Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices

SIMATIC WinCC Unified V16
SIMATIC HMI Unified Comfort Panels

https://support.industry.siemens.com/cs/ww/en/view/109481300

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.
By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

1 Introduction

1.1 Motivation

Cyber-attacks on industrial control systems are now an unavoidable aspect of business and will continue to increase. A cyber-attack against your company is therefore not a question of "if", but rather "when".

Accordingly, the topic of industrial security is increasingly important for owners of machinery and plants. In order to become more resistant to cyber-attacks, strategies must be developed to defend against those attacks.

Figure 1-1

1.2 Overview

The goal of this document is to attune your senses to the topic of "security aspects for SIMATIC HMI Unified operator devices".

Top priority is given in automation engineering to maintaining production and process control. Any measures taken to prevent the propagation of security risks must not have a negative impact in this context.

This document describes possible risk points, and how you can minimize them with a targeted approach. Using this description, you can take suitable measures to increase security.

The following topic areas will be treated in greater detail with respect to their security aspects in the corresponding chapters:

- Risk analysis in engineering → see chapter 2
- Risk analysis during operation → see chapter 3
- Hardware risk analysis → see chapter 4
- Risk analysis when using services and apps → see chapter 5

1.3 Industrial security

The crucial question is: How can potential risks be significantly minimized and how can adequate, but affordable security be achieved in industrial automation?

Sadly, there is no one-size-fits all solution. In general, however, isolated security measures alone will not be sufficient.

1.3.1 Cybersecurity for critical infrastructure

Cyber-attacks on critical infrastructure are now far from rare. Lawmakers in various countries have already responded and prescribe strict standards and regulations for what companies must do to protect their systems.

You can download the whitepaper "Cybersecurity for critical systems" at the link below. It describes all necessary steps in detail.

https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/downloads/white-paper-infrastructures.html

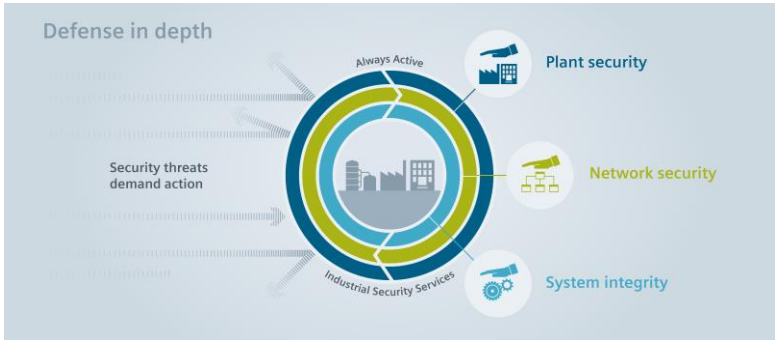
1.3.2 Defense in depth

With a defense-in-depth approach, it is possible to achieve comprehensive and reliable protection of an automation system. The basis is the international IEC 62443 standards series on "IT security for industrial control systems – network and system protection".

The concept of "defense in depth" entails the following three components:

- Plant security
- Network security
- System integrity

Figure 1-2



Plant security

Secure physical access of persons to critical components - through the systematic use of security mechanisms in automation.

- Fenced campus or plant with access control.
- Biometric access control and/or locks on rooms (laboratory, server rooms).
- Alarm systems or video monitoring.

Network security

Industrial communication is a key factor for corporate success – as long as the network is protected.

The first step in network segmentations lies in the **strict** separation between production networks and the other corporate networks.

- Monitored interfaces between the office network and plant network, e.g. via firewalls
- Further segmentation of the plant network (individual protected automation cells).

System integrity

Ensuring system integrity with internal protection functions Antivirus and whitelisting software

- Maintenance and update operations
- User authentication for plant or machine operators
- Access protection mechanisms integrated in automation components

Note If a measure cannot be implemented, the risk should be minimized with an alternative countermeasure.

Note Further information on the topic of industrial security and defense in depth can be found at the following link:

http://www.siemens.com/industrialsecurity

What advantage does this give you?

The concept of "defense in depth" requires a higher initial investment in project planning. This increased expenditure pays for itself in the long run through:

- Increased protection
- Increased plant availability
- Reduced risk
- Protection of intellectual property
- Security support over the entire life cycle

Note Security is also a core aspect of WinCC (TIA Portal).

1.3.3 Security management

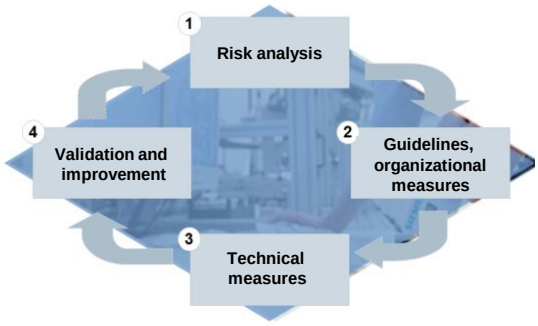
Organizational measures and the introduction of security processes are an indispensable component of plant security.

Organizational measures must be closely tied in with the technical measures and they must be mutually supportive. Most protection goals can only be achieved by combining the two types of measures.

A security management process is indispensable for a well thought out security concept.

Security management process

Figure 1-3



The protection goals are derived from the risk analysis and serve as the basis for concrete organizational and technical measures.
Measured be checked from time to time after implementation.

Brief description of the "Security management process"

1. Risk analysis
   Analysis of risks, definition of measures to reduce risk
2. Guidelines and organizational measures
   Definition of guidelines and coordination of organizational measures
3. Technical measures
   Coordination of technical measures
4. Validation and improvement
   Regular/event-dependent repetition of the risk assessment

Note "Smart" devices and apps must also be taken into consideration in the security management process.

2 Risk analysis in engineering

This chapter describes the handling of projects and individual functions intended to increase plant security.

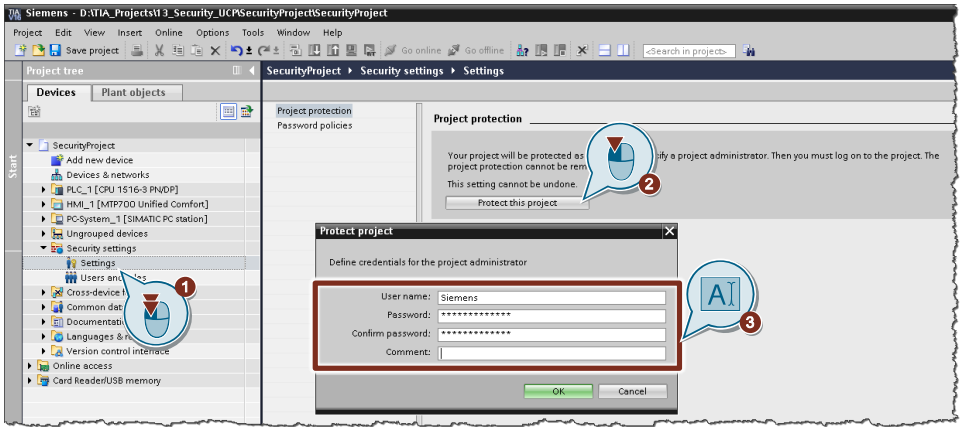
2.1 Opening and editing project engineering

To protect your TIA Portal project from tampering, you can protect opening projects in SIMATIC WinCC Unified V16 with a password, thereby also protecting the editing of projects.

Follow the steps below:

1. In the project tree, double-click on "Security settings".
2. Then click "Protect this project".
3. Enter the username and password in the open "Protect project" dialog box.

Figure 2-1



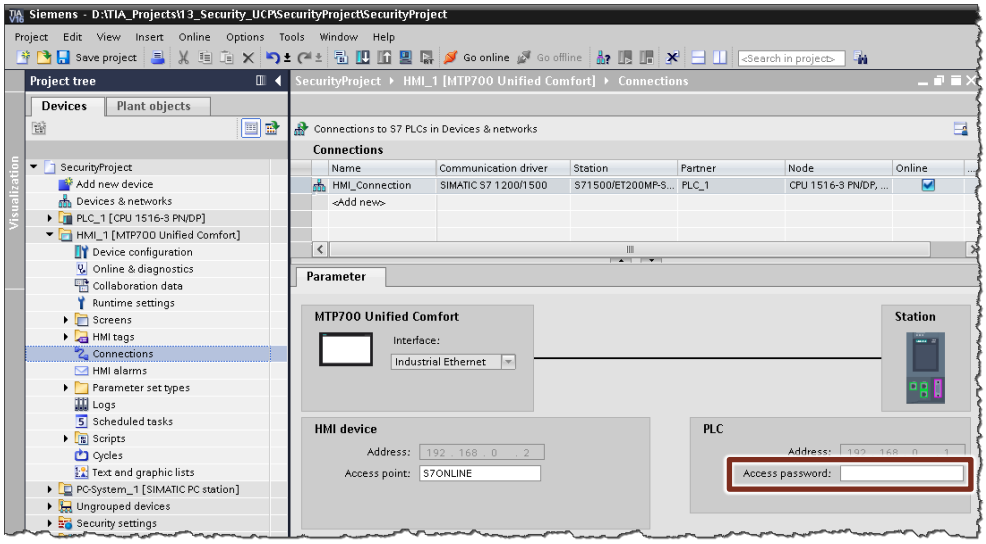
CAUTION	If you have password-protected a project, you can no longer remove it. The project will remain password-protected.

2.2 Use access password for HMI connection

By networking nodes over Ethernet/PROFINET, there is the risk that the values can be read from outside and possibly manipulated.

It is also recommended to protect the PLC with a password. In order to access the protected PLC from a Unified operator device, you must store the access password in the connection settings.

Figure 2-2



2.3 Archiving of tags and messages

External storage devices, such as storage cards and USB drives, are frequently used as a save location for archiving tags and messages. The danger with storage media is that they can be removed in an uncontrolled manner, or can be lost.

Furthermore, archived process values and messages are often "sensitive" data (e.g. performance data or product data), which are used in particular for documenting quality assurance. These data must be protected from unintended or unauthorized modification/theft at all costs.

