Security Guidelines for SIMATIC HMI Operator Panels

HMI Operator Panels / WinCC (TIA Portal) V15

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

Siemens Industry Online Support

Warranty and Liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are correctly used. These Application Examples do not relieve you of the responsibility of safely and professionally using, installing, operating and servicing equipment. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time and without prior notice. If there are any deviations between the recommendations provided in this Application Example and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document.
Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). However, claims arising from a breach of a condition which goes to the root of the contract shall be limited to the foreseeable damage which is intrinsic to the contract, unless caused by intent or gross negligence or based on mandatory liability for injury of life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.
It is not permissible to transfer or copy these Application Examples or excerpts of them without first having prior authorization from Siemens AG in writing.

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 http://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 http://www.siemens.com/industrialsecurity.

Table of Contents

1 Industrial Security

1.1 Strategies to increase security

This document aims to raise awareness of "security aspects of SIMATIC HMI operator panels".

The main priority in automation is to maintain control over production and process. Even actions intended to prevent a security threat from spreading must not affect control over production and process.

This document describes possible critical points and how to specifically minimize them.

The description enables you to take appropriate measures to increase security.

1.2 Document structure

General

The document takes a closer look at the security aspects of the following topics. It describes the different stages from initial configuration to commissioning.

- In the preliminary stages:
  Minimizing/preventing tampering during the configuration
- During operation: Device settings on the panel
  Preventing access to the device settings
- During operation: Use of HMI Runtime
  Plant operation by authorized personnel only
- During operation: Remote access / maintenance
  Suitable preventive action to prevent unwanted remote access
- General: Hardware
  External constructional measures to avoid tampering on the panel

Note

This document covers the security aspects across different device classes. Therefore, some sections may be more relevant to you than others.
You do not have to consider all the details described in the chapters. Only functions you actually use may require action.

1.3 The three major steps

Three simple steps to reduce a majority of potential hazards

Chapters 3 through 6 provide a detailed description of individual potential hazards. In a nutshell, most potential hazards can be reduced to a minimum if the following three aspects are observed.

Make sure to provide multiple protective measures. This ensures security even if you forgot to provide a protective measure or if a measure proves insufficient.

1.3.1 Panel access protection

Assign a password to protect access to the panel's device settings. Without a valid password, the device settings cannot be opened from the "Start Center".

For detailed information, please refer to Chapter 4.2, "Start Center" start menu / "Loader menu".

1.3.2 User administration

Create a user administration feature that governs each panel operation by means of an authorization.

In the object properties, select "Properties > Security" and assign an authorization to the object.

For detailed information, please refer to Chapter 4.1, "Using the configured plant screens".

1.3.3 Storing data on a network drive

Use a "network drive" as the file path for recipes and archives.

A network drive provides wider access protection options than a connected storage device (memory card / USB flash drive).

Chapter 3.4, "Archiving tags and alarms", provides detailed information about what needs to be observed when using a "network drive".

1.4 Secure names and passwords

General information on secure names and passwords

A lot of devices feature integrated access mechanisms to prevent unauthorized persons from accessing device settings, for example.

To this end, many manufacturers often use the following settings:

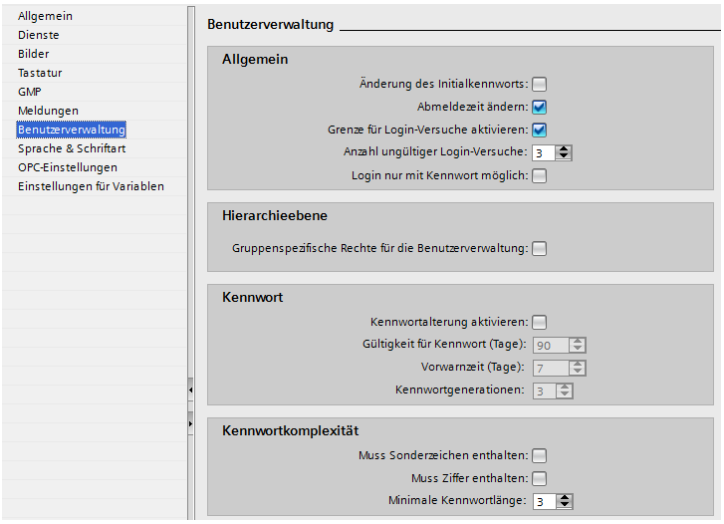
- User name => Admin (administrator)
- Password => 100

What you should do

Change or check any default "user and password data" before commissioning.

In WinCC (TIA Portal), use the possible settings in user administration. Examples of these settings are "Password aging" and "Password complexity" (Figure 1-1).

Figure 1-1



Note Default passwords have not been used since WinCC V13 SP1 (TIA Portal). When commissioning, e.g., the web server, you must first enter a password.

What should a password look like?

A password should

- be at least eight characters long.
- contain upper and lower case letters, special characters (,-) and numbers.
- not be a word listed in a dictionary.
- not consist of a string of adjacent characters on the keyboard (e.g., 123456 or asdfg).
- not contain the same character repeated several times (e.g., AAAA).

1.5 Operational security guideline

1.5.1 Protection of machines and plants

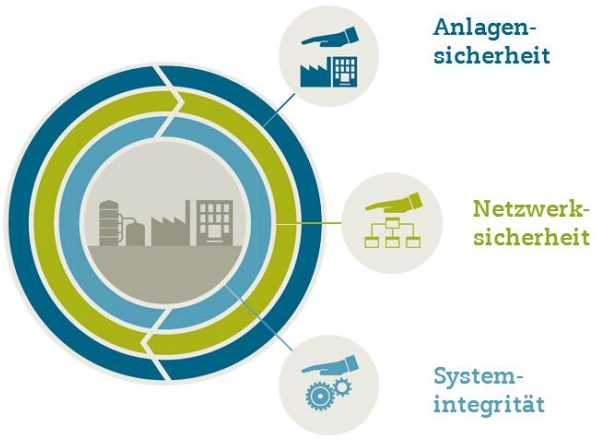
The crucial question is this: How can we significantly minimize potential hazards and achieve sufficient and affordable security in industrial automation?

Unfortunately, there is no universally applicable solution. In general, however, a single security measure alone will always be insufficient.

Using a defense-in-depth approach, an automation system can be protected comprehensively and reliably. It is based on the international standards series IEC 62443, "Industrial communication networks – Network and system security".

The defense-in-depth concept includes the three components listed in Figure 1-2.

Figure 1-2



Plant security
Secure physical access for persons to critical components by consistently using security mechanisms in automation.

- Fenced building/factory premises with access control.
- Biometric access control or locks for rooms (laboratories, server rooms).
- Alarm systems or video surveillance.

Network security
Industrial communication is key to corporate success – provided that the network is protected.

The first step of network segmentation is to **strictly** separate production networks and other corporate networks.

- Controlled interfaces between office and plant network, e.g., using firewalls.
- Further segmentation of the plant network (individually protected automation cells).

System integrity
Protecting system integrity through internal protection functions. Antivirus and whitelisting software

- Maintenance and update processes
- User authentication for plant or machine operators
- Access protection mechanisms built into automation components

Note If a measure cannot be implemented, an alternative countermeasure should be taken to minimize the risk.

For detailed information, read the document at the following link:
http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf

What is the customer benefit?

The defense-in-depth concept initially requires increased project planning efforts. In the long term, however, these extra efforts pay off through:

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

Note Security is also a key part of WinCC (TIA Portal).

1.5.2 Panel operating system

Basic Panels

SIMATIC HMI Basic Panels have an operating system configured and created by Siemens.

Comfort Panels

SIMATIC HMI Comfort Panels have a "WinCE Embedded" operating system configured specifically for SIEMENS.

The functionalities and interfaces of the operating system were largely reduced to the intended use (SMB protocol or registry access, autostart functions, for example, are not included).

1.5.3 Security management

Organizational measures and the introduction of security processes are essential to plant security.

Organizational measures must be closely linked to technical measures and are mutually dependent. Most protection goals can only be achieved by combining the two types of measures.

A security management process is essential to a sophisticated security concept (Figure 1-3).

Security management process

Figure 1-3

The risk analysis results in protection goals that are the basis for concrete, organizational and technical measures.
Once implemented, the measures must be reviewed from time to time.

Brief description of the "security management process"

1. Risk analysis
   Risk analysis with definition of risk reduction measures
2. Guidelines and organizational measures
   Defining guidelines and coordinating organizational measures
3. Technical measures
   Coordinating technical measures
4. Validation and improvement
   Regular/event-based repetition of the risk analysis

Note The security management process must also account for smart devices and apps.

For more information about industrial security, please visit
http://www.siemens.com/industrialsecurity

2 Complete Overview of the Device Functions

This document describes security strategies that do not necessarily apply to all HMI operator panels.

The table specifies which function applies to which device.

Detailed information about the security strategy is given in the individual chapters.

The KP8, KP8F and KP32F operator panels are not described in greater detail in this document as they are parameterized in STEP 7. The operator panel is connected to a SIMATIC controller via PROFINET.

Legend: ✔ = Applies to this device
-- = Function is not supported

Complete overview

Table 2-1

Validity	Basic Panel	2-nd generation Basic Panel	Comfort Panel	2-nd generation Mobile Panel	Mobile Panel 277(F) iWLAN	Runtime Advanced	OP 73, OP 77A, TP 177A	Mobile Panel 177	TP/OP 177B, MP 177	TP/OP 277, MP 277	Mobile Panel 277	MP 377
3 Risk Assessment when Creating and Editing HMI Projects												
3.1 Opening and editing the configuration	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
3.2 Simulating	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
3.3 Transferring the configuration to the panel	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
3.4 Signed images	--	✔	✔	✔	✔	✔	--	--	--	✔	✔	✔
3.5 User administration	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
3.6 Data exchange between HMI operator panel and controller	--	--	✔	✔	--	✔	--	--	--	--	--	--
3.7 Archiving tags and alarms	--	✔	✔	✔	✔	✔	--	--	--	✔	✔	✔
3.8 Working with recipes	✔	✔	✔	✔	✔	✔	✔[1]	✔	✔	✔	✔	✔
3.9 Locking task switching	--	--	✔	✔	✔	✔	--	✔	✔	✔	✔	✔
3.10 Project transfer	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
3.11 Tag access via OPC UA	--	--	✔	✔	--	✔	--	--	--	--	--	--

