SIEMENS

SIMATIC

Instrucciones del TIA Portal Cloud Connector

Manual del usuario

Introducción al TIA Portal Cloud Connector 1

Requisitos del sistema 2

Preparación de la máquina virtual (VM) 3

Uso de la máquina virtual (VM) 4

10/2018
A5E44390482-AA

Notas jurídicas

Filosofía en la señalización de advertencias y peligros

Este manual contiene las informaciones necesarias para la seguridad personal así como para la prevención de daños materiales. Las informaciones para su seguridad personal están resaltadas con un triángulo de advertencia; las informaciones para evitar únicamente daños materiales no llevan dicho triángulo. De acuerdo al grado de peligro las consignas se representan, de mayor a menor peligro, como sigue.

⚠ PELIGRO
Significa que, si no se adoptan las medidas preventivas adecuadas **se producirá** la muerte, o bien lesiones corporales graves.

⚠ ADVERTENCIA
Significa que, si no se adoptan las medidas preventivas adecuadas **puede producirse** la muerte o bien lesiones corporales graves.

⚠ PRECAUCIÓN
Significa que si no se adoptan las medidas preventivas adecuadas, pueden producirse lesiones corporales.

ATENCIÓN
Significa que si no se adoptan las medidas preventivas adecuadas, pueden producirse daños materiales.

Si se dan varios niveles de peligro se usa siempre la consigna de seguridad más estricta en cada caso. Si en una consigna de seguridad con triángulo de advertencia de alarma de posibles daños personales, la misma consigna puede contener también una advertencia sobre posibles daños materiales.

Personal cualificado

El producto/sistema tratado en esta documentación sólo deberá ser manejado o manipulado por **personal cualificado** para la tarea encomendada y observando lo indicado en la documentación correspondiente a la misma, particularmente las consignas de seguridad y advertencias en ella incluidas. Debido a su formación y experiencia, el personal cualificado está en condiciones de reconocer riesgos resultantes del manejo o manipulación de dichos productos/sistemas y de evitar posibles peligros.

Uso previsto de los productos de Siemens

Considere lo siguiente:

⚠ ADVERTENCIA
Los productos de Siemens sólo deberán usarse para los casos de aplicación previstos en el catálogo y la documentación técnica asociada. De usarse productos y componentes de terceros, éstos deberán haber sido recomendados u homologados por Siemens. El funcionamiento correcto y seguro de los productos exige que su transporte, almacenamiento, instalación, montaje, manejo y mantenimiento hayan sido realizados de forma correcta. Es preciso respetar las condiciones ambientales permitidas. También deberán seguirse las indicaciones y advertencias que figuran en la documentación asociada.

Marcas registradas

Todos los nombres marcados con ® son marcas registradas de Siemens AG. Los restantes nombres y designaciones contenidos en el presente documento pueden ser marcas registradas cuya utilización por terceros para sus propios fines puede violar los derechos de sus titulares.

Exención de responsabilidad

Hemos comprobado la concordancia del contenido de esta publicación con el hardware y el software descritos. Sin embargo, como es imposible excluir desviaciones, no podemos hacernos responsable de la plena concordancia. El contenido de esta publicación se revisa periódicamente; si es necesario, las posibles correcciones se incluyen en la siguiente edición.

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
ALEMANIA

A5E44390482-AA
℗ 08/2018 Sujeto a cambios sin previo aviso

Índice

1 Introducción al TIA Portal Cloud Connector....5
1.1 Información de seguridad....5
1.2 Principios básicos para trabajar con el TIA Portal Cloud Connector....5
1.3 Interfaz de usuario del TIA Portal Cloud Connector....7
1.4 Aplicaciones del TIA Portal Cloud Connector....17
1.5 Particularidades al trabajar en una máquina virtual....19
1.6 Uso de certificados....20
2 Requisitos del sistema....23
2.1 Requisitos del sistema de la programadora o PC....23
2.2 Requisitos del sistema VM....24
2.3 Licencias....27
2.4 Asignar licencia del equipo del usuario....27
3 Preparación de la máquina virtual (VM)....31
3.1 Crear una plantilla VM nueva....31
3.2 Almacenamiento centralizado de las configuraciones de usuario y de proyecto....32
3.3 Utilizar un servidor de claves de licencia....34
3.4 Instalación del TIA Portal Cloud Connector en la VM....35
4 Uso de la máquina virtual (VM)....39
4.1 Instalación del TIA Portal Cloud Connector en la programadora o el PC....39
4.2 Configuración del TIA Portal Cloud Connector en la programadora o el PC....40
4.3 Configuración del TIA Portal Cloud Connector en la VM....42
4.4 Utilizar certificados (solo para conexiones HTTPS)....44
4.4.1 Crear un certificado para el cifrado de datos....44
4.4.2 Exportar un certificado para el cifrado de datos....45
4.4.3 Importar un certificado para el cifrado de datos....46
4.4.4 Seleccionar un certificado para el cifrado de datos....47
4.4.5 Crear un certificado para la autenticación de usuarios....48
4.4.6 Exportar un certificado para la autenticación de usuarios....49
4.4.7 Importar un certificado para la autenticación de usuarios....50
4.4.8 Agregar un certificado para la autenticación de usuario....51
4.4.9 Seleccionar un certificado para la autenticación de usuarios....52
4.4.10 Eliminar un certificado para la autenticación de usuarios....53
4.5 Conexión online mediante el TIA Portal Cloud Connector....54
4.6 Uso offline de la máquina virtual (VM)....55

Índice alfabético.....57

Introducción al TIA Portal Cloud Connector 1

1.1 Información de seguridad

Siemens ofrece productos y soluciones con funciones de seguridad industrial con el objetivo de hacer más seguro el funcionamiento de instalaciones, sistemas, máquinas y redes.

Para proteger las instalaciones, los sistemas, las máquinas y las redes de amenazas cibernéticas, es necesario implementar (y mantener continuamente) un concepto de seguridad industrial integral que sea conforme a la tecnología más avanzada. Los productos y las soluciones de Siemens constituyen únicamente una parte de este concepto.

El cliente es responsable de impedir el acceso no autorizado a sus instalaciones, sistemas, máquinas y redes. Los sistemas, las máquinas y los componentes solo deben estar conectados a la red corporativa o a Internet cuando y en la medida que sea necesario y siempre que se hayan tomado las medidas de protección adecuadas (p. ej. uso de cortafuegos y segmentación de la red).

Adicionalmente, deberán observarse las recomendaciones de Siemens en cuanto a las medidas de protección correspondientes. Encontrará más información sobre seguridad industrial en:
http://www.siemens.com/industrialsecurity (http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx)

Los productos y las soluciones de Siemens están sometidos a un desarrollo constante con el fin de mejorar todavía más su seguridad. Siemens recomienda expresamente realizar actualizaciones en cuanto estén disponibles y utilizar únicamente las últimas versiones de los productos. El uso de versiones anteriores o que ya no se soportan puede aumentar el riesgo de amenazas cibernéticas.

Para mantenerse informado de las actualizaciones de productos, recomendamos que se suscriba al Siemens Industrial Security RSS Feed en:
http://www.siemens.com/industrialsecurity (http://www.industry.siemens.com/topics/global/en/industrial-security/Pages/Default.aspx)

1.2 Principios básicos para trabajar con el TIA Portal Cloud Connector

Funcionamiento del TIA Portal Cloud Connector

TIA Portal permite trabajar en un entorno virtual. El TIA Portal Cloud Connector es una opción común a varios productos que permite acceder además a interfaces PG/PC y al hardware SIMATIC conectado a ellas en la ingeniería del TIA Portal, aunque la ingeniería en sí se controle por escritorio remoto desde una nube privada.

El paquete opcional "TIA Portal Cloud Connector" permite acceder desde la VM al hardware SIMATIC conectado localmente a la programadora o al PC. Para ello es necesario instalar el TIA Portal Cloud Connector tanto en la VM como en la programadora o el PC al que esté conectado el hardware SIMATIC. Además, el TIA Portal Cloud Connector permite acceder al hardware SIMATIC de otra programadora u otro PC a través de una conexión de escritorio

remoto. La otra programadora o el otro PC pueden encontrarse en otra red. Este tipo de acceso no es posible sin el TIA Portal Cloud Connector.

El uso de máquinas virtuales junto con el TIA Portal Cloud Connector en una nube privada proporciona las ventajas siguientes:

- Soporte de infraestructuras de nube privada modernas:
  - Libre escalabilidad
  - No se requiere instalación en las distintas estaciones de trabajo
  - Mantenimiento y administración centralizados de TIA Portal en la VM
  - Almacenamiento de datos centralizado para proyectos y librerías
- Acceso online a PLC y dispositivos HMI fuera de la red
- Conexión de seguridad mediante HTTPS (a partir de Windows 8.1)
- Soporte de todas las interfaces locales de las estaciones de trabajo
- Acceso rápido a diferentes versiones de TIA Portal
- Aprovechamiento más eficiente de las licencias disponibles
- Asistencia técnica a distancia sencilla para las máquinas

Existe la posibilidad de crear una plantilla a partir de una VM completamente configurada. La plantilla permite crear nuevas VM. Esto permite ahorrar esfuerzo de instalación y configuración.

Suministro del TIA Portal Cloud Connector

A partir de TIA Portal V14.0, el software del TIA Portal Cloud Connector se suministra con los siguientes paquetes de software SIMATIC:

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

Para poder utilizar el TIA Portal Cloud Connector se requiere una licencia en la programadora o el PC que debe comprarse por separado.

Nota

TIA Portal Cloud Connector

El uso del TIA Portal Cloud Connector está previsto únicamente para trabajos de ingeniería con TIA Portal.

Encontrará más información en el Siemens Industry Online Support, en https://support.industry.siemens.com/cs/ww/es/view/109739390 (https://support.industry.siemens.com/cs/ww/es/view/109739390).

Configuración del TIA Portal Cloud Connector

Antes de establecer una conexión mediante el TIA Portal Cloud Connector es necesario configurarlo. La configuración depende de la función de comunicación que tenga el equipo. El TIA Portal Cloud Connector dispone de dos funciones de comunicación:

- Función de comunicación "Equipo del usuario":
  El equipo del usuario es la programadora o el PC al que está conectado el hardware. En este equipo no es necesario que esté instalado TIA Portal. Esta función de comunicación está predeterminada si el TIA Portal Cloud Connector no se instala conjuntamente con TIA Portal, sino por separado.
  Consulte también: Configuración del TIA Portal Cloud Connector en la programadora o el PC (Página 40)
- Función de comunicación "Equipo remoto"
  El equipo remoto es la VM en la que está instalado el TIA Portal. Esta función de comunicación está predeterminada si el TIA Portal Cloud Connector se instala conjuntamente con TIA Portal.
  Consulte también: Configuración del TIA Portal Cloud Connector en la VM (Página 42)

Consulte también

Interfaz de usuario del TIA Portal Cloud Connector (Página 7)

Aplicaciones del TIA Portal Cloud Connector (Página 17)

Particularidades al trabajar en una máquina virtual (Página 19)

Uso de certificados (Página 20)

Requisitos del sistema (Página 23)

Preparación de la máquina virtual (VM) (Página 31)

Uso de la máquina virtual (VM) (Página 39)

1.3 Interfaz de usuario del TIA Portal Cloud Connector

La interfaz de usuario del TIA Portal Cloud Connector consta de los elementos siguientes:

- Entrada en el área de notificación de la barra de tareas de Windows
- TIA Portal Cloud Connector - Configuración
- TIA Portal Cloud Connector - Indicador de estado
- TIA Portal Cloud Connector - Ventana de información
- TIA Portal: visualización en la barra de estado

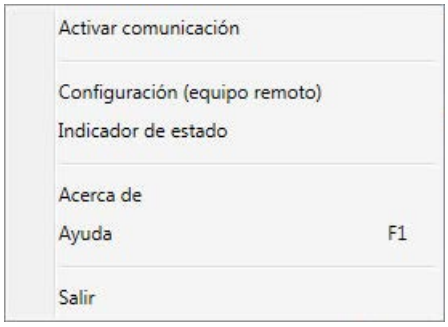
TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows

Al arrancar el TIA Portal Cloud Connector, en el área de notificación de la barra de tareas de Windows se muestra el icono del Cloud Connector. Haciendo clic con el botón derecho del ratón sobre el icono se abre el menú del TIA Portal Cloud Connector.

La figura siguiente muestra el icono del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows cuando los puntos finales de la comunicación están desactivados:

El color del icono varía dependiendo de cuál sea el estado de los puntos finales de la comunicación.

La figura siguiente muestra el menú del área de notificación cuando está ajustada la función de comunicación "Equipo remoto".

