Recommended security settings for IPCs in industrial environments

SIMATIC IPCs

https://support.industry.siemens.com/cs/ww/EN/view/109475014

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.
Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

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

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.
The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Table of contents

1 The task

Introduction

SIMATIC IPCs must meet the highest safety and reliability requirements for the control of machines and plants in industry.

The Windows operating system offers extensive options for configuring an IPC. The measures proposed in this contribution increase the availability and IT security of the operating system. Important settings for this are contained in the Group Policy. There are two ways to change the Group Policy:

- Editor for Local Group Policy Editor
- Microsoft Management Console

Description of the automation task

This configuration example gives you recommendations for necessary settings. This minimizes risks for IPCs in the industrial environment. A distinction is made here between IPCs without a network connection ("stand-alone operation") and IPCs with network access for which further settings are required.

Note When discussing security on IPCs, also refer to the Security Guide in the article 55390879.

2 Solution

2.1 Security Checklist

The following checklist lists a number of risks and their solutions.

These notes are divided into recommendations for IPCs without a network connection ("stand-alone operation") and for IPCs with a network connection for which additional settings are required.

Settings for IPCs without network connection

Table 2-1

Risk	Weak point	Solution
Unauthorized modification of system parameters	Only one administrator account exists	Section 4.1: Operation of the SIMATIC software as a user with restricted rights
Employees with user rights can install any programs they like	Application installation also possible by user	Section 4.2: Suppressing the password query for administrator rights
Changes to the system	System files can be manipulated	Section 4.3: Due to the UWF, changes to system files are only possible in RAM.
Process stop possible	Shutdown option freely accessible	Section 4.4: Allow shutdown only after user login
Unauthorized execution of software	Running any malicious software	Section 4.5: Access control to software through AppLocker
Modification of system data, access to Internet Explorer, workstation, network connection	Desktop - Access to applications	Section 4.6: Prevent Windows applications and their properties from being accessed from the desktop.
Change of system data/network environment, IPC lock/shutdown	Start menu and taskbar - access to applications	Section 4.7: Preventing access to Windows applications from the Start menu
Processes and services can be stopped, incorrect configuration of the IPCs	Change password, Lock IPC, Access Task Manager	Section 4.8: Restriction of functions according to <Ctrl+Alt+Del>
Processes and services can be stopped, incorrect configuration of the IPCs	Changing the System Parameters in the Control Panel	Section 4.9: Prevent access to Control Panel
Infect IPC with malware, unwanted installation of programs	Access to removable media (e.g. USB sticks)	Section 4.10: Preventing access to removable media
Infect IPC with malware, unwanted installation of programs	Automatic execution of software (Autoplay function)	Section 4.11: Deactivating Autoplay or Autorun
Infect IPC with malware, unwanted installation of programs	Installations of removable media	Section 4.12: Disable removable disk installation

Risk	Weak point	Solution
Change system configuration (group policies, firewall settings, etc.)	Access to MMC (Microsoft Management Console)	Section 4.13: Deny access to MMC (Microsoft Management Console)
Unwanted access to applications	Access to paths when searching	Section 4.14: Deny access to paths when searching
Unauthorized access to system-relevant information, possibility of manipulation	Access to drives from the workstation	Section 4.16: Restrict access to network and specific drives

Additional settings for IPCs with network access

Table 2-2

Risk	Weak point	Solution
Sensitive process data can be viewed	Windows Firewall switched off / not configured	Section 5.1: Enable and configure Windows Firewall
Hacker attacks by online scanners, unauthorized accesses	Use default passwords	Section 5.2: Configure password policies correctly
Unauthorized modification of LAN connections, unauthorized removal/addition of components	Free access to the network connections	Section 5.3: Deny access to network connections
Free access to the Internet	Free access to Internet communication management	Section 5.4: Restricting Internet Access
Process stop possible	Access to Anytime Upgrade and Update	Section 5.5: Deny access to Anytime Upgrade and Windows Update
Unsafe connection - sensitive process data can be viewed	Remote maintenance via VPN is configured insecurely	Section 5.6: Using a Virtual Private Network (VPN) and its Configuration
Invalid access rights	Unsecure remote desktop connection	Section 5.7: Safe configuration of the remote desktop

Note The security check list shows only the recommended settings, but without any guarantee of completeness. Consult your security expert for final assessment and configuration.

Required knowledge

Basic knowledge of installation, configuration, networking and operation of IPCs in industrial environments is required.

2.2 Hardware and software components

Validity

This application is valid for all SIMATIC IPCs or other computers with Windows 10 Enterprise operating system.

Note The application example can also be used for other Windows 10 operating systems, but the menus may differ depending on the version.

Example files and projects

The following list contains all files and projects used in this example.

Table 2-3

Components	Note
109475014_Securityeinstellungen_IPCs_Win10_de.pdf	This document.

3 Basics

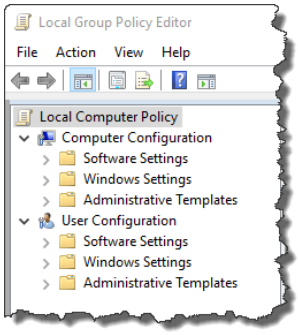
3.1 Basics about the editors

3.1.1 Editor for Local Group Policy Editor

Call

1. Open the "Local Group Policy Editor". Enter "gpedit.msc" in the Windows search and confirm with "Enter" ("Return").

Figure 3-1



Properties

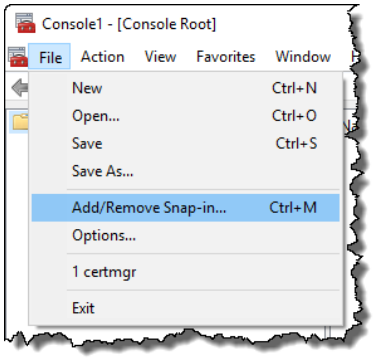
- Changing the computer configuration
- Changing the user configuration for all users

3.1.2 Microsoft Management Console

Call:

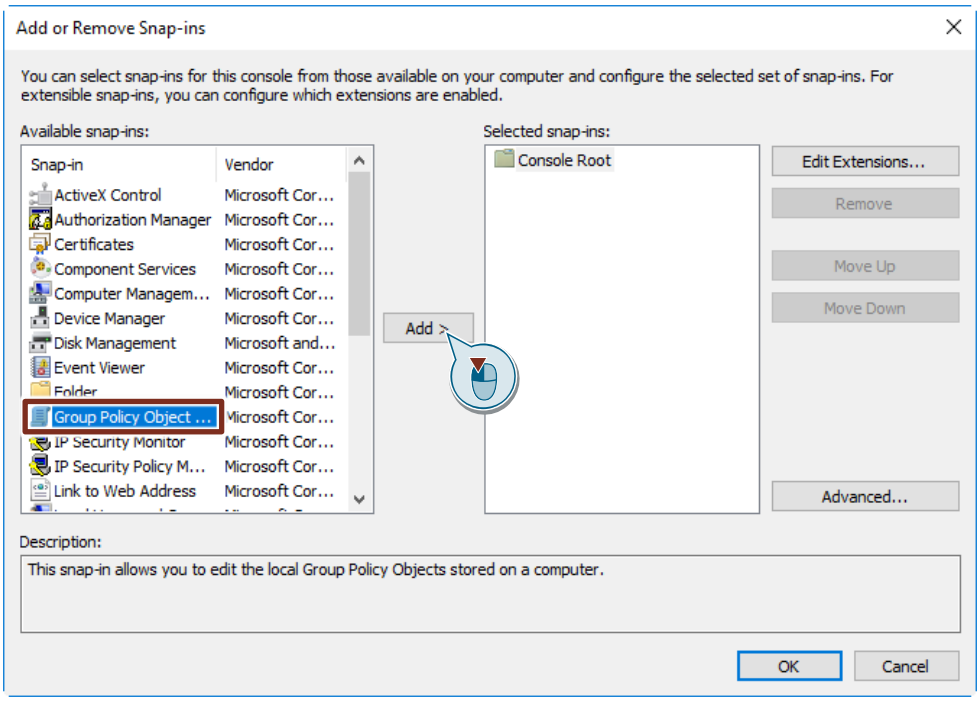
1. Open the "Microsoft Management Console". Enter "MMC.exe" in the Windows search and confirm with "Enter" ("Return").
2. Open the "Add or Remove Snap-Ins" dialog via the "File > Add/Remove Snap-Ins" menu item ("File > Add/Remove Snap-ins").

Figure 3-2:



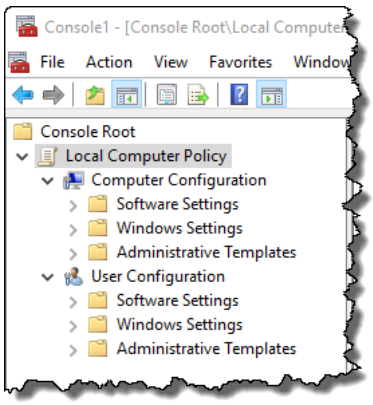
3. In the following dialog select the entry "Group Policy Objects" and click the button "Add >".

Figure 3-3



4. Confirm the following dialog with "Finish" and the "Add or Remove Snap-ins" window with the "OK" button.
5. The Microsoft Management Console now contains the "Local Group Policy".

Figure 3-4



Properties

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

Note In the following screenshots all changes are made for all users. These changes can also only be applied to selected users.

Note The following screenshots are created with Windows 10 in the design "Windows - classic". These may differ for other operating system variants.

4 Security settings for IPCs without network connection

4.1 User accounts and their rights

Risk: Unauthorized modification of system parameters

Weak point: Only one administrator account exists

Solution: Operation of the SIMATIC software as a user with restricted rights

4.1.1 Differentiation between administrator and user account

The basic prerequisite for a secure system is the distribution of access rights according to requirements, i.e. the user should only have the most necessary rights. If more rights are granted than are necessary for the task of the corresponding user, the operational safety of the IPC is unnecessarily endangered.

The correct setting of user accounts is crucial for the security of the system. Normal user and administrator should be used separately. This is necessary to prevent the unwanted execution of software.

Administrator account

The administrator account can be used to change security settings and install software and hardware. An administrator account can make settings for other users.

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

Users with restricted rights

A user account with limited rights may not make any system changes. If certain actions require administrator privileges, the user must log on as an administrator. Once the action has been completed, the original, restricted permissions apply again.

Additional information is available at:

Configuring Windows 10 for a default user account

https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts

What is User Account Control?

https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview

4.1.2 Operation of the SIMATIC software as a user with restricted rights

Software Controller

The SIMATIC software controller can be used without restriction under the restricted user account.

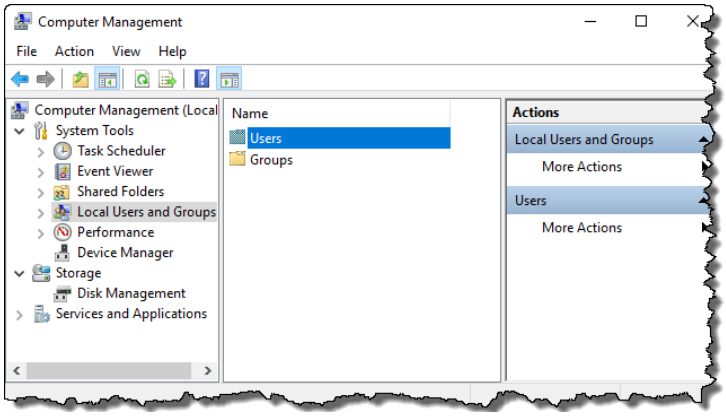
4.1.3 Create user account

To create a Windows user account with limited access rights, you must log on as an administrator.

There are several ways to create a new user account under Windows. The recommended way to create a new account using Computer Management is described in the following instructions. This sets up a default user, i.e. a user with restricted privileges.

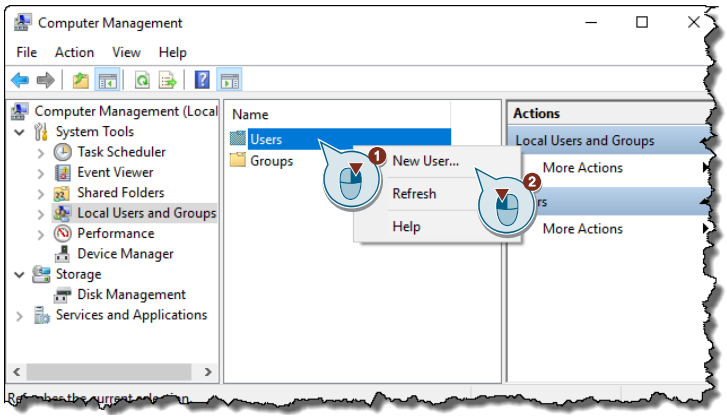
1. Open the Computer Management. To do this, enter "Computer Management" in the Windows search. Press "Enter".
2. Open the user management via "Computer Management > Local Users and Groups"

Figure 4-1



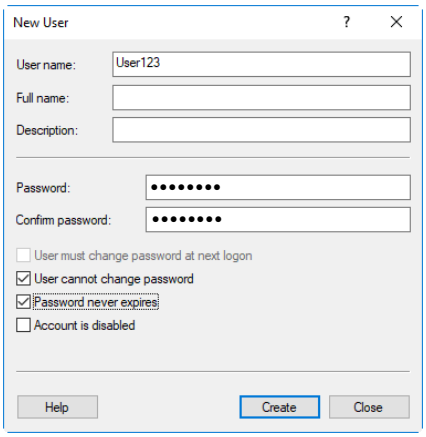
3. Right-click on the entry "Users" (1) and in the context menu on the entry "New User...". (2)

Figure 4-2



4. Fill in the window for the new user as shown in the following figure.

Fig. 4-3



5. Click "Create".

Note

For the account, you can define whether the user can change the password and whether or when it expires.

You can define the account as follows:

- User can change password
- User must change password after login
- User must update password after a certain period of time

Due to the special requirements in industrial use, it is recommended never to let the password expire for all users and not to allow password changes. Basically, the passwords should meet the complexity requirements (see Table 5-1).

