

SIEMENS



Configuration Example 10/2016

Integration of Network Information from the SINEMA Server in WinCC

SINEMA Server V13 SP 1



<https://support.industry.siemens.com/cs/ww/en/view/109740549>

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The sample applications do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these sample applications, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these sample applications at any time without prior notice.

If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document. Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these sample applications or excerpts hereof is prohibited without the expressed consent of Siemens AG.

Security Information

Siemens provides products and solutions with industrial security 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 security concept. Siemens’ products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit <http://www.siemens.com/industrialsecurity>.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <http://www.siemens.com/industrialsecurity>.

Contents

Warranty and Liability	2
1 Introduction	4
1.1 Overview.....	4
1.2 Function.....	5
1.3 Components Used.....	6
2 Engineering	7
2.1 General Overview.....	7
2.2 Configuration	8
2.2.1 Useful Tips	8
2.2.2 SINEMA Server Logon	9
2.2.3 Search Network	11
2.2.4 Make Network Visible in OPC UA	13
2.2.5 Create Secure OPC UA Connection in WinCC.....	15
2.2.6 Start Encrypted OPC UA Data Exchange	24
3 History.....	27
4 Related Literature	27

1 Introduction

1.1 Overview

Request

Using a network monitoring software it is possible to call up the status of the network and provide further network information.

The acquired data should be made accessible on an existing HMI system. This should be done exclusively via standardized protocols.

Possible solution

One possible solution for this request is to use SINEMA Server and the communication protocol OPC UA.

The network management software SINEMA Server monitors the devices installed in the network and reads out data via SNMP, PROFINET and the SIMATIC protocol. In addition it has extensive diagnostics and reporting functions for early recognition and clearing of network problems.

An integrated OPC server permits users or HMI devices to access the acquired network data.

Implementation

This document shows how you can use the SINEMA Server to provide a higher-level HMI system with the monitored data via a signed and encrypted OPC UA connection.

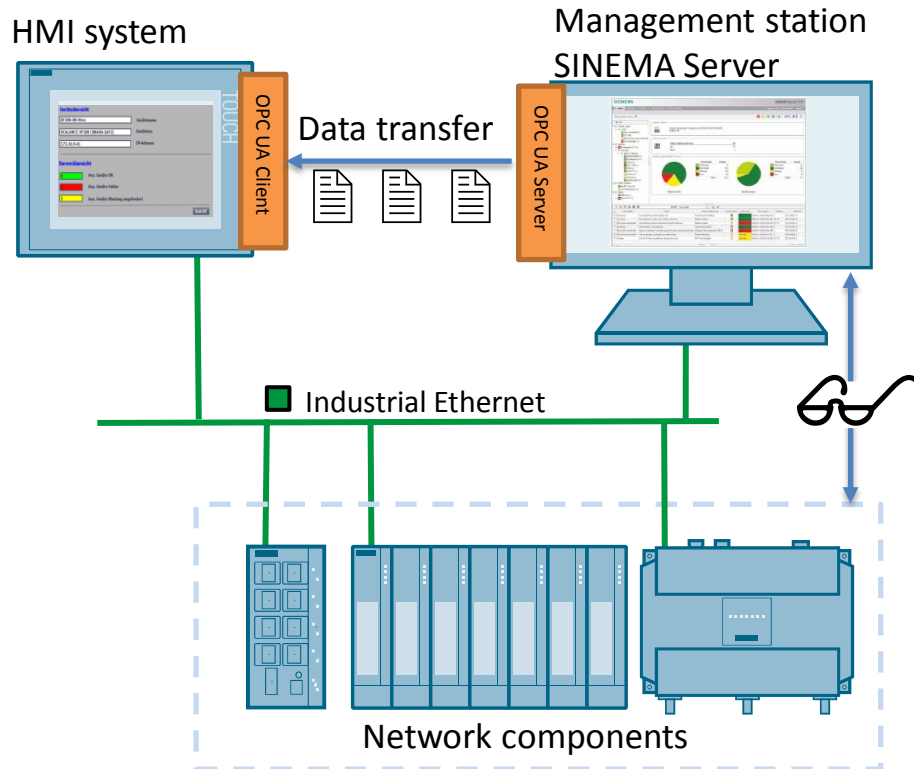
The key elements here are:

- In the SINEMA Server: Installation of the interface - additional for OPC UA applications - as access to the network data.
- In the HMI System: Settings required for access to the acquired data in the SINEMA Server via OPC UA.

1.2 Function

The diagram below shows the basic principles of the solution.

Figure 1-1



1.3 Components Used

Software component

The software below is required for this solution.

Table 1-1

Software	Article number / Designation
SINEMA Server V13 SP1	DVD: 6GK1781-1BA13-0AA0 [50 nodes] 6GK1781-1DA13-0AA0 [100 nodes] 6GK1781-1JA13-0AA0 [250 nodes] 6GK1781-1TA13-0AA0 [500 nodes] 6GK1781-2AA13-0AA0 [Update SP 1] Download (Online Support): 6GK1781-1BA13-0AK0 [50 nodes] 6GK1781-1DA13-0AK0 [100 nodes] 6GK1781-1JA13-0AK0 [250 nodes] 6GK1781-1TA13-0AK0 [500 nodes] 6GK1781-2AA13-0AK0 [Update SP 1]
- Internet Explorer 10.0 - Firefox 42.0	These browser versions are the minimum requirements. You can also use higher versions of the browsers.
SIMATIC STEP 7 PROFESSIONAL V13 SP1	6ES7822-1AA03-0YA5
WinCC Professional V13 SP1	6AV2105-0BA03-0AA0 [128 power tags]

Install these software packages on a PC/PG with

- Windows 7 SP1 64-bit (Prof., Ult., Ent)
- Windows 2008 Server R2 SP1 64-bit

Note

As far as possible do not change the proposed installation path of the software. The following instructions include path specifications that refer to the standard installation directory.

