

SIEMENS



Application example • 06/2016

Diagnostic and Remote Maintenance of SIMATIC Industrial PCs

SIMATIC IPC with Intel® AMT



<https://support.industry.siemens.com/cs/ww/en/view/52310936>

Warranty and liability

Note

The Application Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Application Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These Application Examples do not relieve you of the responsibility to use safe practices in application, installation, operation and maintenance. When using these Application Examples, you recognize that we cannot be made liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these Application Examples at any time without prior notice.

If there are any deviations between the recommendations provided in these Application Examples and other Siemens publications – e.g. Catalogs – the contents of the other documents have priority.

We do not accept any liability for the information contained in this document. Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act (“Produkthaftungsgesetz”), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract (“wesentliche Vertragspflichten”). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

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 only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit <http://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <http://www.siemens.com/industrialsecurity>.

Table of contents

Warranty and liability	2
1 Task	4
1.1 Overview	4
1.2 Requirements.....	4
2 Solution	5
2.1 Solution overview	5
2.2 Description of the core functionality.....	5
2.3 Hardware and software components.....	6
2.3.1 Hardware.....	6
2.3.2 Software.....	6
3 Functional Mechanisms	7
3.1 Connection between management PC and SIMATIC IPC	7
3.2 SIMATIC IPC (remote IPC).....	8
3.3 Management PC (local PC)	9
4 Configuration	10
4.1 Possible connection paths	10
4.1.1 Direct connection.....	10
4.1.2 Connection via the internet with standard router.....	11
4.1.3 Connection via the internet with VPN (Virtual Private Network)	12
4.2 Configuration of the remote SIMATIC IPC (BIOS/MEBx)	13
4.2.1 Resetting Intel® AMT to default values	13
4.2.2 Enabling Intel® AMT (basic configuration).....	13
4.2.3 Configuring the IP address manually.....	14
4.3 SIMATIC IPC Remote Manager Setup.....	15
4.4 Optional: Configuring the DSL modem	16
4.5 Transport Layer Security (TLS) configuration	16
4.5.1 Configure remote SIMATIC IPC for TLS.....	17
4.5.2 Adding the remote SIMATIC IPC	20
4.5.3 Creating a certificate.....	21
4.5.4 Create profile.....	22
4.5.5 Loading a profile to the Management Engine	25
4.5.6 Installing certificates on further management PCs – Exporting certificates from the Director	26
4.5.7 Installing certificates on the management PC – Importing certificates.....	28
5 Operation	31
5.1 Non-encrypted connections	31
5.1.1 Operation with the SIMATIC IPC Remote Manager viewer	31
5.1.2 Operation with the WEB GUI	33
5.2 Encrypted connections.....	34
5.2.1 Operation with the SIMATIC IPC Remote Manager viewer	34
5.2.2 Operation with the WEB GUI	35
5.3 Scenario 1 – SIMATIC WinAC	36
5.4 Scenario 2 – Restoring a SIMATIC IPC with an ISO image	38
6 Further Notes, Tips & Tricks, etc.	40
7 Glossary	41
8 Related literature	42
9 History	42

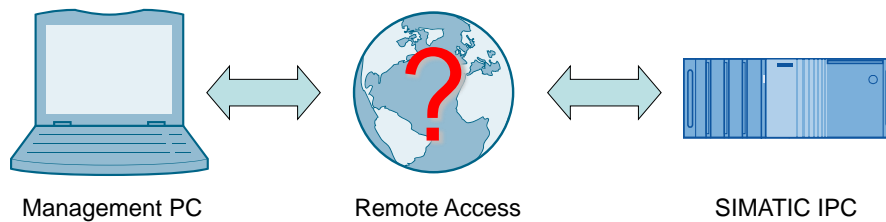
1 Task

1.1 Overview

Overview of the automation task

The figure below provides an overview of the automation task.

Figure 1-1



Description of the automation task

The increasing worldwide distribution of plants increases the demand for accessing automation components, e.g. SIMATIC industrial PCs (IPCs) in remote plants. To be able to use the remote access effectively, it should also be possible for a SIMATIC IPC that is switched-off or no longer operating. A remote operator shall be able to use the same functions as an operator directly in front of the SIMATIC IPCE. In the service case, this may make operation on site unnecessary and save time and costs.

1.2 Requirements

Connection paths

The remote access to the SIMATIC IPC shall be possible via different connection paths.

- Direct connection, for example in the corporate network
- Connection via the Internet

Remote maintenance possible in any situation

Remote maintenance is to be possible irrespective of the status of the SIMATIC IPC. This means that all necessary operating steps are to be possible even if the SIMATIC IPC stops responding or is turned off.

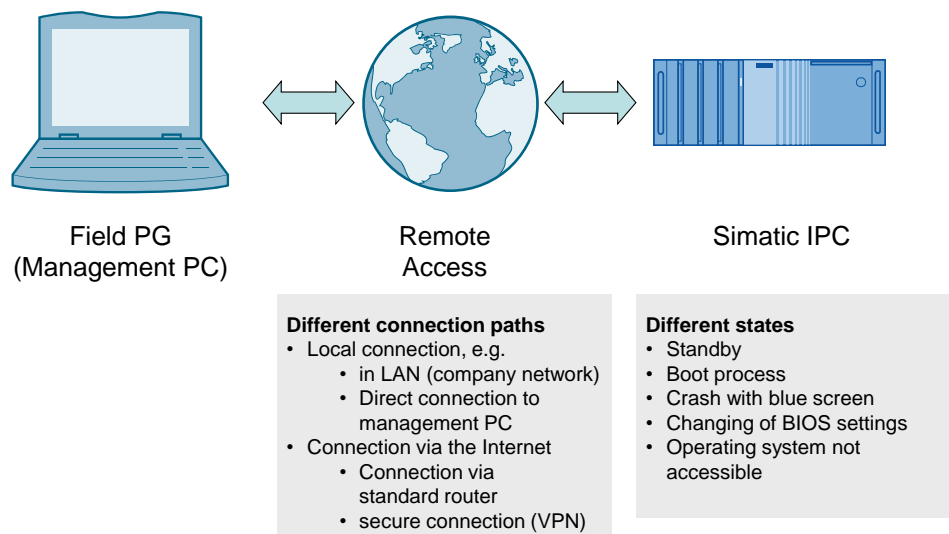
2 Solution

2.1 Solution overview

Schematic layout

The figure below shows a schematic overview of the most important components of the solution:

Figure 2-1



2.2 Description of the core functionality

C, D and E generation SIMATIC IPCs support the Intel® Active Management Technology remote maintenance function.

Intel® AMT is used for remote maintenance of the SIMATIC IPCs. It allows remote maintenance of the SIMATIC IPCs, irrespective of the system status. The administrator performing remote maintenance is thus provided with all the functions that an operator sitting directly in front of the SIMATIC IPC would also have.

This example illustrates different connection paths and, where appropriate, refers to further examples in Online Support.

Intel® Active Management Technology

Active Management Technology (AMT) is an Intel® technology for remote maintenance of SIMATIC Industrial PCs (IPCs) with Intel® AMT using a management PC. It is not necessary to install an operating system on the remote SIMATIC IPC. Intel® AMT provides a large number of functions, for example:

- **Redirecting keyboard, video and mouse (KVM - Keyboard Video Mouse)**
A KVM connection is always possible with the KVM server that is integrated in the firmware. KVM allows access to SIMATIC IPCs with corrupted or missing operating system since the KVM server is integrated in the Intel® AMT hardware. KVM enables you to reboot remote SIMATIC IPCs and make changes to BIOS settings.

2.3 Hardware and software components

- **Remote power management**
The remote SIMATIC IPC can be turned on and off, and restarted from another PC.
- **Remote reboot / IDE redirection**
A remote SIMATIC IPC can be booted from a bootable ISO file on the management PC by integrating it as a DVD disk drive.

2.3 Hardware and software components

2.3.1 Hardware

Using Intel® AMT is only possible on SIMATIC IPCs as of the C generation or on Field PGs as of M4 with Core i5, Core i7 and Xeon processors. Other processors (e.g. Celeron, Core i3 or Core2) do not support Intel® AMT.

Intel® AMT can only be used via Ethernet interface 82577LM / 82579LM / WGI217LM / I217LM.

Note With SIMATIC IPC547G Intel® AMT is only available for motherboard (C236 chipset).

A SIMATIC IPC677D (6AV7260-5GM40-0XX0) was used for this application. The names of the menu items in the BIOS setup and in the MEBx may deviate slightly when using a different device.

2.3.2 Software

Remote SIMATIC IPC

No additional software is necessary on the remote SIMATIC IPC.

Management station

Table 2-1

Component	Qty.	Article number	Note
SIMATIC IPC Remote Manager (single license)	1	6ES7648-6EA01-2YA0	Software for remote maintenance of IPCs with Intel® AMT technology
Manageability Director	1	Intel internet page: http://www.intel.com/ Direct link: \8\	

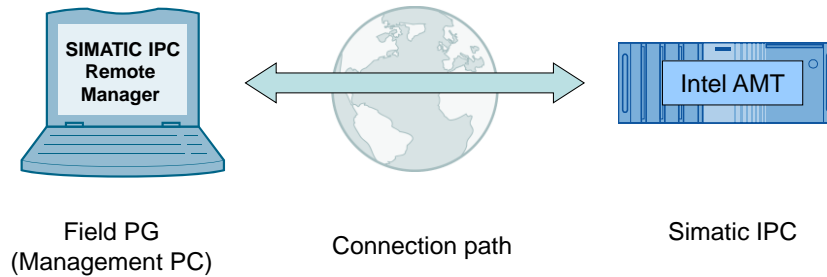
3 Functional Mechanisms

3.1 Connection between management PC and SIMATIC IPC

General

Basically, the management PC with the SIMATIC IPC Remote Manager software establishes a connection to the remote SIMATIC IPC.

Figure 3-1



Via this connection, the SIMATIC IPC screen content is displayed on the management PC and the keyboard and mouse inputs are sent from the management PC to the SIMATIC IPC.

Encrypted/non-encrypted connection

SIMATIC IPC Remote Manager provides the option to use an encrypted connection independent of the connection path.

