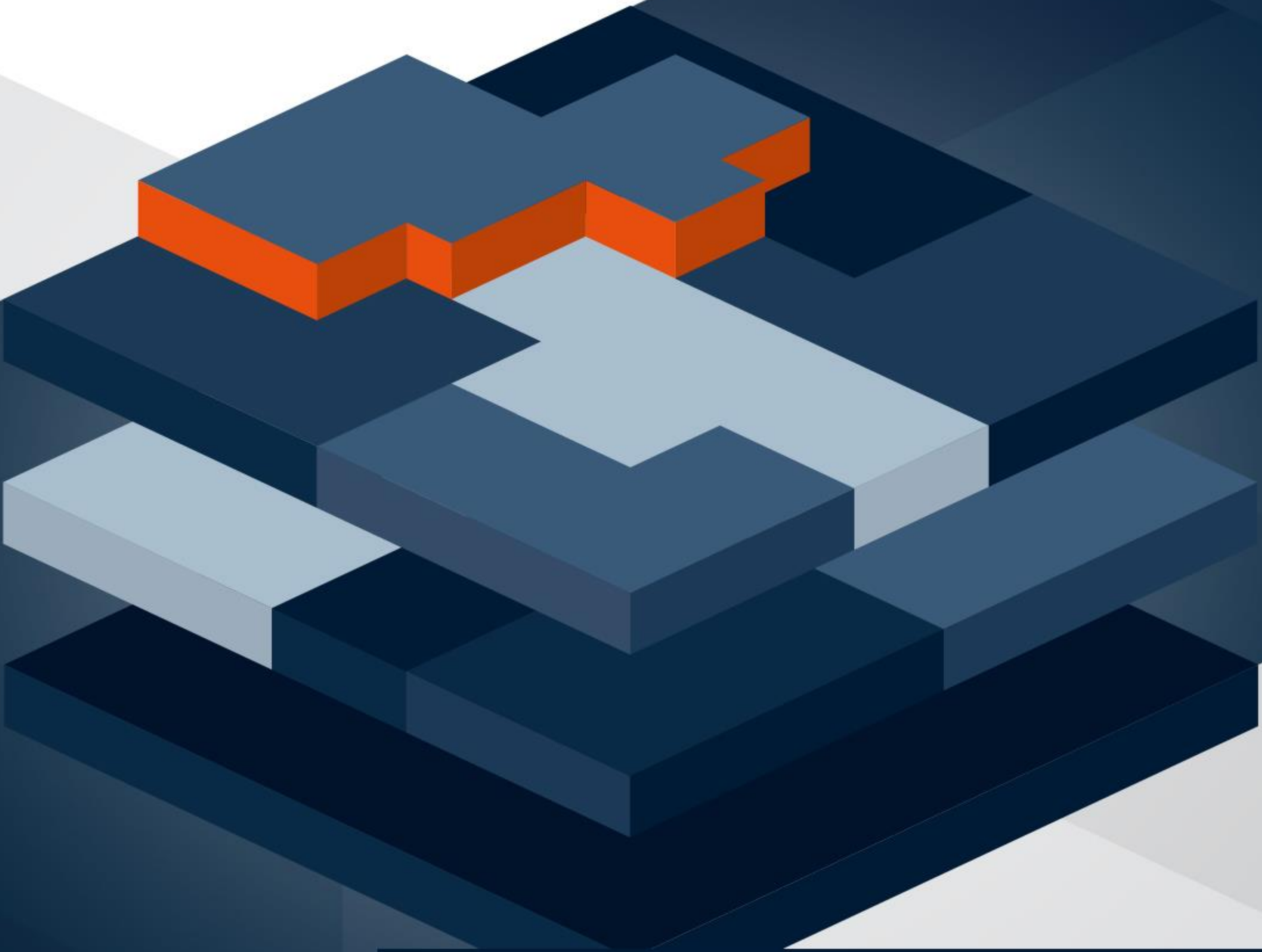


zenon manual

zenon Security Guide

v.8.20

Contents

1 Welcome to COPA-DATA help

ZENON VIDEO TUTORIALS

You can find practical examples for project configuration with zenon in our YouTube channel (https://www.copadata.com/tutorial_menu). The tutorials are grouped according to topics and give an initial insight into working with different zenon modules. All tutorials are available in English.

GENERAL HELP

If you cannot find any information you require in this help chapter or can think of anything that you would like added, please send an email to documentation@copadata.com.

PROJECT SUPPORT

You can receive support for any real project you may have from our customer service team, which you can contact via email at support@copadata.com.

LICENSES AND MODULES

If you find that you need other modules or licenses, our staff will be happy to help you. Email sales@copadata.com.

2 zenon Security Guide

Security is an important issue for COPA-DATA. zenon, zenon Logic and zenon Analyzer are therefore analyzed for security risks not just internally, but also together with universities, research institutes and security services providers. Weak spots that are identified are rectified immediately.

The security of a system is always only as strong as its weakest link. In accordance with the **Security in Depth** principle, measures are carried out at different levels to minimize security risks.

The points where security measures can be made are very diverse and depend on the respective situation. The idea, for example, that a firewall can be the only security measure to protect the production equipment, has now been superseded. Security measures can take many different forms. For example:

- Activation of security functions.
- Use of additional security products.
- Deactivation of functions that are not needed.
- Logging and monitoring of all communication.
- Isolation of areas, both network areas and physical areas.
- Switching off systems if other security measures cannot reduce risk with reasonable effort.

In order to continually improve security, we recommend:

- Regular validation and reevaluation of the possible risks and measures carried out
- Application of norms and standards
- Possible support from a security services provider
- Reevaluation of risks and measures each time a system is changed

Penetration Tests can be used to check whether the measures carried out offer sufficient protection.

This manual is primarily concerned with the system on which zenon Runtime is installed. It informs you of possible risks and strategies to rectify these. There are also recommendations for general security measures. You should however consider measures beyond these.

The protection of your automation environment includes, among other things, the following important areas:

1. IT-Systems general:
   - Protection of your operating system and all additional software such as SQL Server.
   - Creation and anchoring of general rules for each item of software, the network and users.
2. HMI/SCADA with zenon:
   - Protection of the Runtime and its communication in the network.
   - Protection of the Editor.

HOW CAN COPA-DATA SUPPORT YOU WHEN PROTECTING YOUR SYSTEMS?

IN PRINCIPLE, THE FOLLOWING APPLIES:

- COPA-DATA offers functions that make attacks on zenon server, clients and the communication in the network between zenon products more difficult.

- The communication between Runtime and control can only be protected if this is supported by protocol, drivers and PLC.
- zenon does not take over the task of taking care of the general IT security. This is the IT experts' task. If an attacker has overcome the IT hurdles and has access to the local data system, then an attack on zenon can also be carried out with appropriate expertise.
- If there is unauthorized file access with administrator rights, the zenon application can no longer guarantee the security and stability of the system.

THIS IS HOW COPA-DATA MAKES PROVISIONS

COPA-DATA:

- works together with university departments, universities of applied sciences and security experts
- has zenon reviewed also externally for security risks
- keeps a close watch on all attacks on automation software and security tests
- Analyzes known weak spots of other systems for their effect on zenon, zenon Logic and zenon Analyzer
- has been working together on the topic of security for years with other suppliers e.g. NERC

COPA-DATA provides information about how your products can be used securely. Neither COPA-DATA nor your products offer protection against negligent configuration.
Recommendation: Obtain advice from security experts if the necessary expertise is not or is only partially available in your company.

3 Protect the IT

The security of COPA-DATA products also depends on the security of the IT environment in which it is used. COPA-DATA recommends to restrictively protect operating systems, networks and physical access to systems and computers using the expertise of a security expert.

COPA-DATA can only advise you on the security-related configuration of COPA-DATA products. The following general recommendations for IT systems are based on experience and analyses of COPA-DATA, but do not replace an actual analysis and evaluation of your system by security experts.

⚠Attention

Security loopholes and threats can change very quickly.
Recommendation:

- Use the help of knowledgeable experts for the security of your equipment and systems.
- Note also the security standards and guidelines from Microsoft.

3.1 Putting a computer out of operation

Security must also be ensured with computers that are taken out of operation. Ensure that, in your company, there is a defined process that regulates how systems on which zenon are installed are taken out of operation. Ensure that this process is carried out and adhered to.

