Security recommendations

COMPACT, GOLD, SuperWISE I and II

Swegon

Content

The document was originally written in Swedish.

1. Introduction

All organizations ensure that their assets are protected from unauthorized access, which means that all connected products/systems should have effective and cost efficient protection.

Swegon's products are primarily associated with indoor climate, but the products are also technically advanced and connected devices.

Operating disruptions affect the indoor environment, irrespective of whether it concerns work areas, server halls or other areas where sensitive assets are kept.

This document describes how Swegon's products perform in terms of IT and information security.

1.1 Purpose

This document has two main aims:

- To describe how Swegon's products comply with requirements and recommendations according to established standards, frameworks and templates including ISO 27000 series, NIST SP 800-53, COBIT, BITS, etcetera.
- To provide specific recommendations regarding installation, configuration and maintenance of Swegon's products to maximize operation and information security.

Recommendations described in this document are applicable, irrespective of whether an organization intends to follow an established standard or not.

1.2 Target group

This document has five target groups:

- Requirements management.

Information about how Swegon satisfies requirements regarding information and IT security.

- System/information owner.

Recommendations for the product's entire life cycle and help in the choice of security measures.

- Installation.

Recommendations regarding, among others, placement, connections and configuration.

- Administration.

Recommendations regarding, among others, maintenance, revision management and backup.

- Review/revision.

Comparison of recommended configurations with actual configurations.

1.3 Reading instructions

In order to make it easier for the reader, the following chapters in this document are classified in accordance with the headings in ISO 27000.

Each chapter begins with a short description of the area and how it relates to Swegon's products. It is shown where the configuration can be made where applicable.

This is followed by specific recommendations from Swegon regarding how an organization should react to satisfy the requirements described in ISO 27000 and best practice.

2. Responsibility and ownership

Reference: SS-ISO/IEC 27002:2014, section 8.1 Responsibility for assets.

2.1 Background

In order to ensure a secure and well-functioning IT environment, servers and other equipment, which manage sensitive information or are critical to activities, should be identified. A list of these should be compiled and ownership as well as responsibility assigned.

Examples of typical areas of responsibility for the owner are to secure severs and other equipment:

- Are included in the list.
- Has information been classified and labelled in terms of confidentiality integrity and availability.
- Managed correctly with respect to implementation, maintenance, modifications and taking out of service.
- Used in accordance with established regulations and procedures.

2.2 Recommendations

Swegon's products are not intended to manage other information than data that has a direct link to air handling.

However, these data include user name/password for the unit, system configuration, log files as well as potential connections to other systems which is why ownership should be assigned to each device.

Swegon recommends that the sections described in this document make up the basis for which areas of responsibility are taken into consideration when assigning an owner.

3. Control of access

Reference: SS-ISO/IEC 27002:2014, section 9.4 System and application access control.

3.1 Background

Access to information needs to be limited to prevent sensitive data from falling into the wrong hands, being erased or changed improperly.

Before a user may access information or make changes to the configuration, the user needs to identify and authenticate themselves with valid user details. It is possible to create unique user accounts linked to one of the access levels set out below:

GOLD, version E/F, SuperWISE II

- Local (restricted access) intended for reading measurement data.
- Installation (extended access) intended for reading and writing device configurations.
- Service (privileged access) intended for device configuration and management of users.

The function to administer user accounts can be found under the User menu option.

GOLD version C/D, Compact, SuperWISE I

- Reader (restricted access) intended for reading measurement data. Alarms can be reset.
- Writer (extended access) intended for reading/writing basic device configurations.
- Service (extended access) intended for reading/writing advance device configurations.
- Admin (privileged access) intended for advance device configuration, management of users and communications settings.

The function to administer user accounts can be found under the Admin/User menu option.

3.2 Recommendations

Swegon recommends that standard user names and passwords are changed when a device is put into service.

A separate account, intended only for emergencies, should be created to prevent a lockout. Authentication details should be printed out and stored securely.

Each user should be assigned a unique and personal user account, and be prompted to change the password when logging in for the first time.

User accounts with privileged access should be used solely for device configuration.

Access levels Local and Reader are sufficient for the supervision and reading of devices.

4. Encryption

(Only GOLD version E/F and SuperWISE II with software version 1.80 or later)

Reference: SS-ISO/IEC 27002:2014, section 10.1 Cryptographic controls.

4.1 Background

Encryption technology should be used to protect sensitive information from unauthorized access.

GOLD version E/F

GOLD supports encryption with the encryption method SSL/TLS for web and e-mail communications.

The function to activate encryption for each protocol can be found under the Communications menu option.

