SIEMENS

Installation

Programming and Operating Manual

11/2025

Notes on the installation 1

Parallel installation 2

Licensing 3

System requirements for installation 4

Overview of processes and services of TIA Portal components 5

Using Security Logging 6

Installation log 7

Checking the integrity 8

Performing the installation 9

Displaying the installed software 10

Modifying or updating installed products 11

Repairing installed products 12

Starting to uninstall 13

Installing updates and support packages 14

Installing support packages automatically 15

Installing and uninstalling TIA Project Server 16

Installing and uninstalling TIA Administrator 17

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

Ⓟ 10/2025 Subject to change

Copyright © Siemens 2025.
All rights reserved

Table of contents

1 Notes on the installation 7

2 Parallel installation 9

3 Licensing 11

3.1 Notes on licenses 11

3.2 Licensing STEP 7 and WinCC 12

3.3 Licensing of WinCC Unified options 24
3.3.1 Basis 24
3.3.2 Logging 24
3.3.3 Parameter sets 26
3.3.4 Process diagnostics 27
3.3.5 Client 27
3.3.6 Reporting 29
3.3.7 Runtime Openness 30
3.3.7.1 Unified GraphQL 30
3.3.8 Unified Collaboration 30
3.3.9 Audit 31
3.3.10 Unified Data Hub 32
3.3.11 Redundancy 34

3.4 Licensing of Plant Intelligence options 34
3.4.1 Calendar 34
3.4.2 Performance Insight 35
3.4.3 Sequence 36
3.4.4 Line Coordination 37

3.5 Handling licenses and license keys 38

3.6 Upgrade of licenses 42

3.7 Licensing of HMI devices 43

3.8 Licensing WinCC Runtime on PC-based HMI devices 43

3.9 Licensing WinCC Runtime Asian 44

3.10 STEP 7 without license for PC-CP 45

4 System requirements for installation 47

4.1 Notes on the system requirements 47

4.2 General software and hardware requirements 48

4.3 Use of high-resolution monitors 50

4.4 Product-specific special characteristics 51
4.4.1 Installing WinCC 51
4.4.2 Uninstalling WinCC Unified 51
4.4.3 Installation of WinCC Runtime Unified 52
4.4.4 Installation of WinCC Runtime Professional 58

4.4.5 Removing an SQL instance ... 60
5 Overview of processes and services of TIA Portal components ... 61
6 Using Security Logging ... 69
6.1 Security Logging in the TIA Portal ... 69
6.2 Activating and deactivating Security Logging ... 69
6.3 Overview of events ... 70
6.4 Displaying and managing events ... 78
7 Installation log ... 81
8 Checking the integrity ... 83
8.1 Basic information about the integrity check ... 83
8.2 Performing an integrity check ... 83
8.3 Error cases during the integrity check ... 85
9 Performing the installation ... 87
10 Displaying the installed software ... 93
11 Modifying or updating installed products ... 95
12 Repairing installed products ... 97
13 Starting to uninstall ... 99
14 Installing updates and support packages ... 101
14.1 Checking availability of updates and support packages and installing them ... 101
14.2 Working with a company-internal server ... 104
14.2.1 Properties and advantage of a corporate server ... 104
14.2.2 Configuring a corporate server for updates ... 105
14.2.3 Distributing updates to different areas ... 124
14.2.4 Providing updates on a corporate server ... 125
15 Installing support packages automatically ... 127
15.1 Installing support packages automatically ... 127
15.2 Return values from the installation process ... 128
15.3 Log file ... 129
16 Installing and uninstalling TIA Project Server ... 131
16.1 Notes on installing the project server ... 131
16.2 Installing a project server ... 133
16.3 Uninstalling a project server ... 135
17 Installing and uninstalling TIA Administrator ... 137
17.1 Introduction to the TIA Administrator ... 137
17.2 System requirements ... 137
17.3 Installing TIA Administrator ... 137

17.4 Uninstalling TIA Administrator 138
17.5 Starting and exiting TIA Administrator 139
17.5.1 Starting the TIA Administrator locally 139
17.5.2 Starting the TIA Administrator with remote access 139
17.5.3 Closing the TIA Administrator 140

Notes on the installation

1

Content

Information that could not be included in the online help and important information about product characteristics.

Installation in a virtual environment (private cloud)

You can find instructions on how to install TIA Portal in a virtual environment (private cloud) on the installation data medium in the directory "Documents\Readme\<language directory>". You can open the PDF document "TIAPortalCloudConnectorHowTo<language ID>.pdf" here.

Automatic installation

A description of automated installation is available on the product DVD in the directory "Documents\Readme\<Language directory>".

Use of the same versions of TIA Portal products during installation

When installing different TIA Portal products, make sure that you use the same versions of service packs and updates for the installation. For example, if you have installed SP1 for STEP 7 V13, you must also install SP1 for WinCC V13. The service packs and updates must be installed for all products at the same time. Do not start TIA Portal until all products have been upgraded.

You can download the service packs from the Internet under Siemens Industry online support (https://support.industry.siemens.com/cs/de/en/).

Target directory of the installation

Do not use any UNICODE characters (for example, Chinese characters) in the installation path.

The installation path cannot be changed after installing one of the TIA Portal products.

Security settings for the installation of WinCC

When you install WinCC, security settings are changed in your operating system. These security settings are listed during the installation.

You must confirm the changes to the security settings.

If you make changes to your operating system after installing it, the security settings can be changed by installing TIA Portal.

You can restore the security settings by installing TIA Portal as follows:
"Start > All Programs > Siemens Automation > Security Controller > Restore settings".

Use of antivirus programs

During the installation, read and write access to already installed files is necessary. Some antivirus programs block this access. Therefore, configure your antivirus program for the installation of TIA Portal so that access to these files is possible.

FAQs on TIA Portal

FAQs on TIA Portal are available under FAQs (http://support.automation.siemens.com/WW/view/en/28919804/133000).

Parallel installation

2

Parallel installation of WinCC V21 and other SIMATIC HMI products

Parallel installation of WinCC V21 with versions of WinCC flexible earlier than WinCC flexible 2008 SP5 is not permitted.

Parallel installation of WinCC V21 Comfort/Advanced with versions of WinCC earlier than WinCC V7.3 is not permitted.

The parallel installation of WinCC Professional (ES and RT) with WinCC V7.x, WinCC V8.x is not permitted.

The parallel installation of WinCC Unified (ES and RT) with WinCC V7.x and WinCC V8.x is not permitted.

Parallel installation of WinCC Professional with a previous version.

Parallel installation of WinCC Professional V21 (ES or RT) with an earlier version of WinCC Professional (ES or RT) is not permitted.

Alternatively you can install a different WinCC Professional version in a virtual environment.

Installation of WinCC Unified RT and WinCC RT Professional on one device

You have installed the Runtime for WinCC Unified and WinCC Professional on one device. To avoid conflicts between WinCC Unified RT and WinCC RT Professional, you must change the default port numbers for WebUX and WebNavigator.

To change the port numbers, follow these steps:

1. Change the port number of the WebUX web page for HTTPS communication from 443 to 4443. This eliminates the conflict with the Unified Runtime default port number.
2. Change the port number for internal communication between WebUX WebRH(Node Server) and GfxRTS from 1345 to a different number.
3. Change the port number of the WebNavigator web page for HTTPS communication from 443 to 4430. This eliminates the conflict with the Unified Runtime default port number.
4. Create a firewall rule for incoming data traffic to allow TCP traffic with the new WebUX port number 4443.
5. Set firewall rules for incoming data traffic to allow TCP traffic with the new WebNavigator port number 4430.
6. Make sure the firewall rules are securely created.
7. Check that WebUX and WebNavigator websites are accessible with their respective new port numbers.

Note

Note that the following ports are currently used by WinCC Unified RT:

- Port 443 is used for Unified RT.
- Port 1345 is used for internal communication between the Unified Node and Unified GfxRTS.

Licensing

3

3.1 Notes on licenses

Availability of licenses

The licenses for the products of the TIA Portal are shipped on an installation data medium or via online software delivery (OSD).

Before you uninstall the TIA Portal, you must transfer and back up the licenses still required. Use the Automation License Manager for this purpose.

Provision of the Automation License Manager

The Automation License Manager is supplied on the installation data medium and is transferred automatically during the installation process.

If you uninstall the TIA Portal, the Automation License Manager remains installed on your system.

Working with the Automation License Manager

The Automation License Manager is a product of Siemens AG, which is used for handling license keys (technical representatives of licenses).

Software products that require license keys for operation, such as the TIA Portal, register the need for license keys automatically with the Automation License Manager . If the Automation License Manager finds a valid license key for this software, the software can be used according to the license usage terms associated with this license key.

Note

For additional information on how to manage your licenses with the Automation License Manager , refer to the documentation supplied with the Automation License Manager .

See also

Notes on the system requirements (Page 47)

Performing the installation (Page 87)

Displaying the installed software (Page 93)

Modifying or updating installed products (Page 95)

Repairing installed products (Page 97)

Starting to uninstall (Page 99)
Installation log (Page 81)

3.2 Licensing STEP 7 and WinCC

Introduction

You require a License Key to license the following STEP 7 editions:

- STEP 7 Basic
- STEP 7 Professional

You can install the corresponding License Key for STEP 7 using the Automation License Manager after the installation has been completed.

There are other licenses available for the optional packages of STEP 7. You can get detailed information in the documentation of the corresponding option package.

You can transfer the corresponding license keys for STEP 7 and STEP 7 options after the installation with the Automation License Manager.

For licensing the following editions in WinCC, you need a License Key:

- WinCC Engineering System
- WinCC Runtime
- Options for WinCC Engineering System
- Options for WinCC Runtime system

You transfer licenses for WinCC and the WinCC add-ons after installation with the Automation License Manager.

Note

The licensee also recognizes that the software (SW) from the Microsoft Corporation or subsidiaries contains licensed software. The licensee hereby agrees to be bound by and comply with the terms of the attached license agreement between Microsoft SQL Server and End User.

Licenses

The following licenses with the corresponding License Keys are available:

- STEP 7 Basic
- STEP 7 Professional
- STEP 7 Professional Combo
- WinCC Basic
- WinCC Comfort
- WinCC Comfort Combo

- WinCC Advanced
- WinCC Advanced Combo
- WinCC Professional
- WinCC Professional Combo
- WinCC Unified Basic Engineering
- WinCC Unified Comfort Engineering
- WinCC Unified PC Engineering
- WinCC RT Advanced
- WinCC RT Professional
- Optionen für WinCC RT Professional
- WinCC Professional Runtime Client
- WinCC Unified PC Runtime
- Optionen für WinCC Unified PC Runtime

Usage possibilities of licenses and devices

The following table shows which devices you can use with which license:

Existing license	**Devices that can be used**						
	Unified Devices			Classic Devices			
	WinCC Unified PC	Comfort Panels	Basic Panels	RT Professional	RT Advanced	Comfort Panels	Basic Panels
WinCC Unified Basic ES	No	No	Yes	No	No	No	Yes
WinCC Unified Comfort ES	No	Yes	Yes	No	No	Yes	Yes
WinCC Unified PC 10k ES	Yes (10k*)	Yes	Yes	No	Yes	Yes	Yes
WinCC Unified PC 100k ES	Yes (100k*)	Yes	Yes	Yes	Yes	Yes	Yes
WinCC Unified PC max ES	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WinCC Basic	No	No	Yes	No	No	No	Yes
WinCC Comfort	No	Yes	Yes	No	No	Yes	Yes
WinCC Advanced	Yes (10k*)	Yes	Yes	No	Yes	Yes	Yes
WinCC Professional 512	Yes (10k*)	Yes	Yes	Yes (512*)	Yes	Yes	Yes
WinCC Professional 4096	Yes (10k*)	Yes	Yes	Yes (4096*)	Yes	Yes	Yes
WinCC Professional max	Yes (100k*)	Yes	Yes	Yes	Yes	Yes	Yes

* Maximum possible number of PowerTags

Validity of license keys for older versions of STEP 7

With a valid License Key for V21.x of STEP 7 Professional and STEP 7 Professional Combo, you can also operate older versions of STEP 7 without restrictions. The following table provides more detailed information about this:

Edition	License	Valid for
STEP 7 Basic V21.x	STEP 7 Basic	• STEP 7 Basic V21.x • STEP 7 Basic V20.x • STEP 7 Basic V19.x • STEP 7 Basic V18.x • STEP 7 Basic V17.x • STEP 7 Basic V16.x • STEP 7 Basic V15.x • STEP 7 Basic V14.x • STEP 7 Basic V13.x • STEP 7 Basic V12.x • STEP 7 Basic V11.x
STEP 7 Professional V21.x	STEP 7 Professional	• STEP 7 Professional V21.x • STEP 7 Professional V20.x • STEP 7 Professional V19.x • STEP 7 Professional V18.x • STEP 7 Professional V17.x • STEP 7 Professional V16.x • STEP 7 Professional V15.x • STEP 7 Professional V14.x • STEP 7 Professional V13.x • STEP 7 Professional V12.x • STEP 7 Professional V11.x • STEP 7 Basic V21.x • STEP 7 Basic V20.x • STEP 7 Basic V19.x • STEP 7 Basic V18.x • STEP 7 Basic V17.x • STEP 7 Basic V16.x • STEP 7 Basic V15.x • STEP 7 Basic V14.x • STEP 7 Basic V13.x • STEP 7 Basic V12.x • STEP 7 Basic V11.x

Edition	License	Valid for
STEP 7 Professional V21.x	STEP 7 Professional Combo	• STEP 7 Professional V21.x • STEP 7 Professional V20.x • STEP 7 Professional V19.x • STEP 7 Professional V18.x • STEP 7 Professional V17.x • STEP 7 Professional V16.x • STEP 7 Professional V15.x • STEP 7 Professional V14.x • STEP 7 Professional V13.x • STEP 7 Professional V12.x • STEP 7 Professional V11.x • STEP 7 Basic V21.x • STEP 7 Basic V20.x • STEP 7 Basic V19.x • STEP 7 Basic V18.x • STEP 7 Basic V17.x • STEP 7 Basic V16.x • STEP 7 Basic V15.x • STEP 7 Basic V14.x • STEP 7 Basic V13.x • STEP 7 Basic V12.x • STEP 7 Basic V11.x • STEP 7 V5.7 • STEP 7 V5.6 • STEP 7 V5.5 • STEP 7 V5.4 • STEP 7 Professional 2021 • STEP 7 Professional 2017 • STEP 7 Professional 2010

Validity of license keys for older versions of WinCC

With a valid License Key for WinCC V21.x, you can also operate older versions of WinCC without restrictions.

You can find more detailed information in the following table:

WinCC Engineering System

Edition	License	Valid for
WinCC Basic V21.x	WinCC Basic	• WinCC Basic V21.x • WinCC Basic V20.x • WinCC Basic V19.x • WinCC Basic V18.x • WinCC Basic V17.x • WinCC Basic V16.x • WinCC Basic V15.x • WinCC Basic V14.x • WinCC Basic V13.x • WinCC Basic V12.x • WinCC Basic V11.x • WinCC Unified Basic V21.x • WinCC Unified Basic V20.x • WinCC Unified Basic V19.x • WinCC Unified Basic V18.x

Edition	License	Valid for
WinCC Comfort/Advanced V21.x	WinCC Comfort	• WinCC Basic, Comfort V21.x • WinCC Basic, Comfort V20.x • WinCC Basic, Comfort V19.x • WinCC Basic, Comfort V18.x • WinCC Basic, Comfort V17.x • WinCC Basic, Comfort V16.x • WinCC Basic, Comfort V15.x • WinCC Basic, Comfort V14.x • WinCC Basic, Comfort V13.x • WinCC Basic, Comfort V12.x • WinCC Basic, Comfort V11.x • WinCC Unified Basic, Comfort V21.x • WinCC Unified Basic, Comfort V20.x • WinCC Unified Basic, Comfort V19.x • WinCC Unified Basic, Comfort V18.x • WinCC Unified Comfort V17.x • WinCC Unified Comfort V16.x
	WinCC Comfort Combo	• WinCC flexible Compact, Standard >= 2005 • WinCC Basic, Comfort V21.x • WinCC Basic, Comfort V20.x • WinCC Basic, Comfort V19.x • WinCC Basic, Comfort V18.x • WinCC Basic, Comfort V17.x • WinCC Basic, Comfort V16.x • WinCC Basic, Comfort V15.x • WinCC Basic, Comfort V14.x • WinCC Basic, Comfort V13.x • WinCC Basic, Comfort V12.x • WinCC Basic, Comfort V11.x • WinCC Unified Basic, Comfort V21.x • WinCC Unified Basic, Comfort V20.x • WinCC Unified Basic, Comfort V19.x • WinCC Unified Basic, Comfort V18.x • WinCC Unified Comfort V17.x • WinCC Unified Comfort V16.x
	WinCC Advanced	• WinCC Basic, Comfort, Advanced V21.x • WinCC Basic, Comfort, Advanced V20.x • WinCC Basic, Comfort, Advanced V19.x • WinCC Basic, Comfort, Advanced V18.x • WinCC Basic, Comfort, Advanced V17.x • WinCC Basic, Comfort, Advanced V16.x

Edition	License	Valid for
		• WinCC Basic, Comfort, Advanced V15.x • WinCC Basic, Comfort, Advanced V14.x • WinCC Basic, Comfort, Advanced V13.x • WinCC Basic, Comfort, Advanced V12.x • WinCC Basic, Comfort, Advanced V11.x • WinCC Unified Basic, Comfort, Unified PC V21.x • WinCC Unified Basic, Comfort, Unified PC V20.x • WinCC Unified Basic, Comfort, Unified PC V19.x • WinCC Unified Basic, Comfort, Unified PC V18.x • WinCC Unified Comfort, Unified PC V17.x • WinCC Unified Comfort, Unified PC V16.x
	WinCC Advanced Combo	• WinCC flexible Compact, Standard, Advanced >= 2005 • WinCC Basic, Comfort, Advanced V21.x • WinCC Basic, Comfort, Advanced V20.x • WinCC Basic, Comfort, Advanced V19.x • WinCC Basic, Comfort, Advanced V18.x • WinCC Basic, Comfort, Advanced V17.x • WinCC Basic, Comfort, Advanced V16.x • WinCC Basic, Comfort, Advanced V15.x • WinCC Basic, Comfort, Advanced V14.x • WinCC Basic, Comfort, Advanced V13.x • WinCC Basic, Comfort, Advanced V12.x • WinCC Basic, Comfort, Advanced V11.x • WinCC Unified Basic, Comfort, Unified PC V21.x • WinCC Unified Basic, Comfort, Unified PC V20.x • WinCC Unified Basic, Comfort, Unified PC V19.x • WinCC Unified Basic, Comfort, Unified PC V18.x • WinCC Unified Comfort, Unified PC V17.x • WinCC Unified Comfort, Unified PC V16.x

Edition	License	Valid for
WinCC Professional V21.x	WinCC Professional (512) WinCC Professional (4096) WinCC Professional (max.)	• WinCC Basic, Comfort, Advanced, Professional V21.x • WinCC Basic, Comfort, Advanced, Professional V20.x • WinCC Basic, Comfort, Advanced, Professional V19.x • WinCC Basic, Comfort, Advanced, Professional V18.x • WinCC Basic, Comfort, Advanced, Professional V17.x • WinCC Basic, Comfort, Advanced, Professional V16.x • WinCC Basic, Comfort, Advanced, Professional V15.x • WinCC Basic, Comfort, Advanced, Professional V14.x • WinCC Basic, Comfort, Advanced, Professional V13.x • WinCC Basic, Comfort, Advanced, Professional V12.x • WinCC Basic, Comfort, Advanced, Professional V11.x • WinCC Unified Basic, Comfort, Unified PC V21.x • WinCC Unified Basic, Comfort, Unified PC V20.x • WinCC Unified Basic, Comfort, Unified PC V19.x • WinCC Unified Basic, Comfort, Unified PC V18.x • WinCC Unified Comfort, Unified PC V17.x • WinCC Unified Comfort, Unified PC V16.x
	WinCC Professional (512) Combo WinCC Professional (4096) Combo WinCC Professional (max.) Combo	• WinCC flexible Compact, Standard, Advanced >= 2008 SP3 • WinCC Basic, Comfort, Advanced, Professional V21.x • WinCC Basic, Comfort, Advanced, Professional V20.x • WinCC Basic, Comfort, Advanced, Professional V19.x • WinCC Basic, Comfort, Advanced, Professional V18.x • WinCC Basic, Comfort, Advanced, Professional V17.x • WinCC Basic, Comfort, Advanced, Professional V16.x • WinCC Basic, Comfort, Advanced, Professional V15.x • WinCC Basic, Comfort, Advanced, Professional V14.x • WinCC Basic, Comfort, Advanced, Professional V13.x • WinCC Basic, Comfort, Advanced, Professional V12.x • WinCC Basic, Comfort, Advanced, Professional V11.x • WinCC Unified Basic, Comfort, Unified PC V21.x • WinCC Unified Basic, Comfort, Unified PC V20.x • WinCC Unified Basic, Comfort, Unified PC V19.x • WinCC Unified Basic, Comfort, Unified PCV18.x • WinCC Unified Comfort, Unified PC V17.x • WinCC Unified Comfort, Unified PC V16.x

Edition	License	Valid for
WinCC Unified Basic V21.x	WinCC Unified Basic ES	• WinCC Basic V21.x • WinCC Basic V20.x • WinCC Basic V19.x • WinCC Basic V18.x • WinCC Unified Basic V21.x • WinCC Unified Basic V20.x • WinCC Unified Basic V19.x • WinCC Unified Basic V18.x
WinCC Unified Comfort V21.x	WinCC Unified Comfort ES	• WinCC Basic, Comfort V21.x • WinCC Basic, Comfort V20.x • WinCC Basic, Comfort V19.x • WinCC Basic, Comfort V18.x • WinCC Basic, Comfort V17.x • WinCC Basic, Comfort V16.x • WinCC Unified Basic, Comfort V21.x • WinCC Unified Basic, Comfort V20.x • WinCC Unified Basic, Comfort V19.x • WinCC Unified Basic, Comfort V18.x • WinCC Unified Comfort V17.x • WinCC Unified Comfort V16.x

Edition	License	Valid for
WinCC Unified PC ES V21.x	WinCC Unified PC (10k) ES	• WinCC Unified Basic, Comfort V21.x • WinCC Basic, Comfort, Advanced V20.x • WinCC Basic, Comfort, Advanced V19.x • WinCC Basic, Comfort, Advanced V18.x • WinCC Basic, Comfort, Advanced V17.x • WinCC Basic, Comfort, Advanced V16.x • WinCC Unified Basic, Comfort, Unified PC V21.x • WinCC Unified Basic, Comfort, Unified PC V20.x • WinCC Unified Basic, Comfort, Unified PC V19.x • WinCC Unified Basic, Comfort, Unified PC V18.x • WinCC Unified Comfort, Unified PC V17.x • WinCC Unified Comfort, Unified PC V16.x
	WinCC Unified PC (100k) ES WinCC Unified PC (max.) ES	• WinCC Basic, Comfort, Advanced, Professional V21.x • WinCC Basic, Comfort, Advanced, Professional V20.x • WinCC Basic, Comfort, Advanced, Professional V19.x • WinCC Basic, Comfort, Advanced, Professional V18.x • WinCC Basic, Comfort, Advanced, Professional V17.x • WinCC Basic, Comfort, Advanced, Professional V16.x • WinCC Unified Basic, Comfort, Unified PC V21.x • WinCC Unified Basic, Comfort, Unified PC V20.x • WinCC Unified Basic, Comfort, Unified PC V19.x • WinCC Unified Basic, Comfort, Unified PC V18.x • WinCC Unified Comfort, Unified PC V17.x • WinCC Unified Comfort, Unified PC V16.x

WinCC Runtime

Edition	License	Valid for
WinCC RT Advanced V17.x	WinCC RT Advanced (16384) WinCC RT Advanced (8192) WinCC RT Advanced (4096) WinCC RT Advanced (2048) WinCC RT Advanced (512) WinCC RT Advanced (128)	• WinCC RT Advanced V17.x • WinCC RT Advanced V16.x • WinCC RT Advanced V15.x • WinCC RT Advanced V14.x • WinCC RT Advanced V13.x • WinCC RT Advanced V12.x • WinCC RT Advanced V11.x
WinCC RT Professional V21.x	WinCC RT Professional (262144) WinCC RT Professional (153600) WinCC RT Professional (102400) WinCC RT Professional (65536) WinCC RT Professional (8192) WinCC RT Professional (4096) WinCC RT Professional (2048) WinCC RT Professional (512) WinCC RT Professional (128) WinCC Client for RT Professional	• WinCC RT Professional V21.x • WinCC RT Professional V20.x • WinCC RT Professional V19.x • WinCC RT Professional V18.x • WinCC RT Professional V17.x • WinCC RT Professional V16.x • WinCC RT Professional V15x • WinCC RT Professional V14.x • WinCC RT Professional V13.x • WinCC RT Professional V12.x • WinCC RT Professional V11.x • WinCC Client for RT Professional V21.x • WinCC Client for RT Professional V20.x • WinCC Client for RT Professional V19.x • WinCC Client for RT Professional V18.x • WinCC Client for RT Professional V17.x • WinCC Client for RT Professional V16.x • WinCC Client for RT Professional V15.x • WinCC Client for RT Professional V14.x • WinCC Client for RT Professional V13.x • WinCC Client for RT Professional V12.x • WinCC Client for RT Professional V11.x
WinCC Unified PC RT V21.x[1]	WinCC Unified PC (150) RT WinCC Unified PC (500) RT WinCC Unified PC (1k) RT WinCC Unified PC (2,5k) RT WinCC Unified PC (5k) RT WinCC Unified PC (10k) RT WinCC Unified PC (50k) RT WinCC Unified PC (100k) RT WinCC Unified PC (max.) RT	• WinCC Unified PC V21.x • WinCC Unified PC V20.x • WinCC Unified PC V19.x • WinCC Unified PC V18.x • WinCC Unified PC V17.x • WinCC Unified PC V16.x

[1] You can find more information under Licensing of WinCC Unified options (Page 24).

Validity of licenses for WinCC options

WinCC options with version-independent license keys can also be used for future versions.

Starting without a valid license key

If you start the TIA Portal without a valid License Key , the system alerts you that you are working in non-licensed mode. You have the one-time option of activating a Trial License. However, this license is valid for a limited period only and expires after 21 days.

When the Trial License expires, the following scenarios can occur:

- TIA Portal has never been licensed on the PC in question:
  - No license-based actions can be performed in the TIA Portal.
- TIA Portal was already licensed on the PC in question:
  - A window requiring acknowledgment presents an alert for non-licensed mode every 10 minutes and for every action requiring a license.

Trial licenses for RT Professional

If you do not have a valid license, the system alerts you that you are working in non-licensed mode.

