



**zenon**  
by COPA-DATA



The background features a series of overlapping, 3D-rendered rectangular blocks in various shades of blue and orange, creating a sense of depth and perspective. The blocks are arranged in a stepped, staircase-like pattern that recedes towards the top right of the frame.

# Manuel de zenon zenon Security Guide

v.8.20



**COPADATA**

© 2020 Ing. Punzenberger COPA-DATA GmbH.

Tous droits réservés.

La distribution et/ou reproduction de ce document ou partie de ce document, sous n'importe quelle forme, n'est autorisée qu'avec la permission écrite de la société COPA-DATA. Les données techniques ne sont utilisées que pour décrire le produit et ne sont pas des propriétés garanties au sens légal. Document sujet aux changements, techniques ou autres.

# Contenu

<b>1</b>	<b>Welcome to COPA-DATA help .....</b>	<b>5</b>
<b>2</b>	<b>zenon Security Guide .....</b>	<b>5</b>
<b>3</b>	<b>Protect the IT.....</b>	<b>7</b>
3.1	Putting a computer out of operation.....	8
3.2	Operating system.....	8
3.2.1	Secure installation and operation of the operating system.....	9
3.2.2	Benutzerverwaltung .....	13
3.2.3	Windows Sicherheitseinstellungen .....	14
3.2.4	Spezielle Windows-Einstellungen.....	15
3.3	Installation zenon .....	16
3.3.1	Firewall Ausnahmen .....	16
3.3.2	Ports für zenon und zenon Analyzer .....	18
3.4	Microsoft SQL Server.....	21
3.4.1	Rollen und Berechtigungen für Datenbanken.....	22
3.5	Hardware.....	24
<b>4</b>	<b>Protect zenon .....</b>	<b>26</b>
4.1	Supported Operating systems for zenon. ....	27
4.2	Runtime .....	27
4.2.1	Protect zenon file system.....	27
4.2.2	Benutzerverwaltung .....	30
4.2.3	Encryption in the network .....	33
4.2.4	zenon API .....	39
4.2.5	IEC 61850.....	39
4.2.6	Voice over IP - Message Control .....	39
4.2.7	Process Gateways.....	41
4.3	Editor .....	41
4.3.1	Encryption .....	41
4.3.2	Editor computer without distributed engineering.....	41
4.3.3	Netzwerk: Multi Homed .....	42
4.3.4	Projektsicherung und Arbeitsplatzsicherung .....	42
4.3.5	Änderungshistorie .....	42
4.3.6	Project versioning with XML export.....	43
4.3.7	User Administration .....	43
4.3.8	Runtime Tests .....	43



4.3.9 Import from variables.....	43
4.4 PLC communication.....	43
4.5 Monitoring devices with SNMP.....	44
4.6 Web server/Web client .....	45
<b>5 Further information and consulting.....</b>	<b>45</b>

## 1 Welcome to COPA-DATA help

### TUTORIELS VIDÉO DE ZENON.

Des exemples concrets de configurations de projets dans zenon sont disponibles sur notre chaîne YouTube ([https://www.copadata.com/tutorial\\_menu](https://www.copadata.com/tutorial_menu)). Les tutoriels sont regroupés par sujet et proposent un aperçu de l'utilisation des différents modules de zenon. Les tutoriels sont disponibles en anglais.

### AIDE GÉNÉRALE

Si vous ne trouvez pas certaines informations dans ce chapitre de l'aide ou si vous souhaitez nous suggérer d'intégrer un complément d'information, veuillez nous contacter par e-mail : [documentation@copadata.com](mailto:documentation@copadata.com).

### ASSISTANCE PROJET

Vous pouvez obtenir de l'aide pour tout projet en contactant par e-mail notre service d'assistance : [support@copadata.com](mailto:support@copadata.com)

### LICENCES ET MODULES

Si vous vous rendez compte que vous avez besoin de licences ou de modules supplémentaires, veuillez contacter l'équipe commerciale par e-mail : E-mail [sales@copadata.com](mailto: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:  
[\(https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/\\_content/m/m04/m04.html\)  
Focuses on practical measures for security.](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04.html)
- ▶ 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.

### Informations

Viele Computer werden mit vorinstalliertem Betriebssystem geliefert. Setzen Sie das Betriebssystem komplett neu auf, bevor zenon Runtime und/oder Editor installiert werden.

**Hintergrund:** Viele Hersteller installieren standardmäßig viele unterschiedliche Tools und Programme, die für zenon nicht benötigt werden und zusätzliche Sicherheitsrisiken mit sich bringen können.

**Empfehlung:** Installieren Sie immer nur die Komponenten und Programme, die für den Betrieb nötig sind.

## 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 order 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 Benutzerverwaltung

COPA-DATA empfiehlt, Benutzer und Passwörter so frei wie nötig und so eingeschränkt wie möglich zu konfigurieren. Wie Sie Benutzer in zenon verwalten, lesen Sie im Handbuch **Benutzerverwaltung** im Kapitel **zenon Login und Benutzerverwaltung in der Runtime**.

## BENUTZER

Für den Betrieb von zenon benötigen Sie in der Regel 4 Windows-Benutzer:

Rolle	Beispiel	Rechte
System-Administrator	zenon_ADMIN	Administrator
System-Services	zenon_SERVICE	Standardbenutzer
System-Engineer	zenon_ENGINEER	Standardbenutzer
Benutzer (für Desktop-Login oder Autostart)	zenon_USER	Standardbenutzer

Diese Benutzer werden auch für die Konfiguration des SQL Servers eingesetzt. Welche Rollen und Berechtigungen benötigt werden, lesen Sie im Kapitel **Rollen und Berechtigungen für Datenbanken** (à la page 22).

## PASSWÖRTER

Passwörter sollten eine angemessene Länge und Stärke verlangen. Dazu gehört die Verwendung von Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen.

### Empfehlung:

- ▶ Vergeben Sie bereits bei der Installation ein Passwort für den lokalen Administrator.
- ▶ Erzwingen Sie ein Passwort für jedes Konto, auch Gästekonten.
- ▶ Zwingen Sie Administratoren, besonders starke Passwörter zu benutzen.
- ▶ Zwingen Sie Benutzer, starke Passwörter zu verwenden.
- ▶ Informieren Sie Benutzer, wie man sich starke Passwörter merkt, ohne sie zu notieren.

