SIEMENS

SIMATIC HMI

WinCC Unified
OPC UA - Open Platform Communications

System Manual

Online documentation

11/2023
Online documentation

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.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: Online documentation
Ⓟ 11/2023 Subject to change

Copyright © Siemens 2023.
All rights reserved

Table of contents

Introduction

1

1.1 Principle

OPC is a standardized manufacturer-independent software interface for data exchange in automation engineering.

OPC UA is the technology succeeding OPC. OPC UA is platform-independent and supports different protocols as communication medium.

1.2 OPC UA specifications and compatibility

Overview

OPC UA specifies interfaces to gain access to the following objects in WinCC Unified:

- Process values (OPC UA 1.04)
- Tag-based alarms (OPC UA 1.04)

For detailed information about the individual OPC specifications, refer to the website of the OPC Foundation (http://www.opcfoundation.org).

Compatibility

Interoperability with OPC products from other manufacturers is guaranteed by participation in "OPC Interoperability Workshops".

Using OPC UA certificates 2

2.1 Introduction to OPC UA certificates

Introduction

Communication between an OPC UA server and its OPC UA clients that is protected by certificates requires the following:

- A valid OPC UA server certificate is installed on the server and a valid OPC UA client certificate is installed on the clients.
- The client devices trust the OPC UA server certificate and vice versa.

The type of the certificate used determines how the trust is established between OPC UA server and OPC UA clients:

- When a communication partner uses a certificate issued by a certificate authority (CA) and the other communication partners trust the root certificate of the certificate authority, they automatically trust the OPC UA certificate.

  Note

  Support of external certificate authorities

  The OPC UA certificate of a Unified device cannot be issued by an external certificate authority. The WinCC Unified Certificate Manager tool is required to create the root certificate and the OPC UA certificate.

- When a communication partner uses a self-signed OPC UA certificate, the other communication partners must explicitly trust this certificate.

  Note

  Restriction for self-signed Unified OPC UA server and client certificates

  A self-signed default certificate is generated for the Unified OPC UA server:

  - Unified PC: When installing Runtime on the PC
  - Unified Comfort Panel: When starting Runtime if no OPC UA server certificate is found in the certificate store

  In order not to use a certificate issued by a certification authority for a Unified OPC UA server, use this certificate.

  The use of a self-signed OPC UA client certificate is not possible for Unified OPC UA clients.

How you proceed to create the trust relationship on a Unified device also depends on whether you are using the Unified device as an OPC UA server or client.

If you are using a Unified device as a client, the engineering system also acts as an OPC UA client during configuration of the device.

Provision of the certificates

The following sections describe how to provide the certificates:

	Used as	Section
Unified PC	OPC UA server	Using root certificates (Unified PC as OPC UA server) (Page 9) Using self-signed certificates (Unified PC as OPC UA server) (Page 11)
	OPC UA client	Using root certificates (Unified PC as OPC UA client) (Page 12)
Unified Comfort Panel	OPC UA server	Using root certificates (UCP as OPC UA server) (Page 14) Using self-signed certificates (UCP as OPC UA server) (Page 16)
	OPC UA client	Using root certificates (UCP as OPC UA client) (Page 17) Using self-signed certificates (UCP as OPC UA client) (Page 19)
Engineering System	OPC UA client	Providing certificates for the engineering systems as OPC UA client (Page 20)

Unified tools

When you use certificates issued by a certificate authority, the following tools support you in providing the certificates:

Task	Device	Tool
Creating the root certificate of the Unified OPC UA device (if not already done)	Unified PC that is used as certification authority for the Unified OPC UA device	WinCC Unified Certificate Manager
Creating a Unified OPC UA certificate		
Installing the • Unified root certificate (if not yet done) • Unified OPC UA certificate	Unified PC that is used as OPC UA device	WinCC Unified Certificate Manager
	Unified Comfort Panel that is used as OPC UA device	Control Panel > Security > Certificates
Distribute Unified root certificate and its CRL file to the OPC UA communication partners	Unified PC that is used as certificate authority for the Unified OPC UA device[1]	WinCC Unified Certificate Manager
Import the root certificate of the OPC UA communication partner and its CRL file	Unified PC that is used as OPC UA device	SIMATIC Runtime Manager
	Unified Comfort Panel that is used as OPC UA device	Control Panel > Security > Certificates

[1] If the OPC UA device is a Unified PC, you can alternatively distribute the root certificate and CRL file directly on the device using SIMATIC Runtime Manager.

When you use self-signed OPC UA certificates, the following tools support you in providing the certificates:

Task	Device	Tool
Importing or trusting the certificate of the communication partner	OPC UA Unified PC	SIMATIC Runtime Manager
	OPC UA Unified Comfort Panel	Control Panel > Security > Certificates

Note

Operation of the Certificate Manager and Runtime Manager

For more detailed information on operating the Certificate Manager and the Runtime Manager, refer to the Runtime online help.

Certificate store of Unified devices

The OPC UA certificates are stored in the certificate store of the Unified device.

For Unified PC: `C:\ProgrammData\SCADAProjects\certstore`

2.2 Providing certificates on a Unified PC

2.2.1 Using a Unified PC as OPC UA server

2.2.1.1 Using root certificates (Unified PC as OPC UA server)

This section describes how you provide the certificates for the following case:

- A Unified PC is used as OPC UA server.

Note

Operating Certificate Manager and Runtime Manager

For more detailed information on operating the Certificate Manager and the Runtime Manager, refer to the Runtime online help.

Requirement

- A root certificate was generated on the Unified PC that serves as certificate authority.

Sequence

The following steps are included in providing the certificates:

1. Generate the OPC UA server certificate and export its certificate configuration.
2. Install the certificate configuration on the Unified OPC UA server.
3. Trust the OPC UA client on the Unified OPC UA server.
4. Trust the Unified OPC UA server on the OPC UA client.

Generating the server certificate and exporting the certificate configuration

1. Open the Certificate Manager on the Unified PC that serves as certificate authority.
2. Generate a OPC UA server certificate for the Unified PC that is used as OPC UA server.
3. Export the certificate configuration to an external data storage medium.
   This step can be omitted when the device that serves as certificate authority is also used as OPC UA server.

Installing the certificate configuration on the Unified OPC UA server

1. Connect the Unified PC that is used as OPC UA server to the external data storage medium.
   This step can be omitted when the device that serves as certificate authority is also used as OPC UA server.
2. Install the certificate configuration on the PC using the Certificate Manager.

The following certificates are installed:

- The root certificate including CRL file
- The OPC UA server certificate

Trusting the OPC UA client on the Unified OPC UA server

1. Save the root certificate of the OPC UA client and its CRL file (Certificate Revocation List) to an external data storage medium.
2. Connect the Unified PC that is used as OPC UA server to the external data storage medium.
3. Open the Runtime Manager on the Unified PC.
4. Import the root certificate of the OPC UA client.
   The root certificate is imported and classified as trusted.
5. Import the associated CRL file.

The Unified OPC UA server trusts the OPC UA client certificate when the next connection attempt is made.

Trusting the Unified OPC UA server on the OPC UA client

1. Ppen the Certificate Manager on the Unified PC that serves as the certification authority of the Unified OPC UA server.
2. In the Certificate Manager, export the root certificate and its CRL file (Certificate Revocation List) to an external data storage medium.

Note

Alternative

On the Unified PC that is used as OPC UA server, use the Runtime Manager to export the root certificate and CRL file.

3. Connect the OPC UA client to the external data storage medium.
4. Copy both files in the certificate store of the OPC UA client into the folder for trusted certificates. To do this, proceed as described in the application help of the client.

The OPC UA client accepts the Unified OPC UA server certificate when the next connection attempt is made.

2.2.1.2 Using self-signed certificates (Unified PC as OPC UA server)

This section describes how you provide the certificates for the following case:

- A Unified PC is used as OPC UA server.
- The OPC UA certificates of the OPC UA server and the client are self-signed.