For taking systems on which zenon is installed, COPA-DATA recommends the following steps:

- Examine the existing data.
- Back up the data still required.
- Check to see whether the backups created can also be restored.
- Physically destroy the data media. This prevents saved information being able to be subsequently read.
- Make any data backups on other systems or data media unusable.

3.2 Operating system

The COPA-DATA products and their components can run on different systems and in different configurations:

From a Runtime with a zenon standalone project on a scrapped system with a Windows desktop operating system, to a system with Windows server operating system, zenon Runtime server and zenon web server with zenon web clients on systems that are in different networks. However COPA-DATA products can also be used on systems with operating systems other than Microsoft Windows, for example the Everywhere App or the HTML 5 client.

GENERAL NOTES

For a current overview of technical, organizational, personal and infrastructure notices on basic IT protection, we recommend the German **Bundesamtes für Sicherheit in der Informationstechnik** (**BSI**).

The DES **BSI** information is generally in German, but sometimes available in other languages too. Additional information:

- BSI general basic protection: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html)
- BSI international basic protection:https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/itgrundschutzinternational_node.html (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/itgrundschutzinternational_node.html)
- "**M 4 Hardware und Software**" catalog of measures: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04.html (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04.html)
  Focuses on practical measures for security.
- International technical specification from the **IEC/TS 62443** range, especially the parts from the **IEC/TR 62443-3** range.

MICROSOFT OPERATING SYSTEMS

Microsoft provides, on its website, comprehensive information and also tools for backup and secure operation of your operating system.

3.2.1 Secure installation and operation of the operating system

The operating system is, like zenon, a component of the automation system and contributes to the overall security of the system. The requirements for secure the installation and running of the operating system differ in complexity and depend on the type:

- Standalone client operating system
- Client operating system in a domain group
- Server operating system

GENERAL NOTES

The IT department may be able to support you with the secure installation and secure operation of computers with zenon, zenon Logic or zenon Analyzer. In doing so, please note the special features of the systems in the production environment: For example, an email server can be restarted in the night without problems in order to install security updates. For a system with zenon Runtime, this is generally only possible by agreement and during a maintenance interval.

Recommendation: Commission expert people with the planning, design, installation and operation of the operating system for the computers in your automation system. This can also include computers on which the zenon Editor is used.

> ### Information
>
> Many computers come with preinstalled operating systems. Reinstall the operating system from scratch before installing the zenon Runtime or Editor.
>
> **Background:** Many providers install many different tools and programs by default, which are not necessary for zenon and may increase security risks.
>
> **Recommendation:** Always only install the components and programs required for the operation.

ADDITIONAL NOTICES

This section provides additional notices for operating systems and their components in conjunction with zenon.

EQUIPMENT ADMINISTRATION

Ensure complete documentation of which:

- Systems are used in your equipment
- Operating systems are used on the systems
- Roles the systems fulfill
- Software products are installed, the exact version thereof

If it is necessary to replace a system, this information helps to get the system able to run again.
For example: In oder for a certain driver to run in one of your zenon projects, certain additional software must be installed. In addition, a Build of the zenon software is installed, which rectifies a problem in your project configuration. If this information or backups of these setups are missing, this makes putting it back into operation longer.

ANTI-VIRUS

Real-time protection from anti-virus software can slow processes if these processes access the data medium. Check the interaction of anti-virus software with zenon Runtime. If necessary, defined exceptions for real-time protection in the anti-virus software to enable zenon Runtime to have access to Runtime data.

Establish processes in the company that define what exactly is to happen if anti-virus software discovers malware.
Note: With a false-positive report, cleaning of the system can, under certain circumstances, disable

the computer or impair functionality. If an executable file of zenon software is detected as possibly infected, check the validity of the digital signature first. In the event of doubt, contact your local COPA-DATA support.

If malware is in fact discovered, it is not sufficient to delete the infected file or prevent access to the file. There must also be an investigation to find out how the malware got into the system, how far it has spread and what damage it may already have caused.

USER ROLES

For the operation of zenon Runtime, the limited rights of a user from the Windows **User** user group are sufficient. Ensure that the user who is executing Runtime only belongs to this user group.

OPERATING SYSTEM UPDATES

In principle, it is recommended that the operating system is always kept current and that the security updates at least are installed. Check updates on your own system before installation for possible interaction with zenon, zenon Logic or zenon Analyzer .

Check in time to see what it means for the systems in your company if an operating system is discontinued and consequently no more security updates are provided by the manufacturer. Plan updates for systems carefully and check the systems in a test environment. The current version of zenon always supports the operating systems available at the time of release and allows the conversion of older zenon projects to the respective current version. Isolate systems that cannot be updated and undertake measures to increase the security of such systems.

DIGITAL SIGNATURE

All executable files of zenon software are digitally signed. With this signature, it is possible to check whether the software still corresponds to the original. The digital signature can also be used, under certain circumstances, by Application Whitelisting software, in order to prevent the execution of third-party software or manipulated software.

INTERNET CONNECTION

An Internet connection is not required for operation of zenon software.
Recommendation: Never connect systems in productive use to the Internet directly. If a connection is absolutely necessary, use a DMZ at least.

Define mechanisms and processes that also allows installations without an Internet connection for:

- Security updates for the operating system
- Updates of signatures of anti-virus software
- Updates of zenon software

BACKING UP DATA AND FILES

Create backups of not just Runtime data, but also compiled Runtime files. This is applicable most of all if you do not have project backups or workspace backups. Also consider whether you want to back up log data from the zenon diagnosis server and Windows events, in order to subsequently establish what happened in the event of a problem. Take good care of these backups, protect the backups from unauthorized access and ensure that they can also be restored again.

BACKUP OF INSTALLATION MEDIA

Create backups of installation media and also back up possible Patches/Builds for the COPA-DATA software that you have installed. Installation sets for required third-party software should also be backed up. In the event of an emergency, a system can also be set up from scratch without an Internet connection using this.

SYSTEM BACKUP

Create a backup of the system each time a change is made. Take good care of the backups and note who has access to the backups. Also check whether the backup can actually be restored. A system backup is only for restarting the system in the event of an emergency. It can also serve to carry out a forensic comparison with the current system or tests in a test environment.

ADDITIONAL SOFTWARE

Restrict, on the systems on which zenon software is used, the use of further software to what is absolutely necessary and check for interaction between zenon and other products. If you use further software, ensure that there are processes that ensure that you are informed about possible security vulnerabilities in this software and that ensure that corresponding measures have been implemented, such as an update or uninstalling the software.

MANUAL INSTALLATION OF REMOVABLE MEDIA

Windows makes it possible to shut off automatic access to removable media. Each new piece of removable media must be permitted on a one-off basis by an administrator, in order for this to be able to be used. If removable media actually needs to be used, this mechanism reduces the risk of unwanted removable media being used in the system.

3.2.2 User Administration

COPA-DATA recommends that users and passwords are configured as freely as necessary and as limited as possible. You can read how you administer users in zenon in the **user administration** manual in the **zenon login and user administration in the Runtime** chapter.

USERS

For the operation of zenon in general 4 Windows users are required:

Role	Example	Rights
System Administrator	zenon_ADMIN	Administrator
System Services	zenon_SERVICE	Standard user
System Engineer	zenon_ENGINEER	Standard user
User (for Desktop Login or Autostart)	zenon_USER	Standard user

These users are also used to configure the SQL Server. You can read about the roles and authorizations that are required in the **Roles and authorizations for databases** (on page 21)chapter**.**

PASSWORDS

Passwords should require an appropriate length and strength. This includes the use of capital letters, small letters, characters and special characters.

Recommendation:

- Already create a password for the local administrator during the installation.
- Enforce a password for every account, including guest accounts.
- Force administrators to use particularly strong passwords.
- Force user to use particularly strong passwords.
- Inform users on how to memorize strong passwords without writing them down.

> ⚠**Attention**
>
> Note:
>
> - It is best to just use signs which can be entered with any keyboard, so for instance no German umlauts.
> - Passwords for Autologon accounts may not expire automatically.

3.2.3 Windows security settings

Windows offers a number of security settings. With regard to this, please also read the Microsoft documentation.

