SIEMENS

Installation

Programmier- und Bedienhandbuch

11/2025

Hinweise zur Installation 1

Parallelinstallationen 2

Lizenzierung 3

Systemvoraussetzungen für die Installation 4

Übersicht über Prozesse und Services von TIA Portal-Komponenten 5

Security Logging verwenden 6

Installationsprotokoll 7

Integrität prüfen 8

Installation ausführen 9

Installierte Software anzeigen 10

Installierte Produkte modifizieren oder hochrüsten 11

Installierte Produkte reparieren 12

Deinstallation starten 13

Updates und Support Packages installieren 14

Support Packages automatisiert installieren 15

TIA Project-Server installieren und deinstallieren 16

TIA Administrator installieren und deinstallieren 17

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠ **GEFAHR**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **WARNUNG**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **VORSICHT**
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziert sind Personen, die aufgrund ihrer Ausbildung und Erfahrung mit Aufstellung, Montage, Inbetriebsetzung, Betrieb, Außerbetriebsetzung und Demontage des Produkts vertraut und im Stande sind, Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäße Verwendung von Siemens-Produkten

Beachten Sie Folgendes:

⚠ **WARNUNG**
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen Nutzungsinformation beschriebene, vorgesehene Verwendung eingesetzt werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens Aktiengesellschaft. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Ⓟ 10/2025 Änderungen vorbehalten

Copyright © Siemens 2025.
Alle Rechte vorbehalten

Inhaltsverzeichnis

1 Hinweise zur Installation 7

2 Parallelinstallationen 9

3 Lizenzierung 11

3.1 Hinweise zu Lizenzen 11

3.2 Lizenzierung von STEP 7 und WinCC 12

3.3 Lizenzierung von WinCC Unified Optionen 24
3.3.1 Grundlage 24
3.3.2 Archivierung 24
3.3.3 Parametersätze 26
3.3.4 Prozessdiagnose 27
3.3.5 Client 28
3.3.6 Reporting 29
3.3.7 Runtime Openness 30
3.3.7.1 Unified GraphQL 30
3.3.8 Unified Collaboration 31
3.3.9 Audit 31
3.3.10 Unified Data Hub 33
3.3.11 Redundanz 34

3.4 Lizenzierung von Plant Intelligence Optionen 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 Umgang mit Lizenzen und License Keys 39

3.6 Upgrade von Lizenzen 42

3.7 Lizenzierung von Bediengeräten 43

3.8 Lizenzierung von WinCC Runtime auf PC-basierten Bediengeräten 44

3.9 Lizenzierung WinCC Runtime asiatisch 45

3.10 STEP 7 ohne Lizenz für PC-CP 46

4 Systemvoraussetzungen für die Installation 47

4.1 Hinweise zu den Systemvoraussetzungen 47

4.2 Allgemeine Software- und Hardwarevoraussetzungen 48

4.3 Verwendung von hochauflösenden Monitoren 51

4.4 Produktspezifische Besonderheiten 52
4.4.1 Installation von WinCC 52
4.4.2 Deinstallation von WinCC Unified 52
4.4.3 Installation von WinCC Runtime Unified 52
4.4.4 Installation von WinCC Runtime Professional 59

4.4.5 Deinstallation einer SQL-Instanz ... 61
5 Übersicht über Prozesse und Services von TIA Portal-Komponenten ... 63
6 Security Logging verwenden ... 71
6.1 Security Logging im TIA Portal ... 71
6.2 Security Logging aktivieren und deaktivieren ... 71
6.3 Übersicht über Ereignisse ... 72
6.4 Ereignisse anzeigen und verwalten ... 81
7 Installationsprotokoll ... 83
8 Integrität prüfen ... 85
8.1 Grundlagen zur Integritätsprüfung ... 85
8.2 Integritätsprüfung durchführen ... 85
8.3 Fehlerfälle bei der Integritätsprüfung ... 87
9 Installation ausführen ... 89
10 Installierte Software anzeigen ... 95
11 Installierte Produkte modifizieren oder hochrüsten ... 97
12 Installierte Produkte reparieren ... 101
13 Deinstallation starten ... 103
14 Updates und Support Packages installieren ... 105
14.1 Verfügbarkeit von Updates und Support Packages prüfen und installieren ... 105
14.2 Arbeiten mit einem unternehmenseigenen Server ... 108
14.2.1 Eigenschaften und Vorteile eines unternehmenseigenen Servers ... 108
14.2.2 Unternehmenseigenen Server für Updates konfigurieren ... 109
14.2.3 Updates auf unterschiedliche Bereiche verteilen ... 122
14.2.4 Updates auf einem unternehmenseigenen Server bereitstellen ... 122
15 Support Packages automatisiert installieren ... 125
15.1 Support Packages automatisiert installieren ... 125
15.2 Rückgabewerte des Installationsprozesses ... 126
15.3 Protokolldatei ... 127
16 TIA Project-Server installieren und deinstallieren ... 129
16.1 Hinweise zur Installation des Projekt-Servers ... 129
16.2 Projekt-Server installieren ... 131
16.3 Projekt-Server deinstallieren ... 133
17 TIA Administrator installieren und deinstallieren ... 135
17.1 Einführung zum TIA Administrator ... 135
17.2 Systemvoraussetzungen ... 135
17.3 TIA Administrator installieren ... 135

17.4 TIA Administrator deinstallieren 136
17.5 TIA Administrator starten und beenden 137
17.5.1 TIA Administrator lokal starten 137
17.5.2 TIA Administrator per Fernzugriff starten 137
17.5.3 TIA Administrator beenden 138

Hinweise zur Installation

1

Inhalt

Hinweise, die nicht mehr in der Online-Hilfe berücksichtigt werden konnten und wichtige Hinweise zu Produkt-Eigenschaften.

Installation in einer virtuellen Umgebung (Private Cloud)

Eine Anleitung zur Installation des TIA Portals in einer virtuellen Umgebung (Private Cloud) finden Sie auf dem Installationsdatenträger im Verzeichnis "Documents\Readme\<Sprachverzeichnis>". Öffnen Sie hier das PDF-Dokument "TIAPortalCloudConnectorHowTo<Sprachkennung>.pdf".

Automatisierte Installation

Eine Beschreibung zur automatisierten Installation finden Sie auf der Produkt-DVD im Verzeichnis "Documents\Readme\<Sprachverzeichnis>".

Verwendung gleicher Versionen der TIA Portal Produkte bei der Installation

Achten Sie bei der Installation von verschiedenen TIA Portal Produkten darauf, dass Sie für die Installation die gleichen Stände der Service Packs und Updates verwenden. Wenn Sie also z. B. bei STEP 7 V13 das SP1 installiert haben, dann müssen Sie auch für WinCC V13 das SP1 installieren. Die Installation der Service Packs und Updates muss für alle Produkte zu einem gemeinsamen Zeitpunkt erfolgen. Starten Sie das TIA Portal nicht, bevor Sie nicht alle Produkte hochgerüstet haben.

Die Servicepacks können Sie im Internet unter Siemens Industry Online Support (https://support.industry.siemens.com/cs/de/de/) herunterladen.

Zielverzeichnis der Installation

Verwenden Sie keine UNICODE-Zeichen (z. B. chinesische Schriftzeichen) im Installationspfad.

Der Installationspfad kann nach der Installation von einem der TIA Portal-Produkte nicht mehr geändert werden.

Sicherheitseinstellungen bei der Installation von WinCC

Wenn Sie WinCC installieren, werden in Ihrem Betriebssystem Sicherheitseinstellungen verändert. Diese Sicherheitseinstellungen werden während der Installation aufgelistet.

Die Änderungen der Sicherheitseinstellungen müssen Sie bestätigen.

Wenn Sie nach der Installation an Ihrem Betriebssystem Änderungen vornehmen, können dadurch die Änderungen der Sicherheitseinstellungen durch die Installation des TIA Portals verändert werden.

Die Änderungen der Sicherheitseinstellungen durch die Installation des TIA Portals können Sie folgenderweise wiederherstellen:
"Start > Alle Programme > Siemens Automation > Security Controller > Einstellungen wiederherstellen".

Verwendung von Virenscannern

Während der Installation ist es notwendig, dass auf bereits installierte Dateien lesend und schreibend zugegriffen werden kann. Einige Virenscanner verhindern dies. Konfigurieren Sie Ihren Virenscanner für die Installation des TIA Portals daher so, dass ein Zugriff auf diese Dateien möglich ist.

FAQs zum TIA Portal

FAQs zum TIA Portal finden Sie unter FAQs (http://support.automation.siemens.com/WW/view/de/28919804/133000).

Parallelinstallationen

2

Parallelinstallation von WinCC V21 und anderen SIMATIC HMI Produkten

Die parallele Installation von WinCC V21 mit Versionen von WinCC flexible vor WinCC flexible 2008 SP5 ist nicht zulässig.

Die parallele Installation von WinCC V21 Comfort/Advanced mit Versionen von WinCC vor WinCC V7.3 ist nicht zulässig.

Die parallele Installation von WinCC Professional (ES und RT) mit WinCC V7.x, WinCC V8.x ist nicht zulässig.

Die parallele Installation von WinCC Unified (ES und RT) mit WinCC V7.x und WinCC V8.x ist nicht zulässig.

Parallelinstallation von WinCC Professional mit einer früheren Version

Eine Parallelinstallation von WinCC Professional V21 (ES oder RT) mit einer früheren Version von WinCC Professional (ES oder RT) ist nicht zulässig.

Alternativ können Sie eine andere WinCC Professional-Version in einer virtuellen Umgebung installieren.

Installation von WinCC Unified RT und WinCC RT Professional auf einem Gerät

Sie haben die Runtime für WinCC Unified und WinCC Professional auf einem Gerät installiert. Um Konflikte zwischen WinCC Unified RT und WinCC RT Professional zu vermeiden, müssen Sie die voreingestellten Port-Nummern für WebUX und WebNavigator ändern.

Um die Port-Nummern zu ändern, gehen Sie folgendermaßen vor:

1. Ändern Sie die Port-Nummer der WebUX-Webseite für die HTTPS-Kommunikation von 443 auf 4443. Das beseitigt den Konflikt mit der voreingestellten Port-Nummer von Unified Runtime.
2. Ändern Sie die Port-Nummer für die interne Kommunikation zwischen WebUX WebRH(Node Server) und GfxRTS von 1345 auf eine andere Nummer.
3. Ändern Sie die Port-Nummer der WebNavigator-Webseite für die HTTPS-Kommunikation von 443 auf 4430. Das beseitigt den Konflikt mit der voreingestellten Port-Nummer von Unified Runtime.
4. Erzeugen Sie eine Firewall-Regel für den eingehenden Datenverkehr, um den TCP-Verkehr mit der neuen WebUX Port-Nummer 4443 zu erlauben.
5. Setzen Sie Firewall-Regel für den eingehenden Datenverkehr, um den TCP-Verkehr mit der neuen WebNavigator Port-Nummer 4430 zu erlauben.
6. Vergewissern Sie sich, dass die Firewall-Regeln sicher erstellt wurden.
7. Prüfen Sie, ob WebUX- und WebNavigator-Webseiten mit ihren jeweiligen neuen Portnummern zugänglich sind.

Hinweis

Beachten Sie, dass folgende Ports aktuell von WinCC Unified RT verwendet werden:

- Port 443 wird für Unified RT verwendet.
- Port 1345 wird für die interne Kommunikation zwischen dem Unified-Node und Unified GfxRTS verwendet.

Lizenzierung

3

3.1 Hinweise zu Lizenzen

Bereitstellung der Lizenzen

Die Lizenzen für die Produkte des TIA Portals werden auf einem Installationsdatenträger oder via Online Software Delivery (OSD) ausgeliefert.

Bevor Sie das TIA Portal deinstallieren, müssen Sie noch benötigte Lizenzen transferieren und sichern. Verwenden Sie dazu den Automation License Manager.

Bereitstellung des Automation License Managers

Der Automation License Manager wird auf dem Installationsdatenträger mitgeliefert und während des Installationsprozesses automatisch übertragen.

Wenn Sie das TIA Portal deinstallieren, bleibt der Automation License Manager weiterhin auf Ihrem System installiert.

Arbeiten mit dem Automation License Manager

Der Automation License Manager ist ein Produkt der Siemens AG und wird zur Handhabung von License Keys (technische Repräsentanten von Lizenzen) eingesetzt.

Software-Produkte, für deren Betrieb License Keys notwendig sind, z. B. das TIA Portal, melden den Bedarf an License Keys automatisch beim Automation License Manager an. Wenn der Automation License Manager für diese Software einen gültigen License Key findet, so kann die Software entsprechend der mit diesem License Key verbundenen Lizenz-Nutzungsbedingungen verwendet werden.

Hinweis

Weiterführende Informationen, wie Sie mit dem Automation License Manager Ihre Lizenzen verwalten können, finden Sie in der mit dem Automation License Manager mitgelieferten Dokumentation.

Siehe auch

Hinweise zu den Systemvoraussetzungen (Seite 47)

Installation ausführen (Seite 89)

Installierte Software anzeigen (Seite 95)

Installierte Produkte modifizieren oder hochrüsten (Seite 97)

Installierte Produkte reparieren (Seite 101)

Deinstallation starten (Seite 103)

Installationsprotokoll (Seite 83)

3.2 Lizenzierung von STEP 7 und WinCC

Einführung

Für die Lizenzierung der folgenden Editionen von STEP 7 benötigen Sie einen License Key:

- STEP 7 Basic
- STEP 7 Professional

Sie können den entsprechenden License Key für STEP 7 nach der Installation mit dem Automation License Manager übertragen.

Für die Optionspakete von STEP 7 stehen Ihnen weitere Lizenzen zur Verfügung. Detaillierte Information finden Sie in der Dokumentation des jeweiligen Optionspakets.

Sie können die entsprechenden License Keys für STEP 7 und STEP 7 Optionen nach der Installation mit dem Automation License Manager übertragen.

Für die Lizenzierung der folgenden Editionen in WinCC benötigen Sie einen License Key:

- WinCC Engineering System
- WinCC Runtime
- Optionen für WinCC Engineering System
- Optionen für WinCC Runtime System

Lizenzen für WinCC und die WinCC Optionen übertragen Sie nach der Installation mit dem Automation License Manager.

Hinweis

Der Lizenznehmer bestätigt weiterhin, dass die Software (SW) von der Microsoft Corporation oder Tochtergesellschaften lizenzierte Software beinhaltet. Hiermit stimmt der Lizenznehmer zu, an die Geschäftsbedingungen des beigefügten Lizenzvertrags zwischen Microsoft SQL Server und Endabnehmer gebunden zu sein und diese zu erfüllen.

Lizenzen

Folgende Lizenzen mit den entsprechenden License Keys stehen Ihnen zur Verfügung:

- 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

Anwendungsmöglichkeiten der Lizenzen und der Geräte

Die folgende Tabelle zeigt, welche Geräte können Sie mit welcher Lizenz verwenden:

Vorhandene Lizenz	**Anwendbare Geräte**						
	Unified Devices			Classic Devices			
	WinCC Unified PC	Comfort Panels	Basic Panels	RT Professional	RT Advanced	Comfort Panels	Basic Panels
WinCC Unified Basic ES	Nein	Nein	Ja	Nein	Nein	Nein	Ja
WinCC Unified Comfort ES	Nein	Ja	Ja	Nein	Nein	Ja	Ja
WinCC Unified PC 10k ES	Ja (10k*)	Ja	Ja	Nein	Ja	Ja	Ja
WinCC Unified PC 100k ES	Ja (100k*)	Ja	Ja	Ja	Ja	Ja	Ja
WinCC Unified PC max ES	Ja	Ja	Ja	Ja	Ja	Ja	Ja
WinCC Basic	Nein	Nein	Ja	Nein	Nein	Nein	Ja
WinCC Comfort	Nein	Ja	Ja	Nein	Nein	Ja	Ja
WinCC Advanced	Ja (10k*)	Ja	Ja	Nein	Ja	Ja	Ja
WinCC Professional 512	Ja (10k*)	Ja	Ja	Ja (512*)	Ja	Ja	Ja
WinCC Professional 4096	Ja (10k*)	Ja	Ja	Ja (4096*)	Ja	Ja	Ja
WinCC Professional max	Ja (100k*)	Ja	Ja	Ja	Ja	Ja	Ja

* Anzahl der maximal möglichen Powertags

Gültigkeit der License Keys für ältere Versionen von STEP 7

Mit einem gültigen License Key für die V21.x von STEP 7 Professional und STEP 7 Professional Combo können auch ältere Versionen von STEP 7 ohne Einschränkungen betrieben werden. Genauere Informationen dazu entnehmen Sie der nachfolgenden Tabelle:

Edition	Lizenz	Gültig für
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	Lizenz	Gültig für
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

Gültigkeit der License Keys für ältere Versionen von WinCC

Mit einem gültigen License Key für WinCC V21.x können auch ältere Versionen von WinCC ohne Einschränkungen betrieben werden.

Genauere Informationen entnehmen Sie der nachfolgender Tabelle:

WinCC Engineering System

Edition	Lizenz	Gültig für
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	Lizenz	Gültig für
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	Lizenz	Gültig für
		• 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	Lizenz	Gültig für
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	Lizenz	Gültig für
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	Lizenz	Gültig für
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	Lizenz	Gültig für
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] Weitere Informationen finden Sie unter Lizenzierung von WinCC Unified Optionen (Seite 24).

Gültigkeit der Lizenzen für WinCC Optionen

WinCC Optionen mit versionsunabhängigen License Keys können für zukünftige Versionen mitverwendet werden.

Starten ohne gültigen License Key

Wenn Sie das TIA Portal ohne gültigen License Key starten, weist Sie das System mit einer Meldung auf den nicht lizenzierten Modus hin. Sie haben die Möglichkeit, einmalig eine Trial License zu aktivieren. Diese hat jedoch nur eine begrenzte Gültigkeit und läuft nach 21 Tagen ab.

Wenn die Trial License abgelaufen ist, können folgende Fälle auftreten:

- Auf dem betreffenden PC war das TIA Portal noch nie lizenziert:
  - Im TIA Portal lassen sich keine lizenzpflichtigen Aktionen mehr durchführen.
- Auf dem betreffenden PC war das TIA Portal bereits lizenziert:
  - Der nicht lizenzierte Modus wird alle 10 Minuten und bei jeder lizenzpflichtigen Aktion durch ein quittierpflichtiges Fenster angezeigt.

Trial-Lizenzen für RT Professional

Wenn Sie keine gültige Lizenz besitzen, weist Sie das System mit einer Meldung auf den nicht lizenzierten Modus hin.

Sie haben die Möglichkeit, einmalig eine Trial License zu aktivieren.

Diese Trial License hat jedoch nur eine begrenzte Gültigkeit und läuft nach 21 Tagen ab.

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

Lizenzbedarf bei Simulation in STEP 7

Wenn Sie in STEP 7 die SPS-Simulation über den Menübefehl "Online > Simulation" starten, benötigen Sie keine weiteren PLCSIM-Lizenzen.

Lizenzbedarf bei Simulation in WinCC Runtime

Wenn folgende Bedingungen erfüllt sind, benötigen Sie auch bei der Simulation die entsprechenden Lizenzen für WinCC Runtime und für lizenzpflichtige Optionen:

- Sie starten den Simulator über den Menübefehl "Online > Simulation > starten".

Wenn Sie keine gültige Lizenz besitzen, können Sie die Simulation für eine Stunde aktivieren.

Lizenzen für den TIA Portal Cloud Connector

Für das Arbeiten mit dem TIA Portal Cloud Connector benötigen Sie auf jedem Gerät, das Sie im TIA Portal Cloud Connector als "Benutzergerät" festlegen, einen gültigen License Key. Der License Key ist auch dann erforderlich, falls auf diesem Gerät das TIA Portal installiert ist. Für Geräte, die Sie als "Remotegerät" verwenden, ist kein License Key erforderlich.

Siehe auch

Umgang mit Lizenzen und License Keys (Seite 39)

3.3 Lizenzierung von WinCC Unified Optionen

3.3.1 Grundlage

Gültigkeit der License Keys für ältere Versionen

SIMATIC Lizenzen sind abwärts kompatibel. Mit einem neueren Licence Key von WinCC Unified Optionen können auch ältere Versionen betrieben werden.

3.3.2 Archivierung

Um Ihre Daten zu archivieren, haben Sie in WinCC Unified zwei Möglichkeiten:

- Datei-basierte Archivierung
- Datenbank-basierte Archivierung

Datei-basierte Archivierung

Voraussetzung

WinCC Unified Basic Panel:

- Für die Projektierung benötigen Sie eine WinCC Unified Basic ES (Engineering System) Lizenz.
- Für die Archivierung benötigen Sie keine Lizenz.

WinCC Unified Comfort Panel:

- Für die Projektierung benötigen Sie eine WinCC Unified Comfort ES (Engineering System) Lizenz.
- Für die Archivierung benötigen Sie keine Lizenz.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

WinCC Unified Basic Panel ermöglicht die Datei-basierte Archivierung von 50 Archivvariablen, die in jedem Gerät inbegriffen sind.

WinCC Unified Comfort Panel ermöglicht die Datei-basierte Archivierung von 5000 Archivvariablen, die in jedem Gerät inbegriffen sind.

WinCC Unified PC RT ermöglicht die Datei-basierte Archivierung bis zu 5000 Archivvariablen in einer SQL Lite Datenbank. Für die Archivierung von maximal 5000 Archivvariablen benötigen Sie eine

oder mehrere Lizenzen entsprechend der Anzahl der zu archivierenden Variablen. Entnehmen Sie dazu die Lizenzen in der nachfolgend aufgeführten Tabelle.

Upgrade

Beim Upgrade des Systems benötigen Sie für die Archivierung keine Upgrade-Lizenz.

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie Archivvariablen im Trial Modus projektieren.

Datenbank-basierte Archivierung

Die Datenbank-basierte Archivierung ermöglicht Ihnen alle Archivvariablen bis zu der oberen Grenze in einer MS SQL Datenbank zu archivieren.

Voraussetzung

WinCC Unified Basic Panel:

- Nicht verfügbar

WinCC Unified Comfort Panel:

- Nicht verfügbar

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Die Datenbank-basierte Archivierung beinhaltet neben der Funktionalität auch einen MS SQL Server und daher benötigen Sie die Lizenz "WinCC Unified Database Storage".

Weiterhin benötigen Sie eine oder mehrere Lizenzen entsprechend der Anzahl der zu archivierenden Variablen. Entnehmen Sie dazu die Lizenzen in der nachfolgend aufgeführten Tabelle.

Datei- oder Datenbank-basierte Lizenzen

Die benötigte Lizenz oder Lizenzen, entsprechend der Anzahl der zu archivierenden Variablen, entnehmen Sie der folgenden Tabelle:

Lizenz	Anzahl der Archivvariablen[1]	Datei-basiert	Datenbank-basiert
WinCC Unified PC 100 Logging Tags	100	Ja	Ja
WinCC Unified PC 500 Logging Tags	500	Ja	Ja
WinCC Unified PC 1000 Logging Tags	1000	Ja	Ja
WinCC Unified PC 5000 Logging Tags	5000	Ja	Ja
WinCC Unified PC 10000 Logging Tags	10000	Nein	Ja
WinCC Unified PC 30000 Logging Tags	30000	Nein	Ja
WinCC Unified Database Storage[2]	Nein	Nicht nötig	Ja

[1] Die Logging-Tags-Lizenzen können Sie kumulieren. Die Summe der Lizenzen ergibt die mögliche Anzahl der zu archivierenden Variablen.

[2] Die Lizenz ermöglicht das Archivieren in die MS SQL Datenbank.

Upgrade

Beim Upgrade des Systems benötigen Sie für die Archivierung keine Upgrade-Lizenz.

Die WinCC Unified Database Storage-Lizenz ist versionsabhängig und benötigt zum Upgrade die entsprechende Upgrade Lizenz.

Weitere Informationen finden Sie unter "Upgrade von Lizenzen (Seite 42)".

Trial

Für die Datenbank-basierte Archivierung ist kein Trial Modus verfügbar.

3.3.3 Parametersätze

Voraussetzung

WinCC Unified Basic Panel:

- Für die Projektierung benötigen Sie eine WinCC Unified Basic ES (Engineering System) Lizenz.

WinCC Unified Comfort Panel:

- Für die Projektierung benötigen Sie eine WinCC Unified Comfort ES (Engineering System) Lizenz.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Verwendung von Parametersätzen auf einem WinCC Unified Basic Panel benötigen Sie keine Lizenz.

Für die Verwendung von Parametersätzen auf einem WinCC Unified Comfort Panel benötigen Sie keine Lizenz.

Für die Verwendung von Parametersätzen auf einem Runtime PC benötigen Sie eine WinCC Unified Parameter Control (PC) Lizenz.

Upgrade

Die Lizenz ist versionsabhängig und benötigt zum Upgrade die entsprechende Upgrade-Lizenz.

Die Upgrade-Lizenz ist im Upgrade des Unified Basissystems enthalten.

Weitere Informationen finden Sie unter "Upgrade von Lizenzen (Seite 42)".

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die Parametersätze im Trial Modus projektieren.

3.3.4 Prozessdiagnose

Voraussetzung

WinCC Unified Basic Panel:

- Die Option Prozessdiagnose wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Für die Projektierung benötigen Sie eine WinCC Unified Comfort ES (Engineering System) Lizenz.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Verwendung von Prozessdiagnose auf einem WinCC Unified Comfort Panel benötigen Sie eine WinCC Unified ProDiag Lizenz.

Für die Verwendung von Prozessdiagnose auf einem WinCC Unified PC RT benötigen Sie eine WinCC Unified ProDiag Lizenz.

Upgrade

Die Lizenz ist versionsabhängig und benötigt zum Upgrade die entsprechende Upgrade-Lizenz.

Die Upgrade-Lizenz ist im Upgrade des Unified Basissystems enthalten.

Weitere Informationen finden Sie unter "Upgrade von Lizenzen (Seite 42)".

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die Prozessdiagnose im Trial Modus projektieren.

3.3.5 Client

WinCC Unified Basic Panel

- Für die Projektierung benötigen Sie eine WinCC Unified Basic ES (Engineering System) Lizenz.

Jedes WinCC Unified Basic Panel beinhaltet einen WinCC Unified Client Operate.

Lizenz	Nur Beobachten	Bedienen und Beobachten
WinCC Unified Client Operate (1)*	Nein	Ja

* Die Anzahl der Clients ist nicht erweiterbar.

WinCC Unified Comfort Panel:

- Für die Projektierung benötigen Sie eine WinCC Unified Comfort ES (Engineering System) Lizenz.
- Auf ein WinCC Unified Comfort Panel können maximal 3 Fernzugriffe gleichzeitig erfolgen.
- Die Lizenz für den ersten Zugriff ist kostenfrei.
- Die Verwendung des Fernzugriffs muss in der Firmware freigeschaltet sein.

Lizenzierung

Für den Fernzugriff benötigen Sie eine Lizenz abhängig von der Anzahl und der Art der Zugriffe. Die benötigte Lizenz entnehmen Sie der folgenden Tabelle:

Lizenz[1]	Nur Beobachten	Bedienen und Beobachten
WinCC Unified Panel Client Monitor (1)	Ja	Nein
WinCC Unified Panel Client Operate (1)	Nein	Ja

[1] Die Client-Lizenzen können Sie kumulieren. Die Summe der Lizenzen ergibt die mögliche Anzahl der Client-Verbindungen.

WinCC Unified PC

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

In der Lizenz für WinCC Unified PC RT sind folgende Client Funktionen enthalten:

- Zwei Zugriffe für Bedienen und Beobachten (zwei lokale Zugriffe oder ein lokaler und ein Fernzugriff)
- Ein Zugriff für Beobachten (ein lokaler Zugriff oder ein Fernzugriff)

Lizenzierung

Für den Fernzugriff benötigen Sie eine Lizenz abhängig von der Anzahl und der Art der Zugriffe. Die benötigte Lizenz entnehmen Sie der folgenden Tabelle:

Lizenz[1]	Nur Beobachten	Bedienen und Beobachten
WinCC Unified Client Monitor (1)	Ja	Nein
WinCC Unified Client Monitor (3)	Ja	Nein
WinCC Unified Client Monitor (10)	Ja	Nein
WinCC Unified Client Monitor (30)	Ja	Nein
WinCC Unified Client Monitor (100)	Ja	Nein
WinCC Unified Client Operate (1)	Nein	Ja
WinCC Unified Client Operate (3)	Nein	Ja
WinCC Unified Client Operate (10)	Nein	Ja
WinCC Unified Client Operate (30)	Nein	Ja
WinCC Unified Client Operate (max pro RT server)	Nein	Ja

[1] Die Client-Lizenzen können Sie kumulieren. Die Summe der Lizenzen ergibt die mögliche Anzahl der Client-Verbindungen.

Upgrade

Die Lizenz ist versionsunabhängig und benötigt kein Upgrade auf eine neue Version.

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie den Client im Trial Modus projektieren.

3.3.6 Reporting

Voraussetzung

WinCC Unified Basic Panel:

- Die Option Reporting wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Für die Projektierung benötigen Sie eine WinCC Unified Comfort ES (Engineering System) Lizenz.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Erstellung der Reports in Excel und die manuelle Ausführung der Reports in Excel oder aus dem Report Runtime Control ist keine Lizenz erforderlich.

Für eine automatische Ausführung von Reporting (Zeit, Ereignis) benötigen Sie auf einem WinCC Unified Comfort Panel eine "WinCC Unified Report Execution" Lizenz.

Für eine automatische Ausführung von Reporting (Zeit, Ereignis) benötigen Sie auf einem WinCC Unified PC RT eine "WinCC Unified Report Execution" Lizenz.

Upgrade

Die Lizenz ist versionsabhängig und benötigt zum Upgrade die entsprechende Upgrade-Lizenz.

Die Upgrade-Lizenz ist im Upgrade des Unified Basissystems enthalten.

Weitere Informationen finden Sie unter "Upgrade von Lizenzen (Seite 42)".

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die Option Reporting im Trial Modus projektieren.

3.3.7 Runtime Openness

3.3.7.1 Unified GraphQL

Voraussetzung

WinCC Unified Basic Panel:

- Die Option Unified GraphQL wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Die Option Unified GraphQL wird nicht unterstützt.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Um über die Schnittstelle GraphQL auf die archivierten Daten auf einem WinCC Unified PC RT zugreifen zu können, benötigen Sie eine "WinCC Unified Connectivity GraphQL Logged Data" Lizenz.

Upgrade

Die Lizenz ist versionsabhängig und benötigt zum Upgrade die entsprechende Upgrade-Lizenz.

Die Upgrade-Lizenz ist im Upgrade des Unified Basissystems enthalten.

Weitere Informationen finden Sie unter "Upgrade von Lizenzen (Seite 42)".

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die Schnittstelle GraphQL im Trial Modus verwenden.