Note

Operating the Runtime Manager

For more detailed information on operating the Runtime Manager, refer to the Runtime online help.

Sequence

1. Trust the OPC UA client on the Unified PC.
2. Trust the self-signed default certificate of the Unified OPC UA server on the OPC UA client.

Trusting the OPC UA client on the Unified OPC UA server

After the first connection attempt

If a connection attempt has already been made between the client and server, the self-signed OPC UA client certificate is available on the Unified PC in the certificate store in the "untrusted" folder.

Follow these steps:

1. Open the Runtime Manager on the Unified PC.
2. Trust the OPC UA client certificate in the Runtime Manager.

The certificate is moved to the "trusted" folder in the certificate store of the Unified PC. The Unified PC accepts the OPC UA client certificate when the next connection attempt is made.

Before the first connection attempt

To trust the self-signed certificate before a connection has been established between server and client, follow these steps:

1. Save the certificate of the OPC UA client to an external data storage medium.
2. Connect the Unified PC to the external data storage medium.

3. Open the Runtime Manager on the Unified PC.
4. Import the OPC UA client certificate.

During the import, the certificate is automatically copied to the "trusted" folder of the certificate store. The Unified PC trusts the OPC UA client certificate when the next connection attempt is made.

Trusting the Unified OPC UA server on the OPC UA client

You use the self-signed default certificate of the Unified OPC UA server.

After the first connection attempt

If a connection attempt has already been made between the client and server, the self-signed OPC UA server certificate is available on the client in the certificate store in the rejected certificates.

Copy the certificate to the certificate store for trusted certificates. To do this, proceed as described in the application help of the client.

The OPC UA client accepts the Unified OPC UA server certificate when the next connection attempt is made.

Before the first connection attempt

To trust the self-signed certificate before a connection has been established between server and client, follow these steps:

1. Copy the self-signed OPC UA server certificate on the Unified PC from the following folder to an external data storage medium:
   `<Certificate store>own\certs`
2. Connect the OPC UA client to the external data storage medium.
3. Copy the certificate to the certificate store for trusted certificates. To do this, proceed as described in the application help of the client.

The OPC UA client accepts the OPC UA server certificate when the next connection attempt is made.

2.2.2 Using a Unified PC as OPC UA client

2.2.2.1 Using root certificates (Unified PC as OPC UA client)

This section describes how you provide the certificates for the following case:

- A Unified PC is used as OPC UA client.
- The OPC UA certificates of the OPC UA server and the client are issued by a certificate authority.

Note

Operating Certificate Manager and Runtime Manager

For more detailed information on operating the Certificate Manager and the Runtime Manager, refer to the Runtime online help.

Requirement

- A root certificate was generated on the Unified PC that serves as certificate authority.

Sequence

The following steps are included in providing the certificates:

1. Generate the OPC UA client certificate and export its certificate configuration.
2. Install the certificate configuration on the OPC UA client.
3. Trust the OPC UA server on the Unified OPC UA client.
4. Trust the Unified OPC UA client on the OPC UA server.

Generating the client certificate and exporting the certificate configuration

1. Open the Certificate Manager on the Unified PC that serves as certificate authority.
2. Generate a OPC UA client certificate for the Unified PC that is used as OPC UA client.
3. Export the certificate configuration to an external data storage medium.
   This step can be omitted when the device that serves as certificate authority is also used as OPC UA client.

Installing the certificate configuration on the Unified OPC UA client

1. Connect the Unified PC that is used as OPC UA client to the external data storage medium.
   This step can be omitted when the device that serves as certificate authority is also used as OPC UA client.
2. Install the certificate configuration on the PC using the Certificate Manager.

The following certificates are installed:

- The root certificate including CRL file
- The OPC UA client certificate.

Trusting the OPC UA server on the Unified OPC UA client

1. Save the root certificate of the OPC UA server and its CRL file (Certificate Revocation List) to an external data storage medium.
2. Connect the Unified PC that is used as OPC UA client to the external data storage medium.
3. Open the Runtime Manager on the Unified PC.

4. Import the root certificate of the OPC UA server.
5. Import the associated CRL file.

The Unified OPC UA client trusts the OPC UA server certificate when the next connection attempt is made.

Trusting the Unified OPC UA client on the OPC UA server

1. Open the Certificate Manager on the Unified PC that serves as the certificate authority of the Unified OPC UA client.
2. In the Certificate Manager, export the root certificate and its CRL file (Certificate Revocation List) to an external data storage medium.

Note

Alternative

On the Unified PC that is used as OPC UA client, use the Runtime Manager to export the root certificate and CRL file.

3. Connect the OPC UA server to the external data storage medium.
4. Copy both files to the certificate store for trusted certificates. To do this, proceed as described in the application help of the server.

The OPC UA server accepts the Unified OPC UA client certificate when the next connection attempt is made.

2.3 Providing certificates on a Unified Comfort Panel

2.3.1 Use the Unified Comfort Panel as an OPC UA server

2.3.1.1 Using root certificates (UCP as OPC UA server)

This section describes how you provide the certificates for the following case:

- A Unified Comfort Panel is used as OPC UA server.
- The OPC UA certificates of the OPC UA server and the client are issued by a certificate authority.

Note

Operating the Certificate Manager

For more detailed information on operating the Certificate Manager, refer to the Runtime online help.

Requirement

- A root certificate was generated on the Unified PC that serves as certificate authority.

Sequence

The following steps are included in providing the certificates:

1. Generate the OPC UA server certificate and export its certificate configuration.
2. Install the certificate configuration on the Unified OPC UA server.
3. Trust the OPC UA client on the Unified OPC UA server.
4. Trust the Unified OPC UA server on the OPC UA client.

Generating the server certificate and exporting the certificate configuration

1. Open the Certificate Manager on the Unified PC that serves as certificate authority.
2. Generate an OPC UA server certificate for the Unified Comfort Panel that is used as OPC UA server.
3. Export the certificate configuration to an external data storage medium.
   The root certificate, its CRL file and the OPC UA Server certificate are exported in encrypted format.

Installing the certificate configuration on the Unified OPC UA server

1. If Runtime starts on the Panel that is used as OPC UA server and no OPC UA server certificate is found, a self-signed default certificate is generated.
   Delete the default certificate. Follow these steps:
   - Select "Security > Certificates" in the Control Panel on the Panel.
   - Select the "My Certificates" entry from the "Certificate store" list.
   - Select the OPC UA server default certificate.
   - Click "Delete".
2. Connect the Panel to the external data storage medium onto which you have exported the certificate configuration.
3. Install the root certificate and the OPC UA server certificate.
   For both certificates, follow these steps:
   - Select "Security > Certificates" in the Control Panel on the Panel.
   - Click the "Import" button.
   - In the "Import certifcates" dialog, select the certificate from the external storage medium.
   - Enter the password and the iteration specified during the export in the Certificate Manager.
   - Confirm your entries.

The following certificates are installed:

- The root certificate including CRL file
- The OPC UA server certificate

Trusting the OPC UA client on the Unified OPC UA server

1. Save the root certificate of the OPC UA client and its CRL file (Certificate Revocation List) to an external data storage medium.
2. Connect the Unified Comfort Panel to the external data storage medium.
3. Select "Security > Certificates" in the Control Panel on the Panel.
4. Click the "Import" button.
5. In the "Import certifcates" dialog, select the certificate from the external storage medium.
6. Confirm your entries.

The root certificate and its CRL are imported and classified as trusted.

The Unified OPC UA server trusts the OPC UA client certificate when the next connection attempt is made.

Trusting the Unified OPC UA server on the OPC UA client

1. Open the Certificate Manager on the Unified PC that serves as the certificate authority of the panel.
2. In the Certificate Manager, export the root certificate and its CRL file (Certificate Revocation List) to an external data storage medium.
3. Connect the OPC UA client to the external data storage medium.
4. Copy both files to the certificate store for trusted certificates. To do this, proceed as described in the application help of the client.

The OPC UA client accepts the Unified OPC UA server certificate when the next connection attempt is made.

