Remote Service

Cybersecurity, Privacy and Connectivity.
Frequently Asked Questions

Published 7 March 2023

Remote Service

Remote Service is an offering from Roche containing Remote Support, Digital Updates and Digital Uploads.

Purpose

The purpose of this document is to describe the technical aspects in regards to Cybersecurity, Privacy and Connectivity of Remote Service.

Cybersecurity and privacy controls of Roche medical devices, e.g. laboratory devices are not within the scope of this document. Details on the security controls on Roche medical devices can be obtained from the respective medical device documentation.

☎ *Please contact your local Roche representative for more information.*

1. Remote Service FAQs

Use case overview

What is Remote Service?

Remote Service is a secure digital infrastructure that allows Roche to provide critical support services including Remote Support, Digital Updates, and Digital Uploads.

Note: This offering varies per device type*.

It can be used for:

Remote Support

Remote error analysis and remote screen sharing

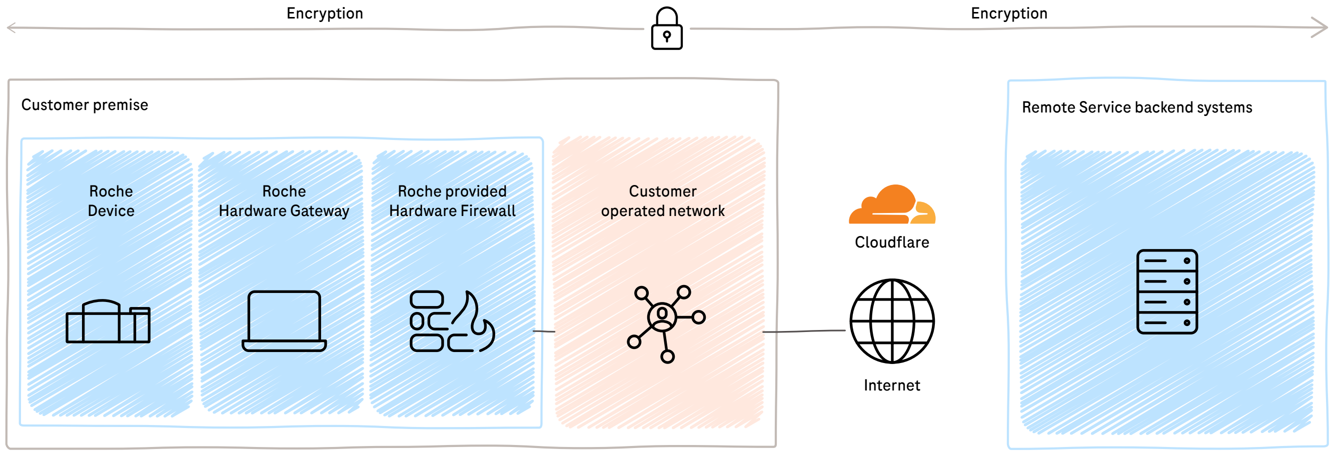
Digital Updates

Production information and software updates

Digital Uploads

Device data transfer for advanced analytics

*Devices can be referred to as Roche products such as gateways, medical devices, middleware, IT and point of care products. For ease of use, in this document the terms device, instrument, IVD system and product are all used interchangeably.



What are the benefits of Remote Service provided capabilities compared to offline operation of devices?

Connecting a Roche device using Remote Service enables a **wide range of benefits** in comparison to operating the same device offline.

These include:

Remote Service enables higher uptime and helps reduce downtime

- Proactive monitoring allows Roche to detect, identify and repair potential issues before parts break, replacing emergency (disruptive) interventions with scheduled maintenance.
- Remote Support enables guidance to the operator when assistance on the operation and maintenance of devices is required.
- Remote repair may be feasible when problems occur, resulting in reduced downtime and improved phone fix rate / first fix rate.