3.3.8 Unified Collaboration

Voraussetzung

WinCC Unified Basic Panel

- Die Option Unified Collaboration wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Für die Projektierung benötigen Sie eine WinCC Unified Comfort ES (Engineering System) Lizenz.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Verwendung der Option Unified Collaboration benötigen Sie auf einem WinCC Unified Comfort Panel eine WinCC Unified Collaboration Lizenz für jedes beteiligte Gerät.

Für die Verwendung der Option Unified Collaboration benötigen Sie auf einem WinCC Unified PC RT jeweils eine WinCC Unified Collaboration Lizenz für jedes beteiligte Gerät.

Upgrade

Die Lizenz ist versionsabhängig und benötigt zum Upgrade die entsprechende Upgrade-Lizenz.

Die Upgrade-Lizenz ist im Upgrade des Unified Basissystems enthalten.

Weitere Informationen finden Sie unter "Upgrade von Lizenzen (Seite 42)".

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die Option Unified Collaboration im Trial Modus projektieren.

3.3.9 Audit

Voraussetzung

WinCC Unified Basic Panel:

- Die Option Audit wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Für die Projektierung benötigen Sie eine WinCC Unified Comfort ES (Engineering System) Lizenz.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Verwendung der Option Audit auf einem WinCC Unified Comfort Panel benötigen Sie eine Lizenz.

Für die Verwendung der Option Audit auf einem WinCC Unified PC RT benötigen Sie eine Lizenz.

Für die Option Audit können Sie folgende Lizenzen nutzen:

Lizenz	Beschreibung
WinCC Unified Audit Basis	Gesicherte Kommunikation Archivierung des Audit Trail Aufzeichnung von Änderungen der Prozessdaten (automatisch, über Skript oder Systemfunktion) Bestätigung mit / ohne Kommentar Audit Trail-Einträge exportieren Audit Trail-Bericht und Anzeige von Manipulationen Audit Trail-Eintrag einloggen und ausloggen[1] Einfache elektronische Unterschrift Sichern und Wiederherstellen der Audit Trail-Datenbanksegmente Direkte Anzeige und Analyse des Audit Trail im Audit Viewer[2]
WinCC Unified Audit Enhanced	Zusätzlich: Mehrfache elektronische Unterschrift (2 Personen)

[1] Ab V18

[2] Ab V18 Update 1

Für die Verwendung der Option Audit benötigen Sie eine Lizenz für jedes beteiligte Gerät.

Lizenz	WinCC Unified Comfort Panel	WinCC Unified PC
WinCC Unified Audit Basis	Ja	Ja
WinCC Unified Audit Enhanced	Ja	Ja

Upgrade

Die Lizenz ist versionsabhängig und benötigt zum Upgrade die entsprechende Upgrade-Lizenz.

Die Upgrade-Lizenz ist im Upgrade des Unified Basissystems enthalten.

Weitere Informationen finden Sie unter "Upgrade von Lizenzen (Seite 42)".

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die Option Audit im Trial Modus projektieren.

3.3.10 Unified Data Hub

Einleitung

Auf dem WinCC Unified Data Hub Server werden zentral alle Prozessinformationen der angeschlossenen Data Hub Clients archiviert. Jedes beteiligte Gerät benötigt eine Data Hub Client-Lizenz.

Die Menge bzw. Art der Prozessinformationen, die im zentralen Archiv auf dem WinCC Unified Data Hub Server gespeichert werden, hängt vom Data Hub Client-Typ ab:

Wird archiviert	WinCC Unified Data Hub Client Small*	WinCC Unified Data Hub Client*	WinCC Unified Data Hub Client Audit Trail*
Variablen	200	Unbegrenzte Anzahl	----------
Meldungen	Alle	Alle	Alle
Audit Trails	----------	----------	Gesamt

* Je nach Bedarf ist die Lizenz für 1, 3 oder 10 Unified Data Hub Clients bestellbar

Die Lizenz für Unified Data Hub Client ist versionsunabhängig und benötigt kein Upgrade auf eine neue Version

Lizenzierung von WinCC Unified Data Hub Server und WinCC Unified Data Hub Client

Voraussetzung

WinCC Unified Basic Panel:

- Die Option WinCC Unified Data Hub wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Die Option WinCC Unified Data Hub wird nicht unterstützt.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.

Lizenzierung

Für die Verwendung von WinCC Unified Data Hub Server auf einem WinCC Unified PC RT benötigen Sie ein "WinCC Unified Data Hub Server"-Lizenzpaket. Das Paket "WinCC Unified Data Hub Server" beinhaltet folgende Lizenzen:

- Unified PC (150) RT
- Unified Database Storage
- Data Hub Client (1) - zur Verwendung auf dem UDH-Server
- Data Hub Server

Für die Verwendung von WinCC Unified Data Hub Client auf einem WinCC Unified PC RT benötigen Sie ein "WinCC Unified Data Hub Client"-Lizenz.

Upgrade

Das Lizenzpaket "WinCC Unified Data Hub Server" ist versionsabhängig und benötigt zum Upgrade das entsprechende Upgrade-Lizenzpaket.

Die "WinCC Unified Data Hub Client" Lizenz ist versionslos. Es ist keine Upgrade-Lizenz nötig.

Weitere Informationen finden Sie unter "Upgrade von Lizenzen (Seite 42)".

Trial

Wenn Sie keine gültige Lizenz haben, können Sie WinCC Unified Data Hub Server im Trial Modus nicht projektieren.

3.3.11 Redundanz

Voraussetzung

WinCC Unified Basic Panel

- Die Option Redundanz wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Die Option Redundanz wird nicht unterstützt.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für den Einsatz in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Verwendung der Option Redundanz bei WinCC Unified PC RT benötigen Sie für jedes beteiligte Gerät eine "WinCC Unified Redundancy" Lizenz.

Das Lizenzpaket beinhaltet jeweils zwei "WinCC Unified Redundancy" Lizenzen.

Upgrade

Die Lizenz ist versionsabhängig und benötigt zum Upgrade die entsprechende Upgrade-Lizenz.

Die Upgrade-Lizenz für eine WinCC Unified PC RT-Station ist im Upgrade des Unified Basissystems enthalten.

Weitere Informationen finden Sie unter "Upgrade von Lizenzen (Seite 42)".

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die Option Redundanz im Trial Modus projektieren.

3.4 Lizenzierung von Plant Intelligence Optionen

3.4.1 Calendar

Voraussetzung

WinCC Unified Basic Panel:

- Die Option Calender wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Die Option Calender wird nicht unterstützt.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für die PI-Option Calendar in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Projektierung der PI-Option Calendar benötigen Sie keine zusätzliche Lizenz.

Für die Verwendung der PI-Option Calendar auf einem WinCC Unified PC RT benötigen Sie folgende Lizenzen:

Lizenz	Beschreibung
WinCC Unified Calendar Base	Pro Server: • 3 unabhängige Basiskalender • Uneingeschränkte Anzahl von abgeleiteten Kalendern • Uneingeschränkte Nutzung der Option • Versionsabhängig
WinCC Unified Calendar Extension (1)*	• 1 zusätzlicher Basiskalender

* Gilt pro Erweiterung, ist versionsunabhängig und kumulativ

Beispiel:

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

Upgrade

Beim Upgrade auf die nächsthöhere Version benötigen Sie eine WinCC Unified Calendar Base Upgrade-Lizenz.

Die WinCC Unified Calendar Extension (1)-Lizenz ist dagegen versionsunabhängig.

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die PI-Option Calendar im Trial Modus projektieren.

3.4.2 Performance Insight

Voraussetzung

WinCC Unified Basic Panel:

- Die Option Performance Insight wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Die Option Performance Insight wird nicht unterstützt.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für die PI-Option Performance Insight in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Projektierung der PI-Option Performance Insight benötigen Sie keine zusätzliche Lizenz.

Für die Verwendung der PI-Option Performance Insight auf einem WinCC Unified PC RT benötigen Sie folgende Lizenzen:

Lizenz	Beschreibung
WinCC Unified Performance Insight Base	Pro Server: • 3 analysierte Anlagenobjekte • Uneingeschränkte Nutzung der Option • Versionsabhängig
WinCC Unified Performance Insight Extension (10)*	• 10 zusätzliche analysierte Anlagenobjekte
WinCC Unified Performance Insight Extension (30)*	• 30 zusätzliche analysierte Anlagenobjekte
WinCC Unified Performance Insight Extension (100)*	• 100 zusätzliche analysierte Anlagenobjekte
WinCC Unified Performance Insight Extension (300)*	• 300 zusätzliche analysierte Anlagenobjekte

* Gilt pro Erweiterung, ist versionsunabhängig und kumulativ

Beispiel:

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

Beim Upgrade auf die nächsthöhere Version benötigen Sie eine WinCC Unified Performance Insight Base Upgrade-Lizenz.

Die WinCC Unified Performance Insight Extension-Lizenzen sind dagegen versionsunabhängig.

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die PI-Option Performance Insight im Trial Modus projektieren.

3.4.3 Sequence

Voraussetzung

WinCC Unified Basic Panel:

- Die Option Sequence wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Die Option Sequence wird nicht unterstützt.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für die PI-Option Sequence in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Projektierung der PI-Option Sequence benötigen Sie keine zusätzliche Lizenz.

Für die Verwendung der PI-Option Sequence auf einem WinCC Unified PC RT benötigen Sie folgende Lizenzen:

Lizenz	Beschreibung
WinCC Unified Sequence Base	Pro Server: • 3 nebenläufige technische Einrichtungen • Uneingeschränkte Nutzung der Option • Versionsabhängig
WinCC Unified Sequence Extension (5)*	• 5 zusätzliche nebenläufige technische Einrichtungen

* Gilt pro Erweiterung, ist versionsunabhängig und kumulativ

Beispiel:

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

Beim Upgrade auf die nächsthöhere Version benötigen Sie eine neue WinCC Unified Sequence Base Upgrade-Lizenz.

Die WinCC Unified Sequence Extension (5)-Lizenz ist dagegen versionsunabhängig.

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die PI-Option Sequence im Trial Modus projektieren.

3.4.4 Line Coordination

Voraussetzung

WinCC Unified Basic Panel:

- Die Option Line Coordination wird nicht unterstützt.

WinCC Unified Comfort Panel:

- Die Option Line Coordination wird nicht unterstützt.

WinCC Unified PC:

- Für die Projektierung benötigen Sie eine WinCC Unified PC ES (Engineering System) Lizenz.
- Für die PI-Option Line Coordination in Runtime benötigen Sie eine WinCC Unified PC RT (Runtime) Lizenz.

Lizenzierung

Für die Projektierung der PI-Option Line Coordination benötigen Sie keine zusätzliche Lizenz.

Für die Verwendung der PI-Option Line Coordination auf einem WinCC Unified PC RT benötigen Sie folgende Lizenzen:

Lizenz	Beschreibung
WinCC Unified Line Coordination Base	Pro Server: • 3 Teilanlagen • Uneingeschränkte Nutzung der Option • Versionsabhängig
WinCC Unified Line Coordination Extension (5)*	• 5 Teilanlagen
WinCC Unified Line Coordination Extension (10)*	• 10 Teilanlagen
WinCC Unified Line Coordination Extension (50)*	• 50 Teilanlagen

* Gilt pro Erweiterung, ist versionsunabhängig und kumulativ

Beispiel:

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

Beim Upgrade auf die nächsthöhere Version, benötigen Sie eine neue WinCC Unified Line Coordination Base Upgrade-Lizenz.

Die WinCC Unified Line Coordination Extension-Lizenzen sind dagegen versionsunabhängig.

Trial

Wenn Sie keine gültige Lizenz besitzen, können Sie die PI-Option Line Coordination im Trial Modus projektieren.

3.5 Umgang mit Lizenzen und License Keys

Einleitung

Zur Nutzung von STEP 7 Basic, STEP 7 Professional sowie WinCC Engineering System, Optionen für WinCC Engineering System und WinCC Runtime benötigen Sie jeweils einen gültigen License Key.

ACHTUNG
Zerstörung von License Keys durch Kopieren Ein License Key ist nicht kopierbar. Das verwendete Kopierschutzverfahren verhindert das Kopieren der License Keys. Beim Versuch, einen License Key zu kopieren, wird der License Key zerstört.

Trial-Lizenz

Wenn Sie das TIA Portal ohne gültigen License Key starten, weist Sie das System mit einer Meldung auf den nicht lizenzierten Modus hin. Sie haben die Möglichkeit, einmalig eine Trial-Lizenz zu aktivieren. Die Trial-Lizenz läuft nach 21 Tagen ab.

Wenn die Trial-Lizenz abgelaufen ist, läuft das TIA Portal nur noch mit Einschränkungen. Für die Vollversion von TIA Portal müssen Sie die entsprechende Lizenz erwerben.

Installation von License Keys für STEP 7 und WinCC

Installieren Sie die Lizenz mit dem Automation License Manager vom mitgelieferten Datenträger auf Ihren PC.

Zur Nutzung von WinCC Runtime oder der Simulation auf dem Engineering-PC über den Menübefehl "Online > Simulation > starten" benötigen Sie zusätzliche License Keys. Sie müssen dazu den Automation License Manager verwenden.

Wenn Sie eine Lizenz installieren, wird der zugehörige License Key vom ursprünglichen Ablageort der License Keys entfernt.

Übertragen von License Keys auf Bediengeräte

Für den Betrieb von WinCC müssen Sie die License Keys auf das Bediengerät übertragen.

Sie übertragen einen License Key in folgenden Fällen auf das Bediengerät:

- Zur Nutzung vom WinCC Runtime
- Zur Nutzung von Optionen von WinCC Runtime

Wenn Sie eine Lizenz auf ein Bediengerät übertragen, wird der zugehörige License Key vom Ablageort der License Keys entfernt.

Wenn Sie die Lizenz nicht mehr benötigen oder Daten sichern möchten, müssen Sie die License Keys vom Bediengerät übertragen. Sie können diese Lizenz an einem anderen PC oder Bediengerät verwenden.

Deinstallation von License Keys

Die Deinstallation von License Keys erfolgt immer mit dem Automation License Manager. Rufen Sie vor der Deinstallation den Automation License Manager auf

und sichern Sie den zu deinstallierenden License Key auf einen anderen Ablageort.

Sie deinstallieren einen License Key in folgenden Fällen:

- Wenn Sie Daten sichern.
- Wenn Sie die Lizenz nicht mehr benötigen.

Sie können eine gültige Lizenz auch an einem anderen PC verwenden.

Modifikation an den Datenträgern des Engineering Systems

Durch Modifikationen der Datenträger des Engineering Systems kann der License Key zerstört werden. Rufen Sie vor derartigen Modifikationen den Automation License Manager auf und sichern Sie den zu deinstallierenden License Key auf einen anderen Ablageort.

ACHTUNG
Zerstörung von License Keys auf PCs Wenn einer der folgenden Fälle zutrifft, deinstallieren Sie zuerst alle License Keys : • Formatieren der Festplatte • Komprimieren der Festplatte • Restaurieren der Festplatte • Starten eines Optimierungsprogramms, das feste Blöcke verschiebt • Installation eines neuen Betriebssystems Lesen Sie die Beschreibung zu Automation License Manager ("Start > Siemens Automation > Dokumentation"). Befolgen Sie alle Warnhinweise und Hinweise.

Datensicherung von Bediengeräten (Back-up/Restore)

Zur Datensicherung am Bediengerät deinstallieren Sie die License Keys am Bediengerät. Rufen Sie dazu den Automation License Manager auf und sichern Sie den License Key auf einen anderen Ablageort.

ACHTUNG
Zerstörung von License Keys auf nicht PC-basierten Bediengeräten Bei folgenden Bediengeräten werden übertragene License Keys durch Back-up-/Restore-Vorgänge zerstört: • 270er-Reihe • 370er-Reihe Gehen Sie vor dem Wiederherstellen wie folgt vor: 1. Überprüfen Sie mit dem Automation License Manager und ProSave, ob auf dem Bediengerät License Keys vorhanden sind. 2. Übertragen Sie die vorhandenen License Keys vom Bediengerät Nach dem Wiederherstellen übertragen Sie die License Keys wieder auf das Bediengerät.

Ungültige Lizenz nach Zeitzonenwechsel

Die installierten Lizenzen funktionieren nicht mehr, wenn Sie auf einem PC die Zeitzone folgendermaßen umstellen: von einer auf die volle Stunde bezogenen Zeitzone auf eine Zeitzone, die sich nicht auf eine volle Stunde bezieht.

Um dieses Verhalten zu umgehen, deinstallieren Sie den License Key mit dem Automation License Manager mit einer Zeitzoneneinstellung, die bei der Installation des License Keys eingestellt war.

Beispiel: Sie möchten das Bediengerät aus der Zeitzone "GMT +3:00" in der Zeitzone "GMT +3:30" einsetzen.

1. Deinstallieren Sie den License Key mit der Zeitzoneneinstellung "GMT +3:00".
2. Ändern Sie die Zeitzoneneinstellungen entsprechend auf Ihrem PC.
3. Installieren Sie den License Key.

Das Verhalten betrifft nicht die Trial License.

Defekte Lizenz

Eine Lizenz ist in folgenden Fällen defekt:

- Wenn der License Key auf dem Ablageort nicht mehr zugänglich ist.
- Wenn der License Key beim Übertragen auf das Ziellaufwerk verschwindet.

Hinweis

Wenn Sie das Systemdatum auf einen früheren Zeitpunkt zurücksetzen, werden alle Lizenzen defekt.

Sie können die defekte Lizenz mithilfe von Automation License Manager reparieren lassen. Benutzen Sie dazu die Funktion "Wiederherstellen" bzw. den "Wiederherstellen-Assistenten" des Automation License Manager. Für die Wiederherstellung nehmen Sie Kontakt mit dem Customer Support auf. Nähere Hinweise hierzu finden Sie im Internet unter: http://support.automation.siemens.com (http://support.automation.siemens.com)

Hinweis

Ein störungsfreier Betrieb von Runtime ist auch bei fehlender bzw. defekter Lizenz sichergestellt. In kurzen Zeitabständen weist Sie das System mit einer Meldung auf den nicht lizenzierten Modus hin.

Microsoft SQL Server

Für die Nutzung der Datenbank Microsoft SQL Server ist eine Lizenz erforderlich. Diese Lizenz liegt bei einer lizenzrechtlich ordnungsgemäßen Installation von WinCC vor.

Der mit der Installation von WinCC lizenzierte SQL Server darf nur in Verbindung mit WinCC eingesetzt werden.

Der Einsatz für andere Zwecke erfordert eine zusätzliche Lizenz. Dazu gehören z. B.:

- Einsatz für eigene Datenbanken
- Einsatz für Fremdapplikationen
- Einsatz von SQL Zugriffsmechanismen, die nicht über WinCC zur Verfügung gestellt werden

Deinstallation

Nach der Deinstallation von WinCC müssen Sie die SQL-Server-Instanz "WinCC" deinstallieren. Wählen Sie unter “Systemsteuerung > Software" den Eintrag "Microsott SQL Server 20..” zur Deinstallation.

Siehe auch

Lizenzierung von STEP 7 und WinCC (Seite 12)

3.6 Upgrade von Lizenzen

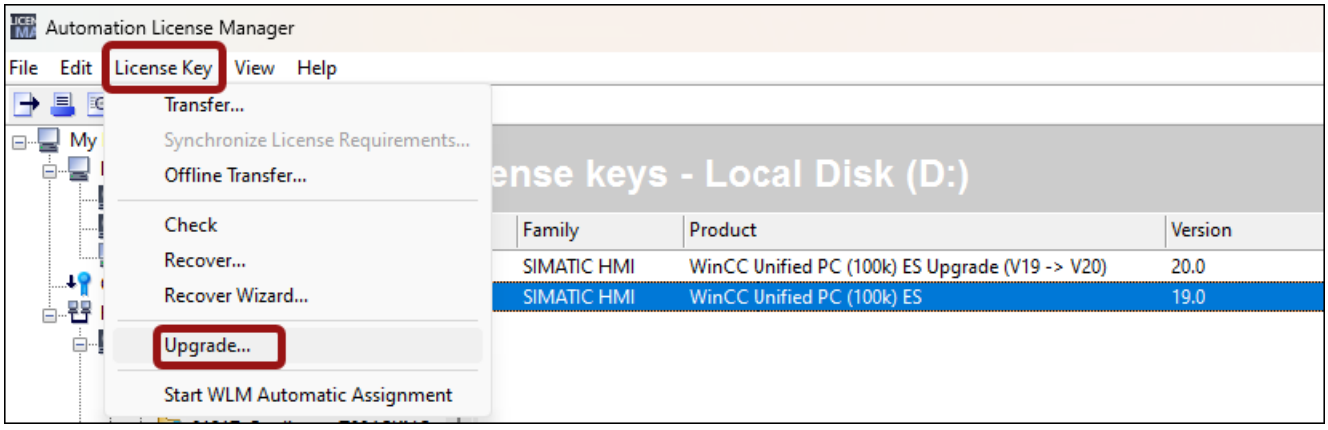
Upgrade von versionsabhängigen Lizenzen

Um eine niedrigere Version auf Ihrem PC hochzurüsten, benötigen Sie entweder die Lizenz für ein Upgrade oder für ein PowerPack.

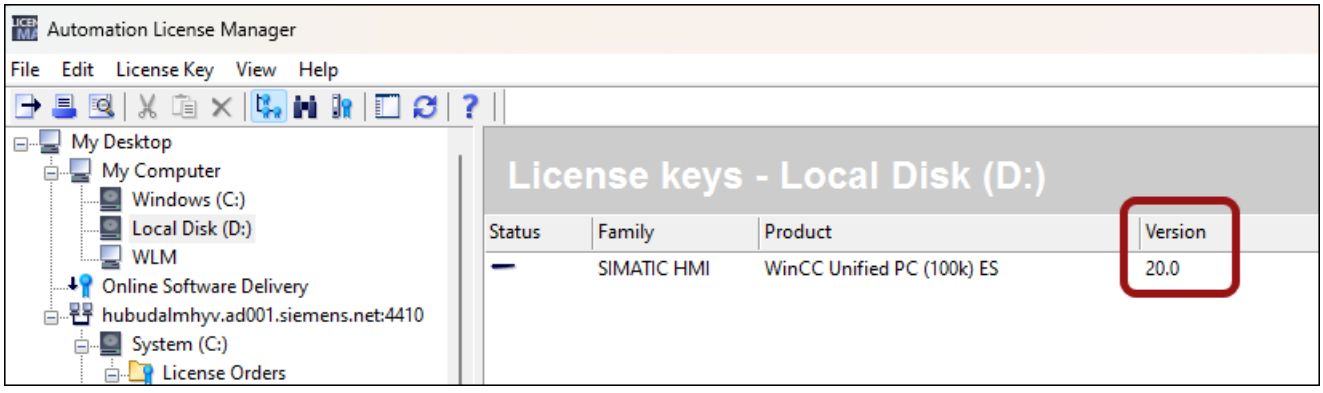
Um das Upgrade durchzuführen, gehen Sie folgendermaßen vor:

Beispiel: Sie haben die Lizenz WinCC Unified PC (100k) ES V19 und müssen auf die Version V20 hochrüsten.

1. Öffnen Sie den Automation License Manager.
2. Öffnen Sie den lokalen Speicherort mit den Lizenzen.
3. Markieren Sie die Lizenz, die Sie hochrüsten wollen.
4. Klicken Sie in der Funktionsleiste die Schaltfläche "License Key" und wählen Sie "Upgrade"



5. Das Upgrade erfolgt automatisch und die Upgrade-Lizenz ersetzt die Lizenz mit der niedrigeren Versionsnummer.



3.7 Lizenzierung von Bediengeräten

Nicht PC-basierte Bediengeräte werden mit Runtime-Lizenzen ausgestattet. Ein License Key für den Runtimebetrieb ist nicht erforderlich.

Zu einer Option für nicht PC-basierte Bediengeräte kann eine Lizenz erforderlich sein. Der License Key der jeweiligen Lizenz schaltet jeweils eine Option zur Nutzung frei.

License Key

Um nicht PC-basierte Bediengeräte mit License Keys lizenzieren zu können, ist das Add-On "SIMATIC HMI License Manager Panel Plugin" notwendig.

Das WinCC Setup installiert standardmäßig dieses Add-On. Das License Manager Panel Plugin öffnen Sie im Automation License Manager über den Menübefehl "Bearbeiten > Zielsystem verbinden > Bediengerät verbinden".

Wenn WinCC nicht installiert ist, ist eine Installation von ProSave 7.2 oder höher notwendig.

Hinweise zum Umgang mit Lizenzen

- Weitere Informationen zur Handhabung der Lizenzen finden Sie in der Hilfe des Automation License Manager.
- Vergewissern Sie sich, bevor Sie mit Lizenzierung beginnen, dass das Bediengerät mindestens mit einem aktuellen Stand des Betriebssystems ausgestattet ist. Gegebenenfalls aktualisieren Sie das Betriebssystem mit ProSave.
- Der Lizenznehmer bestätigt weiterhin, dass die Software (SW) von der Microsoft Corporation oder Tochtergesellschaften lizenzierte Software beinhaltet. Hiermit stimmt der Lizenznehmer zu, an die Geschäftsbedingungen des beigefügten Lizenzvertrags zwischen Microsoft SQL Server und Endabnehmer gebunden zu sein und diese zu erfüllen.

Nicht lizenzierter Modus

Die Runtime-Optionen sind ohne gültige Lizenz vorübergehend ohne Einschränkung der Funktionalität nutzbar. Der nicht lizenzierte Modus wird alle 10 Minuten durch ein quittierpflichtiges Fenster angezeigt.

3.8 Lizenzierung von WinCC Runtime auf PC-basierten Bediengeräten

License Key

Bei PC-basierten Bediengeräten benötigen Sie für Folgendes einen License Key:

- WinCC Runtime, z. B. mit 128 Variablen
- WinCC Optionen

Lizenzen für die WinCC Optionen übertragen Sie nach der Installation mit dem Automation Licence Manager.

Hinweis

Nur mit einem gültigen Certificate of License, entsprechend der darin genannten Version, ist der produktive Betrieb der Software zulässig.

Um WinCC Runtime zu lizenzieren, benötigen Sie die entsprechende, neue Lizenz.

Die Runtime-Lizenzen von WinCC flexible 2008 und von WinCC V7 können Sie mit einer Upgrade Lizenz auf WinCC Runtime hochrüsten.

Hinweise zum Umgang mit Lizenzen

- Wenn Sie von einer älteren Version auf die aktuelle Version hochrüsten, benötigen Sie neue Lizenzen für WinCC Runtime.
- Der Lizenznehmer bestätigt weiterhin, dass die Software (SW) von der Microsoft Corporation oder Tochtergesellschaften lizenzierte Software beinhaltet. Hiermit stimmt der Lizenznehmer zu, an die Geschäftsbedingungen des beigefügten Lizenzvertrages zwischen Microsoft SQL Server und Endabnehmer gebunden zu sein und diese zu erfüllen.

Nicht lizenzierter Modus

WinCC Runtime und die Runtime-Optionen sind ohne gültige Lizenz uneingeschränkt nutzbar. Der nicht lizenzierte Modus wird alle 10 Minuten durch ein quittierpflichtiges Fenster angezeigt.

3.9 Lizenzierung WinCC Runtime asiatisch

Einleitung

Wenn Sie WinCC Runtime in einer asiatischen Sprache verwenden, wird für die Gültigkeitsprüfung der erforderlichen Lizenz zusätzlich ein Dongle eingesetzt.

Der Dongle wird ausgeliefert in Form eines zertifizierten USB-Sticks zusammen mit dem erforderlichen Licence Key für WinCC Runtime Professional und WinCC Unified PC Runtime asiatisch. Der License Key ist auf dem zertifizierten USB-Stick gespeichert.

Einsatz des Dongle für eine asiatische Runtime

Um ein WinCC-Projekt in einer asiatischen Sprache erfolgreich zu lizenzieren, übertragen Sie den erforderlichen License Key mithilfe des "Automation License Manager" von dem zertifizierten USB-Stick auf das Bediengerät.

Stecken Sie den USB-Stick in den USB-Anschluss des Bediengeräts. Der USB-Stick wirkt während Runtime als Dongle. Der Dongle muss in Runtime immer im USB-Anschluss gesteckt bleiben.

Wenn Sie den Dongle in Runtime entfernen, wechselt WinCC Runtime in den Demo-Modus.

Die für die asiatischen Märkte gelieferten USB-Sticks sind für den Dauereinsatz in Produktionsanlagen zertifiziert. Den Inhalt können Sie daher nicht auf einen anderen USB-Datenträger kopieren oder transferieren.

Bei Verlust oder Defekt eines zertifizierten USB-Sticks benötigen Sie einen neuen, zertifizierten USB-Stick.

Simulation eines WinCC-Projekts in einer asiatischen Sprache

Für die Simulation benötigen Sie dann ebenfalls einen zertifizierten USB-Stick als Dongle. Wenn kein Dongle verfügbar ist, läuft die Simulation im Demo-Modus.

3.10 STEP 7 ohne Lizenz für PC-CP

Funktionen von STEP 7 für PC-CP

STEP 7 für PC-CP ist eine vollständige STEP 7Version, die ohne Lizenz installiert wurde. In dieser Version stehen Ihnen nur Konfigurations- und Diagnose-Möglichkeiten für folgende Komponenten zur Verfügung:

- PC-CPs und Applikationen (OPC-Server) für PC-Stationen
- Switches SCALANCE X
- Router SCALANCE W / SCALANCE M
- Security-Module SCALANCE S
- PROFINET IO-Devices und PROFIBUS DP-Slaves
- IE/PB LINK PN IO, IWLAN/PB LINK PN IO
- Reader (RFID) und optische Lesegeräte (MV)

SIMATIC-Stationen und WinAC-Komponenten stehen nur in der Netz- und Topologie-Ansicht zur Verfügung (keine Geräte-Ansicht). Programmierfunktionen stehen nicht zur Verfügung.

Informationssystem

Das in der STEP 7-Version für PC-CP vorhandene Informationssystem beschreibt den vollen Funktionsumfang von STEP 7. Beachten Sie daher die Beschränkung auf die Funktionen zur Konfiguration der zuvor genannten Gerätegruppen.

Auf Funktionsumfang von STEP 7 Professional hochrüsten

Mit der Installation von STEP 7 für PC-CP ist bereits der volle Funktionsumfang von STEP 7 auf Ihrer Engineering-Station vorhanden, aber nur eingeschränkt nutzbar.

Durch eine nachträgliche Lizenzinstallation können Sie jederzeit auf die volle Funktionalität von STEP 7 Professional hochrüsten. Eine erneute Installation ist nicht erforderlich. Zuvor in STEP 7 für PC-CP angelegte Projekte können nach der Installation einer Lizenz ohne Einschränkung weiterverwendet werden.

