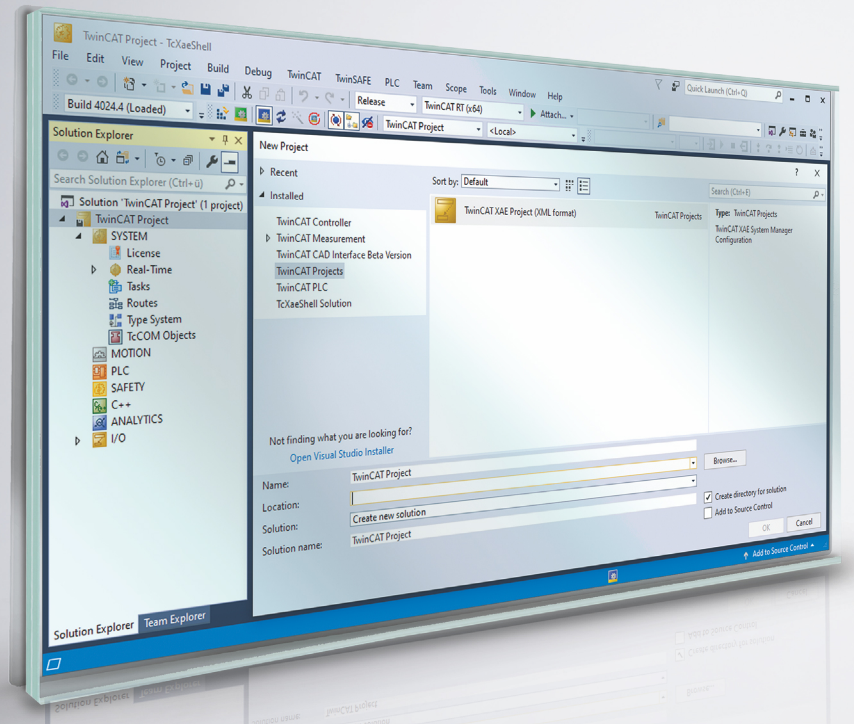
BECKHOFF New Automation Technology

Manual | EN

IPC Security Guideline

for Windows 7



Name: TwinCAT Project

Location:

Solution: Create new solution

Solution name: TwinCAT Project

2024-03-28 | Version: 1.1

Table of contents

1 Notes on the documentation

This description is intended exclusively for trained specialists in control and automation technology who are familiar with the applicable national standards.
For installation and commissioning of the components, it is absolutely necessary to comply with the documentation and the following notes and explanations.
The qualified personnel is always obliged to use the currently valid documentation.

The responsible staff must ensure that the application or use of the products described satisfies all safety requirements, including all the relevant laws, regulations, guidelines, and standards.

Disclaimer

The documentation has been prepared with care. The products described are, however, constantly under development.
We reserve the right to revise and change the documentation at any time and without notice.
No claims to modify products that have already been supplied may be made on the basis of the data, diagrams, and descriptions in this documentation.

Trademarks

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® and XPlanar® are registered and licensed trademarks of Beckhoff Automation GmbH.
If third parties make use of designations or trademarks used in this publication for their own purposes, this could infringe upon the rights of the owners of the said designations.

Patents

The EtherCAT Technology is covered by the following patent applications and patents, without this constituting an exhaustive list:
EP1590927, EP1789857, EP1456722, EP2137893, DE102015105702
and similar applications and registrations in several other countries.

EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany

Copyright

1.1 Report vulnerabilities

We kindly request the security analysts to give us sufficient time to develop a solution for closing a security hole before publishing it. The Coordinated Disclosure ensures that customers get an update on the closure of security holes and that they are not unnecessarily endangered during the development of the update. Once customers are protected, the open discussion about the security hole can help the industry as a whole to improve its products and solutions.

If Beckhoff is the supplier of a product that is suspected of being vulnerable, discoverers and coordinators of security holes should contact product-securityincident@beckhoff.com with a vulnerability report, preferably in English or German. Confidentiality is requested. Means of sending encrypted messages are described in Contact Beckhoff Incident Response Team.

Discoverers are requested to provide all necessary contact information in the vulnerability report so that queries are possible. Nevertheless, anonymous vulnerability reports will also be considered. Please provide as much detailed information as possible so that the cases can be reproduced. If the discoverer wishes to publish the discovery, Beckhoff will attempt to coordinate a suitable preliminary release date within 30 days. The discoverer is informed of the availability of solutions prior to the release date and receives the corresponding Beckhoff Advisory. Beckhoff receives the discoverer's planned publication (including requested CVE where applicable). A final release date is then agreed. On this day, both the discoverer's publication and the Beckhoff Advisory are released. If the discoverer so desires and if he adheres to the above procedure, then a note of thanks, a reference to the discoverer's publication and, if helpful, information about the discoverer's publication will be added to the Advisory.

1.2 Contact Beckhoff Incident Response Team

Address

Beckhoff Automation GmbH & Co. KG
Product Management (Security)
Hülshorstweg 20
33415 Verl
Germany

E-mail

<product-securityincident@beckhoff.com>

E-mails to this address are sent to the responsible members of the Beckhoff Incident Response Team.

Public keys

The Beckhoff Incident Response Team has two keys for establishing contact:

- PGP key with the ID `B4 F4 15 9A` and the fingerprint `C9 6F 56 5C 39 49 43 58 AE B5 07 93 80 95 E1 2D B4 F4 15 9A`
- S/MIME certificate with the ID `43 7E 2F D4 C5 01 A3 76 7D C2 31 9B` and the fingerprint `EE 3C 29 C3 BA BC 4F D6 43 BE D1 B2 6B 0E 4A FD 22 CF 4E E0`

Key download: https://download.beckhoff.com/download/document/product-security/Keys

Working hours

The Incident Response Team normally works between 9:00 and 17:00 and not on public holidays in North Rhine-Westphalia. Time zone: CET (Europe/Berlin).

1.3 Notes on information security

The products of Beckhoff Automation GmbH & Co. KG (Beckhoff), insofar as they can be accessed online, are equipped with security functions that support the secure operation of plants, systems, machines and networks. Despite the security functions, the creation, implementation and constant updating of a holistic security concept for the operation are necessary to protect the respective plant, system, machine and networks against cyber threats. The products sold by Beckhoff are only part of the overall security concept. The customer is responsible for preventing unauthorized access by third parties to its equipment, systems, machines and networks. The latter should be connected to the corporate network or the Internet only if appropriate protective measures have been set up.

In addition, the recommendations from Beckhoff regarding appropriate protective measures should be observed. Further information regarding information security and industrial security can be found in our https://www.beckhoff.com/secguide.

Beckhoff products and solutions undergo continuous further development. This also applies to security functions. In light of this continuous further development, Beckhoff expressly recommends that the products are kept up to date at all times and that updates are installed for the products once they have been made available. Using outdated or unsupported product versions can increase the risk of cyber threats.

To stay informed about information security for Beckhoff products, subscribe to the RSS feed at https://www.beckhoff.com/secinfo.

1.4 Design goals for security

Beckhoff's Industrial PC (IPC) hardware has been designed for general use like a normal PC for office environments but with significant robustness added for use within industrial environments. The complete board has been designed for reliable and highly deterministic operation within such environments. Still the hardware supports general purpose operating systems like Windows® and TwinCAT/BSD which is based on FreeBSD. Consequently, the hardware is designed to support conventional and office-IT grade security mechanisms as provided by the operating systems. It is the duty of the one who integrates the IPC into an operational environment to configure these security features appropriately for the specific environment. Also, that person needs to provide guidance on secure use to the operator. Such configuration and usage guidelines should be the result from or be conformant with a holistic security concept for the specific environment.

Beckhoff's IPCs can be ordered with and without an operating system. Among these operating systems Windows 10 and TwinCAT/BSD are available. These are provided in a way which is called "secure by default" unless specifically ordered otherwise. This means, that only services are enabled with the default configuration such that all access to the device is authenticated and the only pre-configured user is one for administrative access. For historical reasons, the pre-configured user is "Administrator". Beckhoff offers the named operating system images pre-installed on the IPC in two fashions: One fashion has a random password pre-set for "Administrator" which can be read from a label on the device. The second fashion has the well-known password preconfigured for this as documented. Please note: The latter is not "secure by default" with respect to the requirements of some environments while it serves well for others.

The named operating systems are not developed by Beckhoff. The basis of Beckhoff's Windows 10 images is developed and maintained by Microsoft Corporation. The basis of TwinCAT/BSD is developed and maintained by "The FreeBSD Project". Both bases are well reputed regarding their security features since decades for use in office and server environments. They contain and provide state of the art security features. Specific environments and applications have specific needs for the configuration and use of these security features. Because Beckhoff provides the named operating systems for general purpose use and does not want to restrict which applications are implemented by this, Beckhoff cannot foresee the specific security needs which emerge from specific use or integration. Guidance on the secure configuration and use thus needs to be created by the one who integrates the operating system into an environment for specific use. Nonetheless, Beckhoff provides guidance on how to use the IPC and its operating system securely within this guide. Such guidance is to be considered as general hint and not as a complete and sufficient reference. The developers of the operating systems provide complete documentation for the security features of the operating systems.

Beckhoff created extensions to these operating systems, especially to optimize the deterministic behavior of the operating system for use with real-time applications of the automation industry. The extensions are integrated in operating system images distributed by Beckhoff. For those extensions robustness and determinism for availability is the primary target of their design. Still, Beckhoff cares that these extensions do not compromise the security features of the basis of the operating system unless noted otherwise.

Beckhoff distributes a high variety of software products. One example is the product “TwinCAT 3.1 – eXtended Automation Runtime (XAR)”, which is called TwinCAT 3.1 XAR in short. For some IPCs this can be ordered pre-installed within the operating system. The primary purpose of this specific software is to provide a deterministic and robust but highly customizable runtime for automation applications. When it is installed on an IPC then it turns that device into a Programmable Logic Controller (PLC). Besides availability (through robustness and determinism) the software has been added with perimeter security during its development. This means that it can be configured and used in a way that it securely authenticates access through the protocols which are implemented by TwinCAT 3.1 XAR. The perspective for this perimeter security is that the network interfaces of the IPC mark the boundary. The security risk identified by Beckhoff for this kind of security is that an unauthorized user gets access to the IPC via protocols implemented by TwinCAT 3.1 XAR. For historical reasons and backward compatibility TwinCAT 3.1 XAR still provides protocols which do not authenticate before such access. Some IPCs with TwinCAT 3.1 XAR pre-installed have a configuration for TwinCAT 3.1 XAR which is secure by default. That means that this default configuration enables only secure protocols of TwinCAT 3.1 XAR. Please note that lots of IPCs which are shipped with TwinCAT 3.1 XAR pre-installed do not have a configuration which is secure by default for backward compatibility. This security guide contains a complete list of the protocols which are supported by TwinCAT 3.1 XAR and advises about which are secure, please see: Important TCP/UDP ports [▶ 50]. The other software products come with their own documentation and guides. Please note: The latter is true also for TwinCAT functions which can be added via separate installer to TwinCAT 3.1 XAR.

2 Hazards and risk assessment

This section provides an overview of the hazards and risk assessment for an automation system. Different attackers and types of attacks as well as typical threat scenarios and protection principles are described.

2.1 Attackers

Classification according to the position of an attacker

Attackers can be divided into four classes according to their access to a system:

Class	Description
Insider attackers	Attackers who want to perform certain actions on the automation system. The intention is to carry out damaging actions for which the attackers are not authorized. In addition, such attackers have access to private information, e.g. passwords, which they need to perform authorized actions.
Local attackers	Attackers who have direct access to components of the automation system. This class also includes local attackers who can access some components directly via hardware interfaces or change the network topology in different places.
Attackers in the internal network	Attackers who control devices on the internal network. Such attackers are generally unable to change the network topology and can only use existing services in the network.
Attackers from an external network	Attackers who can only execute actions through interfaces that are connected to the internet, for example. With successful attacks on internal components, these attackers can escalate to attackers in the internal network.

Assumptions

For all attackers it must be assumed that:

- they can receive public information such as documentation from the internet or via service calls;
- they are able to acquire any products available on the public market and to prepare targeted attacks by analyzing such products;
- they have significant computing power at their disposal, for example by renting computing time from a cloud provider.

The occasionally promoted categorization according to the motivation of an attacker is generally not expedient, as it involves a number of assumptions and speculations.

The classification helps when creating security analyses, but it should be noted that a real attacker has by all means various capabilities in several categories.

2.2 Attack types

Attacks can be categorized according to their execution. The effort involved in the attack plays a key role:

Category	Description
Broad, viral attacks	The attacks exploit widespread vulnerabilities and spread to reachable neighbors. Such "untargeted attacks" are aimed at attacking as many affected systems as possible in order to benefit the attacker. The benefits for the attacker arise, for example, from extortion to decrypt data ("ransomware") or using the resources of the attacked party ("botnet"). These attacks often use unpatched vulnerabilities or common organizational flaws such as weak passwords.
Vendor and integrator-specific attacks	The attacks exploit vulnerabilities in certain products that may be less common. These attacks can spread automatically, but they target special products or configurations as vulnerabilities (e.g. from Beckhoff or, if applicable, integrator configurations/extensions). Attack targets can also be industry-specific, such as spying out know-how or the like.

Category	Description
User-specific attacks	Such attacks are directed against precisely one system installation, hence the term targeted attacks. They are difficult to detect and are elaborately carried out by the attacker. Targeted system configurations are used to achieve the aim of the attack. Attack targets are manifold and are generally difficult to predict.

Only measures against broad viral and vendor-specific attacks are presented in these security guidelines. User-specific attacks necessitate analyses and counter-measures on the part of the user.

2.3 Typical threat scenarios

This section describes typical threats. However, the list is not exhaustive.

Manipulated boot medium

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

A prepared data storage device is connected to a component and the component is booted from it. This is possible if the boot order in UEFI/BIOS is set to boot from external disks or the attacker is able to change the boot order.

Through the attack an attacker can gain read and write access to all data of the component, especially configurations and know-how. After such an access has occurred, the entire component must be considered insecure.

Defensive measures:

- BIOS password (BIOS settings [▶ 16])
- Set boot media (BIOS settings [▶ 16])
- Locked control cabinet [▶ 14]

Unauthorized PXE boot server

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	covered	not covered
Vendor and integrator-specific attacks	not covered	not covered	covered	not covered

Boot from an unauthorized PXE boot server in the internal network. The attack involves execution of code controlled by the attacker.

Through the attack an attacker can gain read and write access to all data of the component, especially configurations and know-how. After such an access has occurred, the entire component must be considered insecure.

Defensive measures:

- Disable PXE boot (BIOS settings [▶ 16])

Manipulated USB devices

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

If manipulated USB devices are connected, it may be possible for the attacker to execute malicious code on the affected device. In addition, the affected USB device can also be used to steal know-how. For example, any code can be executed by a suitably configured autostart. Unauthorized input can be made or logged by a suitably prepared input device.

Such an attack allows an attacker to gain read and write access to a large number of data relating to the operating system, especially configurations and know-how. After such an access has occurred, the entire component must be considered insecure.

Defensive measures:

- Disable autostart (Autostart [▶ 37])
- Whitelisting USB devices (USB filter [▶ 45])
- Locked control cabinet [▶ 14]
- Disable interfaces in BIOS (BIOS settings [▶ 16])
- Whitelisting for programs [▶ 31]

Guessing of weak passwords through local interface

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

Weak passwords such as default passwords or easily guessed passwords can be exploited by local attackers. Like authorized local users, attackers can login with unmodified default passwords.

Such an attack allows an attacker to gain read and write access to a large number of data relating to the operating system, especially configurations and know-how. After such an access has occurred, the entire component must be considered insecure.

Defensive measures:

- Secure passwords [▶ 21]
- Set up individual users, no collective accounts
- Minimum rights for users ("Least Privilege"), in particular no administrator rights if not necessary

Theft of data carriers

Attack type/attacker	Insider	Local	Internal network	Remote
Widespread viral attacks	not covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

An attacker may gain knowledge of and access information for services in an automation system via unauthorized removal of data carriers.

An attack like this allows an attacker to gain read access to a large amount of data related to the operating system, especially access data, configurations, knowledge and other sensitive private data.

An attacker could also try to gain access to sensitive data by stealing the storage media after it has been disposed of.

Defensive measures:

- File encryption [▶ 20]
- Locked control cabinet [▶ 14]
- Secure data destruction [▶ 14]

Extraction of sensitive data from discarded material

Attack type/attacker	Insider	Local	Internal network	Remote
Widespread viral attacks	not covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	not covered	not covered

An attacker can gain access to discarded material which contains sensitive data on storage media.

An attack like this allows an attacker to gain read access to a large amount of data related to the operating system, especially access data, configurations, knowledge and other sensitive private data.

Defensive measures:

- File encryption [▶ 20]
- Secure data destruction [▶ 14]

Handling untrusted emails

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	covered	covered
Vendor and integrator-specific attacks	not covered	not covered	covered	covered

Untrusted emails are a typical way to spread malware. In particular, attacks exploit opening of hyperlinks with outdated browsers and email attachments. Sometimes emails are formulated in such a way that they appear to be trustworthy.

A successful attack can execute unauthorized actions that are executed with the privileges of the interacting user.

Defensive measures:

- Do not use control computers for handling emails
- Regular or automatic software updates (Updates [▶ 17])
- Whitelisting for programs [▶ 31]

Exploiting known vulnerabilities in outdated software

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	covered	covered	covered	covered
Vendor and integrator-specific attacks	covered	covered	covered	covered

Manufacturers release software updates to correct known vulnerabilities. If software that is in use is not updated, broadly based viral attacks can be carried out successfully.

A successful attack can execute unauthorized actions that have an impact in the context of the affected software.

Defensive measures:

- Windows updates (Updates [▶ 17])
- Regular or automatic software updates (Updates [▶ 17])
- Network-based detection mechanisms (IDS/IPS)
- Disabling unneeded services
- Removing components that are no longer needed [▶ 36]

Manipulated websites

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	not covered	covered
Vendor and integrator-specific attacks	not covered	not covered	not covered	covered

A user is tricked into visiting an untrusted website. A vulnerability in the browser is exploited to execute arbitrary malicious code, or the website is designed in such a way that the user discloses confidential information such as login data.

A successful attack can execute unauthorized actions that are executed with the privileges of the interacting user.

Defensive measures:

- Regular or automatic software updates (Updates [▶ 17])
- Organizational measures for web surfing behavior.

Man-in-the-middle attacks

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	covered	not covered	not covered	not covered
Vendor and integrator-specific attacks	covered	covered	covered	covered

When using an insecure network protocol, an attacker can pretend to be the trusted remote station within the reachable network. This allows the information sent via this protocol to be manipulated or intercepted.

A successful attack can lead to unexpected behavior of the services in the automation system.

Defensive measures:

- Network segmentation
- Use of secure network protocols

Unauthorized use of network services

Attack type/attacker	Insider	Local	Internal network	Remote
Broad, viral attacks	not covered	not covered	covered	covered
Vendor and integrator-specific attacks	not covered	not covered	covered	covered

If network services are provided that an attacker can access, this could result in unauthorized actions.

A successful attack can lead to unexpected behavior of the services in the automation system.

Defensive measures:

- Network segmentation
- Use of authenticating network services
- Disabling unneeded services
- Removing components that are no longer needed [▶ 36]

3 General measures

3.1 Employee training

Trained personnel are an important protection for the system. Employees who have access to the device should know how to operate it. This includes general measures such as the responsible handling of passwords and data carriers such as USB sticks. Every employee should be aware of the possible effects of intervening in the system.

3.2 Physical measures

One of the easiest and safest security measures is physical protection. Make sure that only administrators and technicians have access to the device. Attacks via physical access such as USB flash drives and other data carriers, which represent one of the biggest risks, can be reduced in this way. Physical protection of a device is achieved, for example, by means of a lockable control cabinet.

Locked control cabinet

The standard environment for an industrial controller should be a locked control cabinet. The attack surface is greatly reduced by allowing only individual interfaces to leave the control cabinet. The interfaces led out there should be additionally protected (lockable). Access to the control cabinet should only be given to persons who need it in order to perform their tasks. Electronic locking systems can also be used, for example based on smart cards. As with all key management systems, access to the control cabinet should be revoked when it is no longer required.

Video surveillance

Video surveillance is suitable for shift working in environments where many people need access to a controller or where facilities are geographically dispersed. However, video surveillance can only detect attacks and not prevent them. This measure is therefore only useful in combination with other measures.

3.3 Secure data destruction

In the case of scrapped or decommissioned components, it is important to reliably destroy the data. Multiple overwriting of the data carrier is a suitable and reliable method.