4.2 Detect application installation and request elevated rights with User Account Control (UAC)

Risk: Employees with user rights can install any programs they like

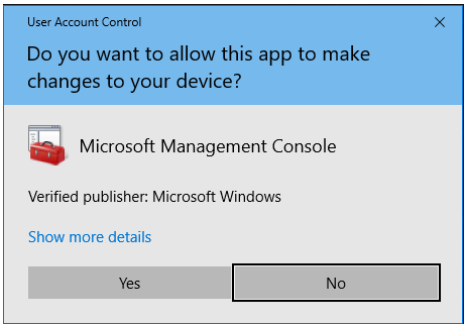
Weak point: Application installation also possible by user

Solution: Deactivation of the password query for administrator rights

Function explanation

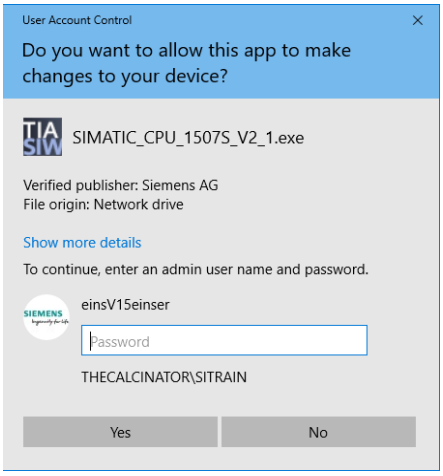
When administrators perform actions that require higher rights, the following dialog will notify them.

Figure 4-4:



For users with restricted rights, the following dialog appears prompting you to log in as an administrator.

Figure 4-5



This function can be deactivated via the User Account Control (UAC). This means that a user with restricted rights no longer has the option of obtaining increased rights.

Note

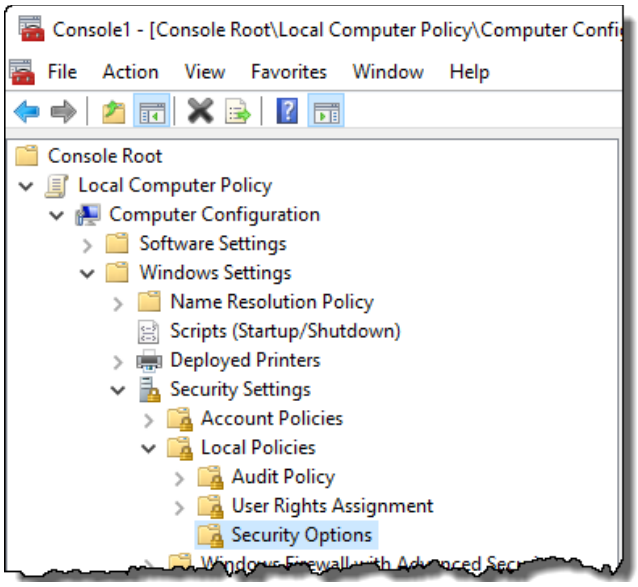
Basically, you should only give your administrator passwords to authorized employees and otherwise keep them secret.

This way you do not have to make this setting. This has the advantage that the admin can also make changes to the system without logging off the active user.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Settings"

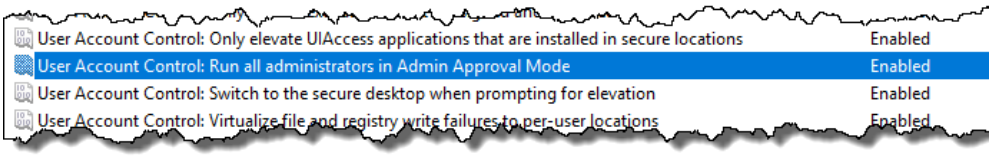
Figure 4-6



2. Change the following policy to "Enabled":

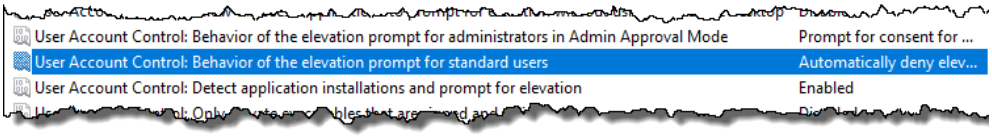
- "User Account Control: Run all administrators in administrator confirmation mode" ("User Account Control: Run all administrators in Admin Approval Mode")

Figure 4-7



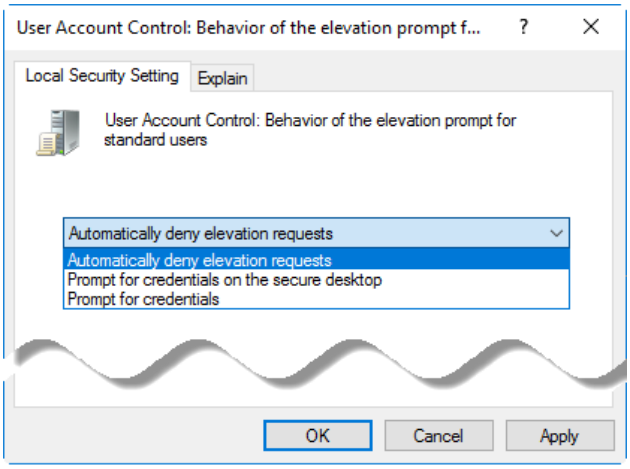
3. Change the "User Account Control policy setting: Behavior of the Increased rights prompt for standard users" ("User Account Control: Behavior of the elevation prompt for standard users").

Figure 4-8:



4. To do this, set the "Automatically deny elevation requests" option in the configuration window of this policy.

Figure 4-9



4.3 Unified Write Filters (UWF)

Risk: Changes to the system

Weak point: System files can be manipulated

Solution: The UWF allows changes to system files only in RAM.

Function explanation

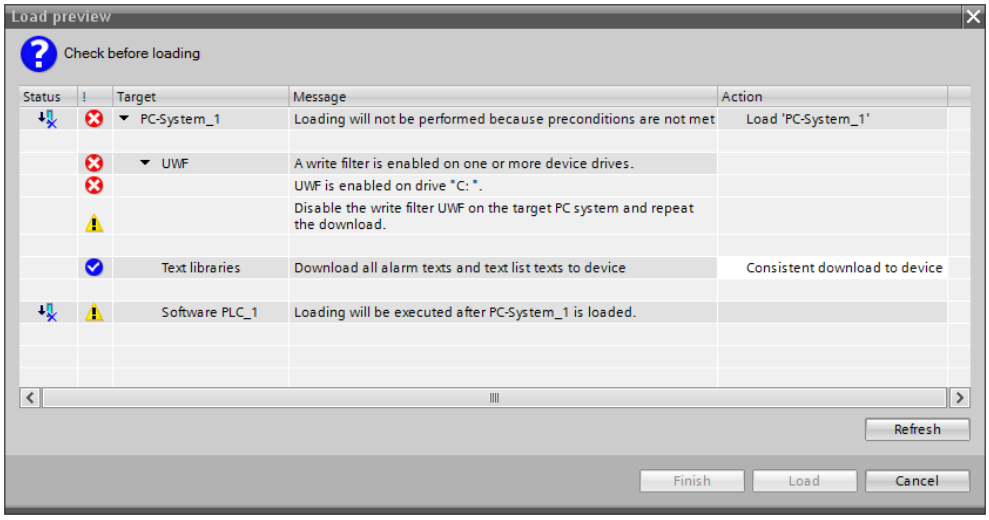
The Unified Write Filter is available in the Windows 10 Enterprise operating system version of the SIMATIC IPCs.

The UWF secures the file system against modification of files. The function redirects all write accesses to the RAM. After a restart, the file system is unchanged. There are no visible restrictions for the user. Malicious programs that have gained access during operation are no longer available after a restart. More information about the Unified Write Filter can be found under the following link: https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/unified-write-filter.

The advantages of the UWF come to bear when the system is restarted. If an IPC runs continuously, an active UWF brings no benefits.

CAUTION	If the UWF is active, the paths for configuration and program of the SIMATIC S7-1500 software controller must be set to a partition not protected by the UWF. When the UWF is active, loading the software controller or other configurations (e.g. WinCC) on the device. (Figure 4-10:)

Figure 4-10:

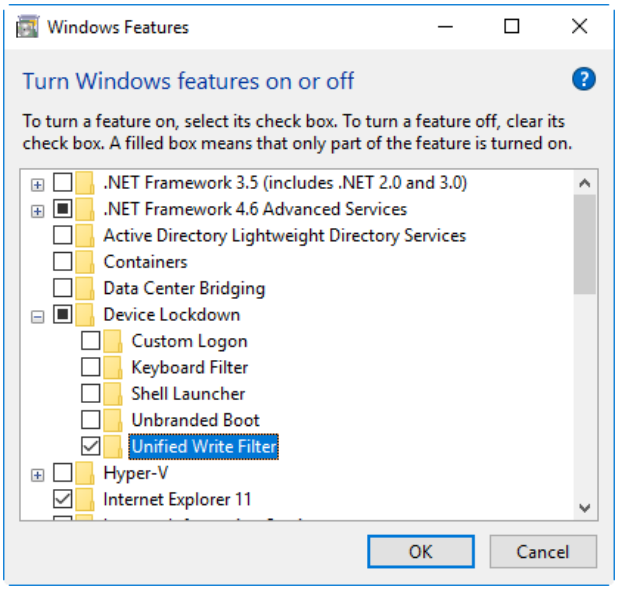


Adjustment of the necessary settings

Before you can use the UWF, you must enable it in the Windows features.

1. In the Windows Search, type the term "Features". Open the application "Enable or disable Windows features" ("Turn Windows features on or off").
2. In the Windows Feature window that opens, select "Device Lockdown > Unified Write Filter".

Figure 4-11



You can use the "UWFMGR.EXE" program to set and switch on/off the UWF. The program is called via the command prompt. An excerpt of the most important functions can be found in Table 4-1.

Note

To enable the UWF, you must run the CMD console as an administrator.

Enter "cmd" into the Windows search. Right-click the CMD application. Select the entry "Run as administrator".

Table 4-1

Function	Command
Overview of the current configuration	`uwfmgr get-config`
Write-protect drive C: Switch on	`uwfmgr volume protect c:`
Write-protect drive C: Switch off	`uwfmgr volume unprotect c:`
Activate UWF filter (required)	`uwfmgr filter enable`
Disable UWF Filter	`uwfmgr filter disable`
Exception for subdirectory C: Setting up	`uwfmgr file add-exclusion c:\foo\`
Exception for subdirectory C: Removing	`uwfmgr file remove-exclusion c:\foo\`
Activate maintenance mode (allows changes to protected directories)	`uwfmgr servicing enable`
Disable Servicing mode	`uwfmgr servicing disable`
Allow the installation of Windows updates only	`uwfmgr servicing update-windows`
Display UWF Help	`uwfmgr help`

Note The UWF commands regarding write protection are only effective after a restart of the IPC.

Note Further functions or special features for the use of the UWF can be found in the manual of the IPC used or at https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/uwfmgrexe.

4.4 Do not allow the system to shut down without logging in

Risk: Process stop possible

Weak point: Shutdown option freely accessible

Solution: Shutdown only possible after user login

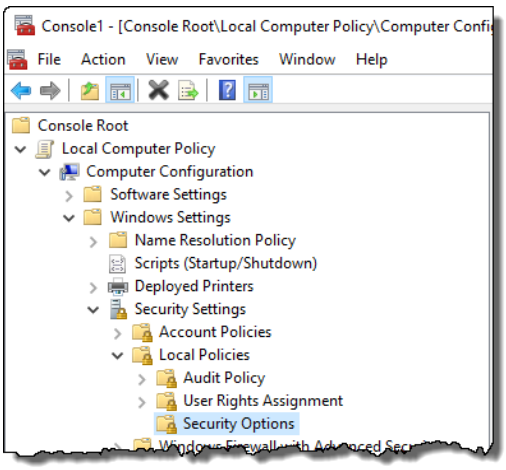
Function explanation

With some operator stations it may be necessary to prevent the station from shutting down or to enable this option only for certain operators.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2. Then open the following path:
   "Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options".

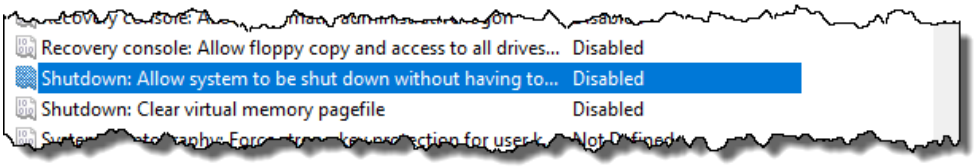
Figure 4-12



2. Change the following policy to "Disabled":

- "Shutdown: Allow system to be shut down without having to log on"

Figure 4-13



4.5 Software Restriction Guidelines - AppLocker

Risk: Unauthorized execution of software

Weak point: Running any malicious software

Solution: Access control to software through AppLocker

Function explanation

Access to software should only be granted to the extent required and desired. This prevents the misuse and in particular the installation of malware. The AppLocker application responsible for this is not available on all Windows variants. (Table 4-2).

