POC module for **navify**® Integrator

Primary care provider administrator

User Guide

Publication version 5.2

Revision history

Revision history

Publication version	Software version	Revision date	Change description
1.0	1.0	November 2019	First version
1.1	1.1	May 2020	
2.0	2.0	December 2021	
3.0	2.0.2	June 2022	
4.0	2.0.3	September 2022	
4.1	2.0.4	November 2022	
4.2	2.0.7	September 2023	
4.3	2.1.0 and higher	June 2024	
5.0	3.0	November 2024	
5.1	3.1 and higher	June 2025	
5.2	3.3 and higher	January 2026	What is new in publication version 3.3 (10)

Revision history

Edition notice

This publication is intended for users of POC module for **navify**® Integrator.

Every effort has been made to ensure that all the information contained in this publication is correct at the time of publishing. However, the manufacturer of this product may need to update the publication information as output of product surveillance activities, leading to a new version of this publication.

Where to find information

The **User Assistance** and the **User Guide** contain all information about the product, including the following:

- Safety
- Routine operation
- Troubleshooting information

Privacy notice

When you use User Assistance online, viewing events (topics viewed and searches performed) and IP addresses are logged.
The data collected is for Roche internal use only and is never forwarded to third parties. It is anonymized, and after one year it is automatically deleted.
Viewing events are analyzed to improve User Assistance content and search functionality. IP addresses are used to classify regional behavior.

Training

Do not carry out tasks unless you have received training. Leave tasks that are not described in the user documentation to a trained administrator.

Multimedia

The screenshots and videos in this publication have been added exclusively for illustration purposes.

Warranty

Any customer modification to the system renders the warranty or service agreement null and void.

For conditions of warranty, contact your local sales representative or refer to your warranty contract partner.

Copyright

License information

POC module for **navify**® Integrator software is protected by contract law, copyright law, and international treaties. POC module for **navify**® Integrator contains a user license between F. Hoffmann-La Roche Ltd. and a license holder, and only authorized users may access the software and use it. Unauthorized use and distribution may result in civil and criminal penalties.

Open-source and commercial software

Portions of the POC module for **navify**® Integrator might include components or modules that are open source or commercial software programs. For copyright and other notices and licensing information regarding such software programs, see the **Software licenses** tab in the information section of the application

Trademarks

The following trademarks are acknowledged:

COBAS, NAVIFY, COBAS and LIAT, COBAS B, COBAS H, COBAS U, URISYS, COAGUCHEK and LIFE NEEDS ANSWERS are trademarks of Roche.

All other trademarks are the property of their respective owners.

Feedback

Every effort has been made to ensure that this publication fulfills the intended use. All feedback on any aspect of this publication is welcome and is considered during updates. Contact your Roche representative, should you have any such feedback.

Contact address

Roche Diagnostics GmbH
Sandhofer Strasse 116
68305 Mannheim
Germany

Made in Switzerland

Distributed in the United States by:

Roche Diagnostics

9115 Hague Road

Indianapolis, IN 46256

USA

REF **10404094001**

Table of contents

Intended use

POC module for **navify**® Integrator is intended to be used to connect POC medical devices to POC data management system over a public or private network (e.g. Internet / LAN / WAN) in a secure way in order to transfer data.

POC module for **navify**® Integrator is intended to be used to provide the transport layer between Roche Business Applications and Roche POC devices, located at the customer sites. The system is intended to transport (bi-directional) data (payload) between Roche Business Applications and POC devices in a secure way.

The system is not intended for diagnosis, screening, monitoring or treatment of patients. POC module for **navify**® Integrator will not change any data while it is being transferred between the connected systems and devices.

Intended users

User group	Description of use
Primary care site manager	• Installs the Terminal (POC) at the primary care and configures it (with assistance of local IT support / SP / RCSC / CO) • Connects the Terminal (POC) to the CM (using registration information provided by the SP or CO) • Connects POC instruments to the Terminal (POC) • Calls Service Provider / local IT Support for assistance

Intended users

User group	Description of use
Service Provider (POCC / Hospital IT)	• Registers / configures Terminals (POC) in the CM and provides registration information to PCP • Assists the PCP with installing / configuring Terminals (POC) and connecting POC instruments, performs 1st level Support • Monitors health and connection status of all connected PCPs Terminals, receives alerts / notifications • Calls RCSC for inquiries and complaints
Roche Global and Local Customer Support.	• Enabling the service to end customers (onboarding) • Automatic SW and LOT package distribution • Registration of POC device on Roche business application • Status monitoring

Intended users

Symbols and abbreviations

Product names

Except where the context clearly indicated otherwise, the following product names and descriptors are used.

Product name	Descriptor
POC module for **navify**® Integrator	System
navify® Connector for Community	System

Product names

Symbols used in the publication

The following symbols are used:

Symbol	Explanation
•	List item
	Related topics containing further information
	Tip: extra information on correct use or useful hints
	Start of a task
	Caution, consult accompanying documents
	Extra information within a task
	Result of an action within a task
	Materials that are required for a task
	Prerequisites of a task
	Topic (used in cross-references to topics)
	Task (used in cross-references to tasks)
	Figure (used in figure titles and cross-references to figures)
	Table (used in table titles and cross-references to tables)

Symbols used in the publication

Symbols used in system

Symbol	Explanation
	Catalog number
	Global Trade Item Number
	Manufacturer
	Consult instructions for use
	Caution

Symbols used in the system

Abbreviations

The following abbreviations are used

Abbreviations	Definition
CPU	Central processing unit
DMS	Data management system

Abbreviations

Abbreviations	Definition
IIS	Internet Information Services
IT	Information Technology
LAN	Local area network
POC	Point of Care
RAM	Random access memory
SSL	Secure Sockets Layer
USB	Universal Serial Bus
WAN	Wide area network

Abbreviations

What is new in publication version 3.3

List of technical requirements

Included four new URLs for DigiCert certificate validation.

List of technical requirements (30)

Creating POC service provider

Introduces data privacy levels framework that includes a new alert system at the Service Provider (SP) level.

Creating POC service providers

Safety

Page intentionally left blank.

Safety information

1

In this chapter

Page intentionally left blank.

Safety classifications

The safety precautions and important user notes are classified according to the applicable standards. Familiarize yourself with the following meanings and icons:

⚠ Safety alert

- The safety alert symbol is used to alert you to potential physical injury hazards. Obey all safety messages that follow this symbol to avoid possible damage to the system, injury, or death.

These symbols and signal words are used for specific hazards:

⚠ WARNING!

Warning...

- ...indicates a hazardous situation that, if not avoided, could result in death or serious injury.

⚠ CAUTION!

Caution...

- ...indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.

NOTICE!

Notice...

- ...indicates a hazardous situation which, if not avoided, may result in damage to the system.

Important information that is not safety relevant is indicated with the following icon:

Tip...

...indicates additional information on correct use or useful tips.

System safety

Failure to observe the safety information may result in incorrect results, data corruption, patient harm, and data losses.

Incorrect or corrupt data due to unauthorized access

Data security is breached if unauthorized users have access to your user name and password.

- Use strong passwords.
- Always enter your password unobserved.
- Do not write down your password.
- Never write down the password in a contact form, in an address book or in a file on the computer.
- Do not disclose your password to anyone. Roche never asks you for your password.
- If you ever disclose your password to anyone, change it immediately after.
- If you think anyone else has access to your account, contact your system administrator immediately.
- Enforce users to change the default password on first usage.
- Always lock the workstations when leaving them unattended.

Changing regional settings impacts default measurement units for POC device configuration

Default measurement units for POC devices are linked to the regional settings. Therefore, when changing the regional settings, disallowed default measurement units could be generated in the QR code for POC device configuration.

- Ensure that the regional settings are configured correctly.

Data security

The IT manager of your organization should ensure that the following safety measures are implemented.

Monitor the system for suspicious activity and report suspected compromise

If you find any of the typical signs of malicious software or unauthorized access to the system (unexpected warning messages, files, or log entries like multiple failed logon attempts; significantly degraded user interface performance; seemingly random crashes of the system; automated typing of text; and so on), the following recommendations are essential:

- Physically disconnect the system from the network.
- Contact the IT responsible in your organization to report and verify the finding.
- Mistrust results produced while the system has been compromised.
- Contact your Roche Service representative to initiate the system recovery.

Unauthorized system access and data loss

External storage devices can transmit computer malware, which may be used to gain unauthorized access to data or cause unwanted changes to software.

The operators are responsible for the IT security of their IT infrastructure and for protecting it against malicious software and hacker attacks. Failure to do so may result in data loss or may render the system unusable.

Roche recommends the following precautions:

- Allow connection only to authorized external devices.
- Implement physical access controls to ensure that only authorized staff operate the system at all times.
- To protect all external devices, make sure that you use appropriate security software.
- To protect access to all external devices, make sure that you use appropriate security equipment.
- Do not use the USB ports to connect other storage devices unless your Roche Service representative or an operating instruction tells you to do so.
- Exercise care when you use external storage device such as USB drives, CDs, or DVDs. Do not connect to the system any external storage device that you use on public or home computers.
- Keep all external storage devices in a secure place, and make sure that only authorized personnel can access them.
- Back up your data regularly.
- Make sure to use secure channels to download software updates of the system.
- Allow only internet access to trusted websites and web services.
- Do not include confidential development data in service documentation, user documentation, or marketing materials.
- Use state-of-the-art security mechanisms (e.g. WPA2 EAP) to protect Wi-Fi connections.
- Delete user accounts for personnel no longer requiring access to the system.

Network security

Malicious software and hacker attacks may impair IT security.

- To protect and separate Roche systems from other laboratory infrastructure, it is recommended to secure the connection to the POC Gateway through a Network Firewall.
- Configure the firewall of gateway hosts to block unnecessary incoming network traffic.
- Secure all devices and services used in the laboratory infrastructure against malicious software and unauthorized access.
- Secure the network environment to be resilient against traffic redirection and eavesdropping.
- Enable data execution preventions on gateway hosts.
- Verify the code signature of gateway software after download and prior to installation.

Checking website certificates

Valid website certificates ensure that the identity of a website operator is verified by a certificate authority. Website certificates are valid for up to two years.

To check a website certificate in Google Chrome

1 In the address bar for the website, choose the padlock icon.

2 In the context menu, choose **Certificate (valid)**.
➔ The **Certificate** dialog box is displayed.

3 Check the details of the certificate validity.
- For example, check who issued the certificate, to whom the certificate is issued to, and the certificate's expiry date.

System description

Page intentionally left blank.

Overview of the system

In this chapter 2

Page intentionally left blank.

About the system

POC module for **navify**® Integrator is a cloud-based system that connects POC devices in a remote location to a data management system in a secure and encrypted way over publicly available networks. The system brings testing closer to the patient at remote sites in the same way it is currently implemented in hospitals. It enables new services for laboratories and improves workflows for primary care providers.

Patient data is not accessible from the system. The status of connected components, organizations, and users can be viewed from within the system.

