SIEMENS

TIA Portal Cloud Connector

Programming and Operating Manual

03/2024
A5E53553201-AA

Legal information

Warning notice system

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

⚠ **DANGER**
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ **WARNING**
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ **CAUTION**
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E53553201-AA
Ⓟ 04/2024 Subject to change

Table of contents

Security information

1

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 constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

In this case, you should not use an unencrypted TCP connection. We recommend using an encrypted HTTPS connection or an encrypted VPN tunnel.

For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity)

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under:
https://www.siemens.com/cert (https://www.siemens.com/cert)

Introduction to the TIA Portal Cloud Connector 2

2.1 Safety Guidelines

Safety guidelines

This Help 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**
with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

Note

indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

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 device/system may only be set up and used in conjunction with this documentation. Commissioning and operation of a device/system may only be performed by qualified personnel. Within the context of the safety notes in this documentation qualified persons are defined as persons who are authorized to commission, ground and label devices, systems and circuits in accordance with established safety practices and standards.

Prescribed Usage

Note the following:

⚠ WARNING

This device may only be used for the applications described in the catalog or the technical description and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens. Correct, reliable operation of the product requires proper transport, storage, positioning and assembly as well as careful operation and maintenance.

Trademarks

Disclaimer of Liability

2.2 Basics of the TIA Portal Cloud Connector

Introduction

The TIA Portal allows you to work in a virtual environment. The TIA Portal Cloud Connector is an option for a variety of products that lets you access local PG/PC interfaces and the SIMATIC hardware connected to them in the TIA Portal engineering even though the engineering itself is operated in a private cloud.

You can use the add-on software "TIA Portal Cloud Connector" to access the SIMATIC hardware connected locally on your PG/PC from the VM. This requires an installation of the TIA Portal Cloud Connector on both the VM and on the PG/PC to which the hardware is connected. The TIA Portal Cloud Connector also allows remote access to the hardware of another PG/PC from the VM connected remotely, even if it is in a private network. Such access is not possible without the TIA Portal Cloud Connector.

Note

TIA Portal Cloud Connector

The TIA Portal Cloud Connector is only intended for engineering tasks with the TIA Portal. Online access during productive operation (for example SCADA) is thus not permitted. This applies especially to security programs. Also make sure that no time-critical processes are running on the system during access via the Cloud Connector.

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, or Industrial Edge box 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 33)
- "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 35)

TIA Portal Cloud

TIA Portal Cloud is a highly efficient online service with which you can work in a virtual environment anywhere and at any time. Via the TIA Portal Cloud Connector, you can access local PG/PC interfaces and SIMATIC hardware connected to them in TIA Portal Engineering in the cloud environment. The documentation of TIA Portal Cloud therefore supplements the documentation of TIA Portal Cloud Connector in some places.

For more information, refer to the documentation on TIA Portal Cloud:

https://premiumservices.siemens.com/tia_portal_cloud/help/en-US/index.html (https://premiumservices.siemens.com/tia_portal_cloud/help/en-US/index.html)

See also

User interface of the TIA Portal Cloud Connector for Windows (Page 9)

Using certificates (Page 22)

Installing the TIA Portal Cloud Connector for Windows (Page 23)

Configuring the TIA Portal Cloud Connector for Windows (Page 33)

Using TIA Portal Cloud Connector (Page 49)

2.3 User interface of the TIA Portal Cloud Connector for Windows

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

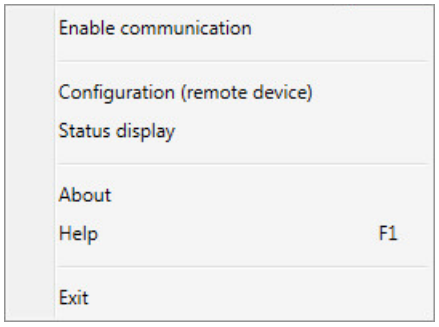
TIA Portal Cloud Connector in the information area of the Windows taskbar

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":

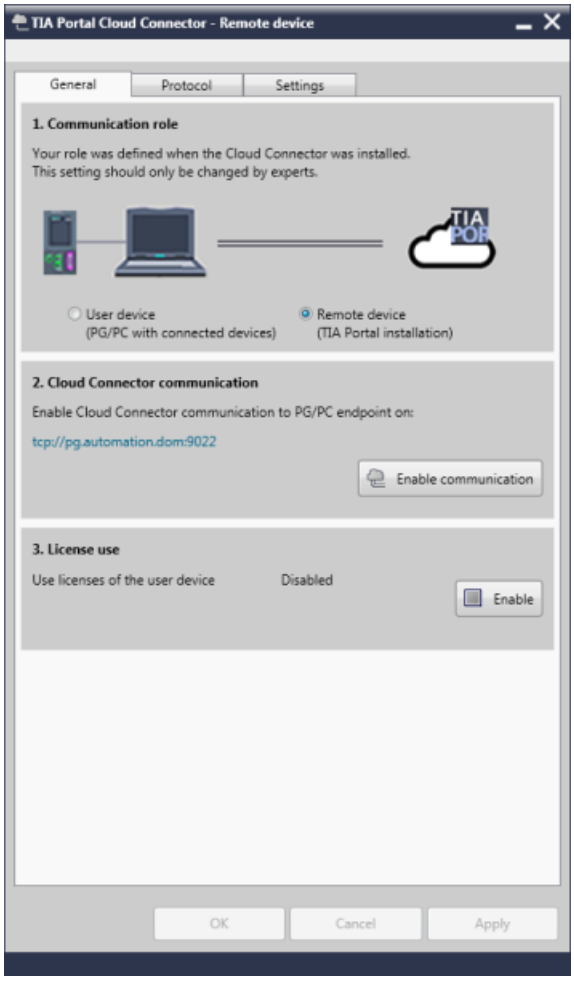


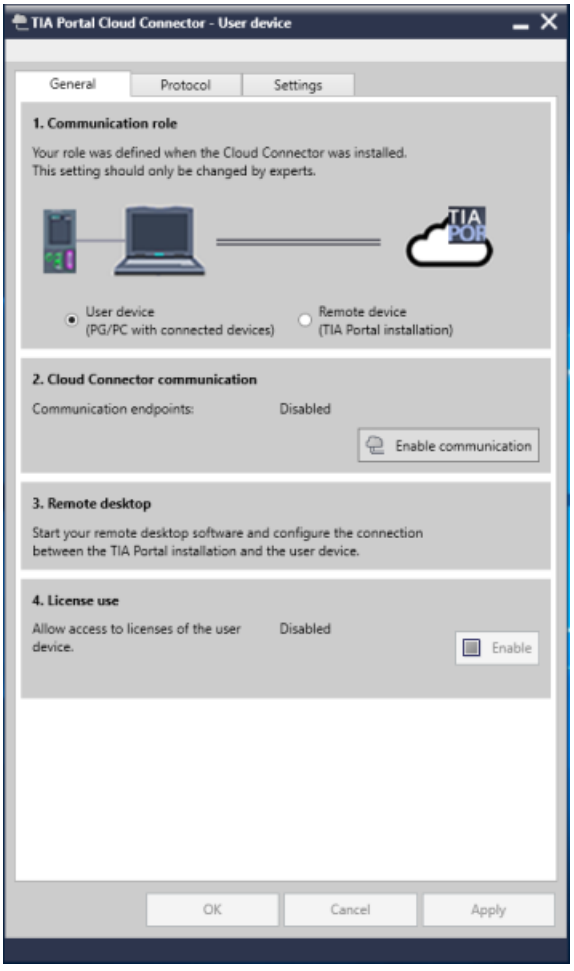
The menu gives you access to the following actions:

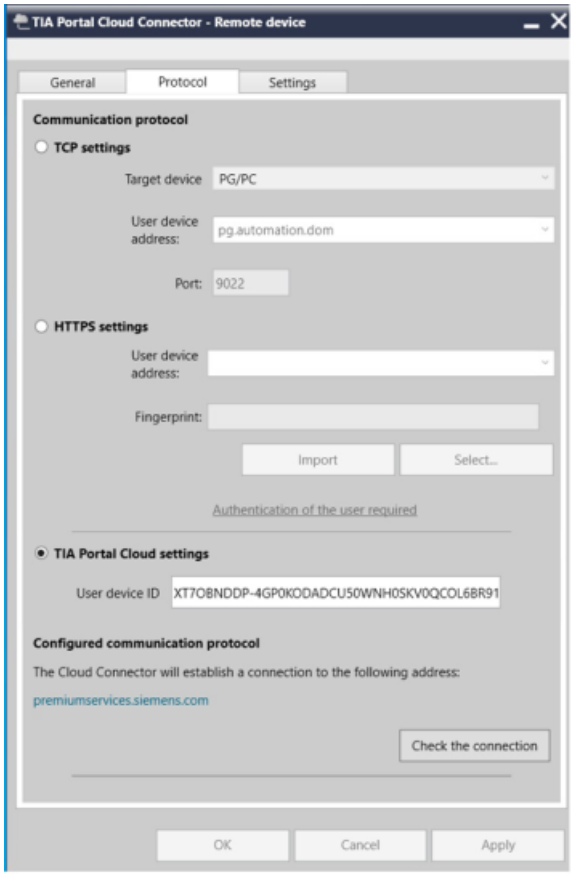
- Enable communication: Use this command to enable communication on both the remote and the user device.
- Configuration (remote device/user device): Opens the TIA Portal Cloud Configurator in the respective communication role.
- Status display: Opens the status display in which you are informed of all 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.

