Secure operation guidelines

Getinge Connect Control Center and applications

1 About the guidelines

The secure operation guidelines describe how to securely operate Getinge Connect Control Center and its applications in a healthcare organization. The guidelines are intended for personnel within information system security. This includes the roles:

- IT managers
- IT security managers
- Personnel that install and maintain Getinge Connect Control Center and its applications.

In these guidelines, Getinge Connect Control Center and its applications are referred to as *the system*.

2 Secure operation guidelines

To ensure that the system operates securely, do as follows:

- Host the system on a dedicated physical server with restricted physical access control. Do not host other services on the same server.
- Make sure that hardware, firmware, and the operating system that the system is installed on is kept up to date.
- Harden the operating system that the system is installed on according to security configuration benchmarks. For example, according to the Center for Internet Security (CIS) or the Defence Information Systems Agency (DISA) benchmarks.
- Disable root access on the operating system that the system is installed on.
- Install software for intrusion detection and prevention on the virtual machine that the system is installed on.
- Monitor network traffic and host activity to detect and remediate malevolent activities.
- Make sure that devices and web browsers used to access the system are kept up to date and that their configuration is managed.
- Encrypt data at rest, including when it is backed up. Control Center will encrypt all its data in transit.

3 System overview

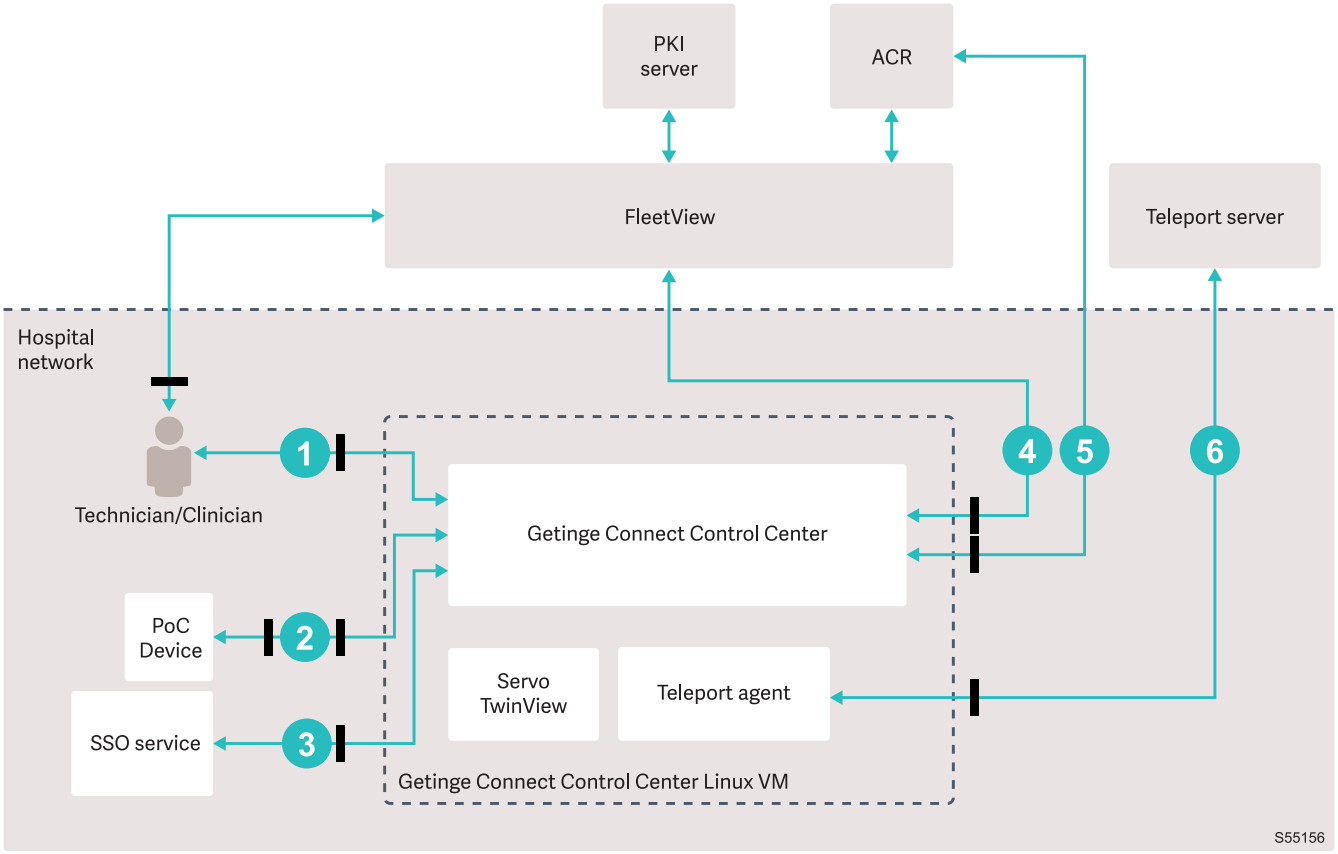
3.1 Product description

Getinge Connect Control Center runs on a local server set up by responsible IT personnel at the healthcare organization. The server provides a runtime environment and common services for applications such as Servo TwinView. Point-of-care (PoC) devices connect and transfer data to Getinge Connect Control Center through the hospital network. The data is used by applications or FleetView services.

Servo TwinView is a web-based application that subscribes to clinical and location data from Servo ventilator systems. The data is used to show twins of the user interfaces of connected ventilator systems in near real-time.

FleetView is a web-based service that supports device maintenance. In FleetView, PoC device logs and usage data is shown. FleetView also gives access to a public key infrastructure (PKI) server for certificate administration. From Getinge Connect Control Center v1.2 and higher, it is possible to opt-out of data transfer to FleetView.

