SIEMENS

SIMATIC

Istruzioni relative all'TIA Portal Cloud Connector

Manuale d'uso

10/2018
A5E44390476-AA

Avvertenze di legge

Concetto di segnaletica di avvertimento

Questo manuale contiene delle norme di sicurezza che devono essere rispettate per salvaguardare l'incolumità personale e per evitare danni materiali. Le indicazioni da rispettare per garantire la sicurezza personale sono evidenziate da un simbolo a forma di triangolo mentre quelle per evitare danni materiali non sono precedute dal triangolo. Gli avvisi di pericolo sono rappresentati come segue e segnalano in ordine descrescente i diversi livelli di rischio.

⚠ PERICOLO
questo simbolo indica che la mancata osservanza delle opportune misure di sicurezza **provoca** la morte o gravi lesioni fisiche.

⚠ AVVERTENZA
il simbolo indica che la mancata osservanza delle relative misure di sicurezza **può causare** la morte o gravi lesioni fisiche.

⚠ CAUTELA
indica che la mancata osservanza delle relative misure di sicurezza può causare lesioni fisiche non gravi.

ATTENZIONE
indica che la mancata osservanza delle relative misure di sicurezza può causare danni materiali.

Nel caso in cui ci siano più livelli di rischio l'avviso di pericolo segnala sempre quello più elevato. Se in un avviso di pericolo si richiama l'attenzione con il triangolo sul rischio di lesioni alle persone, può anche essere contemporaneamente segnalato il rischio di possibili danni materiali.

Personale qualificato

Il prodotto/sistema oggetto di questa documentazione può essere adoperato solo da **personale qualificato** per il rispettivo compito assegnato nel rispetto della documentazione relativa al compito, specialmente delle avvertenze di sicurezza e delle precauzioni in essa contenute. Il personale qualificato, in virtù della sua formazione ed esperienza, è in grado di riconoscere i rischi legati all'impiego di questi prodotti/sistemi e di evitare possibili pericoli.

Uso conforme alle prescrizioni di prodotti Siemens

Si prega di tener presente quanto segue:

⚠ AVVERTENZA
I prodotti Siemens devono essere utilizzati solo per i casi d'impiego previsti nel catalogo e nella rispettiva documentazione tecnica. Qualora vengano impiegati prodotti o componenti di terzi, questi devono essere consigliati oppure approvati da Siemens. Il funzionamento corretto e sicuro dei prodotti presuppone un trasporto, un magazzinaggio, un'installazione, un montaggio, una messa in servizio, un utilizzo e una manutenzione appropriati e a regola d'arte. Devono essere rispettate le condizioni ambientali consentite. Devono essere osservate le avvertenze contenute nella rispettiva documentazione.

Marchio di prodotto

Tutti i nomi di prodotto contrassegnati con ® sono marchi registrati della Siemens AG. Gli altri nomi di prodotto citati in questo manuale possono essere dei marchi il cui utilizzo da parte di terzi per i propri scopi può violare i diritti dei proprietari.

Esclusione di responsabilità

Abbiamo controllato che il contenuto di questa documentazione corrisponda all'hardware e al software descritti. Non potendo comunque escludere eventuali differenze, non possiamo garantire una concordanza perfetta. Il contenuto di questa documentazione viene tuttavia verificato periodicamente e le eventuali correzioni o modifiche vengono inserite nelle successive edizioni.

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANIA

A5E44390476-AA
℗ 08/2018 Con riserva di modifiche

Copyright © Siemens AG 2018.
Tutti i diritti riservati

Indice del contenuto

Introduzione a TIA Portal Cloud Connector 1

1.1 Avvertenze di sicurezza

Siemens commercializza prodotti e soluzioni dotati di funzioni Industrial Security che contribuiscono al funzionamento sicuro di impianti, soluzioni, macchine e reti.

La protezione di impianti, sistemi, macchine e reti da minacce cibernetiche, richiede l'implementazione e la gestione continua di un concetto globale di Industrial Security che corrisponda allo stato attuale della tecnica. I prodotti e le soluzioni Siemens costituiscono soltanto una componente imprescindibile di questo concetto.

È responsabilità del cliente prevenire accessi non autorizzati ad impianti, sistemi, macchine e reti. Il collegamento di sistemi, macchine e componenti, se necessario, deve avvenire esclusivamente nell'ambito della rete aziendale o tramite Internet previa adozione di opportune misure (ad es. impiego di firewall e segmentazione della rete).

Attenersi inoltre alle raccomandazione Siemens concernenti misure di sicurezza adeguate. Ulteriori informazioni su Industrial Security sono disponibili al sito: http://www.siemens.com/industrialsecurity (http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx)

I prodotti e le soluzioni Siemens vengono costantemente perfezionati per incrementarne la sicurezza. Siemens raccomanda espressamente di eseguire gli aggiornamenti non appena sono disponibili i relativi update e di impiegare sempre le versioni aggiornate dei prodotti. L'uso di prodotti non più attuali o di versioni non più supportate incrementa il rischio di attacchi cibernetici.

Per essere costantemente aggiornati sugli update dei prodotti, abbonarsi a Siemens Industrial Security RSS Feed al sito http://www.siemens.com/industrialsecurity (http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx).

1.2 Nozioni di base per l'utilizzo di TIA Portal Cloud Connector

Funzione di TIA Portal Cloud Connector

TIA Portal consente di operare in un ambiente virtuale. Il TIA Portal Cloud Connector è un'opzione utilizzabile in più progetti, che consente di accedere ad interfacce PG/PC locali e all'hardware SIMATIC ad esse collegato nel TIA Portal Engineering, nonostante l'engineering stesso venga utilizzato tramite desktop remoto in un Private Cloud.

Mediante il pacchetto opzionale "TIA Portal Cloud Connector" è possibile accedere dalla VM all'hardware locale SIMATIC collegato al PG/PC. Per questo è necessario installare TIA Portal Cloud Connector sia nella VM che sul PG/PC con il quale è collegato l'hardware SIMATIC. TIA Portal Cloud Connector consente inoltre di accedere all'hardware SIMATIC di un altro PG/PC mediante una connessione desktop remoto. L'altro PG/PC può trovarsi anche in un'altra rete. Un accesso di questo tipo non è possibile senza TIA Portal Cloud Connector.

L'utilizzo delle macchine virtuali con TIA Portal Cloud Connector in un Private Cloud offre i seguenti vantaggi:

- Supporto di moderne infrastrutture private cloud:
  - Scalabilità libera
  - Non è necessaria un'installazione sulle singole workstation
  - Manutenzione centrale e amministrazione di TIA Portal nella VM
  - Salvataggio centrale dei dati per progetti e biblioteche
- Accesso online a PLC e dispositivi HMI oltre i limiti della rete
- Collegamento protetto tramite HTTPS (a partire da Windows 8.1)
- Supporto di tutte le interfacce locali delle workstation
- Accesso rapido a diverse versioni di TIA Portal
- Sfruttamento più efficiente delle licenze disponibili
- Facilità di manutenzione remota delle macchine

Da una VM preconfigurata è possibile generare un modello. Da questo modello si possono ricavare nuove VM. In questo modo è possibile evitare procedure di installazione e configurazione.

Messa a disposizione di TIA Portal Cloud Connector

Il software del TIA Portal Cloud Connector viene fornito in dotazione con i seguenti pacchetti software SIMATIC da TIA Portal V14.0 in poi:

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

Per utilizzare TIA Portal Cloud Connector è necessaria una licenza sul PG/PC da acquistare separatamente.

Nota

TIA Portal Cloud Connector

L'utilizzo di TIA Portal Cloud Connector è previsto soltanto per operazioni di engineering con TIA Portal.

Per ulteriori informazioni consultare Siemens Industry Online Support al link https://support.industry.siemens.com/cs/ww/de/view/109739390 (https://support.industry.siemens.com/cs/ww/it/view/109739390).

Configurazione di TIA Portal Cloud Connector

Prima di poter creare un collegamento con TIA Portal Cloud Connector è necessario configurare TIA Portal Cloud Connector. La configurazione dipende dal ruolo di comunicazione del dispositivo. TIA Portal Cloud Connector conosce due ruoli di comunicazione:

- Ruolo di comunicazione “Dispositivo utente":
  Il dispositivo utente è il proprio PG/PC al quale è collegato l’hardware. Su questo dispositivo non deve essere installato TIA Portal. Questo ruolo di comunicazione viene preimpostato automaticamente se si installa TIA Portal Cloud Connector separatamente, quindi non insieme a TIA Portal.
  Vedere anche: Configurazione di TIA Portal Cloud Connector sul PG/PC (Pagina 40)
- Ruolo di comunicazione “Dispositivo remoto":
  Il dispositivo remoto è la VM nella quale è installato TIA Portal. Questo ruolo di comunicazione viene preimpostato automaticamente se si installa TIA Portal Cloud Connector insieme a TIA Portal.
  Vedere anche: Configurazione di TIA Portal Cloud Connector nella VM (Pagina 42)

Vedere anche

Interfaccia utente di TIA Portal Cloud Connector (Pagina 7)

Casi applicativi di TIA Portal Cloud Connector (Pagina 17)

Particolarità dell’utilizzo di una macchina virtuale (Pagina 19)

Utilizzo di certificati (Pagina 20)

Requisiti di sistema (Pagina 23)

Messa a disposizione della macchina virtuale (VM) (Pagina 31)

Utilizzo della macchina virtuale (VM) (Pagina 39)

1.3 Interfaccia utente di TIA Portal Cloud Connector

L’interfaccia utente di TIA Portal Cloud Connector è costituita dagli elementi seguenti:

- Registrazione nell’area di notifica della barra delle applicazioni di Windows
- TIA Portal Cloud Connector - Impostazioni
- TIA Portal Cloud Connector - Visualizzazione di stato
- TIA Portal Cloud Connector - Finestra informazioni
- TIA Portal - Visualizzazione nella barra di stato

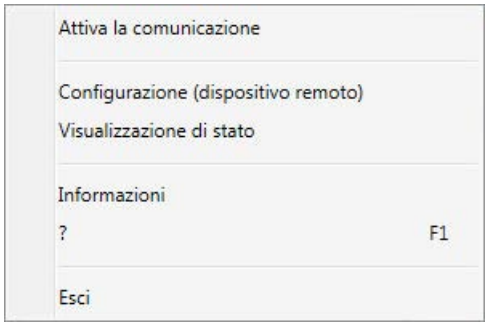
TIA Portal Cloud Connector nell’area di notifica della barra delle applicazioni di Windows

Dopo aver avviato TIA Portal Cloud Connector nell’area di notifica della barra delle applicazioni di Windows compare l’icona di Cloud Connector. Facendo clic sull’icona con il tasto destro del mouse si apre il menu di TIA Portal Cloud Connector.

La figura seguente mostra l’icona di TIA Portal Cloud Connector nell’area di notifica della barra delle applicazioni di Windows quando i punti finali della comunicazione sono disattivati:

Il colore del simbolo varia in funzione dello stato dei punti finali della comunicazione.

La figura seguente mostra il menu nell'area di notifica con il ruolo di comunicazione impostato "Dispositivo remoto".

