Brainlab Connected Care

Technical information

Table of Contents

Brainlab solutions are designed for maximum utility. Seamless connectivity of the technology and everyone involved is a key prerequisite in ensuring systems are used to their full potential.

Brainlab Connected Care is a comprehensive IoT solution that digitally connects you, your Brainlab equipment and our Brainlab Service & Support experts. Specially designed for perfect integration into your hospital IT infrastructure, Brainlab Connected Care can be implemented in less than ten minutes and requires no IT maintenance effort.

As a key component of every Brainlab solution, Brainlab Connected Care enables the delivery of unsurpassed service in a fast, efficient and cost-effective way. Let's get connected to ensure that you get the most out of your Brainlab systems!

Brainlab Connected Care at a glance
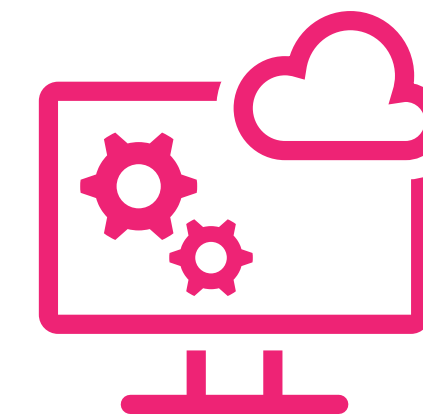
Services

Virtual Assistance

The person in need of support while using a Brainlab device can contact Brainlab Service & Support and initiate a screen sharing session. Once the end-to-end connection is established with certificate-based authentication, the Brainlab service engineer will provide you with remote, real-time support. The session details are documented both on the device and in the Brainlab infrastructure to ensure full transparency.

Only authorized Brainlab experts, based on a comprehensive authorization model, are allowed to provide virtual assistance over Brainlab Connected Care.

System monitoring

Your Brainlab devices will send technical and statistical information to help us effectively detect and quickly respond to any performance anomalies.

Software installation and updates

Brainlab can remotely install and configure software using Brainlab Connected Care based on your license agreement. At your convenience, the Brainlab service engineer will plan when the update will take place in advance to guarantee minimum downtime.
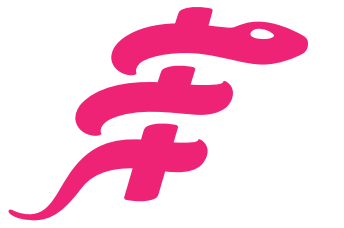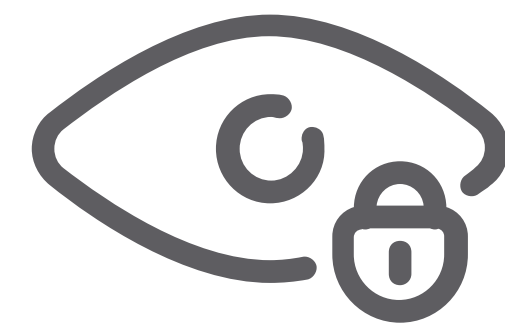
How we support you

Brainlab Connected Care at a glance

Key features

Security

You'll receive a high level of security for user authentication, data transfer and data storage. Secured communication uses encryption TLS 1.2 as default (256-bit AES encryption). Communication is outbound only.

Privacy

We ensure compliance with relevant industry standards and regulations, such as GDPR and HIPAA. Brainlab operates an ISO/IE 27001:2013 certified Information Security Management System (ISMS) that conforms to the requirements that preserve the confidentiality and privacy of patient and customer data.
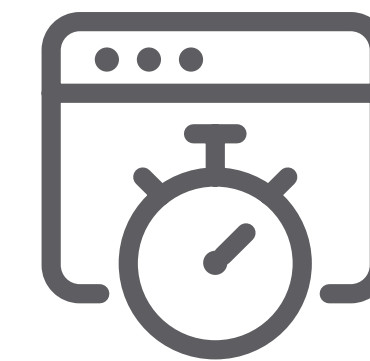
Effortless and adaptable setup

