, it must be possible to access the computers immediately.
- Activate multicast forwarding to the network routers between the servers and the clients.

Speed of the network connections

For slow network connections, we recommend:

- Restricting the quantity of data to be transferred, for example, by avoiding complicated graphics.
- Using the local pdl cache of the WinCC client.
- Using the ISDN router for a WinCC client in multi-link mode (channel bundling). Bandwidths below 128 Kbps have proved insufficient.
- Integrate only one WinCC client for each additional ISDN channel.
- The operation of WinCC via ISDN routers depends on the stability and availability of the ISDN network.
- Reserve the maximum bandwidth of the connection for WinCC.

Note

Connection via ISDN and operation using slow connections has not been approved for clients without a local project.

Connecting to an office network with a central firewall

Some network configurations can increase the load on the firewall.

You can avoid the described reaction by assigning unique IP addresses to all WinCC stations.

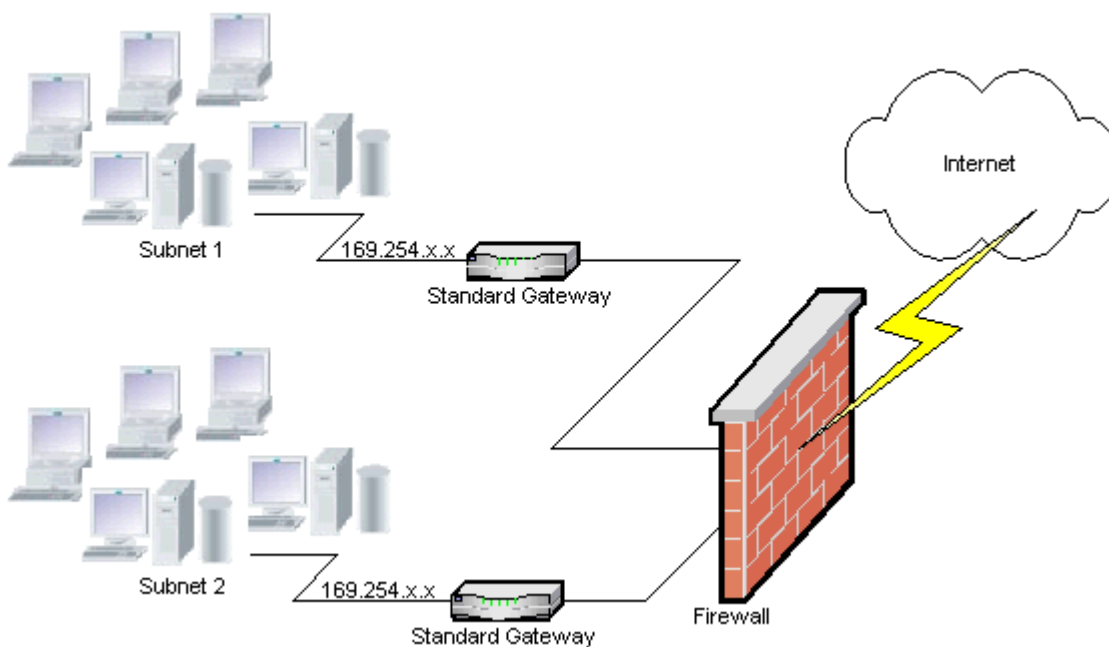
Basic system characteristics

- With a standard installation of Microsoft Windows, the computer is assigned a random IP address from the DHCP server.

Requirements

The following conditions can lead to undesirable reactions when operating WinCC:

- The IP address band used in the terminal network is higher than the APIPA address band (169.254.x.x).
- IP addresses are routed via the default gateway.
- IP addresses from the APIPA band are routed to the firewall.



Cause of the increased load at the firewall

Following a system startup, each WinCC station sends its IP address once to all the other WinCC stations in the network. The WinCC stations define the WinCC station with the lowest IP address as the server that coordinates availability of the project.

If a WinCC station does not receive an address from the DHCP server and is therefore missing in the APIPA process, this station becomes the coordinating server. As a result, all the other WinCC stations attempt to access this server cyclically to publish the project.

The coordinating server, however, cannot be addressed because the IP address from the APIPA band is automatically transferred to the firewall. This also causes an increased network load at the central firewall.

Solution

This reaction can be avoided by assigning a unique IP address to each WinCC station.

Information on uninterruptible power system

Prevent damaged files during power outages

If a power failure occurs while using Microsoft Windows systems when the WinCC system is active, files can be corrupted or lost.

Operation using the NTFS file system offers more security.

Secure continuous operation can only be guaranteed when an uninterruptible power system (UPS) is used.

Uninterruptible power system for client-server systems

If the server in a client-server system should be buffered by an UPS system, it must be capable of bridging a power failure for up to 30 minutes. This value depends on the configuration and number of computers, especially in a multi-user system. A great deal of time is required for the configuration.

See also

SiePortal: "Installation and operation of WinCC in a Microsoft domain environment" (<https://support.industry.siemens.com/cs/ww/en/view/78346833>)

1.2.3 Notes on WinCC

1.2.3.1 General information on WinCC and configurations

General information

WinCC Demo project

WinCC demo projects for WinCC V7/V8 can be downloaded from the Internet:

- SiePortal: WinCC demo projects (search) (<https://support.industry.siemens.com/cs/products?search=demo&ntp=ExampleOfUse&o=DefaultRankingDesc&pnid=14867&lc=en-WW>)
- SiePortal: WinCC V8.0 demo project (download, entry ID 109823232) (<https://support.industry.siemens.com/cs/ww/en/view/109823232>)
Requirement: WinCC V8.0 Update 2
The demo project was created with WinCC V8.0 Update 2. Install Update 2 or a more recent update of WinCC V8.0 from the download page:
SiePortal: Updates for WinCC 8.0 and WinCC V8.0 ASIA (downloads, entry ID 109818723) (<https://support.industry.siemens.com/cs/ww/en/view/109818723>)

WinCC passwords: Migration of WinCC projects

As of version V7.2, WinCC offers improved encryption of passwords.

Note for migrated project that were created with WinCC prior to V7.2:

- You must re-enter the user name and the password for "WinCC Service Mode" operating mode.
- To increase security of WinCC through improved encryption, you have to re-enter the passwords in the User Administrator.

Make sure that the WinCC passwords meet the standard security guidelines.

Define the minimum complexity in the User Administrator, e.g. the required number of special characters.

In the User Administrator you can also configure the locking of users after multiple failed login attempts.

Migrate WinCC projects remotely only with UNC paths

Use only UNC paths to migrate WinCC projects remotely. Release the project path or the folder above it. Use this UNC path as project directory for the WinCC Project Migrator.

No update of the operating system with WinCC started

An update of the operating system is not permitted if WinCC is started. Start the computer again after updating the operating system.

WinCC documentation: WinCC Information System

The information in the online help is more up-to-date than the information in the printable PDF files.

Openness and system stability

WinCC enables high performance programming of actions on individual graphic objects up to complete functions and global action scripts that are independent of the individual components.

C scripting

WinCC and Windows API functions can be called in the action scripts. In addition, the integrated script programming contains a C interpreter with a large number of standard functions complying to ANSI-C.

Please note that, due to the openness of the system, it is possible to write actions that block the system and lead to system crashes in runtime due to continuous loops, incorrectly initialized pointers, etc. Pay attention to the availability of allocated memory.

VB scripting

VBScript (VBS) enables access to tags and objects of the graphical runtime system during runtime. In addition to VBS standard functions and constants, the Windows Scripting Host and the MS Automation interface can also be used to make the Windows environment dynamic.

1.2 WinCC Release Notes

There is no guarantee nor WinCC support for the VBS functionality with regard to its adaptation to the Windows environment.

You can find more information in the following sections of the WinCC Information System:

- "ANSI-C for Creating Functions and Actions"
- "VBS for Creating Procedures and Actions"
- "Process Picture Dynamics"

Time synchronization

Time synchronization between the servers and automation systems is essential for the correct functioning of:

- Redundancy synchronization
- Chronological messaging
- Search and sorting criteria using the time code
- Operating multi-user projects in one domain

You can find more information in the following sections of the WinCC Information System:

- "Redundant systems"
- "Chronological reporting"
- "Multi-user systems"
- "Time synchronization"

Complete download of redundant systems

Do not perform a complete download to the redundant systems in SIMATIC Manager using the "Target system / Compile and Download Objects..." function, as this can create inconsistent data on the target system.

Instead, select the "Download" option in the SIMATIC manager in the shortcut menu of the operating system.

Information on multi-user systems

Clients without their own project in multi-user systems

In multi-user systems, there may be a delay in the selection of the first picture following a redundancy switchover for clients without their own project.

If you are changing the runtime language of a client without its own project in a multi-user system, you will have to close WinCC on the client and exit the WinCC project on the server. Only then will the language be altered.

Remote access from a client without its own project

The server data editor is not available in the WinCC Explorer on a client without its own project.

The "Archive Configuration" entry is not available in Tag Logging and Alarm Logging.

Notes on integration into SIMATIC Manager

Symbolic data block name: Maximum of 16 characters long

If you want to transfer tags from a data block to WinCC, the symbolic name must not exceed 16 characters.

Creating a DCF file

If the DCF file cannot be read after migration, a message regarding the defective file is written to the migration log file.

In order to create another DCF file, proceed as follows. The sequence must be adhered to in all cases:

1. Open the project in the configuration mode.
2. Remember your own symbolic computer name (server prefix) needed for later export.
3. Remember the storage location of the imported server data.
4. Remember the preferred server and the default server.
5. Delete your own and imported server data.
6. Close the project.
7. Delete the DCF file in project directory (typically ProjectName.dcf).
8. Reopen the project in the configuration mode.
9. Create your own server data, making sure to maintain the original symbolic computer name (server prefix) (see step 2).
10. Import all imported packages again (see step 3).
11. Reconfigure the preferred server and default server (see step 4).
12. Close the project.

You can find more information on DCF files on the Internet under Entry ID 109763043:

- SiePortal: "How do you delete the DCF file of your WinCC project?" (<https://support.industry.siemens.com/cs/ww/en/view/109763043>)

CPU load

If data, transferred from a server to a client, cannot be processed at the same speed, the client rejects the data frames from a specified threshold value.

The following process control messages are issued in conjunction with this:

- 1000200: "WCCRT:Status"

1.2 WinCC Release Notes

You will find the following additional information in the comment of this message or in the log file "WinCC_Sys_<x>.log":

- 1000200,4,,<Computer name>, DataManager Runtime, RPC call took longer than 5000 msec
(Client requires a very long time to process the data)
- 1000200,4,,<Computer name>, DataManager Runtime, Update data for Client '<client name>' lost,
(message frames for the client are discarded on the server)

Data may be lost on the client.

Notes on internal functions

Diagnostic functions and special functions

Special key functions can be enabled via Registry Keys for the internal diagnostics of WinCC Graphics Runtime via the following path:
"HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SIEMENS\WinCC\Graphic-Settings\General\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SIEMENS\WinCC\Graphic-Settings\General\EnableGlobalSettings".

- <F1>: Switch between GDI+ and D2D
- <F2>: Performance test
- <F3>: Display shadow
- <F4>: Switch between default/HW/SW mode
- <F6>: Switch to "WinCC Classic" design
- <F7> – <F9>: Switch between designs 1–3
- <F10>: Show Runtime overlay

Note

For internal diagnostic purposes only

These functions may only be used by Siemens Support employees for internal diagnostic purposes.

See also

SiePortal: WinCC demo projects (search) (<https://support.industry.siemens.com/cs/products?search=demo&ctp=ExampleOfUse&o=DefaultRankingDesc&pnid=14867&lc=en-WW>)

SiePortal: WinCC V8.0 demo project (download, entry ID 109823232) (<https://support.industry.siemens.com/cs/ww/en/view/109823232>)

SiePortal: "How do you delete the DCF file of your WinCC project?" (<https://support.industry.siemens.com/cs/ww/en/view/109763043>)

SiePortal: Updates for WinCC 8.0 and WinCC V8.0 ASIA (downloads, entry ID 109818723) (<https://support.industry.siemens.com/cs/ww/en/view/109818723>)

1.2.3.2 Information on WinCC CS

General information

Using several WinCC editors

Do not use multiple WinCC editors at the same time because the editors can access the same WinCC components. For example, use of the "Text Distributor" and "Cross Reference" editors or automatic update of the Cross Reference when the Graphics Designer is being accessed simultaneously via interfaces.

If you would like to work in several WinCC editors in parallel, activate the function "Multi-User-Engineering" in the WinCC project.

Information on the Graphics Designer

Custom ActiveX controls (SIMATIC WinCC/ODK)

You must verify compatibility of custom ActiveX controls (SIMATIC WinCC/ODK) with the WinCC Basic System, WebNavigator Server, and WebNavigator Client.

This applies to both a direct installation of the ActiveX control on the computer with WinCC, Web server or Web client and the installation using a plug-in, such as on the Web client.

- With a direct installation, the ActiveX control should therefore be installed prior to WinCC Basic System, Web Server or Web Client.
If the custom ActiveX controls do not function without error after this step, there is no compatibility.
- If the custom ActiveX Control was packaged in a plug-in and installed via download, an upgrade of WinCC Basic System, Web Server or Web Client will also require generation of a new plug-in using this ActiveX Control.
When creating the plug-in, care should be taken to use compatible binaries (DLL, OCX, etc.).

Visual C++ Redistributable for Visual Studio

Microsoft Redistributable Packages for Visual Studio C++ 2015 are installed along with WinCC.

For example, if you are using ActiveX controls or Visual Basic projects created with versions prior to Visual Studio 2015, you must install the corresponding package.

The installation files for redistributables < Visual Studio 2015 are included in the WinCC scope of delivery:

- "Additional Content" DVD:
"VCRedist" folder

1.2 WinCC Release Notes

Select the setup for the required version:

- 2005x86 / 2005x64
- 2008x86 / 2008x64
- 2010x86 / 2010x64
- 2012x86 / 2012x64

Do not change the folder "GraCS/SVGLibrary"

Do not save any process pictures or faceplate types in the project folder under "GraCS/SVGLibrary".

The folder "SVGLibrary" is only used for SVG libraries.

OLE object of the type "Adobe Acrobat Document"

You can receive error messages in connection with OLE objects of the type "Adobe Acrobat Document" under the following circumstances:

- If you are using an OLE object of the type "Adobe Acrobat Document" in a picture and you save the picture multiple times, saving is aborted with an error message.
- If you then open the respective picture, the file cannot be opened correctly due to an error.
- If you try to save a picture with an OLE object of the type "Adobe Acrobat Document" multiple times, an error message appears when the object is inserted.

If one of the error messages listed occurs, install the latest version of Adobe Acrobat Reader.

You can download the Adobe Acrobat Reader free of charge from the following URL:

- <http://www.adobe.com/products/acrobat> (<http://www.adobe.com/products/acrobat>)

I/O fields copied from WinCC < V7.3: No data format "Date/Time"

When you copy an I/O field created in WinCC < V7.3, the "Date/Time" data format is not available for the pasted I/O field.

Pictures with transparent areas: Using file formats with alpha channel

If you want to use a graphic for Direct2D display which contains transparent areas, use only graphic formats with an alpha channel, e.g. BMP or PNG.

Information on the logging system

Print barcode: "Code 39 Logitogo" font

The "Code 39 Logitogo" font is language-dependent.

If you are using this font in a layout, not all languages may be printed correctly.

Solution

To print barcodes, use the "Version for MS Dynamics German + English" font.

This font is language-independent. The barcodes are printed even if the computers have different language settings.

More information is available from Product Support under the entry ID 109750328:

- SiePortal: FAQ 109750328 (<https://support.industry.siemens.com/cs/ww/en/view/109750328>)

Information on VBA**VBA updates**

The user is solely responsible for the installation of updates for VBA.

The corresponding updates for VBA are made available by Microsoft on the download pages. Siemens does not supply any updates from Microsoft.

Install the updates for VBA after installing WinCC.

Notes on the channels**Name of a channel with national characters**

When you enter a name with national characters in the "SIMATIC S7 Protocol Suite" channel and especially in the "Named Connections" channel unit, you must have set the corresponding code page in the language options of the operating system.

See also

Scope of delivery (Page 7)

SiePortal: FAQ 109750328 (<https://support.industry.siemens.com/cs/ww/en/view/109750328>)

1.2.3.3 Information on WinCC runtime**Information on multi-user systems****Copying large amounts of data via the terminal bus**

Copying larger amounts of data on a computer connected to a terminal bus can effect communication in a multi-user system. One of the possible causes is the use of hubs with a low data throughput.

Information on Tag Logging / Alarm Logging

Editing archive data already saved

Archived measured values/messages of previously saved archives cannot and should not be changed due to reasons of data security and consistency.

WinCC controls: CSV export of Runtime data

If the CSV file reaches a size of 128 MB during the export, the data records are transferred incompletely.

You can find additional information on the truncated data records in the following log file:

- <Installation directory>\WinCC\Diagnose\WinCC_Sys_02.log
Parameter: ms_dwMaxClientCallbackDataSizeMaximum

Information on OPC

SIMATIC WinCC OPC Server: Automatic assignment of DCOM rights

The DCOM rights required for operation of the OPC server are assigned automatically. The settings are performed during the installation. Depending on the WinCC operating mode, further configurations are performed.

You must not edit these settings manually.

No deinstallation of SIMATIC WinCC OPC Server when the OPC channel is used

When you use the OPC channel, you must not remove the SIMATIC WinCC OPC DA Server.

OPC tags: Timestamp for Alarm Logging and Tag Logging

If messages are triggered by OPC tags, the message timestamp is used by the OPC server, comparable to chronological reporting.

For Tag Logging the timestamp is generated by the Tag Logging server.

OPC Data Access

During operation of the OPC DA server on the WinCC client:

While the connection of the OPC client is being established, the WinCC server with which the OPC client exchanges data must be in Runtime.

If the WinCC server is deactivated, not all properties of the items will be provided.

Since the display of data types in OPC Item Manager requires a lot of time, the display should be turned off if it is not needed.

OPC Historical Data Access

Return value "OPC_E_MAXEXCEEDED" for archive access

If the OPC client demands data from more than 2000 values during synchronous or asynchronous reading, the call is rejected with a return message OPC_E_MAXEXCEEDED.

This limit serves to limit the computer load and duration of the call.

This restriction does not apply if the entire time range is read.

OPC Alarm&Event

Avoid bounding values

Avoid using bounding values when reading historical alarms via the WinCC-OPC-A&E-server.

Otherwise, processing read access requests can take a long time, depending on the size of the archive.

Filtering messages when using format instructions in the user text block

The OPC source of a message is shown in an user text block. This is user text block 2 with the default setting.

If you use format instructions in this user text block, you need to use wild cards for the filter setting.

This ensures correct filtering when the OPC sources are generated dynamically in Runtime.

1.2.3.4 Information on Smart tools

WinCC Configuration Studio: Replacement of SmartTools

Compared to earlier WinCC versions, the following SmartTools have been replaced by the editors in the WinCC Configuration Studio:

SmartTool	WinCC Configuration Studio
Tag Export/Import	Export/import function of the "Tag Management" and "Tag Logging" editors
WinCC ConfigurationTool	
WinCC Archive ConfigurationTool	
Tag simulator	WinCC TAG Simulator

WinCC ConfigurationTool / WinCC Archive ConfigurationTool

As of WinCC V7.3 you import and export the WinCC data via the WinCC Configuration Studio.

To import already existing files from the WinCC Configuration Tool/WinCC Archive ConfigurationTool into the WinCC Configuration Studio, use the menu command "Import" in the WinCC Configuration Studio.

In addition to the file name, select the "ConfigTool file (*.xlsx)" or "Archive Config Tool file (*.xlsx)" entry in the file selection dialog.

1.2 WinCC Release Notes

If you have configured the colors of message types in the WinCC Configuration Tool, the colors are not imported into the WinCC Configuration Studio from the Configuration Tool. You either need to create the message colors in the WinCC project before migrating the WinCC project to WinCC V7.3 and higher or, alternatively, manually configure the message colors later after the import in the WinCC Configuration Studio.

Tag Export/Import

To export tags from a WinCC project or import them into a WinCC project, use the WinCC Configuration Studio.

For compatibility reasons, the "Tag Export/Import" tool is still included in the "uTools" installation path.

Information on the Dynamic Wizard Editor

Opening the Dynamic Wizard Editor

The Dynamic Wizard Editor and the Graphics Designer should not be opened at the same time.

1.2.3.5 Information on process communication

Information on the WinCC "SIMATIC S7 Protocol Suite" channel

Process communication with an S7-300 via "SINUMERIK" instead of "SIMATIC S7 Protocol Suite"

As of WinCC V8.1, communication with a PLC S7-300 is configured via the "SINUMERIK" communication channel.

After migrating to WinCC V8.1, you will find S7-300-type PLCs configured in older versions under the "SINUMERIK" communication channel.

S7DOS configuration: Enabling the IPv4 protocol

If using S7DOS, you will require the IPv4 protocol as of the "S7DOS V9" version.

Therefore, leave the IPv4 protocol enabled in the Ethernet properties for the network adapter or the SIMATIC Ethernet CPs.

In this way, you ensure that the S7DOS module detection works for the TCP, RFC1006, and ISO protocols.

PROFIBUS: Number of connections

With WinCC V7/V8, up to 8 MPI connections or PROFIBUS Softnet connections, for example, CP5622, are licensed. Additional PROFIBUS Softnet licenses are not required.

With a corresponding SIMATIC NET license, you can also create more than 8 PROFIBUS connections. You need PROFIBUS Hardnet for this, for example, CP5623.

Time change on an S7 automation system when using AR_SEND

Archive data transferred from the S7-AS to WinCC with AR_SEND is ignored if the time is reset on the AS, e.g. following time synchronization. This is because the archive already contains the reset time period.

Information on the WinCC "WinCC-OPC-UA" channel

OPC UA: Displaying imported OPC UA tags

Tags created with a WinCC version older than V7.4 are shown as imported in the "Symbols" view of the Configuration Studio.

However, in this case "Raw data" tag types are not shown as imported. The "Access" column is disabled, although these tags have been correctly created in the Tag Management.

Reimport these tags and delete the incorrectly displayed tags in the Configuration Studio.

WinCC OPC UA server: Methods - Output parameters

When you address VB scripts using OPC UA, the output parameters of the scripts always have the data type "Variant".

The OPC UA client always receives the output value as "Variant" in the response to the call.

The client extracts the correct data type of the output value from the received variant.

Migrated projects: Updating the OpenSSL version for WinCC OPC UA

OpenSSL 3.0 is used for WinCC OPC UA as of the following WinCC versions:

- WinCC V7.5 SP2 Update 15
- WinCC V8.0 Update 3
- WinCC V8.1

If the OPC UA certificate of an HMI device was created with a WinCC version that does not yet use OpenSSL 3.0, the certificate becomes incompatible when the device is upgraded.

Recreate the certificate.

HMI device uses CA-based certificate

The OPC UA certificate of the HMI device was created using WinCC Certificate Manager.

1. Upgrade the certificate authority device and the HMI device.
2. Recreate the OPC UA certificate of the HMI device on the certificate authority device using WinCC Certificate Manager.
3. Install the certificate on the HMI device using WinCC Certificate Manager.

HMI device uses a self-signed certificate

1. Delete the certificate from the certificate storage before upgrading the HMI device:
 - OPC UA client certificate:
C:\Program Files (x86)\Siemens\WinCC\opc\UAClient\PKI
 - OPC UA server certificate:
C:\Program Files (x86)\Siemens\WinCC\opc\UAServer\PKI
 - If you use the WinCC/Connectivity Pack with a WinCC Connectivity Station, delete the WinCC Connectivity Station server certificate:
C:\Program Files (x86)\Siemens\ConnectivityStation\OPC\UAServer\PKI\CADelete both the DER file and the PFX file.
2. Upgrade the HMI device.
The OPC UA server certificate on the HMI device is automatically created and installed.
3. Start Runtime and establish the connection between the OPC UA client and OPC UA server.
The OPC UA client certificate is automatically created and installed.
4. Trust the certificate on the communication peers.

HMI device uses CA-based certificate created with a third-party tool

The OPC UA certificate of the HMI device was created with a third-party tool.

1. Migration of WinCC versions prior to V8.0:
If needed, delete the root certificate of the third-party vendor and the OPC UA application certificate from the certificate storage before upgrading the HMI device:
 - OPC UA client certificate:
C:\Program Files (x86)\Siemens\WinCC\opc\UAClient\PKI
 - OPC UA server certificate:
C:\Program Files (x86)\Siemens\WinCC\opc\UAServer\PKI
 - If you use the WinCC/Connectivity Pack with a WinCC Connectivity Station, delete the WinCC Connectivity Station server certificate:
C:\Program Files (x86)\Siemens\ConnectivityStation\OPC\UAServer\PKI\CADelete both the DER file and the PFX file of the application certificate.
2. Upgrade the HMI device.
3. Upgrade the third-party tool to a version that uses OpenSSL 3.0.
4. Recreate the OPC UA certificate of the HMI device with the tool.
5. To install the certificate on the HMI device, copy it to the certificate storage on the HMI device:
 - OPC UA client certificate:
C:\Program Files (x86)\Siemens\WinCC\opc\UAClient\PKI
 - OPC UA server certificate:
C:\Program Files (x86)\Siemens\WinCC\opc\UAServer\PKI
 - If you use the WinCC/Connectivity Pack with a WinCC Connectivity Station, copy the certificate to the WinCC Connectivity Station:
C:\Program Files (x86)\Siemens\ConnectivityStation\OPC\UAServer\PKI\CA

If the communication partner already trusts the root certificate of the certificate authority, it automatically also trusts the newly created OPC UA certificate of the HMI device.

Information on the "SIMATIC S7-1200, S7-1500 Channel" WinCC channel

No raw data communication with S7-1200/S7-1500 controllers

The "SIMATIC S7-1200, S7-1500 Channel" channel does not support any raw data communication via the S7 communication "BSEND/BRCV" function.

Information on the WinCC "Mitsubishi Ethernet" channel

Bit addressing with incorrect data type

Ensure that the bit addressing has the correct data type.

Incorrect addressing can result in the incorrect data type being written and as a result the adjacent bits being influenced.

The addressing of, for example a BOOL address with the data type WORD can result in the adjacent bits of the addressed bit being overwritten.

Information on the WinCC "SIMATIC S5 PROFIBUS DP" channel

PROFIBUS DP and SIMATIC Net V14

In order to use the "PROFIBUS DP" channel with SIMATIC Net V14, you must disable the "OPC UA" property for the "DP" protocol in the communication settings of SIMATIC Net V14.

Information on the WinCC "SIMATIC 505 TCPIP" channel

LMode and LStatus data types

The channel has been extended by the data types LMode and LStatus.

- LMode (loop mode): unsigned 16-bit value (bit array); access: read and write
- LStatus (loop status): unsigned 16-bit value (bit array); access: Read ONLY

The offset to be specified during addressing identifies the loop whose mode or status should be requested.

1.2.3.6 Remote access and Remote Desktop Protocol (RDP)

Remote access to WinCC stations

You can find current instructions for remote access in the FAQ 78463889:

- SiePortal: Remote access to WinCC stations (<http://support.automation.siemens.com/WW/view/en/78463889>)

For more information on remote configuration in the WinCC Information System:

- "Configurations > Distributed systems > Remote configuration"

Released scenarios

The following scenarios have been tested:

- WinCC as single-user system
- WinCC as distributed system
- WinCC in redundant mode
- WinCC/WebUX server

You can also use communication via OPC in the released scenarios.

Use of RealVNC

For instructions on how to use "RealVNC", refer to FAQ 55422236:

- SiePortal: Access via "RealVNC" to WinCC stations and PCS 7 stations (<https://support.automation.siemens.com/WW/view/en/55422236>)

No keyboard lock with RealVNC

With "RealVNC", the keyboard lock is not supported.

The keyboard lock is only in effect with a Remote Desktop Protocol connection.

Remote maintenance of WinCC systems via RDP

Use of the Remote Desktop Protocol (RDP) is only permitted when the WinCC server or the single-user system is running in WinCC ServiceMode.

Restrictions when using RDP

The following restrictions apply when using RDP:

- Start the WinCC project with a user which is a member of the local "SIMATIC HMI" user group. This means that all services are started when operating via the remote console. More information is available under "Configurations > WinCC ServiceMode"
- Use in integrated operation in SIMATIC Manager is not released.

NOTICE
Data loss after interruption of the remote desktop connection
When the remote desktop connection is interrupted, for example, because the network cable was removed from the computer of the Remote Desktop Client, the archives and the OPC server, among others things, will no longer receive values from the data manager.
This status will persist until the connection has been restored, or the timeout of approximately 35 seconds has expired.

Starting the Remote Desktop

You can access WinCC systems with a Remote Desktop client via a console session.

Access via the Remote Desktop Protocol may only be gained by means of console takeover with the same user, or initial login.

User groups and access rights

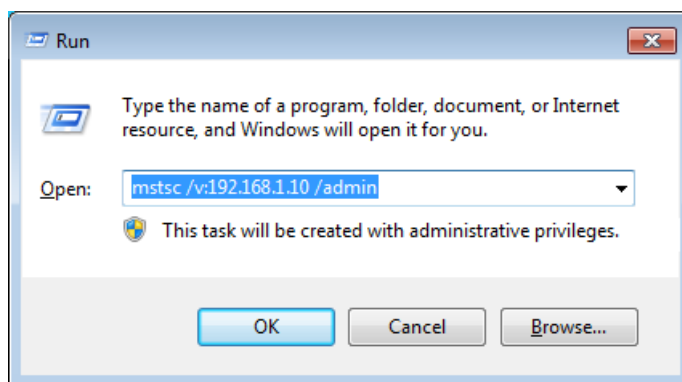
All "Remote Desktop" users must be members of the "SIMATIC HMI" user group on the target PC.

Procedure

1. To start a console session, open the "Run" dialog, for example, with <Windows button+R>.
2. Enter the following command:

– `mstsc /v:<Server> /admin`

Enter the computer name or the IP address as server.



For information on more parameters, enter the following command:

– `mstsc /?`

Migration: Migrate WinCC projects remotely only with UNC paths

To migrate WinCC projects remotely, use only UNC paths.

Release the project path or the folder above it.

Use this UNC path as project directory for the WinCC Project Migrator.

See also

Notes on Data and System Security (Page 25)

SiePortal: Remote access to WinCC stations (<http://support.automation.siemens.com/WW/view/en/78463889>)

SiePortal: Access via "RealVNC" to WinCC stations and PCS 7 stations (<https://support.automation.siemens.com/WW/view/en/55422236>)

1.2.3.7 Ports and protocols

Network settings

The following table shows network ports that are used for internal and external communication. These ports cannot be used in any other way.

The setup configures the ports for the firewall in such a way that smooth operation is ensured. The default settings for port and protocol refer to the state after installation.

Note

Assigning TCP/IP port numbers

Accept the default port numbers without changing them.

If the port numbers are changed due to company IT administration specifications, the user is responsible for ensuring that no collisions occur.

Port assignments

The list is not complete. Depending on the installed products and the components used, additional network ports can be occupied.

Service	Port number	Transport protocol	Communication direction	Function	Description
Client-server communication					
SCS Secure Communication	8910	TCP/UDP	Inbound Outbound	Client-server communication (encrypted)	
RPC	*	UDP	Inbound Outbound	Client-server communication (CCAgent, unencrypted)	
RPC	*	UDP	Inbound Outbound	Client-server communication (CCEServer/CCEClient, unencrypted)	
HTTPS	443	TCP	Inbound Outbound	WinCC/WebUX	Secure communication with a Web server
HTTPS	4430	TCP	Inbound Outbound	WinCC/WebNavigator WinCC/DatatMonitor	Secure communication with a Web server
SQL server					
SQL	1442	TCP	Inbound Outbound	Remote access to a WinCC instance	
OPC UA					

Service	Port number	Transport protocol	Communication direction	Function	Description
OPC UA Service	4861	TCP	Inbound	OPC UA server (OPC UA server for Connectivity Station)	Primary communication via OPC UA The service is enabled and configured during installation.
OPC UA Service (WinCC)	4862	TCP	Inbound	OPC UA server (OPC UA server for WinCC)	Primary communication via OPC UA The service is enabled and configured during installation.
OPC UA Discovery	4840 52601	TCP	Inbound	OPC UA server (LocalDiscovery)	Provides information about installed OPC servers The service is installed and configured by the OPC UA server.
Additional components					
RFC 1006	102	TCP	Outbound	S7 channel	Communication with the S7 controller via Ethernet/PROFINET
DCOM	135	TCP	Inbound	OPC server	Part of the Microsoft Windows operating system Since communication via OPC (DA) is based on DCOM, the service is required to initialize OPC (DA) connections.
DCOM	*	TCP	Inbound	OPC server	Communication via OPC (DA) is based on DCOM and uses unspecified ports assigned by the system. Take this into account when using OPC (DA) and creating rules for firewalls.
NetBIOS Name Service ¹⁾	137	UDP	Inbound	OPC server	Part of the Microsoft Windows operating system Access to this service is required, for example, for browsing.
NetBIOS ¹⁾	138	UDP	Inbound	OPC server	Part of the Microsoft Windows operating system Access to this service is required, for example, for browsing.
NetBIOS Session Service ¹⁾	139	TCP	Inbound	Server-client communication	
SMB ²⁾	445	TCP	Inbound	Server-client communication	
ALM	4410 ³⁾	TCP	Inbound Outbound	License service	Functionality for software licenses The service is used by the Automation License Manager as well as by all license-relevant software products.
Unified Collaboration	5678	TCP	Inbound Outbound	WinCC Unified Collaboration	

* Port is assigned automatically (dynamic port number)

1.2 WinCC Release Notes

- 1) When resolving the computer name via WINS, the "NetBIOS Name Service" and "NetBIOS Session Service" services must be enabled.
- 2) The Microsoft Windows File Share Protocol is used for ES/OS loading. Ensure that the "SMB" service is enabled.
- 3) Default port that can be changed by user configuration.

See also

Microsoft SQL Server for WinCC (Page 23)

Notes on Data and System Security (Page 25)

1.2.4 Notes on WinCC Redundancy

Notes on redundant systems

Redundancy behavior in case of double failure

Double failures are not covered by redundancy.

A double failure occurs, for example, when the terminal bus was pulled on server 1 while server 2 was deactivated.

Delay in swapping out archives

The swapping of archives will be delayed if a redundant partner is not available or deactivated.. Swapping of archives will not start or continue until the partner is available once again and after archive synchronization.

An extended failure of the redundant partner may result in data loss, because the memory capacity of the circular buffer for Tag Logging and Alarm Logging is limited.

No reloading of messages after network failure

The reloading of messages after network failure is not permitted for redundant systems.

Configuring used standard gateway

For redundancy, it is recommended to configure a standard gateway for the correct detection of failure scenarios. The standard gateway must be properly configured on both redundancy servers for this. This can be done manually or via DHCP.

For a configured standard gateway, ensure that this gateway cannot only be reached but is also accessible using a "ping".

Use of DHCP: Starting computer only with active network connection

If you are using DHCP on the terminal bus network card, note the following in a redundant system:

The computer must obtain a valid IP address from the DHCP server during startup.

Otherwise, the redundancy status is always indicated as "fault". This status can only be reset by restarting the computer.

Message sequence report in a redundant system

If you output a message sequence report on a client, you may encounter problems during logging when switching to the redundant partner.

1.2.5 Notes on Process Control Options

Creating a New Project

If you create a new project manually, you must first run the OS Project Editor.

While creating an OS using PCS 7 Engineering Station, the OS project editor is automatically called in the background and initialized using the default settings.

Removing unneeded "@*.PDL" pictures before migration

If the OS Project Editor has processed a WinCC project, the "@*.PDL" pictures of Basic Process Control will have been installed in the Graphics Designer.

If you do not need these pictures following the migration, you not only have to remove the "*@.PDL" pictures prior to migration, but also the "PAS" files and "SSM.cfg".

After the migration, the files from Basic Process Control are no longer added.

Multiple languages

Online documentation in the WinCC Information System is available only in English, French, German and Chinese (Simplified, PR China).

If you work with a French, English or German version of Microsoft Windows computer software and install a different language, it is possible that terms in WinCC appear in this language even if WinCC is operated with the same language as Microsoft Windows.

Different buttons have English labels especially in the multi-lingual versions of Microsoft Windows independent of the language setting and independent of the WinCC language. This affects dialog boxes in particular which the user must respond with Yes/No, OK/Cancel etc.

Tags with @ prefix

Project engineers may not create any tags with @ prefix. This is reserved for the WinCC-PCS 7 software.

1.2 WinCC Release Notes

You are not allowed to manipulate these system tags.

The system tags are required so that the product works properly.

While configuring AS and OS monitoring using Lifebeat Monitoring, device names should not be identical to area names in Picture Tree or internal tags with the "@" name prefix.

Area names in Alarm Logging and in the Picture Tree

Area names in Alarm Logging and in Picture Tree must not contain any spaces at the beginning or end.

Area names in distributed systems

With distributed systems, the area names in the projects of the various WinCC servers must be unique in order to ensure correct filtering and display of the messages according to the area.

Process picture in the plant view: Level 16 is hidden

Level 16 is always hidden when you create a new process picture in SIMATIC Manager in the plant view or with the WinCC Explorer.

Do not change this setting if you are using PCS 7 ASSET. The hidden level contains an "@RTBehaviourParams" object that is used for diagnostic purposes.

Image painting time

To optimize the image painting time, set the "WinCC Classic" design in the WinCC project properties.

User authorization "No. 8 Controlling archives"

User authorization "No. 8 Controlling archives" in User Administrator is no longer used by the system.

Authorization check in WinCC ServiceMode

There are three possible scenarios for WinCC in ServiceMode that influence the Runtime behavior through the authorization check:

- No Microsoft Windows user is logged on.
A user is defined as "User in service context" in WinCC User Administrator.
The authorizations of this user in the service context will be checked in Runtime. This setting will influence the trigger authorization for the signaling device.
- No Microsoft Windows user is logged on.
No user is defined as "User in service context" in WinCC User Administrator.
The signaling device will always be activated in Runtime.
- A Microsoft Windows user is logged on. Interactive user inputs are possible.
If a user is defined in the service context does not have an effect in Runtime.
The authorizations of the logged on WinCC user will be checked in Runtime.

Lifebeat Monitoring: Direct WinCC connection instead of OPC DA connection

Use the direct connection from WinCC to PC to configure the Lifebeat Monitoring

As of WinCC V8.1 you do not require an OPC DA connection between the WinCC stations anymore.

1.3 WinCC/Connectivity Pack Installation Notes

1.3.1 Connectivity Pack licensing

Introduction

The WinCC/Connectivity Pack enables licensed access to online and archive data of WinCC.

The Connectivity Pack includes licenses for access using:

- WinCC OPC-DA Server
- WinCC OPC HDA Server
- WinCC OPC A&E Server
- WinCC OPC UA Server
- WinCC REST communication
- "WinCC Unified Channel" WinCC channel

Starting from WinCC/Connectivity Pack V7.0, a WinCC Client Access License (WinCC/CAL) is no longer required.

1.3.2 Installation of the Connectivity Pack Server

Introduction

The installation of the Connectivity Pack server includes the following components:

- WinCC OLE DB Provider
- Microsoft SQL Server 2022 64-bit
- "Automation License Manager" for Management of WinCC Licenses
- WinCC Archive Connector
- WinCC DataConnector
- WinCC Basic Components
- Documentation
- Examples

Requirement

- Hardware requirement:
Observe the hardware requirements of WinCC V8.1 for WinCC servers.
- Operating system:
 - Microsoft Windows 10 Pro / Enterprise / Enterprise LTSC (max. 3 clients) 64-bit
 - Microsoft Windows 11 Pro / Enterprise (max. 3 clients) 64-bit
 - Microsoft Windows Server 2019 Standard / Datacenter 64-bit
 - Microsoft Windows Server 2022 Standard / Datacenter 64-bit
- Microsoft Message Queuing is installed and configured during WinCC installation.
- For access to WinCC RT archives, WinCC V8.1 must be installed.

Note

To use more than three clients, you must install the server version.
With the workstation version, you can use max. three clients.

Procedure

1. In order to configure a computer as Connectivity Pack Server, run the Connectivity Pack Server setup on the computer.
2. Select the "ConnectivityPack-Server" entry on the WinCC Product DVD in the "Program Packages" dialog.

Licensing

For operation of the Connectivity Pack Server, the license for the WinCC Connectivity Pack option is required.

Access rights

All users of the WinCC/Connectivity Pack have to be included in the Microsoft Windows user group "SIMATIC HMI".

The user has to be a member of the user group "SIMATIC HMI" on the Connectivity Pack server for remote access of a Connectivity Pack client.

1.3.3 Installation of the Connectivity Pack Client

Introduction

The installation of the Connectivity Pack Client includes the following components:

- WinCC OLE DB Provider
- WinCC DataConnector
- SQL Connectivity Tools
- Documentation

Note

In order to install the SQL Connectivity Tools, you will need administrator rights on the computer.

Requirement

- Operating system:
 - Microsoft Windows 10 Pro / Enterprise / Enterprise LTSC 64-bit
 - Microsoft Windows 11 Pro / Enterprise 64-bit
 - Microsoft Windows Server 2019 Standard / Datacenter 64-bit
 - Microsoft Windows Server 2022 Standard / Datacenter 64-bit
- Microsoft Message Queuing is installed and configured during WinCC installation.

Procedure

1. In order to configure a computer as Connectivity Pack Client, run the Connectivity Pack Client setup on the computer.
2. Select the "ConnectivityPack-Client" entry on the WinCC Product DVD in the "Program Packages" dialog.
3. If WinCC V8.1 is already installed on the client, an additional installation of the Connectivity Pack Client is not required.

Access rights

All users of the WinCC/Connectivity Pack have to be included in the Microsoft Windows user group "SIMATIC HMI".

The user has to be a member of the user group "SIMATIC HMI" on the Connectivity Pack server for remote access of a Connectivity Pack client.

1.4 WinCC/Connectivity Pack Release Notes

1.4.1 Information on the Connectivity Pack

Content

These release notes contain important information.

The statements in these release notes take precedence over information provided in the manuals and in the online help.

Please read these release notes carefully as they contain useful information.

Exchange of data between OPC client and Connectivity Station via OPC UA

The OPC UA server on a WinCC Connectivity Station can be reached via this address:

- "opc.tcp://[HostName]:[Port]"

HostName	Placeholder for the computer name. The name is entered automatically.
Port	Port number. The default is "4864".

Limitation for use of WinCC OLEDB Provider

As of WinCC V7.2, the function "Import" via the interface "WinCC OLEDB Provider" does not run in MS Office Excel.

1.5 WinCC/DataMonitor Installation Notes

1.5.1 Requirements of installing DataMonitor

Introduction

Certain hardware and software configuration requirements must be fulfilled for installation.

Note

A DataMonitor server cannot be operated on a WinCC client without a project of its own.

Only use a DataMonitor server on a computer which is not operated in WinCC ServiceMode.

Hardware requirements

To work with WinCC/DataMonitor efficiently, select a system that meets the recommended specifications for an optimum configuration.

DataMonitor server

		Minimum	Recommended
DataMonitor server on WinCC server for more than 10 clients	CPU	Dual core CPU; 2.5 GHz	Multi core CPU; 3.5 GHz
	Work memory	4 GB	8 GB
DataMonitor server on WinCC server with WinCC project in runtime	CPU	Dual core CPU; 2.5 GHz	Multi core CPU; 3.5 GHz
	Work memory	4 GB	8 GB
DataMonitor server on WinCC server	CPU	Dual core CPU; 2.5 GHz	Multi core CPU; 3.5 GHz
	Work memory	4 GB	> 4 GB
DataMonitor server on WinCC single-user system or WinCC client with its own project	CPU	Dual core CPU; 2.5 GHz	Multi core CPU; 3.5 GHz
	Work memory	4 GB	> 4 GB

DataMonitor client

	Minimum	Recommended
CPU	Dual core CPU; 2 GHz	Multi core CPU; 3 GHz
Work memory	1 GB	2 GB

Software requirements

Certain requirements concerning operating system and software configuration must be met for the installation.

Microsoft Internet Information Service (IIS)

During the WinCC installation, the Microsoft Internet Information Service (IIS) is installed and configured.

DataMonitor server on WinCC server

Operating system	Software
Microsoft Windows Server 2019 Standard / Datacenter 64-bit Microsoft Windows Server 2022 Standard / Datacenter 64-bit	WinCC Basic System V8.1 or WinCC File Server V8.1

If you want to publish Intranet information, the following is required:

- A network-capable computer with a LAN connection
- A system that converts computer names into IP addresses. This step allows users to use "alias names" instead of IP addresses when connecting to your server.

If you want to publish information on the Internet, the following is required:

- An Internet connection and an IP address from your Internet service provider (ISP). You can only publish information in the Internet, if you have a connection to the Internet provided by the ISP.
- A network adapter that is suitable for connecting to the Internet.
- A DNS registration for your IP address. This step allows users to use "alias names" instead of IP addresses when connecting to your server.

DataMonitor server on WinCC single-user system or WinCC client with its own project

Operating system	Software
Microsoft Windows 10 Pro / Enterprise / Enterprise LTSC 64-bit (max. 3 clients) Microsoft Windows 11 Pro / Enterprise 64-bit (max. 3 clients) Microsoft Windows Server 2019 Standard / Datacenter 64-bit Microsoft Windows Server 2022 Standard / Datacenter 64-bit	WinCC Basic System V8.1 or WinCC File Server V8.1 For the components "Excel Workbook Wizard" and "Excel Workbook": • Microsoft Office 2019 32-bit version, 64-bit version ¹⁾ • Microsoft Office 2021 32-bit version, 64-bit version ¹⁾ • Microsoft Office 365 32-bit version, 64-bit version ¹⁾

1) ActiveX controls that were created with a 32-bit version are not compatible with the 64-bit version of Microsoft Office 365. You can only use the Excel add-in with the 32-bit version of Microsoft Office 365.

You also need access to the Intranet/Internet or a TCP/IP connection to the Web client.

DataMonitor client

Operating system	Software
Microsoft Windows 10 Pro / Enterprise / Enterprise LTSC 64-bit Microsoft Windows 10 Pro / Enterprise 64-bit Microsoft Windows Server 2019 Standard / Datacenter 64-bit Microsoft Windows Server 2022 Standard / Datacenter 64-bit Also other operating systems via MS Terminal Services	For the components "Excel Workbook Wizard" and "Excel Workbook": • Microsoft Office 2019 32-bit version, 64-bit version ¹⁾ • Microsoft Office 2021 32-bit version, 64-bit version ¹⁾ • Microsoft Office 365 32-bit version, 64-bit version ¹⁾

1) ActiveX controls that were created with a 32-bit version are not compatible with the 64-bit version of Microsoft Office 365. You can only use the Excel add-in with the 32-bit version of Microsoft Office 365.

You also need access to the Intranet / Internet or a TCP/IP connection to the Web server.

1.5.2 User rights for installing the DataMonitor client

Introduction

You can install the DataMonitor client as follows:

- Installation from the product DVD
In this case, certain Microsoft Windows user rights are required, depending on the operating system.
- Installation via the Intranet/Internet
In this case, certain Microsoft Windows user rights are required, depending on the operating system.
- Installation using the group policy-based software distribution in networks
This can be done without any user interaction and using the Microsoft Windows user rights of the current user.

Microsoft Windows user rights required for installation and initial logon of the client

Depending on the operating system, specific minimum user rights are required to install the DataMonitor client via Intranet/Internet.

After installation, the client must log in with the following user identification for initial registration on the DataMonitor server:

- Under a user identification with Windows user rights higher or equal to those defined by the user identification that was given for the installation.

The connections must be established successfully. The subsequent logins can then be performed under a different Windows user authorization with possibly limited rights.

Minimum required user rights:

- Administrator

Installing the DataMonitor client with limited Microsoft Windows user rights

Using Microsoft Windows Installer technology (MSI), DataMonitor clients can also be installed with limited Windows user permissions, i.e. permissions other than "Power user" or "Administrator".

This procedure can be set during the installation using the group policy based software distribution in networks.

Even the add-ins and plug-ins for the DataMonitor client can be installed in this way. The minimum user permissions described above are also required to install plug-ins created with WinCC Plug-In Builder.

Using MSI technology, it is also possible to install the DataMonitor client for a configured group of users or computers.

Installation for a configured group of users or computers

The following is possible with the Microsoft Systems Management Server or a group policy on a Domain Controller:

- The installation for a group of users or computers configured by the administrator
 - To do this, the "WinCCDataMonitorClient.msi" MSI file is published on the domain controller and then released for a user group. The installation is then performed according to the configuration of the group policy based software distribution either during login of the defined users or when the computer is started.
 - When using a Microsoft Systems Management Server, the installation is configured by the administrator, triggered and executed when the relevant computer boots. Additional information on Microsoft Systems Management Server is available in the Internet on the Microsoft Homepage.

Group policy based software distribution

Software is normally installed with the access rights of the current Microsoft Windows user. When using MSI technology, the installation is performed by an operating system service with a higher level of 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.

In order to use the group policy-based software distribution, a group policy is created on the domain controller and assigned to the distributing software or published using Active Directory.

- Assignment: The software distribution can be assigned to a user or a computer. In this case, the software to be distributed is automatically installed when the user logs in or the computer is started.
- Publication: The software distribution can be published for single users. In this case, when the user logs onto the client computer, the software to be distributed appears in a dialog and can be selected for installation.

See also

Installing DataMonitor (Page 97)

1.5.3 Installing DataMonitor

Introduction

This section describes the installation of the DataMonitor server and DataMonitor client. Installation on the DataMonitor client depends on the DataMonitor tool used.

DataMonitor server scope of installation

A DataMonitor server is installed and set up as the web server to enable WinCC/DataMonitor to be used.

This installation allows you to access the WinCC Runtime archive using "Trends & Alarms".

Only "Webcenter" and "Trends & Alarms" are installed on a computer with WinCC file server, for example, used as a archive server, because the other components require WinCC Runtime. "Webcenter" and "Trends & Alarms" install all necessary components in the process.

Microsoft Internet Information Service (IIS)

During the WinCC installation, the Microsoft Internet Information Service (IIS) is installed and configured.

DataMonitor client installation conditions

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

You can install the Excel add-ins "ExcelWorkbook Wizard" and "Excel Workbook" individually under "Reports/Download area" on the DataMonitor start page for the "Reports".

"Microsoft Excel" is needed for "Excel Workbook". The following 32-bit versions of Office are released:

- Microsoft Office 2019
- Microsoft Office 2021
- Microsoft Office 365

Depending on the operating system, specific user rights may be required for installing the DataMonitor client. For more information, refer to "User rights for installing the DataMonitor client (Page 96)".

Note

Downloading the client setup

To save the client setup on the client computer, select the "Save" option when downloading the client software from the DataMonitor server. 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 has already been installed from DVD and you want to install an updated version of the client via the Intranet/Internet, you must save the client setup on the target computer.

64-bit computer as client

If the DataMonitor client is a 64-bit machine, you first need to install the required Visual C++ Redistributable, which is required for the DataMonitor client. Use the link that is displayed during installation via intranet/Internet.

The required Visual C++ Redistributable must also be available for domain environments as an "msi" package.

If the DataMonitor clients on the 64-bit computers are integrated in domain group policies, the users of the clients must install "DataMonitorClient_x64_AddOn.msi" themselves.

Excel Workbook Wizard requires Microsoft .Net Framework

In order to use Excel Workbook Wizard make sure that the .Net Framework is installed on the DataMonitor client.

Client installation on a DataMonitor server

Proceed as follows if you also wish to install the DataMonitor client or WebNavigator client on a DataMonitor server:

1. Use the Services Manager in Microsoft Windows to set the start type of the "CCArchiveConnMon" service to manual.
 2. Restart the computer.
 3. Install the client.
Ensure that no WebNavigator clients or DataMonitor clients access the server during installation.
 4. Switch the start type of the "CCArchiveConnMon" service back to automatic.
-

Requirement

- The DataMonitor server requires the Internet Information Services (IIS).
- The DataMonitor server requires the WinCC configuration data.
- You need Microsoft Windows "Administrator" rights to install the DataMonitor server.

Procedure

1. Insert the WinCC DVD into the DVD drive.
2. If the automatic execution of an autorun file is activated, after a few seconds the setup program starts automatically.
The setup can also be started manually in case the installation is performed from a network drive or the autorun function has been disabled.
The setup program is started.
3. To install, click the text "Install Software".
4. In the following dialog, select the component "DataMonitor Server" or "DataMonitor Client".
5. Follow the instructions of the setup program.

See also

User rights for installing the DataMonitor client (Page 96)

1.5.4 DataMonitor licensing

DataMonitor client

No license is required for the DataMonitor client on the computer.

The DataMonitor clients are licensed on the DataMonitor server. Install the license keys for the client access to the server on the DataMonitor server.

DataMonitor server

As a prerequisite for the WinCC basic system, the WinCC RT basic license is required.

Licenses are available for 1 / 3 / 10 / 30 clients that can simultaneously access the DataMonitor server. The licenses are cumulative.

A message will appear if the number of licensed clients is exceeded during a login attempt by a DataMonitor client. No further logins will be possible.

Note

The connection to the DataMonitor server is maintained if the user closes the DataMonitor start page without logging off with the "Log off" button.

The license remains allocated and is only released after approximately 20 minutes.

License count

DataMonitor distinguishes between the following function groups:

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

The following table shows the maximum number of clients or connections per license based on the function group. The values are valid only within a function group.

License	Excel Workbooks ¹⁾	Webcenter, Trends & Alarms, Reports ¹⁾
1 Client	1	3
3 Clients	3	6
10 clients	10	20
30 Clients	30	60

1) The same values apply even if you cumulate licenses.

In the following example, two licenses are installed on the DataMonitor server: "1 Client" a "3 Clients".

The following cumulative values apply depending on the selected function group:

Example: Excel Workbooks

Installed licenses	Function group	Maximum logged on users
"1 Client" + "3 Clients"	Excel Workbooks	4 users

Example: Webcenter, Trends & Alarms, Reports

Installed licenses	Function group	Maximum logged on users
"1 Client" + "3 Clients"	Webcenter, Trends & Alarms, Reports	8 users

No operation without a valid license

If no license is available, DataMonitor displays a page reporting the missing license.

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

Using DataMonitor versions prior to V7.4

DataMonitor versions up to V7.3 do not recognize licenses from DataMonitor V7.4 and higher.

Once you install the current DataMonitor licenses on a computer, a DataMonitor installation of a version prior to V7.4 is no longer licensed.

This also applies if you upgrade to the new cumulative licenses through an upgrade license. The upgraded licenses are no longer recognized by DataMonitor V7.3 or earlier versions.

The upgrade to DataMonitor V7.4 or higher cannot be reversed.

1.5.5 Setting up a secure connection over HTTPS

Introduction

You can configure the DataMonitor server in such a way that only HTTPS connections are supported.

In this way, you increase the security of your connections.

You need a digital certificate for the DataMonitor server to set up the secure connection.

Requirement

- The Microsoft Windows "Internet Information Service" component is installed.
- WinCC Web Configurator is installed.
- WinCC DataMonitor server is installed.
- A DataMonitor web page has been set up and the Web folder is created.

Creating an SSL certificate

1. Open the "Internet Information Services (IIS) Manager".
2. In the "Connections" navigation area, select the local computer.
The home page of the local computer is displayed in the data area.
3. On the home page of the local computer, double-click "Server certificates" under "IIS".
4. Select "Create a self-signed certificate..." in the "Actions" area.
The "Create a self-signed certificate" dialog opens.
5. Specify the name of the certificate.
6. Select the certificate store "Personal" for the certificate.
7. Confirm your entries with "OK".
The dialog closes.
The certificate has been created.

More information

You can find information on self-signed certificates when using different web browsers on the Internet under Entry ID 109773769:

- SiePortal: "How do you fix problems when using self-signed certificates from WebUX or WebNavigator with different web browsers?" (<https://support.industry.siemens.com/cs/ww/en/view/109773769>)

Setting up a secure connection

1. Open the "Internet Information Services (IIS) Manager".
2. Open the "Sites" folder in the "Connections" navigation area.
3. Select "WebNavigator".

4. Select the "Edit bindings" command in the shortcut menu.
The "Site bindings" dialog opens.
5. Select "Add...".
The "Add site binding" dialog opens.
6. Select the type "https".
7. Specify the required port.
8. Select the created certificate under "SSL certificate".
9. Confirm your entries with "OK".
10. Delete the binding of the type "http" in the "Site bindings" dialog.
11. Exit the configuration with "Close".
12. In the data area "Default Web Site Home", select the "SSL settings" under "IIS".
13. Activate the "Require SSL" option and select the setting for client certificates.
14. To test the connection, enter the URL and the port number in the Internet Explorer or in the WinCC Viewer RT, for example, "https://webserver:444".

See also

SiePortal: "How do you fix problems when using self-signed certificates from WebUX or WebNavigator with different web browsers?" (<https://support.industry.siemens.com/cs/ww/en/view/109773769>)

1.6 WinCC/DataMonitor Release Notes

1.6.1 Notes about DataMonitor

Notes about DataMonitor

These release notes contain important information.

The statements in these release notes take precedence over information provided in the manuals and in the online help.

Please read these release notes carefully as they contain useful information.

Using a secure connection over HTTPS

To improve the security of your communication, configure the DataMonitor server in such a way that only HTTPS connections are supported.

You need a digital certificate for the DataMonitor server for this purpose. Also use SSL certificates on the DataMonitor clients.

You can find more detailed information under "Setting up a secure connection over HTTPS (Page 102)".

System load through large amounts of data

Note that SQL queries returning large amounts of data can affect system functionality.

Select filter criteria which limit the amount of data in a useful manner.

Opening Excel workbooks on a computer not connected to the Internet

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

- Open Internet Explorer.
- Select the "Internet Options" command from the "Tools" menu.
- Click "Advanced".
- In the "Security" section, deactivate the setting "Check for publisher's certificate revocation".

Excel workbook functions and print jobs after deactivating and activating WinCC Runtime

If you deactivate WinCC Runtime and then reactivate it, you also need to restart the Web application.

Excel workbook: volume of requested data for archived values

Although you can limit the requested data volume with the "Data resolution" property, all data of the defined time period is initially used internally. This may have the result that the internal system limit is reached. Use compression archives to limit the data volume.

Web Client: Display of ActiveX controls in Internet Explorer

ActiveX controls are disabled in Internet Explorer by default. For this reason, the WinCC controls are not displayed correctly in Internet Explorer on a Web client.

To display the WinCC controls correctly, add the Web server as a trusted website and enable the ActiveX controls only for the "Trusted sites" zone.

To continue protecting Internet Explorer from foreign ActiveX controls, check that the restricted security settings still apply to the other zones after making the changes.

For more information, refer to the following documentation:

- WinCC/DataMonitor: "WinCC/DataMonitor Documentation > Configuring the DataMonitor System > Working with the DataMonitor Client > Configuring Security Settings in Internet Explorer"

DataMonitor server: Remote access to WinCC file server

Remove access from one DataMonitor server to a WinCC file server is possible only if the firewall is disabled on the WinCC file server.

Excel workbook: Local times on DataMonitor client and DataMonitor server

Note when requesting archive data that the local times on the server and client may differ if they have not been sufficiently synchronized, for example because automatic synchronization is not possible.

The DataMonitor client attempts to establish the current time of the DataMonitor server when archive data is requested. If it succeeds, the query will be based on the server time. For the display of data in the Excel table, the time stamp represents the server time but in the local time zone of the client.

If the query of the server time is unsuccessful, the DataMonitor client will base the time period of the query on its local time. An entry will also be made in the Microsoft Windows event display on the DataMonitor client. For the display of data in the Excel table, the time stamp represents the client time.

Excel workbook: Client on terminal server

In the case of operation on a terminal server, an Excel Workbook client will run in a session of the terminal services. A maximum of only 10 Excel workbook clients can be operated; otherwise, MS Excel will overload the computer.

Trends & Alarms: Display of archive data after copying a project

To copy a WinCC project between computers and then display the archive data of the project on the target computer in "Trends & Alarms", you will first need to copy the project using the WinCC Project Duplicator.

If you use Microsoft Windows Explorer rather than the Project Duplicator to copy the project, the runtime data will not be adapted to the target computer. The computer name of the source computer and not that of the target computer is displayed in the archive selection in "Trends and Alarms". The computer name of the target computer is displayed in the selection field only after the archive has been reset in Alarm Logging and Tag Logging.

See also

Setting up a secure connection over HTTPS (Page 102)

1.7 WinCC/WebNavigator Installation Notes

1.7.1 General information on the WebNavigator installation

Scope of delivery

You can find the following components for WinCC/WebNavigator on the WinCC DVD:

- WebNavigator server
- WebNavigator client
- WinCCViewerRT
- WebNavigator diagnostics client
- WinCC Web Publishing Wizard (PublishingWizard)
- WebNavigator Plug-In Builder
- Documentation
- Release notes

Note

WinCC/WebNavigator V8.1: Installation is only released on the basis of WinCC V8.1

You cannot install the V8.1 WebNavigator server/client on a computer with WinCC versions earlier than V8.1.

Nor can a WebNavigator server/client version older than V8.1 be installed on a computer with WinCC V8.1.

Note that mixed use of European and Asian versions of WinCC and WebNavigator is not permitted in the configuration.

1.7.2 WebNavigator installation requirements

1.7.2.1 Hardware and software requirements for WebNavigator

Introduction

This section describes the hardware and operating system requirements for WinCC/WebNavigator.

Notes on the software requirements

Microsoft Internet Information Service (IIS)

During the WinCC installation, the Microsoft Internet Information Service (IIS) is installed and configured.

WinCC client without its own project

A WebNavigator server cannot be operated on a WinCC client without a project of its own.

WebNavigator client

Hardware

	Minimum	Recommended
CPU	Dual core CPU; 2 GHz	Multi core CPU; 3 GHz
Work memory	1 GB	2 GB

Software

Operating system	Microsoft Windows 10 Pro / Enterprise 64-bit Microsoft Windows 10 Enterprise LTSC 64-bit Microsoft Windows 11 Pro / Enterprise 64-bit Microsoft Windows Server 2019 Standard / Datacenter 64-bit Microsoft Windows Server 2022 Standard / Datacenter 64-bit Also other operating systems via MS Terminal Services Microsoft Windows Embedded Standard 7 including SP1 in combination with SIMATIC IPC 4x7D and SIMATIC IPC 4x7E
Software	Web browser, current version
Other	Access to the intranet/Internet or a TCP/ IP connection to the WebNavigator server

WebNavigator server on a WinCC single-user system

Hardware

	Minimum	Recommended
CPU	Dual core CPU; 2.5 GHz	Multi core CPU; 3.5 GHz
Work memory	2 GB	> 4 GB

Software

Operating system	Microsoft Windows 10 Pro / Enterprise 64-bit Microsoft Windows 10 Enterprise LTSC 64-bit Microsoft Windows 11 Pro / Enterprise 64-bit Microsoft Windows Server 2019 Standard / Datacenter 64-bit Microsoft Windows Server 2022 Standard / Datacenter 64-bit
Software	Web browser, current version WinCC Basic System V8.1
Other	Access to Intranet/Internet or TCP/IP connection to the WebNavigator client

WebNavigator server on WinCC server or WinCC client with its own project**Hardware**

	Minimum	Recommended
CPU	Dual core CPU; 2.5 GHz	Multi core CPU; 3.5 GHz
Work memory	4 GB	8 GB

Software

Operating system	Microsoft Windows Server 2019 Standard / Datacenter 64-bit Microsoft Windows Server 2022 Standard / Datacenter 64-bit
Software	Web browser, current version WinCC Basic System V8.1
Other	Access to Intranet/Internet If you wish to publish on the Intranet , you will need a system that converts computer names into IP addresses. This step allows users to use alias names instead of IP addresses when connecting to the server. You will need DNS registration for your IP address if you wish to publish on the Internet . This step allows users to use alias names instead of IP addresses when connecting to the server.

