

SIEMENS

SIMATIC

Anleitung zum TIA Portal Cloud Connector

Bedienhandbuch

Einführung in den TIA Portal
Cloud Connector

1

Systemvoraussetzungen

2

Virtuelle Maschine (VM)
bereitstellen

3


Virtuelle Maschine (VM)
verwenden


4


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. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

 WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet 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 AG. 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.

Inhaltsverzeichnis

1	Einführung in den TIA Portal Cloud Connector.....	5
1.1	Security-Hinweise.....	5
1.2	Grundlagen zum Arbeiten mit dem TIA Portal Cloud Connector.....	5
1.3	Bedienoberfläche des TIA Portal Cloud Connectors.....	7
1.4	Anwendungsfälle des TIA Portal Cloud Connectors.....	17
1.5	Besonderheiten beim Arbeiten in einer virtuellen Maschine.....	19
1.6	Verwendung von Zertifikaten.....	20
2	Systemvoraussetzungen.....	23
2.1	Systemvoraussetzungen PG/PC.....	23
2.2	Systemvoraussetzungen VM.....	24
2.3	Lizenzen.....	27
2.4	Lizenz des Benutzergeräts belegen.....	28
3	Virtuelle Maschine (VM) bereitstellen.....	31
3.1	Neue VM-Vorlage erstellen.....	31
3.2	Benutzer- und Projekteinstellungen zentral speichern.....	32
3.3	License-Key-Server nutzen.....	34
3.4	TIA Portal Cloud Connector in der VM installieren.....	35
4	Virtuelle Maschine (VM) verwenden.....	39
4.1	TIA Portal Cloud Connector auf dem PG/PC installieren.....	39
4.2	TIA Portal Cloud Connector am PG/PC konfigurieren.....	40
4.3	TIA Portal Cloud Connector in der VM konfigurieren.....	42
4.4	Zertifikate verwenden (nur für HTTPS-Verbindungen).....	44
4.4.1	Zertifikat für die Datenverschlüsselung erstellen.....	44
4.4.2	Zertifikat für die Datenverschlüsselung exportieren.....	45
4.4.3	Zertifikat für die Datenverschlüsselung importieren.....	46
4.4.4	Zertifikat für die Datenverschlüsselung auswählen.....	47
4.4.5	Zertifikat für die Benutzerauthentifikation erstellen.....	48
4.4.6	Zertifikat für die Benutzerauthentifikation exportieren.....	49
4.4.7	Zertifikat für die Benutzerauthentifikation importieren.....	50
4.4.8	Zertifikat für die Benutzerauthentifikation hinzufügen.....	51
4.4.9	Zertifikat für die Benutzerauthentifikation auswählen.....	52
4.4.10	Zertifikat für die Benutzerauthentifikation entfernen.....	53
4.5	Online-Verbindung über den TIA Portal Cloud Connector.....	54
4.6	Virtuelle Maschine (VM) offline verwenden.....	55

Index.....57

Einführung in den TIA Portal Cloud Connector

1.1 Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z. B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter: <http://www.siemens.com/industrialsecurity> (<http://www.industry.siemens.com/topics/global/de/industrial-security/Seiten/Default.aspx>)

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter:

<http://www.siemens.com/industrialsecurity> (<http://www.industry.siemens.com/topics/global/de/industrial-security/Seiten/Default.aspx>)

1.2 Grundlagen zum Arbeiten mit dem TIA Portal Cloud Connector

Funktion des TIA Portal Cloud Connectors

Das TIA Portal erlaubt Ihnen das Arbeiten in einer virtuellen Umgebung. Der TIA Portal Cloud Connector ist eine produktübergreifende Option, die es zudem ermöglicht, auf lokale PG/PC-Schnittstellen und daran angeschlossene SIMATIC Hardware im TIA Portal Engineering zuzugreifen, obwohl das Engineering selbst per Remote Desktop in einer Private Cloud betrieben wird.

Mithilfe des Optionspakets "TIA Portal Cloud Connector" können Sie aus der VM heraus auf Ihre lokal am PG/PC angeschlossene SIMATIC-Hardware zugreifen. Dazu ist eine Installation des TIA Portal Cloud Connectors sowohl in der VM als auch auf dem PG/PC notwendig, mit dem die SIMATIC-Hardware verbunden ist. Zusätzlich ermöglicht Ihnen der TIA Portal Cloud Connector über die Remote Desktop-Verbindung den Zugriff auf die SIMATIC-Hardware eines

anderen PG/PCs. Das andere PG/PC kann sich dabei in einem anderen Netzwerk befinden. Ein solcher Zugriff ist ohne TIA Portal Cloud Connector nicht möglich.

Die Verwendung von virtuellen Maschinen zusammen mit dem TIA Portal Cloud Connector in einer Private Cloud bietet Ihnen folgende Vorteile:

- Unterstützung moderner Private Cloud-Infrastrukturen:
 - Freie Skalierbarkeit
 - Keine Installation auf den einzelnen Arbeitsplatzrechnern notwendig
 - Zentrale Wartung und Administration des TIA Portals in der VM
 - Zentrale Datenablage für Projekte und Bibliotheken
- Netzwerkübergreifender Online-Zugriff auf PLCs und HMI-Geräte
- Gesicherte Verbindung über HTTPS (ab Windows 8.1)
- Unterstützung aller lokalen Schnittstellen der Arbeitsplatzrechner
- Schnellen Zugriff auf unterschiedliche Versionen des TIA Portals
- Effizientere Auslastung der vorhandenen Lizenzen
- Einfache Fernwartung von Maschinen

Sie haben die Möglichkeit, aus einer fertig konfigurierten VM eine Vorlage zu erzeugen. Aus dieser Vorlage können Sie neue VMs ableiten. Dadurch können Sie Installations- und Konfigurationsaufwand sparen.

Bereitstellung des TIA Portal Cloud Connectors

Die Software des TIA Portal Cloud Connectors wird mit den folgenden SIMATIC-Softwarepaketen ab dem TIA Portal V14.0 mitgeliefert:

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

Sie benötigen für die Verwendung des TIA Portal Cloud Connectors eine Lizenz auf dem PG/PC, die Sie separat erwerben müssen.

Hinweis

TIA Portal Cloud Connector

Die Nutzung des TIA Portal Cloud Connectors ist nur für Engineering-Arbeiten mit dem TIA Portal vorgesehen.

Weitere Informationen finden Sie im Siemens Industry Online Support unter <https://support.industry.siemens.com/cs/ww/de/view/109739390> (<https://support.industry.siemens.com/cs/ww/de/view/109739390>).

TIA Portal Cloud Connector konfigurieren

Bevor Sie mithilfe des TIA Portal Cloud Connectors eine Verbindung herstellen können, müssen Sie den TIA Portal Cloud Connector konfigurieren. Die Konfiguration ist abhängig von der Kommunikationsrolle Ihres Geräts. Der TIA Portal Cloud Connector kennt zwei Kommunikationsrollen:

- Kommunikationsrolle "Benutzergerät":
Das Benutzergerät ist Ihr PG/PC, an dem die Hardware angeschlossen ist. Auf diesem Gerät muss kein TIA Portal installiert sein. Diese Kommunikationsrolle wird automatisch voreingestellt, wenn Sie den TIA Portal Cloud Connector separat installieren, also nicht zusammen mit dem TIA Portal.
Siehe auch: TIA Portal Cloud Connector am PG/PC konfigurieren (Seite 40)
- Kommunikationsrolle "Remotegerät":
Das Remotegerät ist die VM, in welcher das TIA Portal installiert ist. Diese Kommunikationsrolle wird automatisch voreingestellt, wenn Sie den TIA Portal Cloud Connector zusammen mit dem TIA Portal installieren.
Siehe auch: TIA Portal Cloud Connector in der VM konfigurieren (Seite 42)

Siehe auch

Bedienoberfläche des TIA Portal Cloud Connectors (Seite 7)
Anwendungsfälle des TIA Portal Cloud Connectors (Seite 17)
Besonderheiten beim Arbeiten in einer virtuellen Maschine (Seite 19)
Verwendung von Zertifikaten (Seite 20)
Systemvoraussetzungen (Seite 23)
Virtuelle Maschine (VM) bereitstellen (Seite 31)
Virtuelle Maschine (VM) verwenden (Seite 39)

1.3 Bedienoberfläche des TIA Portal Cloud Connectors

Die Bedienoberfläche des TIA Portal Cloud Connectors besteht aus den folgenden Elementen:

- Eintrag im Infobereich der Windows-Taskleiste
- TIA Portal Cloud Connector - Einstellungen
- TIA Portal Cloud Connector - Statusanzeige
- TIA Portal Cloud Connector - Info-Fenster
- TIA Portal - Anzeige in der Statusleiste

TIA Portal Cloud Connector im Infobereich der Windows-Taskleiste

Nach dem Starten des TIA Portal Cloud Connectors finden Sie im Infobereich der Windows-Taskleiste das Symbol für den Cloud Connector. Wenn Sie mit der rechten Maustaste auf das Symbol klicken, öffnet sich das Menü des TIA Portal Cloud Connectors.

Das folgende Bild zeigt das Symbol des TIA Portal Cloud Connectors im Infobereich der Windows-Taskleiste, wenn die Kommunikationsendpunkte deaktiviert sind:



Abhängig vom Status der Kommunikationsendpunkte variiert das Symbol in der Farbe.

Das folgende Bild zeigt das Menü im Infobereich mit der eingestellten Kommunikationsrolle "Remotegerät":

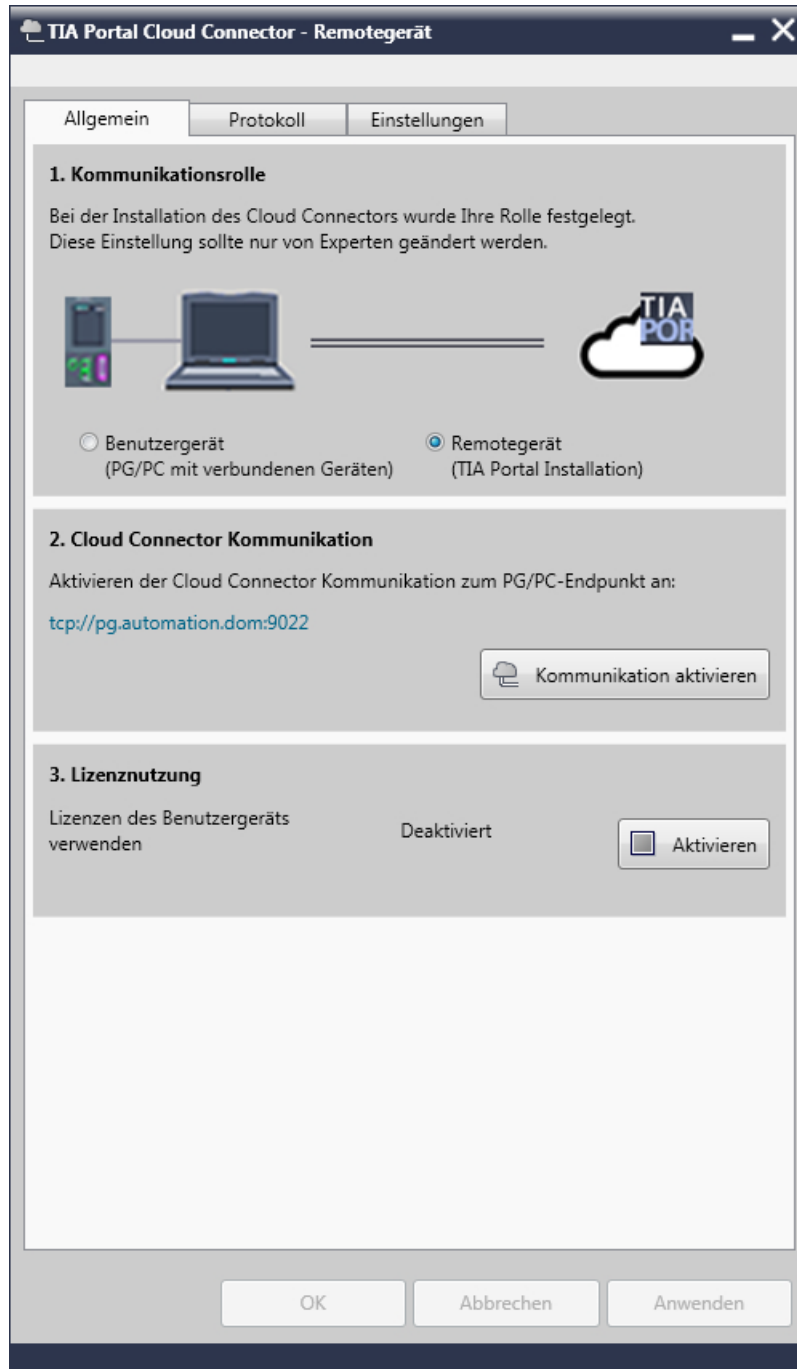


Über das Menü haben Sie Zugriff auf die folgenden Aktionen:

- Kommunikation aktivieren: Über diesen Befehl können Sie sowohl am Remote- als auch am Benutzergerät die Kommunikation aktivieren.
- Konfiguration (Remotegeräte/Benutzergerät): Öffnet den TIA Portal Cloud Configurator in der jeweiligen Kommunikationsrolle.
- Statusanzeige: Öffnet die Statusanzeige, in der Sie über alle Vorgänge informiert werden.
- Info: Öffnet das Info-Fenster des TIA Portal Cloud Connectors. Hier finden Sie z. B. die Versionsnummer.
- Hilfe: Öffnet die Online-Hilfe des TIA Portal Cloud Connectors.
- Beenden: Beendet den TIA Portal Cloud Connector.

