

**SIEMENS**



Configuration Example • 09/2015

# Recommended Security Settings for IPCs in the Industrial Environment

SIMATIC IPCs

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

## Warranty and Liability

### Note

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

We do not accept any liability for the information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this application example will be excluded. Such an exclusion will 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 compensation for damages due to a breach of a fundamental contractual obligation is, 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 Siemens Industry Sector.

### Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens’ products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit <http://www.siemens.com/industrialsecurity>.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit <https://support.industry.siemens.com>.

# Table of Contents

<b>Warranty and Liability</b> .....	<b>2</b>
<b>1 Task</b> .....	<b>4</b>
<b>2 Solution</b> .....	<b>5</b>
2.1 Security check list.....	5
2.2 Hardware and software components .....	7
<b>3 Basics</b> .....	<b>8</b>
3.1 Basics on the editors .....	8
3.1.1 Local Group Policy Editor.....	8
3.1.2 Microsoft Management Console .....	9
<b>4 Security Settings for IPCs without Network Access</b> .....	<b>11</b>
4.1 User accounts and respective rights .....	11
4.1.1 Differentiation between administrator and user account.....	11
4.1.2 SIMATIC software by the user with restricted rights .....	12
WinAC RTX .....	12
Station Configuration Editor .....	12
4.1.3 Creating a user account .....	13
4.2 Detecting user installation and elevation request with User Account Control (UAC).....	15
4.3 Enhanced Write Filter.....	17
4.4 Do not shut down the system without login.....	19
4.5 Software restriction policies – AppLocker .....	21
4.6 Configuring Desktop policies and restrictions .....	23
4.7 Start menu and taskbar – Configuring policies .....	27
4.8 Configure Ctrl+Alt+Del .....	31
4.9 Preventing access to Control Panel .....	33
4.10 Configuring access to removable storage medium .....	33
4.11 Deactivate Autoplay function.....	35
4.12 Prevent removable disk access for all installations.....	36
4.13 Refusing access to Microsoft Management Console .....	39
4.14 Refuse access to restore option.....	41
4.15 Refusing access to paths when searching.....	44
4.16 Prevent access to certain or all drives .....	46
<b>5 Security Settings for IPCs with Network Access</b> .....	<b>50</b>
5.1 Activating and configuring Windows firewall .....	50
5.2 Configuring password guidelines correctly.....	53
5.3 Refusing access to network connections .....	55
5.4 Restricting internet access .....	57
5.5 Refusing access to Anytime upgrade and Windows update.....	62
5.6 Tunnel connection with IPSec (VPN IPsec).....	66
5.7 Appropriate configuration for Remote Desktop.....	74
<b>6 Links &amp; Literature</b> .....	<b>82</b>
<b>7 History</b> .....	<b>82</b>

# 1 Task

## Introduction

IPCs for controlling machines and systems in industry need to meet the highest requirements regarding security and reliability.

The Windows operating system provides extensive options of configuring an IPC. The measures suggested in this entry increase the IT security of the operating system as well as availability. Important tools are the group policies where various settings can be made. There are two possible ways of changing the group policies:

- Local Group Policy Editor
- Microsoft Management Console

## Description of the automation task

In this configuration example, recommendations on the required settings are given in order to minimize risks for IPCs in the industrial environment. It is differentiated here between IPCs without network connection (“stand-alone mode”) or the additional settings necessary for IPCs with network access.

### Note

Regarding the topic of security for IPCs please also consider the security guideline [55390879](#).

## 2 Solution

### 2.1 Security check list

The following check list mentions a number of risks and the respective solution.

These notes are divided into recommendations for IPCs without network connection ("stand-alone mode") as well as additionally recommended settings for IPCs with network access.

#### Settings for IPCs without network connection

Table 2-1

Risk	Weak points	Solution
Unauthorized modification of system parameters	Only one administrator account exists	<a href="#">Chapter 4.1</a> : Operating the SIMATIC software as user with restricted user rights
Staff with user rights can install any program	Installing applications also possible by the user	<a href="#">Chapter 4.2</a> : Automatic rejection of password query for administrator rights
Changes at the system	System files can be manipulated	<a href="#">Chapter 4.3</a> : Due to the EWF, modifications at system files can only be performed in the RAM
Possible process stop	Shut-down option freely accessible	<a href="#">Chapter 4.4</a> : Enable shut-down only after user login
Unauthorized execution of software	Executing possible malware	<a href="#">Chapter 4.5</a> : Access control to software by means of AppLocker
Changing system data, access to Internet Explorer, workspace, network environment	Desktop - access to applications	<a href="#">Chapter 4.6</a> : Preventing access to Windows applications and their properties via the Desktop
Changing system data/network environment, blocking/shutting down IPC	Start menu and task bar - Access to applications	<a href="#">Chapter 4.7</a> : Preventing access to Windows applications via the Start menu
Processes and services can be stopped, faulty IPC configuration	Changing the password, blocking the IPCs, access to Task Manager	<a href="#">Chapter 4.8</a> : Restriction of functions after "Ctrl+Alt+Del"
Processes and services can be stopped, faulty IPC configuration	Changing the system parameters in Control Panel	<a href="#">Chapter 4.9</a> : Preventing access to Control Panel
Infecting IPC with malware, undesired installation of programs	Access to removable storage medium (e.g. USB sticks)	<a href="#">Chapter 4.10</a> : Preventing access to removable storage medium
Infecting IPC with malware, undesired installation of programs	Automatic execution of software (Autoplay function)	<a href="#">Chapter 4.11</a> : Deactivating Autoplay or Autorun
Infecting IPC with malware, undesired installation of programs	Installations from removable storage medium	<a href="#">Chapter 4.12</a> : Deactivating the installation of removable storage medium
Changing the system configuration (group policies, firewall settings, etc.)	Access to MMC (Microsoft Management Console)	<a href="#">Chapter 4.13</a> : Refusing access to MMC (Microsoft Management Console)
Undesired system changes	Access to restore options	<a href="#">Chapter 4.14</a> : Restricting the restore options
Undesired access to applications	Access paths when searching	<a href="#">Chapter 4.15</a> : Refusing access

## 2 Solution

### 2.1 Security check list

Risk	Weak points	Solution
		to paths when searching
Unauthorized access to system-relevant information, manipulation option	Accessing drives from the workspace	<a href="#">Chapter 4.16</a> : Restricting access to network and certain drives

### Additional settings for IPCs with network connection

Table 2-2

Risk	Weak points	Solution
Sensitive process data can be viewed	Windows firewall switched off / not configured	<a href="#">Chapter 5.1</a> : Activating and configuring Windows firewall
Attacks by hackers through online scanner, unauthorized access	Using standard passwords	<a href="#">Chapter 5.2</a> : Configuring password guidelines correctly
Unauthorized changes of LAN connections, unauthorized removing/adding of components	Free access to network connections	<a href="#">Chapter 5.3</a> : Refusing access to network connections
Free access to the internet	Free on access to internet communication management	<a href="#">Chapter 5.4</a> : Restricting internet access
Possible process stop	Access to Anytime Upgrade and Update	<a href="#">Chapter 5.5</a> : Refusing access to Anytime upgrade and Windows update
Unsecured connection - sensitive process data can be viewed	Unsecured connection of remote maintenance via VPN	<a href="#">Chapter 5.6</a> : Using a virtual private network (VPN) that has been configured correctly
Unauthorized access rights	Unsecured remote - Desktop connection	<a href="#">Chapter 5.7</a> : Secure configuration of the remote Desktop

#### Note

The security check list only shows the recommended settings, however, without guarantee of completeness. For the final configuration, please consult your security expert.

### Assumed knowledge

Basic knowledge about installation, configuration, networking and operation of IPCs in the industrial environment is assumed.

## 2.2 Hardware and software components

### Validity

This application is valid for

- all current SIMATIC IPCs
- Windows 7 operating systems (for other operating systems, the described menus may deviate)

### Example files and projects

The following list includes all files and projects that are used in this example.

Table 2-3

Component	Note
109475014_Securityeinstellungen_IPCs_en.pdf	This document.

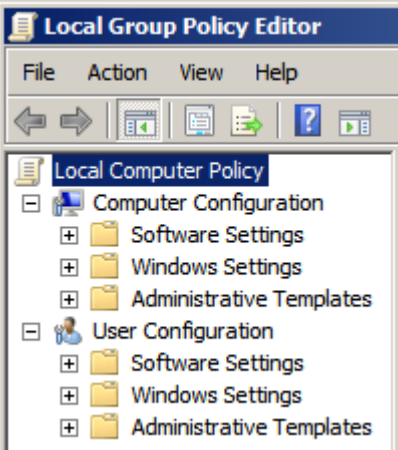
# 3 Basics

## 3.1 Basics on the editors

### 3.1.1 Local Group Policy Editor

**Call**

Table 3-1

Process	Action
1.	Open the “Local Group Policy Editor” via Start >Execute> “gpedit.msc”
2.	The “Local Group Policy Editor” opens 

**Properties**

- Changing the Computer Configuration
- Changing the user configuration for all users



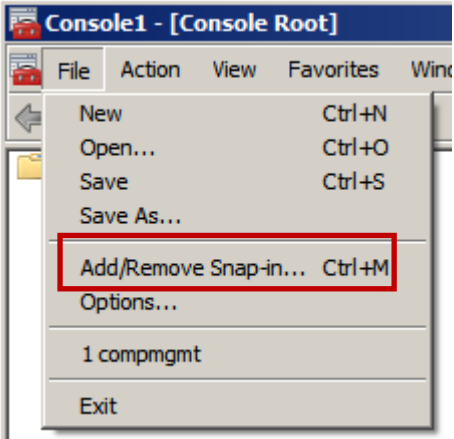
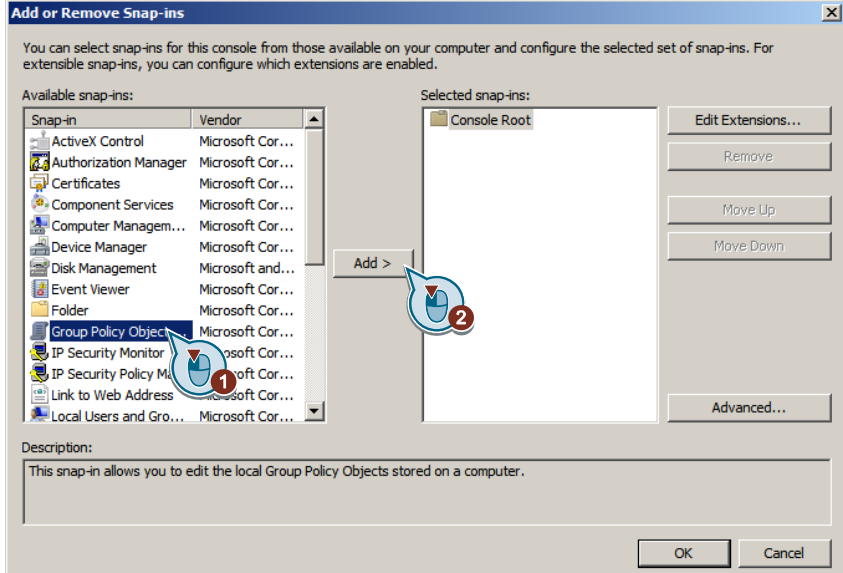
### 3 Basics

#### 3.1 Basics on the editors

#### 3.1.2 Microsoft Management Console

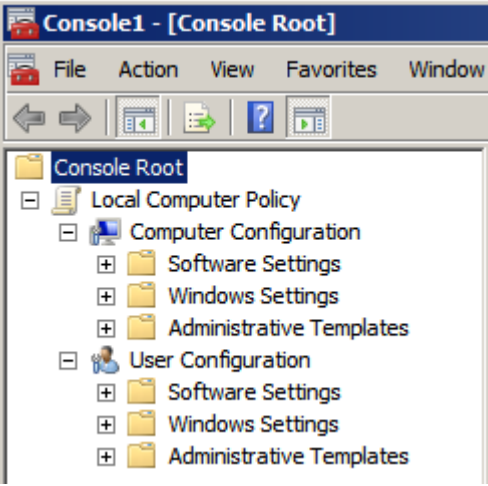
#### Call

Table 3-2

Process	Action
1.	Open "MMC.exe" via "Start > Execute"
2.	<p>Open the "Add/Remove Snap-Ins" dialog via menu entry "File &gt; Add/Remove Snap-Ins".</p> 
3.	<p>In the following dialog you select the entry "Group Policy Object Editor" and press the "Add" button.</p> 
4.	Confirm the following dialog with "Complete" and the "Add/Remove Snap-Ins" dialog with "OK".

### 3 Basics

#### 3.1 Basics on the editors

Process	Action
5.	<p>The “Microsoft Management Console” opens</p> 

#### Properties

- Changing the computer and user configuration for all users
- Changing the user configuration for all selected users

**Note** In the following screenshot all modifications are performed by the user. These modifications may also be adopted for selected users only.

**Note** The following screenshot have been created with Windows 7 in the “Windows – classic” design. For other operating system variants, these may deviate.

## 4 Security Settings for IPCs without Network Access

### 4.1 User accounts and respective rights

**Risk:** Unauthorized modification of system parameters

**Weak point:** Only one administrator account exists

**Solution:** Operating the SIMATIC software as user with restricted user rights

#### 4.1.1 Differentiation between administrator and user account

The basic requirement for a secure system is the appropriate distribution of access rights, i.e. the user should only have the basic rights. If more rights are provided than necessary for the task of the respective user, the operational security of the IPCs is jeopardized unnecessarily.

The correct settings of the user accounts are decisive for the security of the system. Normal user and administrator should be separated. This is necessary to prevent undesired execution of software.

##### Administrator account

With the Administrator account you can change security settings, as well as install software and hardware. An Administrator account enables making settings for other users.

If administrator rights are required for a certain action, the administrator receives a warning message which he can simply acknowledge.

##### User with restricted rights

A user account with restricted rights must not perform any system changes. If certain actions require administrator authorization, the user must log on as administrator. After completing the action, the original restricted authorizations apply again.

Continuing information is available at:

Configuring Windows 7 for a standard user account

<https://technet.microsoft.com/en-gb/library/ee623984%28v=ws.10%29.aspx>

What is user account control?

<http://windows.microsoft.com/en-gb/windows/what-is-user-account-control>

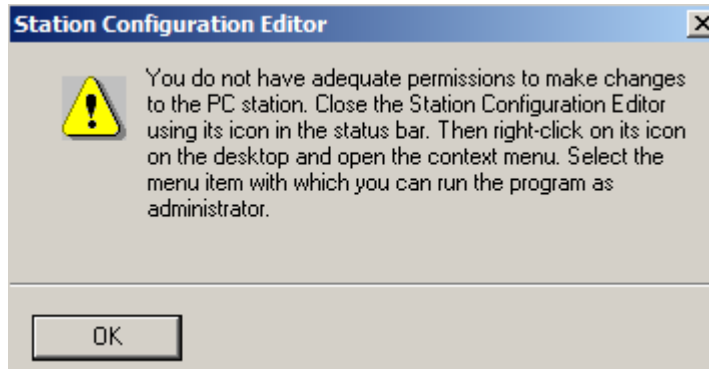
### 4.1.2 SIMATIC software by the user with restricted rights

#### WinAC RTX

With the restricted user account, the SIMATIC WinAC RTX soft PLC can be used without restriction.

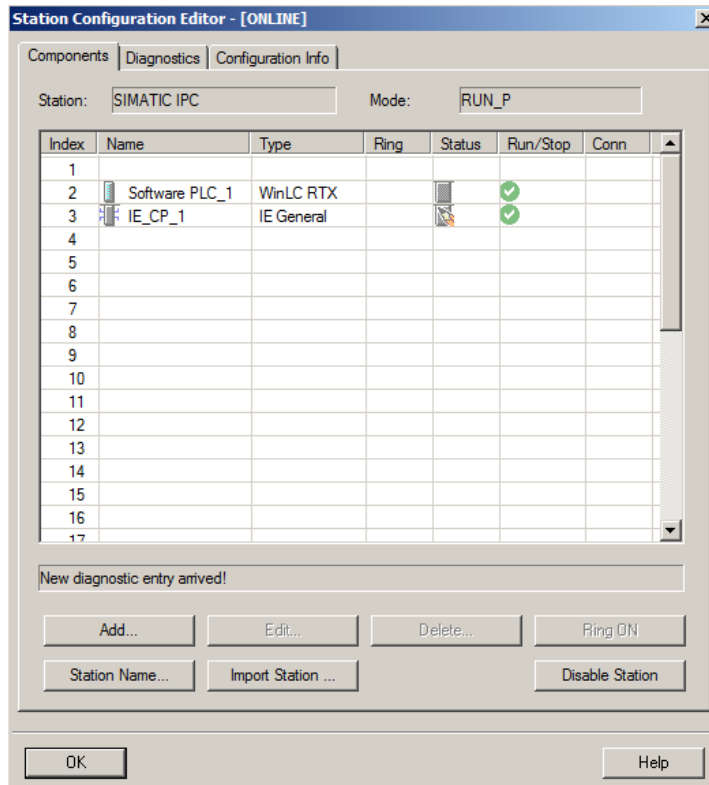
#### Station Configuration Editor

Figure 4-1



For the component configurator (English: station configurator) only read access is possible. Downloading a changed configuration is only possible on the IPC (mode: RUN\_P).

Figure 4-2

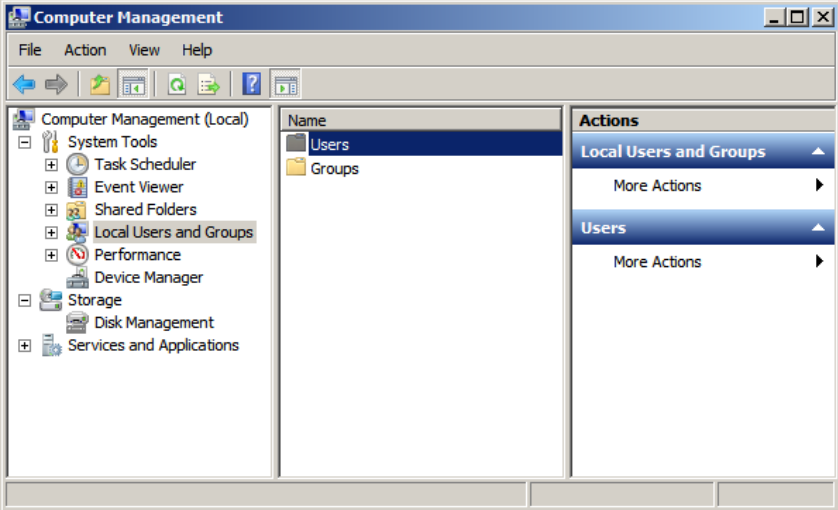
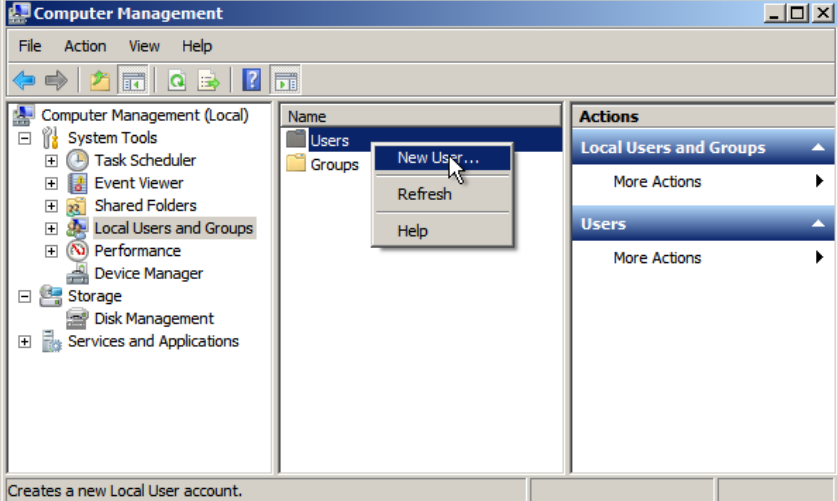


**4.1.3 Creating a user account**

To create a user account with restricted access rights in Windows, registration as administrator is necessary.

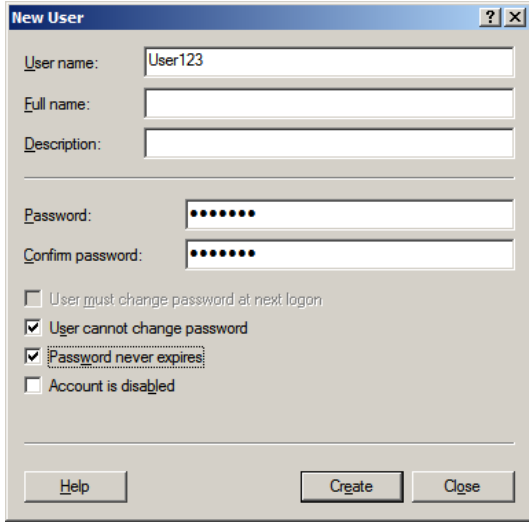
To create a new user account, there are several options in Windows. The recommended option, creating a new account using the Computer Management, is described in the table below. In this way, a standard user is created, i.e. a user with restricted rights.

Table 4-1

Process	Action
1.	<p>Open the “User Management” via “Start &gt; Computer &gt; Management &gt; Computer Management (Local) &gt; Local Users and Groups &gt; User”</p>  <p>The screenshot shows the Computer Management console window. The left-hand tree view is expanded to 'Local Users and Groups'. The main pane shows a list with 'Users' selected. The right-hand 'Actions' pane shows 'Local Users and Groups' and 'Users' sections, each with a 'More Actions' button.</p>
2.	<p>Right-click on “User &gt; New User...”</p>  <p>The screenshot shows the same Computer Management console window. The 'Users' folder in the main pane is right-clicked, and a context menu is displayed with the 'New User...' option highlighted. The status bar at the bottom of the window reads 'Creates a new Local User account.'</p>

## 4 Security Settings for IPCs without Network Access

### 4.1 User accounts and respective rights

Process	Action
3.	<p>Perform the settings as described in the screenshot.</p> 

#### Note

For the account you can define whether the user is permitted to change the password or when it expires (see [Table 4-1](#) Step 3).

Due to the particular requirements in industry, it is recommended to never let the password expire and to not permit any password change. Principally, the passwords should meet the complexity requirements (see [Table 5-4](#)).

## 4.2 Detecting user installation and elevation request with User Account Control (UAC)

**Risk:** Staff with user rights can install any program

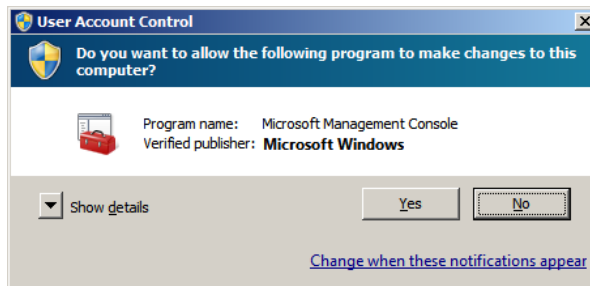
**Weak point:** Installing applications also possible by the user

**Solution:** Deactivating the password query for administrator rights

### Explaining the function

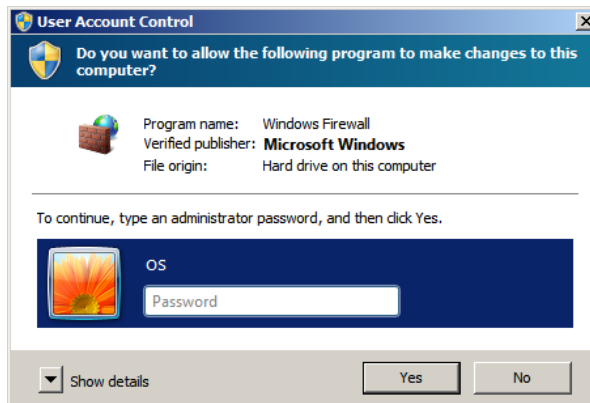
If administrators should execute actions that require elevated rights, these are prompted with the following dialog.

Figure 4-3



For users with restricted rights, the following dialog appears with the prompt to log on as administrator.

Figure 4-4



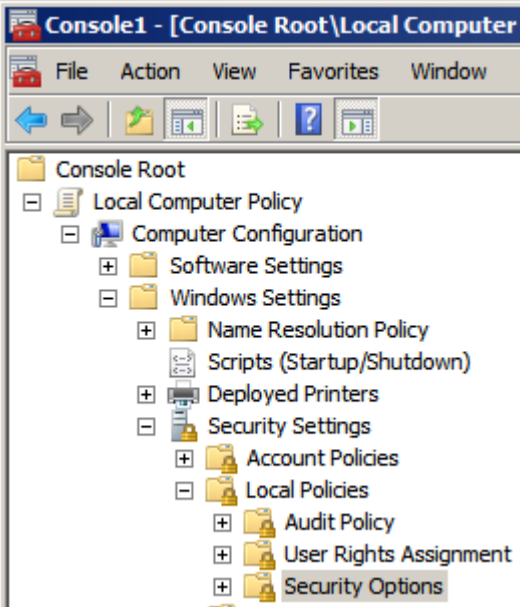
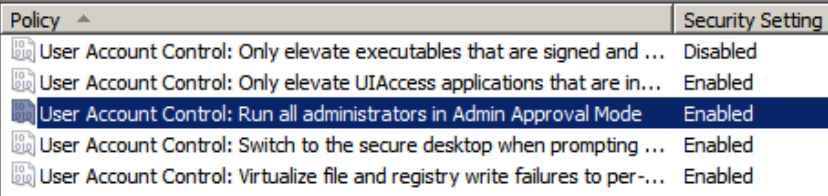
This function can be deactivated via the User Account Control (UAC). A user with restricted rights has no further option of gaining elevated rights.