Compatible devices

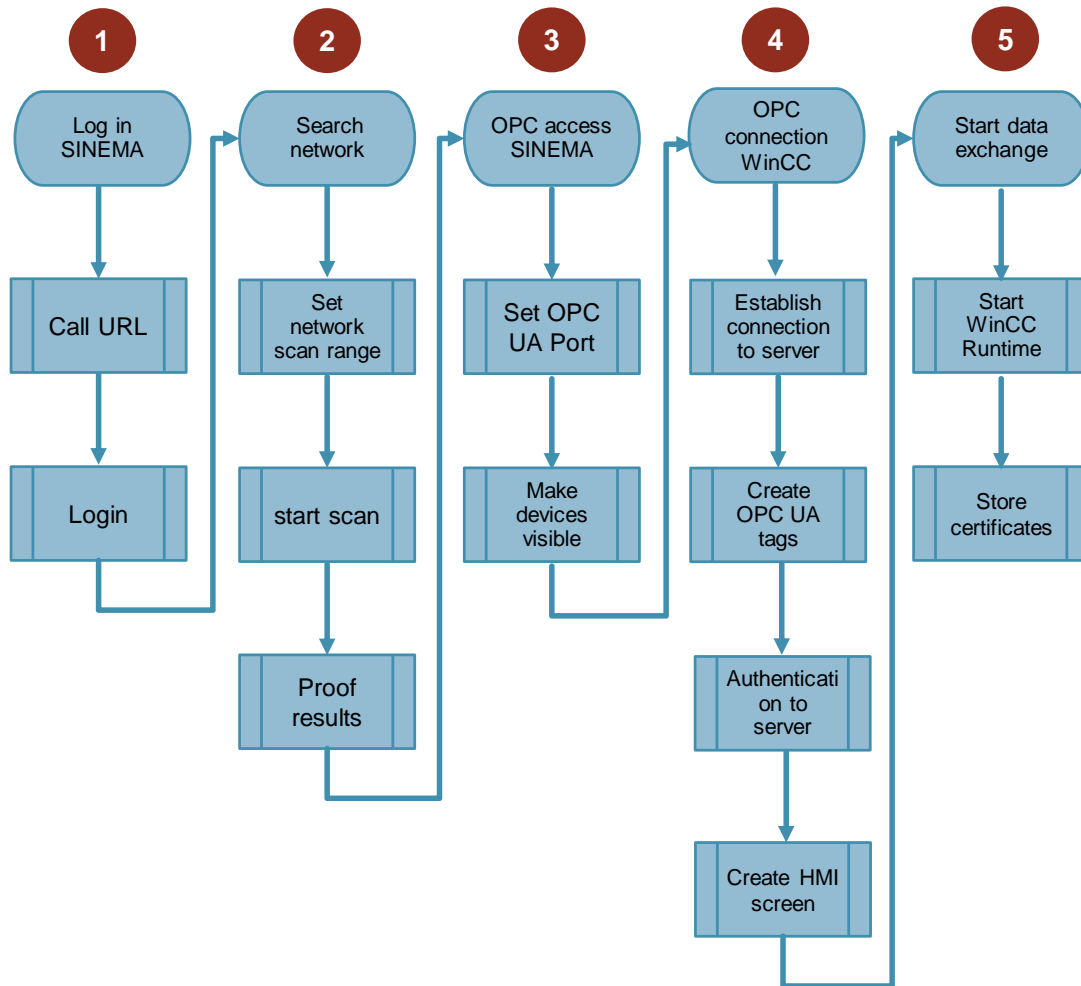
These instructions are valid for all network components that can be monitored with SINEMA Server.

2 Engineering

2.1 General Overview

The diagram below shows the principal procedure for achieving the task in 5 steps.

Figure 2-1



2.2 Configuration

2.2.1 Useful Tips

Role assignment

The roles are assigned as below for the following solution.

Table 2-1

Software	OPC role
SINEMA Server	OPC UA Server
WinCC V13 SP1/ WinCC Runtime	OPC UA Client

Devices used

In the following configuration instructions the following IP parameters are assigned to the monitored network.

Table 2-2

No.	Component	Article number	IP address	Subnet mask
1	CPU 315-2 PN/DP	6ES7 315-2EH14-0AB0	172.16.9.20	255.255.0.0
2	CP 343-1	6GK7 343-1EX30-0XE0	172.16.9.21	255.255.0.0
3	ET200ECO PN 8DI	6ES7 141-6BF00-0AB0	172.16.9.23	255.255.0.0
4	CPU 1511-1 PN	6ES7 511-1AK00-0AB0	172.16.9.30	255.255.0.0
5	ET200MP IM155-5 ST	6ES7 155-5AA00-0AB0	172.16.9.31	255.255.0.0
6	ET 200SP IM155-6 PN ST	6ES7 155-6AU00-0BN0	172.16.9.32	255.255.0.0
7	SCALANCE XM408-8C	6GK5 408-8GS00-2AM2	172.16.9.40	255.255.0.0
8	SCALANCE XF208	6GK5 208-0BA00-2AF2	172.16.9.41	255.255.0.0
9	SCALANCE XF208	6GK5 208-0BA00-2AF2	172.16.9.42	255.255.0.0
10	SCALANCE W774-1 RJ45	6GK5 774-1FX00-0AA0	172.16.9.80	255.255.0.0
11	SCALANCE W761-1 RJ45	6GK5 761-1FC00-0AA0	172.16.9.81	255.255.0.0

Display data

In the following configuration instructions the following data is to be integrated in a higher-level HMI system.

- Network information like
 - Number of devices with status "OK"
 - Number of devices with status "Error"
 - Number of devices with status "Maintenance requested"
- Device information from a SCALANCE XF208:
 - Device name
 - Device type
 - IP address

Display

Note that the data types "Array [] of STRING" and "Array [] of INT" are not correctly displayed in the interaction between WinCC Professional V13 SP1 and SINEMA Server V13 SP1.

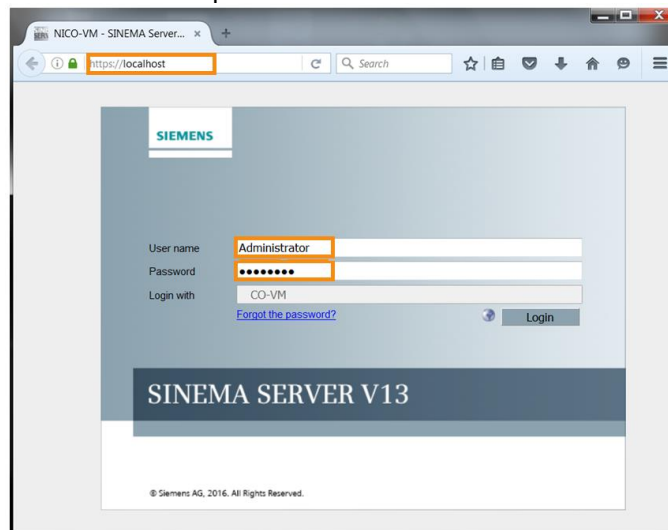
Engineering PC

In the following instructions it is assumed that all the software packages listed in [section 1.3](#) are installed on one common PC. These are:

- TIA Portal V13 SP1
- WinCC Professional V13 SP 1 incl. WinCC Runtime
- SINEMA Server V13 SP1

2.2.2 SINEMA Server Logon

1. Start your browser and enter the SINEMA Server URL in the address line. Use the default URL <https://localhost> if SINEMA is newly installed or a system restore has been performed.



2. Log on to the SINEMA Server with the following logon data:
Default logon data:

- User name: Administrator
- Password: SinemaA

User-specific logon data:

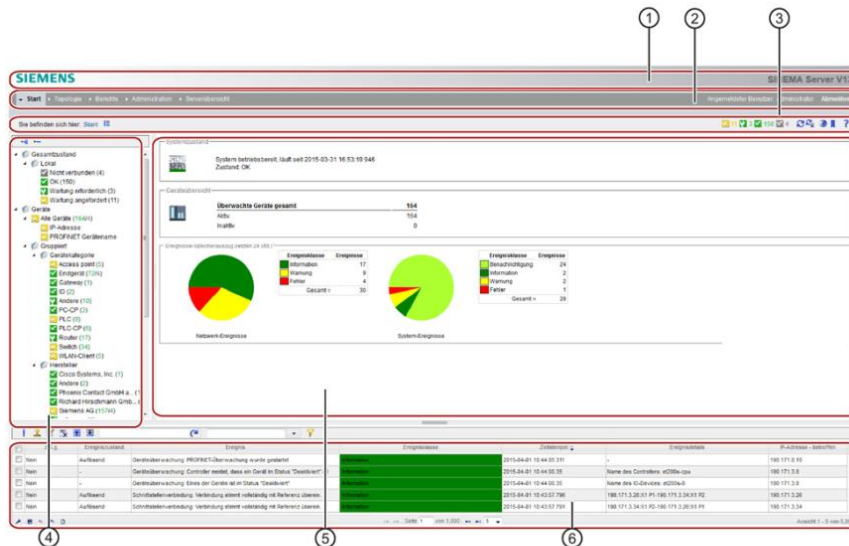
- User name: <...>
- Password: <...>

Note

You must change the default logon data after the first logon.