You have the one-time option of activating a Trial License.

However, this Trial License is valid for a limited period only and expires after 21 days.

- WinCC RT Professional (65536)
- WinCC WebUX Operate (150)
- WinCC DataMonitor (50)
- WinCC WebNavigator (50)

License requirement for simulation In STEP 7

You do not require additional PLCSIM licenses when you use the menu command "Online > Simulation" to start the PLC simulation in STEP 7.

License requirement for simulation In WinCC Runtime

If the following conditions are fulfilled, you also need the appropriate licenses for WinCC Runtime and for licensed options for the simulation:

- Start the simulator with the menu command "Online > Simulation > Start".

If you do not have a valid license, you can activate the simulation for one hour.

Licenses for the TIA Portal Cloud Connector

For working with the TIA Portal Cloud Connector, you need a valid License Key for each device that you specify as "User device" in the TIA Portal Cloud Connector. The License Key is also required if the TIA Portal is installed on this device. A License Key is not required for devices that you are using as "remote device".

See also

Handling licenses and license keys (Page 38)

3.3 Licensing of WinCC Unified options

3.3.1 Basis

Validity of license keys for older versions

SIMATIC licenses are downward compatible. With a newer License Key from WinCC Unified options, older versions can also be operated.

3.3.2 Logging

You have two options for logging your data in WinCC Unified:

- File-based logging
- Database-based logging

File-based logging

Requirement

WinCC Unified Basic Panel:

- For configuration, you need a WinCC Unified Basic ES (Engineering System) license.
- No license is required for logging.

WinCC Unified Comfort Panel:

- For configuration, you need a WinCC Unified Comfort ES (Engineering System) license.
- No license is required for logging.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

WinCC Unified Basic Panel enables file-based logging of 50 logging tags, which are included in each device.

WinCC Unified Comfort Panel enables file-based logging of 5000 logging tags, which are included in each device.

WinCC Unified PC RT enables file-based logging of up to 5000 logging tags in an SQL Lite database. To log a maximum of 5000 logging tags, you need

one or more licenses according to the number of tags to be logged. The table below lists the licenses available for this.

Upgrade

No upgrade license is required for logging when you upgrade the system.

Trial

If you do not have a valid license, you can configure the logging tags in trial mode.

Database-based logging

Database-based logging allows you to log all logging tags up to the high limit in an MS SQL database.

Requirement

WinCC Unified Basic Panel:

- Not available

WinCC Unified Comfort Panel:

- Not available

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

Besides the functionality, database-based logging also includes an MS SQL server. Therefore, you need the "WinCC Unified Database Storage" license.

You also need one or more license(s) according to the number of tags to be logged. The table below lists the licenses available for this.

File-based or database-based licenses

Refer to the following table for the license(s) needed for the number of tags to be logged:

License	Number of logging tags[1]	File-based	Database-based
WinCC Unified PC 100 Logging Tags	100	Yes	Yes
WinCC Unified PC 500 Logging Tags	500	Yes	Yes
WinCC Unified PC 1000 Logging Tags	1000	Yes	Yes

License	Number of logging tags[1]	File-based	Database-based
WinCC Unified PC 5000 Logging Tags	5000	Yes	Yes
WinCC Unified PC 10000 Logging Tags	10000	No	Yes
WinCC Unified PC 30000 Logging Tags	30000	No	Yes
WinCC Unified Database Storage[2]	No	Not required	Yes

[1] You can cumulate the logging tag licenses. The sum of the licenses yields the number of tags that can be logged.

[2] The license allows logging into the MS SQL database.

Upgrade

No upgrade license is required for logging when you upgrade the system.

The WinCC Unified Database Storage license is version-dependent and requires the corresponding upgrade license for the upgrade.

You can find more information under "Upgrade of licenses (Page 42)".

Trial

No trial mode is available for database-based logging.

3.3.3 Parameter sets

Requirement

WinCC Unified Basic Panel:

- For configuration, you need a WinCC Unified Basic ES (Engineering System) license.

WinCC Unified Comfort Panel:

- For configuration, you need a WinCC Unified Comfort ES (Engineering System) license.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

No license is required to use parameter sets on a WinCC Unified Basic Panel.

No license is required for use of parameter sets on a WinCC Unified Comfort Panel.

To use parameter sets on a Runtime PC, you need a WinCC Unified Parameter Control (PC) license.

Upgrade

The license is version-dependent and requires the corresponding upgrade license for the upgrade.

The upgrade license is included in the upgrade of the Unified Basic System.

You can find more information under "Upgrade of licenses (Page 42)".

Trial

If you do not have a valid license, you can configure the parameter sets in trial mode.

3.3.4 Process diagnostics

Requirement

WinCC Unified Basic Panel:

- The Process diagnostics option is not supported.

WinCC Unified Comfort Panel:

- For configuration, you need a WinCC Unified Comfort ES (Engineering System) license.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

To use process diagnostics on a WinCC Unified Comfort Panel, you need a WinCC Unified ProDiag license.

To use process diagnostics on a WinCC Unified PC RT, you need a WinCC Unified ProDiag license.

Upgrade

The license is version-dependent and requires the corresponding upgrade license for the upgrade.

The upgrade license is included in the upgrade of the Unified Basic System.

You can find more information under "Upgrade of licenses (Page 42)".

Trial

If you do not have a valid license, you can configure the process diagnostics in trial mode.

3.3.5 Client

WinCC Unified Basic Panel

- For configuration, you need a WinCC Unified Basic ES (Engineering System) license.

Every WinCC Unified Basic Panel includes a WinCC Unified Client Operate license.

License	Monitoring only	Operator control and monitoring
WinCC Unified Client Operate (1)*	No	Yes

* The number of clients cannot be extended.

WinCC Unified Comfort Panel:

- For configuration, you need a WinCC Unified Comfort ES (Engineering System) license.
- A WinCC Unified Comfort Panel can be accessed by a maximum of 3 simultaneous remote access operations.
- The license for first access is free of charge.
- The use of remote access must be activated in the firmware.

Licensing

For remote access, you need a license according to the number and type of accesses. Refer to the table below for the license needed:

License[1]	Monitoring only	Operator control and monitoring
WinCC Unified Panel Client Monitor (1)	Yes	No
WinCC Unified Panel Client Operate (1)	No	Yes

[1] You can cumulate the client licenses. The sum of the licenses yields the possible number of client connections.

WinCC Unified PC

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

The following client functions are included in the license for WinCC Unified PC RT:

- Two accesses for operator control and monitoring (two local accesses or one local and one remote access)
- One access for monitoring (one local access or one remote access)

Licensing

For remote access, you need a license according to the number and type of accesses. Refer to the table below for the license needed:

License[1]	Monitoring only	Operator control and monitoring
WinCC Unified Client Monitor (1)	Yes	No
WinCC Unified Client Monitor (3)	Yes	No
WinCC Unified Client Monitor (10)	Yes	No
WinCC Unified Client Monitor (30)	Yes	No
WinCC Unified Client Monitor (100)	Yes	No
WinCC Unified Client Operate (1)	No	Yes
WinCC Unified Client Operate (3)	No	Yes
WinCC Unified Client Operate (10)	No	Yes

License[1]	Monitoring only	Operator control and monitoring
WinCC Unified Client Operate (30)	No	Yes
WinCC Unified Client Operate (max pro RT server)	No	Yes

[1] You can cumulate the client licenses. The sum of the licenses yields the possible number of client connections.

Upgrade

The license is version independent and does not require any upgrade to a new version.

Trial

If you do not have a valid license, you can configure the client in trial mode.

3.3.6 Reporting

Requirement

WinCC Unified Basic Panel:

- The Reporting option is not supported.

WinCC Unified Comfort Panel:

- For configuration, you need a WinCC Unified Comfort ES (Engineering System) license.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

No license is required to create reports in Excel or to manually run reports in Excel or from the Runtime control "Reports".

For automatic running of reports (time-, event-based) on a WinCC Unified Comfort Panel, you need a "WinCC Unified Report Execution" license.

For automatic running of reports (time-, event-based) on a WinCC Unified PC RT, you need a "WinCC Unified Report Execution" license.

Upgrade

The license is version-dependent and requires the corresponding upgrade license for the upgrade.

The upgrade license is included in the upgrade of the Unified Basic System.

You can find more information under "Upgrade of licenses (Page 42)".

Trial

If you do not have a valid license, you can configure the Reporting option in trial mode.

3.3.7 Runtime Openness

3.3.7.1 Unified GraphQL

Requirement

WinCC Unified Basic Panel:

- The Unified GraphQL option is not supported.

WinCC Unified Comfort Panel:

- The Unified GraphQL option is not supported.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

To access the logged data on a WinCC Unified PC RT via the GraphQL interface, you need a "WinCC Unified Connectivity GraphQL Logged Data" license.

Upgrade

The license is version-dependent and requires the corresponding upgrade license for the upgrade.

The upgrade license is included in the upgrade of the Unified Basic System.

You can find more information under "Upgrade of licenses (Page 42)".

Trial

If you do not have a valid license, you can use the GraphQL interface in trial mode.

3.3.8 Unified Collaboration

Requirement

WinCC Unified Basic Panel

- The Unified Collaboration option is not supported.

WinCC Unified Comfort Panel:

- For configuration, you need a WinCC Unified Comfort ES (Engineering System) license.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

To use the Unified Collaboration option on a WinCC Unified Comfort Panel, you need a WinCC Unified Collaboration license for each device involved.

To use the Unified Collaboration option on a WinCC Unified PC RT, you need a WinCC Unified Collaboration license for each device involved.

Upgrade

The license is version-dependent and requires the corresponding upgrade license for the upgrade.

The upgrade license is included in the upgrade of the Unified Basic System.

You can find more information under "Upgrade of licenses (Page 42)".

Trial

If you do not have a valid license, you can configure the Unified Collaboration option in trial mode.

3.3.9 Audit

Requirement

WinCC Unified Basic Panel:

- The Audit option is not supported.

WinCC Unified Comfort Panel:

- For configuration, you need a WinCC Unified Comfort ES (Engineering System) license.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

To use the Audit option on a WinCC Unified Comfort Panel, you need a license.

To use the Audit option on a WinCC Unified PC RT, you need a license.

You can use the following licenses for the Audit option:

License	Description
WinCC Unified Audit Basis	Secured communication Logging the Audit Trail Recording of process data changes (automatically, via script or system function) Confirmation with / without comment Exporting Audit Trail entries Audit Trail report and tamper indication Logging in and logging out Audit Trail entries[1] Simple electronic signature Backing up and restoring Audit Trail database segments Direct display and analysis of the Audit Trail in the Audit Viewer[2]
WinCC Unified Audit Enhanced	In addition: Multiple electronic signature (2 persons)

[1] V18 or higher

[2] V18 Update 1 or higher

To use the Audit option, you need a license for each device involved.

License	WinCC Unified Comfort Panel	WinCC Unified PC
WinCC Unified Audit Basis	Yes	Yes
WinCC Unified Audit Enhanced	Yes	Yes

Upgrade

The license is version-dependent and requires the corresponding upgrade license for the upgrade.

The upgrade license is included in the upgrade of the Unified Basic System.

You can find more information under "Upgrade of licenses (Page 42)".

Trial

If you do not have a valid license, you can configure the Audit option in trial mode.

3.3.10 Unified Data Hub

Introduction

All the process information of the connected Data Hub Clients is centrally archived on the WinCC Unified Data Hub Server. Each participating device needs a Data Hub Client license.

The quantity or the type of process information that is stored in the central archive on the WinCC Unified Data Hub Server depends on the Data Hub Client type:

Is archived	WinCC Unified Data Hub Client Small*	WinCC Unified Data Hub Client*	WinCC Unified Data Hub Client Audit Trail*
Tags	200	Unlimited number	----------
Alarms	All	All	All
Audit Trails	----------	----------	Total

* Depending on requirements, the license can be ordered for 1, 3 or 10 Unified Data Hub clients

The license for Unified Data Hub clients is version independent and does not require any upgrade to a new version.

Licensing of the WinCC Unified Data Hub Server and WinCC Unified Data Hub Client

Requirement

WinCC Unified Basic Panel:

- The WinCC Unified Data Hub option is not supported.

WinCC Unified Comfort Panel:

- The WinCC Unified Data Hub option is not supported.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.

Licensing

To use WinCC Unified Data Hub Server on a WinCC Unified PC RT, you need a "WinCC Unified Data Hub Server" license package. The "WinCC Unified Data Hub Server" package contains the following licenses:

- Unified PC (150) RT
- Unified Database Storage
- Data Hub Client (1) - for use on the UDH server
- Data Hub Server

To use WinCC Unified Data Hub Client on a WinCC Unified PC RT, you need a "WinCC Unified Data Hub Client" license.

Upgrade

The license package "WinCC Unified Data Hub Server" is version-dependent and requires the corresponding upgrade license package for the upgrade.

The "WinCC Unified Data Hub Client" license is versionless. No upgrade license is required.

You can find more information under "Upgrade of licenses (Page 42)".

Trial

If you do not have a valid license, you can configure WinCC Unified Data Hub Server in trial mode.

3.3.11 Redundancy

Requirement

WinCC Unified Basic Panel

- The Redundancy option is not supported.

WinCC Unified Comfort Panel:

- The Redundancy option is not supported.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For use in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

To use the Redundancy option on WinCC Unified PC RT, you need a "WinCC Unified Redundancy" license for each device involved.

Each license package contains two "WinCC Unified Redundancy" licenses.

Upgrade

The license is version-dependent and requires the corresponding upgrade license for the upgrade.

The upgrade license for a WinCC Unified PC RT station is included in the upgrade of the Unified Basic System.

You can find more information under "Upgrade of licenses (Page 42)".

Trial

If you do not have a valid license, you can configure the Redundancy option in trial mode.

3.4 Licensing of Plant Intelligence options

3.4.1 Calendar

Requirement

WinCC Unified Basic Panel:

- The Calender option is not supported.

WinCC Unified Comfort Panel:

- The Calender option is not supported.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For the PI option Calendar in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

No additional license is required for configuration of the PI option Calendar .

To use the PI option Calendar on a WinCC Unified PC RT, you need the following licenses:

License	Description
WinCC Unified Calendar Base	Per server: • Three independent basic calendars • Unlimited number of derived calendars • Unrestricted use of the option • Version-based
WinCC Unified Calendar Extension (1)*	• One additional basic calendar

* Valid per extension, is independent of version and cumulative

Example:

WinCC Unified Calendar Base + WinCC Unified Calendar Extension (1) → 3 + 1 = 4

Upgrade

To upgrade to the next higher version, you need a WinCC Unified Calendar Base Upgrade license.

The WinCC Unified Calendar Extension (1) license, however, is version-independent.

Trial

If you do not have a valid license, you can configure the Calendar PI option in trial mode.

3.4.2 Performance Insight

Requirement

WinCC Unified Basic Panel:

- The Performance Insight option is not supported.

WinCC Unified Comfort Panel:

- The Performance Insight option is not supported.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For the PI option Performance Insight in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

No additional license is required for configuration of the PI option Performance Insight .

To use the PI option Performance Insight on a WinCC Unified PC RT, you need the following licenses:

License	Description
WinCC Unified Performance Insight Base	Per server: • Three analyzed plant objects • Unrestricted use of the option • Version-based
WinCC Unified Performance Insight Extension (10)*	• 10 additional analyzed plant objects
WinCC Unified Performance Insight Extension (30)*	• 30 additional analyzed plant objects
WinCC Unified Performance Insight Extension (100)*	• 100 additional analyzed plant objects
WinCC Unified Performance Insight Extension (300)*	• 300 additional analyzed plant objects

* Valid per extension, is independent of version and cumulative

Example:

WinCC Unified Performance Insight Base + WinCC Unified Performance Insight Extension (10) → 3 + 10 = 13

WinCC Unified Performance Insight Base + WinCC Unified Performance Insight Extension (10) + WinCC Unified Performance Insight Extension (30) → 3 + 10 + 30 = 43

Upgrade

To upgrade to the next higher version, you need a WinCC Unified Performance Insight Base Upgrade license.

The WinCC Unified Performance Insight Extension licenses, however, are version-independent.

Trial

If you do not have a valid license, you can configure the Performance Insight PI option in trial mode.

3.4.3 Sequence

Requirement

WinCC Unified Basic Panel:

- The Sequence option is not supported.

WinCC Unified Comfort Panel:

- The Sequence option is not supported.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For the PI option Sequence in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

No additional license is required for configuration of the PI option Sequence.

To use the PI option Sequence on a WinCC Unified PC RT, you need the following licenses:

License	Description
WinCC Unified Sequence Base	Per server: • 3 concurrent equipment modules • Unrestricted use of the option • Version-based
WinCC Unified Sequence Extension (5)*	• 5 additional concurrent equipment modules

* Valid per extension, is independent of version and cumulative

Example:

WinCC Unified Sequence Base + WinCC Unified Sequence Extension (5) → 3 + 5 = 8

WinCC Unified Sequence Base + WinCC Unified Sequence Extension (5) + WinCC Unified Sequence Extension (5) → 3 + 5 + 5 = 13

Upgrade

To upgrade to the next higher version, you need a new WinCC Unified Sequence Base Upgrade license.

The WinCC Unified Sequence Extension (5) license, however, is version-independent.

Trial

If you do not have a valid license, you can configure the Sequence PI option in trial mode.

3.4.4 Line Coordination

Requirement

WinCC Unified Basic Panel:

- The Line Coordination option is not supported.

WinCC Unified Comfort Panel:

- The Line Coordination option is not supported.

WinCC Unified PC:

- For configuration, you need a WinCC Unified PC ES (Engineering System) license.
- For the PI option Line Coordination in Runtime, you need a WinCC Unified PC RT (Runtime) license.

Licensing

No additional license is required for configuration of the PI option Line Coordination.

To use the PI option Line Coordination on a WinCC Unified PC RT, you need the following licenses:

License	Description
WinCC Unified Line Coordination Base	Per server: • 3 units • Unrestricted use of the option • Version-based
WinCC Unified Line Coordination Extension (5)*	• 5 units
WinCC Unified Line Coordination Extension (10)*	• 10 units
WinCC Unified Line Coordination Extension (50)*	• 50 units

* Valid per extension, is independent of version and cumulative

Example:

WinCC Unified Line Coordination Base + WinCC Unified Line Coordination Extension (5)
→ 3 + 5 = 8

WinCC Unified Line Coordination Base + WinCC Unified Line Coordination Extension (5) + WinCC Unified Line Coordination Extension (10)

→ 3 + 5 + 10 = 18

Upgrade

To upgrade to the next higher version, you need a new WinCC Unified Line Coordination Base Upgrade license.

The WinCC Unified Line Coordination Extension licenses, however, are version-independent.

Trial

If you do not have a valid license, you can configure the Line Coordination PI option in trial mode.

3.5 Handling licenses and license keys

Introduction

You need a valid License Key in each case to use STEP 7 Basic, STEP 7 Professional as well as WinCC Engineering System, options for WinCC Engineering System and WinCC Runtime.

NOTICE
Destruction of license keys by copying A License Key cannot be copied. The copy protection prevents the License Keys from being copied. If there is an attempt to copy a License Key, the License Key gets destroyed.

Trial License

If you start the TIA Portal without a valid License Key, the system alerts you that you are working in non-licensed mode. You can activate a trial license once. The trial license expires after 21 days.

When the trial license has expired, the TIA Portal only runs with restrictions. For the full version of the TIA Portal, you need to purchase the corresponding license.

Installing license keys for STEP 7 and WinCC

Install the license with the Automation License Manager from the accompanying data storage medium to your PC.

You need additional License Keys to use WinCC Runtime or simulation on the Engineering-PC with the menu command "Online > Simulation > Start". You need to use Automation License Manager for this.

When you install a license, the relevant License Key will be removed from the original storage location of the License Keys.

Transferring license keys to the HMI device

You must transfer the License Keys to the HMI device to operate WinCC.

You transfer a License Key to the HMI device in the following cases:

- To operate WinCC Runtime
- To use add-ons for WinCC Runtime

When you transfer a license to an HMI device, the associated License Key is removed from the License Keys storage location.

If you no longer need the license or want to back up data, you must transfer the License Keys from the operator panel. You can then use this license on another PC or HMI device.

Uninstalling license keys

License Keys are always uninstalled using the Automation License Manager. Call the Automation License Manager before uninstalling

and back up the license key to be uninstalled to another storage location.

You uninstall a License Key in the following cases:

- When backing up data.
- If you no longer require the license.

You can also use a valid license on another PC.

Modification to the data media of the engineering system

Modifying the data medium of the engineering system can destroy the License Key. To do this before such modifications, open the Automation License Manager and back up License Key to be uninstalled to another storage location.

NOTICE
Destruction of license keys on PCs If one of the following cases applies, first, uninstall all License Keys : • Format the hard disk • Compress the hard disk • Restore the hard disk • Start an optimization program that moves fixed blocks • Install a new operating system Read the description of Automation License Manager ("Start > Siemens Automation > Documentation"). Comply with all warnings and notices.

Data backup of operating panels (Backup/Restore)

When backing up data on the HMI device, remove the License Keys on the HMI device. To do this, open the Automation License Manager and back up the License Key to another storage location.

NOTICE
Destruction of license keys on non-PC-based HMI devices License keys transferred as a result of backup/restore operations are destroyed in the case of the following HMI devices: • 270s series • 370s series Proceed as follows before restoring: 1. Use the Automation License Manager and ProSave to check if there are License Keys on the HMI device. 2. Transfer the existing License Keys from the HMI device. After restoring has been carried out, transfer the License Keys back to the HMI device.

Invalid license after time zone change

The installed licenses will no longer work if you change the time zone on a PC as follows: from a full-hour time zone to a time zone that is not based on a full hour.

To avoid this inconvenience, uninstall the License Key with the Automation License Manager under the time zone setting that was set when the License Keys was installed.

Example: You want to use the HMI device from the time zone "GMT +3:00" in the time zone "GMT +3:30".

1. Uninstall the License Key with the time zone setting "GMT +3:00".
2. Change the time zone settings accordingly on your PC.
3. Install the License Key.

This behavior does not apply to the Trial License.

Defective license

A license is defective in the following cases:

- If the License Key is no longer accessible at the storage area.
- If the License Key disappears during its transfer to the destination drive.

Note

If you reset the system date to an earlier time, all licenses are invalidated.

You can use the Automation License Manager to repair the defective license. Use the "Restore" function or the "Restore wizard" of the Automation License Manager for this purpose. Contact Customer Support to restore them. You can find more detailed information on the Internet: http://support.automation.siemens.com (https://support.industry.siemens.com/cs/de/en/)

Note

Runtime can also be operated without errors if the license is missing or defective. The system alerts you at brief intervals that you are working in non-licensed mode.

Microsoft SQL Server

A license is required for use of the Microsoft SQL Server database. The license is included in a properly licensed and installed version of WinCC.

The SQL Server which is licensed with the installation of WinCC can only be used in connection with WinCC.

Its use for other purposes requires an additional license. These include, for example:

- Use for custom databases
- Use for third-party applications
- Use of SQL access mechanisms which are not provided via WinCC.

Uninstalling

After uninstalling WinCC, you must uninstall the "WinCC" SQL server instance. To do this, select the entry "Microsoft SQL Server 20.." under "Control Panel > Programs" and uninstall it.

See also

Licensing STEP 7 and WinCC (Page 12)

3.6 Upgrade of licenses

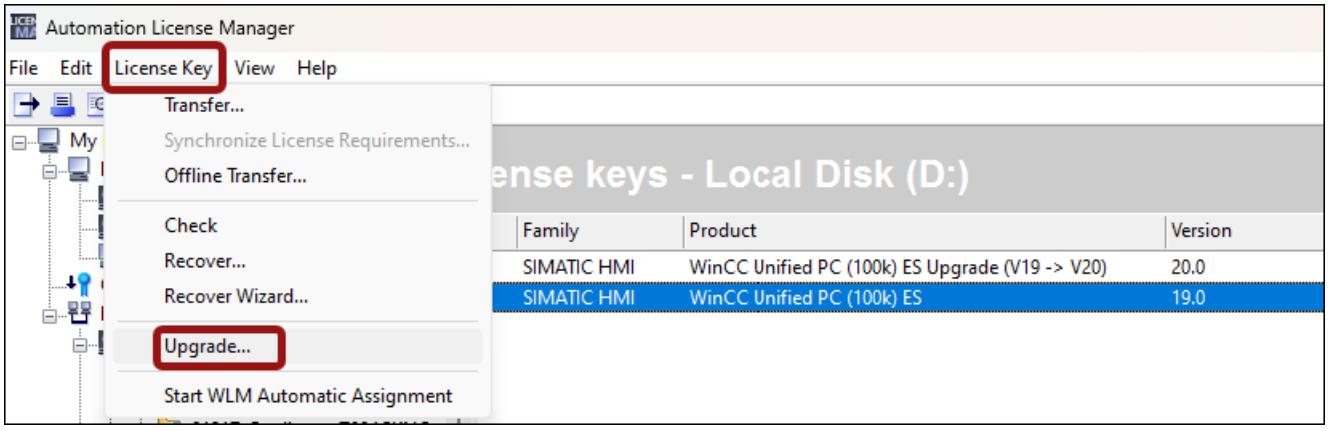
Upgrade of version-dependent licenses

To upgrade a lower version on your PC, you need the license for an upgrade or the license for a PowerPack.

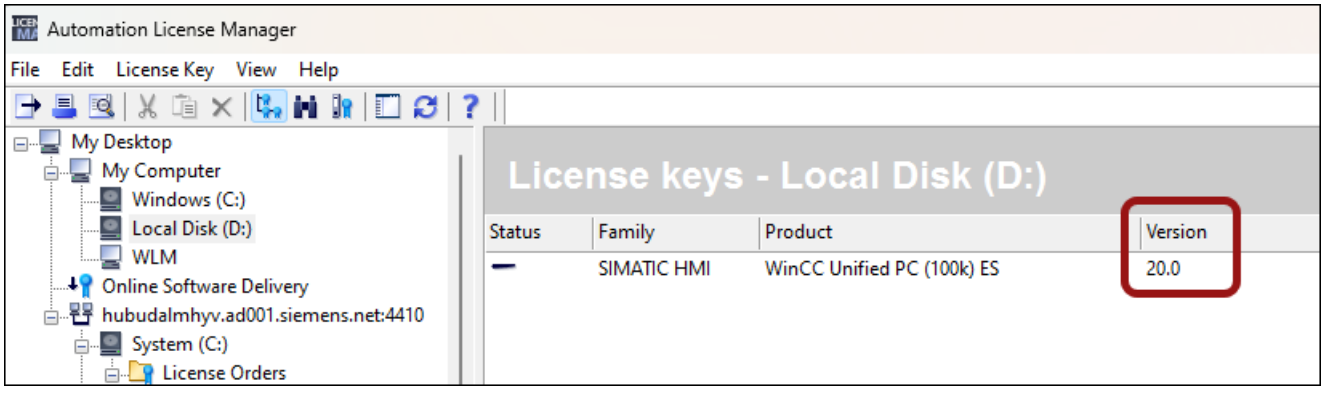
To perform the upgrade, follow these steps:

Example: You have the license WinCC Unified PC (100k) ES V19 and must upgrade to Version V20.