WebNavigator diagnostics client**Software**

Operating system	Microsoft Windows 10 Pro / Enterprise 64-bit Microsoft Windows 10 Enterprise LTSC 64-bit Microsoft Windows 11 Pro / Enterprise 64-bit Microsoft Windows Server 2019 Standard / Datacenter 64-bit Microsoft Windows Server 2022 Standard / Datacenter 64-bit
Software	Web browser, current version
Other	Access to Intranet/Internet

See also

<https://support.microsoft.com/en-us/kb/3072449> (<https://support.microsoft.com/en-us/kb/3072449>)

1.7.2.2 Licensing WebNavigator

WebNavigator client

No license is required for the PC on which the WebNavigator client is running, as server licenses are available on the WebNavigator server.

WebNavigator server

As a prerequisite for the WinCC basic system, the WinCC RT basic license is required. No WinCC server license is required if no local WinCC clients are to be operated. Even when operating a WinCC client as a dedicated web server, you do not require a WinCC server license for the WinCC client.

Licenses are available for 1 / 3 / 10 / 30 / 100 clients. If you have upgraded a WebNavigator version prior to V7.4, there may also be licenses for 5 / 25 / 50 / 150 clients.

As of WinCC V8.1, there is also an "Unlimited" license for an unlimited number of connected clients.

The packages are version-independent and can be combined. Up to 150 clients can access the WebNavigator server simultaneously.

A message will appear if the number of licensed clients is exceeded during a login attempt by a WebNavigator client. No further logins will be possible.

WinCC/WebUX clients

If the WinCC/WebUX option is also used in the WinCC system, a WebUX client can also occupy a WebNavigator license. This reduces the number of available WebNavigator licenses.

You can find more information in the documentation for WinCC/WebUX.

Test mode

If there is no WebNavigator license or if the license has been removed, the WebNavigator server runs in Test mode.

Test mode runs for a maximum of 21 days from the date of installation. Once 21 days have expired after the installation, the WebNavigator server can only be started with an installed license.

WebNavigator diagnostics client

A "Diagnostics client" license is required on the client computer for the diagnostics client.

The diagnostics client can access on the WebNavigator server in the following cases:

- When the maximum number of simultaneous accesses has been reached on WebNavigator server.
- When no WebNavigator license is installed on the WebNavigator server.

Diagnostics client without corresponding license

If the diagnostics client is installed without the corresponding license, a message will appear about one hour after each start-up of the computer.

Install the diagnostics client license or remove the diagnostics client software.

No access via RDP

Access via Remote Desktop Protocol (RDP) is not enabled for the diagnostics client.

Note

Computer with WinCC basic system and diagnostics client

If you install a diagnostics client on a computer with the WinCC basic system, you will have to reinstall the diagnostics client after removing WinCC.

Overview of licenses for WebNavigator server and client

You can combine WebNavigator and diagnostics licenses.

Server	Client has no license ¹⁾	Client has diagnostics client license ¹⁾
No WinCC license No WebNavigator license	Client in test mode Unlimited number	Client in test mode Unlimited number
WinCC license No WebNavigator license	Client in test mode Unlimited number	Diagnostics client One license per diagnostics client
WebNavigator license No WinCC license	Client in test mode Unlimited number	Client in test mode Unlimited number
WebNavigator license + WinCC license	WebNavigator client Number up to maximum of the server license	Diagnostics client One license per diagnostics client
WebNavigator license + WinCC license + "Load Balancing" license	WebNavigator client Number up to maximum of the server license	Diagnostics client One license per diagnostics client
WebNavigator license + WinCC license + WinCC Redundancy license + "Load Balancing Step-Up" license	WebNavigator client Number up to maximum of the server license	Diagnostics client One license per diagnostics client

1) Note the behavior in test mode. Test mode runs for a maximum of 30 days from the date of installation.

Restarting the WebNavigator client after license modification

If the WebNavigator licenses on the WebNavigator server are modified, e.g. to a different number of clients, Internet Explorer must be restarted on each connected WebNavigator client, and the WebNavigator client must log in again. Otherwise, the WebNavigator client will switch to demo mode. This also applies to automatic reconnection of the WebNavigator client.

Using WebNavigator versions prior to V7.4

WebNavigator versions up to V7.3 do not recognize licenses from WebNavigator V7.4 and higher.

Once you install the current WebNavigator licenses on a computer, a WebNavigator installation of a version prior to V7.4 is no longer licensed.

This also applies if you upgrade to the new cumulative licenses through an upgrade license. The upgraded licenses are no longer recognized by WebNavigator V7.3 or earlier versions.

It is not possible to undo the upgrade to WebNavigator V7.4 or higher.

1.7.2.3 Requirements for the Use of Terminal Services

The WebNavigator client is released for Microsoft Windows Terminal Services.

A maximum of 150 sessions per terminal server are permitted.

Terminal server

Hardware

	Minimum	Recommended
CPU	Dual core CPU; 2 GHz	Multi core CPU; 3 GHz
Work memory	1 GB	2 GB

Note

Memory requirements

Each terminal client will increase the memory requirements and the processor load.

You must therefore ensure that the terminal server has adequate memory and processor load capacity.

Software

Operating system	Microsoft Windows Server 2019 Standard / Datacenter 64-bit Microsoft Windows Server 2022 Standard / Datacenter 64-bit It must be possible to repeatedly call and execute applications that are to be executed on the clients.
Miscellaneous:	If many users want to access the server, you will need to use a high-performance network card.

Terminal client

Minimum requirement:	Network adapter with TCP/IP Terminal client RDP 5.0 Display or monitor Pointing device
----------------------	---

Note

Terminal Services Client Access Licenses (CALs)

As with Microsoft Windows Server CAL, there are two different CAL terminal services:

- The TS device CAL enables a device to run user-independent Windows sessions on a Microsoft Windows Server.
- The TS user CAL enables a user to run device-independent Windows sessions on a Microsoft Windows Server.

A Microsoft Windows Server Terminal Server CAL "TS CAL" is required for every user or every device.

Additional information can be found in the Microsoft documentation "<https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/terminal-server-licensing>".

See also

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/terminal-server-licensing> (<https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/terminal-server-licensing>)

1.7.3 Installing a WebNavigator server

1.7.3.1 Overview: Installing the WebNavigator server

Requirements

- The software requirements for the Microsoft Windows operating system have been met.
- Local administrator rights.
- The WinCC basic system is installed.

NOTICE
WebNavigator server: Using a secure connection over HTTPS
To increase the security of your communication, configure the WebNavigator server in such a way that only HTTPS connections are supported. You need a digital certificate for your WebNavigator server for this.
You can find more detailed information under "Setting up a secure connection over HTTPS (Page 115)".

WinCC options previously installed

If you have already installed other WinCC options prior to the installation of WinCC/ WebNavigator, you may have to re-install these options.

See also

Installing the WebNavigator server (Page 114)

Setting up a secure connection over HTTPS (Page 115)

1.7.3.2 Installing the WebNavigator server

Requirements

- Local administrator rights
- The Internet Information Server is installed.

Procedure

1. Insert the WinCC DVD in the drive.
The DVD starts automatically if Autorun is enabled in the operating system.
If the autorun function is not activated, start the program Setup.exe on the DVD.
2. In the "Installation Type" dialog, select "Package Installation".
3. Select the "WebNavigator Server" installation.
4. Before the installation, the security settings that are adapted for WinCC are displayed in the "System Settings" dialog.
The firewall is configured automatically.
Confirm the changes to the system settings.
5. Start the installation.
You can track the status of the installation in the displayed dialog.
Select "Cancel" to cancel the installation.

6. You can transfer the license key for the product after installation of the WebNavigator server. To do so, click on "Transfer License Key". Select "Next" if you have already transferred the license key or want to install it at a later time.

Note

License keys will not be transferred automatically.

You will have to transfer missing license keys during or after installation with "Automation License Manager" .

7. Restart the computer when prompted to do so by setup.

Result

The WebNavigator server is installed and is displayed in the navigation window of the WinCC Explorer.

1.7.3.3 Setting up a secure connection over HTTPS

Introduction

You can configure the WebNavigator server in such a way that only HTTPS connections are supported.

In this way, you increase the security of your connections.

You need a digital certificate for the WebNavigator server to set up the secure connection.

Requirement

- The Microsoft Windows "Internet Information Service" component is installed.
- WinCC Web Configurator is installed.
- WinCC WebNavigator server is installed.
- A WebNavigator web page has been set up and the Web folder is created.

Creating an SSL certificate

1. Open the "Internet Information Services (IIS) Manager".
2. In the "Connections" navigation area, select the local computer.
The home page of the local computer is displayed in the data area.
3. On the home page of the local computer, double-click "Server certificates" under "IIS".
4. Select "Create a self-signed certificate..." in the "Actions" area.
The "Create a self-signed certificate" dialog opens.
5. Specify the name of the certificate.

1.7 WinCC/WebNavigator Installation Notes

6. Select the certificate store "Personal" for the certificate.
7. Confirm your entries with "OK".
The dialog closes.
The certificate has been created.

More information

You can find information on self-signed certificates when using different web browsers on the Internet under Entry ID 109773769:

- SiePortal: "How do you fix problems when using self-signed certificates from WebUX or WebNavigator with different web browsers?" (<https://support.industry.siemens.com/cs/ww/en/view/109773769>)

Setting up a secure connection

1. Open the "Internet Information Services (IIS) Manager".
2. Open the "Sites" folder in the "Connections" navigation area.
3. Select "WebNavigator".
4. Select the "Edit bindings" command in the shortcut menu.
The "Site bindings" dialog opens.
5. Select "Add...".
The "Add site binding" dialog opens.
6. Select the type "https".
7. Specify the required port.
8. Select the created certificate under "SSL certificate".
9. Confirm your entries with "OK".
10. Delete the binding of the type "http" in the "Site bindings" dialog.
11. Exit the configuration with "Close".
12. In the data area "Default Web Site Home", select the "SSL settings" under "IIS".
13. Activate the "Require SSL" option and select the setting for client certificates.
14. To test the connection, enter the URL and the port number in the Internet Explorer or in the WinCC Viewer RT, for example, "https://webserver:444".

See also

General information about WebNavigator (Page 128)

SiePortal: "How do you fix problems when using self-signed certificates from WebUX or WebNavigator with different web browsers?" (<https://support.industry.siemens.com/cs/ww/en/view/109773769>)

1.7.4 Installing the WebNavigator client

1.7.4.1 Installing the WebNavigator client

Introduction

You can install the WebNavigator client as follows:

- Installation from the WinCC product DVD.
In this case, certain Microsoft Windows user rights are required, depending on the operating system.
- Installation via the Intranet/Internet.
In this case, certain Microsoft Windows user rights are required, depending on the operating system.
- Installation without user interaction:
 - Using the Microsoft Windows user rights of the current user
 - Or in networks, using group policy-based software distribution

In addition, you can also install the WebNavigator client on the WebNavigator server.

This is useful, for example, if you want to check the WinCC project locally on the server in Internet Explorer.

Remote communication

If the WebNavigator client is not running on the same computer as the WebNavigator server, enable remote communication on both computers in the "Simatic Shell" dialog.

Note

.Net controls on the WebNavigator client

If you wish to use .Net controls on the WebNavigator client, you need to install the .Net Framework 4.0 or higher on the client from the WinCC product DVD.

The .Net controls must not be copied to the Microsoft Windows "Common Files" folder. Instead, use the following path:

- <Installation directory>WinCC\WebNavigator\Client\bin

Note

Parallel installation of WinCC/WebNavigator client and WinCC Runtime Advanced

Avoid the installation of the web client on a PC on which WinCC Runtime Advanced is installed as well.

If you run both installations on the same PC, you require administrator rights in order to work with the web client. No pictures are loaded into the web browser without administrator rights.

WinCCViewerRT

The web viewer "WinCCViewerRT" is installed upon installation of 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

If you are installing from the DVD or using software distribution based on group policy, you can directly upgrade an older version of the WebNavigator client without having to remove the older client first.

If you install the WebNavigator server on a PC after the WebNavigator client, you will have to install the client again.

Plug-in reinstallation

The plug-ins "User Archive Control", "FunctionTrend Control", "Hard Copy" and "Web Client" are already integrated in the WebNavigator client as of version V7.0 upon installation.

If a WebNavigator client as of V7.0 is connected to a WebNavigator server older than V7.0 (e.g. V6.2 SP3), you will be offered these plug-ins for installation in the download area of the Web navigation user interface.

The plug-ins are already installed. Do not reinstall these plug-ins.

Information on the setup and installation of the WebNavigator client:

- Before downloading and installing a new version on the WebNavigator client, check the languages installed on the client and connected server.
Only the languages of the connected server will be available on the client computer following client installation by download.
- WebNavigator client setup will be 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 whether WinCC has been included in the Autostart directory.
Remove the entry if necessary and then restart the computer to execute WebNavigator client installation.
- You will need at least 70 MB of free memory space on the local hard disk to install the WebNavigator client.
Otherwise, the MSI setup will cancel installation with a corresponding error message.
- When installing the WebNavigator client by downloading it from the Intranet/Internet, you can select to either "Open" or "Save" the setup file.
The procedure you select upon initial installation of the WebNavigator client must also be selected for the subsequent installation of plug-ins or ActiveX controls. Otherwise, the "MSI Installer" service will output the error message "Error 1316".
- Prior to installation via download, the latest cumulative security update for Internet Explorer must be installed.
Information on the installation of ActiveX controls: Microsoft entry KB3072449 (<https://support.microsoft.com/en-us/kb/3072449>).

- WebNavigator client on a 64-bit PC:
The required Microsoft Visual C++ Redistributable must be installed on the WebNavigator client before the connection to the WebNavigator server is established. This installation is a requirement for the Web client.
Use the link that is displayed during installation via intranet/Internet.

Note**Installation of Microsoft Visual C++ Redistributable in domain environments**

The required Visual C++ Redistributable must also be available for domain environments as an "msi" package:

- If the WebNavigator client on the 64-bit computer is not upgraded to the latest version via the DVD, "Webnavigatorclient.msi" and "WebNavigatorClient_x64_AddOn.msi" can be made available to the user via the domain controller.
 - If the WebNavigator clients on the 64-bit computers are integrated in domain group policies, the users of the clients must install "WebNavigatorClient_x64_AddOn.msi" themselves.
-
- In the download area of the Web Navigation user interface, the Plug-Ins which can be installed are displayed.
The same minimum user rights are required for installing these plug-ins as for installation of the WebNavigator client.
If you select a plug-in in the Web Navigation user interface, WebNavigator client setup will start. You will have to confirm the selected plug-in again.

Upgrading the WebNavigator client from a previous version

When you connect a web client to a web server, it is tested whether the client has the same version installed as on the web server.

If an older version is present, you can upgrade the WebNavigator client when accessing the Web project.

Upgrade from WinCC V6.2 SP3

Perform a repair installation after upgrading from WinCC V6.2 SP3.

Start the WinCC/WebNavigator client installation in the Control Panel via "Uninstall or change a program" and select "Repair".

Otherwise, controls may be reinstalled during operation.

Restart the computer.

Installation of the WebNavigator client under Microsoft Windows Server

Installation of the WebNavigator client under Microsoft Windows Server with a lower user authorization than "Administrator" is not possible with the default setting of group policies.

Enable the installation of the WebNavigator client in the group policy by

- Assigning and making the software public
- Or activating the setting "Always install with elevated privileges" under "Administrative Templates / Windows Components / Windows Installer".
You must activate "Never" for the "Deactivate Windows Installer" option.

WinCC/WebNavigator: Central installation on web clients

For an installation without user interactions on a web client start the setup via the following command line:

- Installation with default settings:

```
msiexec /i C:\TEMP\WebnavigatorClient.msi /quiet /log  
C:\temp\installWebNav.log
```
- Installation with reduced user interface:

```
msiexec /i C:\TEMP\WebnavigatorClient.msi /qb /log  
C:\temp\installWebNav.log
```

See also

The "Central installation" function (Page 45)

<https://support.microsoft.com/en-us/kb/3072449> (<https://support.microsoft.com/en-us/kb/3072449>)

1.7.4.2 User rights and user groups for WebNavigator clients

Microsoft Windows user rights required for installation and initial registration of the WebNavigator client

"Administrator" rights are required for installing the WebNavigator client via Intranet/Internet or using the product DVD. The initial registration of the client on the WebNavigator server must take place with the user identification used during installation and the same or higher Windows user rights. The connections must be established successfully. All subsequent logins can then be performed by users with different Windows user rights, which may be more restricted.

Microsoft Windows user groups "SIMATIC HMI" / "SIMATIC HMI VIEWER"

Following WinCC installation, WinCC automatically establishes the following local groups in Microsoft Windows User and Group Administration:

SIMATIC HMI	These members can create local projects, and can process, start, and access these projects remotely. Access to the WinCC database is limited to the minimum rights necessary (read/write).
SIMATIC HMI Viewer	These members have read access only to configuration and runtime data in the WinCC database.

In the following cases, you need to add users of the WebNavigator client to a Microsoft Windows user group:

- The WebNavigator client is installed on a PC on which WinCC is already installed: Users of the Web client must be members of the user group "SIMATIC HMI VIEWER" or "SIMATIC HMI".
- The WebNavigator client accesses the WebNavigator server as "Remote Desktop" user: Users of the Web client must be members of the user group "SIMATIC HMI VIEWER".

Installing the WebNavigator client with limited Microsoft Windows user rights

The MSI technology used allows you to install the WebNavigator client even with limited Windows user rights. This procedure can be set during the installation using the group policy based software distribution in networks.

Even the add-ins and plug-ins for the WebNavigator client can be installed. "Administrator" rights are required for the installation of plug-ins that were created with the WinCC Plug-In Builder.

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. Installation is then performed either during login of the defined users or when the computer is started, depending on the configuration of the group policy-based software distribution.
- 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

Software is normally installed with the access rights of the current Microsoft Windows user. When using MSI technology, the installation is performed by an operating system service with a higher level of rights. This enables installations for which the Windows user does not have the necessary rights. Applications which require higher rights for installation 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.

A group policy is created in the domain controller for use of group policy-based software distribution. The software to be distributed is then assigned or made public using Active Directory.

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

1.7.4.3 Settings in the web browser (WebNavigator client)

Introduction

You have to adapt the web browser security settings in order to utilize the full functionality of the WebNavigator client.

The procedure depends on the browser used and is described using the example of the "Internet Explorer" browser.

Procedure

1. Click "Tools > Internet Options" in Internet Explorer.
2. Select the "Security" tab.
Select the corresponding zone, for example, "Local Intranet" or "Internet".
3. Click "Custom Level...".
4. Enable the "Script ActiveX controls marked safe for scripting" and "Download signed ActiveX controls" options.
5. Enable "Active Scripting" under "Scripting".
6. Click "OK". Carry out the modifications in the subsequent dialog.
7. Click the "Trusted Sites" icon.
Click the "Sites..." button to open the "Trusted sites" dialog.
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".
Deactivate the "Require server verification (https:) for all sites in this zone" option.
Click "Add". Click "OK".
9. Click the "Trusted Sites" icon.
Click the "Standard level" button and then the "Custom Level" button.
Enable "Initialize and script ActiveX controls not marked as safe". Click "OK".
10. Click on the "General" tab.
Click in the "Settings" area on the "Temporary Internet Files" button.
Enable the "Automatic" option under "Check for newer versions of stored pages:". Click "OK".
11. Close the "Internet Options" dialog by clicking "OK".

See also

Hardware and software requirements for WebNavigator (Page 107)

General information about WebNavigator (Page 128)

Notes on Internet Explorer for WebNavigator (Page 136)

1.7.4.4 Installation from the DVD (WebNavigator client)

Requirements

- For the installation and use of the WebNavigator client, the information in Settings in the web browser (WebNavigator client) (Page 122) applies.
- Depending on the operating system, specific minimum user rights are required to install the WebNavigator client; see User rights and user groups for WebNavigator clients (Page 120).

Procedure

1. Insert the WinCC DVD in the drive.
The DVD starts automatically if Autorun is enabled in the operating system. If the Autorun function is not activated, start the program Setup.exe on the DVD.
2. In the "Installation Type" dialog, select "Package Installation".
3. Select the "WebNavigator Client" program package.
4. Before the installation, the security settings that are adapted for WinCC are displayed in the "System Settings" dialog. The firewall is configured automatically. Confirm the changes to the system settings.
5. Start the installation. You can track the status of the installation in the displayed dialog. Select "Cancel" to cancel the installation.
6. Restart the computer when prompted to do so by setup.

Result

The WebNavigator client is now installed and has been added as a function to the navigation window of the WinCC Explorer.

1.7.4.5 Installation via the Intranet/Internet (WebNavigator client)

Requirements

- For the installation and use of the WebNavigator client, the information in Settings in the web browser (WebNavigator client) (Page 122) applies.
- Depending on the operating system, specific minimum user rights are required to install the WebNavigator client; see User rights and user groups for WebNavigator clients (Page 120).
- The WebNavigator server must be installed on a computer:
 - The Internet Information Server must be configured with the WinCC Web Configurator.
 - The users must be registered in the WinCC User Administrator.
 - The WinCC project must be in runtime.

1.7 WinCC/WebNavigator Installation Notes

- The latest cumulative security update for Internet Explorer must be installed. This applies to all installed versions of Internet Explorer. Information on the installation of ActiveX controls: Microsoft entry KB3072449 (<https://support.microsoft.com/en-us/kb/3072449>).
- The required Microsoft Visual C++ Redistributable must be installed on the WebNavigator client with a 64-bit computer before the connection to the WebNavigator server is established.

Procedure

1. Enter the address of the WebNavigator server in the address bar of the Internet browser, e.g. the IP address.
For installation in a virtual directory, the URL can be as follows:
 - "https://www.servername/WebNavigator/"
2. Type in the user name and password.
3. The first time you access the WebNavigator server, you will be prompted to install the WebNavigator client.
If the client is a 64-bit computer, an additional link is displayed in order to install the required "Visual C++ Redistributable".
This installation is a requirement for the Web client.
4. Click on the "WinCC WebNavigator client" 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

Installing Visual C++ Redistributable

If you have installed the WebNavigator client without first installing the Visual C++ Redistributable, you can install the software later.

Select the menu "Web Navigator and System Updates" in the "download area" of the Navigation user interface of "MainControl.asp".

If you have already installed the WebNavigator client and wish to install a more recent version via intranet/Internet, open the client setup straight away. You do not need to save the installation file on the target computer. Remove the old installation file first if you wish to save the new one. Alternatively, you can save the new version of the file in a different directory.

5. Leave the Internet Explorer open and open Microsoft Windows Explorer.
Navigate to the directory in which you saved the setup file.
Start setup by double-clicking on the file.
6. Follow the instructions on the screen and enter the information and settings necessary.
The client-side controls of the WebNavigator will be installed.
Close the Setup dialog.

Result

Following successful installation, the WebNavigator client connects to the WinCC project currently in runtime.

Note

Virtual keyboard: .net installation

If you want to use the on-screen keyboard, you also have to install .net 4.0 or higher.

If you install the WebNavigator client from the WinCC DVD, .net 4.0 is already included.

See also

<https://support.microsoft.com/en-us/kb/3072449> (<https://support.microsoft.com/en-us/kb/3072449>)

1.7.5 Installing the WebNavigator diagnostics client

Introduction

The software for the WebNavigator diagnostics client is installed on the client computer from the DVD.

Requirements

- To do this, you must have administrator rights.
- Access via Remote Desktop Protocol (RDP) is not enabled for the diagnostics client.

Procedure

1. Insert the WinCC DVD in the drive.
The DVD starts automatically if Autorun is enabled in the operating system.
If the Autorun function is not activated, start the program Setup.exe on the DVD.
2. In the "Installation Type" dialog, select "Custom Installation".
3. Select the "Diagnostics Client" program in the "Web Navigator" program group.
4. Before the installation, the security settings that are adapted for WinCC are displayed in the "System Settings" dialog. The firewall is configured automatically.
Confirm the changes to the system settings.
5. Start the installation.
You can track the status of the installation in the displayed dialog.
Select "Cancel" to cancel the installation.
6. Restart the computer when prompted to do so by setup.

Result

The WebNavigator diagnostics client is now installed.

1.7.6 WebNavigator Demo Project

Introduction

The WinCC Demo Project can be downloaded as a self-extracting ZIP file from:

- SiePortal: WinCC demo projects (<https://support.industry.siemens.com/cs/products?search=demo&ntp=ExampleOfUse&o=DefaultRankingDesc&pnid=14867&lc=en-WW>)

Installation

To install the project, copy the file in a local target directory and start the decompressing process by double-clicking the file.

The following logins are already configured in the demo project:

WinCC	Logon	Password
Demo User German	winccd	winccpass
Demo User English	wincce	winccpass

See also

SiePortal: WinCC demo projects (<https://support.industry.siemens.com/cs/products?search=demo&ntp=ExampleOfUse&o=DefaultRankingDesc&pnid=14867&lc=en-WW>)

1.7.7 Uninstalling the WebNavigator

Introduction

You can remove the WebNavigator server and WebNavigator client in the usual way, as in Microsoft Windows.

Procedure: Uninstalling via the WinCC Product DVD

1. Start the WinCC product DVD.
The DVD starts automatically if Autorun is enabled in the operating system.
If the Autorun function is not activated, start the Setup.exe program on the DVD.
2. Follow the on-screen instructions.
3. Select "Remove" as the setup type.
4. Select the components that you want to remove.

Alternative procedure: Uninstalling via the Control Panel

1. Open the "Uninstall or change a program" dialog in the Microsoft Windows Control Panel.
2. Select the WebNavigator server or client and click "Remove".
Follow the instructions on the screen.

Result

The WebNavigator Server or WebNavigator client has now been removed from the computer.

1.8 WinCC/WebNavigator Release Notes

1.8.1 General information about WebNavigator

Introduction

These release notes contain important information.

The statements in these release notes take precedence over information provided in the manuals and in the online help.

Read these release notes carefully as they contain useful information.

Notes on the security of the system

Cybersecurity information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept.

Siemens' products and solutions constitute one element of such a concept.

You can find additional information about industrial cybersecurity under:

- <https://www.siemens.com/cybersecurity-industry> (<https://www.siemens.com/cybersecurity-industry>)

Security restrictions with the WebNavigator client

NOTICE
Security restrictions and response times in Internet Explorer
Please note the Internet-specific security restrictions when using the WebNavigator client.
The WebNavigator client may take significantly longer (>20 seconds) than a regular WinCC client to recognize that the WebNavigator server is down or that the communication is faulty.

Using a secure connection via HTTPS

To increase the security of your communication, configure the WebNavigator server in such a way that only HTTPS connections are supported.

You need a digital certificate for the WebNavigator server for this. Also use the SSL certificate on the WebNavigator client.

You can find more detailed information under "Setting up a secure connection via HTTPS (Page 115)".

Communication via proxy server

When communicating through a proxy server, the following applies:

- The WebNavigator client must be a member of the server domain.
- If the users registered on the WebNavigator client have no access to the proxy server, logon to the proxy server with NTLM authentication is as follows:
 1. The logon dialog for the proxy server appears.
 2. The logon dialog for the WinCC user appears.
 3. The logon dialog for the proxy server appears again.

Avoid cross-site request forgery for the WebNavigator

Cross-site request forgery is similar to the vulnerability caused by cross-site scripting (XSS, Cross Site Scripting).

The attack is triggered when an authenticated user clicks on a malicious link. However, this vulnerability also works if the user has disabled scripting in the browser.

Siemens recommends:

- Do not work with other applications or services that have anything to do with the Internet.
- Log off when you no longer need the WebNavigator.

Defense in depth

Follow the instructions on "Industrial Cybersecurity" on the Siemens website:

- <http://www.siemens.com/industrialsecurity> (<http://www.siemens.com/industrialsecurity>)

WebNavigator server: Do not configure the standard port "80"

When configuring the port in the WinCC Web Configurator, use "8080", for example, rather than the standard port "80".

General information about WebNavigator

Project Change

Following a change of projects, a sporadic inoperable period of the Internet Information Services (IIS) may occur.

The computer must then be restarted.

Terminal server: Login with user certificate

The following group policy affects the logon behavior of a user with a user certificate:

Local group policy	Setting
Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options: "System cryptography: Force strong key protection for user keys stored on the computer"	User must enter a password each time they use a key

This setting can cause the password prompt for the user certificate to be displayed in the session of another logged-on user when the terminal session is established.

Corrective measure

To prevent this Windows behavior, use the default setting "Not defined" on the system that is used as the terminal server.

This behavior occurs only when this group policy is activated.

Custom ActiveX controls (Industrial X)

Compatibility with WinCC and WebNavigator server or WebNavigator client must be ensured if custom ActiveX controls (Industrial X) are used:

- Direct installation of the ActiveX control on the computer with WinCC and WebNavigator server or client.
You must install the ActiveX control before installing WinCC and the WebNavigator server or client.
If the ActiveX control does not function without errors after this step, there is no compatibility.
- Installation as a plug-in via the Web Navigation user interface on the WebNavigator client.
If the ActiveX Control is packaged in a plug-in and installed via download, an upgrade of WinCC and the WebNavigator server or client will also require the generation of a new plug-in using this ActiveX control.
Ensure compatible binaries (DLL, OCX, etc.) are used when creating the plug-in.

Visual C++ Redistributable for Visual Studio

Microsoft Redistributable Packages for Visual Studio C++ 2015 are installed along with WinCC.

For example, if you are using ActiveX controls or Visual Basic projects created with versions prior to Visual Studio 2015, you must install the corresponding package.

The installation files for redistributables < Visual Studio 2015 are included in the WinCC scope of delivery:

- "Additional Content" DVD:
"VCRedist" folder

Select the setup for the required version:

- 2005x86 / 2005x64
- 2008x86 / 2008x64

- 2010x86 / 2010x64
- 2012x86 / 2012x64

See also

Settings in the web browser (WebNavigator client) (Page 122)

Setting up a secure connection over HTTPS (Page 115)

<https://www.siemens.com/cybersecurity-industry> (<https://www.siemens.com/cybersecurity-industry>)

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

1.8.2 Notes on WebNavigator installation

Notes on installation

Uninstalling WinCC: WebNavigator client must be installed later

If you uninstall WinCC, you will need to post-install the WebNavigator client.

Message after installation of a plug-in

The Program Compatibility Wizard may possibly output an message during installation of a plug-in.

The plug-in is installed correctly.

Therefore, confirm this message with "The program was installed correctly."

WebNavigator client: WinCC Computer with "Basic Process Control"

The plug-in "WinCC Basic Process Control" must be installed on the WebNavigator client if the client is connected to a computer with WinCC Basic Process Control.

Without the plug-in, the functionality of WinCC Basic Process Control will not be available on the WebNavigator client. For example, the relevant ActiveX controls and the group display will not be available.

Installing the plug-in

The plug-in is located on the WebNavigator server in the folder
<wincc_installationpath>"WebNavigator\Server\Web\Install\Custom".

You can download the plug-in via the WebNavigator navigation user interface from the download area.

A description of the functions supported/not supported can be found in the WinCC Information System:

- "Options for Process Control > Overview of process control system options > Configuration in the PCS 7 environment > Web client"

Dedicated Web server with WinCC Basic Process Control

If the WebNavigator client is to be installed on a dedicated web server with WinCC Basic Process Control, the plug-in "WinCC Basic Process Control" must be installed immediately after installation of the WebNavigator client.

The download page for the plug-in is displayed. You will only be able to exit this page after installation of the plug-in for displaying the process pictures.

For more information on the supported functionalities of the WebNavigator client when connected to a PCS 7 OS, please refer to the PCS 7 documentation.

WebNavigator server: User WNUSR_DC92D7179E29

After the installation of the WinCC/WebNavigator server, the user "WNUSR_DC92D7179E29" is created during the initial configuration with the WinCC Web Configurator.

The user is only used internally. To maintain the functioning of the Web server, do not delete or modify this user.

To increase the security of the system, change the password for the user on a regular basis. To do this, use the tool "CCSetWebNavPwd.exe".

You can find more information in the documentation for WinCC/WebNavigator:

- "WinCC/WebNavigator Documentation > Configuring the WebNavigator system > Configuring the WebNavigator Server > Configuring the WebNavigator web page > WinCC Web Configurator"

Setting a password for the configuration

To define your own password before configuration, you can create a temporary key in the PC's registry.

You can find more information in the "Industry Support Siemens".

1.8.3 General notes on WebNavigator client

Notes on the web client

Security restrictions with the WebNavigator client

NOTICE
Security restrictions and response times in Internet Explorer
Please note the Internet-specific security restrictions when using the WebNavigator client.
The WebNavigator client may take significantly longer (>20 seconds) than a regular WinCC client to recognize that the WebNavigator server is down or that the communication is faulty.

Microsoft Windows Server operating system: Loading process pictures in WinCCViewerRT

It is possible that the web client does not display any process pictures in WinCCViewerRT on PCs with the "Microsoft Windows Server 2016 / 2019 / 2022" operating systems.

Check the settings of the web client:

1. To display the icons in the control panel, select, for example, "Small icons" in the "View by" drop-down list.
2. Click the "Internet options" entry.
The property dialog opens.
3. Deactivate the following entry in the "Advanced" tab in the "Security" area:
 - Do not save encrypted pages to the disk
4. Close the dialog with "OK".

Changing setting via group policy

If you manage the web clients via group policies, follow these steps:

1. To open the editor for local group policies, enter "gpedit.msc" in the Microsoft Windows search field.
2. Select the following entry in the navigation area:
 - Computer configuration > Administrative templates > Windows components > Internet Explorer > Internet control system > "Advanced" PageTo sort the list alphabetically, click the column header "Setting".
3. Double-click "Do not save encrypted pages to disk".
4. Select the "Disabled" or "Not Configured" option.
5. Close the dialog with "OK".

WebNavigator client: Firewall settings for printing from WinCC controls

To be able to print out on the client, you need to define the following Firewall settings for the profiles used:

1. Open "Control panel > System and security > Windows firewall".
2. In the navigation bar, click "Allow a program or feature through Windows Firewall".
3. In the "Allowed programs and features:" list, activate the entry "File and printer sharing" for the relevant profile.
4. Return to the Windows Firewall home page.
5. In the navigation bar, click "Turn Windows Firewall on or off".
6. If the firewall is enabled, disable the setting "Block all incoming connections, including those in the list of allowed programs".

WebNavigator client: ODK function "PWRTCheckPermissionOnPicture"

In order to use the ODK function "PWRTCheckPermissionOnPicture" on a WebNavigator client, install the plug-in "WinCC Basic Process Control" and "Advanced Process Control".

WebNavigator client: WinCC Alarm Control on a WebNavigator server in WinCC ServiceMode

Initial Situation

The WebNavigator client is connected with a WebNavigator server operated in WinCC ServiceMode.

Behavior

If you are using WinCC Alarm Control prior to WinCC V7 that is connected via a server prefix, you will not be able to open the selection dialog.

Solution

Use the WinCC AlarmControl that is offered as of WinCC V7.

WebNavigator client: Diagnostics file "WebNavReconnect.log"

After installation of the WebNavigator client, the diagnostics file "WebNavReconnect.log" is saved in the folder "<User>\Application Data\LocalLow\Siemens\SIMATIC.WinCC\WebNavigator\Client".

The diagnostics file will be saved into the respective user profile so that this user no longer requires administrator rights.

WebNavigator client: Control "WinCC Channel Diagnosis"

You cannot use the "WinCC Channel Diagnosis" Control on a web client without WinCC installation.

WebNavigator client: "FLAG_COMMENT_DIALOG" of the "GCreateMyOperationMsg" function

The WebNavigator client does not support the parameter "FLAG_COMMENT_DIALOG" for the "GCreateMyOperationMsg" function.

WinCC/ODK: SSMRT functions in the web client

The "SSMRT" functions of the Split Screen Manager do not work in the WebNavigator client.

Instead, use the appropriate "SSM" function.

The "SSMRTOpenTopFieldEx" ODK function is not available in the WebNavigator client.

Example

The following script checks the environment and can thus be called in the WebNavigator client and in WinCC Runtime.

```
void OnClick(char* lpszPictureName, char* lpszObjectName, char* lpszPropertyName)
{
    #pragma code("ssmrt.dll")
    #include "ssmrt.h"
    #pragma code()
    char szFullTopfieldPath[MAXFULLPATHLEN] = { 0 };
    long lBufferLen = MAXFULLPATHLEN;
    OPENTOPFIELDSTYLE MyStyle;
    CMN_ERRORA Err;
    BOOL bResult;
    DWORD dwTopfieldStyle = 0;
    long lTopfieldUsed;
    #ifndef RUN_ON_WEBNAVIGATOR
        MyStyle.bAdaptSize = TRUE;
        bResult = SSMRTOpenTopFieldEx (SSMGetScreen(lpszPictureName), "PictureA.pdl",
szFullTopfieldPath, lBufferLen, &MyStyle, &Err);
    #else
        // Declaration of _SSMOpenTopField3:
        //      BOOL _SSMOpenTopField3 (TCHAR Screen, TCHAR* PictureName, DWORD dwStyle,
TCHAR* retPictureName, DWORD dwReturnPathLen, long* plTopfieldUsed, LPCMN_ERROR Err, long
lXPos, long lYPos, BOOL bDefaultPos)
        // dwTopfieldStyle can be 0, TOP_FIELDFIXEDSIZE, TOP_ATTACHTOWORKFIELD, or
TOP_FIELDFIXEDSIZE + TOP_ATTACHTOWORKFIELD
        dwTopfieldStyle = TOP_FIELDFIXEDSIZE;
        bResult = _SSMOpenTopField3 (SSMGetScreen(lpszPictureName), "PictureA.pdl",
dwTopfieldStyle, szFullTopfieldPath, lBufferLen, &lTopfieldUsed, &Err, 0, 0, TRUE);
    #endif
}
```

1.8.4 Notes on Internet Explorer for WebNavigator

Notes on Internet Explorer

Security settings in Internet Explorer: Installation via SSL connection

If you want to download the WebNavigator from an ASP portal via an SSL connection, note that the download is not possible under certain conditions.

You can correct this with one of the following settings:

- Deactivate the "Do not save encrypted pages to disk" option in the "Advanced" tab for the Internet options of the Internet Explorer.
- Deactivate the "Internet Explorer Enhanced Security Configuration" option in the "Control Panel/Add/Remove Programs/Windows Components".

WebNavigator server: Display virtual folder in Internet Explorer

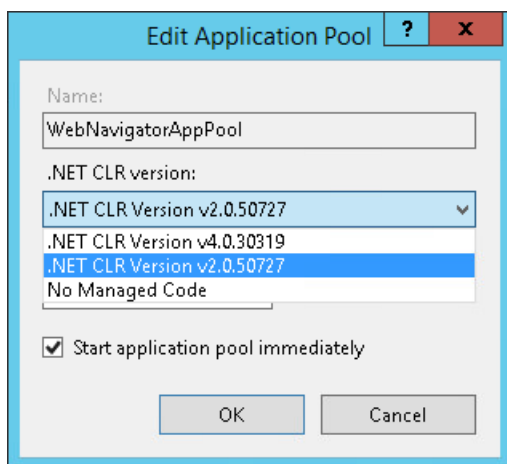
Note the following when using Internet Explorer as WebNavigator browser:

To add a virtual folder to an existing website, create this website in a subdirectory of the drive.

When the website is created in the root directory, e.g. under D:\, Internet Explorer may not show the contents of the virtual folder.

To always display the contents, change the .NET settings in the IIS:

1. Open the Internet Information Services (IIS) Manager.
2. In the navigation, click on the entry "Application pools".
3. In the shortcut menu of "WebNavigatorAppPool", select the "Basic settings" entry.
4. In the ".NET CLR version" list, select the .NET version "v2", for example:



WebNavigator client: Display of ActiveX controls in Internet Explorer

ActiveX controls are disabled in Internet Explorer by default.

For this reason, the WinCC controls are not displayed correctly in Internet Explorer on a WebNavigator client.

To display the WinCC controls correctly, add the Web server as a trusted website and enable the ActiveX controls only for the "Trusted sites" zone.

To continue protecting Internet Explorer from foreign ActiveX controls, check that the restricted security settings still apply to the other zones after making the changes.

For more information, refer to the following documentation:

- WinCC/WebNavigator: "WinCC/WebNavigator Installation Notes > Installation of WebNavigator Client > Settings in the web browser (WebNavigator client) (Page 122)"

WebNavigator client: Updating pictures with faceplates

To display changed faceplates in process pictures, refresh the view of the web client in the browser, e.g. with <F5> or using the  button.

See also

Settings in the web browser (WebNavigator client) (Page 122)

1.9 WinCC/WebUX

1.9.1 WebUX licensing

The WinCC/WebUX basic package with an integrated WinCC WebUX Monitor license is included in WinCC.

WebUX client

The WebUX clients are licensed on the WebUX server.

No license is required for the WebUX client on the computer.

WebUX server

The WebUX server is installed on a WinCC system. The WinCC basic system requires at least the WinCC basic RT license.

The license keys are differentiated as described below and run in parallel on the WinCC/WebUX server:

License ¹⁾	Function	Comments
WinCC WebUX Monitor	The user has only read access.	The authorization level 1002 "Web access - monitoring only" is configured for the user in the User Administrator. If the available "Monitor" licenses have been allocated, an "Operate" license can also be allocated to a WebUX client for read access.
WinCC WebUX Operate	The user has read and write access.	
WinCC/WebNavigator	The user's authorizations determine whether write access is possible in addition to read access.	

1) If a WinCC/WebNavigator license is also installed in the WinCC system, the WebNavigator license can also be allocated to a WebUX client.

To do so, the following option must be enabled in the WebNavigator dialog "WinCC Web settings":

- "Allow WebUX to use the WebNavigator licenses".

First, however, all available WebUX licenses are used.

License packages

The license packages are available with 1, 3, 10, 30 and 100 clients.

If you have upgraded from WebUX V7.3, there may also be licenses for 5 / 25 / 50 / 150 clients.

As of WinCC V8.1, there is also an "Unlimited" license for an unlimited number of connected clients.

If the number of licensed clients is exceeded during the logon attempt by a WebUX client, no further logon is permitted.

The packages are version-independent and can be combined.

WebUX demo license

With WinCC/WebUX you also receive a demo license for accessing the WebUX server.

This allows a maximum of one user without a valid WebUX license or WebNavigator license to have read access to the project.

Reserved license

A reserved WebUX license always gives the user guaranteed access to the WebUX server.

A connection remains reserved for the user. The number of freely available WebUX licenses is reduced by each configured reserved license.

Applications

Possible applications include:

- Remote operator access:
If the connections to the WebUX server are occupied by read-only access, a connection remains reserved for operation.
- Central display:
Central client stations are always connected, for example, to display the status of the WinCC system.

Reserving WebUX licenses

In the User Administrator, you assign one of the available licenses to a WebUX user as a reserve license.

To do this, enable the "Reserve WebUX license" option for the user. The field "WebUX Number of reserved licenses" shows how many WebUX licenses are assigned through reservation.

Reserved licenses cannot be configured for user groups, only for individual users.

If more reserved licenses are configured than those available on the WebUX server, the licenses of the first users logged on are used.

Using WebNavigator licenses

You can also use WebNavigator licenses for WebUX clients.

To enable licenses for WebUX clients, open the "WinCC Web settings" dialog in the shortcut menu of the "WebNavigator" editor in the WinCC Explorer.

In the "Runtime" tab, enable the "Allow WebUX to use the WebNavigator licenses" option.

Administering clients in runtime

To identify inactive clients and to disconnect them, if necessary, use the page "`http://<servername>/status.html`".

1.9 WinCC/WebUX

You can find further information in the documentation of the WinCC/WebNavigator option under:

- WinCC/WebNavigator documentation > Operating a WinCC project > Diagnosis of the Connections with "Status.html"

See also

Installation of WebUX (Page 140)

1.9.2 Installation of WebUX

Software requirements

Certain requirements concerning operating system and software configuration must be met for the installation.

WebUX server: Operating system

Software	Configuration	Comments
Microsoft Windows 10	Pro Enterprise	Standard installation 64-bit A maximum of 9 WebUX clients can connect to the WebUX server. ¹⁾
Microsoft Windows 10	Enterprise LTSC (Long-Term Servicing Channel)	Standard installation 64-bit A maximum of 9 WebUX clients can connect to the WebUX server. ¹⁾
Microsoft Windows 11	Pro Enterprise	64-bit A maximum of 9 WebUX clients can connect to the WebUX server. ¹⁾
Microsoft Windows Server 2019	Standard Datacenter	64-bit
Microsoft Windows Server 2022	Standard Datacenter	64-bit

1) Only a limited number of connections is possible:

The maximum number of WebUX clients depends on the number of connections that the IIS supports on the installed Microsoft Windows version.

The number of available connections can decrease if other applications access these connections, e.g. WinCC/WebNavigator.

In the Microsoft Windows system monitor, use the "Performance Monitor" application to analyze the connection status.

Additional software requirements

	Version / setting	Relevant for	Comments
Web browser	The browser must support HTML5.	WebUX client / terminal	WebUX can be used with any browser. The display is optimized for the Chrome browser.
WinCC version	WinCC V8.1	WebUX server	The WebUX server is installed on a WinCC system.
SIMATIC Logon version (optional)	SIMATIC Logon V2.0	WebUX server	Only relevant if you are using SIMATIC Logon for central user administration.
User rights for installation	Administrator rights	WebUX server	Required rights for installing the WebUX server.
User rights for operation	Default user rights	WebUX client WebUX server	Required rights on the WebUX server and WebUX client.
Microsoft Internet Information Service (IIS)	WWW Services > Common HTTP Features or Shared HTTP Features: • Standard document • Static content WWW Services > Performance Features: • Compression of dynamic content • Compression of static content WWW Services > Application Development Features: • ASP.NET ≥ 4.5	WebUX server	During the WinCC installation, the Microsoft Internet Information Service (IIS) is installed and configured.

WebUX client (terminal)

You only need an HTML5-capable Web browser such as Chrome, Firefox or Safari on a terminal that accesses the WebUX server.

Note**Browser-dependent representation**

Differences in display and behavior are possible in the different browser versions.

To display a configured character set, for example, this must also be available in the browser or on the device.

Installation of the WebUX server

You can install WinCC/WebUX during the installation of WinCC.

When you install the server WebUX at a later time, proceed as follows:

1. Start the WinCC installation DVD.
2. Select the installation type "Custom Installation".

1.9 WinCC/WebUX

3. In the "WinCC" group of the "Program" dialog, select the entry "WinCC WebUX".
4. Transfer the WebUX license. You can find more information under:
 - WebUX licensing (Page 138)

You can find information about configuring WebUX under:

- Configuring the WebUX website (Page 142)

Limiting the number of connections

The number of the connections between WebUX server and WebUX clients was limited to a standard limit value of 150.

If the number of WebUX client connections reaches this limit value, further connections are rejected by the WebUX server. This supports the defense against DoS attacks.

You can modify the connection limit value in the `config.js` file.

Configuring the limit value

1. Log into the WebUX server with administrator rights.
2. Navigate to the folder:
 - `C:\inetpub\wwwroot\Siemens\WebRH\conf\`This contains the file `config.js`.
3. Open the file `config.js` with a text editor.
4. Search the text line `"config.sessionLimit = 150;"`.
The default limit value is 150.
5. Change the value `"config.sessionLimit"` and save the file.
6. Open the Internet Information Services (IIS) Manager and restart the WebUX website.

See also

WebUX licensing (Page 138)

Configuring the WebUX website (Page 142)

1.9.3 Configuring the WebUX website

Configure the WebUX website on the WebUX server and the connection via HTTPS to communicate with the WebUX clients.

WinCC WebUX Configurator

After WinCC and WinCC/WebUX are installed, the WinCC WebUX Configurator opens.

To make changes later, you can find the WinCC WebUX Configurator in the "Siemens Automation" program group.

You use the WebUX Configurator to set up the standard configuration for the use of WebUX.

- Configuration of the Microsoft Internet Information Service
- Settings of the Web server
- SSL certificate for HTTPS connections
- Virtual folder

You can find more information in the documentation for WinCC/WebUX:

- WinCC Web Configurator
- Creating a new default web page
- Creating a virtual folder

See also

Installation of WebUX (Page 140)

1.9.4 Communication: SSL certificate for HTTPS connections

To improve the security of your communication, WebUX only supports HTTPS connections.

You need a digital SSL certificate for the WebUX server.

NOTICE

Protecting the infrastructure

Setting up a Web server may enable access to your plant infrastructure.

Therefore, protect the computer on which the Web server is installed. Make sure that the following rules are followed:

- The computer is only accessible via secure connections.
- The check mechanisms provided by software vendors are activated and cannot be bypassed under any circumstances.

Install a SSL certificate

You have the following options when setting up the WebUX website:

- Select an existing certificate
- Create self-signed certificate
- Install a certificate after setting it up

Creating a new certificate

1. Activate the "Create a new certificate" option.
2. Enter a name of your choice.

1.9 WinCC/WebUX

When the configuration is completed, a self-signed certificate is created. The certificate is valid for 1 year.

Additional information

You can find information on self-signed certificates when using different web browsers on the Internet under Entry ID 109773769:

- SiePortal: "How do you fix problems when using self-signed certificates from WebUX or WebNavigator with different web browsers?" (<https://support.industry.siemens.com/cs/ww/en/view/109773769>)

Note

Restricted authentication

The certificates that you create when you configure the WebUX website itself are not verified by an official certification body. Depending on your browser settings, a warning message is displayed when you access the website.

To better secure the server authentication, install the certificate of an official certification body.

Display of secure data sources only

For display of web pages and external files, one of the following conditions must be met:

- Call via the HTTPS connection
 - Call of a trusted site
-

Enabling SSL in IIS

To use SSL, configure SSL access in the Internet Information Service (IIS).

Requirement

- You have administrator rights on the WebUX server.

Procedure

1. Open the "Internet Information Services (IIS) Manager".
2. Select the web page under "Sites" in the "Connections" navigation area.
3. Click "Bindings" in the "Actions" area.
The "Site bindings" dialog opens.
4. To configure the settings, click "Add".
The "Add site bindings" dialog opens.
5. Select the website type, IP address and the port.
To display the fields for configuration of the SSL certificate, select the type "https".
6. Select the SSL certificate from the list or with "Select".
7. Confirm with "OK" to close the dialog.
You can delete the other entries in the "Site bindings" dialog.
8. Exit the configuration with "Close".

9. In the data area "Default Web Site Home", select the "SSL settings" under "IIS".
10. Activate the "Require SSL" option and select the setting for client certificates.

See also

SiePortal: "How do you fix problems when using self-signed certificates from WebUX or WebNavigator with different web browsers?" (<https://support.industry.siemens.com/cs/ww/en/view/109773769>)

1.10 Service and Support

1.10.1 Warnings

Security information

Warning notice system

This manual contains notices you must observe to ensure your personal safety and to prevent damage to property. Notices referring to your personal safety are highlighted in the manual by a safety alert symbol; notices referring to property damage only have no safety alert symbol. The warning 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 may result if proper precautions are not taken.

NOTICE

indicates that property damage may result if proper precautions are not taken.

Note

indicates important information about the product and its use or a specific section of the documentation to which you should pay particular attention.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A warning notice 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 information. 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

Note the following:



WARNING

Proper use of Siemens products

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 adhered to. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining names in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit:

- <https://www.siemens.com/cybersecurity-industry> (<https://www.siemens.com/cybersecurity-industry>)

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under:

- <https://www.siemens.com/cert> (<https://www.siemens.com/cert>)

Disclaimer of liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since discrepancies cannot be precluded entirely, we cannot guarantee full agreement. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions. Suggestions for improvement are welcomed.

Information in the online documentation is more binding than that in the manuals and PDF files.

Observe the Release Notes and Installation Notes. Information in the Release Notes and Installation Notes is more binding than that in the manuals and online help.

Copyright © Siemens 2024

All rights reserved

The reproduction, transmission or use of this document or its contents is not permitted without express written authorization. Offenders will be held liable for payment of damages. All rights, including rights created by patent grant or registration of a utility or design, are reserved.

Siemens Aktiengesellschaft

Division Digital Industries

SIMATIC Human Machine Interfaces

P.O. Box 4848

D-90026 Nuremberg, Germany

See also

<https://www.siemens.com/cybersecurity-industry> (<https://www.siemens.com/cybersecurity-industry>)

<https://www.siemens.com/cert> (<https://www.siemens.com/cert>)

1.10.2 GDPR - General Data Protection Regulations

Siemens takes data privacy principles, such as the privacy by design and default principle, into account when developing its products and services.

For the SIMATIC WinCC V8.1 product, including options, this means the following:

Personal data processed by the application

This product collects and processes the following personal data:

- User names, i.e. credentials, which may directly contain or establish a reference to family names and/or first names
- Timestamps: date / time of login, logoff and access
In the WinCC "Option for Process Control" application "Split Screen Manager", the login timestamp and user name are saved without encryption with the picture management data. In the WinCC/WebNavigator diagnostic page, logged in users and timestamps are saved without encryption.
- Location data (time zone)
- Computer name
- IP addresses
- MAC addresses
- Email addresses (WinCC Options)
- In case of using UMC, additional personal data can be added in the tool, e. g. telephone numbers or addresses.
This data is not needed for the product functionality and should not be stored on the same medium.

If the user links the above mentioned data with other data, e. g. shift plans, or stores personal data on the same medium, e. g. hard disk, and thus establishes a personal reference, the user must ensure compliance with data protection regulations.

Purposes

The above data is required for the following purposes:

- Access protection and security measures (e. g. Login, IP address)
- Process synchronization and integrity (e. g. time zone information, IP addresses)
- Archiving system for traceability and verification of processes (e. g. access timestamps)
- Message system for traceability and availability (e. g. email notification)

The storage of data is appropriate and limited to what is necessary, as it is essential to identify the authorized operators and process events.

Data configuration

The customer may configure the data collected via the product as follows:

- Display data in process pictures
- Data output in form of reports, e. g. for printing or display as electronic file
- Data collection and evaluation in form of graphics, e. g. for KPI analysis

Deletion policy

The product does not provide an automatic deletion of the above data.

1.10 Service and Support

If necessary, these can be deleted manually if desired. To do this, please refer to the product documentation or contact customer support.

Securing of data

The above data will not be stored anonymously or pseudonymized, because the purpose of access and event identification cannot be achieved otherwise.

The above data is secured by adequate technical measures, such as:

- Encryption of log data
- Storing the process data in access-protected SQL databases
The user must ensure the access protection as part of their process configuration.

1.10.3 Customer support

Customer Support, Technical Support

You can access the SIMATIC hotlines via the support request form on the Internet.

The SIMATIC hotline employees speak German and English. The Authorization hotline offers French, Italian or Spanish customer support in addition to German and English.

Technical support

Technical support is available around the clock from Monday to Friday.

The latest Technical Support information can be found at the following URL:

- <https://support.industry.siemens.com/cs/ww/en/sc/4868> (<https://support.industry.siemens.com/cs/ww/en/sc/4868>)

Form for support requests:

- <https://www.siemens.com/supportrequest> (<https://www.siemens.com/supportrequest>)

Siemens Industry Service Card

The "Siemens Industry Service Card" enables an additional Technical Support, such as fast response via "Priority Call-Back". You can find more information at the following URL:

- <https://support.industry.siemens.com/cs/ww/en/sc/4869> (<https://support.industry.siemens.com/cs/ww/en/sc/4869>)

SiePortal: The SIMATIC Online Support

Service and Support

You can find the SiePortal and an overview of the support offer under this URL:

- <https://sieportal.siemens.com/> (<https://sieportal.siemens.com/>)
- <https://support.industry.siemens.com/> (<https://support.industry.siemens.com/cs/ww/en/>)
- <https://support.industry.siemens.com/cs/ww/en/view/93906404> (<https://support.industry.siemens.com/cs/ww/en/view/93906404>)

In Product Support, for example, you will find downloads of firmware updates, service packs and useful applications.

The app is available for mobile Siemens Support:

- <https://support.industry.siemens.com/cs/sc/2067> (<https://support.industry.siemens.com/cs/ww/en/sc/2067>)

Videos and help pages are available so that you can successfully use the Support offer:

- <https://support.industry.siemens.com/cs/ww/en/sc/4866> (<https://support.industry.siemens.com/cs/ww/en/sc/4866>)
- <https://support.industry.siemens.com/cs/ww/en/sc/2063> (<https://support.industry.siemens.com/cs/ww/en/sc/2063>)

WinCC FAQs

WinCC Online Support with information on FAQs (Frequently Asked Questions) may also be found at the following URL:

- <https://support.industry.siemens.com/cs/ww/en/ps/14866/faq> (<https://support.industry.siemens.com/cs/ww/en/ps/14866/faq>)

Technical Forum

The Technical Forum supports exchange with other SIMATIC users. You can find the forum at the following URL:

- <https://support.industry.siemens.com/tf/> (<https://support.industry.siemens.com/tf/ww/en/>)

Technical documentation for SIMATIC products

You can find a guide to the technical documentation provided for individual SIMATIC products and systems at the following URL:

- <http://www.siemens.com/simatic-tech-doku-portal> (<http://www.siemens.com/simatic-tech-doku-portal>)

Local partners database

To contact your local partner, search the local partners database at the following URL:

- http://w3.siemens.com/aspa_app/ (http://w3.siemens.com/aspa_app/?lang=en)

Product Information

SIMATIC WinCC

Go to the following URL for general information about WinCC:

- WinCC Landing Page:
<https://support.industry.siemens.com/cs/ww/en/view/93906404> (<https://support.industry.siemens.com/cs/ww/en/view/93906404>)
- SIMATIC HMI software product overview:
<http://www.siemens.com/wincc> (<http://www.siemens.com/wincc>)

SIMATIC Products

Go to the following URL for general information about SIMATIC products:

- <http://www.siemens.com/simatic> (<http://www.siemens.com/simatic>)

See also

SiePortal - Home (<https://sieportal.siemens.com/>)

SiePortal: Support request (<https://www.siemens.com/supportrequest>)

SiePortal: Technical support (<https://support.industry.siemens.com/cs/ww/en/sc/4868>)

SiePortal: Siemens Industry Service Card (<https://support.industry.siemens.com/cs/ww/en/sc/4869>)

SiePortal: SIMATIC WinCC in Online Support / Landing Page (<https://support.industry.siemens.com/cs/ww/en/view/93906404>)

SiePortal: Service and Support (<https://support.industry.siemens.com/cs/ww/en/>)

SiePortal: Information and help for support (<https://support.industry.siemens.com/cs/ww/en/sc/4866>)

SiePortal: Support - How-to Videos (<https://support.industry.siemens.com/cs/ww/en/sc/2063>)

SiePortal: Mobile use via support app (<https://support.industry.siemens.com/cs/ww/en/sc/2067>)

SiePortal: WinCC FAQs (<https://support.industry.siemens.com/cs/ww/en/ps/14866/faq>)

SiePortal: Support Technical Forum (<https://support.industry.siemens.com/tf/ww/en/>)

SiePortal: Technical documentation for SIMATIC products (<http://www.siemens.com/simatic-tech-doku-portal>)

Internet: Contact person database (http://w3.siemens.com/aspa_app/?lang=en)

Internet: Information about WinCC (<http://www.siemens.com/wincc>)

Internet: SIMATIC Products (<http://www.siemens.com/simatic>)

1.10.4 Support request

Dear customer

In order to provide you with fast and effective support, please complete the "Support Request" form online on the Internet. Describe the problem in as much detail as possible. We would appreciate if you would provide us with all project data so that we can reproduce the error situation or shorten the turn-around time.

Before filling out the support request, check whether your configured quantity structure is within the range of tested quantity structures (see "Performance Data" section).

Support Request form

The Support Request form is available at the following URL:

- SiePortal: Support request (<https://www.siemens.com/supportrequest>)

When filling out the report, you will be guided through several steps.

The data required by the Technical Support are described in the FAQ 16607894:

- <https://support.industry.siemens.com/cs/ww/en/view/16607894> (<https://support.industry.siemens.com/cs/ww/en/view/16607894>)

You can find more information on technical support at the following URL:

- <https://support.industry.siemens.com/cs/ww/en/sc/2100> (<https://support.industry.siemens.com/cs/ww/en/sc/2100>)

Procedure

1. Open the "Support Request" form via the link and click "New request"
Step 1 "Product search" is displayed.
2. Enter the order number or the product name in the field. Upper/lower case is not relevant. Search for parts of the product name or enter the full product name in the correct order. You can e. g. search for the following terms:
 - "WinCC Runtime V7"
 - "wincc editor"
 - "WinCC DataMonitor"
 - "wincc webnav"
 - "Connectivity"The found products are offered in the "Product selection" field.
If you have any questions about licensing, activate the option "Licensing/Authorization".
3. Select the desired product and click "Next".
Step 2 "Problem description" is displayed.
4. Fill in the form.
Depending on the selection, suggested solutions and FAQs that were found for the selected keywords are listed.
If you have found a suggested solution for your problem, close the form in the browser.

1.10 Service and Support

5. Describe your problem as exactly as possible in the "Details" field. Please also check your WinCC installation and the configuration.
If you have any idea what has caused the error, please let us know. No detail should be omitted, even if you consider it unimportant.
Pay particular attention to the following questions and comments:
 - Was the configuration data created with older WinCC versions?
 - How can the error be reproduced?
 - Are other programs running simultaneously with WinCC?
 - Have you activated screen savers, virus scanners, power management?
 - Search your computer for log files (WinCC\Diagnose*.log, drwatson.log, drwtsn32.log). The log files are needed for error analysis. Therefore, be sure to send the log files as well.
 - To assemble diagnostic and system information from computers and other devices, use the "SIMATIC Assessment Suite - Data Collector" (SAS-DC) diagnostics tool.
More information is available in the Support entry 65976201 (<https://support.industry.siemens.com/cs/ww/en/view/65976201>).
6. To load your project directory and the log files into the Support Request, drag and drop the files into the gray field.
To do this, compress the data, for example, as a zip file.
7. When you have entered all the information, click "Next"
Step 3 "Check and submit" is displayed.
8. Enter your contact details and review the summary.
9. You close the support request by clicking the "Send" button.
Your data will be transmitted to Customer Support and processed there.
You will receive an order confirmation by email.
Step 4 "Confirmation" is displayed.
10. To print out your data, click "Request - Show/print details".

Thank you for your cooperation. We hope that we can be of assistance in solving your problems.

Your WinCC Team

See also

SiePortal: Support request (<https://www.siemens.com/supportrequest>)

SiePortal: Specifications for the Technical Support (<https://support.industry.siemens.com/cs/ww/en/view/16607894>)

SiePortal: Support - service catalog (<https://support.industry.siemens.com/cs/ww/en/sc/2100>)

SiePortal: SIMATIC Assessment Suite - Data Collector (SAS-DC) (<https://support.industry.siemens.com/cs/ww/en/view/65976201>)

WinCC/Connectivity Pack documentation

2.1 WinCC/Connectivity Pack

Content

Through the WinCC Connectivity Pack, you receive licensed access to WinCC databases via OPC or WinCC OLE DB Provider.