Installation takes just a few minutes and can be customized to your needs, ensuring minimum disruption to your IT and security infrastructure while guaranteeing transparency.
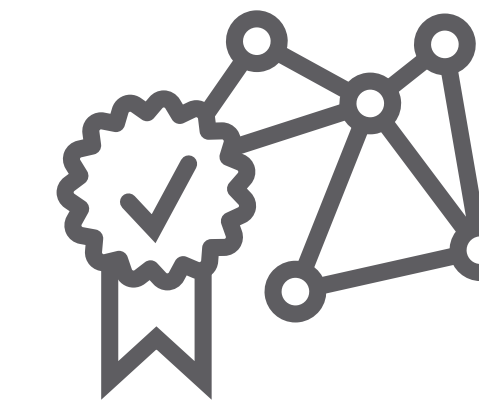
Proven Technology

As with many leading manufacturers, Brainlab uses PTC ThingWorx hosted in Microsoft Azure cloud infrastructure. PTC ThingWorx is certified and audited according to international standards (e.g. ISO 27001, HIPAA, FedRAMP, SSAE16 SOC2 Type II Attestation Report).

Information Security Management
ISO 27001 Certified

Multi-factor authentication

FR FedRAMP

HIPAA COMPLIANT

AICPA SOC **SOC 2 TYPE II** CERTIFIED

System architecture

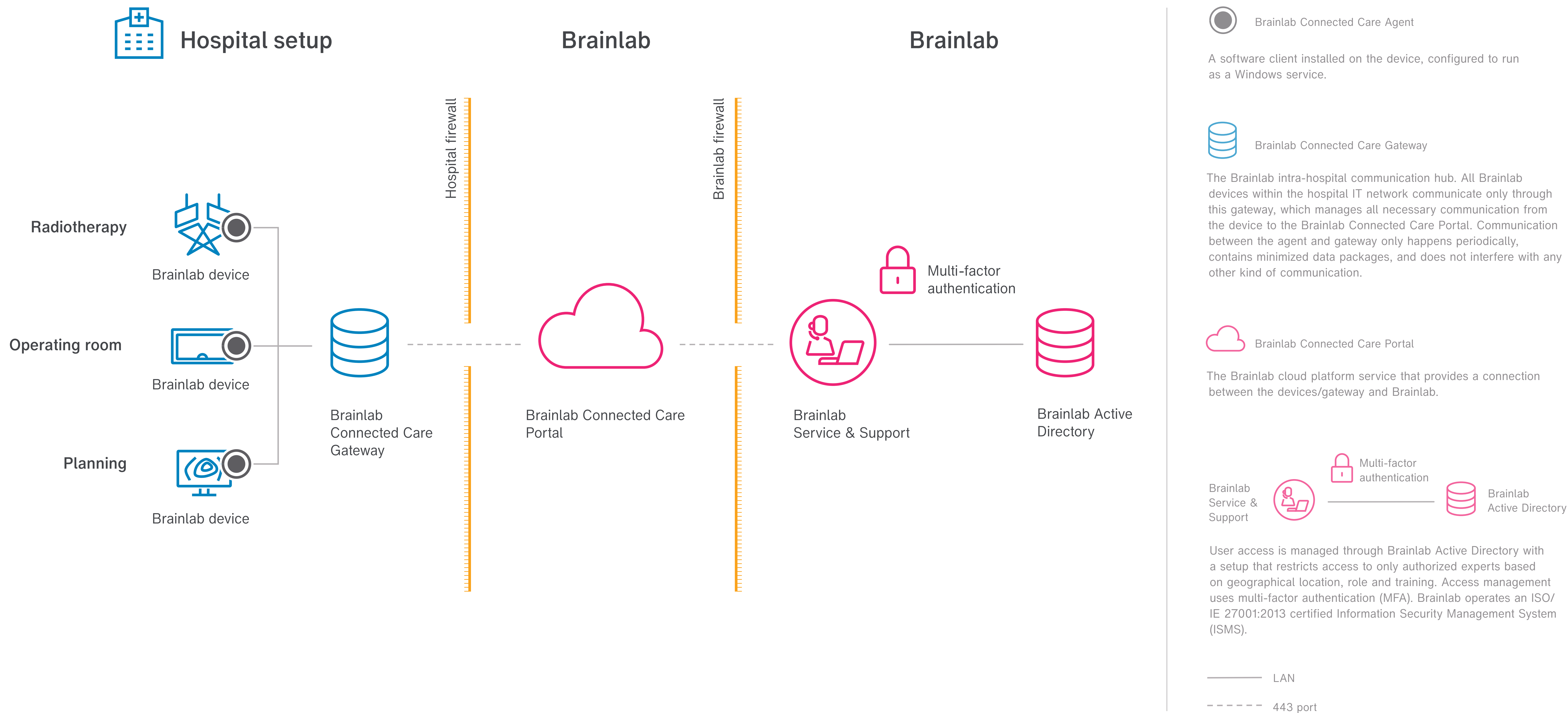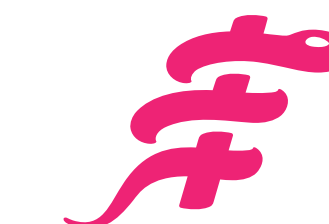## Overview and components

