



# S7-1200: Basic Controller with Advanced Functions

Integrated Security Functions

# Industrial Security

## Granted Certificates

**SIEMENS**  
*Ingenuity for life*



- TIA Ethernet based devices
- E.g. S7-1500, 1505S, S7-300, CP343-1 SCALANCE S, ...

- Protection against DoS attacks
- Defined behavior in case of attack
- Improved Availability

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

- Development process

- Certification of "Secure Product Development Lifecycle" for Division DF and PD based on IEC 62443-4-1

- S7- 1500 Controllers
- SCALANCE XM408-8C

- First security level certification (CSPN – Certification de Sécurité de Premier Niveau)

Find more information:

[http://ssi.gouv.fr/certification\\_cspn/simatic-s7-1518-4-version-du-micrologiciel-1-83/](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](http://www.ssi.gouv.fr/entreprise/certification_cspn/scalance-xm408-8c)



# Industrial Security

The Siemens solution for system integrity

Defense in depth

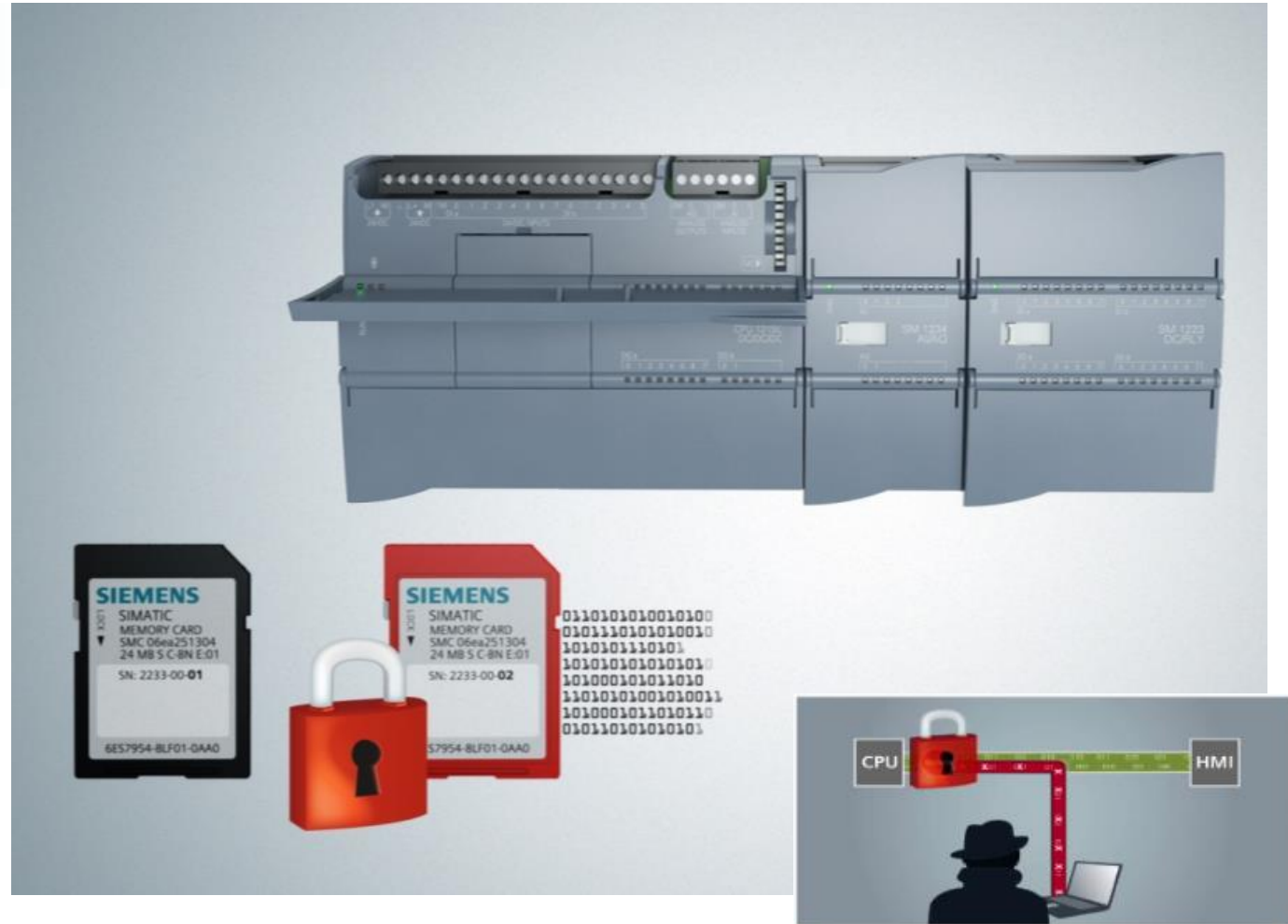


# Security Integrated

## S7-1200 Security Features Overview

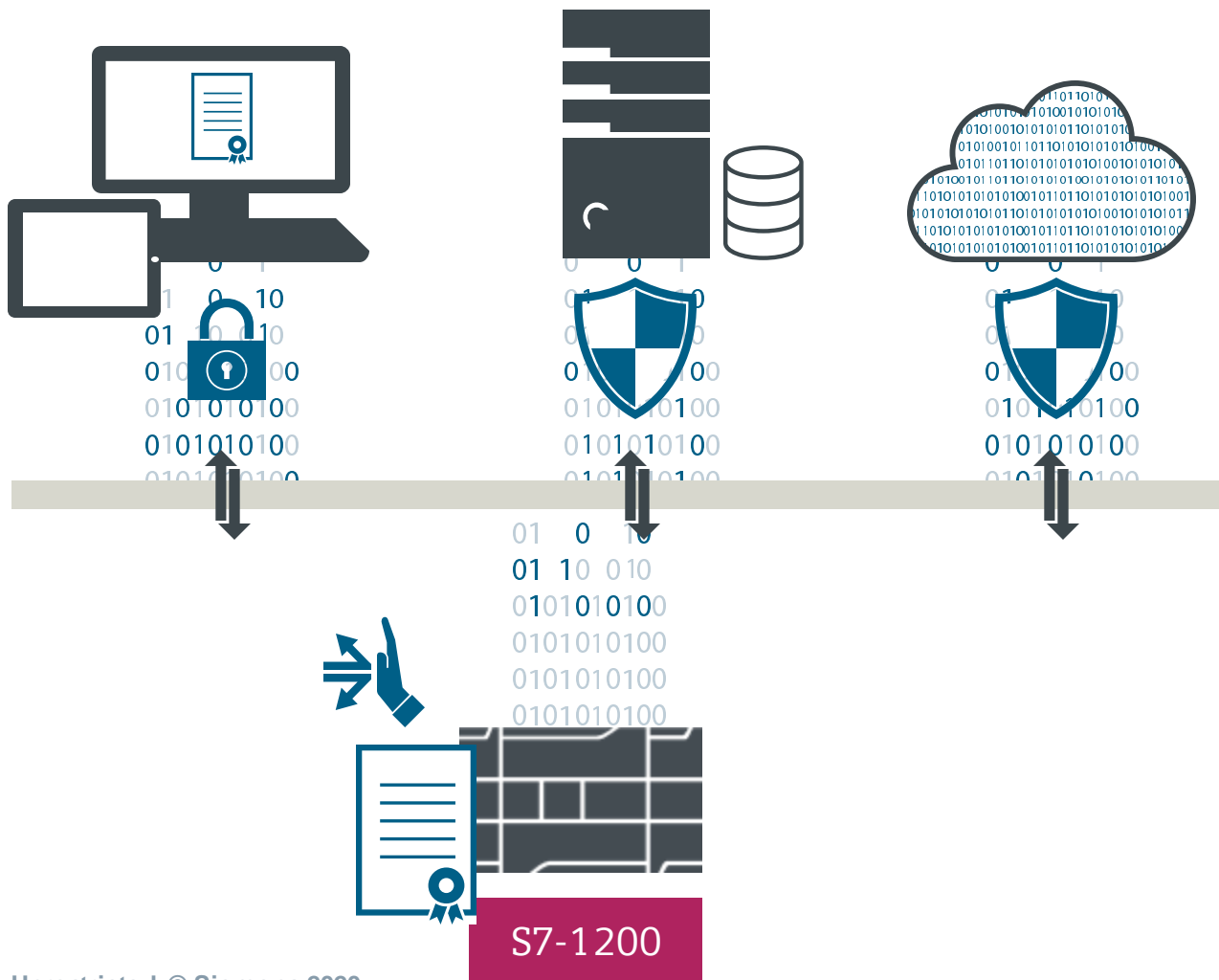
### System Integrity

- Protection of offline project (UMAC)
- Access Protection
- Multifactor authorization
- Manipulation Protection
- Know-How Protection
- Web Server Access Protection
- Certificate authentication
- Secure communications  
(OPC UA, HTTPS, FTPS, TLS...)



