

The Siemens logo is displayed in a white rectangular box with a thin black border. The word "SIEMENS" is written in a bold, teal, sans-serif font. The background of the entire page is a blurred industrial setting with a man in a light blue shirt looking at a tablet. Overlaid on the image are various blue, semi-transparent digital icons and text elements, including a clock, a folder, a 24/7 circular arrow icon, a news icon, a network diagram, and the text "Industry Online Support" and "Home".

SIEMENS

Security guidelines for SIMATIC HMI operator devices

HMI operator devices / WinCC (TIA Portal) V17

<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

Legal information	2
1 Industrial security	5
1.1 Strategies to increase security	5
1.2 Structure of this document	5
1.3 The three major safeguards	5
1.3.1 Panel access protection	6
1.3.2 User management	6
1.3.3 Data storage on a network drive	6
1.4 Security of names and passwords	6
1.5 Operational security guideline	8
1.5.1 Protection of machines and plants	8
1.5.2 Panel operating system	9
1.5.3 Security management	10
2 Master overview of device functions	11
3 Risk analysis when creating and editing HMI projects	14
3.1 Opening and editing a configuration	14
3.1.1 WinCC (TIA Portal) until V14 SP1	14
3.1.2 WinCC (TIA Portal) V15 or higher	15
3.2 Simulating and testing a configuration	15
3.3 Transferring configuration to the Panel	16
3.4 Signed images	16
3.5 User management	17
3.6 Data exchange between HMI device and controller	17
3.7 Archiving of tags and messages	18
3.8 Working with recipes	20
3.9 Locking task switching	20
3.10 Project transfer	21
3.11 Access to tags via OPC UA	22
3.12 Data exchange between HMI devices	23
3.13 Remote access to a Panel's tags via Excel	23
3.14 Sending emails via the Panel	24
3.15 TIA Portal Multiuser Engineering	24
3.16 TIA Portal Cloud Connector	25
3.17 User Management Component (UMC)	25
3.18 RFID user management	26
4 Risk analysis when operating the Panel	28
4.1 Operation of configured plant screens	28
4.2 "Start Center" / "Loader Menu" start menu	29
4.3 Terminating the HMI runtime	31
4.4 Generating and transferring a Pack&Go file	31

4.5	Backup and restoration of Panel data	31
4.6	SIMATIC HMI Option+	33
4.6.1	Features	34
4.6.2	Remote access and logon security	38
5	Risk analysis when using remote maintenance services	41
5.1	Background information	41
5.2	Use of Sm@rt options	42
5.2.1	General.....	42
5.2.2	SmartService monitor.....	43
5.2.3	VPN for SmartService	43
5.2.4	SOAP web service	43
5.3	SIMATIC apps	44
5.4	ProSave.....	47
5.5	Ports used by operator devices.....	49
6	Hardware risk analysis.....	50
6.1	External storage devices	50
6.2	Device communication interfaces	50
6.3	WLAN / LAN security.....	50
7	Appendix	52
7.1	Service and support	52
7.2	Industry Mall	53
7.3	Links and literature	53
7.4	Change documentation	55

1 Industrial security

1.1 Strategies to increase security

The goal of this document is to give the reader an appreciation for the security aspects with SIMATIC HMI 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.

1.2 Structure of this document

General

This document addresses the following topic areas in greater detail with respect to their security aspects. The topic areas describe the various phases, beginning with the initial configuration and ending with commissioning.

- Preliminary measures:
Minimization/prevention of manipulation during configuration
- In operation: Device settings on the panel
Prevent access to device settings
- In operation: HMI runtime operator actions
Only authorized personnel may operate the plant
- In operation: Remote access / servicing
Prevent unwanted remote access with suitable safeguards
- General: Hardware
External physical measures prevent tampering with the panel

Note

This document addresses security aspects of various device classes from a holistic point of view. For this reason, not all the content described within is necessarily relevant for you.
You do not necessarily have to follow all the points listed in each of the chapters. There may only be a need to act when the features you actually use are concerned.

1.3 The three major safeguards

Three simple steps to reduce a majority of the threat potential

Chapters [3](#) to [6](#) describe individual hazards in detail. In summary, following the three points described below can minimize a majority of the potential hazards.

Always make sure to put multiple safeguards in place. In this way, safety and security are still ensured even if one safeguard is forgotten or proves to be insufficient.

1.4 Security of names and passwords

1.3.1 Panel access protection

Protect access to the device settings of the Panel by setting a password. Without a valid password, it is not possible to open the device settings via the "Start Center".

For detailed information, refer to chapter [4.2](#) "'Start Center" / "Loader Menu" start menu'.

1.3.2 User management

Link each operator action on the panel with a permission by setting up user management.

In the object properties, select the menu "Properties > Security" and assign the object a permission.

For detailed information, refer to chapter [4.1](#) "Operating configured plant screens".

1.3.3 Data storage on a network drive

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

A network drive offers more comprehensive access protection features than an insertable storage device (storage card or USB drive).

Detailed information and tips on what to pay attention to when using a network drive can be found in chapter [3.7](#) "Archiving of tags and messages".

1.4 Security of names and passwords

General remark on name and password security

SIMATIC HMI operator devices have pre-configured access mechanisms which prevent unauthorized persons from obtaining access to device settings, for example.

If you add a new operator device in TIA Portal, the default user "Administrator" is created in the WinCC user management (see [Figure 1-1](#)). Because this user also needs a password, a default password is likewise used.

- Username => Administrator
- Password => administrator

What should you do?

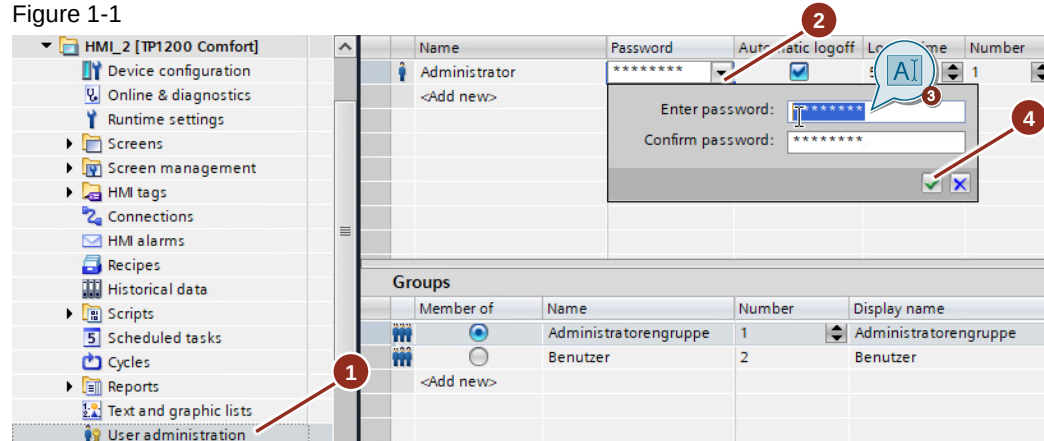
Change and/or inspect preset "user and password data" before beginning with commissioning (see [Figure 1-1](#)).

1 Industrial security

1.4 Security of names and passwords

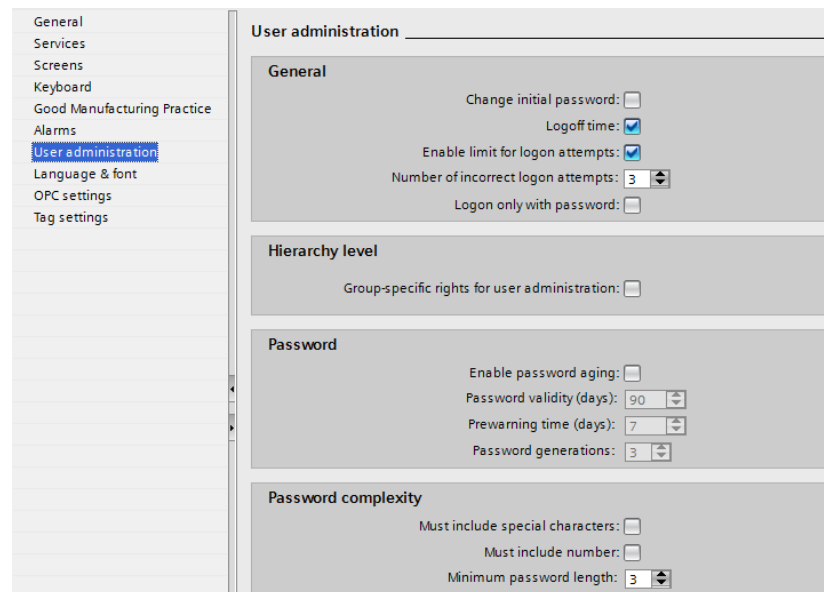
In WinCC (TIA Portal), navigate to the HMI operator device and then to "User management" (1). Existing users are listed in the "Users" window. Select the "Password" column (2). Enter a new password and confirm it by repeating the password (3). Click the Confirm button (4). You have assigned a new password to the selected user.

Figure 1-1



Also use the available user management settings in WinCC (TIA Portal). The example shows "Password aging" and "Password complexity" (Figure 1-2).

Figure 1-2



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

As of WinCC V13 SP1 (TIA Portal), there are no longer preset passwords for the web server or Sm@rtServer. During commissioning, a password must first be set for the default users.

1.5 Operational security guideline

1.5.1 Protection of machines and plants

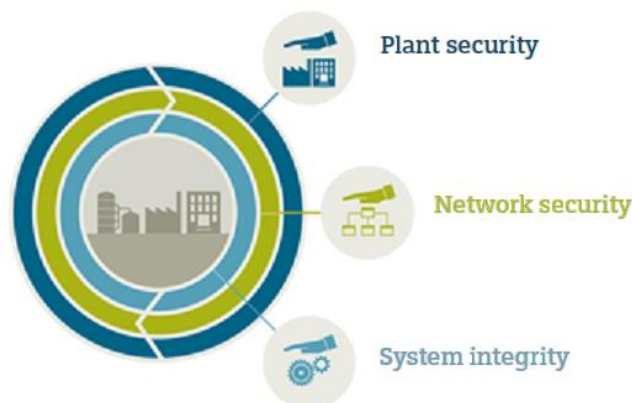
The crucial question is: How can potential risks be significantly minimized and how can adequate yet affordable security be achieved in industrial automation?

Unfortunately, there is no standard solution that can always be applied. In general, however, isolated security measures alone will not be sufficient.

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 "defense in depth" concept entails the three components listed in [Figure 1-3](#).

Figure 1-3



Plant security

Secure physical access of persons to critical components through 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

1.5 Operational security guideline

- 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 must be minimized with an alternative countermeasure.

For detailed information, visit the Siemens topic page "Cybersecurity for Industry" (see link [\13\](#)).

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).

1.5.2 Panel operating system

Basic Panels

SIMATIC HMI Basic Panels have an operating system that is created and preconfigured by Siemens.

Comfort Panels

SIMATIC HMI Comfort Panels have an operating system, "WinCE Embedded", that has been specially configured for SIEMENS.

