

SIEMENS

SIMATIC

Instructions on the TIA Portal Cloud Connector

Operating Manual

Introduction to the TIA Portal Cloud Connector	1
System requirements	2
Providing a virtual machine (VM)	3
Using the virtual machine (VM)	4

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.
⚠ WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.
⚠ CAUTION
indicates that minor personal injury can result if proper precautions are not taken.
NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

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

Table of contents

1	Introduction to the TIA Portal Cloud Connector.....	5
1.1	Security information.....	5
1.2	Basics of working with the TIA Portal Cloud Connector.....	5
1.3	User interface of the TIA Portal Cloud Connector.....	7
1.4	Application cases of the TIA Portal Cloud Connector.....	17
1.5	Special considerations when working in a virtual machine.....	19
1.6	Using certificates.....	20
2	System requirements.....	23
2.1	System requirements PG/PC.....	23
2.2	System requirements for VM.....	24
2.3	Licenses.....	26
2.4	Allocating a license of the user device.....	27
3	Providing a virtual machine (VM).....	29
3.1	Creating a new VM template.....	29
3.2	Saving user and project settings centrally.....	30
3.3	Using a license key server.....	32
3.4	Installing the TIA Portal Cloud Connector in the VM.....	32
4	Using the virtual machine (VM).....	37
4.1	Installing the TIA Portal Cloud Connector on the PG/PC.....	37
4.2	Configuring the TIA Portal Cloud Connector on the PG/PC.....	38
4.3	Configuring the TIA Portal Cloud Connector in the VM.....	40
4.4	Using certificates (for HTTPS connections only).....	42
4.4.1	Creating certificate for data encryption.....	42
4.4.2	Exporting certificate for data encryption.....	43
4.4.3	Importing certificate for data encryption.....	44
4.4.4	Selecting certificate for data encryption.....	45
4.4.5	Creating certificate for user authentication.....	46
4.4.6	Exporting certificate for user authentication.....	47
4.4.7	Importing certificate for user authentication.....	48
4.4.8	Adding certificate for user authentication.....	49
4.4.9	Selecting certificate for user authentication.....	50
4.4.10	Removing certificate for user authentication.....	51
4.5	Online connection via the TIA Portal Cloud Connector.....	51
4.6	Using the virtual machine (VM) offline.....	52

Index.....55

Introduction to the TIA Portal Cloud Connector

1.1 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> (<http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx>).

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> (<http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx>).

1.2 Basics of working with the TIA Portal Cloud Connector

Function of the TIA Portal Cloud Connector

The TIA Portal allows you to work in a virtual environment. The TIA Portal Cloud Connector is a cross-product option, which also allows access to local PG/PC interfaces and SIMATIC hardware connected to them in TIA Portal Engineering, even though the engineering itself is operated via Remote Desktop in a private cloud.

The "TIA Portal Cloud Connector" add-on package allows you to access your local SIMATIC hardware connected to the PG/PC from the VM. This requires installation of the TIA Portal Cloud Connector in the VM as well as on the PG/PC to which the SIMATIC hardware is connected. In addition, the TIA Portal Cloud Connector allows you to access the SIMATIC hardware of another PG/PC via the remote desktop connection. The other PG/PC can be located in a different network. Such access is not possible without the TIA Portal Cloud Connector.

1.2 Basics of working with the TIA Portal Cloud Connector

The use of virtual machines together with the TIA Portal Cloud Connector in a private cloud offers the following advantages:

- Support for modern private cloud infrastructures:
 - Full scalability
 - No installation on individual workstations required
 - Central maintenance and administration of the TIA Portal in the VM
 - Central data storage for projects and libraries
- Cross-network online access to PLCs and HMI devices
- Secure connection via HTTPS (Windows 8.1 and higher)
- Support for all local interfaces of workstations
- Quick access to different versions of the TIA Portal
- More efficient utilization of available licenses
- Easy remote maintenance of machines

You have the option of creating a template from a pre-configured VM. You can derive new VMs from this template. This can save you work in installation and configuration.

Providing the TIA Portal Cloud Connector

The TIA Portal Cloud Connector software is supplied with the following SIMATIC software packages as of TIA Portal V14.0:

- STEP 7 Basic
- STEP 7 Professional
- WinCC Basic
- WinCC Professional
- WinCC Comfort/Advanced

You need to purchase a separate license to use the TIA Portal Cloud Connector on the PG/PC.

Note

TIA Portal Cloud Connector

The TIA Portal Cloud Connector is only intended for engineering tasks with the TIA Portal.

You can find additional information at Siemens Industry Online Support under <https://support.industry.siemens.com/cs/document/109739390/> (<https://support.industry.siemens.com/cs/ww/en/view/109739390>).

Configuring the TIA Portal Cloud Connector

Before establishing a connection using the TIA Portal Cloud Connector, you must configure the TIA Portal Cloud Connector. The configuration depends on the communication role of your device. The TIA Portal Cloud Connector has two communication roles:

- "User device" communication role:
The user device is your PG/PC to which the hardware is connected. TIA Portal does not need to be installed on this device. This communication role is preset automatically when you install the TIA Portal Cloud Connector separately, in other words, not together with the TIA Portal.
See also: [Configuring the TIA Portal Cloud Connector on the PG/PC \(Page 38\)](#)
- "Remote device" communication role:
The remote device is the VM on which the TIA Portal is installed. This communication role is preset automatically when you install the TIA Portal Cloud Connector together with the TIA Portal.
See also: [Configuring the TIA Portal Cloud Connector in the VM \(Page 40\)](#)

See also

[User interface of the TIA Portal Cloud Connector \(Page 7\)](#)
[Application cases of the TIA Portal Cloud Connector \(Page 17\)](#)
[Special considerations when working in a virtual machine \(Page 19\)](#)
[Using certificates \(Page 20\)](#)
[System requirements \(Page 23\)](#)
[Providing a virtual machine \(VM\) \(Page 29\)](#)
[Using the virtual machine \(VM\) \(Page 37\)](#)

1.3 User interface of the TIA Portal Cloud Connector

The user interface of the TIA Portal Cloud Connector consists of the following elements:

- Entry in the information area of the Windows taskbar
- TIA Portal Cloud Connector - Settings
- TIA Portal Cloud Connector - Status display
- TIA Portal Cloud Connector - Info window
- TIA Portal - Display in the status bar

TIA Portal Cloud Connector in the information area of the Windows taskbar

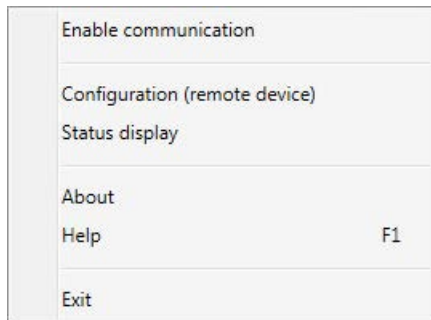
After starting the TIA Portal Cloud Connector, you will find an icon for the Cloud Connector in the information area of Windows taskbar. When you right-click on the icon, the menu of the TIA Portal Cloud Connector opens.

The following figure shows the icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar when the communication endpoints are disabled:



The icon varies in color depending on the status of the communication endpoints.

The following figure shows the menu in the information area with the configured communication role "Remote device":