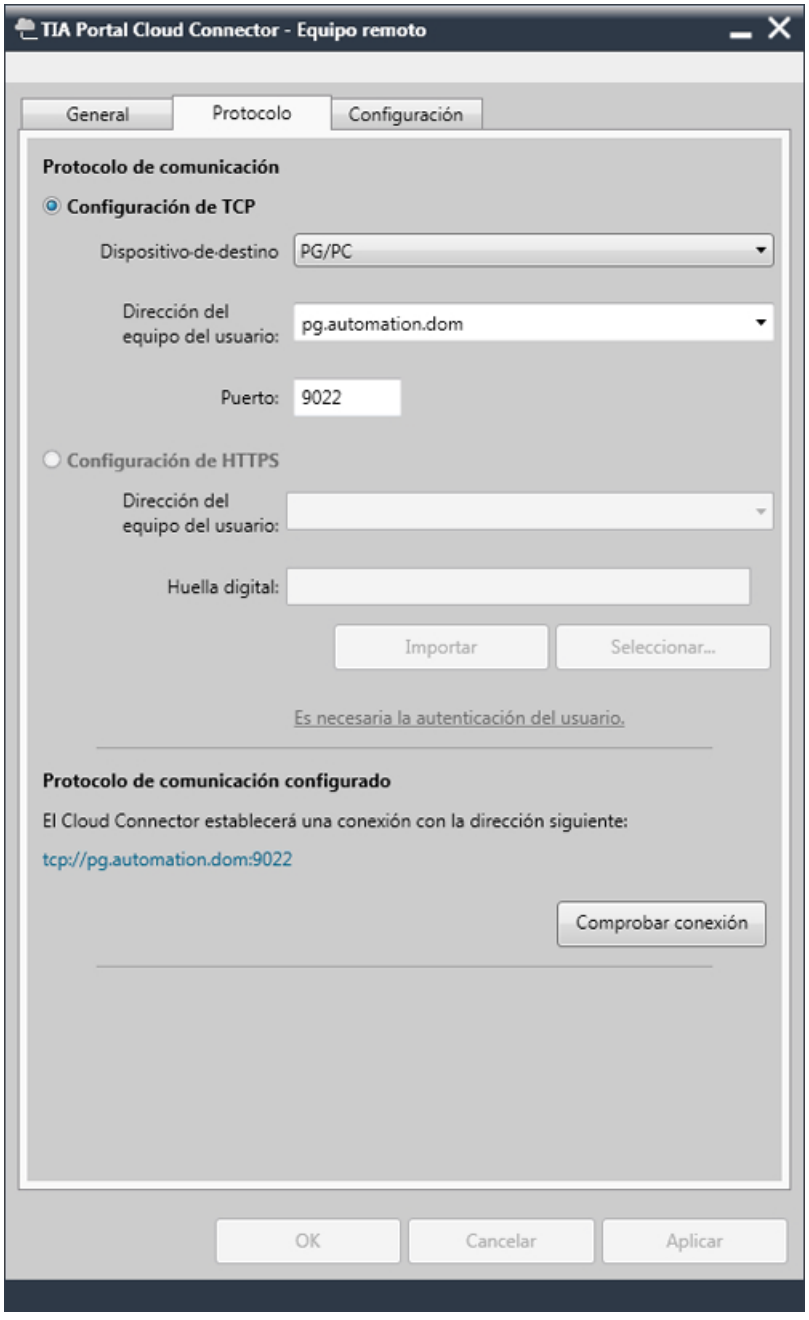


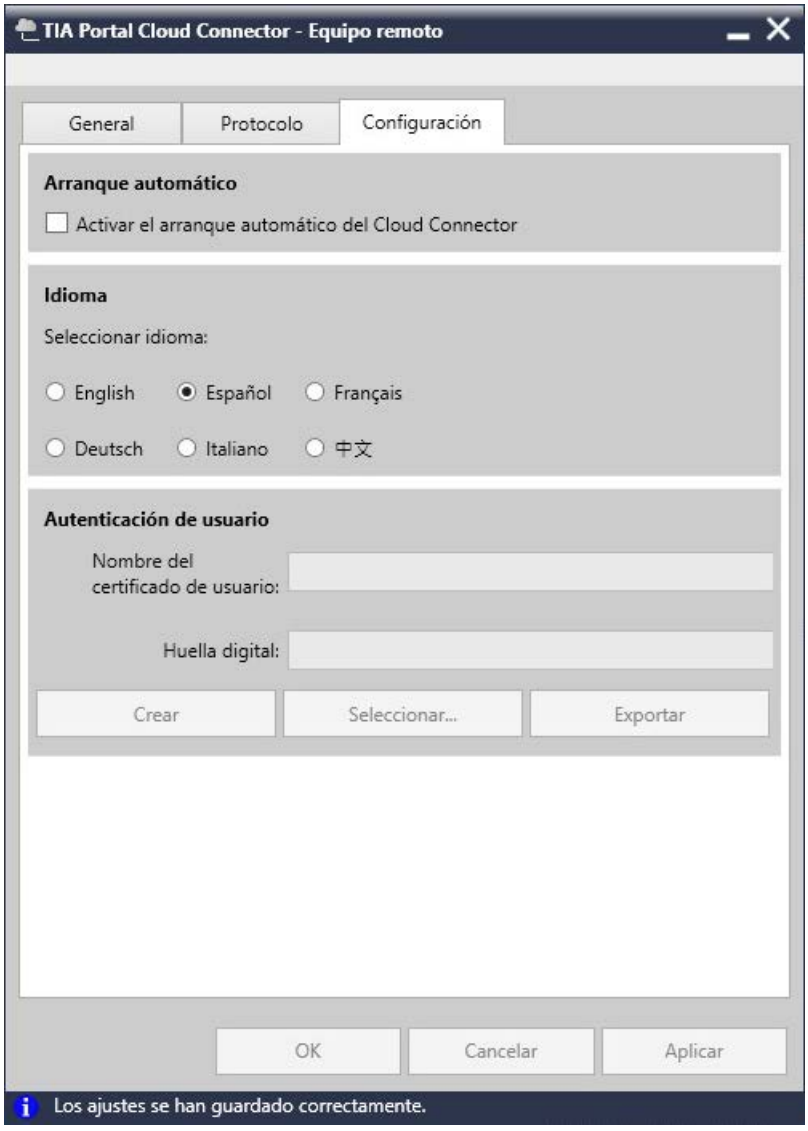
A través del menú se accede a las acciones siguientes:

- Activar comunicación: este comando permite activar la comunicación tanto en el equipo remoto como en el equipo del usuario.
- Configuración (equipo remoto/equipo del usuario): abre el TIA Portal Cloud Configurator con la función de comunicación correspondiente.
- Indicador de estado: abre el indicador de estado, que proporciona información sobre todas las operaciones.
- Acerca de: abre la ventana de información del TIA Portal Cloud Connector. Encontrará, p. ej., el número de versión.
- Ayuda: abre la ayuda en pantalla del TIA Portal Cloud Connector.
- Salir: cierra el TIA Portal Cloud Connector.

TIA Portal Cloud Connector - Configuración

La interfaz del TIA Portal Cloud Connector varía según la función de comunicación configurada. Las figuras siguientes muestran las diferentes fichas de configuración del TIA Portal Cloud Connector en la función de comunicación "Equipo remoto":


TIA Portal Cloud Connector - Equipo remoto
General
Protocolo
Configuración
Protocolo de comunicación
Configuración de TCP
Dispositivo de destino
PG/PC
Dirección del equipo del usuario:
pg.automation.dom
Puerto:
9022
Configuración de HTTPS
Dirección del equipo del usuario:
Huella digital:
Importar
Seleccionar...
Es necesaria la autenticación del usuario.
Protocolo de comunicación configurado
El Cloud Connector establecerá una conexión con la dirección siguiente:
tcp://pg.automation.dom:9022
Comprobar conexión
OK
Cancelar
Aplicar



Dentro de las diferentes fichas pueden realizarse todos los ajustes necesarios para una conexión.

La tabla siguiente ofrece una vista general de los ajustes posibles y los botones disponibles para la función de comunicación "Equipo remoto":

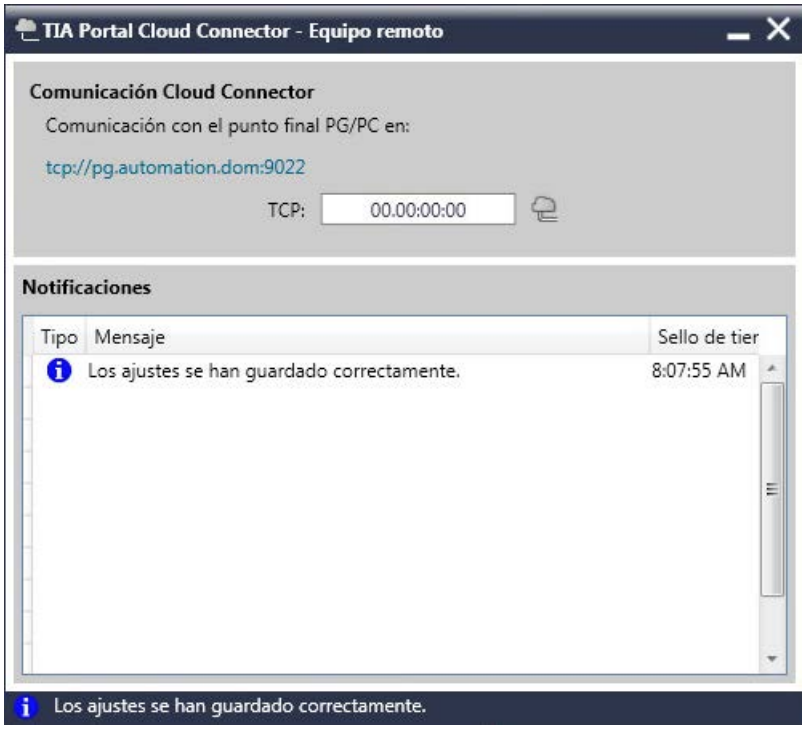
Ficha	Área	Ajuste/botón	Descripción
General	Función de comunicación	Equipo del usuario	Programadora o PC que posibilita el contacto físico con el hardware SIMATIC.
		Equipo remoto	Máquina virtual (VM) en la que está instalado el TIA Portal. Se puede acceder a ella desde el equipo del usuario a través de una conexión de escritorio remoto.
	Comunicación Cloud Connector	Activar comunicación Desactivar comunicación	Activa y desactiva la comunicación con un punto final de la programadora o PC.
	Accesos a licencia	Activar Desactivar	Activa y desactiva el uso de una licencia del equipo del usuario.
Protocolo	Protocolo de comunicación		Define el mecanismo de transporte entre los puntos finales de la comunicación. Las opciones disponibles son TCP o HTTPS (a partir de Windows 8.1).
	Configuración de TCP	Dispositivo de destino	Tipo del interlocutor de comunicación.
		Dirección del equipo del usuario	Dirección IP o nombre del equipo del usuario
		Puerto	Número de puerto a través del que se llevará a cabo el transporte
	Configuración de HTTPS	Dirección del equipo del usuario	Dirección IP o nombre del equipo del usuario
		Huella digital	Asegura la integridad del certificado.
		Importar	Importa un certificado existente a la memoria de certificados de Windows. Un certificado importado puede utilizarse para cifrar datos que se envían vía HTTPS.
		Seleccionar	Selección de un certificado previamente importado para el cifrado de datos.
	Protocolo de comunicación configurado	Comprobar conexión	Comprueba si la conexión puede establecerse correctamente.
Configuración	Arranque automático	Activar el arranque automático del Cloud Connector	Activa o desactiva el arranque automático para el TIA Portal Cloud Connector al iniciar el sistema.
	Idioma	Seleccionar el idioma	Define el idioma de la interfaz de usuario para el TIA Portal Cloud Connector.
	Autenticación de usuario	Nombre del certificado de usuario	Muestra el certificado de usuario que se utiliza actualmente.
		Huella digital	Suma de verificación del certificado para asegurar la integridad
		Crear	Crea un certificado nuevo para la autenticación del usuario.
		Seleccionar	Permite seleccionar un certificado existente de la memoria de certificados de Windows.
		Exportar	Exporta el certificado que se utiliza actualmente.