This software may restrict access to software packages. AppLocker allows/prevents the execution of the following application types:

- Executable files ("*.exe" and "*.com")
- Scripts ("*.js", "*.ps1", "*.vbs", "*.cmd" and "*.bat")
- Windows Installer files ("*.msi" and "*.msp")
- DLL files ("*.dll" and "*.ocx")

Table 4-2

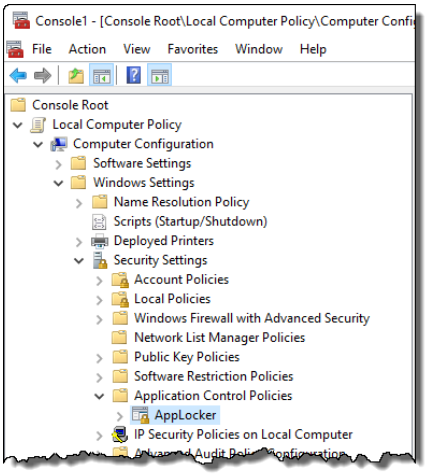
Windows version	AppLocker active
Windows 10 Enterprise	✓
Windows 10 Enterprise	✓
Windows 10 Home	X
Windows 10 Professional	X

CAUTION	An AppLocker configuration can be made with all Windows versions, but the configuration is only considered for the versions listed in Table 4-2

Adjustment of the necessary settings

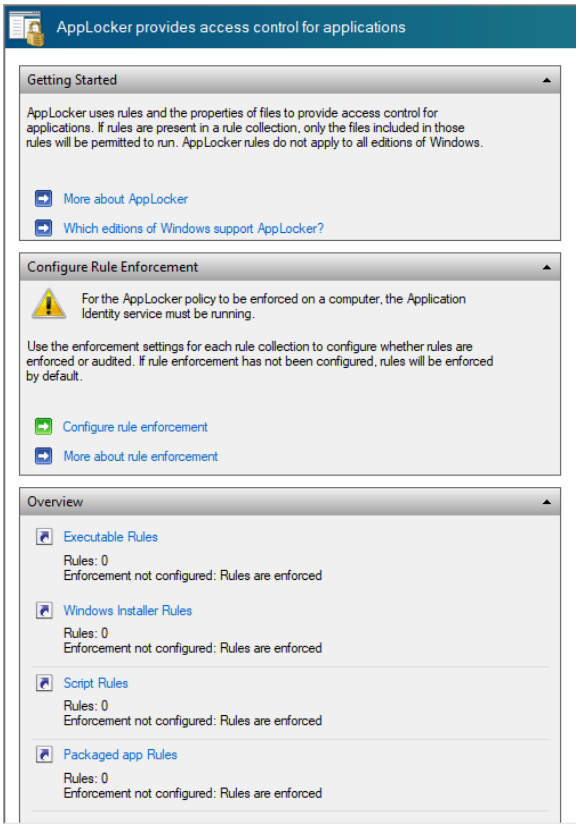
1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker".

Figure 4-14



2. Now define your corresponding rules. More information about the AppLocker and its configuration can be found under the following link: https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview.

Figure 4-15



4.6 Configuring Desktop Policies and Restrictions

Risk: Modification of system data, access to Internet Explorer, workstation, network environment

Weak point: Desktop - Access to applications

Solution: Prevent Windows applications and their properties from being accessed from the desktop.

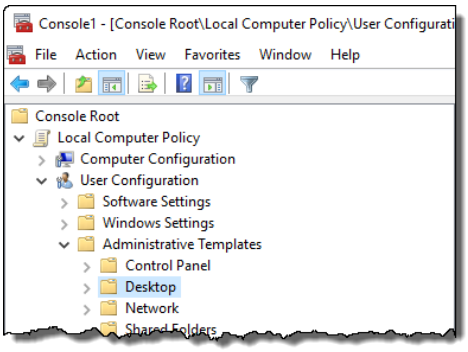
Function explanation

To avoid access to operating system functions or the Internet by the operator, it is necessary to change the default setting of the desktop policies.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Desktop"

Figure 4-16:



2. Change the following policies to "Enabled":

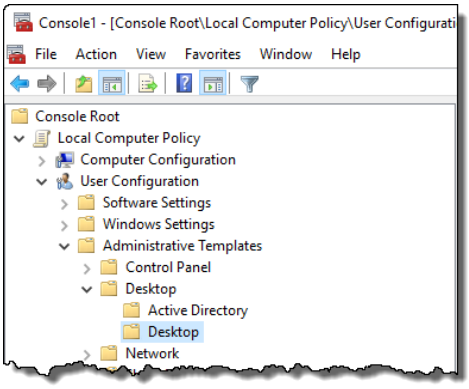
- "Prohibit User from manually redirecting Profile Folders"
- "Hide Internet Explorer icon on desktop"
- "Remove Computer icon on desktop"
- "Hide Network Locations icon on desktop"
- "Remove Properties from the Computer icon context menu"
- "Remove Properties from the Documents icon context menu"
- "Remove Properties from the Recycle Bin context menu"
- "Prevent adding, dragging, dropping and closing the Taskbar's Toolbars"
- "Prohibit adjusting desktop toolbars"

Figure 4-17

Setting	State	Comment
Active Directory		
Desktop		
Prohibit User from manually redirecting Profile Folders	Enabled	No
Hide and disable all items on the desktop	Not configured	No
Remove the Desktop Cleanup Wizard	Not configured	No
Hide Internet Explorer icon on desktop	Enabled	No
Remove Computer icon on the desktop	Enabled	No
Remove My Documents icon on the desktop	Not configured	No
Hide Network Locations icon on desktop	Enabled	No
Remove Properties from the Computer icon context menu	Enabled	No
Remove Properties from the Documents icon context menu	Not configured	No
Do not add shares of recently opened documents to Networ...	Not configured	No
Remove Recycle Bin icon from desktop	Enabled	No
Remove Properties from the Recycle Bin context menu	Enabled	No
Don't save settings at exit	Not configured	No
Turn off Aero Shake window minimizing mouse gesture	Not configured	No
Prevent adding, dragging, dropping and closing the Taskbar...	Enabled	No
Prohibit adjusting desktop toolbars	Enabled	No

3. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Desktop > Desktop".

Figure 4-18



4. Change the following policies to "Enabled":

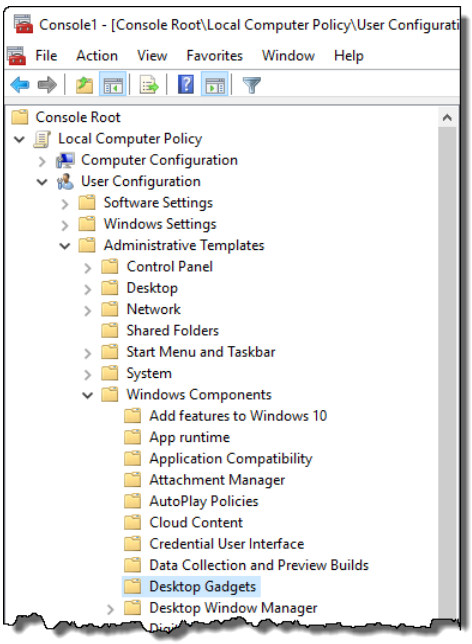
- "Disable Active Desktop"
- "Prohibit deleting items"
- "Prohibit editing items"

Figure 4-19

Setting	State	Comment
Enable Active Desktop	Not configured	No
Disable Active Desktop	Enabled	No
Prohibit changes	Not configured	No
Desktop Wallpaper	Not configured	No
Prohibit adding items	Not configured	No
Prohibit closing items	Not configured	No
Prohibit deleting items	Enabled	No
Prohibit editing items	Enabled	No
Disable all items	Not configured	No
Add/Delete items	Not configured	No
Allow only bitmapped wallpaper	Not configured	No

5. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Windows Components > Desktop Gadgets".

Figure 4-20



6. Change the following policy to "Enabled":

- "Disable desktop gadgets."

Figure 4-21

Setting	State	Comment
Turn off desktop gadgets	Enabled	No
Restrict unpacking and installation of gadgets that are not d...	Not configured	No
Turn Off user-installed desktop gadgets	Not configured	No

4.7 Start Menu and Taskbar - Configuring Policies

Risk: Change of system data/network environment, IPC lock/shutdown

Weak point: Start menu and taskbar - access to applications

Solution: Preventing access to Windows applications from the Start menu

Function explanation

Menu entries such as "Search", "Games" or "Music" are normally not required and should be deactivated.

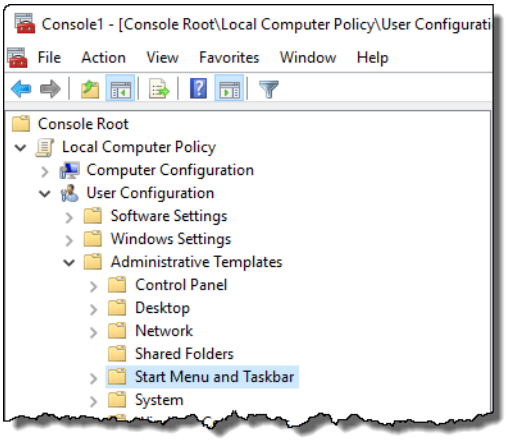
For security reasons, "Printers" and "Network Connections" should also not be offered ("Disable Programs in Settings Menu" policy).

Please note that some policies only deny access to the menu items. Some of the functions can be reached in other ways (e.g. under C:\Windows\system32).

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Start Menu and Taskbar".

Figure 4-22

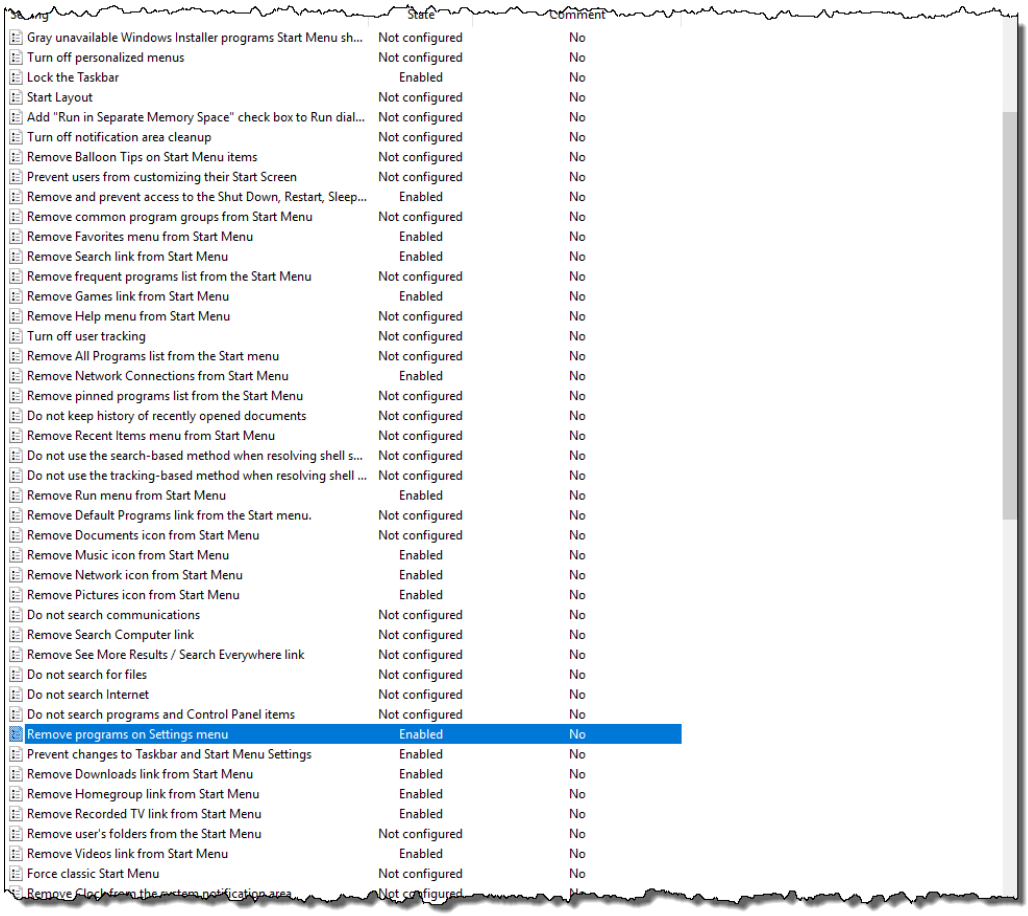


2. Change the following policies to "Enabled":

- "Lock the Taskbar"
- "Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands"
- "Remove Favorites menu from Start Menu"
- "Remove Search link from Start Menu"
- "Remove Games link from the Start Menu"
- "Remove Network Connections from Start Menu"
- "Remove Run menu from Start Menu"
- "Remove Music icon from Start Menu"
- Remove Network icon from Start Menu
- "Remove Pictures icon from Start Menu"
- "Remove programs on Settings menu"

- "Prevent changes to Taskbar and Start Menu Settings"
- "Remove Download link from Start Menu"
- "Remove Homegroup link from Start Menu"
- "Remove Recorded TV link from Start Menu"
- "Remove Videos link from Start Menu"

Figure 4-23



Setting	State	Comment
Gray unavailable Windows Installer programs Start Menu sh...	Not configured	No
Turn off personalized menus	Not configured	No
Lock the Taskbar	Enabled	No
Start Layout	Not configured	No
Add "Run in Separate Memory Space" check box to Run dial...	Not configured	No
Turn off notification area cleanup	Not configured	No
Remove Balloon Tips on Start Menu items	Not configured	No
Prevent users from customizing their Start Screen	Not configured	No
Remove and prevent access to the Shut Down, Restart, Sleep...	Enabled	No
Remove common program groups from Start Menu	Not configured	No
Remove Favorites menu from Start Menu	Enabled	No
Remove Search link from Start Menu	Enabled	No
Remove frequent programs list from the Start Menu	Not configured	No
Remove Games link from Start Menu	Enabled	No
Remove Help menu from Start Menu	Not configured	No
Turn off user tracking	Not configured	No
Remove All Programs list from the Start menu	Not configured	No
Remove Network Connections from Start Menu	Enabled	No
Remove pinned programs list from the Start Menu	Not configured	No
Do not keep history of recently opened documents	Not configured	No
Remove Recent Items menu from Start Menu	Not configured	No
Do not use the search-based method when resolving shell s...	Not configured	No
Do not use the tracking-based method when resolving shell ...	Not configured	No
Remove Run menu from Start Menu	Enabled	No
Remove Default Programs link from the Start menu.	Not configured	No
Remove Documents icon from Start Menu	Not configured	No
Remove Music icon from Start Menu	Enabled	No
Remove Network icon from Start Menu	Enabled	No
Remove Pictures icon from Start Menu	Enabled	No
Do not search communications	Not configured	No
Remove Search Computer link	Not configured	No
Remove See More Results / Search Everywhere link	Not configured	No
Do not search for files	Not configured	No
Do not search Internet	Not configured	No
Do not search programs and Control Panel items	Not configured	No
Remove programs on Settings menu	Enabled	No
Prevent changes to Taskbar and Start Menu Settings	Enabled	No
Remove Downloads link from Start Menu	Enabled	No
Remove Homegroup link from Start Menu	Enabled	No
Remove Recorded TV link from Start Menu	Enabled	No
Remove user's folders from the Start Menu	Not configured	No
Remove Videos link from Start Menu	Enabled	No
Force classic Start Menu	Not configured	No
Remove Clock from the system notification area	Not configured	No

4.8 Strg+Alt+Del configuring

Risk: Processes and services can be stopped, incorrect configuration of the IPCs

Weak point: Change password, Lock IPC, Access Task Manager

Solution: Restriction of functions according to <Ctrl+Alt+Del>

Function explanation

You can use the computer configuration to switch off the key combination <Ctrl+Alt+Del> for user logon.

(Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Interactive Login: No STRG + ALT + ENTF required).

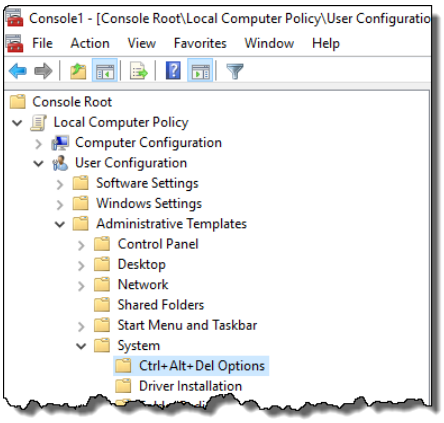
Alternatively, you can use the user configuration to set which actions are possible when pressing <Ctrl+Alt+Del> (e.g. no access to Task Manager).

CAUTION	**This setting prevents access to the Task Manager!** It is recommended not to change this computer configuration setting, as this setting applies to all users, including administrators. If you do enable this option, make sure that applications that may need to be shut down have their own shutdown routines. If the "Microsoft Management Console" has not been locked, you can also disable this option again to gain access to the task manager.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > System > Ctrl+Alt+Del Options".

Figure 4-24



2. Change the following policies to "Enabled":

- "Remove Change Password"
- "Remove Lock Computer"
- "Remove Task Manager"

Figure 4-25:

Setting	State	Comment
Remove Change Password	Enabled	No
Remove Lock Computer	Enabled	No
Remove Task Manager	Enabled	No
Remove Logoff	Not configured	No

4.9 Prevent access to Control Panel

Risk: Processes and services can be stopped, incorrect configuration of the IPCs

Weak point: Changing the System Parameters in Control Panel

Solution: Prevent access to Control Panel

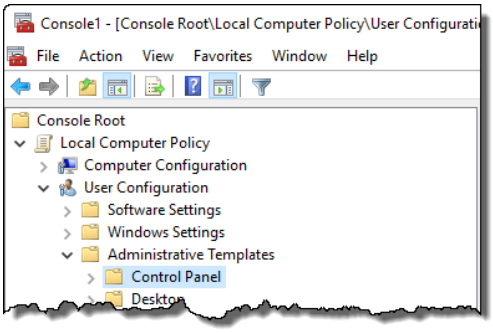
Function explanation

The Control Panel can be used to make unwanted changes to the system, such as network connections, uninstalling programs, etc. Access to the Control Panel should therefore be prevented.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Control Panel".

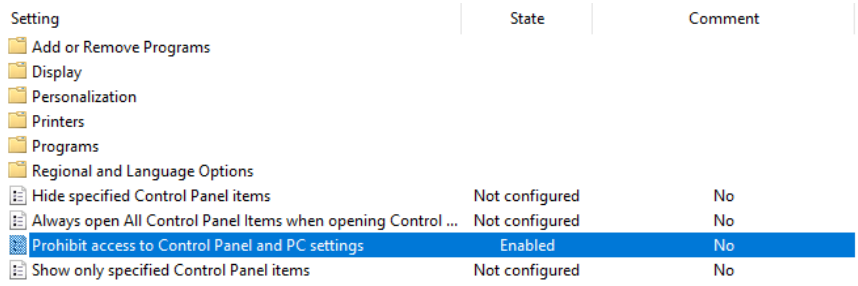
Figure 4-26



2. Change the following policy to "Enabled":

- "Prohibit access to Control Panel and PC settings"

Figure 4-27



4.10 Configure removable disk access

Risk: Infect IPC with malware, unwanted installation of programs

Weak point: Access to removable media (e.g. USB sticks)

Solution: Preventing access to removable media

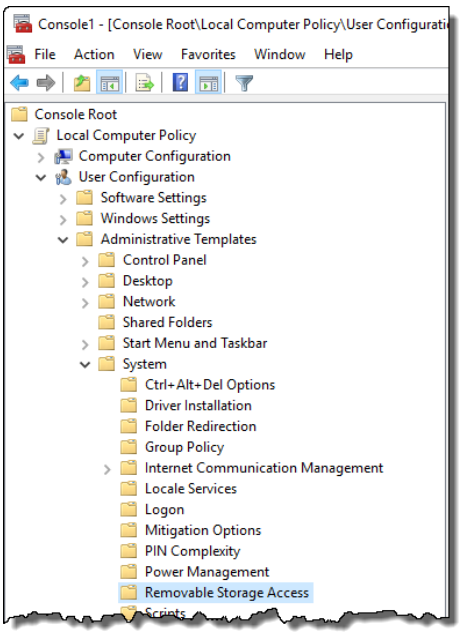
Function explanation

By inserting a USB stick, the IPC can be infected with a malicious program. Therefore, it is recommended to deny access to various removable disks in the Group Policy settings. It is possible to either deny read and/or write access or to deny "any access".

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2. Open the following path:
"User Configuration > Administrative Templates > System > Removable Storage Access".

Figure 4-28



2. Change the following policies to "Enabled":

- "Removable Disks: Deny write access"
- "Removable Disks: Deny write access"
- "All Removable storage classes: Deny all access"
- "WPD Devices: Deny read access"
- "WPD-Devices: Deny write access"

Figure 4-29

Setting	State	Comment
Set time (in seconds) to force reboot	Not configured	No
CD and DVD: Deny read access	Not configured	No
CD and DVD: Deny write access	Not configured	No
Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny read access	Not configured	No
Floppy Drives: Deny write access	Not configured	No
Removable Disks: Deny read access	Enabled	No
Removable Disks: Deny write access	Enabled	No
All Removable Storage classes: Deny all access	Enabled	No
Tape Drives: Deny read access	Not configured	No
Tape Drives: Deny write access	Not configured	No
WPD Devices: Deny read access	Enabled	No
WPD Devices: Deny write access	Enabled	No

4.11 Disable Autoplay function

Risk: Infect IPC with malware, unwanted installation of programs

Weak point: Automatic execution of software (Autoplay function)

Solution: Deactivating Autoplay or Autorun

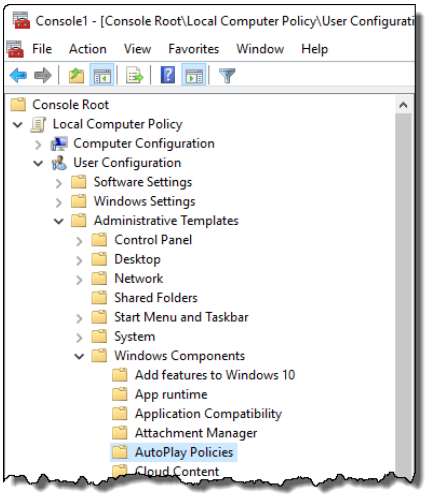
Function explanation

USB sticks and external hard drives may contain an autoplay file ("autorun.inf"). In this way, viruses, for example, could infect the system. The following table shows how to disable the Autoplay feature and AutoRun ("AutoRun Default Behavior" policy).

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Windows Components > AutoPlay Policies".

Figure 4-30



2. Change the following policies to "Enabled":

- "Turn off Autoplay"
- "Set the default behavior for AutoRun"

Figure 4-31

Setting	State	Comment
Turn off Autoplay	Enabled	No
Prevent AutoPlay from remembering user choices.	Not configured	No
Disallow Autoplay for non-volume devices	Not configured	No
Set the default behavior for AutoRun	Enabled	No

4.12 Prevent removable disk access for all installations

Risk: Infect IPC with malware, unwanted installation of programs

Weak point: Installations of removable media

Solution: Disable removable disk installation

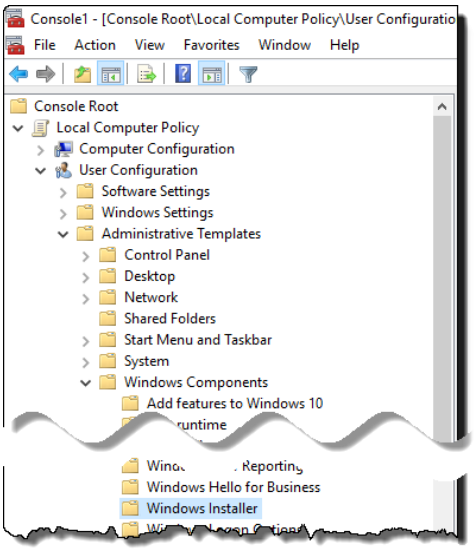
Function explanation

If it is not possible for you to prohibit access to USB media in general (see section 4.10), you should prevent software from being installed from removable media. This allows you to prevent malware or other unwanted programs from removable media from being installed on your IPC.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Windows Components > Windows Installer".

Figure 4-32



2. Change the following policy to "Enabled":

- "Prevent removable media source for any installation"

Figure 4-33

Setting	State	Comment
Always install with elevated privileges	Not configured	No
Prevent removable media source for any installation	Enabled	No
Prohibit rollback	Not configured	No
Specify the order in which Windows Installer searches for ins...	Not configured	No

4.13 Deny access to Microsoft Management Console

Risk: Change system configuration (group policies, firewall settings, etc.)

Weak point: Access to MMC (Microsoft Management Console)

Solution: Deny access to MMC (Microsoft Management Console)

Function explanation

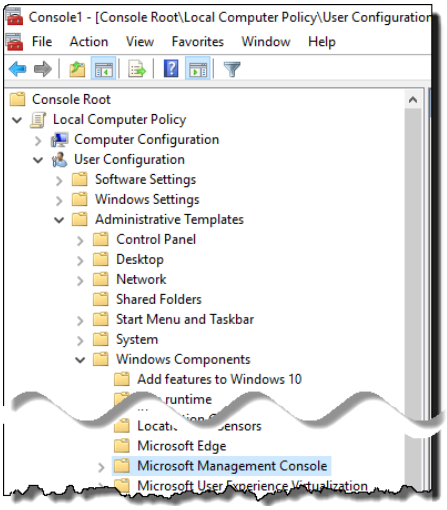
The graphical user interface "Microsoft Management Console" (MMC) is used to manage computers and users. You can configure if and how the MMC can be used.

CAUTION	**With this setting you deny any IPC user access to the Microsoft Management Console!** You may need to restart your computer if you want to make changes to Local Computer Policies or other settings in options that are already disabled (e.g. Control Center). Disable access to this console only if you are absolutely sure that the settings are complete and correct. Later change requests cannot be carried out. For this a new installation is necessary.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Windows Components > Microsoft Management Console".

Figure 4-34



2. Change the following policies to "Enabled":

- "Restrict the user from entering author mode"
- "Restrict users to the explicitly permitted list of snap-ins"

Figure 4-35

Setting	State	Comment
Restricted/Permitted snap-ins		
Restrict the user from entering author mode	Enabled	No
Restrict users to the explicitly permitted list of snap-ins	Enabled	No

4.14 Deny access to recovery options

Risk: Unwanted system changes

Weak point: Access to recovery options

Solution: Restricting recovery options

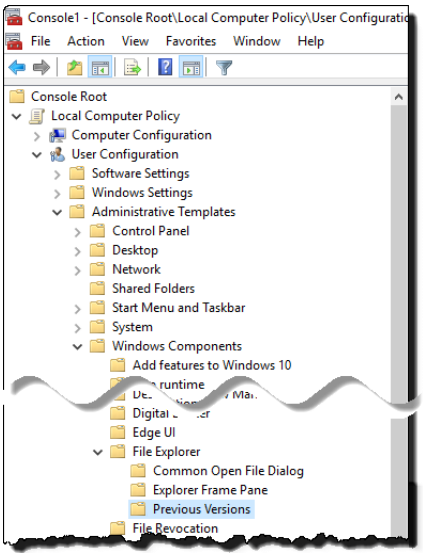
Function explanation

By disabling the recovery options of the operating system, it is no longer possible to return to previous states of the operating system. This prevents users from undoing changes to the system.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Windows Components > File Explorer > Previous Versions".

Figure 4-36



2. Change the following policies to "Enabled":

- "Prevent restoring previous versions from backups"
- "Prevent restoring local previous versions"
- "Prevent restoring remote previous versions"

Figure 4-37

Setting	State	Comment
Prevent restoring previous versions from backups	Enabled	No
Hide previous versions list for local files	Not configured	No
Prevent restoring local previous versions	Enabled	No
Hide previous versions list for remote files	Not configured	No
Prevent restoring remote previous versions	Enabled	No
Hide previous versions of files on backup location	Not configured	No

4.15 Deny access to paths when searching

Risk: Unwanted access to applications

Weak point: Access to paths when searching

Solution: Deny access to paths when searching

Function explanation

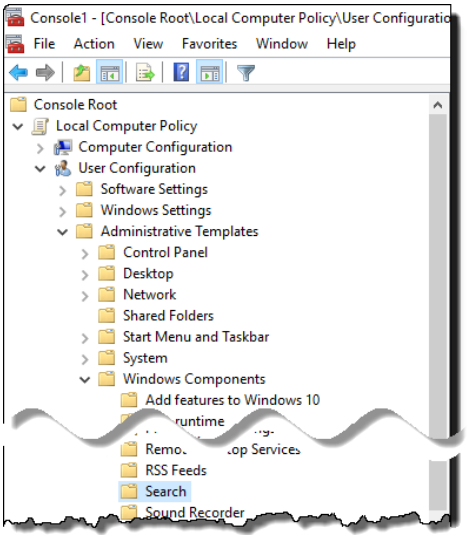
To deny access to system paths (for example, "C:\Windows\system32"), you can explicitly specify which paths are excluded from the search.

Note This setting is made in the user configuration. Thus, this policy applies to both the administrator account and the restricted user accounts.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2. Open the following path:
   "User Configuration > Administrative Templates > Windows Components > Search".