## 4 Security Settings for IPCs without Network Access

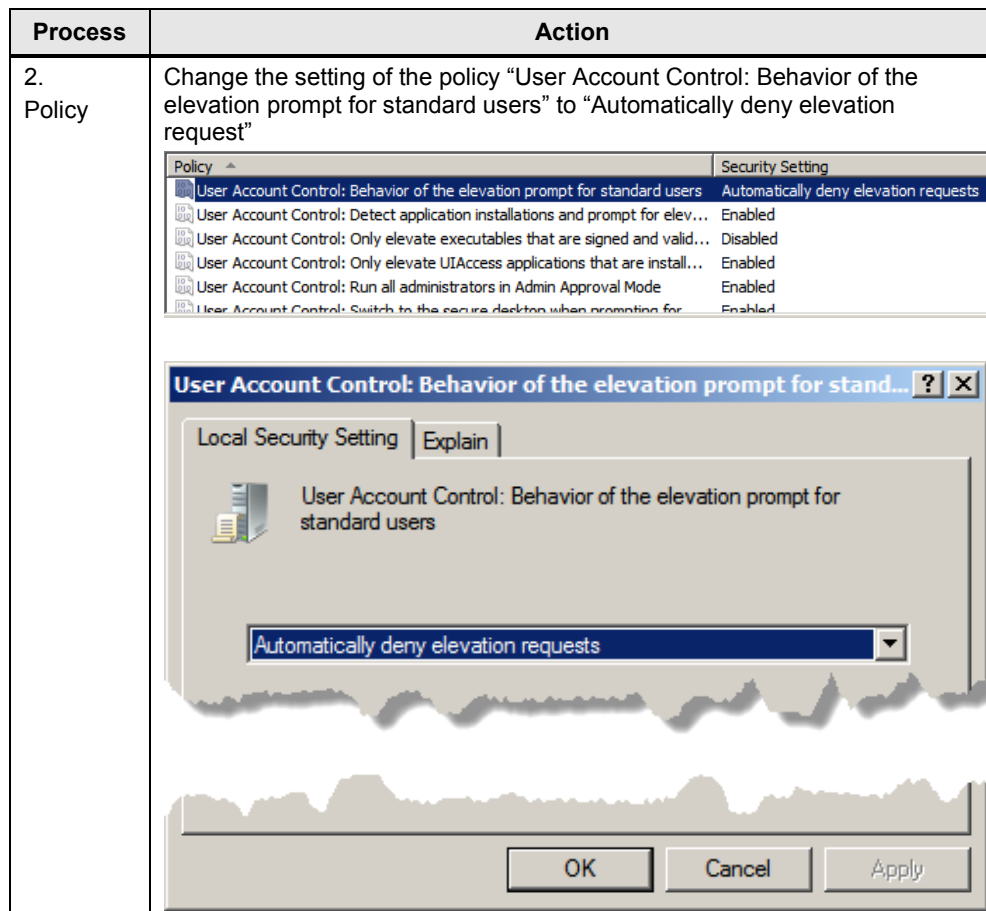
### 4.2 Detecting user installation and elevation request with User Account Control (UAC)

#### Adaptation of the required settings

Table 4-2

Process	Action
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Local Policies &gt; Security Options”</p> 
1. Policy	<p>Change the setting of the policy “User Account Control: Run all administrators in Admin Approval Mode” to “Enabled”</p> 





© Siemens AG 2015. All rights reserved

### 4.3 Enhanced Write Filter

**Risk:** Changes at the system

**Weak point:** System files can be manipulated

**Solution:** Due to the EWF, changes at the system files are only possible in RAM

#### Explaining the function

The Enhanced Write Filter (EWF) is a function available to the embedded operating system variants of the SIMATIC IPCs. EWF secures the file system against changing of files. The function redirects any write access to RAM. After a restart, the file system remains unchanged. There are no visible restrictions for the user. Malware that gained access during runtime, no longer exists after restart.

The advantages of the EWF become effective upon restarting the system. If an IPC runs continuously, an active EWF has no advantage.

<b>NOTICE</b>	If the EWF is active, the paths for WinAC RTX configuration and WinAC RTX program need to be set to a partition not protected by the EWF.
---------------	---

## 4 Security Settings for IPCs without Network Access

### 4.3 Enhanced Write Filter

**NOTICE** If the EWF is activated, the component configurator is grayed out and is in “RUN” mode. (Figure 4-5) Downloading a configuration is no longer possible. (Figure 4-6).

Figure 4-5 Component configurator for activated EWF

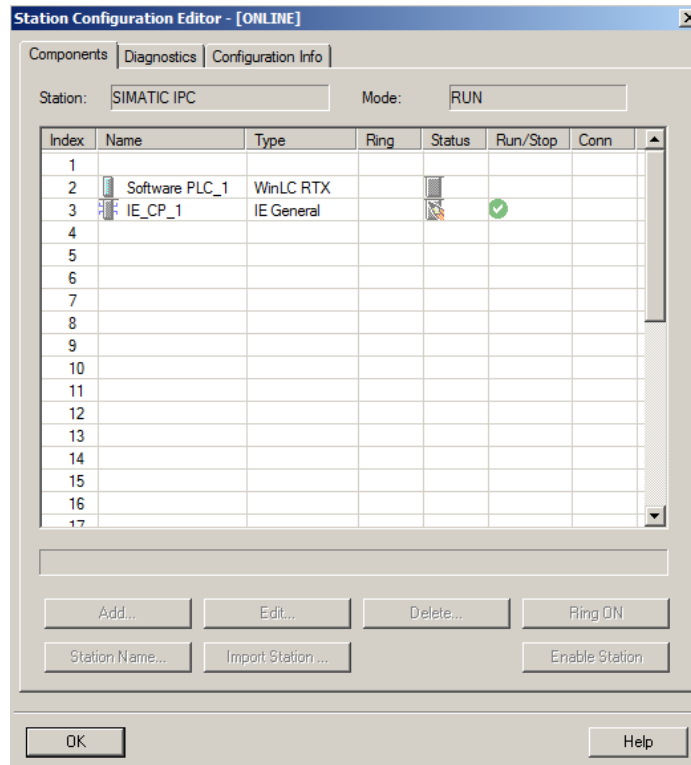
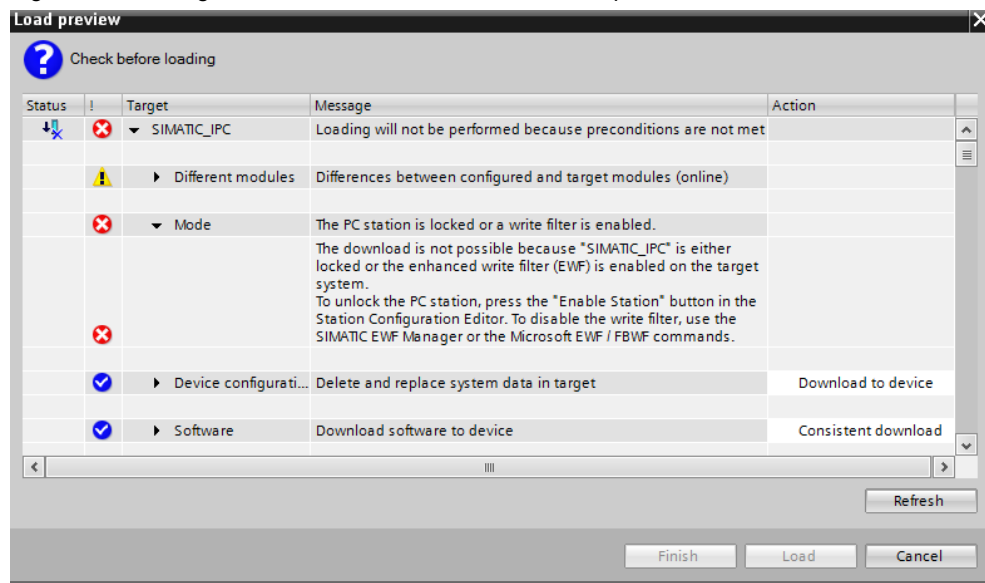


Figure 4-6 Message in the TIA Portal for download attempt at activated EWF



4.4 Do not shut down the system without login

**Adaptation of the required settings**

For setting the EWF as well as switching it on and off, you can use the EWFMgr.EXE program. The program call is performed via the Command prompt. The following functions are available

Table 4-3

Function	Command
Enable the write protection of drive C:	ewfmgr c: -enable
Disable the write protection of drive C: (changed data is adopted)	ewfmgr c: -commitanddisable
Adopt changed data on drive C:	ewfmgr c: -commit
Display information on the EWF drive.	ewfmgr c:
View help	ewfmgr c: /h

**Note** The EWF commands regarding the write protection only become effective after renewed booting.

**Note** Other functions or special features regarding the application of the EWF are available in the manual of the IPC used by you.

**4.4 Do not shut down the system without login**

**Risk:** Possible process stop

**Weak point:** Shut-down option freely accessible

**Solution:** Shut-down only possible after user login

**Explaining the function**

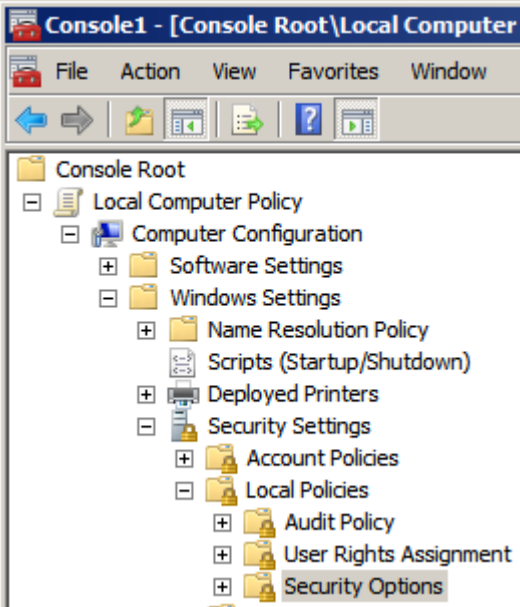
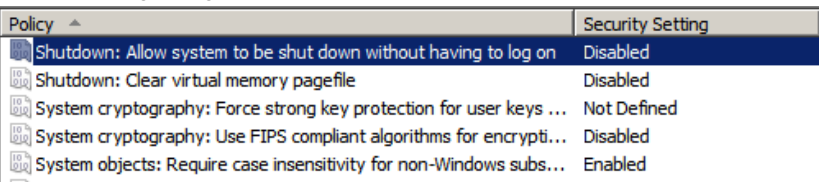
For some control stations it may be necessary to prevent shutting down the station, or only grant this right to certain users.

## 4 Security Settings for IPCs without Network Access

### 4.4 Do not shut down the system without login

#### Adaptation of the required settings

Table 4-4

Process	Action
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Local Policies &gt; Security Options”</p> 
1. Policy	<p>Change the setting of the policy “Shutdown: Allow system to be shut down without having to log on” to “Disabled”</p> 

## 4.5 Software restriction policies – AppLocker

**Risk:** Unauthorized execution of software

**Weak point:** Executing possible malware

**Solution:** Access control to software by means of AppLocker

### Explaining the function

Access to software should only be allowed within the required and necessary range to prevent misuse and in particular prevent the installation of malware. However, the respective AppLocker application is not available for all Windows variants (see following table).

This software can restrict the access to software packages. Using AppLocker enables/prevents the execution of the following application types:

- Executable files (EXE und COM)
- Scripts (JS, PS1, VBS, CMD und BAT)
- Windows Installer files (MSI and MSP)
- DLL files (DLL and OCX)

Continuing information is available at:

[http://technet.microsoft.com/en-gb/library/dd548340\(v=ws.10\).aspx](http://technet.microsoft.com/en-gb/library/dd548340(v=ws.10).aspx)

Table 4-5

Windows version	AppLocker active
Windows 7 Enterprise	
Windows 7 Ultimate	
Windows 7 Ultimate for Embedded Systems	
WES7P	
WES7E	X
WES7C	X
Windows 7 Professional	X

#### NOTICE

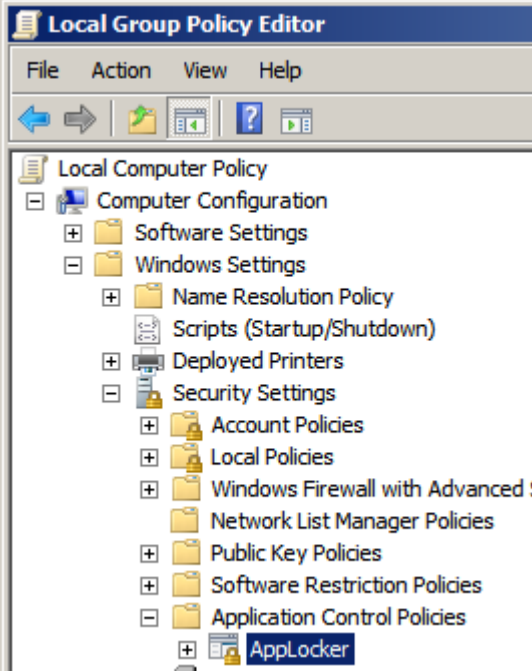
An AppLocker configuration can be made with all Windows versions, however, the configuration is only taken into consideration for the versions listed in [Table 4-5](#).

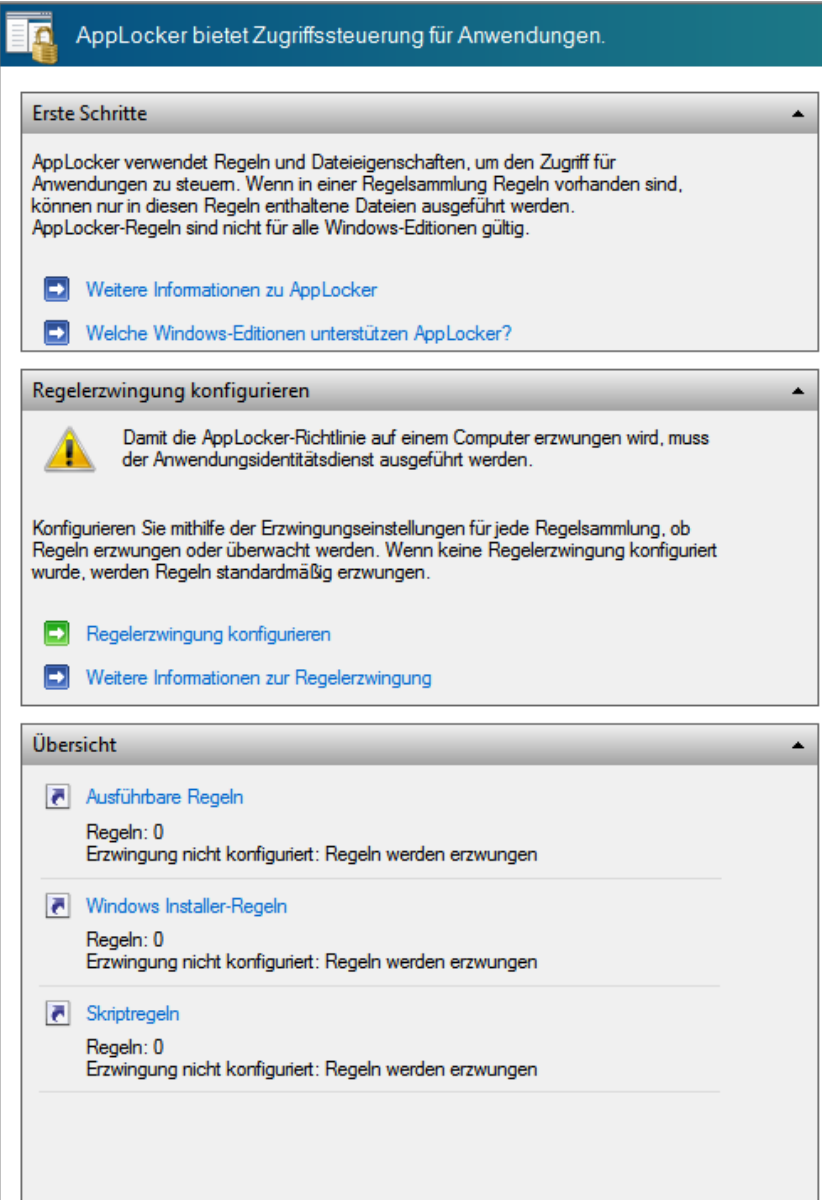
## 4 Security Settings for IPCs without Network Access

### 4.5 Software restriction policies – AppLocker

#### Adaptation of the required settings

Table 4-6

Process	Action
1.	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path: “Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Application Control Policies &gt; AppLocker”</p>  <p>The screenshot shows the Local Group Policy Editor window. The title bar reads 'Local Group Policy Editor'. The menu bar includes 'File', 'Action', 'View', and 'Help'. Below the menu bar is a toolbar with navigation icons. The main area displays a tree view of the Local Computer Policy. The tree is expanded to show the following structure: Local Computer Policy &gt; Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Application Control Policies &gt; AppLocker. The 'AppLocker' folder is highlighted with a blue selection bar.</p>

Process	Action
2.	<p>Now you define your appropriate rules.</p> 

## 4.6 Configuring Desktop policies and restrictions

**Risk:** Changing system data, access to Internet Explorer, workspace, network environment

**Weak point:** Desktop - access to applications

**Solution:** Preventing access to Windows applications and their properties via the Desktop

## 4 Security Settings for IPCs without Network Access

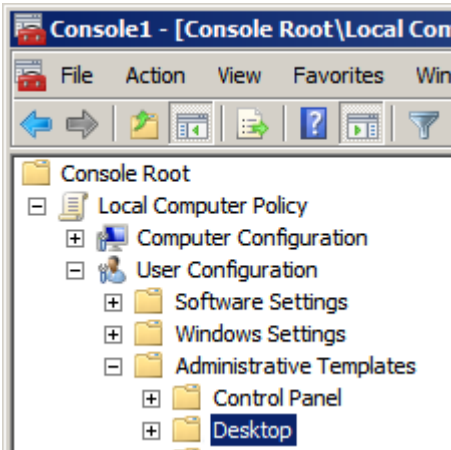
### 4.6 Configuring Desktop policies and restrictions

#### Explaining the function

In order to prevent access to functions of the operating system or to the internet by the operating staff, it is necessary to change the standard settings of the Desktop policy.

#### Adaptation of the required settings

Table 4-7

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path: “User Configuration &gt; Administrative Templates &gt; Desktop”</p> 										
1. Policy	<p>Change the setting of the policy “Prohibit User from manually redirecting Profile Folders” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit User from manually redirecting Profile Folders</td> <td>Enabled</td> </tr> <tr> <td>Remove Computer icon on the desktop</td> <td>Not configured</td> </tr> <tr> <td>Remove My Documents icon on the desktop</td> <td>Not configured</td> </tr> <tr> <td>Remove Properties from the Computer icon context menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit User from manually redirecting Profile Folders	Enabled	Remove Computer icon on the desktop	Not configured	Remove My Documents icon on the desktop	Not configured	Remove Properties from the Computer icon context menu	Not configured
Setting	State										
Prohibit User from manually redirecting Profile Folders	Enabled										
Remove Computer icon on the desktop	Not configured										
Remove My Documents icon on the desktop	Not configured										
Remove Properties from the Computer icon context menu	Not configured										
2. Policy	<p>Change the setting of the policy “Hide Internet Explorer icon on desktop” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Hide Internet Explorer icon on desktop</td> <td>Enabled</td> </tr> <tr> <td>Hide Network Locations icon on desktop</td> <td>Not configured</td> </tr> <tr> <td>Prevent adding, dragging, dropping and dosing the Taskbar's to...</td> <td>Not configured</td> </tr> <tr> <td>Prohibit adjusting desktop toolbars</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Hide Internet Explorer icon on desktop	Enabled	Hide Network Locations icon on desktop	Not configured	Prevent adding, dragging, dropping and dosing the Taskbar's to...	Not configured	Prohibit adjusting desktop toolbars	Not configured
Setting	State										
Hide Internet Explorer icon on desktop	Enabled										
Hide Network Locations icon on desktop	Not configured										
Prevent adding, dragging, dropping and dosing the Taskbar's to...	Not configured										
Prohibit adjusting desktop toolbars	Not configured										
3. Policy	<p>Change the setting of the policy “Remove Computer icon on the desktop” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Computer icon on the desktop</td> <td>Enabled</td> </tr> <tr> <td>Remove My Documents icon on the desktop</td> <td>Not configured</td> </tr> <tr> <td>Remove Properties from the Computer icon context menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Properties from the Documents icon context menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Computer icon on the desktop	Enabled	Remove My Documents icon on the desktop	Not configured	Remove Properties from the Computer icon context menu	Not configured	Remove Properties from the Documents icon context menu	Not configured
Setting	State										
Remove Computer icon on the desktop	Enabled										
Remove My Documents icon on the desktop	Not configured										
Remove Properties from the Computer icon context menu	Not configured										
Remove Properties from the Documents icon context menu	Not configured										



## 4 Security Settings for IPCs without Network Access

### 4.6 Configuring Desktop policies and restrictions

Process	Action										
4. Policy	<p>Change the setting of the policy "Hide Network Location icon on desktop" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Hide Network Locations icon on desktop</td> <td>Enabled</td> </tr> <tr> <td>Prevent adding, dragging, dropping and closing the Taskbar's to...</td> <td>Not configured</td> </tr> <tr> <td>Prohibit adjusting desktop toolbars</td> <td>Not configured</td> </tr> <tr> <td>Prohibit User from manually redirecting Profile Folders</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Hide Network Locations icon on desktop	Enabled	Prevent adding, dragging, dropping and closing the Taskbar's to...	Not configured	Prohibit adjusting desktop toolbars	Not configured	Prohibit User from manually redirecting Profile Folders	Not configured
Setting	State										
Hide Network Locations icon on desktop	Enabled										
Prevent adding, dragging, dropping and closing the Taskbar's to...	Not configured										
Prohibit adjusting desktop toolbars	Not configured										
Prohibit User from manually redirecting Profile Folders	Not configured										
5. Policy	<p>Change the setting of the policy "Remove Properties from the Computer icon context menu" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Properties from the Computer icon context menu</td> <td>Enabled</td> </tr> <tr> <td>Remove Properties from the Documents icon context menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Properties from the Recycle Bin context menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Recycle Bin icon from desktop</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Properties from the Computer icon context menu	Enabled	Remove Properties from the Documents icon context menu	Not configured	Remove Properties from the Recycle Bin context menu	Not configured	Remove Recycle Bin icon from desktop	Not configured
Setting	State										
Remove Properties from the Computer icon context menu	Enabled										
Remove Properties from the Documents icon context menu	Not configured										
Remove Properties from the Recycle Bin context menu	Not configured										
Remove Recycle Bin icon from desktop	Not configured										
6. Policy	<p>Change the setting of the policy "Remove Properties from the Documents icon context menu" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Properties from the Documents icon context menu</td> <td>Enabled</td> </tr> <tr> <td>Remove Properties from the Recycle Bin context menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Recycle Bin icon from desktop</td> <td>Not configured</td> </tr> <tr> <td>Remove the Desktop Cleanup Wizard</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Properties from the Documents icon context menu	Enabled	Remove Properties from the Recycle Bin context menu	Not configured	Remove Recycle Bin icon from desktop	Not configured	Remove the Desktop Cleanup Wizard	Not configured
Setting	State										
Remove Properties from the Documents icon context menu	Enabled										
Remove Properties from the Recycle Bin context menu	Not configured										
Remove Recycle Bin icon from desktop	Not configured										
Remove the Desktop Cleanup Wizard	Not configured										
7. Policy	<p>Change the setting of the policy "Remove Properties from the Recycle Bin context menu" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Properties from the Recycle Bin context menu</td> <td>Enabled</td> </tr> <tr> <td>Remove Recycle Bin icon from desktop</td> <td>Not configured</td> </tr> <tr> <td>Remove the Desktop Cleanup Wizard</td> <td>Not configured</td> </tr> <tr> <td>Turn off Aero Shake window minimizing mouse gesture</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Properties from the Recycle Bin context menu	Enabled	Remove Recycle Bin icon from desktop	Not configured	Remove the Desktop Cleanup Wizard	Not configured	Turn off Aero Shake window minimizing mouse gesture	Not configured
Setting	State										
Remove Properties from the Recycle Bin context menu	Enabled										
Remove Recycle Bin icon from desktop	Not configured										
Remove the Desktop Cleanup Wizard	Not configured										
Turn off Aero Shake window minimizing mouse gesture	Not configured										
8. Policy	<p>Change the setting of the policy "Prevent adding, dragging, dropping and closing the Taskbar's toolbars" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent adding, dragging, dropping and closing the Taskbar's toolbars</td> <td>Enabled</td> </tr> <tr> <td>Prohibit adjusting desktop toolbars</td> <td>Not configured</td> </tr> <tr> <td>Prohibit User from manually redirecting Profile Folders</td> <td>Not configured</td> </tr> <tr> <td>Remove Computer icon on the desktop</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Enabled	Prohibit adjusting desktop toolbars	Not configured	Prohibit User from manually redirecting Profile Folders	Not configured	Remove Computer icon on the desktop	Not configured
Setting	State										
Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Enabled										
Prohibit adjusting desktop toolbars	Not configured										
Prohibit User from manually redirecting Profile Folders	Not configured										
Remove Computer icon on the desktop	Not configured										
9. Policy	<p>Change the setting of the policy "Prohibit adjusting desktop toolbars" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit adjusting desktop toolbars</td> <td>Enabled</td> </tr> <tr> <td>Prohibit User from manually redirecting Profile Folders</td> <td>Not configured</td> </tr> <tr> <td>Remove Computer icon on the desktop</td> <td>Not configured</td> </tr> <tr> <td>Remove My Documents icon on the desktop</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit adjusting desktop toolbars	Enabled	Prohibit User from manually redirecting Profile Folders	Not configured	Remove Computer icon on the desktop	Not configured	Remove My Documents icon on the desktop	Not configured
Setting	State										
Prohibit adjusting desktop toolbars	Enabled										
Prohibit User from manually redirecting Profile Folders	Not configured										
Remove Computer icon on the desktop	Not configured										
Remove My Documents icon on the desktop	Not configured										

## 4 Security Settings for IPCs without Network Access

### 4.6 Configuring Desktop policies and restrictions

Table 4-8

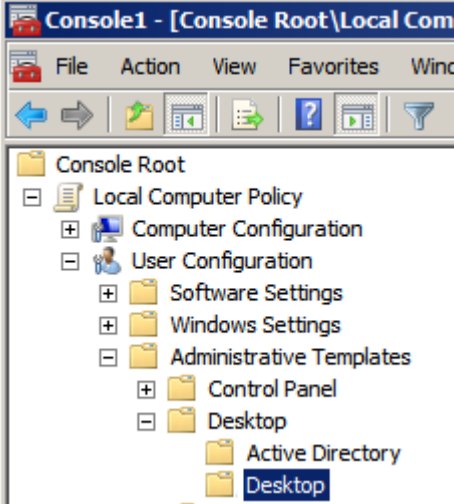
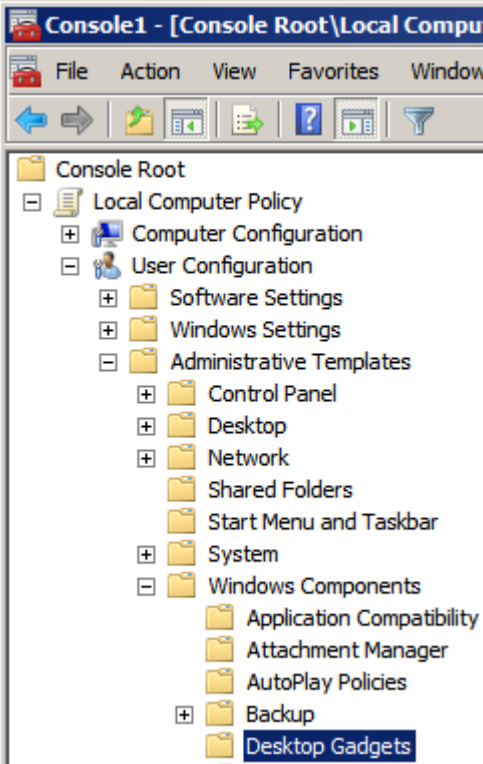
Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; Desktop &gt; Desktop”</p> 										
1. Policy	<p>Change the setting of the policy “Disable Active Desktop” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Disable Active Desktop</td> <td>Enabled</td> </tr> <tr> <td>Disable all items</td> <td>Not configured</td> </tr> <tr> <td>Enable Active Desktop</td> <td>Not configured</td> </tr> <tr> <td>Prohibit adding items</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Disable Active Desktop	Enabled	Disable all items	Not configured	Enable Active Desktop	Not configured	Prohibit adding items	Not configured
Setting	State										
Disable Active Desktop	Enabled										
Disable all items	Not configured										
Enable Active Desktop	Not configured										
Prohibit adding items	Not configured										
2. Policy	<p>Change the setting of the policy “Prohibit deleting items” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit deleting items</td> <td>Enabled</td> </tr> <tr> <td>Prohibit editing items</td> <td>Not configured</td> </tr> <tr> <td>Disable all items</td> <td>Not configured</td> </tr> <tr> <td>Add/Delete items</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit deleting items	Enabled	Prohibit editing items	Not configured	Disable all items	Not configured	Add/Delete items	Not configured
Setting	State										
Prohibit deleting items	Enabled										
Prohibit editing items	Not configured										
Disable all items	Not configured										
Add/Delete items	Not configured										
3. Policy	<p>Change the setting of the policy “Prohibit deleting items” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit deleting items</td> <td>Enabled</td> </tr> <tr> <td>Prohibit editing items</td> <td>Not configured</td> </tr> <tr> <td>Disable all items</td> <td>Not configured</td> </tr> <tr> <td>Add/Delete items</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit deleting items	Enabled	Prohibit editing items	Not configured	Disable all items	Not configured	Add/Delete items	Not configured
Setting	State										
Prohibit deleting items	Enabled										
Prohibit editing items	Not configured										
Disable all items	Not configured										
Add/Delete items	Not configured										

Table 4-9

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Desktop Gadgets”</p> 										
1. Policy	<p>Change the setting of the policy “Turn off desktop gadgets” to “Enabled”</p> <table border="1" data-bbox="539 1272 1361 1422"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Override the More Gadgets link</td> <td>Not configured</td> </tr> <tr> <td>Turn off desktop gadgets</td> <td>Enabled</td> </tr> <tr> <td>Restrict unpacking and installation of gadgets that are not digital...</td> <td>Not configured</td> </tr> <tr> <td>Turn Off user-installed desktop gadgets</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Override the More Gadgets link	Not configured	Turn off desktop gadgets	Enabled	Restrict unpacking and installation of gadgets that are not digital...	Not configured	Turn Off user-installed desktop gadgets	Not configured
Setting	State										
Override the More Gadgets link	Not configured										
Turn off desktop gadgets	Enabled										
Restrict unpacking and installation of gadgets that are not digital...	Not configured										
Turn Off user-installed desktop gadgets	Not configured										

© Siemens AG 2015 All rights reserved

## 4.7 Start menu and taskbar – Configuring policies

**Risk:** Changing system data/network environment, blocking/shutting down IPC

**Weak point:** Start menu and task bar - Access to applications

**Solution:** Preventing access to Windows applications via the Start menu

### Explaining the function

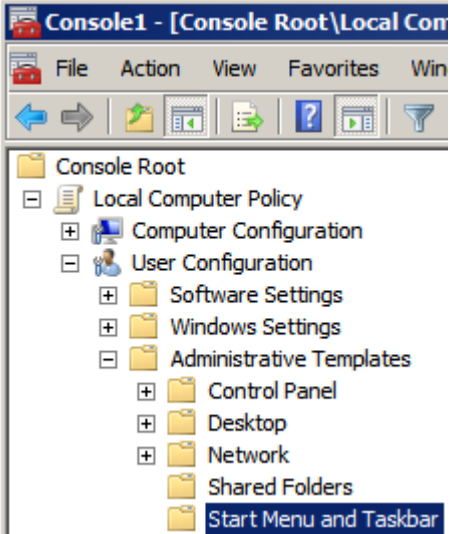
Menu entries such as “Search”, “Games” or “Music”, are normally not required and should therefore be disabled.