[1] Except OP73

Validity	Basic Panel	2-nd generation Basic Panel	Comfort Panel	2-nd generation Mobile Panel	Mobile Panel 277(F) iWLAN	Runtime Advanced	OP 73, OP 77A, TP 177A	Mobile Panel 177	TP/OP 177B, MP 177	TP/OP 277, MP 277	Mobile Panel 277	MP 377
3.12 Data exchange between operator panels	--	--	✔	✔	✔	✔	--	✔[2]	✔[2]	✔	✔	✔
3.13 Remote access to the tags of a panel using Excel	--	--	✔	✔	✔	✔	--	✔[2]	✔[2]	✔	✔	✔
3.14 Sending email notifications via the panel	--	--	✔	✔	✔	✔	--	✔[2]	✔[2]	✔	✔	✔
3.15 TIA Portal Multiuser Engineering	✔[3]	✔[3]	✔[3]	✔[3]	✔[3]	✔[3]	--	✔[3]	--	--	✔[3]	--
3.16 TIA Portal Cloud Connector	✔[3]	✔[3]	✔[3]	✔[3]	✔[3]	✔[3]	--	✔[3]	--	--	✔[3]	--
3.17 User Management Component (UMC)	✔[3]	✔[3]	✔[3]	✔[3]	✔[3]	✔[3]	--	✔[3]	--	--	✔[3]	--
3.18 RFID user management	--	--	✔	✔	✔	✔	--	--	--	--	--	--
4 Risk Assessment when Using the Panel												
4.1 Using the configured plant screens	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
4.2 "Start Center" start menu / "Loader menu"	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
4.3 Stopping HMI Runtime	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
4.4 Creating and transferring a Pack&Go file	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
4.5 Backing up and restoring panel data	✔	✔	✔	✔	✔	--	✔	✔	✔	✔	✔	✔
4.6 SIMATIC HMI Option+ V1	--	--	✔	--	--	--	--	--	--	--	--	--
4.7 SIMATIC HMI Option+ V2	--	--	✔	--	--	--	--	--	--	--	--	--
5 Risk Assessment when Using Remote Maintenance Services												
5.2 Using the Sm@rt options	--	✔[4]	✔	✔	✔	✔	--	✔[5]	✔	✔	✔	✔
5.3 SIMATIC apps	--	--	✔	--	--	✔	--	--	--	--	--	--
5.4 ProSave	✔	✔	✔	✔	✔	--	✔	✔	✔	✔	✔	✔
5.5 Ports used by operator panels	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
6 Risk Assessment of the Hardware Used												
6.1 External storage media	--	✔	✔	✔	✔	✔	--	--	--	✔	✔	✔

[2] Only devices with PROFINET interface
[3] Access via the engineering system
[4] WinCC V14 or higher
[5] No devices with PROFIBUS interface

Validity	Basic Panel	2-nd generation Basic Panel	Comfort Panel	2-nd generation Mobile Panel	Mobile Panel 277(F) iWLAN	Runtime Advanced	OP 73, OP 77A, TP 177A	Mobile Panel 177	TP/OP 177B, MP 177	TP/OP 277, MP 277	Mobile Panel 277	MP 377
6.2 Device communication interfaces	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
6.3 WLAN / LAN security	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Note

WinCC V15 or higher no longer supports the following devices.
OP 73, OP 77A, TP 177A, TP/OP 177B, TP/OP 277, MP 177, MP277, MP377.

For more information, please refer to the following entry:
https://support.industry.siemens.com/cs/ww/en/view/109753803,
section "Changed device support".

3 Risk Assessment when Creating and Editing HMI Projects

Protective measures for backup and configuration

The chapter describes how to handle projects and individual functions intended to increase plant security.

3.1 Opening and editing the configuration

3.1.1 WinCC (TIA Portal) V14 SP1 or lower

By default, an HMI configuration can be opened and edited by any person who has the suitable software program. It is impossible to prove which person last edited the file.

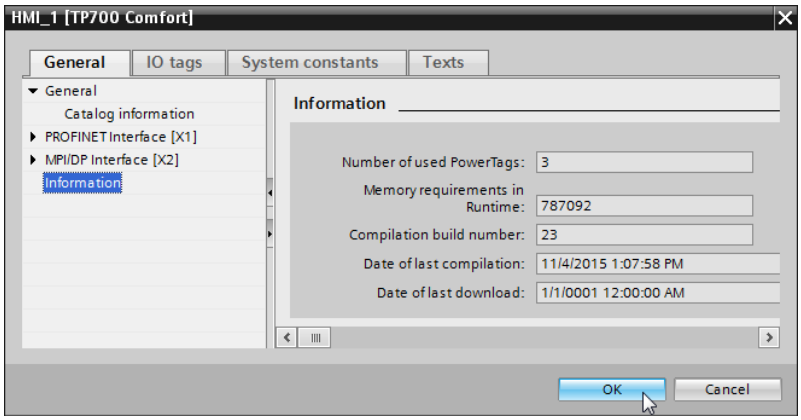
Remedy

After completing the project or commissioning, we recommend noting down the version number, the last generation date and the last saved date.

Procedure:

- In the project tree, right-click the project name of the HMI operator panel and open the "Properties".
- Select the "General > Information" menu command.
- The "Information" (Figure 3-1) menu allows you to view the version number and the project's date of last compilation.

Figure 3-1



Save and archive your projects on a secure drive with restricted access. Create a configuration .ZIP file and password-protect it.

Go to detailed device overview: →

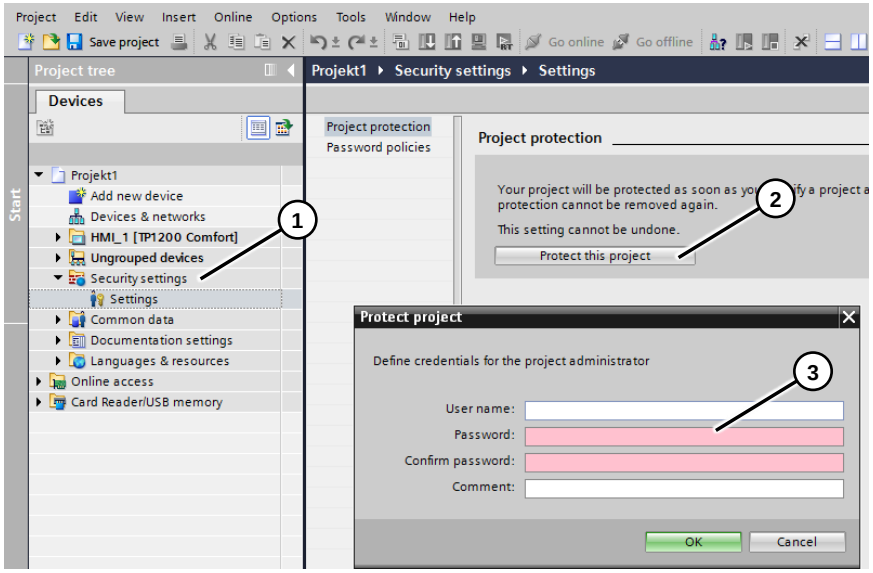
3.1.2 WinCC (TIA Portal) V15 or higher

WinCC (TIA Portal) V15 or higher allows you to password-protect opening the configuration.

In the project tree, select the "Security settings" (1). Clicking the "Protect this project" button (2) opens a dialog where you can enter the password (3).

Note This function cannot be undone.

Figure 3-2



Go to detailed device overview: →

3.2 Simulating and testing the configuration

When the configuration is open, any user can start the simulation. If there is an active connection to the configured PLC, the machine can be operated using this connection, which can cause dangerous operating states.

Remedy

Lock operation from the PC/laptop if it is out of your line of sight. This is particularly important during commissioning. Never leave the PC/laptop unattended.

Go to detailed device overview: →

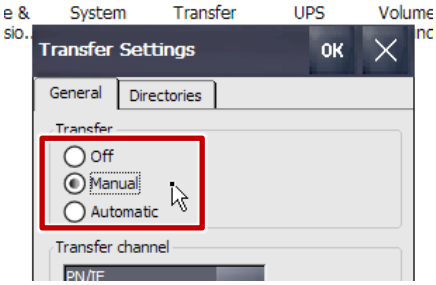
3.3 Transferring the configuration to the panel

Any user can transfer the configuration to the panel. If plant parts are already in operation, this requires an increased level of attention. If the wrong operator panel is used to download the project, this can cause the operator panel's runtime to automatically stop and the plant part can no longer be operated.

Remedy

Prevent the panel runtime from stopping automatically when, for example, a project download is triggered. To do this, open the panel device settings. Click "Transfer > General" and select the "Manual" or "Off" radio button (Figure 3-3).
Select "Off" if you do not expect the configuration to be modified any further (completion of commissioning).

Figure 3-3



Go to detailed device overview: →

3.4 Signed images

The image file of an HMI operator panel (operating system) depends on the version and is installed on the configuration PC together with the WinCC (TIA Portal) engineering software.

This involves the risk of unknown software being transferred to the HMI operator panel without being noticed due to manipulation of the image file.

Remedy

WinCC V14 or higher provides the image file with a signature. Before downloading a project, the HMI operator panel checks the image signature. If it does not match, the download will be aborted. Checking the image file can be disabled, if necessary. For details, please refer to the appropriate manual (2nd-generation Basic Panels / Comfort Panels).

If an error message appears when downloading a WinCC V13 project to a Basic Panel (that has a SIMATIC WinCC V14 image), please refer to the following FAQ (see \15\).

Go to detailed device overview: →

3.5 User administration

User administration is a particularly sensitive area. If, for example, the "administrator password" is known and a user view has been configured, the user data can be modified online.

Remedy

Use the comprehensive setting options provided by the "Runtime settings > User administration" menu item. It provides options such as

- Change initial password
- Password aging
- Name must include special characters etc.

The following special characters are allowed for passwords:

- + . , / * : \ " ? _ ( ) = ^ ! € % ~ § ' { } [ ] < > # $; & | @

Go to detailed device overview: →

3.6 Data exchange between HMI operator panel and controller

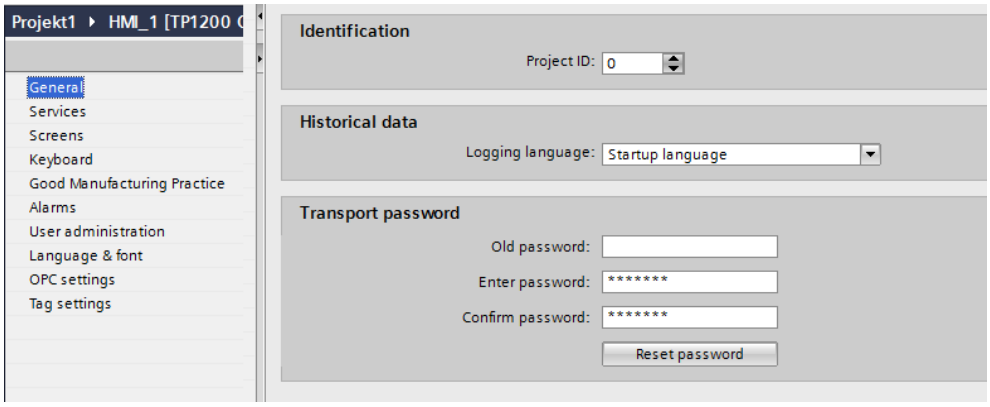
Connecting the devices via Ethernet/PROFINET involves the risk of values being read and maybe even manipulated from the outside.

Remedy

To encrypt data exchange between a SIMATIC S7-1200 or S7-1500, WinCC V14 or higher allows you to specify a password for data exchange.

To do this, go to the project tree and open "Runtime settings > General". The "Transport password" section allows you to specify a password.

Figure 3-4



When transferring the configuration to the operator panel, a dialog requesting the password opens once in Runtime.

Note The transport password must be identical to the "access password" specified in the connection settings and have the "access level" set in the SIMATIC controller's device configuration (Protection & Security).

Go to detailed device overview: →

3.7 Archiving tags and alarms

External storage media such as memory cards and USB flash drives are frequently used to archive tags and alarms. These storage media involve the risk of being removed in an uncontrolled manner or getting lost.