Hospital setup

Radiotherapy

Brainlab device

Operating room

Brainlab device

Planning

Brainlab device

Brainlab
Connected Care
Gateway

Hospital firewall

Brainlab

Brainlab Connected Care
Portal

Brainlab firewall

Brainlab

Multi-factor
authentication

Brainlab
Service & Support

Brainlab Active
Directory

Brainlab Connected Care Agent

A software client installed on the device, configured to run as a Windows service.

Brainlab Connected Care Gateway

The Brainlab intra-hospital communication hub. All Brainlab devices within the hospital IT network communicate only through this gateway, which manages all necessary communication from the device to the Brainlab Connected Care Portal. Communication between the agent and gateway only happens periodically, contains minimized data packages, and does not interfere with any other kind of communication.

Brainlab Connected Care Portal

The Brainlab cloud platform service that provides a connection between the devices/gateway and Brainlab.

Brainlab
Service &
Support

Multi-factor
authentication

Brainlab
Active Directory

User access is managed through Brainlab Active Directory with a setup that restricts access to only authorized experts based on geographical location, role and training. Access management uses multi-factor authentication (MFA). Brainlab operates an ISO/IE 27001:2013 certified Information Security Management System (ISMS).

LAN

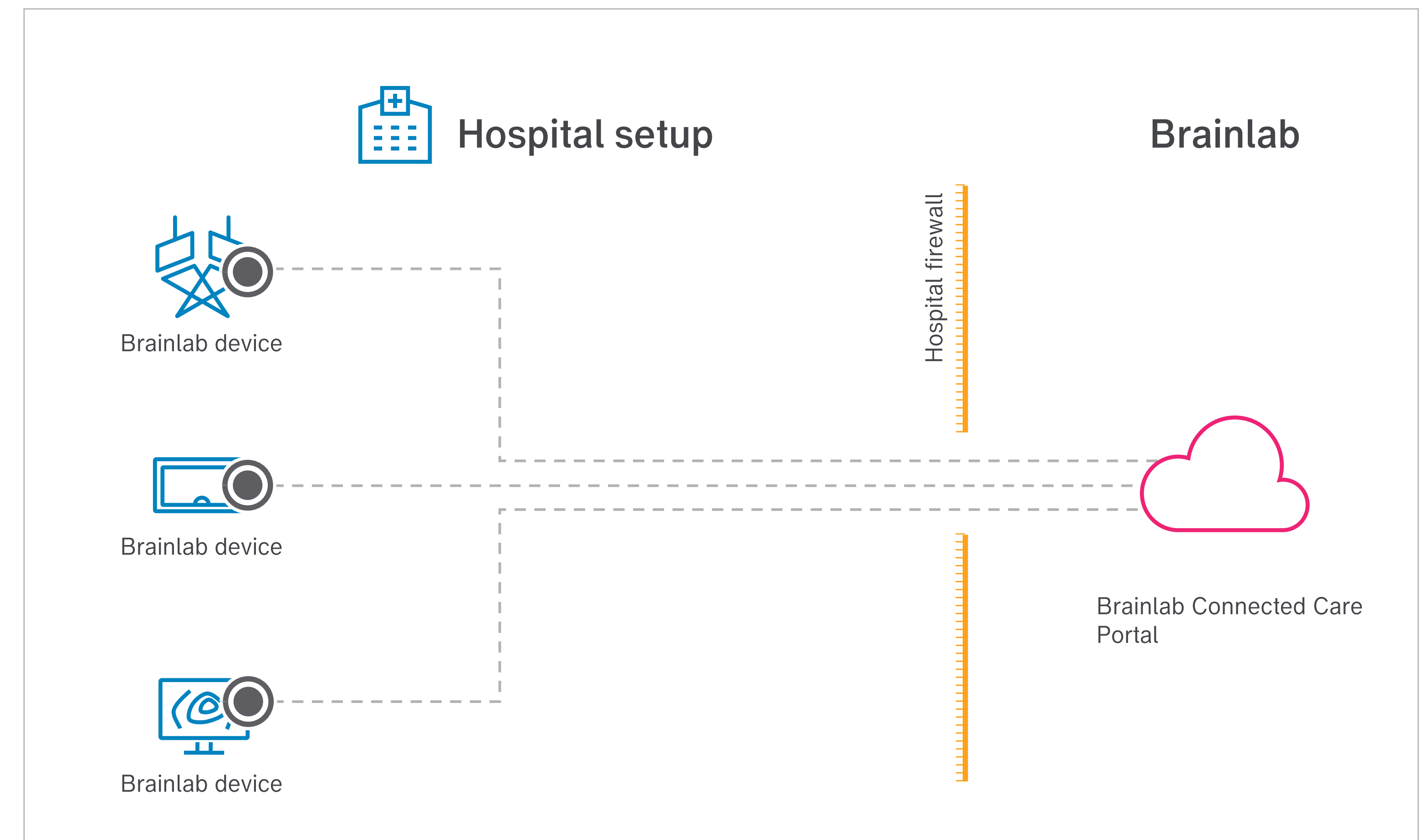443 port

System architecture
Secure communication
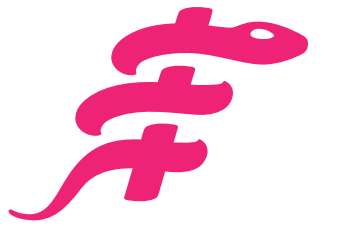
All communication flows from the Brainlab Connected Care agent running on your device to the Brainlab Connected Care Portal at support.brainlab.com using the HTTPS protocol with TCP port 443 and 256-bit TLS (transport layer security) end-to-end encryption. This connection is always outbound. There are two existing configuration options regarding the connection of devices:

**1** Connection of Brainlab devices with Brainlab Connected Care Gateway
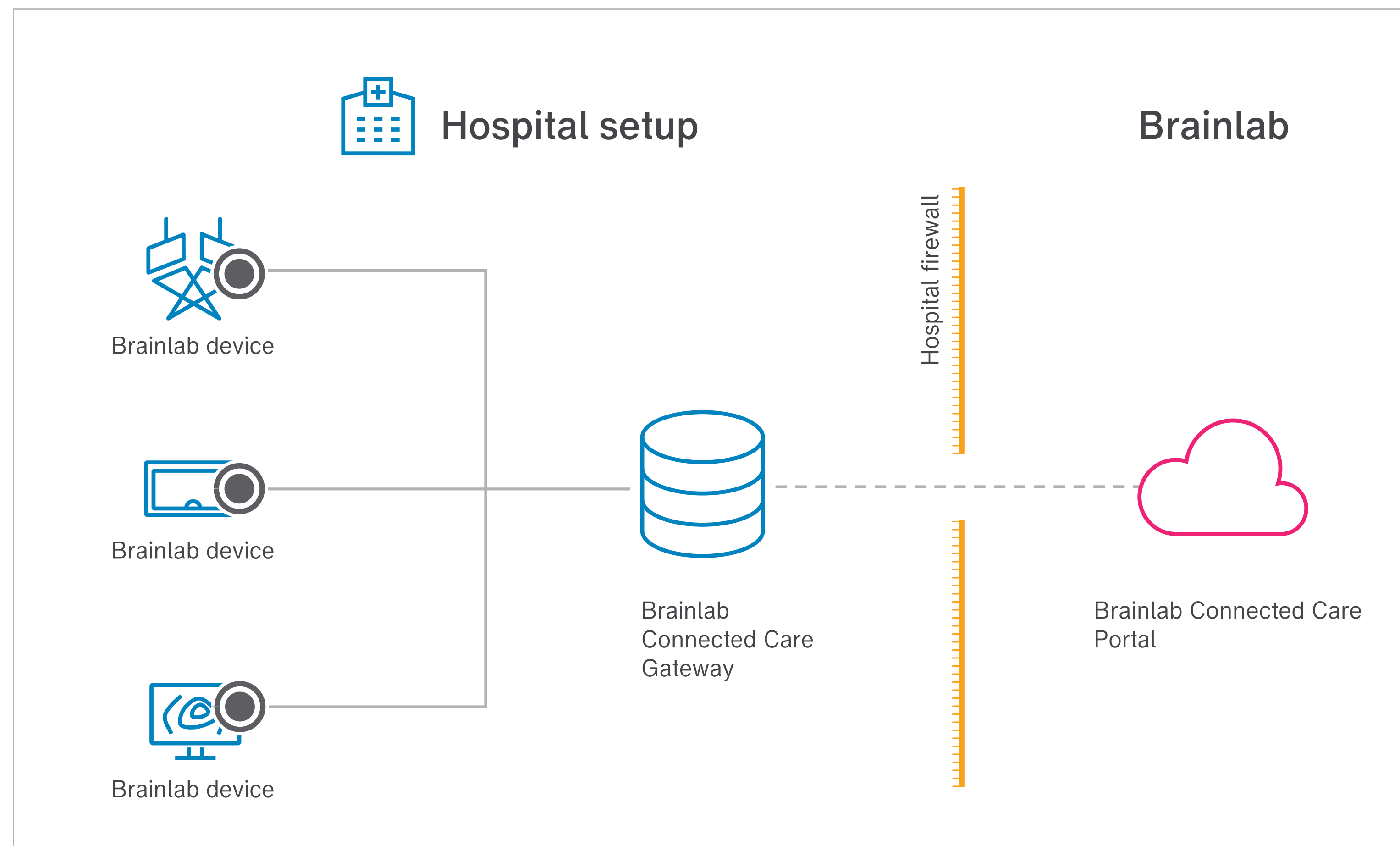
2 Direct connection of each Brainlab device

