Industrial Thin Client configuration examples

SIMATIC ITC

https://support.industry.siemens.com/cs/ww/en/view/109758315

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG (“Siemens”). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

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

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

1 Industrial Thin Clients (ITC)

The SIMATIC Industrial Thin Clients are terminal devices specially developed for the industrial environment. They are designed to be used in client-server architectures to provide remote access to server systems.

The computing power is provided by the server, and the ITC serves as an I/O device. Therefore, the ITC does not need high-performance hardware components or a fan, which is reflected in the price of the devices and maintenance.

Remote protocols supported by the ITCs are:

- RDP (TCP/UDP),
- VNC and
- Sm@rtServer.

Furthermore, the ITC's V3 devices provide an HTML5 browser that allows them to access web applications.

The ITCs have a touch display as standard, which makes them a complete operator terminal without additional hardware. The devices are available in different display sizes (12, 15, 19 and 22 inches). They can be easily installed in the control cabinet or with a VESA mount. The integrated USB interfaces can be connected to further I/O devices (mouse/keyboard) to increase the ease of use. An integrated Gigabit LAN interface ensures fast and secure communication. The ITCs have an embedded operating system and do not have their own mass storage media, which prevents the installation of programs on the devices and reduces further maintenance of the devices. Siemens offers the SIMATIC TC-EX device variants for use in potentially explosive environments.

The uncomplicated set-up of the devices enables you to quickly integrate into new and existing systems. For ease of use of the devices during operation, the following features were integrated:

- Automatic connection setup at the start of the ITC.
- Auto-reconnect if a connection is lost.
- The ability to maintain multiple connections to servers.
- Fast, easy switching between the active compounds.

These features make ITCs the ideal thin client for virtually all terminal applications.

Other advantages that distinguish the devices are:

- A mean backlight operating time of 80,000 h.
- Protection class IP65 (installation in the control cabinet)
- Shock resistance
- Temperature compatibility from 0 to 50°C

Thanks to the additional service and support period of 9-11 years, the SIMATIC ITCs also offer very high investment security.

2 Supported protocols

2.1 Remote Desktop Protocol (RDP)

RDP is a system-bound network protocol from Microsoft, which was developed especially for remote access to Windows computers. It does not require any additional installation of software as it is integrated directly into the operating system. This makes it possible to remotely access the server before logging in.

On RDP, screen control commands are not transmitted to the graphics card, but sent over the network. A client evaluates these commands and displays them on the local screen. The client sends its input commands back to the server via this connection.

This makes the protocol very effective. However, it is strongly linked to the Windows architecture. Essentially, GDI (Graphic Device Interface) commands are sent. GDI is a library of graphics commands developed by Microsoft for Windows operating systems. If RDP is implemented on a different operating system, the commands of the external OS must be converted to Windows commands.

At the server computer, the user is logged off and the current screen is no longer displayed as soon as a client is connected.

The connection via the network is implemented via IP address (IPv4 and IPv6) via TCP or, since RDP V8.0, also via UDP. The default port for access via RDP is 3389.

2.2 Virtual Network Computing (VNC)

VNC is a software that mirrors the screen content of a remote computer (server) on a local computer (client). It is also possible to transfer virtual screens. In return, the client sends keyboard and mouse movements to the server. It lets you work on a remote system as if you were there.

VNC uses the Remote Frame Buffer Protocol (RFB) to transmit screen content and user input. The RFB is a network protocol for accessing the graphical user interfaces (GUI) of other computers. It is thus platform-independent usable, in contrast to other remote maintenance software.

This principle makes the protocol universally applicable, so it can be used on any operating system. For example, it is possible to access a Mac or Linux computer from a Windows PC.

However, VNC is not very efficient. It will transfer large amounts of data. However, the entire screen content is sometimes not sent, but only the difference to the previous one. Nevertheless, the protocol is slow, especially at high latencies, even though the data is usually compressed. In addition, VNC software must be installed and started on the server and the client. This circumstance makes it necessary for another user to first boot the server system, log on to the system, and start the VNC software.

2.2.1 Sm@rtServer

The Sm@rtServer is an optional package from WinCC and is based on VNC technology. It enables remote control and monitoring of SIMATIC HMI products via Industrial Ethernet via the intranet and Internet. Here, simple server-client mechanisms are provided for the devices. The Sm@rtServer is available for use on SIMATIC HMI panels or systems with installed RT Advanced and is integrated as standard in the RT-Advanced and Comfort Panels products. The Sm@rtClient can act as a fully functional operator station either in "View only" mode or with operating rights. It can access up to three panel applications and up to five clients for PC applications.

Just as with the VNC system, the server's screen is mirrored on the client and the operating commands are forwarded from the client to the server.

The activation of the Sm@rtServer takes place with one click via the engineering system TIA Portal.

2.3 Hypertext transfer protocol (http)

Thanks to the integrated web browser, the ITCs can establish communication via http. This browser is integrated into the V3 devices of the ITCs and allows the interpretation of the markup language HTML5.

The Hypertext Markup Language, abbreviated HTML, is a text-based markup language for structuring digital documents such as texts with hyperlinks, images and other content primarily on the internet. Compared to its predecessor versions, HTML5 offers new features to implement video, audio, local storage, and dynamic 2D and 3D graphics without the need for additional plug-ins.

2.3.1 WinCC WebUX

WinCC WebUX is an optional package developed for device-independent use on smartphones, tablets, PCs and other mobile devices. It translates runtime application images into HTML5 code and makes them available via the IIS (Microsoft Internet Information Service). This makes it possible to operate and monitor the runtime on any operating system. The only requirement is an HTML5-capable browser in which the project can be called up. To use WebUX, no client-side installation of Siemens software is required.

So, it is possible to access your system from any place at any time. Communication is secured via HTTPS and SSL certificates.

2.3.2 Web server

Many Siemens products provide an HTML5 web server. These web servers provide predefined default Web pages for easy viewing of service and diagnostic information. They can be activated with little effort when configuring the devices. In addition, products such as the S7-1500 can also be used to generate individually designed user-defined web pages. As with WebUX, client-side use of the web server requires only an HTML5-enabled browser.

2.4 Intel Active Management Technology (iAMT)

The iATM is an Intel-developed system-based lights-out management (LOM) system for the administration and remote maintenance of computer systems. It is based on the Intel vPro platform, which the manufacturer has developed for PCs in the office environment. The iAMT consists of a separate hardware component that is independent of the rest of the computer system, the Intel Management Engine (Intel ME). In current chipsets from Intel, this hardware is built in the form of its own microcontroller.

This autonomous microcontroller is powered by the permanent 5V supply of the power supply. It is therefore always in operation as long as the computer is plugged in, even if it is not switched on (with correct settings in the BIOS). The microcontroller has its own internal interfaces and is equipped with an externally accessible Ethernet interface. Thus, all system components can be accessed even when the computer system is in a non-functional or powered-down state. The iAMT offers various fix-programmed software modules, including its own VNC server and a web server.

The AMT web server makes it possible to read system information and control system functions. Furthermore, it can also be used to change the settings of the AMT. The user can remotely access the computer and mirror its screen via the AMT-VNC server. The advantage here is that the VNC server is active even without a logged-in user or operating system and so the BIOS (except MEBx settings) can be accessed.

iAMT is used in virtually all desktops, servers and tablets based on Intel vPro. Among other things, these are the Intel Core i series i3, i5, i7 and the Intel Xeon processor families, which are also used in certain SIMATIC IPCs.

3 Configuration examples of ITCs

This section shows you some configuration examples of SIMATIC ITCs. This means that you can choose the right application for your needs.

3.1 Virtualization server

A virtualization server has software called a hypervisor. This software is responsible for the resource management of a computer. Thus, the hypervisor makes it possible to divide the hardware of a physical computer into several virtual computer systems.

It is possible for the resources of each virtual machine such as,

- CPU cores,
- RAM and
- disk space

to be allocated freely.

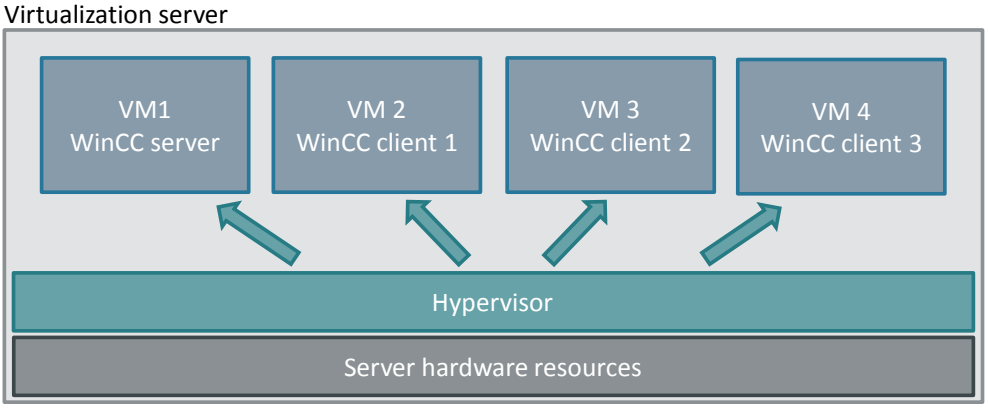
The number of virtual machines (VM) is limited by the available hardware resources.

Each of these VMs forms a self-contained system that can operate as a complete machine independent of the other VMs. Therefore, it is possible to install a separate operating system and different software on each VM. Another advantage of the virtualization server is that the VMs, including the software they contain, can be easily duplicated.

This means that you can quickly equip a staff with a suitable system for his work, without much installation effort and without having to provide his own physical computer. Via the ITC, the user can log on to his VM via RDP and work on it as usual. Another advantage of these systems is that the individual computers no longer need to be maintained, but only the server.

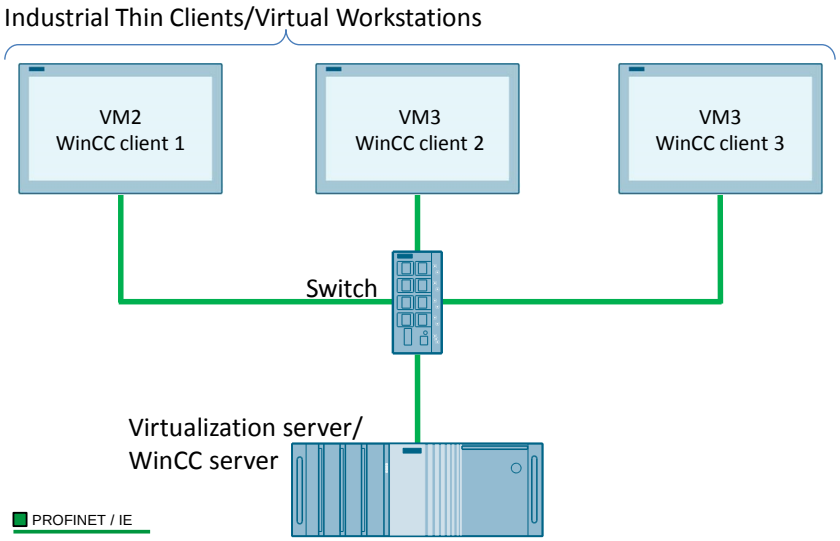
Figure 3-1

Virtualization server



A scenario for using a virtualization server in conjunction with WinCC is a multiuser application. One VM serves as WinCC server and the others as WinCC clients. ITCs allow several users to move in their own session in one project at the same time.

Figure 3-2



3.2 Remote operation of systems

It often happens that remote access to systems is required. There are three different protocols that support the SIMATIC ITCs. Each of these protocols has its own special features, which were already described in section 2.

Remote control via RDP

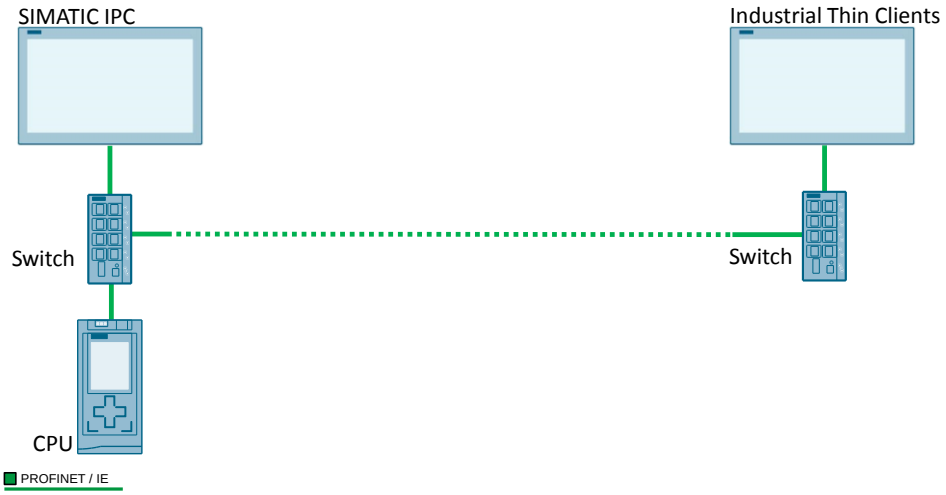
With the RDP it is possible to access an operating system that has already been booted up. This allows remote restarts
without the need for an on-site operator. Therefore, this type of access is particularly suitable for remote facilities without the presence of expert personnel. Since the RDP does not transmit large amounts of data, this protocol guarantees the highest performance.

Remote control via VNC

Since the VNC server has to be started from the operating system, it is not possible to restart a system with it. Otherwise, however, all the functionalities are the same as the remote computer being accessed. However, since a large amount of image data is sent via Ethernet, delays in transmission may occur.

Remote control via Sm@rtServer

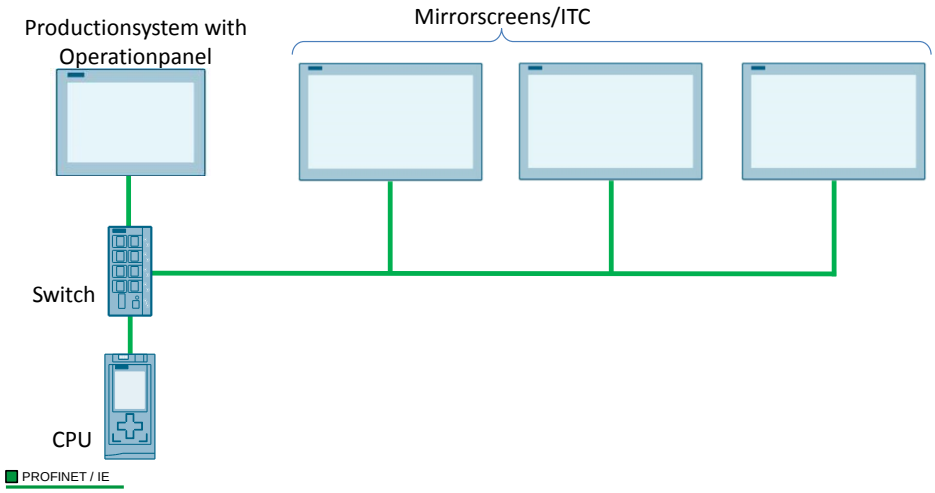
The Sm@rtServer is a VNC server, developed by Siemens, which is adapted to the requirements of runtime advanced and panel systems. The Sm@rtServer can be easily set up on the panels and computers that have an RT Advanced installed. It offers the same functionality as the traditional VNC server.



3.3 Operation of a system of several operating stations

For large distributed systems, using VNC or Sm@rtserver is a good idea because all clients present a mirrored image of the server in this remote access. This allows the operator to control and monitor the same project/system from each operator station.

If more than one client is used, it must be ensured that the VNC server is designed for concurrent access of multiple devices. The Sm@rtServer supports up to five computer systems and up to three clients on the panel. In this configuration example, make sure that the individual clients do not overlap the operation, as this can lead to problems.



3.4 Online applications for WinCC projects

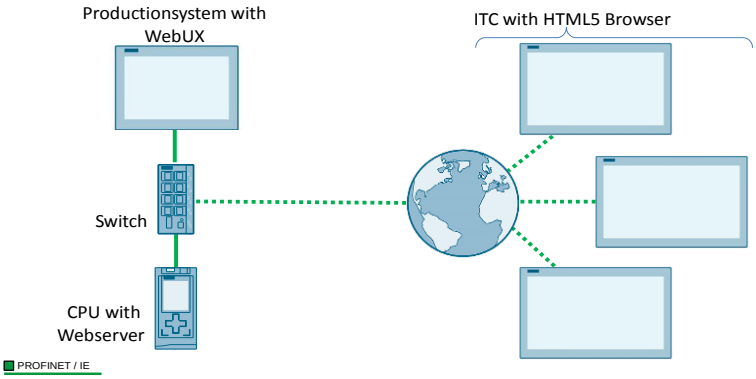
The V3 models of the SIMATIC ITCs support the use of HTML5 with the integrated web browser.

With the WinCC WebUX option, it is possible to release application pictures and entire HMI projects from WinCC via Microsoft IIS. This allows any device that has an HTML5 browser to access your applications over the Internet from anywhere, at any time, with an authorized user.

This application is particularly suitable for the observation of production processes and the triggering of non-critical control commands, for which it is not necessary to be on-site, such as the changing of recipes and the commissioning of production goods.

Access is only possible to the contents released in runtime and only by authorized web users.

The ITCs enable a straightforward connection to the provided WebUX process pictures and the operation and monitoring of WinCC projects via the Internet/Intranet.



3.5 Decentralized operation of SIMATIC WinCC and virtual workstation

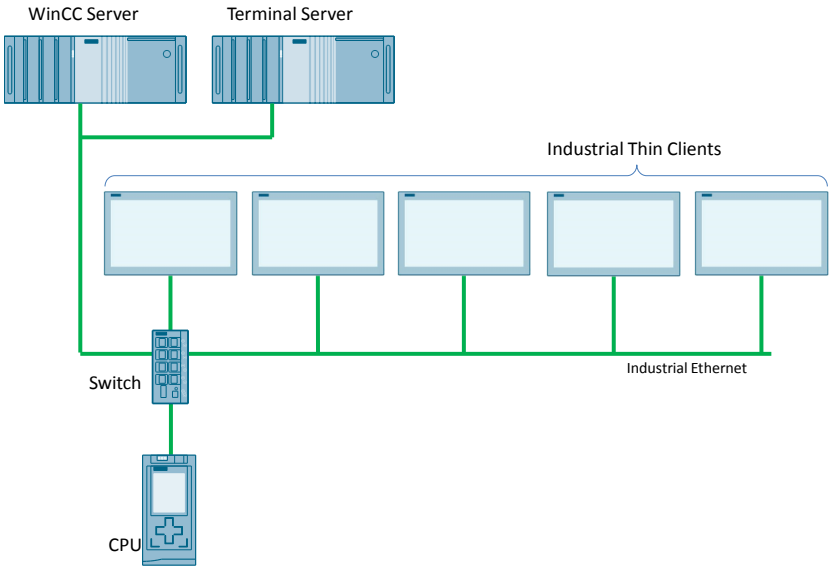
This application provides several Windows sessions and applications from a terminal server. The terminal server is equipped with a Windows server operating system and provides a separate Windows session for each ITC, which is called up using RDP.

The ITCs serve as a terminal where the individual users can work independently. Each user can login with their credentials to each ITC and work with the provided applications and data on the server.

Thus, not every worker needs his own full-fledged PC, because the computing power is provided by the server. In this way, license costs can be saved. Also, the maintenance of individual systems can be centralized and simplified.

This configuration, in conjunction with a WinCC server and the optional WebNavigator package, enables distributed use of a WinCC project. Every registered user can access the WinCC project completely independently of the others via his Windows session and the Internet Explorer. A major advantage of this system is the decentralized use of WinCC without requiring separate licenses for each WinCC client.

The complete article with a sample project can be found under this link (Article ID: 28309119).



3.6 Remote maintenance of systems

3.6.1 Remote maintenance via VNC, Sm@rtServe and AMT

The VNC protocol is particularly suitable for the remote maintenance of systems. It offers the advantage that the displayed screen is mirrored and not completely transferred to the remote client. Thus, both users can view all information at the same time on the system's computer and at the ITC. The trained professional does not need to be on-site to analyze the system and troubleshoot. The production worker can watch the troubleshooting live and intervene when minor errors occur again.

The Sm@rtServer is a Siemens-developed VNC server, which is adapted to the requirements of runtime advanced and panel systems. This can be easily set up on the panels and computers that have an RT advanced installed. It offers the same functionality as the traditional VNC server.

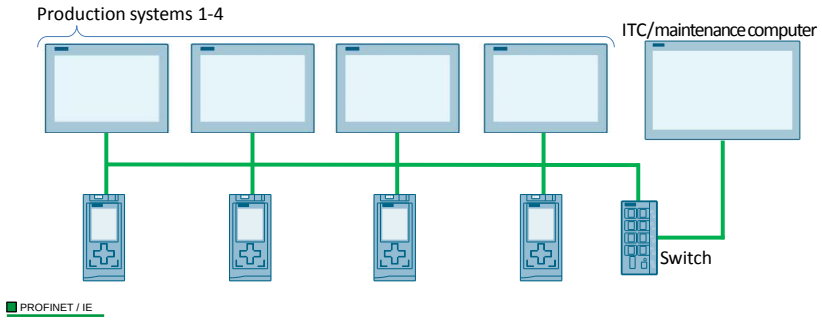
The Intel AMT also has an integrated VNC server. This offers all the functionality of the conventional VNCs. Since the AMT belongs to the LOM systems, the AMT VNC server is always active when the device is connected to the mains. This means that restarts and settings in the BIOS are possible with this type of remote maintenance. This provides the client with almost any opportunity to access the computer system that a field technician has, and makes the AMT an ideal system for such tasks.