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

1.5.3 Security management

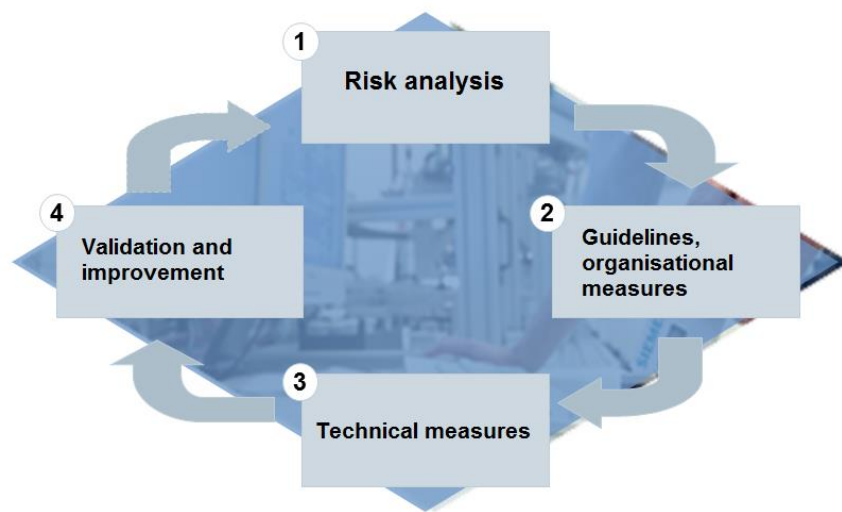
Organizational measures and the introduction of security processes are an indispensable component of plant security.

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 (Fehler! Verweisquelle konnte nicht gefunden werden.).

Security management process

Abbildung 1-4



The protection goals are derived from the risk analysis and serve as the basis for concrete organizational and technical measures.

Measures must be checked from time to time after implementation.

Brief description of the "Security management process"

1. Risk analysis
Risk analysis with definition of risk minimization measures
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.

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

2 Master overview of device functions

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

Use the Table to find which feature applies for which device.

Details on the security strategy are described in the individual chapters.

The KP8, KP8F and KP32F operator devices will not be examined further in this document since their parameters are assigned in STEP 7. The HMI device is connected via PROFINET to a SIMATIC controller.

Legend: ✓ = Applies for this device,
 -- = Feature not supported.

Master overview

Table 2-1

Applies to	Basic Panel	Basic Panel 2nd generation	Comfort Panel	Mobile Panel 2nd generation	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 analysis when creating and editing HMI projects												
3.1 Opening and editing a configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.2 Simulating and testing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.3 Transferring configuration to the Panel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.4 Signed images	--	✓	✓	✓	✓	✓	--	--	--	✓	✓	✓
3.5 User management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.6 Data exchange between HMI device and controller	--	--	✓	✓	--	✓	--	--	--	--	--	--
3.7 Archiving of tags and messages	--	✓	✓	✓	✓	✓	--	--	--	✓	✓	✓
3.8 Working with recipes	✓	✓	✓	✓	✓	✓	✓ ¹	✓	✓	✓	✓	✓
3.9 Locking task switching	--	--	✓	✓	✓	✓	--	✓	✓	✓	✓	✓
3.10 Project transfer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3.11 Access to tags via OPC UA	--	--	✓	✓	--	✓	--	--	--	--	--	--

¹ Except OP73

Applies to	Basic Panel	Basic Panel 2nd generation	Comfort Panel	Mobile Panel 2nd generation	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 HMI devices	--	--	✓	✓	✓	✓	--	✓ ²	✓ ²	✓	✓	✓
3.13 Remote access to a Panel's tags via Excel	--	--	✓	✓	✓	✓	--	✓ ²	✓ ²	✓	✓	✓
3.14 Sending emails 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 analysis when operating the Panel												
4.1 Operation of configured plant screens	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.2 "Start Center" / "Loader Menu" start menu	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.3 Terminating the HMI runtime	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.4 Generating and transferring a Pack&Go file	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4.5 Backup and restoration of Panel data	✓	✓	✓	✓	✓	--	✓	✓	✓	✓	✓	✓
4.6 SIMATIC HMI Option+	--	--	✓	--	--	--	--	--	--	--	--	--
5 Risk analysis when using remote maintenance services												
5.2 Use of Sm@rt options	--	✓ ⁴	✓	✓	✓	✓	--	✓ ⁵	✓	✓	✓	✓
5.3 SIMATIC apps	--	--	✓	--	--	✓	--	--	--	--	--	--
5.4 ProSave	✓	✓	✓	✓	✓	--	✓	✓	✓	✓	✓	✓
5.5 Ports used by operator devices	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

² Only devices with PROFINET port

³ Access via the engineering system

⁴ WinCC V14 or later

⁵ Excludes devices with PROFIBUS port

Applies to		Basic Panel	Basic Panel 2nd generation	Comfort Panel	Mobile Panel 2nd generation	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 Hardware risk analysis													
6.1	External storage devices	--	✓	✓	✓	✓	✓	--	--	--	✓	✓	✓
6.2	Device communication interfaces	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.3	WLAN / LAN security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Note

As of WinCC V15, the following devices are no longer supported.
OP 73, OP 77A, TP 177A, TP/OP 177B, TP/OP 277, MP 177, MP277, MP377.

For more information, refer to the following article:

<https://support.industry.siemens.com/cs/ww/en/view/109753803>

Subheading "Changed device support".

3 Risk analysis when creating and editing HMI projects

Security and configuration measures

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

3.1 Opening and editing a configuration

3.1.1 WinCC (TIA Portal) until V14 SP1

By default, an HMI configuration can be opened and edited by anyone who has the necessary software. It is not possible to prove who last used the file.

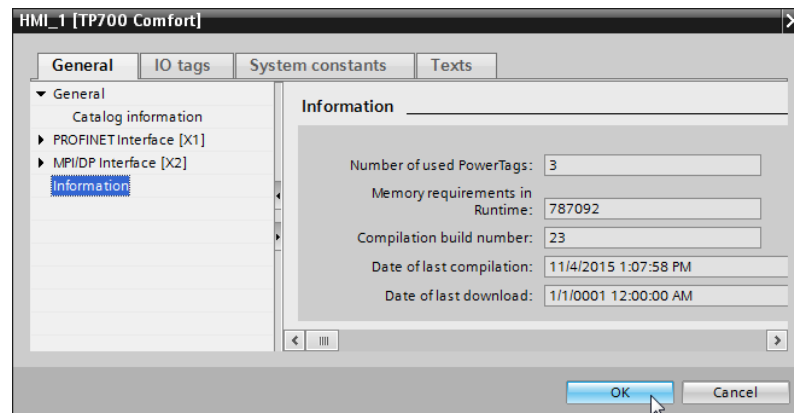
Remedy

After finishing the project or after commissioning is complete, it is recommended to note down the file's version number, last date generated and the date it was saved.

Procedure:

- Right-click in the project tree on the project name of the HMI operator device and open the "Properties".
- Select the menu command "General > Information".
- The "Information" menu ([Figure 3-1](#)) shows the version number and the date on which the project was last compiled.

Figure 3-1



Save and archive your projects on a secure drive that is not accessible to just anyone. Store the configuration file as a ZIP file and give it a password.

Detailed device overview here: [→](#)

3.1.2 WinCC (TIA Portal) V15 or higher

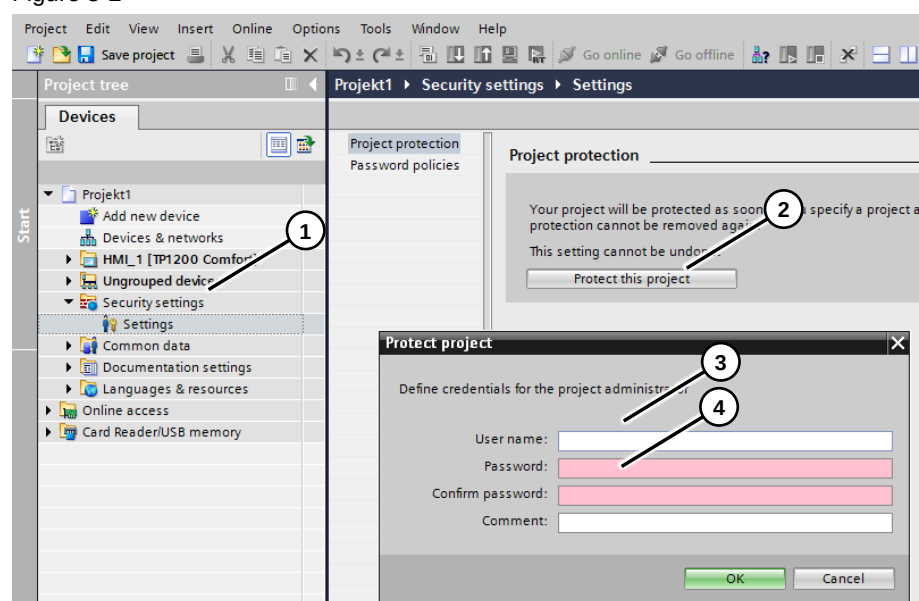
As of WinCC (TIA Portal) V15, you can require a password to open the configuration.

Go to the "Security settings" (1) in the project tree. Pressing "Protect this project" (2) will open a dialog window in which you can define a project administrator (3) and a password (4).

Note

This action cannot be undone.

Figure 3-2



Detailed device overview here: [→](#)

3.2 Simulating and testing a configuration

If the configuration is open, any user can start the simulation. If there is an active connection to a configured PLC, then the connection can be used to operate the machine. This can cause hazardous situations.

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.

Detailed device overview here: [→](#)

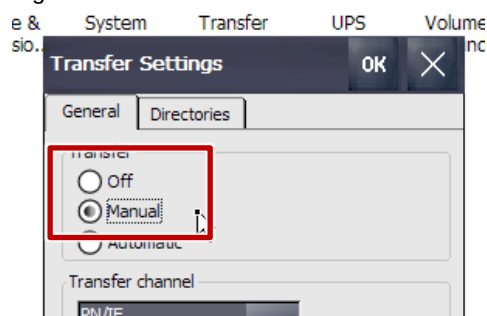
3.3 Transferring configuration to the Panel

The configuration can be transferred to the Panel by any user. Increased caution is required if system components are in operation. 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.

Remedy

Prevent automatic termination of the Panel runtime, for example in the event that a project download is triggered. To do this, open the Panel device settings. Under "Transfer > General", select the option "Manual" or "Off" ([Figure 3-3](#)). Select the "Off" option if you do not expect any more changes to the configuration (commissioning is complete).

Figure 3-3



Detailed device overview here: [→](#)

3.4 Signed images

The image file of an HMI operator device (operating system) is version-dependent. It is installed on the engineering PC along with the installation of the WinCC (TIA Portal) engineering software.

The risk here is that unknown software may be unwittingly transferred to the HMI device through tampering with the image file.

Remedy

As of WinCC V14, the image file is accompanied by a signature. Prior to a project download, the HMI device checks the image signature. If it does not match, the download is cancelled. You can disable image file verification if necessary. For details, refer to the appropriate manual (2nd-generation Basic Panel / Comfort Panel).

If you receive an error message when downloading a WinCC V13 project to a Basic Panel (which has a SIMATIC WinCC V14 image), please refer to the following FAQ article (see [\15](#)).

Detailed device overview here: [→](#)

3.5 User management

User management is an especially sensitive aspect. For example, the "administrator password" is known and User Administration is configured, then user data can be modified online.

Remedy

Use the powerful settings under the "Runtime settings > User Administration" menu. It contains options, such as those for

- changing the initial password
- password aging
- requiring the name to contain a special character, etc.

The following special character are permitted in passwords:

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

Detailed device overview here: [⇒](#)

3.6 Data exchange between HMI device and controller

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

Remedy

As of TIA Portal version V17 and CPU firmware version V2.9 (S7-1500) or V4.5 (S7-1200), communication is based on the TLS internet standard (Transport Layer Security). This supports unique identification of CPUs by means of certificates, as well as encrypted communication.

