



S7-1200: controlador básico con Funciones avanzadas

Funciones de seguridad integradas

Seguridad Industrial Certificados Otorgados



- Dispositivos basados en Ethernet TIA •
P. ej., S7-1500, 1505S, S7-300, CP343-1
SCALANCE S, ...
- Protección contra ataques DoS
- Comportamiento definido en caso de ataque
- Disponibilidad mejorada

Encuentre más información: <https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security/certification-standards.html>

Sin restricciones © Siemens 2020



- Proceso de desarrollo
- Certificación de “Producto Seguro”
Ciclo de vida del desarrollo para
División DF y PD en base a
CEI 62443-4-1



- Controladores S7-1500 •
SCALANCE XM408-8C
- Certificación de primer nivel de seguridad
(CSPN – Certificación de Seguridad de Premier Niveau)

Encuentre más
información: http://ssi.gouv.fr/certification_cspn/simatic-s7-1518-4-version-du-micrologiciel-1-83/, http://www.ssi.gouv.fr/entreprise/certification_cspn/scalance-xm408-8c/

usa.siemens.com/s7-1200

SIEMENS
Ingenuity for life



Seguridad Industrial

La solución de Siemens para la integridad del sistema



Defense in depth



Seguridad Integrada

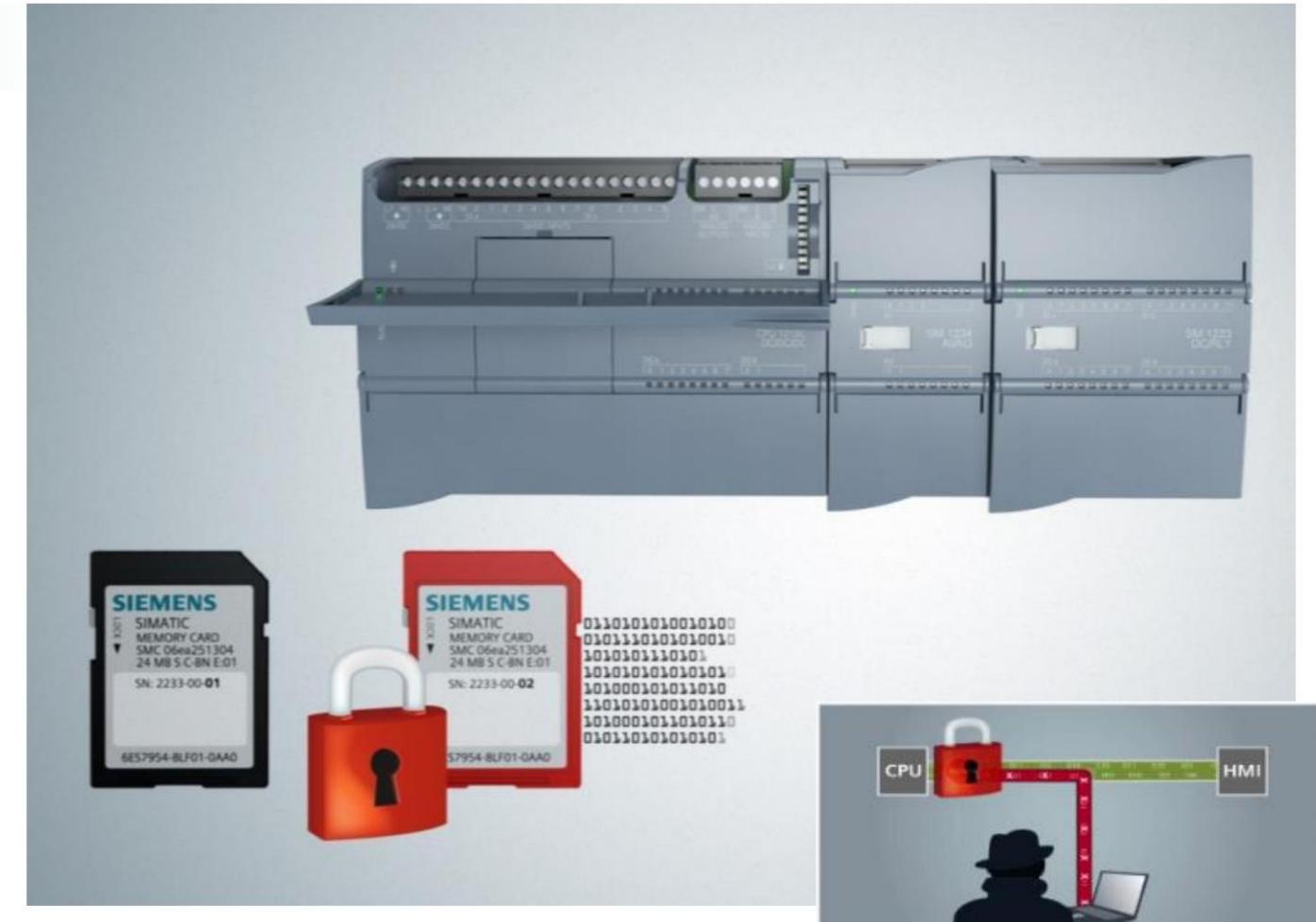
Descripción general de las características de seguridad del S7-1200



Integridad del sistema

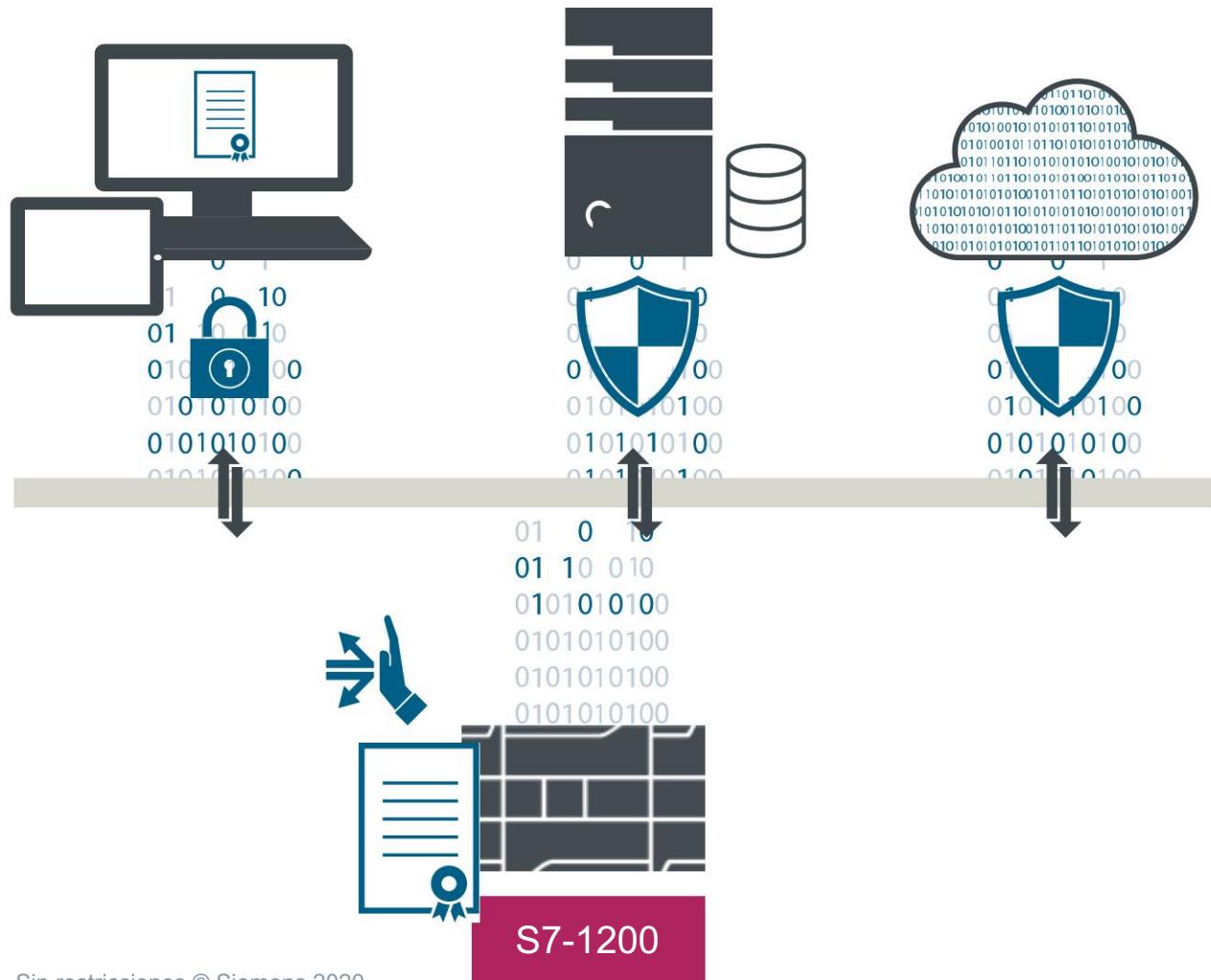
- Protección de proyecto fuera de línea (UMAC)
- Protección de acceso
- Autorización multifactorial
- Protección contra manipulación
- Protección del saber hacer
- Protección de acceso al servidor web
- Autenticación de certificados
- Comunicaciones seguras

(OPC UA, HTTPS, FTPS, TLS...)



OPC UA

Mecanismos de seguridad integrados



Seguridad OPC UA



Políticas de seguridad
seleccionables en Controlador y Clientes



Autenticación de dispositivos/aplicaciones
basada en certificados



Protección de la
integridad y comunicación cifrada



Autenticación de usuarios y acceso
restringido a etiquetas de PLC



Contraseñas de seguridad para demostración



Contraseñas de nivel de acceso:

Acceso completo (lectura/escritura): Siemens1!

Acceso de lectura (solo lectura): solo lectura

Acceso HMI: <ninguno>

Inicio de sesión de usuario de HMI

Nombre de usuario	Contraseña	Derechos de acceso
OEM	OEM	Administración (lectura/escritura)
Werner	Werner	Operador (solo lectura)
<ninguno>	<ninguno>	Operar solo HMI

Proyecto fuera de línea (UMAC)

Contraseña:

Usuario: Siemens1!

Contraseña: Siemens1!

Protección del saber hacer

Contraseña (FB2):

Contraseña: S3curity

Protección de escritura

Contraseña (FB6):

Contraseña: FB6_write

Usuario del servidor web y

Contraseña:

Usuario: Siemens1!

Contraseña: Siemens1!