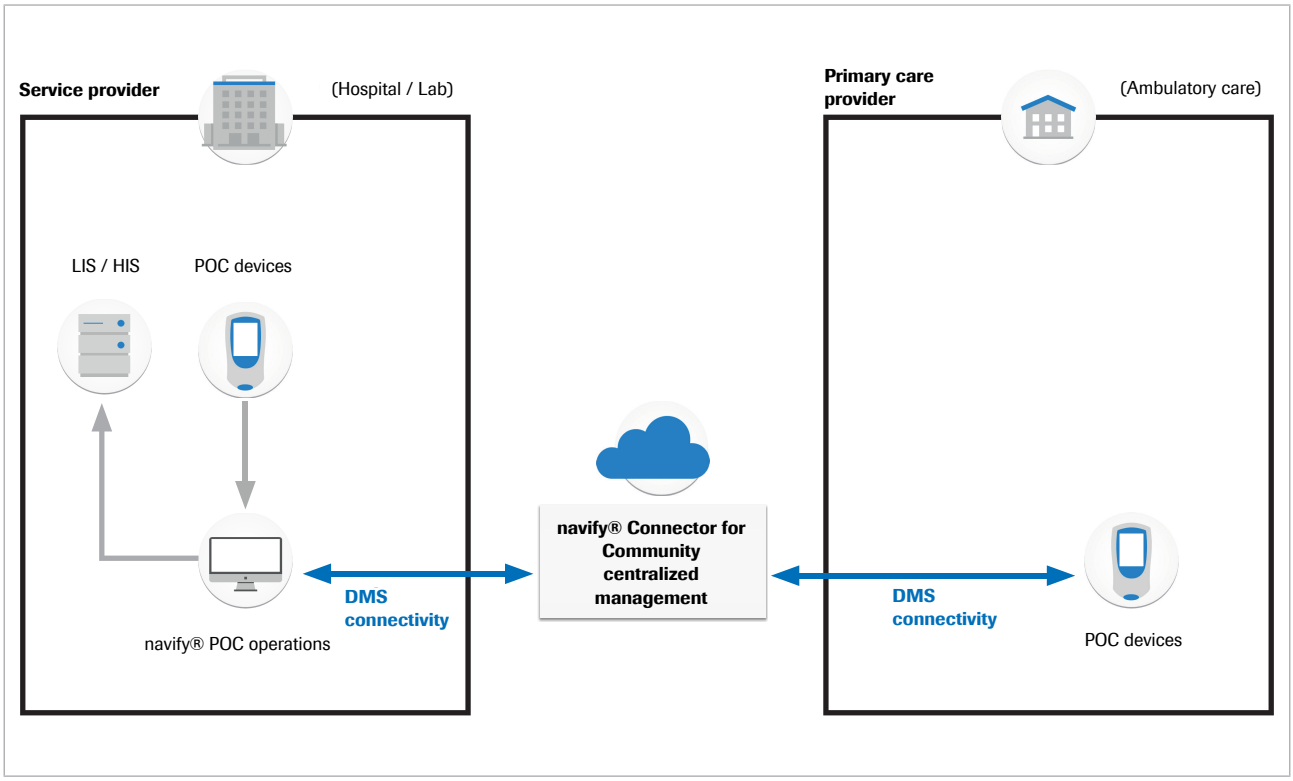
The following offerings are available

- **navify**® Connector for Community (DMS connectivity)
- POC module for **navify**® Integrator

Not all offerings are available in all countries.

navify® Connector for Community offering

Secure DMS connectivity via the operational interface:



navify® Connector for Community offering (DMS connectivity)

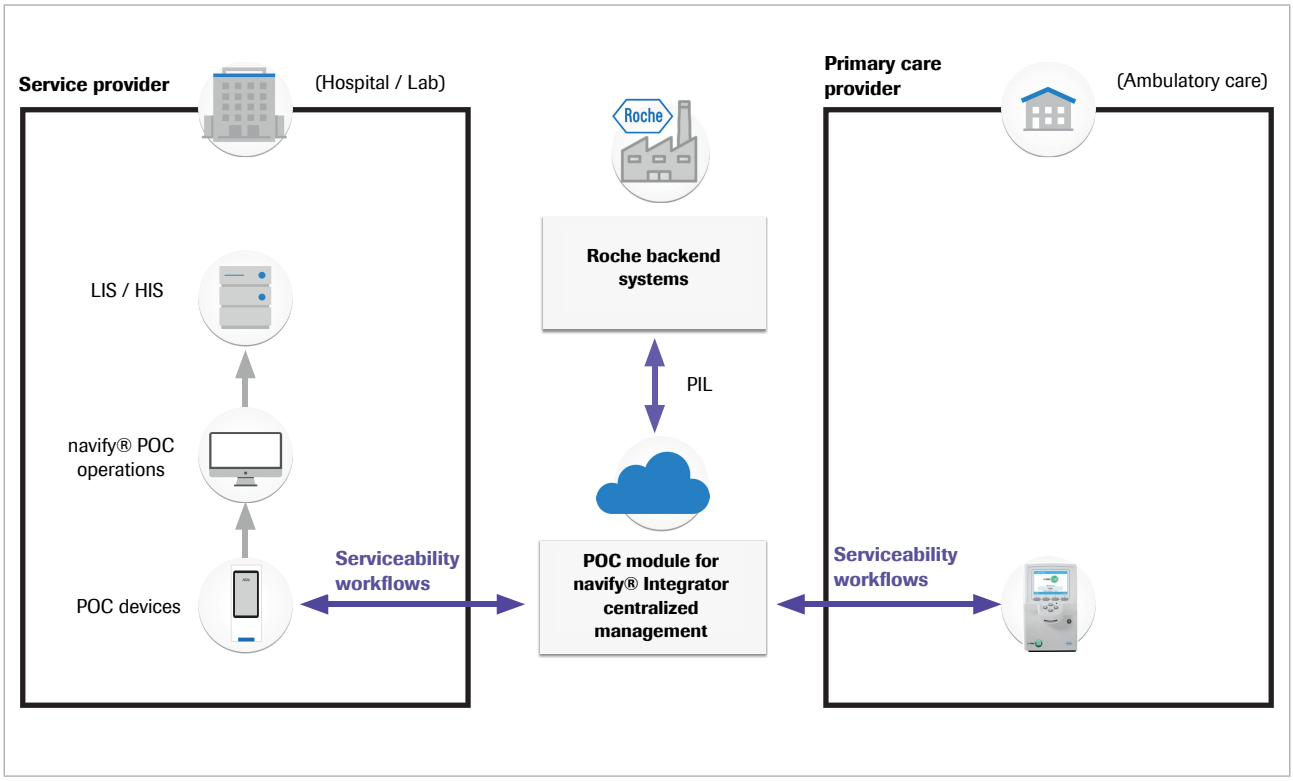
POC module for navify® Integrator offering

Another field of application of POC module for **navify**® Integrator is the service of new generation Roche POC devices (devices that can connect back to Roche to support specific service workflows). This will enable Roche to remotely maintain those POC devices in a secure way.

Supported serviceability workflows are:

- Installation, configuration, and registration
- Software distribution
- Lot data distribution
- Service data extraction

Secure serviceability connection for devices located at the POC service provider or in primary care provider locations:



POC module for **navify**® Integrator offering (serviceability)

Related topics

- Where to find information about the different offerings (27)
- About monitoring (57)
- About organizations (63)
- About gateways (69)
- About user management (127)

Where to find information about the different offerings

POC module for **navify**® Integrator is a single product that comprises a number of elements (different types of gateways and different capabilities in the Centralized Management (CM) system) that can be combined in different ways to provide the different offerings **navify**® Connector for Community and POC module for **navify**® Integrator.

Some sections of this manual describe core elements of the product and are relevant to all of these offerings. Other sections apply only to one offering. The list below shows which section of this manual applies to which offering.

Core elements relevant for all offerings

- Centralized management system operation
- Organization management
- Gateway management (sections related to POC device gateways)
- User management
- System settings

Sections relating to the navify® Connector for Community offering

- Gateway management (sections related to DMS gateways)
- POC device management

Sections relating to the POC module for navify® Integrator offering

- POC device configuration
- Software management
- Lot management

List of supported data management systems

The system supports the following data management systems:

- **navify**® POC Operations

For the **navify**® Connector for Community offering, **navify**® POC Operations 2.1.0 or higher is required.

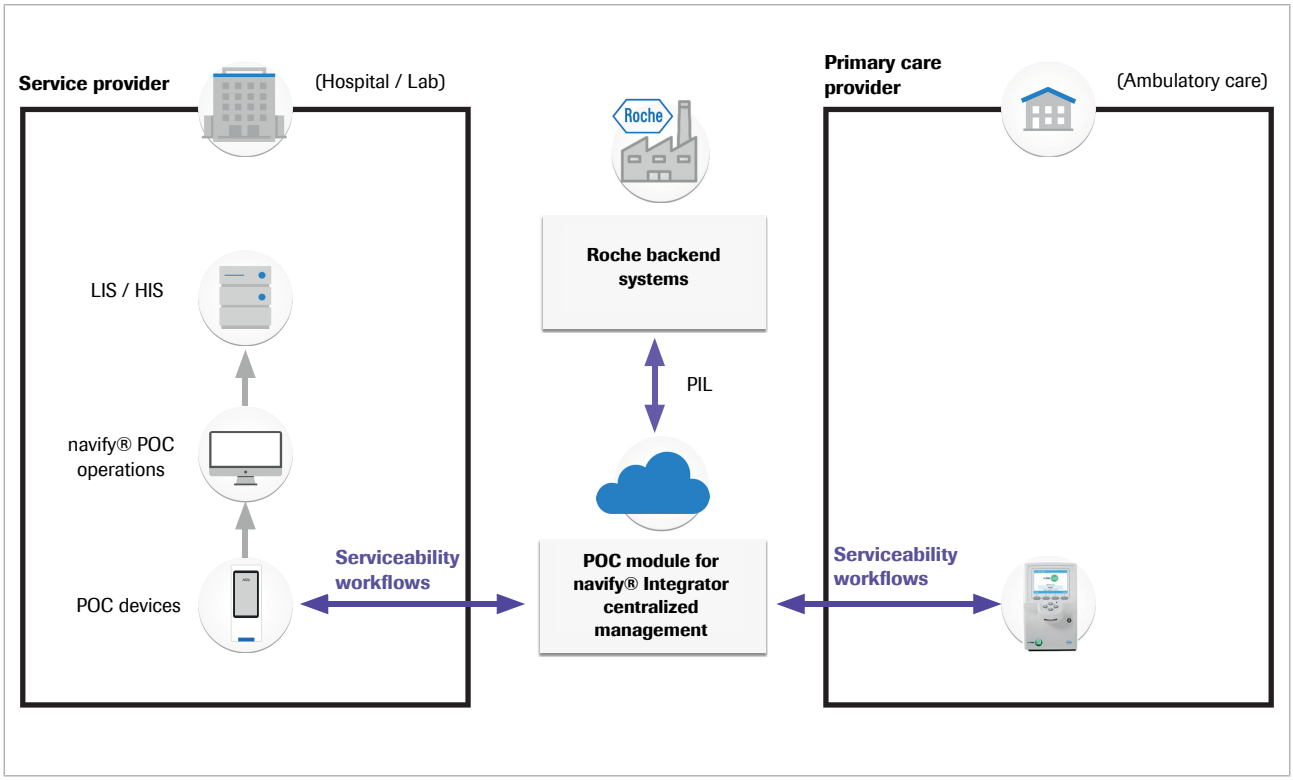
For the POC module for **navify**® Integrator 2.1 offering, the connection of new generation Roche POC devices to 3rd party DMS systems via the operational interface is also supported. The functionality depends on the implementation of the communication protocol of the 3rd party DMS provider.

About Roche backend systems

This chapter only applies to the POC module for **navify**® Integrator offering.

POC module for **navify**® Integrator connects the new generation Roche POC devices to a variety of Roche backend systems for the purpose of device registration (SAP sales and Rexis), instrument software distribution, lot data distribution, and service data extraction for different analytics platforms.