# OPC UA

## Integrated security mechanisms



### OPC UA Security



Selectable security policies  
in Controller and Clients



Device/application authentication  
based on certificates



Integrity protection  
and encrypted communication



User authentication and restricted  
access to PLC tags



# Security Passwords for Demo



## Access Level Passwords:

Full Access (Read/Write): **Siemens1!**  
Read Access (Read Only): **ReadOnly**  
HMI Access: <none>

## HMI User Login

<u>User Name</u>	<u>Password</u>	<u>Access Rights</u>
OEM	<b>OEM</b>	Administration (read/write)
Werner	<b>Werner</b>	Operator (read only)
<none>	<none>	Operate HMI only

## Offline Project (UMAC) Password:

User: **Siemens1!**  
Password: **Siemens1!**

## Know-how protection Password (FB2):

Password: **S3cur!ty**

## Write Protection Password (FB6):

Password: **FB6\_write**

## Web Server User & Password:

User: **Siemens1!**  
Password: **Siemens1!**



# User Management and Access Control (UMAC)

# User Management and Access Control UMAC in TIA Portal

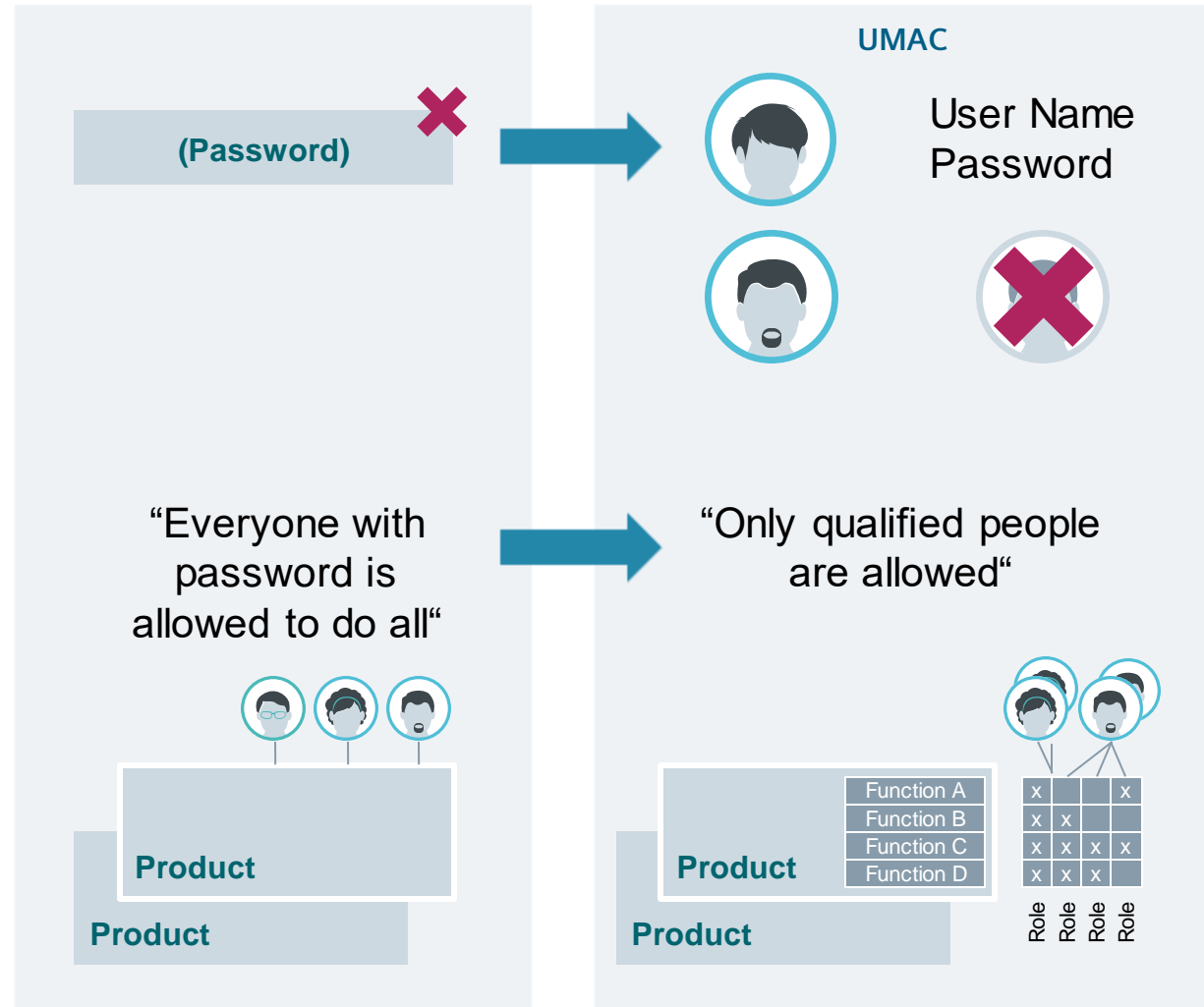
## What is it aiming for?

### Security: Protection of industrial machines/plants

- Personalized Access instead of Password Access
- Unauthorized Access is prevented

### Efficiency: Centralized management

- Of Users in a project or even for multiple projects
- Of Roles summarizing Function Rights of products
- Assignment of Users/Groups to Role/s
- Substitutes product-local solutions





# Security Features

## UMAC - Opening a secured project

Siemens Totally Integrated Automation PORTAL

Open existing project

Recently used

Project	Path	Last change
S7-1200 Tabletop Demo V16 KTP700 V3.ap16	C:\Users\Siemens\Documents\Automation\S7-1200 Tabletop Demo V16 KTP700 V3	6/27/2020 6:43:22 PM
S7-1200 Tabletop Demo V16 KTP700 V3 Secured.ap16	C:\Users\Siemens\Documents\Automation\S7-1200 Tabletop Demo V16 KTP700 V3 Secured	6/27/2020 6:38:18 PM