3.6.2 Remote maintenance via web server

The AMT (Active Management Technology) of the company Intel has an integrated web server. It provides access to system information, enabling remote diagnostics over the Internet/Intranet. Furthermore, it is possible to trigger certain control commands via the web server, such as restarting the computer. Thus, no service employee has to be on site for this type of maintenance.

Note Full access to the functions of the AMT is provided by the SIMATIC IPC Remote Manager tool. So it is also possible to access the BIOS remotely.

Other devices such as the CPUs S7-1500 and SITOP power supplies also have an integrated HTML5-capable web server, which can be activated in the TIA Portal with just a few settings. With this, as with the AMT, it is possible to access the diagnostic pages of various SIMATIC products and trigger system-related control commands.

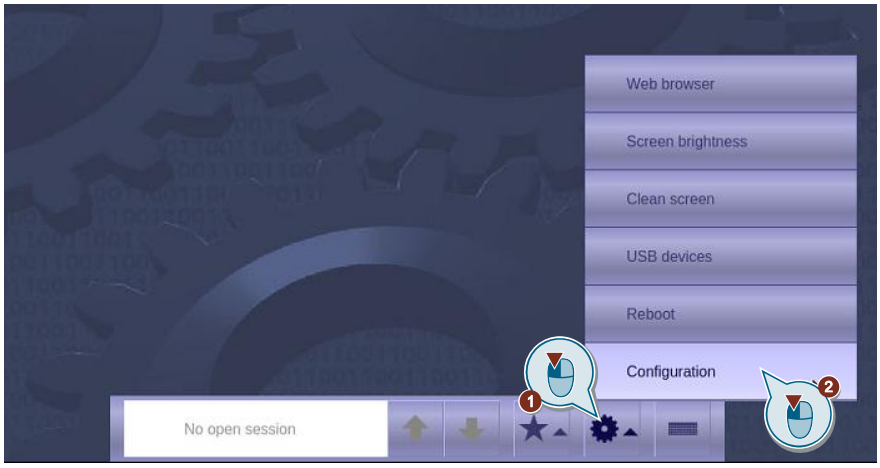


4 Configuration of the ITC

For the first use, it is necessary to make some settings at the ITC that allow the creation of new remote connections. These settings and other features are explained in this section.

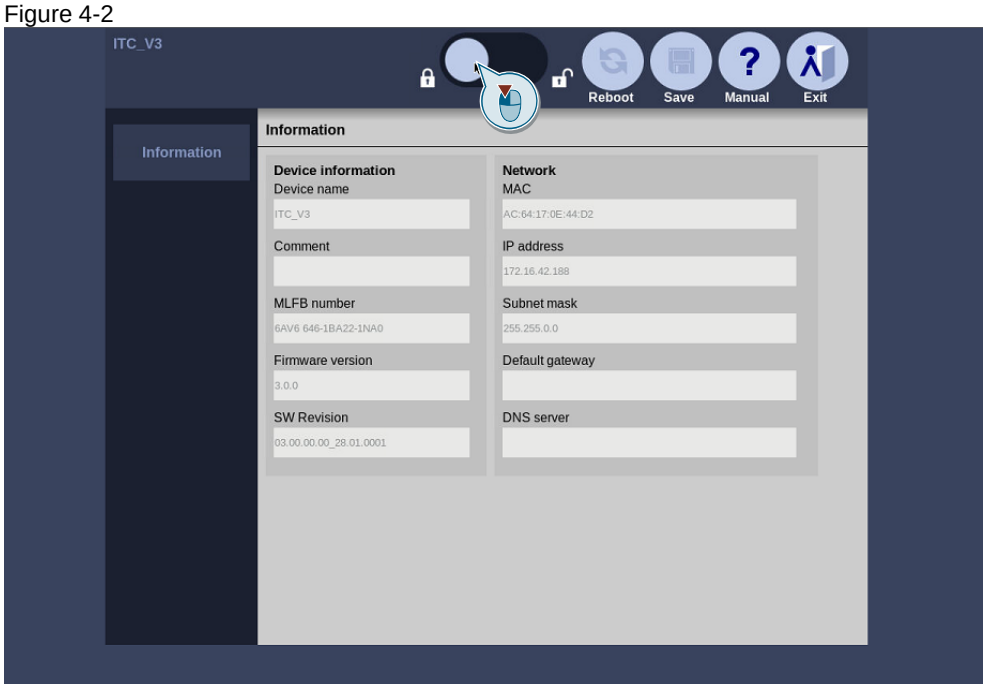
1. Start the ITC. At the bottom of the screen you can see the user interface of the ITC. The rest of the screen is reserved for viewing the image of the currently connected remote server.
2. Click on the gear icon in the menu bar. (1) This opens a drop-down list. Click on the entry "Configuration". (2) This opens the configuration screen of the ITC. Here you can see various information about the device

Figure 4-1



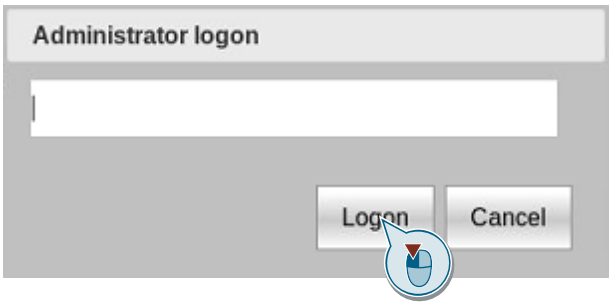
3. Click on the "Login" button to change these settings.

Figure 4-2



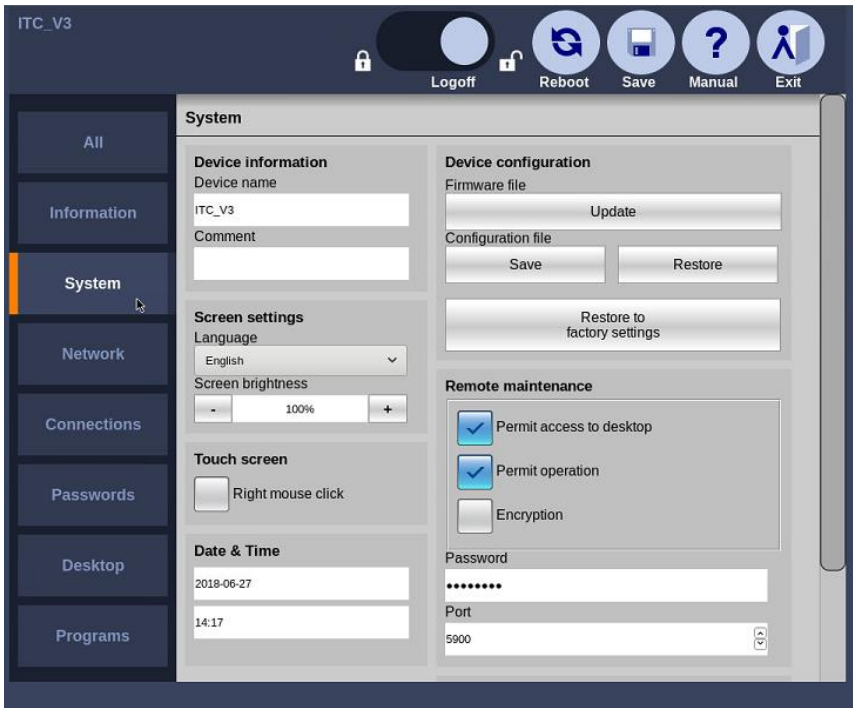
4. This opens the login window. Enter your login password and confirm the entry with the "Logon" button. If you have not yet assigned your own password, the default password is "admin".

Figure 4-3



5. Entering the password gives you full access to the settings of the device. The menu bar on the left side is expanded with the correct entry of the password. Open the system settings by clicking on the "System" button.

Figure 4-4



6. Optional: In the system settings, the following settings:

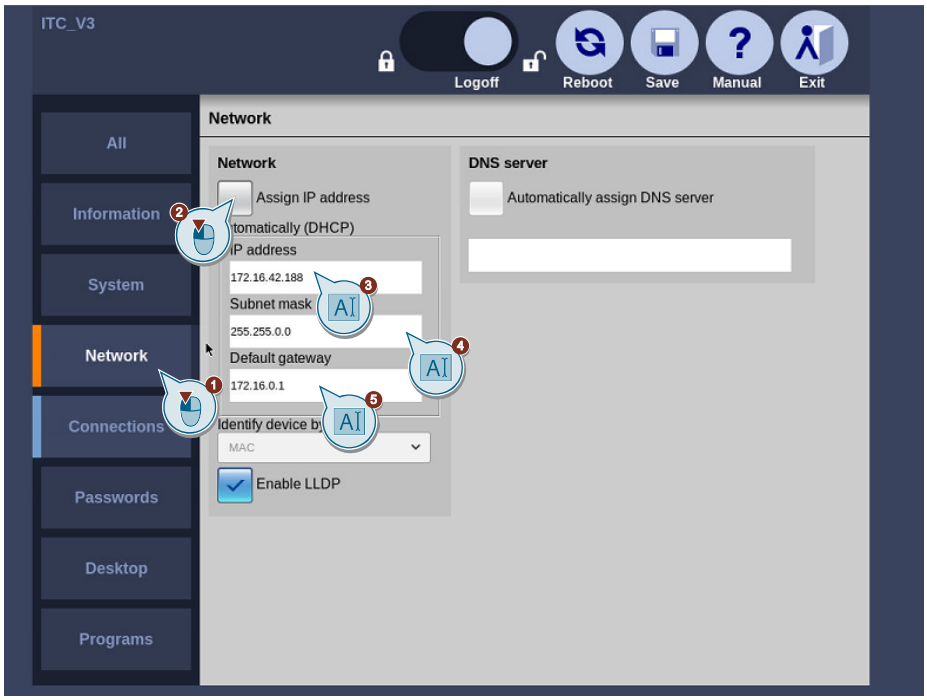
- The device name, as well as the
- Screen-,
- Touch and
- time settings

  can be changed.

Furthermore, in this menu you can influence the firmware and set up the system's internal VNC server if you want to remotely access the ITC. Adjust the settings according to your requirements.

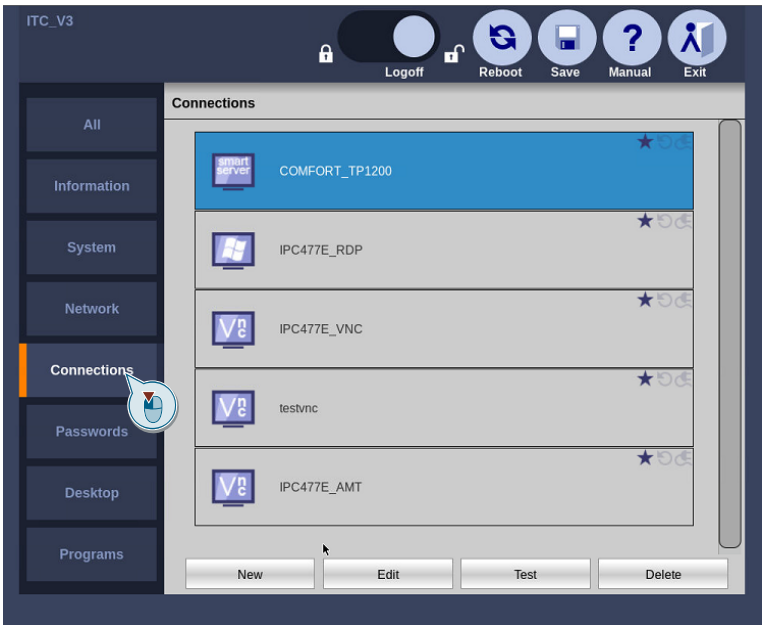
7. Open the network settings by clicking on the entry "Network" (1). Uncheck the check box "Assign IP address" (2) and assign an IP address (3) and subnet mask (4) if you do not want automatic assignment via DHCP. Allocation of the default gateway is still required for access to the Internet. (5)

Figure 4-5



8. A new remote connection is set up under the connection settings. Open it by clicking on the "Connection" button. The creation of various connections is described in more detail in the later sections "Setting up the" ... "connection with the ITC".

Figure 4-6



9. This opens a window in which you can see your previously configured connections. At the bottom of the window are four buttons that allow you to create, edit, test, and delete connections.
10. You can change the password in the password settings. These can be accessed via the "Passwords" button. The password request is a minimum length of 8 characters.
11. If you have adjusted all the settings to your requirements, confirm them with the "Save" button. The configuration is saved and the device is restarted.

Result

You have successfully completed the basic ITC settings and can create new connections and use them for remote access.

5 Setup of the connections

5.1 Remote Desktop Protocol

This section briefly explains what settings you need to make on the server machine to enable the RDP server and how to connect to the ITC via RDP.

5.1.1 Components used

This application example was created with these hardware and software components:

Table 5-1

Components	Number	Article number	Note
IPC477E	1	6AV7241-7LH44-0FA0	• Generally the configuration is possible with all Windows systems
ITC2200 V3	1	6AV6 646-1BA22-1NA0	
Windows 10 Enterprise 2016 LTSB	1		

5.1.2 Configuration of RDP

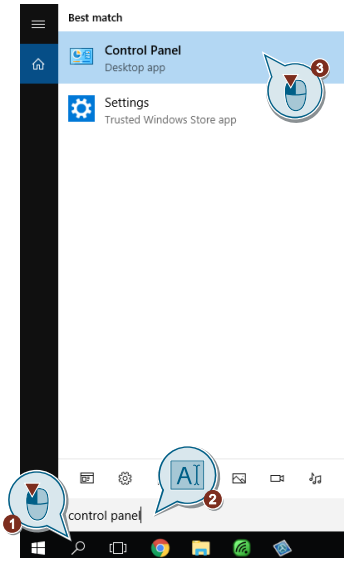
Setup of RDP on Windows 10

This section will show you how to allow remote desktop connections on your PC system.

Note The computer accessed via RDP and the ITC must be connected via Industrial Ethernet. The IP addresses and subnet masks must be set so that the two devices can reach each other.

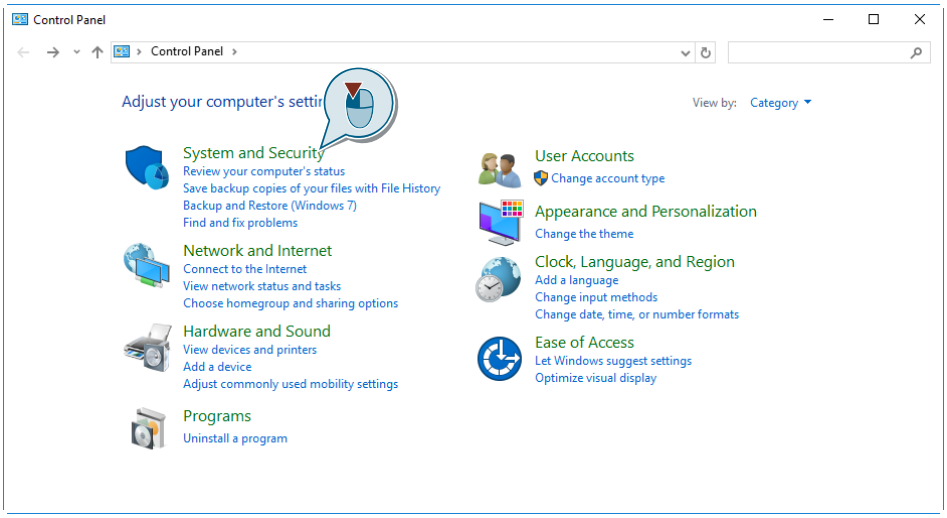
1. Open the Control Panel of your IPC. Click on the search symbol. (1) Enter "Control Panel" in the search window. (2) Click on the entry "Control Panel". (3)

   Figure 5-1



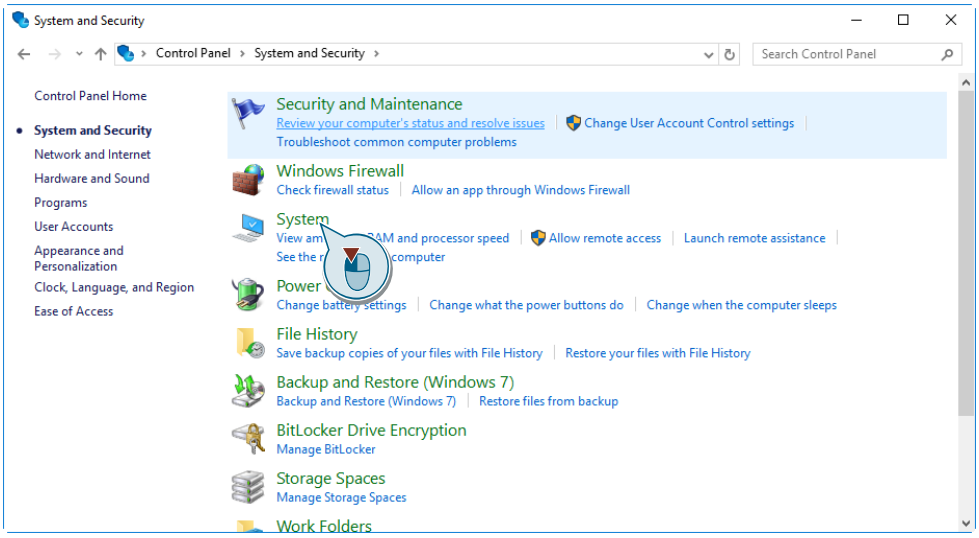
2. In the "Control Panel", select the "System and Security" category.

Figure 5-2



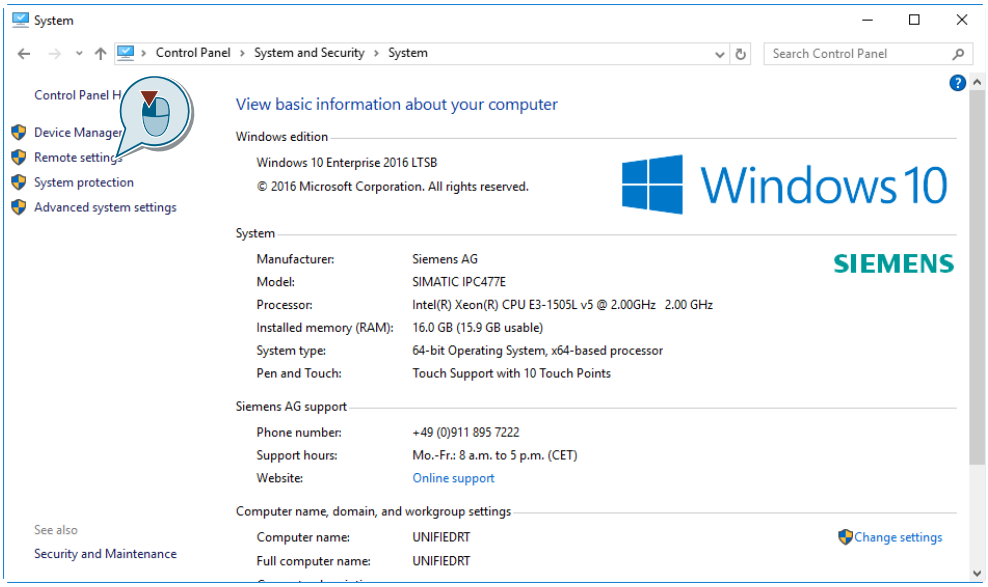
3. Open the system information by clicking on the "System" category.

Figure 5-3



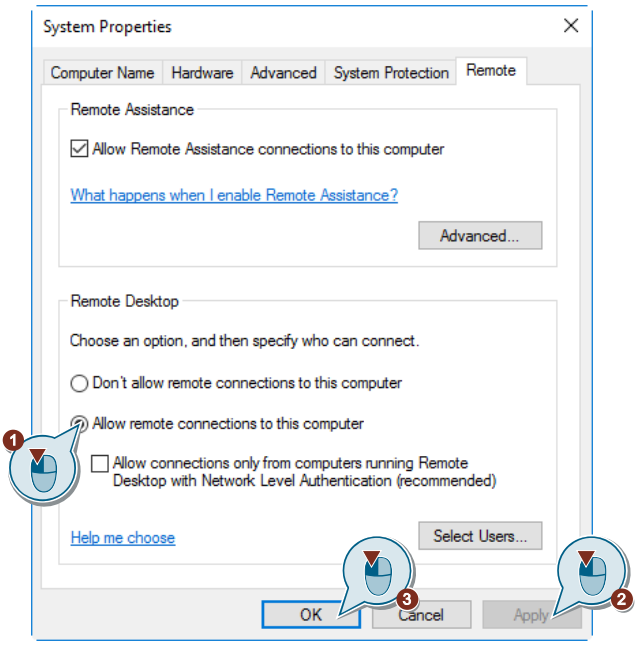
4. Click on the entry "Remote settings" in the list on the left side of the window. This opens a window with the settings for remote access.