TIA Portal Cloud Connector - Einstellungen

Die Oberfläche des TIA Portal Cloud Connectors unterscheidet sich abhängig von der eingestellten Kommunikationsrolle. Die folgenden Bilder zeigen die verschiedenen Einstellungsregister des TIA Portal Cloud Connectors in der Kommunikationsrolle "Remotegerät":







Innerhalb der unterschiedlichen Register können Sie alle Einstellungen vornehmen, die für eine Verbindung notwendig sind.

1.3 Bedienoberfläche des TIA Portal Cloud Connectors

Die folgende Tabelle zeigt eine Übersicht über die möglichen Einstellungen und die vorhandenen Schaltflächen für die Kommunikationsrolle "Remotegerät":

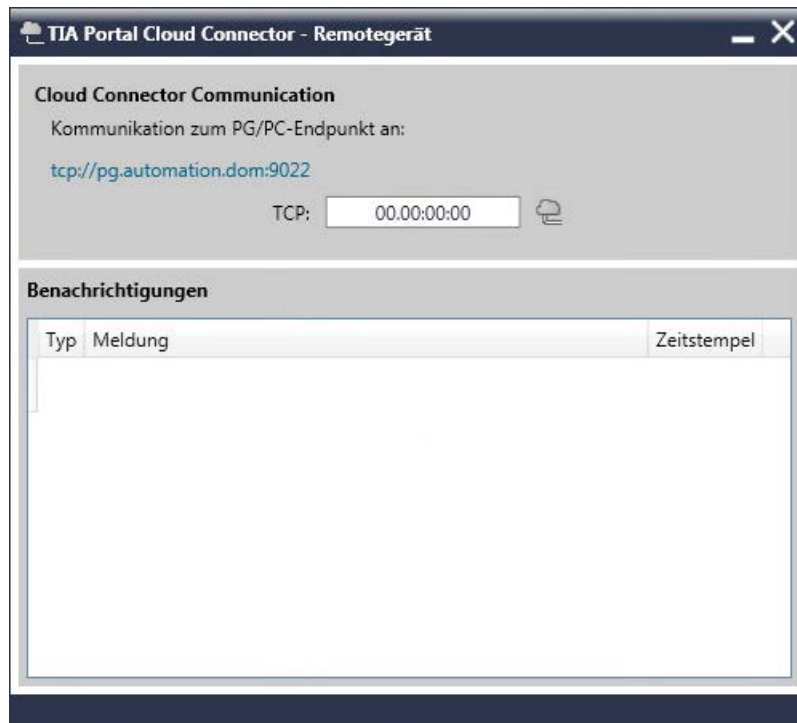
Register	Bereich	Einstellung/Schaltfläche	Beschreibung
Allgemein	Kommunikationsrolle	Benutzergerät	PG/PC, das den physikalischen Kontakt zur SIMATIC Hardware ermöglicht.
		Remotegerät	Virtuelle Maschine (VM), auf der das TIA Portal installiert ist. Vom Benutzergerät kann darauf via Remote Desktop-Verbindung zugegriffen werden.
	Cloud Connector Kommunikation	Kommunikation aktivieren Kommunikation deaktivieren	Aktiviert bzw. deaktiviert die Kommunikation zu einem PG/PC-Endpunkt.
	Lizenzzugriffe	Aktivieren Deaktivieren	Aktiviert bzw. deaktiviert die Verwendung einer Lizenz vom Benutzergerät.
Protokoll	Kommunikationsprotokoll		Definiert den Transportmechanismus zwischen den Kommunikationsendpunkten. Es stehen Ihnen TCP oder HTTPS (ab Windows 8.1) zur Verfügung.
	TCP-Einstellungen	Zielgerät	Typ des Verbindungspartners
		Adresse des Benutzergeräts	IP-Adresse oder Name des Benutzergeräts
		Port	Portnummer, über die der Transport erfolgen soll
	HTTPS-Einstellungen	Adresse des Benutzergeräts	IP-Adresse oder Name des Benutzergeräts
		Fingerabdruck	Stellt die Integrität des Zertifikats sicher.
		Importieren	Importiert ein vorhandenes Zertifikat in den Windows-Zertifikatsspeicher. Sie können ein importiertes Zertifikat für die Verschlüsselung von Daten verwenden, die über HTTPS verschickt werden.
		Auswählen	Auswahl eines zuvor importierten Zertifikats zur Datenverschlüsselung.
	Konfiguriertes Kommunikationsprotokoll	Verbindung überprüfen	Prüft, ob die Verbindung fehlerfrei aufgebaut werden kann.
	Einstellungen	Autostart	Autostart des Cloud Connectors aktivieren
Sprache		Sprache auswählen	Legt die Oberflächensprache für den TIA Portal Cloud Connector fest.
Benutzer-Authentifizierung		Name des Benutzerzertifikats	Zeigt das aktuell verwendete Benutzer-Zertifikat an.
		Fingerabdruck	Prüfsumme des Zertifikats zur Sicherstellung der Integrität
		Erstellen	Erstellt ein neues Zertifikat zur Benutzerauthentifizierung.
		Auswählen	Ermöglicht Ihnen die Auswahl eines vorhandenen Zertifikats aus dem Windows-Zertifikatsspeicher.
		Exportieren	Exportiert das aktuell verwendete Zertifikat.

Die folgende Tabelle zeigt eine Übersicht über die möglichen Einstellungen und die vorhandenen Schaltflächen für die Kommunikationsrolle "Benutzergerät":

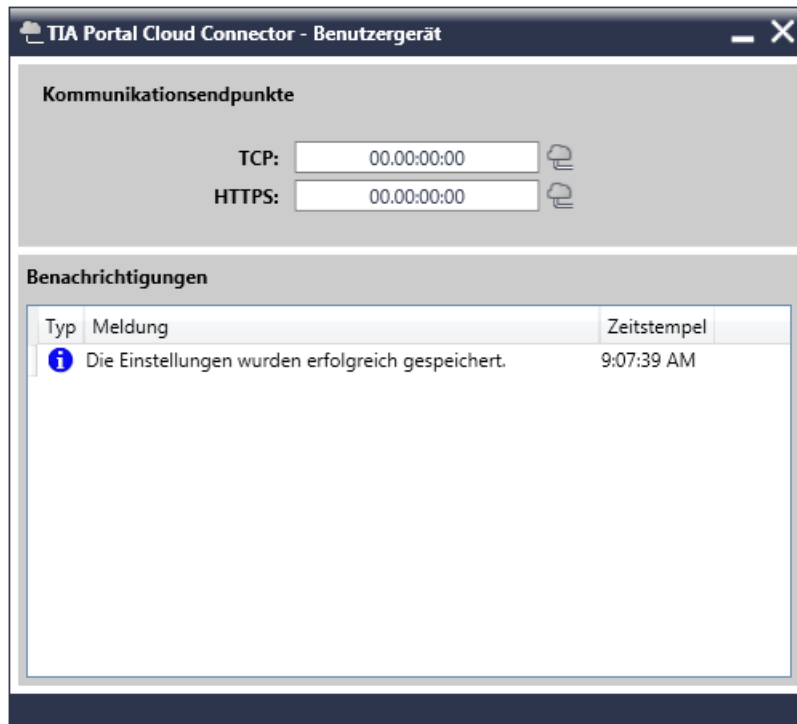
Register	Bereich	Einstellung/Schaltfläche	Beschreibung
Allgemein	Kommunikationsrolle	Benutzergerät	PG/PC, das den physikalischen Kontakt zur SIMATIC Hardware ermöglicht.
		Remotegerät	Virtuelle Maschine im Private Cloud Server, auf dem das TIA Portal installiert ist, welches von einem Benutzergerät aus via Remote Desktop-Verbindung betrieben wird.
	Cloud Connector Kommunikation	Kommunikation aktivieren Kommunikation deaktivieren	Aktiviert bzw. deaktiviert die Kommunikation zu einem PG/PC-Endpunkt.
	Lizenzzugriffe	Aktivieren Deaktivieren	Aktiviert bzw. deaktiviert die Verwendung einer Lizenz vom Benutzergerät.
Protokoll	TCP-Endpunkt	Port	Portnummer, über die die Kommunikation erfolgen soll. Die Portnummer des Benutzergeräts muss mit der Portnummer des Remotegeräts übereinstimmen.
	HTTPS-Endpunkt	Adresse des Benutzergeräts	IP-Adresse oder Name des Benutzergeräts
		Fingerabdruck	Stellt die Integrität des Zertifikats sicher.
		Erstellen	Erstellt ein neues Zertifikat zur Datenverschlüsselung.
		Exportieren	Exportiert das aktuell verwendete Zertifikat.
		Auswählen	Ermöglicht Ihnen die Auswahl eines vorhandenen Zertifikats.
Einstellungen	Autostart	Autostart des Cloud Connectors aktivieren	Aktiviert oder deaktiviert den Autostart für den TIA Portal Cloud Connector beim Systemstart.
	Sprache	Sprache auswählen	Legt die Oberflächensprache für den TIA Portal Cloud Connector fest.
	Benutzer-Authentifizierung	Vertrauenswürdige Benutzerzertifikate	Zeigt die Liste aller verfügbaren und vertrauenswürdigen Benutzer-Zertifikate.
		Importieren	Ermöglicht Ihnen den Import eines Benutzer-Zertifikats, das auf dem Remotegerät erzeugt wurde, in den Windows-Zertifikatsspeicher.
		Hinzufügen	Ermöglicht Ihnen das Hinzufügen eines Zertifikats aus dem Windows-Zertifikatsspeicher zur Liste der vertrauenswürdigen Zertifikate.
		Entfernen	Entfernt das selektierte Zertifikat aus der Liste der vertrauenswürdigen Zertifikate. Im Windows-Zertifikatsspeicher bleibt es aber dennoch erhalten.

TIA Portal Cloud Connector - Statusanzeige

Über die Statusanzeige erhalten Sie Informationen, Warnungen und Fehlermeldungen während der Nutzung des TIA Portal Cloud Connectors. Das folgende Bild zeigt die Statusanzeige in der Kommunikationsrolle "Remotegerät":

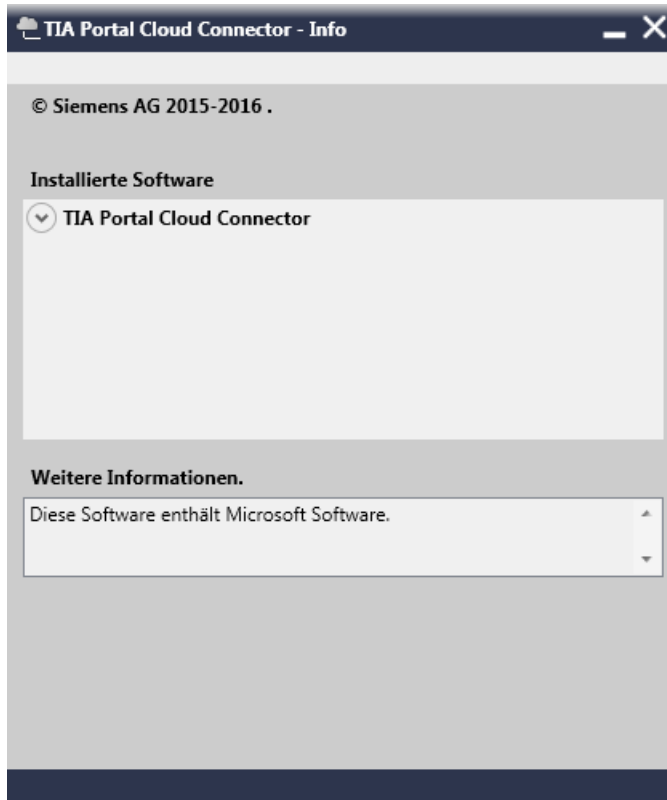


Das folgende Bild zeigt die Statusanzeige in der Kommunikationsrolle "Benutzergerät":



TIA Portal Cloud Connector - Info-Fenster

Im Info-Fenster finden Sie die Information über die installierte Version des TIA Portal Cloud Connectors.