Result:

The "home page" of the SINEMA server is displayed.

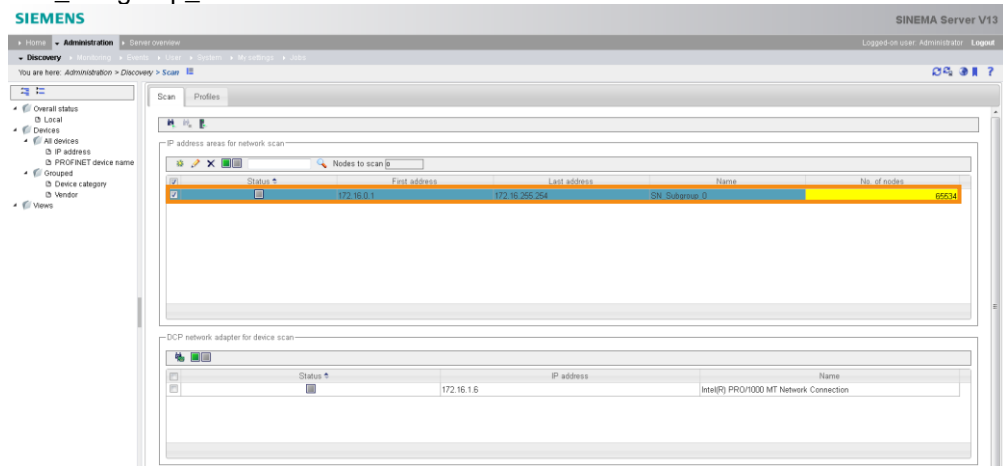


- | | |
|---------------------|-----------------|
| ① Kopfbereich | ④ Gerätebaum |
| ② Navigationsleiste | ⑤ Hauptfenster |
| ③ Statuszeile | ⑥ Ereignisliste |

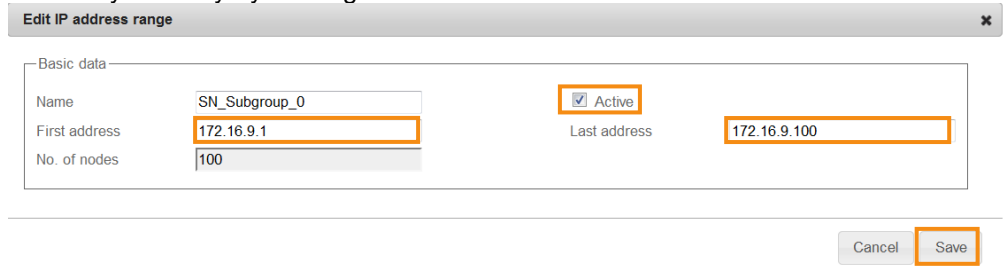
2.2.3 Search Network

Set the network scan range

1. In the menu bar you go to the menu "Administration > Discovery > Scan".
2. Under "DCP network adapter for device scan" you select the function "Scanning for network adapters".
3. The network adapters available on the Management Station are displayed. In the table you select the network adapters via which the search is to be executed and enable them via the function "Enable network card for device scan".
4. In the menu bar you go again to the menu "Administration > Discovery > Scan".
5. Under "IP address areas for network scan" you select the item with the name "SN_Subgroup_0".

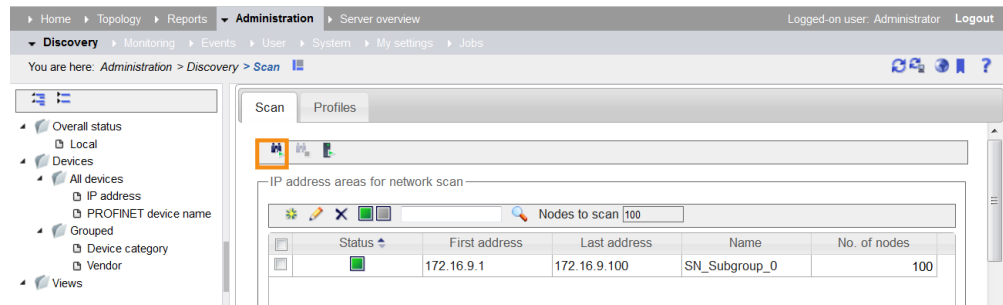


6. Click the icon "Edit IP address area" or double-click the selected item.
7. In the dialog that opens you specify the IP address range that includes the SCALANCE devices to be upgraded and check the check box "Active" to enable the specified IP address range.
8. Confirm your entry by clicking the "Save" button.



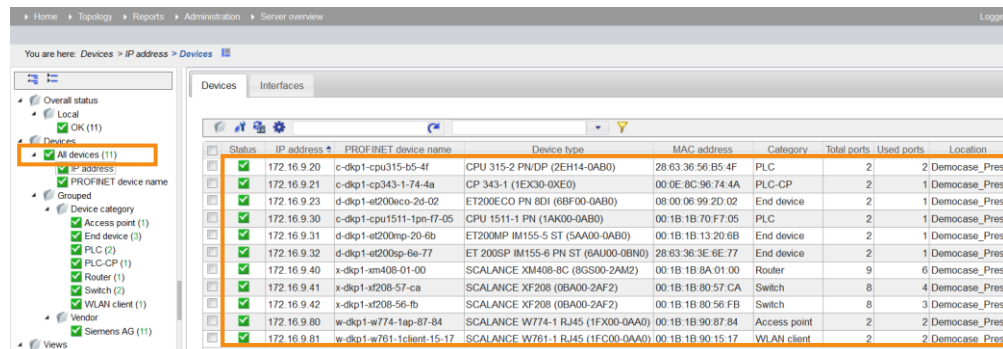
Start network scan

Then click the "Start scan" icon to start the scanning process.



Check scan result

Check whether the SCALANCE devices have been found by SINEMA Server. All the devices found are displayed in the device tree on the left side: "Devices > All Devices"

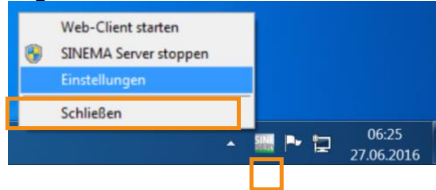


2.2.4 Make Network Visible in OPC UA

In this section the SINEMA Server is set for its role as OPC UA Server.