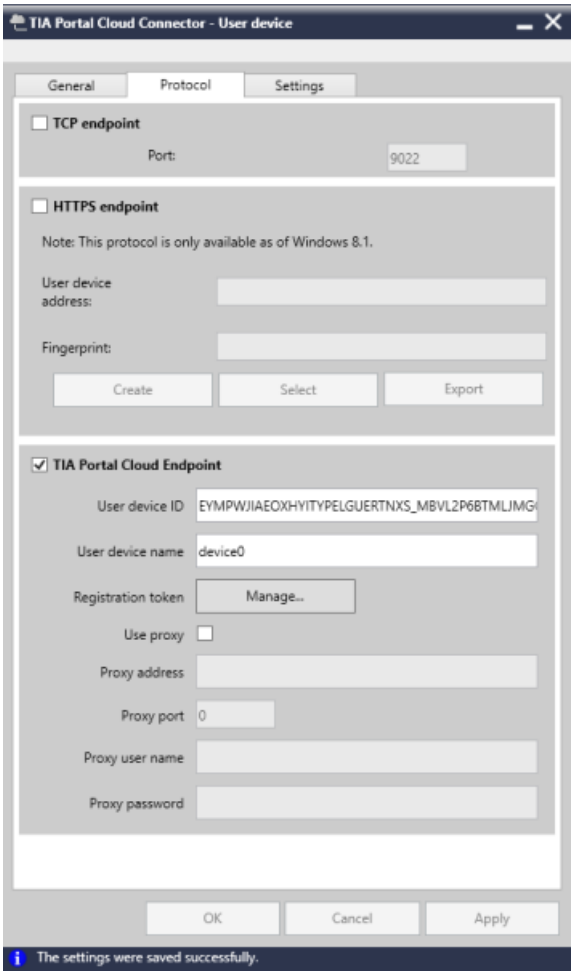
TIA Portal Cloud Connector - Settings

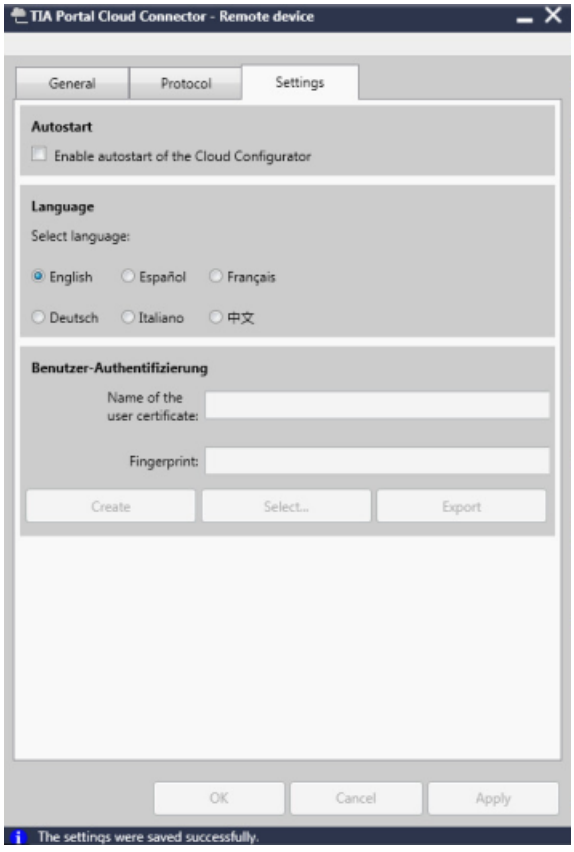
The user interface of the TIA Portal Cloud Connector differs depending on the selected communication role. The figures below show the various settings tabs of TIA Portal Cloud Connector for the communication roles "Remote device" and "User device":

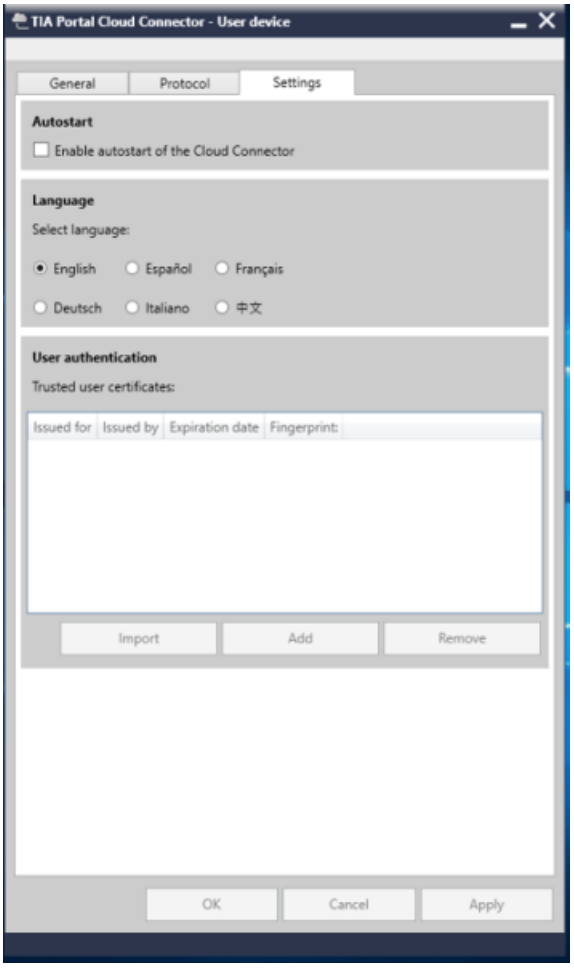





TIA Portal Cloud Connector - Remote device
General
Protocol
Settings
Communication protocol
TCP settings
Target device
PG/PC
User device address:
pg.automation.dom
Port:
9022
HTTPS settings
User device address:
Fingerprint:
Import
Select...
Authentication of the user required
TIA Portal Cloud settings
User device ID
XT7OBNDDP-4GP0KODADCU50WNH0SKV0QCOL6BR91
Configured communication protocol
The Cloud Connector will establish a connection to the following address:
premiumservices.siemens.com
Check the connection
OK
Cancel
Apply


TIA Portal Cloud Connector - User device
General
Protocol
Settings
TCP endpoint
Port:
9022
HTTPS endpoint
Note: This protocol is only available as of Windows 8.1.
User device address:
Fingerprint:
Create
Select
Export
TIA Portal Cloud Endpoint
User device ID
EYMPWJIAEOXHYITYPELGUERTNXS_MBVL2P6BTMLJMG
User device name
device0
Registration token
Manage...
Use proxy
Proxy address
Proxy port
0
Proxy user name
Proxy password
OK
Cancel
Apply
The settings were saved successfully.





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

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 use	Enable Disable	Enables or disables the use of a license on the user device.

Tab	Area	Setting/button	Description
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.
	TIA Portal Cloud settings	User device ID	Shows the ID of the user device used in TIA Portal Cloud.
	Configured communication protocol	Check the connection	Checks whether the connection can be established without problems.
Settings	Autostart	Enable autostart 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.