Recommendations:

- Deactivate Autorun for all drives.
- Prevent the automatic execution of updates for the operating system and applications.
  Only install updates after you have examined them for smooth operation with their applications in a test environment.
  Some Service Packs/Updates can reactivate the **automatic update** property without notifying the user.
- Deactivate all non-essential services.
- Set a strong password for every account.
- Also create passwords for deactivated guest accounts.
- Disable automatic login.
- Prevent network access to the accounts of local administrators and guest accounts.
- Protect shared printers.
  Only enable the printer for a precisely-defined group of users.

Information

Group policy

Many security-related settings can be adjusted via group policy. It also depends on the operating system which settings are selected in which place. Please find details on this in the corresponding Microsoft documentation.

You can also find information online. For example:

- Group policy for beginners:
  http://www.microsoft.com/download/en/details.aspx?id=20092
  (http://www.microsoft.com/download/en/details.aspx?id=20092)
- Microsoft Technet Security and Updates:
  http://technet.microsoft.com/en-us/library/cc498723.aspx
  (http://technet.microsoft.com/en-us/library/cc498723.aspx)
- Mircosoft Technet Solution Accelerators:
  http://technet.microsoft.com/en-us/library/cc936627.aspx
  (http://technet.microsoft.com/en-us/library/cc936627.aspx)
- Microsoft Compliance Manager:
  http://technet.microsoft.com/en-us/library/cc677002.aspx
  (http://technet.microsoft.com/en-us/library/cc677002.aspx)

3.2.4 Specific Windows settings

Increase the system security by adhering to some specific settings for Windows. With this regard please also read the Microsoft documentation.

Recommendations for increased Windows system security:

- Always use the classic logon screen.
  Entering the user name and password is required and it is not displayed which accounts are available.
- Deactivate the following functionalities:
  - Remote support and remote control.
  - Automatic updates of the root certificates.
  - Automatic Updates during an installation.
  - Help and Support Center.
  - Service for target server.
    Only activate this service if a computer must actually act as a time server.

3.3 Installation zenon

Before the installation of zenon, ensure that the installation medium corresponds to the original of COPA-DATA. Create secure checksums of downloads and contact COPA-DATA to compare the checksums.

Note: Even if you have obtained a file from s source that you think is secure, there is the possibility the the file has been manipulated during transport.

The following assumptions are made during installation:

- The system on which the product is installed is free of malware such as viruses, Trojan horses, etc.
- There are no software products on it that are not required for operation.
- The system is in a protected environment without direct access to the Internet.

Note:

If you do not install the software in the standard folder, ensure that only users with administrator rights can amend files in, or add files to the selected folder. This is ensured by Windows in the standard folders **%Program Files%** and **%Program Files (x86)%**.

3.3.1 Firewall exceptions

Some exceptions in the Windows firewall are configured during installation. Depending on the area of use, the applications used and the functionality, these exceptions are not necessary under certain circumstances.

The table lists the exceptions and information on their necessity.

Program or service	Executable file	Comment
CodeMeter Runtime Server	**C:\Program Files (x86)\CodeMeter\Runtime\bin\CodeMeter.exe**	Necessary.
CodeMeterFWEx1	**C:\Program Files (x86)\CodeMeter\Runtime\bin\CodeMeter.exe**	Necessary.
zenon Logic Runtime	**STRATONRT.exe**	Required if the remote computer communicates with zenon Logic Runtime on this computer
zenAdminSrv - Administration service	**zenAdminSrv.exe**	Not necessary.
zenDBSrv - Database service for SQL Server communication	**zenDBSrv.exe 32 bit**	Necessary if **distributed engineering** is used.
zenDBSrv - Database service for SQL Server communication	**zenDBSrv.exe 64 bit**	Necessary if **distributed engineering** is used.
zenLogSrv - Diagnosis server	**zenLogSrv.exe**	Necessary if: ▸ This computer is defined as a remote logging server or ▸ If access to this computer is required by a remote computer with the Diagnosis Viewer
zenNetSrv - Network communication service	**zenNetSrv.exe 32 bit**	Necessary if Runtime is running on this computer

Program or service	Executable file	Comment
		as a **Server 1** or **Server 2**.
zenNetSrv - Network communication service	**zenNetSrv.exe 64 bit**	Necessary if Runtime is running on this computer as a **Server 1** or **Server 2**.
zenon Process Gateway	**zenProcGateway.exe**	Necessary if the zenon **Process Gateway** is used on this computer.
ZenSysSrv - Transport service	**zenSysSrv.exe 32 bit**	Necessary if remote transport to this computer is required.
ZenSysSrv - Transport service	**zenSysSrv.exe 64 bit**	Necessary if remote transport to this computer is required.

Note: See also the **Ports for zenon and zenon Analyzer** (on page 17) chapter.

3.3.2 Ports for zenon and zenon Analyzer

During the installation of zenon, exceptions are created in the Windows firewall by the Setup for some applications and services that open a TCP Listening Port.

Information

After installation, configure the exceptions in the Windows firewall more restrictively, appropriate to their environment and to the necessary applications and services.

On multi-homed systems with multiple network cards, zenon applications and services, with their default settings, open the TCP Listening Port for all network cards present in the system. However communication throughout all network cards is often not necessary and not desirable.

Note: After installation, use the **Startup Tool** to configure the TCP Listening Ports for the respective services and applications, according to their environment and requirements. Only allow communication between the network card or IP address that is required for this. If you assign a service the **local loopback** adapter or the IP address *127.0.0.1*, you only allow local communication. This way, local diagnosis server access to local diagnosis clients can be limited.

Information

If a port that is different to the standard port is configured for a connection, this does not mean that an unwanted connection is no longer possible. A attacker only needs some more time to find the correct port.

When using non-standard ports, the standard port can be used as a **Canary** under certain circumstances. To do this, you monitor the standard ports in an **Intrusion Detection System** that you may have and set alarms for any attempt to connect to these ports. Such connection attempts can be caused by:

- An incorrectly-configured computer
- By an attacker who is using the default ports

PORTS

Application	File	Exercise	TCP port	UDP port
Network project	**zenNetSrv.exe**	Runtime communication.	*1100*	
Remote Transport	**zenSysSrv.exe**	Data transfer via Remote Transport (editor) and Diagnosis Server.	*1101*	
zenon Web Server	**zenWebsrv.exe**	On-site logging machine between **Web Client** and Runtime	*1102*	
Distributed Engineering	**zenDBSrv.exe**	Distributed Engineering	*1103*	
CodeMeter WebAdmin		Configuration of **CodeMeter** Dongles.	*22350*	
WibuyKey		Monitoring **WibuKey** Dongles.	*22347*	
SQL server with multi-user projects		Administration of objects being executed.	*1433*	*1434*

Recommendation: Open only ports required for a smooth operation.
Ports can be amended in the **Startup Tool** in the **Listening ports** tab. In this case, all devices involved must be amended accordingly.

STANDARD PORTS IN COPA-DATA PRODUCTS

The following ports are used by COPA-DATA products by default:

ZENON

Application	Standard port
Network Service	*1100*
Transport Service	*1101*
WEB Service Classic	*1102*
DB Service	*1103*
SQL Browser Service, (for distributed engineering in the Editor)	*1434*
zenAdminSrv.exe	*50777*
zenLicTransfer (License Transfer Service)	*50784*
Logging Service	*50780*
SNMP Trap Service	*50782*
WEB Service Tunneling	*8080*

ZENON LOGIC

Application	Standard port
Assigned port for zenon Logic or straton depends on the project and service. E.g.: First zenon Logic project used *1200* and *9000*, second project *1201* and *9001* etc.	*1200 - 1210* *4500 - 4510* *7000 - 7010* *9000 - 9010*

ZENON ANALYZER

Application	Standard port
Administration Service	*50777*
Analyzer Connector Service	*50778*
Analyzer License Service	*50779*

Application	Standard port
ZAMS	*50781*

DRIVERS

Application	Standard port
Driver Simulation	*6000 - 6020*
Process Gateway OPC Server	*135*
Process Gateway SNMP	*161*
Process Gateway Modbus	*502*
Process Gateway IEC60870-5 104 slave	*2402*
Process Gateway DEC	*5555*
Process Gateway DNP3 Slave	*20000*

SERVICE GRID

Application	Standard port
Service Grid API	*9400*
Hub Controller	*9410*
Data Hub	*9411*
Hub Controller: Dedicated port for connection to **Data Hub**	*9412*
Configuration Backend	*9420*
Identity Service	*9430*
Policy Service	*9440*

Note: zenon drivers that communicate by means of Ethernet use TCP and thus need authorizations in the firewall in this case, regardless of the port used.