Figure 5-4



5. A window with the settings for remote access appears. Enable the "Allow remote connections to this computer" option. (1) Save the setting with the "Apply" button. (2) Close the window with the "OK" button. (3)

Figure 5-5

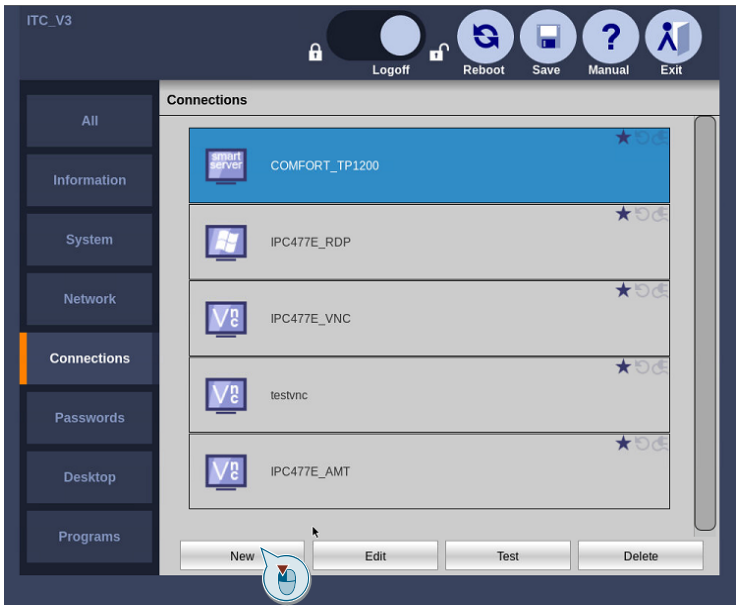


5.1.3 Setup the RDP connection with the ITC

This section describes how to connect the ITC to an RDP server.

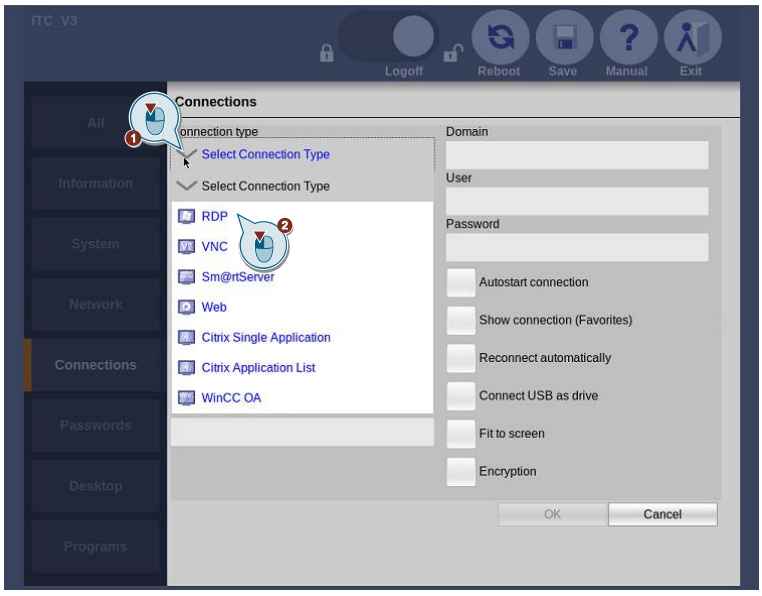
1. Open the settings of the ITC and log in as administrator. Open the configuration window for the configured connections (as described in section 4).
2. Click the "New" button at the bottom of the image to create a new connection. You will be directed to the configuration screen for setting up and editing remote connections. Depending on the selected connection type, unnecessary fields are grayed out.

Figure 5-6



3. Open the drop-down list labeled "Select Connection Type" (1) and select the RDP connection. (2)

Figure 5-7



4. Enter the parameters

- Connection name (freely selectable),
- Server IP address (address of the server computer),
- Port (standard port 3389),
- Username (Windows username on the RDP server) and
- User password (Windows password of the user on the RDP server)

in the appropriate fields.

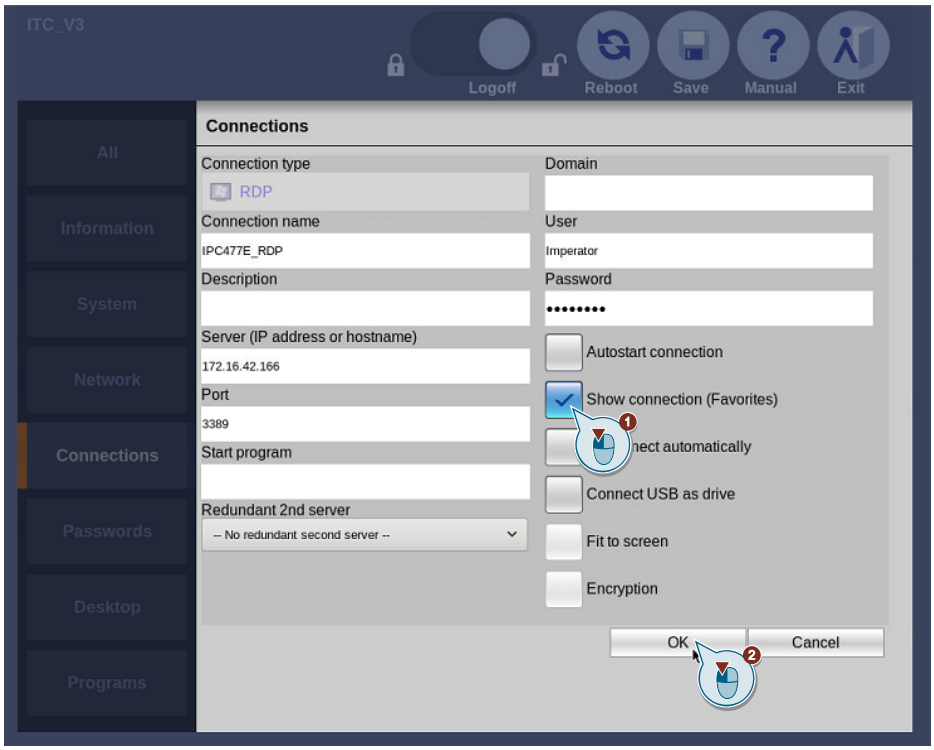
In the checkboxes you can activate and deactivate further functions of the connections. Only the functions that are relevant for the used protocol type can be selected.

5. Enable the "Show Connection (Favorites)" function to quickly access this connection. (1)

Note Note that the maximum number of favorite connections is limited to nine.

6. Confirm the creation of the connection with the "OK" button. (2)

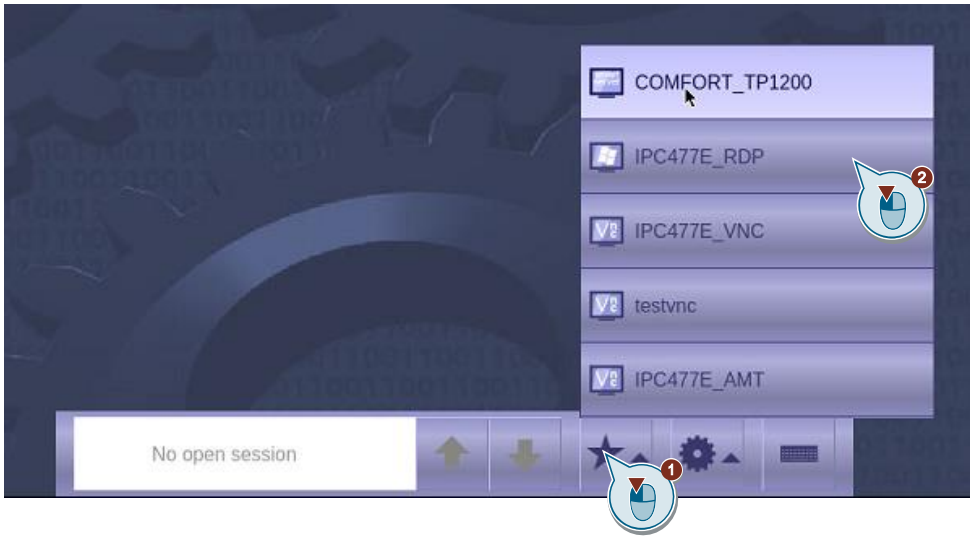
Figure 5-8



Result

You have successfully configured an RDP connection. You can find it on the start screen by clicking on the star icon (Favorites). (1) Clicking on the connection allows you to remotely access the screen of your RDP server and see its contents. (2)

Figure 5-9



5.2 Virtual Network Computing

This section explains what settings you need to make on the server machine to set up VNC and how to connect to the ITC

5.2.1 Components used

This application example was created with these hardware and software components:

Table 5-2

Components	Number	Article number	Note
IPC477E	1	6AV7241-7LH44-0FA0	
ITC2200 V3	1	6AV6 646-1BA22-1NA0	
Windows 10 Enterprise 2016 LTSB	1		
TightVNC V2.7.10	1		• Other VNC server programs are possible

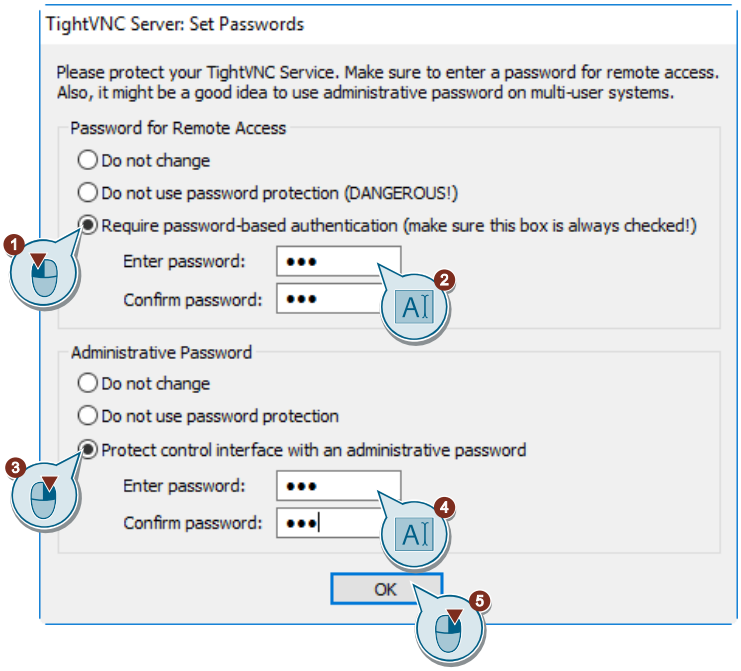
Note Make sure that the software you use is compatible with Siemens software and hardware.

Siemens provides a Compatibility tool for this purpose.

5.2.2 Setting up the VNC server

1. Install the software (in this example TightVNC) on your server computer. (here IPC 477E)
2. When you finish installing the Tight VNC server program, a configuration window opens. Enable the password option for remote access. (1) Enter a password and confirm it. (2) Enable the password option for the administrator settings. (3) Enter a password and confirm it. (4) Finish the configuration with the "OK" button. (5)

Figure 5-10



Result:

You have successfully installed and configured your VNC server. It is automatically active and starts automatically when a user logs in.

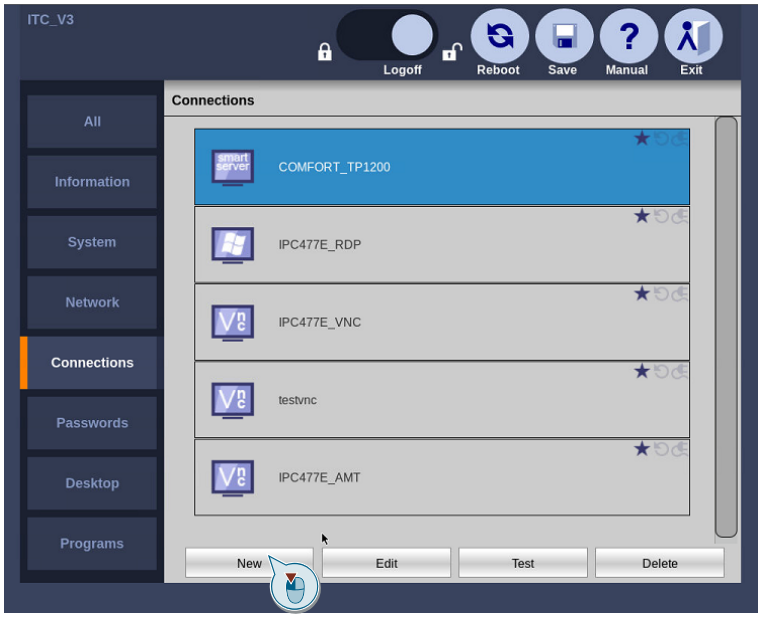
5.2.3 Setting up the VNC connection with the ITC

This section describes how to connect the ITC to a VNC server.

1. Open the settings of the ITC and log in as administrator. Open the configuration window for the configured connections (as described in section 4).

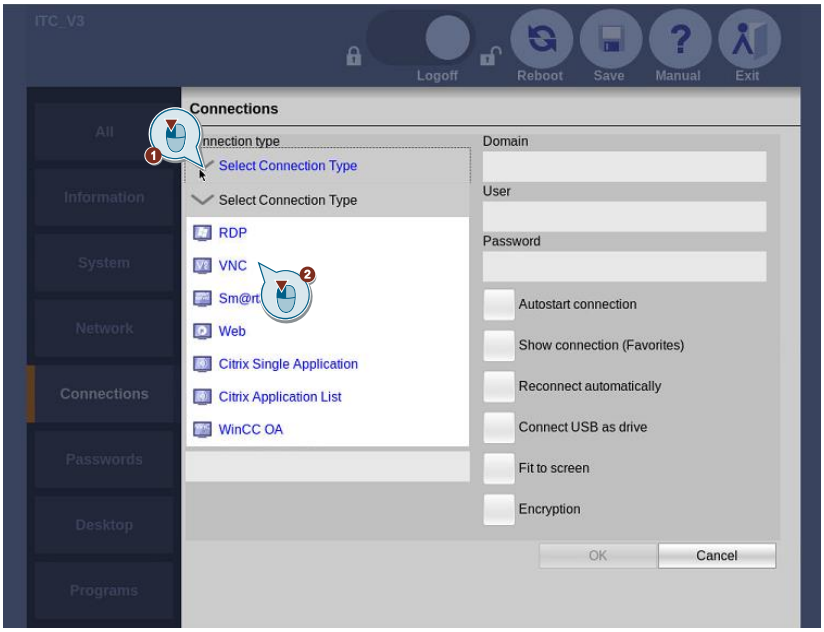
2. Click the "New" button at the bottom of the image to create a new connection. You will be directed to the configuration screen for setting up and editing remote connections. Depending on the selected connection type, unnecessary fields are grayed out.

Figure 5-11



3. Open the drop-down list labeled "Select Connection Type" (1) and select the VNC connection. (2)

Figure 5-12



4. Enter the parameters

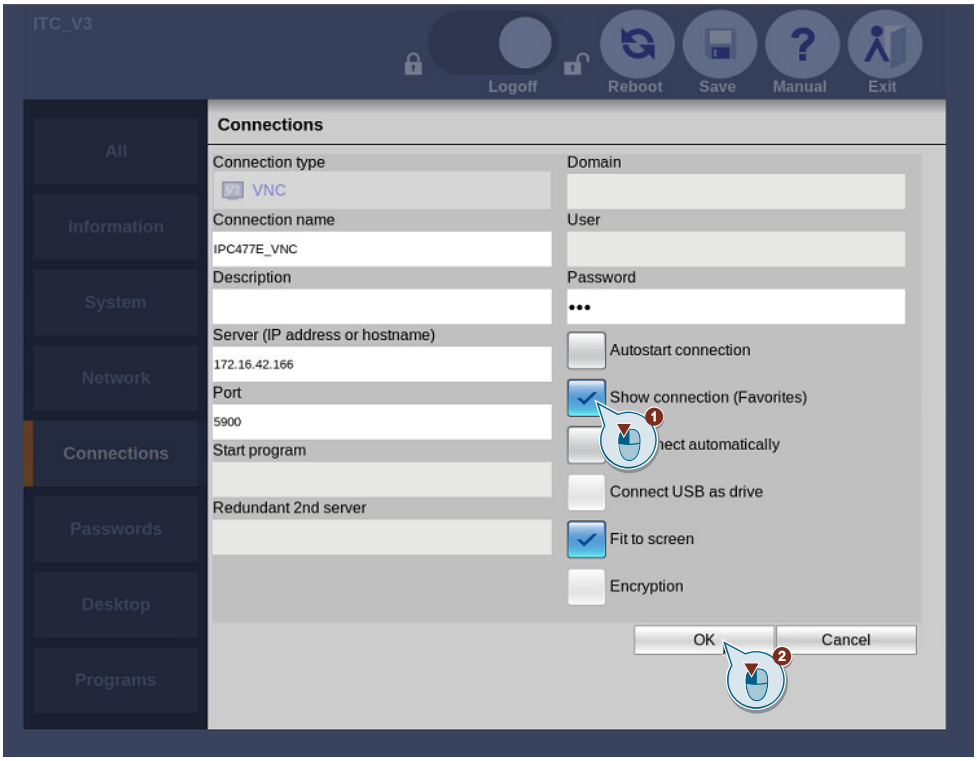
- Connection name (freely selectable),
- Server IP address (address of the server computer),
- Port (standard port 5900),
- Password (previously set VNC server password)

in the appropriate fields.

In the checkboxes you can activate and deactivate further functions of the connections. Only the functions that are relevant for the used protocol type can be selected.

5. Enable the "Show Connection (Favorites)" function to quickly access this connection. (1)
6. Confirm the creation of the connection with the "OK" button. (2)

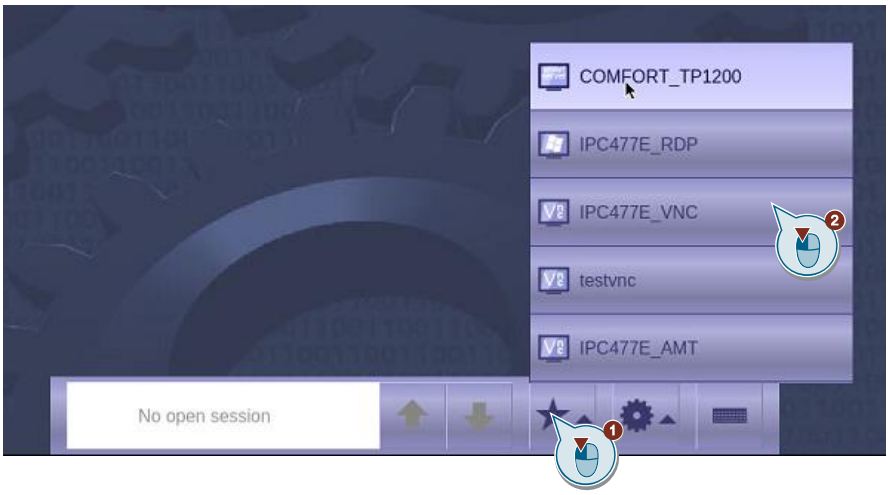
Figure 5-13



Result

You have successfully configured a VNC connection. You can find them on the start screen by clicking on the star icon (Favorites). (1) Clicking on the connection allows you to remotely access the screen of your VNC server and see its contents. (2)

Figure 5-14



5.3 Sm@rtServer

This section explains how to enable the Sm@rtServer on a comfort panel and how to connect to the ITC.