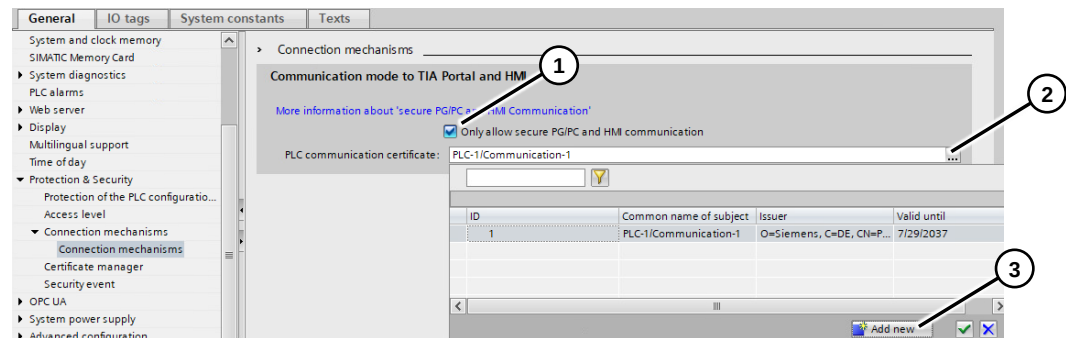
When you add an eligible CPU to the project from the hardware catalog in TIA Portal, a wizard will appear and guide you through the security settings. The wizard will prompt you for the desired PG/PC and HMI communication mode, among other things. You can also find the settings in the CPU properties in the "Protection & Security" – "Connection mechanisms" section (see [Figure 3-4](#)).

Here you can decide whether to permit only the new, TLS-based "secure communication" (1). If you uncheck the box, the communication method you have been using up until now ("Legacy") will be allowed.

- Only secure communication: higher security standard, communication to TIA Portal <V17 and HMI systems <V17 not possible
- Legacy and secure communication: Communication mode and security standard depend on support from the devices involved. Communication to TIA Portal <V17 and HMI systems <V17 not possible.

You can also select the certificate required for secure communication (2), or generate a new certificate with "Add" (3).

Figure 3-4



For further information on working with certificates and the new security features, refer to the article "Questions and answers about the new security features in TIA Portal V17" (see [\28\](#)) or the SIMATIC WinCC V17 system manual (see [\26\](#)).

3.7 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 simply lost.

Furthermore, archived process values and messages are often "sensitive" data which are used in particular for documenting quality assurance. It is necessary to ensure that these data are not falsified or lost.

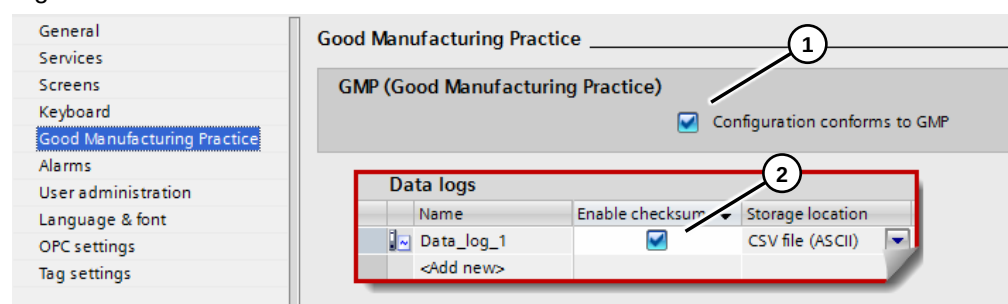
Remedy 1, "GMP"

If you are using HMI devices that support the "Good Manufacturing Practice" ("GMP") option (1), you can activate the "Enable checksum" option (2) on the tag or message archives ([Figure 3-5](#)).

Then you can verify after the fact whether archive data have been tampered with.

Use the available "HmiCheckLogIntegrity" program to verify the integrity of the records. For details on the program and/or "GMP", refer to the WinCC V17 system manual (TIA Portal) (see [\20\](#)).

Figure 3-5



Note

You can find the "HmiCheckLogIntegrity.exe" in the installation directory under: "SIEMENS > Automation > WinCC Runtime Advanced".

Additional information on the "GMP" option

The "GMP" option also lets you analyze potential operator errors.

In plant environments, the question is often:

- Who last operated the system?
- Who last modified parameters?
- Why were the changes made?

The "GMP" option provides answers to these questions.

Depending on the parameter assignment, a notification may appear on the Panel when a value is entered, for example. This notification window first requires a comment to be entered and the value change to be confirmed.

Remedy 2, "archiving on a network drive"

Instead of removable storage devices, archiving on a network drive offers more comprehensive access protection options ([Figure 3-6](#)).

If you specify a network drive as the archiving path, you can tightly regulate access by using the properties of a folder.

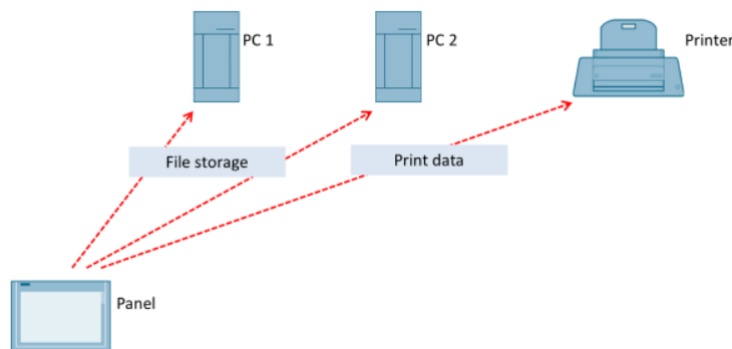
You can define access rights accordingly under the folder properties "Sharing" and "Security".

For more information on these settings, refer to the article

"Integrating HMI Operator Panels in TCP/IP Networks and data exchange via 'SIMATIC Option+ Manager'" (see [17](#)).

Figure 3-6

Integrating HMI Operator Panels in TCP/IP Networks



Notes

- The article "Integrating HMI Operator Panels in TCP/IP Networks and data exchange via 'SIMATIC Option+ Manager'" also describes how to implement data exchange between a PC and HMI device using SIMATIC Option+ Manager (see [17](#) in chapter 5).
- Network drives should **not** be used in the office network infrastructure. It is better to use a demilitarized zone (DMZ). For more information on this topic, see the article "Understanding and Using Firewall of Industrial Security Appliance SCALANCE S" (see [10](#)).
- Data loss may occur if the connection to the file server is lost or interrupted. An archiving process that is interrupted will not be automatically restarted.

3.8 Working with recipes

Recipes 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 recipes 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:
Significant damage to property can occur if the wrong recipe is selected. There is also the possibility of manually modifying individual parameters.

Remedy

You have access to various protective mechanisms when it comes to recipes.

- Operator input at the recipe view:
Make operator actions require an authorization. To do this, set up user management. Under the properties of the recipe display, select the "Properties > Security" menu and assign the object a permission level.
- Save location on a network drive:
If you specify a network drive as the storage location, you can tightly regulate access by using the properties of a folder.
You can define access rights accordingly under the folder properties "Sharing" and "Security". Information on these settings can be found in the article "Integrating HMI Operator Panels in TCP/IP Networks and data exchange via 'SIMATIC Option+ Manager'" (see [17](#)).

Alternative to Recipe View

Rather than using the default recipe view, use a custom recipe view that you assemble yourself. The functions for the "Recipe View" screen object can be found under the feature "Keyboard control for screen objects". For more information on this topic, see the article "WinCC flexible: Engineering with Recipes Using Integrated Functionalities" (see [18](#)).

You can then assign custom permissions to each button.

To do this, select the menu "Properties > Security" and assign the button a permission.

Detailed device overview here: [→](#)

3.9 Locking task switching

If you connect a USB keyboard to a Windows-based HMI device such as a Comfort Panel or a PC runtime system, then you can use keyboard shortcuts (keyboard combinations) to open and edit device settings on the Panel. One example is opening the Task Manager with the keyboard combination <Ctrl+Alt+Del>.

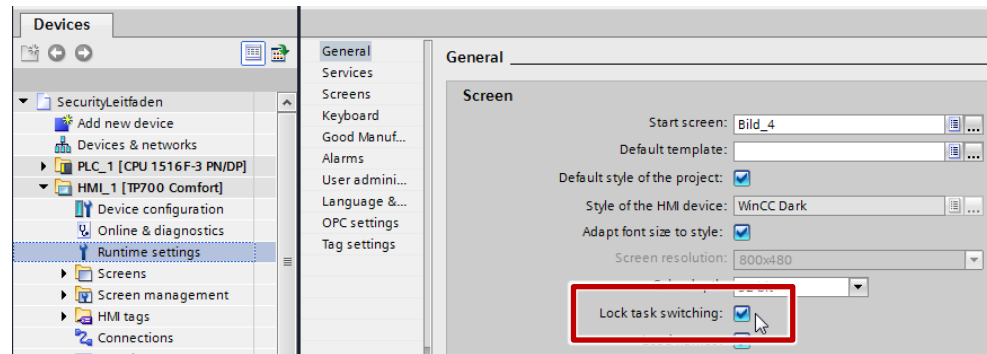
3.10 Project transfer

Remedy

Regardless of whether you are using a PC runtime of a Windows CE-based HMI device (Comfort Panel), disable the "Lock task switching" option in the configuration under the menu "Runtime settings" ([Figure 3-7](#)).

This prevents the user from launching another program or using the keyboard to call up the device settings or Control Panel.

Figure 3-7



Detailed device overview here: [=>](#)

3.10 Project transfer

The transfer of configuration data from the engineering PC to the HMI device is not encrypted. The data cannot be manipulated since the download files cannot be edited after the fact. You can take the following precautions to protect the confidentiality of the data.

Remedy 1: Establish a direct connection

Establish a direct connection between the engineering PC and the Panel. Alternatively, only interface with a secure network so as to prevent/minimize outside tampering.

Remedy 2: "Transport password" for private passkey

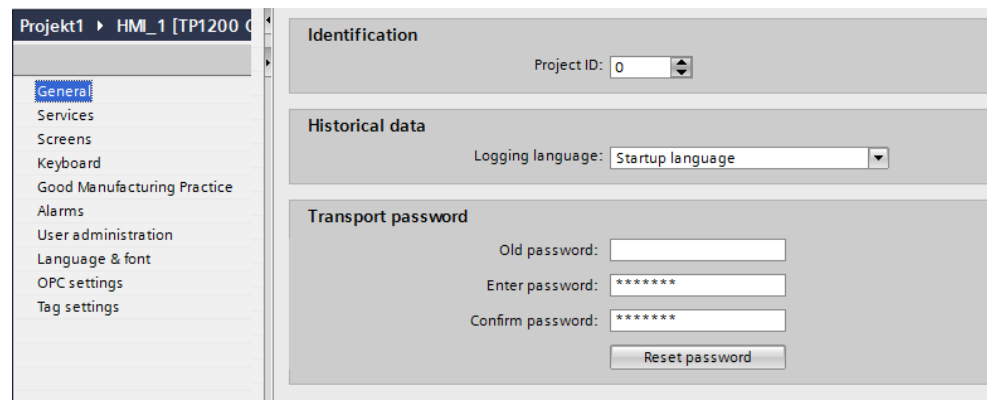
Connection setup to the CPU can be protected with access levels in TIA Portal. In this case, go to "Connections" in the HMI device and set an access password for connecting to the CPU.

Access passwords you have configured will be saved as private passkeys. When transferring to the HMI device, you can use a "transport password" to protect private passkeys against unauthorized access.

Open "Runtime settings > General" in the project tree to do this. You can set a password in the "Transport password" section ([Figure 3-8](#)).

3.11 Access to tags via OPC UA

Figure 3-8



When you transfer the configuration to the HMI device, a runtime dialog will appear and prompt you for the password. The dialog only appears if the configuration you are transferring contains an access password. Assuming the password you have entered is correct, a certificate for decrypting the passwords will be saved to the certificate store of the operator device. If you change a password, download the project with the new password to the operator device and launch the runtime. Because of the certificate that was saved earlier, the password prompt will not appear again.

