SIEMENS

COMOS

Security-relevant configuration

Operating Manual

10/2014
A5E34401884-AC

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: A5E34401884-AC
℗ 09/2016 Subject to change

Table of contents

Introduction

1

This document contains information regarding more secure handling of COMOS.

Functionalities in COMOS undergo a threat and risk analysis by default. In this process, measures for improving the standard product are identified and implemented.

Security-relevant settings and recommendations are described below.

General information

You will find suggestions and recommendations for general technical and organizational security measures under the following links:

- Suggestions and recommendations (http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf)
- General security information (www.siemens.com/industrialsecurity)

Security information

2

Information and links

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

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

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit Product updates (http://support.automation.siemens.com).

Holistic approach

3

Industrial security solutions require a holistic approach based on different protection levels.

Plant security

- Protection against access by unauthorized persons
- Physical access protection for critical components

Network security

- Controlled interfaces between the office and plant networks, e.g., using firewalls
- Additional segmentation of the plant network

System integrity

- Use of antivirus software
- Maintenance and update processes
- User authentication for machine or plant operators
- Integrated access protection mechanisms in automation components

Security management

4

Continuously check security measures and adjust them to your individual requirements.

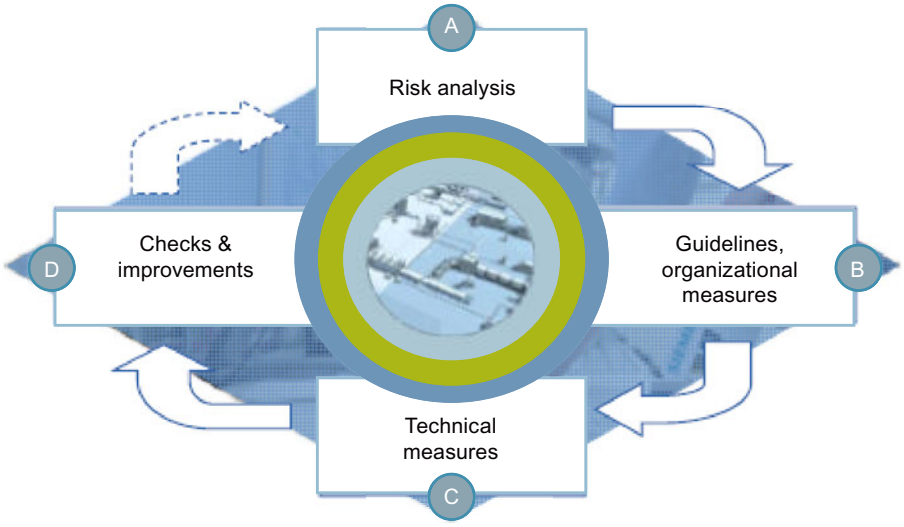
Security management

Security management is an essential component of any industrial security concept. Define security measures to fit your individual plant based on the identified hazards and risks. A continuous security management process is needed to achieve and maintain a required security level:

- Risk analysis including evaluation of current threats and definition of countermeasures for reducing the risk to an acceptable level
- Agreed-upon organizational and technical measures
- Periodic / event-driven repetition

Products, plants, and processes must meet applicable duty-of-care requirements based on laws, standards, internal guidelines, and the state of the art.

Security management process



COMOS - General

5

5.1 Notes on interfaces

Files that are created during an export from COMOS or are imported into COMOS can include sensitive information.

This includes, for example, the Microsoft Project interface, eCl@ss, NOXIE, working layer export or database export.

Take the necessary precautions to protect these files from misuse.

Make sure that the files are protected from theft and manipulation during storage or transfer.

Suitable measures include saving the files to encrypted data storage media or to encrypted file containers as well as sending the data by means of encrypted emails only.

5.2 Protecting communication between Enterprise Server and Enterprise Server Monitor

Make sure that only the administrator and the ES account user have read/write access to the directory specified in the configuration under TmpConfigFileFolder.