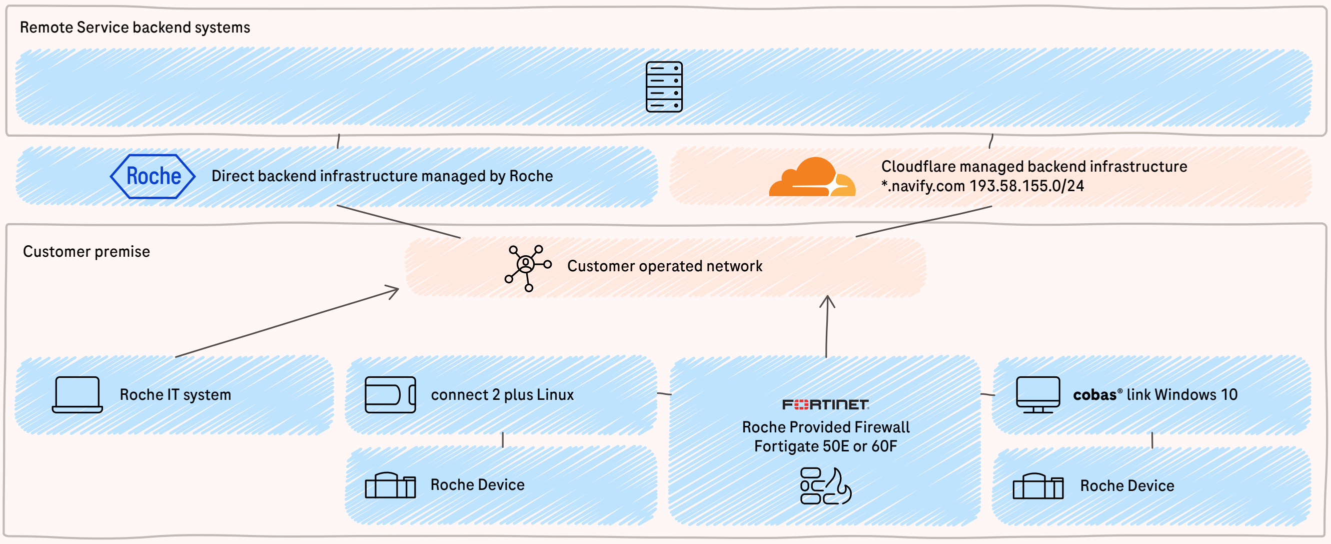
Remote Service can help minimize ecological footprint and supports maximized efficiency

- Digital Updates replace physical media, and avoid printing of package inserts and user manuals.
- Remote Support means less time needed to 'explain' problems as the call center agents can see the device status remotely.

Connecting a Roche device using Remote Service will enable a ***wide range of benefits.***

2. What are the components involved?

The main infrastructure consists of both **hardware** and **software** components. A high level overview is depicted below:



Remote Service backend systems
Roche
Direct backend infrastructure managed by Roche
Cloudflare managed backend infrastructure
*.navify.com 193.58.155.0/24
Customer premise
Customer operated network
Roche IT system
connect 2 plus Linux
Roche Device
FORTINET
Roche Provided Firewall
Fortigate 50E or 60F
cobas® link Windows 10
Roche Device

Main elements are governed by the Roche Vulnerability & Incident Handling Policy and Product Cybersecurity Statement:

Vulnerability & Incident Handling Policy
https://diagnostics.roche.com/global/en/legal/vulnerability-and-incident-handling-policy.html

Product Cybersecurity Statement
https://diagnostics.roche.com/global/en/legal/diagnostics-product-cyber-security-statement.html

Remote Service backend systems

1. One main element of the backend systems is built on the PTC ThingWorx™ platform, which is implemented according to the specific needs of Roche. It enables Remote Support, Digital Updates and Digital Upload services. https://www.ptc.com/en/resources/iiot/product-brief/thingworx-platform

thingworx®

2. The second main element of the backend systems is a Roche custom built platform which is specialized for product information distribution, which is part of Digital Updates.

3. A third element of the backend systems is the FortiManager, Fortinet's Central Management platform for FortiGates. Roche's FortiManager is hosted on Roche-managed Microsoft Azure nodes and provides a suite of services to centrally manage the Roche provided Fortigate devices around the globe.

