SIEMENS

TIA Portal Cloud

Application Manual

Introduction 1

System requirements 2

Starting TIA Portal Cloud 3

Using an instance 4

Accessing PLCs in a company network 5

Problem solving and troubleshooting 6

Troubleshooting TIA Portal Cloud Connector 7

02/2026
A5E55384080-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 persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the application described in the catalog and the associated usage information. 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

A5E55384080-AA
Ⓟ 02/2026 Subject to change

Copyright © Siemens 2026.
All rights reserved

Table of contents

1 Introduction 5

1.1 Cybersecurity information 5

1.2 Introduction to TIA Portal Cloud 5

1.3 Versions of TIA Portal Cloud 6

1.4 Licenses 8

1.5 Basics of working with TIA Portal Cloud 8

2 System requirements 11

3 Starting TIA Portal Cloud 13

4 Using an instance 17

4.1 User instance 17

4.2 Using an instance 19

4.3 Hibernate / Stop Instance 20

4.4 Copying projects/files to the instance 22

4.5 Copying projects/files from the instance to your local PC 22

4.6 Files Synchronization 23

5 Accessing PLCs in a company network 25

5.1 Accessing PLCs in a company network 25

5.2 Request registration token and log in user device 26

5.3 Working with user devices 29

6 Problem solving and troubleshooting 33

7 Troubleshooting TIA Portal Cloud Connector 35

7.1 Introduction 35

7.2 Registry 35

7.3 License 36

7.4 How to launch Cloud Connector 37

7.5 Configuration 38

7.5.1 Configuring Cloud Connector 38

7.5.2 TCP endpoint 38

7.5.3 HTTPS endpoint 39

7.5.4 TIA Portal Cloud endpoint 41

7.5.5 Registration Token handling 42

7.5.6 TIA Cloud Services 43

7.5.7 Error scenario 43

7.5.8 PLC online connectivity issue 44

1 Introduction

1.1 Cybersecurity information

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html)

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://new.siemens.com/global/en/products/services/cert.html (https://new.siemens.com/global/en/products/services/cert.html)

1.2 Introduction to 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.

Log in to TIA Cloud Services, click "TIA Portal Cloud" tile, different options of TIA Portal Cloud related to versions are displayed.

You can see which version of TIA Portal Cloud and software packages are installed by clicking on the required tile. Updates to the packages that are available at the time of deployment are installed automatically.

Term definition

Instance: TIA Portal Cloud instance that is displayed in a browser window (referred to below as "instance").

Notes on software packages

WinCC Unified Runtime

- A browser is required for runtime or simulation of a WinCC Unified project. The recommended browser for this is Google Chromium. A current version of Google Chromium is pre-installed in the TIA Portal Cloud environment.

SIMIT:

- SIMIT manuals and application examples are available in Siemens Industry Online Support under the search term "SIMATIC SIMIT Simulation Platform".

TIA Portal Cloud supports the following additional functionalities

GSDML

TIA Portal Cloud consist of a dedicated folder structure for GSDML files in the TIA Cloud Storage application. When you launch the virtual machine (VM) and open a project that contains GSDML files, the files are automatically installed during the project's opening process.

If you reopen a project, the installation of GSDML files will not occur again for the files that are already installed. This prevents redundant installations and ensures efficient usage of the GSDML functionality within the TIA Portal Cloud.

TIA Portal Add-Ins

TIA Portal Cloud provides an AddIn folder structure within the TIA Cloud Storage application. You must upload the necessary AddIn files to the respective TIA variant subfolder in the AddIn folder of the TIA Cloud Storage application.

When files are added to the TIA Cloud Storage location, they are automatically synchronized with the virtual machine (VM) from the TIA Cloud Storage. Once you open the TIA Portal in project view, they can see all the AddIn files listed under the AddIn task bar, specifically under the Corporate AddIns section.

1.3 Versions of TIA Portal Cloud

Trial

The free trial version is limited to 21 days. During this time, the instance is automatically terminated after a maximum of 1 hour. You will receive a message before it ends. You need to log on to the TIA Cloud Services again after this and start a new instance.

When the trial version is started for the first time, you need to activate it. Afterwards, the label of the button will change and you can see in addition how many remaining days you have to use the trial version.

In this variant, you can terminate the instance using the "Terminate" button respectively.

Note

If you accidentally close the instance, you can restart it within 20 minutes without losing data. Once this time has timed out, a new instance is started during a restart.

Pay-per-use (usage-based billing)

Requirements: You have purchased the product in the Siemens Industry Mall under "Digital Offerings" or you have been granted usage rights.

It is billed per started hour.

Monthly subscription

Requirements: You have purchased the product in the Siemens Industry Mall under "Digital Offerings".

You pay a monthly fee starting from the first day of the contractual period.

Annual subscription

Requirements: You have purchased the product in the Siemens Industry Mall under "Digital Offerings".

You pay an early fee starting from the first day of the contractual period.

Note

Paid subscriptions

An instance can be active for a maximum of **12** hours, after 12 hours, the instance will enter the hibernate mode. If you do not operate your active instance for some time (idle time), it will move to hibernate mode after 60 minutes. You will receive a message 10 minutes before hibernation. To avoid data loss, back up your data in good time.

In respective subscription variants, you can terminate or hibernate the instance using the "Terminate" or "Hibernate" button respectively.

General notes on all versions

- The addition/modification of files are synchronized automatically.
- When a network error occurs, a message is displayed. You can look up detailed information on this in the section "Problem solving and troubleshooting".

- In paid subscriptions, an active instance that remains idle is automatically hibernated after 60 minutes. A notification is sent 10 minutes before the timeout, after which the same instance continues.
- While using the instance, you cannot log off from the TIA Cloud Services. If you do this, the browser window closes.
  The Trial variant is an exception; this is automatically timed out after 20 minutes (or after the runtime has elapsed).
- If you are working with different TIA Portal versions, make sure that the TIA Portal projects have a unique name. Otherwise, you may cause errors when synchronizing data to the TIA Cloud Storage and your projects may become unusable.

1.4 Licenses

No additional licenses are required. However, there are differences between the individual versions in the handling of the instances.

Pay per use / Monthly subscription / Annual subscription / Trial

In the Pay per Use, Monthly, Annual and Trial subscription, the instances have an internal connection to the license server. This means that the software packages in the instance use the licenses on this license server.

The license servers cannot be reached by the user.

1.5 Basics of working with TIA Portal Cloud

Installed operating system

The installation of MS Windows in the instance does not include all Windows features. Please note the following restrictions:

- No administrator rights are available. This means that you can only work with the programs that are already installed and cannot install any software and/or hardware on the instance.
- All features that require administrator rights in the TIA Portal cannot currently be used.
- For security reasons, access to the Internet from the instance is not possible.
- You can only terminate / hibernate / stop the instance. In the trial variant, the instance can only be terminated.

TIA Portal settings

Product-specific settings that you make in the TIA Portal are sorted in the TIA Cloud Storage (under "TIA / _internals / Settings / <Product name>") and are always available to you. However, there is no need to make changes to these files, as these can affect the performance of the installed products.

Touch screen

The instance is touchscreen capable.

Online help for the installed products

If you call up the online help for the individual products, it can happen that individual topics cannot be called up, because they are linked to the internet. In these cases, you receive an error message, because internet access is not possible via the instance.

Sending logs

To send logs to Customer Support (e.g. in the event of a problem with TIA Portal or an option package or software package in the instance), you have to synchronize the files and then make them accessible to Customer Support on the TIA Cloud Storage.

Logs which are not saved in the project and therefore are not automatically synchronized, must be copied into the D:\Automation folder.

Always enter the date, time and your account name so Customer Support can identify your data.

FAQs

FAQs on TIA Portal Cloud are available under FAQ (https://support.industry.siemens.com/cs/products?search=TIA%20Portal%20cloud&dtp=Faq&mfn=ps&o=DefaultRankingDesc&lc=en-WW).

System requirements

2

TIA Portal Cloud is a browser-based application, which means that there are no restrictions in relation to operating systems, guest operating systems or virtualization platforms.

Supported browsers

The following browsers are supported:

- Google Chrome V72.0 or higher
- Chromium V71.0 or higher
- Mozilla Firefox V59.0 or higher
- Safari V11.1 or higher
- Microsoft Edge V17.0 or higher

We do not guarantee that TIA Cloud Services and TIA Portal Cloud will run with any other browsers (use at your own risk) or it is incompatible and leads to an error message.

Internet speed

To work efficiently with TIA Portal Cloud, you need an Internet speed of at least 3.2 Mbps. 10 Mbps or higher is recommended.