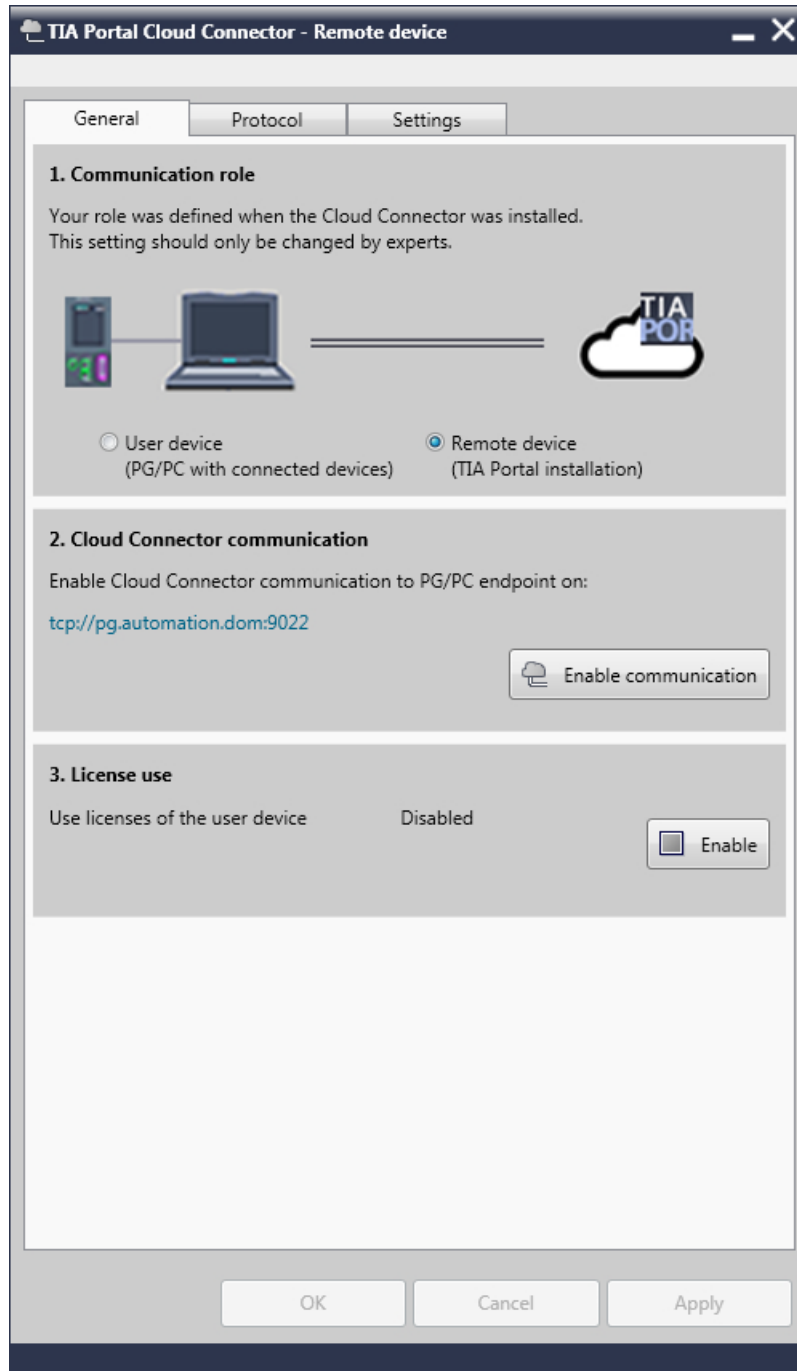


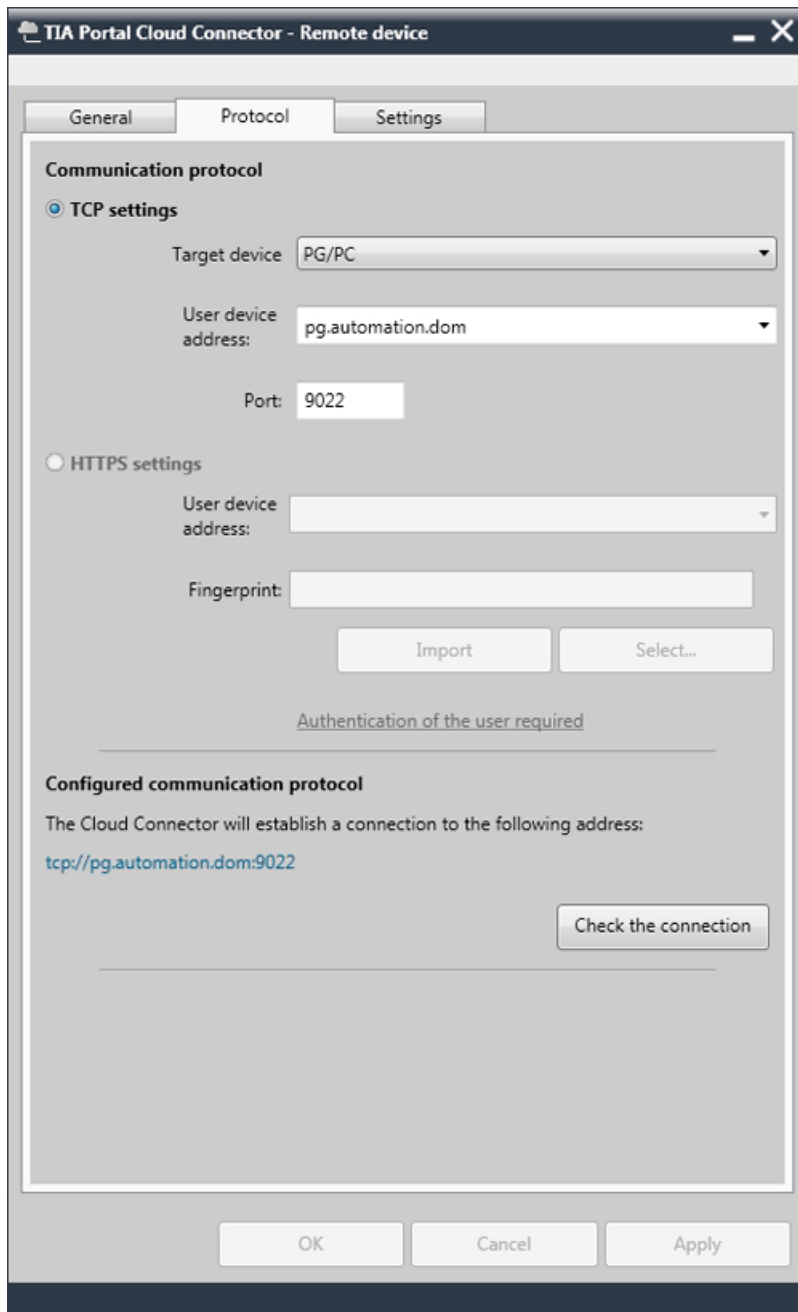
The menu gives you access to the following actions:

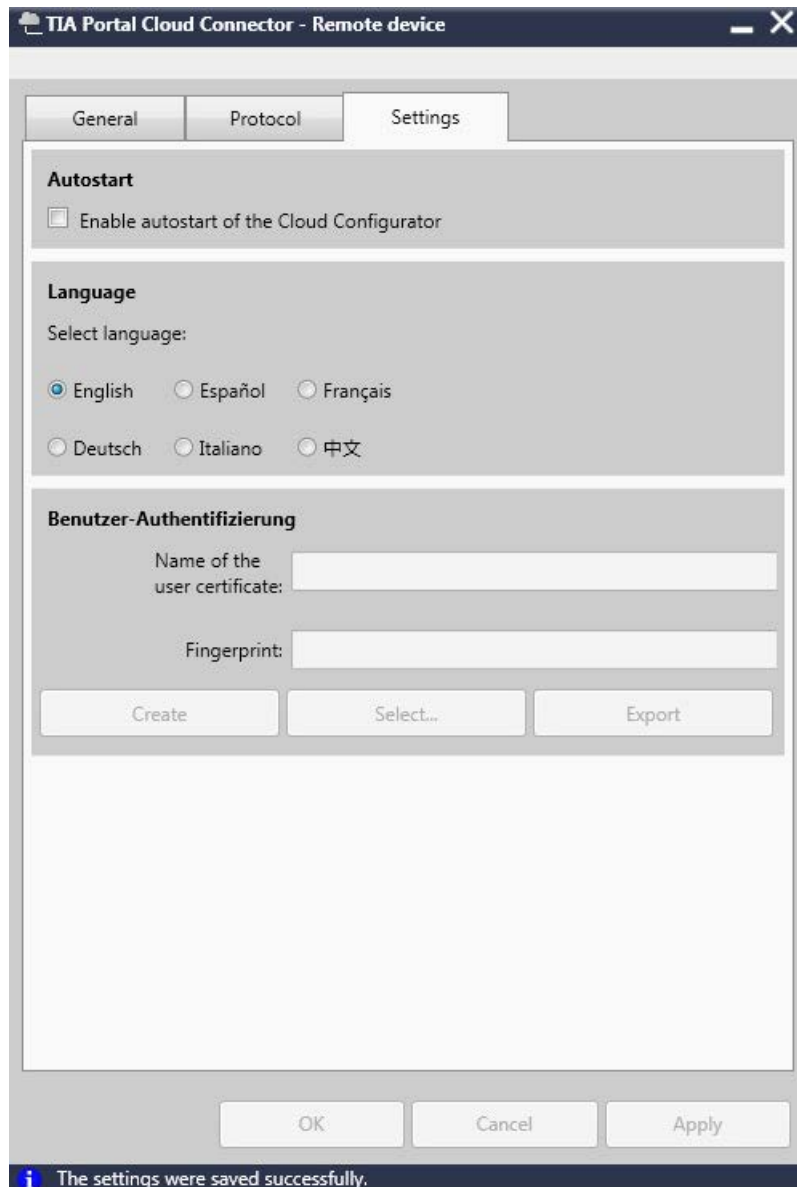
- Enable communication: Use this command to enable communication on both the remote and the user device.
- Configuration (remote device/user device): Opens the TIA Portal Cloud Configurator in the respective communication role.
- Status display: Opens the status display in which you are informed of all operations.
- About: Opens the About window of the TIA Portal Cloud Connector. You can find the version number here, for example.
- Help: Open the online help of the TIA Portal Cloud Connector.
- Exit: Closes the TIA Portal Cloud Connector.

TIA Portal Cloud Connector - Settings

The user interface of the TIA Portal Cloud Connector differs depending on the selected communication role. The figures below show the various setting tabs of the TIA Portal Cloud Connector in the communication role "Remote device":







You can make all settings that are required for a connection in the different tabs.

1.3 User interface of the TIA Portal Cloud Connector

The table below provides an overview of the possible settings and the existing buttons for the communication role "Remote device":

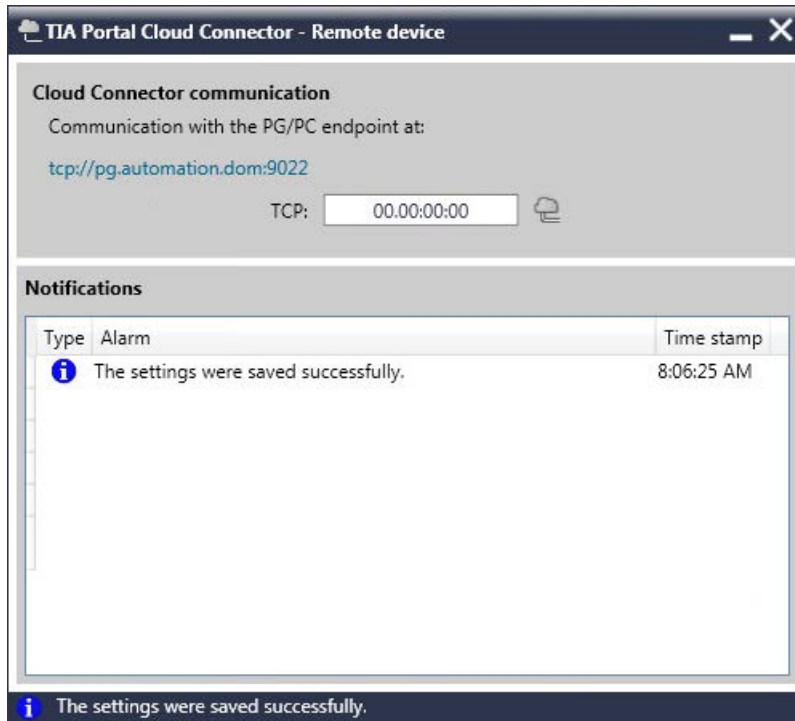
Tab	Area	Setting/button	Description
General	Communication role	User device	PG/PC that establishes the physical contact to the SIMATIC hardware.
		Remote device	Virtual machine (VM) on which the TIA Portal is installed. The user device can be accessed via Remote Desktop connection.
	Cloud Connector communication	Enable communication Disable communication	Enables or disables communication to a PG/PC endpoint.
	License accesses	Enable Disable	Enables or disables the use of a license on the user device.
Protocol	Communication protocol		Defines the transport mechanism between the communication endpoints. You have a choice of TCP or HTTPS (Windows 8.1 and higher).
	TCP settings	Target device	Type of connection partner
		User device address	IP address or name of user device
		Port	Port number through which the transport is to take place
	HTTPS settings	User device address	IP address or name of user device
		Fingerprint	Ensures the integrity of the certificate.
		Import	Imports an existing certificate into the Windows certificate store. You can use an imported certificate for the encryption of data that is sent over HTTPS.
		Select	Selection of a previously imported certificate for data encryption.
	Configured communication protocol	Check the connection	Checks whether the connection can be established without problems.
Settings	Autostart	Enable automatic start of the Cloud Connector	Enables or disables automatic start of the TIA Portal Cloud Connector during system start.
	Language	Select language	Specifies the user interface language for the TIA Portal Cloud Connector.
	User authentication	Name of the user certificate	Shows the currently used user certificate.
		Fingerprint	Checksum of the certificate to ensure integrity
		Create	Creates a new certificate for user authentication.
		Select	Gives you the option to select an existing certificate from the Windows certificate store.
		Export	Exports the currently used certificate.