3.4 Microsoft SQL server

The Microsoft SQL Server is only required for the zenon Editor and for the zenon Analyzer. It is also installed during the installation of the zenon Editor or zenon Analyzer. The respectively required MS SQL Server is also contained on the installation medium. In the installation of the zenon Runtime no SQL server is installed.

The version of MS SQL Server that is installed is the one that is current at the time the installation medium is created. COPA-DATA recommends to install patches and updates after the installation.

In doing so, please note:

- Load and install updates and patches individually instead of on an automated basis.
- Check all updates and patches for unwanted effects on a test system before installation.
- Only implement updates and patches on a productive system after they have been successfully tested.

> **⚠Attention**
>
> For the maintenance and backup of the SQL Server, use the corresponding documentation and guidelines from Microsoft.

3.4.1 Roles and authorizations for databases

zenon uses MS SQL Server for certain tasks:

- Editor
- SQL export in the Runtime
- Databases for IMM and IPA
- Process Gateway SQL

Standard users from zenon are used for this. You can find details in relation to this in the **User Administration** (on page 12) chapter. They may need roles and authorizations on the SQL Server.

ROLES AND AUTHORIZATIONS ON THE SQL SERVER

Certain actions require the following roles and minimal authorizations on the SQL Server.

GENERAL

Module	Action	Role	Additional permission
Startup Tool	**Database** configure.		

EDITOR

Module	Action	Role	Additional permission
General	Use Editor.	*DB_DataReader* *DB_DataWriter*	--
Historian	Evacuate to SQL. There is not yet a corresponding table.	*DB_DataReader* *DB_DataWriter*	*CREATE TABLE*
IPA	Create database.	*DB_DataReader* *DB_DataWriter*	*CREATE TABLE*
Metering point administration	Create database.	*DB_DataReader* *DB_DataWriter*	*CREATE TABLE*
MS Azure	Configuration.		
Project Backup	Backup / restore project.		
Distributed engineering	Distributed engineering.		
WinCC Wizard	WinCC database connection.		

RUNTIME

Module	Action	Role	Additional permission
AML	Export.	*DB_DataReader* *DB_DataWriter*	--
AML	Export. There is not yet a corresponding table.	*DB_DataReader* *DB_DataWriter*	*CREATE TABLE*
AML	Incremental export.	*DB_DataReader* *DB_DataWriter*	--
AML	Incremental export. There is not yet a corresponding table.	*DB_DataReader* *DB_DataWriter*	*CREATE TABLE*

Module	Action	Role	Additional permission
Historian	Evacuate to SQL. Table exists.	*DB_DataReader* *DB_DataWriter*	--
CEL	Export.	*DB_DataReader* *DB_DataWriter*	--
CEL	Export. There is not yet a corresponding table.	*DB_DataReader* *DB_DataWriter*	*CREATE TABLE*
CEL	Incremental export.	*DB_DataReader* *DB_DataWriter*	--
CEL	Incremental export. There is not yet a corresponding table.	*DB_DataReader* *DB_DataWriter*	*CREATE TABLE*
Connector	SQL connector.		
Extended Trend	Evacuated archives.		
Process Gateway	AccessSQL.		
Report Generator	SQL.		
Shift Management	SQL Export.		
Driver	ExportSQL32 driver.		
Driver	SQL driver.		
WPF	DataGrid.		

ZENON ANALYZER

Module	Action	Role	Additional permission
Connector	SQL connector.		
Linked Server	Linked Azure Server; SQL instance.		

3.5 Hardware

Also protect the hardware from attacks. For this purpose, also adhere to the documentation of the corresponding devices.

Recommendations for the hardware protection:

- Protect access to the **BIOS** with a password.
  The **BIOS** contains some areas relevant for security. Only the administrator should be authorized to change these settings.
- Protect the start process with a password, if there is no good reason not to do this.
  Reasons not to set a boot password:
  - A server should automatically boot after a system error.
    In this case, physically protect the server by means of a locked cabinet.
  - Dual boot is not possible. Only the pre-set operating system can be booted.
  - Complete encryption of the hard drive, which demands the entry of a password before booting.
  - Several users share the computer.
- Avoid wireless communication.
  It is possible to intercept the communication of wireless keyboards (radio waves, infrared, Bluetooth) to and from the system, even from a great distance.
- Avoid biometric access controls; instead, use PKI-based smart cards.
  It is now known that biometric access checks for computers can be circumvented in several ways. They should not be used in productive systems.
  Recommendation: Use PKI-based smartcards. These can also be linked to biometric checks. For example, a fingerprint reader on the smartcard reader can allow the access to the smartcard. zenon supports login by means of chip identification system in the Runtime.
- Deactivate wake-on LAN if it is not needed for administrative purposes.
- Deactivate Hardware virtualization.
- Deactivate interfaces for removable media (USB).
  Note: You can also get COPA-DATA dongles for internal USB ports for licensing.
- Protect physical access to your systems. The room with server cabinets should be locked and access should be monitored. Replace the standard locks that come with server cabinets with security locks. Cabinets for equipment computers and controllers should be locked. Cable connections should also be protected.
- For unmanned areas, use camera systems with motion detection and alarming.

- Consider which components you store, so that critical components can be replaced, even when there are supplier bottlenecks.
- Ensure that you are informed if a product is discontinued or can no longer be supplied by the manufacturer and create a replacement strategy.

4 Protect zenon

zenon ensures up-to-date protection with:

- Separation of Editor and Runtime:
  The Editor and Runtime are administered separately in zenon. An infection of the Editor database by an attacker does not automatically lead to an infection of Runtime.
- Encryption (from version 7.00):
  Optional strong encryption of communication in the zenon network and in the communication between Editor and Runtime.
- Encrypted passwords:
  The password for the Editor database can be stored in an encrypted form.
- SQL server:
  The MS SQL server is only required on computers with the zenon Editor for configuration or for the zenon Analyzer server. The zenon Runtime does not require an SQL server. Only install the MS SQL server if you need it for operation of zenon and configure it restrictively.
- File signature (from Version 7.00 on):
  checking the Runtime file signature.
- Authentication (from Version 7.00 on):
  Only authenticated clients will have access to a zenon server.
- Limited rights:
  The zenon software is able to run in the user context of a standard user.
- Start as a service without GUI:
  zenon Runtime can be configured so that it starts as a service with the operating system without a user interface. This option can be used for systems on which Runtime runs as as server.
- Clients or zenon web clients on the terminal server:
  <CD_PROCUCTNAME> Runtime as a client and the zenon web client can run one one terminal server. A thin client can thus be used for an operating station. The administration and protection of thin clients and terminal servers can be central.
- General functionalities such as:
  - Configurable ports
  - Components that can be deactivated, such as COM Interface and Everywhere Server

- Current communication standards with security aspects, such as OPC UA

4.1 Supported Operating systems for zenon.

Which operating systems are supported depends on the applied zenon version. zenon is continuously being developed also with regard to security. It is recommended to use the latest zenon version on a current operating system with the latest patches.

> ### Information
>
> Many computers come with preinstalled operating systems. Reinstall the operating system from scratch before installing the zenon Runtime or Editor.
>
> **Background:** Many providers install many different tools and programs by default, which are not necessary for zenon and may increase security risks.
>
> **Recommendation:** Always only install the components and programs required for the operation.

The following information refers to the zenon version.

4.2 Runtime

zenon Runtime is protected in operation with the zenon user administration (including connection to Active Directory) by:

- authentication of the client at the server (from version 7 on)
- Strong encryption (on page 31) (from version 7 on)
- Data storage in binary format
- no SQL database used
  (only required for the zenon Editor)

You can further increase the protection by:

- limiting the access to the zenon Runtime folder (on page 26)
- disabling the zenon API (on page 38)

4.2.1 Protect zenon file system

The access to the zenon file system should be strongly protected so that data cannot be manipulated externally. Only one Windows user should have read and write access. All other users should not have rights in the zenon Runtime folder. Operators in the Runtime log in as zenon users.