More information can be found in the manual "SIMATIC STEP 7 Basic/Professional V17 and SIMATIC WinCC V17" ([\26](#)) in the chapter entitled "Password protection in runtime".

Detailed device overview here: [⇒](#)

3.11 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 is disabled by default. Do not use an unencrypted connection if you use this feature.

Remedy

Always make sure to use a secure connection for communication between client and server. Some examples are:

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

Only use the setting "none" if, for example, you are testing the OPC UA connection for the first time while commissioning.

An application example with various scenarios involving OPC UA can be found here: "Communication via OPC UA with SIMATIC HMI systems" [\18](#).

Detailed device overview here: [⇒](#)

3.12 Data exchange between HMI devices

You can exchange data between HMI devices using HTTP communication. One possible application of this could be an "overview page" that summarizes a selection of values from various HMI devices (similar to a control room).

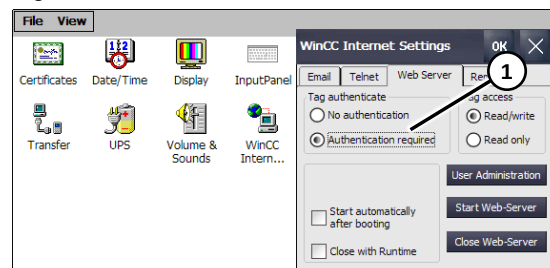
Transmission can be over `http://` and `https://`. With "`http://`" there is the risk that data could be modified or read from an unsecured connection, thus divulging "know how" (recipe parameters). Therefore, never use unencrypted communication.

Remedy

Use "`https://`" wherever possible. "HTTPS" allows for an encrypted connection (one that cannot be eavesdropped) between HMI devices. You can use the connection settings of the HTTPS client to define how the client verifies server certificates and reacts to any errors.

To accomplish this, select the option "Authentication required" (1) under the "WinCC Internet Settings" icon in the device settings ([Figure 3-9](#)).

Figure 3-9



Detailed device overview here: [⇒](#)

3.13 Remote access to a Panel's tags via Excel

The "Simple Object Access Protocol" (SOAP) web service lets you access the tags on an HMI device via Ethernet from an external application such as Excel.

In this example, the external Excel application contains a VBA script that performs the login to the server (Comfort Panel).

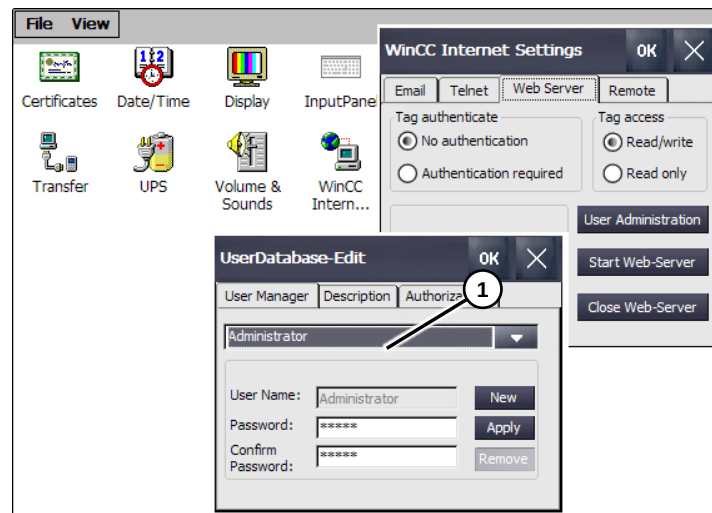
There is a risk that third parties may clandestinely make changes to parameters.

Remedy

In the device settings under the icon "WinCC Internet Settings", you can set the required login credentials (1) for the external application ([Figure 3-10](#)). This prevents access to the tags on the Panel from the Excel application without first logging on. Note that the connection is unencrypted.

3.14 Sending emails via the Panel

Figure 3-10



There is a FAQ on this topic entitled "How do you read out or write tag values with an Excel application?" (see [4.1](#)).

So that only authorized persons have access to the device settings, follow the recommendations in chapter [4.2](#) "Protecting the Start Center against unauthorized operator actions".

Detailed device overview here: [→](#)

3.14 Sending emails via the Panel

Not all machines in a plant can be monitored by personnel at all times. Consequently, it is often not possible to respond promptly to pending messages on the HMI device.

Email notifications represent a possible solution to this challenge. Emails are sent via SMTP communication.

In this context, make sure that emails cannot be eavesdropped by third parties.

Remedy

When configuring the email program, make sure to implement encryption with "SSL" or "TLS".

Information on this topic can be found in the application example "Toolbox for HMI Projects" in the chapter entitled "Transferring data - sending emails" (see [4.9](#)).

Detailed device overview here: [→](#)

3.15 TIA Portal Multiuser Engineering

With Multiuser Engineering in TIA Portal, you can work on a project with multiple users simultaneously. By working on multiple objects in parallel within one multiuser project, you can significantly reduce configuration times.

3.16 TIA Portal Cloud Connector

In order to work with Multiuser Engineering, a network must already be set with the appropriate Windows settings, IP addresses, firewalls, etc.

"TIA Portal Multiuser Server" defines permissions for working with

- Multiuser Server connections,
- Multiuser projects and
- local sessions

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

For details on this topic, refer to the application example "Multiuser Engineering with TIA Portal Project Server" (see [\23\](#)).

Detailed device overview here: [→](#)

3.16 TIA Portal Cloud Connector

TIA Portal Cloud Connector grants you central administration of engineering software on one server. From one engineering station, you can work via remote desktop connection with the instance of TIA Portal installed on the server. TIA Portal Cloud Connector serves as the communication tunnel in this context.

TIA Portal Cloud Connector supports secure connections via HTTPS as of Windows 8.1.

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

The following certificates are necessary in order to establish a connection between a user and a remote device:

- Certificate for data encryption
- Certificate for user authentication

If a certificate is not present or if the certificates of the user and the remote device do not match, no connection is possible.

Details on this topic can be found in the application example "Working with the TIA Portal Cloud Connector" (see [\24\](#)).

Detailed device overview here: [→](#)

3.17 User Management Component (UMC)

UMC (User Management Component) is a database for the central administration of user data.

You can add global users and user groups to a project once they have been created in UMC (User Management Component). This lets these users and user groups work with the project if they have been assigned the corresponding permissions.

If a user needs to access multiple protected projects, minimize your administrative overhead by adding that user in each project, either individually as a global user or together with a user group. Global users can be managed in UMC. Changes propagate to all projects that these users or user groups belong to.

You have the option of synchronizing the user management in TIA Portal with UMC so that inconsistencies do not occur when users or user groups are modified in

3.18 RFID user management

UMC. In order to find out whether synchronization is necessary, you can check the synchronization status.

User Management Component:

- Centralized, cross-project management of users in the plant.
- Management of user groups.
- Importing Windows users and user groups is possible.
- Efficient administration of users/user groups in a plant.
- Failure safety thanks to redundant UMC domain design.
- Load distribution of login request spikes thanks to multiple UMC stations in a UMC domain.
- Licensing based on the number of users.

For details on this topic, refer to the application example on UMC (see [\27\](#)) or the STEP 7/WinCC "Programming and operating manual" (see [\26\](#)). Alternatively, you can find more information in the WinCC (TIA Portal) information system. Search for: "User Management Component" => "Managing global users and user groups".

The installation file for UMC and the English-language documentation for UMC can be found on the TIA Portal installation media ("..\support", "...Documents\Readme\English").

It is highly recommended to read in full the UMC documentation before using the user management feature, especially the sections on "Secure Application Data Support (SADS)". SADS is strictly required in order to use the user management feature in TIA Portal.

Detailed device overview here: [➔](#)

3.18 RFID user management

Unauthorized personnel and consequent operator error open the door to interruptions in production operations. To prevent this, it is recommended to set up an access restriction to system functions so that only authorized persons have access.

SIEMENS offers two systems that can automatically log in users:

1. User login to HMI devices with RFID card reader.
2. User login to HMI devices via RFID and the Sirius ACT ID key-operated switch.

In the **first** scenario, RFID card-based user management is implemented using the "PM-LOGON Basic" software, integrated in SIMATIC HMI Option+ (see chapter [4.6](#)). Here, a user holds his card to a reader and is then logged into the WinCC Advanced Runtime. The UID of the card serves as a password.

Details on this topic can be found in the application example "SIMATIC HMI Option+" in the chapter entitled "RFID logon" (see [\22\](#)).

In the **second** scenario, an electronic "ID key switch" is used. Keys possessing different encodings allow the switch to move between up to four switch positions. 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 as a "password" to the user in the user management.

3.18 RFID user management

In order to perform an operation on the HMI device, the plant operator first inserts his ID key into the ID key switch.

If the ID number it reads matches the ID number stored in the user management, the assigned function is allowed.

Details on this topic can be found in the application example "User login on HMI operator panels via RFID and the SIRIUS ACT ID Key Switch" (see [\25\](#)).

Advantages

Both systems have the following features in common:

- Automatic user login on the HMI device. This avoids incorrect entries of user names and passwords.
- Easy login even under unfavorable conditions, e.g. when the operator is wearing work gloves.
- High flexibility (e.g. changing user data)

Note

Due to the simple nature of the login process, place particular importance on secure storage of the keys to prevent unauthorized persons from accessing the plant.

Detailed device overview here: [→](#)

4 Risk analysis when operating the Panel

General note on operating a plant

The safe operation of a plant requires a high degree of security with respect to the person in front of the Panel.

Some examples are:

- Modification or specification of values by unauthorized persons (e.g. entering speed setpoints 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 Panel operation from unauthorized access. It also shows how you can prevent tampering with device settings.

4.1 Operation of configured plant screens

Plant screens of the operator devices are used, for example, to switch drives on and off. Unauthorized operator actions can cause significant damage.

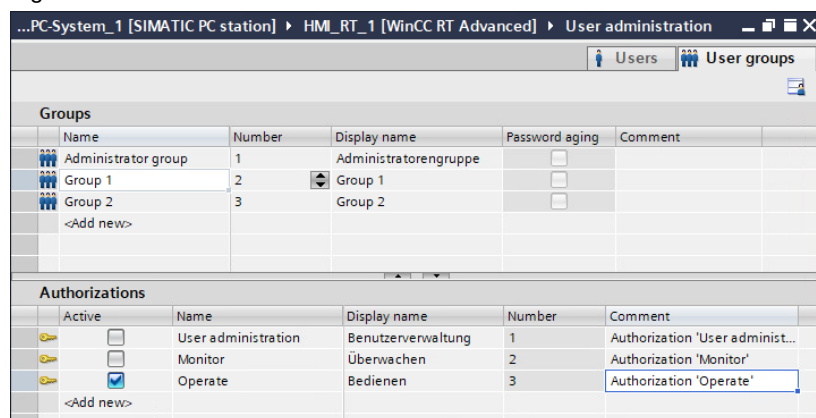
Remedy

To limit operator actions to authorized operators, individual functions can be set up with permissions. This can ensure that only authorized persons can enter values at a Panel, for instance.

Users (operators / maintenance personnel) are assigned to groups via the "User administration" system function ([Figure 4-1](#)).

You can structure the groups so that, for example, "Group 1" contains only persons who will operate the plant, but who cannot modify values. Then, for example, you can populate "Group 2" with persons who have full access to the Panel's controls.

Figure 4-1



The screenshot shows the 'User administration' window in SIMATIC Manager. It has two tabs: 'Users' and 'User groups'. The 'User groups' tab is active, showing a table of groups and a table of authorizations.