This chapter will show you

- how to install the Connectivity Pack Server and Client;
- the OPC servers of WinCC;
- how to configure access to the alarm message archive;
- how to configure access to the process value archive.
- how to configure the Connectivity Station.

Target group of this documentation

This documentation was designed for developers with Visual Basic and SQL Server knowledge.

2.2 Overview: WinCC/Connectivity Pack

Introduction

Licensed access to online and archive data of WinCC is enabled with the WinCC / Connectivity Pack.

The WinCC OLE DB Provider makes access to the process value and alarm archives possible. Data that is stored, compressed in the database can be read as decompressed data.

The WinCC OLE DB Provider also provides analysis functions such as Minimum, Maximum of archive tags for example.

OPC enables cross-manufacturer communication in automation via the following standardized interfaces:

- OPC HDA 1.20 (Historical Data Access)
- OPC A&E 1.10 (Alarm & Events)
- OPC DA 2.05a, 3.00
- OPC XML DA 1.01
- OPC UA 1.03

As a result, WinCC operating as an OPC server can forward current process data and messages to other OPC clients (e.g. Microsoft Excel).

The WinCC Connectivity Station also uses OPC to access data of different WinCC stations.

The Connectivity Pack includes:

- The WinCC OLE DB Provider for directly accessing process value and alarm archives in the SQL server database on the WinCC RT computer and on an archive server.
- The tool "Archive Connector" for configuring the database access.
With it, swapped out WinCC archive databases can be connected to or disconnected for the SQL server. In doing so, an overview of the individual database segments is generated. The Archive Connector can monitor folders and automatically connect copied in archives.
- WinCC DataConnector for configuration and access to the process value and alarm archives in process images.
- WinCC Connectivity Station
- License for Server OPC HDA 1.20 (Historical Data Access) for access to historical data in the WinCC archive system.
- License for Server OPC A&E 1.10 (Alarms & Events) for forwarding and acknowledging of messages.
- License for Server OPC XML DA 3.00 (OPC eXtensible Markup Language).
- License for the OPC UA Server 1.03
- The licenses for access to the WinCC archive databases through the WinCC OLE DB-Provider or WinCC User Archive through Microsoft OLE DB.

WinCC OLE DB Provider

The WinCC OLE DB Provider is available on the following systems:

- Connectivity Pack Client
- Connectivity Pack Server
- The WinCC Station
- Connectivity Station

Using WinCC OLE DB Provider, the Connectivity Pack Client has direct access to the WinCC archive data in the process value and message archives.

Access may take place under various configurations of the Connectivity Pack Client:

- A WinCC software like WinCC Basis, Web Navigator Server, DataMonitor Server or Connectivity Pack Server exists on the client computer.
The Connectivity Pack client does not have to be installed explicitly.
Licensing is provided through WinCC licenses.
- The client computer has no installation of WinCC software.
In this case, the Connectivity Pack client needs to be installed on the client computer.

Simultaneous access to archive and Runtime databases

The Connectivity Pack provides the function "ArchiveMonitor".

The function automatically merges the data from runtime and archive databases of the activated WinCC project into an SQL database "CC_ExternalBrowsing" and creates the "AMT" and "ARCHIVE" views in it. Since these views provide all the necessary information for the WinCC OLE DB Provider, the "CC_ExternalBrowsing" database can be used as a data source for the provider.

On deactivating WinCC runtime, views additionally created in "CC_ExternalBrowsing" are deleted.

When an archive server does not contain any runtime databases, access to the archive databases using the "CC_ExternalBrowsing" database is not possible.

WinCC OLE DB Provider as a "Linked Server"

The WinCC OLE DB Provider can be registered in the SQL server in the list of "Linked Servers".

This is independent of whether the database is local or remote.

Note

SQL server settings

When configuring WinCC OLE DB Provider as a "Linked Server", the "WinCC OLE DB Provider for Archives" entry must be selected in the "Provider Name" field of the "Linked Server Properties" dialog.

Activate the "AllowInProcess" checkbox in the "Provider Options" dialog.

You will find more detailed information in the "SQL Server Books Online" under "Configuring OLE DB Providers for Distributed Queries".

Example of a WinCC OLE DB Provider as a Linked Server with the server name "WinCC":

```
select min(realvalue) from openquery(WINCC, 'Tag:R,1, ''0000-00-00
00:01:00.000'', ''0000-00-00 00:00:00.000'')

select * from openquery(WINCC, 'Tag:R,1, ''0000-00-00
00:01:00.000'', ''0000-00-00 00:00:00.000'')
```

Access to tags of the data type String / Int64 / UInt64

To access process values of the following tag types, replace the "TAG:R" schema with "TAG_EX:R":

- Text tag, 8-bit character set / 16-bit character set
- Floating-point number 64-bit IEEE 754

In queries with analysis functions, use the "VARIANT" data type for the column name.

WinCC Archive Connector

The Connectivity Pack also includes the tool "Archive Connector" for the configuration of the database access.

With it, swapped out WinCC archives can be reconnected to an SQL server.

The archive data is made available again via the WinCC OLE DB Provider.

With the Archive Connector, the following functions are possible:

- Manual Connection:
Locally swapped out WinCC archive databases are selected and connected to the local SQL server.
- Manual Disconnection:
Connected databases are selected and disconnected from the SQL server.
- Automatic Connection:
Local folders for swapped out WinCC archives are selected.
All archives in the selected folders are automatically connected to the SQL server when copied in.

The Archive Connector may only be operated using a local SQL Server and a Connectivity Pack license.

Note

If you access message archives or swapped out archives via "CC_ExternalBrowsing", this access may take several minutes.

WinCC DataConnector

The DataConnector provides the following functions:

- Using the DataConnector Wizard, a process picture may be configured in Graphics Designer for an archive inquiry for message or process value archives.
- DataConnector Control will execute the archive inquiry in Runtime after opening the process picture and will display the data found.

Inquiries using relative or absolute time ranges are possible.

The result of the inquiry may be shown in table format for messages, and in table or trend format for process values.

OPC

Access via OPC can only take place on computers on which WinCC Runtime is running.

WinCC OPC HDA server

WinCC supplies historical data from the archive system to other applications via the WinCC OPC HDA server.

An OPC HDA client - such as a reporting tool - can specify the beginning and the end of a time interval and specifically request the corresponding data. An OPC HDA client can also specifically request previously processed data on the WinCC OPC HDA server and actively affect data compression prior to data transfer.

WinCC OPC A&E server

With the WinCC OPC A&E server, a WinCC message is portrayed as an alarm. The alarm can only be forwarded with its accompanying process values to the production or management level of the company, where it is also acknowledged. Via filters, only selected data is transferred.

WinCC OPC XML server

The WinCC OPC-XML server provides the OPC-XML client with the OPC process data as a web service. OPC-XML clients can access WinCC runtime data via any platforms as well as via both Intranet and Internet.

WinCC OPC UA server

The WinCC OPC UA Server provides process values, values from tag archives, and WinCC messages.

Note

WinCC archive databases: Connectivity Pack license

For access to WinCC archive databases using OPC HDA, process values with OPC XML and alarms with OPC A&E, a Connectivity Pack license is required on the computer with this data.

An installation of Connectivity Pack Server or Client is not required.

OPC DA is licensed with a valid RT license for WinCC.

WinCC Connectivity Station

The Connectivity Station allows access to the data of various different WinCC stations, such as the WinCC server.

The Connectivity Station is configured in the S7 projects, which also manage these WinCC stations.

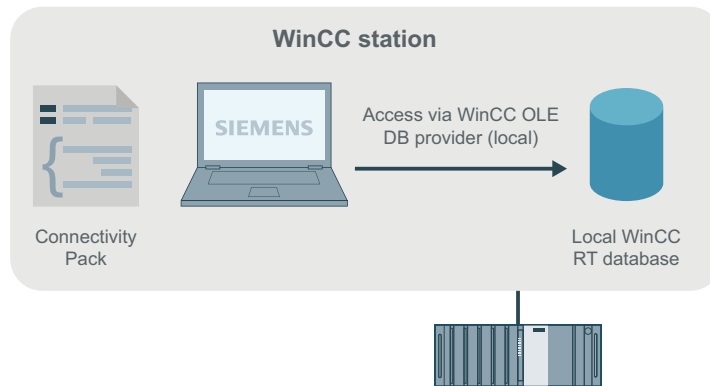
You will access the WinCC stations via an OPC client via the OPC-Server.

See also

[Access Using OPC to WinCC Archives, Tags, and Messages \(Page 168\)](#)

2.3 Applications

2.3.1 Use Case 1: Local Access to WinCC RT Databases



Principles

An application uses WinCC OLE DB Provider to access the local WinCC RT database.

You may locally analyze the archive data and may, for example, calculate the standard deviation of a process value.

Software requirements

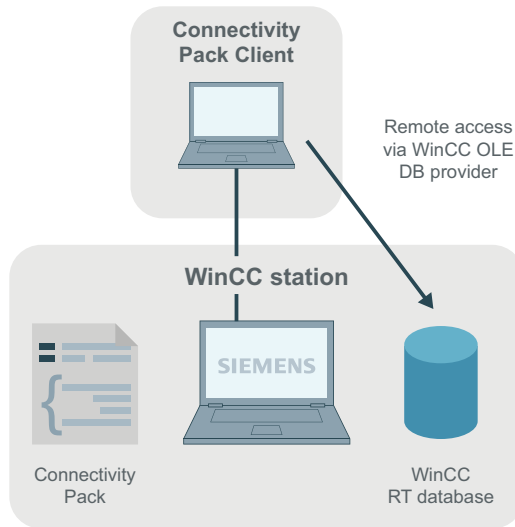
On the WinCC station, the following licenses need to be installed:

- A valid RT license for WinCC
- WinCC Option Connectivity Pack

See also

Examples for Access Using OLE DB Provider (Page 318)

2.3.2 Use Case 2: Remote Access to WinCC RT Databases



Principles

The Connectivity Pack Client remotely accesses the WinCC RT database of a WinCC station. Via the WinCC OLE DB Provider, the Connectivity Pack Client reads the data of the process value and alarm message archives.

Since in this use case, the swapped-out WinCC archive is not accessed, the Archive Connector does not have to connect WinCC archives to an SQL server.

You may use the Connectivity Pack Client to display, analyze, or process the data, e.g. by exporting it to a CSV file.

Software requirements

On the WinCC station, the following licenses need to be installed:

- A valid RT license for WinCC
- WinCC Option Connectivity Pack

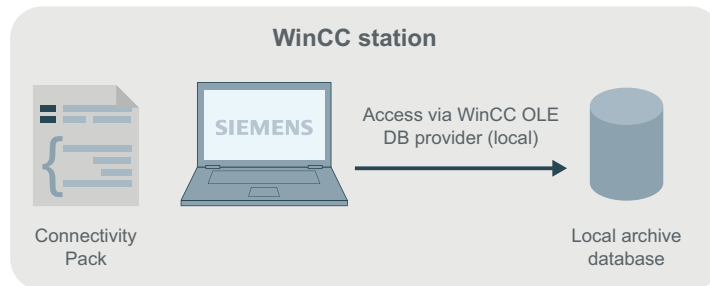
The access may take place under various configurations of the Connectivity Pack Client.

- A WinCC software like WinCC Basis, Web Navigator Server, DataMonitor Server or Connectivity Pack Server exists on the client computer.
The Connectivity Pack Client does not have to be installed explicitly. Licensing is provided through WinCC licenses.
- The client computer has no installation of WinCC software.
Then the Connectivity Pack Client needs to be installed on the client computer.

See also

Examples for Access Using OLE DB Provider (Page 318)

2.3.3 Use Case 3: Local Access to WinCC Archive Databases



Principles

An application accesses the local archive database using WinCC OLE DB Provider. The older archive data are copied from the WinCC RT database to a separate directory on the same computer.

With the Archive Connector, the swapped out WinCC archives are reconnected to an SQL Server. The archives are then available for access using WinCC OLE DB Provider.

Local archive data may be displayed, searched or analyzed, e.g. to search for process errors or to optimize processes.

Software requirements

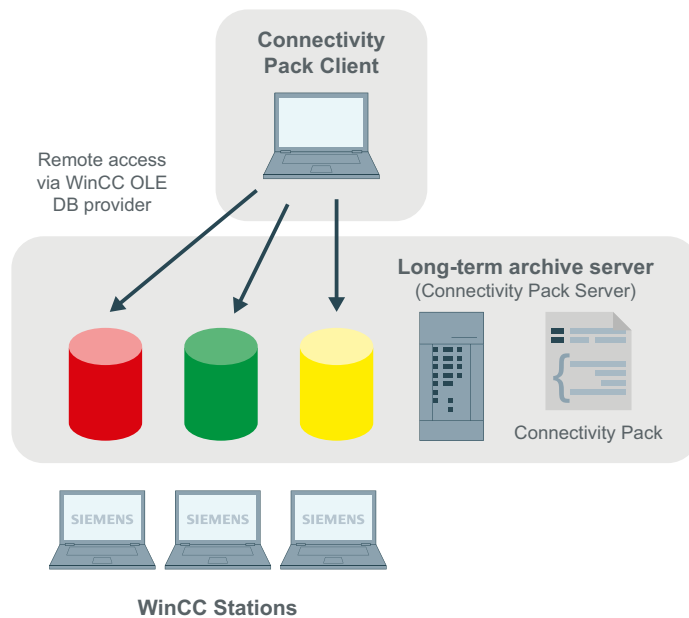
The WinCC station requires the following installations:

- WinCC Basic System
- A valid RT license for WinCC
- License for WinCC Option Connectivity Pack

See also

Examples for Access Using OLE DB Provider (Page 318)

2.3.4 Use Case 4: Remote Access to WinCC Archive Databases



Principles

A long-term archive server is used to secure database files of process value and message archives, for example, in a monthly backup.

With the Archive Connector, the swapped out WinCC archives are reconnected to an SQL Server. The archives are then available for access using WinCC OLE DB Provider.

The Connectivity Pack Client accesses the archives via the WinCC OLE DB Provider. Using a VB application, for example, the archives may be analyzed, and process values of a specific day may be displayed.

Note

If you access message archives or swapped out archives via "CC_ExternalBrowsing", this access may take several minutes.

Software Requirements

The long-term archive server requires the following to be installed:

- Connectivity Pack Server
- License for WinCC Connectivity Pack

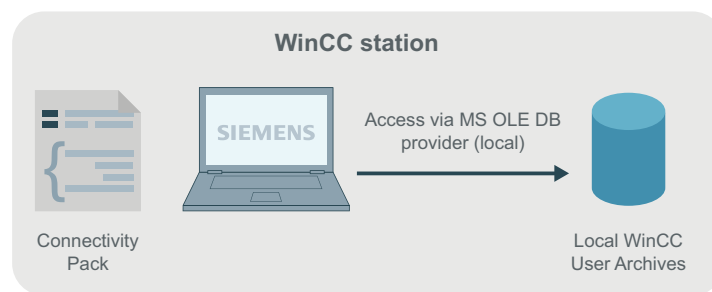
Access may take place under various configurations of the Connectivity Pack Client.

- A WinCC software like WinCC Basis, Web Navigator Server, DataMonitor Server or Connectivity Pack Server exists on the client computer.
The Connectivity Pack Client does not have to be installed explicitly. Licensing is provided through WinCC licenses.
- The client computer has no installation of WinCC software.
Then the Connectivity Pack Client needs to be installed on the client computer.

See also

Examples for Access Using OLE DB Provider (Page 318)

2.3.5 Use Case 5: Local Access to WinCC User Archive



Principles

An application accesses the local archive WinCC user archives using the MS OLE DB Provider.

Using a VB application, for example, you may display, search, and write back modified values for local archive data.

Software requirements

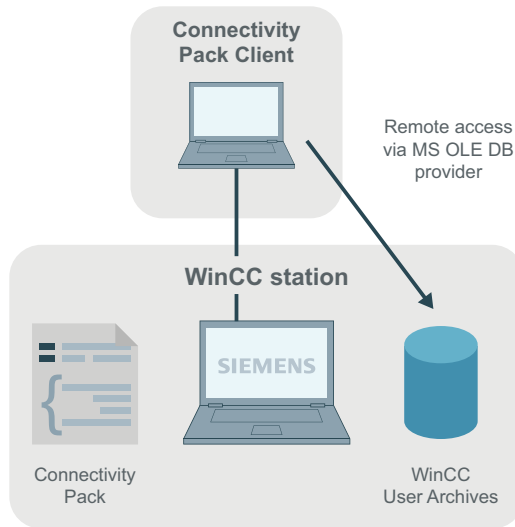
The WinCC station requires the following installations:

- WinCC Basic System
- A valid RT license for WinCC
- License for WinCC Option Connectivity Pack

See also

Examples for Access Using OLE DB Provider (Page 318)

2.3.6 Use Case 6: Remote Access to WinCC User Archives



Principles

The Connectivity Pack Client accesses the WinCC user archives using the MS OLE DB Provider.

Using a VB application, for example, you may display, search, and write back modified values for archive data.

Software requirements

The WinCC server requires the following installations:

- WinCC Basic System
- A valid RT license for WinCC
- License for WinCC Connectivity Pack

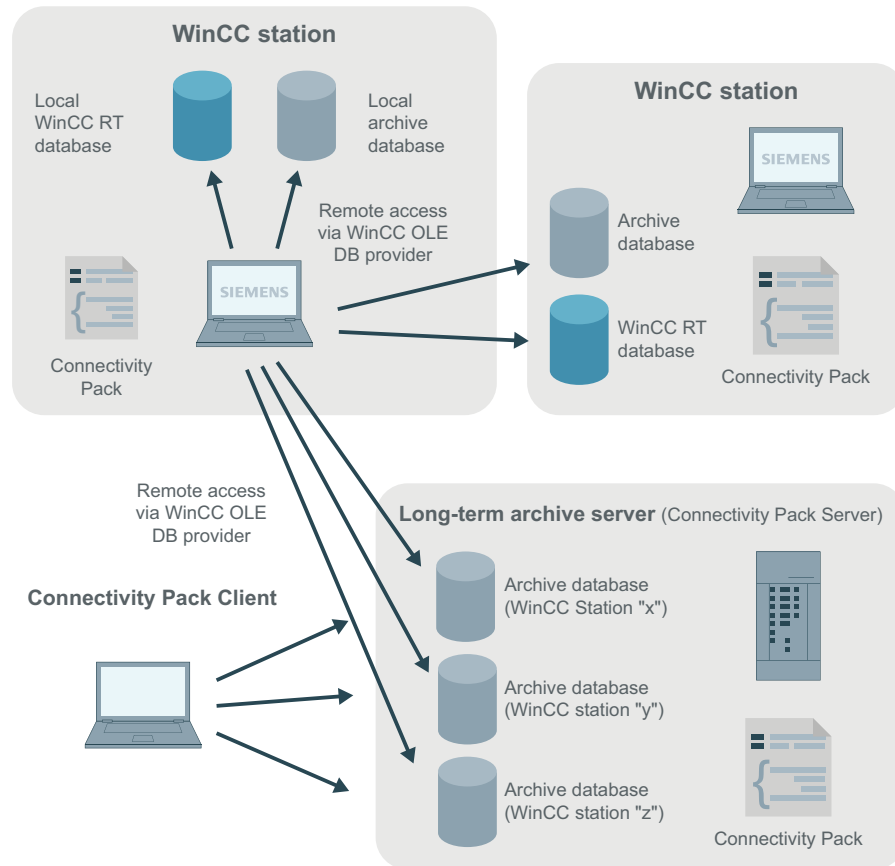
Access may take place under various configurations of the Connectivity Pack Client.

- A WinCC software like WinCC Basis, Web Navigator Server, DataMonitor Server or Connectivity Pack Server exists on the client computer. The Connectivity Pack Client does not have to be installed explicitly. Licensing is provided through WinCC licenses.
- The client computer has no installation of WinCC software.
Then the Connectivity Pack Client needs to be installed on the client computer.

See also

Examples for Access Using OLE DB Provider (Page 318)

2.3.7 Use Case 7: Access Via the WinCC OLE DB Provider



Principles

WinCC OLE DB Provider may be used to access WinCC databases while employing the Wizard "SQL Server Import/Export".

The Wizard "SQL Server Import/Export" enables data to be extracted from different sources and their export into other formats, e.g. in Excel table. Databases are linked using OLE DB, and access to WinCC databases using WinCC OLE-DB Provider. You can save the inquiry of data in a DTSX-Package.

The DTSX-Packages can be bound in scripts, to obtain a time-controlled inquiry and transfer of data into the target format. Equally, tasks may be tied into packages, for example, in order to initiate a notification by mail following execution of the package.

Using WinCC computers, access to runtime and archive databases may be established locally or remotely. In the case of long-term archive servers, local or remote access is only possible to the archive databases since they have no runtime databases.

Software requirements

The WinCC station requires the following installations:

- WinCC Basic System
- A valid RT license for WinCC
- License for WinCC Option Connectivity Pack

For further information, refer to the chapter "Configure Access via the Wizard SQL Server Import/Export."

See also

Examples for Access Using OLE DB Provider (Page 318)

Configure Access via the Wizard "SQL Server Import/Export" (Page 199)

2.3.8 Access Using OPC to WinCC Archives, Tags, and Messages

Introduction

OPC enables licensed access to online and archive data of WinCC. WinCC OPC-Servers provide WinCC data to the OPC client through the OPC software interface. As OPC client, any software can be implemented which is based on the respective OPC specification.

OPC DA

The WinCC OPC DA server makes the data from the WinCC project available to other applications. These applications may be running locally or on computers linked to the network environment. In this way WinCC tags can for example be exported to Microsoft Excel. The WinCC-OPC-DA server and its licensing are components of the WinCC base system.

OPC XML

Within a distributed system, WinCC clients have views of several WinCC servers. The WinCC OPC-XML server provides the OPC-XML client with the OPC process data as a web service. You can access the web service via the Internet using HTTP. The OPC XML client is no longer limited to the local network. In this way, OPC XML clients can access WinCC Runtime data via any platform as well as through an intranet or the Internet.

OPC HDA

Using the OPC HDA (Historical Data Access) server permits access to historical data of the WinCC archive system.

Installations without write access permit only reading and analyzing of WinCC archive data. Write access permits analyzing, adding, deleting, and updating of data.

An OPC HDA client may be used for analysis and evaluation of archive data and for process controlling of archives from different OPC HDA servers.

Note

OPC HDA does not permit access to message archives. Application permits access to process value archives only.

OPC A&E

The OPC A&E (Alarms & Events) server permits forwarding or acknowledging of WinCC messages.

An OPC A&E client, for example, may be used for analysis and joint archiving of alarms from different OPC A&E servers.

WinCC OPC-Servers in a Redundant System

In a redundant system, the WinCC servers monitor each other during runtime for early recognition of any server outage. The WinCC OPC-Servers make WinCC Runtime data available to the OPC client, using the OPC software interface. An OPC client with a simultaneous view of several WinCC-OPC-Servers can be used for centralized monitoring of various redundant systems.

As OPC client, any software can be implemented which is based on the respective OPC specification.

For additional information, please refer to chapter "OPC" - Open Connectivity.

Note**Error OPC_E_MAXEXCEEDED for archive access via OPC**

If the OPC client requests more than 2,000 values during synchronous or asynchronous data reading, the request is rejected with the OPC_E_MAXEXCEEDED error message. This limit serves to limit the computer load and duration of the call.

This limit does not apply if the entire time range is read.

2.3.9 Transparent access to archived data

Introduction

The archiving of process values and messages is used to register, manage and archive process data from an industrial system.

The registered process data is swapped out onto an archive server, e.g. a "Process Historian", by the WinCC stations at regular intervals.

The archived process data of a longer time period are therefore distributed to two archive databases.

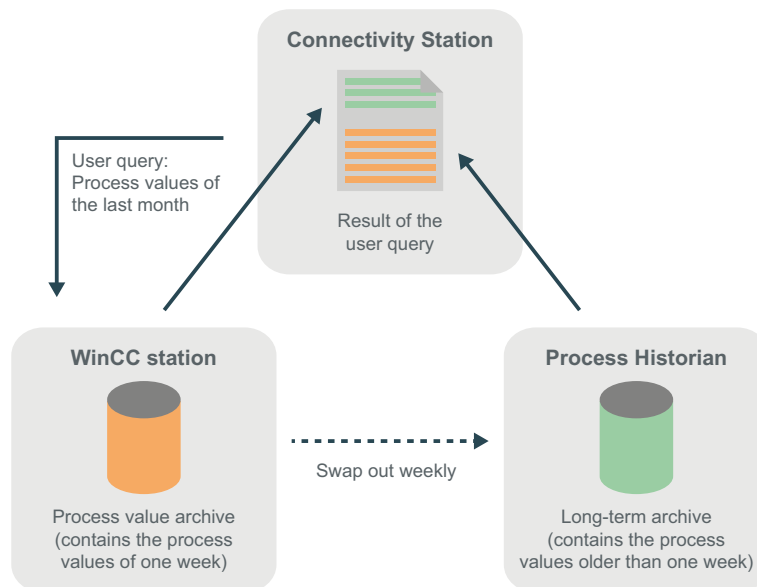
The transparent access will ensure that the requested process data from the two archive databases are combined.

Note

A Multiclient can also be used for transparent access instead of a Connectivity Station.

How it works

The following screen will show the principle of transparent access using an example of a user query for process values of the previous month:



The result of the user query is shown to the user as though the process values stem from a data source.

Transparent access in redundant systems

With redundant systems, the transparent access functions by the same principle, but with the following difference:

If a server fails during a user query, the user query will automatically be rerouted to the redundant partner server.

Transparent access with OPC

With OPC, you have transparent access to all archive databases of the WinCC stations:

OPC Server	Server name
OPC DA	WinCCConnectivity.OPCDAServer
OPC HDA	WinCCConnectivity.OPCHDAServer.1
OPC A&E	WinCCConnectivity.OPCAEServer.1

Transparent access via OLE DB-Provider

Using OLE DB-Provider you can access process value archives in a transparent manner.

Use the following syntax for transparent access for database link:

Data source

<SYMBOLIC COMPUTER NAME>::\WinCC

Catalog

Name of the WinCC project

2.3.10 Functions of SQL Servers

Introduction

In the following you find a short description of important functions already implemented in Microsoft SQL Server.

The technical documentation for the Microsoft SQL Server is made available by Microsoft on the Internet:

- SQL Server 2019 documentation (<https://docs.microsoft.com/en-us/sql/sql-server/?view=sql-server-ver15>)

Functions

Wizard "SQL Server Import/Export"

Use the "SQL Server Import/Export" wizard to extract data coming from distributed sources. You can transfer this data to one or more destinations.

A description of a use case can be found in the sections "Access via WinCC OLE DB Provider (Page 167)" and "Configure Access via the Wizard "SQL Server Import/Export" (Page 199)".

Jobs and Alerts

A job is a series of operations that are executed sequentially by the SQL Server Agent.

Extensive functions, such as Transact SQL scripts, command line applications and ActiveX scripts, can be executed in a job.

Jobs allow the execution of repetitive or time-controlled tasks.

Through settings of displays, so-called "Alerts", a job may automatically inform the user of the execution status.

Backup

The "Backup" component of the SQL server provides important protection for critical data in SQL server databases.

This will prevent damage caused by memory media malfunctions, user errors or the permanent loss of a server.

2.3 Applications

In addition, the component can be useful in other cases, for example:

- Copying databases between different servers
- Making a copy of a database via backup and subsequent restore to another computer

Replication

The "Replication" component enables copying, distributing, and modifying of data within the corporate level.

For this purpose, SQL server contains several methods and options for designing a replication, implementation, monitoring and administration.

In this way, SQL server provides the required functionality for distributing data and maintaining data consistency.

Database Maintenance Plans

After creating and supplementing objects and data and using them, maintenance of a database may also be required.

For example, it is important to back up the database regularly or create new indexes to improve performance.

Take these items into consideration during creation of the database to minimize the effect on users and to minimize the time and resources required for such maintenance.

You can use a wizard and the "Database Maintenance Plans" component to create one or more maintenance schedules.

Linked Server

The Microsoft SQL Server allows creating a connection to OLE DB databases by using the "Linked Server".

The use of a "Linked Server" offers the following advantages, for example.

- Accessing data records from the OLE DB databases and displaying them in tabular form using Transact-SQL instructions.
- Transmission of commands to the OLE DB data sources and tabular representation of the result data via Transact-SQL instructions.

A description of a use case for WinCC OLE DB Provider as "Linked Server" can be found in the section "Overview: WinCC/Connectivity Pack (Page 156)".

See also

Overview: WinCC/Connectivity Pack (Page 156)

Configure Access via the Wizard "SQL Server Import/Export" (Page 199)

Use Case 7: Access Via the WinCC OLE DB Provider (Page 167)

SQL Server 2019 documentation (<https://docs.microsoft.com/en-us/sql/sql-server/?view=sql-server-ver15>)

2.4 Access Via the OLE DB Provider

2.4.1 Access to Archive Data Using OLE DB Provider

Introduction

Using OLE DB, you have the following options for accessing WinCC archive data and for displaying these using an external interface.

Access using WinCC OLE DB Provider

WinCC OLE DB provides access to all WinCC archive data.

Depending on the configuration, process data of WinCC are stored in compressed form. WinCC OLE DB Provider permits transparent access even to these data.

Use the "SQL Server Import / Export Wizard" to take advantage of standard SQL queries. You can save the unzipped files to an intermediate database using the wizard; you access the database with standard SQL queries.

Access with Microsoft OLE DB

Microsoft OLE DB provides access to all WinCC user archives.

Note

Microsoft OLE DB is only tested and released for access to WinCC User Archives but not to alarm and process value archives.

Use the WinCC OLE DB Provider to access message and process value archives.

Configuration Options

For access to databases with WinCC OLE DB, you may write your own applications. For the communication with the WinCC OLE DB Provider, applications - created with, for example, Visual Basic, VBScript or VBA - use the ADO DB.

Note

Special characters in tag names

Please note that programming languages such as Visual Basic, VBScript or VBA only allow the following characters in the tag names: "A...Z", "a...z", "0...9" and "_".

In WinCC if you use special characters such as ",", " or ";" in the tag names then the script will be aborted with an error message. In such a case use the "Tag-ID" to access a tag with special characters in the script name.

The procedure in principle

1. For access to archive data, the computer must have WinCC Basic, Connectivity Pack Server or Connectivity Pack Client installed.
2. For swapped out archives, establish the connection between the SQL database and the swapped out archives with the WinCC Archive Connector.

Note

WinCC RT archives in directory "<Project Directory> \ ArchiveManager" and the associated subdirectories must not be connected to or disconnected from the Archive Connector since their connection to the SQL server is managed by the WinCC Basic system.

3. Establish the connection to the database, for example by using MS Excel or your own application. Define the desired selection criteria and read the archive data.
4. The query result, for example, may be displayed in MS Excel or be exported as a csv file.

See also

Configure Access via the Wizard "SQL Server Import/Export" (Page 199)

Querying the Archive Data (Page 183)

Establishing the Connection to the Archive Database (Page 179)

WinCC Archive Connector (Page 175)

Bases of OLE DB (Page 174)

2.4.2 Bases of OLE DB

Introduction

Using the OLE DB interface and the associated database provider supplied by WinCC, you have access to process value and message archives.

OLE DB

OLE DB is an open standard for a fast access to different databases. It is irrelevant whether the database is relational or not.

The connection between the OLE DB level and the database is established through a database provider.

OLE DB interfaces and providers are offered from various manufacturers.

WinCC OLE DB Provider

Using WinCC OLE DB Provider, you may directly access WinCC archive data stored in the MS SQL server database. Depending on the configuration, process data of WinCC are stored in compressed form. WinCC OLE DB Provider permits transparent access even to these data.

Note

If WinCC closes a full archive and opens a new one, no data from the message and process value archives are read momentarily via the OLE DB Provider.

Microsoft OLE DB

Microsoft OLE DB only provides access to WinCC user archives.

As protection from unauthorized access using MS OLE DB, the administrator of the databases can take appropriate actions. Additional information may be found in Chapter "Security Settings for Access to SQL Databases Using MS OLE DB".

Note

Microsoft OLE DB is only tested and released for access to WinCC User Archives but not to alarm and process value archives.

Use the WinCC OLE DB Provider to access message and process value archives.

See also

Security Settings During Access to SQL Databases Using MS OLE DB (Page 208)

Access to Archive Data Using OLE DB Provider (Page 173)

2.4.3 WinCC Archive Connector

Introduction

The WinCC "Archive Connector" is used for configuring the access to the archive database. The tool is an integral part of WinCC DataMonitor and Connectivity Pack. With the Archive Connector, already swapped out WinCC archives can be reconnected to an SQL Server. DataMonitor client or WinCC OLE DB provider can then access the archives.

2.4 Access Via the OLE DB Provider

Functions of the WinCC Archive Connector:

- Manual Connection: Local databases may be selected and connected to the local SQL server.
- Manual Disconnection: Connected databases may be selected and disconnected from the SQL server.
- Automatic Connection: Local directories can be selected in which WinCC archives have been exported. All the archives are automatically linked to the SQL servers which were added to the selected directories from the moment change monitoring was activated.

The Archive Connector can only be operated on a local SQL server and a license for WinCC DataMonitor or WinCC Connectivity Pack.

Once the configuration has been completed, the Archive Connector may be terminated.

Note

WinCC RT archives in directory "<Project Directory> \ ArchiveManager" and the associated subdirectories must not be connected to or disconnected from the Archive Connector since their connection to the SQL server is managed by the WinCC Basic system.

The path for the swapped out WinCC archives is set in WinCC with the Archive Configurator, e.g. of Tag Logging, not with the WinCC Archive Connector.

If access is to be made to swapped archives which are on interchangeable media such as tape or MOD drives, pay attention that the connection to these archives on this medium is disconnected using the Archive Connector before changing the medium in the drive. After changing the medium, the user should check the Archive Connector whether or not the archives on the new medium are connected.

Configuration of the WinCC Archive Connector should be accessible to a limited circle of people only. Therefore, access to the Tool should be protected using Windows user authorization "Administrators" or other Windows protective measures, such as storage in a protected directory.

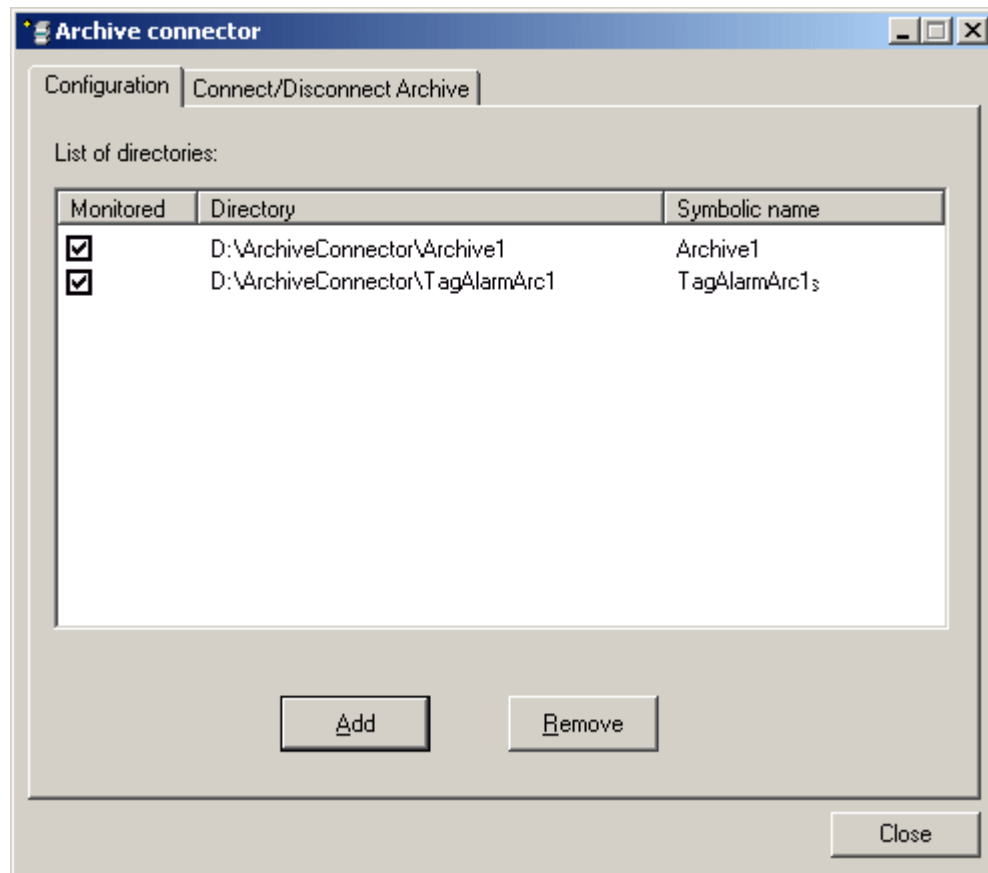
Note

Use the Archive Connector to access the linked archives using the Connectivity Pack or DataMonitor.

The following objects do not give any access to the linked archives using Archive Connector:

- WinCC Alarm Control
 - WinCC Online Trend Control
 - WinCC Online Table Control
 - WinCC Online Function Control
-

The "Configuration" Tab



In the "Configuration" tab, archiving folders are displayed and managed that are to be accessed through the Web or the WinCC OLE DB Provider.

Via buttons, archiving folders can be added or removed. For each archiving folder, a symbolic, unique name has to be assigned during the configuration.

DataMonitor client or the WinCC OLE DB-Provider use the symbolic name to access the archive.

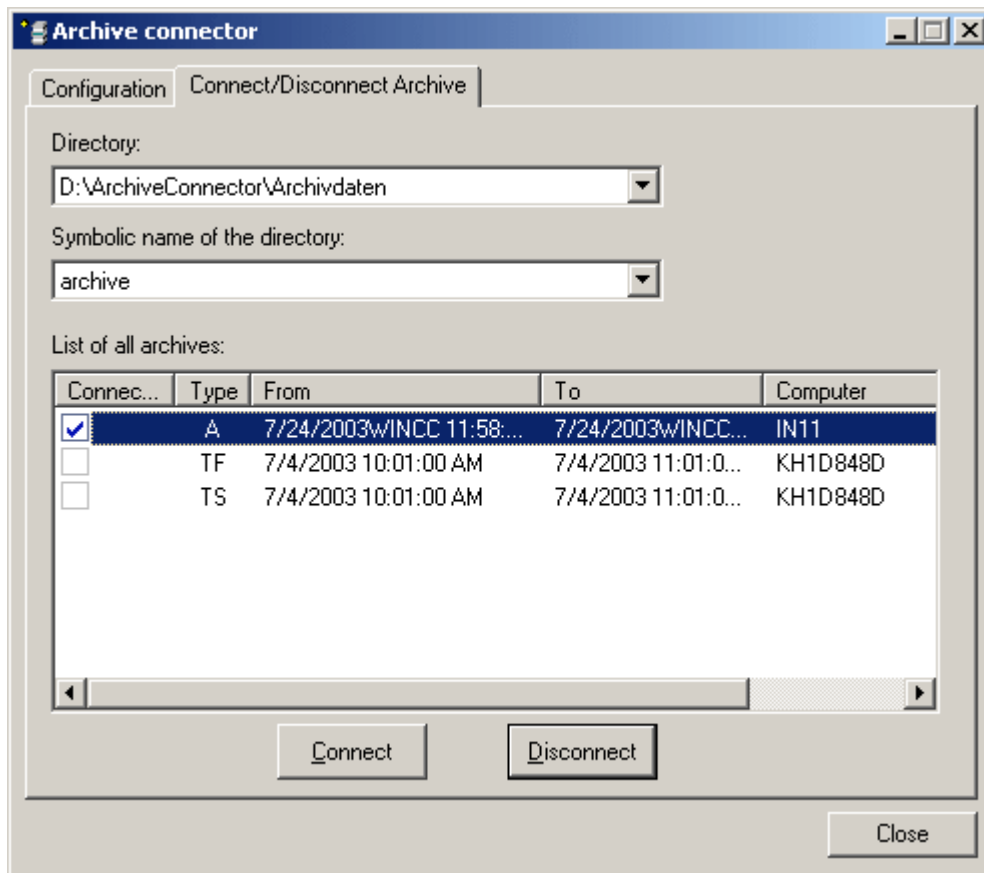
The name is also used for managing and connecting exported data from multiple computers or projects.

The symbolic names must only contain SQL-syntax-permissible characters.

By activating the corresponding checkbox, all archives added to the selected folder at the time of activation will automatically be connected to the SQL Server.

If you activate or deactivate monitoring, the changes will not be activated until you close the Archive Connector.

The "Connect/Disconnect Archive" Tab



The "Connect/Disconnect Archive" tab lists all archives existing in the archiving directories.

The connection status of each archive is displayed. The connection to the archives can be established or terminated via buttons.

The archive type is shown in the "Type" field:

- "A" = Alarm Logging;
- "TF" = Tag Logging (Fast);
- "TS" = Tag Logging (Slow).

The columns "From" and "To" provide information on the local time zone.

Note

The connection of multiple, swapped-out archives to the SQL server may take several seconds.

It is not possible to connect a database file with the same name twice.

The WinCC Archive Connector connects finalized and backed up (swapped-out) archives to the SQL server. Archives not finalized are not supported.

The user interface language of the Archive Connector is based on the settings of the regional and language options in Windows.

Note

Archives created with SQL Server 2000 can only be connected if you remove the write protection of the archive. Archives that are once linked can no longer be linked using the Archive Connector of the Connectivity Pack under SQL Server 2000.

In order to connect swapped out archives on CD or DVD, copy the archives to a media where you will be able to remove the write protection.

2.4.4 Establishing the Connection to the Archive Database

Introduction

For ActiveX data objects (ADO), the connection between the application and the archive database is established by the connection object.

An important parameter here is the `ConnectionString`.

The `ConnectionString` contains all necessary information for access to the database using OLE DB Provider.

Structure of theConnectionString

"Provider = Name of the OLE DB Provider; Catalog=Database name;Data Source=Server name;"

Parameter	Description
Provider	Name of the OLE DB Provider, e.g.: WinCCOLEDBProvider
Catalog	Name of the WinCC database With WinCC RT databases, you use database names that end in "R": <Database name_R> The database "CC_ExternalBrowsing" can also be used. If you have connected swapped-out WinCC archives to the SQL Server via the WinCC Archive Connector, use their symbolic name. Note Enter the WinCC project name for "Catalog" for transparent access; e.g.: - Catalog=WinCC_Project_Name Note If you access message archives or swapped out archives via "CC_ExternalBrowsing", this access may take several minutes.
Data Source	Server name Local: .\WinCC" or "<Computer Name>\WinCC Remote: <Computer name>\WinCC Note With transparent access to an archive server or with redundant servers via the OLE DB Provider, enter the following for "Data Source": <Symbolic Computer Name>:\WinCC. Note Use the archive tag name to directly access an archive tag in a database containing 8-byte value IDs, e.g. on an archive server. In this case, the archive server returns the server ID and not the archive tag ID as ID: <Symbolic computer name>\<Archive_Var_Name>

Example Process Value and Message Archive:

In the following example, a connection object is created with subsequent opening of the connection to the WinCC database (process value and message archive).

```
Set conn = CreateObject("ADODB.Connection")
```

```
conn.open
```

```
"Provider=WinCCOLEDBProvider.1;Catalog=CC_OpenArch_03_05_27_14_11_46  
R;Data Source=.\WinCC"
```

Example User Archive:

In the following example, a connection object is created with subsequent opening of the connection to the WinCC user archive.

```
Set conn = CreateObject("ADODB.Connection")  
conn.open "Provider=SQLNCLI11; Integrated Security=SSPI;  
Persist Security Info=false; Initial  
Catalog=CC_OpenArch_03_05_27_14_11_46R; Data Source=.\WinCC"
```

Note

In order to improve performance during local access, enter "<Computer name>\WinCC" as the data source instead of ".\WinCC".

See also

Example: Configuring Access to Archive Data Using DataConnector Wizard (Page 320)

Example: Configuring the Access to Archive Data Using VB (Page 318)

Query for User Archives (Page 196)

Querying Alarm Message Archives (Page 192)

Querying Process Value Archives (Page 184)

2.4.5 Querying the Archive Data

2.4.5.1 Displaying Process Value Archives

Introduction

The query result is returned as recordset.

In this section, the structure of the recordset for process value archives is described.

Extended "TAG_EX" schema

To access tags with the following data type, use the extended "TAG_EX" schema:

- String
- Int64
- UInt64

For compatibility reasons, you can also use "TAG_EX" to access tags that are normally accessed using the "TAG" schema.

If you use the "TAG" schema to read String values, the value "0" is returned. This means that all text tags have the value "0".

Recordset structure**Schema "TAG:R"**

Field name	Type	Comment
ValueID	Integer 4 bytes or Integer 8 bytes	Unique identification of value. The length depends on the type of query.
TimeStamp	Datetime	Time stamp
RealValue	Real 8 bytes	Tag value
Quality	Integer 4 bytes	Quality code of value (e.g. "good" or "bad").
Flags	Integer 4 bytes	Internal control parameter

Schema "TAG_EX:R"

Field name	Type	Comment
ValueID	Integer 4 bytes or Integer 8 bytes	Unique identification of value. The length depends on the type of query.
TimeStamp	Datetime	Time stamp
TimeStampExt	Datetime	Time stamp of the external device
VariantValue	Variant 16 bytes	Tag value
Bytes	Real 8 bytes	Tag value
Quality	Integer 4 bytes	Quality code of value (e.g. "good" or "bad").
Flags	Integer 4 bytes	Internal control parameter

See also

Querying the Archive Data (Page 183)

Establishing the Connection to the Archive Database (Page 179)

Access to Archive Data Using OLE DB Provider (Page 173)

Bases of OLE DB (Page 174)

2.4.5.2 Querying the Archive Data

Introduction

The queries are forwarded to the database by the command object. An important parameter, aside from "ConnectionString", is CommandText. The CommandText transmits the query. The result is returned as the Recordset.

Note

Time range for archive inquiries for message and process values

If the query for message or process value archives specifies a time range for which no messages or other values exist within the archives, no information message or other status display occurs. If this status is to be displayed, error handling must be implemented by the user.

A simple version of this error handling routine is described in the sample script under the topic "Example: Reading message archive data via the WinCC OLE DB Provider".

In the following examples, a command object each is generated and the query transmitted as CommandText.

In the following structure examples, CommandText also includes the ConnectionString whose structure is described under "Establishing Connection to Archive Database".

Structure of CommandText

Process Value Archives:

```
Set oRs = CreateObject("ADODB.Recordset")
Set oCom = CreateObject("ADODB.Command")
oCom.CommandType = 1
Set oCom.ActiveConnection = conn
oCom.CommandText = "TAG:R, 'PVArchive\Tag1', '0000-00-00
00:10:00.000', '0000-00-00 00:00:00.000'"
```

Alarm Message Archives:

```
Set oRs = CreateObject("ADODB.Recordset")
Set oCom = CreateObject("ADODB.Command")
oCom.CommandType = 1
Set oCom.ActiveConnection = conn
oCom.CommandText = "ALARMVIEW:Select * FROM AlgViewEnu"
```

User archives

```
Set oRs = CreateObject("ADODB.Recordset")
Set oCom = CreateObject("ADODB.Command")
oCom.CommandType = 1
```

2.4 Access Via the OLE DB Provider

```
Set oCom.ActiveConnection = conn  
oCom.CommandText = "SELECT * FROM UA#Test"
```

Specifying the RecordSet location

To specify the location of RecordSet for query of the archive data, you need to set the value "3" for the "CursorLocation" property, for example, "conn.CursorLocation = 3". The RecordSet is created on the client.

See also

Example: Reading Process Value Archive With WinCC OLE DB Provider and Visual Basic 6 (Page 326)

Displaying User Archives (Page 198)

Displaying Alarm Message Archives (Page 194)

Displaying Process Value Archives (Page 181)

Query for User Archives (Page 196)

Querying Alarm Message Archives (Page 192)

Querying Process Value Archives (Page 184)

Establishing the Connection to the Archive Database (Page 179)

WinCC Archive Connector (Page 175)

Bases of OLE DB (Page 174)

Examples for Access Using OLE DB Provider (Page 318)

2.4.5.3 Querying Process Value Archives

Principle

With the following query, a process value archive can be accessed.

The data can be selected using filter criteria.

The queries are forwarded to the database by the command object.

Note**Length of the ValueID**

The length of the ValueID can be different:

- For example, databases processed on a central archive server have a ValueID length of 8 bytes.
It includes a ValueID assigned by the respective server in the LO-DWORD area and a server ID in the HI-DWORD area.
- For all other databases, the ValueID is 4 bytes long.
It includes only the unique ValueID assigned by the WinCC server.

The 4-byte query via TAG:R and TAG_EX:R is still possible for compatibility in any case. The 4-byte ValueID returned here is no longer unique in the case of databases with 8-byte ValueIDs.

Queries for process value archives are limited to a maximum of 20 tags, each with a maximum of 128 characters per tag.

Syntax

The query must not contain any spaces.

Request of ValueIDs 8 Bytes long:

```
TAG_LLVID:R,<ValueID or  
ValueName>,<TimeBegin>,<TimeEnd>[,<SQL_clause>][,<TimeStep>]
```

Request of ValueIDs 4 Bytes long:

```
TAG:R,<ValueID or ValueName>,<TimeBegin>,<TimeEnd>[,<SQL_clause>]  
[,<TimeStep>]
```

Schema "TAG_EX"

To access process values of the following tag types, use the "TAG_EX:R" schema:

- Text tag, 8-bit character set / 16-bit character set
- Floating-point number 64-bit IEEE 754

Replace "TAG_LLVID:R" with "TAG_LLVID_EX:R".

Parameter

Parameter	Description
ValueID	Value ID from the database table Multiple names are possible, for example: "TAG:R,(ValueID_1;ValueID_2;ValueID_x),<TimeBegin>,<TimeEnd>"
ValueName	ValueName in the format 'ArchiveName\Value_Name'. The parameter <ValueName> must be enclosed in single quotes. Multiple names are possible, for example: "TAG:R,('ValueName_1';'ValueName_2';'ValueName_x'), <TimeBegin>,<TimeEnd>" Note: Tag names Programming languages such as Visual Basic, VBScript and VBA allow only the following characters in tag names: "A...Z", "a...z", "0...9" and "_" If you use special characters such as ",", or ";" in WinCC tag names, the script will be aborted with an error message. To address a tag with special characters in the name in the script, use the "Tag ID".
TimeBegin	Start time in the format: 'YYYY-MM-DD hh:mm:ss.msc' While using <TimeStep> you must specify <TimeBegin> as absolute time. A relative statement or "0000-00-00 00:00:00.000" are not permitted.
TimeEnd	End time in the format: 'YYYY-MM-DD hh:mm:ss.msc'
SQL_Clause	Filter criterion in SQL syntax: [WHERE search_condition] [ORDER BY {order_expression [ASC DESC] }] "ORDER BY" criterion can only be used with the given sort sequence "{order_expression [ASC DESC] }". Example: The following query returns all values of the tags "ValueName_1" and "ValueName_2" which are below 50 or above 100. "TAG:R,('ValueName_1';'ValueName_2'),<TimeBegin>,<TimeEnd>, 'WHERE RealValue > 100 OR RealValue < 50'"

Parameter	Description	
TimeStep	Values in the stated time interval are summarized, beginning with the start time <TimeBegin>. - Format: 'TIMESTEP=x,y' - x = interval in seconds - y = Aggregation type, defines the interval result The following values are possible for aggregation type:	
	Without interpolation	With interpolation
	1 (FIRST)	257 (FIRST_INTERPOLATED)
	2 (LAST)	258 (LAST_INTERPOLATED)
	3 (MIN)	259 (MIN_INTERPOLATED)
	4 (MAX)	260 (MAX_INTERPOLATED)
	5 (AVG)	261 (AVG_INTERPOLATED)
	6 (SUM)	262 (SUM_INTERPOLATED)
	7 (COUNT)	263 (COUNT_INTERPOLATED)
Interpolation Without interpolation means: - If no values are present in the interval, no interval result will be returned. With interpolation means: - If no values are present in the interval, the value is calculated by linear interpolation of the results of the neighboring intervals that are not empty. - No extrapolation is done. Example: For TIMESTEP=60.257 for each interval of 60 seconds, the first value of this interval or - if there are no values in this interval - the linear, interpolated value from the first values of the neighboring intervals will be returned. "TAG:R,1,'2004-07-09 09:03:00.000','0000-00-00 00:10:00.000',TIMESTEP=60,257" "STRING" data type For the "STRING" data type, only the following aggregation types are supported: 1 (FIRST) 2 (LAST) 7 (COUNT) Interpolation is not supported for the "STRING" data type. The algorithm supports only numeric types (integers and fixed-point numbers).		

Note**<TimeBegin> and <TimeEnd>**

<TimeBegin> and <TimeEnd> must never both be "ZERO" = "0000-00-00 00:00:00.000".

Performance: Use ValueID instead of ValueName

In order to improve performance, use the parameter "ValueID" instead of "ValueName" during the query.

The "ValueID" may be determined from the table "Archives".

Time unit under 1 second

Some applications cannot process the time in steps of 1 ms with process values which can lead to inaccuracies.

An example for the ungrouping of the milliseconds from the time stamp of process values can be found in the VB script "SplitDateTimeAndMs" under:

- "Example: Reading Process Value Archive With WinCC OLE DB Provider and Visual Basic 6 (Page 326)"
-

Selection of an Absolute Time Interval

Reading from start time <TimeBegin> until the end time <TimeEnd> .

Example A1:

Reads the values of the ValueID 1 from start time 9:03 hours to end time 9:10 hours.

```
"TAG:R,1,'2004-07-09 09:03:00.000','2004-07-09 09:10:00.000'"
```

Selection of a Relative Time Interval

Reads from beginning of recording:

```
<TimeBegin> = '0000-00-00 00:00:00.000'
```

Reads until end of recording:

```
<TimeEnd> = '0000-00-00 00:00:00.000'
```

<TimeBegin> and <TimeEnd> should both not be "ZERO" = '0000-00-00 00:00:00.000'.

Note**Relative time period: Do not use months**

Enter a relative period you want to query in a linked archive database using the following format:

- 0000-00-DD hh:mm:ss.msc

If you indicate the time frame in months, the content can be faulty, because a month can have 28 to 31 days.

Example B1:

Reads the absolute time from "TimeBegin" to end of recording, i.e. the last archived value.

```
<TimeBegin> = '2003-02-02 12:00:00.000', <TimeEnd> = '0000-00-00  
00:00:00.000'
```

Example B2:

Reads the absolute time from "TimeBegin" for the next 10 seconds.

```
<TimeBegin> = '2003-02-02 12:00:00.000', <TimeEnd> = '0000-00-00  
00:00:10.000'
```

Example B3:

Reads 10 seconds backward from the absolute time from "TimeEnd".

```
<TimeBegin> = '0000-00-00 00:00:10.000', <TimeEnd> = '2003-02-02  
12:00:00.000'
```

Example B4:

Reads the values of the last hour starting from the time of the last archived value for multiple valueIDs (1;3;5;6).

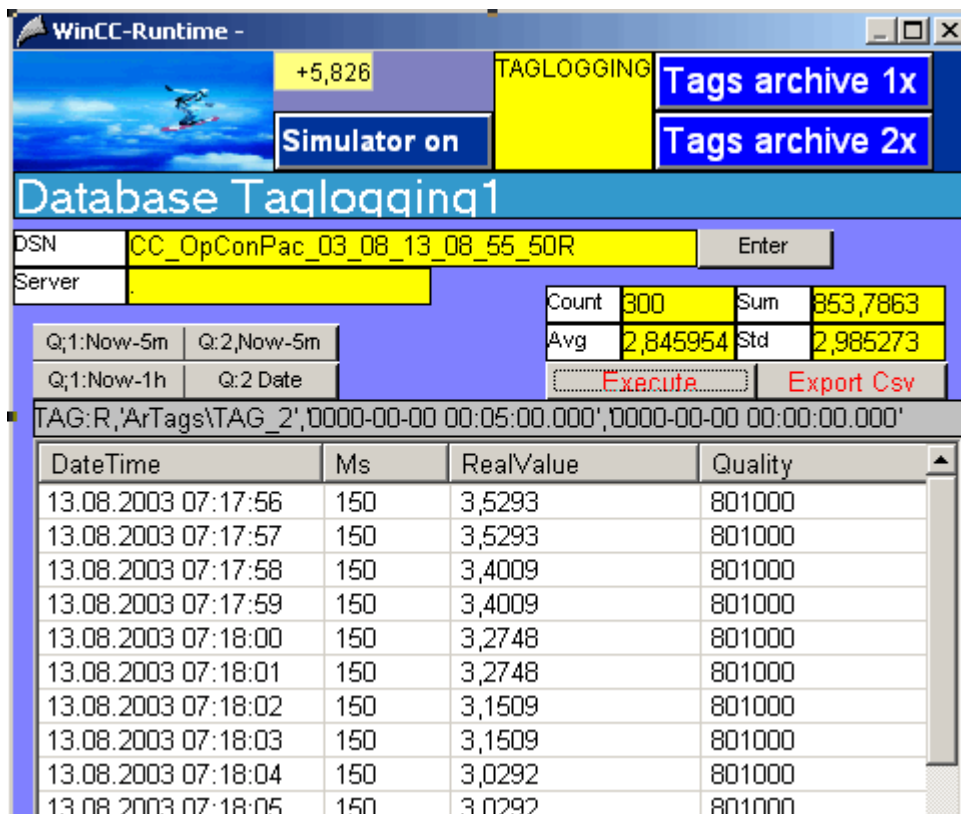
```
"TAG:R, (1;3;5;6), '0000-00-00 01:00:00.000', '0000-00-00  
00:00:00.000' "
```

Example B5:

Reads the values of the last five minutes starting from the time of the last archived value for "TAG_2" tag from the "ArTags" archive.

```
"TAG:R, 'ArTags\TAG_2', '0000-00-00 00:05:00.000', '0000-00-00  
00:00:00.000' "
```

The following diagram shows a possible result of this example:



Multiple Return Values to a Query Using a Filter on Tag Value

Example C1:

The following query also uses the <SQL_Clause> parameter and returns all tag values that have the ValueID "3" and "6" and are below 50 or above 100.

```
"TAG:R, (3;6), <TimeBegin>, <TimeEnd>, 'WHERE RealValue > 100 OR RealValue < 50'"
```

Query with parameter <TimeStep>

Example C2:

The following query uses the <TimeStep> parameter and returns all values of ValueID "1" - starting from start time "TimeBegin" till 5 minutes later in intervals of "60" seconds with the aggregation type "5" = "Average value without Interpolation".

```
"TAG:R,1, '2004-10-13 17:00:00.000', '0000-00-00 00:05:00.000', 'TIMESTEP=60,5'"
```

The following diagram shows the query result:

- The left table displays the archive data which were archived in an archiving cycle of 30 seconds.
- The right table displays the query result.
It determines the average between two archive values at "0" seconds and "30" seconds, displayed with the first time stamp of the averaging interval, i.e. second "0".

TIMESTEP = 60,5



ValueID	Datetime	RealValue	Quality
1	2004-10-13 17:00:00.000	3.0	801000
1	2004-10-13 17:00:30.000	4.0	801000
1	2004-10-13 17:01:00.000	2.0	801000
1	2004-10-13 17:01:30.000	4.0	801000
1	2004-10-13 17:02:00.000	4.0	801000
1	2004-10-13 17:02:30.000	1.0	801000
1	2004-10-13 17:03:00.000	3.0	801000
1	2004-10-13 17:03:30.000	3.0	801000
1	2004-10-13 17:04:00.000	1.0	801000
1	2004-10-13 17:04:30.000	0.0	801000
1	2004-10-13 17:05:00.000	3.0	801000

ValueID	Datetime	RealValue	Quality
1	2004-10-13 17:00:00.000	3.5	801000
1	2004-10-13 17:01:00.000	3.0	801000
1	2004-10-13 17:02:00.000	2.5	801000
1	2004-10-13 17:03:00.000	3.0	801000
1	2004-10-13 17:04:00.000	0.5	801000
1	2004-10-13 17:05:00.000	3.0	801000

Example C3:

The following query uses the <TimeStep> parameter and returns all values of ValueID "1" and "2" - starting from start time "TimeBegin" till 2 minutes later in intervals of "15" seconds with the aggregation type "261" = "Average value with linear Interpolation".

```
"TAG:R, (1;2), '2004-10-13 17:00:00.000', '0000-00-00 00:02:00.000',  
'TIMESTEP=15.261'"
```

The following diagram shows the query result:

- The left table displays the archive data which were archived in an archiving cycle of 30 seconds.
- The right table displays the query result.
The archive values at "0" and "30" seconds are displayed in the query result unchanged with their time stamp.
For second "15," the linear, interpolated value is formed of archive values at seconds "0" and "30".
For the "45" second, the linear, interpolated value is taken from the archive values of "30" second of the same minute and the "0" second of the next minute.

TIMESTEP = 15, 261



ValueID	Datetime	RealValue	Quality
1	2004-10-13 17:00:00.000	3,0	801000
2	2004-10-13 17:00:00.000	12,0	801000
1	2004-10-13 17:00:30.000	4,0	801000
2	2004-10-13 17:00:30.000	14,0	801000
1	2004-10-13 17:01:00.000	2,0	801000
2	2004-10-13 17:01:00.000	16,0	801000
1	2004-10-13 17:01:30.000	4,0	801000
2	2004-10-13 17:01:30.000	17,0	801000
1	2004-10-13 17:02:00.000	4,0	801000
2	2004-10-13 17:02:00.000	14,0	801000
1	2004-10-13 17:02:30.000	1,0	801000
2	2004-10-13 17:02:30.000	13,0	801000
1	2004-10-13 17:03:00.000	3,0	801000
2	2004-10-13 17:03:00.000	13,0	801000

ValueID	Datetime	RealValue	Quality
1	2004-10-13 17:00:00.000	3,0	801000
1	2004-10-13 17:00:15.000	3,5	801000
1	2004-10-13 17:00:30.000	4,0	801000
1	2004-10-13 17:00:45.000	3,0	801000
1	2004-10-13 17:01:00.000	2,0	801000
1	2004-10-13 17:01:15.000	3,0	801000
1	2004-10-13 17:01:30.000	4,0	801000
1	2004-10-13 17:01:45.000	4,0	801000
1	2004-10-13 17:02:00.000	4,0	801000
2	2004-10-13 17:00:00.000	12,0	801000
2	2004-10-13 17:00:15.000	13,0	801000
2	2004-10-13 17:00:30.000	14,0	801000
2	2004-10-13 17:00:45.000	15,0	801000
2	2004-10-13 17:01:00.000	16,0	801000
2	2004-10-13 17:01:15.000	16,5	801000
2	2004-10-13 17:01:30.000	17,0	801000
2	2004-10-13 17:01:45.000	15,5	801000
2	2004-10-13 17:02:00.000	14,0	801000

See also

Example: Reading Process Value Archive With WinCC OLE DB Provider and Visual Basic 6 (Page 326)

Displaying Process Value Archives (Page 181)

Configure Access via the Wizard "SQL Server Import/Export" (Page 199)

2.4.5.4 Querying Alarm Message Archives**Introduction**

With the following query, the message archive can be accessed.

The data can be selected using filter criteria. The queries are forwarded to the database by the command object.

