Diagnostics Tools for SIMATIC IPCs

SIMATIC IPC DiagMonitor, SIMATIC Runtime Advanced V14

https://support.industry.siemens.com/cs/ww/en/view/109478242

Siemens Industry Online Support

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete with regard to configuration, equipment or any contingencies. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for the correct operation of the described products. These Application Examples do not relieve you of the responsibility of safely and professionally using, installing, operating and servicing equipment. When using these Application Examples, 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 Application Examples at any time and without prior notice. If there are any deviations between the recommendations provided in this Application Example and other Siemens publications – e. g. catalogs – the contents of the other documents shall 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 fundamental contractual obligations ("wesentliche Vertragspflichten"). The compensation for damages due to a breach of a fundamental contractual obligation is, 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 Application Examples 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.

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. Products and solutions from Siemens are only one part of such a concept.

It is the customer's responsibility to prevent unauthorized access to the customer's plants, systems, machines and networks. Systems, machines and components should only be connected with the company's network or the Internet, when and insofar as this is required and the appropriate protective measures (for example, use of firewalls and network segmentation) have been taken.

In addition, Siemens' recommendations regarding appropriate protective action should be followed. For more information on Industrial Security, visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them even more secure. Siemens strongly recommends to carry out updates as soon as the respective updates are available and always only to use the current 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.

In order to always be informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at http://www.siemens.com/industrialsecurity.

Table of Contents

1 Introduction

1.1 Overview of diagnostic and maintenance software for SIMATIC IPCs

The following diagnostic and signaling software tools are available for SIMATIC IPCs:

SIMATIC IPC DiagBase

SIMATIC IPC DiagBase is pre-installed on every SIMATIC IPC. This software is used to monitor your IPC and detect potential system failure in due time, plan maintenance activities and avoid plant downtimes. SIMATIC IPC DiagBase makes the following diagnostics data available locally:

Depending on the model, the following monitoring functions are supported:

- Monitoring the processor, mainboard and RAM temperature
- Monitoring the fans and battery
- Monitoring the hard disks and CompactFlash cards
- Operating hours counter

Furthermore it is possible to save or load your BIOS settings or a BIOS image.

Note The following application example addresses the use of the SIMATIC IPC DiagMonitor and DiagBase.

Diagnostics options for SIMATIC IPCs (with IPC DiagBase, IPC DiagMonitor, WinCC (TIA Portal), or WinCC V7)
***SIOS Entry ID:* 109478242**

SIMATIC IPC DiagMonitor

SIMATIC IPC DiagMonitor includes the functional scope of the SIMATIC IPC DiagBase. In addition, the provided diagnostics data can be sent via SNMP or OPC UA. SIMATIC IPC DiagMonitor can also access diagnostics data from remote SIMATIC IPCs and send messages and alarms per email or SMS to prevent plant downtimes.

In this application example, diagnostics data are collected using SIMATIC IPC DiagMonitor and provided to the network with secure OPC UA communication as well as in WinCC Runtime.

SIMATIC IPC Remote Manager

The SIMATIC IPC Remote Manager is used for remote access to your SIMATIC IPC. This enables you to perform BIOS or program updates or troubleshooting activities on the SIMATIC IPC via remote access without having to be on site. Prerequisites to using the SIMATIC IPC Remote Manager is that the Intel AMT (Active Management Technology) function is activated on the SIMATIC IPC.

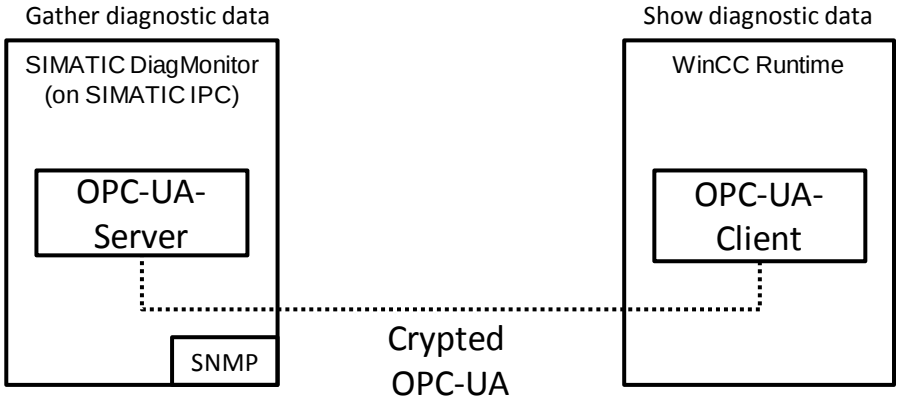
Note The following application example shows how to operate your SIMATIC IPC via remote access using the SIMATIC IPC Remote Manager:

SIMATIC IPC with Intel® AMT: Diagnostics and Remote Maintenance of SIMATIC Industrial PCs
***SIOS Entry ID:* 52310936**

1.2 Mode of operation

This application example describes how to display the diagnostics data in SIMATIC applications. The possibility of displaying the diagnostic data in the SIMATIC IPC DiagMonitor on the same or another IPC is not affected from this application example.

Figure 1-1 Transfer of diagnostics data via OPC UA connection



- The SIMATIC IPC DiagMonitor V5.0 software collects diagnostics data of a SIMATIC IPC and makes them available via an OPC UA server for further analysis.
- The diagnostics data can either be outputted to the local SIMATIC Panel PC or to another Panel PC via OPC UA. In this example, a secure OPC UA connection is used.
- The diagnostics data of the SIMATIC IPC are displaying on a WinCC Runtime Advanced V14
  Optional: Use of a SIMATIC Rack PC. The diagnostics data of the rack PC are transferred to WinCC Runtime Advanced V14 via OPC UA communication too.

Software and operating system

The SIMATIC Rack PC has a Windows Server 2012 R2 operating system installed on it. In addition, SIMATIC DiagMonitor V5.0 is installed.

The Panel PC has a Windows 7 operating system installed on it. In addition, SIMATIC DiagMonitor V5.0 is installed.