The table below provides an overview of the possible settings and the existing buttons for the communication role "User device":

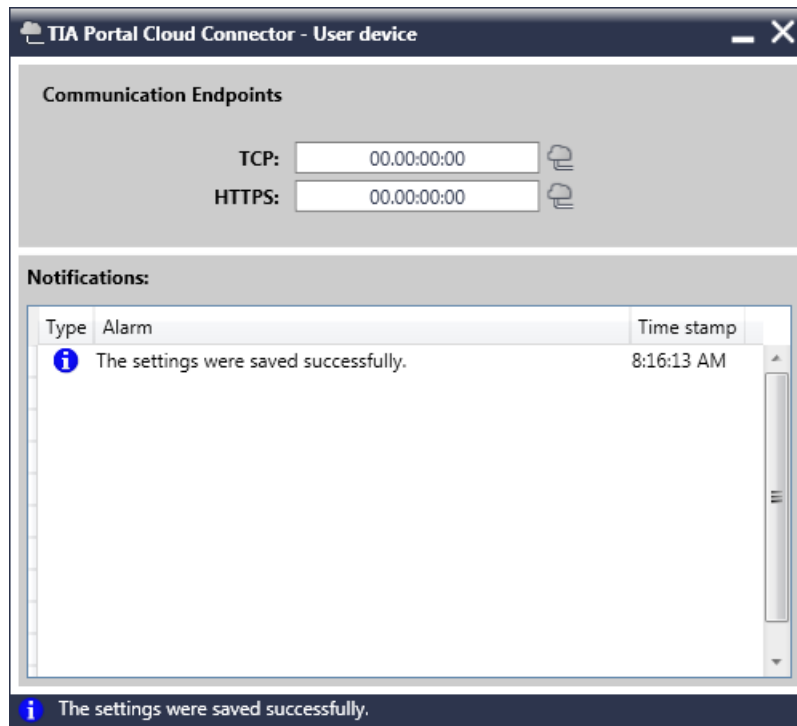
Tab	Area	Setting/button	Description
General	Communication role	User device	PG/PC that establishes the physical contact to the SIMATIC hardware.
		Remote device	Virtual machine in the private cloud server on which the TIA Portal is installed which is operated from a user device via a Remote Desktop connection.
	Cloud Connector communication	Enable communication Disable communication	Enables or disables communication to a PG/PC endpoint.
	License accesses	Enable Disable	Enables or disables the use of a license on the user device.
Protocol	TCP endpoint	Port	Port number through which communication is to take place. The port number of the user device must match the port number of the remote device.
	HTTPS endpoint	User device address	IP address or name of user device
		Fingerprint	Ensures the integrity of the certificate.
		Create	Creates a new certificate for data encryption.
		Export	Exports the currently used certificate.
Select	Gives you the option of selecting an existing certificate.		
Settings	Autostart	Enable automatic start of the Cloud Connector	Enables or disables automatic start of the TIA Portal Cloud Connector during system start.
	Language	Select language	Specifies the user interface language for the TIA Portal Cloud Connector.
	User authentication	Trusted user certificates	Shows the list of all available and trusted user certificates.
		Import	Gives you the option of importing a user certificate that was created on the remote device into the Windows certificate store.
		Add	Gives you the option of adding a certificate from the Windows certificate store to the list of trusted certificates.
		Remove	Removes the selected certificate from the list of trusted certificates. However, it is still retained in the Windows certificate store.

TIA Portal Cloud Connector - Status display

The status display provides information, warnings and error messages while using the TIA Portal Cloud Connector. The following figure shows the status display in the "Remote device" communication role:

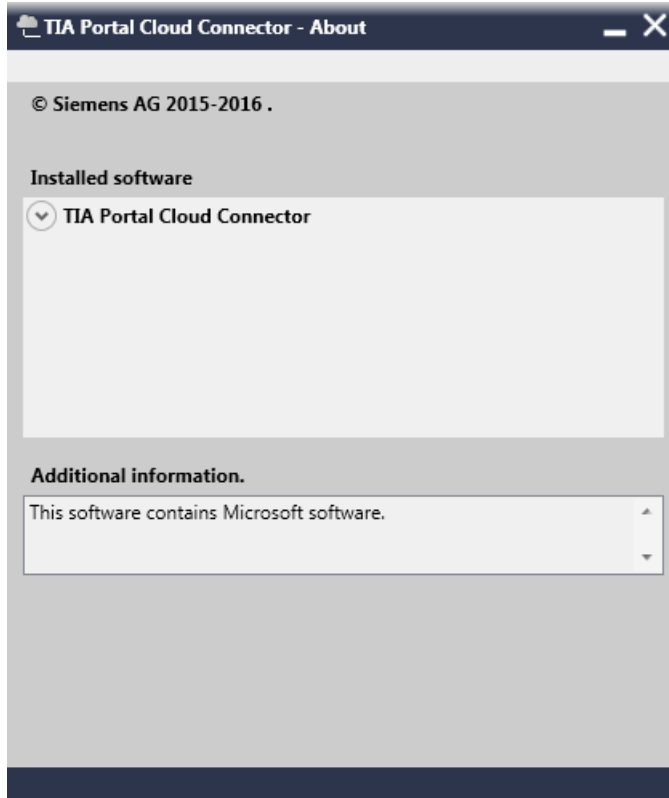


The following figure shows the status display in the "User device" communication role:



TIA Portal Cloud Connector - Info window

The Info window includes information on the installed version of the TIA Portal Cloud Connector.



TIA Portal - Display in the status bar

In the TIA Portal you are informed in the status bar about an existing online connection to the SIMATIC hardware through the TIA Portal Cloud Connector. In addition to the online displays, the following icon is displayed in the status bar for a connection through the TIA Portal Cloud Connector:



See also

- Basics of working with the TIA Portal Cloud Connector (Page 5)
- Application cases of the TIA Portal Cloud Connector (Page 17)
- Special considerations when working in a virtual machine (Page 19)
- Using certificates (Page 20)
- System requirements (Page 23)

Providing a virtual machine (VM) (Page 29)

Using the virtual machine (VM) (Page 37)

1.4 Application cases of the TIA Portal Cloud Connector

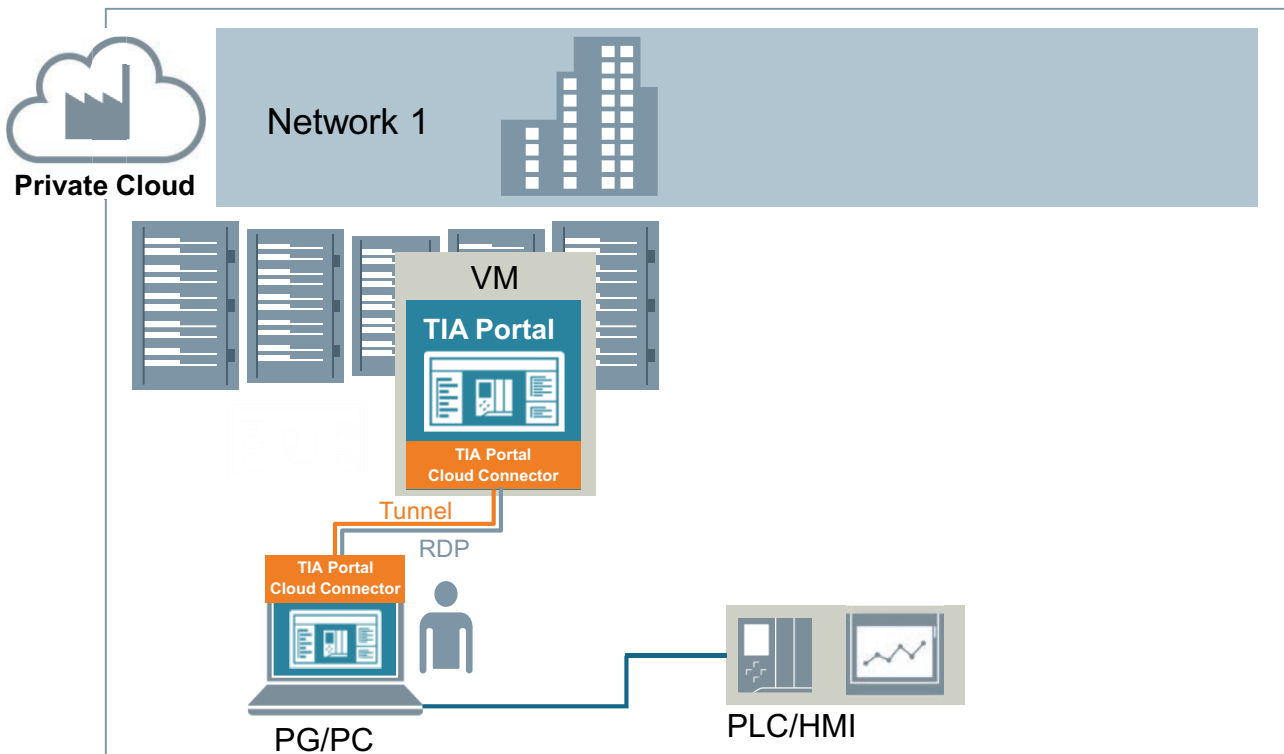
The TIA Portal Cloud Connector enables you to cover the following applications:

- Access to hardware connected to its own PG/PC
- Access to hardware that is connected to another PG/PC. The PG/PC can be located in or outside your own network.