Data on intact hard disks can be completely and unrecoverably erased by overwriting using special software. The data are overwritten once or several times with specified characters or random numbers, which is sufficient in most cases.

Windows now overwrites a partition completely with zeros during "slow" formatting. In the case of old hard disks (< 80 GB), the data should be overwritten 7 times. Modern hard disks allow the use of the command ATA-"Enhanced Security Erase". Here, a vendor-specific routine is initiated in the hard disk that should erase the entire hard disk, including defective memory areas. This method of erasure is recommended with SSD or SSHD. The command should be combined with the overwriting procedure mentioned above. The data carriers can still be used after overwriting.

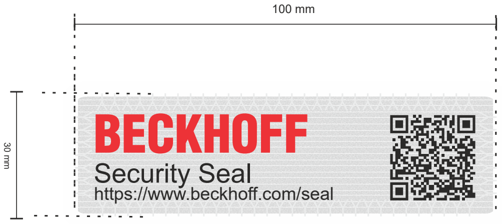
Both freeware and commercial products are available on the market that perform the overwriting methods mentioned. Most of these tools offer different overwriting methods. We recommend the use of programs to overwrite the hard disk that can be started from a bootable medium (e.g. CD, USB flash drive) and overwrite the entire hard disk.

Physical destruction

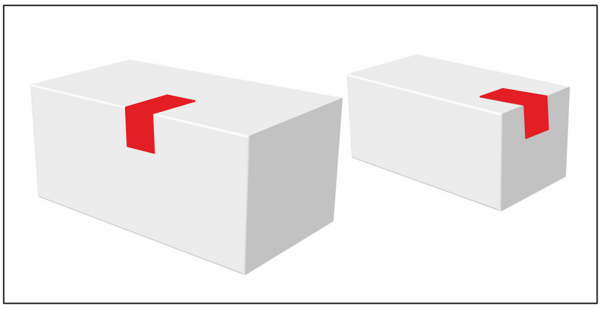
If you don't wish to overwrite a hard disk or cannot do so due to a defect, you should physically damage or destroy the hard disk.

3.4 Security seal on product packaging

From the end of 2021, seals with security features will be affixed in the factory to certain product packaging for Industrial PCs and Embedded PCs:



The position and nature of the seal are such that the removal of the goods from the packaging leads to irreversible and visible changes to the packaging and the seal. The intactness of the product can therefore be checked before opening by means of a visual inspection.



The seal is an aid to an efficient procedure for checking packed products. Because absolute security is impossible, the use of the seal is limited to the following applications: It allows a justified assumption to be made of the intactness, completeness and authenticity of the goods in the packaging without having to open the packaging. If the seal or the packaging is damaged, the recipient should ascertain the correct condition of the goods when accepting or using them. If the goods are intended for applications in which aspects of IT security are relevant, the recipient of the goods can, for example, stipulate that the goods are to be checked for tampering before use if the condition of the seal or packaging gives cause to suspect tampering during dispatch.

The design and stipulation of meaningful processes and rules for the acceptance and use of products from Beckhoff remain the responsibility of the recipient.

Opened seal

Products from Beckhoff often reach the recipient via a multi-step distribution chain. The seal may have been opened during the processing of the product. An opened seal is not grounds for a warranty claim.

4 BIOS settings

It is recommended that you set a password for the BIOS to ensure that critical settings such as boot order, CPU clock or important settings cannot be changed without authorization. It may also be useful to set the boot order and prevent external disks from booting. Settings in the BIOS should only be made by well-versed persons. The changing of unknown parameters can have a negative effect on the function of the system.

5 Operating system

5.1 Backup and recovery

A backup and recovery strategy should be drawn up for each device and protects against:

- security incidents,
- data loss due to defective storage media,
- or from corrupt data due to improper shutdown.

The last backup created can be restored in the shortest possible time, thus preventing major production downtime. Apart from creating backups, it is also important to define a restore process.

Backup and recovery are not exclusively security matters, but help to minimize downtime in case of security incidents.

A process both for creating a safety copy as well as a process to restore it should be defined. Security aspects should also be taken into consideration when doing so.

If a completely automated backup solution is used, the backup system itself is mostly accessible in the network and thus also vulnerable; manual ("offline") backups are better here. Offsite backups, i.e. backups that are stored locally separated, have the advantage that they can be restored even in the case of a local incident where the machine itself is not affected.

A wide variety of implementations are thus available and conceivable.

Since the TwinCAT boot projects and all necessary information are stored as files on the file system of the respective operating system, file-based security is sufficient in this case.

Beckhoff provides a backup and recovery solution in the form of the "Beckhoff Service Tool (BST)". For more information on the BST, see: Infosys entry on BST.

If your Industrial PC is shipped with BitLocker encryption enabled for the system partition, then the key to decrypt the partition during an unattended boot is protected by the Trusted Platform Module (TPM) on the mainboard of the device. The TPM module provides the Windows kernel with the key for decryption only if the measurement of the early startup process shows that previously trusted software with a known configuration has been started and that neither the software nor the configuration nor the next software to be started (i.e. the kernel) has been manipulated.

A full backup must include the boot partition and the system partition. If you back up the entire boot disk as a raw device, your backup contains the encrypted system partition. In addition to the backup, you must also export a recovery key. A recovery key is especially needed to restore and use the backup on another hardware. Please keep this recovery key in a safe and secure place. It is also strongly recommended to always have a recovery key on hand in case legitimate changes have been made to the software and configuration that are part of the early startup process. This can be the case, for example, if the boot sequence of the firmware (BIOS) is changed by authorized persons.

If BitLocker encryption is enabled, there is an alternative to a full backup of the partitions including the encrypted system partition: you can temporarily disable the encryption of the system partition and create an offline backup as usual. Please do not forget to re-enable the encryption afterwards.

5.2 Updates

There are various ways to keep your operating system and programs up-to-date:

- Updating the entire image
- Updating individual programs
- Integrated operating system updates

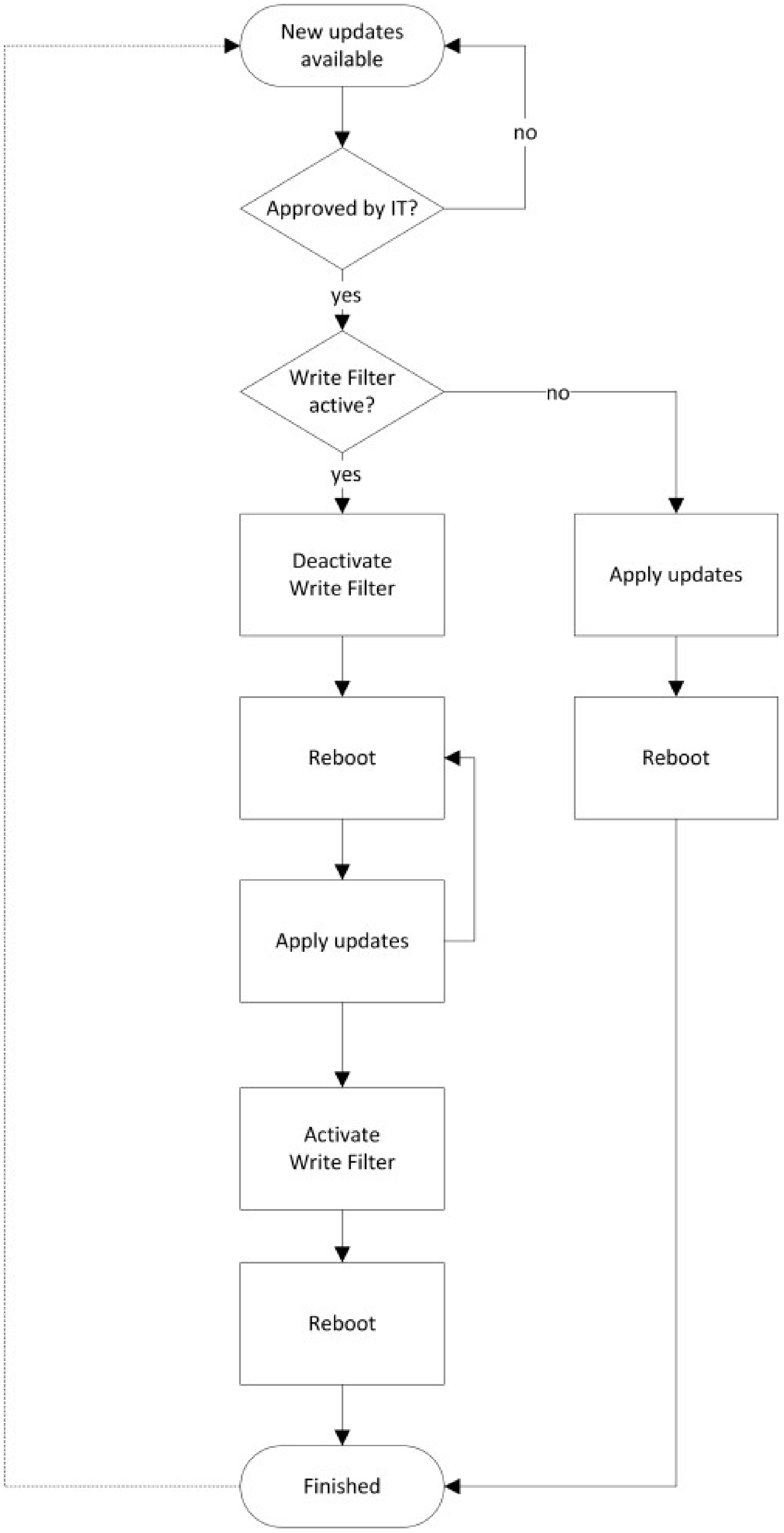
NOTICE

Avoiding data loss

Back up your data before carrying out an update. First of all, create a backup image of the PC with the help of a BST (Beckhoff Service Tool, https://www.beckhoff.de/default.asp?industrial_pc/bst.htm).

The Windows 7/10 operating system has its own update mechanism, the Windows Update Service. To prevent changes being made inadvertently to the system, the Windows Update Service is disabled in the images provided by Beckhoff. Windows updates can still be downloaded from Microsoft and installed manually. If the Windows Update Service is enabled, the updates are procured from the Microsoft Windows Update Server with the standard settings. Communication with the server takes place via an encrypted and signed connection. The updates procured are signed with an official certificate from Microsoft so that their authenticity can be checked.

Engineering computers should be kept up-to-date with updates. This can be more difficult for computers in industrial environments. For example, if a write filter is used, updates installed without further measures are discarded upon reboot. To avoid this, the following procedure is recommended:


New updates available
Approved by IT?
no
yes
Write Filter active?
no
yes
Deactivate Write Filter
Apply updates
Reboot
Reboot
Apply updates
Activate Write Filter
Reboot
Finished

After this procedure, intensive tests by the operator are required to ensure that the system is functioning properly.
Beckhoff devices are delivered with half-yearly updated and tested images that contain compatible Windows updates.

These images can be requested through Beckhoff Service for Windows 7 / 10. The serial number of the device is required for this.

See also:

- https://www.beckhoff.de/default.asp?industrial_pc/bst.htm

5.3 File encryption

NOTICE

Malfunctions

Do not encrypt the entire system partition, Windows system files or the TwinCAT folder. This can lead to malfunctions.

As a rule, an established access control is sufficient to protect sensitive files and directories against unauthorized access. If the data carrier gets lost, however, the protection of these data is no longer guaranteed and necessitates additional protection by the encryption of individual files and directories.

With EFS (Encrypted File System), Windows provides an encryption function with which individual files or entire directories can be encrypted. An additional security level and cryptographic protection is thus made available.

An important post-encryption aspect is the administration of keys and the clarification of the following questions:

- Who should be given access?
- What authentication options are there? (USB token, PIN, password, user name + password, etc.)
- How are the keys managed?

In any case the data are unprotected when they are decrypted and used.

By comparison, BitLocker supports the encryption of complete data carriers. In addition, BitLocker offers maximum protection when it is used with TPM (Trusted Platform Module), as described in the TPM documentation.

Activating EFS

1. Right-click a folder or file and select **Properties** from the context menu that opens.
2. Open the **General** tab and click **Advanced**.
3. To encrypt the folder or file, select the **Encrypt contents to secure data** check box.

⇨ If this is the first data encrypted in this way, Windows automatically creates an EFS certificate in the local certificate store. Make sure the certificate is saved, because otherwise it is impossible to restore the data (see Saving the certificate [▶ 20]).

Saving the certificate

1. Launch **certmgr.msc**.
2. Click **Add**, select **My user account** and click **Finish**.
3. Expand the "Personal" folder and click **Certificates**

   ⇨ You should see a certificate with "Encrypting File System" as the "Intended Purpose".
4. To save the certificate, right-click on the certificate and select **All Tasks > Export**.
5. Select **Export Private Key**.
6. Select **Personal Information Exchang**e, **Include all certificates…** and **Enable strong protection**.
7. Specify a password to protect the certificate. This certificate is required later for the import.

8. Specify the path under which the certificate is to be saved. Save the certificate in another secure location.

5.4 User and rights management

5.4.1 Secure passwords

Secure passwords are an important prerequisite for ensuring the security of a system. Beckhoff delivers the images with standard user names and standard passwords for the operating system. These must be changed by the customer. Otherwise, your device is vulnerable to attack via the network and access by unauthorized personnel.

Controllers are delivered without password in the UEFI/BIOS. Here, too, it is recommended to assign a password.

A Security Wizard is integrated in the system. This is started directly after booting up the device during local access. This wizard requests the user to change the password. However, the password can also be changed locally using operating system tools.

The following applies:

- Passwords should be unique for each user and service.
- Password complexity: the password should contain capital and lower-case letters, numbers, punctuation marks and special characters.
- Password length: the password should be at least 10 characters long.
- Contrary to some previous recommendations, it is recommended that passwords are no longer changed regularly, but only after an incident in which passwords have become known to unauthorized persons. See also https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/
- It may be useful to schedule a mandatory waiting time after unsuccessful logon attempt.

Generate secure password

There are many ways to create a secure password. The following table describes a method of generating passwords. The procedure can also help to remember complex passwords:

Procedure	Example
1. Start with one or two sentences.	Complex passwords are more secure
2. Remove the spaces.	Complexpasswordsaremoresecure
3. Abbreviate words or add spelling mistakes.	Complxpasswordsarmorescure
4. Insert numbers and special characters to extend the password.	Complxpasswordsarmorescure#529954#

Problematic passwords

Cyber criminals use sophisticated tools that enable high-performance attacks on passwords. Therefore, it is advisable to avoid:

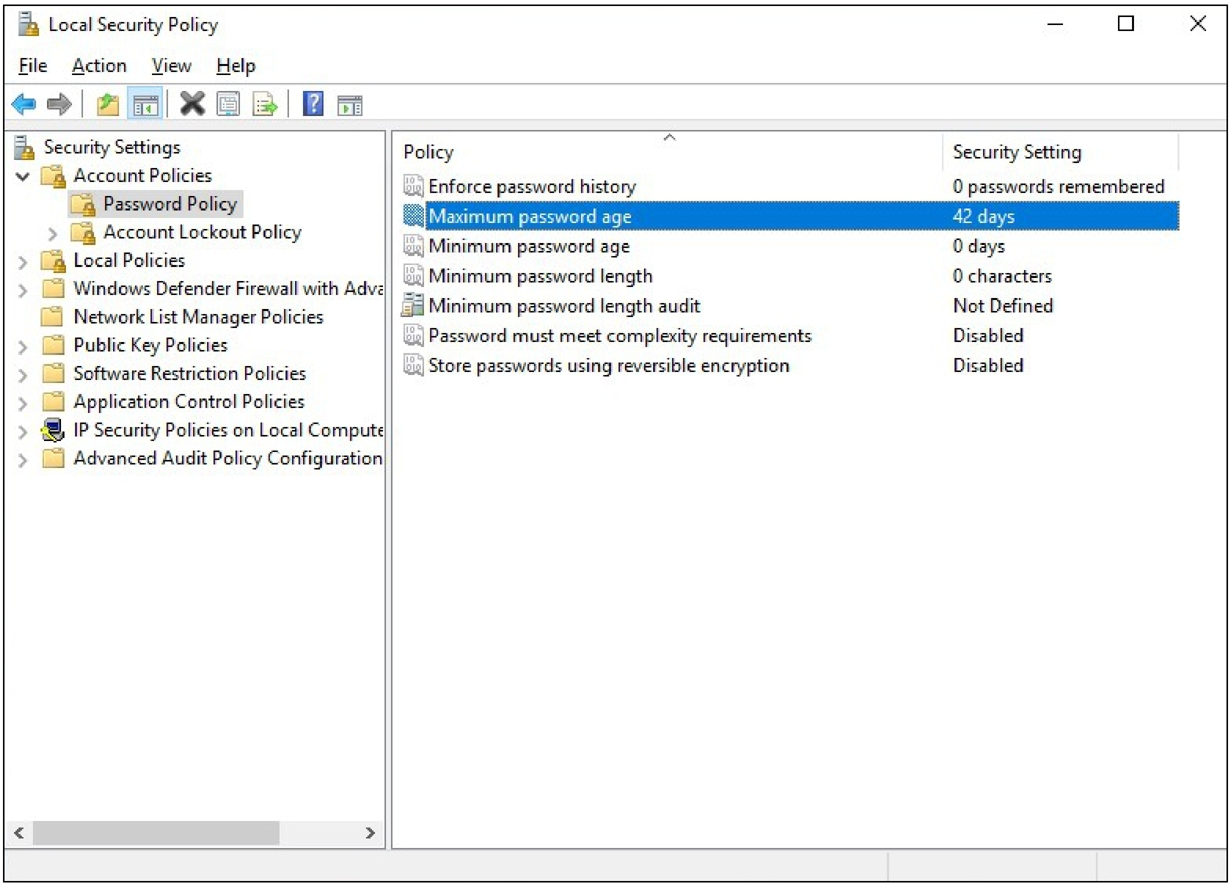
- Words contained in dictionaries
- Words written backwards, common spelling mistakes, and abbreviations
- Repetitive sequences, e.g. 12345678 or abcdefgh
- Personal information, e.g. birthdays, ID numbers, telephone numbers

5.4.1.1 Change password

5.4.1.2 Password policies

Password policies make it possible to restrict the choice of passwords for user accounts, forcing users to choose secure passwords. A separate password policy protects the system against the use of weak passwords. Set the length and complexity of the user passwords used.

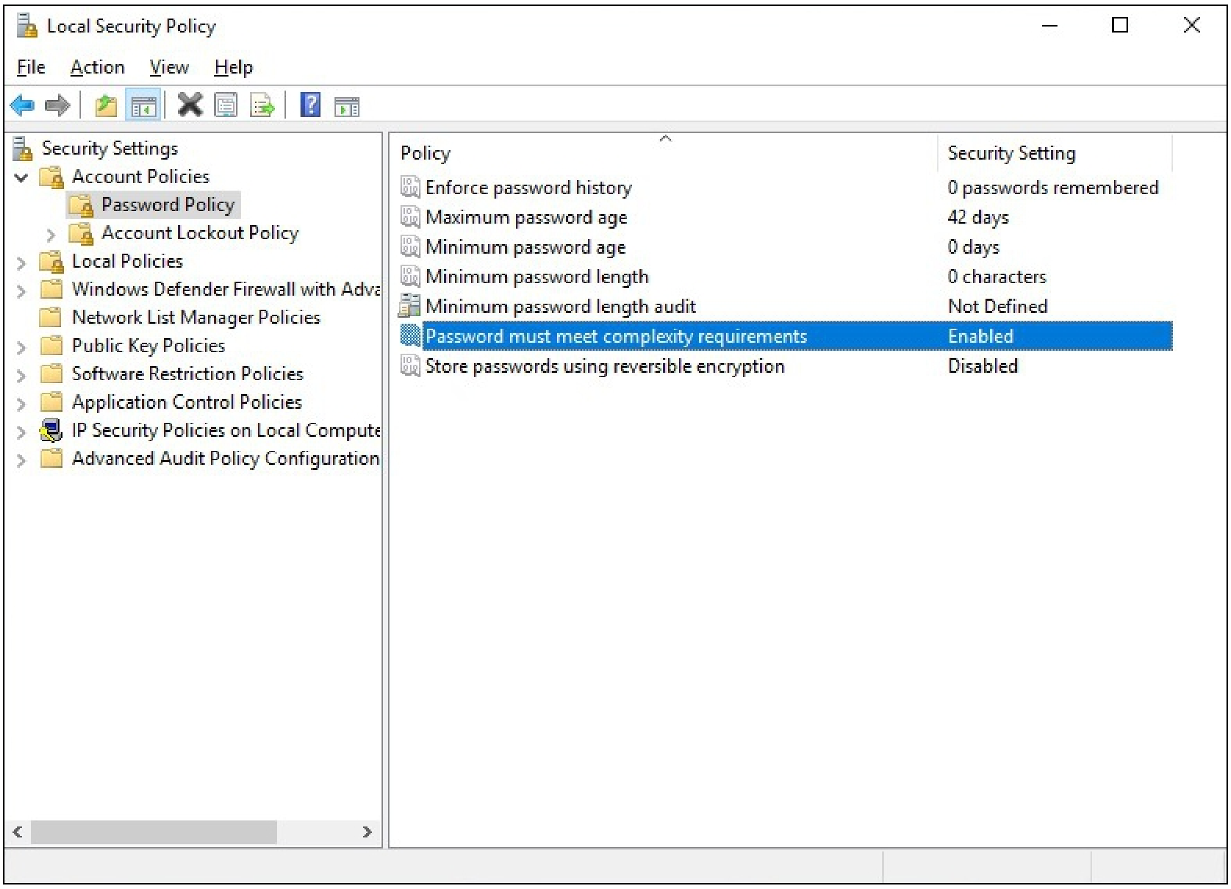
1. Open the **Control Panel** and select **Administrative Tools > Local Security Policy**.
2. Select **Account Policies > Password Policy** in the window that opens
3. Specify the password policy settings.
4. To set a maximum password age, a time period (in days) can be defined for the policy **Maximum password age** before the system prompts the user to change the password.