1.3 Components used

This application example has been created with the following hardware and software components:

Table 1-1 Components used

Component	Number	Article number	Note
SIMATIC IPC 847D	1	6AG4114-2….-….	Rack PC, OPC server
SIMATIC IPC 477D	1	6AV7240-.B…-….	Panel PC, OPC Client
SIMATIC IPC DiagMonitor V5.0	2	6ES7648-6CA05-0YX0	
WinCC Advanced V14 (TIA Portal)	1	6AV210.-….4-0	
WinCC RT Advanced V14	1	6AV2104-….4-0	
Windows Server 2012 R2 Standard	1		For IPC 847D
Windows 7 Ultimate	1		For IPC 477D

This application example consists of the following components:

Table 1-2 Components of the application example

Component	File name	Note
Documentation	109478242_Diagnostic_IPC_WinCCV14_DOC_en.pdf	
Example project	109478242_Diagnostic_IPC_WinCCV14.zip	

2 Valuable Information

2.1 Configuring the SNMP service

Before you can use the DiagMonitor, you have to configure the SNMP service on each device running DiagMonitor.

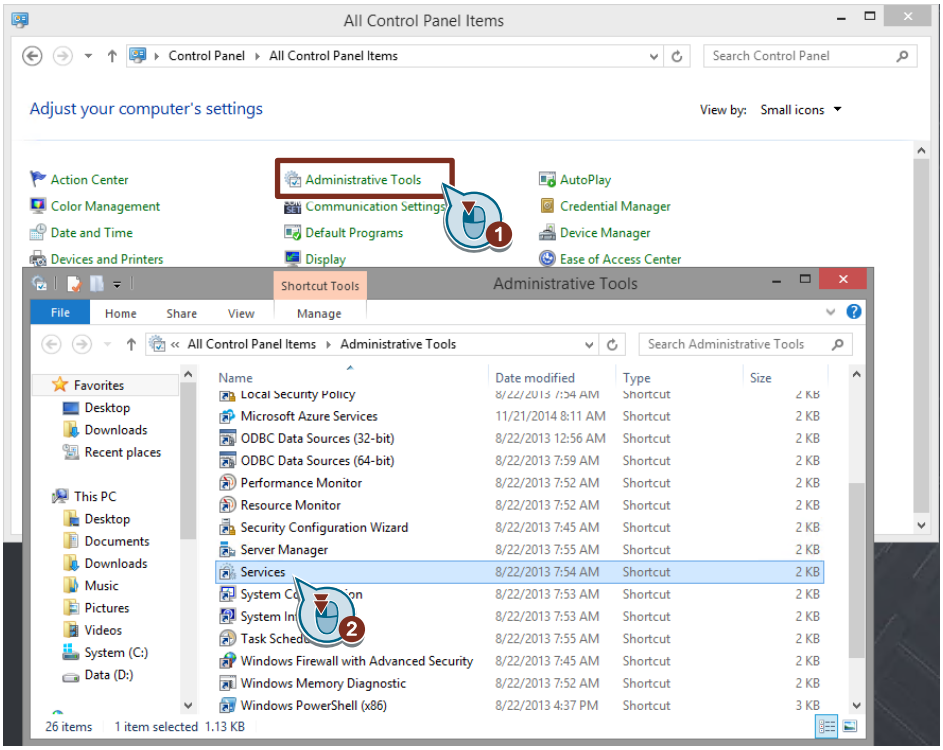
The SNMP service is preconfigured to only accept SNMP packages from previously set “hosts”.

You have to add the IPCs to the list of “trusted hosts” before you can use SIMATIC DiagMonitor V5.0. Proceed as follows:

Operating system

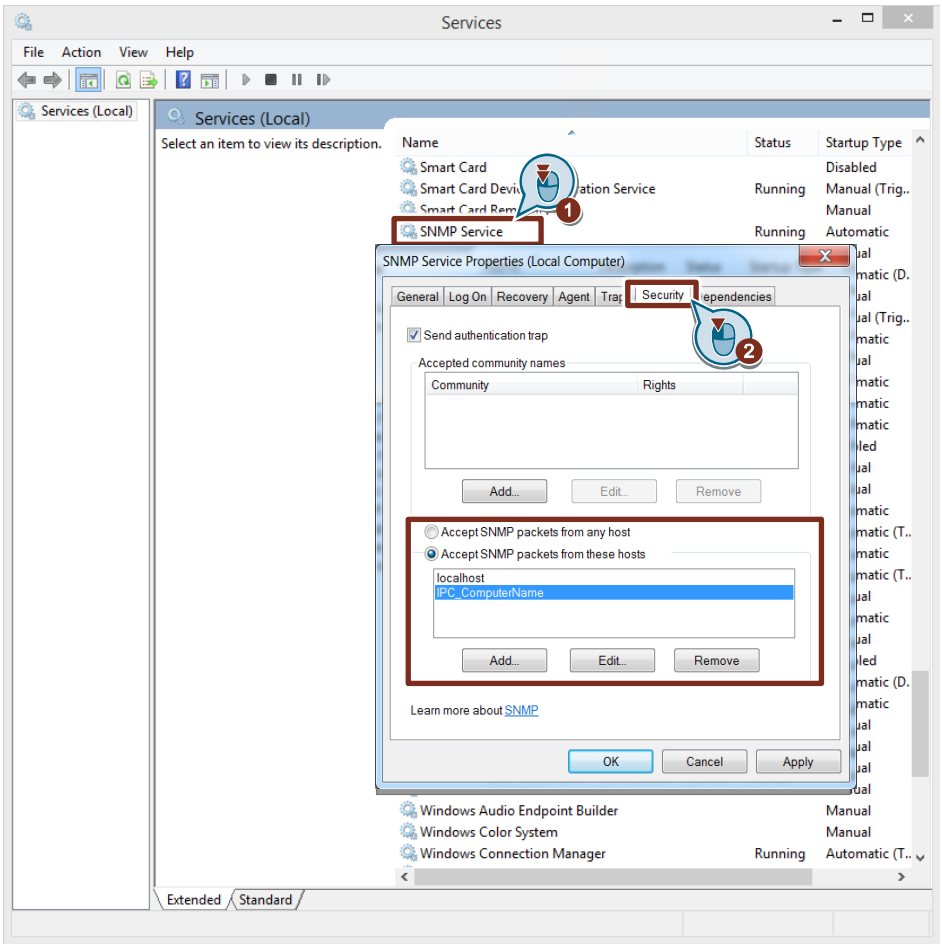
1. Open the “Control Panel”.
2. Click on “Administrative Tools” and open “Services”.