2.3.1.2 Using self-signed certificates (UCP as OPC UA server)

This section describes how you provide the certificates for the following case:

- A Unified Comfort Panel is used as OPC UA server.
- The OPC UA certificates of the OPC UA server and the client are self-signed.

Sequence

1. Trust the OPC UA client on the Unified Comfort Panel.
2. Trust the self-signed default certificate of the Unified OPC UA server on the OPC UA client.

Trusting the OPC UA client on the Unified OPC UA server

After the first connection has been established between server and client, the self-signed OPC UA client certificate is available on the Unified Comfort Panel. The Panel does not yet trust the certificate. Follow these steps:

1. Select "Security > Certificates" in the Control Panel on the Panel.
2. Select the "Other Certificates" entry from the "Certificate store" list.
3. Select the OPC UA client certificate.
   The certificate has the status "Untrusted".
4. Click "Trust".

The Unified Comfort Panel accepts the OPC UA client certificate when the next connection attempt is made.

Trusting the Unified OPC UA server on the OPC UA client

You use the self-signed default certificate of the Unified OPC UA server.

After the first connection is established between the server and client, the self-signed certificate of the OPC UA server is available on the OPC UA client. The client does not yet trust the certificate.

Trust the Unified OPC UA server certificate on the OPC UA client.

The client accepts the server certificate the next time it attempts to connect.

2.3.2 Use the Unified Comfort Panel as an OPC UA client

2.3.2.1 Using root certificates (UCP as OPC UA client)

This section describes how you provide the certificates for the following case:

- A Unified Comfort Panel is used as OPC UA client.
- The OPC UA certificates of the OPC UA server and the client are issued by a certificate authority.

Note

Operating the Certificate Manager

For more detailed information on operating the Certificate Manager, refer to the Runtime online help.

Requirement

- A root certificate was generated on the Unified PC that serves as certificate authority.

Sequence

The following steps are included in providing the certificates:

1. Generate the OPC UA client certificate and export its certificate configuration.
2. Install the certificate configuration on the Unified OPC UA client.
3. Trust the OPC UA server on the Unified OPC UA client.
4. Trust the Unified OPC UA client on the OPC UA server.

Generating the client certificate and exporting the certificate configuration

1. Open the Certificate Manager on the Unified PC that serves as certificate authority.
2. Generate an OPC UA client certificate for the Unified Comfort Panel that is used as OPC UA client.
3. Export the certificate configuration to an external data storage medium.

Installing the certificate configuration on the Unified OPC UA client

1. Connect the Panel to the external data storage medium onto which you have exported the certificate configuration.
2. Install the root certificate and the OPC UA Client certificate.
   For both certificates, follow these steps:
   - Select "Security > Certificates" in the Control Panel on the Panel.
   - Click the "Import" button.
   - In the "Import certifcates" dialog, select the certificate from the external storage medium.
   - Enter the password and the iteration specified during the export in the Certificate Manager.
   - Confirm your entries.

   The following certificates are installed:
   - The root certificate including CRL file
   - The OPC UA client certificate.

Trusting the OPC UA server on the Unified OPC UA client

1. Save the root certificate of the OPC UA server and its CRL file (Certificate Revocation List) to an external data storage medium.
2. Connect the Unified Comfort Panel that is used as Unified OPC UA client to the external data storage medium.
3. Select "Security > Certificates" in the Control Panel on the Panel.
4. Click the "Import" button.
5. In the "Import certificates" dialog, select the certificate from the external storage medium.
6. Confirm your entries.

The root certificate and its CRL are imported and classified as trusted.

The Unified OPC UA client trusts the OPC UA server certificate when the next connection attempt is made.

Trusting the Unified OPC UA client on the OPC UA server

1. Open the Certificate Manager on the Unified PC that serves as the certificate authority of the panel.
2. In the Certificate Manager, export the root certificate and its CRL file (Certificate Revocation List) to an external data storage medium.
3. Connect the OPC UA server to the external data storage medium.
4. Copy both files to the certificate store for trusted certificates. To do this, proceed as described in the application help of the server.

The OPC UA server accepts the Unified OPC UA client certificate when the next connection attempt is made.

2.3.2.2 Using self-signed certificates (UCP as OPC UA client)

This section describes how you provide the certificates for the following case:

- A Unified Comfort Panel is used as OPC UA client.
- The OPC UA server certificate is self-signed.
- The OPC UA client certificate is issued by a certificate authority.

Note

No use of self-signed Unified OPC UA client certificates

The use of a self-signed OPC UA client certificate is not possible for a Unified OPC UA client.

Sequence

1. Generate your own self-signed OPC UA client certificate for the Unified Comfort Panel.
2. Install the self-signed certificate on the Panel.
3. Trust the OPC UA server on the Unified OPC UA client.
4. Trust the Unified OPC UA client on the OPC UA server.

Trusting the OPC UA server on the Unified OPC UA client

After the first connection has been established between the server and client, the self-signed OPC UA server certificate is available on the Unified Comfort Panel. The Panel does not yet trust the certificate. Follow these steps:

1. Select "Security > Certificates" in the Control Panel on the Panel.
2. Select the "Other Certificates" entry from the "Certificate store" list.

3. Select the OPC UA server certificate.
   The certificate has the status "Untrusted".
4. Click "Trust".

The Unified Comfort Panel accepts the OPC UA server certificate when the next connection attempt is made.

Trusting the Unified OPC UA client on the OPC UA server

1. Open the Certificate Manager on the Unified PC that serves as the certificate authority of the panel.
2. In the Certificate Manager, export the root certificate and its CRL file (Certificate Revocation List) to an external data storage medium.
3. Connect the OPC UA server to the external data storage medium.
4. Copy both files to the certificate store for trusted certificates. To do this, proceed as described in the application help of the server.

The OPC UA server accepts the Unified OPC UA client certificate when the next connection attempt is made.

2.4 Providing certificates for the engineering systems as OPC UA client

Engineering system as an OPC UA client

If the engineering system acts as an OPC UA client, provide the certificates as follows:

- When the connection is first established, the client certificate is created automatically and transferred to the server.

  Note

  Trust the client certificate

  Move the client certificate on the server from the "untrusted" folder to the "trusted" folder.

- The engineering system automatically receives the server certificate and trusts it without your having to take any action.

WinCC Unified OPC UA server 3

3.1 General information about Unified OPC UA servers

3.1.1 Using the WinCC Unified OPC UA server

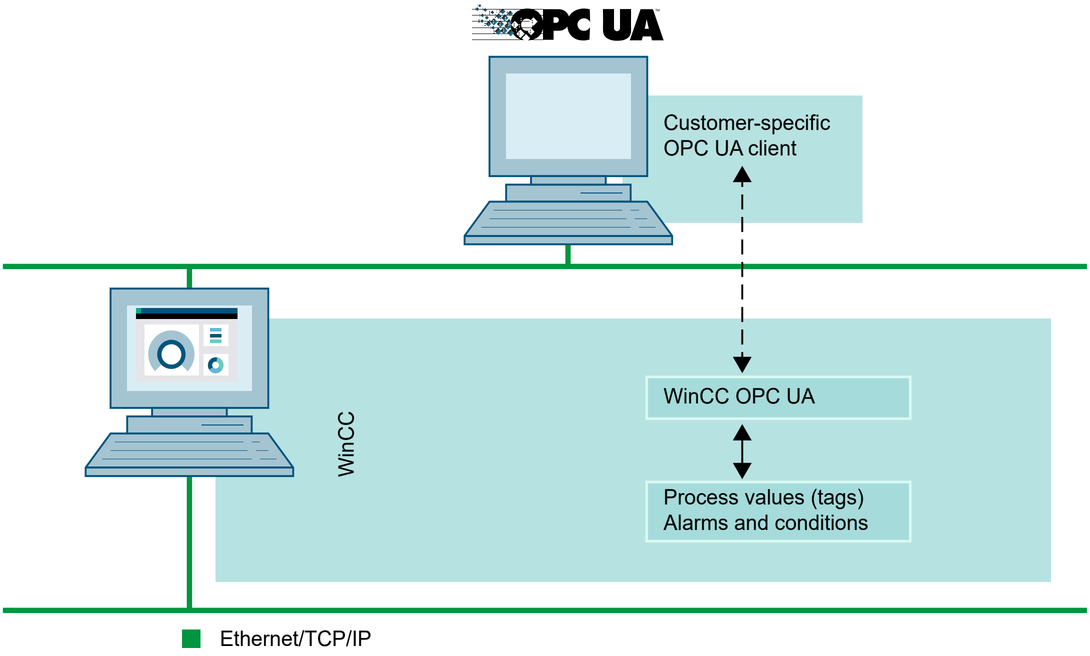
Introduction

Servers are available for the following OPC UA interfaces in WinCC Unified:

- OPC Unified Architecture: Access to the data management of WinCC Unified.