Figure 4-38



2. Change the following policy to "Enabled":

- "Prevent indexing certain paths"

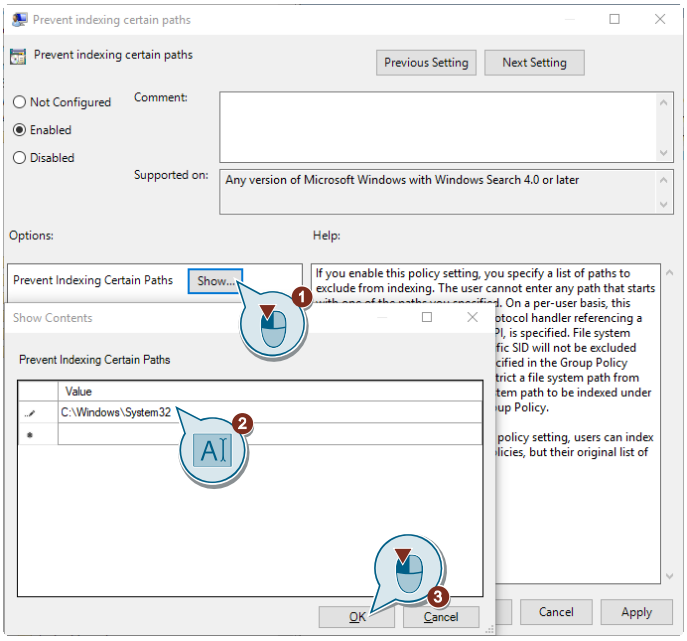
Figure 4-39

Setting	State	Comment
Default excluded paths	Not configured	No
Default indexed paths	Not configured	No
Turn off storage and display of search history	Not configured	No
Prevent adding UNC locations to index from Control Panel	Not configured	No
Prevent indexing certain paths	Enabled	No
Prevent customization of indexed locations in Control Panel	Not configured	No

3. In the settings of this policy, specify which search paths you want to exclude. Click on the "Show" button (1) and enter the desired paths in the window that opens (2). Confirm the entries by clicking "OK"(3).

4.15 Deny access to paths when searching

Figure 4-40



4.16 Deny access to certain or all drives

Risk: Unauthorized access to system-relevant information, manipulation possibilities

Weak point: Installations of removable media

Solution: Restrict access to network and specific drives

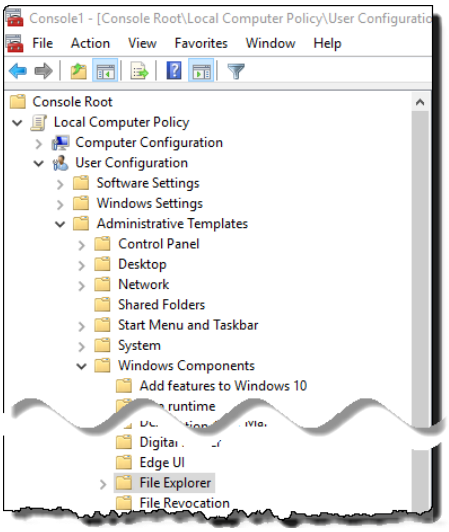
Function explanation

You can restrict access to drives to prevent manipulation.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Windows Components > File Explorer".

Figure 4-41



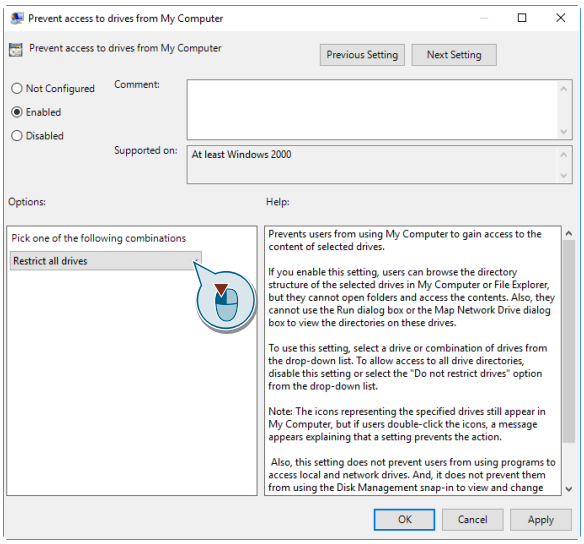
2. Change the following policies to "Enabled":

- "No Entire Network in Network Locations"
- "Remove Search button from File Explorer"
- "Prevent access to drives from My Computer"

  To enable this option, you must also specify in the window that opens which drives you want to disable access to.

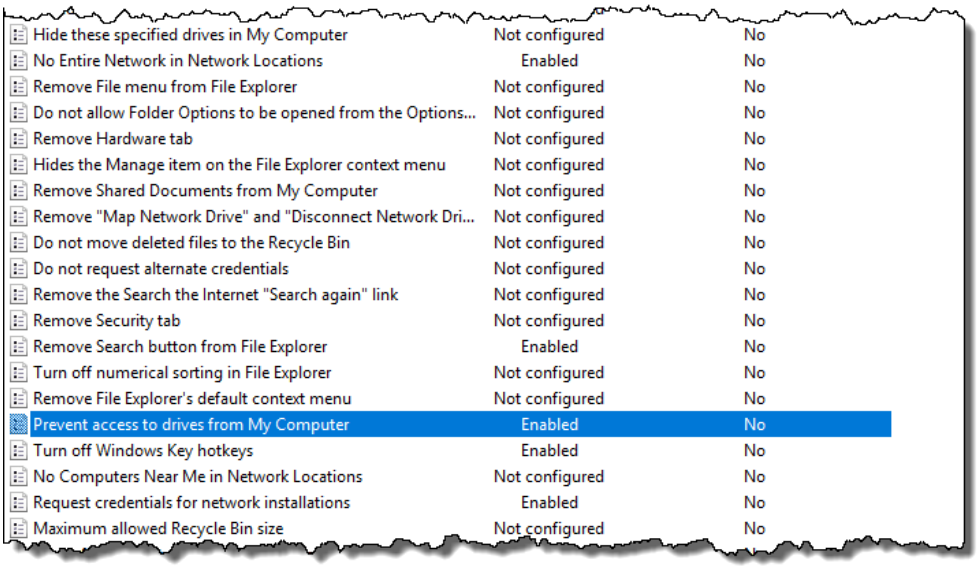
4.16 Deny access to certain or all drives

Figure 4-42



- "Turn off Windows Key hotkeys"
- "Request credentials for network installations"

Figure 4-43



5 Security settings for IPCs with networkconnection

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

This section lists the settings that apply to this application scenario.

5.1 Enable and configure Windows Firewall

Risk: Sensitive process data can be viewed

Weak point: Windows Firewall switched off / not configured

Solution: Enable and configure Windows Firewall

Function explanation

It is strongly recommended to leave the Windows Firewall enabled! 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 temporarily allow ping requirements.

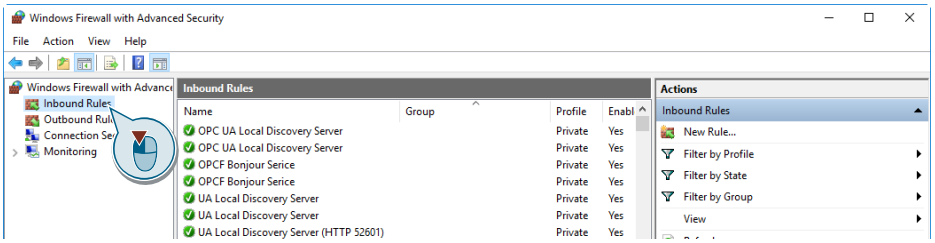
Adjustment of the necessary settings

1. Open the Windows Firewall configuration menu. Enter the term "Firewall" in the Windows search and confirm with "Enter" ("Return").
2. Click on the menu item "Advanced settings".

Figure 5-1

3. Select the entry "Inbound Rules".

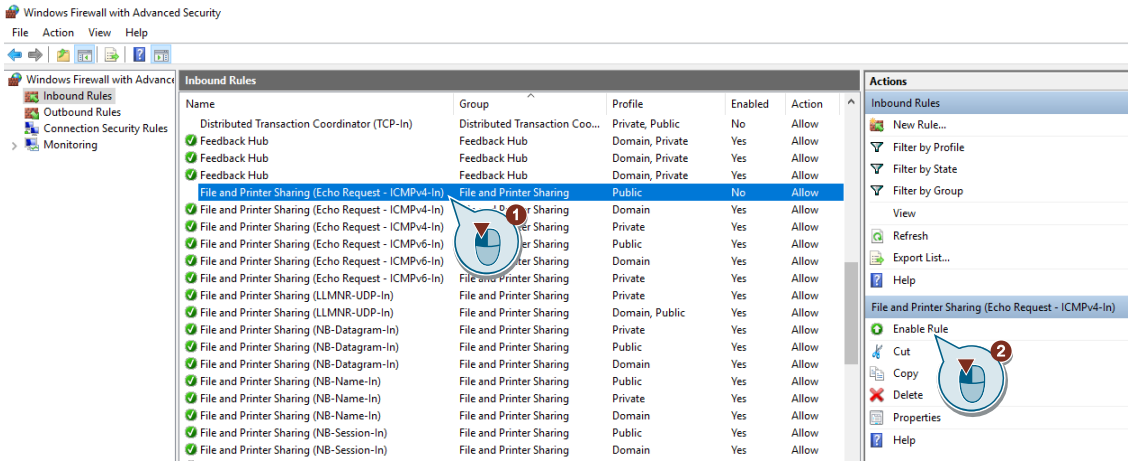
Figure 5-2



4. Select the list entry "File and printer sharing (echo request - ICMPv4 incoming)" -> Profile "Public" ("File and Printer Sharing (Echo Request - ICMPv4-In)" -> Profile "Public") (1). Activate the rule using the action ("Enable Rule") (2).

Note: It is possible that these rules are already activated in your firewall. You can recognize this by the green tick in front of the name of the rules. In this case, you do not need to change the rule.

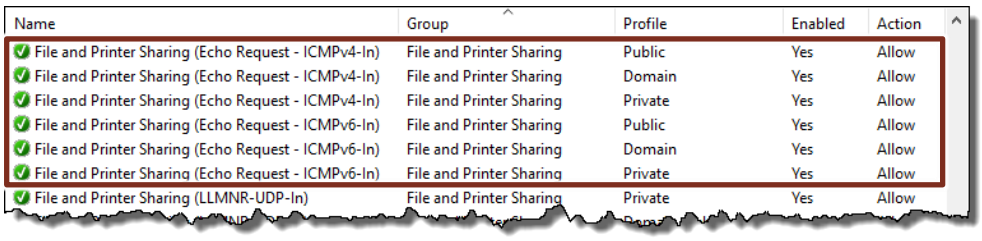
Figure 5-3



5. Repeat step 4 for the entries:

- File and printer sharing (echo request -ICMPv4 incoming) -> Profile "Domain" ("File and Printer Sharing (echo request - ICMPv4-In)" -> Profile "Domain")
- File and Printer Sharing (echo request - ICMPv4 incoming) -> Profile "Private" ("File and Printer Sharing (echo request - ICMPv4-In)" -> Profile "Private")
- File and Printer Sharing (echo request -ICMPv6 incoming) -> Profile "Public" ("File and Printer Sharing (echo request - ICMPv6-In)" -> Profile "Public")
- File and printer sharing (echo request - ICMPv6 incoming) -> Profile "Domain" ("File and Printer Sharing (Echo Request - ICMPv4-In)" -> Profile "Domain")
- File and Printer Sharing (echo request -ICMPv6 incoming) -> Profile "Private" ("File and Printer Sharing (echo request - ICMPv4-In)" -> Profile "Private")

Figure 5-4



5.2 Configure password policies correctly

Risk: Hacker attacks by online scanners, unauthorized accesses

Weak point: Use default passwords

Solution: Configure password policies correctly

Function explanation

By configuring the password policies, the user is "forced" to follow the appropriate rules for assigning his password. These guidelines counter misuse.

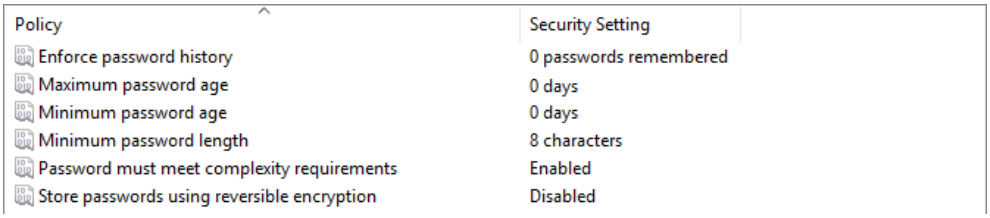
Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Windows Settings > Security Settings > Account Policies > Password Policy".
2. Change the account policy settings recommended for IPCs using the following table/illustration.

Table 5-1

Guideline	Safety setting	
	Default values:	Recommended settings:
Password must meet complexity requirements	Enabled / disabled	Enabled
Enforce password history	24 / 0 saved Passwords	0 saved Passwords
Store passwords with reversible encryption	Disabled	Disabled
Maximum password age (days)	42	0
Minimum password length	7 / 0 characters	8
Minimum password age	1 / 0 Days	0

Figure 5-5



5.3 Deny access to network connections

Risk: Unauthorized modification of LAN connections, unauthorized removal/addition of components

Weak point: Free access to the network connections

Solution: Deny access to network connections

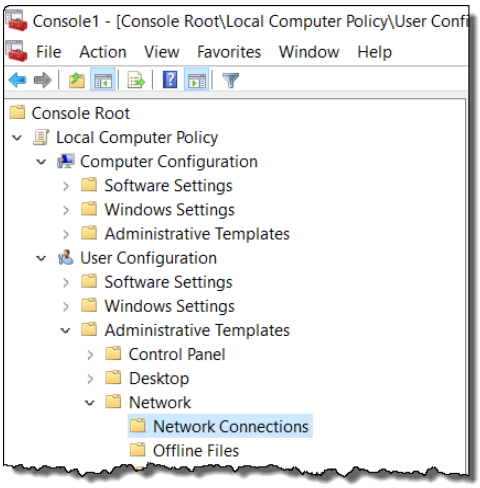
Function explanation

Denying access to network connections limits the possibilities for unwanted installation of malware on the IPC.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2. Open the following path:
"User Configuration > Administrative Templates > Network > Network Connections".