Figure 2-1 Service administration under Windows 7



3. Double-click on “SNMP Service”.
4. Click the “Security” tab.
5. Add all IP addresses or computer names of the computers that you would like to exchange SNMP packets with under “Accept SNMP packets from these hosts” or select “Accept SNMP packets from any hosts”.

Figure 2-2 SNMP configuration

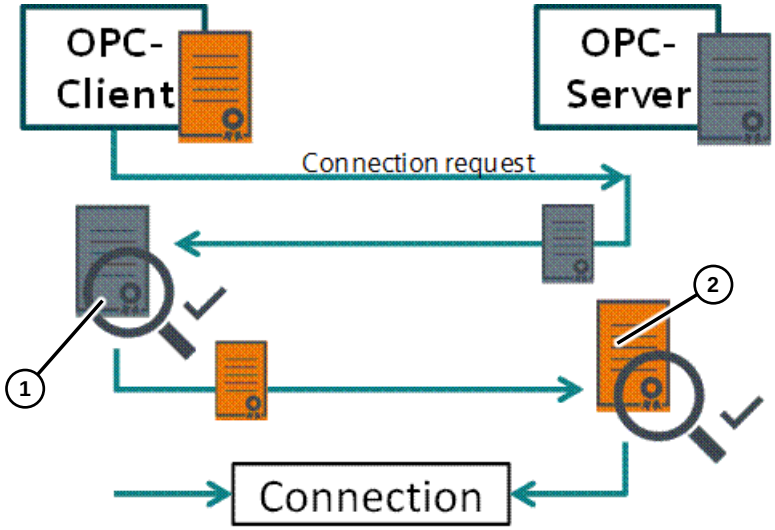


2.2 Certificate administration

2.2.1 Exchange of certificates when establishing a secure OPC UA connection

Certificates are exchanged between server and client when establishing a secure OPC UA connection. The sequence is, simplified, as follows:

Figure 2-3 Establishing a secure OPC UA connection



The client sends a connection request to the server. The server returns its public OPC UA server certificate. The client checks the server certificate for validity (1).

The client sends its certificate to the server once the certificate has been classified as valid and trustworthy. Then the server checks, if the client certificate is valid and trustworthy (2).

Note The OPC UA server saves unknown client certificates in the "rejected" directory in its certificate administration, according to the settings in chapter 2.2.2.

2.2.2 File path of the certificates in the file system

OPC server and OPC client save the certificates in the Windows file system under the following file paths:

Table 2-1 File path of the certificates

Object	Storage location
OPC server (DiagMonitor V5.0)	C:\Program Files (x86)\Siemens\Automation\DiagnosticManagement\DiagMonitor\OpcUaCertStore **\issuers** **\certs** **\crl** **\own** *(server certificates)* **\certs** *(1 public certificate *.der)* **\private** *(1 private certificate *.pem)* **\rejected** *(contains rejected client certificates)* **\trusted** **\certs** *(contains trusted client certificates)* **\crl**
OPC client (RT Advanced)	C:\ProgramData\Siemens\CoRtHmiRTm\OPC\PKI\CA\default **\certs** *(contains trusted client and server certificates)* **\private** **\rejected** *(contains rejected server certificates)*
OPC client (WinCC V7.4)	C:\ProgramData\Siemens\WinCC\opc\UAClient\PKI

Note The file paths refer to the default installation paths. If you have chosen other installation paths, the file paths where the certificates are saved may differ.

2.3 Firewall settings

2.3.1 OPC UA client

The use of the Windows firewall is possible for use with WinCC V7.4 and WinCC Runtime V14. You can configure your Windows settings and the firewall for WinCC V7.4 and WinCC Runtime V14 with the SecurityController.

1. To do this, open the tool SecurityController (Programs > Siemens Automation > Security Controller).
2. Click on “Repeat settings”.
3. Close the tool.

2.3.2 OPC UA server

Open the following port for incoming TCP connections:

48010 (see configuration of the OPC UA server in chapter 3.3)

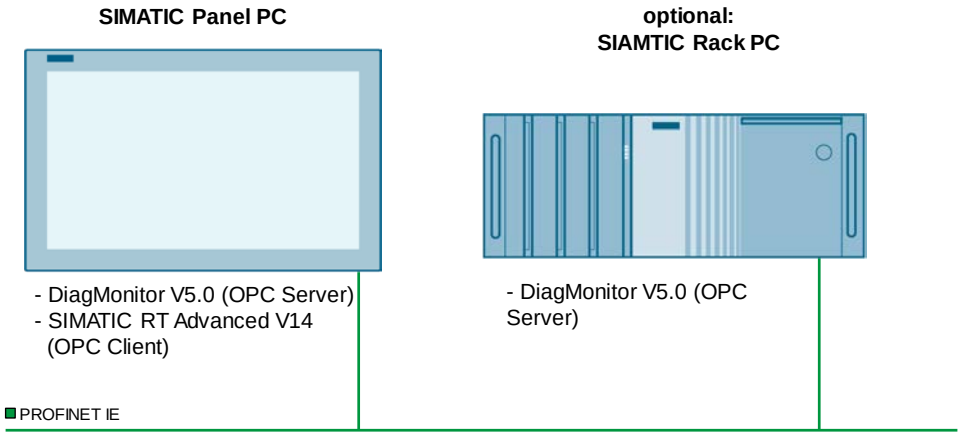
Note Opening ports in the firewall poses a security risk. Therefore, only open the ports required for the TIA Portal or WinCC.