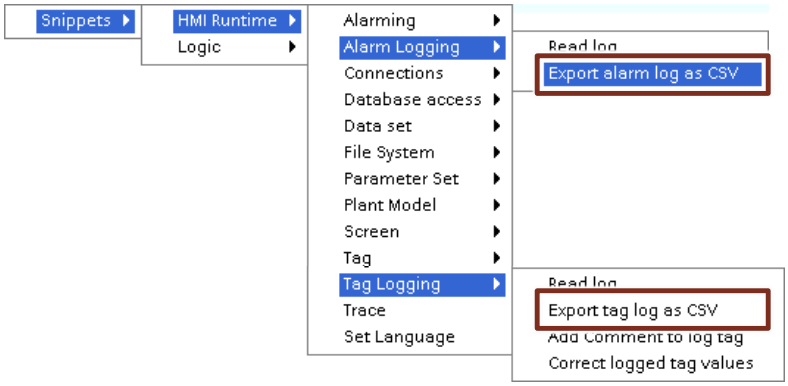
2.3.1 Archiving on a SIMATIC HMI Unified Comfort Panel

Unified Comfort Panels support file-based archiving in the form of "SQLite". You can configure the save location on both the SD card and on the USB drive.

In order to prevent abuse or theft of archived data, you should protect the interfaces of the Unified Comfort Panel from unauthorized access, for instance by installing the panel in a lockable control cabinet (see chapter 4.1.1, heading "Physical safeguards").

As an additional security measure, you should regularly export the archived data as a CSV file to an access-protected save location (snippet "Export log as CSV").

Figure 2-3, snippets to export log data as CSV



Note Keep yourself informed about developments on the topic of tamper protection for data on WinCC Unified Comfort Panels.

2.3.2 Archiving on WinCC Unified PC Runtime

With the WinCC Unified PC Runtime, you have two ways of archiving your data:

- file-based archiving form (SQLite)
- database archiving (Microsoft SQL)

Protection with file-based archiving form (SQLite)

If you use the file-based archiving form on a PC station, you should make sure that the storage location of the logs is access-protected.

Furthermore, it is recommended here to regularly export the archived data as a CSV file to an access-protected save location (snippet "Export log as CSV").

Protection with database archiving (Microsoft SQL)

On Microsoft SQL servers, you can protect the databases of the archives by using the Windows Group "Simatic HMI" (read/write) and "Simatic HMI Viewer" (read). Only members of this group have direct access to the databases.

2.4 Working with parameter sets

Parameter sets are frequently used in process engineering facilities and in production plants that manufacture multiple different products with one station or machine.

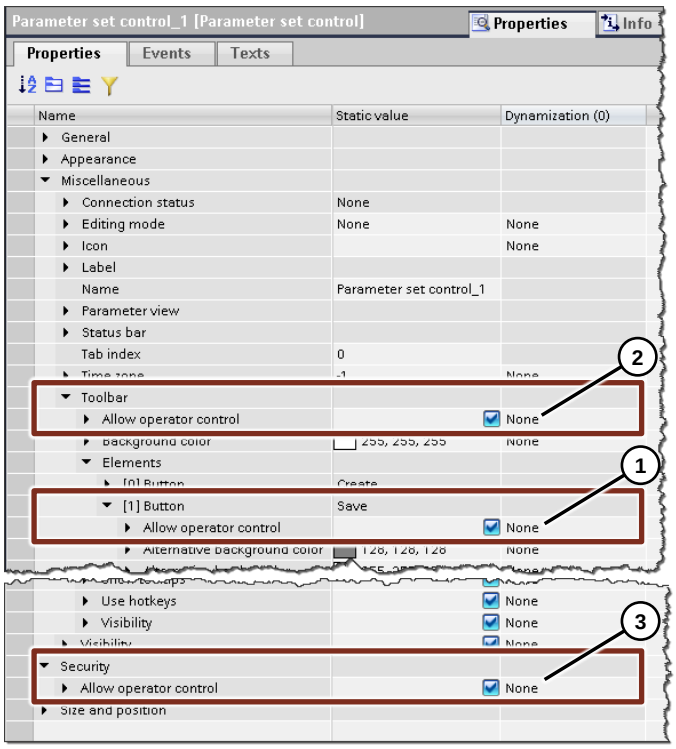
Depending on the application, the risk can be divided into two areas.

- Loss of "know how" through theft:
  Development of new parameter sets in process engineering requires significant resources in the form of time and capital. If these data fall into a competitor's hands, then a potential loss of competitiveness is at stake.
- Damage due to operator error:
  Selecting the wrong parameter set can result in major material damages. There is also the possibility of manually modifying individual parameters.

Access protection for controls

In order to hinder unauthorized persons from accessing parameter set data, you can use dynamization of the parameter set display to make access harder.

Figure 2-4



You can create different access levels at the control with the "Allow operator control" property.

You can control operator permission, starting from a single button in the icon bar (1), to the entire icon bar (2), all the way to full "parameter set display" control (3).

Saving on external storage media

If you specify an external storage medium (SD card or USB drive) on your SIMATIC HMI Unified Comfort Panel as the save location for the parameter sets, then another consideration of yours should be that the external media also can't fall into the hands of unauthorized persons (see chapter 4.1.1).

2.5 Access to tags via OPC UA

In the world of automation, there are many communication interfaces (often manufacturer-specific). OPC UA represents a manufacturer-independent standard which field devices can use to communicate with each other.

OPC UA in WinCC Unified

In WinCC Unified, OPC UA is disabled by default. If you enable the function, make sure that you do not use an unencrypted connection. Further information on encryption can be found in chapter 2.9.

Security policies

At the OPC UA server in WinCC Unified, you can select the following "Security policies":

- Basic128Rsa15
- Basic256
- Basic256Sha256

Message Security Mode

For "Message Security Mode", you can choose between the following types:

- Sign
- SignAndEncrypt

Note For an overview of which OPC UA communication functions are supported by SIMATIC WinCC Unified and SIMATIC HMI Unified Comfort Panels, refer to the FAQ entitled "How do SIMATIC and SITOP products support communication via OPC UA?".

https://support.industry.siemens.com/cs/ww/en/view/109763315

Note Use the setting "none" only if, for example, you are testing the OPC UA connection for the first time while commissioning.

2.6 Creating user administration

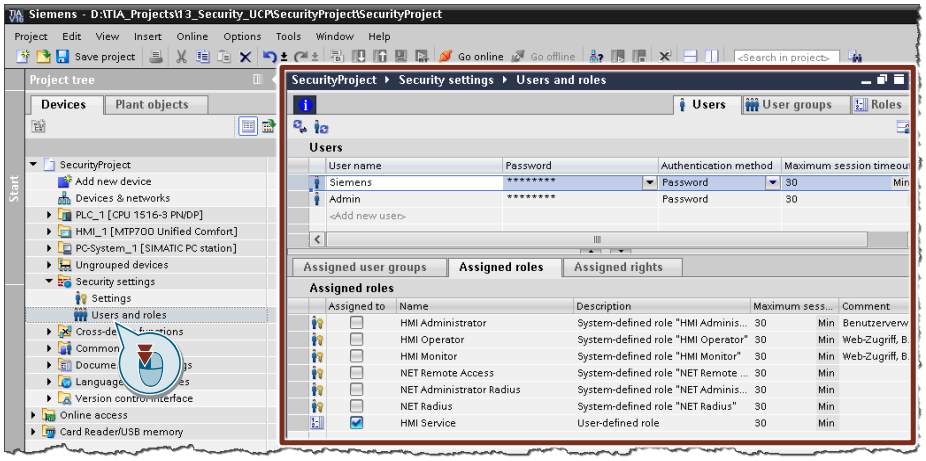
User administration is an especially sensitive area from a security lens. If, for example, the "Administrator password" is known, the user data can be changed on the operator device.

To prevent this, you should always work with a user administration system and keep it up to date.

User administration in WinCC Unified projects

WinCC Unified gives you the ability to manage users and roles under the "Security settings".

Figure 2-5



A user always consists of:

- User name
- Password and
- at least one assigned role

What should make up a password?

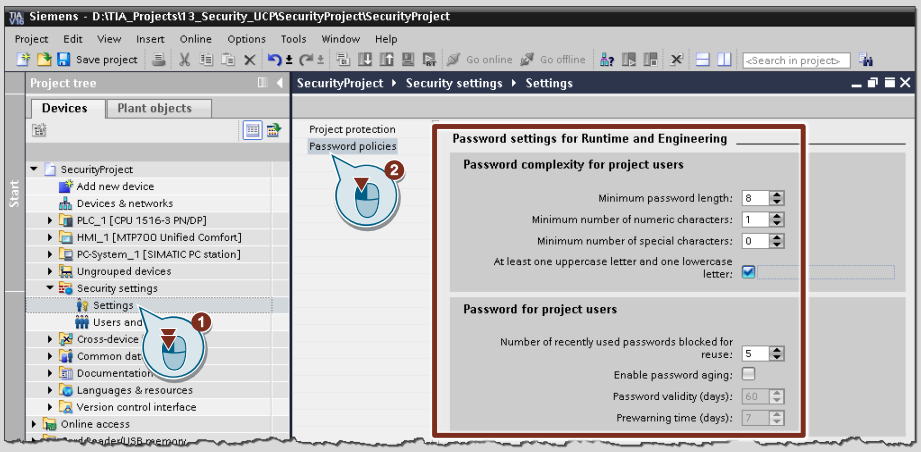
A password should:

- be at least eight characters long
- not consist only of letters, but also upper- and lowercase letters, special characters and numbers
- if at all possible, not be a word listed in the dictionary
- not be composed of characters that are next to each other on the keyboard (e.g. 123456 or asdfg)
- not contain the same repeating character (e.g. AAAA)