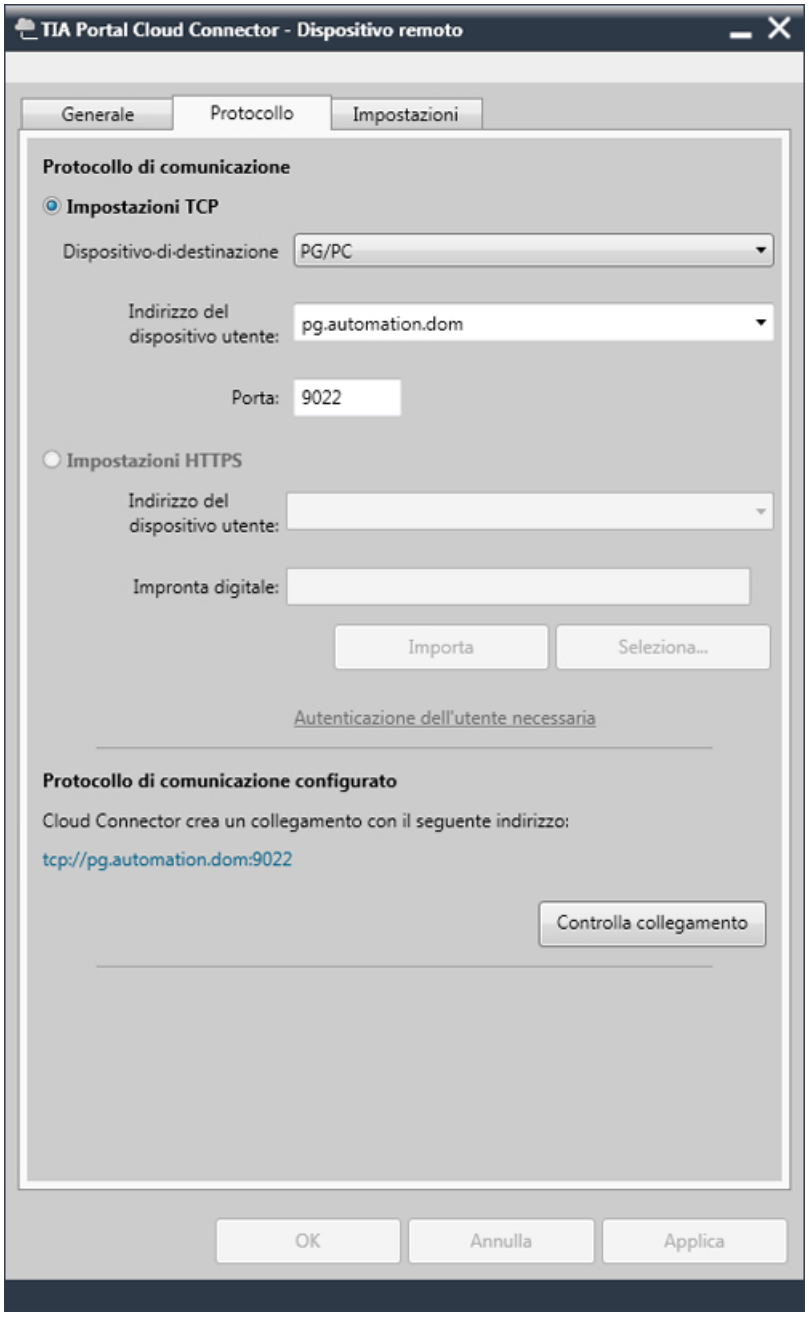


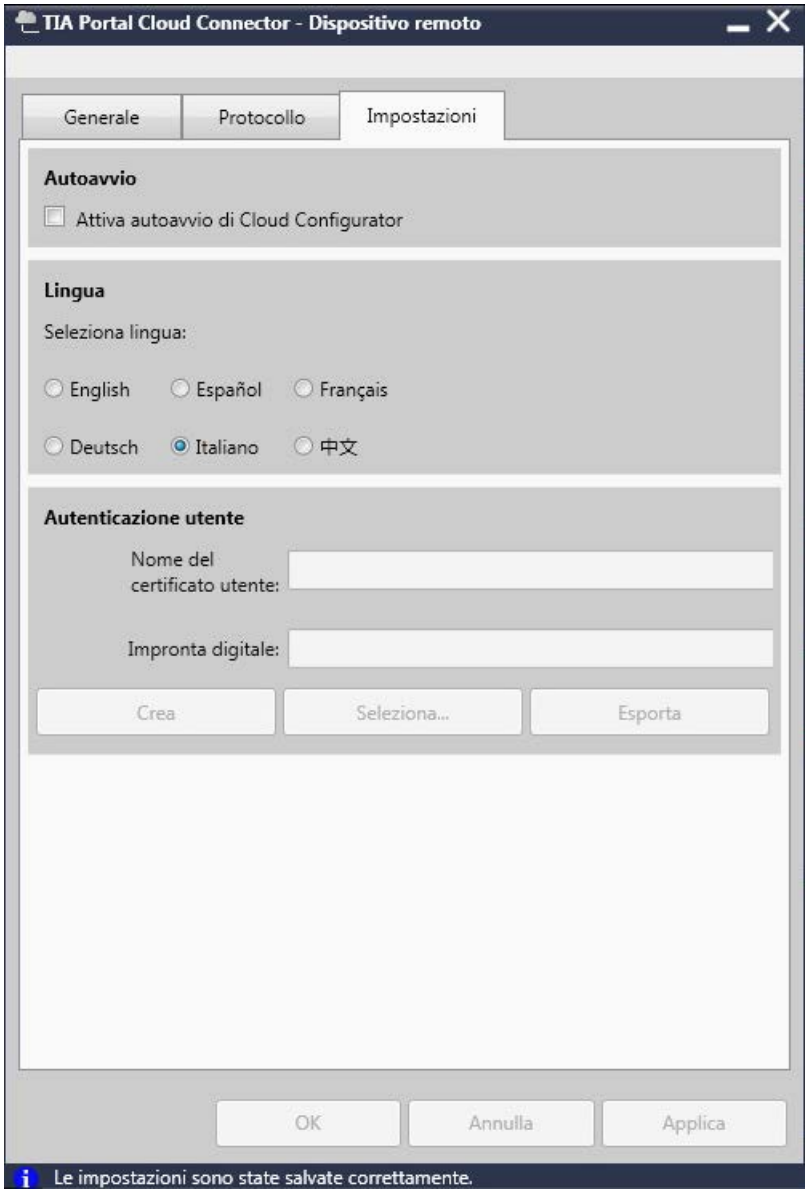
Dal menu si ha accesso alle azioni seguenti:

- Attiva la comunicazione: con questo comando è possibile attivare la comunicazione sia sul dispositivo remoto che sul dispositivo utente.
- Configurazione (dispositivi remoti/dispositivo utente): apre TIA Portal Cloud Configurator nel ruolo di comunicazione corrispondente.
- Visualizzazione di stato: apre la visualizzazione di stato, che fornisce informazioni su tutte le operazioni.
- Informazioni: apre la finestra informazioni di TIA Portal Cloud Connector. Qui si trova ad es. il numero di versione.
- ?: apre la Guida in linea di TIA Portal Cloud Connector.
- Esci: esce da TIA Portal Cloud Connector.

TIA Portal Cloud Connector - Impostazioni

L'interfaccia utente di TIA Portal Cloud Connector varia in funzione del ruolo di comunicazione impostato. Le figure seguenti mostrano le diverse schede di impostazione del TIA Portal Cloud Connector nel ruolo di comunicazione "Dispositivo remoto":


TIA Portal Cloud Connector - Dispositivo remoto
Generale
Protocollo
Impostazioni
Protocollo di comunicazione
Impostazioni TCP
Dispositivo-di-destinazione
PG/PC
Indirizzo del dispositivo utente:
pg.automation.dom
Porta:
9022
Impostazioni HTTPS
Indirizzo del dispositivo utente:
Impronta digitale:
Importa
Seleziona...
Autenticazione dell'utente necessaria
Protocollo di comunicazione configurato
Cloud Connector crea un collegamento con il seguente indirizzo:
tcp://pg.automation.dom:9022
Controlla collegamento
OK
Annulla
Applica



All'interno delle diverse schede è possibile eseguire tutte le impostazioni necessarie per un collegamento.

La seguente tabella mostra una panoramica delle impostazioni possibili e dei pulsanti esistenti per il ruolo di comunicazione “Dispositivo remoto":

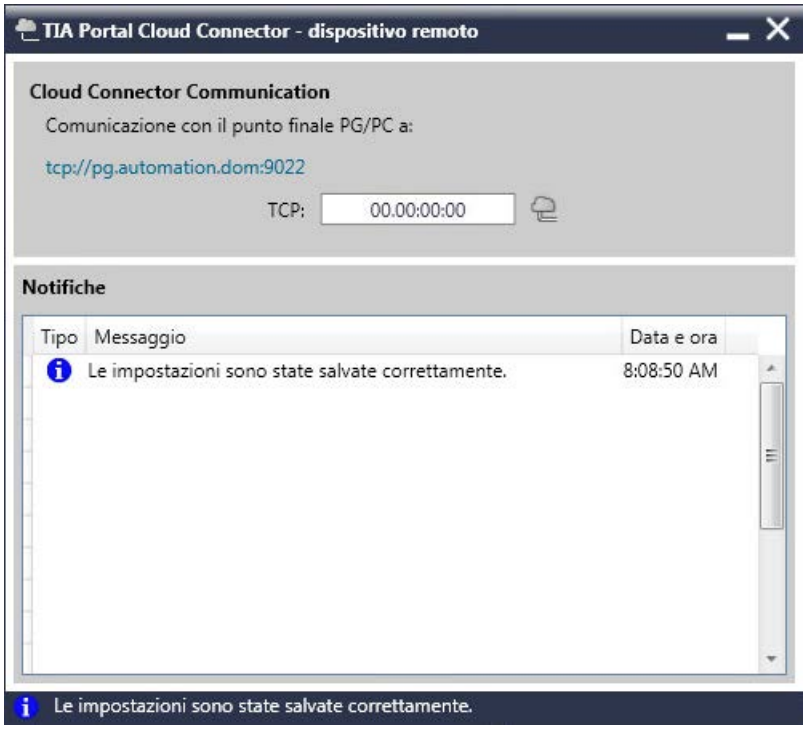
Scheda	Area	Impostazione/pulsante	Descrizione
Generale	Ruolo di comunicazione	Dispositivo utente	PG/PC che consente il contatto fisico con l’hardware SIMATIC.
		Dispositivo remoto	Macchina virtuale (VM) sulla quale è installato TIA Portal. È possibile accedervi dal dispositivo utente attraverso una connessione desktop remoto.
	Comunicazione Cloud Connector	Attiva la comunicazione Disattiva la comunicazione	Attiva o disattiva la comunicazione con un punto finale PG/PC.
	Accessi alle licenze	Attivazione Disattiva	Attiva e disattiva l'uso di una licenza del dispositivo utente.
Protocollo	Protocollo di comunicazione		Definisce il meccanismo di trasporto tra i punti terminali della comunicazione. Sono disponibili TCP o HTTPS (a partire da Windows 8.1).
	Impostazioni TCP	Dispositivo di destinazione	Tipo del partner di collegamento locale
		Indirizzo del dispositivo utente	Indirizzo IP o nome del dispositivo utente
		Porta	Numero di porta sulla quale deve essere eseguito il trasporto
	Impostazioni HTTPS	Indirizzo del dispositivo utente	Indirizzo IP o nome del dispositivo utente
		Impronta digitale	Garantisce l’integrità del certificato.
		Importa	Importa un certificato esistente nell’archivio certificati di Windows. Un certificato importato può essere utilizzato per la crittografia dei dati che vengono inviati tramite HTTPS.
		Seleziona	Selezione di un certificato importato in precedenza per la crittografia dei dati.
	Protocollo di comunicazione configurato	Controlla collegamento	Controlla se il collegamento può essere realizzato senza errori.
Impostazioni	Autoavvio	Attiva autoavvio di Cloud Connector	Attiva o disattiva l’avvio automatico per TIA Portal Cloud Connector durante l’avvio del sistema.
	Lingua	Selezionare la lingua	Definisce la lingua dell’interfaccia per TIA Portal Cloud Connector.
	Autenticazione utente	Nome del certificato utente	Visualizza il certificato utente attualmente utilizzato.
		Impronta digitale	Somma di controllo del certificato per garantire l’integrità
		Crea	Crea un nuovo certificato per l’autenticazione utente.
		Seleziona	Consente la selezione di un certificato esistente dall’archivio certificati di Windows.
		Esportazione	Esporta il certificato attualmente utilizzato.

La seguente tabella mostra una panoramica delle impostazioni possibili e dei pulsanti esistenti per il ruolo di comunicazione “Dispositivo utente":

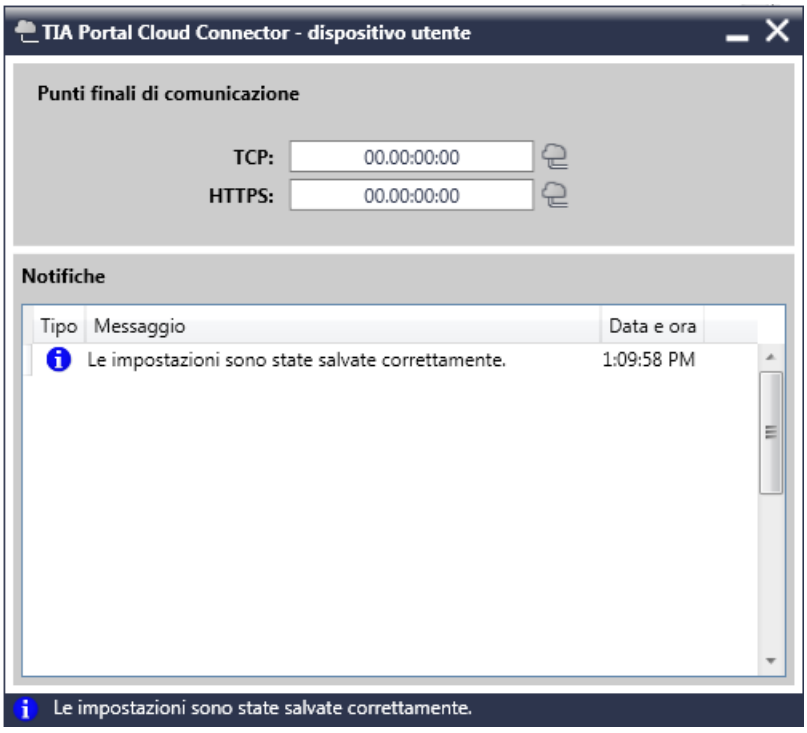
Scheda	Area	Impostazione/pulsante	Descrizione
Generale	Ruolo di comunicazione	Dispositivo utente	PG/PC che consente il contatto fisico con l’hardware SIMATIC.
		Dispositivo remoto	Macchina virtuale sul Private Cloud Server nel quale è installato TIA Portal che viene utilizzato dal dispositivo utente tramite connessione al desktop remoto.
	Comunicazione Cloud Connector	Attiva la comunicazione Disattiva la comunicazione	Attiva o disattiva la comunicazione con un punto finale PG/PC.
	Accessi alle licenze	Attivazione Disattiva	Attiva e disattiva l'uso di una licenza del dispositivo utente.
Protocollo	Punto finale TCP	Porta	Numero di porta sulla quale deve essere eseguita la comunicazione. Il numero di porta del dispositivo utente deve corrispondere al numero di porta del dispositivo remoto.
	Punto finale HTTPS	Indirizzo del dispositivo utente	Indirizzo IP o nome del dispositivo utente
		Impronta digitale	Garantisce l’integrità del certificato.
		Crea	Crea un nuovo certificato per la crittografia dei dati.
		Esportazione	Esporta il certificato attualmente utilizzato.
		Seleziona	Consente la selezione di un certificato esistente.
Impostazioni	Autoavvio	Attiva autoavvio di Cloud Connector	Attiva o disattiva l’avvio automatico per TIA Portal Cloud Connector durante l’avvio del sistema.
	Lingua	Selezionare la lingua	Definisce la lingua dell’interfaccia per TIA Portal Cloud Connector.
	Autenticazione utente	Certificati utente attendibili	Visualizza l’elenco di tutti i certificati utente disponibili e attendibili.
		Importa	Consente di importare un certificato creato nel dispositivo remoto nell’archivio certificati di Windows.
		Aggiungi	Consente di aggiungere un certificato dall’archivio certificati di Windows all’elenco dei certificati attendibili.
		Rimuovi	Rimuove il certificato selezionato dall’elenco dei certificati attendibili. Tuttavia questo certificato viene mantenuto nell’archivio certificati di Windows.