SuperWISE II (with software version 1.80 or later)

In SuperWISE II, e-mail communications are always encrypted using encryption method TLS.

The function to encrypt web communications can be found under the Settings/Communications menu option from version 1.80.

4.2 Recommendations

Swegon recommends the use of encryption technology, for example, by activating https and e-mail via SSL/TLS. Unencrypted communications channels are blocked through firewall configuration in the in-house IT environment.

5. Physical security

Reference: SS-ISO/IEC 27002:2014, section 11.2.1 Equipment siting and protection

5.1 Background

Physical boundaries should be defined and implemented to prevent unauthorized physical access to equipment. Access should only be granted to authorized personnel.

Devices have one or more digital inputs and outputs. In the event of unauthorized access, these could be used to listen in, or to connect non-approved devices to the network.

5.2 Recommendations

Swegon recommends that devices are positioned so that unauthorized access is minimized, for example, through placement in locked areas.

Data and power cables should also be protected and kept separate to prevent interference.

6. Maintenance

Reference: SS-ISO/IEC 27002:2014, section 11.2.4 Equipment maintenance.

6.1 Background

Equipment should be maintained at fixed intervals to ensure continuous function and security.

This section concerns maintenance from a security perspective. For information regarding general maintenance, see the manual for each product.

The products are designed to meet the demand of a minimum of general maintenance. It is therefore especially important to plan security maintenance to avoid a device being 'forgotten'.

6.2 Recommendations

Swegon recommends that manual maintenance and functional checks are performed by qualified personnel at least once a year.

Maintenance activities should be adapted to the services and functions that are active, but some general recommendations for activities are to:

- Ensure that no old or redundant user accounts exist (chapter 3).
- Check that the device configuration corresponds with the commissioning protocol (chapter 7) and documented changes (chapter 8).
- Check that there are backups of device configurations (chapter 9) and that they are intact.
- Make sure that the device is updated with the latest software from Swegon (chapter 12).

7. Device configuration documentation

(Only GOLD version E/F and SuperWISE II)

Reference: SS-ISO/IEC 27002:2014, section 12.1.1 Document and use your operating procedures.

7.1 Background

In order to ensure correct, efficient operation and administration of an IT environment, the network, network components, connection points as well as the relationship between systems should be documented.

GOLD version E/F

GOLD makes it possible to create a commissioning record that contains information, among others, about the device's software, communications, and user settings.

The function to create a commissioning record can be found under the Base settings menu option.

SuperWISE II

SuperWISE makes it possible to create a commissioning record that contains information, among others, about the device's software settings.

The function to create a commissioning record can be found under the Documentation/Commissioning record menu option.

7.2 Recommendations

Swegon recommends that a commissioning record is created with start up and commissioning.

The commissioning record is downloaded from devices and stored protected from unauthorized access together with other documentation of the IT environment.

8. Change management

Reference: SS-ISO/IEC 27002:2014, section 12.1.2 Change management.

8.1 Background

In order to reduce the risk of downtime or disturbances system changes should be planned, tested, approved and documented prior to being carried out.

The products include many functions and configuration options in terms of air handling. The products also include network and communications settings that can impact on the performance and function of the device.

8.2 Recommendations

Swegon recommends that significant changes are not implemented until approval has been obtained from the device owner (chapter 1).

A backup of the device configuration (chapter 9) should be created prior to the change being implemented. This is so the original configuration can be easily restored in the event of the change being unsuccessful.

Functionality should also be verified once the change has been implemented. The changes made should be reflected in the device's documentation (chapter 7).

SuperWISE II

There is an option to export a change log concerning changes to functions and their settings. The function to create a change log can be found under the Change log menu option.

9. Backup

(Only GOLD version E/F and SuperWISE II)

Reference: SS-ISO/IEC 27002:2014, section 12.3 Backup.

9.1 Background

Backups of information and configuration settings should be created to prevent the loss of data, to increase operating reliability and to facilitate trouble shooting.

The products provide the opportunity to create backups of the air handling settings and communications settings.

GOLD version E/F

The function to create a backup of each setting can be found under the Base settings menu option.

SuperWISE II

The function to create a backup of each setting can be found under the Settings/Backup & restoring menu option.

9.2 Recommendations

Swegon recommends that backups are created after the device's initial commissioning and before major changes are made regarding the device configuration.

10. Logging and supervision

(Only GOLD version E/F and SuperWISE II)

Reference: SS-ISO/IEC 27002:2014, section 12.4 Logging and monitoring.

10.1 Background

Logging of the operating status and incidents in IT systems is a prerequisite to ensure a secure and fully functional IT environment.