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

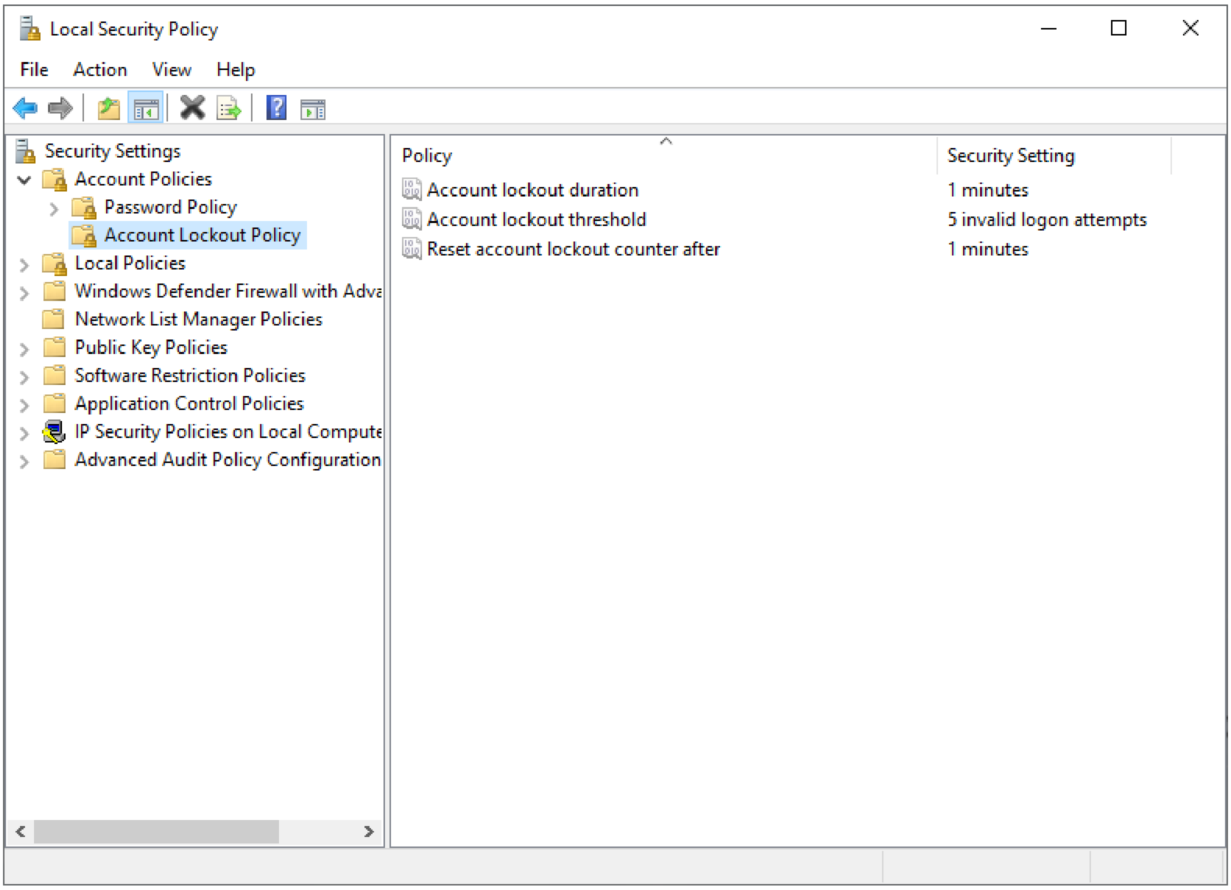
Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

5. In order to demand a password complexity, the policy **Password must meet complexity requirements** can be set. On enabling this policy, any passwords set in future must contain at least upper case letters, lower case letters, numbers and special characters.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

6. To prevent attacks to guess user authentication data, the settings can be set at **Account Lockout Policy**. Set the number of failed login attempts after which a user account should be locked out. You can use the **Account lockout duration** policy to set the duration in minutes that a locked account remains locked before it is automatically unlocked.


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	1 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	1 minutes

⇨ Definition of the password policies

5.4.1.3 IPC Security Wizard

User passwords can be set via the IPC diagnostics webpage. It can be reached by https on Port 443.

In the delivery state, the IPC Security Wizard is started when a user connects by https or works locally on the device.

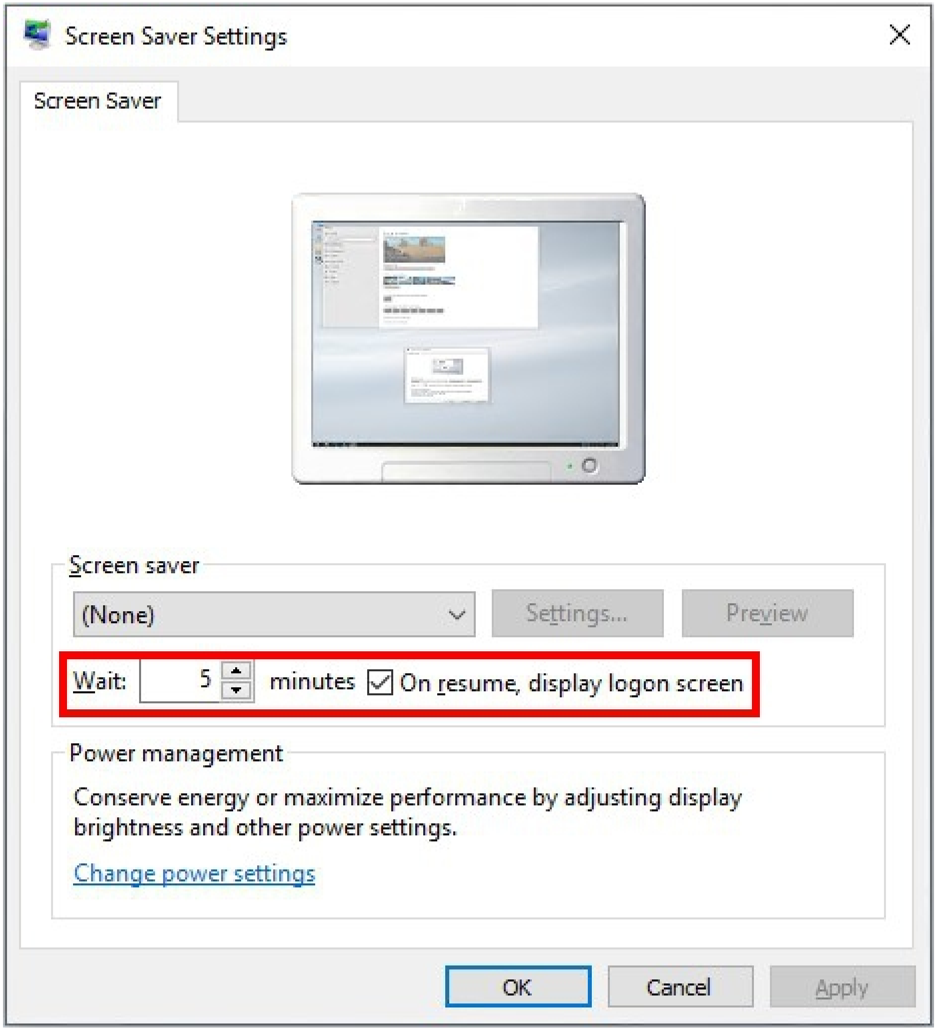
The IPC Security Wizard prompts the user to change the default password.

See also:

- Documentation on IPC diagnostics in the info system

5.4.2 Automatic logout

So that a system cannot be misused when it has not been used for a while by an already logged-on user, an automatic user logout can be set. To do this, a time can be defined in the Screen Saver setting. On expiry of the time, an unused system is locked and the user is required to authenticate himself again.



Screen saver

(None)

Wait: 5 minutes ☑ On resume, display logon screen

Power management

Conserve energy or maximize performance by adjusting display brightness and other power settings.

Change power settings

5.4.3 Audit policy

As part of a security concept for the integration of a device into a network, it should be specified which level of security audit is suitable for detecting potential attacks. Security audit means that an industrial PC creates audit logs of events as soon as an interaction with the device takes place. For example, file and folder accesses can be logged each time a user accesses the selected files or folders.

These logs are intended for review to detect deviations from normal use that could indicate an attack, or for forensic purposes to reconstruct details about an attack. The check can be carried out immediately or at regular intervals by automated mechanisms or manually. It depends on the environment and the application as to which deviations are relevant. Therefore, rules that describe which actions are logged are usually configured using audit policies.

However, configuring too many rules can lead to a kind of blindness. The logs can become overloaded with irrelevant entries, with the relevant entries easily overlooked by humans or not processed quickly enough by automatic monitoring mechanisms. Sometimes it is good practice to forward logs to a central location for automatic review and/or archiving, among other things to avoid exhausting limited log capacity.

Microsoft has published a guide to security audits for Windows with the relevant settings and best practices. The basic audit policies include the following categories, which can be enabled and are disabled by default:

- Audit account logon events [▸ 26]
- Audit directory service access [▸ 27]
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use

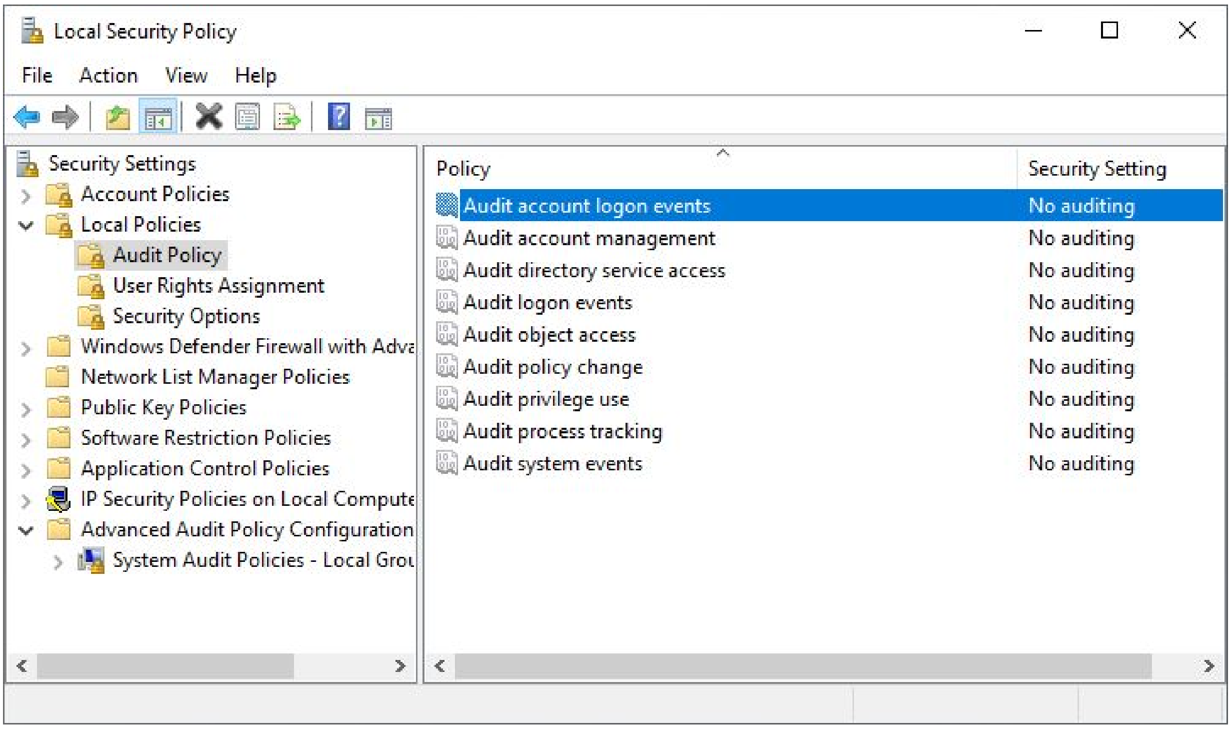
- Audit process tracking
- Audit system events

5.4.3.1 Audit account logon events

Audit logon events in the Beckhoff Device Manager and enable the appropriate policy if you want to determine who has logged on to the web interface from which IP address, for example.

Proceed as follows:

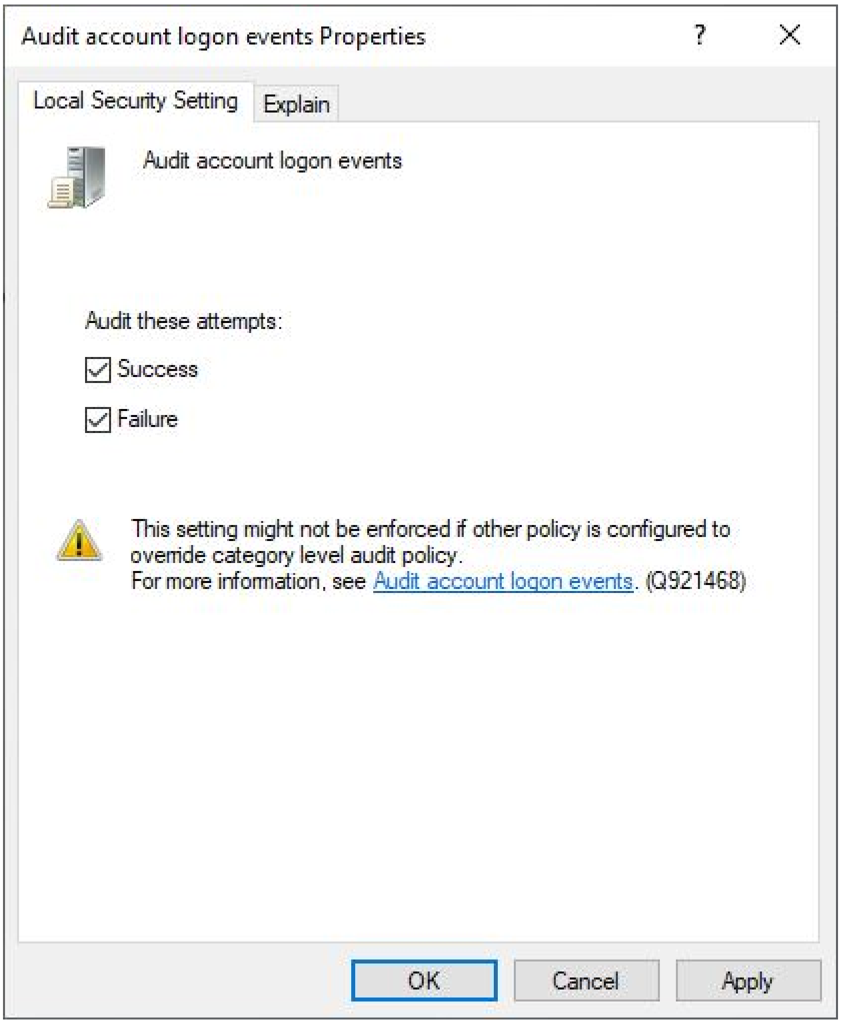
1. Call up the Run dialog via the shortcut **[Windows key] + [R]** and enter **secpol.msc**.
   The **Local Security Policy** window appears.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
System Audit Policies - Local Grou

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

2. Click on **Local Policies > Audit Policy** in the structure tree on the left and select the policy **Audit account logon events**.

3. Select the **Failure** check box if you only want to log unsuccessful attempts. Also select the **Success** check box if you also want to log successful attempts.



Audit account logon events

Audit these attempts:

☑ Success

☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account logon events. (Q921468)

⇨ The logged entries can now be viewed in the **Event Viewer**, which you can call up with **[Windows key] + [R]** and the entry **eventvwr**. The entries can then be viewed under **Windows Logs > Security**.

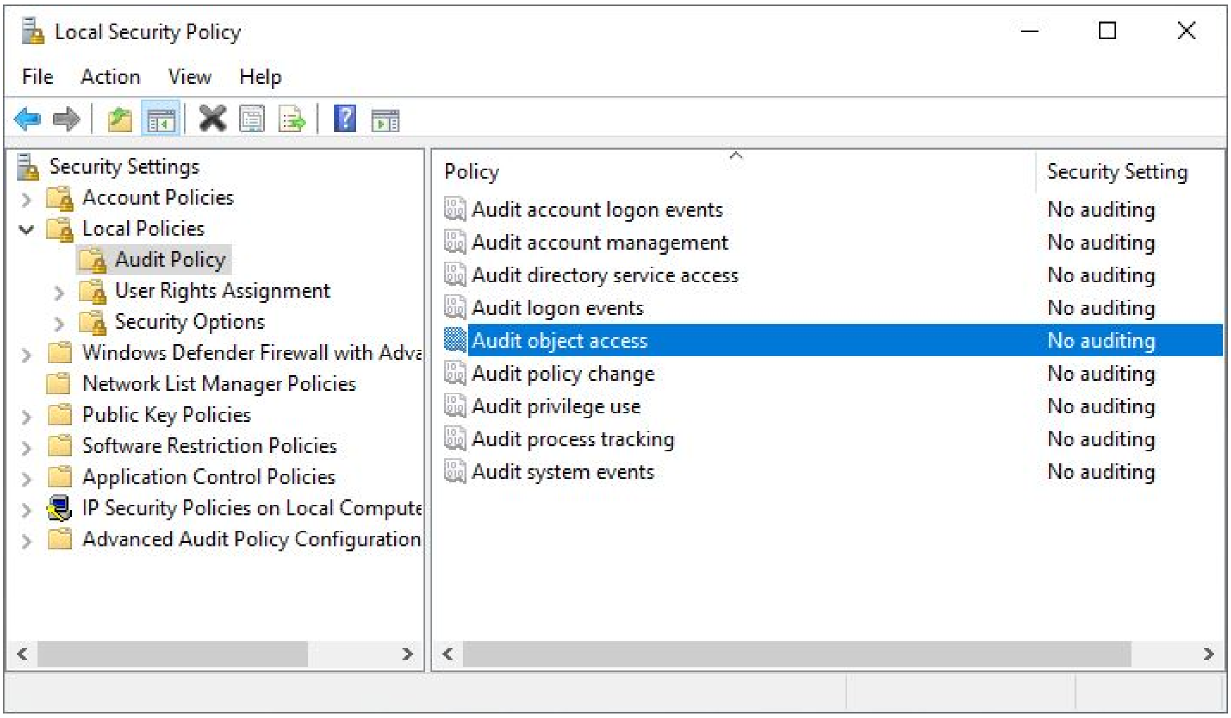
5.4.3.2 Audit directory service access

The size of the Windows log grows with each log entry. Note the available hard disk space.

File and folder access operations can be logged in Windows. Each time a user accesses the selected files or folders, a so-called audit event is recorded in the Windows log.

Create audit policy for file and folder access:

1. Call up the Run dialog via the shortcut **[Windows key] + [R]** and enter **secpol.msc**.
   The **Local Security Policy** window appears.