TIA Portal Cloud Connector - Visualizzazione di stato

La visualizzazione di stato fornisce informazioni, avvisi e messaggi di errore durante l'utilizzo di TIA Portal Cloud Connector. La figura seguente mostra la visualizzazione di stato nel ruolo di comunicazione "Dispositivo remoto":

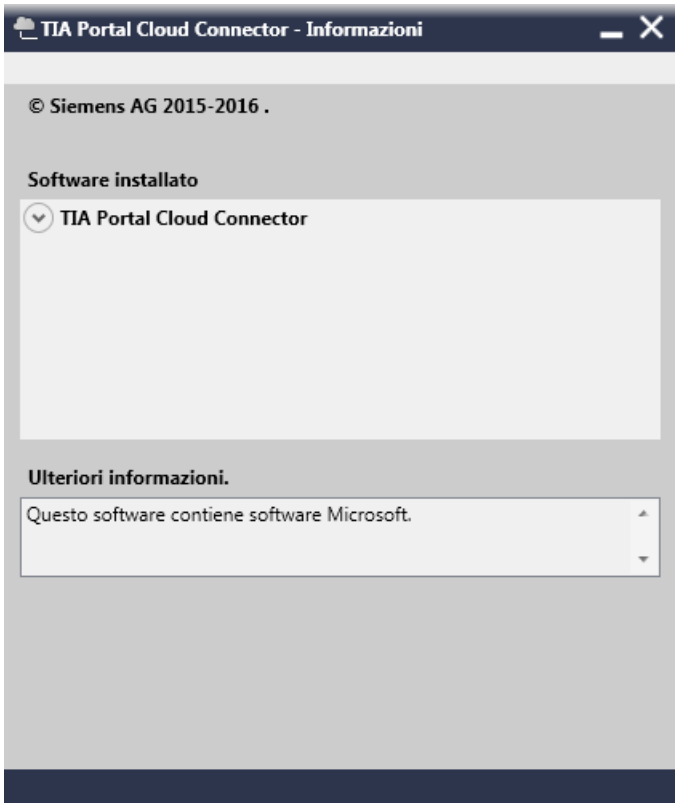


La figura seguente mostra la visualizzazione di stato nel ruolo di comunicazione "Dispositivo utente":


TIA Portal Cloud Connector - dispositivo utente
Punti finali di comunicazione
TCP:
00.00:00:00
HTTPS:
00.00:00:00
Notifiche
Tipo
Messaggio
Data e ora
Le impostazioni sono state salvate correttamente.
1:09:58 PM
Le impostazioni sono state salvate correttamente.

TIA Portal Cloud Connector - Finestra informazioni

Nella finestra informazioni si trovano informazioni sulla versione installata del TIA Portal Cloud Connector.



TIA Portal - Visualizzazione nella barra di stato

Nella barra di stato del TIA Portal si ottengono informazioni sui collegamenti online in atto con l'hardware SIMATIC Hardware tramite TIA Portal Cloud Connector. Oltre alle visualizzazioni online, in un collegamento tramite TIA Portal Cloud Connector viene visualizzata la seguente icona nella barra di stato:

Vedere anche

Nozioni di base per l'utilizzo di TIA Portal Cloud Connector (Pagina 5)

Casi applicativi di TIA Portal Cloud Connector (Pagina 17)

Particolarità dell'utilizzo di una macchina virtuale (Pagina 19)

Utilizzo di certificati (Pagina 20)

Requisiti di sistema (Pagina 23)

Messa a disposizione della macchina virtuale (VM) (Pagina 31)

Utilizzo della macchina virtuale (VM) (Pagina 39)

1.4 Casi applicativi di TIA Portal Cloud Connector

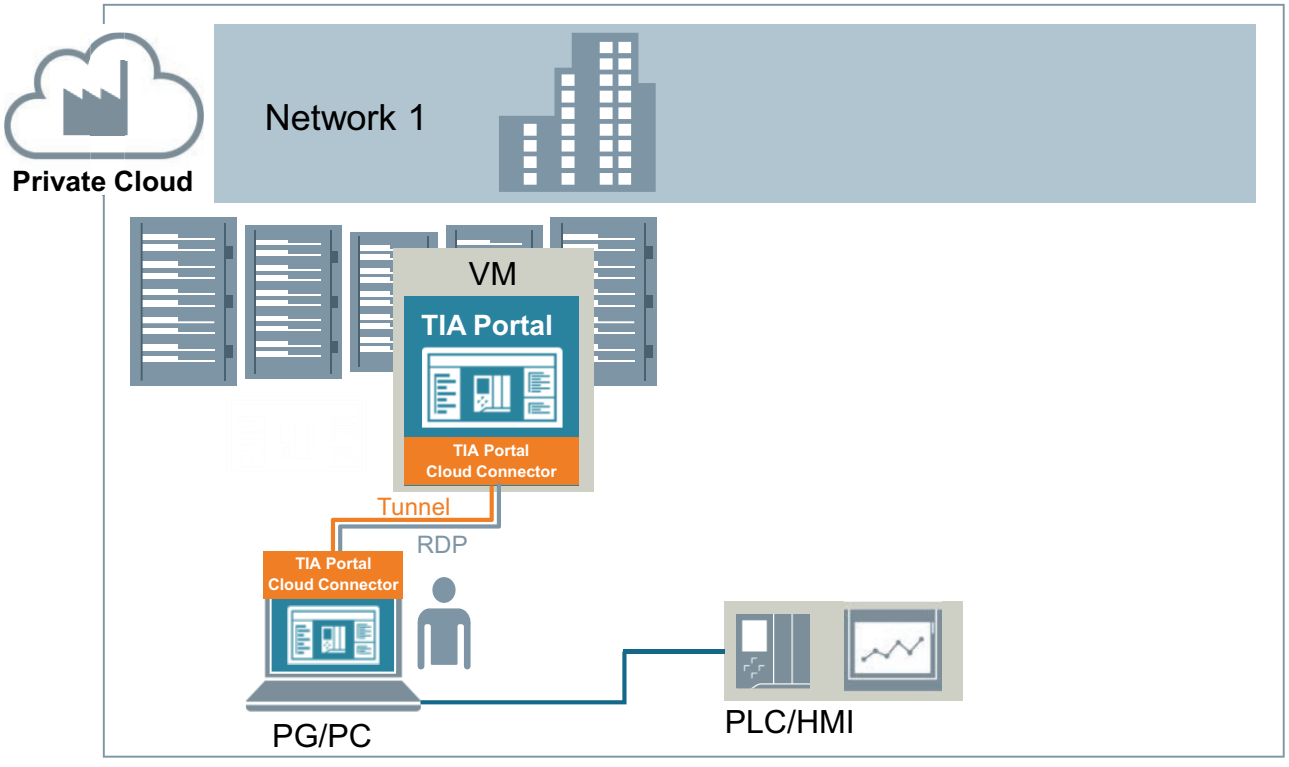
Con TIA Portal Cloud Connector è possibile realizzare i seguenti casi applicativi:

- Accesso all'hardware collegato al proprio PG/PC.
- Accesso all'hardware collegato a un altro PG/PC. Questo può trovarsi all'interno o all'esterno della propria rete.

Accesso all'hardware collegato al proprio PG/PC

TIA Portal viene installato nel private cloud dell'azienda. Sul PG/PC dell'utente, invece, non è presente nessuna installazione di TIA Portal. L'hardware di automazione (PLC/HMI) è collegato al PG/PC dell'utente. TIA Portal Cloud Connector è installato sia nella VM che sul proprio PG/PC. Sul PG/PC è necessaria una licenza per TIA Portal Cloud Connector. Attraverso una connessione desktop remoto l'utente si collega con la VM e può utilizzare come di consueto TIA Portal. Con l'aiuto di TIA Portal Cloud Connector è possibile accedere all'hardware collegato localmente al PG/PC.

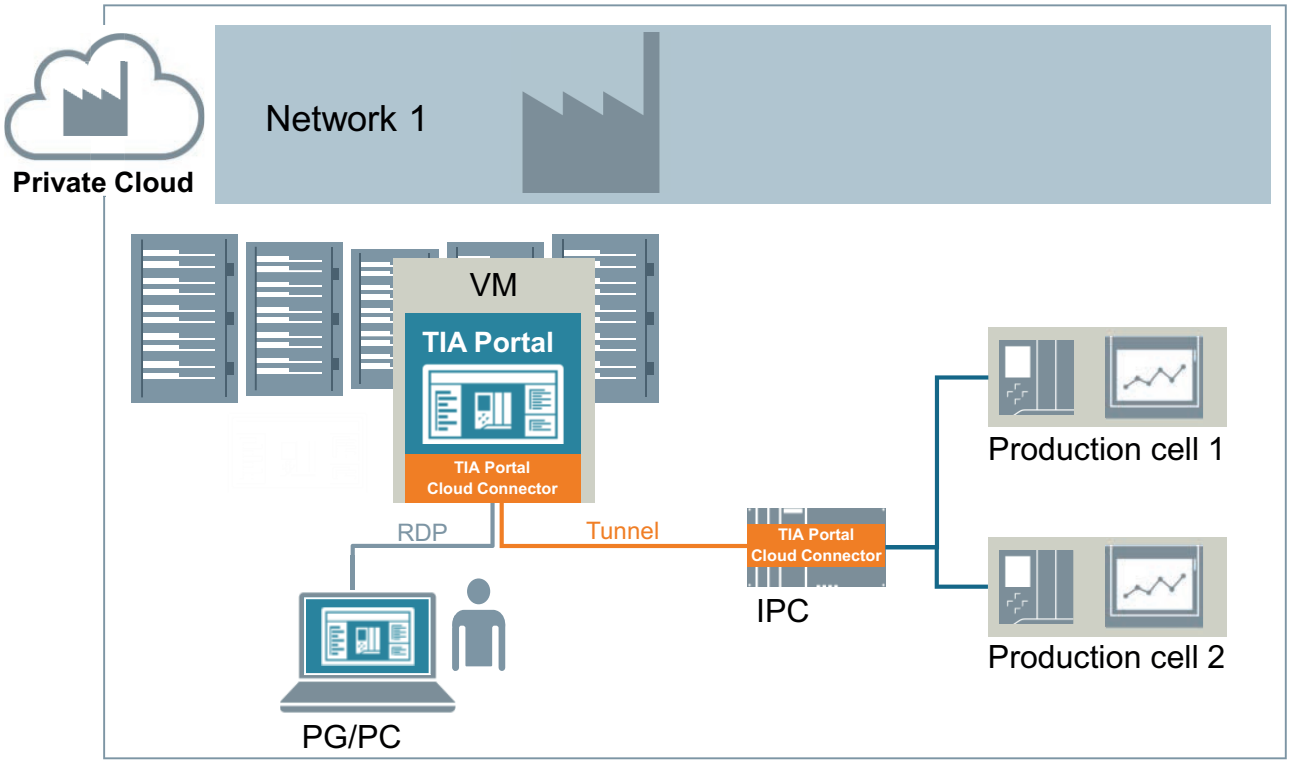
La figura seguente mostra l'impiego di TIA Portal Cloud Connector in un ambiente virtuale quando l'hardware è collegato al proprio PG/PC:

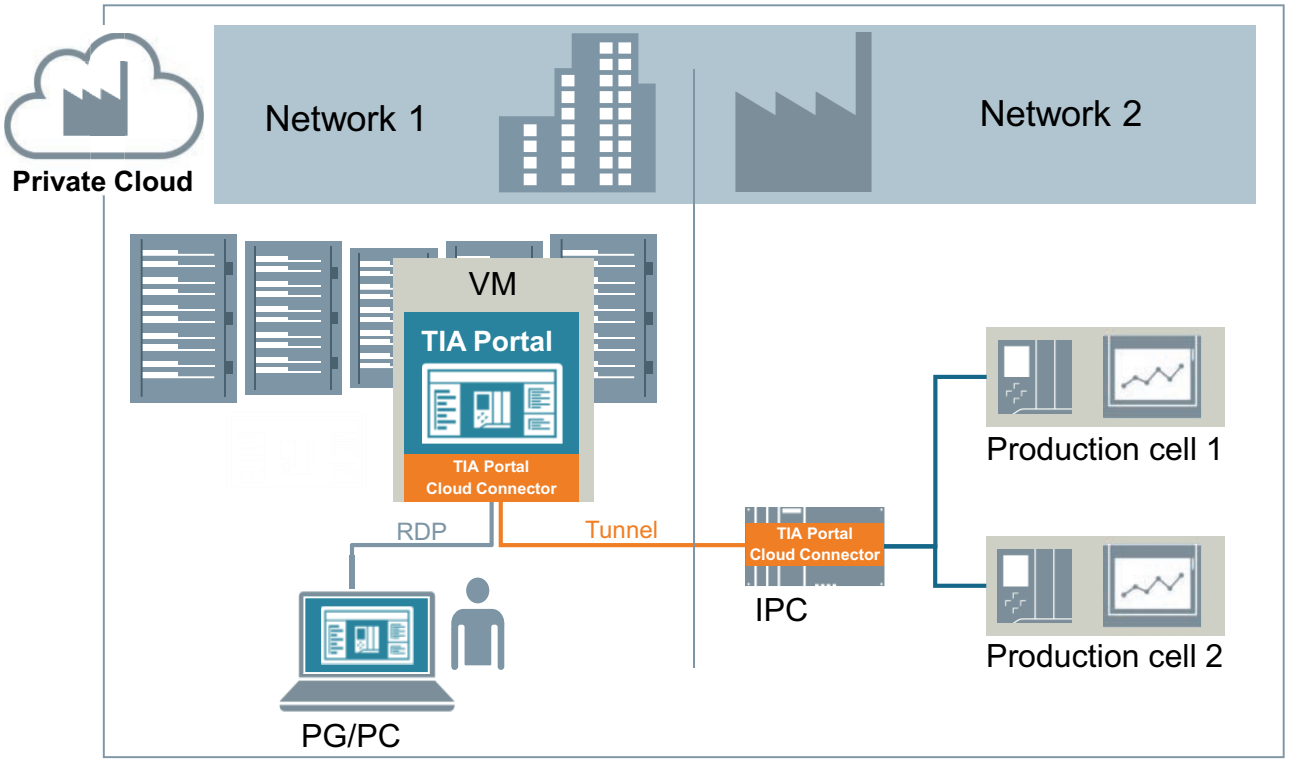


Accesso all'hardware collegato a un altro PG/PC

TIA Portal viene installato in una macchina virtuale. Sul proprio PG/PC, invece, non è presente nessuna installazione di TIA Portal. L'hardware di automazione è collegato con un PG/PC, ad es. un IPC che si trova nella stessa rete o in una rete diversa (figura in basso) da quella del proprio PG/PC. TIA Portal Cloud Connector è installato su un alto PG/PC e nella VM. Attraverso una connessione desktop remoto l'utente si collega dapprima con la VM e può utilizzare come di consueto TIA Portal. Con TIA Portal Cloud Connector è possibile realizzare una connessione tra VM e l'altro PG/PC e accedere all'hardware di automazione.

Le figure seguenti mostrano l'impiego di TIA Portal Cloud Connector in un ambiente virtuale quando l'hardware è collegato ad un altro PG/PC, ad es. un IPC:





Vedere anche

Nozioni di base per l'utilizzo di TIA Portal Cloud Connector (Pagina 5)
Interfaccia utente di TIA Portal Cloud Connector (Pagina 7)
Particolarità dell'utilizzo di una macchina virtuale (Pagina 19)
Utilizzo di certificati (Pagina 20)
Requisiti di sistema (Pagina 23)
Messa a disposizione della macchina virtuale (VM) (Pagina 31)
Utilizzo della macchina virtuale (VM) (Pagina 39)

1.5 Particolarità dell'utilizzo di una macchina virtuale

Simulazione

Per poter simulare un programma PLC è necessario prima disattivare TIA Portal Cloud Connector. Per la simulazione dei dispositivi HMI, tuttavia, questo non è necessario.

Utilizzo di aggiornamenti e support package

Gli aggiornamenti e i support package possono essere già installati nel modello di VM o essere installati successivamente nelle singole VM. Impiegare a tal fine i meccanismi di aggiornamento del TIA Portal.

Per ulteriori informazioni osservare il sistema di informazione di TIA Portal.

Confronto tra la topologia progettata e quella effettivamente presente

Il confronto della topologia non viene supportato da TIA Portal Cloud Connector.

Vedere anche

Nozioni di base per l'utilizzo di TIA Portal Cloud Connector (Pagina 5)

Interfaccia utente di TIA Portal Cloud Connector (Pagina 7)

Casi applicativi di TIA Portal Cloud Connector (Pagina 17)

Utilizzo di certificati (Pagina 20)

Requisiti di sistema (Pagina 23)

Messa a disposizione della macchina virtuale (VM) (Pagina 31)

Utilizzo della macchina virtuale (VM) (Pagina 39)

1.6 Utilizzo di certificati

Utilizzo di certificati in TIA Portal Cloud Connector

A partire da Windows 8.1 è possibile utilizzare collegamenti HTTPS per la comunicazione. TIA Portal Cloud Connector utilizza certificati per garantire la sicurezza dei collegamenti HTTPS. I seguenti certificati sono necessari per la realizzazione di un collegamento tra il dispositivo utente e il dispositivo remoto:

- Certificato per la crittografia dei dati.
- Certificato per l'autenticazione utente.

Se non esiste un certificato o se i certificati del dispositivo utente e del dispositivo remoto non corrispondono, non è possibile realizzare un collegamento.

Certificato per la crittografia dei dati.

Creare il certificato per la crittografia dei dati nel dispositivo utente. Successivamente il certificato deve essere copiato in un drive del dispositivo remoto e importato in TIA Portal Cloud Connector. Se i certificati corrispondono, un collegamento tra i dispositivi è possibile non appena sono stati scambiati anche i certificati per l'autenticazione utente.

Certificato per l'autenticazione utente.

Creare il certificato per l'autenticazione utente nel dispositivo remoto. Successivamente il certificato deve essere copiato nel dispositivo utente e importato in TIA Portal Cloud Connector. Se i certificati corrispondono, un collegamento tra i dispositivi è possibile se sono stati scambiati anche i certificati per la crittografia dei dati.

Vedere anche

Nozioni di base per l'utilizzo di TIA Portal Cloud Connector (Pagina 5)
Interfaccia utente di TIA Portal Cloud Connector (Pagina 7)
Casi applicativi di TIA Portal Cloud Connector (Pagina 17)
Particolarità dell'utilizzo di una macchina virtuale (Pagina 19)
Creazione del certificato per la crittografia dei dati (Pagina 44)
Esportazione del certificato per la crittografia dei dati (Pagina 45)
Importazione del certificato per la crittografia dei dati (Pagina 46)
Selezione del certificato per la crittografia dei dati (Pagina 47)
Creazione del certificato per l'autenticazione utente (Pagina 48)
Esportazione del certificato per l'autenticazione utente (Pagina 49)
Importazione del certificato per l'autenticazione utente (Pagina 50)
Aggiunta del certificato per l'autenticazione utente (Pagina 51)
Selezione del certificato per l'autenticazione utente (Pagina 52)
Eliminazione del certificato per l'autenticazione utente (Pagina 53)

Requisiti di sistema 2

2.1 Requisiti di sistema PG/PC

Sistemi operativi supportati

Per poter utilizzare TIA Portal Cloud Connector deve essere installato sul PG/PC uno dei seguenti sistemi operativi:

- Windows Server 2012 R2 StdE (installazione completa)
- Windows Server 2016 Standard (installazione completa)
- 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 versione 1703
- Windows 10 Enterprise Version 1703
- Windows 10 Enterprise 2016 LTSB
- Windows 10 IoT Enterprise 2015 LTSB
- Windows 10 IoT Enterprise 2016 LTSB

Nota

Osservare le avvertenze seguenti:

- Non è possibile utilizzare TIA Portal Cloud Connector sui sistemi operativi a 32 bit.
- Assicurarsi che il sistema operativo sia sempre aggiornato all'ultima versione. Eseguire tutti i principali aggiornamenti di Windows quando sono disponibili.
- Se la versione installata di SIMATIC NET è inferiore alla V15.0.1, TIA Portal Cloud Connector non può essere attivato.
- Affinché la risoluzione del nome funzioni in rete, attivare nelle impostazioni di rete di Windows l'opzione "Attiva individuazione rete" o "Attiva condivisione file e stampanti". In alternativa si può utilizzare un nome di server esterno.

Licenze per TIA Portal Cloud Connector

Per utilizzare TIA Portal Cloud Connector è necessaria una License Key valida su ogni dispositivo definito come "dispositivo utente" in TIA Portal Cloud Connector. Per i dispositivi definiti come "dispositivo remoto" non è necessaria nessuna License Key.

La License Key si può installare congiuntamente all'installazione oppure a posteriori con Automation License Manager.

Vedere anche

Requisiti di sistema sulla VM (Pagina 24)

Licenze (Pagina 27)

2.2 Requisiti di sistema sulla VM

Sistemi operativi guest supportati e piattaforme di virtualizzazione

TIA Portal può essere utilizzato nell'ambito di una macchina virtuale (VM). Utilizzare pertanto una delle seguenti piattaforme di virtualizzazione nella versione indicata o in una versione più recente:

- 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

Nella VM si possono installare uno o più pacchetti software tra quelli qui indicati:

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

Oltre ai pacchetti software è possibile installare anche altri pacchetti opzionali STEP 7 e WinCC.

Nota

Funzionamento di TIA Portal Cloud Connector con un' installazione esistente di SIMATIC NET

Se nella VM è installato SIMATIC NET, TIA Portal Cloud Connector non può essere attivato.

A seconda del pacchetto software selezionato, all'interno della VM sono supportati diversi sistemi operativi guest:

Sistema operativo guest	SIMATIC STEP 7 Basic	SIMATIC STEP 7 Professional	SIMATIC WinCC Basic	SIMATIC WinCC Professional	SIMATIC WinCC Advanced
Windows Server 2012 R2 StdE (installazione completa) (64 bit)	X	X	X	X	X
Windows Server 2016 Standard (installazione completa) (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 versione 1703 (64 bit)	X	X	X	X	X
Windows 10 Enterprise version 1703 (64 bit)	X	X	X	X	X
Windows 10 Enterprise 2016 LTSB (64 Bit)	X	X	X	X	X
Windows 10 IoT Enterprise 2015 LTSB (64 bit)	X	X	X	X	X
Windows 10 IoT Enterprise 2016 LTSB (64 bit)	X	X	X	X	X
- Sistema operativo non supportato X Sistema operativo supportato					

Nota

Prestare attenzione a quanto segue:

- I sistemi operativi a 32 bit non sono supportati.
- Per i sistemi operativi guest valgono gli stessi requisiti hardware del rispettivi prodotti TIA.
- SIMATIC USB Prommer non è supportato.
- Se si vogliono utilizzare schede SD nella VM, è necessario incorporarle prima come supporti dati rimovibili nella VM. Per il procedimento esatto consultare la Guida alla piattaforma di virtualizzazione in uso.
- Assicurarsi che il sistema operativo sia sempre aggiornato all'ultima versione. Eseguire tutti i principali aggiornamenti di Windows quando sono disponibili.

Installazione di TIA Portal Cloud Connector

Per installare TIA Portal Cloud Connector si può procedere in due modi:

- Durante l'installazione di uno dei pacchetti software SIMATIC sopra indicati è possibile attivare TIA Portal Cloud Connector come opzione. In seguito verrà installato insieme al pacchetto software.
- TA Portal Cloud Connector si può installare indipendentemente da un pacchetto software SIMATIC. Il file di installazione si trova sul supporto di installazione nella cartella "Support". È possibile mettere a disposizione questo file di installazione nella propria rete. In questo modo, in quanto amministratore della VM, sarà possibile anche creare script che consentano l'aggiornamento automatico di TIA Portal Cloud Connector. Tenere presente, tuttavia, che su ogni PG/PC deve essere disponibile una licenza valida di TIA Portal Cloud Connector.

Licenze per TIA Portal Cloud Connector

Per utilizzare TIA Portal Cloud Connector nella VM non è necessaria una licenza di TIA Portal Cloud Connector se il ruolo di comunicazione definito è "dispositivo utente".

Vedere anche

Requisiti di sistema PG/PC (Pagina 23)

Licenze (Pagina 27)

2.3 Licenze

Attivazione delle licenze dei pacchetti software SIMATIC

Per utilizzare i singoli pacchetti software SIMATIC di TIA Portal (STEP 7, WinCC) in un ambiente virtuale è necessaria una licenza per ogni installazione. Se si copia o si clona un modello di VM, anche questa è considerata un'installazione a parte. Sul PG/PC dal quale si accede a una VM, invece, non è necessaria una licenza per l'uso di TIA Portal finché non è presente un'installazione locale.