Access to the hardware connected to its own PG/PC

The TIA Portal is installed in the company's private cloud. There is no installation of the TIA Portal on the user's PG/PC, however. The automation hardware (PLCs/HMIs) is connected to the user's PG/PC. The TIA Portal Cloud Connector is installed in both the VM and on your PG/PC. A license for the TIA Portal Cloud Connector is required on the PG/PC. You log on to the VM using Remote Desktop Connection and can work with the TIA Portal as usual. Using the TIA Portal Cloud Connector, you can access the hardware that is connected locally to the PG/PC.

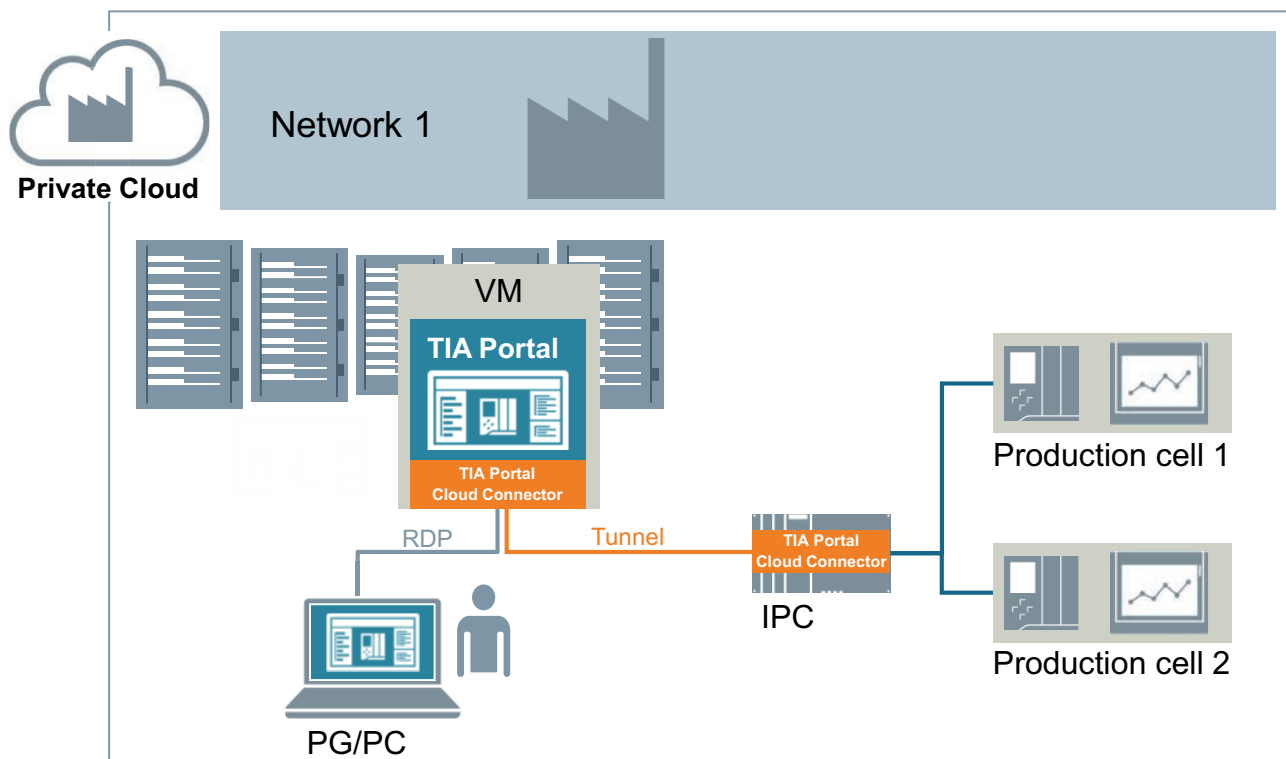
The figure below shows the use of the TIA Portal Cloud Connector in a virtual environment when the hardware is connected to its own PG/PC:

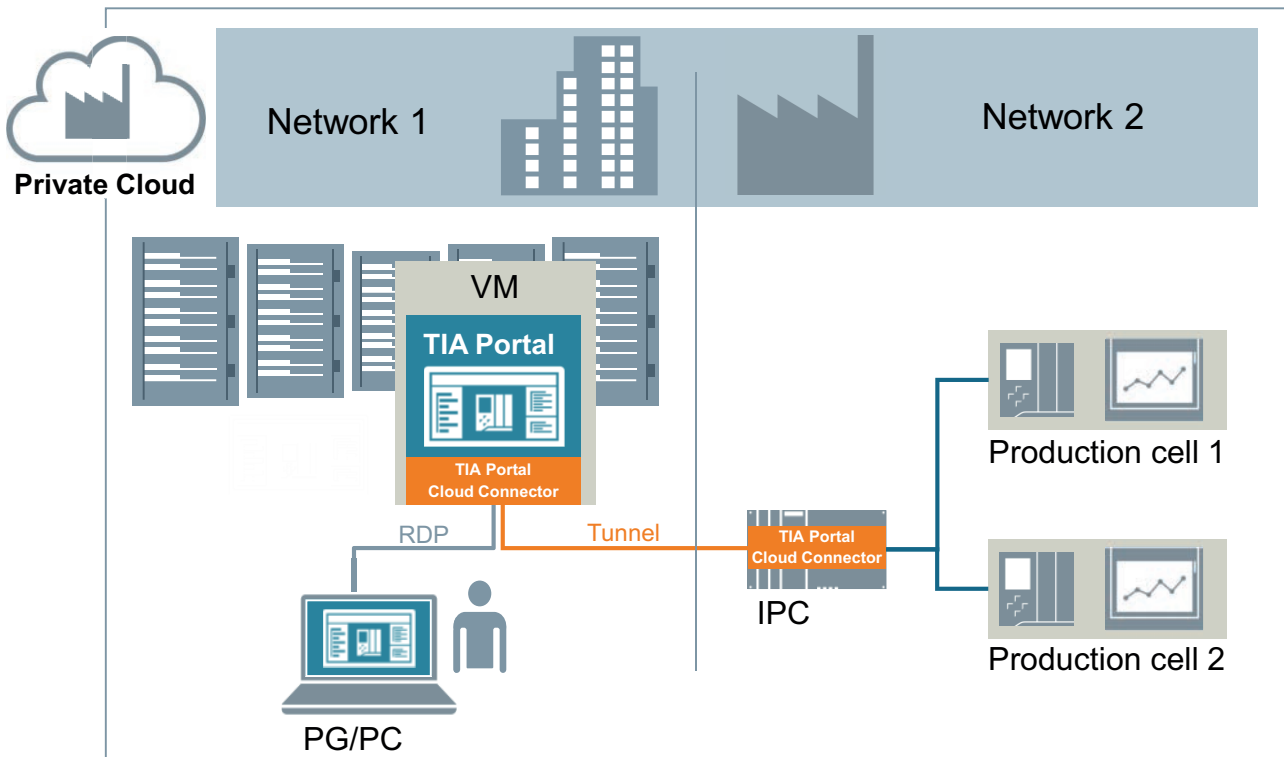


Access to hardware that is connected to another PG/PC

The TIA Portal is installed in a virtual machine. There is no installation of the TIA Portal on your PG/PC, however. The automation hardware is connected to a PG/PC, for example an IPC, which is in the same (figure above) or in a different network (figure below) to your own PG/PC. The TIA Portal Cloud Connector is installed on the other PG/PC and in the VM. First you log on to the VM using Remote Desktop Connection and can work with the TIA Portal as usual. You establish a connection between the VM and the other PG/PC with the TIA Portal Cloud Connector and can access the automation hardware.

The figure below shows the use of the TIA Portal Cloud Connector in a virtual environment when the hardware is connected to another PG/PC, an IPC in the example:





See also

- Basics of working with the TIA Portal Cloud Connector (Page 5)
- User interface of the TIA Portal Cloud Connector (Page 7)
- Special considerations when working in a virtual machine (Page 19)
- Using certificates (Page 20)
- System requirements (Page 23)
- Providing a virtual machine (VM) (Page 29)
- Using the virtual machine (VM) (Page 37)

1.5 Special considerations when working in a virtual machine

Simulation

In order to simulate a PLC program, you must first disable the TIA Portal Cloud Connector. However, this is not necessary for the simulation of HMI devices.

Handling updates and support packages

Updates and support packages can already be installed in the VM template or afterward in the individual VMs. To do this use the update mechanisms of the TIA Portal.

For more information see the TIA Portal information system.

Comparison between the configured and actual topology

Topology comparison is not supported by the TIA Portal Cloud Connector.

See also

Basics of working with the TIA Portal Cloud Connector (Page 5)

User interface of the TIA Portal Cloud Connector (Page 7)

Application cases of the TIA Portal Cloud Connector (Page 17)

Using certificates (Page 20)

System requirements (Page 23)

Providing a virtual machine (VM) (Page 29)

Using the virtual machine (VM) (Page 37)

1.6 Using certificates

Using certificates in the TIA Portal Cloud Connector

As of Windows 8.1 you can use HTTPS connections for communication. The TIA Portal Cloud Connector uses certificates to ensure the security of HTTPS connections. The following certificates are required to establish a connection between user device and remote device:

- Certificate for data encryption
- Certificate for user authentication

A connection cannot be established if a certificate is not available or if the certificates of the user device and the remote device do not match.

Certificate for data encryption

You generate the certificate for data encryption on the user device. Next the certificate must be copied to a local drive of the remote device and imported into the TIA Portal Cloud Connector. If the certificates match, a connection can be established between the devices as soon as the certificates for user authentication have been exchanged as well.

Certificate for user authentication

You generate the certificate for data encryption on the remote device. Next the certificate must be copied to the user device and imported into the TIA Portal Cloud Connector. If the certificates match, a connection can be established between the devices when the certificates for data encryption have been exchanged as well.