Hospital setup — Brainlab

Brainlab device
Brainlab device
Brainlab device

Brainlab Connected Care Gateway

Hospital firewall

Brainlab Connected Care Portal

Hospital setup — Brainlab

Brainlab device
Brainlab device
Brainlab device

Hospital firewall

Brainlab Connected Care Portal

Installation

Effortless implementation
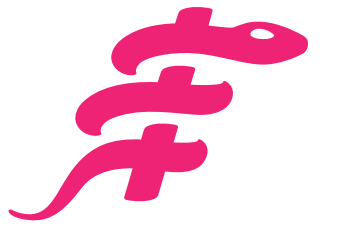
Brainlab Connected Care can be implemented in less than 10 minutes and requires no maintenance by you, all while guaranteeing the highest quality and security standards.

| 1. Installation | 2. Allow communication | 3. Your device is Brainlab Connected Care ready! |

There are two installation possibilities:

> Installation by Brainlab – Software is either preinstalled on the device or installation is done during system installation onsite.

> Installation by the customer – Brainlab will share the installation package with you.

Allow outbound communication on port 443 (HTTPS) on the device/gateway to:

1. Brainlab Connected Care Portal
   https://support.brainlab.com

2. Minimum two Global Access Servers (GAS) of your region (please see List of Global Access Servers)

If your organization uses a proxy server, the Brainlab service engineer will need to know the settings and authentication requirements to configure Brainlab Connected Care.

FAQs

What data is being collected by Brainlab Connected Care?

In order to maximize the utility of your device, Brainlab Connected Care collects technical and statistical data. The data will be collected and processed exclusively for this purpose. The data may include system settings and configuration, diagnostic/log files, component and parts status, device utilization and list of installed software.

For the purpose of identifying and resolving potential issues, Brainlab authorized experts may remotely collect certain diagnostic log files that contain protected health information (PHI) on demand. These files will be encrypted at rest and in transit and automatically deleted from the Brainlab Connected Care portal within 24 hours. The activities required in this context shall only be performed by authorized employees and carried out according to Brainlab organizational measures for the protection of personal data.

Who can access my device through Brainlab Connected Care?