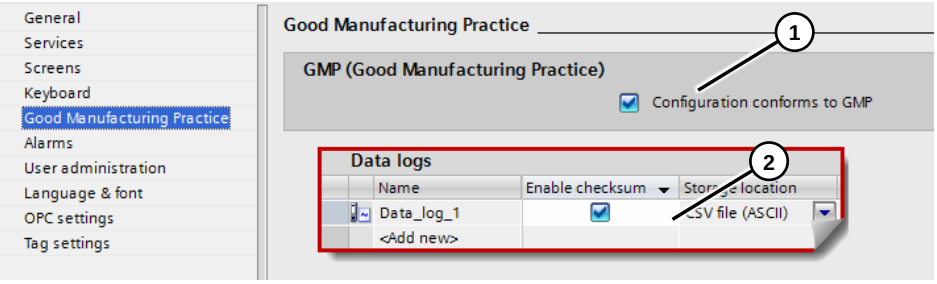
Moreover, the archived process values and alarms are often "sensitive" data used in particular to verify quality assurance. It must be ensured that this data is not tampered with or lost.

Remedy 1, "GMP"

If you are using operator panels that support the "Good Manufacturing Practice" option (1) ("GMP"), you can check the "Enable checksum" check box (2) in the data and alarm logs (Figure 3-5).
This feature allows you to subsequently check whether log data has been changed.

The "HmiCheckLogIntegrity" program allows you to check the integrity. For details on the program or "GMP", please refer to the WinCC V14 (TIA Portal) system manual (see \21\).

Figure 3-5



Note The "HmiCheckLogIntegrity.exe" program is located in the installation directory under:
"SIEMENS > Automation > WinCC Runtime Advanced".

Additional information on the "GMP" option

The "GMP" option also allows you to analyze possible operator errors.

In plant areas, it is frequently important to know:

- Who last operated the plant?
- Who last changed possible parameters?
- Why were the changes made?

The "GMP" option allows you to answer these questions.

Depending on the parameter assignment, a message box appears, e.g., when entering a value on the panel. The user must enter a comment in this message box and confirm the value change.

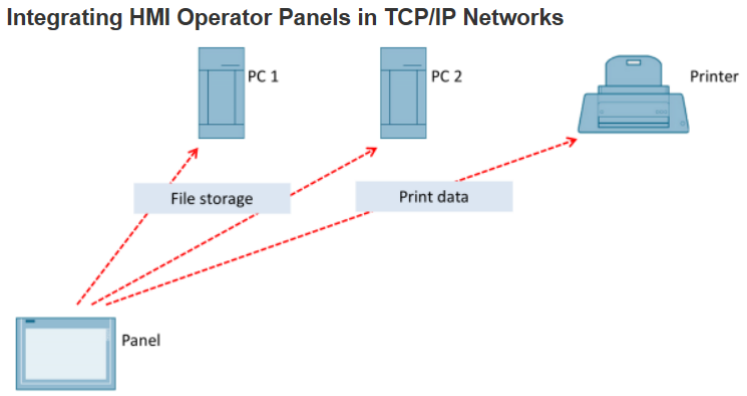
Remedy 2, "archiving to a network drive"

Instead of connected storage media, archiving to a network drive provides more extensive access protection options (Figure 3-6).

If you specify a network drive as the archiving path, you can precisely control access using a folder's properties.
In the folder properties, "Share" and "Security" allow you to define the access rights.

For information on these settings, please refer to the following entry: "Integrating HMI Operator Panels in TCP/IP Networks" (see \7\).

Figure 3-6



Notes

- Network drives should **not** be used from the office infrastructure. It is more advisable to use a demilitarized zone (DMZ). For more information, please refer to the following entry: "Protection of an Automation Cell Using the SCALANCE S602 V3 and SCALANCE S623 Security Modules via a Firewall" (see \10\).
- Interruption / failure of the connection to the file server may result in data loss. An aborted archiving process will not be restarted automatically.

Go to detailed device overview: →

3.8 Working with recipes

Recipes are frequently used in process engineering and production facilities that manufacture several different products on one station/machine.

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

- Loss of know-how through theft:
  Developing new recipes in process engineering requires many resources in terms of time and money. If such data is disclosed to a competitor, competitiveness might suffer.
- Damage caused by maloperation:
  Selecting an incorrect recipe can cause significant material damage. Moreover, it is possible to manually change individual parameters.

Remedy

Different protection mechanisms are available for recipes.

- Use of the recipe view:
  Assign an authorization for using the view. To this end, create a user administration feature. In the recipe view properties, select the "Properties > Security" menu and assign an authorization to the object.
- Storage location on a network drive:
  If you specify a network drive as the storage location, you can precisely control access using a folder's properties.
  In the folder properties, "Share" and "Security" allow you to define the access rights. For information on these settings, please refer to the following entry: "Integrating HMI Operator Panels in TCP/IP Networks" (see \7\).

Alternative to the recipe view

Use a customized recipe view instead of the default recipe view. You will find the functions for the "RecipeView" screen object under the "Keyboard operation for screen objects" system function. For more information, please refer to the following entry: "Engineering with Recipes Using Integrated Functionalities" (see \8\).

You can then assign individual authorizations to the buttons. To do this, select the "Properties > Security" menu and assign an authorization to the button.

Go to detailed device overview: →

3.9 Locking task switching

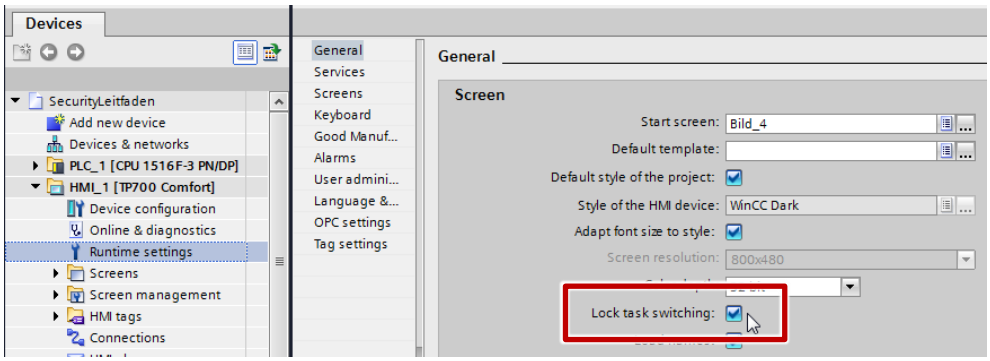
If you connect a USB keyboard to a Windows based operator panel, e.g. a Comfort Panel or PC Runtime system, you can open and edit the device settings on the panel using keyboard shortcuts. One example of this is task switching.

Remedy

Regardless of whether you are using a PC Runtime- or Windows CE-based operator panel (Comfort Panel), check the "Lock task switching" check box in the "Runtime settings" menu in the configuration (Figure 3-7).

This prevents the user from starting another program or opening the device settings / Control Panel using the keyboard.

Figure 3-7



Go to detailed device overview: →

3.10 Project transfer

An encrypted transfer of the configuration data to the panel is not possible by default. Data manipulation, however, is almost impossible as the download files cannot be subsequently edited.

Remedy

Establish a direct connection between the configuration PC and the panel. Alternatively, connect to a secure network only to prevent/minimize access from the outside.

Go to detailed device overview: →

3.11 Tag access via OPC UA

In the world of automation, there are various communication interfaces that are often vendor-specific. OPC UA is a vendor-independent standard that allows field devices to communicate with each other.

OPC UA is not enabled by default. Do not use an unencrypted connection when using this function.

Remedy

Make sure to always configure a secure connection between the client and the server for communication. Example:

- Security Policy: Basic128Rsa15
- Message Security Mode: Sign/Encrypt.

Use the "none" setting, for example, only when testing the OPC UA connection for the first time during commissioning.

For an application example with various OPC UA scenarios, please refer to the following entry: "Communication via OPC UA with SIMATIC HMI systems (Comfort Panels, Runtime Advanced, Runtime" (see \19\).

Go to detailed device overview: →

3.12 Data exchange between operator panels

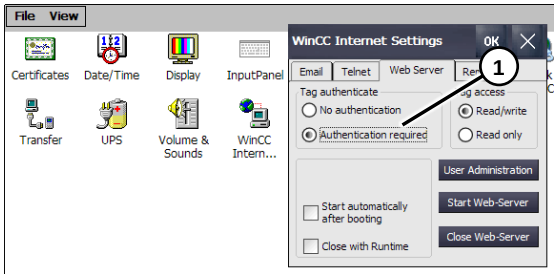
Using HTTP communication, you can exchange data between operator panels. An "overview page" is an application example that allows you to combine selected values from various operator panels (-> similar to a control desk).

Data can be transferred via http:// and https://. "http:// " involves the risk of data being modified or read if the connection is not secure, resulting in the loss of know-how (parameters of a recipe). For this reason, do not use unencrypted communication.

Remedy

Where possible, use "https://". "HTTPS" allows an encrypted connection (tap-proof communication) between the operator panels. In the HTTPS client's connection settings, you can specify how the client will verify the server certificates and respond to possible errors.
On the panel, this requires you to select the "Authentication required" radio button (1) in the device settings under the "WinCC Internet Settings" icon (Figure 3-8).

Figure 3-8



Go to detailed device overview: →

3.13 Remote access to the tags of a panel using Excel

The "Simple Object Access Protocol" (SOAP) web service allows you to access the tags of an operator panel from an external application such as Excel via Ethernet.

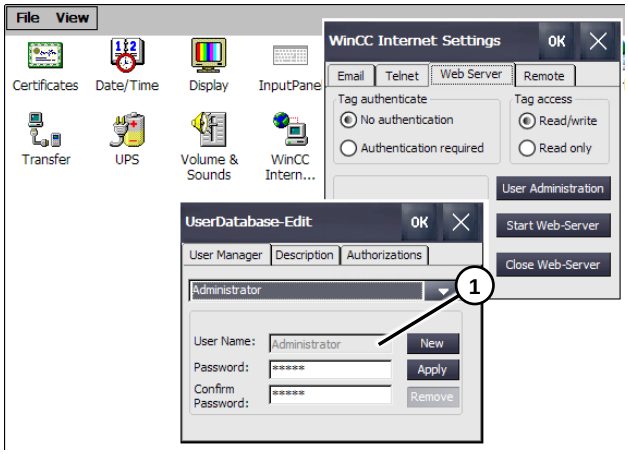
In this example, the external Excel application contains a VBA script that is used to log in to the server (Comfort Panel).

There is a risk that parameters are changed from the outside without someone noticing.

Remedy

In the device settings, the "WinCC Internet Settings" icon allows you to store the required login data (1) for the external application (Figure 3-9). As a result, the panel's tags cannot be accessed using the "Excel application" before logging in. Please note: The connection is unencrypted.

Figure 3-9



There is an FAQ on this subject: "How do you read out or write tag values with an Excel application?" (see \4\).

To give only authorized persons access to the device settings, follow the information provided in Chapter 4.2, "Protecting the Start Center against unauthorized operation".