Note

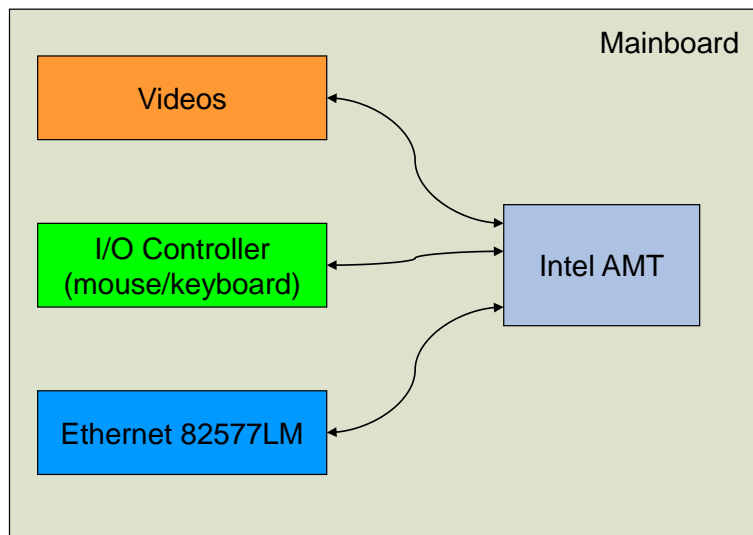
It is recommended to always establish an encrypted connection since, by establishing the remote connection, the user has the same control over the SIMATIC IPC as a user who is located directly in front of the device.

3.2 SIMATIC IPC (remote IPC)

Integration in hardware

Intel® AMT is not software; it is integrated in the hardware.

Figure 3-2



Addressing the SIMATIC IPC

The remote SIMATIC IPC must always be addressable, even if it is turned off or has stopped responding.

Intel® AMT technology that is integrated in the BIOS obtains an IP address via a DHCP server, even when the SIMATIC IPC is turned off. Alternatively, you can manually assign an IP address if no DHCP server is available.

The settings must be made in the extended BIOS menu "Intel® Management Engine" prior to a remote access. (Called with "CTRL-P" or "ESC > MEBx")

Note

The assigned IP address must be static (static IP).

Signaling the remote request/connection

When establishing a remote connection to a remote SIMATIC IPC that is currently being used by a local user, the local user sees a red or red-yellow frame on the screen.

In addition, SIMATIC IPC Remote Manager offers the option to allow the remote connection only after entering a defined PIN code. The local user is then provided with information on a temporarily generated PIN code and must communicate this code to the remote user by appropriate means (telephone, e-mail, etc.).

3.3 Management PC (local PC)

SIMATIC IPC Remote Manager allows to establish a remote connection to a SIMATIC IPC.

The software here is both, management software and operating option for the remote SIMATIC IPCs.

Operating options

SIMATIC IPC Remote Manager provides the operating option of the remote SIMATIC IPC. Local mouse and keyboard inputs are then transmitted to the remote SIMATIC IPC.

Note

The greater part of the data volume associated with this process is generated by the transmitted video signals. When using slow connections (for example, analog modem or GPRS mobile communications), display generation may be delayed.

4 Configuration

4.1 Possible connection paths

General

The following sections list possible connection paths for remote maintenance of SIMATIC IPCs with Intel® AMT.

The basic configuration of the management PC is independent of the connection path and therefore described using the example of a direct connection. Where additional settings are still necessary, they are referred to in the appropriate section.

4.1.1 Direct connection

Definition

At this point, the direct connection designates the connection path when management PC and SIMATIC IPC are in the same network.

Figure 4-1



Accessibility

Management PC and SIMATIC IPC are in the same physical and logical network and can therefore access one another. When using a firewall, the respective ports must be enabled (16992-16995).

This connection path is the simplest case.

Encrypted communication for remote maintenance

Intel® AMT provides encrypted communication (see Chapter 5.2 “Encrypted connections”).

To protect your data, it is recommended to use this encrypted connection.

Configuration

The direct connection does not require any additional configuration steps. Follow the instructions to configure the remote SIMATIC IPC and the management PC. See Chapter 4.2 “Configuration of the remote SIMATIC IPC (BIOS/MEBx)”.

4 Configuration

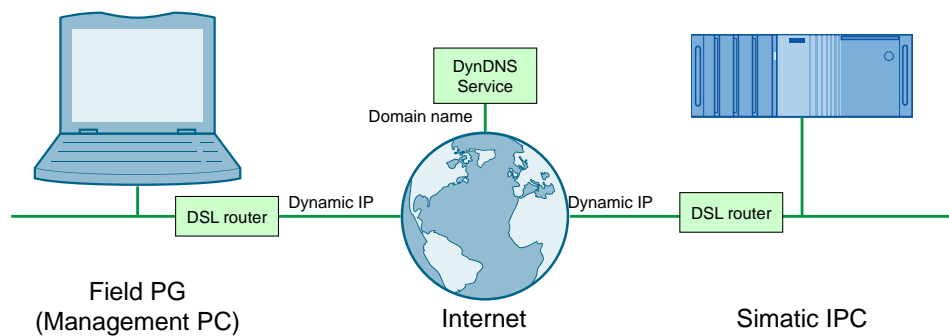
4.1 Possible connection paths

4.1.2 Connection via the internet with standard router

Definition

DynDNS (Dynamic Domain Name System) is an Internet service that allows to set up a fixed host name as an alias for a dynamically changing IP address. It thus enables an Internet user to be always available under the same domain name despite the dynamic IP address.

Figure 4-2



Configuration

Further information as well as an example configuration is available in the “IP based remote networks” application example ([4](#)).

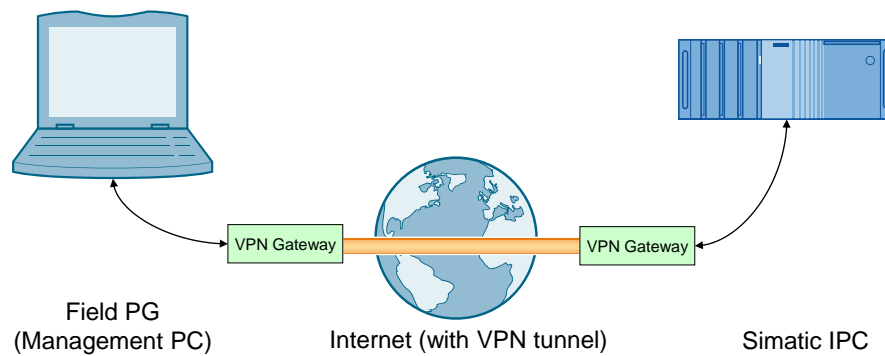
4.1.3 Connection via the internet with VPN (Virtual Private Network)

Definition

The virtual private network (VPN) is a data network which is used to transport private data through a public network (e.g. the Internet). It enables the safe transmission of data via an insecure network.

This connection is usually encrypted and thus secure; however, this is not always the case. A VPN, also referred to as a tunnel, can also be an unsecured clear text tunnel.

Figure 4-3



Configuration

Further information, as well as example configurations, is available in the “IP based remote networks” application example ([4](#)).

4.2 Configuration of the remote SIMATIC IPC (BIOS/MEBx)


Please execute the following steps directly at the SIMATIC IPC. The configuration cannot be performed via remote access.

4.2.1 Resetting Intel® AMT to default values

If Intel® AMT has already been configured at an earlier point, it is advisable to cancel all previous Intel® AMT settings in the MEBx. If the computer is brand-new, you can skip this point.

To reset Intel® AMT to the default values, please proceed as follows:

Table 4-1

No.	Step
1.	When booting, press “ESC” to enter the BIOS selection menu. Select “SCU” and confirm with “Enter” For older SIMATIC IPCs you press “F2” to enter the BIOS.
2.	In the Advanced menu in “Active Management Technology Support”, enable the “Unconfigure ME” option.
3.	Use “F10” (Save and Exit) to exit the BIOS and acknowledge with “Yes”. After automatic restart, the following prompt is displayed: 
4.	Confirm the prompt with "Y" ("Z" on a German keyboard) to cancel all previous settings in the Management Engine (ME).

4.2.2 Enabling Intel® AMT (basic configuration)

To activate Intel® AMT, please proceed as follows:

Table 4-2

No.	Step
1.	If necessary, first reset Intel® AMT to default (see: REF_Ref399224602 \h * CHARFORMAT * MERGEFORMAT Resetting Intel® AMT to default values).
2.	When booting, press “ESC” to enter the BIOS selection menu. Select “SCU” and confirm with “Enter” For older SIMATIC IPCs you press “F2” to enter the BIOS.
3.	In the “Advanced > Active Management Technology Support” menu you set the “Intel AMT Support” option to “Enabled”.
4.	Use “F10” (Save and Exit) to exit the BIOS.
5.	Press “ESC” to enter the BIOS selection menu. Select “MEBx” and confirm with “Enter”
6.	Select “MEBx Login” and confirm with “Enter”.
7.	Enter the standard Password admin .

4 Configuration

4.2 Configuration of the remote SIMATIC IPC (BIOS/MEBx)

No.	Step
8.	<p>Change the default password. The new password must meet the following requirements:</p> <ul style="list-style-type: none">• at least eight characters• one upper case letter• one lower case letter• one number• one special character (! @ # \$ % ^ & *)• underscore _ and blank characters are valid password characters; however, they do not increase password complexity. <p>Note</p> <p>The password must be known only to the remote maintenance staff. If the password is known, this means full access to the SIMATIC IPC.</p> <p>The keyboard layout in the MEBx is "English". When using a German keyboard, you need to consider this when assigning the password.</p>
9.	Enable "Intel® AMT Configuration > Manageability Feature Selection".
10.	Select the option "Activate Network Access" and acknowledge with "Y" ("Z" on a German keyboard)

4.2.3 Configuring the IP address manually

If no DHCP server is available, IP address and subnet mask must be assigned manually.

Procedure


Proceed as follows to manually assign the IP address and subnet mask.

Table 4-3

No.	Step
1.	Go to the following submenu: "Network Setup > TCP/IP Settings > Wired LAN IPV4 Configuration" or "Wired LAN IPV6 Configuration".
2.	In this submenu, make the following settings: <ul style="list-style-type: none">• DHCP mode = DISABLED• IPV4 address = desired IP address• Subnet mask address = desired subnet mask
3.	Press the "ESC" key until the "Are you sure you want to exit?" query appears. Confirm the prompt with "Y" ("Z" on a German keyboard).

4.3 SIMATIC IPC Remote Manager Setup

Table 4-4

No.	Step
1.	<p>Double-click on the "Setup.exe" file to start the installation of SIMATIC IPC Remote Manager on the management PC.</p> 
2.	<p>Follow the instructions of the installer to install SIMATIC IPC Remote Manager.</p>
3.	<p>After successful installation, you have to license SIMATIC IPC Remote Manager with your license key. To do so, open the following shortcut: "Start > All Programs > Siemens Automation > Remote Manager > Advanced > Enter VNC Viewer Plus License Key" Enter your license key.</p>
4.	<p>After successful licensing, you can open the KVM Viewer of SIMATIC IPC Remote Manager as follows: "Start > All Programs > Siemens Automation > Remote Manager > VNC Viewer Plus"</p> <p>Note For details on operation, please refer to Chapter Operation.</p>

4.4 Optional: Configuring the DSL modem

Connection via the Internet with standard router

These two steps are only necessary if you have selected the connection via the Internet with a standard router.