TIA Portal - Anzeige in der Statusleiste

Im TIA Portal werden Sie in der Statusleiste über eine bestehende Online-Verbindung zur SIMATIC Hardware über den TIA Portal Cloud Connector informiert. Zusätzlich zu den Online-Anzeigen wird bei einer Verbindung über den TIA Portal Cloud Connector das folgende Symbol in der Statusleiste angezeigt:



Siehe auch

Grundlagen zum Arbeiten mit dem TIA Portal Cloud Connector (Seite 5)

Anwendungsfälle des TIA Portal Cloud Connectors (Seite 17)

Besonderheiten beim Arbeiten in einer virtuellen Maschine (Seite 19)

Verwendung von Zertifikaten (Seite 20)

Systemvoraussetzungen (Seite 23)

Virtuelle Maschine (VM) bereitstellen (Seite 31)

Virtuelle Maschine (VM) verwenden (Seite 39)

1.4 Anwendungsfälle des TIA Portal Cloud Connectors

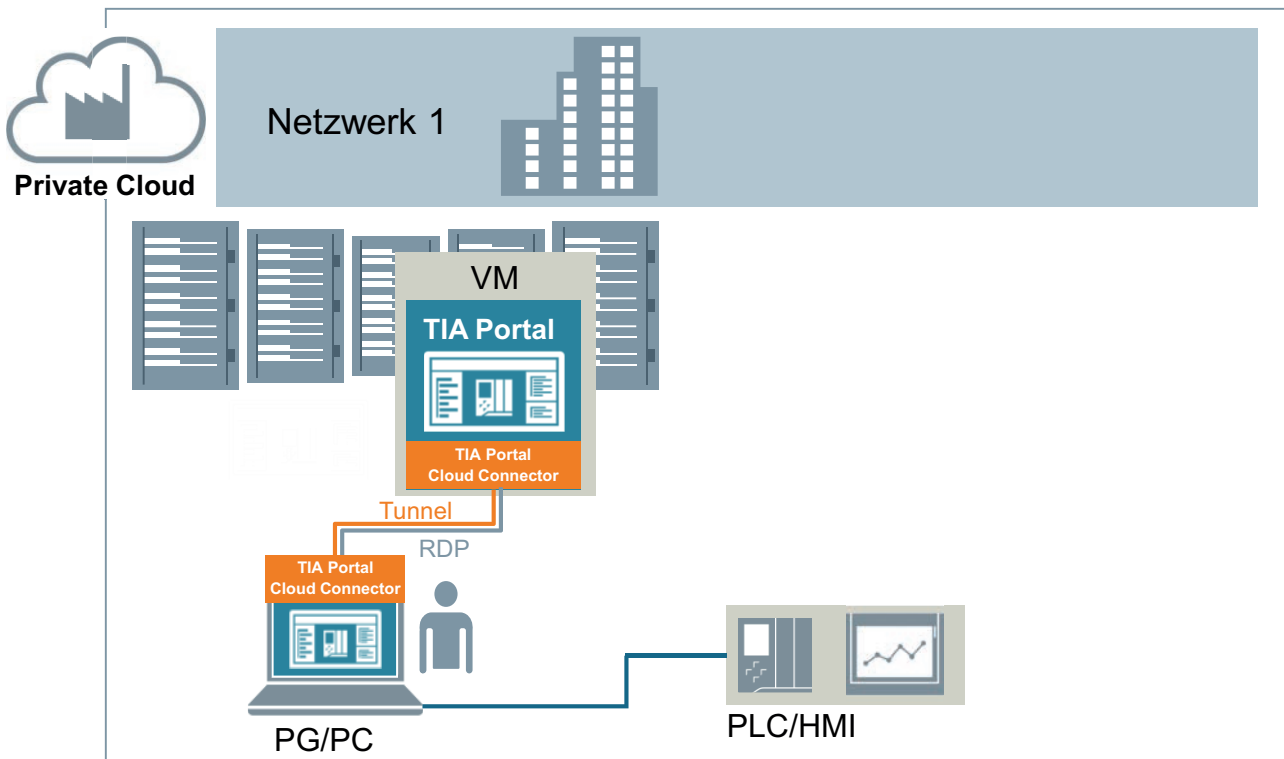
Mit dem TIA Portal Cloud Connector können Sie die folgenden Anwendungsfälle abdecken:

- Zugriff auf Hardware, die am eigenen PG/PC angeschlossen ist.
- Zugriff auf Hardware, die an einem anderen PG/PC angeschlossen ist. Diese kann sich innerhalb oder außerhalb des eigenen Netzwerks befinden.

Zugriff auf Hardware, die am eigenen PG/PC angeschlossen ist

Das TIA Portal wird in der Private Cloud des Unternehmens installiert. Auf dem PG/PC des Anwenders dagegen befindet sich keine Installation des TIA Portals. Die Automatisierungshardware (PLCs/HMIs) ist mit dem PG/PC des Anwenders verbunden. Der TIA Portal Cloud Connector ist sowohl in der VM als auch auf Ihrem PG/PC installiert. Auf dem PG/PC wird eine Lizenz für den TIA Portal Cloud Connector benötigt. Über eine Remote Desktop Verbindung (RDP) melden Sie sich an der VM an und können wie gewohnt mit dem TIA Portal arbeiten. Mithilfe des TIA Portal Cloud Connectors können Sie dabei auf die Hardware zugreifen, die lokal am PG/PC angeschlossen ist.

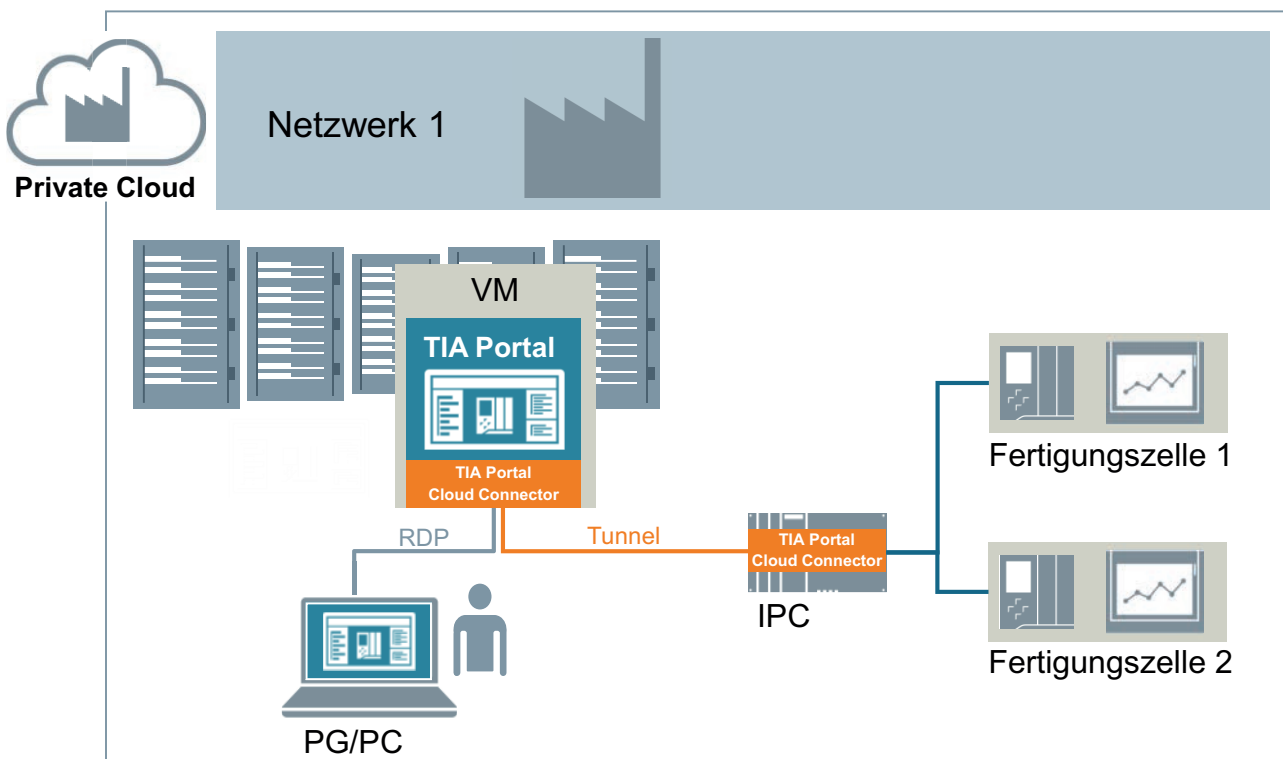
Das folgende Bild zeigt den Einsatz des TIA Portal Cloud Connectors in einer virtuellen Umgebung, wenn die Hardware am eigenen PG/PC angeschlossen ist:

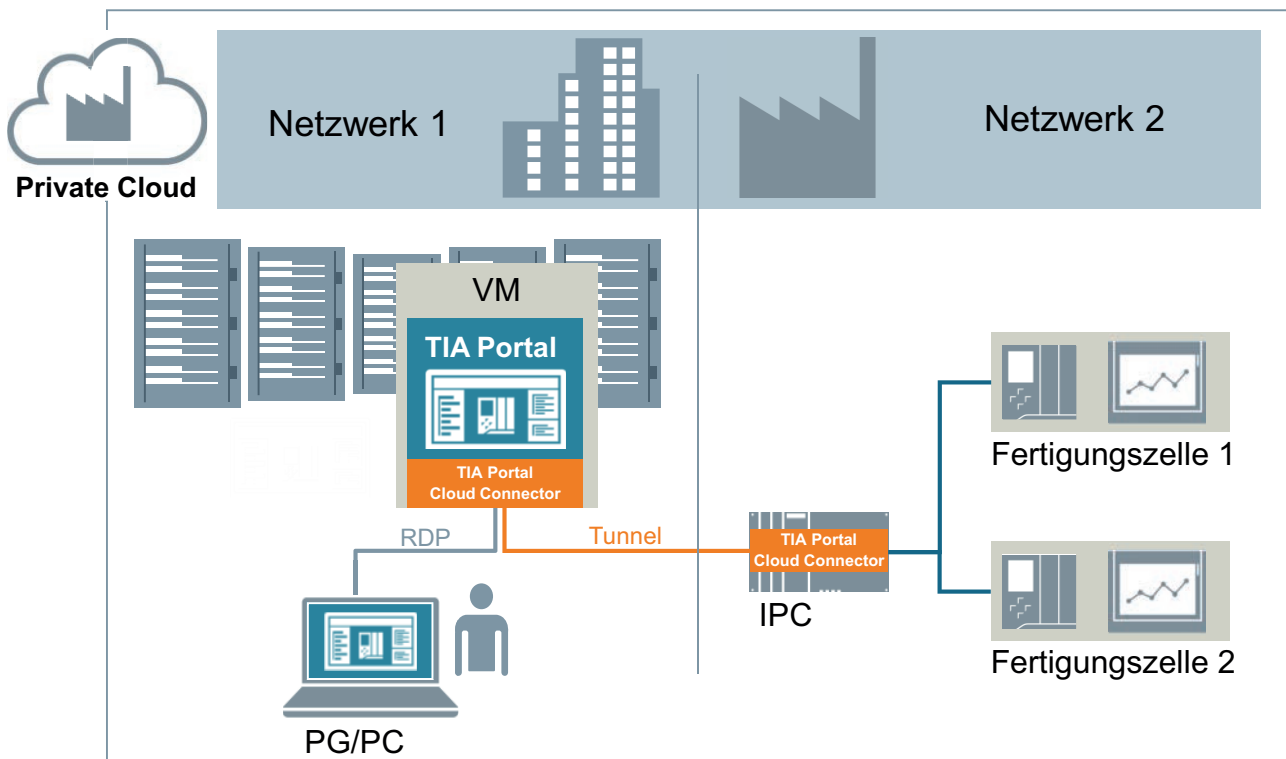


Zugriff auf Hardware, die an einem anderen PG/PC angeschlossen ist

Das TIA Portal wird in einer virtuellen Maschine installiert. Auf Ihrem PG/PC dagegen befindet sich keine Installation des TIA Portals. Die Automatisierungshardware ist mit einem PG/PC, z. B. einem IPC, verbunden, der sich im gleichen (oberes Bild) oder in einem anderen Netzwerk (unteres Bild) wie Ihr eigenes PG/PC befindet. Der TIA Portal Cloud Connector ist auf dem anderen PG/PC und in der VM installiert. Über eine Remote Desktop Verbindung (RDP) melden Sie sich zunächst an der VM an und können wie gewohnt mit dem TIA Portal arbeiten. Mithilfe des TIA Portal Cloud Connectors stellen Sie eine Verbindung zwischen VM und dem anderen PG/PC her und können auf die Automatisierungshardware zugreifen.

Die folgenden Bilder zeigen den Einsatz des TIA Portal Cloud Connectors in einer virtuellen Umgebung, wenn die Hardware an einem anderen PG/PC, im Beispiel ein IPC, angeschlossen ist:





Siehe auch

- Grundlagen zum Arbeiten mit dem TIA Portal Cloud Connector (Seite 5)
- Bedienoberfläche des TIA Portal Cloud Connectors (Seite 7)
- Besonderheiten beim Arbeiten in einer virtuellen Maschine (Seite 19)
- Verwendung von Zertifikaten (Seite 20)
- Systemvoraussetzungen (Seite 23)
- Virtuelle Maschine (VM) bereitstellen (Seite 31)
- Virtuelle Maschine (VM) verwenden (Seite 39)

1.5 Besonderheiten beim Arbeiten in einer virtuellen Maschine

Simulation

Um ein PLC-Programm simulieren zu können, müssen Sie zuvor den TIA Portal Cloud Connector deaktivieren. Für die Simulation von HMI-Geräten ist dies jedoch nicht notwendig.

Umgang mit Updates und Support Packages

Updates und Support Packages können entweder schon in der VM-Vorlage installiert werden oder nachträglich in den einzelnen VMs. Nutzen Sie dazu die Update-Mechanismen des TIA Portals.

Beachten Sie für weitere Informationen das Informationssystem des TIA Portals.

Vergleich zwischen projektierte und tatsächlich vorhandener Topologie

Der Topologievergleich wird durch den TIA Portal Cloud Connector nicht unterstützt.

Siehe auch

Grundlagen zum Arbeiten mit dem TIA Portal Cloud Connector (Seite 5)

Bedienoberfläche des TIA Portal Cloud Connectors (Seite 7)

Anwendungsfälle des TIA Portal Cloud Connectors (Seite 17)

Verwendung von Zertifikaten (Seite 20)

Systemvoraussetzungen (Seite 23)

Virtuelle Maschine (VM) bereitstellen (Seite 31)

Virtuelle Maschine (VM) verwenden (Seite 39)

1.6 Verwendung von Zertifikaten

Verwendung von Zertifikaten im TIA Portal Cloud Connector

Ab Windows 8.1 können Sie HTTPS-Verbindungen zur Kommunikation nutzen. Der TIA Portal Cloud Connector verwendet dabei Zertifikate, um die Sicherheit der HTTPS-Verbindungen zu gewährleisten. Die folgenden Zertifikate sind für das Zustandekommen einer Verbindung zwischen Benutzer- und Remotegerät notwendig:

- Zertifikat zur Datenverschlüsselung
- Zertifikat zur Benutzerauthentifikation

Ist ein Zertifikat nicht vorhanden oder passen die Zertifikate von Benutzer- und Remotegerät nicht zusammen, kann keine Verbindung hergestellt werden.