### ⚠ Attention

Beachten Sie:

- ▶ Verwenden Sie am besten nur Zeichen, die mit jeder Tastatur eingegeben werden können, also z.B. keine deutschen Umlaute.
- ▶ Passwörter für Autologon-Konten dürfen nicht automatisch verfallen.

### 3.2.3 Windows Sicherheitseinstellungen

Windows bietet eine Reihe von Sicherheitseinstellungen. Beachten Sie dazu auch die Dokumentation von Microsoft.

#### Empfehlungen:

- ▶ Deaktivieren Sie Autorun für alle Laufwerke.
- ▶ Vermeiden Sie das automatische Ausführen von Updates für Betriebssystem und Anwendungen.  
Spielen Sie Updates nur ein, nachdem Sie diese in einer Testumgebung auf die reibungslose Funktion mit Ihren Applikationen überprüft haben.  
Manche Service Packs/Updates können die Eigenschaft **Automatisches Update** ohne weitere Benutzerbenachrichtigung wieder aktivieren.
- ▶ Deaktivieren Sie alle Dienste, die nicht benötigt werden.
- ▶ Setzen Sie für jedes Konto ein starkes Passwort.
- ▶ Vergeben Sie auch für deaktivierte Gast-Konten ein Passwort.
- ▶ Unterbinden Sie automatische Anmeldungen.
- ▶ Verhindern Sie den Netzwerkzugriff auf die Konten lokaler Administratoren und auf Gastkonten.
- ▶ Schützen Sie frei gegebene Drucker.  
Geben Sie Drucker nur für eine exakt definierte Gruppe von Benutzern frei.

## 💡 Informations

### Gruppenrichtlinien

Viele sicherheitsrelevante Einstellungen können über Gruppenrichtlinien gesetzt werden. Welche Einstellungen wo getroffen werden, hängt auch vom eingesetzten Betriebssystem ab. Details dazu lesen Sie in der jeweiligen Microsoft Dokumentation.

Informationen finden Sie auch online. Zum Beispiel:

- ▶ 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 Sicherheit und Updates:  
[\(http://technet.microsoft.com/en-us/library/cc498723.aspx\)](http://technet.microsoft.com/en-us/library/cc498723.aspx)
- ▶ Microsoft 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 Spezielle Windows-Einstellungen

Erhöhen Sie die Systemsicherheit, indem Sie einige spezielle Einstellungen für Windows beachten. Lesen Sie dazu auch die Dokumentation von Microsoft.

Empfehlungen für erhöhte Windows Systemsicherheit:

- ▶ Benutzen Sie immer das klassische Anmeldefenster.  
Dieses verlangt die Eingabe des Benutzernamens und des Passworts und zeigt nicht an, welche Konten zur Verfügung stehen.
- ▶ Deaktivieren Sie folgende Funktionalitäten:
  - ▶ Remote-Unterstützung und Fernsteuerung.
  - ▶ Automatische Updates der Wurzelzertifikate.
  - ▶ Automatische Updates bei einer Installation.
  - ▶ Hilfe und Support-Center.

- ▶ Dienst für Zeitserver.  
Aktivieren Sie diesen Dienst nur, wenn ein Rechner wirklich als Time Server agieren muss.

### 3.3 Installation zenon

Stellen Sie vor der Installation von zenon sicher, dass das Installationsmedium dem Original der COPA-DATA entspricht. Erstellen Sie sichere Prüfsummen von Downloads und kontaktieren Sie COPA-DATA, um die Prüfsummen zu vergleichen.

**Hinweis:** Auch wenn Sie eine Datei aus einer vermeintlich sicheren Quelle bezogen haben, besteht die Möglichkeit, dass die Datei während des Transports manipuliert wurde.

Bei der Installation wird von folgenden Annahmen ausgegangen:

- ▶ Das System, auf dem das Produkt installiert wird, ist frei von Schadsoftware wie Viren, Trojaner usw.
- ▶ Es befinden sich keine Softwareprodukte darauf, die nicht für den Betrieb erforderlich sind.
- ▶ Das System befindet sich in einer geschützten Umgebung ohne direkten Zugriff auf das Internet.

**Hinweis:**

Wenn Sie die Software nicht im Standardordner installieren, stellen Sie sicher, dass nur Benutzer mit Administratorrechten im gewählten Ordner Dateien ändern oder hinzufügen können. In den Standardordnern **%Program Files%** und **%Program Files (x86)%** wird das von Windows sichergestellt.

#### 3.3.1 Firewall Ausnahmen

Während der Installation werden vom Setup-Programm einige Ausnahmen in der Windows Firewall konfiguriert. Abhängig vom Einsatzbereich sowie von genutzten Anwendungen und Funktionalität sind diese Ausnahmen unter Umständen nicht erforderlich.

Die Tabelle listet die Ausnahmen und Informationen zu deren Notwendigkeit auf.

Programm oder Service	Ausführbare Datei	Kommentar
CodeMeter Runtime Server	C:\Program Files (x86)\CodeMeter\Runtime\bin\Code Meter.exe	Erforderlich.
CodeMeterFWEx1	C:\Program Files (x86)\CodeMeter\Runtime\bin\Code Meter.exe	Erforderlich.
zenon Logic Runtime	STRATONRT.exe	Erforderlich, wenn der entfernte Rechner mit der zenon Logic Runtime auf

Programm oder Service	Ausführbare Datei	Kommentar
		diesem Rechner kommuniziert.
zenAdminSrv - Administration service	zenAdminSrv.exe	Nicht erforderlich.
zenDBSrv - Database service for SQL Server communication	zenDBSrv.exe 32 bit	Erforderlich, wenn <b>Verteiltes Engineering</b> verwendet wird.
zenDBSrv - Database service for SQL Server communication	zenDBSrv.exe 64 bit	Erforderlich, wenn <b>Verteiltes Engineering</b> verwendet wird.
zenLogSrv - Diagnosis server	zenLogSrv.exe	Erforderlich, wenn: <ul style="list-style-type: none"> <li>▶ dieser Rechner als Remote Logging Server definiert ist oder</li> <li>▶ wenn von einem entfernten Rechner mit dem Diagnose Viewer auf diesen Rechner zugegriffen werden muss</li> </ul>
zenNetSrv - Network communication service	zenNetSrv.exe 32 bit	Erforderlich, wenn die Runtime auf diesem Rechner als <b>Serveur 1</b> oder <b>Serveur 2</b> läuft.
zenNetSrv - Network communication service	zenNetSrv.exe 64 bit	Erforderlich, wenn die Runtime auf diesem Rechner als <b>Serveur 1</b> oder <b>Serveur 2</b> läuft.
zenon Process Gateway	zenProcGateway.exe	Erforderlich, wenn das zenon <b>Process Gateway</b> auf diesem Rechner verwendet wird.
ZenSysSrv - Transport service	zenSysSrv.exe 32 bit	Erforderlich, wenn Remote Transport zu diesem Rechner benötigt wird.