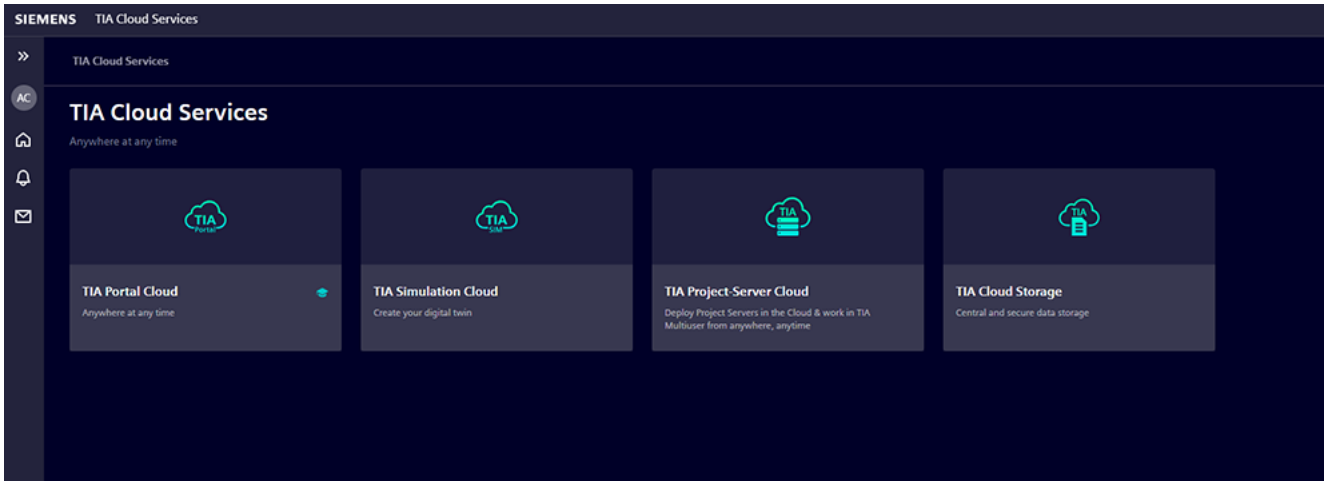
Starting TIA Portal Cloud

3

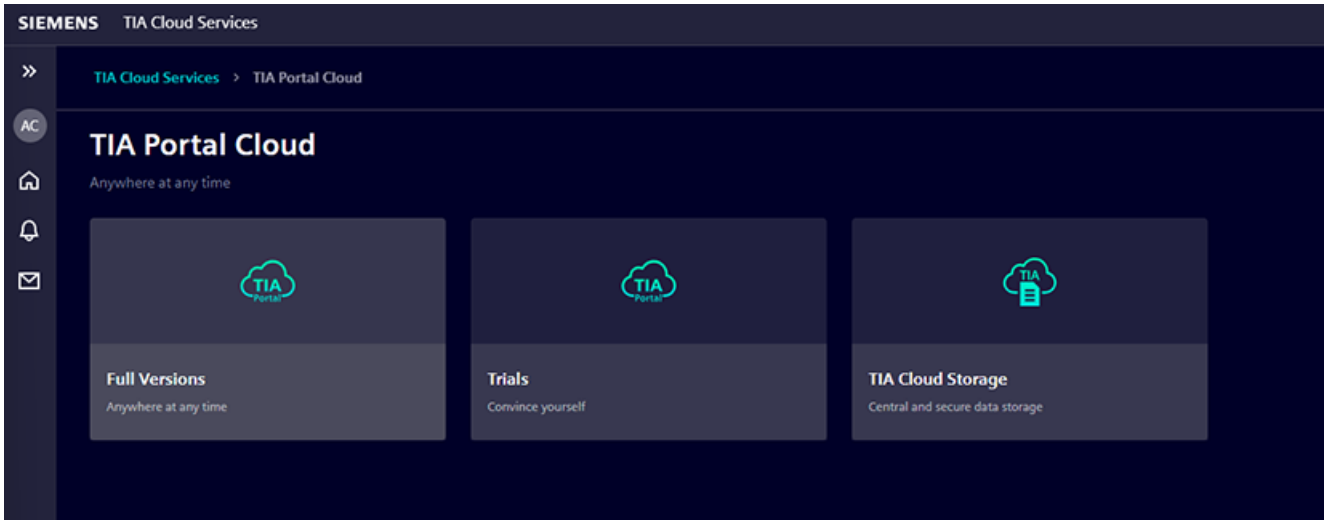
Procedure

To launch TIA Portal Cloud or TIA Simulation Cloud, follow these steps:

1. Start the TIA Cloud Services or the Digital Offering Store and log on.
   TIA Cloud Services page open.



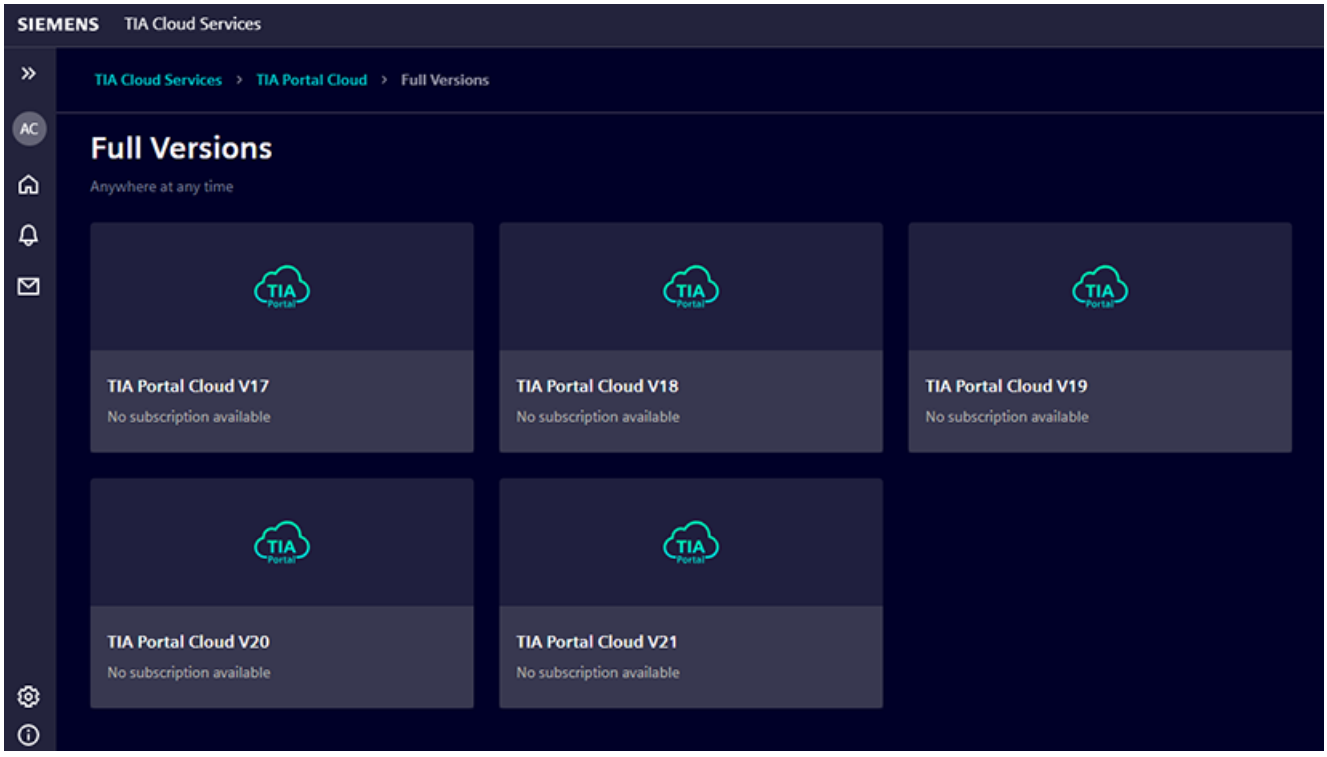
2. Click the TIA Portal Cloud tile, the TIA Portal Cloud page opens.



The following information is displayed on the TIA Portal Cloud page.

- TIA Cloud Storage is the central and secured storage for project files and folders.
- Full Versions consists of all the versions to which you have subscribed. These versions provide full access to the functionalities of the TIA Portal Cloud.
- Trials consists of various trial versions of TIA Portal Cloud. These trial versions allow you to try the software before purchase.

3. Click the Full Versions folder to see the different versions within the selected folder.



On each versions of the TIA Portal Cloud tile, the status of that particular version is displayed:

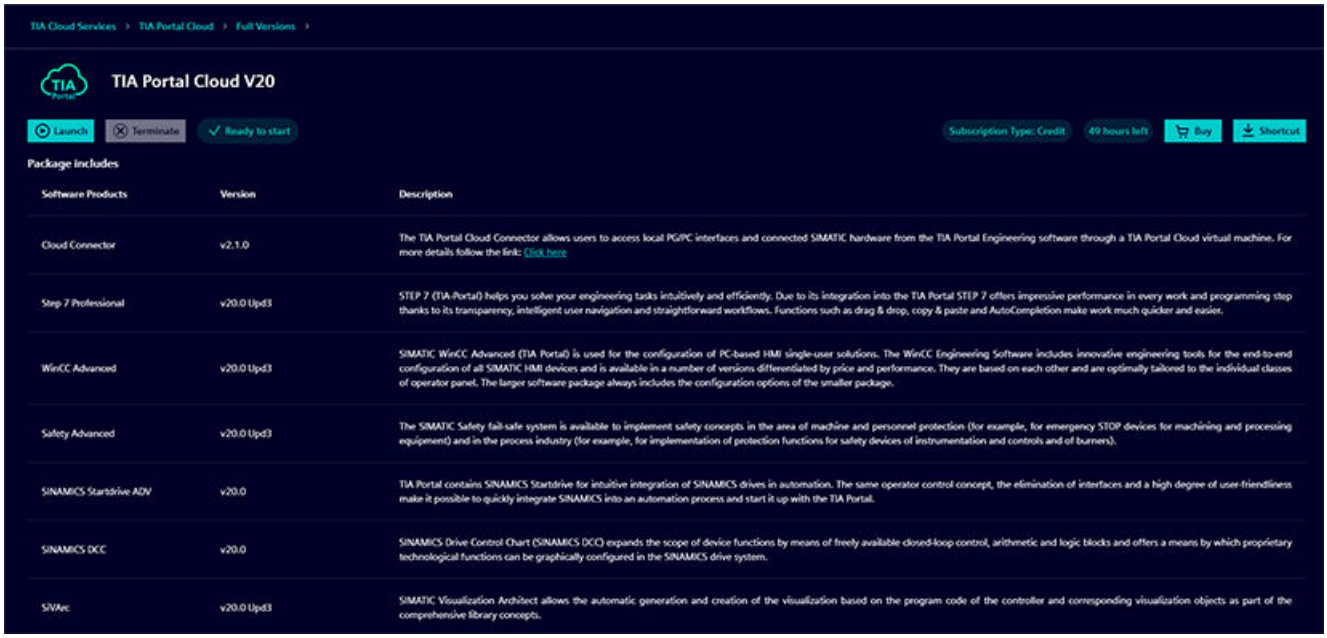
- In hibernation: this status represents the VM is in hibernation.
- Running: this status represents the VM is running.
- Ready to start: this status represents this VM is ready to launch.