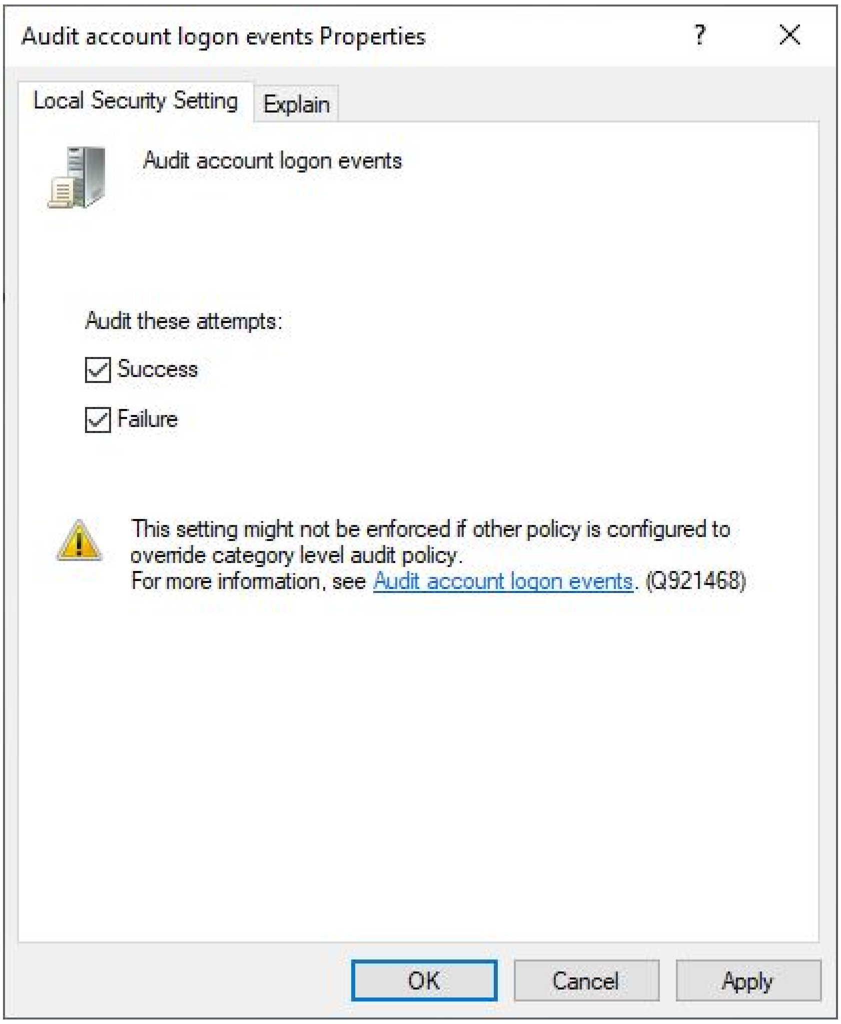


- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Adva
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

2. Click on **Local Policies > Audit Policy** in the structure tree on the left and select the policy **Audit object access**.

3. Select the **Failure** check box if you only want to log unsuccessful accesses. Also select the **Success** check box if you also want to log successful accesses.



Audit account logon events Properties

Audit account logon events

Audit these attempts:

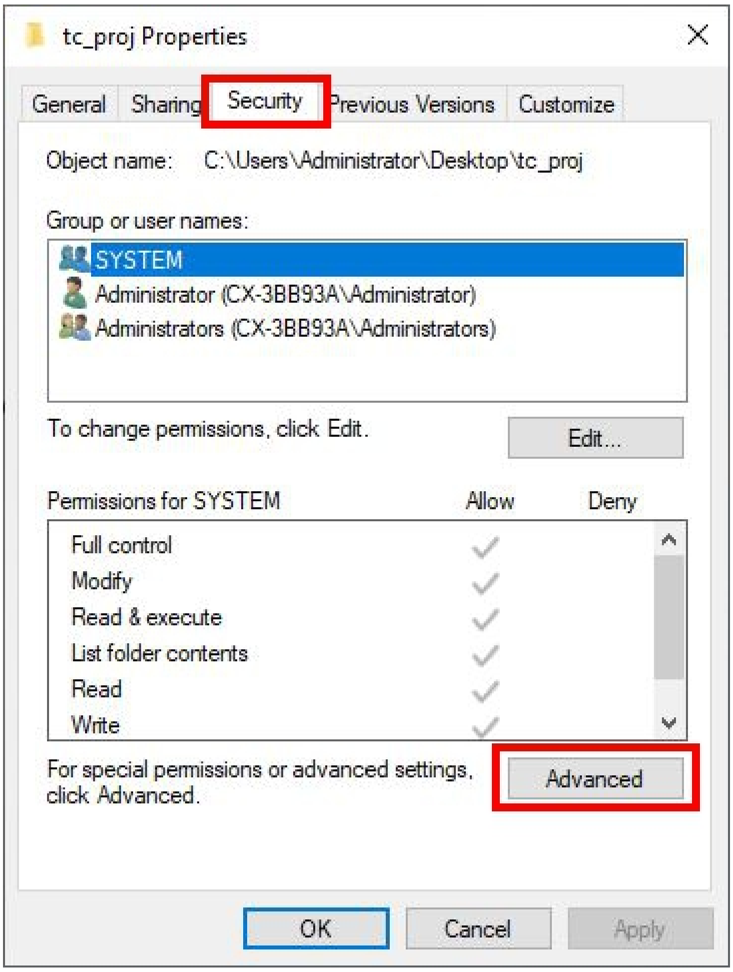
☑ Success

☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account logon events. (Q921468)

4. Right-click on the relevant file or folder and then on **Properties**.

5. Select the **Security** tab and then click on **Advanced**.



Object name: C:\Users\Administrator\Desktop\tc_proj

Group or user names:

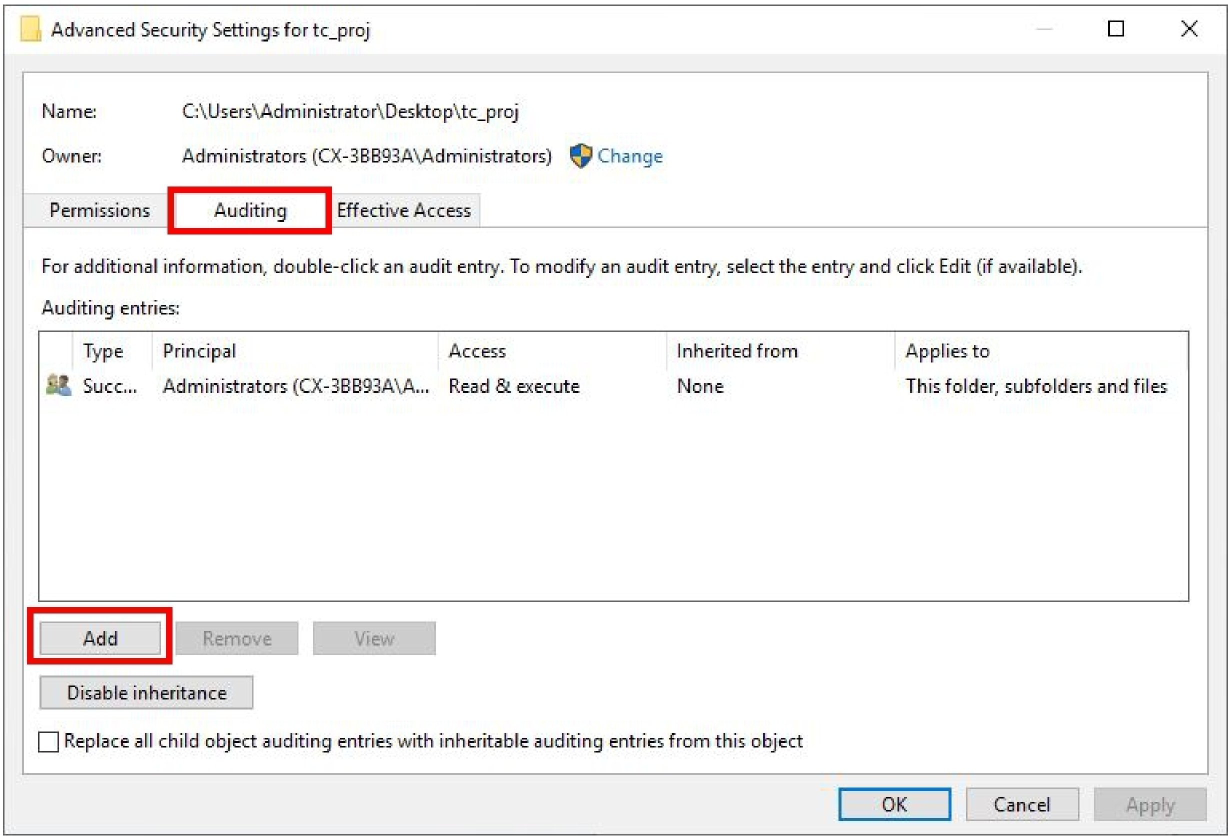
- SYSTEM
- Administrator (CX-3BB93A\Administrator)
- Administrators (CX-3BB93A\Administrators)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

6. Select the **Auditing** tab, click on **Add** to create a new entry for auditing.



Name: C:\Users\Administrator\Desktop\tc_proj

Owner: Administrators (CX-3BB93A\Administrators)

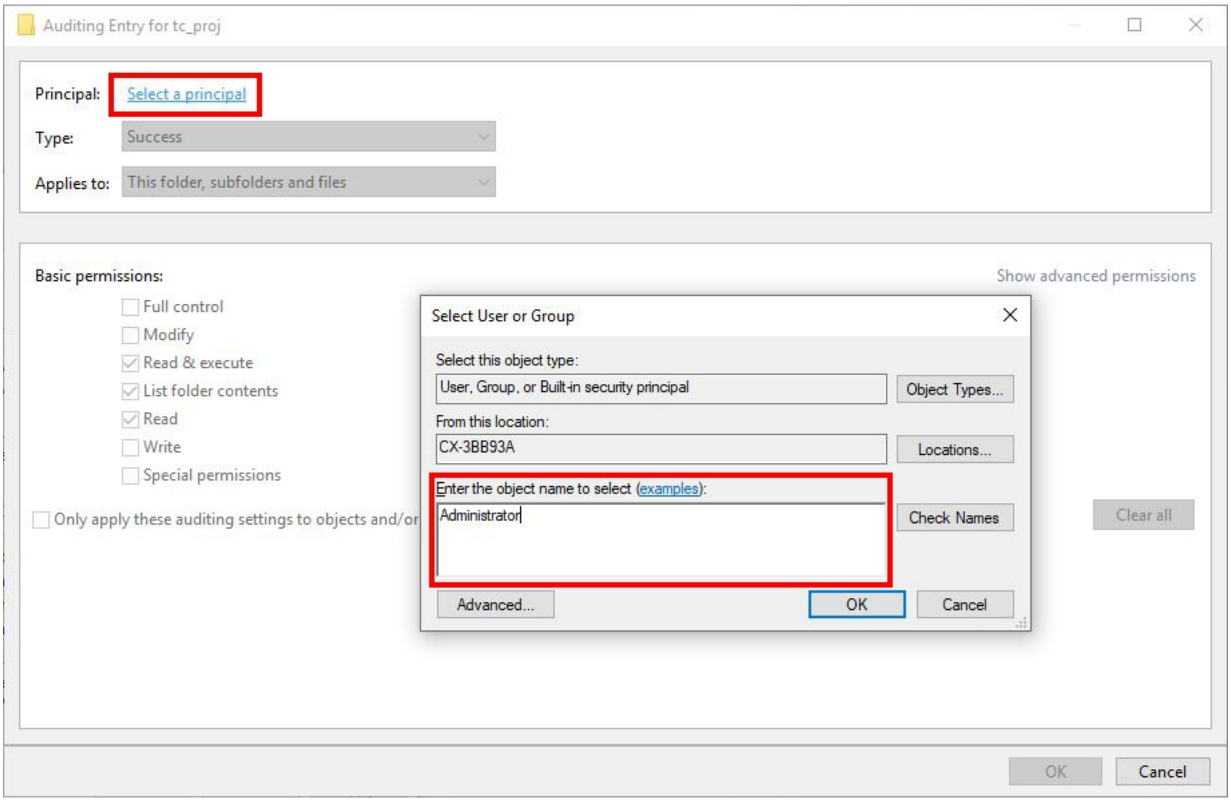
For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Administrators (CX-3BB93A\A...	Read & execute	None	This folder, subfolders and files

□ Replace all child object auditing entries with inheritable auditing entries from this object

7. To set up auditing for a user or group, enter the name of the desired user or group and then select **OK**.



Auditing Entry for tc_proj

Principal: Select a principal

Type: Success

Applies to: This folder, subfolders and files

Basic permissions:

□ Full control
□ Modify
☑ Read & execute
☑ List folder contents
☑ Read
□ Write
□ Special permissions

□ Only apply these auditing settings to objects and/or

Select User or Group

Select this object type: User, Group, or Built-in security principal

From this location: CX-3BB93A

Enter the object name to select (examples): Administrator

8. The logged entries can now be viewed in the **Event Viewer**, which you can call up with **[Windows key] + [R]** and the entry **eventvwr**. The entries can then be viewed under **Windows Logs > Security**.

5.5 Programs

5.5.1 Whitelisting for programs

Application Whitelisting prevents the execution of all programs that have not been approved for the system. Via a Whitelist, the administrator creates a list of approved applications that the system is allowed to execute. Unlike with antivirus software, no continuous updates are necessary in order to close current security holes. The list only needs to be expanded when new applications are added. In industrial practice, this list is often easier to maintain than antivirus software. The built-in Windows 10 feature is called AppLocker.

Whitelisting measures allow you to specify explicitly which programs can be executed on the system. These measures provide protection against untrusted code.

Windows offers two different methods for whitelisting:

- Software Restriction Policies (SRP)
- AppLocker

The Software Restriction Policies offer scope for explicitly specifying which programs can be executed on the system. All other programs can then no longer be executed. These policies are available through the Local Security Policy.

AppLocker is available from Windows 7 and has an extended range of functions. Differences between AppLocker and SRP are documented here.

5.5.1.1 Software Restriction Policies (SRP)

A security level can be set as default. Exceptions can be defined for the default levels.

Security level	Description
Not permitted	Programs cannot be executed.
Default user	Programs can be run with the permissions of a default user.
Not restricted	Each user can run programs without restriction.

The following exception rules can be defined for certain programs. They are referred to as additional rules:

Type	Description
Hash Rule	For unmodified program files in a certain version, the file name is ignored. *Notice* **For updates, these hash rules must be updated.**
Certificate Rule	For correctly signed program files whose publisher certificate is set.
Path Rule	For program files in certain paths. The paths can also contain placeholders and environment variables (such as %PROGRAMFILES%).
Internet zone Rule	Programs located in the network zones defined by Internet Explorer.

The following steps help you to set up a kiosk mode for Windows 10, in which several applications can be run:

https://docs.microsoft.com/en-us/windows/configuration/lock-down-windows-10-applocker

A general deployment guide from Microsoft can be found here:

https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-policies-deployment-guide

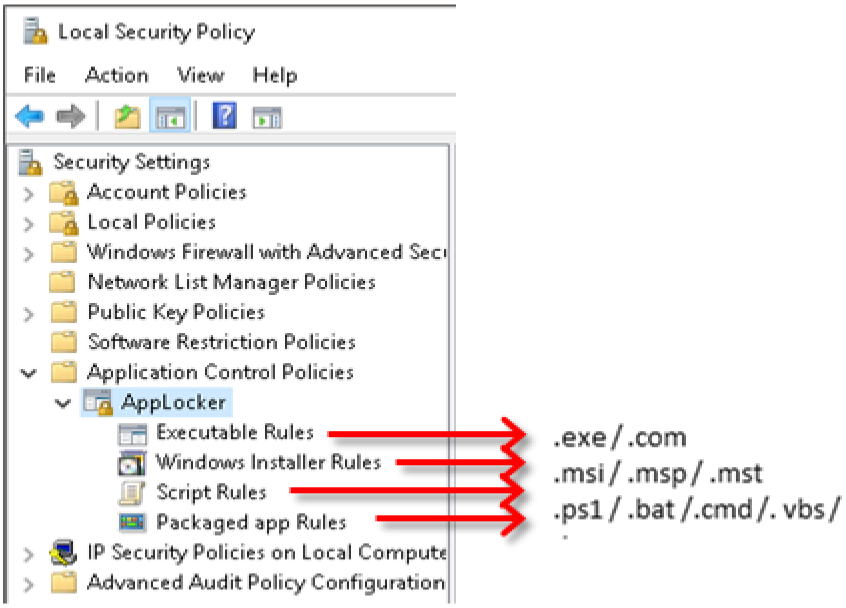
See also:

- AppLocker [▶ 32]

5.5.1.2 AppLocker

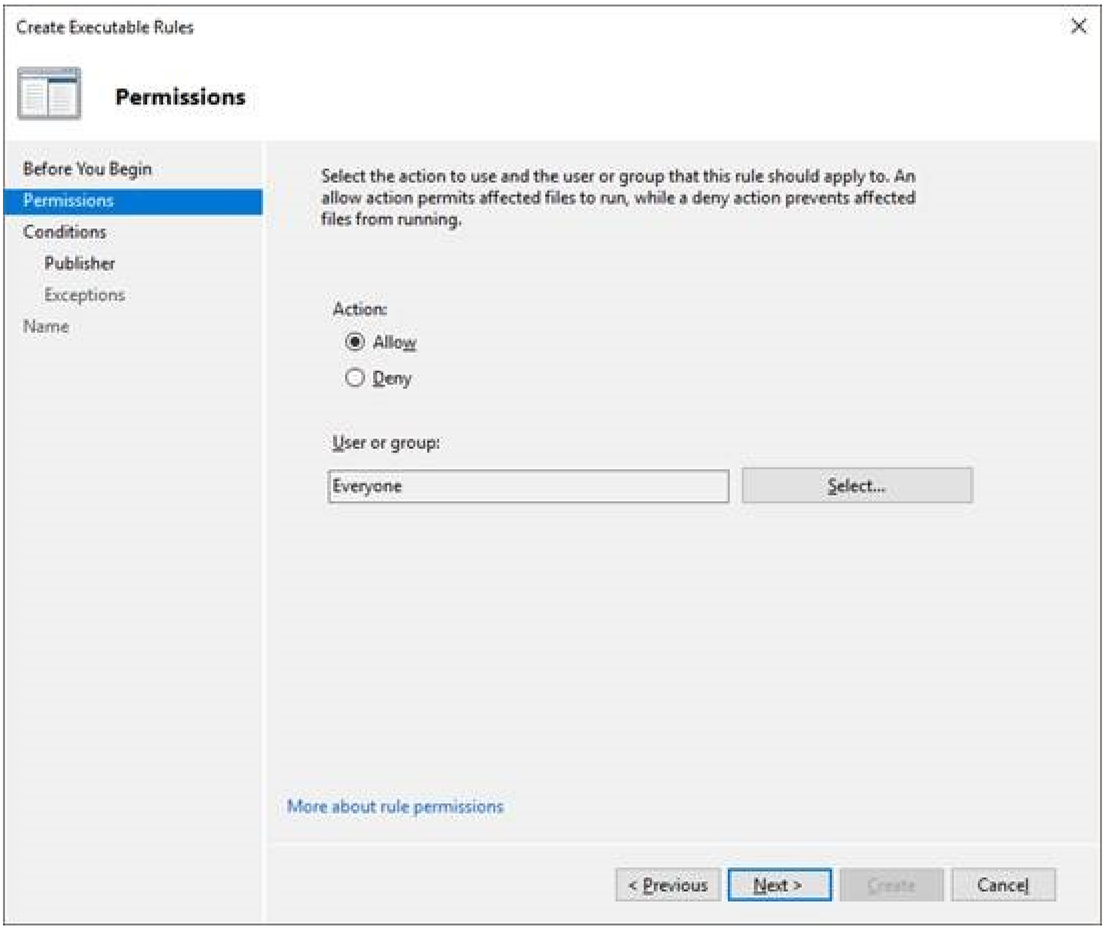
The AppLocker offers the possibility to restrict the running of programs.

1. Open the security policies by running **secpol.msc**. Select **Application control policies** and below that **AppLocker**. Various data types can be covered by the rules:


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
Packaged app Rules
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
.exe / .com
.msi / .msp / .mst
.ps1 / .bat /.cmd /. vbs /

2. You can select **Create new rule** by right clicking one of the rules.

3. Select **Allow** or **Refuse** and a **User** or a **Group**, to whom the rule should apply:



Create Executable Rules

Permissions

Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.