Programm oder Service	Ausführbare Datei	Kommentar
ZenSysSrv - Transport service	zenSysSrv.exe 64 bit	Erforderlich, wenn Remote Transport zu diesem Rechner benötigt wird.

**Hinweis:** Siehe auch Kapitel **Ports für zenon und zenon Analyzer** (à la page 18).

### 3.3.2 Ports für zenon und zenon Analyzer

Bei der Installation von zenon werden durch das Setup Ausnahmen in der Windows Firewall erstellt für manche Anwendungen und Dienste, die einen TCP Listening Port öffnen.

#### 💡 Informations

Konfigurieren Sie nach der Installation die Ausnahmen in der Windows Firewall restriktiver, passend zu Ihrer Umgebung sowie zu den benötigten Anwendungen und Diensten.

Auf sogenannten multi-homed Systemen mit mehreren Netzwerkkarten öffnen zenon Anwendungen und Dienste mit ihren Standardeinstellungen den TCP Listening Port für alle im System vorhandene Netzwerkkarten. Vielfach ist eine Kommunikation über alle Netzwerkkarten jedoch nicht erforderlich und nicht erwünscht.

**Hinweis:** Konfigurieren Sie nach der Installation über das **Startup Tool** die TCP Listening Ports für die jeweiligen Dienste und Anwendungen, entsprechend Ihrer Umgebung und Anforderungen. Erlauben Sie die Kommunikation nur über jene Netzwerkkarte oder IP-Adresse, für die das erforderlich ist. Wenn Sie einem Dienst den **local loopback** Adapter oder die IP-Adresse 127.0.0.1 zuweisen, erlauben sie nur die lokale Kommunikation. Auf diese Art lässt sich z.B. der Zugriff für den lokalen Diagnose Server auf lokalen Diagnose Clients einschränken.

#### 💡 Informations

Wird für eine Verbindung ein anderer Port als der Standard-Port konfiguriert, dann bedeutet das nicht, dass eine unerwünschte Verbindung nicht mehr möglich ist. Ein Angreifer benötigt nur etwas mehr Zeit, um den richtigen Port zu finden.

Bei der Verwendung von Nicht-Standard Ports kann unter Umständen der Standard-Port als **Canary** verwendet werden. Dazu überwachen Sie in einem eventuell vorhandenen **Intrusion Detection System** die Standard-Ports und setzen Sie Alarne für jeglichen Verbindungsversuch zu diesen Ports. Solche Verbindungsversuche könnten verursacht werden durch:

- ▶ nicht korrekt konfigurierte Rechner
- ▶ durch einen Angreifer, der sich der Default Ports bedient

## POR TS

Anwendung	Datei	Aufgabe	TCP-Port	UDP-Port
Netzwerkprojekt	zenNetSrv.exe	Runtime-Kommunikation.	1100	
Remote-Transport	zenSysSrv.exe	Datenübertragung mittels Remote-Transport (Editor) und Diagnose Server.	1101	
zenon Web Server	zenWebsrv.exe	Protokollumsetzer zwischen <b>Web Client</b> und Runtime.	1102	
Distributed Engineering	zenDBSrv.exe	Distributed Engineering	1103	
CodeMeter WebAdmin		Konfiguration von <b>CodeMeter</b> Dongles.	22350	
WibuyKey		Überwachung der <b>WibuKey</b> Dongles.	22347	
SQL Server bei mehrplatzfähigen Projekten		Verwaltung der in Bearbeitung befindlichen Objekte.	1433	1434

**Empfehlung:** Öffnen Sie nur Ports, die Sie für den reibungslosen Betrieb benötigen.

Ports können im **Startup Tool** in der Registerkarte **Listening ports** angepasst werden. In diesem Fall müssen alle beteiligten Geräte angepasst werden!

## STANDARD-POR TS IN COPA-DATA PRODUKTEN

Folgende Ports werden von COPA-DATA Produkten standardmäßig genutzt:

### ZENON

Application	Port standard
Network Service	1100
Transport Service	1101
WEB Service Classic	1102
DB Service	1103
SQL Browser Service,	1434

Application	Port standard
(pour le développement distribué dans Editor)	
<b>zenAdminSrv.exe</b>	50777
<b>zenLicTransfer</b> (Service de transfert de licence)	50784
<b>Logging Service</b>	50780
<b>SNMP Trap Service</b>	50782
<b>WEB Service Tunneling</b>	8080

**ZENON LOGIC**

Application	Port standard
Le port attribué à zenon Logic ou straton dépend du projet et du service.	1200 - 1210 4500 - 4510
Par exemple : Premier projet zenon Logic utilisé 1200 et 9000, deuxième projet 1201 et 9001, etc.	7000 - 7010 9000 - 9010

**ZENON ANALYZER**

Application	Port standard
Administration Service	50777
Analyzer Connector Service	50778
Analyzer License Service	50779
ZAMS	50781

**DRIVERS**

Application	Port standard
Driver Simulation	6000 - 6020
Process Gateway OPC Server	135
Process Gateway SNMP	161
Process Gateway Modbus	502

Application	Port standard
Process Gateway IEC60870-5 104 slave	2402
Process Gateway DEC	5555
Process Gateway DNP3 Slave	20000

## SERVICE GRID

Application	Port standard
Service Grid API	9400
Hub Controller	9410
Data Hub	9411
Hub Controller : Port dédié pour la connexion à Data Hub	9412
Configuration Backend	9420
Identity Service	9430
Policy Service	9440

**Hinweis:** zenon Treiber, die über Ethernet kommunizieren, verwenden TCP und benötigen daher gegebenenfalls Berechtigungen in der Firewall, abhängig vom verwendeten Port.