Port forwarding

If the remote SIMATIC IPC is connected to the Internet via a DSL modem, port forwarding must be set up for TCP ports 16992 to 16995 to the SIMATIC IPC in the router.

Dynamic DNS

DSL providers frequently assign dynamic IP addresses to their subscribers. Dynamic DNS (DDNS) can be used to obtain a static address for the SIMATIC IPC. This ensures that despite the dynamic IP address, the SIMATIC IPC is always accessible via a static name ("Fully qualified domain name" (FQDN)), for example, PC1.TESTDomain.test.

Details for setting up DDNS depend on the DDNS provider. Basically, two steps are necessary to obtain a static FQDN by means of DDNS.

1. Set up an account with a DDNS provider.
2. Enable DDNS in the DSL modem and enter the access and configuration data of the DDNS provider.

4.5 Transport Layer Security (TLS) configuration

Intel® AMT provides the option to encrypt connections (e.g., with SIMATIC IPC Remote Manager and the WEB interface) by means of the commonly used TLS method.

The SIMATIC IPC must be configured accordingly.

A certificate is created and stored in the remote SIMATIC IPC as well as in the management PC.

Manageability Director

The Manageability Director is a program from the Intel® Active Management Technology Developer Tool Kit (Intel® AMT DTK). DTK is available for download from the Internet at the following address: [\8\](#).

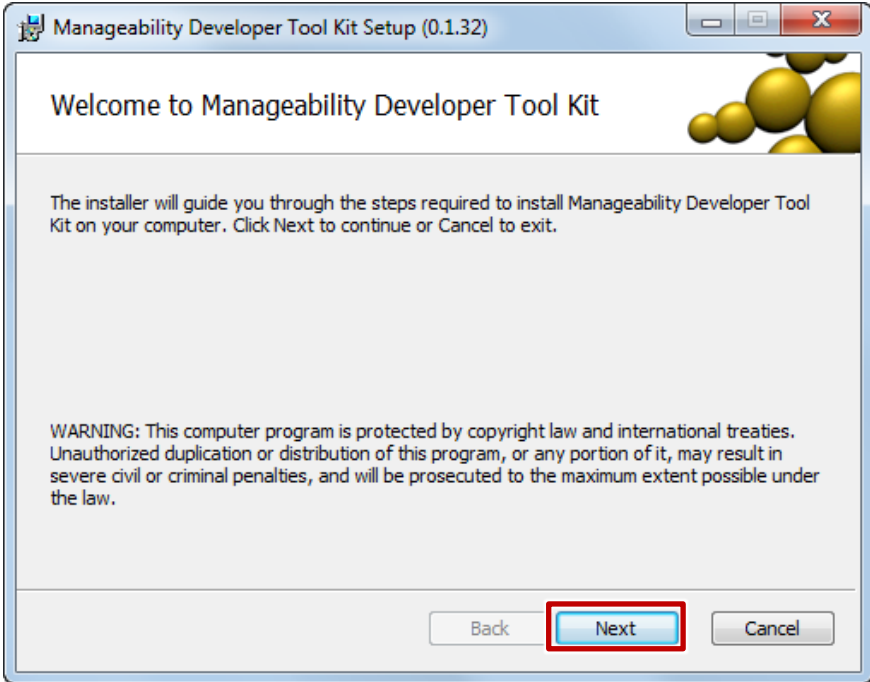
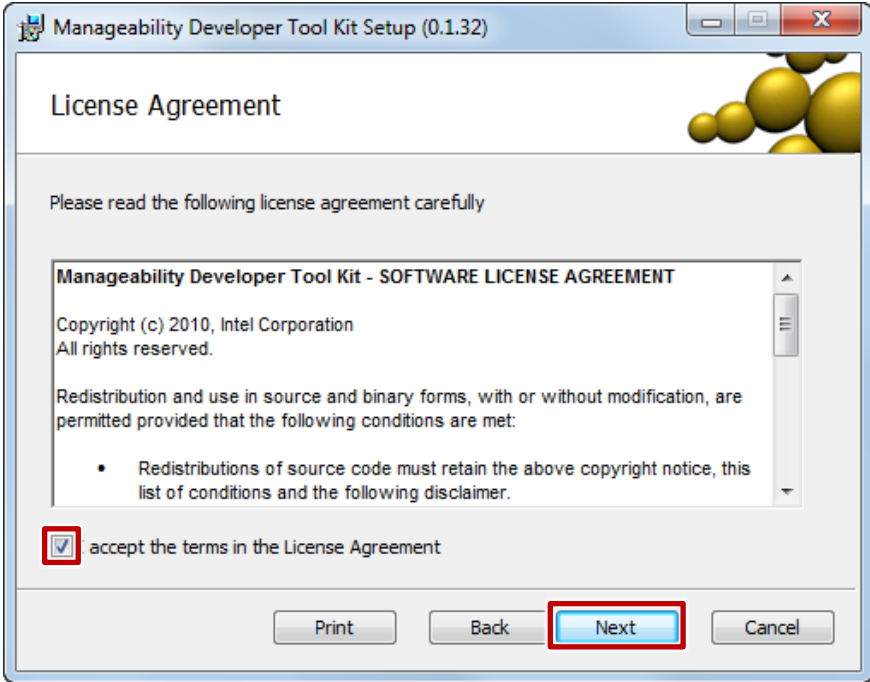
To create a certificate, load it to the Management Engine and configure the ME for TLS, follow the steps listed in the tables below:

4 Configuration

4.5 Transport Layer Security (TLS) configuration

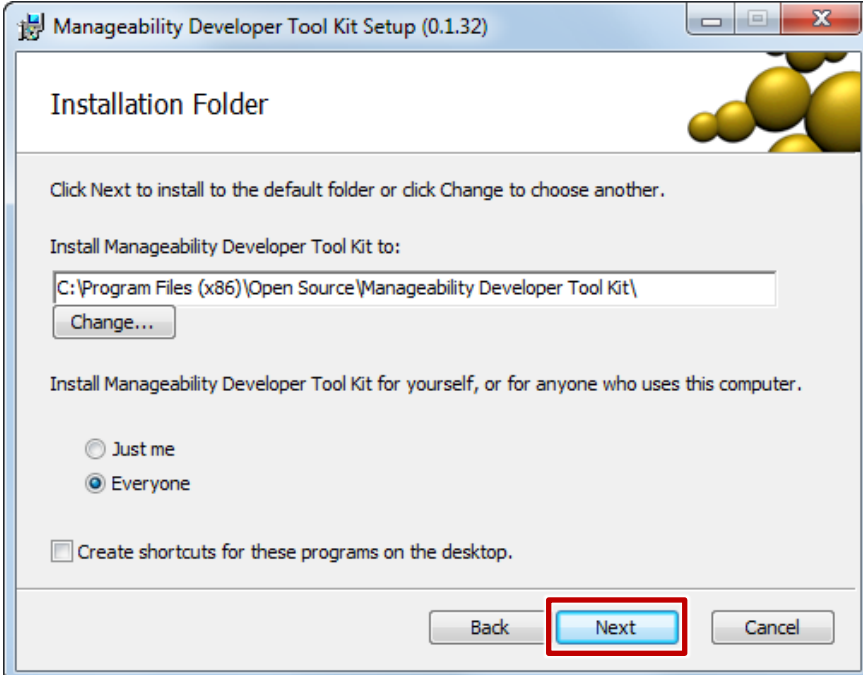
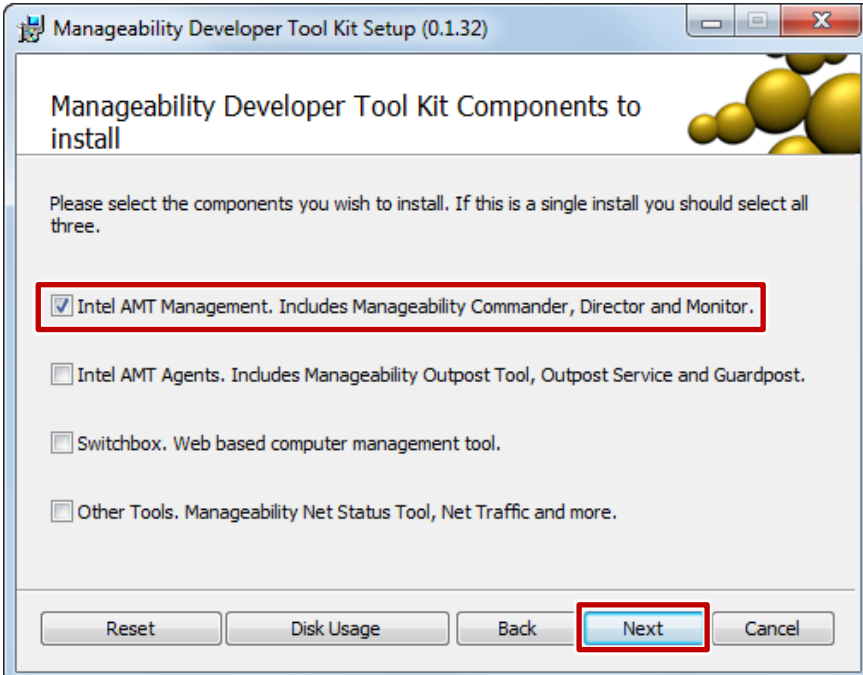
4.5.1 Configure remote SIMATIC IPC for TLS

Table 4-5

No.	Step
1.	Download the DTK that contains the Director.
2.	Install the DTK on the management PC.
3.	Click on "Next". 
4.	If you agree to the license agreement, select "I Agree". 