Note

WinCC Unified gives you the ability to set your own password policy. For further information, refer to the system manual "SIMATIC WinCC Engineering V16 - Runtime Unified" in the chapter entitled "Setting password policies":

https://support.industry.siemens.com/cs/ww/en/view/109773780/131129220235



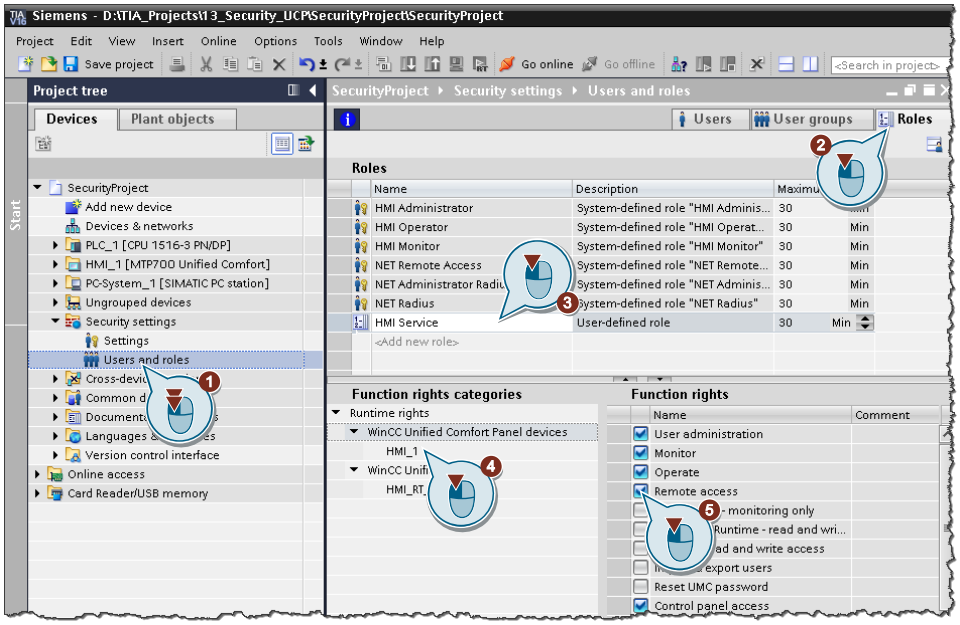
Roles and function rights

As mentioned above, one or more roles may be assigned to users in WinCC Unified.

In this case, each role has different function rights where you can store permissions for the runtime. You can set the function rights of a role for each Unified device separately.

When creating a project, make sure that each role receives only the operator device function rights that it absolutely needs. Furthermore, each user should be assigned the role that he/she has permission for.

Figure 2-6



2.7 Transferring the configuration to the HMI device

2.7.1 Select the correct operator device

The configuration can be transferred to the panel by any user. If system components are already in operation, heightened attention is required so that you download the project to the correct operator device.

If the wrong operator device is selected for the project download, this can cause the runtime of the operator device to be automatically terminated, and the system component will no longer be operable.

2.7.2 Signed panel images

The image file (operating system) from a SIMATIC HMI Unified Comfort Panel is version-dependent and is installed as part of the installation of the WinCC Unified (TIA Portal) engineering software on the configuration PC.

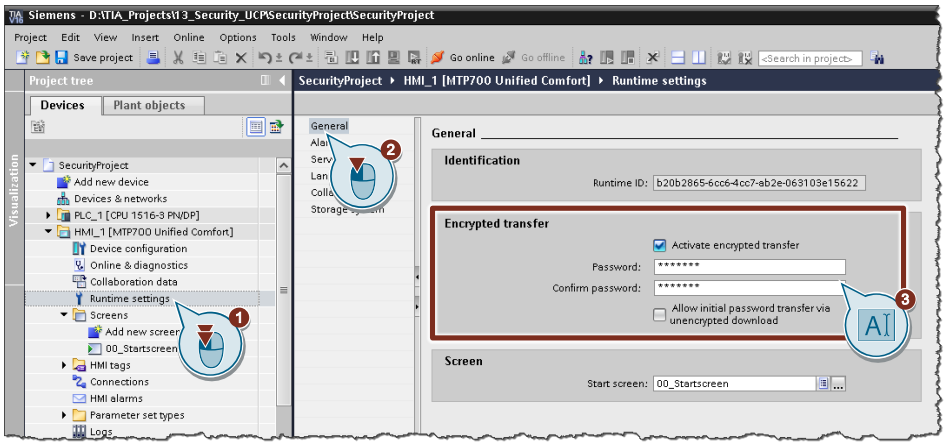
The image file is always signed. Prior to a project download, the HMI operator device checks the image signature. If it does not match, the download is cancelled.

2.7.3 Encrypted project transfer

By networking nodes over Ethernet/PROFINET, there is the risk that the values can be read from outside and possibly manipulated.

In WinCC Unified V16, you can encrypt the project transfer to the operator device. To do this, you can enable encrypted transfer in the runtime settings and set a password.

Figure 2-7



Note

The new password must meet the following conditions:

- Character length between 8 and 120 characters
- At least one uppercase and one lowercase letter
- At least one number
- At least one special character

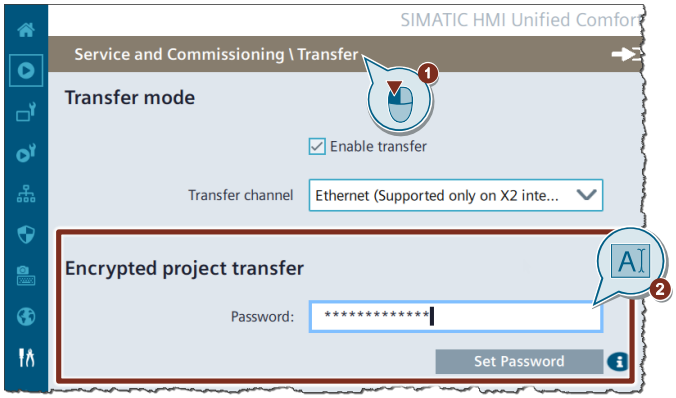
Then, you must also store the password on the runtime device.

SIMATIC HMI Unified Comfort Panel

On the SIMATIC HMI Unified Comfort Panel, enter the password directly at the operator device.

1. To do this, open the menu item "Service and Commissioning > Transfer" in the Control Panel.
2. Then, under "Encrypted project transfer", enter the password that you set during the engineering step, and confirm with "Set Password".

Figure 2-8



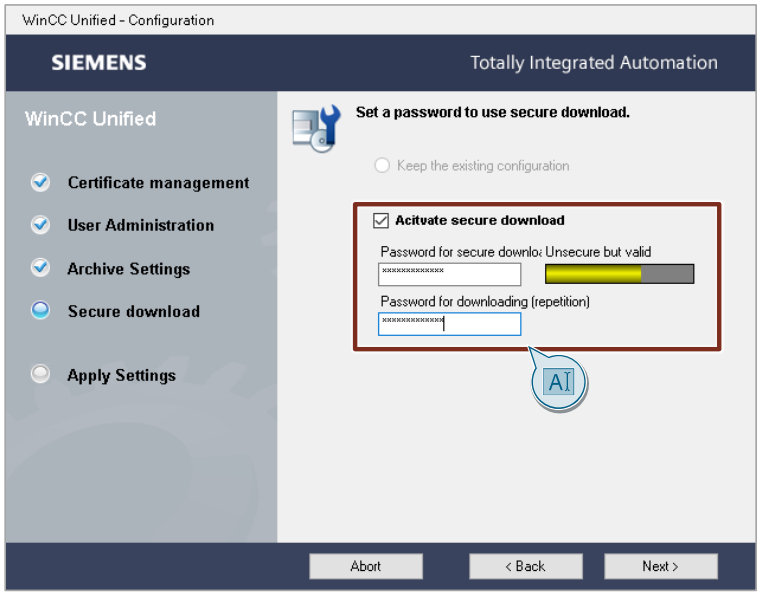
Note If you want to simulate your configuration, the settings must be made in the same manner as for the WinCC Unified PC Runtime.

WinCC Unified PC Runtime

For a PC station with a WinCC Unified Runtime, you can also use an encrypted project transfer.

Set the password for the PC runtime with the program "WinCC Unified Configuration" in the step "Secure Download".

Figure 2-9



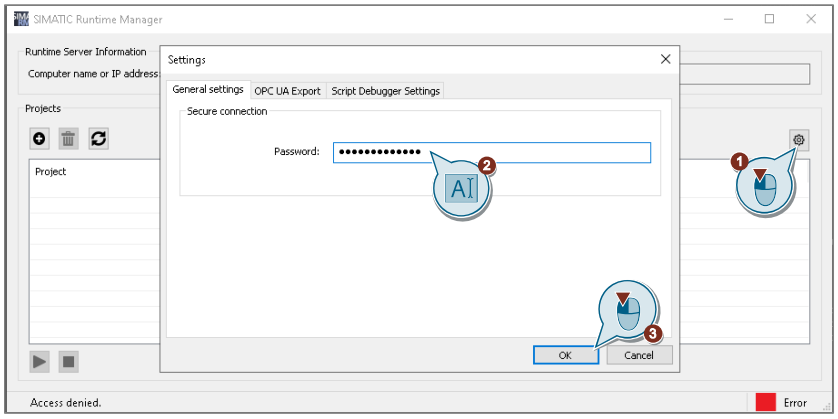
Note When you enable encrypted transfer, make sure that these settings also match the settings in the "WinCC Unified Configuration".

If the settings are different, you will see the error message "Error during loading - Contact Siemens Customer Support". You can find more information at the following link:

https://support.industry.siemens.com/cs/ww/en/view/109775493

To be able to also start runtime projects via the SIMATIC Runtime Manager, you must also store the password in the SIMATIC Runtime Manager settings.

Figure 2-10



2.8 Simulating and testing configuration

If the configuration is open, any use can start the simulation. If there is an active connection to a configured PLC, then the machine can be operated via this connection, which can lead to dangerous operating states.

Remedy

Lock the PC or laptop if it is out of your sight. This should be observed most of all when commissioning. Do not leave the PC or laptop unattended.

2.9 Configuring encrypted connection between Unified devices

With WinCC Unified, communication can also occur between multiple Unified devices.

To protect communication between WinCC Unified devices, use of encrypted communication protocols can guarantee security. Any communication partner receives a unique certificate which is used for all authentication and encryption.