GOLD version E/F

GOLD allows you to create and supervise logging of climate data. GOLD can also transfer logs automatically to a central log facility via e-mail and/or FTP.

The function for the automatic transfer of log information is available via the Log menu option.

SuperWISE II

SuperWISE II allows you to create and supervise logging of climate data. SuperWISE II can also change and supervise the setting values of functions.

Files with log information are available via the Graph & Log/Log menu option.

The function to create a change log can be found under the Change log menu option.

10.2 Recommendations

GOLD

A unique user account with restricted privileges should be created on the destination host to ensure the secure transfer of log information via FTP.

GOLD only requires write privileges to a directory intended for system logs in order to transfer log information.

11. Clock synchronization

(Only GOLD version E/F and SuperWISE II)

Reference: SS-ISO/IEC 27002:2014, section 12.4.4 Clock synchronization.

11.1 Background

In order to ensure the correct date/time data in incident logs, alarms and other information, the device's system clock should be synchronized with a central reference source for time.

GOLD version E/F

GOLD supports clock synchronization via SNTP and BACNet. Settings for automatic synchronization of time and can be found under the Time and Schedule menu option.

SuperWISE II

Swegon SuperWISE II supports time synchronization via NTP.

Settings for automatic synchronization of time and can be found under the Settings/Time & date menu option.

11.2 Recommendations

Swegon recommends that the function for automatic time synchronization is used.

12. Security updates

Reference: SS-ISO/IEC 27002:2014, section 12.6.1 Control of technical vulnerabilities.

12.1 Background

In order to prevent technical exploitation of technical vulnerabilities, information about security updates should be obtained and managed quickly.

Swegon ensures security updates are installed in connection with scheduled service of the device. If an organization lacks a service agreement, it is the responsibility of the organization itself to ensure that security updates are installed.

12.2 Recommendations

Swegon recommends that security updates are coordinated with maintenance (chapter 6) and change management (chapter 8).

13. Communications security

13.1 Security measures for networks

(Only GOLD version E/F and SuperWISE II)

Reference: SS-ISO/IEC 27002:2014, section 13.1.1 Network controls.

In order to ensure the security of information in the network and the protection of connected services, such services and functions should be managed in cooperation with applicable security measures.

The products have several digital inputs/outputs, services and protocols with different application areas.

GOLD version E/F

The function to activate or deactivate services and protocols can be found under the Communications menu option.

SuperWISE II

The function to activate or deactivate services and protocols can be found under the Settings/Communications and Settings/BACnet menu options.

13.2 Recommendations

(Only GOLD version E/F and SuperWISE II)

Swegon recommends that networks are segregated (section 13.3). Services and protocols that are not used are disabled.

Examples and services and protocols that should be considered are:

GOLD version E/F

- SSH
- Wireless LAN
- Modbus
- BACNet
- Exoline

A commissioning record can be created and used to gain an overview of the configuration of all services and protocols.

SuperWISE II

- SSH (only software version 1.80 or later)
- Modbus
- BACNet

13.3 Network segregation

Reference: SS-ISO/IEC 27002:2014, section 13.1.2 Segregation in networks.

13.3.1 Background

A well-defined demarcation between different network domains based on trust levels, organization departments and functionality can prevent sensitive information from falling into the wrong hands or that violations occur.

The products communicate via standardized protocols. Access to and from the device should be controlled in conjunction with appropriate security measures.

13.3.2 Recommendations

Swegon recommends that the operating network is segmented solely for Swegon products, this is to ensure operation of the indoor climate system.

This can be achieved, for example, by creating a unique VLAN for the operating network, through the firewall configuration or by creating a separate physical or wireless network.

13.4 Remote access

Reference: SS-ISO/IEC 27002:2014, section 6.2.2 Teleworking

13.4.1 Background

Teleworking and remote access to internal systems can be an efficient tool to facilitate administration, trouble shooting, etcetera.

To prevent communications from being intercepted, when passing through potentially unsecured communication channels, this type of functionality should be administered in conjunction with appropriate security measures.

Remote access to the products is possible through the application of a VPN tunnel or firewall configuration in the in-house IT environment.

13.4.2 Recommendations

Swegon recommends that access to the products is limited to the organization's internal network and advises against exposure to the Internet.

If remote access is necessary, the connection should be encrypted with SSL/TLS (see chapter 4) or IPsec.

The permit use of remote access should be limited to equipment that the organization has provided and approves.

13.5 Ports and protocols

GOLD version E/F:

The table below illustrates which ports and protocols GOLD version E/F uses. The table can be used as a reference during installation and firewall configuration.