The communication between POC module for **navify**® Integrator and the Roche backend systems is bundled through the POC integration layer (PIL).



POC module for **navify**® Integrator offering (serviceability)

List of technical requirements

In this section

General requirements

Centralized management system requirements

The minimum screen resolution required to operate the centralized management system is 1024 x 768. The optimum screen resolution is 1920 x 1080.

The following browsers are recommended to access the centralized management system:

- Google Chrome
- Microsoft Edge
- Firefox
- Safari

Gateway connectivity requirements

To ensure system operation and gateway connectivity, you allow these mandatory URLs.

EU Instance

The following URL allows you to connect to the POC module for **navify**® Integrator portal:

- https://eu.cobas-infinity-edge.com

To retrieve the instrument specific certificates, the POC gateway needs to be to establish an outbound connection to the following URL's: This is applicable only if the instrument supports the retrieval of TEPI certificates via the POC gateway.

URL	Port	Protocol	Note
DPS:			

Gateway connectivity requirements (EU Instance)

URL	Port	Protocol	Note
https://global.azure-devices-provisioning.net	443	https & AMQP	Azure IoT Hub Device Provisioning Service (DPS)
https://dps-euprod-iconnect.azure-devices-provisioning.net	443	https	Azure IoT Hub Device Provisioning Service (DPS)
IoT Hub:			
https://iothub-euprod-iconnect.azure-devices.net	443	https	Azure IoT Hub endpoint
Storage accounts:			
https://swidextractstorageeuprod.blob.core.windows.net	443	https	Storage path for software packages
https://stpilpackagestorageprod.blob.core.windows.net	443	https	Storage path for lot data
https://servicedatastorageeuprod.blob.core.windows.net	443	https	Storage path for service data
https://appauditlogseuprod.blob.core.windows.net	443	https	Storage path for audit and activity information
https://euprodgatewaydriverfile.blob.core.windows.net	443	https	Storage path for gateway driver files
https://euprodgwmsgstore.blob.core.windows.net	443	https	Storage path for gateway logs
https://euprodinstrumentdrivers.blob.core.windows.net	443	https	Storage path for instrument driver files
URLs required for certificate validation:			
http://ocsp.digicert.com	80	OCSP	DigiCert OCSP responder
http://crl3.digicert.com	80	https	DigiCert CRL distribution point
http://crl4.digicert.com	80	https	DigiCert CRL distribution point
http://cacerts.digicert.com	80	https	DigiCert certificate chain
http://crl-pki-rd.roche.com	80	http	Roche CRL distribution point
Others:			
https://euapi.cobas-infinity-edge.com/gwapi	443	https	API Interface for gateways
https://eu.cobas-infinity-edge.com	443	https	Web UI for management portal

Gateway connectivity requirements (EU Instance)

US Instance

The following URL allows you to connect to the POC module for **navify**® Integrator portal:

- https://us.cobas-infinity-edge.com

Use the following URLs and ports for the POC device gateway, and DMS gateway (US Innstance):

URL	Port	Protocol	Note
DPS:			
https://global.azure-devices-provisioning.net	443	https	Azure IoT Hub Device Provisioning Service (DPS)
https://dps-usprd-iconnect.azure-devices-provisioning.net	443	https	Azure IoT Hub Device Provisioning Service (DPS)
IoT Hub:			
https://iothub-usprd-iconnect.azure-devices.net	443	https	Azure IoT Hub endpoint
Storage accounts:			
https://swidextractstorageeuprod.blob.core.windows.net	443	https	Storage path for software packages
https://stpilpackagestorageprod.blob.core.windows.net	443	https	Storage path for lot data
https://servicedatastorageeuprod.blob.core.windows.net	443	https	Storage path for service data
https://appauditlogsusprd.blob.core.windows.net	443	https	Storage path for audit and activity information
https://usprdgatewaydriverfile.blob.core.windows.net	443	https	Storage path for gateway driver files
https://usprdgwmsgstore.blob.core.windows.net	443	https	Storage path for gateway logs
https://usprdinstrumentdrivers.blob.core.windows.net	443	https	Storage path for instrument driver files
URLs required for certificate validation:			
http://ocsp.digicert.com	80	OCSP	DigiCert OCSP responder
http://crl3.digicert.com	80	https	DigiCert CRL distribution point
http://crl4.digicert.com	80	https	DigiCert CRL distribution point

Gateway connectivity requirements (US Instance)

URL	Port	Protocol	Note
http://cacerts.digicert.com	80	https	DigiCert certificate chain
http://crl-pki-rd.roche.com	80	http	Roche CRL distribution point
Others:			
https://usapi.cobas-infinity-edge.com/gwapi	443	https	API interface for gateways
https://us.cobas-infinity-edge.com	443	https	Web UI of management portal

Gateway connectivity requirements (US Instance)

TEPI servers

Trust Establishment for Post-market Instruments (TEPI) servers are a way to improve security by getting certificates onto devices that are already on the market.

Use the following URLs to access the TEPI servers for various instruments (EU and US instance):

URL[a]	Port	Protocol	Note
https://liat.tepi.navify.com	443	https	This service distributes security certificates for cobas Liat.
https://hbm.tepi.navify.com	443	https	This service distributes security certificates for CCP2.
https://b123.tepi.navify.com	443	https	This service distributes security certificates for cobas b123.

(a) Only applicable if this instrument type is used and the instrument firmware supports certificate retrieval from TEPI server via edge gateway.

TEPI servers

The following ports can be configured before gateway installation and activation:

Ports to be allowed for inbound connections[a][b]	Port	Protocol
Web API proxy:		
Reverse proxy for cobas Liat	58011	https
Reverse proxy for cobas b123	58012	https
Reverse proxy for CoaguChek Pro II	58013	https

(a) Ports to be allowed for inbound connections from instruments connected to the local network. You do not need an internet connection to reach ports.

(b) Only applicable if this instrument type is used and the instrument firmware supports certificate retrieval from TEPI server via edge gateway.

Ports connectivity requirements

navify® Connector for Community requirements

Minimum hardware requirements for POC device gateways

In scenario 1, an average office computer is described. Other applications may be running in parallel with the POC device gateway.

In scenario 2, a miniature computer is described. This is a dedicated, low-budget computer where no other applications are being run.

	Scenario 1	Scenario 2
Minimum CPU type	64 bit Intel i5 core or similar	Intel Atom X5 or similar
Minimum CPU cores	2	4
Minimum CPU performance	1.6 GHz	1.4 GHz
Minimum free memory (RAM)	8 GB	8 GB
Minimum free hard disk storage space	20 GB	20 GB
Network interface cards	1	1

Minimum POC device gateway hardware requirements

Minimum hardware requirements for DMS gateways

The DMS gateway must be installed on the same server the DMS is hosted.

The minimum requirements for a DMS gateway depend on the expected number of POC devices that will be connected.

In scenario 1, medium, the number of POC devices connected is less than 300.

In scenario 2, large, the number of POC devices connected is greater than 300.

	Scenario 1: Medium	Scenario 2: Large
Minimum CPU type	64 bit Intel Xeon or similar	64 bit Intel Xeon or similar
Minimum CPU cores	4	4
Minimum CPU performance	2.4 GHz	2.4 GHz
Minimum free memory (RAM)	4 GB	8 GB
Minimum free hard disk storage space	20 GB	40 GB
Network interface cards	1	1

Minimum DMS gateway hardware requirements

Minimum software requirements for POC device gateways

For the installation and activation of a POC device gateway, the following is required:

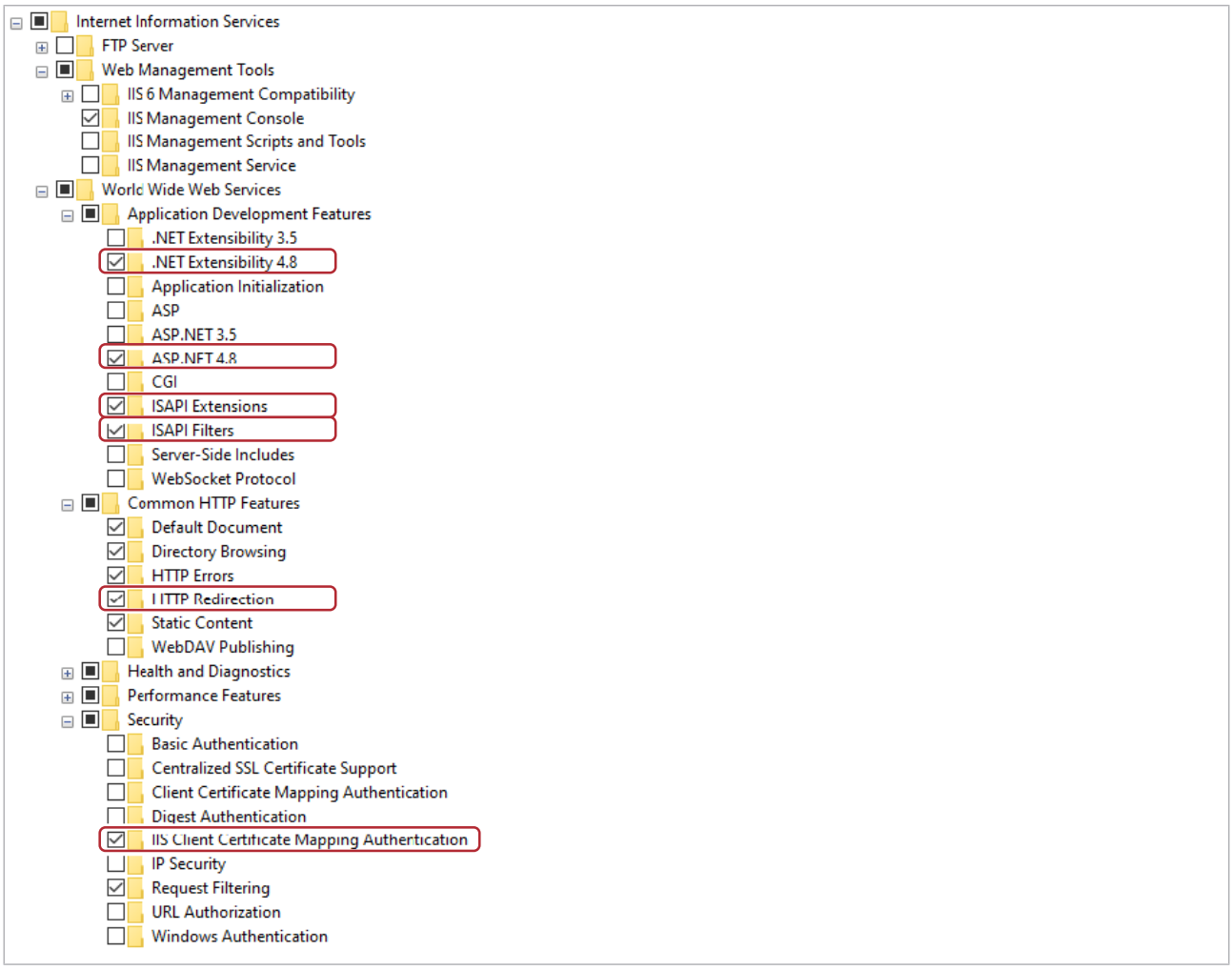
- The host machine is configured with a fixed IP address in the local network.
- The gateway software can be installed only on systems with Windows Volume marked as “C” i.e., Windows programs must be installed on the C drive of the system.
- The user performing the installation has full local administrative rights.
- IIS must be enabled before installation of the gateway (see instructions below).
- The following ports are internally used by the gateway and must not be used by any other applications. All incoming traffic shall be blocked in the firewall on these ports:
  - Port 21101, 21102, and 21105: Gateway UI

Important: It is highly recommended to manually check the firewall configuration after installation of the gateway to ensure that all communication is blocked on these ports.