Action:

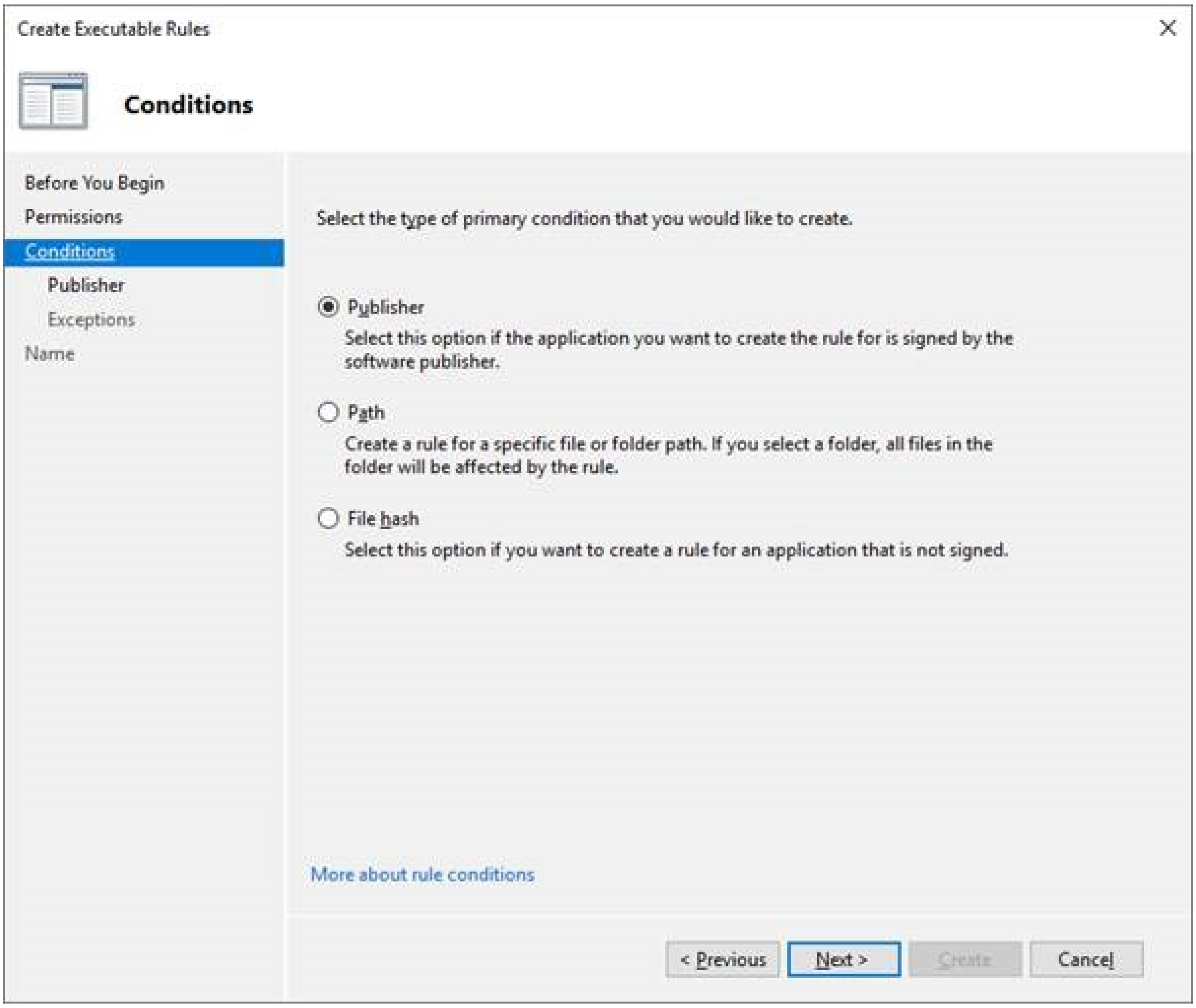
● Allow

○ Deny

User or group:

Everyone

4. Select the type of primary condition for your new rule:



Create Executable Rules

Conditions

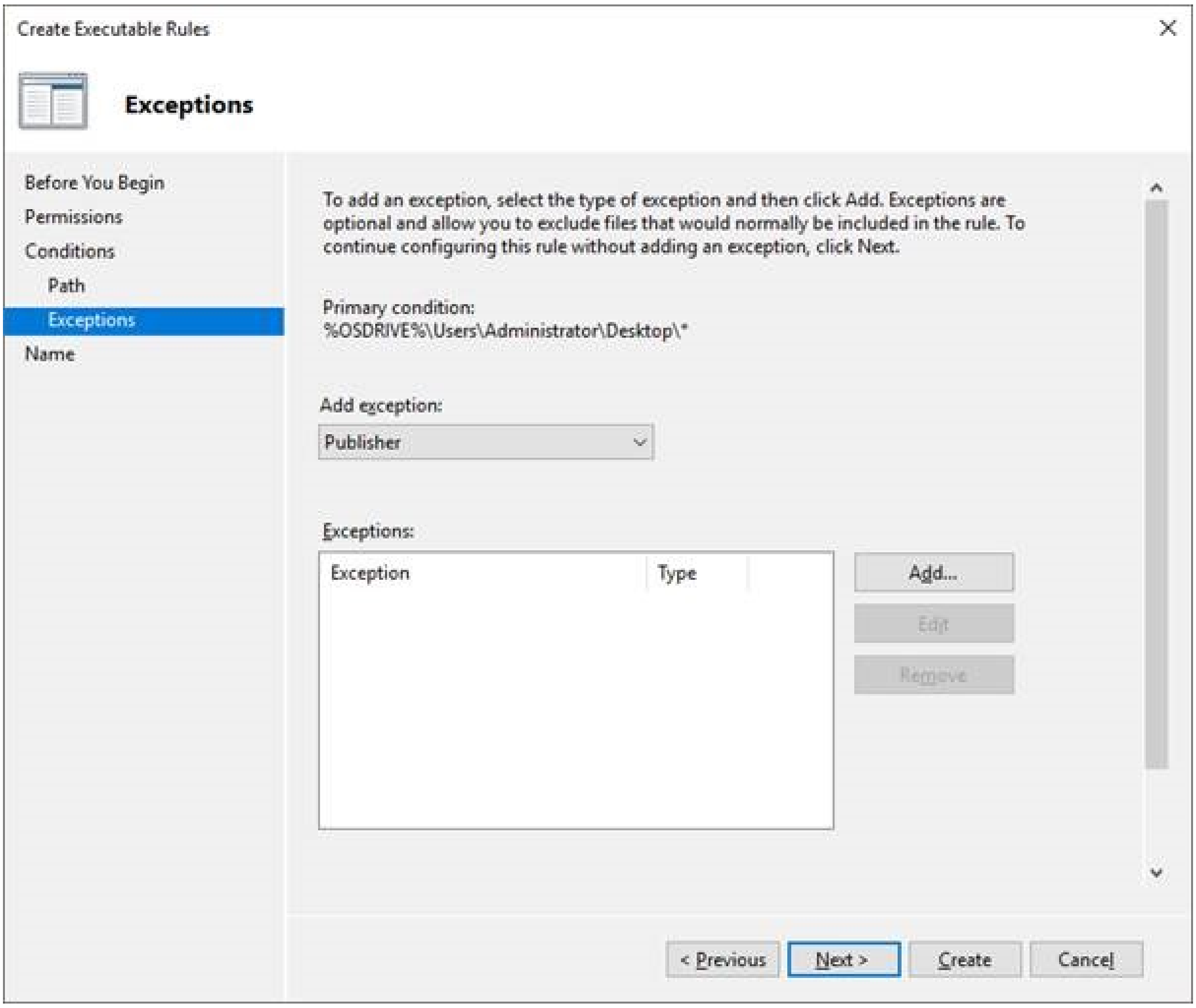
Select the type of primary condition that you would like to create.

● Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.

○ Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

○ File hash
Select this option if you want to create a rule for an application that is not signed.

5. You can specify the rule more precisely by specifying **Publisher, Path** or **File hash**. In addition, Publishers, Paths and File hashes can each be excluded from the rule:



Create Executable Rules

Exceptions

To add an exception, select the type of exception and then click Add. Exceptions are optional and allow you to exclude files that would normally be included in the rule. To continue configuring this rule without adding an exception, click Next.

Primary condition:
%OSDRIVE%\Users\Administrator\Desktop\*

Add exception:
Publisher

Exceptions:

Exception	Type

⇨ The configuration is now complete.

Notes:

- AppLocker works by default as an "Allow list".
  - AppLocker initially checks whether there are any rules that refuse the actions.
  - Rules that refuse an action are given a higher priority than rules that allow an action.
- All Windows system files should be allowed.
- So-called "standard rules" (rules for Windows system files) can be created.
- You can lock yourself out of your own system via the AppLocker.

Additional notes:

- Rules can be imported / exported from one machine to another.
- The rules are saved in HLKM\Software\Policies\Microsoft\Windows\SrpV2.
- The application identity service (Appidsvc) must be started for the file identification.

Further information can be found in the Microsoft documentation:

- https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/using-software-restriction-policies-and-applocker-policies

5.5.2 Hiding programs

To prevent the use of features that should only be accessible to a limited group of users, they can be blocked or hidden through operating system functions.

Programs and their execution can also be restricted by whitelisting measures.

See also:

Whitelisting for programs [▶ 31]

Under Windows, the following functions can be hidden via changes in the registry:

Registry

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
```

An entry with the name "DisableRegistryTool" and value 1 prevents a user from starting a registry editor.

Command prompt

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
```

An entry called "DisableCMD" has a different effect depending on the value:

- 0: Command line access is allowed and batch files can be executed.
- 1: Command line access is not allowed and batch files cannot be executed.
- 2: Command line access is not allowed but batch files can be executed.

Network Environment

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEum\
```

A DWORD entry with the name "{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}" and value 1 hides the network environment.

Individual drive letters

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
```

REG_DWORD entries with the names "NoViewOnDrive" and "NoDrives" can be used to configure which drive letters should be restricted. "NoViewOnDrives" restricts access to drives. "NoDrives" only hides the drive letters. Access is still possible. The value to be entered is the sum of the entries for the corresponding letters in the following table:

A: 1	**G**: 64	**M**: 4096	**S**: 262144	**Y**: 16777216
B: 2	**H**: 128	**N**: 8192	**T**: 524288	**Z**: 33554432
C: 4	**I**: 256	**O**: 16384	**U**: 1048576	**All**: 67108863
D: 8	**J**: 512	**P**: 32768	**V**: 2097152	
E: 16	**K**: 1024	**Q**: 65536	**W**: 4194304	
F: 32	**L**: 2048	**R**: 131072	**X**: 8388608	

For example, to restrict access to drives A, B, D and P, enter the value 1 + 2 + 8 + 32768 = 32779. After setting the value, the operating system must be restarted for the setting to take effect.

Further setting options are summarized here.

5.5.3 Removing components that are no longer needed

To reduce the size of the attack surface, unneeded programs and operating system components should be removed.

The removal of system components should only be done by well-versed persons. Negative side effects may occur and programs can no longer be run correctly.

In the **Control Panel** under **Programs and Features** you can uninstall programs and Windows components that are not needed.

Run "control appwiz.cpl" to access this feature directly.

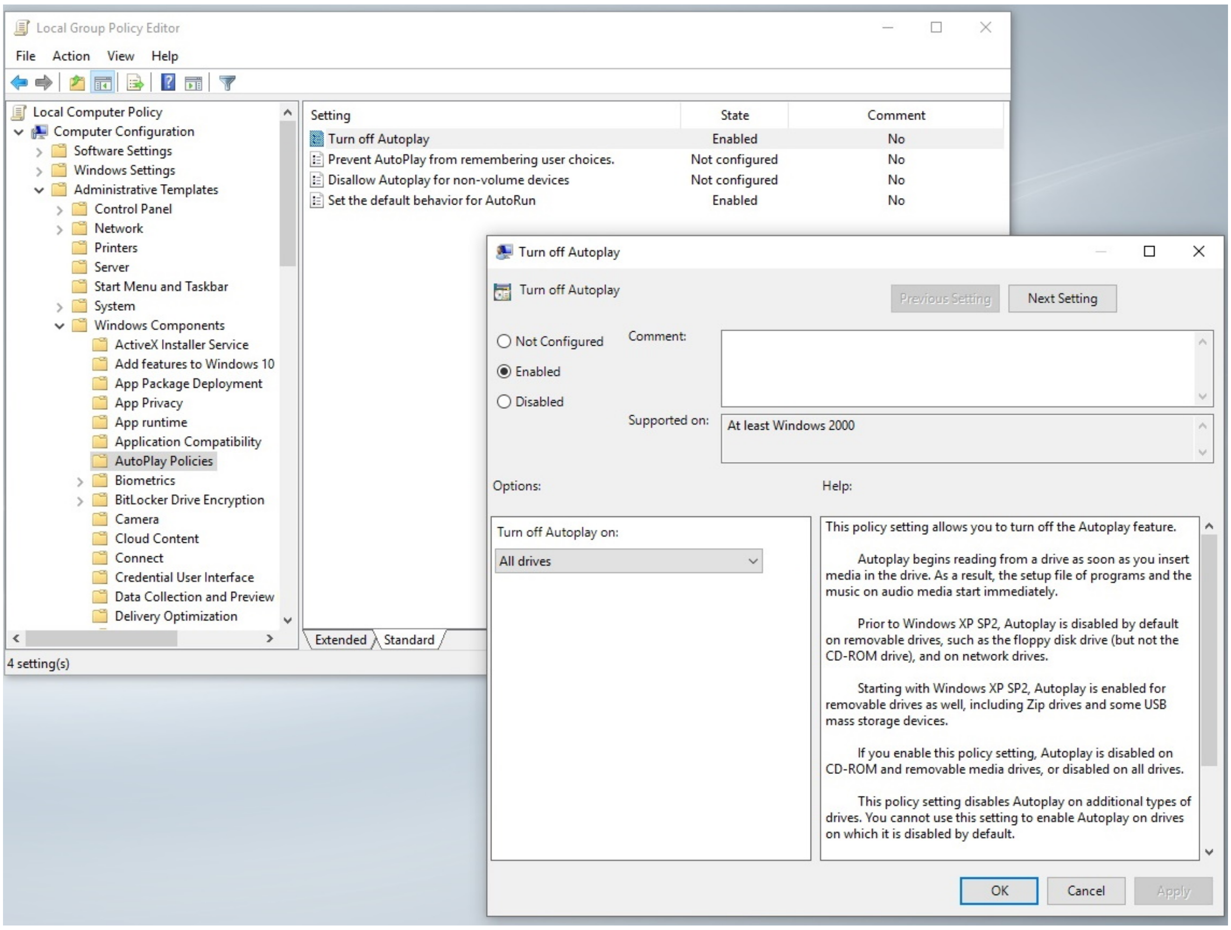
5.5.4 Autostart

A controller can easily be infected via the mechanisms when external devices are connected (e.g. USB storage media or keyboards). This applies in particular if the operating system executes automatic actions as soon as a USB medium is plugged in.

If these mechanisms are not needed, they should be deactivated. A distinction is made here between AutoPlay (playback of media with already installed software) and AutoRun (starting of programs).

In order to completely deactivate AutoRun and AutoPlay via the group policies, the following steps should be taken.

1. Open the group policies (run "gpedit.msc") and navigate to Computer Configuration> Administrative Templates > Windows Components > **AutoPlay Policies**. There, configure the policies **Turn off AutoPlay** and **Set the default behavior for AutoRun** as follows



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

Turn off Autoplay

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

Turn off Autoplay on: All drives

This policy setting allows you to turn off the Autoplay feature.

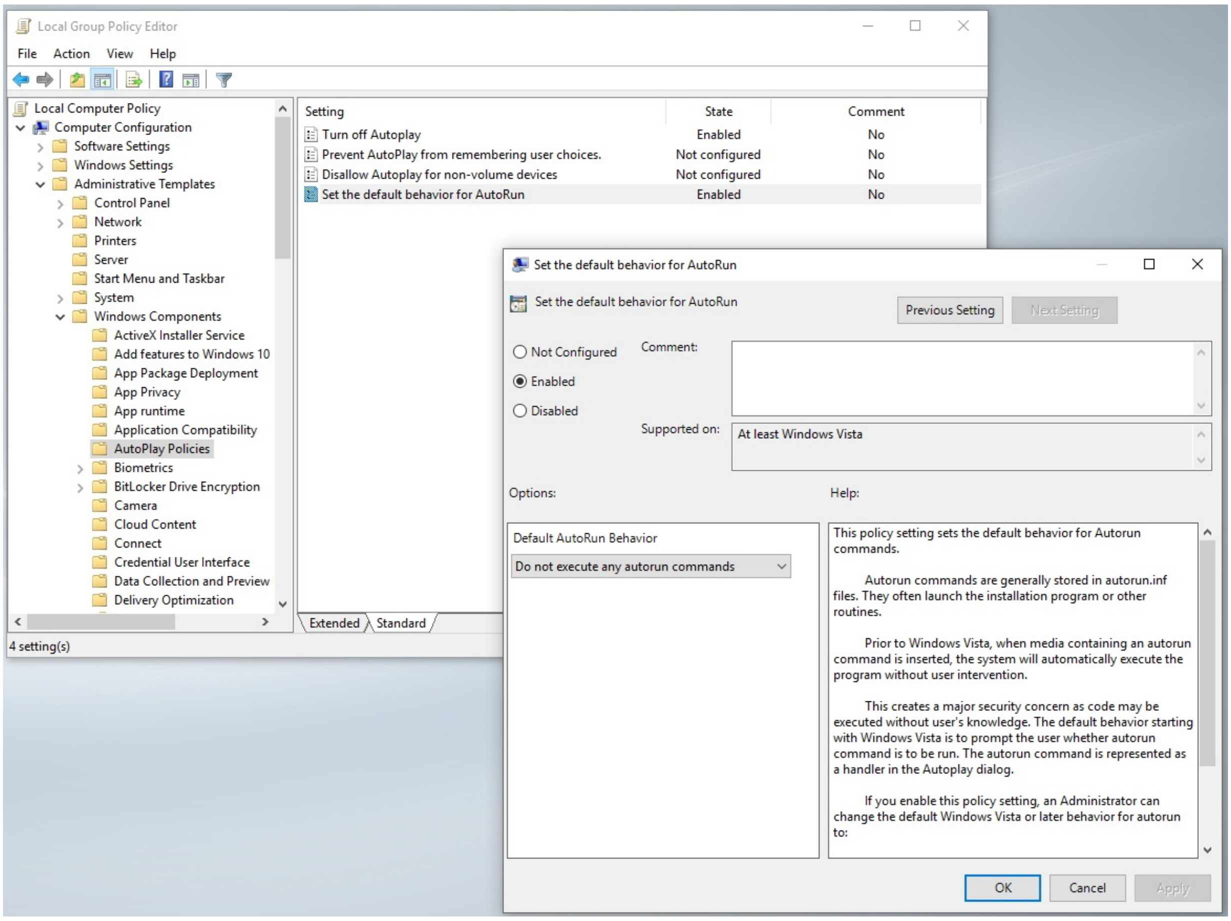
Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately.

Prior to Windows XP SP2, Autoplay is disabled by default on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.

Starting with Windows XP SP2, Autoplay is enabled for removable drives as well, including Zip drives and some USB mass storage devices.

If you enable this policy setting, Autoplay is disabled on CD-ROM and removable media drives, or disabled on all drives.

This policy setting disables Autoplay on additional types of drives. You cannot use this setting to enable Autoplay on drives on which it is disabled by default.



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

Set the default behavior for AutoRun

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

Default AutoRun Behavior: Do not execute any autorun commands

This policy setting sets the default behavior for Autorun commands.

Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines.

Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention.

This creates a major security concern as code may be executed without user's knowledge. The default behavior starting with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

If you enable this policy setting, an Administrator can change the default Windows Vista or later behavior for autorun to:

⇨ Following a restart, the settings are complete.

5.5.5 Antivirus programs

Antivirus software protects the system against malware that infiltrates the system via data carriers or the network. It represents a blacklist of known malware. Antivirus software must always be kept up to date so that malware can be recognized. There are disadvantages to this.

Antivirus programs recognize already known malware ("blacklist") and attempt to prevent the execution of the malware code.

However, through the necessary updates of this blacklist ("malware pattern") the antivirus programs also increase the danger to a system.

If the same program is always run on a machine, the previously described whitelist method should be used. In every case, you must weigh up whether a blacklist method as in the case of antivirus programs is advantageous on the whole. Overall, the higher configuration effort of the whitelisting method must be compared to the constant updates of the antivirus programs.

Windows Defender has proven in the past to be reliable and compatible with TwinCAT. However, it must always be updated to the latest version in order to close current security holes.