Name	Number	Display name	Password aging	Comment
Administrator group	1	Administratorengruppe	☐	
Group 1	2	Group 1	☐	
Group 2	3	Group 2	☐	
<Add new>				

Active	Name	Display name	Number	Comment
☐	User administration	Benutzerverwaltung	1	Authorization 'User administr...
☐	Monitor	Überwachen	2	Authorization 'Monitor'
☒	Operate	Bedienen	3	Authorization 'Operate'
<Add new>				

Detailed information on how to set up user management can be found in the Online Help and in the TIA Portal user manual (see [chapter 7](#)).

Detailed device overview here: [➔](#)

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

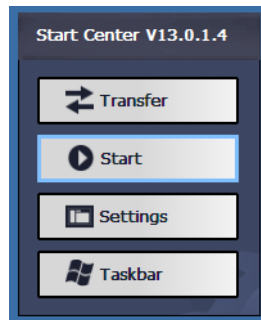
The "Start Center" menu appears by default after the Panel is turned on, or after runtime is shut down ([Figure 4-2](#)).

Press the "Settings" button to access the Panel device settings and modify them.

Press the "Taskbar" button to activate the taskbar, which in turn allows you to call up the Windows CE desktop.

If no settings are changed, individuals inside your plant have access to the functions mentioned above.

Figure 4-2



Remedy

You can protect the "Start Center" against unauthorized operation with the help of a password.

If you protect the "Start Center" with a password, "SecureMode" is automatically enabled ([Figure 4-3](#)).

The "Start Center" now requires a password to operate. "SecureMode" additionally protects the taskbar and the Windows CE desktop.

Figure 4-3



The "Transfer" and "Start" buttons can still be pressed without entering a password.

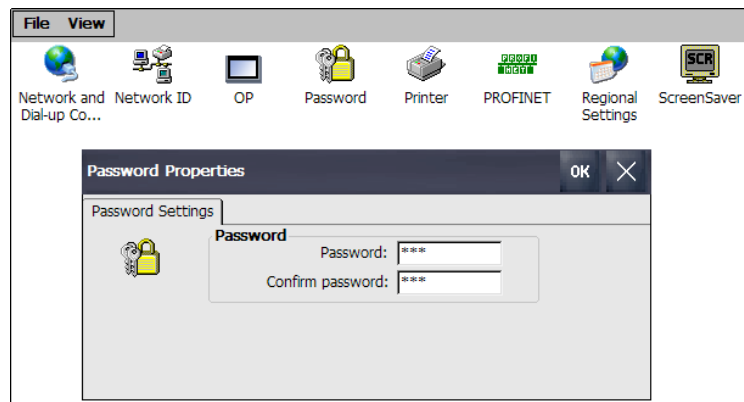
Enable "SecureMode"

In the device settings, open the "Password" icon, then enter a password. To disable, go back to the function and delete anything that was entered in the "Password Settings" window ([Figure 4-4](#)).

Further details can be found in the Panel device manual.

For advice on setting up a secure password, see chapter [1.4](#).

Figure 4-4



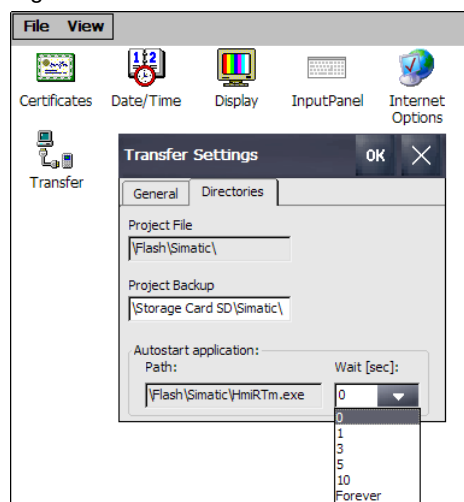
Panel autostart

As an additional safeguard, you can define the wait time until the Panel runtime starts. Do this in the Panel device settings under the "Transfer" icon. The "Start Center" menu will appear during this wait time.

For autostart, set the wait time to "0 seconds" ([Figure 4-5](#)).

After the panel is restarted, the runtime will now be shown right away, without displaying the "Start Center".

Figure 4-5



CAUTION

Make sure to add a button to the configuration with the system function "StopRuntime". Otherwise, you will have no way of returning to the "Start Center" menu.

If you forgot a button with the "StopRuntime" system function, then refer to the article entitled "How do you switch an operator panel to transfer mode when the autostart's timeout is set to 0 seconds?" (see [13](#)).

Detailed device overview here: [→](#)

4.3 Terminating the HMI runtime

Before shutting off the Panel, 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".

If the Panel runtime is terminated too early, for example due to an automatic shutdown of the Panel runtime upon starting a project transfer, then the plant component will no longer be operable using the Panel. The "Start Center" appear after the runtime shuts down.

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".

See the steps in chapter [4.2](#) "Start Center" / "Loader Menu" start menu" for how to do this. You can also prevent the Panel runtime from being terminated automatically. For how to do this, see chapter [3.3](#) "Transferring configuration to the Panel".

Detailed device overview here: [➡](#)

4.4 Generating and transferring a Pack&Go file

If you have no way of connecting the operator device with your engineering PC, then you can generate a Pack&Go file.

The configuration file will then be available as a ZIP file.

Remedy

To prevent unauthorized persons from using this ZIP file, archive it one more time and give the new ZIP file a password.

Detailed device overview here: [➡](#)

4.5 Backup and restoration of Panel data

The "Backup / Restore" and "Service & Commissioning" functions can be found in the Panel device settings.

The former can be used for backup and restoration purposes.

Backup & restore

It is possible to perform a full backup of the Panel data via this menu. 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.

4.5 Backup and restoration of Panel data

Operating system (OS) update via removable storage devices

This function can be used to perform a Panel operating system update. This deletes the existing configuration. The panel then receives no more configuration data.

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

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).

There is a special slot for the system storage card dedicated for this purpose.

For a detailed description, refer to the application example "Backup/restore options for SIMATIC HMI Panels" (see [51](#)).

If access to the storage card locations is open to all and there is access to the device settings on the Panel, then its functioning 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").

Remedy

To prevent unauthorized persons from gaining access to the device settings, follow the recommendations in chapter [4.2](#) "'Start Center" / "Loader Menu" start menu'. Moreover, you can prevent access to storage media with architectural measures, for example by installing the Panel in a lockable control cabinet.

Detailed device overview here: [⇒](#)

4.6 SIMATIC HMI Option+

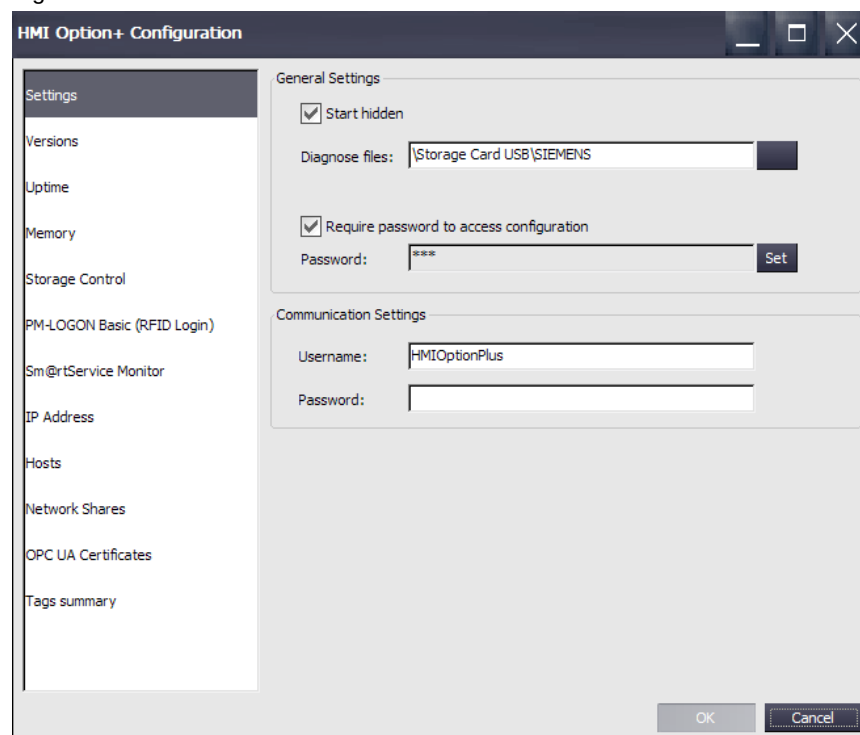
From WinCC (TIA Portal) V15 onward, you can use the "SIMATIC HMI Option+" tool. This tool provides functions that allow you to change various properties of the HMI device. The security-related functions will now be described in detail. Specific information on the individual parameters is listed in the application example "SIMATIC HMI Option+" (see [\22\](#)).

In order to use SIMATIC HMI Option+, the following steps must be carried out for the initial commissioning:

1. Install SIMATIC HMI Option+ on an engineering computer.
2. Transfer SIMATIC HMI Option+ to the operator device using SIMATIC ProSave.
3. Activate essential communications services on the HMI device.
 - a. With SIMATIC HMI Option+ V1, communication runs over the "SOAP" web service (see also chapter [5.2.4](#), "SOAP web service").
 - b. With SIMATIC HMI Option+ V2 onward, communication runs over OPC UA.

[Figure 4-6](#) shows the "SIMATIC HMI Option+ Configuration" view on the operator device.

Figure 4-6



4.6.1 Features

Note

The feature set depends on the HMI Option+ software version you are using. Unless otherwise specified in the title, the following features can be used as of HMI Option+ V1.

"Settings" function

You can use the "Start hidden" checkbox (1) to define how "HMI Option+ Configuration" will start up.

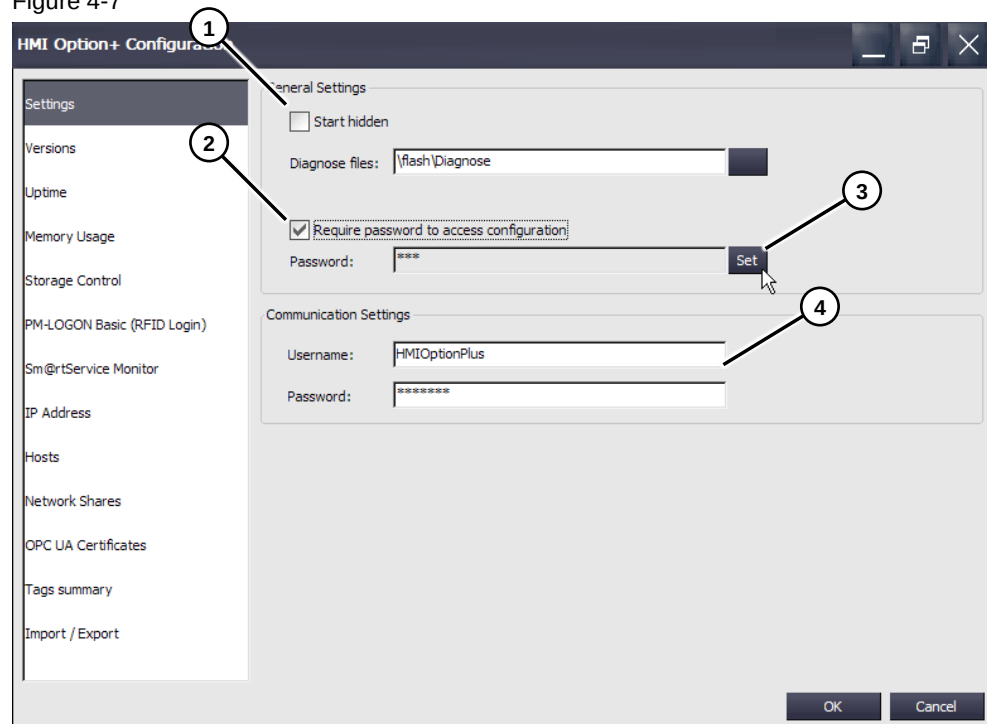
"Start hidden" enabled → Configuration always launches in the background.