1. Open the Automation License Manager.
2. Open the location where the licenses are stored locally.
3. Select the license that you want to upgrade.
4. Click the "License Key" button in the toolbar and select "Upgrade"



5. The upgrade takes place automatically, and the upgrade license replaces the license with the lower version number.



3.7 Licensing of HMI devices

Non-PC-based HMI devices are equipped with Runtime licenses. A License Key is not required for runtime operation.

A license may be required for an add-on for non-PC-based HMI devices. The License Key of the respective license always activates one add-on for use.

License key

In order to license non-PC-based HMI devices with License Keys, the "SIMATIC HMI License Manager Panel Plugin" add-on is needed.

WinCC Setup installs this add-on by default. You open the License Manager Panel Plugin in the Automation License Manager with the "Edit > Connect Target System > Connect HMI Device" menu command.

If WinCC is not installed, an installation of ProSave 7.2 or higher is required.

Notes on handling licenses

- Further information on license handling can be found in the Automation License Manager help.
- Verify that the current version of the operating system (or higher) is installed on the HMI device before you start licensing. If necessary, update the operating system using ProSave.
- The licensee also recognizes that the software (SW) from the Microsoft Corporation or subsidiaries contains licensed software. The licensee hereby agrees to be bound by and comply with the terms of the attached license agreement between Microsoft SQL Server and End User.

Non-licensed mode

Runtime add-ons can be used for a short time without restrictions without a valid license. Non-licensed mode is indicated every 10 minutes by a window, which you must acknowledge.

3.8 Licensing WinCC Runtime on PC-based HMI devices

License key

With PC-based HMI devices, you require a license key for the following:

- WinCC Runtime with 128 tags, for example.
- WinCC add-ons

You transfer licenses for the WinCC add-ons after installation with the Automation License Manager.

Note

Productive operation of the software is only permitted with a valid Certificate of License which specifies the respective version.

The appropriate new license is required to license WinCC Runtime.

You can upgrade the Runtime licenses of WinCC flexible 2008 and WinCC V7 with an upgrade license to WinCC Runtime.

Notes on handling licenses

- When you upgrade an older version to the current version, you need new licenses for WinCC Runtime.
- The licensee also recognizes that the software (SW) from the Microsoft Corporation or subsidiaries contains licensed software. The licensee hereby agrees to accept the terms of the accompanying license agreement between Microsoft SQL Server and end users and to abide by them.

Non-licensed mode

WinCC Runtime and the Runtime add-ons can be used freely without license. Non-licensed mode is indicated every 10 minutes by a window, which you must acknowledge.

3.9 Licensing WinCC Runtime Asian

Introduction

If you are using WinCC Runtime in an Asian language, a dongle is used additionally for the validation of the required license.

The dongle is delivered in form of a certified USB flash drive together with the Licence Key required for WinCC Runtime Professional and WinCC Unified PC Runtime Asian. The license key is stored on the certified USB flash drive.

Using the dongle for an Asian Runtime

To successfully license a WinCC project in an Asian language, transfer the required license key from the certified USB flash drive to the HMI device using the "Automation License Manager".

Plug the USB flash drive into the USB port of the HMI device. The USB flash drive acts as a dongle during runtime. The dongle must always remain plugged in the USB port during runtime.

If you remove the dongle during runtime, WinCC Runtime switches to Demo mode.

The USB flash drives supplied for the Asian markets are certified for permanent use in production. Therefore, you cannot transfer or copy the content to another USB medium.

If you lose the certified USB flash drive or it becomes defective, you need a new, certified USB flash drive.

Simulation of a WinCC project in an Asian language

You then also need a certified USB flash drive as dongle for the simulation. If no dongle is available, the simulation runs in Demo mode.

3.10 STEP 7 without license for PC-CP

Functions of STEP 7 for PC-CP

STEP 7 for PC-CP is a full version of STEP 7 that was installed without license. This version only supports configuration and diagnostic options for the following components:

- PC-CPs and applications (OPC server) for PC stations
- SCALANCE X switches
- SCALANCE W / SCALANCE M routers
- SCALANCE S security module
- PROFINET IO devices and PROFIBUS DP slaves
- IE/PB LINK PN IO, IWLAN/PB LINK PN IO
- Readers (RFID) and optical readers (MV)

SIMATIC stations and WinAC components are only available in the network and topology view (no device view). Programming functions are not available.

Information system

The information system for PC-CP available in STEP 7 describes the full scope of STEP 7 functions. You should therefore remember that the functions are restricted to the configuration of the previously listed device groups.

Upgrading to the range of functions of STEP 7 Professional

The full scope of STEP 7 functions is already available on your engineering station with the installation of STEP 7 for PC-CP, although its use is restricted.

By installing a license later, you can upgrade at any time to the full functionality of STEP 7. There is no need for a new installation. Any projects created previously in STEP 7 for PC-CP can still be used without restrictions once a license is installed.

System requirements for installation

4

4.1 Notes on the system requirements

System requirements for individual products

The system requirements might differ depending on the products you want to install. You should therefore check the individual system requirements of your products.

If you want to install several products, make sure that your system meets the demands of the product with the highest requirements.

Displaying PDF files

To be able to read the supplied PDF files, you need a PDF reader that is compatible with PDF format 1.7, such as Adobe (R) Reader.

Character sets

Since Windows 10 Update Version 1809, Windows allows the installation of character sets either with administrator rights for each user (command "Install for all users" in the context menu) or for specific users. In order to use WinCC character sets without restrictions and load them onto an operator panel, the character sets must always be installed with administrator rights.

Note that the "Install" button in the view of a character set only initiates a user-specific installation.

See also

Notes on licenses (Page 11)

Performing the installation (Page 87)

Displaying the installed software (Page 93)

Modifying or updating installed products (Page 95)

Repairing installed products (Page 97)

Starting to uninstall (Page 99)

FAQ (https://support.industry.siemens.com/cs/ww/en/view/109748887)

4.2 General software and hardware requirements

System requirements for installation

The following table shows the minimum software and hardware requirements that have to be met for the installation:

Hardware/software	Requirement
Processor	Intel® Core™ i3-6100U, 2.30 GHz
RAM	8 GB
Hard disk	S-ATA with at least 20 GB available space
Network	From 100 Mbit
Screen resolution	1024 x 768
Operating systems *	**Windows 10 (64-bit)** • Windows 10 Enterprise 21H2/2021 LTSC **Windows 11 (64-bit)** • Windows 11 Home Version 24H2** • Windows 11 Professional Version 24H2 • Windows 11 Enterprise 24H2 • Windows 11 Enterprise 24H2 LTSC • Windows 11 Enterprise 23H2 **Windows Server (64-bit)** • Windows Server 2025 Standard (full installation) • Windows Server 2022 Standard (full installation)

* Including all Security updates up to Microsoft Security Bulletin Summary for August 2025 (MS25-AUG). For more detailed information on operating systems, refer to the help on Microsoft Windows or the Microsoft Web site.

** Only for Basic editions

Some protocols might also support additional Windows versions. You can find more information in the product-specific requirements or check the compatibility with the compatibility tool. The compatibility tool can be found on the Internet at https://support.industry.siemens.com/compatool/ (https://support.industry.siemens.com/compatool/).

Recommended PC hardware

The following table shows the recommended hardware requirements:

Hardware/software	Requirement
Computer	SIMATIC FIELD PG M6 Comfort or higher (or comparable PC)
Processor	Intel® Core™ i5-8400H (2.5 to 4.2 GHz; 4 cores + hyper-threading; 8 MB smart cache)
RAM	16 GB or more (32 GB for large projects)
Hard disk	SSD with at least 50 GB available memory space
Network	1 GBit (for multiuser)
Monitor	15.6" Full HD Display (1920 x 1080 or higher)

Supported virtualization platforms

You can install the software packages "SIMATIC STEP 7" and "SIMATIC WinCC" on a virtual machine. For this purpose, use one of the following virtualization platforms in the specified version or a newer version:

- VMware vSphere Hypervisor (ESXi) 8.0 or higher
- VMware Workstation V17 or higher
- VMware Player V17 or higher
- Microsoft Hyper-V Server 2019 or higher

The following host and guest operating systems are recommended for these virtualization platforms:

Operating system	VMware vSphere Hypervisor (ESXi)	VMware Workstation	VMware Player	Microsoft Hyper-V
Windows Server 2025 Standard (full installation)	G	-	-	H/G
Windows Server 2022 Standard (full installation)	G	-	-	H/G
Windows Server 2019 Standard (complete installation)	G	-	-	H/G
Windows Server 2016 Standard (full installation)	G	-	-	G
Windows Server 2008 R2 SP1, Windows Server 2012 and Wndows server 2012 R2	G	-	-	G
Windows Server 2008 SP2	G	-	-	G
Windows 10 Enterprise 21H2/2021 LTSC	H/G	H/G	H/G	G
Windows 11 Professional 24H2	H/G	H/G	H/G	G
Windows 11 Enterprise 24H2	H/G	H/G	H/G	G
Windows 11 Enterprise 24H2 LTSC	H/G	H/G	H/G	G
Windows 11 Enterprise 23H2	H/G	H/G	H/G	G

H: Can be used as host operating system

G: Can be used as guest operating system

H/G: Can be used as host and guest operating system

-: Cannot be used as the host or guest operating system

Note

- The same hardware requirements apply to the host operating system as for the respective TIA products.
- The plant operator must ensure that sufficient system resources are available for the host operating systems.
- The hardware certified by the manufacturers is recommended for the use of HyperV server and ESXi.
- When you use Microsoft Hyper-V, accessible stations cannot be displayed.

Supported security programs

The following security programs are compatible with "SIMATIC STEP 7" and "SIMATIC WinCC":

- Antivirus programs:
  - Symantec Endpoint Protection 14.3 RU8 or higher
  - McAfee Endpoint Security (ENS) (Trellix) 10.7 or higher
  - Trend Micro Apex One (Trend Micro Office Scan)
  - Windows Defender
  - Qihoo 360 "Safe Guard" + "Virus Scanner"
  - Crowdstrike Falcon Go (Falcon Prevent and Falcon Device Control)

  Note

  Make sure that your virus scanner and its databases are always up-to-date.

  The last update of the virus pattern was on 20 August 2025.
- Encryption software:
  - Microsoft Bitlocker
- Host-based Intrusion Detection System:
  - McAfee Application Control (Trellix) 8.4 or higher

See also

Notes on licenses (Page 11)
Performing the installation (Page 87)
Checking availability of updates and support packages and installing them (Page 101)
Displaying the installed software (Page 93)
Modifying or updating installed products (Page 95)
Repairing installed products (Page 97)
Starting to uninstall (Page 99)

4.3 Use of high-resolution monitors

Introduction

When working with TIA Portal, you have the option of using high-resolution monitors, e.g. 4K monitors. To get the best display for these monitors, use the scaling recommended in Microsoft Windows under the screen settings if possible. The TIA Portal adapts to a scaling of up to 350 percent. In the "User-defined scaling" area of the "Advanced Scaling Settings" dialog, you can also set a higher scaling. However this may result in blurred, distorted or overlapping text and graphics. Therefore, please use the default setting recommended by Microsoft Windows.

Use of multiple monitors

If you have multiple monitors in use, TIA Portal starts on the primary monitor. In doing so, the TIA Portal adapts to the respective resolution. For a 4K monitor, this adjustment is made up to a scaling of 350 percent. This is the recommended default setting by Microsoft Windows. If you move the TIA Portal or individual windows to another monitor, it depends on the resolution of this monitor how the display looks like. It's possible that the text and graphics may appear blurred, distorted or overlapping. There is no dynamic scaling for this monitor. That means if this monitor doesn't use the same scaling factor as the primary monitor, the previously set scaling may not be suitable for this monitor. In this case, set the scaling back to the recommended value or the value set on the primary monitor.

4.4 Product-specific special characteristics

4.4.1 Installing WinCC

Specific requirements on the operating system and software configuration must be met for the installation.

Note

WinCC is generally authorized for use in a domain or workgroup.

However, be aware that domain group policies and restrictions of the domain can hinder the installation. In this case, remove the computer from the domain prior to installing Microsoft Message Queuing, Microsoft SQL Server and WinCC. Log on to the local machine with administrator rights. Then perform the installation. After successful installation, you can enter the WinCC computer back into the domain. If the domain group policies and restrictions of the domain do not impede the installation, the computer need not be removed from the domain during the installation.

Be aware that domain group policies and restrictions of the domain can also hinder operation. If you cannot avoid these restrictions, run the WinCC computer in a workgroup.

Consult with the domain administrator if needed.

4.4.2 Uninstalling WinCC Unified

Uninstalling WinCC

If you have already installed an update for WinCC Unified V16 and want to install WinCC V17, proceed as follows:

1. Open the Control Panel.
2. Start the uninstallation of SIMATIC WinCC Unified PC V16.0 UPDx.

3. When selecting the components, select "SIMATIC WinCC Update 16.0 UPDx" for uninstallation.
4. After completing this uninstallation, uninstall all desired components of WinCC V16 via the installation medium.

The information is contained in the readme under "Important notes (WinCC Unified)".

4.4.3 Installation of WinCC Runtime Unified

Specific requirements for the operating system and software configuration must be met for the installation.

Installation in domains and workgroups

WinCC Unified is generally approved for operation in a domain or workgroup.

However, be aware that domain group policies and restrictions of the domain might hinder the installation. In this case, remove the computer from the domain before installing WinCC Unified and Microsoft SQL Server. Log on to the local machine with administrator rights. Perform the installation. After successful installation, you can restore the WinCC computer to the domain. If the domain group policies and restrictions of the domain do not impede the installation, the computer need not be removed from the domain during the installation.

Be aware that domain group policies and restrictions of the domain might also hinder operation. If you cannot avoid these restrictions, run the WinCC computer in a workgroup.

Consult with the domain administrator if needed.

Operation on a network server

It is not permitted to operate WinCC Unified Runtime on a network server (e.g. domain controller, file server, name service server, router, software firewall, media server, exchange server).

Windows computer name

Before you start the WinCC installation, specify the Windows computer name. Follow the Windows naming rules.

Note

How to proceed after a subsequent change of the computer name is described in the WinCC Unified Runtime installation manual in the section "Changing the computer name or IP address".

The following characters are not permitted for the computer name:

- . , ; : ! ? " ' ^ ` ~ _
- + = / \ | @ * # $ % &

- ( ) [ ] { } < >
- Space

Follow these recommendations when assigning the Windows computer name:

- Only uppercase letters may be used.
- The first character must be a letter.
- The first 12 characters of the computer name must be unique.
- The computer name can have a maximum of 15 characters.

Hardware requirements for the installation

The following table shows the minimum hardware requirements that have to be met for the installation:

Hardware	Requirement
Processor type	Intel Core i3
RAM	4 GB
Free hard disk space	10 GB, 8 GB CF

Software requirements for the installation

Operating system

Software	Configuration	Comments
Windows 10 Pro	Windows 10 Pro Version 1909 (OS Build 18363) Windows 10 Pro Version 2004 (OS Build 19041) Windows 10 Pro Version 2009/20H2 (OS Build 19042) Windows 10 Pro Version 21H1 (OS Build 19043) Windows 10 Pro Version 21H2 (OS Build 19044)	64-bit
Windows 10 Enterprise	Windows 10 Enterprise Version 1909 (OS Build 18363) Windows 10 Enterprise Version 2004 (OS Build 19041) Windows 10 Enterprise Version 2009/20H2 (OS Build 19042) Windows 10 Enterprise Version 21H1 (OS Build 19043) Windows 10 Enterprise Version 21H2 (OS Build 19044)	
Windows 10 IoT Enterprise LTSB	Windows 10 Enterprise 2016 LTSB (OS Build 14393) (Test for IPC) Windows 10 Enterprise 2019 LTSC (OS Build 17763) (Test for IPC) Windows 10 Enterprise 2021 LTSC (OS Build 19044) (Test for IPC)	

Software	Configuration	Comments
Windows 11	Windows 11 Home Version 21H2 (OS Build 22000) Only suitable for deployment of Runtime Simulation on an Engineering PC.	64-bit
Windows 11 Pro	Windows 11 Pro Version 21H2 (OS Build 22000)	
Windows 11 Enterprise	Windows 11 Pro Version 21H2 (OS Build 22000)	
Windows Server 2016 Standard Windows Server 2019 Standard Windows Server 2022 Standard	Full installation	64-bit

Note

Number of supported clients and connections

Desktop operating systems support a maximum of 5 clients. In server operating systems, more than 5 clients can connect to the server.

Windows limits the number of incoming connections on desktop operating systems to 20. This limits the number of possible accesses to Runtime.

Compatible browsers

Operating system	Browser
Microsoft Windows	• Google Chrome • Microsoft Edge • Mozilla Firefox, Mozilla Firefox ESR
Android	• Google Chrome • Firefox • Edge
iOS, Mac	• Safari • Google Chrome • Firefox • Edge

More information on the use of browsers is available in the SIMATIC Unified PC Readme in the section "Internet browsers for WinCC Unified PC".

Windows specific software settings for IIS (Internet Information Services)

The following settings for IIS are automatically enabled in Windows during the installation of WinCC Runtime Unified:

- HTTP error
- HTTP Redirection
- Default document
- Static content

- .NET extensibility 3.5
- ASP
- ASP.NET 4.5
- ISAPI extensions
- ISAPI filters
- Dynamic Content Compression
- Static Content Compression
- Request Filtering

Table 4-1 Additional software requirements

Topic	Version / setting	Comment
Web browser	The browser must support HTML 5.	
User rights for installation	Administrator rights	
SIMATIC NET	V19	You need this license to be able to operate Runtime Unified with more than 10 connections.

Previously installed versions of WinCC Unified PC Runtime

Installing Unified PC Runtime V19 is possible on devices for which the following applies:

- No Unified PC Runtime installed, or
- WinCC Unified PC Runtime V18 installed

Ports

When a Windows firewall is used, the installation routine of WinCC Unified Runtime sets up the following ports:

- HTTPS: 443
- Network Discovery (IS): 137
- Totally Integrated Automation administrator: 8888
- UMC AttachAgent: 4002
- OPC UA Discovery: 4840

If your system uses a different firewall solution, make sure the ports are set up accordingly.

You can find a list of the ports used by Unified Runtime in the user help SIMATIC Unified PC readme in the section "Security information". Before starting the installation, make sure that the ports listed in the list are free.

Note

Disable HTTP port

For security reasons, it is recommended to disable port 80 on the IIS server:

1. On the Unified PC, launch "Internet Information Services (IIS) Manager".
2. Click "Default Web Sites" on the right.
3. Select "Remove" or "Manage Website > Exit".

Note

Blocked ports after operating system update or upgrade

Updating or upgrading the operating system of the Unified PC, e.g. from Windows Server 2016 to Windows Server 2019, may change the firewall settings. As a result, the OPC UA ports may be blocked.

If this happens, start the Siemens "Security Controller" tool and run "Restore settings".

Virtualization

You can install the "SIMATIC WinCC Runtime Unified" software package on a virtual machine. The following virtualization systems were tested:

- VMware vSphere Hypervisor (ESXi) 6.7 (or higher)
- VMware Workstation 12.5.5 and VMware Workstation 15.5.0 (or higher)
- VMware Player 12.5.5 and VMware Player 15.5.0 (or higher)
- Microsoft Hyper-V Server 2019 (or higher)

In a virtualization platform, all approved operating systems can be used as host operating system.

Requirement

The performance data of the virtual computers must meet the minimum requirements of WinCC clients.

Note

- Ensure that terminal and PLC networks are separated on the host system by using separate network adapters (dedicated, physically separated network adapters).
- The same hardware requirements apply to the host operating system as for the respective TIA products.
- The plant operator must ensure that sufficient system resources are available for the host operating systems.
- The hardware certified by the manufacturers is recommended for the use of HyperV server and ESXi.

Supported security programs

The following security programs are compatible with Unified Runtime:

Virus scanner	Symantec Endpoint Protection 14.3
	McAfee Endpoint Security (ENS) 10.6 and 10.7
	Trend Micro Office Scan 14.0
	Windows Defender (as part of the Windows operating system)
	Qihoo 360 "Safe Guard 12.1" + "Virus Scanner"
Whitelisting	McAfee Application Control 8.3.3
Hard disk encryption	Microsoft BitLocker (as part of the Windows operating system)

Principle

Care must be taken to ensure that the use of the antivirus software does not impair the process operation of a plant.

Rules for antivirus software (virus scanning clients)

- Integrated virus scanner firewall
  In WinCC Unified, the local Windows firewall used is configured with SIMATIC Security Control. Do not install or enable the integrated firewall of the antivirus software.
- Manual scan
  You must not perform a manual scan while Runtime is running. Perform disk on regular intervals on all plant PCs, for example, during the maintenance interval.
- Automatic scan
  For automatic scan it is sufficient to scan the incoming data traffic.
- Scheduled scan
  You must not perform a scheduled scan while Runtime is running.
- Pattern update
  The pattern update of the virus scanning clients (the plant PCs which are checked for viruses) performed by the higher-level virus scanning server (the plant PC which centrally manages the virus scanning clients).
- Dialog
  To avoid impairing the process operation, no dialog messages can be displayed on the virus scanning clients.
- Drives
  To prevent overlapping scans on network drives, only the local drives are scanned.

Otherwise apply the default settings.

What is secured?

The incoming data traffic is checked for viruses. The impairment of the process mode is minimized.

Note

If you are using an anti-virus scanner, make sure that the computer has sufficient system resources.

Supported database types

The following database types are supported by SIMATIC WinCC Unified PC:

HMI device	Supported database type
SIMATIC WinCC Unified PC	SQLite
	Microsoft SQL

Microsoft SQL Server for Unified PC

WinCC Unified PC uses SQLite as the default database type. To use Microsoft SQL Server, the system provides an installation option with a setup package.

- Logging with SQLite is not possible after the installation of Microsoft SQL Server.
- Existing SQLite files are retained, but they cannot be accessed in runtime.
- No backup can be created for SQLite.

If required, you can find the "Microsoft SQL Server Management Studio" on the installation medium in the "Support\SQL Server Management Studio" folder.

4.4.4 Installation of WinCC Runtime Professional

Specific requirements for the operating system and software configuration must be met for the installation.

Installation in domains and workgroups

WinCC is generally approved for operation in a domain or workgroup.

However, be aware that domain group policies and restrictions of the domain might hinder the installation. In this case, remove the computer from the domain before installing Microsoft Message Queuing, Microsoft SQL Server and WinCC. Log on to the local machine with administrator rights. Perform the installation. After successful installation, you can restore the WinCC computer to the domain. If the domain group policies and restrictions of the domain do not impede the installation, the computer need not be removed from the domain during the installation.

Be aware that domain group policies and restrictions of the domain might also hinder operation. If you cannot avoid these restrictions, run the WinCC computer in a workgroup.

Consult with the domain administrator if needed.

Operation on a network server

Operation of WinCC Runtime Professional on a network server (e.g. domain controller, file server, name utility server, router, software firewall, media server, exchange server) is not permitted.

Windows computer name

Do not change the Windows computer name after installing WinCC.

If you change the Windows computer name, you must uninstall the SQL server and reinstall it.

The following characters are not permitted for the computer name:

- . , ; : ! ? " ' ^ ´ ` ~ _
- + = / \ ¦ @ * # $ % & § °
- ( ) [ ] { } < >
- Blanks

Follow these recommendations when assigning the Windows computer name:

- Only uppercase letters may be used.
- The first character must be a letter.
- The first 12 characters of the computer name must be unique.

Activating remote communication

On WinCC systems, remote communication in the dialog "Simatic Shell" is deactivated by default after installation. You have to activate remote communication for the computers involved for the following applications:

- Loading Runtime onto another PC
- Client to server communication
- Redundant system
- WinCC option "WebNavigator"
  If the WebNavigator client is not running on the same computer as the WebNavigator server, remote communication must be activated.

To enable remote access, follow these steps:

1. Open the communication settings in Windows Explorer using the shortcut menu of Simatic Shell.
2. Activate the option "Remote communication".
3. Configure encrypted communication in the network: Select the pre-shared key and the port.
4. Select the network adapter and, if necessary, the multicast settings.

Deactivating NTLMv1 and SMBv1

The NTLMv1 and SMBv1 protocols can be disabled. Deactivating the protocols does not have any effect on the operation of WinCC Runtime Professional.

Note

Security risk from NTLMv1 and SMBv1

Use of the NTLMv1 and SMBv1 protocols is a significant security risk. Communications in the network could be compromised, for example, by man-in-the-middle attacks.

Depending on the operating system, the procedure for deactivating protocols may differ.

4.4.5 Removing an SQL instance

Contents

With the installation of WinCC V20, a new Microsoft SQL Server 2022 instance is installed.

If you already had a version of WinCC Runtime Professional installed, the SQL server is updated automatically.

Note

By removing WinCC Runtime Professional or WinCC Professional you do not remove the instance of the SQL server.

Uninstalling an SQL instance

If you want to uninstall an instance of the Microsoft SQL Server, follow these steps:

1. Open the Control Panel.
2. Click "Remove program".
3. From the list of installed programs, select the version of Microsoft SQL Server to remove and click "Remove/change".
4. Click "Remove" in the dialog.
5. In the "Select instance" dialog, select the instance "WINCC" and click "Next".
6. In the "Select functions" dialog, click "Select all" and then "Next".
7. In the "Function rules" dialog, click "Next".
8. In the "Ready to uninstall" dialog, click "Remove".
9. After removal is complete, click "Close" in the "Completed" dialog.

Overview of processes and services of TIA Portal components

5

Additional processes and services are also installed during the installation of the TIA Portal or components of the TIA Portal.