	Minimum requirements	Responsible for installation
Supported operating systems	• Windows 10 Professional or Enterprise edition (64 bit) • Windows 11 Professional or Enterprise edition (64 bit)	Customer
.NET	8.0	Customer
.NET Framework version	.NET 4.8.3928.0 or higher	Customer
IIS subcomponents	See image below	Customer
Communication server	1.21.0.10909	Gateway installer
Driver framework	4.3.0.13634	Gateway installer

Minimum POC device gateway software requirements

To enable IIS subcomponents, go to **Control Panel > Programs and Features > Turn Windows features on or off**.



Minimum IIS subcomponents for POC device gateways

Minimum software requirements for DMS gateways

For the installation and activation of a DMS gateway, the following is required:

- The host machine is configured with a fixed IP address in the local network.
- The gateway software can be installed only on systems with Windows Volume marked as “C” i.e., Windows programs must be installed on the C drive of the system.
- The user performing the installation has full local administrative rights.
- The following ports are internally used by the gateway and must not be used by any other applications. All incoming traffic shall be blocked in the firewall on these ports:
  - Port 21101, 21102, and 21105: Gateway UI

Important: It is highly recommended to manually check the firewall configuration after installation of the gateway to ensure that all communication is blocked on these ports.

	Minimum requirements	Responsible for installation
Supported operating systems	• Windows Server 2012 R2 (64 bit) • Windows Server 2016 (64 bit) • Windows Server 2019 (64 bit) • Windows Server 2022 (64 bit)	Customer
.NET	8.0	Customer
.NET Framework version	.NET 4.8.3928.0 or higher	Customer
IIS version	Default version installed with Windows Server version	Roche Service representative
IIS subcomponents	Same as host DMS	Roche Service representative
DMS	**navify**® POC Operations application version 2.1.0 or higher	Roche Service representative

Minimum DMS gateway software requirements

POC module for navify® Integrator requirements

Minimum hardware requirements for POC device gateways

When using **navify**® Connector for Community and POC module for **navify**® Integrator, the POC device gateway and the DMS gateway must be installed on different servers.

No miniature computer is supported for POC module for **navify**® Integrator.

	Scenario 3
Roche devices	500
Minimum CPU type	64 bit Intel Core i5 or similar
Minimum CPU cores	2
Minimum CPU performance	1.6 GHz
Minimum free memory (RAM)	6 GB
Minimum free hard disk storage space	20 GB

Minimum POC device gateway hardware requirements

Minimum software requirements for POC device gateways

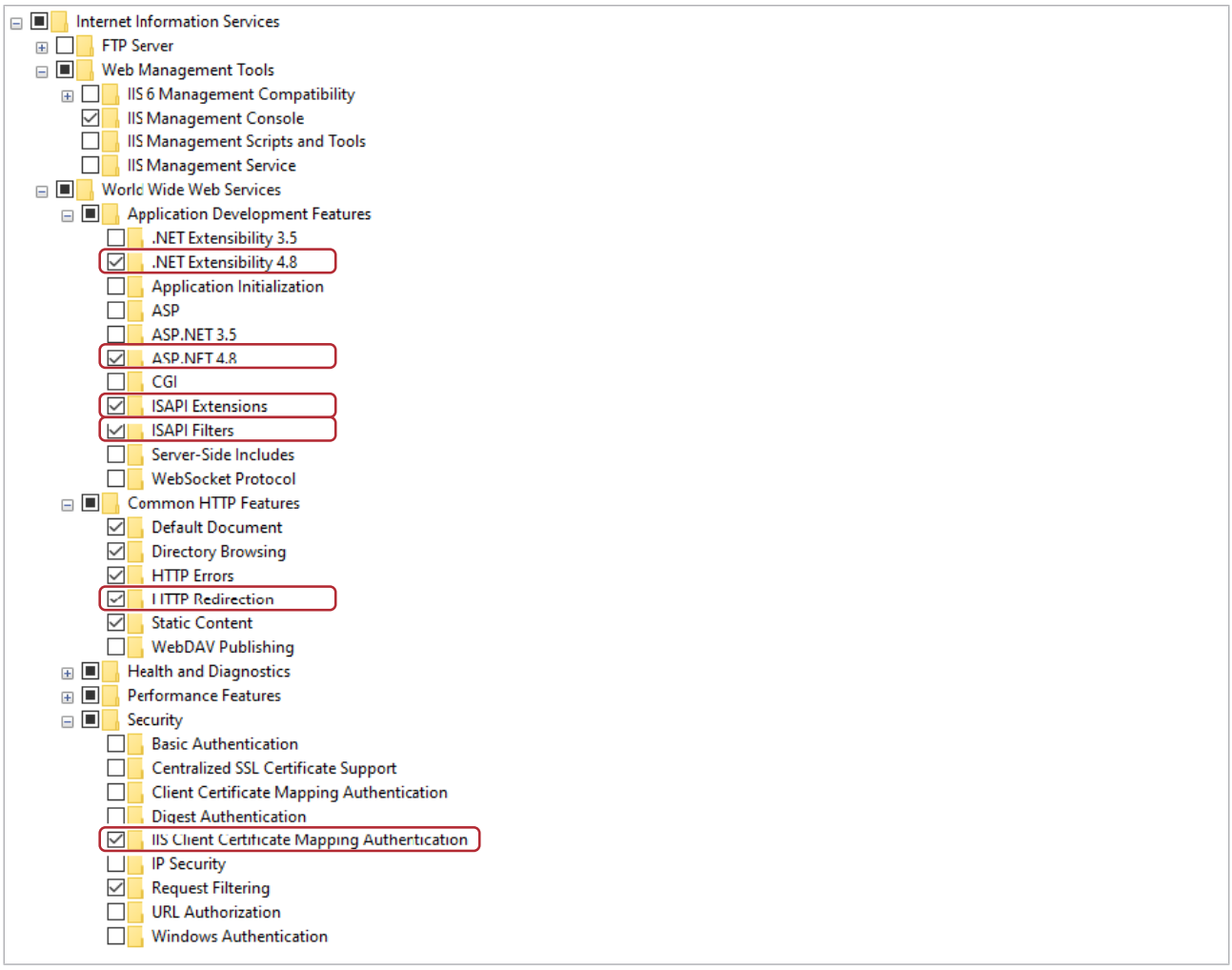
For the installation and activation of a POC device gateway, the following is required:

- The host machine is configured with a fixed IP address in the local network.
- The user performing the installation has full local administrative rights.
- The port used by each POC device is allowed by the Windows firewall.

	Minimum requirements	Responsible for installation
Supported operating systems	• Windows 10 Professional or Enterprise edition (64 bit) • Windows 11 Professional or Enterprise edition (64 bit) • Windows Server 2012 R2 (64 bit) • Windows Server 2016 (64 bit) • Windows Server 2019 (64 bit) • Windows Server 2022 (64 bit)	Customer
.NET	8.0	Customer
.NET Framework version	.NET 4.8.3928.0 or higher	Customer
IIS version	Default version installed with Windows Server version	Customer
IIS subcomponents	See image below	Customer

Minimum POC device gateway software requirements

To enable IIS subcomponents, go to **Control Panel > Programs and Features > Turn Windows features on or off**.



Minimum IIS subcomponents for POC device gateways

List of user roles and permissions

Users are only able to see areas of the system that they have permission to work in. This documentation only shows users the tasks and actions that their role allows them to perform.

To give an understanding of what another user at the same or lower level can do, the following tables contain a map of possible user actions.

For information regarding an action that is not shown here, contact your system administrator.

Centralized management system operation task	Primary care provider administrator	Primary care provider user
Logging on for the first time	✓	✓
Logging on	✓	✓
Logging off	✓	✓
Viewing notifications	✓	✓
Changing password	✓	✓
Changing profile settings	✓	✓

Centralized management system operation

Monitoring task	Primary care provider administrator	Primary care provider user
Monitoring primary care providers	✓	✓
Monitoring POC device gateways	✓	✓
Monitoring POC devices	✓	✓

Monitoring

Organization management task	Primary care provider administrator	Primary care provider user
Viewing organizations	✓	✗
Changing organization primary contact	✓	✗

Organization management

Gateway management task	Primary care provider administrator	Primary care provider user
Viewing gateways	✓	✗
Creating POC device gateways	✓	✗
Downloading POC device gateway software	✓	✗
Installing POC device gateway software	✓	✗
Activating gateway software	✓	✗
Editing gateway details	✓	✗
Changing gateway activation status	✓	✗
Deleting DMS gateways	✓	✗
Deleting POC Device gateways	✓	✗

Gateway management

POC device management task	Primary care provider administrator	Primary care provider user
Viewing connected POC device types	✓	✗
Connecting POC device types	✓	✗
Editing connected POC device types	✓	✗
Changing connectivity status of POC device types	✓	✗

POC device management

POC device management task	Primary care provider administrator	Primary care provider user
Viewing connected POC device types	✓	✗
Connecting POC device types	✓	✗
Editing connected POC device types	✓	✗
Changing connectivity status of POC device types	✓	✗

POC device management

Lot management task	Primary care provider administrator	Primary care provider user
Scanning QR code of a strip lot with POC device	✓	✗
Adding strip lot to POC device	✓	✓

Lot management

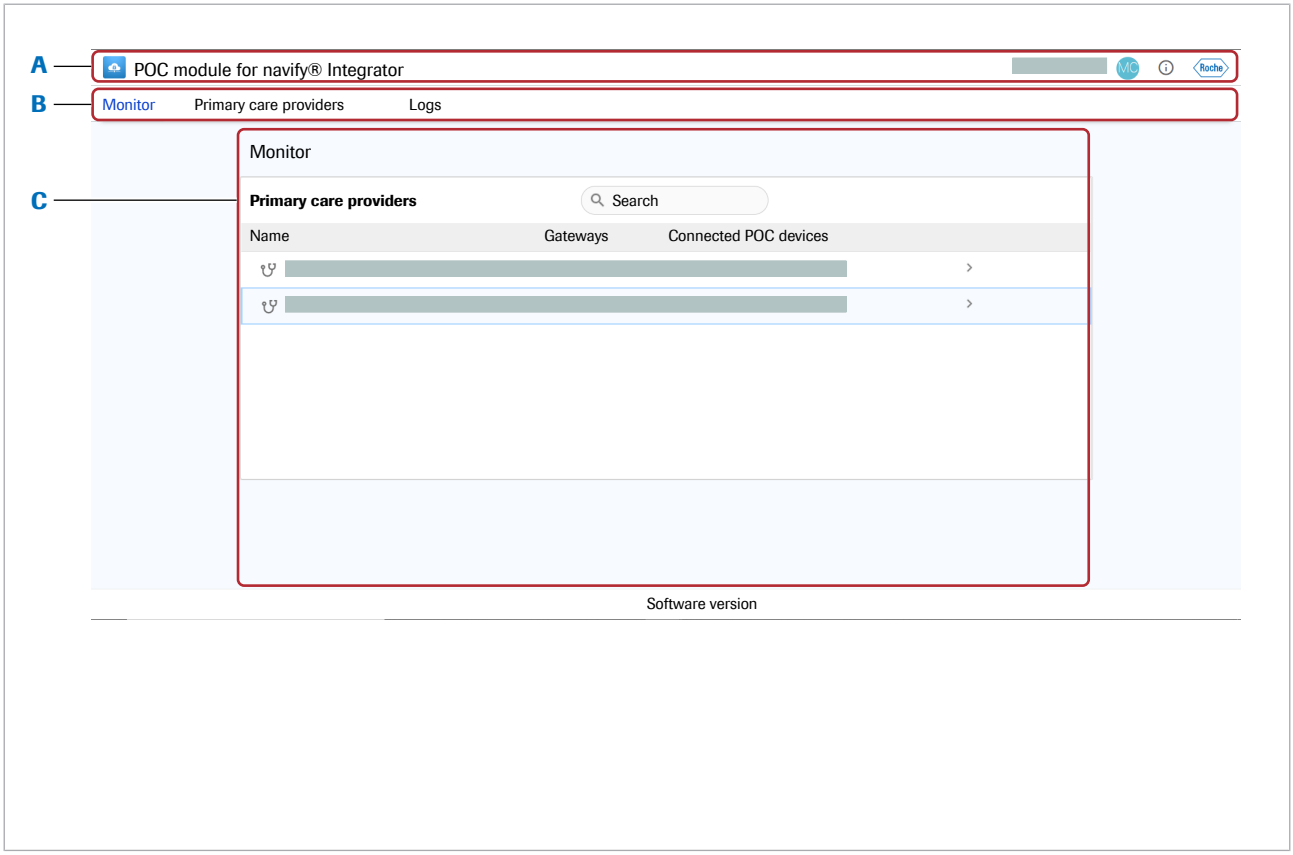
User management task	Primary care provider administrator	Primary care provider user
Viewing users	✓	✗
Creating users	✓	✗
Deleting users	✓	✗
Editing user details	✓	✗
Editing organizations a user is assigned to	✓	✗
Resetting user password	✓	✗