Go to detailed device overview: →

3.14 Sending email notifications via the panel

It is not possible for all machines of a plant to be permanently monitored by staff. As a result, it is often not possible to directly respond to pending messages on the operator panel.

An email notification can remedy this problem. The notification is sent via SMTP communication.

Make sure that the email cannot be read by third parties.

Remedy

When configuring the email program, make sure to use secure encryption using "SSL" or "TLS".

For more information on this subject, please refer to the following application: "E-Mail Notification with the SIMATIC HMI Comfort Panels" (see \9\).

Go to detailed device overview: →

3.15 TIA Portal Multiuser Engineering

Multiuser Engineering in TIA Portal allows multiple users to simultaneously work on one project. Simultaneously working on different objects within a multiuser project allows you to significantly reduce the configuration times.

To use multiuser engineering, a network must already have been set up that considers Windows settings, IP addresses, firewalls etc.

In "TIA Portal Multiuser Server", you define the rights for working

- with multiuser server connections
- with multiuser projects and
- local sessions.

The rights concept is based on Windows access rights for folders and files.

For details on this subject, please refer to the following application example: "Multiuser Engineering in TIA Portal" (see \24\).

Go to detailed device overview: →

3.16 TIA Portal Cloud Connector

The TIA Portal Cloud Connector enables central management of your engineering software on a server. From an engineering workstation, you can work with TIA Portal (which is installed on a server) via a remote desktop connection. In this context, the TIA Portal Cloud Connector serves as a communication tunnel.

The TIA Portal Cloud Connector supports the secure connection via HTTPS when running Windows 8.1 or higher.

For security reasons, always use an HTTPS connection to your virtual environment. To ensure security of the HTTPS connection, the TIA Portal Cloud Connector uses certificates.

The following certificates are required to establish a connection between the user device and the remote device:

- Certificate for data encryption
- Certificate for user authentication

If a certificate does not exist or the certificates of user device and remote device do not match, a connection cannot be established.

For details on this subject, please refer to the following application example: "Working with the TIA Portal Cloud Connector" (see \25\).

Go to detailed device overview: →

3.17 User Management Component (UMC)

UMC (User Management Component) is a database for central user data management.

Global users and user groups created in UMC (User Management Component) can be added to a protected project. This enables these users and user groups to work with the project, provided that they are assigned the appropriate rights.

If a user must access multiple protected projects, you can minimize your management overhead by adding this user to each project – either individually as a global user or together with a user group. Global users can be managed in UMC; the changes then affect all the projects of these users or user groups.

You can synchronize user administration in TIA Portal with UMC to prevent inconsistencies from occurring if users or user groups were modified in UMC. The synchronization status allows you to check whether synchronization is necessary.

User Management Component:

- Central, cross-project user management in the plant.
- Managing user groups.
- Import of Windows users and user groups.
- Efficient administration of users / user groups in a plant.
- Fault tolerance through redundant design of a UMC domain.
- Load distribution of login request surges by means of several UMC stations in a UMC domain.
- Licensing by the number of users.

For details on this subject, please refer to the STEP7/WinCC "programming and operating manual" (see \26\). Alternatively, you will find more information in the WinCC (TIA Portal) Information System. Search for: "User Management Component" => "Managing global users and user groups".

You will find the installation file for UMC and the English UMC documentation on the TIA Portal installation data medium ("..\support", "...\Documents\Readme\English").

We strongly recommend reading the complete UMC documentation before using user management. This applies in particular to the sections dealing with "Secure Application Data Support (SADS)". SADS is mandatory for using user management in TIA Portal.

Go to detailed device overview: →

3.18 RFID user management

Unauthorized personnel can cause maloperation, resulting in faults in the production process. In order to prevent this, it is recommended to restrict access to certain functions of the plant so that only authorized personnel can access these functions.

SIEMENS offers two systems for automatic user login.

1. User login to HMI operator panels with RFID card reader
2. User login to HMI operator panels via RFID and the Sirius ACT ID key switch.

The **first** case implements user management using "PM-LOGON Basic" (software) via RFID cards. To this end, the user holds his card against a reader and is then logged in to WinCC Advanced Runtime. The card UID is used as a password.

For details on this subject, please refer to the following application example: "User Login to Operator Panels with RFID Card Reader" (see \27\).

The **second** case uses an electronic "ID key-operated switch" that can switch up to four positions using differently coded keys. There are four different ID keys that are color coded to distinguish between them more easily.

Each plant operator gets a personal ID key. The personal ID number ("user name") is assigned to the plant operator as a "password" in user administration.

To be able to carry out an operation on the HMI operator panel, the plant operator first inserts his ID key into the ID key switch.

If the read-out ID number matches the ID number stored in user administration, the assigned function is released.

For details on this subject, please refer to the following application example: "User login on HMI operator panels via RFID and the SIRIUS ACT ID Key Switch" (see \28\).

Advantages

What both systems have in common:

- Automatic login of the user to the operator panel. Avoids errors when entering user name and password.
- Easy login even under unfavorable conditions, for example, when the user is wearing work gloves.
- High degree of flexibility (e.g., changing user data)

Note Due to the simplified login process, make sure to store the keys in a safe place so that unauthorized persons cannot access the plant.

Go to detailed device overview: →

4 Risk Assessment when Using the Panel

General notes on operating a plant

Secure operation of a plant also requires a high degree of operating security via the panel.

Example:

- Unauthorized persons edit or enter values (e.g., speed values for drives).
- Changing a plant's operating mode (manual / automatic).
- Using the different plant screens.

This chapter describes measures to protect the panel against unauthorized access. It additionally shows how to prevent manipulation of device settings.

4.1 Using the configured plant screens

The plant screens of the operator panels are used, e.g., to switch drives on and off. If unauthorized persons perform operator actions, this can result in considerable damage.

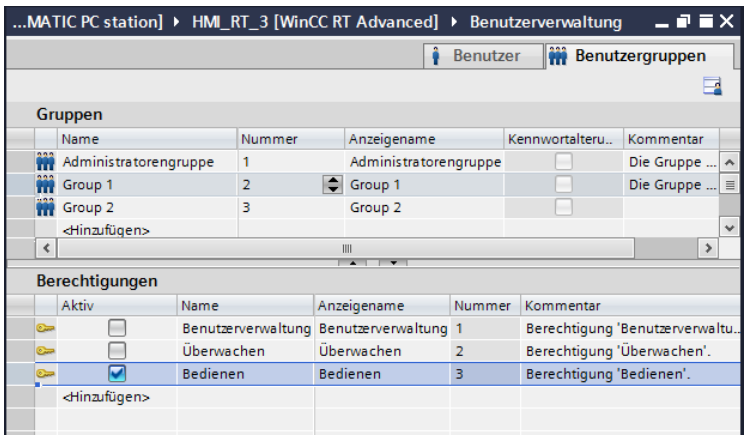
Remedy

To restrict operation to authorized operating staff, you can assign rights to individual functions. This ensures that only authorized persons can make entries on the panel, for example.

The "UserAdministration" (Figure 4-1) system function assigns users (operating staff / maintenance staff) to groups.

You can structure the groups such that, for example, "Group 1" contains only persons who are allowed to operate the plant but not to change values. "Group 2" is, for example, for persons who have full access to the panel.

Figure 4-1



For detailed information on creating a user administration feature, please refer to the online help and the TIA Portal manual (see Chapter 7).

Go to detailed device overview: →

4.2 "Start Center" start menu / "Loader menu"

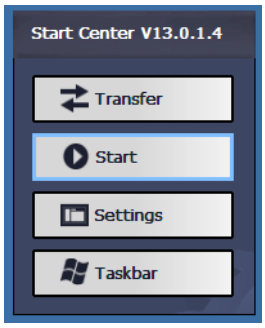
After starting up the panel or shutting down Runtime, the "Start Center" menu is displayed by default (Figure 4-2).

The "Settings" button allows you to open and edit the panel device settings.

The "Taskbar" button allows you to activate the taskbar that you can use to open the Windows CE desktop.

Without any further settings, persons in your plant have access to the above functions.

Figure 4-2



Remedy

You can password-protect the "Start Center" against unauthorized use.
If the "Start Center" is password-protected, "SecureMode" is automatically enabled (Figure 4-3).

To use the "Start Center", the user must now enter a password.
"SecureMode" also protects the taskbar and the Windows CE desktop.

Figure 4-3

The "Transfer" and "Start" buttons do not require a password and can always be used.

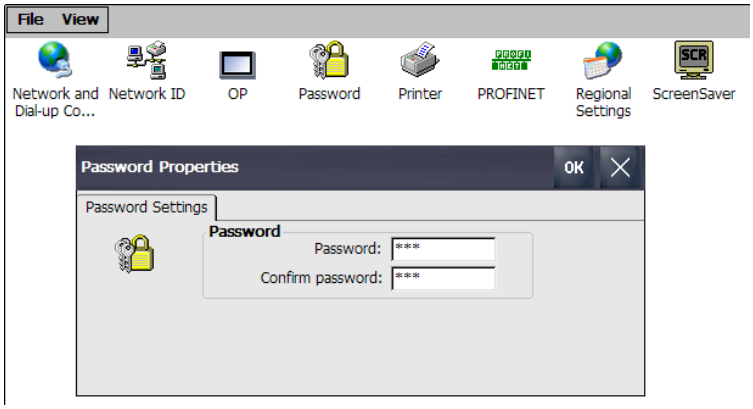
Enabling "SecureMode"

In the device settings, open the "Password" icon and enter the password. To disable the mode, open the function again and delete all entries in the “Password Settings” window (Figure 4-4).

For more information, please refer to the panel manual.

See Chapter 1.4 for information on how to create a secure password.

Figure 4-4

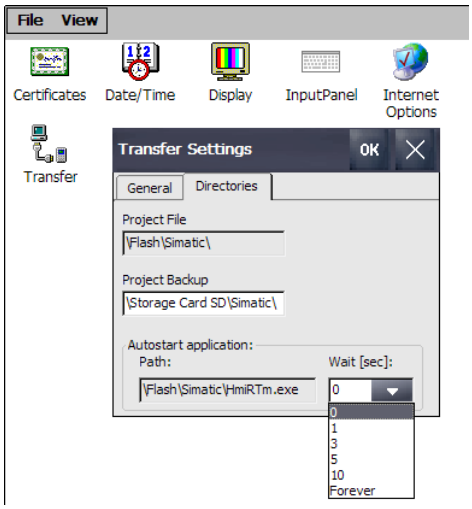


Panel autostart

As an additional protection feature, you can define the waiting time until the panel runtime is started using the "Transfer" icon. During this waiting time, the "Start Center" menu is displayed.

Set the waiting time for "autostart" to "0 seconds" (Figure 4-5).
Following a panel restart, the runtime is now started immediately without the "Start Center" being displayed.

Figure 4-5



NOTICE	**Make sure to configure a button with the "StopRuntime" system function. Otherwise, you cannot access the "Start Center" menu.**

If you forgot to configure the button with the "StopRuntime" system function, please refer to the following entry: "How do you switch an operator panel to transfer mode when the autostart's timeout is set to 0 seconds?" (see \3\).

Go to detailed device overview: →

4.3 Stopping HMI Runtime

Before switching off the panel, you should shut down the panel runtime to prevent loss of data while actions are active (e.g., export or import of data). This is usually done using a configured button on the panel and the "StopRuntime" system function.