La tabla siguiente ofrece una vista general de los ajustes posibles y los botones disponibles para la función de comunicación "Equipo del usuario":

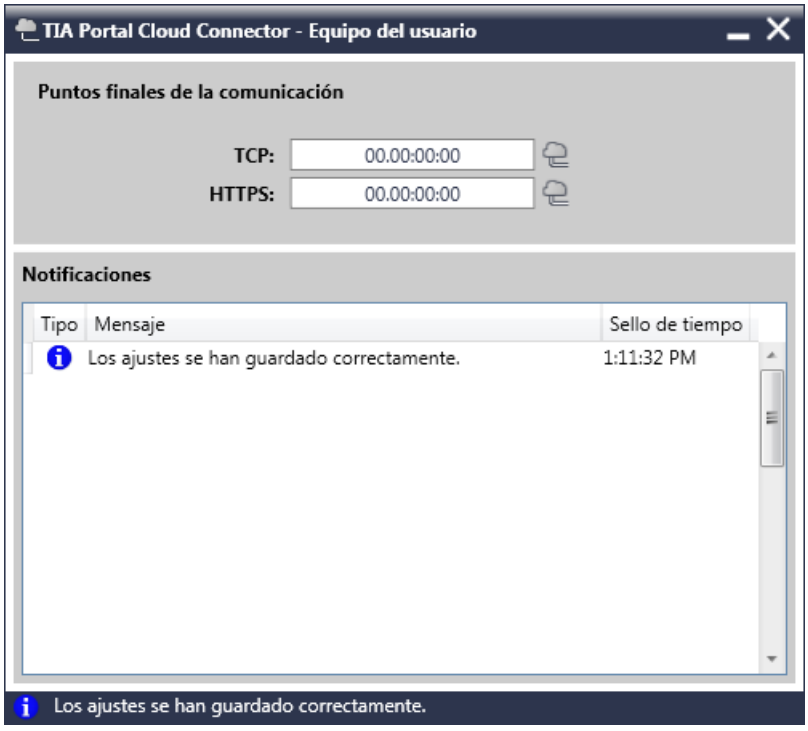
Ficha	Área	Ajuste/botón	Descripción
General	Función de comunicación	Equipo del usuario	Programadora o PC que posibilita el contacto físico con el hardware SIMATIC.
		Equipo remoto	Máquina virtual en el Private Cloud Server en el que está instalado el TIA Portal, que es utilizado por un equipo de usuario a través de una conexión de escritorio remoto.
	Comunicación Cloud Connector	Activar comunicación Desactivar comunicación	Activa y desactiva la comunicación con un punto final de la programadora o PC.
	Accesos a licencia	Activar Desactivar	Activa y desactiva el uso de una licencia del equipo del usuario.
Protocolo	Punto final de TCP	Puerto	Número de puerto a través del que se llevará a cabo la comunicación. El número de puerto del equipo del usuario debe coincidir con el del equipo remoto.
	Punto final de HTTPS	Dirección del equipo del usuario	Dirección IP o nombre del equipo del usuario
		Huella digital	Asegura la integridad del certificado.
		Crear	Crea un certificado nuevo para el cifrado de datos.
		Exportar	Exporta el certificado que se utiliza actualmente.
		Seleccionar	Permite seleccionar un certificado existente.
Configuración	Arranque automático	Activar el arranque automático del Cloud Connector	Activa o desactiva el arranque automático para el TIA Portal Cloud Connector al iniciar el sistema.
	Idioma	Seleccionar el idioma	Define el idioma de la interfaz de usuario para el TIA Portal Cloud Connector.
	Autenticación de usuario	Certificados de usuario de confianza	Muestra la lista de todos los certificados de usuario disponibles y de confianza.
		Importar	Permite importar a la memoria de certificados de Windows un certificado de usuario que se generó en el equipo remoto.
		Agregar	Permite agregar un certificado de la memoria de certificados de Windows a la lista de certificados de confianza.
		Eliminar	Elimina el certificado seleccionado de la lista de certificados de confianza. Sin embargo, se conserva en la memoria de certificados de Windows.

TIA Portal Cloud Connector - Indicador de estado

El indicador de estado proporciona información sobre las advertencias y los mensajes de error que aparecen durante el uso del TIA Portal Cloud Connector. La figura siguiente muestra el indicador de estado en la función de comunicación "Equipo remoto".

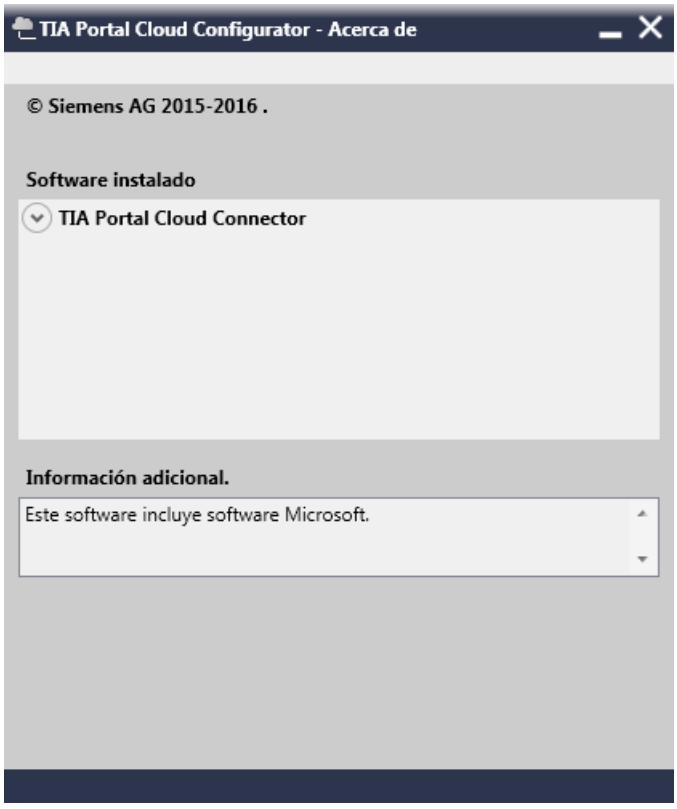


La figura siguiente muestra el indicador de estado en la función de comunicación "Equipo del usuario".


TIA Portal Cloud Connector - Equipo del usuario
Puntos finales de la comunicación
TCP:
00.00:00:00
HTTPS:
00.00:00:00
Notificaciones
Tipo
Mensaje
Sello de tiempo
Los ajustes se han guardado correctamente.
1:11:32 PM
Los ajustes se han guardado correctamente.

TIA Portal Cloud Connector - Ventana de información

En la ventana de información encontrará información relacionada con la versión instalada del TIA Portal Cloud Connector.



TIA Portal: visualización en la barra de estado

En la barra de estado del TIA Portal se indica si existe una conexión online con el hardware SIMATIC a través del TIA Portal Cloud Connector. Además de los indicadores online, en caso de conexión a través del TIA Portal Cloud Connector se muestra el icono siguiente en la barra de estado:

Consulte también

Principios básicos para trabajar con el TIA Portal Cloud Connector (Página 5)

Aplicaciones del TIA Portal Cloud Connector (Página 17)

Particularidades al trabajar en una máquina virtual (Página 19)

Uso de certificados (Página 20)

Requisitos del sistema (Página 23)

Preparación de la máquina virtual (VM) (Página 31)

Uso de la máquina virtual (VM) (Página 39)

1.4 Aplicaciones del TIA Portal Cloud Connector

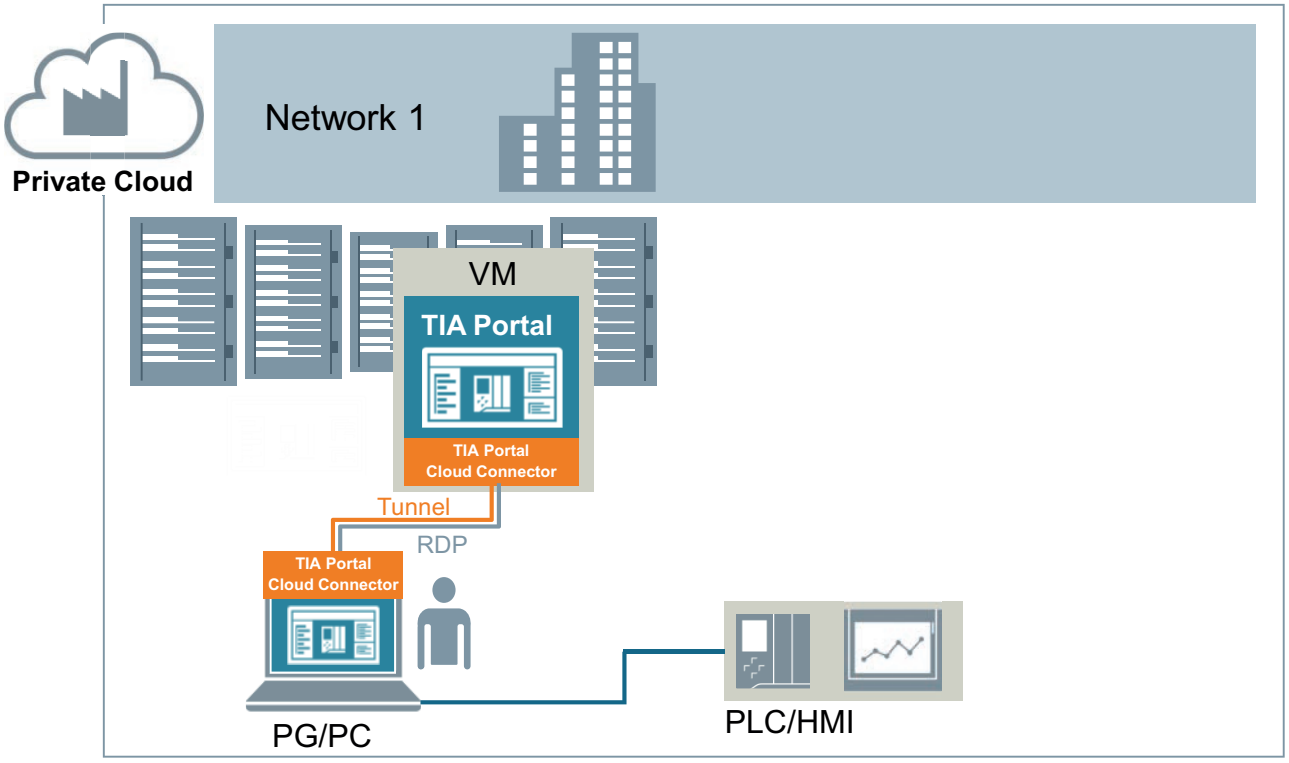
El TIA Portal Cloud Connector permite realizar las aplicaciones siguientes:

- Acceso a hardware conectado a la propia programadora o al propio PC.
- Acceso a hardware conectado a otra programadora u otro PC. Dicho hardware puede estar dentro o fuera de la propia red.

Acceso a hardware conectado a la propia programadora o al propio PC

El TIA Portal se instala en la nube privada de la empresa. Por el contrario, en la programadora o el PC del usuario no está instalado TIA Portal. El hardware de automatización (PLC / HMI) está conectado con la programadora o el PC del usuario. El TIA Portal Cloud Connector está instalado tanto en la VM como en la programadora o el PC. En la programadora o el PC se requiere una licencia para el TIA Portal Cloud Connector. A través de la conexión de escritorio remoto (RDP) se inicia sesión en la VM y se puede trabajar de la forma habitual con el TIA Portal. El TIA Portal Cloud Connector permite acceder al hardware conectado localmente a la programadora o el PC.

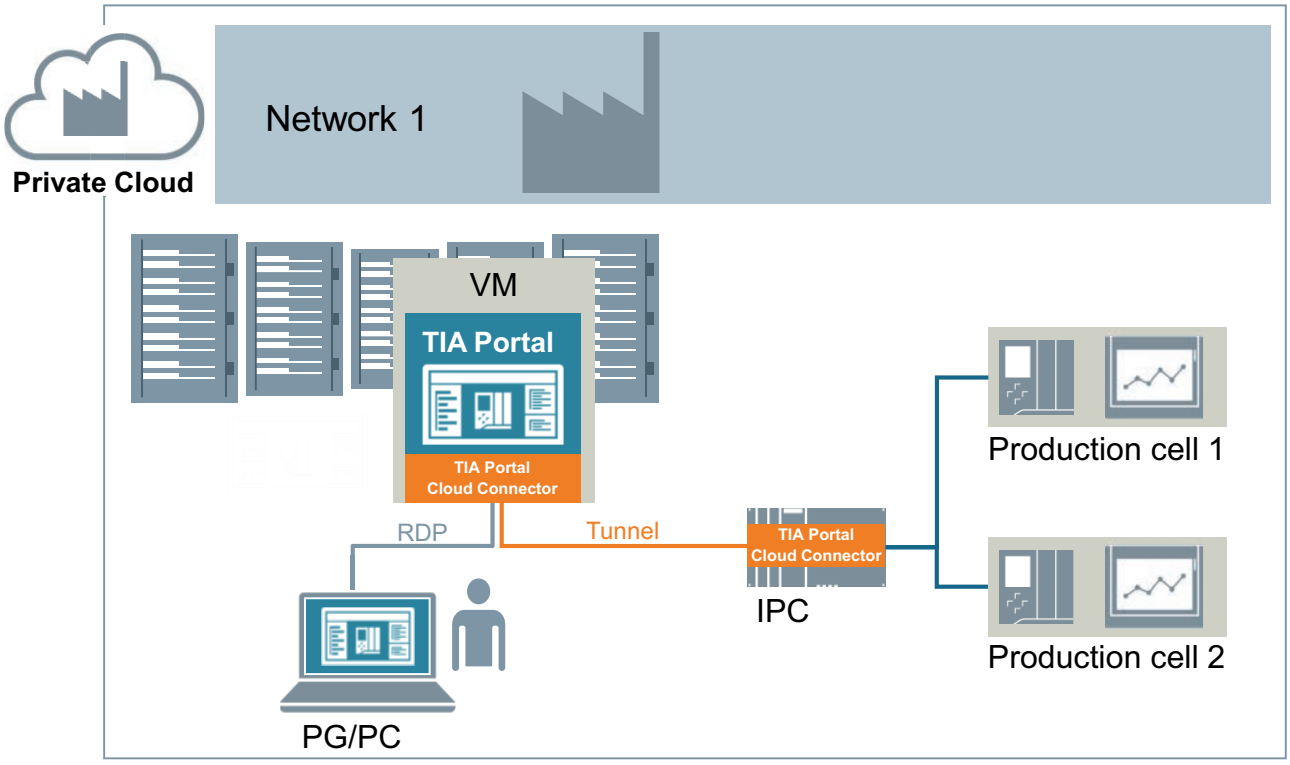
La figura siguiente muestra el uso del TIA Portal Cloud Connector en un entorno virtual cuando el hardware está conectado a una programadora o PC propio:

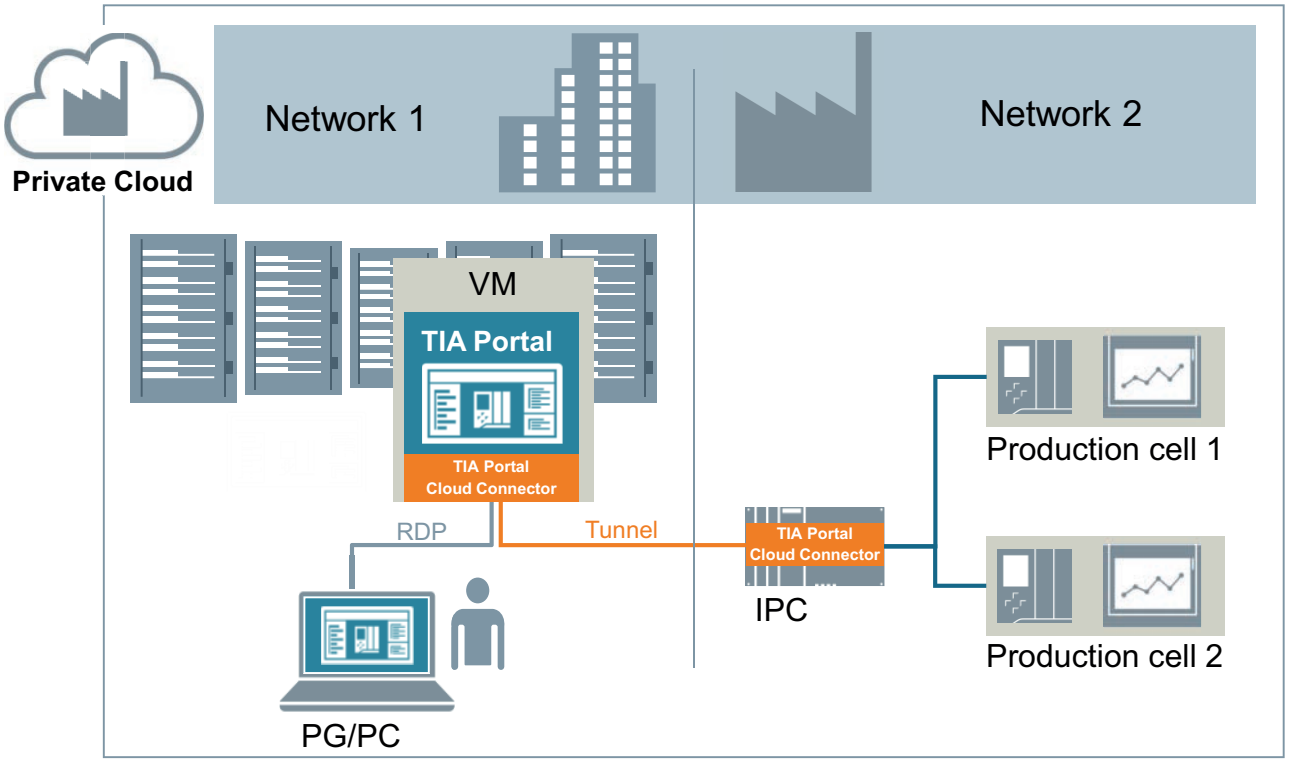


Acceso a hardware conectado a otra programadora u otro PC

El TIA Portal se instala en una máquina virtual. Por el contrario, en la programadora o el PC no está instalado TIA Portal. El hardware de automatización está conectado a una programadora o un PC, p. ej. un IPC, que se encuentra en la misma red (figura superior) o en una red distinta (figura inferior) de la de su propia programadora o PC. El TIA Portal Cloud Connector está instalado en la otra programadora o PC y en la VM. A través de la conexión de escritorio remoto (RDP) se inicia sesión primero en la VM y se puede trabajar de la forma habitual con el TIA Portal. Por medio del TIA Portal Cloud Connector se establece una conexión entre la VM y la otra programadora u el otro PC, con lo que ya es posible acceder al hardware de automatización.

Las figuras siguientes muestran el uso del TIA Portal Cloud Connector en un entorno virtual cuando el hardware está conectado a una programadora o PC distinto al propio, en el ejemplo un IPC:





Consulte también

Principios básicos para trabajar con el TIA Portal Cloud Connector (Página 5)

Interfaz de usuario del TIA Portal Cloud Connector (Página 7)

Particularidades al trabajar en una máquina virtual (Página 19)

Uso de certificados (Página 20)

Requisitos del sistema (Página 23)

Preparación de la máquina virtual (VM) (Página 31)

Uso de la máquina virtual (VM) (Página 39)

1.5 Particularidades al trabajar en una máquina virtual

Simulación

Para simular un programa de PLC es necesario desactivar antes el TIA Portal Cloud Connector. De todas formas, no es necesario hacerlo para simular dispositivos HMI.

Manejo de actualizaciones y Support Packages

Las actualizaciones y los Support Packages pueden instalarse ya en la plantilla de la VM o posteriormente en las diferentes VM. Utilice para ello los mecanismos de actualización del TIA Portal.

Para más información, consulte el sistema de información del TIA Portal.

Comparación entre la topología configurada y la topología realmente existente

El TIA Portal Cloud Connector no soporta la comparación topológica.

Consulte también

Principios básicos para trabajar con el TIA Portal Cloud Connector (Página 5)

Interfaz de usuario del TIA Portal Cloud Connector (Página 7)

Aplicaciones del TIA Portal Cloud Connector (Página 17)

Uso de certificados (Página 20)

Requisitos del sistema (Página 23)

Preparación de la máquina virtual (VM) (Página 31)

Uso de la máquina virtual (VM) (Página 39)

1.6 Uso de certificados

Uso de certificados en el TIA Portal Cloud Connector

A partir de Windows 8.1 existe la posibilidad de utilizar conexiones HTTPS para la comunicación. En este caso, el TIA Portal Cloud Connector utiliza certificados que garantizan la seguridad de las conexiones HTTPS. Los certificados siguientes son necesarios para que se pueda establecer una conexión entre el equipo del usuario y el equipo remoto:

- Certificado para el cifrado de datos
- Certificado para la autenticación de usuarios

Si un certificado no existe o los certificados de los equipos del usuario y remoto no coinciden, no es posible establecer la conexión.

Certificado para el cifrado de datos

El certificado para el cifrado de datos se crea en el equipo del usuario. Seguidamente, el certificado debe copiarse a una unidad de disco local del equipo remoto e importarse al TIA Portal Cloud Connector. Si los certificados coinciden, es posible una conexión entre los dispositivos en cuanto se hayan intercambiado también los certificados para la autenticación de usuarios.

Certificado para la autenticación de usuarios

El certificado para la autenticación de usuarios se crea en el equipo remoto. Seguidamente, el certificado debe copiarse al equipo del usuario e importarse al TIA Portal Cloud Connector. Si los certificados coinciden, es posible una conexión entre los dispositivos en cuanto se hayan intercambiado también los certificados para el cifrado de datos.

Consulte también

Principios básicos para trabajar con el TIA Portal Cloud Connector (Página 5)
Interfaz de usuario del TIA Portal Cloud Connector (Página 7)
Aplicaciones del TIA Portal Cloud Connector (Página 17)
Particularidades al trabajar en una máquina virtual (Página 19)
Crear un certificado para el cifrado de datos (Página 44)
Exportar un certificado para el cifrado de datos (Página 45)
Importar un certificado para el cifrado de datos (Página 46)
Seleccionar un certificado para el cifrado de datos (Página 47)
Crear un certificado para la autenticación de usuarios (Página 48)
Exportar un certificado para la autenticación de usuarios (Página 49)
Importar un certificado para la autenticación de usuarios (Página 50)
Agregar un certificado para la autenticación de usuario (Página 51)
Seleccionar un certificado para la autenticación de usuarios (Página 52)
Eliminar un certificado para la autenticación de usuarios (Página 53)

Requisitos del sistema 2

2.1 Requisitos del sistema de la programadora o PC

Sistemas operativos compatibles

Para utilizar el TIA Portal Cloud Connector es necesario que en la programadora o el PC esté instalado uno de los sistemas operativos siguientes:

- Windows Server 2012 R2 StdE (instalación completa)
- Windows Server 2016 Standard (instalación completa)
- Windows 7 Home Premium SP1
- Windows 7 Professional SP1
- Windows 7 Enterprise SP1
- Windows 7 Ultimate SP1
- Windows 10 Home versión 1703
- Windows 10 Pro versión 1703
- Windows 10 Enterprise versión 1703
- Windows 10 Enterprise 2016 LTSB
- Windows 10 IoT Enterprise 2015 LTSB
- Windows 10 IoT Enterprise 2016 LTSB

Nota

Observe las indicaciones siguientes:

- No es posible utilizar el TIA Portal Cloud Connector en sistemas operativos de 32 bits.
- Asegúrese de que el sistema operativo esté siempre actualizado. Para ello, ejecute todas las actualizaciones importantes de Windows sin mucha demora.
- Si SIMATIC NET está instalado en una versión anterior a 15.0.1 no es posible activar el TIA Portal Cloud Connector.
- Para que la resolución del nombre funcione en la red, active la opción "Activar la detección de redes" o la opción "Activar el uso compartido de archivos e impresoras". Como alternativa también puede utilizarse un servidor de nombres externo.

Licencias para el TIA Portal Cloud Connector

Para trabajar con el TIA Portal Cloud Connector es necesario disponer de una License Key válida para cada equipo que se configure como "equipo del usuario" en el TIA Portal Cloud Connector. Los equipos utilizados como "equipo remoto" no precisan License Key.

La License Key puede instalarse conjuntamente con la instalación o transferirse posteriormente con el Automation License Manager.

Consulte también

Requisitos del sistema VM (Página 24)

Licencias (Página 27)

2.2 Requisitos del sistema VM

Sistemas operativos huésped y plataformas de virtualización compatibles

Existe la posibilidad de utilizar TIA Portal dentro de una máquina virtual (VM). Para ello, utilice una de las siguientes plataformas de virtualización en la versión indicada o en una superior:

- 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

En la VM es posible instalar uno o varios de los paquetes de software siguientes:

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

Además de estos paquetes de software es posible instalar también otros paquetes opcionales de STEP 7 y WinCC.

Nota

Uso del TIA Portal Cloud Connector en caso de estar instalado SIMATIC NET

Si SIMATIC NET está instalado en la VM no es posible activar el TIA Portal Cloud Connector.

Dependiendo de cuál sea el paquete de software seleccionado, dentro de la VM serán compatibles diferentes sistemas operativos huésped:

Sistema operativo huésped	SIMATIC STEP 7 Basic	SIMATIC STEP 7 Professional	SIMATIC WinCC Basic	SIMATIC WinCC Professional	SIMATIC WinCC Advanced
Windows Server 2012 R2 StdE (instalación completa) (64 bits)	X	X	X	X	X
Windows Server 2016 Standard (instalación completa) (64 bits)	X	X	X	X	X
Windows 7 Home Premium SP1 (64 bits)	X	-	X	-	-
Windows 7 Professional SP1 (64 bits)	X	X	X	X	X
Windows 7 Enterprise SP1 (64 bits)	X	X	X	X	X
Windows 7 Ultimate SP1 (64 bits)	X	X	X	X	X
Windows 10 Home versión 1703 (64 bits)	X	-	-	X	-
Windows 10 Pro versión 1703 (64 bits)	X	X	X	X	X
Windows 10 Enterprise versión 1703 (64 bits)	X	X	X	X	X
Windows 10 Enterprise 2016 LTSB (64 bits)	X	X	X	X	X
Windows 10 IoT Enterprise 2015 LTSB (64 bits)	X	X	X	X	X
Windows 10 IoT Enterprise 2016 LTSB (64 bits)	X	X	X	X	X
- El sistema operativo no es compatible X El sistema operativo es compatible					

Nota

Tenga en cuenta las indicaciones siguientes:

- Los sistemas operativos de 32 bits no son compatibles.
- Para los sistemas operativos huésped valen los mismos requisitos de hardware que para los distintos productos TIA.
- La programadora de SIMATIC USB (prommer) no es compatible.
- Si se desea utilizar tarjetas SD en la VM es necesario integrarlas antes en la VM como medios de almacenamiento intercambiables. Sobre el procedimiento preciso tenga en cuenta la ayuda de su plataforma de virtualización.
- Asegúrese de que el sistema operativo esté siempre actualizado. Para ello, ejecute todas las actualizaciones importantes de Windows sin mucha demora.