5.3 Network login

The document directory contains files that are to be protected from unauthorized access and manipulation.

Set up a specific network login user and grant this user full access rights to the document directory. Remove all rights to the document directory from all other users. Use the Network Security Configuration Tool to allow COMOS users to access the document directory.

You can find more information on this topic in the "COMOS Platform Administration" manual, keyword "Network login".

5.4 Option "Allow login with local user name"

Deactivate the "COMOS" option in the "Allow login with local user name" properties of the user profile. Then, only users logged on to a domain are allowed. You can find more information on this topic in the "COMOS Platform Administration" manual, keyword "Opening the properties of a user profile".

5.5 SAP interface with PKI login

If the SAP system is logged onto using Secure Network Communications, you should also use this technology whenever possible in COMOS.

You can find more information on this topic in the "COMOS Platform Interfaces" manual, keyword "Logging in to the SAP target system with a PKI card".

5.6 Windows authentication

Windows authentication for connection to the COMOS DB

As of COMOS V10.2, you can use Windows authentication instead of SQL authentication for connection to the COMOS DB (see documentation). The option offers better traceability regarding DB access and the advantage that access data no longer have to be managed on the client.

This means each COMOS user is authenticated individually for access to the DB and the document directory. The minimum rights in the DB that each user is to receive independent of his or her role can be determined in the documentation.

Because the assignment of permissions in the DB is a lot coarser than the authorizations used by COMOS, Windows authentication should only be used when it is acceptable regarding confidentiality and integrity of the data that users have access to the entire project (this means that in addition to the engineering project, the base project and the system project must be available completely with read access). To this end, it may be necessary to manage different engineering projects in different databases.

Individual objects within a project cannot be protected with DB rights.

See documentation for additional restrictions when using Windows authentication.

5.7 Providing the password for the database via a file

For the initial logon to a server database, the database server user name and password are requested and these are written to a file.

Recommendation for administrators:

Do not provide the password for database access to the user in plain text. Instead, provide the corresponding encrypted file containing the password.

You can find additional information on this topic in the "COMOS Platform Administration" manual, keyword "Access to the database server".

5.8 Revoking administrator rights for @Setup

The user "@Setup" has administrator rights in a supplied database. As COMOS administrator, create a separate account. Assign administrator rights to the account and revoke administrator rights for user "@SETUP".

You can find more information on this topic in the "COMOS Platform Administration" manual, keyword "Users that cannot be deleted".

5.9 Named licenses - License use by unauthorized users

If you do not use Named Licenses, any Windows user can log on to COMOS and automatically occupy a license, regardless of whether this user has the rights required for working with COMOS.

Specify all permitted users in the "Named User" administration.

You can find more information on this topic in the "COMOS Platform Administration" manual, keyword "Managing licenses with COMOS LS".

5.10 Preventing malware in administered documents

Documents (Word, Excel, PowerPoint, XML) can contain malicious code. Use an antivirus program.

Only import files from confidential sources. When files are exchanged via e-mail, verify the identity of the sender.

Encrypt and sign e-mails. For exchange via a file system, restrict write permission to those parties who actually need it.

Imported Excel and XML files pose a potential risk. Besides the security gaps in software components that process these files, the files can contain incorrect parameters that could cause a production outage and even destruction of the plant or its individual components.

See also

Information and newsletter (http://support.automation.siemens.com)

Additional information (http://support.automation.siemens.com)

5.11 Protection of the COMOS installation

Inadequate protection of the COMOS installation can have the result that the COMOS installation and thus the managed documents could be manipulated.

Make sure that the user logged on to the local computer in Windows does not have administrator rights.

Make sure that only the administrator and no other users have write permission for the directory in which COMOS is installed.

5.12 Authorization for File-Share of the Enterprise Server

Ensure that File-Share is sufficiently safeguarded. This means that only the respective users should have write access to the share directories. Read access to directories of other users should also be removed, as sensitive information may be imported.