The following tables provide an overview of these processes, the corresponding services and respective functions:

Table 5-1 Automation License Manager

Process	Corresponding service	Function
almsrv64x.exe	alm service	License management service / main process
almsrvbubble64x.exe	-	Process for tray icon info bubbles
almgui64x.exe	-	Graphical user interface of the Automation License Manager

Table 5-2 TIA administrator

Process	Corresponding service	Function
almsrv64x.exe	alm service	License management service
node.exe	SiemensAwb	Main process of the TIA Administrator website
TiaAdminNotifier.exe	-	User notifications and tray icon of the TIA Administrator

Table 5-3 ProSave

Process	Corresponding service	Function
PTProSave.exe	-	ProSave, graphical user interface main process
S7TraceService64x.exe	S7TraceServiceX	S7Dos related tracing
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event and parameter handling
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (accessibility via PN device name)
TraceConceptX.exe	TraceConceptX	S7Dos related tracing
ALMPanelPlugin.exe	-	Plugin for communication with Automation License Manager
-	S7DOS SCP Remote	Is also installed, but is only active with Cloud Connector
CommunicationSettings.exe	-	Setting access points

Table 5-4 WinCC Audit Viewer

Process	Corresponding service	Function
AuditViewer.exe	-	WinCC Audit Viewer main process

Table 5-5 Port Configuration Tool (PCT)

Process	Corresponding service	Function
Siemens.Simatic.Pct.ApplicationLoader.exe	-	Main process of the Port Configuration Tool (PCT)
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event and parameter handling
S7TraceService64x.exe	S7TraceServiceX	S7Dos related tracing
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (accessibility via PN device name)
TraceConceptX.exe	TraceConceptX	S7Dos related tracing
s7elonls64.exe	-	Routing between 32- and 64-bit application parts
CommunicationSettings.exe	-	Setting access points
-	S7DOS SCP Remote	Is also installed, but is only active with Cloud Connector

Table 5-6 Cloud Connector

Process	Corresponding service	Function
CloudConfigurator.exe	-	GUI for configuring the Cloud Connector
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event and parameter handling
S7TraceService64x.exe	S7TraceServiceX	S7Dos related tracing
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (accessibility via PN device name)
TraceConceptX.exe	TraceConceptX	S7Dos related tracing
CC.TunnelServiceHost.exe	S7DOS SCP Remote	Host of the tunnel service for the Cloud Connector
CommunicationSettings.exe	-	Setting access points

Table 5-7 Project server

Process	Corresponding service	Function
Siemens.Automation.Portal.Server(.exe)	prjserv	TIA Portal project server main process
Siemens.Automation.Portal.Project.Server(.exe)	-	TIA Portal project server main process
Siemens.Automation.Portal.Server.Configuration(.exe)	-	User interface for configuring the project server

Process	Corresponding service	Function
Siemens.Automation.Portal.Server.Administration(.exe)	-	User interface for the administration of the project server
Siemens.Automation.ProjectServer.AccessControl(.exe)	-	Controls the access authorization of the administration tool

Table 5-8 WinCC Runtime Advanced

Process	Corresponding service	Function
ScsServer.exe	-	Central data communication
StartCenter.exe	-	Start Center which permits starting of runtime, for example
HmiRTm.exe	-	The actual WinCC Advanced Runtime
s7elonls64.exe	-	Routing between 32- and 64-bit application parts
Miniweb.exe	-	Web contents of the WinCC Runtime Advanced
CodeMeterCC.exe	-	Runtime service of the code meter
CmWebAdmin.exe	CmWebAdmin.exe	Web administrator of the code meter
SmartServer.exe	cortsmartserver	Smart Server host process for remote connection
CodeMeter.exe	CodeMeter.exe	Code meter licensing during runtime
S7TraceService64x.exe	S7TraceServiceX	S7Dos related tracing
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event and parameter handling
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (accessibility via PN device name)
-	OpcEnum	Service is only installed, but not started.

Table 5-9 TIA Portal with STEP 7 / WinCC Comfort / Advanced

Process	Corresponding service	Function
CodeMeterCC.exe	-	Runtime service of the code meter
Siemens.Automation.Portal.exe	-	The TIA Portal itself
Siemens.Automation.ObjectFrame.FileStorage.Server.exe	-	Process for data management in TIA Portal projects
Siemens.Automation.Diagnostics.CrashDetector.exe	-	Process for detecting TIA Portal crashes and displaying the crash box
Siemens.Automation.Tracing.ETW.EventCollector.ServiceHost.exe	Siemens Diagnostics Data Collector Service	Process for event data collection
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event and parameter handling
CmWebAdmin.exe	CmWebAdmin.exe	Web administrator of the code meter
CodeMeter.exe	CodeMeter.exe	Code meter licensing during runtime
S7TraceService64x.exe	S7TraceServiceX	S7Dos related tracing

Process	Corresponding service	Function
Siemens.Simatic.TelemetryConnector.WindowsService.exe	Siemens Telemetry Connector Service	Service for collecting and sending telemetry data
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (accessibility via PN device name)
TraceConceptX.exe	TraceConceptX	S7Dos related tracing
IPCSecCom.exe	umscsvc	Communication to an UMC server
um.Ris.exe	-	Basic executable for UMC
um.sso.exe	-	Single sign-on for UMC
um.ess.exe	-	Basic executable for UMC
S7otbxsx64.exe	-	S7Dos block administration
-	OpcEnum	Service is only installed, but not started
-	UMC Service	Only used when UMC / UMAC is used
Siemens.Automation.Help.Viewer.Web.Service.exe	Siemens TIA Help Viewer Service	Enables the information system to be displayed in the default browser

Table 5-10 STEP 7 / Safety / WinCC Professional ES incl. simulation

Process	Corresponding service	Function
CodeMeterCC.exe	-	Runtime service of the code meter
Siemens.Automation.Portal.exe	-	The TIA Portal itself
Siemens.Automation.ObjectFrame.FileStorage.Server.exe	-	Process for data management in TIA Portal projects
Siemens.Automation.Diagnostics.CrashDetector.exe	-	Process for detecting TIA Portal crashes and displaying the crash box
Siemens.Automation.Tracing.ETW.EventCollector.ServiceHost.exe	Siemens Diagnostics Data Collector Service	Process for event data collection
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event and parameter handling
CmWebAdmin.exe	CmWebAdmin.exe	Web administrator of the code meter
CodeMeter.exe	CodeMeter.exe	Code meter licensing during runtime
S7TraceService64x.exe	S7TraceServiceX	S7Dos related tracing
Siemens.Simatic.TelemetryConnector.WindowsService.exe	Siemens Telemetry Connector Service	Service for collecting and sending telemetry data
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (accessibility via PN device name)
TraceConceptX.exe	TraceConceptX	S7Dos related tracing
IPCSecCom.exe	umscsvc	Communication to an UMC server
um.Ris.exe	-	Basic executable for UMC
um.sso.exe	-	Single sign-on for UMC
um.ess.exe	-	Basic executable for UMC
S7otbxsx64.exe	-	S7Dos block administration
CCDeltaLoader.exe	CCDeltaLoader	Responsible for determining whether a delta download is possible

Process	Corresponding service	Function
RedundancyControl.exe	RedundancyControl	Responsible for the determination and management of the state of the redundant WinCC partner
CCTextServer.exe	CCTextServer	Server for runtime display of texts
CCPerfMon.exe	CCPerfMon	WinCC STOBS, monitoring of the system parameters and WinCC processes
SCSFsX.exe	SCSFsX	WinCC File Service between clients and servers
CCRtsLoader_x64.exe	CCRtsLoader	WinCC RT Tag management
CCSystemDiagnosticsHost.exe	CCSystemDiagnosticsHost	Host for displaying system diagnostics
CcAlgRtServer.exe	CCAlgRtServer	WinCC Alarm Logging Runtime Server
CCArchiveManager.exe	CCArchiveManagerService	Management of WinCC archives
CCRedundancyAgent.exe	CCRedundancyAgent Service	Archiving component for managing and reconciliation of the RT archive
CCTlgServer.exe	CCTlgServer	WinCC Tag Logging Server
CCUsrAcv.exe	CCUsrAcv	Responsible for managing user archives
CCProfileServer.exe	CCProfileServer	Saving RT persistence data of the WinCC Controls
sqlservr.exe	MSSQL$WINCC	SQL server for WinCC
CCAgent.exe	CCAgent	WinCC RT component for communication between WinCC stations
CCEServer_x64.exe	CCEServer	WinCC RT component for communication between WinCC stations
CCProjectMgr.exe	CCProjectMgr	WinCC Project Manager, handling of WinCC projects
SDiagRT.exe	-	System diagnostics data collector
gscrt.exe	-	WinCC Global Script Runtime
PassDBRT.exe	-	Managing login data and passwords
CCUAImport.exe	-	WinCC RT User Archive component for importing TIA recipes
script.exe	-	WinCC RT C Scripting component
PdlRt.exe	-	Graphic runtime
SCSDistServiceX.exe	SCS Distribution Service	WinCC RT component for communication between WinCC stations
SCSMX.exe	SCSMonitor	WinCC RT component for communication between WinCC stations
sqlbrowser.exe	SQLBrowser	Microsoft SQL process (WinCC uses SQL server)
sqlwriter.exe	SQLWriter	Microsoft SQL process (WinCC uses SQL server)
CCDBUtils.exe	CCDBUtils	WinCC component for managing the WinCC SQL database
CCRemoteService.exe	CCRemoteService	WinCC component for remote management of the WinCC SQL database
sqlceip.exe	SQLTELEMETRY$WINCC	Microsoft SQL process (WinCC uses SQL server)

Process	Corresponding service	Function
CCEClient_x64.exe	CCEClient	WinCC RT component for communication between WinCC stations
RedundancyState.exe	RedundancyState	Client-side monitoring of the WinCC server states
CCPackageMgr.exe	CCPackageMgr	WinCC components for managing the server packages
CCNSInfo2Provider.exe	CCNSInfo2Provider	WinCC component for browsing WinCC/ STEP 7 tags
Siemens.Simatic.Srm.RdpComp.Data.ContextMgrX.exe	-	SCADA RT Professional Compiler component
CCDmRuntimePersistence.exe	-	WinCC RT component for reconciliation of the internal tags in redundant systems
CCWriteArchiveServer.exe	-	Responsible for writing archive data in the SQL database (3 instances: TLG-fast / TLG-slow / ALG)
CCLicenseService.exe	CCLicenseService	Responsible for allocation and release of licenses
CCUCSurrogate.exe	-	WinCC RT Professional application for the system tray icon in the Windows taskbar
Simulation.exe	-	WinCC RT Professional tag simulation
CCConfigStudio.exe	-	WinCC Config Studio is an application for the WinCC RT Professional tag simulation
WinCCChnDiag.exe	-	WinCC channel diagnostics
-	CCTMTimeSyncServer	Is used in redundant servers to synchronize time stamps
-	CcUaDAS	WinCC OPC UA component
-	CCOpcUaImporter	WinCC OPC UA component
-	CCAlgIAlarmDataCollector	WinCC RT Professional alarm system
-	SQLAgent$WINCC	Microsoft SQL process (WinCC uses SQL server)
-	OpcEnum	OPC Foundation component (WinCC OPC); Service is only installed, but not started
-	UMC Service	Only used when UMC / UMAC is used

Table 5-11 WinCC Advanced Runtime Simulation

Process	Corresponding service	Function
HmiRTm.exe	-	The actual WinCC Advanced Runtime
Miniweb.exe	-	Web contents of the WinCC Runtime Advanced
SmartServer.exe	cortsmartserver	Smart Server host process for remote connection
HmiRTmSim.exe	-	WinCC Advanced Tag Simulation

Table 5-12 WinCC Unified Engineering Package

Process	Corresponding service	Function
opcualds.exe	UALDS	OPC UA Local Discovery Service
mDNSResponder.exe	OPCF Bonjour Service	DNS name resolution
GfxWebBrowser.exe	-	Graphic rendering

Table 5-13 WinCC Unified Simulation

Process	Corresponding service	Function
WCCILS7pComDrv(.exe)	-	Process for communication with S7-1200 and S7-1500 controllers
RTILtraceTool(.exe)	TraceLogger_WinCC_Unified_PC	Unified Simulation related tracing
RTILtraceTool(.exe)	TraceProfiler_WinCC_Unified_PC	Unified Simulation related tracing
w3wp(.exe)	-	IIS Process Worker, host process for web pages
WCCILscs(.exe)	WCCILScsService	Siemens Communication Service, responsible for the internal data communication
WCCILpmon(.exe)	-	WinCC Process Monitoring
WCCILalg(.exe)	-	WinCC AlarmLogging, responsible for logging alarms
WCCILevent(.exe)	-	WinCC Event handling, responsible for handling events
GfxLicenseServer(.exe)	-	Responsible for granting and releasing licenses
JobSchedulerHost(.exe)	-	Responsible for scheduling jobs
GfxRTS(.exe)	-	Preparation of the graphical runtime
WCCILSDAMgr(.exe)	-	System Diagnostics Manager, responsible for the system diagnostics information
OpennessManagerHost(.exe)	-	Host for the Openness Manager
WCCILdist(.exe)	-	WinCC Unified Simulation basic process
WCCILdata(.exe)	-	WinCC Unified data manager
WCCILals(.exe)	-	WinCC AlarmServer, responsible for receiving and acknowledging alarms
WCCILpaco(.exe)	-	WinCC Parameter Control
WCCILtlg(.exe)	-	WinCC TagLogging, responsible for logging tags
WCCILs7(.exe)	-	Process for communication with S7-300 and S7-400 controllers
umcd(.exe)	UmclService	EMS basic process
idp(.exe)	UmclIdpService	EMS basic process
-	EventLogger	Event Logging Service
-	UmclWebUMService	Web service for User Management
-	umscsvc	User Management Secure Communication Service

Process	Corresponding service	Function
-	w3logsvc	IIS Logging Service
-	WMSVC	IIS Web Management Service
UAAppStarterHost.exe	UAAppStarterHost.exe	System function to jump from the web client to the TIA Portal for ProDiag scenarios.
OpcUAServerRTIL.exe	OpcUAServerRTIL.exe	Provides access to WinCC Unified via OPC UA protocol.
webums.exe	-	Web interface for user management with User Management Component (UMC) to manage UMC objects.
REPDataProviderHost.exe	-	Reporting enables the configuration of templates and the creation of Excel- and PDF-based reports on production data.
WCCILgraphQLServer.exe	GraphQL server	GraphQL Web API

Table 5-14 Add-Ins

Process	Corresponding service	Function
Siemens.Automation.AddIn.Rollout.Service.exe	Siemens Add-In Rollout Service	Mass rollout of Corporate Add-Ins

Using Security Logging

6

6.1 Security Logging in the TIA Portal

Security Logging in the TIA Portal is a function to acquire, save and analyze security-relevant event and log data from the Engineering System, as well as from components of the automation environment.

The event and log data is stored locally in Windows systems. This data can be analyzed, saved and exported through the Windows Event Viewer.

In a further step, the event and log data can be transferred to SIEM systems (**S**ecurity **I**nformation and **E**vent **M**anagement). Thus, Security Logging makes it possible to centrally collect and analyze security-relevant events from different systems in the network, and to react to threats. Security Logging is part of a bundle of measures recommended by international security standards and regulations for increasing security.

Security Logging is disabled by default in the TIA Portal. Administrators can initially activate Security Logging through a batch file. When Security Logging has been activated, the function can be deactivated and re-activated either by means of batch files or through the Windows Registry.

See also

Activating and deactivating Security Logging (Page 69)

6.2 Activating and deactivating Security Logging

The event channel for Security Logging is registered when the TIA Portal is installed on the computer; however, the function is disabled by default. You can activate and deactivate Security Logging in the Windows Registry by setting the corresponding value in the "AuditLogOn" key. The value "1" activates Security Logging while other values deactivate it. By default, Security Logging is deactivated in the TIA Portal.

The "AuditLogOn" key is not created at the time of installation of the TIA Portal. There are two batch files in the installation directory of the TIA Portal in the "bin" folder:

- The batch file "SecurityAuditLoggingEnable.bat" activates Security Logging.
- The batch file "SecurityAuditLoggingDisable.bat" deactivates Security Logging.

Security Logging is version-specific. The setting does not have any effect on other versions of the TIA Portal.

Requirements

- You have Windows administrator rights.
- To log user accounts, the project must be protected.

Activating Security Logging with a batch file

1. Navigate to the "bin" folder in the installation directory of the TIA Portal.
2. Run the batch file "SecurityAuditLoggingEnable.bat".

Deactivating Security Logging with a batch file

1. Navigate to the "bin" folder in the installation directory of the TIA Portal.
2. Run the batch file "SecurityAuditLoggingDisable.bat".

Activating and deactivating Security Logging in the Windows Registry

1. In Windows, open the Registry Editor.
2. Go to the "HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Automation\SecurityLogging\21.0\Settings" key.
3. To activate Security Logging, in the "LoggingOn" key, input the value "1".
   To deactivate Security Logging, in the "LoggingOn" key, delete or change the value "1".
4. Confirm your input with "OK".

See also

Security Logging in the TIA Portal (Page 69)

Overview of events (Page 70)

6.3 Overview of events

The following tables provide an overview of user actions, the relevant log entries, the event categories and event types:

In addition to the content of the events listed in the following tables, each event contains the following information:

- Version of the TIA Portal
- Name of the project
- Name of the logged-on user from the user administration (UMAC - User Management and Access Control)

Note

Name of the logged-on user

The value for the name of the logged-on user from the user administration (UMAC) is set in three different categories:

- Category 1: The text "No user logged in." appears in the case where user administration (UMAC) is either not enabled in the project or no user is logged on outside the project on a device under "Accessible devices".
- Category 2: The text "Background process" appears in the case where UMAC is enabled for the project but a safety-critical operation is triggered by a background process (e.g. when a process loads data into a device in Multiuser Commissioning in "asynchronous mode").
- Category 3: The name of the logged-on user from the user administration (UMAC) appears in the case where UMAC is enabled for the project and the event was written by the TIA Portal main process.

Overview of events

Table 6-1 User administration (UMAC - User Management and Access Control)

User action	Log entry	Event category	Type of event
Adding a local user	Local user "{target user}" added	Access control	Information
Deleting a local user	Local user "{target user}" deleted	Access control	Information
Adding a central user	Global user "{target user}" added	Access control	Information
Deleting a central user	Global user "{target user}" removed	Access control	Information
Adding a user group	User group "{target user}" added	Access control	Information
Deleting a user group	User group "{target user}" removed	Access control	Information
Logging on to a protected project	Local / Global user "{target user}" with role(s) "{semicolon seperated list of roles}" logged in successfully Local / Global user "{target user}" login failed Anonymous user with role(s) "{semicolon seperated list of roles}" logged in successfully Anonymous user login failed For Auto Log On No DSSO Session : Global user login failed as no desktop session is available	Access control	Information, errors

User action	Log entry	Event category	Type of event
Logging off from a protected project	Local / Global user "{target user}" logged out Anonymous user logged out	Access control	Information
Changing a user name of a local user	User "{target user}" renamed to "{new target user name}"	Configuration	Information
Changing the password of a local user or your own password	Local / Global user "{target user}" password changed	Configuration	Information
Activating a local user, central user or user group	Local / Global user / group "{target user}" activated	Configuration	Information
Deactivating a local user, central user or user group	Local / Global user / group "{target user}" de-activated	Configuration	Information
Changing the properties of a user	User "{target user}" property '{property name}' changed to {new property value}	Configuration	Information
Creating a user-defined role in the TIA Portal	Custom role "{role name}" created	Configuration	Information
Deleting a user-defined role in the TIA Portal	Custom role "{role name}" deleted	Configuration	Information
Renaming a user-defined role in the TIA Portal	Custom role "{old role name}" renamed to "{new role name}"	Configuration	Information
Changing the assignment of a function right to a user-defined role in the TIA Portal.	Custom role "{role name}" function rights assignment changed to "{semicolon seperated list of function rights}"	Configuration	Information
Changing the runtime timeout of a user-defined role in the TIA Portal	Custom role "{role name}" property 'Runtime timeout' changed to {new runtime timeout}	Configuration	Information
Assigning a role to a user or a user group	Local user / Global user / User group "{target user name}" roles assignment changed to "{semicolon seperated list of roles}"	Configuration	Information

Table 6-2 Changes to CPU data (offline)

User action	Log entry	Event category	Type of event
Checking project integrity	Data integrity check succeeded / failed. A {data integrity error type} Integrity corruption found in object {object id} in project {project name}	AuditLog	Supervision successful, error

Table 6-3 Loading to CPU

User action	Log entry	Event category	Type of event
Loading a hardware configuration to a CPU	Download of hardware configuration to {PLC name} with address {address}	Configuration	Supervision successful
Loading a standard user program to a CPU (Start alert)	Software download started to target PLC: {PLC name} with address {address} Operating mode during download: {RUN|STOP} Type of download: {Delta|Complete}	Configuration	Information
Loading a standard user program into a CPU (list of blocks to be loaded or deleted, if necessary several times)	Software objects downloaded (+) / deleted (-): {+|-} {full qualified name of object} {+|-} {full qualified name of object} ...	Configuration	Information
Loading a standard user program into a CPU (completion message with software signature)	Successful: Software download succeeded Software signature after sownload {signature|"null"} Error: Software download aborted with error: {error message} • PLC was left in an inconsistent state → Download in STOP • PLC software contents was rolled back → Download in RUN	Configuration	Supervision successful, error
Loading a failsafe program to a CPU	Downloaded safety program with the collective F-signature {collective F-signature}.	Configuration	Supervision successful

Table 6-4 Loading the device as a new station

User action	Log entry	Event category	Type of event
Loading a configuration from a CPU	Upload of {PLC name} with address {address}.	Configuration	Supervision successful, error

Table 6-5 Changes to CPU data (online)

User action	Log entry	Event category	Type of event
Accessing a CPU	Successful: Login to Plc {PLC name} with address {address} is successful. Error: Login to Plc {PLC name} with address {address} failed.	Access control	Supervision successful, error
Forcing variables via online access to a CPU	Forcejob installed on target CPU: {PLC name} with address {address} Forced variables (address : value): Adr1 : value1 Adr2 : value2 ... Forcejob on target PLC replaced: {PLC name} with address {address} Forced variables (address : value): Adr1 : value1 Adr2 : value2 ... Forcejob on target CPU stopped: {PLC name} with address {Address}	Configuration	Supervision successful
Changing the IP/network configuration of a CPU via online access	Change the network settings of {device name}({address}) to [IpAddress:{address to set}| SubnetMask:{subnet mask}| Router address:{router address}]	Configuration	Supervision successful, error
Changing the password for protecting confidential configuration data via online access	Set password for "Protection of PLC configuration data" of {PLC name}({address}) Delete password for "Protection of PLC configuration data" of {PLC name}({address})	Configuration	Supervision successful, error
Changing the operating state of a CPU via online access	Set {PLC name}({address}) to Run/Stop	Configuration	Supervision successful, error
Changing the system time of a CPU via online access	Change the system time of {device name}({address}) to {date time}	Configuration	Supervision successful, error

User action	Log entry	Event category	Type of event
Backing up/restoring a CPU via online access	Backup: Backup created from {PLC name} with address {address}. Restore: Online backup {backup name} restored to {PLC Name} with address {address}.	Configuration	Supervision successful
Initiating firmware update of a CPU via online access	Firmware update of {PLC name} ({address}) to version {fw version}	Configuration	Supervision successful, error
Resetting the CPU to factory settings	Reset to factory setting of {PLC name} ({address}). Settings: • Delete IP address • Delete master password • Format memory card	Configuration	Supervision successful, error
MRES via online access	Memory reset of {PLC name} {address}	Configuration	Supervision successful, error
Format memory card	Formatting the memory card of {PLC name}{address}	Configuration	Supervision successful, error

Table 6-6 Changing the access level

User action	Log entry	Event category	Type of event
Changing the access level	Protection access level is changed from "{previously selected access level}" to "{current selection access level}" for {PLC name}	Configuration	Supervision successful, error
Configuring the password for full access	Protection Access password is configured successfully / failed to configure for "Full Access" for {PLC name}	Configuration	Supervision successful, error
Changing the password for full access	Protection access password is changed successfully / failed to change for "Full Access" for {PLC name}	Configuration	Supervision successful, error
Configuring the password for full access including failsafe (no protection)	Protection access password is configured successfully / failed to configure for "Full access incl. fail safe (no protection)" for {PLC name}	Configuration	Supervision successful, error
Changing the password for full access including failsafe (no protection)	Protection access password is changed successfully / failed to change for "Full Access incl. fail safe (no protection)" for {PLC name}	Configuration	Supervision successful, error

User action	Log entry	Event category	Type of event
Configuring the password for read access	Protection access password is configured successfully / fail to change for "Read Access" for {PLC name}	Configuration	Supervision successful, error
Changing the password for read access	Protection access password is changed successfully / fail to change for "Read Access" for {PLC-name}	Configuration	Supervision successful, error
Configuring the password for HMI access	Protection access password is configured successfully / failed to configure for "HMI Access" for {PLC name}	Configuration	Supervision successful, error
Changing the password for HMI access	Protection access password is changed successfully / fail to change for "HMI Access" for {PLC name}	Configuration	Supervision successful, error

Table 6-7 Protection of CPU configuration data

User action	Log entry	Event category	Type of event
Deactivating protection of confidential CPU configuration data	"Protection of PLC configuration data" is disabled / failed to disable for {PLC name}	Configuration	Supervision successful, error
Activating protection of confidential CPU configuration data	"Protection of PLC configuration data" is enabled / failed to enable for {PLC name}	Configuration	Supervision successful, error
Configuring the password for protection of confidential CPU configuration data	Password for "Protection of PLC configuration data" is configured successfully / failed to configure for {PLC name}	Configuration	Supervision successful, error
Changing the password for protection of confidential CPU configuration data	Password for "Protection of PLC configuration data" is changed successfully / failed to change for {PLC name}	Configuration	Supervision successful, error
Resetting the password for protection of confidential CPU configuration data	Password for "Protection of PLC configuration data" is reset successfully / failed to reset for {PLC name}	Configuration	Supervision successful, error

Table 6-8 WinCC ES

User action	Log entry	Event category	Type of event
OPC UA: Toggle guest authentication	Device {deviceName}: OPC UA guest authentication {enabled | disabled}>	Configuration	Information
OPC UA: Toggle authentication by means of username and password	Device {deviceName}: OPC UA username and password authentication {enabled | disabled}	Configuration	Information

User action	Log entry	Event category	Type of event
Activating or deactivating an OPC UA server	Device {deviceName}: OPC UA server {activated | deactivated}	Configuration	Information
OPC UA: Activating or deactivating security policies	Device {deviceName}: OPC UA security policy {policyName} {enabled | disabled}	Configuration	Information
Runtime setting: Changing the maximum number of failed login attempts	Device {deviceName}: Account deactivation changed from {oldValue} to {newValue}	Configuration	Information
Runtime setting: Changing the maximum number of failed login attempts	Device {deviceName}: Account deactivation {enabled | disabled}	Configuration	Information
Runtime setting: Changing the central/local user management for Runtime	Device {deviceName}: UMAC source changed to {central | local}	Configuration	Information
Runtime setting: Changing central UMAC server password for Runtime	Device {deviceName}: Change of central UMAC server settings. {fieldName}: {oldValue} → {newValue}	Configuration	Information
Runtime setting: Changing the configuration in the Runtime security editor	Device {deviceName}: RT configuration change for configuration item {item}: {property}	Configuration	Information
Runtime setting: Changing the configuration in the Runtime security editor	Device {deviceName}: RT configuration change: {item} created.	Configuration	Information
Runtime setting: Changing the configuration in the Runtime security editor	Device {deviceName}: RT configuration change: {item} deleted.	Configuration	Information
Initiating online backup	Device {deviceName}: Online backup initiated	Backup, restore	Information
Initiating online restore	Device {deviceName}: Online restore initiated	Backup, restore	Information
Entering the transport password	Successful: Device {deviceName}: Transport password entered by user verified Error: Device {deviceName}: Failed to verify transport password entered by user	Access control	Supervision successful, error
Start downloading to device	Software download started to target {deviceName} with address {address}. Load Preview settings: {Listing of settings}.	Configuration	Information

User action	Log entry	Event category	Type of event
Configuring secure communication	Device {deviceName}: Secure communication was {enabled | disabled} for remote device with systemId {systemId}.	Configuration	Information
Configuring server settings of the smart server	Device {deviceName}: Smart Server service {service} {enabled | disabled}	Configuration	Information
Configuring settings of the web client	Device {deviceName}: Web Client is {enabled | disabled}	Configuration	Information
Changing authorization property for screen item	Device {deviceName}: Authorization property changed for item {screenItem} from {oldValue} to {newValue}	Configuration	Information
Creating transport password for loading of certificates and encrypted passwords for RT Advanced or Professional	Device {deviceName}: Transport password created	Configuration	Information
Changing transport password for loading of certificates and encrypted passwords for RT Advanced or Professional	Device {deviceName}: Transport password changed	Configuration	Information
Removing transport password for loading of certificates and encrypted passwords for RT Advanced or Professional	Device {deviceName}: Transport password removed	Configuration	Information
Creating a new device certificate	Device {deviceName}: Device certificate with fingerprint {fingerprint} created	Configuration	Information
Activating or deactivating know-how protection	Device {deviceName}: Know-how protection {enabled | disabled} for item {item}	Configuration	Information
Renaming a device	Device {oldDeviceName}: Device name changed to {newDeviceName}	Configuration	Information

See also

Security Logging in the TIA Portal (Page 69)

Displaying and managing events (Page 78)

6.4 Displaying and managing events

Events can be displayed and managed in Windows in the Event Viewer. In addition to this, functions are provided via Microsoft Windows to track events automatically.
To centrally collect, analyze and further process events from different systems in the network, events can be transmitted in a SIEM (**S**ecurity **I**nformation and **E**vent **M**anagement) system. Use the documentation of the provider for information on transferring events to a SIEM system.