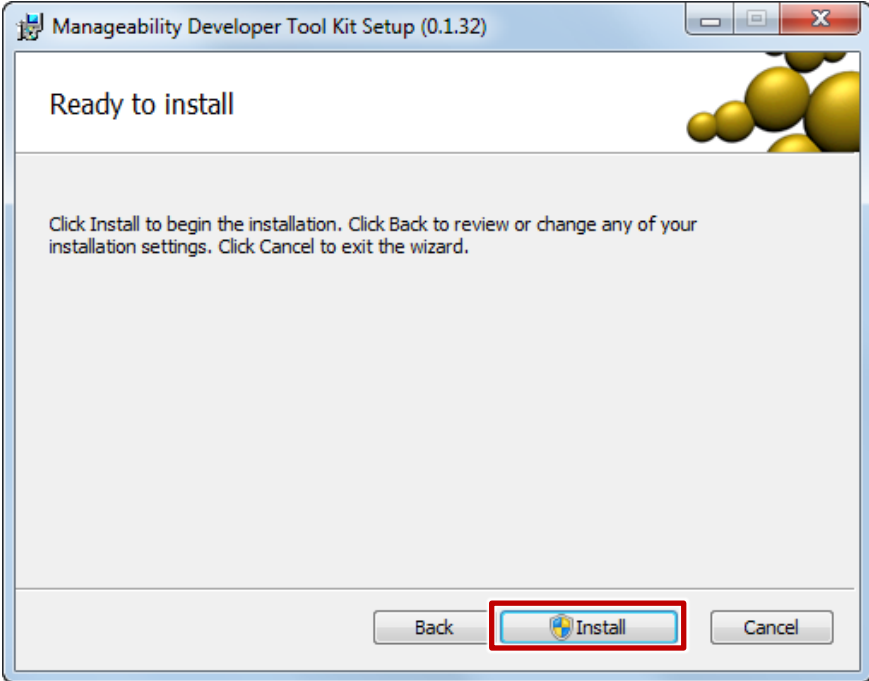
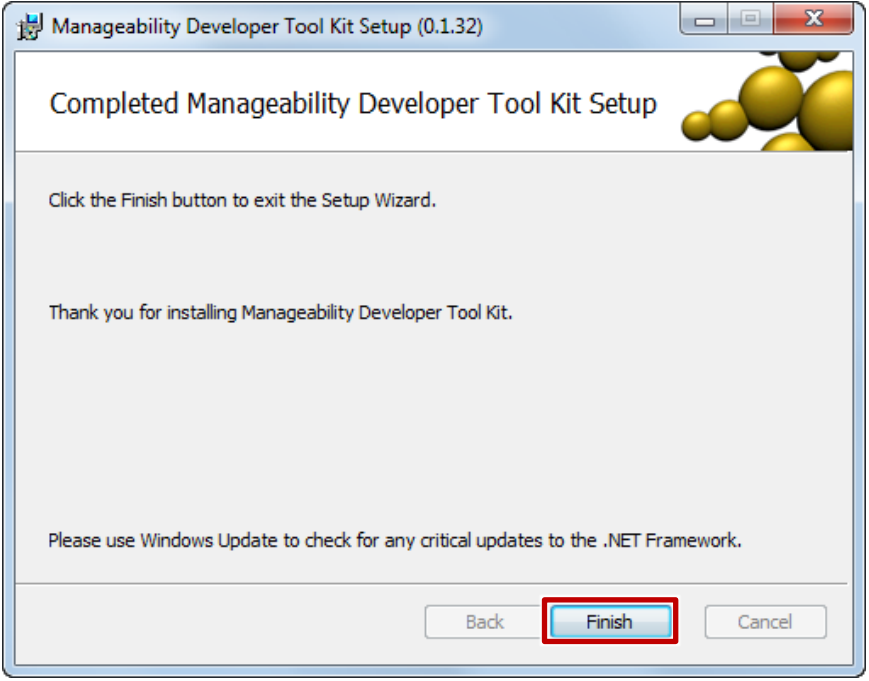
4 Configuration

4.5 Transport Layer Security (TLS) configuration

No.	Step
5.	<p>Select the installation folder and click on "Next" to confirm.</p> 
6.	<p>Select the choice as shown and click on "Next" to confirm.</p> 

4 Configuration

4.5 Transport Layer Security (TLS) configuration

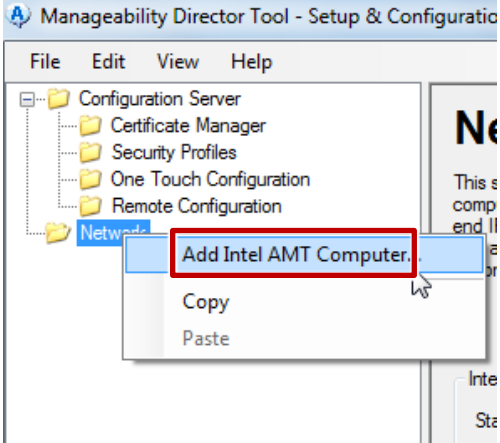
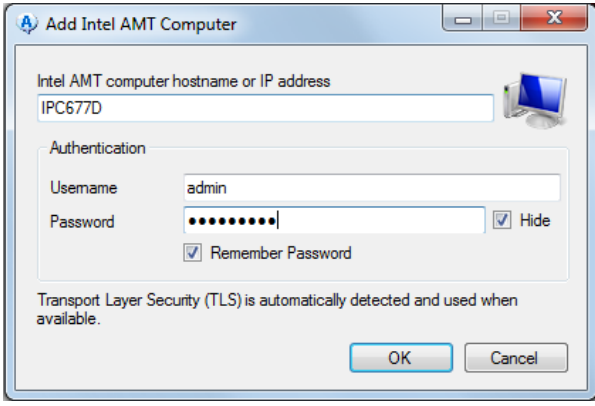
No.	Step
7.	<p>Select "Next" to confirm the installation.</p>  <p>An "Installation Complete" message is displayed. Click on "Finish" to exit the dialog box.</p> 
8.	Start "Start > All Programs > Manageability Developer Tool Kit > Manageability Director Tool".

4 Configuration

4.5 Transport Layer Security (TLS) configuration

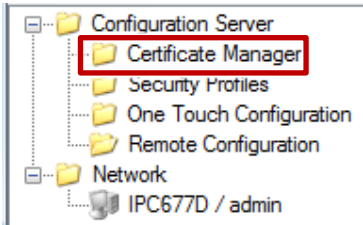
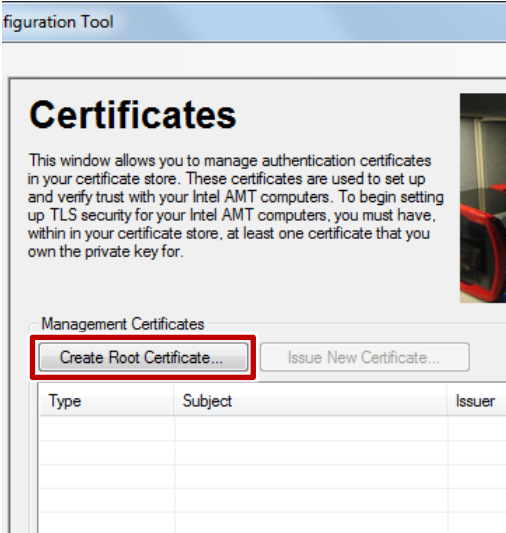
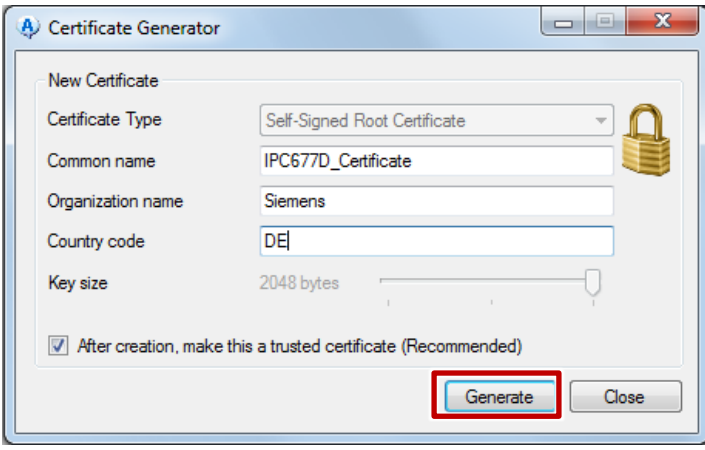
4.5.2 Adding the remote SIMATIC IPC

Table 4-6

No.	Step
1.	In the tree on the left side of the Director, select the "Network" node.
2.	In the context menu, select "Add Intel AMT Computer". 
3.	Enter the FQDN or the IP address as well as the authentication for the remote SIMATIC IPC.  The SIMATIC IPC is added to the tree.

4.5.3 Creating a certificate

Table 4-7

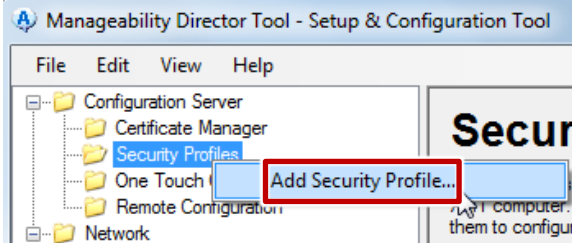
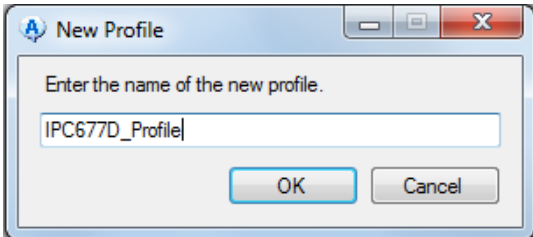
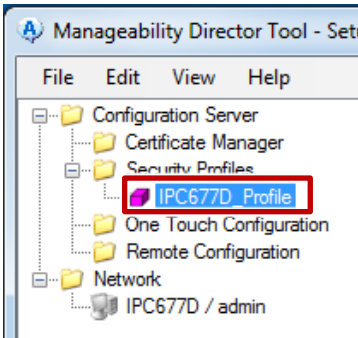

No.	Step
1.	<p>In the tree, select “Configuration Server > Certificate Manager”.</p> 
2.	<p>On the right side, press the “Create Root Certificate” button.</p> 
3.	<p>Fill in the fields in the “Certificate Generator” dialog. Press the “Generate” button.</p>  <p>Confirm the warning message with “Yes”.</p>