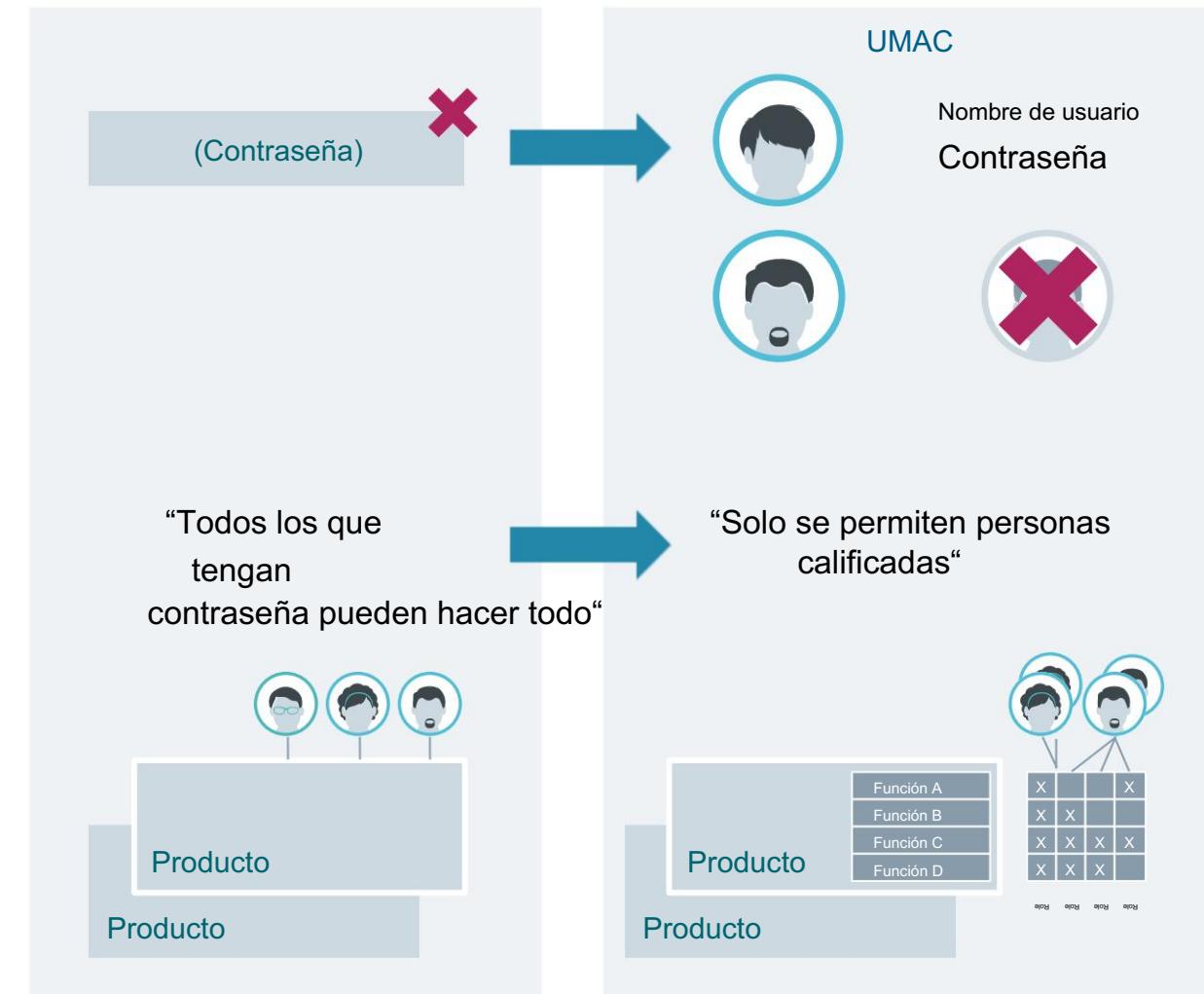
Gestión de Usuarios y Control de Acceso (UMAC)

Gestión de Usuarios y Control de Acceso UMAC en TIA Portal

¿Qué pretende?

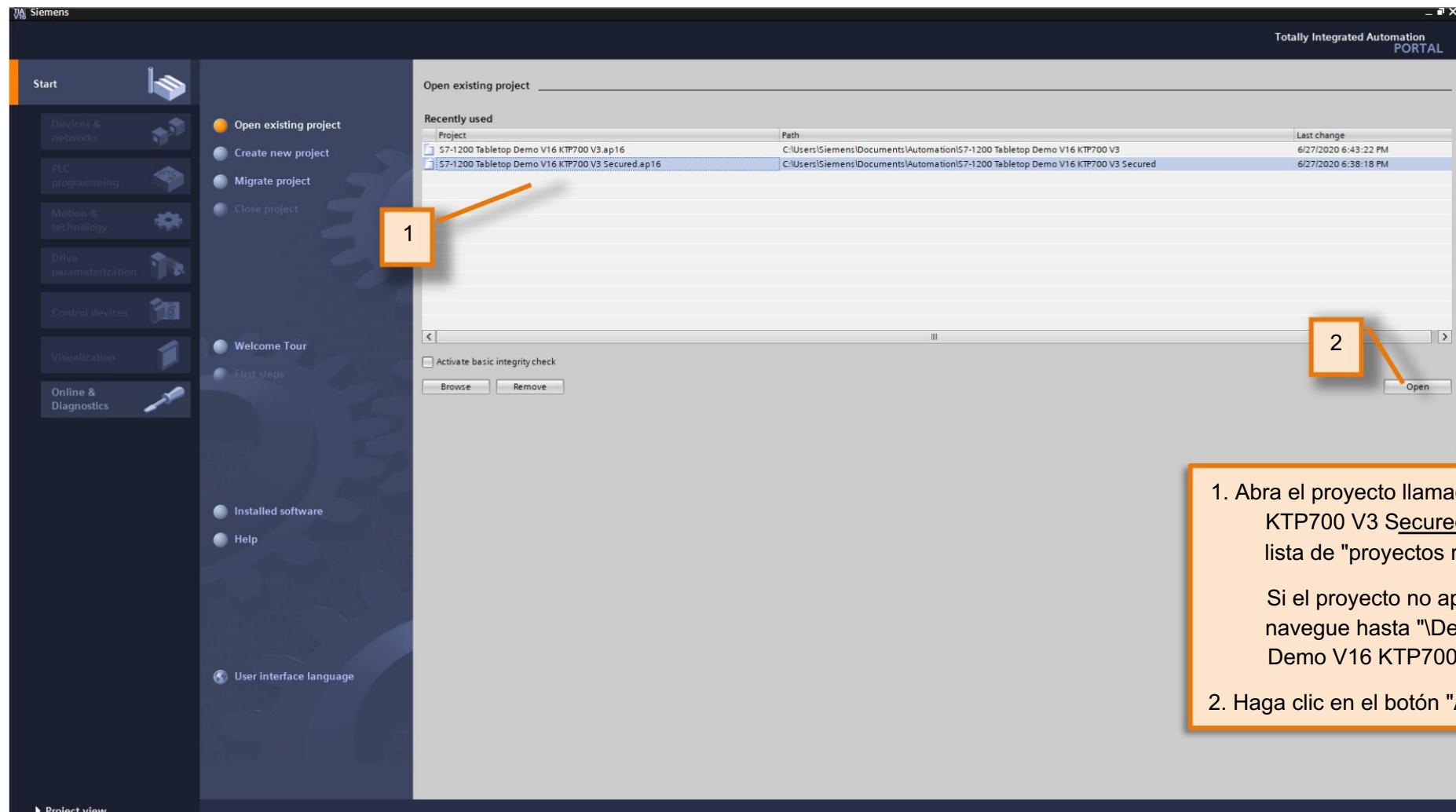


- Seguridad: Protección de máquinas/plantas industriales** • Acceso personalizado en lugar de acceso con contraseña
- Se evita el acceso no autorizado



Características de seguridad

UMAC - Abriendo un proyecto asegurado



1. Abra el proyecto llamado 'S7-1200 Tabletop Demo KTP700 V3 Secured.ap16' haciendo doble clic en él en la lista de "proyectos recientes".

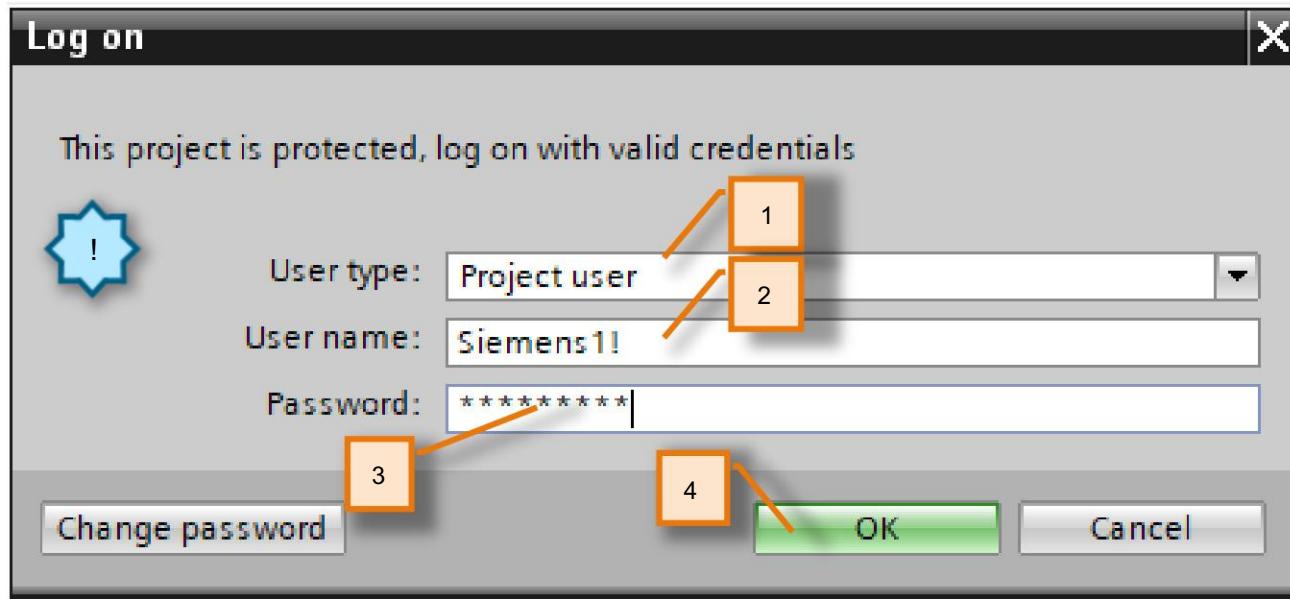
Si el proyecto no aparece en la lista, presione Examinar y navegue hasta "\Desktop\S7-1200 Event\S7-1200 Tabletop Demo V16 KTP700 V3 Secured.ap16"

2. Haga clic en el botón "Abrir".



Características de seguridad

UMAC - Ingreso de contraseña de usuario



SIEMENS
Ingenuity for life



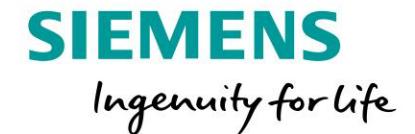
Observe que al abrir el proyecto, se le solicita que ingrese una información de usuario/contraseña. Este proyecto está protegido con contraseña para diferentes usuarios. Cada usuario puede tener diferentes funciones habilitadas.

1. Seleccione el tipo de usuario "Usuario del proyecto" en el menú desplegable menú
2. Introduzca el nombre de usuario: Siemens1!
3. Introduzca la contraseña: Siemens1!
4. Haga clic en Aceptar.
5. Vaya a la vista Proyecto y guarde el proyecto en un nombre/directorio diferente.



Características de seguridad

UMAC - Usuarios y Reglas



TIA Siemens - C:\Users\Siemens\Documents\Automation\S7-1200 Tabletop Demo V16 KTP700 V3 Secured\S7-1200 Tabletop Demo V16 KTP700 V3 Secured

Project Edit View Insert Online Options Tools Window Help

Save project Go online Go offline Search in project

Project tree

- Devices
- Plant objects

Name Version

- S7-1200 Tabletop Demo V16 KTP700 V3 Secured
 - Add new device
 - Devices & networks
 - CPU 1215C [CPU 1215C DC/DC/DC]
 - HMI KTP700 [KTP700 Basic PN]
 - Ungrouped devices
 - Security settings
 - Settings
 - Users and roles
 - Security features
 - Cross-device functions
 - Common data
 - Documentation settings
 - Languages & resources
 - Version control interface
 - Online access
 - Card Reader/USB memory

S7-1200 Tabletop Demo V16 KTP700 V3 Secured > Security settings > Users and roles

Users

User name	Password	Authentication
Siemens1!	*****	Password
User2	*****	Password
<Add new user>		

Assigned user groups **Assigned roles** **Assigned rights**

Assigned roles

Assigned to	Name	Description
<input checked="" type="checkbox"/>	Engineering administrator	System-defined role "Engineering a..."
<input type="checkbox"/>	Engineering standard	System-defined role "Engineering s..."
<input type="checkbox"/>	HMI Administrator	System-defined role "HMI Administ..."
<input type="checkbox"/>	HMI Operator	System-defined role "HMI Operator"
<input type="checkbox"/>	HMI Monitor	System-defined role "HMI Monitor"
<input type="checkbox"/>	NET Administrator	System-defined role "NET Administr..."
<input type="checkbox"/>	NET Standard	System-defined role "NETStandard"
<input type="checkbox"/>	NET Diagnose	System-defined role "NETDiagnose"
<input type="checkbox"/>	NET Remote Access	System-defined role "NETRemote A..."
<input type="checkbox"/>	NET Administrator Radius	System-defined role "NETAdministratorRadius"
<input type="checkbox"/>	NET Radius	System-defined role "NETRadius"
<input type="checkbox"/>	Read Only	User-defined role
<input checked="" type="checkbox"/>	Admin	User-defined role

1. Vaya a la configuración de Seguridad en el árbol del proyecto y haga doble clic en 'Usuarios y roles'.

2. Aviso Hay dos usuarios para este proyecto:

- 'Siemens1!' Tiene plenos derechos de administrador
- 'User2' está limitado a un rol de sólo lectura.