OPC UA communications concept of WinCC Unified

The figure below shows the OPC UA communication concept of WinCC Unified:



Licensing

OPC server	Licensing
WinCC OPC UA Server	A valid Runtime license for WinCC Unified

3.1.2 Requirements for use

Windows firewall settings (Unified PC as OPC UA server)

After installation of WinCC Unified, the Windows firewall settings of the OPC UA servers of WinCC Unified are correctly configured.

If OPC UA clients access OPC UA servers in different subnets, you must adapt the configuration of the permitted network areas to the OPC UA servers.

TIA Portal settings

In order to work with OPC UA in WinCC Unified, the OPC UA server must be enabled in the TIA Portal.

To do to this, select the "Operate as OPC UA server" option in the runtime settings under "OPC UA server > General". As soon as the option is selected, you can make additional settings.

More information is available under Configuring a Unified OPC UA server (Unified PC) (Page 35) and Using the Unified Comfort Panel as OPC UA server (Page 38).

3.1.3 Operating principle of the OPC UA server

How it works

The OPC UA server provides the following values:

- Process values
- Tag-based alarms

The OPC UA server supports only the "UA-TCP UA-SC UA Binary" communication profile. The used port number is adjustable.

You can find more information about configuration of the OPC UA server here:

- For Unified PC: In the section "Configuring a Unified OPC UA server (Unified PC) (Page 35)"
- For Unified Comfort Panel: In the section "Configuring the Unified OPC UA server (UCP) (Page 38)"

Supported specifications

OPC UA Architecture is a specification for the transmission of process values and alarms. The OPC UA server supports the OPC UA specification 1.04.

For more information about supported OPC UA functions, refer to "OPC UA specifications and compatibility (Page 5)".

Starting the OPC UA server

The OPC UA server is run automatically when Runtime is started after successful configuration in the TIA Portal.

URL of the OPC UA server

You can reach the OPC UA server via the following URL:

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

Parameter	Description
HostName	Placeholder for the computer name. Is used automatically.
Port	Specifies the port number. "4890" is set by default. Do not use a port number that is already assigned to another application.

Discovery Server (Unified PC as OPC UA server)

The "Discovery Server" is available by the OPC foundation. The "Discovery Server" is by default installed on the HMI device as Windows service.

The "Discovery Server" makes information available to UA clients about OPC UA servers that are subscribed to the "Discovery Server".

The OPC UA server registers itself at the start of Runtime to no, one or more configured and available "Discovery Servers" depending on its configuration. Registration is then repeated cyclically. When you end Runtime, the OPC UA server is automatically logged off from the "Discovery Server".

You can find information on disabling the OPC UA Local Discovery Server in Siemens Industry Online Support (https://support.industry.siemens.com/cs/document/109749461/how-do-you-disable-the-opcua-local-discovery-server-service-for-wincc-v7-and-wincc-tia-portal-?dti=0&lc=en-WW) (Entry ID 109749461).

Supported languages in the WinCC Unified address area

The OPC UA server supports the WinCC Unified address area in the following languages:

- English

3.1.4 Security concept of OPC UA

Introduction

The OPC UA security concept is based on:

- Authentication and authorization of the participating applications and users
- Ensuring the integrity and confidentiality of messages exchanged between the applications.

Certificates

Certificates represent the authentication mechanism of OPC UA applications. Each application has its own instance certificate and thereby identifies itself within the public key infrastructure.

Instance certificate of the OPC UA server

Each OPC UA server for secure operation requires a separate instance certificate with a private key. The certificate is only valid on the respective computer and may be used only by the OPC UA server installed there.

When you install the server, a self-signed instance certificate of the server is created and stored in the certificate folder of the server.

The private key for this certificate is only stored in the certificate store. Access to the folder with the private key must be restricted to:

- The server itself (account of the local system)
- The system administrator

NOTICE

Restricted access to the private key folder

Except for the server and the system administrator, no other users and applications may have access to the private key of the OPC UA server for security reasons.

Restricted access to the private key is therefore pre-configured after installing WinCC Unified.

The instance certificate generated during installation and the associated private key can be replaced by the system administrator. In accordance with the respective security concept of the plant, the new instance certificate may be self-signed or created by a certification authority.

The certificate and the private key are stored under this folder:
"C:\ProgramData\SCADAProjects\Certstore\own".

The private key is stored in the subfolder "private".

Validation of the server instance certificate

The instance certificate of the server is validated during the start of the OPC UA server. If the public key or the private key cannot be found or if the certificate is invalid (for example, because it has expired or is corrupt), the server stops and an appropriate entry is made in the trace log.

Trusted client certificates

The OPC UA server supports secure communication to trusted clients only. A client is trusted:

- when the client has a valid self-signed certificate that is located in the certificate store of trusted certificates of the OPC UA server
- or if the valid client certificate was issued by a certification authority. The valid certificate of the certification authority must be located in the certificate store of the trustworthy certification authorities of the OPC UA server. In this case, only the certificate from the certification authority is required. The instance certificate of the client does not need to be in the certificate store of trusted certificates.

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.

Trusted certificates are stored in the directory "C:\ProgramData\SCADAProjects\Certstore\Trusted\certs".

The certificates from certificate authorities that are required for the verification of a client certificate chain are also stored in the certificate store of the certificate authorities.

Client certificates not accepted

When a OPC UA client accesses the OPC UA server without its trusted certificate, the OPC UA server rejects secure communication and copies the client certificate to the folder for rejected certificates. These certificates are stored in the directory "C:\ProgramData\SCADAProjects\Certstore\Trusted\untrusted".

To enable secure communication with this client, you will have to move the rejected certificate to the certificate memory for trusted certificates.

3.1.5 Supported OPC UA services and profiles

OPC UA services

The following table sets out the functionality supported by OPC UA server 1.04:

OPC UA Service Sets	Services	Comment
Discovery Service Set	FindServers GetEndpoints	-
Secure Channel Service Session Service Set	All	-
View Service Set	Browse BrowseNext	Determination of the WinCC Unified data shown: Process values and archived data

OPC UA Service Sets	Services	Comment
Attribute Service Set	Read Write	only WinCC Unified tags only WinCC Unified tags
Subscription Service Set	CreateSubscription SetPublishingMode Publish RePublish DeleteSubscription	
MonitoredItem Service Set	CreateMonitoredItems SetMonitoringMode DeleteMonitoredItems	only "Value" attribute of the WinCC Unified tags .EventNotifier during access to WinCC Unified alarms

OPC UA profiles and Conformance Units

The OPC UA server supports the following OPC UA 1.03 profiles without restrictions:

- 6.5.5 Base Server Behavior Facet
- 6.5.16 Standard Event Subscription Server Facet
- 6.5.131 UA TCP UA SC UA Binary
- 6.5.148 SecurityPolicy - Basic128Rsa15
- 6.5.149 SecurityPolicy - Basic256
- 6.5.150 SecurityPolicy - Basic256SHA256

The OPC UA server supports the following OPC UA profiles shown in the following table with restrictions:

Profile	"Group"	Not supported "Conformance Unit"
6.5.11 Standard DataChange Subscription Server Facet Subscription Server Facet	Monitored Item Services	ModifyMonitoredItems DeadBand Filter Monitor MinQueueSize_02
6.5.12 Enhanced DataChange Subscription Server Facet	Monitored Item Services	Monitor MinQueueSize_05
6.5.2 Core Server Facet	Attribute Services	Attribute Write Index
6.5.14 Data Access Server Facet	Data Access	Data Access Analog Data Access Multistate Data Access PercentDeadBand Data Access Semantic Changes Data Access Two State
6.5.55 Standard UA Server Profile	Attribute Services	Attribute Write StatusCode & TimeStamp
6.5.55 Standard UA Server Profile	Attribute Services	Attribute Write StatusCode & Timestamp

Profile	"Group"	Not supported "Conformance Unit"
6.5.16 Standard Event Subscription Server Facet	Event Access	Base Info EventQueueOverflowEventType Base Info Progress Events Base Info SemanticChange Base Info System Status Base Info System Status underlying system Base Info Device Failure
6.5.17 Address Space Notifier Server Facet	Event Access	
6.5.18 A & C Base Condition Server Facet	Alarms and Conditions	
6.5.20 A & C Address Space Instance Server Facet	Alarms and Conditions	
6.5.21 A & C Enable Server Facet	Alarms and Conditions	
6.5.22 A & C Alarm Server Facet	Alarms and Conditions	A & C Comment A & C Discrete A & C OffNormal A & C SystemOffNormal A & C Trip
6.5.23 A & C Acknowledgeable Alarm Server Facet	Alarms and Conditions	

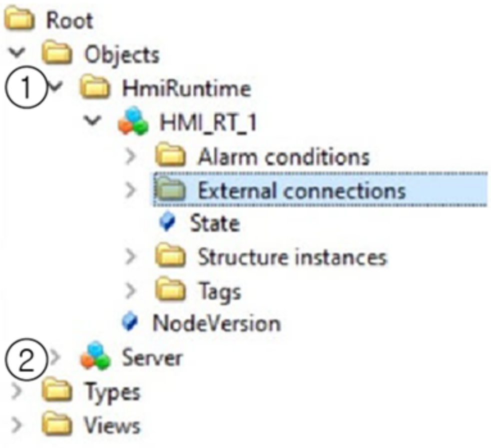
3.1.6 Address space of the OPC UA server

Introduction

A WinCC Unified device that is used as an OPC UA server makes the following runtime data of its system available to its OPC UA clients in its address space:

- Process values (WinCC Unified tags)
- Alarms (tag-based WinCC Unified alarms)

The address space of the OPC UA server is added below "Root > Objects" and has the following hierarchical structure:



① The folder for the Runtime system node
Folders for the alarm conditions and tags of the system are located under the node.
The structure in the tags folder corresponds to the structure of the tags in WinCC Unified.

② The server node

Mapping of the WinCC Unified tag

Connections are displayed by OPC UA objects of the "HMIConnectionType" type.

Internal and external WinCC Unified tags are displayed by OPC UA tags of the "HMISimpleTagType" type.

The following table shows the most important attributes of the OPC UA tags that represent a WinCC Unified tag. You can find the complete list of attributes in the "OPC UA Part 3 - Address Space Model 1.03 Specification" under paragraph "5.6":

Attribute	Description	Comment
NodeId	Unique designation of the WinCC Unified tag	-
BrowseName	Name of the WinCC Unified tag	-
DisplayName	Name of the WinCC Unified tag	-
Value	Tag value and status	-
DataType	OPC UA data type that corresponds to the WinCC Unified tag type, for example: • Int32; signed 32 bit value • UInt32; unsigned 32 bit value	-
AccessLevel	"CurrentRead" / "CurrentWrite"	• Correspondingly to the WinCC Unified tag configuration. • System tags "CurrentRead" only.
ValueRank	Always "Scalar"	-

Mapping of the WinCC Unified alarms

Depending on their state machine, the alarms are mapped to the following OPC UA types:

State machine of the alarm	OPC UA type
RaiseClear RaiseClearRequiresReset	HmiConditionType
RaiseOptionalClearOrAcknowledgment RaiseClearOptionalAcknowledgement RaiseClearOptionalAcknowledgementAndReset RaiseRequiresAcknowledgement RaiseClearRequiresAcknowledgement RaiseClearRequiresAcknowledgementAndReset	HmiAlarmType

Priority

For the configuration of the alarms in WinCC Unified, you select a priority between "0" and "255". The OPC UA specification defines a value range between "1" for the lowest severity and "1000" for the highest severity.

The value of the priority must therefore be selected to match the OPC UA severity. In a standard mapping, the priority "0" is assigned to the OPC UA severity "1", and the priority "255" to the OPC UA severity "1000". All other values are interpolated linearly between "0" and "1000".

Mapping the OPC UA properties

The alarm condition consists of OPC UA event properties and WinCC Unified alarm properties. The properties of the alarm condition may vary depending on the OPC UA event type.

The following table provides the most important properties of the OPC UA events and shows how the WinCC Unified alarm system provides the information.

Note

Optional properties

Optional properties are not disclosed in the server address space.

OPC UA property	Description/Mapping
For all event types:	
EventId	A unique identifier for event notification.
EventType	The NodeId of the HmiConditionType node or HmiAlarmType node
SourceNode	NodeId of the Runtime object
SourceName	Name of the Runtime object
Time	RAISETIME of the WinCC Unified alarm Time stamp when the alarm was triggered at the source.
ReceiveTime	When the server has received the event from the underlying system.

OPC UA property	Description/Mapping
LocalTime	Information about the local time from which the event originated.
Message	EVENTTEXT of the WinCC Unified alarm, multilingual text for messages and alarms.
Severity	PRIORITY of the WinCC Unified alarm that is mapped to the OPC UA severity.
For the HmiConditionType and HmiAlarmType event types:	
ConditionId	NodeId of the condition instance
ConditionClassId	NodeId of the ProcessConditionClassType node
ConditionClassName	ProcessConditionClassType
ConditionName	NAME of the WinCC Unified alarm
BranchId	Not relevant
Retain	RETAIN of the WinCC Unified alarm TRUE for pending alarms
EanbledState/Id	ENABLESTATE of the WinCC Unified alarm TRUE for active alarms
Quality	VALUEQUALITY of the WinCC Unified alarm when the alarm became active
LastServerity	Not relevant
Comment	COMMENTS of the WinCC Unified alarm provided by the operator
ClientUserId	USER that is related to the WinCC Unified alarm
For the HmiAlarmType event type:	
AckedState	Mapped to STATE of the WinCC Unified alarm TRUE for acknowledged alarms
ConfirmedState/Id[1]	Mapped to STATE of the WinCC Unified alarm TRUE for confirmed alarms
ActiveState/Id	Mapped to STATE of the WinCC Unified alarm TRUE for active alarms
InputNode	NodeId of the tag assigned to the alarm
SupressedState/Id	Mapped to SUPPRESSIONSTATE of the WinCC Unified alarm TRUE for suppressed alarm
SupressedOrShelved	Mapped to SUPPRESSIONSTATE of the WinCC Unified alarm TRUE for reset or suppressed alarms
MaxTimeShelved	Not supported

[1] Only for alarms with the state machine RaiseClearRequiresAcknowledgmentAndReset

The following table provides the configurable properties of the WinCC Unified alarms. The properties are mapped one-to-one to OPC UA event properties.