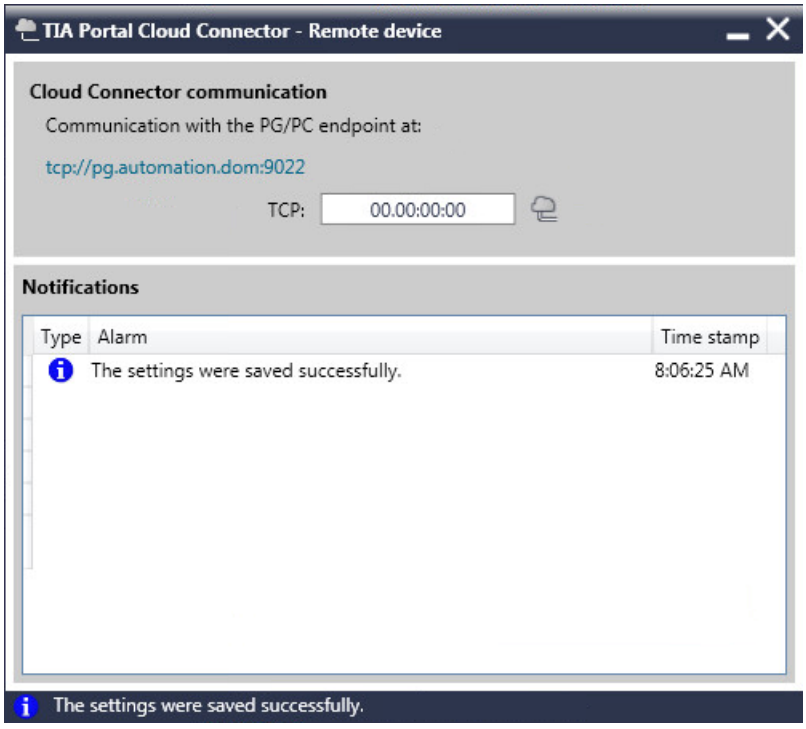
The table below provides an overview of the possible settings and the existing buttons for the communication role "User device":

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 use	Enable Disable	Enables or disables the use of a license on the user device.

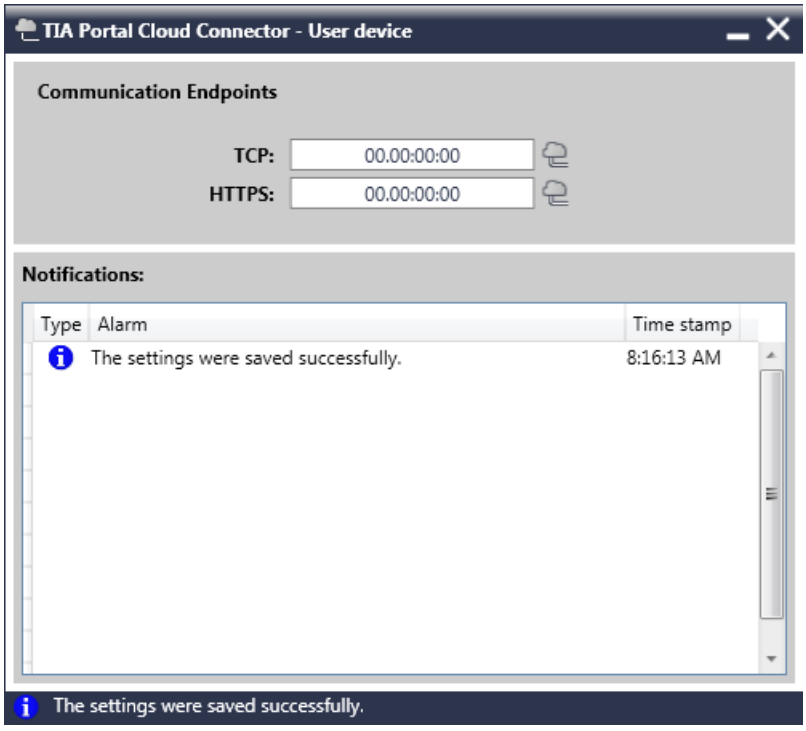
Tab	Area	Setting/button	Description
Protocol	TCP endpoint	Port	Port number through which communication is to take place. The port number of the user device must match the port number of the remote device.
	HTTPS endpoint	User device address	IP address or name of user device
		Fingerprint	Ensures the integrity of the certificate.
		Create	Creates a new certificate for data encryption.
		Select	Gives you the option of selecting an existing certificate.
		Export	Exports the currently used certificate.
	TIA Portal Cloud endpoint	User device ID	Shows the ID of the user device used in TIA Portal Cloud.
		User device name	Shows the name of the user device.
		Registration token > Manage	Opens the "TIA Portal Cloud Connector - Manage registration token" dialog, where you can manage your registration tokens.
		Using a proxy	Select this check box if you are using a proxy server.
		Proxy address	Shows die proxy address.
		Proxy port	Port number through which communication is to take place. The port must be identical to the one specified on the remote device.
		Proxy user name	Shows the proxy user name.
		Proxy password	Shows the proxy password.
Settings	Autostart	Enable autostart 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:

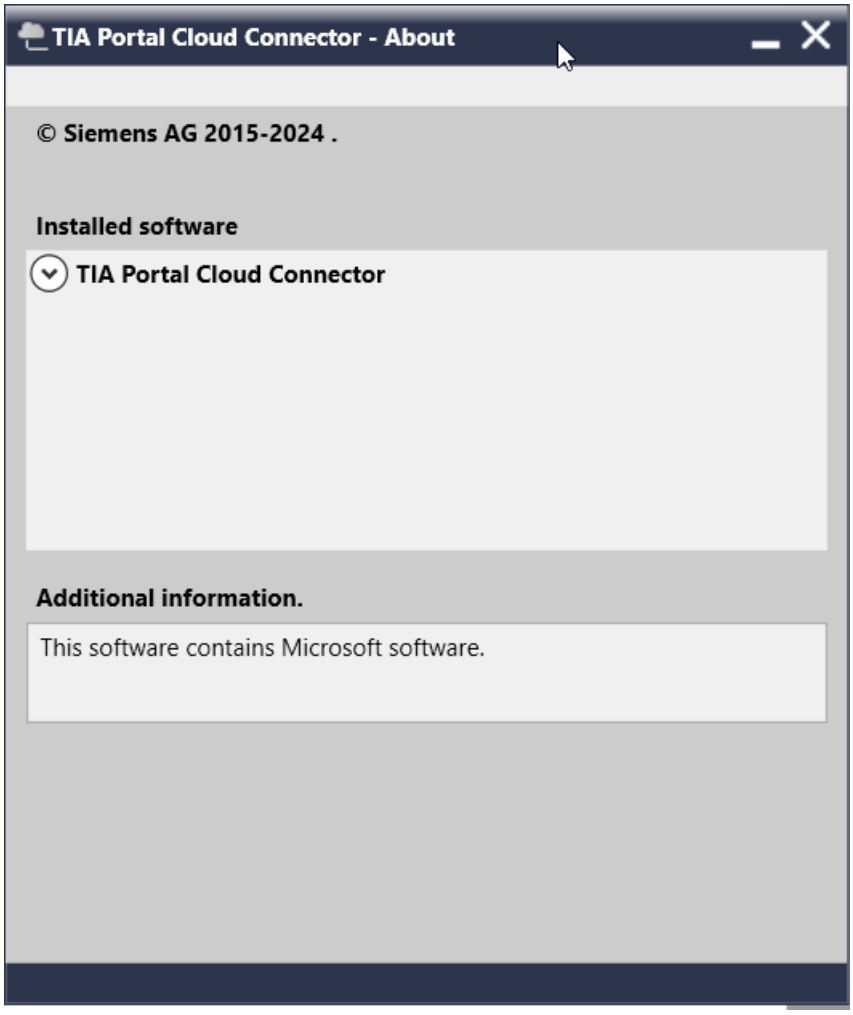


The following figure shows the status display in the "User device" communication role:


TIA Portal Cloud Connector - User device
Communication Endpoints
TCP:
00.00:00:00
HTTPS:
00.00:00:00
Notifications:
Type
Alarm
Time stamp
The settings were saved successfully.
8:16:13 AM
The settings were saved successfully.

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 the TIA Portal Cloud Connector (Page 8)

Using certificates (Page 22)

2.4 Registering user devices for TIA Portal Cloud

In the TIA Portal Cloud Connector, you have the option of configuring a TIA Portal Cloud endpoint in the user device in the "Protocol" tab. This option requires that you generate a secure registration token in TIA Portal Cloud. This user-specific token connects the TIA Portal Cloud Connector to the TIA Portal Cloud endpoint. A maximum of 100 user devices can be registered with a valid token.

More information on generating the registration token can be found in the documentation on TIA Portal Cloud.