Teleport is an opt-in feature to support remote access. Teleport is not required but highly recommended and needs to be permitted by the user.



ID	Product interface	Network interface type	Internet layer	Transported or accessible assets (intrahospital unless indicated)
1	Web browser	Ethernet	WebSocket Secure/ HTTPS:443	Getinge Connect Control Center: Service and maintenance interface. Servo TwinView: Clinical and location data.
2	PoC device	Ethernet	MQTT/TLS:8883	PoC device onboarding, data transfer from PoC device, and over-the-air (OTA) software updates when applicable.

ID	Product interface	Network interface type	Internet layer	Transported or accessible assets (intrahospital unless indicated)
3	Single sign-on (SSO) service	Ethernet	Configured by the healthcare organization	SSO integration to the healthcare organization´s SAML IdP.
4	FleetView	Ethernet	MQTT/TLS:443	PoC device onboarding, equipment data, and user account information.
			HTTP/TLS:443	License token to establish MQTT connection.
				System metrics (data about the resources of the virtual machine)
5	Azure Container Registry (ACR)	Ethernet	HTTPS:443	Software installation or update. Application chart and images are pulled from the cloud registry.
6	Teleport	Ethernet	TLS:443	Remote assistance access to Getinge Connect Control Center from Getinge. Teleport connects to a Getinge server to enable remote access to Getinge Connect Control Center. Data transported is any data within Getinge Connect Control Center.

3.2 Security measures

To protect critical functionality, the system includes the security measures:

- All connections to the system are encrypted. See the figure and table in *3.1 Product description* on page 2.
- Connections to PoC devices and FleetView are authenticated through certificates. All certificates are signed through certificate signing requests (CSRs) to the Getinge PKI server.
- The admin account is protected by a limit on the number of sign-in attempts.
- System security settings cannot be configured.
- Role based access to system functionality connects to the healthcare personnel Active Directory (AD) through Security Assertion Markup Language (SAML) integration.
- Authenticity and integrity of software installations and updates are ensured through cryptographic signing of software packages.
- Remote assistance is done through a Teleport connection. No access to the system from Getinge is possible without local administrator activation of the connection.
- There is no failsafe mode for the system. Failsafe mode is N/A.

3.3 Security controls

Threats and risks addressed by the system can be controlled by the use environment to mitigate the vulnerability.