The table applies to all event types:

Optional	Property	Description
-	INSTANCEID	Instance index used to reference an active multi-instance alarm within the (configured) HmiAlarm.
-	ALARM	Pointer to the corresponding HmiAlarm
-	ALARMCLASS	Pointer to the alarm class May differ from the alarm class reference of the associated HmiAlarm.
-	ALARMCLASSSYMBOL	Symbol (abbreviation) of the referenced alarm class
-	TEXTCOLOR	Text color
-	BACKCOLOR	Background color
-	FLASHING	Flashing
-	SUPPRESSIONSTATE	Indicates whether the alarm is reset, suppressed or not suppressed.
✓	ALARMTEXT1 ... ALARMTEXT9	Additional multi-lingual texts (Text 1 to Text 9)
✓	ALARMPARAMETERVALUES1 ... ALARMPARAMETERVALUES16	Parameter value 1 to parameter value 16
-	INVALIDFLAGS	Indicator of invalid property values Bit-by-bit interpretation
✓	ORIGIN	Dynamic alarm-instance-specific name of the alarm-triggering object.
✓	AREA	Dynamic alarm-instance-specific name of the area to which the alarm-triggering object belongs.
✓	LOOPINALARM	Function that is called to navigate from the alarm control, for example, to the screen that shows the source of the alarm or to an application that provides more information.
✓	COMPUTER	Name of the machine that hosts the originator of the alarm.
✓	USERNAME	Name of the user associated with the event (operator alarms only).
✓	VALUE	Current value at the time when the alarm became active. Updated value at the time the alarm became inactive.
✓	VALUEQUALITY	Current quality at the time when the alarm became active.
✓	VALUELIMIT	Current limit at the time when the alarm became active. For dynamic limits: Updated limit at the time the alarm became inactive.

Optional	Property	Description
✓	DEADBAND	Dead zone value of the alarm condition of an analog alarm at the time when the alarm became active.
✓	CONNECTION	Reference to the corresponding HMI connection
✓	SYSTEMSEVERITY	Severity for alarm-based system voting (redundancy)
-	SOURCETYPE	Defines the alarm generation method
-	STATE	The change of the current alarm condition, including history.
-	STATETEXT	Textual representation of the alarm condition
-	CHANGEREASON	Reason for the change time, see Enumeration definition.
-	ACKTIME	Time stamp of the time when the alarm was acknowledged at the source (or the service in case the alarm source does not provide an acknowledgment).
-	CLEARTIME	Time stamp of the time when the alarm at the source became inactive (or the service, in case the alarm source does not provide date and time information).
-	RESETTIME	Time stamp of the alarm reset time (or service, in case the alarm source does not provide date and time information).
✓	LOCALTIME	Information about the local time from which the alarm originated.
-	USERRESPONSE	The type of tag that represents a property of another node.
✓	DURATION	Returns the time interval in nanoseconds between triggering of the alarm and its previous status change.

3.1.7 OPC UA Data Access

Tags

The WinCC Unified tags are displayed by OPC UA tags of the "HMISimpleTagType" type. Other DataAccess tag types such as "AnalogItem" or "DiscreteType" are not supported.

The OPC UA server supports read access to the OPC UA tag attributes such as "DataType" or "AccessLevel". Writing access and subscriptions are only supported for the "Value" attribute.

Inverse browsing on the OPC UA client

The functionality for inverse browsing of tags is not supported in the OPC UA server.

3.1.8 Alarm conditions

Communication between a WinCC Unified device which is used as an OPC UA server and its OPC UA clients includes tag-based alarms.

Availability in the address space

Based on their state machine, the configured alarms of the system running on the WinCC Unified device are mapped to OPC UA types and loaded with their properties into the address space of the OPC UA server. See section Address space of the OPC UA server (Page 27).

OPC UA clients have read access to the alarms and their properties in the address space.

Monitoring alarms

OPC UA clients can monitor changes to the WinCC Unified alarms by subscribing to the server object or directly to the runtime system for monitoring. A client can subscribe to one object (server or runtime system) or several objects for monitoring.

When a configured alarm becomes active or a property of an active alarm changes, the OPC UA client is automatically notified.

OPC UA clients can perform the following actions for monitored alarms:

Action	Availability	Result
Acknowledge	For alarms of the OPC UA type HmiAlarmType	The alarm state is updated accordingly in the address space in the properties of the alarm. The runtime system reflects this change.
Confirm	For alarms of the OPC UA type HmiAlarmType	
Activate	For alarms of the OPC UA types HmiConditionType and HmiAlarmType	
Disable		
Shelve		
Unshelve alarm	For alarms of the OPC UA type HmiAlarmType	

3.1.9 Managing OPC UA server certificates

If you use a WinCC Unified device as an OPC UA server and the OPC UA communication is protected by certificates, the following applies:

- An OPC UA server certificate must be installed on the Unified device.
- The OPC UA clients must trust the OPC UA server certificate.
- The Unified device must trust the OPC UA client certificates.

Section Introduction to OPC UA certificates (Page 7) describes how you proceed to provide the certificates required for communication.

3.2 Using the Unified PC as OPC UA server

3.2.1 Exporting tags

Offline export of tags using the OPC UA server

SIMATIC Runtime Manager allows you to export the tags configured for the active Runtime project to an OPC UA Nodeset using the OPC UA server. The exported data can be imported into another application, e.g. the TIA Portal, without the need for a connection to the OPC UA server.

The export makes it easier to apply an existing configuration to a new Runtime system.

Requirement

- The OPC UA server for WinCC Unified is running.
- A WinCC Unified Runtime project is running on the server.
- The following applies to the user who started the export:
  - The user has the role "SIMATIC HMI".
  - The user has the function right for read and write access to OPC UA.
- The OPC UA server certificate and the WinCC Unified OPC UA exporter certificate trust each other.
  If you have generated and installed the certificates again via the Certificate Manager, this is automatically the case.
  If you want to use the default certificates created during the Runtime installation, move the certificates so that they trust each other:

Source directory	Target directory
`C:\SCADAProjects\certstore\own\certs`	`C:\SCADAProjects\certstore\trusted\certs`

Procedure

Follow these steps to export the tags of the active Runtime using the OPC UA server:

1. Start "SIMATIC Runtime Manager".
2. Click the button ⚙ in the toolbar.
3. Configure the export settings in the "OPC UA Export" tab:
   - Select the name and the folder of the output file.
   - Type in the user name and password of the user who started the export.
4. Click "Export".

Result

You can see whether the export was successful in the "Status" field.

If the export is successful, the file is written to the specified folder.

For diagnostic purposes, a trace file is written to the following folder: [ProgramData]/Siemens/Automation/Logfiles

See also

Requirements for use (Page 22)

3.2.2 Configuring a Unified OPC UA server (Unified PC)

3.2.2.1 OPC UA server

General

OPC is a standardized manufacturer-independent software interface for data exchange in automation engineering. OPC UA is the technology succeeding OPC. OPC UA is platform-independent and supports different protocols as communication medium.

To work with OPC UA in WinCC Unified, the OPC UA server must be enabled in the TIA Portal in the Runtime settings of the HMI device.

Read/write tags and register tags/alarms

When you enable the "Operate as OPC UA server" option in the HMI device, the protection for unauthorized internal and external access is downgraded.

- Enable the "Operate as OPC UA server" option.
  A security note is displayed.

After enabling the option, all other settings of the OPC UA Server will become available.

Alarms and Conditions

- To display alarm conditions in the address range of the server, select the option "Enable Alarms and Conditions on the OPC UA server".
- To disable or acknowledge alarms on the OPC UA Client, for example, select the option "Allow operation of alarms on the OPC UA Client". To enable this option, the "Enable Alarms and Conditions on the OPC UA server" option must be enabled.

Options

General

Define the following settings:

- Port
  Default value: 4890
  Do not use a port number that is already assigned to another application.
- Maximum session timeout (s)
  Default value: 600000 s
- Maximum number of OPC UA sessions
  Default value: 100

Subscriptions

Define the following settings:

- Minimum publication interval (ms)
  Default value: 100 ms
- Maximum number of monitored items
  Default value: 0

Security

Secure connection

Security policies

⚠ **CAUTION**

Reduced security

When the option "No OPC UA Server Security" is enabled, any OPC UA client can connect to the OPC UA server regardless of the following settings.

The following section contains a list of all security policies available on the server.

- Activate the required security policies.