In particular in connection with TwinCAT, the use of antivirus programs is to be precisely evaluated, as they set themselves up deep in the operating system and can thus impair the real-time integration of TwinCAT.

TwinCAT has its own description for compatibility with antivirus programs:

Compatibility of antivirus programs

For more information, see the Microsoft documentation: https://support.microsoft.com/en-us/help/4013263/windows-10-stay-protected-with-windows-security

5.6 Write filter

Windows write filters are tools specially developed by Microsoft Windows to protect a partition against write accesses. The write accesses are redirected to the RAM and the partition is secured in a preconfigured state as a result. Following a restart, the system is automatically reset to the originally defined state.

A write protection filter can be configured, depending on the use case. In this way the system is protected from undesirable write access. Exclusions define the folders that still allow write accesses.

Significance for IT security

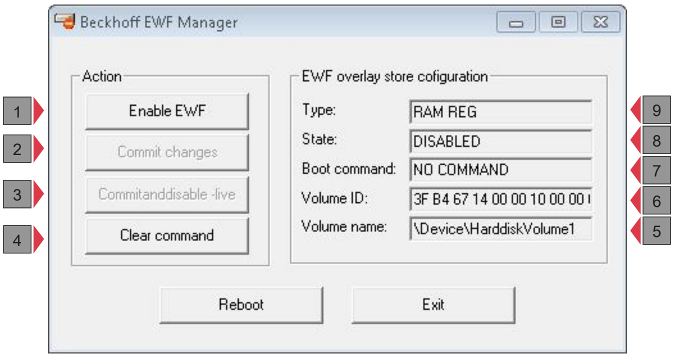
From an operator point of view, it makes sense if the changes made by malware are reversed after a restart and operation can be resumed. As a result of this, however, less information can be collected about the infection or attack, which may occur again.

Also, turning the write filter on and off is not secured. If the user in whose context the attack takes place can change the write filter settings, an attacker can do this, too.

EWF

The EWF (Enhanced Write Filter) protects the entire partition from write accesses without exceptions. If the EWF is active, all write accesses are redirected to the RAM. Following a restart or a power failure, the system is returned to its original state.

The EWF is controlled by the Beckhoff EWF Manager software, which is already installed by default.



Type: RAM REG
State: DISABLED
Boot command: NO COMMAND
Volume ID: 3F B4 67 14 00 00 10 00 00 0
Volume name: \Device\HarddiskVolume1

Fig. 1: Beckhoff EWF Manager, user interface.

Table 1: Key to Beckhoff EWF Manager.

No.	Description
1	Switch EWF on, switch EWF off.
2	Data can be accepted at runtime if the EWF is active.
3	Switch EWF off without a restart.
4	Reset boot command to NO COMMAND.
5	Name of the partition.
6	ID of the partition on which the EWF is executed (in hexadecimal).
7	Indicates which commands are executed after the restart. The following commands exist: • NO COMMAND, no changes. • ENABLE, the EWF is switched on after the restart. • DISABLE, the EWF is switched off after the restart. • COMMIT, data are written to the storage medium when shutting down, even though the EWF is switched on.
8	Indicates the current status, i.e. whether the EWF is switched on or switched off.
9	Indicates the EWF mode. In RAM REG mode, all accesses are redirected to the RAM and the EWF settings are stored in the Registry.

Requirements:

- Windows Embedded Standard 2009 or
- Windows Embedded Standard 7 P

Activate the EWF as follows:

1. Start the Industrial PC or Embedded PC and click **Beckhoff EWF Manager** under **Start < All Programs < Beckhoff EWF Manager**.
2. Under **Action**, click the **Enable EWF** button.
3. Confirm the settings so that the changes become effective.

⇨ The changes are only active after a restart. You have successfully activated the EWF.

FBWF

As opposed to the EWF, the FBWF operates at file level. This makes it possible to define possible exceptions and to allow write accesses to individual files or folders. All other write accesses are redirected to the RAM. Following a restart, the system is returned to its original state.

As soon as the FBWF is activated, some folders are released for direct write access. For example, the folder *C:\Data* is available for writing permanent data. Through the release of the folder *C:\TwinCAT\Boot*, a new TwinCAT boot project can be loaded to the computer without having to deactivate the FBWF first

EWF vs. FBWF

Do not run EWF and FBWF at the same time

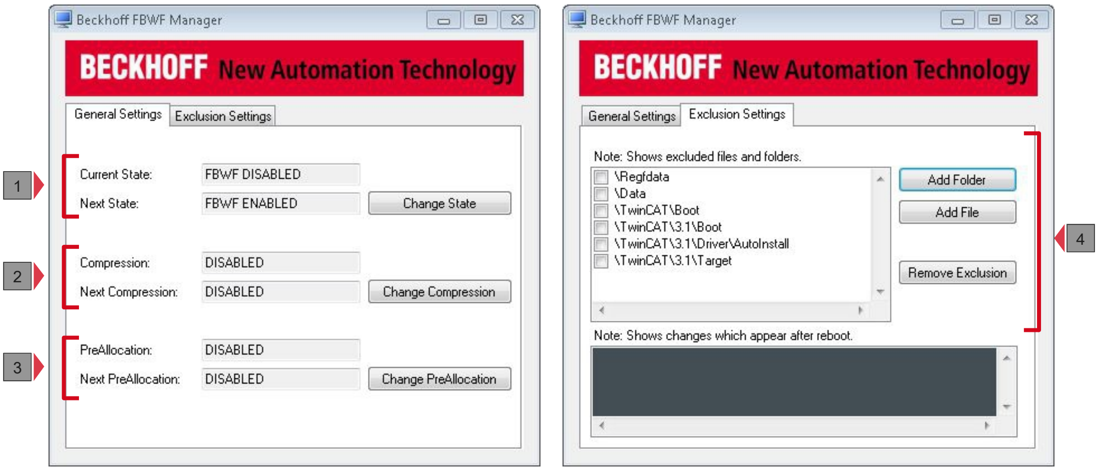
If both write filters are activated, the FBWF exceptions will be intercepted by the EWF and will be lost when the computer is restarted.

Do not activate the two write filters EWF and FBWF at the same time.

In most cases the FBWF is the better choice, as it is simpler to operate and allows direct write accesses. However, there are scenarios in which the EWF is indispensable, e.g. HORM (Hibernate Once/Resume Many) is not supported by the FBWF. In addition, the use of compressed NTFS volumes is not possible with the FBWF.

Control with the Beckhoff FBWF Manager

The FBWF is controlled by the Beckhoff FBWF Manager software, which is already installed by default.



Current State: FBWF DISABLED
Next State: FBWF ENABLED
Compression: DISABLED
Next Compression: DISABLED
PreAllocation: DISABLED
Next PreAllocation: DISABLED

Note: Shows excluded files and folders.
□ \Regfdata
□ \Data
□ \TwinCAT\Boot
□ \TwinCAT\3.1\Boot
□ \TwinCAT\3.1\Driver\AutoInstall
□ \TwinCAT\3.1\Target

Note: Shows changes which appear after reboot.

Fig. 2: Beckhoff FBWF Manager, user interface.

Table 2: Key to Beckhoff FBWF Manager.

No.	Description
1	The FBWF is switched on or off by the **Change State** button. The current and next states are displayed. Changes are only ever accepted after a restart.
2	Compression can only be activated when the FBWF is active. Indicates whether the compression of the FBWF overlay is active.
3	PreAllocation can only be activated when the FBWF is active. Indicates whether the PreAllocation is activated.
4	Exclusions are created on the **Exclusion Settings** tab. When an FBWF is active, folders are added to the exclusion list by default.

Requirements:

- Windows Embedded Standard 2009 or
- Windows Embedded Standard 7 P

Activate the FBWF as follows:

1. Start the Industrial PC or Embedded PC and click **Beckhoff FBWF Manager** under **Start < All Programs < Beckhoff FBWF Manager**.
2. Click the **Change Settings** button on the **General Settings** tab.
3. The **Next State** display changes and the message FBWF ENABLED appears.
4. Restart the Industrial or Embedded PC.

⇨ The changes are only active after a restart. The display **Current State** changes after the restart to FBWF ENABLED. You have successfully activated the FBWF.

5.7 Keyboard filter

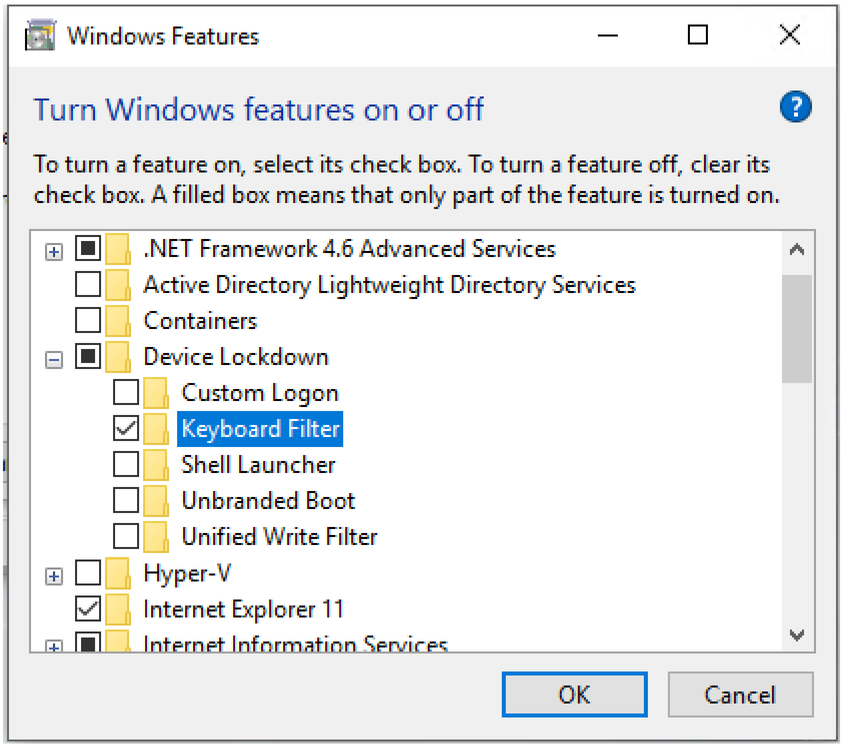
The keyboard filter is a possibility to protect the system from undesirable access. For example, a shortcut that leads to the closing of an application can be blocked. Only keyboard inputs required for the operation of the application are enabled. In addition, shortcuts can be specified that disable the keyboard filter. The option that deactivates the filter for the administrator is also helpful.

Keyboard filters offer a further option to limit a user in his dealing with the operating system and thus to minimize attack possibilities.

Typically, a "kiosk mode" is configured in which, for example, a successfully logged-in user can only start an HMI application. The user has no further possibility to start other programs or to send commands to the IPC, such as shutdown, for example.

Windows 10 provides a service for this purpose. Here, we describe how this is activated and how it can be configured.

First turn on the built-in Windows 10 feature to use the service. To do this, open the dialog **Turn Windows features on or off** and select the feature **Keyboard Filter** under the menu item **Device Lockdown**. Then restart the PC.

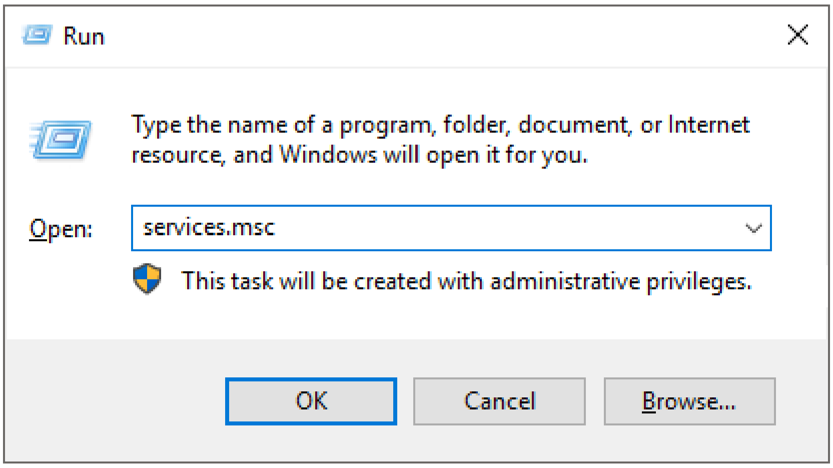


Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ■ .NET Framework 4.6 Advanced Services
- □ Active Directory Lightweight Directory Services
- □ Containers
- ■ Device Lockdown
  - □ Custom Logon
  - ☑ Keyboard Filter
  - □ Shell Launcher
  - □ Unbranded Boot
  - □ Unified Write Filter
- □ Hyper-V
- ☑ Internet Explorer 11
- ■ Internet Information Services

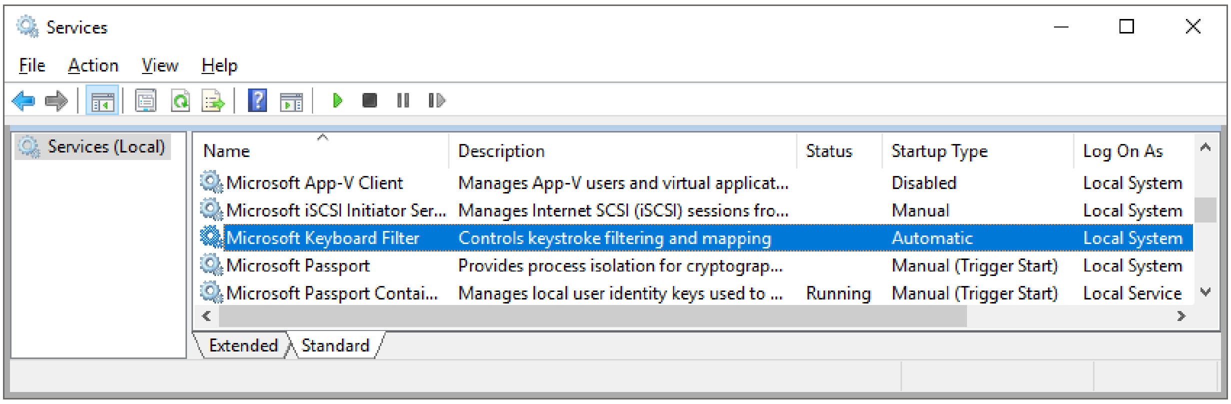
1. Start the **Microsoft Keyboard Filter** service.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

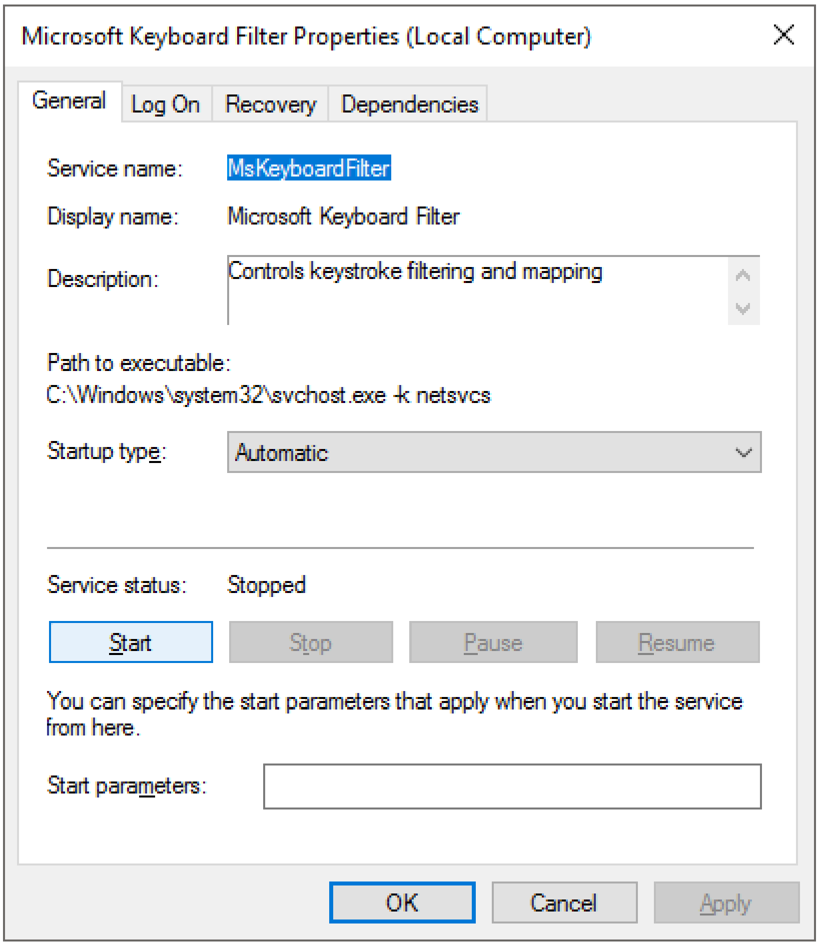
Open: services.msc

This task will be created with administrative privileges.



Name	Description	Status	Startup Type	Log On As
Microsoft App-V Client	Manages App-V users and virtual applicat...		Disabled	Local System
Microsoft iSCSI Initiator Ser...	Manages Internet SCSI (iSCSI) sessions fro...		Manual	Local System
Microsoft Keyboard Filter	Controls keystroke filtering and mapping		Automatic	Local System
Microsoft Passport	Provides process isolation for cryptograp...		Manual (Trigger Start)	Local System
Microsoft Passport Contai...	Manages local user identity keys used to ...	Running	Manual (Trigger Start)	Local Service

2. Set the startup type to **automatic**:



Service name: MsKeyboardFilter

Display name: Microsoft Keyboard Filter

Description: Controls keystroke filtering and mapping

Path to executable:
C:\Windows\system32\svchost.exe -k netsvcs

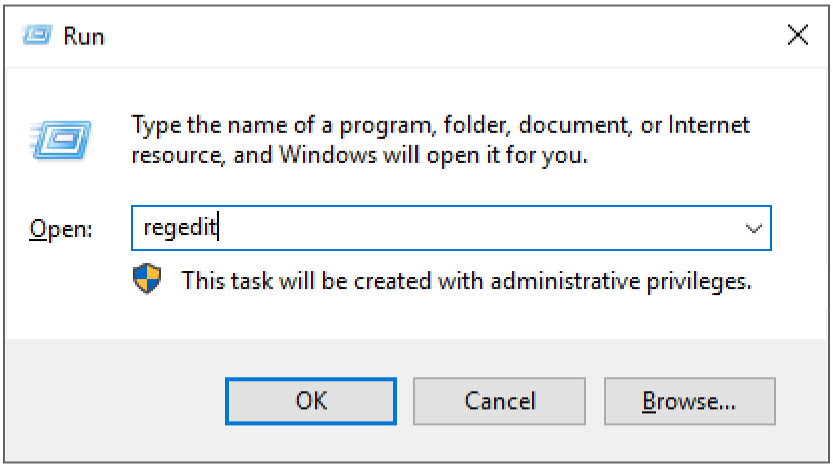
Startup type: Automatic

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

3. Open the **Registry Editor**



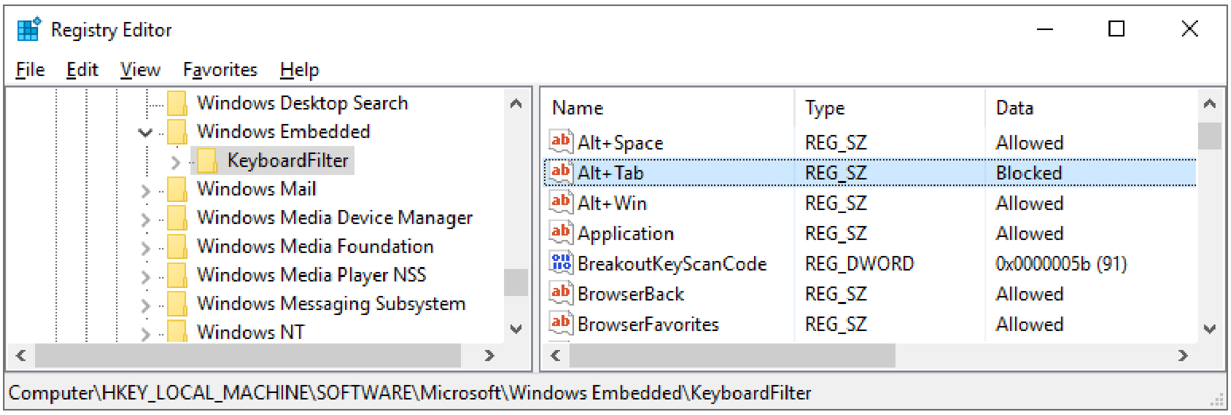
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

This task will be created with administrative privileges.