Risks	Expected controls in the use environment
The intended use environment is not safe and system isolation from the network is required.	The system is dependent of the firewall, make sure the firewall is OK.
Eavesdropping of network traffic, with the intention to access patient data.	The Linux VM and the web browser is up-to-date.
Phishing emails designed to exploit the permissions of legitimate users to interact with the system.	The Linux VM and the web browser is up-to-date.

3.4 Strategy to mitigate known security risks

The strategy to mitigate known security risks, including risks derived from required software is:

- High degree of internal segmentation to isolate the parts of Getinge Connect Control Center and reduce vulnerability.
- Regularly apply patches and updates to reduce the amount of vulnerable third-party components.
- Modern software stack that supports current standards.
- Meet the quality of the healthcare organization´s security standards.
- Reduce personal and software privileges to mitigate the vulnerability of the system.
- Use detailed technical logs, including security logs.
- Use the industry standard protocols and key management techniques to protect the confidentiality, integrity and authenticity of all data while in transit.

The strategy is the base for the actions described in section *2 Secure operation guidelines* on page 1.

3.5 Secure network deployment and servicing

To permit secure network deployment and servicing if a suspected attack or a severe vulnerability is discovered in the system, the system can be temporarily disabled without affecting the clinical functionality of the connected PoC devices.

The system does not have a safe state. However, if recommended by Getinge, the system can be uninstalled and then reinstalled again. See the Getinge Connect Control Center installation instructions, section Reinstall Getinge Connect Control Center.

3.6 SBOM

A digital SBOM can be received upon request. Contact your local Getinge support or use the form:

https://www.getinge.com/int/contact/other/documentation

3.7 Expected security controls

The expected security controls to be provided by the intended use environment is gathered and described in the section *2 Secure operation guidelines* on page 1.

3.8 System security responsibility

To ensure the security of the system and the system environment make sure to follow the recommended guidelines, see section *2 Secure operation guidelines* on page 1. The healthcare organization is responsible for the security of their systems and regular maintenance is expected to be performed.

The responsibility of the software is categorized as follows:

- Maintained software, software item for which Getinge will assume the risk related to security.
- Supported software, software item for which Getinge will notify the healthcare organization regarding known risks related to security.
- Required software, software item for which Getinge will consider security-related risks known before release of the software.

Software item	Category
Getinge Connect Control Center	Maintained software
Kubernetes	Maintained software
Teleport	Supported software
The operating system	Required software
The server	Required software

The healthcare organization needs to consider if the patient is to be informed about collection of information to fulfill the general data protection regulation (GDPR), the health insurance portability and accountability act (HIPAA), or similar national regulations on data privacy.

3.9 Security information and incident reports

Create a complaint or contact a service representative for any type of issues. Security incidents can also be reported back to Getinge via the form at Getinge Security Webpage, see https://www.getinge.com/int/security/.

3.10 Residual risks to security

The system collects data about system use and treatment. This data can be seen as indirectly identifiable personal information because it is related to a device ID timestamp. Data can also be related to a location, if set by the user. The occurrence of a residual risk can cause such data to be compromised.

The remaining residual risks to security can require user actions to be prevented.

RESIDUAL RISK	REQUIRED USER ACTION
Software runs with root privileges.	Make sure to operate Getinge Connect Control Center on a secure, dedicated server and monitor its activity, see *2 Secure operation guidelines* on page 1.
Security logs are not collected or analyzed centrally by Getinge.	Make sure to monitor the logs, see *2 Secure operation guidelines* on page 1.
During remote support sessions there is an increased attack surface.	Utilize the Teleport session recording, contact your local Getinge support.
Although the admin account is protected, the account can still increase the risk of cyberattacks.	Make sure to create a strong password.

4 Use environment

The intended use environment is in professional healthcare facilities used by healthcare providers. The system can be accessed anywhere on the healthcare organization's network.

Installation and use of the system outside of its intended use environment increases risk of:

- Physical- and network-based attacks.
- Exposure of potentially sensitive information.
- Downtime of the system and delayed information to applications. This is not considered to lead to increased risk of patient harm.