FORTINET

Roche provided hardware firewall

The hardware firewall is a device located within the customer laboratory network to protect Roche devices from cybersecurity threats. It is a stateful firewall manufactured by a leading firewall vendor, with a Roche custom configuration to protect Roche medical devices. Please contact your local Roche organization for more details on the firewall.

Roche Hardware gateway (cobas® link/connect 2 plus)

The **cobas**® link and connect 2 plus are both small form factor computers located within the customer laboratory network. They host the Remote Service Edge Agent and additional software to enable connectivity and further functionality. The gateways are placed behind the Roche provided hardware firewall.

Remote Service Edge Agent (REA)

REA is a software gateway which can be installed on certified Roche devices and on Roche IT products (e.g. software only solutions) where the customer owns and manages the hardware and operating system. As REA is installed on customer maintained hosts, usually no Roche provided hardware firewall is present and the customer is responsible for providing accurate security measures. REA is also governed by the Roche product vulnerability management process and security updates are automatically deployed as required.

The solution is subject to ***industry standard security penetration testing*** *by both internal Roche teams and independent 3rd parties.*

3. Privacy considerations

How does Roche protect customer privacy?

A **universal standard** on processing personal data and contractual agreements with 3rd parties is established and adopted by all Roche companies to provide preventive safeguards against infringement of privacy rights through inappropriate processing of personal data.

Roche has stated that compliance with data privacy laws while processing personal data is a corporate objective. As such, Roche is committed to respecting the personal rights and privacy of individuals.

The Roche Directive on the Protection of Personal Data can be found at: https://www.roche.com/stories/data-sharing-in-personalised-healthcare.

How is privacy assured during the transmission of data between the laboratory and the Remote Service backend systems?

All data transports (transport layer) are **encrypted end-to-end** from the Remote Service Edge Agent to the Remote Service backend systems.

Is privacy ensured during Remote Support?

Remote Support – like any other workflow – is established over a secured connection using **transport layer security (TLS) protocol**. Remote Support may be necessary to troubleshoot and restore a system to its operational state. This usually occurs after a customer notifies the Roche call center about a problem or a Roche employee contacts the customer after observing abnormal system behavior indicating a potential compromise of the device. Remote Support data, e.g. the screen sharing sessions, are not persistent and are not recorded.

Who is authorized to access and use the Remote Service offerings?

Access is controlled with a user management system. Only authorized and trained Roche personnel with business reason have access to the system. Users are always authenticated based on their Roche credentials and access is only possible using a Roche provided and maintained computer.

Audit log #1.25

To comply with regulations and support forensic investigations, the enterprise system generates an audit log for all Remote Support sessions containing device, user identification and start-/end-time.

Please contact your local Roche representative to obtain audit log information.

What is the purpose for collection of Roche device data?

Data collected by Roche is used for subsequent analysis (e.g. device/test performance) and stored in compliance with applicable laws and regulations.

Please contact your local Roche representative for more information.

*Data stored in external hosting centers is subject to the **same regulations** as data stored in Roche-hosted data centers.*

4. Technical FAQ

Roche backend infrastructure

Which URLs, IP-addresses, ports and protocols are required to establish connectivity?

As the solution contains multiple components, a **set of connections** to backend infrastructure components is required.

The technical setup includes two sets of connections:

- **Direct backend infrastructure** fully governed and managed by Roche
- **Cloudflare managed infrastructure** (governed by Roche) using a Roche domain and IP-addresses