Note

Under TIA Simulation cloud folder, 3D Simulation variants support the Stop mode.

You can launch the VM from this page by clicking the icon. Similarly, you can terminate the VM by clicking the icon.

4. Click the required TIA Portal Cloud tile. The corresponding TIA Portal Cloud launch page opens, displaying detailed information about the software packages.



The following information is displayed on the launch page:

- Launch: using this button you can launch TIA Portal Cloud.
- Terminate: using this button you can terminate TIA Portal Cloud.
- Status: displays the status of the selected TIA Portal Cloud.
- Subscription type: displays the subscribed package.
- Buy: using this button you can buy TIA Portal Cloud subscription.
- Shortcut: using the shortcut button you can download the particular version TIA Portal Cloud to your local PC. Next time when you want to use TIA Portal Cloud, you can directly use from the local PC.

5. Click "Launch" to start the TIA Portal Cloud.

TIA Portal Cloud will open in a separate window.

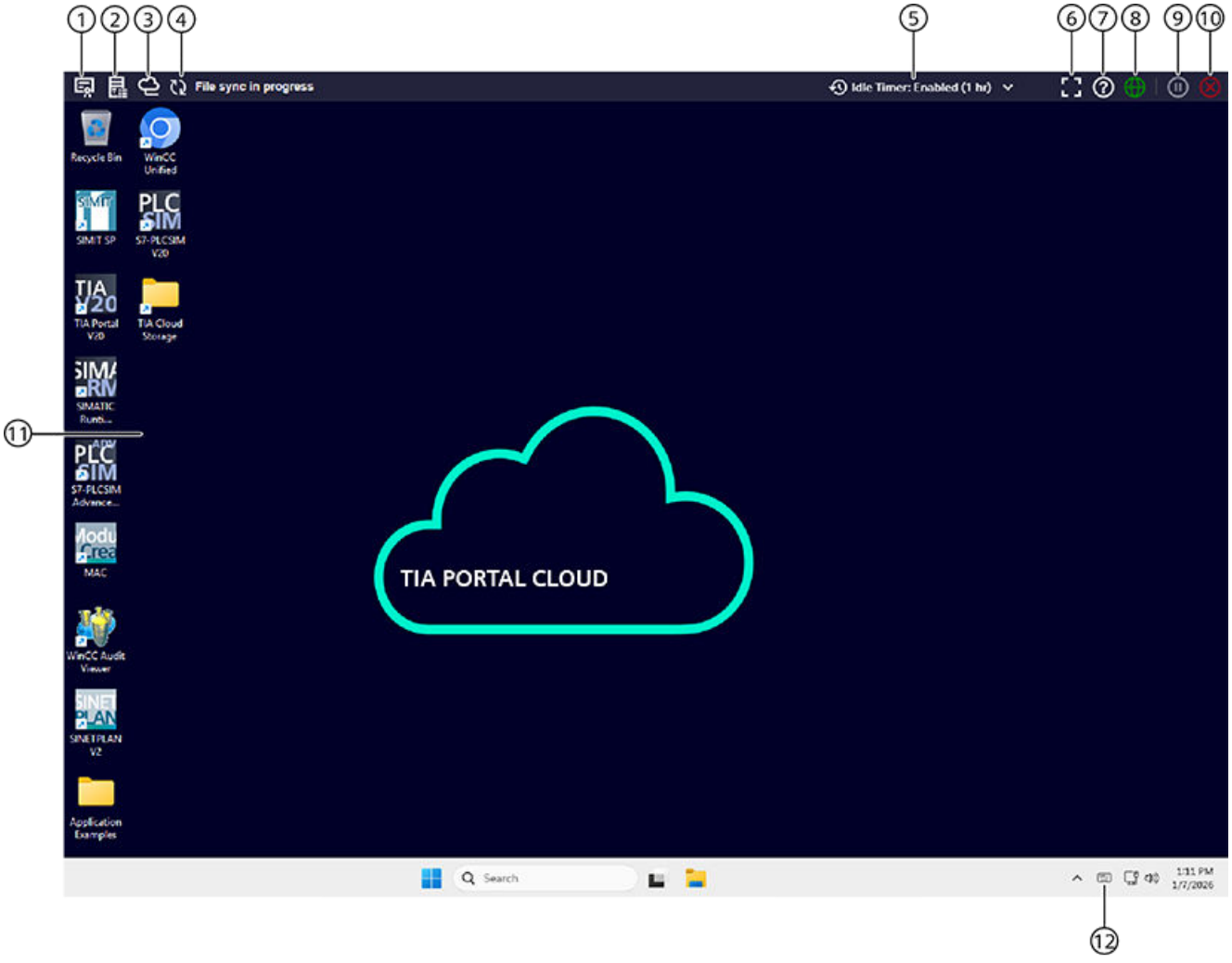
Using an instance

4

4.1 User instance

Elements of the user interface

The user interface looks like this (example):



1 - "Request registration token" button (only in the variants subject to charge)

2 - "List of user devices" button (only in the variants subject to charge)

3 - Online connection status

- Green: Online
- Grey: Offline

4 - File sync in progress (Automatic file synchronization happens between TIA Portal Cloud Storage and instance and vice versa)

5 - Idle Timer: Enabled (1 hr) (Available only for paid subscriptions)

Note

The Idle Timer feature is enabled by default. After 1 hour of inactivity, the instance will hibernate, stop, or terminate (only for trial variant). Users have the option to disable this feature if preferred, but only in paid subscriptions.

6 - "Full screen" button.

Note

Once you click the "Full screen" button, it will take a few seconds to render the instance on a full-screen mode.

7 - Display of the manual and the information window for TIA Portal Cloud.

8 - Internet connection status

- Green: The connection is active.
- Grey: The connection has been lost.

When you hover over the icon, you can see approximately how long you have been using the instance.

9 - Button for hibernating the instance (Only in the variants subject to charge).

10 - Button for terminating the instance.

11 - Display of installed TIA Portal and option packages.

12 - On-screen keyboard.

Note

- If you set a zoom factor > 100%, problems can occur in the operation. In this case, you will receive a note prompting you to adjust the zoom factor accordingly.
- If you change the default font of your Internet browser, display problems such as overlapping buttons can occur.

Special features of keyboard operation in TIA Portal Cloud

Not all keyboard shortcuts can be used in the instance. In such cases, use the on-screen keyboard available in the task bar.

4.2 Using an instance

After you log in, the instances created for you are displayed. Click the desired tile (e.g. "TIA Portal Cloud V19") and then click "Launch TIA Portal Cloud V19 " button.

Procedure

After the instance is started, you will see the most important products on the desktop and can start them with a double-click. You might have to accept the terms of use when starting an option or software package for the first time.

The "?" symbol is displayed in the taskbar on the right. Via this button, you can open the help (manual) and view information on the product version and copyright.

Note

Note the following:

- Access to the Internet from the instance is not possible.
- No software or hardware can be installed on the instance.

Supported languages

TIA Portal Cloud supports the following languages:

- English

The instance is opened in English irrespecitve of the language set in the TIA Cloud Services. The keyboard is set to "English" by default.

Note

Note the following:

- The first time it is started, TIA Portal is launched in the language of the instance and the default settings are used. Changes to the settings in TIA Portal are saved and used again the next time it is started. If you start the instance in a different language the next time, however, TIA Portal still opens in the language used last. You need to explicitly change the language in TIA Portal.

Full-screen mode

To switch on full-screen mode, click the respective button in the tool bar on the upper right. Pressing the button again switches the full-screen mode off again.

Note

Once you click the "Full screen" button, it will take a few seconds to render the instance on a full-screen mode.

4.3 Hibernate / Stop Instance

TIA Portal Cloud supports the hibernation / stopping of VM. After every 12 hours, the VM will enter the hibernate / stop mode. You will receive a message 15 minutes before it hibernates / stops. If you want to use the VM, you must relaunch it using the "Launch" button. After relaunch, you can resume your work from where you left off.

When your Virtual Machine is switched to hibernate / stop mode while TIA Portal is connected online, all the online connections are suspended.

Once VM wakes up from hibernate / stop instance mode:

- The online connections are not automatically restored.
- Sometimes you may observe data loss or interruption of program execution of the connected devices.

To prevent data loss and program interruption, it is advisable to either keep the TIA Portal offline during hibernate / stop mode or close the TIA Portal instance when the VM wakes up from hibernate / stop instance mode.

Note

- Hibernate instance mode is applicable only to paid versions and 2D Simulation versions.
- Stop instance mode is applicable only to 3D Simulation versions.
- Relaunching of stop instance mode gurantees the recovery of saved data only.

Below are the different ways your instance switches to hibernate / stop mode:

VM is idle for 50 minutes

If your VM remains idle for 50 minutes, a notification will appear on your screen with a timer stating "your VM will hibernate / stop in 10 minutes". If you do not use the VM within 10 minutes, your VM will automatically enter the hibernate / stop instance mode.

VM browser is closed

Suppose you are working on a VM, and you close the browser. In this scenario, if you relaunch the VM within 20 minutes, you can continue to use the same VM. If you do not relaunch the VM within 20 minutes, VM will enter the hibernate / stop instance mode.

Hibernating / Stopping the VM manually

You can also move your VM to hibernate instance mode manually. Click the icon on your instance page to move your VM to hibernate mode.

You can also move your VM to stop instance mode manually. Click the icon on your instance page to move your VM to stop mode.

Continuously active for 12 hours

If you are using a VM continuously for 12 hours, your VM will move to the hibernate / stop mode. You will receive a notification 15 minutes before hibernation / stop happens, stating "your VM will move to hibernate / stop instance mode in 15 minutes". After completion of 12 hours, the VM moves to hibernate / stop instance mode.

You must relaunch the VM to continue using.