4 Systemvoraussetzungen für die Installation

4.1 Hinweise zu den Systemvoraussetzungen

Systemvoraussetzungen für einzelne Produkte

Je nachdem, welche Produkte Sie installieren möchten, gelten unterschiedliche Systemvoraussetzungen. Beachten Sie daher die individuellen Systemvoraussetzungen Ihrer Produkte.

Möchten Sie mehrere Produkte installieren, berücksichtigen Sie bitte die Systemvoraussetzungen des Produkts mit den höchsten Anforderungen.

Anzeigen von PDF-Dateien

Um mitgelieferte PDF-Dateien zu lesen, benötigen Sie einen PDF Reader, der das PDF-Format 1.7 unterstützt, z. B. Adobe (R) Reader.

Zeichensätze

Seit Windows 10 Update Version 1809 bietet Windows die Möglichkeit, Zeichensätze entweder mit Administratorrechten für jeden Benutzer (Befehl "Für alle Benutzer installieren" im Kontextmenü) oder benutzerspezifisch zu installieren. Um in WinCC Zeichensätze uneingeschränkt nutzen und auf ein Bediengerät laden zu können, müssen Zeichensätze immer mit Administratorrechten installiert werden.

Bitte beachten Sie, dass die Schaltfläche "Installieren" in der Ansicht eines Zeichensatzes nur eine benutzerspezifische Installation durchführt.

Siehe auch

Hinweise zu Lizenzen (Seite 11)

Installation ausführen (Seite 89)

Installierte Software anzeigen (Seite 95)

Installierte Produkte modifizieren oder hochrüsten (Seite 97)

Installierte Produkte reparieren (Seite 101)

Deinstallation starten (Seite 103)

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

4.2 Allgemeine Software- und Hardwarevoraussetzungen

Voraussetzungen für die Installation

Die folgende Tabelle zeigt die minimalen Software- und Hardwarevoraussetzungen, die für die Installation mindestens erfüllt sein müssen:

Hardware/Software	Voraussetzung
Prozessor	Intel® Core™ i3-6100U, 2.30 GHz
RAM	8 GB
Festplatte	S-ATA mit mindestens 20 GB verfügbarem Speicherplatz
Netzwerk	Ab 100 Mbit
Bildschirmauflösung	1024 x 768
Betriebssysteme *	**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 (Vollinstallation) • Windows Server 2022 Standard (Vollinstallation)

* Inklusive aller Security Updates bis zum Microsoft Security Bulletin Summary für August 2025 (MS25-AUG). Weitere Informationen zu den Betriebssystemen finden Sie in der Hilfe zu Microsoft Windows oder auf der Homepage von Microsoft.

** Nur für Basic-Editionen

Möglicherweise unterstützen bestimmte Produkte weitere Versionen von Windows. Weitere Informationen dazu finden Sie bei den produktspezifschen Systemvoraussetzungen oder Sie überprüfen die Kompatibiltät mit dem Kompatibilitäts-Tool. Das Kompatibilitäts-Tool finden Sie im Internet unter https://support.industry.siemens.com/compatool/ (https://support.industry.siemens.com/compatool/).

Empfohlene PC-Hardware

Die folgende Tabelle zeigt die empfohlenen Hardwarevoraussetzungen:

Hardware/Software	Voraussetzung
Rechner	Ab SIMATIC FIELD PG M6 Comfort (oder vergleichbarer PC)
Prozessor	Intel® Core™ i5-8400H (2,5 bis 4,2 GHz; 4 Kerne + Hyper-Threading; 8 MB Smart Cache)
RAM	16 GB oder mehr (für große Projekte 32 GB)
Festplatte	SSD mit mindestens 50 GB verfügbarem Speicherplatz
Netzwerk	1 GBit (für Multiuser)
Bildschirm	15,6" Full HD Display (1920 x 1080 oder größer)

Unterstützte Virtualisierungsplattformen

Sie können die Softwarepakete "SIMATIC STEP 7" und "SIMATIC WinCC" in einer virtuellen Maschine installieren. Verwenden Sie dazu eine der folgenden Virtualisierungsplattformen in der angegebenen oder einer neueren Version:

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

Für diese Virtualisierungsplattformen werden die folgenden Host- und Gast-Betriebssysteme empfohlen:

Betriebssystem	VMware vSphere Hypervisor (ESXi)	VMware Workstation	VMware Player	Microsoft Hyper-V
Windows Server 2025 Standard (Vollinstallation)	G	-	-	H/G
Windows Server 2022 Standard (Vollinstallation)	G	-	-	H/G
Windows Server 2019 Standard (Vollinstallation)	G	-	-	H/G
Windows Server 2016 Standard (Vollinstallation)	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: als Host-Betriebssystem verwendbar

G: als Gast-Betriebssystem verwendbar

H/G: als Host- und Gast-Betriebssystem verwendbar

-: nicht als Host- oder Gast-Betriebssystem verwendbar

Hinweis

- Für die Gast-Betriebssysteme gelten dieselben Hardware-Anforderungen wie für die jeweiligen TIA-Produkte selbst.
- Der Betreiber der Anlage muss dafür Sorgen, dass den Gast-Betriebssystemen ausreichend Systemressourcen zur Verfügung gestellt werden.
- Für den Einsatz von HyperV-Server und ESXi wird die von den Herstellern zertifizierte Hardware empfohlen.
- Bei der Verwendung von Microsoft Hyper-V ist das Anzeigen der erreichbaren Teilnehmer nicht möglich.

Unterstützte Sicherheitsprogramme

Folgende Sicherheitsprogramme sind kompatibel zu "SIMATIC STEP 7" und "SIMATIC WinCC":

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

  Hinweis

  Achten Sie darauf, dass Ihr Virenscanner und dessen Datenbanken immer auf dem aktuellen Stand sind.

  Die letzte Aktualisierung der Viren-Pattern erfolgte am 20.08.2025.
- Verschlüsselungssoftware:
  - Microsoft Bitlocker
- Host-basiertes Intrusion Detection System:
  - McAfee Application Control (Trellix) 8.4 oder höher

Siehe auch

Hinweise zu Lizenzen (Seite 11)

Installation ausführen (Seite 89)

Verfügbarkeit von Updates und Support Packages prüfen und installieren (Seite 105)

Installierte Software anzeigen (Seite 95)

Installierte Produkte modifizieren oder hochrüsten (Seite 97)

Installierte Produkte reparieren (Seite 101)

Deinstallation starten (Seite 103)

4.3 Verwendung von hochauflösenden Monitoren

Einführung

Beim Arbeiten mit dem TIA Portal haben Sie die Möglichkeit, hochauflösende Monitore zu verwenden, z. B. 4K-Monitore. Um für diese Monitore die optimale Anzeige zu erhalten, verwenden Sie möglichst die in Microsoft Windows unter den Bildschirmeinstellungen empfohlene Skalierung. Das TIA Portal passt sich dabei bis zu einer Skalierung von 350 Prozent an. Sie können im Dialog "Erweiterte Skalierungseinstellungen" im Bereich "Benutzerdefinierte Skalierung" auch eine höhere Skalierung einstellen. Allerdings kann es dann zu unscharfen, verzerrten oder sich überlagernden Texten und Grafiken kommen. Verwenden Sie daher die von Microsoft Windows empfohlene Standardeinstellung.

Verwendung von mehreren Monitoren

Wenn Sie mehrere Monitore im Einsatz haben, startet das TIA Portal auf dem primären Monitor. Dabei passt sich das TIA Portal an die jeweilige Auflösung an. Bei einem 4K-Monitor erfolgt diese Anpassung bis zu einer Skalierung von 350 Prozent. Das ist die von Microsoft Windows empfohlene Standardeinstellung. Verschieben Sie das TIA Portal oder einzelne Fenster auf einen anderen Monitor, hängt es von der Auflösung dieses Monitors ab, wie die Anzeige aussieht. Möglicherweise werden die Texte und Grafiken unscharf oder verzerrt dargestellt oder überlagern sich. Für diesen Monitor erfolgt keine dynamische Skalierung. Das heißt, falls dieser Monitor nicht den gleichen Skalierungsfaktor wie der primäre Monitor verwendet, kann die zuvor eingestellte Skalierung für diesen Monitor unpassend sein. Stellen Sie in diesem Fall die Skalierung wieder auf den empfohlenen Wert oder den Wert, der beim primären Monitor eingestellt ist.

4.4 Produktspezifische Besonderheiten

4.4.1 Installation von WinCC

Für die Installation müssen bestimmte Anforderungen an Betriebssystem und Software-Konfiguration erfüllt sein.

Hinweis

WinCC ist grundsätzlich für den Betrieb in einer Domäne oder Arbeitsgruppe freigegeben.

Beachten sie jedoch, dass Domänen-Gruppenrichtlinien und Einschränkungen der Domäne die Installation behindern können. Entfernen Sie in diesem Fall den Rechner vor der Installation von Microsoft Message Queuing, Microsoft SQL Server und WinCC aus der Domäne. Melden Sie sich an dem betreffenden Rechner lokal mit Administratorrechten an. Führen Sie die Installation durch. Nach der erfolgreichen Installation können Sie den WinCC-Rechner wieder in die Domäne aufnehmen. Wenn die Domänen-Gruppenrichtlinien und Einschränkungen der Domäne die Installation nicht behindern, dann muss der Rechner während der Installation nicht aus der Domäne entfernt werden.

Beachten sie, dass Domänen-Gruppenrichtlinien und Einschränkungen der Domäne auch den Betrieb behindern können. Wenn Sie diese Einschränkungen nicht aufheben können, dann betreiben Sie die WinCC-Rechner in einer Arbeitsgruppe.

Wenden Sie sich gegebenenfalls an den Domänen-Administrator.

4.4.2 Deinstallation von WinCC Unified

Deinstallation von WinCC

Wenn Sie bereits ein Update zu WinCC Unified V16 installiert haben und WinCC V17 installieren möchten, gehen Sie wie folgt vor:

1. Öffnen Sie die Systemsteuerung.
2. Starten Sie die Deinstallation von SIMATIC WinCC Unified PC V16.0 UPDx.
3. Wählen Sie bei der Auswahl der Komponenten "SIMATIC WinCC Update 16.0 UPDx" zur Deinstallation aus.
4. Nach Abschluss dieser Deinstallation, deinstallieren Sie alle gewünschten Komponenten von WinCC V16 über das Installationsmedium.

Die Information befindet sich in der Readme unter „Wichtige Hinweise (WinCC Unified).

4.4.3 Installation von WinCC Runtime Unified

Für die Installation müssen bestimmte Anforderungen an Betriebssystem und Software-Konfiguration erfüllt sein.

Installation in Domänen und Arbeitsgruppen

WinCC Unified ist grundsätzlich für den Betrieb in einer Domäne oder Arbeitsgruppe frei gegeben.

Beachten Sie jedoch, dass Domänen-Gruppenrichtlinien und Einschränkungen der Domäne die Installation behindern können. Entfernen Sie in diesem Fall den Rechner vor der Installation von WinCC Unified und Microsoft SQL Server aus der Domäne. Melden Sie sich an dem betreffenden Rechner lokal mit Administratorrechten an. Führen Sie die Installation durch. Nach der erfolgreichen Installation können Sie den WinCC-Rechner wieder in die Domäne aufnehmen. Wenn die Domänen-Gruppenrichtlinien und Einschränkungen der Domäne die Installation nicht behindern, muss der Rechner während der Installation nicht aus der Domäne entfernt werden.

Beachten Sie, dass Domänen-Gruppenrichtlinien und Einschränkungen der Domäne auch den Betrieb behindern können. Wenn Sie diese Einschränkungen nicht aufheben können, betreiben Sie die WinCC-Rechner in einer Arbeitsgruppe.

Wenden Sie sich gegebenenfalls an den Domänen-Administrator.

Betrieb auf einem Netzwerk Server

Der Betrieb von WinCC Unified Runtime auf einem Netzwerk Server (z. B. Domain Controller, File-Server, Namensdienst-Server, Router, Software Firewall, Media Server, Exchange Server) ist nicht zulässig.

Windows Computername

Bevor Sie die WinCC-Installation starten, legen Sie den Windows-Computernamen fest. Beachten Sie die Windows-Benennungsregeln.

Hinweis

Wie Sie nach einer nachträglichen Änderung des Computernamen vorgehen, ist in der Installationsanleitung der WinCC Unified Runtime im Kapitel "Änderung des Computernamen oder der IP-Adresse" beschrieben.

Folgende Zeichen sind im Computernamen nicht zulässig:

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

Bei der Vergabe der Windows-Computernamen beachten Sie Folgendes:

- Es darf nur Großschreibung verwendet werden.
- Das erste Zeichen muss ein Buchstabe sein.
- Die ersten 12 Zeichen des Computernamens müssen eindeutig sein.
- Der Computername darf maximal 15 Zeichen haben.

Hardwarevoraussetzungen für die Installation

Die folgende Tabelle zeigt die minimalen Hardwarevoraussetzungen, die für die Installation erfüllt sein müssen:

Hardware	Voraussetzung
Prozessortyp	Intel Core i3
RAM	4 GB
Freier Festplattenspeicher	10 GB, 8 GB CF

Softwarevoraussetzungen für die Installation

Betriebssystem

Software	Konfiguration	Bemerkungen
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)	
Windows 11	Windows 11 Home Version 21H2 (OS Build 22000) Nur für den Einsatz von Runtime Simulation auf einem Engineering PC geeignet.	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

Hinweis

Anzahl unterstützter Clients und Verbindungen

Die Desktop-Betriebssysteme unterstützen maximal 5 Clients. Bei den Server-Betriebssystemen können sich mehr als 5 Clients mit dem Server verbinden.

Windows limitiert die Anzahl der eingehenden Verbindungen auf Desktop-Betriebssystemen auf 20. Dies limitiert die Anzahl der möglichen Zugriffe auf Runtime.

Kompatible Browser

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

Weiterführende Informationen zur Verwendung der Browser erhalten Sie in der Liesmich SIMATIC Unified PC im Kapitel "Internet-Browser für WinCC Unified PC".

Windows-spezifische Softwareeinstellungen für IIS (Internet Information Services)

Bei der Installation der WinCC Runtime Unified werden für IIS folgende Einstellungen in Windows automatisch aktiviert:

- HTTP-Fehler
- HTTP-Umleitung
- Standarddokument
- Statischer Inhalt
- .NET- Erweiterbarkeit 3.5
- ASP
- ASP.NET 4.5
- ISAPI-Erweiterungen
- ISAPI-Filter
- Komprimierung dynamischer Inhalte
- Komprimierung statischer Inhalte
- Anforderungsfilterung

Tabelle 4-1 Weitere Software-Voraussetzungen

Thema	Version / Einstellung	Bemerkung
Web-Browser	Der Browser muss HTML 5 unterstützen.	
Benutzerrechte für die Installation	Administrationsrechte	
SIMATIC NET	V19	Damit Sie Runtime Unified mit mehr als 10 Verbindungen betreiben können, benötigen Sie diese Lizenz.

Vorher installierte Versionen von WinCC Unified PC Runtime

Die Installation von Unified PC Runtime V19 ist möglich auf Geräten, für die gilt:

- Kein Unified PC Runtime installiert, oder
- WinCC Unified PC Runtime V18 installiert

Ports

Bei Verwendung einer Windows Firewall richtet die WinCC Unified Runtime Installationsroutine folgende Ports ein:

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

Wenn Ihr System eine andere Firewall-Lösung verwendet, stellen Sie sicher, dass die Ports entsprechend eingerichtet werden.

Eine Liste der von Unified Runtime verwendeten Ports finden Sie in der Anwenderhilfe Liesmich SIMATIC Unified PC im Kapitel "Security-Hinweise". Stellen Sie vor Start der Installation sicher, dass die in der Liste aufgeführten Ports frei sind.

Hinweis

HTTP-Port sperren

Aus Sicherheitsgründen wird empfohlen, am IIS-Server Port 80 zu deaktiveren:

1. Starten Sie auf dem Unified PC "Internetinformationsdienste (IIS)-Manager".
2. Klicken Sie rechts "Default Web Sites".
3. Wählen Sie "Entfernen" oder "Website verwalten > Beenden".

Hinweis

Blockierte Ports nach Aktualisierung oder Hochrüstung des Betriebssystems

Die Aktualisierung oder Hochrüstung des Betriebssystems des Unified PCs, z. B. von Windows Server 2016 auf Windows Server 2019, kann die Firewall-Einstellungen ändern. In der Folge können die OPC UA-Ports blockiert sein.

Starten Sie in dem Fall das Siemens-Werkzeug “Security Controller” und führen Sie “Einstellungen wiederherstellen” aus.

Virtualisierung

Sie können das Softwarepaket "SIMATIC WinCC Runtime Unified" in einer virtuellen Maschine installieren. Folgende Virtualisierungssysteme wurden getestet:

- VMware vSphere Hypervisor (ESXi) 6.7 (oder höher)
- VMware Workstation 12.5.5 und VMware Workstation 15.5.0 (oder höher)
- VMware Player 12.5.5 und VMware Player 15.5.0 (oder höher)
- Microsoft Hyper-V Server 2019 (oder höher)

In einer Virtualisierungsplattform können alle frei gegebenen Betriebssysteme als Host-Betriebssystem verwendet werden.

Voraussetzung

Die Leistungsdaten der virtuellen Rechner müssen den Mindestanforderungen von WinCC-Clients entsprechen.

Hinweis

- Beachten Sie, dass Terminal- und PLC-Netzwerke durch separate Netzwerkkarten auf dem Host-System getrennt sind (dezidierte, physikalisch getrennte Netzwerkkarten).
- Für die Gast-Betriebssysteme gelten dieselben Hardware-Anforderungen wie für die jeweiligen TIA-Produkte selbst.
- Der Betreiber der Anlage muss dafür sorgen, dass den Gast-Betriebssystemen ausreichend Systemressourcen zur Verfügung gestellt werden.
- Für den Einsatz von HyperV-Server und ESXi empfehlen die Hersteller zertifizierte Hardware.

Unterstützte Sicherheitsprogramme

Folgende Sicherheitsprogramme sind kompatibel zu Unified Runtime:

Virenscanner	Symantec Endpoint Protection 14.3
	McAfee Endpoint Security (ENS) 10.6 und 10.7
	Trend Micro Office Scan 14.0
	Windows Defender (als Teil des Windows-Betriebssystems)
	Qihoo 360 "Safe Guard 12.1" + "Virus Scanner"

Whitelisting	McAfee Application Control 8.3.3
Festplattenverschlüsselung	Microsoft bit-locker (als Teil des Windows-Betriebssystems)

Grundsatz

Der Einsatz eines Virenscanners darf den Prozessbetrieb einer Anlage nicht beeinträchtigen.

Regeln für lokale Virenscanner (Virenscan-Clients)

- Integrierte Firewall der Virenscanner
  In WinCC Unified wird die verwendete lokale Windows-Firewall über den SIMATIC Security Control parametriert. Die integrierte Firewall der Virenscanner dürfen Sie nicht installieren bzw. aktivieren.
- Manueller Scan
  Einen manuellen Scan dürfen Sie nicht durchführen, während die Runtime in Betrieb ist. Führen Sie diesen Scan in regelmäßigen Abständen auf allen Anlagen-PCs durch, z. B. während eines Wartungsintervalls.
- Automatischer Scan
  Beim automatischen Scan reicht es aus, den eingehenden Datenverkehr zu durchsuchen.
- Zeitgesteuerter Scan
  Den zeitgesteuerten Scan dürfen Sie nicht durchführen, während die Runtime in Betrieb ist.
- Patternupdate
  Das Patternupdate der Virenscan-Clients (die Anlagen-PCs, die auf Viren geprüft werden) erfolgt vom übergeordneten Virenscan-Server (der Anlagen-PC, der die Virenscan-Clients zentral verwaltet).
- Dialoge
  Um den Prozessbetrieb nicht zu beeinträchtigen, darf auf den Virenscan-Clients keine Dialogmeldung angezeigt werden.
- Laufwerke
  Ausschließlich die lokalen Laufwerke werden gescannt, um überschneidende Scans auf Netzwerk-Laufwerken zu verhindern.

Übernehmen Sie sonst die Defaulteinstellungen.

Was wird sichergestellt?

Der eingehende Datenverkehr wird auf Viren geprüft. Die Beeinträchtigung des Prozessbetriebs wird minimiert.

Hinweis

Achten Sie beim Einsatz eines Virenscanners darauf, dass der Rechner über genügend System-Ressourcen verfügt.

Unterstützte Datenbanktypen

Folgende Datenbanktypen werden von SIMATIC WinCC Unified PC unterstützt:

Bediengerät	Unterstützter Datenbanktyp
SIMATIC WinCC Unified PC	SQLite
	Microsoft SQL

Microsoft SQL Server für Unified PC

WinCC Unified PC verwendet SQLite als voreingestellten Datenbanktyp. Für die Verwendung von Microsoft SQL Server stellt das System eine Installationsoption mit einem Setup-Paket zur Verfügung.

- Nach der Installation von Microsoft SQL Server ist keine Archivierung mit SQLite möglich.
- Bestehende SQLite-Dateien bleiben erhalten, sind aber nicht über Runtime erreichbar.
- Für SQLite kann kein Back-up erstellt werden.

Das "Microsoft SQL Server Management Studio" finden Sie bei Bedarf auf dem Installations-Medium im Ordner "Support\SQL Server Management Studio".

4.4.4 Installation von WinCC Runtime Professional

Für die Installation müssen bestimmte Anforderungen an Betriebssystem und Software-Konfiguration erfüllt sein.

Installation in Domänen und Arbeitsgruppen

WinCC ist grundsätzlich für den Betrieb in einer Domäne oder Arbeitsgruppe freigegeben.

Beachten Sie jedoch, dass Domänen-Gruppenrichtlinien und Einschränkungen der Domäne die Installation behindern können. Entfernen Sie in diesem Fall den Rechner vor der Installation von Microsoft Message Queuing, Microsoft SQL Server und WinCC aus der Domäne. Melden Sie sich an dem betreffenden Rechner lokal mit Administratorrechten an. Führen Sie die Installation durch. Nach der erfolgreichen Installation können Sie den WinCC-Rechner wieder in die Domäne aufnehmen. Wenn die Domänen-Gruppenrichtlinien und Einschränkungen der Domäne die Installation nicht behindern, muss der Rechner während der Installation nicht aus der Domäne entfernt werden.

Beachten Sie, dass Domänen-Gruppenrichtlinien und Einschränkungen der Domäne auch den Betrieb behindern können. Wenn Sie diese Einschränkungen nicht aufheben können, betreiben Sie die WinCC-Rechner in einer Arbeitsgruppe.

Wenden Sie sich gegebenenfalls an den Domänen-Administrator.

Betrieb auf einem Netzwerk Server

Der Betrieb von WinCC Runtime Professional auf einem Netzwerk Server (z. B. Domain Controller, File-Server, Namensdienst-Server, Router, Software Firewall, Media Server, Exchange Server) ist nicht zulässig.

Windows Rechnername

Ändern Sie den Windows Rechnernamen nach der WinCC-Installation nicht.

Wenn Sie den Windows Rechnernamen ändern, müssen Sie den SQL-Server deinstallieren und neu installieren.

Folgende Zeichen sind im Rechnernamen nicht zulässig:

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

Bei der Vergabe der Windows Rechnernamen beachten Sie Folgendes:

- Es darf nur Großschreibung verwendet werden.
- Das erste Zeichen muss ein Buchstabe sein.
- Die ersten 12 Zeichen des Rechnernamens müssen eindeutig sein.

Remote-Kommunikation aktivieren

Auf WinCC-Systemen ist die Remote-Kommunikation im Dialog "Simatic Shell" nach der Installation standardmäßig deaktiviert. Für folgende Anwendungsfälle müssen Sie die Remote-Kommunikation für die beteiligten Rechner aktivieren:

- Laden der Runtime auf einen anderen PC
- Client-Server-Kommunikation
- Redundantes System
- WinCC-Option "WebNavigator"
  Wenn der WebNavigator-Client nicht auf dem gleichen Rechner läuft wie der WebNavigator-Server, muss die Remote-Kommunikation aktiviert sein.

Um den Remote-Zugriff zu ermöglichen, gehen Sie folgendermaßen vor:

1. Öffnen Sie im Windows Explorer über das Kontextmenü von Simatic Shell die Kommunikationseinstellungen.
2. Aktivieren Sie die Option "Remote Kommunikation".
3. Konfigurieren Sie die verschlüsselte Kommunikation im Netzwerk: Wählen Sie den PSK-Schlüssel und den Port.
4. Wählen Sie den Netzwerkadapter sowie gegebenenfalls die Multicast-Einstellungen.

NTLMv1 und SMBv1 deaktivieren

Die Protokolle NTLMv1 und SMBv1 können deaktiviert werden. Die Deaktivierung der Protokolle hat keinen Einfluss auf den Betrieb von WinCC Runtime Professional.

Hinweis

Sicherheitsrisiko durch NTLMv1 und SMBv1

Die Verwendung der Protokolle NTLMv1 und SMBv1 stellt ein erhebliches Sicherheitsrisiko dar. Die Kommunikation im Netzwerk kann z. B. durch Man-in-the-Middle-Angriffe kompromittiert werden.

Abhängig vom Betriebssystem unterscheidet sich das Vorgehen zur Deaktivierung der Protokolle.

4.4.5 Deinstallation einer SQL-Instanz

Inhalt

Mit der Installation von WinCC V20 wird eine neue Microsoft SQL Server 2022 Instanz installiert.

Wenn Sie bereits eine Version von WinCC Runtime Professional installiert hatten, erfolgt die Aktualisierung des SQL Servers automatisch.

Hinweis

Durch eine Deinstallation von WinCC Runtime Professional oder von WinCC Professional wird die Instanz des SQL-Servers nicht deinstalliert.

Deinstallation einer SQL-Instanz

Wenn Sie eine Instanz des Microsoft SQL Server deinstallieren wollen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Systemsteuerung.
2. Klicken Sie auf "Programm deinstallieren".
3. Wählen Sie in der Liste der installierten Programme die zu deinstallierende Version von Microsoft SQL Server und klicken Sie auf "Deinstallieren/ändern".
4. Klicken Sie im Dialog auf "Entfernen".
5. Wählen Sie im Dialog "Instanz auswählen" die Instanz "WINCC" und klicken Sie auf "Weiter".
6. Klicken Sie im Dialog "Funktionen auswählen" auf "Alles auswählen" und anschließend auf "Weiter".
7. Klicken Sie im Dialog "Funktionsregeln" auf "Weiter".
8. Klicken Sie im Dialog "Bereit zur Deinstallation" auf "Entfernen".
9. Klicken Sie nach Abschluss der Deinstallation im Dialog "Abgeschlossen" auf "Schließen".

Übersicht über Prozesse und Services von TIA Portal-Komponenten

5

Bei der Installation des TIA Portals oder Komponenten des TIA Portals werden weitere Prozesse und Services mitinstalliert.

Die folgenden Tabellen bieten eine Übersicht über diese Prozesse, die zugehörigen Services und jeweiligen Funktionen:

Tabelle 5-1 Automation License Manager

Prozess	Zugehöriger Service	Funktion
almsrv64x.exe	almservice	Lizenzmanagement-Service / Hauptprozess
almsrvbubble64x.exe	-	Prozess für Tray Icon Info-Bubbles
almgui64x.exe	-	Grafische Benutzeroberfläche des Automation License Managers

Tabelle 5-2 TIA Administrator

Prozess	Zugehöriger Service	Funktion
almsrv64x.exe	almservice	Lizenzverwaltungs-Service
node.exe	SiemensAwb	Hostprozess der TIA Administrator Website
TiaAdminNotifier.exe	-	Anwenderbenachrichtigung und Tray Icon des TIA Administrators

Tabelle 5-3 ProSave

Prozess	Zugehöriger Service	Funktion
PTProSave.exe	-	ProSave, grafische Benutzeroberfläche Hauptprozess
S7TraceService64x.exe	S7TraceServiceX	S7Dos betreffendes Tracing
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event- und Parameterhandling
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (Erreichbarkeit via PN-Gerätename)
TraceConceptX.exe	TraceConceptX	S7Dos betreffendes Tracing
ALMPanelPlugin.exe	-	Plugin zur Kommunikation mit dem Automation License Manager
-	S7DOS SCP Remote	Wird mitinstalliert, ist jedoch nur bei Cloud Connector aktiv
CommunicationSettings.exe	-	Einstellung von Zugriffspunkten

Tabelle 5-4 WinCC Audit Viewer

Prozess	Zugehöriger Service	Funktion
AuditViewer.exe	-	WinCC Audit Viewer Hauptprozess

Tabelle 5-5 Port Configuration Tool (PCT)

Prozess	Zugehöriger Service	Funktion
Siemens.Simatic.Pct.ApplicationLoader.exe	-	Hauptprozess des Port Configuration Tools (PCT)
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event- und Parameterhandling
S7TraceService64x.exe	S7TraceServiceX	S7Dos betreffendes Tracing
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (Erreichbarkeit via PN-Gerätename)
TraceConceptX.exe	TraceConceptX	S7Dos betreffendes Tracing
s7elonls64.exe	-	Routing zwischen 32- und 64-bit-Applikationsteilen
CommunicationSettings.exe	-	Einstellung von Zugriffspunkten
-	S7DOS SCP Remote	Wird mitinstalliert, ist jedoch nur bei Cloud Connector aktiv

Tabelle 5-6 Cloud Connector

Prozess	Zugehöriger Service	Funktion
CloudConfigurator.exe	-	GUI zur Konfiguration des Cloud Connectors
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event- und Parameter-Handling
S7TraceService64x.exe	S7TraceServiceX	S7Dos betreffendes Tracing
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (Erreichbarkeit via PN-Gerätename)
TraceConceptX.exe	TraceConceptX	S7Dos betreffendes Tracing
CC.TunnelServiceHost.exe	S7DOS SCP Remote	Host des Tunnel-Services für den Cloud Connector
CommunicationSettings.exe	-	Einstellung von Zugriffspunkten

Tabelle 5-7 Projekt-Server

Prozess	Zugehöriger Service	Funktion
Siemens.Automation.Portal.Server(.exe)	prjserv	TIA Portal Projekt-Server Hauptprozess
Siemens.Automation.Portal.Project.Server(.exe)	-	TIA Portal Projekt-Server Hauptprozess
Siemens.Automation.Portal.Server.Configuration(.exe)	-	Oberfläche zur Konfiguration des Projekt-Servers

Prozess	Zugehöriger Service	Funktion
Siemens.Automation.Portal.Server.Administration(.exe)	-	Oberfläche zur Administration des Projekt-Servers
Siemens.Automation.ProjectServer.AccessControl(.exe)	-	Steuert die Zugriffsberechtigung des Administrationstools

Tabelle 5-8 WinCC Runtime Advanced

Prozess	Zugehöriger Service	Funktion
ScsServer.exe	-	Zentrale Datenkommunikation
StartCenter.exe	-	Start Center, welches beispielsweise den Start der Runtime erlaubt
HmiRTm.exe	-	Die WinCC-Advanced Runtime selbst
s7elonls64.exe	-	Routing zwischen 32- und 64-bit-Applikationsteilen
Miniweb.exe	-	Webinhalte der WinCC Runtime Advanced
CodeMeterCC.exe	-	Laufzeitservice des CodeMeters
CmWebAdmin.exe	CmWebAdmin.exe	Web-Administrator des CodeMeters
SmartServer.exe	cortsmartserver	Smart Server Hostprozess zur Remote-Verbindung
CodeMeter.exe	CodeMeter.exe	CodeMeter-Lizenzierung zur Laufzeit
S7TraceService64x.exe	S7TraceServiceX	S7Dos betreffendes Tracing
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event- und Parameter-Handling
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (Erreichbarkeit via PN-Gerätename)
-	OpcEnum	Service wird nur installiert, aber nicht gestartet.