3 Configuration

This chapter shows how to transfer diagnostics data from SIMATIC IPCs locally or via a secure OPC connection and how to display them in a WinCC Runtime Advanced V14.

3.1 Overview

Figure 3-1 Hardware setup with software components



The OPC server of the SIMATIC Panel PC provides the diagnostics data of DiagMonitor V5.0. These data are visualized on the Panel PC on a configured panel image of WinCC Runtime Advanced V14.

In addition, a Rack PC with Windows Server 2012 R2 and DiagMonitor V5.0 installed is added. The Rack PC diagnostics data will also be displayed on the WinCC Runtime of the Panel PC.

The diagnostics data are transferred via the OPC UA interface.

3.2 Prerequisites

Make sure to accomplish the following steps to run this application example:

- The software SIMATIC IPC DiagMonitor V5.0 is installed on each SIMATIC IPC.
- The SIMATIC Panel PC can be accessed from the Engineering PC via TCP/IP.
- The required ports have been opened in your firewall (chapter 2.3)

3.3 Initial setup of the OPC server

To configure the WinCC Runtime Advanced, you first need to set up the OPC server of the DiagMonitor V5.0. This step is required to be able to browse online on the OPC server and add HMI tags when configuring WinCC Advanced.

Once setup is completed, you will configure the OPC server for secure operation.

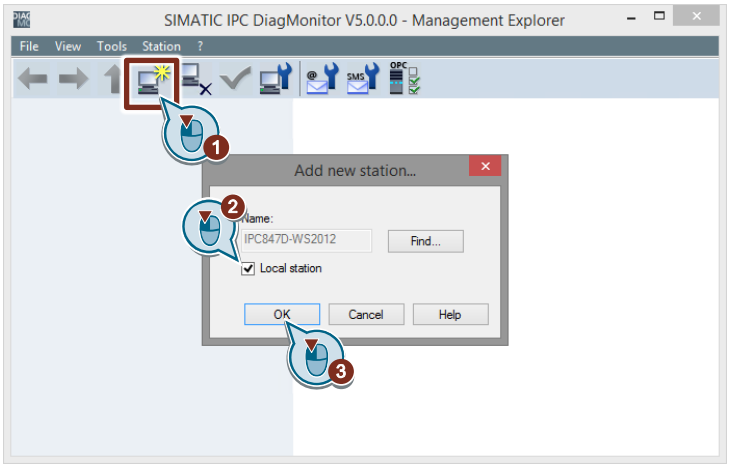
Note Alternatively, you can add the OPC variables manually without browsing.

In order to prepare the OPC server for the next steps, proceed as follows:

DiagMonitor: add “Station”

1. Start "SIMATIC IPC DiagMonitor V5.0", e.g. by double-clicking the icon of the AlarmManager in the system tray.
2. Click on "Add station" (1).
3. Check the "Local Station" (2) check box and click "OK" (3).

Figure 3-2: DiagMonitor – add “Station”



Note If you receive the message that the station cannot be added, then check the SNMP settings of your system, see chapter 2.1 Configuring the SNMP service.

Configuring the OPC server

To configure the OPC server, you have to manually adapt the XML configuration file "OPCUaConfig.xml”.

1. To do this, open the “SIMATIC IPC DiagMonitor V5.0” installation folder.

Default file path: C:\Program Files (x86)\Siemens\Automation\DiagnosticManagement\DiagMonitor

2. Open the file "OpcUaConfig.xml" with a text editor with administrator rights.
3. As a first step, only change the IP address of the OPC server.
   The default entry is: *<Url> opc.tcp://**[NodeName]** </Url>.*
   Instead of *[NodeName]*, enter the IP address of the IPC running on the DiagMonitor add port 48010:

   Result: *<Url> opc.tcp://**172.16.50.10:48010** </Url>.*

Figure 3-3: Changes in the OPC server configuration file

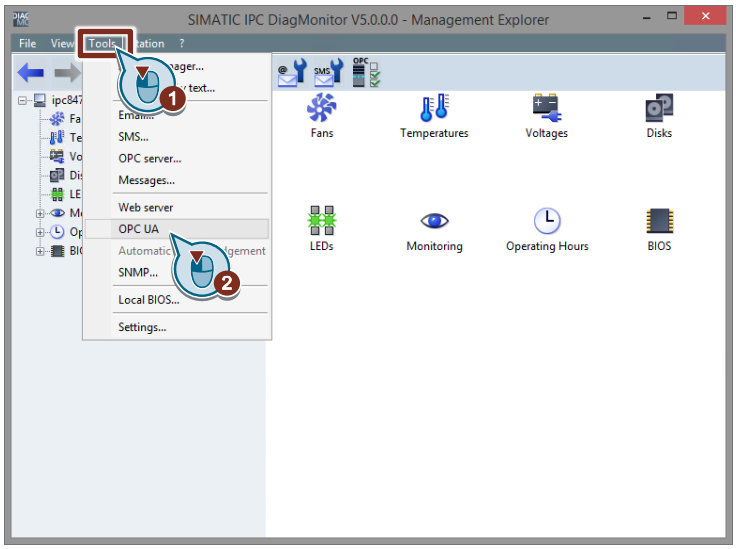
```
<Url>opc.tcp://[NodeName]172.16.50.10:48010</Url>¶
<!--·Optional·URL·that·allows·to·define·a·specific·address·the·stack·should·use·to·bind·to.¶
Can·be·used·to·bind·the·endpoint·to·a·specific·network·card·or·to·localhost·only.¶
<StackUrl>opc.tcp://192.168.0.15:48010</StackUrl>¶
-->¶
<SecuritySetting>¶
   →   <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#None</SecurityPolicy>¶
   →   <MessageSecurityMode>None</MessageSecurityMode>¶
</SecuritySetting>¶
<SecuritySetting>¶
   →   <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15</SecurityPolicy>¶
   →   <MessageSecurityMode>Sign</MessageSecurityMode>¶
   →   <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>¶
</SecuritySetting>¶
<SecuritySetting>¶
   →   <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Basic256</SecurityPolicy>¶
   →   <MessageSecurityMode>Sign</MessageSecurityMode>¶
   →   <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>¶
</SecuritySetting>¶
<!--·Flag·indicating·if·the·endpoint·is·provided·in·GetEndpoints·and·is·therefore·visible·to·a·client.·
```

4. Save the file and close the Editor.

Activating the OPC server

To activate the OPC UA server, click on "Tools > OPC UA" in the navigation bar.