If the VM moves to hibernate / stop instance mode by any of the above ways, it will stay in the hibernate / stop instance mode for 20 days. After 20 days, the VM will be terminated. Here are the various notifications you will receive during these 20 days:

- On the 10th day of hibernation / stop, you will receive an email notification saying "Your VM will terminate in 10 days".
- On the 18th day of hibernation / stop, you will receive another email notification saying "Your VM will terminate in two days".

If you relaunch the VM within 20 days, you can continue using it. If you do not relaunch the VM within 20 days, your VM will be terminated.

Deployment of new version

After the deployment of new version, if you are still using an outdated VM, you will receive a toolbar notification saying "An updated version of the instance is available. Please terminate and relaunch".

If you want to use an outdated VM, you can use it for 20 days. Here are the various notifications you will receive during these 20 days:

- On the 10th day of using an outdated VM, you will receive a notification saying "Updated variant available, instance will be terminated automatically in 10 days. Please ensure to save your important data".
- On the 18th day of using an outdated VM, you will receive another notification saying "Updated variant available, instance will be terminated automatically in 2 days. Please ensure to save your important data".

If you continue to use the outdated VM for 20 days, after completion of 20 days, your VM Will be terminated.

Older version of the VM is incompatible

In most of the cases, whenever there is a new deployment, the outdated version of the VM works properly for 20 days. In rare case the outdated version VM may not work due to the incompatibility of the older version VM.

In this case you will receive an email 10 days before the deployment of new version, saying "Incompatible update planned in 10 days. All hibernated / stopped instances will be terminated. Please save your data".

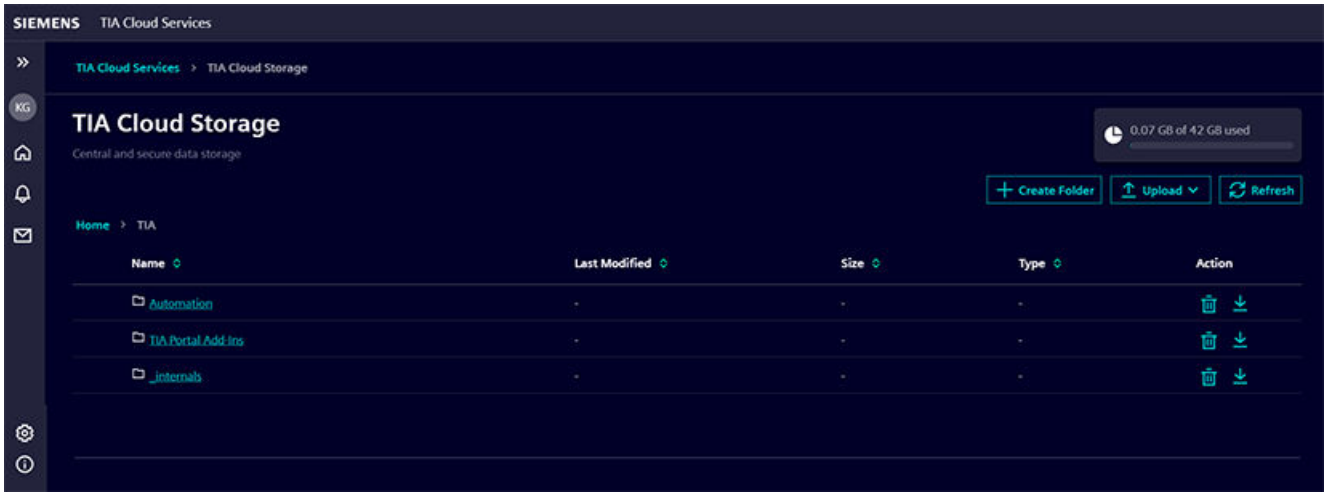
You will receive another email 2 days before the deployment of new version saying "Incompatible update planned in 2 days. All hibernated / stopped instances will be terminated. Please save your data".

4.4 Copying projects/files to the instance

Procedure

To copy projects or files that you need for your work to the instance, follow these steps:

1. Open the TIA Cloud Services and click the "TIA Cloud Storage" tile.
2. In the TIA Cloud Storage, navigate to the folder TIA > Automation. If this folder does not exist, you must create it. **Only the files/folders that are stored here are synchronized with the instance.**
3. Then select "Upload" and choose "Upload Files" or "Upload Folder" from the drop-down.
   If you select "Upload Files", you can select individual files and upload them.
   If you select "Upload folder", you can select the entire folder and upload.



The uploaded files and folders are automatically synchronized in the instance.

Result

After synchronization, the files/folders are available under D:\Automation or click on "TIA Cloud Storage" on the desktop to open the specified folder.

4.5 Copying projects/files from the instance to your local PC

Procedure

To copy projects or files that you have edited back to your PC, follow these steps:

1. Click "TIA Cloud Storage" tile in the TIA Cloud Services.
2. Navigate to the TIA folder.
3. Select the files/folders that you want to download and select Download under "Action".

Result

The selected files/folders are saved in the "Downloads" folder on your PC.

Copy and pasting the text from the instance to local PC

You can copy and paste the text from the instance to the local PC and vice versa.

Note: In the Instance, a confirmation dialog box appears which you will have to confirm to be able to copy and paste the text.

See also

Files Synchronization (Page 23)

4.6 Files Synchronization

The synchronization of files are done automatically after starting and before exiting a TIA Portal cloud instance.

Overview

The synchronized files are stored in D:\Automation and in other subfolders (e.g. User_Projects).

In the TIA Cloud Storage of the TIA Cloud Services, you can find the files and folders under TIA/Automation. The product-specific settings are stored under TIA / _internals / Settings / <Product name>.

Note

Note the following:

- The product-specific settings are automatically synchronized when the instance is started. Do not ever change them outside the TIA Portal! To use your own, already existing settings in the instance, copy them to the TIA Cloud Storage (folder "TIA / _internals / Settings / <Product name> ").
- Loss of data can occur if the synchronization of large projects is started too late, especially shortly before the instance ends. It is therefore advisable to save the files and your work progress at suitable intervals.
- Make sure that your projects have unique names, especially when you are working with different instances. If you are using projects with the same name in different instances, data is overwritten when synchronizing to the TIA Cloud Storage. This results in faulty projects and/or crashing of the TIA Portal.

Accessing PLCs in a company network 5

5.1 Accessing PLCs in a company network

Using TIA Portal Cloud Connector, TIA Portal Cloud 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 company network (private cloud). TIA Portal Cloud provides a safe endpoint for communication with user devices.

Requirements

- Access to SIMATIC hardware in a company network is only possible in the paid variants of TIA Portal Cloud. You can find a list of the approved TIA Portal hardware products in Siemens Industry Online Support under the following entry ID:
  https://support.industry.siemens.com/cs/ww/en/view/109780755
- The current version (> V1.1 SP4) of the optional software TIA Portal Cloud Connector is installed and configured in your company network.
  If you have not installed this version, you can download it on the Premium Portal page in the TIA Portal Cloud tile. The download link can be found at the bottom of the page.

Note

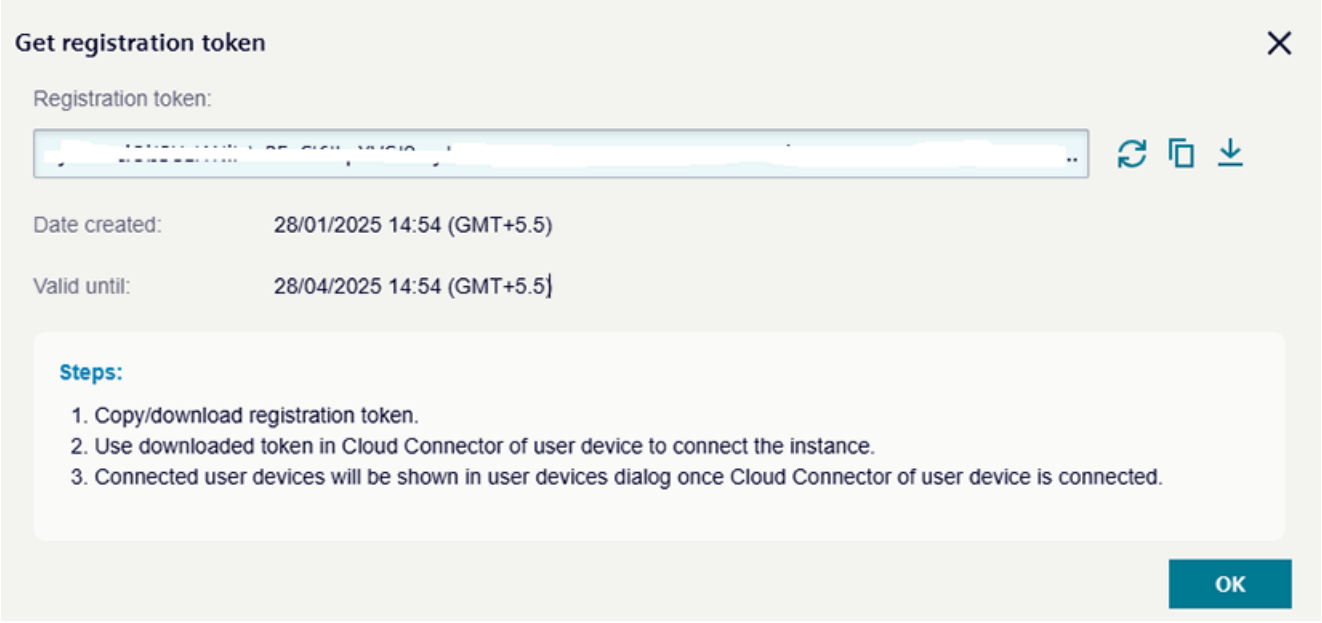
- This documentation does not cover the general configuration and mode of operation of the TIA Portal Cloud Connector; please refer to the product documentation for the necessary information.
  Only the steps necessary for working with TIA Portal Cloud are described below.
- The TIA Portal Cloud Connector 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.