If the panel runtime is stopped early, e.g. because the panel runtime shuts down automatically when starting a project transfer, it is no longer possible to operate the plant part using the panel. Moreover, the "Start Center" is displayed after shutting down the runtime.

Remedy

Make sure that only authorized staff can execute the 'Stop Runtime' function. To this end, go to "Properties > Security" and configure an authorization on the button.

Follow the information provided in Chapter 4.2, "Start Center" start menu / "Loader menu". Furthermore, you should prevent the panel runtime from stopping automatically. See Chapter 3.3, "Transferring the configuration to the panel".

Go to detailed device overview: →

4.4 Creating and transferring a Pack&Go file

If you are unable to connect the operator panel to your configuration PC, you can create a Pack&Go file. The configuration file is then available as a ".ZIP file".

Remedy

To prevent unauthorized persons from using the ".ZIP file", zip the file again and password-protect the new ".ZIP file".

Go to detailed device overview: →

4.5 Backing up and restoring panel data

The panel device settings include the "Backup / Restore" function and the "Service & Commissioning" function.

This function allows you to perform backup and restore functions.

Backup & Restore
The menu allows you to back up all panel data. The file cannot be edited, but it can be transferred back to another device identical in design (loss of know-how).
The restore operation deletes the existing data on the operator panel. If, by mistake or deliberately, an incorrect plant configuration is transferred to the panel, the plant can no longer be operated function-specifically using the panel.

Operating system (OS) update using storage media
This function allows you to run an operating system update of the panel. This update deletes the existing configuration. After the update, the panel does not contain any configuration data.

If the memory card slots and the device settings on the panel are freely accessible, unauthorized persons can make changes.

Service concept for Comfort Panels
The "automatic backup" is a continuous automatic backup of all the process-relevant operator panel data on a "SIMATIC HMI SD storage card" (system memory card).

There is a special slot for the system memory card.

For a detailed description on the subject, please refer to the following application: "Comfort Panels Service Concept: Continuous automatic backup of all the process-relevant control panels" (see \5\).

If the memory card slots are freely accessible and the device settings on the panel can be accessed, the function can be disabled or interrupted by removing the memory card. Furthermore, the data can be transferred to another device identical in design (loss of know-how).

Remedy

To give only authorized persons access to the device settings, follow the information provided in Chapter 4.2, "Start Center" start menu / "Loader menu". In addition, you can prevent access to storage media by means of constructional measures, e. g. by installing the panel in a locked control cabinet.

Go to detailed device overview: →

4.6 SIMATIC HMI Option+ V1

Note The following options can be used with "SIMATIC HMI Option+ V1" or higher.

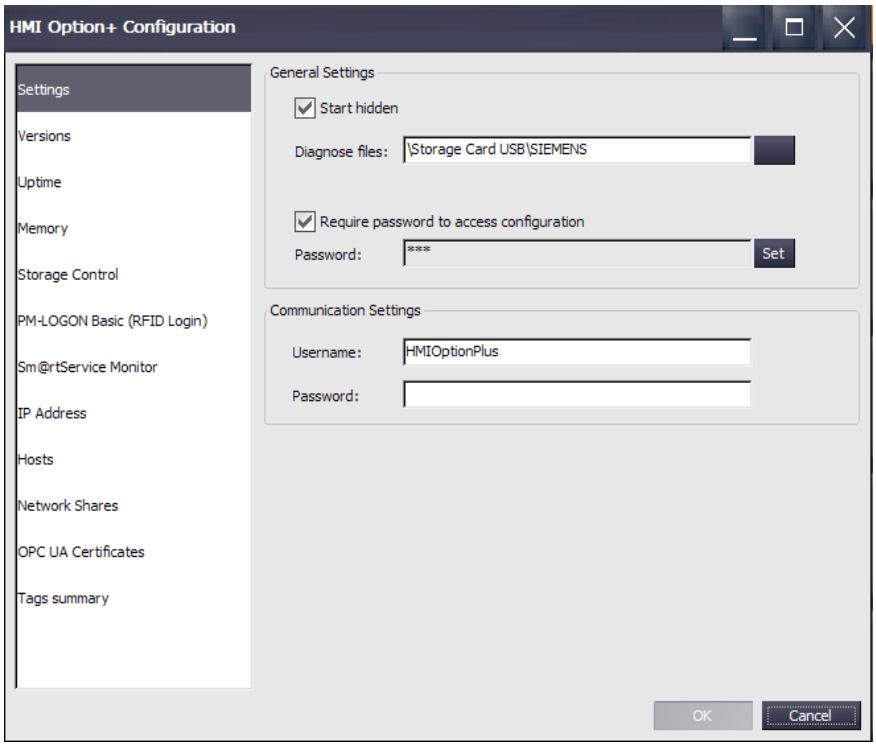
When running WinCC (TIA Portal) V15 or higher, you can use the "SIMATIC HMI Option+" tool. The tool provides functions that allow you to influence various properties of the HMI operator panel. At this point, the security-related tools are described in greater detail.
For detailed information on the individual parameters, please refer to the "SIMATIC HMI Option+" manual. For the manual, please refer to 'Links & Literature' (see \23\).

After installing the "SIMATIC HMI Option+" software on the configuration PC, you can transfer the tool to the operator panel using the "ProSave" program.

In order to run, the tool requires the "SOAP web service" (see also Chapter 5.2.4, "SOAP web service").

"SIMATIC HMI Option+ Configuration" view on the operator panel.

Figure 4-6



Go to detailed device overview: →

4.6.1 HMI Option+ Configuration

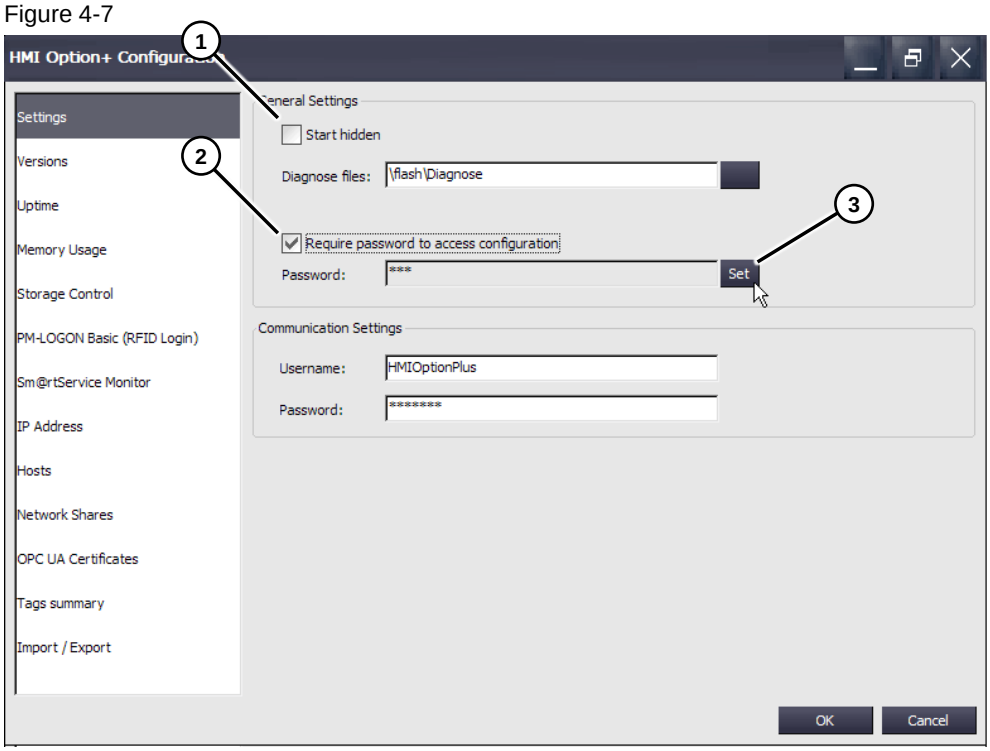
"Settings" function

The "Start Hidden" check box (1) allows you to specify how the "HMI Option+ Configuration" is started.
When "Start hidden" is checked ➔, the configuration is started hidden.

Check the "Require password to access configuration" check box (2) to make sure that only authorized persons can make changes to the parameters. The "Set" button (3) allows you to change an existing password.

The "SOAP" web service is required for communication between the operator panel and the "HMI Option+ Configuration". A user and password are stored on the operator panel in "WinCC Internet Settings > Web Server > User Administration". This user name and the associated password are stored here (3).

Figure 4-7



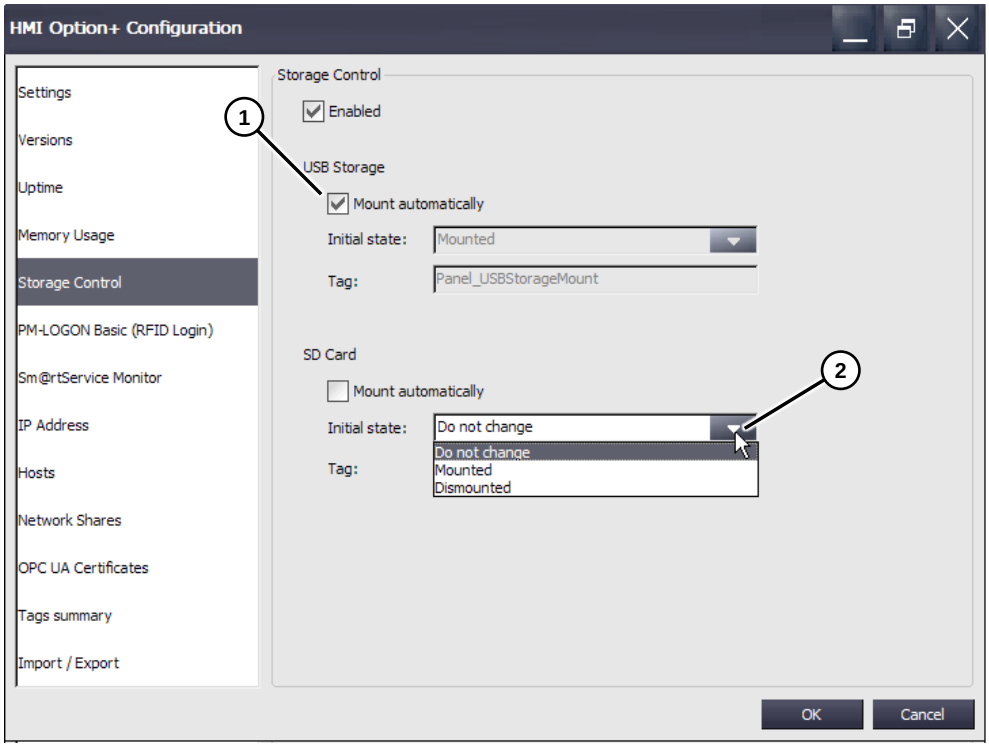
Go to detailed device overview: →

"Storage Control" function

The "Mount automatically" check box (1) allows you to specify whether or not an inserted USB flash drive or an inserted SD card is automatically detected by the system. With this function, you can prevent data from being downloaded from the panel to an unauthorized USB flash drive or software (virus) from being installed on the panel without being noticed.