4. Navigate to **KeyboardFilter**: **HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows Embedded**



Registry Editor

Name	Type	Data
Alt+Space	REG_SZ	Allowed
Alt+Tab	REG_SZ	Blocked
Alt+Win	REG_SZ	Allowed
Application	REG_SZ	Allowed
BreakoutKeyScanCode	REG_DWORD	0x0000005b (91)
BrowserBack	REG_SZ	Allowed
BrowserFavorites	REG_SZ	Allowed

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Embedded\KeyboardFilter

5. Both values and commonly used shortcuts are listed in the tables below.

⇨ The keyboard filter is now activated.

The following values stand for the individual shortcuts:

Value	Description
"Allowed"	Allow shortcut
"Blocked"	Block shortcut
DisableKeyboardFilterForAdministrator to "1"	Keyboard filter is disabled for administrators
BreakoutKeyScanCode to „01“	Scancode for ESC as Breakout

The following shortcuts are usually blocked:

Value	Description
CTRL-SHIFT-ESC	Open task manager
CTRL-ALT-DEL	Open menu with the following options: Lock system Open task manager Change password Shutdown system Switch user

Please refer to the Microsoft documentation for more information: https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/keyboardfilter

5.8 USB filter

In a similar way to whitelisting for applications, USB devices can also be listed as trusted. USB devices that are not in the approved list will not be accepted by the operating system. Hence, for the maintenance of the devices, uniform USB service flash drives can be defined that contain only approved applications and are checked regularly. Non application-specific (e.g. private) USB flash drives therefore cannot cause any harm. The USB filter serves all devices that are connected via USB. These also include, for example, HID devices such as mouse/keyboard, and all mass storage devices such as USB flash drives, hard disks and card readers.

However, the USB filters in an operating system refer to a vendor and product ID (Vendor ID [VID] / Product ID [PID]) in the USB, which have no cryptographic security and can be forged.

In order to block external interfaces such as USB, they can be physically secured, e.g. by a control cabinet. But even if the device is installed in a control cabinet, there are situations where a USB port has been or must be used. In order to reduce the available attack surface, the use of the interface should be adapted and limited in the operating system.

However, the IDs used with the USB filters are not cryptographically secured, meaning that malicious attacks with prepared USB devices can circumvent the USB filters.

There are several ways to restrict USB devices at the operating system level.

- If the device has not yet been installed, installation can be prevented by denying the current user and the SYSTEM user access to the following files:
    - %SystemRoot%\Inf\Usbstor.pnf
    - %SystemRoot%\Inf\Usbstor.inf
    - %SystemRoot%\System32\DriverStore\Usbstor.inf*
- In order to prevent the general use of USB mass storage devices, the entry "ImagePath" can be set to an invalid path in the registry under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSer\services\USBSTOR`.
- How to restrict the use of USB devices more granularly via policy settings (Group Policy) is described here.
- USB interfaces can also be switched off in the BIOS. Note that input devices such as the keyboard and mouse no longer work via interfaces that are switched off in this way.

Note that values set via the registry are NOT automatically synchronized with the values set in the group policy. It is recommended to make the settings exclusively via the group policy.

6 Network communication

At this point an overview will be provided of some relevant measures with regard to communication. Topics outside of the actual IPC – such as network segmenting – are not dealt with.

A list of the ports used for TwinCAT products can be found here: Important TCP/UDP ports [▶ 50] .

6.1 Remote maintenance

Remote maintenance plays an important role in industrial facilities. It enables service technicians and programmers to carry out maintenance work remotely in the event of a malfunction.

Since remote maintenance access routes are generally always available for maintenance purposes and security measures are often neglected in order to be able to react quickly in the event of a malfunction, such access routes are often used for attacks.

Measures at this point are absolutely necessary to prevent attacks that could disrupt system operation.

See also:

- VPN [▶ 49]
- RDP [▶ 49]

6.2 Firewall

Firewall settings are a means of protecting the system from network attacks. Incoming ports that are not needed should be blocked. Even better than that, however, is not to start any services that open these ports. The necessary settings require an overview of the ports used that is coordinated with everyone involved.

A firewall can be used to filter the network packets that are passing through. Depending on the firewall technology, filter rules can be formulated on the basis of address, port, state of communication relationship, content of the packet and much more. Firewalls are thus a tool to reduce the attack surface.

A firewall can be additionally installed software, part of the operating system or a self-contained device. Each of these forms has advantages and disadvantages. For example, unlike an external firewall, with a firewall that is part of the operating system rules for programs can be configured, but it is also easier for malware to modify and activate or deactivate it.

Firewalls with deep-packet inspection, which also evaluate the user data of the data packets, are not able to see the contents of encrypted connections. In order to be able to process the content (e.g. web applications), encryption is often terminated at the firewall and the data for the client is re-encrypted. As a result of this, the contents are visible to the firewall, but the end-to-end encryption is interrupted.

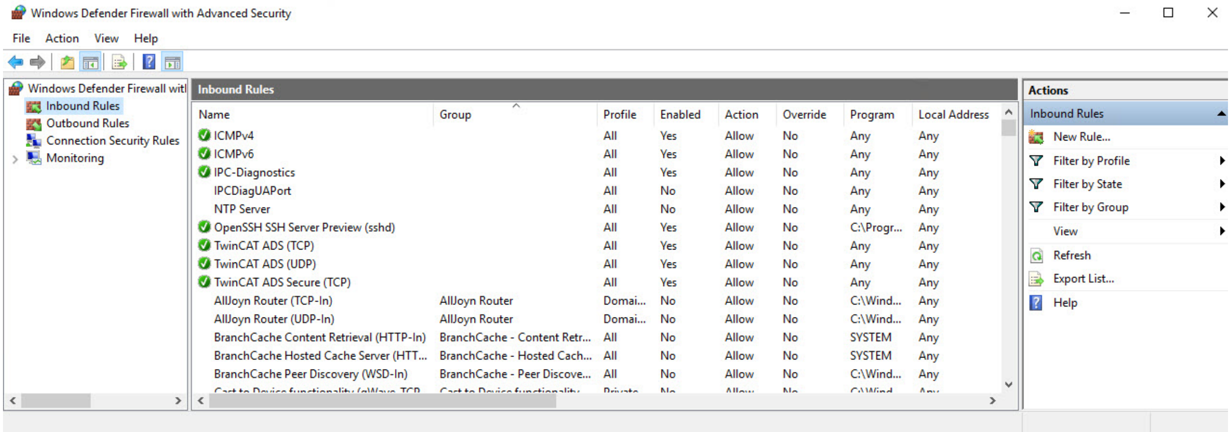
Restrictive, explicit settings for communication via a firewall are an important measure to allow network access only to the necessary extent.

Important TCP/UDP ports [▶ 50] contains a list of TCP/UDP ports that typically need to be considered in order to configure a firewall.

To configure the firewall, the MMC snap-in **Windows Firewall with Advanced Security** can be opened from the command line with the command **wf.msc**. The **New Rule** button can be used to add rules.

Selected rules for the opening of ports or services can be closed again. By right-clicking a rule, the rule can be disabled with **Disable Rule** or deleted with **Delete**.

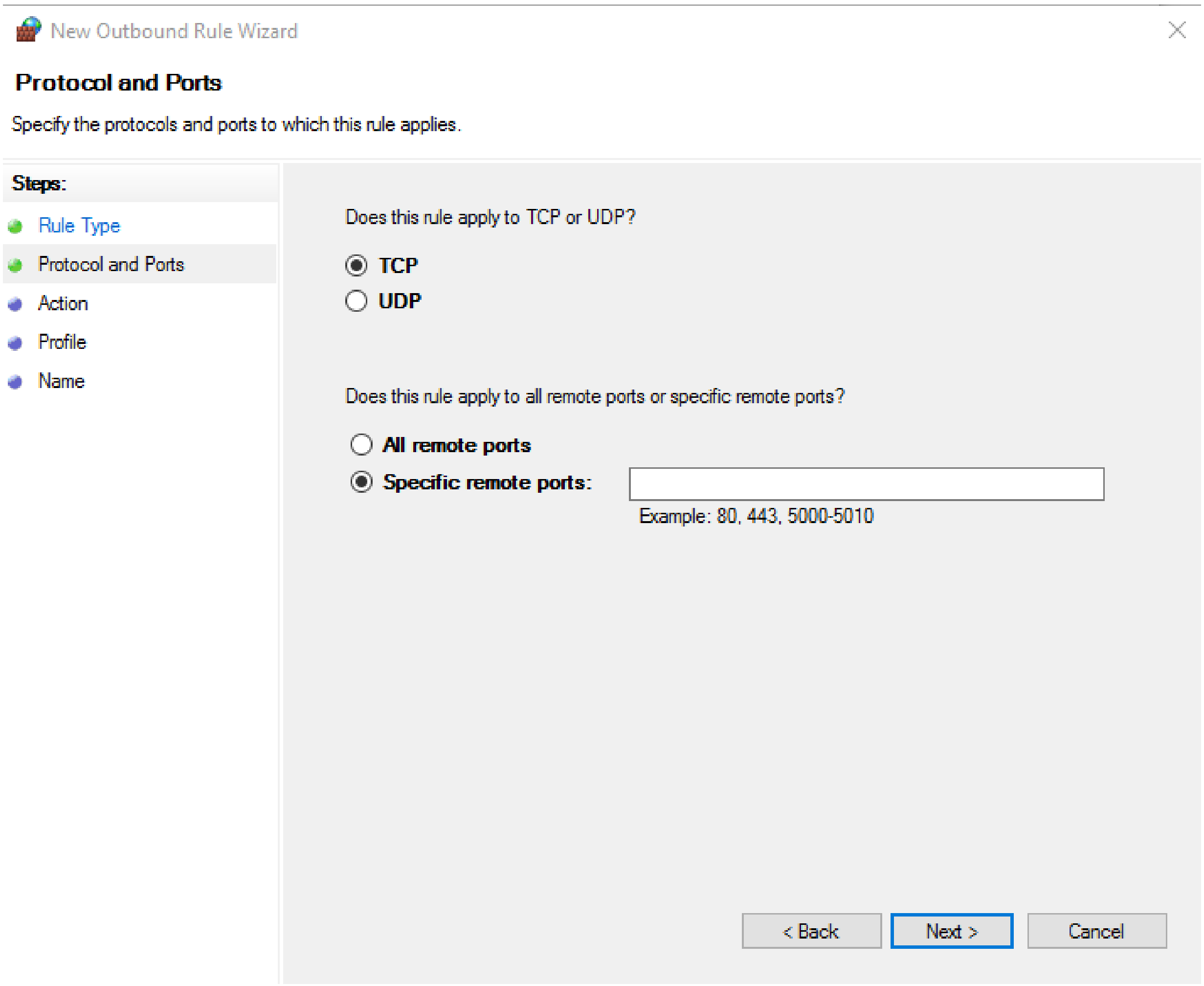
1. Open the firewall settings



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
✓ ICMPv4		All	Yes	Allow	No	Any	Any
✓ ICMPv6		All	Yes	Allow	No	Any	Any
✓ IPC-Diagnostics		All	Yes	Allow	No	Any	Any
IPCDiagUAPort		All	No	Allow	No	Any	Any
NTP Server		All	No	Allow	No	Any	Any
✓ OpenSSH SSH Server Preview (sshd)		All	Yes	Allow	No	C:\Progr...	Any
✓ TwinCAT ADS (TCP)		All	Yes	Allow	No	Any	Any
✓ TwinCAT ADS (UDP)		All	Yes	Allow	No	Any	Any
✓ TwinCAT ADS Secure (TCP)		All	Yes	Allow	No	Any	Any
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	No	Allow	No	C:\Wind...	Any
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	No	Allow	No	C:\Wind...	Any
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	C:\Wind...	Any

2. You can change an existing rule, i.e. allow or block connections, by double-clicking the rule. A new rule is created using **New Rule**.
This starts a wizard that guides you through the options:



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

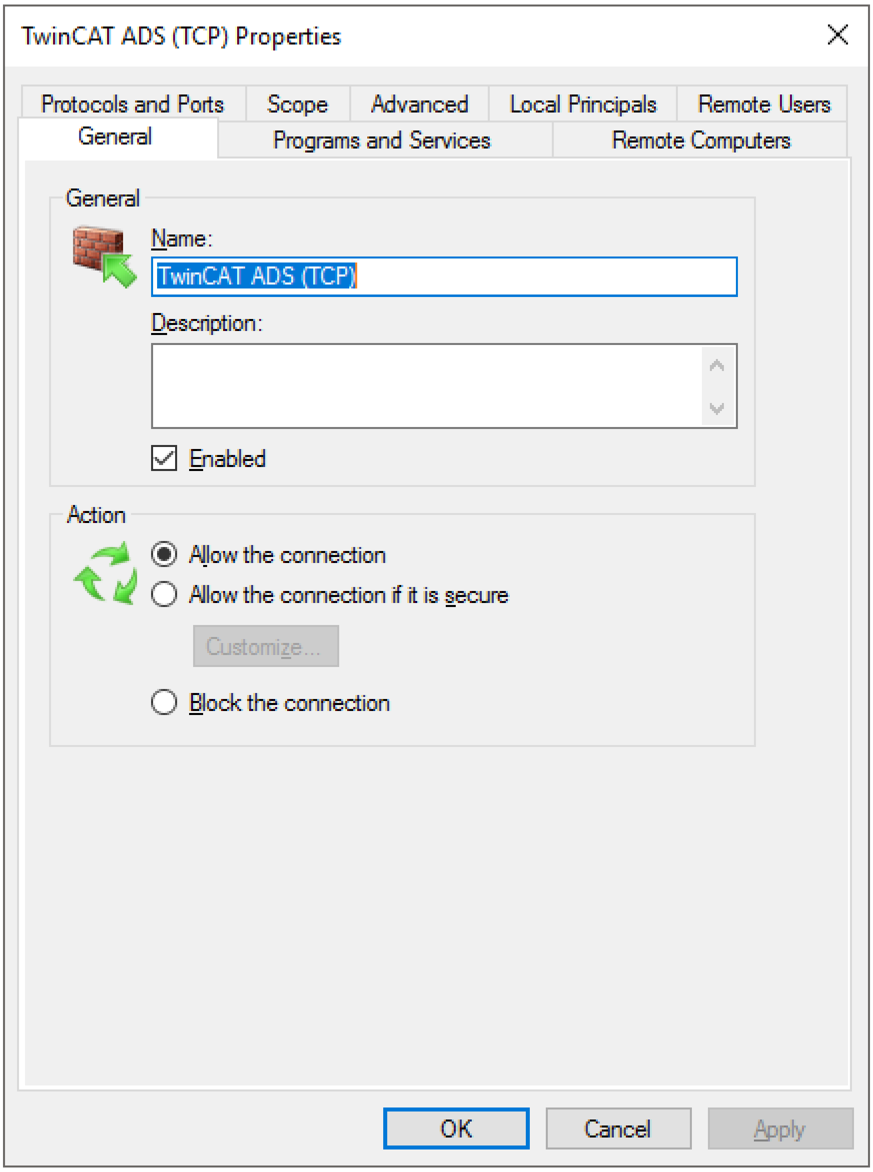
● TCP
○ UDP

Does this rule apply to all remote ports or specific remote ports?

○ All remote ports
● Specific remote ports:

Example: 80, 443, 5000-5010

3. The options of these rules can also be changed afterwards:



TwinCAT ADS (TCP) Properties

General

Name: TwinCAT ADS (TCP)

Description:

☑ Enabled

Action

● Allow the connection

○ Allow the connection if it is secure

○ Block the connection

⇨ You have created a new rule for the firewall.

Further information can be found in the Microsoft documentation:

https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ics/windows-firewall-integration-and-best-practices

6.3 Network technologies

This section describes the security-relevant features of some protocols.

6.3.1 Modbus

The Modbus protocol was originally developed in the late 1970s as a serial communication protocol. The main objectives were to provide a communication protocol for industrial applications that was easy to set up and maintain and transfers data without the need to develop an information model. Because of this simplicity, it has been very popular for 30 years. But this simplicity makes it difficult to use Modbus in modern industrial plants that place more complex demands on a communication protocol, such as security and information models. The original Modbus protocol does not include security measures such as encryption or authentication.

Even though Beckhoff provides two TwinCAT functions for Modbus RTU and Modbus TCP, it is advisable to use more advanced protocols such as OPC UA, which inherently implement security mechanisms.

6.3.2 ADS

The Automation Device Specification (ADS) is a proprietary communication protocol developed by Beckhoff. It is designed for high throughput and portability over different transport protocols (e.g. TCP or serial). ADS was not designed with security in mind and does not include cryptographic operations because of their negative effect on performance and throughput.

It is recommended to use ADS only in secured environments or to use appropriately secured transport channels.

For ADS there are currently two TCP transport channels that support encryption:

- ADS-over-MQTT
- Secure ADS

6.3.3 OPC UA

OPC Unified Architecture (IEC 62541) is the new technology generation of the OPC Foundation for the secure, reliable and manufacturer-neutral transport of raw data and pre-processed information from the manufacturing level into the production planning or ERP system. With OPC UA, all desired information is available to every authorized application and every authorized person at any time and in any place.

Further information can be found in the documentation: TF6100 TC3 OPC UA

6.3.4 VPN

A Virtual Private Network (VPN) makes it possible to establish a virtual LAN between different devices via public networks. In most cases, the data traffic transmitted over the public network is encrypted. VPN solutions can be used, for example, to temporarily tunnel insecure protocols until secure alternatives are operational.

6.3.5 RDP

Remote Desktop Protocol (RDP) is a proprietary Microsoft protocol for graphical remote access.

6.3.6 CerHost

CerHost is a proprietary, non-encrypted protocol from Microsoft for graphic remote access to Windows CE-based operating systems.

It is recommended to use CerHost only in secured environments (for example via secured transport channels).

6.4 Security Gateway

A further option to protect the system from network influences is the use of a security gateway. This hardware solution can be installed in a network in front of an IPC. This way, certain network segments or every single PC can be protected.

In addition to the network protection function, the devices also offer the option, for example, to run antivirus software and thus to monitor a file transfer that is implemented via a local clipboard – without limiting the real-time capability of the actual control computer.

6.5 Important TCP/UDP ports

Depending on the application case, unsecured protocols must be disabled or secured by a lower-level layer, for example by a physically secured network or VPN.

In the case of secured protocols, the security must be commissioned in accordance with the product documentation.

