

GETINGE *
**Connect
Control
Center**



GETINGE Connect Control Center Instructions

[Home](#) » [GETInGE](#) » GETINGE Connect Control Center Instructions 

Contents

- [1 GETINGE Connect Control Center](#)
- [2 Product Usage Instructions](#)
- [3 Install a virtual machine](#)
- [4 Configure the network](#)
- [5 Install Getinge Connect Control Center](#)
- [6 Documents / Resources](#)
 - [6.1 References](#)
- [7 Related Posts](#)

GETINGE *

GETINGE Connect Control Center



Specifications:

- Operating Systems: Ubuntu 20.04 LTS, 22.04 LTS, Red Hat Enterprise Linux (RHEL) 8, 9
- Minimum Requirements for Virtual Machine:
 - 8 vCPUs
 - 16 GB of RAM
 - 80 GB of disk storage
 - 1 Gbit/s network bandwidth

Product Usage Instructions

Installation Instructions:

Install a Virtual Machine:

Getinge Connect Control Center is installed on a Linux virtual machine. Follow these steps:

1. Install a hypervisor like VMware ESXi or Microsoft Hyper-V on a server connected to the hospital network.
2. Install one of the recommended virtual machines:
 - Ubuntu 20.04 LTS or 22.04 LTS
 - Red Hat Enterprise Linux (RHEL) 8 or 9

Configure the Network:

Configure network settings for communication with Device and Data Manager and other services:

1. Ensure port 443 is open for outbound TCP traffic.
2. Open ports 443 and 8883 for hospital network traffic.

Install Getinge Connect Control Center:

Follow these steps to install Getinge Connect Control Center:

1. Install Teleport:

1. Visit the Teleport installation page and follow the instructions for DEB or RHEL package installation.

2. Install Getinge Connect Control Center:

1. Debian-based OS:

1. Add a user named g3c on the virtual machine.
2. Install the DEB package using 'sudo apt install g3c-.deb'.
3. Access the setup wizard through a web browser using the VM's IP address.
4. Follow the setup wizard instructions.

2. RHEL-based OS:

1. Add a user named g3c on the virtual machine.
2. Install the k3s-selinux RPM package using appropriate methods.

FAQ:

How long does it take to install Getinge Connect Control Center?

The installation process typically takes around five minutes to complete.

What should I do if I encounter error 503 during setup?

If you encounter error 503, wait for a few minutes as it may take up to ten minutes for the system to start on low resource machines.

Install a virtual machine

Getinge Connect Control Center is installed on a Linux virtual machine managed by the responsible organization. Installation packages for Getinge Connect Control Center are available for APT and RPM package management systems.

1. If necessary, install a hypervisor on a server connected to the hospital network. VMware ESXi or Microsoft Hyper-V is recommended.

2. Install one of the following virtual machines on the hypervisor:

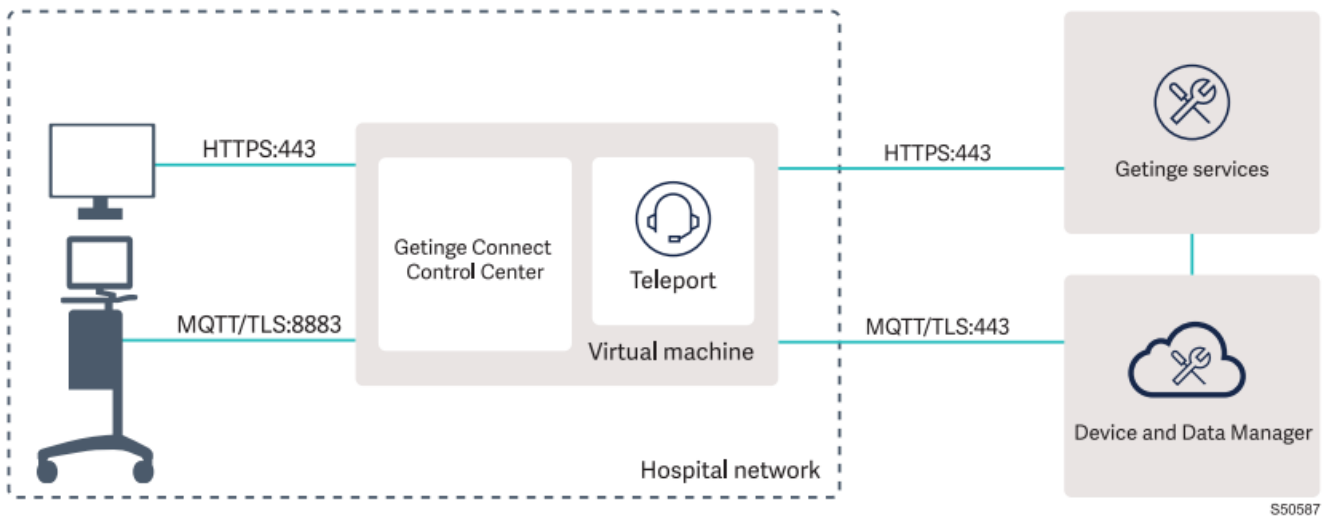
- Ubuntu 20.04 LTS or 22.04 LTS
- Red Hat Enterprise Linux (RHEL) 8 or 9