Se si utilizzano chiavi di licenza Floating è possibile rendere disponibili le licenze attraverso un server per le chiavi di licenza.

Attivazione delle licenze di TIA Portal Cloud Connector

Per utilizzare TIA Portal Cloud Connector è necessaria una License Key valida su ogni dispositivo definito come "dispositivo utente" in TIA Portal Cloud Connector. Per i dispositivi definiti come "dispositivo remoto" non è necessaria nessuna License Key.

La License Key si può installare congiuntamente all'installazione oppure a posteriori con Automation License Manager.

Accesso alle licenze del dispositivo utente dal dispositivo remoto

Attraverso TIA Portal Cloud Connector il TIA Portal del dispositivo remoto può accedere alle licenze che si trovano nel dispositivo utente. Per inoltrare le richieste delle licenze dal dispositivo remoto al dispositivo utente, TIA Portal Cloud Connector si serve di un tunnel. Una volta inoltrata la richiesta di accesso di TIA Portal Cloud Connector, l'ALM rifiuta le richieste degli altri calcolatori remoti. Le applicazioni a cui erano già state assegnate licenze potranno proseguirne l'utilizzo. Si possono assegnare licenze locali alle applicazioni sia sui dispositivi remoti che sui dispositivi utente.

Vedere anche: Assegnazione di una licenza del dispositivo utente (Pagina 27)

Vedere anche

Requisiti di sistema PG/PC (Pagina 23)

Requisiti di sistema sulla VM (Pagina 24)

Utilizzo del server per le chiavi di licenza (Pagina 34)

2.4 Assegnazione di una licenza del dispositivo utente

Il TIA Portal installato sul dispositivo remoto può accedere alle licenze che si trovano nel dispositivo utente purché su entrambi i dispositivi sia stata attivata l'opzione che abilita l'uso delle licenze esterne. La procedura per attivare questa opzione è la stessa per entrambi i dispositivi. Per capire se l'opzione è attiva e se alcune licenze esterne sono in uso si deve osservare il colore dei simboli riportati sul pulsante "Attiva" e "Disattiva".

La seguente tabella descrive i simboli di stato e il loro significato:

Simbolo	Significato
	L'opzione di assegnazione delle licenze è disattivata.
	L'opzione di assegnazione delle licenze è attiva, ma il dispositivo remoto non sta utilizzando le licenze del dispositivo utente.
	L'opzione di assegnazione delle licenze è attiva e il dispositivo remoto sta utilizzando delle licenze del dispositivo utente.
	Lo scambio di dati tra TIA Portal e l'hardware di automazione SIMATIC è stato interrotto. Compare la visualizzazione di stato che contiene ulteriori dettagli sulla causa.

L'assegnazione delle licenze può essere disattivata in qualsiasi momento.

Attivazione dell'uso delle licenze esterne

Per attivare l'accesso alle licenze nel dispositivo utente procedere nel seguente modo:

1. Selezionare il dispositivo utente, fare clic con il tasto destro del mouse sull'icona di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni e selezionare il comando "Configurazione".
   TIA Portal Cloud Connector si apre.
2. Aprire la scheda "Generale".
3. Fare clic sul pulsante "Attiva" nell'area "Accessi alle licenze".
4. Stabilire una connessione desktop remoto con la VM in cui si trova il dispositivo remoto.
5. Selezionare il dispositivo remoto, fare clic con il tasto destro del mouse sull'icona di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni e selezionare il comando "Configurazione".
   TIA Portal Cloud Connector si apre.
6. Fare clic sul pulsante "Attiva" nell'area "Accessi alle licenze".
   Viene attivata l'opzione che consente al TIA Portal del dispositivo remoto di utilizzare le licenze del dispositivo utente. Il testo del pulsante "Attiva" viene sostituito dal testo "Disattiva" e il simbolo cambia colore e diventa giallo.

Disattivazione dell'uso delle licenze esterne

Per disattivare l'accesso alle licenze nel dispositivo utente procedere nel seguente modo:

1. Selezionare il dispositivo utente, fare clic con il tasto destro del mouse sull'icona di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni e selezionare il comando "Configurazione".
   TIA Portal Cloud Connector si apre.
2. Aprire la scheda "Generale".
3. Fare clic sul pulsante "Disattiva" nell'area "Accessi alle licenze".
4. Stabilire una connessione desktop remoto con la VM in cui si trova il dispositivo remoto.

5. Selezionare il dispositivo remoto, fare clic con il tasto destro del mouse sull'icona di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni e selezionare il comando "Configurazione".
   TIA Portal Cloud Connector si apre.
6. Fare clic sul pulsante "Disattiva" nell'area "Accessi alle licenze".
   Viene disattivata l'opzione che consente al TIA Portal del dispositivo remoto di utilizzare le licenze del dispositivo utente. Il testo del pulsante "Disattiva" viene sostituito dal testo "Attiva" e il simbolo cambia colore e diventa giallo.

Vedere anche

Licenze (Pagina 27)

Utilizzo del server per le chiavi di licenza (Pagina 34)

Messa a disposizione della macchina virtuale (VM) 3

3.1 Creazione di un nuovo modello VM

È possibile utilizzare le seguenti piattaforme di virtualizzazione:

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

A seconda della piattaforma di virtualizzazione utilizzata, esistono alcune differenze nella creazione di un modello sulla base di una macchina virtuale esistente (VM). Per ulteriori informazioni consultare la Guida della piattaforma di virtualizzazione in uso.

Configurare l'ambiente di sviluppo SIMATIC nella VM come in ciascun PG/PC.

Passi principali per la creazione di un nuovo modello di VM

Per creare un nuovo modello di VM procedere nel modo seguente:

1. Creare una VM.
2. Installare il software SIMATIC desiderato, ad es. SIMATIC STEP 7 (TIA Portal a partire da V14) o SIMATIC WinCC (TIA Portal a partire da V14), nell'edizione necessaria (Basic, Professional, Comfort/Advanced).

   Nota

   Il procedimento di installazione di TIA Portal in una macchina virtuale (VM) è identico a quello per l'installazione su un PG/PC. Maggiori dettagli sull'installazione si trovano nelle istruzioni per l'installazione di TIA Portal.

3. Se necessario, installare ulteriori pacchetti opzionali necessari, ad es. SIMATIC STEP 7 Safety Advanced.
4. Se necessario, installare ulteriori pacchetti software compatibili da mettere a disposizione di tutti gli utenti.
5. Configurare la VM in base alle proprie esigenze.
6. Creare un modello dalla VM in base alle istruzioni della propria piattaforma di virtualizzazione.

Risultato

È stato creato un modello di VM che può essere copiato e distribuito. Tenere presente, tuttavia, che per utilizzare una copia del modello devono essere disponibili le licenze necessarie. Per gestire le proprie licenze è possibile utilizzare un server delle licenze separato (VM).

Vedere anche

Salvataggio centrale delle impostazioni dell'utente e del progetto (Pagina 32)

Utilizzo del server per le chiavi di licenza (Pagina 34)

Installazione di TIA Portal Cloud Connector nella VM (Pagina 35)

3.2 Salvataggio centrale delle impostazioni dell'utente e del progetto

Se gli utenti della VM salvano le proprie impostazioni e i propri progetti all'interno della VM, impostazioni e progetti andranno persi una volta che si cancella la VM. Per rendere disponibili le impostazioni e i progetti anche in altre VM è necessario salvarle al di fuori della VM. Nella VM è possibile impostare variabili d'ambiente con i percorsi di salvataggio per impostazioni e progetti specifici dell'utente. Impostare le variabili d'ambiente prima di avviare TIA Portal per la prima volta. Se al primo avvio di TIA Portal non esistono variabili d'ambiente, TIA Portal salva il file per le impostazioni nella directory standard e in futuro utilizzerà sempre questo file. Finché esiste questo file, TIA Portal ignora variabili d'ambiente impostate a posteriori.

Con le variabili d'ambiente è possibile definire i seguenti percorsi:

- Impostazioni definite dall'utente: le impostazioni vengono salvate nella directory indicata.
- Progetti: il percorso di salvataggio indicato viene utilizzato come percorso standard alla creazione di un nuovo progetto. Tuttavia è possibile salvare un progetto in qualsiasi momento in un'altra directory.

Le variabili d'ambiente si possono impostare manualmente o con uno script. Per l'impostazione delle variabili d'ambiente per le impostazioni e per i progetti è possibile utilizzare uno script ciascuna oppure impostare entrambe le variabili d'ambiente con un unico script.

Il file per le impostazioni ha lo stesso nome per tutti gli utenti. Perché ogni utente possa accedere alle proprie impostazioni è necessario indicare una directory per ogni utente. In caso contrario le impostazioni verrebbero sempre sovrascritte da altri utenti. Utilizzando una variabile, è possibile adeguare il percorso all'utente di volta in volta connesso.

Esempio di struttura della directory per il salvataggio centrale delle impostazioni

Le impostazioni devono essere salvate in una directory "UserSettings" condivisa nella rete. La struttura sotto "UserSettings" è la seguente:

```
UserSettings
            User1
            User2
            User3
```

"`User1`", "`User2`" e "`User3`" sono i nomi degli utenti VM. Il percorso della variabile d'ambiente sarà "\\MyServer\UserSettings\%USERNAME%".

"MyServer" in questo esempio è una rete di computer accessibili. "%USERNAME%" è la variabile per il nome utente. Questa variabile viene risolta al momento della connessione dell'utente e la variabile d'ambiente viene modificata di conseguenza. Se questo deve avvenire per diversi utenti, si consiglia di salvare lo script nella directory dell'avvio automatico. La

variabile d'ambiente viene così reimpostata a ogni nuova connessione e il percorso di salvataggio per le impostazioni adeguato all'utente connesso.

Presupposti

- Tutti gli utenti hanno diritti di scrittura nelle aree server che devono essere utilizzate come nuovi percorsi di salvataggio.
- Le directory utente sono presenti.

Impostazione delle variabili d'ambiente con uno script

Per impostare le variabili d'ambiente con l'aiuto di uno script, procedere come segue:

1. Creare un nuovo script e aprirlo per modificarlo. In alternativa è possibile anche ampliare uno script esistente.
2. Inserire nello script le righe seguenti:
   `setx TiaUserSettingsPath \\<Server>\<Settings>\%USERNAME%`
   `setx TiaDefaultProjectPath \\<Server>\<Projects>\%USERNAME%`
   Sostituire "`<Server>\<Settings>`" e "`<Server>\<Projects>`" con le directory nella rete in cui salvare le impostazioni e i progetti.
3. Salvare lo script.
4. Per consentire l'uso dello script da parte di diversi utenti, copiarlo nella directory dell'avvio automatico di Windows.
   La variabile "%USERNAME%" viene risolta al momento della successiva connessione al dispositivo remoto. Il percorso di salvataggio per le impostazioni viene così adeguato all'utente connesso.

Se si preferisce utilizzare due script anziché uno, eseguire i passi da 1 a 4 per ogni script e inserire sempre solo uno dei due comandi "`setx`".

Impostazione manuale delle variabili d'ambiente

Per impostare le variabili d'ambiente manualmente, procedere come segue:

1. Avviare la VM da distribuire come modello.
2. Aprire la finestra per l'impostazione delle variabili d'ambiente in Windows.
3. Creare una nuova variabile di sistema con il nome "TiaUserSettingsPath".
4. Inserire come valore il percorso della directory nella rete in cui salvare le impostazioni utente. Tenere presente che il nome dell'utente deve essere inserito come variabile "%USERNAME%".
5. Confermare con "OK" i dati inseriti.
6. Creare un'ulteriore variabile di sistema con il nome "TiaDefaultProjectPath".

7. Inserire come valore il percorso della directory nella rete da utilizzare come percorso standard per i progetti. È possibile inserire il nome dell'utente come variabile "%USERNAME%“ per salvare i progetti in altre sottodirectory. Se si omette di indicare "%USERNAME%", tutti i progetti vengono salvati nella stessa directory.
8. Confermare con "OK" i dati inseriti.
   La variabile "%USERNAME%" viene risolta al momento della successiva connessione al PG/PC. Il percorso di salvataggio per le impostazioni viene così adeguato all'utente connesso.

Vedere anche

Creazione di un nuovo modello VM (Pagina 31)

Utilizzo del server per le chiavi di licenza (Pagina 34)

Installazione di TIA Portal Cloud Connector nella VM (Pagina 35)

3.3 Utilizzo del server per le chiavi di licenza

Introduzione

Al momento dell'installazione di TIA Portal o di TIA Portal Cloud Connector viene installato anche Automation License Manager (ALM). Quest'ultimo è necessario per il trasferimento e la gestione delle licenze.

Maggiori informazioni su Automation License Manager e sulla configurazione di un server delle licenze sono disponibili nella documentazione utente di Automation License Manager.