Set OPC UA port in the SINEMA Server Monitor

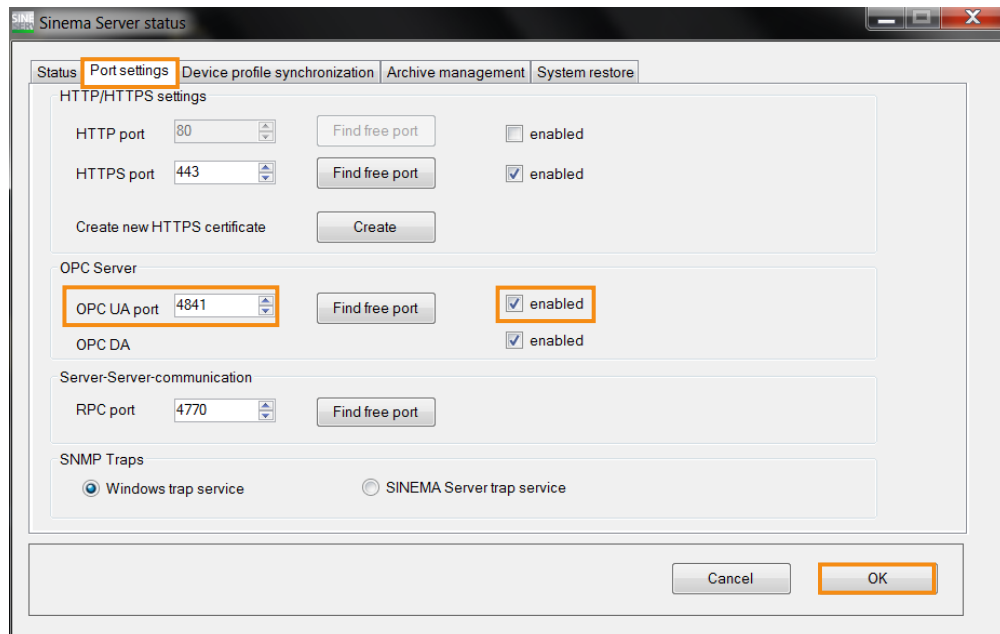
1. Via the Windows "Info area toolbar" you navigate to the program "SINEMA Server Monitor".
2. Right-click the "SINEMA Server Monitor" icon and then "Settings".



Note

If the SINEMA Server Monitor icon is not visible, you have to start the SINEMA Server Monitor once manually. For this, you navigate to the folder "C:\Siemens\SINEMAServer\Sinema_Server_Monitor\bin" and start the program "SinemaServerMonitor.exe".

3. In the SINEMA Server Status Monitor you select the "Port Settings" tab. Check that the OPC UA Port 4841 is enabled and then click the "OK" button.



Note

By default the OPC UA Port is set to the value 4841 and enabled. During the installation of SINEMA Server the Windows Firewall was set to enable incoming and outgoing traffic of the Port 4841 TCP.

If you change the OPC UA standard port, this has to be correspondingly permitted manually in the Windows Firewall (incoming traffic).

Make monitored devices visible for OPC UA

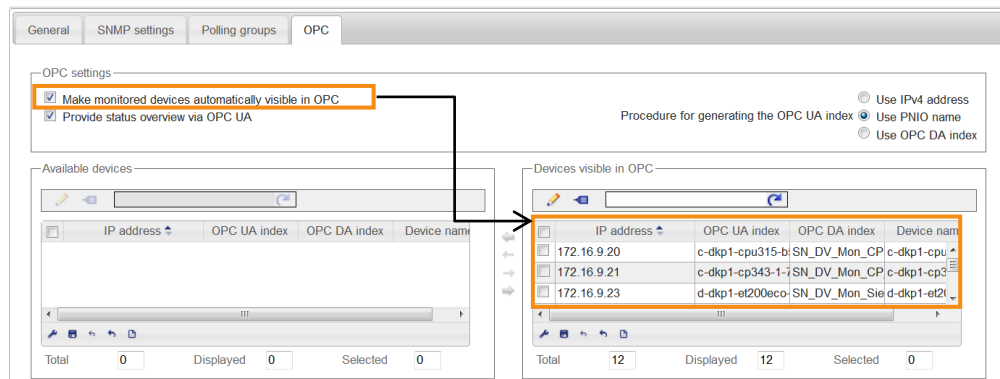
- In SINEMA Server you navigate to the menu item "Administration > Monitoring > OPC". On the left side you enable the two selection fields
 - "Make monitored devices automatically visible in OPC" and
 - "Provide status overview via OPC UA".
- In the area on the right you select the procedure for generating the OPC UA index (in the example: "Use PNIO name").



Note

You can change the PROFINET names individually with SINEMA Server.

- In this way all the monitored network devices transfer their data to the higher-level HMI system automatically via the OPC UA interface.



Note

If you do not want to integrate all devices in the higher-level HMI system, you have to deselect the check box "Make monitored devices automatically visible in OPC".

Then in the "Available devices" window on the left you can select each device individually and add them to the devices in OPC via the icon "Generate the OPC UA index according to the selected procedure".

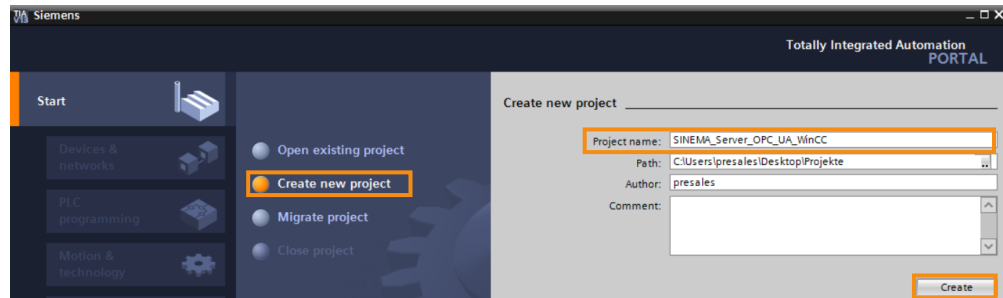
To select several devices in SINEMA Server you press and hold the CTRL key and select the devices by mouse-click.

2.2.5 Create Secure OPC UA Connection in WinCC

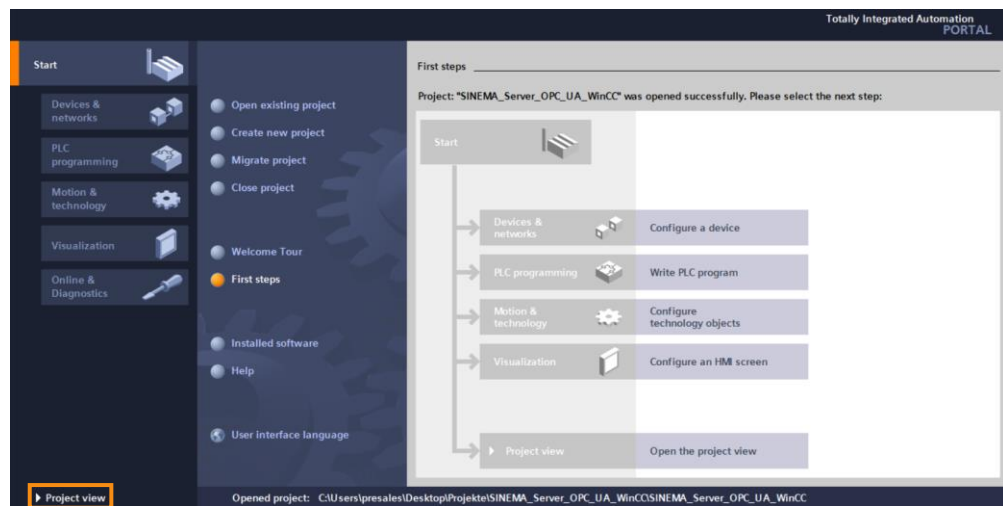
In this section WinCC is set for its role as OPC UA Client.