4 Configuration

4.5 Transport Layer Security (TLS) configuration

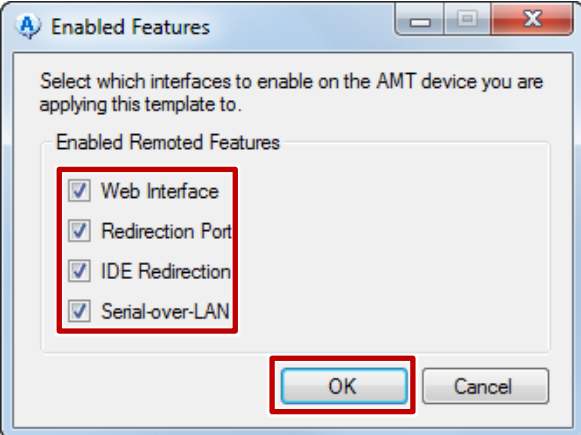
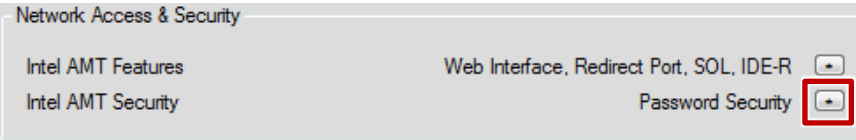
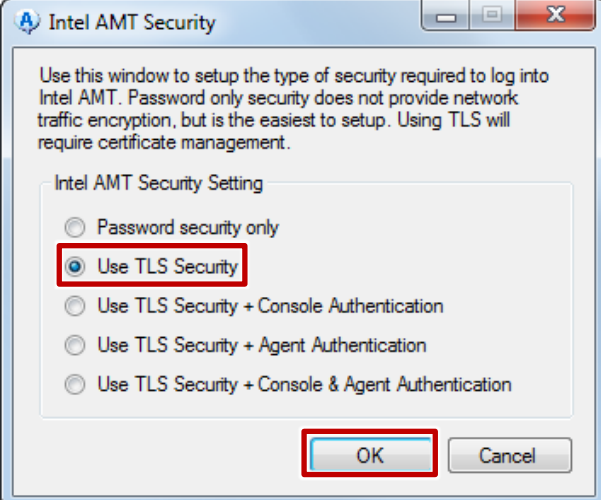
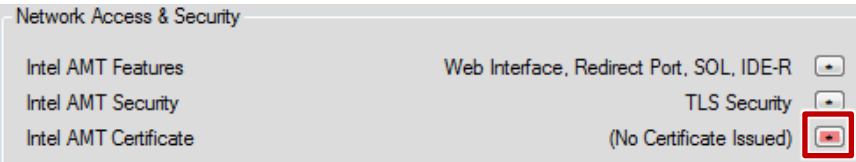
4.5.4 Create profile

Table 4-8

No.	Step
1.	In the tree, select "Configuration Server > Security Profiles".
2.	In the context menu, select "Add Security Profile...". 
3.	In the next dialog box, enter a name for the profile and select "OK". 
4.	In the tree, select the newly created profile. 
5.	On the right side, press the button next to the "Intel AMT Features" text. 

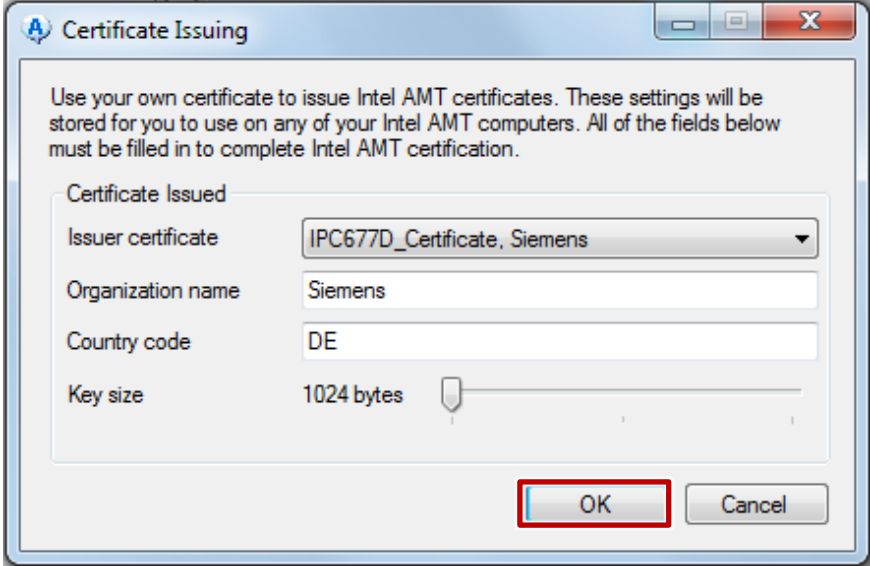
4 Configuration

4.5 Transport Layer Security (TLS) configuration

No.	Step
6.	<p>In the next dialog box, check all check boxes and select "OK".</p> 
7.	<p>On the right side, press the button next to the "Intel AMT Security" text.</p> 
8.	<p>In the next dialog box, select "Use TLS Security" and press "OK".</p> 
9.	<p>Press the button next to the "Intel AMT Certificate" text.</p> 

4 Configuration

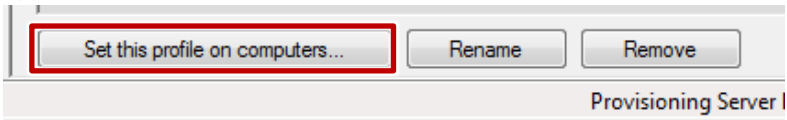
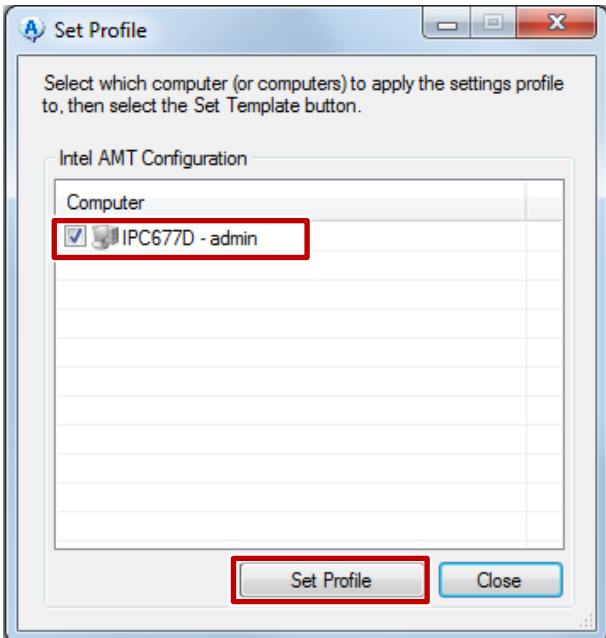
4.5 Transport Layer Security (TLS) configuration

No.	Step
10.	<p>In the next dialog box, select the previously created certificate in the “Issuer Certificate” drop-down list and press “OK”.</p> 

4.5.5 Loading a profile to the Management Engine

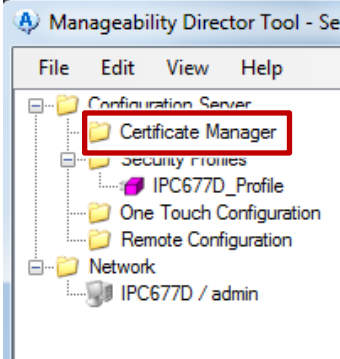

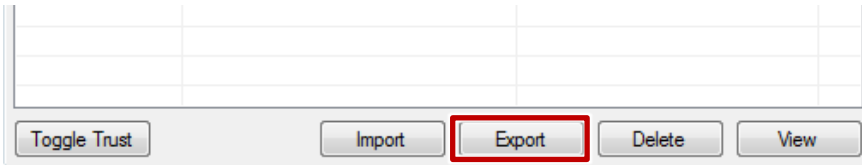
Note The following steps require a connection between management PC and remote SIMATIC IPC.

Table 4-9

No.	Step
1.	<p>Press the “Set this profile on computers...” button on the bottom edge of the application.</p> 
2.	<p>In the next dialog box, select the previously added SIMATIC IPC and press the “Set Profile” button.</p>  <p>The PC icon in “Network” takes on a blue color if the profile was set successfully.</p>

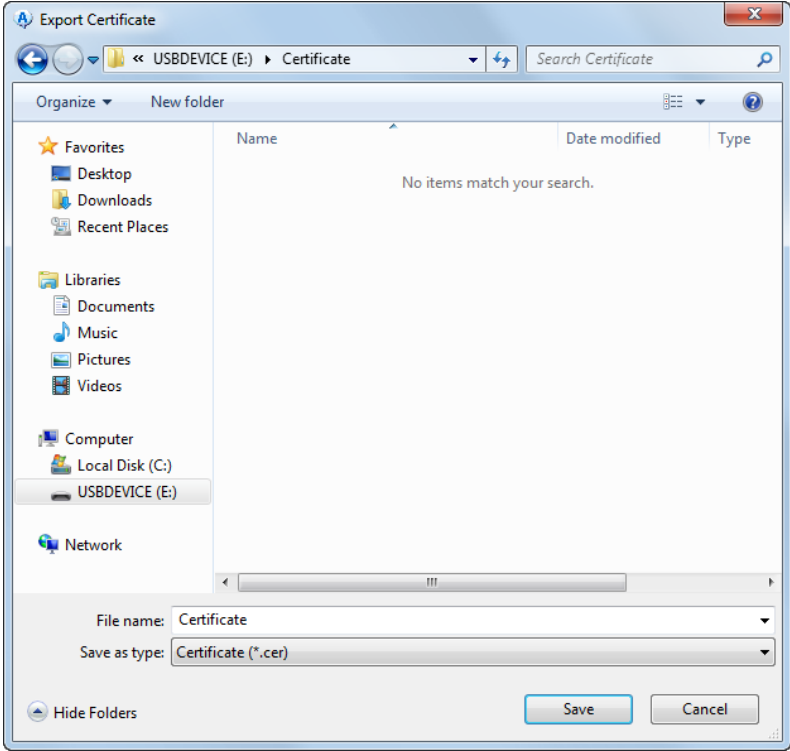
4.5.6 Installing certificates on further management PCs – Exporting certificates from the Director

Table 4-10

No.	Step
1.	<p>In the Director, select the “Configuration Server > Certificate Manager” node.</p> 
2.	<p>Select the certificate you created.</p> 
3.	<p>Press the “Export” button.</p> 