Vedere anche

Licenze (Pagina 27)

Assegnazione di una licenza del dispositivo utente (Pagina 27)

Creazione di un nuovo modello VM (Pagina 31)

Salvataggio centrale delle impostazioni dell'utente e del progetto (Pagina 32)

Installazione di TIA Portal Cloud Connector nella VM (Pagina 35)

3.4 Installazione di TIA Portal Cloud Connector nella VM

TIA Portal Cloud Connector si può installare nella VM in due modi diversi:

- Installazione di TIA Portal Cloud Connector insieme a TIA Portal
  TIA Portal Cloud Connector si può installare insieme a TIA Portal. In questo caso, attivare l'opzione "TIA Portal Cloud Connector" durante l'installazione.
- Installazione di TIA Portal Cloud Connector senza TIA Portal
  Inoltre, sul supporto di installazione si trova un programma Setup con cui si può installare TIA Portal Cloud Connector senza TIA Portal. Questo file di installazione può essere messo a disposizione anche di altri utenti attraverso un drive di rete.

Installazione di Cloud Connector insieme a TIA Portal

Per installare Cloud Connector insieme a TIA Portal procedere nel modo seguente:

1. Inserire il supporto dati per l'installazione nell'apposito lettore.
   Se la funzione di avvio automatico non è disattivata sul PG/PC il programma di setup si avvia automaticamente.
2. Se il programma di setup non si avvia automaticamente, avviarlo manualmente facendo doppio clic sul file "Start.exe".
   Si apre la finestra di dialogo per la selezione della lingua di setup.
3. Selezionare la lingua nella quale si desiderano visualizzare le finestre di dialogo del programma di setup.
4. Per leggere le avvertenze sull'installazione e sul prodotto, fare clic sul pulsante "Leggi le avvertenze" oppure "Avvertenze di installazione".
   Si apre il file della Guida con le avvertenze richieste.
5. Terminata la lettura chiudere questo file e fare clic sul pulsante "Avanti".
   Si apre la finestra di dialogo per la selezione delle lingue del prodotto.
6. Selezionare le lingue per l'interfaccia utente del prodotto e fare clic sul pulsante "Avanti".

   Nota

   La lingua "Inglese" viene sempre installata come lingua di base del prodotto.

   Si apre la finestra di dialogo per la selezione della configurazione del prodotto.
7. Fare clic sul pulsante "Personalizzato".
8. Attivare la casella di scelta "TIA Portal Cloud Connector" ed eventualmente le caselle per ulteriori prodotti da installare.
9. Se si vuole creare un collegamento per TIA Portal sul desktop, attivare la casella di scelta "Crea un link sul desktop".
10. Se si desidera modificare la directory di destinazione per l'installazione fare clic sul pulsante "Sfoglia". Assicurarsi che il percorso di installazione non superi una lunghezza di 89 caratteri.
11. Fare clic sul pulsante "Avanti".
    Si apre la finestra di dialogo delle condizioni di licenza.

12. Per proseguire con l'installazione, leggere e accettare tutte le condizioni di licenza e fare clic su "Avanti".
    La finestra di dialogo per le impostazioni di sicurezza si apre nel caso in cui l'installazione di TIA Portal richieda la modifica delle impostazioni di sicurezza e dei diritti.
13. Per proseguire con l'installazione, accettare le modifiche delle impostazioni di sicurezza e dei diritti e fare clic sul pulsante "Avanti".
    Nella finestra di dialogo successiva viene visualizzato un riepilogo delle impostazione di installazione.
14. Controllare le impostazioni di installazione scelte. Per introdurre eventuali modifiche premere il pulsante "Indietro" fino a tornare al punto da modificare nella finestra di dialogo. Dopo aver apportato le modifiche desiderate, tornare alla Vista generale con il pulsante "Avanti".
15. Fare clic sul pulsante "Installa".
    L'installazione viene avviata.

    Nota

    Se durante l'installazione sul PC non viene rilevata la chiave di licenza, sussiste la possibilità di eseguire ora il trasferimento. Il trasferimento può anche essere saltato ed eseguito in un secondo momento in Automation License Manager.

    Dopo l'installazione viene visualizzato un messaggio che segnala se l'installazione è riuscita o meno.

16. Potrebbe essere necessario riavviare il computer. In questo caso attivare l'opzione "Sì, riavvia ora il sistema". Successivamente fare clic sul pulsante "Riavvio".
17. Se il sistema non deve essere riavviato, fare clic sul pulsante "Fine".

Installazione di Cloud Connector senza TIA Portal

Per installare Cloud Connector senza TIA Portal procedere nel modo seguente:

1. Inserire il supporto dati per l'installazione nell'apposita unità o cercare il file di installazione nel sistema di file del computer.
   Sul supporto di installazione si trova il file di installazione nella directory "Support".
2. Fare doppio clic sul file di installazione "TIA Portal Cloud Connector_<versione>.exe".
   Viene visualizzato il controllo dell'account utente di Windows.
3. Confermare il controllo dell'account utente con "Sì".
   Si apre la finestra di dialogo di installazione.
4. Fare clic su "Avanti".
   Vengono visualizzate alcune delle lingue di setup disponibili.
5. Selezionare la lingua di setup desiderata e fare clic su "Avanti".
   I file necessari vengono decompressi e si apre la finestra di installazione successiva.
6. Chiudere eventuali programmi in esecuzione e fare clic su "Avanti".
   Vengono visualizzate le condizioni di licenza.
7. Accettare le condizioni di licenza e fare clic su "Avanti".
   Vengono visualizzati i programmi disponibili per l'installazione e lo spazio di memoria necessario.

8. Fare clic su "Avanti".
   Si apre una finestra di dialogo in cui è visualizzata una panoramica delle impostazioni di sistema che vengono modificate durante l'installazione.
9. Attivare la casella di scelta per accettare le modifiche.
10. Fare clic su "Avanti".
    Viene visualizzata una panoramica dei programmi da installare.
11. Fare clic su "Installa".
    L'installazione viene avviata.
12. Potrebbe essere necessario riavviare il computer. In questo caso attivare l'opzione "Sì, riavvia ora il sistema". Successivamente fare clic sul pulsante "Fine".

Vedere anche

Creazione di un nuovo modello VM (Pagina 31)

Salvataggio centrale delle impostazioni dell'utente e del progetto (Pagina 32)

Utilizzo del server per le chiavi di licenza (Pagina 34)

Utilizzo della macchina virtuale (VM) 4

4.1 Installazione di TIA Portal Cloud Connector sul PG/PC

Nota

Prestare attenzione a quanto segue:

- Per TIA Portal Cloud Connector è necessaria una licenza valida.
- Impostazioni nel firewall di Windows: Per stabilire un collegamento in entrata è necessario che nel firewall, nella scheda "Eccezioni" del service "Siemens SCP Remote Connection", sia indicata la porta utilizzata dal TIA Portal Cloud Connector. È preimpostato "Qualsiasi".

Procedura

Per installare TIA Portal Cloud Connector, procedere nel seguente modo:

1. Inserire il supporto dati per l'installazione nell'apposita unità o cercare il file di installazione nel sistema di file del computer.
   Sul supporto di installazione si trova il file di installazione nella directory "Support".
2. Fare doppio clic sul file di installazione "TIA Portal Cloud Connector_<versione>.exe".
   Viene visualizzato il controllo dell'account utente di Windows.
3. Confermare il controllo dell'account utente con "Sì".
   Si apre la finestra di dialogo di installazione.
4. Fare clic su "Avanti".
   Vengono visualizzate alcune delle lingue di setup disponibili.
5. Selezionare la lingua di setup desiderata e fare clic su "Avanti".
   I file necessari vengono decompressi e si apre la finestra di installazione successiva.
6. Chiudere eventuali programmi in esecuzione e fare clic su "Avanti".
   Vengono visualizzate le condizioni di licenza.
7. Accettare le condizioni di licenza e fare clic su "Avanti".
   Vengono visualizzati i programmi disponibili per l'installazione e lo spazio di memoria necessario.
8. Fare clic su "Avanti".
   Si apre una finestra di dialogo in cui è visualizzata una panoramica delle impostazioni di sistema che vengono modificate durante l'installazione.
9. Attivare la casella di scelta per accettare le modifiche.
10. Fare clic su "Avanti".
    Viene visualizzata una panoramica dei programmi da installare.

11. Fare clic su "Installa".
    L'installazione viene avviata.
12. Potrebbe essere necessario riavviare il computer. In questo caso attivare l'opzione "Sì, riavvia ora il sistema". Successivamente fare clic sul pulsante "Fine".

Vedere anche

Configurazione di TIA Portal Cloud Connector sul PG/PC (Pagina 40)

Configurazione di TIA Portal Cloud Connector nella VM (Pagina 42)

Collegamento online attraverso TIA Portal Cloud Connector (Pagina 54)

Utilizzo della macchina virtuale (VM) offline (Pagina 55)

4.2 Configurazione di TIA Portal Cloud Connector sul PG/PC

Nota

Protocollo di comunicazione

Per consentire al proprio PG/PC di creare un collegamento alla VM, è necessario definire un protocollo di comunicazione. A partire da Windows 8.1, per motivi di sicurezza è opportuno utilizzare sempre HTTPS.

Configurazione del collegamento TCP

Per configurare un collegamento TCP per il PG/PC, procedere nel seguente modo:

1. Con il tasto destro del mouse fare clic sull'icona di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni e selezionare il comando "Configurazione".
   TIA Portal Cloud Connector si apre.
2. Aprire la scheda "Impostazioni" ed eventualmente modificare la lingua dell'interfaccia utente di TIA Portal Cloud Connector.
3. Passare alla scheda "Generale" e controllare il ruolo di comunicazione. Eventualmente modificare l'impostazione in "Dispositivo utente".
4. Passare alla scheda "Protocollo".
5. Attivare la casella di scelta "Punto finale TCP".
6. Indicare la porta attraverso la quale deve essere eseguita la comunicazione. La porta deve essere identica a quella assegnata nel dispositivo remoto.
7. Aprire nuovamente la scheda "Generale".
8. Nell'area "Comunicazione Cloud Connector" fare clic sul pulsante "Attiva la comunicazione".

Configurazione del collegamento HTTPS

Per configurare un collegamento HTTPS per il PG/PC, procedere nel seguente modo:

1. Con il tasto destro del mouse fare clic sull'icona di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni e selezionare il comando "Configurazione".
   TIA Portal Cloud Connector si apre.
2. Aprire la scheda "Impostazioni" ed eventualmente modificare la lingua dell'interfaccia utente di TIA Portal Cloud Connector.
3. Passare alla scheda "Generale" e controllare il ruolo di comunicazione. Eventualmente modificare l'impostazione in "Dispositivo utente".
4. Passare alla scheda "Protocollo".
5. Attivare la casella opzione "Punto finale HTTPS".
6. Creare un nuovo certificato per la crittografia dei dati o selezionare un certificato già esistente dall'archivio certificati Windows.
   Vedere anche:
   Creazione del certificato per la crittografia dei dati (Pagina 44)
   Selezione del certificato per la crittografia dei dati (Pagina 47)
7. Se non si dispone ancora di un certificato per l'autenticazione utente nel dispositivo utente, creare il certificato nel dispositivo remoto e copiarlo nel drive locale del dispositivo utente.
   Vedere anche:
   Creazione del certificato per l'autenticazione utente (Pagina 48)
8. Passare alla scheda "Impostazioni".
9. Importare un nuovo certificato per l'autenticazione utente o aggiungere un certificato esistente dell'archivio certificati di Windows all'elenco dei certificati attendibili.
   Vedere anche:
   Importazione del certificato per l'autenticazione utente (Pagina 50)
   Aggiunta del certificato per l'autenticazione utente (Pagina 51)
10. Aprire nuovamente la scheda "Generale".
11. Nell'area "Comunicazione Cloud Connector" fare clic sul pulsante "Attiva la comunicazione".

Risultato

Il PG/PC è pronto per la comunicazione con la VM. Come passo successivo configurare TIA Portal Cloud Connector nella VM.

Vedere anche

Installazione di TIA Portal Cloud Connector sul PG/PC (Pagina 39)

Configurazione di TIA Portal Cloud Connector nella VM (Pagina 42)

Collegamento online attraverso TIA Portal Cloud Connector (Pagina 54)

Utilizzo della macchina virtuale (VM) offline (Pagina 55)

4.3 Configurazione di TIA Portal Cloud Connector nella VM

Nota

Protocollo di comunicazione

Per consentire a un PG/PC di creare un collegamento alla VM, è necessario definire il protocollo di comunicazione da utilizzare. A partire da Windows 8.1, per motivi di sicurezza è opportuno utilizzare sempre HTTPS. Inoltre, controllare l'identità del partner richiedente prima di accettare un collegamento.

Configurazione del collegamento TCP

Per configurare un collegamento TCP per la VM, procedere nel modo seguente:

1. Creare una connessione desktop remoto con la VM.
2. Con il tasto destro del mouse fare clic sull'icona di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni e selezionare il comando "Configurazione". TIA Portal Cloud Connector si apre.
3. Aprire la scheda "Impostazioni" ed eventualmente modificare la lingua dell'interfaccia utente di TIA Portal Cloud Connector.
4. Passare alla scheda "Generale" e controllare il ruolo di comunicazione. Eventualmente modificare l'impostazione in "Dispositivo remoto".
5. Aprire la scheda "Protocollo".
6. Nell'area "Protocollo di comunicazione" attivare la casella opzione "Impostazioni TCP".
7. Selezionare un sistema di destinazione.