Use cases

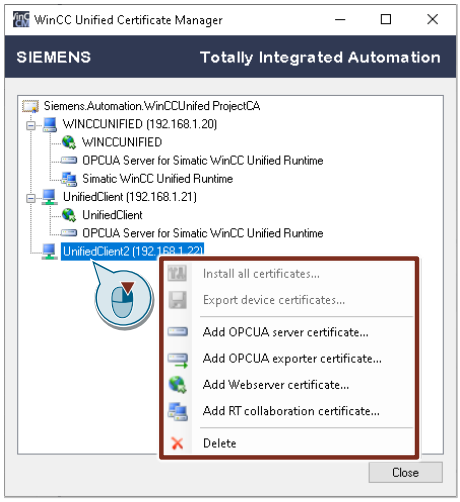
Communication between Unified devices is required to be encrypted for the following use cases:

- Server/client communication
- OPC UA connections
- Runtime collaboration

Creating and managing certificates

With the "WinCC Unified Certificate Manager", you can create, manage and install the necessary certificates for all three use cases.

Figure 2-11



Note

You can find additional information in the operating manual for the "SIMATIC WinCC Unified Certificate Manager":

https://support.industry.siemens.com/cs/ww/en/view/109779117/134276049675

3 Risk analysis during operation

General note on operating a plant

The safe operation of a plant requires a high degree of accuracy in the operating safety with the operator device.

Some examples are:

- Modification of specification of values from unauthorized persons (e.g. entering speed figures for drives).
- Switching the operating mode of a plant (manual/automatic operation).
- Operation of various plant screens.

This chapter describes measures you can take to protect operation from unauthorized access.

3.1 Operation of configured plant screen

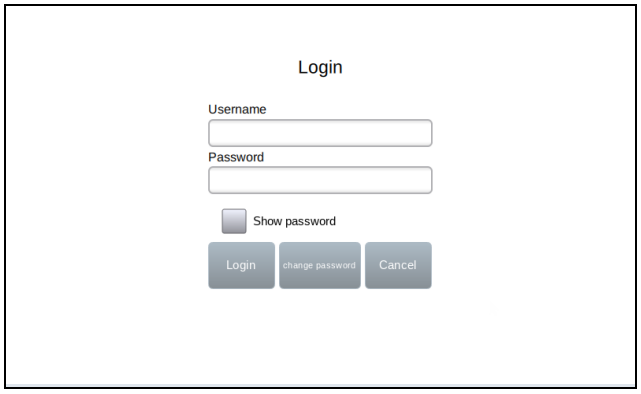
Plant screens of the operator devices are used, for example, to switch drives on and off. If unauthorized persons are able to carry out operator actions, then considerable damage can occur.

Remedy

In order to restrict operation to authorized personnel, individual roles with function rights can be assigned. This can ensure that only authorized persons can carry out an enabling action at a panel, for instance.

If an unauthorized operator presses an access-protected screen object, then the login dialog will appear and request login credentials.

Figure 3-1



If permissions are not sufficient, the notice "Authentication has failed" will appear.

Note

For more information on how to use user administration in the engineering step, refer to chapter 2.6 or the system manual "SIMATIC WinCC Engineering V16 - Runtime Unified" in the chapter "Configuring user administration".

https://support.industry.siemens.com/cs/de/en/view/109773780/129323781515

3.2 Ending HMI runtime

Before shutting off the operator device or PC, the Panel's runtime should be shut down in order to avoid data loss in ongoing actions (e.g. export or import of data). This is usually accomplished with a configured button on the panel and the system function "StopRuntime".

Remedy

Make sure that the function for ending the runtime can only be executed by authorized personnel. To do this, configure a permission on the button under "Properties > Security > Permissions".

3.3 Using encrypted connection between Unified devices

During operation, make sure that only encrypted connections are used between SIMATIC WinCC Unified devices.

The is the case with:

- Server/client connections
- OPC UA connections
- Runtime collaboration connections

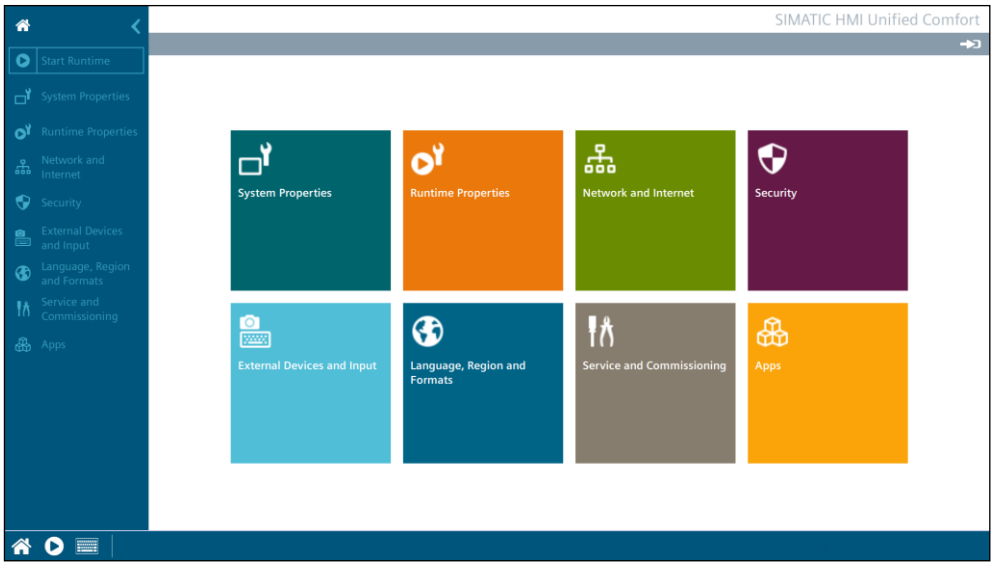
Note Further information on encryption can be found in chapter 2.6.

3.4 SIMATIC HMI Unified Comfort Panel (specific)

3.4.1 Enable access protection for the Control Panel

After turning on the panel, or after ending the runtime, the "Control Panel" menu will appear by default.

Figure 3-2



Using the individual tiles, you can call up the device settings and make changes to them.

In the absence of further settings, persons in your plant have access to all settings and functions of the operator device.

Note

You can use the system function "ShowControlPanel" to show individual Control Panel menu functions from the runtime.

Further information on the "ShowControlPanel" system function can be found in the system manual "SIMATIC WinCC Engineering V16 - Runtime Unified".

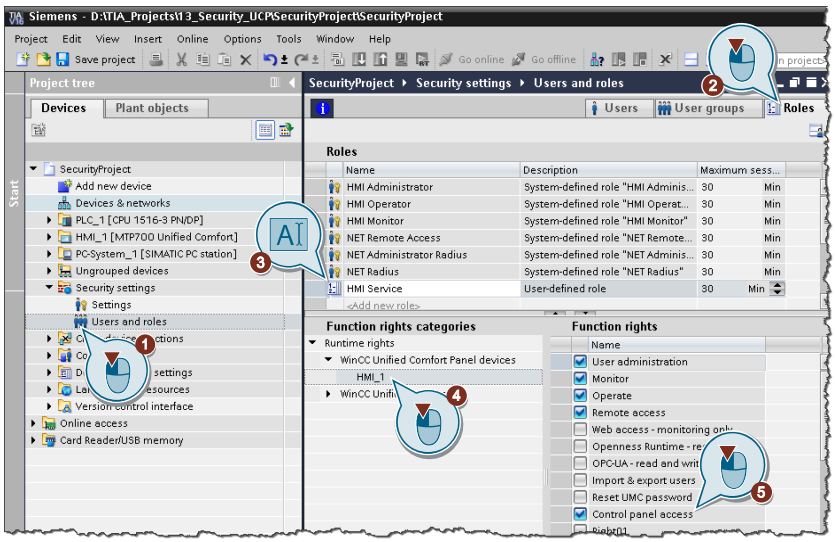
https://support.industry.siemens.com/cs/ww/en/view/109773780/123793475083

Configuring users for access protection

You have the ability to password-protect the Control Panel and thus protect it from unauthorized operation.

The following steps are required for this:

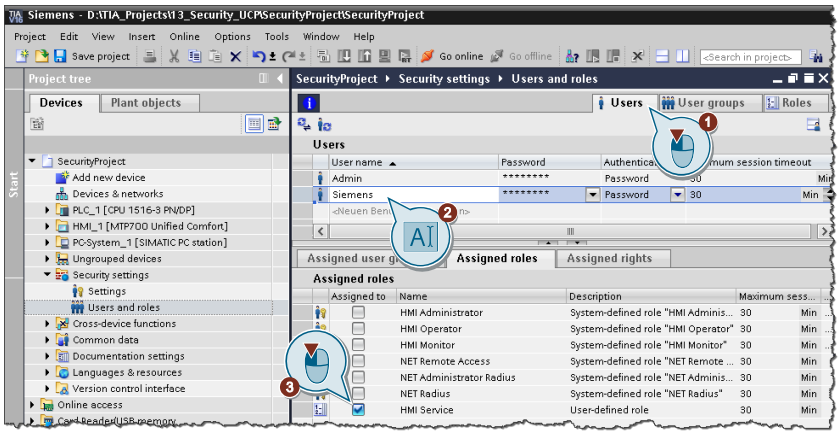
1. Add role
   - In TIA Portal under "Security settings", open the item "Users and roles" (1).
   - Then open the "Roles" tab (2).
   - Add a new role, "HMI Service" (3).
   - Select the operator device where you wish to configure access protection (4).
   - Enable the function right "Control panel access" (5).



Note:

In step 4, you can also select the entire device group "WinCC Unified Comfort Panel devices" instead of a single operator device.

2. Adding users
   - Switch back to the "Users" tab (1).
   - Add another user (2).
   - Assign the user the role "HMI Service" (3).

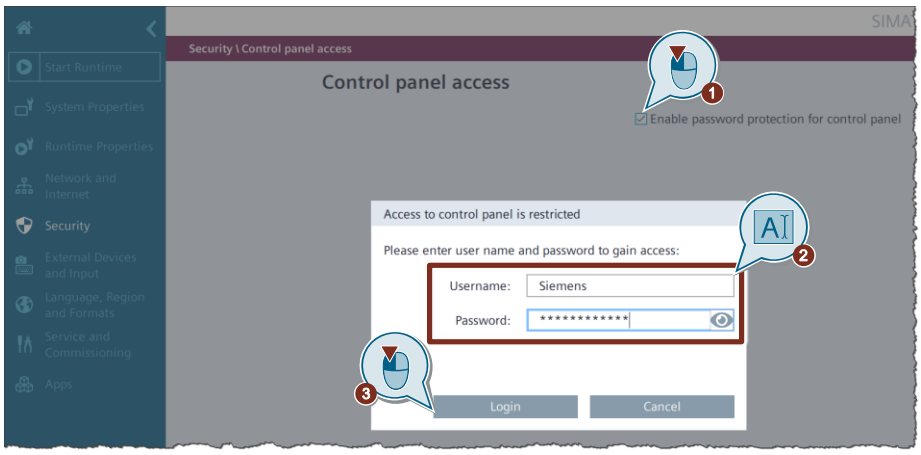


3. Download your project to the Unified Comfort Panel.

Enabling access protection on the panel

1. In the Control Panel on the operator device, open the menu "Security > Control panel access".
2. Enable access protection
   - Check the box "Enable password protection for control panel" (1).
   - In the next step, enter the user name and password of the user created previously (2).
   - Confirm the entry with "Login" (3).