Displaying events in the Event Viewer

1. In Windows, open the Event Viewer.
2. In the left-hand column, go to the node "Event Viewer (Local) > Application and Services Logs > SiemensAG > Automation > TIAPortal".
3. Select the "Operational" log.
   The events of the log are displayed in the upper part of the main window.
4. Select an event.
   Information on the selected event is displayed in the lower part of the main window, in the tabs "General" and "Details".
5. To open the information on an event in a new window, double-click the event.

Managing events in the Event Viewer

1. In the Event Viewer, switch to the right-hand column, "Actions".
2. Use the actions to manage your log files.
   You can, for example, filter, search, save and delete logs.

Automated event tracking

The following Microsoft Windows functions can be used for automated event tracking:

- The command line program **wevtutil** can be used to read events from the command line. The program is provided via Microsoft Windows.
- TIA Portal provides the events via **E**vent **T**racing for **W**indows - **ETW**. Applications (for example, a SIEM system) that wish to call the events can access these events via the event source "SiemensAG-Automation-TIAPortal".

For more information on implementing automated event tracing, use Microsoft's documentation of features.

See also

Security Logging in the TIA Portal (Page 69)

Installation log

7

Function of the installation log

The progress during the following installation processes is logged in a file:

- Installing products
- Modifying or updating already installed products
- Repairing an existing installation
- Uninstalling products

If errors occur during the installation process or warnings are issued, these can be evaluated with the help of the log file. You can do this yourself or contact product support.

Installation logs storage location

The log file is the most recent file with the file extension ".log" and the name of which that starts with "SIA". The storage location of the log file depends on the operating system, e.g. "C:\Program data\Siemens\Automation\Logfiles\Setup" in Windows. You can paste this path into the address bar of Windows Explorer.

After a certain time from the start of the Installation, the location of the log file is saved in the environment tag "%autinstlog%". You can enter this environment variable in the address bar of Windows Explorer to open the folder with the log files. Alternatively, you can navigate to the corresponding directory by entering "CD %autinstlog%" in the command line.

Setup_Report (CAB file)

To make it easier to provide Product Support with all necessary files, an archive file that contains the installation log and all other required files is saved in CAB format. This log can be found at "%autinstlog%\Reports\Setup_report.cab". Send this CAB file to Product Support if you need assistance with installation. With this information, Product Support can determine whether the installation was executed properly. CAB files that were generated during earlier installation processes are saved with a date ID in the "Reports" directory.

See also

Notes on licenses (Page 11)

Performing the installation (Page 87)

Checking availability of updates and support packages and installing them (Page 101)

Displaying the installed software (Page 93)

Modifying or updating installed products (Page 95)

Repairing installed products (Page 97)

Starting to uninstall (Page 99)

8 Checking the integrity

8.1 Basic information about the integrity check

Introduction

It is important to check the integrity and authenticity of the installation source and the installed products to ensure that no modified files are present. Siemens supplies the following two validators as command line tools:

- Integrity Validator
  The Integrity Validator is used to check the setup files of an installation source, i.e. an installation medium or downloaded software packages, for modifications. This validator is executed automatically at the beginning of an installation. The Integrity Validator is not installed on your system. You will find it in the installation source in the "IntegrityValidator" directory. From there, you can run it to perform an integrity check manually. You can use the "appsettings.json" configuration file to specify the path to the setup files.
- Installation Integrity Validator
  The Installation Integrity Validator is installed together with every Siemens product bundle that supports the software integrity check. Unlike the Integrity Validator, the Installation Integrity Validator is not executed automatically. You can run it yourself at any time to check the integrity of your system. If your system is connected to the Internet, it is recommended that you repeat this check at a certain time interval.

Both validators create a validation report during validation, in which you can see whether the integrity check was successful or failed. If the integrity check fails, you can see the possible reasons in the report.

More information on the topic of cybersecurity can be found online in the TIA documentation portal in the following document:

Cybersecurity in TIA Portal (https://docs.tia.siemens.cloud/access?ft:clusterId=CybersecurityTIAPortal&ft:locale=en-US)

8.2 Performing an integrity check

With the two validators "Integrity Validator" and "Installation Integrity Validator", you can check the integrity of the setup files before installation and of your system at any time after installation. Before you check your system with the Installation Integrity Validator, you should first ensure that it has been installed correctly. With the Integrity Validator, you have the option of customizing the path to the setup files. This is only necessary if you want to place the Integrity Validator outside the installation source.

Both validators have their own help, which you can call up in the command line with "-h" or "--help". This describes, for example, possible commands and the exit codes.

Changing the path to the setup files for the Integrity Validator

To change the path to the setup files, follow these steps:

1. Open Windows Explorer and navigate to the "IntegrityValidator" directory.
2. Open the "appsettings.json" file in a text editor.
3. Enter the desired path for "Path" in "InputDirectory".
4. Save the file.
   The Integrity Validator will now check the setup files that it finds under the specified path during validation.

Checking setup files with the Integrity Validator

To check the setup files with the Integrity Validator, follow these steps:

1. Open the Windows command prompt.
2. Navigate to the "IntegrityValidator" directory. This directory is in the installation source by default. If you have stored it somewhere else, go to that location.
3. To check the setup files, enter the following command:
   `IntegrityValidator.exe validate`
   The validation is performed and the result is displayed together with the exit codes.

Checking the installation of the Installation Integrity Validator

To ensure that the Installation Integrity Validator has been installed correctly on your system, follow these steps:

1. Open the Windows command prompt.
2. Enter the following command:
   `cd %COMMONPROGRAMFILES%\Siemens\Automation\Installation Integrity Validator\InstallationIntegrityValidator.exe --version`
3. Confirm the entry with <Return>.
   If the Installation Integrity Validator is installed correctly, the installed version of the tool will be displayed.

Checking the integrity of the system with the Installation Integrity Validator

To check the integrity of your system with the Installation Integrity Validator, follow these steps:

1. Open the Windows command prompt.
2. To start the validation, enter the following command:
   `cd %COMMONPROGRAMFILES%\Siemens\Automation\Installation Integrity Validator\InstallationIntegrityValidator.exe validate <if necessary, further options>`
3. Confirm the entry with <Return>.
   The validation is performed and the result is displayed together with the exit codes.
   See also: Error cases during the integrity check (Page 85)

8.3 Error cases during the integrity check

After the integrity check is performed with the Integrity Validator or the Installation Integrity Validator, the result of the validation is displayed. The colors of the texts have the following meanings:

- Green: Indicates a successful validation.
- Light blue: Displays information.
- Red: Displays validation errors and other error messages.
- Yellow: Displays warnings.

Possible error cases with suggested solutions

The following table shows the possible error cases with suggested solutions:

Error case	Suggested solution
Files missing	Reinstall the setup bundle that provided these files.
Additional files present	Delete the additional files.
Modified files present	Delete the modified files and reinstall the setup bundle that provided these files.
The catalog files for a directory were not found.	Reinstall the setup bundle that provided these files.
The installation directory for a product has not been found.	Contact the Siemens help desk and provide the installation logs.
The installation directory information for a product could not be retrieved.	Contact the Siemens help desk and provide the installation logs.
The self-check/integrity check for the CLI itself has failed for the Installation Integrity Validator. This means that the EXE file or the dependent assembly has been manipulated or is missing.	Reinstall the setup bundle to obtain a correct version of the Installation Integrity Validator.
Incorrect use of the "validate" command. Multiple verbosity modes have been specified.	Only one verbosity mode can be specified together with the "validate" command ("-v" or "-d"). Multiple verbosity modes are not allowed.

Performing the installation

9

Introduction

The installation of the software packages is carried out by a setup program that guides you through the installation.

Note

Integrity check

During the installation process, no additional integrity check is performed after the initial validation.
This poses a security risk in potentially compromised environments. Such conditions may lead to unauthorized changes to the installation process.
As a post-installation security measure, it is strongly recommended to perform the validation of all installed components (Page 83) to ensure their integrity and authenticity. In addition, the security measures contained in the document "Cybersecurity for Industry - Operational Guidelines" should be followed. You can find the document on the "Siemens ProductCERT and Siemens CERT (https://www.siemens.com/cert)" website.

Requirements

- The software packages to be installed are available either on an installation medium or as a download.
- Hardware and software of the programming device or PC meet the system requirements.
- You have administrator privileges on your computer.
- All other applications are closed.

Ensuring software integrity and authenticity

Before you start the Installation, you should make sure that your Installation source is trustworthy and was actually provided by Siemens. To do this, you can perform an integration check of your installation source. You can find more information in the "Performing an integrity check (Page 83)" section.

More information on how to ensure software integrity and authenticity can be found in the "Cybersecurity in the TIA Portal" document in the "Secure installation (https://docs.tia.siemens.cloud/access?ft:clusterId=cybersec_000011&;ft:locale=en-US)" section.

Starting the installation

To start the software package installation, follow these steps:

1. Navigate to the "Start.exe" file in the installation source and double-click it.
   The Windows dialog for the user account control is displayed.
2. If you want to be sure that the software package really comes from Siemens, click on "Show more details". Otherwise, continue with step X.
3. To display the certificate of the software package, click on "Show information about this publisher's certificate".
4. In the "Siemens AG" dialog, open the "Details" tab and scroll to the "Fingerprint" field.
5. Compare the fingerprint value with the value that is specified on the following Internet page for the software package:
   Valid certificates (https://docs.tia.siemens.cloud/access?ft:clusterId=cybersec_000010&;ft:locale=en-US)
6. After you have compared the fingerprint value, close the dialog "Siemens AG".
7. To continue the installation, confirm the user account control with "Yes".
   The start screen is displayed and the requirements are checked. This check may take some time to complete. If the check is successful, the dialog for selecting the installation language opens.

Selecting the installation language

You can carry out the installation in your preferred language. If you have previously installed other language packs, you can also select these languages as installation language.

To select the installation language, follow these steps:

1. Select the language in which you want the setup program dialogs to be displayed.
2. To read the information on the installation, click the "Read installation notes" button.
   The help file containing the notes opens.
3. Once you have read the notes, close the help file and click "Next".
   The dialog for selecting the product languages opens.

Selecting product languages

The product interface of the TIA Portal is available in various languages. The "English" product language is always installed as the base language and cannot be disabled. Additional languages are available via language packs.

To select the language for the product user interface, follow these steps:

1. Select the languages for the product user interface, and click "Next".
   A dialog with additional information on the products may open.
2. In this case, read the information and click "Next".
   The dialog for selecting the product configuration opens.

Selecting the product configuration

You can choose between two predefined configurations or select which products to install yourself. In addition, you can create a desktop shortcut and select the target directory.

To select the product configuration, follow these steps:

1. Select the products you want to install:
   - If you wish to install the program in a minimal configuration, click "Minimal". You can also select additional products here; the view then automatically switches to "User-defined". The product configuration "Minimal" is not changed as a result.
   - If you wish to install the program in a typical configuration, click "Typical". You can also select additional products here; the view then automatically switches to "User-defined". The product configuration "Typical" is not changed as a result.
   - If you wish to personally select the products to be installed, click "User-defined". Then select the check boxes for the products you wish to install.
2. If you want to create a shortcut on the desktop, select the "Create desktop shortcut" check box.
3. Click "Browse" if you want to change the target directory for the installation.

   Note

   Note the following:

   - The length of the installation path must not exceed 89 characters.
   - You can only change the installation path if no other product from the software package which you intend to install, has been installed, yet.
   - To increase security, select a directory that is protected by administrator rights as the target directory.
4. Click "Next".
   The dialog for the license terms opens.

Read and accept the license terms

To continue the installation, you must accept the Siemens license terms and confirm that you have read the security information. The security information can be found in the Readme files of the products.

1. Read the license terms carefully.
2. If you agree, select the two check boxes for the license terms and the security information. If you do not agree, you cannot continue with the installation.
3. Once you have selected the two check boxes, click "Next".
   The "TIA Help Viewer" dialog opens.

Specifying the port for the TIA Help Viewer

The new browser-based information system of the TIA Portal is displayed in your default browser. A free port is required for this. The default port number is "5112". This port number is checked and the result of this check is displayed.

1. If the "5112" port is valid, you can confirm this by clicking on the "Confirm" button. Optionally, you can also specify another free port and confirm this. When "Confirm" is clicked, a check is carried out as to whether this port number is already being used. If this is the case, enter a different port number and click "Confirm" again.
   The specified port is used to call up the information system in your default browser.
2. If you have entered a valid port number, click "Next".
   The "TIA Software Update server configuration" dialog opens.

Configuring TIA software update server

You can receive the software updates of the TIA Portal either via the TIA Automation Software Update Server from Siemens or via a company server.

1. Select the update server that you want to use:
   - No further configuration is required for the Siemens update server.
   - If you want to use a company server, you must specify the server path and the production line.
     More information on working with a company server can be found in the "Working with a company-internal server (Page 104)" section.
   - If you have already provided this information previously, you can select the "Use current settings" option. If you are no longer sure what your current settings are, you can check them in the TIA Administrator.
2. Click "Next".
   If changes to the security and permission settings are required in order to install the TIA Portal, the security settings dialog opens.

Accepting security settings

To continue the installation, you must accept the changes to the security and rights settings.

1. Read the changes to the security and rights settings thoroughly. Optionally, you can save the report via "Save report" or print it out via "Print report".
2. If you agree, select the check box for the security and rights settings. If you do not agree, you cannot continue with the installation.
3. Click "Next".
   The next dialog displays an overview of the installation settings.

Overview of the installation settings and starting the installation

You will receive an overview of all selected installation settings. You can check this before starting the installation and change it if necessary.

1. Check the selected installation settings.
2. If you want to make any changes, click "Back" until you reach the point in the dialog where you want to make changes. Once you have completed the desired changes, return to the overview by clicking "Next".
3. Click the "Install" button to start the installation.
   Installation is started.

   Note

   If no license key is found during the installation, you will be given the opportunity to transfer it to your PC. If you skip the license transfer, you can register it later with the Automation License Manager.

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

4. It may be necessary to restart the computer. If this is the case, select the "Yes, restart my computer now." option button.
   Then click "Restart".
5. If the computer does not reboot, click "Exit".

Result

TIA Portal along with the products and licenses you have ordered and the Automation License Manager have been installed on your computer.

See also

Installation log (Page 81)

Basic information about the integrity check (Page 83)

Notes on the system requirements (Page 47)

Notes on licenses (Page 11)

Displaying the installed software (Page 93)

Modifying or updating installed products (Page 95)

Repairing installed products (Page 97)

Starting to uninstall (Page 99)

Displaying the installed software

10

You can find out which software is installed at any time. In addition, you can display more information on the installed software.

Procedure

To display an overview of the software installed, follow these steps:

1. Click "Installed software" in the "Help" menu.
   The "Installed software" dialog opens. You will see the installed software products in the dialog. Expand the entries to see which version is installed in each case.
2. If you would like to display additional information on the installed automation software, click the link on the "Detailed information about installed software" dialog.
   The "Detailed information" dialog opens.
3. Chose the topic you want more information about in the area navigation.

See also

Notes on the system requirements (Page 47)

Notes on licenses (Page 11)

Performing the installation (Page 87)

Modifying or updating installed products (Page 95)

Repairing installed products (Page 97)

Starting to uninstall (Page 99)

Installation log (Page 81)

Modifying or updating installed products

11

You have the option to modify installed products using the setup program or to update to a new version.

Blocks with know-how protection from earlier versions of the TIA Portal are not automatically upgraded with the project. Remove the know-how protection of the blocks before you update the TIA Portal. Then set up the know-how protection with the current version of TIA Portal. For more detailed information, refer to the information system.

Requirement

- The software packages to be installed are available either on an installation medium or as a download.
- Hardware and software of the programming device or PC meet the system requirements.
- You have administrator privileges on your computer.
- All running programs are closed.
- Optional: You have checked the integrity and authenticity of the installation source.
  See also: Performing the installation (Page 87)

Procedure

To modify or update installed products, follow these steps:

1. Navigate to the "Start.exe" file in the installation source and double-click it.
   The dialog for selecting the setup language opens.
2. Select the language in which you want the setup program dialogs to be displayed. If you have previously installed other language packs, you can also select these languages as installation language.
3. To read the information on the installation, click the "Read installation notes" button.
   The installation instructions will be opened.
4. Once you have read the notes, close the help file and click "Next".
   The dialog for selecting the installation variant opens.
5. Select the "Modify/Upgrade" option button and click "Next".
   The dialog for selecting the product languages opens.
6. Select the check boxes of the product languages that you want to install. You can remove previously installed product languages by clearing the corresponding check boxes.

   Note

   Note that the product language "English" cannot be removed.

7. Click "Next".
   The dialog for selecting the product configuration opens.

8. Select the check boxes of the components that you want to install. You can remove previously installed components by clearing the corresponding check boxes.
9. Click "Next".

   Note

   Note that you cannot change the target directory because the existing installation is being modified.

   If changes to the security and permission settings are required in order to install the TIA Portal, the security settings dialog opens.
10. 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.
11. Click the "Modify" button.
    This starts the installation of the additional components.

    Note

    Following installation, you will receive a message indicating whether the existing installation was successfully changed.

12. It may be necessary to restart the computer. If this is the case, select the "Yes, restart my computer now." option button. Then click "Restart".
13. If the computer does not reboot, click "Exit".

Result

The existing installation has been modified on your computer.

See also

Notes on the system requirements (Page 47)

Notes on licenses (Page 11)

Displaying the installed software (Page 93)

Repairing installed products (Page 97)

Starting to uninstall (Page 99)

Installation log (Page 81)

Repairing installed products

12

You have the option to repair installed products by completely reinstalling them using the setup program.

Requirement

- The software packages to be installed are available either on an installation medium or as a download.
- Hardware and software of the programming device or PC meet the system requirements.
- You have administrator privileges on your computer.
- All running programs are closed.
- Optional: You have checked the integrity and authenticity of the installation source.
  See also: Performing the installation (Page 87)

Procedure

To repair installed products, follow these steps:

1. Navigate to the "Start.exe" file in the installation source and double-click it.
   The dialog for selecting the setup language opens.
2. Select the language in which you want the setup program dialogs to be displayed.
3. To read the information on the installation, click the "Read installation notes" button.
   The installation instructions will be opened.
4. Once you have read the notes, close the help file and click "Next".
   The dialog for selecting the installation variant opens.
5. Select the "Repair" option button and click "Next".
   The next dialog displays an overview of the installation settings.
6. Click the "Repair" button.
   This starts the repair of the existing installation.

   Note

   Following installation, you will receive a message indicating whether the existing installation was successfully repaired.

7. It may be necessary to restart the computer. If this is the case, select the "Yes, restart my computer now." option button. Then click "Restart".
8. If the computer does not reboot, click "Exit".

Result

The installed products have been reinstalled.

See also

Notes on the system requirements (Page 47)
Notes on licenses (Page 11)
Displaying the installed software (Page 93)
Modifying or updating installed products (Page 95)
Starting to uninstall (Page 99)
Installation log (Page 81)

Starting to uninstall

13

Introduction

The uninstallation of the software packages is carried out by a setup program, which guides you step by step through the entire uninstallation process.

You have two options for removing:

- Removing selected components via the Control Panel
- Uninstalling a product using the installation source

Note

The Automation License Manager will not be removed automatically when you remove the software packages, because it is used for the administration of several license keys for products supplied by Siemens AG.

Removing selected components via the Control Panel

To remove selected software packages, follow these steps:

1. Open the Control Panel.
2. Under "Programs", click "Programs and Features".
   A dialog with the list of installed programs opens.
3. Select the software package to be removed and click the "Uninstall" button.
   The dialog for selecting the setup language opens.
4. Select the language in which you want the dialogs of the setup program to be displayed and click "Next".
   The dialog for selecting the products you want to remove opens.
5. Select the check boxes for the products that you want to remove and click "Next".
   The next dialog displays an overview of the installation settings.
6. Check the list with the products to be removed. If you want to make any changes, click the "Back" button.
7. Click the "Uninstall" button.
   Removal begins.
8. It may be necessary to restart the computer. If this is the case, select the "Yes, restart my computer now." option button. Then click "Restart".
9. If the computer does not reboot, click "Exit".

Uninstalling a product using an installation source

Check the integrity and authenticity of the installation source, if necessary. See also: Performing the installation (Page 87)

To remove all software packages, follow these steps:

1. Navigate to the "Start.exe" file in the installation source and double-click it.
   The dialog for selecting the setup language opens.
2. Select the language in which you want the setup program dialogs to be displayed.
3. To read the information on the installation, click the "Read installation notes" button.
   The installation instructions will be opened.
4. Once you have read the notes, close the help file and click "Next".
   The dialog for selecting the installation variant opens.
5. Select the "Uninstall" option button and click "Next".
   The next dialog displays an overview of the installation settings.
6. Click the "Uninstall" button.
   Removal begins.
7. It may be necessary to restart the computer. If this is the case, select the "Yes, restart my computer now." option button. Then click "Restart".
8. If the computer does not reboot, click "Exit".

See also

Installation log (Page 81)

Notes on the system requirements (Page 47)

Notes on licenses (Page 11)

Displaying the installed software (Page 93)

Modifying or updating installed products (Page 95)

Repairing installed products (Page 97)

Installing updates and support packages 14

14.1 Checking availability of updates and support packages and installing them

By default, the TIA Portal checks automatically if new software updates or support packages are available, for example, Hardware Support Packages (HSPs). The automatic search for updates takes place after each computer restart and then cyclically every 24 hours. You can also deactivate the automatic search at any time or reactivate it. You can also search for updates manually.

If updates are found, you can download and install them.

Note

Updates and support packages from TIA Portal V13 or higher are supported.

Deactivate or activate automatic search for software updates

To deactivate or reactivate the automatic search for software updates, follow these steps:

1. Select the "Settings" command in the "Options" menu.
   The "Settings" window is displayed in the work area.
2. Select the "General > Software Updates" group in the area navigation.
3. Deselect the "Check for updates daily" check box if you want to deactivate the automatic search for software updates.
4. Select the "Check for updates daily" check box if you want to reactivate the automatic search for software updates.

Manually searching for software updates

If you want to search for software updates manually, follow these steps:

1. Click "Installed software" in the "Help" menu.
   The "Installed software" dialog opens.
2. Click "Check for updates".
   The TIA Administrator opens.
3. Click on the "Manage software" tile.
   The available updates are displayed.

Or:

1. Select the "Settings" command in the "Options" menu.
   The "Settings" window is displayed in the work area.
2. Select the "General > Software Updates" group in the area navigation.

3. Click "Check for updates now".
   The TIA Administrator opens.
4. Click on the "Manage software" tile.
   The available updates are displayed.

Or:

1. Open the TIA Administrator via "Start > All Programs > Siemens Automation > TIA Administrator".
2. Click on the "Manage software" tile and on the "Check for updates" button there.
   The available updates are displayed.

Setting the server

You must set the corresponding server depending on whether you want to download updates and/or support packages from the TIA Automation Update Server or from a corporate server. To do this, follow these steps:

1. Open the TIA Administrator.
2. Click "Options" and select the "TIA Automation Software Update Server" option in the dialog that appears in the "Server used to check for updates" area.
   The software searches for available updates on the server of the manufacturer.

Or:

1. Open the TIA Administrator.
2. Click "Settings" and select the "Corporate server" option in the "Software management" tab.
3. Enter the server URL which you received from your administrator. The URL must be entered either in the format https://[URL of the server]/[path to the file directory] or in the format https://[server IP address]/[path to the directory]. If you are not sure which format to use, contact your administrator!
   The software looks for available updates on the server of your company.
4. Check the name of the production line and change this if necessary "ProductionLine1" is set by default.
   The purpose of production lines is to provide different users with specific updates/support packages. If your company does not work with different production lines, retain the specified entry.
   You can find detailed information on creating projects and working with production lines in the help on the TIA Updater Corporate Configuration Tool.

You can set a different server on which the updates are to be searched for at any time. However, changing this setting is blocked during a download process. After switching the server, all downloaded updates and support packages are displayed, even if they are not available on the currently set server.

Installing updates/support packages

For the exact procedure for installing updates/support packages, refer to the TIA Administrator help.

Alternative procedures for the installation of support packages

Another procedure is available for the installation of a support package. To do this, follow these steps:

1. Click "Support packages" in the "Options" menu of the TIA Portal.
   The "Detailed information" dialog opens. A table lists all support packages from the directory that you selected as the storage location for support packages in the settings.
2. If you want to install a support package that is not in the list, you have the following options:
   - If the support package is already on your computer, you can add it to the list by selecting "Add from file system".
   - If you add a support package from the "Service & Support" page on the Internet, first you download it by selecting "Download from the Internet". Then you can add it from the file system.
3. Select the support package that you want to install.
4. Click "Install".
5. Close and then restart the TIA Portal.