5.3.1 Components used

This application example was created with these hardware and software components:

Table 5-3

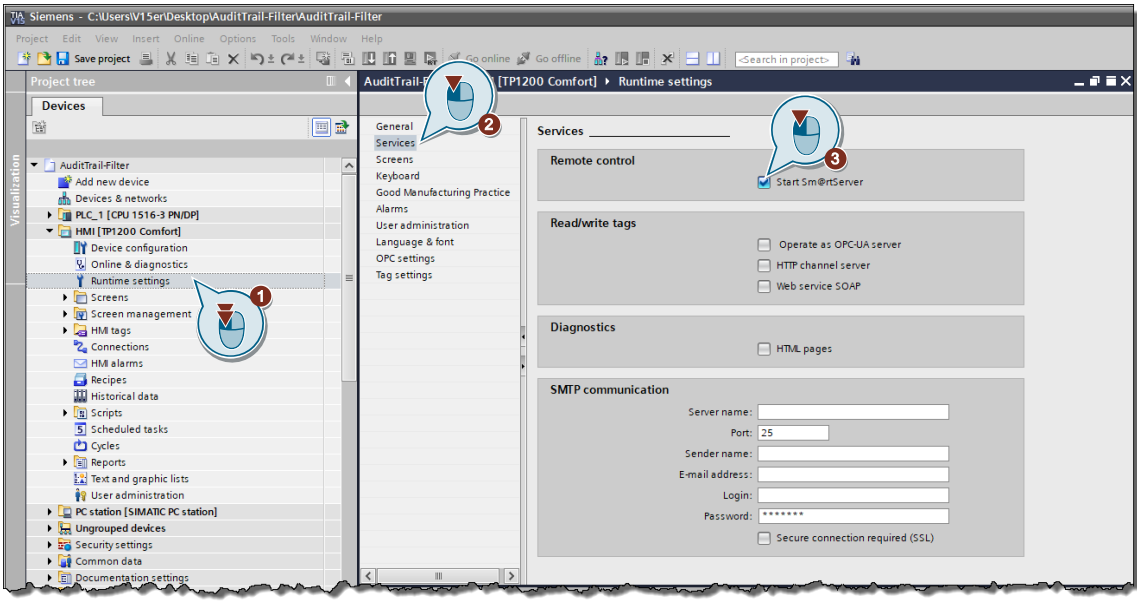
Components	Number	Article number	Note
TP1200 comfort panel	1	6AV2124-0MC01-0AX0	Or other comfort panels
ITC2200 V3	1	6AV6646-1BA22-1NA0	
SIMATIC STEP 7 Prof. V15	1	6ES7822-1AA05-0YA5	• Floating license • With USB stick • With DVD
SIMATIC WinCC Professional V15 (SIMATIC WinCC Advanced V15 is sufficient for configuration)	1	6AV2103-0DA05-0AA5	• With 512 power tags • With DVD

5.3.2 Activating the Sm@rtServer

This section describes which settings you must make in the WinCC project to set up a Sm@rtServer. This option is only available for WinCC Advanced and Panels.

1. Open the "Runtime Settings" of your HMI system in the "Project Tree". (1)
2. Select the "Services" category from the area navigation. (2) Put the check mark in the "Remote control" area of the "Start Sm@rtServer" option. (3)

Figure 5-15



Result

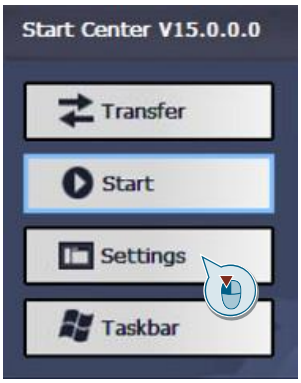
You have successfully activated the Sm@rtServer. It is set up when the runtime is downloaded to the device.

5.3.3 Modification of the Sm@rtServer password

The default password of the Sm@rtServer is "100". To adjust this, you need to perform the following steps.

1. Stop the runtime on the panel.
2. Open the panel settings by clicking on the "Settings" button in the Start Center.

Figure 5-16

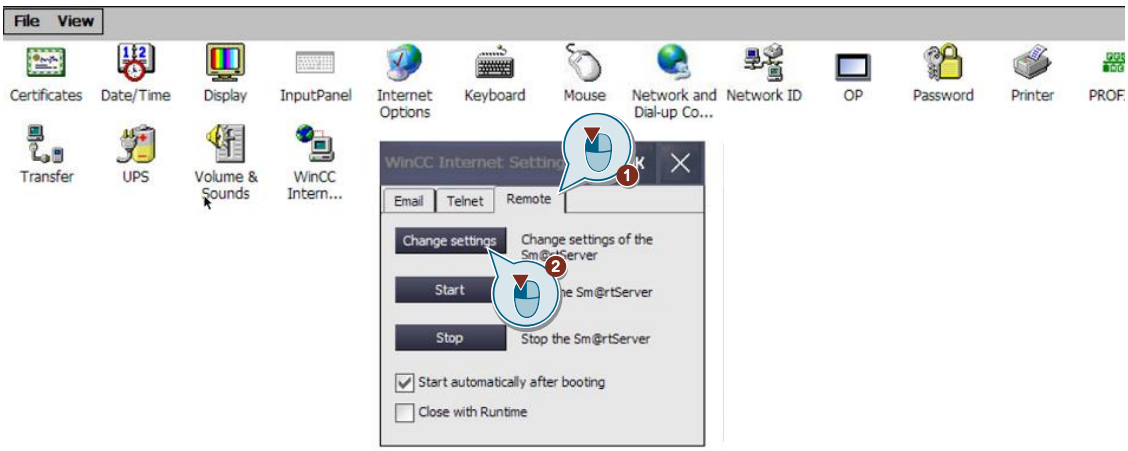


3. Double click on the icon labeled "WinCC Internet Settings".

Figure 5-17

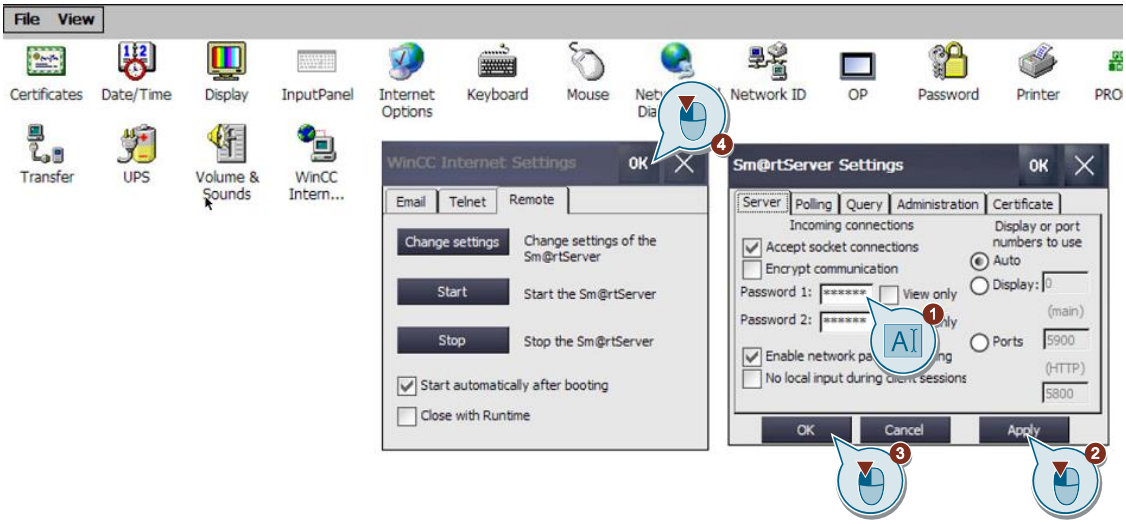
4. Click on the entry "Remote" in the upper selection bar. (1) Click the "Change Settings" button to open the "Sm@rtServer Settings". (2)

Figure 5-18



5. Assign two passwords and determine whether the user can use this password for operator control, monitoring or just operation. Enter a password and remove the checkbox labeled "View only". (1). Confirm your entry with the "Apply" button. (2) Close the settings with the "OK" buttons of the menus. (3) (4)

Figure 5-19



Result

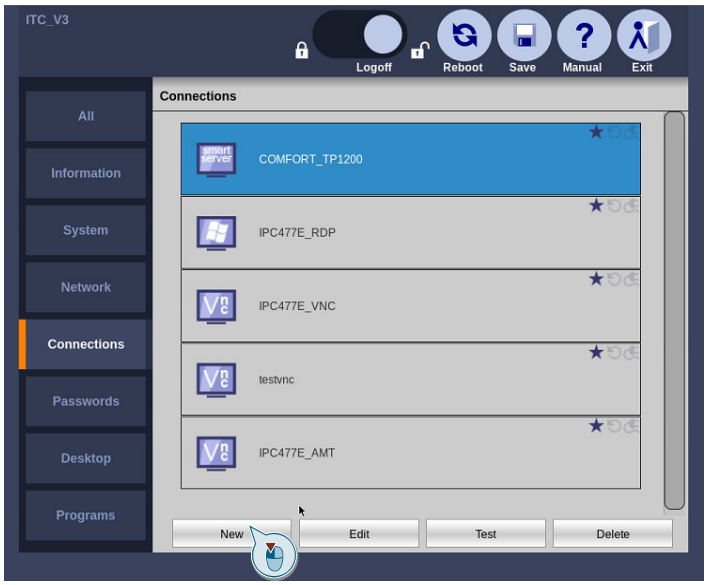
You have successfully changed the password of your Sm@rtServer. You will need this for access from a client.

5.3.4 Set up the connection with the ITC

This section briefly describes how to connect the ITC to a Sm@rtServer.

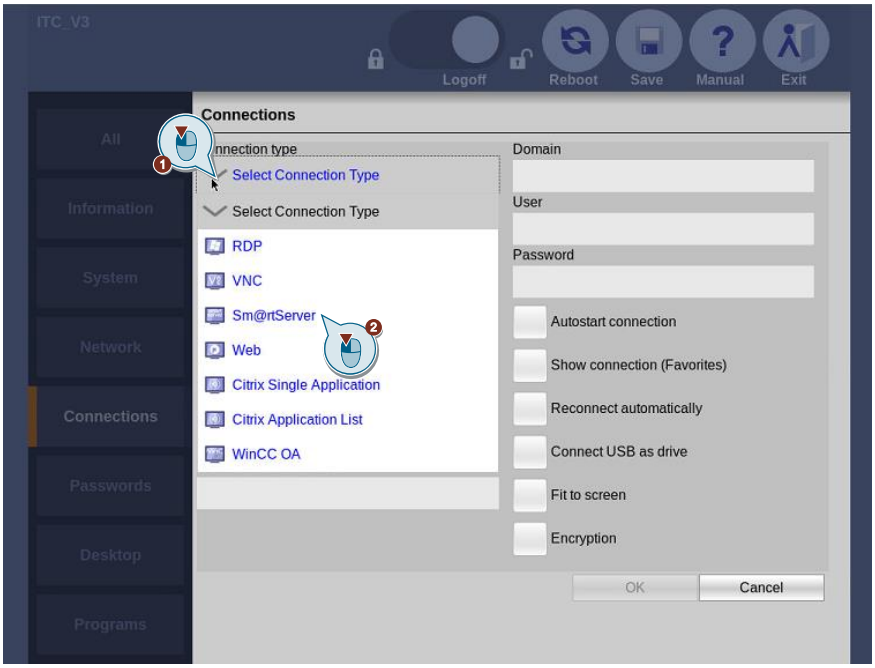
1. Open the settings of the ITC and log in as administrator. Open the configuration window for the configured connections (as described in section 4).
2. Click the "New" button at the bottom of the image to create a new connection.

Figure 5-20



3. You will be directed to the configuration screen for setting up and editing remote connections. Depending on the selected connection type, unnecessary fields are grayed out. Open the drop-down list labeled "Select Connection Type" (1) and select the Sm@rtServer connection. (2)

Figure 5-21



4. Enter the parameters

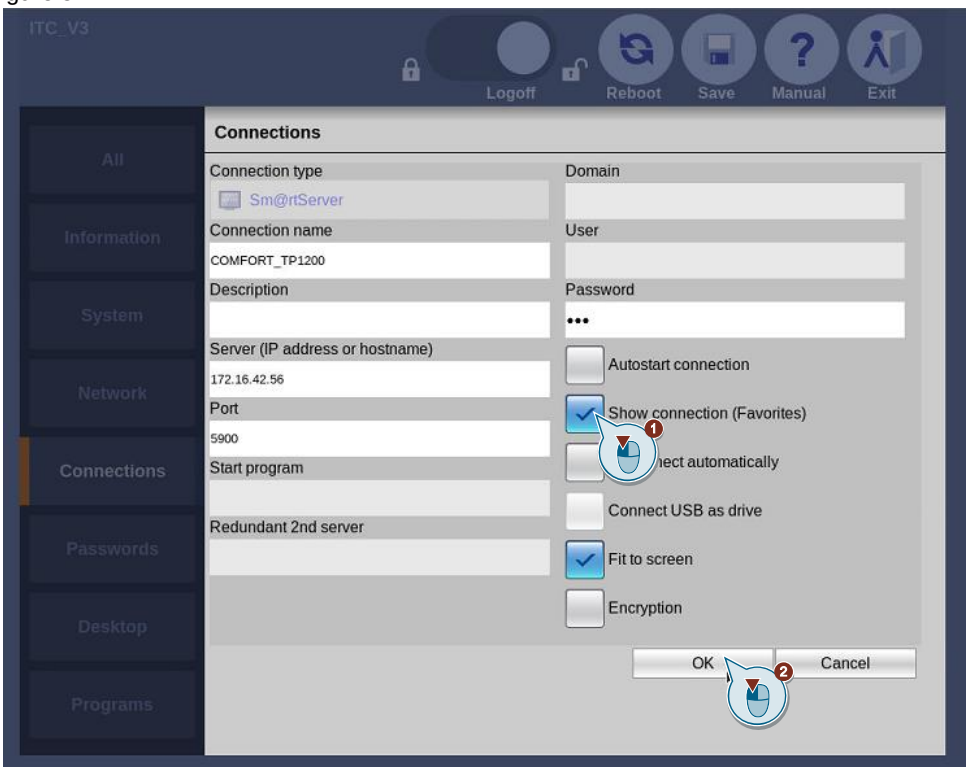
- Connection name (freely selectable),
- Server IP address (IP address of the panel),
- Port (standard port 5900),
- Password (default password "100" or previously set Sm@rtServer server password)

in the appropriate fields.

In the checkboxes you can activate and deactivate further functions of the connections. Only the functions that are relevant for the used protocol type can be selected.

5. Enable the function "Show connection (Favorites)" to quickly call up the connection. (1)
6. Confirm the creation of the connection with the "OK" button. (2)

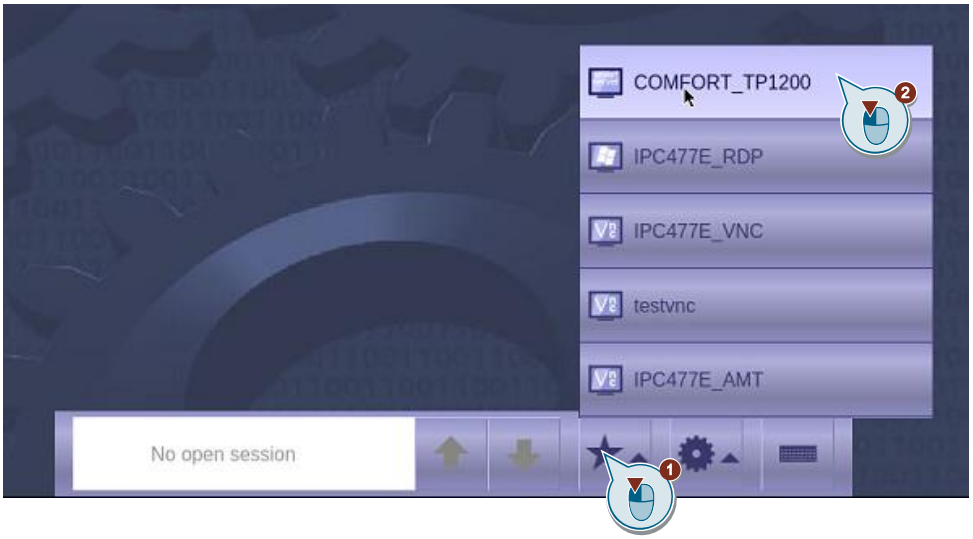
Figure 5-22



Result

You have successfully configured a Sm@rtServer connection. You can find them on the start screen by clicking on the star icon (Favorites). (1) By clicking on the connection, you should be able to remotely access the screen of your Sm@rtServer and see its contents. (2)

Figure 5-23



5.4 Intel AMT VNC server

This section explains what settings you need to make on the server machine to enable the AMT VNC server and how to connect to the ITC.

5.4.1 Components used

This application example was created with these hardware and software components:

Table 5-4

Components	Number	Article number	Note
IPC477E	1	6AV7241-7LH44-0FA0	• Generally the configuration is possible with all Windows systems
ITC2200 V3	1	6AV6 646-1BA22-1NA0	
Intel AMT SDK			

5.4.2 Setting up the Intel AMT-VNC Server

Depending on the IPC and installed BIOS/AMT version, the settings and their location may change. Information about your device can be found in the corresponding manual. Upon entering the type designation of your IPC into the filter mask under the following link (https://support.industry.siemens.com/cs/ww/en/ps/16740/man), you will be redirected to the appropriate manual.

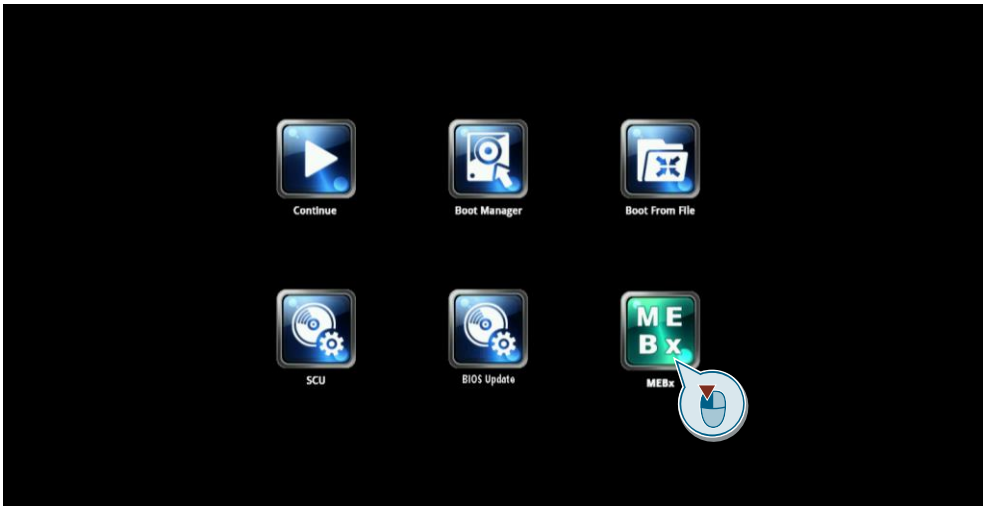
Settings in the BIOS

1. Start the computer and press the <ESC> button on startup to open the BIOS selection menu.

Note The setup refers to the system of the IPC 477E and may differ in other computer systems. Please inform yourself about keyboard shortcuts and settings of the MEBx of your PC.

2. Use the arrow keys to go to the "MEBx" option and open it with the <Enter> button.

Figure 5-24



3. Select "MEBx Login".
4. Enter the standard password "admin".

Change the password. The new password must comprise:

- At least eight characters
- An upper case letter
- A lower case letter
- A number
- A special character (! @ # $ % ^ & *)
- The underscore "_" and space characters are valid in the string but do not increase the complexity of the password.

Note If you no longer know the password, you must reset Intel® AMT to the default settings. Backup the password in case it is lost.

5. Switch to the submenu "Intel (R) AMT Configuration" and activate "Manageability Feature Selection".
6. Activate the option KVM in the "SOL/IDERKVM" settings.
7. In the "Intel (R) AMT Configuration" submenu, enable access to the network via "Activate Network Access".
8. Confirm the following dialogs with "Y".
9. Disable the "DHCP mode" in the "Intel (R) AMT Configuration > Intel (R) ME Network Setup > TCP/IP Settings > Wired LAN IPV4 Configuration" settings. Assign the desired IP address, a suitable subnet mask and the default gateway if you want to communicate with systems outside your network.

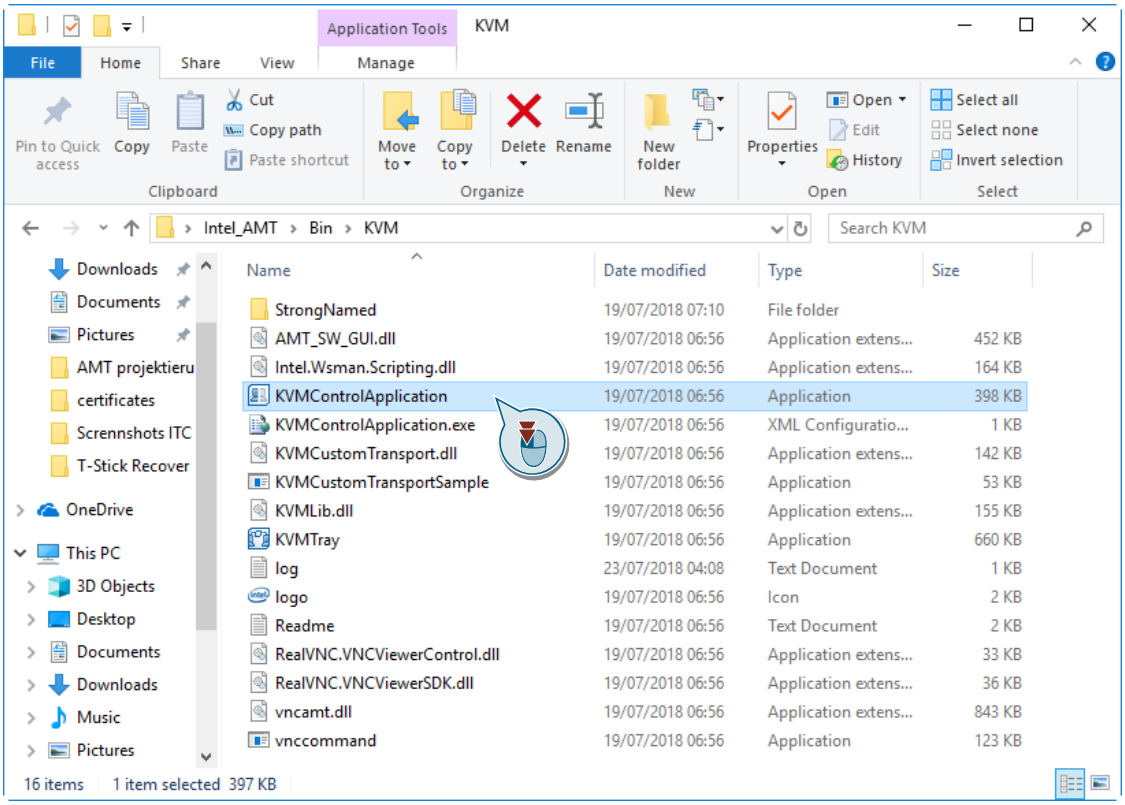
Note The IP address must be different from the actual IP address of the IPC, otherwise there will be communication problems! When exiting the MEBx configuration, save your settings.