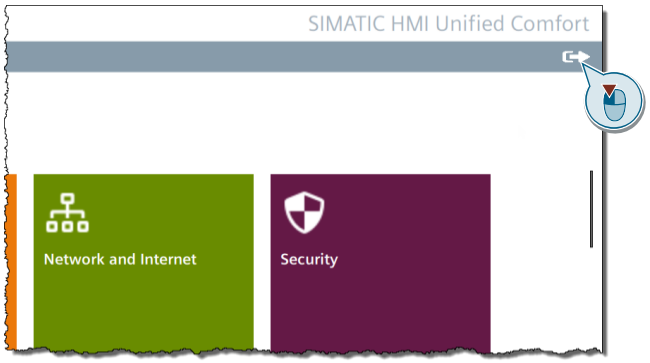
Figure 3-3



Once successfully enabled, the check box will appear checked.

3. Log off the "Siemens" user from the operator device.

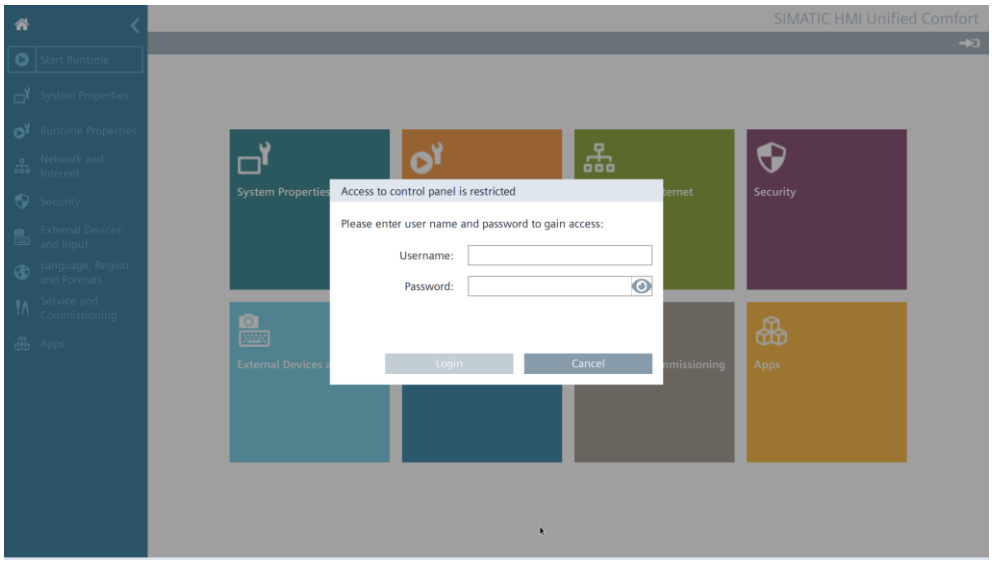
Figure 3-4



Behavior in case of unauthorized access

If a user tries to operate the Control Panel without authorization, the login dialog will appear.

Figure 3-5

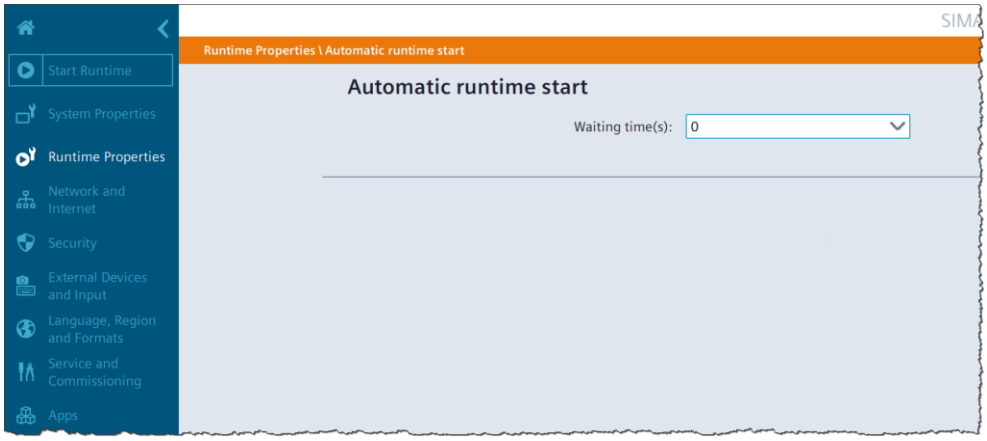


3.4.2 Changing runtime autostart

As an additional safeguard, you can set the wait time until the panel runtime starts in the panel device settings in the menu "Runtime Properties > Automatic runtime start". During this wait time, the "Control Panel" will show the start menu.

Set the wait time for the "Autostart" to "0 seconds".
After the panel is restarted, the runtime will now be shown right away, without displaying the "Control Panel".

Figure 3-6



3.5 SIMATIC WinCC Unified PC Runtime (specific)

Use Windows Kiosk mode

Using the Windows system settings, you can prohibit access to default Windows functions.

Another option with Windows Functional Update 1809 is to use the Microsoft Edge browser in Kiosk mode.

This means that, once logged on, the user has access to only one program. In this way, Kiosk mode can be used to display only the Unified PC runtime. Access to Windows settings and system settings is thus impossible.

Note Additional information can be found in the FAQ "How do you operate WinCC Unified in the Windows 10 full-screen mode/kiosk mode?":

https://support.industry.siemens.com/cs/ww/en/view/109771719

4 Hardware risk analysis

4.1 SIMATIC HMI Unified Comfort Panel (specific)

4.1.1 Protect SD and USB ports

External storage devices (SD card / USB drive) can be used as a save location for the archiving of process values and messages, or for storing documents. Depending on where the panel is installed, access to the storage locations is often very easy.

This presents the risk that:

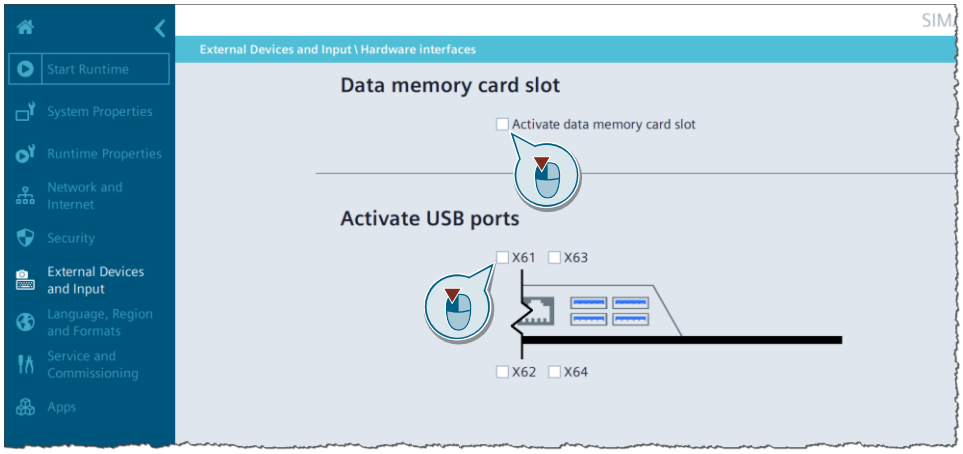
- sensitive data (e.g. recipe data records) can be stolen;
- data (e.g. in logs) can be manipulated;
- that dangerous programs and files can be transferred to the device.

Turning off expansion ports

The SIMATIC HMI Unified Comfort Panel Control Panel gives you the ability to disable the expansion ports with the menu item "External Devices and Input > Hardware Interfaces".

All unnecessary interfaces should be disabled by default.

Figure 4-1



Note If you disable USB ports, they will no longer be recognized by the operating system. However, the ports will still have power.

Physical safeguards

As an additional security measure, you can physically secure the USB port with a USB port lock.

If you still need USB or SD storage expansion, it is recommended to install the operator device in a lockable control cabinet so that the rear side of the Unified Comfort Panel is protected from unauthorized access.

4.1.2 Disable network interfaces

In addition to the SD and USB ports of the Unified Comfort Panel, the network interfaces also represent a risk. The risk in this case lies, among other things, in the loss of operability, e.g. due to the Ethernet connection being pulled out.

Another hazard potential is that communication may be recorded or modified if additional components are added, for example.

You have the following four ways of reducing this risk:

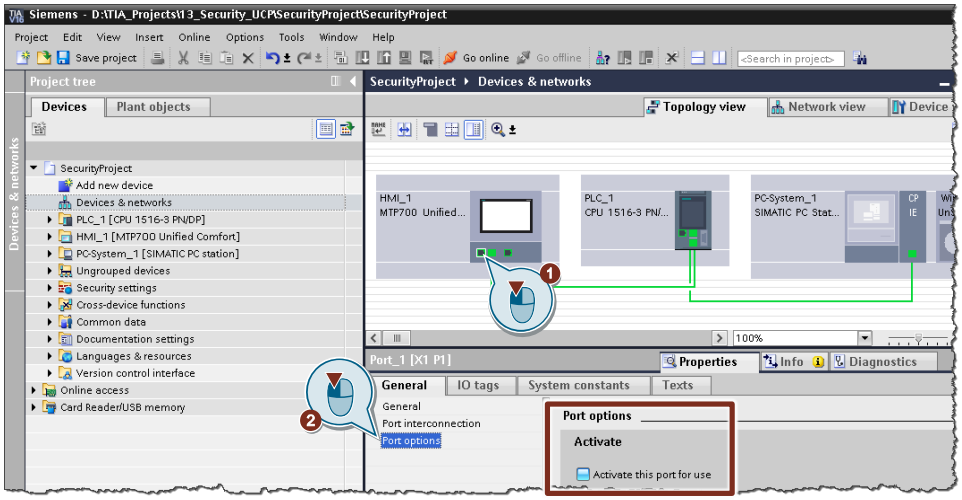
1. Enable/disable network adapter in engineering
2. Enable/disable network interfaces in the Control Panel
3. Enable/disable network adapter in the runtime
4. Physical safeguards

By default, you should only enable the ports and network adapters on the operator device that you need.