The drop-down list (2) allows you to define how the panel responds to an external storage medium after a restart. The setting can be configured "manually" using the drop-down list or "dynamically" using a tag from Runtime.

Figure 4-8



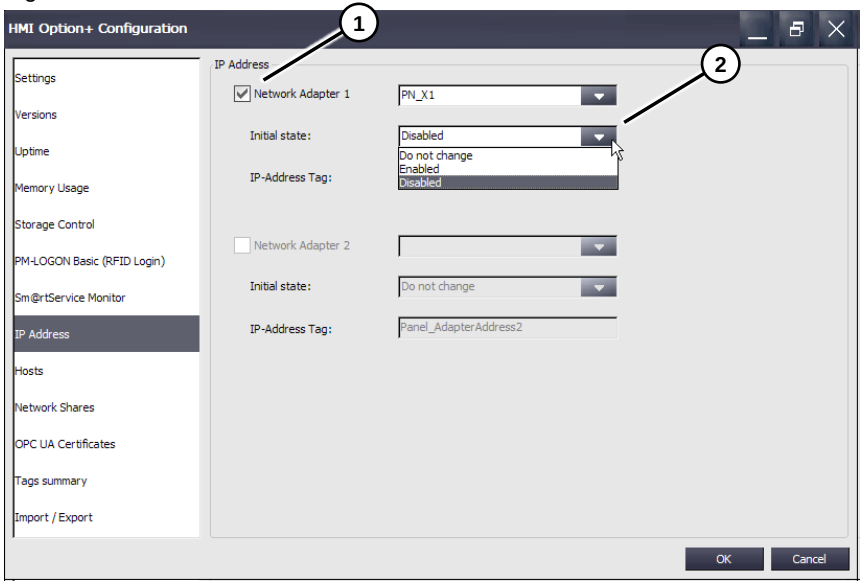
Go to detailed device overview: →

IP Address

The function allows you to enable / disable the network interfaces (1).

The drop-down list (2) allows you to specify the network interface behavior. The setting can be configured "manually" using the drop-down list or "dynamically" using a tag from Runtime.

Figure 4-9



Go to detailed device overview: →

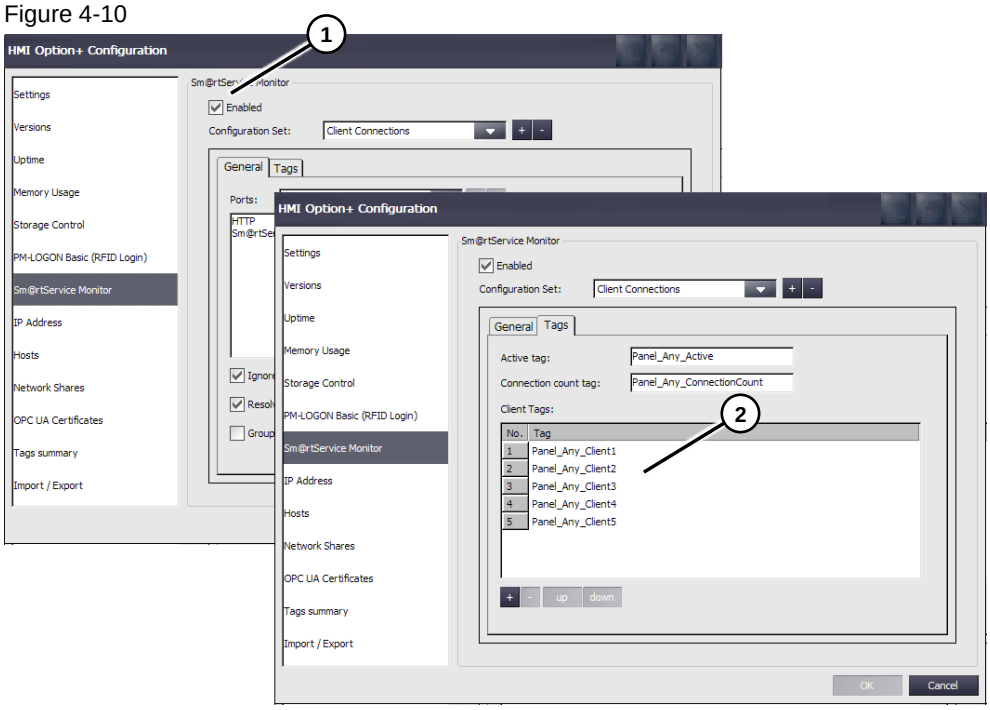
Sm@rt Service Monitor

Remote access to an operator panel is enabled via "Sm@rtService". For this purpose, a "remote server" is installed on the operator panel when transferring the configuration and started with Runtime.

By enabling the "Sm@rtService Monitor" function (1), you can now evaluate the names and number of "clients" connected to the "server".

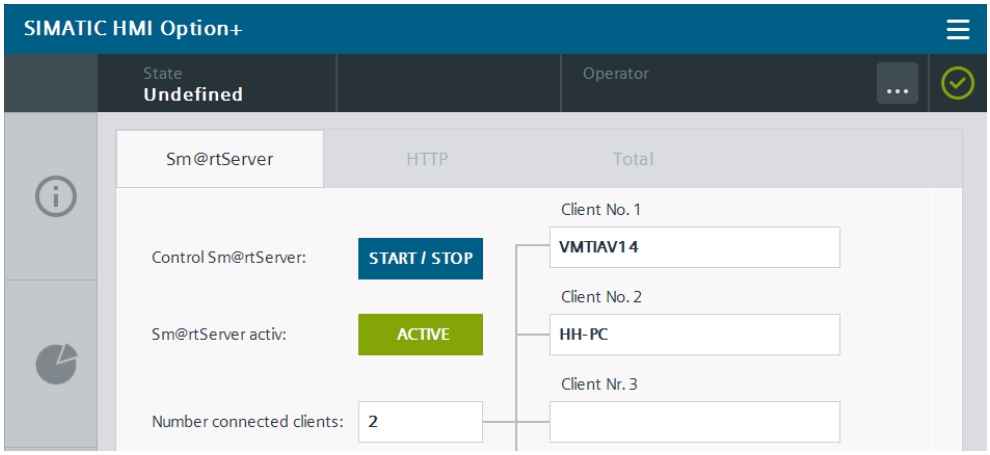
Tags (2) allow you to specify the information you want to output.

Figure 4-10



Sample view (snippet) of a configured plant screen on the Comfort Panel, with information about the number and names of the connected clients.

Figure 4-11



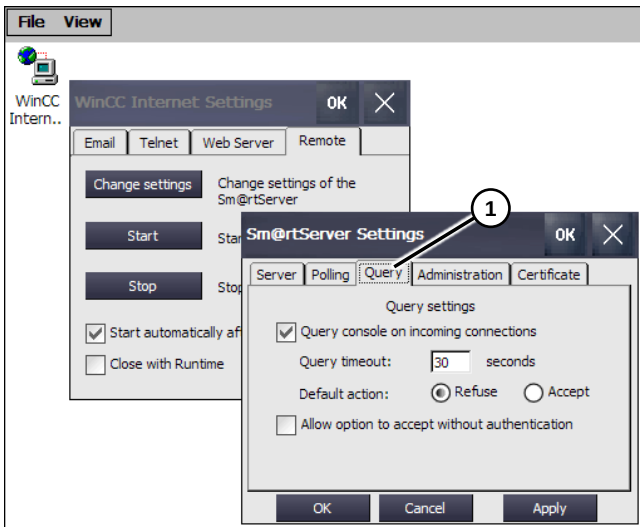
The functionality gives you detailed control/logging over the connected "remote nodes".

Go to detailed device overview: →

4.6.2 Increasing login security

To increase login security before remote access, you can check a check box (1) in the "Sm@rtServer Settings" (in this example: on the operator panel) to display an additional window on the server (operator panel) when a "client" (e.g., a PC) wants to connect to the "server".

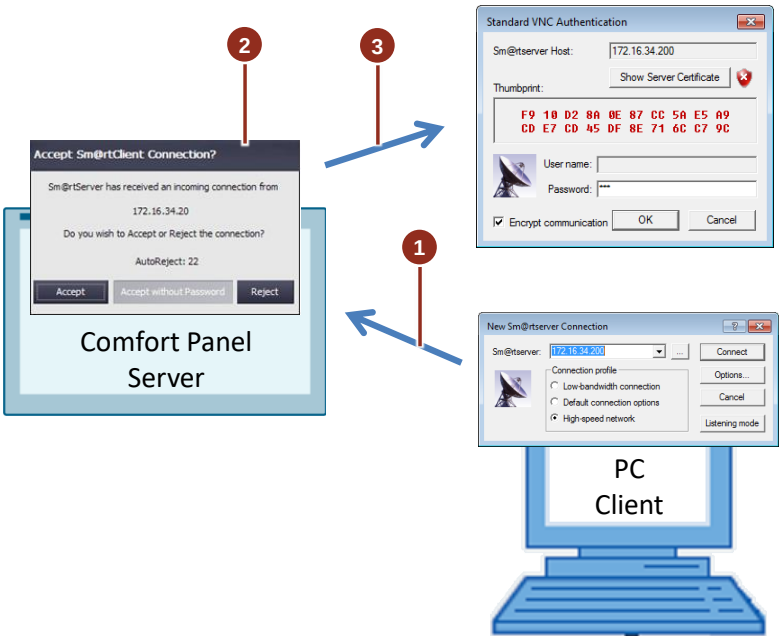
Figure 4-12



Runtime history

Before a "client" connects to the "server" (1), a screen with an "additional prompt" (2) appears on the "server". Among other things, the screen shows the client's IP address. You can accept or reject access. If access was accepted, login continues (3).

Figure 4-13



Note "SIMATIC HMI Option+ V2" or higher provides an additional "Sm@rtServer" option.

Go to detailed device overview: →

4.7 SIMATIC HMI Option+ V2

Note The following options can be used with "SIMATIC HMI Option+ V2" or higher (V2 includes the options of the previous version).

Remote access monitoring (Sm@rtService Monitor)

The "Sm@rtService Monitor" function that used to be available separately has been integrated and developed in SIMATIC HMI Option+.

With the aid of "Sm@rtService Monitor", connections that access the device (e.g., Sm@rtClient) can be cyclically polled.

The identified connection partners (IP address, host name) are written to Comfort Panel Runtime tags and can therefore be easily archived. This can be used, for example, to determine which and how many Sm@rtClients access the HMI.

If you have logged in to the operator panel on site, it may happen that a user simultaneously connects to the same operator panel via a Sm@rtClient connection. The Sm@rtClient user is now logged in with your credentials and has your authorization level for the plant.

To prevent this, the "Sm@rtService Monitor" function includes an appropriate protection feature.

For details on the configuration, please refer to the "SIMATIC HMI Option+" documentation (see \23\).