## 3.4 Microsoft SQL Server

Der Microsoft SQL Server wird nur für den zenon Editor und für den zenon Analyzer benötigt. Er wird jeweils bei der Installation des zenon Editors oder zenon Analyzer mitinstalliert. Der jeweils benötigte MS SQL Server ist auch auf dem Installationsmedium enthalten. Bei der Installation der zenon Runtime wird kein SQL Server installiert.

Der MS SQL Server wird in der Version installiert, die zum Zeitpunkt der Erstellung des Installationsmediums aktuell ist. COPA-DATA empfiehlt, nach der Installation für die Installation von Patches und Updates zu sorgen.

Beachten Sie dabei:

- ▶ Laden und installieren Sie Updates und Patches individuell statt automatisiert.
- ▶ Überprüfen Sie alle Updates und Patches vor der Installation auf einem Testsystem auf unerwünschte Auswirkungen.
- ▶ Setzen Sie Updates und Patches nur nach erfolgreichem Test auf Produktivsystemen ein.

### ⚠ Attention

Nutzen Sie für die Wartung und Absicherung des SQL Servers die entsprechenden Dokumentationen und Leitfäden von Microsoft.

### 3.4.1 Rollen und Berechtigungen für Datenbanken

zenon nutzt für bestimmte Aufgaben MS SQL Server:

- ▶ Editor
- ▶ SQL-Export in der Runtime
- ▶ Datenbanken für IMM und IPA
- ▶ Process Gateway SQL

Dafür werden Standardbenutzer aus zenon verwendet. Details dazu lesen Sie im Kapitel **Benutzerverwaltung** (à la page 13). Diese benötigen am SQL Server eventuell Rollen und Berechtigungen.

### ROLLEN UND BERECHTIGUNGEN AM SQL SERVER

Bestimmte Aktionen benötigen folgende Rollen und minimalen Berechtigungen am SQL Server.

#### ALLGEMEIN

Modul	Aktion	Rolle	Permission zusätzlisch
Startup Tool	Database konfigurieren.		

#### EDITOR

Modul	Aktion	Rolle	Permission zusätzlisch
Allgemein	Editor benutzen.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	--
Archivserver	Auslagerung nach SQL. Es existiert noch keine entsprechende Tabelle.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	<i>CREATE TABLE</i>
IPA	Datenbank erstellen.	<i>DB_DataReader</i>	<i>CREATE TABLE</i>

Modul	Aktion	Rolle	Permission zusätzlich
		<i>DB_DataWriter</i>	
<b>Messtellenverwaltung</b>	Datenbank erstellen.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	<i>CREATE TABLE</i>
<b>MS Azure</b>	Konfiguration.		
<b>Projektsicherung</b>	Projekt sichern/zurücklesen.		
<b>Verteiltes Engineering</b>	Verteiltes Engineering.		
<b>WinCC Wizard</b>	Datenbankverbindung WinCC.		

**RUNTIME**

Modul	Aktion	Rolle	Permission zusätzlich
<b>AML</b>	Export .	<i>DB_DataReader</i> <i>DB_DataWriter</i>	--
<b>AML</b>	Export.  Es existiert noch keine entsprechende Tabelle.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	<i>CREATE TABLE</i>
<b>AML</b>	Export inkrementell.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	--
<b>AML</b>	Export inkrementell.  Es existiert noch keine entsprechende Tabelle.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	<i>CREATE TABLE</i>
<b>Archivserver</b>	Auslagerung nach SQL.  Tabelle existiert.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	--
<b>CEL</b>	Export.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	--
<b>CEL</b>	Export .  Es existiert noch keine	<i>DB_DataReader</i> <i>DB_DataWriter</i>	<i>CREATE TABLE</i>

Modul	Aktion	Rolle	Permission zusätzlich
	entsprechende Tabelle.		
<b>CEL</b>	Export inkrementell.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	--
<b>CEL</b>	Export inkrementell.  Es existiert noch keine entsprechende Tabelle.	<i>DB_DataReader</i> <i>DB_DataWriter</i>	<i>CREATE TABLE</i>
<b>Connector</b>	SQL Connector.		
<b>Erweiterter Trend</b>	Ausgelagerte Archive.		
<b>Process Gateway</b>	AccessSQL.		
<b>Report Generator</b>	SQL.		
<b>Schichtmanagem ent</b>	SQL-Export.		
<b>Treiber</b>	ExportSQL32 Treiber.		
<b>Treiber</b>	SQL Treiber.		
<b>WPF</b>	DataGrid.		

## ZENON ANALYZER

Modul	Aktion	Rolle	Permission zusätzlich
<b>Connector</b>	SQL Connector.		
<b>Linked Server</b>	Linked Azure Server; SQL Instanz.		

## 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 a server.
- ▶ Clients or zenon web clients on the terminal server:  
<CD\_PRODUCTNAME> Runtime as a client and the zenon web client can run on 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.

### Informations

Viele Computer werden mit vorinstalliertem Betriebssystem geliefert. Setzen Sie das Betriebssystem komplett neu auf, bevor zenon Runtime und/oder Editor installiert werden.

**Hintergrund:** Viele Hersteller installieren standardmäßig viele unterschiedliche Tools und Programme, die für zenon nicht benötigt werden und zusätzliche Sicherheitsrisiken mit sich bringen können.

**Empfehlung:** Installieren Sie immer nur die Komponenten und Programme, die für den Betrieb nötig sind.

The following information refers to the zenon version.