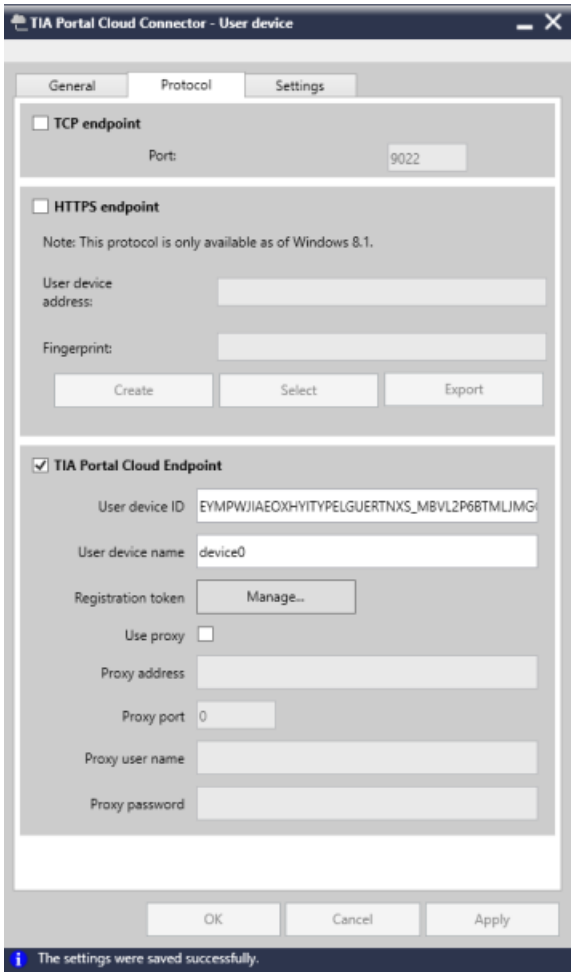
Requirement

You have generated a valid registration token in TIA Portal Cloud.

Procedure

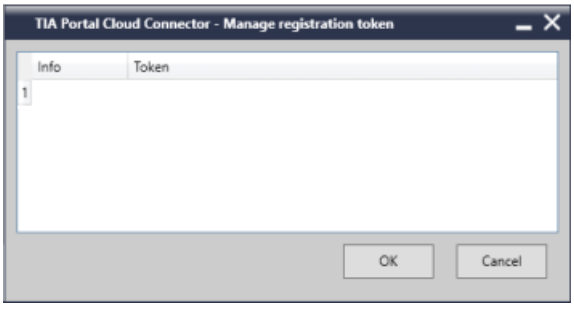
Follow these steps to register user devices:

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. Switch to the "Protocol" tab.



3. Select the "TIA Portal Cloud Endpoint" check box.
4. Enter a name for the user device.

5. Click the "Manage..." button in the "Registration token" line.
   The "TIA Portal Cloud Connector - Manage registration token" dialog opens.



6. Insert the registration token from TIA Portal Cloud in the "Token" column.
7. Optionally, enter additional information, such as the name of the token user, in the "Info" column.
8. Insert additional user devices into the table as needed. You can register a maximum of 100 user devices with the same token. After this number has been exceeded, you receive a message and you can deregister a device to register a new device, if desired.

2.5 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.

2.6 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 the TIA Portal Cloud Connector (Page 8)

User interface of the TIA Portal Cloud Connector for Windows (Page 9)

Creating certificate for data encryption (Page 37)

Exporting certificate for data encryption (Page 38)

Importing certificate for data encryption (Page 39)

Selecting certificate for data encryption (Page 40)

Creating certificate for user authentication (Page 41)

Exporting certificate for user authentication (Page 42)

Importing certificate for user authentication (Page 43)

Adding certificate for user authentication (Page 44)

Selecting certificate for user authentication (Page 45)

Removing certificate for user authentication (Page 46)

Installing the TIA Portal Cloud Connector for Windows

3

3.1 System requirements

3.1.1 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 10 Professional
- Windows 10 Enterprise
- Windows 11 Professional
- Windows 11 Enterprise
- Windows Server 2019 Standard
- Windows Server 2022 Standard

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".

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 25)

3.1.2 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

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.

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 25)

3.1.3 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 26)

See also

System requirements PG/PC (Page 23)

System requirements for VM (Page 24)

3.1.4 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 25)

3.2 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".

3.3 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".

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".

3.4 Updating the TIA Portal Cloud Connector

You can determine the version of the TIA Portal Cloud Connector that is installed on the device via the TIA Portal Cloud Connector info window. If a newer version is available, you can update the TIA Portal Cloud Connector.

Determining the installed version of the TIA Portal Cloud Connector

Follow these steps to determine the installed version of the TIA Portal Cloud Connector:

1. Right-click on the icon for the TIA Portal Cloud Connector in the information area of the taskbar and select the "About" command.
   The TIA Portal Cloud Connector info window opens.
2. In the "Installed software" area, click on the down arrow in front of the "TIA Portal Cloud Connector" entry.
   The version number of the TIA Portal Cloud Connector is shown.

Updating the TIA Portal Cloud Connector

Follow these steps to update the TIA Portal Cloud Connector:

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".

Configuring the TIA Portal Cloud Connector for Windows

4

4.1 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. By default, the communication protocol is set to HTTPS and "TIA Portal Cloud Endpoint".

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 37)
   Selecting certificate for data encryption (Page 40)
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 41)
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 43)
   Adding certificate for user authentication (Page 44)
10. Open the "General" tab again.
11. Click "Enable communication" in the "Cloud Connector Communication" area.

Configuring the TIA Portal Cloud connection

If you work with a paid version of TIA Portal Cloud and want to access user devices in your company network from there, proceed as follows to configure a connection:

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 "TIA Portal Cloud endpoint" check box.
6. Enter the name in the "User device name" field.
7. Click the "Manage" button.
   The "TIA Portal Cloud Connector - Manage registration token" dialog opens.
8. Copy the registration token generated in TIA Portal Cloud into a field in the "Token" column.
9. If you are using a proxy server, select the "Use Proxy" check box and enter the necessary information in the boxes below.
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.

4.2 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 connection can be established from a VM to the PG/PC. 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.
- **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.

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.
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 39)
   Selecting certificate for data encryption (Page 40)
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 41)
    Selecting certificate for user authentication (Page 45)
11. Open the "General" tab again.
12. Click "Enable communication" in the "Cloud Connector Communication" area.

Configuring the TIA Portal Cloud connection

If you work with a paid version of TIA Portal Cloud and want to access user devices in your company network from there, proceed as follows to configure a connection:

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. Switch to the "Protocol" tab.
6. Activate the "TIA Portal Cloud Settings" check box.
   The ID of the user device is entered automatically.

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.

4.3 Using certificates (for HTTPS connections only)

4.3.1 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 22)
Exporting certificate for data encryption (Page 38)
Importing certificate for data encryption (Page 39)
Selecting certificate for data encryption (Page 40)

4.3.2 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 22)

Creating certificate for data encryption (Page 37)

Importing certificate for data encryption (Page 39)

Selecting certificate for data encryption (Page 40)

4.3.3 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 22)

Creating certificate for data encryption (Page 37)

Exporting certificate for data encryption (Page 38)

Selecting certificate for data encryption (Page 40)

4.3.4 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 22)
Creating certificate for data encryption (Page 37)
Exporting certificate for data encryption (Page 38)
Importing certificate for data encryption (Page 39)

4.3.5 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 22)
Exporting certificate for user authentication (Page 42)
Importing certificate for user authentication (Page 43)
Adding certificate for user authentication (Page 44)
Selecting certificate for user authentication (Page 45)
Removing certificate for user authentication (Page 46)

4.3.6 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 22)
Creating certificate for user authentication (Page 41)
Importing certificate for user authentication (Page 43)
Adding certificate for user authentication (Page 44)
Selecting certificate for user authentication (Page 45)
Removing certificate for user authentication (Page 46)

4.3.7 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 22)
Creating certificate for user authentication (Page 41)
Exporting certificate for user authentication (Page 42)
Adding certificate for user authentication (Page 44)
Selecting certificate for user authentication (Page 45)
Removing certificate for user authentication (Page 46)

4.3.8 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 22)
Creating certificate for user authentication (Page 41)
Exporting certificate for user authentication (Page 42)
Importing certificate for user authentication (Page 43)
Selecting certificate for user authentication (Page 45)
Removing certificate for user authentication (Page 46)

4.3.9 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 22)
Creating certificate for user authentication (Page 41)
Exporting certificate for user authentication (Page 42)
Importing certificate for user authentication (Page 43)
Adding certificate for user authentication (Page 44)
Removing certificate for user authentication (Page 46)

4.3.10 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 22)
Creating certificate for user authentication (Page 41)
Exporting certificate for user authentication (Page 42)
Importing certificate for user authentication (Page 43)

Adding certificate for user authentication (Page 44)
Selecting certificate for user authentication (Page 45)

Using TIA Portal Cloud Connector

5

5.1 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.