Only authorized and trained Brainlab experts have access to Brainlab Connected Care and to your device information. Access is strictly managed through the Brainlab Active Directory, restricting access to employees based on geographical location, role and certification. Any change to the employee's status is automatically and immediately applied, which cannot be guaranteed with any other remote support solution.
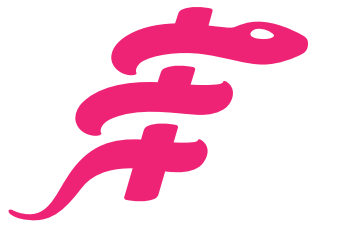
Additionally, all users accessing the Brainlab Connected Care Portal must be further verified with a multi-factor authentication system, increasing the security of Brainlab Connected Care.

All remote sessions are documented to ensure full transparency. Reports about individual sessions are stored both on customer and Brainlab servers.

Your questions, our answers

FAQs

What is the technology behind Brainlab Connected Care?

Brainlab Connected Care is a service built on PTC ThingWorx and hosted on Microsoft Azure servers. Combining the power of these platforms, Brainlab Connected Care uses only industry-standard security features through HTTPS, including encrypted storage and transmission of sensitive data, security logging sub-systems, and support for TLS 1.2 to ensure that all data transmitted is safely encrypted with Advanced Encryption Standard (AES) 256-bit.

PTC is constantly audited by third-parties and strives to maintain a rigorous security program to align and maintain:

> ISO 27001 audit and certification for PTC Cloud operations

> SSAE 16 SOC 2 Type II Security Trust Principle attestation for PTC Cloud's data centers

> International Standard on Assurance Engagements (ISAE) 3402 for PTC Cloud

> Federal Risk and Authorization Management Program (FedRAMP) for PTC Cloud

> ISO 27001 certification for PTC Cloud Data Centers, additionally strengthened with ISO 14001 and ISO 900

Do I need to have my devices permanently connected?

Brainlab Connected Care can be configured and customized to your needs.

We recommend keeping the Brainlab Connected Care application running on your device in the background so we can monitor and support your devices 24/7. This option will not interfere with the performance of the machine and you do not need to start the application after reboot.
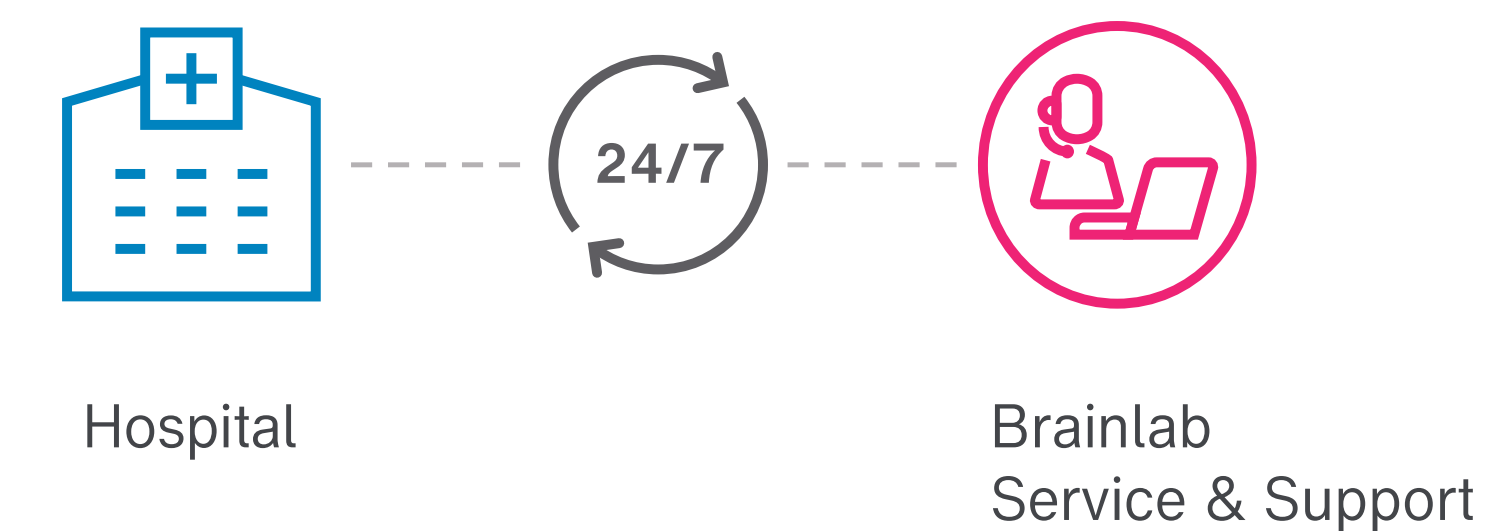
If needed, Brainlab Connected Care can also be configured to be available upon request. If not running in the background, Brainlab cannot offer full support, but can still offer remote assistance for specific issues through remote sessions. In this case, the Brainlab Connected Care application must be started and stopped manually on the device itself.