Figure 3-4: DiagMonitor – Starting the OPC UA server



Note

The OPC server is now activated without security settings.

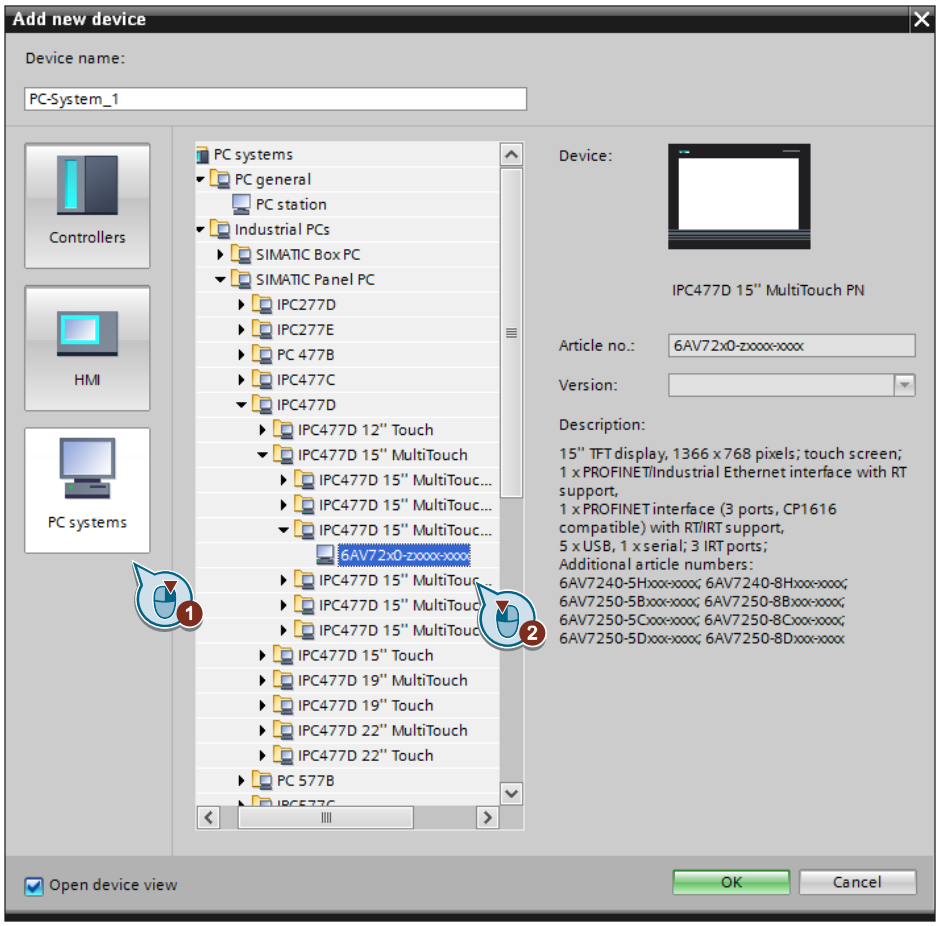
Make sure to configure the OPC server after the WinCC configuration, so that only secure connections are possible (see chapter 3.6)

3.4 Configuration of the SIMATIC Panel PC

Adding devices

1. Open TIA Portal on your engineering PC and create a new project.
2. Add the device "IPC477D 15" Multitouch PN".

Figure 3-5



3. Add a "WinCC RT Advanced" to the added device with drag&drop.

3.4.1 SIMATIC Panel PC: WinCC Runtime Advanced configuring

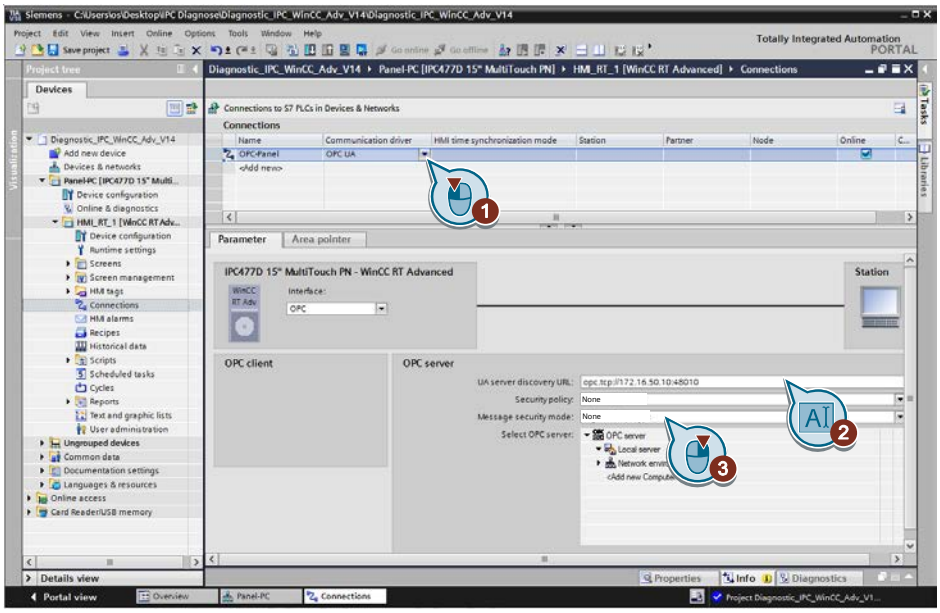
Creating the OPC UA connection

1. Select the operator panel (SIMATIC Panel PC).
2. In the project tree, open the “Connections” of the WinCC RT Advanced.
3. Create a new connection of the type “OPC UA” (1).
4. Make the following settings in the section "OPC server":