You can find more information on this topic in the "COMOS Enterprise Server" manual, keyword "User folder".

5.13 Protecting communication between Enterprise Server and Enterprise Server Monitor

Make sure that the directory specified in the configuration under "TmpConfigFileFolder" can only be edited or viewed by the administrator and the user of the Enterprise Server user account.

5.14 Only using UNC paths in the configuration of the Enterprise Server

Always use the UNC paths, and not links, for "TmpConfigFileFolder" and Share Folder.

5.15 Do not use an Access DB

Access databases do not offer adequate protection against unauthorized access. Use the Microsoft SQL Server.

5.16 Activating encryption of the Microsoft SQL Server network traffic

Activation

Activating the following options has the result that each connection to this SQL Server instance is encrypted. This is regardless of the client and the software used. If you wish to use encryption only for COMOS databases, operate these in a separate SQL Server instance.

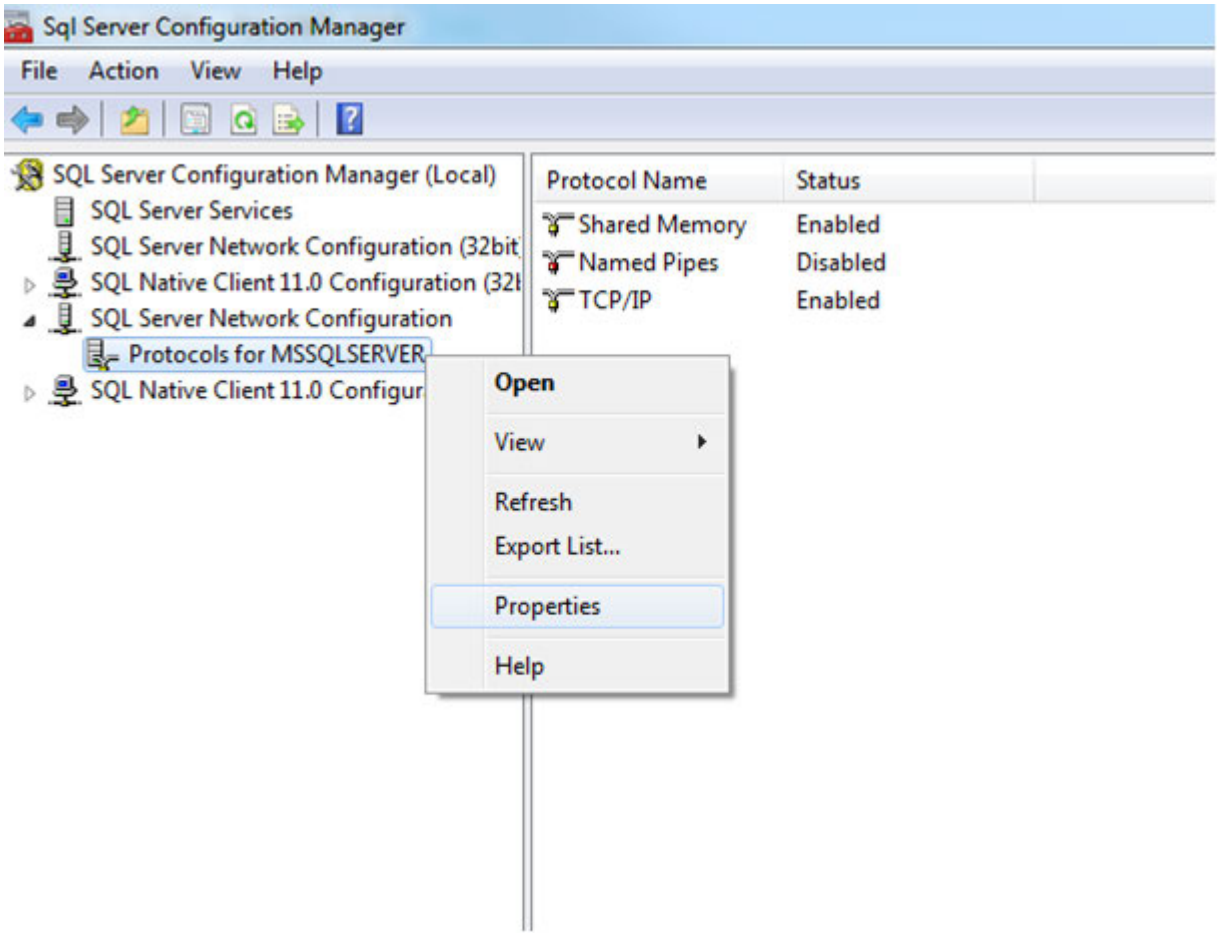
Note

Performance

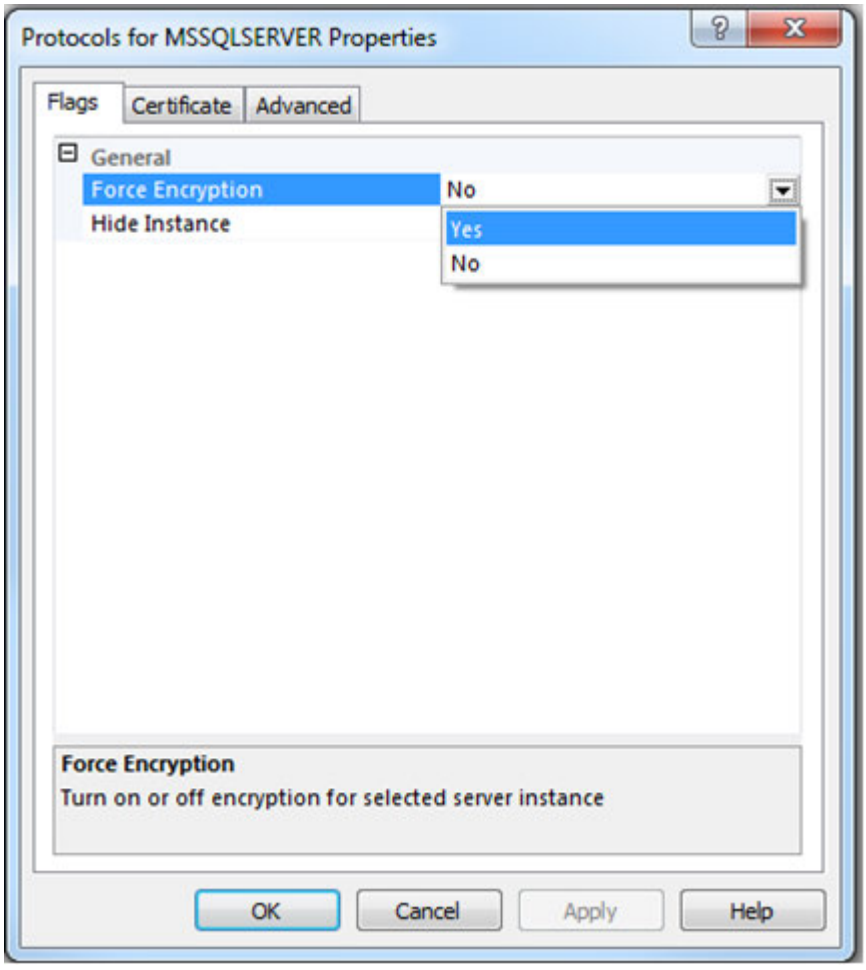
Using this option affects performance. Additional CPU resources are required both on the server and on the client for encryption and decryption. Depending on the software in use and on the server load, a significant reduction in performance may result, particularly on systems which are already operating close to their limits. For this reason, only use the option if the network cannot be protected adequately at a low level.