Standard services

The table below provides an overview of the incoming ports that are opened in the normal case in the delivered images

Service	Ports (incoming)
IPC diagnostics	https: 443 / tcp
Remote Desktop – RDP (Windows 7/10 only)	3389 / tcp
TwinCAT ADS	Discovery: 48899 / udp (also outgoing) Not secured: 48898 / tcp (also outgoing). Port under TwinCAT/BSD® closed Secure ADS: 8016 / tcp (also outgoing)

Further services

The table below provides an overview of frequently used services that can additionally be opened

Service	Ports (incoming)
SMB	137-139 / tcp 445 / tcp OPC-UA: 4852 / tcp
Cerhost (Windows CE)	987 / tcp
FTP	21 / tcp

TwinCAT services

The table below provides an overview of the ports typically used with TwinCAT products:

Service	Port (default setting)
TF1810 TwinCAT PLC HMI Web	80 / tcp (incoming) See also: Documentation on TF1810
TF2000 TwinCAT HMI	1010 / tcp (local) 1020 / tcp (incoming) See also: Documentation on TF2000
TF6100 OPC UA	4840 / tcp (UA Server, incoming), changeable 48050/tcp (UA Gateway, incoming), changeable See also: Documentation on TF6100
TF6100 OPC DA	Dynamic (depending on DCOM) between 1024 and 65535 (incoming) See also: Documentation on TF6120
TF6250 Modbus TCP	502 / tcp (incoming), changeable See also: Documentation on TF6250
TF6310 TCP-IP	changeable / tcp (incoming, outgoing) See also: Documentation on TF6310

Service	Port (default setting)
TF6311 TCP/UDP Realtime	changeable / tcp (incoming, outgoing) The communication cannot be influenced by an operating system firewall. See also: Documentation on TF6311
TF6300 FTP	20 / tcp (outgoing) 21 / tcp (outgoing) See also: Documentation on TF6300
TF6420 Database Server	changeable depending on the database / tcp (outgoing) See also: Documentation on TF6420
TF67xx IoT TF35xx Analytics	changeable depending on the broker / tcp (outgoing) See also: Documentation on TF670x and TF35xx
TwinCAT EAP	34980 / udp (incoming), if EAP is used via UDP. The communication cannot be influenced by an operating system firewall. See also: Documentation of EAP
TwinCAT ADS-over-MQTT	changeable depending on the broker / tcp (outgoing) See also: Documentation on ADS-over-MQTT

6.6 IIS web server

By default, the IIS web server is active under Windows and is used, for example, for the Beckhoff Device Manager and for the PLC HMI. In order to further secure the system and restrict access via the web server, you can:

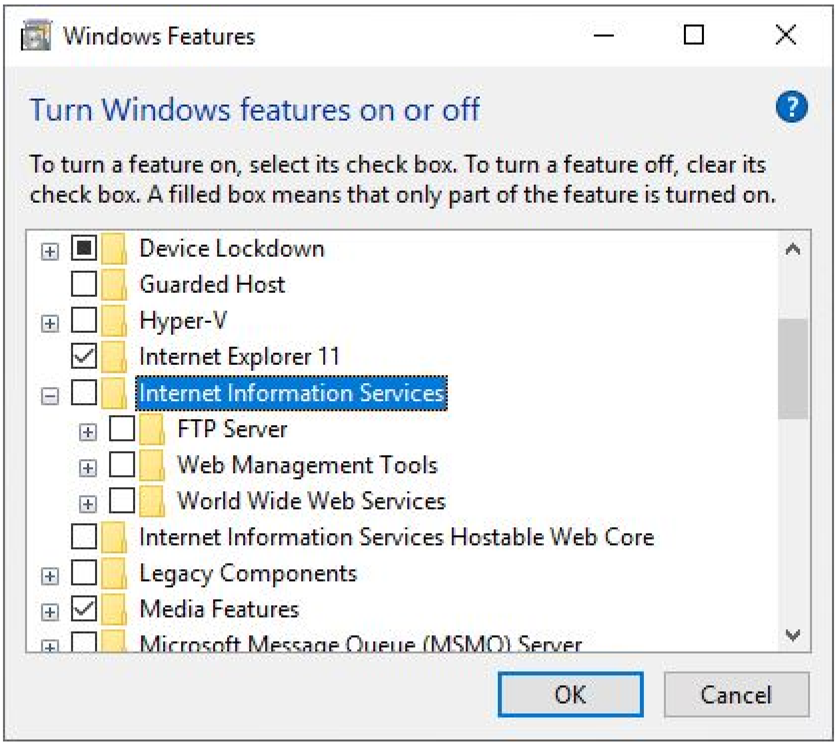
- disable the IIS web server
- or restrict access from outside.

The decision as to which of the two options is the right one for you depends on your conditions of use. Please note that in the case of complete deactivation all applications that access the IIS web server are affected and will no longer work. With restricted access, only the Beckhoff Device Manager is no longer accessible. The local access to the Beckhoff Device Manager can still be used and all other applications are unaffected by a deactivation.

Deactivating the IIS web server:

1. Call the execute dialog with the shortcut **[Windows key] + [R]** and enter **optionalfeatures**.
   The Windows Features window opens.

2. Disable the option under **Internet Information Service**.



Turn Windows features on or off

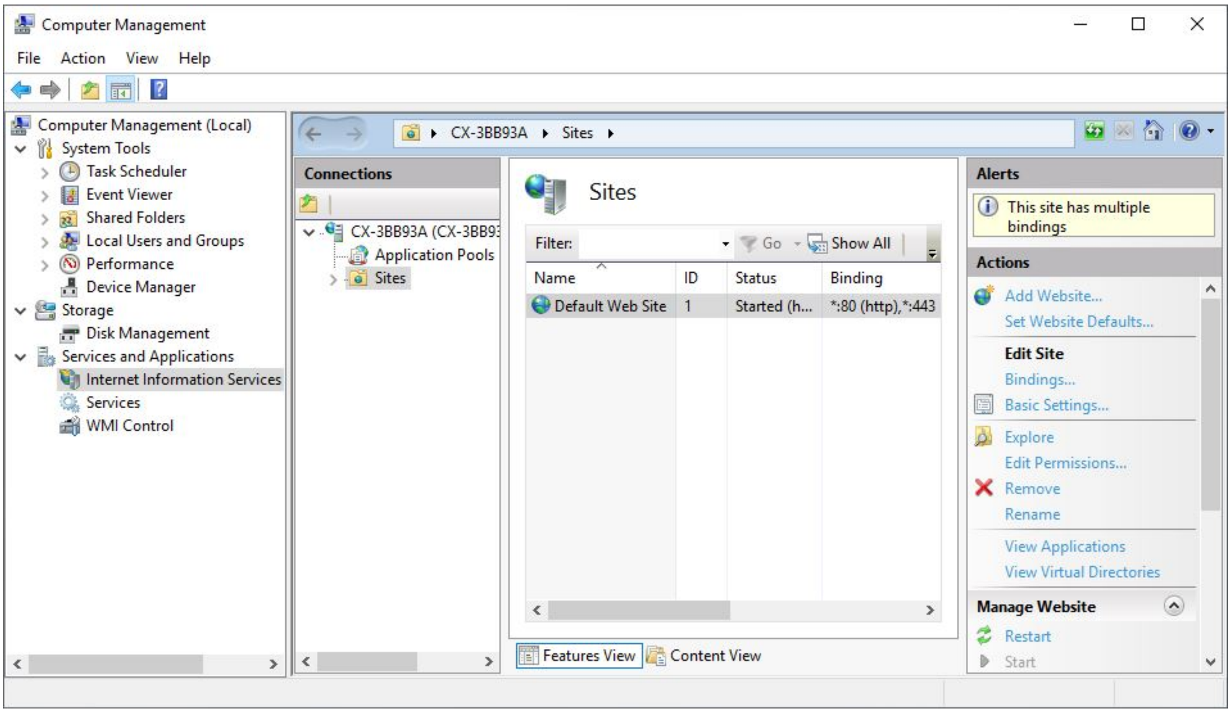
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ⊞ ■ Device Lockdown
- □ Guarded Host
- ⊞ □ Hyper-V
- ☑ Internet Explorer 11
- ⊟ □ Internet Information Services
  - ⊞ □ FTP Server
  - ⊞ □ Web Management Tools
  - ⊞ □ World Wide Web Services
- □ Internet Information Services Hostable Web Core
- ⊞ □ Legacy Components
- ⊞ ☑ Media Features
- ⊞ □ Microsoft Message Queue (MSMQ) Server

3. The IIS web server is thus disabled. All applications that access the IIS web server are affected by this change.

Restricting access from outside:

1. In order to disable access from outside, call the execute dialog with the shortcut **[Windows key] + [R]** and enter **compmgmt.msc**.
2. On the left in the structure tree, select the entry **Internet Information Services** and under **Connections** the folder **Sites**.

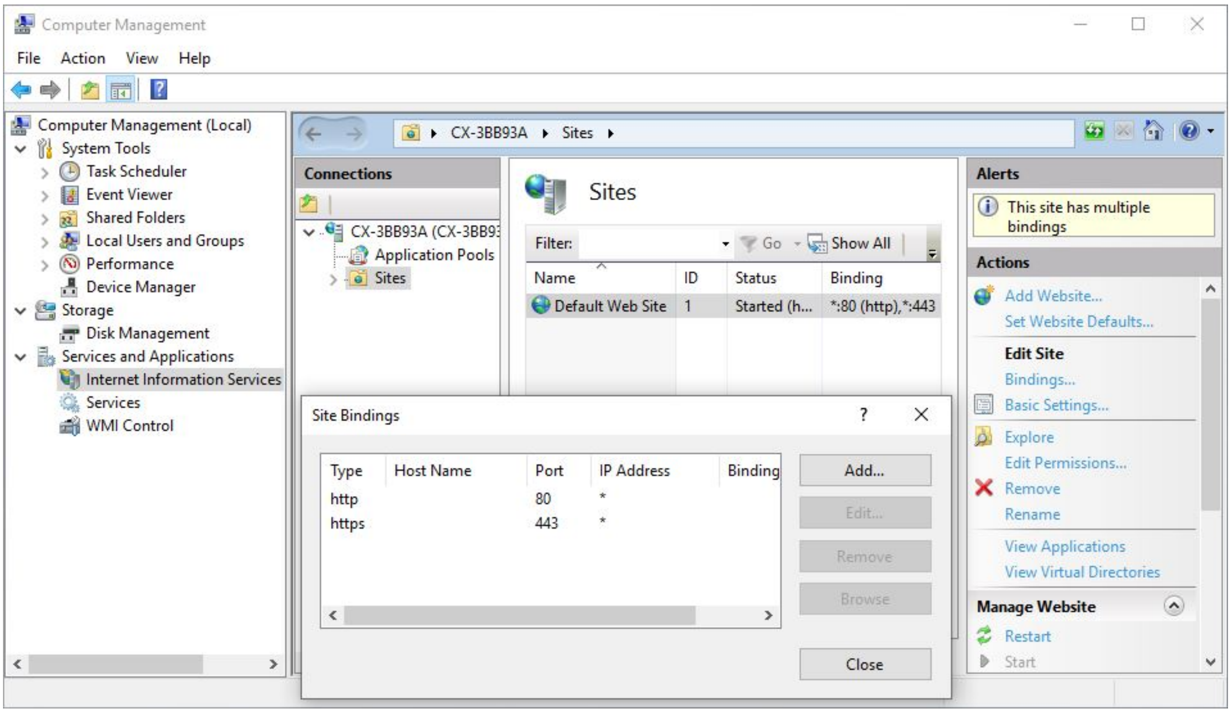


Sites

Name	ID	Status	Binding
Default Web Site	1	Started (h...	*:80 (http),*:443

This site has multiple bindings

3. On the right under Actions, click **Bindings**. In the window **Site Bindings**, an asterisk (*) is displayed in the column **IP Address** for http and https.



Sites

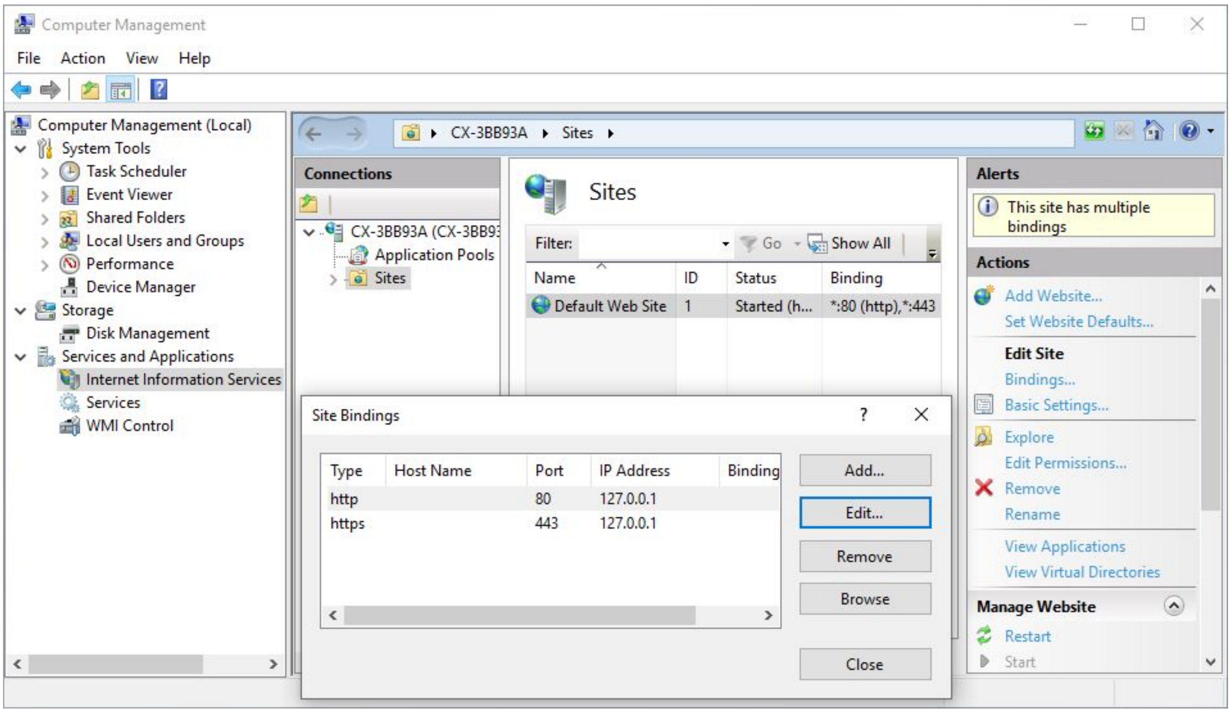
Name	ID	Status	Binding
Default Web Site	1	Started (h...	*:80 (http),*:443

Site Bindings

Type	Host Name	Port	IP Address	Binding
http		80	*	
https		443	*	

All accesses from outside are thus allowed.

4. Edit the entries for http or https and allow only local access with the entry **127.0.0.1**.



Sites

Name	ID	Status	Binding
Default Web Site	1	Started (h...	*:80 (http),*:443

Site Bindings

Type	Host Name	Port	IP Address	Binding
http		80	127.0.0.1	
https		443	127.0.0.1	

⇨ Access to the Beckhoff Device Manager from outside is restricted from now on. Local access is still possible with **127.0.0.1/config** and all other applications are unaffected by a complete deactivation.

7 TwinCAT

What is considered a threat for eXtended Automation Engineering (XAE) and eXtended Automation Runtime (XAR) must emerge from a security concept for the plant. The IEC 62433 standard, which explains, among other things, the necessary threat analysis, provides assistance in creating a security concept. In addition, the VDMA guide can be consulted to help with security in operating processes and the resilience of products against cyberattacks: https://www.vdma.org/viewer/-/v2article/render/16110956

This chapter lists some example threats related to XAE and XAR without claiming to be complete.

7.1 eXtended Automation Engineering (XAE)

Table 3: Unauthorized manipulation of the source code.

Countermeasures	Description
Technical	• Define authorizations and implement them with software protection • Use version control system to make changes traceable • Use individual access control for version control system
Organizational	• Use IT security management system (e.g. according to ISO 27001) • Use version control system (see: Source-Control): • Use "Staging": ◦ Check-in first in development source control repository ◦ Use separate (pre-)release build repository to build alpha, beta, RC and release versions from there ◦ Transfer development repository -> (pre-)release build repository only after review, for example via Project Compare Tool (see: Project Compare Tool)

Table 4: Unauthorized access to the source code.

Countermeasures	Description
Technical	• Store source code encrypted using software protection (see: Software protection)
Organizational	• Use IT security management system (e.g. according to ISO 27001). • Secure access to the storage locations. • Use encrypted storage.

7.2 eXtended Automation Runtime (XAR)

Table 5: Unauthorized access via ADS or Secure ADS.

Countermeasures	Description
Technical	Use Secure ADS (see: Secure ADS): • Open only for defined remote stations • Firewall restriction • Static routes • Secure remote stations against manipulation
Organizational	• Replace accesses via Secure ADS with accesses via OPC UA.

Table 6: Influencing the real time via ADS / Secure ADS.

Countermeasures	Description
Technical	Use Secure ADS (see: Secure ADS): • Open only for defined remote stations

Countermeasures	Description
	• Firewall restriction • Static routes • Secure remote stations against manipulation
Organizational	• Replace accesses via Secure ADS with accesses via OPC UA.

7.3 Further technical information

This chapter summarizes further topics in a link collection, which concern the security of TwinCAT. Links are provided to further Beckhoff documentation that describes the respective topics in detail. The selection is a guide. It is intended as the first place to look and does not claim to be complete.

TwinCAT general	Further information
TwinCAT 3 Software Protection	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_security_management/index.html&id=355557539833111233
ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_intro/index.html&id=7262890787652929099
Disable ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/6917981195.html&id=5745105416081707706
Secure ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/index.html&id=2501949194726739202
ADS over MQTT	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_over_mqtt/index.html&id=120186874503837909

OPC UA	Further information
Server-Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1448394251.html&id=2325029100913163478
IO Client-Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=
PLCLib Client Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=7305736008379229744
Gateway Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=954414165455750259

8 Appendix

8.1 Further reading

IEC 62443 is a series of international standards for security in automation systems. Some individual sections are still under development. The parts that have already been published describe the organizational and technical concepts and measures for systems and components. URL: https://webstore.iec.ch/publication/7029

NIST SP800-82 Guide to Industrial Control Systems Security specifically describes the analysis of and measures against security threats to industrial facilities. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

BSI IT Basic Protection Compendium offers structured function blocks for the analysis of risks and the application of measures. The compendium also contains function blocks relating to industrial IT URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

8.2 Advisories

Our Security Advisories are intended to help our customers protect their Beckhoff Industrial PCs and Embedded PCs against certain effects. The following table provides an overview of the available advisories and includes a link to download the document.

These Security Advisories are also provided as an RSS Feed. In addition, Beckhoff also publishes these advisories as part of the CERT@VDE together with other manufacturers: https://cert.vde.com/en/advisories/vendor/beckhoff/.

If you suspect security vulnerabilities in one of our products, please inform us via the procedure described in Coordinated Disclosure.

Number	Title	Version	Language	Download
2023-001	Open redirect in TwinCAT/BSD package “authelia-bhf”	1.0	EN	Link
2022-001	Null Pointer Dereference vulnerability in products with OPC UA technology	1.0	EN	Link
2021-003	Relative path traversal vulnerability through TwinCAT OPC UA Server	1.0	EN	Link
2021-002	Stack Overflow and XXE vulnerability in various OPC UA products	1.0	EN	Link
2021-001	DoS-Vulnerability for TwinCAT OPC UA Server and IPC Diagnostics UA Server	1.2	EN	Link
2020-003	Privilege Escalation through TwinCAT System Tray (TcSysUI.exe)	1.1	EN	Link
2020-002	EtherLeak in TwinCAT RT network driver	1.1	EN	Link
2020-01	BK9000 couplers - Denial of service inhibits function	1.0	EN	Link
2019-07	Denial-of-Service on TwinCAT using Profinet protocol	1.1	EN	Link
2019-06	CE Remote Display behaves incorrectly with wrong credentials	1.2	EN	Link
2019-05	Remote Code Execution in Remote Desktop Service ("Dejablue")	1.0	EN	Link
2019-04	ADS Discovery	1.1	EN	Link

Number	Title	Version	Language	Download
2019-03	Remote Code Execution in Remote Desktop Service	1.4	EN	Link
2019-02	Microarchitectural Data Sampling (MDS) vulnerabilities	1.2	EN	Link
2019-01	Spectre-V2 and impact on application performance as well as TwinCAT compatibility	1.4	EN	Link
2018-02	Updates for OPC-UA components (Several Vulnerabilities)	1.0	EN	Link
2018-01	TwinCAT 2 and 3.1 Kernel Driver Privilege Escalation	1.1	EN	Link
2017-02	Add Route using "Encrypted Password" bases on fixed key	1.3	EN	Link
2017-01	ADS is only designed for use in protected environments	1.4	EN	Link
2015-001	Potential misuse of IPC Diagnostics version < 1.8 backend	1.1	EN	Link
2014-003	Recommendation to change default passwords	1.1	EN	Link
2014-002	ADS communication port allows password bruteforce	1.1	EN	Link
2014-001	Potential misuse of several administrative services	1.1	EN	Link

8.3 Support and Service

Beckhoff and their partners around the world offer comprehensive support and service, making available fast and competent assistance with all questions related to Beckhoff products and system solutions.

Download finder

Our download finder contains all the files that we offer you for downloading. You will find application reports, technical documentation, technical drawings, configuration files and much more.

The downloads are available in various formats.

Beckhoff's branch offices and representatives

Please contact your Beckhoff branch office or representative for local support and service on Beckhoff products!

The addresses of Beckhoff's branch offices and representatives round the world can be found on our internet page: www.beckhoff.com

You will also find further documentation for Beckhoff components there.

Beckhoff Support

Support offers you comprehensive technical assistance, helping you not only with the application of individual Beckhoff products, but also with other, wide-ranging services:

- support
- design, programming and commissioning of complex automation systems
- and extensive training program for Beckhoff system components

Hotline:	+49 5246 963-157
e-mail:	support@beckhoff.com

Beckhoff Service

The Beckhoff Service Center supports you in all matters of after-sales service:

- on-site service
- repair service
- spare parts service
- hotline service

Hotline:	+49 5246 963-460
e-mail:	service@beckhoff.com

Beckhoff Headquarters

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

Phone:	+49 5246 963-0
e-mail:	info@beckhoff.com
web:	www.beckhoff.com

List of tables

List of figures

More Information:
www.beckhoff.com

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Germany
Phone: +49 5246 9630
info@beckhoff.com
www.beckhoff.com