See also

- Basics of working with the TIA Portal Cloud Connector (Page 5)
- User interface of the TIA Portal Cloud Connector (Page 7)
- Application cases of the TIA Portal Cloud Connector (Page 17)
- Special considerations when working in a virtual machine (Page 19)
- Creating certificate for data encryption (Page 42)
- Exporting certificate for data encryption (Page 43)
- Importing certificate for data encryption (Page 44)
- Selecting certificate for data encryption (Page 45)
- Creating certificate for user authentication (Page 46)
- Exporting certificate for user authentication (Page 47)
- Importing certificate for user authentication (Page 48)
- Adding certificate for user authentication (Page 49)
- Selecting certificate for user authentication (Page 50)
- Removing certificate for user authentication (Page 51)

System requirements

2.1 System requirements PG/PC

Supported operating systems

In order to use the TIA Portal Cloud Connector, one of the following operating systems must be installed on your PG/PC:

- Windows Server 2012 R2 StdE (full installation)
- Windows Server 2016 Standard (full installation)
- Windows 7 Home Premium SP1
- Windows 7 Professional SP1
- Windows 7 Enterprise SP1
- Windows 7 Ultimate SP1
- Windows 10 Home Version 1703
- Windows 10 Pro Version 1703
- Windows 10 Enterprise Version 1703
- Windows 10 Enterprise 2016 LTSC
- Windows 10 IoT Enterprise 2015 LTSC
- Windows 10 IoT Enterprise 2016 LTSC

Note

Please note the following:

- The TIA Portal Cloud Connector cannot be used in 32-bit operating systems.
 - Make sure that the operating system is always up to date. To do this, perform all critical Windows updates in a timely manner.
 - If SIMATIC NET is installed in a version smaller than 15.01, the TIA Portal Cloud Connector cannot be activated.
 - Name resolution in the network only functions correctly if in the Windows Control Panel > Network and Sharing Center > Advanced sharing settings, you select either the option "Turn on network discovery" or the option "Turn on file and printer sharing". Alternatively, you can also use an external name server.
-

Licenses for the TIA Portal Cloud Connector

To work with the TIA Portal Cloud Connector, you need a valid License Key on every device that you specify as a "User device" in the TIA Portal Cloud Connector. No License Key is required for devices that are used as "remote devices".

2.2 System requirements for VM

You can either include the License Key in the installation or transfer it using the Automation License Manager after the installation.

See also

System requirements for VM (Page 24)

Licenses (Page 26)

2.2 System requirements for VM

Supported guest operating systems and virtualization platforms

You have the option of using the TIA Portal within a virtual machine (VM). For this purpose, use one of the following virtualization platforms in the specified version or a newer version:

- VMware vSphere Hypervisor (ESXi) V6.5
- Microsoft Hyper-V Server 2016
- Microsoft Windows Azure Pack V1.0
- VMware Workstation 12.5.5
- VMware Player 12.5.5

You can install one or more of the following software packages in the VM:

- SIMATIC STEP 7 Basic
- SIMATIC STEP 7 Professional
- SIMATIC WinCC Basic
- SIMATIC WinCC Comfort/Advanced
- SIMATIC WinCC Professional

In addition to these software packages you can also install additional STEP 7 and WinCC option packages.

Note

Operation of the TIA Portal Cloud Connector with an existing installation of SIMATIC NET

The TIA Portal Cloud Connector cannot be enabled when SIMATIC NET is installed in the VM.

Depending on the selected software package, various guest operating systems are supported within the VM:

Guest operating system	SIMATIC STEP 7 Basic	SIMATIC STEP 7 Professional	SIMATIC WinCC Basic	SIMATIC WinCC Professional	SIMATIC WinCC Advanced
Windows Server 2012 R2 StdE (full installation) (64-bit)	X	X	X	X	X
Windows Server 2016 Standard (full installation) (64-bit)	X	X	X	X	X
Windows 7 Home Premium SP1 (64-bit)	X	-	X	-	-
Windows 7 Professional SP1 (64-bit)	X	X	X	X	X
Windows 7 Enterprise SP1 (64-bit)	X	X	X	X	X
Windows 7 Ultimate SP1 (64-bit)	X	X	X	X	X
Windows 10 Home Version 1703 (64-bit)	X	-	-	X	-
Windows 10 Pro Version 1703 (64-bit)	X	X	X	X	X
Windows 10 Enterprise Version 1703 (64-bit)	X	X	X	X	X
Windows 10 Enterprise 2016 LTSB (64-bit)	X	X	X	X	X
Windows 10 IoT Enterprise 2015 LTSB (64-bit)	X	X	X	X	X
Windows 10 IoT Enterprise 2016 LTSB (64-bit)	X	X	X	X	X
- Operating system is not supported.					
X operating system is supported					

Note

Please note the following:

- 32-bit operating systems are not supported.
 - The same hardware requirements apply to the guest operating systems as to the respective TIA products.
 - The SIMATIC USB prommer is not supported.
 - If you want to use SD cards in the VM, you first need to integrate them in the VM as a removable medium. Refer to the help for your virtualization platform for the exact procedure.
 - Make sure that the operating system is always up to date. To do this, perform all critical Windows updates in a timely manner.
-

Installation of the TIA Portal Cloud Connector

There are two ways to install the TIA Portal Cloud Connector:

- You can activate the TIA Portal Cloud Connector as an option during the installation of the SIMATIC software packages mentioned above. It is then installed together with the software package.
- You can install the TIA Portal Cloud Connector independent of a SIMATIC software package. The installation file is located in the "Support" folder on the installation medium. You have the option of making this installation file available in your network. This allows you, as an administrator of the VM, to also create scripts that enable automatic updating of the TIA Portal Cloud Connector. Note, however, that a valid license for the TIA Portal Cloud Connector is required on every PG/PC.

Licenses for the TIA Portal Cloud Connector

To work with the TIA Portal Cloud Connector in the VM, you do not need a license from the TIA Portal Cloud Connector when you configure "Remote device" as the communication role.

See also

System requirements PG/PC (Page 23)

Licenses (Page 26)

2.3 Licenses

Licensing the SIMATIC software packages

You need a separate license for each installation to use the various SIMATIC software packages of the TIA Portal (STEP 7, WinCC) within a virtual environment. If a VM template is copied or cloned, this is also considered a separate installation. On the PG/PC used to access a VM, however, no license for the TIA Portal is required as long as there is no local installation.

When floating license keys are used, the licenses can be provided by a license key server.

Licensing the TIA Portal Cloud Connector

To work with the TIA Portal Cloud Connector, you need a valid License Key on every device that you specify as a "User device" in the TIA Portal Cloud Connector. No License Key is required for devices that are used as "remote devices".

You can either include the License Key in the installation or transfer it using the Automation License Manager after the installation.

Access to the user device licenses by the remote device

The TIA Portal Cloud Connector enables the TIA Portal of the remote device to access the licenses of the user device. To do this, the TIA Portal Cloud Connector forwards the license requests of the remote device to the user device through the tunnel. Once the license access has been enabled by the TIA Portal Cloud Connector, all further license requests from other remote computers are rejected by the ALM. Applications that have already been licensed continue to be licensed, however. The local licenses can be assigned by applications, both on the remote devices as well as on the user devices.

See also: Allocating a license of the user device (Page 27)

See also

System requirements PG/PC (Page 23)





System requirements for VM (Page 24)

Using a license key server (Page 32)

2.4 Allocating a license of the user device

The TIA Portal installed on the remote device can access existing licenses of the user device. For this, the use of external licenses must be enabled both on the user device and on the remote device. The procedure for activating the use of external licenses is identical for the user device and the remote device. You can recognize whether the use of external licenses is enabled or whether external licenses are used by the color of the symbol on the "Enable" or "Disable" button.

The following table provides an overview of the symbols and their meanings:

Icon	Meaning
	The license allocation is disabled.
	The license allocation is enabled, but no licenses are currently being used by the remote device on the user device.
	The license allocation is enabled and the remote device uses the licenses of the user device.
	The data exchange between the TIA Portal and the SIMATIC automation hardware was interrupted. The status display is shown to provide you with more details about the cause.

You can disable the license allocation at any time.

Activating the use of external licenses

To enable license access to the user device, follow these steps:

1. On the user device, right-click on the icon for the TIA Portal Cloud Connector in the information area of the taskbar and select the "Configuration" command.
The TIA Portal Cloud Connector opens.
2. Open the "General" tab.
3. Click "Enable" in the "License accesses" area.
4. Set up a Remote Desktop connection to the VM that contains your remote device.
5. On the remote device, right-click on the icon for the TIA Portal Cloud Connector in the information area of the taskbar and select the "Configuration" command.
The TIA Portal Cloud Connector opens.
6. Click "Enable" in the "License accesses" area.
The TIA Portal of the remote device is now ready to use the licenses of the user device. The text on the "Enable" button changes to "Disable" and the color of the symbol changes to yellow.

Deactivating the use of external licenses

To disable license access to the user device, follow these steps:

1. On the user device, right-click on the icon for the TIA Portal Cloud Connector in the information area of the taskbar and select the "Configuration" command.
The TIA Portal Cloud Connector opens.
2. Open the "General" tab.
3. Click "Disable" in the "License accesses" area.
4. Set up a Remote Desktop connection to the VM that contains your remote device.
5. On the remote device, right-click on the icon for the TIA Portal Cloud Connector in the information area of the taskbar and select the "Configuration" command.
The TIA Portal Cloud Connector opens.
6. Click "Disable" in the "License accesses" area.
The use of the user device licenses by the TIA Portal of the remote device is disabled. The text of the "Disable" button changes to "Enable" and the color of the symbol changes to gray.

See also

Licenses (Page 26)

Using a license key server (Page 32)

Providing a virtual machine (VM)

3.1 Creating a new VM template

You have the option of using the following virtualization platforms:

- VMware vSphere Hypervisor (ESXi) V6.0
- Microsoft Windows Server 2012 R2 Hyper-V
- Microsoft Windows Azure Pack V1.0

Depending on the virtualization platform used, there are differences when creating a template based on an existing virtual machine (VM). You can find additional information in the respective help for the virtualization platform used.

Set up your SIMATIC development environment in the VM as you would on any PG/PC.

Basic steps for creating a new virtual machine template

To create a new virtual machine template, follow these steps:

1. Create a VM.
2. Install the required SIMATIC software, e.g. SIMATIC STEP 7 (TIA Portal V14 and higher) or SIMATIC WinCC (TIA Portal V14 and higher), in the required edition (Basic, Professional, Comfort/Advanced).

Note

The procedure for installing the TIA Portal in a virtual machine (VM) is identical to the procedure for installing it on a PG/PC. You can find detailed information about installation in the installation instructions for the TIA Portal.

3. If necessary, install any required optional packages, e.g. SIMATIC STEP 7 Safety Advanced.
4. If required, install additional compatible software packages that should be available to all users.
5. Configure the VM to meet your requirements.
6. Follow the instructions of your virtualization platform to create a template from the VM.