Settings on the computer

To access the VTC server of the Intel AMT chip with the ITC, you must first change the ports of the VNC because the ITC cannot access the protocol of the standard port.

1. To do this, download the "Intel® Active Management Technology SDK" software at the following link (https://software.intel.com/en-us/amt-sdk/download) on a computer that is in the same network as the IPC and its AMT.
2. Unpack the zip file.
3. Open the just unpacked folder named "AMT_SDK_12.0.0.9". Navigate to the path "AMT_SDK_12.0.0.9 > Windows > Intel_AMT > Bin > KVM" and open the program "KVMControlApplikation".

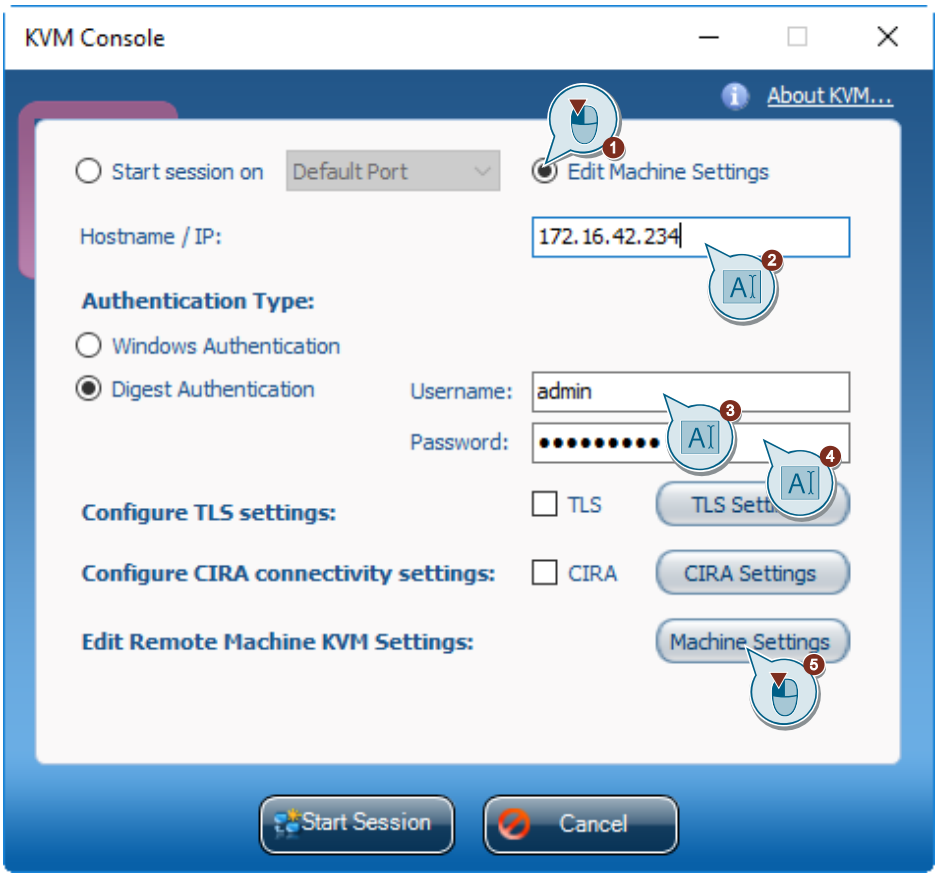
Figure 5-25



Note If the program does not start, depending on the system, it may be necessary to copy the dll files from the path "Intel_AMT > Bin64 > KVM" to the folder "Intel_AMT > Bin > KVM".

4. This opens the "KVM Console". Activate the option "Edit Machine Settings". (1) In the Hostname/IP field, enter the IP address you assigned to the AMT chip in the previous section. (2) Enter the default user name "admin" in the field labeled "Username". (3) Enter the AMT password set in the previous section into the password field. (4) Continue by clicking on the "Machine Settings" button. (5)

Figure 5-26



Note

Make sure that the computer on which you configure the "Machine Settings" and the computer on which you want to set up the AMT VNC server communicate with each other. Furthermore, you should make sure to enter all information for the connection correctly, as it may otherwise lead to a deterioration of the functionality of the KVM console.

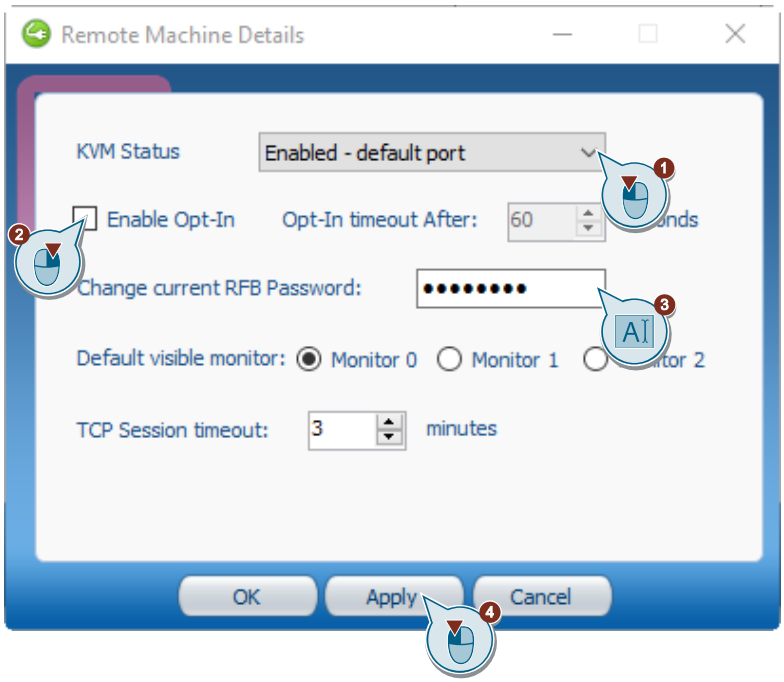
5. This opens the "Remote Machine Details" window. Set "KVM Status" in the drop-down list to "Enable default port". (1) Disable the "Enable Opt-In" option. (2) Now enter a password for the VNC access in the field "Change current RFB Password". (3) You will need this to connect to the AMT VNC server. It may be different from the AMT access password. Apply the settings with the "Apply" button. (4)

Note

The RFB password must meet the following conditions:

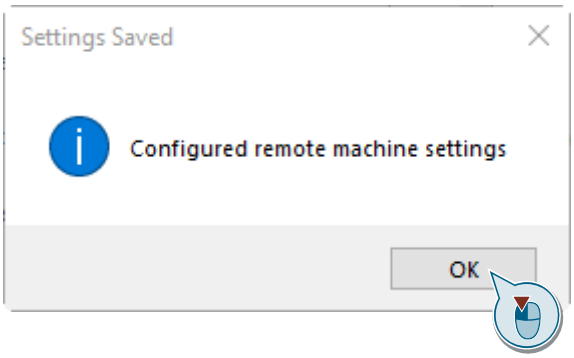
- It has to be 8 digits,
- Upper/lower case text,
- Numbers,
- and contain special characters.

Figure 5-27



6. A window opens which confirms the changes made to the machine settings. Close the window and the window of the "Remote Machine Details" with the "OK" buttons.

Figure 5-28



Result

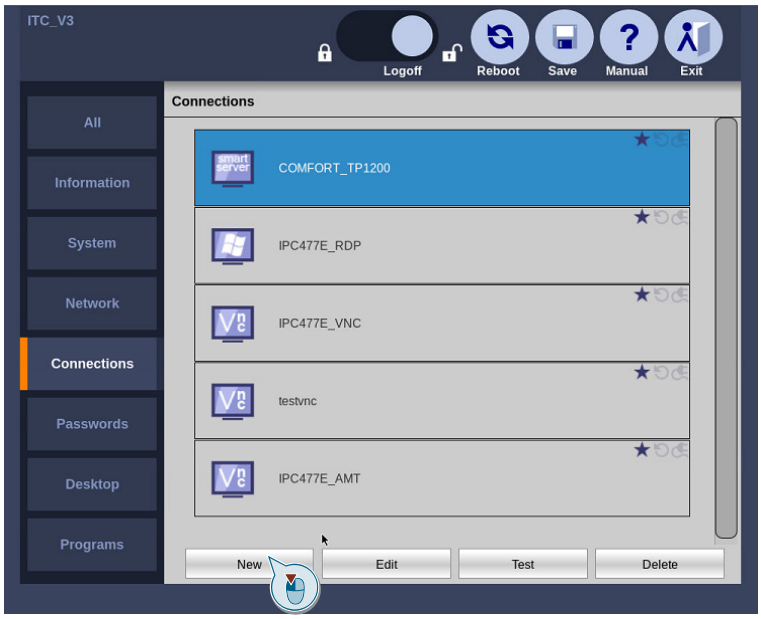
You have successfully configured the Intel AMT VNC server and can now connect to the ITC.

5.4.3 Setting up the AMT-VNC connection with the ITC

This section describes how to connect the ITC to an AMT-VNC server.

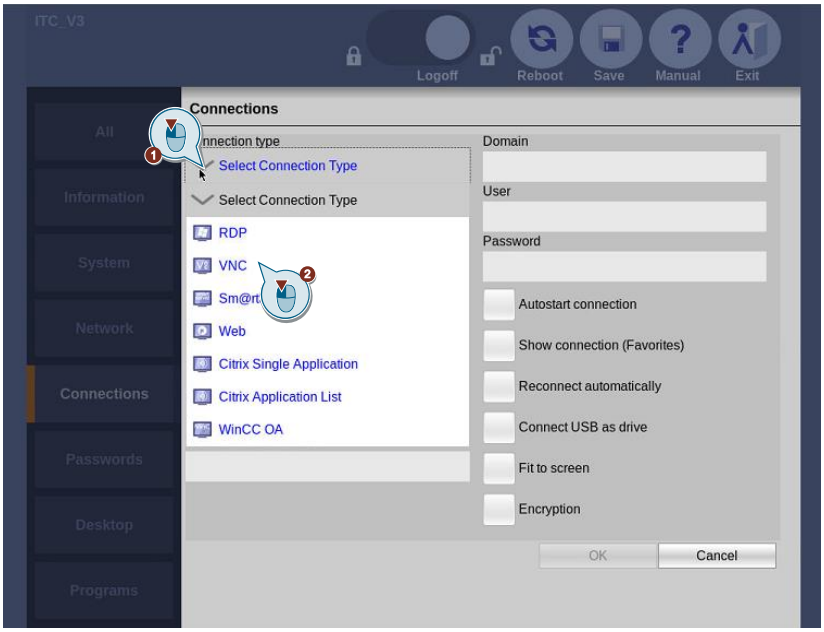
1. Open the settings of the ITC and log in as administrator. Open the configuration window for the configured connections (as described in section 4).
2. Click the "New" button at the bottom of the image to create a new connection.

Figure 5-29



3. You will be directed to the configuration screen for setting up and editing remote connections. Depending on the selected connection type, unnecessary fields are grayed out. Open the drop-down list labeled "Select Connection Type" (1) and select the VNC connection. (2)

Figure 5-30



4. Enter the parameters

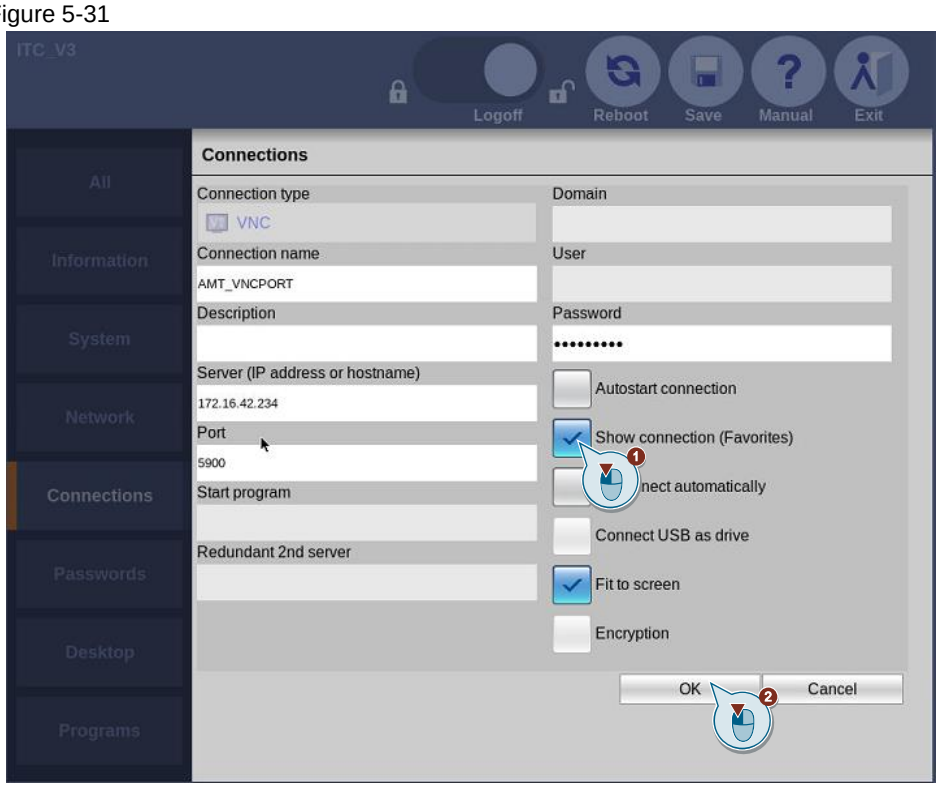
- Connection name (freely selectable),
- Server IP address (address that you have configured in the MEBx settings),
- Port (standard port 5900),
- Password (RFB password set via KVM Configuration Tool)

in the appropriate fields.

In the checkboxes you can activate and deactivate further functions of the connections. Only the functions that are relevant for the used protocol type can be selected.

5. Activate the "Show connection (Favorites)" function to quickly call the connection. (1)
6. Confirm the creation of the connection with the "OK" button. (2)

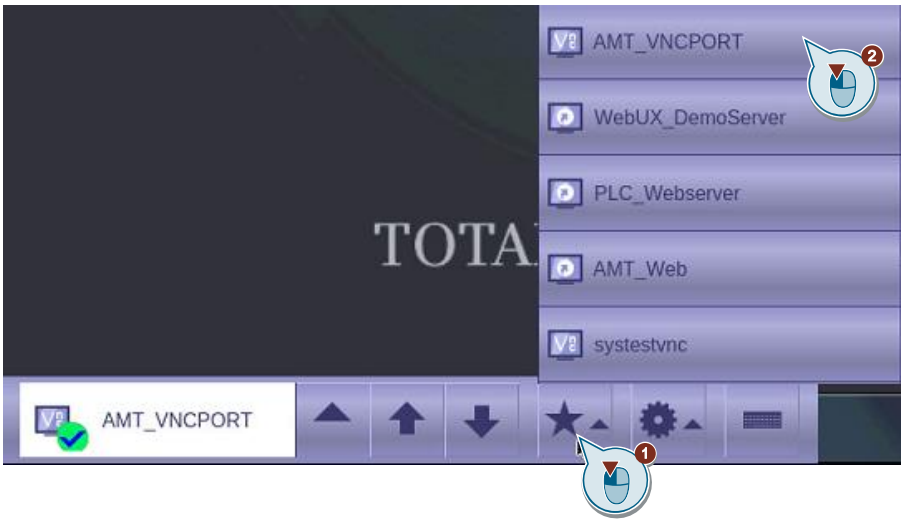
Figure 5-31



Result

You have successfully configured an AMT-VNC connection. You can find it on the start screen by clicking on the star icon (Favorites). (1) Clicking on the connection allows you to remotely access the screen of your AMT-VNC server and see its contents. (2) The main advantage is that the AMT-VNC server is active with the AC adapter plugged in, allowing you to remotely access the BIOS and remotely reboot the system. The screen accessed via AMT is marked with a red/amber blinking frame as long as the connection is active.

Figure 5-32



5.5 Intel AMT web server

This section explains what settings you need to make on the server machine to enable the AMT web server and how to connect to the ITC.

5.5.1 Components used

This application example was created with these hardware and software components:

Table 5-5

Components	Number	Article number	Note
IPC477D	1	6AV7240-8MD00-0PA8	
ITC2200 V3	1	6AV6 646-1BA22-1NA0	

5.5.2 Setting up the Intel AMT web server

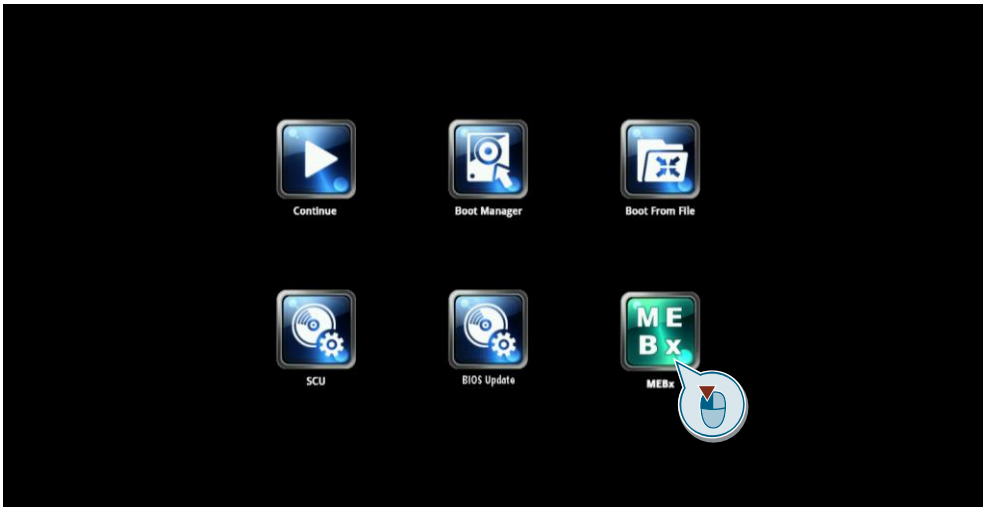
Depending on the IPC and installed BIOS/AMT version, the settings and their location may change. Information about your device can be found in the corresponding manual. Upon entering the type designation of your IPC into the filter mask under the following link, you will be redirected to the appropriate manual.

7. Restart the computer and press the <ESC> button upon startup to open the BIOS selection menu.

Note The setup applies to the system of the IPC 477E and may differ in other computer systems. Please familiarize yourself with keyboard shortcuts and settings of the MEBx of your PC.

8. Use the arrow keys to go to the "MEBx" option and open it with the <Enter> button.

Figure 5-33



9. Select "MEBx Login".
10. Enter the standard password "admin".

Change the password. The new password must comprise:

- At least eight characters
- An upper case letter
- A lower case letter
- A number
- A special character (! @ # $ % ^ & *)
- The underscore "_" and space characters are valid in the string but do not increase the complexity of the password.

Note If you no longer know the password, you must reset Intel® AMT to the default settings. Backup the password in case it is lost.

11. Switch to the submenu "Intel (R) AMT Configuration" and activate "Manageability Feature Selection".
12. In the "Intel (R) AMT Configuration" submenu, enable access to the network via "Activate Network Access".
13. Confirm the following dialogs with "Y".
14. Disable the "DHCP mode" in the "Intel (R) AMT Configuration > Intel (R) ME Network Setup > TCP/IP Settings > Wired LAN IPV4 Configuration" settings. Assign the desired IP address, a suitable subnet mask and the standard gateway if you want to communicate with systems outside your network.