Establish connection to the OPC server

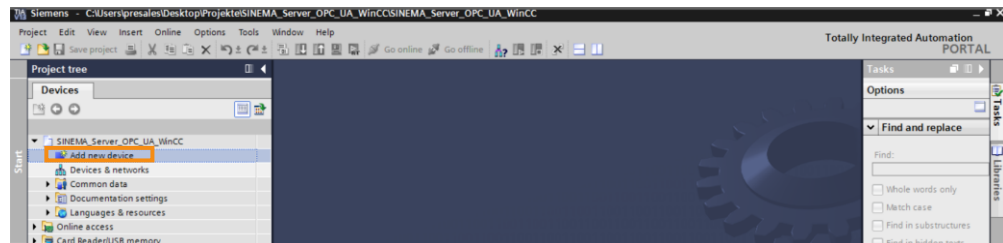
1. Start TIA Portal V13 SP1 with integrated WinCC Professional V13 SP1. Create a new project in the TIA Portal ("Create new project" button). Assign a project name and click the "Create" button.



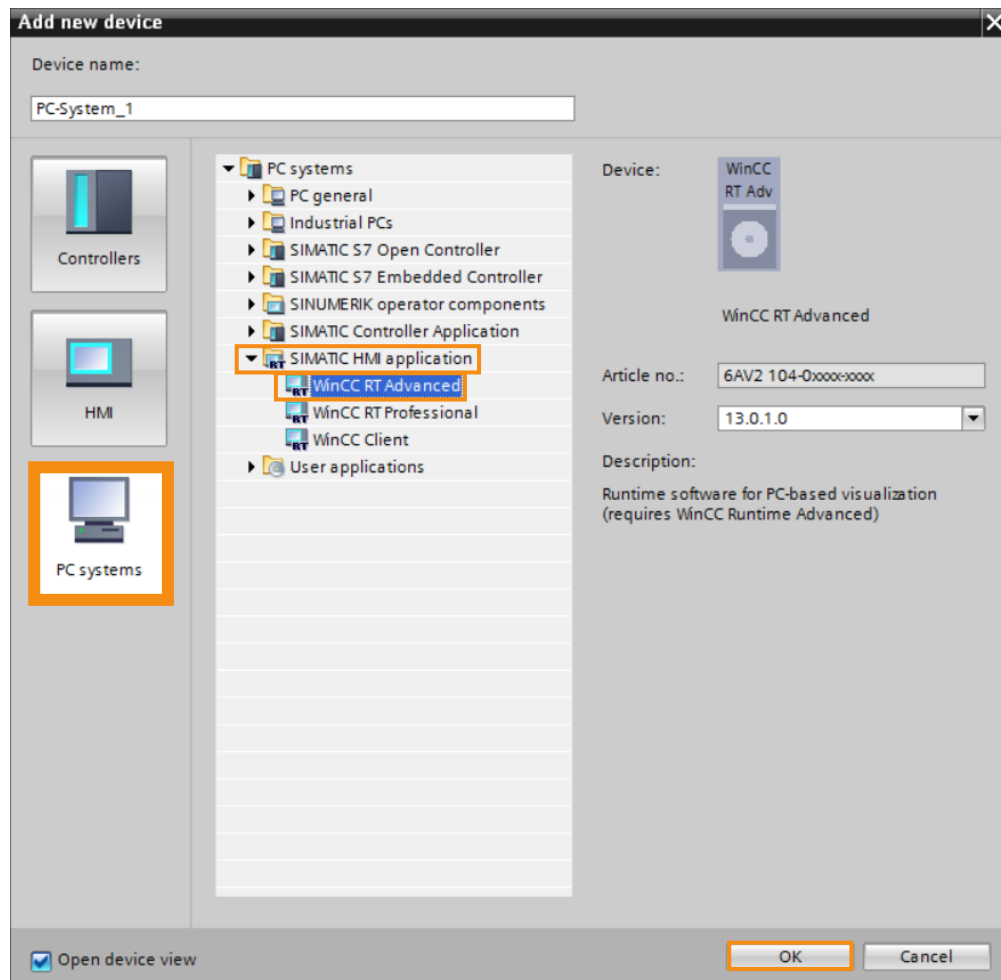
2. Switch to the Project view.



3. Create a new device via the function "Add new device" in the project tree.

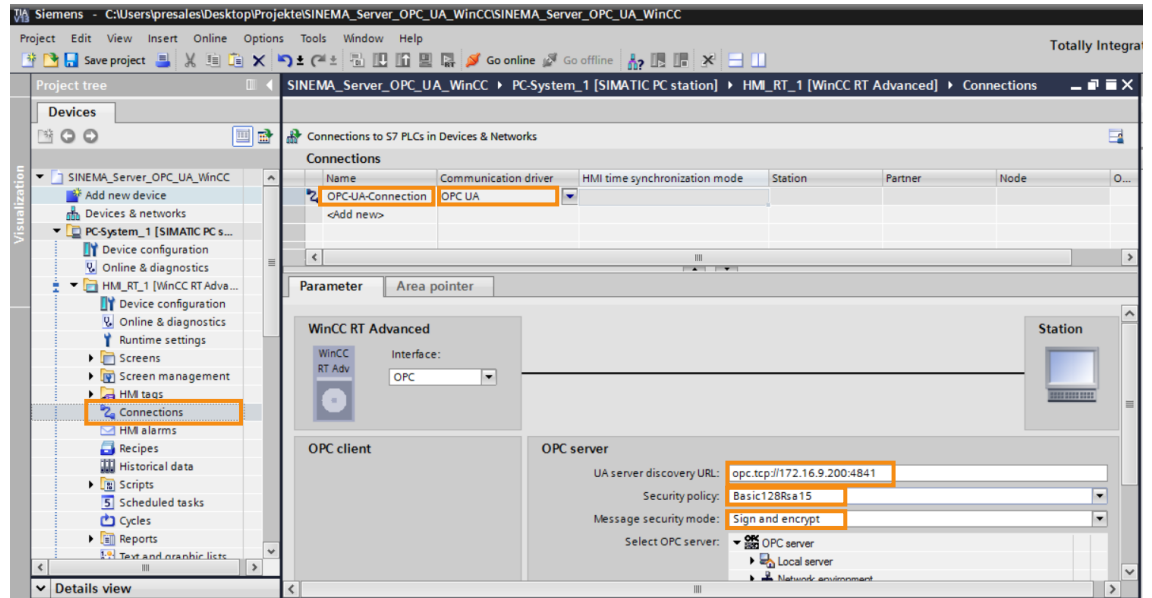


4. Select the "PC systems" icon and in the device tree you navigate to the item "SIMATIC HMI application > WinCC RT Advanced". Confirm this entry by clicking the "OK" button.



5. In the project tree you navigate to the item "Connections" and select it with a double-click. In the center top window you create a new OPC UA connection with the following parameters:
 - Name: <free choice, OPC-UA-Connection, for example>
 - Communication driver: OPC UA

6. Create a signed and encrypted OPC UA Server connection with these parameters:
 - UA server discovery URL: opc.tcp://<IP address OPC server>:4841
 - Security policy: Basic128Rsa15
 - Message security mode: Sign and encrypt



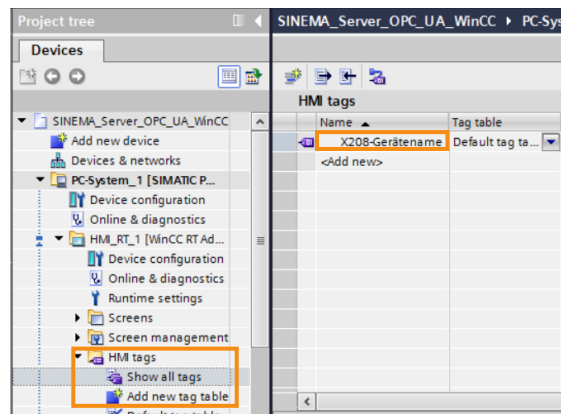
Note

For this example we configure a signed and encrypted OPC UA connection which later requires certificate exchange between WinCC OPC UA Client and SINEMA OPC UA Server.