Tabelle 5-9 TIA Portal mit STEP 7 / WinCC Comfort / Advanced

Prozess	Zugehöriger Service	Funktion
CodeMeterCC.exe	-	Laufzeitservice des CodeMeters
Siemens.Automation.Portal.exe	-	Das TIA Portal selbst
Siemens.Automation.ObjectFrame.FileStorage.Server.exe	-	Prozess zur Datenverwaltung bei TIA Portal-Projekten
Siemens.Automation.Diagnostics.CrashDetector.exe	-	Prozess zur Erkennung von TIA Portal-Crashes und Anzeige der Crash-Box
Siemens.Automation.Tracing.ETW.EventCollector.ServiceHost.exe	Siemens Diagnostics Data Collector Service	Prozess zur Eventdatensammlung
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event- und Parameter-Handling
CmWebAdmin.exe	CmWebAdmin.exe	Web-Administrator des CodeMeters
CodeMeter.exe	CodeMeter.exe	CodeMeter-Lizenzierung zur Laufzeit

Prozess	Zugehöriger Service	Funktion
S7TraceService64x.exe	S7TraceServiceX	S7Dos betreffendes Tracing
Siemens.Simatic.TelemetryConnector.WindowsService.exe	Siemens Telemetry Connector Service	Service zum Sammeln und Versenden von Telemetriedaten
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (Erreichbarkeit via PN-Gerätename)
TraceConceptX.exe	TraceConceptX	S7Dos betreffendes Tracing
IPCSecCom.exe	umscsvc	Kommunikation zu einem UMC-Server
um.Ris.exe	-	Basis-Executable von UMC
um.sso.exe	-	Single Sign-on bei UMC
um.ess.exe	-	Basis-Executable von UMC
S7otbxsx64.exe	-	S7Dos Block-Administration
-	OpcEnum	Service wird nur installiert, aber nicht gestartet
-	UMC Service	Wird nur bei Benutzung von UMC / UMAC genutzt
Siemens.Automation.Help.Viewer.Web.Service.exe	Siemens TIA Help Viewer Service	Ermöglicht die Anzeige des Informationssystems im Standard-Browser

Tabelle 5-10 STEP 7 / Safety / WinCC Professional ES inkl. Simulation

Prozess	Zugehöriger Service	Funktion
CodeMeterCC.exe	-	Laufzeitservice des CodeMeters
Siemens.Automation.Portal.exe	-	Das TIA Portal selbst
Siemens.Automation.ObjectFrame.FileStorage.Server.exe	-	Prozess zur Datenverwaltung bei TIA Portal-Projekten
Siemens.Automation.Diagnostics.CrashDetector.exe	-	Prozess zur Erkennung von TIA Portal-Crashes und Anzeige der Crash-Box
Siemens.Automation.Tracing.ETW.EventCollector.ServiceHost.exe	Siemens Diagnostics Data Collector Service	Prozess zur Eventdatensammlung
s7oiehsx64.exe	s7oiehsx64	S7Dos Helper Service
s7epasrv64x.exe	-	Event- und Parameterhandling
CmWebAdmin.exe	CmWebAdmin.exe	Web-Administrator des CodeMeters
CodeMeter.exe	CodeMeter.exe	CodeMeter-Lizenzierung zur Laufzeit
S7TraceService64x.exe	S7TraceServiceX	S7Dos betreffendes Tracing
Siemens.Simatic.TelemetryConnector.WindowsService.exe	Siemens Telemetry Connector Service	Service zum Sammeln und Versenden von Telemetriedaten
s7oPNDiscoveryx64.exe	SIMATIC PnDiscovery Service	PN Discovery (Erreichbarkeit via PN-Gerätename)
TraceConceptX.exe	TraceConceptX	S7Dos betreffendes Tracing
IPCSecCom.exe	umscsvc	Kommunikation zu einem UMC-Server
um.Ris.exe	-	Basis-Executable von UMC
um.sso.exe	-	Single Sign-on bei UMC
um.ess.exe	-	Basis-Executable von UMC
S7otbxsx64.exe	-	S7Dos Block-Administration

Prozess	Zugehöriger Service	Funktion
CCDeltaLoader.exe	CCDeltaLoader	Zuständig für die Erkennung, ob ein Delta-Download möglich ist
RedundancyControl.exe	RedundancyControl	Zuständig für die Erkennung und Verwaltung des Zustands der redundanten WinCC-Partner
CCTextServer.exe	CCTextServer	Server zur Runtime-Anzeige von Texten
CCPerfMon.exe	CCPerfMon	WinCC STOBS, Überwachung von Systemparametern und WinCC-Prozessen
SCSFsX.exe	SCSFsX	WinCC File Service zwischen Clients und Servern
CCRtsLoader_x64.exe	CCRtsLoader	WinCC RT Variablenhaushalt
CCSystemDiagnosticsHost.exe	CCSystemDiagnosticsHost	Host für die Anzeige von Systemdiagnose
CcAlgRtServer.exe	CCAlgRtServer	WinCC Alarm Logging Runtime Server
CCArchiveManager.exe	CCArchiveManagerService	Management von WinCC-Archiven
CCRedundancyAgent.exe	CCRedundancyAgent-Service	Archivierungskomponente zur Verwaltung und zum Abgleich der RT-Archive
CCTlgServer.exe	CCTlgServer	WinCC Tag Logging Server
CCUsrAcv.exe	CCUsrAcv	Zuständig für die Verwaltung von User-Archiven
CCProfileServer.exe	CCProfileServer	Speicherung von RT-Persistenzdaten der WinCC-Controls
sqlservr.exe	MSSQL$WINCC	SQL-Server für WinCC
CCAgent.exe	CCAgent	WinCC RT-Komponente für die Kommunikation zwischen WinCC-Stationen
CCEServer_x64.exe	CCEServer	WinCC RT-Komponente für die Kommunikation zwischen WinCC-Stationen
CCProjectMgr.exe	CCProjectMgr	WinCC Project Manager, Handling für WinCC-Projekte
SDiagRT.exe	-	Systemdiagnose Datenkollektor
gscrt.exe	-	WinCC Global Script Runtime
PassDBRT.exe	-	Verwaltung von Anmeldedaten und Passwörtern
CCUAImport.exe	-	WinCC RT User Archive Komponente, um TIA Rezepte zu importieren
script.exe	-	WinCC RT C Scripting Komponente
PdlRt.exe	-	Grafische Runtime
SCSDistServiceX.exe	SCS Distribution Service	WinCC RT-Komponente für die Kommunikation zwischen WinCC-Stationen
SCSMX.exe	SCSMonitor	WinCC RT-Komponente für die Kommunikation zwischen WinCC-Stationen
sqlbrowser.exe	SQLBrowser	Microsoft SQL-Prozess (WinCC benutzt den SQL-Server)
sqlwriter.exe	SQLWriter	Microsoft SQL-Prozess (WinCC benutzt den SQL-Server)
CCDBUtils.exe	CCDBUtils	WinCC Komponente zur Verwaltung der WinCC SQL-Datenbank

Prozess	Zugehöriger Service	Funktion
CCRemoteService.exe	CCRemoteService	WinCC Komponente zur Remote-Verwaltung der WinCC SQL-Datenbank
sqlceip.exe	SQLTELEMETRY$WINCC	Microsoft SQL-Prozess (WinCC benutzt den SQL-Server)
CCEClient_x64.exe	CCEClient	WinCC RT-Komponente für die Kommunikation zwischen WinCC-Stationen
RedundancyState.exe	RedundancyState	Clientseitige Überwachung der Zustände der WinCC-Server
CCPackageMgr.exe	CCPackageMgr	WinCC-Komponente zur Verwaltung der Server Packages
CCNSInfo2Provider.exe	CCNSInfo2Provider	WinCC Komponente zum Browsen von WinCC- / STEP 7-Variablen
Siemens.Simatic.Srm.RdpComp.Data.ContextMgrX.exe	-	SCADA RT Professional Compiler-Komponente
CCDmRuntimePersistence.exe	-	WinCC RT-Komponente zur Abgleich der internen Variablen in redundanten Systemen
CCWriteArchiveServer.exe	-	Zuständig, um Archivdaten in die SQL-Datenbank zu schreiben (3 Instanzen: TLG-fast / TLG-slow / ALG)
CCLicenseService.exe	CCLicenseService	Zuständig für die Belegung und Freigabe von Lizenzen
CCUCSurrogate.exe	-	WinCC RT Professional Anwendung für das System Tray Icon in der Windows-Taskleiste
Simulation.exe	-	WinCC RT Professional Variablensimulation
CCConfigStudio.exe	-	WinCC Config Studio ist eine Applikation für die WinCC RT Professional Variablensimulation
WinCCChnDiag.exe	-	WinCC Kanaldiagnose
-	CCTMTimeSyncServer	Wird bei redundantem Server zur Synchronisation von Zeitstempeln genutzt
-	CcUaDAS	WinCC OPC UA-Komponente
-	CCOpcUaImporter	WinCC OPC UA-Komponente
-	CCAlgIAlarmDataCollector	WinCC RT Professional Meldesystem
-	SQLAgent$WINCC	Microsoft SQL-Prozess (WinCC benutzt den SQL-Server)
-	OpcEnum	OPC Foundation-Komponente (WinCC OPC); Service wird nur installiert, aber nicht gestartet
-	UMC Service	Wird nur bei Benutzung von UMC / UMAC genutzt

Tabelle 5-11 WinCC Advanced Runtime Simulation

Prozess	Zugehöriger Service	Funktion
HmiRTm.exe	-	Die WinCC-Advanced Runtime selbst
Miniweb.exe	-	Webinhalte der WinCC Runtime Advanced
SmartServer.exe	cortsmartserver	Smart Server Hostprozess zur Remote-Verbindung
HmiRTmSim.exe	-	WinCC Advanced Variablensimulation

Tabelle 5-12 WinCC Unified Engineering-Paket

Prozess	Zugehöriger Service	Funktion
opcualds.exe	UALDS	OPC UA Local Discovery Service
mDNSResponder.exe	OPCF Bonjour Service	DNS-Namensauflösung
GfxWebBrowser.exe	-	Grafisches Rendering

Tabelle 5-13 WinCC Unified Simulation

Prozess	Zugehöriger Service	Funktion
WCCILS7pComDrv(.exe)	-	Prozess zur Kommunikation mit S7-1200 und S7-1500 Steuerungen
RTILtraceTool(.exe)	TraceLogger_WinCC_Unified_PC	Unified Simulation betreffendes Tracing
RTILtraceTool(.exe)	TraceProfiler_WinCC_Unified_PC	Unified Simulation betreffendes Tracing
w3wp(.exe)	-	IIS Process Worker, Hostprozess für Webseiten
WCCILscs(.exe)	WCCILScsService	Siemens Communication Service, zuständig für die interne Datenkommunikation
WCCILpmon(.exe)	-	WinCC Process Monitoring
WCCILalg(.exe)	-	WinCC AlarmLogging, zuständig für die Protokollierung von Alarmen
WCCILevent(.exe)	-	WinCC Event handling, zuständig für das Handling von Events
GfxLicenseServer(.exe)	-	Zuständig für das Belegen und Freigeben von Lizenzen
JobSchedulerHost(.exe)	-	Zuständig für das Scheduling von Aufträgen
GfxRTS(.exe)	-	Aufbereitung der grafischen Runtime
WCCILSDAMgr(.exe)	-	System Diagnostics Manager, zuständig für die Systemdiagnose-Informationen
OpennessManagerHost(.exe)	-	Host für den Openness-Manager
WCCILdist(.exe)	-	WinCC Unified Simulation Basisprozess
WCCILdata(.exe)	-	WinCC Unified Datamanager
WCCILals(.exe)	-	WinCC AlarmServer, zuständig für das Empfangen und Quittieren von Alarmen

Prozess	Zugehöriger Service	Funktion
WCCILpaco(.exe)	-	WinCC Parameter Control
WCCILtlg(.exe)	-	WinCC TagLogging, zuständig für die Protokollierung von Tags
WCCILs7(.exe)	-	Prozess zur Kommunikation mit S7-300 und S7-400 Steuerungen
umcd(.exe)	UmclService	UMS Basisprozess
idp(.exe)	UmclIdpService	UMS Basisprozess
-	EventLogger	Event Logging Service
-	UmclWebUMService	Webservice für User Management
-	umscsvc	User Management Secure Communication Service
-	w3logsvc	IIS Logging Service
-	WMSVC	IIS Web Management Service
UAAppStarterHost.exe	UAAppStarterHost.exe	Systemfunktion, um für ProDiag-Szenarien vom Web Client zum TIA Portal zu springen.
OpcUAServerRTIL.exe	OpcUAServerRTIL.exe	Bietet den Zugriff auf WinCC Unified via OPC UA-Protokoll.
webums.exe	-	Webinterface für die Benutzerverwaltung mit User Management Component (UMC), um UMC-Objekte zu verwalten.
REPDataProviderHost.exe	-	Reporting ermöglicht die Konfiguration von Vorlagen und die Erstellung von Excel- und PDF-basierten Berichten über Produktionsdaten.
WCCILgraphQLServer.exe	GraphQL Server	GraphQL Web API

Tabelle 5-14 Add-Ins

Prozess	Zugehöriger Service	Funktion
Siemens.Automation.AddIn.Rollout.Service.exe	Siemens Add-In Rollout Service	Massen-Rollout von Corporate Add-Ins

Security Logging verwenden

6

6.1 Security Logging im TIA Portal

Security Logging im TIA Portal ist eine Funktion, um sicherheitsrelevante Ereignis- und Protokolldaten aus dem Engineering System sowie von Komponenten der Automatisierungsumgebung zu erfassen, zu speichern und zu analysieren.

Die Ereignis- und Protokolldaten werden in Windows-Systemen lokal gespeichert. Über die Windows Ereignisanzeige können diese Daten analysiert, gespeichert und exportiert werden.

In einem weiteren Schritt können die Ereignis- und Protokolldaten an SIEM-Systeme (**S**ecurity **I**nformation and **E**vent **M**anagement) übertragen werden. Somit ermöglicht Security Logging, sicherheitsrelevante Ereignisse von verschiedenen Systemen im Netzwerk zentral zu sammeln, zu analysieren und auf Bedrohungen zu reagieren. Security Logging reiht sich ein in ein Bündel von Maßnahmen, wie sie von internationalen Security-Standards und -Regularien zur Erhöhung der Sicherheit empfohlen werden.

Security Logging ist im TIA Portal standardmäßig deaktiviert. Administratoren können Security Logging über eine Batch-Datei initial aktivieren. Wenn Security Logging aktiviert wurde, kann die Funktion anschließend entweder über Batch-Dateien oder über die Windows-Registrierungsdatenbank deaktiviert und wieder aktiviert werden.

Siehe auch

Security Logging aktivieren und deaktivieren (Seite 71)

6.2 Security Logging aktivieren und deaktivieren

Der Ereigniskanal für Security Logging wird mit der Installation des TIA Portals auf dem Computer registriert, jedoch ist die Funktion standardmäßig deaktiviert. Security Logging aktivieren und deaktiveren Sie in der Windows-Registrierungsdatenbank (Registry), indem Sie im Schlüssel "AuditLogOn" den entsprechenden Wert setzen. Mit dem Wert "1" ist Security Logging aktiviert, mit anderen Werten ist Security Logging deaktiviert. Standardmäßig ist Security Logging im TIA Portal deaktiviert.

Der Schlüssel "AuditLogOn" wird bei der Installation des TIA Portals nicht angelegt. Sie finden im Installationsverzeichnis des TIA Portals im Ordner "bin" zwei Batch-Dateien:

- Die Batch-Datei "SecurityAuditLoggingEnable.bat" aktiviert Security Logging.
- Die Batch-Datei "SecurityAuditLoggingDisable.bat" deaktiviert Security Logging.

Security Logging ist versionsspezifisch. Die Einstellung hat auf andere Versionen des TIA Portals keine Auswirkung.

Voraussetzungen

- Sie haben Windows-Administratorrechte.
- Um Benutzeraccounts zu protokollieren, muss das Projekt geschützt sein.

Security Logging per Batch-Datei aktivieren

1. Navigieren Sie im Installationsverzeichnis des TIA Portals zum Ordner "bin".
2. Führen Sie die Batch-Datei "SecurityAuditLoggingEnable.bat" aus.

Security Logging per Batch-Datei deaktivieren

1. Navigieren Sie im Installationsverzeichnis des TIA Portals zum Ordner "bin".
2. Führen Sie die Batch-Datei "SecurityAuditLoggingDisable.bat" aus.

Security Logging in der Windows-Registrierungsdatenbank aktivieren und deaktivieren

1. Öffnen Sie unter Windows den Registrierungs-Editor.
2. Navigieren Sie zum Schlüssel "HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\Automation\SecurityLogging\21.0\Settings".
3. Um Security Logging zu aktivieren, geben Sie im Schlüssel "LoggingOn" den Wert "1" ein. Um Security Logging zu deaktivieren, löschen oder ändern Sie im Schlüssel "LoggingOn" den Wert "1".
4. Bestätigen Sie Ihre Eingabe mit "OK".

Siehe auch

Security Logging im TIA Portal (Seite 71)

Übersicht über Ereignisse (Seite 72)

6.3 Übersicht über Ereignisse

Die folgenden Tabellen bieten eine Übersicht über Anwenderaktionen, die zugehörigen Log-Einträge, die Ereigniskategorien und Ereignistypen.

Zusätzlich zum Inhalt der in den folgenden Tabellen aufgeführten Ereignisse enthält jedes Ereignis die folgenden Informationen:

- Version des TIA Portals
- Name des Projekts
- Name des angemeldeten Benutzers aus der Benutzerverwaltung (UMAC - User Management and Access Control)

Hinweis

Name des angemeldeten Benutzers

Der Wert für den Namen des angemeldeten Benutzers aus der Benutzerverwaltung (UMAC) wird in drei verschiedenen Kategorien gesetzt:

- Kategorie 1: Der Text "No user logged in." erscheint in dem Fall, wenn die Benutzerverwaltung (UMAC) entweder im Projekt nicht aktiviert ist oder außerhalb des Projekts an einem Gerät unter "Erreichbare Teilnehmer" kein Benutzer angemeldet ist.
- Kategorie 2: Der Text "Background process" erscheint in dem Fall, wenn UMAC für das Projekt aktiviert ist, aber eine sicherheitskritische Operation von einem Hintergrundprozess ausgelöst wird (z. B. wenn im Multiuser Commissioning im "asynchronen Modus" ein Prozess Daten in ein Gerät lädt).
- Kategorie 3: Der Name des angemeldeten Benutzers aus der Benutzerverwaltung (UMAC) erscheint in dem Fall, wenn UMAC für das Projekt aktiviert ist und das Ereignis von dem TIA Portal Hauptprozess geschrieben wurde.

Übersicht über Ereignisse

Tabelle 6-1 Benutzerverwaltung (UMAC - User Management and Access Control)

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Lokalen Benutzer hinzufügen	Local user "{target user}" added	Zugriffssteuerung	Informationen
Lokalen Benutzer löschen	Local user "{target user}" deleted	Zugriffssteuerung	Informationen
Zentralen Benutzer hinzufügen	Global user "{target user}" added	Zugriffssteuerung	Informationen
Zentralen Benutzer löschen	Global user "{target user}" removed	Zugriffssteuerung	Informationen
Benutzergruppe hinzufügen	User group "{target user}" added	Zugriffssteuerung	Informationen
Benutzergruppe löschen	User group "{target user}" removed	Zugriffssteuerung	Informationen
An einem geschützten Projekt anmelden	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	Zugriffssteuerung	Informationen, Fehler

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Von einem geschützten Projekt abmelden	Local / Global user "{target user}" logged out Anonymous user logged out	Zugriffssteuerung	Informationen
Benutzernamen eines lokalen Benutzers ändern	User "{target user}" renamed to "{new target user name}"	Konfiguration	Informationen
Passwort eines lokalen Benutzers oder eigenes Passworts ändern	Local / Global user "{target user}" password changed	Konfiguration	Informationen
Lokalen Benutzer, zentralen Benutzer oder Benutzergruppe aktivieren	Local / Global user / group "{target user}" activated	Konfiguration	Informationen
Lokalen Benutzer, zentralen Benutzer oder Benutzergruppe deaktivieren	Local / Global user / group "{target user}" de-activated	Konfiguration	Informationen
Eigenschaften eines Benutzers ändern	User "{target user}" property '{property name}' changed to {new property value}	Konfiguration	Informationen
Benutzerdefinierte Rolle im TIA Portal anlegen	Custom role "{role name}" created	Konfiguration	Informationen
Benutzerdefinierte Rolle im TIA Portal löschen	Custom role "{role name}" deleted	Konfiguration	Informationen
Benutzerdefinierte Rolle im TIA Portal umbenennen	Custom role "{old role name}" renamed to "{new role name}"	Konfiguration	Informationen
Zuweisung eines Funktionsrechts zu einer benutzerdefinierten Rolle im TIA Portal ändern	Custom role "{role name}" function rights assignment changed to "{semicolon seperated list of function rights}"	Konfiguration	Informationen
Runtime Timeout einer benutzerdefinierten Rolle im TIA Portal ändern	Custom role "{role name}" property 'Runtime timeout' changed to {new runtime timeout}	Konfiguration	Informationen
Einem Benutzer oder einer Benutzergruppe eine Rolle zuweisen	Local user / Global user / User group "{target user name}" roles assignment changed to "{semicolon seperated list of roles}"	Konfiguration	Informationen

Tabelle 6-2 Änderungen von CPU-Daten (offline)

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Projektintegrität prüfen	Data integrity check succeeded / failed. A {data integrity error type} Integrity corruption found in object {object id} in project {project name}	AuditLog	Überwachung erfolgreich, Fehler

Tabelle 6-3 Laden in CPU

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Hardware-Konfiguration in eine CPU laden	Download of hardware configuration to {PLC name} with address {address}	Konfiguration	Überwachung erfolgreich
Standard-Anwenderprogramm in eine CPU laden (Startmeldung)	Software download started to target PLC: {PLC name} with address {address} Operating mode during download: {RUN|STOP} Type of download: {Delta|Complete}	Konfiguration	Informationen
Standard-Anwenderprogramm in eine CPU laden (Liste der zu ladenden oder zu löschenden Bausteine, ggf. mehrfach)	Software objects downloaded (+) / deleted (-): {+|-} {full qualified name of object} {+|-} {full qualified name of object} ...	Konfiguration	Informationen
Standard-Anwenderprogramm in eine CPU laden (Abschlussmeldung mit Software-Signatur)	Erfolgreich: Software download succeeded Software signature after sownload {signature|"null"} Fehler: 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	Konfiguration	Überwachung erfolgreich, Fehler
Failsafe-Programm in eine CPU laden	Downloaded safety program with the collective F-signature {collective F-signature}.	Konfiguration	Überwachung erfolgreich

Tabelle 6-4 Laden des Geräts als neue Station

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Konfiguration von einer CPU laden	Upload of {PLC name} with address {address}.	Konfiguration	Überwachung erfolgreich, Fehler

Tabelle 6-5 Änderungen von CPU-Daten (online)

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Auf eine CPU zugreifen	Erfolgreich: Login to Plc {PLC name} with address {address} is successful. Fehler: Login to Plc {PLC name} with address {address} failed.	Zugriffssteuerung	Überwachung erfolgreich, Fehler
Variablen über Online-Zugang auf eine CPU forcen	Forcejob auf Ziel-CPU installiert: {PLC name} with address {address} Forced variables (address : value): Adr1 : value1 Adr2 : value2 ... Forcejob auf Ziel-PLC ersetzt: {PLC name} with address {address} Forced variables (address : value): Adr1 : value1 Adr2 : value2 ... Forcejob auf Ziel-CPU gestoppt: {PLC name} with address {Address}	Konfiguration	Überwachung erfolgreich
IP / Netzwerkkonfiguration einer CPU über Online-Zugang ändern	Change the network settings of {device name}({address}) to [IpAddress:{address to set}| SubnetMask:{subnet mask}| Router address:{router address}]	Konfiguration	Überwachung erfolgreich, Fehler
Passwort zum Schutz vertraulicher Konfigurationsdaten über Online-Zugang ändern	Set password for "Protection of PLC configuration data" of {PLC name}({address}) Delete password for "Protection of PLC configuration data" of {PLC name}({address})	Konfiguration	Überwachung erfolgreich, Fehler
Betriebszustand einer CPU über Online-Zugang ändern	Set {PLC name}({address}) to Run/Stop	Konfiguration	Überwachung erfolgreich, Fehler
Systemzeit einer CPU über Online-Zugang ändern	Change the system time of {device name}({address}) to {date time}	Konfiguration	Überwachung erfolgreich, Fehler

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Sichern / Wiederherstellen einer CPU über Online-Zugang initiieren	Sichern: Backup created from {PLC name} with address {address}. Wiederherstellen: Online backup {backup name} restored to {PLC Name} with address {address}.	Konfiguration	Überwachung erfolgreich
Firmware-Update einer CPU über Online-Zugang initiieren	Firmware update of {PLC name} ({address}) to version {fw version}	Konfiguration	Überwachung erfolgreich, Fehler
CPU auf Werkseinstellungen zurücksetzen	Reset to factory setting of {PLC name} ({address}). Einstellungen: • IP-Adresse löschen • Master-Passwort löschen • Memory Card formatieren	Konfiguration	Überwachung erfolgreich, Fehler
MRES über Online-Zugang	Memory reset of {PLC name} {address}	Konfiguration	Überwachung erfolgreich, Fehler
Memory Card formatieren	Formatting the memory card of {PLC name}{address}	Konfiguration	Überwachung erfolgreich, Fehler

Tabelle 6-6 Änderungen Zugriffsstufe

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Zugriffsstufe ändern	Protection access level is changed from "{previously selected access level}" to "{current selection access level}" for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für vollen Zugriff konfigurieren	Protection Access password is configured successfully / failed to configure for "Full Access" for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für vollen Zugriff ändern	Protection access password is changed successfully / failed to change for "Full Access" for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für vollen Zugriff inkl. Failsafe (kein Schutz) konfigurieren	Protection access password is configured successfully / failed to configure for "Full access incl. fail safe (no protection)" for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für vollen Zugriff inkl. Failsafe (kein Schutz) ändern	Protection access password is changed successfully / failed to change for "Full Access incl. fail safe (no protection)" for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Passwort für Lesezugriff konfigurieren	Protection access password is configured successfully / fail to change for "Read Access" for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für Lesezugriff ändern	Protection access password is changed successfully / fail to change for "Read Access" for {PLC-name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für HMI-Zugriff konfigurieren	Protection access password is configured successfully / failed to configure for "HMI Access" for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für HMI-Zugriff ändern	Protection access password is changed successfully / fail to change for "HMI Access" for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler

Tabelle 6-7 Schutz von CPU-Konfigurationsdaten

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Schutz von vertraulichen CPU-Konfigurationsdaten deaktivieren	"Protection of PLC configuration data" is disabled / failed to disable for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Schutz von vertraulichen CPU-Konfigurationsdaten aktivieren	"Protection of PLC configuration data" is enabled / failed to enable for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für Schutz von vertraulichen CPU-Konfigurationsdaten konfigurieren	Password for "Protection of PLC configuration data" is configured successfully / failed to configure for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für Schutz von vertraulichen CPU-Konfigurationsdaten ändern	Password for "Protection of PLC configuration data" is changed successfully / failed to change for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler
Passwort für Schutz von vertraulichen CPU-Konfigurationsdaten zurücksetzen	Password for "Protection of PLC configuration data" is reset successfully / failed to reset for {PLC name}	Konfiguration	Überwachung erfolgreich, Fehler

Tabelle 6-8 WinCC ES

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
OPC UA: Gastauthentifizierung umschalten	Device {deviceName}: OPC UA guest authentication {enabled | disabled}>	Konfiguration	Informationen
OPC UA: Authentifizierung mit Benutzername und Passwort umschalten	Device {deviceName}: OPC UA username and password authentication {enabled | disabled}	Konfiguration	Informationen

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
OPC UA-Server aktivieren oder deaktivieren	Device {deviceName}: OPC UA server {activated | deactivated}	Konfiguration	Informationen
OPC UA: Sicherheitsrichtlinien aktivieren oder deaktivieren	Device {deviceName}: OPC UA security policy {policyName} {enabled | disabled}	Konfiguration	Informationen
Runtime-Einstellung: Maximale Anzahl fehlgeschlagener Anmeldeversuche ändern	Device {deviceName}: Account deactivation changed from {oldValue} to {newValue}	Konfiguration	Informationen
Runtime-Einstellung: Maximale Anzahl fehlgeschlagener Anmeldeversuche ändern	Device {deviceName}: Account deactivation {enabled | disabled}	Konfiguration	Informationen
Runtime-Einstellung: Zentrale/lokale Benutzerverwaltung der Runtime ändern	Device {deviceName}: UMAC source changed to {central | local}	Konfiguration	Informationen
Runtime-Einstellung: Zentrales UMAC-Serverpasswort für die Runtime ändern	Device {deviceName}: Change of central UMAC server settings. {fieldName}: {oldValue} → {newValue}	Konfiguration	Informationen
Runtime-Einstellung: Konfiguration im Runtime-Securityeditor ändern	Device {deviceName}: RT configuration change for configuration item {item}: {property}	Konfiguration	Informationen
Runtime-Einstellung: Konfiguration im Runtime-Securityeditor ändern	Device {deviceName}: RT configuration change: {item} created.	Konfiguration	Informationen
Runtime-Einstellung: Konfiguration im Runtime-Securityeditor ändern	Device {deviceName}: RT configuration change: {item} deleted.	Konfiguration	Informationen
Online-Sicherung initiieren	Device {deviceName}: Online backup initiated	Sichern, Wiederherstellen	Informationen
Online-Wiederherstellung initiieren	Device {deviceName}: Online restore initiated	Sichern, Wiederherstellen	Informationen
Transportpasswort eingeben	Erfolgreich: Device {deviceName}: Transport password entered by user verified Fehler: Device {deviceName}: Failed to verify transport password entered by user	Zugriffssteuerung	Überwachung erfolgreich, Fehler
Laden in Gerät starten	Software download started to target {deviceName} with address {address}. Load Preview settings: {Listing of settings}.	Konfiguration	Informationen

Anwenderaktion	Log-Eintrag	Ereigniskategorie	Ereignistyp
Sichere Kommunikation konfigurieren	Device {deviceName}: Secure communication was {enabled | disabled} for remote device with systemId {systemId}.	Konfiguration	Informationen
Server-Einstellungen des Smart Servers konfigurieren	Device {deviceName}: Smart Server service {service} {enabled | disabled}	Konfiguration	Informationen
Einstellungen des Web Clients konfigurieren	Device {deviceName}: Web Client is {enabled | disabled}	Konfiguration	Informationen
Autorisierungseigenschaft auf Screen Item ändern	Device {deviceName}: Authorization property changed for item {screenItem} from {oldValue} to {newValue}	Konfiguration	Informationen
Transportpasswort zum Laden von Zertifikaten und verschlüsselten Passwörtern für RT Advanced oder Professional erstellen	Device {deviceName}: Transport password created	Konfiguration	Informationen
Transportpasswort zum Laden von Zertifikaten und verschlüsselten Passwörtern für RT Advanced oder Professional ändern	Device {deviceName}: Transport password changed	Konfiguration	informationen
Transportpasswort zum Laden von Zertifikaten und verschlüsselten Passwörtern für RT Advanced oder Professional entfernen	Device {deviceName}: Transport password removed	Konfiguration	Informationen
Neues Gerätezertifikat erstellen	Device {deviceName}: Device certificate with fingerprint {fingerprint} created	Konfiguration	Informationen
Know-how-Schutz aktivieren oder deaktivieren	Device {deviceName}: Know-how protection {enabled | disabled} for item {item}	Konfiguration	Informationen
Gerät umbenennen	Device {oldDeviceName}: Device name changed to {newDeviceName}	Konfiguration	Informationen

Siehe auch

Security Logging im TIA Portal (Seite 71)

Ereignisse anzeigen und verwalten (Seite 81)

6.4 Ereignisse anzeigen und verwalten

Ereignisse lassen sich unter Windows in der Ereignisanzeige anzeigen und verwalten. Daneben werden über Microsoft Windows Funktionen bereitgestellt, um Ereignisse automatisiert zu verfolgen.
Um Ereignisse von verschiedenen Systemen im Netzwerk zentral zu sammeln, zu analysieren und weiter zu verarbeiten, können Ereignisse in ein SIEM-System (**S**ecurity **I**nformation and **E**vent **M**anagement) übertragen werden. Für Informationen zur Übertragung von Ereignissen in ein SIEM-System nutzen Sie die Dokumentation des Anbieters.