Disable network interfaces in engineering

As soon as the engineering phase you can define which ports will be enabled/disabled, e.g. with the Topology view. During project download, the settings will be transferred to the device.

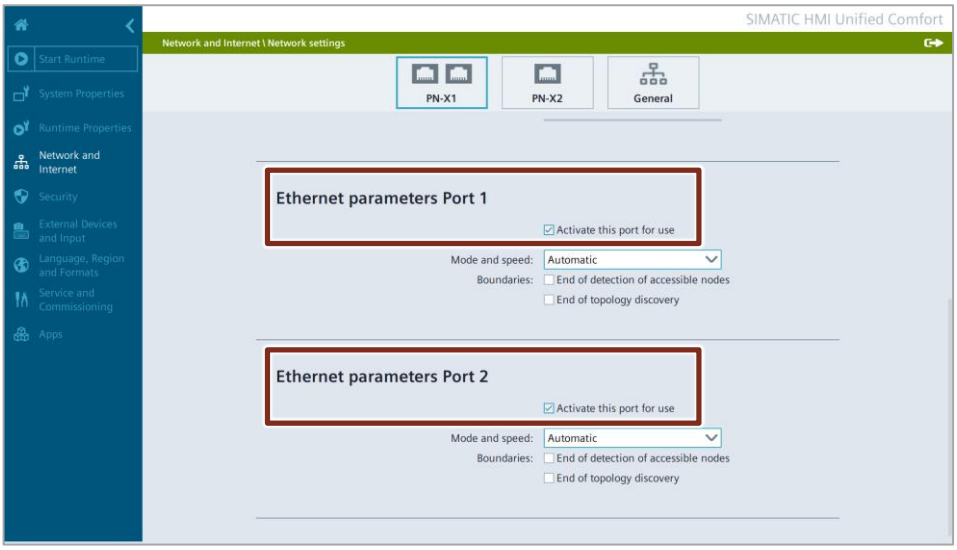
Figure 4-2



Disable network interfaces in the Control Panel

If a port still has to be enabled, you have the ability to enable/disable the individual ports of the X1 and X2 network interface with the Control Panel menu "Network and Internet > Network Settings". In this case, however, the user requires the right to operate the Control Panel.

Figure 4-3

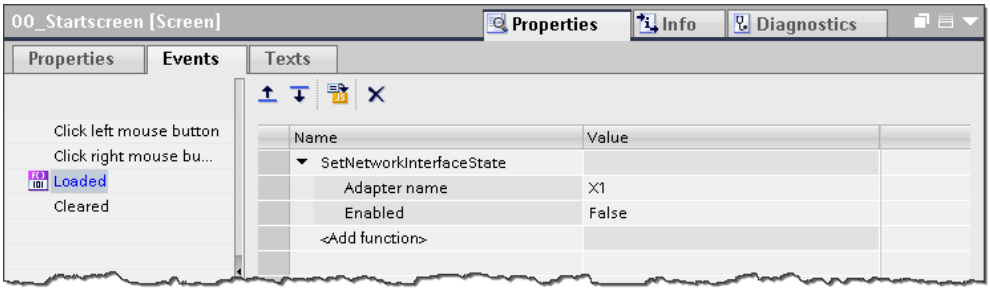


Disable network interfaces in the runtime

If the operator does not have Control Panel access, but still have permission to enable/disable network adapters, you can control the status of the network adapter from the runtime.

For this purpose, you have access to the system function "SetNetworkInterfaceState" in TIA Portal with a Unified Comfort Panel.

Figure 4-4



Note For more information on the "SetNetworkInterfaceState" system function, refer to the system manual "WinCC Unified V16 – Runtime Unified" in the chapter "SetNetworkInterfaceState".

https://support.industry.siemens.com/cs/ww/en/view/109773780/123775992459

Physical safeguards

As an additional safeguard, you can restrict access with architectural measures, for example by installing the panel in a lockable control cabinet.

4.1.3 Update the operating system

SIMATIC HMI Unified Comfort Panels have a Linux operating system specially configured for SIEMENS.

In the process, the functionalities, drivers and interfaces of the operating system have been largely reduced to suit the intended application.

Security Updates for the operator device

There are continuous Security Updates for the SIMATIC HMI Unified Comfort Panel. These are contained in the firmware image.

It is recommended to always upgrade the image of your operator device to the latest version in order to reduce possible risks.

Note For an overview of the currently available operator device images, refer to the download "Image downloads for HMI operator panels".

https://support.industry.siemens.com/cs/ww/en/view/109746530

4.1.4 Backup and restoration of panel data

In the Panel device settings, there is the menu item "Service and Commissioning".

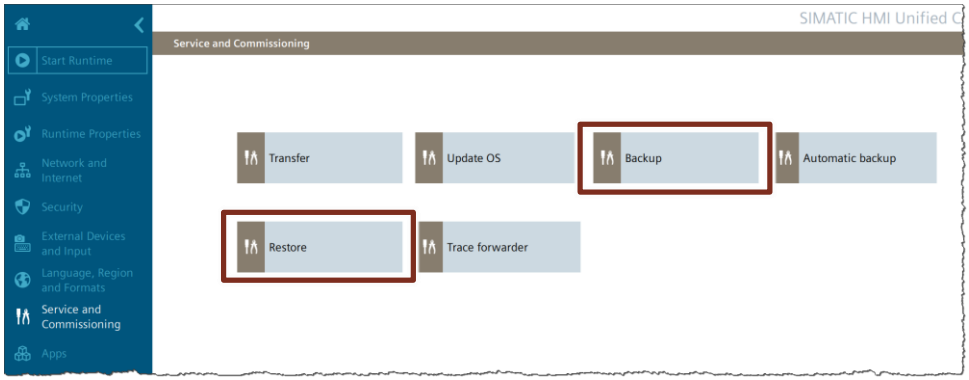
Using this function, the following backup and restore functions can be carried out:

- Backup & restore
- Update OS
- Automatic backup

Backup & restore

It is possible to perform a full backup of the panel data via the "Backup & Restore" submenu. The file cannot be edited, but it can be transferred back to another device of the same model (loss of "know how").

During the restore process, the data on the operator device will be deleted. If, whether deliberately or inadvertently, an incorrect system configuration is transferred to the panel, the system can no longer be operated via the panel in accordance with its specific function. Figure 4-5

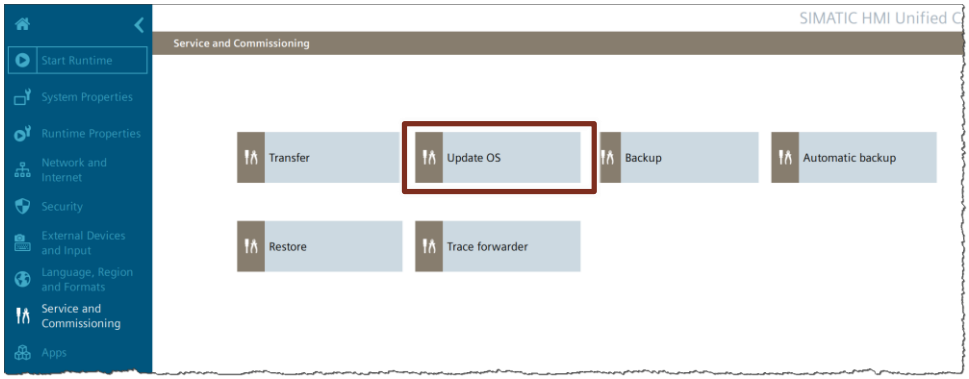


"Update OS" via storage media

Using this function, it is possible to perform an operating system update of the panel. This deletes the existing configuration. The panel then receives no more configuration data.

If the access to the storage card locations and the device settings is open to all, unauthorized persons can make changes.

Figure 4-6

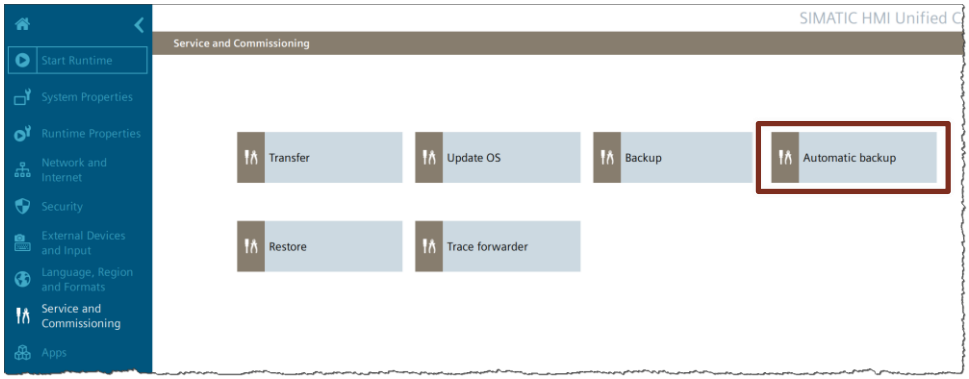


Service concept for the Comfort Panels

In an "Automatic Backup", a continuous automated backup of all process-related operator device data is made to a "SIMATIC HMI SD memory card" (system storage card).

If the access to the storage card locations is open to all and there is access to the device settings on the panel, then the function can be disabled and/or interrupted by pulling out the storage card. Furthermore, the data can be transferred to another device of the same make (loss of "know how").

Figure 4-7



So that only authorized persons may have access to the device settings, you should protect access to the Control Panel (see chapter 3.4.1).

Moreover, you can prevent access to storage media with architectural measures, for example by installing the panel in a lockable control cabinet.

4.1.5 LAN security

An increasing number of devices communicate with each other over "Ethernet". As the number of devices grows, so does the number of people who have access to the LAN.