Table 3-1 OPC server settings

Setting	Value
UA server URL	opc.tcp://172.16.50.10:48010
"Security policy"	None
"Message security mode"	None

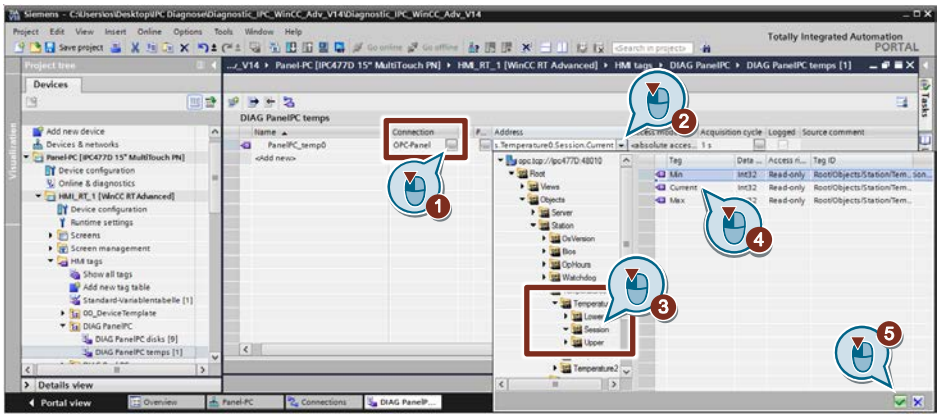
Figure 3-6: Configuring the OPC connection



Creating HMI tags

1. To monitor diagnostics data, you create HMI tags. Connect the HMI tags with the appropriate OPC tags.
   To do this, proceed as follows:

Figure 3-7: Adding tags



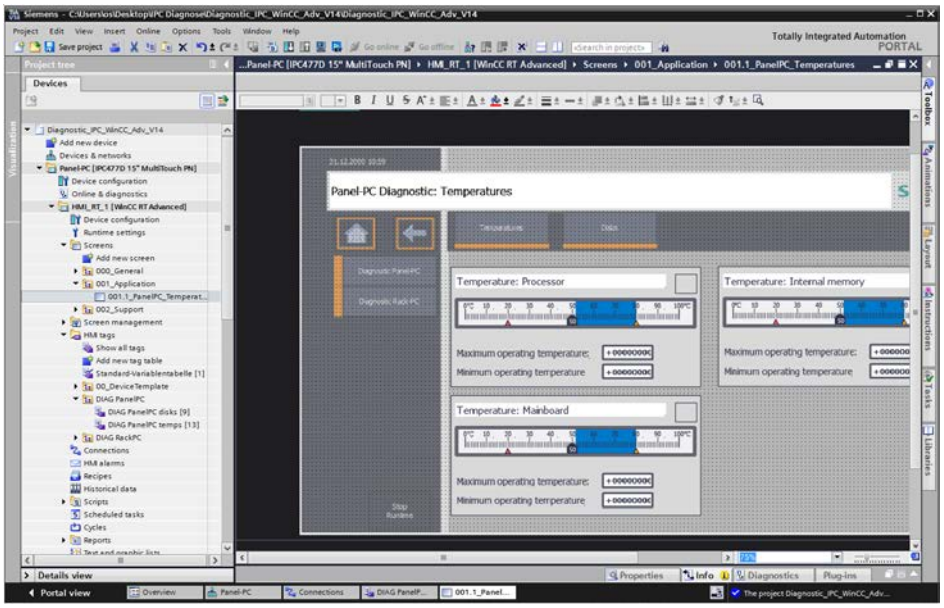
- Create a new tag.
- Select the OPC connection (1).
- Select the appropriate address to the server (2-4).
- Click on the button to confirm your choice (5).

Proceed as described for the other tags.

Creating an HMI screen

1. Create a new HMI screen.
2. Place I/O fields, bars or gauge controls in the screen to display the diagnostics data.

Figure 3-8



3. Connect the objects with the created HMI tags.
4. Load the project into the Panel PC.

3.5 Configuration of the SIMATIC Rack PC

Note This section is optional. The example configuration will also work without the Rack PC. If you do not use a Rack PC, continue with the next chapter.

Preparation

Check the connection from the Panel PC to the OPC server of the Rack PC after you have configured it with “DiagMonitor V5”.

SIMATIC Rack PC: WinCC Runtime Advanced configuring

1. Select the operator panel (SIMATIC Rack PC).
2. Create another OPC connection for the Rack PC in the WinCC Runtime of the Panel PC. Proceed as described in chapter 3.4.
3. Create HMI tags to monitor the Rack PC diagnostics data. Connect them with the respective OPC tags.
   Proceed as described in chapter 3.4.
4. Create a new screen.
5. Place I/O fields, bars or gauge controls in the screen to display the diagnostics data.
6. Connect the objects with the HMI tags.
7. Load the project into the Panel PC.

3.6 OPC server security settings

Once the WinCC Advanced configuration is completed, you configure the security settings for the OPC server.

Adapting the XML configuration file

To adapt the XML file PCUaConfig.xml", first stop the DiagMonitor OPC server.