Result

You have created a VM template, which you can copy and pass along. Note, however, that the required licenses must be available when you use a copy of the template. You can use a separate license server (VM) to manage your licenses.

See also

Saving user and project settings centrally (Page 30)

Using a license key server (Page 32)

Installing the TIA Portal Cloud Connector in the VM (Page 32)

3.2 Saving user and project settings centrally

If VM users save their settings and projects within the VM, these settings and projects are lost when the VM is deleted. For settings and projects to be available also in other VMs, they must be stored outside the VM. You can set environment variables in the VM that store the locations for user-specific settings and projects. Set the environment variables before you start the TIA Portal for the first time. If the environment variables do not exist when the TIA Portal is started for the first time, the TIA Portal stores the settings file in the default directory and always uses this file in the future. As long as this file exists, the TIA Portal ignores any environment variables that were set later.

You can specify the following paths through environment variables:

- User-specific settings: The settings are saved in the specified directory.
- Projects: The specified location is used as the default location when a new project is created. However, you can save a project in a different directory at any time.

The environment variables can be set either manually or through a script. You can have separate scripts for setting the environment variable for the settings and for the projects, or one script for both environment variables.

The file for the settings has the same name for all users. A separate directory must be specified for each user to enable all users access to their own settings. Otherwise, the settings will be continually overwritten by other users. Using a tag, the path can be adapted for the logged on user.

Example of a directory structure for central storage of settings

The settings are stored in a "User Settings" directory, which is shared on the network. The structure below "UserSettings" appears as follows:

```
UserSettings
    User1
    User2
    User3
```

"User1", "User2" and "User3" are the user names of the VM users here. The path of the environment variable is then "\\MyServer\UserSettings\%USERNAME%".

"MyServer" is an available computer in the network in this example. "%USERNAME%" is the tag for the user name. This tag is resolved when the user logs on and the environment variable is changed accordingly. If this is done for multiple users, it is advisable to save the script in the Autostart folder. This environment variable is reset with every logon, and the storage location for the settings is adapted to the logged on user.

Requirement

- All users have write access to the server areas that are to be used as new locations.
- The user-defined directories exist.

Setting environment variables using a script

To set the environment variables using a script, follow these steps:

1. Create a new script and open it for editing. Alternatively, you can also amend an existing script.

2. Add the following lines to your script:

```
setx TiaUserSettingsPath \\<Server>\<Settings>\%USERNAME%
setx TiaDefaultProjectPath \\<Server>\<Projects>\%USERNAME%
```

Replace "<Server>\<Settings>" and "<Server>\<Projects>" with the directories in the network in which the settings and projects are to be stored.

3. Save the script.

4. In order for the script to be used by different users, copy it into the Autostart folder of Windows.

The "%USERNAME%" tag is resolved on the next logon to the remote device. This adapts the storage location for the settings for the logged-on user.

If you want to use two scripts instead of one script, perform steps 1 through 4 for each script and add only one of the two "setx" commands to each one.

Setting the environment variables manually

To set the environment variables manually, follow these steps:

1. Start the VM that you want to distribute as a template.
2. In Windows, open the dialog for setting the environment variables.
3. Create a new system tag with the name "TiaUserSettingsPath".
4. As a value, enter the path to the directory in the network in which the user settings are to be stored. Be sure to specify the name of the user as a "%USERNAME%" tag.
5. Confirm your entries with "OK".
6. Create another system tag with the name "TiaDefaultProjectPath".
7. As a value, enter the path to the directory in the network to be used as the default storage location for projects. You can specify the name of the user as a "%USERNAME%" tag to save the projects in subdirectories. If you omit "%USERNAME%", all projects are saved in the same directory.
8. Confirm your entries with "OK".
The "%USERNAME%" tag is resolved on the next logon to the PG/PC. This adapts the storage location for the settings for the logged-on user.

3.4 Installing the TIA Portal Cloud Connector in the VM

See also

Creating a new VM template (Page 29)

Using a license key server (Page 32)

Installing the TIA Portal Cloud Connector in the VM (Page 32)

3.3 Using a license key server

Introduction

During the installation of the TIA Portal or the TIA Portal Cloud Connector, the Automation License Manager (ALM) is installed as well. You need this for license transfer and handling.

You can find additional information on the Automation License Manager and setting up a license server in the user documentation for Automation License Manager.

See also

Licenses (Page 26)

Allocating a license of the user device (Page 27)

Creating a new VM template (Page 29)

Saving user and project settings centrally (Page 30)

Installing the TIA Portal Cloud Connector in the VM (Page 32)

3.4 Installing the TIA Portal Cloud Connector in the VM

You can install the TIA Portal Cloud Connector in the VM in two ways:

- Installation of the TIA Portal Cloud Connector together with the TIA Portal
You have the option of installing the TIA Portal Cloud Connector together with the TIA Portal. You activate the "TIA Portal Cloud Connector" option during the installation process.
- Installation of the TIA Portal Cloud Connector without TIA Portal
You can also find a setup program on the installation medium allowing you to install the TIA Portal Cloud Connector without the TIA Portal. You can make this installation file accessible to other users via a network drive.

Installing the Cloud Connector together with the TIA Portal

To install the Cloud Connector together with the TIA Portal, follow these steps:

1. Insert the installation medium in the relevant drive.
The setup program starts automatically unless you have disabled Autostart on the programming device or PC.
2. If the setup program does not start up automatically, start it manually by double-clicking the "Start.exe" file.
The dialog for selecting the setup language opens.
3. Choose the language in which you want the setup program dialogs to be displayed.
4. To read the information on the product and installation, click the "Read Notes" or "Installation Notes" button.
The help file containing the notes opens.
5. Once you have read the instructions, close the help file and click the "Next" button.
The dialog for selecting the product languages opens.
6. Select the languages for the product user interface and click "Next".

Note

"English" is always installed as the basic product language.

The dialog for selecting the product configuration opens.

7. Click "User-defined".
8. Then select the "TIA Portal Cloud Connector" check box and, if required, the check boxes for other products that you want to install.
9. If you want to create a shortcut for the TIA Portal on the desktop, select the "Create desktop shortcut" check box.
10. Click the "Browse" button if you want to change the target directory for the installation. Note that the length of the installation path must not exceed 89 characters.
11. Click the "Next" button.
The dialog for the license terms opens.
12. To continue the installation, read and accept all license agreements and click "Next".
If changes to the security and permission settings are required in order to install the TIA Portal, the security settings dialog opens.
13. To continue the installation, accept the changes to the security and permissions settings, and click "Next".
The next dialog displays an overview of the installation settings.
14. Check the selected installation settings. If you want to make any changes, click "Back" until you reach the point in the dialog where you want to make changes. Once you have completed the desired changes, return to the overview by clicking "Next".

3.4 Installing the TIA Portal Cloud Connector in the VM

15. Click "Install".
Installation is started.

Note

If no license key is found during installation, you have the option of transferring it to your PC. If you skip the license transfer, you can carry it out later with the Automation License Manager.

Following installation, you receive a message indicating whether the installation was successful.

16. You may be required to restart the computer. In this case, select the "Yes, restart my computer now." option button. Then click "Restart".
17. If the computer does not reboot, click "Exit".

Installing the Cloud Connector without TIA Portal

To install the Cloud Connector without the TIA Portal, follow these steps:

1. Insert the installation medium in the appropriate drive or navigate to the installation file in the file system of your computer.
You can find the installation file in the "Support" directory on the installation medium.
2. Double-click on the installation file "TIA Portal Cloud Connector_<Version>.exe".
The Windows user account control is displayed.
3. Confirm the user account control with "Yes".
The installation dialog opens.
4. Click "Next".
A selection of the available setup languages is displayed.
5. Select the desired setup language and click "Next".
The required files are unzipped and the next installation dialog opens.
6. Close any programs still running and click "Next".
The license conditions are displayed.
7. Accept the license conditions and click "Next".
The available programs and the memory requirements for installation are displayed.
8. Click "Next".
A dialog box opens showing an overview of the system settings that can be changed during installation.
9. Select the check box to apply the changes.
10. Click "Next".
An overview of the programs to be installed is displayed.
11. Click "Install".
Installation is started.
12. You may be required to restart the computer. In this case, select the "Yes, restart my computer now." option button. Then click "Finish".

See also

Creating a new VM template (Page 29)

Saving user and project settings centrally (Page 30)

Using a license key server (Page 32)

Using the virtual machine (VM)

4.1 Installing the TIA Portal Cloud Connector on the PG/PC

Note

Please note the following:

- You need a valid license for the TIA Portal Cloud Connector.
 - Settings in the Windows firewall: A prerequisite for an incoming connection is that the port used in the TIA Portal Cloud Connector is entered in your firewall in the "Exceptions" tab for the service "Siemens SCP Remote Connection". The default is "Any".
-

Procedure

To install the TIA Portal Cloud Connector, follow these steps:

1. Insert the installation medium in the appropriate drive or navigate to the installation file in the file system of your computer.
You can find the installation file in the "Support" directory on the installation medium.
2. Double-click on the installation file "TIA Portal Cloud Connector_<Version>.exe".
The Windows user account control is displayed.
3. Confirm the user account control with "Yes".
The installation dialog opens.
4. Click "Next".
A selection of the available setup languages is displayed.
5. Select the desired setup language and click "Next".
The required files are unzipped and the next installation dialog opens.
6. Close any programs still running and click "Next".
The license conditions are displayed.
7. Accept the license conditions and click "Next".
The available programs and the memory requirements for installation are displayed.
8. Click "Next".
A dialog box opens showing an overview of the system settings that can be changed during installation.
9. Select the check box to apply the changes.
10. Click "Next".
An overview of the programs to be installed is displayed.
11. Click "Install".
Installation is started.
12. You may be required to restart the computer. In this case, select the "Yes, restart my computer now." option button. Then click "Finish".

See also

Configuring the TIA Portal Cloud Connector on the PG/PC (Page 38)

Configuring the TIA Portal Cloud Connector in the VM (Page 40)

Online connection via the TIA Portal Cloud Connector (Page 51)

Using the virtual machine (VM) offline (Page 52)

4.2 Configuring the TIA Portal Cloud Connector on the PG/PC

Note

Communication protocol

In order for your PG/PC to connect to the VM, you need to specify a communication protocol. For security reasons, you should always use HTTPS as of Windows 8.1.