Procedure

1. To activate the property, start the "Sql Server Configuration Manager".
2. Right-click on "Protocols for <instance name>".
3. Select "Properties" from the context menu.



4. Select "Yes" in the "Force Encryption" row of the "Protocols for <instance name>" window.



5. Click "OK" to confirm your entries.

Result

Encryption is active.

5.17 Updating the software environment

Keep the operating system, web server, and other relevant components updated to the latest version at all times.

Out-of-date software may contain security gaps through which malware can be introduced or sensitive data can be spied on.

Notes on COMOS installation on a Citrix server 6

6.1 No integration of client drives

The integration of local drives enables data to be transferred from the server to the client where it can be taken without permission.

Set up the Citrix server in such a way that integration of client drives is not possible.

Special notes for Portable and Direct 7

Data exchange

In the Portable and Direct area, explosion-proof PDAs, often with optional barcode or RFID scanner, are used. The application there runs offline without an active connection to another computer or a database. The data are exchanged between a device and a COMOS workstation by an authorized COMOS user using ActiveSync and COMOS Enterprise Server (XML).

7.1 Restricting network communication with mobile devices

Devices connected directly to the Internet may have security gaps in their operating system and other installed applications via which malware can be introduced.

For mobile devices, disable all possibilities for connecting to networks, especially Wi-Fi. If network communication is absolutely necessary, allow only connections to trusted networks.

7.2 Connecting mobile devices only to authorized workstations

Risk: Mobile devices could become infected with malware through connection to compromised workstations. Under certain circumstances, sensitive information could be taken from the mobile device in this way.

Connect mobile devices for synchronizing only to trusted workstations that have been designated for synchronization and that comply with the usual security guidelines.

Special notes for COMOS Web 8

8.1 Access via VPN

A server that is directly accessible from the Internet has a high risk of being attacked, especially by denial-of-service or hacking.

Protect your web server from direct access from the Internet.

If remote access from laptops or mobile devices is needed, access using a VPN connection is preferred since this ensures that only devices and user accounts allowed in the network are used. With VPN, an authentication between the end device and the VPN access server takes place before the start of a session, which enables access to COMOS Web via a browser or app after successful logon.

8.2 https

When data are transmitted using the unencrypted http protocol, sensitive customer data can be intercepted and manipulated by third parties. The authentication information (session ID) can also be intercepted and misused.

Configure the web server in such a way that COMOS Web can be reached only using Hypertext Transfer Protocol Secure (https). Configure the firewall appropriately so that only incoming connections to tcp/443 are allowed. You can find more information on this topic in the "COMOS Web" manual, keyword "Setting up SSL".

8.3 Inclusion of documents in the system as with a Full Client

Note

When documents are uploaded via COMOS Web, the same information concerning security applies as for a Full Client. See chapter Preventing malware in administered documents (Page 15). This means that the files are not checked for any malicious code (macro viruses, exploits). The user is responsible for ensuring that harmful documents are not checked in.

8.4 Configuring the web server securely

Comply with the recommendations of the manufacturer regarding security when configuring the web server. You can find more information, for example, under http://technet.microsoft.com/en-us/library/dd450371.aspx (http://technet.microsoft.com/en-us/library/dd450371.aspx).

Incorrect configuration produces security gaps that can result in introduction of malware, stealing of sensitive data, and harm to the data integrity.

8.5 Dedicated server

Multiple applications on one server access the same resources and can cause interference to one another.

Operation of the web server and database server, for example, on the same computer increases the security risk. This is because when the web server is compromised, the customer data in the database are also at risk.

If possible, operate COMOS Web on a dedicated server on which no other applications are run and that is separate from the database server, the server for COMOS document directory, and the COMOS license server.

8.6 Server hardening

The machine on which the web server is operated should be subject to additional measures for closing potential security gaps. For example, deactivate all unneeded user accounts.