1

2

Open

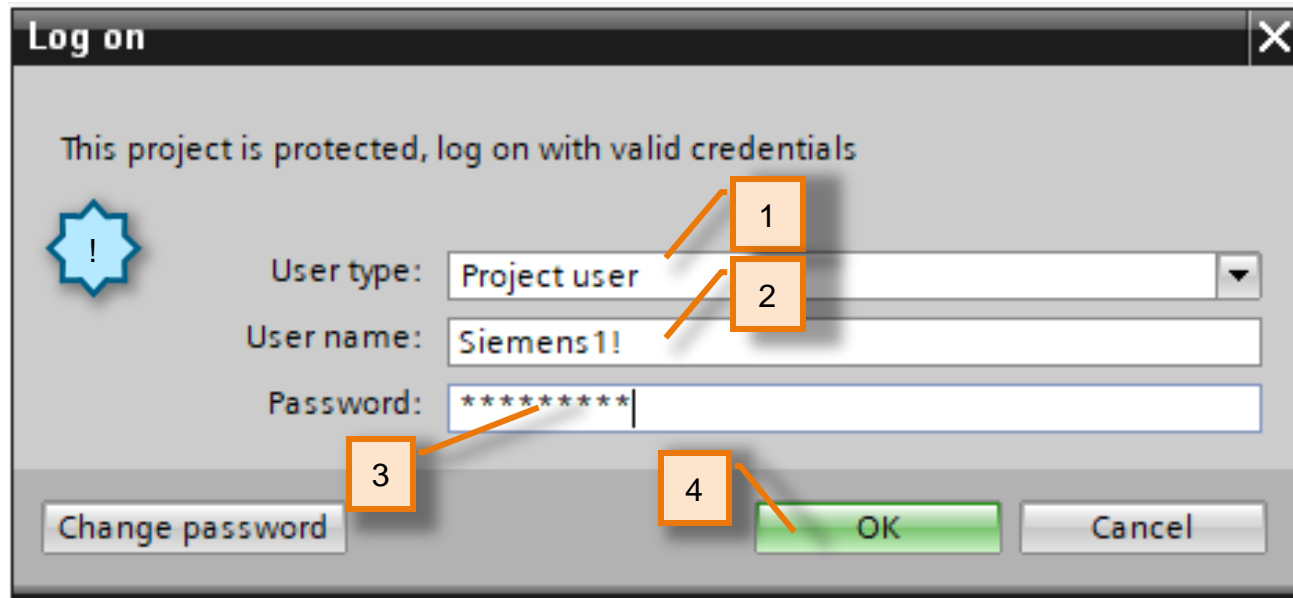
Project view

1. Open the project called 'S7-1200 Tabletop Demo KTP700 V3 **Secured.ap16**' by double clicking on it on the "recent projects" list.  
  
If the project does not appear in the list, press Browse and navigate to the "Desktop\S7-1200 Event\S7-1200 Tabletop Demo V16 KTP700 V3 **Secured.ap16**"
2. Click the "Open" Button.



# Security Features

## UMAC - Entering User Password



The screenshot shows a 'Log on' dialog box with the following elements:

- 1**: A blue starburst icon with an exclamation mark on the left side of the dialog.
- 2**: A dropdown menu for 'User type' with 'Project user' selected.
- 3**: A text input field for 'User name' containing 'Siemens1!'.
- 4**: A text input field for 'Password' containing '\*\*\*\*\*'.
- 5**: A 'Change password' button on the bottom left.
- 6**: A green 'OK' button in the center.
- 7**: A grey 'Cancel' button on the bottom right.



Notice upon opening the project, you are prompted to enter a user/password information. This project is password protected for different users. Each user can have different features enabled.

1. Select User type "Project user" from the dropdown menu
2. Enter the User name: Siemens1!
3. Enter the password: Siemens1!
4. Click OK.
5. Go to the Project view and **Save the project under a different name/directory.**



# Security Features

## UMAC - Users and Rules

1. Go to the Security settings in the project tree and double-click 'Users and roles'.

2. Notice There are two users for this project:

- 'Siemens1!' Has full Administrator rights
- 'User2' is limited to a Read Only role.

A user with 'Engineering Administrator' role can create new users, new Roles, and assign Roles to the different users.

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 Administr...
<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 "NET Standard"
<input type="checkbox"/>	NET Diagnose	System-defined role "NET Diagnose"
<input type="checkbox"/>	NET Remote Access	System-defined role "NET Remote ..."
<input type="checkbox"/>	NET Administrator Radius	System-defined role "NET Administr..."
<input type="checkbox"/>	NET Radius	System-defined role "NET Radius"
<input type="checkbox"/>	Read Only	User-defined role
<input checked="" type="checkbox"/>	Admin	User-defined role

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 Administr..."
<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 "NET Standard"
<input type="checkbox"/>	NET Diagnose	System-defined role "NET Diagnose"
<input type="checkbox"/>	NET Remote Access	System-defined role "NET Remote ..."
<input type="checkbox"/>	NET Administrator Radius	System-defined role "NET Administr..."
<input type="checkbox"/>	NET Radius	System-defined role "NET Radius"
<input checked="" type="checkbox"/>	Read Only	User-defined role
<input type="checkbox"/>	Admin	User-defined role



# CPU Access Level Protection

# Security Features

## CPU Access Protection

Access level \_\_\_\_\_

Select the access level for the PLC.

Access level	Access			Access permi...
	HMI	Read	Write	Password
<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.

The following slide describes how to configure an access level and enter passwords for an S7-1200 CPU as of V4.

For an S7-1200 CPU, you can enter multiple passwords and thereby set up different access rights for individual user groups.

The passwords are entered in a table in such a way that exactly one access level is assigned to each password.

The effect of the password is given in the "Access level" column.

- The password in row 1 (**Full access (no protection)**) allows access as if the CPU were completely unprotected. Users who know this password have unrestricted access to the CPU.
- The password in row 2 (**read access**) allows access as if the CPU were write-protected. Users who know this password have read-only access to the CPU.
- The password in row 3 (**HMI access**) allows access as if the CPU were write-protected and read-protected so that only HMI access is possible for users who know this password.



# Security Features

## CPU Access Protection

The screenshot displays the SIMATIC Manager interface. On the left, the Project tree shows the hierarchy: S7-1200 Tabletop Demo V16 KTP700 V3 Secured > CPU 1215C [CPU 1215C DC/DC/DC] > Device configuration (1). The main workspace shows a rack diagram with the CPU 1215C highlighted (2). The Properties window is open to the 'Protection & Security' tab, showing the 'Access level' section with 'HMI access' selected (3).

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

1. Double-click "Device configuration" under the CPU in the project tree.
2. Select the 'Properties' tab in the inspector window
3. Go to 'Protection & Security'.

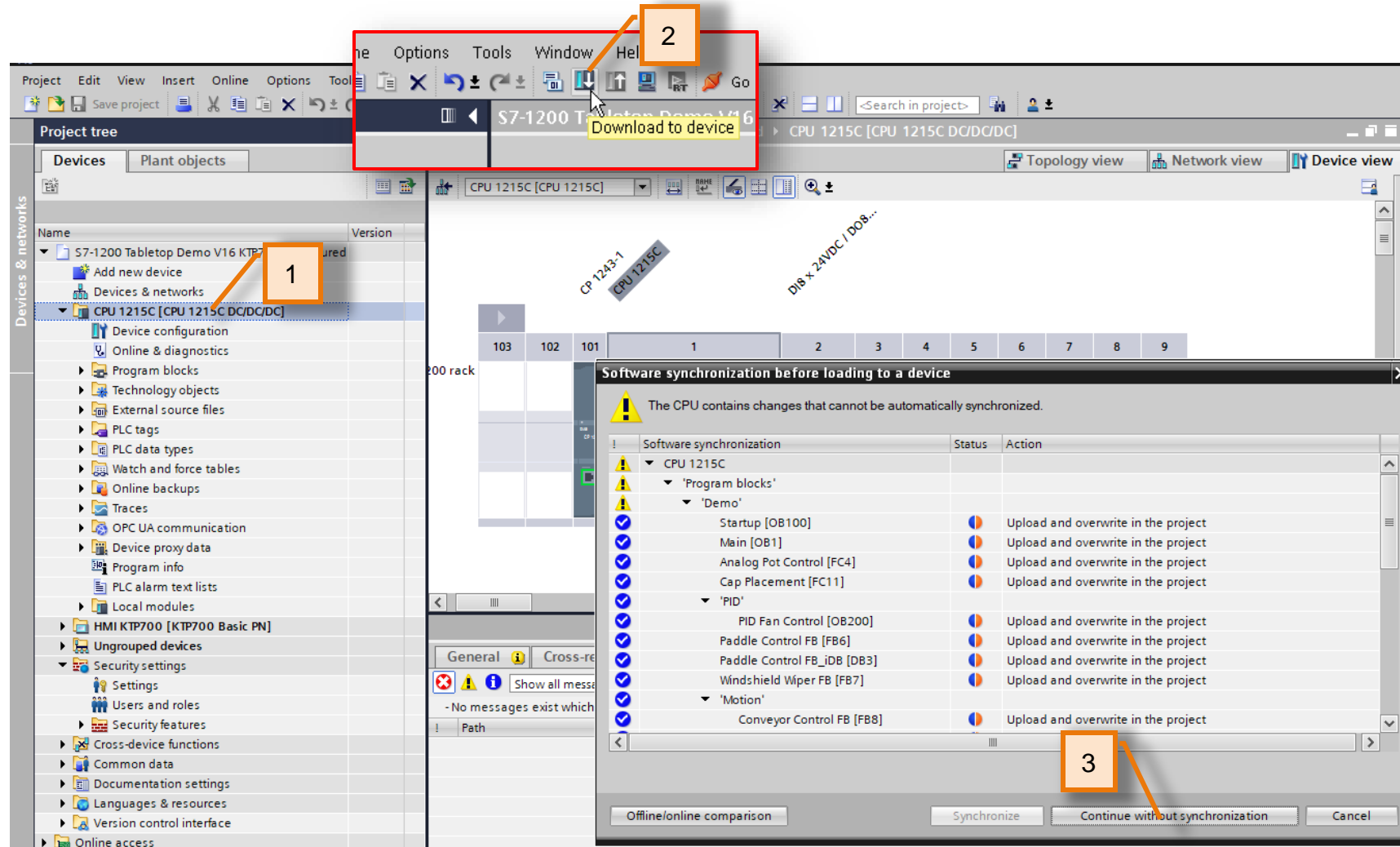
! Notice: The CPU is configured for "HMI access" level only. With this access level, only HMI access and access to diagnostics data is possible without entering a separate password.