Configuring the TCP connection

To configure a TCP connection for the PG/PC, follow these steps:

1. Right-click on the icon for the TIA Portal Cloud Connector in the information area of the taskbar and select the "Configuration" command.
The TIA Portal Cloud Connector opens.
2. Open the "Settings" tab and change the user interface language of the TIA Portal Cloud Connector, if required.
3. Go to the "General" tab and check the communication role. If required, change the setting to "User device".
4. Switch to the "Protocol" tab.
5. Select the "TCP endpoint" check box.
6. Enter the port through which communication is to be performed. The port must be identical to the one specified on the remote device.
7. Open the "General" tab again.
8. Click "Enable communication" in the "Cloud Connector Communication" area.

Configuring the HTTPS connection

To configure an HTTPS connection for the PG/PC, follow these steps:

1. Right-click on the icon for the TIA Portal Cloud Connector in the information area of the taskbar and select the "Configuration" command.
The TIA Portal Cloud Connector opens.
2. Open the "Settings" tab and change the user interface language of the TIA Portal Cloud Connector, if required.
3. Go to the "General" tab and check the communication role. If required, change the setting to "User device".
4. Switch to the "Protocol" tab.
5. Select the "HTTPS endpoint" check box.
6. You either create a new certificate for data encryption or you select an existing certificate from the Windows certificate store.
See also:
Creating certificate for data encryption (Page 42)
Selecting certificate for data encryption (Page 45)
7. If you do not have a certificate for user authentication on the user device, create it on the remote device and copy it to a local drive of the user device.
See also:
Creating certificate for user authentication (Page 46)
8. Switch to the "Settings" tab.
9. Import a new certificate for user authentication or add an existing certificate from the Windows certificate store to the list of trusted certificates.
See also:
Importing certificate for user authentication (Page 48)
Adding certificate for user authentication (Page 49)
10. Open the "General" tab again.
11. Click "Enable communication" in the "Cloud Connector Communication" area.

Result

Your PG/PC is now ready to communicate with the VM. Next, configure the TIA Portal Cloud Connector in the VM.

See also

- Installing the TIA Portal Cloud Connector on the PG/PC (Page 37)
- Configuring the TIA Portal Cloud Connector in the VM (Page 40)
- Online connection via the TIA Portal Cloud Connector (Page 51)
- Using the virtual machine (VM) offline (Page 52)

4.3 Configuring the TIA Portal Cloud Connector in the VM

Note

Communication protocol

You must specify the communication protocol that is going to be used so that a PG/PC can establish a connection to the VM. For security reasons, you should always use HTTPS as of Windows 8.1. You should also check the identity of the requesting connection partner before you accept a connection.

Configuring the TCP connection

To configure a TCP connection for the VM, follow these steps:

1. Set up a Remote Desktop connection to the VM.
2. Right-click on the icon for the TIA Portal Cloud Connector in the information area of the taskbar and select the "Configuration" command.
The TIA Portal Cloud Connector opens.
3. Open the "Settings" tab and change the user interface language of the TIA Portal Cloud Connector, if required.
4. Go to the "General" tab and check the communication role. If required, change the setting to "Remote device".
5. Open the "Protocol" tab.
6. Under "Communications protocol" select the option "TCP settings".
7. Select a target device.

Note

Connection to SCALANCE

Make sure that the connection to SCALANCE is encrypted with SINEMA RC or other encryption technology. Otherwise, the data transfer is not encrypted.

8. Enter the IP address of the user device or select the "Automatic configuration" entry to have the address determined automatically.
9. Enter the port through which communication is to be performed. The port must be identical to the one specified on the user device.
10. Open the "General" tab again.
11. Click "Enable communication" in the "Cloud Connector Communication" area.

Configuring the HTTPS connection

To configure an HTTPS connection for the VM, follow these steps:

1. Set up a Remote Desktop connection to the VM.
2. Right-click on the icon for the TIA Portal Cloud Connector in the information area of the taskbar and select the "Configuration" command.
The TIA Portal Cloud Connector opens.
3. Open the "Settings" tab and change the user interface language of the TIA Portal Cloud Connector, if required.
4. Open the "General" tab and check the communication role. If required, change the setting to "Remote device".
5. Open the "Protocol" tab.
6. Under "Communications protocol" select the option "HTTPS settings".
7. Enter the IP address of the user device or select the "Automatic configuration" entry to have the address determined automatically.
8. You either import the certificate for data encryption you have created on the user device or you select an existing certificate from the Windows certificate store.
See also:
Importing certificate for data encryption (Page 44)
Selecting certificate for data encryption (Page 45)
9. Switch to the "Settings" tab.
10. You either create a new certificate for user authentication or you select an existing certificate from the Windows certificate store.
See also:
Creating certificate for user authentication (Page 46)
Selecting certificate for user authentication (Page 50)
11. Open the "General" tab again.
12. Click "Enable communication" in the "Cloud Connector Communication" area.

Result

The TIA Portal Cloud Connector is ready for communication. After activating both communication partners, you can access the locally connected SIMATIC hardware (PLCs/HMIs) from the user device.

See also

- Installing the TIA Portal Cloud Connector on the PG/PC (Page 37)
- Configuring the TIA Portal Cloud Connector on the PG/PC (Page 38)
- Online connection via the TIA Portal Cloud Connector (Page 51)
- Using the virtual machine (VM) offline (Page 52)

4.4 Using certificates (for HTTPS connections only)

4.4.1 Creating certificate for data encryption

As of Windows 8.1 you can use an HTTPS connection for communication. To increase security, a certificate is required for data encryption; it is created on the user device to be used by the remote device.

Procedure

To create a certificate for data encryption, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar on the user device.
2. Select the "Configuration (user device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS endpoint" check box.
The buttons "Create" and "Select" are activated.
5. Click "Create".
The "TIA Portal Cloud Connector - Create certificate" dialog opens.
6. Enter a domain name or select the domain from the drop-down list.

Note

Use the "+" button to apply the domain to the domain list. Use the "-" button to remove a domain from the domain list.

7. Click "Browse".
The "Save as" dialog opens.
8. Select a storage location and enter a file name for the certificate.
9. Click "Save".
10. Select the date as of which the certificate is to be valid.
11. Select the date as until which the certificate is to be valid.
12. Click "OK".

Result

The certificate is created and used for the HTTPS endpoint on the user device. In addition, it is saved at the specified storage location as file with the file name extension ".cer"; from there it can be copied to the remote device. The certificate is also added to the Windows certificate store.

See also

Using certificates (Page 20)

Exporting certificate for data encryption (Page 43)

Importing certificate for data encryption (Page 44)

Selecting certificate for data encryption (Page 45)

4.4.2 Exporting certificate for data encryption

You can export the currently used certificate for data encryption at any time.

Requirement

The certificate for data encryption has been created and is displayed under the HTTPS endpoint of the user device.

Procedure

To export a certificate for data encryption, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar on the user device.
2. Select the "Configuration (user device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS endpoint" check box.
The buttons "Create" and "Select" and "Export" are activated.
5. Click "Export".
The "Save as" dialog opens.
6. Select a storage location and enter a name for the certificate.
7. Click "Save".

Result

The currently used certificate for data encryption is saved at the specified storage location as file with the file name extension ".cer".

See also

Using certificates (Page 20)

Creating certificate for data encryption (Page 42)

Importing certificate for data encryption (Page 44)

Selecting certificate for data encryption (Page 45)

4.4.3 Importing certificate for data encryption

To establish an HTTPS connection between the user device and the remote device, you must import the certificate for data encryption created on the user device to the TIA Portal Cloud Connector of the remote device.

Requirement

- The certificate for data encryption was created on the user device.
- The certificate for data encryption was copied to a local drive of the remote device.

Procedure

To import a certificate for data encryption to the TIA Portal Cloud Connector of the remote device, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar on the remote device.
2. Select the "Configuration (remote device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS settings" check box.
The buttons "Import" and "Select" are activated.
5. Click on "Import".
The "Open" dialog box opens.
6. Select the certificate file in the file system. You recognize the certificate files by their file name extension ".cer".
7. Click "Open".

Result

The certificate is imported and it is used immediately for communication. The certificate is also added to the Windows certificate store.

See also

Using certificates (Page 20)

Creating certificate for data encryption (Page 42)

Exporting certificate for data encryption (Page 43)

Selecting certificate for data encryption (Page 45)

4.4.4 Selecting certificate for data encryption

You can select a certificate for data encryption from the Windows certificate store. This is possible on the user device as well as the remote device.

Requirement

The certificate for data encryption has been created beforehand (user device) or imported (remote device) and is available in the Windows certificate store.

Procedure

To select and use an existing certificate for data encryption from the Windows certificate store, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar.
2. Select the "Configuration (user device)" or "Configuration (remote device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS endpoint" check box (user device) or the "HTTPS settings" check box (remote device).
The "Select" button becomes active.
5. Click "Select".
The "Windows Security" dialog opens and the available certificates are displayed.
6. Select a certificate. If necessary, you can display additional properties of the certificate.
7. Click "OK".

Result

The selected certificate is used for communication. The same certificate must be set on the user device and the remote device for communication to take place.

See also

Using certificates (Page 20)

Creating certificate for data encryption (Page 42)

Exporting certificate for data encryption (Page 43)

Importing certificate for data encryption (Page 44)

4.4.5 Creating certificate for user authentication

As of Windows 8.1 you can use an HTTPS connection for communication. To increase security, a certificate is required for user authentication; it is created on the remote device to be used by the user device.

Procedure

To create a certificate for user authentication, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar on the remote device.
2. Select the "Configuration (remote device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS settings" check box.
The area for user authentication becomes active in the "Settings" tab.
5. Switch to the "Settings" tab.
6. Click "Create" in the "User authentication" area.
The "TIA Portal Cloud Connector - User authentication" dialog opens.
7. Enter a name for the new certificate in the "Certificate name" field.
8. Click "Browse".
The "Save as" dialog opens.
9. Select a storage location and enter a file name for the certificate.
10. Click "Save".
11. Select the date as of which the certificate is to be valid.
12. Select the date as until which the certificate is to be valid.
13. Click "OK".

Result

The certificate is created and used on the remote device. In addition, it is saved at the specified storage location as file with the file name extension ".cer"; from there it can be copied to the user device. The certificate is also added to the Windows certificate store.