User authentication

Guest authentication

- To allow access by anonymous users to the OPC UA server, enable the option "Enable guest authentication".
  An authentication by means of user name and password is not required for guests.
  Security is restricted to the degree that you determine by assigning rights to this user.

Authentication by means of user name and password

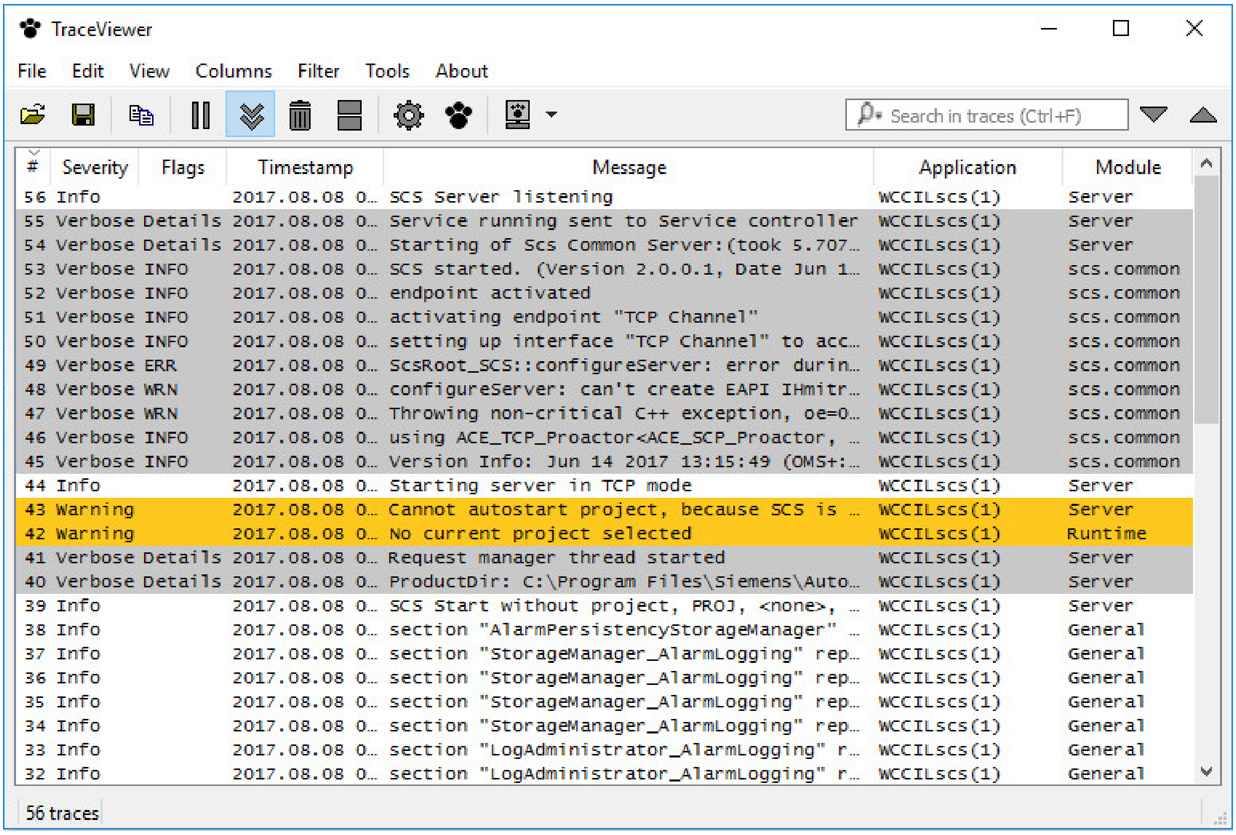
- To allow access by users with user name and password to the OPC UA server, enable the option "Authentication with user name and password".
  If access to the OPC UA server is to require the user name and password, the user must be assigned the role "HMI Administrator". The "HMI Administrator" role has the system-defined "OPC UA - read and write access" function right. The settings made must then be synchronized with the user management in runtime.

3.2.3 Trace

WinCC Unified provides trace logging for error analysis. The OPC UA traces including SDK can be logged for test purposes and for troubleshooting.

TraceViewer

The log files can be viewed with the TraceViewer. This tool is available in the installation directory of WinCC Unified under "WinCCUnified\bin". Start the file "RTILtraceViewer.exe".



```
#  Severity Flags   Timestamp       Message                                      Application   Module
56 Info             2017.08.08 0…   SCS Server listening                         WCCILscs(1)   Server
55 Verbose Details  2017.08.08 0…   Service running sent to Service controller   WCCILscs(1)   Server
54 Verbose Details  2017.08.08 0…   Starting of Scs Common Server:(took 5.707…   WCCILscs(1)   Server
53 Verbose INFO     2017.08.08 0…   SCS started. (Version 2.0.0.1, Date Jun 1…   WCCILscs(1)   scs.common
52 Verbose INFO     2017.08.08 0…   endpoint activated                           WCCILscs(1)   scs.common
51 Verbose INFO     2017.08.08 0…   activating endpoint "TCP Channel"            WCCILscs(1)   scs.common
50 Verbose INFO     2017.08.08 0…   setting up interface "TCP Channel" to acc…   WCCILscs(1)   scs.common
49 Verbose ERR      2017.08.08 0…   ScsRoot_SCS::configureServer: error durin…   WCCILscs(1)   scs.common
48 Verbose WRN      2017.08.08 0…   configureServer: can't create EAPI IHmitr…   WCCILscs(1)   scs.common
47 Verbose WRN      2017.08.08 0…   Throwing non-critical C++ exception, oe=0…   WCCILscs(1)   scs.common
46 Verbose INFO     2017.08.08 0…   using ACE_TCP_Proactor<ACE_SCP_Proactor, …   WCCILscs(1)   scs.common
45 Verbose INFO     2017.08.08 0…   Version Info: Jun 14 2017 13:15:49 (OMS+:…   WCCILscs(1)   scs.common
44 Info             2017.08.08 0…   Starting server in TCP mode                  WCCILscs(1)   Server
43 Warning          2017.08.08 0…   Cannot autostart project, because SCS is …   WCCILscs(1)   Server
42 Warning          2017.08.08 0…   No current project selected                  WCCILscs(1)   Runtime
41 Verbose Details  2017.08.08 0…   Request manager thread started               WCCILscs(1)   Server
40 Verbose Details  2017.08.08 0…   ProductDir: C:\Program Files\Siemens\Auto…   WCCILscs(1)   Server
39 Info             2017.08.08 0…   SCS Start without project, PROJ, <none>, …   WCCILscs(1)   Server
38 Info             2017.08.08 0…   section "AlarmPersistencyStorageManager" …   WCCILscs(1)   General
37 Info             2017.08.08 0…   section "StorageManager_AlarmLogging" rep…   WCCILscs(1)   General
36 Info             2017.08.08 0…   section "StorageManager_AlarmLogging" rep…   WCCILscs(1)   General
35 Info             2017.08.08 0…   section "StorageManager_AlarmLogging" rep…   WCCILscs(1)   General
34 Info             2017.08.08 0…   section "StorageManager_AlarmLogging" rep…   WCCILscs(1)   General
33 Info             2017.08.08 0…   section "LogAdministrator_AlarmLogging" r…   WCCILscs(1)   General
32 Info             2017.08.08 0…   section "LogAdministrator_AlarmLogging" r…   WCCILscs(1)   General
```

3.3 Using the Unified Comfort Panel as OPC UA server

3.3.1 Configuring the Unified OPC UA server (UCP)

3.3.1.1 OPC UA server

General

OPC is a standardized manufacturer-independent software interface for data exchange in automation engineering. OPC UA is the technology succeeding OPC. OPC UA is platform-independent and supports different protocols as communication medium.

To work with OPC UA in WinCC Unified, the OPC UA server must be enabled in the TIA Portal in the Runtime settings of the HMI device.