5.2 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.

TIA Portal Cloud Connector for Edge

6

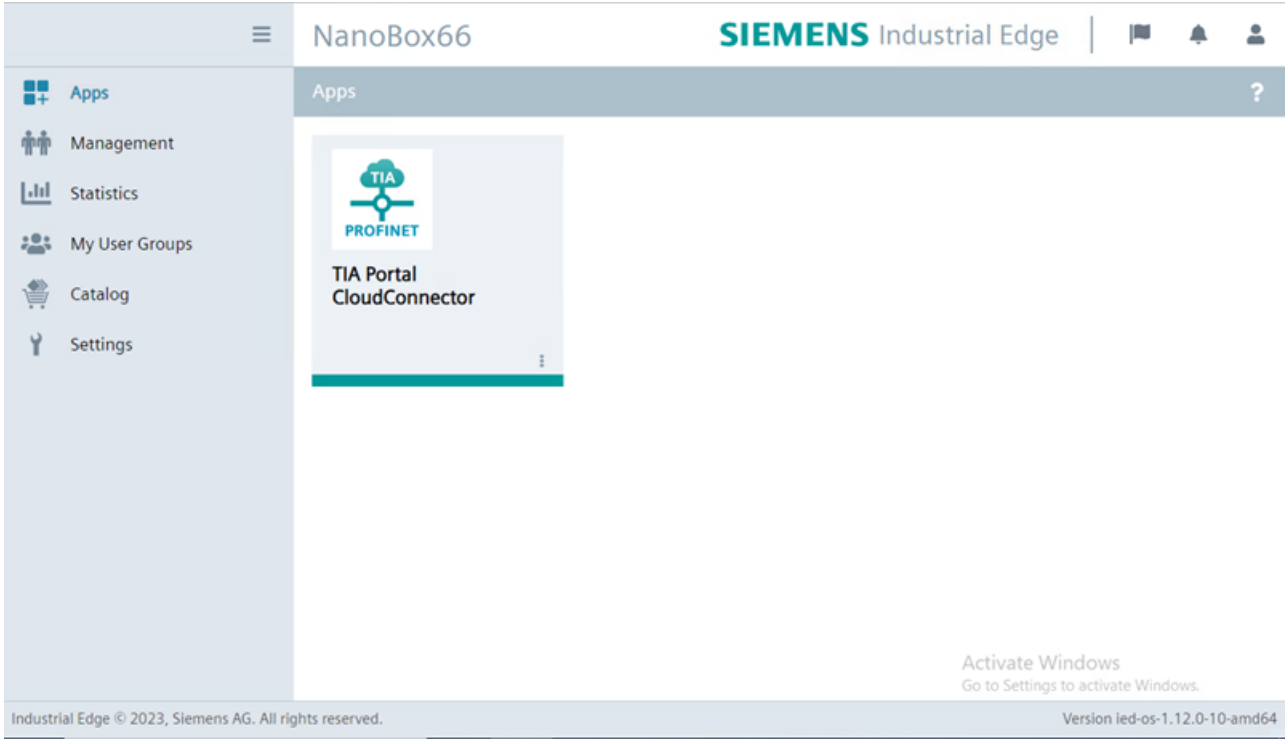
6.1 Introduction to TIA Portal Cloud Connector for Edge

Prerequistes

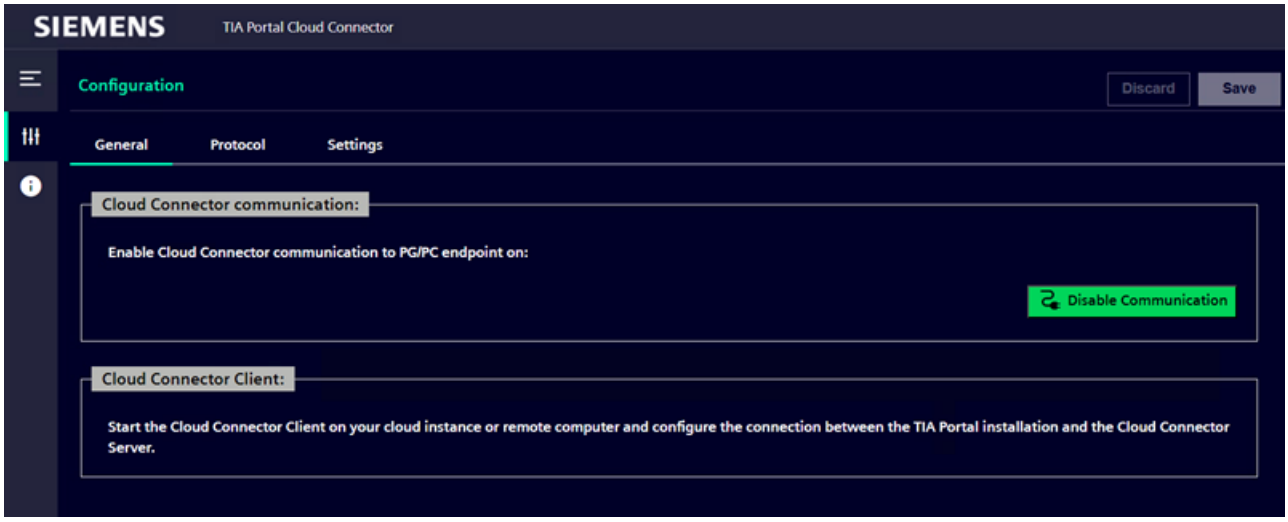
- Set up Industrial Edge Device (IED) or Edge Box.
- Download the TIA Portal Cloud Connector application from the Siemens Digital Exchange (SDEX) > "Industrial Edge Marketplace".
- Install TIA Portal Cloud Connector Edge application on the Edge Box or IED.

6.2 Launching TIA Portal Cloud Connector Edge Application for IED

1. Log in to IED.
   You will see TIA Portal Cloud Connector under “Apps”.



2. Click TIA Portal Cloud Connector, the application will launch in the browser.



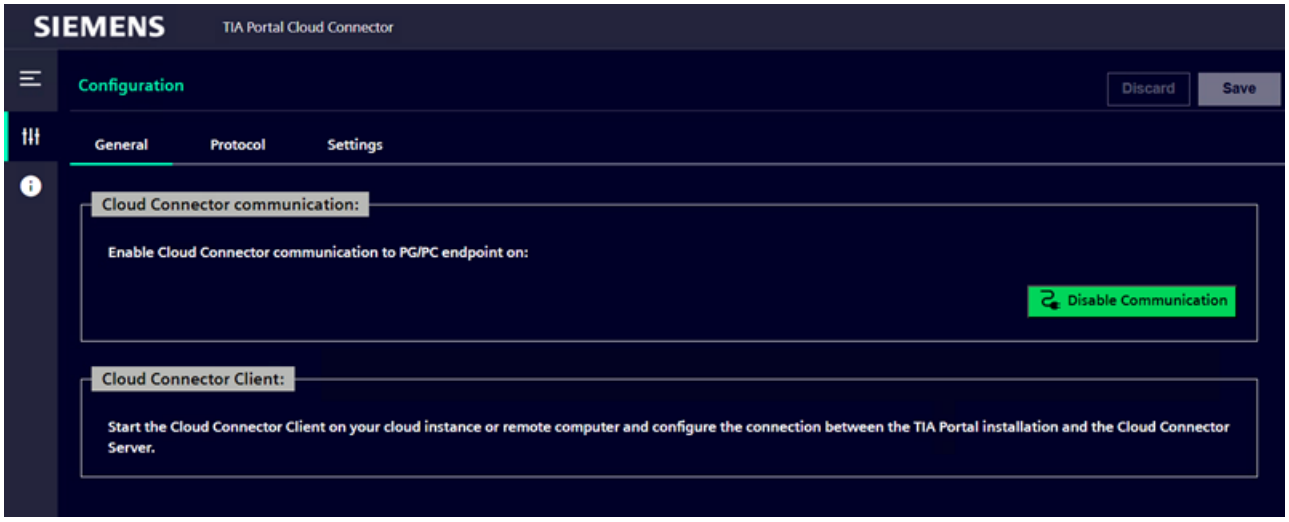
6.3 Configuring TIA Portal Cloud Connector Edge Application for IED

Registering a User device

To establish a connection between User device and Remote device, you must get the registration token from the Siemens Industry Premium Portal.