See also

- Using certificates (Page 20)
- Exporting certificate for user authentication (Page 47)
- Importing certificate for user authentication (Page 48)
- Adding certificate for user authentication (Page 49)
- Selecting certificate for user authentication (Page 50)
- Removing certificate for user authentication (Page 51)

4.4.6 Exporting certificate for user authentication

When creating the certificate for user authentication, you must export the certificate to make it available to a user device. You can export the currently used certificate again at any time.

Requirement

The certificate for user authentication has been created on the remote device beforehand and it is displayed in the "Settings" tab under "User authentication".

Procedure

To export a certificate for user authentication, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar on the remote device.
2. Select the "Configuration (remote device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS settings" check box.
The area for user authentication becomes active in the "Settings" tab.
5. Switch to the "Settings" tab.
6. Click "Export" in the "User authentication" area.
The "Save as" dialog opens.
7. Select a storage location and enter a name for the certificate.
8. Click "Save".

Result

The currently used certificate for user authentication is saved at the specified storage location as file with the file name extension ".cer".

See also

Using certificates (Page 20)

Creating certificate for user authentication (Page 46)

Importing certificate for user authentication (Page 48)

Adding certificate for user authentication (Page 49)

Selecting certificate for user authentication (Page 50)

Removing certificate for user authentication (Page 51)

4.4.7 Importing certificate for user authentication

To establish an HTTPS connection between the user device and the remote device, you must import the certificate for user authentication created on the remote device to the TIA Portal Cloud Connector of the user device.

Requirement

- The certificate for user authentication was created on the remote device.
- The certificate for user authentication was copied to a local drive of the remote device.

Procedure

To import a certificate for user authentication, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar on the user device.
2. Select the "Configuration (user device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS endpoint" check box.
The area for user authentication becomes active in the "Settings" tab.
5. Switch to the "Settings" tab.
6. Click "Import" in the "User authentication" area.
The "Open" dialog box opens.
7. Select the certificate file in the file system. You recognize the certificate files by their file name extension ".cer".
8. Click "Open".

Result

The certificate is imported and added to the list of trusted certificates. You can use this list to specify the remote devices with which the user device may communicate. The addressed remote device must have the same certificate for user authentication as the user device.

See also

Using certificates (Page 20)

Creating certificate for user authentication (Page 46)

Exporting certificate for user authentication (Page 47)

Adding certificate for user authentication (Page 49)

Selecting certificate for user authentication (Page 50)

Removing certificate for user authentication (Page 51)

4.4.8 Adding certificate for user authentication

Instead of importing a certificate from the file system, you also add the to the list of trusted certificates from the Windows certificate store.

Requirement

The required certificate is available in the Windows certificate store.

Procedure

To add a certificate for user authentication from the Windows certificate store, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar on the user device.
2. Select the "Configuration (user device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS endpoint" check box.
The area for user authentication becomes active in the "Settings" tab.
5. Switch to the "Settings" tab.
6. Click "Add" in the "User authentication" area.
The "Select certificate" dialog opens and the available certificates are displayed.
7. Select a certificate. If necessary, you can display the certificate.
8. Click "OK".

Result

The certificate from the Windows certificate store is added to the list of trusted certificates. You can use this list to specify the remote devices with which the user device may communicate. The addressed remote device must have the same certificate for user authentication as the user device.

See also

Using certificates (Page 20)

Creating certificate for user authentication (Page 46)

Exporting certificate for user authentication (Page 47)

Importing certificate for user authentication (Page 48)

Selecting certificate for user authentication (Page 50)

Removing certificate for user authentication (Page 51)

4.4.9 Selecting certificate for user authentication

Instead of creating a new certificate on the remote device, you can also select and use an existing certificate from the Windows certificate store.

Requirement

The certificate for user authentication has been created beforehand and is available in the Windows certificate store.

Procedure

To select a certificate for user authentication from the Windows certificate store, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar on the remote device.
2. Select the "Configuration (remote device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS settings" check box.
The area for user authentication becomes active in the "Settings" tab.
5. Switch to the "Settings" tab.
6. Click "Select" in the "User authentication" area.
The "Windows Security" dialog opens and the available certificates are displayed.
7. Select a certificate. If necessary, you can display additional properties of the certificate.
8. Click "OK".

Result

The certificate is used on the remote device for user authentication. If necessary, it can be exported to exchange it with the user device.

See also

Using certificates (Page 20)

Creating certificate for user authentication (Page 46)

Exporting certificate for user authentication (Page 47)

Importing certificate for user authentication (Page 48)

Adding certificate for user authentication (Page 49)

Removing certificate for user authentication (Page 51)

4.4.10 Removing certificate for user authentication

You can remove a certificate for user authentication from the list of trusted certificates on the user device at any time.

Procedure

To remove a certificate for user authentication from the list of trusted certificates, follow these steps:

1. To open the TIA Portal Cloud Connector, right-click on the status icon of the TIA Portal Cloud Connector in the information area of the Windows taskbar on the user device.
2. Select the "Configuration (user device)" command from the shortcut menu.
The configuration window of the TIA Portal Cloud Connector opens.
3. Switch to the "Protocol" tab.
4. Select the "HTTPS endpoint" check box.
The area for user authentication becomes active in the "Settings" tab.
5. Switch to the "Settings" tab.
6. Select the certificate you want to remove in the list of trusted certificates.
7. Click "Remove" in the "User authentication" area.

Result

The certificate is removed from the list of trusted certificates. A connection to the remote device which uses this certificate for user authentication is no longer possible.

See also

Using certificates (Page 20)

Creating certificate for user authentication (Page 46)

Exporting certificate for user authentication (Page 47)

Importing certificate for user authentication (Page 48)

Adding certificate for user authentication (Page 49)

Selecting certificate for user authentication (Page 50)

4.5 Online connection via the TIA Portal Cloud Connector





Introduction

If you use the TIA Portal Cloud Connector for the connection to the hardware, working in the TIA Portal is no different from a normal online connection to the hardware. Once you have enabled tunnel communication, you can therefore compile, load or monitor your data as usual.

For more information about establishing an online connection and working in online mode, refer to the online help for the TIA Portal.

Overview of the status symbols

If you establish an online connection via the TIA Portal Cloud Connector, you can see status symbols in the information area of the Windows taskbar which indicate the status of the connection. The following table shows an overview of the status symbols and their meanings:

Status symbol	Meaning
	Communication is disabled.
	Communication is enabled but there is no data exchange between the TIA Portal and the SIMATIC automation hardware.
	Communication is enabled and data exchange between the TIA Portal and the SIMATIC automation hardware is taking place.
	The data exchange between the TIA Portal and the SIMATIC automation hardware was interrupted. The status display is shown to provide you with more details about the cause.

Status display

In the information area in the Windows taskbar, you can show a status display on both the remote device as well as on the user device. This opens the window "TIA Portal Cloud Connector - Remote device" or "TIA Portal Cloud Connector - User device." This window provides you with all the information, warnings and error messages of the TIA Portal Cloud Connector. In addition, it shows how long a TCP or HTTPS connection has been running.

You can hide the status bar at any time.

See also

Installing the TIA Portal Cloud Connector on the PG/PC (Page 37)

Configuring the TIA Portal Cloud Connector on the PG/PC (Page 38)

Configuring the TIA Portal Cloud Connector in the VM (Page 40)

Using the virtual machine (VM) offline (Page 52)

4.6 Using the virtual machine (VM) offline

You have the option of working offline with a virtual machine. To do this, you can copy the VM from the remote device to your PG/PC. You can then start the VM on your PG/PC and use the TIA Portal with the hardware that is either connected to your PG/PC or in the network.

You have the following options for using the VM:

- The hardware is connected via Ethernet to your PG/PC and is located in the same subnet.
- The hardware is connected via Ethernet or Profibus to your PG/PC and is located in a different subnet.

You do not need the TIA Portal Cloud Connector for every type of connection. The following scenarios may occur:

- If your hardware is connected directly to your PG/PC via an Ethernet or USB adapter, you can set a "Bridged" network connection.
The TIA Portal Cloud Connector must be disabled in the VM with this connection type.
- If your hardware is attached to the network via its own USB or network adapter, you can use the "Host-only" option. In this case, the TIA Portal Cloud Connector must be enabled in the VM so that you can also use the PROFIBUS interface.

After using the VM locally, you can copy it back to the remote device.

Requirement

- The appropriate software for starting the VM, for example, VMware Workstation, is installed on your PG/PC.
- Automation License Manager is installed on the PG/PC.

Transferring the virtual machine (VM) from the remote device to the PG/PC

To work with the virtual machine offline, follow these steps:

1. Copy the VM to your local programming device/PC. The exact procedure depends on the virtualization environment used. Refer to the corresponding documentation if you need help.
2. Open the Automation License Manager and transfer the required licenses for the SIMATIC software in the TIA Portal to your local drive.
3. Copy all required project data from the server to your local drive.
4. Start the VM and configure the network connection. Read the notes at the top of the page.

Transferring the virtual machine (VM) from the PG/PC to the remote device

To transfer the virtual machine back to the remote device, follow these steps:

- Copy the VM from your local PG/PC to the remote device. The exact procedure depends on the virtualization environment used. Refer to the corresponding documentation if you need help.
- Open the Automation License Manager and transfer the licenses from your local drive back to the ALM Server.
- Copy all required project data from your local drive back to the server.

See also

Installing the TIA Portal Cloud Connector on the PG/PC (Page 37)

Configuring the TIA Portal Cloud Connector on the PG/PC (Page 38)

Configuring the TIA Portal Cloud Connector in the VM (Page 40)

Online connection via the TIA Portal Cloud Connector (Page 51)

Index

C

- Certificate, 20
 - Adding, 49
 - Creating, 42, 46
 - Exporting, 43, 47
 - Importing, 44, 48
 - Removing, 51
 - Selecting, 45, 50
- Configuration, 7
- Configuring the HTTPS connection, 39, 41
- Configuring the TCP connection, 38, 40

I

- Info area, 7

O

- Online connection, 51

P

- PG/PC
 - Configuring, 38

S

- Simulation, 19
- Status display, 14, 52
- Status symbols, 52
- Support packages, 19

T

- Taskbar, 7
- TIA Portal Cloud Connector
 - Application case, 17
 - Basics, 5
 - Certificate, 20
 - Configuring, 7
 - Online connection, 51
 - Provision, 6
 - Status display, 14
 - User interface, 7

U

- User interface, 7

V

- VM
 - Configuring, 40