Un usuario con rol de 'Administrador de Ingeniería' puede crear nuevos usuarios, nuevos Roles y asignar Roles a los diferentes usuarios

2

Users

User name	
Siemens1!	
User2	
<Add new user>	

Assigned user groups

Assigned roles

Assigned to	Name	Description
<input type="checkbox"/>	Engineering administrator	System-defined role "Engineering a..."
<input type="checkbox"/>	Engineering standard	System-defined role "Engineering s..."
<input type="checkbox"/>	HMI Administrator	System-defined role "HMI Administ..."
<input type="checkbox"/>	HMI Operator	System-defined role "HMI Operator"
<input type="checkbox"/>	HMI Monitor	System-defined role "HMI Monitor"
<input type="checkbox"/>	NET Administrator	System-defined role "NET Administr..."
<input type="checkbox"/>	NET Standard	System-defined role "NETStandard"
<input type="checkbox"/>	NET Diagnose	System-defined role "NETDiagnose"
<input type="checkbox"/>	NET Remote Access	System-defined role "NETRemote A..."
<input type="checkbox"/>	NET Administrator Radius	System-defined role "NETAdministratorRadius"
<input type="checkbox"/>	NET Radius	System-defined role "NETRadius"
<input checked="" type="checkbox"/>	Read Only	User-defined role
<input type="checkbox"/>	Admin	User-defined role





Protección de nivel de acceso a la CPU

Características de seguridad

Protección de acceso a la CPU



Access level _____

Select the access level for the PLC.

Access level	Access			Access permi...
	HMI	Read	Write	
<input type="radio"/> Full access (no protection)	✓	✓	✓	*****
<input type="radio"/> Read access	✓	✓		*****
<input type="radio"/> HMI access	✓			*****
<input checked="" type="radio"/> No access (complete protection)				

No access (complete protection):
TIA Portal users and HMI applications will not have access to any functions.

Mandatory password:
For full access, TIA Portal users need to enter the "full access" password.

Optional password:
A "read access" password can be defined for read access to all functions.
For access by HMI applications, an "HMI access" password can be defined.

Some HMI devices do not support all possible characters. If you want to access the PLC from an HMI device, use only the standard characters. Please refer to the documentation of the device.

La siguiente diapositiva describe cómo configurar un nivel de acceso e ingresar contraseñas para una CPU S7-1200 a partir de V4.

Para una CPU S7-1200, puede ingresar varias contraseñas y, por lo tanto, configurar diferentes derechos de acceso para grupos de usuarios individuales.

Las contraseñas se ingresan en una tabla de tal manera que se asigna exactamente un nivel de acceso a cada contraseña.

El efecto de la contraseña se indica en la columna "Nivel de acceso".

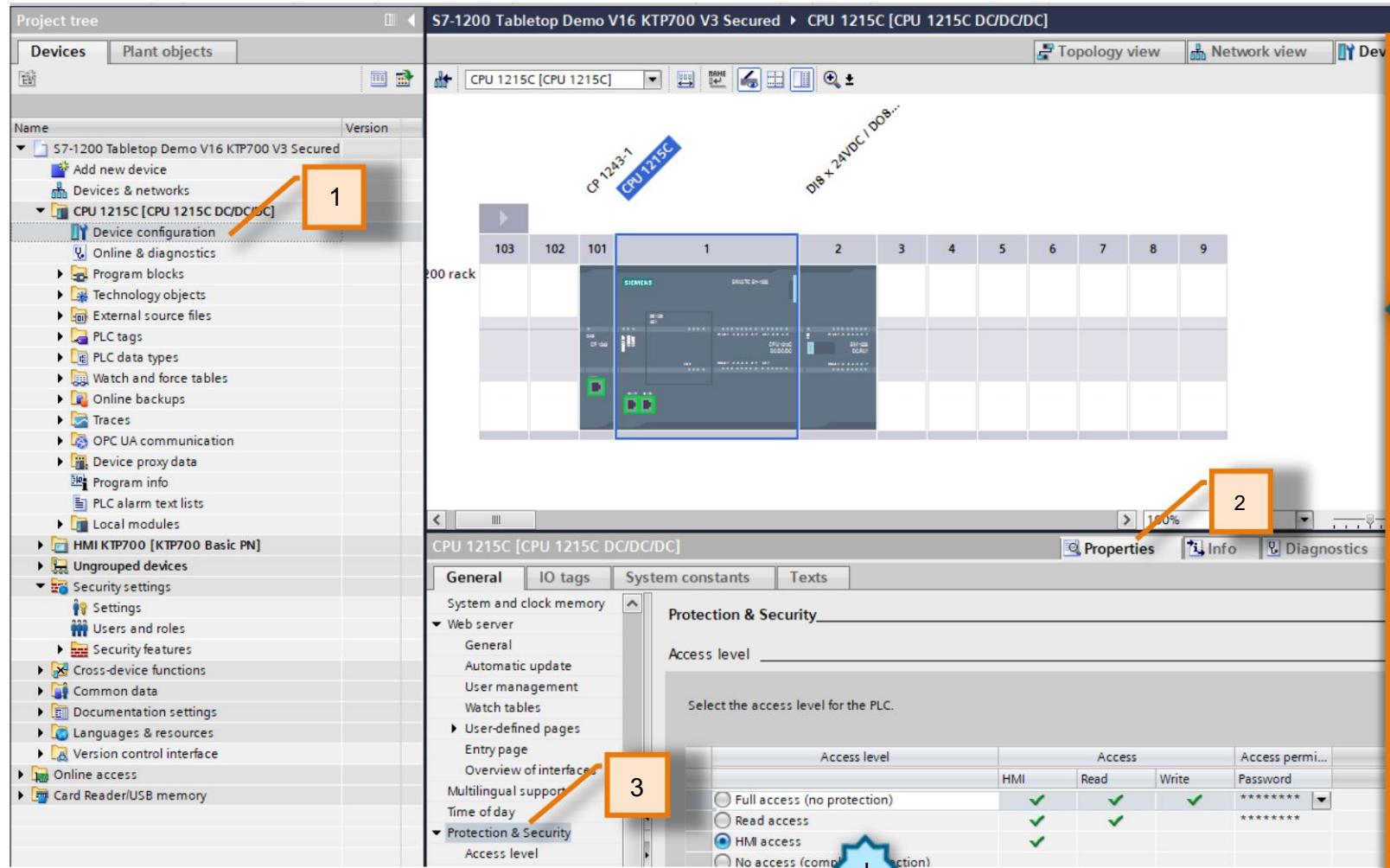
- La contraseña de la fila 1 (Acceso completo (sin protección)) permite el acceso como si la CPU estuviera completamente desprotegida. Los usuarios que conocen esta contraseña tienen acceso ilimitado a la CPU.
- La contraseña en la fila 2 (acceso de lectura) permite el acceso como si la CPU estuviera protegida contra escritura. Los usuarios que conocen esta contraseña tienen acceso de solo lectura a la CPU.
- La contraseña en la fila 3 (acceso HMI) permite el acceso como si la CPU fuera de escritura protegido y protegido contra lectura para que solo sea posible el acceso HMI para los usuarios que conocen esta contraseña.



Características de seguridad

Protección de acceso a la CPU

SIEMENS
Ingenuity for life



1. Haga doble clic en "Configuración de dispositivos" debajo de la CPU en el árbol del proyecto.
2. Seleccione la pestaña 'Propiedades' en la ventana del inspector
3. Vaya a 'Protección y seguridad'.

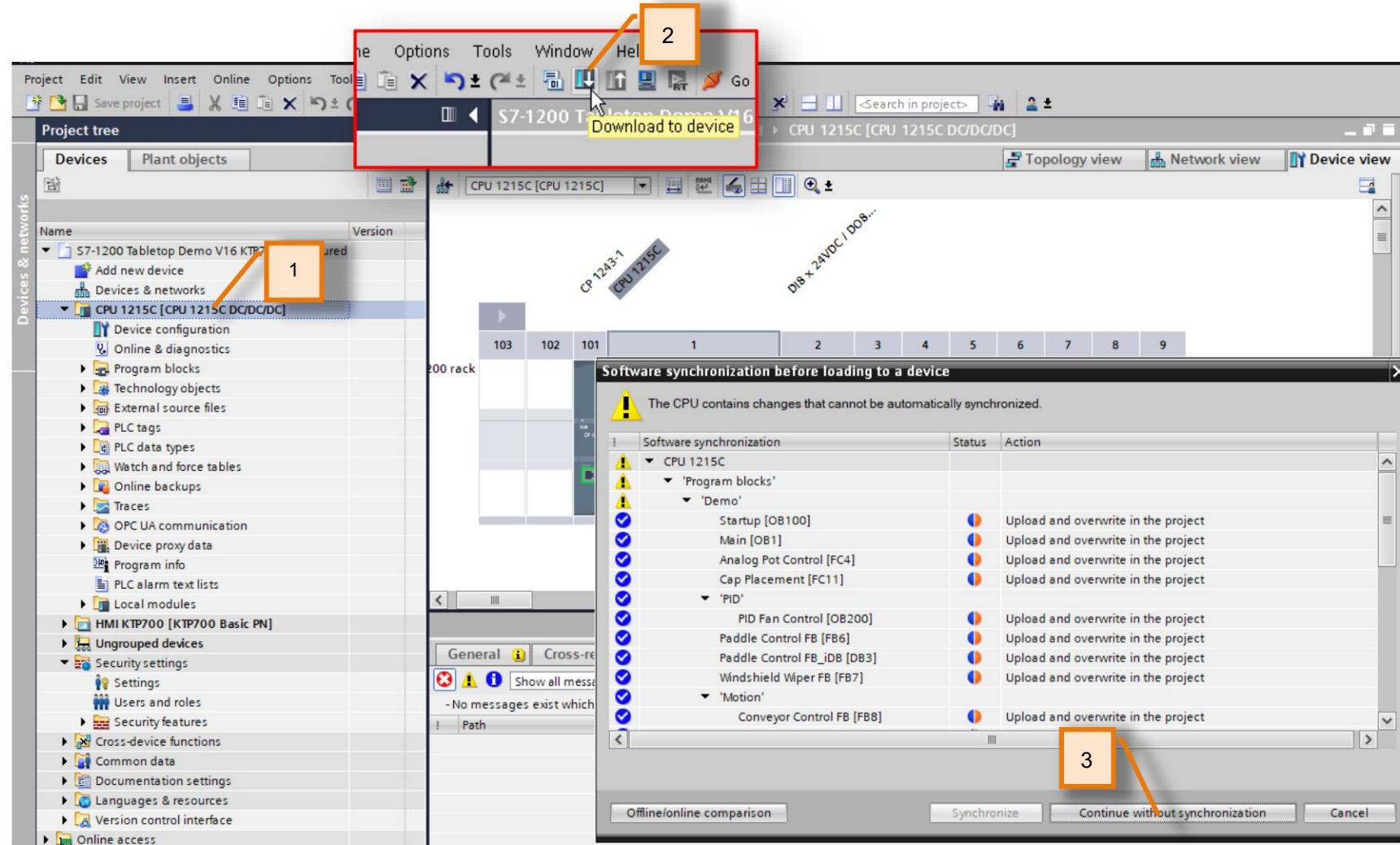
! Aviso: la CPU está configurada solo para el nivel "Acceso HMI". Con este nivel de acceso, solo es posible el acceso HMI y el acceso a los datos de diagnóstico sin ingresar una contraseña separada.