For troubleshooting TIA Portal Cloud Connector, refer Troubleshooting TIA Portal Cloud Connector. (Page 35)

5.2 Request registration token and log in user device

Registration token

Click the "Request registration token" button in your instance to receive a secure registration token. This user-specific token connects the TIA Portal Cloud Connector with the TIA Portal Cloud endpoint. It is valid for a limited number of days. The creation and expiry dates are shown in the dialog. After the validity has expired, you receive a message and you can no longer register with the old token. You then need to request a new token. A maximum of 32 user devices can be registered with a valid token.



Follow these steps:

1. Click the "" button to request a new token. As soon as the token has been created, it is displayed in the "Registration token" field.
2. Click the "" or "" button to copy the token or download it to a .txt file.

Note

Note that each click of the "" button generates a new token and the active token becomes invalid for all disconnected user devices. This means that you have to register these user devices again. You should therefore only use this button after the validity of an existing token has expired.

Registering a user device

Prerequisites

Install Cloud Connector application from the “Download Cloud Connector” button available in Tia portal cloud (Need administrator rights for installation).

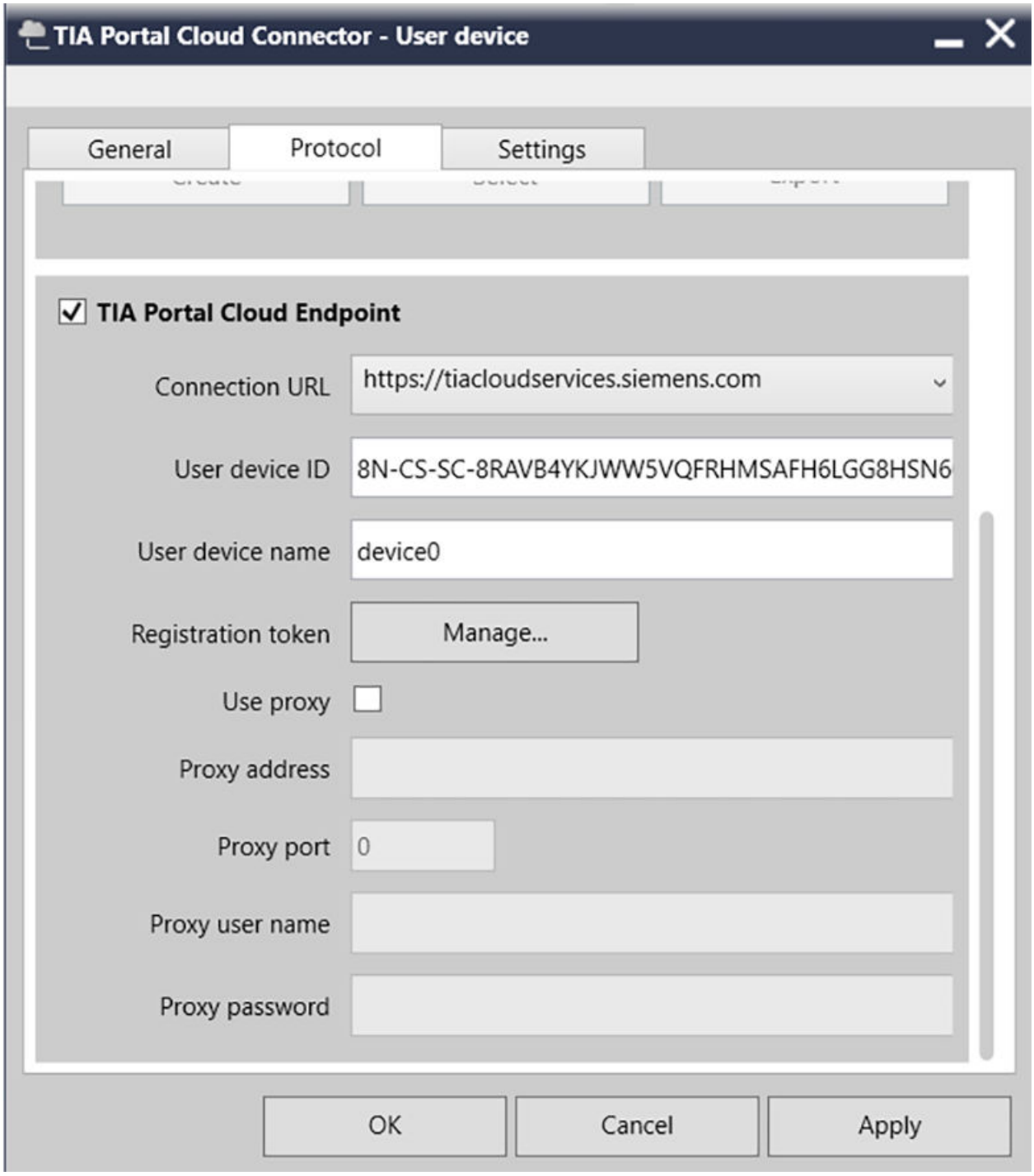
Follow the steps to make the necessary infrastructure changes on the PC where cloud connector is installed:

- Internet access must be available for the PC at system level. To establish a successful communication below protocols must be allowed in the network:
  Communication protocols “HTTPS” with port number “443 ” allowed in the network.
- PC must have two NIC (Network Interface Card) cards. (One NIC must be connected to the plant devices and another NIC card must be connected to the internet)

Follow these steps to register user devices:

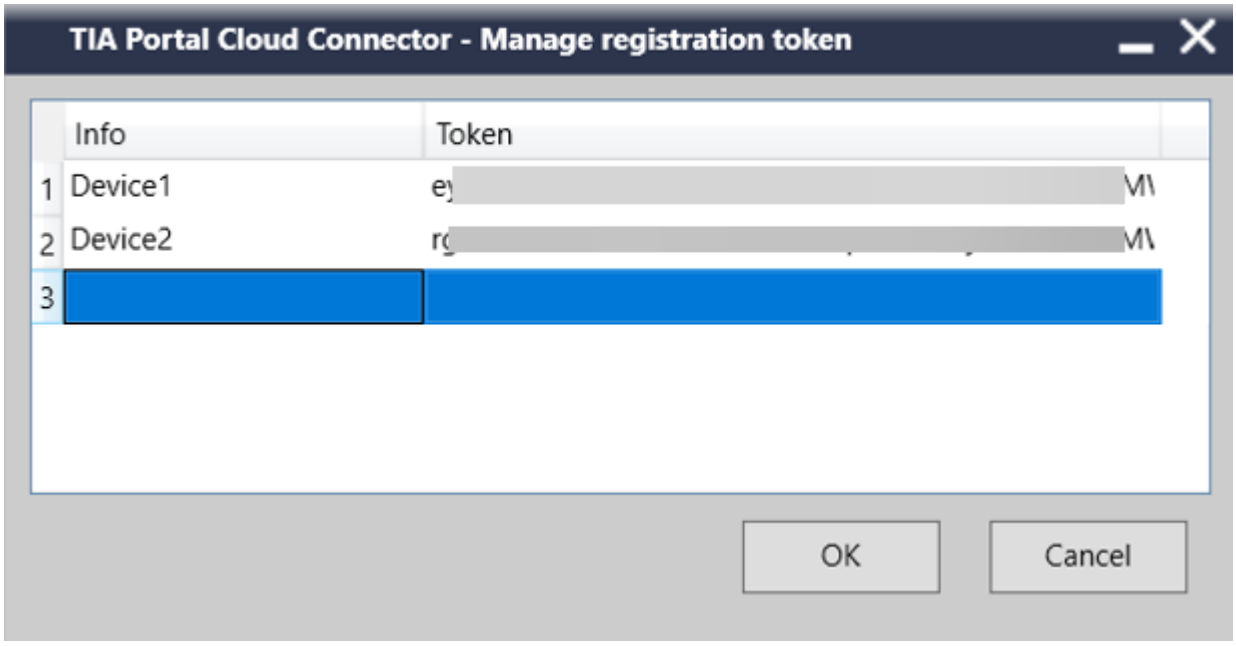
1. Open the TIA Portal Cloud Connector in the company network.
2. Set the "User device" communication role in the "General" tab.

3. Switch to the "Protocol" tab.



4. Enable the "TIA Portal Cloud Endpoint" entry.

5. Enter a name for the user device and click the "Manage..." button in the "Registration token" line.



6. Insert the previously copied/downloaded token in the "Token" column.
   Proceed in the same way for other user devices by sharing the registration token.
   Multiple tokens can be entered on separate lines for different users. The column "Info" is optional; here e.g. the name of the token user can be entered.
   A maximum of 100 user devices can be registered with a valid token.

   Note

   Enter unique and easily identifiable names for the user devices. The names can contain a maximum of 50 alphanumeric characters, including hyphen (-) or underscore (_).