In order to limit access to the file system:

1. Only create a single Windows user (for instance: **zenon_ADMIN)** who is authorized to start zenon as well as to read and write in the zenon Runtime folder.
2. Disable access to the zenon Runtime folder for all other Windows users – including read authorizations!
3. Disable any remote access to the user **zenon_ADMIN**.
4. Block any software for remote maintenance or remote access.
5. Make sure that zenon can only be started if this user (**zenon_ADMIN)** is logged in.
   Since other Windows users do not have read authorization Runtime will only start in the context of this user (**zenon_ADMIN)**.
6. Make sure that zenon runs as shell:
   a) For this purpose, create a zenon autostart with **Keyblock Runtime Start**
   b) Activate the property **Lock system keys** in the group **Runtime settings** of project properties.
   c) Start zenon in full-screen mode: Set property **Runtime title** to *No title*.
   d) Ensure that you also take multi-monitor systems into account during configuration.
   e) Disable Explorer start
   f) Do not offer file selection dialogs.
   Note: In this case, no functions that require the user to select files in the Runtime can be configured.

Access to the zenon file system is thus restricted.

The zenon tool **Keyblock Runtime Start** can be used to implement further protective measures by blocking the system keys.

4.2.1.1 Blocking system keys

Keyblock Runtime Start is a program with which zenon Runtime runs as a **Shell**. In doing so, zenon Runtime is started, but all **Windows** system tasks are blocked. Keyboard shortcuts such as **Windows** key or **Ctrl+Alt+Del** no longer have an effect. User can no longer access the operating system but only work on the zenon user interface.

The precondition for this is that the project properties are set **Runtime title** to *No title (full screen)*. Then zenon runs in full screen mode and the Runtime cannot be minimized.

Note: The blocking of the **Windows-** key can be circumvented. You should therefore block the **Windows** key using the corresponding entry in the **Startup Tool**

USE

To use **Keyblock Runtime Start**:

1. In the Windows start folder, under COPA-DATA, open the zenon **Tools**.
2. Select **Keyblock Runtime Start**.
3. The program is opened and automatically starts Runtime.
4. The program blocks all access to the operating system:

- locked shortcuts:

  Ctrl+Alt+Del

  Ctrl+Esc

  Alt+Tab

  Alt+Esc

  Alt+F4

  Windows key (except **Windows + L**)

  Notes:

  When locking the system keys, the normal operation of the scroll bars with the mouse in the Runtime is also blocked. This block can be circumvented with the context menu.
  If the system is blocked using the keyboard shortcut **Windows + L**, All **Windows** keyboard shortcuts are available again when signing in again. To prevent this, in the **Startup Tool** under **Application -> Options -> General**, deactivate the **Windows** key.

- Hiding the Control Panel in the start menu
- Locking the toolbar for operation
- Prevents

  Changing passwords

  Closing Windows

  Logout

  Locking the computer

  User change

- Hiding all element in the task manager

Information

If **Keyblock Runtime Start** is started using the startup process of the operating system, then note the following:

- The Autostart folder is user specific:
  If another user logs in, the program is not executed.
- Execution of the Autostart programs can be prevented by pressing the **Shift** key when the operating system is booting.

This locking cannot be bypassed during Runtime. When the Runtime is closed normally, the system restrictions are canceled. If the Runtime is to be operable without these limitations, Runtime must be started without the **Keyblock Runtime Start**.

Attention

Take care that you engineer a possibility to close the Runtime in your project. There is no possibility to end the Runtime regularly.

- It can only be ended by shutting the computer down using the hardware
- All system keys also remain blocked after restarting

In order to make system keys accessible again after not being shut down properly (in the event of a power cut for example):

- start the Runtime again with the help of **Keyblock Runtime Start**
- end the Runtime regularly via a close button

4.2.2 User Administration

zenon supports a user administration for the Editor and for the online operation (Runtime). The password system meets the guidelines of the FDA (Food and Drug Administration, 21 CFR Part 11).

You can read about the roles and authorizations that are required for the SQL Server in the **Roles and authorizations for databases** (on page 21) chapter.

THE CONCEPT

The password design assumes that different users have different operating rights (password levels). Administrators also have different authorization levels. However they also have additional administration-related functions, such as administering users.

The zenon password design allows to allocate several selective (separately defined) authorization levels (operating rights) to each user. A maximum of 128 (0 to -127) authorization levels can be configured. Users can be assigned to the individual authorization levels and the attendant project-specific password design in relation to this can be created completely freely. Each user can have any level allocated. Thus e.g. user 1 can have levels 0, 1, 5 and 6 assigned and user 2 can have levels 0, 1, 6, 8 and 10 assigned. Authorizations can only be issued if the administrator has those rights himself.

A user is logged in to Runtime during online operation by activating the Login function. If the user should be logged in automatically based on an event (e.g. position of a key known to the system), the function Login without password is used. This function is projected with a limit value or a Rema of the variable in the variable management, respectively.

The Logout function is used for the independent logging out of a user. The user who is the automatically newly logged into the system is the **SYSTEM** user. If during a defined period of time there is no operation, an automatic time-triggered logout can be engineered.

For the creation and administration of users, as well as the assignment of passwords, please also note the information in the Protecting the zenon file system (on page 26) chapter:

4.2.2.1 Options in Runtime

User administration in the Runtime offers different possibilities.

Windows AD or AD LDS can also be used for user administration. Users can be logged in permanently or temporarily and administered in the Runtime.

Note: It is not possible to rename user groups in the Runtime.

> ⚠**Attention**
>
> In order for the settings for users that have been changed in the Editor to be applied in the Runtime, the **Runtime changeable data** project property (**General** group) must allow overwriting of user properties when writing Runtime files.
>
> Settings changed in Runtime can be applied using the **Import Runtime files** command (Runtime files toolbar) in the Editor. To do this, decompiling must be permitted in the **Runtime changeable data** property. This is the case if the checkbox for *User Administration* has been deactivated in the *Do not decompile* column.

SIGNATURE NECESSARY

User actions can also be protected by means of a signature. This applies, for example, to dynamic elements, functions, actions via a menu or changes in variables of the recipe group manager.

To additionally protect user actions with a signature:

1. Configure the **Signature necessary** property for the respective element in the Editor.
2. Select from the drop-down list:
    - *Signature with password*: A signature and a password are required for operation of the element.
      For security reasons, a password is requested here again even for a user who is already logged in. The signature text is logged in the Chronological Event List (CEL) after it has been used successfully.
      Caution: Only users who are logged in can sign an action. Signing actions with temporary login is no longer possible.
    - *Signature without password*: A signature is necessary to operate the element. This can be entered without entering a password. The signature text is logged in the Chronological Event List (CEL) after the successful use of the element.
3. In the **Signature text** property, enter the signature text for the CEL.

IN THE RUNTIME, THE USER WILL BE REQUESTED TO SIGN THE USER ACTION. DEPENDING ON THE CONFIGURATION, THE USER MUST ALSO CONFIRM THIS WITH HIS OR HER PASSWORD. IN ADDITION, AN ENTRY IS CREATED IN THE CHRONOLOGICAL EVENT LIST.PERMANENT AND TEMPORARY LOGIN

After a permanent login, the user is permanently logged in and can carry out all operations that they are authorized to do. For actions that the user is not authorized to carry out, a message is shown accordingly.

Permanent login can be effected by means of:

- A screen switch to a *login* screen
- The function **Login with dialog**
- The **Login without password** function

Hint: Password-protected buttons can be made invisible for logged-in users. To do this, the **Locked buttons** property (**Project properties** -> **User Administration** -> **Login and signature**) must be configured accordingly.

- **Note:** Temporary login is not possible for logged-in users. Logged-in users therefore do not receive a dialog to log in temporarily for functions for which they do not have sufficient authorization.

4.2.3 Encryption in the network

Data traffic in the zenon network is encrypted.

zenon enables strong encryption of communication in the zenon network. Strong encryption works from zenon Version 7.0 for all supported operating systems and for the zenon Web Client.