Ereignisse in der Ereignisanzeige anzeigen

1. Öffnen Sie unter Windows die Ereignisanzeige.
2. Navigieren Sie in der linken Spalte zu dem Knoten "Ereignisanzeige (Lokal) > Anwendungs- und Dienstprotokolle > SiemensAG > Automation > TIAPortal".
3. Wählen Sie das Protokoll "Operational" aus.
   Im oberen Teil des Hauptfensters werden die Ereignisse des Protokolls angezeigt.
4. Wählen Sie ein Ereignis aus.
   Im unteren Teil des Haupfensters werden in den Registerkarten "Allgemein" und "Details" Informationen zu dem ausgewählten Ereignis angezeigt.
5. Um Informationen zu einem Ereignis in einem neuen Fenster zu öffnen, doppelklicken Sie auf das Ereignis.

Ereignisse in der Ereignisanzeige verwalten

1. Wechseln Sie in der Ereignisanzeige in die rechte Spalte "Aktionen".
2. Nutzen Sie die Aktionen, um Ihre Protokolldateien zu verwalten.
   Sie können z. B. Protokolle filtern, durchsuchen, speichern und löschen.

Ereignisse automatisiert verfolgen

Die folgenden Funktionen von Microsoft Windows lassen sich für die automatisierte Verfolgung von Ereignissen verwenden:

- Das Befehlszeilenprogramm **wevtutil** lässt sich zum Auslesen von Ereignissen über die Kommandozeile nutzen. Das Programm wird über Microsoft Windows bereitgestellt.
- Das TIA Portal stellt die Ereignisse über die **Ereignisablaufverfolgung für Windows** (**E**vent **T**racing for **W**indows - **ETW**) bereit. Anwendungen (z. B. ein SIEM-System), die die Ereignisse abrufen wollen, können auf diese Ereignisse über die Ereignisquelle "SiemensAG-Automation-TIAPortal" zugreifen.

Für weitere Informationen zur Umsetzung der automatisierten Verfolgung von Ereignissen nutzen Sie die Dokumentation der Funktionen von Microsoft.

Siehe auch

Security Logging im TIA Portal (Seite 71)

Installationsprotokoll

7

Funktion des Installationsprotokolls

Während folgender Installationsprozesse werden die Fortschritte in einer Datei protokolliert:

- Produkte installieren
- Bereits installierte Produkte modifizieren oder hochrüsten
- Eine bereits vorhandene Installation reparieren
- Produkte deinstallieren

Wenn während des Installationsprozesses Fehler auftreten oder Warnungen ausgegeben werden, können diese mithilfe der Protokolldatei ausgewertet werden. Dies können Sie entweder selbst tun oder Sie wenden sich an den Produkt-Support.

Ablageort der Installationsprotokolle

Die Protokolldatei ist die neueste Datei mit der Dateinamenerweiterung ".log", deren Name mit "SIA" beginnt. Der Ablageort der Protokolldatei ist abhängig vom Betriebssystem, z. B. "C:\Programdata\Siemens\Automation\Logfiles\Setup" in Windows. Diesen Pfad können Sie in die Adressleiste des Windows Explorers einfügen.

Nach einer gewissen Zeit ab Start der Installation wird der Ablageort der Protokolldatei in der Umgebungsvariablen "%autinstlog%" gespeichert. Diese Umgebungsvariable können Sie ebenfalls in die Adressleiste des Windows Explorers eingeben, um den Ordner mit den Protokolldateien zu öffnen. Alternativ können Sie mit "CD %autinstlog%" über die Kommandozeile zum entsprechenden Verzeichnis navigieren.

Setup_Report (CAB-Datei)

Damit Sie alle notwendigen Dateien an den Produkt-Support liefern können, wird zusätzlich eine Archiv-Datei im CAB-Format abgelegt, die das Installationsprotokoll und alle anderen benötigten Dateien enthält. Dieses Archiv finden Sie unter "%autinstlog% \Reports\Setup_report.cab". Übermitteln Sie diese CAB-Datei dem Produkt-Support, wenn Sie Unterstützung bei der Installation benötigen. Damit kann der Produkt-Support schnell feststellen, ob die Installation einwandfrei durchgelaufen ist. CAB-Dateien, die bei früheren Installationsprozessen erzeugt wurden, werden mit einer Datumskennung im Verzeichnis "Reports" gespeichert.

Siehe auch

Hinweise zu Lizenzen (Seite 11)

Installation ausführen (Seite 89)

Verfügbarkeit von Updates und Support Packages prüfen und installieren (Seite 105)

Installierte Software anzeigen (Seite 95)

Installierte Produkte modifizieren oder hochrüsten (Seite 97)

Installierte Produkte reparieren (Seite 101)

Deinstallation starten (Seite 103)

8 Integrität prüfen

8.1 Grundlagen zur Integritätsprüfung

Einführung

Die Prüfung der Integrität und Authentizität der Installationsquelle und der installierten Produkte ist wichtig, um sicherzustellen, dass keine modifizierten Dateien vorhanden sind. Siemens liefert dazu die folgenden beiden Validatoren als Kommandozeilentools mit:

- Integrity Validator
  Der Integrity Validator dient dazu, die Setup-Dateien einer Installationsquelle, d. h. einem Installationsmedium oder heruntergeladenen Software-Paketen, auf Modifikationen zu prüfen. Dieser Validator wird zu Beginn einer Installation automatisch ausgeführt. Der Integrity Validator wird nicht auf Ihrem System installiert. Sie finden ihn in der Installationsquelle im Verzeichnis "IntegrityValidator". Von dort können Sie ihn ausführen, um eine Integritätsprüfung manuell durchzuführen. Über die Konfigurationsdatei "appsettings.json" haben Sie die Möglichkeit, den Pfad zu den Setup-Dateien anzugeben.
- Installation Integrity Validator
  Der Installation Integrity Validator wird zusammen mit jedem Produkt-Bundle von Siemens installiert, das die Software-Integritätsprüfung unterstützt. Im Gegensatz zum Integrity Validator wird der Installation Integrity Validator nicht automatisch ausgeführt. Sie können ihn jederzeit selbst ausführen, um Ihr System auf Integrität zu prüfen. Wenn Ihr System mit dem Internet verbunden ist, ist es empfehlenswert, diese Prüfung in einem gewissen Zeitintervall zu wiederholen.

Beide Validatoren erstellen bei der Validierung einen Validierungsbericht, in dem Sie sehen können, ob die Integritätsprüfung erfolgreich war oder fehlgeschlagen ist. Bei einer fehlgeschlagenen Integritätsprüfung können Sie dem Bericht die möglichen Gründe entnehmen.

Weitere Informationen zu dem Thema Cyber-Sicherheit finden Sie online im TIA Dokumentationsportal in folgendem Dokument:

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

8.2 Integritätsprüfung durchführen

Mit den beiden Validatoren "Integrity Validator" und "Installation Integrity Validator" können Sie die Integrität der Setup-Dateien vor der Installation und Ihres Systems zu einem beliebigen Zeitpunkt nach der Installation prüfen. Bevor Sie Ihr System mit dem Installation Integrity Validator prüfen, sollten Sie zunächst sicherstellen, dass er korrekt installiert wurde. Beim Integrity Validator haben Sie die Möglichkeit, den Pfad zu den Setup-Dateien anzupassen. Dies ist nur notwendig, wenn Sie den Integrity Validator außerhalb der Installationsquelle ablegen möchten.

Beide Validatoren verfügen über eine eigene Hilfe, die Sie in der Kommandozeile mit "-h" oder "--help" aufrufen können. Darin werden zum Beispiel mögliche Kommandos und die Exit-Codes beschrieben.

Pfad zu den Setup-Dateien für den Integrity Validator ändern

Um den Pfad zu den Setup-Dateien zu ändern, gehen Sie folgendermaßen vor:

1. Öffnen Sie den Windows-Explorer und navigieren Sie zu dem Verzeichnis "IntegrityValidator".
2. Öffnen Sie die Datei "appsettings.json" in einem Texteditor.
3. Geben Sie bei "InputDirectory" für "Path" den gewünschten Pfad ein.
4. Speichern Sie die Datei.
   Der Integrity Validator wird beim Validieren nun die Setup-Dateien prüfen, die er unter dem angegebenen Pfad findet.

Setup-Dateien mit dem Integrity Validator prüfen

Um die Setup-Dateien mit dem Integrity Validator zu prüfen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Eingabeaufforderung von Windows.
2. Navigieren Sie zu dem Verzeichnis "IntegrityValidator". Standardmäßig ist dieses Verzeichnis in der Installationsquelle. Falls Sie es woanders abgelegt haben, navigieren Sie dorthin.
3. Um die Setup-Dateien zu prüfen, geben Sie den folgenden Befehl ein:
   `IntegrityValidator.exe validate`
   Die Validierung wird durchgeführt und das Ergebnis wird zusammen mit den Exit-Codes angezeigt.

Installation des Installation Integrity Validator prüfen

Um sicherzustellen, dass der Installation Integrity Validator korrekt auf Ihrem System installiert wurde, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Eingabeaufforderung von Windows.
2. Geben Sie den folgenden Befehl ein:
   `cd %COMMONPROGRAMFILES%\Siemens\Automation\Installation Integrity Validator\InstallationIntegrityValidator.exe --version`
3. Bestätigen Sie die Eingabe mit <Return>.
   Wenn der Installation Integrity Validator korrekt installiert ist, wird Ihnen die installierte Version des Tools angezeigt.

Integrität des Systems mit dem Installation Integrity Validator prüfen

Um die Integrität Ihres Systems mit dem Installation Integrity Validator zu prüfen, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Eingabeaufforderung von Windows.
2. Um die Validierung zu starten, geben Sie den folgenden Befehl ein:
   `cd %COMMONPROGRAMFILES%\Siemens\Automation\Installation Integrity Validator\InstallationIntegrityValidator.exe validate <ggf. weitere Optionen>`
3. Bestätigen Sie die Eingabe mit <Return>.
   Die Validierung wird durchgeführt und das Ergebnis wird zusammen mit den Exit-Codes angezeigt.
   Siehe auch: Fehlerfälle bei der Integritätsprüfung (Seite 87)

8.3 Fehlerfälle bei der Integritätsprüfung

Nach der Ausführung der Integritätsprüfung mit dem Integrity Validator oder dem Installation Integrity Validators wird das Ergebnis der Validierung angezeigt. Dabei haben die Farben der Texte die folgenden Bedeutungen:

- Grün: Zeigt eine erfolgreiche Validierung an.
- Hellblau: Zeigt Informationen an.
- Rot: Zeigt Validierungsfehler sowie weitere Fehlermeldungen an.
- Gelb: Zeigt Warnungen an.

Mögliche Fehlerfälle mit Lösungsvorschlägen

Die folgende Tabelle zeigt die möglichen Fehlerfälle mit Lösungsvorschlägen:

Fehlerfall	Vorgeschlagene Lösung
Dateien fehlen	Installieren Sie das Setup-Bundle neu, das diese Dateien bereitgestellt hat.
Zusätzliche Dateien vorhanden	Löschen Sie die zusätzlichen Dateien.
Modifizierte Dateien vorhanden	Löschen Sie die modifizierten Dateien und installieren Sie das Setup-Bundle neu, das diese Dateien bereitgestellt hat.
Die Katalogdateien für ein Verzeichnis wurden nicht gefunden.	Installieren Sie das Setup-Bundle neu, das diese Dateien bereitgestellt hat.
Das Installationsverzeichnis für ein Produkt wurde nicht gefunden.	Kontaktieren Sie den Siemens-Helpdesk und stellen Sie die Installationsprotokolle zur Verfügung.
Die Installationsverzeichnis-Informationen für ein Produkt konnten nicht abgerufen werden.	Kontaktieren Sie den Siemens-Helpdesk und stellen Sie die Installationsprotokolle zur Verfügung.

Fehlerfall	Vorgeschlagene Lösung
Die Selbstüberprüfung/Integritätsprüfung für das CLI selbst ist für den Installation Integrity Validator fehlgeschlagen. Das bedeutet, dass die EXE-Datei oder die abhängige Assembly manipuliert wurde oder fehlt.	Installieren Sie das Setup-Bundle neu, um eine korrekte Version des Installation Integrity Validator zu erhalten.
Falsche Verwendung des Befehls "validate". Es wurden mehrere Verbositätsmodi angegeben.	Es kann nur ein Verbositätsmodus zusammen mit dem Befehl "validate" angegeben werden ("-v" oder "-d"). Mehrere Verbositätsmodi sind nicht erlaubt.

Installation ausführen

9

Einführung

Die Installation der Softwarepakete wird durch ein Setup-Programm ausgeführt, das Sie durch die Installation führt.

Hinweis

Integritätsprüfung

Während des Installationsprozesses findet nach der initialen Validierung keine zusätzliche Integritätsprüfung statt.
Dies stellt ein Sicherheitsrisiko in potenziell kompromittierten Umgebungen dar. Solche Bedingungen können zu unbefugten Änderungen am Installationsprozess führen.
Als Sicherheitsmaßnahme nach der Installation wird dringend empfohlen, die Validierung aller installierten Komponenten durchzuführen (Seite 85), um deren Integrität und Authentizität sicherzustellen. Darüber hinaus sollten die in dem Dokument "Cybersecurity for Industry - Operational Guidelines" enthaltenen Sicherheitsmaßnahmen befolgt werden. Das Dokument finden Sie auf der Website "Siemens ProductCERT and Siemens CERT (https://www.siemens.com/cert)".

Voraussetzungen

- Die zu installierenden Softwarepakte sind entweder auf einem Installationsmedium oder als Download verfügbar.
- Hardware und Software des PG/PC entsprechen den Systemanforderungen.
- Sie haben Administrationsrechte auf Ihrem Computer.
- Alle weiteren Anwendungen sind geschlossen.

Software-Integrität und Authentizität sicherstellen

Bevor Sie die Installation starten, sollten Sie sicherstellen, dass Ihre Installationsquelle integer ist und auch wirklich von Siemens bereitgestellt wurde. Dazu können Sie eine Integrationsprüfung Ihrer Installationsquelle durchführen. Weitere Informationen finden Sie im Kapitel "Integritätsprüfung durchführen (Seite 85)".

Weitere Informationen, wie Sie die Software-Integrität und Authentizität sicherstellen können, finden Sie im Dokument "Cybersecurity im TIA Portal" im Kapitel "Sichere Installation (https://docs.tia.siemens.cloud/access?ft:clusterId=cybersec_000011&;ft:locale=de-DE)".

Installation starten

Um die Installation der Softwarepakete zu starten, gehen Sie folgendermaßen vor:

1. Navigieren Sie zu der Datei "Start.exe" in der Installationsquelle und doppelklicken Sie darauf. Der Windows-Dialog zur Benutzerkontensteuerung wird angezeigt.
2. Wenn Sie sicherstellen möchten, dass das Software-Paket wirklich von Siemens stammt, klicken Sie auf "Weitere Details zeigen". Fahren Sie ansonsten mit Schritt X fort.
3. Um das Zertifkat des Software-Pakets anzuzeigen, klicken Sie auf "Informationen zum Herausgeberzertifikat anzeigen".
4. Öffnen Sie im Dialog "Siemens AG" das Register "Details" und scrollen Sie zum Feld "Fingerabdruck".
5. Vergleichen Sie den Fingerabdruck-Wert mit dem Wert, der auf der folgenden Internet-Seite für das Software-Paket angegeben ist:
   Gültige Zertifikate (https://docs.tia.siemens.cloud/access?ft:clusterId=cybersec_000010&;ft:locale=de-DE)
6. Nachdem Sie den Fingerabdruck-Wert verglichen haben, schließen Sie den Dialog "Siemens AG".
7. Um mit der Installation fortzufahren, bestätigen Sie die Benutzerkontensteuerung mit "Ja". Der Startbildschirm wird angezeigt und die Voraussetzungen werden überprüft. Diese Überprüfung kann einige Zeit in Anspruch nehmen. Wenn die Überprüfung erfolgreich ist, wird der Dialog zur Auswahl der Installationssprache geöffnet.

Installationssprache auswählen

Sie können die Installation in Ihrer bevorzugten Sprache durchführen. Falls Sie zuvor weitere Language Packs installert haben, können Sie auch diese Sprachen als Installationssprache auswählen.

Um die Installationssprache auszuwählen, gehen Sie folgendermaßen vor:

1. Wählen Sie die Sprache, in der Sie die Dialoge des Setup-Programms angezeigt bekommen möchten.
2. Um die Installationshinweise zu lesen, klicken Sie auf die Schaltfläche "Installationshinweise lesen".
   Die entsprechende Hilfedatei mit den Hinweisen wird geöffnet.
3. Wenn Sie die Hinweise gelesen haben, schließen Sie die Hilfedatei und klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog zur Auswahl der Produktsprachen wird geöffnet.

Produktsprachen auswählen

Die Produktoberfläche des TIA Portals ist in verschiedenen Sprachen verfügbar. Die Produktsprache "Englisch" wird als Basissprache immer installiert und kann nicht deaktiviert werden. Zusätzliche Sprachen sind über Language Packs verfügbar.

Um die Sprachen für die Produktoberfläche auszuwählen, gehen Sie folgendermaßen vor:

1. Wählen Sie die Sprachen für die Produktoberfläche und klicken Sie auf die Schaltfläche "Weiter".
   Möglicherweise wird ein Dialog mit zusätzlichen Informationen zu den Produkten geöffnet.
2. Lesen Sie in diesem Fall die Informationen und klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog zur Auswahl der Produktkonfiguration wird geöffnet.

Produktkonfiguration wählen

Sie können zwischen zwei vordefinierten Konfigurationen wählen oder selbst auswählen, welche Produkte installiert werden sollen. Zusätzlich können Sie eine Desktop-Verknüpfung anlegen lassen und das Zielverzeichnis wählen.

Um die Produktkonfiguration auszuwählen, gehen Sie folgendermaßen vor:

1. Wählen Sie die Produkte, die Sie installieren möchten:
   - Wenn Sie das Programm mit einer minimalen Programmzusammenstellung installieren möchten, klicken Sie auf die Schaltfläche "Minimal". Sie können auch hier weitere Produkte auswählen, die Ansicht wechselt dann automatisch zu "Benutzerdefiniert". Die Produktkonfiguration "Minimal" wird dadurch nicht verändert.
   - Wenn Sie das Programm mit produkttypischen Programmzusammenstellungen installieren möchten, klicken Sie auf die Schaltfläche "Typisch". Sie können auch hier weitere Produkte auswählen, die Ansicht wechselt dann automatisch zu "Benutzerdefiniert". Die Produktkonfiguration "Typisch" wird dadurch nicht verändert.
   - Wenn Sie selbst auswählen möchten, welche Produkte installiert werden sollen, klicken Sie auf die Schaltfläche "Benutzerdefiniert". Aktivieren Sie anschließend die Optionskästchen für die Produkte, die Sie installieren möchten.
2. Wenn eine Verknüpfung auf dem Desktop angelegt werden soll, aktivieren Sie das Optionskästchen "Desktop-Verknüpfung anlegen".
3. Klicken Sie auf die Schaltfläche "Durchsuchen", wenn Sie das Zielverzeichnis für die Installation ändern möchten.

   Hinweis

   Beachten Sie die folgenden Hinweise:

   - Die Länge des Installationspfades darf 89 Zeichen nicht überschreiten.
   - Sie können den Installationspfad nur ändern, wenn noch kein Produkt des Software-Pakets installiert ist, das Sie installieren möchten.
   - Um die Sicherheit zu erhöhen, wählen Sie als Zielverzeichnis ein Verzeichnis, das durch Administratorrechte geschützt ist.

4. Klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog zu den Lizenzbedingungen wird geöffnet.

Lizenzbedingungen lesen und akzeptieren

Um die Installation fortsetzen zu können, müssen Sie die Lizenzbedingungen von Siemens akzeptieren und bestätigen, dass Sie die Securityhinweise gelesen haben. Die Securityhinweise finden Sie in den Readme-Dateien der Produkte.

1. Lesen Sie die Lizenzbedingungen gründlich durch.
2. Wenn Sie einverstanden sind, aktivieren Sie die beiden Optionskästchen zu den Lizenzbedingungen und den Securyhinweisen. Wenn Sie nicht einverstanden sind, können Sie die Installation nicht fortsetzen.
3. Wenn Sie die beiden Optionskästchen aktiviert haben, klicken Sie auf "Weiter".
   Der Dialog "TIA Help Viewer" wird geöffnet.

Port für den TIA Help Viewer angeben

Das neue browser-basierte Informationssystem des TIA Portals wird in Ihrem Standard-Browser angezeigt. Dazu wird ein freier Port benötigt. Die Standardportnummer ist "5112". Diese Portnummer wird geprüft und das Ergebnis dieser Prüfung wird Ihnen angezeigt.

1. Wenn der Port "5112" gültig ist, können Sie diesen mit einem Klick auf die Schaltfläche "Bestätigen" bestätigen.
   Optional können Sie auch einen anderen freien Port angeben und diesen bestätigen. Durch den Klick auf "Bestätigen" wird geprüft, ob diese Portnummer bereits verwendet wird. Wenn dies der Fall ist, geben Sie eine andere Portnummer ein und klicken erneut auf "Bestätigen". Der angegebene Port wird für den Aufruf des Informationssystems in Ihrem Standard-Browser verwendet.
2. Wenn Sie eine gültige Portnummer eingegeben haben, klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog "TIA Software Update Server-Konfiguration" wird geöffnet.

TIA Software Update-Server konfigurieren

Sie können die Software Updates des TIA Portals entweder über den TIA Automation Software Update Server von Siemens bekommen oder über einen unternehmenseigenen Server.

1. Wählen Sie den Update-Server aus, den Sie verwenden möchten:
   - Beim Update Server von Siemens ist keine weitere Konfiguration notwendig.
   - Wenn Sie einen unternehmenseigenen Server verwenden möchten, müssen Sie den Server-Pfad und die Fertigungslinie angeben.
     Weitere Informationen zum Arbeiten mit einem unternehmenseigenem Server finden Sie im Kapitel "Arbeiten mit einem unternehmenseigenen Server (Seite 108)".
   - Wenn Sie diese Angaben bereits zuvor gemacht haben, können Sie die Option "Aktuelle Einstellungen verwenden" aktivieren. Wenn Sie sich nicht mehr sicher sind, was Ihre aktuellen Einstellungen sind, können Sie diese im TIA Administrator prüfen.
2. Klicken Sie auf "Weiter".
   Für den Fall, dass für die Installation des TIA Portals Sicherheits- und Rechteeinstellungen geändert werden müssen, wird der Dialog zu den Sicherheitseinstellungen geöffnet.

Sicherheitseinstellungen akzeptieren

Um die Installation fortsetzen zu können, müssen Sie die die Änderungen an den Sicherheits- und Rechteeinstellungen akzeptieren.

1. Lesen Sie die Änderungen an den Sicherheits- und Rechteeinstellungen gründlich durch. Optional können Sie den Bericht über "Bericht speichern" speichern oder über "Bericht drucken" ausdrucken.
2. Wenn Sie einverstanden sind, aktivieren Sie das Optionskästchen zu den Sicherheits- und Rechteeinstellungen. Wenn Sie nicht einverstanden sind, können Sie die Installation nicht fortsetzen.
3. Klicken Sie auf die Schaltfläche "Weiter".
   Im nächsten Dialog wird eine Übersicht der Installationseinstellungen angezeigt.

Übersicht über die Installationseinstellungen und Installation starten

Sie erhalten eine Übersicht über alle gewählten Installationseinstellungen. Diese können Sie vor dem Start der Installation prüfen und ggf. ändern.

1. Überprüfen Sie die gewählten Installationseinstellungen.
2. Wenn Sie Änderungen vornehmen möchten, klicken Sie auf die Schaltfläche "Zurück", bis Sie die zu ändernde Stelle im Dialog erreicht haben. Wenn Sie die gewünschten Änderungen vorgenommen haben, kehren Sie mit "Weiter" wieder zur Übersicht zurück.
3. Um die Installation zu starten, klicken Sie auf die Schaltfläche "Installieren".
   Die Installation wird gestartet.

   Hinweis

   Wenn während der Installation kein License Key gefunden wird, erhalten Sie die Möglichkeit, diesen auf Ihren PC zu übertragen. Wenn Sie den Lizenztransfer überspringen, können Sie dies später mit dem Automation License Manager nachholen.

   Nach der Installation erhalten Sie eine Meldung darüber, ob die Installation erfolgreich durchgeführt wurde.

4. Möglicherweise muss der Computer neu gestartet werden. Aktivieren Sie dann das Optionsfeld "Ja, Computer jetzt neu starten".
   Klicken Sie anschließend auf die Schaltfläche "Neu starten".
5. Wenn der Computer nicht neu gestartet werden muss, klicken Sie auf die Schaltfläche "Beenden".

Ergebnis

Auf Ihrem Computer wurde das TIA Portal zusammen mit den erworbenen Produkten und Lizenzen und der Automation License Manager installiert.

Siehe auch

Installationsprotokoll (Seite 83)

Grundlagen zur Integritätsprüfung (Seite 85)

Hinweise zu den Systemvoraussetzungen (Seite 47)
Hinweise zu Lizenzen (Seite 11)
Installierte Software anzeigen (Seite 95)
Installierte Produkte modifizieren oder hochrüsten (Seite 97)
Installierte Produkte reparieren (Seite 101)
Deinstallation starten (Seite 103)

Installierte Software anzeigen

10

Sie können sich jederzeit darüber informieren, welche Software installiert ist. Zusätzlich können Sie sich weitere Informationen zur installierten Software anzeigen lassen.

Vorgehen

Um eine Übersicht über die installierte Software aufzurufen, gehen Sie folgendermaßen vor:

1. Klicken Sie im Menü "Hilfe" auf "Installierte Software".
   Der Dialog "Installierte Software" wird geöffnet. Innerhalb des Dialogs sehen Sie die installierten Software-Produkte. Klappen Sie die Einträge auf, um die jeweils installierte Version zu sehen.
2. Wenn Sie sich weitere Informationen zu der installierten Automatisierungssoftware anzeigen lassen möchten, klicken Sie auf den Link innerhalb des Dialogs "Weitere Informationen zu installierter Software".
   Der Dialog "Detailinformation" wird geöffnet.
3. Wählen Sie in der Bereichsnavigation das Thema, zu dem Sie sich weitere Informationen ansehen möchten.

Siehe auch

Hinweise zu den Systemvoraussetzungen (Seite 47)

Hinweise zu Lizenzen (Seite 11)

Installation ausführen (Seite 89)

Installierte Produkte modifizieren oder hochrüsten (Seite 97)

Installierte Produkte reparieren (Seite 101)

Deinstallation starten (Seite 103)

Installationsprotokoll (Seite 83)

Installierte Produkte modifizieren oder hochrüsten 11

Sie haben die Möglichkeit, installierte Produkte über das Setup-Programm zu ändern oder auf eine neue Version hochzurüsten (Update).

Bausteine mit Know-how-Schutz aus früheren Versionen des TIA Portals werden nicht automatisch mit dem Projekt hochgerüstet. Entfernen Sie den Know-how-Schutz der Bausteine, bevor Sie das TIA Portal aktualisieren. Richten Sie den Know-how-Schutz anschließend mit der aktuellen Version des TIA Portals wieder ein. Weitere Informationen finden Sie im Informationssystem.