See also

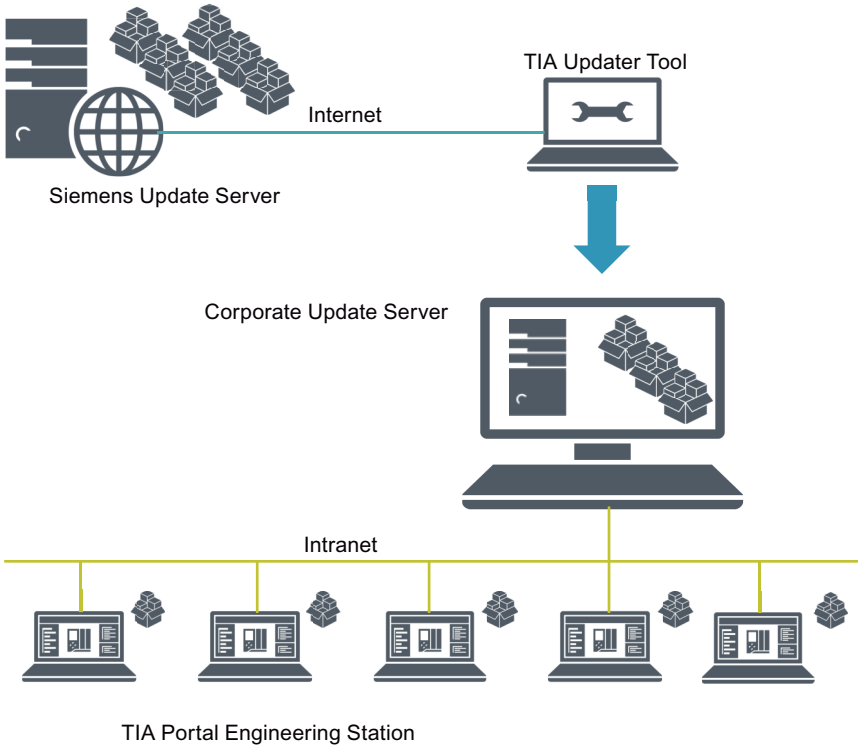
Installation log (Page 81)

14.2 Working with a company-internal server

14.2.1 Properties and advantage of a corporate server

Introduction

Using a corporate server, you can place selected updates / support packages on a local server and make them available to users, e.g. for different production lines. This has the advantage that users do not have to access the Internet, but can install updates via the intranet, an external hard disk, etc. Since users do not need direct access to the Internet, the protection against trojans or malicious software that contacts the Internet from the internal company network is significantly increased.



Configuring the server and creating projects

In the first phase, the corporate server is configured by a server administrator and the updates / support packages are deployed using the TIA Updater Corporate Configuration Tool. In addition, projects for different production lines can be created through which users can receive the updates they require. Users need to have access to the server area and have the name of the production line and be informed about the storage directory.

You can find detailed information on creating projects and working with production lines in the help on the TIA Updater Corporate Configuration Tool.

Working with the server

With the TIA Updater, users can download and install the updates and support packages that are relevant and relevant for them. Multiple download operations can be initiated at the same time. The installation of the updates / support packages must be done one after the other.

14.2.2 Configuring a corporate server for updates

Introduction

To provide available updates, support packages and language packages to users from a central location, you must configure a corporate server. Use the Microsoft Server Manager to do this.

The following is an example of the steps required to create and configure the server using the TIA Updater Corporate Configuration Tool (with the Microsoft Server 2016 operating system). Further settings which may be required for operation in your company are **not** covered in this description!

Note

Please note that the structure of the start menu and the storage location of the programs may vary depending on the different operating systems.

For more detailed information on configuration and operating the Server Manager, refer to the Microsoft help.

Requirement

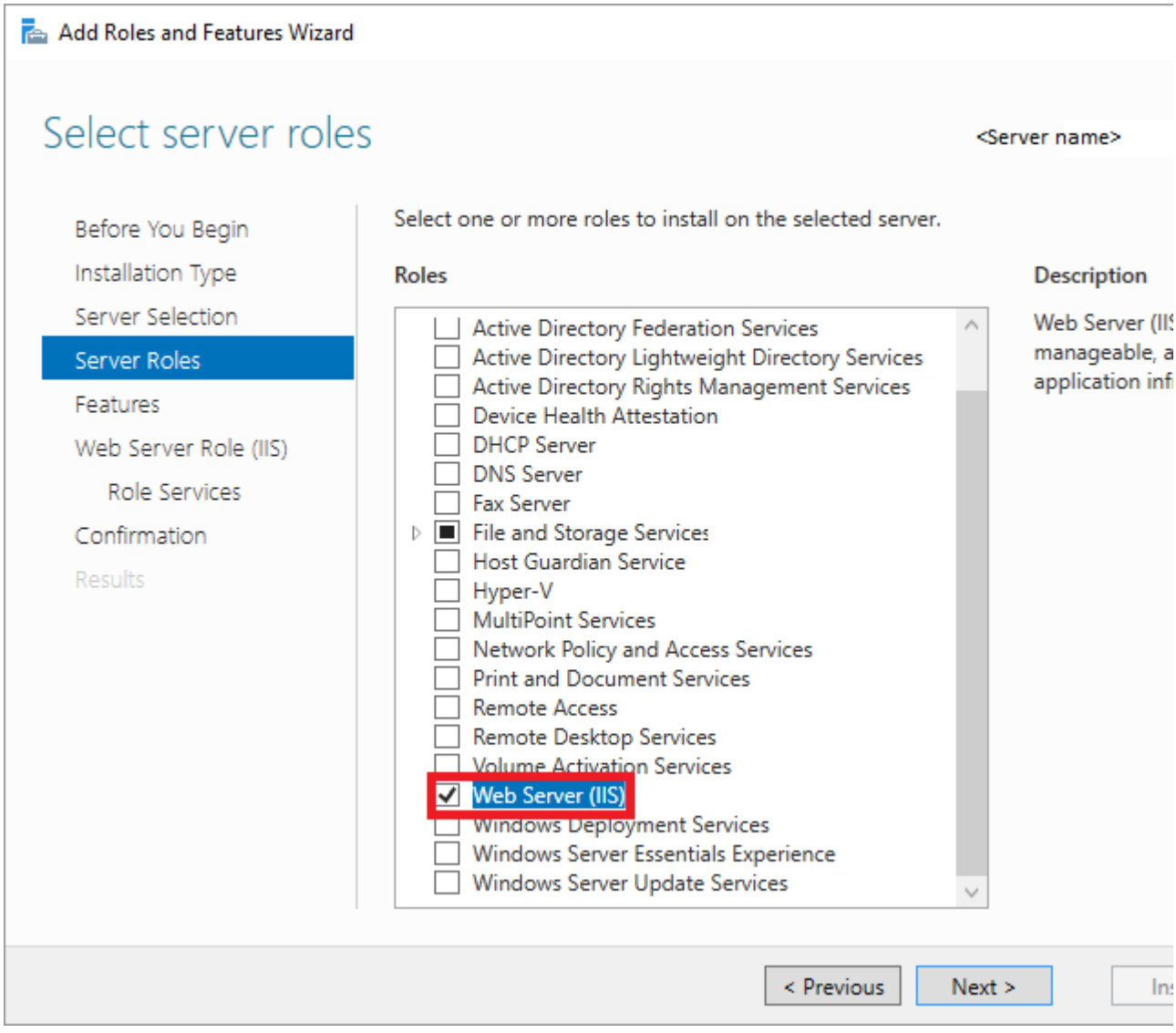
You must have administrator rights.

Install Web server role (IIS)

To install the required Web server role, follow these steps:

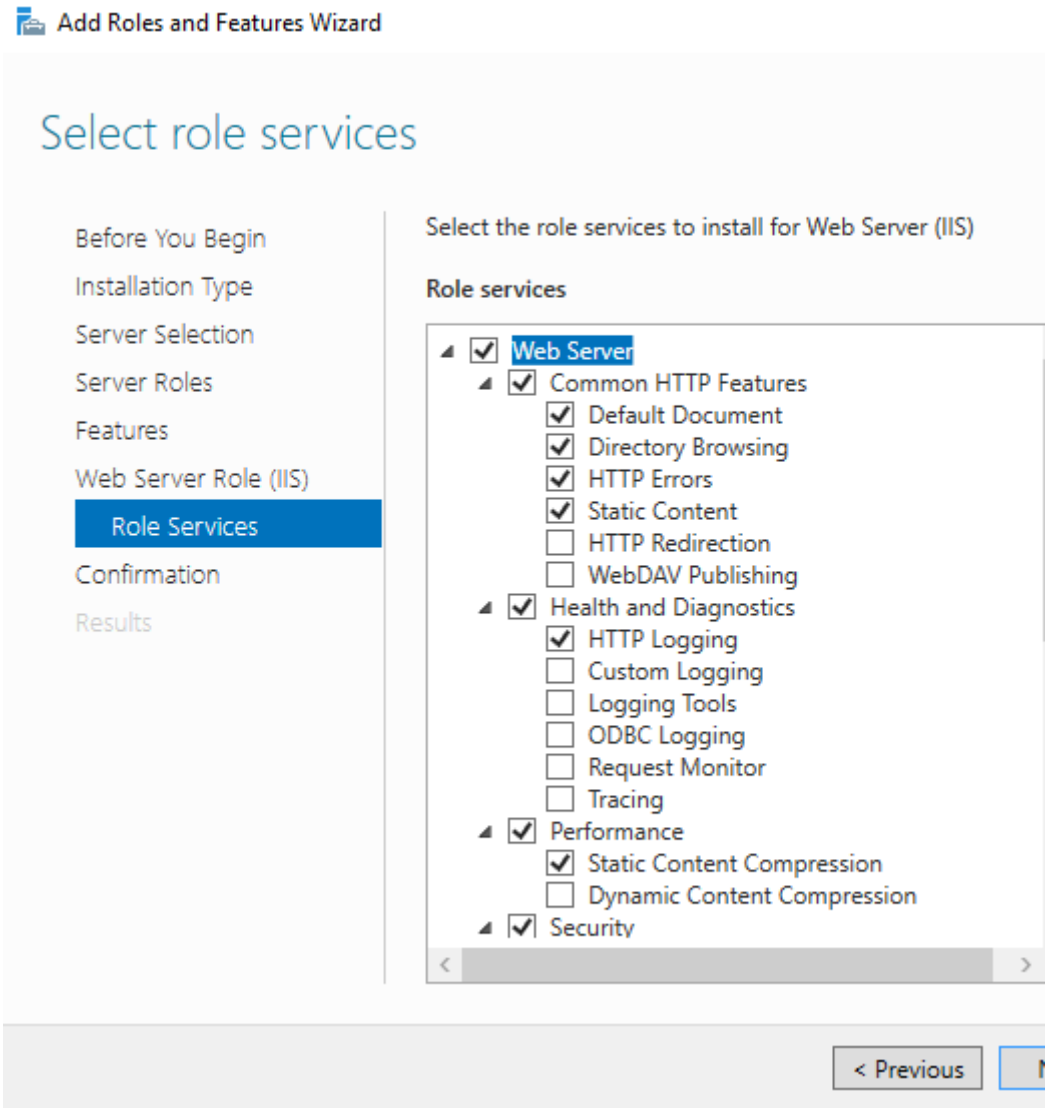
1. Open the start menu and select "Server Manager".
2. Click "Add roles and features" in the dashboard.
3. Use the "Add roles and features" wizard to add the Web server roles.
   Before the wizard starts, it is verified that a complex password has been assigned to the administrator, that the network settings have been configured accordingly and that the latest Windows security updates have been installed.
4. Select "Role-based or feature-based installation" as the installation type and click "Next".
5. Select the target server and click "Next".

6. Note the pre-selected roles that are installed by default, and then select the additional role "Web Server (IIS)".



7. Click "Add features" followed by "Next". The features for the web server are displayed.

8. Click "Role Services" and make sure that the following features are selected or select them:



"Web server" area

- Default document
- Directory browsing
- HTTP errors
- Static content

"Health and diagnostics" area

- HTTP logging
- Request monitor

"Performance features" area

- Static content compression

"Security" area

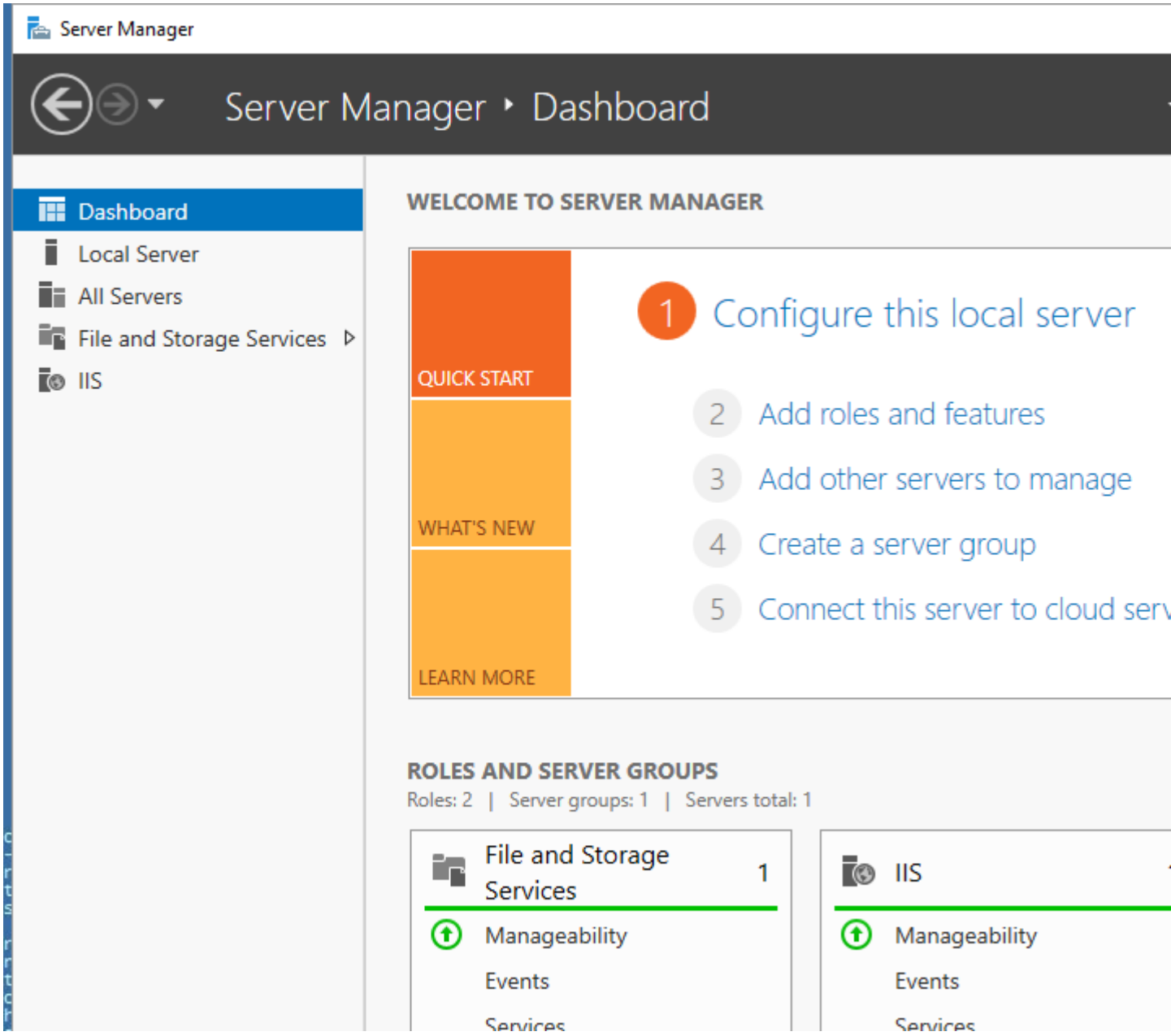
- Request filtering

"Application Development Features" area

- .NET Extensibility 3.5
- .NET Extensibility 4.6
- ASP.NET 3.5
- ASP.NET 4.6
- ISAPI Extensions
- ISAPI Filters

9. Click "Next".
10. Check your selection in the "Confirm installation selection" dialog box and click "Install".

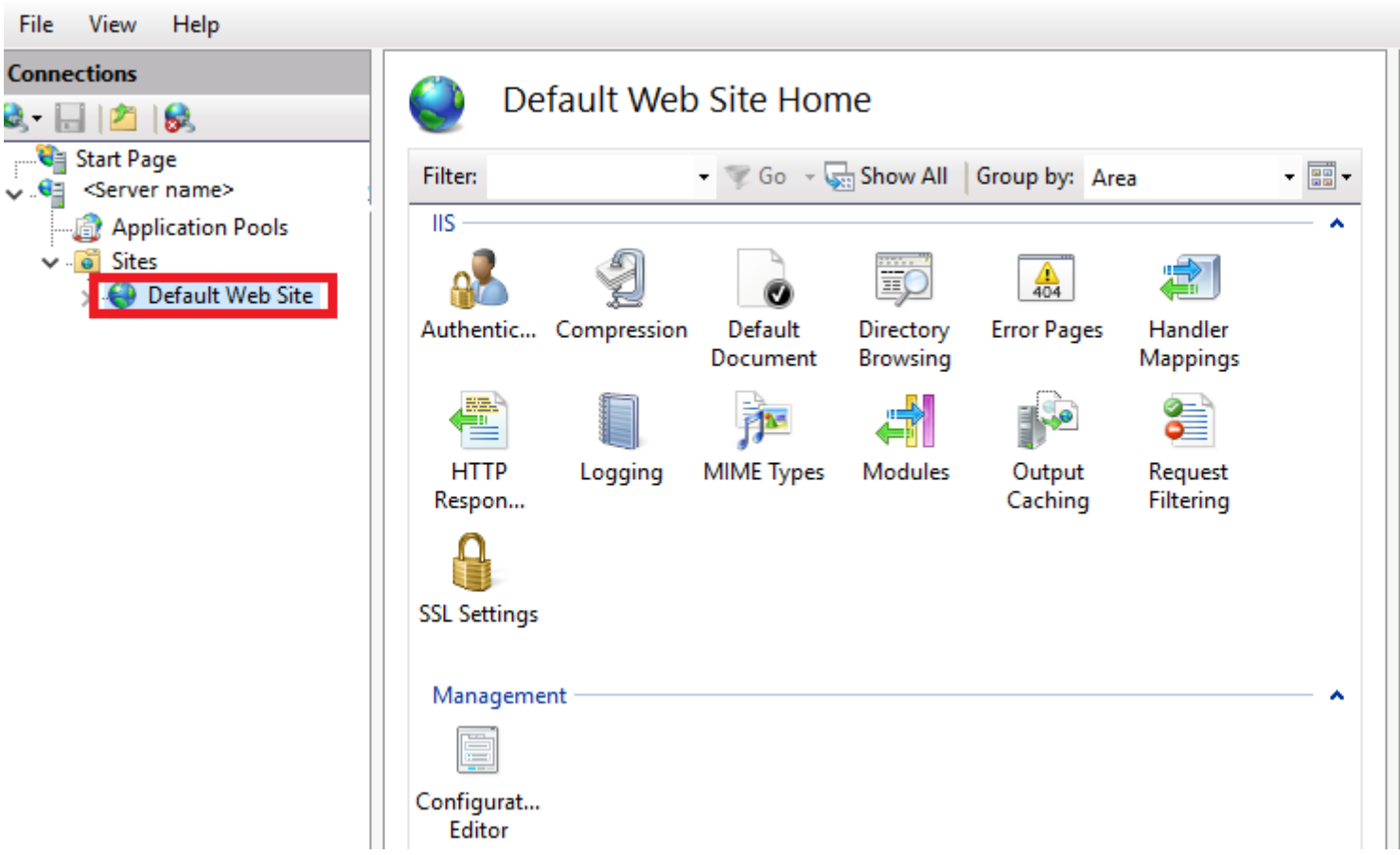
"IIS" is added in the dashboard and can be further configured.



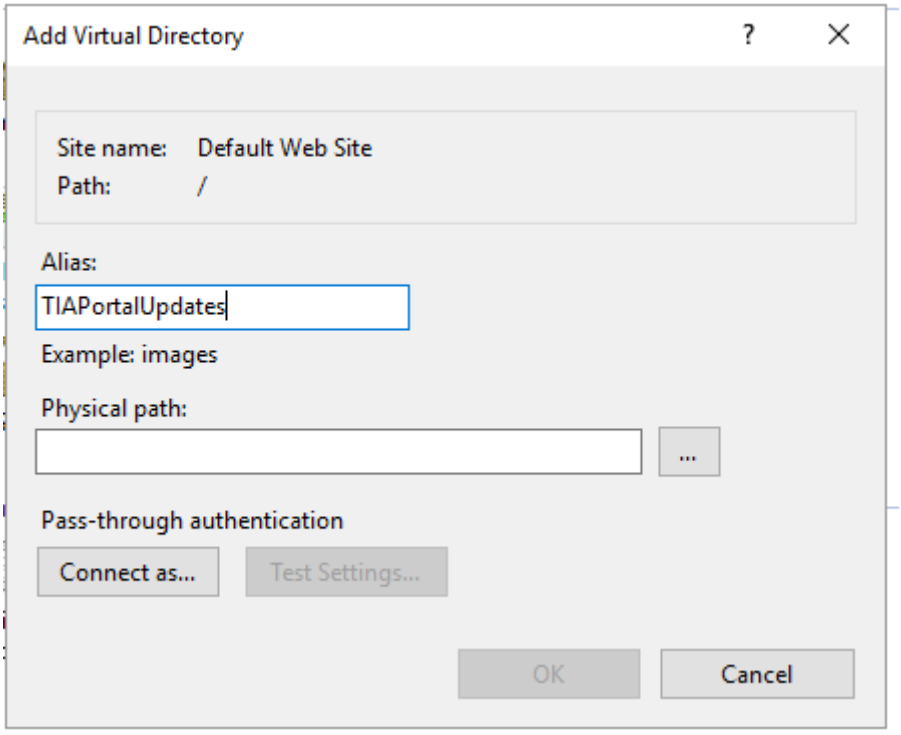
Create website

1. In the navigation area, click "IIS" and right-click in the "Servers" area and select "Internet Information Services (IIS) Manager".
2. In the "Connections" area, click "Sites" and then "Default Web site".

3. Right-click to select the "Add Virtual Directory..." option.



4. In the dialog that opens, enter a display name in the "Alias" field, for example, "TIAPortalUpdates".



5. In the "Physical Path" field, enter the physical path of the folder in which the website is located or click the button to browse (**...**), in order to search for the folder in the file system.

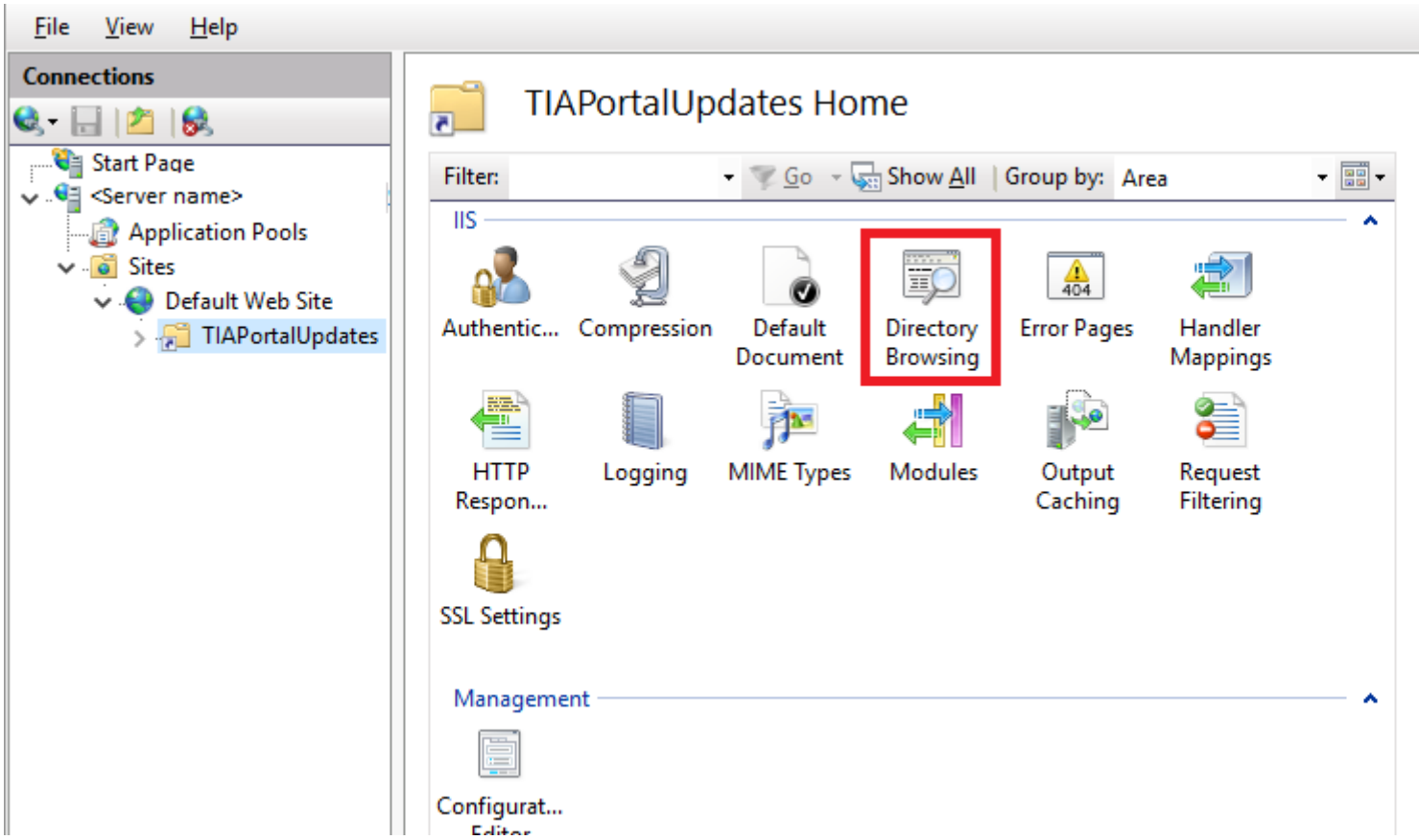
Note

The default website must be created in the directory that contains the 'UpdatesSummaryCatalog.xml' file.