If encryption is active, communication between the Primary Server, Standby Server, Clients and zenon Web Clients is in encrypted form; the zenon Web Server only forwards data packets and is not affected by encryption.

Information

Network communication was also encrypted in earlier versions of zenon. The method has changed with version 7. The term "encryption" in conjunction with zenon 7 or later always means strong encryption.

Note: No encryption is available for *VoIP* in the **Message Control** module. This type of dispatch should therefore not be used if there is a need for security.

4.2.3.1 Basics

Encryption for zenon Runtime is available from version 7.00. It is not possible to communicate with earlier versions of zenon if encryption is switched on. Encryption does not impair any zenon functionality.

BASIC ENCRYPTION FROM ZENON 7.00

To use the strong encryption of the zenon network, note:

- The password is encrypted individually on each computer and stored in **zenon6.ini**. That means:
  - The password cannot be transferred by copying **zenon6.ini** to another computer.
  - If hardware components are changed, in the network adapter area in particular, the password may be invalid and need to be re-entered.
- Encryption must always be activated or deactivated for all components involved in the zenon network. Communication between encrypted and unencrypted systems is not possible. **zenon Web Server**s only act as a proxy computer and are not affected by encryption.
- If encryption is activated on a computer, it always applies for the projects of this computer with the **Network active** property active.

Information

AES 192 from Microsoft (https://msdn.microsoft.com/en-us/magazine/cc164055.aspx) is used as the encryption algorithm for network communication.

SHA 256 from Microsoft (https://msdn.microsoft.com/en-us/library/system.security.cryptography.sha256%28v=vs.110%29.aspx) is used in order to generate the key from the entered password.

COMPATIBILITY

Encryption is not compatible with versions prior to zenon 7.00 SP0. That means:

System 1	System 2	Communication
zenon 7 encrypted	zenon 7 encrypted	Yes
zenon 7 unencrypted	zenon 7 unencrypted or zenon prior to version 7 unencrypted	Yes
zenon 7 encrypted	zenon 7 unencrypted or zenon prior to version 7 unencrypted	No

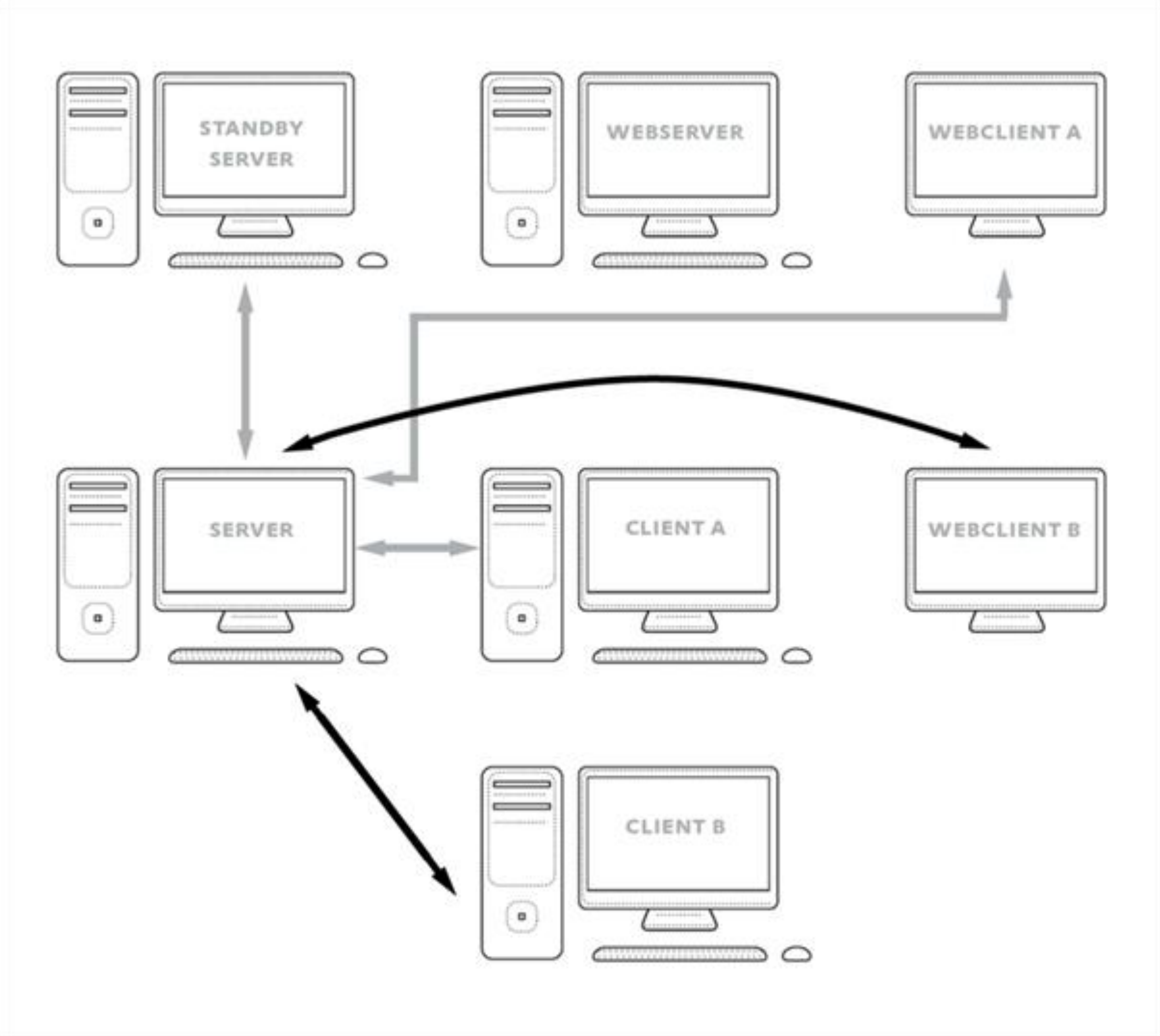
Errors are logged in the Diagnosis Viewer's LOG file.

EXAMPLE

The following illustration shows an example of a network with Primary Server, Standby Server, two clients, one zenon Web Server and two Web Clients. All devices are running zenon 7.00 SP0. The devices are configured as follows:

- Encryption is activated on the Primary Server using the Startup Tool (on page 35).
- Encryption is also activated on the Standby Server and client A via Remote Transport (on page 37) when Runtime files are transferred.
- Client B and Web Client B still communicate without encryption.
- On Web Client A, encryption is activated on the server using the Startup Tool (on page 35).
- Because the zenon Web Server does not evaluate the data packets, but instead forwards these on immediately, it does not require encryption. In theory, it can also have an older version, and the Web Clients can nevertheless create encrypted connections.

This configuration leads to the following result:



- The Standby Server communicates successfully with the Primary Server.
- Client A can log in to the Primary Server and exchange data.
- Because client B sends unencrypted messages and these are rejected by the Primary Server because encryption is active, client B cannot communicate with the Primary Server and is therefore offline.
- Web Client A logs on to the server via the zenon Web Server and can exchange data.
- The unencrypted messages from Web Client B are forwarded from the zenon Web Server to the Primary Server, but the server rejects these. Web Client B cannot communicate with the Primary Serverr and is therefore offline.

As soon as encryption via Remote Transport or the Startup Tool configuration on client B and via **Encrypt network communication** on Web Client B is activated, these connections can also make connections to the Primary Server.

4.2.3.2Activate encryption

Encryption can be activated in different ways:

- By means of the **Startup Tool** (on page 35) for the local computer and the zenon web client
- via Remote Transport (on page 37)

> 👍 **Hint**
>
> For quick, easy activation of the encryption, it is recommended that the configuration is carried our on a computer using Remote Transport (on page 37).