To prevent unauthorized persons from making changes to parameters, tick the checkbox "Require password to access configuration" (2). An existing password can be updated with the "Set" button (3).

Depending on the service you are using to exchange data, you will modify the respective settings in the "Communication Settings" section (4):

- HMI Option+ V1, "SOAP" web service: Enter the username and password that you defined on the operator device.
- HMI Option+ V2 onward, OPC UA server: Enter the address of the OPC UA server here and, if necessary, the port.

Figure 4-7



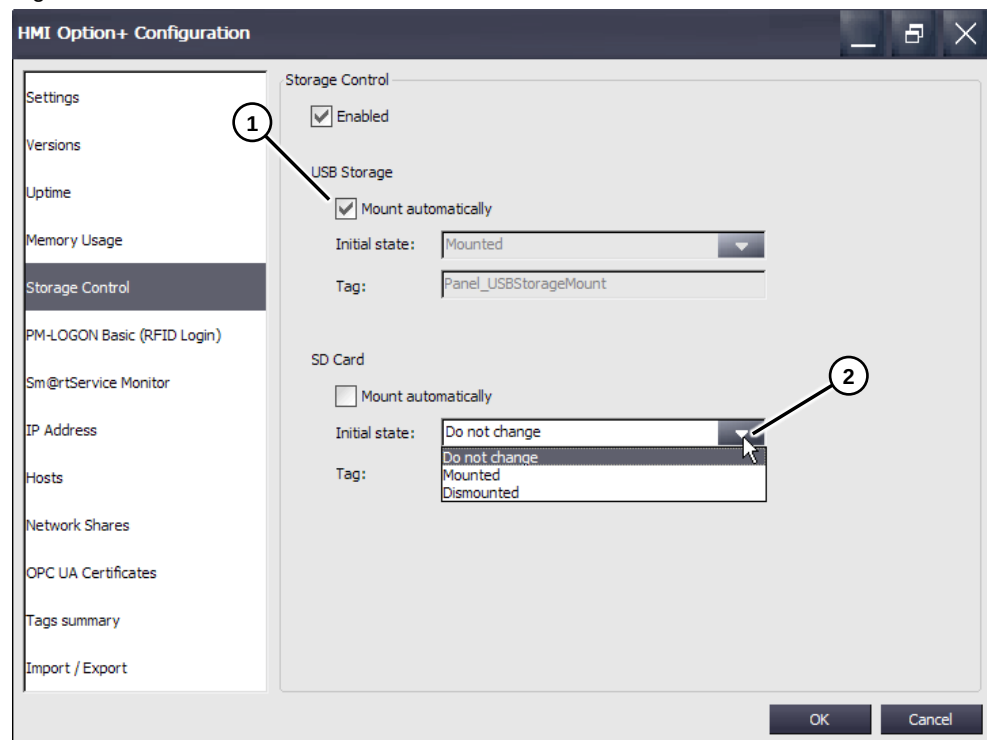
Detailed device overview here: [→](#)

"Storage Control" function

You can use the "Mount automatically" checkbox (1) to define whether an inserted USB drive or SD card will be automatically recognized by the system or not. Should an unauthorized USB drive be inserted, you can use this function to prevent data from being downloaded from the Panel or software (such as a virus) from being secretly transferred to the Panel.

Use the dropdown list (2) to set whether the Panel will respond to the presence of an external storage device when it restarts. The setting can be defined "manually" with the dropdown list or "dynamically" with a tag from the runtime.

Figure 4-8



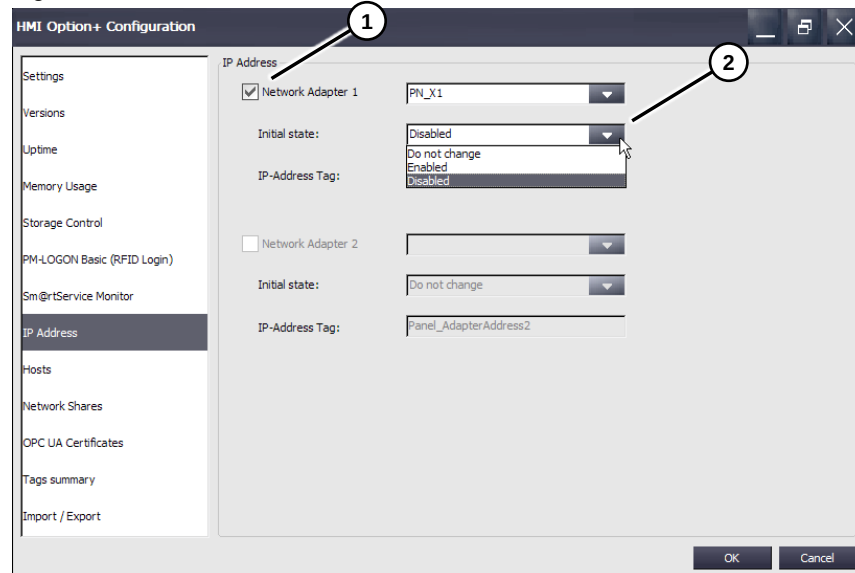
Detailed device overview here: [➔](#)

"IP Address" function

This function can be used to enable or disable the network interfaces (1).

Specify the behavior of the network interface via the dropdown list (2). The setting can be defined "manually" with the dropdown list or "dynamically" with a tag from the runtime.

Figure 4-9



Detailed device overview here: [⇒](#)

"PM-LOGON Basic" function (RFID logon)

Using the function "PM-LOGON Basic (RFID Logon)", you have the ability to authenticate at the Comfort Panel with an RFID card. To do this, a user holds his RFID card to a reader and is then logged into the Comfort Panel runtime. The unique ID (short: UID) of the card is used as a password for this purpose.

Configuration details can be found in the documentation for "SIMATIC HMI Option+". See [\22\](#).

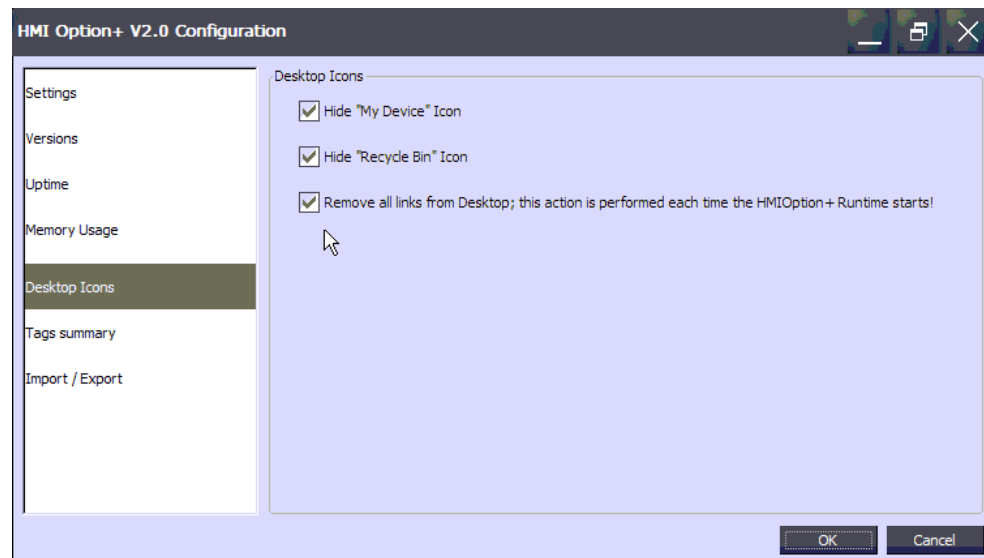
"Desktop Icons" function (show/hide desktop icons) - HMI Option+ V2 onward

The function "Desktop Icons" lets you hide the icons on the Windows CE desktop of the SIMATIC HMI Comfort Panel. You have three options in this case (see [Figure 4-10](#)):

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

Details can be found in the documentation on "SIMATIC HMI Option+". See [\22\](#).

Figure 4-10



Detailed device overview here: [⇒](#)

4.6.2 Remote access and logon security

"Sm@rtService Monitor" function (remote access monitoring)

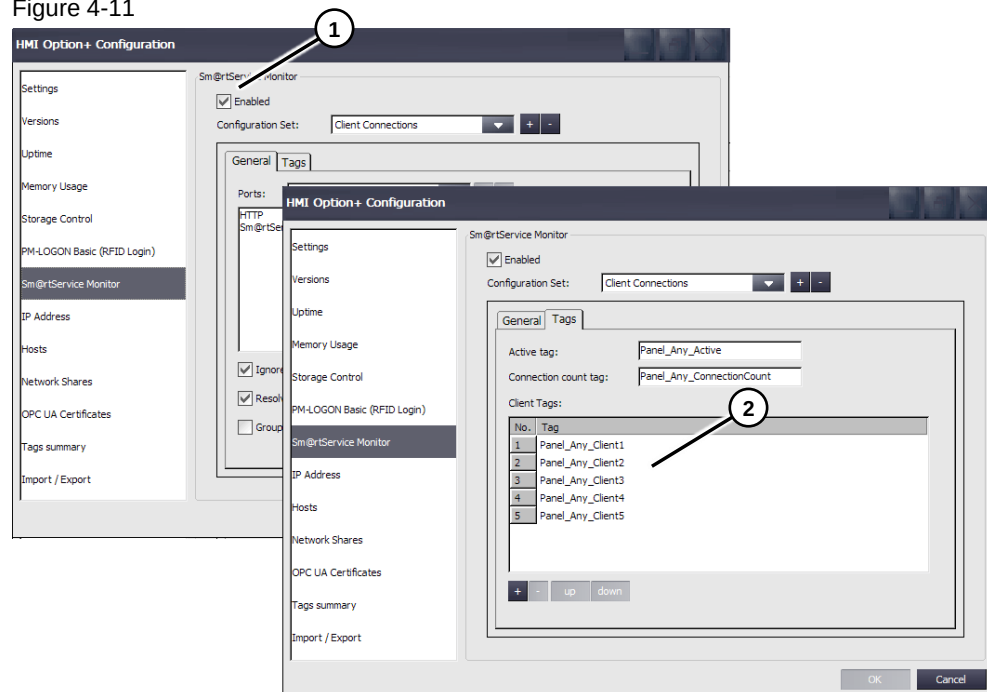
The "Sm@rtService Monitor" function, which in the past was available separately, has been developed further and is integrated into SIMATIC HMI Option+.

Connections that access the device (e.g. Sm@rtClient) can be cyclically polled with the help of "Sm@rtService Monitor".

The connection parameters detected (IP address, hostname) are written to tags of the Comfort Panel runtime, thereby making it easy to archive them. In this way it is possible to determine, for instance, which and how many Sm@rtClients are accessing the HMI.

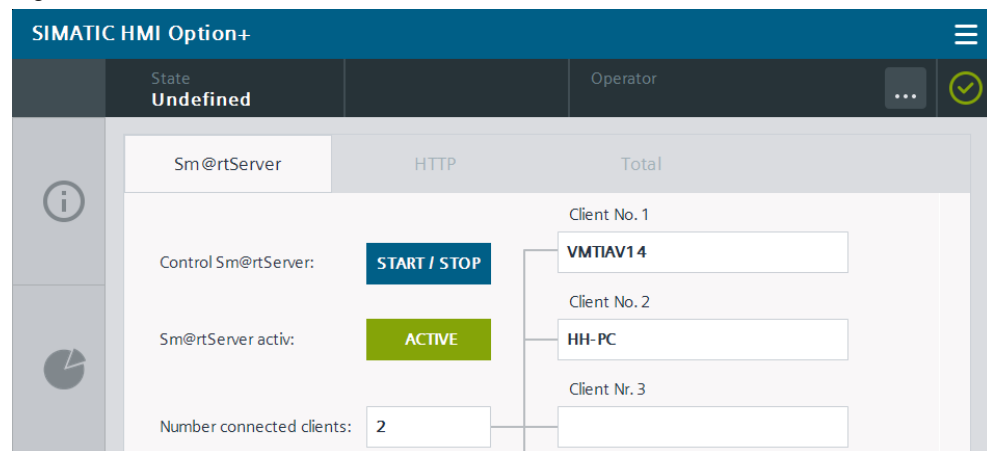
Enable the "Sm@rtService Monitor" function (1). You can now analyze the names and number of clients that are connected with the server. You can use tags (2) to define which information you will output.