Instalación del TIA Portal Cloud Connector

Existen dos posibilidades de instalar el TIA Portal Cloud Connector:

- Durante la instalación de uno de los paquetes de software SIMATIC mencionados anteriormente se puede activar el TIA Portal Cloud Connector como opción. En tal caso se instalará conjuntamente con el paquete de software.
- También es posible instalar el TIA Portal Cloud Connector independientemente de cualquier paquete de software SIMATIC. El archivo de instalación se encuentra en el soporte de datos de instalación dentro de la carpeta "Support". Tiene la posibilidad de hacer que este archivo de instalación esté disponible en su red. De este modo, en calidad de administrador de la VM puede crear scripts que permitan una actualización automática del TIA Portal Cloud Connector. Pero recuerde que en cada programadora o PC debe existir una licencia válida del TIA Portal Cloud Connector.

Licencias para el TIA Portal Cloud Connector

Para trabajar con el TIA Portal Cloud Connector en la VM no es necesario disponer de licencias del TIA Portal Cloud Connector si se selecciona la función de comunicación "Equipo remoto".

Consulte también

Requisitos del sistema de la programadora o PC (Página 23)

Licencias (Página 27)

2.3 Licencias

Obtención de licencias de paquetes de software SIMATIC

Para utilizar los diferentes paquetes de software SIMATIC del TIA Portal (STEP 7, WinCC) en un entorno virtual se requiere de una licencia propia para cada instalación. La copia o clonación de una plantilla de VM también se considera una instalación. Por el contrario, siempre que no exista una instalación local, no es necesario disponer de una licencia para TIA Portal en la programadora o el PC con el que se accede a una VM.

Si se utilizan Floating License Keys, las licencias se pueden obtener a través de un servidor de claves de licencia.

Obtención de licencias del TIA Portal Cloud Connector

Para trabajar con el TIA Portal Cloud Connector es necesario disponer de una License Key válida para cada equipo que se configure como "equipo del usuario" en el TIA Portal Cloud Connector. Los equipos utilizados como "equipo remoto" no precisan License Key.

La License Key puede instalarse conjuntamente con la instalación o transferirse posteriormente con el Automation License Manager.

Acceso a licencias del equipo del usuario desde el equipo remoto

El TIA Portal Cloud Connector permite al TIA Portal del equipo remoto acceder a licencias del equipo del usuario. Para ello el TIA Portal Cloud Connector transmite las consultas de licencia del equipo remoto al equipo del usuario a través del túnel. En cuanto se ha activado el reenvío del acceso a licencia a través del TIA Portal Cloud Connector, el ALM rechaza todas las demás consultas de licencia de otros equipos remotos. Las aplicaciones que ya han ocupado licencias sí que conservan su licencia. La asignación de las licencias locales a aplicaciones es posible tanto en equipos remotos como del usuario.

Consulte también: Asignar licencia del equipo del usuario (Página 27)

Consulte también

Requisitos del sistema de la programadora o PC (Página 23)

Requisitos del sistema VM (Página 24)

Utilizar un servidor de claves de licencia (Página 34)

2.4 Asignar licencia del equipo del usuario

El TIA Portal instalado en el equipo remoto puede acceder a licencias existentes del equipo del usuario. Para ello es necesario que el uso de licencias externas esté activado tanto en el equipo del usuario como en el remoto. El procedimiento para activar el uso de licencias externas es idéntico para el equipo del usuario y el remoto. Para ver si el uso de licencias externas está activado o si estas se están utilizando debe observarse el color del símbolo del botón "Activar" o "Desactivar".

La tabla siguiente muestra una descripción general de los símbolos y sus significados:

Símbolo	Significado
	La asignación de licencias está desactivada.
	La asignación de licencias está activada, pero actualmente el equipo remoto no utiliza licencias del equipo del usuario.
	La asignación de licencias está activada y el equipo remoto utiliza licencias del equipo del usuario.
	El intercambio de datos entre el TIA Portal y el hardware de automatización SIMATIC se ha interrumpido. Se muestra el indicador de estado y se proporcionan más detalles sobre la causa.

La asignación de licencias puede desactivarse en cualquier momento.

Activar el uso de licencias externas

Para activar el acceso a licencias del equipo del usuario, proceda del siguiente modo:

1. En el equipo del usuario, haga clic con el botón derecho del ratón en el icono del TIA Portal Cloud Connector en el área de notificación de la barra de tareas y elija el comando "Configuración".
   Se abre el TIA Portal Cloud Connector.
2. Abra la ficha "General".
3. En el área "Accesos a licencia", haga clic en el botón "Activar".
4. Establezca una conexión de escritorio remoto con la VM contenida en el equipo remoto.
5. En el equipo remoto, haga clic con el botón derecho del ratón en el icono del TIA Portal Cloud Connector en el área de notificación de la barra de tareas y elija el comando "Configuración".
   Se abre el TIA Portal Cloud Connector.
6. En el área "Accesos a licencia", haga clic en el botón "Activar".
   El uso de las licencias del equipo del usuario desde el TIA Portal del equipo remoto está ahora preparado. El texto del botón "Activar" cambia a "Desactivar" y el color del símbolo cambia a amarillo.

Desactivar el uso de licencias externas

Para desactivar el acceso a licencias del equipo del usuario, proceda del siguiente modo:

1. En el equipo del usuario, haga clic con el botón derecho del ratón en el icono del TIA Portal Cloud Connector en el área de notificación de la barra de tareas y elija el comando "Configuración".
   Se abre el TIA Portal Cloud Connector.
2. Abra la ficha "General".
3. En el área "Accesos a licencia", haga clic en el botón "Desactivar".
4. Establezca una conexión de escritorio remoto con la VM contenida en el equipo remoto.

5. En el equipo remoto, haga clic con el botón derecho del ratón en el icono del TIA Portal Cloud Connector en el área de notificación de la barra de tareas y elija el comando "Configuración".
   Se abre el TIA Portal Cloud Connector.
6. En el área "Accesos a licencia", haga clic en el botón "Desactivar".
   El uso de las licencias del equipo del usuario desde el TIA Portal del equipo remoto está ahora desactivado. El texto del botón "Desactivar" cambia a "Activar" y el color del símbolo cambia a gris.

Consulte también

Licencias (Página 27)

Utilizar un servidor de claves de licencia (Página 34)

Preparación de la máquina virtual (VM) 3

3.1 Crear una plantilla VM nueva

Es posible utilizar las plataformas de virtualización siguientes:

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

Dependiendo de cuál sea la plataforma de virtualización utilizada, existen diferencias a la hora de crear una plantilla basada en una máquina virtual (VM) ya existente. Encontrará más información al respecto en la ayuda correspondiente de la plataforma de virtualización utilizada.

Prepare su entorno de desarrollo SIMATIC en la VM igual que en cualquier programadora o PC.

Pasos básicos para crear una plantilla VM nueva

Para crear una plantilla VM nueva, proceda del siguiente modo:

1. Cree una VM.
2. Instale el software SIMATIC que desee, p. ej. SIMATIC STEP 7 (TIA Portal V14 o superior) o SIMATIC WinCC (TIA Portal V14 o superior), en la edición requerida (Basic, Professional, Comfort/Advanced).

   Nota

   El procedimiento para instalar TIA Portal en una máquina virtual (VM) es idéntico al procedimiento para instalarlo en una programadora o un PC. Encontrará indicaciones detalladas sobre la instalación en las instrucciones de instalación de TIA Portal.

3. En caso necesario, instale paquetes opcionales adicionales, p. ej. SIMATIC STEP 7 Safety Advanced.
4. Si es preciso, instale otros paquetes de software compatibles que deban estar disponibles para todos los usuarios.
5. Configure la VM según sus necesidades.
6. Cree una plantilla de la VM siguiendo las instrucciones de la plataforma de virtualización.

Resultado

Se ha creado una plantilla VM que puede copiarse y transferirse posteriormente. Pero tenga en cuenta que si se utiliza una copia de la plantilla debe disponerse de las licencias necesarias. Puede utilizar un servidor de licencias independiente (VM) para administrar las licencias.

Consulte también

Almacenamiento centralizado de las configuraciones de usuario y de proyecto (Página 32)

Utilizar un servidor de claves de licencia (Página 34)

Instalación del TIA Portal Cloud Connector en la VM (Página 35)

3.2 Almacenamiento centralizado de las configuraciones de usuario y de proyecto

Los ajustes y proyectos guardados por los usuarios en la VM se pierden cuando se borra la VM. Para que los ajustes y proyectos también estén disponibles en otras VM deben guardarse fuera de la VM. Es posible activar en la VM variables de entorno con las ubicaciones para configuraciones personalizadas y proyectos. Establezca las variables del entorno antes de iniciar el TIA Portal por primera vez. Si las variables del entorno no están disponibles la primera vez que se inicia el TIA Portal, este deposita el archivo de los ajustes en el directorio predeterminado y en el futuro utilizará siempre este archivo. Mientras exista este archivo, el TIA Portal ignorará las variables del entorno que se establezcan con posterioridad.

Con las variables del entorno se definen las rutas siguientes:

- Configuraciones personalizadas: los ajustes se guardan en el directorio indicado.
- Proyectos: la ubicación indicada se utiliza como ruta estándar al crear un proyecto nuevo. Pero también es posible guardar un proyecto en cualquier otro directorio.

Las variables de entorno pueden activarse manualmente o mediante un script. Es posible crear sendos scripts para activar la variable de entorno para los ajustes y los proyectos, o bien se pueden activar con un solo script ambas variables de entorno.

El archivo de configuración tiene el mismo nombre para todos los usuarios. Para que cada usuario pueda acceder a su propia configuración es necesario indicar un directorio propio de cada usuario. En caso contrario cualquier usuario podría sobrescribir la configuración. Mediante una variable es posible adaptar la ruta al usuario que inicia la sesión.

Ejemplo de una estructura de directorios para guardar la configuración de forma centralizada

La configuración debe guardarse en un directorio compartido "UserSettings" en la red. La estructura de "UserSettings" es la siguiente:

```
UserSettings
            User1
            User2
            User3
```

"`User1`", "`User2`" y "`User3`" son los nombres de usuario de los usuarios de la VM. En tal caso la ruta de las variables de entorno es "\\MyServer\UserSettings\%USERNAME%".

En este ejemplo, "MyServer" es un ordenador al que se puede acceder en la red. "%USERNAME%" es la variable del nombre de usuario. Esta variable se resuelve al iniciarse la sesión del usuario, y la variable de entorno se modifica en consecuencia. Si debe procederse así para varios usuarios, se recomienda guardar el script en el directorio de inicio automático.

De este modo la variable de entorno se activa de nuevo con cada inicio de sesión, y la ubicación de la configuración se adapta al usuario que inicia la sesión.

Requisitos

- Todos los usuarios tienen derecho de escritura en las áreas de servidor que van a utilizarse como ubicaciones nuevas.
- Los directorios de usuario están presentes.

Activación de variables de entorno mediante un script

Para activar las variables de entorno mediante un script, proceda del siguiente modo:

1. Cree un nuevo script y ábralo para editarlo. Como alternativa también es posible ampliar un script ya existente.
2. Agregue al script las líneas siguientes:
   `setx TiaUserSettingsPath \\<Server>\<Settings>\%USERNAME%`
   `setx TiaDefaultProjectPath \\<Server>\<Projects>\%USERNAME%`
   Reemplace "`<Server>\<Settings>`" y "`<Server>\<Projects>`" por los directorios de la red donde deban guardarse los ajustes y proyectos.
3. Guarde el script.
4. Para que el script pueda utilizarse para diferentes usuarios, cópielo en el directorio de inicio automático de Windows.
   Las variables "%USERNAME%" se resuelven con el siguiente inicio de sesión en el equipo remoto. De este modo la ubicación de la configuración se adapta al usuario que inicia la sesión.

Si desea utilizar dos scripts en vez de uno, ejecute los pasos 1 a 4 para cada uno de los scripts y agregue en cada caso solo uno de los dos comandos "`setx`".

Activación manual de variables de entorno

Para activar manualmente las variables de entorno, proceda del siguiente modo:

1. Arranque la VM que desea distribuir como plantilla.
2. En Windows, abra el cuadro de diálogo para activar variables de entorno.
3. Cree una nueva variable de sistema con el nombre "TiaUserSettingsPath".
4. Como valor indique la ruta al directorio de la red en el que deban guardarse las configuraciones de usuarios. Asegúrese de que indica el nombre del usuario en forma de variable "%USERNAME%".
5. Confirme las entradas realizadas con "Aceptar".
6. Cree otra 'variable de sistema' con el nombre "TiaDefaultProjectPath".