Hospital — 24/7 — Brainlab Service & Support

Hospital — on request — Brainlab Service & Support
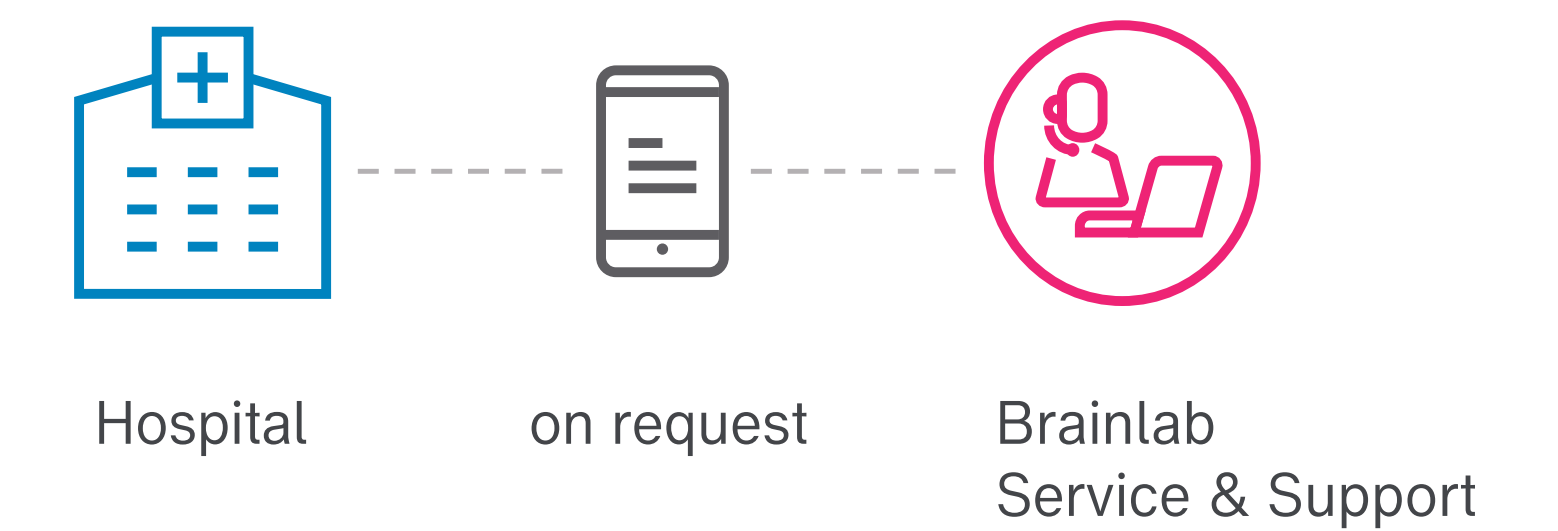
List of Global Access Servers