Sin ingresar la contraseña, no puede cargar bloques y configuración de hardware en la CPU, ni cargar bloques y configuración de hardware desde la CPU en el dispositivo de programación. Además, lo siguiente no es posible sin una contraseña: Escribir funciones de prueba, cambiar el estado operativo (RUN/STOP) y actualizaciones de firmware.

El acceso adicional a las funciones en línea, como la lectura/escritura de la lógica, requerirá la contraseña de nivel de acceso adecuada una vez que se descargue este proyecto.

Características de seguridad

Descargar proyecto de CPU segura



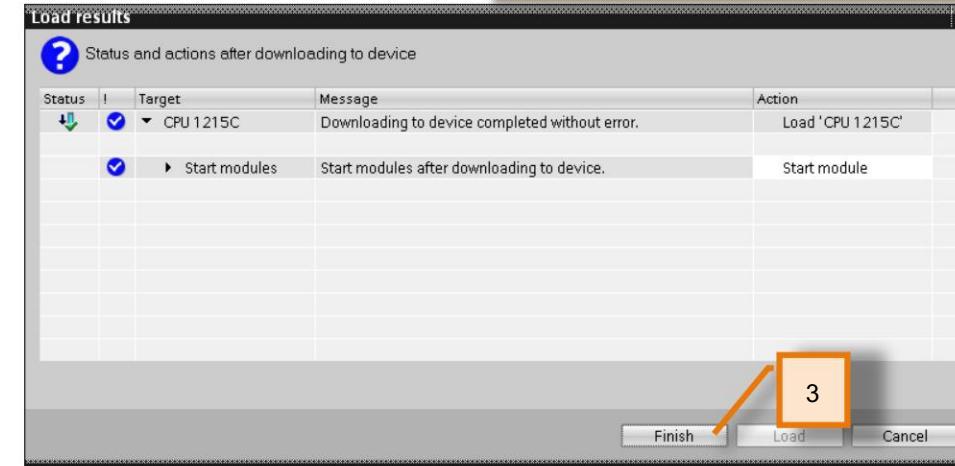
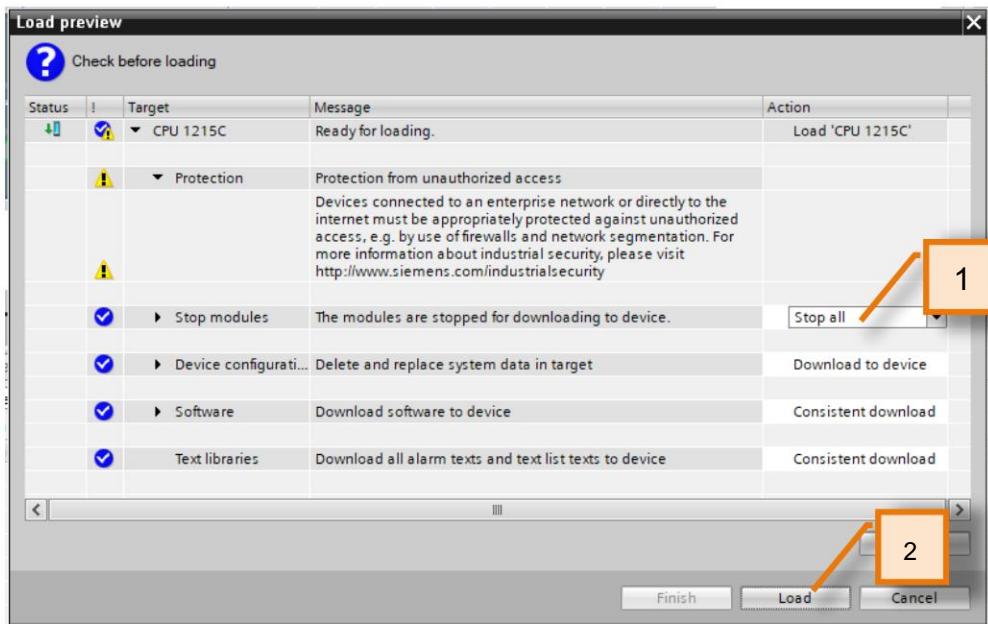
SIEMENS
Ingenuity for life

1. Seleccione la CPU1215C en el proyecto árbol. La descarga se basa en lo que tiene el foco en el proyecto.
 2. Seleccione el ícono Descargar en la barra de herramientas
 3. Dado que este proyecto está sobrescribiendo el proyecto en la CPU, puede aparecer el cuadro de diálogo de sincronización. Seleccione el botón "Continuar sin sincronización" y continúe
- Nota:
- Es posible que se le presente la ventana emergente "Descarga extendida al dispositivo". Si necesita ayuda, consulte el módulo "04 Funciones de diagnóstico y mantenimiento en línea" para obtener instrucciones paso a paso sobre cómo proceder.



Características de seguridad

Descargar proyecto de CPU segura



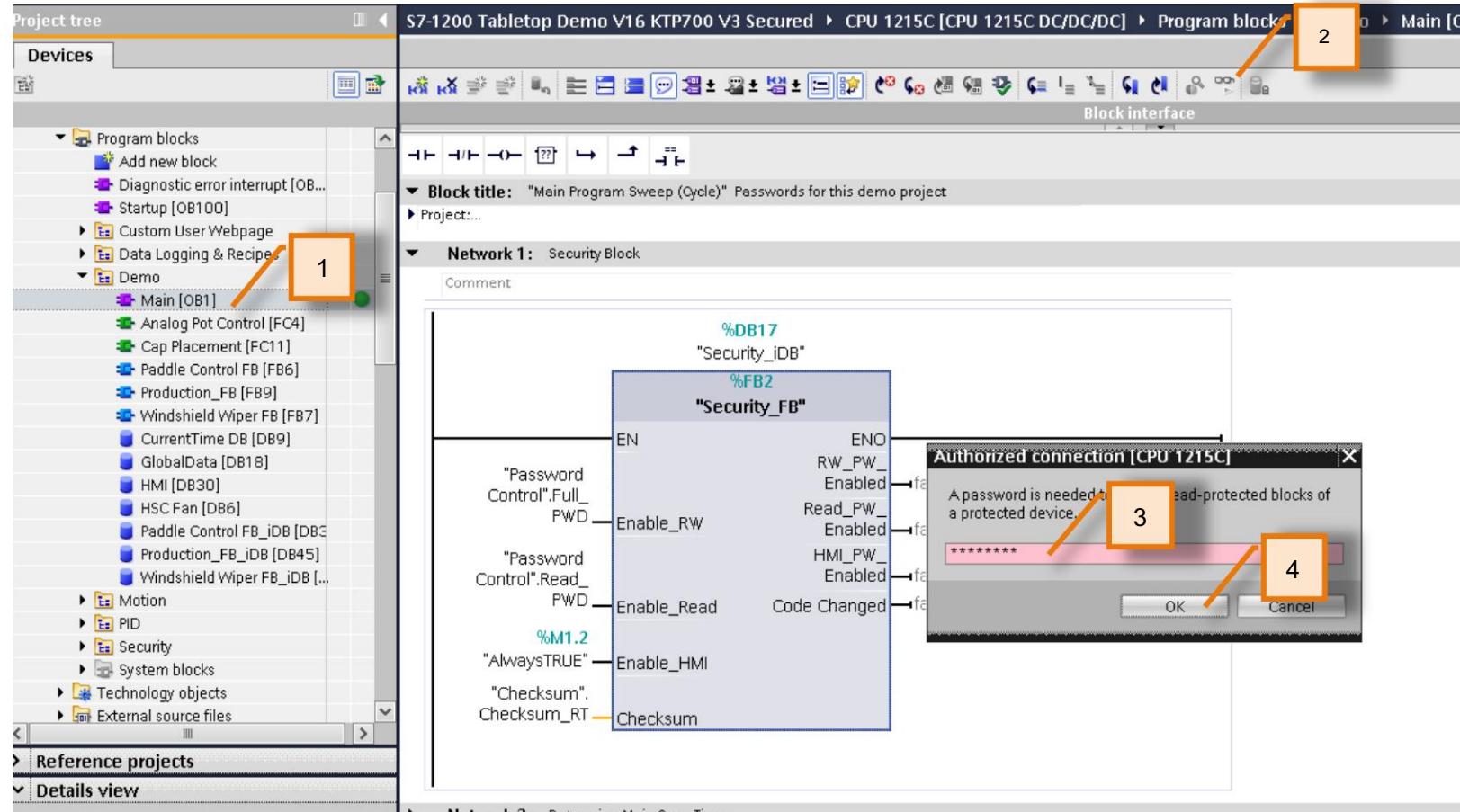
Nota: Dado que este proyecto tiene cambios en la configuración de hardware del PLC (niveles de acceso configurados), requerirá un STOP del PLC.

1. Seleccione "Detener todo" en el menú desplegable cuando se le solicite.
2. Seleccione el botón 'Cargar'. Esto cargará el proyecto con la nueva configuración de seguridad en la CPU.
3. Luego, el botón 'Finalizar' en la siguiente pantalla.



Características de seguridad

Niveles de acceso: solo lectura



SIEMENS
Ingenuity for life

1. Abra el bloque "Main {OB1}" en el árbol del proyecto en las carpetas Bloques de programa/Demo.
2. Seleccione el ícono Monitoreo activado/desactivado en la barra de herramientas de la ventana del editor.
3. Introduzca el acceso de lectura de la CPU contraseña: solo lectura
4. Haga clic en Aceptar

Darse cuenta:

Independientemente de ingresar la contraseña de nivel de acceso correcta, el sistema no le otorga acceso. Esto se debe a que hemos implementado una autenticación de usuario secundario con la instrucción ENDIS_PW antes de ingresar la contraseña de nivel de acceso correcta. Esta segunda autenticación podría ser un inicio de sesión de usuario único en la HMI, credencial de empleado, interruptor de llave, etc.

Esta característica evita que los usuarios no autorizados tengan acceso a ciertas funciones a pesar de tener la contraseña de nivel de acceso (por ejemplo, una "nota adhesiva" con la contraseña de "administrador").