For security reasons, the “Printer” and “Network Connections” should not be offered (policy “Disable programs on Settings menu”).

It must be ensured here, that some guidelines only refuse access to the menu entries. The functions can partly be reached in other ways (e.g. at C:\Windows\system32).

**Adaptation of the required settings**

Table 4-10

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; Start Menu and Taskbar”</p> 										
1. Policy	<p>Change the setting of the policy “Lock the Taskbar” to “Enabled”</p> <table border="1" data-bbox="539 1064 1361 1220"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Lock the Taskbar</td> <td>Enabled</td> </tr> <tr> <td>Prevent changes to Taskbar and Start Menu Settings</td> <td>Not configured</td> </tr> <tr> <td>Prevent grouping of taskbar items</td> <td>Not configured</td> </tr> <tr> <td>Prevent users from adding or removing toolbars</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Lock the Taskbar	Enabled	Prevent changes to Taskbar and Start Menu Settings	Not configured	Prevent grouping of taskbar items	Not configured	Prevent users from adding or removing toolbars	Not configured
Setting	State										
Lock the Taskbar	Enabled										
Prevent changes to Taskbar and Start Menu Settings	Not configured										
Prevent grouping of taskbar items	Not configured										
Prevent users from adding or removing toolbars	Not configured										
2. Policy	<p>Change the setting of the policy “Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands” to “Enabled”</p> <table border="1" data-bbox="539 1294 1361 1422"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands</td> <td>Enabled</td> </tr> <tr> <td>Remove Balloon Tips on Start Menu items</td> <td>Not configured</td> </tr> <tr> <td>Remove Clock from the system notification area</td> <td>Not configured</td> </tr> <tr> <td>Remove common program groups from Start Menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Enabled	Remove Balloon Tips on Start Menu items	Not configured	Remove Clock from the system notification area	Not configured	Remove common program groups from Start Menu	Not configured
Setting	State										
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Enabled										
Remove Balloon Tips on Start Menu items	Not configured										
Remove Clock from the system notification area	Not configured										
Remove common program groups from Start Menu	Not configured										
3. Policy	<p>Change the setting of the policy “Remove Favorites menu from the Start Menu” to “Enabled”</p> <table border="1" data-bbox="539 1496 1361 1662"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Favorites menu from Start Menu</td> <td>Enabled</td> </tr> <tr> <td>Remove frequent programs list from the Start Menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Games link from Start Menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Help menu from Start Menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Favorites menu from Start Menu	Enabled	Remove frequent programs list from the Start Menu	Not configured	Remove Games link from Start Menu	Not configured	Remove Help menu from Start Menu	Not configured
Setting	State										
Remove Favorites menu from Start Menu	Enabled										
Remove frequent programs list from the Start Menu	Not configured										
Remove Games link from Start Menu	Not configured										
Remove Help menu from Start Menu	Not configured										
4. Policy	<p>Change the setting of the policy “Remove Search link from the Start Menu” to “Enabled”</p> <table border="1" data-bbox="539 1736 1361 1892"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Search link from Start Menu</td> <td>Enabled</td> </tr> <tr> <td>Remove See More Results / Search Everywhere link</td> <td>Not configured</td> </tr> <tr> <td>Remove the “Undock PC” button from the Start Menu</td> <td>Not configured</td> </tr> <tr> <td>Remove the Action Center icon</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Search link from Start Menu	Enabled	Remove See More Results / Search Everywhere link	Not configured	Remove the “Undock PC” button from the Start Menu	Not configured	Remove the Action Center icon	Not configured
Setting	State										
Remove Search link from Start Menu	Enabled										
Remove See More Results / Search Everywhere link	Not configured										
Remove the “Undock PC” button from the Start Menu	Not configured										
Remove the Action Center icon	Not configured										

## 4 Security Settings for IPCs without Network Access

### 4.7 Start menu and taskbar – Configuring policies

Process	Action										
5. Policy	<p>Change the setting of the policy “Remove Games link from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting ^</th> <th>State</th> </tr> </thead> <tbody> <tr> <td> Remove Games link from Start Menu</td> <td>Enabled</td> </tr> <tr> <td> Remove Help menu from Start Menu</td> <td>Not configured</td> </tr> <tr> <td> Remove Homegroup link from Start Menu</td> <td>Not configured</td> </tr> <tr> <td> Remove links and access to Windows Update</td> <td>Not configured</td> </tr> </tbody> </table>	Setting ^	State	Remove Games link from Start Menu	Enabled	Remove Help menu from Start Menu	Not configured	Remove Homegroup link from Start Menu	Not configured	Remove links and access to Windows Update	Not configured
Setting ^	State										
Remove Games link from Start Menu	Enabled										
Remove Help menu from Start Menu	Not configured										
Remove Homegroup link from Start Menu	Not configured										
Remove links and access to Windows Update	Not configured										
6. Policy	<p>Change the setting of the policy “Remove Network Connections from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting ^</th> <th>State</th> </tr> </thead> <tbody> <tr> <td> Remove Network Connections from Start Menu</td> <td>Enabled</td> </tr> <tr> <td> Remove Network icon from Start Menu</td> <td>Not configured</td> </tr> <tr> <td> Remove Pictures icon from Start Menu</td> <td>Not configured</td> </tr> <tr> <td> Remove pinned programs from the Taskbar</td> <td>Not configured</td> </tr> </tbody> </table>	Setting ^	State	Remove Network Connections from Start Menu	Enabled	Remove Network icon from Start Menu	Not configured	Remove Pictures icon from Start Menu	Not configured	Remove pinned programs from the Taskbar	Not configured
Setting ^	State										
Remove Network Connections from Start Menu	Enabled										
Remove Network icon from Start Menu	Not configured										
Remove Pictures icon from Start Menu	Not configured										
Remove pinned programs from the Taskbar	Not configured										
7. Policy	<p>Change the setting of the policy “Remove Run menu from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting ^</th> <th>State</th> </tr> </thead> <tbody> <tr> <td> Remove Run menu from Start Menu</td> <td>Enabled</td> </tr> <tr> <td> Remove Search Computer link</td> <td>Not configured</td> </tr> <tr> <td> Remove Search link from Start Menu</td> <td>Not configured</td> </tr> <tr> <td> Remove See More Results / Search Everywhere link</td> <td>Not configured</td> </tr> </tbody> </table>	Setting ^	State	Remove Run menu from Start Menu	Enabled	Remove Search Computer link	Not configured	Remove Search link from Start Menu	Not configured	Remove See More Results / Search Everywhere link	Not configured
Setting ^	State										
Remove Run menu from Start Menu	Enabled										
Remove Search Computer link	Not configured										
Remove Search link from Start Menu	Not configured										
Remove See More Results / Search Everywhere link	Not configured										
8. Policy	<p>Change the setting of the policy “Remove Music icon from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting ^</th> <th>State</th> </tr> </thead> <tbody> <tr> <td> Remove Music icon from Start Menu</td> <td>Enabled</td> </tr> <tr> <td> Remove Network Connections from Start Menu</td> <td>Not configured</td> </tr> <tr> <td> Remove Network icon from Start Menu</td> <td>Not configured</td> </tr> <tr> <td> Remove Pictures icon from Start Menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting ^	State	Remove Music icon from Start Menu	Enabled	Remove Network Connections from Start Menu	Not configured	Remove Network icon from Start Menu	Not configured	Remove Pictures icon from Start Menu	Not configured
Setting ^	State										
Remove Music icon from Start Menu	Enabled										
Remove Network Connections from Start Menu	Not configured										
Remove Network icon from Start Menu	Not configured										
Remove Pictures icon from Start Menu	Not configured										
9. Policy	<p>Change the setting of the policy “Remove Network icon from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting ^</th> <th>State</th> </tr> </thead> <tbody> <tr> <td> Remove Network icon from Start Menu</td> <td>Enabled</td> </tr> <tr> <td> Remove Pictures icon from Start Menu</td> <td>Not configured</td> </tr> <tr> <td> Remove pinned programs from the Taskbar</td> <td>Not configured</td> </tr> <tr> <td> Remove pinned programs list from the Start Menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting ^	State	Remove Network icon from Start Menu	Enabled	Remove Pictures icon from Start Menu	Not configured	Remove pinned programs from the Taskbar	Not configured	Remove pinned programs list from the Start Menu	Not configured
Setting ^	State										
Remove Network icon from Start Menu	Enabled										
Remove Pictures icon from Start Menu	Not configured										
Remove pinned programs from the Taskbar	Not configured										
Remove pinned programs list from the Start Menu	Not configured										
10. Policy	<p>Change the setting of the policy “Remove Pictures icon from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting ^</th> <th>State</th> </tr> </thead> <tbody> <tr> <td> Remove Pictures icon from Start Menu</td> <td>Enabled</td> </tr> <tr> <td> Remove pinned programs from the Taskbar</td> <td>Not configured</td> </tr> <tr> <td> Remove pinned programs list from the Start Menu</td> <td>Not configured</td> </tr> <tr> <td> Remove programs on Settings menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting ^	State	Remove Pictures icon from Start Menu	Enabled	Remove pinned programs from the Taskbar	Not configured	Remove pinned programs list from the Start Menu	Not configured	Remove programs on Settings menu	Not configured
Setting ^	State										
Remove Pictures icon from Start Menu	Enabled										
Remove pinned programs from the Taskbar	Not configured										
Remove pinned programs list from the Start Menu	Not configured										
Remove programs on Settings menu	Not configured										
11. Policy	<p>Change the setting of the policy “Prevent changes to Taskbar and Start Menu Settings” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting ^</th> <th>State</th> </tr> </thead> <tbody> <tr> <td> Prevent changes to Taskbar and Start Menu Settings</td> <td>Enabled</td> </tr> <tr> <td> Prevent grouping of taskbar items</td> <td>Not configured</td> </tr> <tr> <td> Prevent users from adding or removing toolbars</td> <td>Not configured</td> </tr> <tr> <td> Prevent users from moving taskbar to another screen dock lo...</td> <td>Not configured</td> </tr> </tbody> </table>	Setting ^	State	Prevent changes to Taskbar and Start Menu Settings	Enabled	Prevent grouping of taskbar items	Not configured	Prevent users from adding or removing toolbars	Not configured	Prevent users from moving taskbar to another screen dock lo...	Not configured
Setting ^	State										
Prevent changes to Taskbar and Start Menu Settings	Enabled										
Prevent grouping of taskbar items	Not configured										
Prevent users from adding or removing toolbars	Not configured										
Prevent users from moving taskbar to another screen dock lo...	Not configured										

## 4 Security Settings for IPCs without Network Access

### 4.7 Start menu and taskbar – Configuring policies

Process	Action										
12. Policy	<p>Change the setting of the policy “Remove Downloads link from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Downloads link from Start Menu</td> <td>Enabled</td> </tr> <tr> <td>Remove drag-and-drop and context menus on the Start Menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Favorites menu from Start Menu</td> <td>Not configured</td> </tr> <tr> <td>Remove frequent programs list from the Start Menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Downloads link from Start Menu	Enabled	Remove drag-and-drop and context menus on the Start Menu	Not configured	Remove Favorites menu from Start Menu	Not configured	Remove frequent programs list from the Start Menu	Not configured
Setting	State										
Remove Downloads link from Start Menu	Enabled										
Remove drag-and-drop and context menus on the Start Menu	Not configured										
Remove Favorites menu from Start Menu	Not configured										
Remove frequent programs list from the Start Menu	Not configured										
13. Policy	<p>Change the setting of the policy “Remove Homegroup link from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Homegroup link from Start Menu</td> <td>Enabled</td> </tr> <tr> <td>Remove links and access to Windows Update</td> <td>Not configured</td> </tr> <tr> <td>Remove Logoff on the Start Menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Music icon from Start Menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Homegroup link from Start Menu	Enabled	Remove links and access to Windows Update	Not configured	Remove Logoff on the Start Menu	Not configured	Remove Music icon from Start Menu	Not configured
Setting	State										
Remove Homegroup link from Start Menu	Enabled										
Remove links and access to Windows Update	Not configured										
Remove Logoff on the Start Menu	Not configured										
Remove Music icon from Start Menu	Not configured										
14. Policy	<p>Change the setting of the policy “Remove Recorded TV link from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Recorded TV link from Start Menu</td> <td>Enabled</td> </tr> <tr> <td>Remove Run menu from Start Menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Search Computer link</td> <td>Not configured</td> </tr> <tr> <td>Remove Search link from Start Menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Recorded TV link from Start Menu	Enabled	Remove Run menu from Start Menu	Not configured	Remove Search Computer link	Not configured	Remove Search link from Start Menu	Not configured
Setting	State										
Remove Recorded TV link from Start Menu	Enabled										
Remove Run menu from Start Menu	Not configured										
Remove Search Computer link	Not configured										
Remove Search link from Start Menu	Not configured										
15. Policy	<p>Change the setting of the policy “Remove Video link from the Start Menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Videos link from Start Menu</td> <td>Enabled</td> </tr> <tr> <td>Show QuickLaunch on Taskbar</td> <td>Not configured</td> </tr> <tr> <td>Turn off all balloon notifications</td> <td>Not configured</td> </tr> <tr> <td>Turn off automatic promotion of notification icons to the task...</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Videos link from Start Menu	Enabled	Show QuickLaunch on Taskbar	Not configured	Turn off all balloon notifications	Not configured	Turn off automatic promotion of notification icons to the task...	Not configured
Setting	State										
Remove Videos link from Start Menu	Enabled										
Show QuickLaunch on Taskbar	Not configured										
Turn off all balloon notifications	Not configured										
Turn off automatic promotion of notification icons to the task...	Not configured										
16. Policy	<p>Change the setting of the policy “Remove programs on Settings menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove programs on Settings menu</td> <td>Enabled</td> </tr> <tr> <td>Remove Recent Items menu from Start Menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Recorded TV link from Start Menu</td> <td>Not configured</td> </tr> <tr> <td>Remove Run menu from Start Menu</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove programs on Settings menu	Enabled	Remove Recent Items menu from Start Menu	Not configured	Remove Recorded TV link from Start Menu	Not configured	Remove Run menu from Start Menu	Not configured
Setting	State										
Remove programs on Settings menu	Enabled										
Remove Recent Items menu from Start Menu	Not configured										
Remove Recorded TV link from Start Menu	Not configured										
Remove Run menu from Start Menu	Not configured										

## 4.8 Configure Ctrl+Alt+Del

**Risk:** Processes and services can be stopped, faulty IPC configuration

**Weak point:** Changing the password, blocking the IPCs, access to Task Manager

**Solution:** Restriction of functions after “Ctrl+Alt+Del”

### Explaining the function

The computer configuration gives you the option of switching off the key combination “Ctrl+Alt+Del” for the user login.

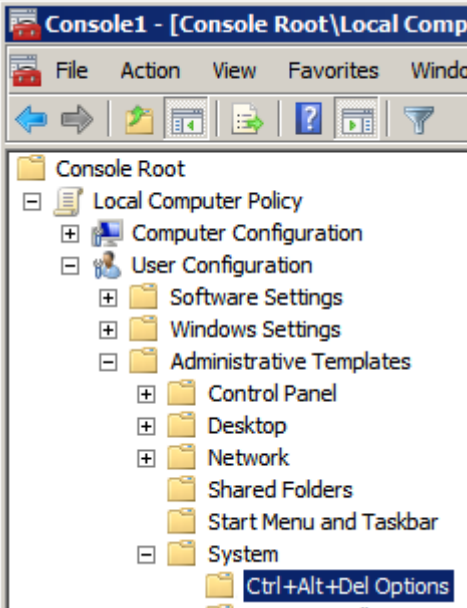
“Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Interactive Login: no CTRL + ALT + DEL required)

It is recommended not to change these settings of the Computer Configuration since these settings apply to all users, including administrator.

Alternatively, there is the option via the user configuration to set which actions are possible for pressing “Ctrl+Alt+Del” (e.g. no access to Task Manager).

**Adaptation of the required settings**

Table 4-11

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; System &gt; CTRL+ALT+DEL (Options)”</p> 										
1. Policy	<p>Change the setting of the policy “Remove Change Password” to “Enabled”</p> <table border="1" data-bbox="539 1176 1361 1344"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Change Password</td> <td>Enabled</td> </tr> <tr> <td>Remove Lock Computer</td> <td>Not configured</td> </tr> <tr> <td>Remove Logoff</td> <td>Not configured</td> </tr> <tr> <td>Remove Task Manager</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Change Password	Enabled	Remove Lock Computer	Not configured	Remove Logoff	Not configured	Remove Task Manager	Not configured
Setting	State										
Remove Change Password	Enabled										
Remove Lock Computer	Not configured										
Remove Logoff	Not configured										
Remove Task Manager	Not configured										
2. Policy	<p>Change the setting of the policy “Remove Lock Computer” to “Enabled”</p> <table border="1" data-bbox="539 1388 1361 1556"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Lock Computer</td> <td>Enabled</td> </tr> <tr> <td>Remove Change Password</td> <td>Not configured</td> </tr> <tr> <td>Remove Logoff</td> <td>Not configured</td> </tr> <tr> <td>Remove Task Manager</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Lock Computer	Enabled	Remove Change Password	Not configured	Remove Logoff	Not configured	Remove Task Manager	Not configured
Setting	State										
Remove Lock Computer	Enabled										
Remove Change Password	Not configured										
Remove Logoff	Not configured										
Remove Task Manager	Not configured										
3. Policy	<p>Change the setting of the policy “Remove Task Manager” to “Enabled”</p> <table border="1" data-bbox="539 1601 1361 1758"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Remove Task Manager</td> <td>Enabled</td> </tr> <tr> <td>Remove Lock Computer</td> <td>Not configured</td> </tr> <tr> <td>Remove Change Password</td> <td>Not configured</td> </tr> <tr> <td>Remove Logoff</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Remove Task Manager	Enabled	Remove Lock Computer	Not configured	Remove Change Password	Not configured	Remove Logoff	Not configured
Setting	State										
Remove Task Manager	Enabled										
Remove Lock Computer	Not configured										
Remove Change Password	Not configured										
Remove Logoff	Not configured										



## 4.9 Preventing access to Control Panel

**Risk:** Processes and services can be stopped, faulty IPC configuration

**Weak point:** Changing the system parameters in Control Panel

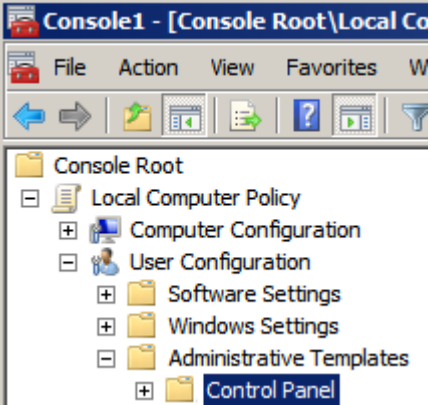
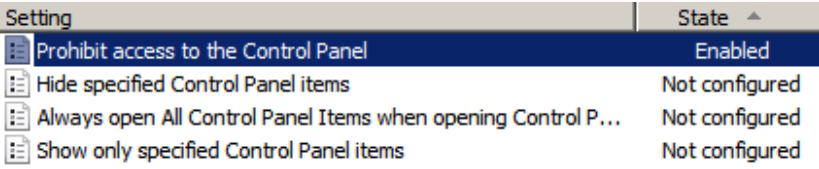
**Solution:** Preventing access to Control Panel

### Explaining the function

Undesired changes at the system can be made via the Control Panel (e.g. network connections, uninstall program, etc.) Access to the Control Panel should therefore be prevented.

### Adaptation of the required settings

Table 4-12

Process	Action
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path: “User Configuration &gt; Administrative Templates &gt; Control Panel”</p> 
1. Policy	<p>Change the setting of the policy “Prohibit access to Control Panel” to “Enabled”</p> 

© Siemens AG 2015. All rights reserved.

## 4.10 Configuring access to removable storage medium

**Risk:** Infecting IPC with malware, undesired installation of programs

**Weak point:** Access to removable storage medium (e.g. USB sticks)

**Solution:** Preventing access to removable storage medium

### Explaining the function

The IPC can be infected with malware by plugging in a USB stick. It is therefore recommended to refuse access to various removable storage devices in the group

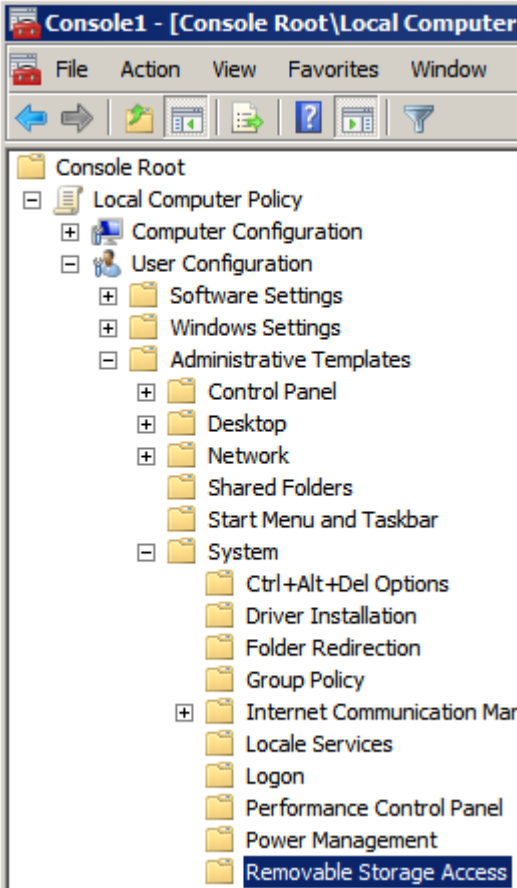
## 4 Security Settings for IPCs without Network Access

### 4.10 Configuring access to removable storage medium

policy settings. There is the option to refuse read and/or write access as well as “all access”.