Zertifikat zur Datenverschlüsselung

Das Zertifikat zur Datenverschlüsselung erzeugen Sie auf dem Benutzergerät. Anschließend muss das Zertifikat auf ein lokales Laufwerk des Remotegeräts kopiert und in den TIA Portal Cloud Connector importiert werden. Passen die Zertifikate zueinander, ist eine Verbindung zwischen den Geräten möglich, sobald auch die Zertifikate zur Benutzerauthentifikation ausgetauscht wurden.

Zertifikat zur Benutzerauthentifikation

Das Zertifikat zur Benutzerauthentifikation erzeugen Sie auf dem Remotegerät. Anschließend muss das Zertifikat auf das Benutzergerät kopiert und in den TIA Portal Cloud Connector importiert werden. Passen die Zertifikate zueinander, ist eine Verbindung zwischen den Geräten möglich, wenn auch die Zertifikate zur Datenverschlüsselung ausgetauscht wurden.

Siehe auch

Grundlagen zum Arbeiten mit dem TIA Portal Cloud Connector (Seite 5)

Bedienoberfläche des TIA Portal Cloud Connectors (Seite 7)

Anwendungsfälle des TIA Portal Cloud Connectors (Seite 17)

Besonderheiten beim Arbeiten in einer virtuellen Maschine (Seite 19)

Zertifikat für die Datenverschlüsselung erstellen (Seite 44)

Zertifikat für die Datenverschlüsselung exportieren (Seite 45)

Zertifikat für die Datenverschlüsselung importieren (Seite 46)

Zertifikat für die Datenverschlüsselung auswählen (Seite 47)

Zertifikat für die Benutzerauthentifikation erstellen (Seite 48)

Zertifikat für die Benutzerauthentifikation exportieren (Seite 49)

Zertifikat für die Benutzerauthentifikation importieren (Seite 50)

Zertifikat für die Benutzerauthentifikation hinzufügen (Seite 51)

Zertifikat für die Benutzerauthentifikation auswählen (Seite 52)

Zertifikat für die Benutzerauthentifikation entfernen (Seite 53)

Systemvoraussetzungen

2.1 Systemvoraussetzungen PG/PC

Unterstützte Betriebssysteme

Um den TIA Portal Cloud Connector einsetzen zu können, muss auf Ihrem PG/PC eines der folgenden Betriebssysteme installiert sein:

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

Hinweis

Beachten Sie die folgenden Hinweise:

- Die Verwendung des TIA Portal Cloud Connectors auf 32-Bit-Betriebssystemen ist nicht möglich.
 - Stellen Sie sicher, dass das Betriebssystem immer auf dem aktuellsten Stand ist. Führen Sie dazu alle wichtigen Windows-Updates zeitnah durch.
 - Wenn SIMATIC NET in einer Version kleiner als 15.0.1 installiert ist, lässt sich der TIA Portal Cloud Connector nicht aktivieren.
 - Damit die Namensauflösung im Netzwerk funktioniert, aktivieren Sie unter Windows in den Netzwerkeinstellungen entweder die Option "Netzwerkerkennung einschalten" oder die Option "Datei- und Druckerfreigabe aktivieren". Alternativ können Sie auch einen externen Namensserver verwenden.
-

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. Für Geräte, die Sie als "Remotegerät" verwenden, ist kein License Key erforderlich.

Sie können den License Key entweder bei der Installation gleich mitinstallieren oder nach der Installation mit dem Automation License Manager übertragen.

Siehe auch

Systemvoraussetzungen VM (Seite 24)

Lizenzen (Seite 27)

2.2 Systemvoraussetzungen VM

Unterstützte Gast-Betriebssysteme und Virtualisierungsplattformen

Sie haben die Möglichkeit, das TIA Portal innerhalb einer Virtuellen Maschine (VM) zu nutzen. Verwenden Sie dazu eine der folgenden Virtualisierungsplattformen in der angegebenen oder einer neueren Version:

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

In der VM können Sie eines oder mehrere der folgenden Softwarepakete installieren:

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

Zusätzlich zu diesen Softwarepaketen können Sie auch weitere STEP 7- und WinCC-Optionspakete installieren.

Hinweis

Betrieb des TIA Portal Cloud Connectors bei einer vorhandenen Installation von SIMATIC NET

Wenn in der VM SIMATIC NET installiert ist, lässt sich der TIA Portal Cloud Connector nicht aktivieren.

Abhängig vom gewählten Softwarepaket werden innerhalb der VM verschiedene Gast-Betriebssysteme unterstützt:

Gast-Betriebssystem	SIMATIC STEP 7 Basic	SIMATIC STEP 7 Professional	SIMATIC WinCC Basic	SIMATIC WinCC Professional	SIMATIC WinCC Advanced
Windows Server 2012 R2 StdE (Vollinstallation) (64 Bit)	X	X	X	X	X
Windows Server 2016 Standard (Vollinstallation) (64 Bit)	X	X	X	X	X
Windows 7 Home Premium SP1 (64 Bit)	X	-	X	-	-
Windows 7 Professional SP1 (64 Bit)	X	X	X	X	X
Windows 7 Enterprise SP1 (64 Bit)	X	X	X	X	X
Windows 7 Ultimate SP1 (64 Bit)	X	X	X	X	X
Windows 10 Home Version 1703 (64 Bit)	X	-	-	X	-
Windows 10 Pro Version 1703 (64 Bit)	X	X	X	X	X
Windows 10 Enterprise Version 1703 (64 Bit)	X	X	X	X	X
Windows 10 Enterprise 2016 LTSC (64 Bit)	X	X	X	X	X
Windows 10 IoT Enterprise 2015 LTSC (64 Bit)	X	X	X	X	X
Windows 10 IoT Enterprise 2016 LTSC (64 Bit)	X	X	X	X	X
- Betriebssystem wird nicht unterstützt					
X Betriebssystem wird unterstützt					

Hinweis

Beachten Sie folgende Hinweise:

- 32-Bit-Betriebssysteme werden nicht unterstützt.
 - Für die Gast-Betriebssysteme gelten dieselben Hardware-Anforderungen wie für die jeweiligen TIA-Produkte selbst.
 - Der SIMATIC USB Prommer wird nicht unterstützt.
 - Wenn Sie innerhalb der VM SD-Karten verwenden möchten, müssen Sie diese zunächst in der VM als Wechseldatenträger einbinden. Zur genauen Vorgehensweise beachten Sie die Hilfe zu Ihrer Virtualisierungsplattform.
 - Stellen Sie sicher, dass das Betriebssystem immer auf dem aktuellsten Stand ist. Führen Sie dazu alle wichtigen Windows-Updates zeitnah durch.
-

Installation des TIA Portal Cloud Connectors

Sie haben zwei Möglichkeiten, den TIA Portal Cloud Connector zu installieren:

- Sie können während der Installation eines der oben genannten SIMATIC Softwarepakete den TIA Portal Cloud Connector als Option aktivieren. Dann wird er zusammen mit dem Softwarepaket installiert.
- Sie können den TIA Portal Cloud Connector unabhängig von einem SIMATIC Softwarepaket installieren. Die Installationsdatei befindet sich auf dem Installationsdatenträger im Ordner "Support". Sie haben die Möglichkeit, diese Installationsdatei in Ihrem Netzwerk zur Verfügung zu stellen. Dadurch können Sie als Administrator der VM auch Skripte erstellen, die einen automatischen Update des TIA Portal Cloud Connectors ermöglichen. Beachten Sie jedoch, dass auf jedem PG/PC eine gültige Lizenz des TIA Portal Cloud Connectors vorhanden sein muss.

Lizenzen für den TIA Portal Cloud Connector

Für das Arbeiten mit dem TIA Portal Cloud Connector in der VM benötigen Sie keine Lizenz des TIA Portal Cloud Connectors, wenn Sie als Kommunikationsrolle "Remotegerät" festlegen.

Siehe auch

Systemvoraussetzungen PG/PC (Seite 23)

Lizenzen (Seite 27)

2.3 Lizenzen

Lizenzierung der SIMATIC-Softwarepakete

Um die einzelnen SIMATIC Softwarepakete des TIA Portals (STEP 7, WinCC) innerhalb einer virtuellen Umgebung zu verwenden, benötigen Sie für jede Installation eine eigene Lizenz. Wird eine VM-Vorlage kopiert oder geklont, ist das ebenfalls eine eigene Installation. Auf dem PG/PC, mit dem auf eine VM zugegriffen wird, muss dagegen keine Lizenz für das TIA Portal vorhanden sein, solange keine lokale Installation vorhanden ist.

Bei Verwendung von Floating License Keys kann die Bereitstellung der Lizenzen über einen License-Key-Server erfolgen.

Lizenzierung des TIA Portal Cloud Connectors

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. Für Geräte, die Sie als "Remotegerät" verwenden, ist kein License Key erforderlich.

Sie können den License Key entweder bei der Installation gleich mitinstallieren oder nach der Installation mit dem Automation License Manager übertragen.

Zugriff auf die Lizenzen des Benutzergeräts durch das Remotegerät

Mithilfe des TIA Portal Cloud Connectors kann das TIA Portal des Remotegeräts auf die Lizenzen des Benutzergeräts zugreifen. Dazu leitet der TIA Portal Cloud Connector die Lizenzanfragen des Remotegeräts durch den Tunnel an das Benutzergerät weiter. Sobald die Weiterleitung des Lizenzzugriffs durch den TIA Portal Cloud Connector aktiviert wurde, werden alle weiteren Lizenzanfragen von anderen Remote-Rechnern durch den ALM abgelehnt. Applikationen, die bereits Lizenzen belegt haben, sind jedoch weiterhin lizenziert. Die Belegung der lokalen Lizenzen durch Applikationen, sowohl auf den Remotegeräten als auch auf den Benutzergeräten, ist möglich.

Siehe auch: Lizenz des Benutzergeräts belegen (Seite 28)

Siehe auch

Systemvoraussetzungen PG/PC (Seite 23)





Systemvoraussetzungen VM (Seite 24)

License-Key-Server nutzen (Seite 34)

2.4 Lizenz des Benutzergeräts belegen

Das TIA Portal, das auf dem Remotegerät installiert ist, kann auf vorhandene Lizenzen des Benutzergeräts zugreifen. Dazu muss sowohl auf dem Benutzergerät als auch auf dem Remotegerät die Nutzung externer Lizenzen aktiviert sein. Die Vorgehensweise bei der Aktivierung der Nutzung von externen Lizenzen ist für das Benutzergerät und das Remotegerät identisch. Ob die Nutzung externer Lizenzen aktiviert ist bzw. ob externe Lizenzen genutzt werden, können Sie an der Farbe des Symbols auf der Schaltfläche "Aktivieren" bzw. "Deaktivieren" erkennen.

Die folgende Tabelle zeigt eine Übersicht über die Symbole und ihre Bedeutungen:

Symbol	Bedeutung
	Die Lizenzbelegung ist deaktiviert.
	Die Lizenzbelegung ist aktiviert, aber es werden aktuell keine Lizenzen durch das Remotegerät auf dem Benutzergerät verwendet.
	Die Lizenzbelegung ist aktiviert und das Remotegerät verwendet Lizenzen des Benutzergeräts.
	Der Datenaustausch zwischen dem TIA Portal und der SIMATIC Automatisierungs-Hardware wurde unterbrochen. Die Statusanzeige wird angezeigt und liefert Ihnen weitere Details zur Ursache.

Sie können die Lizenzbelegung jederzeit wieder deaktivieren.

Nutzung von externen Lizenzen aktivieren

Um den Lizenzzugriff auf das Benutzergerät zu aktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf dem Benutzergerät mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol für den TIA Portal Cloud Connector und wählen Sie den Befehl "Konfiguration".
Der TIA Portal Cloud Connector wird geöffnet.
2. Öffnen Sie das Register "Allgemein".
3. Klicken Sie im Bereich "Lienzzugriffe" auf die Schaltfläche "Aktivieren".
4. Stellen Sie eine Remote-Desktop-Verbindung zur VM her, die Ihr Remotegerät enthält.
5. Klicken Sie auf dem Remotegerät mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol für den TIA Portal Cloud Connector und wählen Sie den Befehl "Konfiguration".
Der TIA Portal Cloud Connector wird geöffnet.
6. Klicken Sie im Bereich "Lienzzugriffe" auf die Schaltfläche "Aktivieren".
Die Verwendung der Lizenzen des Benutzergeräts durch das TIA Portal des Remotegeräts ist nun vorbereitet. Der Text der Schaltfläche "Aktivieren" ändert sich zu "Deaktivieren" und die Farbe des Symbols wechselt zu gelb.

Nutzung von externen Lizenzen deaktivieren

Um den Lizenzzugriff auf das Benutzergerät zu deaktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf dem Benutzergerät mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol für den TIA Portal Cloud Connector und wählen Sie den Befehl "Konfiguration".
Der TIA Portal Cloud Connector wird geöffnet.
2. Öffnen Sie das Register "Allgemein".
3. Klicken Sie im Bereich "Lizenzzugriffe" auf die Schaltfläche "Deaktivieren".
4. Stellen Sie eine Remote-Desktop-Verbindung zur VM her, die Ihr Remotegerät enthält.
5. Klicken Sie auf dem Remotegerät mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol für den TIA Portal Cloud Connector und wählen Sie den Befehl "Konfiguration".
Der TIA Portal Cloud Connector wird geöffnet.
6. Klicken Sie im Bereich "Lizenzzugriffe" auf die Schaltfläche "Deaktivieren".
Die Verwendung der Lizenzen des Benutzergeräts durch das TIA Portal des Remotegeräts ist deaktiviert. Der Text der Schaltfläche "Deaktivieren" ändert sich zu "Aktivieren" und die Farbe des Symbols wechselt zu grau.