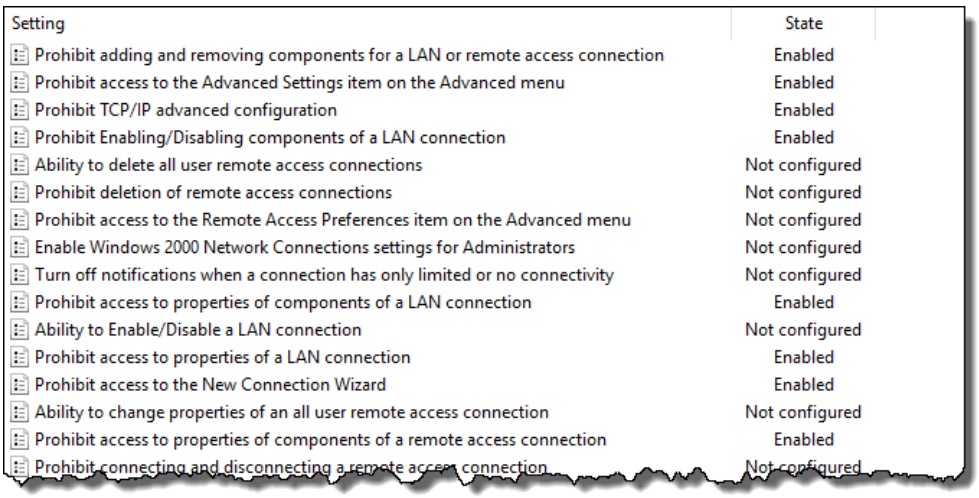
Figure 5-6



2. Change the following policies to "Enabled":

- "Prohibit adding and removing components for a LAN or remote access connection"
- "Prohibit access to the Advanced Settings item on the Advanced menu"
- "Prohibit TCP/IP advanced configuration"
- "Prohibit Enabling/Disabling components of a LAN connection"
- "Prohibit Enabling/Disabling components of a LAN connection"
- "Prohibit access to properties of a LAN connection"
- "Prohibit access to the New Connection Wizard"
- "Prohibit access to properties of components of a remote access connection"

Figure 5-7



Setting	State
Prohibit adding and removing components for a LAN or remote access connection	Enabled
Prohibit access to the Advanced Settings item on the Advanced menu	Enabled
Prohibit TCP/IP advanced configuration	Enabled
Prohibit Enabling/Disabling components of a LAN connection	Enabled
Ability to delete all user remote access connections	Not configured
Prohibit deletion of remote access connections	Not configured
Prohibit access to the Remote Access Preferences item on the Advanced menu	Not configured
Enable Windows 2000 Network Connections settings for Administrators	Not configured
Turn off notifications when a connection has only limited or no connectivity	Not configured
Prohibit access to properties of components of a LAN connection	Enabled
Ability to Enable/Disable a LAN connection	Not configured
Prohibit access to properties of a LAN connection	Enabled
Prohibit access to the New Connection Wizard	Enabled
Ability to change properties of an all user remote access connection	Not configured
Prohibit access to properties of components of a remote access connection	Enabled
Prohibit connecting and disconnecting a remote access connection	Not configured

5.4 Restricting Internet Access

Risk: Free access to the Internet

Weak point: Free access to Internet communication management

Solution: Restricting Internet Access

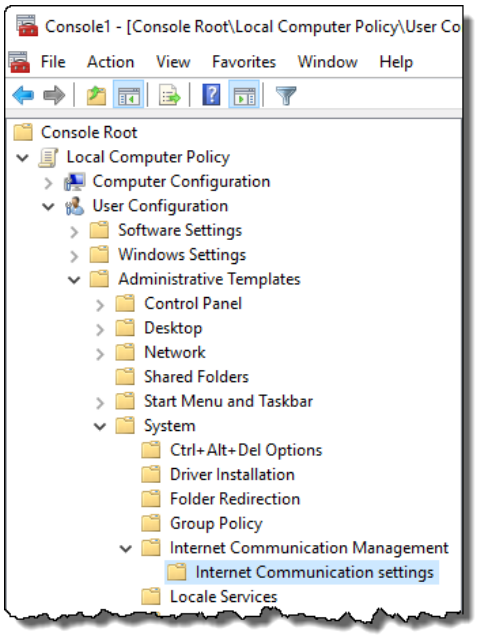
Function explanation

The denial of Internet access limits the possibilities for unwanted installation of malware on the IPC.

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication settings".

Figure 5-8



2. Change the following policies to "Enabled":

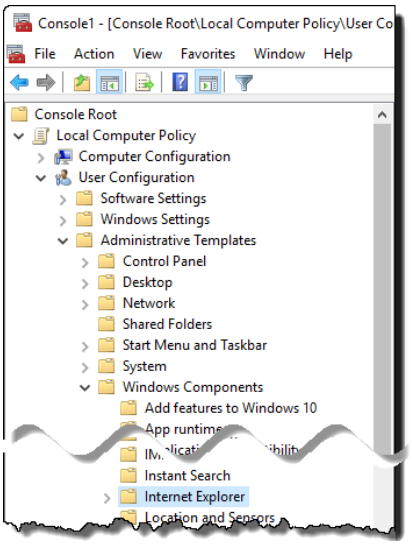
- "Turn off Help Ratings"
- "Turn off Help Experience Improvement Program"
- "Turn off Windows Online"
- "Turn off Internet File Association service"
- "Turn off Internet download for Web publishing and online ordering wizards"
- Turn off the "Order Prints" picture task"
- "Turn off the "Publish to Web" task for files and folders"
- "Turn off the Windows Messenger Customer Experience Improvement Program"

Figure 5-9

Setting	State	Comment
Turn off Help Ratings	Enabled	No
Turn off Help Experience Improvement Program	Enabled	No
Turn off Windows Online	Enabled	No
Turn off handwriting recognition error reporting	Not configured	No
Turn off printing over HTTP	Not configured	No
Turn off downloading of print drivers over HTTP	Not configured	No
Turn off Internet File Association service	Enabled	No
Turn off access to the Store	Not configured	No
Turn off Internet download for Web publishing and online ordering wizards	Enabled	No
Turn off the "Order Prints" picture task	Enabled	No
Turn off the "Publish to Web" task for files and folders	Enabled	No
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled	No
Turn off handwriting personalization data sharing	Not configured	No

3. Open the "Microsoft Management Console" as described in section 3.1.2. Open the following path:
"User Configuration > Administrative Template > Windows Components > Internet Explorer".

Figure 5-10



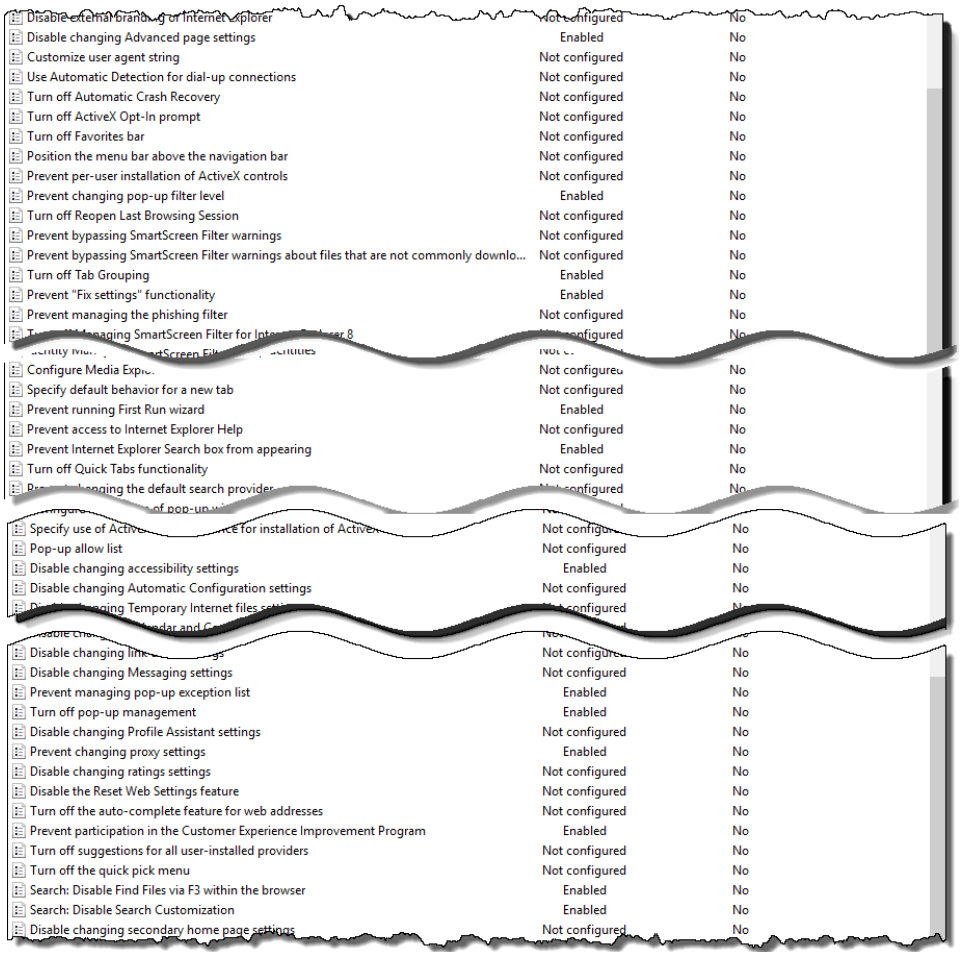
Note You can block other browsers and applications using the AppLocker. See section 4.5.

4. Change the following policies to "Enabled":

- "Disable changing Advanced page settings"
- "Prevent changing pop-up filter level"
- "Turn off Tab Grouping"
- "Prevent "Fix settings" functionality"
- "Prevent running First Run wizard"
- "Prevent Internet Explorer Search box from appearing"
- "Disable changing accessibility settings"
- "Prevent managing pop-up exception list"
- "Turn off pop-up management"

- "Prevent changing proxy settings"
- "Prevent participation in the Customer Experience Improvement Program"
- "Search: Disable Find Files via F3 within the browser"
- "Search: Disable Search Customization"

Figure 5-11



5.5 Preventing access to Windows Update

Risk: Process stop possible

Weak point: Access to update

Solution: Preventing access to Windows Update

Function explanation

If system updates are performed automatically, an unwanted restart of the system may occur.

You can prevent this by configuring Windows Updates not to run automatically.

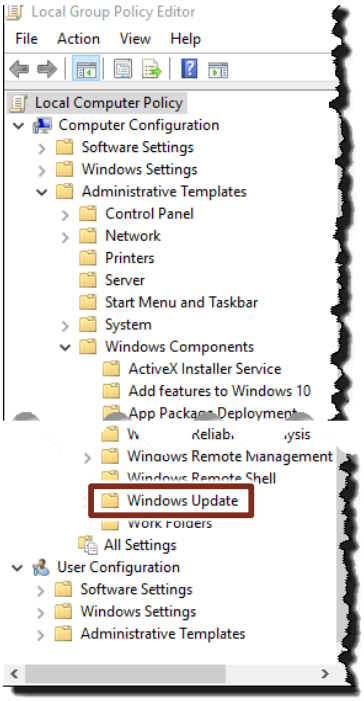
Note

If you want to have full control over Windows updates and only want to selectively install certain updates, you can set up a WSUS server. The following article explains how this works:
https://support.industry.siemens.com/cs/de/en/view/109754089

Adjustment of the necessary settings

1. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "Computer Configuration > Administrative Templates > Windows Components > Windows Update"

Figure 5-12



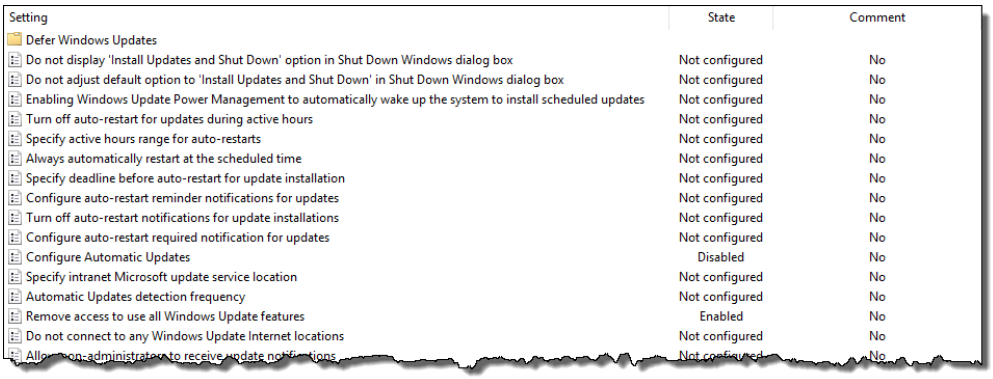
2. Change the following policy to "Disabled":

- "Configure Automatic Updates"

3. Change the following policy to "Enabled":

- "Remove access to use all Windows Update features"

Figure 5-13



Setting	State	Comment
Defer Windows Updates		
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Not configured	No
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Not configured	No
Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates	Not configured	No
Turn off auto-restart for updates during active hours	Not configured	No
Specify active hours range for auto-restarts	Not configured	No
Always automatically restart at the scheduled time	Not configured	No
Specify deadline before auto-restart for update installation	Not configured	No
Configure auto-restart reminder notifications for updates	Not configured	No
Turn off auto-restart notifications for update installations	Not configured	No
Configure auto-restart required notification for updates	Not configured	No
Configure Automatic Updates	Disabled	No
Specify intranet Microsoft update service location	Not configured	No
Automatic Updates detection frequency	Not configured	No
Remove access to use all Windows Update features	Enabled	No
Do not connect to any Windows Update Internet locations	Not configured	No
Allow non-administrators to receive update notifications	Not configured	No

5.6 Tunneling connection with IPSec (VPN IPSec)

Risk: Unsafe connection - sensitive process data can be viewed

Weak point: Remote maintenance via VPN is configured insecurely

Solution: Using a Virtual Private Network (VPN) that is configured correctly

Function explanation

With a Virtual Private Network (VPN), a public network (e.g. Internet) is used as a transit network for the transmission of private data.