#### Adaptation of the required settings

Table 4-13

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; System &gt; Removable Storage Access”</p> 										
1. Policy	<p>Change the setting of the policy “Removable Disks: Deny read access” to “Enabled”.</p> <table border="1" data-bbox="539 1563 1361 1731"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Removable Disks: Deny read access</td> <td>Enabled</td> </tr> <tr> <td>Removable Disks: Deny write access</td> <td>Not configured</td> </tr> <tr> <td>Tape Drives: Deny read access</td> <td>Not configured</td> </tr> <tr> <td>Tape Drives: Deny write access</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Removable Disks: Deny read access	Enabled	Removable Disks: Deny write access	Not configured	Tape Drives: Deny read access	Not configured	Tape Drives: Deny write access	Not configured
Setting	State										
Removable Disks: Deny read access	Enabled										
Removable Disks: Deny write access	Not configured										
Tape Drives: Deny read access	Not configured										
Tape Drives: Deny write access	Not configured										
2. Policy	<p>Change the setting of the policy “Removable Disks: Deny write access” to “Enabled”.</p> <table border="1" data-bbox="539 1798 1361 1962"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Removable Disks: Deny write access</td> <td>Enabled</td> </tr> <tr> <td>Tape Drives: Deny read access</td> <td>Not configured</td> </tr> <tr> <td>Tape Drives: Deny write access</td> <td>Not configured</td> </tr> <tr> <td>Time (in seconds) to force reboot</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Removable Disks: Deny write access	Enabled	Tape Drives: Deny read access	Not configured	Tape Drives: Deny write access	Not configured	Time (in seconds) to force reboot	Not configured
Setting	State										
Removable Disks: Deny write access	Enabled										
Tape Drives: Deny read access	Not configured										
Tape Drives: Deny write access	Not configured										
Time (in seconds) to force reboot	Not configured										

4.11 Deactivate Autoplay function

Process	Action										
3. Policy	<p>Change the setting of the policy “All Removable Storage classes: Deny all access” to “Enabled”.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>All Removable Storage classes: Deny all access</td> <td>Enabled</td> </tr> <tr> <td>CD and DVD: Deny read access</td> <td>Not configured</td> </tr> <tr> <td>CD and DVD: Deny write access</td> <td>Not configured</td> </tr> <tr> <td>Custom Classes: Deny read access</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	All Removable Storage classes: Deny all access	Enabled	CD and DVD: Deny read access	Not configured	CD and DVD: Deny write access	Not configured	Custom Classes: Deny read access	Not configured
Setting	State										
All Removable Storage classes: Deny all access	Enabled										
CD and DVD: Deny read access	Not configured										
CD and DVD: Deny write access	Not configured										
Custom Classes: Deny read access	Not configured										
4. Policy	<p>Change the setting of the policy “WPD Devices: Deny read access” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>WPD Devices: Deny read access</td> <td>Enabled</td> </tr> <tr> <td>Time (in seconds) to force reboot</td> <td>Not configured</td> </tr> <tr> <td>Tape Drives: Deny write access</td> <td>Not configured</td> </tr> <tr> <td>Tape Drives: Deny read access</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	WPD Devices: Deny read access	Enabled	Time (in seconds) to force reboot	Not configured	Tape Drives: Deny write access	Not configured	Tape Drives: Deny read access	Not configured
Setting	State										
WPD Devices: Deny read access	Enabled										
Time (in seconds) to force reboot	Not configured										
Tape Drives: Deny write access	Not configured										
Tape Drives: Deny read access	Not configured										
5. Policy	<p>Change the setting of the policy “WPD Devices: Deny write access” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>WPD Devices: Deny write access</td> <td>Enabled</td> </tr> <tr> <td>WPD Devices: Deny read access</td> <td>Not configured</td> </tr> <tr> <td>Time (in seconds) to force reboot</td> <td>Not configured</td> </tr> <tr> <td>Tape Drives: Deny write access</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	WPD Devices: Deny write access	Enabled	WPD Devices: Deny read access	Not configured	Time (in seconds) to force reboot	Not configured	Tape Drives: Deny write access	Not configured
Setting	State										
WPD Devices: Deny write access	Enabled										
WPD Devices: Deny read access	Not configured										
Time (in seconds) to force reboot	Not configured										
Tape Drives: Deny write access	Not configured										

## 4.11 Deactivate Autoplay function

**Risk:** Infecting IPC with malware, undesired installation of programs

**Weak point:** Automatic execution of software (Autoplay function)

**Solution:** Deactivating Autoplay or Autorun

### Explaining the function

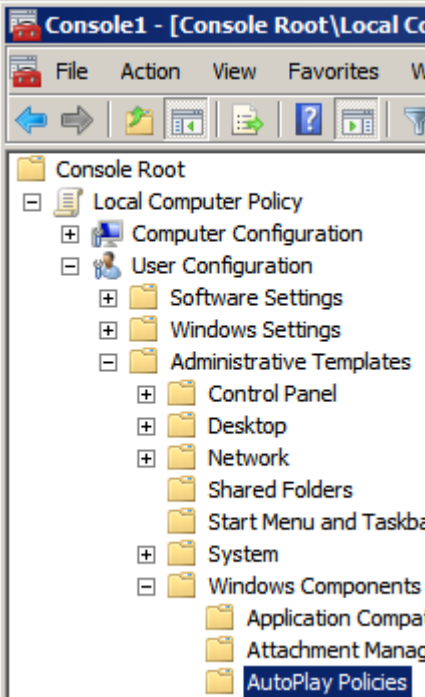
USB sticks and external disks may contain an Autoplay file (autorun.inf). In this way, viruses can infect the system, for example. The following table shows how do disable the Autoplay function as well as “AutoRun” (policy “AutoRun standard behavior”).

## 4 Security Settings for IPCs without Network Access

### 4.12 Prevent removable disk access for all installations

#### Adaptation of the required settings

Table 4-14

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; AutoPlay Policies”</p> 										
1. Policy	<p>Change the setting of the policy “Deactivate Autoplay” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off Autoplay</td> <td>Enabled</td> </tr> <tr> <td>Turn off Autoplay for non-volume devices</td> <td>Not configured</td> </tr> <tr> <td>Don't set the always do this checkbox</td> <td>Not configured</td> </tr> <tr> <td>Default behavior for AutoRun</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off Autoplay	Enabled	Turn off Autoplay for non-volume devices	Not configured	Don't set the always do this checkbox	Not configured	Default behavior for AutoRun	Not configured
Setting	State										
Turn off Autoplay	Enabled										
Turn off Autoplay for non-volume devices	Not configured										
Don't set the always do this checkbox	Not configured										
Default behavior for AutoRun	Not configured										
2. Policy	<p>Change the setting of the policy “Default behavior for AutoRun” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Default behavior for AutoRun</td> <td>Enabled</td> </tr> <tr> <td>Turn off Autoplay</td> <td>Not configured</td> </tr> <tr> <td>Turn off Autoplay for non-volume devices</td> <td>Not configured</td> </tr> <tr> <td>Don't set the always do this checkbox</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Default behavior for AutoRun	Enabled	Turn off Autoplay	Not configured	Turn off Autoplay for non-volume devices	Not configured	Don't set the always do this checkbox	Not configured
Setting	State										
Default behavior for AutoRun	Enabled										
Turn off Autoplay	Not configured										
Turn off Autoplay for non-volume devices	Not configured										
Don't set the always do this checkbox	Not configured										

## 4.12 Prevent removable disk access for all installations

**Risk:** Infecting IPC with malware, undesired installation of programs

**Weak point:** Installations from removable storage medium

**Solution:** Deactivating the installation of removable storage medium

#### **Explaining the function**

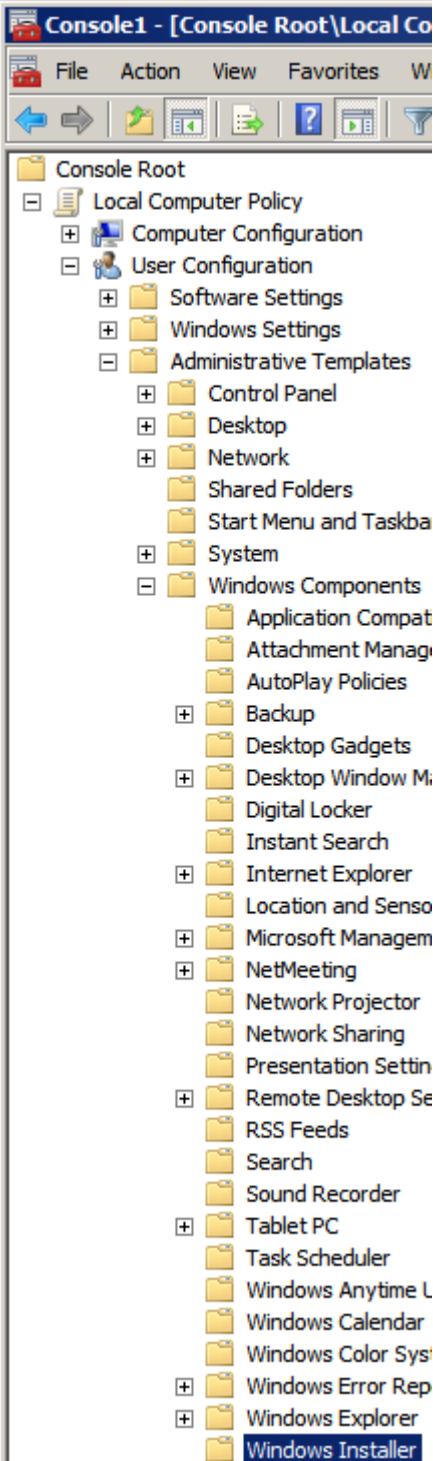
If it is not possible to generally prohibit access to USB media (see Chapter [4.10](#)), software should be prevented from being installed from removable storage devices. This prevents malware or other undesired programs from being installed on the IPC.

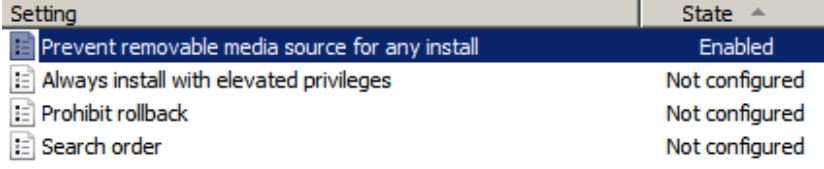
4 Security Settings for IPCs without Network Access

4.12 Prevent removable disk access for all installations

**Adaptation of the required settings**

Table 4-15

Process	Action
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Windows Installer”</p>  <p>The screenshot shows the MMC console with the following tree structure:</p> <ul style="list-style-type: none"> <li>Console Root             <ul style="list-style-type: none"> <li>Local Computer Policy</li> <li>Computer Configuration</li> <li>User Configuration                     <ul style="list-style-type: none"> <li>Software Settings</li> <li>Windows Settings</li> <li>Administrative Templates                             <ul style="list-style-type: none"> <li>Control Panel</li> <li>Desktop</li> <li>Network</li> <li>Shared Folders</li> <li>Start Menu and Taskba</li> <li>System</li> <li>Windows Components                                     <ul style="list-style-type: none"> <li>Application Compat</li> <li>Attachment Manag</li> <li>AutoPlay Policies</li> <li>Backup</li> <li>Desktop Gadgets</li> <li>Desktop Window M</li> <li>Digital Locker</li> <li>Instant Search</li> <li>Internet Explorer</li> <li>Location and Senso</li> <li>Microsoft Managem</li> <li>NetMeeting</li> <li>Network Projector</li> <li>Network Sharing</li> <li>Presentation Settin</li> <li>Remote Desktop Se</li> <li>RSS Feeds</li> <li>Search</li> <li>Sound Recorder</li> <li>Tablet PC</li> <li>Task Scheduler</li> <li>Windows Anytime L</li> <li>Windows Calendar</li> <li>Windows Color Sys</li> <li>Windows Error Rep</li> <li>Windows Explorer</li> <li>Windows Installer</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>

Process	Action										
1. Policy	Change the setting of the policy "Prevent removable media source for any install" to "Enabled"  <table border="1"><thead><tr><th>Setting</th><th>State</th></tr></thead><tbody><tr><td>Prevent removable media source for any install</td><td>Enabled</td></tr><tr><td>Always install with elevated privileges</td><td>Not configured</td></tr><tr><td>Prohibit rollback</td><td>Not configured</td></tr><tr><td>Search order</td><td>Not configured</td></tr></tbody></table>	Setting	State	Prevent removable media source for any install	Enabled	Always install with elevated privileges	Not configured	Prohibit rollback	Not configured	Search order	Not configured
Setting	State										
Prevent removable media source for any install	Enabled										
Always install with elevated privileges	Not configured										
Prohibit rollback	Not configured										
Search order	Not configured										

### 4.13 Refusing access to Microsoft Management Console

**Risk:** Changing the system configuration (group policies, firewall settings, etc.)

**Weak point:** Access to MMC (Microsoft Management Console)

**Solution:** Refusing access to MMC (Microsoft Management Console)

#### Explaining the function

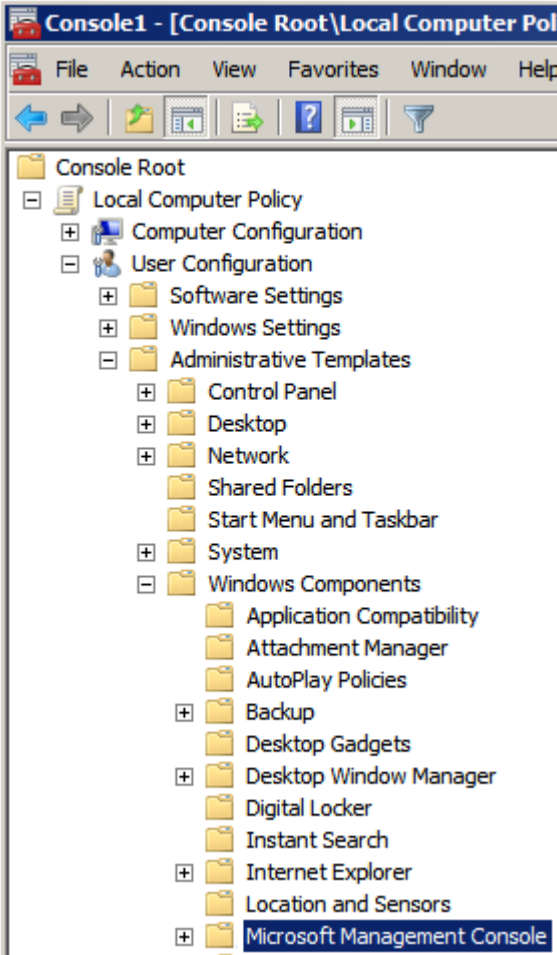
The graphic user interface "Microsoft Management Console" (MMC) is used for managing computers and users. It can be configured whether and how the MMC can be used.

## 4 Security Settings for IPCs without Network Access

### 4.13 Refusing access to Microsoft Management Console

#### Adaptation of the required settings

Table 4-16

Process	Action						
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Microsoft Management Console”</p> 						
1. Policy	<p>Change the setting of the policy “Restrict the user from entering author mode” to “Enabled”</p> <table border="1" data-bbox="539 1536 1361 1630"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Restrict the user from entering author mode</td> <td>Enabled</td> </tr> <tr> <td>Restrict users to the explicitly permitted list of snap-ins</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Restrict the user from entering author mode	Enabled	Restrict users to the explicitly permitted list of snap-ins	Not configured
Setting	State						
Restrict the user from entering author mode	Enabled						
Restrict users to the explicitly permitted list of snap-ins	Not configured						
2. Policy	<p>Change the setting of the policy “Restrict users to the explicitly permitted list of snap-ins” to “Enabled”</p> <table border="1" data-bbox="539 1709 1361 1803"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Restrict users to the explicitly permitted list of snap-ins</td> <td>Enabled</td> </tr> <tr> <td>Restrict the user from entering author mode</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Restrict users to the explicitly permitted list of snap-ins	Enabled	Restrict the user from entering author mode	Not configured
Setting	State						
Restrict users to the explicitly permitted list of snap-ins	Enabled						
Restrict the user from entering author mode	Not configured						



## 4.14 Refuse access to restore option

**Risk:** Undesired system changes

**Weak point:** Access to restore options

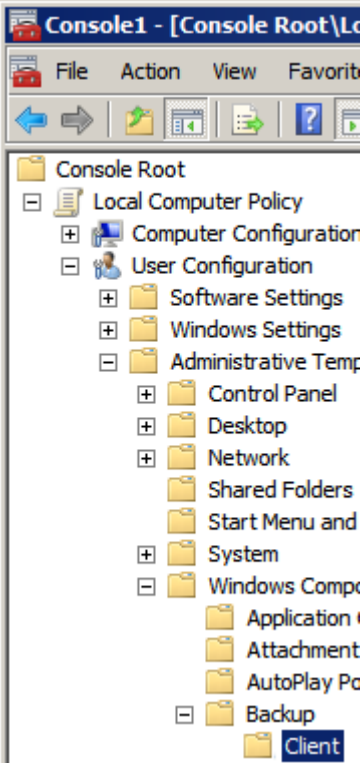
**Solution:** Restricting the restore options

### Explaining the function

Due to the deactivation of the restore option of the operating system, it is no longer possible to return to former versions of the operating system.

### Adaptation of the required settings

Table 4-17

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Backup &gt; Client”</p> 										
1. Policy	<p>Change the setting of the policy “Prevent the user from running the Backup Status and Configuration program” to “Enabled”</p> <table border="1" data-bbox="539 1738 1361 1879"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent the user from running the Backup Status and Configuration program</td> <td>Enabled</td> </tr> <tr> <td>Prevent backing up to local disks</td> <td>Not configured</td> </tr> <tr> <td>Prevent backing up to network location</td> <td>Not configured</td> </tr> <tr> <td>Prevent backing up to optical media (CD/DVD)</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prevent the user from running the Backup Status and Configuration program	Enabled	Prevent backing up to local disks	Not configured	Prevent backing up to network location	Not configured	Prevent backing up to optical media (CD/DVD)	Not configured
Setting	State										
Prevent the user from running the Backup Status and Configuration program	Enabled										
Prevent backing up to local disks	Not configured										
Prevent backing up to network location	Not configured										
Prevent backing up to optical media (CD/DVD)	Not configured										

## 4 Security Settings for IPCs without Network Access

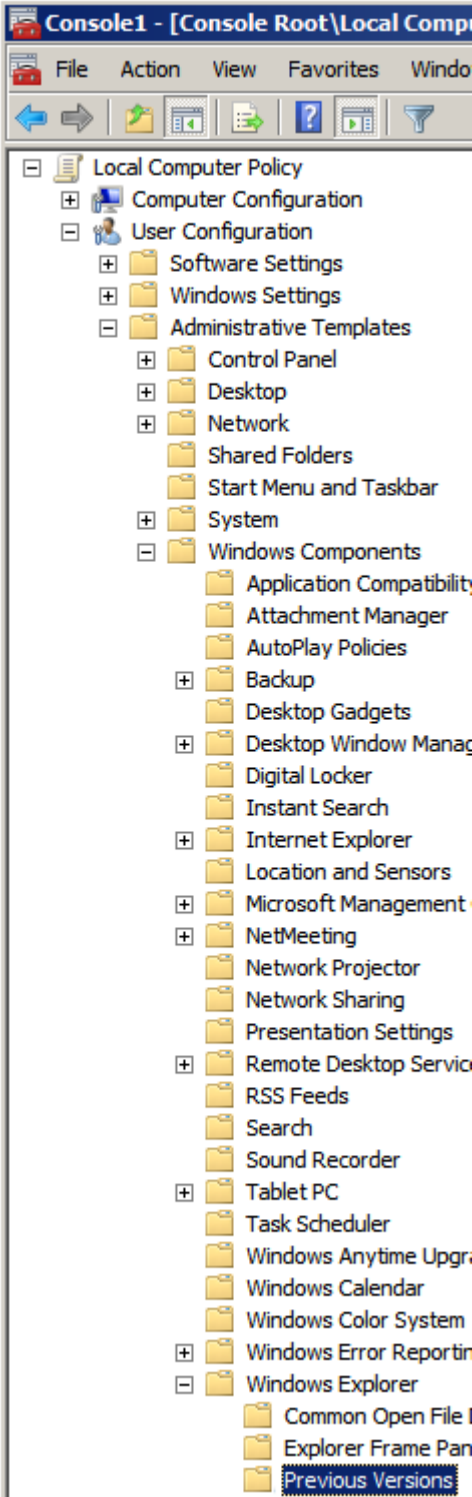
### 4.14 Refuse access to restore option

Process	Action										
2. Policy	<p>Change the setting of the policy "Prevent backing up to local disks" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State ^</th> </tr> </thead> <tbody> <tr> <td> Prevent backing up to local disks</td> <td>Enabled</td> </tr> <tr> <td> Prevent backing up to network location</td> <td>Not configured</td> </tr> <tr> <td> Prevent backing up to optical media (CD/DVD)</td> <td>Not configured</td> </tr> <tr> <td> Turn off the ability to back up data files</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State ^	Prevent backing up to local disks	Enabled	Prevent backing up to network location	Not configured	Prevent backing up to optical media (CD/DVD)	Not configured	Turn off the ability to back up data files	Not configured
Setting	State ^										
Prevent backing up to local disks	Enabled										
Prevent backing up to network location	Not configured										
Prevent backing up to optical media (CD/DVD)	Not configured										
Turn off the ability to back up data files	Not configured										
3. Policy	<p>Change the setting of the policy "Prevent backing up to network location" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State ^</th> </tr> </thead> <tbody> <tr> <td> Prevent backing up to network location</td> <td>Enabled</td> </tr> <tr> <td> Prevent backing up to optical media (CD/DVD)</td> <td>Not configured</td> </tr> <tr> <td> Turn off the ability to back up data files</td> <td>Not configured</td> </tr> <tr> <td> Turn off restore functionality</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State ^	Prevent backing up to network location	Enabled	Prevent backing up to optical media (CD/DVD)	Not configured	Turn off the ability to back up data files	Not configured	Turn off restore functionality	Not configured
Setting	State ^										
Prevent backing up to network location	Enabled										
Prevent backing up to optical media (CD/DVD)	Not configured										
Turn off the ability to back up data files	Not configured										
Turn off restore functionality	Not configured										
4. Policy	<p>Change the setting of the policy "Turn off the ability to back up data files" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State ^</th> </tr> </thead> <tbody> <tr> <td> Turn off the ability to back up data files</td> <td>Enabled</td> </tr> <tr> <td> Prevent the user from running the Backup Status ...</td> <td>Not configured</td> </tr> <tr> <td> Prevent backing up to local disks</td> <td>Not configured</td> </tr> <tr> <td> Prevent backing up to network location</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State ^	Turn off the ability to back up data files	Enabled	Prevent the user from running the Backup Status ...	Not configured	Prevent backing up to local disks	Not configured	Prevent backing up to network location	Not configured
Setting	State ^										
Turn off the ability to back up data files	Enabled										
Prevent the user from running the Backup Status ...	Not configured										
Prevent backing up to local disks	Not configured										
Prevent backing up to network location	Not configured										
5. Policy	<p>Change the setting of the policy "Turn off restore functionality" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State ^</th> </tr> </thead> <tbody> <tr> <td> Turn off restore functionality</td> <td>Enabled</td> </tr> <tr> <td> Turn off the ability to back up data files</td> <td>Not configured</td> </tr> <tr> <td> Prevent the user from running the Backup Status ...</td> <td>Not configured</td> </tr> <tr> <td> Prevent backing up to local disks</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State ^	Turn off restore functionality	Enabled	Turn off the ability to back up data files	Not configured	Prevent the user from running the Backup Status ...	Not configured	Prevent backing up to local disks	Not configured
Setting	State ^										
Turn off restore functionality	Enabled										
Turn off the ability to back up data files	Not configured										
Prevent the user from running the Backup Status ...	Not configured										
Prevent backing up to local disks	Not configured										
6. Policy	<p>Change the setting of the policy "Turn off the ability to create a system image" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State ^</th> </tr> </thead> <tbody> <tr> <td> Turn off the ability to create a system image</td> <td>Enabled</td> </tr> <tr> <td> Turn off restore functionality</td> <td>Not configured</td> </tr> <tr> <td> Turn off the ability to back up data files</td> <td>Not configured</td> </tr> <tr> <td> Prevent the user from running the Backup Status ...</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State ^	Turn off the ability to create a system image	Enabled	Turn off restore functionality	Not configured	Turn off the ability to back up data files	Not configured	Prevent the user from running the Backup Status ...	Not configured
Setting	State ^										
Turn off the ability to create a system image	Enabled										
Turn off restore functionality	Not configured										
Turn off the ability to back up data files	Not configured										
Prevent the user from running the Backup Status ...	Not configured										

## 4 Security Settings for IPCs without Network Access

### 4.14 Refuse access to restore option

Table 4-18

Process	Action
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Windows Explorer &gt; Previous Versions”</p> 

4.15 Refusing access to paths when searching

Process	Action										
1. Policy	<p>Change the setting of the policy "Prevent restoring previous versions from backups" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent restoring previous versions from backups</td> <td>Enabled</td> </tr> <tr> <td>Prevent restoring local previous versions</td> <td>Not configured</td> </tr> <tr> <td>Hide previous versions of files on backup location</td> <td>Not configured</td> </tr> <tr> <td>Hide previous versions list for remote files</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prevent restoring previous versions from backups	Enabled	Prevent restoring local previous versions	Not configured	Hide previous versions of files on backup location	Not configured	Hide previous versions list for remote files	Not configured
Setting	State										
Prevent restoring previous versions from backups	Enabled										
Prevent restoring local previous versions	Not configured										
Hide previous versions of files on backup location	Not configured										
Hide previous versions list for remote files	Not configured										
2. Policy	<p>Change the setting of the policy "Hide previous versions list for local files" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Hide previous versions list for local files</td> <td>Enabled</td> </tr> <tr> <td>Prevent restoring remote previous versions</td> <td>Not configured</td> </tr> <tr> <td>Prevent restoring local previous versions</td> <td>Not configured</td> </tr> <tr> <td>Hide previous versions of files on backup location</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Hide previous versions list for local files	Enabled	Prevent restoring remote previous versions	Not configured	Prevent restoring local previous versions	Not configured	Hide previous versions of files on backup location	Not configured
Setting	State										
Hide previous versions list for local files	Enabled										
Prevent restoring remote previous versions	Not configured										
Prevent restoring local previous versions	Not configured										
Hide previous versions of files on backup location	Not configured										
3. Policy	<p>Change the setting of the policy "Prevent restoring local previous versions" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent restoring local previous versions</td> <td>Enabled</td> </tr> <tr> <td>Hide previous versions list for local files</td> <td>Not configured</td> </tr> <tr> <td>Prevent restoring remote previous versions</td> <td>Not configured</td> </tr> <tr> <td>Hide previous versions of files on backup location</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prevent restoring local previous versions	Enabled	Hide previous versions list for local files	Not configured	Prevent restoring remote previous versions	Not configured	Hide previous versions of files on backup location	Not configured
Setting	State										
Prevent restoring local previous versions	Enabled										
Hide previous versions list for local files	Not configured										
Prevent restoring remote previous versions	Not configured										
Hide previous versions of files on backup location	Not configured										

## 4.15 Refusing access to paths when searching

**Risk:** Undesired access to applications

**Weak point:** Access paths when searching

**Solution:** Refusing access to paths when searching

### Explaining the function

To refuse access to system paths (for example C:\Windows\system32), it can be explicitly determined which paths to exempt from the search.

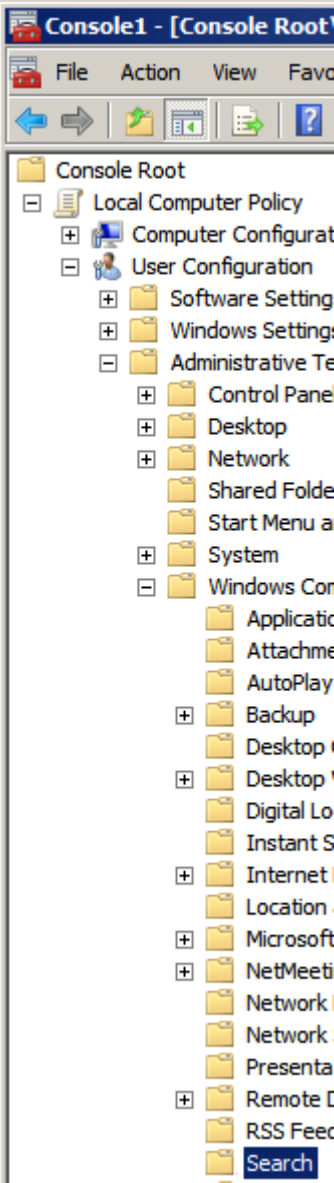
Unfortunately, this setting is made in Computer Configuration. Therefore, this policy applies for the administrator account as well as the restricted user accounts.