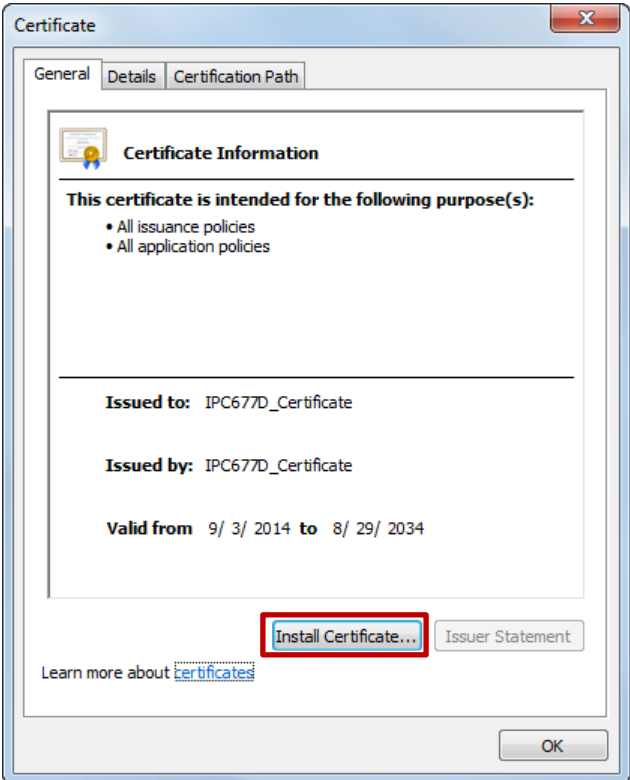
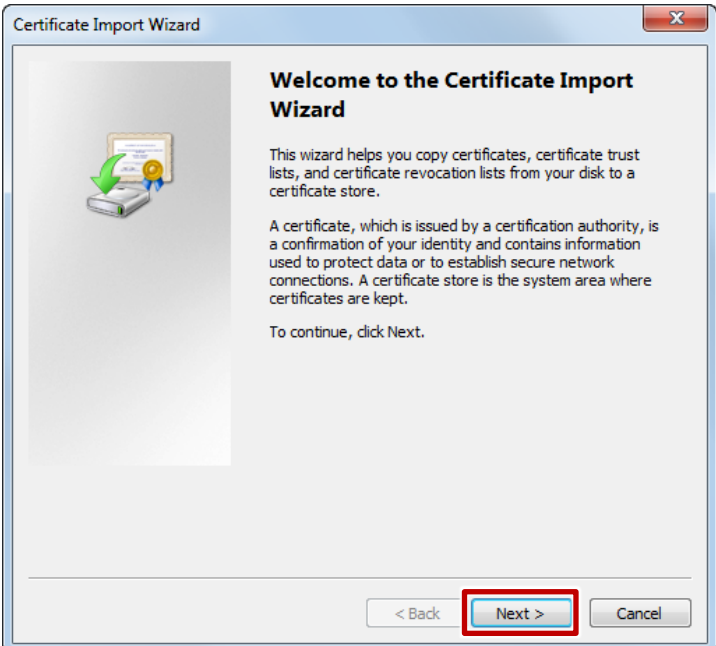
4 Configuration

4.5 Transport Layer Security (TLS) configuration

No.	Step
4.	<p>In the next dialog box, save the certificate to a USB flash drive (storage medium).</p>  <p>The screenshot shows a Windows Explorer window titled 'Export Certificate'. The address bar indicates the current location is 'USBDEVICE (E:) > Certificate'. The left sidebar shows the navigation pane with 'USBDEVICE (E:)' selected. The main pane is empty, displaying 'No items match your search.' The 'File name' field contains 'Certificate' and the 'Save as type' dropdown is set to 'Certificate (*.cer)'. The 'Save' button is highlighted in blue.</p>

4.5.7 Installing certificates on the management PC – Importing certificates

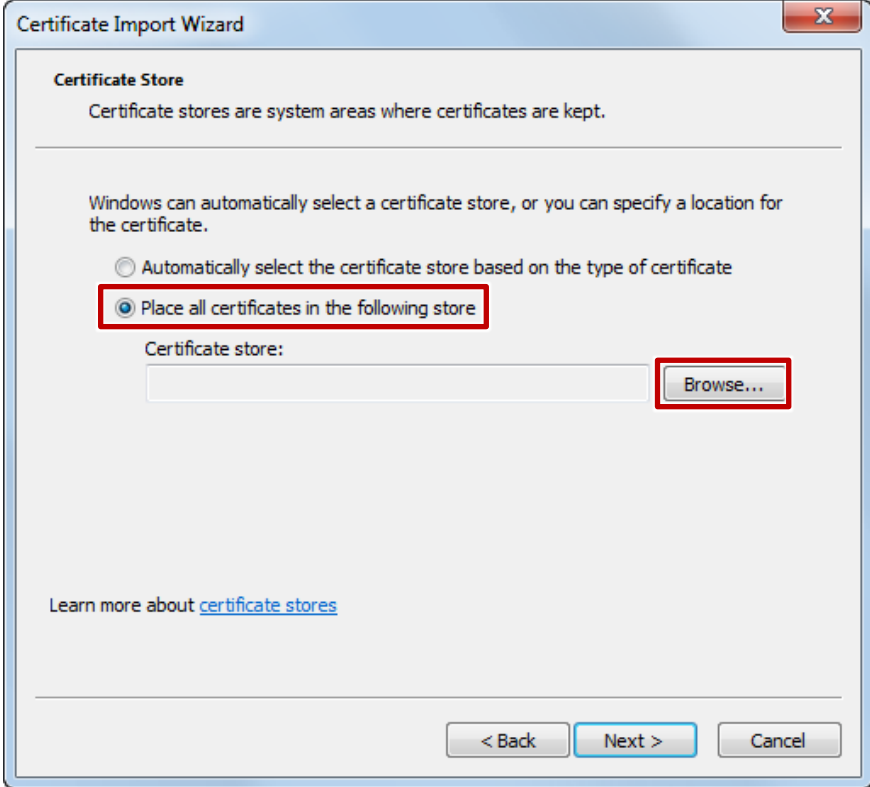
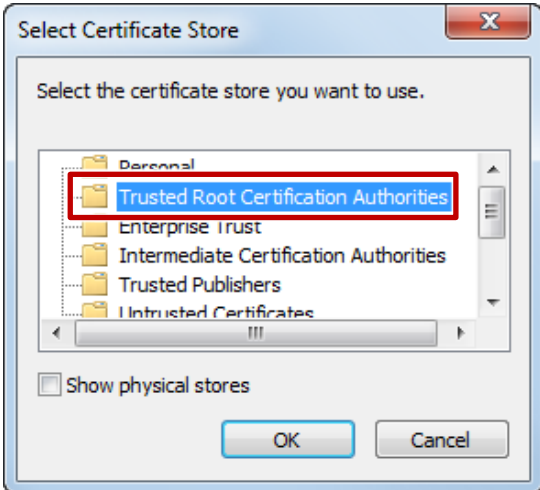
Table 4-11

No.	Step
1.	On the management PC, double-click on the certificate on the USB flash drive to open it.
2.	<p>In the next dialog box, press the “Install Certificate...” button.</p> 
3.	<p>In the next dialog box, select the “Next” button.</p> 

© Siemens AG 2016 All rights reserved

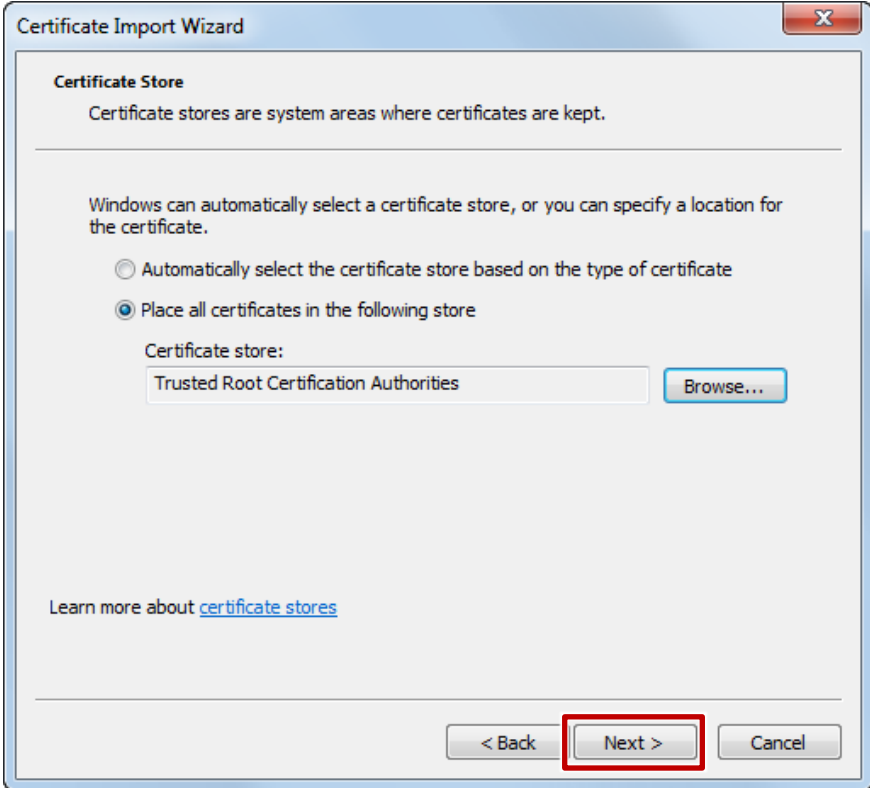
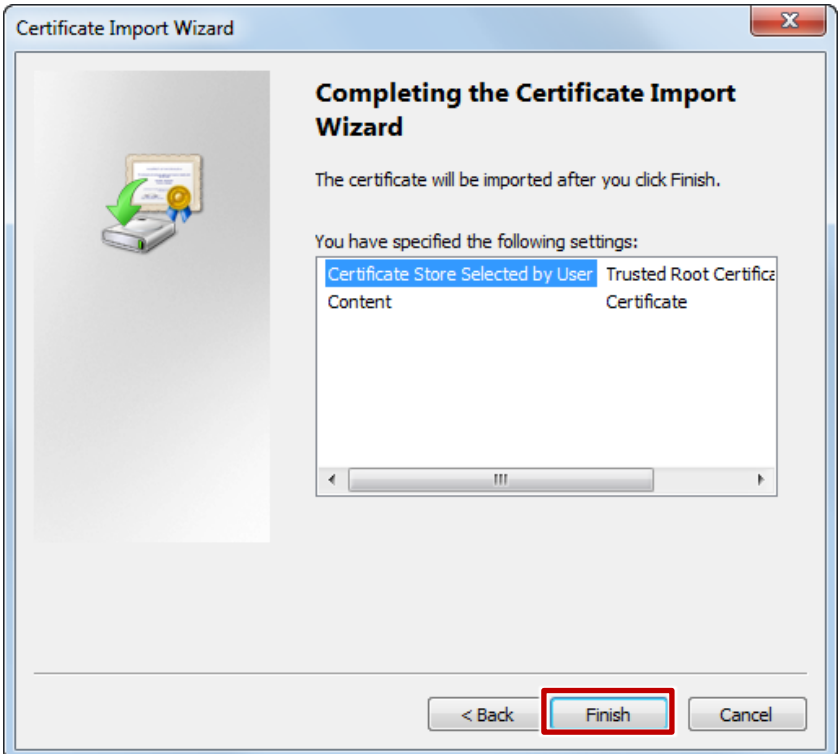
4 Configuration

4.5 Transport Layer Security (TLS) configuration

No.	Step
4.	<p>In the next dialog box, select "Place all certificates, in the following store". Press the "Search" button.</p>  <p>Certificate Import Wizard</p> <p>Certificate Store Certificate stores are system areas where certificates are kept.</p> <p>Windows can automatically select a certificate store, or you can specify a location for the certificate.</p> <p><input type="radio"/> Automatically select the certificate store based on the type of certificate</p> <p><input checked="" type="radio"/> Place all certificates in the following store</p> <p>Certificate store: <input type="text"/> Browse...</p> <p>Learn more about certificate stores</p> <p>< Back Next > Cancel</p>
5.	<p>Select "Trusted Root Certification Authorities".</p>  <p>Select Certificate Store</p> <p>Select the certificate store you want to use.</p> <ul style="list-style-type: none">PersonalTrusted Root Certification AuthoritiesEnterprise TrustIntermediate Certification AuthoritiesTrusted PublishersUntrusted Certificates <p><input type="checkbox"/> Show physical stores</p> <p>OK Cancel</p>

4 Configuration

4.5 Transport Layer Security (TLS) configuration

No.	Step
6.	<p>Press the "Next >" button.</p> 
7.	<p>Press the "Finish" button.</p> 

5 Operation

General

This chapter describes the basic handling of Intel® AMT Technology.