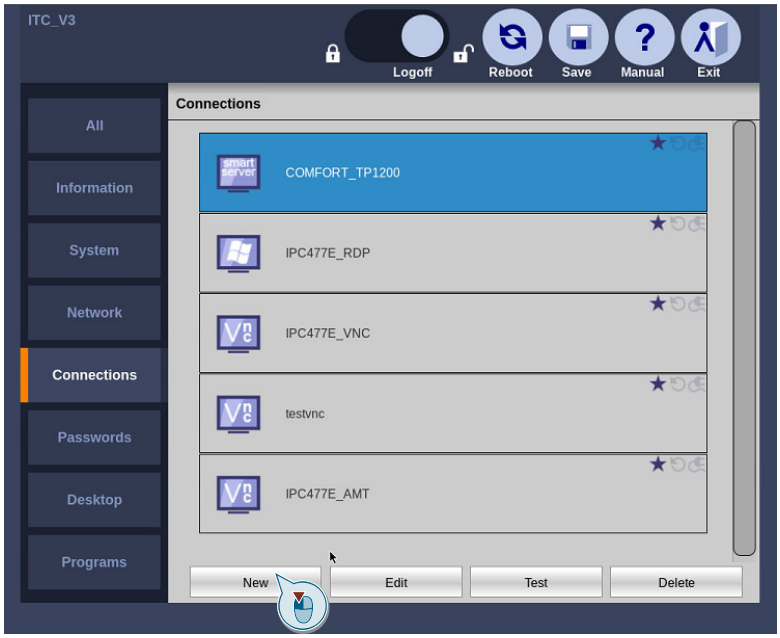
Note The IP address must be different from the actual IP address of the IPC, otherwise there will be communication problems! When exiting the MEBx configuration, save your settings.

5.5.3 Setting up the AMT web server connection with the ITC

This section describes how to connect the ITC to the AMT web server of an IPC477D.

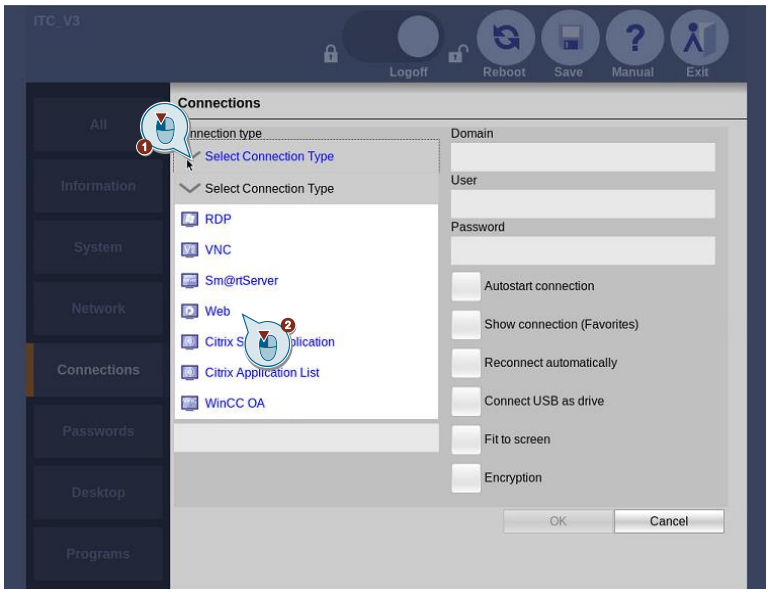
1. Open the settings of the ITC and log in as administrator. Open the configuration window for the configured connections (as described in section 4).
2. Click the "New" button at the bottom of the image to create a new connection.

Figure 5-34



3. You will be directed to the configuration screen for setting up and editing remote connections. Depending on the selected connection type, unnecessary fields are grayed out. Open the drop-down list labeled "Select Connection Type" (1) and select the web connection. (2)

Figure 5-35



4. Enter the parameters

- Connection name (freely selectable),
- URL="http//" + server IP address + ":" + port (standard port 16992),

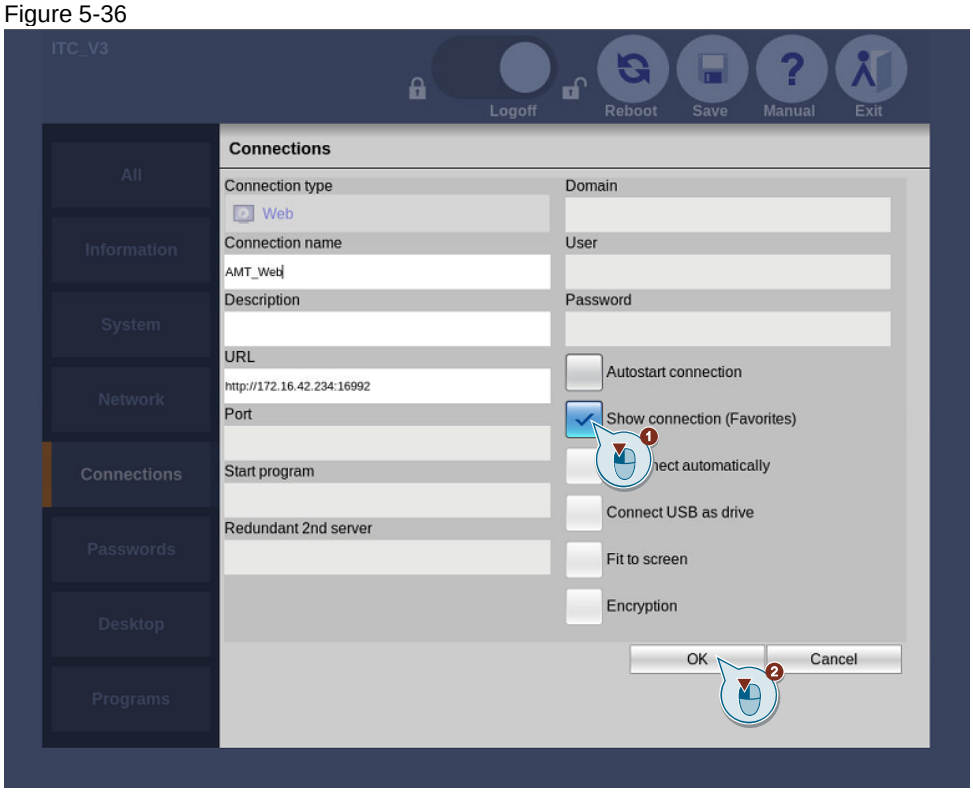
in the appropriate fields.

Note For the web connection, the port is appended to the IP address in the "URL" field. A ":" is set as separator between the IP address and the port number. The port field is grayed out when configuring the web connection.

In the checkboxes you can activate and deactivate further functions of the connections. Only the functions that are relevant for the used protocol type can be selected.

5. Activate the "Show Connection (Favorites)" function to quickly call the connection. (1)
6. Confirm the creation of the connection with the "OK" button. (2)

Figure 5-36



Result

You have successfully configured a connection to the AMT web server. You can find it on the start screen by clicking on the star icon (Favorites). (1) Click on the connection to access the screen of your AMT web server. (2)

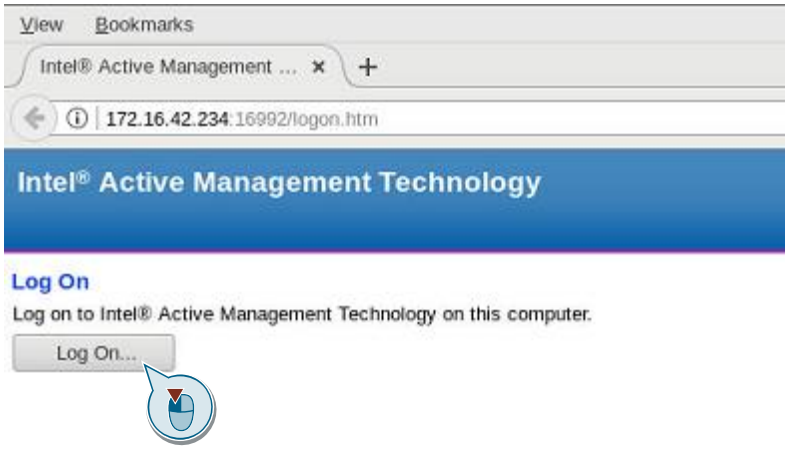
Figure 5-37

Demonstration AMT webserver

This example shows you how to connect to the AMT web server of an IPC.

1. Call up the connection to the web server that you configured in the previous section via ITC. You will get to the login page of the AMT server. Click on the "Log On ..." button to log in.

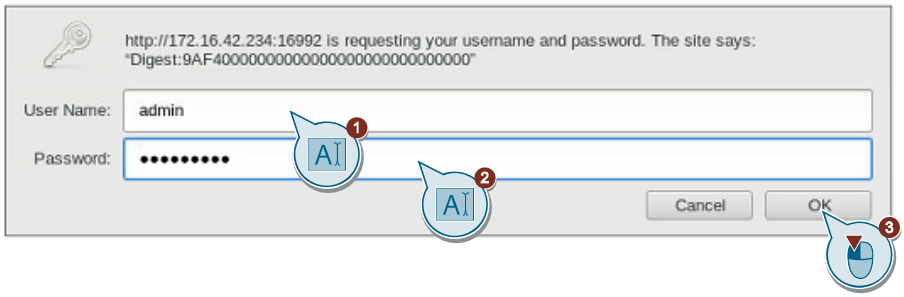
Figure 5-38



2. This opens a login windows in which you must enter the username (1) and the password you configured in the AMT settings. (2) Confirm your entries with the "OK" button. (3)

Note The default username for accessing the AMT web server is "admin".

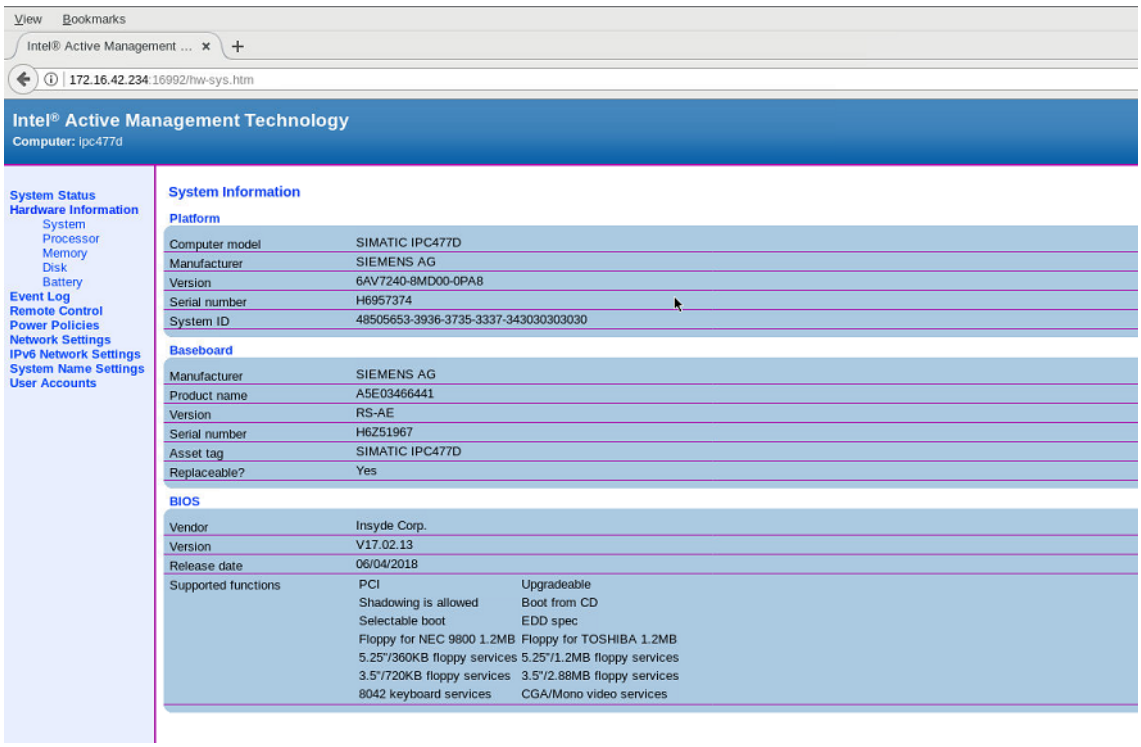
Figure 5-39



Result

You now have access to the web servers of the Intel AMT technology. Here you can view various information as well as an event log of your computer, restart the PC and change various settings of the AMT technology.

Figure 5-40



5.6 WinCC project with web-enabled runtime

This section explains which settings you have to make on the server computer and on the WinCC project (V7.4/V15) and how to connect to the ITC via WebUX.

5.6.1 Components used

This application example was created with these hardware and software components:

Table 5-6

Components	Number	Article number	Note
ITC2200 V3	1	6AV6646-1BA22-1NA0	
SIMATIC WinCC Professional V15	1	6AV2103-0DA05-0AA5	• With 512 power tags • With DVD
SIMATIC STEP 7 Prof. V15	1	6ES7822-1AA05-0YA5	• Floating license • With USB stick • With DVD
SIMATIC WinCC V7.4		6AV6381-2BN07-4AX0	• With USB stick • With DVD

5.6.2 Software requirements to the server

For your computer to be able to share pictures on the web, it is necessary to activate the functions of the IIS in the system.

To enable the use of WebUX, it is necessary to configure the firewall of your system. To do this, you must create incoming and outgoing rules for the WebUX port. The default port that WebUX uses is https port 443.

Additional information on the configuration of web-enabled WinCC projects is available at the following link. (Article ID: 109744149)

5.6.3 Configuration of the server V7.4

This section shows you which settings you must make in the WinCC project (V7.4) in order to make the HMI web-enabled.

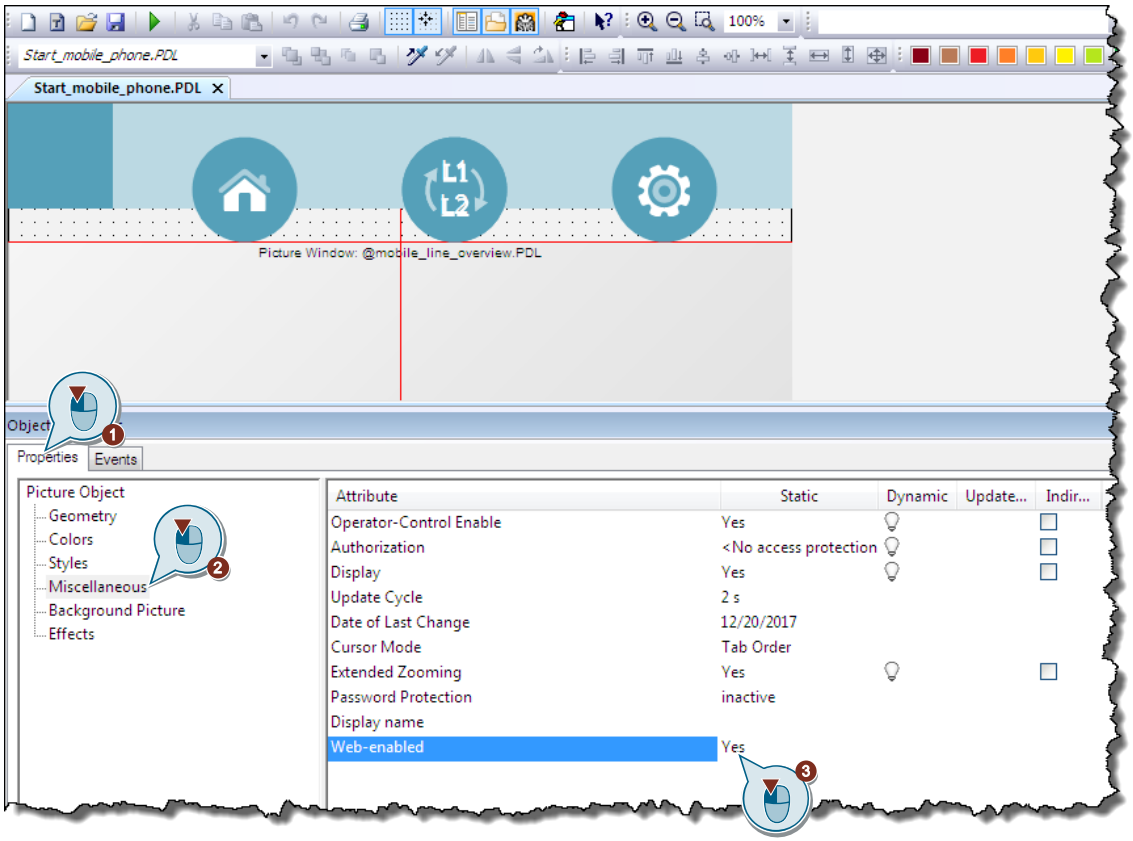
Setting in the process picture

Any image that you would like to access via the HTML5 browser must first be shared with WebUX.

1. To do this, open the required pictures of the WinCC project in the "Graphic Designer".

2. Open the "Object properties" and switch to the settings with the button "Properties". (1) In the left list, select the category "Miscellaneous". (2) Set the web-enabled option to "Yes". (3)

Figure 5-41



3. Repeat these steps for all images that you want to make web-enabled.

Result

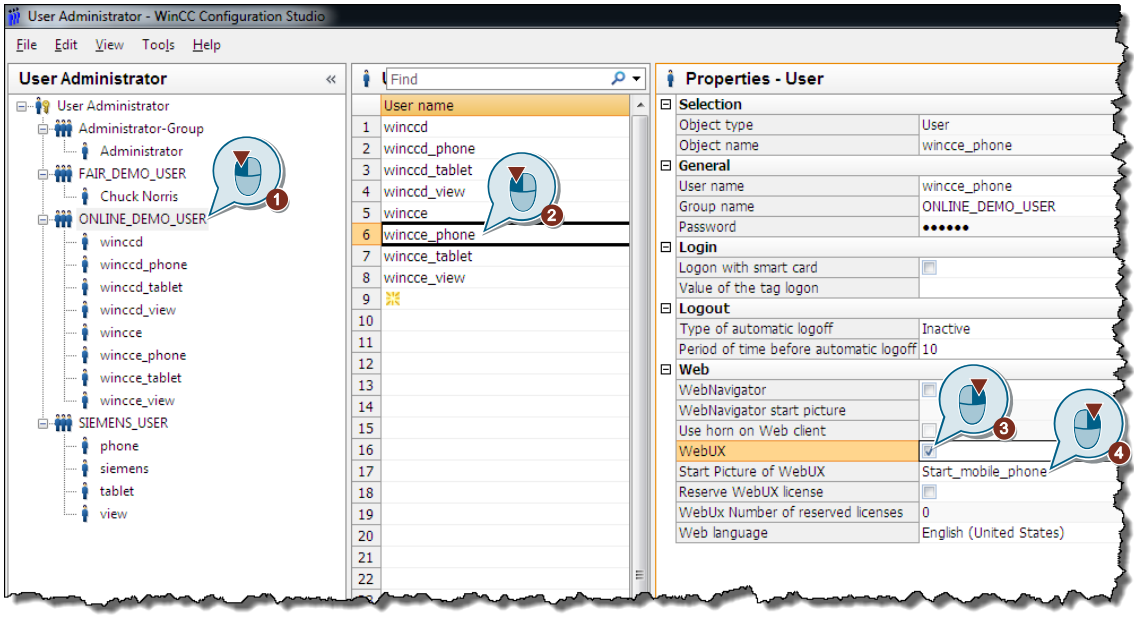
The images you want can now be accessed via the HTML5 browser.

Settings in the user administration

To log in via a user in the online project, you must first release it for web applications and assign it a start screen.

1. Open "User Administration" in your project.
2. Select a user group. (1) Select the user who should have online access. (2) Activate the entry "WebUX" in the category "Web" and check the box. (3) Define the desired start screen for this user. (4)

Figure 5-42



3. Carry out step 2 for all users who are to receive web access.

Note User credentials are the same as local access to the project. A separate start screen for online access can be set for each user. They see this as soon as they log in via a web browser.

5.6.4 Configuration of the server V15

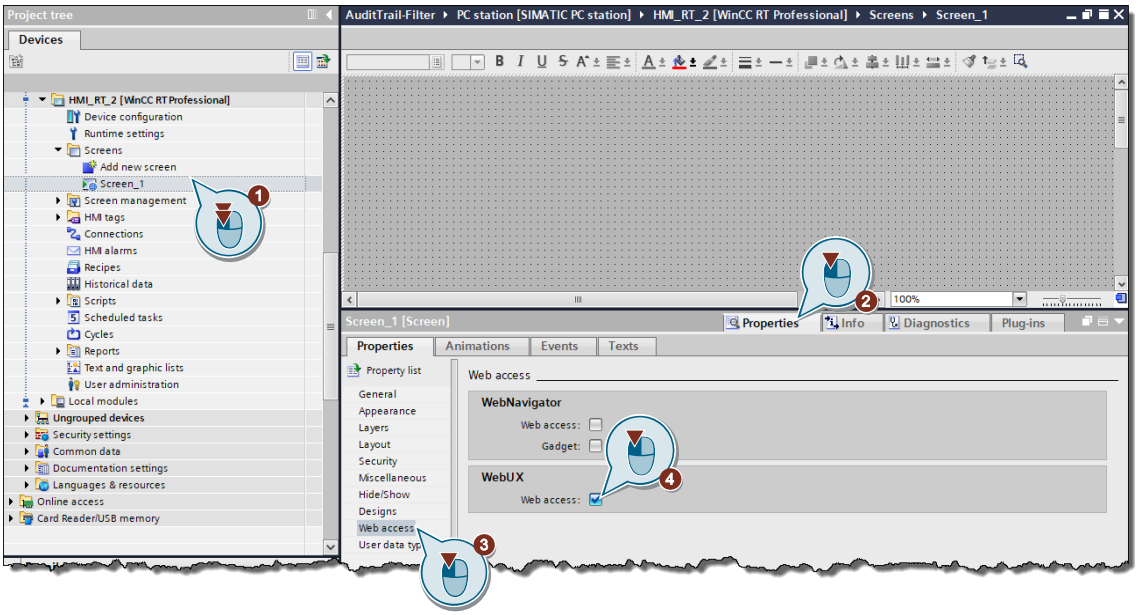
This section describes which settings you must make in the WinCC project (V15) in order to make the HMI web-enabled. This option is only available for WinCC Professional.