Voraussetzung

- Die zu installierenden Softwarepakte sind entweder auf einem Installationsmedium oder als Download verfügbar.
- Hardware und Software des PG/PC entsprechen den Systemanforderungen.
- Sie haben Administrationsrechte auf Ihrem Computer.
- Alle laufenden Programme sind beendet.
- Optional: Sie haben die Integrität und Authentizität der Installationsquelle geprüft.
  Siehe auch: Installation ausführen (Seite 89)

Vorgehen

Um installierte Produkte zu ändern oder hochzurüsten, gehen Sie folgendermaßen vor:

1. Navigieren Sie zu der Datei "Start.exe" in der Installationsquelle und doppelklicken Sie darauf.
   Der Dialog zur Auswahl der Setup-Sprache wird geöffnet.
2. Wählen Sie die Sprache, in der Sie die Dialoge des Setup-Programms angezeigt bekommen möchten. Falls Sie zuvor weitere Language Packs installert haben, können Sie auch diese Sprachen als Installationssprache auswählen.
3. Um die Installationshinweise zu lesen, klicken Sie auf die Schaltfläche "Installationshinweise lesen".
   Die Installationsanleitung wird geöffnet.
4. Wenn Sie die Hinweise gelesen haben, schließen Sie die Hilfedatei und klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog zur Auswahl der Installationsvariante wird geöffnet.
5. Aktivieren Sie das Optionsfeld "Modifizieren/Hochrüsten" und klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog zur Auswahl der Produktsprachen wird geöffnet.

6. Aktivieren Sie die Optionskästchen der Produktsprachen, die Sie installieren möchten. Bereits installierte Produktsprachen können Sie durch Deaktivieren der entsprechenden Optionskästchen deinstallieren.

   Hinweis

   Beachten Sie, dass Sie die Produktsprache "Englisch" nicht deinstallieren können.

7. Klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog zur Auswahl der Produktkonfiguration wird geöffnet.
8. Aktivieren Sie die Optionskästchen der Bestandteile, die Sie installieren möchten. Bereits installierte Bestandteile können Sie durch Deaktivieren der entsprechenden Optionskästchen deinstallieren.
9. Klicken Sie auf die Schaltfläche "Weiter".

   Hinweis

   Beachten Sie, dass Sie das Zielverzeichnis nicht ändern können, da die vorhandene Installation verändert wird.

   Für den Fall, dass für die Installation des TIA Portals Sicherheits- und Rechteeinstellungen geändert werden müssen, wird der Dialog zu den Sicherheitseinstellungen geöffnet.
10. Um die Installation fortzusetzen, akzeptieren Sie die Änderungen der Sicherheits- und Rechteeinstellungen und klicken Sie auf die Schaltfläche "Weiter".
    Im nächsten Dialog wird eine Übersicht der Installationseinstellungen angezeigt.
11. Klicken Sie auf die Schaltfläche "Modifizieren".
    Die Installation der zusätzlichen Bestandteile wird gestartet.

    Hinweis

    Nach der Installation erhalten Sie eine Meldung darüber, ob die bestehende Installation erfolgreich geändert wurde.

12. Möglicherweise muss der Computer neu gestartet werden. Aktivieren Sie dann das Optionsfeld "Ja, Computer jetzt neu starten". Klicken Sie anschließend auf die Schaltfläche "Neu starten".
13. Wenn der Computer nicht neu gestartet werden muss, klicken Sie auf die Schaltfläche "Beenden".

Ergebnis

Auf Ihrem Computer wurde die bestehende Installation geändert.

Siehe auch

Hinweise zu den Systemvoraussetzungen (Seite 47)

Hinweise zu Lizenzen (Seite 11)

Installierte Software anzeigen (Seite 95)

Installierte Produkte reparieren (Seite 101)

Deinstallation starten (Seite 103)
Installationsprotokoll (Seite 83)

Installierte Produkte reparieren

12

Sie haben die Möglichkeit, installierte Produkte mithilfe des Setup-Programms durch eine vollständige Reinstallation zu reparieren.

Voraussetzung

- Die zu installierenden Softwarepakte sind entweder auf einem Installationsmedium oder als Download verfügbar.
- Hardware und Software des PG/PC entsprechen den Systemanforderungen.
- Sie haben Administrationsrechte auf Ihrem Computer.
- Alle laufenden Programme sind beendet.
- Optional: Sie haben die Integrität und Authentizität der Installationsquelle geprüft.
  Siehe auch: Installation ausführen (Seite 89)

Vorgehen

Um installierte Produkte zu reparieren, gehen Sie folgendermaßen vor:

1. Navigieren Sie zu der Datei "Start.exe" in der Installationsquelle und doppelklicken Sie darauf.
   Der Dialog zur Auswahl der Setup-Sprache wird geöffnet.
2. Wählen Sie die Sprache, in der Sie die Dialoge des Setup-Programms angezeigt bekommen möchten
3. Um die Installationshinweise zu lesen, klicken Sie auf die Schaltfläche "Installationshinweise lesen".
   Die Installationsanleitung wird geöffnet.
4. Wenn Sie die Hinweise gelesen haben, schließen Sie die Hilfedatei und klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog zur Auswahl der Installationsvariante wird geöffnet.
5. Aktivieren Sie das Optionsfeld "Reparieren" und klicken Sie auf die Schaltfläche "Weiter".
   Im nächsten Dialog wird eine Übersicht der Installationseinstellungen angezeigt.
6. Klicken Sie auf die Schaltfläche "Reparieren".
   Das Reparieren der bestehenden Installation wird gestartet.

   Hinweis

   Nach der Installation erhalten Sie eine Meldung darüber, ob die installierten Produkte erfolgreich repariert wurden.

7. Möglicherweise muss der Computer neu gestartet werden. Aktivieren Sie dann das Optionsfeld "Ja, Computer jetzt neu starten". Klicken Sie anschließend auf die Schaltfläche "Neu starten".
8. Wenn der Computer nicht neu gestartet werden muss, klicken Sie auf die Schaltfläche "Beenden".

Ergebnis

Die installierten Produkte wurden erneut installiert.

Siehe auch

Hinweise zu den Systemvoraussetzungen (Seite 47)

Hinweise zu Lizenzen (Seite 11)

Installierte Software anzeigen (Seite 95)

Installierte Produkte modifizieren oder hochrüsten (Seite 97)

Deinstallation starten (Seite 103)

Installationsprotokoll (Seite 83)

Deinstallation starten

13

Einführung

Die Deinstallation der Softwarepakete erfolgt durch ein Setup-Programm, welches Sie Schritt für Schritt durch den gesamten Vorgang der Deinstallation führt.

Sie haben zwei Möglichkeiten für die Deinstallation:

- Deinstallation von ausgewählten Komponenten über die Systemsteuerung
- Deinstallation eines Produkts mithilfe der Installationsquelle

Hinweis

Der Automation License Manager wird mit der Deinstallation der Softwarepakete nicht automatisch entfernt, da dieser für die Verwaltung der License Keys mehrerer Produkte der Siemens AG eingesetzt wird.

Deinstallation von ausgewählten Komponenten über die Systemsteuerung

Um ausgewählte Softwarepakete zu deinstallieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Systemsteuerung.
2. Klicken Sie unter "Programme" auf "Programm deinstallieren".
   Ein Dialog mit der Liste der installierten Programmen wird geöffnet.
3. Wählen Sie die zu deinstallierenden Softwarepakete und klicken Sie auf die Schaltfläche "Deinstallieren".
   Der Dialog zur Auswahl der Setup-Sprache wird geöffnet.
4. Wählen Sie die Sprache, in der Sie die Dialoge des Setup-Programms angezeigt bekommen möchten, und klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog zur Auswahl der Produkte, die Sie deinstallieren möchten, wird geöffnet.
5. Aktivieren Sie die Optionskästchen für die Produkte, die Sie deinstallieren möchten, und klicken Sie auf die Schaltfläche "Weiter".
   Im nächsten Dialog wird eine Übersicht der Installationseinstellungen angezeigt.
6. Überprüfen Sie die Liste mit den Produkten, die deinstalliert werden. Wenn Sie Änderungen vornehmen möchten, klicken Sie auf die Schaltfläche "Zurück".
7. Klicken Sie auf die Schaltfläche "Deinstallieren".
   Die Deinstallation wird gestartet.
8. Möglicherweise muss der Computer neu gestartet werden. Aktivieren Sie dann das Optionsfeld "Ja, Computer jetzt neu starten". Klicken Sie anschließend auf die Schaltfläche "Neu starten".
9. Wenn der Computer nicht neu gestartet werden muss, klicken Sie auf die Schaltfläche "Beenden".

Deinstallation eines Produkts mithilfe einer Installationsquelle

Prüfen Sie gegebenenfalls die Integrität und Authentizität der Installationsquelle. Siehe auch: Installation ausführen (Seite 89)

Um alle Softwarepakete zu deinstallieren, gehen Sie folgendermaßen vor:

1. Navigieren Sie zu der Datei "Start.exe" in der Installationsquelle und doppelklicken Sie darauf. Der Dialog zur Auswahl der Setup-Sprache wird geöffnet.
2. Wählen Sie die Sprache, in der Sie die Dialoge des Setup-Programms angezeigt bekommen möchten.
3. Um die Installationshinweise zu lesen, klicken Sie auf die Schaltfläche "Installationshinweise lesen".
   Die Installationsanleitung wird geöffnet.
4. Wenn Sie die Hinweise gelesen haben, schließen Sie die Hilfedatei und klicken Sie auf die Schaltfläche "Weiter".
   Der Dialog zur Auswahl der Installationsvariante wird geöffnet.
5. Aktivieren Sie das Optionsfeld "Deinstallieren" und klicken Sie auf die Schaltfläche "Weiter". Im nächsten Dialog wird eine Übersicht der Installationseinstellungen angezeigt.
6. Klicken Sie auf die Schaltfläche "Deinstallieren".
   Die Deinstallation wird gestartet.
7. Möglicherweise muss der Computer neu gestartet werden. Aktivieren Sie dann das Optionsfeld "Ja, Computer jetzt neu starten". Klicken Sie anschließend auf die Schaltfläche "Neu starten".
8. Wenn der Computer nicht neu gestartet werden muss, klicken Sie auf die Schaltfläche "Beenden".

Siehe auch

Installationsprotokoll (Seite 83)

Hinweise zu den Systemvoraussetzungen (Seite 47)

Hinweise zu Lizenzen (Seite 11)

Installierte Software anzeigen (Seite 95)

Installierte Produkte modifizieren oder hochrüsten (Seite 97)

Installierte Produkte reparieren (Seite 101)

Updates und Support Packages installieren 14

14.1 Verfügbarkeit von Updates und Support Packages prüfen und installieren

Per Voreinstellung prüft das TIA Portal automatisch, ob neue Software Updates oder Support Packages verfügbar sind, z. B. Hardware Support Packages (HSPs). Die automatische Suche nach Updates findet nach jedem Neustart des Rechners und danach zyklisch alle 24 Stunden statt. Sie können die automatische Suche jederzeit deaktivieren bzw. erneut aktivieren. Zusätzlich können Sie manuell nach Updates suchen.

Falls Updates gefunden werden, können Sie diese herunterladen und installieren.

Hinweis

Es werden Updates und Support Packages ab TIA Portal V13 unterstützt.

Automatische Suche nach Software Updates deaktivieren oder aktivieren

Um die automatische Suche nach Software Updates zu deaktivieren oder erneut zu aktivieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Menü "Extras" den Befehl "Einstellungen".
   Das Fenster "Einstellungen" wird im Arbeitsbereich angezeigt.
2. Wählen Sie in der Bereichsnavigation die Gruppe "Allgemein > Software Updates".
3. Deaktivieren Sie das Optionskästchen "Täglich nach Updates suchen", wenn Sie die automatische Suche nach Software Updates deaktivieren möchten.
4. Aktivieren Sie das Optionskästchen "Täglich nach Updates suchen", wenn Sie die automatische Suche nach Software Updates erneut aktivieren möchten.

Manuell nach Software Updates suchen

Wenn Sie manuell nach Software Updates suchen möchten, gehen Sie folgendermaßen vor:

1. Klicken Sie im Menü "Hilfe" auf "Installierte Software".
   Der Dialog "Installierte Software" wird geöffnet.
2. Klicken Sie auf "Nach Updates suchen".
   Der TIA Administrator wird geöffnet.
3. Klicken Sie auf die Kachel "Software verwalten".
   Die verfügbaren Updates werden angezeigt.

Oder:

1. Wählen Sie im Menü "Extras" den Befehl "Einstellungen".
   Das Fenster "Einstellungen" wird im Arbeitsbereich angezeigt.
2. Wählen Sie in der Bereichsnavigation die Gruppe "Allgemein > Software Updates".

3. Klicken Sie auf "Jetzt nach Updates suchen".
   Der TIA Administrator wird geöffnet.
4. Klicken Sie auf die Kachel "Software verwalten".
   Die verfügbaren Updates werden angezeigt.

Oder:

1. Öffnen Sie den TIA Administrator über "Start > Alle Programme > Siemens Automation > TIA Administrator".
2. Klicken Sie auf die Kachel "Software verwalten" und dort auf die Schaltfläche "Nach Updates suchen".
   Die verfügbaren Updates werden angezeigt.

Server einstellen

Abhängig davon, ob Sie die Updates bzw. Support Packages vom TIA Automation Update Server oder von einem unternehmenseigenen Server herunterladen möchten, müssen Sie den entsprechenden Server einstellen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie den TIA Administrator.
2. Klicken Sie auf "Einstellungen" und wählen Sie im aufgeblendeten Dialog im Bereich "Server auf dem nach Updates gesucht werden soll" die Option "TIA Automation Software Update Server".
   Die Software sucht auf dem Server des Herstellers nach verfügbaren Updates.

Oder:

1. Öffnen Sie den TIA Administrator.
2. Klicken Sie auf "Einstellungen" und wählen Sie im Register "Software-Verwaltung" die Option "Unternehmenseigener Server".
3. Geben Sie die Server-URL ein, die Sie von Ihrem Administrator bekommen haben. Die URL muss entweder im Format https://[URL des Servers]/[Pfad auf Ablageverzeichnis] oder im Format https://[IP-Adresse des Servers]/[Pfad auf Ablageverzeichnis] eingegeben werden. Sollten Sie sich nicht sicher sein, welches Format verwendet wird, wenden Sie sich an Ihren Administrator!
   Die Software sucht auf dem Server Ihres Unternehmens nach verfügbaren Updates.
4. Prüfen Sie den Namen der Fertigungsline und ändern Sie diesen bei Bedarf. Standardmäßig ist "ProductionLine1" eingestellt.
   Fertigungslinien dienen dazu, um verschiedenen Anwendern gezielt bestimmte Updates/ Support Packages bereitzustellen. Wenn Ihr Unternehmen nicht mit verschiedenen Fertigungslinien arbeitet, behalten Sie den vorgegebenen Eintrag bei.
   Ausführliche Informationen zum Erstellen von Projekten und Arbeiten mit Fertigungslinien entnehmen Sie der Hilfe zum TIA Updater Corporate Configuration Tool.

Sie können die Optionen, auf welchem Server nach Updates gesucht werden soll, jederzeit umstellen. Während eines Download-Vorgangs ist die Umstellung jedoch blockiert. Nach der Umstellung des Servers werden alle bereits heruntergeladenen Updates und Support Packages angezeigt, auch wenn sie auf dem aktuell eingestellten Server nicht verfügbar sind.

Updates/Support Packages installieren

Die genaue Vorgehensweise zum Installieren von Updates/Support Packages entnehmen Sie der Hilfe zum TIA Administrator.

Alternative Vorgehensweise für die Installation von Support Packages

Für die Installation eines Support Packages steht Ihnen eine zusätzliche Vorgehensweise zur Verfügung. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie im TIA Portal im Menü "Extras" auf "Support Packages".
   Der Dialog "Detailinformation" wird geöffnet. In einer Tabelle werden alle Support Packages aus dem Verzeichnis aufgelistet, das Sie als Speicherort für Support Packages in den Einstellungen festgelegt haben.
2. Falls Sie ein Support Package installieren möchten, das in der Liste nicht aufgeführt wird, haben Sie folgende Möglichkeiten:
   - Wenn sich das Support Package bereits auf Ihrem Computer befindet, können Sie es über "Aus dem Dateisystem hinzufügen" in die Liste aufnehmen.
   - Wenn Sie ein Support Package von der "Service & Support"-Seite im Internet hinzufügen möchten, laden Sie es zunächst mit "Aus dem Internet laden" herunter. Anschließend können Sie es aus dem Dateisystem hinzufügen.
3. Selektieren Sie das Support Package, das Sie installieren möchten.
4. Klicken Sie auf "Installieren".
5. Beenden Sie das TIA Portal und starten Sie es erneut.

Siehe auch

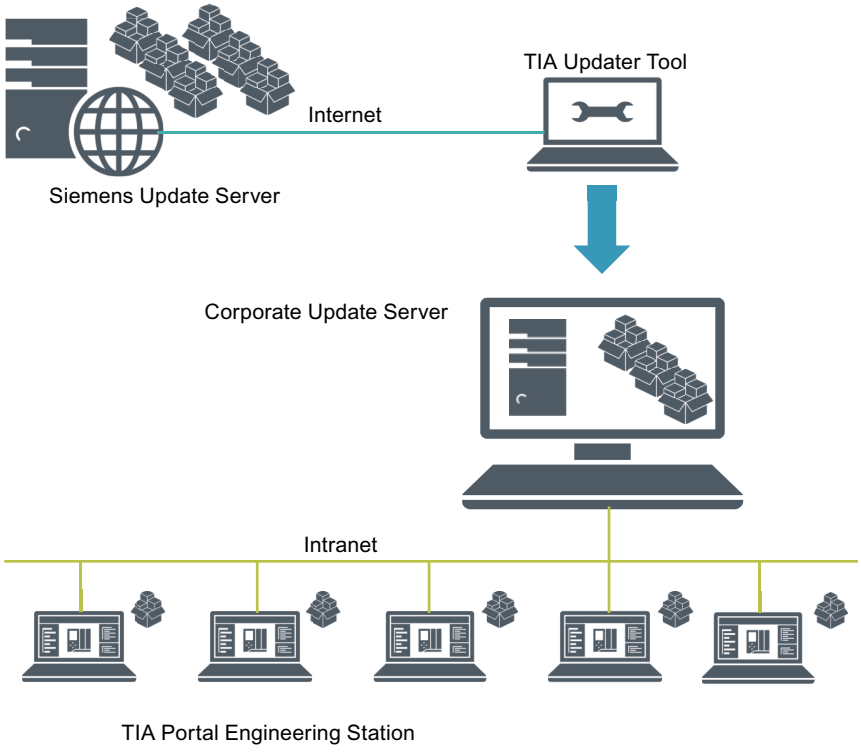
Installationsprotokoll (Seite 83)

14.2 Arbeiten mit einem unternehmenseigenen Server

14.2.1 Eigenschaften und Vorteile eines unternehmenseigenen Servers

Einleitung

Mithilfe eines unternehmenseigenen Servers können Sie ausgewählte Updates/Support Packages auf einem lokalen Server ablegen und den Anwendern zur Verfügung stellen, z. B. für unterschiedliche Fertigungslinien. Dies hat den Vorteil, dass die Anwender nicht auf das Internet zugreifen müssen, sondern die Updates über das Intranet, eine externe Festplatte etc. installieren können. Da die Anwender keinen direkten Zugriff ins Internet benötigen, wird der Schutz vor Trojanern oder schädlicher Software, die Kontakt aus dem internen Firmennetzwerk ins Internet aufnimmt, deutlich erhöht.



Konfigurieren des Servers und Erstellen von Projekten

In der ersten Phase wird der unternehmenseigene Server durch einen Server-Administrator konfiguriert, und mittels TIA Updater Corporate Configuration Tool werden die Updates/Support Packages bereitgestellt. Zusätzlich können Projekte für verschiedene Fertigungslinien erstellt werden, über die der Anwender die von ihm benötigten Updates erhalten kann. Die Anwender müssen Zugriff auf den Serverbereich und den Namen der Fertigungslinie haben und über das Ablageverzeichnis in Kenntnis gesetzt werden.

Ausführliche Informationen zum Erstellen von Projekten und Arbeiten mit Fertigungslinien entnehmen Sie der Hilfe zum TIA Updater Corporate Configuration Tool.

Arbeiten mit dem Server

Mit dem TIA Updater können die Anwender die bereitgestellten und für sie relevanten Updates/ Support Packages herunterladen und installieren. Es können gleichzeitig mehrere Download-Vorgänge angestoßen werden; die Installation der Updates/Support Packages muss jedoch hintereinander erfolgen.

14.2.2 Unternehmenseigenen Server für Updates konfigurieren

Einfühung

Um den Anwendern zentral die verfügbaren Updates, Support Packages und Sprachpakete zur Verfügung zu stellen, können Sie einen unternehmenseigenen Server konfigurieren. Verwenden Sie hierzu den Microsoft Server Manager.

Nachfolgend sind beispielhaft die Schritte beschrieben, die zum Erstellen und Konfigurieren des Servers zur Nutzung des TIA Updater Corporate Configuration Tools (mit dem Betriebssystem Microsoft Server 2016) notwendig sind. Weitere Einstellungen, die evtl. zum Betrieb in Ihrem Unternehmen notwendig sind, sind **nicht** Bestandteil dieser Beschreibung!

Hinweis

Bitte beachten Sie, dass der Aufbau des Startmenüs und der Ablageort der Programme unter den verschiedenen Betriebssystemen unterschiedlich sein kann.

Genaue Informationen zur Konfiguration und Bedienung des Server Managers finden Sie in der Microsoft-Hilfe.

Voraussetzung

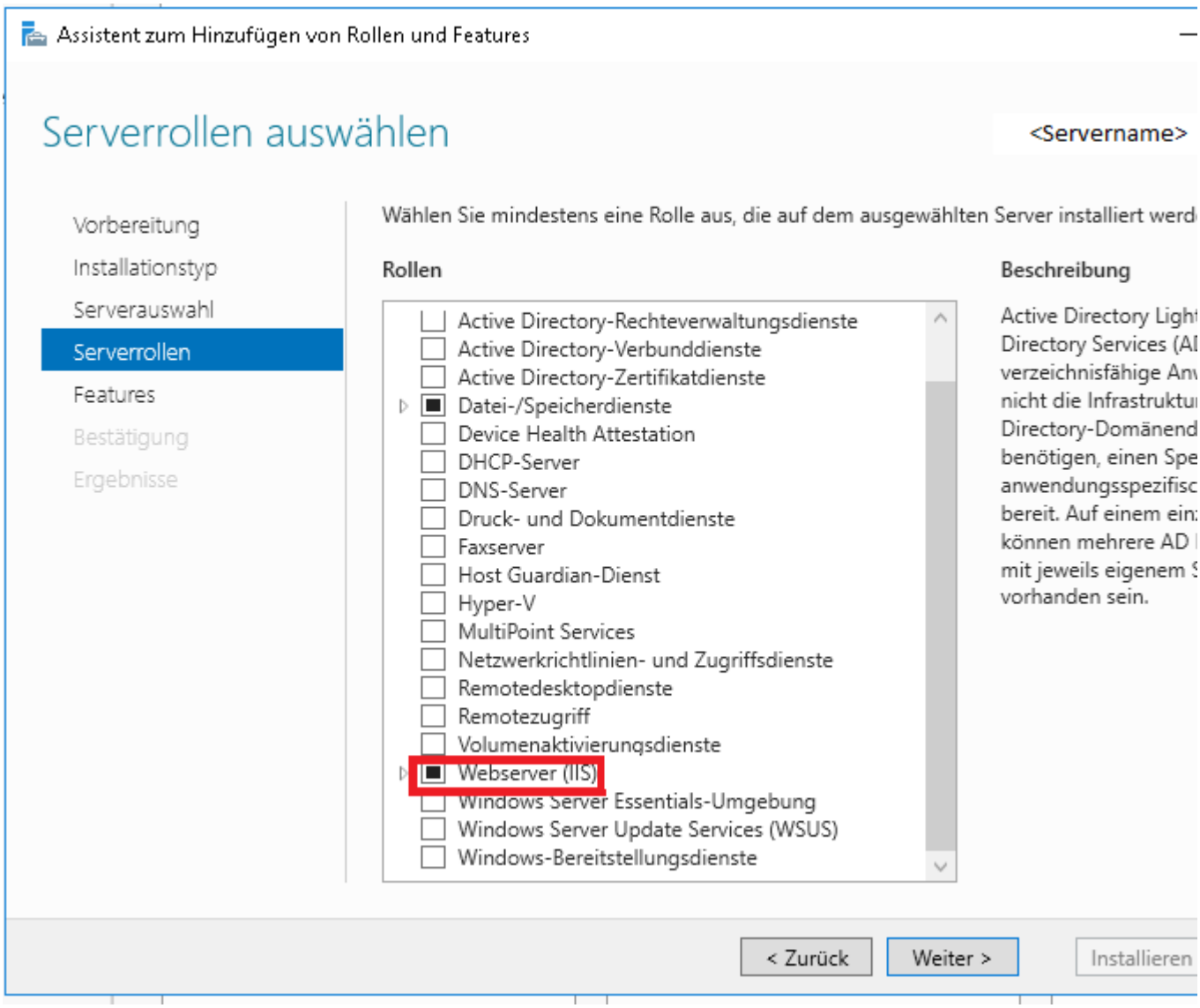
Sie müssen Administratorrechte besitzen.

Webserverrolle (IIS) installieren

Um die notwendige Webserverrolle zu installieren, gehen Sie folgendermaßen vor:

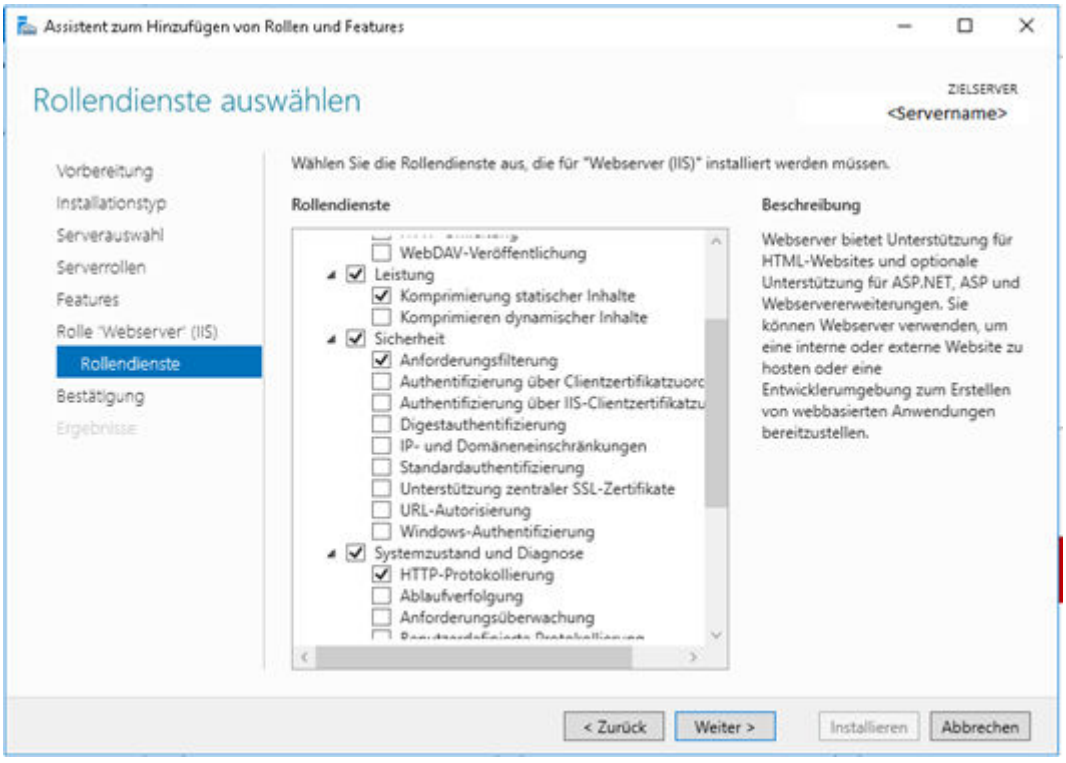
1. Öffnen Sie das Startmenü und wählen Sie "Server Manager" aus.
2. Klicken Sie im Dashboard auf "Rollen und Features hinzufügen".
3. Verwenden Sie den Assistenten "Rollen und Features hinzufügen", um die Webserverrolle hinzuzufügen.
   Vor dem Start des Assistenten wird verifiziert, dass der Administrator ein komplexes Passwort vergeben hat, dass die Netzwerkeinstellungen entsprechend konfiguriert sind und dass die neusten Windows Sicherheits-Updates installiert sind.
4. Wählen Sie als Installationstyp "Rollenbasierte oder featurebasierte Installation" und klicken Sie auf "Weiter".
5. Wählen Sie dann den Ziel-Server aus und klicken Sie auf "Weiter".

6. Beachten Sie die vorausgewählten Rollen, die standardmäßig installiert werden, und wählen Sie dann die zusätzliche Rolle "Webserver (IIS)" aus.



7. Klicken Sie auf "Features hinzufügen" und dann auf "Weiter". Die Features für den Web Server werden angezeigt.

8. Klicken Sie auf "Rollendienste" und prüfen Sie, dass die folgenden Features ausgewählt sind, bzw. wählen Sie diese aus:



Bereich "Webserver"

- Standarddokument
- Verzeichnis durchsuchen
- HTTP-Fehler
- Statischer Inhalt

Bereich "Systemzustand und Diagnose"

- HTTP-Protokollierung
- Anforderungsüberwachung

Bereich "Leistung"

- Komprimierung statischer Inhalte

Bereich "Sicherheit"

- Anforderungsfilterung

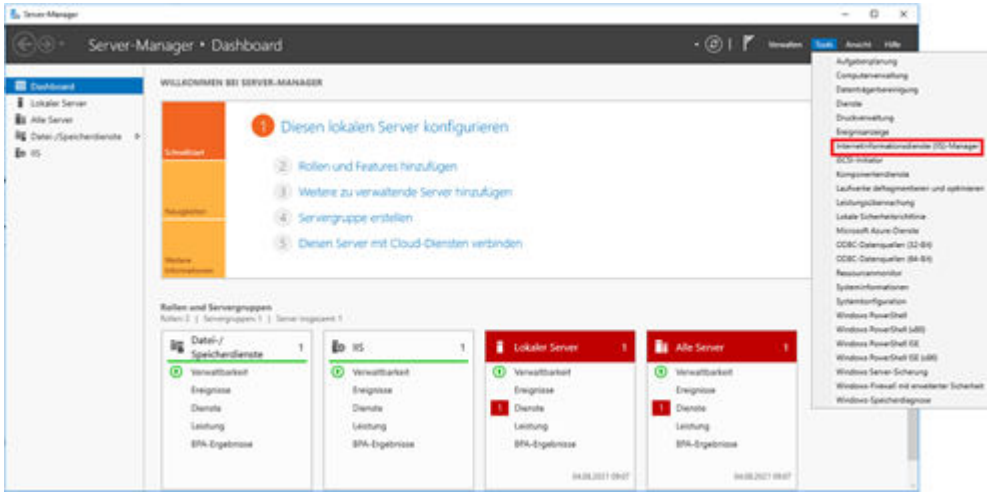
Bereich "Anwendungsentwicklung"

- .NET-Erweiterbarkeit 3.5
- .NET-Erweiterbarkeit 4.6
- ASP.NET 3.5
- ASP.NET 4.6

- ISAPI-Erweiterungen
- ISAPI-Filter

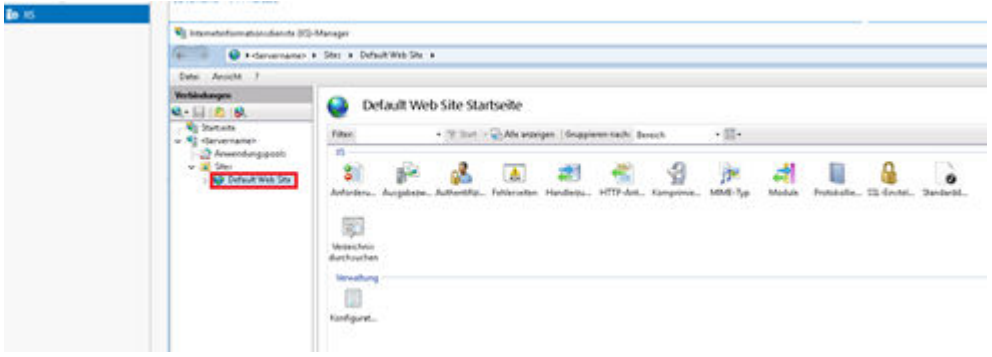
9. Klicken Sie auf "Weiter".
10. Überprüfen Sie Ihre Auswahl im Dialog "Installationsauswahl bestätigen" und klicken Sie auf "Installieren".