Siehe auch

Lizenzen (Seite 27)

License-Key-Server nutzen (Seite 34)

Virtuelle Maschine (VM) bereitstellen

3.1 Neue VM-Vorlage erstellen

Sie haben die Möglichkeit, die folgenden Virtualisierungsplattformen zu nutzen:

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

Abhängig von der verwendeten Virtualisierungsplattform gibt es Unterschiede beim Erzeugen einer Vorlage auf der Basis einer bestehenden Virtuellen Maschine (VM). Weitere Informationen dazu finden Sie in der jeweiligen Hilfe der verwendeten Virtualisierungsplattform.

Richten Sie Ihre SIMATIC Entwicklungsumgebung in der VM genauso wie auf jedem PG/PC ein.

Grundsätzliche Schritte beim Erstellen einer neuen VM-Vorlage

Um eine neue VM-Vorlage zu erstellen, gehen Sie folgendermaßen vor:

1. Erstellen Sie eine VM.
2. Installieren Sie die gewünschte SIMATIC Software, z. B. SIMATIC STEP 7 (TIA Portal ab V14) oder SIMATIC WinCC (TIA Portal ab V14), in der benötigten Edition (Basic, Professional, Comfort/Advanced).

Hinweis

Die Vorgehensweise zur Installation des TIA Portals in einer Virtuellen Maschine (VM) ist identisch zu der Vorgehensweise zur Installation auf einem PG/PC. Detaillierte Hinweise zur Installation finden Sie in der Installationsanleitung des TIA Portals.

3. Installieren Sie bei Bedarf zusätzlich benötigte Optionspakete, z. B. SIMATIC STEP 7 Safety Advanced.
4. Installieren Sie bei Bedarf weitere kompatible Softwarepakete, die allen Anwendern zur Verfügung stehen sollen.
5. Konfigurieren Sie die VM nach Ihren Anforderungen.
6. Erzeugen Sie nach der Anleitung Ihrer Virtualisierungsplattform eine Vorlage aus der VM.

Ergebnis

Sie haben eine VM-Vorlage erstellt, die Sie kopieren und anschließend weitergeben können. Beachten Sie jedoch, dass bei der Verwendung einer Kopie der Vorlage die notwendigen Lizenzen vorhanden sein müssen. Sie können einen separaten Lizenz-Server (VM) verwenden, um Ihre Lizenzen zu verwalten.

Siehe auch

Benutzer- und Projekteinstellungen zentral speichern (Seite 32)

License-Key-Server nutzen (Seite 34)

TIA Portal Cloud Connector in der VM installieren (Seite 35)

3.2 Benutzer- und Projekteinstellungen zentral speichern

Wenn die VM-Benutzer ihre Einstellungen und Projekte innerhalb der VM speichern, gehen diese Einstellungen und Projekte mit dem Löschen der VM verloren. Damit die Einstellungen und Projekte auch in anderen VMs zur Verfügung stehen, müssen sie außerhalb der VM gespeichert werden. Sie können in der VM Umgebungsvariablen mit den Speicherorten für benutzerspezifische Einstellungen und Projekte setzen. Setzen Sie die Umgebungsvariablen bevor Sie das TIA Portal zum ersten Mal starten. Sind die Umgebungsvariablen beim ersten Starten des TIA Portals nicht vorhanden, legt das TIA Portal die Datei für die Einstellungen im Standardverzeichnis ab und verwendet künftig immer diese Datei. Solange diese Datei vorhanden ist, ignoriert das TIA Portal später gesetzte Umgebungsvariablen.

Sie können folgende Pfade über Umgebungsvariablen festlegen:

- Benutzerspezifische Einstellungen: Die Einstellungen werden im angegebenen Verzeichnis gespeichert.
- Projekte: Der angegebene Speicherort wird als Standardpfad beim Anlegen eines neuen Projekts verwendet. Sie können ein Projekt aber auch jederzeit in einem anderen Verzeichnis speichern.

Das Setzen der Umgebungsvariablen kann entweder manuell oder über ein Skript erfolgen. Sie können entweder für das Setzen der Umgebungsvariable für die Einstellungen und die Projekte jeweils ein eigenes Skript erstellen oder beide Umgebungsvariablen mit einem Skript setzen.

Die Datei für die Einstellungen heißt für alle Anwender gleich. Damit jeder Anwender auf seine eigenen Einstellungen zugreifen kann, ist es erforderlich, dass für jeden Anwender ein eigenes Verzeichnis angegeben wird. Ansonsten würden die Einstellungen immer von anderen Anwendern überschrieben werden. Mithilfe einer Variablen kann der Pfad jeweils an den angemeldeten Anwender angepasst werden.

Beispiel für eine Verzeichnisstruktur für das zentrale Speichern der Einstellungen

Die Einstellungen sollen in einem Verzeichnis "UserSettings" gespeichert werden, das im Netzwerk freigegeben ist. Die Struktur unterhalb von "UserSettings" ist folgendermaßen:

```
UserSettings
  User1
  User2
  User3
```

"User1", "User2" und "User3" sind dabei die Benutzernamen der VM-Benutzer. Der Pfad der Umgebungsvariablen ist dann "\\MyServer\UserSettings\%USERNAME%".

"MyServer" ist in diesem Beispiel ein im Netzwerk erreichbarer Rechner. "%USERNAME%" ist die Variable für den Benutzernamen. Diese Variable wird beim Anmelden des Benutzers aufgelöst und die Umgebungsvariable wird entsprechend geändert. Wenn dies für mehrere Anwender erfolgen soll, empfiehlt es sich, das Skript im Autostart-Verzeichnis zu speichern. Dadurch wird die Umgebungsvariable mit jedem Anmelden neu gesetzt und der Speicherort für die Einstellungen wird an den angemeldeten Benutzer angepasst.

Voraussetzung

- Alle Anwender haben Schreibrechte auf den Serverbereichen, die als neue Speicherorte verwendet werden sollen.
- Die Anwenderverzeichnisse sind vorhanden.

Umgebungsvariablen mithilfe eines Skripts setzen

Um die Umgebungsvariablen mithilfe eines Skripts zu setzen, gehen Sie folgendermaßen vor:

1. Erstellen Sie ein neues Skript und öffnen Sie dieses zur Bearbeitung. Alternativ können Sie auch ein bestehendes Skript erweitern.
2. Fügen Sie die folgenden Zeilen in Ihr Skript ein:

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

Ersetzen Sie dabei "<Server>\<Settings>" und "<Server>\<Projects>" durch die Verzeichnisse im Netzwerk, in denen die Einstellungen und Projekte gespeichert werden sollen.
3. Speichern Sie das Skript.
4. Damit das Skript für verschiedene Anwender verwendet werden kann, kopieren Sie es in das Autostart-Verzeichnis von Windows.
Das Auflösen der Variablen "%USERNAME%" erfolgt bei der nächsten Anmeldung am Remotegerät. Dadurch wird der Speicherort für die Einstellungen an den angemeldeten Benutzer angepasst.

Wenn Sie statt einem Skript zwei Skripte verwenden möchten, führen Sie die Schritte 1 bis 4 für jedes Skript einmal aus und fügen Sie immer nur einen der beiden "setx"-Befehle ein.

Umgebungsvariablen manuell setzen

Um die Umgebungsvariablen manuell zu setzen, gehen Sie folgendermaßen vor:

1. Starten Sie die VM, die Sie als Vorlage verteilen möchten.
2. Öffnen Sie in Windows den Dialog für das Setzen der Umgebungsvariablen.
3. Legen Sie eine neue Systemvariable mit dem Namen "TiaUserSettingsPath" an.
4. Geben Sie als Wert den Pfad zu dem Verzeichnis im Netzwerk an, an dem die Anwendereinstellungen gespeichert werden sollen. Beachten Sie, dass Sie den Namen des Anwenders als Variable "%USERNAME%" angeben.
5. Bestätigen Sie Ihre Eingaben mit "OK".
6. Legen Sie eine weitere Systemvariable mit dem Namen "TiaDefaultProjectPath" an.

3.3 License-Key-Server nutzen

7. Geben Sie als Wert den Pfad zu dem Verzeichnis im Netzwerk an, das als Standardspeicherort für Projekte verwendet werden soll. Sie können den Namen des Anwenders als Variable "%USERNAME%" angeben, um die Projekte in Unterverzeichnisse zu speichern. Wenn Sie "%USERNAME%" weglassen, werden alle Projekte im gleichen Verzeichnis gespeichert.
8. Bestätigen Sie Ihre Eingaben mit "OK".
Das Auflösen der Variablen "%USERNAME%" erfolgt bei der nächsten Anmeldung am PG/PC. Dadurch wird der Speicherort für die Einstellungen an den angemeldeten Benutzer angepasst.

Siehe auch

Neue VM-Vorlage erstellen (Seite 31)

License-Key-Server nutzen (Seite 34)

TIA Portal Cloud Connector in der VM installieren (Seite 35)

3.3 License-Key-Server nutzen

Einführung

Bei der Installation des TIA Portals oder des TIA Portal Cloud Connectors wird auch der Automation License Manager (ALM) installiert. Diesen benötigen Sie für den Lizenztransfer und das Lizenzhandling.

Weitere Informationen zum Automation License Manager und zum Einrichten eines Lizenz-Servers finden Sie in der Anwenderdokumentation zum Automation License Manager.

Siehe auch

Lizenzen (Seite 27)

Lizenz des Benutzergeräts belegen (Seite 28)

Neue VM-Vorlage erstellen (Seite 31)

Benutzer- und Projekteinstellungen zentral speichern (Seite 32)

TIA Portal Cloud Connector in der VM installieren (Seite 35)

3.4 TIA Portal Cloud Connector in der VM installieren

Sie können den TIA Portal Cloud Connector auf zwei Arten in der VM installieren:

- Installation des TIA Portal Cloud Connectors zusammen mit dem TIA Portal
Sie haben die Möglichkeit, den TIA Portal Cloud Connector zusammen mit dem TIA Portal zu installieren. Dabei aktivieren Sie die Option "TIA Portal Cloud Connector" während des Installationsvorgangs.
- Installation des TIA Portal Cloud Connectors ohne TIA Portal
Auf dem Installationsdatenträger finden Sie zusätzlich ein Setup-Programm, mit dem Sie den TIA Portal Cloud Connector ohne das TIA Portal installieren können. Diese Installationsdatei können Sie über ein Netzlaufwerk auch anderen Anwendern zugänglich machen.

Cloud Connector zusammen mit dem TIA Portal installieren

Um den Cloud Connector zusammen mit dem TIA Portal zu installieren, gehen Sie folgendermaßen vor:

1. Legen Sie den Installationsdatenträger in das entsprechende Laufwerk ein.
Das Setup-Programm startet automatisch, falls der Autostart auf dem PG/PC nicht deaktiviert ist.
2. Wenn das Setup-Programm nicht automatisch startet, starten Sie es manuell durch Doppelklick auf die Datei "Start.exe".
Der Dialog zur Auswahl der Setup-Sprache wird geöffnet.
3. Wählen Sie die Sprache, in der Sie die Dialoge des Setup-Programms angezeigt bekommen möchten.
4. Um die Produkt- und Installationshinweise zu lesen, klicken Sie auf die Schaltfläche "Hinweise lesen" bzw. "Installationshinweise".
Die entsprechende Hilfedatei mit den Hinweisen wird geöffnet.
5. 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.
6. Wählen Sie die Sprachen für die Produktoberfläche und klicken Sie auf die Schaltfläche "Weiter".

Hinweis

Die Produktsprache "Englisch" wird als Basis immer installiert.

Der Dialog zur Auswahl der Produktkonfiguration wird geöffnet.

7. Klicken Sie auf die Schaltfläche "Benutzerdefiniert".
8. Aktivieren Sie anschließend das Optionskästchen "TIA Portal Cloud Connector" und bei Bedarf die Optionskästchen für weitere Produkte, die Sie installieren möchten.
9. Wenn für das TIA Portal eine Verknüpfung auf dem Desktop angelegt werden soll, aktivieren Sie das Optionskästchen "Desktop-Verknüpfung anlegen".
10. Klicken Sie auf die Schaltfläche "Durchsuchen", wenn Sie das Zielverzeichnis für die Installation ändern möchten. Beachten Sie dabei, dass die Länge des Installationspfades 89 Zeichen nicht überschreiten darf.

3.4 TIA Portal Cloud Connector in der VM installieren

11. Klicken Sie auf die Schaltfläche "Weiter".
Der Dialog zu den Lizenzbedingungen wird geöffnet.
12. Um die Installation fortzusetzen, lesen und akzeptieren Sie alle Lizenzvereinbarungen und 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.
13. 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.
14. Überprüfen Sie die gewählten Installationseinstellungen. 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.
15. 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.

16. 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".
17. Wenn der Computer nicht neu gestartet werden muss, klicken Sie auf die Schaltfläche "Beenden".