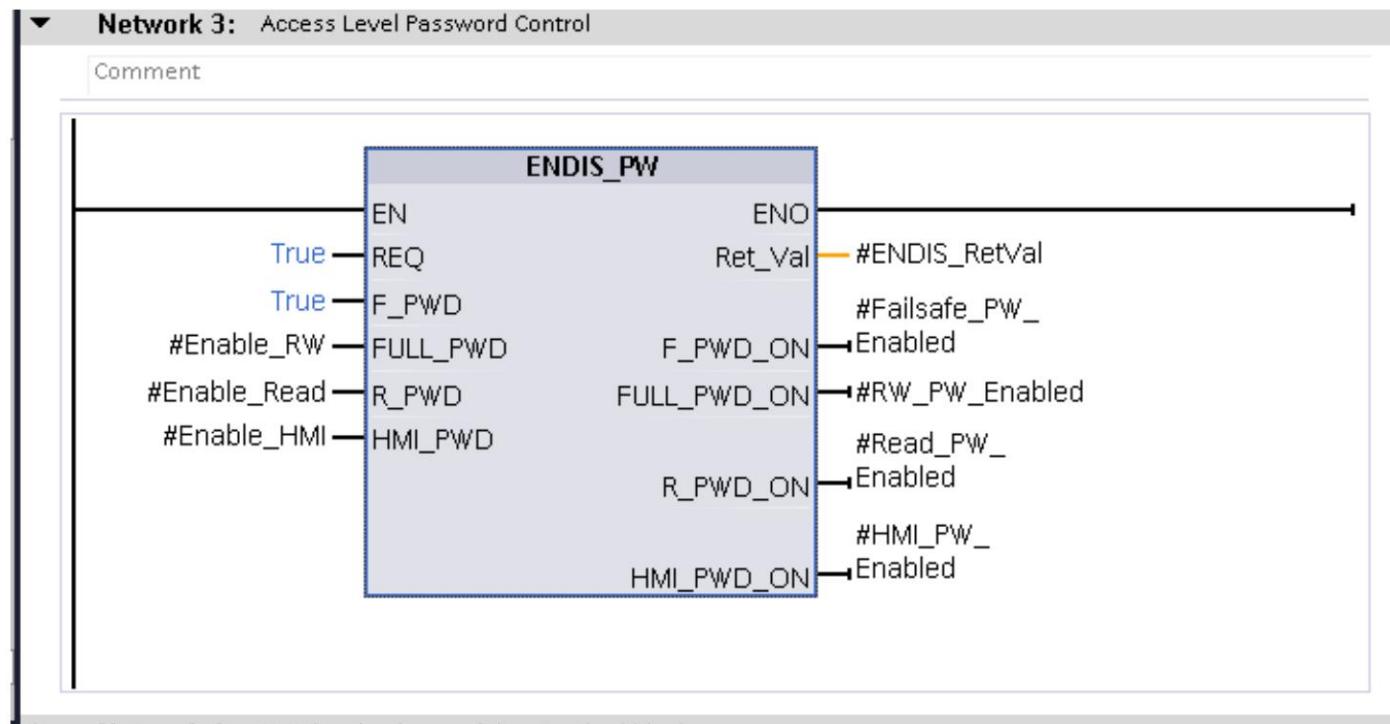




Autenticación de derechos de acceso multifactor

Características de seguridad

Autenticación secundaria con instrucción 'ENDIS_PW'



Puede usar la instrucción "ENDIS_PW" para especificar si la contraseña del nivel de acceso configurado puede habilitarse o no para la CPU. Por lo tanto, puede evitar conexiones legítimas incluso cuando se conoce la contraseña correcta.

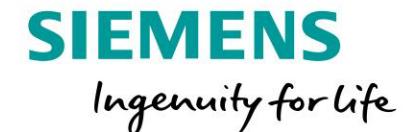
Dado que las entradas en cada nivel de acceso tienen la condición VERDADERA, usted habilita el acceso al PLC con la(s) contraseña(s) de nivel de acceso del PLC respectiva(s).

En este ejercicio, utilizaremos los inicios de sesión de usuario de HMI como autorización de acceso secundario, sin embargo, esto podría ser en forma de cualquier otro tipo de entrada (es decir, interruptor de llave, credencial de identificación, etc.)



Características de seguridad

Autenticación de 2 niveles



Ahora habilitaremos el nivel de acceso secundario para que podamos conectarnos en línea con nuestro proyecto utilizando el nivel de acceso de solo lectura.

1. En la HMI, vaya a la pantalla "Seguridad"



Aviso:

La pantalla muestra que solo se autoriza el nivel de acceso "HMI". Los niveles de acceso "Solo lectura" y "Lectura/escritura" aún no están autorizados porque el usuario correspondiente no ha iniciado sesión.

2. Presione los puntos suspensivos en el campo 'Operador' para abrir la pantalla de inicio de sesión del usuario.



Características de seguridad

Autenticación de 2 niveles



User Name
Werner

Password

LOGIN **CLOSE**

S7-1200: Compact Controller with Advanced Capabilities

State **Idle** Lot Number **10000** Operator **werner**

Program Setpoint Checksum
C9 6D 0D D4 05 02 24 AD

Program Running Checksum
C9 6D 0D D4 05 02 24 AD

Approved PLC Access Level **HMI Read Only** !

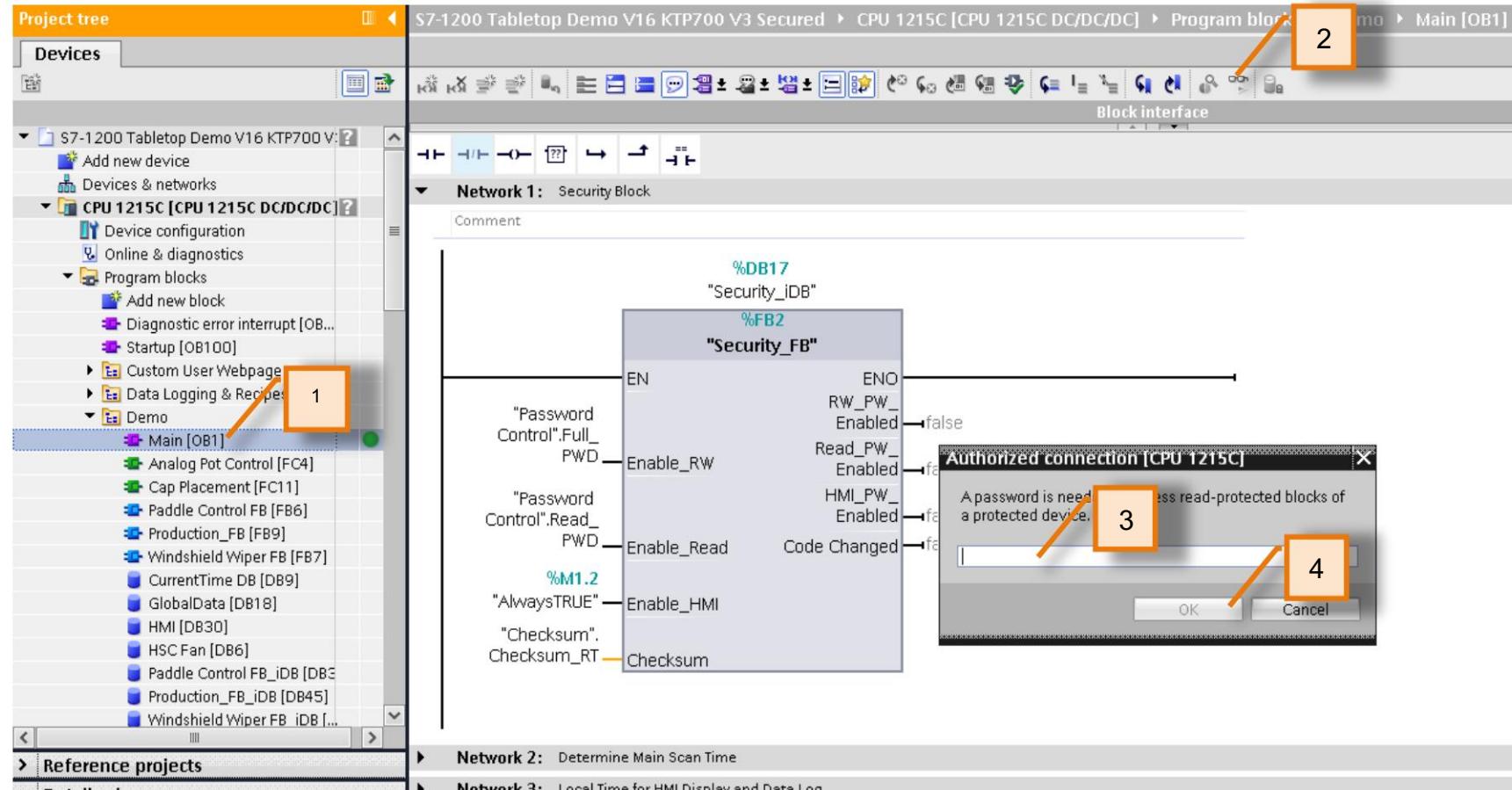
Demo PID Motion Wiper Security Recipe Web Server

1. Ingrese 'Werner' como nombre de usuario 2.
 - Ingrese 'Werner' como contraseña (¡La contraseña distingue entre mayúsculas y minúsculas!)
 3. Pulse 'INICIAR SESIÓN'
 4. Cierra la pantalla presionando 'CERRAR'
- Darse cuenta:
Ahora ha iniciado sesión con un usuario que tiene autorización de "Solo lectura".



Características de seguridad

Niveles de acceso: solo lectura



SIEMENS
Ingenuity for life

1. Abra el bloque "Main {OB1}" en el árbol del proyecto en las carpetas Bloques de programa/Demo.
2. Seleccione el ícono Monitoreo activado/desactivado en la barra de herramientas de la ventana del editor.
3. Introduzca el acceso de lectura de la CPU contraseña: solo lectura
4. Haga clic en Aceptar.

Ahora está monitorizando online el OB1 con derechos de acceso de "solo lectura" al control. Cualquier modificación en el proyecto es posible, pero requerirá autorización para el acceso de "lectura/escritura" antes de descargarlo a la CPU.

Paso opcional: Si cierra la sesión a través de la HMI, se cancelará automáticamente el acceso en línea en el TIA Portal, ya que se ha revocado el nivel de acceso "Solo lectura".

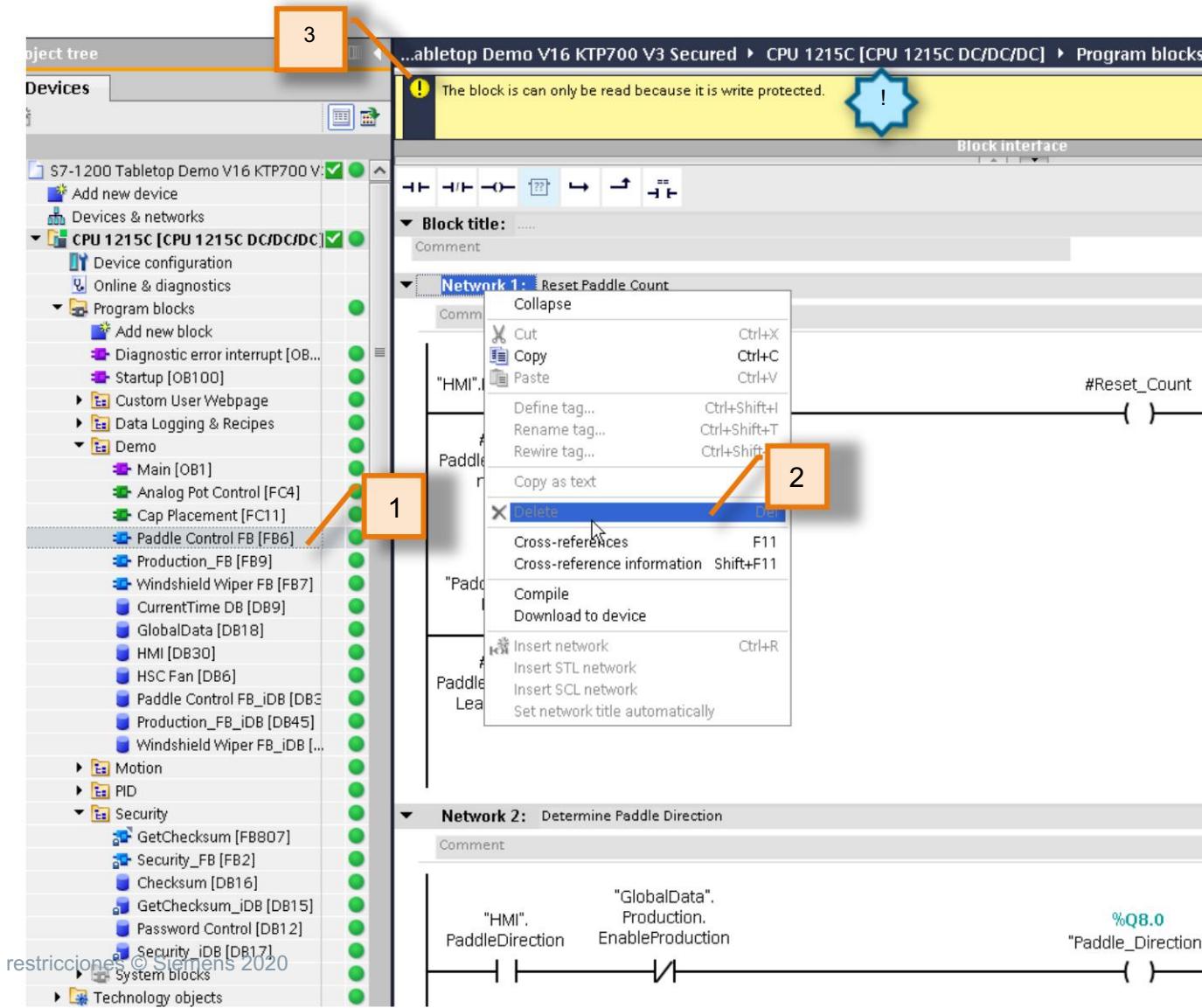




Protección de escritura

Características de seguridad

Bloques protegidos de solo lectura



SIEMENS
Ingenuity for life

1. Abra 'Paddle Control FB [FB6]'
 2. Intente eliminar la red 1; descubrirá que esto no está permitido. Asimismo , no se permite ninguna modificación en FB6 porque el bloque tiene habilitada la "protección contra escritura".
 3. Haga clic en el indicador en la parte superior de la interfaz del bloque. !
- ! Aviso: el mensaje en la parte superior de la interfaz del bloque indica que el bloque está protegido contra escritura). Una vez que se ha asignado un bloque como protegido contra escritura, es imposible editar este bloque y cualquier bloque subordinado (anidado) a menos que se elimine el atributo de protección contra escritura de las propiedades del bloque.