## 4.2 Runtime

Die zenon Runtime wird im Betrieb mit der zenon Benutzerverwaltung (inklusive Anbindung an Active Directory) geschützt durch:

- ▶ Authentifizierung des Clients beim Server (ab Version 7)
- ▶ Starke Verschlüsselung (à la page 33) (ab Version 7)
- ▶ Speicherung der Daten im binären Format
- ▶ keine SQL-Datenbank in Verwendung  
(wird nur für zenon Editor benötigt)

Sie können den Schutz weiter erhöhen, indem Sie:

- ▶ den Zugang zum zenon Runtime-Ordner (à la page 27) limitieren
- ▶ die zenon API (à la page 39) abschalten

### 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.

Pour limiter l'accès au système de fichiers :

1. Crée seulement un utilisateur Windows (par ex. : **zenon\_ADMIN**) autorisé à démarrer zenon ainsi qu'à lire et écrire dans le dossier du Runtime zenon.
2. Désactivez l'accès au dossier du Runtime de zenon pour tous les autres utilisateurs de Windows – et notamment les autorisations en lecture !
3. Désactivez tout accès à distance à l'utilisateur **zenon\_ADMIN**.
4. Bloquer tout logiciel de maintenance à distance ou d'accès à distance.
5. Assurez-vous que zenon peut uniquement être démarré si cet utilisateur (**zenon\_ADMIN**) est connecté.  
Puisque les autres utilisateurs Windows ne disposent pas de l'autorisation en lecture, le Runtime démarre uniquement dans le contexte de cet utilisateur (**zenon\_ADMIN**).
6. Assurez-vous que zenon s'exécute sous forme d'invite de commande :
  - a) Pour cela, créez une fonction d'exécution automatique de zenon avec **Keyblock Runtime Start**.
  - b) Activez la propriété **Bloquer les touches système** dans le groupe **Paramètres du Runtime** des propriétés du projet.
  - c) Démarrez zenon en mode plein écran : Définissez la propriété **Titre runtime** sur *Pas de titre*.
  - d) Assurez-vous de prendre également en compte les systèmes multi-moniteurs pendant la configuration.
  - e) Désactivez le démarrage depuis l'Explorateur.
  - f) N'offre pas des boîtes de dialogue de sélection du fichier.  
Remarque : Dans ce cas, aucune fonction nécessitant que l'utilisateur sélectionne des fichiers dans le Runtime ne peut être configurée.

L'accès au système de fichiers de zenon est alors protégé.

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 **Titre runtime** 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

## 💡 Informations

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 Benutzerverwaltung

zenon sieht sowohl für den Editor als auch für den Onlinebetrieb (Runtime) eine Benutzerverwaltung vor. Das Passwortsystem erfüllt die Richtlinien der FDA (Food and Drug Administration, 21 CFR Part 11).

Welche Rollen und Berechtigungen am SQL Server benötigt werden, lesen Sie im Kapitel **Rollen und Berechtigungen für Datenbanken** (à la page 22).

### DAS KONZEPT

Das Passwortkonzept geht davon aus, dass unterschiedliche Anwender unterschiedliche Bedienrechte (Passwortebenen) besitzen. Auch Administratoren verfügen über unterschiedliche Berechtigungsebenen. Sie haben aber zusätzliche verwaltungsbezogene Funktionen, wie das Administrieren von Benutzern.

Im zenon Passwortkonzept ist es möglich, jedem Benutzer mehrere selektive (einzelnen definierte) Passwortebenen (Bedienrechte) zuzuweisen. Es sind maximal 128 (0-127) Passwortebenen projektierbar. Die Zuordnung der Benutzer zu den einzelnen Passwortebenen und der damit verbundene Aufbau des projektspezifischen Passwortkonzepts kann vollständig frei erfolgen. Jedem Benutzer können beliebige Ebenen zugewiesen werden. So kann z.B. der Benutzer 1 über die Ebenen 0, 1, 5, 6 verfügen und der Benutzer 2 über die Ebenen 0, 1, 6, 8, 10. Es können nur Berechtigungen vergeben werden, über die der Administrator selbst verfügt.

Das Anmelden des Benutzers im Onlinebetrieb erfolgt über die Aktivierung der Funktion Login. Soll der Benutzer aufgrund eines Ereignisses automatisch angemeldet werden (z.B. Schlüsselschalterstellung als Meldung im System vorhanden), wird die Funktion Login ohne Passwort verwendet. Die Funktion wird in einem Grenzwert bzw. in einer Rema der Variable in der Variablenverwaltung projektiert.

Das eigenständige Abmelden des Benutzers im Onlinebetrieb erfolgt mit der Funktion Logout. Der dann automatisch neu am System angemeldete Benutzer ist der Benutzer **SYSTEM**. Wird über einen projektierten Zeitraum lang keine neuerliche Bedienaktion vorgenommen, kann ein automatisches, zeitgesteuertes Abmelden erfolgen.

Für die Erstellung und Verwaltung der Benutzer sowie die Vergabe von Passwörtern, beachten Sie auch die Hinweise im Kapitel zenon Dateisystem schützen (à la page 27).

#### 4.2.2.1 Optionen zur Runtime

In der Runtime bietet die Benutzerverwaltung verschiedene Möglichkeiten.

Il est également possible d'utiliser Windows AD ou AD LDS pour la gestion des utilisateurs. Les utilisateurs peuvent se connecter de façon permanente ou temporaire et être administrés dans le Runtime.

**Remarque :** Il n'est pas possible de renommer des groupes d'utilisateurs dans le Runtime.

##### **⚠ Attention**

Les paramètres des utilisateurs modifiés dans Editor peuvent uniquement être appliqués si la propriété de projet **Données modifiables dans le Runtime** (groupe **Général**) autorise le remplacement des propriétés d'utilisateurs lors de l'écriture de fichiers dans le Runtime.

Les paramètres modifiés dans le Runtime peuvent être appliqués à l'aide de la commande **Importer les fichiers de Runtime** (barre d'outils Fichiers du Runtime) dans Editor. Pour cela, la décompilation doit être autorisée dans la propriété **Données modifiables dans le Runtime**. C'est le cas si la case pour la *Gestion des utilisateurs* a été désactivée dans la colonne *Ne pas décompiler*.

## SIGNATURE NÉCESSAIRE

Les actions d'utilisateurs peuvent également être protégées par une signature. Cela s'applique par exemple aux éléments dynamiques, fonctions, actions via un menu ou des modifications dans les variables du Recipe Group Manager.

Afin de protéger davantage les actions de l'utilisateur par une signature :

1. Configurez la propriété **Signature nécessaire** pour l'élément respectif dans l'Editor.
2. Effectuez votre sélection dans la liste déroulante :
  - ▶ *Signature avec mot de passe* : Une signature et un mot de passe sont requis pour utiliser l'élément.  
Pour des raisons de sécurité, un mot de passe est à nouveau demandé ici, même si l'utilisateur est déjà connecté. Le texte de signature est consigné dans la liste d'événements chronologiques (CEL) après une utilisation réussie.  
**Attention** : seuls les utilisateurs connectés peuvent signer une action. La signature d'actions avec un identifiant temporaire n'est plus possible.
  - ▶ *Signature sans mot de passe* : Une signature est nécessaire pour actionner l'élément. Elle peut être entrée sans entrer de mot de passe. Le texte de la signature est consigné dans la liste d'événements chronologiques (CEL) après une utilisation réussie de l'élément.
3. Dans la propriété **Texte de signature**, entrez le texte de la signature pour la CEL.

