Swegon

Sensitivity	Public
Owner	Head of Cybersecurity
Date	2026-11-18

Swegon Connected Products Security & Secure Deployment Guide

Information Security

2026-11-18 | Version 1.0



Table of Contents

1. Introduction 2
2. Built-in Protections & Deployment Assumptions 3
3. Deployment Models & Shared Responsibility 3
4. Planning 5
  4.1. Intended Operational Environment 5
  4.2. Network Architecture & Segmentation 6
  4.3. Documenting the Design 6
5. Commissioning 7
6. Operation & Maintenance 7
7. Responding & Decommissioning 8
8. Further Information 9
9. Appendix: Secure Deployment Checklist 10

1. Introduction

Connectivity has become central to how modern buildings are run. Connected Swegon products, including air handling units, controllers and the services around them, make it possible to monitor, configure, analyse and optimise indoor climate remotely and at scale. With that connectivity, cybersecurity becomes part of keeping a building running safely and reliably.

Security is built into Swegon's connected products from the design stage. This guide explains, in plain terms, how to deploy and operate connected Swegon products securely. It is deliberately product-agnostic: it describes principles and practices that apply across the connected portfolio.

It is one of three layers of the security documentation Swegon provides to customers:

- **Swegon Security & Trust Overview**: how Swegon approaches security as an organisation, its governance, secure development, vulnerability management, incident response and regulatory alignment**.**
- **Connected Products Security & Secure Deployment Guide** (this guide): how to deploy and operate connected Swegon products securely, across the portfolio.
- **Each product's own documentation**, including a dedicated Security & Trust Overview where published: the product specifics (security architecture, interfaces, defaults and version-specific behaviour) and assessment or certification evidence.

This guide tells you *what* to do and *why*; the product documents tell you *where* and *how*.

This guide is for:

- Building owners and operators assessing cyber risk in HVAC systems
- Procurement and compliance teams performing supplier security reviews
- System integrators and consultants designing or reviewing BMS architectures
- Installation and service personnel responsible for secure deployment and maintenance

> **Scope and limitations**: This guide does not replace a product's documentation (and Security & Trust Overview where published), Swegon security advisories, applicable contractual terms, or your own site-specific risk assessment. Where any of those differ from this guide for a specific product, they prevail.

2. Built-in Protections & Deployment Assumptions

Security is treated as a core quality attribute of connected Swegon products, addressed across the whole product lifecycle: secure by design, with secure defaults wherever interoperability with existing building systems allows, and protected through defence in depth.

For deployment, what matters is which protections are built in and which you provide. Depending on the product and its software version, the built-in protections typically include unique per-device credentials (or a credential change at commissioning) and role-based access separation; where a product connects to a Swegon cloud service, that connection is encrypted and mutually authenticated. Some products also expose automation and building-control interfaces that are intentionally left unauthenticated for interoperability and depend on a segmented network (see Section 4.1). The exact defaults for a given product are in its product documentation.

The Swegon Security & Trust Overview describes how Swegon works as an organisation: security governance, secure development, vulnerability management and coordinated disclosure, incident response, and alignment with standards and regulations. Of those, the EU Radio Equipment Directive (via EN 18031-1) and the Cyber Resilience Act apply to the products; NIS2 applies to Swegon as an organisation and to the supply-chain requirements our customers may need to meet.

3. Deployment Models & Shared Responsibility

Cybersecurity for connected HVAC systems is a shared responsibility, but the line between what Swegon secures and what the customer secures shifts with how the product is connected. The more of the connectivity Swegon provides, the more of the responsibility Swegon carries.

Broadly, connectivity follows one of two patterns, which may be combined:

- **Customer-provided connectivity**: The customer connects the product using their own network and, if needed, their own remote-access solution. This ranges from a well-segmented network through to, at worst, exposing an interface directly to the internet, which Swegon strongly advises against (see Section 4). The customer owns the network and any remote-access transport.
- **Swegon-managed connectivity**: Swegon offers a managed connectivity option, for example a pre-configured cellular gateway with an included data plan, that is essentially plug-and-play and connects the product to Swegon's cloud service over secured operator and backend links. The customer installs the device; the transport and the path to the cloud are managed by Swegon and its connectivity providers, with on-premises interfaces never directly exposed to the internet through that path. The two patterns are usually combined: a product that uses the managed gateway is normally also connected to the customer's building network for local control. The gateway then belongs in the customer's network design as a documented connection point (see Section 4.2), and the product documentation states whether the gateway can pass traffic between the operator link and the local network.

Where a Swegon cloud service is used, authorised users access the equipment (monitoring, control, visualisation) through that service, which authenticates the user and relays the connection; products are not exposed directly to the internet.