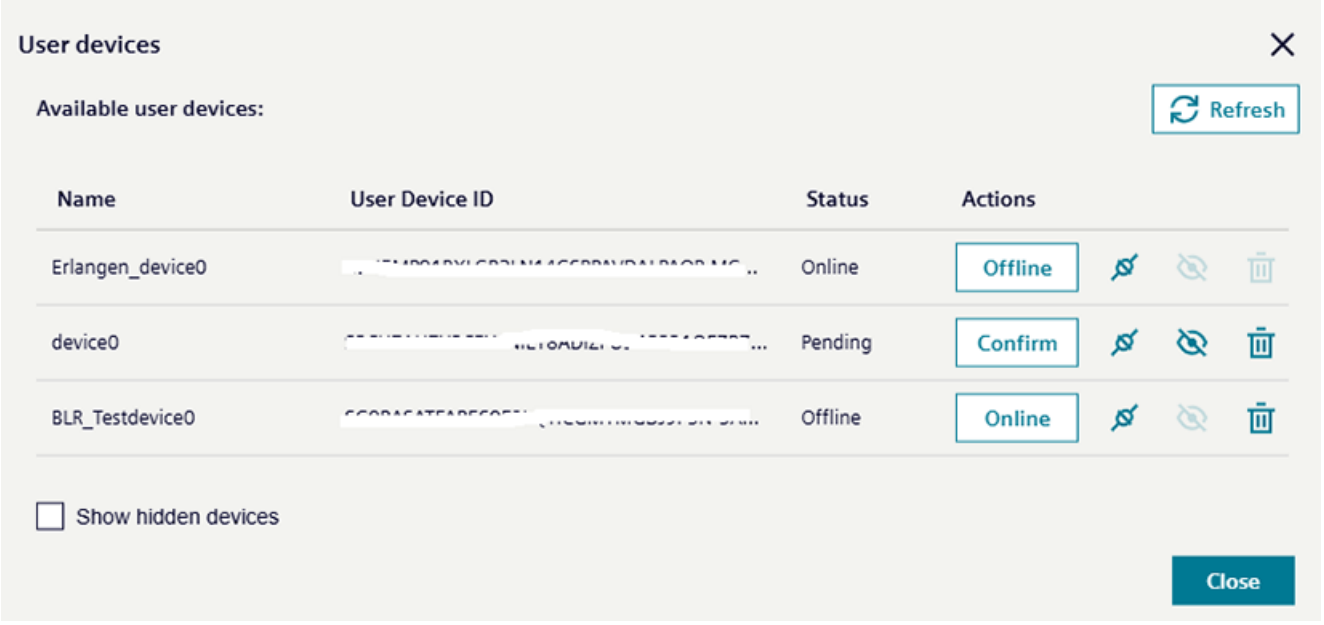
7. If you are using a proxy server, select the "Use Proxy" check box and enter the necessary information in the boxes below.
8. Click the "Apply" button to confirm your settings.
9. Switch to the "General" tab and click the "Enable communication" button. You can then close the TIA Portal Cloud Connector.

5.3 Working with user devices

After you have registered the desired devices in TIA Portal Cloud Connector, you can work with them in TIA Portal Cloud.

To establish communication with the desired user device, follow these steps:

1. Click the "User devices" button in your instance.
   You will see an example illustration of the dialog below:



Important note

Within a company network, a user device can only be accessed by **one** TIA Portal Cloud user. It is therefore advisable to set the user device to the "Offline" status if you no longer need it so that it is available to other users.

A maximum of 32 user devices can be registered with a valid token. After this number has been exceeded, you receive a message and you can deregister a device to register a new device, if desired.

Column	Meaning
ID	Unique ID of the user device
Name	Name of the user device that you defined in the TIA Portal Cloud Connector.
Status	Status of the user device
Actions (interactive buttons)	
Confirm	To accept a newly registered device, click the "Confirm" button. The user device is set to the "Offline" status. As soon as a device is in the "Online" status, other users who use this functionality will see the "In use" status in their instances.
Online	Click the "Online" button to enable the device. If a device is already online and another device is to be switched to online, you must confirm a message that the connected device should be deactivated; this sets it to the "Offline" status.

Column	Meaning
	Click the "Offline" button to disable the device.
	Note: If a device is already in the "Online" status in another instance, the "InUse" status is displayed in this instance.
	The user device is connected to the TIA Portal Cloud endpoint. Clicking this button will disconnect the user device.
	The connection to the user device is timed out. For devices to which the connection has been timed out, note that this connection needs to be established again in the TIA Portal Cloud Connector.
	To delete a user device, click on the icon. Devices that have the "Online" status cannot be deleted. To be able to work with a user device that has been deleted again, you need to register it again in the TIA Portal Cloud Connector.
	If you have a large number of registered user devices, it may make sense to hide infrequently used devices so that they are not always shown in the list of available devices. To do this, click on the icon in the row of the user device to be hidden. To make it visible again, click the grayed out icon again. To hide the column completely, disable the option "Show hidden devices".

Problem solving and troubleshooting

6

Network error

The status indicator in the user interface provides information about the current connection status.

When a network error occurs, a message is displayed. Try to rectify the fault and then close the instance and restart the session.

The instance is terminated in the event of permanent network disruptions.

If a network disruption occurs while an online function (e.g. upload, download) is in progress, then the TIA Portal may become unresponsive. In these cases, it is recommended to restart the TIA Portal and go online again.

Cloud security

The TIAP Cloud application needs a certain Internet bandwidth to work correctly. Programs that set up a secure connection to company networks sometimes cannot provide the required bandwidth. Therefore, if you determine network problems, you should exit such programs and connect directly to the TIAP Cloud.

Emptying the cache

To improve the performance and to ensure that you are exploiting the full range of functions of TIA Portal Cloud, you should regularly empty the browser cache. To do so, with the browser open, use the shortcut CTRL+F5 before you start the instance.

Display problems

Depending on the browser you are using (e.g. Google Chrome), texts may not be displayed completely or are illegible. In the browser, go to "Settings > Advanced > System" and disable the setting "Use hardware acceleration when available". The display will be correct after restarting the browser.

SIMIT version

When SIMIT is used, the project files will be stored on drive **C:** in the folder where the SIMIT version is installed in the instance. In order to synchronize the files to TIA Cloud Storage, you have to copy the project files manually from drive **C:** to drive **D:**\Automation\... or vice versa if projects are synchronized from the TIA Cloud Storage to the instance. The current project data will not be available if this manual copy operation is not executed.

Troubleshooting TIA Portal Cloud Connector 7

7.1 Introduction

Purpose

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

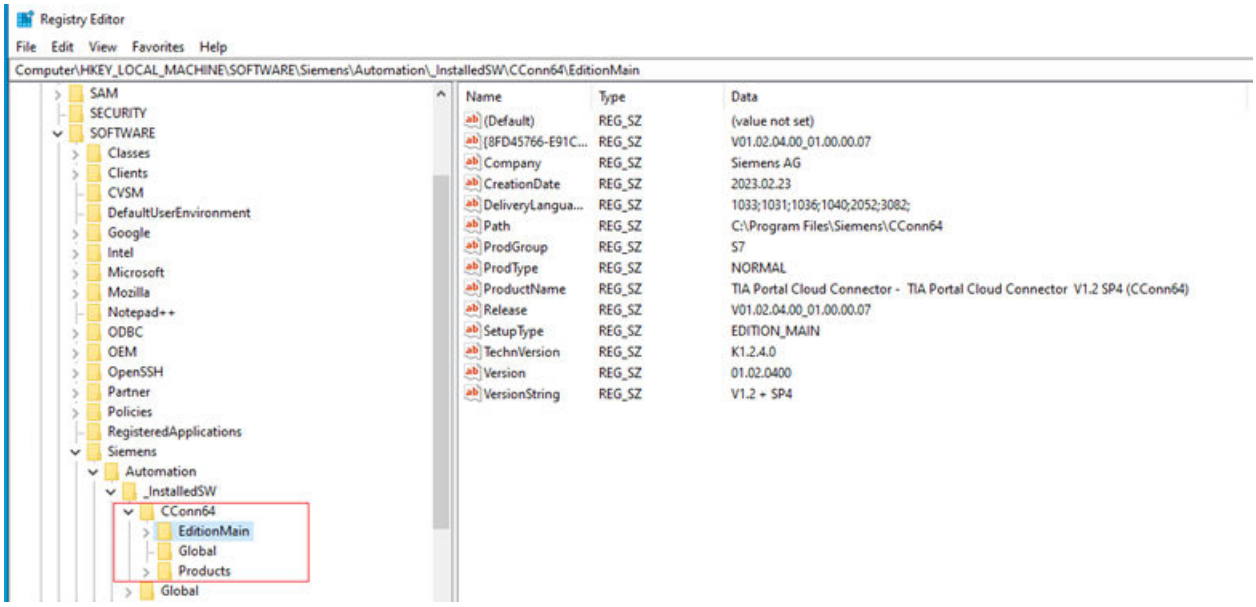
Basic Information

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

7.2 Registry

For installing Cloud Connector refer Installing the TIA Portal Cloud Connector. After successful installation of Cloud Connector check the registry in the below location:

HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Automation_InstalledSW\CConn64

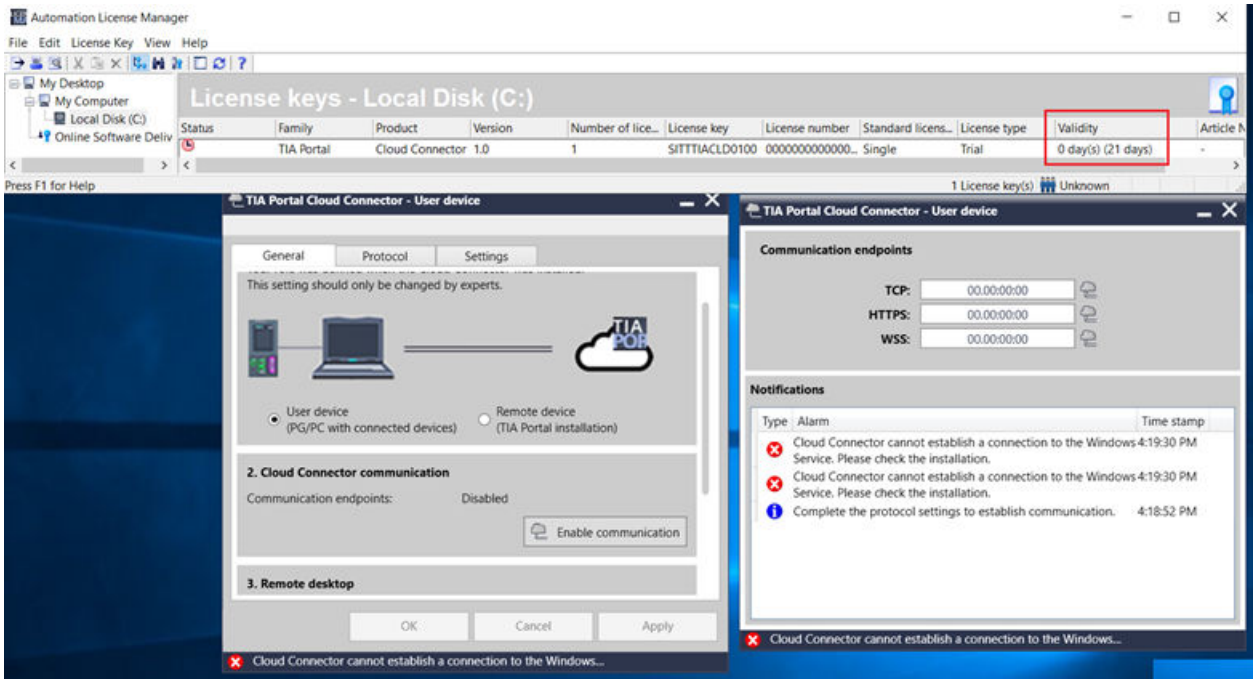


If the registry is not similar to the image shown above, then the registry is not properly updated.