To register a User device, follow these steps:

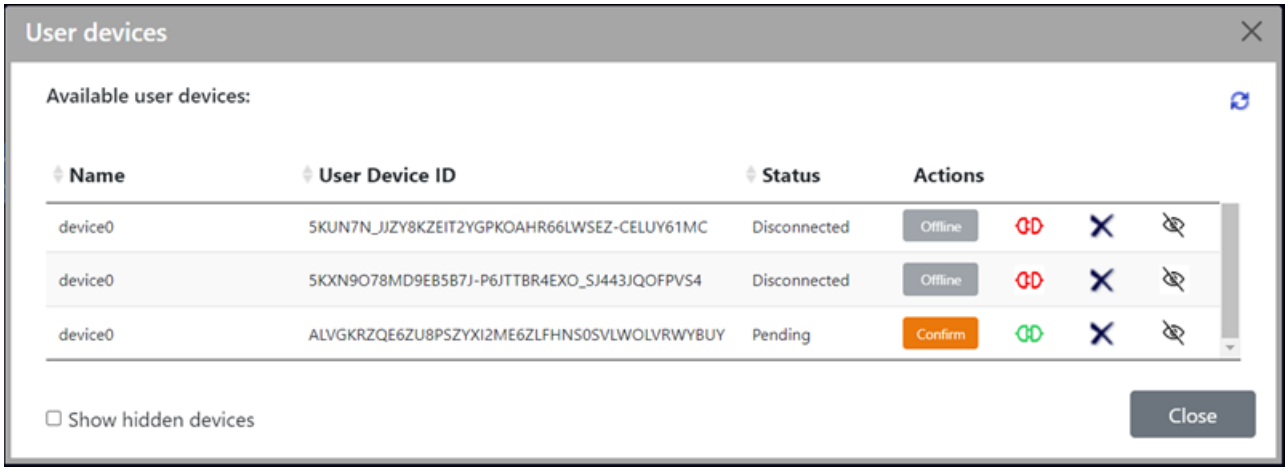
1. Launch TIA Portal Cloud Connector in IED.



2. Go to the “Protocol” tab and click "Manage".
   Manage registration token dialog box opens.
3. Click “Add Token”.
4. In the “Token” column, enter a valid token key that is taken from the Siemens Industry Premium Portal.
   You can register a maximum of 100 User devices with a valid token. After this number exceeds, you receive a message and you can deregister a device to register a new device, if required.
5. Optionally, enter additional information, such as, name of the token user, in the "Info" column.
6. Click “OK”. Manage registration token dialog box closes.
7. Click “Save” to save the changes. In case if you want to discard the changes, click “Discard”.
8. To communicate with the Remote device, go to the “General” tab and click "Enable Communication".

Once connection is successful, “Enable Communication” will turn to yellow color and the text will change to “Disable Communication”.

Once TIA Portal Cloud Connector is connected to Remote device, the connected User device is visible under User device list in the respective TIA Portal Cloud VM.



To establish a connection between User device and Remote device follow these steps:

1. Click “User devices” in your TIA Portal Cloud VM.
2. To accept a newly registered User device, click “Confirm”. A confirmation dialog appears.
3. Click “Accept”.
   The User device is set to the "Offline" status.
   The User device status will turn to online. As soon as a device is in the "Online" status, other users who use this functionality will see the "In use" status in their VM.
   For more information, refer Working with User devices chapter from TIA Portal Cloud online help document.
   If you wan to disable the device, click “Offline”.
4. Launch TIA Portal from the Remote device.
5. Click “Project View”.
   Once you click project view on the Remote device, “Disable Communication” color will change from yellow to green.

Troubleshooting 7

7.1 Introduction

Purpose

This chapter describes the user issues and troubleshooting steps while working with “Cloud Connector”.

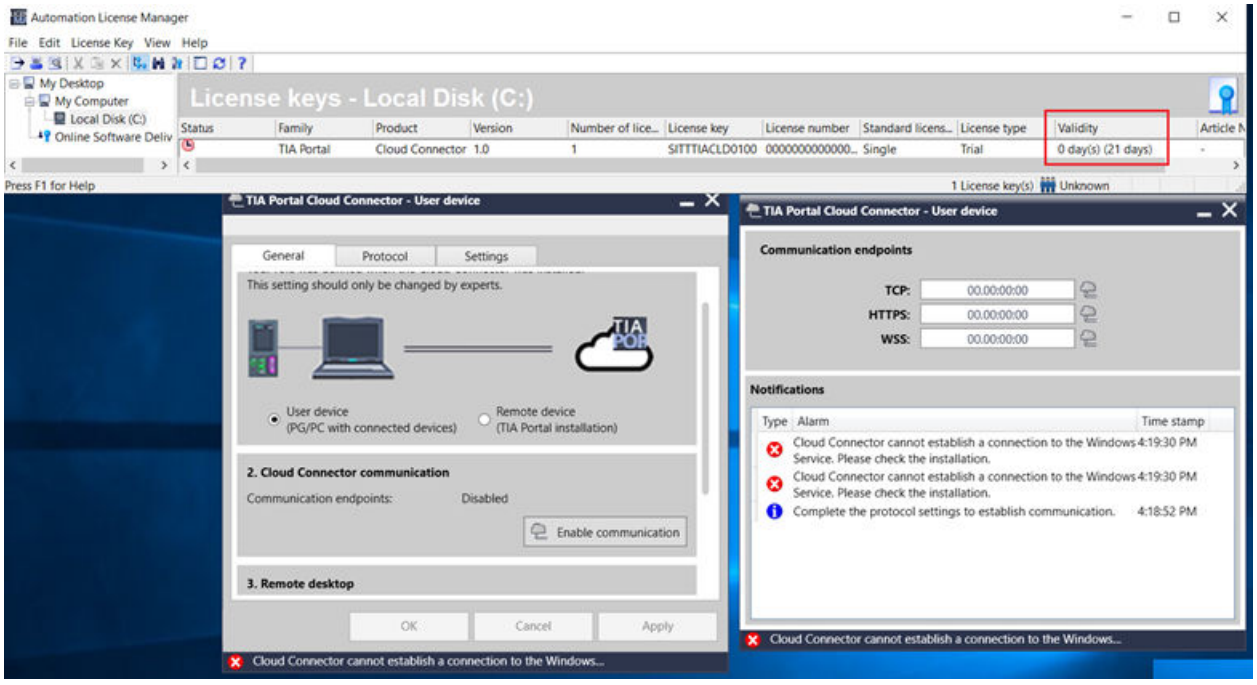
Basic Information

Refer TIAPortalCloudConnectorHowToenUS.pdf from the DVD folder to know how to use Cloud Connector in detail.