There are also a multitude of network configurations to consider.

Some examples are:

- Ring line / redundant ring line
- Common / separated network for office and production site
- Encrypted connection, e.g. WPA2 etc.

Network security guideline

Siemens offers numerous examples and solutions on the topic of network security and network architecture. To present them here in detail would surpass the scope of this guide.

For further information, see the article "SIMATIC NET Industrial Ethernet Security Setting up security - Getting Started":

https://support.industry.siemens.com/cs/ww/en/view/109738462

Using on simple test networks, here you can learn how to work with the security modules and the "Security Configuration Tool". You will also learn how to implement the security functions of security modules in the network, without significant configuration effort.

4.2 SIMATIC WinCC Unified PC Runtime (specific)

In this chapter you will find links to documents for further reading which provide general information on the security settings of IPC and PC stations. You will also find the recommended settings for:

- User accounts
- Firewalls and virus scanners
- Access restrictions on Windows and Linux functions (e.g. prohibit access to system settings)

Windows operating system

If you have deployed an IPC with a Windows operating system, then you can find detailed information on the required settings in the application example "Recommended Security Settings for IPCs in the Industrial Environment":

https://support.industry.siemens.com/cs/ww/en/view/109475014

Linux operating system

For Linux operating systems, the application example "SIMATIC IPC - Security Guidelines for Linux systems" contains detailed information on which settings must be made:

https://support.industry.siemens.com/cs/ww/en/view/109768383

5 Risk analysis when using services and apps

Background information

While using various services for remote maintenance offers many advantages, it also carries risks which must be taken into account.

5.1 Openness to other applications

5.1.1 Engineering Openness

TIA Portal Openness describes open interfaces for engineering with TIA Portal. This allows you to control the engineering in TIA Portal externally, via a program that you create. You can thereby perform the following actions:

- Write project data
- Modify projects and project data
- Share projects and project data with other applications

Note More information can be found in the system manual "SIMATIC TIA Portal Openness: Automating creation of projects":

https://support.industry.siemens.com/cs/ww/en/view/109773802

With this in mind, there are security risks which must be considered, because otherwise data from your engineering project may be read or modified.

User group

In order for a user to use the TIA Portal Openness function, the user must belong to the Windows user group "Siemens TIA Openness".

For security reasons, make sure that only authorized users belong to the user group "Siemens TIA Openness".

Note Make sure that users cannot add themselves to the user group. One way to do this is to limit access to Windows functions (see chapter 4.2).

Openness Firewall

In addition, the initial Openness connection to TIA Portal will show a prompt where you can allow or deny access.

Simply confirm the connection with "Yes", because the prompt will appear if you make another connection, and the authorization will not be saved.

Note More information can be found in the system manual "SIMATIC TIA Portal Openness: Automating creation of projects" in the chapter entitled "TIA Portal Openness Firewall":

https://support.industry.siemens.com/cs/ww/en/view/109773802/117605127179

5.1.2 Runtime Openness (ODK)

As another option, Runtime Openness (ODK) offers a runtime API which describes the open programming interface of the WinCC Unified runtime. This allows you to access selected data from the runtime and modify them (e.g. in the case of tags or messages).

As a result, Runtime Openness allows data to be stolen or manipulated. On the security front, this is a major risk and must be accounted for accordingly.

User group

For Runtime Openness (ODK) to be used, the user must belong to the Windows user group "Siemens HMI". Make sure that only authorized users from belong to the "Siemens HMI" user group, so as to hinder manipulation of the runtime data.

Note

For further information, refer to the system manual "SIMATIC WinCC Engineering V16 - Runtime Unified" in the chapter entitled "Runtime API":

https://support.industry.siemens.com/cs/de/en/view/109773780/129370904843

and in the application example "Creation of ODK applications for WinCC Unified Runtime":

https://support.industry.siemens.com/cs/ww/en/view/109781803

5.1.3 Open Pipe

With Open Pipe, WinCC Unified makes it possible to connect a customer application to WinCC Unified Runtime. In comparison to Openness RT (ODK), Open Pipe provides a limited number of functions.

The connection code can be composed in any programming language that supports the pipe technology. Even batch access to the pipe is possible.

Security assessment

The Open Pipe functionality itself can only be used locally. Forwarding of data must be carried out by another application, so security measures are implemented on the side of the other application.

Make sure that you do not store any files of unknown origin on your operator device or PC system.

Note

You can find additional information in the operating manual "SIMATIC HMI WinCC Unified Open Pipe".

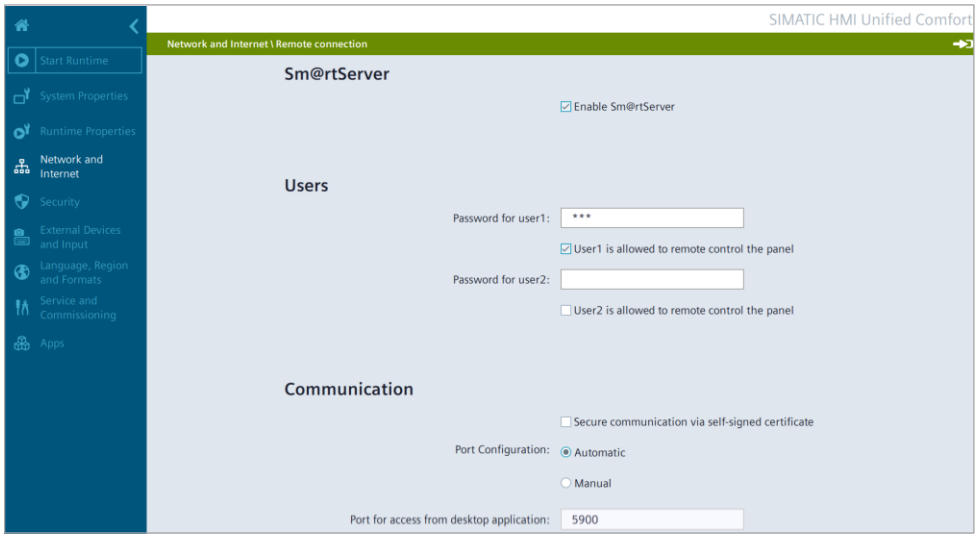
https://support.industry.siemens.com/cs/ww/en/view/109778823

5.2 SIMATIC HMI Unified Comfort Panel (specific)

5.2.1 Use of Sm@rt Service

Sm@rt Service gives you the ability to operate your Unified Comfort Panel via remote access.

Figure 5-1



Only enable Sm@rt Service if necessary

If you need Sm@rt Service for your facility's production operation, proceed with great caution. WinCC Unified V16 does not yet support an encrypted connection to the Sm@rt Server.

It is recommended to disable Sm@rt Service by default and only enable it when needed. One way to do this is with the Control Panel in the menu "Network and Internet > Remote Connection", or in the runtime with the system function "SetSmartServerState".

Note The Sm@rt Service service on the Unified Comfort Panel in connection with the Sm@rt Client App for mobile end-user devices is not yet supported with WinCC Unified V16.

Network security

If the application requires the "Sm@rt Service" service to be permanently enabled, then you should take additional security precautions on the network side.

Further information on this topic can be found in the manual "SIMATIC NET Industrial Ethernet Security Setting up security - Getting Started".

https://support.industry.siemens.com/cs/ww/en/view/109477612

5.2.2 SIMATIC ProSave

You can perform a variety of functions with the SIMATIC ProSave software. They include:

- Creating backups
- Restoring from panel images (restore function)
- OS update

So that unauthorized persons cannot use "SIMATIC ProSave" to download or otherwise manipulate project data, the following measures are recommended.

Protect connection parameters

The IP address of the panel must be specified in the connection parameters, for instance. If it is unknown, then a connection cannot be established to the panel. Therefore, make sure that the device settings cannot be retrieved in order to change the Ethernet settings (see chapter 3.4.1).

Restrict access to SIMATIC ProSave

Only allow authorized users to start the SIMATIC ProSave application. You can implement this, for example, with an access restriction in Windows (see chapter 4.2).

5.2.3 Uninstall unneeded apps

The Unified Comfort Panel provides a number of apps by default. There is the possibility that a Word file, for example, discreetly runs a script and causes damage.

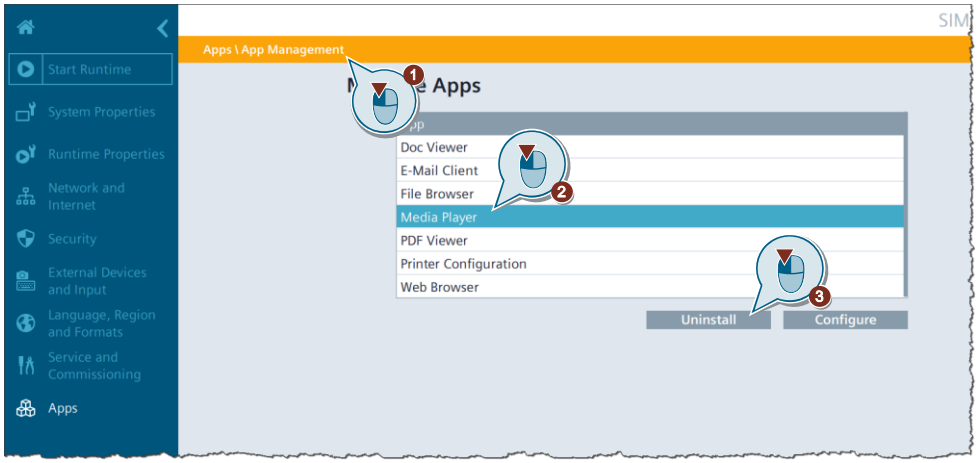
Uninstalling apps

In order to reduce the risk, you should uninstall all unneeded apps from your Unified Comfort Panel.

Proceed as follows:

1. In the Control Panel, open the menu "Apps > App Management" (1).
2. Then select the app that you wish to uninstall (2).
3. Then click "Uninstall" (3).