## 4 Security Settings for IPCs without Network Access

### 4.15 Refusing access to paths when searching

#### Adaptation of the required settings

Table 4-19

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Search”</p> 										
1. Policy	<p>Change the setting of the policy “Prevent indexing certain paths” to “Enabled”.</p> <table border="1" data-bbox="539 1753 1361 1939"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent indexing certain paths</td> <td>Enabled</td> </tr> <tr> <td>Default excluded paths</td> <td>Not configured</td> </tr> <tr> <td>Default indexed paths</td> <td>Not configured</td> </tr> <tr> <td>Prevent adding UNC locations to index from Contr...</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prevent indexing certain paths	Enabled	Default excluded paths	Not configured	Default indexed paths	Not configured	Prevent adding UNC locations to index from Contr...	Not configured
Setting	State										
Prevent indexing certain paths	Enabled										
Default excluded paths	Not configured										
Default indexed paths	Not configured										
Prevent adding UNC locations to index from Contr...	Not configured										

## 4.16 Prevent access to certain or all drives

**Risk:** Unauthorized access to system-relevant information, manipulation option

**Weak point:** Installations from removable storage medium

**Solution:** Restricting access to network and certain drives

### Explaining the function

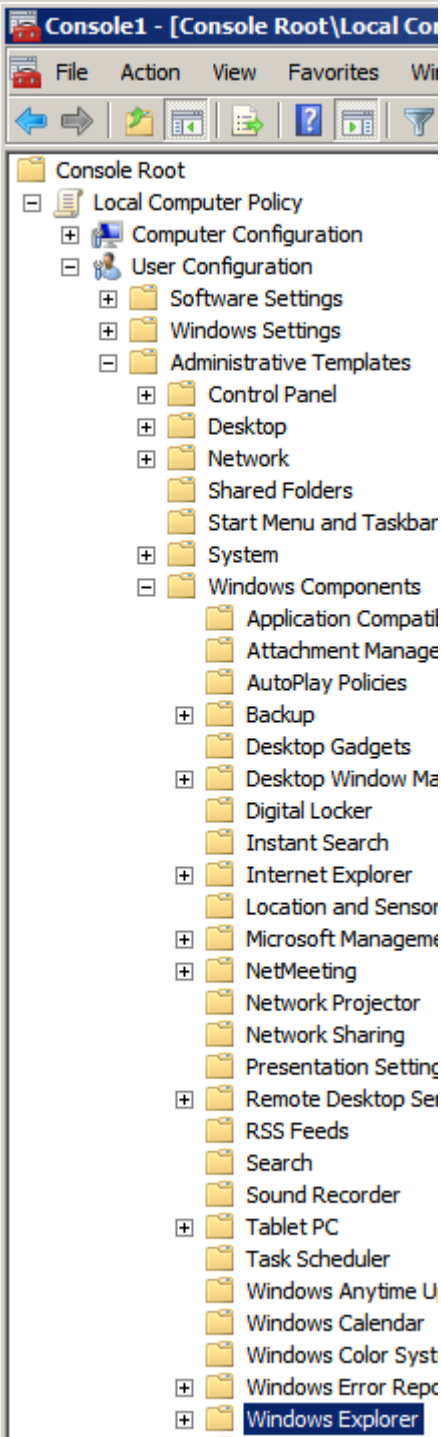
It is possible to restrict access to drives to prevent manipulation options.

## 4 Security Settings for IPCs without Network Access

### 4.16 Prevent access to certain or all drives

#### Adaptation of the required settings

Table 4-20

Process	Action
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Windows Explorer”</p> 

## 4 Security Settings for IPCs without Network Access

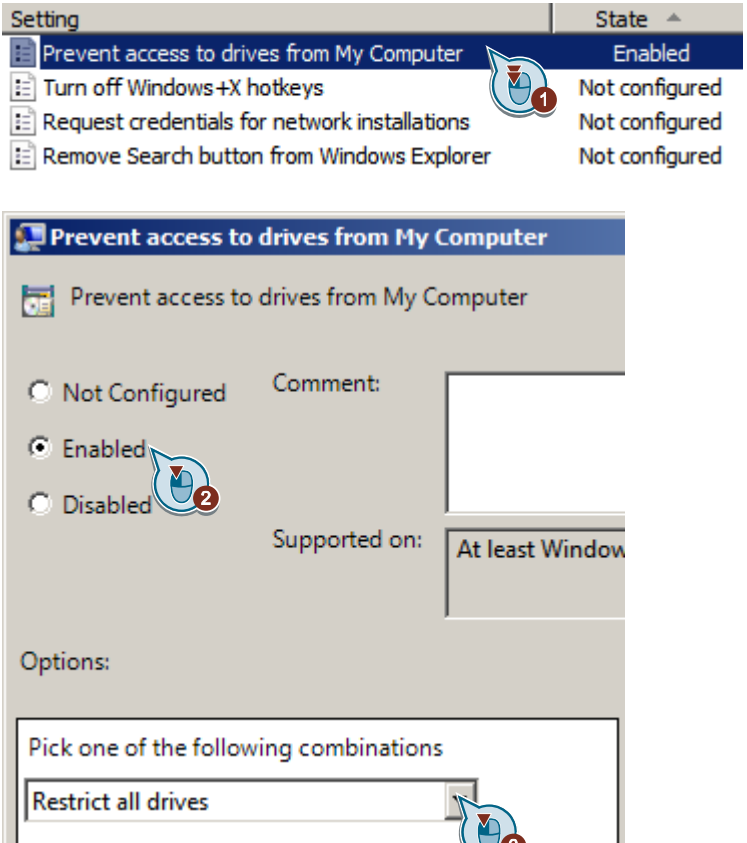
### 4.16 Prevent access to certain or all drives

Process	Action										
1. Policy	<p>Change the setting of the policy "Request credentials for network installations" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State ^</th> </tr> </thead> <tbody> <tr> <td> Request credentials for network installations</td> <td>Enabled</td> </tr> <tr> <td> Allow only per user or approved shell extensions</td> <td>Not configured</td> </tr> <tr> <td> Disable binding directly to IPropertySetStorage wi...</td> <td>Not configured</td> </tr> <tr> <td> Disable Known Folders</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State ^	Request credentials for network installations	Enabled	Allow only per user or approved shell extensions	Not configured	Disable binding directly to IPropertySetStorage wi...	Not configured	Disable Known Folders	Not configured
Setting	State ^										
Request credentials for network installations	Enabled										
Allow only per user or approved shell extensions	Not configured										
Disable binding directly to IPropertySetStorage wi...	Not configured										
Disable Known Folders	Not configured										
2. Policy	<p>Change the setting of the policy "Remove Search button from Windows Explorer" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State ^</th> </tr> </thead> <tbody> <tr> <td> Remove Search button from Windows Explorer</td> <td>Enabled</td> </tr> <tr> <td> Allow only per user or approved shell extensions</td> <td>Not configured</td> </tr> <tr> <td> Disable binding directly to IPropertySetStorage wi...</td> <td>Not configured</td> </tr> <tr> <td> Disable Known Folders</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State ^	Remove Search button from Windows Explorer	Enabled	Allow only per user or approved shell extensions	Not configured	Disable binding directly to IPropertySetStorage wi...	Not configured	Disable Known Folders	Not configured
Setting	State ^										
Remove Search button from Windows Explorer	Enabled										
Allow only per user or approved shell extensions	Not configured										
Disable binding directly to IPropertySetStorage wi...	Not configured										
Disable Known Folders	Not configured										
3. Policy	<p>Change the setting of the policy "No Entire Network in Network Locations" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State ^</th> </tr> </thead> <tbody> <tr> <td> No Entire Network in Network Locations</td> <td>Enabled</td> </tr> <tr> <td> Turn off Windows+X hotkeys</td> <td>Not configured</td> </tr> <tr> <td> Request credentials for network installations</td> <td>Not configured</td> </tr> <tr> <td> Remove Search button from Windows Explorer</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State ^	No Entire Network in Network Locations	Enabled	Turn off Windows+X hotkeys	Not configured	Request credentials for network installations	Not configured	Remove Search button from Windows Explorer	Not configured
Setting	State ^										
No Entire Network in Network Locations	Enabled										
Turn off Windows+X hotkeys	Not configured										
Request credentials for network installations	Not configured										
Remove Search button from Windows Explorer	Not configured										
4. Policy	<p>Change the setting of the policy "Turn off Windows+X hotkeys" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State ^</th> </tr> </thead> <tbody> <tr> <td> Turn off Windows+X hotkeys</td> <td>Enabled</td> </tr> <tr> <td> Allow only per user or approved shell extensions</td> <td>Not configured</td> </tr> <tr> <td> Disable binding directly to IPropertySetStorage wi...</td> <td>Not configured</td> </tr> <tr> <td> Disable Known Folders</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State ^	Turn off Windows+X hotkeys	Enabled	Allow only per user or approved shell extensions	Not configured	Disable binding directly to IPropertySetStorage wi...	Not configured	Disable Known Folders	Not configured
Setting	State ^										
Turn off Windows+X hotkeys	Enabled										
Allow only per user or approved shell extensions	Not configured										
Disable binding directly to IPropertySetStorage wi...	Not configured										
Disable Known Folders	Not configured										



## 4 Security Settings for IPCs without Network Access

### 4.16 Prevent access to certain or all drives

Process	Action										
5. Policy	<p>Change the setting of the policy "Prevent access to drives from My Computer" to "Enabled" and select the dropdown list entry "Restrict all drives"</p>  <table border="1"><thead><tr><th>Setting</th><th>State</th></tr></thead><tbody><tr><td>Prevent access to drives from My Computer</td><td>Enabled</td></tr><tr><td>Turn off Windows+X hotkeys</td><td>Not configured</td></tr><tr><td>Request credentials for network installations</td><td>Not configured</td></tr><tr><td>Remove Search button from Windows Explorer</td><td>Not configured</td></tr></tbody></table> <p><b>Prevent access to drives from My Computer</b></p> <p>Prevent access to drives from My Computer</p> <p><input type="radio"/> Not Configured    Comment:</p> <p><input checked="" type="radio"/> Enabled</p> <p><input type="radio"/> Disabled</p> <p>Supported on: At least Window</p> <p>Options:</p> <p>Pick one of the following combinations</p> <p>Restrict all drives</p>	Setting	State	Prevent access to drives from My Computer	Enabled	Turn off Windows+X hotkeys	Not configured	Request credentials for network installations	Not configured	Remove Search button from Windows Explorer	Not configured
Setting	State										
Prevent access to drives from My Computer	Enabled										
Turn off Windows+X hotkeys	Not configured										
Request credentials for network installations	Not configured										
Remove Search button from Windows Explorer	Not configured										

# 5 Security Settings for IPCs with Network Access

In addition to the settings described in the previous chapters, there are further risks for computers with network access.

This chapter lists settings which apply for this application scenario

## 5.1 Activating and configuring Windows firewall

**Risk:** Sensitive process data can be viewed

**Weak point:** Windows firewall switched off / not configured

**Solution:** Activating and configuring Windows firewall

### Explaining the function

It is urgently recommended to have the Windows firewall activated! The standard configuration is configured in a meaningful way.

If Siemens software requires additional settings, these are configured during the installation (for example during the installation of SIMATIC NET).

During commissioning it may make sense to permit the ping request temporarily.

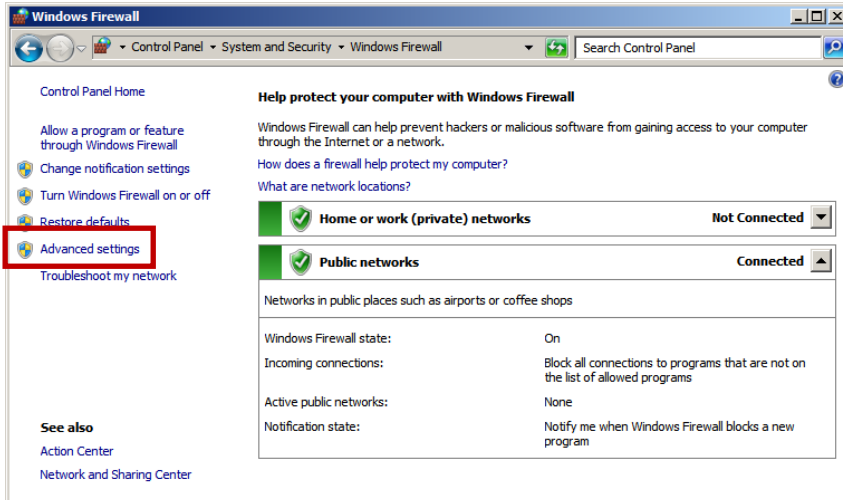
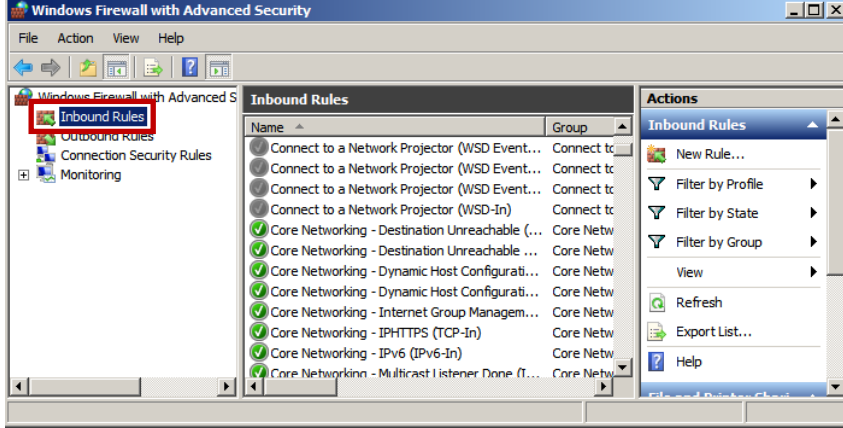
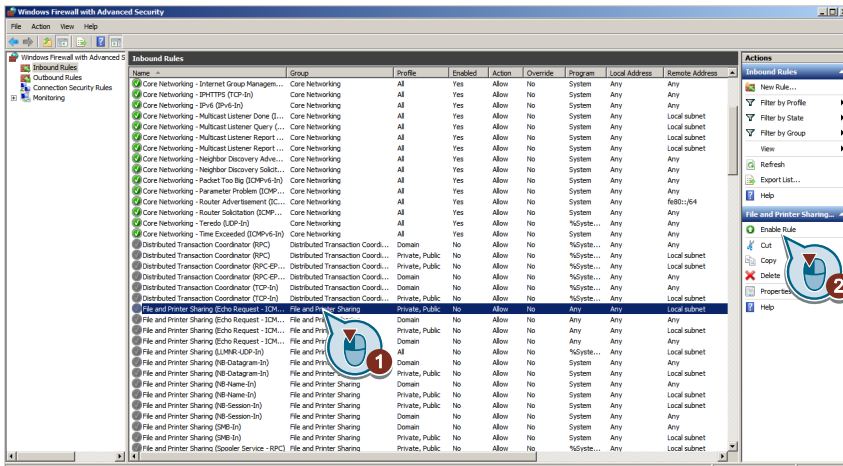
### Adaptation of the required settings

Table 5-1

Process	Action
1.	<p>Open the “Windows Firewall with extended security” via “Start &gt; Control Panel &gt; System and Security &gt; Windows Firewall”</p>  <p>The screenshot shows the Windows Control Panel window titled 'System and Security'. The left-hand navigation pane lists various system settings, with 'System and Security' selected. The main content area displays several system categories: Action Center, Windows Firewall (highlighted with a red rectangular box), System, Windows Update, Power Options, Backup and Restore, BitLocker Drive Encryption, and Administrative Tools. Each category includes a brief description and links to related settings.</p>

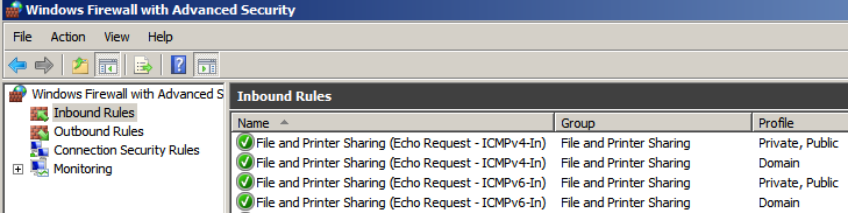
## 5 Security Settings for IPCs with Network Access

### 5.1 Activating and configuring Windows firewall

Process	Action
2.	<p>Click on the menu entry "Advanced settings".</p> 
3.	<p>Select the "Inbound Rules" entry.</p> 
4.	<p>Select the "File and Printer Sharing (Echo Request ICMPv4 incoming)" -&gt; Profile "Private, Public" and activate the rule via the "Activate rule" action</p> 

## 5 Security Settings for IPCs with Network Access

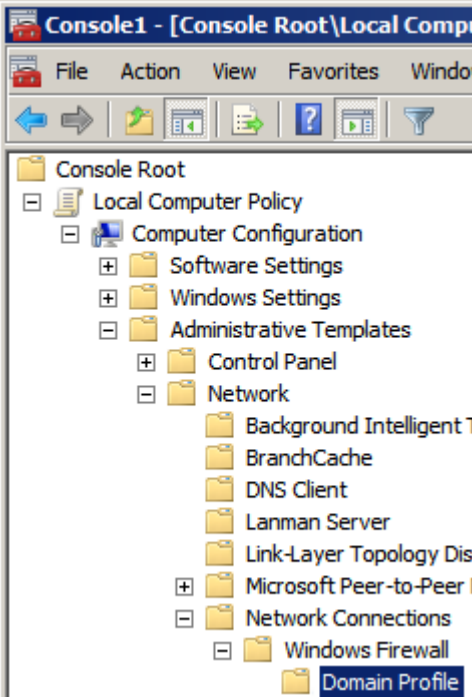
### 5.1 Activating and configuring Windows firewall

Process	Action															
5.	<p>Repeat step 4 for the entries:</p> <ul style="list-style-type: none"><li>• File and Printer Sharing (Echo Request ICMPv4 incoming -&gt; Profile "Domain")</li><li>• File and Printer Sharing (Echo Request -ICMPv6 incoming -&gt; Profile "Private, Public")</li><li>• File and Printer Sharing (Echo Request ICMPv6 incoming -&gt; Profile "Domain")</li></ul>  <p>The screenshot shows the Windows Firewall with Advanced Security console. The 'Inbound Rules' list is expanded, showing four rules with green checkmarks, indicating they are active. The rules are:</p> <table border="1"><thead><tr><th>Name</th><th>Group</th><th>Profile</th></tr></thead><tbody><tr><td>File and Printer Sharing (Echo Request - ICMPv4-In)</td><td>File and Printer Sharing</td><td>Private, Public, Domain</td></tr><tr><td>File and Printer Sharing (Echo Request - ICMPv4-In)</td><td>File and Printer Sharing</td><td>Domain</td></tr><tr><td>File and Printer Sharing (Echo Request - ICMPv6-In)</td><td>File and Printer Sharing</td><td>Private, Public, Domain</td></tr><tr><td>File and Printer Sharing (Echo Request - ICMPv6-In)</td><td>File and Printer Sharing</td><td>Domain</td></tr></tbody></table>	Name	Group	Profile	File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private, Public, Domain	File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private, Public, Domain	File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain
Name	Group	Profile														
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private, Public, Domain														
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain														
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private, Public, Domain														
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain														

#### Note

For some Windows installations, these settings are grayed and the administrator cannot change them. If this is the case, the respective group policy (see [Table 5-2](#)) must be activated.

Table 5-2

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “Computer Configuration &gt; Administrative Templates &gt; Network &gt; Network Connections &gt; Windows Firewall &gt; Domain Profile”</p> 										
1. Policy	<p>Change the settings of the policy “Windows Firewall: Allow ICMP exceptions” to “Enabled” and select the option “Allow incoming Echo Requests”.</p> <table border="1" data-bbox="539 1227 1356 1377"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Windows Firewall: Allow ICMP exceptions</td> <td>Enabled</td> </tr> <tr> <td>Windows Firewall: Allow logging</td> <td>Not configured</td> </tr> <tr> <td>Windows Firewall: Prohibit notifications</td> <td>Not configured</td> </tr> <tr> <td>Windows Firewall: Allow local port exceptions</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Windows Firewall: Allow ICMP exceptions	Enabled	Windows Firewall: Allow logging	Not configured	Windows Firewall: Prohibit notifications	Not configured	Windows Firewall: Allow local port exceptions	Not configured
Setting	State										
Windows Firewall: Allow ICMP exceptions	Enabled										
Windows Firewall: Allow logging	Not configured										
Windows Firewall: Prohibit notifications	Not configured										
Windows Firewall: Allow local port exceptions	Not configured										

© Siemens AG 2015. All rights reserved

## 5.2 Configuring password guidelines correctly

**Risk:** Attacks by hackers through online scanner, unauthorized access

**Weak point:** Using standard passwords

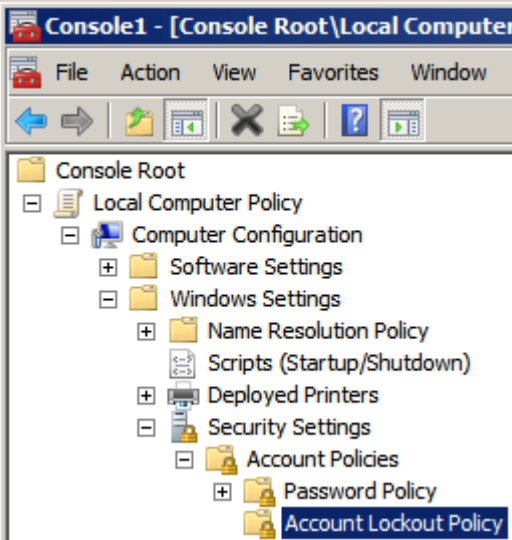
**Solution:** Configuring password guidelines correctly

### Explaining the function

The configuration of the Password Policy “forces” the user to meet the respective rules for assigning his password and hence counters misuse.

**Adaptation of the required settings**

Table 5-3

Process	Action
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Local Policies &gt; Password Policy”</p> 
2. Policy	<p>Change the settings recommended for IPCs to the account policies using the following table.</p>

5.3 Refusing access to network connections

Table 5-4

Policy	Security setting	
	Default value: Domain controller / independent server	Recommended settings
Password must meet the complexity requirements	Activated / Deactivated	Enabled
Force password chronic	24 / 0 saved passwords	0
Save passwords with reversible encoding	Deactivated	Deactivated
Maximum password age	42	0
Minimum password length	7 / 0 characters	8
Minimum password age	1 / 0 days	0

### 5.3 Refusing access to network connections

**Risk:** Unauthorized changes of LAN connections, unauthorized removing/adding of components

**Weak point:** Free access to network connections

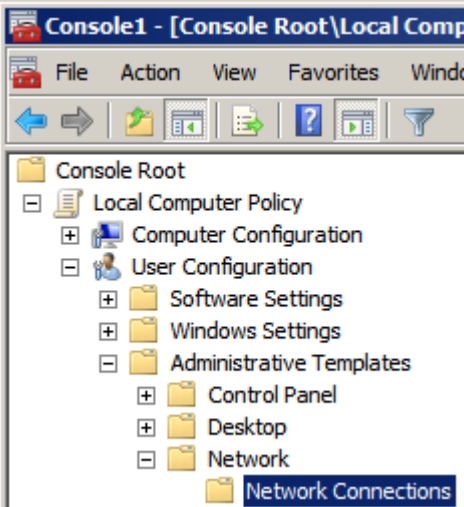
**Solution:** Refusing access to network connections

#### Explaining the function

Refusing access to network connections restricts the possibilities for undesired installation of malware on the IPC.

**Adaptation of the required settings**

Table 5-5

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; Network &gt; Network Connections”</p> 										
1. Policy	<p>Change the setting of the policy “Prohibit Enabling/Disabling components of a LAN connection” to “Enabled”</p> <table border="1" data-bbox="539 1086 1361 1243"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit Enabling/Disabling components of a LAN connection</td> <td>Enabled</td> </tr> <tr> <td>Prohibit renaming private remote access connections</td> <td>Not configured</td> </tr> <tr> <td>Prohibit TCP/IP advanced configuration</td> <td>Not configured</td> </tr> <tr> <td>Prohibit viewing of status for an active connection</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit Enabling/Disabling components of a LAN connection	Enabled	Prohibit renaming private remote access connections	Not configured	Prohibit TCP/IP advanced configuration	Not configured	Prohibit viewing of status for an active connection	Not configured
Setting	State										
Prohibit Enabling/Disabling components of a LAN connection	Enabled										
Prohibit renaming private remote access connections	Not configured										
Prohibit TCP/IP advanced configuration	Not configured										
Prohibit viewing of status for an active connection	Not configured										
2. Policy	<p>Change the setting of the policy “Prohibit adding and removing components for a LAN or remote access connection” to “Enabled”</p> <table border="1" data-bbox="539 1310 1361 1456"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit adding and removing components for a LAN or remote access connection</td> <td>Enabled</td> </tr> <tr> <td>Prohibit changing properties of a private remote access connection</td> <td>Not configured</td> </tr> <tr> <td>Prohibit connecting and disconnecting a remote access connection</td> <td>Not configured</td> </tr> <tr> <td>Prohibit deletion of remote access connections</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit adding and removing components for a LAN or remote access connection	Enabled	Prohibit changing properties of a private remote access connection	Not configured	Prohibit connecting and disconnecting a remote access connection	Not configured	Prohibit deletion of remote access connections	Not configured
Setting	State										
Prohibit adding and removing components for a LAN or remote access connection	Enabled										
Prohibit changing properties of a private remote access connection	Not configured										
Prohibit connecting and disconnecting a remote access connection	Not configured										
Prohibit deletion of remote access connections	Not configured										
3. Policy	<p>Change the setting of the policy “Prohibit TCP/IP advanced configuration” to “Enabled”</p> <table border="1" data-bbox="539 1523 1361 1691"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit TCP/IP advanced configuration</td> <td>Enabled</td> </tr> <tr> <td>Prohibit Enabling/Disabling components of a LAN connection</td> <td>Not configured</td> </tr> <tr> <td>Ability to delete all user remote access connections</td> <td>Not configured</td> </tr> <tr> <td>Prohibit deletion of remote access connections</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit TCP/IP advanced configuration	Enabled	Prohibit Enabling/Disabling components of a LAN connection	Not configured	Ability to delete all user remote access connections	Not configured	Prohibit deletion of remote access connections	Not configured
Setting	State										
Prohibit TCP/IP advanced configuration	Enabled										
Prohibit Enabling/Disabling components of a LAN connection	Not configured										
Ability to delete all user remote access connections	Not configured										
Prohibit deletion of remote access connections	Not configured										
4. Policy	<p>Change the setting of the policy “Prohibit access to New Connection Wizard” to “Enabled”</p> <table border="1" data-bbox="539 1758 1361 1915"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit access to the New Connection Wizard</td> <td>Enabled</td> </tr> <tr> <td>Prohibit access to the Remote Access Preferences item on the A...</td> <td>Not configured</td> </tr> <tr> <td>Prohibit adding and removing components for a LAN or remote a...</td> <td>Not configured</td> </tr> <tr> <td>Prohibit changing properties of a private remote access connection</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit access to the New Connection Wizard	Enabled	Prohibit access to the Remote Access Preferences item on the A...	Not configured	Prohibit adding and removing components for a LAN or remote a...	Not configured	Prohibit changing properties of a private remote access connection	Not configured
Setting	State										
Prohibit access to the New Connection Wizard	Enabled										
Prohibit access to the Remote Access Preferences item on the A...	Not configured										
Prohibit adding and removing components for a LAN or remote a...	Not configured										
Prohibit changing properties of a private remote access connection	Not configured										