Service	Direction	Port	Protocol	Destination address	Description
DHCP (Client)	Outgoing	68	UDP		DHCP
DHCP (Server)	Incoming	67	UDP		DHCP
SNTP	Outgoing	123	UDP		Clock synchronization
SSH	Incoming	22	TCP		Remote access
HTTP	Incoming	80*	TCP		Administration
HTTPS	Incoming	443	TCP		Administration
DNS	Outgoing	53	UDP		DNS
DNS	Outgoing	53	TCP		DNS
SMTP	Outgoing	25*	TCP		E-mail
SMTPS	Outgoing	465	TCP		E-mail
Rsync	Incoming	873	TCP		Hand-held terminal sync
Modbus	Incoming	502*	TCP		Master access
BACnet	Incoming	47808*	UDP		Master access
Exoline	Incoming	26486*	TCP		Master access

** Possibility for the user to select port number.*

SuperWISE II:

The table below illustrates which ports and protocols SuperWISE II uses. The table can be used as a reference during installation and firewall configuration.

Also see the documentation Project Planning Guide – Electricity & Control for more information.

Service	Direction	Port	Protocol	Destination address	Description
DHCP (Client)	Outgoing	68	UDP		DHCP
DHCP (Server)	Incoming	67	UDP		DHCP on Service port
NTP	Outgoing	123	UDP		Clock synchronization
SSH	Incoming	22	TCP		Remote access
HTTP	Incoming	80	TCP		Administration
HTTPS	Incoming	443	TCP		Administration
DNS	Outgoing	53	UDP		DNS
DNS	Outgoing	53	TCP		DNS
SMTP	Outgoing	25*	TCP		E-mail
SMTP	Outgoing	587	TCP		E-mail Swegon Connect
Rsync	Incoming	873	TCP		Hand-held terminal synchronization via Serviceport. Software upgrade via Operating network port.
Modbus	Incoming	502**	TCP		Master access
BACnet	Incoming	47808*	UDP		Master access
MQTT	Incoming	1883	TCP		Internal comms.
Swegon GOLD	Outgoing	10080	TCP		Internal comms.
Swegon	Incoming	12347	UDP		Internal comms.

** Possibility for the user to select port number.*
*** Possibility for the user to select port number only from software version 1.80 or later.*

GOLD Version C/D, Compact, SuperWISE I:

The table below illustrates which ports and protocols that GOLD version C/D, Compact and SuperWISE I use. The table can be used as a reference during installation and firewall configuration.

Service	Direction	Port	Protocol	Destination address	Description
DHCP (Client)	Outgoing	68	UDP		DHCP
DHCP (Server)	Incoming	67	UDP		DHCP
SSH	Incoming	22	TCP		Remote access
Winsock	Incoming	10001	TCP		Remote access
HTTP	Incoming	80*	TCP		Administration
DNS	Outgoing	53	UDP		DNS
DNS	Outgoing	53	TCP		DNS
SMTP	Outgoing	25*	TCP		E-mail
Modbus	Incoming	502*	TCP		Master access
BACnet	Incoming	47808*	UDP		Master access

** Possibility for the user to select port number.*

Firewall settings for Swegon Cloud

Swegon cloud solution is using Microsoft Azure services and certificates from Digicert to secure the connection. If the firewall in front of the products are allowing outbound traffic to internet it will work. If the firewall is set up to control outbound traffic the following ports and destinations must be allowed. If only filtering on ports, 443 and 8883 are used.

If your firewall allows wildcards in allow list, then recommendation is to use this. Otherwise add the specific URL:s in the parentheses in table below.

Domain (including sub domain)	Port	Protocol	Note
***.azure-devices-provisioning.net** (dps-SwegonCloud-common-we.azure-devices-provisioning.net global.azure-devices-provisioning.net)	443 8883	https mqtt	Azure Device Provisioning Service
***.azure-devices.net** (iot-SwegonCloud-prod-we.azure-devices.net)	443 8883	https mqtt	Azure IoT Hub
***.blob.core.windows.net** (stswciotfilestorageprod.blob.core.windows.net)	443	https	Azure storage
clientauth.one.digicert.com	443	https	Digicert Enrolment over Secure Transport (EST) for certificate enrolment and reenrolment

In the product

Make sure that the product have a valid certificate.

Make sure that the default gateway is set correctly to reach the internet.

A proper DNS server must be set up.

14. Security incidents

Reference: SS-ISO/IEC 27002:2014, section 16.1 Management of information security incidents and improvements.

14.1 Background

For quick and effective management of security incidents, there should be established procedures for how incidents are identified, reported and managed.

14.2 Recommendations

In the event security incidents can be attributed to a failure in Swegon's products, Swegon should be contacted immediately. Contact details are available at swegon.com.