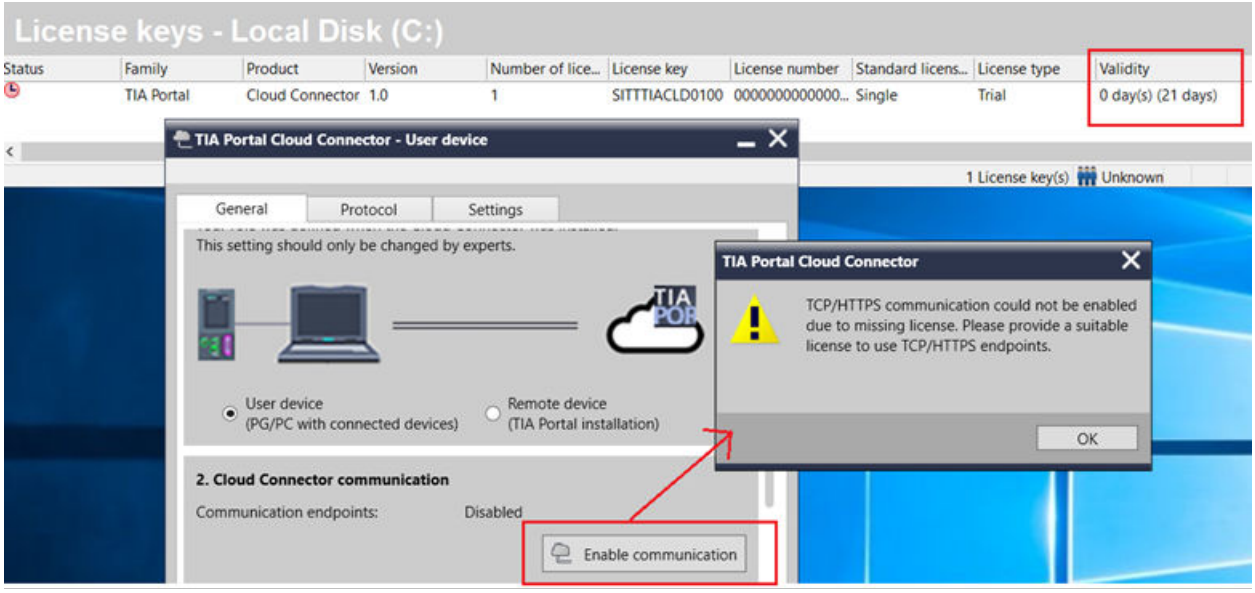
7.2 License

- After successful installation of Cloud Connector, 21 days trial license is available.
- Once communication is established by clicking “Enable Communication”, license activates.
- Licenses are only required on server side.

- If Cloud Connector is running, and its license has expired, below error is displayed:



- If TCP/HTTPS endpoints are selected and its license has expired. On clicking "Enable communication" a missing license warning pop-pup appears.



7.3 How to launch Cloud Connector

Cloud Connector User Interface (UI) or Configuration window will be launched in two ways:

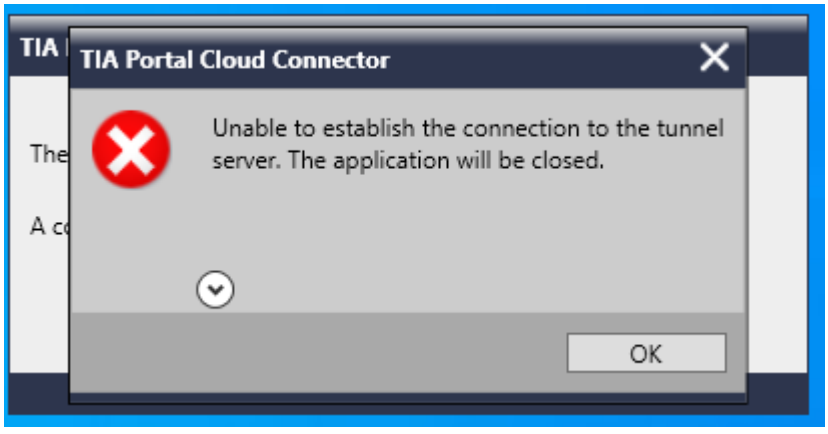
- From Windows Start menu > “TIA Portal Cloud Connector".
- Right click the "TIA Portal Cloud Connector" from the system tray.

Check Cloud Connector service status

Once the setup is installed, search “TIA Portal Cloud Connector” from the Windows Start menu.

Click "TIA Portal Cloud Connector", "TIA Portal Cloud Connector" window opens.

Issue 1: After launching Cloud Connector, if below error occurs:



Solution: Check if the “S7DOS SCP Remote” service is running or not, if not, start the S7DOS SCP Remote service.

Issue 2: If “S7DOS SCP Remote” service is not running or stopped after launching Cloud Connector, Cloud Connector and System tray User Interface will be in greyed out state.

Solution: Check if the “S7DOS SCP Remote” service is running or not, if not start the S7DOS SCP Remote service.

Check whether Cloud Connector server is running and how you can validate each step

1. Once the setup is complete, search “TIA Portal Cloud Connector” from the Windows Start menu.
2. Click "TIA Portal Cloud Connector". "TIA Portal Cloud Connector" window opens.

3. If TIA Portal is installed, select Remote device (RD) as the default communication role.
4. If Cloud Connector license is available, then select User device (UD) as the default communication role.

Note

Cloud Connector license is required only for User device.

If Cloud Connector license is not available, User device will be greyed out.

To check Cloud Connector license, open Automation License Manager (ALM) and check the validity.

7.4 Configuration

7.4.1 Configuring Cloud Connector

TCP and HTTPS endpoints support enterprise network within two different subnets.

Refer TIAPortalCloudConnectorHowToenUS.pdf chapter 1.3 - User interface of the TIA Portal Cloud Connector.

7.4.2 TCP endpoint

User device:

- Default port number is 9022.
- From the General tab enable communication.

Remote device:

- You must enter TCP settings parameters like Target device, User device address, User device configured port number.

  Note

  Two types of target devices are there, PG/PC for Windows communication and SCALANCE for Linux.

  – If you enter an incorrect port number during enable communication, an error saying " A connection to user device is aborted" will be displayed.
- You can verify the accessibility of User device by clicking the URL under “Configured Communication Protocol” in the "Protocol" tab, and “Cloud Connector Communication” URL in the "General" tab.
- Once User device and Remote device “Enable Communication” is successful, “Enable Communication” button gets changed to “Disable Communication” and color will be in yellow.

- In Cloud Connector status window, under “communication endpoint” section, TCP connection icon also will get changed to yellow color.
- Cloud Connector connection will be established from Remote device and User device, while going to TIA Portal “Portal View”. Once connection is established successfully the “Disable Communication” button will be in green color in Remote device and User device.
- Cloud Connector status window “communication endpoint” section, TCP connection icon also will be changed to green color and timer will start.
- Once connection is established in Remote device and User device, you cannot “Disable Communication” until TIA Portal is up and running. Same way you cannot “Disable Communication” in Remote device until Cloud Connector User device communication is disabled.
- Once TIA Portal is getting closed, Cloud Connector connection will be closed automatically. This will be observed by seeing Cloud Connector's “Disable Communication” button color changing to yellow.

7.4.3 HTTPS endpoint

User device

You can create a new certificate, or you can select the existing certificate from the protocol tab (From Remote device and User device). You must import valid User device and Remote device certificate for authentication.

To create User device certificate, follow the below steps:

1. In the "Protocol" tab, click "Create". "Create Certificate" dialog opens.
2. In the "Domain names" text field, enter domain names or select domain names from the drop-down and click the + button for confirmation.
3. Click "Browse", and select export file location.
4. Select Valid from and Expiration date, and click "OK".
5. Click "Apply".
   You can use available certificate using “Select” option.

Remote device

User device certificate can be used in “Import” option from “Protocol” tab under “Https Settings”.

To create Remote device certificate, follow the below steps:

1. Click “Authentication of user required” link or go to "Settings" > “User Authentication” section for creating Remote device certificate.
2. Create Remote device certificate using “create certificate” dialog or select exiting certificate and click "Apply".