User management

Troubleshooting task	Primary care provider administrator	Primary care provider user
Viewing logs	✓	✗
Exporting centralized management system log files to CSV	✓	✗
Restarting gateways	✓	✗

Troubleshooting

Overview of the user interface



A Global information area

B Navigation bar

C Main panel

Global information area

From the global information area, the following can be accessed:

- Edit your profile settings.
- Access the User Assistance, about box, and software licenses information area.

Navigation bar

From the navigation bar, the following system sections can be accessed:

- Monitor
- Organizations
- Users
- Logs
- Settings

Main panel

The information on the main panel is dependent on where in the application the user is. See individual tasks for more detailed descriptions of each section.

Operation

Page intentionally left blank.

Centralized management system operation

In this chapter 3

Page intentionally left blank.

Logging on for the first time

When a user logs on for the first time, they are prompted to set their password for future access. If this prompt does not appear, the account may be compromised and the local system administrator should be contacted immediately.

- ☐ An account is created in the system.
- ☐ The user receives an email with one-time logon credentials.

To log on for the first time

1. On the logon screen, enter the user name and one-time password.
   → A screen prompting the user to change the password is displayed.
2. Enter a new password.
3. Confirm the new password.
4. Choose the **Save** button.

Related topics

- About user account and password (52)

Logging on

To access the system you must log onto the system in a browser.

- ☐ A valid user account with access rights exists.
- ☐ A valid browser.
- ☐ Pop-up messages are allowed in the browser settings.

To log on

1. On the logon screen, enter your email address.
2. Choose the **Log on** button.
3. Enter your password.
4. Choose the **Sign in** button.

Related topics

- About user account and password (52)

Logging off

You can log off from the home screen of the application.

To log off

1 Choose the jd button.

ⓘ The initials in the profile button change according to the user.

2 Choose the **Log off** button.

➔ A confirmation message is displayed.

About user account and password

Apply precautions to your account and password in the system to ensure that security is not compromised.

Apply the following precautions:

- Ensure that there are no entries in any configuration file or name within the system relating to user names or passwords.
- Users are not allowed to share their user accounts.

The system requires strong passwords. The characteristics of strong passwords are as follows:

- Passwords cannot contain the user name or a part of the name of the user that exceeds 2 consecutive characters.
- Passwords must be at least 8 characters in length.
- Passwords must contain characters from 3 of the following 4 categories:
  - English upper-case characters (A through Z).
  - English lower-case characters (a through z).
  - Digits from 0 through 9.
  - Special characters (!, $, #, %).

Changing passwords

A new password can be set at any time.

To change a password

1 Choose the jd button.

2 On the profile panel, choose **Profile settings**.

3 Choose the **State** accordion item.

4 Enter the fields.

5 Choose the **Name** button.
➔ A confirmation message is displayed.

Related topics

- About user account and password (52)

Changing profile settings

The following profile settings can be changed:

- Display language
- Time format
- Time zone
- Date format

To change profile settings

1 Choose the jd button.

2 On the profile panel, choose **Profile settings**.

3 On the **Profile settings** accordion item, adjust the system profile settings.

4 Choose the **Save** button.

➔ A confirmation message is displayed.

Monitoring

In this chapter 4

Page intentionally left blank.

About monitoring

Monitoring provides an overview of all connected organizations, gateways, and POC devices. An organization, gateway, or POC device can only be monitored if it is active. A user can only see monitoring details for an organization or gateway that is at the same or lower level as the user.

The following can be monitored:

- Primary care provider
- POC device gateway
- POC devices

Monitoring primary care providers

The following primary care provider attributes can be monitored:

- The number of associated gateways.
- The number of connected POC devices, which shows the number of currently connected devices out of the total number of devices known to be associated with the primary care provider by the system.
- The phone number and email address of the primary contact.

To monitor primary care providers

1 Choose the **Monitor** tab.

➔ High-level details of the primary care providers the user is assigned to are displayed.

2 For more detailed information, choose the > button for the appropriate primary care provider.

➔ The **Details** and **Gateways** for the chosen primary care provider are displayed.

Monitoring POC device gateways

POC device gateways can be monitored by accessing more detailed information about the primary care provider that they are connected to.

The following gateway attributes can be monitored:

- Gateway name
- Gateway ID
- Connection status
- Activation status
- Number of connected POC devices
- Gateway software version
- Gateway IP address
- Gateway host name

The connection status of a POC device gateway is **Connected** as long as there is a heartbeat between the POC device gateway and the centralized management system at least once every 30 minutes. If there is no heartbeat for more than 30 minutes, the connection status is **Disconnected**.

The connection status of a POC device is **Connected** as long as an acknowledgment message from the centralized management system is received by the POC device gateway within the defined timeout. If no acknowledgement message is received within the defined timeout, the connection status is **Disconnected**. The timeout period can be set individually for the operational interface and the service interface in **System settings > POC device disconnection threshold**.

To monitor POC device gateways

1. Choose the **Monitor** tab.
2. Choose the **POC device gateways** tab.
   → High-level details of the connected POC device gateways are displayed.
3. For more detailed information, choose the > button for the appropriate gateway.
   → The **Details** and **Connected POC devices** for the chosen gateway are displayed.

Related topics

- Deleting gateways (85)
- Creating POC device gateways (77)

Monitoring POC devices

The following POC device attributes can be monitored:

- POC device name
- Connection status to operational interface and service interface:
  - Connected - communication has occurred within the defined timeout
  - Disconnected - no communication has occurred within the defined timeout
- Date and time of last communication
- POC device type
- POC device serial number
- POC device firmware version
- POC device hardware version

To monitor POC devices

1. Choose the **Monitor** tab.
2. On the **Primary care providers** panel, choose the › button for the appropriate primary care provider.
3. On the **POC device gateways** panel, choose the › button for the appropriate POC device gateway.
4. Choose the ⌄ button in the row of the appropriate POC device.
   ➔ The POC device details accordion item is expanded.

Related topics

- Enabling POC device types (95)

Organization management

In this chapter 5

Page intentionally left blank.

About organizations

An organization is responsible for the service or operation of a part of the system. The organization types are as follows.

Organization type	Description
Roche affiliate	A Roche affiliate refers to the organization responsible for delivering and maintaining Roche products in individual countries. This organization is responsible for the high-level maintenance and support of the application, including creating associated POC service provider organizations and users. Multiple POC service providers and primary care providers can be associated with a single Roche affiliate.
POC service provider	A POC service provider refers to a hospital, laboratory, or primary care facility which is a direct customer of Roche Diagnostics. In the **navify**® Connector for Community offering, the POC service provider is responsible for the management of its related primary care providers.
primary care provider	A primary care provider refers to organizations including pharmacies, general practitioners offices, elderly care sites, etc. which are direct customers of a POC service provider in the **navify**® Connector for Community offering.

Organization types

Viewing organizations

Administrators can see a list of organizations that they are assigned to or have administrator rights over.
Administrators cannot view an organization that they are a part of if it is made inactive.

To view organizations

1 Choose the **Primary care provider** tab and navigate to the organization.

2 To see additional information about an organization, choose the > button in the row of the organization.
➔ The organization details screen is displayed.

Related topics

- About organizations (63)

Changing organization primary contact

The primary contact of a primary care provider can be changed.

An organization can only have 1 primary contact.

To change the primary contact of an organization

1 Choose the **Primary care provider** tab and navigate to the organization.

2 Choose the **Primary contact** tab.

3 Choose the **Edit primary contact** button.

4 Choose the new primary contact.

The new primary contact must be an administrator assigned to the same entity.

5 Choose the **Save** button.

➔ A confirmation message is displayed.

Related topics

- Deleting users (130)
- Creating additional users (129)

Page intentionally left blank.

Gateway management

In this chapter 6

Page intentionally left blank.

About gateways

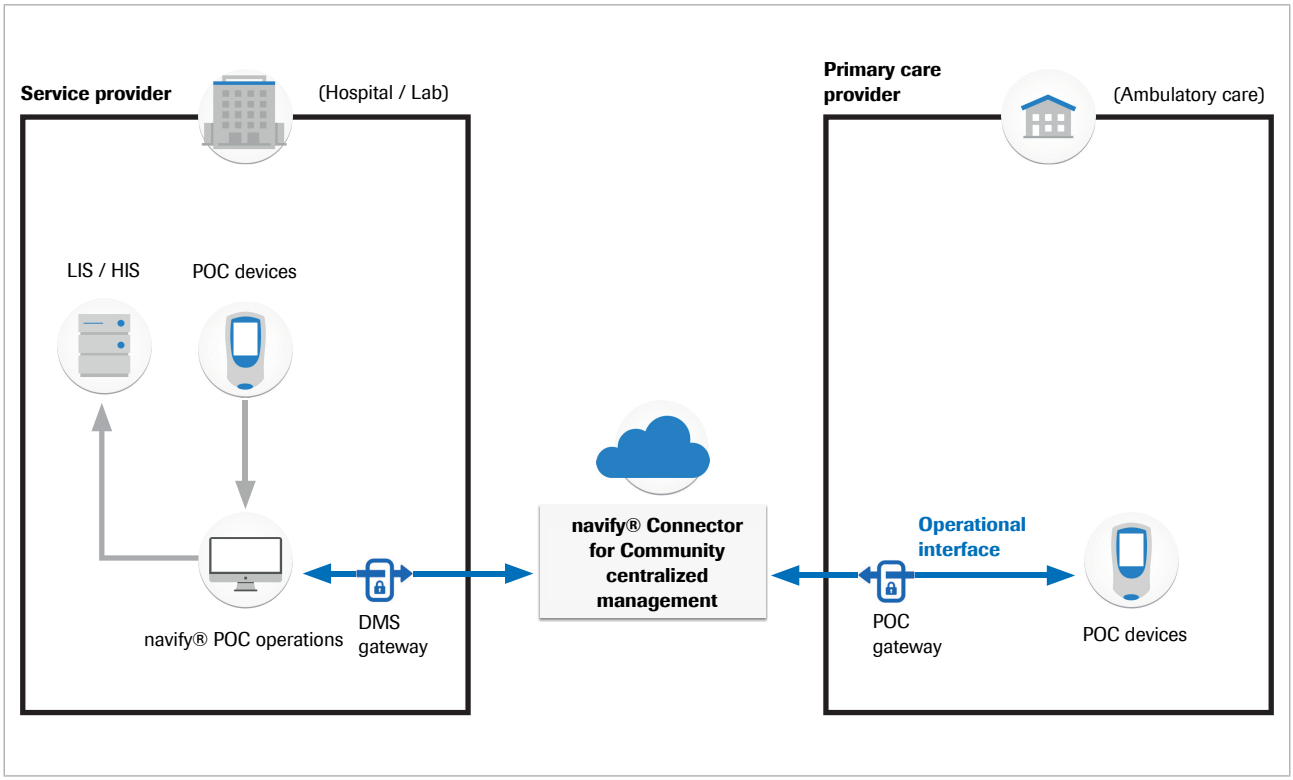
Gateways allow for secure and encrypted transmission of data between the centralized management system, local networks, and connected applications or devices. They enable information to be sent securely over the internet.