Read/write tags and register tags/alarms

When you enable the "Operate as OPC UA server" option in the HMI device, the protection for unauthorized internal and external access is downgraded.

- Enable the "Operate as OPC UA server" option.
  A security note is displayed.

After enabling the option, all other settings of the OPC UA Server will become available.

Alarms and Conditions

- To display alarm conditions in the address range of the server, select the option "Enable Alarms and Conditions on the OPC UA server".
- To disable or acknowledge alarms on the OPC UA Client, for example, select the option "Allow operation of alarms on the OPC UA Client". To enable this option, the "Enable Alarms and Conditions on the OPC UA server" option must be enabled.

Options

General

Define the following settings:

- Port
  Default value: 4890
  Do not use a port number that is already assigned to another application.
- Maximum session timeout (s)
  Default value: 600000 s
- Maximum number of OPC UA sessions
  Default value: 100

Subscriptions

Define the following settings:

- Minimum publication interval (ms)
  Default value: 100 ms
- Maximum number of monitored items
  Default value: 0

Security

Secure connection

Security policies

> ⚠ **CAUTION**
>
> **Reduced security**
>
> When the option "No OPC UA Server Security" is enabled, any OPC UA client can connect to the OPC UA server regardless of the following settings.

The following section contains a list of all security policies available on the server.

- Activate the required security policies.

User authentication

Guest authentication

- To allow access by anonymous users to the OPC UA server, enable the option "Enable guest authentication".
  An authentication by means of user name and password is not required.
  Security is restricted to the degree that you determine by assigning rights to this user.

Authentication by means of user name and password

- To allow access by users with user name and password to the OPC UA server, enable the option "Authentication with user name and password".
  If access to the OPC UA server is to require the user name and password, the user must be assigned the role "HMI Administrator". The "HMI Administrator" role has the system-defined "OPC UA - read and write access" function right. The settings made must then be synchronized with the user management in runtime.

WinCC Unified OPC UA client 4

4.1 Using the WinCC Unified OPC UA client

As OPC UA clients, WinCC Unified devices can integrate the following data from OPC UA servers into their projects:

- Alarm instances received from the OPC UA server
- OPC UA server tags

When configuring this data in the engineering system, the engineering system also becomes the OPC UA client.

4.2 Defining connection settings to the OPC UA server

Requirement

- In the engineering system, a WinCC project is open that has had a Unified device added to it.
- The "Connections" editor is open.

Procedure

Double-click in the "Add" cell and define the connection settings:

- "Communication driver": OPC UA
- Set the following parameters in the "Parameters" tab under "OPC server":
  - "UA server discovery URL": Enter the OPC UA server IP and port
    Use the following notation: opc.tcp://<IP>:<Port>
    Alternatively, you can also determine the server via "Select OPC server".
  - Select the desired security settings.
    See also Defining the security settings for communication with the OPC UA server (Page 42).

Result

The Unified OPC UA client uses the settings to establish a connection to the OPC UA server.

4.3 Defining the security settings for communication with the OPC UA server

Requirement

A connection with the communication driver "OPC UA" is configured in a WinCC project on a Unified device. See also section Defining connection settings to the OPC UA server (Page 41).

Procedure

Select the security settings that meet the requirements of the OPC UA server:

1. Open the "Connections" editor.
   You make the security settings in the "OPC UA Server" area.
2. To protect the connection with a security policy, follow these steps:
   - Select the security policy.
     The communication with the server is protected by a certificate.

     Note

     Make OPC UA certificates available

     Make sure that the required certificates are available on the OPC UA server and client. See also Introduction to OPC UA certificates (Page 7).

     Note

     Connection without security policy

     If you do not select a security policy, it is urgently recommended that the OPC UA server and client are installed on the same device.
   - Select whether communication is signed or signed and encrypted.
3. To protect communication with the OPC UA server by a user name and password, follow these steps:
   - Disable the "Anonymous" option.
   - Enter the user name and password of a user account configured on the OPC UA server.
4. For anonymous communication, select the option "Anonymous".

4.4 Integrating OPC UA server alarm instances into a Unified client

You have the option of integrating alarm instances from an OPC UA server into your Runtime project.

Note

Restrictions

- The OPC UA server is a SINUMERIK device.
- The OPC UA server is based on the OPC UA specification 1.03.

Requirement

- The OPC UA server alarm instances are available in a NodeSet XML file.
- You have access to the XML file on the device on which the engineering system is installed.

Procedure

1. In the engineering system, add a Unified HMI device to a WinCC project.
2. Set the connection settings to an OPC UA server for the HMI device.
   See also section Defining connection settings to the OPC UA server (Page 41).
3. Import the XML file with the OPC UA server alarm instances into the WinCC project.
   See also section Importing OPC UA server alarm instances (Page 44).
4. Generate HMI alarms for the OPC UA server alarm instances.
   See also section Generating HMI alarms for OPC UA server alarm instances (Page 45).
5. Add a screen to the HMI device.
6. Place an alarm display on the screen.
7. Compile the HMI device in a Runtime project, load the Runtime project onto the HMI device and start the project in Runtime.

   Note

   Loss of the ability to compile and load changes

   If you load the OPC UA server alarm instances on the HMI device and then update the alarm instances in the engineering, because the alarm class has been changed for example, you lose the option in the engineering to compile and load only the changes to the project. The project must now be fully compiled and loaded.

Result

In Runtime, the alarm instances received from the OPC UA server are displayed in the alarm display. The following attributes are mapped to each other:

Attributes of an OPC UA server alarm instance	Attribute of an HMI alarm
"Message"	"Alarm text"
"SourceName"	"Origin"

If alarm archiving is activated, the alarms are archived.

Status changes to the alarm instances on the OPC UA server are reflected in Runtime. The Runtime OPC UA client can request status changes on the server. The status change is always done on the server.

4.4.1 Importing OPC UA server alarm instances

Requirement

- In the engineering system, a WinCC project is open that has had a Unified device added to it.
- The OPC UA server alarm instances are available in a NodeSet XML file.
- You have access to the XML file on the device on which the engineering system is installed.

Procedure

To import OPC UA server alarm instances into a WinCC project, follow these steps:

1. Open the "HMI alarms" editor.
2. Select the "OPC UA A&C" tab.
3. Under "Connection" in the right area, select the OPC UA connection.
4. Click "Import" next to "Connection":
5. Select the XML file.
6. Click "Import".

Result

The content of the XML file is imported into the "OPC UA browser" area. It contains the hierarchical OPC UA NodeSpace with the OPC UA server alarm instances.

Then generate HMI alarms for the OPC UA server alarm instances.

See also

Generating HMI alarms for OPC UA server alarm instances (Page 45)

4.4.2 Generating HMI alarms for OPC UA server alarm instances

Requirement

- In the engineering system a WinCC-project is open, to which a HMI device has been added.
- The "HMI alarms" editor of the device is open.
- An XML file with the OPC UA server alarm instances was imported into the editor.

Procedure

1. Select the "OPC UA A&C" tab.
2. Expand the objects in the "OPC UA browser" area up to the node under which the OPC UA server alarm instances are located.
3. Press and hold the left mouse button to drag the node to the "Node ID" cell of the "Add" row of the table in the "OPC UA types" area.
   An entry for an alarm type is added to the table. The table provides detailed information on the properties of the alarm type.
4. Select an alarm class that matches the alarm type of the OPC UA server alarm instances and supports the state machine "Alarm without status active with acknowledgment".
5. In the "OPC UA types" area, click the button to generate and update the alarm instances:
   🔄

Note

Loss of the ability to compile and load changes

If you load the OPC UA server alarm instances on the HMI device and then update the alarm instances in the engineering, because the alarm class has been changed for example, you lose the option in the engineering to compile and load only the changes to the project. The project must now be fully compiled and loaded.

Result

HMI alarms are generated for the OPC UA server alarm instances.

When loading the project into a Runtime, the mapping between the HMI alarms and the OPC UA server alarm instances are loaded into the target device.

See also

Importing OPC UA server alarm instances (Page 44)