The matrix below shows, at a high level, who typically owns what under each pattern. Treat it as indicative; the authoritative split for a specific product or service is in its product documentation.

Responsibility	Customer-provided connectivity	Swegon-managed connectivity (+ cloud service)
Product & firmware security	Swegon	Swegon
Cloud platform & services	Not applicable	Swegon
Local device accounts	Customer	Customer
Cloud identity & access	Not applicable	Brokered by Swegon (RBAC/MFA where offered); customer assigns roles and decides on the use of MFA, which Swegon recommends for every account
Remote-access transport	Customer	Swegon
Connectivity link	Customer	Swegon (when the managed option is supplied)
Local network segmentation, firewalls	Customer	Customer
Physical security of equipment	Customer	Customer
Product/firmware updates: develop, verify and publish	Swegon	Swegon
Product/firmware updates: install	Customer	Customer, unless the product documentation states that the cloud service distributes them
Monitoring & incident response	Customer	Customer on site; Swegon monitors the cloud service and informs the customer of security events that affect it

Swegon's security assumptions and support guidance apply when products are deployed within their intended operational environment, as described below.

4. Planning

Good security starts before installation. The decisions in this section shape the security of everything that follows.

4.1. Intended Operational Environment

Connected Swegon products are designed for integration within Building Management Systems (BMS) that operate in controlled, professional environments, typically isolated from public networks and managed by facility operators with defined security practices. In this context, a product's security relies significantly on the protections enforced by its deployment environment.

Those protections are assumed to include:

Physical controls

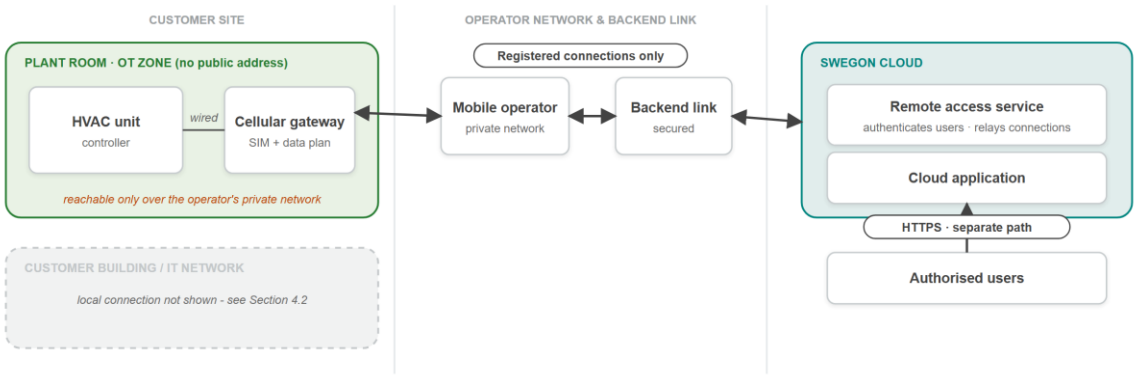
- Equipment installed in physically secure locations, controlled-access plant rooms, server rooms or maintenance areas.
- Physical access limited to authorised personnel (e.g. maintenance technicians, facility managers).

Logical controls

- Network segmentation separating critical infrastructure from general-purpose networks.
- Firewalls and network security devices deployed and managed by the building operator.
- Remote and internet-facing access restricted to essential, authorised services only.
- Network infrastructure maintained to current best practice.

Connected products rely on these environmental protections. Some products expose automation and building-control protocols that are intentionally provided without built-in authentication or encryption, for interoperability; where present, such interfaces are only safe within a restricted, segmented network. Network segmentation and the absence of direct internet exposure are therefore assumptions the product's security model depends on, not optional hardening. Which interfaces a given product exposes, and their defaults, are in its product documentation.

The Swegon-managed pattern looks like this:



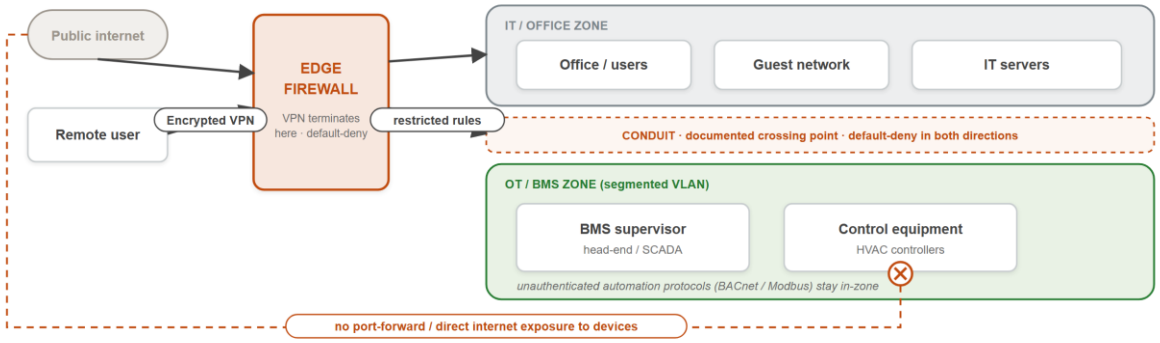
The pre-configured gateway is reachable only over the operator's private network, never from the public internet, and forwards connections only to the product interfaces registered