Setting in the process picture

Any image that you would like to access via the HTML5 browser must first be shared with WebUX.

1. In the "Project tree" of your RT Professional, open the image that you want to make web-enabled. (1)
2. Open the "Properties" with the button of the same name at the bottom of the screen. (2) In the area navigation, click the Web Access category. (3) Tick the checkbox of the WebUX option. (4)

Figure 5-43

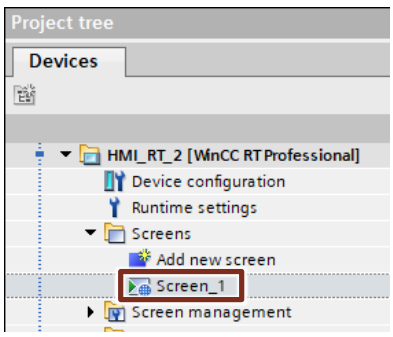


Repeat these steps for all images that you want to make web-enabled.

Result

The images you want can now be accessed via the Internet/Intranet. You can see that the image is web-enabled, by the small blue Internet symbol on the image icon in the project navigator.

Figure 5-44

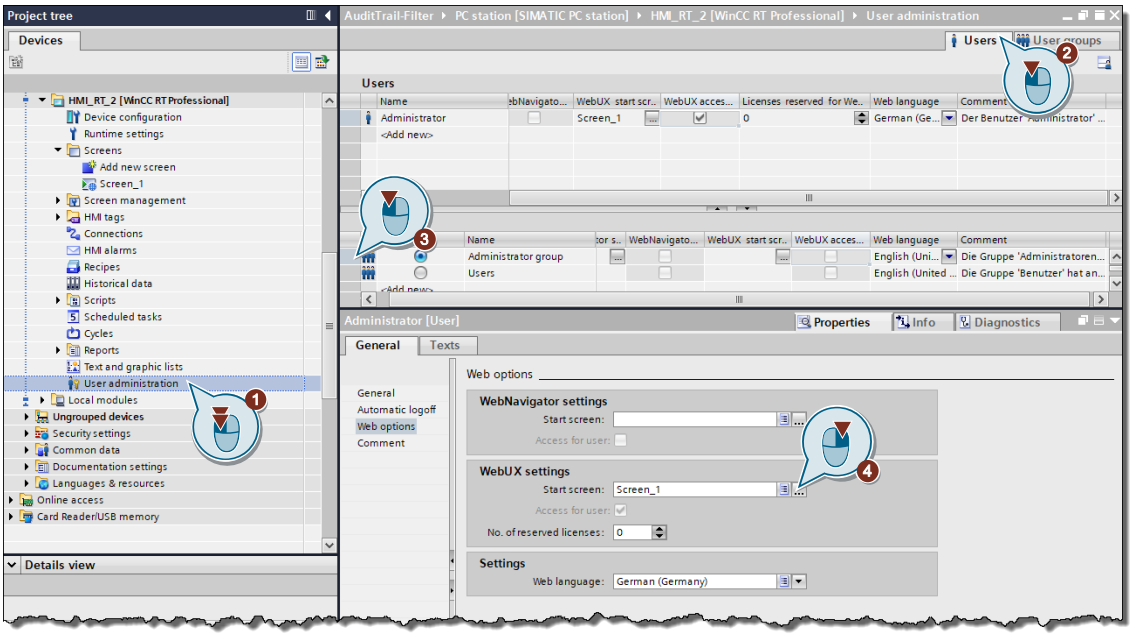


Settings in the user administration

To log in via a user in the online project, you must first release it for web applications and assign it a start screen.

1. Open the "User Administration" in your project. (1)
2. Switch to the "User" tab. (2) Select the user who is to have online access. (3) Define the desired start screen for this user in the WebUX area. (4) The check mark for "Access for User" is set automatically when the image is selected.

Figure 5-45



3. Carry out step 2 for all users who are to receive web access.

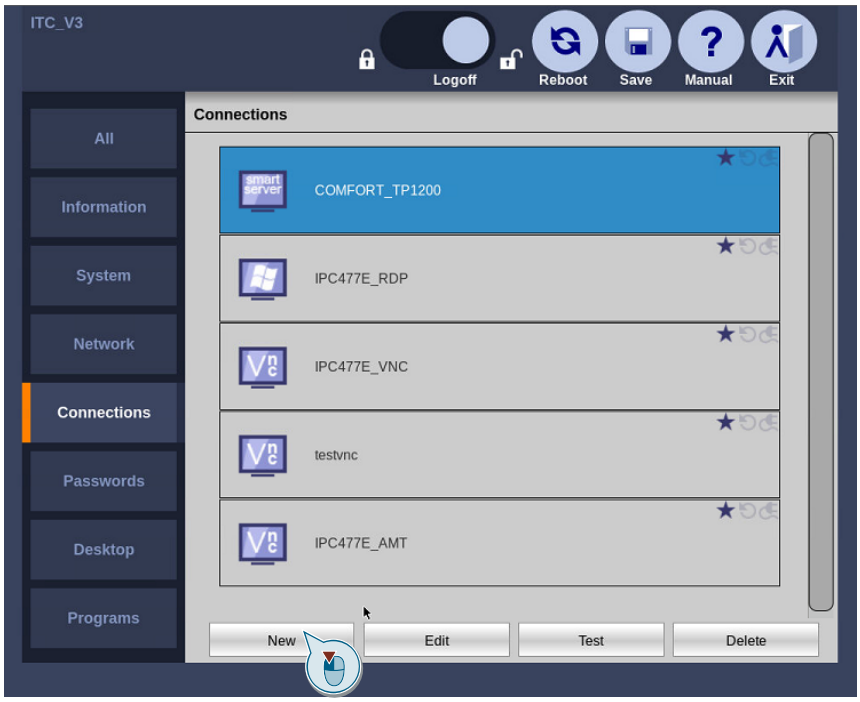
Note User credentials are the same as local access to the project. A separate start screen for online access can be set for each user. They see this as soon as they log in via a web browser.

5.6.5 Set up the connection with the ITC

This section describes how to connect the ITC to a WebUX web server. The configuration is shown as an example for the WebUX demo access of the Ecole filling system. Additional information is available at the following link. (Article ID: 45027800)

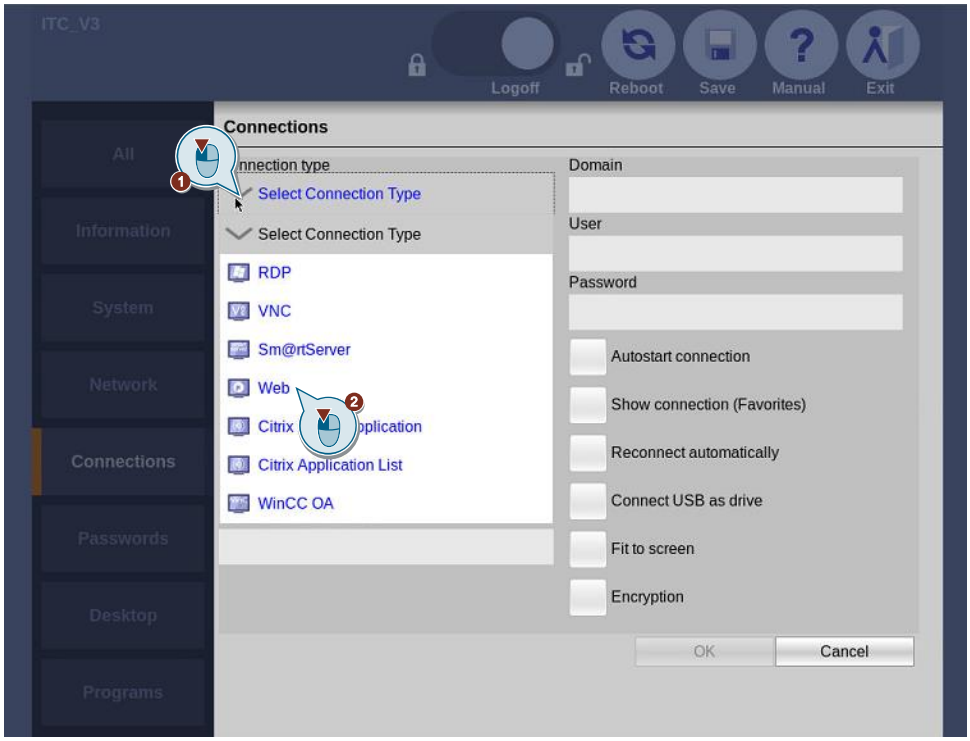
1. Open the settings of the ITC and log in as administrator. Open the configuration window for the configured connections (as described in section 4).
2. Click the "New" button at the bottom of the image to create a new connection. You will be directed to the configuration screen for setting up and editing remote connections. Depending on the selected connection type, unnecessary fields are grayed out.

Figure 5-46



3. Open the drop-down list labeled "Select Connection Type" (1) and select the web connection. (2)

Figure 5-47



4. Enter the parameters

- Connection name (freely selectable) and
- URL (Ecole access: https://62.245.153.66:433)

  in the appropriate fields.

Note

The entry "https" always points to the standard port "443". If you have changed this in your system, the entry of the URL is as follows:

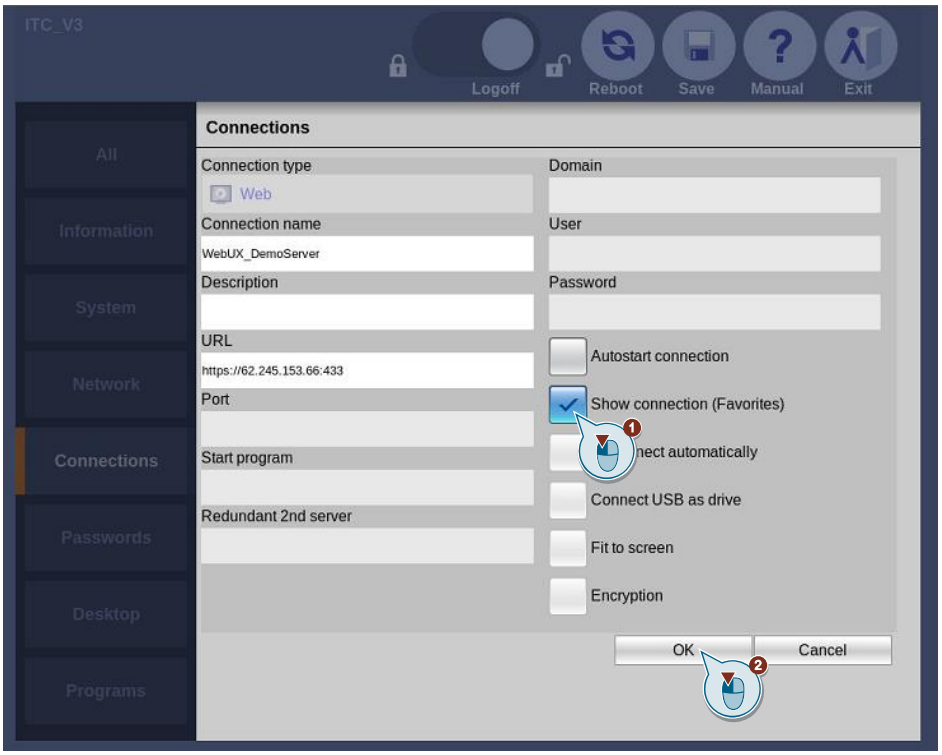
"https://" + "IP" + ":" + "Port",

As shown in Figure 5-8.

In the checkboxes you can activate and deactivate further functions of the connections. Only the functions that are relevant for the used protocol type can be selected.

5. Activate the "Show Connection (Favorites)" function to quickly call it up. (1)
6. Confirm the creation of the connection with the "OK" button. (2)

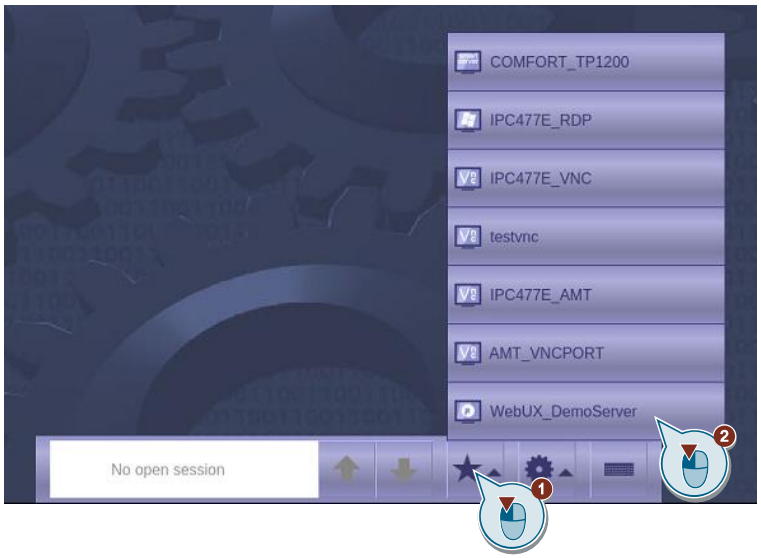
Figure 5-48



Result

You have successfully set up a WebUX connection. You can find them on the start screen by clicking on the star icon (Favorites). (1) Click on the connection to open the ITC web browser. (2) You will then have access to the web view of your WinCC project.

Figure 5-49



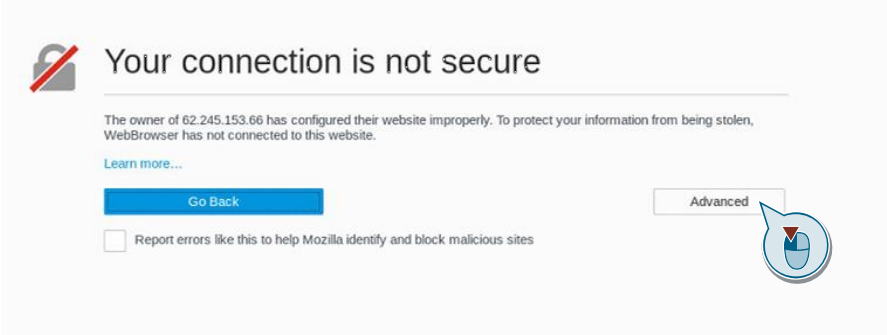
5.6.6 Demonstration of the WebUX server:

This example shows how to connect to the demo web server of the Ecole bottling plant via WebUX. This project has been made available online to give you an idea of web applications and their benefits.

Since certificates between your computer and the server cannot be easily exchanged, the connection is classified as insecure. However, you can safely access it with just a few clicks described below.

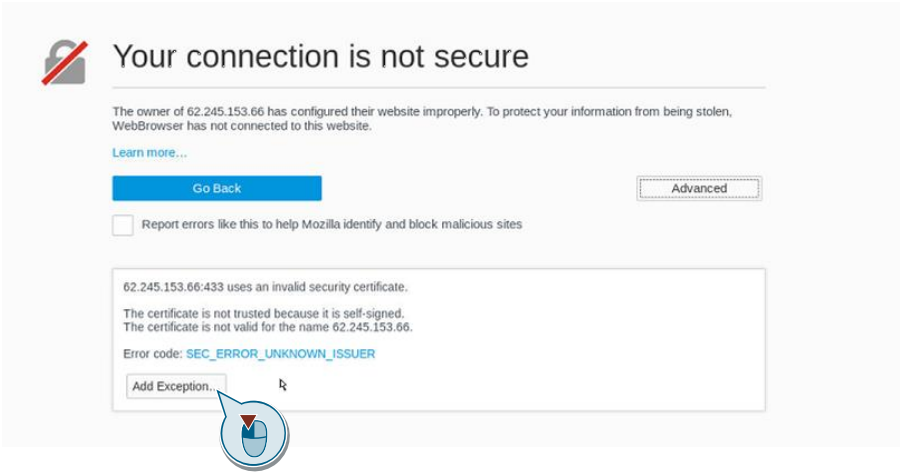
1. Invoke the level in the previous section Configured Web Connection to the ITC.
2. Click the "Advanced" button in the next window.

Figure 5-50



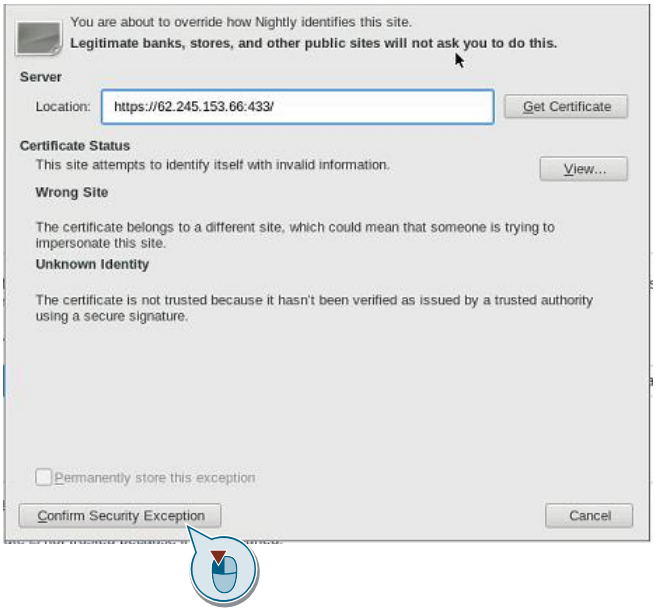
3. Click on the "Add Exception ..." button in the area that opens.

Figure 5-51



4. In the window that opens, click the "Confirm Security Exception" button.

Figure 5-52



5. This takes you to the online login window of the WinCC project. Enter the username "wincce" and the password "winccpass" in the login window for the classic view in English. (1) Confirm the entries with the "Login" button. (2) Further valid login information can be found under the following link. (Article ID: 45027800)

Figure 5-53

Result

You have successfully connected to the ITC on the WinCC demo project and can navigate through the individual screens and view various values and settings.

Figure 5-54

5.7 PLC with web server

This section explains how to enable the web server of an S7-1500 and how to connect to the ITC via the web. Such web servers are already installed in many SIMATIC products and can be activated and called up in a similar way.

5.7.1 Components used

This application example was created with these hardware and software components:

Table5-7

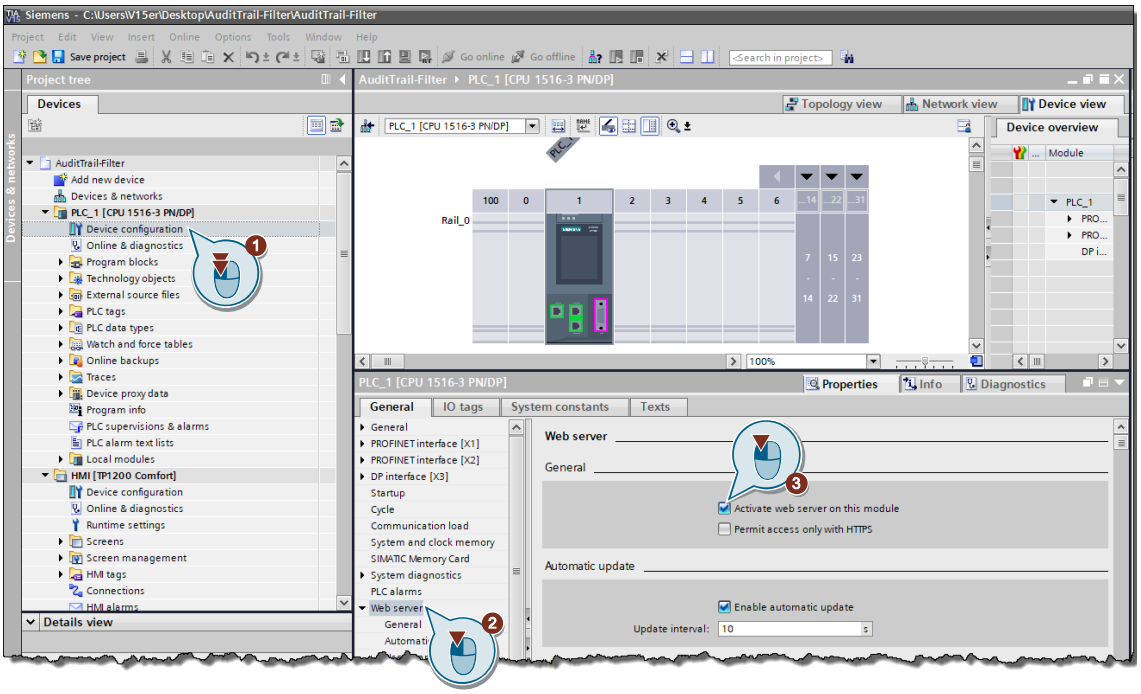
Components	Number	Article number	Note
S7 1500 CPU 1516-3 PN/DP	1	6ES7 516-3AN01-0AB0	Or other S7-1500 CPUs
ITC2200 V3	1	6AV6 646-1BA22-1NA0	

5.7.2 Activating the web server of a PLC S7-1500

This section shows you how to activate the web server of a PLC S7-1500. This is an example and should clarify how uncomplicated the activation of the web server of SIMATIC products is.