Figure 5-2

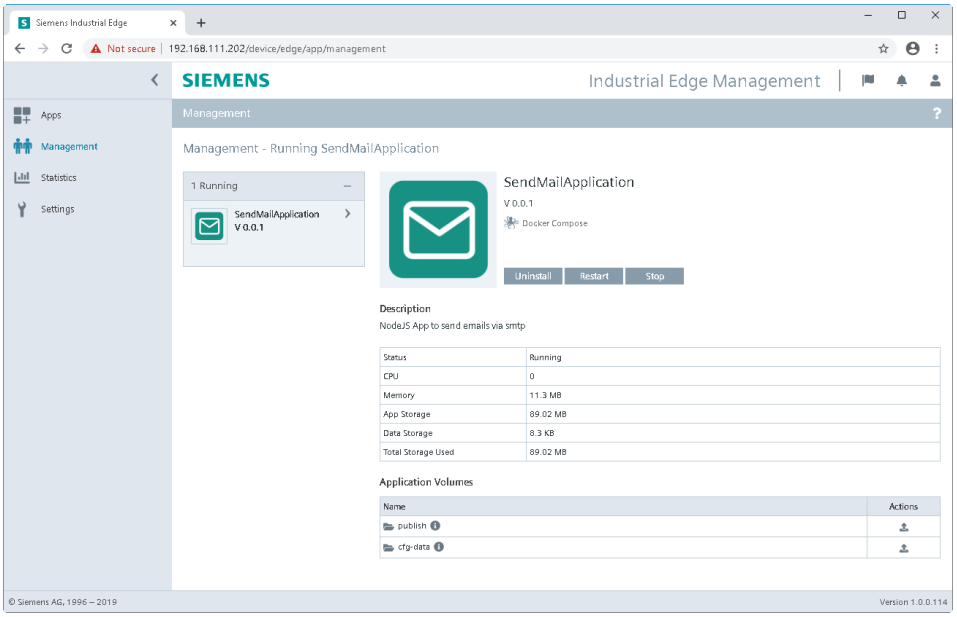


5.2.4 SIMATIC Edge

The Unified Comfort Panel is at the same time a SIMATIC Edge device. This means that you can create your own Edge apps and transfer them to the operator device.

Using these Edge apps, you can significantly extend the functionality of the operator device, for instance with open source software.

Figure 5-3



The functional expansion with SIMATIC Edge apps also entails security risks, however, which must be borne in mind.

There are essentially three approaches to reducing this risk:

- Only enable SIMATIC Edge where needed
- Use user roles in TIA Portal
- Edge apps from trusted sources

Enabling only where needed

Leave the "SIMATIC Edge" function disabled by default. Enable the function in the Control Panel of your Unified Comfort Panel only in cases where you need it.

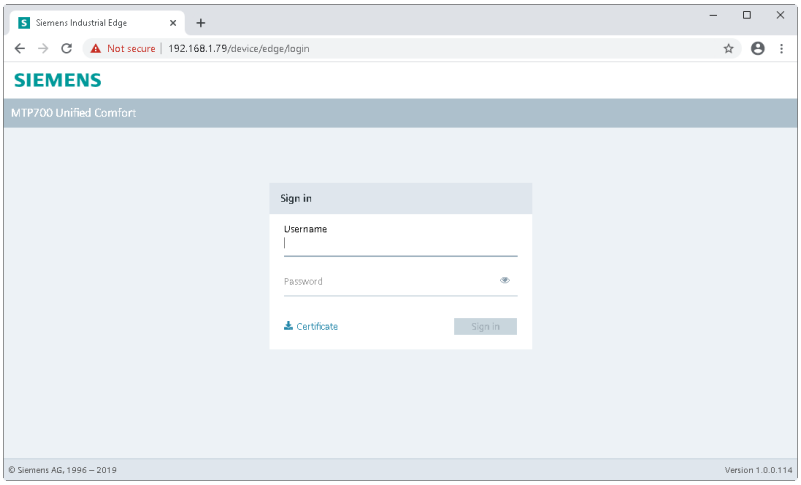
Figure 5-4

Assign user permission

In order for a user to log in to Edge Management, he or she needs the role of "HMI Administrator" in the TIA Portal User Administration (see chapter 2.6).

Accordingly, make sure in step 2 that when assigning the role, only authorized users receive the role "HMI Administrator".

Figure 5-5



Edge apps from trusted sources

Only install SIMATIC Edge apps from trustworthy sources.

Regularly check for available updates to the already installed apps, and always install the latest version. Most updates also close security holes.

5.3 SIMATIC WinCC Unified PC Runtime (specific)

5.3.1 Access to automation systems with mobile end devices

Mobile end-user devices such as smartphones or tablets can also access the WinCC Unified runtime via a browser (like Chrome or Safari) if you are connected to the network.

To similarly protect these networks from manipulation or unauthorized access, security considerations are required on three separate levels.

1. Security of smartphones and tablets, including apps
   (Protection against unauthorized access events and loss/theft of the saved data → see following heading "Security of smartphones and tablets including apps")
2. Security of communication
   (Protection against changes and unauthorized network access by eavesdropping of communication → see chapter 2.9)
3. Security of the automation solution
   (Protection against unauthorized access and reduced availability due to loss of confidential information → see entire document)

Note

The use of smart devices in the automation environment requires its own analysis in the security management process.

Additional information is available at the following link:

http://www.siemens.com/industrialsecurity

Security of smartphones and tablets, including apps

The use of smart devices carries many dangers, e.g. due to loss, theft or unauthorized access. In some cases, unauthorized persons can gain access to the system and misappropriate knowledge of the system.

In order to safeguard your smartphone against unauthorized operation in case it is lost or stolen, consider the following points:

- Use a PIN or password to unlock your smartphone. Don't use gestures or a simple swipe to unlock the device.
- Enable encryption on the storage (SD card, internal storage). Configure a VPN profile if needed.

A smartphone still faces danger from external attack. Reduce the risk in the following ways:

- Use antivirus software to guard against malware and reduce risks.
- Do not use alternative keyboard, as they can theoretically read everything you type and send it to third parties.
- Only use apps from trustworthy sources, so as to reduce the risk of attacks from dubious applications.
- "Jailbreaks" and "rooting" represent a security risk. Do not employ such devices in your automation system.

5.3.2 Note the ports in use

The assignment of TCP and UDP ports is set by the IANA (Internet Assigned Numbers Authority). When using a firewall, the ports listed in the tables must be opened.

When opening ports, make sure that doing so does not open any security holes.

Remedy

Only open ports that you absolutely need. Limit access, for example by defining user groups.

You can find a listing of the ports in the Readme file of Update 2 to WinCC Unified PC Runtime.

https://support.industry.siemens.com/cs/ww/en/view/109773716

5.3.3 Script debugger in the "Chrome" browser

You can use Chrome's script debugger to debug your scripts inside of the runtime.

Make sure that you do not use this in production operations, because doing so opens an additional port (default port: 9222).

Note More information on the script debugger can be found in the FAQ "How do you use the Script Debugger with WinCC Unified and the Chrome browser?"

https://support.industry.siemens.com/cs/ww/en/view/109779192

6 Additional information

This chapter provides further information and links on the topic of industrial security.

Recommendations from the German Federal Information Security Agency (BSI)

The website of the German Federal Information Security Agency provides general recommendations as well as recommendations for operating entities, manufacturers and system integrators on IT security in the fields of factory automation and process control.

You can find more information at the following link:

https://www.bsi.bund.de/EN/Topics/Industry_CI/ICS/Download/download_node.html

Known security threats with Siemens products

The "Siemens ProductCERT and Siemens CERT" website gives an overview of all known security threats with respect to Siemens products, solutions, services or the Siemens IT infrastructure.

You can find more information at the following link:

https://new.siemens.com/global/en/products/services/cert.html

Additional sources

For more information on the topic of industrial security, please visit:

- Whitepaper (German language) "Protection of industrial controllers" https://assets.new.siemens.com/siemens/assets/api/uuid:2b57b21f-c87f-4dec-8368-90333cedd18e/whitepaper_securityen082018web.pdf
- "Operational Guidelines for Industrial Security" (English) https://cert-portal.siemens.com/operational-guidelines-industrial-security.pdf

7 Appendix

7.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts.

Please send queries to Technical Support via Web form:

support.industry.siemens.com/cs/my/src

SITRAIN – Digital Industry Academy

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

support.industry.siemens.com/cs/ww/en/sc/2067

7.2 Industry Mall

The Siemens Industry Mall is the platform on which the entire siemens Industry product portfolio is accessible. From the selection of products to the order and the delivery tracking, the Industry Mall enables the complete purchasing processing – directly and independently of time and location:
mall.industry.siemens.com

7.3 Links and literature

Table 7-1

No.	Subject
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/109481300
\3\	Operational Guidelines for Industrial Security https://assets.new.siemens.com/siemens/assets/api/uuid:c9a2de6e-6bd0-4c32-bba0-f64cac44fcc9/industrial-security-operational-guidelines-en.pdf
\4\	Application example "Setting up a secure VPN connection between SINEMA Remote Connect Client, SCALANCE S615 and SINEMA Remote Connect Server" https://support.industry.siemens.com/cs/ww/en/view/109479599
\5\	System manual " SIMATIC WinCC Engineering V16 - Runtime Unified" https://support.industry.siemens.com/cs/ww/en/view/109773780
\6\	Getting started "SIMATIC NET Industrial Ethernet Security Setting up security - Getting Started" https://support.industry.siemens.com/cs/ww/en/view/109738462
\7\	FAQ "How do SIMATIC and SITOP products support communication via OPC UA?" https://support.industry.siemens.com/cs/ww/en/view/109763315
\8\	FAQ "Error during loading - Contact Siemens Customer Support" https://support.industry.siemens.com/cs/ww/en/view/109775493
\9\	Operating Manual "SIMATIC WinCC Unified Certificate Manager" https://support.industry.siemens.com/cs/ww/en/view/109779117/134276049675
\10\	FAQ "How do you operate WinCC Unified in the Windows 10 full-screen mode/kiosk mode?" https://support.industry.siemens.com/cs/ww/en/view/109771719
\11\	Application example "Recommended security settings for IPCs in industrial environments" https://support.industry.siemens.com/cs/ww/en/view/109475014
\12\	Linux operating system "SIMATIC IPC - Security Guidelines for Linux systems" https://support.industry.siemens.com/cs/ww/en/view/109768383

7.4 Change documentation

Table 7-2

Version	Date	Change
V1.0	11/2020	First edition