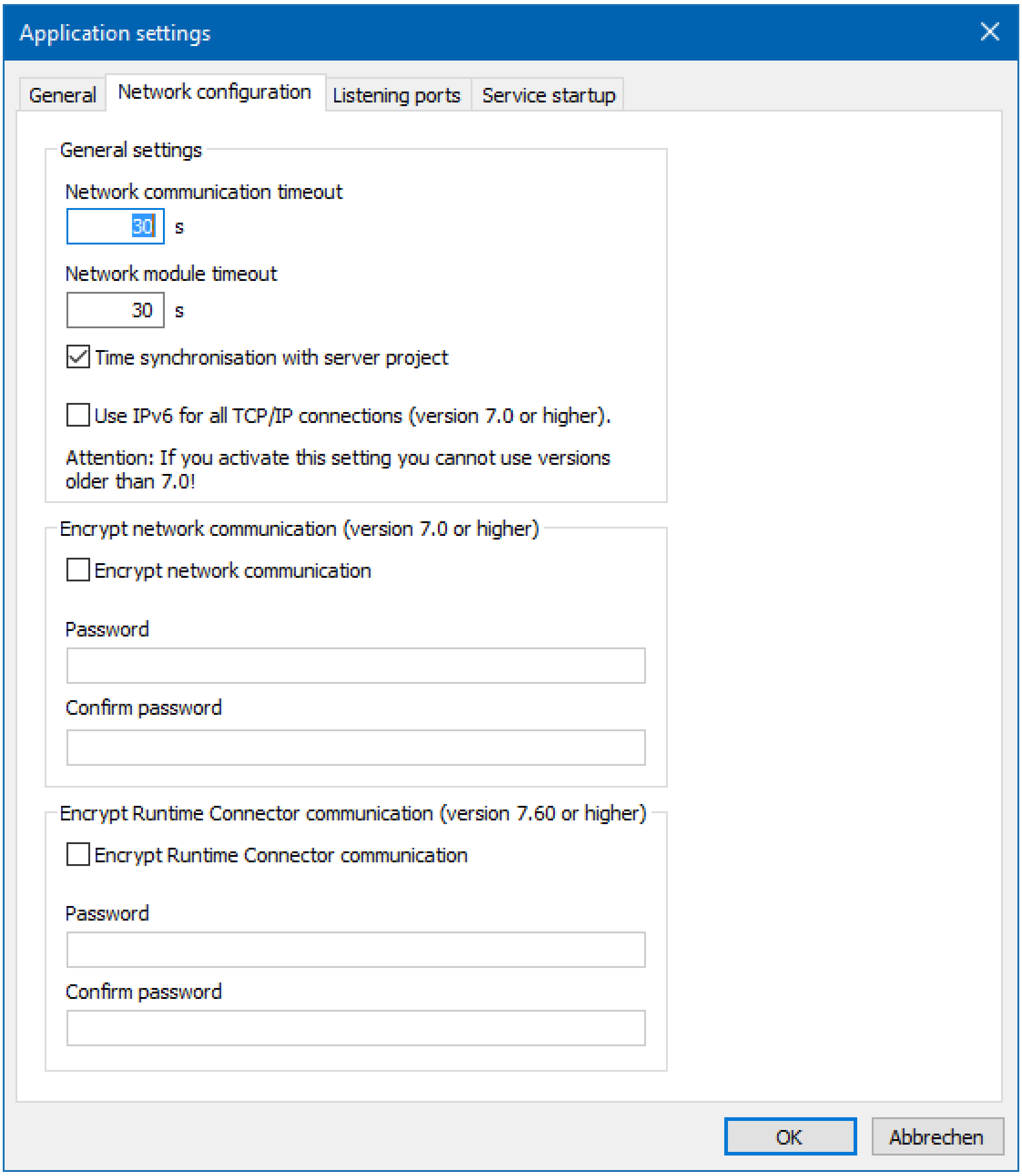
4.2.3.2.1Locally via the Startup Tool

To activate encryption on the local computer or for the <CD_PRODUCTNAME Web> Client:

1. Open the zenon **Startup Tool**.
2. Click **Application -> Options**.

   The dialog for the settings is opened.

3. Select the **Network configuration** tab.



Application settings

General | Network configuration | Listening ports | Service startup

General settings

Network communication timeout: 30 s

Network module timeout: 30 s

☑ Time synchronisation with server project

□ Use IPv6 for all TCP/IP connections (version 7.0 or higher).

Attention: If you activate this setting you cannot use versions older than 7.0!

Encrypt network communication (version 7.0 or higher)

□ Encrypt network communication

Password

Confirm password

Encrypt Runtime Connector communication (version 7.60 or higher)

□ Encrypt Runtime Connector communication

Password

Confirm password

4. Activate the checkbox **Encrypt network communication.**
5. Enter the password and verify it.
6. Confirm the dialog by clicking on **OK**.

CONNECTOR ENCRYPTION

In order to activate the encryption for the SCADA Runtime Connector zenon or zenon Analyzer, the HTML web engine or for the Runtime remote driver, configure the Encrypt Runtime connector communication group of properties.

4.2.3.2.2 Via Remote Transport

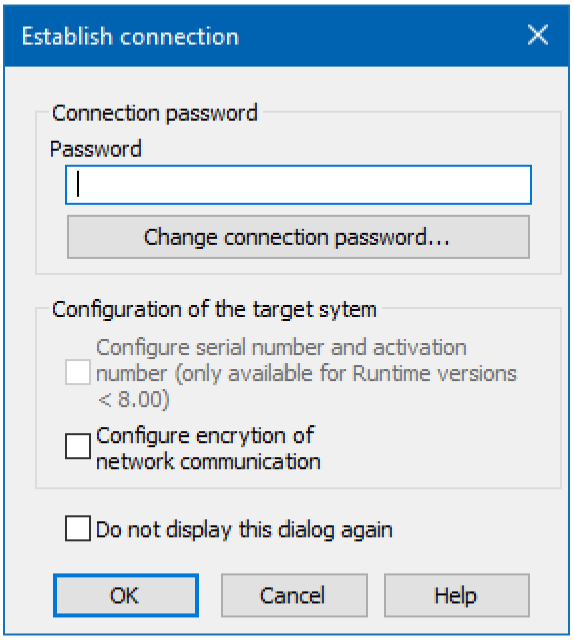
Encryption can be activated on remote computers using Remote Transport. However, this is only possible if the Remote Transport connection is protected with a password.

To activate encryption using Remote Transport:

1. Click on the corresponding button in the Remote Transport toolbar

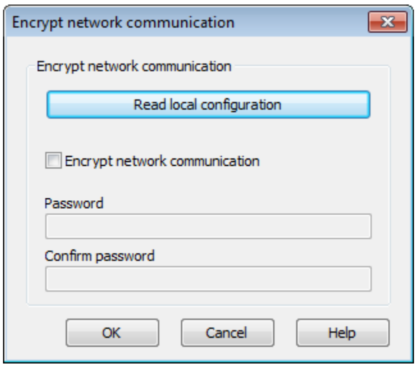
   or select, in the project's context menu: **Set up Remote Transport> connection.**

   The dialog for setting up the connection is opened

   
   Establish connection
Connection password
Password
Change connection password...
Configuration of the target sytem
□ Configure serial number and activation number (only available for Runtime versions < 8.00)
□ Configure encrytion of network communication
□ Do not display this dialog again
OK
Cancel
Help

2. Enter the connection password or create one, if none has been set
3. Activate the **Configure encryption of network communication** checkbox
4. Click on **OK**.

   The dialog for encryption of network communication is opened

   
   Encrypt network communication
Encrypt network communication
Read local configuration
□ Encrypt network communication
Password
Confirm password
OK
Cancel
Help

5. Activate the **Encrypt network communication** checkbox

6. Issue a password (for criteria, see the **network password encryption** section.)
   To quickly transfer the local configuration to other computers, the local password can first be read via **Read local configuration**.
7. Confirm the dialog by clicking on the **OK** button.

4.2.4 zenon API

The zenon API allows access to zenon by means of VBA and VSTA. Individual extensions can thus be programmed and many procedures can be further automated. In sensitive environments, this access constitutes a security risk and can be prevented in part.

Note: zenon does not support DCOM. For this reason, a remote access to the API is not possible.

> ### Information
>
> With the key combination **Ctrl+Pause** (**BREAK**) running code can be interrupted and the VBA editor accessed this way. If you use VBA or VSTA in the project disable the function **BREAK**.

DEACTIVATING THE SENDING OF EVENTS

To deactivate the sending of COM events:

1. Open the **zenon6.ini**.
2. Navigate to the section **[VBA]**.
3. Enter the value *0* for the **EVENT=** key word.
   The sending of Events to external applications is thus prevented.

4.2.5 IEC 61850

zenon supports the IEC 61850 protocol as well as OPC UA including security features.