Without entering the password, you can neither load blocks and hardware configuration into the CPU, nor load blocks and hardware configuration from the CPU into the programming device. In addition, the following is not possible without a password: Writing test functions, changing the operating state (RUN/STOP) and firmware updates.

Additional access to online features such as read/write of the logic will require the appropriate access level password once this project is downloaded.

# Security Features

## Download Secured CPU Project



1. Select the CPU1215C in the project tree. The download is based on what has focus in the project.
2. Select the Download icon on the toolbar
3. Since this project is overwriting the project in the CPU, the synchronization dialog may appear. Select the "Continue without synchronization" button and continue

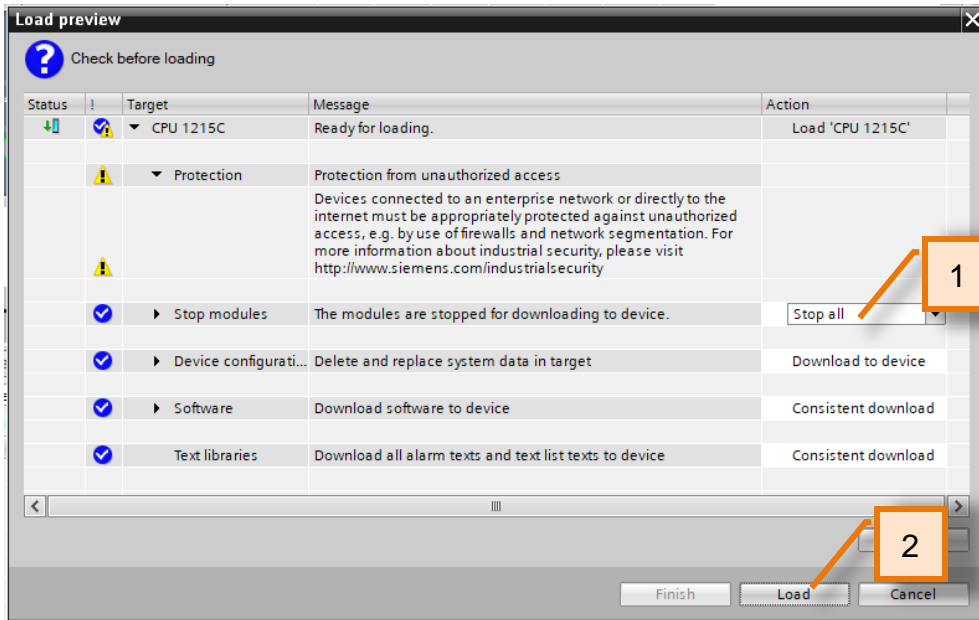
### Note:

You may be presented with the "Extended download to device" popup. If you need assistance, please review the module "04 Online Maintenance & Diagnostic Functions" for step-by-step instructions on proceeding.



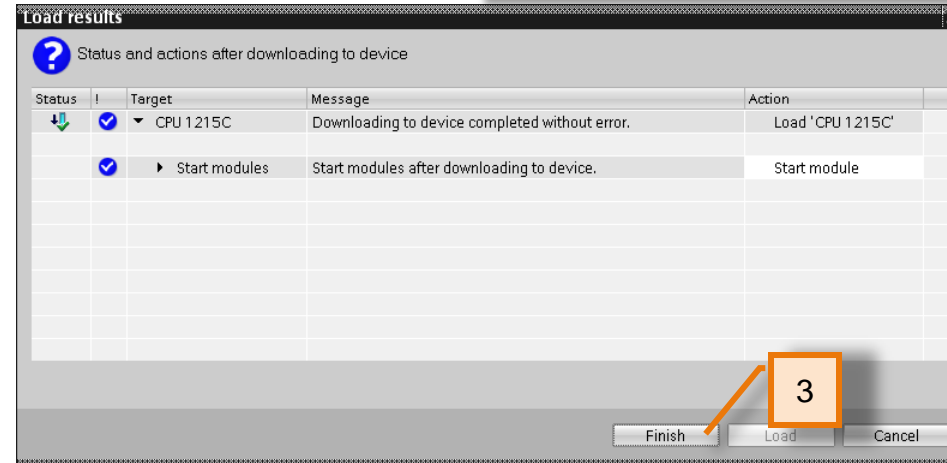
# Security Features

## Download Secured CPU Project



Note: Since this project has changes to the **hardware configuration** of the PLC (access levels configured), it will require a STOP of the PLC.

1. Select "Stop all" from the dropdown menu when prompted.
2. Select the 'Load' button. This will load the project with the new security settings into the CPU.
3. Then the 'Finish' button on the next screen.





# Security Features

## Access Levels – Read Only

Project tree: S7-1200 Tabletop Demo V16 KTP700 V3 Secured > CPU 1215C [CPU 1215C DC/DC/DC] > Program blocks > Main [OB1]

Block interface: "Main Program Sweep (Cycle)" Passwords for this demo project

Network 1: Security Block

Comment

Security\_FB Block:

- EN
- ENO
- "Password Control".Full\_PWD
- Enable\_RW
- "Password Control".Read\_PWD
- Enable\_Read
- %M1.2 "AlwaysTRUE"
- Enable\_HMI
- Checksum\_RT
- Checksum
- RW\_PW\_Enabled
- Read\_PW\_Enabled
- HMI\_PW\_Enabled
- Code Changed

Authorized connection [CPU 1215C] dialog box:

A password is needed to read-protected blocks of a protected device.

\*\*\*\*\*

OK Cancel

1. Open the "Main {OB1}" block in the project tree under the Program blocks/Demo folders.
2. Select the Monitoring On/Off icon in the editor window toolbar
3. Enter the CPU Read access password: **ReadOnly**
4. Click OK

**Notice:**

Regardless of entering the correct access level password, the system does not grant you access. This is because we have implemented a secondary user authentication with the ENDIS\_PW instruction before entering the correct access level password. This second authentication could be a unique user login on the HMI, employee badge, key switch, etc.