6. Click "Test Settings..." to check whether the settings are correct.
7. Click "OK".

Activating virtual directory

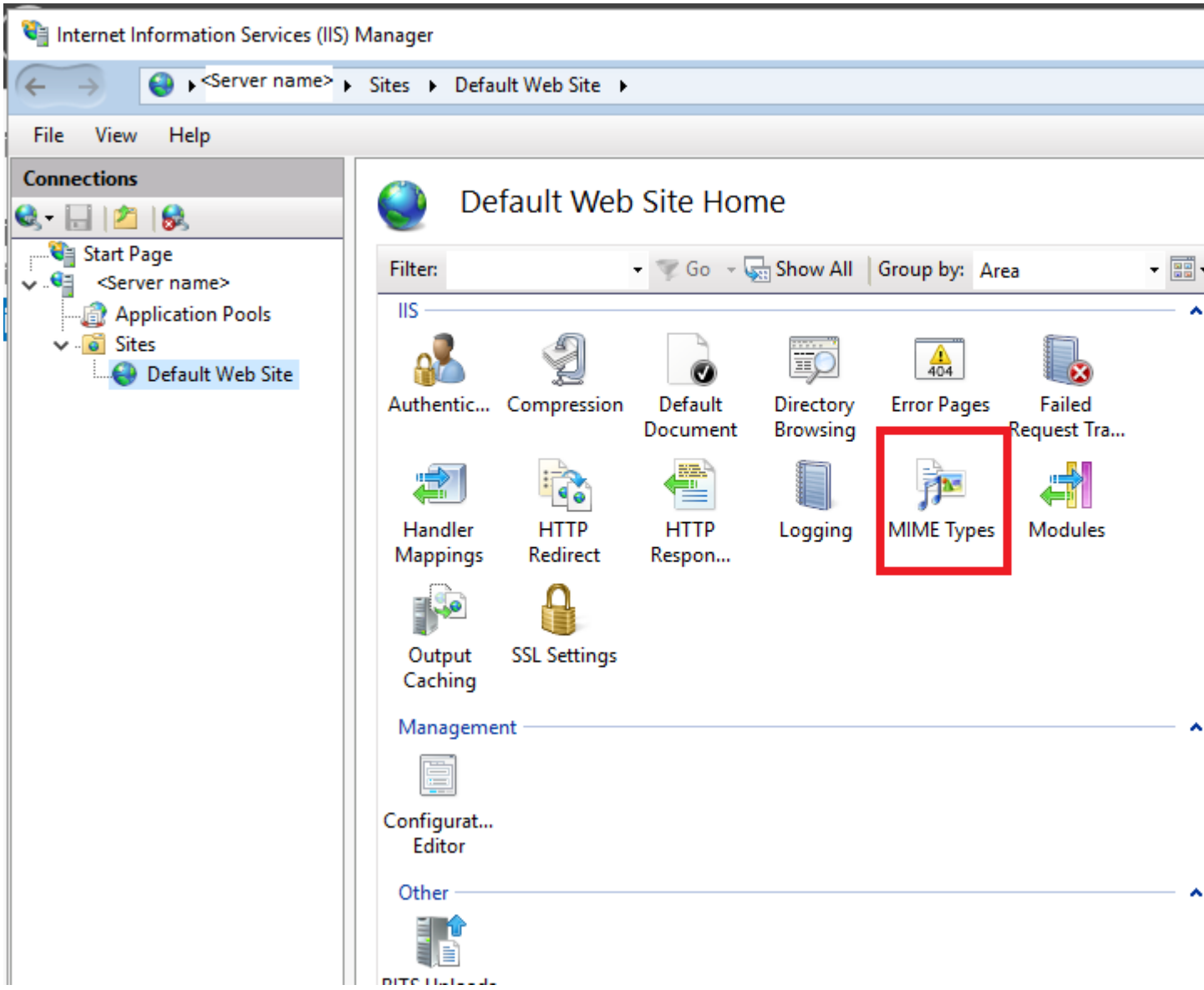
1. In the area "Connections > Sites > Default Web site", select the virtual directory you created.
2. In the "Features" view, double-click the item "Directory browsing".



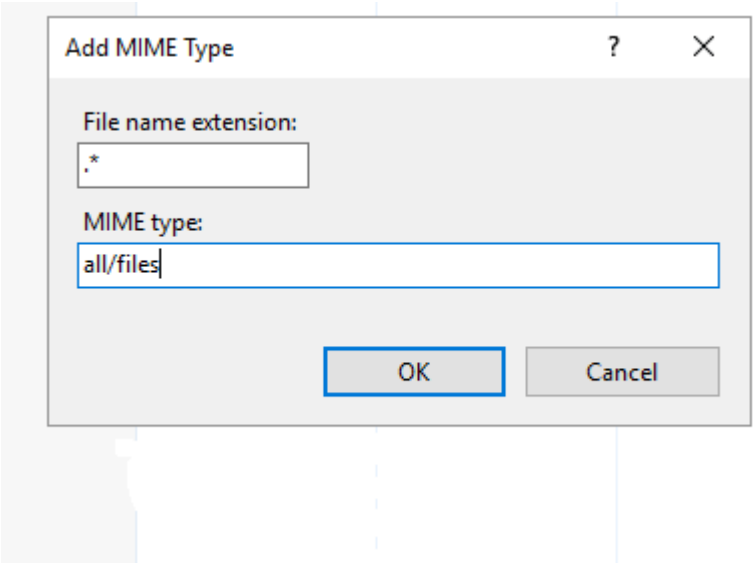
3. Click "Enable" in the "Actions" area.

Adding and configuring MIME type

1. In the "Connections" area, select the website you created.
2. Double-click "MIME type" in the "Features" view.

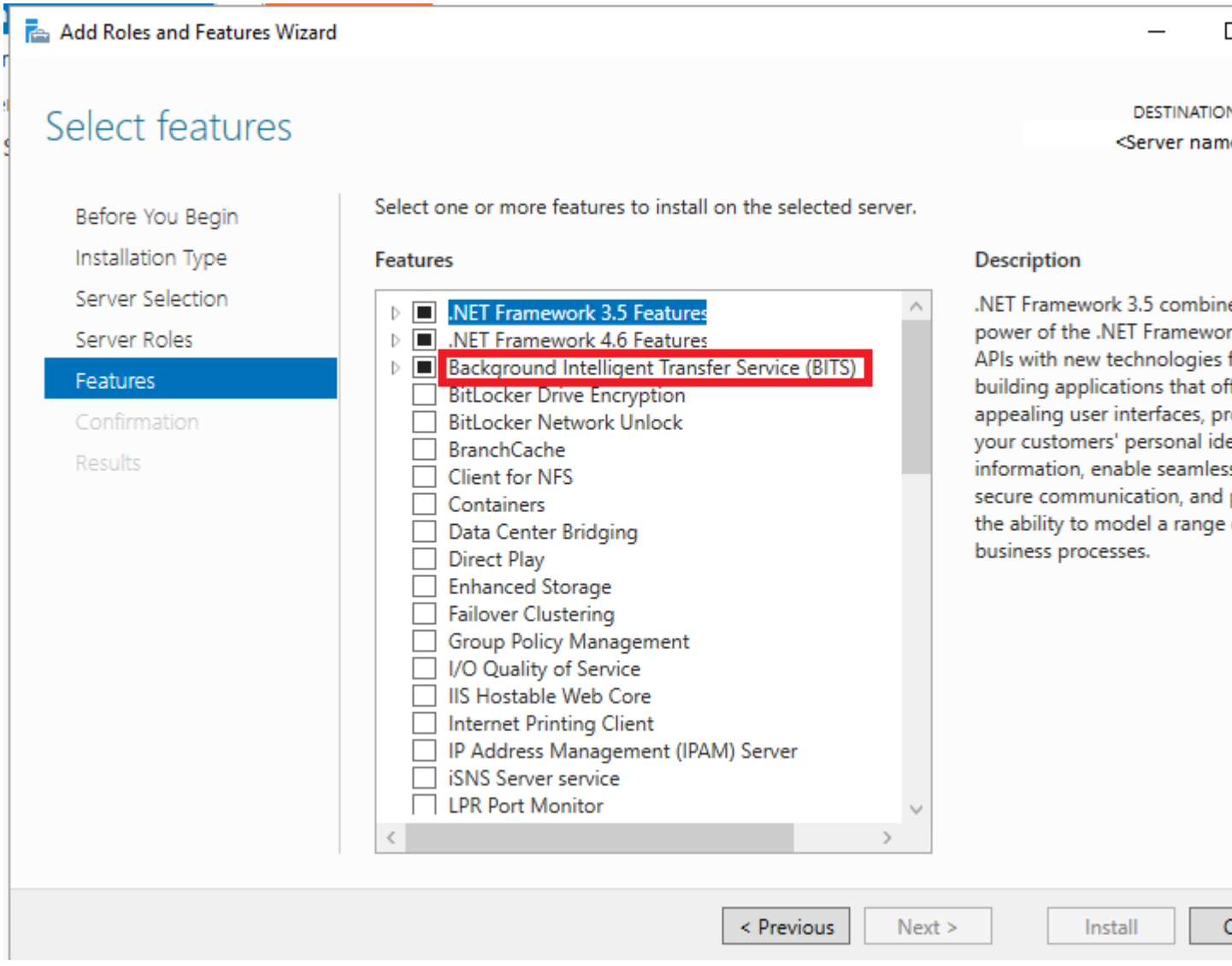


3. Click "Add" in the "Actions" area.
4. Enter .* in the "File name extension" text field in the "Add MIME type" dialog.
5. Enter "all/files" in the "MIME type" text field.
6. Click "OK".

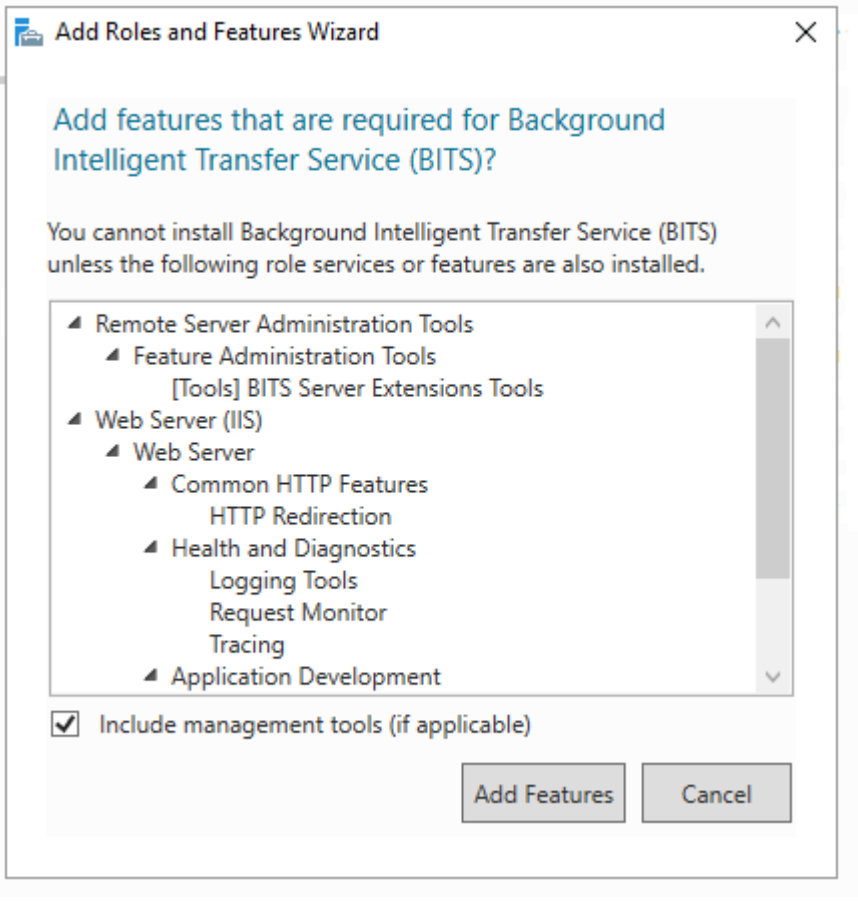

Add MIME Type
File name extension:
.*
MIME type:
all/files
OK
Cancel

Activate BITS-IIS server extension

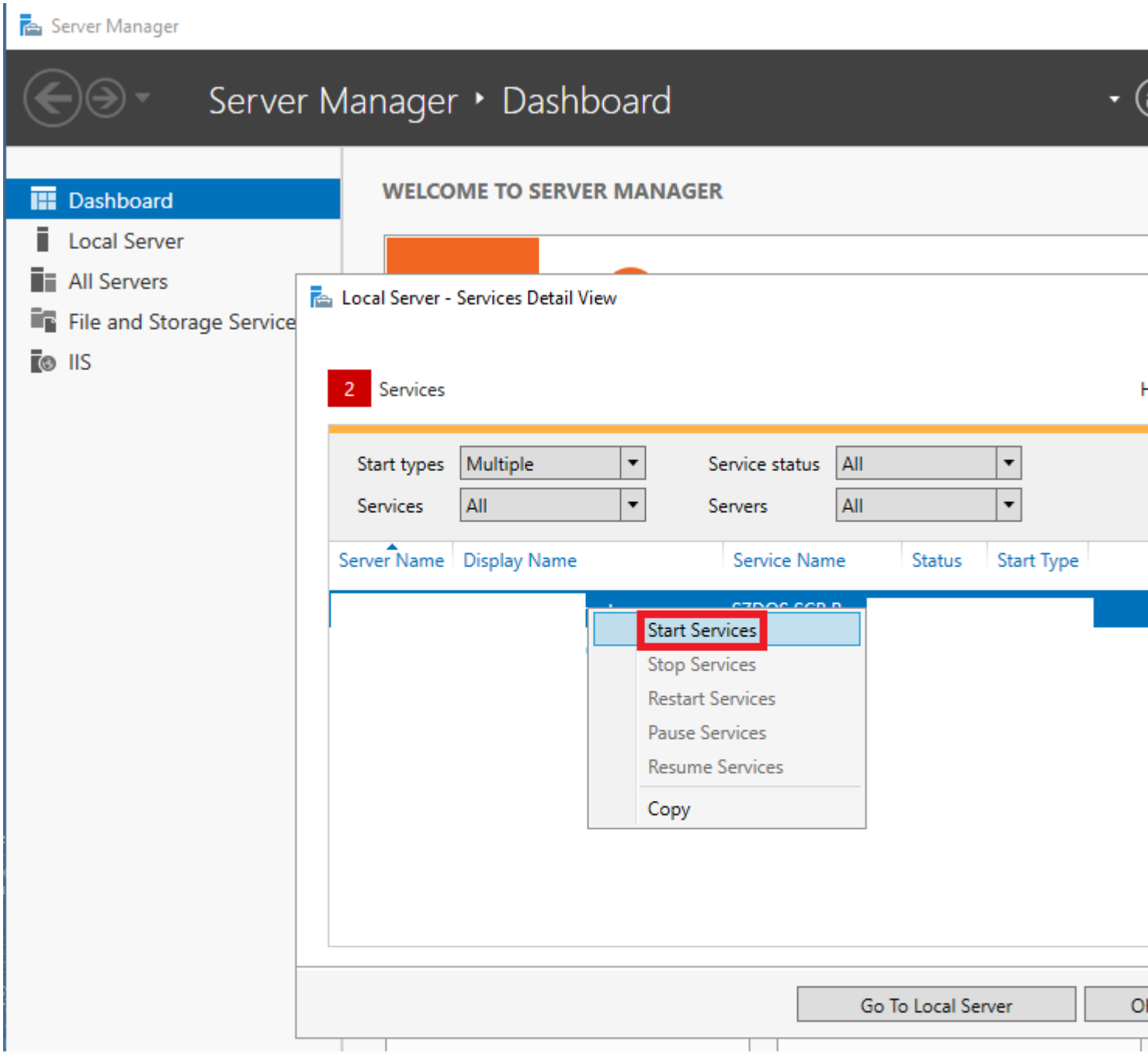
1. Switch to the virtual directory in the IIS Manager.
2. Click "Add roles and features" to verify that BITS is installed. If necessary, enable and install the "Background Intelligent Transfer Service" feature.



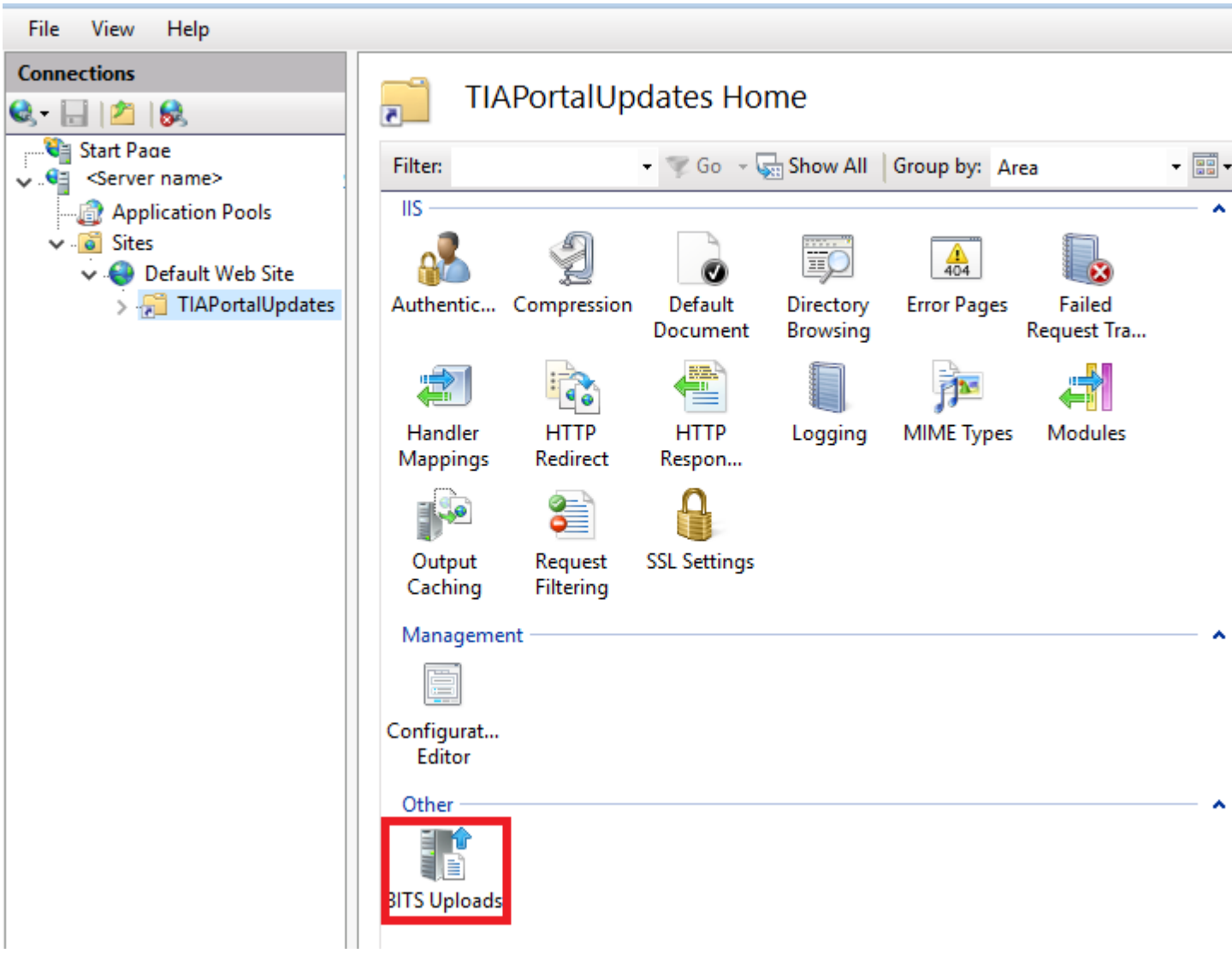
3. In the Dashboard, in the "Local Server" area, click "Services".



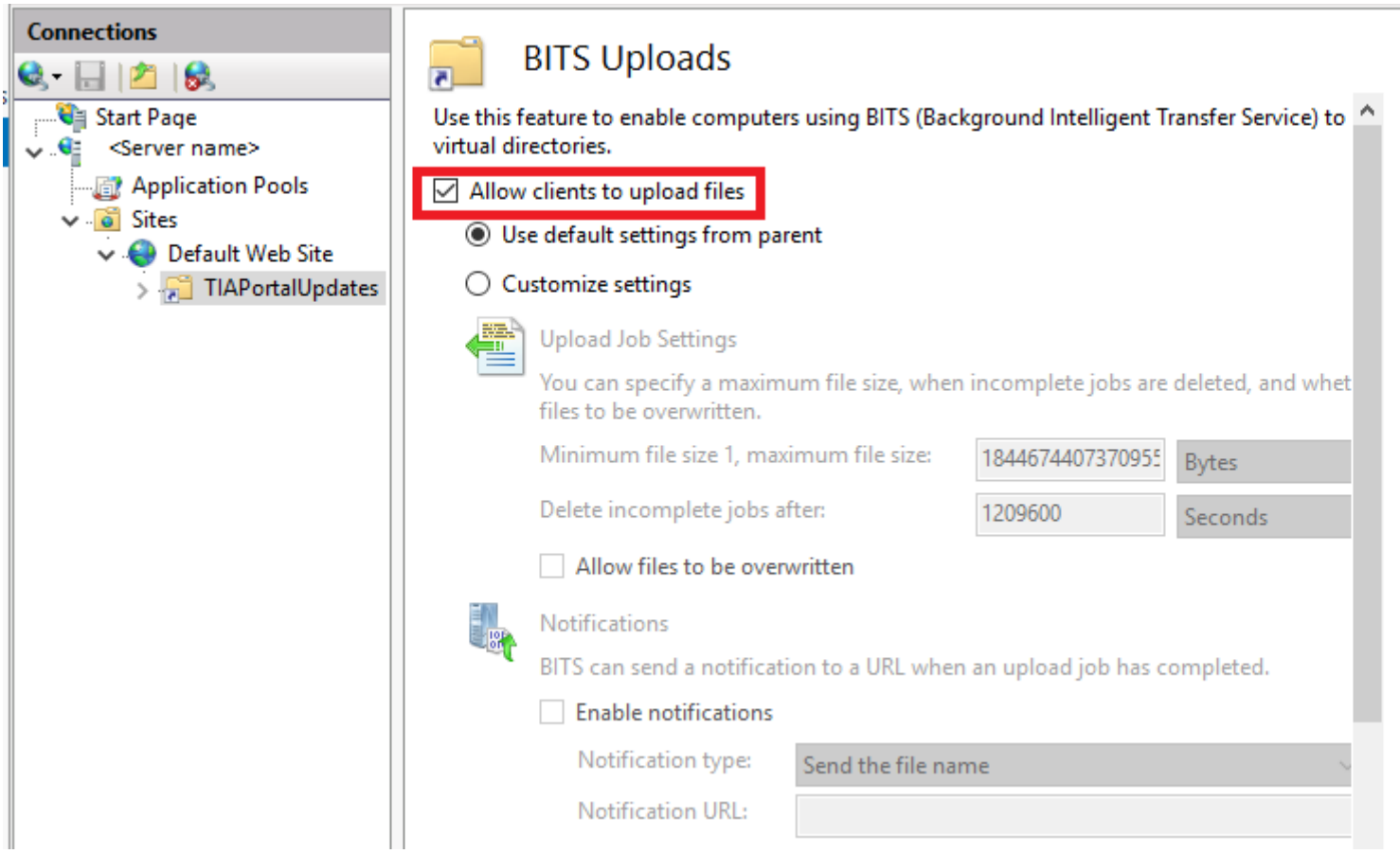
4. Select the local server, right-click and select the menu command "Start Services".


Server Manager
Server Manager ‣ Dashboard
Dashboard
Local Server
All Servers
File and Storage Service
IIS
WELCOME TO SERVER MANAGER
Local Server - Services Detail View
2 Services
Start types Multiple
Service status All
Services All
Servers All
Server Name
Display Name
Service Name
Status
Start Type
Start Services
Stop Services
Restart Services
Pause Services
Resume Services
Copy
Go To Local Server

5. Change to the virtual directory feature view and double-click "BITS Uploads".



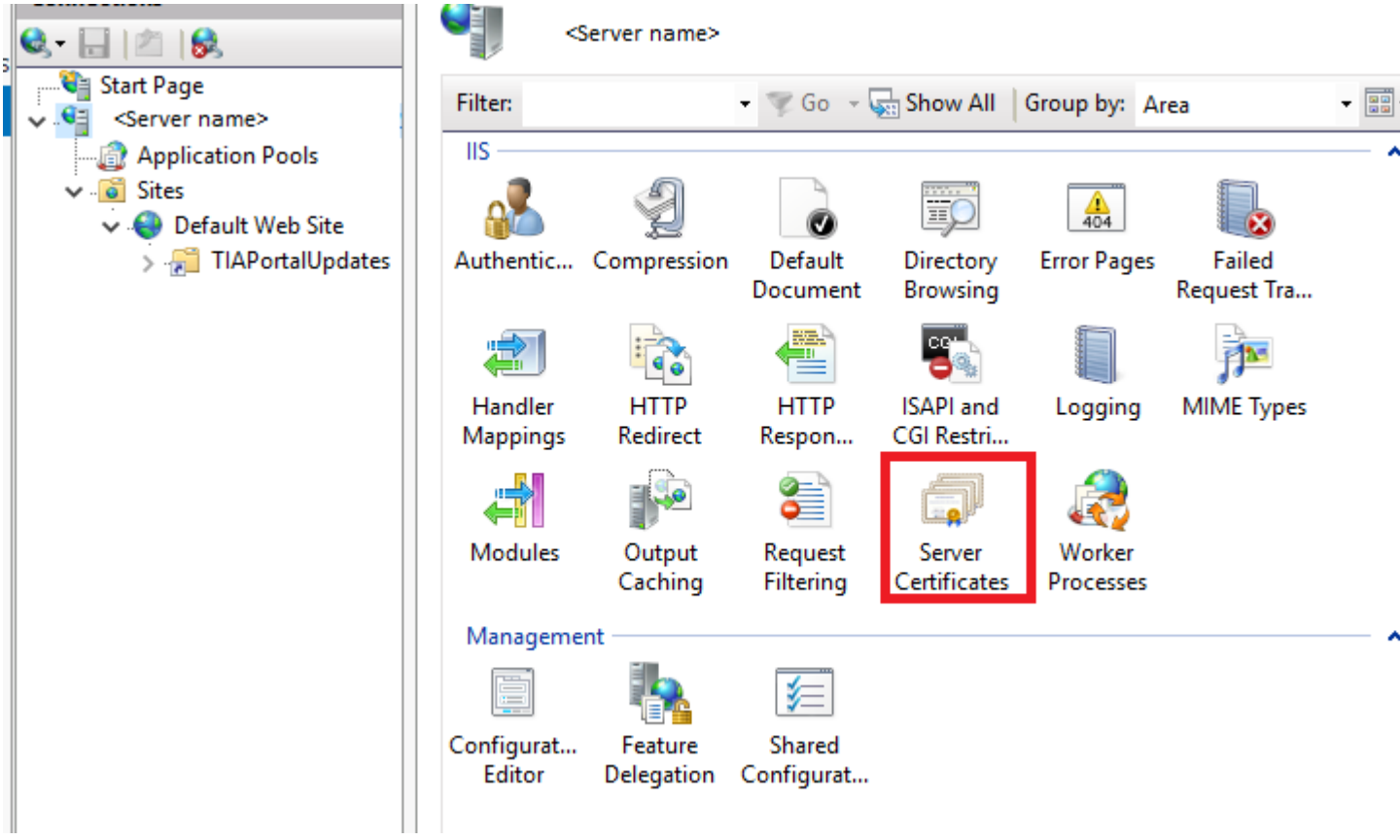
6. Select the "Allow clients to upload files" check box and click "Apply".


