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
Industry Sector
Postfach 48 48
90226 NÜRNBERG
GERMANY

ASE34401884-AA
© 07/2014 Subject to change
Copyright © Siemens AG 2013.
All rights reserved
Table of contents

1 Introduction...........................................................................................................................................5
2 Security information..............................................................................................................................7
3 Holistic approach................................................................................................................................9
4 Security management..........................................................................................................................11
5 COMOS - General.............................................................................................................................13
  5.1 Network login...............................................................................................................................13
  5.2 Option "Allow login with local user name".............................................................................13
  5.3 SAP interface with PKI login.................................................................................................13
  5.4 Providing the password for the database via a file...............................................................14
  5.5 Revoking administrator rights for @Setup..............................................................................14
  5.6 Named licenses - License use by unauthorized users..............................................................14
  5.7 Preventing malware in administered documents.................................................................15
  5.8 No administrator rights on local computers...........................................................................15
  5.9 No write permission for COMOS installation directory.......................................................15
  5.10 Authorization for File-Share of the Enterprise Server.........................................................16
  5.11 Restricting the running of exports of the Enterprise Server using authorizations..............16
6 Notes on COMOS installation on a Citrix server.............................................................................17
  6.1 No integration of client drives....................................................................................................17
7 Special notes for Portable and Direct............................................................................................19
  7.1 Restricting network communication with mobile devices....................................................19
  7.2 Connecting mobile devices only to authorized workstations..............................................19
8 Special notes for COMOS Web........................................................................................................21
  8.1 Access via VPN.........................................................................................................................21
  8.2 Always using https....................................................................................................................21
  8.3 Updating the software environment of the COMOS web server..........................................21
  8.4 Inclusion of documents in the system as with a Full Client................................................22
  8.5 Configuring the web server securely.......................................................................................22
  8.6 Dedicated server.......................................................................................................................22
  8.7 Server hardening.......................................................................................................................23
9 Special notes for iPad use..................................................................................................................25
  9.1 Always assigning a PIN..............................................................................................................25

Security concept
Operating Manual, 11/2013, A5E34401884-AA
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2</td>
<td>Setting up a PIN input for the device</td>
<td>25</td>
</tr>
<tr>
<td>10</td>
<td>Special notes for the COMOS Sharepoint plug-in</td>
<td>27</td>
</tr>
<tr>
<td>10.1</td>
<td>Access via VPN</td>
<td>27</td>
</tr>
<tr>
<td>10.2</td>
<td>Observing the security information of the manufacturer</td>
<td>27</td>
</tr>
<tr>
<td>11</td>
<td>Special notes on data exchange with SIMATIC PCS 7</td>
<td>29</td>
</tr>
<tr>
<td>11.1</td>
<td>Review of the generated code</td>
<td>29</td>
</tr>
<tr>
<td>11.2</td>
<td>Confidential handling of imported files</td>
<td>29</td>
</tr>
<tr>
<td>11.3</td>
<td>Protecting the MDB file</td>
<td>29</td>
</tr>
</tbody>
</table>
This document contains information regarding 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.

In some cases, however, the necessary improvements are not implemented in the standard product but rather must be carried out by you as the customer.

Example

- You make use of a certain COMOS functionality instead of an non-secure COMOS functionality.
- You change certain settings within your infrastructure.

General information

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

- General security information (www.siemens.com/industrialsecurity)
Security information

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

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 and whitelisting software
- Maintenance and update processes
- User authentication for machine or plant operators
- Integrated access protection mechanisms in automation components
Security management

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

5.1 Network login

Measure
Authorization for the COMOS document directory

Authorize a user and all COMOS operations use this user. You can find more information on this topic in the "COMOS Platform Administration" manual, keyword "Network login".

Risk
Unauthorized access to or manipulation of documents (external documents or reports) or revisions.

5.2 Option "Allow login with local user name"

Recommendation
Deactivate the option in the 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".

Risk
An attacker can set up its own local user account that is identical to any COMOS user in order to obtain the rights of the other user.

5.3 SAP interface with PKI login

Measure
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".