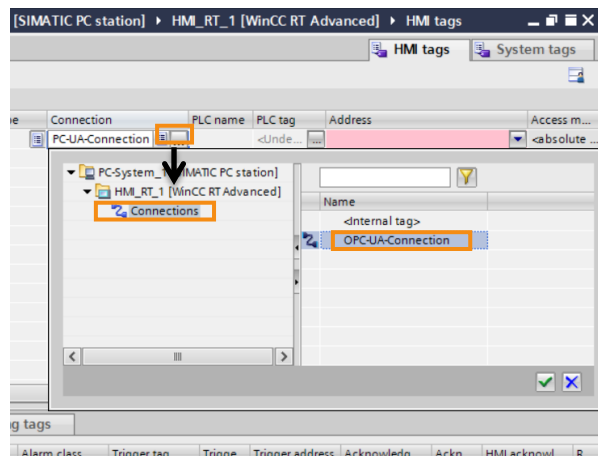
If you select a non-secure connection type, there is no certificate exchange.

Create OPC UA tags

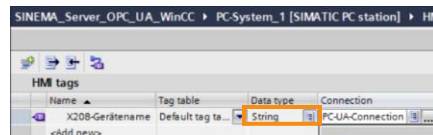
1. In the project tree you navigate to the item "HMI tags > Show all tags" and select it with a double-click. In the center top window you create the first new HMI tag by defining a tag name in the first line of the "Name" column (here: "X208-Gerätename").



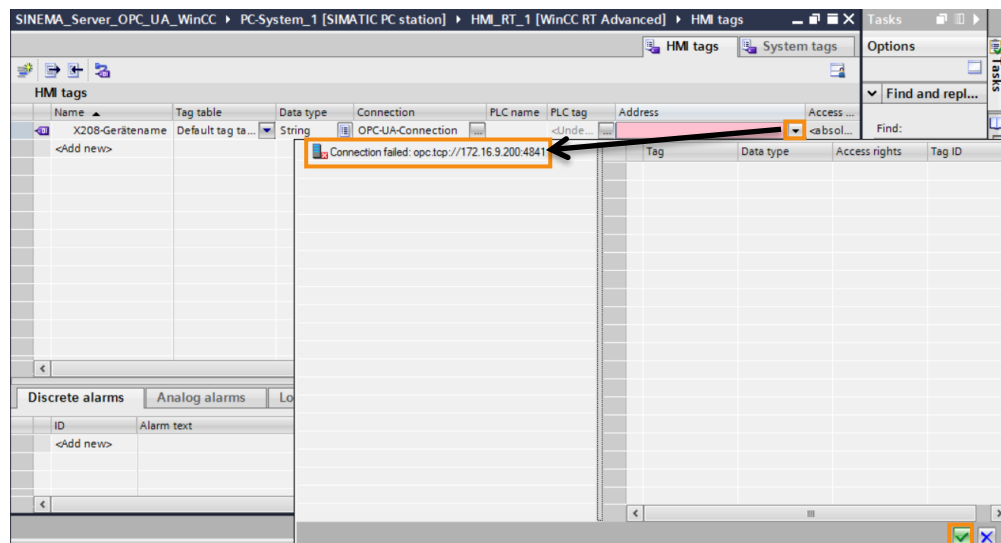
2. In the "Connection" column you select an "OPC-UA-Connection".



3. Then define the data type "String" for the new tag.



4. Finally, in the "Address" field you double-click the drop-down menu icon so that the "Connection failed" error message is displayed. Finish this dialog by clicking the green "OK" icon.



Result:

When trying to establish a connection the WinCC OPC UA Client has to authenticate itself to the SINEMA OPC UA Server on a certificate basis.

Since the SINEMA OPC UA Server finds no matching WinCC OPC UA Client certificate in its memory for trusted certificates, it denies the WinCC OPC UA Client establishment of a connection.

The rejected WinCC OPC UA Client certificate is stored in the "rejected" folder.

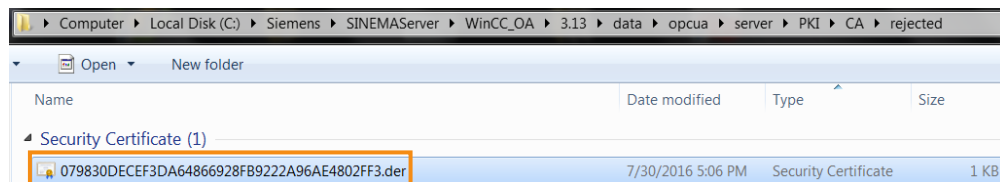
Authentication on the SINEMA OPC UA Server

Note

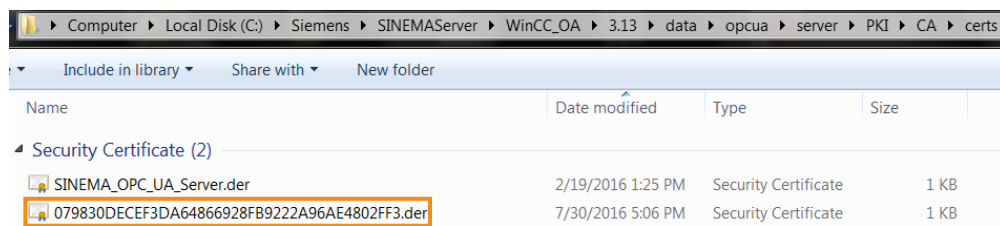
The WinCC OPC UA Client certificate must be made known to the SINEMA OPC UA Server for browsing the OPC UA tags stored in WinCC.

You perform the other steps on the PC with the TIA Installation or Engineering Station (ES).

1. Open the Windows Explorer on the PC [keyboard shortcut: Windows + E]. In the standard installation directory of SINEMA Server go to the "C:\Siemens\SINEMAServer\WinCC_OA\3.13\data\opcua\server\PKI\CA\rejected" that contains the rejected WinCC OPC UA Client certificate.