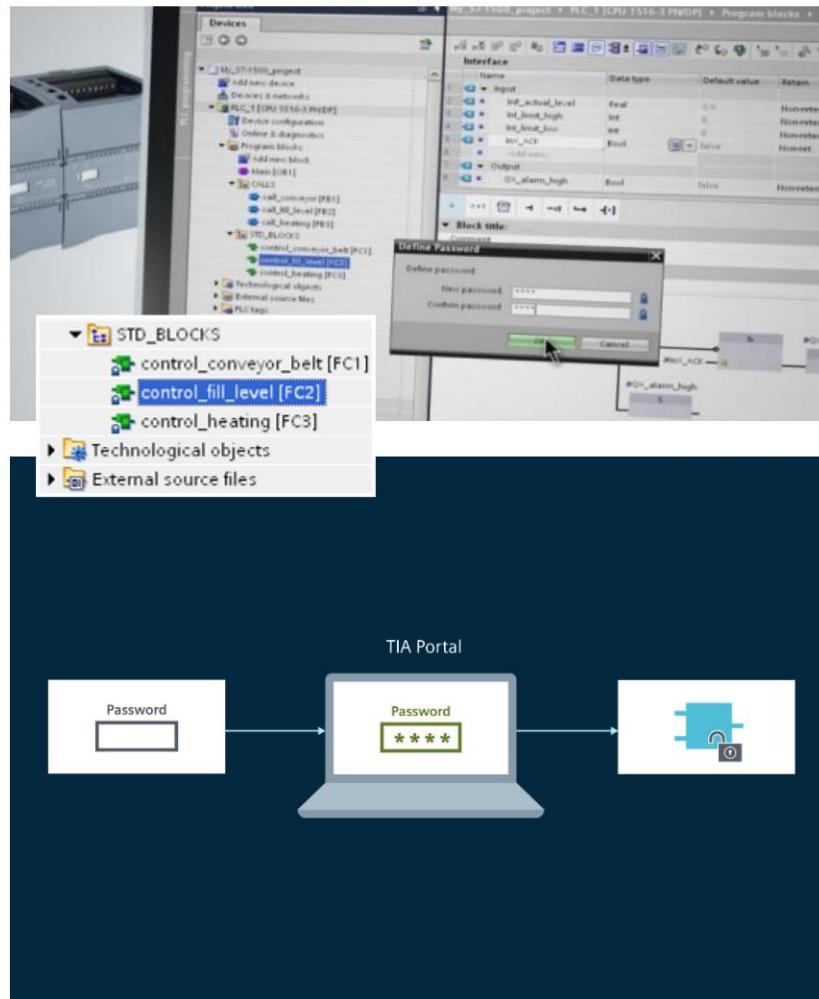




Protección del saber hacer

Características de seguridad

Protección del saber hacer



Aspectos destacados de la seguridad

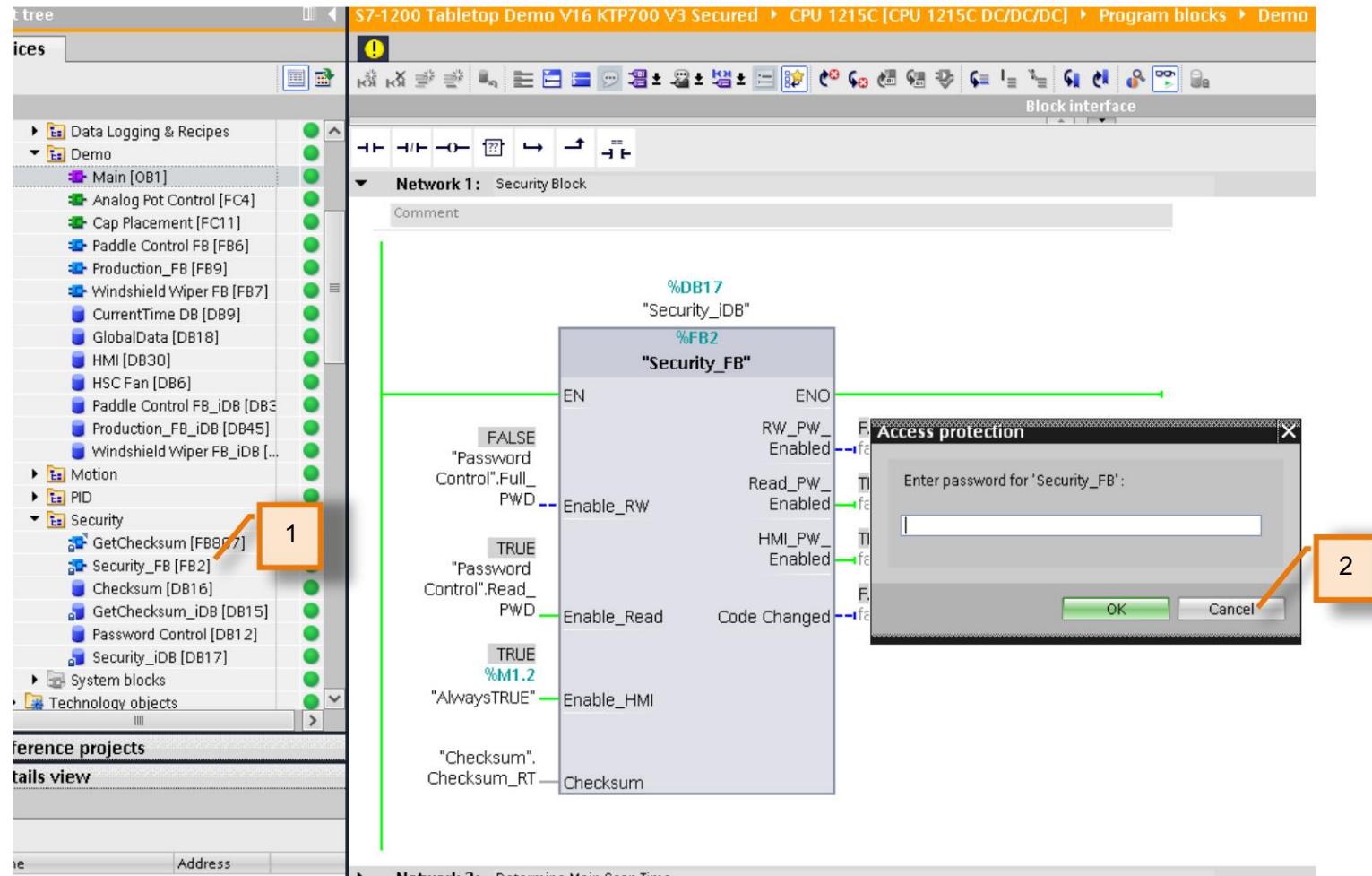
Para **SIMATICS7-1200**, **TIAPortal** ofrece varias funciones de seguridad para proteger su inversión contra lecturas y copias no autorizadas:

- Mayor protección de know-how para programas
 - Evita la lectura, la copia de contenido y los cambios inadvertidos de los bloques de programa
 - Protege los bloques de programa en el proyecto de ingeniería y en el controlador
 - Protección de bloques de programa en proyectos y bibliotecas



Características de seguridad

Protección del saber hacer



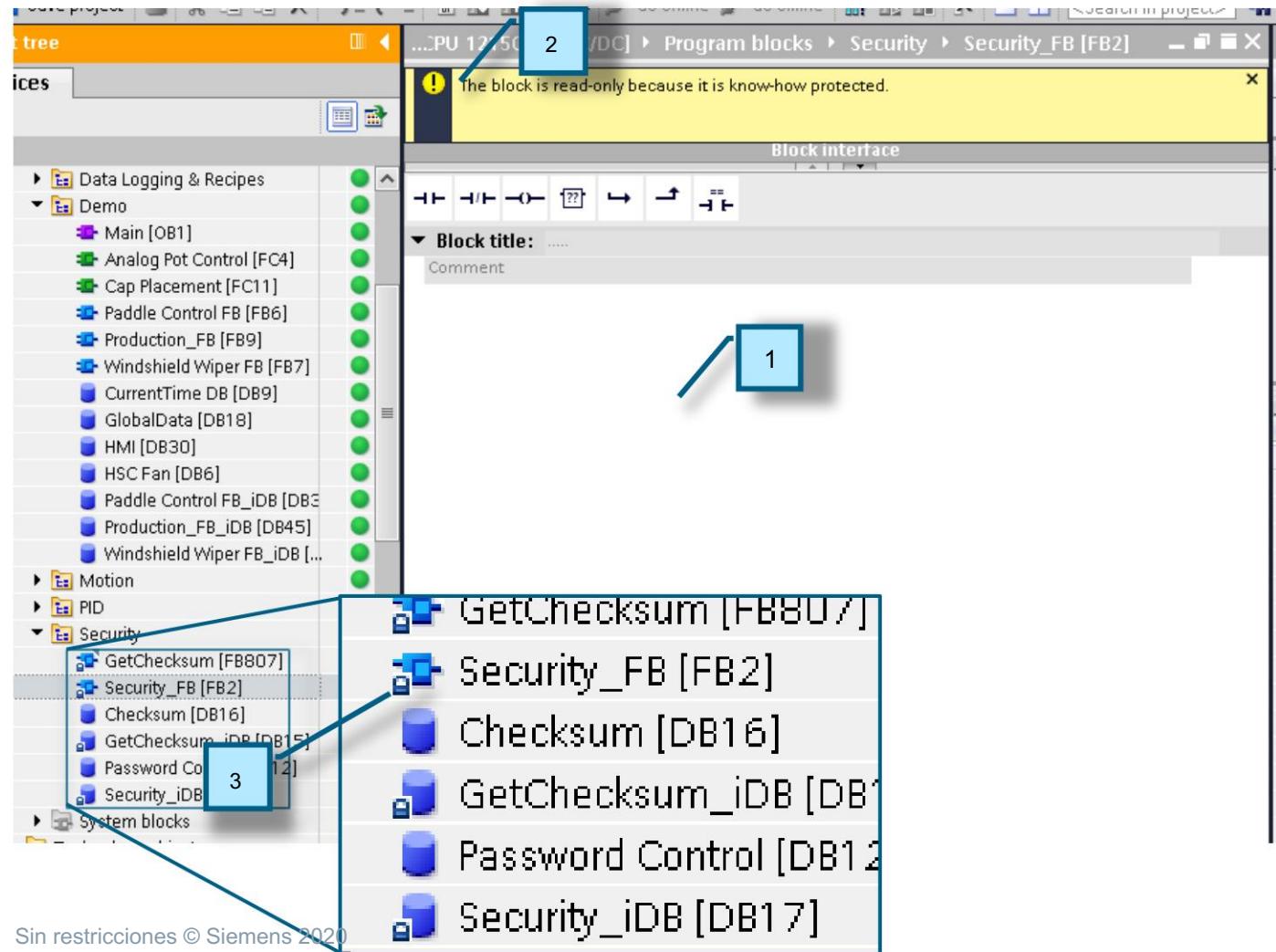
1. Haga doble clic en FB2 "Security_FB" del árbol del proyecto para abrir el bloque
Inmediatamente se le pedirá que ingrese una contraseña. Esta es la contraseña de Know-How.
2. Haga clic en Cancelar.