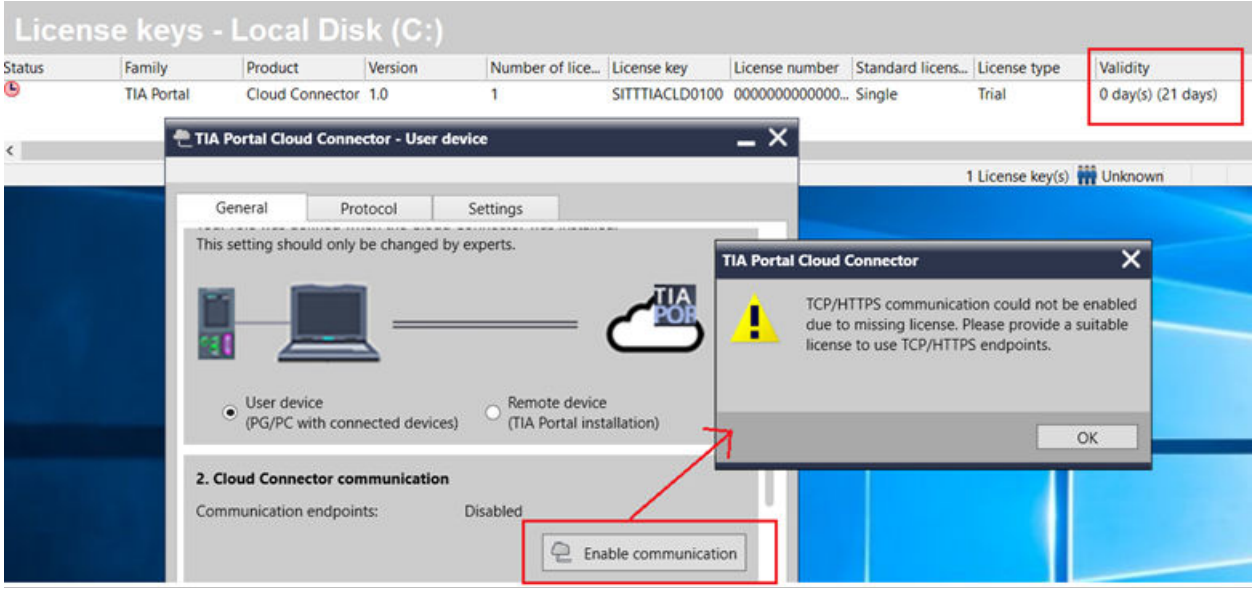
If the registry is not properly updated, uninstall Cloud Connector from Add or remove programs, and reinstall it either via TIA Portal media or standalone Cloud Connector.

7.3 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.



7.4 How to launch Cloud Connector

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

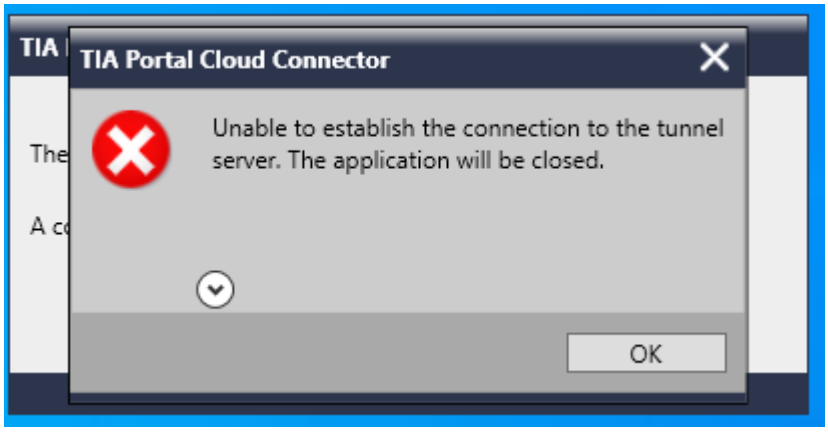
- From Windows Start menu > “TIA Portal Cloud Connector".
- Right click the "TIA Portal Cloud Connector" from the system tray.

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.

7.5 Configuration

7.5.1 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.

7.5.2 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.

7.5.3 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".

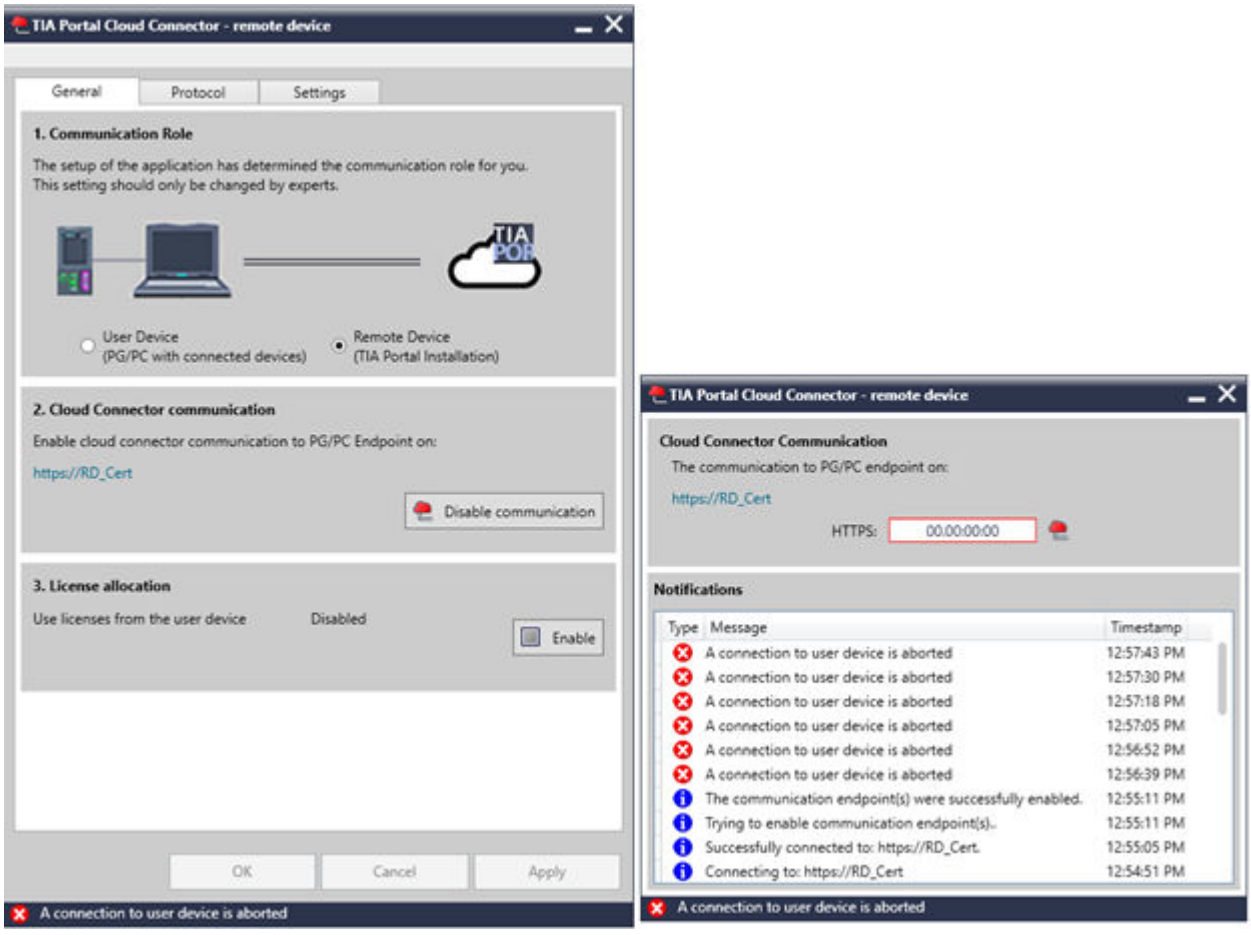
3. Once Remote device certificate is created, go to User device "Settings" > "User authentication", and import Remote device certificate.
4. Once User device and Remote device certificates are applied, go to the "General" tab and click "Enable Communication".
   Once User device and Remote device "Enable 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.

7.5.4 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).

7.5.5 Registration Token handling

Note

- Generate and copy registration token from TIA Cloud Services (https://tiacloudservices.siemens.com (https://tiacloudservices.siemens.com)), using the “Get registration token” dialog.
- Generated registration token is applicable only for that TIA Cloud Services 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.

7.5.6 TIA Cloud Services

TIA Cloud Services "User devices" dialog contains newly established User device communication device information with "Pending" status.

Once you click "Confirm", TIA Cloud instance 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 TIA Cloud instance 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 TIA Cloud instance 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.

7.5.7 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".