## DANS LE RUNTIME, L'UTILISATEUR EST INVITÉ À SIGNER L'ACTION DE L'UTILISATEUR. SELON LA CONFIGURATION, L'UTILISATEUR DOIT ÉGALEMENT LA CONFIRMER AVEC SON MOT DE PASSE. DE PLUS, UNE ENTRÉE EST CRÉÉE DANS LA LISTE CHRONOLOGIQUE D'ÉVÉNEMENTS.PERMANTENES UND TEMPORÄRES LOGIN

Après une connexion permanente, l'utilisateur est connecté de façon permanente et peut effectuer toutes les opérations qu'il est autorisé à effectuer. Pour les actions que l'utilisateur n'est pas autorisé à effectuer, un message correspondant est affiché.

Une connexion permanente peut être effectuée comme ceci :

- ▶ Un appel d'un synoptique *Connexion*
- ▶ La fonction **Connexion avec boîte de dialogue**
- ▶ La fonction **Connexion sans mot de passe**

**Conseil** : les boutons protégés par un mot de passe peuvent être masqués pour les utilisateurs connectés. Pour cela, la propriété **Boutons protégés (Propriétés du projet -> Gestion des utilisateurs -> Connexion et signature)** doit être correctement configurée.

- ▶ **Remarque :** la connexion temporaire n'est pas disponible pour les utilisateurs connectés. Les utilisateurs connectés ne voient donc pas de boîte de dialogue de connexion temporaire pour les fonctions nécessitant un niveau d'utilisateur supérieur au leur.

### 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.

#### Informations

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 Notions fondamentales

Le chiffrement dans le Runtime de zenon est disponible à compter de la version 7.00. Il est impossible de communiquer avec les versions antérieures de zenon si le chiffrement est activé. Le chiffrement n'interdit aucune fonctionnalité de zenon.

### CHIFFREMENT DE BASE DE ZENON 7.00

Pour utiliser la fonction de chiffrement fort du réseau zenon, veuillez noter ceci :

- ▶ Le mot de passe est chiffré individuellement sur chaque ordinateur, puis stocké dans **zenon6.ini**. Ceci signifie :
  - ▶ Le mot de passe ne peut pas être transféré en copiant **zenon6.ini** vers un autre ordinateur.
  - ▶ Si des composants matériels sont modifiés, et plus particulièrement au niveau de l'adaptateur de réseau, le mot de passe peut être non valide ; il doit alors être saisi à nouveau.
- ▶ Le chiffrement doit toujours être activé ou désactivé pour tous les composants concernés sur le réseau zenon. Les communications entre les systèmes chiffrés et non chiffrés ne sont pas

autorisées. Les **zenon Web Server**servent uniquement d'ordinateur proxy, et ne sont pas affectés par le chiffrement.

- ▶ Si le chiffrement est activé sur un ordinateur, il s'applique toujours aux projets de cet ordinateur dans lesquels la propriété **Réseau actif** est active.

### Informations

AES 192 de Microsoft

(<https://msdn.microsoft.com/en-us/magazine/cc164055.aspx>) est utilisé comme algorithme de chiffrement pour la communication réseau.

SHA 256 de Microsoft

(<https://msdn.microsoft.com/en-us/library/system.security.cryptography.sha256%28v=vs.110%29.aspx>) est utilisé afin de générer la clé à partir du mot de passe saisi.

## COMPATIBILITÉ

Le chiffrement est incompatible avec les versions antérieures à zenon 7.00 SP0. Ceci signifie :

Système 1	Système 2	Communications
zenon 7 chiffrées	zenon 7 chiffrées	Oui
zenon 7 non chiffrées	zenon 7 non chiffrées ou zenon avant version 7 non chiffrées	Oui
zenon 7 chiffrées	zenon 7 non chiffrées ou zenon avant version 7 non chiffrées	Non

Les erreurs sont consignées dans le fichier journal de l'outil Diagnosis Viewer.