Figure 4-11



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

Figure 4-12



This feature gives you fine control and logging across all connected remote participants.

If you logged in at the operator device on site, it can occur that a user connects to the same operator device simultaneously via Sm@rtClient connection. The Sm@rtClient user is now logged in with your login credentials and has your permission level for the system.

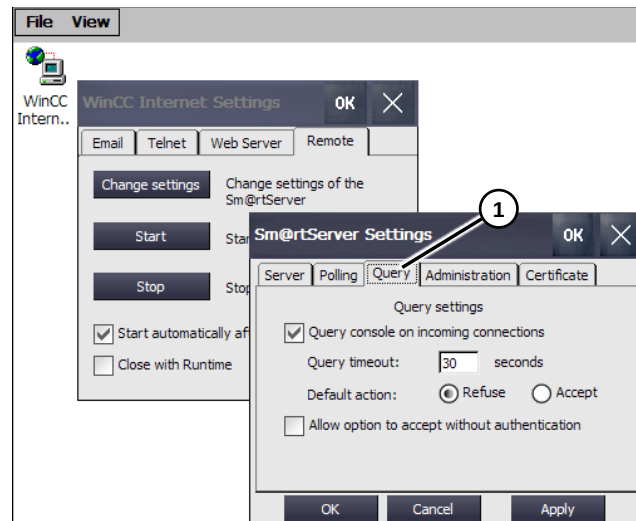
A corresponding safeguard, the "Sm@rtService Monitor" function, is built in to prevent this as of HMI Option+ V2. The active local user will be logged off if a remote connection is active.

Configuration details can be found in the documentation for "SIMATIC HMI Option+". See [\22\](#).

Login security

To increase login security with regard to remote access, you can enable an option (1) in the "Sm@rtServer Settings" (in this example, on the HMI device) which will cause the server (HMI device) to display an additional window when a client (such as a PC) wishes to connect with the server.

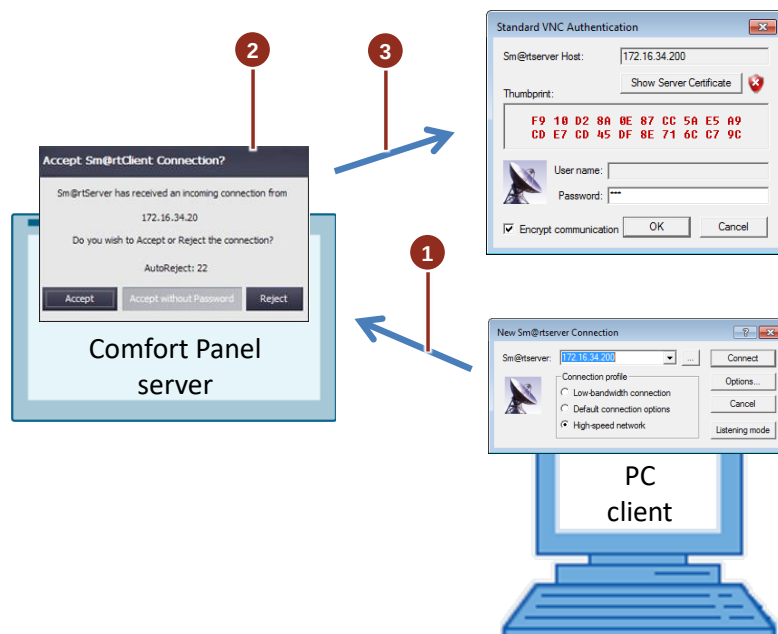
Figure 4-13



Runtime behavior

Before a client connects to the server (1), a screen will appear with a supplementary prompt (2) on the server. This screen shows, among other things, the IP address of the client. You can permit or deny the access attempt. If access has been granted, the login will proceed (3).

Figure 4-14



5 Risk analysis when using remote maintenance services

5.1 Background information

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

Even with password-protected remote access, there is still the risk that someone will sign in with another person's login information and perform operator actions.

Moreover, the logged-in operator has view of the plant. Should operator actions be carried out by remote access in this scenario, this can have severe consequences.

Outside intervention must not cause any risk to personnel on site or to the plant itself. Thus, it is important to block remote maintenance users from accessing certain functions (such as manual control of a gripper arm). In addition, on-site personnel must be informed of remote access, and they must be able to terminate it at any time if needed.

Next, it is necessary to ensure that only authorized persons obtain access to the plant. Unfortunately, perfect network security is impossible to guarantee in today's world. Therefore it is prudent for personnel to be informed not only of the remote access event *per se* but also of the person carrying out the remote access.

For more information, refer to the article entitled "Remote access to SIMATIC HMI Operator Panels" (see [111](#)).

Network security – for secure industrial communication

Securing your network against unauthorized access is of utmost importance if you wish to avoid incalculable risks.

Defense in depth

To ensure comprehensive protection of industrial systems from internal and external cyber attacks, precautions must be taken on all levels simultaneously – from the plant level to the field level, from access control to copy protection.

This is why Siemens' approach to comprehensive protection offers defense throughout all levels – "defense in depth", according to the recommendations of ISA99 / IEC 62443, the leading standard for security in industrial automation.

See also chapter [1.5](#) "Operational security guideline".

5.2 Use of Sm@rt options

5.2.1 General

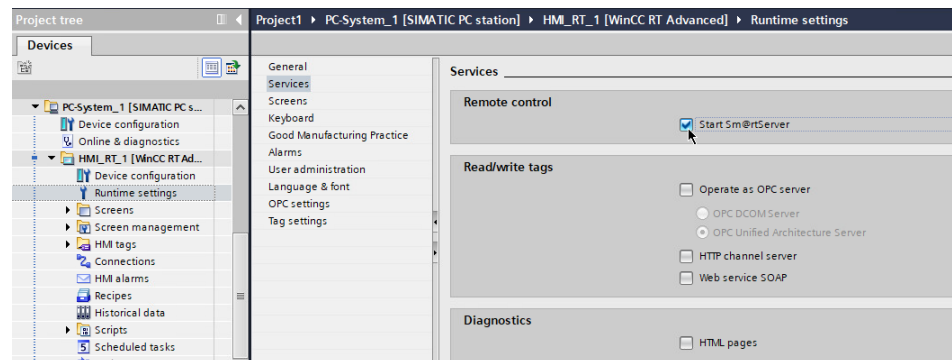
WinCC services let you use TCP/IP connections (e.g. LAN) to implement communication between a PCs and HMI systems.

Some sample applications include:

- Remote control of an HMI system over the internet, intranet or LAN.
- Send emails based on messages and events.
- Standard HTML pages on the HMI system that provide service / maintenance information and diagnostic functions.

These services can be enabled in the project tree of the HMI configuration under "Runtime settings > Services" ([Figure 5-1](#)).

Figure 5-1



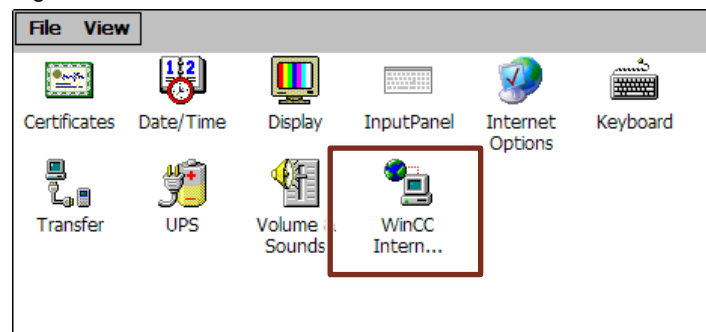
Use of "Sm@rt options" entails risks as described in chapter [5.1](#) "Background information".

Remedy

Settings on the Panel

You can change settings for secure access with a Comfort Panel in the device settings, under the "WinCC Internet Settings" icon ([Figure 5-2](#)) (Basic Panels differ in this respect; see manual).

Figure 5-2



For details on the individual parameters, refer to the WinCC system manuals for SIMATIC Basic, Comfort or Advanced (see [\12\](#), [\19\](#) and [\20\](#)).

5.2 Use of Sm@rt options

To prevent unauthorized access to the Panel device settings, refer to chapter [4.2](#) "'Start Center" / "Loader Menu" start menu'.

5.2.2 SmartService monitor

The "Sm@rtServiceMonitor" tool (for Comfort Panel only) detects the current Sm@rtClient connections and provides them to the HMI runtime where these data can be processed for other purposes. This allows remote access to be monitored and, if necessary, prevented by the operator onsite.

For an application example on this topic, see "Remote Access to SIMATIC HMI Operator Panels" ([11](#)).

5.2.3 VPN for SmartService

Access to a remote operator device be over the internet.

To prevent unauthorized persons from gaining access to the operator device and/or data in transmission, you will need to configure a secure connection.

The following application examples demonstrate VPN-based solutions.

- "Remote access to SIMATIC HMI Operator Panels" [11](#).
- "SIMATIC WinCC SmartClient.exe remote maintenance for SIMATIC HMI" [16](#).
- "Setting up a secure VPN Connection between SINEMA Remote Connect Client, SCALANCE SC and SINEMA Remote Connect Server" [17](#).

5.2.4 SOAP web service

The "SOAP" web service is used to

- interface with the Office ecosystem. For example, MS Excel in combination with a VBA script can be used to obtain read/write access to the tags of an operator device.

For this purpose, the HMI device must support the SOAP web service.

For an application example on this topic, see [21](#).

The SOAP web service

- facilitates the use of the "SIMATIC HMI Option+" tool (see chapter [4.6](#), "SIMATIC HMI Option+ V1").

Enable the SOAP web service under "Runtime settings > Services > Read/write tags" on the operator device.

Detailed device overview here: [→](#)

5.3 SIMATIC apps

Access to automation systems with mobile end devices

Mobile end-user devices such as smartphones and tablets are ubiquitous in private life, supplying us with information and services.

The functional scope of Siemens automation and drive products has now been expanded with apps.

- **SIMATIC WinCC Sm@rtClient app**
Encrypted, mobile remote monitoring and control of SIMATIC HMI systems via industrial WLAN in conjunction with SIMATIC Sm@rtServer.
- **SIMATIC S7 app**
Secure connection to the web server of your SIMATIC S7-1200/1500 and ET 200SP.
- **LOGO! app**
Monitoring and control of LOGO! 0BA7 and 0BA8 via smart devices.
- **SIMATIC Notifier app**
Monitoring of your plant, production line or machine with mobile end-user devices such as smart watches, smartphones, tablets, etc. in conjunction with an OPC UA server – or via S7 Plus or S7 Classic connections.

Security considerations

Security considerations are required on different levels.

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

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.

Remedy

Smartphone security

The points listed below will help you protect your smartphone against unauthorized use or misappropriation of data in the event of loss or theft.

- Use a PIN or password to unlock your smartphone. Don't use gestures or a simple swipe to unlock the device.

5.3 SIMATIC apps

- 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.

App security features

The following app-based settings will increase security.

Sm@rtClient app

- Enable encrypted communication (only in the full version!).

Note

Encrypted communication requires more resources on the Sm@rtServer (operator device) and on the smartphone. This can increase screen rendering times.