7.5.8 PLC online connectivity issue

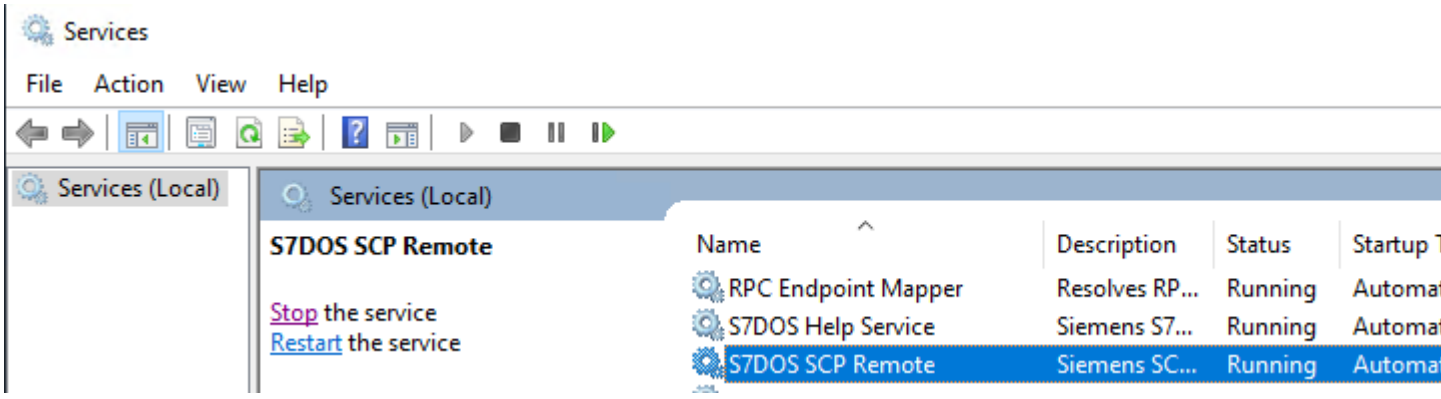
For TIA Portal Cloud endpoint, If enable communication is not successful after installation / upgrade, it might be due to internet access not available at the system level. Ensure to enable the internet access at system level.

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

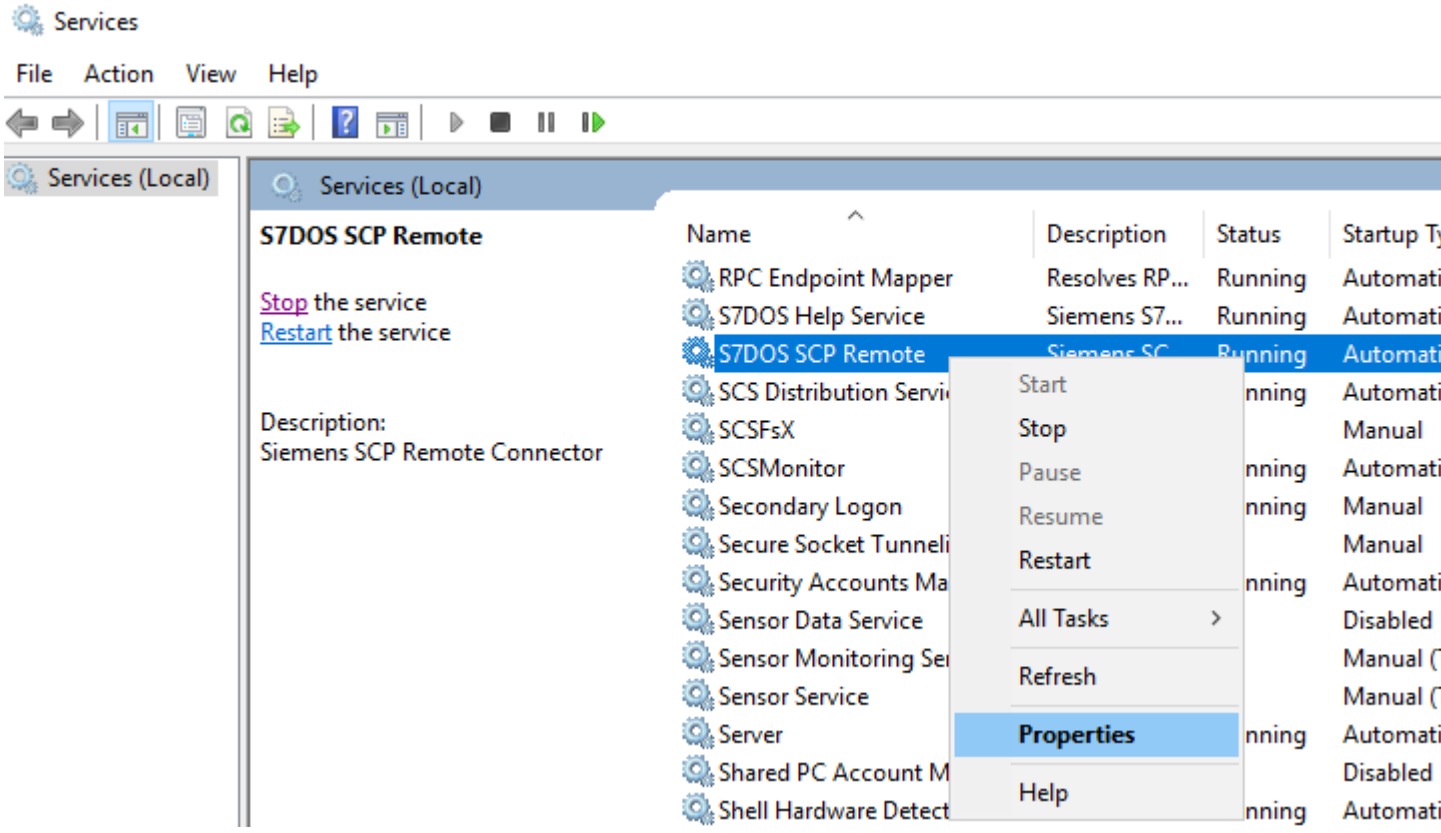
Follow below steps to run Cloud Connector on Local user Account:

1. Provide write/read registry access for local user account for the following registry path: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Shared Tools\S7DOS64
2. Open Services.msc from Command Prompt.

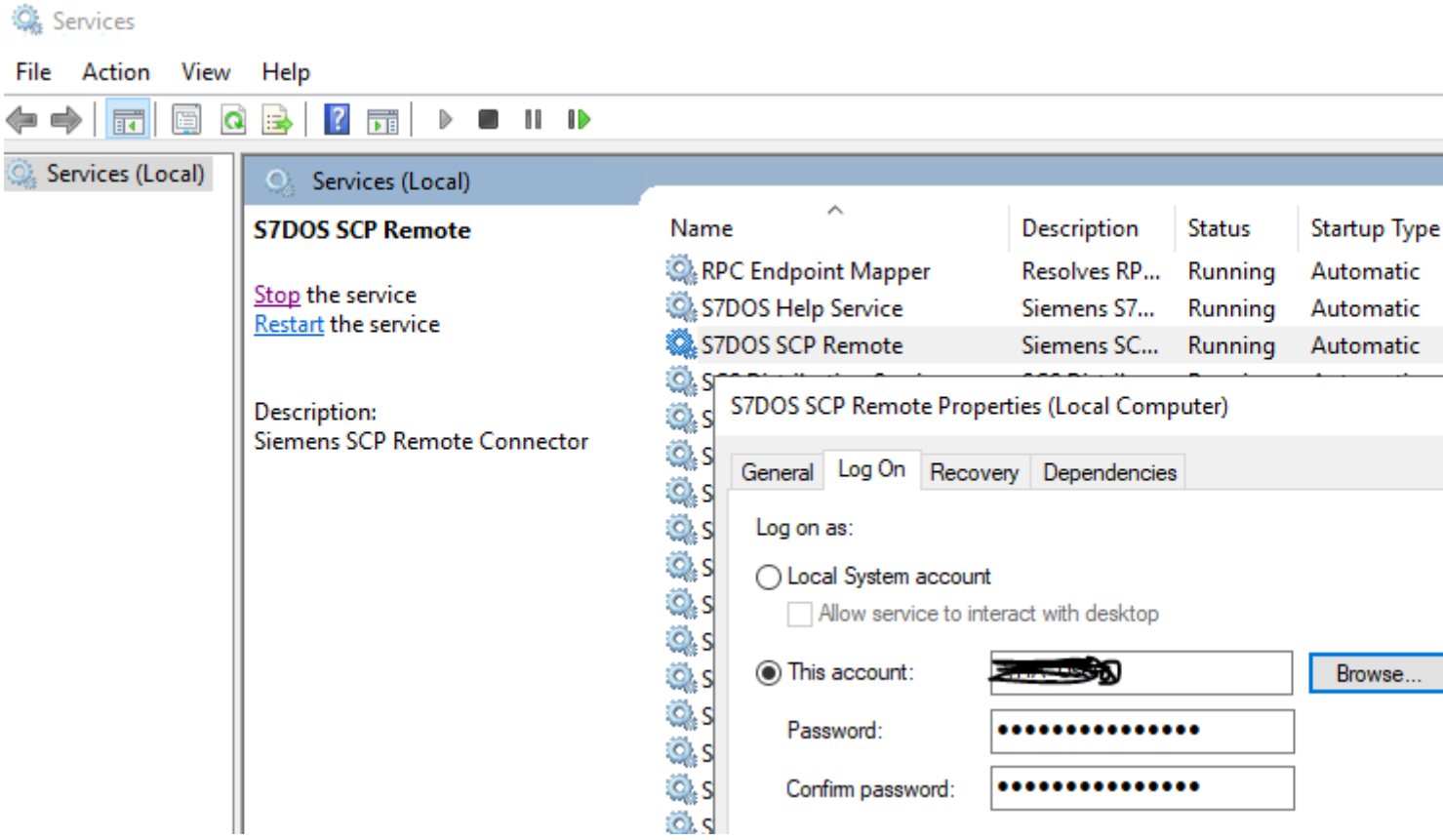
3. Search for the service S7DOS SCP Remote, and stop the service if it is in running state.



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.