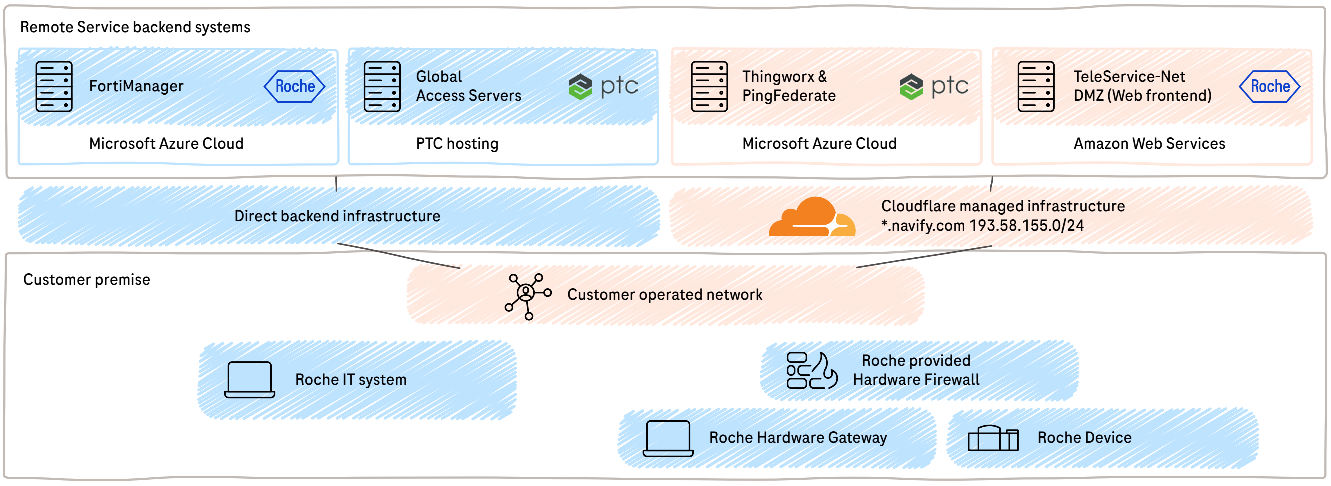
Backend infrastructure managed by Roche

Direct backend infrastructure connections can be identified by specific URLs and IP-addresses not belonging to the Roche owned IP-address range managed by Cloudflare.

Backend infrastructure managed by Cloudflare

Remote Service is utilizing Cloudflare services to not only enable the **latest security technologies** but also to **gain flexibility** for future needs. The Roche owned domain (navify.com) together with the Roche owned IP-address range (193.58.155.0/24, meaning all IP-addresses from 193.58.155.1 to 193.58.155.254) is managed using Cloudflare and their BYOIP (bring your own IP) service.

Further information can be found at:
https://blog.cloudflare.com/bringing-your-own-ips-to-cloudflare-byoip/


Remote Service backend systems
FortiManager
Roche
Microsoft Azure Cloud
Global Access Servers
ptc
PTC hosting
Thingworx & PingFederate
ptc
Microsoft Azure Cloud
TeleService-Net DMZ (Web frontend)
Roche
Amazon Web Services
Direct backend infrastructure
Cloudflare managed infrastructure
*.navify.com 193.58.155.0/24
Customer premise
Customer operated network
Roche IT system
Roche provided Hardware Firewall
Roche Hardware Gateway
Roche Device

Roche backend infrastructure – Detailed table

URL	IP	Port	Type	Description
*.navify.com	193.58.155.0/24	443	Cloudflare	Main connections enabling Remote Service
remoteservice-gas1.roche.com	62.209.44.21	443	Direct	Dedicated connections enabling Remote Support
remoteservice-gas2.roche.com	62.209.44.22	443	Direct	Dedicated connections enabling Remote Support
remoteservice-gas3.roche.com	209.202.167.19	443	Direct	Dedicated connections enabling Remote Support
remoteservice-gas4.roche.com	209.202.167.20	443	Direct	Dedicated connections enabling Remote Support
remoteservice-gas5.roche.com	120.136.45.231	443	Direct	Dedicated connections enabling Remote Support
remoteservice-gas6.roche.com	120.136.45.230	443	Direct	Dedicated connections enabling Remote Support
remoteservice-gas15.roche.com	35.76.193.4	443	Direct	Dedicated connections enabling Remote Support
remoteservice-gas16.roche.com	52.193.219.53	443	Direct	Dedicated connections enabling Remote Support
rln-cm-**.dia.roche.com	52.178.37.238	514 / 541	Direct	Dedicated connections enabling FortiGate management

* = specific URLs to identify individual systems
** = EMEA, NALA or APAC, specific URLs by region

CLOUDFLARE

What is Cloudflare?