Location	Region	Host Name	Port
Authentication Server	Mandatory Worldwide	support.brainlab.com	443
Germany	EMEA	gas-de2.axeda.com	443
Germany	EMEA	gas-de3.axeda.com	443
Ireland	EMEA	gas-ie1.axeda.com	443
Ireland	EMEA	gas-ie2.axeda.com	443
UK	EMEA	ghuk2.axeda.com	443
UK	EMEA	ghuk3.axeda.com	443
Australia East	ASIA	gas-aus2.axeda.com	443
Australia West	ASIA	gas-aus3.axeda.com	443
Japan	JP	ghjap1.axeda.com	443
Japan	JP	ghjap2.axeda.com	443
CA, United States	NCA/LA	ghsj1.axeda.com	443
CA, United States	NCA/LA	ghsj2.axeda.com	443
CA, United States	NCA/LA	gas-sj4.axeda.com	443
MS, United States	NCA/LA	ghsom1.axeda.com	443
MS, United States	NCA/LA	gas-bo3.axeda.com	443
MS, United States	NCA/LA	gas-bo6.axeda.com	443
MS, United States	NCA/LA	gas-bo7.axeda.com	443
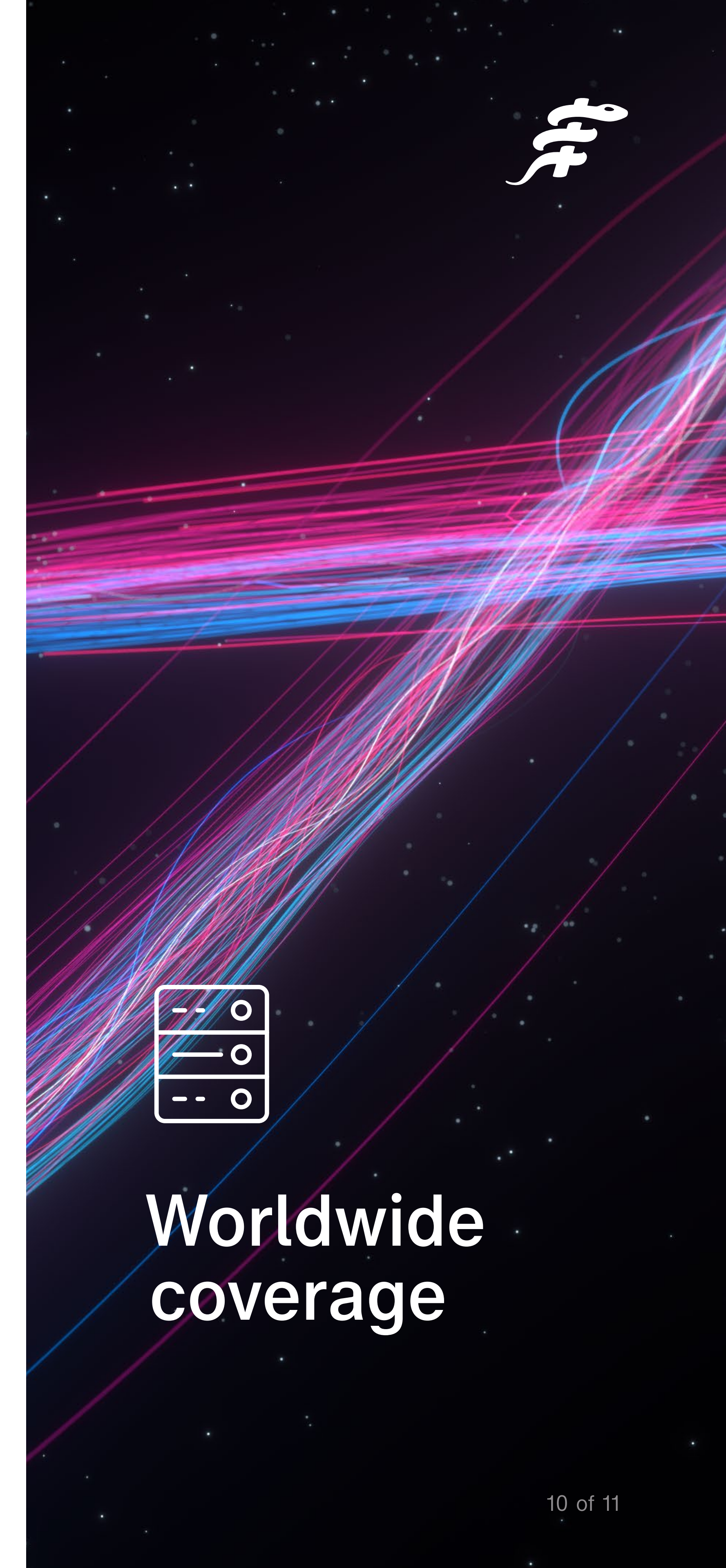
Worldwide coverage

Still have questions? Please reach out to us.
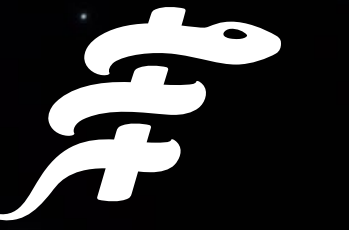
Brainlab Service & Support
for Europe, Middle East, Africa,
Asia and Australia
Telephone: +49 89 99 15 68 1044
Email: support@brainlab.com

Brainlab Service & Support
for North America and Latin America
Telephone: +1 (800) 597-5911
Email: us.support@brainlab.com