7. Como valor indique la ruta al directorio de la red que deba utilizarse como ubicación estándar para proyectos. El nombre del usuario se puede indicar en forma de variable "%USERNAME%" para guardar los proyectos en subdirectorios. Si no indica "%USERNAME%", todos los proyectos se guardarán en el mismo directorio.
8. Confirme las entradas realizadas con "Aceptar".
   Las variables "%USERNAME%" se resuelven con el siguiente inicio de sesión en la programadora o el PC. De este modo la ubicación de la configuración se adapta al usuario que inicia la sesión.

Consulte también

Crear una plantilla VM nueva (Página 31)

Utilizar un servidor de claves de licencia (Página 34)

Instalación del TIA Portal Cloud Connector en la VM (Página 35)

3.3 Utilizar un servidor de claves de licencia

Introducción

Al instalar el TIA Portal o el TIA Portal Cloud Connector se instala también el Automation License Manager (ALM). Este es necesario para la transferencia y el manejo de licencias.

Encontrará más información sobre el Automation License Manager y sobre cómo crear un servidor de licencias en la documentación de usuario del Automation License Manager.

Consulte también

Licencias (Página 27)

Asignar licencia del equipo del usuario (Página 27)

Crear una plantilla VM nueva (Página 31)

Almacenamiento centralizado de las configuraciones de usuario y de proyecto (Página 32)

Instalación del TIA Portal Cloud Connector en la VM (Página 35)

3.4 Instalación del TIA Portal Cloud Connector en la VM

Existen dos maneras de instalar el TIA Portal Cloud Connector en la VM:

- Instalación del TIA Portal Cloud Connector conjuntamente con el TIA Portal
  Existe la posibilidad de instalar el TIA Portal Cloud Connector conjuntamente con el TIA Portal. Para ello, active la opción "TIA Portal Cloud Connector" durante el proceso de instalación.
- Instalación del TIA Portal Cloud Connector sin el TIA Portal
  En el soporte de datos de instalación encontrará además un programa de instalación que le permitirá instalar el TIA Portal Cloud Connector sin TIA Portal. Este archivo de instalación se puede hacer accesible a otros usuarios a través de una unidad de red.

Instalación del Cloud Connector conjuntamente con TIA Portal

Para instalar el Cloud Connector conjuntamente con TIA Portal, proceda del siguiente modo:

1. Inserte el soporte de datos de instalación en la unidad de disco correspondiente.
   El programa de instalación arranca automáticamente a menos que el inicio automático esté desactivado en la programadora o el PC.
2. Si el programa de instalación no se inicia automáticamente, hágalo manualmente con un doble clic en el archivo "Start.exe".
   Se abre el cuadro de diálogo para seleccionar el idioma de instalación.
3. Elija el idioma en el que desea ver los cuadros de diálogo del programa de instalación.
4. Para leer las instrucciones del producto y de la instalación, haga clic en el botón "Leer indicaciones" o "Indicaciones de instalación".
   Se abre el archivo de ayuda correspondiente con las indicaciones.
5. Tras haberlas leído, cierre el archivo de ayuda y haga clic en el botón "Siguiente".
   Se abre el cuadro de diálogo para seleccionar los idiomas del producto.
6. Elija los idiomas para la interfaz del producto y haga clic en el botón "Siguiente".

   Nota

   El idioma base de instalación del producto es siempre "English".

   Se abre el cuadro de diálogo para seleccionar la configuración de producto.
7. Haga clic en el botón "Personalizada".
8. A continuación, active la casilla de verificación "TIA Portal Cloud Connector" y, en caso necesario, las casillas de verificación de otros productos que desee instalar.
9. Si desea crear un acceso directo a TIA Portal en el escritorio, active la casilla de verificación "Crear acceso directo en el escritorio".
10. Haga clic en el botón "Examinar" si desea cambiar el directorio de destino para la instalación. Tenga en cuenta que el nombre de la ruta de instalación no debe tener más de 89 caracteres.
11. Haga clic en el botón "Siguiente".
    Se abre el cuadro de diálogo correspondiente a las condiciones de licencia.

12. Para continuar la instalación, lea y acepte todos los acuerdos de licencia y haga clic en "Siguiente".
    En caso de que sea necesario modificar opciones de seguridad y permisos para la instalación de TIA Portal, se abrirá el cuadro de diálogo para la configuración de seguridad.
13. Para continuar la instalación, acepte todos los cambios efectuados en las opciones de seguridad y permisos y haga clic en "Siguiente".
    En el siguiente cuadro de diálogo aparecen listados los ajustes de instalación.
14. Compruebe los ajustes de instalación seleccionados. Si desea efectuar cambios, haga clic en el botón "Atrás" hasta acceder al ajuste que desea modificar del cuadro de diálogo. Una vez efectuados los cambios deseados, regrese a la vista general con "Siguiente".
15. Haga clic en el botón "Instalar".
    Se inicia la instalación.

    Nota

    Si durante la instalación no se encuentra ninguna clave de licencia (license key), existe la posibilidad de transferir ésta al PC. Si se omite la transferencia de licencias, este paso puede realizarse posteriormente con el Automation License Manager.

    Tras la instalación aparece un mensaje indicando si la instalación se ha completado correctamente.

16. Es posible que deba reiniciar el equipo. En ese caso, active el botón de opción "Sí, deseo reiniciar mi equipo ahora". A continuación, haga clic en el botón "Reiniciar".
17. Si no es preciso volver a iniciar el equipo, haga clic en el botón "Finalizar".

Instalación del Cloud Connector sin TIA Portal

Para instalar el Cloud Connector sin TIA Portal, proceda del siguiente modo:

1. Inserte el soporte de datos de instalación en la unidad de disco correspondiente o navegue en el sistema de archivos de su ordenador hasta el archivo de instalación.
   El archivo de instalación se encuentra en el soporte de datos de instalación, en el directorio "Support".
2. Haga doble clic en el archivo de instalación "TIA Portal Cloud Connector_<Versión>.exe".
   Se muestra el control de cuentas de usuario de Windows.
3. Confirme el control de cuentas de usuario con "Sí".
   Se abre el cuadro de diálogo de instalación.
4. Haga clic en "Siguiente".
   Aparece una selección de los idiomas de instalación disponibles.
5. Seleccione el idioma de instalación deseado y haga clic en "Siguiente".
   Los archivos necesarios se descomprimen y se abre el siguiente cuadro de diálogo de instalación.
6. Cierre otros programas que se estén ejecutando y haga clic en "Siguiente".
   Se muestran las condiciones de licencia.
7. Acepte las condiciones de licencia y haga clic en "Siguiente".
   Se muestran los programas disponibles para la instalación y la memoria necesaria.

8. Haga clic en "Siguiente".
   Se abre un cuadro de diálogo que muestra una vista general de los ajustes del sistema que cambiarán durante la instalación.
9. Active la casilla de verificación para aceptar los cambios.
10. Haga clic en "Siguiente".
    Se muestra una vista general de los programas que se van a instalar.
11. Haga clic en "Instalar".
    Se inicia la instalación.
12. Es posible que deba reiniciar el equipo. En ese caso, active el botón de opción "Sí, deseo reiniciar mi equipo ahora". A continuación, haga clic en el botón "Finalizar".

Consulte también

Crear una plantilla VM nueva (Página 31)

Almacenamiento centralizado de las configuraciones de usuario y de proyecto (Página 32)

Utilizar un servidor de claves de licencia (Página 34)

Uso de la máquina virtual (VM) 4

4.1 Instalación del TIA Portal Cloud Connector en la programadora o el PC

Nota

Tenga en cuenta las indicaciones siguientes:

- Se requiere una licencia válida para el TIA Portal Cloud Connector.
- Configuración del Firewall de Windows Para que funcione una conexión es necesario que en su Firewall esté ajustado en la ficha "Excepciones", en el servicio "Siemens SCP Remote Connection", el puerto ajustado en el TIA Portal Cloud Connector. La opción predeterminada en "Cualquiera".

Procedimiento

Para instalar el TIA Portal Cloud Connector, proceda del siguiente modo:

1. Inserte el soporte de datos de instalación en la unidad de disco correspondiente o navegue en el sistema de archivos de su ordenador hasta el archivo de instalación.
   El archivo de instalación se encuentra en el soporte de datos de instalación, en el directorio "Support".
2. Haga doble clic en el archivo de instalación "TIA Portal Cloud Connector_<Versión>.exe".
   Se muestra el control de cuentas de usuario de Windows.
3. Confirme el control de cuentas de usuario con "Sí".
   Se abre el cuadro de diálogo de instalación.
4. Haga clic en "Siguiente".
   Aparece una selección de los idiomas de instalación disponibles.
5. Seleccione el idioma de instalación deseado y haga clic en "Siguiente".
   Los archivos necesarios se descomprimen y se abre el siguiente cuadro de diálogo de instalación.
6. Cierre otros programas que se estén ejecutando y haga clic en "Siguiente".
   Se muestran las condiciones de licencia.
7. Acepte las condiciones de licencia y haga clic en "Siguiente".
   Se muestran los programas disponibles para la instalación y la memoria necesaria.
8. Haga clic en "Siguiente".
   Se abre un cuadro de diálogo que muestra una vista general de los ajustes del sistema que cambiarán durante la instalación.
9. Active la casilla de verificación para aceptar los cambios.
10. Haga clic en "Siguiente".
    Se muestra una vista general de los programas que se van a instalar.

11. Haga clic en "Instalar".
    Se inicia la instalación.
12. Es posible que deba reiniciar el equipo. En ese caso, active el botón de opción "Sí, deseo reiniciar mi equipo ahora". A continuación, haga clic en el botón "Finalizar".

Consulte también

Configuración del TIA Portal Cloud Connector en la programadora o el PC (Página 40)

Configuración del TIA Portal Cloud Connector en la VM (Página 42)

Conexión online mediante el TIA Portal Cloud Connector (Página 54)

Uso offline de la máquina virtual (VM) (Página 55)

4.2 Configuración del TIA Portal Cloud Connector en la programadora o el PC

Nota

Protocolo de comunicación

Para que la programadora o el PC puedan establecer una conexión con la VM es necesario definir un protocolo de comunicación. Por motivos de seguridad se recomienda utilizar siempre HTTPS a partir de Windows 8.1.

Configurar una conexión TCP

Para configurar una conexión TCP para la programadora o el PC, proceda del siguiente modo:

1. Haga clic con el botón derecho del ratón sobre el icono del TIA Portal Cloud Connector en el área de notificación de la barra de tareas, y elija el comando "Configuración".
   Se abre el TIA Portal Cloud Connector.
2. Abra la ficha "Configuración" y, en caso necesario, cambie el idioma de la interfaz de usuario del TIA Portal Cloud Connector.
3. Cambie a la ficha "General" y compruebe la función de comunicación. En caso necesario, cambie el ajuste a "Equipo del usuario".
4. Cambie a la ficha "Protocolo".
5. Active la casilla de verificación "Punto final de TCP".
6. Indique el puerto a través del que se realizará la comunicación. El puerto debe ser idéntico al asignado en el equipo remoto.
7. Abra de nuevo la ficha "General".
8. En el área "Comunicación Cloud Connector", haga clic en el botón "Activar comunicación".

Configurar una conexión HTTPS

Para configurar una conexión HTTPS para la programadora o el PC, proceda del siguiente modo:

1. Haga clic con el botón derecho del ratón sobre el icono del TIA Portal Cloud Connector en el área de notificación de la barra de tareas, y elija el comando "Configuración".
   Se abre el TIA Portal Cloud Connector.
2. Abra la ficha "Configuración" y, en caso necesario, cambie el idioma de la interfaz de usuario del TIA Portal Cloud Connector.
3. Cambie a la ficha "General" y compruebe la función de comunicación. En caso necesario, cambie el ajuste a "Equipo del usuario".
4. Cambie a la ficha "Protocolo".
5. Active la casilla de verificación "Punto final de HTTPS".
6. Cree un certificado nuevo para el cifrado de datos o bien seleccione un certificado ya existente de la memoria de certificados de Windows.
   Consulte también:
   Crear un certificado para el cifrado de datos (Página 44)
   Seleccionar un certificado para el cifrado de datos (Página 47)
7. Si en el equipo del usuario todavía no hay disponible ningún certificado para la autenticación del usuario, créelo en el equipo remoto y cópielo en una unidad de disco local del equipo del usuario.
   Consulte también:
   Crear un certificado para la autenticación de usuarios (Página 48)
8. Cambie a la ficha "Configuración".
9. Importe un certificado nuevo para la autenticación de usuario o bien agregue a la lista de certificados de confianza un certificado existente de la memoria de certificados de Windows.
   Consulte también:
   Importar un certificado para la autenticación de usuario (Página 50)
   Agregar un certificado para la autenticación de usuario (Página 51)
10. Abra de nuevo la ficha "General".
11. En el área "Comunicación Cloud Connector", haga clic en el botón "Activar comunicación".

Resultado

La programadora o el PC están preparados para la comunicación con la VM. A continuación, configure el TIA Portal Cloud Connector en la VM.