1. Open the "SIMATIC DiagMonitor V5.0" installation folder.

   Default file path: C:\Program Files (x86)\Siemens\Automation\ DiagnosticManagement\DiagMonitor
2. (optional) First create a copy of the unchanged file "OpcUaConfig.xml", if you want to re-establish the original state.
3. Open the file "OpcUaConfig.xml" with a text editor with administrator rights.
4. An overview of the description of the individual XML elements can be found under:

   https://support.industry.siemens.com/cs/ww/en/view/109741042.
5. To ensure secure communication between the OPC UA server and the OPC UA clients, you adapt the following XML elements:

Deleting or commenting out the following XML elements

Table 3-2

XML element	Property of the XML element
<SecuritySetting>	Contains the XML element <MessageSecurityMode> with the value "None"
<MessageSecurityMode>	Contains the value "Sign"

Changing the value of the following XML elements

Table 3-3

XML element	Default value	New value
<Url>	opc.tcp:// [NodeName]:48010	opc.tcp:// <IP address of the computer running the OPC server>, e.g. 172.16.50:10:48010
<AutomaticallyTrustAll ClientCertificates>	true	false

Figure 3-9: Summary of the required changes in OpcUaConfig.xml

```
<Url>opc.tcp://[NodeName]172.16.50.10:48010</Url>
<!-- Optional URL that allows to define a specific address the stack should use to bind to.
Can be used to bind the endpoint to a specific network card or to localhost only.
<StackUrl>opc.tcp://192.168.0.15:48010</StackUrl>
-->
<SecuritySetting>
     <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#None</SecurityPolicy>
     <MessageSecurityMode>None</MessageSecurityMode>
</SecuritySetting>
<SecuritySetting>
     <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15</SecurityPolicy>
     <MessageSecurityMode>Sign</MessageSecurityMode>
     <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
</SecuritySetting>
<SecuritySetting>
     <SecurityPolicy>http://opcfoundation.org/UA/SecurityPolicy#Basic256</SecurityPolicy>
     <MessageSecurityMode>Sign</MessageSecurityMode>
     <MessageSecurityMode>SignAndEncrypt</MessageSecurityMode>
</SecuritySetting>
<!-- Flag indicating if the endpoint is provided in GetEndpoints and is therefore visible to a client.
<IsVisible>true</IsVisible>
<!-- Flag indicating if the endpoint URL is provided as discovery URL. Default is true. -->
<IsDiscoveryUrl>true</IsDiscoveryUrl>
<!-- This option can be activated if certificates are used only for message security but not for appli
If set to true, all client certificates will be accepted automatically and they are not stored.
It is strongly recommended to use this option only together with user authentication. -->
<AutomaticallyTrustAllClientCertificates>truefalse</AutomaticallyTrustAllClientCertificates>
<!-- Some of the OPC UA security checks are optional in OPC UA or cause interoperability issues with c
and can be disabled by an administrator of the OPC UA server through the following configuration optio
```

6. Save the file.

Note If the OPC UA server has already been started up, shut down the OPC UA server and re-start it for the changes in file "OpcUaConfig.xml" to take effect.

3.7 Adjusting the OPC connections in the TIA Portal

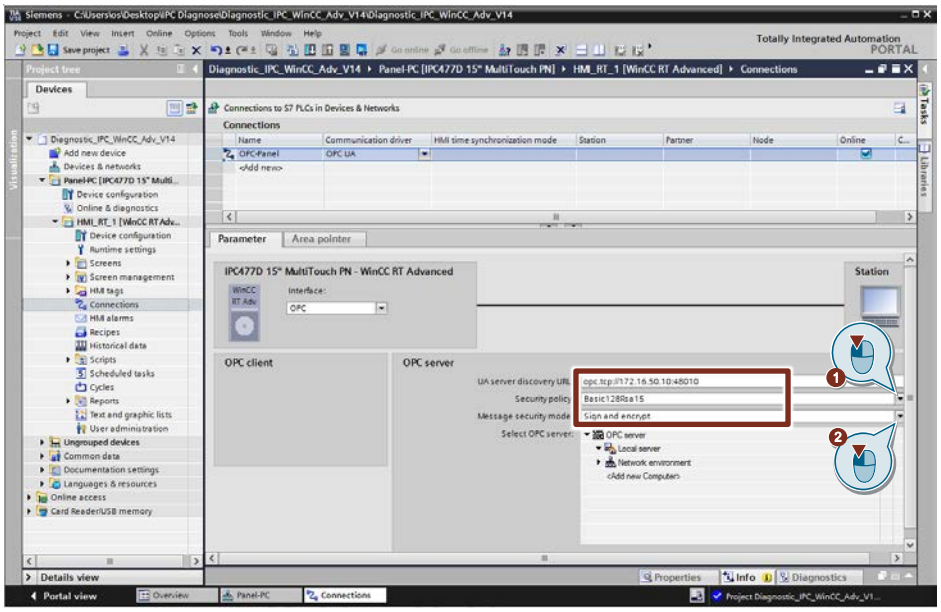
To adapt the OPC connections to the security settings of the OPC server, proceed as follows:

1. Open the TIA Portal project.
2 In the project tree, open the “Connections” of the WinCC Runtime Advanced.
3 Change the settings of the existing OPC connections as follows:

Table 3-4 Changes of the OPC server settings

Setting	Value
"Security policy"	"Basic128Rsa15"
"Message security mode"	"Sign and encrypt"

Figure 3-10 Changing the OPC connection



3.8 Exchange of certificates

The general function principle of how certificates are exchanged for encrypted OPC connections is described in chapter 2.2. This chapter is important for understanding the instructions given below.

Note Figure 2-3 Establishing a secure OPC UA connection shows the process of exchanging certificates which is described below.

1. To create the certificates, start the Runtime.
2. Immediately after this is done, exit the runtime.
3. On the PC of the WinCC Runtime, browse to the file path of the OPC client certificates (here: WinCC Runtime) in Windows Explorer:

   C:\ProgramData\Siemens\CoRtHmiRTm\OPC\PKI\CA\default\rejected
4. During the previous start of the runtime, the OPC server certificate was stored in the “rejected” folder of the OPC client.
   Cut the certificate and paste it in the “trusted” folder.

   C:\ProgramData\Siemens\CoRtHmiRTm\OPC\PKI\CA\default\trusted
5. Then start the runtime once again. Exit the runtime after it has started.
6. During the previous start of the runtime, the OPC client certificate was stored in the “rejected” folder of the OPC server (DiagMonitor).