Im Dashboard wird "IIS" hinzugefügt und kann weiter konfiguriert werden.

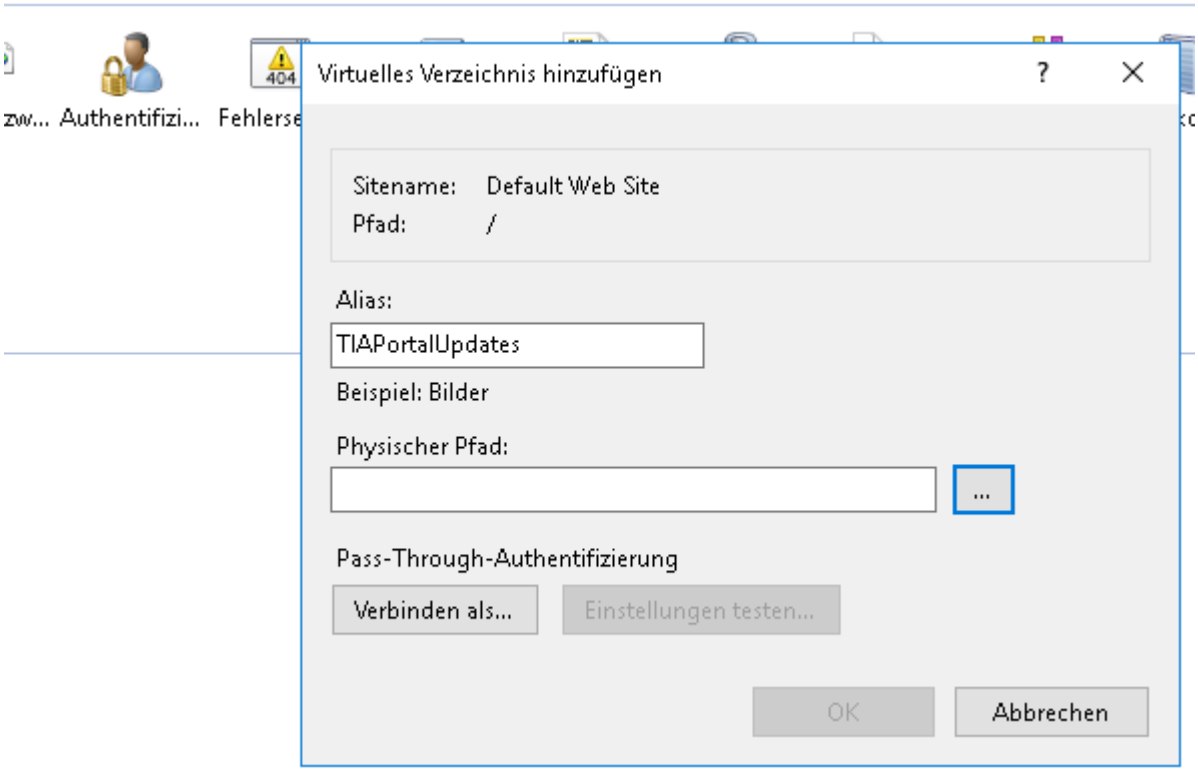


Website erstellen

1. Klicken Sie im Navigationsbereich auf "IIS" und im Bereich "Server" klicken Sie mit der rechten Maustaste und wählen Sie "Internetinformationsdienste (IIS)-Manager".
2. Klicken Sie im Bereich "Verbindungen" auf "Sites" und klicken Sie dann auf "Default Web Site".
3. Wählen Sie mit einem rechten Mausklick die Option "Virtuelles Verzeichnis hinzufügen...".



4. Geben Sie im aufgeblendeten Dialog einen Anzeigenamen in das Feld "Alias" ein, z. B. "TIAPortalUpdates".



5. Geben Sie im Feld "Physischer Pfad" den physischen Pfad des Ordners ein, in dem sich die Website befindet, oder klicken Sie auf die Schaltfläche zum Durchsuchen (**...**), um den Ordner im Dateisystem zu suchen.

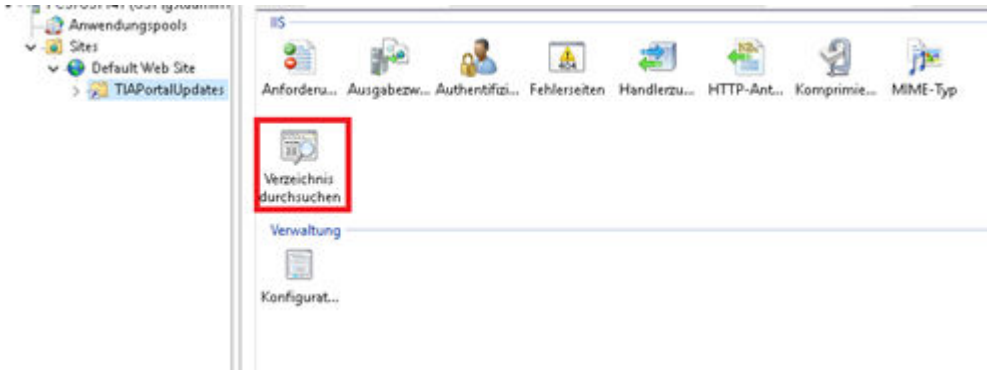
   Hinweis

   Die Default Web Site muss in dem Verzeichnis angelegt werden, das die Datei 'UpdatesSummaryCatalog.xml' enthält.

6. Klicken Sie auf "Einstellungen testen...", um zu prüfen, ob die Einstellungen korrekt sind.
7. Klicken Sie auf "OK".

Virtuelles Verzeichnis aktivieren

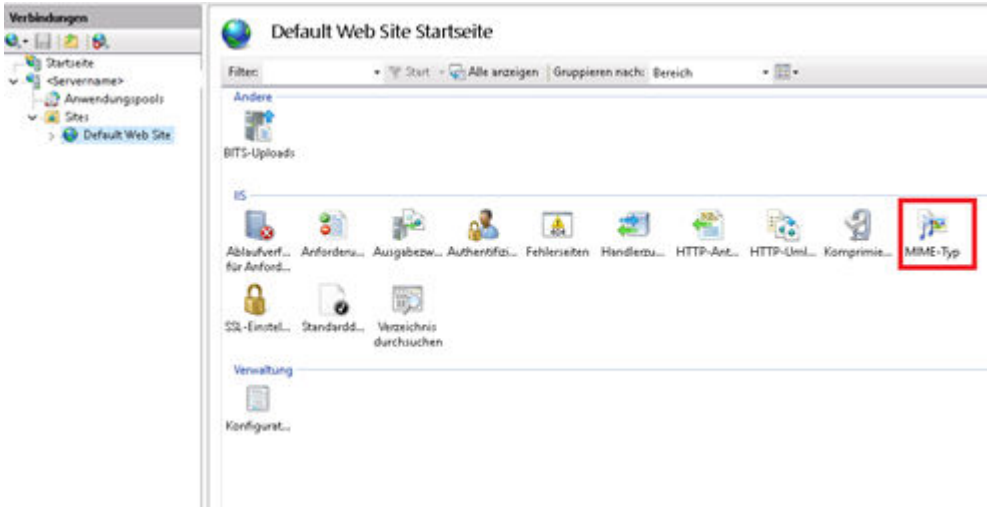
1. Markieren Sie im Bereich "Verbindungen > Sites > Default Web Site" das von Ihnen erstellte virtuelle Verzeichnis.
2. Doppelklicken Sie in der Ansicht "Features" den Eintrag "Verzeichnis durchsuchen".



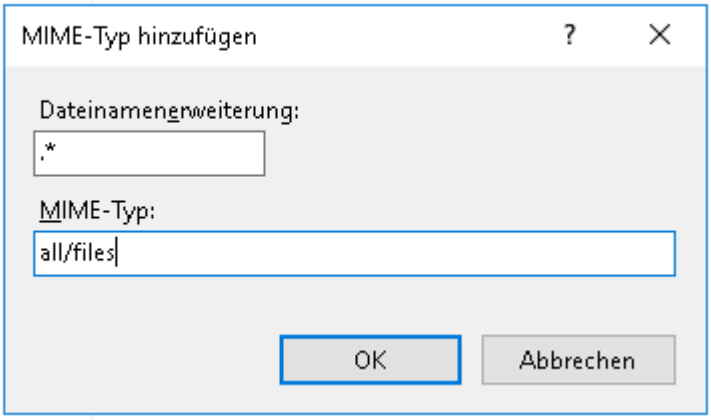
3. Klicken Sie im Bereich "Aktionen" auf "Aktivieren".

MIME-Typ hinzufügen und konfigurieren

1. Markieren Sie im Bereich "Verbindungen" die von Ihnen erstellte Website.
2. Doppelklicken Sie in der Ansicht "Features" auf "MIME-Typ".

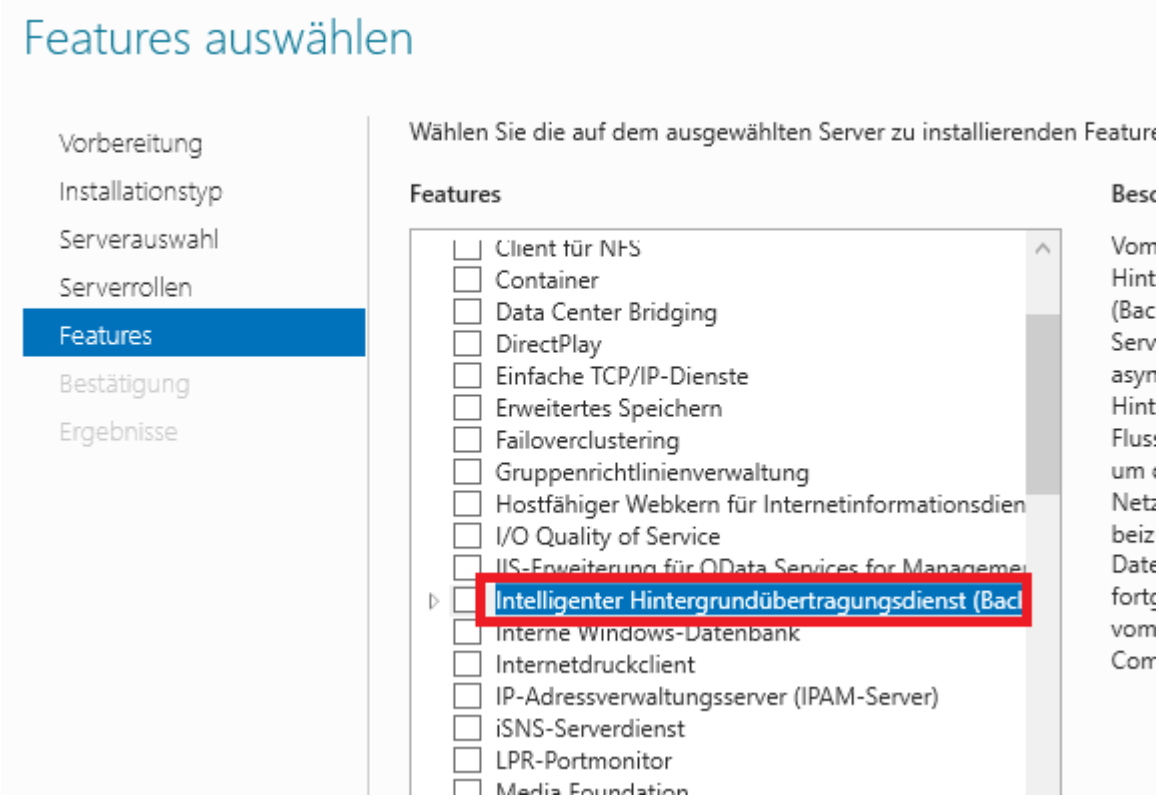


3. Klicken Sie im Bereich "Aktionen" auf "Hinzufügen".
4. Geben Sie im Dialog "MIME-Typ hinzufügen" im Textfeld "Dateinamenerweiterung" .* ein.
5. Geben Sie im Textfeld "MIME-Typ" "all/files" ein.
6. Klicken Sie auf "OK".

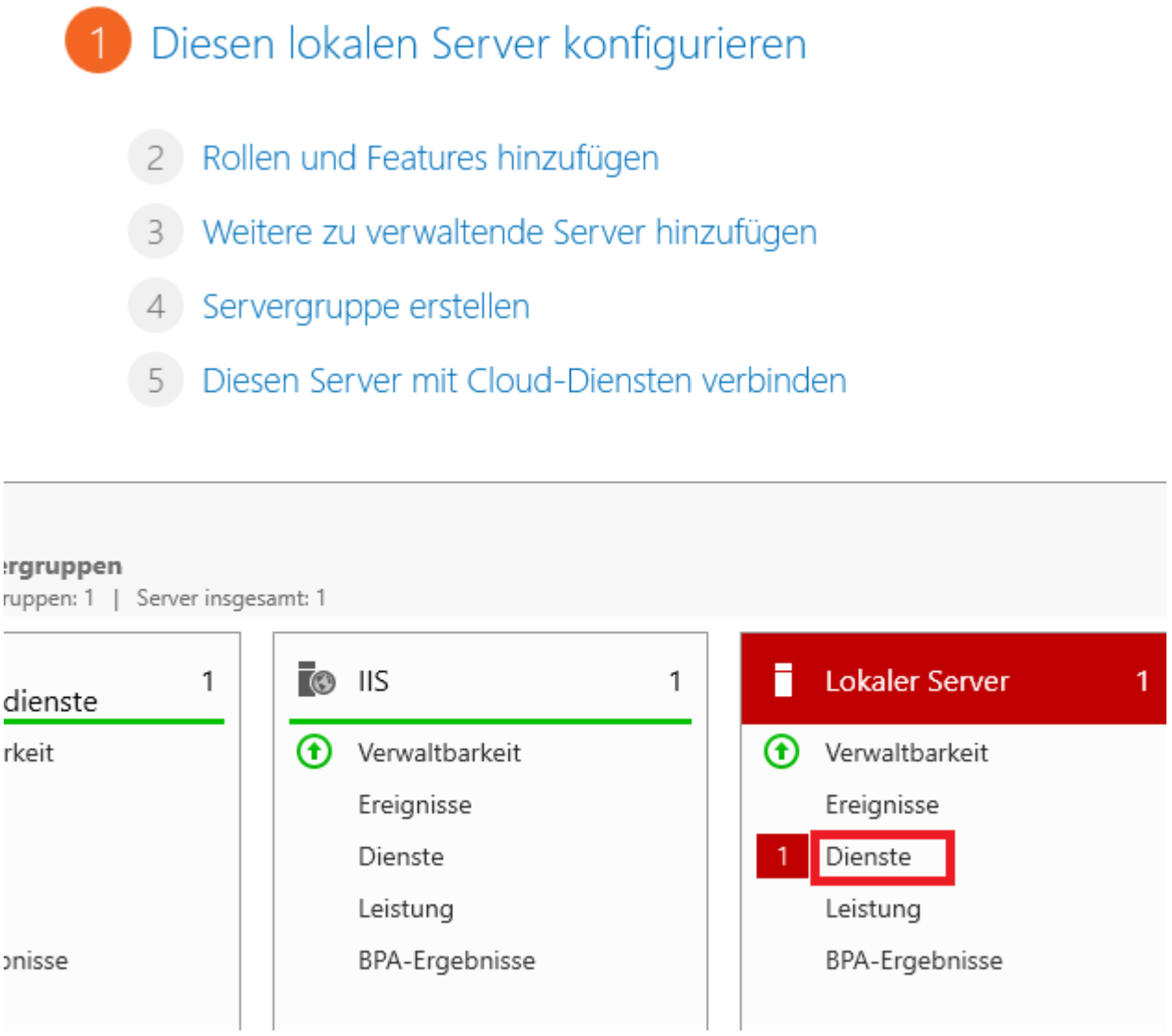


BITS-IIS-Servererweiterung aktivieren

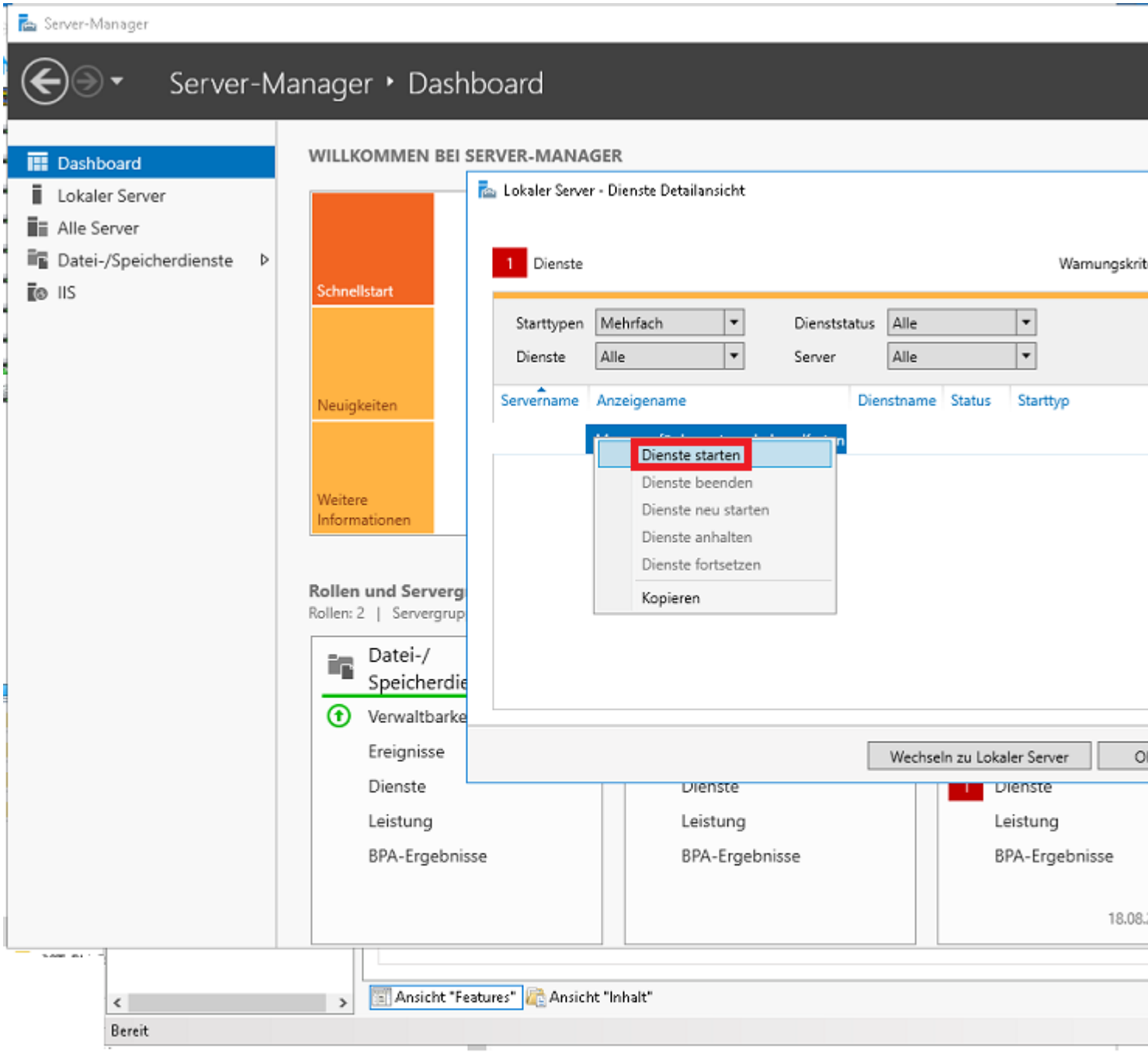
1. Wechseln Sie zum virtuellen Verzeichnis im IIS-Manager.
2. Klicken Sie auf "Rollen und Features hinzufügen", um zu überprüfen, dass BITS installiert ist. Aktivieren Sie gegebenenfalls das Feature "Intelligenter Hintergrundübertragungsdienst" und installieren Sie dieses.



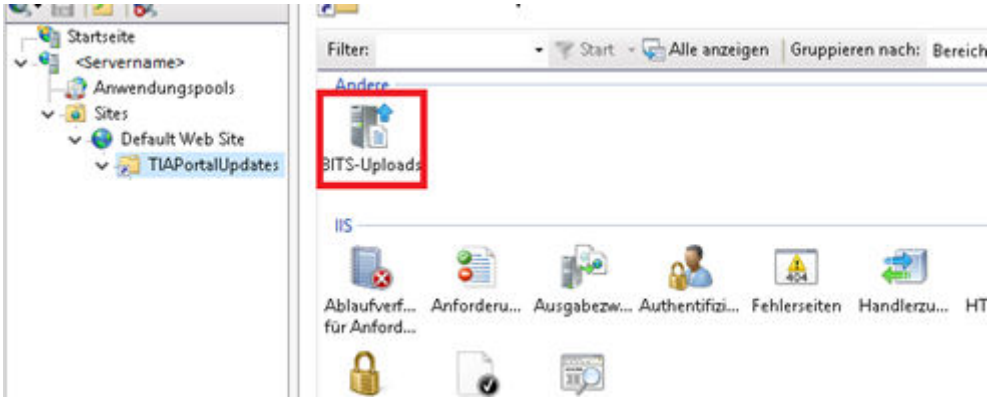
3. Klicken Sie im Dashboard im Bereich "Lokaler Server" auf "Dienste".



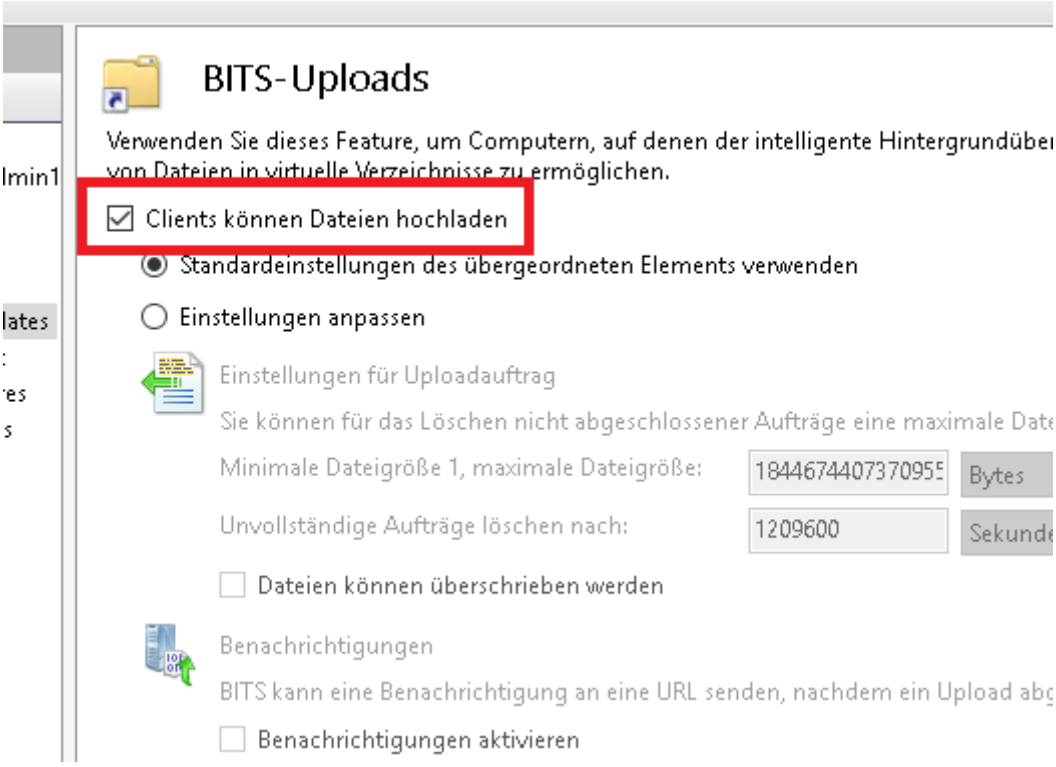
4. Selektieren Sie den lokalen Server, klicken Sie mit der rechten Maustaste und wählen Sie den Menübefehl "Dienste starten".


Server-Manager
Server-Manager • Dashboard
Dashboard
Lokaler Server
Alle Server
Datei-/Speicherdienste
IIS
WILLKOMMEN BEI SERVER-MANAGER
Schnellstart
Neuigkeiten
Weitere Informationen
Rollen und Serverg
Rollen: 2 | Servergrup
Datei-/ Speicherdie
Verwaltbarke
Ereignisse
Dienste
Leistung
BPA-Ergebnisse
Lokaler Server - Dienste Detailansicht
1 Dienste
Warnungskrit
Starttypen Mehrfach
Dienststatus Alle
Dienste Alle
Server Alle
Servername
Anzeigename
Dienstname
Status
Starttyp
Dienste starten
Dienste beenden
Dienste neu starten
Dienste anhalten
Dienste fortsetzen
Kopieren
Wechseln zu Lokaler Server
Ansicht "Features"
Ansicht "Inhalt"
Bereit

5. Wechseln Sie zur Featureansicht des virtuellen Verzeichnisses und doppelklicken Sie auf "BITS-Uploads".



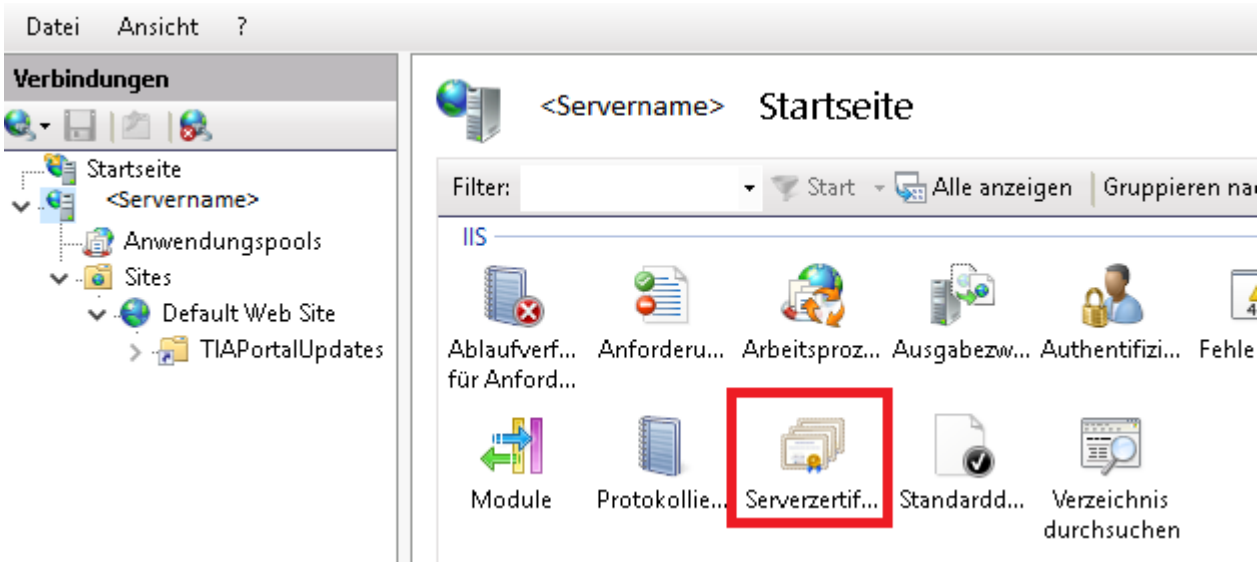
6. Aktivieren Sie das Optionskästchen "Clients können Dateien hochladen" und klicken Sie dann auf "Übernehmen".



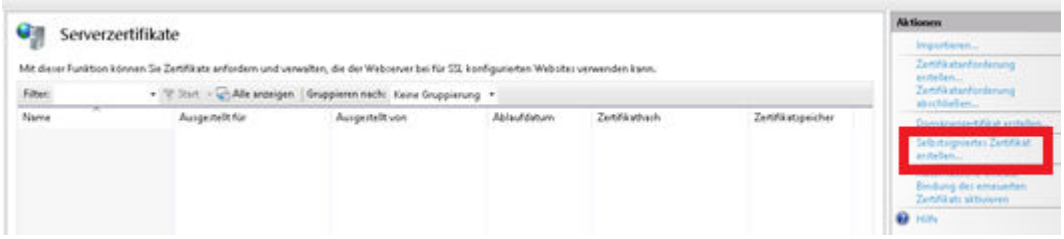
Selbstsigniertes Serverzertifikat erstellen

Es wird nachdrücklich empfohlen, ein von der IT-Abteilung Ihres Unternehmens erstelltes signiertes Zertifikat zu verwenden; dadurch erhält der unternehmenseigene Server ein qualifiziertes (sicheres) Zertifikat. Sie können ein solches Zertifikat auch von vertrauenswürdigen Fremdfirmen/Zertifizierungsstellen erwerben.
Sollte dies für Sie nicht möglich sein, können Sie ein selbstsigniertes Zertifikat erstellen. Beachten Sie hierbei, dass ein solches Zertifikat nicht sicher ist! Gehen Sie dazu folgendermaßen vor:

1. Navigieren Sie im Bereich "Verbindungen" zu der Ebene, die Sie verwalten möchten.
2. Doppelklicken Sie in der Ansicht "Features" auf "Serverzertifikate".



3. Klicken Sie im Bereich "Aktionen" auf "Selbstsigniertes Zertifikat erstellen".



4. Geben Sie im Dialog "Selbstsigniertes Zertifikat erstellen" im Feld "Anzeigename für das Zertifikat" einen Anzeigenamen für das Zertifikat ein und klicken Sie auf "OK".