2. Move this certificate into the folder of the standard installation directory "C:\Siemens\SINEMAServer\WinCC_OA\3.13\data\opcua\server\PKI\CA\certs"

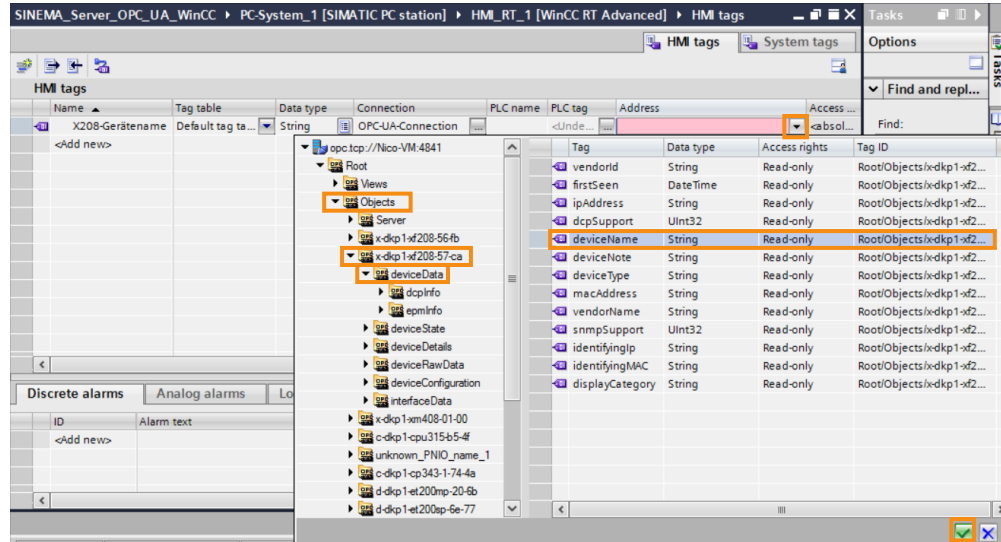


3. Go back to the TIA Portal and then to the last project step (see [Step 4](#) of the last section).
4. In the "Address" field you again double-click the drop-down menu icon.

Result:

Through the certificate exchange the OPC UA connection can be established and a list of the monitored network devices is displayed.

- In the device tree you navigate to the required device (in the example [Root > Objects > x-dkp1-xf208-57-ca > Device Data]).
Displayed in the right window are all the available OPC UA objects for the selected device.
For this example you select the "deviceName" tag.

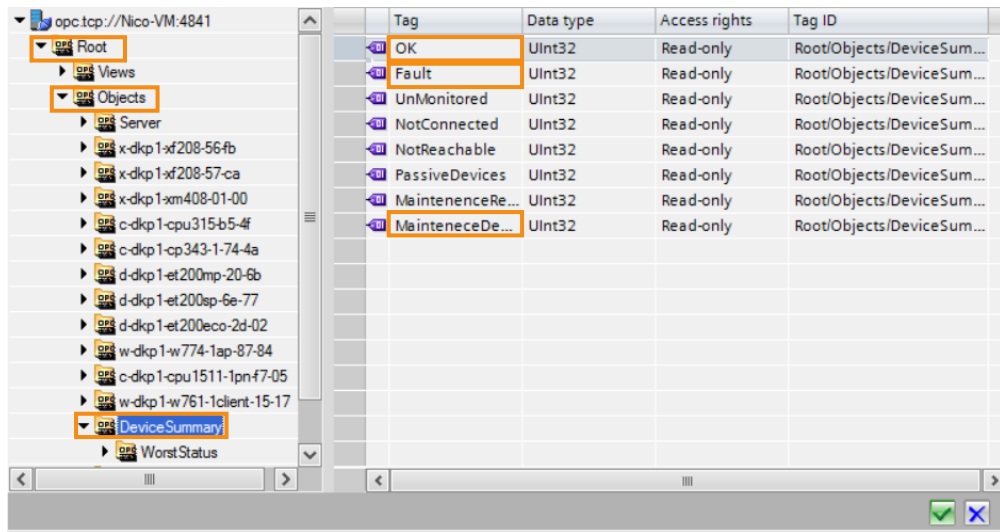


- Finish this dialog by clicking the green "OK" icon.
- In the example, a total of six different values are to be transferred to the higher-level HMI system via OPC UA. These are described in the table below.

No.	Name of the OPC UA tag	Data type
1.	X208 device name	String
2.	X208 device type	String
3.	X208 IP address	String
4.	SINEMA-Server-Number-Devices-OK	UInt32
5.	SINEMA-Server-Number-Devices-Fault	UInt32
6.	SINEMA-Server-Number-Devices-Maintenance_requested	UInt32

Repeat the previous section "Create OPC UA tags" from [Step 1](#) onwards and create the tags 2 to 6 in the HMI tag table.

Tags 4 to 6 are in the device tree under the item "Objects > Device Summary".



Create visualization screen

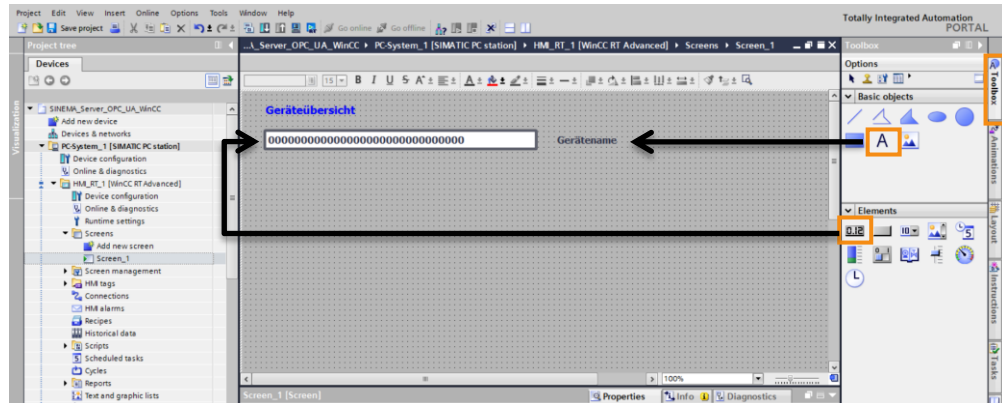
1. In the project tree you navigate to the item "Screens" and create a new visualization window. For this you double-click the item "Add new Screen".
2. Now in the "Screen_1" window that opens you create the desired HMI objects. In the example six output fields are linked with the following OPC UA tags:

No.	OPC UA tag	Field length
1.	X208 device name	String[30]
2.	X208 device type	String[30]
3.	X208 IP address	String[30]
4.	SINEMA-Server-Number-Devices-OK	Decimal[10]
5.	SINEMA-Server-Number-Devices-Fault	Decimal[10]
6.	SINEMA-Server-Number-Devices-Maintenance_requested	Decimal[10]

To open a new text and output field you open the "Toolbox" on the right.

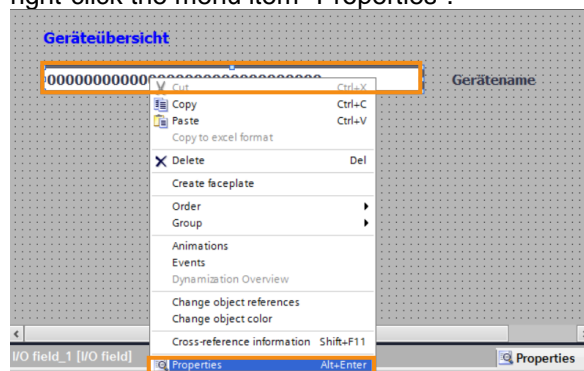
- The output field ("IO field") is in the "Elements" area.
- The text field ("text field") is in the "Basic objects" area.

Drag and drop them to the newly created "Screen_1".



3. Link the output field (IO field) to the HMI tag.

- a. For example, you select the newly created output field "Device name" and right-click the menu item "Properties".