You can find more information under:

- http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=17606 (http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=17606)
- http://www.microsoft.com/en-us/download/details.aspx?id=24696 (http://www.microsoft.com/en-us/download/details.aspx?id=24696)
- http://windows.microsoft.com/en-us/windows7/Security-checklist-for-Windows-7 (http://windows.microsoft.com/en-us/windows7/Security-checklist-for-Windows-7)

Special notes for iPad use

9

9.1 COMOS app

Assignment of a PIN for using the COMOS app on an iPad is optional. To prevent unauthorized use of the COMOS app, always assign a PIN.

This measure provides additional protection over and above the COMOS authentication.

9.2 Setting up a PIN input for the device

Set up the iPad in such a way that a PIN must be entered to switch it on.

This provides additional protection against unauthorized access and use.

Special notes for the COMOS Sharepoint plug-in 10

10.1 Access via VPN

Protect your Sharepoint server from direct access from the Internet.

If remote access from laptops or mobile devices is needed, access using a VPN connection is preferred since this ensures that only devices and user accounts allowed in the network are used. With VPN, an authentication between the end device and the VPN access server takes place before the start of a session, which enables access to COMOS Web via a browser or app after successful logon.

10.2 Observing the security information of the manufacturer

During installation, configuration, and operation of Sharepoint, observe the security information of the manufacturer.

If not observed, sensitive data may reach unauthorized persons and the integrity of user data may be harmed

You can find more information under http://technet.microsoft.com/en-us/library/cc288143.aspx (http://technet.microsoft.com/en-us/library/cc288143.aspx).

Special notes on data exchange with SIMATIC PCS 7 11

11.1 Protecting the MDB file

The database used by AdvES is kept in a file located locally on the machine. In order to prevent destruction or modification of data in the database or forwarding of these data to third parties, you must take additional measures to protect this file. Set appropriate Windows access rights so that only the logged on user has access to the MDB file. Perform regular backups.

Special notes for COMOS Walkinside 12

12.1 Restricting rights for uploading

Measure

Grant rights for uploading projects to the Walkinside Server only to trusted users.

Risk

Persons who have uploading rights could upload manipulated files and thus cause operating faults.

12.2 Protecting the database server

Measure

Install the Walkinside Server and the SQL Server in a suitable environment with restricted access.

Risk

The database may contain important data. The risk of data theft can be reduced by granting access to the database server to administrators only.

12.3 Restricting connection to the SQL Server

Measure

Only allow the Walkinside Server to connect to the SQL Server. The clients do not require a direct connection to the SQL Server.

Risk

With this measure, you reduce the risk of data saved on the database server being manipulated or compromised.

12.4 Administrator rights

Measure

Do not grant users Windows administrator rights on the computers.

Risk

With administrator rights, it would be easier for users to infiltrate the computer with malware, which damages sensitive data.

12.5 Using XML files from trusted sources

Recommendation

When you import XML files and projects to Walkinside, make sure that the data originates from a trusted source.

Risk

XML files could contain manipulated or corrupt contents that could result in a faulty data import and the loss of confidential information.

12.6 Using SSL

Measure

Use SSL when configuring the Walkinside Server.

Risk

Data that is queried by the Walkinside Viewer and Browser via http from the Walkinside Server is not encrypted and can be seen by hackers. If you use SSL and query data via https, you reduce the risk of losing confidential information.

12.7 Notes on configuration

12.7.1 Firewall configuration

License ports

COMOS Walkinside uses Flexera for license management. If you use floating licenses, configure two ports. The administrator can configure these ports. The default settings for the ports are 27000 and 27001, even though Flexera recommends reserving 27000 to 27009. The use of a firewall is only necessary if the licenses are accessed from outside the LAN.

12.7.2 Access rights for specific files and directories

Exchange folder

If you are using COMOS Walkinside Integration Interface, there is an exchange folder to which all users have write permissions. By default, this folder is contained in the directory "c:/exchange". This setting can be changed by any user.