Cloud Connector ohne TIA Portal installieren

Um den Cloud Connector ohne das TIA Portal zu installieren, gehen Sie folgendermaßen vor:

1. Legen Sie den Installationsdatenträger in das entsprechende Laufwerk ein oder navigieren Sie im Dateisystem Ihres Rechners zu der Installationsdatei.
Auf dem Installationsdatenträger finden Sie die Installationsdatei im Verzeichnis "Support".
2. Klicken Sie doppelt auf die Installationsdatei "TIA Portal Cloud Connector_<Version>.exe".
Die Windows-Benutzerkontensteuerung wird angezeigt.
3. Bestätigen Sie die Benutzerkontensteuerung mit "Ja".
Der Installationsdialog wird geöffnet.
4. Klicken Sie auf "Weiter".
Eine Auswahl der verfügbaren Setupsprachen wird angezeigt.
5. Wählen Sie die gewünschte Setupsprache und klicken Sie auf "Weiter".
Die benötigten Dateien werden entpackt und der nächste Installationsdialog wird geöffnet.
6. Schließen Sie eventuell noch laufende Programme und klicken Sie auf "Weiter".
Die Lizenzbedingungen werden angezeigt.

7. Akzeptieren Sie die Lizenzbedingungen und klicken Sie auf "Weiter".
Die zur Installation verfügbaren Programme und der benötigte Speicherbedarf werden angezeigt.
8. Klicken Sie auf "Weiter".
Ein Dialog wird geöffnet, in dem eine Übersicht über die Systemeinstellungen angezeigt wird, die während der Installation verändert werden.
9. Aktivieren Sie das Optionskästchen, um die Änderungen zu akzeptieren.
10. Klicken Sie auf "Weiter".
Eine Übersicht über die zu installierenden Programme wird angezeigt.
11. Klicken Sie auf "Installieren".
Die Installation wird gestartet.
12. Möglicherweise muss der Computer neu gestartet werden. Aktivieren Sie dann das Optionsfeld "Ja, Computer jetzt neu starten". Klicken Sie anschließend auf die Schaltfläche "Beenden".

Siehe auch

Neue VM-Vorlage erstellen (Seite 31)

Benutzer- und Projekteinstellungen zentral speichern (Seite 32)

License-Key-Server nutzen (Seite 34)

Virtuelle Maschine (VM) verwenden

4.1 TIA Portal Cloud Connector auf dem PG/PC installieren

Hinweis

Beachten Sie folgende Hinweise:

- Sie benötigen eine gültige Lizenz für den TIA Portal Cloud Connector.
 - Einstellungen in der Windows-Firewall: Voraussetzung für eine eingehende Verbindung ist, dass in Ihrer Firewall im Register "Ausnahmen" beim Service "Siemens SCP Remote Connection" der im TIA Portal Cloud Connector verwendete Port eingetragen ist. Voreingestellt ist "Beliebig".
-

Vorgehen

Um den TIA Portal Cloud Connector zu installieren, gehen Sie folgendermaßen vor:

1. Legen Sie den Installationsdatenträger in das entsprechende Laufwerk ein oder navigieren Sie im Dateisystem Ihres Rechners zu der Installationsdatei.
Auf dem Installationsdatenträger finden Sie die Installationsdatei im Verzeichnis "Support".
2. Klicken Sie doppelt auf die Installationsdatei "TIA Portal Cloud Connector_<Version>.exe".
Die Windows-Benutzerkontensteuerung wird angezeigt.
3. Bestätigen Sie die Benutzerkontensteuerung mit "Ja".
Der Installationsdialog wird geöffnet.
4. Klicken Sie auf "Weiter".
Eine Auswahl der verfügbaren Setupsprachen wird angezeigt.
5. Wählen Sie die gewünschte Setupsprache und klicken Sie auf "Weiter".
Die benötigten Dateien werden entpackt und der nächste Installationsdialog wird geöffnet.
6. Schließen Sie eventuell noch laufende Programme und klicken Sie auf "Weiter".
Die Lizenzbedingungen werden angezeigt.
7. Akzeptieren Sie die Lizenzbedingungen und klicken Sie auf "Weiter".
Die zur Installation verfügbaren Programme und der benötigte Speicherbedarf werden angezeigt.
8. Klicken Sie auf "Weiter".
Ein Dialog wird geöffnet, in dem eine Übersicht über die Systemeinstellungen angezeigt wird, die während der Installation verändert werden.
9. Aktivieren Sie das Optionskästchen, um die Änderungen zu akzeptieren.
10. Klicken Sie auf "Weiter".
Eine Übersicht über die zu installierenden Programme wird angezeigt.

4.2 TIA Portal Cloud Connector am PG/PC konfigurieren

11. Klicken Sie auf "Installieren".
Die Installation wird gestartet.
12. Möglicherweise muss der Computer neu gestartet werden. Aktivieren Sie dann das Optionsfeld "Ja, Computer jetzt neu starten". Klicken Sie anschließend auf die Schaltfläche "Beenden".

Siehe auch

- TIA Portal Cloud Connector am PG/PC konfigurieren (Seite 40)
- TIA Portal Cloud Connector in der VM konfigurieren (Seite 42)
- Online-Verbindung über den TIA Portal Cloud Connector (Seite 54)
- Virtuelle Maschine (VM) offline verwenden (Seite 55)

4.2 TIA Portal Cloud Connector am PG/PC konfigurieren

Hinweis

Kommunikationsprotokoll

Damit Ihr PG/PC eine Verbindung zur VM herstellen kann, müssen Sie ein Kommunikationsprotokoll festlegen. Ab Windows 8.1 sollten Sie aus Sicherheitsgründen immer HTTPS verwenden.

TCP-Verbindung konfigurieren

Um für das PG/PC eine TCP-Verbindung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol für den TIA Portal Cloud Connector und wählen Sie den Befehl "Konfiguration".
Der TIA Portal Cloud Connector wird geöffnet.
2. Öffnen Sie das Register "Einstellungen" und wechseln Sie bei Bedarf die Oberflächensprache des TIA Portal Cloud Connectors.
3. Wechseln Sie in das Register "Allgemein" und prüfen Sie die Kommunikationsrolle. Stellen Sie ggf. die Einstellung auf "Benutzergerät" um.
4. Wechseln Sie in das Register "Protokoll".
5. Aktivieren Sie das Optionskästchen "TCP-Endpunkt".
6. Geben Sie den Port an, über den die Kommunikation erfolgen soll. Der Port muss identisch sein mit dem, der am Remotegerät vergeben wurde.
7. Öffnen Sie das Register "Allgemein" erneut.
8. Klicken Sie im Bereich "Cloud Connector Kommunikation" auf die Schaltfläche "Kommunikation aktivieren".

HTTPS-Verbindung konfigurieren

Um für das PG/PC eine HTTPS-Verbindung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol für den TIA Portal Cloud Connector und wählen Sie den Befehl "Konfiguration".
Der TIA Portal Cloud Connector wird geöffnet.
2. Öffnen Sie das Register "Einstellungen" und wechseln Sie bei Bedarf die Oberflächensprache des TIA Portal Cloud Connectors.
3. Wechseln Sie in das Register "Allgemein" und prüfen Sie die Kommunikationsrolle. Stellen Sie ggf. die Einstellung auf "Benutzergerät" um.
4. Wechseln Sie in das Register "Protokoll".
5. Aktivieren Sie das Optionskästchen "HTTPS-Endpunkt".
6. Erstellen Sie entweder ein neues Zertifikat zur Datenverschlüsselung oder wählen Sie ein bereits vorhandenes Zertifikat aus dem Windows-Zertifikatsspeicher.
Siehe auch:
Zertifikat für die Datenverschlüsselung erstellen (Seite 44)
Zertifikat für die Datenverschlüsselung auswählen (Seite 47)
7. Falls Sie noch kein Zertifikat für die Benutzerauthentifikation auf dem Benutzergerät zur Verfügung haben, erstellen Sie es im Remotegerät und kopieren Sie es auf ein lokales Laufwerk des Benutzergeräts.
Siehe auch:
Zertifikat für die Benutzerauthentifikation erstellen (Seite 48)
8. Wechseln Sie in das Register "Einstellungen".
9. Importieren Sie ein neues Zertifikat für die Benutzerauthentifikation oder fügen Sie ein vorhandenes Zertifikat aus dem Windows-Zertifikatsspeicher der Liste der vertrauenswürdigen Zertifikate hinzu.
Siehe auch:
Zertifikat für die Benutzerauthentifikation importieren (Seite 50)
Zertifikat für die Benutzerauthentifikation hinzufügen (Seite 51)
10. Öffnen Sie das Register "Allgemein" erneut.
11. Klicken Sie im Bereich "Cloud Connector Kommunikation" auf die Schaltfläche "Kommunikation aktivieren".

Ergebnis

Ihr PG/PC ist nun für die Kommunikation mit der VM vorbereitet. Konfigurieren Sie als nächstes den TIA Portal Cloud Connector in der VM.

Siehe auch

- TIA Portal Cloud Connector auf dem PG/PC installieren (Seite 39)
- TIA Portal Cloud Connector in der VM konfigurieren (Seite 42)

Online-Verbindung über den TIA Portal Cloud Connector (Seite 54)

Virtuelle Maschine (VM) offline verwenden (Seite 55)

4.3 TIA Portal Cloud Connector in der VM konfigurieren

Hinweis

Kommunikationsprotokoll

Damit ein PG/PC eine Verbindung zur VM herstellen kann, müssen Sie das zu verwendende Kommunikationsprotokoll festlegen. Ab Windows 8.1 sollten Sie aus Sicherheitsgründen immer HTTPS verwenden. Überprüfen Sie zusätzlich die Identität des anfragenden Verbindungspartners, bevor Sie eine Verbindung akzeptieren.

TCP-Verbindung konfigurieren

Um für die VM eine TCP-Verbindung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Stellen Sie eine Remote-Desktop-Verbindung zur VM her.
2. Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol für den TIA Portal Cloud Connector und wählen Sie den Befehl "Konfiguration".
Der TIA Portal Cloud Connector wird geöffnet.
3. Öffnen Sie das Register "Einstellungen" und wechseln Sie bei Bedarf die Oberflächensprache des TIA Portal Cloud Connectors.
4. Wechseln Sie in das Register "Allgemein" und prüfen Sie die Kommunikationsrolle. Stellen Sie ggf. die Einstellung auf "Remotegerät" um.
5. Öffnen Sie das Register "Protokoll".
6. Aktivieren Sie im Bereich "Kommunikationsprotokoll" das Optionsfeld "TCP-Einstellungen".
7. Wählen Sie ein Zielgerät aus.

Hinweis

Verbindung zum SCALANCE

Stellen Sie sicher, dass die Verbindung zum SCALANCE mit SINEMA RC oder einer anderen Verschlüsselungstechnologie abgesichert ist. Ansonsten erfolgt die Datenübertragung unverschlüsselt.

8. Geben Sie die IP-Adresse des Benutzergeräts an oder wählen Sie in der Klappliste den Eintrag "Automatische Konfiguration", um die Adresse automatisch ermitteln zu lassen.
9. Geben Sie den Port an, über den die Kommunikation erfolgen soll. Der Port muss identisch sein mit dem, der am Benutzergerät vergeben wurde.
10. Öffnen Sie das Register "Allgemein" erneut.
11. Klicken Sie im Bereich "Cloud Connector Kommunikation" auf die Schaltfläche "Kommunikation aktivieren".

HTTPS-Verbindung konfigurieren

Um für die VM eine HTTPS-Verbindung zu konfigurieren, gehen Sie folgendermaßen vor:

1. Stellen Sie eine Remote-Desktop-Verbindung zur VM her.
2. Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol für den TIA Portal Cloud Connector und wählen Sie den Befehl "Konfiguration". Der TIA Portal Cloud Connector wird geöffnet.
3. Öffnen Sie das Register "Einstellungen" und wechseln Sie bei Bedarf die Oberflächensprache des TIA Portal Cloud Connectors.
4. Öffnen Sie das Register "Allgemein" und prüfen Sie die Kommunikationsrolle. Stellen Sie ggf. die Einstellung auf "Remotegerät" um.
5. Öffnen Sie das Register "Protokoll".
6. Aktivieren Sie im Bereich "Kommunikationsprotokoll" das Optionsfeld "HTTPS-Einstellungen".
7. Geben Sie die IP-Adresse des Benutzergeräts an oder wählen Sie in der Klappliste den Eintrag "Automatische Konfiguration", um die Adresse automatisch ermitteln zu lassen.
8. Importieren Sie entweder das Zertifikat zur Datenverschlüsselung, das Sie am Benutzergerät erstellt haben, oder wählen Sie ein bereits vorhandenes Zertifikat aus dem Windows-Zertifikatsspeicher.
Siehe auch:
Zertifikat für die Datenverschlüsselung importieren (Seite 46)
Zertifikat für die Datenverschlüsselung auswählen (Seite 47)
9. Wechseln Sie in das Register "Einstellungen".
10. Erstellen Sie entweder ein neues Zertifikat zur Benutzerauthentifikation oder wählen Sie ein bereits vorhandenes Zertifikat aus dem Windows-Zertifikatsspeicher.
Siehe auch:
Zertifikat für die Benutzerauthentifikation erstellen (Seite 48)
Zertifikat für die Benutzerauthentifikation auswählen (Seite 52)
11. Öffnen Sie das Register "Allgemein" erneut.
12. Klicken Sie im Bereich "Cloud Connector Kommunikation" auf die Schaltfläche "Kommunikation aktivieren".

Ergebnis

Der TIA Portal Cloud Connector ist für die Kommunikation vorbereitet. Nach dem Aktivieren beider Kommunikationspartner können Sie vom Benutzergerät auf die an diesem lokal angeschlossene SIMATIC Hardware (PLCs/HMIs) zugreifen.