for it; authorised users reach the equipment only through the authenticated cloud service. The figure shows the cloud path only. Where the product is also connected to the local building network, that connection is designed as in Section 4.2.

4.2. Network Architecture & Segmentation

- **Place control equipment on a separate network**, segmented from office, guest and similar networks, for example a dedicated VLAN, a firewalled segment, or a separate physical/wireless network. This protects both the availability of the climate system and the confidentiality of other systems.
- **Think in zones and conduits**. Group equipment of similar criticality and trust into zones, and allow traffic between zones only through defined, documented connection points ("conduits"), initiating cross-zone connections from the more-trusted side where feasible. This is the zones-and-conduits concept from IEC 62443. A Swegon-managed gateway is one such conduit: document it in the network design like any other.
- **Keep equipment behind the organisation's firewall**, and restrict access to required interfaces by source, port and protocol.
- **Default-deny, in both directions**. Permit only the destinations, ports and protocols a device genuinely needs for normal and emergency operation, and block the rest by default. A product using a Swegon cloud service needs only specific outbound destinations; its product documentation lists them.
- **Do not expose control equipment directly to the public internet**. Where remote access is needed, use a Swegon cloud service that provides remote access, or another secured remote-access solution that avoids direct exposure (see Section 3), rather than forwarding a port to the device.

When you provide your own connectivity, a recommended layout looks like this:



Control equipment sits on a dedicated, segmented OT network reachable only through the firewall under restricted rules; remote access arrives over a VPN that terminates at the firewall, or at a jump host in a separate segment from which the OT network is reached; unauthenticated automation protocols stay within the OT segment.

4.3. Documenting the Design

- Document networks, components, connection points and the relationships between systems. Where a product can generate a commissioning record, use it as the reference configuration for later reviews and audits, and store it securely with the rest of your IT documentation.

5. Commissioning

When putting equipment into service:

- **Replace the initial credentials**. Follow the product's credential procedure and set your own strong values on every account the product is delivered with, before the device is connected to a shared network. Do the same after a factory reset, which may restore the delivered credentials.
- **Favour passphrases** over short, complex passwords: length and unpredictability matter more than special characters, and a passphrase of several unrelated words is both stronger and easier to remember.
- **Give every user a unique, personal account** where the product supports it, and require a password change at first login. Avoid shared accounts; the break-glass account below is the only accepted exception. Individual accounts limit credential exposure and, where supported, let changes be traced to a person.
- **Enable multi-factor authentication (MFA)** where the product or its cloud service supports it. Require it at least for privileged and remote access; MFA is the strongest single defence against stolen or guessed credentials.
- **Apply least privilege**: grant no more access than the role needs. The lowest access level is usually enough for monitoring or reading values; reserve privileged accounts for configuration.
- **Keep a break-glass account**: one emergency-only account, with credentials printed and stored securely, to avoid lock-out.
- **Enable encryption** where supported, TLS for the web interface (HTTPS) and for e-mail, and have everyone connect over HTTPS rather than plain HTTP; where the product allows it, disable or restrict plain HTTP once HTTPS is verified. Where both the product and its peer support a secured protocol variant (e.g. HTTPS, OPC UA over TLS, Modbus/TCP Security, BACnet/SC), prefer it to the plaintext version.
- **Disable services and protocols you do not use**, and confirm only required interfaces are reachable.
- **Disable wireless you do not use**. Turn off Wi-Fi access points, Bluetooth or other radios that are not required; where wireless is needed, protect it with a strong passphrase (WPA2 or later).
- **Lock down unused physical ports**. Block or seal USB and service ports that are reachable without opening the unit and are not needed for operation; ports enclosed within the product's casing are covered by the physical controls in Section 4.1.
- **Take a configuration backup** once the device is commissioned.
- **Record who is responsible.** At handover, write down who manages the equipment and its accounts from then on, and how it is reached remotely, and keep this with the commissioning record.

6. Operation & Maintenance

Connected products require little routine maintenance, so security maintenance must be scheduled explicitly to avoid devices being "forgotten." As a baseline, have authorised personnel review each device at least once a year, and confirm that the person recorded as responsible still is.