   Nota

   Collegamento a SCALANCE

   Assicurarsi che il collegamento a SCALANCE con SINEMA RC o un'altra tecnologia crittografica sia sicuro. Altrimenti il trasferimento avviene in modo non crittografata.

8. Inserire l'indirizzo IP del dispositivo utente o selezionare dalla casella di riepilogo la voce "Configurazione automatica" per far rilevare l'indirizzo automaticamente.
9. Indicare la porta attraverso la quale deve essere eseguita la comunicazione. La porta deve essere identica a quella assegnata nel dispositivo utente.
10. Aprire nuovamente la scheda "Generale".
11. Nell'area "Comunicazione Cloud Connector" fare clic sul pulsante "Attiva la comunicazione".

Configurazione del collegamento HTTPS

Per configurare un collegamento HTTPS per la VM, procedere nel modo seguente:

1. Creare una connessione desktop remoto con la VM.
2. Con il tasto destro del mouse fare clic sull'icona di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni e selezionare il comando "Configurazione".
   TIA Portal Cloud Connector si apre.
3. Aprire la scheda "Impostazioni" ed eventualmente modificare la lingua dell'interfaccia utente di TIA Portal Cloud Connector.
4. Aprire la scheda "Generale" e controllare il ruolo di comunicazione. Eventualmente modificare l'impostazione in "Dispositivo remoto".
5. Aprire la scheda "Protocollo".
6. Nell'area "Protocollo di comunicazione" attivare la casella opzione "Impostazioni HTTPS".
7. Inserire l'indirizzo IP del dispositivo utente o selezionare dalla casella di riepilogo la voce "Configurazione automatica" per far rilevare l'indirizzo automaticamente.
8. Importare il certificato per la crittografia dei dati creato nel dispositivo utente o selezionare un certificato già esistente dall'archivio certificati di Windows.
   Vedere anche:
   Importazione del certificato per la crittografia dei dati (Pagina 46)
   Selezione del certificato per la crittografia dei dati (Pagina 47)
9. Passare alla scheda "Impostazioni".
10. Creare un nuovo certificato per l'autenticazione utente o selezionare un certificato già esistente dall'archivio certificati di Windows.
    Vedere anche:
    Creazione del certificato per l'autenticazione utente (Pagina 48)
    Selezione del certificato per l'autenticazione utente (Pagina 52)
11. Aprire nuovamente la scheda "Generale".
12. Nell'area "Comunicazione Cloud Connector" fare clic sul pulsante "Attiva la comunicazione".

Risultato

TIA Portal Cloud Connector è pronto per la comunicazione. Dopo l'attivazione di entrambi i partner di comunicazione è possibile accedere dal dispositivo utente all'hardware SIMATIC collegato localmente (PLC/HMI).

Vedere anche

Installazione di TIA Portal Cloud Connector sul PG/PC (Pagina 39)

Configurazione di TIA Portal Cloud Connector sul PG/PC (Pagina 40)

Collegamento online attraverso TIA Portal Cloud Connector (Pagina 54)

Utilizzo della macchina virtuale (VM) offline (Pagina 55)

4.4 Utilizzo di certificati (solo per collegamenti HTTPS)

4.4.1 Creazione del certificato per la crittografia dei dati

A partire da Windows 8.1 è possibile utilizzare un collegamento HTTPS per la comunicazione. Per aumentare la sicurezza è necessario un certificato per la crittografia dei dati, creato nel dispositivo utente e utilizzato quindi dal dispositivo remoto.

Procedura

Per creare un certificato per la crittografia dati procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull'icona di stato di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni di Windows nel dispositivo utente.
2. Nel menu di scelta rapida selezionare il comando "Configurazione (dispositivo utente)". Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda "Protocollo".
4. Attivare la casella opzione "Punto finale HTTPS". Vengono attivati i pulsanti "Crea" e "Seleziona".
5. Fare clic su "Crea". Si apre la finestra di dialogo "TIA Portal Cloud Connector - Crea certificato".
6. Inserire un nome per il dominio oppure selezionare un dominio dalla casella di riepilogo.

   Nota

   Dal pulsante "+" è possibile acquisire domini nell'elenco domini. Il pulsante "-" consente di rimuovere nuovamente un dominio dall'elenco dei domini.

7. Fare clic sul pulsante "Sfoglia". Si apre la finestra di dialogo "Salva con nome".
8. Selezionare un percorso di salvataggio e inserire un nome di file per il certificato.
9. Fare clic su "Salva".
10. Selezionare la data a partire dalla quale il certificato deve essere valido.
11. Selezionare la data fino alla quale il certificato deve essere valido.
12. Fare clic su "OK".

Risultato

Il certificato viene creato e utilizzato per il punto finale HTTPS nel dispositivo utente. Inoltre, nel percorso di salvataggio indicato esso viene salvato come file con l'estensione ".cer" nel nome del file e da qui può essere copiato nel dispositivo remoto. Il certificato è inoltre stato aggiunto all'archivio certificati di Windows.

Vedere anche

Utilizzo di certificati (Pagina 20)

Esportazione del certificato per la crittografia dei dati (Pagina 45)

Importazione del certificato per la crittografia dei dati (Pagina 46)

Selezione del certificato per la crittografia dei dati (Pagina 47)

4.4.2 Esportazione del certificato per la crittografia dei dati

Il certificato attualmente utilizzato per la crittografia dei dati può essere esportato in qualsiasi momento.

Presupposti

Il certificato per la crittografia dei dati è stato dapprima creato e viene visualizzato nel punto finale HTTPS del dispositivo utente.

Procedura

Per esportare un certificato per la crittografia dati procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull'icona di stato di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni di Windows nel dispositivo utente.
2. Nel menu di scelta rapida selezionare il comando "Configurazione (dispositivo utente)". Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda "Protocollo".
4. Attivare la casella opzione "Punto finale HTTPS". Vengono attivati i pulsanti "Crea", "Seleziona" e "Esporta".
5. Fare clic su "Esporta". Si apre la finestra di dialogo "Salva con nome".
6. Selezionare un percorso di salvataggio e inserire un nome per il nuovo certificato.
7. Fare clic su "Salva".

Risultato

Il certificato attualmente utilizzato per la crittografia dei dati viene salvato come file con l'estensione ".cer" nel nome del file.

Vedere anche

Utilizzo di certificati (Pagina 20)

Creazione del certificato per la crittografia dei dati (Pagina 44)

Importazione del certificato per la crittografia dei dati (Pagina 46)

Selezione del certificato per la crittografia dei dati (Pagina 47)

4.4.3 Importazione del certificato per la crittografia dei dati

Per poter realizzare un collegamento HTTPS tra il dispositivo utente e il dispositivo remoto è necessario importare il certificato creato nel dispositivo utente per la crittografia dei dati nel TIA Portal Cloud Connector del dispositivo remoto.

Presupposti

- Il certificato per la crittografia dei dati è stato creato nel dispositivo utente.
- Il certificato per la crittografia dei dati è stato copiato nel drive locale del dispositivo remoto.

Procedura

Per importare un certificato per la crittografia dati nel TIA Portal Cloud Connector del dispositivo remoto procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull'icona di stato di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni di Windows nel dispositivo remoto.
2. Nel menu di scelta rapida selezionare il comando "Configurazione (dispositivo remoto)". Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda "Protocollo".
4. Attivare l'opzione "Impostazioni HTTPS". Vengono attivati i pulsanti "Importa" e "Seleziona".
5. Fare clic su "Importa". Si apre la finestra di dialogo "Apri".
6. Selezionare il file del certificato nel sistema di file. I file del certificato sono riconoscibili dall'estensione ".cer" nel nome del file.
7. Fare clic su "Apri".

Risultato

Il certificato viene importato e utilizzato subito per la comunicazione. Il certificato è inoltre stato aggiunto all'archivio certificati di Windows.

Vedere anche

Utilizzo di certificati (Pagina 20)

Creazione del certificato per la crittografia dei dati (Pagina 44)

Esportazione del certificato per la crittografia dei dati (Pagina 45)

Selezione del certificato per la crittografia dei dati (Pagina 47)

4.4.4 Selezione del certificato per la crittografia dei dati

Dall'archivio dei certificati di Windows è possibile selezionare un certificato per la crittografia dei dati. Questa selezione è possibile sia nel dispositivo utente sia nel dispositivo remoto.

Presupposti

Il certificato per la crittografia dei dati è stato dapprima creato (dispositivo utente) o importato (dispositivo remoto) ed è disponibile nell'archivio dei certificati di Windows.

Procedura

Per selezionare e utilizzare un certificato esistente per la crittografia dei dati dall'archivio dei certificati di Windows procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull'icona di stato di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni di Windows.
2. Nel menu di scelta rapida selezionare il comando "Configurazione (dispositivo utente)" o "Configurazione (dispositivo remoto)".
   Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda "Protocollo".
4. Attivare la casella opzione "Punto finale HTTPS" (dispositivo utente) o la casella opzione "Impostazioni HTTPS" (dispositivo remoto).
   Si attiva il pulsante "Seleziona".
5. Fare clic su "Seleziona".
   Si apre la finestra di dialogo "Sicurezza di Windows" e vengono visualizzati i certificati disponibili.
6. Selezionare un certificato. Se necessario è possibile visualizzare ulteriori proprietà del certificato.
7. Fare clic su "OK".

Risultato

Il certificato selezionato viene utilizzato per la comunicazione. Per consentire una comunicazione, nel dispositivo utente e nel dispositivo remoto deve essere impostato lo stesso certificato.

Vedere anche

Utilizzo di certificati (Pagina 20)

Creazione del certificato per la crittografia dei dati (Pagina 44)

Esportazione del certificato per la crittografia dei dati (Pagina 45)

Importazione del certificato per la crittografia dei dati (Pagina 46)

4.4.5 Creazione del certificato per l'autenticazione utente

A partire da Windows 8.1 è possibile utilizzare un collegamento HTTPS per la comunicazione. Per aumentare la sicurezza è necessario un certificato per l'autenticazione utente, creato nel dispositivo remoto e utilizzato quindi dal dispositivo utente.

Procedura

Per creare un certificato per l'autenticazione utente procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull'icona di stato di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni di Windows nel dispositivo remoto.
2. Nel menu di scelta rapida selezionare il comando "Configurazione (dispositivo remoto)". Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda "Protocollo".
4. Attivare l'opzione "Impostazioni HTTPS". Nella scheda "Impostazioni" viene attivata l'area per l'autenticazione utente.
5. Passare alla scheda "Impostazioni".
6. Nell'area "Autenticazione utente" fare clic sul pulsante "Crea". Si apre la finestra di dialogo "TIA Portal Cloud Connector - Autenticazione utente".
7. Nella casella "Nome del certificato" indicare un nome per il nuovo certificato.
8. Fare clic sul pulsante "Sfoglia". Si apre la finestra di dialogo "Salva con nome".
9. Selezionare un percorso di salvataggio e inserire un nome di file per il nuovo certificato.
10. Fare clic su "Salva".
11. Selezionare la data a partire dalla quale il certificato deve essere valido.
12. Selezionare la data fino alla quale il certificato deve essere valido.
13. Fare clic su "OK".

Risultato

Il certificato viene creato e utilizzato nel dispositivo remoto. Inoltre, nel percorso di salvataggio indicato esso viene salvato come file con l'estensione ".cer" nel nome del file e da qui può essere copiato nel dispositivo utente. Il certificato è inoltre stato aggiunto all'archivio certificati di Windows.

Vedere anche

Utilizzo di certificati (Pagina 20)
Esportazione del certificato per l’autenticazione utente (Pagina 49)
Importazione del certificato per l’autenticazione utente (Pagina 50)
Aggiunta del certificato per l’autenticazione utente (Pagina 51)
Selezione del certificato per l’autenticazione utente (Pagina 52)
Eliminazione del certificato per l’autenticazione utente (Pagina 53)

4.4.6 Esportazione del certificato per l’autenticazione utente

Durante la creazione del certificato per l’autenticazione utente è necessario esportare il certificato per metterlo a disposizione di un dispositivo utente. Il certificato attualmente utilizzato può essere esportato di nuovo in qualsiasi momento.

Presupposti

Il certificato per l’autenticazione utente è stato dapprima creato nel dispositivo remoto e viene visualizzato nella scheda “Impostazioni" in “Autenticazione utente".

Procedura

Per esportare un certificato per l’autenticazione utente procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull’icona di stato di TIA Portal Cloud Connector nell’area di notifica della barra delle applicazioni di Windows nel dispositivo remoto.
2. Nel menu di scelta rapida selezionare il comando “Configurazione (dispositivo remoto)". Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda “Protocollo".
4. Attivare l'opzione “Impostazioni HTTPS". Nella scheda “Impostazioni" viene attivata l’area per l’autenticazione utente.
5. Passare alla scheda “Impostazioni".
6. Nell'area "Autenticazione utente" fare clic sul pulsante "Esporta". Si apre la finestra di dialogo "Salva con nome".
7. Selezionare un percorso di salvataggio e inserire un nome per il nuovo certificato.
8. Fare clic su "Salva".