Cloudflare is one of the biggest networks operating on the Internet. People use Cloudflare services for the purposes of increasing the security and performance of their web sites and services.
https://www.cloudflare.com/learning/what-is-cloudflare/

What services of Cloudflare are used by Roche Remote Service?

1. **Web Application Firewall**
   Protects backend systems from attacks like DDOS
   https://www.cloudflare.com/waf/
2. **Bring Your Own IP**
   Allows use of Roche owned IP-addresses
   https://blog.cloudflare.com/bringing-your-own-ips-to-cloudflare-byoip/
3. **Server Name Indication**
   Redirects incoming agent traffic to corresponding backend system
   https://www.cloudflare.com/learning/ssl/what-is-sni/
4. **Border Gateway Protocol**
   Allows use of the same IP globally and to connect to the closest data center
   https://www.cloudflare.com/learning/security/glossary/what-is-bgp/

These services are available using the Roche domain: *.navify.com and the Roche owned IP-address Range 193.58.155.1–193.58.155.254.

Root Certificates

Digital certificates are used to establish encrypted communication and to confirm the identity of communication endpoints (necessary for the TLS protocol). Advanced network protection systems such as firewalls, proxies or content filters may not allow communication until these certificates are manually loaded as trusted certificates into these systems.

Depending on the infrastructure, different root certificates are used:

Direct backend infrastructure connections utilize a **Roche provided root certificate**. Roche root certificates can be obtained publicly from the Roche Certificate Authority:

https://certinfo.roche.com/

Cloudflare managed infrastructure connections utilize **public root certificates**. Further information is available at the following loaction:

https://developers.cloudflare.com/ssl/reference/certificate-authorities/

The Remote Service backend systems enable ***secure communication*** *with Roche devices.*

5. Remote Service Edge Agent

What is the Remote Service Edge Agent (REA)?

The Remote Service Edge Agent is a software component to connect Roche Hardware Gateways and Roche devices and enables Remote Service workflows. It is based on the ThingWorx™ SDK (software development kit) and is to be installed on qualified Roche devices only. Every Remote Service Edge Agent instance needs to pass the trust process before communication with the backend systems is enabled. The trust process ensures only eligible devices and gateways communicate with the platform.

Is the Remote Service Edge Agent protected against viruses and worms, and malware in general?

When the Roche device is software only, e.g. the Roche software is installed on a customer provided host, antivirus protection, OS updates and further security measures are in the responsibility of the customer. Please contact your local Roche representative for antivirus installation guidance for a specific Roche product.

How are security patches handled for the Remote Service Edge Agent?

REA is updated as required; hence there is no fixed update schedule. REA updates are provided for vulnerabilities and comply with the Roche vulnerability management policy. REA is monitored by the Roche vulnerability process and applicable security updates are implemented as needed. Updates are validated before deployment is executed to ensure proper functionality. REA is a separate component designed to be installed on qualified Roche Hardware Gateways and qualified Roche devices and security patching can be done remotely.
https://diagnostics.roche.com/global/en/legal/vulnerability-and-incident-handling-policy.html

__Time savings__ and __greater efficiency__ for Roche devices operated online.

6. Hardware Gateways

cobas® link

The section below provides further details about the **cobas®** link security protection measures. Physical protection of the **cobas®** link must be ensured by the customer.

Minimizing system attack surface

- Hardened Windows 10 IoT Enterprise LTSC 2019 Operating System
- Expiration of user sessions after a set period of inactivity
- Temporary lock out of user accounts after a set number of failed login attempts

Additional security controls

- User segmentation – low-privileged users restricted from installing software and executing arbitrary programs, commands and system utilities
- Anti-virus / malware scanner installed and configured
- Limited inbound and outbound communication of all network services controlled by the Windows 10 embedded firewall
- Communication channels for remote administration provide end-to-end security encryption
- Restricted execution of software from untrusted storage devices like USB sticks
- Wireless interfaces – if any – are disabled by default

How is network access to cobas® link protected?

cobas® link is preconfigured with security hardening mechanisms. For instance, it has a Roche controlled security-relevant configuration applied to the BIOS, account groups / policies, system components and interfaces.

cobas® link is protected using security policies of the operating system. On the network interfaces only IPs, ports and protocols required for the communication with the Remote Service applications and connected Roche devices are authorized.

cobas® link should only be installed in a secure customer environment (e.g. a laboratory room with physical access controls). A Roche provided hardware firewall is mandatory for enhanced protection.