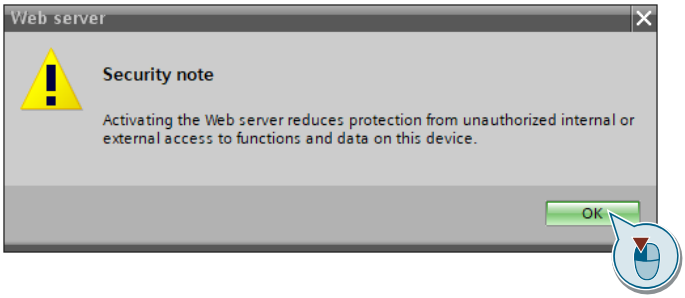
1. Open the "Device configuration" of your controller with a double-click. (1)
2. In the properties window at the bottom of the screen, select the entry "Web server". (2) In the "General" area, activate the web server by ticking the option "Activate webserver on this module". (3)

Figure 5-55



3. A warning follows that states that the security of your system is reduced by activating the web server. Confirm your acknowledgment of the safety warning with the "OK" button.

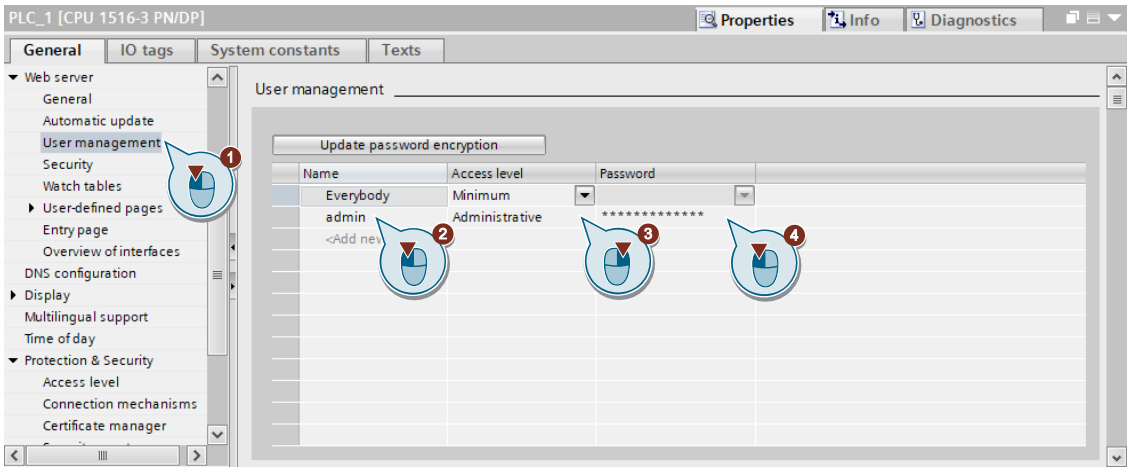
Figure 5-56



Note You can improve the security of the controller by allowing the web server to communicate only through the system's HTTPS port. (lower checkbox in the "General" section) However, this would still require the exchange of certificates for the connection, which is not taken into account in this application example.

4. For full access to the functions of the PLC web server, it is necessary to create an authorized user. In the PLC properties, go to the category "Web server > User management". (1) Create a new user. (2) Assign the rights the user should receive (in this example he will get all rights). (3) Assign a password for the user. (4)

Figure 5-57



5. Save and upload your project to your controller.

Result

You have successfully activated the web server of the PLC and created an authorized user. You can now access it via the web browser.

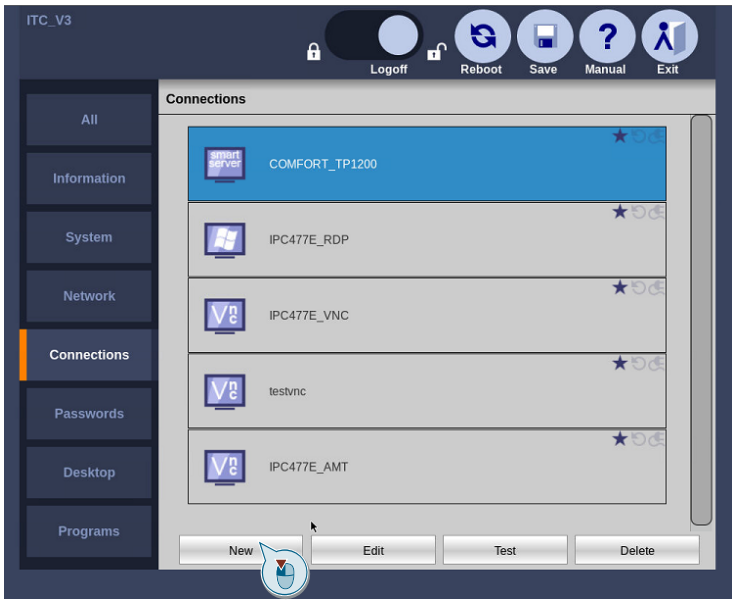
5.7.3 Setting up the S7-1500 web server connection with the ITC

This section describes how to connect the ITC to the web server of a PLC S7-1500.

1. Open the settings of the ITC and log in as administrator. Open the configuration window for the configured connections (as described in section 4).
2. Click the "New" button at the bottom of the image to create a new connection. You will be directed to the configuration screen for setting up and editing

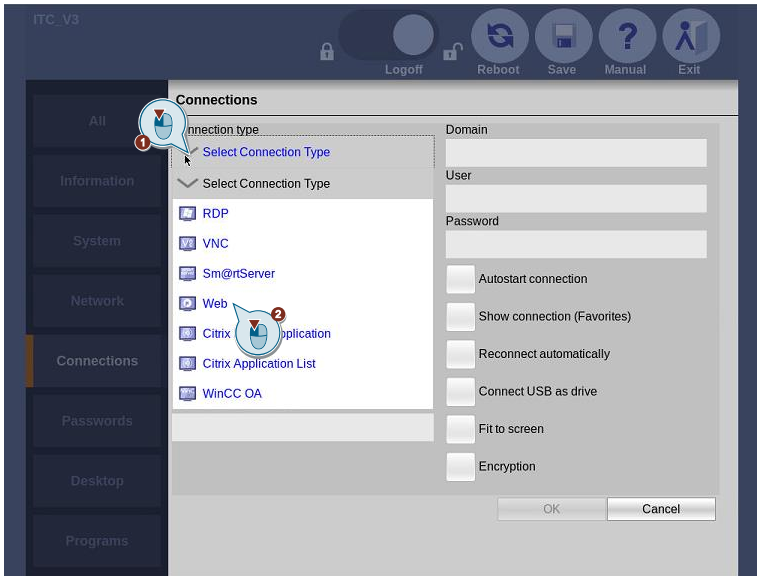
remote connections. Depending on the selected connection type, unnecessary fields are grayed out.

Figure 5-58



3. Open the drop-down list labeled "Select Connection Type" (1) and select the web connection. (2)

Figure 5-59



4. Enter the parameters

- Connection name (freely selectable) and
- URL = "http: //" + "IP address" (address of the S7-1500)

in the appropriate fields.

In the checkboxes you can activate and deactivate further functions of the connections. Only the functions that are relevant for the used protocol type can be selected.

5. Activate the "Show connection (Favorites)" function to be able to call up the function quickly. (1)
6. Confirm the creation of the connection with the "OK" button. (2)

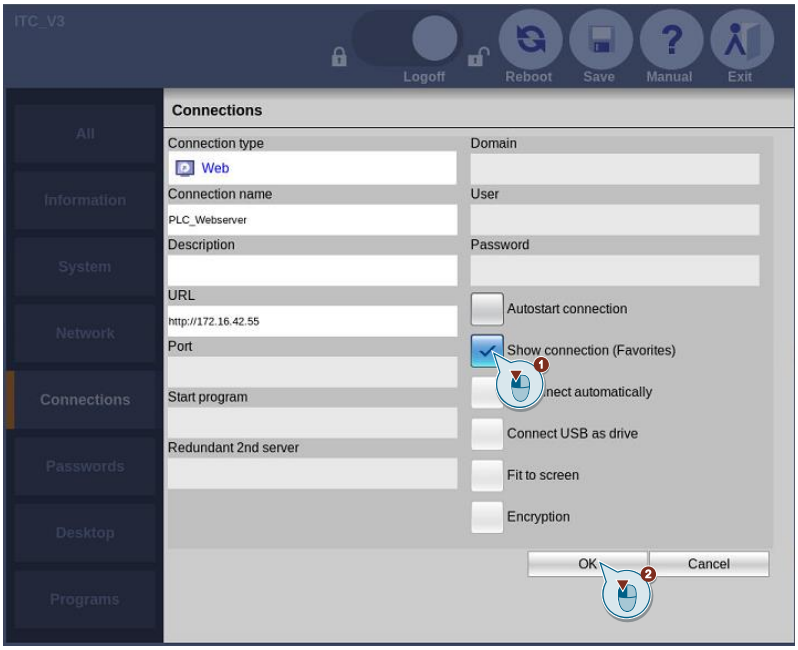
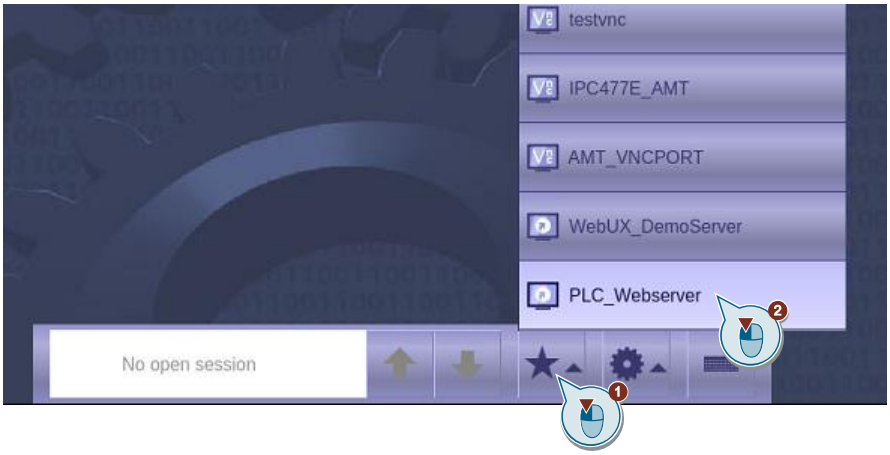


Figure 5-60

Result

You have successfully configured the connection to the web server of the PLC. You can find it on the start screen by clicking on the star icon (Favorites). (1) Click on the connection to open the ITC web browser. (2) You will then be granted access to the web server.

Figure 5-61



5.7.4 Demonstration of the PLC web server:

This section shows you how to connect to the web server of an S7-1500.

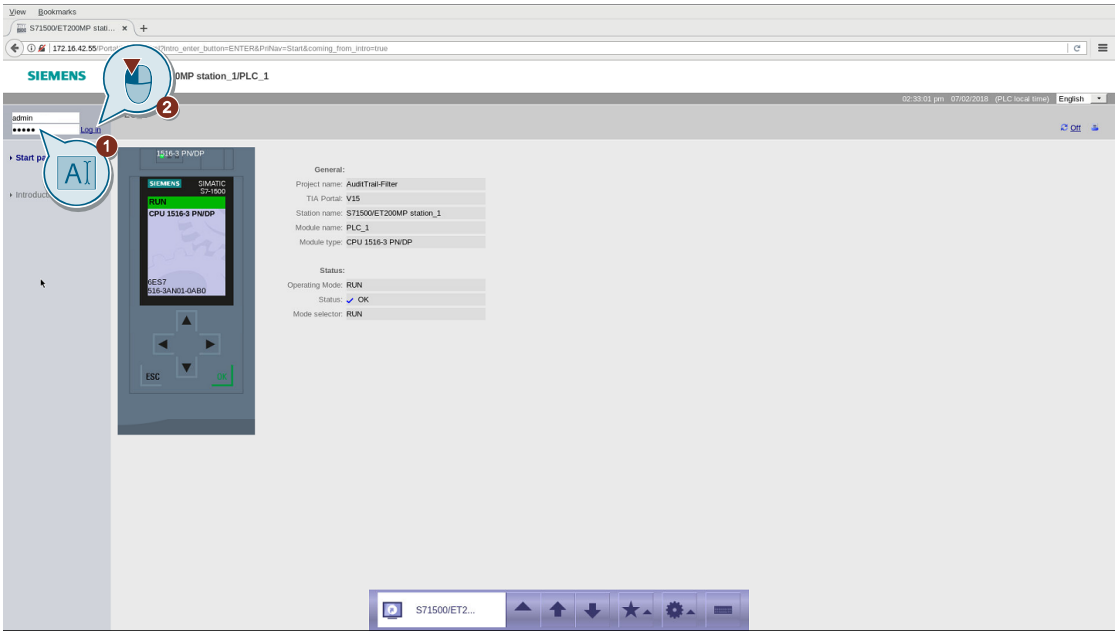
Since no certificates are exchanged between your ITC and your PLC, the connection is classified as insecure.

1. Call up the connection to the web server via ITC. This takes you to the intro page of the S7-1500 web server. Continue by clicking on the "Enter" button.

Figure 5-62

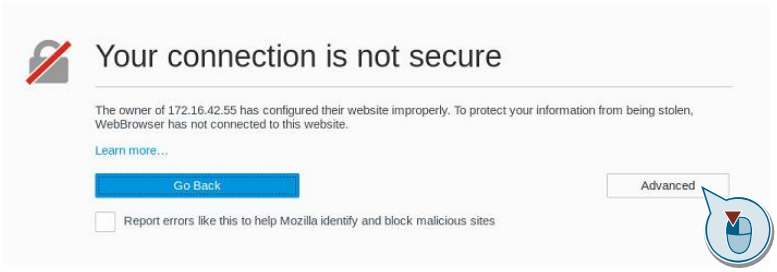
2. This opens the start page of your PLC web server. Enter the user information you have created. (1) Confirm your entries with the "Log in" button. (2)

Figure 5-63



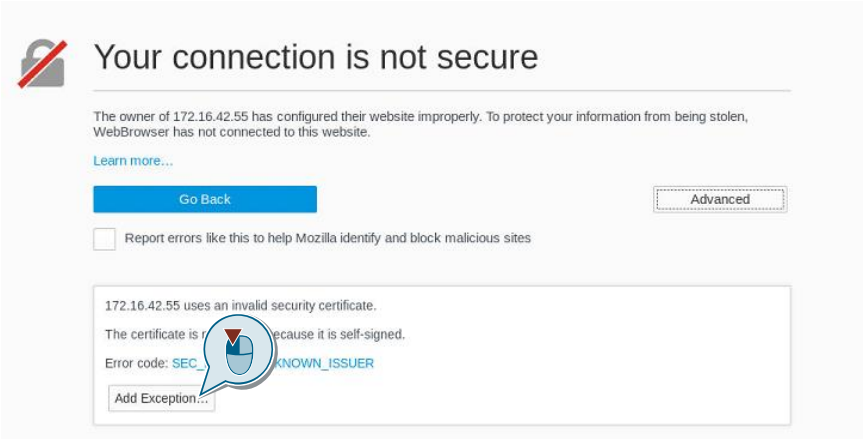
3. Since the browser does not classify this website as safe, you will need to take a few more steps to get full access to the PLC's web server. Click the "Advanced" button in the next window.

Figure 5-64



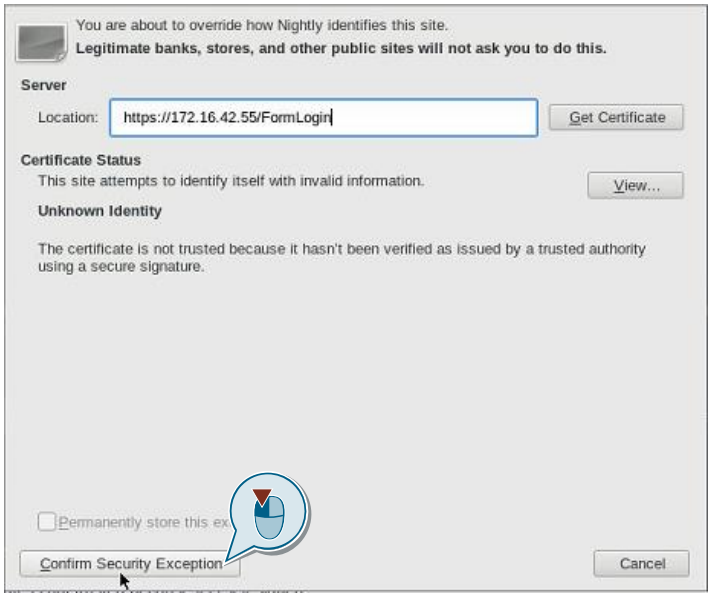
4. Click on the "Add Exception ..." button in the area that opens.

Figure 5-65



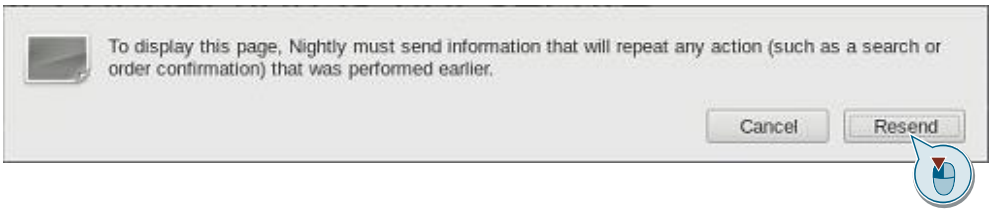
5. In the window that opens, click the "Confirm Security Exception" button.

Figure 5-66



6. Submit the credentials again. Do this by clicking on the "Resend" button.

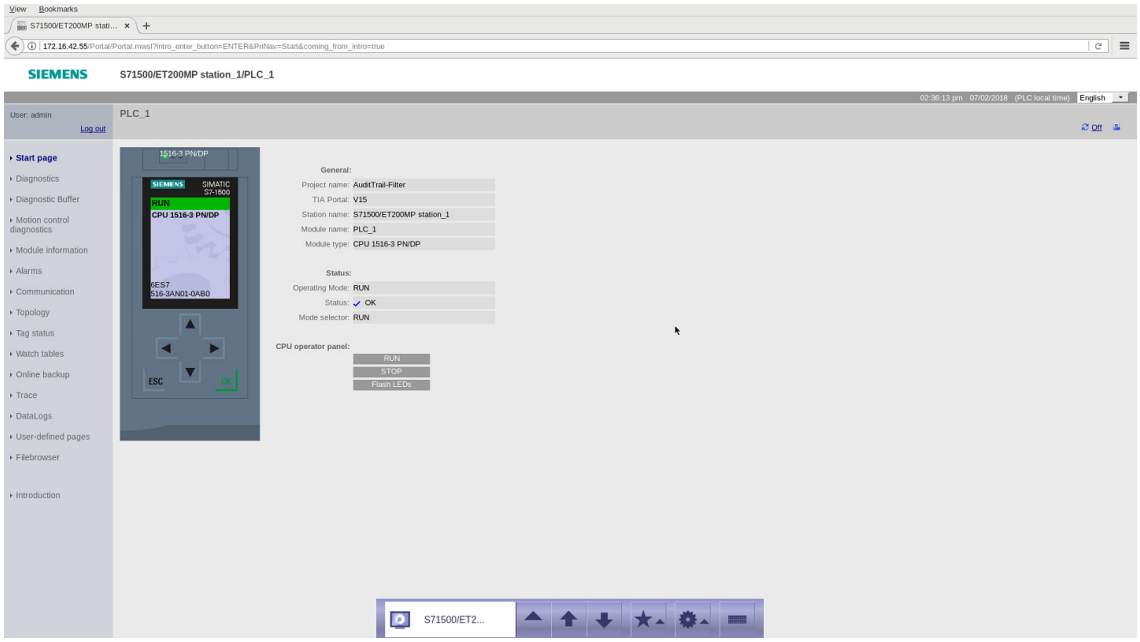
Figure 5-67



Result

You now have full access to the web server of your PLC and can therefore read/change system information or influence the operating status. More information about the S7-1500 web server is available at the following link. (Article ID: 59193560)

Figure 5-68



6 Appendix

6.1 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:
https://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:
www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

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:
www.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:
https://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 Apple iOS, Android and Windows Phone:
https://support.industry.siemens.com/cs/ww/en/sc/2067

6.2 Links and literature

Table 6-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/109758315
\3\	

6.3 Change documentation

Table 6-2

Version	Date	Change
V1.0	MM/YYYY	08/2018