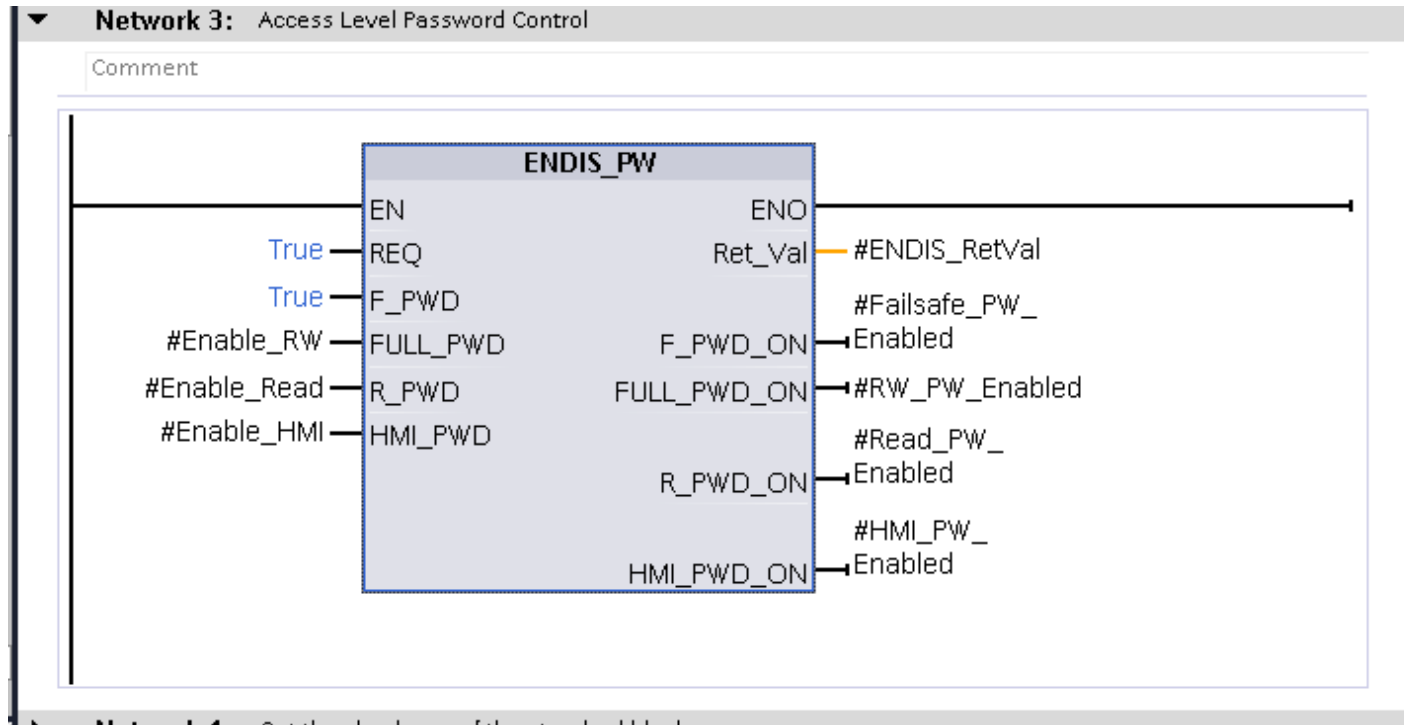
This feature prevents unauthorized users from having access to certain functions despite having the access level password (for example a "sticky note" with the 'admin' password).



# Multifactor Access Rights Authentication

# Security Features

## Secondary Authentication with 'ENDIS\_PW' Instruction



You can use the "ENDIS\_PW" instruction to specify whether configured access level password may be enabled or not for the CPU. Therefore, you can prevent legitimated connections even when the correct password is known.

With inputs at each access level being TRUE condition, you therefore enable access to the PLC with the respective PLC access level password(s).

In this exercise, we will utilize HMI user logins as the secondary access authorization, however this could be in the form of any other type of input (i.e. key switch, ID Badge, etc.)



# Security Features

## 2-level Authentication



We will now enable the secondary access level so that we can go online with our project using the Read Only access level.

1. On the HMI, go to the "Security" screen

Notice:

The screen shows that only "HMI" access level is authorized. Both "Read Only" and "Read/Write" access levels are not authorized yet because the appropriate user has not logged in.

2. Press the ellipses in the 'Operator' field to open the user login screen.



# Security Features

## 2-level Authentication

User Name

1

Password

2

3

4

**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 !

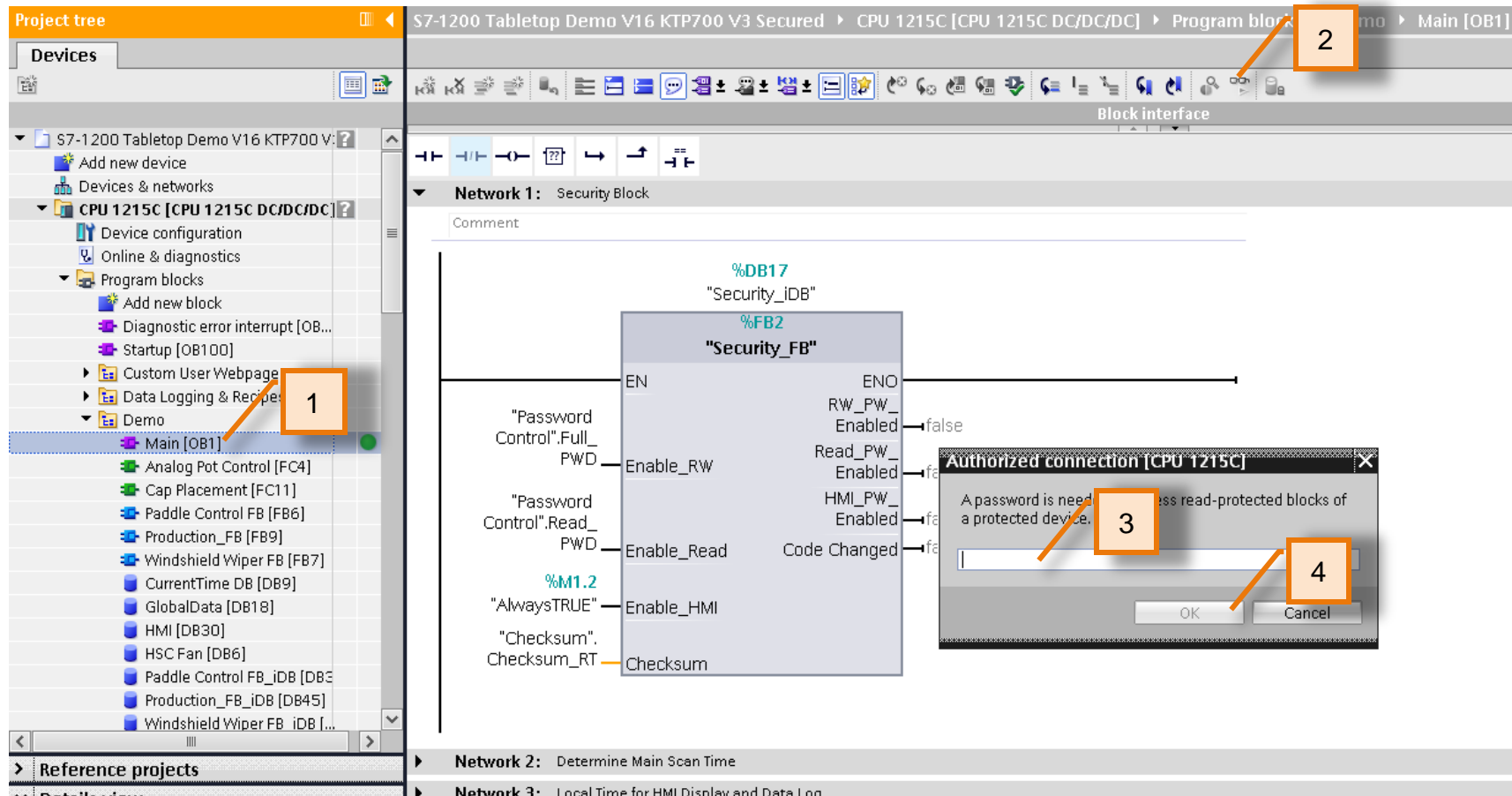
Demo PID Motion Wiper Security Recipe Web Server

1. Enter '**Werner**' as the username
  2. Enter '**Werner**' as the password (**Password is case-sensitive!**)
  3. Press 'LOGIN'
  4. Close the screen by pressing 'CLOSE'
- ! Notice:  
You now have logged in with a user who has "Read Only" authorization.