Siehe auch

- TIA Portal Cloud Connector auf dem PG/PC installieren (Seite 39)
- TIA Portal Cloud Connector am PG/PC konfigurieren (Seite 40)
- Online-Verbindung über den TIA Portal Cloud Connector (Seite 54)
- Virtuelle Maschine (VM) offline verwenden (Seite 55)

4.4 Zertifikate verwenden (nur für HTTPS-Verbindungen)

4.4.1 Zertifikat für die Datenverschlüsselung erstellen

Ab Windows 8.1 können Sie eine HTTPS-Verbindung zur Kommunikation nutzen. Um die Sicherheit zu erhöhen, ist ein Zertifikat für die Datenverschlüsselung notwendig, das am Benutzergerät erstellt und dann vom Remotegerät verwendet wird.

Vorgehen

Um ein Zertifikat für die Datenverschlüsselung zu erstellen, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie am Benutzergerät im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Benutzergerät)". Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionskästchen "HTTPS-Endpunkt". Die Schaltflächen "Erstellen" und "Auswählen" werden aktiv.
5. Klicken Sie auf "Erstellen". Der Dialog "TIA Portal Cloud Connector - Zertifikat erstellen" wird geöffnet.
6. Geben Sie einen Domännennamen ein oder wählen Sie die Domäne aus der Klappliste aus.

Hinweis

Über die Schaltfläche "+" können Sie die Domäne in die Domänenliste übernehmen. Mit der Schaltfläche "-" können Sie eine Domäne wieder aus der Domänenliste entfernen.

7. Klicken Sie auf "Durchsuchen". Der Dialog "Speichern unter" wird geöffnet.
8. Wählen Sie einen Speicherort und geben Sie einen Dateinamen für das Zertifikat ein.
9. Klicken Sie auf "Speichern".
10. Wählen Sie das Datum, ab dem das Zertifikat gültig sein soll.
11. Wählen Sie das Datum, bis zu dem das Zertifikat gültig sein soll.
12. Klicken Sie auf "OK".

Ergebnis

Das Zertifikat wird erstellt und für den HTTPS-Endpunkt am Benutzergerät verwendet. Zusätzlich wird es am angegebenen Speicherort als Datei mit der Dateinamenserweiterung ".cer" gespeichert und kann von dort aus auf das Remotegerät kopiert werden. Das Zertifikat wurde zudem dem Windows-Zertifikatsspeicher hinzugefügt.

Siehe auch

- Verwendung von Zertifikaten (Seite 20)
- Zertifikat für die Datenverschlüsselung exportieren (Seite 45)
- Zertifikat für die Datenverschlüsselung importieren (Seite 46)
- Zertifikat für die Datenverschlüsselung auswählen (Seite 47)

4.4.2 Zertifikat für die Datenverschlüsselung exportieren

Sie können das aktuell verwendete Zertifikat für die Datenverschlüsselung jederzeit exportieren.

Voraussetzung

Das Zertifikat für die Datenverschlüsselung wurde zuvor erstellt und wird unter dem HTTPS-Endpunkt des Benutzergeräts angezeigt.

Vorgehen

Um ein Zertifikat für die Datenverschlüsselung zu exportieren, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie am Benutzergerät im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Benutzergerät)". Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionskästchen "HTTPS-Endpunkt". Die Schaltflächen "Erstellen", "Auswählen" und "Exportieren" werden aktiv.
5. Klicken Sie auf "Exportieren". Der Dialog "Speichern unter" wird geöffnet.
6. Wählen Sie einen Speicherort und geben Sie einen Namen für das Zertifikat ein.
7. Klicken Sie auf "Speichern".

Ergebnis

Das aktuell verwendete Zertifikat für die Datenverschlüsselung wird am angegebenen Speicherort als Datei mit der Dateinamenserweiterung ".cer" gespeichert.

Siehe auch

- Verwendung von Zertifikaten (Seite 20)
- Zertifikat für die Datenverschlüsselung erstellen (Seite 44)

4.4 Zertifikate verwenden (nur für HTTPS-Verbindungen)

Zertifikat für die Datenverschlüsselung importieren (Seite 46)

Zertifikat für die Datenverschlüsselung auswählen (Seite 47)

4.4.3 Zertifikat für die Datenverschlüsselung importieren

Damit Sie eine HTTPS-Verbindung zwischen Benutzer- und Remotegerät herstellen können, ist es notwendig, das am Benutzergerät erstellte Zertifikat für die Datenverschlüsselung in den TIA Portal Cloud Connector des Remotegeräts zu importieren.

Voraussetzung

- Das Zertifikat für die Datenverschlüsselung wurde am Benutzergerät erstellt.
- Das Zertifikat für die Datenverschlüsselung wurde auf ein lokales Laufwerk des Remotegeräts kopiert.

Vorgehen

Um ein Zertifikat für die Datenverschlüsselung in den TIA Portal Cloud Connector des Remotegeräts zu importieren, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie am Remotegerät im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Remotegerät)". Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionsfeld "HTTPS-Einstellungen". Die Schaltflächen "Importieren" und "Auswählen" werden aktiv.
5. Klicken Sie auf "Importieren". Der Dialog "Öffnen" wird geöffnet.
6. Wählen Sie die Zertifikatsdatei im Dateisystem. Zertifikatsdateien erkennen Sie an der Dateinamenserweiterung ".cer".
7. Klicken Sie auf "Öffnen".

Ergebnis

Das Zertifikat wird importiert und ab sofort für die Kommunikation verwendet. Das Zertifikat wurde zudem dem Windows-Zertifikatsspeicher hinzugefügt.

Siehe auch

Verwendung von Zertifikaten (Seite 20)

Zertifikat für die Datenverschlüsselung erstellen (Seite 44)

Zertifikat für die Datenverschlüsselung exportieren (Seite 45)

Zertifikat für die Datenverschlüsselung auswählen (Seite 47)

4.4.4 Zertifikat für die Datenverschlüsselung auswählen

Sie können aus dem Windows-Zertifikatsspeicher ein Zertifikat für die Datenverschlüsselung auswählen. Dies ist sowohl am Benutzer- als auch am Remotegerät möglich.

Voraussetzung

Das Zertifikat für die Datenverschlüsselung wurde zuvor erstellt (Benutzergerät) oder importiert (Remotegerät) und ist im Windows-Zertifikatsspeicher verfügbar.

Vorgehen

Um ein vorhandenes Zertifikat für die Datenverschlüsselung aus dem Windows-Zertifikatsspeicher auszuwählen und zu verwenden, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Benutzergerät)" oder "Konfiguration (Remotegerät)".
Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionskästchen "HTTPS-Endpunkt" (Benutzergerät) oder das Optionsfeld "HTTPS-Einstellungen" (Remotegerät).
Die Schaltfläche "Auswählen" wird aktiv.
5. Klicken Sie auf "Auswählen".
Der Dialog "Windows Sicherheit" wird geöffnet und die verfügbaren Zertifikate werden angezeigt.
6. Wählen Sie ein Zertifikat aus. Bei Bedarf können Sie sich weitere Eigenschaften des Zertifikats anzeigen lassen.
7. Klicken Sie auf "OK".

Ergebnis

Das gewählte Zertifikat wird für die Kommunikation verwendet. Damit eine Kommunikation möglich ist, muss am Benutzer- und am Remotegerät das gleiche Zertifikat eingestellt sein.

Siehe auch

Verwendung von Zertifikaten (Seite 20)

Zertifikat für die Datenverschlüsselung erstellen (Seite 44)

Zertifikat für die Datenverschlüsselung exportieren (Seite 45)

Zertifikat für die Datenverschlüsselung importieren (Seite 46)

4.4.5 Zertifikat für die Benutzerauthentifikation erstellen

Ab Windows 8.1 können Sie eine HTTPS-Verbindung zur Kommunikation nutzen. Um die Sicherheit zu erhöhen, ist ein Zertifikat für die Benutzerauthentifikation notwendig, das am Remotegerät erstellt und dann vom Benutzergerät verwendet wird.

Vorgehen

Um ein Zertifikat für die Benutzerauthentifikation zu erstellen, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie am Remotegerät im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Remotegerät)".
Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionsfeld "HTTPS-Einstellungen".
Im Register "Einstellungen" wird der Bereich zur Benutzerauthentifikation aktiv.
5. Wechseln Sie in das Register "Einstellungen".
6. Klicken Sie im Bereich "Benutzer-Authentifizierung" auf die Schaltfläche "Erstellen".
Der Dialog "TIA Portal Cloud Connector - Benutzerauthentifizierung" wird geöffnet.
7. Geben Sie in das Feld "Zertifikatname" einen Namen für das neue Zertifikat ein.
8. Klicken Sie auf "Durchsuchen".
Der Dialog "Speichern unter" wird geöffnet.
9. Wählen Sie einen Speicherort und geben Sie einen Dateinamen für das Zertifikat ein.
10. Klicken Sie auf "Speichern".
11. Wählen Sie das Datum, ab dem das Zertifikat gültig sein soll.
12. Wählen Sie das Datum, bis zu dem das Zertifikat gültig sein soll.
13. Klicken Sie auf "OK".

Ergebnis

Das Zertifikat wird erstellt und am Remotegerät verwendet. Zusätzlich wird es am angegebenen Speicherort als Datei mit der Dateinamenserweiterung ".cer" gespeichert und kann von dort aus auf das Benutzergerät kopiert werden. Das Zertifikat wurde zudem dem Windows-Zertifikatsspeicher hinzugefügt.

Siehe auch

- Verwendung von Zertifikaten (Seite 20)
- Zertifikat für die Benutzerauthentifikation exportieren (Seite 49)
- Zertifikat für die Benutzerauthentifikation importieren (Seite 50)
- Zertifikat für die Benutzerauthentifikation hinzufügen (Seite 51)
- Zertifikat für die Benutzerauthentifikation auswählen (Seite 52)
- Zertifikat für die Benutzerauthentifikation entfernen (Seite 53)

4.4.6 Zertifikat für die Benutzerauthentifikation exportieren

Beim Erstellen des Zertifikats für die Benutzerauthentifikation ist es notwendig, das Zertifikat zu exportieren, um es einem Benutzergerät zur Verfügung zu stellen. Sie können das aktuell verwendete Zertifikat jederzeit erneut exportieren.

Voraussetzung

Das Zertifikat für die Benutzerauthentifikation wurde zuvor auf dem Remotegerät erstellt und wird im Register "Einstellungen" unter "Benutzer-Authentifizierung" angezeigt.

Vorgehen

Um ein Zertifikat für die Benutzerauthentifikation zu exportieren, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie am Remotegerät im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Remotegerät)". Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionsfeld "HTTPS-Einstellungen". Im Register "Einstellungen" wird der Bereich zur Benutzerauthentifikation aktiv.
5. Wechseln Sie in das Register "Einstellungen".
6. Klicken Sie im Bereich "Benutzer-Authentifizierung" auf die Schaltfläche "Exportieren". Der Dialog "Speichern unter" wird geöffnet.
7. Wählen Sie einen Speicherort und geben Sie einen Namen für das Zertifikat ein.
8. Klicken Sie auf "Speichern".

Ergebnis

Das aktuell verwendete Zertifikat für die Benutzerauthentifikation wird am angegebenen Speicherort als Datei mit der Dateinamenserweiterung ".cer" gespeichert.

Siehe auch

- Verwendung von Zertifikaten (Seite 20)
- Zertifikat für die Benutzerauthentifikation erstellen (Seite 48)
- Zertifikat für die Benutzerauthentifikation importieren (Seite 50)
- Zertifikat für die Benutzerauthentifikation hinzufügen (Seite 51)
- Zertifikat für die Benutzerauthentifikation auswählen (Seite 52)
- Zertifikat für die Benutzerauthentifikation entfernen (Seite 53)

4.4.7 Zertifikat für die Benutzerauthentifikation importieren

Damit Sie eine HTTPS-Verbindung zwischen Benutzer- und Remotegerät herstellen können, ist es notwendig, das am Remotegerät erstellte Zertifikat für die Benutzerauthentifikation in den TIA Portal Cloud Connector des Benutzergeräts zu importieren.

Voraussetzung

- Das Zertifikat für die Benutzerauthentifikation wurde am Remotegerät erstellt.
- Das Zertifikat für die Benutzerauthentifikation wurde auf ein lokales Laufwerk des Benutzergeräts kopiert.

Vorgehen

Um ein Zertifikat für die Benutzerauthentifikation zu importieren, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie am Benutzergerät im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Benutzergerät)". Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionskästchen "HTTPS-Endpunkt". Im Register "Einstellungen" wird der Bereich zur Benutzerauthentifikation aktiv.
5. Wechseln Sie in das Register "Einstellungen".
6. Klicken Sie im Bereich "Benutzer-Authentifizierung" auf die Schaltfläche "Importieren". Der Dialog "Öffnen" wird geöffnet.
7. Wählen Sie die Zertifikatsdatei im Dateisystem. Zertifikatsdateien erkennen Sie an der Dateinamenserweiterung ".cer".
8. Klicken Sie auf "Öffnen".

Ergebnis

Das Zertifikat wird importiert und der Liste der vertrauenswürdigen Zertifikaten hinzugefügt. Über diese Liste können Sie festlegen, mit welchen Remotegeräten das Benutzergerät kommunizieren darf. Das jeweils angesprochene Remotegerät muss das gleiche Zertifikat für die Benutzerauthentifikation bei sich eingebunden haben.