You can find additional information of the status of messages in the WinCC Information System under:

- "Working with WinCC > ANSI-C Function for Creation of Functions and Actions > ANSI-C Function descriptions > Appendix > Structure Definitions > Structure Definition MSG_RTDATA_STRUCT".

When querying message archives, the result is summarized by archive, but without sorting the queried archive segments.

The filter condition needs to be extended accordingly if the segments are to be sorted, e.g., for the chronological sorting "ORDER BY DateTime ASC, MS ASC".

Syntax

```
ALARMVIEWEX:SELECT * FROM <ViewName>[WHERE <Condition>...., optional]
```

Parameter

Parameter	Description
ViewName	Name of the database table. The table has to be specified in the desired language. The "ViewName" for the five European language is e.g.: • ALGVIEWEXDEU: German message archive data • ALGVIEWEXENU: English message archive data • ALGVIEWEXESP: Spanish message archive data • ALGVIEWEXFRA: French message archive data • ALGVIEWEXITA: Italian message archive data The "ViewName" for the Asian language is e.g.: • ALGVIEWEXCHS: Chinese (simplified) message archive data • ALGVIEWEXCHT: Chinese (traditional) message archive data • ALGVIEWEXJPN: Japanese message archive data • ALGVIEWEXKOR: Korean message archive data Note The languages that are installed in the WinCC base system or that are configured in the WinCC Text Library are supported. Information concerning the possible query-languages or the respective "ViewName" can be found in the SQL-Server in the linked alarm archives under "Views". All languages that are supported in the corresponding archive are shown here with their IDs, e.g. "ALGVIEWEXENU".
Condition	Filter criterion, for example: • DateTime>'2003-06-01' AND DateTime<'2003-07-01' • DateTime>'2003-06-01 17:30:00' • MsgNr = 5 • MsgNr in (4, 5) • State = 2 With DateTime, only absolute time indications can be used.

Example 1:

Reads all entries of message number 5 that were recorded after July 5, 2003.

```
"ALARMVIEWEX:SELECT * FROM ALGVIEWEXENU WHERE MsgNr = 5 AND
DateTime>'2003-07-05' "
```

Example 2:

Reads all messages with a time stamp between July 3, 2003 and July 5, 2003.

2.4 Access Via the OLE DB Provider

```
"ALARMVIEWEX:SELECT * FROM ALGVIEWEXENU WHERE DateTime>'2003-07-03'
AND DateTime<'2003-07-05'"
```

The following picture shows a possible result of this example.

Database Alarms					
DSN	CC_OpConPac_03_07_30_15_59_32R			Enter	
Server				Count	4204
				Sum	287411
F:All	F:MsgNr=5		Avg	68,36608	Std
F:State=2	F:'Date1'< D<'Date2'				216,5581
			Execute		Csv + Hitlist
WHERE DateTime>'2003-07-03' AND DateTime <'2003-07-05'					
DateTime	MsgNr	State	Type		
08.07.2003 15:21:37	2	1	Alarm		
08.07.2003 15:21:59	1	1	Alarm		
08.07.2003 15:22:21	1	2	Alarm		
08.07.2003 15:22:21	2	2	Alarm		
08.07.2003 15:22:21	3	1	Warnung		
08.07.2003 15:22:43	1	16	Alarm		
08.07.2003 15:22:43	1	1	Alarm		
08.07.2003 15:23:05	2	16	Alarm		
08.07.2003 15:23:05	2	1	Alarm		
08.07.2003 15:23:05	1	2	Alarm		

See also

Displaying Alarm Message Archives (Page 194)

2.4.5.5 Displaying Alarm Message Archives

Introduction

The query result is returned as Recordset.

The table contains the structure of the Recordset for message archives.

You will find information about the status of messages in the WinCC Information System under "Working with WinCC > ANSI-C Function for Creation of Functions and Actions > ANSI-C Function descriptions > Structure Definitions > Structure Definition MSG_RTDATA_STRUCT".

Recordset structure for "ALARMVIEWEX"

Position	Field name	Type	Comment
1	MsgNr	Integer 4 bytes	Message number
2	State	Small integer 2 bytes	Status of the message

Position	Field name	Type	Comment
3	DateTime	DateTime 8 bytes	Time stamp of message (Date/time without milliseconds)
4	Ms	Small integer 2 bytes	Time stamp of message (milliseconds)
5	Instance	VarChar (255)	Instance name of the message
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)	Comment
31	Username	VarChar (255)	User name
32	Counter	Integer 4 bytes	Running message counter
33	TimeDiff	Integer 4 bytes	Time difference to "Came in" status
34	Classname	VarChar (255)	Name of the message class
35	Type name	VarChar (255)	Name of the message type
36	Class	Small integer 2 bytes	ID of the message class
37	Type	Small integer 2 bytes	ID of the message type
38 to 47	Text1 to Text10	VarChar (255)	Message text 1 to 10
48	AG_NR	Small integer 2 bytes	PLC number
49	CPU_NR	Small integer 2 bytes	CPU number
50	CrForeColor	Integer 4 bytes	Foreground color for the "Came in" status
51	CrBackColor	Integer 4 bytes	Background color for the "Came in" status
52	Priority	Integer 4 bytes	Priority
53	AP_type	Integer 4 bytes	Loop in alarm
54	AP_name	VarChar (255)	Loop in alarm function name
55	AP_PAR	VarChar (255)	Loop in alarm picture
56	InfoText	VarChar (255)	Info text
57	StateText	VarChar (255)	Acknowledgment status
58	AlarmTag	Integer 4 bytes	Message tag
59	AckType	Small integer 2 bytes	Acknowledgment type
60	Params	Integer 4 bytes	Parameters
61	Server name	VarChar (255)	Server name

Recordset structure for "ALARMVIEW" (migrated projects)

Position	Field name	Type	Comment
1 to 49	see ALARMVIEWEX		
50	CrComeFor	Integer 4 bytes	Foreground color for the "Came in" status
51	CrComeBack	Integer 4 bytes	Background color for the "Came in" status
52	CrGoFor	Integer 4 bytes	Foreground color for the "Went out" status
53	CrGoBack	Integer 4 bytes	Background color for the "Went out" status
54	CrAckFor	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 picture
61	InfoText	VarChar (255)	Info text
62	TxtCame	VarChar (255)	Text came in
63	TxtWent	VarChar (255)	Text went out
64	TxtCameNWent	VarChar (255)	Text came in and went out
65	TxtAck	VarChar (255)	Text acknowledged
66	AlarmTag	Integer 4 bytes	Message tag
67	AckType	Small integer 2 bytes	Acknowledgment type
68	Params	Integer 4 bytes	Parameters
69	Server name	VarChar (255)	Server name

See also

Querying the Archive Data (Page 183)

Establishing the Connection to the Archive Database (Page 179)

Access to Archive Data Using OLE DB Provider (Page 173)

Bases of OLE DB (Page 174)

2.4.5.6 Query for User Archives**Introduction**

With the following query, you may use MS OLE DB Provider to access WinCC user archives. Access may be read or write enabled in order to analyze the saved data and to modify and save same.

The data can be selected using filter criteria. The queries are forwarded to the database by the command object.

Note

Consider the following when accessing WinCC user archives via the MS OLE DB Provider:

- Ensure that the write access is not enabled simultaneously via the MS OLE DB Provider and WinCC. This prevents inconsistencies in the archives.
 - Changes via MS OLE DB Provider will not be displayed in WinCC Runtime until the user archive table controls are selected by a picture change. The current data of the user archives are read again.
 - User archives changed via MS OLE DB Provider are not synchronized in a redundant system.
 - Note that WinCC updates can cause changes in the database scheme. The scheme can also be changed by the installation of hot fixes and service packs. In this case, you must adapt the read and write access accordingly.
-

Syntax

Reading of Values

```
SELECT * FROM UA#<ArchiveName>[WHERE <Condition>...., optional]
```

Writing of Values

```
UPDATE UA#<ArchiveName> SET UA#<ArchiveName>.<Column_n> = <Value>  
[WHERE <Condition>...., optional]
```

Inserting a Data Set

```
INSERT INTO UA#<ArchiveName> (ID,<Column_1>,<Column_2>,<Column_n>)  
VALUES (<ID_Value>, Value_1,Value_2,Value_n)
```

Deleting a Data Set

```
DELETE FROM UA#<ArchiveName> WHERE ID = <ID_Number>
```

Parameter

Parameter	Description
ArchiveName	Name of the user archive.
Condition	Filter criterion e.g.: LastAccess>'2004-06-01' AND LastAccess<'2004-07-01' DateTime>'2004-06-01 17:30:00' ID = 5 ID > 3

Example 1:
Reads all data in the user archive "Test".

2.4 Access Via the OLE DB Provider

```
SELECT * FROM UA#Test
```

Example 2:

Reads all data in the user archive "Test" that were changed between June 1, 2004 and July 1, 2004.

```
SELECT * FROM UA#Test WHERE LastAccess>'2004-06-01' AND  
LastAccess<'2004-07-01'
```

Example 3:

Enters the value 'New_String' in the field F_STRING of the ID 3.

```
UPDATE UA#TEST SET F_STRING = 'New_String' WHERE ID = 3
```

Example 4:

Inserts a data set with the ID 100.

```
INSERT INTO UA#Test (ID,F_Integer,F_Float,F_Double,F_String) VALUES  
(100.10, '10.0', 'AAAA')
```

Example 5:

Deletes the data set with the ID 100.

```
DELETE FROM UA#Test WHERE ID = 100
```

See also

Displaying User Archives (Page 198)

2.4.5.7 Displaying User Archives

Introduction

Each user archive consists of data fields with editable properties.

Each data field has properties such as name, alias name, type, lengths, value, etc.

The representation of the data fields and properties in the Editor User Archives is done in lines and columns. Therefore, we are talking of rows instead of data fields and of columns instead of properties.

The possible structure of a user archive is described below as an example.

Example: Layout of a user archive

Field name	Type	Comment
ID	Integer	Unique identification of Value
F_Integer	Integer	Example for Value

Field name	Type	Comment
F_Float	Float	Example for Value
F_Double	Double	Example for Value
F_String	String	Sample character string

See also

Querying the Archive Data (Page 183)

Establishing the Connection to the Archive Database (Page 179)

Access to Archive Data Using OLE DB Provider (Page 173)

Bases of OLE DB (Page 174)

2.4.5.8 Configure Access via the Wizard "SQL Server Import/Export"

Introduction

WinCC OLE DB Provider may be used to access WinCC databases while employing the Wizard "SQL Server Import/Export".

You can save the unzipped data to an intermediate database using the wizard; you access the database with standard SQL queries.

- Using WinCC computers, access to runtime and archive databases may be established locally or remotely.
- In the case of long-term archive servers, local or remote access is only possible to the archive databases since they have no runtime databases.

Procedure

1. Start the "SQL Server Management Studio" and select the desired database.
2. In the shortcut menu of the database, select "Tasks > Export Data".
The SQL Server Import/Export Wizard opens.
3. Configure the data source:
 - In the "Data source" field, select the entry "WinCC OLE DB-Provider for Archives".
 - Click the "Properties" button.
 - The "Data Link Properties" dialog opens.

4. Configure the correct Provider settings:

- In the field "Data Source" enter the following text as data source: .\WinCC
The entry for "Location" remains empty.
- Under "Enter the initial catalog to use", enter either the desired Runtime database or the symbolic name, which was configured in the "WinCC Archive Connector" tool.
The correct spelling of the name may be found in "SQL Server Management Studio" in the "Databases" directory.
Alternatively, you can also enter the "CC_ExternalBrowsing" database for runtime data and archive data.

Note

In order to improve performance during local access, enter "<Computer Name>\WinCC" in the "Data Source" field instead of ".\WinCC".

5. Click the "Advanced" tab.

- In the "Connect timeout" property, select the desired time in seconds.
 - In the "Access permissions" property, only select the "ReadWrite" check box.
- Click "OK" to close the dialog and click "Next".

6. Configure the destination of the data:

- In the "Destination" field, select the entry "SQL Server Native Client", for example.
- The server name can be any SQL Server instance.
- The database name which you enter in the field "Database" can be any self-created target database.

Note

You can also leave the "Database" field empty. No target tables are then created.

7. Configure the query conditions:

- Select the option "Write a query to specify the data to transfer" and then click "Next".
- Enter the desired query condition or use "Browse" to load a query file *.sql.
For example, the values of the last 10 minutes of the archiving are read with the query "Tag:R,1,'0000-00-00 00:10:00.000','0000-00-00 00:00:00.000" of the ValueID "1".
If necessary, check the query via "Parse".
Additional information on the syntax can be found in section "Querying Process Value Archives (Page 184)".

8. If required, edit the query via "Edit Mappings".

9. Select the storage location, if necessary.

10. To export the data, use "Finish" to close the wizard.

Result

The wizard executes the data export to the target database.

If the data export was successful, the uncompressed data in the target database is saved in the newly created table "dbo.Query".

You can change the table name.

Even if you do not change the table name, data will not be overwritten with a new export. New tables with names "Query1", "Query2" etc. are created by the wizard.

See also

Use Case 7: Access Via the WinCC OLE DB Provider (Page 167)

Querying Process Value Archives (Page 184)

2.4.5.9 Meeting prerequisites for using the Reporting Services

Introduction

With WinCC, you can use the Reporting Services of Microsoft SQL Server.

This makes it possible to provide reports created with Microsoft Visual Studio with archive data on the network.

Requirements

The use of the Reporting Services with WinCC requires the following other software prerequisites.

- Internet Information Services
- Reporting Services of the Microsoft SQL Server 2022

Note

Take the installation steps in precisely the indicated order.

Installing Microsoft SQL Server Reporting Services

You install the Reporting Services from the WinCC DVD or from the WinCC setup path in the file system.

1. Open the "Uninstall or change a program" dialog in the Windows control system.
2. In the shortcut menu of "Microsoft SQL Server 2022" select the entry "Uninstall/Change".
3. Select "Add" and select the path "InstData > SQL > SQL2022STD > setup" in WinCC Setup. The Microsoft SQL Server Installation Wizard is opened. Follow the on-screen instructions.
4. Under "Installation type", select the "Add features to an existing SQL Server 2022 instance" option and the "WINCC" instance. The Management Tools and thus the SQL Server Data Tools have already been installed.

2.4 Access Via the OLE DB Provider

5. Activate "Reporting Services - Native" and follow the instructions.
The Reporting Services are installed.
6. In the Windows program group "Microsoft SQL Server 2022", start the Configuration Manager for Reporting Services.
Configure the reporting services.

Configuring the Internet Information Services

1. Open the Computer Management.
2. Under "Services and Applications", select the "Internet Information Services (IIS) Manager".
3. Open the "Authentication" feature and select "Edit" in the shortcut menu of "Anonymous authentication".
4. Select the option "Specific user" and enter the user name and password.
The user name has the following format: <Domain or computer name>\<User>

Note

We recommend restarting the computer after completing the installation.

Result

This makes the prerequisites for using the Reporting Services.

You can now create reports and provide them on the internet.

2.4.6 Analysis Functions for Messages and Process Values

2.4.6.1 Analysis Functions for Messages and Process Values

Introduction

Different analysis functions are available with WinCC for querying archived messages and process values.

The analysis is triggered by a query with parameters for different aggregate functions. Calculation of the aggregate function is performed on the Connectivity Pack server, and only the result is transferred to the client.

Additional information on CommandText and ConnectionString which are used in the following examples may be found under "Establishing Connection to Archive Database" and "Querying Archive Data".

Analysis Functions for Messages

The analysis query for alarm logs archives returns a specific recordset which contains configuration and runtime data for each message as well as results of the aggregate functions.

The returned recordset for analysis queries of alarm logs is not identical to the recordset of normal queries of message archives. Additional information may be found in the section "Display of Alarm Logs for Analysis Queries".

For each message, the following aggregate functions are calculated. The column descriptions of the result list are placed in parenthesis.

- Sum of message frequency ("FreqOfAlarm")
- Cumulative duration from "Message Incoming" until "Message Outgoing" ("CumDurationComeGo")
- Average duration from "Message Incoming" until "Message Outgoing" ("AvDurationComeGo")
- Cumulative duration from "Message Incoming" until initial acknowledgment ("CumDurationComeAckn1")
- Average duration from "Message Incoming" until initial acknowledgment ("AvDurationComeAckn1")
- Cumulative duration from "Message Incoming" until second acknowledgment ("CumDurationComeAckn2")
- Average duration from "Message Incoming" until second acknowledgment ("AvDurationComeAckn2")
- Cumulative duration from "Message Incoming" until "Message Incoming" ("CumDurationComeGo")
- Average duration from "Message Incoming" until "Message Incoming" ("AvDurationComeCome")

Note

"String" data type is not supported

If you use these functions for the "String" data type, the analysis function returns the result "0".

Syntax

For the calculation of aggregate functions for messages, the following command is issued to WinCC OLE DB Provider.

```
"AlarmHitView: SELECT * FROM <ViewName>[WHERE <Condition>]"
```

Here:

<ViewName> = Name of the database table in the desired language, e.g. ALGVIEWMENU for English.

[WHERE <Condition>] = optional filter criterion as WHERE condition in the SQL syntax.

Additional information on the syntax of parameters may be found in the section "Query for Alarm Logs".

Example

The example provides results of the aggregate functions for all messages for the time range between 7/15/2004 12:00 p.m. and 12:15 p.m. from the "ALGVIEWENU" database.

ConnectionString:

```
"Provider=WinCCOLEDBProvider.1;Catalog=CC_OpenArch_03_05_27_14_11_46  
R;Data Source=.\WinCC"
```

CommandText:

```
"AlarmHitView: SELECT * FROM ALGVIEWENU WHERE DateTime>'2004-07-15  
12:00:00' AND DateTime<'2004-07-15 12:15:00'"
```

Analysis Functions for Process Values

The analysis of process values returns the result of an aggregate function. Only one aggregate function can be calculated in a query.

The following aggregate functions are available for process values.

- MIN (minimum)
- MAX (maximum)
- AVG (average)
- SUM (sum of all values)
- COUNT (count of process values)
- COUNTER (number of entries with value "1", e.g., query of binary tags)
- STDEV (statistical standard deviation)
- VAR (statistical variance)

Note**Text tags are not supported**

In a query for text tags (8-bit character set / 16-bit character set) via TAG_EX:R, the analysis function returns the result "0".

Syntax

For the calculation of aggregate functions for process values, a query is issued to the MS SQL OLE DB Provider and the procedure "cp_TagStatistic" from database "SQL Server Master" is executed.

Note

The analysis functions for process values in transparent access function only with Connectivity Station on a client with own project.

The following parameters are transferred to the "cp_TagStatistic" procedure.

```
cp_TagStatistic @P1,@P2,@P3[,@P4]
```

Where:

"@P1" = database name (e.g. WinCC Runtime database or symbolic name of the directory with the swapped out archives). For transparent access, use the WinCC project name instead of the database name.

"@P2" = WinCC OLE DB-Provider String for process values.

"@P3" = desired aggregate function.

"@P4" = <Symbolic computer name>:\WinCC (required only for transparent access).

Additional information on the syntax of parameters "@P1" and "@P2" may be found in the section "Query for Process Value Archives".

Note

Analysis functions for process values with Asian archive tag names

If you use archive tag names with Asian character sets to calculate an analysis function, the request for Unicode character sets has to be adapted.

Add the prefix "N" in front of both parameters.

Example: `cp_TagStatistic N'TestDB',N'TAG:R,17,"2004-05-17 12:00:00","2004-05-17 13:00:00","AVG"`

Example

This query will return the average of process values in the time range between 5/17/2004 12:00 and 13:00 for ValueID "17" from database "TestDB".

ConnectionString:

```
"Provider=SQLNCL11;Integrated Security=SSPI;Persist Security
Info=False;Initial Catalog=master ;Data Source=.\WinCC"
```

CommandText:

```
"cp_TagStatistic 'TestDB','TAG:R,17','2004-05-17
12:00:00','2004-05-17 13:00:00','AVG'"
```

Example of transparent access

This query delivers the average process value in the time range between 14.09.2006 10:00 hrs and 11:00 hrs for the ValueID "7" from the "WinCCProj".

ConnectionString:

```
"Provider=SQLNCL11;Integrated Security=SSPI;Persist Security
Info=False;Initial Catalog=master ;Data Source=.\WinCC"
```

CommandText:

```
"cp_TagStatistic 'WinCCProj','TAG:R,7','2006-09-14
10:00:00','2006-09-14 11:00:00','AVG','Symb_WinCCProj:.\WinCC'"
```

See also

Querying the Archive Data (Page 183)

Establishing the Connection to the Archive Database (Page 179)

Display of Message Archives for Analysis Queries (Page 206)

Use of OLE DB interface of the Connectivity Station (Page 347)

2.4.6.2 Display of Message Archives for Analysis Queries

Introduction

The analysis query for message archives returns a specific recordset which contains configuration and runtime data for each message as well as results of the aggregate functions. This Recordset is not identical to the Recordset of normal queries of message archives.

Recordset Structure for Analysis of Message Archives

Upon query of message archives using the analysis function "AlarmHitView", the result is returned as recordset with the following structure.

Location	Field name	Type	Comments
1	MsgNo	Integer 4 Bytes	Message number
2	State	Small Integer 2 Bytes	Alarm Log Status
3	DateTime	DateTime 8 Bytes	Time stamp of the message (date/time without milliseconds)
4	Ms	Small Integer 2 Bytes	Time stamp of the message (milliseconds)
5	Instance	VarChar (255)	Instance Name of the Alarm Log
6	Flags1	Integer 4 Bytes	(only for internal use)
7	Counter	Integer 4 Bytes	Running Alarm Message Counter
8	TimeDiff	Integer 4 Bytes	Time difference to "Came in" status
9	ClassName	VarChar (255)	Name of the message class.
10	Typename	VarChar (255)	Name of the message type.
11	Class	Small Integer 2 Bytes	Message class ID
12	Type	Small Integer 2 Bytes	Message type ID
13 to 22	Text1 to Text10	VarChar (255)	Message Text 1 to 10
23	AG_NR	Small Integer 2 Bytes	Number of the PLC
24	CPU_NR	Small Integer 2 Bytes	Number of the CPU
25	CrComeFore	Integer 4 Bytes	Foreground Color for the "Came in" Status
26	CrComeBack	Integer 4 Bytes	Background Color for the "Came in" Status
27	CrGoFore	Integer 4 Bytes	Foreground Color for the "Went out" Status
28	CrGoBack	Integer 4 Bytes	Background Color for the "Went out" Status
29	CrAckFore	Integer 4 Bytes	Foreground Color for the "Acknowledged" Status

Location	Field name	Type	Comments
30	CrAckBack	Integer 4 Bytes	Background Color for the "Acknowledged" Status
31	Priority	Integer 4 Bytes	Priority
32	AP_type	Integer 4 Bytes	Loop in Alarm
33	AP_name	VarChar (255)	Loop-in-Alarm Function Name
34	AP_PAR	VarChar (255)	Loop-in-Alarm Screen
35	InfoText	VarChar (255)	Infotext
36	TxtCame	VarChar (255)	Text came in
37	TxtWent	VarChar (255)	Text went out
38	TxtCameNWent	VarChar (255)	Text came in and went out
39	TxtAck	VarChar (255)	Text acknowledged
40	AckType	Small Integer 2 Bytes	Acknowledgment Type
41	FreqOfAlarm	Integer 4 Bytes	Sum of message frequency
42	CumDurationComeGo	Integer 4 Bytes	Cumulative duration from "Message Came In" until "Message Went Out"
43	AvDurationComeGo	Real 8 Bytes	Average duration from "Message Came In" until "Message Went Out"
44	CumDurationComeAckn1	Integer 4 Bytes	Cumulative duration from "Message Came In" until initial acknowledgment
45	AvDurationComeAckn1	Real 8 Bytes	Average duration from "Message Came In" until initial acknowledgment
46	CumDurationComeAckn2	Integer 4 Bytes	Cumulative duration from "Message Came In" until second acknowledgment
47	AvDurationComeAckn2	Real 8 Bytes	Average duration from "Message Came In" until second acknowledgment
48	CumDuration Come-Come	Integer 4 Bytes	Cumulative duration from "Message Came In" until "Message Came In"
49	AvDurationComeCome	Real 8 Bytes	Average duration from "Message Came In" until "Message Came In"

See also

Analysis Functions for Messages and Process Values (Page 202)

2.5 Security Settings During Access to SQL Databases Using MS OLE DB

Introduction

Using MS OLE DB, users may access SQL databases, such as WinCC user archives, and may modify these.

It is therefore possible for unauthorized users to do so.

To protect against unauthorized access, the administrators of the databases must take suitable measures.

Principle

One way of protecting access is to create a user or user group for accessing SQL databases in the Microsoft SQL Server. This user or user group will then be assigned certain authorizations for access to SQL databases.

This may use local or global Windows user groups on the SQL server to organize such access authorizations in SQL.

Alternatively, Windows users can be transferred to the SQL server—either directly as Windows users or as individually defined SQL users.

Server Roles

Part of the security structure of an SQL server are the so-called "Server Roles".

This organizes users into groups for administrative purposes, similar to Windows.

"Server Roles" are used to assign server-wide security settings to a login or if there are no corresponding Windows user groups.

The technical documentation for the Microsoft SQL Server is made available by Microsoft on the Internet:

- SQL Server 2022 documentation (<https://learn.microsoft.com/en-us/sql/sql-server/?view=sql-server-ver16>)

See also

Bases of OLE DB (Page 174)

SQL Server 2022 documentation (<https://learn.microsoft.com/en-us/sql/sql-server/?view=sql-server-ver16>)

2.6 Access via OPC - Open Connectivity

2.6.1 OPC Channel

2.6.1.1 WinCC OPC Channel

Introduction

WinCC can be used as both an OPC server and as an OPC client. The OPC channel is the OPC client application of WinCC.

The OPC communication driver can be used as OPC DA client, OPC XML client, and OPC UA client. The documentation for the OPC UA client is available under "OPC UA channel".

The following OPC components are installed automatically:

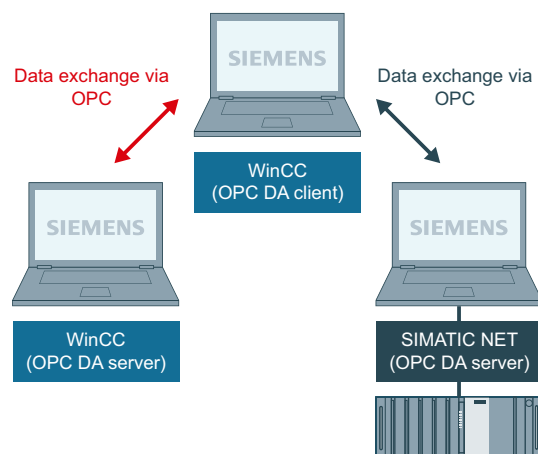
- OPC communication driver
- OPC Item Manager

Possible Applications

WinCC as an OPC DA client

If WinCC is used as an OPC DA client, the OPC channel must be added to the WinCC project. A connection for data exchange is created in the WinCC project of the WinCC OPC DA client; this is used to handle access to the WinCC tags of the OPC DA server.

To simplify the process, the OPC Item Manager is used. A WinCC OPC DA client can access multiple OPC DA servers. This requires that a connection be created for each OPC server. In this way, the WinCC OPC DA client can be used as a central operation and monitoring station.



Note

The WinCC OPC channel establishes connections only to OPC servers which have the status "OPC_STATUS_RUNNING".

Note

"OPC" channel

Unicode is not supported for connection names. Make sure that you name all connections in the project in the same language. Open the Control Panel of your computer to set the code page of this language for use in programs that do not support Unicode.

2.6.1.2 OPC Item Manager

Introduction

A connection and a WinCC tag are configured in the WinCC project of the WinCC OPC client to enable access to tags of an OPC server. The OPC Item Manager simplifies this process for you. The OPC Item Manager is automatically installed with WinCC.

Note

"OPC" channel

Unicode is not supported for connection names. Make sure that you name all connections in the project in the same language. Open the Control Panel of your computer to set the code page of this language for use in programs that do not support Unicode.

Requirements

The following requirements must be met in order to use the OPC Item Manager for configuration:

- The OPC server is an OPC DA server.
- A tag is already configured on the OPC server.
- If WinCC is to be used as the OPC server the WinCC project of the WinCC OPC server must be enabled. If this is not the case, the OPC Item Manager cannot access the WinCC OPC server.
- It must be possible to access the computer of the OPC servers via the IP address or HTTP.
- The OPC server must support the browser functionality. If that is not the case, access to the tag of the OPC server must be configured manually.

Note

If you change language in the WinCC Explorer while the OPC Item Manager is open, no tags are displayed when you click the "Browse Server" button. Exit the OPC Item Manager before changing language.

Tasks of the OPC Item Manager

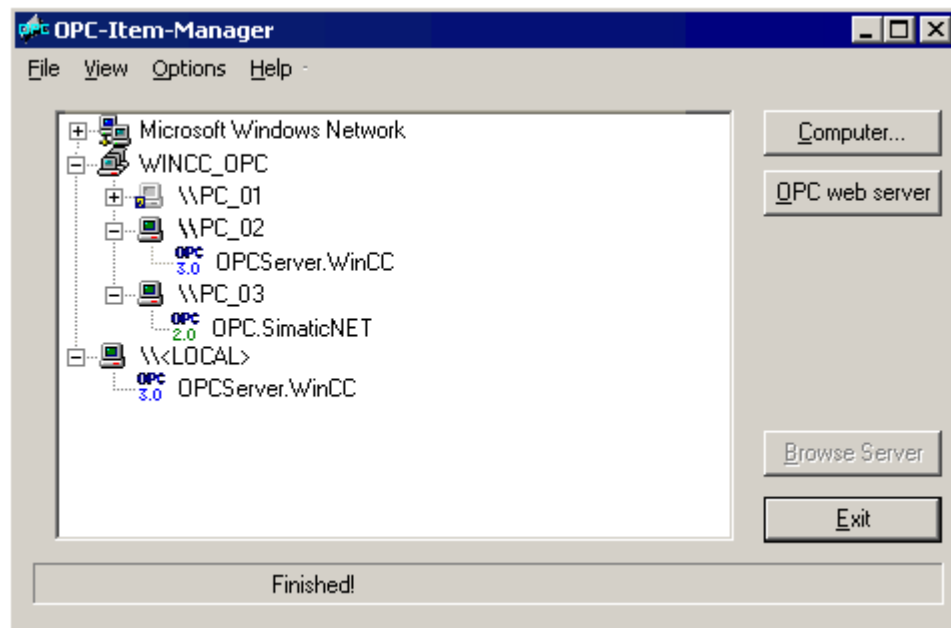
The OPC Item Manager assumes the following tasks:

- Select OPC server
- Creating a connection
- Tag selection
- Adding a tag

Selecting the OPC server

OPC DA server

The OPC Item Manager can be used to determine the name of the OPC DA server in the network. These OPC DA servers can run on the same computer or on different computers in the connected network environment. For further details, refer to "WinCC OPC DA client".



Icons of the OPC Item Manager	Description
	A networked computer has not yet been searched for installed OPC DA servers.
	The computer was not found in the network or the computer could not be accessed.
	A networked computer has been searched for installed OPC DA servers.
	A networked computer contains the OPC DA server designated with the OPC symbol. The number indicates which OPC DA specification of the WinCC OPC DA client is used.
	Refers to the computer running the OPC Item Manager.

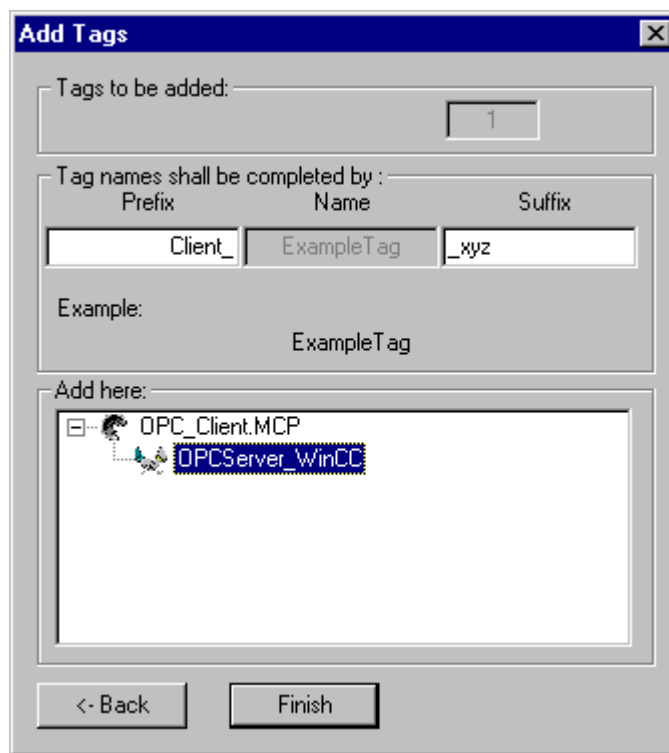
Creating a connection

The OPC Item Manager configures all required settings when creating a connection. If a connection to the OPC server has already been created, this function is not available.

Tag selection

You may use the tag selection dialog to select one or more tags on the OPC server which the WinCC OPC client is to access. Filter criteria can be used to limit the choices in the tag selection dialog.

Adding a tag



The names of the WinCC tags that access the tags of the OPC server can be set in the "Add Tags" dialog.

The WinCC tag name consists of the "prefix", "name" and "suffix". The "Name" field is preconfigured with the "ExampleTag" text. "ExampleTag" stands for the WinCC tag name of the WinCC OPC server.

You can assign a prefix or suffix to distinguish the WinCC tag name on the WinCC OPC client from the WinCC tag name on the WinCC OPC server. When configuring project monitoring, a prefix or suffix must be assigned.

The tag name may be assigned only once in a given WinCC project.

Example

The WinCC tag name on the WinCC OPC DA server is called "OPC_Server_Tag". The "Client_" value is entered in the prefix field and "_xyz" in the suffix field. In the WinCC project of the WinCC OPC DA client, the WinCC tag "Client_OPC_Server_Tag_xyz" is created.

If the tag name on the OPC server contains special characters, they are replaced by an underscore ("_ "), because not all special characters occurring in tag names are supported by the OPC Item Manager.

Click "Finish" to add the WinCC tags to the WinCC project of the WinCC OPC DA client. The OPC Item Manager automatically sets the data type, the name and the address parameters for the WinCC tag.

See also

How to Access a WinCC Tag with the OPC Item Manager (Page 216)

2.6.1.3 Overview of the Supported WinCC Data Types

The list below shows the data types that are supported by the WinCC OPC DA client and WinCC OPC DA server:

- Binary tag
- Signed 8-bit value
- Unsigned 8-bit value
- Signed 16-bit value
- Unsigned 16-bit value
- Signed 32-bit value
- Unsigned 32-bit value
- Floating-point number 32-bit IEEE 754
- Floating-point number 64-bit IEEE 754
- Text tag, 8-bit character set
- Text tag, 16-bit character set
- Raw data type
- Structure types
- Text reference
- Date/Time

Note

Structure types

For structure types, only the structure elements are supported, not the structure itself. However, the structure can be configured later. For more information, refer to the topic "Using structures on the WinCC OPC DA client."

Text reference

If a text tag is created with the OPC Item Manager, it is assigned a length of 160 characters. This length can be changed to any length.

See also

How to Use Structures on the WinCC OPC DA Client (Page 223)

2.6.1.4 WinCC OPC DA Client

Functionality of the WinCC OPC DA Client

Introduction

The OPC channel does not require a separate communication module. The OPC channel is an application which employs the OPC software interface to use an OPC DA server to access process data.

If WinCC is to be used as an OPC DA client, the OPC channel must be added to the WinCC project.

If a communication is established to a WinCC OPC DA server, the values of the WinCC tags are exchanged. To do this, a connection is set up in the WinCC project of the WinCC OPC DA client; it is used to handle access to the WinCC OPC DA server.

For the WinCC OPC DA client to access multiple OPC DA servers, a connection for each of the OPC DA servers must be set up in the WinCC project. For more information about troubleshooting channels and tags, refer to "Troubleshooting".

Note

The WinCC OPC channel establishes connections only to OPC servers which have the status "OPC_STATUS_RUNNING".

Note

"OPC" channel

Unicode is not supported for connection names. Make sure that you name all connections in the project in the same language. Open the Control Panel of your computer to set the code page of this language for use in programs that do not support Unicode.

Connection Monitoring

Three mechanisms are integrated for connection monitoring in the WinCC OPC-DA client. It is thus possible to take the best possible measures in the event of a network error or malfunction of an OPC DA server.

1. If the processing period for a DCOM activation exceeds warning value of 5 seconds, the tag is assigned the value "Addressing Error". If the processing period exceeds the cancellation value of 10 seconds, the connection to the OPC DA server is interrupted. This is displayed in the "Connection Status" dialog of the WinCC Explorers.

The OPC DA specification 3.00 is provided with the "Keep-Alive" feature. If the OPC DA server supports the OPC DA specifications 3.00, this feature is used. The feature causes the OPC DA server to automatically trigger cyclic updating (call OnDataChange) even if the tag values have not changed. If this regular updating is disabled, the WinCC OPC DA client terminates the connection.

The same behavior applies in the case of an OPC DA server which supports the OPC DA specifications 2.05a. In order to check the connection to the OPC DA server, the WinCC OPC DA client requests the status cyclically every 10 seconds. If this regular updating is disabled, the WinCC OPC DA client terminates the connection.

Generally, the WinCC OPC DA client terminates the connection to the OPC DA server when the connection is not capable of functioning. The WinCC OPC DA client attempts to re-establish the connection again, automatically, every 10 seconds.

See also

[How to Use Structures on the WinCC OPC DA Client \(Page 223\)](#)

[Accessing a WinCC Tag without the OPC Item Manager \(Page 221\)](#)

[Configuring Access with the OPC Item Manager \(Page 217\)](#)

[Overview of the Supported WinCC Data Types \(Page 213\)](#)

[OPC Item Manager \(Page 210\)](#)

[OPC specifications and compatibility \(Page 231\)](#)

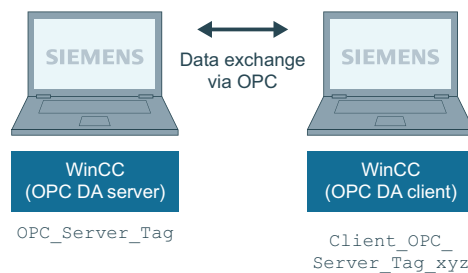
[Functionality of the WinCC OPC DA Server \(Page 235\)](#)

How to Access a WinCC Tag with the OPC Item Manager

How to Access a WinCC Tag with the OPC Item Manager

Introduction

When an OPC connection is made between WinCC and WinCC, data exchange occurs using WinCC tags. The WinCC OPC DA client uses an OPC connection to read the WinCC tag "OPC_Server_Tag" on the WinCC OPC DA server. To simplify the process, the OPC Item Manager is used.



Requirements

- Two computers with WinCC projects.
- Both computers must be accessible via their IP addresses.

Configuration Steps

The following configurations are required in the WinCC project of the WinCC OPC DA client:

- Creation of a connection.
- Configuration of the "XMLClient_OPC_Var1_xyz" WinCC tag on the WinCC OPCXML client which accesses the WinCC tag of the WinCC OPC DA server.

See also

Configuring Access with the OPC Item Manager (Page 217)

Configuring the OPC Channel on the WinCC OPC DA Client (Page 216)

Example of WinCC to WinCC Connection (Page 238)

Configuring the OPC Channel on the WinCC OPC DA Client

Introduction

To use OPC for data exchange, the OPC channel must be set up in the WinCC project.

Procedure

1. Click the "Tag Management" icon in the navigation window of the WinCC Explorer on the WinCC OPC DA client.
2. Select "Add New Driver" from the "Tag Management" shortcut menu. The "Add New Driver" dialog is opened.
3. Select the "OPC.chn" driver and click the "Open" button. The channel is created and the communication driver is displayed in the tag management.

See also

Configuring Access with the OPC Item Manager (Page 217)

Configuring Access with the OPC Item Manager

Introduction

This section explains how to use the OPC Item Manager to configure access to the WinCC tag "OPC_Server_Tag" of the WinCC OPC DA server.

Requirements

- Configure an internal tag named "OPC_Server_Tag" of the data type "signed 16-bit value" in the WinCC project of the WinCC OPC DA server.
- Enable the WinCC project of the WinCC OPC DA server.
- Add the "OPC" channel to the WinCC project of the WinCC OPC DA client.

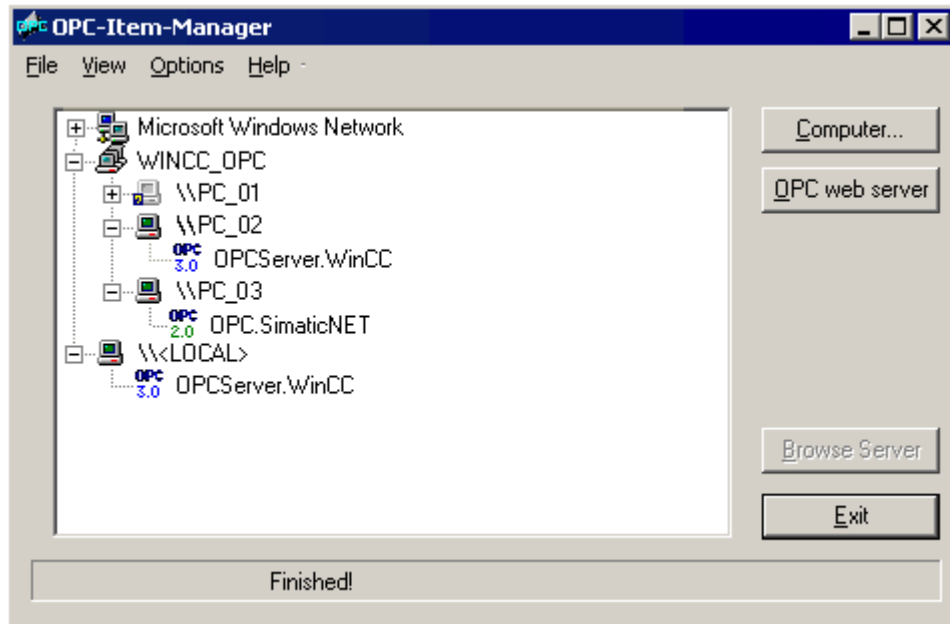
Note

"OPC" channel

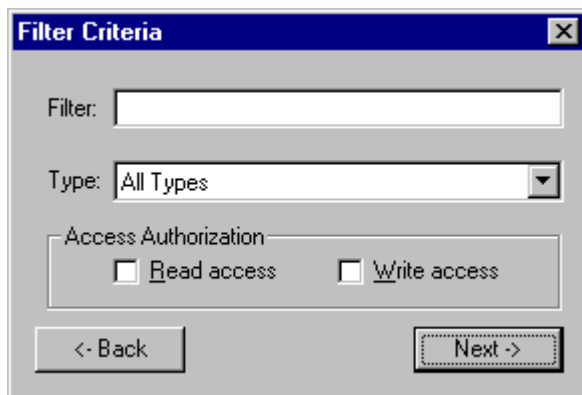
Unicode is not supported for connection names. Make sure that you name all connections in the project in the same language. Open the Control Panel of your computer to set the code page of this language for use in programs that do not support Unicode.

Procedure

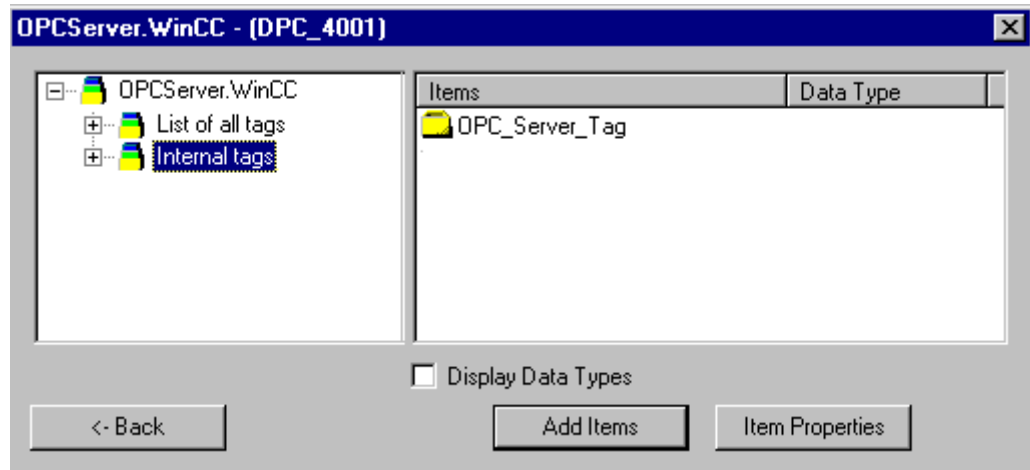
1. In the shortcut menu of the channel unit "OPC Groups(OPCHN Unit#1)" on the WinCC OPC DA client, select "System Parameters". The "OPC Item Manager" opens.



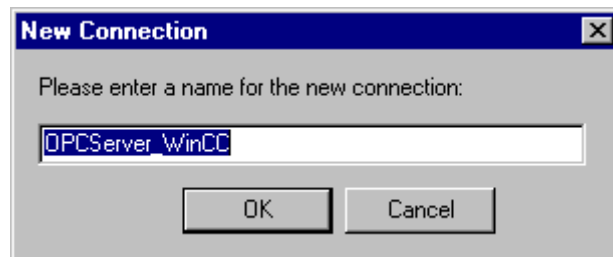
2. Choose the name of the computer to be used as the WinCC OPC DA server from the selection dialog.
Select "OPCServer.WinCC" from the list displayed.
3. Click the "Browse Server" button.
The "Filter criteria" dialog is opened.



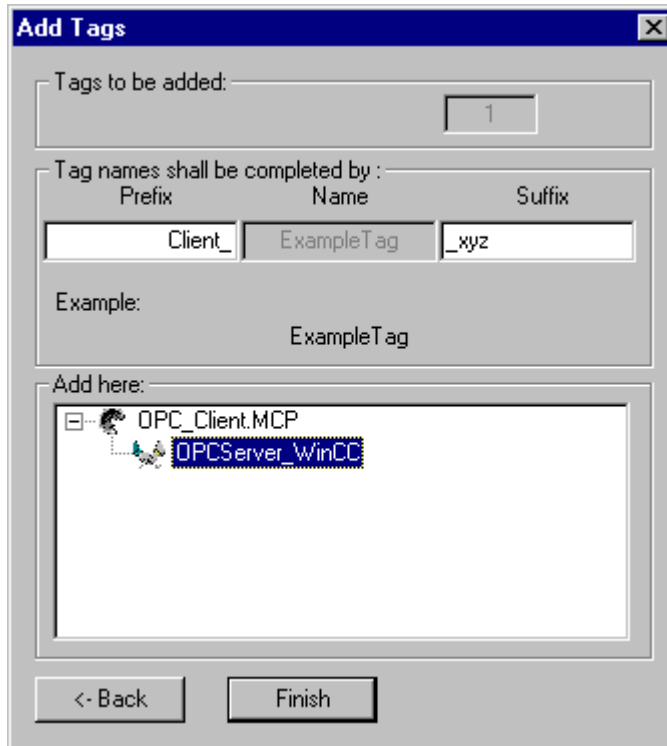
4. Click "Next".
The "OPCServer.WinCC ..." dialog is opened.



5. Select the WinCC tag "OPC_Server_Tag".
Click the "Add Items" button.
6. If a connection to the WinCC OPC DA server already exists, continue with step 6.
If a connection has not been created, a message will be displayed.
Click on the "Yes" button. The "New Connection" dialog is opened.



7. Enter "OPCServer_WinCC" as the name of the connection. Click "OK".
The "Add Tags" dialog opens.



8. Enter the text "Client_" in the prefix field and the text "_xyz" in the suffix field.
9. Select connection "OPCServer_WinCC".
Click "Finish".
10. Click the "Back" button in the "OPCServer.WinCC ..." dialog.
Click "Exit" to close the OPC Item Manager.

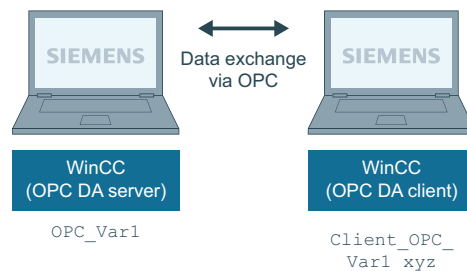
See also

Configuring the OPC Channel on the WinCC OPC DA Client (Page 216)

Accessing a WinCC Tag without the OPC Item Manager

Introduction

OPC servers that do not support browser functionality require access to be configured manually. Configuration of WinCC tags on the WinCC OPC DA client is shown using an example of a WinCC-WinCC OPC connection.



Note

To access a WinCC tag without the OPC Item Manager, the ItemID must be set manually. When addressing WinCC tags, the symbolic computer name (server prefix) can also be specified. The ItemID has the following syntax: Server prefix::WinCC tag. If the WinCC tag of the local WinCC project is addressed, the server prefix is omitted.

The following configurations are required in the WinCC project of the WinCC OPC DA client:

1. Selection of the "OPC_Var1" WinCC tag to be accessed.
2. Creation of a connection.
3. Configuration of the "Client_OPC_Var1_xyz" WinCC tag that accesses the WinCC tag of the WinCC OPC DA server.

Requirements

- Two computers with WinCC projects.
- Both computers must be accessible via their IP addresses.
- Configure an internal tag named "OPC_Var1" with data type "signed 16-bit value" in the WinCC project of the WinCC OPC DA server.
- Enable the WinCC project of the WinCC OPC DA server.
- Add the OPC channel to the WinCC project of the WinCC OPC DA client.

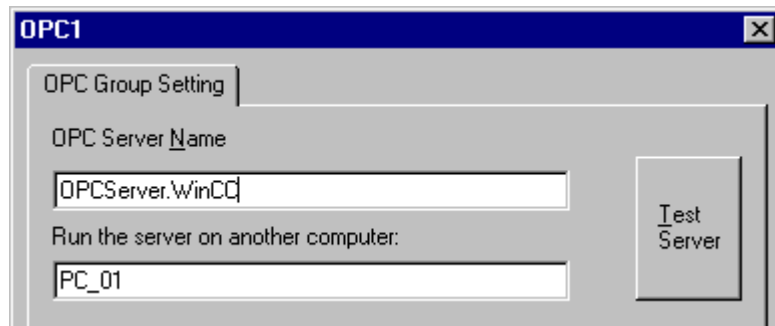
Note

"OPC" channel

Unicode is not supported for connection names. Make sure that you name all connections in the project in the same language. Open the Control Panel of your computer to set the code page of this language for use in programs that do not support Unicode.

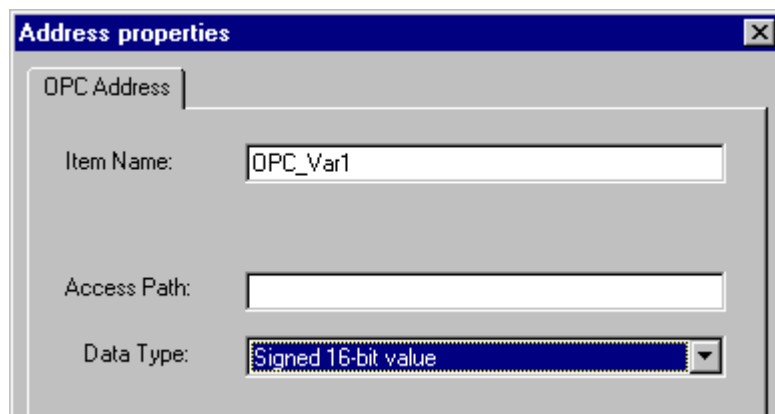
Procedure

1. Select "New Connection" from the shortcut menu of the channel unit "OPC Groups(OPCHN Unit#1)" on the WinCC OPC DA client. The "Connection Properties" dialog is opened. Enter a name for the connection in the corresponding field.
2. Click the "Properties" button. A dialog with the connection name in its title is displayed.



For connections to WinCC V 6, the entry in the "OPC Server Name" field must be "OPCServer.WinCC".

3. Enter the name of the computer to be used as the OPC DA server in the "Start Server on this Computer" field. Click "Test Server", to check the connection to the WinCC OPC DA server.
4. Select "New Tag" from the shortcut menu of the connection. The "Tag Properties" dialog opens.
5. Enter the name "Client_OPC_Var1_xyz" in the "Tag" field. Set the data type to "signed 16-bit".
6. In the "Tag Properties" dialog, click the "Select" button. The "Address Properties" dialog opens.



Enter the name of the WinCC tag of the WinCC OPC DA server in the "Item Name" field. Leave the entry in the "Access Path" field unchanged. Set the data type to "signed 16-bit".

7. Click "OK" to close all open dialogs.

Using Structures on a WinCC OPC DA Client

How to Use Structures on the WinCC OPC DA Client

Introduction

Structures are used to organize tags and tag types that form a logical unit. This allows them to be referenced using a single logical name.

Structures are not supported by the OPC DA specification. As a result, structures cannot be set up using the OPC Item Manager, only the individual tags in a structure. If you wish to use structures on the WinCC OPC DA client nonetheless, the data structure must be configured subsequently in the WinCC project of the WinCC OPC DA client in order to supply it with the relevant item names of the server tags.

Requirements

- Two computers with WinCC projects.
- Both computers must be accessible via their IP addresses.

Configuration steps

The following configuration steps are necessary to use structures on the WinCC OPC DA client:

- Configuring structures and structure tags on the WinCC OPC DA server
- Using structures on the WinCC OPC DA client in the WinCC project

See also

[How to Configure Structures on the WinCC OPC DA Client \(Page 224\)](#)

[Configuring Structures and Structure Tags on the WinCC OPC DA Server \(Page 223\)](#)

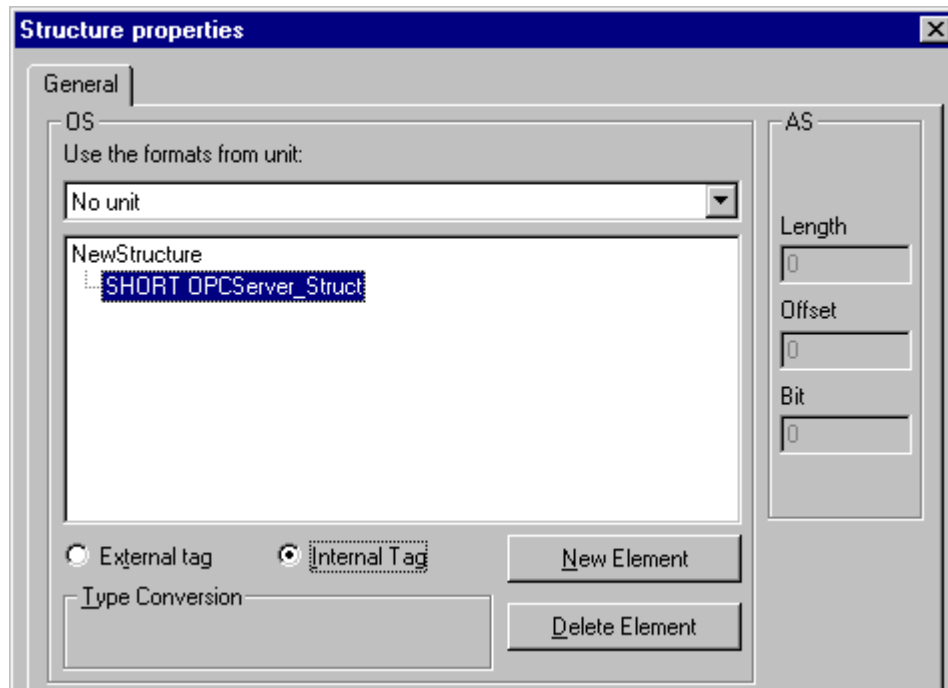
Configuring Structures and Structure Tags on the WinCC OPC DA Server

Introduction

In this section a structure and a structure tag is created in the WinCC project of the OPC DA server. This configuration is required for the OPC DA client to access the structure tag.

Procedure

1. Select "New Structure Type" from the structure types shortcut menu on the WinCC OPC DA server. The "Structure Properties" dialog is displayed.
2. Click "New Element" and create the internal tag "OPCServer_Struct" of data type SHORT.



Click "OK" to close the dialog.

3. In the navigation window, click the plus sign in front of the icon for tag management. Select "New Tag" from the internal tag shortcut menu. Create a WinCC tag named "Var" with this structure type.
4. The data frame of the WinCC Explorer shows the single tag "Var" and the structure tag "Var.OPCServer_Struct".
5. Activate the WinCC project.

See also

How to Configure Structures on the WinCC OPC DA Client (Page 224)

How to Configure Structures on the WinCC OPC DA Client

Introduction

Structures are not supported by the OPC DA specification. As a result, structures cannot be set up using the OPC Item Manager. In this section, the structure already present in the WinCC project of the WinCC OPC DA server is configured for the WinCC project of the WinCC OPC DA client. A WinCC tag that accesses the existing structure tag on the WinCC OPC DA server is configured on the WinCC OPC DA client.

Requirements

- Create a structure and a structure tag named "Var.OPCServer_Struct" in the WinCC project of the WinCC OPC DA server.
- Enable the WinCC project of the WinCC OPC DA server.
- Add the OPC channel to the WinCC project of the WinCC OPC DA client.

Note

"OPC" channel

Unicode is not supported for connection names. Make sure that you name all connections in the project in the same language. Open the Control Panel of your computer to set the code page of this language for use in programs that do not support Unicode.

Procedure

1. Select "New Structure Type" from the structure types shortcut menu on the WinCC OPC DA client. The "Structure Properties" dialog is displayed.
2. Click the "New Element" button and set up an external tag. Name the element exactly as it is in the WinCC project of the OPC-DA server. Click "OK" to close the "Structure Properties" dialog.
3. If a connection to the OPC DA server already exists, continue with step 6.
If no connection has been created, select "New Connection" from the shortcut menu of the channel unit "OPC". The "Connection Properties" dialog is opened. Enter a name for the connection in the corresponding field.
4. Click the "Properties" button. A dialog with the connection name in its title is displayed. For connections to WinCC V 6, the entry in the field "OPC Server Name" must be "OPCServer.WinCC".
5. Enter the name of the computer to be used as the WinCC OPC DA server in the field "Start Server on this Computer". Click "Test Server", to check the connection to the WinCC OPC DA server. Click "OK" to close the dialog.
6. Select "New Tag" from the shortcut menu of the connection. The "Tag Properties" dialog opens. Select the newly created structure type as the data type.
7. In the "Tag Properties" dialog, click the "Select" button. The "Address properties" dialog opens. In the "Item Name" field, enter the name "Var.OPCServer_Struct" for the structure tag of the WinCC OPC DA server. Leave the entry in the "Access Path" field unchanged.
8. Click "OK" to close all open dialogs.

See also

Configuring the OPC Channel on the WinCC OPC DA Client (Page 216)

Configuring Structures and Structure Tags on the WinCC OPC DA Server (Page 223)

Error Handling in the Event of Disturbed OPC DA Communication

Error Handling in the Event of Disturbed OPC Communication

Introduction

The procedure for communication testing is independent of how WinCC is used.

WinCC Used as the OPC DA Server

Use the channel diagnostics on the WinCC OPC DA client to determine whether a connection to the OPC DA server can be established. For more information regarding channel problem analysis, refer to "Troubleshooting".

WinCC Used as the OPC DA Client

Use the channel diagnostics on the WinCC OPC DA client to determine whether a connection to the OPC DA server can be established. For more information regarding channel problem analysis, refer to "Troubleshooting".