- **Keep software up to date**. Run the latest supported version; updates can add features, improve usability and close security gaps. Apply them promptly, via the

management interface or memory card depending on the product. Contact the Swegon company or partner you bought the product from if you need help; Swegon's offices and distributors are listed at swegon.com/contact.

- **Maintain backups**. Back up information and configuration after commissioning and before any significant change; store backups securely and test that they restore.
- **Manage change**. Plan, test, approve and document changes before applying them; take a configuration backup first so you can roll back, and verify intended function afterwards.
- **Log and monitor**. Enable logging where available and, where supported, export logs to a central facility using a dedicated least-privilege account. Where a product only offers an unencrypted export protocol, keep the export path inside the control segment. Enable automatic time synchronisation (NTP/SNTP) so events and alarms carry accurate timestamps.
- **Review access**. Remove stale or unused accounts and re-confirm role assignments.
- **Control removable media**. Treat USB sticks and memory cards brought to the equipment as a risk path: use them only when needed (for example firmware updates), with known-clean, pre-scanned media, and keep unused ports blocked. Storage media that are part of the product, such as a memory card holding its configuration and logs, stay in place and are protected by the physical security of the installation.
- **Govern third-party remote access**. When integrators or service partners need access, make it time-bound and individually credentialed, log it, and avoid standing back-channels into the control network that you have not approved and documented (such as a vendor's own modem or VPN). A Swegon-managed gateway is not such a back-channel when it is documented as a conduit in your network design and is reachable only over the operator's private network, forwarding only the connections registered for it (see Section 3).

7. Responding & Decommissioning

Swegon operates a documented incident response capability and continuously monitors for vulnerabilities. Where a security incident or an actively exploited vulnerability could affect customers, Swegon promptly informs the affected users it can identify directly, and all users through the channels in which its security advisories are published, tells them what measures they can take, and makes any required regulatory notifications. Swegon's security advisories, incident response, vulnerability management and coordinated disclosure are described in the Swegon Security & Trust Overview.

Suspected incidents. Isolate affected equipment if necessary, preserve logs, and contact Swegon at security@swegon.com.

Vulnerabilities. If you discover a security vulnerability in a Swegon product or service, report it through the Swegon Vulnerability Disclosure Policy (swegon.com/security/vulnerability-disclosure-policy).

Decommissioning. When equipment is retired, perform a factory reset and remove any memory card or USB storage; check the product documentation for what a reset keeps (on some products certificates, logs and configuration backups), unenrol it from any connected or remote-access service, revoke any device certificates issued to it, cancel the data subscription of a managed gateway, and dispose of it securely.

8. Further Information

Swegon's security documentation is available from the Swegon security pages (swegon.com/security): the Swegon Security & Trust Overview, this guide, and the published product Security & Trust Overviews and security requirements.

- Swegon's organisation-level security: the Swegon Security & Trust Overview (governance, secure development, vulnerability management, incident response, standards and regulatory alignment).
- Product- and service-specific security documentation: each connected product's and service's documentation, including a Security & Trust Overview where published (interfaces, port tables, defaults, version-specific behaviour, assessment or certification evidence).
- Detailed security inquiries or requests for additional documentation: contact your Swegon sales representative, or Swegon at swegon.com/contact; the request is passed to Swegon's cybersecurity function and the product team.

9. Appendix: Secure Deployment Checklist

A printable, tear-off summary of the measures explained in the sections above. Use it at handover and at each periodic review.

Commissioning

- ☐ Initial credentials replaced with strong passphrases (unique per device or changed during commissioning, per product)
- ☐ Unique personal accounts; least privilege applied; break-glass credentials stored securely
- ☐ MFA enabled where supported (privileged/remote access)
- ☐ HTTPS/TLS enabled and plain HTTP disabled or restricted where supported; unused services, protocols, wireless and ports disabled
- ☐ Remote access provided through a secured service only, with no direct internet exposure
- ☐ Commissioning record and configuration backup stored securely
- ☐ Responsible person and remote-access route recorded

Periodic maintenance

- ☐ Latest supported software; advisories reviewed and acted on
- ☐ Backups kept current, secured and tested
- ☐ Stale accounts removed; roles re-confirmed
- ☐ Removable media controlled
- ☐ Third-party remote access time-bound and logged
- ☐ Configuration checked against the commissioning record
- ☐ Changes documented

Decommissioning

- ☐ Factory reset performed; memory card and USB storage removed
- ☐ Equipment unenrolled from connected/remote services; certificates revoked and gateway subscription cancelled
- ☐ Equipment disposed of securely