Minimum requirements for the virtual machine:

- 8 vCPUs
- 16 GB of RAM
- 80 GB of disk storage
- 1 Gbit/s network bandwidth

Configure the network

Getinge Connect Control Center communicates with Device and Data Manager (DDM) and other Getinge services. DDM is a cloud service used for onboarding of devices, session control, and data filtering. Getinge services includes the Getinge package repository and Teleport remote assistance.



1. Make sure that port 443 is open for outbound TCP traffic. Port 443 is used for MQTT over HTTPS to DDM, for download of data from Azure service endpoints, and for traffic to support-act.getinge.com for Teleport remote assistance.
2. Make sure that the following ports are open for traffic on the hospital network:
 - Port 443. Used for front-end access by clinicians, biomed, and service technicians.
 - Port 8883. Used for connections by devices and connectivity nodes.

Install Getinge Connect Control Center

Install Teleport

Teleport is used for remote assistance in Getinge Connect Control Center.

1. Go to <https://goteleport.com/docs/installation/#linux>.
2. Follow instructions for installation of the DEB or RHEL package. The Teleport service is disabled by default.

Install Getinge Connect Control Center on a virtual machine

- Select the applicable procedure:
 - 3.2.1 Install Getinge Connect Control Center on a Debian-based operating system on page 2.
 - 3.2.2 Install Getinge Connect Control Center on a RHEL-based operating system on page 3.

Install Getinge Connect Control Center on a Debian-based operating system

1. Add a user named g3c on the virtual machine. It is not necessary to give the user root access.
2. Install the Getinge Connect Control Center DEB package from Getinge: `sudo apt install g3c-<version>.deb`
3. Wait for approximately five minutes for the installation to complete.

The Getinge Connect Control Center setup wizard can be accessed through a web browser.

4. Copy the IP address of the virtual machine.
5. Enter the IP address in a web browser.

The setup wizard opens in the web browser.

NOTE:

If the web application returns error 503, wait for some minutes. It can take up to ten minutes for Getinge

Connect Control

Center to start on a system with low CPU and memory resources.

6. Sign in with admin as username and admin as password. The password is changed in the setup wizard.
7. Follow the instructions in the setup wizard. During the setup wizard, enter a license token from Getinge and see 3.2.3 Get an SSL/TLS certificate on page 4 and 3.2.5 Set up the hospital domain on page 4.
8. Do a backup of Getinge Connect Control Center according to hospital routines.

Install Getinge Connect Control Center on a RHEL-based operating system

1. Add a user named g3c on the virtual machine. It is not necessary to give the user root access.
2. Install the k3s-selinux RPM package with one of the following methods:
 - Download the latest version from <https://github.com/k3s-io/k3s-selinux>.
 - Create a YUM repository file named /etc/yum.repos.d/rancher-k3s-common.repo and add the following content, where <version> is the version of RHEL:
[k3s-selinux] name=K3S-SELinux
baseurl=<https://rpm.rancher.io/k3s/stable/common/centos/<version>/noarch>
enabled=1
gpgcheck=1
gpgkey=<https://rpm.rancher.io/public.key>

3. Install the latest k3s-selinux and container-selinux packages: `sudo dnf install container-selinux k3s-selinux`

4. Install the Getinge Connect Control Center RPM package from Getinge: `sudo dnf localinstall g3c-<version>.rpm`

5. Wait for approximately five minutes for the installation to complete.

The Getinge Connect Control Center setup wizard can be accessed through a web browser.