Is the software on cobas® link regularly updated?

Roche updates the operating system and related software components with current security patches published by the corresponding manufacturer on a regular schedule. Updates are validated before deployment to ensure proper functionality.

How is the security of cobas® link tested?

In the event of major product changes, and on a regular basis, penetration tests are performed on **cobas**® link by 3rd party cybersecurity companies.

connect 2 plus

The section below provides further details about the connect 2 plus security protection measures. Physical protection of the connect 2 plus must be ensured by the customer.

Minimizing system attack surface

- Roche tailored Linux Operating System to minimize vulnerability likelihood
- Certificate based authentication for Roche Service personnel only

Additional security controls

- Limited inbound and outbound communication of all network services controlled by the Linux embedded firewall
- Communication channels for remote administration provide end-to-end security encryption
- Restricted execution of software from untrusted storage devices like USB sticks
- Wireless interfaces – if any – are disabled by default

How is network access to connect 2 plus protected?

connect 2 plus is preconfigured with security hardening mechanisms. For instance, it has a Roche controlled security-relevant configuration applied to the BIOS, account groups / policies, system components and interfaces.

connect 2 plus is protected using security policies of the operating system. On the network interface, only IPs, ports and protocols required for the communication with the Remote Service applications and connected Roche devices are authorized.

connect 2 plus should only be installed in a secure customer environment (e.g. a laboratory room with physical access controls). A Roche provided hardware firewall is mandatory for enhanced protection.

Is the software on connect 2 plus regularly updated?

Roche updates the operating system and related software components with the current security patches published by the corresponding manufacturer on a regular schedule. Updates are tested before deployment to ensure proper functionality.

How is the security of connect 2 plus tested?

In the event of major product changes, and on a regular basis, penetration tests are performed on connect 2 plus by 3rd party cybersecurity companies.

FortiGate Central Management

FortiManager is Fortinet's Central Management platform for FortiGates. Roche's FortiManager is hosted on Roche-managed Microsoft Azure nodes. FortiManager provides:

- **Status monitoring** for registered FortiGates
- **Monitoring of unauthorized (blocked) communication** attempting to cross a FortiGate
- **Scheduled remote firmware upgrades** (of course in coordination with the customer as a firmware upgrade requires a FortiGate reboot)

FortiManager is protected by means of:

- Communication between FortiGate and FortiManager is done through only two ports using TLS encryption: 514 (sending logs to FortiManager) and 541 (FortiGate management). Communication on both ports is based on TCP.
- FortiManager software version is updated when needed in order to ensure running a secure and stable version.
- Only specific Roche authorized personnel from the local or regional support organization have access to FortiManager (via the global Roche credentials solution). In many regions, only a few selected Roche IT experts are selected to administrate it.
- Azure perimeter protection based on Azure security groups as well management access performed within FortiManager, enabled only from Roche-registered IP-addresses.

Risk Assessment

Both FortiGate and FortiManager are periodically assessed by the **PCERT** (Product Cybersecurity Emergency Response Team) department. Further decisions on upgrading systems to a higher version are based on assessment results.

The Remote Service backend infrastructure is
ISO/IEC 27001, ISO 27017, ISO 27018 and ISO 13485 certified

Information Security Management System ISO 27001 Certified
Information Security Management System ISO 27017 Certified
Information Security Management System ISO 27018 Certified
Information Security Management System ISO 13485 Certified

The PTC ThingWorx™ platform used by Remote Service is in the process to receive HIPAA compliance

Roche Diagnostics International Ltd, CH-6343 Rotkreuz, Switzerland

www.diagnostics.roche.com