A gateway is created for each external system that is connected to the system. Supported external systems include data management systems (DMS) and POC devices. The gateway is hosted in a private network that allows for a connection to the cloud.

During the installation of the gateway, it is possible that certain antivirus applications are quarantining executable files. In this case, you need to stop the antivirus application temporarily during the gateway installation or customer IT needs to apply the required exception/exclusion.

navify® Connector for Community

Gateway deployment overview for the **navify®** Connector for Community offering:



navify® Connector for Community offering

For this offering, the POC gateway is installed on a host machine in the primary care provider network and hosts the instrument drivers which enable a secure communication via the operational interface of the POC

devices to the centralized management system. The instrument drivers hosted on a specific POC gateway are managed through the centralized management system.

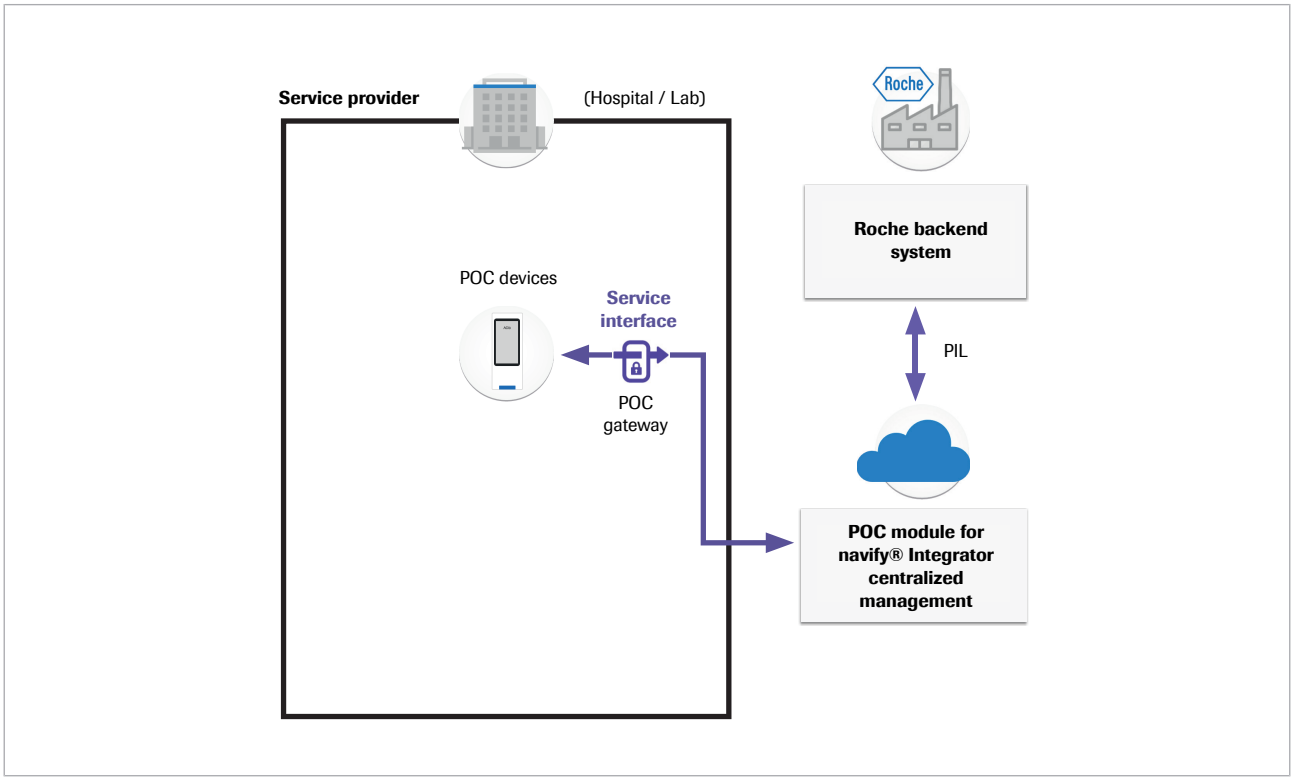
The DMS gateway must be installed on the same server where the DMS (**navify**® POC Operations) is hosted and enables a secure communication between the DMS and the centralized management system.

The data that can be communicated between a POC device gateway (via operational interface) and the DMS gateway includes the following:

- Patient results
- QC results
- Patient lists
- Operator lists
- Test lots
- QC lots
- Configurations needed for POC device governance
- POC device firmware upgrades
- POC device events

POC module for navify® Integrator

Gateway deployment overview for the POC module for **navify**® Integrator offering:



POC module for **navify**® Integrator offering

For this offering, the POC gateway is installed on a host machine located in the service provider network and establishes a secure connection via the service interface between the new generation ROCHE POC devices and the centralized management system.

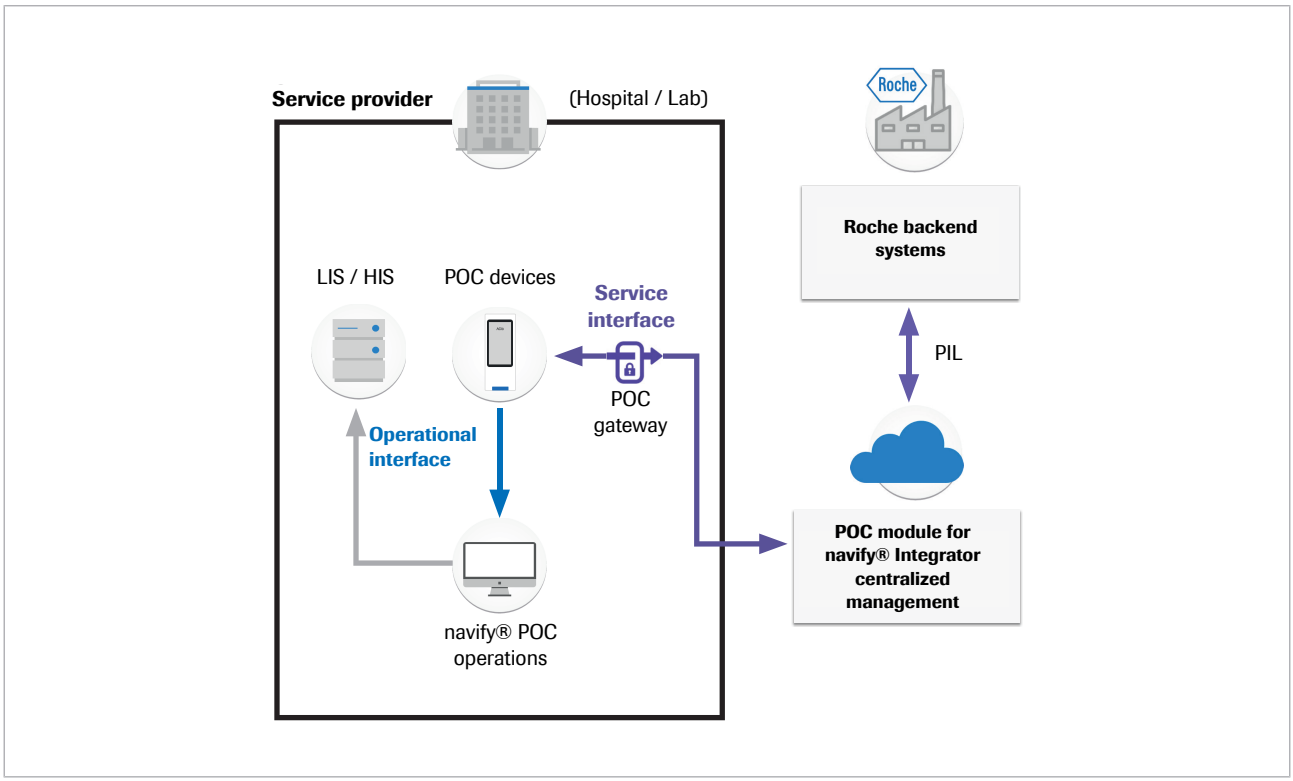
The following serviceability features are available:

- Supported WLAN Security:
  - WPA/WPA2 Personal
- Installation, configuration, and registration:
  - For the Roche device[1] configuration, only POC module for **navify**® Integrator is used:
    - WPA2 personal WLAN settings
    - Roche device[2] settings
  - Roche device[s(2)] are automatically registered in Rexis/SAP sales
- Software distribution:
  - Software distribution and scheduling in POC module for **navify**® Integrator for Roche software packages and 3rd party applications[2]
- Lot data distribution:
  - Barcode scanning of test strip containers on a Roche device[2]. The Roche device[2] then retrieves the lot information via service interface from POC module for **navify**® Integrator.
  - QR code scanning of a specific lot directly in POC module for **navify**® Integrator
- Service data extraction:
  - Automatic service data extraction from Roche devices[2] via POC module for **navify**® Integrator according to the configured level of the **Anonymous-data sharing setting** option.
  - Distribution of service data to consumers in Roche backend via the PIL interface

POC module for navify® Integrator + DMS

Gateway deployment overview for the POC module for **navify**® Integrator offering with DMS:

[1] Only applicable to Roche products that support service interface.



POC module for **navify**® Integrator offering with DMS

For this offering, the POC gateway is installed on a host machine located in the service provider network and establishes a secure connection via the service interface between the new generation Roche POC devices and the centralized management system. In this scenario, the POC gateway cannot be installed on the same host machine where the DMS (**navify**® POC Operations) is installed.