6. Copy the IP address of the virtual machine.

7. Enter the IP address in a web browser.

The setup wizard opens in the web browser.

NOTE:

If the web application returns error 503, wait for some minutes. It can take up to ten minutes for Getinge Connect Control

Center to start on a system with low CPU and memory resources.

8. Sign in with admin as username and admin as password. The password is changed in the setup wizard.
9. Follow the instructions in the setup wizard. During the setup wizard, enter a license token from Getinge and see 3.2.3 Get an SSL/TLS certificate on page 4 and 3.2.5 Set up the hospital domain on page 4.
10. Do a backup of Getinge Connect Control Center according to hospital routines.

Get an SSL/TLS certificate

1. Get an SSL certificate for the chosen domain. Depending on the organization policy, it can be a certificate signed by an internal certificate authority (CA) or from an external CA.

For evaluation purposes, a free certificate from Let's Encrypt with DNS-01 challenge can be used, see

<https://letsencrypt.org/docs/challenge-types/#dns-01-challenge>.

2. Make sure that the certificate contains PEM-encoded CERTIFICATE and PRIVATE KEY blocks and has a .pem or .crt suffix.

3. If the blocks are in different files, add the blocks to the same file.

Example of .pem file:

—BEGIN CERTIFICATE—

<certificate>

—END CERTIFICATE—

—BEGIN RSA PRIVATE KEY—

<certificate private key>

—END RSA PRIVATE KEY—

4. Upload the certificate to Getinge Connect Control Center in the setup wizard. Getinge Connect Control Center does not support alternative certificate installation methods.

Allow proxy interception

If a proxy intercepts Getinge Connect Control Center traffic, there can be communication problems with the security assertion markup language (SAML) provider and the Getinge public key infrastructure (PKI) server.

To allow proxy interception, CA variables can be configured. The variables are only read at installation and upgrade of Getinge Connect Control Center and can be set to the path of the same file.

1. Edit /etc/default/g3c on the virtual machine.
2. If applicable, set SAML_CA to the path of the file that contains the PEM-encoded CA chain of the proxy that is between
Getinge Connect Control Center and the SAML provider.
3. If applicable, set MITM_CA to the path of the file that contains the PEM-encoded CA chain of the proxy that is between
Getinge Connect Control Center and the Getinge PKI server.

Set up the hospital domain

1. Get the IP address of the virtual machine.
2. Create a DNS A resource record that points the hospital domain to the IP address. The domain name is selected in the setup wizard.

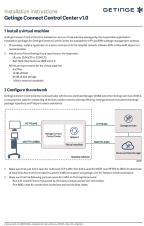
Uninstall Getinge Connect Control Center

- Select the applicable procedure:
 - Uninstall Getinge Connect Control Center from a Debian-based operating system: `sudo apt purge g3c`
 - Uninstall Getinge Connect Control Center from a RHEL-based operating system: `sudo dnf remove g3c`

Uninstall Teleport

- Select the applicable procedure:
 - Uninstall Teleport from a Debian-based operating system: `sudo apt purge teleport`
 - Uninstall Teleport from a RHEL-based operating system: `sudo dnf remove teleport`

Documents / Resources

	<p>GETINGE Connect Control Center [pdf] Instructions Connect Control Center, Control Center, Center</p>
---	---

References

- [🔑 Challenge Types - Let's Encrypt](#)
- [✳️ Welcome to Getinge](#)
- [🐙 GitHub - k3s-io/k3s-selinux: SELinux policy for k3s](#)
- [⚙️ Installing Teleport | Teleport Docs](#)
- [🔑 Challenge Types - Let's Encrypt](#)
- [🌐 rpm.rancher.io/public.key](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.