Go to detailed device overview: →

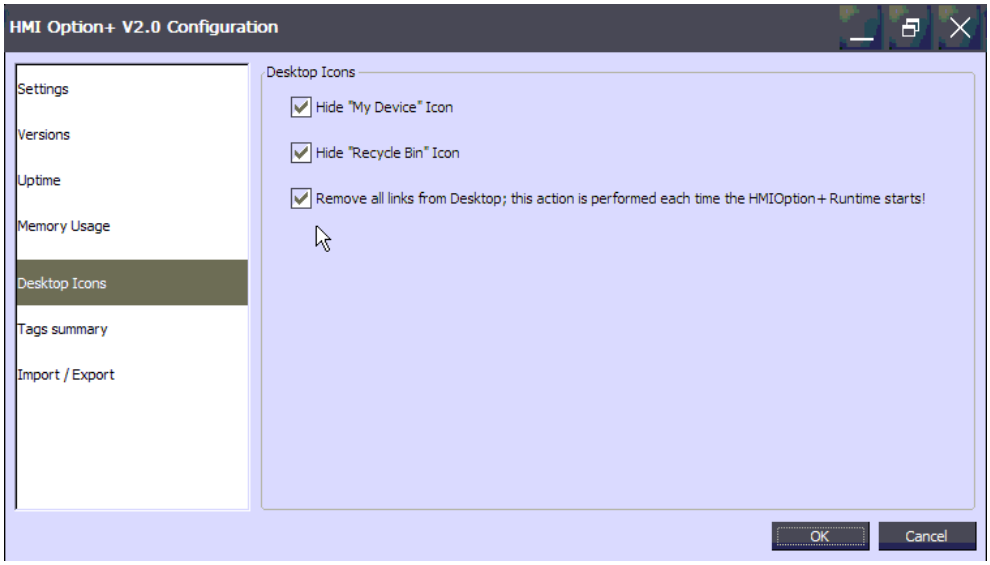
Showing / hiding Windows CE desktop icons

The "Desktop Icons" function allows you to hide the icons on the SIMATIC HMI Comfort Panel's desktop. The following three options are available:

- Hide "My Device" icon
  (hides the "My Device" desktop icon)
- Hide "Recycle Bin" icon
  (hides only the "Recycle Bin" desktop icon)
- Remove all links from Desktop
  (hides all desktop icons except "My Device" and "Recycle Bin")

For details on how to use the function, please refer to the "SIMATIC HMI Option+" documentation (see \23\).

Figure 4-14



Go to detailed device overview: →

5 Risk Assessment when Using Remote Maintenance Services

5.1 Background information

The different services for remote maintenance provide great benefits, but they also involve risks that must be taken into consideration.

Even though remote access is password-protected, there is always a risk of a person logging in with someone else's credentials and performing operator actions.

Also, the logged-in user does not have a view of the plant. If, in this case, operator actions are performed via remote access, this can have severe consequences.

The intervention must not put the staff on site or the plant at risk. To this end, it is important that you lock certain functions (e.g., manual control of a gripper) for the remote maintenance user. In addition, the staff on site should be informed of an intervention and be able to stop it at any time if necessary.

Moreover, it must be ensured that only authorized persons are provided with access to the plant. Unfortunately, total network security cannot be guaranteed. Therefore, it makes sense to inform the staff not only of the remote access operation, but also of the person accessing the plant.

For more information, please refer to the following entry: "Remote Access to SIMATIC HMI Control Panels" (see \11\).

Network security – for secure industrial communication

Protecting your network against unauthorized access is essential in order to prevent incalculable risks.

Defense in depth

All-embracing protection of industrial plants against cyber attacks must act at all levels at the same time – from plant management to the field level, from access control to copy protection.

For this purpose, Siemens uses the defense-in-depth concept, a comprehensive protection scheme in line with the recommendations of ISA99 / IEC 62443, the leading security standard in industrial automation.

See also Chapter 1.5, "Operation Security Guideline".

5.2 Using the Sm@rt options

5.2.1 General

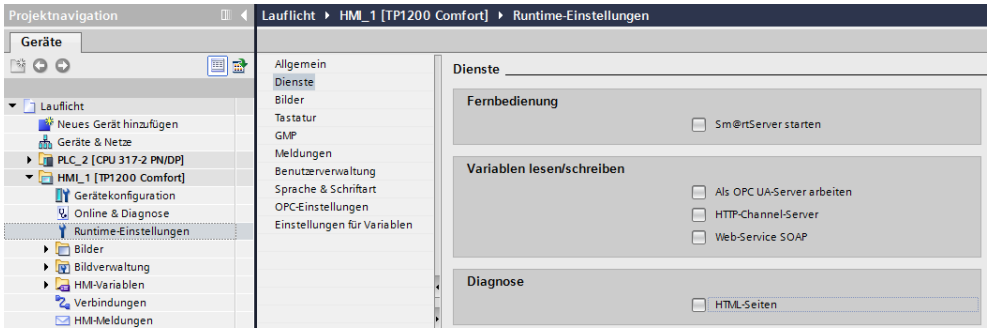
Using the WinCC services, you can implement communication between PC and HMI systems via TCP/IP connections (e.g., LAN).

Use cases include:

- Remote control of an HMI system over the internet, intranet and LAN.
- Sending emails based on alarms and events.
- Providing standard HTML pages on the HMI system with service and maintenance information and diagnostic functions.

The services are enabled in the project tree of the HMI configuration in "Runtime settings > Services" (Figure 5-1).

Figure 5-1



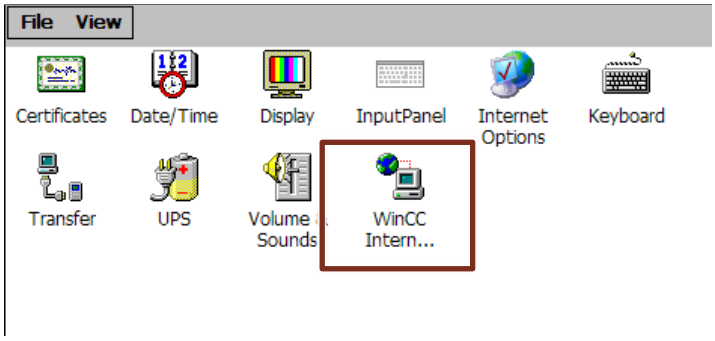
Using the "Sm@rt options" involves the risks described in Chapter 5.1, "Background information".

Remedy

Settings on the panel

E.g., for the Comfort Panel, the secure access settings are made in the device settings, "WinCC Internet Settings" icon (Figure 5-2) (Basic Panel differs, see manual).

Figure 5-2



For details on the individual parameters, please refer to the WinCC system manuals for SIMATIC Basic, Comfort or Advanced (see \12\, \20\ or \21\).

To give only authorized persons access to the panel device settings, follow the information provided in Chapter 4.2, "Start Center" start menu / "Loader menu".

5.2.2 Sm@rtServiceMonitor

The "Sm@rtServiceMonitor" tool (Comfort Panels only) reads the current Sm@rtClient connections and forwards them to HMI Runtime for further processing. This enables the operator on site to monitor remote access and interrupt it if necessary.

Application example: "Remote Access to SIMATIC HMI Operator Panels" \16\.

5.2.3 VPN for Sm@rtService

Access to a remote operator panel can be implemented over the internet.
To prevent unauthorized persons from accessing the operator panel or the data to be transferred, you must configure a secure connection.

The following application examples show solutions via VPN.

- "Remote Access to SIMATIC HMI Operator Panels" \16\.
- "Sm@rtClient App Demo Access" \17\.
- "Setting up a secure VPN Connection ..." \18\.

5.2.4 SOAP web service

The SOAP web service

- connects you to the office world. For example, MS Excel and a VBA script allow read / write access to the tags of an operator panel.
  The operator panel must support the web service (SOAP).
  For an application example, see \22\.

The SOAP web service

- enables you to use the "SIMATIC HMI Option+" tool (see Chapter 4.6,"SIMATIC HMI Option+").

The SOAP web service is enabled in the operator panel's "Runtime settings > Services > Read/write tags".

Go to detailed device overview: →

5.3 SIMATIC apps

Using mobile devices to access automation systems

Mobile devices such as smartphones or tablet computers are common in our private lives and provide services and information.

Now apps add to the range of functions provided by Siemens automation and drive products.

- **SIMATIC WinCC Sm@rtClient app**
  Encrypted, mobile remote operator control and monitoring of SIMATIC HMI systems via industrial WLAN in conjunction with SIMATIC SM@RT Server.
- **SIMATIC S7 app**
  Secure connection to the web server of your SIMATIC S7-1200/1500 and ET 200SP.
- **LOGO! App**
  Operator control and monitoring of the LOGO! 0BA7 and 0BA8 using smart devices.

Security considerations

Security considerations are necessary at different levels.

1. Protection of smartphones and tablet computers, incl. apps (protection against unauthorized access and loss/theft of stored data)
2. Protection of communication
   (Protection against changes and unauthorized network access by eavesdropping on communication)
3. Protection of the automation solution
   (Protection against unauthorized access and reduced availability due to loss of confidential information)

Using smart devices in the automation environment requires a specific assessment in the security management process.

For more information, please use the following link:

http://www.siemens.com/industrialsecurity

Protection of smartphones and tablet computers, incl. apps

The use of smart devices involves many risks, e.g., due to loss, theft or unauthorized access. This may give unauthorized persons access to the plant and its know-how.

Remedy

Protecting smartphones

The below actions protect your smartphone against unauthorized use or misuse of data in case of loss or theft.

- Enable a PIN or password to unlock your smartphone. Do not use gestures or swiping to unlock the device.
- Enable data media encryption (SD card / internal memory). Configure a VPN profile if necessary.

Your smartphone may also be at risk from external attacks. Perform the following actions to reduce the risk:

- Use antivirus software for protection against malware.
- Do not use alternative keyboards as these could theoretically eavesdrop on all your entries, making them accessible to third parties.
- Only use apps from trusted sources.
- Jailbreak or rooting are security risks. Do not use such devices in your automation system.

Protection functions of the apps

The following settings in the apps increase security.

Sm@rtClient app

- Enable encrypted communication (full version only!).

Note

Encrypted communication requires more resources on the Sm@artServer (operator panel) and on the smartphone. As a result, screen loading times can increase.

- Do not assign a password to the profile data in the app so that it must be entered manually.
- Enable the app password for starting the app. You will be prompted to do so when opening the app for the first time or navigate to "Settings > Change password".

SIMATIC S7 app and LOGO! app

- Enable encrypted communication (for all S7 controllers and LOGO! 0BA8). If you are using a LOGO! 0BA7, additional mechanisms such as VPN are strongly recommended.
- Enable the password prompt for starting the app. You will be prompted to do so when opening the app for the first time or navigate to "Settings > Change password".
- Do not assign a password to the profile data in the app for accessing the controller/LOGO! web server so that it must be entered manually.