4.2.6 Voice over IP - Message Control

In the zenon **Message Control** module, the *Voice over IP* (*VoIP*) dispatch type is also available. It is only for the sending of messages. No incoming calls are taken.

> ### ⚠Attention
>
> There is no encryption available for *VoIP*. This type of dispatch should therefore not be used if there is a need for security.

4.2.7 Process Gateways

ACCESSOPCUA

Ensure the following when using the **AccessOPCUA** process gateway:

- In the configuration, only safe connections are permitted, and integrated user authentication should be used.
- OPC UA clients should use MessageMode Security Sign&Encrypt.
- An authenticated and authorized OPC UA client should not place increased load on the AccessOPCUA server, by sending many (invalid) queries for example.

4.3 Editor

The concept of zenon allows the operation of Runtime and the Editor on separate computers. Often, the security of systems on which Runtime is running is rated as more important than that of Editor systems. However both must be rated as equally important.

Background: An attacker who has managed to get into a production network and discover, for example, a PLC with Modbus, cannot detect which processes and values are behind it using the Coils, Holding Registers or Inputs. A PLC program, technical illustrations or even also the HMI/SCADA software offer attackers the required information under certain circumstances.

4.3.1 Encryption

The zenon Editor can - just like zenon Runtime - transmit the data in the network in encrypted form. Activate this encryption. You can find details in the section Encryption in the network (on page 31).

4.3.2 Editor computer without distributed engineering

If the zenon is only installed on one computer as an Editor and the project configuration is carried out on this computer, we recommend the following checks and changes after installation:

- SQL:
  - Change the standard password for the SQL user **sa**.
  - Change the standard password for the SQL user **zenonsrv** both in the SQL server instance and using the **Startup Tool**.

    Attention: For systems that use **distributed engineering**, the same password must be used for the user **zenonsrv** on the server and clients

  - Deactivate the SQL browser service on computers with the zenon Editor, if this is not needed by other SQL server instances on this computer.
  - Deactivate the remote access to the SQL server.
    Note: Systems with **distributed engineering** need remote access.
- Limit the execution of the Editor and Runtime to precisely-defined users.

  In addition to the backup of the zenon projects using the user administration, it is also possible to use the Windows security settings to determine which users can execute the zenon Editor.
- Do not close the required ports (on page 17).
- Activate network encryption and set the password according to your Runtime systems, provided you use Remote Transport.
- Check the firewall exceptions (on page 16) that are added during installation.
  Remove exceptions for applications that are not used.

4.3.3 Network: Multi Homed

Prohibit operation of several networks on one computer.

Dual-Homed or Multi-Homed computers are a popular target for attackers. They can very often easily be configured to a bridge and then allow direct access from one network to another network. Existing firewalls are thus easily circumvented. Because a computer with the Editor is not always assigned to production, it may happen that such a computer is both connected to the company network and also to the production network. This configuration is unsafe and must be avoided.

4.3.4 Project backup and workspace backup

Project backups and workspace backups should only be restored from trustworthy sources.

Encrypt copies of project backups or workspace backups before transport or storage at a central location. If necessary, use the additional functions or additional software. Before restoring to the Editor, the backup must be restored from the encrypted copy.

4.3.5 History of Changes

Activate the revision history, so that changes can be logged in the project. Set a password so that the change history cannot be deactivated without authorization. It usually makes sense to activate the revision history only once the equipment has been supplied.

4.3.6 Project versioning with XML export

Activate the project versioning in the project with the *XML export* option. The project backups also contain the XML export. This allows a further comparison between project backups and thus also incremental restoration of individual components.

4.3.7 User Administration

Use the user administration in the Editor too.
You can thus prevent unauthorized loading of a project and link the editing to authorization levels granularly.

You can read about the roles and authorizations that are required for Editor on the SQL Server in the **Roles and authorizations for databases** (on page 21) chapter**.**

4.3.8 Runtime tests

Use the driver simulation for Runtime tests.

4.3.9 Import from variables

The online import of variables from the PLC directly replaces a connection between the Editor computer and the PLC. The use of a "third-party" computer in the production network that was also used in other networks constitutes a risk.

You should therefore use, if possible, offline import or an Editor computer that is a fixed part of the production network. Otherwise use a test environment for online import and check the PLC before this is integrated into the production network again.

4.4 PLC communication

With most protocols for communication with controllers, there is no possibility to encrypt the data used or to check the authentication. Many controllers also do not themselves offer the possibility to also encrypt the transport channel.

A SCADA system or a PLC thus has no possibility to check whether communication is actually taking place directly or if there is a compromised computer between them (man in the middle), which an attacker can use to view and also modify the data if they know the protocol.

For communication via Ethernet, use Switches, that have **Port Security** if possible, thus preventing the diversion of communication via a compromised computer or making it more difficult. Intrusion Detection systems can also monitor ARP or NDP and report attempts to divert communication.

4.5 Monitoring devices with SNMP

zenon offers an **SNMP_NG** driver that supports **SNMPv1**, **SNMPv2** and **SNMPv3**. This driver can be used on networked computers to monitor the devices connected to the Runtime, such as Runtime clients or the PLC and to display and monitor the status of network components such as switches or network printers.

READING SNMP AGENTS - RECEIVING TRAPS

The **SNMP_NG** driver can read data from SNMP-compatible devices. It can use the ping status to establish whether the end device can be reached using the ICMP protocol and receive SNMP traps.

PING STATUS POSITIVE

The SNMP_NG driver can be used not just to read devices via SNMP, but also to cyclically ping devices connected to the network that are not SNMP agents. The result can be evaluated in Runtime and an alarm can be triggered if a device no longer responds.

PING STATUS NEGATIVE: SECURITY ZONES - DMZ - COMPANY NETWORK - INTERNET

The ping status can also be used for negative tests. If a networked computer is used together with zenon Runtime in an environment in which no connection to other security zones, the DMZ, the company network or to the Internet is to be possible, the ping status of the SNMP_NG driver can also be monitored cyclically. In the case the ping should always fail. If there is nevertheless a response to a ping, an alarm can be triggered accordingly.

WINDOWS EVENTS AS SNMP TRAPS

The Windows event logs log much information about the local system. Messages that may be relevant to security are also logged there. However, if these messages are not collected and checked centrally, important notices and early warnings may be lost under certain circumstances. Events from the Windows event logs cannot be read into zenon directly. However this is possible with the Windows standard function and the SNMP_NG driver.

Windows offers an SNMP agent that can be activated as configured as a service using the Control Panel. With this service, the local computer can be configured as a trap recipient. The **evntwin.exe** (Event to Trap Translator) program can then be used to generate an SNMP trap for any desired Windows events. The SNMP traps can then be created in zenon as a trap variable. The reading of an initial value is not possible for this trap, however it is possible to set an alarm in Runtime if a certain Windows event is generated and a corresponding trap is received.

Non-networked computers can also be monitored this way. It is not just the local computer that can be configured as a trap, but also other computers in the network. The central monitoring of networked computers is thus possible via zenon Runtime and the SNMP_NG driver, even for Windows computers on which zenon Runtime is not installed.

Additional information:

- Security check and attack detection:
  https://msdn.microsoft.com/en-us/library/cc875806.aspx
  (https://msdn.microsoft.com/en-us/library/cc875806.aspx)
- Event log monitoring:
  http://www.redblue.team/2015/09/spotting-adversary-with-windows-event.html
  (http://www.redblue.team/2015/09/spotting-adversary-with-windows-event.html)

4.6 Web server/Web client

zenon Web Server and zenon Web Client are only designed for use in a protected network. The web server should not be contactable via the Internet, either directly or indirectly via port forwarding.

In principle, it is possible to connect a web client at a certain location to a Runtime at another location using a web server. In doing so, the design of the network architecture must be solid. The web server should be configured this way in a DMZ. Communication between the networks of the web server and the client is ideally implemented by means of a VPN tunnel.

5 Further information and consulting

COPA-DATA can only provide support for the configuration of our own products. For general questions regarding security in IT, operating systems, networks etc. contact your IT consultant.

For questions regarding the security in zenon please contact the COPA-DATA Consulting, either via the phone number stated in your service contract or via e-mail to support@copadata.com.