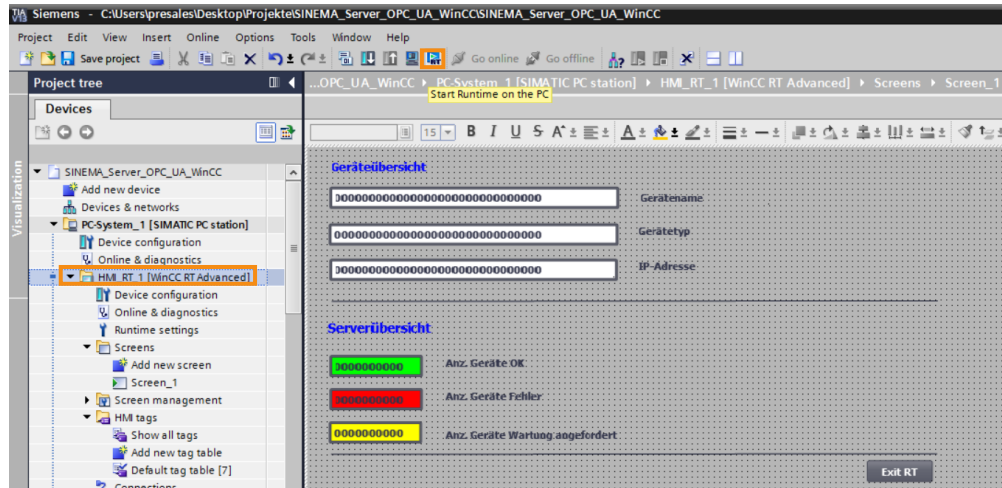


- b. In the menu [Properties] you select the "General" item in the Property list.
- c. In the center bottom window, in the "Type" area you select Mode = Output as the output mode.
- d. In the "Process" area you click the "... " icon.
- e. In the dialog that opens you select the HMI tag with the name "X208 Device name".
- f. Finish this dialog by clicking the green "OK" icon.

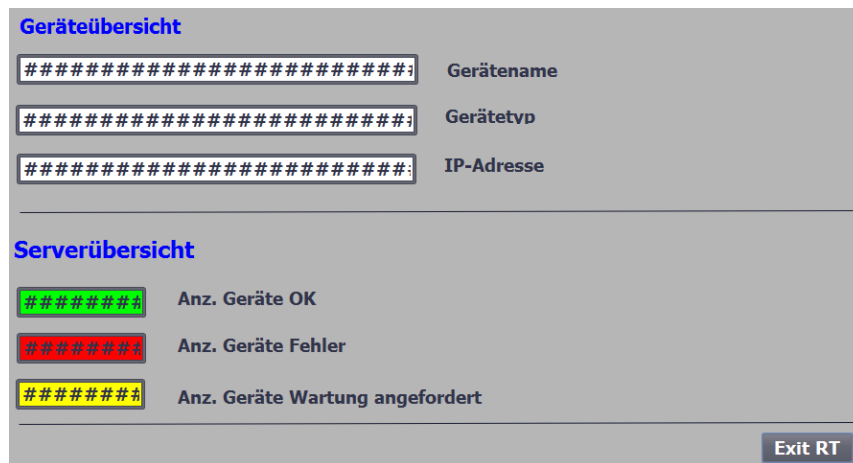
2.2.6 Start Encrypted OPC UA Data Exchange

Start WinCC Runtime

1. In the project tree you navigate to the item "HMI_RT_1" and in the toolbar you click the "Start Runtime on the PC" button to start WinCC Runtime.



2. The started WinCC Client Runtime can still show no values. It is absolutely necessary to leave the displayed visualization screen open even if it is not yet showing any correct data.



Note

When you start the Runtime the OPC UA Client initiates establishment of a connection to the OPC UA Server. In doing so the OPC UA Server sends its certificate, but this is not known to the OPC UA Client. Therefore the OPC UA Client rejects the server certificate and stores it in its internal "rejected" folder.

Store certificates

For encrypted OPC UA data exchange the certificates of the OPC UA Client and OPC UA Server have to be made known to their respective "counterpart".

Since each client has its own certificate, this making known of the certificate has to be done for each client.

Note

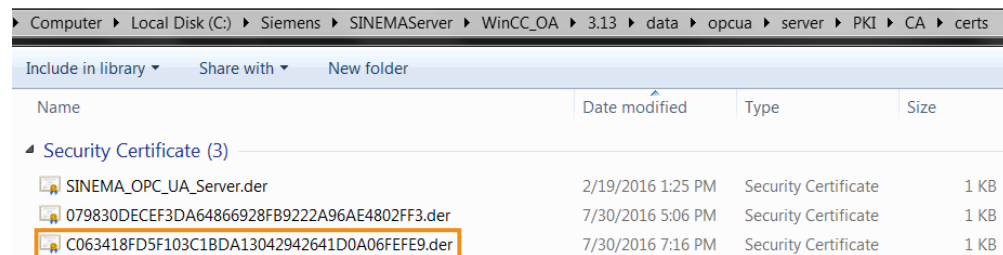
In this example the Engineering PC is also used for the WinCC Runtime. If this not the case in your situation, you have to perform the following steps on the device on which the WinCC Runtime is running.

1. Open the Windows Explorer [keyboard shortcut: Windows + E]. The directory "<C:\ProgramData\Siemens\CoRtHmiRTm\OPC\PKI\CA\default\rejected>" now contains the rejected SINEMA OPC UA Server certificate.
2. Move this certificate into the directory "<C:\ProgramData\Siemens\CoRtHmiRTm\OPC\PKI\CA\default\certs>".

Result:

Now the OPC UA Server certificate is known to the OPC UA Client. Because of the bidirectional nature of OPC UA communication you also have to make the OPC UA Client certificate known to the OPC UA Server.

3. For this you again open the Windows Explorer [keyboard shortcut: Windows + E]. The directory "C:\Siemens\SINEMAServer\WinCC_OA\3.13\data\opcua\server\PKI\CA\rejected" now contains the second rejected WinCC OPC UA Client certificate.
4. Move this certificate too into the folder of the standard installation directory "C:\Siemens\SINEMAServer\WinCC_OA\3.13\data\opcua\server\PKI\CA\certs".



Name	Date modified	Type	Size
Security Certificate (3)			
SINEMA_OPC_UA_Server.der	2/19/2016 1:25 PM	Security Certificate	1 KB
079830DECEF3DA64866928FB9222A96AE4802FF3.der	7/30/2016 5:06 PM	Security Certificate	1 KB
C063418FD5F103C1BDA13042942641D0A06FEFE9.der	7/30/2016 7:16 PM	Security Certificate	1 KB

Result:

After these steps both OPC UA Client certificates are now known to the SINEMA OPC UA Server and the OPC UA Client knows the required OPC Server certificate. In this way the client can establish a signed and encrypted connection to the server.

The visualization screen now shows the corresponding data "correctly".

The screenshot displays two sections: 'Geräteübersicht' and 'Serverübersicht'. The 'Geräteübersicht' section contains three input fields with labels: 'XF208-DK-Nico' (Gerätename), 'SCALANCE XF208 (0BA00-2AF2)' (Gerätetyp), and '172.16.9.41' (IP-Adresse). The 'Serverübersicht' section shows three status indicators: a green box with '9' for 'Anz. Geräte OK', a red box with '0' for 'Anz. Geräte Fehler', and a yellow box with '2' for 'Anz. Geräte Wartung angefordert'. An 'Exit RT' button is located in the bottom right corner.

Note

More information is available in the SINEMA Server Operating Instructions (Chapter 5): <https://support.industry.siemens.com/cs/ww/en/view/109482957>

3 History

Table 3-1

Version	Date	Change
V1.0	09/2016	First edition

4 Related Literature

Table 4-1

	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Download page of this entry https://support.industry.siemens.com/cs/ww/en/view/109740549
\3\	