- Have the app remember profile data but do not remember a password. This way, the password must be entered manually each time.
- Enable the app password to launch the app. You will be prompted to do this when you open the app for the first time. Alternatively, navigate to "Settings > Change password".

SIMATIC S7 app and LOGO! app

- Enable encrypted communication (for all S7 controllers and with the LOGO! 0BA8).
If you are using a LOGO! 0BA7, then it is strongly recommended to consider additional mechanisms such as a VPN.
- Enable the password prompt to launch the app. You will be prompted to do this when you open the app for the first time. Alternatively, navigate to "Settings > Change password".
- Have the app remember profile data for accessing the web server of the controller or LOGO! device, but do not remember a password. This way, the password must be entered manually each time.

5.3 SIMATIC apps

SIMATIC Notifier app

- Enable the password prompt to launch the app. Navigate to "Settings > Security > Use an app password" and set a password. Select at least the "Medium" security level so that your password will be requested each time you open the app. If your smartphone has the necessary hardware, biometric authentication can also be used.
- To prevent unauthorized connection attempts, do not divulge the notifier ID of the mobile device to unauthorized parties.

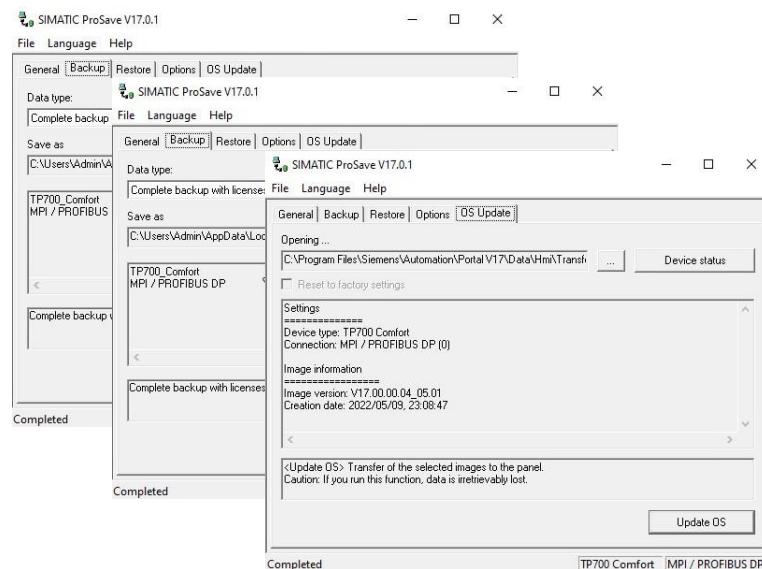
Detailed device overview here: [→](#)

5.4 ProSave

You can perform a variety of functions with the ProSave software ([Figure 5-3](#)). Some examples are:

- Creating backups:
 - Back up the configuration file.
 - Back up user management.
 - Back up recipes.
- Restore function:
 - Restore the configuration file.
 - Restore user management.
 - Restore recipes.
- Transfer options
 - e.g. "SIMATIC HMI Option+"
 - or printer drivers...
- OS update

Figure 5-3



So that unauthorized persons cannot use "ProSave" to download or otherwise manipulate project data, some countermeasures are described below.

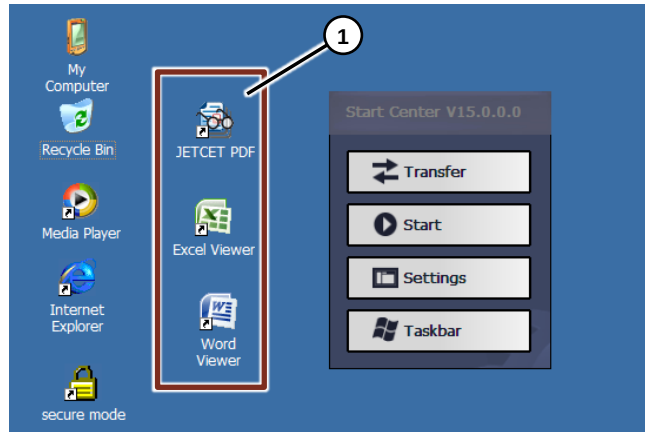
Remedy

- The functions in "ProSave" require the Panel runtime be terminated first. Therefore, make sure that the Panel runtime cannot be terminated automatically but rather only by authorized persons. Further information can be found in chapter [3.3](#) "Transferring configuration to the Panel".
- For example, the IP address of the Panel must be specified in the connection parameters. If it is unknown, then a connection cannot be established to the Panel. Therefore, make sure that the device settings cannot be accessed to change the Ethernet settings. More information can be found in chapter [4.2](#) "'Start Center' / 'Loader Menu' start menu'".

Uninstall WORD and EXCEL viewer

Comfort Panels have the "WORD, EXCEL and PDF" viewers pre-installed. It is possible, for example, that a WORD file can silently run a script and cause damage (1).

Figure 5-4



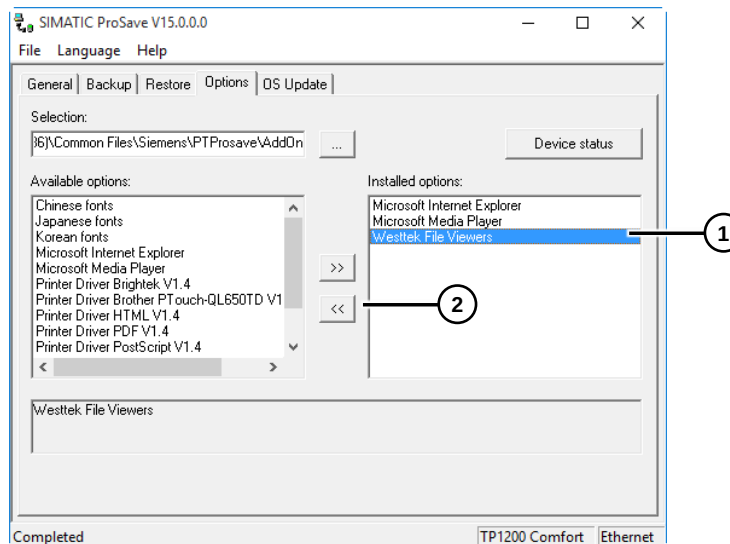
As of WinCC (TIA Portal) V15, you can uninstall the WORD, EXCEL and PDF viewers on the Comfort Panels.

Use the "ProSave" software to uninstall them.

Select the option "Westtek File Viewers" (1) in the "Options > Installed options" tab.

The "<<" button (2) removes the option from the operator device. You can transfer the option back if necessary.

Figure 5-5



Detailed device overview here: [→](#)

5.5 Ports used by operator devices

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, note that doing so can open security holes.

Remedy

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

A list of ports can be found in the Online Help for WinCC (TIA Portal). See the tab "Contents > Readme > WinCC Comfort/Advanced > Security information".

For further information, also refer to the article entitled "Which ports are used by WinCC Advanced...?" (see [14](#)).

Detailed device overview here: [→](#)

6 Hardware risk analysis

6.1 External storage devices

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 slots is often very easy. Sensitive data can be easily lost or modified as a result. See also chapter [1.5.1](#) "Protection of machines and plants". There is also the possibility that the wrong program could be transferred to the Panel in this way. For more on this, see chapter [4.5](#) "Backup and restoration of Panel data".

Remedy

A USB port lock can be used on the USB port. You should also use a lockable control cabinet to safeguard other media, such as SD cards, against unauthorized access. Alternatively, you can store data on a PC via the network. For more on this see chapter [3.7](#) "Archiving of tags and messages".

Detailed device overview here: [→](#)

6.2 Device communication interfaces

Access to communication ports entails similar considerations to those described in chapter [6.1](#). The risk in this case lies, among other things, in the loss of operability, e.g. if the Ethernet connection is pulled out. A more significant risk is that communication may be recorded or tampered with, for example when new components are added.

Remedy

Use architectural measures to prevent access, for example by installing the Panel in a lockable control cabinet.

Detailed device overview here: [→](#)

6.3 WLAN / 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 WLAN/LAN network.

There are also a multitude of network configurations to consider.

Some examples are:

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

Remedy

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" ([16](#)).

Using simple test networks, here you can learn how to work with the security modules and the "Security Configuration Tool". Learn how to implement the security features of security modules in the network with minimal configuration effort.

Detailed device overview here: [→](#)

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.	Topic
\1\	Siemens Industry Online Support http://support.industry.siemens.com
\2\	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/de/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 "Backup/restore options for SIMATIC HMI Operator Panels" https://support.industry.siemens.com/cs/ww/en/view/68373729
\6\	Manual: "SIMATIC NET Industrial Ethernet Security Setting up security" https://support.industry.siemens.com/cs/ww/en/view/109742841
\7\	Application example: "Integrating HMI Operator Panels in TCP/IP Networks and data exchange via 'SIMATIC Option+ Manager'" https://support.industry.siemens.com/cs/ww/en/view/92346478
\8\	Application example: "WinCC flexible: Engineering with Recipes Using Integrated Functionalities" https://support.industry.siemens.com/cs/ww/en/view/23901413
\9\	Application example: "Toolbox for HMI projects" – Transferring data – Sending emails https://support.industry.siemens.com/cs/ww/en/view/106226404
\10\	Application example: "Understanding and Using Firewall of Industrial Security Appliance SCALANCE S" 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\	"Cybersecurity for Industry" topic area https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html

No.	Topic
\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\	Download: "SIMATIC WinCC SmartClient.exe remote maintenance for SIMATIC HMI" https://support.industry.siemens.com/cs/ww/en/view/109482434
\17\	Application example: "Setting up a secure VPN Connection between SINEMA Remote Connect Client, SCALANCE SC and SINEMA Remote Connect Server" https://support.industry.siemens.com/cs/ww/en/view/109479599
\18\	Application example: "Communication over OPC UA with SIMATIC HMI systems (Comfort Panels, Runtime Advanced, Runtime Professional)" https://support.industry.siemens.com/cs/de/en/view/63481236
\19\	Manual: "SIMATIC HMI operator devices - Basic Panels 2nd Generation" https://support.industry.siemens.com/cs/ww/en/view/90114350
\20\	System manual: "SIMATIC HMI WinCC (TIA Portal) WinCC Engineering V17 – Options" https://support.industry.siemens.com/cs/ww/en/view/109794201
\21\	Application example: "How do you read out or write tag values with an Excel application?" (SOAP) https://support.industry.siemens.com/cs/ww/en/view/69846238
\22\	Application example: "SIMATIC HMI Option+" with Option+ Manager https://support.industry.siemens.com/cs/ww/en/view/109754400
\23\	Application example: "Multiuser Engineering with TIA Portal Project Server" https://support.industry.siemens.com/cs/ww/en/view/109740141
\24\	Application example: "Working with the TIA Portal Cloud Connector" https://support.industry.siemens.com/cs/ww/en/view/109747305
\25\	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
\26\	Manual: "SIMATIC STEP 7 Basic/Professional V17 and SIMATIC WinCC V17" https://support.industry.siemens.com/cs/ww/en/view/109798671
\27\	Application example: Central User Management with "User Management Component (UMC)" https://support.industry.siemens.com/cs/ww/en/view/109780337
\28\	FAQ: Questions and answers about the new security features in TIA Portal V17 https://support.industry.siemens.com/cs/ww/en/view/109799540

7.4 Change documentation

Table 7-2

Version	Date	Change
V1.0	03/2016	First version
V1.1	05/2017	Added features for WinCC V14.
V1.2	04/2018	Added Comfort Pro und Option+
V1.3	04/2019	Added features for WinCC V15.
V1.3	05/2020	Changed link \9\
V1.4	07/2022	Revision and addition of features for WinCC V17