# Security Features

## Access Levels – Read Only



1. Open the "Main {OB1}" block in the project tree under the Program blocks/Demo folders.
2. Select the Monitoring On/Off icon in the editor window toolbar.
3. Enter the CPU Read access password: **ReadOnly**
4. Click OK.

You are now online monitoring OB1 with "Read Only" access rights to the PLC. Any modifications in the project is possible, but will require authorization for "read/write" access before downloading to the CPU.

Optional step: If you log off via the HMI, you will automatically be kicked off online access in TIA Portal as the "Read Only" Access level has been revoked.



# Write Protection

# Security Features

## Read Only Protected Blocks

3

The block is can only be read because it is write protected.

1

2

Block interface

Block title: .....

Comment

Network 1: Reset Paddle\_Count

Comm

Collapse

Cut Ctrl+X

Copy Ctrl+C

Paste Ctrl+V

Define tag... Ctrl+Shift+I

Rename tag... Ctrl+Shift+T

Rewire tag... Ctrl+Shift+R

Copy as text

Delete

Cross-references F11

Cross-reference information Shift+F11

Compile

Download to device

Insert network Ctrl+R

Insert STL network

Insert SCL network

Set network title automatically

#Reset\_Count

Network 2: Determine Paddle Direction

Comment

"HMI". PaddleDirection

"GlobalData". Production. EnableProduction

%Q8.0 "Paddle\_Direction"

1. Open 'Paddle Control FB [FB6]'
2. Attempt to delete network 1 – you will find this is not permitted. Likewise any modification to FB6 is not permitted because the block has "write protection" enabled
3. Click on the indicator at the top of the block interface. !

! Notice: the message at the top of the block interface indicating the block is write protected).

Once a block has been assigned as write-protected, it is impossible to edit this block and any subordinate (nested) blocks unless the write protection attribute is removed from the block properties.

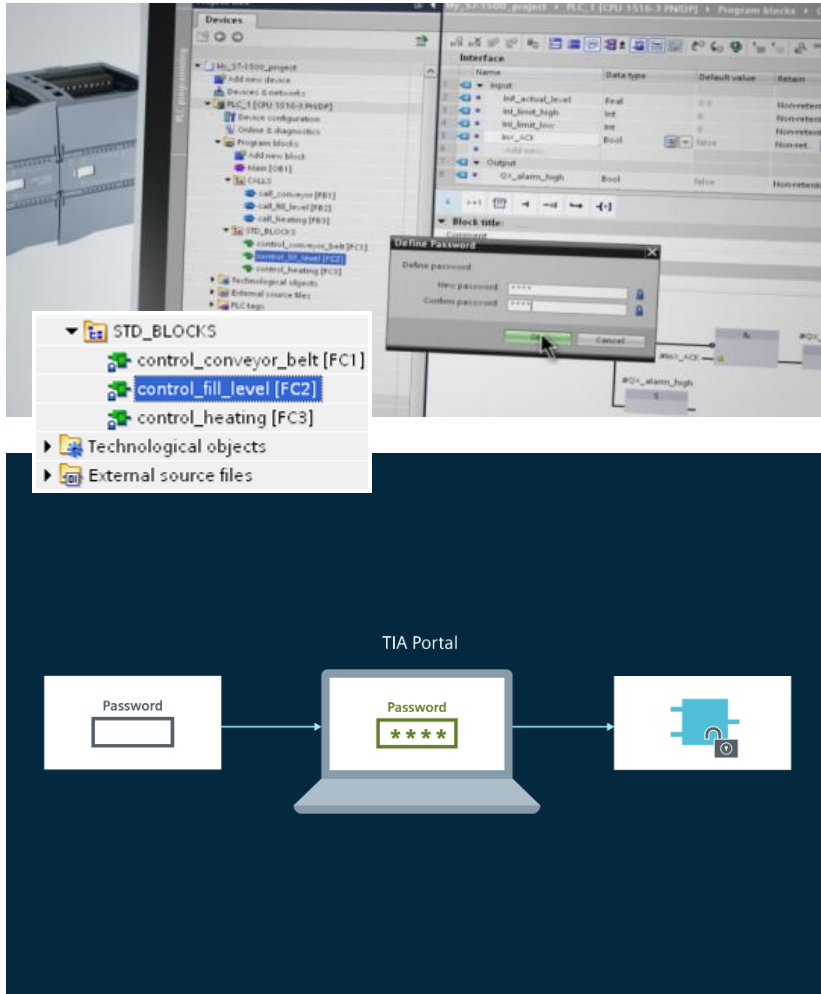




# Know-How Protection

# Security Features

## Know-How Protection



## Security Highlights

For SIMATIC **S7-1200** the **TIA Portal** provides several security features to protect your investment against unauthorized reading and copying:

- **Increased Know-how Protection for Programs**
  - Prevents reading, content copying and unnoticed changes of program blocks
  - Protects program blocks in the engineering project and in the controller
  - Program block protection in projects and libraries



# Security Features

## Know-How Protection

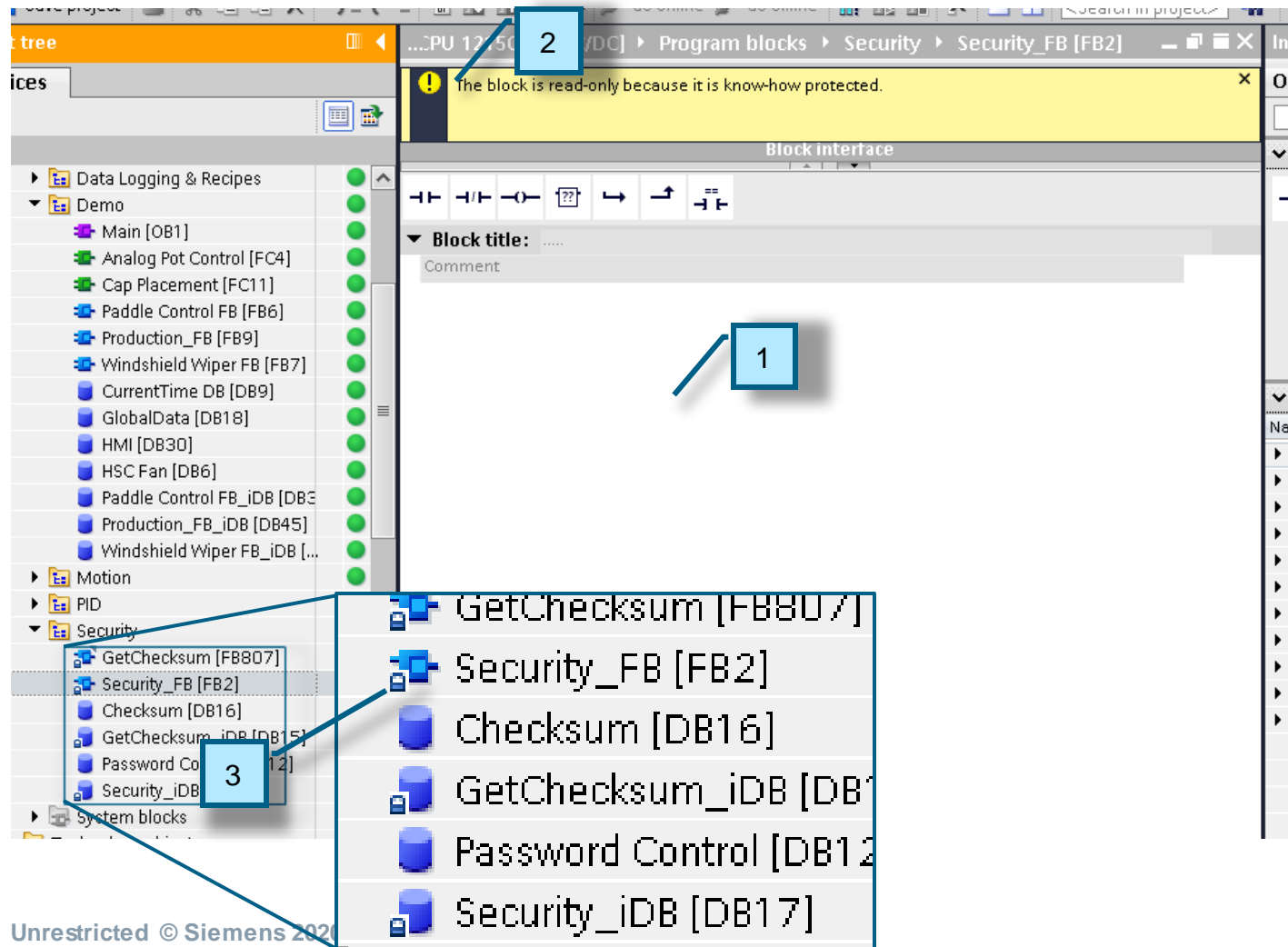
The screenshot displays the SIMATIC Manager interface. On the left, the project tree shows the 'Security' folder expanded, with 'Security\_FB [FB2]' highlighted. An orange box with the number '1' points to this block. The main workspace shows the 'Security\_FB' block with its inputs and outputs. An orange box with the number '2' points to the 'Cancel' button in the 'Access protection' dialog box, which is overlaid on the workspace. The dialog box contains the text 'Enter password for 'Security\_FB':' and a text input field.