5.4 Restricting internet access

Process	Action										
5. Policy	<p>Change the setting of the policy “Prohibit access to properties of a LAN connection” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit access to properties of a LAN connection</td> <td>Enabled</td> </tr> <tr> <td>Prohibit access to properties of components of a LAN connection</td> <td>Not configured</td> </tr> <tr> <td>Prohibit access to properties of components of a remote access ...</td> <td>Not configured</td> </tr> <tr> <td>Prohibit access to the Advanced Settings item on the Advanced ...</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit access to properties of a LAN connection	Enabled	Prohibit access to properties of components of a LAN connection	Not configured	Prohibit access to properties of components of a remote access ...	Not configured	Prohibit access to the Advanced Settings item on the Advanced ...	Not configured
Setting	State										
Prohibit access to properties of a LAN connection	Enabled										
Prohibit access to properties of components of a LAN connection	Not configured										
Prohibit access to properties of components of a remote access ...	Not configured										
Prohibit access to the Advanced Settings item on the Advanced ...	Not configured										
6. Policy	<p>Change the setting of the policy “Prohibit access to properties of components of a LAN connection” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit access to properties of components of a LAN connection</td> <td>Enabled</td> </tr> <tr> <td>Prohibit access to properties of components of a remote access ...</td> <td>Not configured</td> </tr> <tr> <td>Prohibit access to the Advanced Settings item on the Advanced ...</td> <td>Not configured</td> </tr> <tr> <td>Prohibit access to the New Connection Wizard</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit access to properties of components of a LAN connection	Enabled	Prohibit access to properties of components of a remote access ...	Not configured	Prohibit access to the Advanced Settings item on the Advanced ...	Not configured	Prohibit access to the New Connection Wizard	Not configured
Setting	State										
Prohibit access to properties of components of a LAN connection	Enabled										
Prohibit access to properties of components of a remote access ...	Not configured										
Prohibit access to the Advanced Settings item on the Advanced ...	Not configured										
Prohibit access to the New Connection Wizard	Not configured										
7. < Policy	<p>Change the setting of the policy “Prohibit access to properties of components of a remote access connection” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit access to properties of components of a remote access connection</td> <td>Enabled</td> </tr> <tr> <td>Prohibit access to the Advanced Settings item on the Advanced menu</td> <td>Not configured</td> </tr> <tr> <td>Prohibit access to the New Connection Wizard</td> <td>Not configured</td> </tr> <tr> <td>Prohibit access to the Remote Access Preferences item on the Advanced ...</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit access to properties of components of a remote access connection	Enabled	Prohibit access to the Advanced Settings item on the Advanced menu	Not configured	Prohibit access to the New Connection Wizard	Not configured	Prohibit access to the Remote Access Preferences item on the Advanced ...	Not configured
Setting	State										
Prohibit access to properties of components of a remote access connection	Enabled										
Prohibit access to the Advanced Settings item on the Advanced menu	Not configured										
Prohibit access to the New Connection Wizard	Not configured										
Prohibit access to the Remote Access Preferences item on the Advanced ...	Not configured										
8. Policy	<p>Change the setting of the policy “Prohibit access to the Advanced Settings item on the Advanced menu” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prohibit access to the Advanced Settings item on the Advanced menu</td> <td>Enabled</td> </tr> <tr> <td>Prohibit access to the New Connection Wizard</td> <td>Not configured</td> </tr> <tr> <td>Prohibit access to the Remote Access Preferences item on the Advanced ...</td> <td>Not configured</td> </tr> <tr> <td>Prohibit adding and removing components for a LAN or remote access con...</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prohibit access to the Advanced Settings item on the Advanced menu	Enabled	Prohibit access to the New Connection Wizard	Not configured	Prohibit access to the Remote Access Preferences item on the Advanced ...	Not configured	Prohibit adding and removing components for a LAN or remote access con...	Not configured
Setting	State										
Prohibit access to the Advanced Settings item on the Advanced menu	Enabled										
Prohibit access to the New Connection Wizard	Not configured										
Prohibit access to the Remote Access Preferences item on the Advanced ...	Not configured										
Prohibit adding and removing components for a LAN or remote access con...	Not configured										

© Siemens AG 2015. All rights reserved

## 5.4 Restricting internet access

**Risk:** Free access to the internet

**Weak point:** Free on access to internet communication management

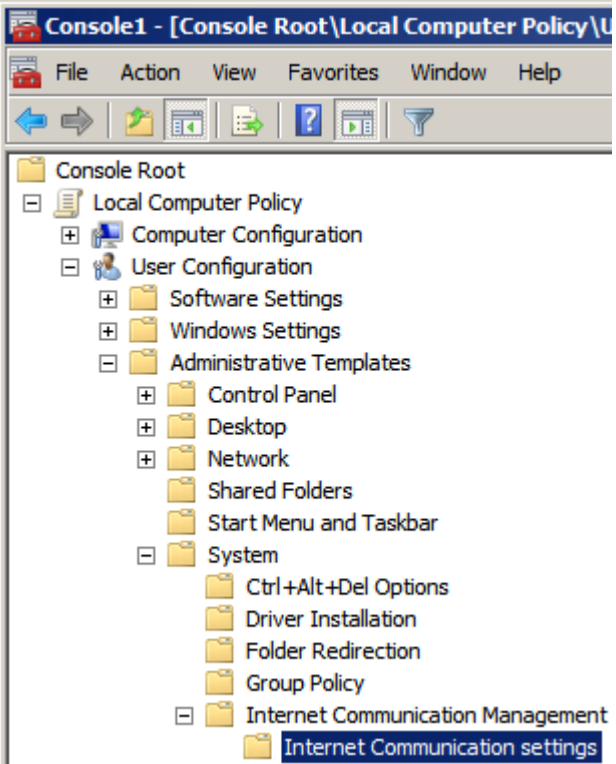
**Solution:** Restricting internet access

### Explaining the function

Refusing internet access restricts the possibilities for undesired installation of malware on the IPC.

**Adaptation of the required settings**

Table 5-6

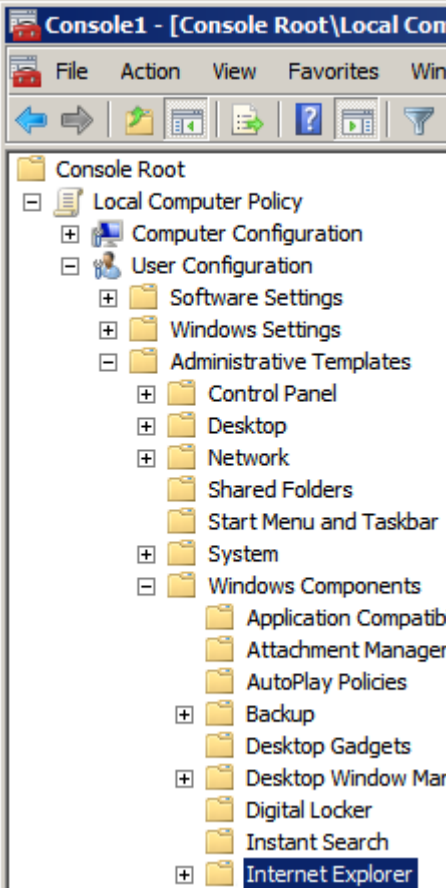
Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; System &gt; Internet Communication Management &gt; Internet Communication settings”</p> 										
1. Policy	<p>Change the setting of the policy “Turn off the “Order Prints” picture task” to “Enabled”</p> <table border="1" data-bbox="539 1339 1361 1482"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off the "Order Prints" picture task</td> <td>Enabled</td> </tr> <tr> <td>Turn off the "Publish to Web" task for files and folders</td> <td>Not configured</td> </tr> <tr> <td>Turn off the Windows Messenger Customer Experience Improvement Pro...</td> <td>Not configured</td> </tr> <tr> <td>Turn off Windows Online</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off the "Order Prints" picture task	Enabled	Turn off the "Publish to Web" task for files and folders	Not configured	Turn off the Windows Messenger Customer Experience Improvement Pro...	Not configured	Turn off Windows Online	Not configured
Setting	State										
Turn off the "Order Prints" picture task	Enabled										
Turn off the "Publish to Web" task for files and folders	Not configured										
Turn off the Windows Messenger Customer Experience Improvement Pro...	Not configured										
Turn off Windows Online	Not configured										
2. Policy	<p>Change the setting of the policy “Turn off the ability to back up data files” to “Enabled”</p> <table border="1" data-bbox="539 1556 1361 1700"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off the "Publish to Web" task for files and folders</td> <td>Enabled</td> </tr> <tr> <td>Turn off downloading of print drivers over HTTP</td> <td>Not configured</td> </tr> <tr> <td>Turn off handwriting personalization data sharing</td> <td>Not configured</td> </tr> <tr> <td>Turn off handwriting recognition error reporting</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off the "Publish to Web" task for files and folders	Enabled	Turn off downloading of print drivers over HTTP	Not configured	Turn off handwriting personalization data sharing	Not configured	Turn off handwriting recognition error reporting	Not configured
Setting	State										
Turn off the "Publish to Web" task for files and folders	Enabled										
Turn off downloading of print drivers over HTTP	Not configured										
Turn off handwriting personalization data sharing	Not configured										
Turn off handwriting recognition error reporting	Not configured										
3. Policy	<p>Change the setting of the policy “Turn off Internet File Association service” to “Enabled”</p> <table border="1" data-bbox="539 1774 1361 1917"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off Internet File Association service</td> <td>Enabled</td> </tr> <tr> <td>Turn off printing over HTTP</td> <td>Not configured</td> </tr> <tr> <td>Turn off the "Order Prints" picture task</td> <td>Not configured</td> </tr> <tr> <td>Turn off the "Publish to Web" task for files and folders</td> <td>Enabled</td> </tr> </tbody> </table>	Setting	State	Turn off Internet File Association service	Enabled	Turn off printing over HTTP	Not configured	Turn off the "Order Prints" picture task	Not configured	Turn off the "Publish to Web" task for files and folders	Enabled
Setting	State										
Turn off Internet File Association service	Enabled										
Turn off printing over HTTP	Not configured										
Turn off the "Order Prints" picture task	Not configured										
Turn off the "Publish to Web" task for files and folders	Enabled										

## 5 Security Settings for IPCs with Network Access

### 5.4 Restricting internet access

Process	Action										
4. Policy	<p>Change the setting of the policy "Turn off Windows Messenger Customer Experience Improvement Program" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off the Windows Messenger Customer Experience Improvement Program</td> <td>Enabled</td> </tr> <tr> <td>Turn off Internet File Association service</td> <td>Not configured</td> </tr> <tr> <td>Turn off downloading of print drivers over HTTP</td> <td>Not configured</td> </tr> <tr> <td>Turn off handwriting personalization data sharing</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off the Windows Messenger Customer Experience Improvement Program	Enabled	Turn off Internet File Association service	Not configured	Turn off downloading of print drivers over HTTP	Not configured	Turn off handwriting personalization data sharing	Not configured
Setting	State										
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled										
Turn off Internet File Association service	Not configured										
Turn off downloading of print drivers over HTTP	Not configured										
Turn off handwriting personalization data sharing	Not configured										
5. Policy	<p>Change the setting of the policy "Turn off Help Experience Improvement Program" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off Help Experience Improvement Program</td> <td>Enabled</td> </tr> <tr> <td>Turn off Help Ratings</td> <td>Not configured</td> </tr> <tr> <td>Turn off Internet download for Web publishing and online ordering wizards</td> <td>Not configured</td> </tr> <tr> <td>Turn off printing over HTTP</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off Help Experience Improvement Program	Enabled	Turn off Help Ratings	Not configured	Turn off Internet download for Web publishing and online ordering wizards	Not configured	Turn off printing over HTTP	Not configured
Setting	State										
Turn off Help Experience Improvement Program	Enabled										
Turn off Help Ratings	Not configured										
Turn off Internet download for Web publishing and online ordering wizards	Not configured										
Turn off printing over HTTP	Not configured										
6. Policy	<p>Change the setting of the policy "Turn off Help Ratings" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off Help Ratings</td> <td>Enabled</td> </tr> <tr> <td>Turn off Internet download for Web publishing and online ordering wizards</td> <td>Not configured</td> </tr> <tr> <td>Turn off printing over HTTP</td> <td>Not configured</td> </tr> <tr> <td>Turn off the "Order Prints" picture task</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off Help Ratings	Enabled	Turn off Internet download for Web publishing and online ordering wizards	Not configured	Turn off printing over HTTP	Not configured	Turn off the "Order Prints" picture task	Not configured
Setting	State										
Turn off Help Ratings	Enabled										
Turn off Internet download for Web publishing and online ordering wizards	Not configured										
Turn off printing over HTTP	Not configured										
Turn off the "Order Prints" picture task	Not configured										
7. Policy	<p>Change the setting of the policy "Turn off Internet download for Web publishing and online ordering wizards" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off Internet download for Web publishing and online ordering wizards</td> <td>Enabled</td> </tr> <tr> <td>Turn off printing over HTTP</td> <td>Not configured</td> </tr> <tr> <td>Turn off the "Order Prints" picture task</td> <td>Not configured</td> </tr> <tr> <td>Turn off the "Publish to Web" task for files and folders</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off Internet download for Web publishing and online ordering wizards	Enabled	Turn off printing over HTTP	Not configured	Turn off the "Order Prints" picture task	Not configured	Turn off the "Publish to Web" task for files and folders	Not configured
Setting	State										
Turn off Internet download for Web publishing and online ordering wizards	Enabled										
Turn off printing over HTTP	Not configured										
Turn off the "Order Prints" picture task	Not configured										
Turn off the "Publish to Web" task for files and folders	Not configured										
8. Policy	<p>Change the setting of the policy "Turn off Windows Online" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off Windows Online</td> <td>Enabled</td> </tr> <tr> <td>Turn off the Windows Messenger Customer Experience Improvement Program</td> <td>Not configured</td> </tr> <tr> <td>Turn off Internet download for Web publishing and online ordering wizards</td> <td>Not configured</td> </tr> <tr> <td>Turn off Internet File Association service</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off Windows Online	Enabled	Turn off the Windows Messenger Customer Experience Improvement Program	Not configured	Turn off Internet download for Web publishing and online ordering wizards	Not configured	Turn off Internet File Association service	Not configured
Setting	State										
Turn off Windows Online	Enabled										
Turn off the Windows Messenger Customer Experience Improvement Program	Not configured										
Turn off Internet download for Web publishing and online ordering wizards	Not configured										
Turn off Internet File Association service	Not configured										

Table 5-7

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Internet Explorer”</p> 										
1. Policy	<p>Change the setting of the policy “Search: Disable Search Customization” to “Enabled”</p> <table border="1" data-bbox="539 1422 1361 1568"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Search: Disable Search Customization</td> <td>Enabled</td> </tr> <tr> <td>Set tab process growth</td> <td>Not configured</td> </tr> <tr> <td>Turn off ActiveX opt-in prompt</td> <td>Not configured</td> </tr> <tr> <td>Turn off Automatic Crash Recovery Prompt</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Search: Disable Search Customization	Enabled	Set tab process growth	Not configured	Turn off ActiveX opt-in prompt	Not configured	Turn off Automatic Crash Recovery Prompt	Not configured
Setting	State										
Search: Disable Search Customization	Enabled										
Set tab process growth	Not configured										
Turn off ActiveX opt-in prompt	Not configured										
Turn off Automatic Crash Recovery Prompt	Not configured										
2. Policy	<p>Change the setting of the policy “Search: Disable Find Files via F3 within the browser” to “Enabled”</p> <table border="1" data-bbox="539 1635 1361 1780"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Search: Disable Find Files via F3 within the browser</td> <td>Enabled</td> </tr> <tr> <td>Search: Disable Search Customization</td> <td>Not configured</td> </tr> <tr> <td>Set tab process growth</td> <td>Not configured</td> </tr> <tr> <td>Turn off ActiveX opt-in prompt</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Search: Disable Find Files via F3 within the browser	Enabled	Search: Disable Search Customization	Not configured	Set tab process growth	Not configured	Turn off ActiveX opt-in prompt	Not configured
Setting	State										
Search: Disable Find Files via F3 within the browser	Enabled										
Search: Disable Search Customization	Not configured										
Set tab process growth	Not configured										
Turn off ActiveX opt-in prompt	Not configured										
3. Policy	<p>Change the setting of the policy “Disable changing Advanced page settings” to “Enabled”</p> <table border="1" data-bbox="539 1859 1361 2002"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Disable changing Advanced page settings</td> <td>Enabled</td> </tr> <tr> <td>Disable changing Automatic Configuration settings</td> <td>Not configured</td> </tr> <tr> <td>Disable changing Calendar and Contact settings</td> <td>Not configured</td> </tr> <tr> <td>Disable changing certificate settings</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Disable changing Advanced page settings	Enabled	Disable changing Automatic Configuration settings	Not configured	Disable changing Calendar and Contact settings	Not configured	Disable changing certificate settings	Not configured
Setting	State										
Disable changing Advanced page settings	Enabled										
Disable changing Automatic Configuration settings	Not configured										
Disable changing Calendar and Contact settings	Not configured										
Disable changing certificate settings	Not configured										

## 5 Security Settings for IPCs with Network Access

### 5.4 Restricting internet access

Process	Action										
4. Policy	<p>Change the setting of the policy "Turn off pop-up management" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off pop-up management</td> <td>Enabled</td> </tr> <tr> <td>Turn off Quick Tabs functionality</td> <td>Not configured</td> </tr> <tr> <td>Turn off Reopen Last Browsing Session</td> <td>Not configured</td> </tr> <tr> <td>Turn off suggestions for all user-installed providers</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off pop-up management	Enabled	Turn off Quick Tabs functionality	Not configured	Turn off Reopen Last Browsing Session	Not configured	Turn off suggestions for all user-installed providers	Not configured
Setting	State										
Turn off pop-up management	Enabled										
Turn off Quick Tabs functionality	Not configured										
Turn off Reopen Last Browsing Session	Not configured										
Turn off suggestions for all user-installed providers	Not configured										
5. Policy	<p>Change the setting of the policy "Prevent "Fix settings" functionality" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent "Fix settings" functionality</td> <td>Enabled</td> </tr> <tr> <td>Prevent Bypassing SmartScreen Filter Warnings</td> <td>Not configured</td> </tr> <tr> <td>Prevent Internet Explorer Search box from displaying</td> <td>Not configured</td> </tr> <tr> <td>Prevent participation in the Customer Experience Improvement Program</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prevent "Fix settings" functionality	Enabled	Prevent Bypassing SmartScreen Filter Warnings	Not configured	Prevent Internet Explorer Search box from displaying	Not configured	Prevent participation in the Customer Experience Improvement Program	Not configured
Setting	State										
Prevent "Fix settings" functionality	Enabled										
Prevent Bypassing SmartScreen Filter Warnings	Not configured										
Prevent Internet Explorer Search box from displaying	Not configured										
Prevent participation in the Customer Experience Improvement Program	Not configured										
6. Policy	<p>Change the setting of the policy "Prevent performance of First Run Customize settings" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent performance of First Run Customize settings</td> <td>Enabled</td> </tr> <tr> <td>Restrict changing the default search provider</td> <td>Not configured</td> </tr> <tr> <td>Restrict search providers to a specific list of providers</td> <td>Not configured</td> </tr> <tr> <td>Search: Disable Find Files via F3 within the browser</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prevent performance of First Run Customize settings	Enabled	Restrict changing the default search provider	Not configured	Restrict search providers to a specific list of providers	Not configured	Search: Disable Find Files via F3 within the browser	Not configured
Setting	State										
Prevent performance of First Run Customize settings	Enabled										
Restrict changing the default search provider	Not configured										
Restrict search providers to a specific list of providers	Not configured										
Search: Disable Find Files via F3 within the browser	Not configured										
7. Policy	<p>Change the setting of the policy "Prevent Internet Explorer Search box from displaying" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent Internet Explorer Search box from displaying</td> <td>Enabled</td> </tr> <tr> <td>Prevent participation in the Customer Experience Improvement Program</td> <td>Not configured</td> </tr> <tr> <td>Prevent performance of First Run Customize settings</td> <td>Not configured</td> </tr> <tr> <td>Restrict changing the default search provider</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prevent Internet Explorer Search box from displaying	Enabled	Prevent participation in the Customer Experience Improvement Program	Not configured	Prevent performance of First Run Customize settings	Not configured	Restrict changing the default search provider	Not configured
Setting	State										
Prevent Internet Explorer Search box from displaying	Enabled										
Prevent participation in the Customer Experience Improvement Program	Not configured										
Prevent performance of First Run Customize settings	Not configured										
Restrict changing the default search provider	Not configured										
8. Policy	<p>Change the setting of the policy "Disable changing accessibility settings" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Disable changing accessibility settings</td> <td>Enabled</td> </tr> <tr> <td>Disable changing Advanced page settings</td> <td>Not configured</td> </tr> <tr> <td>Disable changing Automatic Configuration settings</td> <td>Not configured</td> </tr> <tr> <td>Disable changing Calendar and Contact settings</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Disable changing accessibility settings	Enabled	Disable changing Advanced page settings	Not configured	Disable changing Automatic Configuration settings	Not configured	Disable changing Calendar and Contact settings	Not configured
Setting	State										
Disable changing accessibility settings	Enabled										
Disable changing Advanced page settings	Not configured										
Disable changing Automatic Configuration settings	Not configured										
Disable changing Calendar and Contact settings	Not configured										
9. Policy	<p>Change the setting of the policy "Turn off Managing Pop-up Allow list" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off Managing Pop-up Allow list</td> <td>Enabled</td> </tr> <tr> <td>Turn off managing Pop-up filter level</td> <td>Not configured</td> </tr> <tr> <td>Turn off Managing SmartScreen Filter</td> <td>Not configured</td> </tr> <tr> <td>Turn off page zooming functionality</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off Managing Pop-up Allow list	Enabled	Turn off managing Pop-up filter level	Not configured	Turn off Managing SmartScreen Filter	Not configured	Turn off page zooming functionality	Not configured
Setting	State										
Turn off Managing Pop-up Allow list	Enabled										
Turn off managing Pop-up filter level	Not configured										
Turn off Managing SmartScreen Filter	Not configured										
Turn off page zooming functionality	Not configured										
10. Policy	<p>Change the setting of the policy "Turn off pop-up management" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off pop-up management</td> <td>Enabled</td> </tr> <tr> <td>Turn off Quick Tabs functionality</td> <td>Not configured</td> </tr> <tr> <td>Turn off Reopen Last Browsing Session</td> <td>Not configured</td> </tr> <tr> <td>Turn off suggestions for all user-installed providers</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off pop-up management	Enabled	Turn off Quick Tabs functionality	Not configured	Turn off Reopen Last Browsing Session	Not configured	Turn off suggestions for all user-installed providers	Not configured
Setting	State										
Turn off pop-up management	Enabled										
Turn off Quick Tabs functionality	Not configured										
Turn off Reopen Last Browsing Session	Not configured										
Turn off suggestions for all user-installed providers	Not configured										
11. Policy	<p>Change the setting of the policy "Disable changing proxy settings" to "Enabled"</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Disable changing proxy settings</td> <td>Enabled</td> </tr> <tr> <td>Disable changing ratings settings</td> <td>Not configured</td> </tr> <tr> <td>Disable changing secondary home page settings</td> <td>Not configured</td> </tr> <tr> <td>Disable changing Temporary Internet files settings</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Disable changing proxy settings	Enabled	Disable changing ratings settings	Not configured	Disable changing secondary home page settings	Not configured	Disable changing Temporary Internet files settings	Not configured
Setting	State										
Disable changing proxy settings	Enabled										
Disable changing ratings settings	Not configured										
Disable changing secondary home page settings	Not configured										
Disable changing Temporary Internet files settings	Not configured										

Process	Action										
12. Policy	<p>Change the setting of the policy “Prevent participation in the Customer Experience Improvement Program” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent participation in the Customer Experience Improvement Program</td> <td>Enabled</td> </tr> <tr> <td>Prevent performance of First Run Customize settings</td> <td>Not configured</td> </tr> <tr> <td>Restrict changing the default search provider</td> <td>Not configured</td> </tr> <tr> <td>Restrict search providers to a specific list of providers</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Prevent participation in the Customer Experience Improvement Program	Enabled	Prevent performance of First Run Customize settings	Not configured	Restrict changing the default search provider	Not configured	Restrict search providers to a specific list of providers	Not configured
Setting	State										
Prevent participation in the Customer Experience Improvement Program	Enabled										
Prevent performance of First Run Customize settings	Not configured										
Restrict changing the default search provider	Not configured										
Restrict search providers to a specific list of providers	Not configured										
13. Policy	<p>Change the setting of the policy “Turn off Tab Grouping” to “Enabled”</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Turn off Tab Grouping</td> <td>Enabled</td> </tr> <tr> <td>Turn off tabbed browsing</td> <td>Not configured</td> </tr> <tr> <td>Turn off the activation of the quick pick menu</td> <td>Not configured</td> </tr> <tr> <td>Turn off the auto-complete feature for web addresses</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Turn off Tab Grouping	Enabled	Turn off tabbed browsing	Not configured	Turn off the activation of the quick pick menu	Not configured	Turn off the auto-complete feature for web addresses	Not configured
Setting	State										
Turn off Tab Grouping	Enabled										
Turn off tabbed browsing	Not configured										
Turn off the activation of the quick pick menu	Not configured										
Turn off the auto-complete feature for web addresses	Not configured										

## 5.5 Refusing access to Anytime upgrade and Windows update

**Risk:** Possible process stop

**Weak point:** Access to Anytime Upgrade and Update

**Solution:** Refusing access to Anytime upgrade and Windows update

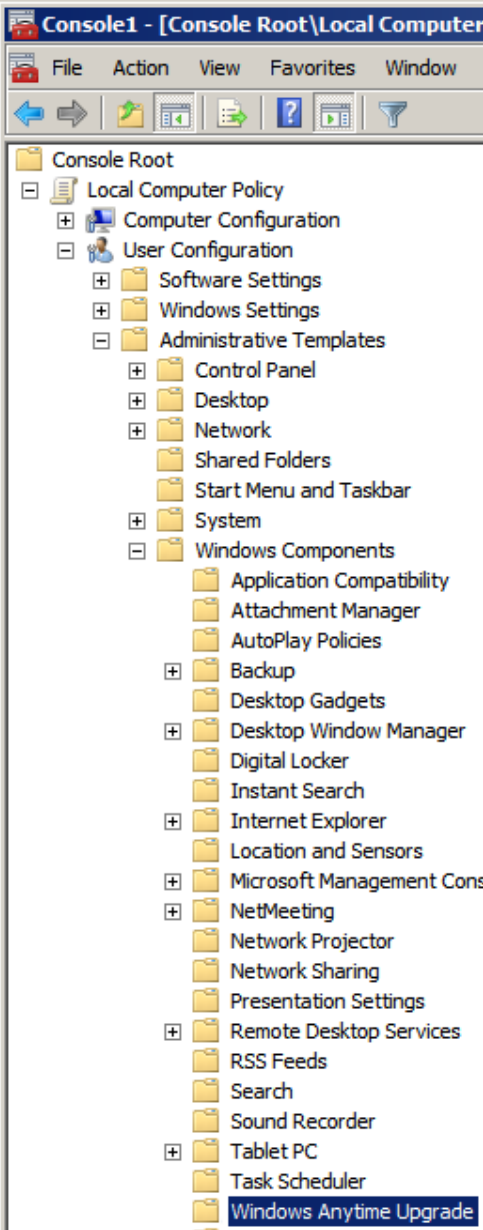
### Explaining the function

If system updates are automatically executed, this may cause an undesired restart of the system.