The following serviceability features are available:

- Supported WLAN Security:
  - WPA/WPA2 Personal
  - WPA/WPA2 Enterprise (only via DMS)
- Installation, configuration, and registration:
  - Small configuration in POC module for **navify**® Integrator:
    - WPA2 Personal WLAN settings
    - DMS IP and port
  - Only DMS is used for the Roche device[2] configuration:
    - WPA2 Personal WLAN settings
    - WPA2 Enterprise WLAN settings (EAP)
    - Full Roche device[3] configuration
  - Roche devices[3] are automatically registered in Rexis/SAP sales
- Software distribution:

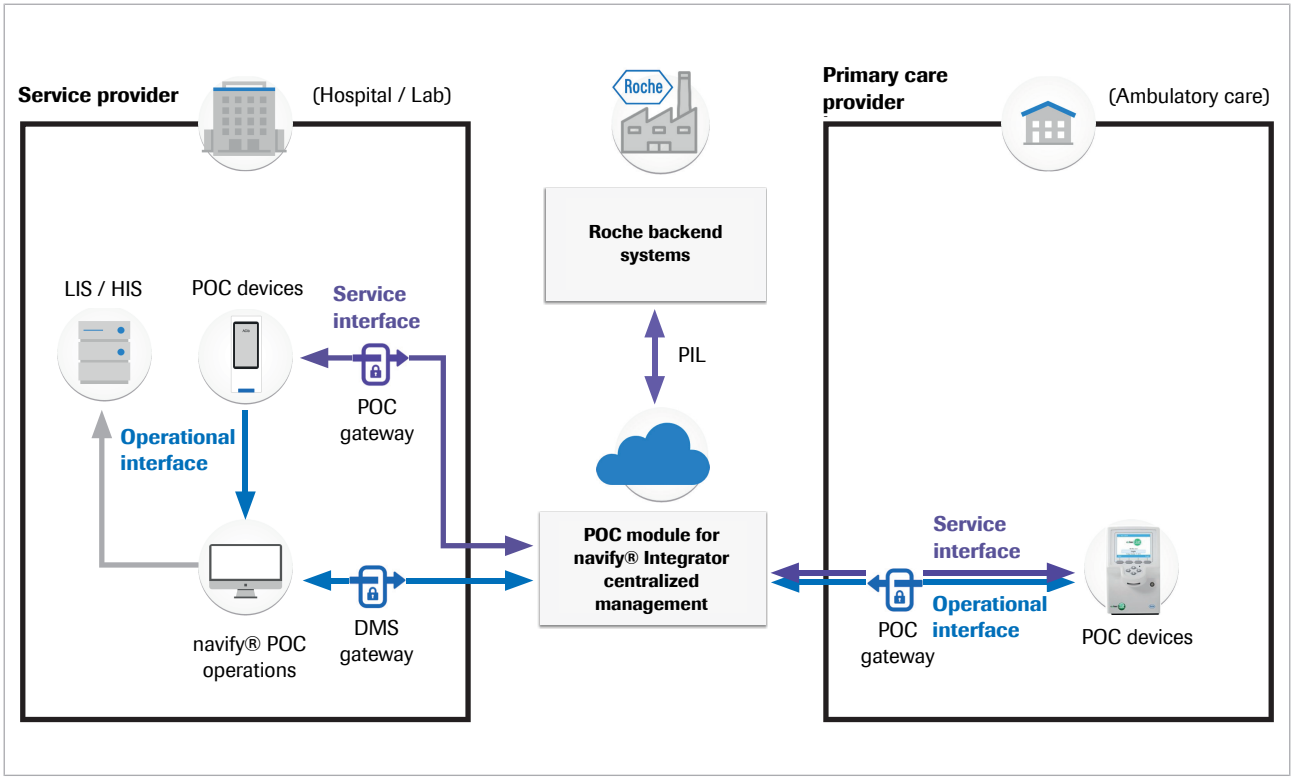
[2] Only applicable to Roche products that support service interface.

- Software distribution and scheduling in POC module for **navify**® Integrator for Roche software packages and 3rd party applications[3]

- Lot data distribution:
  - Barcode scanning of test strip containers on Roche devices[3]. The Roche device[3] then retrieves the lot information via service interface from POC module for **navify**® Integrator.
  - QR code scanning of a specific lot directly in POC module for **navify**® Integrator
  - Lot distribution to specific locations via DMS
  - Automatic lot distribution to Roche devices[3] via DMS
- Service data extraction:
  - Automatic service data extraction from Roche devices[3] via POC module for **navify**® Integrator according to the configured level of the **Anonymous-data sharing setting** option.
  - Distribution of service data to consumers in Roche backend via the PIL interface

POC module for navify® Integrator + DMS combined with navify® Connector for Community

Gateway deployment overview for the POC module for **navify**® Integrator offering with DMS combined with the **navify**® Connector for Community offering:



POC module for **navify**® Integrator offering with DMS combined with the **navify**® Connector for Community offering

This scenario combines the features of the POC module for **navify**® Integrator and the **navify**® Connector for Community offering. In this scenario, the POC gateway which is used for the service provider cannot be installed on the same server which hosts the DMS (**navify**® POC Operations) and the DMS gateway! The POC gateway which is installed on a host machine in the primary care provider network connects to the POC devices via service and operational interface.

Accessing gateway user interface

The gateway user interface can be accessed locally on the machine where the gateway is installed. Basic troubleshooting and maintenance tasks can be performed through the interface. The DMS and POC device gateways can all be accessed in the same way.

☐ The gateway is activated.

To access the gateway user interface

1 On the desktop, choose the **cobas infinity edge** gateway shortcut.

➔ The gateway user interface is launched in the default browser.

Viewing gateways

DMS and POC device gateways can be viewed.

To view gateways

1. Choose the **Primary care provider** tab and navigate to the organization.
2. In the row of the organization that hosts the appropriate gateways, choose the › button.
3. Choose the **Software** accordion and choose the **DMS** or **POC device** tab.
4. To see additional information about a gateway, choose the › button in the row of the gateway.
   → The gateway data screen is displayed.

Related topics

- About gateways (69)

Creating POC device gateways

- Ensure that the host machine can meet the technical requirements of the gateway.
- When adding the device types that the POC device gateway will support, default ports are provided. Check with the local IT of the primary care provider to confirm that the default POC device type ports can be used. If they cannot be used, ensure that a list of desired ports is provided.

- ☐ The primary care provider is created.
- ☐ The POC device types that will be connected to the gateway are known.
- ☐ The default POC device type ports can be used or the desired ports are known.

To create a POC device gateway

1. Choose the **Primary care provider** tab.
2. In the row of the appropriate primary care provider, choose the › button.
3. Choose the **Software** accordion item.
4. Choose the **Create POC device gateway** button.
5. In the **Gateway** accordion item, enter the gateway name.
6. Choose the **Next** button.
   ➔ To enable remote access for Roche 1st and 2nd level support via Roche ThingWorx Platform (RTP), make sure the **Remote support** toggle button is switched on.
7. From the **DMS gateway name** drop-down list, choose the name of the associated gateway.
8. In the **POC device types** section, select each POC device type that will be connected to the gateway.
9. Choose the **Save** button.
   ➔ A confirmation message is displayed.

Once the gateway is created, the gateway activation key that is generated is only valid for 5 days. If the gateway is not activated within that time, a new gateway must be created.

Downloading POC device gateway software

Once a gateway is created, the gateway software can be downloaded. It can then be installed and configured.

- Contact local IT if it is not clear whether all prerequisites have been met.
- The gateway can only be activated once. After activation, the option to download POC device gateway software is disabled, unless the gateway software is reinstalled.

- ☐ The POC device gateway is created in the system.
- ☐ The user has the administrative rights on the target gateway host system.
- ☐ The host system meets the hardware, software, and security requirements.
- ☐ The host system has a fixed IP address.

To download POC device gateway software

1. Choose the **Primary care provider** tab.
2. In the row of the appropriate organization, choose the > button.
3. Choose the **Software** accordion item.
4. For the POC device gateway being set up, choose the > button.
5. Choose the **Gateway software** accordion item.
6. Choose the **Download** button.
   - ➔ The progress of the download is displayed.
   - ➔ A message confirming the completed download is displayed.

Related topics

- List of technical requirements (30)
- Creating POC device gateways (77)
- Installing POC device gateway software (79)

Installing POC device gateway software

Installing the POC device gateway enables communication from POC devices to the centralized management system.

Contact local IT if it is not clear whether all prerequisites have been met.
To see more information about the REA agent, see the following Roche Diagnostics Knowledge (RDK) article: Integration of REA Agent in POC Gateway (https://rdkm.roche.com/explore/products/392490/troubleshooting/441467)

- ☐ The user has administrative rights within the organization network.
- ☐ The POC device gateway must be installed on the same local IP network where the POC devices are located.
- ☐ A gateway can only be activated once, ensure it is being installed on the correct host.
- ☐ IIS are enabled.

To install POC device gateway software

1. Locate the POC device gateway software ZIP file that was downloaded through the Downloading POC device gateway software (78) task.
2. Right-click the POC gateway software ZIP file and choose **Extract All... > Extract**.
   ➔ A sub folder containing a POC.zip file and a config.json file are created.
3. In the sub folder, right-click the POC.zip file and choose **Extract All... > Extract**.
4. In the \POC sub folder, double-click **Installer**.
   ➔ A setup dialog box is displayed.
5. If a proxy server is required:
   - In the setup dialog box, select the **Server Address and Port** check box.
   - Enter the address and port of the proxy server.
6. Choose the **Install** button.
   ⓘ The installation may take a few minutes. Do not turn off the machine.
   ➔ The installation process begins.
7. Once the installation process is complete, choose the **Restart** or the **Close** button, whichever is available.

To complete the gateway activation process, continue by following the Activating gateway software task.

Related topics

- List of technical requirements (30)
- Downloading POC device gateway software (78)
- Activating gateway software (81)

Activating gateway software

After installing the gateway software on the correct host, it must be activated. The activation is only successful if the activation key matches the configuration details in the installed software.

Contact local IT if it is not clear whether all prerequisites have been met.

- ☐ A gateway activation key that was generated no more than 5 days before activation.
- ☐ The gateway software for the specific gateway has been downloaded and installed on the correct host machine.

To activate gateway software

1. On the desktop, choose the **cobas infinity edge gateway** shortcut.
2. On the gateway activation dialog box, enter the 16-digit activation key.
   - The activation key is emailed to the user who creates the gateway.

After gateway activation, the REA agent needs to be configured, and trust must be established if a Roche ThingWorx Platform (RTP) connection is required for the installation.
For more information and instructions, refer to the following Roche Diagnostics Knowledge (RDK) article: Integration of REA Agent in POC Gateway (https://rdkm.roche.com/explore/products/392490/backgrounds/432233)

3. Choose the **Activate** button.
   - The activation process may take a few minutes. Do not turn off the machine.
   - ➔ A message confirming the activation was successful is displayed.

- For POC device gateways, the firewall rule must be enabled before communication is possible.

Enabling the firewall rule for POC device gateways

In order for POC devices to be able to connect to the POC device gateway, the following firewall rule must be enabled.

☐ The POC device gateway has been installed.

To enable the firewall rule for POC device gateways

1. On the computer, go to **Control Panel > Windows Defender Firewall > Advanced Settings > Inbound Rules > New Rule**.
2. Choose **Program > Next**.
3. In the **This program path:** field, enter `C:\Program Files (x86)\Roche\Roche.DP.CommServer\CommServer\bin\host.exe`
4. Choose the **Next** button.
5. Choose **Allow the connection > Next**.
6. Enable the **Domain**, **Private**, and **Public** profiles.
7. Choose the **Next** button.
8. In the name field, enter **POC drivers**.
9. Choose the **Finish** button.

Editing gateway details

Only the gateway name can be edited on the Gateway details accordion item. All other gateway data is inherited from the host organization or the gateway technical specifications.

To edit gateway details

1. Choose the **Primary care provider** tab and navigate to the organization.
2. In the row of the organization hosting the gateway, choose the > button.
3. Choose the **Software** accordion item.
4. In the row of the gateway being edited, choose the > button.
5. On the **Gateway** accordion item, choose the ✎ button.
6. Make the edit.
7. Choose the **Save** button.
   → A confirmation message is displayed.

Related topics

- Changing organization primary contact (65)

Changing gateway activation status

Changing the activation status of a gateway impacts communication between the DMS hosted by a POC service provider and POC devices hosted by a primary care provider. A gateway must be active in both locations in order for the system to function.