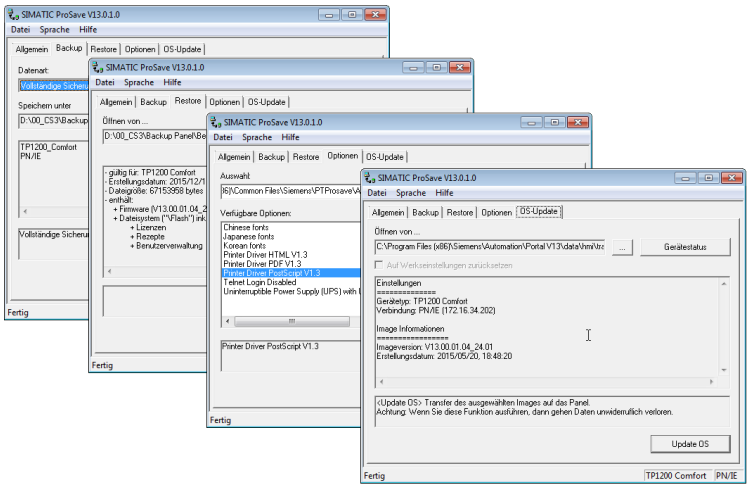
Go to detailed device overview: →

5.4 ProSave

The ProSave software enables you to perform a number of functions (Figure 5-3). Example:

- Create backups:
  - Back up configuration file.
  - Back up user administration.
  - Back up recipes.
- Restore function
  - Restore configuration file.
  - Restore user administration.
  - Restore recipes.
- Transfer options
  - E.g., "SIMATIC HMI Option+".
  - E.g., printer driver …
- Operating system update (OS update)

Figure 5-3



The following measures are described in order to prevent unauthorized persons from downloading project data using "ProSave" or manipulating the system in any other way.

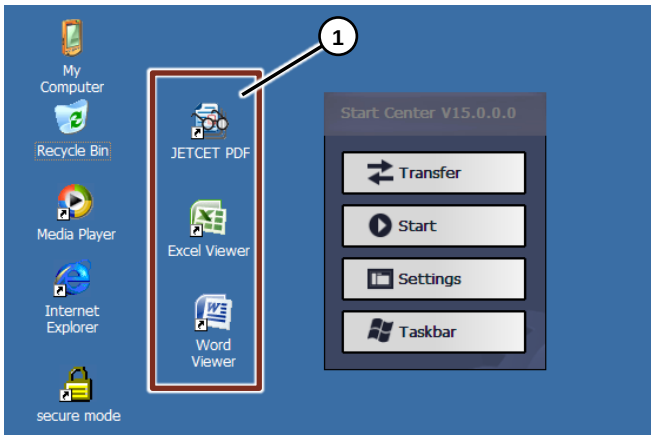
Remedy

- For the "ProSave" functions, the panel runtime must first be stopped. Therefore, make sure that the panel runtime cannot be stopped automatically, but by authorized persons only. For more information, please refer to Chapter 3.3, "Transferring the configuration to the panel".
- In the connection parameters, for example, the panel's IP address must be specified. If it is unknown, a connection to the panel cannot be established. Therefore, make sure that the device settings cannot be opened to change the Ethernet settings. For more information, please refer to Chapter 4.2, "Start Center start menu / Loader menu".

Uninstalling the WORD and EXCEL viewers

By default, the "WORD, EXCEL and PDF" viewers are installed on the Comfort Panels. For example, it is possible that a WORD file executes a script without anyone noticing and causes damage (1).

Figure 5-4

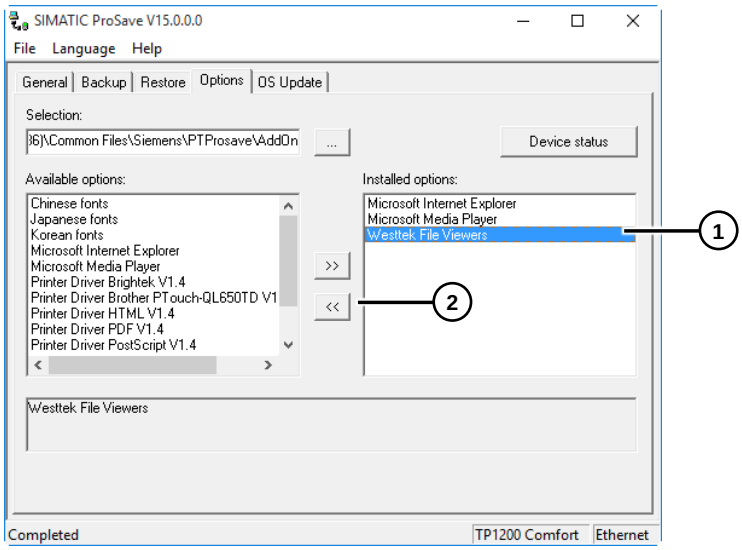


When running WinCC (TIA Portal) V15 or higher, you can uninstall the WORD, EXCEL and PDF viewers in the Comfort Panels.

Use the "ProSave" software to uninstall the viewers.
In the "Options > Installed Options" tab (1), select the "Westtek File Viewers" option.

The "<<" button (2) removes the option from the operator panel. If required, you can transfer the option back to the panel.

Figure 5-5



Go to detailed device overview: →

5.5 Ports used by operator panels

The IANA (Internet Assigned Numbers Authority) assigns the TCP / UDP ports. When using a firewall, the ports specified in the tables must be enabled.

Please note that enabling a port can create a security vulnerability.

Remedy

Only enable ports you really need. Restrict access, e.g, by defining user groups.

For a list of ports, please refer to the WinCC Online Help (TIA Portal): Select "Content > Readme > WinCC Comfort/Advanced > Security notes".

For more information, please refer to the following entry:
"Which ports are used by WinCC Advanced…" (see \14\).

Go to detailed device overview: →

6 Risk Assessment of the Hardware Used

6.1 External storage media

External storage media (SD card / USB flash drive) can be used to archive process values and alarms or to store documents. Depending on where the panel is installed, the storage devices are frequently easily accessible. As a result, sensitive data can easily be lost or modified. For more information, please see Chapter 3.4. In addition, there is a possibility that an incorrect program is transferred to the panel. For more information, please see Chapter 4.5, "Backing up and restoring panel data".

Remedy

A USB lock can be used to protect the USB interface. In addition, you should use a locked control cabinet to protect other media such as SD cards against unauthorized access. Alternatively, you can save the data to a PC over the network. For more information, please see Chapter 3.4, "Archiving tags and alarms".

Go to detailed device overview: →

6.2 Device communication interfaces

Access to the communication interfaces is similar to the scenario described in Chapter 6.1. One threat is the loss of usability, e.g, by disconnecting the Ethernet connection. However, a greater potential hazard is tampering of the communication, e.g, by installing additional components that log or modify the communication.

Remedy

Restrict access by means of constructional measures, e.g., by installing the panel in a locked control cabinet.

Go to detailed device overview: →

6.3 WLAN / LAN security

The number of devices that communicate with each other via Ethernet is increasing. As the number of devices grows, so does the number of persons who can access the WLAN/LAN.

Moreover, there is a great number of network configurations that must be considered individually.

Example:

- Ring line / redundant ring line
- Shared / separate network of office and production facility
- Encrypted connection such as WPA2 etc.

Remedy

Siemens offers a variety of examples and solutions regarding network security and architecture. A detailed description would be beyond the scope of this document.

For related information, please refer to the following entry: "SIMATIC NET Industrial Ethernet Security Setting up security – Getting Started" (see \6\).

Based on simple test networks, you will learn how to handle the security modules and the Security Configuration Tool. Learn how to implement the protection functions of security modules in the network without any major configuration overhead.

Go to detailed device overview: →

7 Links & Literature

Table 7-1

	Topic	Title
\1\	Siemens Industry Online Support	http://support.industry.siemens.com
\2\	Download page of the entry	https://support.industry.siemens.com/cs/ww/en/view/109481300
\3\	FAQ	How do you switch an operator panel to transfer mode when the autostart's timeout is set to 0 seconds? https://support.industry.siemens.com/cs/en/en/view/23034454
\4\	FAQ	How do you read out or write tag values with an Excel application? https://support.industry.siemens.com/cs/ww/en/view/69846238
\5\	Application example	Comfort Panels Service Concept: Continuous automatic backup of all the process-relevant control panels https://support.industry.siemens.com/cs/ww/en/view/68373729
\6\	Application example	SIMATIC NET Industrial Ethernet Security Setting up security – Getting Started https://support.industry.siemens.com/cs/ww/en/view/109477612
\7\	Application example	Integrating HMI Operator Panels in TCP/IP Networks https://support.industry.siemens.com/cs/ww/en/view/92346478
\8\	Application example	WinCC flexible recipes: Engineering with Recipes Using Integrated Functionalities https://support.industry.siemens.com/cs/ww/en/view/23901413
\9\	Application example	E-mail Notification with the SIMATIC HMI Comfort Panels https://support.industry.siemens.com/cs/ww/en/view/56720728
\10\	Application example	Protection of an Automation Cell Using the SCALANCE S602 V3 and SCALANCE S623 Security Modules via a Firewall https://support.industry.siemens.com/cs/ww/en/view/22376747
\11\	Application example	Remote Access to SIMATIC HMI Operator Panels https://support.industry.siemens.com/cs/ww/en/view/109476153
\12\	Manual	SIMATIC HMI HMI devices Comfort Panels https://support.industry.siemens.com/cs/ww/en/view/49313233
\13\	Document	Operational Guidelines for Industrial Security http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf
\14\	FAQ	Which ports are used by WinCC Advanced, WinCC Runtime Advanced, WinCC Runtime Professional, Basic Panels, Comfort Panels, Panels and IPC? https://support.industry.siemens.com/cs/ww/en/view/80917729
\15\	FAQ	With SIMATIC WinCC V14 Image, why do you get an error message when downloading a project to a Basic Panel? https://support.industry.siemens.com/cs/ww/en/view/109743844
\16\	Application example	Remote Access to SIMATIC HMI Operator Panels https://support.industry.siemens.com/cs/en/en/view/109476153
\17\	Application example	Sm@rtClient App Demo Access https://support.industry.siemens.com/cs/ww/en/view/92190359

	Topic	Title
\18\	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
\19\	Application example	Communication via OPC UA in Conjunction with a SIMATIC HMI Comfort Panel https://support.industry.siemens.com/cs/en/en/view/63481236
\20\	Manual	SIMATIC HMI HMI devices Basic Panels 2nd Generation https://support.industry.siemens.com/cs/ww/en/view/90114350
\21\	Manual	SIMATIC WinCC WinCC Advanced V14 https://support.industry.siemens.com/cs/ww/en/view/109742297
\22\	Application example	How do you read out or write tag values with an Excel application? https://support.industry.siemens.com/cs/ww/en/view/69846238
\23\	Application example	HMI Option+ https://support.industry.siemens.com/cs/ww/en/view/109754400
\24\	Application example	Multiuser Engineering in TIA Portal https://support.industry.siemens.com/cs/ww/en/view/109740141
\25\	Application example	Working with the TIA Portal Cloud Connector https://support.industry.siemens.com/cs/ww/en/view/109747305
\26\	Manual	STEP 7 Basic/Professional V15.1 and SIMATIC WinCC V15.1 https://support.industry.siemens.com/cs/ww/en/view/109755202
\27\	Application example	User Login to Operator Panels with RFID Card Reader https://support.industry.siemens.com/cs/ww/en/view/99808171
\28\	Application example	User login on HMI operator panels via RFID and the SIRIUS ACT ID Key Switch https://support.industry.siemens.com/cs/ww/en/view/109749912

8 History

Table 8-1

Version	Date	Modifications
V1.0	03/2016	First version
V1.1	05/20217	Functions extended by WinCC V14.
V1.2	04/2018	Comfort Pro and Option+ added
V1.3	04/2019	Functions extended by WinCC V15.