See also

WinCC is used as the OPC DA client, and the connection is not established. (Page 230)

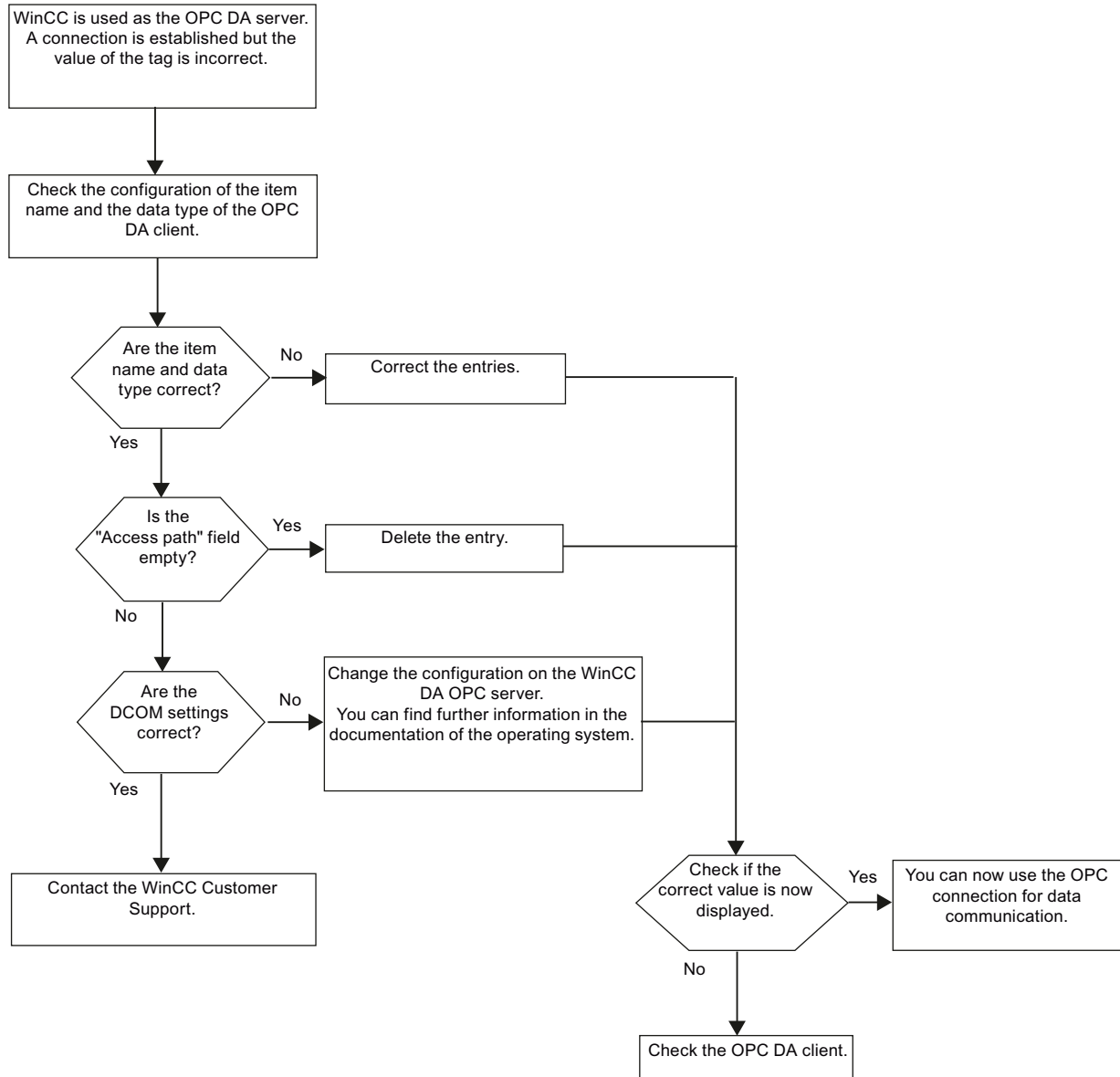
WinCC is used as the OPC DA client, and the connection is established. (Page 229)

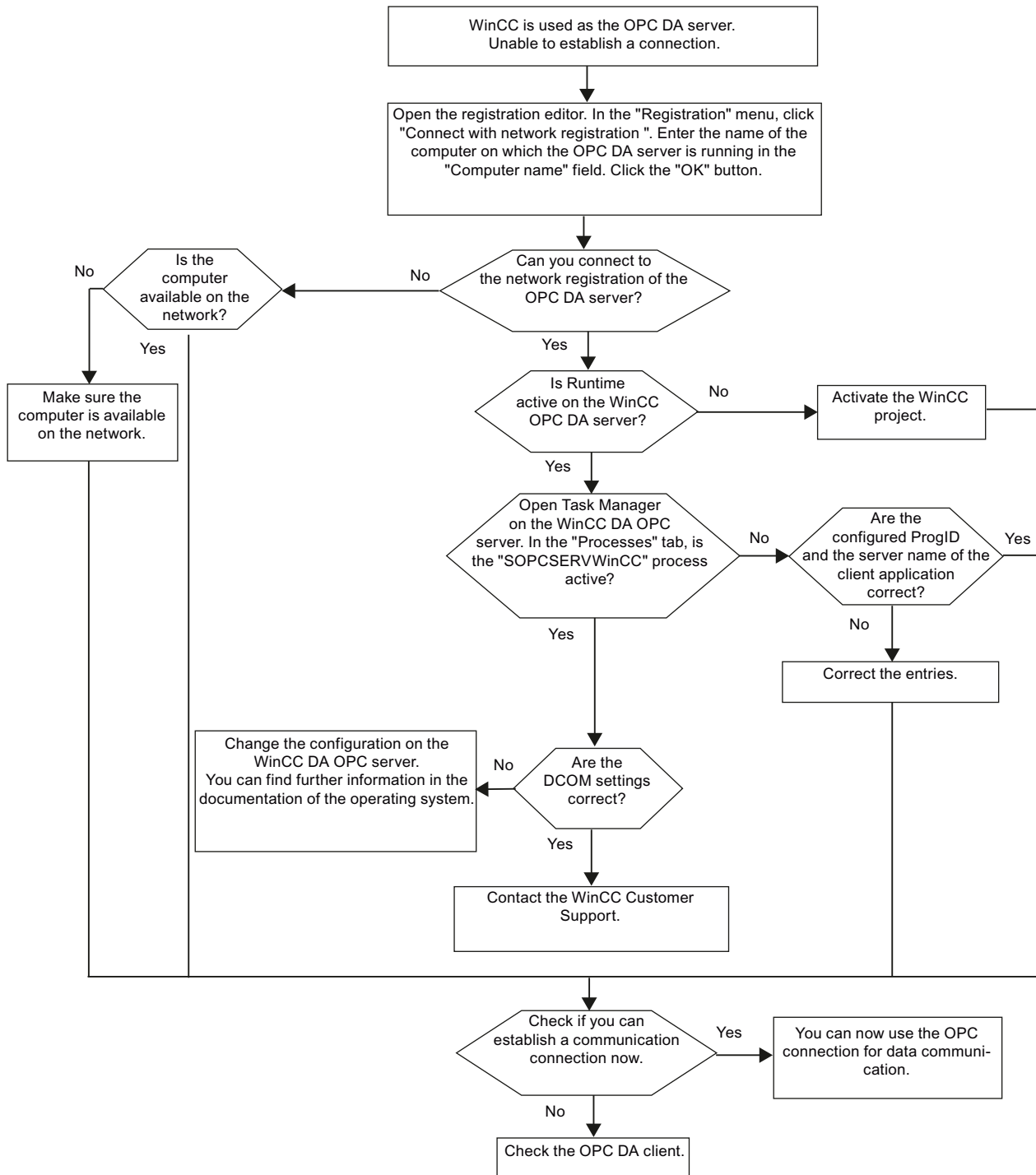
WinCC is used as the OPC DA server, and the connection is not established. (Page 228)

WinCC is used as the OPC DA server, and the connection is established successfully.
(Page 227)

WinCC as OPC DA Server

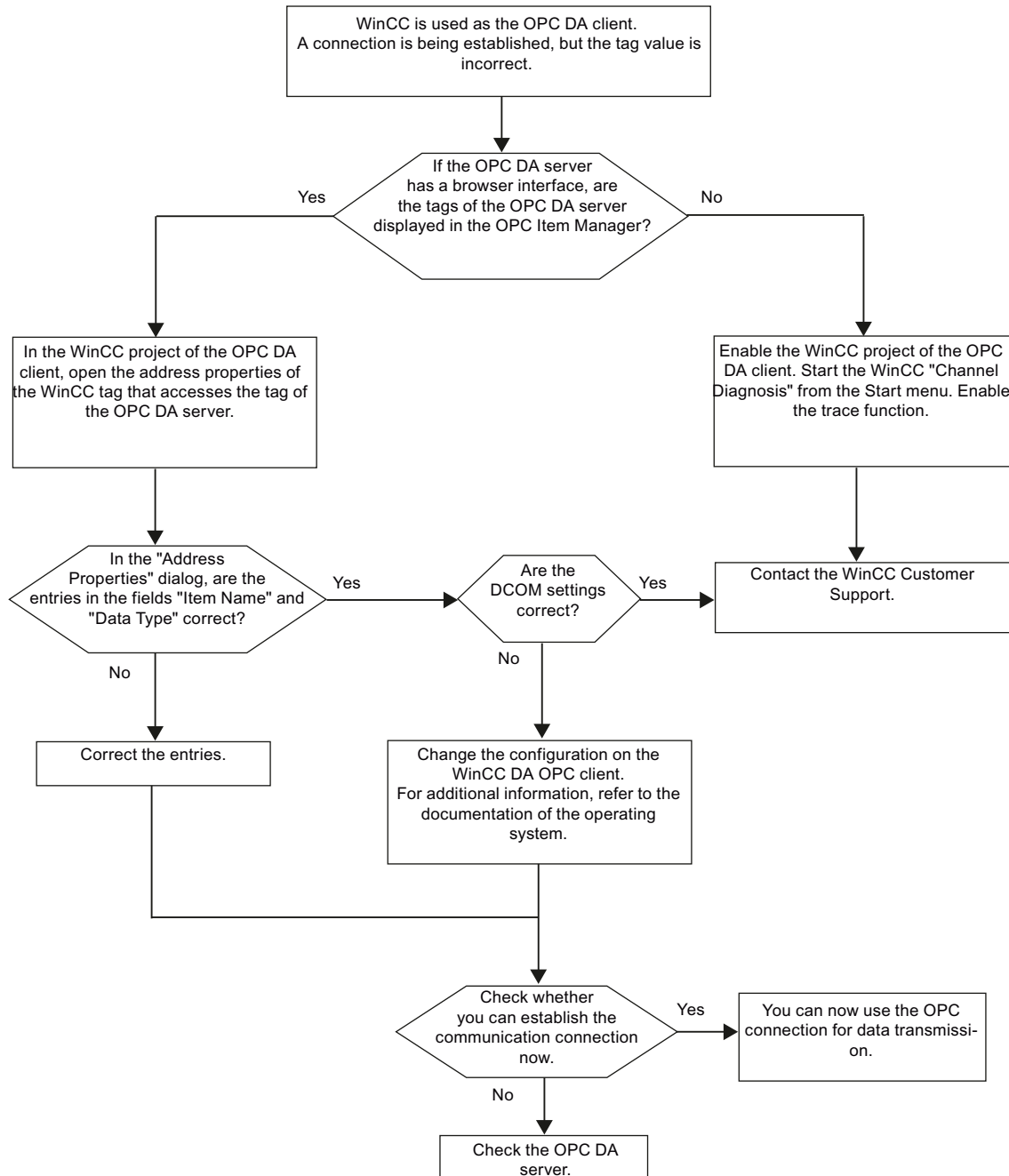
WinCC is used as the OPC DA server, and the connection is established successfully.



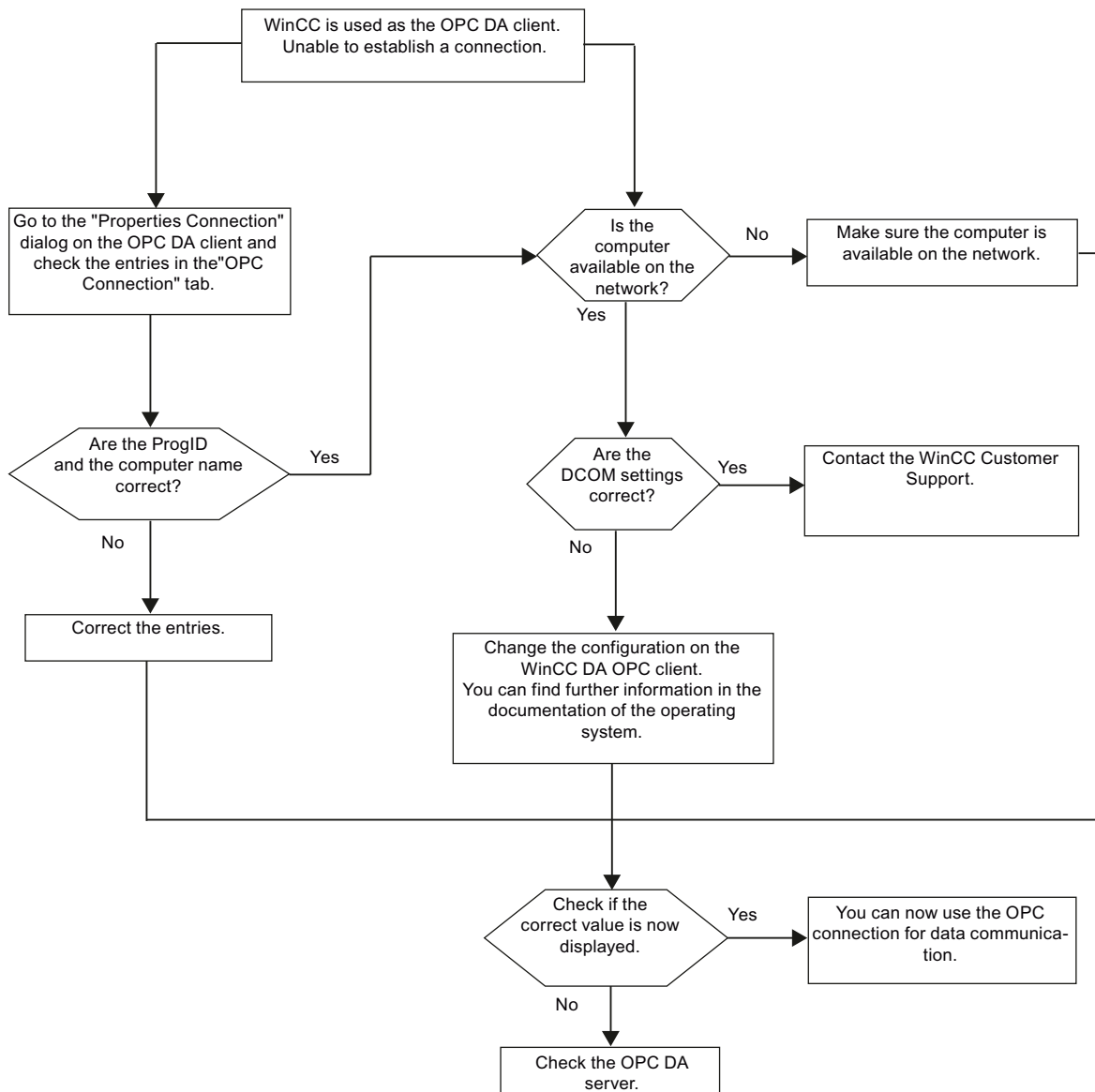
WinCC is used as the OPC DA server, and the connection is not established.

WinCC as OPC DA Client

WinCC is used as the OPC DA client, and the connection is established.



WinCC is used as the OPC DA client, and the connection is not established.



2.6.2 OPC - Open Connectivity

2.6.2.1 OPC - Open Connectivity

Contents

The OPC standardized software interface allows you to combine devices and applications from various manufacturers in a uniform manner.

WinCC can be used as an OPC server or an OPC client. The "OPC" channel represents the OPC client application of WinCC.

This section shows you:

- which OPC servers WinCC has.
- how to use OPC in WinCC.
- how to set up various OPC DA links.
- how to configure the access to the WinCC message system.
- how the WinCC message system is mapped on the OPC A&E.
- how to set up access to the WinCC archive system.

2.6.2.2 Functionality of OPC

OPC is a standardized manufacturer-independent software interface for data exchange in automation engineering.

OPC interfaces allow the standard linking of devices and applications from different manufacturers.

OPC is based on the Windows COM (Component Object Model) and DCOM (Distributed Component Object Model) technologies.

OPC XML DA provides an additional software interface that is based on the XML, SOAP and HTTP Internet standards.

OPC UA (Unified Architecture) is the successor technology to OPC. OPC UA is platform-independent and supports different protocols as communication medium.

2.6.2.3 OPC specifications and compatibility

Overview

OPC specifies interfaces for access to the following objects in WinCC:

- Process values (OPC Data Access 2.05a, 3.0; OPC XML Data Access 1.01; OPC UA 1.04)
- Archived process values (OPC Historical Data Access 1.20; OPC UA Historical Access 1.04)
- Chronological messages (OPC Historical Alarms and Events 1.10)
- Messages (OPC Alarms and Events 1.10; OPC UA Alarms and Conditions 1.04)

For more information about individual OPC specifications, refer to the OPC Foundation (<http://www.opcfoundation.org>) website.

Compatibility

Support of these specifications is regularly monitored by the "Compliance Test Tool" (CTT) of the OPC Foundation. Interoperability with OPC products from other manufacturers is guaranteed by participation in "OPC Interoperability Workshops".

The test results submitted are published on the OPC Foundation website. To view the results, enter the search term "OPC Self-Certified Products".

2.6.2.4 Using OPC in WinCC

Introduction

In WinCC, servers are available for the following OPC interfaces:

- OPC Data Access / OPC XML Data Access: Access to the WinCC body of data
- OPC Historical Data Access: Access to the WinCC archive system
- OPC Alarms&Events: Access to the WinCC message system
- OPC Unified Architecture: Access to the WinCC body of data and archive system

WinCC contains an OPC channel by default. The OPC channel can access the relevant OPC servers as client via OPC DA , OPC XML DA or OPC UA.

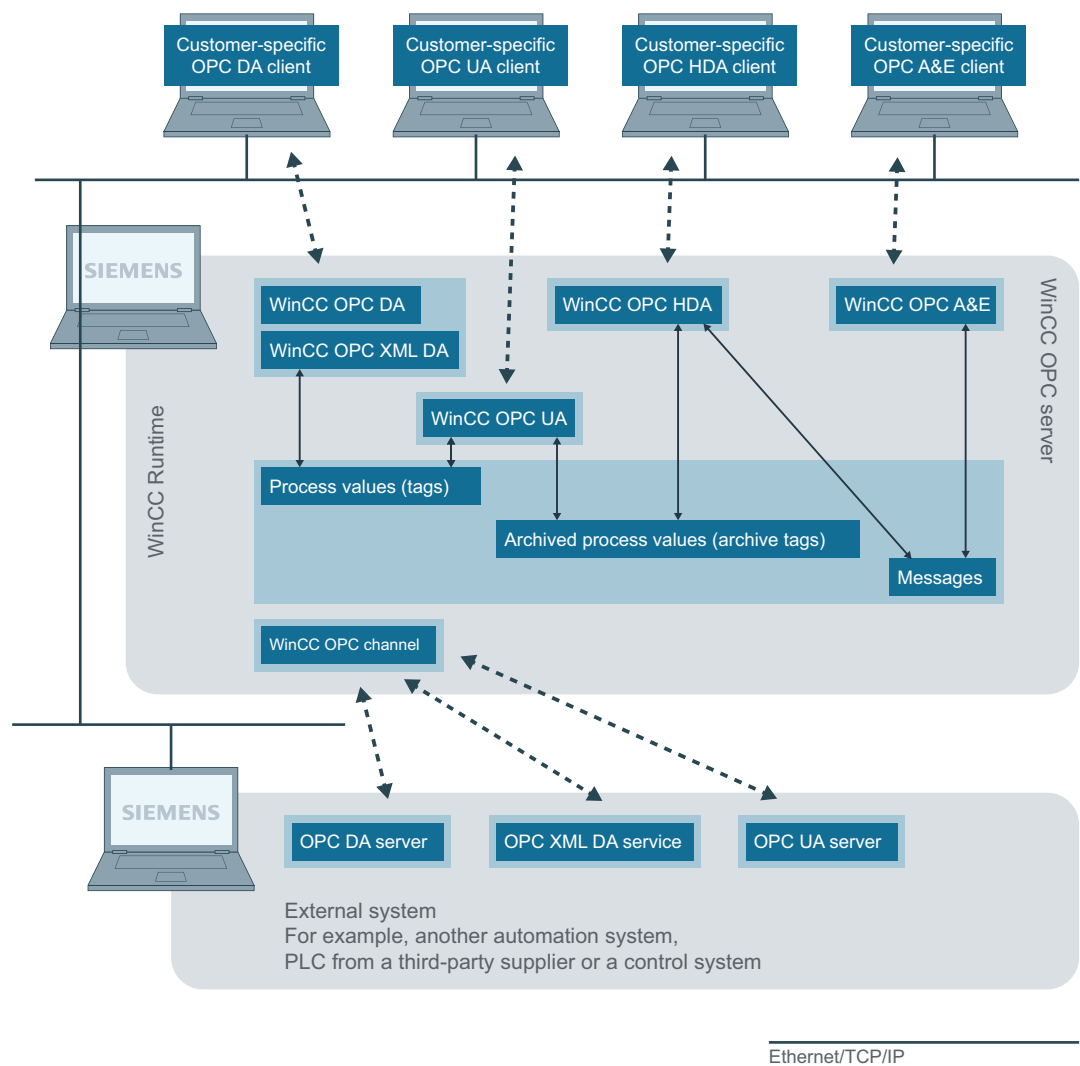
WinCC OPC communications concept

Data exchange between a WinCC OPC server and OPC client is completed via DCOM. After installation of WinCC, the DCOM settings of the WinCC OPC server are correctly configured.

If a WinCC OPC server or client communicates with an external OPC system, corresponding adaptations must be performed. The "Local access" and "Remote access" authorizations must be entered for the user in "DCOM/Workplace/COM Security/Access rights/Edit default" of User Administration on the client.

The OPC XML server of WinCC is implemented as a web service. This gives you access to your PC via the Internet. You therefore need to define appropriate access rights.

The following shows the WinCC OPC communication concept:



Licensing

OPC server	Licensing
WinCC OPC DA server	A valid RT license for WinCC
WinCC OPC XML DA Server	A valid RT license for WinCC
WinCC OPC UA Server	WinCC Option Connectivity Pack
WinCC OPC HDA server	
WinCC OPC A&E Server	

2.6.2.5 How to configure Windows for the use of WinCC OPC

Introduction

The OPC client and the OPC server are DCOM applications. A distributed DCOM application can only be run under the same user account. Therefore the OPC server must recognize the OPC client's user account and vice-versa. If the WinCC OPC servers are used with WinCC OPC clients, the correct configuration is already warranted by the installation.

Declaration of the user account, if an external OPC server or client is used

For additional information on the granting of user rights, refer to the Windows documentation.

Requirements

Log on as the administrator to both the WinCC OPC server and OPC client workstations to configure the user permissions.

Procedure

1. Go to "Control Panel > System and Security > Administrative Tools > Computer Management > Local Users and Groups".
2. In the "Users" shortcut menu, select "New User".
In the "New User" dialog, enter the user account details of the communication partner. Click "Create" and close the dialog.
3. Click the "Users" icon. Double-click the relevant user. The "Properties" dialog for this user is displayed.
4. Click the "Member Of" tab. Click "Add". The "Select group" dialog is opened.
5. Add the group "Users".
If you are on a computer that has WinCC installed, also add the group "SIMATIC HMI". Click "OK" to close all open dialogs.

How to adapt the Windows firewall settings

After installation of WinCC, the Windows firewall settings of the WinCC OPC servers are correctly configured.

If OPC clients access OPC servers in different subnets, you must adapt the configuration of the permitted network areas to the OPC servers.

2.6.2.6 WinCC OPC DA server

Functionality of the WinCC OPC DA Server

Introduction

The WinCC OPC-DA-Server supports OPC Data Access specifications 2.05a and 3.00. This has been confirmed by the compliance test.

The WinCC OPC DA server is a DCOM application. This interface is used by the WinCC OPC DA server to make the required information about WinCC tag available to the WinCC client.

The WinCC OPC DA server is active, if the WinCC OPC DA client is accessing it via a connection. To establish successful OPC communication, the following must be observed:

- The WinCC project of the WinCC OPC DA server must be enabled.
- The computer on which the WinCC OPC DA server runs must be accessible via its IP address.

Installation

The WinCC OPC DA server can be selected during the installation of WinCC. After installation, the WinCC OPC DA server is immediately usable without any further configuration.

The WinCC OPC DA server can be implemented on a WinCC server or a WinCC client.

Notes on configuration

- If the WinCC-OPC-DA server is used, the application "OPC-DA server, OPC-A&E server, OPC-HDA server" must be activated.
You can activate the application in the Editor "Computer" of the WinCC Configuration Studio in the "Processes when starting WinCC Runtime" tab.
- You can assemble tags into tag groups for structuring in the WinCC project. The tags should not have the same name as the group.
- Each write request initiated in WinCC, for example via VBScript or the object "IO field", is always treated as a synchronous "Write" call. The "IOPCSyncIO::Write" interface is used by the WinCC OPC DA server for this. The asynchronous write mechanism is not implemented in the WinCC OPC DA channel.

Note

If the Internet options on a computer are set to automatically detect settings under "Connections -> LAN Settings", access to OPC DA via the web service will take significantly longer.

See also

Querying the OPC DA Server Name (Page 237)

Using Multiple OPC DA Servers (Page 236)

Example of WinCC to WinCC Connection (Page 238)

Example of WinCC - SIMATIC NET FMS OPC Server Connection (Page 242)

Example of a WinCC - SIMATIC NET S7 OPC Server Connection (Page 244)

Example of the WinCC - Microsoft Excel Connection (Page 249)

Overview of the Supported WinCC Data Types (Page 213)

www.opcfoundation.org (<http://www.opcfoundation.org>)

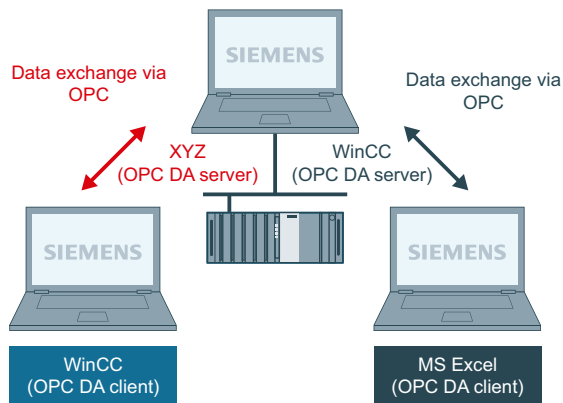
Using Multiple OPC DA Servers

Introduction

More than one OPC DA server may be installed on a computer, and any number may work in parallel.

In this way, the OPC DA server of WinCC and the OPC DA server of another (third-party) provider may be operated independently of one another on the same computer.

The WinCC OPC DA client can access the process data of the automation device via the OPC server of the third-party provider. The OPC DA client of Microsoft Excel can use the WinCC OPC DA server to access the WinCC data.



There are a number of OPC DA servers available from various manufacturers. Each of these OPC DA servers has a unique name (ProgID) for identification. OPC DA clients must use this name to address the OPC server.

The OPC Item Manager can be used to query the name of the OPC DA server. The OPC DA server of WinCC V 7 is named: "OPCServer.WinCC".

See also

Querying the OPC DA Server Name (Page 237)

Querying the OPC DA Server Name

Introduction

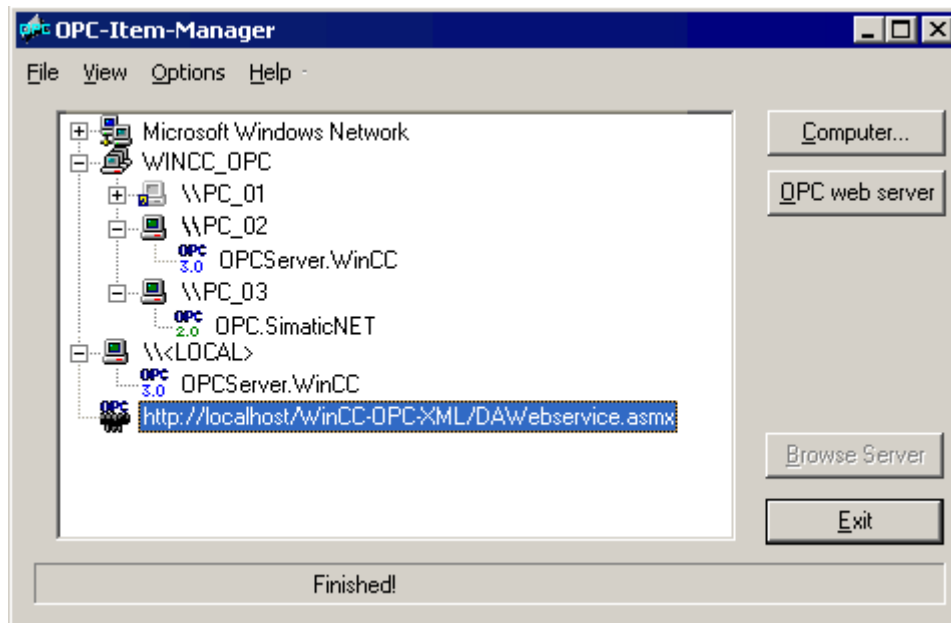
Multiple OPC DA servers can be installed on a single computer. The OPC Item Manager displays the names of the OPC DA servers available to the workstation in a selection window. These OPC DA servers can be run on the same computer or on computers in the network environment.

Requirement

Add the "OPC" channel to the WinCC project of the WinCC OPC DA client.

Procedure

1. In the shortcut menu of the channel unit "OPC Groups(OPCHN Unit#1)" on the WinCC OPC DA client, select "System Parameters". The "OPC Item Manager" is opened.
2. In the navigation window of the OPC Item Manager, select the name of the computer you wish to access.
3. The OPC Item Manager displays the names of the OPC DA servers that available to your computer in a selection window.



See also

OPC Item Manager (Page 210)

Examples of OPC DA Connections

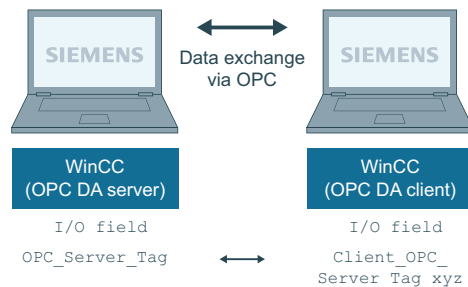
WinCC - WinCC Connection

Example of WinCC to WinCC Connection

Introduction

When establishing a WinCC - WinCC connection, data are exchanged between the WinCC OPC DA server and client by means of the "OPC_Server_Tag" WinCC tag. The "Client_OPC_Server_Tag_xyz" WinCC tag on the client reads the "OPC_Server_Tag" WinCC tag on the server. If the value of the "OPC_Server_Tag" tag on the WinCC OPC server changes, the value of the "Client_OPC_Server_Tag_xyz" WinCC tag on the WinCC OPC DA client also changes. Changes on the client are also reflect on the server.

Tag values are displayed in I/O fields on both computers.



Requirements

- Two computers with WinCC projects.
- Both computers must be accessible via their IP addresses.

Configuration Procedure

The following configurations are required to establish a WinCC - WinCC connection:

1. Configuring a WinCC Project on a WinCC OPC DA Server
2. Configuring a WinCC Project on a WinCC OPC DA Client

See also

How to Configure a WinCC Project on a WinCC OPC DA Server (Page 239)

Configuring the WinCC Project on the WinCC OPC DA Client (Page 239)

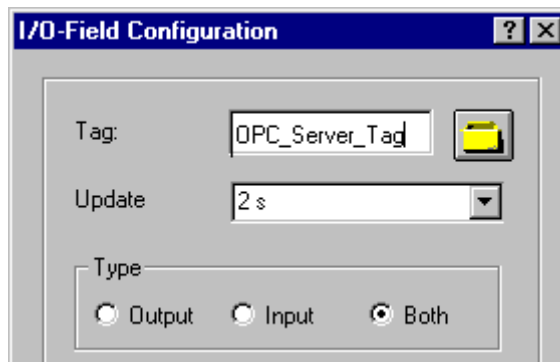
How to Configure a WinCC Project on a WinCC OPC DA Server

Introduction

In this section, a WinCC tag is created in the WinCC project of the WinCC OPC DA server and displayed in an I/O field.

Procedure

1. Select "New Tag" from the shortcut menu of the "Internal Tags" icon on the WinCC OPC DA server. Create a new tag called "OPC_Server_Tag" of the "signed 16-bit value" type.
2. Launch the Graphics Designer and open a new picture.
3. Add an I/O field to the picture. Select the "I/O field" object from the object list under "Smart Objects". The "I/O Field Configuration" dialog is opened.



4. Enter the name "OPC_Server_Tag" in the "Tag" field.
5. Set the update to "2s" and the field type to "I/O field".
6. Click "OK" to close the dialog and save the picture.
7. Enable the WinCC project by clicking the "Activate" button in the Graphics Designer.

See also

Configuring the WinCC Project on the WinCC OPC DA Client (Page 239)

Configuring the WinCC Project on the WinCC OPC DA Client

Introduction

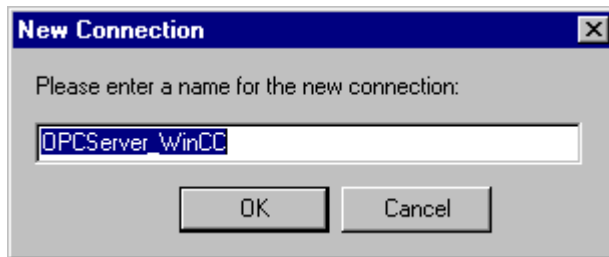
In this section, a WinCC tag is created on the WinCC OPC DA client, in order to read a WinCC tag on the WinCC OPC DA server. The tag value is displayed in an I/O field.

Requirements

- Add the "OPC" channel to the WinCC project of the WinCC OPC DA client.
- Configure an internal tag named "OPC_Server_Tag" of the data type "signed 16-bit value" in the WinCC project of the WinCC OPC DA server.
- Enable the WinCC project of the WinCC OPC DA server.

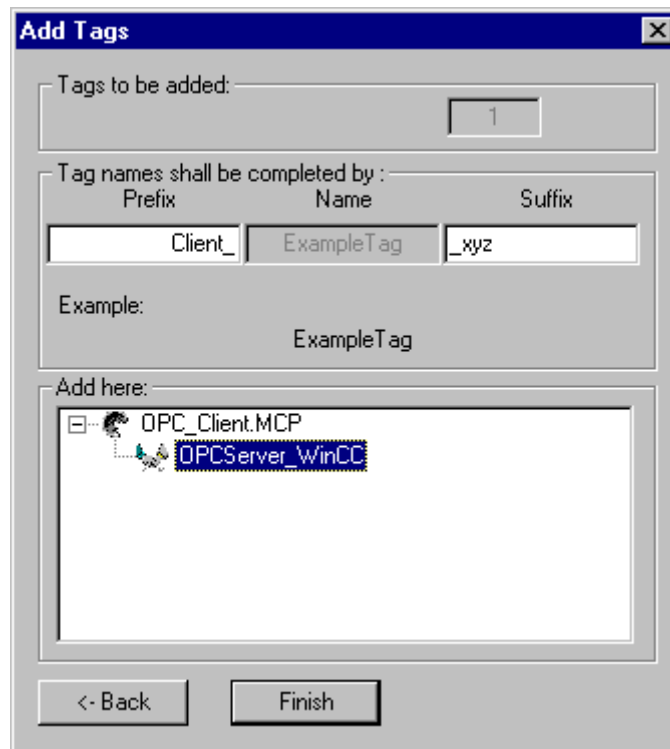
Procedure

1. In the shortcut menu of the channel unit "OPC Groups(OPCHN Unit#1)" on the WinCC OPC DA client, select "System Parameters". The OPC Item Manager is opened.
2. Choose the name of the computer to be used as the OPC DA server from the selection dialog. Select "OPCServer.WinCC" from the list. Click the "Browse Server" button. The "Filter Criteria" dialog is opened.
3. Click the "Next->" button in the "Filter Criteria" dialog. Select the "OPC_Server_Tag" tag in the "OPCServer.WinCC ..." dialog. Click the "Add Items" button.
4. If a connection to the OPC DA server already exists, continue with step 5.
If no connection has been configured, a corresponding message is displayed.
Click "Yes". The "New Connection" dialog is displayed.



Enter "OPCServer_WinCC" as the name of the connection. Click "OK".

5. The "Add Tags" dialog is displayed.
Enter "Client_" in the prefix field and "_xyz" in the suffix field. Select connection "OPCServer_WinCC". Click "Finish".



6. Click the "<- Back" button in the "OPCServer.WinCC ..." dialog. In the "OPC Item Manager", click "Exit" to close the OPC Item Manager.
7. Launch the Graphics Designer and open a new picture. Add an I/O field to the picture. Select the "I/O field" object from the object list under "Smart Objects". The "I/O Field Configuration" dialog is opened.
8. Enter the name "Client_OPC_Server_Tag_xyz" in the "Tag" field. Set the update to "2 s". Set the field type to "I/O field". Close the dialog and save the picture. Enable the WinCC project by clicking the "Activate" button in the Graphics Designer.
9. The value of the configured tags is displayed in the I/O field on both the WinCC OPC DA server and the client. Enter a new value in the I/O field on the WinCC OPC DA server. The new value is displayed in the I/O field on the WinCC OPC DA client.

See also

How to Configure a WinCC Project on a WinCC OPC DA Server (Page 239)

Configuring the OPC Channel on the WinCC OPC DA Client (Page 216)

WinCC - SIMATIC NET FMS OPC Server Connection

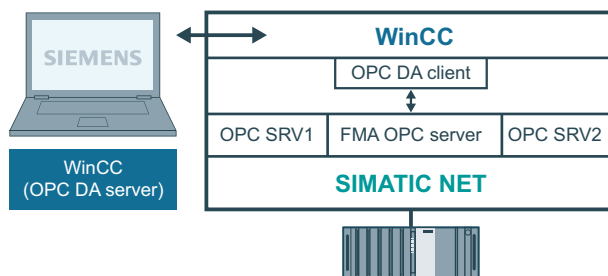
Example of WinCC - SIMATIC NET FMS OPC Server Connection

Introduction

During the installation of SIMATIC NET, you can select the OPC server to be installed. In the following example, a connection between WinCC and SIMATIC NET FMS OPC server is configured. Data from the automation device is made available to WinCC through the SIMATIC NET FMS OPC server.

In this example, WinCC is used as the WinCC OPC DA client. The OPC Item Manager displays the indexes of the object list configured for the automation device.

The current value of the tag is displayed in an I/O field. As soon as the value of the tags on the SIMATIC NET FMS OPC server changes, the new value is reflected on the process picture on the WinCC OPC DA client. Conversely, a value entered in the I/O field is sent to the automation device.



Requirements

- A computer with WinCC, SIMATIC NET software.
- A configured SIMATIC NET FMS OPC server. For additional information regarding the setup of SIMATIC NET S7 OPC servers refer to the SIMATIC NET documentation.

Configuration steps

The following configuration is required in the WinCC project of the WinCC OPC DA client:

1. Configuring a WinCC - SIMATIC NET FMS OPC server connection

Communication Manual

The communication manual contains additional information and extensive examples for the channel configuration. This manual is available for download on the Internet:

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

Search by item number:

- A5E00391327

See also

How to Configure the WinCC - SIMATIC NET FMS OPC Server Connection (Page 243)

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

How to Configure the WinCC - SIMATIC NET FMS OPC Server Connection

Introduction

In this section, a WinCC tag that accesses an FMS index is configured in the WinCC project of the WinCC OPC DA client. The tag value is displayed in an I/O field.

Requirement

- Add the "OPC" channel to the WinCC project of the WinCC OPC DA client.

Procedure

1. In the shortcut menu of the channel unit "OPC Groups(OPCHN Unit#1)" on the WinCC OPC DA client, select "System Parameters". The OPC Item Manager is opened.
2. Choose the name of the computer to be used as the OPC DA server from the selection dialog. Select "OPC.SIMATICNet" from the list. Click the "Browse Server" button. The "Filter Criteria" dialog is opened.
3. Click the "Next->" button in the "Filter Criteria" dialog. The "OPC.SIMATICNet.." dialog is opened. All FMS indexes configured are displayed in a selection list. Select an index. Click the "Add Items" button.
4. If a connection to the SIMATIC NET FMS OPC server already exists, continue with step 5. If no connection has been configured, a corresponding message is displayed. Click "Yes". The "New Connection" dialog is displayed.



Enter "OPC_SlimaticNET" as the name of the connection. Click "OK".

5. The "Add Tags" dialog is opened. Enter "Client_" in the prefix field and "_xyz" in the suffix field. Select the connection "OPC_SimaticNET". Click "Finish".
6. Click the "<- Back" button in the "OPC.SIMATICNet.." dialog. In the "OPC Item Manager", click "Exit" to close the OPC Item Manager.

7. Launch the Graphics Designer and open a new picture. Add an I/O field to the picture. Select the "I/O field" object from the object list under "Smart Objects". The "I/O Field Configuration" dialog is opened.
8. Enter the name of the tags in the "Tag" field. Set the update to "2s". Set the field type to "I/O field".
9. Click "OK" to close the dialog and save the picture. Enable the WinCC project by clicking the "Activate" button in the Graphics Designer.
10. The current value of the FMS index is shown in the I/O field. The value is updated every two seconds. Enter a value in the I/O field. The changed value is passed to the automation device.

See also

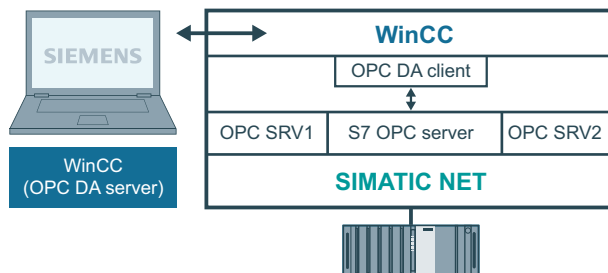
Configuring the OPC Channel on the WinCC OPC DA Client (Page 216)

WinCC - SIMATIC NET S7-OPC Server Connection

Example of a WinCC - SIMATIC NET S7 OPC Server Connection

During the installation of SIMATIC NET, you can select the OPC server to be installed. In the following example, a WinCC - SIMATIC NET S7 OPC server is configured. Data from the automation device is made available to the WinCC client via the SIMATIC NET S7 OPC server.

The current value of the tag is displayed in an I/O field on the WinCC OPC client. As soon as the value of the tags on the SIMATIC NET S7 OPC server changes, the changed value is shown on the process picture. Conversely, a value entered in the I/O field is sent to the automation device.



Requirements

- A computer with WinCC, SIMATIC NET software.
- A configured SIMATIC NET S7 OPC Server. For additional information regarding the setup of SIMATIC NET S7 OPC servers refer to the SIMATIC NET documentation.

Configuration steps

The following configurations are required to establish a WinCC - SIMATIC NET S7 OPC server connection:

1. Adding Tags to a SIMATIC NET S7 OPC Server
2. Configuring Access to the Tags on a SIMATIC NET S7 OPC Server

Communication Manual

The communication manual contains additional information and extensive examples for the channel configuration. This manual is available for download on the Internet:

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

Search by item number:

- A5E00391327

See also

Configuring Access to the Tags of the SIMATIC NET S7 OPC Server (Page 248)

Adding Tags to the SIMATIC NET S7 OPC Server (Page 245)

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

Adding Tags to the SIMATIC NET S7 OPC Server

Introduction

In order for the OPC Item Manager to display the tags, they must be added to the address space of the SIMATIC NET S7 OPC server. The "OPC Scout" program is used for the configuration. OPC Scout is set up by the SIMATIC NET installer. For this example, the marker word "0" in the automation device is addressed.

Table of Parameters Used

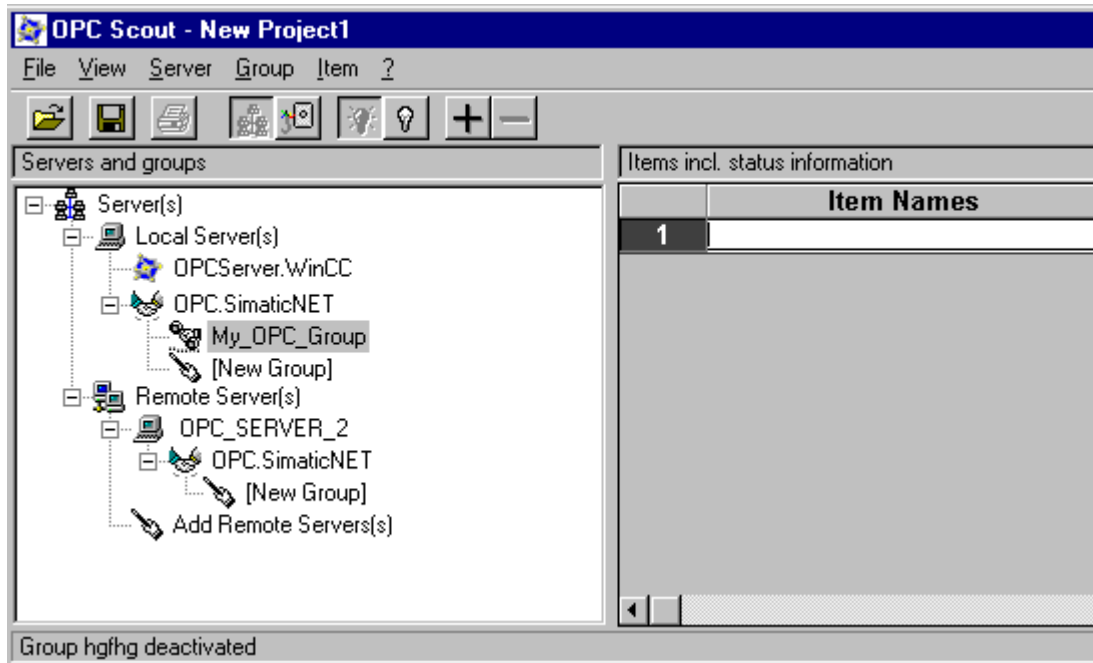
Parameter	Value
Data type	W
Range byte	0
No. values	1
Item alias	MW0

Requirements

- Configure an S7 connection in the SIMATIC NET software. For more information, refer to the SIMATIC NET documentation.

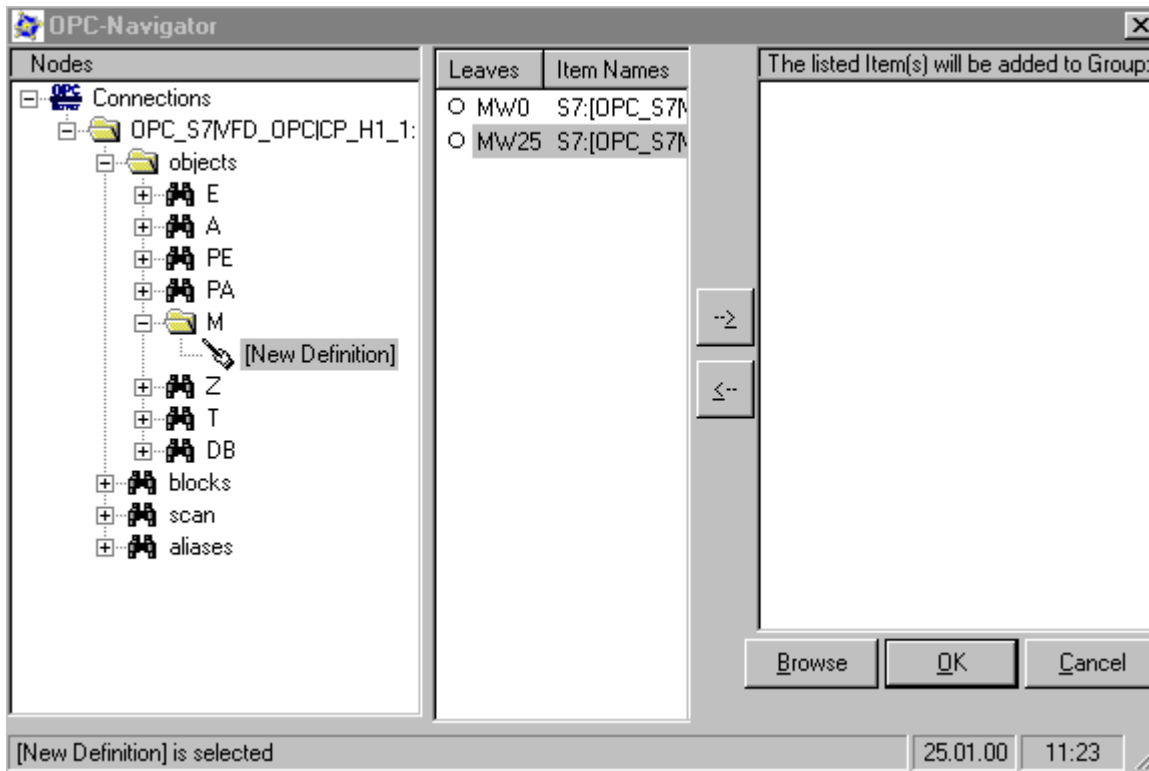
Procedure

1. Open the "OPC Scout" via Start → "Programs" → "SimaticNet" → "OPCServer" → "OPCScout".

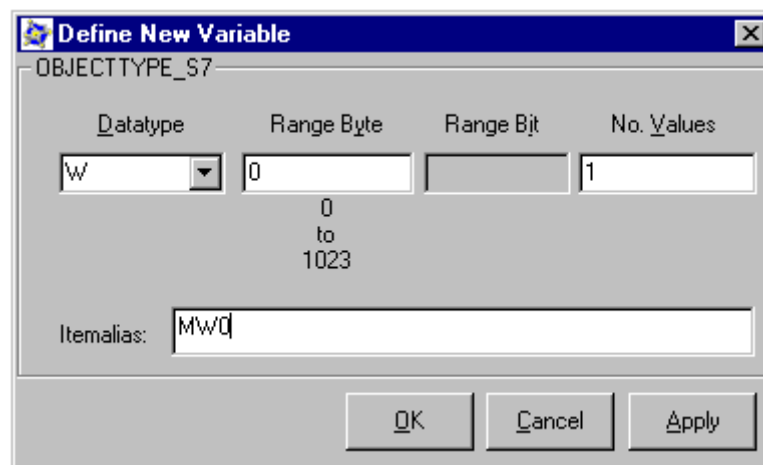


2. Select "OPC.SimaticNet" under "Local Server(s)". If the SIMATIC S7 OPC server is not run on the same computer, select "Add Remote Server(s)" in the "Server(s)" shortcut menu. Enter the name of the computer used as the OPC server in the "Add Remote Server(s)" dialog, then click "OK" to close the dialog.
3. Select "Connect" in the "OPC.SimaticNet" shortcut menu. The "Add Group" dialog is displayed. Enter a name for the group. Click "OK" to close the dialog.

4. Select "Add Item" from the shortcut menu of the added group. The "OPC Navigator" is opened.



5. Select "M" (marker) under "Objects" in the "OPC Navigator". Double-click "(New Definition)" to open the "Define New Tag" dialog.
6. Enter the parameters from the table in the "Define New Tag" dialog.



Click "OK" to close the "Define New Tag" dialog.

7. Mark the tag "MW0" in the "Leaves" area of the OPC Navigator. Click the "-->" button. Click "OK" in the OPC Navigator.

See also

Configuring Access to the Tags of the SIMATIC NET S7 OPC Server (Page 248)

Configuring Access to the Tags of the SIMATIC NET S7 OPC Server

Introduction

In this section, a WinCC tag is configured in the WinCC project of the WinCC OPC DA client. This tag accesses the tag "MW0" in the address space of the SIMATIC NET S7 OPC server. The tag value is displayed in an I/O field.

Requirements

- Create the tag "MW0" using the OPC Scout.
- Add the "OPC" channel to the WinCC project of the WinCC OPC DA client.

Procedure

1. Select "System Parameters" in the shortcut menu of "OPC Groups(OPCHN Unit#1)". The OPC Item Manager is opened.
2. Choose the name of the computer to be used as the OPC server from the selection dialog. Select "OPC.SIMATICNet" from the list. Click the "Browse Server" button. The "Filter Criteria" dialog is opened.
3. Click the "Next->" button in the "Filter Criteria" dialog. The "OPC.SIMATICNet.." dialog is opened. Select the "MW0" tag. Click the "Add Items" button.
4. If a connection to the SIMATIC NET FMS OPC server already exists, continue with step 5. If no connection has been configured, a corresponding message is displayed. Click "Yes". The "New Connection" dialog is displayed.



Enter "OPC_SlimaticNET" as the name of the connection. Click "OK".

5. The "Add Tags" dialog is opened. Enter "Client_" in the prefix field and "_xyz" in the suffix field. Select the connection "OPC_SimaticNET". Click "Finish".
6. Click the "<- Back" button in the "OPC.SIMATICNet .." dialog. In the "OPC Item Manager", click "Exit" to close the OPC Item Manager.

7. Start Graphics Designer and open a picture. Add an I/O field to the picture. Select the "I/O field" object from the object list under "Smart Objects". The "I/O Field Configuration" dialog is opened.
8. Enter the name "Client_MW0_xyz" in the "Tag" field. Set the update to "2s". Set the field type to "I/O field".
9. Close the dialog and save the picture. Enable the WinCC project by clicking the "Activate" button in the Graphics Designer.
10. The I/O field on the WinCC OPC DA client displays the current value of the S7 tags. The value is updated every two seconds. Enter a value in the I/O field. The changed value is passed to the automation device.

See also

Adding Tags to the SIMATIC NET S7 OPC Server (Page 245)

Configuring the OPC Channel on the WinCC OPC DA Client (Page 216)

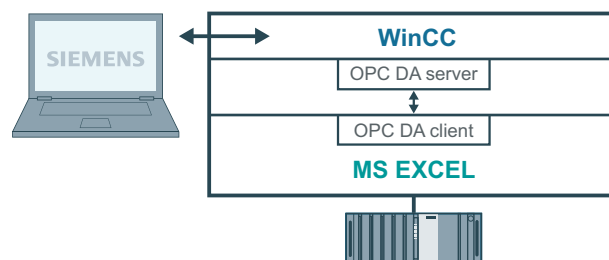
WinCC - Microsoft Excel Connection

Example of the WinCC - Microsoft Excel Connection

Introduction

In this example, an OPC DA client is created in Microsoft Excel using the Visual Basic Editor. The OPC DA client reads a WinCC tag in the WinCC project of the WinCC OPC DA server and writes the value into a cell. If a new value is entered in the cell, the value is passed to the WinCC OPC DA server.

A computer on which both WinCC and Microsoft Excel are installed is used for the connection.



Configuration steps

The following configurations must be made in Microsoft Excel:

1. Creating an OPC DA client in Visual Basic Editor of Microsoft Excel
2. Configuring access to a WinCC tag in Microsoft Excel

See also

How to Configure the Access to a WinCC Tag in Microsoft Excel (Page 252)

Creating an OPC DA Client in Microsoft Excel (Page 250)

Creating an OPC DA Client in Microsoft Excel

Introduction

To use Microsoft Excel as an OPC DA client, a special script must be created in the Visual Basic Editor of Microsoft Excel.

Requirements

Basic knowledge of Visual Basic Editor in Microsoft Excel.

Procedure

1. Open Microsoft Excel with a new workbook.
2. In the "Tools" menu of the Visual Basic Editor, ➔ click "Macro". The Visual Basic Editor for Microsoft Excel is opened.
3. In the "Tools" menu of the Visual Basic Editor, select "References...". The "References - VBAProject" dialog is displayed. Locate entry "Siemens OPC DAAutomation 2.0" in the list of available references. Select the corresponding check box. Click "OK".
4. Copy the script shown below. This script is only available in the online help.
5. Open a new code window by double-clicking "Sheet1" in the project window of the Visual Basic Editor.
6. Paste the script into the code window.
7. Select "Save" from the "File" menu. Select "Close and Return to Microsoft Excel" from the "File" menu.

Example Script

```

Option Explicit
Option Base 1

Const ServerName = "OPCServer.WinCC"

Dim WithEvents MyOPCServer As OpcServer
Dim WithEvents MyOPCGroup As OPCGroup
Dim MyOPCGroupColl As OPCGroups
Dim MyOPCItemColl As OPCItems
Dim MyOPCItems As OPCItems
Dim MyOPCItem As OPCItem

Dim ClientHandles(1) As Long
Dim ServerHandles() As Long
Dim Values(1) As Variant
Dim Errors() As Long
Dim ItemIDs(1) As String
Dim GroupName As String
Dim NodeName As String

'-----
' Sub StartClient()
' Purpose: Connect to OPC_server, create group and add item
'-----
Sub StartClient()
    ' On Error GoTo ErrorHandler
    '----- We freely can choose a ClientHandle and GroupName
    ClientHandles(1) = 1
    GroupName = "MyGroup"
    '----- Get the ItemID from cell "A1"
    NodeName = Range("A1").Value
    ItemIDs(1) = Range("A2").Value
    '----- Get an instance of the OPC-Server
    Set MyOPCServer = New OpcServer
    MyOPCServer.Connect ServerName, NodeName

    Set MyOPCGroupColl = MyOPCServer.OPCGroups
    '----- Set the default active state for adding groups
    MyOPCGroupColl.DefaultGroupIsActive = True
    '----- Add our group to the Collection
    Set MyOPCGroup = MyOPCGroupColl.Add(GroupName)

    Set MyOPCItemColl = MyOPCGroup.OPCItems
    '----- Add one item, ServerHandles are returned
    MyOPCItemColl.AddItem 1, ItemIDs, ClientHandles, ServerHandles, Errors
    '----- A group that is subscribed receives asynchronous notifications
    MyOPCGroup.IsSubscribed = True
    Exit Sub

ErrorHandler:
    MsgBox "Error: " & Err.Description, vbCritical, "ERROR"
End Sub

'-----
' Sub StopClient()

```

2.6 Access via OPC - Open Connectivity

```
' Purpose: Release the objects and disconnect from the server
'-----
Sub StopClient()
    '----- Release the Group and Server objects
    MyOPCGroupColl.RemoveAll
    '----- Disconnect from the server and clean up
    MyOPCServer.Disconnect
    Set MyOPCItemColl = Nothing
    Set MyOPCGroup = Nothing
    Set MyOPCGroupColl = Nothing
    Set MyOPCServer = Nothing
End Sub

'-----
' Sub MyOPCGroup_DataChange()
' Purpose: This event is fired when a value, quality or timestamp in our Group has changed
'-----
'----- If OPC-DA Automation 2.1 is installed, use:
Private Sub MyOPCGroup_DataChange(ByVal TransactionID As Long, ByVal NumItems As Long,
ClientHandles() As Long, ItemValues() As Variant, Qualities() As Long, TimeStamps() As
Date)
    '----- Set the spreadsheet cell values to the values read
    Range("B2").Value = CStr(ItemValues(1))
    Range("C2").Value = Hex(Qualities(1))
    Range("D2").Value = CStr(TimeStamps(1))
End Sub

'-----
' Sub worksheet_change()
' Purpose: This event is fired when our worksheet changes, so we can write a new value
'-----
Private Sub worksheet_change(ByVal Selection As Range)
    '----- Only if cell "B3" changes, write this value
    If Selection <> Range("B3") Then Exit Sub
    Values(1) = Selection.Cells.Value
    '----- Write the new value in synchronous mode
    MyOPCGroup.SyncWrite 1, ServerHandles, Values, Errors
End Sub
```

See also

[How to Configure a WinCC Project on a WinCC OPC DA Server \(Page 239\)](#)

How to Configure the Access to a WinCC Tag in Microsoft Excel

Introduction

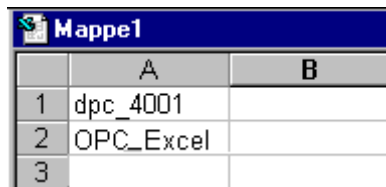
The Excel OPC DA client reads a WinCC tag of the WinCC OPC DA server and writes the value of the tag into a cell. In the WinCC project of the WinCC OPC DA server, the value of the tag is displayed in an I/O field. If the tag value in a cell is changed, this alters the value in the I/O field of the WinCC OPC DA server.

Requirements

- Configure an internal tag named "OPC_Excel" with data type "signed 16-bit value" in the WinCC project of the WinCC OPC DA server.
- Write the value of the "OPC_Excel" tag to an I/O field on the WinCC project of the WinCC OPC DA server.
- Enable the WinCC project of the WinCC OPC DA server.

Procedure

1. In Microsoft Excel, enter the name of the computer used as the OPC server in cell A1. In cell A2, enter the tag name "OPC_Excel".



	A	B
1	dpc_4001	
2	OPC_Excel	
3		

2. In the "Tools" menu in Excel, select "Macro" → "Macros". The "Macro" dialog is opened. Select the entry "Sheet1.StartClient" from the list of macros. Click "Run" to start the OPC client.
3. The value of the tag is written into cell B2, the quality code into C2 and the timestamp into D2.
4. Enter a new value in cell B3. The changed value is displayed in the I/O field on the WinCC OPC server.
5. In the "Tools" menu in Excel, select "Macro" → "Macros". The "Macro" dialog is opened. Select the entry "Sheet1.StopClient" from the list of macros. Click "Run" to stop the OPC client.

2.6.2.7 WinCC OPC HDA server

Functionality of the WinCC OPC HDA server

Introduction

The WinCC OPC HDA server is a DCOM application making data needed from the archive system available to the OPC HDA client. Access the data using Item Handles. Read or write access is enabled. The data can also be analyzed.

The WinCC OPC HDA server supports the OPC Historical Data Access 1.20 specification. This has been confirmed by the compliance test.

The following chapter explains the design of the data structure, as well as the attributes, aggregates and functions supported by the WinCC OPC HDA server. This is not a detailed description, but rather a summary of the most important information. For more information, refer to the "OPC Historical Data Access 1.20" specification.

Installation

The WinCC OPC HDA server can be selected during the installation of WinCC. It is possible to select whether access is made to the WinCC archive system with or without write function. After installation, the WinCC OPC DA server is immediately available for use without any additional configuration.

In the case of installation without write access, the data in the WinCC archive system can only be read and analyzed. In the case of write access, data in the WinCC archive system can be analyzed, added, deleted and updated.

The WinCC OPC HDA server can be implemented on a WinCC server or a WinCC client.

Licensing

In order to operate the WinCC OPC HDA server, the following licenses must be installed on each WinCC computer implemented as an OPC HDA server:

- A valid RT license for WinCC
- WinCC Option Connectivity Pack

Notes on configuration

If the WinCC OPC HDA server is used, the application "OPC DA server, OPC A&E server, OPC HDA server" must be activated.

You can activate the application in the Editor "Computer" of the WinCC Configuration Studio in the "Processes when starting WinCC Runtime" tab.

OPC HDA Client

All OPC HDA clients that conform to the OPC Historical Data Access 1.20 specification can access the WinCC OPC HDA server. You can also create the OPC HDA client yourself. By creating proprietary OPC HDA clients, most user-specific requirements can be met.

Examples of how an OPC HDA client can be used include:

- Analysis and evaluation of archived data
- Statistical process control of archives from different OPC HDA servers

To request for historical values using OPC HDA client, you need to take care of the following during configuration:

- Select a query cycle in such a way that the client can receive the requested data before the next query is sent. Too short cycles can lead to high time delays while receiving data.
- CPU load of the WinCC server depends on the number of tags per query.

Write access to cyclic archive with configured swapping out

In runtime, the data is modified in the cyclic archives on the WinCC server.

Changes are accepted into the swapped-out archive only when the data is changed almost immediately after being created.

If the concerned archive segment of the circulation archive has already been swapped out, then the change is not done subsequently in the swapped-out archive. Even the modified data is deleted when you delete the archive segment on the WinCC server.

See also

Quality codes (Page 260)

Data Structure of a WinCC OPC HDA Server (Page 255)

www.opcfoundation.org (<http://www.opcfoundation.org>)

Data Structure of a WinCC OPC HDA Server

Data Structure of a WinCC OPC HDA Server

Introduction

The data on the WinCC OPC HDA server are structured. The available data structures are listed below. This is not a detailed description, but rather a summary of the most important information. For more information, refer to the "OPC Historical Data Access 1.20" specification.

Data structure

	Description
Attributes	Provide additional quality characteristics for the raw data. Attributes include data type, specifications re. archiving, etc. For more information, see the overview of supported attributes.
Assemblies	Summarize raw data of a specified time interval. Aggregates include average value, minimum, maximum, etc. For more information, see overview of supported aggregates.
StartTime/ EndTime	Set the beginning and end point for the time interval.
Bounding values	Values recorded at the beginning and end. If no bounding values are available, the values closest to these times are used as bounding values.
Raw data	Data from the WinCC archive system of a particular time interval. These data include a time stamp and quality rating.
Item handle	Unique assignment to a WinCC archive tag.
ItemID	Unique identifier of the WinCC archive tag. The ItemID can be used to get an item handle.

See also

Overview of the supported functions (Page 257)

Time Format of a WinCC OPC HDA Server (Page 258)

Overview of the supported attributes (Page 256)

Overview of the supported assemblies (Page 256)

www.opcfoundation.org (<http://www.opcfoundation.org>)

Overview of the supported attributes

Introduction

The following table contains the attributes supported by the WinCC OPC HDA server.

For more information, refer to the "OPC Historical Data Access 1.20" specification.

Attributes

Attribute	Attribute ID	Description
ItemID	OPCHDA_ITEMID	Indicates the WinCC archive tag to be accessed.
Item data type	OPCHDA_DATA_TYPE	Indicates the data type of the WinCC archive tag.
Description	OPCHDA_DESCRIPTION	Returns a description of the WinCC archive tag. The description is defined in WinCC Tag Logging.
Engineering units	OPCHDA_ENG_UNITS	Sets the display of measurement units. The labeling is defined in WinCC Tag Logging.

See also

Data Structure of a WinCC OPC HDA Server (Page 255)

www.opcfoundation.org (<http://www.opcfoundation.org>)

Overview of the supported assemblies

Introduction

The following table lists the aggregates supported by the WinCC OPC HDA server. For more information, refer to the "OPC Historical Data Access 1.20" specification.

Assemblies

Assembly	Description
OPCHDA_COUNT	Returns the raw data count for the specified time interval.
OPCHDA_START	Returns the initial value of the raw data at the beginning of the time interval.
OPCHDA_END	Returns the final value of the raw data at the end of the time interval.
OPCHDA_AVERAGE	Returns the average value of the raw data for the specified time interval.