Características de seguridad

Protección del saber hacer

SIEMENS
Ingenuity for life

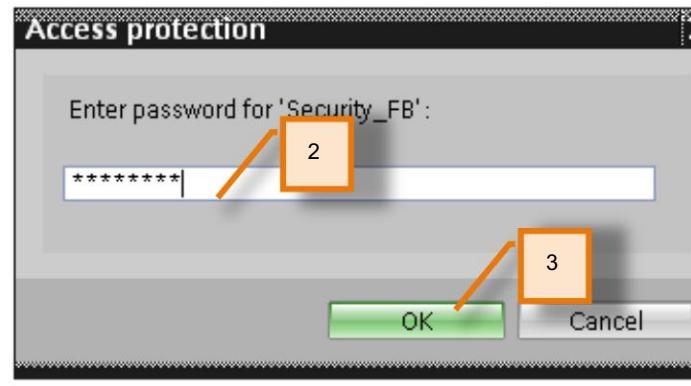
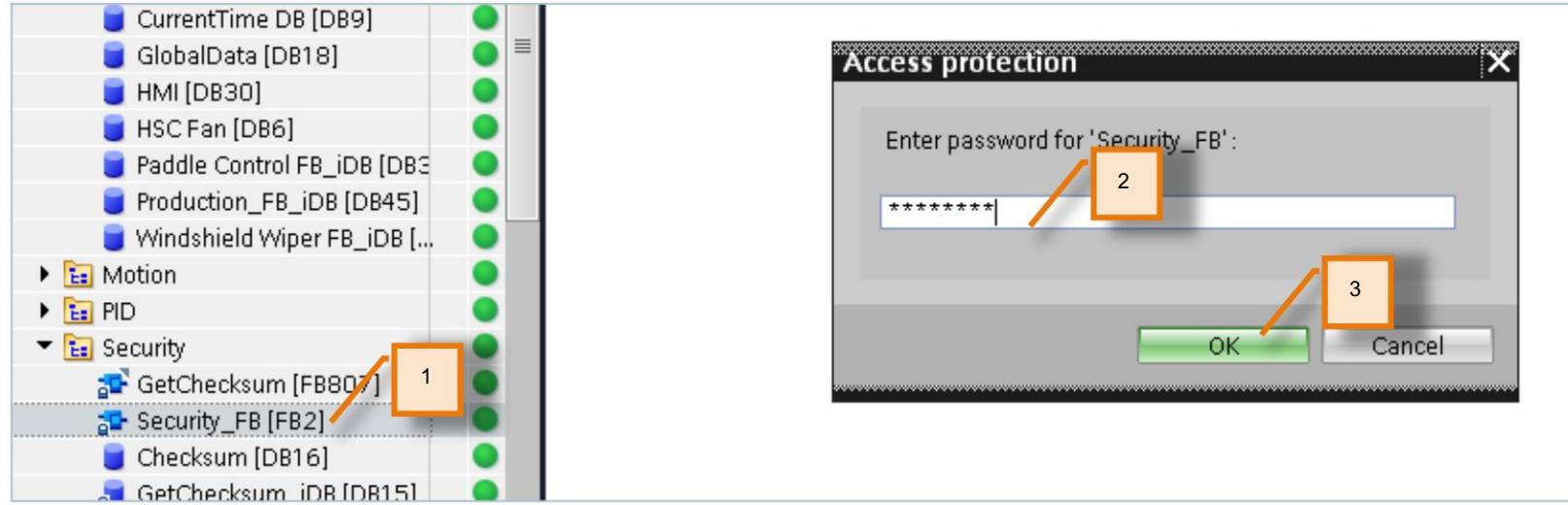


1. Observe que se abre el bloque, pero la lógica interna es oculto.
2. También hay un mensaje en la parte superior del bloque que indica que el bloque está protegido por know-how.
3. También observe que el bloque se muestra como conocimiento protegido mediante el símbolo de "candado" en el árbol del proyecto



Características de seguridad

Protección del saber hacer

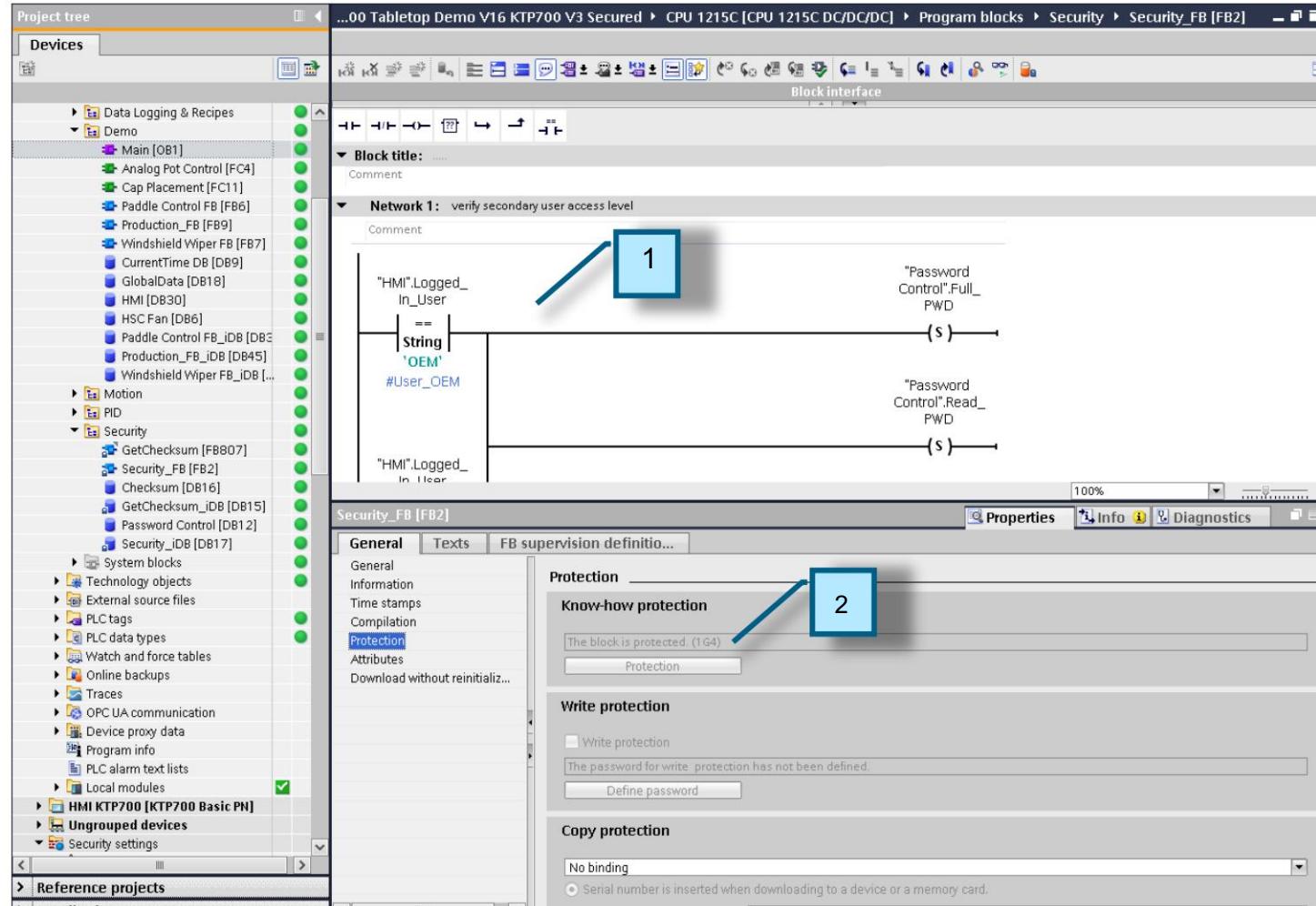


1. Vuelva a hacer doble clic en FB2 desde el árbol del proyecto para abrir la solicitud de inicio de sesión
2. Introduzca la siguiente contraseña de know-how: S3cur!ty
3. Haga clic en Aceptar



Características de seguridad

Protección de CPU



1. Ahora es posible ver y modificar el código.
2. Se selecciona la opción Protección de know-how

Nota: Para realizar cambios en el nivel de protección de un bloque, el editor debe estar cerrado y la CPU desconectada.



Características de seguridad

Edición de bloques protegidos de know-how



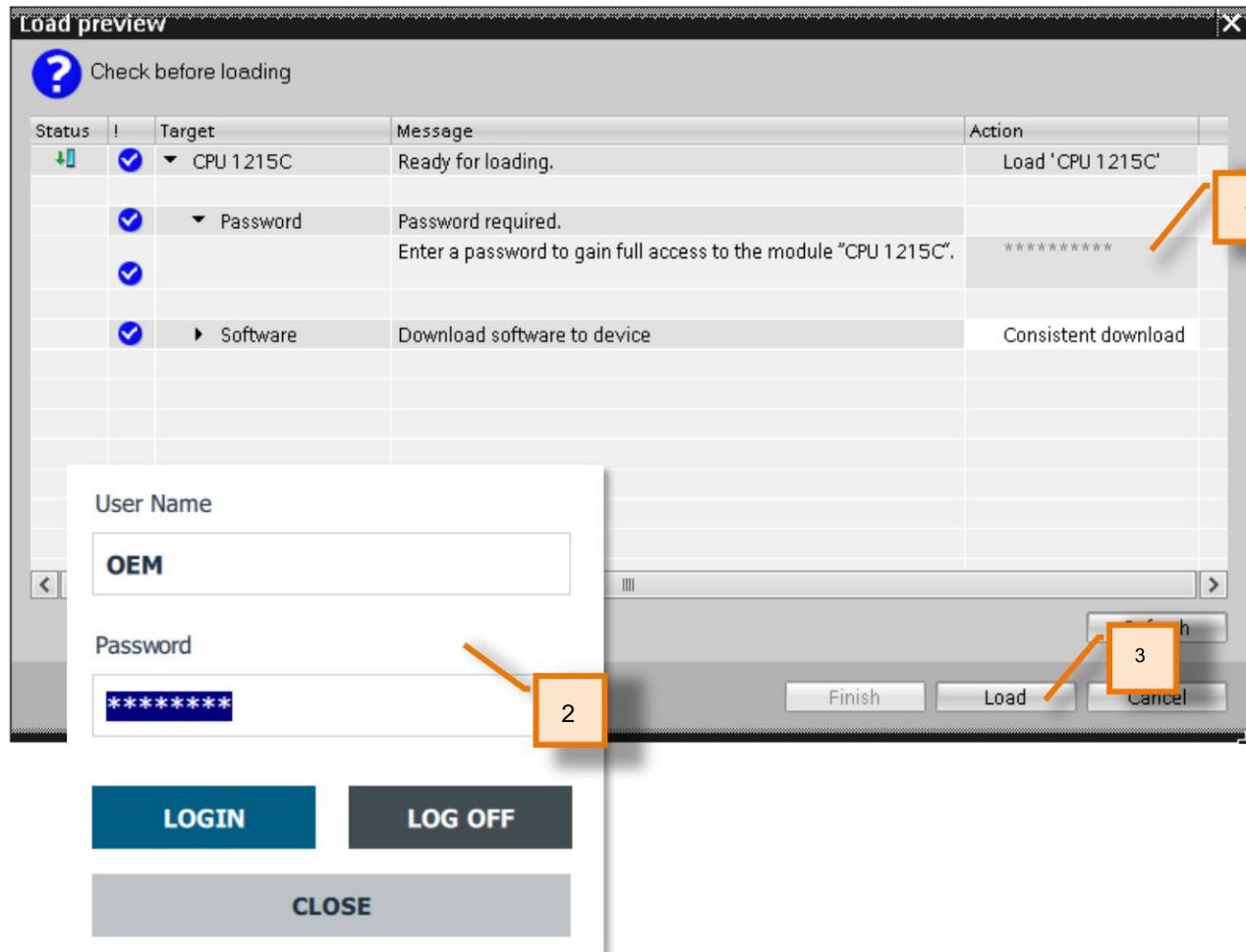
The screenshot shows the Siemens SIMATIC Manager software interface for ladder logic programming. The project tree on the left shows a hierarchy including 'S7-1200 Tabletop Demo V16 KTP700 V3 S:', 'CPU 1215C [CPU 1215C DC/DC/DC]', and 'Program blocks'. The 'Security' folder is selected, containing blocks like 'GetChecksum [FB807]', 'Security_FB [FB2]', 'Checksum [DB16]', 'GetChecksum_iDB [DB15]', 'Password Control [DB12]', and 'Security_iDB [DB17]'. The main workspace displays a ladder logic program titled 'Network 1: verify secondary user access level'. The logic consists of two parallel horizontal branches. The top branch starts with a coil labeled 'String "OEM"' followed by a comparison symbol '==', then a contact labeled '#User_OEM'. This is followed by a normally open contact (highlighted with a red circle and labeled '1') and a normally closed contact (labeled '2'). The output of this branch is connected to a coil labeled '(s)'. The bottom branch starts with a coil labeled 'String "Siemens"' followed by a comparison symbol '==', then a contact labeled 'HMI.Logged_In_User'. This is followed by a normally open contact and a normally closed contact. The output of this branch is also connected to a coil labeled '(s)'. To the right of the coils are comments: 'Password Control".Full_PWD' for the top branch and 'Password Control".Read_PWD' for the bottom branch.