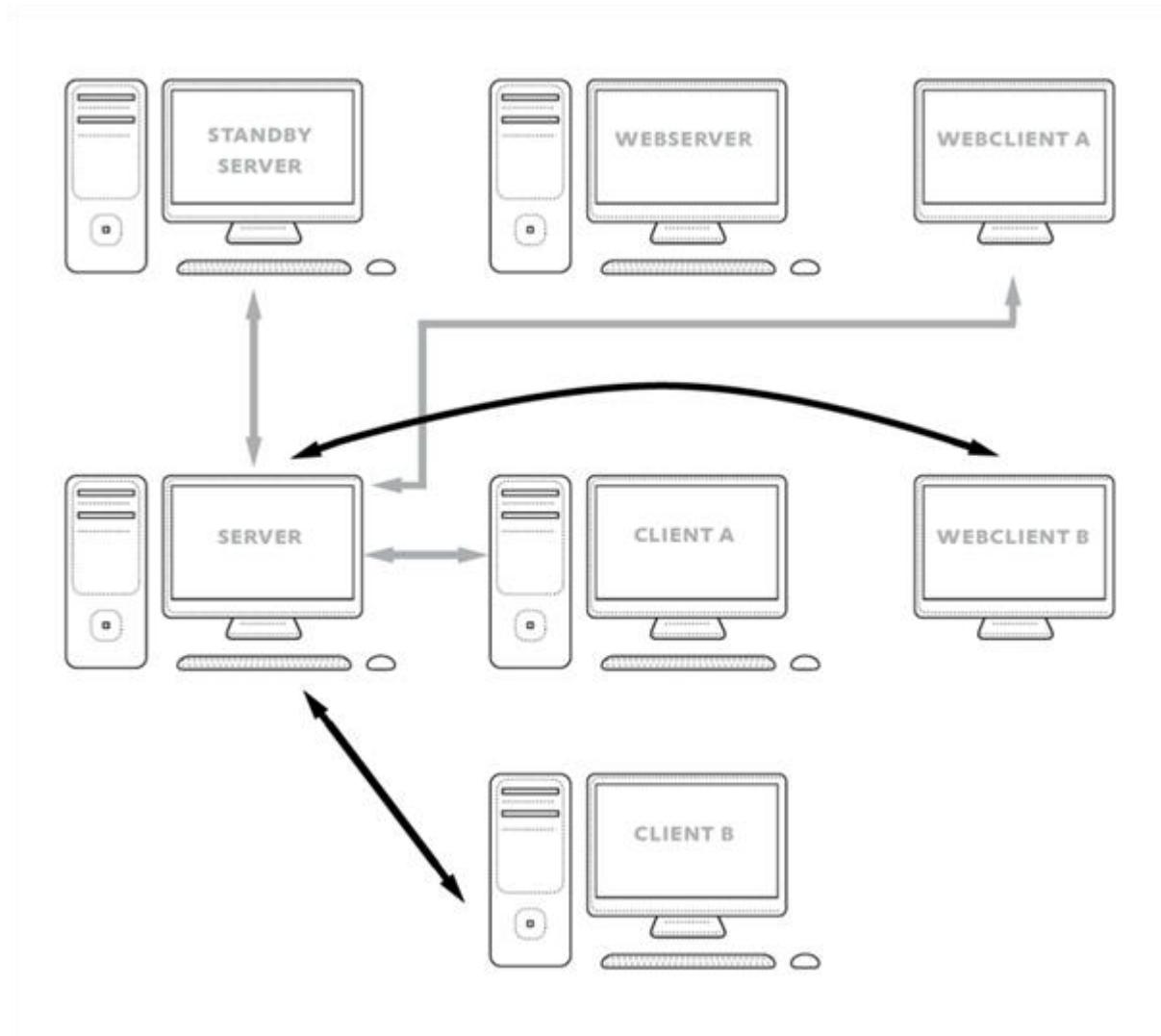
## EXEMPLE

L'illustration suivante montre un exemple de réseau comportant un Serveur principal, un Serveur redondant, deux Clients, un terminal Web Server zenon et deux terminaux Web Client. Tous les équipements exécutent zenon 7.00 SP0. Les équipements sont configurés comme suit :

- ▶ Le chiffrement est activé sur le Serveur principal à l'aide de l'outil Startup Tool (à la page 36).
- ▶ Le chiffrement est également activé sur le Server principal et le Client A via Remote Transport (à la page 38) lors du transfert des fichiers de Runtime.
- ▶ Le Client B et le terminal Web Client B communiquent encore sans chiffrement.
- ▶ Sur le terminal Web Client A, le chiffrement est activé sur le serveur à l'aide de l'outil Startup Tool (à la page 36).

- ▶ Le terminal Web Server zenon n'évalue pas les paquets de données, mais les retransmet immédiatement ; il ne nécessite donc pas de chiffrement. En théorie, il peut également utiliser une version antérieure sans que cela n'empêche les Web Clients de créer des connexions chiffrées.

Cette configuration aboutit au résultat suivant :



- ▶ Le Serveur redondant communique avec le Serveur principal.
- ▶ Le Client A peut se connecter au Serveur principal et échanger des données.
- ▶ Parce que le Client B envoie des messages non chiffrés, qui sont refusés par le Serveur principal parce que le chiffrement est actif, le Client B ne peut pas communiquer avec le Serveur principal et est donc hors ligne.
- ▶ Le terminal Web zenon Client A se connecte au serveur via le terminal Web Server et peut échanger des données.

- ▶ Les messages non chiffrés provenant du terminal Web Client B sont transmis du terminal Web Server zenon au Serveur principal, mais sont refusés par le serveur. Le terminal Web Client B ne peut pas communiquer avec le Serveur principal et est donc hors ligne.

Dès que le chiffrement est activé via Remote Transport ou la configuration de l'outil Startup Tool sur le Client B et via le **Encrypt network communication** sur le terminal Web Client B, ces connexions peuvent établir des connexions au Serveur principal.

#### 4.2.3.2 Activate encryption

Encryption can be activated in different ways:

- ▶ By means of the **Startup Tool** (à la page 36) for the local computer and the zenon web client
- ▶ via Remote Transport (à la page 38)

##### Conseil

For quick, easy activation of the encryption, it is recommended that the configuration is carried our on a computer using Remote Transport (à la page 38).