Assembly	Description
OPCHDA_TIMEAVERAGE	Returns the time-weighted average of the raw data for the specified time interval.
OPCHDA_TOTAL	Returns the sum total value for the specified time interval.
OPCHDA_STDEV	Returns the standard deviation of the raw data for the specified time interval.
OPCHDA_MINIMUMACTUALTIME	Returns the minimum value of the raw data and its time stamp for the specified time interval.
OPCHDA_MINIMUM	Returns the minimum value of the raw data for the specified interval.
OPCHDA_MAXIMUMACTUALTIME	Returns the maximum value of the raw data and its time stamp for the specified time interval.
OPCHDA_MAXIMUM	Returns the maximum value of the raw data for the specified interval.
OPCHDA_DELTA	Returns the difference between the first and last value in the raw data for the specified time interval.
OPCHDA_REGSLOPE	Returns the slope of the regression line of the raw data for the specified time interval.
OPCHDA_REGCONST	Returns the regression value of the raw data at the starting point.
OPCHDA_REGDEV	Returns the standard deviation of the regression of the raw data in the specified time interval.
OPCHDA_VARIANCE	Returns the variance of the raw data for the specified time interval.
OPCHDA_RANGE	Returns the difference between OPCHDA_MAXIMUM and OPCHDA_MINIMUM of the raw data for the specified time interval.
OPCHDA_DURATIONGOOD	Returns the period of time in which the quality of the raw data was good. The period is indicated in seconds.
OPCHDA_DURATIONBAD	Returns the period of time in which the quality of the raw data was bad. The period is indicated in seconds.
OPCHDA_PERCENTGOOD	Returns the percentage of the raw data of good quality.
OPCHDA_PERCENTBAD	Returns the percentage of the raw data of bad quality.
OPCHDA_WORSTQUALITY	Returns the worst quality of the raw data for the specified time interval.

See also

Data Structure of a WinCC OPC HDA Server (Page 255)

Functionality of the WinCC OPC HDA server (Page 253)

www.opcfoundation.org (<http://www.opcfoundation.org>)

Overview of the supported functions

Introduction

The following tables list the functions supported by the WinCC OPC HDA server. These functions can be used by the OPC HDA client for data exchange. For more information, refer to the "OPC Historical Data Access 1.20" specification.

Read

Function	Description
ReadRaw	Returns the raw data, its quality and time stamp for the specified time interval.
ReadProcessed	Returns the calculated value, the quality of the value and the time stamp for the specified time interval. The calculated value is determined by the selected aggregate.
ReadAtTime	Returns the raw data, its quality and time stamp for a particular time interval. If no value is available, the value for this point is interpolated.
ReadAttribute	Returns the item attributes and time stamp for the specified time interval.

See also

Functionality of the WinCC OPC HDA server (Page 253)

www.opcfoundation.org (<http://www.opcfoundation.org>)

Time Format of a WinCC OPC HDA Server

Introduction

The time interval is specified on the WinCC OPC HDA server by setting the starting and ending times. The specified time interval determines the observation period for the historical data. When specifying the times, certain formats must be maintained.

The following options are available for the specification of times:

- Absolute based on UTC
- Relative to the local time of the server

Absolute Value According to UTC

By default, the WinCC OPC HDA server uses the coordinated world time (UTC) as its time base. This time corresponds to the Greenwich Mean Time (Central European Time minus an hour).

Time format

YYYY/MM/DD hh:mm:ss.msmsms

Parameters

YYYY = year

MM = month

DD = day

hh = hours

mm = minutes

ss = seconds

ms = milliseconds

Input example

2002/06/10 09:27:30.000

Specification of Time Relative to Local Time

For this option, the time is entered relative to the local time of the server. The local time zone is set on the computer's "Date/Time" control panel.

Time format

keyword +/-offset1 +/-offset(n)

The offset is the deviation from the local time of the server.

Keywords

NOW = current local time on the server

SECOND = current second

MINUTE = current minute

HOUR = current hour

DAY = current day

WEEK = current week

MONTH = current month

YEAR = current year

Offset

+/-S = deviation in seconds

+/-M = deviation in minutes

+/-H = deviation in hours

+/-D = deviation in days

+/-W = deviation in weeks

+/-MO = deviation in months

+/-Y = deviation in years

Example:

DAY - 1D = previous day

DAY-1D + 7H30 = previous day at 7:30

MO-1D+5H = last day of the previous month at 5:00.

NOW-1H15M = one hour and 15 minutes ago

YEAR+3MO= April of this year

See also

Functionality of the WinCC OPC HDA server (Page 253)

www.opcfoundation.org (<http://www.opcfoundation.org>)

Quality codes

Introduction

Quality codes are used to evaluate the status and quality of the raw data. The quality codes for OPC are described under "6.8 OPC Quality flags" of the "Data Access Custom Interface Standard Version 3.00" specifications.

Quality Codes of the WinCC OPC HDA Server

Code	OPC	Description	Quality
0x00040000	OPCHDA_RAW	Indicates the quality of raw data transmission.	GOOD BAD UNCERTAIN
0x00080000	OPCHDA_CALCULATED	Indicates the quality of calculated data transmission.	GOOD BAD UNCERTAIN
0x00100000	OPCHDA_NOBOUND	No bounding values were found at the starting or ending point.	BAD
0x00200000	OPCHDA_NODATA	No raw data were found for the specified time interval.	BAD
0x00400000	OPCHDA_DATALOST	The raw data in the selected interval were not completely archived.	BAD

See also

www.opcfoundation.org (<http://www.opcfoundation.org>)

Supported Write-Accesses

Introduction

The following table shows the write accesses supported by the WinCC OPC HDA server.

Table element:

	Description
Cyclic archive	The process values to be archived are stored in a cyclic archive. The cyclic archive consists of a configurable number of data buffers. The size and a period of time (e.g. in days) for the data buffer are defined. If all data buffers are full, the process data in the first data buffer is overwritten.
Cyclic archive after swapping	In order to protect process data in the data buffers from being overwritten process, it can be swapped (exported).

	Description
	Supported by WinCC.
	Not supported by WinCC.

Write Accesses

Adding process values later

Cyclic archive	Cyclic archive after swapping	Supported by WinCC	Description
Yes	No		When the time period is contained in the cyclic archive, a process value can be added later.
Yes	Yes		The data buffer of the corresponding time period is swapped to an archive backup. Process values cannot be added later to an archive backup.
No	No		The cyclic archive is not available. The process value cannot be stored.
No	Yes		The cyclic archive is not available. The process value cannot be stored.

Adding process values in Runtime

Cyclic archive	Cyclic archive after swapping	Supported by WinCC	Description
Yes	No		The process value is added in the data buffer currently valid for the cyclic archive.

Inserting future process values

Cyclic archive	Cyclic archive after swapping	Supported by WinCC	Description
YES	No		During write access, no values can be added in the future.
No	No		With write access, no values can be added in the future.

Deleting process values

Cyclic archive	Cyclic archive after swapping	Supported by WinCC	Description
Yes	No		When the time period is contained in the cyclic archive, a process value can be deleted.
Yes	Yes		The data buffer of the corresponding time period is swapped to an archive backup. Process values can be deleted from an archive backup.
No	No		The cyclic archive is not available. The process value cannot be stored.
No	Yes		The cyclic archive is not available. The process value cannot be stored.

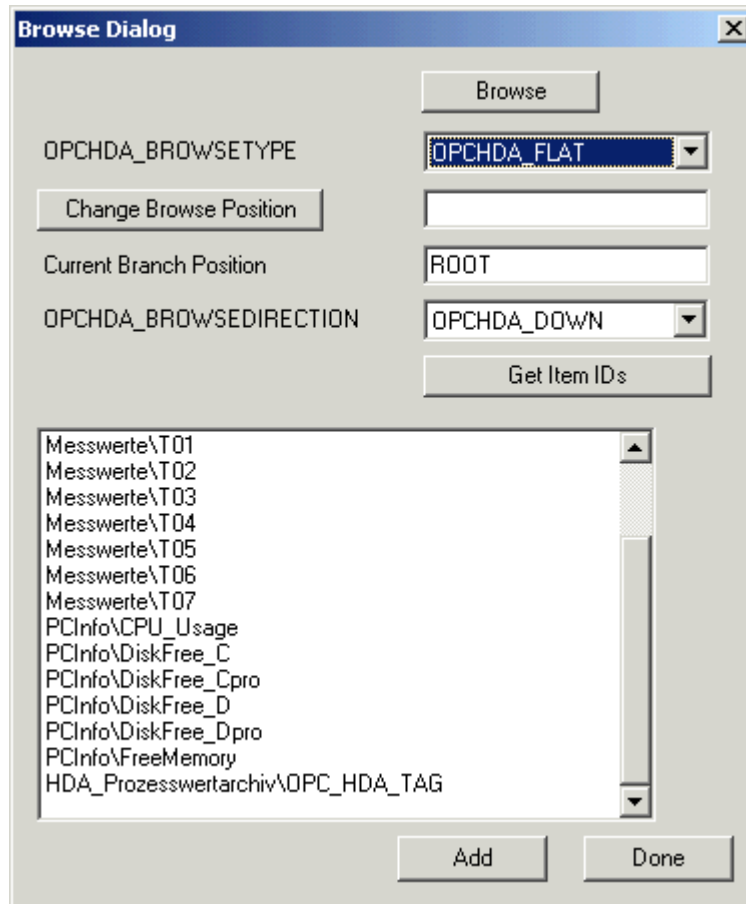
Editing process values

Cyclic archive	Cyclic archive after swapping	Supported by WinCC	Description
Yes	No		When the time period is contained in the cyclic archive, a process value can be edited.
Yes	Yes		The data buffer of the corresponding time period is swapped to an archive backup. Process values cannot be edited in an archive backup.
No	No		The cyclic archive is not available. The process value cannot be stored.
No	Yes		The cyclic archive is not available. The process value cannot be stored.

HDA server browser

Introduction

The OPC HDA client accesses the tag values via item handles. For ease of configuration, the WinCC OPC HDA server supports the browser functionality. The OPC HDA client can use the HDA server browser to search the address space of the WinCC OPC HDA server. The data are listed hierarchically by process value archive.



Note

Access to a WinCC archive tag without the HDA server browser requires manual configuration of the item ID.

When addressing WinCC archive tags, the computer name (server prefix) is included in the path. The ItemID has the following syntax: Server-prefix::process_value_archive\WinCC_archive_tag.

See also

www.opcfoundation.org (<http://www.opcfoundation.org>)

Special features of the OPC HDA server in WinCC for acyclic logging

Introduction

Tag logging is performed in WinCC cyclically or acyclically. The WinCC HDA OPC server works differently depending on the logging method for tags:

- For all cyclically logged values, the OPC HDA server operates in conformity to the HDA specification of the OPC foundation. The OPC aggregates are linearly interpolated.
- Acyclically logged tags are not included in the HDA specification of the OPC Foundation. The OPC aggregates are interpolated incrementally. Especially when a tag experiences no change for a long period of time, no data is available during a time period. The following should be taken into consideration to nevertheless obtain valid data.

Note

The OPC HDA server is not OPC-compliant for acyclically logged tags. The HDA specification of the OPC Foundation does not recognize acyclically logged tags and, therefore, no archive server can handle acyclically logged tags. The supported aggregates are calculated in conformity to the OPC HDA specification. No non-explicitly called functions are supported.

Note

If write access to process value archives is enabled, no future values may be added.

Configuration of acyclically logged tags

For the configuration of acyclically logged tags, the "Archive after segment change" setting needs to be enabled for the tags. This enters the most recent valid value in the the new log when a segment changes.

Supported aggregates of the WinCC OPC HDA server for acyclically logged tags

The OPC HDA server supports the following aggregates:

- OPCHDA_MINIMUM
- OPCHDA_MAXIMUM
- OPCHDA_AVERAGE
- OPCHDA_END
- OPCHDA_INTERPOLATIVE
- OPCHDA_TIMEAVERAGE
- OPCHDA_TOTAL
- OPCHDA_DURATIONGOOD
- OPCHDA_PERCENTGOOD

Supported functions of the WinCC OPC HDA server for acyclically logged tags

- ReadRaw with "boundings" only. ReadRaw for a tag must always be performed with "boundings", in order to find the last real stored value for an area without logged value change.
- ReadProcessed
- DeleteRaw
- DeleteAtTime
- Insert
- InsertReplace
- Replace

Calculating the aggregates for acyclically logged tags

Calculation of the aggregates is based on the extended "RawData" data record, which contains virtual data points for the calculation in addition to real stored values. The WinCC OPC HDA server prepares the contained "RawData" corresponding to the requirements of the "ReadProcessed". The virtual data points needed for the calculation are formed from the bordering real data points. The following significant points are included for the virtual data points:

- Value for the "StartTime"
- Value for the "EndTime"
- Value for interval limits

Example

The values for "00:59:00", "01:02:00" and "01:03:00" are stored for an acyclic tag logging tag. An OPC HDA client postulates with "ReadProcessed" an aggregate with the following parameters:

- StartTime = 01:00:00
- EndTime = 01:04:00
- Interval = 00:02:00

Note

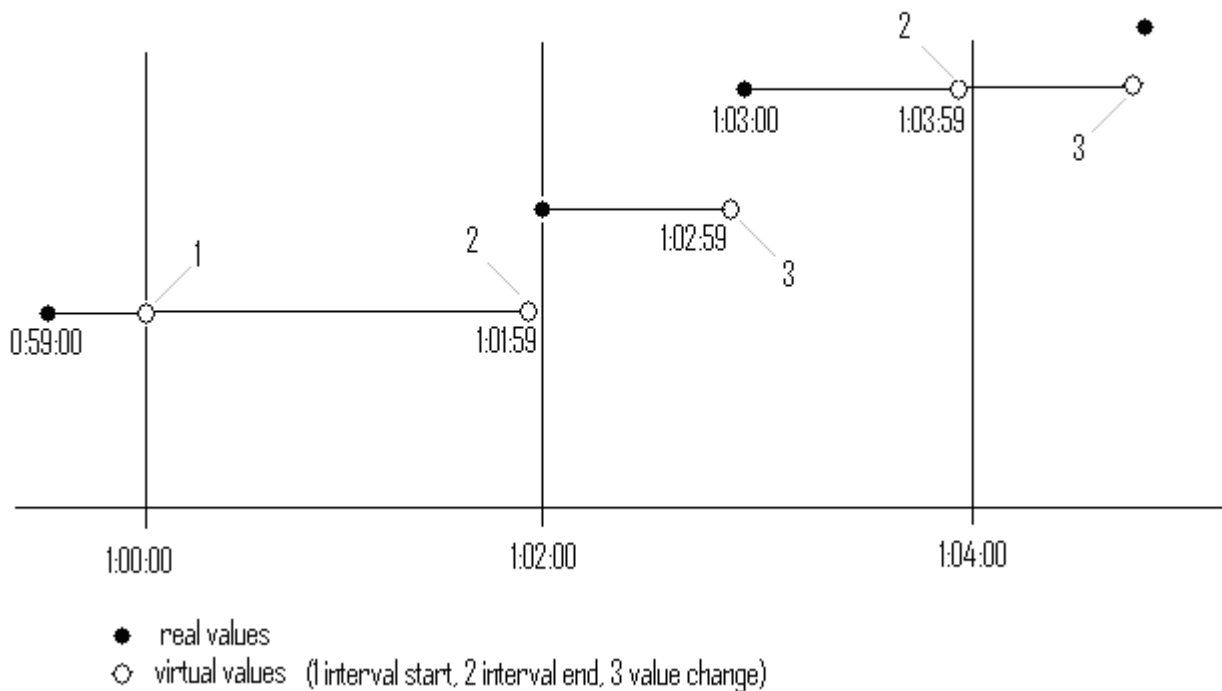
The time period is always 1 μ s less than the time stamp at the limit for the calculation when generating virtual values at limits ("EndTime"/"Interval").

A delta of 1 seconds is used in the following table to provide a better overview. The following graphic illustrates the example.

The OPC server uses the following "RawData" for the calculation of the aggregate:

Number	Time stamp	Real stored values	Generated virtual values
1	00:59:00	1.00	
2	01:00:00		1.00
3	01:01:59		1.00

Number	Time stamp	Real stored values	Generated virtual values
4	01:02:00	2.00	
5	01:02:59		2.00
6	01:03:00	3.00	
7	01:03:59		3.00



2.6.2.8 WinCC OPC A&E Server

Functionality of the WinCC OPC A&E server

Introduction

The WinCC OPC A&E server is a DCOM application. The OPC A&E client is kept informed of status changes for WinCC messages by means of subscriptions. The OPC A&E client can apply a filter to the subscription. This filter determines which messages and attributes are displayed.

The WinCC OPC A&E server supports the specification OPC Alarm&Event 1.10. This has been confirmed by the compliance test.

The following chapter explains the display of the WinCC message system on OPC A&E, as well as the attributes supported by the WinCC OPC A&E server. This is not a detailed description, but rather a summary of the most important information. For more information, refer to the "OPC Alarms & Events 1.10" specification.

Installation

The WinCC OPC A&E server can be selected during the installation of WinCC. After installation, the WinCC OPC A&E server is immediately available for use without any additional configuration.

The WinCC OPC A&E server can be implemented on a WinCC server and a WinCC client.

Licensing

In order to operate the WinCC OPC A&E server, the following licenses must be installed on each WinCC server implemented as an OPC A&E server:

- A valid RT license for WinCC
- WinCC Option Connectivity Pack

Notes on configuration

If the WinCC OPC HDA server is used, the application "OPC DA server, OPC A&E server, OPC HDA server" must be activated.

You can activate the application in the Editor "Computer" of the WinCC Configuration Studio in the "Processes when starting WinCC Runtime" tab.

Server types

The WinCC OPC A&E server supports conditional events and simple events. In addition, there are tracking events.

Condition-related event server

With a condition-related event server, the event is associated with a condition. A condition might, for example, be a limit value violation of a tag. A message is generated in WinCC as soon as the bounding value is exceeded. This message is shown as an alarm in OPC A&E.

Simple event server

Simple events are messages that inform the OPC A&E client about events. Simple events include, for example, starting or exiting programs.

Note

Note the following when using redundant systems:

Simple events interconnected to internal tags are sent twice when tags are updated.

The first message is triggered by the master, the second by the standby.

Tracking event server

If a change in a process occurs, the OPC A&E client receives a message. Such a change might for example be a regulator adjustment.

OPC A&E client

All OPC A&E clients conforming to the OPC Alarms & Events 1.10 specification can access the WinCC OPC A&E server. You can also create the OPC A&E client yourself. By creating proprietary OPC clients, most user-specific requirements can be met. An OPC A&E client can, for example, be used for the analysis and common archiving of alarms from multiple OPC A&E servers.

See also

Quality Codes for OPC A&E (Page 273)

Mapping of the WinCC Message System on OPC A&E (Page 268)

www.opcfoundation.org (<http://www.opcfoundation.org>)

Mapping of the WinCC Message System on OPC A&E

Mapping of the WinCC Message System on OPC A&E

Introduction

During the configuration of the WinCC message system, settings are made to determine which process events generate a message. This message is shown as an alarm in OPC A&E. The table below lists the most important parameters of the alarm. It also describes how the information is made available by the WinCC message system. For more information, refer to "Alarm Structure".

Overview

OPC	WinCC message system
Source	Indicates the source of the message. The source has the format "<server prefix>::@LOCALMACHINE::".
Time	Issues a time stamp for received, sent and acknowledged messages. Issues a time stamp in UTC (Universal Time Coordinated).
Type	Indicates whether the event is a simple, tracking or condition-related event. WinCC - POC A&E server supports simple, condition-related and tracking events.
Severity	Indicates the priority of the WinCC message.
EventCategory	Returns the category of the message. For more information on this topic, refer to "Displaying Message Classes and Types".
Message	Indicates the message text of the corresponding message number.
ConditionName	Indicates the message number.
ChangeMask	Indicates the changed status of the message. For more information, refer to "Acknowledgement Theory".
NewState	Returns the message status. For more information, refer to "Acknowledgement Theory".
ConditionQuality	Returns the quality of the message. For more information, refer to "Quality Codes".

OPC	WinCC message system
AckRequired	Indicates whether the message requires acknowledgement (receipt).
ActiveTime	Returns the time stamp for received messages.
EventAttribute	Lists the attributes required for the respective message. For more information, refer to "Attributes of the WinCC Message System".
Quality	Returns the quality code of the message.
Cookie	Returns the cookie from the OPC A&E server. The cookie corresponds to the message number in the WinCC alarm system

See also

Acknowledgement theory (Page 271)

Attributes of the WinCC Message System (Page 270)

Mapping the WinCC message classes and message types (Page 269)

Mapping the WinCC message classes and message types

Introduction

The WinCC message system informs the user of disturbances and operating conditions in the process. A WinCC message always belongs to a specific message class and message type that is related to the event category.

The mapping of the WinCC message system on OPC is configured via the "CcAeProvider.ini" file.

Event Category

An event category is created on the WinCC OPC A&E server for every combination of a message class and type.

An event category is determined by a category ID and a descriptive "Category Description". The category ID is composed of the WinCC internal IDs for the message class and the message type; the category description is composed of the message class and message type.

Note

If the OPC A&E server is run on a WinCC client of a connectivity station, the OS servers linked to it must have an identical configuration of message classes and message types. If this is not the case, the OPC client used must access the OS server directly.

The names of the message classes and message types can be ascertained exactly via the alarm attributes "CLASSNAME" and "TYPENAME".

Mapping the WinCC message priority

Introduction

The priority of WinCC messages is displayed by the OPC server to the attribute "Severity".

When configuring alarms in the WinCC messaging system, you can configure a priority between 0 and 16. The OPC A&E specification defines a value range from 1 to 1000 for the severity where 1 stands for the lowest and 1000 for the highest severity.

Therefore, the values of the WinCC priority are suitably displayed to the OPC severity. In the standard mapping, the WinCC priority 0 becomes OPC severity 1. All other priority values are interpolated in a linear manner up to severity 1000. Other priority mapping rules can be configured in the CcAeProvider.ini file.

Attributes of the WinCC Message System

Introduction

The following table lists the OPC attributes of the WinCC message system.

The attributes are configured in the WinCC message system.

Some attributes are intended for internal use in WinCC only and are therefore not relevant to an OPC A&E client. These attributes are not contained in the table.

Attributes

OPC attributes	WinCC message system	Data type
CLASSNAME	Outputs the message class name.	VT_BSTR
TYPE NAME	Outputs the message type name.	VT_BSTR
FOREGROUND COLOR	Outputs the text color for activated, deactivated and acknowledged messages.	VT_I4
BACKCOLOR	Outputs the background color for activated, deactivated and acknowledged messages.	VT_I4
FLASHCOLOR	Outputs the flash color.	VT_I4
FLAGS	Indicates whether the message requires acknowledgment.	VT_I4
TEXT01	Outputs the content of UserTextBlock01.	VT_BSTR
TEXT02	Outputs the content of UserTextBlock02.	VT_BSTR
TEXT03	Outputs the content of UserTextBlock03.	VT_BSTR
TEXT04	Outputs the content of UserTextBlock04.	VT_BSTR
TEXT05	Outputs the content of UserTextBlock05.	VT_BSTR
TEXT06	Outputs the content of UserTextBlock06.	VT_BSTR
TEXT07	Outputs the content of UserTextBlock07.	VT_BSTR
TEXT08	Outputs the content of UserTextBlock08.	VT_BSTR
TEXT09	Outputs the content of UserTextBlock09.	VT_BSTR
TEXT10	Outputs the content of UserTextBlock10.	VT_BSTR

OPC attributes	WinCC message system	Data type
PROCESSVALUE01	Outputs the content of ProcessValueBlock01.	VT_VARIANT
PROCESSVALUE02	Outputs the content of ProcessValueBlock02.	VT_VARIANT
PROCESSVALUE03	Outputs the content of ProcessValueBlock03.	VT_VARIANT
PROCESSVALUE04	Outputs the content of ProcessValueBlock04.	VT_VARIANT
PROCESSVALUE05	Outputs the content of ProcessValueBlock05.	VT_VARIANT
PROCESSVALUE06	Outputs the content of ProcessValueBlock06.	VT_VARIANT
PROCESSVALUE07	Outputs the content of ProcessValueBlock07.	VT_VARIANT
PROCESSVALUE08	Outputs the content of ProcessValueBlock08.	VT_VARIANT
PROCESSVALUE09	Outputs the content of ProcessValueBlock09.	VT_VARIANT
PROCESSVALUE10	Outputs the content of ProcessValueBlock10.	VT_VARIANT
STATETEXT	Outputs the status message.	VT_BSTR
INFO TEXT	Outputs the information text for the message.	VT_BSTR
LOOPINALARM	Indicates whether LoopInAlarm is configured.	VT_I4
CLASSID	Outputs the message class ID.	VT_I4
TYPEID	Outputs the message type ID.	VT_I4
MODIFYSTATE	Outputs the value of the status tag of the message.	VT_I4
AGNR	Outputs the number of the AS that generated the message.	VT_I2
CPUNR	Outputs the number of the CPU that generated the message.	VT_I2
DURATION	Outputs the interval between the activation, deactivation and acknowledgment of a message.	VT_I4
COUNTER	Outputs the number of messages after the start of Runtime.	VT_I4
QUITSTATETEXT	Indicates whether the message has been acknowledged.	VT_BSTR
QUITCOUNT	Outputs the number of active, unacknowledged messages.	VT_I4
PARAMETER	Outputs the parameters of message (image of the message configuration).	VT_BSTR
BLOCKINFO	Outputs the current content of the message block.	VT_BSTR
ALARMCOUNT	Outputs the number of messages pending.	VT_I4
LOCKCOUNT	Outputs the number of locked messages.	VT_I4
PRIORITY	Indicates the configured priority of the message.	VT_I4
APPLICATION	Outputs the application which triggered the message.	VT_BSTR
COMPUTER	Outputs the name of the PC that processed the message.	VT_BSTR
USER	Outputs the name of the user who processed the message.	VT_BSTR
COMMENT	Outputs the message comment.	VT_BSTR

Acknowledgement theory

Introduction

For WinCC, the acknowledgment philosophy is how a message is displayed and processed from "came in" to "went out". On the WinCC OPC A&E server, this message status is managed in parameters "ChangeMask" and "NewState".

Conditional, Simple and Tracking Events

Typically, messages from the WinCC system are sent to the client as conditional events. In order for a message to be treated as a simple event, the following conditions must be met during configuration of the message class:

- "Acknowledgment Came In" is not activated.
- "Message Without Status Went Out" is activated.

Depending on the mapping configuration, the messages of the message class "System without Acknowledgement" and of the message type "Operations message" are transferred as OPC Tracking Events.

ChangeMask

The "ChangeMask" parameter keeps track of where the message status was changed.

Parameter values:

- OPC_CHANGE_ACTIVE_STATE
- OPC_CHANGE_ENABLE_STATE
- OPC_CHANGE_ACK_STATE

NewState

The "NewState" parameter indicates the message status after a change.

Parameter values:

- OPC_CONDITION_ACTIVE
- OPC_CONDITION_ENABLED
- OPC_CONDITION_ACKED

Overview

WinCC	NewState	ChangeState
Received message	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACTIVE_STATE
Sent message with receipt	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACTIVE_STATE
Sent message without receipt	OPC_CONDITION_ENABLED	OPC_CHANGE_ACTIVE_STATE
Acknowledged messages (message pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ACKED OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Acknowledged messages (message no longer pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Locked message	-----	OPC_CHANGE_ENABLED_STATE
Unlocked message	OPC_CONDITION_ENABLED	OPC_CHANGE_ENABLED_STATE

WinCC	NewState	ChangeState
Received, acknowledged message	OPC_CONDITION_ACTIVE OPC_CONDITION_ACKED OPC_CONDITION_ENABLED	OPC_CHANGE_ACTIVE_STATE
Received, sent message with receipt	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Received, sent message without receipt	OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Message acknowledged by the system (message pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ACKED OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Message acknowledged by the system (message no longer pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Emergency-acknowledged message (message pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ACKED OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Emergency-acknowledged message (message no longer pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE

See also

www.opcfoundation.org (<http://www.opcfoundation.org>)

Quality Codes for OPC A&E**Introduction**

Quality codes are used to evaluate the status and quality of a message. The quality codes for OPC are described under "6.8 OPC Quality flags" of the "Data Access Custom Interface Standard Version 3.00" specifications.

Quality codes

Code	Quality	Status
0xC0	OPC_GOOD	OK
0x40	OPC_UNCERTAIN	Returned in cases of uncertainty, e.g. in the event of delayed acknowledgement (receipt).
0x00	OPC_BAD	Returned if the connection to the source is interrupted.

OPC A&E server with hierarchical access

Functionality of the OPC A&E server

Introduction

The OPC-A&E server uses DCOM services for transferring messages between OPC-capable applications. The OPC A&E server supports the specification OPC Alarm&Event 1.10.

The following chapter explains the mapping of the WinCC message system on OPC A&E with hierarchical access and the attributes supported by the OPC A&E server. This documentation includes an overview of the specific information. For more information, refer to the "OPC Alarms & Events 1.10" specification.

Principle of operation

The OPC-A&E client receives WinCC messages via subscription. You can use the subscription filter to reduce the number of events that will be transferred with a subscription. The OPC-A&E client can be set for every event category that displays message attributes.

Installation

The WinCC OPC A&E server can be selected during the installation of WinCC. After installation, the WinCC OPC A&E server is immediately available for use without any additional configuration.

The WinCC OPC A&E server can be implemented on a WinCC server and a WinCC client.

Licensing

In order to operate the WinCC OPC A&E server, the following licenses must be installed on each WinCC server implemented as an OPC A&E server:

- A valid RT license for WinCC
- WinCC Option Connectivity Pack

Event types

The OPC-A&E server with hierarchical access supports conditional events, simple events and tracking events.

Condition related events

With a condition related event, the event is associated with a condition. A condition might, for example, be a limit value violation of a tag. This limit violation generates a message that is shown as an alarm with OPC A&E.

Simple events

Simple events are messages that inform the OPC A&E client about events. Simple events include, for example, starting or exiting programs.

Note

Note the following when using redundant systems:

Simple events interconnected to internal tags are sent twice when tags are updated.

The first message is triggered by the master, the second by the standby.

Tracking events

A tracking event is sent with a operator input message to the OPC A&E client. An operator input message is triggered by manual intervention in the process.

OPC A&E client

All OPC A&E clients conforming to the OPC Alarms & Events 1.10 specification can access the OPC A&E server. You can also create the OPC A&E client yourself. By creating proprietary OPC clients, most user-specific requirements can be met. An OPC A&E client, for example, may be used for analysis and joint archiving of alarms from different OPC A&E servers. The acknowledgment of archived messages is not possible; only current alarms and events can be acknowledged.

If you are using the OPC A&E with hierarchical access and want to use all functions, you may need to adapt the OPC A&E client currently used.

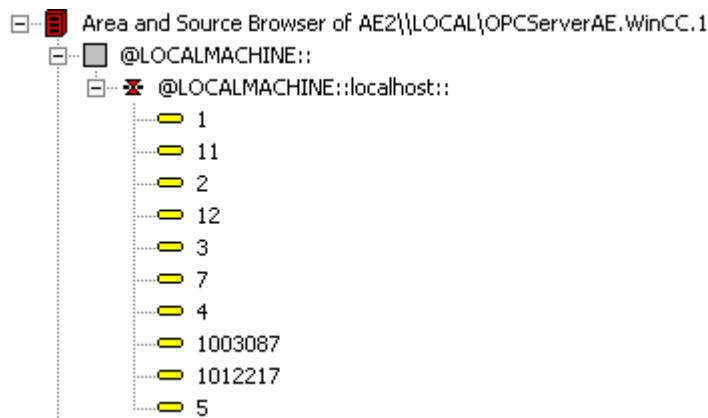
Note**Documentation on OPC**

You can find additional information on OPC in the Chapter "Interfaces > OPC - OLE for Process Control".

Differences between OPC A&E and OPC A&E with hierarchical access**Displaying messages with OPC A&E**

The OPC A&E server supports "conditional events" and "simple events" for accessing the message system. With "conditional events", the message numbers are shown for each source. Since an WinCC server can hold many more message numbers, it is difficult to maintain an overview of the messages.

The following figure shows an example of the display in an OPC browser:



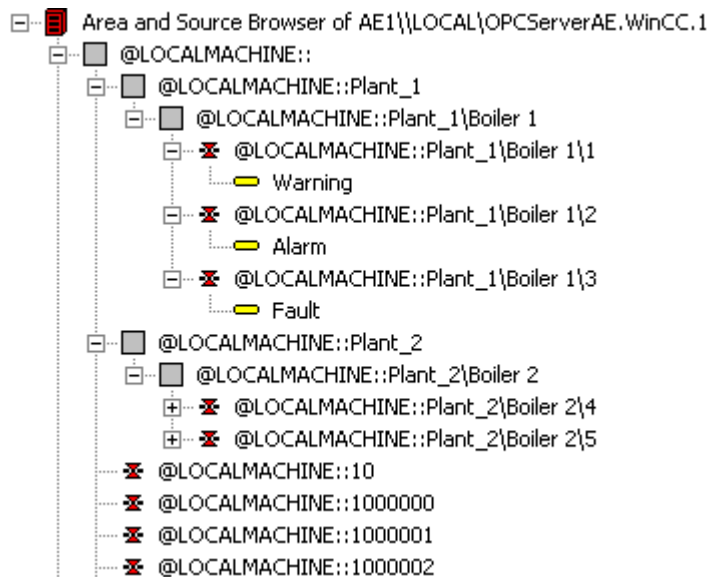
Displaying the messages with OPC A&E and hierarchical access

The OPC A&E server with hierarchical access supports the event types, conditional events, simple events and tracking events.

The user text block 2 determines the source of the messages for "conditional events". With the default setting, user text block 2 corresponds to the fault location. In order to present messages hierarchically, they must be combined in user-defined group messages in alarm logging messages. The structure of group messages is determined by the areas in OPC A&E.

Tracking events occur when operator input messages are triggered in the system.

The following figure shows an example of the display of conditional events in an OPC browser. The "Condition" is shown in addition to "Area" and "Source":



Switching to OPC A&E with hierarchical access

Use an OPC A&E server with hierarchical access when creating a new project.

In an existing project, the OPC A&E server can be used as before or be converted for hierarchical access. The conversion can be undone again without any loss of data.

1. Copy the "CcAeProvider.ini" file into the project folder. The file is located in the WinCC installation path in the folder "OPC\AlarmEvent\Hierarchical-Access".
2. Update the clients or perform a complete download for the OS servers.

Mapping the WinCC Message System on OPC A&E

Mapping the WinCC message system

Introduction

The WinCC message system resulting from the configuration defines which event in the process will generate a message. This message is shown as an event notification in OPC A&E.

Mapping the WinCC message system on OPC A&E with hierarchical access

The OPC source of the WinCC user text block "2" and the OPC message of WinCC user text block "1" are used in WinCC as a default setting for mapping the WinCC message systems.

Overview

The following table shows the most important attributes of the event notifications and the respective information from the WinCC message system.

The events that use the configured attributes are shown in the third column of the table:

- "S" means a simple event
- "C" means a conditional event
- "T" means a tracking event

OPC	WinCC message system	Event type
Area	The structure of the group messages determine the areas in OPC A&E. If there is no group message configured for the message, only the OPC area corresponding to the server prefix is available.	S, C, T
Source	Indicates the source of a message. The source has the format "<server prefix>::Arealuser text block 2". The server prefix of a local computer is "@LOCALMACHINE". The server prefix always shows the top Areas in the hierarchy of the server.	S, C, T
Time	Issues a time stamp for received, sent and acknowledged messages. Issues a time stamp in UTC (Universal Time Coordinated).	S, C, T
Type	Indicates whether the event is a simple, tracking or conditional event.	S, C, T
Severity	Returns the priority of the message.	S, C, T
EventCategory	Indicates the message class. "Event Category" is made up of the "CategoryID" and the "Category Description". "CategoryID" corresponds to the internal ID of the message class. "Category Description" corresponds to the name of the message class.	S, C, T
Message	Indicates the message text of the corresponding message number.	S, C, T

OPC	WinCC message system	Event type
Condition	Indicates the message type.	C
Sub-condition	Corresponds with the "Condition" parameter.	C
ChangeMask	Specifies the change of the condition. For more information, refer to "Acknowledgment Theory".	C
NewState	Indicates the current status of the condition. For more information, refer to "Acknowledgment Theory".	C
ConditionQuality	Returns the quality of the message. For more information, refer to "Quality codes".	C
AckRequired	Indicates whether the message requires acknowledgment.	C
EventAttribute	Lists the attributes required for the respective message. For more information, refer to "Attributes of the WinCC message system".	C
Quality	Returns the quality code of the message.	C
Cookie	Does not include any usable information for the client	C
ActorID	Indicates which user acknowledged the message.	T

Note

If text without wild cards are specified as a filter for the area, only the messages of the area are returned. If you want to include sources that are located in areas outside the specified area, you need to use wild cards.

Note

The message classes and message types **must** be configured identically on the connected OS servers, if you run the OPC A&E server as follows:

- On a WinCC Client
- On a Connectivity station

If the OS server is not configured identically, the employed OPC client must access the respective OS server directly.

Mapping the message priority

Introduction

The priority of messages is mapped by the OPC A&E server to the attribute "Severity".

When configuring alarms in the messaging system, you can configure a priority between "0" and "16". The OPC A&E specification defines a value range of "1" to "1000" for the severity. In this case, "1" stands for the lowest and "1000" for the highest severity.

Therefore, the values of the priority are suitably displayed to the OPC severity. In the standard mapping, priority "0" is assigned to OPC severity "1" and priority "16" to OPC severity "1000". All other priority values are interpolated linearly between "0" and "1000".

Attributes of the WinCC Message System

Introduction

The following table lists the OPC attributes of the WinCC message system.

The attributes are configured in the WinCC message system.

Some attributes are intended for internal use in WinCC only and are therefore not relevant to an OPC A&E client. These attributes are not contained in the table.

Attributes

OPC attributes	WinCC message system	Data type
CLASSNAME	Outputs the message class name.	VT_BSTR
TYPE NAME	Outputs the message type name.	VT_BSTR
FOREGROUND COLOR	Outputs the text color for activated, deactivated and acknowledged messages.	VT_I4
BACKCOLOR	Outputs the background color for activated, deactivated and acknowledged messages.	VT_I4
FLASHCOLOR	Outputs the flash color.	VT_I4
FLAGS	Indicates whether the message requires acknowledgment.	VT_I4
TEXT01	Outputs the content of UserTextBlock01.	VT_BSTR
TEXT02	Outputs the content of UserTextBlock02.	VT_BSTR
TEXT03	Outputs the content of UserTextBlock03.	VT_BSTR
TEXT04	Outputs the content of UserTextBlock04.	VT_BSTR
TEXT05	Outputs the content of UserTextBlock05.	VT_BSTR
TEXT06	Outputs the content of UserTextBlock06.	VT_BSTR
TEXT07	Outputs the content of UserTextBlock07.	VT_BSTR
TEXT08	Outputs the content of UserTextBlock08.	VT_BSTR
TEXT09	Outputs the content of UserTextBlock09.	VT_BSTR
TEXT10	Outputs the content of UserTextBlock10.	VT_BSTR
PROCESSVALUE01	Outputs the content of ProcessValueBlock01.	VT_VARIANT
PROCESSVALUE02	Outputs the content of ProcessValueBlock02.	VT_VARIANT
PROCESSVALUE03	Outputs the content of ProcessValueBlock03.	VT_VARIANT
PROCESSVALUE04	Outputs the content of ProcessValueBlock04.	VT_VARIANT
PROCESSVALUE05	Outputs the content of ProcessValueBlock05.	VT_VARIANT
PROCESSVALUE06	Outputs the content of ProcessValueBlock06.	VT_VARIANT
PROCESSVALUE07	Outputs the content of ProcessValueBlock07.	VT_VARIANT
PROCESSVALUE08	Outputs the content of ProcessValueBlock08.	VT_VARIANT
PROCESSVALUE09	Outputs the content of ProcessValueBlock09.	VT_VARIANT
PROCESSVALUE10	Outputs the content of ProcessValueBlock10.	VT_VARIANT
STATETEXT	Outputs the status message.	VT_BSTR
INFO TEXT	Outputs the information text for the message.	VT_BSTR
LOOPINALARM	Indicates whether LoopInAlarm is configured.	VT_I4
CLASSID	Outputs the message class ID.	VT_I4

OPC attributes	WinCC message system	Data type
TYPEID	Outputs the message type ID.	VT_I4
MODIFYSTATE	Outputs the value of the status tag of the message.	VT_I4
AGNR	Outputs the number of the AS that generated the message.	VT_I2
CPUNR	Outputs the number of the CPU that generated the message.	VT_I2
DURATION	Outputs the interval between the activation, deactivation and acknowledgment of a message.	VT_I4
COUNTER	Outputs the number of messages after the start of Runtime.	VT_I4
QUITSTATETEXT	Indicates whether the message has been acknowledged.	VT_BSTR
QUITCOUNT	Outputs the number of active, unacknowledged messages.	VT_I4
PARAMETER	Outputs the parameters of message (image of the message configuration).	VT_BSTR
BLOCKINFO	Outputs the current content of the message block.	VT_BSTR
ALARMCOUNT	Outputs the number of messages pending.	VT_I4
LOCKCOUNT	Outputs the number of locked messages.	VT_I4
PRIORITY	Indicates the configured priority of the message.	VT_I4
APPLICATION	Outputs the application which triggered the message.	VT_BSTR
COMPUTER	Outputs the name of the PC that processed the message.	VT_BSTR
USER	Outputs the name of the user who processed the message.	VT_BSTR
COMMENT	Outputs the message comment.	VT_BSTR
HIDDEN COUNT	Outputs the number of hidden messages.	VT_I4
BIG COUNTER	Outputs the number of messages after the start of Runtime.	VT_CY
OS-HIDDEN	Outputs the hidden status of the message.	VT_BOOL
OS-EVENTID	Outputs the message number configured for the message.	VT_I4

Acknowledgement Theory

Introduction

The acknowledgment policy in WinCC is how a message from "came in" to "went out" is displayed and processed. On the OPC A&E server, this message status is displayed in the "ChangeMask" and "NewState" parameters.

Conditional events, simple events and tracking events

Messages from the system are sent to the client as conditional events with acknowledgment.

In order for a message to be handled as a simple event, the message class of the message must meet the following conditions:

- "Acknowledgment came in" is not activated.
- "Message without status went out" is activated.

In WinCC, messages of message class "System, does not require acknowledgment" with "Operator input message" message type are transferred as tracking events.

Note

Messages with "System, does not require acknowledgment" message class and "Process control system" message type are transferred as simple events with the "System message" event category.

ChangeMask

The "ChangeMask" parameter keeps track of where the message status was changed.

Parameter values:

- OPC_CHANGE_ACTIVE_STATE
- OPC_CHANGE_ENABLE_STATE
- OPC_CHANGE_ACK_STATE

NewState

The "NewState" parameter indicates the message status after a change.

Parameter values:

- OPC_CONDITION_ACTIVE
- OPC_CONDITION_ENABLED
- OPC_CONDITION_ACKED

Overview

WinCC	NewState	ChangeState
Received message	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACTIVE_STATE
Went out message with acknowledgment	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACTIVE_STATE
Went out message without acknowledgment	OPC_CONDITION_ENABLED	OPC_CHANGE_ACTIVE_STATE
Acknowledged messages (message pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ACKED OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Acknowledged messages (message no longer pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Locked message	-----	OPC_CHANGE_ENABLED_STATE
Unlocked message	OPC_CONDITION_ENABLED	OPC_CHANGE_ENABLED_STATE
Came in, acknowledged message	OPC_CONDITION_ACTIVE OPC_CONDITION_ACKED OPC_CONDITION_ENABLED	OPC_CHANGE_ACTIVE_STATE

2.6 Access via OPC - Open Connectivity

WinCC	NewState	ChangeState
Came in, went out message with acknowledgment	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Came in, went out message without acknowledgment	OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Message acknowledged by the system (message pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ACKED OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Message acknowledged by the system (message no longer pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Emergency-acknowledged message (message pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ACKED OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE
Emergency-acknowledged message (message no longer pending)	OPC_CONDITION_ACTIVE OPC_CONDITION_ENABLED	OPC_CHANGE_ACK_STATE

Note

Historical alarms and events are not acknowledged. The OPC A&E historical events interface only has read access.

Quality Codes for OPC A&E

Introduction

Quality codes are used to evaluate the status and quality of a message. The quality codes for OPC are described under "6.8 OPC Quality flags" of the "Data Access Custom Interface Standard Version 3.00" specifications.

Quality codes

Code	Quality	Status
0xC0	OPC_GOOD	OK
0x40	OPC_UNCERTAIN	Returned in cases of uncertainty, for example in the event of delayed acknowledgment (receipt).
0x00	OPC_BAD	Returned if the connection to the source is interrupted.

Reading archived messages

Accessing archived events

Introduction

You can access the archived messages via the OPC A&E server using an OPC client. Two methods are supported for accessing archived messages:

- Output archived messages from a time period in the past
- Output archived messages from a time period in the past without mentioning end of period. After the output of archived messages, all other newly generated messages are automatically sent to the OPC client.

Note

After reading archived messages, you cannot use the returned "ActiveTime" of a message for acknowledging the message or tracing transitions of the message. To ensure this, the OPC A&E client must check the "EventType" of a message with the extra flag "OPC_HAE_HISTORICAL_EVENTFLAG". The "ActiveTime" is incorrect on archived messages. You can find information on the additional flag under "Identifying archived messages".

Querying the "Historic Alarms and Events" functionalities

In addition to the standard filters, the following filters are offered with the expanded OPC A&E server of WinCC:

Filter	Filter Values	Description
OPC_HAE_FILTER_BY_TIMEFRAME	0x80000000	Matches "ReadRaw" function for OPC Historical Data Access
OPC_HAE_FILTER_BY_STARTTIME	0x40000000	Matches "AdviseRaw" function for OPC Historical Data Access

Source filter and historical alarm request

To request the archive messages, the OPC client must support the "SetFilter" to a subscription functionality. The OPC server will also send archived messages if you also insert keyword "OPCHAEsServer" the array of the "Source Filter" of a subscription. In addition to this keyword, you can use other parameters to define which messages are to be read:

- Method
- Time period
- With or without limits

The lists of sources that are assigned in the filter can include other source names besides the "OPCHAEsServer" source. In such a case, the subscription delivers only the historic events of the given sources. The sequence of the source names is inconsequential.

After configuring the source filter, the selected time period can be called up from the client with a "Refresh" call.

Syntax for accessing archived messages using OPC

Syntax

```
OPCHAEServer hMode=(read|advise) htStartTime=szTime  
[htEndTime=szTime] [bBounds=(TRUE|FALSE)]
```

Parameter

hMode = [read|advise]

This parameter is required. Defines how the archived messages and events are to be read.

Read: Outputs archived messages and events of a definite period from the past (comparable to ReadRaw in case of OPC Historical Data Access).

The following is an example for setting a filter for reading over the last 30 minutes:

```
OPCHAEServer hMode=read htStartTime=NOW-30M bBounds=TRUE
```

Advise: Outputs archived messages and events from a definite period, After receiving all archived messages, new messages are sent in the same way as in the case of an active subscription (comparable to AdviseRaw in case of OPC Historical Data Access).

In the following example, the messages of the last 30 minutes are read (subscription must be active):

```
OPCHAEServer hMode=advise htStartTime=NOW-30M
```

Note

The following notation is supported for parameters "htStartTime" and "htEndTime":

- Relative notations, for example NOW
- Symbolic values, for example NOW, YEAR, MONTH
- Specification of absolute UTC data/time values according to XML notation:
2006-09-01T10:00:00.000Z

Using the symbolic notation corresponds to the syntax from OPC Historical Data Access.

htStartTime =

This parameter is required. Defines the time from when the messages and events are to be read from the archive.

htEndTime =

This parameter is optional. Defines the time up to which the messages and events are to be read from the archive. With "hMode = read", the default setting "NOW" is used.

bBounds = [TRUE|FALSE]

This parameter is optional. Defines how messages close to the start and end time are to be handled. The function is identical to OPC Historical Data Access

bBounds=FALSE:

- The time stamp of the first transferred message $\geq$ htStartTime
- The time stamp of the last transferred message $\geq$ htEndTime

bBounds=TRUE:

- The time stamp of the first transferred message $\leq$ htStartTime
- The time stamp of the last transferred message $\geq$ hEndTime

Default setting is FALSE.

Read methods for archived messages

Introduction

You can use one of two read modes to read archived messages:

- read
- advise

Read mode "read"

Archived messages from a defined period in the past are read with "read" mode. The order of the read messages is always chronological with regard to each OS server from which alarms are being read. By setting the start and end times, you can specify whether the oldest message is to be output first or last. If the start time is earlier than the end time, the oldest message is output last.

If you want to use "read" mode, run the following functions on the subscription:

1. SetFilter
2. Refresh

Event packets with Refresh identifier contain only historical events. The events can also be in queue.

The last Refresh packet of the historical messages contains the "Last Refresh" identifier.

A "SetFilter" during the "Refresh" will be rejected. If you activate the subscription during the "Refresh", it has no effect on the refresh process.

The historical events will continue to be transmitted with the Refresh identifier.

The newly generated events are transmitted according to the standard behavior of an active subscription:

- Taking into account the set filter values with the exception of the "historical" source "OPCHAEServer"
- Without the Refresh identifier

This enables the client to differentiate the received events based on the Refresh identifier. An event packet never contains historical and new events at the same time.

- Event packets with Refresh identifier contain only historical events. These events can also be in queue.
- Event packets without the Refresh identifier contain only newly generated events.

Read mode "advise"

Archived messages starting from a defined period in the past are read with "advise" mode. After all archived messages are read, new messages are sent the same as when a subscription is active. The archived messages are transferred chronologically with respect to each OS server: The archived messages starting from the start time are transmitted first. The newly archived messages are transmitted afterwards.

Note that you must not specify an end time for "advise".

An active subscription is used for "advise" mode. If you run the "SetFilter" function on an active subscription, the historical alarms are transmitted immediately.

If you run the "SetFilter" function on an inactive subscription, the archived messages are only transmitted after activation of the subscription. If you want to use "advise" mode with an inactive subscription, proceed as follows:

1. SetFilter
2. Set subscription to active using SetState

The transmission is ended when you set the subscription to "inactive". A "SetFilter" is rejected while the subscription is active.

A "Refresh" on an active "historical" subscription in "advise" mode functions in the same way as on a standard subscription:

All queued condition related events are transmitted in packets with Refresh identifier.

A "Refresh" call has no effect on the reading of historical alarms in "advise" mode.

Identifying archived messages

General procedure

Archived messages are distinguished using an additional flag in EventType. This flag is linked to the real EventType via a OR link.

Name	EventType	EventType (archived message)
OPC_SIMPLE_EVENT	0x01	0x81
OPC_CONDITION_EVENT	0x04	0x84
OPC_TRACKING_EVENT	0x02	0x82
OPC_HAE_HISTORICAL_EVENTFLAG		0x80

Examples

Example 1

The following source filter is used to output archived messages and events of the last 30 minutes in "read" mode. The oldest message for each OS server is output as the first one. The low limit value is also sent.

```
OPCHAEServer hMode=read htStartTime=NOW-30M bBounds=TRUE
```

Example 2

The following source filter is used to output archived events on September 1, 2006 from 10:00 to 12:00 hours in "read" mode. The newest message for each OS server is output as the first one. The limits for this time period are also sent.

```
OPCHAEServer hMode=read htStartTime=2006-09-01T12:00:00.000Z  
htEndTime=2006-09-01T10:00:00.000Z bBounds=TRUE
```

Example 3

The following source filter is used to output archived messages and events of the last 30 minutes in "advise" mode. After reading the archived messages, newly generated messages are sent in the same way as for an active subscription.

```
OPCHAEServer hmode=advise htStartTime=NOW-30M
```

2.6.2.9 WinCC OPC UA Server

Principle of operation the WinCC OPC UA Server

How it works

The WinCC OPC UA Server provides the following values:

- Process values
- Values from tag archives
- WinCC messages
- Running the configured C/VB scripts

The WinCC OPC UA server is installed as Windows service and started automatically. The WinCC OPC UA server supports only the "UA-TCP UA-SC UA Binary" communication profile. The used port number is adjustable.

Supported specifications

OPC Unified Architecture is a specification for the transmission of process values, archive data and messages. The WinCC OPC UA server supports OPC UA Specification 1.04. For additional information about supported UA functions, refer to "Supported OPC UA services and profiles (Page 294)".

Installation

After WinCC is installed, the WinCC OPC UA server can be used immediately without the need for any further configuration.

The WinCC OPC UA server can be used on a WinCC server or a WinCC client.

URL of the WinCC OPC UA server

You access the WinCC OPC UA server via the following URL:

- "opc.tcp://[NodeName]:[Port]"

Parameter	Description
NodeName	Placeholder for the computer name. Is used automatically
Port	Port number. The default setting is "4862".

Discovery Server

The "Discovery Server" is available by the OPC foundation. The "Discovery Server" is by default installed on the HMI device as Windows service.

On the "Discovery Server" via OPC UA server UA clients information is available that is registered on the "Discovery Server".

Depending on the configuration, the WinCC OPC UA server registers on no, on one or on multiple configured and available "Discovery servers" upon runtime startup. Registration is then repeated cyclically. If you end Runtime, the WinCC OPC UA server is automatically logged off from the "Discovery server".

Supported languages in the WinCC address area

The WinCC OPC A&E Server supports the WinCC address area in the following languages:

- German
- English
- French
- Italian
- Spanish

Security concept of OPC UA

Introduction

The OPC UA security concept is based largely on:

- Authentication and authorization of applications and users involved
- Ensuring the integrity and confidentiality of messages exchanged between the applications

Certificates are the method used for authentication of the OPC UA applications.

Each application has its own instance certificate with which it identifies itself in the public key infrastructure. The instance certificate is also called the "application certificate".

Certificate of the WinCC OPC UA Server

For secure operation, each WinCC OPC UA server requires its own certificate with a private key, a server certificate.

The certificate is only valid on the corresponding computer and may only be used by the WinCC OPC UA server installed on that computer.

A self-signed certificate of the server is created and stored in the certificate folder of the server.

The private key for this server certificate is also stored in the certificate folder. You must restrict access to the folder with the private key to:

- the server itself
- the system administrator

NOTICE

Access to the folder with the private key

For security reasons, no other users or applications apart from the server and the system administrator may have access to the private key of the WinCC OPC UA server.

The administrator of the plant can replace the server certificate and the corresponding private key generated during the installation.

In accordance with the applicable security concept for the system, the new server certificate can be either self-signed or issued by a certification authority.

The certificates used by the WinCC OPC UA server are determined by the settings in the "OpcUaServerWinCC.xml" configuration file: You can find additional information under "Configuration file of the WinCC OPC UA Server (Page 307)".

Storage of server certificates

The "WinCC OPC UA server" application is stored in the following path:

Storage path	Application	Configuration file
<Installation directory>WinCC\opc\UA-Server\	OpcUaServerWinCC.exe	OpcUaServerWinCC.xml

The WinCC OPC UA certificates are stored in the following folders of the WinCC installation path:

WinCC OPC UA server	Certificates	opc\UAServer\PKI\CA\certs
	Private key	opc\UAServer\PKI\CA\private

You can change the storage location in the configuration file.

```
<ServerCertificate>[ApplicationPath]/PKI/CA/certs/</ServerCertificate>
```

Note

Windows-based certificate authority is supported to provide server certificates.

Trusted client certificates

The WinCC OPC UA server supports secure communication with trusted clients only. A client is trusted:

- If the client has a valid self-signed certificate which is stored in the trusted certificates certificate memory of the WinCC OPC UA server
- or if the valid client certificate was issued by a certification authority.
The valid certificate from the certification authority must be located in the trusted certificates certificate memory of the WinCC OPC UA server. In this case, only the certificate from the certification authority is required. The client certificate does not need to be located in the certificate store for trusted certificates.

Storage of client certificates

You specify the storage settings for trusted certificates using the WinCC OPC UA server configuration file:

```
<DefaultApplicationCertificateStore>
  <!--The maximum size of the TrustList in bytes. 0 means no limit.-->
  <MaxTrustListSize>0</MaxTrustListSize>
  <!--For CA signed certificates this flag controls if server shall send the complete certificate chain instead of just sending the certificate.
  <SendCertificateChain>true</SendCertificateChain>
  <!--File based certificate store used with OpenSSL
  <OpenSSLStore>
    <CertificateTrustListLocation>[ApplicationPath]/PKI/CA/certs/</CertificateTrustListLocation>
    <CertificateRevocationListLocation>[ApplicationPath]/PKI/CA/crl/</CertificateRevocationListLocation>
    <IssuersCertificatesLocation>[ApplicationPath]/PKI/CA/certs/</IssuersCertificatesLocation>
    <IssuersRevocationListLocation>[ApplicationPath]/PKI/CA/crl/</IssuersRevocationListLocation>
  </OpenSSLStore>
  <!--Windows based certificate store.
  <!--Application instance certificate for the Server.-->
  <ServerCertificate>
</DefaultApplicationCertificateStore>
```

Note

Certificates from the memory of the certification authorities are not automatically trusted.

For a certification authority to be trusted, its certificate must be located in the memory for trusted certificates.

Note

Windows-based certificate authority is supported to provide server certificates.

Client certificates not accepted

If a UA client accesses the WinCC OPC UA server without having a trusted certificate, the WinCC OPC UA server does not allow secure communication and copies the client certificate to the folder for rejected certificates.

You specify storage settings for rejected certificates using the WinCC OPC UA server configuration file, for example

```
<!--Folder used to store rejected client certificates. Administrators can copy files from here to the trust list.  
[ApplicationPath] can be used as placeholder for the application path.-->  
<RejectedCertificatesDirectory>[ApplicationPath]/PKI/CA/rejected/certs</RejectedCertificatesDirectory>
```

Note

The storage of rejected certificates is "File based".

To enable secured communication with this client, you will have to move the rejected certificate to the certificate store for trusted certificates.

See also

Configuration file of the WinCC OPC UA Server (Page 307)

Configuring the security mechanisms

Introduction

The following is ensured at the communication level:

- UA application authenticity
- The confidentiality of messages exchanged
- The integrity of messages exchanged

The security mechanisms used, for example algorithms for encrypting and signing, are defined by standardized security policies.

The security policies supported by the WinCC OPC UA server are set using the server configuration file in "UaEndpoint" > "SecuritySetting".

EndpointConfiguration

Under "UaEndpoint" > "SecuritySetting" you will find the list of all "Security Profile" and "Message Security Mode" combinations that can be used by the server.

Security Profile	Message Security Mode	Description
http://opcfoundation.org/UA/SecurityPolicy#None	None	Unsecured communication
http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15	Sign or SignAndEncrypt	Secure communication, signed or encrypted and signed messages

2.6 Access via OPC - Open Connectivity

Security Profile	Message Security Mode	Description
http://opcfoundation.org/UA/SecurityPolicy#Basic256	Sign or SignAndEncrypt	Secure communication, signed or encrypted and signed messages
http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256 ¹⁾	Sign or SignAndEncrypt	Secure communication, signed or encrypted and signed messages
http://opcfoundation.org/UA/SecurityPolicy#Aes128_Sha256_RsaOaep ¹⁾	Sign or SignAndEncrypt	Secure communication, signed or encrypted and signed messages
http://opcfoundation.org/UA/SecurityPolicy#Aes256_Sha256_RsaPss ¹⁾	Sign or SignAndEncrypt	Secure communication, signed or encrypted and signed messages

1) Requirement for the Use of Security Policies "Basic256Sha256", "Aes128_Sha256_RsaOaep" and "Aes256_Sha256_RsaPss": Instance certificate with signature algorithm "Sha256" and minimum key length = 2048.

Note

Ensuring secure communication

Secure communication requires server certificates for server and client and a correctly configured certificate store.

Example of a configuration file with maximum functional scope

```
<UaEndpoint>
  <SerializerType>Binary</SerializerType>
  <!-- URL of the Endpoint
  <Url>opc.tcp://[NodeName]:4862</Url>
  <!-- Optional URL that allows to define a specific address the stack should use to bind to.
  <!-- It is up to an administrator to configure the actual exposed SecurityPolicies.
  <SecuritySetting>
    <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#None</SecurityPolicy>
    <MessageSecurityMode>None</MessageSecurityMode>
  </SecuritySetting>
  <!-- The SecurityPolicy Basic128Rsa15 is deprecated and is no longer considered secure.
  <!-- <SecuritySetting>
  <!-- The SecurityPolicy Basic256 is deprecated and is no longer considered secure.
  <!-- <SecuritySetting>
  <SecuritySetting>
    <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256</SecurityPolicy>
    <MessageSecurityMode>Sign</MessageSecurityMode>
    <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
  </SecuritySetting>
  <SecuritySetting>
    <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Aes128_Sha256_RsaOaep</SecurityPolicy>
    <MessageSecurityMode>Sign</MessageSecurityMode>
    <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
  </SecuritySetting>
  <SecuritySetting>
    <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Aes256_Sha256_RsaPss</SecurityPolicy>
    <MessageSecurityMode>Sign</MessageSecurityMode>
    <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
  </SecuritySetting>
  <!-- Flag indicating if the endpoint is provided in GetEndpoints and is therefore visible to a client. Default is true. -->
  <IsVisible>true</IsVisible>
  <!-- Flag indicating if the endpoint URL is provided as discovery URL. Default is true. -->
  <IsDiscoveryUrl>true</IsDiscoveryUrl>
  <!-- This option can be activated if certificates are used only for message security but not for application authentication.
  <AutomaticallyTrustAllClientCertificates>false</AutomaticallyTrustAllClientCertificates>
  <!-- For calculating the server signature, the server needs to append the client certificate to the client nonce.
  <CreateSignatureWithChain>false</CreateSignatureWithChain>
  <!-- Some of the OPC UA security checks are optional in OPC UA or cause interoperability issues with older OPC UA clients
  <SecurityCheckOverrides>
  <!-- Optional list of clients operating with an reverse connect from the server.-->
  <ReverseConnect>
  <!-- Optional list of alternative endpoint URLs known to the server.
  <AlternativeEndpointUrls>
  <!-- Windows based certificate store.
  <!-- Flag indicating if the endpoint is returned in discovery depending on EndpointUrl match. -->
  <ReturnOnlyOnEndpointUrlMatch>false</ReturnOnlyOnEndpointUrlMatch>
</UaEndpoint>
```

User identity

In addition to the security mechanisms of the communication level, the WinCC OPC UA server also supports user authentication for the client applications using the "UserIdentityTokens":

- Anonymous login
- Authentication with the username and password:
A valid combination of user name and password is specified when establishing communication.
The WinCC OPC UA server checks the combination in the user administration of the operating system.
- Authentication with the user certificate:
A valid combination of user certificate and private key is specified when establishing communication.
The WinCC OPC UA server checks the combination and allows communication if the user certificate is trusted.

2.6 Access via OPC - Open Connectivity

The UserIdentityTokens is set in the configuration file of the WinCC OPC UA server.

```
<UserIdentityTokens>
  <!--Enable anonymous login true/false-->
  <EnableAnonymous>true</EnableAnonymous>
  <!--Enable user/password login true/false-->
  <EnableUserPw>true</EnableUserPw>
  <!--Enable certificate based user login true/false-->
  <EnableCertificate>true</EnableCertificate>
  <!--Enable issued token based user login true/false-->
  <EnableIssuedToken>false</EnableIssuedToken>
  <!--The security policy to use when encrypting or signing the UserIdentityToken when it is passed to the server.
  <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256</SecurityPolicy>
  <!--Configuration for file based certificate store to handle user certificates.-->
  <DefaultUserCertificateStore>
    <!--Folder used to store rejected user certificates.-->
    <RejectedUserCertificatesDirectory>[ApplicationPath]/PKI/CA/rejected/certs</RejectedUserCertificatesDirectory>
    <!--Maximum number of certificates stored in the rejected directory.-->
    <RejectedUserCertificatesCount>100</RejectedUserCertificatesCount>
  </DefaultUserCertificateStore>
  <IssuedTokenSettings>
</UserIdentityTokens>
<!--User identity token configuration end-->
```

With this configuration, the WinCC OPC UA server supports both anonymous users and the Policy "UserName" and "Certificate".