   *C:\Program Files (x86)\Siemens\Automation\DiagnosticManagement \DiagMonitor\OpcUaCertStore**rejected***

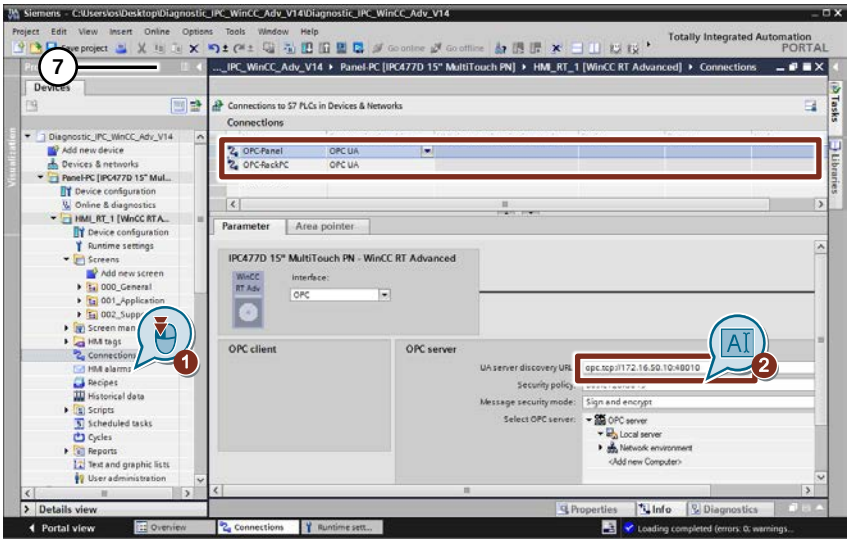
   Cut the certificate and paste it in the “trusted” folder.

   *C:\Program Files (x86)\Siemens\Automation\DiagnosticManagement \DiagMonitor\OpcUaCertStore**trusted\certs***

3.9 Operating the Application Example

1. Download the project file from the entry page of this application example.
2. Unzip and open the file with TIA Portal V14.
3. Change the IP address of the used devices.
4. In the project tree, adapt the OPC UA connections under “Connections”.

Figure 3-11 Configuring the OPC connection

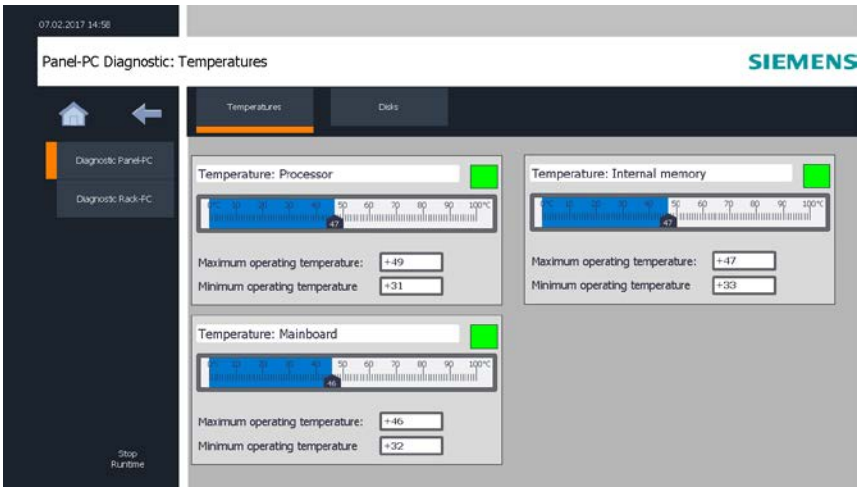


5. Load the project into the Panel PC.

Start the application example

1. Start WinCC Runtime on the Panel PC.
2. Click on “Application” to go to the diagnostics screens.

Figure 3-12 WinCC Runtime Advanced Screen on the SIMATIC Panel PC



Note If now values are displayed, check if there are any certificates for the OPC connection in the “rejected” folders. For this purpose, refer to chapter 2.3.

Navigation

Use the vertical navigation bar to toggle between the diagnostics data of the Panel PC and of the Rack PC. Use the horizontal navigation bar to display diagnostics data for “Temperature values”, “Hard disks” and “Fans”.

4 Appendix

4.1 Service and support

Industry Online Support

Do you have any questions or need support?

Siemens Industry Online Support offers access to our entire service and support know-how as well as to our services.

Siemens Industry Online Support is the central address for information on our products, solutions and services.

Product information, manuals, downloads, FAQs and application examples – all information is accessible with just a few mouse clicks at https://support.industry.siemens.com/.

Technical Support

Siemens Industry's Technical Support offers quick and competent support regarding all technical queries with numerous tailor-made offers – from basic support to individual support contracts.

Please address your requests to the Technical Support via the web form: www.siemens.com/industry/supportrequest .

Service offer

Our service offer comprises, among other things, the following services:

- Product Training
- Plant Data Services
- Spare Parts Services
- Repair Services
- On Site and Maintenance Services
- Retrofit & Modernization Services
- Service Programs and Agreements

Detailed information on our service offer is available in the Service Catalog: https://support.industry.siemens.com/cs/sc

Industry Online Support app

Thanks to the "Siemens Industry Online Support" app, you will get optimum support even when you are on the move. The app is available for Apple iOS, Android and Windows Phone.
https://support.industry.siemens.com/cs/ww/en/sc/2067

4.2 Links and literature

Table 4-1 Link list

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/109478242
\3\	SIMATIC IPC DiagMonitor V5 Manual https://support.industry.siemens.com/cs/ww/en/view/39129913
\4\	Configuration DiagMonitor V5 OPC UA Server https://support.industry.siemens.com/cs/ww/en/view/109741042
\5\	Unified Automation UaExpert https://www.unified-automation.com/downloads/opc-ua-clients.html

4.3 Change documentation

Table 4-2 Change history

Version	Date	Modifications
V1.0	06/2017	First version
V1.1	07/2017	Slight changes