4.1 Cybersecurity standards

The recommended cybersecurity standard for the use environment is the IEC 80001 series.

4.2 Supporting infrastructure

For a description of the requirements on the supporting infrastructure and the recommended use environment, see the Getinge Connect Control Center installation instructions, section Install Getinge Connect Control Center.

For supported connected devices, supported web browsers, requirements on the Getinge Connect Control Center operating system and requirements on the network connection, see the Getinge Connect Control Center user's manual, section Technical data.

5 Development process rigor

Getinge's development process rigor holds valid certifications in alignment with various security standards and ensures that all products are developed in compliance with these standards. The system and its related processes are not classified as a medical device, which limits the applicability of the regular standards. However, the system and its related processes are developed in alignment with the standards ISO 13485, IEC 62304 and IEC 81001-5-1.

Getinge Connect Control Center provides its applications with security functionality to avoid duplication of commonly needed functions. The risk analysis of the functions is done in the Getinge Connect Control Center context. When several possible classifications for an asset are identified, the risk analysis focuses on the worst-case impact. For functions needed by the applications but not provided by Getinge Connect Control Center, the function must be analyzed in the risk analysis for the application.

Getinge Connect Control Center assets are analyzed according to the Getinge Connect Control Center attack tree. The simplified attack tree is designed to analyze possible attack vectors that reach and affect the listed assets. For this analysis the assets considered relevant are:

- Transmitted data (high-level)
  - Control center system (secondary)
  - Kubernetes (secondary)
  - Cryptographic keys and passwords (secondary)
  - Install image (secondary)

6 Security configurations

The recommended configuration of the system entails a high security standard. If the configuration is done differently, it affects the security. For the specific configuration options and instructions, see the Getinge Connect Control Center installation instructions, section Install Getinge Connect Control Center.

Teleport allows remote assistance by granting temporary access to the healthcare organization's server, where the Getinge Connect Control Center is hosted. This access presents a risk, see section *3.10 Residual risks to security* on page 5. However, the benefit is faster and more accurate support, as it provides a clear overview and enables direct inspection of the server, rather than relying solely on customer-provided information.

SSO uses one identity to access multiple services, which benefits administration by centralizing access management. However, if you are locked out of the account or the identity provider fails, you lose access to all services.

The use of SSO provides:

- Identity and resource management from a single place.
- Standard protocol for secure access exchange.
- Reduced vulnerability caused by weak passwords because one strong password is used for all services.

6.1 Account management guidelines

The accounts managed by the system are:

- Technician role
- Clinician role

Users that are signed in with technician accounts can configure and install applications. The technician role is also used by the default admin account, the admin account is only intended for installation, troubleshooting or if the SSO Service is unavailable. Users signed in with clinician accounts can only see and open already installed applications.

There are no special training requirements for users of the system.

7 Security hardening guidelines

7.1 System defence-in-depth strategy

The security hardening guidelines include the system defense-in-depth strategy. The system defense-in-depth strategy is based on the same values as the strategy to mitigate known security risks, see section *3.4 Strategy to mitigate known security risks* on page 4. To implement the system defense-in-depth strategy, a clear division of responsibility between Getinge and the healthcare organization is required. Getinge is responsible to apply actions included in the strategy to mitigate known security risks as part of the defense-in-depth strategy. To fulfill the defense-in-depth strategy, the healthcare organization is responsible for:

- Physical access control to the healthcare organization.
- Physical access control to the server and network infrastructure.
- Digital access control of clients.
- Servers and network infrastructure.
- Update management and configuration management.
- Cybersecurity training for all staff with additional focus on IT staff.
- Client usage restrictions to limit the amount of phishing and malicious installed software.
- Encryption of all sensitive data, including patient information, while stored on servers and on backup storage media.

7.2 Security options and capabilities

To set the default values or to change values to see how changes affect the system's security defense-in-depth strategy, see the Getinge Connect Control Center installation instruction, section Install Getinge Connect Control Center.