1. Double-click on FB2 "Security\_FB" from the project tree to open the block  
  
You will immediately be prompted to enter a password. This is the Know-How password.
2. Click Cancel.



# Security Features

## Know-How Protection

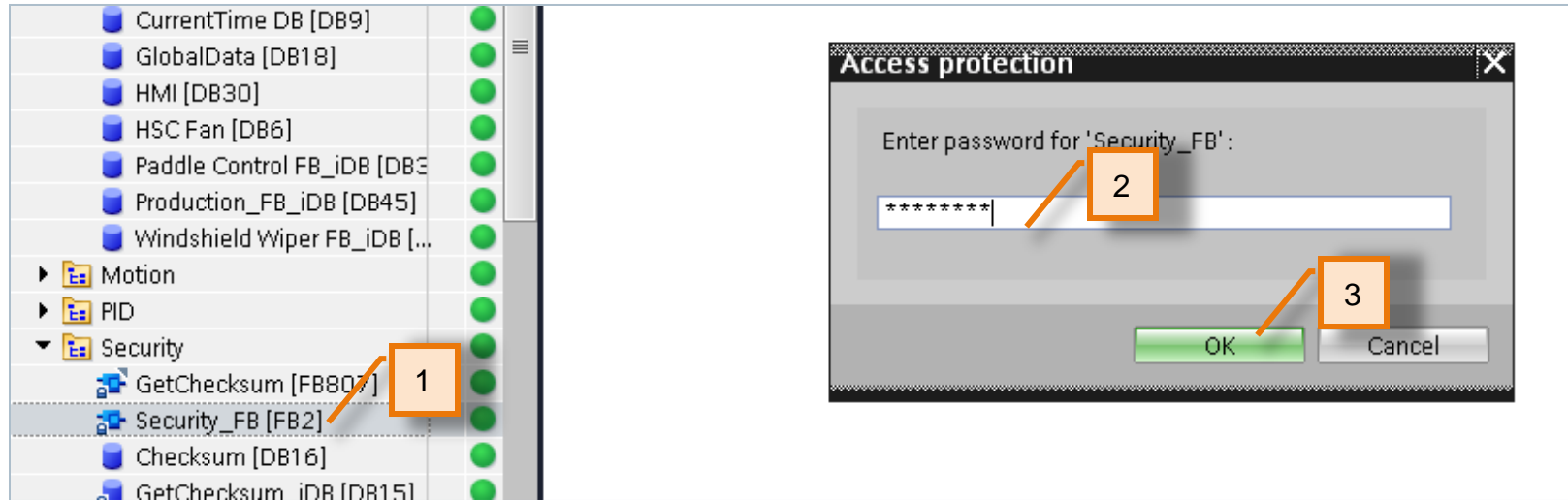


1. Notice the Block opens, but the logic within is hidden.
2. There is also a message at the top of the block indicating that the block is know-how protected.
3. Also notice the block is shown to be know-how protected via the "lock" symbol in the project tree



# Security Features

## Know-How Protection



1. Double-click FB2 again from the project tree to open the login prompt
2. Enter the following know-how password:  
**S3curity**
3. Click OK



# Security Features

## CPU Protection

The screenshot displays the Siemens TIA Portal interface. The top window shows the 'Block interface' for 'Security\_FB [FB2]'. The ladder logic network is visible, with a blue box labeled '1' pointing to the 'String' variable 'OEM' in the first network. The bottom window shows the 'Properties' dialog for 'Security\_FB [FB2]', with a blue box labeled '2' pointing to the 'Know-how protection' section, which is currently selected and shows 'The block is protected. (1 G4)'. The 'Write protection' section is also visible, showing 'The password for write protection has not been defined.' and a 'Define password' button. The 'Copy protection' section is set to 'No binding'.

1. It is now possible to view and modify the code
2. The Know-how protect option is selected


Note: To make changes to the protection level of a block the editor needs to be closed and the CPU to be offline.



# Security Features

## Editing Know-How Protected Blocks

The screenshot shows the Siemens TIA Portal interface. On the left, the Project tree displays the hierarchy: S7-1200 Tabletop Demo V16 KTP700 V3 S: > CPU 1215C [CPU 1215C DC/DC/DC] > Program blocks > Security > Security\_FB [FB2]. The main workspace shows Network 1: verify secondary user access level. The ladder logic consists of two parallel normally open contacts. The top contact is labeled "HMI".Logged\_In\_User with a data type of String and value 'OEM'. The bottom contact is labeled "HMI".Logged\_In\_User with a data type of String and value 'Siemens'. A normally open contact labeled "%M1.2 AlwaysTRUE" is added in parallel to the bottom contact. An orange box labeled '1' points to this contact. Above the network, the toolbar contains a download icon (a blue square with a white arrow pointing down), which is highlighted by an orange box labeled '2'.

1. Modify the block by adding a normally open contact with the “Always TRUE” %M1.2 variable as shown
2. Select the download icon on the toolbar to download the program change to the CPU. 



# Security Features

## Editing Know How Protected Blocks

**Load preview**

Check before loading

Status	!	Target	Message	Action
✓	✓	▼ CPU 1215C	Ready for loading.	Load 'CPU 1215C'
✓	✓	▼ Password	Password required. Enter a password to gain full access to the module "CPU 1215C".	*****
✓	✓	► Software	Download software to device	Consistent download

User Name: OEM

Password: \*\*\*\*\*

LOGIN LOG OFF

CLOSE

Finish Load Cancel

1. Since the online access that is currently enabled is "Read Only" the "Read/Write" access level must be obtained to be able write to the CPU. Enter the Full (read/write) access password: **Siemens1!**
2. Notice: You are unable to enter the access level password for "Read/Write" until a user with "Read/Write" access rights is logged in via the HMI.
2. On the HMI, Login with the following User credentials:  
User Name: **OEM**  
Password: **OEM (all caps)**  
[See Page 21 for logging in via HMI]
3. Now re-enter the access level password from step 1 above and hit Enter. You should now be able to click the 'Load' button. Continue with the download.





# Manipulation detection

# Security Features

## Manipulation detection with digital checksums



**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

After compiling and downloading the modified code, the program checksum has changed. Therefore, the operator is alerted on the screen of a mismatch between the initially commissioned checksum and the new program checksum.

This feature can be used to monitor unauthorized program or firmware changes. It is also possible to monitor changes in text lists to prevent masking of alarms.