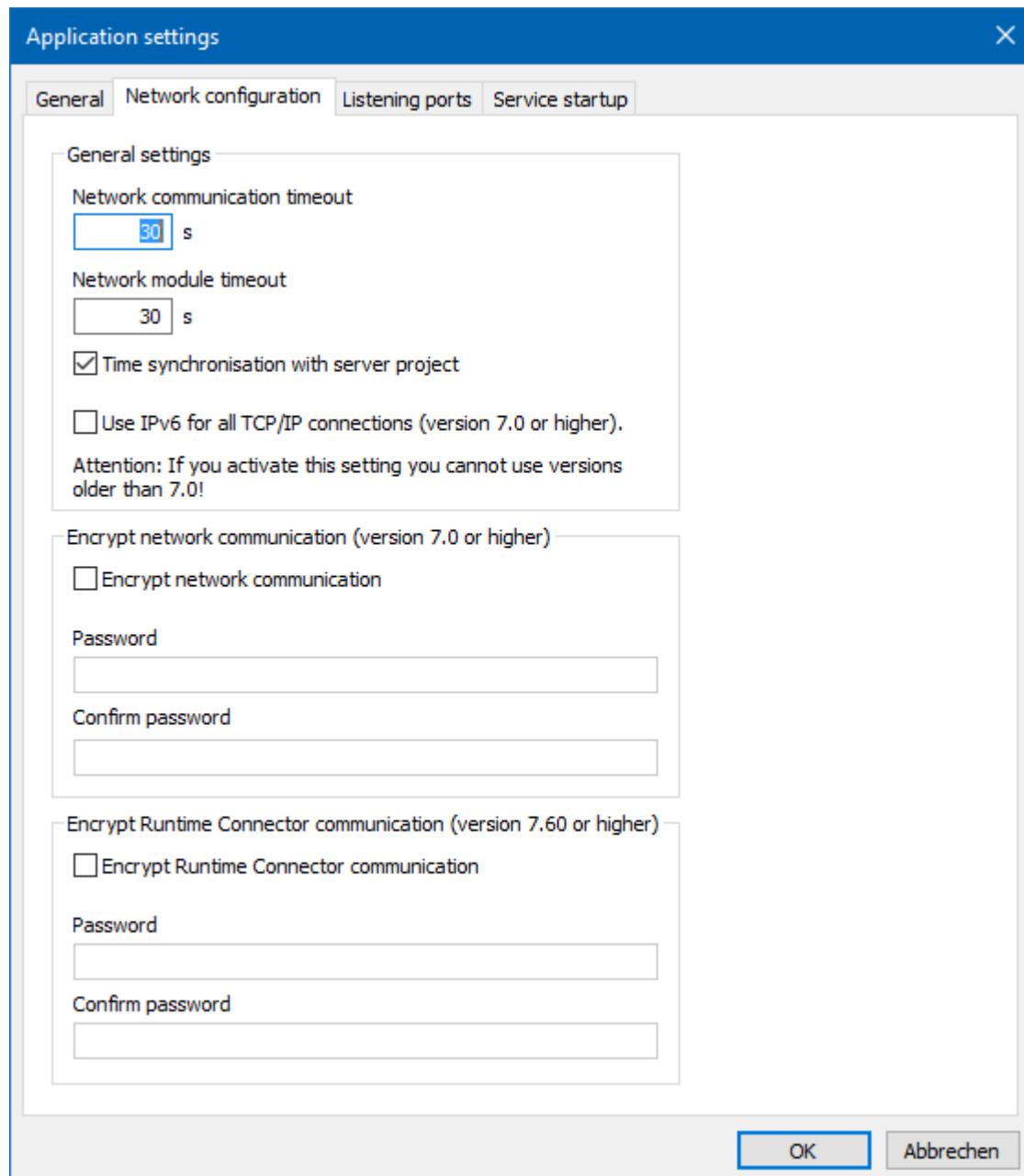
##### 4.2.3.2.1 Locally via the Startup Tool

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.



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.

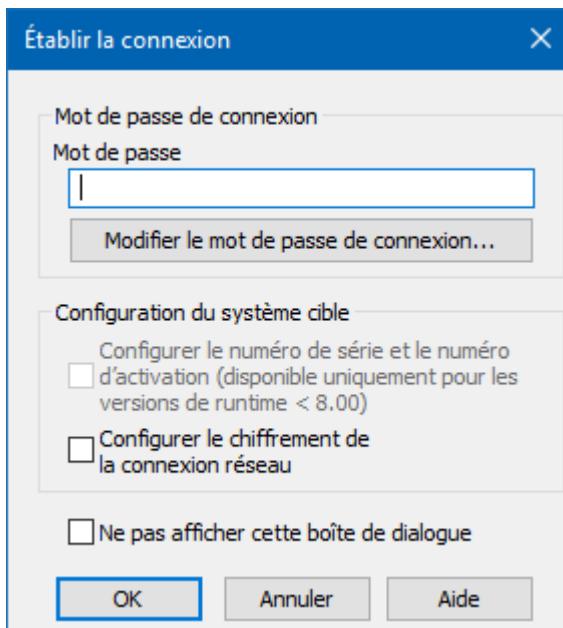
#### 4.2.3.2.2 Via Remote Transport

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:

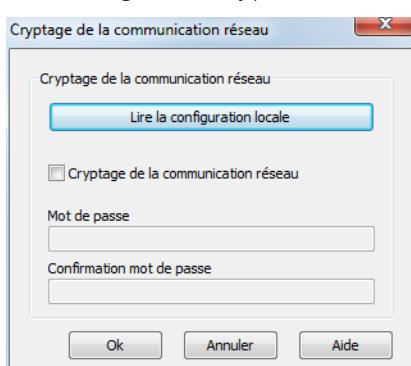
1. Click on the corresponding button in the Remote Transport toolbar  
or select, in the project's context menu: **Set up Remote Transport> connection**.

The dialog for setting up the connection is opened



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



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.

##### Informations

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.

Protect zenon



## 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 (à la page 33).

### 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 (à la page 18).

- ▶ Activate network encryption and set the password according to your Runtime systems, provided you use Remote Transport.

- ▶ Check the firewall exceptions (à la page 16) that are added during installation.

Remove exceptions for applications that are not used.

### 4.3.3 Netzwerk: Multi Homed

Unterbinden Sie in den Betrieb mehrere Netzwerke auf einem Rechner.

Sogenannte Dual-Homed oder Multi-Homed Rechner sind ein begehrtes Ziel für Angreifer. Sie lassen sich oft sehr einfach zu einer Brücke umkonfigurieren und erlauben dann den direkten Zugriff von einem Netzwerk in ein anderes Netzwerk. Vorhandene Firewalls werden damit einfach umgangen. Da ein Rechner mit dem Editor nicht immer der Produktion zugeordnet wird, kann es passieren, dass ein solcher Rechner einerseits mit dem Unternehmensnetzwerk verbunden ist und andererseits mit dem Produktionsnetzwerk. Diese Konfiguration ist unsicher und muss vermieden werden.

### 4.3.4 Projektsicherung und Arbeitsplatzsicherung

Projektsicherungen und Arbeitsplatzsicherungen sollten nur aus vertrauenswürdigen Quellen rückgesichert werden.

Verschlüsseln Sie Kopien von Projektsicherungen oder Arbeitsplatzsicherungen vor dem Transport oder der Ablage an zentraler Stelle. Nutzen Sie bei Bedarf dazu Zusatzfunktionen oder Zusatzsoftware. Vor dem Rücksichern in den Editor muss die Sicherung aus der verschlüsselten Kopie wiederhergestellt werden.

### 4.3.5 Änderungshistorie

Aktivieren Sie die Änderungshistorie, damit Änderungen im Projekt protokolliert werden. Setzen Sie ein Passwort, damit die Änderungshistorie nicht ohne Berechtigung deaktiviert werden kann. Meistens ist es sinnvoll, die Änderungshistorie erst zu aktivieren, wenn die Anlage ausgeliefert wurde.

### 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** (à la page 22) chapter.

### 4.3.8 Runtime Tests

Benutzen Sie die Treibersimulation für Tests der Runtime.

### 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](mailto:support@copadata.com).