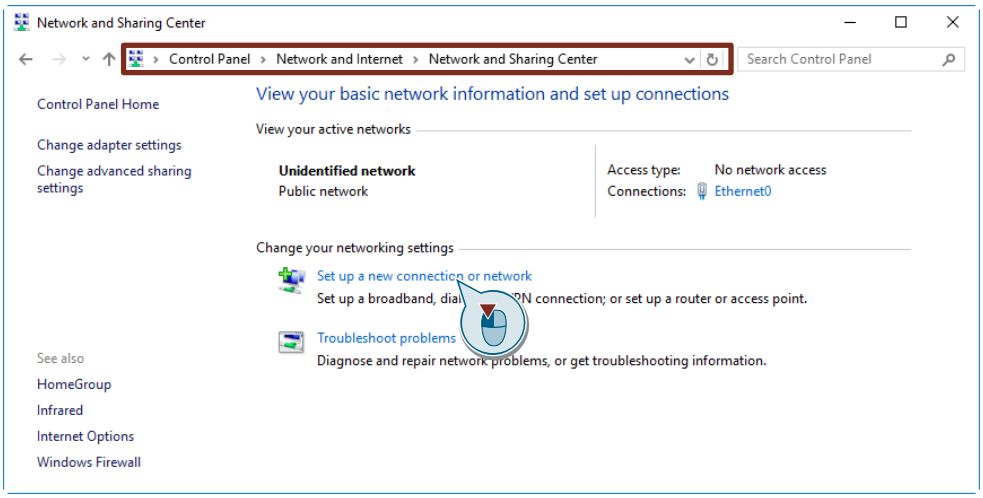
The IPSec protocol enables manufacturer-independent, secure and protected data exchange via IP networks. IPSec uses the tunneling concept. The data transmission between the tunnel endpoints (sender and receiver) cannot be viewed by unauthorized persons due to the encryption.

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

Adjustment of the necessary settings

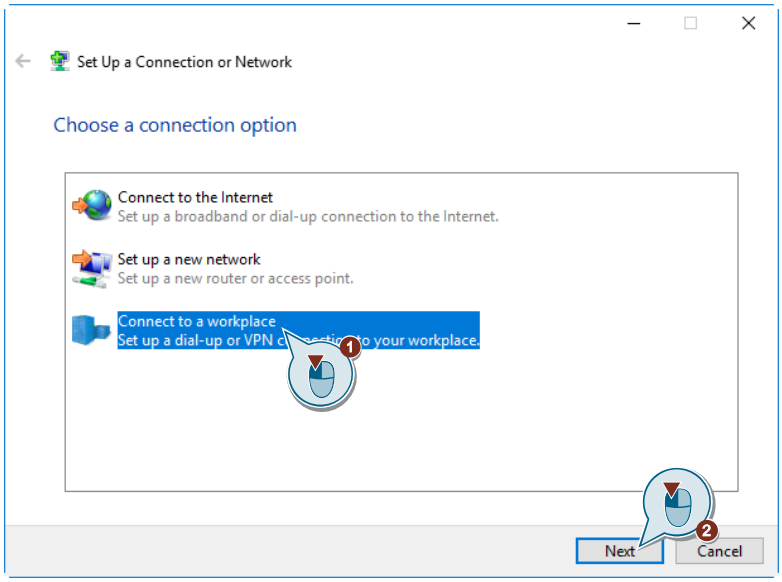
1. Open the Network and Sharing Center by entering the term "Control Panel" in the Windows search and confirm with "Enter". You can find it under the path "Control Panel > Network and Internet > Network and Sharing Center" Click on "Set up a new connection or network".

Figure 5-14



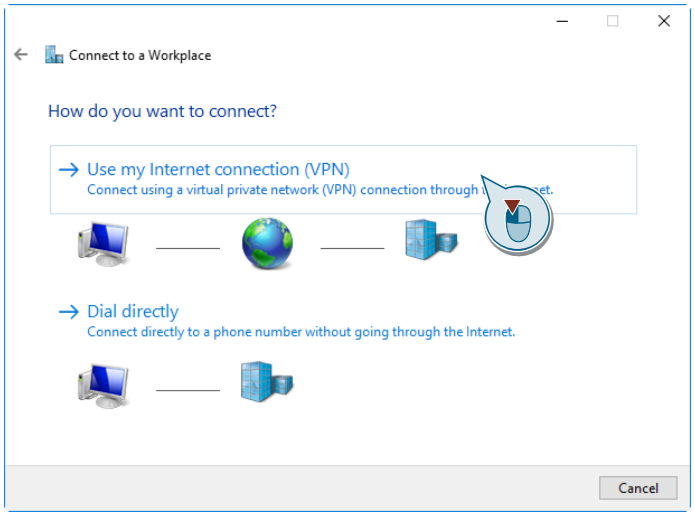
2. In the following dialog select the entry "Connect to a workplace" (1). Click on the button "Next" (2).

Figure 5-15



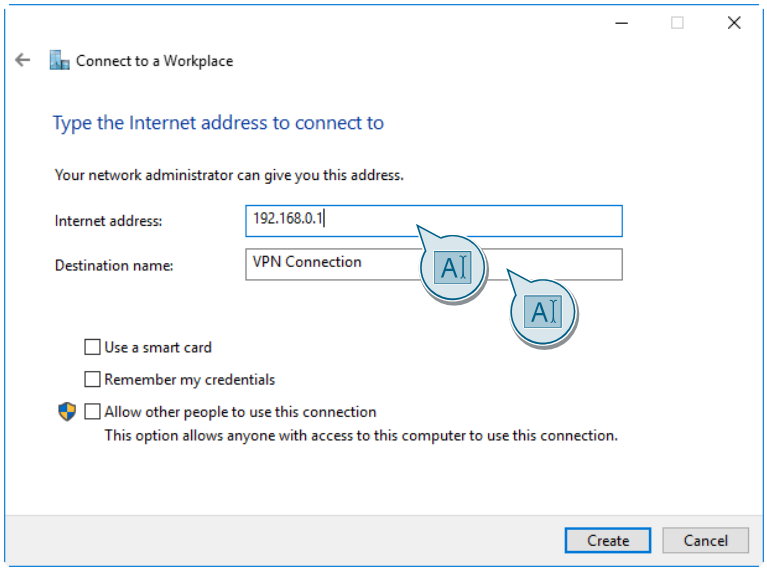
3. Select the option "Use my Internet connection (VPN)".

Figure 5-16



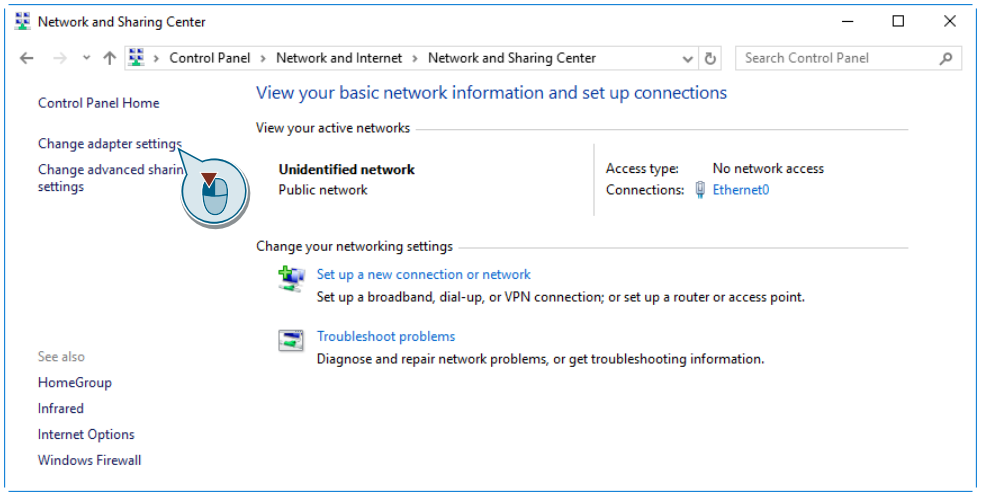
4. Enter the corresponding "Internet address" and the "Destination name". If the computer does not yet have an Internet connection, you will be offered to set up an Internet connection.

Figure 5-17



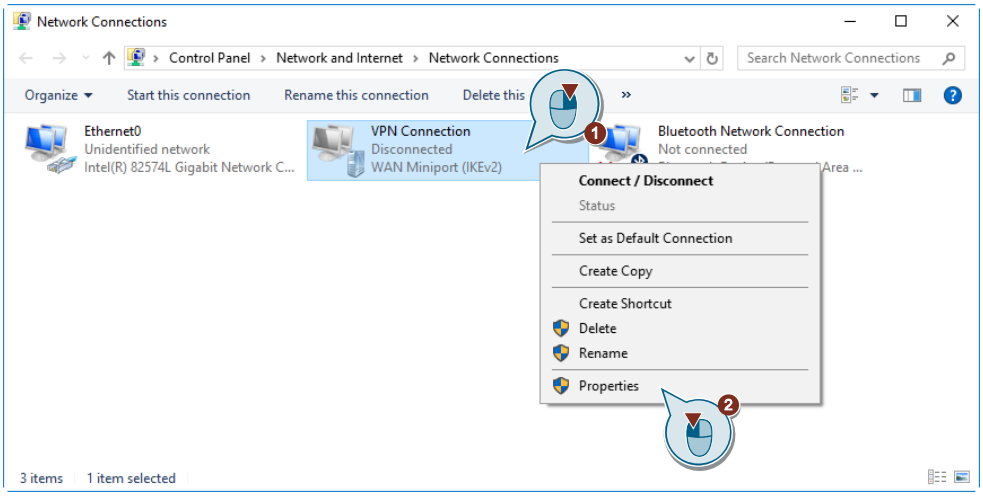
5. Open the "Network and Sharing Center" again as described at the beginning of this section. Click the "Change adapter settings" entry.

Figure 5-18



6. Open the context menu with a right click on the VPN connection (1). Then click on the menu command "Properties" (2).

Figure 5-19

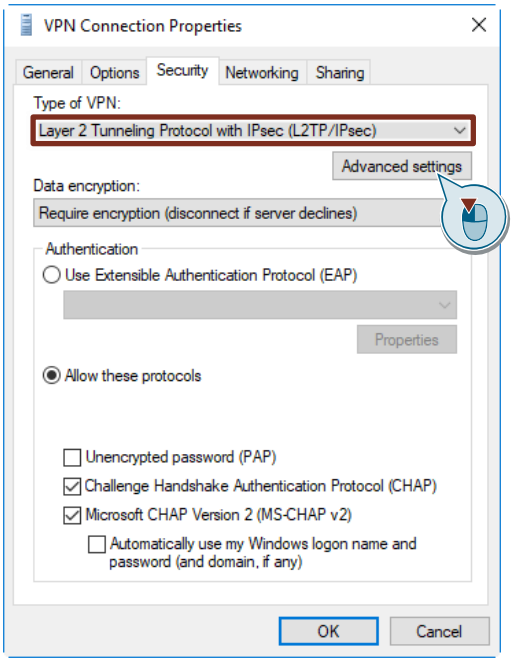


7. Switch to the Security tab and select the VPN type: "Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)". Adjust the other settings in this window to suit your requirements.
8. Now, click the "Advanced settings".

Note

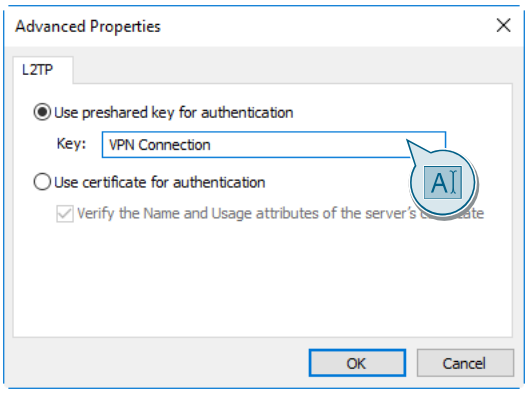
More detailed information on VPN connections can be found under the link: https://support.microsoft.com/de-de/help/20510/windows-10-connect-to-vpn.

Figure 5-20



9. Enter the name of your VPN connection (in the example "VPN Connection") in the entry field "Key".

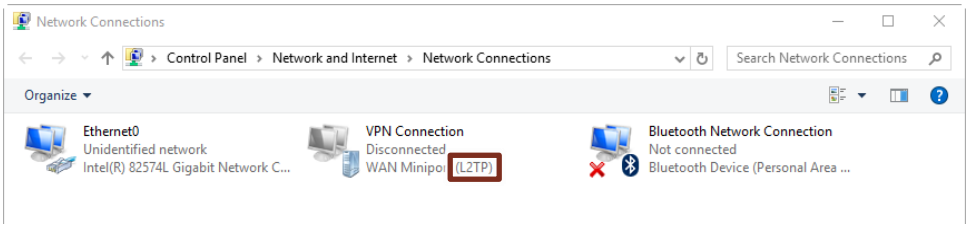
Figure 5-21



10. Click "OK" to confirm both dialogs.

    Now the VPN type "L2TP" is displayed in the connection.

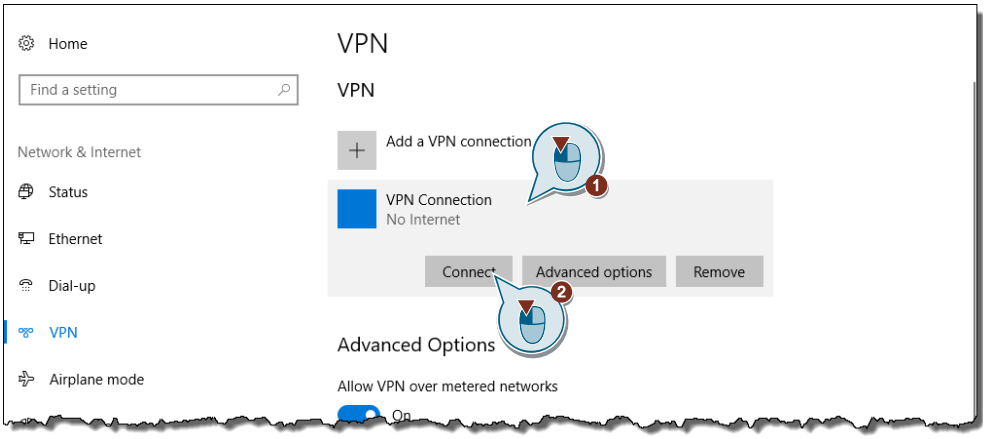
Figure 5-22



11. Open the VPN settings by entering the term "VPN" in the Windows search.

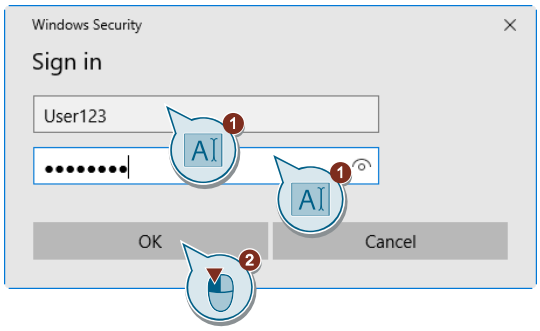
    Click on the newly created connection (1) and then on the "Connect" button that appears below (2).