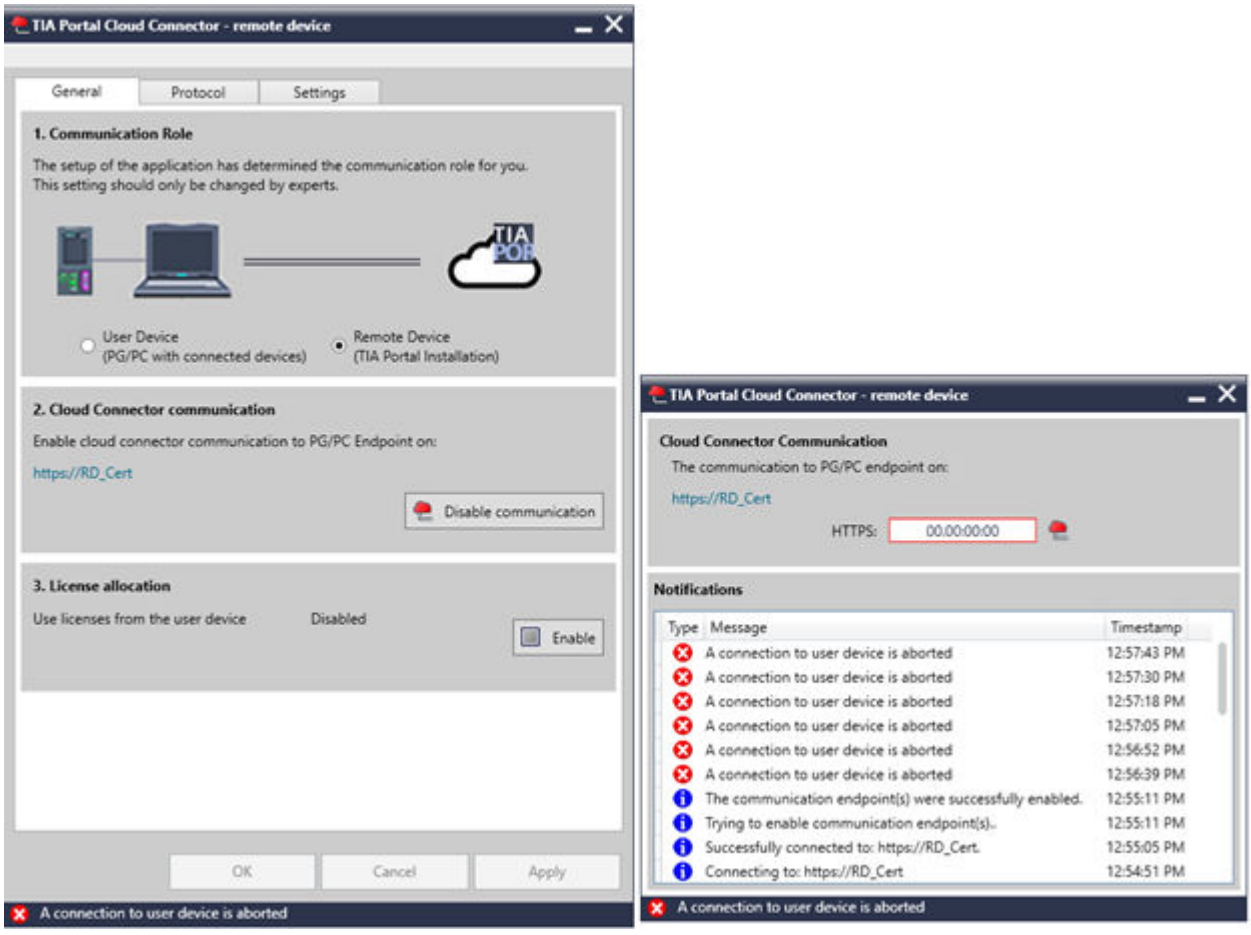
3. Once Remote device certificate is created, go to User device “Settings” > “User authentication”, and import Remote device certificate.
4. Once User device and Remote device certificates are applied, go to the “General” tab and click “Enable Communication”.
   Once User device and Remote device “Enable Communication” is successful. “Enable Communication” button gets changed to “Disable Communication” and color will be in Yellow.
   Cloud Connector status window “communication endpoint” section, and TCP connection icon also will get changed to yellow color.

Note

- Once User device and Remote dvice “Enable Communication” is successful, TIA portal can be launched from Remote device side.
- Cloud Connector connection will be established from Remote device User device, while going to TIA Portal “Portal View”. Once connection is established successfully, “Disable Communication” button will be in green color in Remote device and User device.
- Cloud Connector status window “communication endpoint” section and Https connection icon also will get changed to green color, and timer will start.
- Once connection is established Remote device and User device, you cannot “Disable Communication” until TIA Portal is running. Same way you cannot “Disable Communication” in Remote device until Cloud Connector is running.
- Once TIA Portal is closed, Cloud Connector connection will be closed automatically. This will be observed by seeing Cloud Connector's “Disable Communication” button color changing to yellow.

Error scenarios:

- If HTTPS certificate is invalid, below error is displayed:



- If HTTPs certificate is expired, an error message "Cloud connector cannot establish connection to Windows" is displayed, and a system message "A connection to user device is aborted" is displayed.

7.4.4 TIA Portal Cloud endpoint

Prerequisite

Internet connection is mandatory if TIA Portal Cloud endpoint is selected.

- TIA Portal Cloud Endpoint is the default endpoint selection in the User device.
- Click "Manage", and configure registration token.

- You can enter up to 100 registration tokens which can serve multiple remote devices (up to 100).
- If you enable proxy, proxy information must be configured (Use proxy, Proxy address, port, User name, Password).

7.4.5 Registration Token handling

Note

- Generate and copy registration token from premium portal cloud VM (https:// premiumservices.siemens.com (https://premiumservices.siemens.com)), using the “Get registration token” dialog.
- Generated registration token is applicable only for that premium portal cloud VM or Remote device verification.
- Registration token is valid for 3 months. Using the refresh button you can generate new token. Once you generate new token, old token is invalid.
- Copied registration token must be updated in Cloud Connector User device.

To update registration token in Cloud Connector User device follow the below steps:

1. Launch Cloud Connector and select User device.
2. Go to the "Protocol" tab.
3. Click "Manage registration token".
4. Enter a valid registration token.
5. Click "OK".
6. Click "Apply".
   If you enter a valid registration token, “The settings were saved successfully “ message displayed in both, status bar, and in system tray status display window.

Note

- Once User device “Enable Communication” is successful. The “Enable Communication” button gets changed to “Disable Communication” and color is in Yellow.
- Cloud Connector status window “Communication Endpoint” section, and WSS connection icon also get changed to yellow color.

7.4.6 Premium Portal Cloud VM

Premium portal cloud VM “User devices” dialog contains newly established User device communication device information with “Pending” status.

Once you click “Confirm”, Premium portal service establishes communication with Cloud Connector User device. Once communication is established, User device status get changed to “Offline”.

Note

If you get any Internet issues after clicking confirm, communication between Premium portal service and Cloud Connector User device will disconnect. Again you must Disable and Enable communication from Cloud Connector User device side. New entry is listed under “User devices” with “Pending” status, again user must confirm the request from Cloud Connector User device.

- To establish communication between premium portal service and Cloud Connector Remote device, click “Online” action. Once communication is established, status will change to “Online”.
- Cloud Connector connection will be established from Remote device to User device while launching TIA Portal and going to “Portal View”. Once connection is successful, the “Disable Communication” button is in green color in User device.
- Cloud Connector status window “communication endpoint” section, and WSS connection icon also get changed to green color and timer will start.

7.4.7 Error scenario

Internet connection disabled

If you get an error "The tunnel communication needs to be checked", reason for this error is, internet connection is disconnected.

To resolve this issue, enable internet connection.

Once connection is established in Remote device and User device, you cannot go “Offline” until TIA Portal is running. Same way you cannot “Disconnect” in Remote device until Cloud Connector User device communication is disabled.

Invalid registration token

If you get an error “Invalid tokens (Error number = - XX),” reason for this error is, you have entered an invalid registration token or registration token is expired.

To resolve this error, enter correct registration token, if you enter valid registration token, “The settings were saved successfully “message is displayed in both status bar, and in system tray status display window.

Registration token is not configured

If you get an error “It was not possible to execute the job. (Error number =-1”, reason for this error is, registration token is not configured.

Follow the below steps to resolve the error:

1. Launch Cloud Connector.
2. Go to the "Protocol" tab.
3. Click the "Manage registration token" button.
4. Enter a valid registration token.
5. Click "OK".
6. Click "Apply".
7. Click "Enable communication".

TIA Portal Cloud endpoint is selected on the User device side

If you get an error, “There was a problem enabling communication endpoints”, reason for this error is, only TIA Portal Cloud endpoint is selected on the User device side, follow the below steps to resolve the error:

1. Check if proxy is set and it is configured properly or not. If not configured, configure valid proxy in the system.
3. Restart the system after configuring proxy.
4. Relaunch Cloud Connector.
5. Click "Enable communication".

7.4.8 PLC online connectivity issue

For TIA Portal Cloud endpoint, If enable communication is not successful, it might be due to internet access not available at the system level. Ensure to enable the internet access at system level.

If internet access for your PC is available only at Local user level, then you must run cloud connector on the local user account.

Follow below steps to run Cloud Connector on Local user Account:

1. Provide write/read registry access for local user account for the below registry path: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Shared Tools\S7DOS64
2. Open Services.msc from Command Prompt.
3. Search for the service S7DOS SCP Remote, and stop the service if it is in running state.
4. Select the “S7DOS SCP Remote” service, right click and open properties.
5. Under the “Log On” tab, select “This account” and provide your local user credentials.
6. Start the “S7DOS SCP Remote” service.
7. Open Cloud Connector and follow the registration process.

7.5 Revision history

Sr.No	Date of Revision	Version No	Description of Change	Change Reference	Change Made by
1	15.06.2023	1.2.5	Troubleshooting chapter is added.		Ravikumar Chinnusamy Prachi Pattnaik

Index