7.3 Security related tools

Security related tools are used to monitor clients, servers, network infrastructure and physical access control systems. The security related tools recommended are:

- Intrusion detection prevention system
- SSO
- Teleport
- System monitoring.

7.4 Periodic security maintenance activities

The recommended periodic security maintenance activities are:

- Continuous updates of the software and hardware systems.
- Requested updates of system and the system environment.
- Periodic incident response, including testing the ability to recover the system from encrypted backups.
- User training.
- Review of physical and digital user privileges.

7.5 Security best-practices

The recommended security best-practices for the system are to follow the guidelines in section *2 Secure operation guidelines* on page 1 and to update and apply patches when identified as needed.

8 Security forensics

The security forensics include the capture of forensic evidence and is done through log files.

The log files can be collected in a list or viewed in System insights. To create the log file, see the Getinge Connect Control Center user's manual section Collect Getinge Connect Control Center and to view the log files in System insights, see the Getinge Connect Control Center user's manual, section Use system insights.

If the functionality System monitoring is enabled, it provides logs that can be used to troubleshoot the system. See the Getinge Connect Control Center user's manual, section System monitoring.

9 Backup and restore system and configuration

The system does not continuously store data that needs to be restored as part of a system recovery. However, to facilitate restoration of correct system function if there is a system failure, back-ups are recommended when changes are made in configuration and device location lists. Encrypt backups to protect patient information that are stored temporarily.

10 Anomaly response

The system includes multiple mechanisms to detect potential malicious activity and measures to prevent successful attacks. The local account login is rate-limited, which significantly reduces the risk of brute force password guessing. Device onboarding monitors any attempts to reuse the same factory certificate, reducing the risk of malicious actors to gain trust within the system by certificate reuse. The application management system ensures that only one management action (install, start, stop, upgrade) can run at a time for each application. Additionally, all APIs in the Getinge Connect Control Center have rate limits, making it much harder to carry out a denial of service attack. As an additional security measure, the healthcare organization is recommended to implement best practices to monitor the Getinge Connect Control Center Linux VM.

The system does not give notifications to the user in the event of anomalous conditions.

11 Patchability

Patches to applications are available to download in the Apps & Services page in Getinge Connect Control Center when users are signed in with a technician account. The customer is notified of any patches and updates to Getinge Connect Control Center directly by Getinge via email.

The distribution of Getinge Connect Control Center patches and updates is a manual process. The process requires the tool Secure Managed File Transfer Service (SMFTS) which is hosted by Getinge. For instructions of the process, see the Getinge Connect Control Center installation instruction, section Reinstall Getinge Connect Control Center.

It is important to apply available patches as recommended, to prevent risks with potential impact to safety. One such risk is loss of communication with the PoC devices, which prevents PoC information from showing in Servo TwinView. This requires staff to be physically present with the patients and directly use the screens provided by the PoC devices. In other respects, the system does not affect patient safety, whether during normal operation, in case of failure, or in the event of a cyberattack.

12 Decommission

The process to safely decommission the system regarding cybersecurity is:

1. Uninstall the system, see the Getinge Connect Control Center installation instructions, section Uninstall Getinge Connect Control Center.
2. Remove patient and configuration data.
3. Encrypt the hard drive and remove the virtual machine according to general procedures.

Removal of patient and configuration data is mostly included in the uninstallation process. However, if Teleport was enabled, manually remove the file `/etc/teleport.yaml`.

Disposal of confidential data does not apply to the system because it does not store collected data. Directly personally identifiable information, for example patient names and identification numbers, is not collected by the system.

Glossary

Term	Description
GDPR	General data protection regulation. An EU law with rules for how personal data must be used in an integrity friendly way. Personal data is any information that could identify a living person.
HIPAA	Health insurance portability and accountability act. A federal law with rules to protect medical records and other personal health information.
PoC	Point-of-care. Medical diagnostic at the point of care and not in a laboratory environment.

Manufacturer:
Maquet Critical Care AB · Röntgenvägen 2 · 171 54 Solna · Sweden
www.getinge.com