Consulte también

Instalación del TIA Portal Cloud Connector en la programadora o el PC (Página 39)

Configuración del TIA Portal Cloud Connector en la VM (Página 42)

Conexión online mediante el TIA Portal Cloud Connector (Página 54)

Uso offline de la máquina virtual (VM) (Página 55)

4.3 Configuración del TIA Portal Cloud Connector en la VM

Nota

Protocolo de comunicación

Para que una programadora o un PC puedan establecer una conexión con la VM es necesario definir el protocolo de comunicación que se utilizará. Por motivos de seguridad se recomienda utilizar siempre HTTPS a partir de Windows 8.1. Además, antes de aceptar una conexión compruebe la identidad del interlocutor que solicita la conexión.

Configurar una conexión TCP

Para configurar una conexión TCP para la VM, proceda del siguiente modo:

1. Establezca una conexión de escritorio remoto con la VM.
2. Haga clic con el botón derecho del ratón sobre el icono del TIA Portal Cloud Connector en el área de notificación de la barra de tareas, y elija el comando "Configuración".
   Se abre el TIA Portal Cloud Connector.
3. Abra la ficha "Configuración" y, en caso necesario, cambie el idioma de la interfaz de usuario del TIA Portal Cloud Connector.
4. Cambie a la ficha "General" y compruebe la función de comunicación. En caso necesario, cambie el ajuste a "Equipo remoto".
5. Abra la ficha "Protocolo".
6. En el área "Protocolo de comunicación" active el campo opcional "Configuración de TCP".
7. Seleccione un dispositivo de destino.

   Nota

   Conexión al SCALANCE

   Asegúrese de la conexión al SCALANCE esté protegida con SINEMA RC u otra tecnología de cifrado. De lo contrario los datos se transfieren no cifrados.

8. Introduzca la dirección IP del equipo del usuario o seleccione la entrada "Configuración automática" en la lista desplegable para hacer que la dirección se determine automáticamente.
9. Indique el puerto a través del que se realizará la comunicación. El puerto debe ser idéntico al asignado en el equipo del usuario.
10. Abra de nuevo la ficha "General".
11. En el área "Comunicación Cloud Connector", haga clic en el botón "Activar comunicación".

Configurar una conexión HTTPS

Para configurar una conexión HTTPS para la VM, proceda del siguiente modo:

1. Establezca una conexión de escritorio remoto con la VM.
2. Haga clic con el botón derecho del ratón sobre el icono del TIA Portal Cloud Connector en el área de notificación de la barra de tareas, y elija el comando "Configuración".
   Se abre el TIA Portal Cloud Connector.
3. Abra la ficha "Configuración" y, en caso necesario, cambie el idioma de la interfaz de usuario del TIA Portal Cloud Connector.
4. Abra la ficha "General" y compruebe la función de comunicación. En caso necesario, cambie el ajuste a "Equipo remoto".
5. Abra la ficha "Protocolo".
6. En el área "Protocolo de comunicación" active el campo opcional "Configuración de TCP".
7. Introduzca la dirección IP del equipo del usuario o seleccione la entrada "Configuración automática" en la lista desplegable para hacer que la dirección se determine automáticamente.
8. Importe el certificado para el cifrado de datos que se ha creado en el equipo del usuario o bien seleccione un certificado ya existente de la memoria de certificados de Windows.
   Consulte también:
   Importar un certificado para el cifrado de datos (Página 46)
   Seleccionar un certificado para el cifrado de datos (Página 47)
9. Cambie a la ficha "Configuración".
10. Cree un certificado nuevo para la autenticación de usuarios o bien seleccione un certificado ya existente de la memoria de certificados de Windows.
    Consulte también:
    Crear un certificado para la autenticación de usuarios (Página 48)
    Seleccionar un certificado para la autenticación de usuarios (Página 52)
11. Abra de nuevo la ficha "General".
12. En el área "Comunicación Cloud Connector", haga clic en el botón "Activar comunicación".

Resultado

El TIA Portal Cloud Connector está preparado para la comunicación. Una vez activados los dos interlocutores de la comunicación, desde el equipo del usuario se podrá acceder al hardware SIMATIC (PLC, HMI) conectado localmente al mismo.

Consulte también

Instalación del TIA Portal Cloud Connector en la programadora o el PC (Página 39)

Configuración del TIA Portal Cloud Connector en la programadora o el PC (Página 40)

Conexión online mediante el TIA Portal Cloud Connector (Página 54)

Uso offline de la máquina virtual (VM) (Página 55)

4.4 Utilizar certificados (solo para conexiones HTTPS)

4.4.1 Crear un certificado para el cifrado de datos

A partir de Windows 8.1 existe la posibilidad de utilizar una conexión HTTPS para la comunicación. Para incrementar la seguridad se requiere un certificado para el cifrado de datos que se crea en el equipo del usuario y es utilizado por el equipo remoto.

Procedimiento

Para crear un certificado para el cifrado de datos, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, en el equipo del usuario haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo del usuario)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active la casilla de verificación "Punto final de HTTPS".
   Se activan los botones "Crear" y "Seleccionar".
5. Haga clic en "Crear".
   Se abre el cuadro de diálogo "TIA Portal Cloud Connector - Crear certificado".
6. Introduzca un nombre de dominio o bien seleccione el dominio en la lista desplegable.

   Nota

   Pulsando el botón "+", el dominio se incorpora a la lista de dominios. Pulsando el botón "-", el dominio se elimina de la lista de dominios.

7. Haga clic en "Examinar".
   Se abre el cuadro de diálogo "Guardar como".
8. Elija una ubicación e introduzca un nombre de archivo para el certificado.
9. Haga clic en "Guardar".
10. Seleccione la fecha a partir de la cual debe ser válido el certificado.
11. Seleccione la fecha hasta la que debe ser válido el certificado.
12. Haga clic en "Aceptar".

Resultado

Se crea el certificado que se utilizará en el equipo del usuario para el punto final de HTTPS. También se guardará en la ubicación indicada en forma de archivo con la extensión ".cer" y desde allí podrá copiarse en el equipo remoto. Adicionalmente, el certificado se agrega a la memoria de certificados de Windows.

Consulte también

Uso de certificados (Página 20)

Exportar un certificado para el cifrado de datos (Página 45)

Importar un certificado para el cifrado de datos (Página 46)

Seleccionar un certificado para el cifrado de datos (Página 47)

4.4.2 Exportar un certificado para el cifrado de datos

El certificado que se utiliza para el cifrado de datos puede exportarse en cualquier momento.

Requisitos

El certificado para el cifrado de datos se ha creado anteriormente y se muestra debajo del punto final de HTTPS del equipo del usuario.

Procedimiento

Para exportar un certificado para el cifrado de datos, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, en el equipo del usuario haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo del usuario)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active la casilla de verificación "Punto final de HTTPS".
   Se activan los botones "Crear", "Seleccionar" y "Exportar".
5. Haga clic en "Exportar".
   Se abre el cuadro de diálogo "Guardar como".
6. Elija una ubicación e introduzca un nombre para el certificado.
7. Haga clic en "Guardar".

Resultado

El certificado que se utiliza actualmente para el cifrado de datos se guarda en la ubicación indicada en forma de archivo con la extensión ".cer".

Consulte también

Uso de certificados (Página 20)

Crear un certificado para el cifrado de datos (Página 44)

Importar un certificado para el cifrado de datos (Página 46)

Seleccionar un certificado para el cifrado de datos (Página 47)

4.4.3 Importar un certificado para el cifrado de datos

Para poder establecer una conexión HTTPS entre el equipo del usuario y el equipo remoto, es imprescindible importar al TIA Portal Cloud Connector del equipo remoto el certificado creado en el equipo del usuario para el cifrado de datos.

Requisitos

- El certificado para el cifrado de datos se ha creado en el equipo del usuario.
- El certificado para el cifrado de datos se ha copiado a una unidad de disco local del equipo remoto.

Procedimiento

Para importar un certificado para el cifrado de datos al TIA Portal Cloud Connector del equipo remoto, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, en el equipo remoto haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo remoto)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active el botón de opción "Configuración de HTTPS".
   Se activan los botones "Importar" y "Seleccionar".
5. Haga clic en "Importar".
   Se abrirá el cuadro de diálogo "Abrir".
6. Seleccione el archivo de certificado en el sistema de archivos. Los archivos de certificado se reconocen por la extensión ".cer" en el nombre de archivo.
7. Haga clic en "Abrir".

Resultado

El certificado se importa y se utiliza de inmediato para la comunicación. Adicionalmente, el certificado se agrega a la memoria de certificados de Windows.

Consulte también

Uso de certificados (Página 20)

Crear un certificado para el cifrado de datos (Página 44)

Exportar un certificado para el cifrado de datos (Página 45)

Seleccionar un certificado para el cifrado de datos (Página 47)

4.4.4 Seleccionar un certificado para el cifrado de datos

Existe la posibilidad de seleccionar un certificado para el cifrado de datos en la memoria de certificados de Windows. Puede hacerse tanto en el equipo del usuario como en el equipo remoto.

Requisitos

El certificado para el cifrado de datos se ha creado (equipo del usuario) o importado (equipo remoto) anteriormente y está disponible en la memoria de certificados de Windows.

Procedimiento

Para seleccionar un certificado existente para el cifrado de datos en la memoria de certificados de Windows y utilizarlo, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo del usuario)" o "Configuración (equipo remoto)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active la casilla de verificación "Punto final de HTTPS" (equipo del usuario) o el botón de opción "Configuración de HTTPS" (equipo remoto).
   Se activa el botón "Seleccionar".
5. Haga clic en "Seleccionar".
   Se abrirá el cuadro de diálogo "Seguridad de Windows" y se mostrarán los certificados disponibles.
6. Seleccione un certificado. En caso necesario puede visualizar propiedades adicionales del certificado.
7. Haga clic en "Aceptar".

Resultado

El certificado seleccionado se utiliza para la comunicación. Para que la comunicación sea posible, tanto en el equipo del usuario como en el equipo remoto debe estar ajustado el mismo certificado.

Consulte también

Uso de certificados (Página 20)

Crear un certificado para el cifrado de datos (Página 44)

Exportar un certificado para el cifrado de datos (Página 45)

Importar un certificado para el cifrado de datos (Página 46)

4.4.5 Crear un certificado para la autenticación de usuarios

A partir de Windows 8.1 existe la posibilidad de utilizar una conexión HTTPS para la comunicación. Para incrementar la seguridad se requiere un certificado para la autenticación de usuario que se crea en el equipo remoto y es utilizado por el equipo del usuario.

Procedimiento

Para crear un certificado para la autenticación de usuario, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, en el equipo remoto haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo remoto)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active el botón de opción "Configuración de HTTPS".
   En la ficha "Configuración" se activa el área de la autenticación de usuarios.
5. Cambie a la ficha "Configuración".
6. En el área "Autenticación de usuario", haga clic en el botón "Crear".
   Se abre el cuadro de diálogo "TIA Portal Cloud Connector - Autenticación de usuario".
7. Introduzca un nombre para el nuevo certificado en el campo "Nombre de certificado".
8. Haga clic en "Examinar".
   Se abre el cuadro de diálogo "Guardar como".
9. Elija una ubicación e introduzca un nombre de archivo para el certificado.
10. Haga clic en "Guardar".
11. Seleccione la fecha a partir de la cual debe ser válido el certificado.
12. Seleccione la fecha hasta la que debe ser válido el certificado.
13. Haga clic en "OK".

Resultado

Se crea el certificado que se utilizará en el equipo remoto. También se guardará en la ubicación indicada en forma de archivo con la extensión ".cer" y desde allí podrá copiarse en el equipo del usuario. Adicionalmente, el certificado se agrega a la memoria de certificados de Windows.

Consulte también

Uso de certificados (Página 20)

Exportar un certificado para la autenticación de usuarios (Página 49)

Importar un certificado para la autenticación de usuarios (Página 50)

Agregar un certificado para la autenticación de usuario (Página 51)

Seleccionar un certificado para la autenticación de usuarios (Página 52)

Eliminar un certificado para la autenticación de usuarios (Página 53)

4.4.6 Exportar un certificado para la autenticación de usuarios

A la hora de crear el certificado para la autenticación de usuarios es imprescindible exportarlo para que esté a disposición de un equipo de usuario. El certificado que se utiliza actualmente puede exportarse en cualquier momento.

Requisitos

El certificado para la autenticación de usuarios se ha creado previamente en el equipo remoto y se muestra en "Autenticación de usuario" de la ficha "Configuración".

Procedimiento

Para exportar un certificado para la autenticación de usuarios, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, en el equipo remoto haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo remoto)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active el botón de opción "Configuración de HTTPS".
   En la ficha "Configuración" se activa el área de la autenticación de usuarios.
5. Cambie a la ficha "Configuración".
6. En el área "Autenticación de usuario", haga clic en el botón "Exportación".
   Se abre el cuadro de diálogo "Guardar como".
7. Elija una ubicación e introduzca un nombre para el certificado.
8. Haga clic en "Guardar".