Risk
No directly open vulnerability, but greater security.
5.4 Providing the password for the database via a file

Measure

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 file containing the password.

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

Risk

With the access data for the database, the user has full access to COMOS tables and their contents.

5.5 Revoking administrator rights for @Setup

Measure

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".

Risk

If you do not implement this measure, any user can log on using the @SETUP account and then has full administrator rights.

5.6 Named licenses - License use by unauthorized users

Measure

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".
Risk

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

5.7 Preventing malware in administered documents

Information

Siemens provides automation and drive products with industrial security functions that support the secure operation of plants or machines. They are an important component in a holistic industrial security concept. With this in mind, our products undergo continuous development. We therefore recommend that you keep yourself informed with respect to our product updates.

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

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. You can find more information about industrial security at:

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

5.8 No administrator rights on local computers

Measure

The user logged on to the local computer in Windows should not have administrator rights.

Risk

With administrator rights, it is possible to willfully or accidentally (e.g. by a Trojan) register introduced COM components, thereby harming the integrity of the COMOS application and thus also the data.

5.9 No write permission for COMOS installation directory

Measure

The user logged on in Windows that works with COMOS should not have write permission to the directory in which COMOS is installed.
5.10 Authorization for File-Share of the Enterprise Server

Measure

Ensure that File-Share is sufficiently safeguarded.

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

Risk

Because the files in File-Share are automatically read in by the Enterprise Server, if the File-Share is inadequately safeguarded, it is possible to willfully or accidentally (e.g., by a Trojan) introduce manipulated files, thereby harming the integrity of the data.

5.11 Restricting the running of exports of the Enterprise Server using authorizations

Measure

Use a suitable authorization concept to restrict the export function of the Enterprise Server.

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

Risk

If the export function is inadequately controlled, sensitive data can be exported from COMOS and forwarded to undesired recipients.
Notes on COMOS installation on a Citrix server

6.1 No integration of client drives

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

Risk
The integration of local drives enables data to be transferred from the server to the client where it can be taken without permission.
Special notes for Portable and Direct

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

Measure
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.

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

7.2 Connecting mobile devices only to authorized workstations

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

Risk
Malware can be introduced to mobile devices through connection to compromised workstations. Under certain circumstances, sensitive information could be taken from the mobile device in this way.
Special notes for COMOS Web

8.1 Access via VPN

Measure
Operate the COMOS web server or IIS web server on the internal company network, together with the other necessary servers (database server, server for COMOS document directory, and COMOS license server).

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.

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

8.2 Always using https

Measure
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.

Risk
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.

8.3 Updating the software environment of the COMOS web server

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

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

8.4 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. 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.

8.5 Configuring the web server securely

Measure

Comply with the recommendations of the manufacturer regarding security when configuring the web server.

Risk

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

8.6 Dedicated server

Measure

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.

Risk

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.
8.7 Server hardening

Measure

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 and services.

Risk

Because every application and service contains potential security gaps, these can be exploited once they become known.
Special notes for iPad use

9.1 Always assigning a PIN

Measure
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.

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

9.2 Setting up a PIN input for the device

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

Risk
This provides additional access protection.
10.1 Access via VPN

Measure
Operate the Sharepoint server or IIS web server in the internal company network, together with the other necessary servers (database server, server for COMOS document directory, and COMOS license server).

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.

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

10.2 Observing the security information of the manufacturer

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

Risk
If not observed, sensitive data may reach unauthorized persons and the integrity of user data may be harmed.
11.1 Review of the generated code

Measure
Ensure that the code generated by COMOS for PCS 7 is reviewed or automatically checked for incorrect parameters.

Risk
If incorrect parameters are used willfully or as a result of malware within COMOS for operation of the plant or its individual components, this may cause a production outage or even destruction of the plant or the individual components.

11.2 Confidential handling of imported files

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

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

Risk
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.

11.3 Protecting the MDB file

Note
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.
11.3 Protecting the MDB file

so that only the logged on user has access to the MDB file. If necessary, encrypt the directory containing the file. Perform regular backups.

Risk

The file can be destroyed willfully or as a result of malware or forwarded to unauthorized third parties.