1. Modifique el bloque agregando un contacto normalmente abierto con la variable "Siempre VERDADERO" %M1.2 como se muestra
2. Seleccione el icono de descarga en la barra de herramientas para descargar el cambio de programa a la CPU



Características de seguridad

Edición de Bloques Know How Protegidos



1. Dado que el acceso en línea que está habilitado actualmente es "Solo lectura", se debe obtener el nivel de acceso "Lectura/Escritura" para poder escribir en la CPU. Introduzca la contraseña de acceso completo (lectura/escritura): Siemens1!

2. Aviso: no puede ingresar el nivel de acceso contraseña para "Lectura/Escritura" hasta que un usuario con derechos de acceso "Lectura/Escritura" inicie sesión a través de la HMI.

2. En la HMI, inicie sesión con las siguientes credenciales de usuario :
Nombre de usuario: OEM

Contraseña: OEM (todas las mayúsculas)

[Consulte la página 21 para iniciar sesión a través de HMI]

3. Ahora vuelva a ingresar la contraseña de nivel de acceso del paso 1 anterior y presione Enter. Ahora debería poder hacer clic en el botón 'Cargar'. Continuar con la descarga.





Detección de manipulación

Características de seguridad

Detección de manipulación con sumas de control digitales



S7-1200: Compact Controller with Advanced Capabilities

State **Idle** Lot Number **10000** Operator **OEM**

Warning: an unauthorized change in running PLC code has been detected!

Program Setpoint Checksum
C9 6D 0D D4 05 02 24 AD

Program Running Checksum
97 34 BF 8F DB 3C 37 6E

Approved PLC Access Level
 HMI Read Only Read/Write

Demo PID Motion Wiper Security Recipe Web Server

Después de compilar y descargar el código modificado, la suma de verificación del programa ha cambiado. Por lo tanto, el operador recibe una alerta en la pantalla de una discrepancia entre la suma de verificación puesta en marcha inicialmente y la suma de verificación del nuevo programa.

Esta característica se puede usar para monitorear cambios no autorizados de programas o firmware. También es posible monitorear los cambios en las listas de texto para evitar el enmascaramiento de alarmas.





Niveles de acceso de usuario del servidor web

Características de seguridad

Use HMI para ver la página web de la CPU



Sin restricciones © Siemens 2020

SIEMENS
Ingenuity for life

1. Vaya a la pantalla del servidor web en la HMI para conectarse a la página web de la CPU
2. Haga clic en el botón ENTRAR

usa.siemens.com/s7-1200



Características de seguridad

Use HMI para ver la página web de la CPU



SIMATIC HMI

S7-1200: Compact Controller with Advanced Capabilities

State: Idle | Lot Number: 10003 | Operator: [empty]

SIEMENS

1

SIEMENS 1200 Station_1 / CPU 1215C

02:16:22

Username: _____ Login

Start Page | Introduction

Demo PID Motion Wiper Security Recipe Web Server

F1 F2 F3 F4 F5 F6 F7 F8

Sin restricciones © Siemens 2020

Observe que el servidor web muestra información limitada.

La CPU se ha configurado para restringir el acceso en el servidor web a menos que alguien inicie sesión.

1. Inicie sesión en el servidor web con las siguientes credenciales:

Nombre de usuario: Siemens1! (distingue mayúsculas y minúsculas!)

Contraseña: Siemens1! (distingue mayúsculas y minúsculas!)

Esto permite el acceso a todas las funciones de la página web.

Name	Access level	Password
Everybody	Minimum	*****
Siemens1!	Administrative	*****

usa.siemens.com/s7-1200



Resumen

Seguridad Integrada

Resumen de seguridad del S7-1200: funciones demostradas



Integridad del sistema

Protección de proyecto fuera de línea (UMAC)

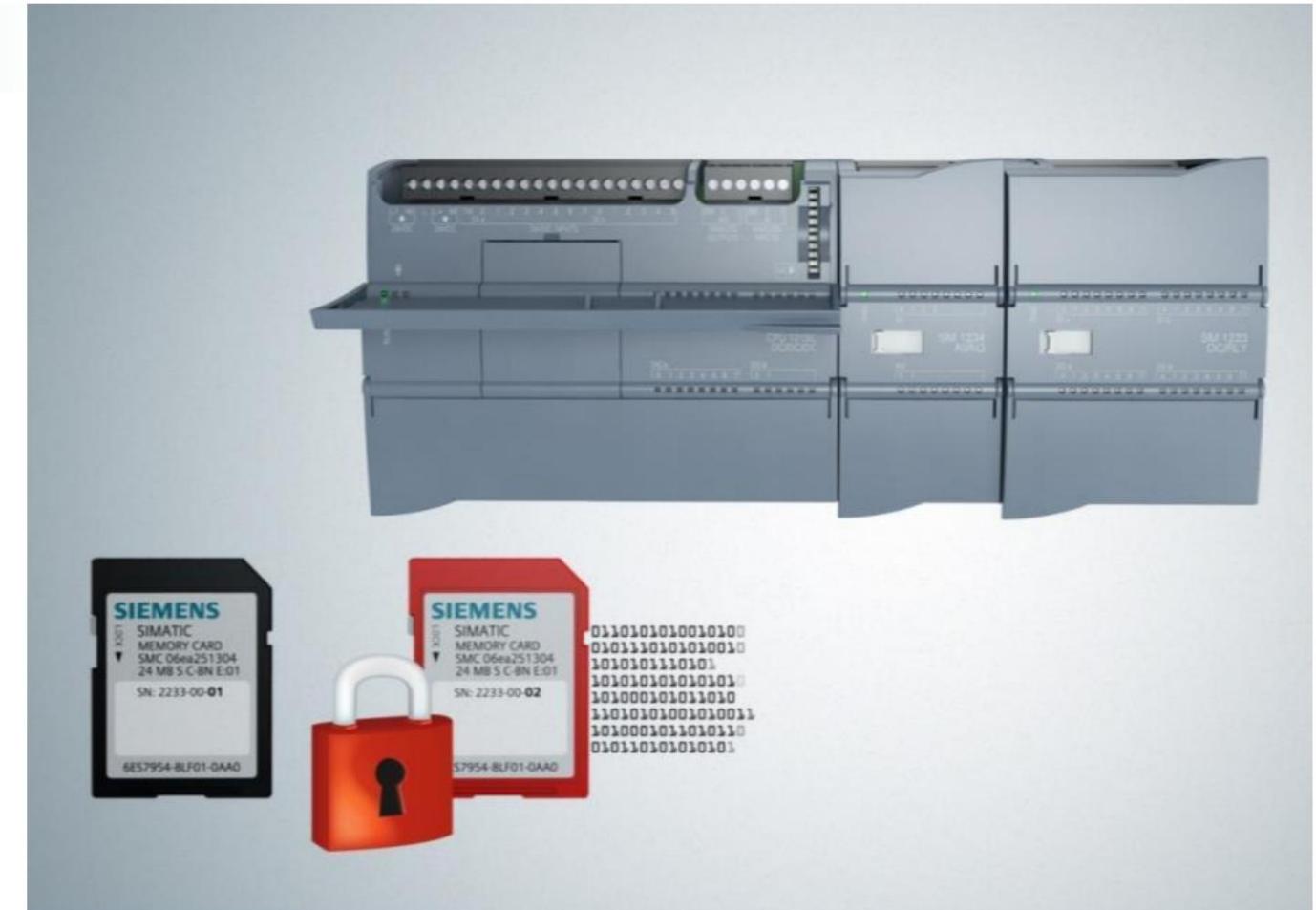
Protección de acceso

Autorización multifactor

Protección contra manipulación

Protección del saber hacer

Protección de acceso al servidor web



Fin de las 'Funciones de Seguridad Integradas'



LA INFORMACIÓN PROPORCIONADA EN ESTE DOCUMENTO SE PROPORCIONA COMO REFERENCIA GENERAL EN RELACIÓN CON EL USO DE PRODUCTOS APLICABLES EN APLICACIONES GENÉRICAS. ESTA INFORMACIÓN SE PROPORCIONA SIN GARANTÍA. ES SU RESPONSABILIDAD ASEGURARSE DE QUE ESTÁ UTILIZANDO TODOS LOS PRODUCTOS MENCIONADOS ADECUADAMENTE EN SU APLICACIÓN ESPECÍFICA. SI USTED UTILIZA LA INFORMACIÓN PROPORCIONADA AQUÍ EN SU APLICACIÓN ESPECÍFICA, COMPRUEBE DOBLEMENTE SU APLICABILIDAD Y TENGA EN CUENTA QUE ESTÁ UTILIZANDO ESTA INFORMACIÓN BAJO SU PROPIO RIESGO. EL COMPRADOR DEL PRODUCTO DEBE CONFIRMAR LA IDONEIDAD DEL PRODUCTO PARA EL USO PREVISTO Y ASUME TODOS LOS RIESGOS Y RESPONSABILIDADES RELACIONADOS CON EL USO.

ESTA GUÍA NO DEBE UTILIZARSE COMO SUSTITUTO O EN LUGAR DE UNA REVISIÓN INTEGRAL Y COMPRENSIÓN DE TODOS LOS MANUALES Y DIRECTRICES ESCRITOS DE INSTRUCCIONES Y FUNCIONAMIENTO.

EL CONTENIDO DE ESTA GUÍA NO FORMARÁ PARTE NI MODIFICARÁ NINGÚN ACUERDO, COMPROMISO O RELACIÓN ANTERIOR O EXISTENTE. EL CONTRATO DE VENTA CONTIENE TODA LA OBLIGACIÓN DE SIEMENS.

LA MODIFICACIÓN O DISTRIBUCIÓN DE ESTE CONTENIDO ESTÁ ESTRICULTAMENTE PROHIBIDA.