Supported OPC UA services and profiles

OPC UA services

The WinCC OPC A&E Server supports the following described functionality.

The following table summarizes the functionality supported by the OPC UA server 1.0.10:

OPC UA Service Sets	Services	Comment
Discovery Service Set	FindServers GetEndpoints	-
Secure Channel Service Session Service Set	All	-
View Service Set	Browse BrowseNext RegisterNodes UnregisterNodes	Determination of the mapped WinCC data: Process values and archived data
Attribute Service Set	Read Write HistoryRead HistoryUpdate*)	only WinCC tags only WinCC tags Only archived tags Only archived tags
Subscription Service Set	CreateSubscription SetPublishingMode Publish RePublish DeleteSubscription	

OPC UA Service Sets	Services	Comment
MonitoredItem Service Set	CreateMonitoredItems SetMonitoringMode DeleteMonitoredItems	Only "Value" attribute of WinCC tags Event Notifier during access to WinCC messages
Method Service Set	Call	Acknowledge ConditionRefresh Configured C-VB scripts
*): With restrictions, see "Supported Write-Accesses (Page 260)"		

OPC UA profile and Conformance Units

The WinCC OPC UA server supports the following OPC UA profiles 1.04 without restrictions:

- 6.6.6 Base Server Behavior Facet
- 6.6.24 Standard Event Subscription Server Facet
- 6.6.26 A & C Base Condition Server Facet
- 6.6.39 Method Server Facet
- 6.6. 48 Historical Raw Data Server Facet
- 6.6.53 Historical Data Insert Server Facet
- 6.6.54 Historical Data Update Server Facet
- 6.6.56 Historical Data Delete Server Facet
- 6.6.143 UA-TCP UA-SC UA Binary
- 6.6.161 SecurityPolicy - None
- 6.6.162 SecurityPolicy - Basic128Rsa15
- 6.6.163 SecurityPolicy - Basic256 #
- 6.6.164 SecurityPolicy [A] - Aes128-Sha256-RsaOaep
- 6.5.165 SecurityPolicy [B] - Basic256Sha256
- 6.6.166 SecurityPolicy - Aes256-Sha256-RsaPss
- 6.6.167 User Token – Anonymous Facet
- 6.6.168 User Token – User Name Password Server Facet
- 6.6.169 User Token – X509 Certificate Server Facet

The WinCC OPC A&E Server supports the following OPC UA profiles shown in the following table, however with restrictions:

Profile	"Group"	Not supported "Conformance Unit"
6.6.2 Core Server Facet	Attribute Services	Attribute Write Index
6.6.16 Standard DataChange Subscription Server Facet	Monitored Item Services	DeadBand Filter
6.6.18 Enhanced DataChange Subscription Server Facet	Monitored Item Services	-

Profile	"Group"	Not supported "Conformance Unit"
6.6.21 Data Access Server Facet	Data Access	Data Access Analog Data Access Multistate Data Access PercentDeadBand Data Access Semantic Changes Data Access Two State
6.6.70 Standard UA Server Profile	Attribute Services	Attribute Write StatusCode & Timestamp

Name area of the WinCC OPC UA server

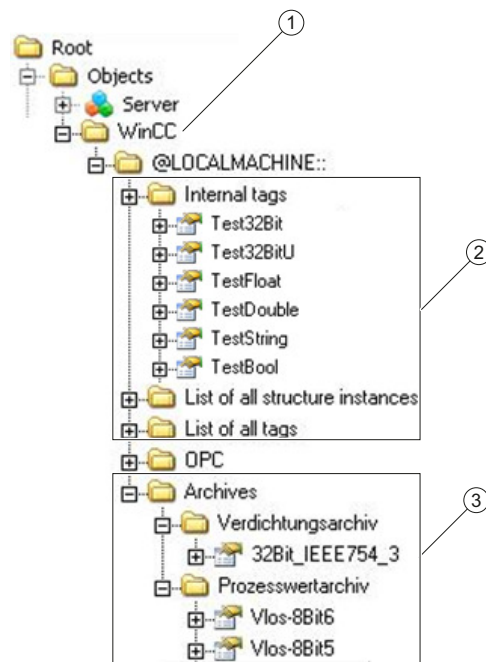
Introduction

The WinCC OPC UA server provides OPC UA clients with a hierarchical namespace and access to the following runtime data:

- Process values (WinCC tags and WinCC tag groups)
- Data logs including archive tags
- WinCC messages
- Configured C-VB scripts

The namespace of the WinCC OPC UA server is attached under the "Objects" default folder.

The following figure shows the namespace of the WinCC OPC UA server of an active WinCC project on the local PC ("@LOCALMACHINE::"):



- ① Start node of the specific namespace of WinCC.
- ② Display of the WinCC tags; the structure corresponds to the structure of the tags in WinCC.
- ③ Display of the data logs
- ④ Configured C/VB scripts

Display of the WinCC tags

Tag groups, communication drivers and connections are displayed by OPC UA objects of the "FolderType" type. Each of these folders has references of the "Organizes" type to the subordinate objects and tags.

Internal and external WinCC tags are displayed by OPC UA tags of the "DataItemType" type. If a WinCC tag is additionally archived, the displayed OPC UA tag has additionally a reference of the "HasHistoricalConfiguration" type for an archive configuration. The "Historizing" and "AccessLevel" attributes are set accordingly.

The following table shows the most important attributes of the OPC UA tags that represent a WinCC tag. You can find the complete list of attributes in the "OPC UA Part 3 - Address Space Model 1.04 Specification" document under "§5.6":

Attribute	Description	Comment
NodeId	Unique designation of the WinCC tag	-
BrowseName	WinCC tag name	-
DisplayName	WinCC tag name	-
Value	Tag value and status	-
DataType	OPC UA data type that corresponds to the WinCC tag type, for example: - Int32; signed 32-bit value - UInt32; unsigned 32-bit value	-

Attribute	Description	Comment
AccessLevel	"CurrentRead" / "CurrentWrite" "HistoryRead" / "HistoryWrite"	correspondingly to the WinCC tag configuration
ValueRank	Always "Scalar"	-

Write protection and read protection

You can protect the WinCC OPC UA server tags against access by clients.

In the Tag Management of the WinCC project, you activate the following setting in the property area of the tags in the "Options" group:

Property	Behavior in Runtime
OPC write protection	Clients only have read access to the tag value.
OPC read protection	Clients can neither read nor write the tag value.

Support for nested structures (UDT in UDT)

WinCC supports a hierarchical organization of tags, in which a tag can contain other tags as members and thus form a different structure.

You import such structure-in-structure tags via "Load from AS" or by browsing on the OPC server.

Display of the archive tags

Process values and compressed archives are displayed by OPC UA objects of the "FolderType" type. Each of these folders has references of the "Organizes" type to the related archive tags.

Archive tags from process value or compressed archives are displayed by OPC UA tags of the "BaseDateVariableType" type. An archive tag always has a reference of the "HasHistoricalConfiguration" type for an archive configuration.

The following table shows the most important attributes of the OPC UA tags that represent a WinCC archive tag. You can find the complete list of attributes in the "OPC UA Part 3 - Address Space Model 1.04 Specification" document under "§5.6":

Attribute	Description	Comment
NodeId	Unique designation of an archive tag	-
BrowseName	Name of the archive tag	-
DisplayName	Name of the archive tag	-
Description	Node description	-
Value	Does not exist	For an archive tag, this attribute can neither be read nor changed.
DataType	OPC UA data type that corresponds to the WinCC tag type, for example: - Double; 64-bit floating-point number - UInt32; unsigned 32-bit value	-
AccessLevel	"HistoryRead" / "HistoryWrite"	-
ValueRank	Always "Scalar"	-

Access to WinCC messages

The start node of the WinCC namespace is an Event Notifier with which the OPC UA clients can receive status changes for WinCC messages in Runtime via Subscriptions.

OPC UA Data Access

Internal and external WinCC tags are displayed by OPC UA tags of the "DataItemType" type. Other DataAccess tag types as "AnalogItem" or "DiscreteType" are not supported.

The WinCC OPC A&E Server supports the reading access on the OPC UA tag attributes as "DataType" or "AccessLevel". Writing access and subscriptions are only supported for the "Value" attribute.

OPC UA Historical Access

Introduction

"OPC Historical Access" enables access to archives and includes the "Historical Data" and "Historical Events" services. The WinCC OPC UA server supports only the "Historical Data" service.

The WinCC OPC UA Server offers the OPC clients access to the raw data of tag archives via "Services".

- HistoryRead (READRAW)
- HistoryUpdate (INSERTDATA, REPLACEDATA, UPDATEDATA, DELETE_RAW)

You can read and limitedly write with an OPC UA client the values of archive tags in the tag archives. Depending on the configuration of the tag archive, the archive tag can contain either raw data or already processed process values.

Characteristics of archive tags

A process tag in WinCC can be located in multiple tag archives. In this case the process tag is linked to one of the corresponding archive tags.

Properties / Properties of archive configurations

The following table shows the Properties of an OPC UA tag configuration of the "HistoricalConfigurationType" type: In the "Description" property, the archive tag comment configured in WinCC is displayed. You can find the complete list of properties in the "OPC UA Part 11 - Historical Access 1.04 Specification" document under "§5.2.2":

Property	Description / Value	Comment
Definition	WinCC process tag name	For a process value archive
Stepped	True	-

The following optional Properties are not supported:

- MaxTimeInterval
- MinTimeInterval

- ExceptionDeviation
- ExceptionDeviationFormat

Limitations for Service "HistoryUpdate"

You can use the Service "HistoryUpdate" only on process value archives.

The following table lists the functions supported by the WinCC OPC UA server: Which functions are supported depends on the configuration of the WinCC OPC UA server as well as the process value archive configuration. You will find additional information in the "OPC UA Part 11 - Historical Access 1.04 Specification" document under "§5.5":

Service	Function	Description
HistoryUpdate	INSERTDATA	Insert new archive values
	REPLACEDATA	Replace existing archive values
	UPDATEDATA	Replace of insert archive values
	DELETE_RAW	Delete archive values

OPC UA Alarm & Conditions

Introduction

As of WinCC 7.3, the OPC UA server provides access to the messages of the WinCC message system.

The OPC UA server forwards WinCC message status changes to OPC UA clients with WinCC-Event-Notifications via Subscriptions and Monitored Event Items but does not maintain a Condition instance in its name space.

The Event Notifier node to be used is the start node of the WinCC name area.

The UA client can filter the messages and define the list of message attributes returned.

The OPC UA server supports the "OPC UA Alarms & Conditions 1.04" specification.

The following section outlines the mapping of the WinCC message system to OPC UA. You can find additional information in the specification in "Part 9: Alarms and Conditions 1.04 Specification".

WinCC message system mapping to OPC UA event types

BaseEventType

"BaseEventType" is the basic type from which the OPC UA Event types "WinCCEventType" and "WinCCAlarmConditionType" are derived.

Note

Filter shows all WinCC messages

When you filter for "BaseEventType", you receive all WinCC messages.

WinCC messages are mapped to the following OPC UA event types:

WinCCEventType

This type is based on "BaseEventType" and maps "simple" WinCC messages with the following acknowledgment theory:

- "Message without status went out" is activated
- "Acknowledgment came in" is not activated

Examples of this type of message are starting and stopping motors.

WinCCAlarmConditionType

This type is based on "AlarmConditionType" and maps all messages which cannot be mapped on "WinCCEventType", for example, acknowledgeable messages and messages with the status "came in" and "went out".

At a message of the "WinCCAlarmConditionType" type, the event is linked to a condition. For example, WinCC generates a message as soon as a tag limit is violated. This message in OPC UA is equivalent to an Alarm Condition.

WinCC message attributes

The two Event types add WinCC-specific message attributes to the basic type. The attributes are mapped 1:1 as UA Event Properties and are described in more detail in the section "Attributes of the WinCC message system".

Message class and message type

The WinCC message system informs the user of disturbances and operating conditions in the process. A WinCC message always belongs to a specific message class and message type, which are specified in the "CLASSID", "TYPEID", "CLASSNAME" and "TYPENAME" attributes of the corresponding UA Events.

Priority

When configuring messages in the WinCC message system, you can configure a priority between "0" and "16". The OPC UA specification defines a value range of "1" to "1000" for the Severity. "1" stands for the lowest and "1000" for the highest Severity.

The values of the priority must therefore be suitably mapped to the OPC severity. In standard mapping, a priority of "0" is assigned to OPC-Severity "1" and a priority of "16" to OPC-Severity "1000". All other values are interpolated linearly between "0" and "1000".

OPC UA mapping rules

During the configuration of the WinCC message system, settings are made to determine which process events generate a message. This message is generally shown as an Event in OPC UA.

The following table shows the most important Properties of Events and how the WinCC message system provides the information.

OPC UA property	Mapping in the WinCC message system
For all event types:	
EventID	Unique message designation
EventType	Event type: Node ID of the WinCCAlarmConditionType node or WinCCEventType node
SourceNode	Not relevant
SourceName	Indicates the source of the message. Mapping is described in more detail below.
Message	Message text for the corresponding message number.
Time	Time of the event. The time stamp is given in UTC
Severity	Priority of the WinCC message
Only with WinCCAlarmConditionType:	
ConditionName	Set text that is output as well as the message. The text output depends on the mapping rule set: "Mode 1" and "Mode 2": Message number "Mode 3": Message class, for example "Process control message"
Quality	Returns the quality of the message
ConditionClassId	Node ID of the "ProcessConditionClassType" node
ConditionClassName	"ProcessConditionClassType"
Retain	"TRUE" with pending messages
NodeId	ConditionId: Designates a UA-Condition uniquely, for example an alarm. Required for acknowledgment, even if no Condition instances are supported
EnabledState	"TRUE" if the message has been enabled
ActiveState/Id	"TRUE" if the message has come in
AckedState/Id	"TRUE" if the message has been acknowledged
ClientUserId	Indicates the user that is logged on

Note

The following OPC UA Condition and Alarm Properties are not supported by the OPC UA server:

- BranchId
- LastSeverity
- InputNode
- ConfirmedState
- SuppressedState
- ShelvingState
- SuppressedOrShelved
- MaxTimeShelved

Message statuses / acknowledgment statuses

The following table shows WinCC message status mapping to the corresponding WinCCAlarmConditionType - Properties:

Message status	EnabledState/Id	ActiveState/Id	AckedState/Id
Locked message	FALSE	-	-
Enabled message	TRUE		
Received message	TRUE	TRUE	FALSE
Sent message with acknowledgment	TRUE	FALSE	TRUE
Sent message without acknowledgment	TRUE	FALSE	FALSE
Acknowledged messages (message pending)	TRUE	TRUE	TRUE
Acknowledged messages (message no longer pending)	TRUE	FALSE	TRUE
Received, acknowledged message	TRUE	TRUE	TRUE
Received, sent message with acknowledgment	TRUE	FALSE	TRUE
Received, sent message without acknowledgment	TRUE	FALSE	FALSE
Message acknowledged by the system (message pending)	TRUE	TRUE	TRUE
Message acknowledged by the system (message no longer pending)	TRUE	FALSE	TRUE
Emergency-acknowledged message (message pending)	TRUE	TRUE	TRUE
Emergency-acknowledged message (message no longer pending)	TRUE	FALSE	TRUE

Settings for mapping the WinCC message system

The configuration of the OPC UA server also applies to the OPC UA server as regards the mapping of the Properties "SourceName" and "Message" of a message.

- With OPC A&E server with hierarchical access:

SourceName	Indicates the source of a message. The Source has the format "<Server prefix>::Area\UserTextBlock 2". The server prefix of the local computer is "@LOCALMACHINE".
Message	Returns the message text of the corresponding message number

- With OPC A&E server without hierarchical access:

SourceName	Indicates the source of a message. The Source has the format "<Server prefix>::localhost:". The server prefix of the local computer is "@LOCALMACHINE".
Message	Returns the message text of the corresponding message number

Alarm groups

In WinCC 7.3, the WinCC alarm groups are not displayed in the name area.

Supported event methods

Acknowledgment

A WinCC message is acknowledged using the "Acknowledge" method of the "AcknowledgeableConditionType" node in the standard OPC UA info model.

Only messages of the "WinCCAlarmConditionType" type can be acknowledged.

ConditionRefresh

Messages still pending are established using the "ConditionRefresh" method of the "ConditionType" node in the standard OPC UA info model.

Filters

The OPC UA client can defined a filter for Monitored Event Items .

The following operators are, however, not supported by the OPC UA server:

- FilterOperator_Cast
- FilterOperator_BitwiseAnd
- FilterOperator_BitwiseOr
- FilterOperator_RelatedTo
- FilterOperator_InView

See also

Attributes of the WinCC message system (Page 305)

Attributes of the WinCC message system

Overview

The following table lists the configurable attributes of the WinCC message system. The attributes are mapped 1:1 as UA Event Properties .

WinCC message attribute	Meaning	Data type
CLASSNAME	Name of message class	String
TYPENAME	Name of message type	String
FORECOLOR	Foreground color for incoming, outgoing and acknowledged messages.	Int32
BACKCOLOR	Background color for incoming, outgoing and acknowledged messages.	Int32
FLASHCOLOR	Flash color	Int32
FLAGS	Indicates whether the message requires acknowledgment.	Int32
TEXT01...TEXT10	Content of user text block #1....#10	String
PROCESSVALUE01...PROCESSVALUE10	Content of process value block #1....#10	
STATETEXT	Status message	String
INFOTEXT	Information text for the message	String
LOOPINALARM	Indicates whether LoopInAlarm was configured	Int32
CLASSID	Message class ID	Int32
TYPEID	Message type ID	Int32
MODIFYSTATE	Value of message status tag	Int32
AGNR	Outputs the number of the automation system that generated the message	Int16
CPUNR	Outputs the number of the CPU that generated the message	Int16
DURATION	Outputs the time period between the incoming state, outgoing state and acknowledgment of a message	Int32
COUNTER	Number of messages after the start of runtime	Int32
QUITSTATETEXT	Indicates whether the message has been acknowledged	String
QUITCOUNT	Number of open, unacknowledged messages	Int32
PARAMETER	Configuration parameter of the message	Int32
BLOCKINFO	Current content of the message block	String
ALARMCOUNT	Number of pending messages	Int32
LOCKCOUNT	Number of locked messages	Int32
PRIORITY	Priority of the message	Int32
APPLICATION	Outputs the application which triggered the message	String
COMPUTER	Outputs the name of the computer which processed the message	String

WinCC message attribute	Meaning	Data type
USER	Outputs the name of the user who processed the message	String
COMMENT	Message comment	String
HIDDEN_COUNT	Number of hidden messages	Int32
OS_HIDDEN	Indicates that the message is hidden	Boolean
OS_EVENTID	WinCC message number	Int32
BIG_COUNTER	Number of messages after the start of Runtime	Int64

Configuration for special WinCC message attributes

Mapping of the WinCC message system on OPC is configured via the "CcAeProvider.ini" file. The configuration file contains three different mapping modes. "Mapping Mode 1" is activated by default. In "Mapping Mode 3" the special message attributes BIG_COUNTER, HIDDEN_COUNT, OS_EVENTID and OS_HIDDEN are additionally active.

Proceed as follows to activate "Mapping Mode 3":

1. Use a text editor to open the file "CcAeProvider.ini" in the WinCC installation path in the folder "OPC\AlarmEvent\bin".
2. In the section "Mapping Mode 3", remove the comment markings at the beginning of the lines "[OpcMapping]", "OpcSource ..." and "OpcMessage ...":

```

;=====
; Mapping Mode 3 "OPC Mapping"
;=====
[OpcMapping]
OpcSource = TEXT02
; EVENTID
; TEXT01...10
; INFOTEXT
OpcMessage = TEXT01
; TEXT01...10
; STATETEXT
; INFOTEXT
; COMMENT

```

3. If required, modify the mapping of the message attributes in the section.
4. Restart Runtime.

The "Mapping Mode 3" of the WinCC OPC UA server with its special message attributes is activated.

See also

OPC UA Alarm & Conditions (Page 300)

Configuration of the WinCC OPC UA server

Configuration file of the WinCC OPC UA Server

Introduction

The WinCC OPC UA server is configured using the configuration file "OPCUAServerWinCC.xml".

The configuration file is broken down into multiple sections. This section describes the layout of the configuration file.

The chapter "How to configure the OPC UA server (Page 311)" describes how you configure the WinCC OPC UA server.

Path of the configuration file

Two configuration files "OPCUAServerWinCC.xml" exist for the WinCC OPC UA server:

Configuration file	Storage path
Server-specific configuration file	<WinCC installation path>\opc\UAServer\
Project-specific configuration file	<WinCC project folder>\OPC\UAServer

Editing the configuration file

You require the following authorizations to carry out changes in the configuration files:

Server-specific configuration file	Windows Administrator rights
Project-specific configuration file	The user must be a member of the "SIMATIC HMI" user group.

Note

Same parameters: Priority of the files

Some parameters are contained in both configuration files.

If the parameters do not match, the settings of the project-specific configuration file have a higher priority.

Structure: Section <UaEndpoint>

You can find additional information on the URL under "Security concept of OPC UA (Page 288)".

<UaEndpoint>	
<Url> <...></...> </Url>	Configuration of the URL of the WinCC OPC UA server.

2.6 Access via OPC - Open Connectivity

<pre> <SecuritySetting> <SecurityPolicy> <...></...> </SecurityPolicy> <MessageSecurityMode> <...></...> </MessageSecurityMode> ... </SecuritySetting> </pre>	Configuration of the supported security policies Use the "none" setting only for test and diagnostics purposes
<pre> <DefaultApplicationCertificateStore> <TrustedCertificateStore> <TrustedCertificates> <...> </pre>	Revision of the default certificate configuration according to OPC UA Specification / Part 6. (optional) These parameters are only contained in the server-specific configuration file.
<pre> </UaEndpoint> </pre>	

Example: OPC UA application security

```

<UaEndpoint>
  <SerializerType>Binary</SerializerType>
  <!-- URL of the Endpoint
  <Url>opc.tcp://[NodeName]:4862</Url>
  <!-- Optional URL that allows to define a specific address the stack should use to bind to.
  <!-- It is up to an administrator to configure the actual exposed SecurityPolicies.
  <SecuritySetting>
    <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#None</SecurityPolicy>
    <MessageSecurityMode>None</MessageSecurityMode>
  </SecuritySetting>
  <!-- The SecurityPolicy Basic128Rsa15 is deprecated and is no longer considered secure.
  <!-- <SecuritySetting>
  <!-- The SecurityPolicy Basic256 is deprecated and is no longer considered secure.
  <!-- <SecuritySetting>
  <SecuritySetting>
    <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256</SecurityPolicy>
    <MessageSecurityMode>Sign</MessageSecurityMode>
    <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
  </SecuritySetting>
  <SecuritySetting>
    <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Aes128_Sha256_RsaOaep</SecurityPolicy>
    <MessageSecurityMode>Sign</MessageSecurityMode>
    <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
  </SecuritySetting>
  <SecuritySetting>
    <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Aes256_Sha256_RsaPss</SecurityPolicy>
    <MessageSecurityMode>Sign</MessageSecurityMode>
    <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
  </SecuritySetting>
  <!-- Flag indicating if the endpoint is provided in GetEndpoints and is therefore visible to a client. Default is true. -->
  <IsVisible>true</IsVisible>
  <!-- Flag indicating if the endpoint URL is provided as discovery URL. Default is true. -->
  <IsDiscoveryUrl>true</IsDiscoveryUrl>
  <!-- This option can be activated if certificates are used only for message security but not for application authentication.
  <AutomaticallyTrustAllClientCertificates>false</AutomaticallyTrustAllClientCertificates>
  <!-- For calculating the server signature, the server needs to append the client certificate to the client nonce.
  <CreateSignatureWithChain>false</CreateSignatureWithChain>
  <!-- Some of the OPC UA security checks are optional in OPC UA or cause interoperability issues with older OPC UA clients
  <SecurityCheckOverrides>
  <!-- Optional list of clients operating with an reverse connect from the server.-->
  <ReverseConnect>
  <!-- Optional list of alternative endpoint URLs known to the server.
  <AlternativeEndpointUrls>
  <!-- Windows based certificate store.
  <!-- Flag indicating if the endpoint is returned in discovery depending on EndpointUrl match. -->
  <ReturnOnlyOnEndpointUrlMatch>false</ReturnOnlyOnEndpointUrlMatch>
</UaEndpoint>

```

Structure: Section <UaServerConfig>

Server-specific parameters are set in this section.

For more information about message security modes, refer to "Security concept of OPC UA (Page 288)".

<UaServerConfig>	
<UserIdentityTokens> <...></...> </UserIdentityTokens>	Configuration of user identification Use the "Anonymous" setting only for test and diagnostics purposes
<FastInsert> <Users> <...></...> </Users> <Clients> <...></...> </Clients> </FastInsert>	Configuration of the optimized WinCC archive write access
</UaServerConfig>	

Structure: Section <ServerCertificate>

You specify the certificate parameters for the WinCC OPC UA server under the <ServerCertificate> heading in the <UaServerConfig> section.

These parameters are only contained in the server-specific configuration file.

You can find additional information on the instance certificates under "Security concept of OPC UA (Page 288)".

<ServerCertificate>	
<CertificateSettings>	
<OrganizationUnit>...</...> <Organization>...</...> <Country>...</...>	Descriptive elements The parameters can be changed and have no effect on the function of the applications.
<KeyLength>...</...>	Length of the private key with which the certificate is created The length depends on the CertificateType. • 1024: Minimum length for secure communication via OPC UA • 2048: Minimum length when Sha256 is used ¹⁾
<CertificateType>...</...>	CertificateType, which is used to sign the certificate • Possible values: Sha1, Sha224, Sha256, Sha384, Sha512 • Usual values: Sha1, Sha256 • Default value: Sha256 with key length 2048 ¹⁾

2.6 Access via OPC - Open Connectivity

<code><YearsValidFor>...</...></code>	Validity period of the certificate in months After the specified time has expired, the server can no longer be operated with this certificate. Default value: 5
<code></CertificateSettings></code> <code></ServerCertificate></code>	

1) To establish a secure connection with the Security Policy "Basic256Sha256", the server as well as the OPC UA client need a certificate with the following values:

- KeyLength: At least 2048
- CertificateType: Sha256

Example: Parameters for the control of the certificate

```

<ServerCertificate>
  <!--File based server certificate store used with OpenSSL
  [ApplicationPath] can be used as placeholder for the application path.-->
  <OpenSSLStore>

  <!--Windows based server certificate store.

  <!--SecurityCheckOverrides for the own server certificate. -->
  <SecurityCheckOverrides>

  <!--Enable server certificate creation if certificate is not available; true/false-->
  <GenerateCertificate>true</GenerateCertificate>
  <!--Settings for a certificate that is generated by the server-->
  <CertificateSettings>
    <!--Name of the application - [ServerName] is the default value to use the configured server name-->
    <CommonName>[ServerName]</CommonName>
    <!--DomainComponent - [NodeName] is the default value to use the hostname of the machine -->
    <DomainComponent>[NodeName]</DomainComponent>
    <!--Name of the organization using the OPC UA server-->
    <Organization>Siemens AG</Organization>
    <!--Name of the organization unit using the OPC UA server-->
    <OrganizationUnit>DI FA HMI</OrganizationUnit>
    <!--Name of the location where the OPC UA server is running -->
    <!--<Locality>LocationName</Locality> -->
    <!--State where the OPC UA server is running -->
    <State>BW</State>
    <!--Two letter code for country where the OPC UA server is running, e.g. DE or US-->
    <Country>DE</Country>
    <!--The number of years the certificate is valid for. The maximum accepted number is 20,
    <YearsValidFor>5</YearsValidFor>
    <!--Key length of the certificate to create. Valid values are 1024, 2048 for RsaMin and 2048, 3072 and 4096 for RsaSha256-->
    <KeyLength>2048</KeyLength>
    <!--Defines the algorithm used to sign the certificate. Valid values are RsaMin and RsaSha256.
    <CertificateType>RsaSha256</CertificateType>
    <!-- An application instance certificate needs to provide one or more DNSNames and/or IPAddresses at which the Endpoint can be reached.
    This information is added to the SubjectAlternativeName of the certificate.
    If this parameter is not set, the [NodeName] is used by default.-->
    <!-- Example for a list with 2 DNSNames plus 2 IPAddresses
    <IPAddress>2a00:1158:400:407:0:0:1b2</IPAddress>
    <IPAddress>213.95.4.190</IPAddress>
    <DNSName>demo.sagautomation.com</DNSName>
    <DNSName>[NodeName]</DNSName> -->
    <DNSName>[NodeName]</DNSName>
  </CertificateSettings>
</ServerCertificate>

```

Changing the storage path of the server certificate

If required, the storage location for the certificate of the WinCC OPC UA server can be adapted by the plant administration.

Example: Storage path of the server certificate

```

<ServerCertificate>
  <!--File based server certificate store used with OpenSSL
        [ApplicationPath] can be used as placeholder for the application path.-->
  <OpenSSLStore>
    <ServerCertificate>[ApplicationPath]/PKI/CA/certs/</ServerCertificate>
    <ServerPrivateKey>[ApplicationPath]/PKI/CA/private/</ServerPrivateKey>
  </OpenSSLStore>

  <!--Windows based server certificate store.
        - <StoreLocation> location of the store. Valid values are LocalMachine and CurrentUser
        - <StoreName> is the name of the certificate store in the local computer
        - <ServerCertificateThumbprint> is the thumbprint of the server certificate used to load from store
  <WindowsStore>
    <StoreLocation>LocalMachine</StoreLocation>
    <StoreName>UA Applications</StoreName>
    <ServerCertificateThumbprint></ServerCertificateThumbprint>
  </WindowsStore> -->

  <!--SecurityCheckOverrides for the own server certificate. -->
  <SecurityCheckOverrides>

  <!--Enable server certificate creation if certificate is not available; true/false-->
  <GenerateCertificate>true</GenerateCertificate>
  <!--Settings for a certificate that is generated by the server-->
  <CertificateSettings>
</ServerCertificate>

```

Creating new server certificates

You need administrator rights to create new certificates on the OPC UA server.

1. Create a backup.
2. Delete the existing certificates and the associated private keys in the corresponding folders.
3. In the configuration file, update the certificate parameters and save the XML file.
4. Open the DOS window "cmd.exe" in Windows with administrator rights.
5. To create the certificates, go to the installation path of the OPC UA application.
6. Enter the following call:
 - OpcUaServerWinCC.exe /CreateCertificate

The new certificates and private keys are created in the storage paths.

How to configure the OPC UA server**Requirement**

A WinCC project has been created.

Opening the configuration file

1. Open the Windows Explorer.
2. Navigate to the directory "<WinCC project folder>\OPC\UAServer".
3. Open the configuration file "OPCUAServerWinCC.xml".
For more information, refer to "Configuration file of the WinCC OPC UA Server (Page 307)"

Changing the port number of the WinCC OPC UA server

1. If necessary, change the port number 4862 at <Url>.
Do not use a port number that is already assigned to another application.
The parameter [NodeName] is the placeholder for the computer name and is determined during runtime.
Example:

```
- <Url>
  opc.tcp://[NodeName]:4862
</Url>
```

Specifying security settings

1. Define the security settings for communication.
For more information, refer to "Security concept of OPC UA (Page 288)"
2. Configure the corresponding "Message security modes" under <UaEndpoint>.
3. To deactivate a setting, delete the entire entry <SecuritySetting>... </SecuritySetting>..

Example:

- <SecuritySetting>
 <SecurityPolicy>http://opcfoundation.org/UA/
 SecurityPolicy#None</SecurityPolicy>
 <MessageSecurityMode>None</MessageSecurityMode>
</SecuritySetting>

Note

Unsecured communication between client and server

Use the "none" setting only for test and diagnostics purposes.

For secure communication between client and server during productive operation, use at least the following settings:

- SecurityPolicy: Basic128Rsa15
 Message Security Mode: Sign
-

Specifying user identification

1. Specify the user identification for the establishment of the connection under `<UserIdentityTokens>`.
For more information, refer to "Security concept of OPC UA (Page 288)"
2. To activate or deactivate a setting, set the value accordingly to "True"/"False"

Example:

- ```
<UserIdentityTokens>
 <EnableAnonymous>true</EnableAnonymous>
 <EnableUserPw>true</EnableUserPw>
 <EnableCertificate>true</EnableCertificate>
</UserIdentityTokens>
```

## Configuring optimized WinCC archive write access

If necessary, configure optimized WinCC archive write access under `<FastInsert>`.

- Set "true" to activate the optimized write access to WinCC archives for all OPC UA clients.
- Set "false" to set optimized WinCC archive write access for specific Windows users or OPC UA clients.

You specify the Windows users under `<Users>`.

You specify the OPC UA clients under `<Clients>`. Use the "Common Name" that is entered in the client certificate as `ClientName`.

Example:

```
- <EnabledByDefault>false</EnabledByDefault>
 <Users>
 <User>domain\user1</User>
 </Users>
 <Clients>
 <Client>ClientName1</Client>
 </Clients>
```

## UaExpert

### General information about UaExpert

#### Introduction

UaExpert is a free OPC UA client from Unified Automation (<https://www.unified-automation.com/products/development-tools/uaexpert.html>) for test purposes.

UaExpert has the following plugins:

- OPC UA Data Access View
- OPC UA Alarms & Conditions View
- OPC UA Historical Trend View
- OPC UA Performance Plugin

## 2.6 Access via OPC - Open Connectivity

- Image Viewer
- Server Diagnostics View
- Simple Datalogger CSV Plugin
- GDS Push-Model Plugin

UaExpert is available for Windows and Linux.

### Principle of operation

The OPC UA client "UaExpert" communicates directly with the OPC UA Server.

The client and the server are connected via Ethernet and communicate via OPC UA using TCP/IP.

#### Requirement

To approve the UaExpert for read and write access to certain PLC tags, these tags must be enabled for OPC UA.

### See also

Principle of operation the WinCC OPC UA Server (Page 287)

### Overview of the supported OPC UA functionalities

The OPC UA client "UaExpert" supports the following functionalities of OPC UA:

- Browse
- Read/Write
- Subscription
- Methods
- Historical Access
- Alarms and Conditions

### Browse and Read/Write

You can search the respective nodes and tags in the "Address Space" view of the UaExpert.

The functions and values of the tags are displayed in the "Attributes" view as soon as you click the respective tag.

To obtain the current value, click "Refresh". In the process you trigger the function "Read".

### Subscription

UaExpert can subscribe to all nodes that have the attribute "EventNotifier".

These nodes can be subscribed to in a subscription to receive their events.

Follow these steps to create a subscription in UaExpert:

1. Drag-and-drop to move the individual variables to the "Data Access View" view.  
The UaExpert then automatically creates a subscription to the tag.
2. In the "Data Access View" view, open the window "Monitored Item Settings" by means of the shortcut menu of the subscribed tag.
3. Configure the following settings:
  - Sampling Intervall
  - Queue Size
  - Discard Oldset
4. Activate the "Publishing Mode" via the shortcut menu of the subscribed tag.
5. To open the shortcut menu of the subscribed tag, open the "Subscription Settings" window and set the settings for the subscription.

## Methods

The available methods of the OPC UA server are displayed in the "Address Space" view with .

Proceed as follows to call a method in the UaExpert:

1. Right-click the respective method and select "Call".
2. In the pop-up window specify the Input Arguments and click "Call".

The method is carried out. The Output Arguments are displayed.

## Historical Access

In the "Attributes" view of the selected tag you can read out whether historical data are collected for the tag and whether the OPC UA client can access the data.

You can query the data cyclically or once in the "History Trend View" view.

The "History Trend View" view is split up into two areas:

- "Configuration":
  - Select different display colors if several data sources exist.
  - If you select Single Update, the displayed data is defined by the time of the start and end.
  - If you select Cyclic Update, the data are called in the configurable interval.
- "History Data": The data are displayed as a diagram.

## Alarms and Conditions

You can drag the nodes that have the attribute "EventNotifier" for the SubscribeToEvents state into the "Event View" view to monitor and edit the current events and alarms in this view.

The "Event View" view is divided into three areas:

- "Configuration": You can select the desired event fields from the list.
- "Events"/ "Alarms": You can toggle between the Events and Alarms view to watch the continuous list of incoming events and the status of pending alarms.
- "Details": You can view the details of the selected events.

## See also

Supported OPC UA services and profiles (Page 294)

## How to read the data with UaExpert

### Requirement

- UaExpert is installed on the WinCC machine.
- OPC UA Server can be reached on the WinCC machine.

### Procedure

To read the data via the OPC UA Client "UaExpert", proceed as follows:

1. Start the UaExpert and click "Add Server".
2. In the pop-up window double-click "< Double click to Add Server... >" in the list area "Custom Discovery".
3. Enter the URL and the port of the OPC UA server (opc.tcp://[IP-Adresse]:4840) and click "OK".
4. Select an end point of the OPC UA server to which you want to establish a connection.
5. Select the authentication method.
6. Set the "Connect Automatically" check box and then confirm with "OK".
7. Accept the server certificate by setting the check box "Accept the server certificate temporarily for this session".  
The certificate is not stored in the trusted list of UaExpert.  
To permanently add the certificate to the trusted list, you must select "Trust Server Certificate".
8. Then click "Continue".  
You are connected to the OPC UA server of the WinCC.
9. In the "Address Space" of the OPC UA server navigate via "Root > Objects > ServerInterfaces" to the selected tags.  
Here you only see the OPC UA nodes that you have configured in the project engineering of the OPC UA server interface.
10. Drag-and-drop the selected tags into the area "Data Access View".  
In the area "Data Access View" you can observe the changing data or edit the data.

### 2.6.2.10 Diagnostics

#### Trace file

All servers offer the possibility to activate the output of diagnostic data for test purposes and for troubleshooting.

The data of a server is written to a trace file.

#### Setting

You specify the output of diagnostic data in the configuration file of the respective server.

For more information, refer to the SIMATIC Customer Support.

## 2.7 Examples for Access Using OLE DB Provider

### 2.7.1 Examples for Access Using OLE DB Provider

#### Overview

The following examples demonstrate different ways of displaying and analyzing archive data.

#### See also

Example: Configuring the Access to Archive Data Using VB (Page 318)

Example: Configuring Access to Archive Data Using DataConnector Wizard (Page 320)

Example: Reading Process Value Archive With WinCC OLE DB Provider and Visual Basic 6 (Page 326)

Example: Reading Process Value Archive With WinCC OLE DB Provider and Visual Basic.NET (Page 332)

Example: Reading Message Archive Data with the WinCC OLE DB Provider and Visual Basic 6 (Page 336)

Example: Reading Message Archive Data With WinCC OLE DB Provider and Visual Basic.NET (Page 340)

### 2.7.2 Example: Configuring the Access to Archive Data Using VB

#### Introduction

The following example shows how to configure a tabular display with Microsoft controls. You may also use other controls or program your own.

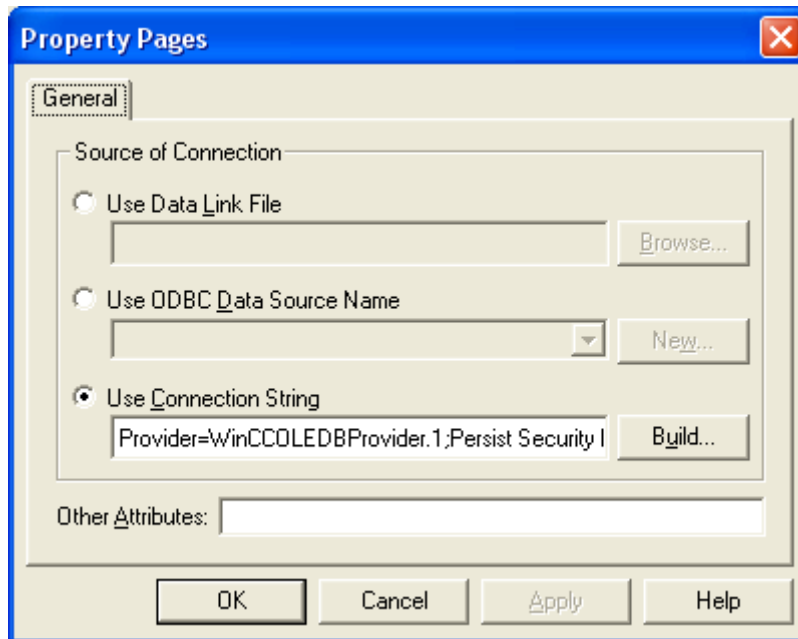
#### Requirements

Archive files are local on the computer and must be connected to the SQL server, e.g., using the WinCC Archive Connector.

#### Procedure

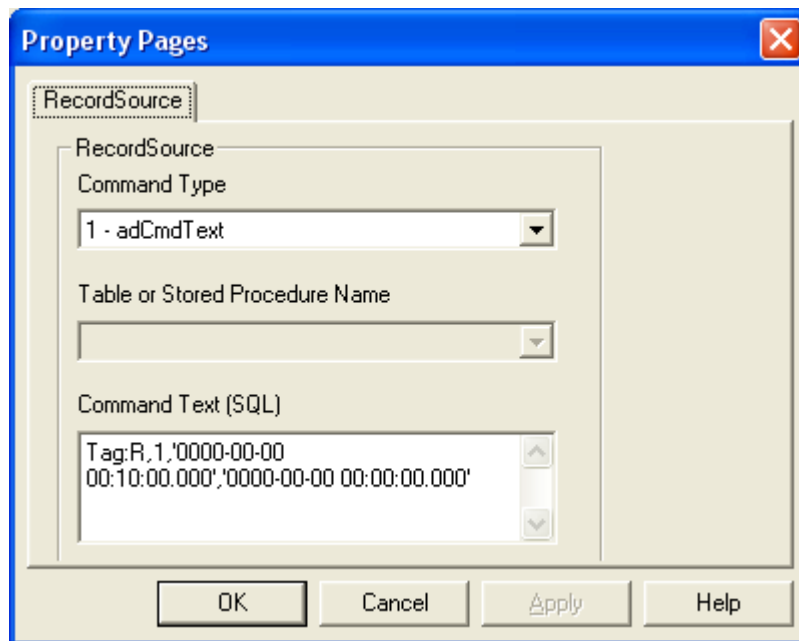
1. In Visual Basic Editor, create a new form that you want to use for displaying the archive data.
2. In Visual Basic Editor, select the menu commands "Project > Components".
3. Activate the controls that you want to use, e.g. an "MS Data Grid Control" and an "MS ADO Data Control".  
The related symbols are displayed in the toolbox.

4. In your form, create an "MS Data Grid Control" for tabular display of archive data, and an "MS ADO Data Control" for navigation within the tabular display.
5. Mark the MS Data Grid Control and select the entry "Adoc1" in the property window under "DataSource" in order to link the two controls.
6. Mark the MS ADO Data Control and click the button "..." in the Property window under "Connection String".  
This opens the "Property pages" dialog.



7. Click on the "Create..." button next to the entry "Use Connection Character Sequence".  
The "Data Link Properties" dialog opens.
8. In the "Provider" tab, select "WinCC OLE DB Provider for Archives" and click on "Next".
9. In the "Connection" tab, enter the data source in the "DataSource" box: <computer name>\WinCC.  
Test the connection by clicking on the button "Test Connection".  
Select the Extended tab. After that, switch to the "All" tab without further changes. This step is necessary to correctly set all parameters for the subsequently created connection character set.
10. In the "All" tab, enter the name of the WinCC database in the "Catalog" box. The database name can be found in the SQL Enterprise Manager at "SQL Server Group" > "<Computer Name>\WinCC" > "Databases" > "<Database name\_R>".  
If the project is active, only use database names that end with "R".  
If you have connected exported WinCC archives to the SQL Server via the WinCC Archive Connector, use the symbolic name of the database or export directory.  
Confirm your settings with "OK".

11. Mark the MS ADO Data Control and click the button "..." in the Property window under "RecordSource". This opens the "Property pages" dialog. Select the setting "1 - adCmdText" for the command type and enter a valid statement such as TAG:R,1,'0000-00-00 00:10:00.000','0000-00-00 00:00:00.000' in the "Command text (SQL)" box.



To access process values of the following tag types, replace the "TAG:R" schema with "TAG\_EX:R":

- Text tag, 8-bit character set / 16-bit character set
- Floating-point number 64-bit IEEE 754

12. Confirm your entries with "OK" and start Visual Basic Runtime.

### 2.7.3 Example: Configuring Access to Archive Data Using DataConnector Wizard

#### Introduction

The following example shows how to configure a tabular display of process values using the DataConnector Wizard in WinCC Graphics Designer.

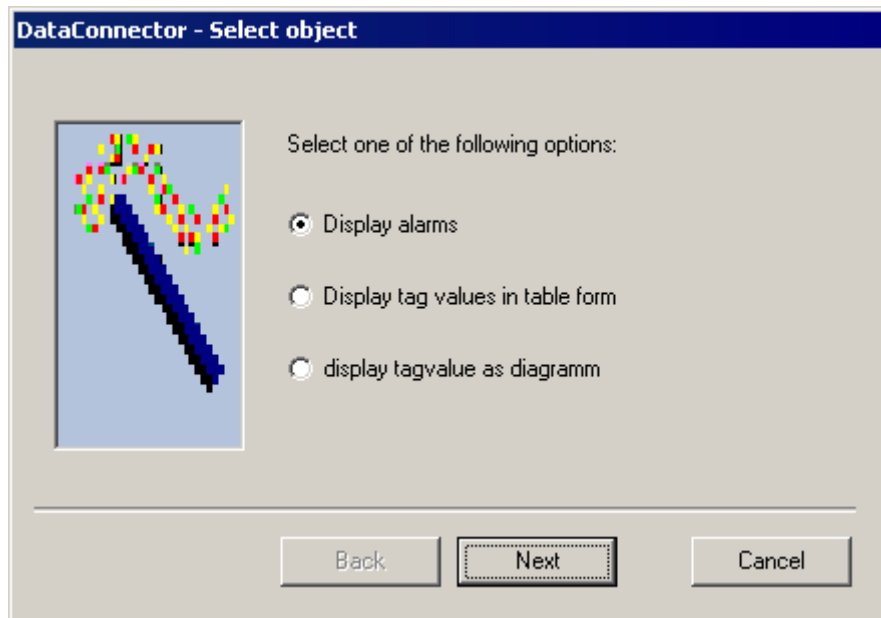
Alternatively, you may also use the DataConnector Wizard to configure the display of messages or graphical display of process values.

#### Requirements

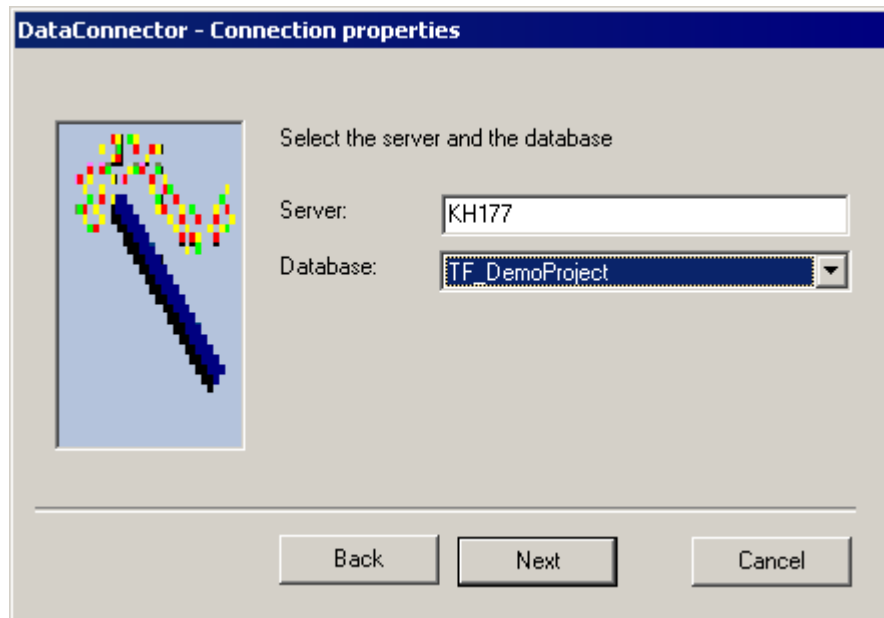
- WinCC Basic system and Connectivity Pack are installed.
- Archive files are connected to the desired SQL server, e.g., using WinCC Archive Connector.

## Procedure

1. Open Graphics Designer and select the entry "Create New Picture" in the "DataConnector" menu. A new process picture opens and the dialog "DataConnector - Select Object" is displayed.
2. For this example, select the option "Display Tag Values in Table Form" and then click the "Continue" button.

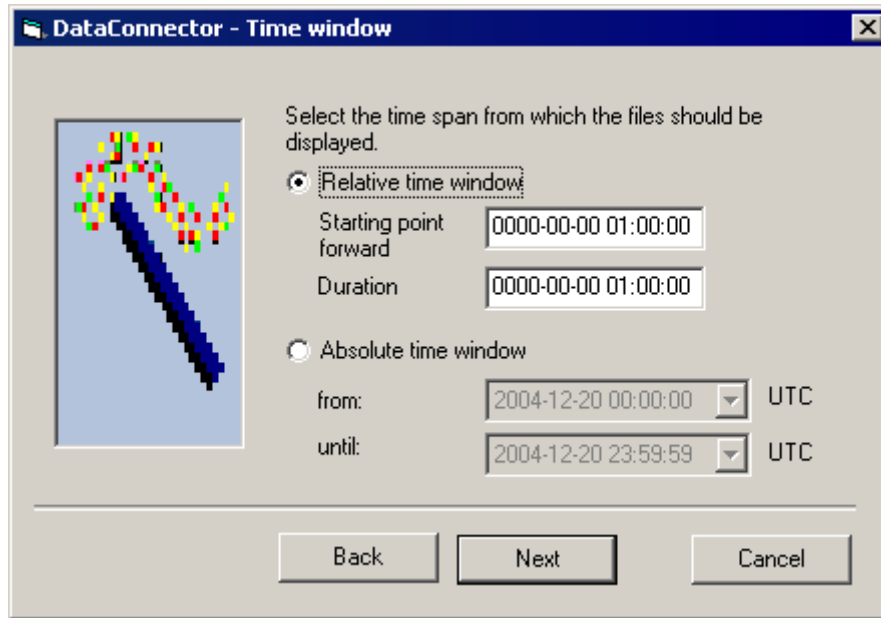


3. The dialog "DataConnector - Connection Properties" opens.  
Enter the name of the server in the "Server" field that contains the desired interlinked databases. The name of the local computer is prescribed.  
Select the desired database in the "Database" field. The currently connected databases of the selected server are available.



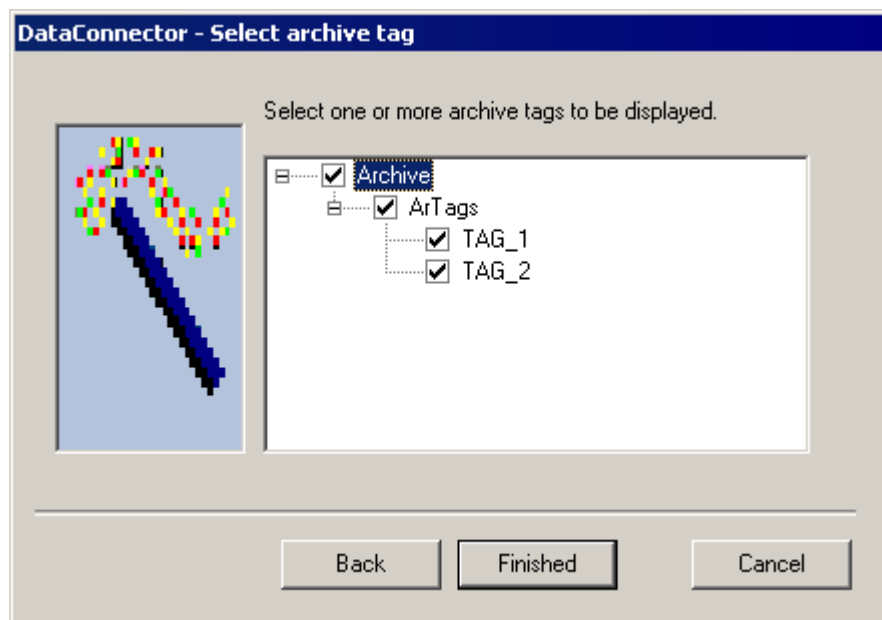
Click "Continue".

4. The dialog "DataConnector - Time window" will open.  
Select the desired time frame from which the data should be displayed, e.g. "Relative time window". Prescribed is a time window for the previous hour. Change the specifications as needed, e.g., in the field "Starting point forward" to the value "0000-00-00 01:00:00" and in the field "Duration" to the value "0000-00-00 01:00:00" in order to display the previous hour. The value in the "Duration" field cannot be larger than the value in field "Starting point forward".



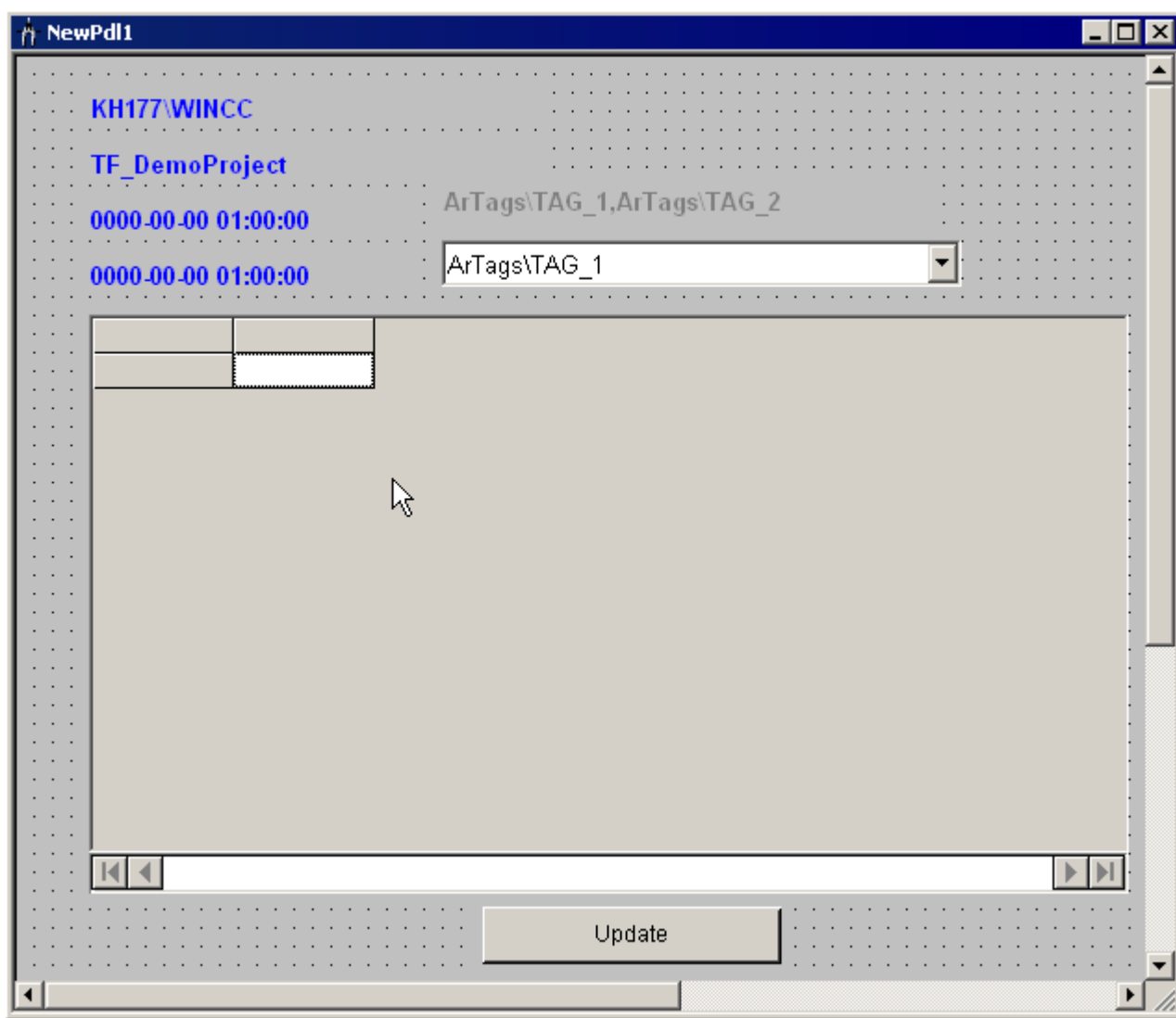
Click "Continue".

5. The dialog "DataConnector - Select Archive Tag" opens.  
Select at least one archive tag.



Click on the "Finish" button.

6. The DataConnector Wizard will insert several elements into the opened process picture.  
The selected server, the database and the time frame are displayed in the static text fields at the top.  
Next to them there will be a text with the selected archive tags and the selection field for the archive tag.  
As per the selection "Display tag values as tables", a data grid control, an ADO data control and a button are inserted below them.  
Save the process screen.  
In order to change the configured values, open this process picture and select the entry "Modify existing connection" in the "DataConnector" menu. The Wizard will restart and you may change the configured values.



7. Start WinCC Runtime and open this process picture with the database query. The query will be initially executed directly upon opening of the process picture.  
In Runtime, the data found will be displayed in tabular form in Data Grid Control, and you may navigate within the table using ADO Data Control.  
With more than one configured archive tags, the tag, whose values are to be displayed can be chosen in the selection field.

## 2.7 Examples for Access Using OLE DB Provider

The displayed data can be updated via the "Update" button, for example, if the most recent hour was indicated as a relative time frame.

---

### Note

#### Archive query using data connector control on the Web client

If an archive query is to be performed on a WebNavigator client using the DataConnector control in a process picture, the Connectivity Pack client must also be installed on the Web client.

---

### See also

Querying Alarm Message Archives (Page 192)

Querying Process Value Archives (Page 184)

## 2.7.4 Examples: Analyzing Process Value Archives

### 2.7.4.1 Example: Reading Process Value Archive With WinCC OLE DB Provider and Visual Basic 6

#### Introduction

In this example, the values of the last 10 minutes of the tag "Tag\_1" are read from the local WinCC RT database.

The data is displayed in a ListView with a time stamp, value and quality code. The output of values is limited to 100 (constant NMAX = 100).

The example does not include error processing.

#### Procedure

1. Create a WinCC tag named 'Tag\_1'.
2. Create a process value archive named "ArTags".  
Connect the WinCC tag "Tag\_1" with the process value archive.
3. Create a Visual Basic project.  
Connect a MS Windows Common Controls 6.0 ListView control with the name "ListView1".  
The columns in the ListView are created by the script.  
Set the property "View" to the option "3 - lwReport" on the ListView control.
4. Create a "CommandButton".  
Copy in the script from the section "Example Script" below.

5. Adapt the script to your project:
  - Change the name of the WinCC Runtime database 'CC\_OpConPac\_04\_10\_01\_10\_36\_36R'.  
The database name can be found in the SQL Enterprise Manager at "SQL Server Group" > "<Computer Name>\WinCC" > "Databases" > "<Database name\_R>".
  - If necessary, change the name of the schema used.  
To access process values of the following tag types, use the "TAG\_EX" schema:
    - Text tag, 8-bit character set / 16-bit character set
    - Floating-point number 64-bit IEEE 754
6. Activate WinCC Runtime and start the VB application.
7. Click on the "CommandButton".

## Example Script

---

### Note

#### Improving performance

To improve the performance, note the following information:

- Replace the "Data Source=.\WinCC" instruction with the "Data Source=<ComputerName>\WinCC" instruction.
  - For the query, use "ValueID" instead of "<ArchiveName>\<TagName>".  
In the example script, the expression 'ArTags\Tag\_1' under point 1.2 would have to be replaced by a "ValueID".
-

---

2.7 Examples for Access Using OLE DB Provider

```
Option Explicit
Const NMAX = 100
Private Sub Command1_Click()
Dim sPro As String
Dim sDsn As String
Dim sSer As String
Dim sTagSchema As String
Dim sCon As String
Dim sSql As String
Dim conn As Object
Dim oRs As Object
Dim oCom As Object

' 1.1 Make connection string for ADODB
sPro = "Provider=WinCCOLEDBProvider.1;"
sDsn = "Catalog=CC_Test_19_05_21_10_23_19R;"
sSer = "Data Source=.\WinCC"
sCon = sPro + sDsn + sSer

' 1.2 Define the Tag Schema Name (TAG or TAG_EX)
sTagSchema = "TAG"

' 1.3 Define command text in sSql (relative time)
sSql = sTagSchema + ":R,'ArTags\Tag_1','0000-00-00
00:10:00.000','0000-00-00 00:00:00.000'"

MsgBox "Open with:" & vbCrLf & sCon & vbCrLf & sSql & vbCrLf

' 2.1 Make connection
Set conn = CreateObject("ADODB.Connection")
conn.ConnectionString = sCon
conn.CursorLocation = 3
conn.Open

' 2.2 Use command text for query
Set oRs = CreateObject("ADODB.Recordset")
Set oCom = CreateObject("ADODB.Command")
oCom.CommandType = 1
Set oCom.ActiveConnection = conn
oCom.CommandText = sSql

' 2.3 Fill the recordset
Set oRs = oCom.Execute
```

```
' 3.1 Fill standard listview object with recordset according to schema
If sTagSchema = "TAG" Then
 Display oRs
Else
 DisplayEx oRs
End If

Set oRs = Nothing
conn.Close
Set conn = Nothing

End Sub

' Display recordset for 'TAG' schema
Sub Display(oRs_in)

 Dim oItem As ListItem
 Dim strDateTime As String
 Dim iMS As Long

 Dim m, n, s, nRec
 m = oRs_in.Fields.Count
 n = 0
 nRec = NMAX

 ' 3.2 Fill standard listview object with recordset
 ListView1.ColumnHeaders.Clear

 ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(1).Name), 2500 '
 DateTime

 ListView1.ColumnHeaders.Add , , "MS", 1500 '
 Millisecond

 ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(0).Name), 1500 ' VarID
 ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(2).Name), 1500 '
 RealValue

 ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(3).Name), 1500 '
 Quality

 ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(4).Name), 1500 ' Flags

 If (m > 0) Then
 oRs_in.MoveFirst
 n = 0
 Do While (Not oRs_in.EOF And n < nRec)
 n = n + 1
```

## 2.7 Examples for Access Using OLE DB Provider

```

SplitDateTimeAndMs oRs_in.Fields(1).Value, strDateTime, iMS 'Split
Millisecond from DateTime
s = FormatDateTime(strDateTime, 2) & " " & FormatDateTime(strDateTime, 3)
Set oItem = ListView1.ListItems.Add()
oItem.Text = s
oItem.SubItems(1) = iMS
oItem.SubItems(2) = oRs_in.Fields(0).Value
oItem.SubItems(3) = FormatNumber(oRs_in.Fields(2).Value, 4)
oItem.SubItems(4) = Hex(oRs_in.Fields(3).Value)
oItem.SubItems(5) = Hex(oRs_in.Fields(4).Value)

oRs_in.MoveNext
Loop
oRs_in.Close
Else
End If

End Sub

' Display recordset for 'TAG_EX' schema
Sub DisplayEx(oRs_in)

Dim oItem As ListItem
Dim strDateTime As String
Dim iMS As Long

Dim m, n, s, nRec
m = oRs_in.Fields.Count
n = 0
nRec = NMAX

' 3.3 Fill standard listview object with recordset
ListView1.ColumnHeaders.Clear
ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(1).Name), 2500 '
DateTime
ListView1.ColumnHeaders.Add , , "MS", 1500 '
Millisecond
ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(0).Name), 1500 ' VarID
ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(3).Name), 1500 '
VariantValue
ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(4).Name), 1500 '
Quality
ListView1.ColumnHeaders.Add , , CStr(oRs_in.Fields(5).Name), 1500 ' Flags

```

```
If (m > 0) Then
oRs_in.MoveFirst
n = 0
Do While (Not oRs_in.EOF And n < nRec)
n = n + 1
SplitDateTimeAndMs oRs_in.Fields(1).Value, strDateTime, iMS 'Split
Millisecond from DateTime
s = FormatDateTime(strDateTime, 2) & " " & FormatDateTime(strDateTime, 3)
Set oItem = ListView1.ListItems.Add()
oItem.Text = s
oItem.SubItems(1) = iMS
oItem.SubItems(2) = oRs_in.Fields(0).Value
oItem.SubItems(3) = oRs_in.Fields(3).Value
oItem.SubItems(4) = Hex(oRs_in.Fields(4).Value)
oItem.SubItems(5) = Hex(oRs_in.Fields(5).Value)

oRs_in.MoveNext
Loop
oRs_in.Close
Else
End If

End Sub

Sub SplitDateTimeAndMs(dtDateTimeWithMs_in, strDateTime_out, strMs_out)

Dim diff
Dim dtTemp
Dim lTemp As Long

lTemp = 86400000 '24 * 60 * 60 * 1000

diff = (CDBl(dtDateTimeWithMs_in) -
CDBl(CDate(CStr(dtDateTimeWithMs_in)))) * lTemp
If (diff < 0) Then
diff = 1000 + diff
dtTemp = CDBl(dtDateTimeWithMs_in) - diff / lTemp
strDateTime_out = CDate(dtTemp)
Else
strDateTime_out = CDate(dtDateTimeWithMs_in)
End If
strMs_out = "00" & Round(diff)
strMs_out = Right(strMs_out, 3)
```

End Sub

## See also

Displaying Process Value Archives (Page 181)

Querying Process Value Archives (Page 184)

Querying the Archive Data (Page 183)

Establishing the Connection to the Archive Database (Page 179)

### 2.7.4.2 Example: Reading Process Value Archive With WinCC OLE DB Provider and Visual Basic.NET

#### Introduction

In this example, the values of the last 10 minutes of the tag "Tag\_1" are read from the local WinCC RT database.