Connections
Start Page
<Server name>
Application Pools
Sites
Default Web Site
TIAPortalUpdates
BITS Uploads
Use this feature to enable computers using BITS (Background Intelligent Transfer Service) to virtual directories.
Allow clients to upload files
Use default settings from parent
Customize settings
Upload Job Settings
You can specify a maximum file size, when incomplete jobs are deleted, and whet files to be overwritten.
Minimum file size 1, maximum file size:
18446744073709555
Bytes
Delete incomplete jobs after:
1209600
Seconds
Allow files to be overwritten
Notifications
BITS can send a notification to a URL when an upload job has completed.
Enable notifications
Notification type:
Send the file name
Notification URL:

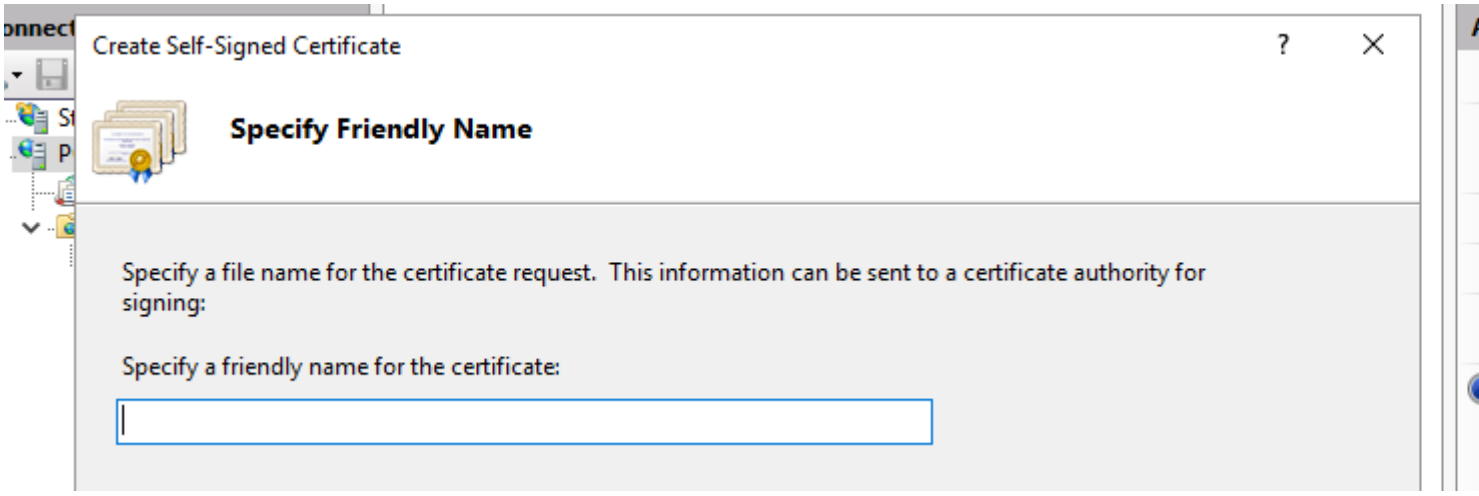
Create a self-signed server certificate

It is strongly recommended that you use a signed certificate created by your company's IT department; in this way the company's own server receives a qualified (secure) certificate. You can also purchase such a certificate from trusted third-party companies/certification authorities. If this is not possible for you, you can create a self-signed certificate. Note that such a certificate is not secure! To do this, follow these steps:

1. In the "Connections" area, navigate to the level which you want to manage.
2. Double-click "Server Certificates" in the "Features" view.



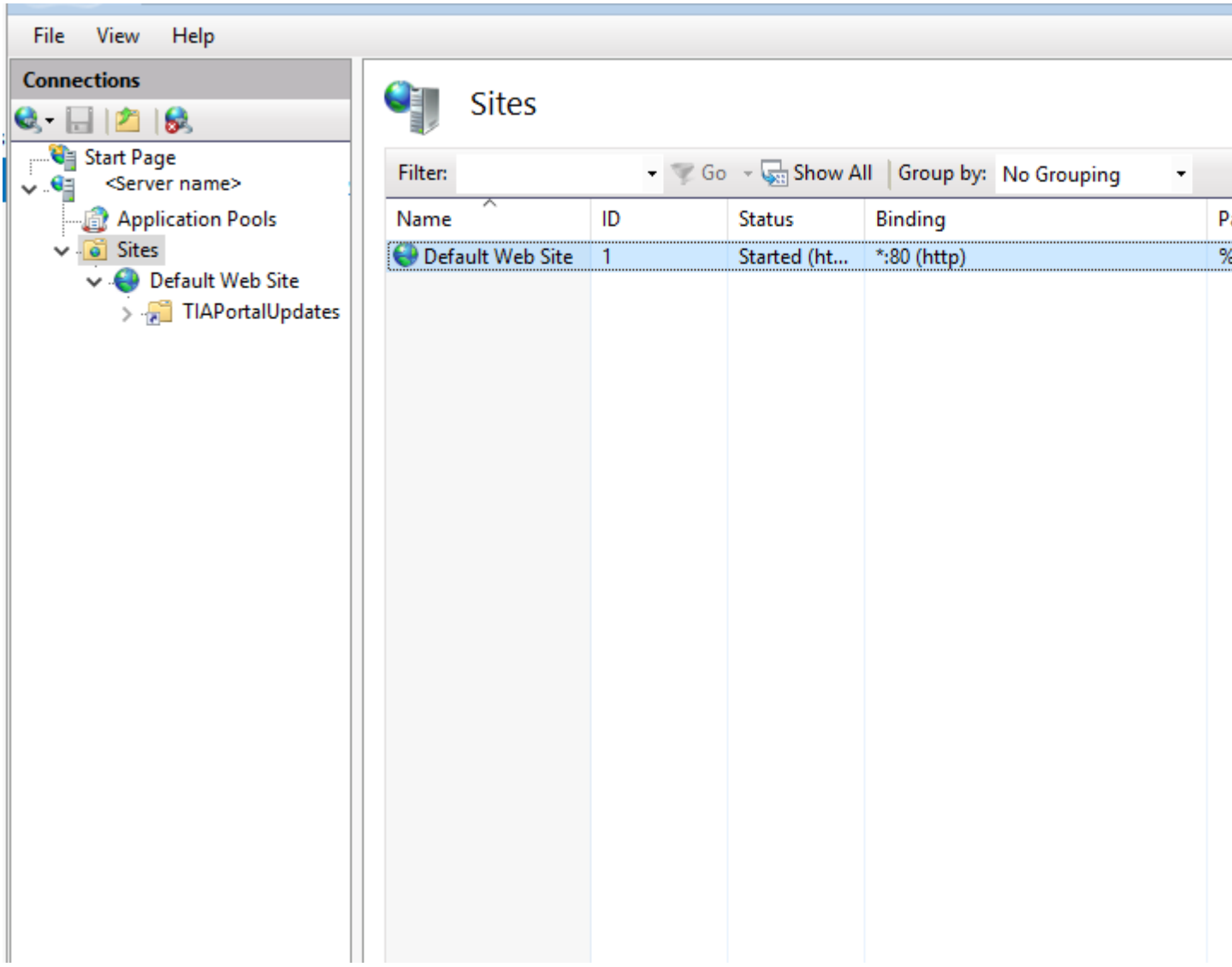
3. Click "Create Self-Signed Certificate" in the "Actions" area.



4. In the "Create Self-Signed certificate" dialog, enter a display name for the certificate in the "Specify a friendly name for the certificate" field and click "OK".

Create SSL binding

1. Expand the "Sites" entry in the "Connections" area, and then click the site to which you want to add a binding.
2. Click "Bindings" in the "Actions" area.



3. In the "Site Bindings" dialog, click "Add".
4. In the "Add Site Binding" dialog, select the certificate you created under "Type" "https" and under "SSL certificate" and then click "OK".

Verify SSL binding

1. In the "Actions" area, click the previously created binding under "Browse website".
   An error page is opened in Internet Explorer, because the self-signed certificate was created by your computer.
2. Click "Continue to this website (not recommended)".
   This message is no longer displayed when you add the certificate to the "Trusted Root Certification Authorities" certificate memory.

Configure SSL settings

1. Double-click "SSL settings" in the "Features" view.
2. Use one of the following procedures in the "Client certificates" area of the "SSL Settings" dialog:
   - Select "Ignore" if no client certificates are to be accepted even if a client has a certificate.
   - Select "Accept" if client certificates are to be accepted.
   - Select "Require" if client certificates are to be required. The "Require SSL" option must be activated to allow the "Require client certificates" option to be used.
3. Click "Apply" in the "Actions" area.

14.2.3 Distributing updates to different areas

It may be the case that different departments need different updates or support packages. In this situation, we recommend creating multiple production lines which offer different updates and support packages. The procedure for this is described in the help of the TIA Updater Corporate Configuration Tool.

Note

The main advantage of different production lines is that less storage space is required. When an already downloaded update, support package, or language pack is added to a new production line, a copy of it is not created, instead, the various production lines reference that update, support package, or language pack.

Procedure

You can also operate multiple servers that provide different updates, support packages, and language packs. To do this, follow these steps:

1. Set up different company-owned servers as described above.

or

1. Set up different company-owned servers as described above.
2. Set up multiple websites.
   Make sure that you assign unique names for these websites and the physical paths so that there will be no confusion.
3. Set the features described previously for the Web server or the websites.

You can now store the required updates and support packages for the different departments in the defined directories.

14.2.4 Providing updates on a corporate server

Introduction

In the TIA Updater Corporate Configuration Tool, you can set a corporate server on which the available updates/support packages/language packs are stored and can be made available to the users.

Requirement

You must have administrator rights.

A corporate server can only be set up on a Microsoft server operating system, because it requires the operation of the BITS IIS service and a running IIS sever.

Adding updates from the TIA Automation Software Update Server

To add updates from the TIA Automation Software Update Server, follow these steps:

1. Open the TIA Updater Corporate Configuration Tool.
   The available updates are displayed.
2. Click the "Add update" button and select the "Add TIA Automation Software Update Server" check box in the dialog that appears.
3. In the dialog "Add update from TIA Automation Software Update Server", select the required updates (software and support packages) and click "Add".
   If updates are already located on the corporate server, these are grayed out. You cannot load them again. During the download process, the status and the remaining time is displayed in the dialog.

Canceling the download process

To cancel the process, follow these steps:

1. Click "Cancel download".
2. Click "Yes" to confirm the dialog that appears.
   The download of the update is cancelled and it is deleted from the list.

Deleting updates from the corporate server

To delete updates, follow these steps:

Select the required updates and click "Remove".

- If an update only belongs to **one** project/**one** production line, confirm the dialog with "Yes". The selected update is removed from the list and deleted from the file system.
- If an update belongs to **multiple** projects/production lines, the following applies:
  - The remove update dialog does not appear.
  - The selected update is only removed from the current project list and not deleted from the file system.

  To delete updates from the file system, all instances of the updates must be deleted. To do this, follow these steps:
  - Open the existing project/global production line from the "Project" menu.
  - Select the updates you want and click "Remove".
  - Confirm the dialog that appeared when deleting the last instance with "Yes".

Server options

In the dialog "TIA Automation Software Update Server", click "Settings" to determine the following:

1. Under "Server path", specify the folder in which the downloads are to be saved. You can select either a local drive or a network drive.

   Note

   When you work directly on the server, the target directory is the same as the provision directory on the server. All changes are applied directly. This procedure is not recommended, as conflicts can occur with active downloads.

   We recommend that you work on another computer; the target directory can be any directory. The content of this directory must then still be copied to the provision directory. Here, also, make sure that no conflicts occur with active downloads.

2. Select the check box "Always run server in background (icon is shown in the taskbar)", if the server is to always run in the background.
3. Confirm your entries with "OK".

See also

Properties and advantage of a corporate server (Page 104)

Configuring a corporate server for updates (Page 105)

Installing support packages automatically 15

15.1 Installing support packages automatically

Introduction

As of V15.1, you can use the Support Package Installer to install or upgrade all support packages automatically via the command line; these include HSPs (hardware support packages) that are compatible with the installed version of the TIA Portal (e.g. isp.15_1).

Requirement

- Hardware and software of the programming device or PC meet the system requirements.
- You have administrator privileges on your computer.
- All running programs have been closed.

Procedure

To start the installation with the desired options directly via the command line, proceed as follows:

1. Open the Windows command prompt with "Start > Run > cmd".
2. Switch to the directory that contains the "Siemens.Automation.SupportPackageInstaller.exe" file. This is the installation directory of your installed TIA Portal.
3. In the command prompt, enter the following command:
   %Installation directory% > Siemens.Automation.SupportPackageInstaller.exe <Support Package(HSP)-storage directory> [-l <Name of log file>] [-warnaserror]

<Support Package-storage_directory>
Mandatory directory containing the support package files (*.isp). This can be either a local folder or a Remote Share.

-l <Storage location of log file>
This parameter is optional and specifies the path to the log file. If it is not set, the log file is created in the binary directory. However, you need to have write permissions in the storage folder.

-warnaserror
This parameter is optional and indicates that every message that would usually have been reported as a warning will be reported as an error instead. If a HSP does not meet the necessary conditions, for example, a corresponding return value/abort value is output to the command line and the affected HSP is skipped.

-?
This parameter is optional and shows the Help.

Note

- If the storage directory or the name of the log file contains spaces, you need to place the name in quotation marks.
- Only support packages located directly in the storage directory are considered; subdirectories are ignored. This means that the *.isp files must be located directly in the storage directory.

See also

Return values from the installation process (Page 128)

Log file (Page 129)

15.2 Return values from the installation process

Return values from the installation process

The following table shows the return values and their descriptions:

Code	Description
0	The installation was successful.
1	The installation was successful and a restart is required.
-1	The installation failed.
-2	The installation failed: The TIA Portal is still running.
-3	The installation failed: Another installation is already running.
-4	The installation failed: You do not have sufficient rights. The installation requires administrator rights.
-6	The installation failed: Insufficient memory space.
-7	The installation failed: A restart is required before the installation can start.

See also

Installing support packages automatically (Page 127)

Log file (Page 129)

15.3 Log file

Contents of the log file

The log file contains detailed information about every installation. If the log file already exists, it is supplemented. Headers and footers are created for each log file between which you can find the desired information.

An entry is generated for the following events:

- Support packages that are listed in the storage directory and are available during the installation but could not be installed due to missing products. The entry in the log file indicates which products and which versions of these products are missing.
- Support packages that could not be installed successfully.
- Support packages that were installed successfully.

The file name of the HSP including the file extension is logged for each entry.

See also

Installing support packages automatically (Page 127)

Return values from the installation process (Page 128)

Installing and uninstalling TIA Project Server 16

16.1 Notes on installing the project server

Introduction

To work with Multiuser Engineering, Multiuser Commissioning and Exclusive Engineering, you need a project server that manages your server projects, server libraries and the local sessions.

You have the following options for installing the "TIA Project Server":

- Together with the installation of the TIA Portal.
- As standalone installation by means of a separate installation process without TIA Portal.

Note

Requirement: Administrator rights

Administrator rights are required for the installation of the TIA Project Server.

More information:

- "Industry Online Support: TIA Project Server - Download (https://support.industry.siemens.com/cs/ww/en/view/109810588)"

Installation of the TIA Project Server with the TIA Portal

The TIA Project Server (referred to as "project server" below) is installed together with the following TIA Portal products:

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

The project server is usually activated by default in the product selection and is then installed with the TIA Portal.

Check the settings during installation of the TIA Portal.

You can find the specific default settings for the project server during setup when selecting the product in the "Options" directory.

By selecting or clearing the options, you can specify if the project server is to be installed along with TIA Portal or not.

Installation of the project server as a standalone installation

The project server can also be installed as a standalone installation.

A description of automated installation is also available in the installation source in the directory "Documents\Readme\<language directory>".

Identical TIA Portal versions during installation

When installing different TIA Portal products on various clients, make sure that all participants use the same versions of software products for the installation.

If, for example, you have installed STEP 7 Professional, WinCC Advanced and Safety as well as the project server in the version Vx.y, all other Team Engineering devices must also have installed this software in identical versions.

The service packs and updates must be installed for all products at the same time.

Note

TIA Project Server: Versioning

As of TIA Portal V18, the TIA Project-Server is supplied with a version number that is independent of the TIA Portal:

- TIA Portal V21 includes TIA Project-Server V2.2

Installation path

Do not use any UNICODE characters (for example, Chinese characters) in the installation path.

Antivirus programs

During the installation, read and write access to installed files is necessary.

Some antivirus programs block this access.

We therefore recommend that you disable antivirus programs during the installation of the project server and enable them again afterwards.

Supported virtualization platforms

You can also install the project server as well as the TIA Portal in a virtual machine.

For this purpose, use one of the following virtualization platforms in the specified version or a newer version:

- VMware vSphere Hypervisor (ESXi) 8.0 or higher
- VMware Workstation V17 or higher
- VMware Player V17 or higher
- Microsoft Hyper-V Windows Server 2019 or higher

Note

Installation of a visualization platform has the same requirements as the installation of the TIA Portal.

See also

Installing a project server (Page 133)

Uninstalling a project server (Page 135)

Industry Online Support: TIA Project Server - Download (https://support.industry.siemens.com/cs/ww/en/view/109810588)

16.2 Installing a project server

Introduction

You can install the "TIA Project Server" as part of the TIA Portal installation or standalone, independently of the TIA Portal.

When installing with TIA Portal, the project server version released for this purpose is always installed. Project server versions that are released afterwards are also released for this TIA Portal version as long as there are no new TIA Portal versions.

A description of automated installation is also available in the installation source in the directory "Documents\Readme\<language directory>".

Note

TIA Project Server: Versioning

As of TIA Portal V18, the TIA Project Server is supplied with a version number that is independent of the TIA Portal:

- TIA Portal V21 includes TIA Project Server V2.2

New installation replaces existing installation

Up to TIA Portal V18, project servers from different versions can be used side by side.

As of TIA Portal V18, versions of the TIA Project server are no longer installed in parallel. The new TIA Project Server version replaces existing installations during installation.

The existing user permissions for the server are applied.

Compatibility of the project server with TIA Portal

Communication between the project server and the TIA Portal is supported for the following applications:

Version of the project server	Version of the TIA Portal
TIA Project Server V2.0 / V2.1 / V2.2	V21, V20, V19, V18, V17, V16, V15.1, V15 and V14
TIA Project Server V1.2	V19, V18, V17, V16, V15.1, V15, and V14
TIA Project Server V1.1	V18, V17, V16, V15.1, V15, and V14
Server V17/TIA Project Server V1.0	V17, V16, V15.1, V15, and V14
Server V16	V16, V15.1, V15, and V14
Server V15.1 [1)]	V15.1, V15, and V14
Server V15 [1)]	V15 and V14
Server V14 [1)]	V14

1) The totally discontinued versions are still supported by the current TIA Project Server.

Note

Notes on the compatibility of the project server

The newly added server functionality for the current version is only available if the current version of TIA Portal is also installed.

If you are still working with an older version of TIA Portal or an older version of the project server, only the functionality included in the respective product version is available.

Multiuser Engineering does not upgrade the project versions.

TIA Portal versions < V18

Up to TIA Portal V18, it is possible for several versions of the project server that use different project versions of TIA Portal to be installed on the same computer.

However, each version of TIA Portal and the project server has only the functionality contained in that version.

Multiuser Engineering does not upgrade the project versions.

As of TIA Portal V18, TIA Project Server as of V1.0 is supplied. The new installations of the TIA Project Server replace the existing installation in each case. Different versions of the project server can no longer be installed on the same PC as of V1.0.

However, versions of the project server installed with TIA Portal versions prior to V18 can continue to run side-by-side on a PC and parallel to TIA Project Server versions as of V1.0.

Requirements for installation

You need administrator rights.

The installation of the server requires specific settings in the Windows firewall and, if needed, a certificate.

System requirements:

- Installation of the project server has the same requirements as the installation of the TIA Portal.

Installing the project server with the TIA Portal

Follow these steps for installation:

1. Note the requirements for the installation of the selected software package.
2. Navigate to the "Start.exe" file in the installation source and double-click it.
3. Select the preferred settings and click the "Install" button.
4. Make sure that the project server is selected in the product selection and observe the notes in the setup dialogs.

Result

The project server was installed on your computer together with the TIA Portal.

Installing the project server as standalone product

Follow these steps for installation:

1. Note the requirements for the installation of the project server.
2. To start the setup, double-click the self-extracting file "TIA_Portal_Projekt_Server_V<x.y>.exe".
   You can find these files in the "Support" directory in the installation source.
3. Select the preferred settings and click the "Install" button.
4. Follow the instructions in the setup dialogs.

Result

The TIA Project Server has been installed on your computer.

See also

Notes on installing the project server (Page 131)

Uninstalling a project server (Page 135)

16.3 Uninstalling a project server

Introduction

The "TIA Project Server" is uninstalled by using the Control Panel.

Installing a new version of the project server replaces an existing installation.

Requirements for removal

A project server is installed on your computer.

Uninstalling the TIA Project Server

Proceed as follows for removal:

1. Open the Control Panel.
2. Double-click on "Uninstall a program" in the Control Panel.
   The "Uninstall or change a program" dialog opens.
3. In the "Add or Remove Programs" dialog, select the entry for the "TIA Project Server".
4. Click on the "Remove" button.
   A security prompt appears.
5. Click "Yes" to confirm this prompt.

Result

The TIA Project Server has been uninstalled from your computer.

See also

Notes on installing the project server (Page 131)

Installing a project server (Page 133)

Installing and uninstalling TIA Administrator 17

17.1 Introduction to the TIA Administrator

The TIA Administrator offers you an overview of installed software packages.

Additional functions are available depending on the installed modules, for example, download of software packages and updates.

For information on installing and uninstalling as well as starting and stopping the TIA Administrator, refer to this document.

Information about configuration and operation of the TIA Administrator can be found in the application help.

17.2 System requirements

The TIA Administrator is a web application and runs completely in the browser. To use the TIA Administrator, one of the following browsers must be installed on your computer:

- Google Chrome version 114 or higher
- Microsoft Edge version 114 or higher
- Mozilla Firefox version 114 or higher

17.3 Installing TIA Administrator

The TIA Administrator can be found in the installation source of the TIA Portal.

Procedure

Check the integrity and authenticity of the installation source, if necessary. See also: Performing the installation (Page 87)

To install the TIA Administrator, follow these steps:

1. Double-click the "Start.exe" installation file.
2. Confirm the security prompt by clicking "Yes".
   The installation program opens.
3. Select the installation language and click "Next"
4. Select one or more product languages and click "Next".
5. Select the components to be installed.
6. If necessary, change the target directory for the installation and click "Next".
7. Read and confirm the license terms and safety information by selecting the check boxes.

8. Click "Next".
9. Set the configuration of the TIA Software Update Server. You have the following options:
   – TIA Automation Software Update Server
   – Corporate server
   – Continue with the current settings
10. If you want to set a corporate server, enter the server path and production line in the entry fields.
    The purpose of production lines is to provide different users with specific updates/support packages. If your company does not work with different production lines, assign a name, e.g. "ProductionLine1".
    You can change these entries later in the settings of the TIA Administrator.
11. Click "Next".
    An overview of the product configuration is displayed.
12. Click "Install".
    The installation is performed with the displayed settings.
    Once the TIA Administrator is installed, the computer must be restarted.

Result

The TIA Administrator is installed on your computer. When you install the TIA Administrator, a digital certificate is installed on your computer. This certificate is required to establish a secure connection.

17.4 Uninstalling TIA Administrator

The TIA Administrator can be uninstalled via the Control Panel.

Procedure

To uninstall the TIA Administrator, follow these steps:

1. Open the Control Panel.
2. Click on the "Programs and Functions" item in the Control Panel.
   The "Uninstall or Change a Program" dialog opens.
3. In the "Uninstall or change program" dialog, select the item for the TIA Administrator and click the "Uninstall" button.
   A security prompt appears.
4. Confirm this prompt by clicking "Yes".
   The uninstall program starts.
5. Select the installation language and click "Next".
6. Select the TIA Administrator to uninstall and click "Next".
7. Click "Uninstall".
8. Click on "Exit" to close the setup program.

Result

The TIA Administrator is uninstalled. The TIA Administrator's digital certificate is removed during uninstallation.

17.5 Starting and exiting TIA Administrator

17.5.1 Starting the TIA Administrator locally

TIA Administrator is stored in the following default directory:

C:\Program Files\Siemens\Automation\AWB_V2\host\awb\

During the installation, a "TIA Administrator V2" shortcut is created in the Start menu under "Siemens Automation".

Starting TIA Administrator

To start TIA Administrator locally, follow these steps:

1. Under Windows, select "Start > Siemens Automation > TIA Administrator V2".
   Your browser establishes a secure connection using the HTTPS protocol to TIA Administrator.
2. In the login window, enter your user name and password in the text boxes under "User Login".
3. Click "Login".
   The main window of TIA Administrator opens in your browser.

17.5.2 Starting the TIA Administrator with remote access

Administrators have the option of accessing the TIA Administrator from another device (for example, a PC or tablet) on the same network.

You must have a compatible browser installed on your device. You may need to set up your firewall for remote access.

Starting the TIA Administrator

To start the TIA Administrator remotely, follow these steps:

1. Open your browser.
2. Enter the URL for the target device in the address bar.

   Note

   URL to target device

   The URL is made up of the HTTPS protocol, the computer name or the IP address and the port.

   Port 8890 is assigned by default.

   Example of a URL: https://w10-setup-serv:8890

   Your browser displays the connection to the target device as an unsafe connection and shows a warning. You can ignore this warning and continue with the login.
3. In the login window, enter your user name and password in the text boxes under "User Login".
4. Click "Login".
   The main window of the TIA Administrator opens in your browser.

17.5.3 Closing the TIA Administrator

To close the TIA Administrator, follow these steps:

1. Open the menu.
2. Click "Log off".
3. Confirm the logoff by clicking "Yes".
4. Close your browser.