Resultado

El certificado que se utiliza actualmente para la autenticación de usuarios se guarda en la ubicación indicada en forma de archivo con la extensión ".cer".

Consulte también

Uso de certificados (Página 20)
Crear un certificado para la autenticación de usuarios (Página 48)
Importar un certificado para la autenticación de usuarios (Página 50)
Agregar un certificado para la autenticación de usuario (Página 51)
Seleccionar un certificado para la autenticación de usuarios (Página 52)
Eliminar un certificado para la autenticación de usuarios (Página 53)

4.4.7 Importar un certificado para la autenticación de usuarios

Para poder establecer una conexión HTTPS entre el equipo del usuario y el equipo remoto, es imprescindible importar al TIA Portal Cloud Connector del equipo del usuario el certificado creado en el equipo remoto para la autenticación de usuarios.

Requisitos

- El certificado para la autenticación de usuarios se ha creado en el equipo remoto.
- El certificado para la autenticación de usuarios se ha copiado a una unidad de disco local del equipo del usuario.

Procedimiento

Para importar un certificado para la autenticación de usuarios, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, en el equipo del usuario haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo del usuario)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active la casilla de verificación "Punto final de HTTPS".
   En la ficha "Configuración" se activa el área de la autenticación de usuarios.
5. Cambie a la ficha "Configuración".
6. En el área "Autenticación de usuario", haga clic en el botón "Importar".
   Se abrirá el cuadro de diálogo "Abrir".
7. Seleccione el archivo de certificado en el sistema de archivos. Los archivos de certificado se reconocen por la extensión ".cer" en el nombre de archivo.
8. Haga clic en "Abrir".

Resultado

El certificado se importa y se agrega a la lista de certificados de confianza. Desde esta lista es posible establecer los equipos remotos con los que puede comunicarse el equipo del usuario. El equipo remoto al que se accede en cada caso debe tener integrado el mismo certificado para la autenticación de usuarios.

Consulte también

Uso de certificados (Página 20)

Crear un certificado para la autenticación de usuarios (Página 48)

Exportar un certificado para la autenticación de usuarios (Página 49)

Agregar un certificado para la autenticación de usuario (Página 51)

Seleccionar un certificado para la autenticación de usuarios (Página 52)

Eliminar un certificado para la autenticación de usuarios (Página 53)

4.4.8 Agregar un certificado para la autenticación de usuario

En lugar de un certificado del sistema de archivos, también es posible agregarlo a la lista de certificados de confianza desde la memoria de certificados de Windows.

Requisitos

El certificado deseado está disponible en la memoria de certificados de Windows.

Procedimiento

Para agregar un certificado para la autenticación de usuarios desde la memoria de certificados de Windows, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, en el equipo del usuario haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo del usuario)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active la casilla de verificación "Punto final de HTTPS".
   En la ficha "Configuración" se activa el área de la autenticación de usuario.
5. Cambie a la ficha "Configuración".
6. En el área "Autenticación de usuario", haga clic en el botón "Agregar".
   Se abrirá el cuadro de diálogo "Seleccionar certificado" y se mostrarán los certificados disponibles.
7. Seleccione un certificado. En caso necesario puede visualizar el certificado.
8. Haga clic en "OK".

Resultado

El certificado de la memoria de certificados de Windows se agrega a la lista de certificados de confianza. Desde esta lista es posible establecer los equipos remotos con los que puede comunicarse el equipo del usuario. El equipo remoto al que se accede en cada caso debe tener integrado el mismo certificado para la autenticación de usuarios.

Consulte también

Uso de certificados (Página 20)

Crear un certificado para la autenticación de usuarios (Página 48)

Exportar un certificado para la autenticación de usuarios (Página 49)

Importar un certificado para la autenticación de usuarios (Página 50)

Seleccionar un certificado para la autenticación de usuarios (Página 52)

Eliminar un certificado para la autenticación de usuarios (Página 53)

4.4.9 Seleccionar un certificado para la autenticación de usuarios

En lugar de crear un certificado nuevo para la autenticación de usuarios en el equipo remoto, también es posible seleccionar y utilizar un certificado existente de la memoria de certificados de Windows.

Requisitos

El certificado para la autenticación de usuarios se ha creado anteriormente y está disponible en la memoria de certificados de Windows.

Procedimiento

Para seleccionar un certificado para la autenticación de usuarios desde la memoria de certificados de Windows, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, en el equipo remoto haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo remoto)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active el botón de opción "Configuración de HTTPS".
   En la ficha "Configuración" se activa el área de la autenticación de usuarios.
5. Cambie a la ficha "Configuración".
6. En el área "Autenticación de usuario", haga clic en el botón "Seleccionar".
   Se abrirá el cuadro de diálogo "Seguridad de Windows" y se mostrarán los certificados disponibles.

7. Seleccione un certificado. En caso necesario puede visualizar propiedades adicionales del certificado.
8. Haga clic en "OK".

Resultado

El certificado se utiliza en el equipo remoto para la autenticación de usuarios. En caso necesario puede exportarse para intercambiarlo con el equipo del usuario.

Consulte también

Uso de certificados (Página 20)

Crear un certificado para la autenticación de usuarios (Página 48)

Exportar un certificado para la autenticación de usuarios (Página 49)

Importar un certificado para la autenticación de usuarios (Página 50)

Agregar un certificado para la autenticación de usuario (Página 51)

Eliminar un certificado para la autenticación de usuarios (Página 53)

4.4.10 Eliminar un certificado para la autenticación de usuarios

Un certificado para la autenticación de usuarios en el equipo del usuario puede eliminarse en cualquier momento de la lista de certificados de confianza.

Procedimiento

Para eliminar un certificado para la autenticación de usuarios de la lista de certificados de confianza, proceda del siguiente modo:

1. Para abrir el TIA Portal Cloud Connector, en el equipo del usuario haga clic con el botón derecho del ratón sobre el icono de estado del TIA Portal Cloud Connector en el área de notificación de la barra de tareas de Windows.
2. En el menú contextual, elija el comando "Configuración (equipo del usuario)".
   Se abre la ventana de configuración del TIA Portal Cloud Connector.
3. Cambie a la ficha "Protocolo".
4. Active la casilla de verificación "Punto final de HTTPS".
   En la ficha "Configuración" se activa el área de la autenticación de usuarios.
5. Cambie a la ficha "Configuración".
6. Seleccione el certificado que desea eliminar en la lista de certificados de confianza.
7. En el área "Autenticación de usuario", haga clic en el botón "Eliminar".

Resultado

El certificado se elimina de la lista de certificados de confianza. Ahora ya no es posible establecer una conexión con el equipo remoto que utiliza este certificado para la autenticación de usuarios.

Consulte también

Uso de certificados (Página 20)

Crear un certificado para la autenticación de usuarios (Página 48)

Exportar un certificado para la autenticación de usuarios (Página 49)

Importar un certificado para la autenticación de usuarios (Página 50)

Agregar un certificado para la autenticación de usuario (Página 51)

Seleccionar un certificado para la autenticación de usuarios (Página 52)

4.5 Conexión online mediante el TIA Portal Cloud Connector

Introducción

Si para la conexión con el hardware se utiliza el TIA Portal Cloud Connector, la forma de trabajar en TIA Portal no se diferenciará de la forma de trabajar con una conexión online normal con el hardware. En cuanto se activa la comunicación por túnel, los datos se pueden compilar, cargar y observar como de costumbre.

Para más información sobre el establecimiento de una conexión online y sobre el trabajo en modo online, consulte la Ayuda en pantalla de TIA Portal.

Vista general de los símbolos de estado

Si se establece una conexión mediante el TIA Portal Cloud Connector, en el área de notificación de la barra de tareas de Windows se muestran símbolos de estado que indican el estado de la conexión. La tabla siguiente muestra una vista general de los símbolos de estado y sus significados:

Símbolo de estado	Significado
	La comunicación está desactivada.
	La comunicación está activada pero no hay intercambio de datos entre el TIA Portal y el hardware de automatización SIMATIC.
	La comunicación está activada y hay intercambio de datos entre el TIA Portal y el hardware de automatización SIMATIC.
	El intercambio de datos entre el TIA Portal y el hardware de automatización SIMATIC se ha interrumpido. Se muestra el indicador de estado y se proporcionan más detalles sobre la causa.

Indicador de estado

Mediante el área de notificación de la barra de tareas de Windows se puede visualizar un indicador de estado tanto en el equipo remoto como en el equipo usuario. De este modo se abre la ventana "TIA Portal Cloud Connector - Equipo remoto" o "TIA Portal Cloud Connector - Equipo del usuario". En esta ventana se proporciona toda la información y se muestran las advertencias y los mensajes de error del TIA Portal Cloud Connector. Además se indica el tiempo que lleva establecida una conexión TCP o HTTPS.

El indicador de estado se puede cerrar en cualquier momento.

Consulte también

Instalación del TIA Portal Cloud Connector en la programadora o el PC (Página 39)

Configuración del TIA Portal Cloud Connector en la programadora o el PC (Página 40)

Configuración del TIA Portal Cloud Connector en la VM (Página 42)

Uso offline de la máquina virtual (VM) (Página 55)

4.6 Uso offline de la máquina virtual (VM)

También existe la posibilidad de trabajar offline con una máquina virtual. Para ello, la VM se copia desde el equipo remoto a la programadora o el PC. A continuación, la VM puede arrancarse en la programadora o el PC y utilizarse TIA Portal con el hardware que esté conectado a la programadora o el PC o que esté conectado a la red.

Existen las posibilidades siguientes de utilizar la VM:

- El hardware está conectado a la programadora o el PC mediante Ethernet y se encuentra en la misma subred.
- El hardware está conectado a la programadora o el PC mediante Ethernet o Profibus y se encuentra en otra subred.

El TIA Portal Cloud Connector no es necesario para todos los tipos de conexión. Se distinguen los casos siguientes:

- Si el hardware está conectado directamente con la programadora o el PC a través de un adaptador Ethernet o USB, se puede ajustar "Bridged" como conexión de red.
  Para este tipo de conexión debe estar desactivado el TIA Portal Cloud Connector en la VM.
- Si su hardware está conectado a la red a través de un adaptador de red o de USB puede usar la opción "Host-only". En este caso debe estar desactivado el TIA Portal Cloud Connector en la VM para poder usar también la interfaz PROFIBUS.

Después de utilizarla localmente, la VM puede copiarse de nuevo al equipo remoto.

Requisitos

- En la programadora o el PC está instalado el software adecuado para poder arrancar la VM, p. ej. VMware Workstation.
- En la programadora o el PC está instalado el Automation License Manager .

Transferencia de la máquina virtual (VM) desde el equipo remoto a la programadora o PC

Para trabajar offline con la máquina virtual, proceda del siguiente modo:

1. Copie la VM a la programadora o PC local. El procedimiento exacto depende del entorno de virtualización utilizado. Si necesita ayuda, consulte la documentación correspondiente.
2. Abra el Automation License Manager y transfiera a la unidad de disco local las licencias necesarias para el software SIMATIC en TIA Portal.
3. Copie todos los datos de proyecto necesarios desde el servidor a la unidad de disco local.
4. Arranque la VM y configure la conexión de red. Tenga en cuenta las indicaciones al principio de la página.

Transferencia de la máquina virtual (VM) desde la programadora o PC al equipo remoto

Para transferir de nuevo la máquina virtual al equipo remoto, proceda del siguiente modo:

- Copie la VM desde la programadora o PC local al equipo remoto. El procedimiento exacto depende del entorno de virtualización utilizado. Si necesita ayuda, consulte la documentación correspondiente.
- Abra el Automation License Manager y transfiera las licencias desde la unidad de disco local hasta el ALM Server.
- Copie todos los datos de proyecto necesarios desde la unidad de disco local al servidor.

Consulte también

Instalación del TIA Portal Cloud Connector en la programadora o el PC (Página 39)

Configuración del TIA Portal Cloud Connector en la programadora o el PC (Página 40)

Configuración del TIA Portal Cloud Connector en la VM (Página 42)

Conexión online mediante el TIA Portal Cloud Connector (Página 54)

Índice alfabético

A

Área de notificación, 7

B

Barra de tareas, 7

C

Certificado, 20
  Agregar, 51
  Crear, 44, 48
  Eliminar, 53
  Exportar, 45, 49
  Importar, 46, 50
  Seleccionar, 47, 52
Conexión online, 54
Configuración, 7
Configurar una conexión HTTPS, 41, 43
Configurar una conexión TCP, 40, 42

I

Indicador de estado, 14, 55
Interfaz de usuario, 7

P

PG/PC
  Configurar, 40

S

Símbolos de estado, 54
Simulación, 19
Support Packages, 20

T

TIA Portal Cloud Connector
  Aplicación, 17
  Certificado, 20
  Conexión online, 54
  Configurar, 7
  Disponibilidad, 6
  Indicador de estado, 14
  Interfaz de usuario, 7
  Principios básicos, 5

V

VM
  Configurar, 42