The data is displayed with a time stamp, value and quality code in a ListView.

The output of values is limited to 100 (constant MaxRows = 100).

The example includes simple error handling.

#### Procedure

1. Create a WinCC tag named "Tag\_1".
2. Create a process value archive named "ArTags".
3. Connect the WinCC tag "Tag\_1" with the process value archive.
4. In Visual Studio, create a new Visual Basic project of the "Windows Application" type.
5. Change to Designer View mode and enlarge the Windows Form "Form1" to a size of approx. 500x600.
6. Drag a "ListView Control" from the Toolbox to the left upper corner of the form and enlarge it to approx. 400x450.
7. Drag a button from the Toolbox to the middle of the form below the Control. The button will automatically be named "Button1".
8. Double-click the button and add the VB.NET sample code listed below IN FRONT OF the instruction "End Sub" in the method "Private Sub Button1\_Click".
9. Select "Build > Build Solution" in the menu or press <CTRL+Shift+B> to compile the finished VB.NET project.

10. Adapt the script to your project:

- Change the name of the WinCC Runtime database  
"CC\_CPSample\_07\_10\_09\_13\_44\_26R".  
The database name can be found in the SQL Server Management Studio under "Object Explorer > <Computer Name>\WinCC > Databases > <Database name\_R>".
- If necessary, change the name of the schema used.  
To access process values of the following tag types, use the "TAG\_EX" schema:
  - Text tag, 8-bit character set / 16-bit character set
  - Floating-point number 64-bit IEEE 754

11. Start WinCC Runtime and select "Debug->Start Debugging" in the menu or press <F5> to start the VB application.

12. Click on the "Button1" button.

## Example Script

```
Const MaxRows = 100

' 1.1 Create connection string for ADO.NET access
Dim ProviderName As String
Dim CatalogName As String
Dim DataSourceName As String
Dim ConnectionString As String
Dim CommandString As String
Dim TagSchema As String

ProviderName = "Provider=WinCCOLEDBProvider.1;"
CatalogName = "Catalog=CC_CPSample_07_10_09_13_44_26R;"
DataSourceName = "Data Source=.\WinCC"

ConnectionString = ProviderName + CatalogName + DataSourceName

' 1.2 Define the Tag Schema Name (TAG or TAG_EX)
TagSchema = "TAG"

' 1.3 Define command string for OLE DB access (relative time range, last 10
minutes)
CommandString = TagSchema + ":R,'ArTags\Tag_1','0000-00-00
00:10:00.000','0000-00-00 00:00:00.000'"

Try

Dim DBConnection As System.Data.OleDb.OleDbConnection
Dim DBCommand As System.Data.OleDb.OleDbCommand
Dim DBReader As System.Data.OleDb.OleDbDataReader

' 2.1 Open an OLE DB connection
DBConnection = New System.Data.OleDb.OleDbConnection(ConnectionString)

DBConnection.Open()

' 2.2 Execute command
DBCommand = New System.Data.OleDb.OleDbCommand(CommandString,
DBConnection)

DBReader = DBCommand.ExecuteReader()

' 3.1 Prepare list view control
Dim DBTimeStamp As System.DateTime
```

```
Dim DBValue As String
Dim DBQualityCode As Integer
Dim DBFlags As Integer
Dim ColumnEntry As String

Me.ListView1.View = View.Details
Me.ListView1.GridLines = True
Me.ListView1.TabIndex = 0
Me.ListView1.Width = 400

Me.ListView1.Columns.Add("TimeStamp", HorizontalAlignment.Center)
Me.ListView1.Columns(0).Width = 150
Me.ListView1.Columns(0).Text = "Time Stamp"

Me.ListView1.Columns.Add("Value", HorizontalAlignment.Center)
Me.ListView1.Columns(1).Width = 60
Me.ListView1.Columns(1).Text = "Value"

Me.ListView1.Columns.Add("QC", HorizontalAlignment.Center)
Me.ListView1.Columns(2).Width = 60
Me.ListView1.Columns(2).Text = "Quality Code"

Me.ListView1.Columns.Add("Flags", HorizontalAlignment.Center)
Me.ListView1.Columns(3).Width = 60
Me.ListView1.Columns(3).Text = "Flags"

Dim SingleRow As ListViewItem

Dim Count As Integer
Count = 0

' 3.2 Fetch subsequent rows of the result set
While (DBReader.Read And Count < MaxRows)

 DBTimeStamp = DBReader.GetDateTime(1)
 If TagSchema = "TAG" Then
 DBValue = DBReader.GetValue(2)
 DBQualityCode = DBReader.GetInt32(3)
 DBFlags = DBReader.GetInt32(4)
 Else
 DBValue = DBReader.GetValue(3)
 DBQualityCode = DBReader.GetInt32(4)
 DBFlags = DBReader.GetInt32(5)
 End If
```

```
' 3.3 Fill list view columns
ColumnEntry = String.Format("{0:dd.MM.yy HH:mm:ss.}{1:D2}", DBTimeStamp,
DBTimeStamp.Millisecond)
SingleRow = New ListViewItem(ColumnEntry)

ColumnEntry = String.Format("{0:F}", DBValue)
SingleRow.SubItems.Add(ColumnEntry)

ColumnEntry = String.Format("{0:X2}", DBQualityCode)
SingleRow.SubItems.Add(ColumnEntry)

ColumnEntry = String.Format("{0:X4}", DBFlags)
SingleRow.SubItems.Add(ColumnEntry)

Me.ListView1.Items.Add(SingleRow)
Count = Count + 1

End While

' 4 Clean up
DBReader.Close()
DBConnection.Close()

' 5 Exception (error) handling
Catch ex As Exception
MessageBox.Show(ex.Message, "Error Occurred !")

End Try
```

## 2.7.5 Examples: Analyzing Alarm Message Archives

### 2.7.5.1 Example: Reading Message Archive Data with the WinCC OLE DB Provider and Visual Basic 6

#### Introduction

In this example, a time interval of 10 minutes is read from the message archive data.

The data are displayed in a ListView Control with a time stamp, message number, status and message type.

The example includes simple error handling.

## Procedure

1. Create a Visual Basic project.  
Connect a Microsoft Windows Common Controls 6.0 ListView control to the name "ListView1".
2. The columns in the ListView are created by the script.
3. Create a "CommandButton".  
Copy in the script from the section "Example Script" below.
4. In the script, change the name of the WinCC Runtime database "CC\_OpenArch\_03\_05\_27\_14\_11\_46R" according to your own project.  
The database name can be found in the SQL Enterprise Manager at "SQL Server Group" > "<Computer Name>\WinCC" > "Databases" > "<Database name\_R>".
5. This example uses the English database table "AlgViewEXEnu".  
If you want to read the message archive data of another language, you need to modify the entry.
6. Activate WinCC Runtime.
7. Start the VB application.
8. Click on the "CommandButton".

## Example Script

---

### Note

#### Improving performance

In order to improve performance, replace the "Data Source=.\\WinCC" instruction with the "Data Source=<Computer name>\\WinCC" instruction.

The output of the values is limited to 100 (n > 100).

The times indicated refer to system time.

---

---

2.7 Examples for Access Using OLE DB Provider

```
Dim sPro As String
Dim sDsn As String
Dim sSer As String
Dim sCon As String
Dim sSql As String

Dim conn As Object
Dim oRs As Object
Dim oCom As Object
Dim oItem As ListItem

Dim m, n, s

On Error GoTo ErrorHandlerA

' 1.1 Make connection string for ADODB
sPro = "Provider=WinCCOLEDBProvider.1;"
sDsn = "Catalog=CC_OpenArch_03_05_27_14_11_46R;"
sSer = "Data Source=.\WinCC"
sCon = sPro + sDsn + sSer

' 1.2 Define command text in sSql
sSql = "ALARMVIEWEX:Select * FROM AlgViewEXEnu WHERE DateTime>'2003-07-30
11:30:00'
AND DateTime<'2003-07-30 11:40:00'"
'sSql = "ALARMVIEWEX:Select * FROM AlgViewEXEnu WHERE MsgNr = 5"
'sSql = "ALARMVIEWEX:Select * FROM AlgViewEXEnu"
MsgBox "Open with:" & vbCrLf & sCon & vbCrLf & sSql & vbCrLf

' 2.1 Make connection
Set conn = CreateObject("ADODB.Connection")
conn.ConnectionString = sCon
conn.CursorLocation = 3
conn.Open

' 2.2 Use command text for query
Set oRs = CreateObject("ADODB.Recordset")
Set oCom = CreateObject("ADODB.Command")
oCom.CommandType = 1
Set oCom.ActiveConnection = conn
oCom.CommandText = sSql

' 2.3 Fill the recordset
```

```
Set oRs = oCom.Execute
m = oRs.Fields.Count

' 3.0 Fill standard listview object with recordset
ListView1.ListItems.Clear
ListView1.ColumnHeaders.Clear
ListView1.ColumnHeaders.Add , , CStr(oRs.Fields(2).Name), 140
ListView1.ColumnHeaders.Add , , CStr(oRs.Fields(0).Name), 60
ListView1.ColumnHeaders.Add , , CStr(oRs.Fields(1).Name), 60
ListView1.ColumnHeaders.Add , , CStr(oRs.Fields(34).Name), 100
If (m > 0) Then
oRs.MoveFirst
n = 0
Do While Not oRs.EOF
n = n + 1
If (n < 100) Then
s = Left(CStr(oRs.Fields(1).Value), 23)
Set oItem = ListView1.ListItems.Add()
oItem.Text = CStr(oRs.Fields(2).Value)
oItem.SubItems(1) = CStr(oRs.Fields(0).Value)
oItem.SubItems(2) = CStr(oRs.Fields(1).Value)
oItem.SubItems(3) = CStr(oRs.Fields(34).Value)
End If
oRs.MoveNext
Loop
oRs.Close
Else

End If
Set oRs = Nothing
conn.Close
Set conn = Nothing

ErrorHandlerA:
MsgBox Err.Description
```

## See also

[Establishing the Connection to the Archive Database \(Page 179\)](#)  
[Displaying Alarm Message Archives \(Page 194\)](#)  
[Querying Alarm Message Archives \(Page 192\)](#)  
[Querying the Archive Data \(Page 183\)](#)

### 2.7.5.2 Example: Reading Message Archive Data With WinCC OLE DB Provider and Visual Basic.NET

#### Introduction

In this example, a time interval of 10 minutes is read from the alarm message archive data.

The data are displayed in a ListView Control with a time stamp, message number, status and message type.

The example includes simple error handling.

#### Procedure

1. Create a new Visual Basic project in Visual Studio 2005 of the type "Windows Application".
2. Change to Designer View mode and enlarge the Windows Form "Form1" to a size of ca. 600x600.
3. Drag a "ListView Control" from the Toolbox to the left upper corner of the form and enlarge it to ca. 500x450.
4. Drag a button from the Toolbox to the middle of the form below the Control. The button will automatically be named "Button1".
5. Double-click the button and add the VB.NET sample code listed below IN FRONT OF the instruction "End Sub" in the method "Private Sub Button1\_Click."
6. Select "Build > Build Solution" in the menu or press <CTRL+Shift+B> to compile the finished VB.NET project.
7. In the script, adjust the name of the WinCC Runtime database "CC\_CPSample\_07\_10\_09\_13\_44\_26R" to your own project. The database name can be found in the SQL Server Management Studio under "Object Explorer > <Computer Name>\WinCC > Databases > <Database name\_R>".
8. Activate WinCC Runtime.
9. Select "Debug > Start Debugging" from the menu or press <F5> to start the VB application.
10. Click on the "Button1" button.

## Example Script

```
Const MaxRows = 100
' 1.1 Create connection string for ADO.NET access
Dim ProviderName As String
Dim CatalogName As String
Dim DSN As String
Dim ConnectionString As String
Dim CommandString As String

ProviderName = "Provider=WinCCOLEDBProvider.1;"
CatalogName = "Catalog=CC_CPSample_07_10_09_13_44_26R;"
DSN = "Data Source=.\WinCC"

ConnectionString = ProviderName + CatalogName + DSN

' 1.2 Define command string for ADO.NET access
CommandString = "ALARMVIEWEX:Select * From AlgViewEXenu WHERE DateTime > '2007-10-10 12:00:00' AND DateTime > '2007-10-10 12:10:00'"
'CommandString = "ALARMVIEWEX:Select * From AlgViewEXenu WHERE MsgNr = 1"
'CommandString = "ALARMVIEWEX:Select * From AlgViewEXenu"

Try

Dim DBConnection As System.Data.OleDb.OleDbConnection
Dim DBCommand As System.Data.OleDb.OleDbCommand
Dim DBReader As System.Data.OleDb.OleDbDataReader

Dim DBConnection As System.Data.OleDb.OleDbConnection
Dim DBCommand As System.Data.OleDb.OleDbCommand
Dim DBReader As System.Data.OleDb.OleDbDataReader

' 2.1 Open an OLE DB connection
DBConnection = New System.Data.OleDb.OleDbConnection(ConnectionString)

DBConnection.Open()

' 2.2 Execute command
DBCommand = New System.Data.OleDb.OleDbCommand(CommandString, DBConnection)

DBReader = DBCommand.ExecuteReader()

' 3.1 Prepare list view control
Dim ColumnEntry As String

Me.ListView1.View = View.Details
Me.ListView1.GridLines = True
Me.ListView1.TabIndex = 0
Me.ListView1.Width = 500

Me.ListView1.Columns.Add("Number", HorizontalAlignment.Center)
Me.ListView1.Columns(0).Width = 90
Me.ListView1.Columns(0).Text = "Number"

Me.ListView1.Columns.Add("Date/Time", HorizontalAlignment.Center)
Me.ListView1.Columns(1).Width = 130
```

---

2.7 Examples for Access Using OLE DB Provider

```
Me.ListView1.Columns(1).Text = "Date/Time"

Me.ListView1.Columns.Add("State", HorizontalAlignment.Center)
Me.ListView1.Columns(2).Width = 60
Me.ListView1.Columns(2).Text = "State"

Me.ListView1.Columns.Add("Type", HorizontalAlignment.Center)
Me.ListView1.Columns(3).Width = 150
Me.ListView1.Columns(3).Text = "Type"

Dim SingleRow As ListViewItem
Dim MsgDateTime As DateTime
Dim MsgMilliSecs As Integer
Dim MsgNumber As Integer
Dim MsgState As Integer
Dim MsgTypeName As String

Dim Count As Integer
Count = 0

' 3.2 Fetch subsequent rows of the result set
While (DBReader.Read And Count < MaxRows)

MsgNumber = DBReader.GetInt32(0)
MsgDateTime = DBReader.GetDateTime(2)
MsgMilliSecs = DBReader.GetInt16(3)
MsgState = DBReader.GetInt16(1)
MsgTypeName = DBReader.GetString(34)

' 3.3 Fill list view columns
ColumnEntry = String.Format("{0:D10}", MsgNumber)
SingleRow = New ListViewItem(ColumnEntry)

ColumnEntry = String.Format("{0:dd.MM.yy HH:mm:ss.}{1:D2}", MsgDateTime, MsgMilliSecs)
SingleRow.SubItems.Add(ColumnEntry)

ColumnEntry = String.Format("{0:D5}", MsgState)
SingleRow.SubItems.Add(ColumnEntry)

ColumnEntry = MsgTypeName
SingleRow.SubItems.Add(ColumnEntry)

Me.ListView1.Items.Add(SingleRow)

Count = Count + 1

End While

' 4 Clean up
DBReader.Close()
DBConnection.Close()

' 5 Exception (error) handling
Catch ex As Exception
MessageBox.Show(ex.Message, "Error Occured !")
```

End Try

## 2.8 Connectivity Station

### 2.8.1 Basics of the Connectivity Station

#### Introduction

With the Connectivity Station, you can access WinCC stations with server packages from a central computer without the WinCC software.

The WinCC stations can be accessed through two different interfaces:

- OPC interfaces of the Connectivity Station
- OLE DB interface of the Connectivity Pack

The access options include different functions.

#### OPC interfaces of the Connectivity Station

The Connectivity Station provides interfaces via which you can access the following content with an OPC client:

- OPC DA server: Tags, such as process values
- OPC HDA server: Archives process values
- OPC A&E server: Messages

#### Licensing

You need the "WinCC Connectivity Station" license to use the OPC interfaces of the Connectivity Station on a computer without WinCC installation.

If you only use the OPC interfaces of a WinCC installation, you only need the "Connectivity Pack" license.

The following table shows the rules:

	WinCC-independent installation at Connectivity Station	Installation of OPC with WinCC
OPC DA	"WinCC Connectivity Station" license	No license required
OPC HDA	"WinCC Connectivity Station" license	"WinCC Connectivity Pack" license
OPC A&E	"WinCC Connectivity Station" license	"WinCC Connectivity Pack" license

#### OLE DB interface of the Connectivity Pack

The Connectivity Pack server or Connectivity Pack client necessary for the operation of the Connectivity Station provides an additional OLE DB interface.

You can access messages and tags via such OLE DB interfaces.

## Transparent access to archived data

The Connectivity Station supports the transparent access to the archive databases of WinCC stations.

## Installation and Configuration

You will need the following to install the Connectivity Station:

- PC with Connectivity Pack Server or Connectivity Pack Client

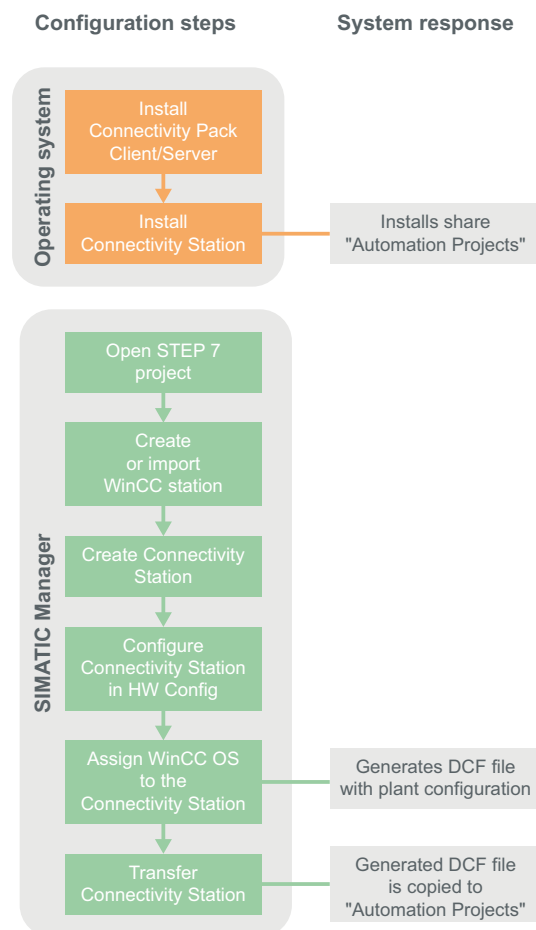
In order to configure a computer as a Connectivity Station, run the Connectivity Pack client setup on the computer.

From the "Installing Software" menu of the installation DVD, select the entry "Connectivity Station".

After the installation, you can set up the access to the WinCC stations with the following program:

- SIMATIC Manager of STEP 7

The figure below provides an overview of the configuration steps for the Connectivity Station:



## Settings for operation with several network cards

Make sure that the correct network card is selected in the settings of the Simatic Shell.

Click on the Simatic Shell icon and select "Settings" in the shortcut menu.

You may have to select a different network card under "Selection of terminal bus".

## See also

Bases of OLE DB (Page 174)

Transparent access to archived data (Page 169)

Functionality of OPC (Page 231)

Use of OPC interface of the Connectivity Station (Page 346)

Use of OLE DB interface of the Connectivity Station (Page 347)

## 2.8.2 Functionality of the Connectivity Station

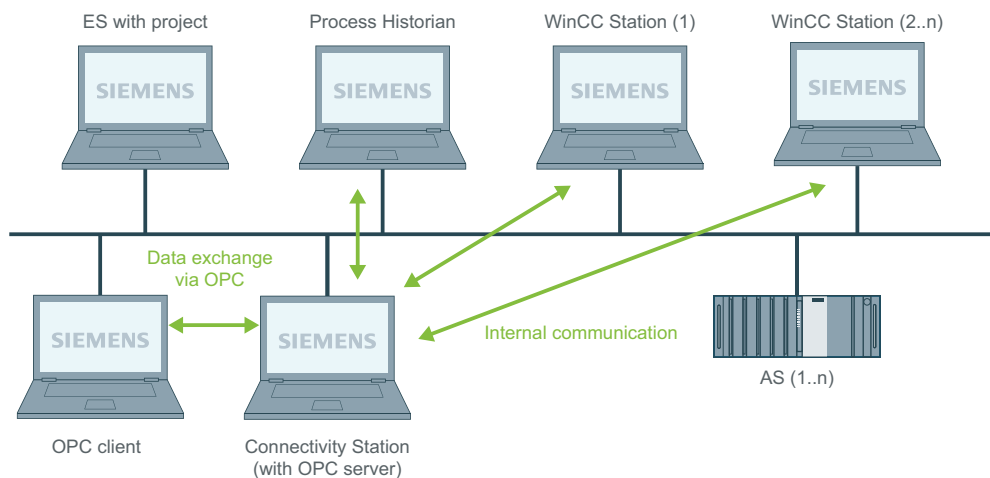
### 2.8.2.1 Use of OPC interface of the Connectivity Station

#### Principle

The Connectivity Station includes the WinCC OPC-Server through which you can access WinCC stations with server packages, using the OPC client.

You can use the OPC client locally on the Connectivity Station or on a separate computer.

The OPC client requires DCOM access rights to the Connectivity Station.



ES = Engineering Station with STEP 7 or NCM PC Manager  
AS = Automation System

## Server name of the OPC-Servers

The data exchange between the OPC client and the Connectivity Station takes place via the OPC.

The following WinCC OPC servers are integrated into the Connectivity Station:

WinCC OPC-Server	Server name
OPC DA	WinCCConnectivity.OPCDAServer
OPC HDA	WinCCConnectivity.OPCHDAServer.1
OPC A&E	WinCCConnectivity.OPCAEServer.1

## Supported OPC Standards

The Connectivity Station supports the following OPC standards:

- OPC DA 2.05a Specification
- OPC DA 3.00 Specification
- OPC XML DA 1.01 Specification
- OPC AE 1.10 Specification
- OPC HDA 1.20 Specification

## Transparent access to archived data

With OPC, you have transparent access to all archive databases of the WinCC stations.

## See also

Basics of the Connectivity Station (Page 344)

Using OPC in WinCC (Page 232)

Access Using OPC to WinCC Archives, Tags, and Messages (Page 168)

Transparent access to archived data (Page 169)

### 2.8.2.2 Use of OLE DB interface of the Connectivity Station

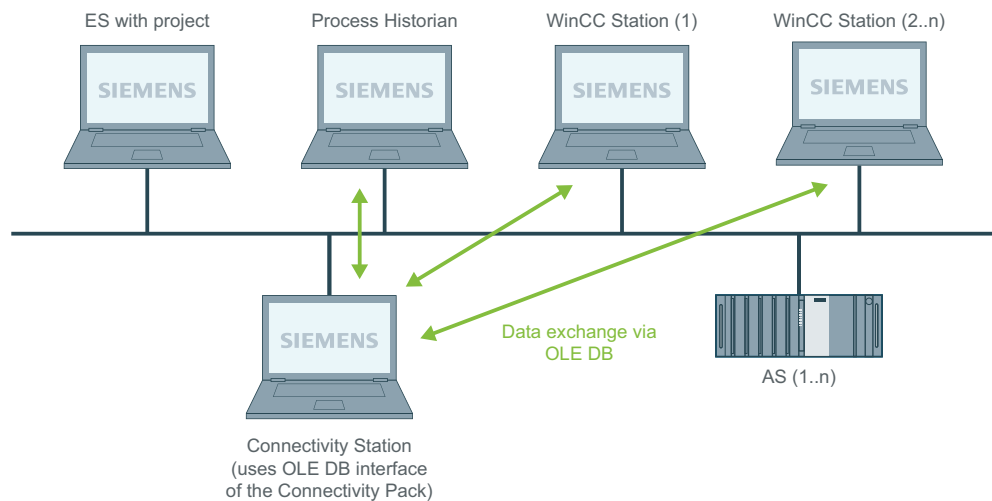
#### Principle

The Connectivity Station can only be used, if there is a Connectivity Pack Server or a Connectivity Pack Client installed.

The WinCC OLE DB provider of the Connectivity Pack Server/Client provides an OLE DB interface.

You can access messages and tags via such OLE DB interfaces.

## 2.8 Connectivity Station



ES = Engineering Station with STEP 7 or NCM PC Manager  
AS = Automation System

### Access to databases with OLE DB

For access to databases with WinCC OLE DB, you may write your own applications.

For the communication with the WinCC OLE DB Provider, applications - created with, for example, Visual Basic, VBScript or VBA - use the ADO DB.

#### Note

##### Connectivity Station on a client with own project

If you use the Connectivity Station on a client with own project and use the OLE-DB interface, then observe the following:

You can only access those WinCC stations, which you entered during the configuration phase of the Connectivity Station.

Connectivity Station does not use the server packages available on the client.

### Transparent access to archived data

With OLE DB, you can only access process value archives transparently.

Only one central archive server, e.g. "Process Historian", may be used in a project for transparent access via WinCC OLE DB Provider.

If you want to use a Connectivity Station in two projects and both these projects contain an archive server, you need to remove the DCF file of the previous project before changing the project.

You can find the DCF file on the Connectivity station under the following path:

- Installation  
directory\Siemens\AutomationProjects\<PROJEKTNAME\_ConnectivityStationName>.DCF

**Note****Use project name as "Catalog"**

Enter the WinCC project name for "Catalog" for transparent access; e.g.:  
"Catalog=WinCC\_Project\_Name".

---

**See also**

Basics of the Connectivity Station (Page 344)

Transparent access to archived data (Page 169)

Analysis Functions for Messages and Process Values (Page 202)

## 2.8.3 Configuring the Connectivity Station in the S7 project

**Introduction**

In order to set up the Connectivity Station, you will add a new "SIMATIC PC Station" to the system configuration.

This "SIMATIC PC Station" receives the properties of the Connectivity Station by configuring the application "SPOSA Application".

Depending on the project type, one of the following objects will be created in the "SPOSA Application".

- With project type "STEP 7", this is the object "Connectivity Station\_(n)".
- With project type "PCS 7", this is the object "Open\_PCS7\_Station\_(n)".

In the following description, the project type "STEP 7" and the respective object name are used.

**Requirements**

- The required software for the Connectivity Station is installed on the Connectivity Station PC.
- The system configuration contains WinCC stations with server packages.

**Procedure**

The configuration procedure for the Connectivity Station consists of the following steps:

1. Create and configure SIMATIC PC Station
2. Assign WinCC Station
3. Transfer connectivity station

### Create and configure SIMATIC PC Station

1. Select the project directory from the navigation window in SIMATIC Manager.
2. Select the menu command "Insert New Object > SIMATIC PC STATION" from the shortcut menu.  
A new "SIMATIC PC Station" object is inserted and remains selected in the navigation window.
3. Select the "Open object" menu command from the shortcut menu of the SIMATIC PC Station.  
The "HW Config" editor opens the view of the new PC station as empty rack.
4. Select the entry "SPOSA Application" in the module catalog in the directory "SIMATIC PC Station > HMI".  
Drag the selected module to a free slot of the rack.
5. Select the menu command "Station > Save and translate".
6. Select the menu command "Station > Exit" to close "HW Config".

### Assign WinCC Station

1. Using the "SPOSA Application", navigate to the "Connectivity Station" icon in the directory of the new PC station.
2. Select the "Assign OS Server..." menu command from the "Connectivity Station" shortcut menu.  
The "Assignment of OS Server for Open\_TIA\_Station" dialog is opened.
3. Select the WinCC stations in the table in the column "OS Information", whose data the Connectivity Station is to gain access to.  
Click "OK" to close the dialog.
4. Select the "Connectivity Station" icon in the navigation window.
5. Select the "Object properties" menu command from the shortcut menu.  
The "Properties - TIA application" dialog appears: "Connectivity Station" is opened.
6. Change to "Destination System" tab and enter the path to the Connectivity Station PC in the "Path" field.  
As an alternative, you may open a selection dialog via the "Browse..." button and search for the computer in the network.
  - After you have entered the PC name, click the "Apply" button.
  - The directory "Automation Projects" will be appended to the computer name.
  - Click "OK" to close the dialog.

Always use the default path "<Installation directory>\Siemens\AutomationProjects" for the Connectivity Station. If you move the Connectivity Station into a different folder after the installation, access will no longer work.

### Transfer connectivity station

1. Check whether the "Connectivity Station" icon is clicked in the directory of the new PC station in the navigation window.
2. Select the "Target System > Load" menu command from the shortcut menu.
3. Acknowledge the message after exiting this process.

## Result

A computer in the hardware configuration in the S7 project is supplemented and configured for the Connectivity Station.

The required project data has been transferred to this computer.

## 2.8.4 Accessing WinCC data with the Connectivity Station

### Introduction

The Connectivity Station allows access to the data of different WinCC stations by means of an OPC client. For this, the OPC client must simply connect to the Connectivity Station.

The data exchange between the OPC client and the Connectivity Station takes place via the OPC. The following WinCC OPC-Servers are integrated into the Connectivity Station.

OPC-Server	Server name
OPC DA	WinCCConnectivity.OPCDAServer
OPC HDA	WinCCConnectivity.OPCHDAServer.1
OPC A&E	WinCCConnectivity.OPCAEServer.1

### Requirements

- The software for the Connectivity Station is installed on the Connectivity Station PC.
- The Connectivity Station is configured in the S7 project and the project data is transferred to the computer of the Connectivity Station.
- An OPC client in accordance with the OPC specifications is available.

### The Procedure in Principle

The following description depicts the basic procedure.

1. Start the OPC client on the PC.
2. Select the OPC-Server according to the desired data.  
The same names as the ones in the above table apply to the WinCC OPC-Server.
3. Define which data should be transferred, e.g. tags.

## Result

The OPC client is connected to the Connectivity Station and receives the WinCC data.

### See also

Examples for Access Using OLE DB Provider (Page 318)

Access Using OPC to WinCC Archives, Tags, and Messages (Page 168)

## 2.8 Connectivity Station

Establishing the Connection to the Archive Database (Page 179)

OPC - Open Connectivity (Page 230)

## 2.9 Connectivity Station for OPC UA

### 2.9.1 Basic information on Connectivity Station for OPC UA

#### Introduction

With the Connectivity Station, you can access WinCC stations with server packages from a central computer without the WinCC software.

You can use the OPC UA interface of the Connectivity Station to access the WinCC stations.

#### OPC interface of the Connectivity Station

The Connectivity Station provides the OPC UA interface, via which you can access the following content with an OPC client:

- Process values
- Values from tag archives
- WinCC messages

#### Licensing

You will need the "WinCC Connectivity Station" license to use the OPC interface of the Connectivity Station on a computer without WinCC installation.

If you are only using the OPC interface of a WinCC installation, you will only need the "Connectivity Pack" license.

The following table shows the rules:

	WinCC-independent installation at Connectivity Station	Installation of OPC with WinCC
OPC UA	"WinCC Connectivity Station" license	"WinCC Connectivity Pack" license

#### WinCC Connectivity Station: OPC UA server

The OPC UA server on a WinCC Connectivity Station can be reached via this address:

- "opc.tcp://[HostName]:[Port]"

HostName	Placeholder for the computer name. The name is entered automatically.
Port	Port number. The default is "4864".

## Transparent access to archived data

The Connectivity Station supports the transparent access to the archive databases of WinCC stations.

## Installation and Configuration

You will need the following to install the Connectivity Station:

- PC with Connectivity Pack Server or Connectivity Pack Client

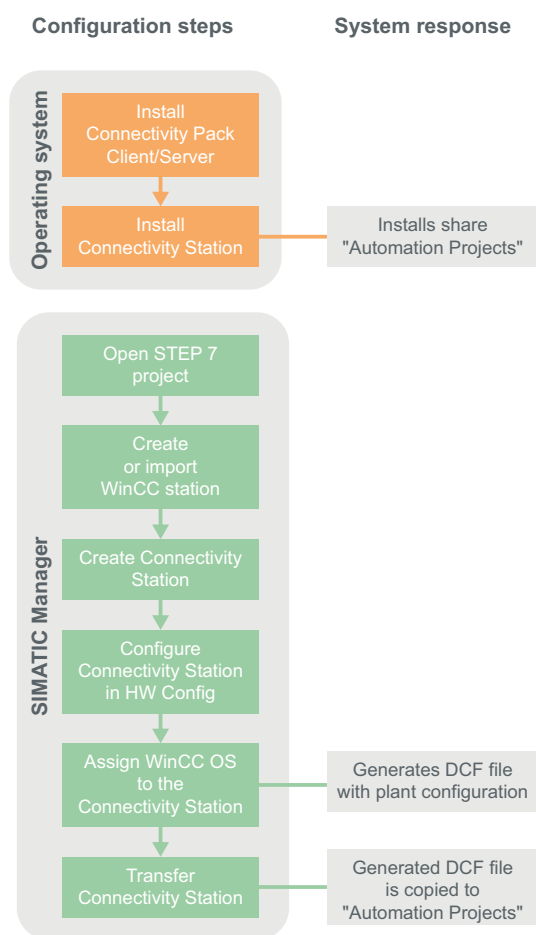
In order to configure a computer as a Connectivity Station, run the Connectivity Pack client setup on the computer.

During installation, select the "Connectivity Station" entry in the "Install software" menu.

After the installation, you can set up the access to the WinCC stations with the following program:

- SIMATIC Manager of STEP 7

The figure below provides an overview of the configuration steps for the Connectivity Station:



## Settings for operation with several network cards

Make sure that the correct network card is selected in the settings of the Simatic Shell.

Click on the Simatic Shell icon and select "Settings" in the shortcut menu.

You may have to select a different network card under "Selection of terminal bus".

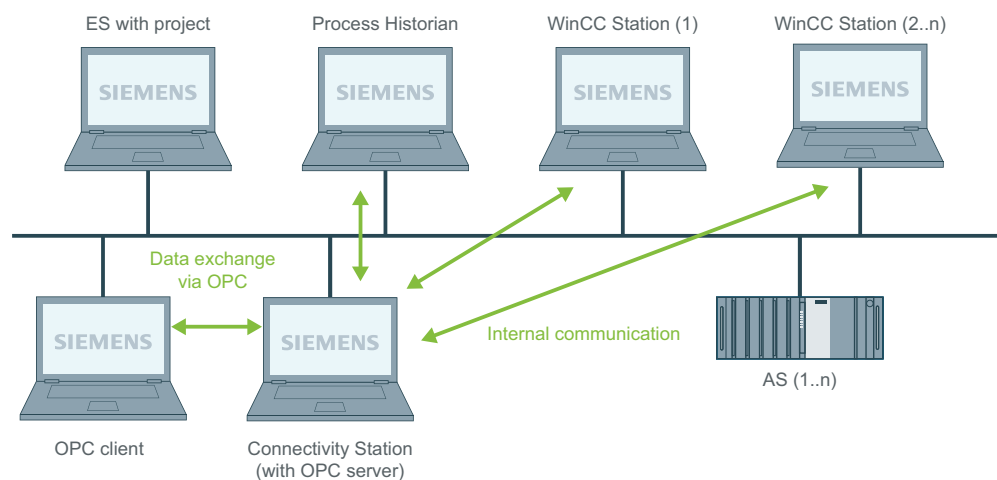
## 2.9.2 Using the OPC UA interface of the Connectivity Station

### Principle

The Connectivity Station includes the WinCC OPC-Server through which you can access WinCC stations with server packages, using the OPC client.

You can use the OPC client locally on the Connectivity Station or on a separate computer.

The exchange of data between the OPC client and the Connectivity Station takes place via the OPC UA.



ES = Engineering Station with STEP 7 or NCM PC Manager  
AS = Automation System

### Server name

The WinCC OPC server "WinCCConnectivity.OPCUAServer" is integrated into the Connectivity Station.

### Supported OPC standard

The WinCC OPC UA server supports OPC UA Specification 1.03.

### 2.9.3 Configuring Connectivity Station in S7 Project (OPC UA)

#### Introduction

In order to set up the Connectivity Station, you will add a new "SIMATIC PC Station" to the system configuration.

This "SIMATIC PC Station" receives the properties of the Connectivity Station by configuring the application "SPOSA Application".

Depending on the project type, one of the following objects will be created in the "SPOSA Application".

- With project type "STEP 7", this is the object "Connectivity Station\_(n)".
- With project type "PCS 7", this is the object "Open\_PCS7\_Station\_(n)".

In the following description, the project type "STEP 7" and the respective object name are used.

#### Requirements

- The required software for the Connectivity Station is installed on the Connectivity Station PC.
- The system configuration contains WinCC stations with server packages.

#### Procedure

The configuration procedure for the Connectivity Station consists of the following steps:

1. Create and configure SIMATIC PC Station
2. Assign WinCC Station
3. Transfer connectivity station

#### Create and configure SIMATIC PC Station

1. Select the project directory from the navigation window in SIMATIC Manager.
2. Select the menu command "Insert New Object > SIMATIC PC STATION" from the shortcut menu.  
A new "SIMATIC PC Station" object is inserted and remains selected in the navigation window.
3. Select the "Open object" menu command from the shortcut menu of the SIMATIC PC Station.  
The "HW Config" editor opens the view of the new PC station as empty rack.
4. Select the entry "SPOSA Application" in the module catalog in the directory "SIMATIC PC Station > HMI".  
Drag the selected module to a free slot of the rack.
5. Select the menu command "Station > Save and translate".
6. Select the menu command "Station > Exit" to close "HW Config".

## Assign WinCC Station

1. Using the "SPOSA Application", navigate to the "Connectivity Station" icon in the directory of the new PC station.
2. Select the "Assign OS Server..." menu command from the "Connectivity Station" shortcut menu.  
The "Assignment of OS Server for Open\_TIA\_Station" dialog is opened.
3. Select the WinCC stations in the table in the column "OS Information", whose data the Connectivity Station is to gain access to.  
Click "OK" to close the dialog.
4. Select the "Connectivity Station" icon in the navigation window.
5. Select the "Object properties" menu command from the shortcut menu.  
The "Properties - TIA application" dialog appears: "Connectivity Station" is opened.
6. Change to "Destination System" tab and enter the path to the Connectivity Station PC in the "Path" field.  
As an alternative, you may open a selection dialog via the "Browse..." button and search for the computer in the network.
  - After you have entered the PC name, click the "Apply" button.
  - The directory "Automation Projects" will be appended to the computer name.
  - Click "OK" to close the dialog.

Always use the default path "<Installation directory>\Siemens\AutomationProjects" for the Connectivity Station. If you move the Connectivity Station into a different folder after the installation, access will no longer work.

## Transfer connectivity station

1. Check whether the "Connectivity Station" icon is clicked in the directory of the new PC station in the navigation window.
2. Select the "Target System > Load" menu command from the shortcut menu.
3. Acknowledge the message after exiting this process.

## Result

A computer in the hardware configuration in the S7 project is supplemented and configured for the Connectivity Station.

The required project data has been transferred to this computer.

## 2.9.4 Accessing WinCC data with the Connectivity Station (OPC UA)

### Introduction

The Connectivity Station allows access to the data of different WinCC stations by means of an OPC client. For this, the OPC client must simply connect to the Connectivity Station.

## 2.9 Connectivity Station for OPC UA

The exchange of data between the OPC client and the Connectivity Station takes place via the OPC UA. The WinCC OPC server "WinCCConnectivity.OPCUAServer" is integrated into the Connectivity Station.

### Requirements

- The software for the Connectivity Station is installed on the Connectivity Station PC.
- The Connectivity Station is configured in the S7 project and the project data is transferred to the computer of the Connectivity Station.
- An OPC client in accordance with the OPC specifications is available.

### The Procedure in Principle

The following description depicts the basic procedure.

1. Start the OPC client on the PC.
2. Select the OPC-Server according to the desired data.  
The names in the table above apply to WinCC OPC servers.
3. Define which data should be transferred, e.g. tags.

### Result

The OPC client is connected to the Connectivity Station and receives the WinCC data.

# Index

## A

- A&E server, 266, 268, 274, 275, 277
  - Condition Related Event, 266
  - Conditional event, 274
  - Hierarchical access, 275
  - Mapping the WinCC message system, 277
  - Mapping WinCC message classes and message types, 277
  - Simple event, 274
  - Tracking event, 266, 274
- A&E Server
  - Mapping of the WinCC message system, 268
- Access protection for SQL database, 208
- Access right, 29, 32, 33, 34
- Access via the WinCC OLE DB, 199
- Acknowledgement theory, 271
- Acknowledgment policy, 280
- ActiveX Control, 73
  - Display in Internet Explorer, 61
- Adding a tag, 210, 217
  - Example of OPC DA, 239
- Address properties, 221
- Aggregate functions for analysis, 202
- Alarm Logging, 88
- AlarmHitView, 202, 206
- ALARMVIEW, 192
- Analysis functions, 202
  - Alarm logs, 202
  - Alarm Message Archives, 206
  - Process value archives, 202
  - Recordset with the analysis of message archives, 206
- Application
  - Access Using OPC, 168
  - Access Via the WinCC OLE DB Provider, 171
- Application scenario, 164
  - Remote access to WinCC archive databases, 164
- Archive configuration, 76
- Archive Connector, 156
- Archive data, 173, 183, 192, 196
  - Access Via the WinCC OLE DB Provider, 167
  - Access via WinCC OLE DB Provider, 173
  - as reports on the network, 201
  - Configure access with Visual Basic.NET, 332, 340
  - Configuring access using DataConnector Wizard, 320
  - Configuring access with Visual Basic, 318
  - Query, 183, 192, 196

- Archive database, 179
  - Connect, 179
- Archive system, 70
- Archive tag, 76
- Area names in distributed systems, 88

## B

- Barcode, 74
- Basics
  - Connectivity Station, 344, 353
- Bounding values, 255

## C

- CAL, 90
- CCAgent, 26
- Client
  - Operating system, 19
  - Remote access, 25, 70
- Client Access License, 90
- Cluster, 63
- Color palette, 60
  - Change, 60
- CommandText, 183
- Commissioning, 317
- Communication
  - IPv4 protocol, 78
- Communication drivers, 7, 19
- Communication process, 78
- Compatibility, 55, 231
- Component, 7, 36, 44
  - Communication drivers, 7
  - Components supplied, 7
- Configuration file
  - Certificates, 307
  - Layout, 307
  - Port number, 307
  - Security settings, 307
  - Storage location, 307
  - URL of the WinCC OPC UA server, 307
  - User identification, 307
  - WinCC logging write access, 307
- configuring
  - Optimized WinCC archive write access, 313
  - Port number, 312

- Security settings, 312
- User identification, 313
- WinCC OPC UA server, 312
- Configuring
  - Connectivity Station, 349, 356
- Connection
  - Creating a connection, 210
- Connection interruption, 63
- Connection Monitoring, 214
- ConnectionString, 179
- Connectivity pack, 156
  - Archive Connector, 156
  - MS OLE DB Provider, 156
  - OPC, 156
  - WinCC OLE DB Provider, 156
- Connectivity Pack
  - Archive Connector, 175
  - Database Access, 175
  - Licensing, 90
  - Use of OLE DB interface, 347
- Connectivity Station
  - Accessing WinCC stations, 351, 358
  - Basics, 344, 353
  - configuring, 349, 356
  - Installing, 345, 354
  - License, 344, 353
  - Supported OPC Standards, 347
  - Use of OPC interface, 346, 355
- cp\_TagStatistic, 202
- Customer support, (See support)

## D

- Data type, 213
  - Supported WinCC data types, 213
  - Supported WinCC data types overview, 213
- Database Access, 175
- DataConnector, 156
- DataMonitor
  - Client, (See DataMonitor client)
  - Installation requirements, 94
- DataMonitor client, 94, 96
  - Installation, 96, 97
- DataMonitor server, 94
  - Installation, 97
- DCF file
  - Create, 71
- DCOM configuration, 58
- Defining new tag, 245
  - Example of OPC DA, 245
- Demo mode, 10
- Demo Project, 126

- DHCP server, 63
- Diagnostics
  - Support request, 153
- Diagnostics client, 110, (See WebNavigator diagnostics client)
- Disabling shortcut keys, 58
- Domain, 19
- Domain-global user group, 33
- Domains, 19
- Driver
  - Unsigned, 35

## E

- Energy-saving mode, 63
  - Network adapter, 63
- Error report, (See support)
- Event display, 49
- Example, 326, 336
  - Read message archive, 336
  - Read Process Value Archive, 326
- Example:, 318
- External application, 55
- External applications, 53

## F

- FAQ, (See support)
- File
  - Unsigned, 35
- File sharing, 29
- Filter criteria, 217
- Firewall, 26, 63
- Folder, 29, (See: Folder)
  - Released folders, 29
- Folder share, 29, (See: Folder share)
- Functionality of the OPC A&E server
  - Conditional event, 274
  - Simple event, 274
  - Tracking event, 274
- Functionality of the WinCC OPC A&E server
  - Simple event, 266

## G

- General information, 55

**H**

Hardware  
    Requirement, 94, 107  
Hardware requirement, 17

**I**

I/O field configuration, 239  
    Example of OPC DA, 239  
Image painting time, 88  
Installation, 7, 35, 36, 58, 90, 92  
    Adapting Security Policy, 35  
    Component, 36, 44  
    Connectivity Pack Client, 92  
    Connectivity Pack Server, 90  
    Domain, 19  
    Multilanguage, 58  
    Notes on installed software, 36  
    PDF files, 7  
    Performing, 36, 51  
    Performing supplementary installation, 44, 45  
    Preparing the installation, 35  
    Removing, 48  
    Requirement, 94, 107, 112  
    Requirements, 16, 17, 19  
    Security settings, 122  
    Supplementary installation of a language, 45  
    Upgrade, 114, 117  
    Upgrading an installation, 51  
    WebNavigator client, 117, 122, 123  
    WebNavigator Diagnostics Client, 125  
    WebNavigator server, 114  
Installation Guide, 7  
Installation Notes, 7  
Installed software, 36  
Installing  
    Connectivity Station, 345, 354  
Internet Explorer, 19, 61, 105, 136  
    Display ActiveX controls, 61  
    Security settings, 122  
IP address, 63  
ISDN router, 63  
Item handle, 255  
Item ID, 255

**L**

Language  
    Performing supplementary installation, 45

Languages, 87  
Layout  
    Print barcode, 74  
License, 10, 110  
    DataMonitor, 100  
    Installation, 10  
    Invalid, 101  
    Reserved WebUX license, 139  
    WebNavigator diagnostics client, 110  
License agreement, 10  
License type, 10  
Licensing  
    Connectivity Station, 344, 353  
Linked Server, 156

**M**

Manual detachment, 62  
Message archive, 183, 192  
    Access with Visual Basic.NET, 340  
    Configuring access using DataConnector, 320  
    Displaying data, 194  
    Querying archive data, 183, 192  
    Recordset, 194  
Message Archive, 336  
    Access with Visual Basic, 318, 336  
    Querying archive data, 336  
Message archive data  
    Access with Visual Basic.NET, 340  
Message classes on OPC A&E servers, 277  
Message types on OPC A&E servers, 277  
Microsoft SQL Server, 10, 12, 23, 49, 62, 201  
Microsoft Windows, 29  
    Toolbar, 25  
Microsoft Windows taskbar, 58  
Migration, 87  
Mitsubishi Ethernet  
    Information on communication, 81  
MS OLE DB, 174  
Multilanguage, 58  
    Installation, 58

**N**

Netware, 58  
    Novell Netware client, 58  
Network adapter, 63  
    Energy-saving mode, 63  
Network client, 58  
Network connection, 63  
    Speed, 63

- Network drive, 63
- Network engineering, 63
  - Access via RAS, 63
  - DHCP server, 63
  - IP address, 63
  - ISDN router, 63
  - Network adapter, 63
  - Network client, 58
  - Network server, 63
  - Notebook, 63
  - Novell client software, 58
  - Supported network protocols, 63
  - TCP/IP protocol, 63
  - WinCC in multiple domains, 63
  - WinCC within a domain, 63
- Network protocol, 63
  - Supported network protocols, 63
  - TCP/IP, 63
- Network server, 63
- New connection, 217
- New user, 234
- Notebook, 63
- Notes, 55
  - For operation, 55
- Novell Netware client, 58

## O

- OLE DB
  - Transparent access, 348
- OLE DB interface
  - Connectivity Pack, 347
- Online help
  - Internet Explorer, 105
- Online Help, 58
  - Runtime, 58
- Online support, (See support)
- OPC, 76, 156
  - Access to tag, 216
  - Adding a tag, 210, 217
  - Address properties, 221
  - Communications concept, 232
  - Compatibility, 231
  - Configuring access to a WinCC tag with the OPC Item Manager, 217
  - Configuring access to a WinCC tag without the OPC Item Manager, 221
  - Configuring an OPC channel on a WinCC OPC DA client, 216
  - Configuring structure, 223
  - Configuring structure tag, 223
  - Creating a connection, 210

- Error handling in event of disturbed OPC communication, 226
- Example, 242, 243, 244, 245, 248, 249, 250, 252
- Example:, 238, 239
- Filter criteria, 217
- Functionality of the OPC A&E server, 274
- Functionality of the WinCC OPC A&E server, 266
- Functionality of the WinCC OPC DA Client, 214
- Functionality of the WinCC OPC DA server, 235
- Functionality of the WinCC OPC HDA server, 253
- HDA server browser, 263
- Historical Data Access, 77
- New connection, 217
- New user, 234
- OPC in WinCC, 209, 232
- OPC Item Manager, 210
- OPC1, 221
- OPCServer.WinCC-(DPC\_4001), 217
- Overview of OPC Item Manager functions, 210
- Principle of operation of the WinCC OPC UA Server, 287
- ProgID, 237
- Querying of ProgID, 210
- Setting up user account on the OPC computers, 234
- Specifications, 231
- Structure properties, 223
- Supported WinCC data types, 213
- Supported WinCC data types overview, 213
- Tag selection, 210
- Trace, 317
- Transparent access, 347
- Using Multiple OPC DA Servers, 236
- Using structures on a WinCC OPC DA client, 223, 224
- WinCC as an OPC DA client, 209, 226
- WinCC as OPC XML client, 209
- OPC A&E, 77
  - OPC source, 77
- OPC A&E server, 77, 266, 269, 274, 275, 277
  - Quality codes, 282
- OPC A&E Server
  - Quality codes, 273
- OPC A&Raw Data, 273
- OPC channel
  - Configuring an OPC channel on a WinCC OPC DA client, 216
- OPC communication, 226
  - Error handling in the event of disturbed OPC DA communication, 226
- OPC DA client, 214
  - Functionality of the WinCC OPC DA Client, 214

- OPC DA server, 235
  - Functionality of the WinCC OPC DA server, 235
  - Using multiple OPC DA servers, 236
- OPC HDA server, 253
  - Assemblies, 256
  - Attributes, 256
  - Bounding values, 255
  - Data structure, 255, 256
  - Item handle, 255
  - Item ID, 255
  - Principle of operation, 253
  - Quality codes, 260, 273
  - Raw data, 253
  - Supported functions, 257
  - Time Format of a WinCC OPC HDA server, 258
  - Write Accesses, 260
- OPC interface
  - Connectivity Station, 346, 355
- OPC Item Manager, 210, 217, 237
  - Overview of OPC Item Manager functions, 210
- OPC Standards
  - supported ~ by the Connectivity Station, 347
- OPC UA
  - Conformance units, 295
  - Display of the archive tags, 298
  - Display of the WinCC tags, 297
  - Information on communication, 79
  - Profile, 295
  - Raw data tag, 79
- OPC UA Data Access, 299
- OPC UA Historical Access, 299
- OPC UA Server
  - Application certificate, 289
  - Certificate, 289
  - Communication profile, 287
  - Configuration file, 307
  - How it works, 287
  - Instance certificate, 289
  - Security policy, 288
  - supported specifications, 287
  - Trusted client certificates, 290
  - URL, 288
- OPC\_E\_MAXEXCEEDED, 77
- OPC1, 221
- OPCScout new project1
  - Example of OPC DA, 245
- OPC-Server
  - Server names, 347
- OPCServer.WinCC-(DPC\_4001), 217
- Operating system, 19, 58
  - Access rights, 29
  - Prevent access, 25

- Operation, 53
  - Domain, 19

## P

- PDF files, 7
- Picture Tree, 88
- Preferred server, 63
  - Connection interruption, 63
- Process value archive, 181, 183, 184, 326
  - Access with Visual Basic, 318, 326
  - Access with Visual Basic.NET, 332
  - Configuring access using DataConnector Wizard, 320
  - display in Visual Basic Runtime, 326
  - Displaying data, 181
  - Query, 184
  - Querying archive data, 183
  - Recordset, 181
- ProgID, 210
  - Querying, 237
  - Querying of ProgID, 210
- Project
  - Example of OPC DA, 239
  - Include in user group, 34
- Project path, (See: Folder)
- Proxy, 63

## Q

- Quality codes, 260, 273, 282
- Query, 184, 192, 196
  - Message archive, 192
  - Process value archive, 184
  - User archive, 196

## R

- RAM, (See: Work memory)
- RAS, 63
- Raw data, 253
- RDP, 82
- Recordset, 181, 194
- Redundancy, 63
  - Configuration of standard gateway, 86
  - Redundant server, 63
- Release
  - Folder, 29
- Release share, (See: Folder share)
- Remote access, 25
- Remote Desktop Protocol, 82

- Reporting Services
  - Requirements, 201
- Reports with archive data
  - Available on the network, 201
- Requirement, 16
  - Hardware, 17, 94, 107
  - Installation, 94, 107
  - Operating system, 19, 94, 107
  - Software, 19, 94, 107
- Runtime, 62
  - Displaying online help, 58
  - Server failure, 62

**S**

- S5 PROFIBUS DP
  - Information on communication, 81
- S7 Protocol Suite, 78
  - Information on communication, 78
  - Time change with AR\_SEND, 78
- S7DOS, 78
- Safety, 25, 29
- Scope of delivery, 7
- Screen, 60
- Screen resolution, 60
- Screen savers, 55
- Security Controller, 36
- Security policy, 35
- Server
  - Operating system, 19
- Server names
  - WinCC OPC-Server, 347
- Server prefix, 63
- Share, 29, (See: Folder share)
- SIMATIC 505 TCP/IP
  - Information on communication, 81
- SIMATIC HMI, 29, 32, 33, 34
  - User group, 29
- SIMATIC Manager
  - User rights, 29
- SIMATIC Security Controller, 36
- Software, 19
  - Requirement, 19, 94, 107
- SQL database, 208
- SQL master database, 62
- SQL queries
  - to WinCC databases, 199
- SQL Server, (See: Microsoft SQL Server)
- SQL Server Import/Export, 167
- SQL Server Import/Export wizard, 199
- Standard SQL queries
  - to WinCC databases, 199

- Start menu, 36
- Structure
  - Configuring structure, 223
  - Using structures on a WinCC OPC DA client, 223
  - Using WinCC OPC client, 224
- Structure properties, 223
- Structure tag, 223
  - Configuring structure tag, 223
- Supplementary installation, 44, 45
  - Languages, 45
  - Performing, 44, 45
- Support, 150, 153
- Support request, 153
- Swapped out WinCC archives on removable media, 175
- System diagnostics, 153
- System stability, 69

## T

- Tag
  - Adding a tag, 210
  - Configuring OPC Item Manager, 217, 221
  - Example of OPC DA, 245, 248, 252
  - HDA server browser, 263
  - OPC Item Manager, 217
  - R, 184
  - Tag selection, 210
- Tags with @ prefix, 87
- TCP/IP protocol, 63
- Technical support, (See support)
- Terminal bus
  - Large amounts of data, 75
- Terminal service, 112
- the Connectivity Station
  - Accessing WinCC station via, 351, 358
- The WinCC Station
  - Access ~ via the Connectivity Station, 351, 358
- Time synchronization, 70
- TIMESTEP, 184
- Toolbar, 25
- Transparent access
  - with OLE DB, 348
  - with OPC, 347

## U

- Uninstalling, 48
  - Performing, 48
- Uninterruptible power supply, 63
- Unsigned driver, 35

- Unsigned file, 35
- Upgrade, 114, 117
- Upgrade installation, 10, 51
  - Performing, 51
- UPS, 63
- URL
  - OPC UA Server, 288
- Use
  - OLE DB interface of the Connectivity Pack, 347
  - OPC interface of the Connectivity Station, 346, 355
- Use case, 161, 162, 163, 165, 166
  - Access to local WinCC Archive Database, 163
  - Access to local WinCC RT Database, 161
  - Access to local WinCC user archives, 165
  - Access Via the WinCC OLE DB Provider, 167
  - Remote Access to WinCC RT Databases, 162
  - Remote Access to WinCC User Archives, 166
- User account, 234
  - Making OPC computers known, 234
- User archive, 196, 198
  - Displaying data, 198
  - Querying archive data, 196
- User authorization, 88
- User group, 29
  - Domain-global user group, 33
  - Include project, 34
  - SIMATIC HMI, 29, 32, 33, 34

## V

- VBA, 75
- Virtualization, 18
- Virus scanner, 55
- Visual Basic, 318
  - Access to Archive Data, 318
- Visual Basic .NET, 332, 340
  - Access to Archive Data, 332, 340

## W

- Web client, (See WebNavigator client)
- WebNavigator
  - Demo Project, 126
  - DVD contents, 107
  - Installation requirements, 107
  - Licenses, 110
- WebNavigator client, 107, 123
  - Installation, 117
  - Installation under the Windows Server, 117

- Licenses, 110
- Upgrade, 117
- WebNavigator diagnostics client, 107
- WebNavigator Diagnostics Client
  - Installation, 125
- WebNavigator server, 107
  - Installation, 114
  - Licenses, 110
  - Upgrade, 114
- WebUX
  - Installation, 140
  - Licensing, 138, 140
  - Reserve license, 139
- WinCC, 63, 68
  - as OPC DA client, 209, 226
  - as OPC XML client, 209
  - General information, 68
  - Installation, 7, 16, 35
  - Installation requirements, 17, 19
  - Limit access, 29
  - Notebook, 63
  - OPC in WinCC, 209, 226, 232
  - Performing installation, 36
  - Performing supplementary installation, 44, 45
  - Preparing the installation, 35
  - Remote access, 25
  - Removing, 48
  - upgrade, 50
  - Upgrading an installation, 51
  - Use in multiple domains, 63
  - Use within a domain, 63
  - WinCC DVD, 7
- WinCC - Microsoft Excel Connection, 249
  - Example of OPC DA, 249
- WinCC - SIMATIC NET FMS OPC server connection, 242
  - Example of OPC DA, 242
- WinCC - SIMATIC NET S7 OPC server connection, 244
  - Example of OPC DA, 244
- WinCC - WinCC connection, 238
  - Example of OPC DA, 238
- WinCC Archive Connector, 156, 175
- WinCC DataConnector, 156
- WinCC DataMonitor client, (See DataMonitor client)
- WinCC DataMonitor server, (See DataMonitor Server)
- WinCC DVD, 7
- WinCC Explorer-OPC\_Client.MPC, 237
- WinCC message system
  - Attributes, 270, 279
  - Mapping WinCC Message Classes and Message Types, 269

- on OPC A&OPC-A&WinCC message system, 268
  - WinCC Message Classes on OPC A&E Server, 269
- WinCC OLE DB, 174
  - basics, 174
  - Microsoft, 174
  - WinCC, 174
- WinCC OLE DB Provider, 156, 173
  - Access to Archive Data, 173
  - Linked Server, 156
  - SQL Server, 156
- WinCC OPC A&E server
  - Hierarchical access, 275
- WinCC OPC UA server, 287
  - configuring, 312
  - Discovery Server, 288
- WinCC OPC-Server
  - Server names, 347
- WinCC project
  - Include in user group, 34
- WinCC ServiceMode, 88
- WinCC V6.x, 50
- WinCC WebNavigator, (See: WebNavigator)
- WinCC/WebNavigator client, (See WebNavigator client)
- WinCC/WebNavigator server, (See WebNavigator server)
- WinCC-OPC-UA
  - Information on communication, 79
- Windows, 19, 29
  - Access rights, 29
  - Operation under Windows, 53
  - Preparation the installation of WinCC, 35
  - Security policy, 35
  - Toolbar, 25
  - User rights, 29
- Windows 7, 19
- Windows 8.1, 19
- Windows event display, 49
- Windows Server 2012, 19
- Windows start menu, 36
- Windows taskbar, 58
  - Prevent display, 58
- Work memory, 17