Figure 5-23



12. Enter your credentials to connect to the VPN server in the dialog box (1) and confirm with the OK button (2) to connect to the server.

Figure 5-24



Note Note that only the settings for the "VPN Client" are described here. On the "VPN server", "Incoming connections" must be allowed for the user used here.

5.7 Useful Configuration for Remote Desktop

Risk: Invalid access rights

Weak point: Unsecure remote desktop connection

Solution: Safe configuration of the remote desktop

Function explanation

To be able to use the remote desktop connection for a restricted user account (without administrator rights), the corresponding user must be added under "Select user...".

You can use Group Policy to extend the settings for Remote Desktop Services. By default, the listed settings are not configured.

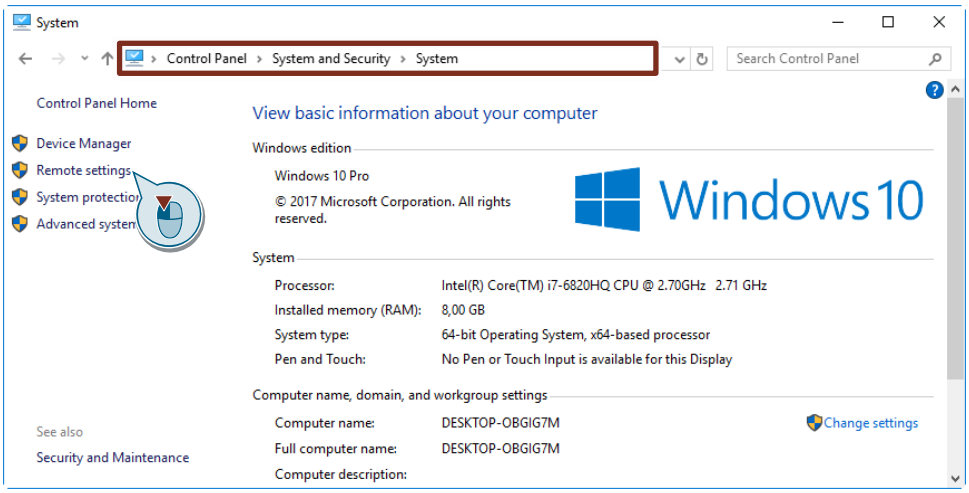
To ensure a higher security of the connection, it is recommended to use the NTLM protocol and not to allow storing passwords.

How to enable these options is explained in the section "Advanced Remote Desktop Settings".

Adjustment of the necessary settings

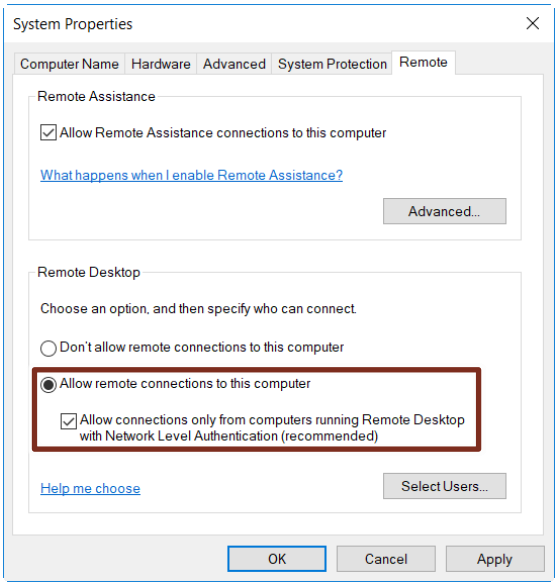
1. Open the "System Properties > Remote" dialog by clicking on the "Remote settings" button. You can find them via the path "Start > Control Panel > System and Security > System"

Figure 5-25



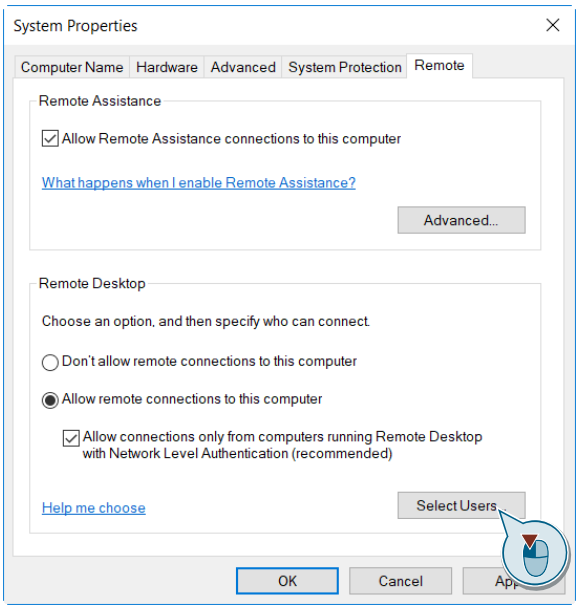
2. Select here the option "Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)"

Figure 5-26



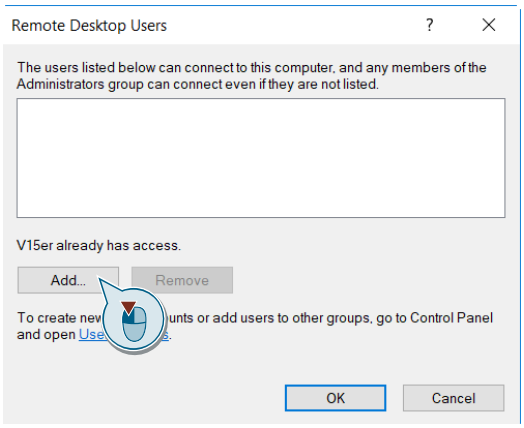
3. Open via the button "Select Users...".
The dialog box "Remote Desktop Users"

Figure 5-27



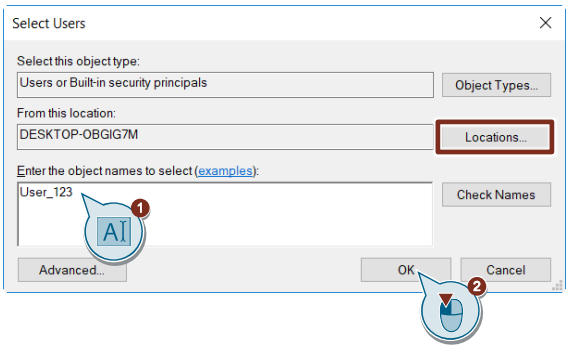
4. Open the "Select Users" dialog box by clicking the "Add..." button. ("Add...").

Figure 5-28



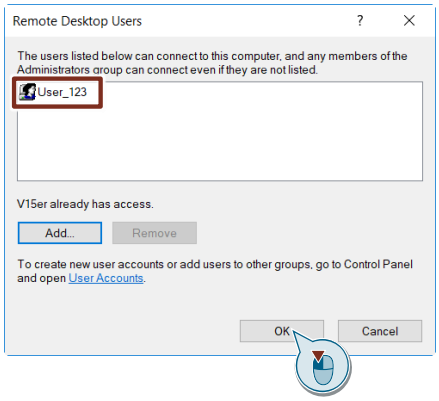
5. Via the "Paths..." button ("Locations...") you specify the computer from which this PC can be accessed via remote connection. Enter the name of a user existing on the target system in the input field (1) and confirm the selection with the "OK" button (2).

Figure 5-29



6. The user is then listed as a Permitted User in the "Remote Desktop Users" dialog box. Close the dialogs with "OK".

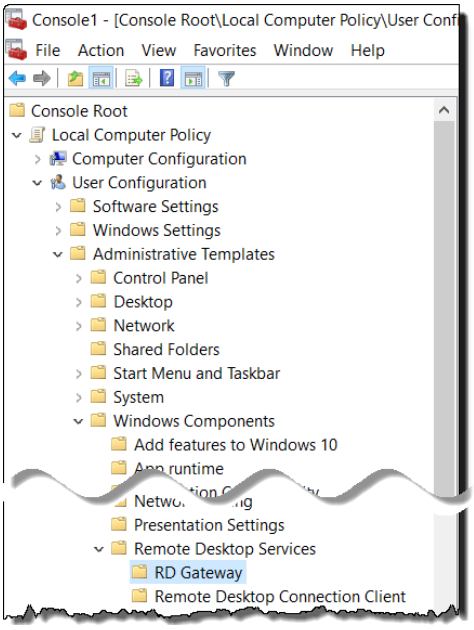
Figure 5-30



Note Further information can be found under: https://support.microsoft.com/de-de/hub/4338813/windows-help?os=windows-10

7. Open the "Microsoft Management Console" as described in section 3.1.2.
   Open the following path:
   "User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > RD Gateway"

Figure 5-31



8. Change the following policy to "Enabled":

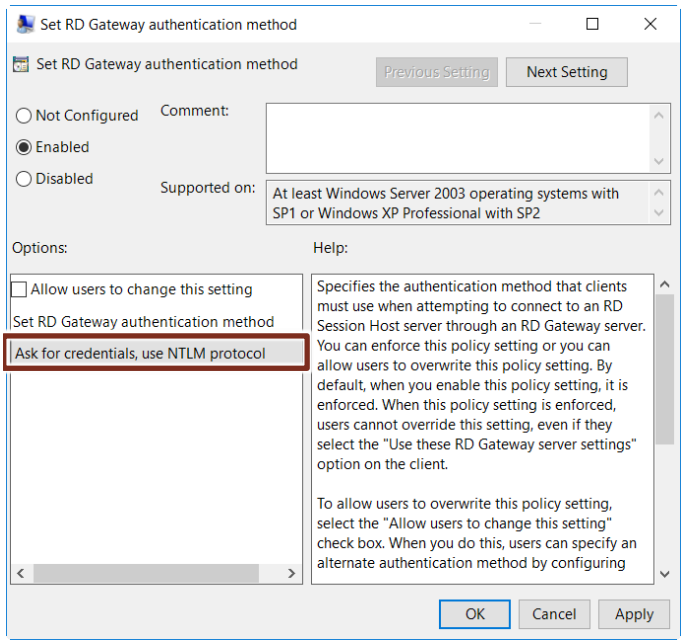
- "Set RD Gateway authentication method"

Figure 5-32

Setting	State	Comment
Set RD Gateway authentication method	Enabled	No
Enable connection through RD Gateway	Not configu...	No
Set RD Gateway server address	Not configu...	No

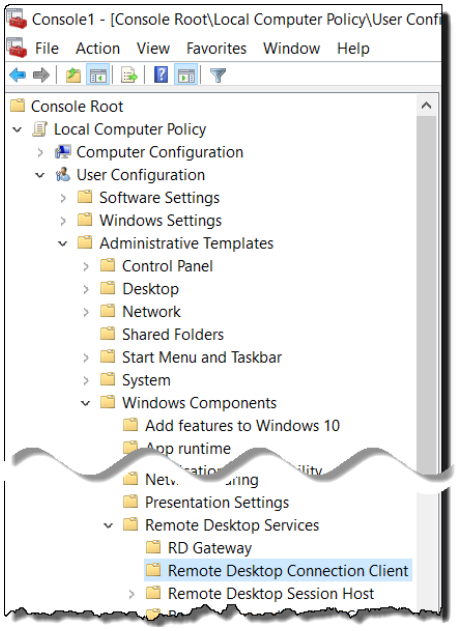
9. In the policy setting, change the "Ask for credentials, use NTLM protocol" drop-down list entry.

Figure 5-33



10. Open the "Microsoft Management Console" as described in section 3.1.2.
Open the following path:
"User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Connection Client"

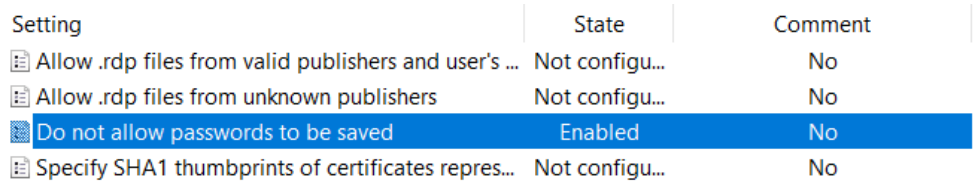
Figure 5-34



11. Change the following policy to "Enabled":

- "Do not allow passwords to be saved"

Figure 5-35



6 Appendix

6.1 Service and Support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:
https://support.industry.siemens.com

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:
www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:
www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:
https://support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:
https://support.industry.siemens.com/cs/ww/en/sc/2067

6.2 Links and Literature

	Subject area	Title
\1\	Siemens Industry Online Support	https://support.industry.siemens.com
\2\	Download page for the entry	https://support.industry.siemens.com/cs/ww/en/view/109475014
\3\	Security Guide for PC-based Automation Systems	https://support.industry.siemens.com/cs/ww/en/view/55390879
\4\	Configuring Windows 10 for a default user account	https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview
\5\	What is User Account Control?	https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts
\6\	Windows 10 AppLocker overview	https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview
\7\	IPSec	http://de.wikipedia.org/wiki/IPsec
\8\	VPN connections	https://support.microsoft.com/de-de/help/20510/windows-10-connect-to-vpn
\9\	NTLM	http://de.wikipedia.org/wiki/NTLM
\10\	Information about Remote Desktop Connections	http://windows.microsoft.com/de-de/windows7/allow-someone-to-connect-to-your-computer-using-remote-desktop-connection

6.3 Version history

Table 6-1

Version	Date	Change
V1.0	01/2019	First version