# Web Server User Access Levels

# Security Features

Use HMI to view the CPU webpage

**SIEMENS**  
*Ingenuity for life*

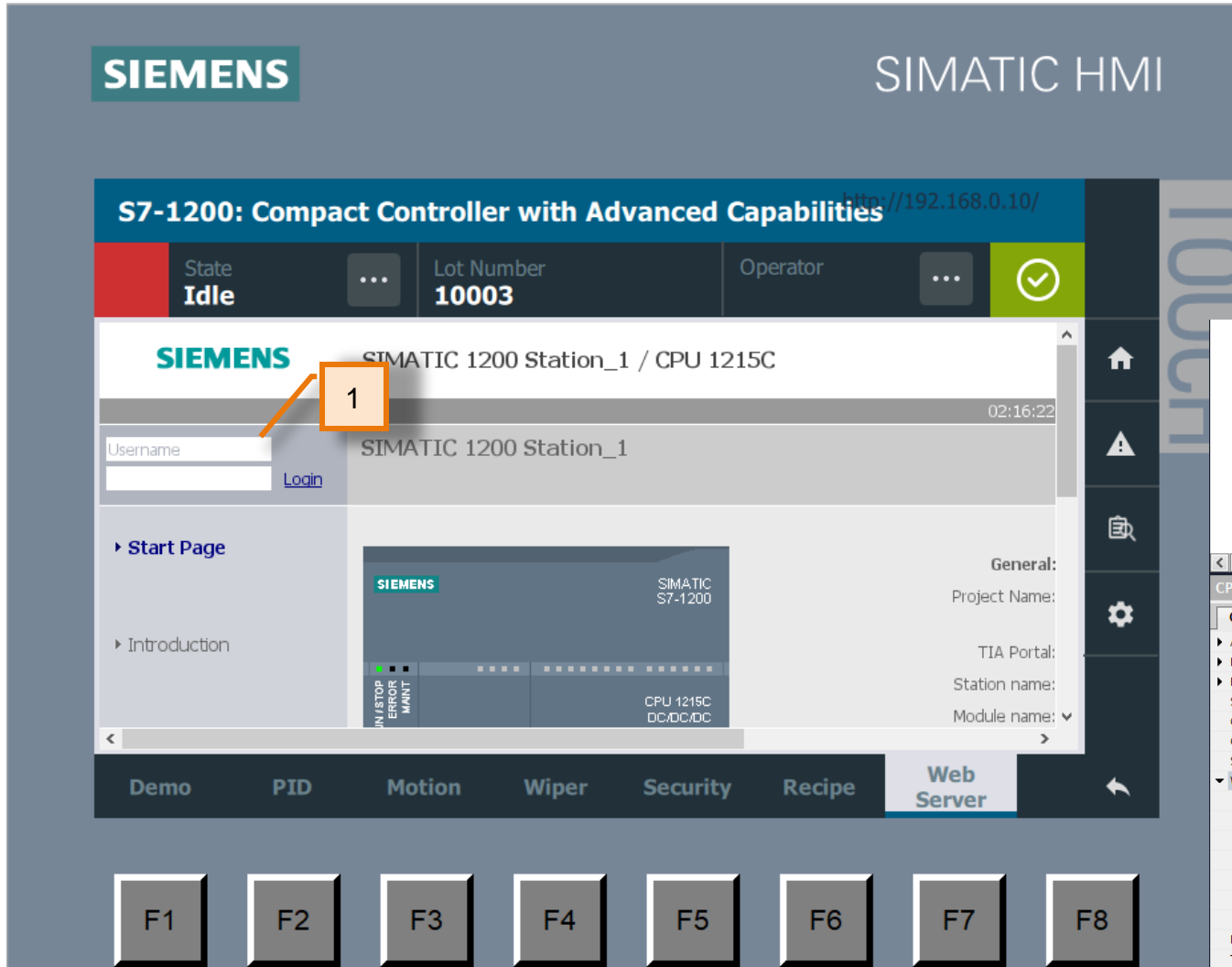


1. Go to the Web server screen on the HMI to connect to the CPU webpage
2. Click the ENTER button



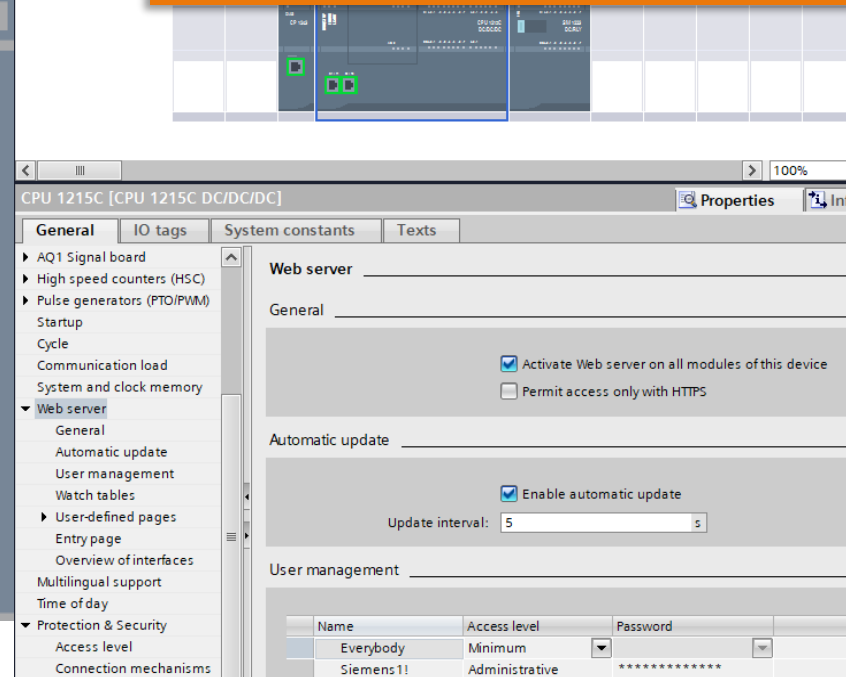
# Security Features

## Use HMI to view the CPU webpage



Notice the Web Server shows limited information. The CPU has been configured to restrict access in the webserver unless someone is login.

1. Login to the web server with the following credentials:  
Username: Siemens1! (case-sensitive!)  
Password: Siemens1! (case-sensitive!)  
This allows access to all the webpage functions.



# Summary

# Security Integrated

## S7-1200 Security Overview – features demonstrated

### System Integrity

- ✓ Protection of offline project (UMAC)
- ✓ Access Protection
- ✓ Multifactor authorization
- ✓ Manipulation Protection
- ✓ Know-How Protection
- ✓ Web Server Access Protection



# End of 'Integrated Security Functions'



THE INFORMATION PROVIDED HEREIN IS PROVIDED AS A GENERAL REFERENCE REGARDING THE USE OF APPLICABLE PRODUCTS IN GENERIC APPLICATIONS. THIS INFORMATION IS PROVIDED WITHOUT WARRANTY. IT IS YOUR RESPONSIBILITY TO ENSURE THAT YOU ARE USING ALL MENTIONED PRODUCTS PROPERLY IN YOUR SPECIFIC APPLICATION. IF YOU USE THE INFORMATION PROVIDED HEREIN IN YOUR SPECIFIC APPLICATION, PLEASE DOUBLE CHECK ITS APPLICABILITY AND BE ADVISED THAT YOU ARE USING THIS INFORMATION AT YOUR OWN RISK. THE PURCHASER OF THE PRODUCT MUST CONFIRM THE SUITABILITY OF THE PRODUCT FOR THE INTENDED USE, AND ASSUME ALL RISK AND LIABILITY IN CONNECTION WITH THE USE.

THIS GUIDE SHOULD NOT BE USED AS A SUBSTITUTE FOR OR IN LIEU OF A THOROUGH REVIEW AND UNDERSTANDING OF ALL WRITTEN INSTRUCTION AND OPERATION MANUALS AND GUIDELINES.

THE CONTENTS OF THIS GUIDE SHALL NOT BECOME PART OF OR MODIFY ANY PRIOR OR EXISTING AGREEMENT, COMMITMENT OR RELATIONSHIP. THE SALES CONTRACT CONTAINS THE ENTIRE OBLIGATION OF SIEMENS.

MODIFICATION AND OR DISTRIBUTION OF THIS CONTENT IS STRICTLY PROHIBITED.