This can be prevented by means of a configuration that prevents Windows Anytime Update and Windows Updates from automatically being executed.

**Adaptation of the required settings**

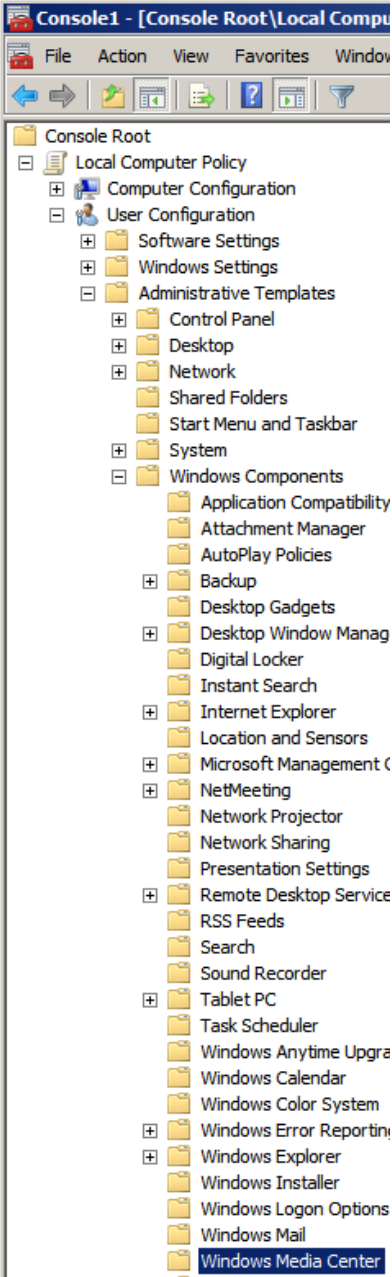
Table 5-8

Process	Action				
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Windows Anytime Upgrade”</p> 				
1. Policy	<p>Change the setting of the policy “Prevent Windows Anytime Upgrade from running” to “Enabled”</p> <table border="1" data-bbox="539 1803 1361 1870"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Prevent Windows Anytime Upgrade from running.</td> <td>Enabled</td> </tr> </tbody> </table>	Setting	State	Prevent Windows Anytime Upgrade from running.	Enabled
Setting	State				
Prevent Windows Anytime Upgrade from running.	Enabled				

## 5 Security Settings for IPCs with Network Access

### 5.5 Refusing access to Anytime upgrade and Windows update

Table 5-9

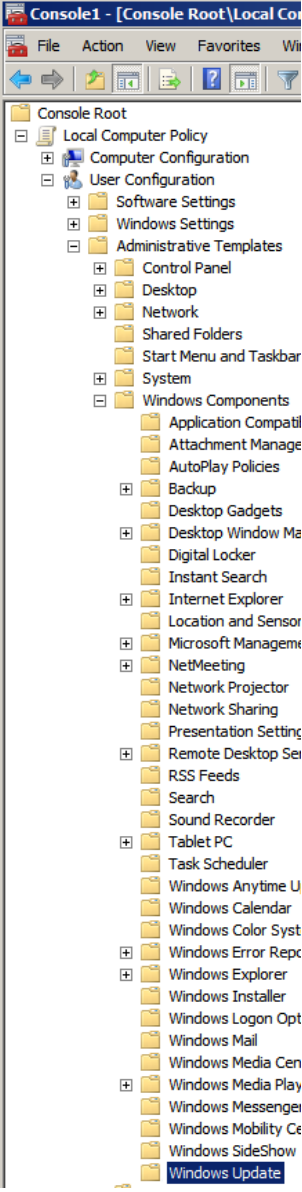
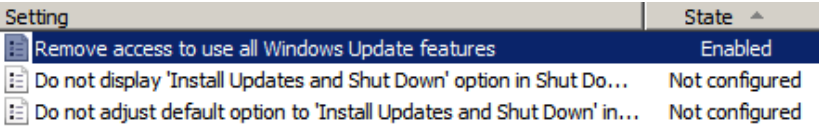
Process	Action				
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Windows Media Center”</p> 				
1. Policy	<p>Change the setting of the policy “Do not allow Windows Media Center to run” to “Enabled”</p> <table border="1" data-bbox="539 1805 1361 1868"> <thead> <tr> <th data-bbox="539 1805 1185 1839">Setting</th> <th data-bbox="1185 1805 1361 1839">State</th> </tr> </thead> <tbody> <tr> <td data-bbox="539 1839 1185 1868">Do not allow Windows Media Center to run</td> <td data-bbox="1185 1839 1361 1868">Enabled</td> </tr> </tbody> </table>	Setting	State	Do not allow Windows Media Center to run	Enabled
Setting	State				
Do not allow Windows Media Center to run	Enabled				



## 5 Security Settings for IPCs with Network Access

### 5.5 Refusing access to Anytime upgrade and Windows update

Table 5-10

Process	Action
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Windows Update”</p> 
1. Policy	<p>Change the setting of the policy “Remove access to use all Windows Update features” to “Enabled”</p> 

## 5.6 Tunnel connection with IPsec (VPN IPsec)

**Risk:** Unsecured connection - sensitive process data can be viewed

**Weak point:** Unsecured connection of remote maintenance via VPN

**Solution:** Using a virtual private network (VPN), that has been configured correctly

### Explaining the function


For a virtual private network (VPN), a public network (for example internet) is used as transit network for transferring private data.

The IPsec protocol provides for manufacturer-independent, secure, and protected data exchange via IP networks. [IPsec](#) uses the tunneling concept. Data transfer between the tunnel end points (sender and recipient) cannot be read by unauthorized persons due to the encryption.

IPsec is part of the Windows installation. To use VPN with IPsec, it is necessary to adjust the IPsec tunnel authorization.

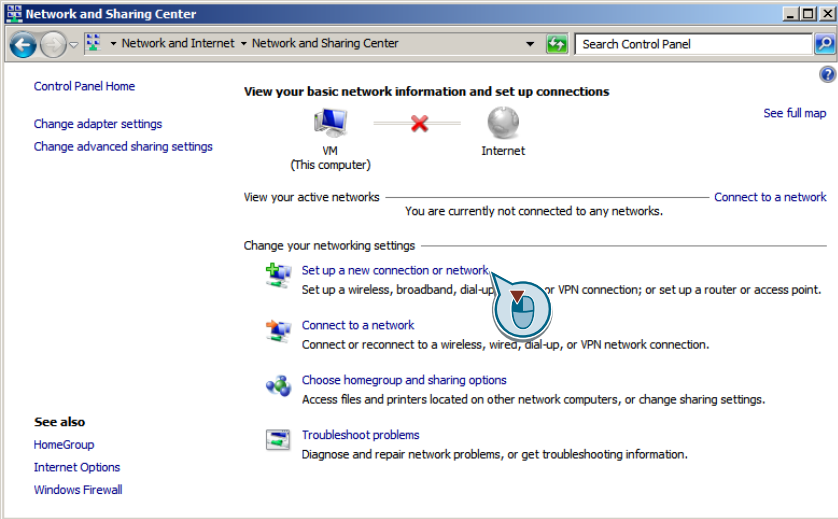
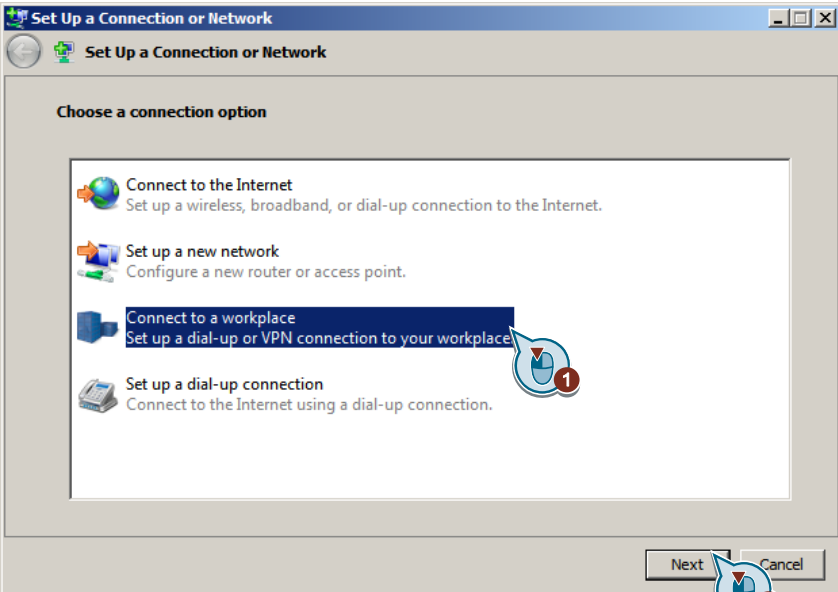
**Adaptation of the required settings**

Table 5-11

Process	Action
1.	<p>Open the Network and Sharing Center via “Start &gt; Control Panel&gt; Network and Internet &gt; Network and Sharing Center”.</p>  

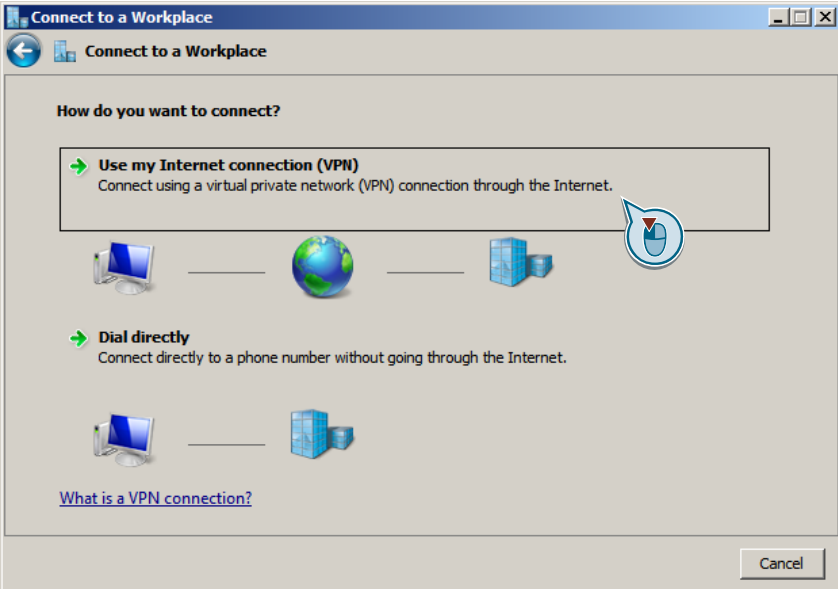
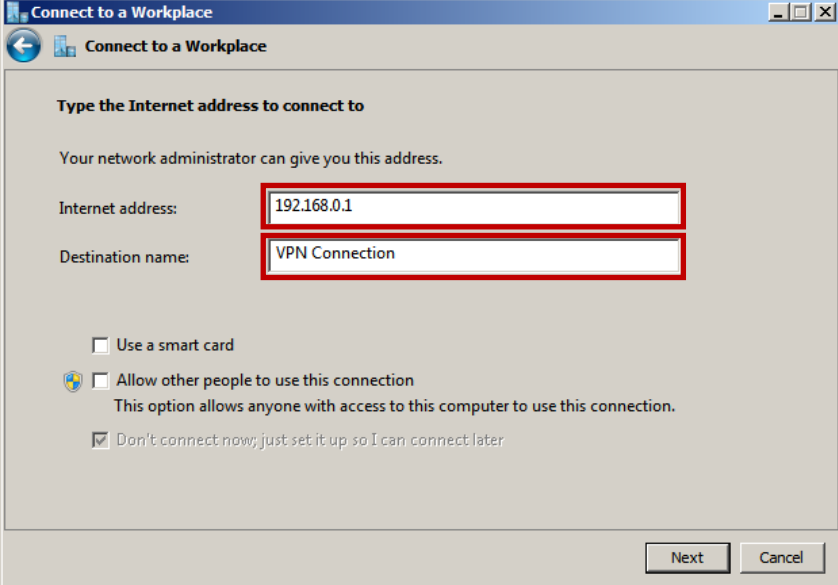
## 5 Security Settings for IPCs with Network Access

### 5.6 Tunnel connection with IPsec (VPN IPsec)

Process	Action
2.	<p>In the “Network and Sharing Center” you select the entry “Setup a new connection or network”.</p> 
3.	<p>In the following dialog you select the entry “Connect to a workplace” and press the “Next” button.</p> 

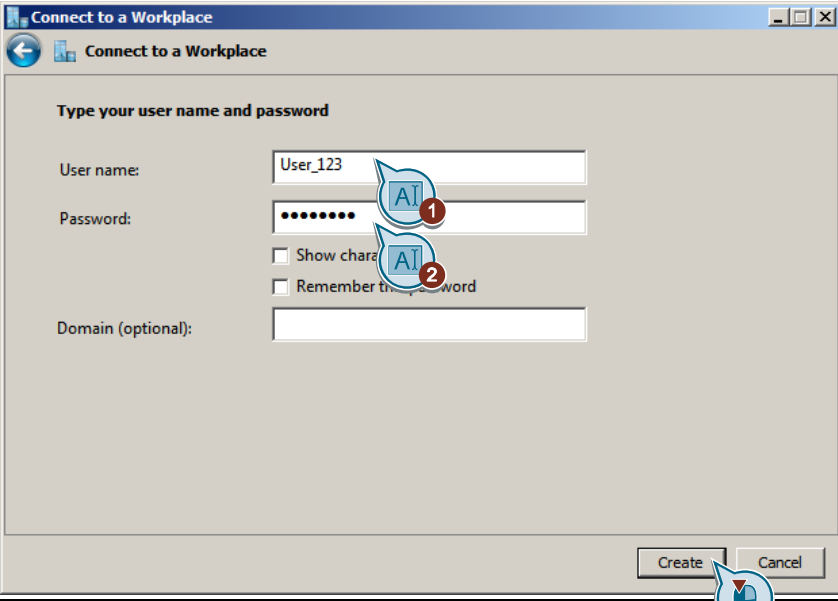
## 5 Security Settings for IPCs with Network Access

### 5.6 Tunnel connection with IPsec (VPN IPsec)

Process	Action
4.	<p>Select the option "Use my Internet connection (VPN)".</p>  <p>The screenshot shows a window titled "Connect to a Workplace" with a "Connect to a Workplace" button. Below the button, the text "How do you want to connect?" is displayed. There are two options: "Use my Internet connection (VPN)" (selected and highlighted with a red box) and "Dial directly". A red callout bubble points to the selected option. The "Use my Internet connection (VPN)" option includes a sub-description: "Connect using a virtual private network (VPN) connection through the Internet." and an icon showing a computer, a globe, and a server. The "Dial directly" option includes a sub-description: "Connect directly to a phone number without going through the Internet." and an icon showing a computer and a server. A link "What is a VPN connection?" is visible at the bottom left. A "Cancel" button is at the bottom right.</p>
5.	<p>Enter the respective "Internet address" and "Destination name".</p>  <p>The screenshot shows a window titled "Connect to a Workplace" with a "Connect to a Workplace" button. Below the button, the text "Type the Internet address to connect to" is displayed. Below this text, the instruction "Your network administrator can give you this address." is shown. There are two input fields: "Internet address:" containing "192.168.0.1" and "Destination name:" containing "VPN Connection". Both fields are highlighted with red boxes. Below the input fields, there are three checkboxes: "Use a smart card" (unchecked), "Allow other people to use this connection" (unchecked), and "Don't connect now; just set it up so I can connect later" (checked). A "Next" button and a "Cancel" button are at the bottom right.</p>

## 5 Security Settings for IPCs with Network Access

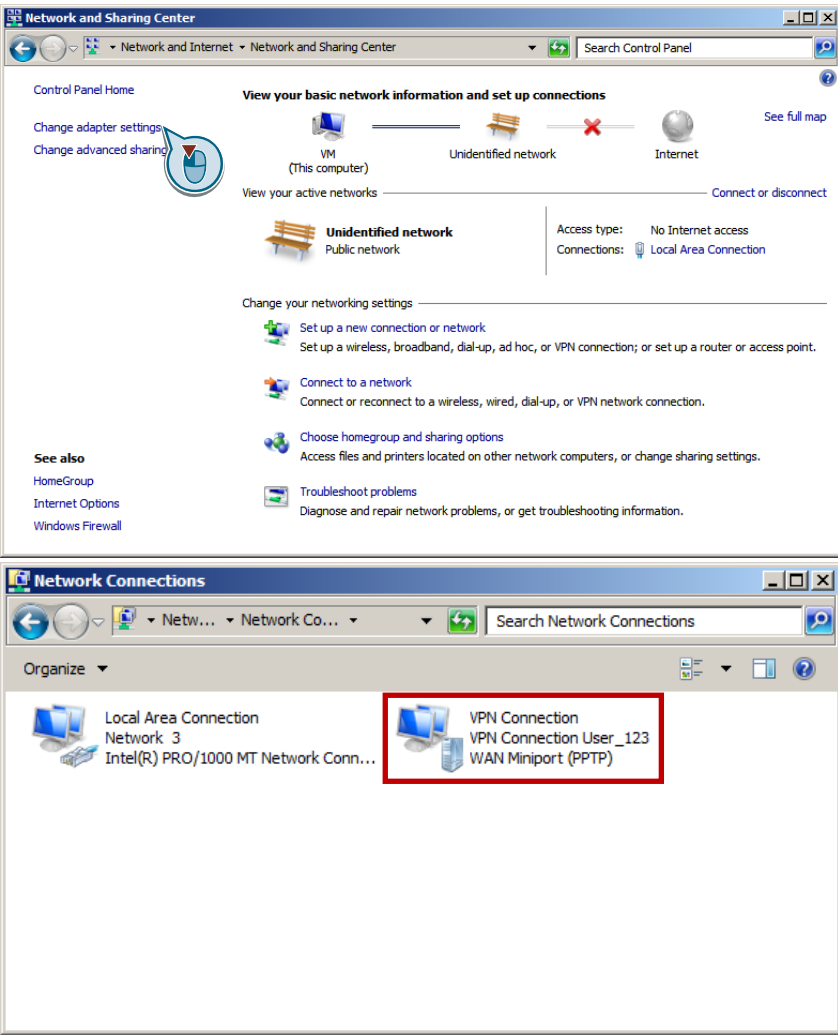
### 5.6 Tunnel connection with IPsec (VPN IPsec)

Process	Action
6.	<p>Enter the "User name" and "Password" and acknowledge the dialog with "Create".</p> 

## 5 Security Settings for IPCs with Network Access

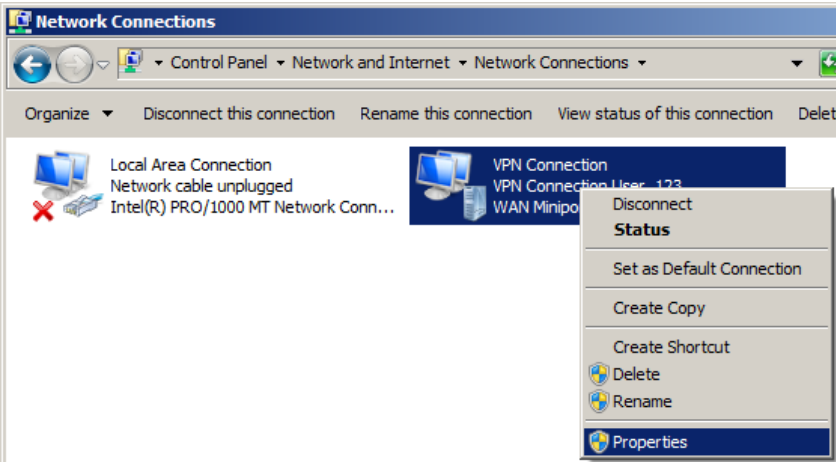
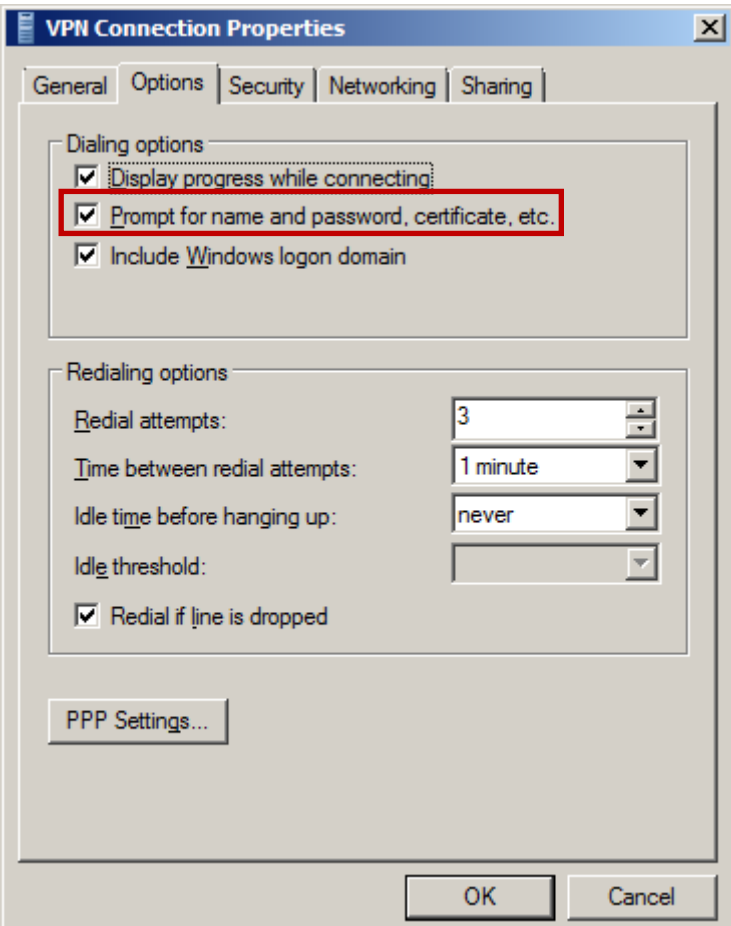
### 5.6 Tunnel connection with IPsec (VPN IPsec)

Table 5-12

Process	Action
1.	Open the Network and Sharing Center again as described in <a href="#">Table 5-11</a> Step 1.
2.	<p>Open the “Network and Sharing Center” window via the entry “Change adapter settings” in the “Network and Sharing Center”.</p>  <p>The screenshot shows two windows from the Windows operating system. The top window is the 'Network and Sharing Center'. It displays a network diagram with 'VM (This computer)', 'Unidentified network', and 'Internet'. Below the diagram, it shows details for the 'Unidentified network' (Public network) with 'Access type: No Internet access' and 'Connections: Local Area Connection'. There are several links for changing networking settings, such as 'Set up a new connection or network', 'Connect to a network', 'Choose homegroup and sharing options', and 'Troubleshoot problems'. The bottom window is 'Network Connections'. It lists several network adapters: 'Local Area Connection Network 3 Intel(R) PRO/1000 MT Network Conn...', 'VPN Connection', 'VPN Connection User_123', and 'WAN Miniport (PPTP)'. The 'VPN Connection' and 'VPN Connection User_123' entries are highlighted with a red rectangular box.</p>

## 5 Security Settings for IPCs with Network Access

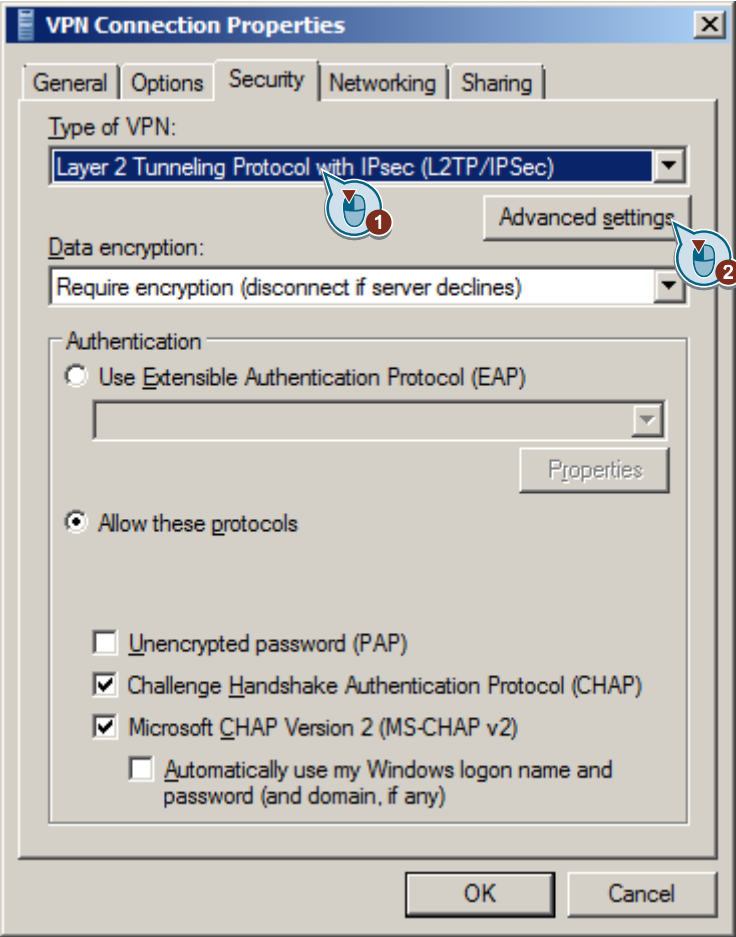
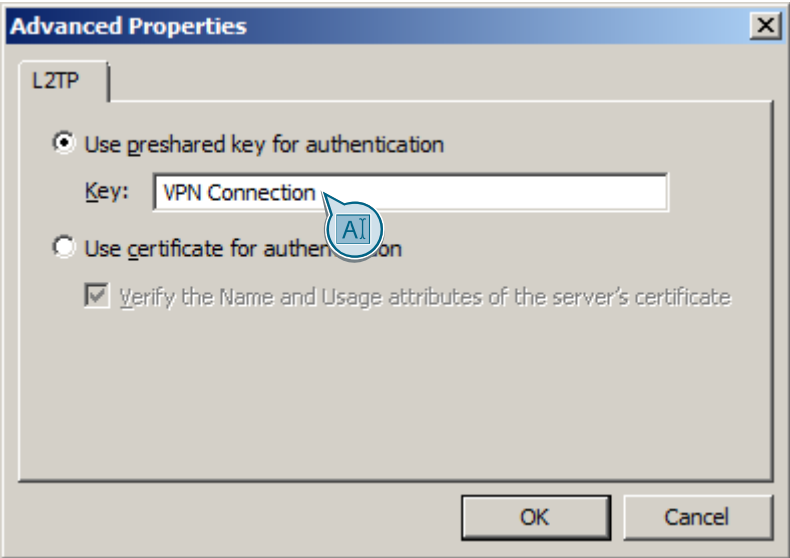
### 5.6 Tunnel connection with IPsec (VPN IPsec)

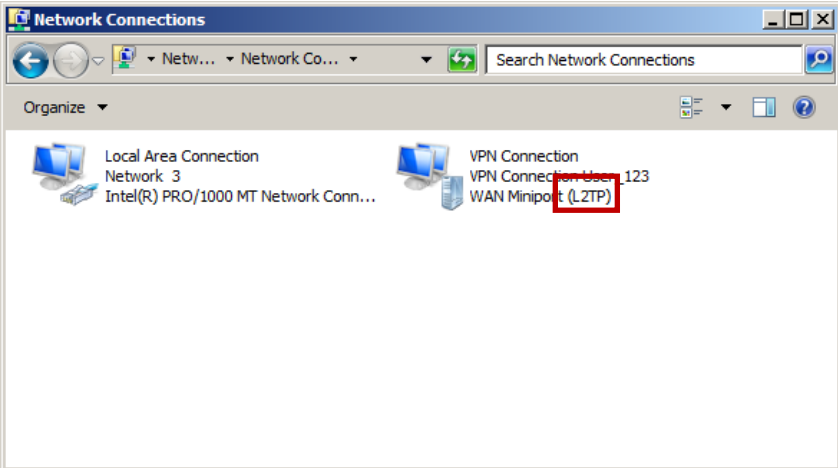
Process	Action
3.	<p>Open the properties of the VPN connection via the context menu.</p>  <p>The screenshot shows the Windows Network Connections window. A context menu is open over a VPN connection, with the 'Properties' option highlighted. The menu items include: Disconnect, Status, Set as Default Connection, Create Copy, Create Shortcut, Delete, Rename, and Properties.</p>
4.	<p>Go to the "Options" tab and check whether the option "Dialing options" "Prompt for name and password, certificate, etc." has been set.</p>  <p>The screenshot shows the 'VPN Connection Properties' dialog box, 'Options' tab. Under 'Dialing options', the checkbox 'Prompt for name and password, certificate, etc.' is checked and highlighted with a red box. Other options include 'Display progress while connecting' and 'Include Windows logon domain'. Under 'Redialing options', there are settings for 'Redial attempts' (3), 'Time between redial attempts' (1 minute), 'Idle time before hanging up' (never), and 'Idle threshold'. A 'PPP Settings...' button is at the bottom left, and 'OK' and 'Cancel' buttons are at the bottom right.</p>



## 5 Security Settings for IPCs with Network Access

### 5.6 Tunnel connection with IPsec (VPN IPsec)

Process	Action
5.	<p>Go to the Security tab and select the VPN type: "Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)".</p> <p>Now press the "Advanced settings" button and enter the name of your VPN connection ("VPN Connection" in the example) in the "Key" field.</p>  <p>The screenshot shows the 'VPN Connection Properties' dialog box with the 'Security' tab selected. The 'Type of VPN' dropdown is set to 'Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)'. The 'Data encryption' dropdown is set to 'Require encryption (disconnect if server declines)'. Under 'Authentication', the 'Allow these protocols' radio button is selected, and 'Challenge Handshake Authentication Protocol (CHAP)' and 'Microsoft CHAP Version 2 (MS-CHAP v2)' are checked. The 'Advanced settings' button is highlighted with a red circle and a blue arrow labeled '2'. A red circle with '1' is also present near the 'Type of VPN' dropdown.</p>  <p>The screenshot shows the 'Advanced Properties' dialog box with the 'L2TP' tab selected. The 'Use preshared key for authentication' radio button is selected, and the 'Key' field contains 'VPN Connection'. The 'Verify the Name and Usage attributes of the server's certificate' checkbox is checked. A blue arrow labeled 'AI' points to the 'Key' field.</p>

Process	Action
6.	<p>Confirm the two dialogs by clicking “OK”. Now the VPN type “L2TP” is shown in the connection.</p>  <p>The screenshot shows the Windows Network Connections window. It displays two network connections: 'Local Area Connection Network 3' and 'VPN Connection VPN Connection User_123'. The 'VPN Connection' is highlighted with a red box, and its type is listed as 'WAN Miniport (L2TP)'.</p>

**Note**

Please note, that in this case only the settings for the “VPN client” were described. “Incoming connections” for the User used here must be permitted on the “VPN server”.