It starts with the general operation and continues with different scenarios to illustrate the operation for special use cases.

First, connect the SIMATIC IPC to the LAN.

5.1 Non-encrypted connections

5.1.1 Operation with the SIMATIC IPC Remote Manager viewer

Table 5-1

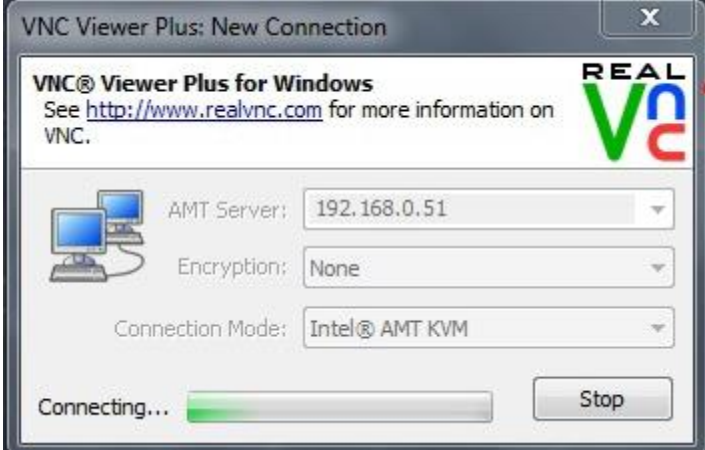

1.	Start the KVM viewer of the SIMATIC IPC Remote Manager via “Start > All Programs > Siemens Automation > Remote Manager > VNC Viewer Plus”. The “New Connection” dialog box is displayed.
2.	Click on the “Options” button. In the open dialog you click on the “Advanced” button and go to the “AMT Server” tab. Deactivate “Always connect using FQDN”, if you do not wish to create the connection with the remote SIMATIC IPC via FQDN.

The screenshot shows the 'Options' dialog box with the following details:

- Title bar: Options
- Section: AMT Options (Control various Intel® AMT settings)
- Logo: REAL VNC
- Tabs: Display, Inputs, Connection, Printing, **AMT Server** (highlighted), Expert
- Wi-Fi section:
 - When connecting to Wi-Fi-enabled AMT Server:
 - The host computer can use its Wi-Fi network
 - The host computer can be controlled during a restart
- Host computer user consent:
 - Contact host computer user for consent code
 - Connect without requiring consent
- Fully-qualified domain name (FQDN):
 - Turn on to look up a FQDN for an IP address or host name. This may be required for an encrypted connection or in a Kerberos network.
 - Always connect using FQDN (highlighted with a red box)
- Use these settings for all new connections:
- Buttons: Basic..., OK, Cancel

5 Operation

5.1 Non-encrypted connections

3.	<p>In the “New Connection” dialog box, enter the following data.</p> <ul style="list-style-type: none">• Address (FQDN or IP address) of the remote SIMATIC IPC• Encryption = None• Connection Mode = Intel® AMT KVM 
4.	<p>Press the “Connect” button.</p>
5.	<p>In the next dialog box, log on with the user account that is stored in the Management Engine (see: Chapter 4.2.2 “Enabling Intel® AMT (basic configuration)”, step 8). The desired KVM connection to the remote SIMATIC IPC is established.</p> 

© Siemens AG 2016 All rights reserved

Toolbar

The KVM Viewer has a toolbar on its top edge that enables you to operate the KVM Viewer. Using the toolbar, you can also execute various Intel® AMT commands such as Remote Power Management and IDE Redirection.

Once opened, the non-encrypted connection is identified in the Viewer toolbar by a “crossed out lock” icon.

Figure 5-1



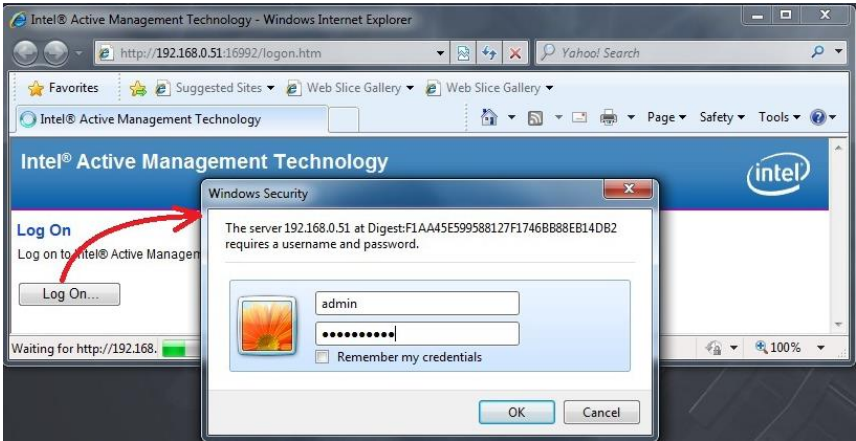
5 Operation

5.1 Non-encrypted connections

5.1.2 Operation with the WEB GUI

Aside from a KVM connection, Intel® AMT can also be operated using a WEB GUI (Graphical User Interface). Proceed as follows:

Table 5-2

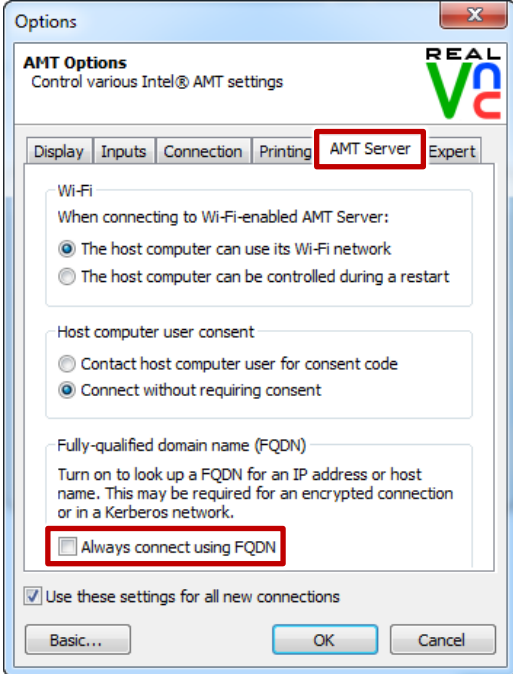
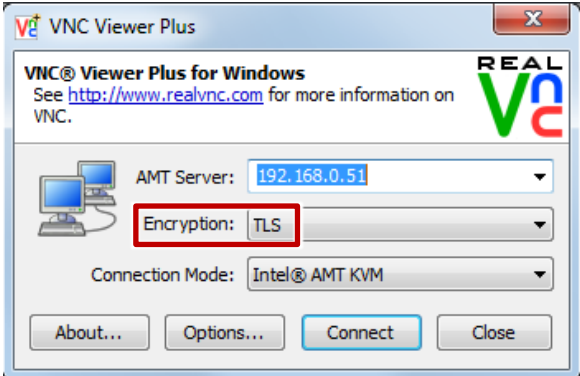
No.	Step
1.	Enter the IP address of the SIMATIC IPC in the WEB browser. [http://IP address:16992] A page with the login option is displayed.
2.	Click on the “Log On ...” button:
3.	In the next dialog box, log on with the user account that is stored in the Management Engine.  Once you have logged on, the WEB GUI provides detailed system information on the remote SIMATIC IPC, access to the Intel® AMT event Log and the option to turn the SIMATIC IPC on and off.

5.2 Encrypted connections

5.2.1 Operation with the SIMATIC IPC Remote Manager viewer

Proceed as follows:

Table 5-3

No.	Step
1.	Start the KVM viewer of the SIMATIC IPC Remote Manager via “Start > All Programs > Siemens Automation > Remote Manager > VNC Viewer Plus”. The “New Connection” dialog box is displayed.
2.	<p>Click on the “Options” button. In the open dialog you click on the “Advanced” button and go to the “AMT Server” tab.</p> <p>Deactivate “Always connect using FQDN”, if you do not wish to create the connection with the remote SIMATIC IPC via the FQDN.</p> 
3.	<p>In the “New Connection” dialog box, enter the following data:</p> <ul style="list-style-type: none"> • Address of the remote SIMATIC IPC • Encryption = "TLS" • Connection Mode = Intel® AMT KVM 

5 Operation

5.2 Encrypted connections


Once opened, the encrypted TLS connection is identified in the Viewer toolbar by a lock icon.

Figure 5-2



5.2.2 Operation with the WEB GUI

Table 5-4

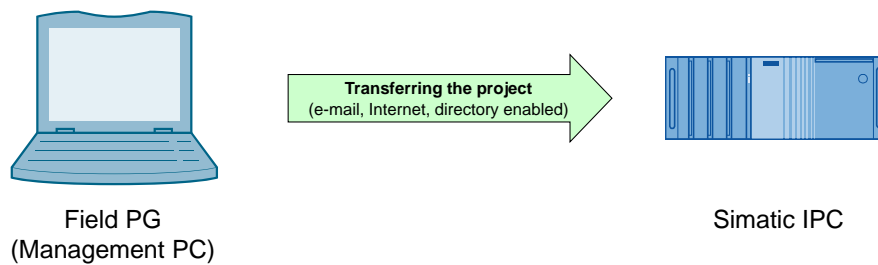
No.	Step
1.	<p>To open the WEB GUI with an encrypted connection to the remote SIMATIC IPC, enter the following URL in the WEB browser: [https:// Fully qualified domain name:16993].</p>  <p>Note</p> <p>Once opened, the encrypted connection is identified in the WEB browser by a lock icon next to the URL. In the context menu of the lock icon, you can display and analyze the certificate that is used for TLS encryption.</p>
2.	<p>Click on the “Log On ...” button and log on with the user account that is stored in the Management Engine.</p> <p>Once you have logged on, the WEB GUI provides detailed system information on the remote SIMATIC IPC, access to the Intel® AMT event Log and the option to turn the SIMATIC IPC on and off.</p>

5.3 Scenario 1 – SIMATIC WinAC

This scenario describes how to load a program to SIMATIC WinAC on a remote SIMATIC IPC.