Risultato

Il certificato attualmente utilizzato per l’autenticazione utente viene salvato come file con l’estensione ".cer" nel nome del file.

Vedere anche

Utilizzo di certificati (Pagina 20)
Creazione del certificato per l'autenticazione utente (Pagina 48)
Importazione del certificato per l'autenticazione utente (Pagina 50)
Aggiunta del certificato per l'autenticazione utente (Pagina 51)
Selezione del certificato per l'autenticazione utente (Pagina 52)
Eliminazione del certificato per l'autenticazione utente (Pagina 53)

4.4.7 Importazione del certificato per l'autenticazione utente

Per poter realizzare un collegamento HTTPS tra il dispositivo utente e il dispositivo remoto è necessario importare il certificato creato nel dispositivo remoto per l'identificazione utente nel TIA Portal Cloud Connector del dispositivo utente.

Presupposti

- Il certificato per l'autenticazione utente è stato creato nel dispositivo remoto.
- Il certificato per l'autenticazione utente è stato copiato nel drive locale del dispositivo utente.

Procedura

Per importare un certificato per l'autenticazione utente procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull'icona di stato di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni di Windows nel dispositivo utente.
2. Nel menu di scelta rapida selezionare il comando "Configurazione (dispositivo utente)". Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda "Protocollo".
4. Attivare la casella opzione "Punto finale HTTPS". Nella scheda "Impostazioni" viene attivata l'area per l'autenticazione utente.
5. Passare alla scheda "Impostazioni".
6. Nell'area "Autenticazione utente" fare clic sul pulsante "Importa". Si apre la finestra di dialogo "Apri".
7. Selezionare il file del certificato nel sistema di file. I file del certificato sono riconoscibili dall'estensione ".cer" nel nome del file.
8. Fare clic su "Apri".

Risultato

Il certificato viene importato e aggiunto all'elenco dei certificati attendibili. Da questo elenco è possibile definire i dispositivi remoti con i quali può comunicare il dispositivo utente. Il rispettivo dispositivo remoto richiamato deve avere associato lo stesso certificato per l'autenticazione utente.

Vedere anche

Utilizzo di certificati (Pagina 20)

Creazione del certificato per l'autenticazione utente (Pagina 48)

Esportazione del certificato per l'autenticazione utente (Pagina 49)

Aggiunta del certificato per l'autenticazione utente (Pagina 51)

Selezione del certificato per l'autenticazione utente (Pagina 52)

Eliminazione del certificato per l'autenticazione utente (Pagina 53)

4.4.8 Aggiunta del certificato per l'autenticazione utente

Anziché importare un certificato dal sistema di file, è anche possibile aggiungere un certificato dell'archivio dei certificati di Windows all'elenco dei certificati attendibili.

Presupposti

Il certificato desiderato è disponibile nell'archivio dei certificati di Windows.

Procedura

Per aggiungere un certificato per l'autenticazione utente dall'archivio dei certificati di Windows procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull'icona di stato di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni di Windows nel dispositivo utente.
2. Nel menu di scelta rapida selezionare il comando "Configurazione (dispositivo utente)". Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda "Protocollo".
4. Attivare la casella opzione "Punto finale HTTPS". Nella scheda "Impostazioni" viene attivata l'area per l'autenticazione utente.
5. Passare alla scheda "Impostazioni".
6. Nell'area "Autenticazione utente" fare clic sul pulsante "Aggiungi". Si apre la finestra di dialogo "Seleziona certificato" e vengono visualizzati i certificati disponibili.
7. Selezionare un certificato. Se necessario è possibile visualizzare il certificato.
8. Fare clic su "OK".

Risultato

Il certificato dell'archivio dei certificati di Windows viene aggiunto all'elenco dei certificati attendibili. Da questo elenco è possibile definire i dispositivi remoti con i quali può comunicare il dispositivo utente. Il rispettivo dispositivo remoto richiamato deve avere associato lo stesso certificato per l'autenticazione utente.

Vedere anche

Utilizzo di certificati (Pagina 20)

Creazione del certificato per l'autenticazione utente (Pagina 48)

Esportazione del certificato per l'autenticazione utente (Pagina 49)

Importazione del certificato per l'autenticazione utente (Pagina 50)

Selezione del certificato per l'autenticazione utente (Pagina 52)

Eliminazione del certificato per l'autenticazione utente (Pagina 53)

4.4.9 Selezione del certificato per l'autenticazione utente

Anziché creare nel dispositivo remoto un nuovo certificato per l'autenticazione utente, è anche possibile selezionare e utilizzare un certificato esistente nell'archivio dei certificati di Windows.

Presupposti

Il certificato per l'autenticazione utente è stato dapprima creato ed è disponibile nell'archivio dei certificati di Windows.

Procedura

Per selezionare un certificato per l'autenticazione utente dall'archivio dei certificati di Windows procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull'icona di stato di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni di Windows nel dispositivo remoto.
2. Nel menu di scelta rapida selezionare il comando "Configurazione (dispositivo remoto)". Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda "Protocollo".
4. Attivare l'opzione "Impostazioni HTTPS". Nella scheda "Impostazioni" viene attivata l'area per l'autenticazione utente.
5. Passare alla scheda "Impostazioni".
6. Nell'area "Autenticazione utente" fare clic sul pulsante "Seleziona". Si apre la finestra di dialogo "Sicurezza di Windows" e vengono visualizzati i certificati disponibili.

7. Selezionare un certificato. Se necessario è possibile visualizzare ulteriori proprietà del certificato.
8. Fare clic su "OK".

Risultato

Il certificato viene utilizzato nel dispositivo remoto per l'autenticazione utente. Se necessario esso può essere esportato per essere scambiato con il dispositivo utente.

Vedere anche

Utilizzo di certificati (Pagina 20)
Creazione del certificato per l'autenticazione utente (Pagina 48)
Esportazione del certificato per l'autenticazione utente (Pagina 49)
Importazione del certificato per l'autenticazione utente (Pagina 50)
Aggiunta del certificato per l'autenticazione utente (Pagina 51)
Eliminazione del certificato per l'autenticazione utente (Pagina 53)

4.4.10 Eliminazione del certificato per l'autenticazione utente

Nel dispositivo utente è possibile eliminare di nuovo in qualsiasi momento un certificato per l'autenticazione utente dall'elenco dei certificati attendibili.

Procedura

Per eliminare un certificato per l'autenticazione utente dall'elenco dei certificati attendibili procedere nel modo seguente:

1. Per aprire TIA Portal Cloud Connector, con il tasto destro del mouse fare clic sull'icona di stato di TIA Portal Cloud Connector nell'area di notifica della barra delle applicazioni di Windows nel dispositivo utente.
2. Nel menu di scelta rapida selezionare il comando "Configurazione (dispositivo utente)". Si apre la finestra di configurazione di TIA Portal Cloud Connector.
3. Passare alla scheda "Protocollo".
4. Attivare la casella opzione "Punto finale HTTPS". Nella scheda "Impostazioni" viene attivata l'area per l'autenticazione utente.
5. Passare alla scheda "Impostazioni".
6. Selezionare il certificato che si desidera eliminare nell'elenco dei certificati attendibili.
7. Nell'area "Autenticazione utente" fare clic sul pulsante "Rimuovi".

Risultato

Il certificato viene eliminato dall'elenco dei certificati attendibili. Non è più possibile un collegamento con il dispositivo remoto che utilizza questo certificato per l'autenticazione utente.

Vedere anche

Utilizzo di certificati (Pagina 20)

Creazione del certificato per l'autenticazione utente (Pagina 48)

Esportazione del certificato per l'autenticazione utente (Pagina 49)

Importazione del certificato per l'autenticazione utente (Pagina 50)

Aggiunta del certificato per l'autenticazione utente (Pagina 51)

Selezione del certificato per l'autenticazione utente (Pagina 52)

4.5 Collegamento online attraverso TIA Portal Cloud Connector

Introduzione

Se si utilizza TIA Portal Cloud Connector per il collegamento all'hardware, l'utilizzo di TIA Portal non è diverso da un normale collegamento online con l'hardware. Non appena si è attivata la comunicazione via tunnel, è possibile compilare, caricare o controllare i dati come sempre.

Per maggiori informazioni sulla creazione di un collegamento online e sull'utilizzo della modalità online consultare la Guida in linea a TIA Portal.

Panoramica dei simboli di stato

Quando si crea un collegamento online attraverso TIA Portal Cloud Connector, nell'area di notifica della barra delle applicazioni di Windows vengono visualizzati dei simboli che indicano lo stato del collegamento. La seguente tabella mostra una panoramica dei simboli di stato con relativo significato:

Simbolo di stato	Significato
	La comunicazione è disattivata.
	La comunicazione è attivata, tuttavia non avviene nessuno scambio di dati tra TIA Portal e l'hardware di automazione SIMATIC.
	La comunicazione è attivata, tra TIA Portal e l'hardware di automazione SIMATIC avviene uno scambio di dati.
	Lo scambio di dati tra TIA Portal e l'hardware di automazione SIMATIC è stato interrotto. Viene visualizzata la visualizzazione di stato, che contiene ulteriori dettagli sulla causa.

Visualizzazione di stato

Dall'area di notifica nella barra delle applicazioni di Windows è possibile visualizzare una visualizzazione di stato sia sul dispositivo remoto che sul dispositivo utente. Si apre la finestra "TIA Portal Cloud Connector - Dispositivo remoto" o "TIA Portal Cloud Connector - Dispositivo utente". In questa finestra si trovano tutte le informazioni, gli avvisi e i messaggi di errore del TIA Portal Cloud Connector. Inoltre viene visualizzato da quanto tempo è attivo un collegamento TCP o HTTPS.

La visualizzazione di stato si può chiudere in qualsiasi momento.

Vedere anche

Installazione di TIA Portal Cloud Connector sul PG/PC (Pagina 39)

Configurazione di TIA Portal Cloud Connector sul PG/PC (Pagina 40)

Configurazione di TIA Portal Cloud Connector nella VM (Pagina 42)

Utilizzo della macchina virtuale (VM) offline (Pagina 55)

4.6 Utilizzo della macchina virtuale (VM) offline

Una macchina virtuale si può utilizzare anche offline. Allo scopo è possibile copiare la VM dal dispositivo remoto al proprio PG/PC. In seguito è possibile avviare la VM sul PG/PC e utilizzare TIA Portal con l'hardware collegato al PG/PC o alla rete.

Esistono le seguenti possibilità di utilizzare la VM:

- L'hardware è collegato al proprio PG/PC attraverso Ethernet e si trova nella stessa sottorete.
- L'hardware è collegato al proprio PG/PC attraverso Ethernet o PROFIBUS e si trova in un'altra sottorete.

TIA Portal Cloud Connector non è necessario per tutti i tipi di collegamento. Si distinguono i casi seguenti:

- Se l'hardware è collegato direttamente al proprio PG/PC con un adattatore Ethernet o USB, è possibile impostare "Bridged" come collegamento di rete.
  Per questo genere di collegamento, TIA Portal Cloud Connector deve essere disattivato nella VM.
- Se l'hardware è collegato alla rete con un proprio adattatore di rete o con un adattatore USB, è possibile utilizzare l'opzione "Host-only". In questo caso il TIA Portal Cloud Connector deve essere attivato nella VM per poter utilizzare l'interfaccia PROFIBUS.

Dopo aver utilizzato la VM localmente è possibile ricopiarla nel dispositivo remoto.

Presupposti

- Sul PG/PC dell'utente è installato il software necessario con cui avviare la VM, ad es. VMware Workstation.
- Sul PG/PC dell'utente è installato Automation License Manager .

Trasferimento della macchina virtuale (VM) dal dispositivo remoto al PG/PC

Per utilizzare la macchina virtuale offline, procedere nel seguente modo:

1. Copiare la VM sul PG/PC locale. Il procedimento preciso dipende dall'ambiente di virtualizzazione utilizzato. Se necessario, consultare la documentazione corrispondente.
2. Aprire Automation License Manager e trasferire le licenze necessarie per il software SIMATIC in TIA Portal sul proprio drive locale.
3. Copiare tutti i dati del progetto necessari dal server al drive locale.
4. Avviare la VM e configurare il collegamento di rete. Tenere presente le note all'inizio della pagina.

Trasferimento della macchina virtuale (VM) dal PG/PC al dispositivo remoto

Per ritrasferire la macchina virtuale sul dispositivo remoto, procedere nel seguente modo:

- Copiare la VM dal PG/PC locale al dispositivo remoto. Il procedimento preciso dipende dall'ambiente di virtualizzazione utilizzato. Se necessario, consultare la documentazione corrispondente.
- Aprire Automation License Manager e ritrasferire le licenze dal drive locale a ALM Server.
- Ricopiare tutti i dati del progetto necessari dal drive locale al server.

Vedere anche

Installazione di TIA Portal Cloud Connector sul PG/PC (Pagina 39)

Configurazione di TIA Portal Cloud Connector sul PG/PC (Pagina 40)

Configurazione di TIA Portal Cloud Connector nella VM (Pagina 42)

Collegamento online attraverso TIA Portal Cloud Connector (Pagina 54)

Indice analitico