SSL-Bindung erstellen

1. Erweitern Sie im Bereich "Verbindungen" den Eintrag "Sites" und klicken Sie anschließend auf die Site, der Sie eine Bindung hinzufügen möchten.
2. Klicken Sie im Bereich "Aktionen" auf "Bindungen".





3. Klicken Sie im Dialog "Sitebindungen" auf "Hinzufügen".
4. Wählen Sie im Dialog "Sitebindung hinzufügen" unter "Typ" "https" und unter "SSL-Zertifikat" das von Ihnen erstellte Zertifikat aus und klicken Sie dann auf "OK".

SSL-Bindung verifizieren

1. Klicken Sie im Bereich "Aktionen" unter "Website durchsuchen" auf die zuvor erstellte Bindung.
   Im Internet Explorer wird eine Fehlerseite geöffnet, weil das selbstsignierte Zertifikat von Ihrem Computer erstellt wurde.
2. Klicken Sie auf "Laden dieser Website fortsetzen (nicht empfohlen)".
   Wenn Sie das Zertifikat in den Zertifikatspeicher "Vertrauenswürdige Stammzertifizierungsstellen" hinzufügen, wird diese Meldung nicht mehr angezeigt.

SSL-Einstellungen konfigurieren

1. Doppelklicken Sie in der Ansicht "Features" auf "SSL-Einstellungen".
2. Verwenden Sie eines der folgenden Verfahren im Dialog "SSL-Einstellungen" im Bereich "Clientzertifikate":
   - Wählen Sie "Ignorieren", wenn auch dann keine Clientzertifikate akzeptiert werden sollen, wenn ein Client ein Zertifikat vorweisen kann.
   - Wählen Sie "Akzeptieren", wenn Clientzertifikate akzeptiert werden sollen.
   - Wählen Sie "Erforderlich", wenn Clientzertifikate erforderlich sein sollen. Damit die Option "Clientzertifikate erforderlich" verwendet werden kann, muss die Option "SSL erforderlich" aktiviert sein.
3. Klicken Sie im Bereich "Aktionen" auf "Übernehmen".

14.2.3 Updates auf unterschiedliche Bereiche verteilen

Es kann vorkommen, dass verschiedene Abteilungen unterschiedliche Updates oder Support Packages benötigen. In diesem Fall ist es empfehlenswert, mehrere Produktionslinien für Updates zu erstellen, die unterschiedliche Updates und Support Packages anbieten. Die Vorgehensweise hierzu ist in der Hilfe des TIA Updater Corporate Configuration Tools beschrieben.

Hinweis

Der Hauptvorteil von unterschiedlichen Produktionslinien liegt darin, dass weniger Speicherplatz benötigt wird. Wenn ein bereits heruntergeladenes Update, Support Package oder Sprachpaket zu einer neuen Produktionslinie hinzugefügt wird, wird keine Kopie hiervon angelegt, sondern von unterschiedlichen Produktionslinien wird auf dieses Update, Support Package oder Sprachpaket referenziert.

Vorgehen

Sie können auch mehrere Server betrieben, die unterschiedliche Updates, Support Packages und Sprachpakete bereitstellen. Gehen Sie dazu folgendermaßen vor:

1. Erstellen Sie unterschiedliche unternehmenseigene Server wie zuvor beschrieben.

oder

1. Erstellen Sie unterschiedliche unternehmenseigene Server wie zuvor beschrieben.
2. Erstellen Sie mehrere Websites.
   Beachten Sie, dass Sie eindeutige Namen für diese Websites und die physikalischen Pfade vergeben, damit es nicht zu Verwechselungen kommt!
3. Stellen Sie die zuvor beschriebenen Features für den Webserver bzw. die Websites ein.

Sie können nun die erforderlichen Updates und Support Packages für die verschiedenen Abteilungen in den definierten Verzeichnissen ablegen.

14.2.4 Updates auf einem unternehmenseigenen Server bereitstellen

Einführung

Im TIA Updater Corporate Configuration Tool können Sie einen unternehmenseigenen Server einstellen, auf dem Sie die verfügbaren Updates/Support Packages/Sprachpakete ablegen und den Anwendern zur Verfügung stellen können.

Voraussetzung

Sie müssen Administratorrechte besitzen.

Ein unternehmenseigener Server kann nur auf einem Microsoft Server Betriebssystem aufgesetzt werden, da zum Betrieb der BITS IIS-Dienst und ein laufender IIS-Sever benötigt wird.

Updates vom TIA Automation Software Update Server hinzufügen

Um Updates vom TIA Automation Software Update Server hinzuzufügen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das TIA Updater Corporate Configuration Tool.
   Die verfügbaren Updates werden angezeigt.
2. Klicken Sie auf die Schaltfläche "Update hinzufügen" und aktivieren Sie im aufgeblendeten Dialog das Optionskästchen "Vom TIA Automation Software Update Server hinzufügen".
3. Wählen Sie im Dialog "Update vom TIA Automation Software Update Server hinzufügen" die gewünschten Updates (Software und Support Packages) aus und klicken Sie auf "Hinzufügen".
   Wenn sich bereits Updates auf dem unternehmenseigenen Server befinden, so werden diese gegraut dargestellt. Sie können nicht erneut geladen werden. Während des Download-Vorgangs werden der Status und die verbleibende Zeit im Dialog angezeigt.

Abbrechen des Download-Vorgangs

Um den Vorgang abzubrechen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche "Download abbrechen".
2. Bestätigen Sie den aufgeblendeten Dialog mit "Ja".
   Der Download des Updates wurde abgebrochen und es wurde aus der Liste gelöscht.

Updates vom unternehmenseigenen Server löschen

Um Updates zu löschen, gehen Sie folgendermaßen vor:

Wählen Sie die gewünschten Updates aus und klicken Sie auf die Schaltfläche "Entfernen".

- Wenn ein Update nur zu **einem** Projekt/**einer** Fertigunglinie gehört, bestätigen Sie den aufgeblendeten Dialog mit "Ja".
  Das ausgewählte Update wird aus der Liste und aus dem Dateisystem gelöscht.
- Wenn ein Update zu **mehreren** Projekten/Fertigungslinien gehört, gilt Folgendes:
  - Der Dialog zum Entfernen des Updates wird nicht angezeigt.
  - Das ausgewählte Update wird nur aus der aktuellen Projektliste entfernt und nicht aus dem Dateisystem.

  Um Updates aus dem Dateisystem zu löschen, müssen alle Instanzen der Updates gelöscht werden. Gehen Sie dazu folgendermaßen vor:
  - Öffnen Sie das bestehende Projekt/die Globale Fertigungslinie über das Menü "Projekt".
  - Wählen Sie die gewünschten Updates aus und klicken Sie auf "Entfernen".
  - Bestätigen Sie den beim Löschen der letzten Instanz aufgeblendeten Dialog mit "Ja".

Server-Optionen

Klicken Sie im Dialog " TIA Automation Software Update Server" auf "Einstellungen", um Folgendes festzulegen:

1. Geben Sie unter "Server-Pfad" den Ordner an, in dem die Downloads gespeichert werden sollen. Sie können sowohl ein lokales Laufwerk als auch ein Netzlaufwerk auswählen.

   Hinweis

   Wenn Sie direkt auf dem Server arbeiten, ist das Zielverzeichnis gleich dem Bereitstellungsverzeichnis auf dem Server. Alle Änderungen werden direkt übernommen. Diese Vorgehensweise wird nicht empfohlen, da Konflikte mit aktiven Downloads auftreten können!

   Es wird empfohlen, auf einem sonstigen Rechner arbeiten; das Zielverzeichnis ist ein beliebiges Verzeichnis. Der Inhalt dieses Verzeichnisses muss dann noch in das Bereitstellungsverzeichnis kopiert werden. Stellen Sie hierbei ebenfalls sicher, dass keine Konflikte mit aktiven Downloads auftreten!

2. Aktivieren Sie das Optionskästchen "Server immer im Hintergrund laufen lassen (Symbol in der Taskleiste wird angezeigt)", wenn der Server immer im Hintergrund laufen soll.
3. Bestätigen Sie Ihre Eingaben mit "OK".

Siehe auch

Eigenschaften und Vorteile eines unternehmenseigenen Servers (Seite 108)

Unternehmenseigenen Server für Updates konfigurieren (Seite 109)

Support Packages automatisiert installieren 15

15.1 Support Packages automatisiert installieren

Einleitung

Mit dem Support Package Installer können Sie ab V15.1 alle Support Packages wie z. B. HSPs (Hardware Support Packages), die kompatibel zur installierten Version des TIA Portals sind (z. B. isp.15_1), automatisiert über die Kommandozeile installieren bzw. hochrüsten.

Voraussetzung

- Hardware und Software des PG/PC entsprechen den Systemanforderungen.
- Sie haben Administrationsrechte auf Ihrem Computer.
- Alle laufenden Programme sind beendet.

Vorgehen

Um die Installation direkt über die Kommandozeile mit den gewünschten Optionen zu starten, gehen Sie folgendermaßen vor:

1. Starten Sie die Eingabeaufforderung von Windows über "Start > Ausführen > cmd".
2. Wechseln Sie in das Verzeichnis, das die Datei "Siemens.Automation.SupportPackageInstaller.exe" enthält. Dies ist das Installationsverzeichnis Ihres installierten TIA Portals.
3. Geben Sie in der Eingabeaufforderung den folgenden Befehl ein:
   %Installationsverzeichnis% > Siemens.Automation.SupportPackageInstaller.exe <Support Package(HSP)-Ablageverzeichnis> [-l <Name der Protokolldatei>] [-warnaserror]

<Support Package-Ablageverzeichnis>
Zwingend erforderliches Verzeichnis, in dem die Support Package-Dateien (*.isp) liegen. Dies kann sowohl ein lokaler Ordner oder ein Remote Share sein.

-l <Ablageort der Protokolldatei>
Dieser Parameter ist optional und gibt den Pfad zur Protokolldatei an. Wenn er nicht gesetzt ist, wird die Protokolldatei im Binärverzeichnis erstellt. Sie müssen über Schreibrechte im Ablageordner verfügen!

-warnaserror
Dieser Parameter ist optional und gibt an, dass jede Nachricht, die in der Regel als Warnungen gemeldet worden wäre, stattdessen als Fehler gemeldet wird. Wenn beispielsweise ein HSP nicht den notwendigen Voraussetzungen entspricht, wird ein entsprechender Rückgabe-/Abbruchwert an die Kommandozeile ausgegeben und das betreffende HSP wird übersprungen.

-?
Dieser Parameter ist optional und zeigt die Hilfe an.

Hinweis

- Wenn das Ablageverzeichnis oder der Name der Protokolldatei Leerzeichen enthält, müssen Sie die Bezeichnungen in Anführungszeichen setzen.
- Es werden nur Support Packages berücksichtigt, die direkt im Ablageverzeichnis liegen; Unterverzeichnisse werden ignoriert. D. h. die *.isp-files müssen unmittelbar im Ablageverzeichnis liegen.

Siehe auch

Rückgabewerte des Installationsprozesses (Seite 126)

Protokolldatei (Seite 127)

15.2 Rückgabewerte des Installationsprozesses

Rückgabewerte des Installationsprozesses

Die folgende Tabelle zeigt die Rückgabewerte und ihre Beschreibungen:

Code	Beschreibung
0	Die Installation war erfolgreich.
1	Die Installation war erfolgreich, es ist ein Neustart erforderlich.
-1	Die Installation ist fehlgeschlagen.
-2	Die Installation ist fehlgeschlagen: Das TIA Portal läuft noch.
-3	Die Installation ist fehlgeschlagen: Eine andere Installation läuft bereits.
-4	Die Installation ist fehlgeschlagen: Sie haben nicht genügend Rechte. Für die Installation sind Administrationsrechte erforderlich.
-6	Die Installation ist fehlgeschlagen: Unzureichender Speicherplatz.
-7	Die Installation ist fehlgeschlagen: Es ist ein Neustart erforderlich bevor die Installation starten kann.

Siehe auch

Support Packages automatisiert installieren (Seite 125)

Protokolldatei (Seite 127)

15.3 Protokolldatei

Inhalt der Protokolldatei

Die Protokolldatei enthält detaillierte Informationen über jede Installation. Wenn die Protokolldatei bereits existiert, wird sie ergänzt. Für jede Installation werden Kopf- und Fußzeilen erstellt, zwischen denen Sie die gewünschten Informationen finden.

Für die folgenden Ereignisse wird ein Eintrag erzeugt:

- Support Packages, die zwar im Ablageverzeichnis aufgeführt und bei der Installation verfügbar sind, aber aufgrund fehlender Produkte nicht installiert werden konnten. Dem Eintrag in der Protokolldatei ist zu entnehmen, welche Produkte und welche Versionen dieser Produkte fehlen.
- Support Packages, die nicht erfolgreich installiert werden konnten.
- Support Packages, die erfolgreich installiert werden konnten.

Für jeden Eintrag wird der Dateiname des HSPs einschließlich der Dateiendung protokolliert.

Siehe auch

Support Packages automatisiert installieren (Seite 125)

Rückgabewerte des Installationsprozesses (Seite 126)

TIA Project-Server installieren und deinstallieren 16

16.1 Hinweise zur Installation des Projekt-Servers

Einführung

Um mit Multiuser Engineering, mit Multiuser Commissioning und mit Exclusive Engineering zu arbeiten, benötigen Sie einen Projekt-Server, der Ihre Serverprojekte, Server-Bibliotheken und die lokalen Sessions verwaltet.

Sie haben folgende Möglichkeiten, den "TIA Project-Server" zu installieren:

- Zusammen mit der Installation des TIA Portals.
- Als Standalone-Installation über einen eigenständigen Installationsprozess ohne TIA Portal.

Hinweis

Voraussetzung: Administratorrechte

Für die Installation des TIA Project-Server werden Administratorrechte benötigt.

Weitere Informationen:

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

Installation des TIA Project-Server mit dem TIA Portal

Die Installation des TIA Project-Server (nachfolgend "Projekt-Server" genannt) erfolgt zusammen mit der Installation folgender TIA Portal-Produkte:

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

Der Projekt-Server ist in der Produktauswahl teilweise per Voreinstellung aktiviert und wird dann mitinstalliert.

Überprüfen Sie die Einstellung während der Installation des TIA Portals.

Sie finden die jeweilige Voreinstellung für den Projekt Server während des Setups bei der Produktauswahl im Verzeichnis "Options".

Wählen Sie hier durch das Setzen oder entfernen des Häkchens aus, ob der Projekt-Server während der Installation des TIA Portals mitinstalliert werden soll oder nicht.

Installation des Projekt-Servers als Standalone-Installation

Die Installation des Projekt-Servers kann auch als Standalone-Installation durchgeführt werden.

Eine Beschreibung zur automatisierten Installation finden Sie auch in der Installationsquelle im Verzeichnis "Documents\Readme\<Sprachverzeichnis>".

Gleiche TIA Portal-Versionen bei der Installation

Achten Sie bei der Installation von TIA Portal-Produkten auf den verschiedenen Clients darauf, dass alle Teilnehmer für die Installation die gleichen Stände der Software-Produkte verwenden.

Wenn Sie also z. B. STEP 7 Professional, WinCCAdvanced und Safety sowie den Projekt-Server mit der Version Vx.y installiert haben, müssen alle anderen Teilnehmer von Team Engineering ebenfalls diese Software in identischen Versionen installiert haben.

Die Installation von Service Packs und Updates muss für alle Produkte zu einem gemeinsamen Zeitpunkt erfolgen.

Hinweis

TIA Project-Server: Versionierung

Ab TIA Portal V18 wird der TIA Project-Server mit einer vom TIA Portal unabhängigen Versionsnummer geliefert:

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

Installationspfad

Verwenden Sie keine Unicode-Zeichen (z. B. chinesische Schriftzeichen) im Installationspfad.

Virenscanner

Während der Installation ist es notwendig, dass auf bereits installierte Dateien lesend und schreibend zugegriffen werden kann.

Einige Virenscanner verhindern dies.

Daher wird empfohlen, während der Installation des Projekt-Servers Virenscanner zu deaktivieren und erst danach wieder zu aktivieren.

Unterstützte Virtualisierungsplattformen

Sie können den Projekt-Server ebenso wie das TIA Portal auch in einer virtuellen Maschine installieren.

Verwenden Sie dazu eine der folgenden Virtualisierungsplattformen in der angegebenen oder einer neueren Version:

- VMware vSphere Hypervisor (ESXi) 8.0 oder höher
- VMware Workstation V17 oder höher

- VMware Player V17 oder höher
- Microsoft Hyper-V Windows Server 2019 oder höher

Hinweis

Für die Installation einer Visualisierungsplattform gelten die gleichen Voraussetzungen wie für die Installation des TIA Portals.

Siehe auch

Projekt-Server installieren (Seite 131)

Projekt-Server deinstallieren (Seite 133)

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

16.2 Projekt-Server installieren

Einleitung

Den "TIA Project-Server" installieren Sie im Rahmen der TIA Portal-Installation oder standalone unabhängig vom TIA Portal.

Bei der Installation mit dem TIA Portal wird immer die dafür frei gegebene Version des Projekt-Servers installiert. Projekt-Server-Versionen, die danach veröffentlicht werden, sind auch für diese TIA Portal-Version frei gegeben, solange keine neue TIA Portal-Version existiert.

Eine Beschreibung zur automatisierten Installation finden Sie auch in der Installationsquelle im Verzeichnis "Documents\Readme\<Sprachverzeichnis>".

Hinweis

TIA Project-Server: Versionierung

Ab TIA Portal V18 wird der TIA Project-Server mit einer vom TIA Portal unabhängigen Versionsnummer geliefert:

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

Neuinstallation ersetzt bestehende Installation

Bis TIA Portal V18 sind Projekt-Server aus verschiedenen Versionen nebeneinander einsetzbar.

Ab TIA Portal V18 werden Versionen des TIA Project-Server nicht mehr parallel installiert. Die neue TIA Project-Server-Version ersetzt bei der Installation bereits bestehende Installationen.

Dabei werden die für den Server vorhandenen Benutzerberechtigungen übernommen.

Kompatibilität des Projekt-Servers mit dem TIA Portal

Die Kommunikation zwischen dem Projekt-Server und dem TIA Portal wird für folgende Anwendungsfälle unterstützt:

Version des Projekt-Servers	Version des TIA Portals
TIA Project-Server V2.0 / V2.1 / V2.2	V21, V20, V19, V18, V17, V16, V15.1, V15 und V14
TIA Project-Server V1.2	V19, V18, V17, V16, V15.1, V15 und V14
TIA Project-Server V1.1	V18, V17, V16, V15.1, V15 und V14
Server V17 / TIA Project-Server V1.0	V17, V16, V15.1, V15 und V14
Server V16	V16, V15.1, V15 und V14
Server V15.1 [1)]	V15.1, V15 und V14
Server V15 [1)]	V15 und V14
Server V14 [1)]	V14

1) Die abgekündigten Versionen werden weiterhin vom aktuellen TIA Project-Server unterstützt.

Hinweis

Hinweise zur Kompatibilität des Projekt-Servers

Die für die aktuelle Version neu hinzugefügte Serverfunktionalität ist nur dann verfügbar, wenn auch das aktuelle TIA Portal installiert ist.

Arbeiten Sie noch mit einer älteren TIA Portal-Version oder mit einer älteren Projekt-Server-Version, so ist nur die in der jeweiligen Produktversion enthaltene Funktionalität verfügbar.

Multiuser Engineering führt kein Upgrade der Projektversionen durch.

TIA Portal-Versionen < V18

Bis TIA Portal V18 können auf einem Computer mehrere Versionen des Projekt-Servers installiert sein, die unterschiedliche Projektversionen des TIA Portals verwenden.

Jede Version des TIA Portals und des Projekt-Servers verfügt jedoch jeweils nur über die in dieser Version enthaltene Funktionalität.

Multiuser Engineering führt kein Upgrade der Projektversionen durch.

Ab TIA Portal V18 wird der TIA Project-Server ab V1.0 geliefert. Die Neuinstallationen des TIA Project-Server ersetzen jeweils die bestehende Installation. Unterschiedliche Versionen des Projekt-Servers können ab V1.0 nicht mehr auf dem gleichen PC installiert werden.

Versionen des Projekt-Servers, die mit TIA Portal-Versionen kleiner als V18 installiert wurden, können jedoch weiterhin nebeneinander auf einem PC und parallel zum TIA Project-Server ab V1.0 laufen.

Voraussetzungen für die Installation

Sie benötigen Administratorrechte.

Die Installation des Servers benötigt Einstellungen in der Windows-Firewall und gegebenenfalls ein Zertifikat.

Systemvoraussetzungen:

- Für die Installation des Projekt-Servers gelten die gleichen Voraussetzungen wie für die Installation des TIA Portals.

Projekt-Server mit dem TIA Portal installieren

Für die Installation gehen Sie folgendermaßen vor:

1. Beachten Sie die Voraussetzungen für die Installation des ausgewählten Softwarepakets.
2. Navigieren Sie zu der Datei "Start.exe" in der Installationsquelle und doppelklicken Sie darauf.
3. Wählen Sie die gewünschten Einstellungen und klicken Sie auf die Schaltfläche "Installieren".
4. Vergewissern Sie sich, dass der Projekt-Server in der Produktauswahl angewählt ist, und folgen Sie den Hinweisen in den Setup-Dialogen.

Ergebnis

Der Projekt-Server wurde auf Ihrem Computer zusammen mit dem TIA Portal installiert.

Projekt-Server standalone installieren

Für die Installation gehen Sie folgendermaßen vor:

1. Beachten Sie die Voraussetzungen für die Installation des Projekt-Servers.
2. Um das Setup zu starten, doppelklicken Sie auf die selbstextrahierende Datei "TIA_Portal_Projekt_Server_V<x.y>.exe".
   Sie finden diese Datei im "Support"-Verzeichnis in der Installationsquelle.
3. Wählen Sie die gewünschten Einstellungen und klicken Sie auf die Schaltfläche "Installieren".
4. Folgen Sie den Anweisungen in den Setup-Dialogen.

Ergebnis

Der TIA Project-Server wurde erfolgreich auf Ihrem Computer installiert.

Siehe auch

Hinweise zur Installation des Projekt-Servers (Seite 129)

Projekt-Server deinstallieren (Seite 133)

16.3 Projekt-Server deinstallieren

Einleitung

Den "TIA Project-Server" deinstallieren Sie über die Systemsteuerung.

Die Installation einer neuen Version des Projekt-Servers ersetzt eine bestehende Installation.

Voraussetzungen für die Deinstallation

Auf Ihrem Computer ist eine Projekt-Server-Installation vorhanden.

TIA Project-Server deinstallieren

Für die Deinstallation gehen Sie vor wie folgt:

1. Öffnen Sie die Systemsteuerung.
2. Doppelklicken Sie in der Systemsteuerung auf den Eintrag "Software".
   Der Dialog "Software" wird geöffnet.
3. Wählen Sie im Dialog "Software" den Eintrag für den "TIA Project-Server".
4. Klicken Sie auf die Schaltfläche "Entfernen".
   Eine Sicherheitsabfrage erscheint.
5. Bestätigen Sie die Sicherheitsabfrage, indem Sie auf die Schaltfläche "Deinstallieren" klicken.

Ergebnis

Der TIA Project-Server wurde auf ihrem Computer deinstalliert.

Siehe auch

Hinweise zur Installation des Projekt-Servers (Seite 129)

Projekt-Server installieren (Seite 131)

TIA Administrator installieren und deinstallieren 17

17.1 Einführung zum TIA Administrator

Der TIA Administrator bietet Ihnen einen Überblick über installierte Software-Pakete.

Abhängig von den installierten Modulen sind weitere Funktionen verfügbar, z. B. der Download von Software-Paketen und Updates.

Informationen zur Installation und Deinstallation sowie zum Starten und Beenden des TIA Administrators finden Sie im vorliegenden Dokument.

Informationen zur Konfiguration und Bedienung des TIA Administrators finden Sie in der Hilfe der Anwendung.

17.2 Systemvoraussetzungen

Der TIA Administrator ist eine Webapplikation und läuft vollständig im Browser. Damit Sie den TIA Administrator verwenden können, muss einer der folgenden Browser auf Ihrem Rechner installiert sein:

- Google Chrome Version 114 oder höher
- Microsoft Edge Version 114 oder höher
- Mozilla Firefox Version 114 oder höher

17.3 TIA Administrator installieren

Den TIA Administrator finden Sie in der Installationsquelle des TIA Portals.

Vorgehen

Prüfen Sie gegebenenfalls die Integrität und Authentizität der Installationsquelle. Siehe auch: Installation ausführen (Seite 89)

Um den TIA Administrator zu installieren, gehen Sie folgendermaßen vor:

1. Doppelklicken Sie auf die Installatonsdatei "Start.exe".
2. Bestätigen Sie die Sicherheitsabfrage, indem Sie auf "Ja" klicken.
   Das Installationsprogramm wird geöffnet.
3. Wählen Sie die Installationssprache aus und klicken Sie auf "Weiter"
4. Wählen Sie eine oder mehrere Produktsprachen aus und klicken Sie auf "Weiter".
5. Wählen Sie die zu installierenden Komponenten aus.
6. Ändern Sie gegebenenfalls das Zielverzeichnis für die Installation und klicken Sie auf "Weiter".

7. Lesen und bestätigen Sie die Lizenzbedingungen und Sicherheitshinweise, indem Sie die Kontrollkästchen aktivieren.
8. Klicken Sie auf "Weiter".
9. Stellen Sie die Konfiguration des TIA Software Update Servers ein. Sie haben folgende Optionen:
   - TIA Automation Software Update Server
   - Unternehmenseigener Server
   - Fahren Sie mit den aktuellen Einstellungen fort
10. Wenn Sie einen unternehmenseigenen Server einstellen wollen, geben Sie den Server-Pfad und die Fertigungslinie in die Eingabefelder ein.
    Fertigungslinien dienen dazu, um verschiedenen Anwendern gezielt bestimmte Updates/ Support Packages bereitzustellen. Wenn Ihr Unternehmen nicht mit verschiedenen Fertigungslinien arbeitet, vergeben Sie einen Namen, z. B. "ProductionLine1".
    Diese Einträge können Sie später in den Einstellungen des TIA Administrators ändern.
11. Klicken Sie auf "Weiter".
    Eine Übersicht über die Produktkonfiguration wird angezeigt.
12. Klicken Sie auf "Installieren".
    Die Installation wird mit den angezeigten Einstellungen durchgeführt.
    Nach der Installation des TIA Administrators ist ein Neustart des Rechners erforderlich.

Ergebnis

Der TIA Administrator wird auf Ihrem Rechner installiert. Bei der Installation des TIA Administrators wird ein digitales Zertifikat auf Ihrem Rechner installiert. Dieses Zertifikat wird zum Aufbau einer sicheren Verbindung benötigt.

17.4 TIA Administrator deinstallieren

Der TIA Administrator kann über die Systemsteuerung deinstalliert werden.

Vorgehen

Um den TIA Administrator zu deinstallieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Systemsteuerung.
2. Klicken Sie in der Systemsteuerung auf den Eintrag "Programme und Funktionen".
   Der Dialog "Programm deinstallieren oder ändern" wird geöffnet.
3. Wählen Sie im Dialog "Programm deinstallieren oder ändern" den Eintrag für den TIA Administrator aus und klicken Sie auf die Schaltfläche "Deinstallieren".
   Es erscheint eine Sicherheitsabfrage.
4. Bestätigen Sie die Sicherheitsabfrage, indem Sie auf die Schaltfläche "Ja" klicken.
   Das Deinstallationsprogramm startet.
5. Wählen Sie die Installationssprache aus und klicken Sie auf "Weiter".
6. Wählen Sie den TIA Administrator zur Deinstallation aus und klicken Sie auf "Weiter".

7. Klicken Sie auf "Deinstallieren".
8. Um das Setup-Programm zu beenden, klicken Sie auf "Beenden".

Ergebnis

Der TIA Administrator wird deinstalliert. Das digitale Zertifikat des TIA Administrators wird bei der Deinstallation entfernt.

17.5 TIA Administrator starten und beenden

17.5.1 TIA Administrator lokal starten

Standardmäßig wird der TIA Administrator bei der Installation im folgenden Verzeichnis gespeichert:

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

Bei der Installation wird im Startmenü unter "Siemens Automation" eine Verknüpfung "TIA Administrator V2" angelegt.

TIA Administrator starten

Um den TIA Administrator lokal zu starten, gehen Sie folgendermaßen vor:

1. Wählen Sie unter Windows den Befehl "Start > Siemens Automation > TIA Administrator V2". Ihr Browser baut eine sichere Verbindung über das HTTPS-Protokoll zum TIA Administrator auf.
2. Geben Sie im Anmeldefenster unter "Benutzer-Login" Ihren Benutzernamen und Ihr Kennwort in die Eingabefelder ein.
3. Klicken Sie auf die Schaltfläche "Einloggen".
   Das Hauptfenster des TIA Administrators öffnet sich in Ihrem Browser.

17.5.2 TIA Administrator per Fernzugriff starten

Für Administratoren ist die Möglichkeit vorgesehen, von einem anderen Gerät (z. B. PC, Tablet) im gleichen Netzwerk auf den TIA Administrator zuzugreifen.

Dazu muss auf Ihrem Gerät ein kompatibler Browser installiert sein. Unter Umständen müssen Sie ihre Firewall für den Fernzugriff einrichten.

TIA Administrator starten

Um den TIA Administrator per Fernzugriff zu starten, gehen Sie folgendermaßen vor:

1. Öffnen Sie Ihren Browser.
2. Geben Sie die URL zum Zielgerät in die Adressleiste ein.

   Hinweis

   URL zum Zielgerät

   Die URL setzt sich zusammen aus dem HTTPS-Protokoll, dem Rechnernamen oder der IP-Adresse und dem Port.

   Standardmäßig ist der Port 8890 vorgegeben.

   Beispiel für eine URL: https://w10-setup-serv:8890

   Ihr Browser stellt die Verbindung zum Zielgerät als unsichere Verbindung dar und zeigt eine Warnung an. Sie können diese Warnung ignorieren und mit der Anmeldung fortfahren.
3. Geben Sie im Anmeldefenster unter "Benutzer-Login" Ihren Benutzernamen und Ihr Kennwort in die Eingabefelder ein.
4. Klicken Sie auf die Schaltfläche "Einloggen".
   Das Hauptfenster des TIA Administrators öffnet sich in Ihrem Browser.

17.5.3 TIA Administrator beenden

Um den TIA Administrator zu beenden, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Menü.
2. Klicken Sie auf "Abmelden".
3. Bestätigen Sie die Abmeldung, indem Sie auf "Ja" klicken.
4. Schließen Sie Ihren Browser.