First the program must be transferred to the SIMATIC IPC. This is done, as usual, via the Internet, e-mail or storage media.

Figure 5-3



Once you have transferred the project to the remote SIMATIC IPC and connected to the remote SIMATIC IPC using Remote Manager, you can download the WinAC by means of Step 7, as you have in the past.

Note

To load the program to SIMATIC WinAC, this SIMATIC IPC must have an engineering station (STEP 7).

5 Operation

5.3 Scenario 1 – SIMATIC WinAC

Table 5-5

Configuration		Monitoring	Operation	Load
A		X	X	X
B		X	X	X
C		X	X	--


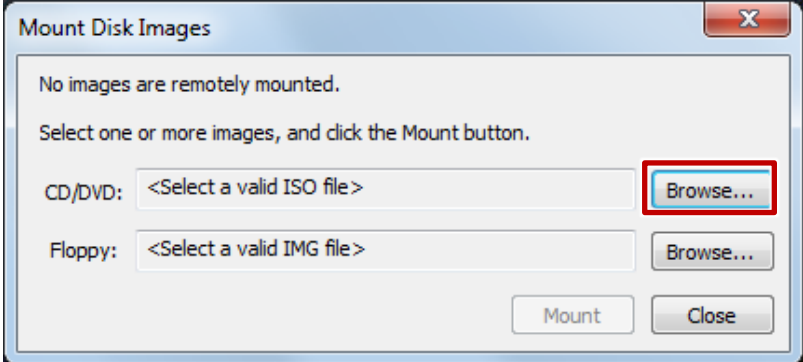
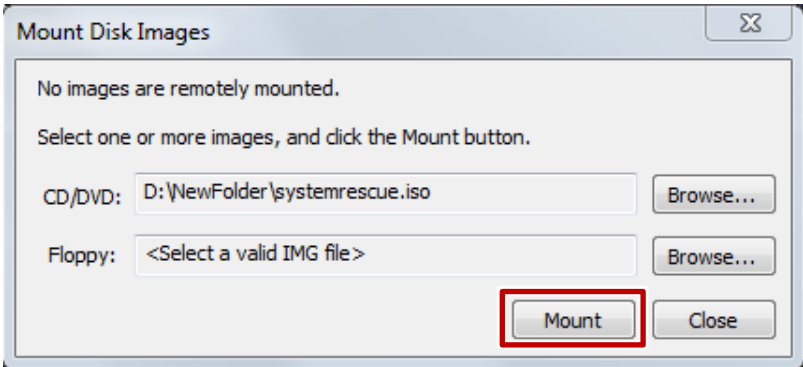

5.4 Scenario 2 – Restoring a SIMATIC IPC with an ISO image

Initial situation

You are in front of the management PC; an ISO image of the installation DVD is stored for the SIMATIC IPC. You have established a remote connection to the remote SIMATIC IPC. The remote SIMATIC IPC is turned off.

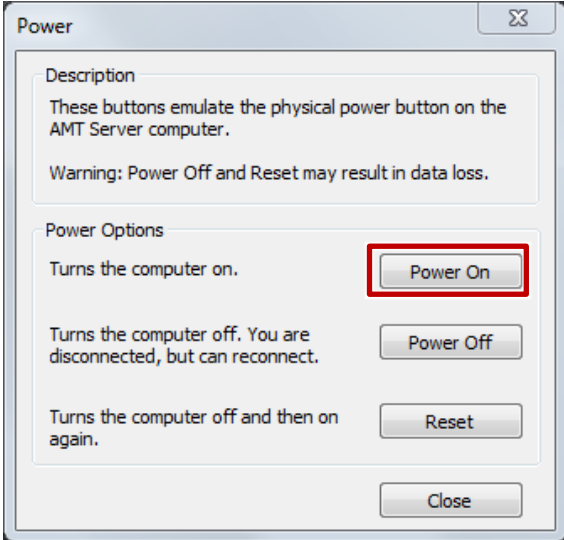
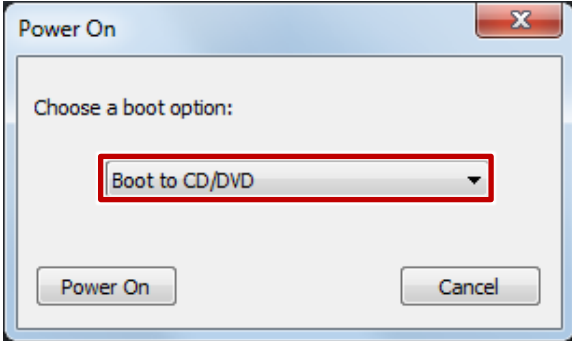
Procedure

Table 5-6

No.	Step
1.	<p>Click on the “Mount Disk Images” button.</p>  <p>The “Mount Disk Images” dialog box opens.</p>
2.	<p>In the open dialog box, click on the “Browse” button to select the relevant ISO image.</p> 
3.	<p>Click on “Mount” to confirm the selected image.</p> 
4.	<p>Turn on the remote SIMATIC IPC.</p> 

5 Operation

5.4 Scenario 2 – Restoring a SIMATIC IPC with an ISO image

No.	Step
5.	<p>In the next dialog box, select "Power On".</p>  <p>The screenshot shows a dialog box titled "Power" with a close button in the top right. It contains a "Description" section with text: "These buttons emulate the physical power button on the AMT Server computer." and a warning: "Warning: Power Off and Reset may result in data loss." Below this is a "Power Options" section with three rows of text and buttons: "Turns the computer on." with a "Power On" button (highlighted with a red rectangle), "Turns the computer off. You are disconnected, but can reconnect." with a "Power Off" button, and "Turns the computer off and then on again." with a "Reset" button. A "Close" button is at the bottom.</p>
6.	<p>Select the "Boot to CD/DVD" boot option.</p>  <p>The screenshot shows a dialog box titled "Power On" with a close button in the top right. It contains a "Choose a boot option:" label and a dropdown menu with "Boot to CD/DVD" selected (highlighted with a red rectangle). Below the dropdown are "Power On" and "Cancel" buttons.</p> <p>The system boots from the ISO image. You can now remotely reinstall the SIMATIC IPC.</p>

6 Further Notes, Tips & Tricks, etc.

DiagMonitor integration

If DiagMonitor version 4.3 or higher is installed on a PC with SIMATIC IPC Remote Manager, the SIMATIC IPC Remote Manager Viewer will be integrated into the DiagMonitor software. In the DiagMonitor, you can open the Viewer from the “Tools” menu and the context menu.

Teaming

Concurrent operation of Intel® AMT and Teaming (teaming multiple physical network cards to a single logical network card (NIC) to provide redundancy) is **not** possible with the 82577LM on-board Ethernet controller.

However, you can nonetheless use Intel® AMT and Teaming concurrently by inserting an additional Ethernet module with an Intel® controller (e.g., 82574L or another Intel® GbE controller). This additional Ethernet card and the 82574L on-board Ethernet controller allow concurrent operation of Teaming and Intel® AMT.

Maximum resolution

The used MEBx version 6.1.1.1045 supports a maximum resolution of 1920x1080. From version 7.0 on, a maximum resolution of 1920x1200 is supported.

Passwords

In the basic setting (see Enabling Intel® AMT (basic configuration)) a password must be assigned for the user “admin”. You can then use the admin user and the password to log to the MEBx, WEB interface and RealVNC Viewer.

The MEBx and the WEB interface provide the option to assign two different passwords for the admin user: one password for logon to the MEBx and another password for the WEB interface and RealVNC Viewer.

The MEBx password can be changed at “MEBx > Intel® ME General Settings > Change Intel® ME Password”. The WEB interface password can be changed in “WEB-Interface > User Accounts > Change Administrator Account”.

If you have set different passwords, make sure to use the correct password when logging on to the MEBx, WEB interface or RealVNC Viewer.

Troubleshooting connection problems

If a KVM connection cannot be established, please refer to the troubleshooting checklist in the “Getting connected > Troubleshooting connection” chapter of the VNC® Viewer Plus User Guide ([6](#)).

7 Glossary

Table 7-1

Abbreviation	Term	Meaning
AMT	Active Management Technology	Remote maintenance technology
DDNS	Dynamic DNS	Mechanism for assigning a static FQDN to an Internet connection with dynamic IP address
DHCP	Dynamic Host Configuration Protocol	Protocol for the configuration of IP networks
DNS	Domain Name System	Service for determining the IP address of an FQDN
DTK	Developer Tool Kit	Developer tools used for testing and configuring Intel® AMT, etc.
GUI	Graphical user interface	Graphical user interface
FQDN	Fully qualified domain name	Fully qualified domain name
IDER	IDE redirection	Remote integration of an ISO file as a drive
IE	Internet Explorer	
IPC	Industrial PC	Particularly rugged computer for use in the industrial environment
KVM	Keyboard Video Mouse	
KVM viewer	Keyboard Video Mouse viewer	In SIMATIC IPC Remote Manager, the RealVNC Viewer is used for this purpose.
ME	Management Engine	Firmware & hardware which implement Intel® AMT
MEBx	Management Engine BIOS Extension	User interface for the basic configuration of Intel® AMT
SCS	Setup and Configuration Service	Intel® application on the Intel® AMT configuration
SOL	Serial over LAN	Text-based remote operation
TLS	Transport Layer Security	Network protocol for encrypted transmission. Successor to SSL.

8 Related literature

Table 8-1

	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Download page of this entry https://support.industry.siemens.com/cs/ww/en/view/52310936
\3\	AMT web page of Intel® https://software.intel.com/en-us/business-client/manageability
\4\	IP based remote networks https://support.industry.siemens.com/cs/ww/en/view/26662448
\5\	Operating instructions of the SIMATIC IPCs https://support.industry.siemens.com/cs/ww/en/ps/16740/man
\6\	VNC® Viewer Plus User Guide http://www.realvnc.com/products/viewerplus/1.2/docs/VNC_Viewer_Plus_User_Guide.pdf
\7\	SIMATIC IPC Remote Manager Manual https://support.industry.siemens.com/cs/ww/en/view/48707158
\8\	Manageability Director http://www.meshcommander.com/open-manageability

9 History

Table 9-1

Version	Date	Modifications
V1.0	06/2011	First version
V1.1	11/2014	Update (new software/hardware)
V1.1	06/2016	Update (new hardware)