Siehe auch

Verwendung von Zertifikaten (Seite 20)

Zertifikat für die Benutzerauthentifikation erstellen (Seite 48)

Zertifikat für die Benutzerauthentifikation exportieren (Seite 49)

Zertifikat für die Benutzerauthentifikation hinzufügen (Seite 51)

Zertifikat für die Benutzerauthentifikation auswählen (Seite 52)

Zertifikat für die Benutzerauthentifikation entfernen (Seite 53)

4.4.8 Zertifikat für die Benutzerauthentifikation hinzufügen

Statt ein Zertifikat aus dem Dateisystem zu importieren, können Sie es auch aus dem Windows-Zertifikatsspeicher der Liste der vertrauenswürdigen Zertifikate hinzufügen.

Voraussetzung

Das gewünschte Zertifikat ist im Windows-Zertifikatsspeicher verfügbar.

Vorgehen

Um ein Zertifikat für die Benutzerauthentifikation aus dem Windows-Zertifikatsspeicher hinzuzufügen, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie am Benutzergerät im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Benutzergerät)". Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionskästchen "HTTPS-Endpunkt". Im Register "Einstellungen" wird der Bereich zur Benutzerauthentifikation aktiv.
5. Wechseln Sie in das Register "Einstellungen".
6. Klicken Sie im Bereich "Benutzer-Authentifizierung" auf die Schaltfläche "Hinzufügen". Der Dialog "Zertifikat auswählen" wird geöffnet und die verfügbaren Zertifikate werden angezeigt.
7. Wählen Sie ein Zertifikat aus. Bei Bedarf können Sie sich das Zertifikat anzeigen lassen.
8. Klicken Sie auf "OK".

Ergebnis

Das Zertifikat aus dem Windows-Zertifikatsspeicher wird der Liste der vertrauenswürdigen Zertifikate hinzugefügt. Über diese Liste können Sie festlegen, mit welchen Remotegeräten das Benutzergerät kommunizieren darf. Das jeweils angesprochene Remotegerät muss das gleiche Zertifikat für die Benutzerauthentifikation bei sich eingebunden haben.

Siehe auch

Verwendung von Zertifikaten (Seite 20)

Zertifikat für die Benutzerauthentifikation erstellen (Seite 48)

Zertifikat für die Benutzerauthentifikation exportieren (Seite 49)

Zertifikat für die Benutzerauthentifikation importieren (Seite 50)

Zertifikat für die Benutzerauthentifikation auswählen (Seite 52)

Zertifikat für die Benutzerauthentifikation entfernen (Seite 53)

4.4.9 Zertifikat für die Benutzerauthentifikation auswählen

Statt am Remotegerät ein neues Zertifikat für die Benutzerauthentifikation zu erstellen, können Sie auch ein bestehendes Zertifikat aus dem Windows-Zertifikatsspeicher auswählen und verwenden.

Voraussetzung

Das Zertifikat für die Benutzerauthentifikation wurde zuvor erstellt und ist im Windows-Zertifikatsspeicher verfügbar.

Vorgehen

Um ein Zertifikat für die Benutzerauthentifikation aus dem Windows-Zertifikatsspeicher auszuwählen, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie am Remotegerät im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Remotegerät)". Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionsfeld "HTTPS-Einstellungen". Im Register "Einstellungen" wird der Bereich zur Benutzerauthentifikation aktiv.
5. Wechseln Sie in das Register "Einstellungen".
6. Klicken Sie im Bereich "Benutzer-Authentifizierung" auf die Schaltfläche "Auswählen". Der Dialog "Windows Sicherheit" wird geöffnet und die verfügbaren Zertifikate werden angezeigt.

7. Wählen Sie ein Zertifikat aus. Bei Bedarf können Sie sich weitere Eigenschaften des Zertifikats anzeigen lassen.
8. Klicken Sie auf "OK".

Ergebnis

Das Zertifikat wird am Remotegerät für die Benutzerauthentifikation verwendet. Bei Bedarf kann es exportiert werden, um es mit dem Benutzergerät auszutauschen.

Siehe auch

Verwendung von Zertifikaten (Seite 20)

Zertifikat für die Benutzerauthentifikation erstellen (Seite 48)

Zertifikat für die Benutzerauthentifikation exportieren (Seite 49)

Zertifikat für die Benutzerauthentifikation importieren (Seite 50)

Zertifikat für die Benutzerauthentifikation hinzufügen (Seite 51)

Zertifikat für die Benutzerauthentifikation entfernen (Seite 53)

4.4.10 Zertifikat für die Benutzerauthentifikation entfernen

Sie können im Benutzergerät ein Zertifikat für die Benutzerauthentifikation jederzeit wieder aus der Liste der vertrauenswürdigen Zertifikate entfernen.

Vorgehen

Um ein Zertifikat für die Benutzerauthentifikation aus der Liste der vertrauenswürdigen Zertifikate zu entfernen, gehen Sie folgendermaßen vor:

1. Um den TIA Portal Cloud Connector zu öffnen, klicken Sie am Benutzergerät im Infobereich der Windows-Taskleiste mit der rechten Maustaste auf das Statussymbol des TIA Portal Cloud Connectors.
2. Wählen Sie im Kontextmenü den Befehl "Konfiguration (Benutzergerät)". Das Konfigurationsfenster des TIA Portal Cloud Connectors wird geöffnet.
3. Wechseln Sie in das Register "Protokoll".
4. Aktivieren Sie das Optionskästchen "HTTPS-Endpunkt". Im Register "Einstellungen" wird der Bereich zur Benutzerauthentifikation aktiv.
5. Wechseln Sie in das Register "Einstellungen".
6. Wählen Sie das Zertifikat in der Liste der vertrauenswürdigen Zertifikate, das Sie entfernen möchten.
7. Klicken Sie im Bereich "Benutzer-Authentifizierung" auf die Schaltfläche "Entfernen".

Ergebnis

Das Zertifikat wird aus der Liste der vertrauenswürdigen Zertifikate entfernt. Eine Verbindung zu dem Remotegerät, das dieses Zertifikat für die Benutzerauthentifikation nutzt, ist nicht mehr möglich.

Siehe auch

Verwendung von Zertifikaten (Seite 20)

Zertifikat für die Benutzerauthentifikation erstellen (Seite 48)

Zertifikat für die Benutzerauthentifikation exportieren (Seite 49)

Zertifikat für die Benutzerauthentifikation importieren (Seite 50)

Zertifikat für die Benutzerauthentifikation hinzufügen (Seite 51)

Zertifikat für die Benutzerauthentifikation auswählen (Seite 52)

4.5 Online-Verbindung über den TIA Portal Cloud Connector





Einführung

Wenn Sie für die Verbindung zur Hardware den TIA Portal Cloud Connector verwenden, unterscheidet sich das Arbeiten im TIA Portal nicht zu einer normalen Online-Verbindung zur Hardware. Sobald Sie die Tunnelkommunikation aktiviert haben, können Sie daher wie gewohnt Ihre Daten übersetzen, laden oder beobachten.

Weitere Informationen zum Herstellen einer Online-Verbindung und zum Arbeiten im Online-Modus finden Sie in der Online-Hilfe zum TIA Portal.

Übersicht über die Statussymbole

Wenn Sie eine Online-Verbindung über den TIA Portal Cloud Connector herstellen, erhalten Sie im Infobereich der Windows-Taskleiste Statussymbole angezeigt, über die Sie den Status der Verbindung ablesen können. Die folgende Tabelle zeigt eine Übersicht über die Statussymbole und ihre Bedeutungen:

Statussymbol	Bedeutung
	Die Kommunikation ist deaktiviert.
	Die Kommunikation ist zwar aktiviert, es findet jedoch kein Datenaustausch zwischen dem TIA Portal und der SIMATIC Automatisierungs-Hardware statt.
	Die Kommunikation ist aktiviert und es findet ein Datenaustausch zwischen dem TIA Portal und der SIMATIC Automatisierungs-Hardware statt.
	Der Datenaustausch zwischen dem TIA Portal und der SIMATIC Automatisierungs-Hardware wurde unterbrochen. Die Statusanzeige wird angezeigt und liefert Ihnen weitere Details zur Ursache.

Statusanzeige

Über den Infobereich in der Windows-Taskleiste können Sie sowohl auf dem Remotegerät als auch auf dem Benutzergerät eine Statusanzeige einblenden. Dadurch öffnet sich das Fenster "TIA Portal Cloud Connector - Remotegerät" bzw. "TIA Portal Cloud Connector - Benutzergerät". In diesem Fenster erhalten Sie alle Informationen, Warnungen und Fehlermeldungen des TIA Portal Cloud Connectors. Zusätzlich wird angezeigt, wie lange eine TCP- oder HTTPS-Verbindung bereits besteht.

Sie können die Statusanzeige jederzeit wieder schließen.

Siehe auch

TIA Portal Cloud Connector auf dem PG/PC installieren (Seite 39)

TIA Portal Cloud Connector am PG/PC konfigurieren (Seite 40)

TIA Portal Cloud Connector in der VM konfigurieren (Seite 42)

Virtuelle Maschine (VM) offline verwenden (Seite 55)

4.6 Virtuelle Maschine (VM) offline verwenden

Sie haben die Möglichkeit, auch offline mit einer Virtuellen Maschine zu arbeiten. Dazu können Sie die VM vom Remotegerät auf Ihr PG/PC kopieren. Anschließend können Sie die VM auf Ihrem PG/PC starten und das TIA Portal mit der Hardware nutzen, die entweder an Ihrem PG/PC angeschlossen ist oder im Netzwerk hängt.

Dabei haben Sie die folgenden Möglichkeiten, die VM zu verwenden:

- Die Hardware ist über Ethernet an Ihrem PG/PC angeschlossen und befindet sich im selben Subnetz.
- Die Hardware ist über Ethernet oder Profibus an Ihrem PG/PC angeschlossen und befindet sich in einem anderen Subnetz.

Nicht bei jeder Verbindungsart benötigen Sie den TIA Portal Cloud Connector. Es werden die folgenden Fälle unterschieden:

- Wenn Ihre Hardware über einen Ethernet- oder USB-Adapter direkt mit Ihrem PG/PC verbunden ist, können Sie als Netzwerk-Verbindung "Bridged" einstellen. Bei dieser Verbindungsart muss der TIA Portal Cloud Connector in der VM deaktiviert sein.
- Wenn Ihre Hardware über einen eigenen Netzwerk- oder USB-Adapter im Netzwerk hängt, können Sie die Option "Host-only" nutzen. In diesem Fall muss der TIA Portal Cloud Connector in der VM aktiviert sein, damit Sie auch die PROFIBUS-Schnittstelle verwenden können.

Nach der lokalen Verwendung der VM können Sie diese wieder zurück auf das Remotegerät kopieren.

4.6 Virtuelle Maschine (VM) offline verwenden

Voraussetzung

- Auf Ihrem PG/PC ist die passende Software installiert, mit der die VM gestartet werden kann, z. B. VMware Workstation.
- Auf Ihrem PG/PC ist der Automation License Manager installiert.

Virtuelle Maschine (VM) vom Remotegerät auf das PG/PC transferieren

Um mit der Virtuellen Maschine offline zu arbeiten, gehen Sie folgendermaßen vor:

1. Kopieren Sie die VM auf Ihr lokales PG/PC. Die genaue Vorgehensweise ist abhängig von der genutzten Virtualisierungsumgebung. Informieren Sie sich in der zugehörigen Dokumentation, falls Sie Hilfe benötigen.
2. Öffnen Sie den Automation License Manager und transferieren Sie die notwendigen Lizenzen für die SIMATIC Software im TIA Portal auf Ihr lokales Laufwerk.
3. Kopieren Sie alle notwendigen Projektdaten vom Server auf Ihr lokales Laufwerk.
4. Starten Sie die VM und konfigurieren Sie die Netzwerk-Verbindung. Beachten Sie dabei die Hinweise am Anfang der Seite.

Virtuelle Maschine (VM) vom PG/PC auf das Remotegerät transferieren

Um die Virtuelle Maschine wieder auf das Remotegerät zu transferieren, gehen Sie folgendermaßen vor:

- Kopieren Sie die VM von Ihrem lokalen PG/PC auf das Remotegerät. Die genaue Vorgehensweise ist abhängig von der genutzten Virtualisierungsumgebung. Informieren Sie sich in der zugehörigen Dokumentation, falls Sie Hilfe benötigen.
- Öffnen Sie den Automation License Manager und transferieren Sie die Lizenzen von Ihrem lokalen Laufwerk zurück zum ALM Server.
- Kopieren Sie alle notwendigen Projektdaten von Ihrem lokalen Laufwerk zurück auf den Server.

Siehe auch

TIA Portal Cloud Connector auf dem PG/PC installieren (Seite 39)

TIA Portal Cloud Connector am PG/PC konfigurieren (Seite 40)

TIA Portal Cloud Connector in der VM konfigurieren (Seite 42)

Online-Verbindung über den TIA Portal Cloud Connector (Seite 54)

Index

B

Bedienoberfläche, 7

H

HTTPS-Verbindung konfigurieren, 41, 43

I

Infobereich, 7

K

Konfiguration, 7

O

Online-Verbindung, 54

P

PG/PC
konfigurieren, 40

S

Simulation, 19
Statusanzeige, 14, 55
Statussymbole, 54
Support Packages, 20

T

Taskleiste, 7
TCP-Verbindung konfigurieren, 40, 42
TIA Portal Cloud Connector
Anwendungsfall, 17
Bedienoberfläche, 7
Bereitstellung, 6
Grundlagen, 5
konfigurieren, 7
Online-Verbindung, 54

Statusanzeige, 14
Zertifikat, 20

V

VM
konfigurieren, 42

Z

Zertifikat, 20
auswählen, 47, 52
entfernen, 53
erstellen, 44, 48
exportieren, 45, 49
hinzufügen, 51
importieren, 46, 50