## 5.7 Appropriate configuration for Remote Desktop

**Risk:** Unauthorized access rights

**Weak point:** Unsecured remote - Desktop connection

**Solution:** Secure configuration of the remote Desktop

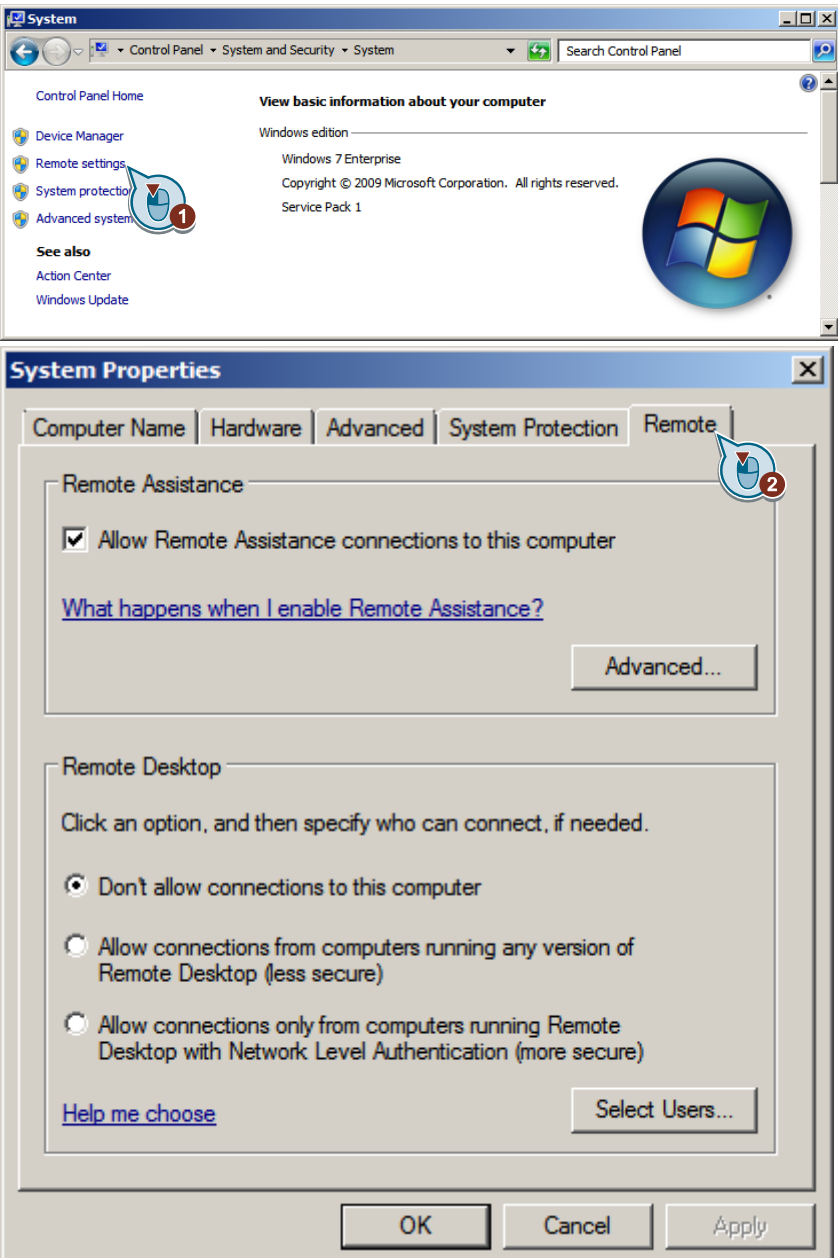
### Explaining the function

To be able to use the Remote Desktop connection for a restricted user account (without administrator rights), the respective user must be added in “Select user...” (see [Table 5-13](#))

Using the group policies enables expanding the settings for the Remote Desktop services. By default, the listed settings (see [Table 5-14](#) and [Table 5-15](#)) are not configured. To provide a higher connection security, it is recommended to use the [NTLM](#) protocol as well as not permit the saving of passwords.

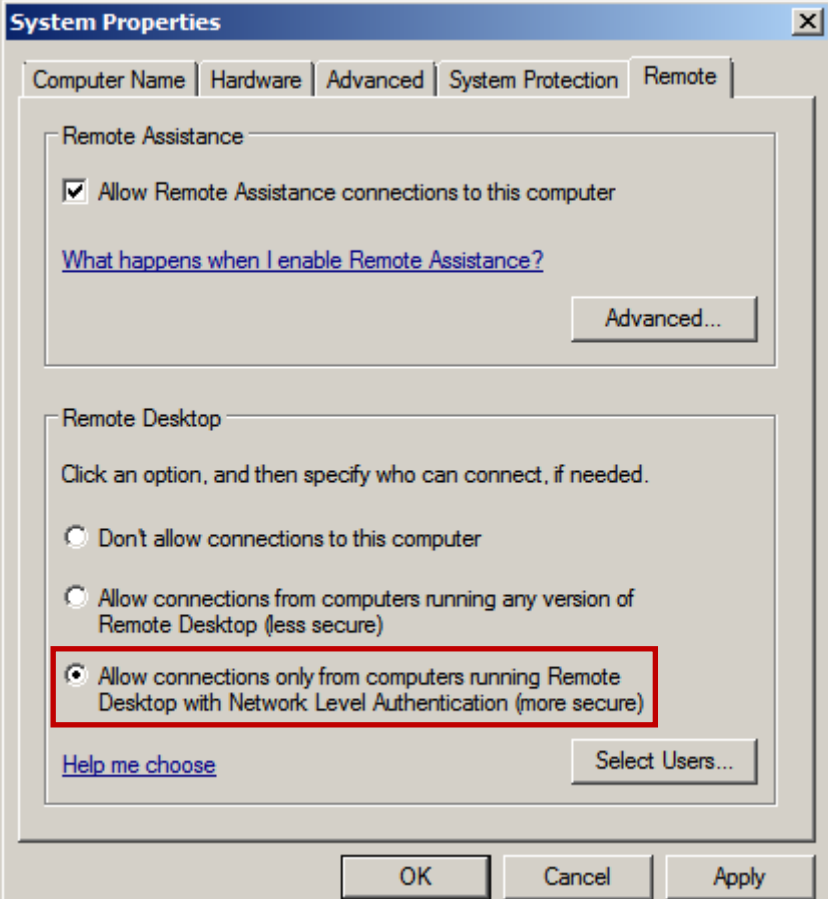
**Adaptation of the required settings**

Table 5-13

Process	Action
1.	<p>Open the “System Properties” via “Start &gt; Control Panel &gt; System and Security &gt; Windows Firewall” and go to the “Remote” tab.</p>  <p>The screenshot shows two windows. The top window is the 'System' page in the Control Panel, showing basic information about the computer (Windows 7 Enterprise, Service Pack 1). A red circle with the number '1' is placed over the 'Remote settings' link in the left-hand navigation pane. The bottom window is the 'System Properties' dialog box, with the 'Remote' tab selected. A red circle with the number '2' is placed over the 'Remote Assistance' section, which has the checkbox 'Allow Remote Assistance connections to this computer' checked. The 'Remote Desktop' section below it has the radio button 'Don't allow connections to this computer' selected.</p>

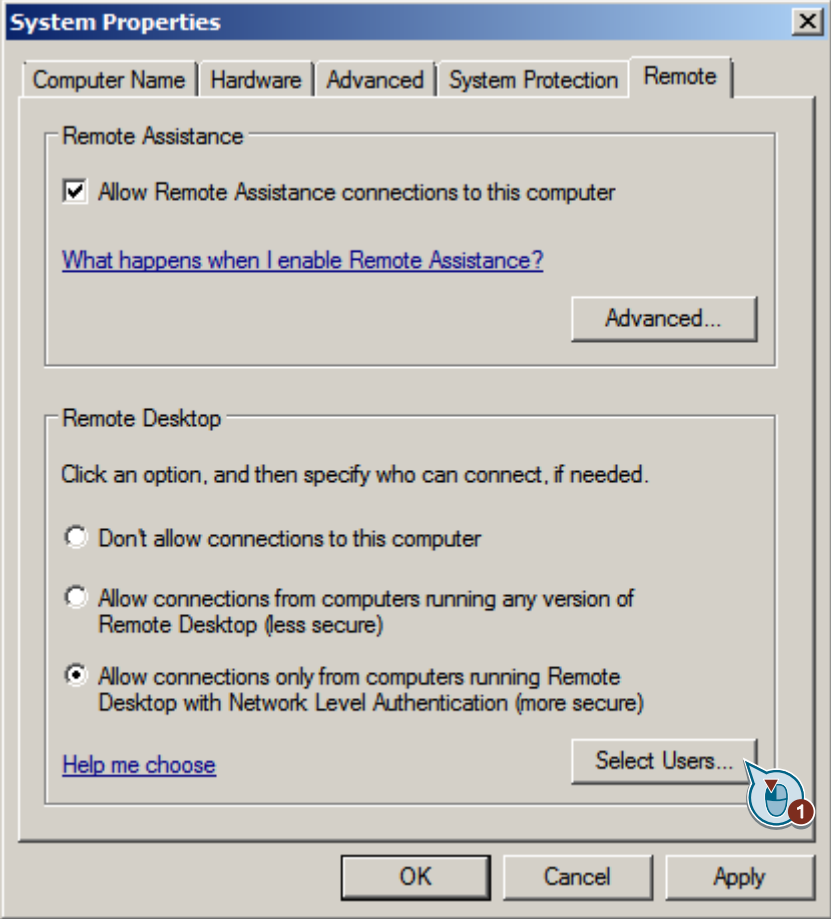
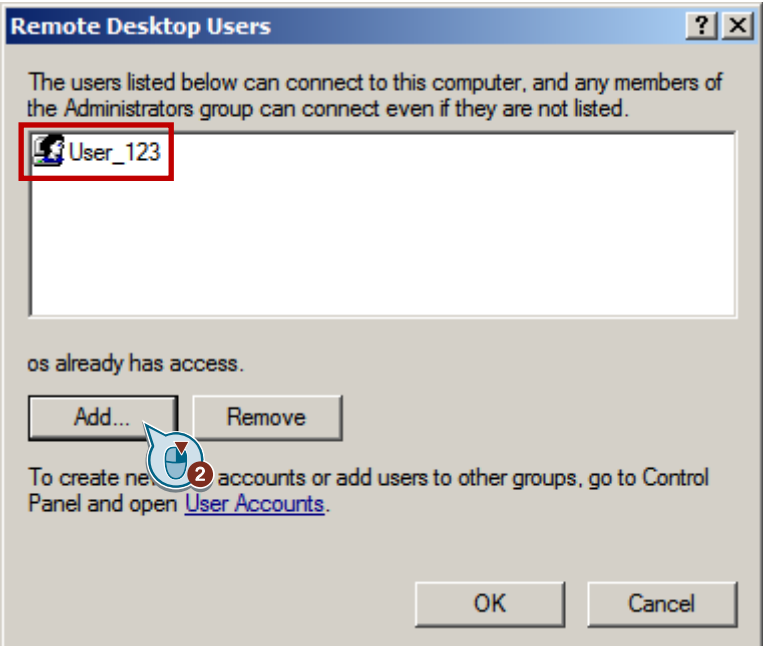
## 5 Security Settings for IPCs with Network Access

### 5.7 Appropriate configuration for Remote Desktop

Process	Action
2.	<p>In this case you select the option “Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)”</p>  <p><b>System Properties</b></p> <p>Computer Name   Hardware   Advanced   System Protection   Remote</p> <p>Remote Assistance</p> <p><input checked="" type="checkbox"/> Allow Remote Assistance connections to this computer</p> <p><a href="#">What happens when I enable Remote Assistance?</a></p> <p>Advanced...</p> <p>Remote Desktop</p> <p>Click an option, and then specify who can connect, if needed.</p> <p><input type="radio"/> Don't allow connections to this computer</p> <p><input type="radio"/> Allow connections from computers running any version of Remote Desktop (less secure)</p> <p><input checked="" type="radio"/> Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)</p> <p><a href="#">Help me choose</a></p> <p>Select Users...</p> <p>OK Cancel Apply</p>

## 5 Security Settings for IPCs with Network Access

### 5.7 Appropriate configuration for Remote Desktop

Process	Action
3.	<p>In "Select Users" in the "Remote Desktop Users" dialog you enter the respective user(s) via the "Add" button.</p>  

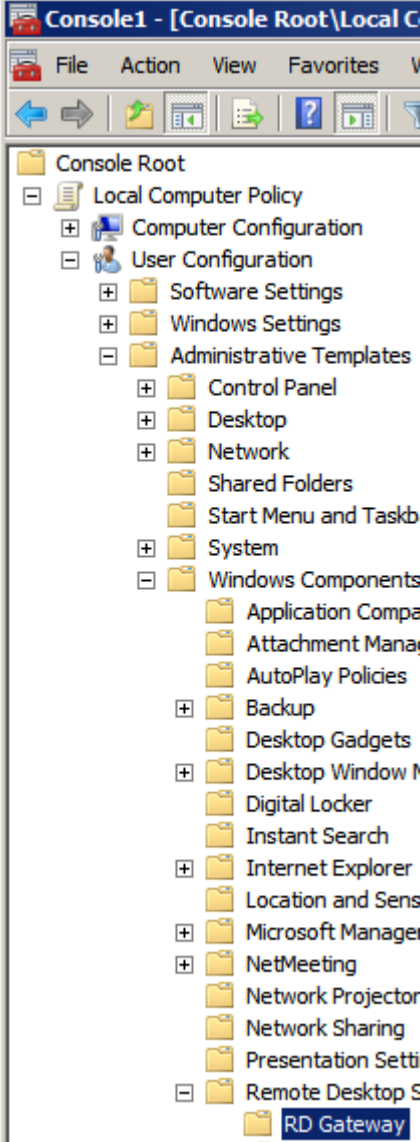
**Note**

Further information is available at: <http://windows.microsoft.com/en-gb/windows7/allow-someone-to-connect-to-your-computer-using-remote-desktop-connection>

5 Security Settings for IPCs with Network Access

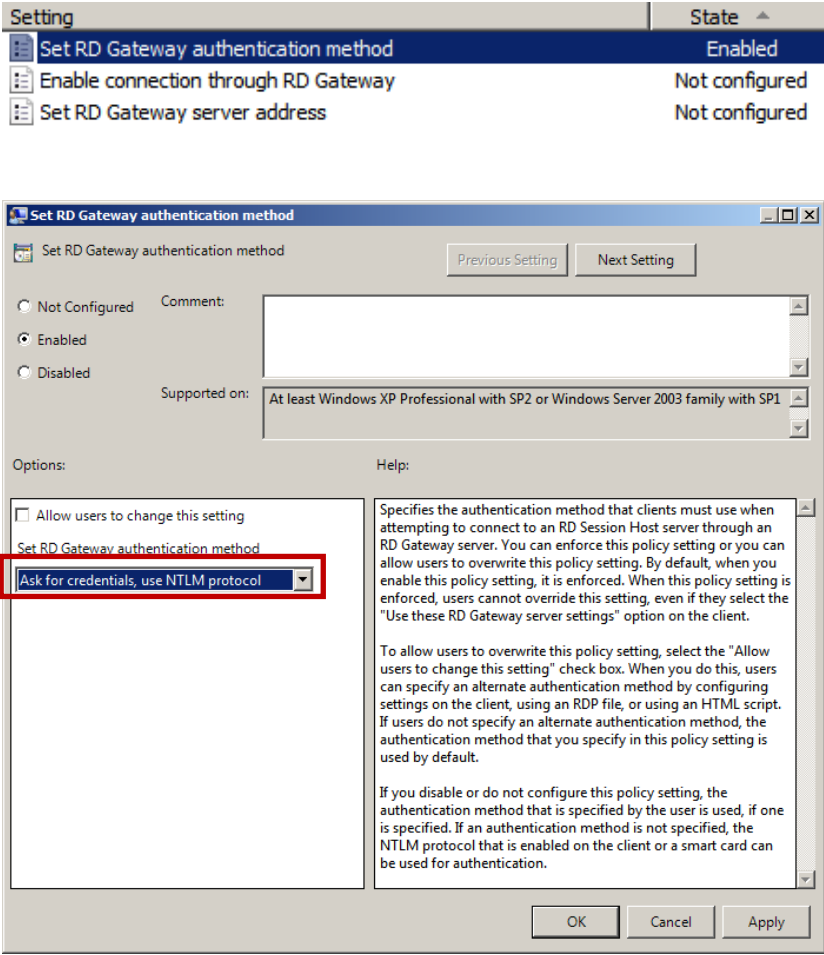
5.7 Appropriate configuration for Remote Desktop

Table 5-14

Process	Action
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:                      “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Remote Desktop Services &gt; RD Gateway”</p> 

## 5 Security Settings for IPCs with Network Access

### 5.7 Appropriate configuration for Remote Desktop

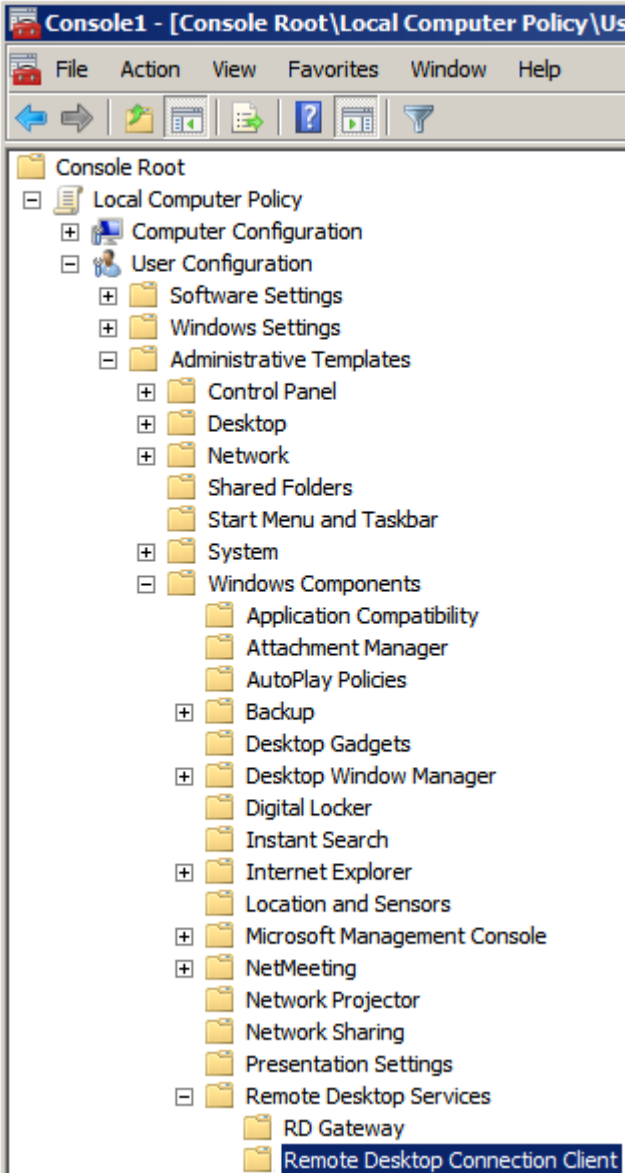
Process	Action								
<p>1. Policy</p>	<p>Change the setting of the policy "Set RD Gateway authentication method" to "Enabled" and select the dropdown list entry "Ask for credentials, use NTLM protocol"</p>  <p>The screenshot shows the Group Policy Editor interface. At the top, a table lists policy settings:</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Set RD Gateway authentication method</td> <td>Enabled</td> </tr> <tr> <td>Enable connection through RD Gateway</td> <td>Not configured</td> </tr> <tr> <td>Set RD Gateway server address</td> <td>Not configured</td> </tr> </tbody> </table> <p>Below this is the configuration dialog for 'Set RD Gateway authentication method'. It has radio buttons for 'Not Configured', 'Enabled' (selected), and 'Disabled'. The 'Supported on' dropdown is set to 'At least Windows XP Professional with SP2 or Windows Server 2003 family with SP1'. Under 'Options', the 'Allow users to change this setting' checkbox is unchecked. The 'Set RD Gateway authentication method' dropdown is set to 'Ask for credentials, use NTLM protocol', which is highlighted with a red box. A 'Help' section provides detailed instructions on enforcing and overriding the policy.</p>	Setting	State	Set RD Gateway authentication method	Enabled	Enable connection through RD Gateway	Not configured	Set RD Gateway server address	Not configured
Setting	State								
Set RD Gateway authentication method	Enabled								
Enable connection through RD Gateway	Not configured								
Set RD Gateway server address	Not configured								



## 5 Security Settings for IPCs with Network Access

### 5.7 Appropriate configuration for Remote Desktop

Table 5-15

Process	Action										
Path	<p>Open the “Microsoft Management Console” as described in <a href="#">Table 3-2</a> and then open the following path:            “User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Remote Desktop Services &gt; Remote Desktop Connection Client”</p> 										
1. Policy	<p>Change the setting of the policy “Do not allow passwords to be saved” to “Enabled”</p> <table border="1" data-bbox="539 1704 1361 1865"> <thead> <tr> <th>Setting</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Do not allow passwords to be saved</td> <td>Enabled</td> </tr> <tr> <td>Allow .rdp files from valid publishers and user's default .rdp settings</td> <td>Not configured</td> </tr> <tr> <td>Allow .rdp files from unknown publishers</td> <td>Not configured</td> </tr> <tr> <td>Specify SHA1 thumbprints of certificates representing trusted .rd...</td> <td>Not configured</td> </tr> </tbody> </table>	Setting	State	Do not allow passwords to be saved	Enabled	Allow .rdp files from valid publishers and user's default .rdp settings	Not configured	Allow .rdp files from unknown publishers	Not configured	Specify SHA1 thumbprints of certificates representing trusted .rd...	Not configured
Setting	State										
Do not allow passwords to be saved	Enabled										
Allow .rdp files from valid publishers and user's default .rdp settings	Not configured										
Allow .rdp files from unknown publishers	Not configured										
Specify SHA1 thumbprints of certificates representing trusted .rd...	Not configured										

## 6 Links & Literature

Table 6-1

	Topic	Title
\1\	Siemens Industry Online Support	<a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>
\2\	Download page of the entry	<a href="https://support.industry.siemens.com/cs/ww/en/view/109475014">https://support.industry.siemens.com/cs/ww/en/view/109475014</a>
\3\	Security guideline for PC-based automation systems	<a href="https://support.industry.siemens.com/cs/ww/en/view/55390879">https://support.industry.siemens.com/cs/ww/en/view/55390879</a>
\4\	Configuring Windows 7 for a standard user account	<a href="http://technet.microsoft.com/en-gb/library/ee623984(v=ws.10).aspx">http://technet.microsoft.com/en-gb/library/ee623984(v=ws.10).aspx</a>
\5\	What is user account control?	<a href="http://windows.microsoft.com/en-gb/windows/what-is-user-account-control">http://windows.microsoft.com/en-gb/windows/what-is-user-account-control</a>
\6\	Windows 7 AppLocker Overview	<a href="http://technet.microsoft.com/en-gb/library/dd548340(v=ws.10).aspx">http://technet.microsoft.com/en-gb/library/dd548340(v=ws.10).aspx</a>
\7\	IPSec	<a href="http://en.wikipedia.org/wiki/IPsec">http://en.wikipedia.org/wiki/IPsec</a>
\8\	NTLM	<a href="http://en.wikipedia.org/wiki/NTLM">http://en.wikipedia.org/wiki/NTLM</a>
\9\	Information on remote desktop connections	<a href="http://windows.microsoft.com/en-gb/windows7/allow-someone-to-connect-to-your-computer-using-remote-desktop-connection">http://windows.microsoft.com/en-gb/windows7/allow-someone-to-connect-to-your-computer-using-remote-desktop-connection</a>

## 7 History

Table 7-1

Version	Date	Modifications
V1.0	05/2015	First version