- ☐ To activate a gateway, the host organization must be active.

To change gateway activation status

1. Choose the **Primary care provider** tab and navigate to the organization.
2. In the row of the appropriate organization, choose the › button.
3. Choose the **Software** accordion item.
4. In the row of the appropriate gateway, choose the › button.
5. Choose the **Status** accordion item.
6. Choose the ✎ button.
7. Switch the **Status** toggle button to the appropriate activation status.
   ➔ A confirmation message is displayed.

Deleting gateways

Deleting a gateway cannot be undone.

- ☐ In order to delete a DMS gateway, there can be no active POC device gateway associated with it.

To delete a gateway

1. Choose the **Primary care provider** tab and navigate to the organization.
2. In the row of the appropriate organization, choose the › button.
3. Choose the **Software** accordion item.
4. For the gateway being deleted, choose the › button.
5. Choose the **Delete** button.
   ➔ A message asking to confirm the action is displayed.
6. Choose the **Confirm** button.
   ➔ A confirmation message is displayed.

Related topics

- Deleting users (130)

Uninstalling gateways

Uninstalling a gateway removes 3 folders created in the 'Program Files (x86)' folder:

- 'AUIConnectGW'
- 'IConnectGWPackages'
- 'IConnectGW'

Uninstalling a gateway also removes the certificates created in the 'Public' folder.

To uninstall a gateway

1 In Windows File Explorer, navigate to **Local Disk (C:) > IConnectUninstaller**.

2 Double-click the **IConnectUninstall** application.

➔ The gateway will be uninstalled.
The Vanilla Agent will not be removed.

Recertifying gateway software

You can recertify a DMS or POC device gateway software and its corresponding encryption certification.

To recertify a gateway software

1. In the row of the appropriate organization, choose the > button.
2. Choose the **Software** accordion item.
3. For the DMS or POC device gateway being recertified, choose the > button.
4. Choose the **Gateway software** accordion item.
5. Choose the **Recertify** button.
   ➔ A message confirming the recertification is displayed.

Reinstalling gateway software

You can reinstall a DMS or POC device gateway software. This might be needed when you want to install the gateway or another server, for example.

To reinstall a gateway software

1 In the row of the appropriate organization, choose the › button.

2 Choose the **Software** accordion item.

3 For the DMS or POC device gateway being reinstalled, choose the › button.

4 Choose the **Gateway software** accordion item.

5 Choose the **Reinstall** button.

➔ A message confirming the reinstallation is displayed.

6 Download the relevant gateway software:

- Downloading DMS gateway software
- Downloading POC device gateway software (78)

7 Install the downloaded file on the existing gateway machine.

Requesting TLS certificate for POC device gateway

The system does the TLS certificate retrieval for POC device gateways automatically before they expire. In case that the automatic process does not renew automatically, create a manual renewal request.

The TLS certificate has to be requested manually also when there are certification problems.

To manually request a TLS certificate for a POC device gateway

1 Choose the **Primary care provider** tab and navigate to the organization.

2 In the row of the appropriate primary care provider, choose the › button.

3 Choose the **Software** accordion item.

4 In the row of the appropriate POC device gateway, choose the › button.

5 Choose the **Request TLS certificate** button

6 Choose the **Confirm** button.
➔ A confirmation message is displayed.

Page intentionally left blank.

POC device management

In this chapter 7

Page intentionally left blank.

About POC device management

POC device management is different at each organization level.

At the Roche global administrator and Roche affiliate level, the POC device types that are supported by the system are set and configured. This includes making available the appropriate drivers for the POC device gateways to prepare the data management system to connect with the device type.

At the POC service provider level, administrators can set the device types that will be allowed to connect with a specific data management system. In order to set an allowed POC device type, the data management system must first be prepared to accept communications from the POC device type by installing the required POC device drivers on the DMS server.

At the primary care provider level, administrators can connect the specific POC device types that will be used by that primary care provider. If the POC devices are linked to a DMS gateway, this choice is limited to the options that are allowed by the POC service provider on the associated DMS gateway.

POC module for **navify**® Integrator supports multiple GTINs for all POC device types.

Viewing enabled POC device types

POC device types are enabled for each POC device gateway by the primary care provider. Viewing enabled POC device types displays a list of all POC device types that are configured to connect to the system.

The following information can be viewed:

- POC device type name
- Current driver version
- Configured port
- Encryption (operational interface)
- Configuration status
- Enabled or disabled indicator

To view enabled POC device types

1. Choose the **Primary care provider** tab and navigate to the organization.
2. In the row of the appropriate primary care provider, choose the > button.
3. Choose the **Software** accordion item.
4. In the row of the appropriate POC device gateway, choose the > button.
5. Choose the **POC device types** accordion item.
   → A list of supported POC device types is displayed.

Related topics

- Enabling POC device types (95)

Enabling POC device types

Enabling a new POC device type on a POC device gateway allows for individual POC devices of that type to be connected to the associated data management system.

☐ If connecting to a DMS gateway, the POC device type has been added to the list of allowed devices for the connected DMS gateway.

To enable a POC device type

1. Choose the **Primary care provider** tab and navigate to the organization.
2. In the row of the appropriate primary care provider, choose the › button.
3. Choose the **Software** accordion item.
4. In the row of the appropriate POC device gateway, choose the › button.
5. Choose the **POC device types** accordion item.
6. For each POC device type being enabled, switch the **Status for operational interface** toggle button to the desired status.
   ➔ A confirmation message is displayed.

Related topics

- Viewing enabled POC device types (94)

Editing enabled POC device types

The configured port and the SSL status of an enabled POC device type can be edited.

To edit an enabled POC device type

1. Choose the **Primary care provider** tab and navigate to the organization.
2. In the row of the appropriate primary care provider, choose the › button.
3. Choose the **Software** accordion item.
4. In the row of the appropriate POC device gateway, choose the › button.
5. Choose the **POC device types** accordion item.
6. Choose the ✎ button.
7. Make the edits.
8. Choose the **Save** button.
   ➔ A confirmation message is displayed.

Changing connectivity status of POC device types

Changing the status of a POC device type will either enable or disable all communication from POC devices of that type with the system.

To change the connectivity status of a POC device type

1 Choose the **Primary care provider** tab and navigate to the organization.

2 In the row of the appropriate primary care provider, choose the › button.

3 Choose the **Software** accordion item.

4 In the row of the appropriate POC device gateway, choose the › button.

5 Choose the **POC device types** accordion item.

6 In the row of the appropriate POC device type, switch the **Status for operational interface** toggle button to the desired status.

➔ A message asking to confirm the action is displayed.

7 Choose the **Confirm** button.

➔ A confirmation message is displayed.

Removing connected POC devices from a POC device gateway

It is possible to remove individual POC devices from a POC device gateway.

The procedure outlined below removes all types of POC devices (not only the new generation Roche POC devices).

☐ The specific POC device being removed must be disconnected.

To remove a connected POC device from a POC device gateway

1. Choose the **Primary care provider** tab and navigate to the organization.
2. In the row of the appropriate primary care provider, choose the › button.
3. Choose the **Software** accordion item.
4. In the row of the appropriate POC device gateway, choose the › button.
5. Choose the **POC device types** accordion item.
6. In the row of the appropriate POC device type, choose the ⊕ button.
   ➔ A list of individual POC devices of the selected type is displayed.
7. In the row of the device being removed, choose the 🗑 button.
   ➔ A message asking to confirm the action is displayed.
8. Choose the **Confirm** button.
   ➔ A confirmation message is displayed.

Registering POC devices manually

POC devices which are connected to the service interface are automatically registered in REXIS/SAP Sales.

Manual registration is only required, when the POC devices are not connected to the service interface, for example in the **navify**® Connector for Community offering.

To register a POC device manually

1. Choose the **Primary care provider** tab and navigate to the organization.
2. Choose the **Devices overview** tab.
3. Choose the **Register POC device** button.
4. Enter the required fields.
5. Choose the **Save** button.
   ➔ A confirmation message is displayed.

Viewing POC devices of an organization

Viewing POC devices displays a list of all registered POC devices of an organization. Only the new generation Roche POC devices are displayed, which are connected to the service interface or were manually registered.

To view POC devices of an organization

1 Choose the **Primary care provider** tab and navigate to the organization.

2 Choose the **Devices overview** tab.
→ All registered POC devices of the organization are listed.

3 To view details of a POC device, in the row of the appropriate POC device, choose the › button.
- Choose the **Back** button.

Editing POC devices of an organization

POC devices of an organization can be edited.

Currently, only manually registered POC devices can be edited.

To edit POC devices of an organization

1 Choose the **Primary care provider** tab and navigate to the organization.

2 Choose the **Devices overview** tab.

➔ All registered POC devices of the organization are listed.

3 In the row of the appropriate POC device, choose the > button.

4 Choose the ✎ button.

5 Make the edits.

ⓘ You can edit the log level and choose one of the 4 suggested levels.

6 Choose the **Save** button.

Deleting POC devices from an organization

POC devices can be deleted from an organization. Deletion only applies to the new generation Roche POC devices which are connected to the service interface or were manually registered.

POC devices can also be deleted from Rexis.

To remove POC devices from a POC device gateway that is not a "new generation Roche POC device", refer to this procedure:

Removing connected POC devices from a POC device gateway (98)

To delete a POC device from an organization

1. Choose the **Primary care provider** tab and navigate to the organization.
2. Choose the **Devices overview** tab.
3. Choose the POC devices being deleted.
4. Choose the **Delete device** button.
5. Choose the reason for deletion in the displayed message.
   ➔ If the **I have already sent these devices for repair or will do so** option is selected, an informational message is displayed. Once the repair is complete, the system automatically deletes the device.

POC device configuration

In this chapter 8

Page intentionally left blank.

About POC device configuration

POC device configuration applies only to new generation Roche POC devices that can be configured by scanning a QR code.

The system deletes all configurations when users change any of the following POC service provider details:

- Anonymous data-sharing setting
- Data management system (DMS)
- Regulatory region

The Anonymous data-sharing setting, Data management system (DMS), or Regulatory region is editable only at the organization level upon contractual agreement and involves associated compliance risks.

Immediately destroy old printed QR codes to avoid outdated configurations. You generate a new QR code after you set up a new device configuration.

Only devices with a camera can be configured via QR code scanning.

Depending on the scenario in use, POC devices are configured either through POC module for **navify**® Integrator or via the data management system.

Each configuration is location-specific and shares connectivity details for the WLAN and the network.

Scenario without DMS

When a POC service provider uses POC devices without a DMS, POC device configuration is completely done in POC module for **navify**® Integrator (WLAN and network settings and POC device configuration).

For a detailed explanation of all configuration items, refer to the relevant Roche device* User Assistance, chapters *Initial configuration* and *General configuration*.
*Some Roche devices do not support all functionalities.

Scenario with a DMS

When a POC service provider uses POC devices in conjunction with a DMS, POC device configuration is mainly done in the DMS. The configuration function in POC module for **navify**® Integrator is only used to setup the

connectivity (WLAN and network configuration) and some service functions (i.e., synchronization interval or session timeout).

Loading configuration to POC devices

A configuration can be loaded onto a POC device via a QR code. The QR code is generated within POC module for **navify**® Integrator.

Creating a POC device configuration

For each POC device type at least one configuration has to be created. The configuration has location-specific WLAN and network settings and is created for a selected POC device firmware.

The configuration scope depends on the scenario in use (with/without DMS).

For a detailed explanation of all configuration items, refer to the Roche device* User Assistance, chapters *Initial configuration* and *General configuration*.
*Some Roche devices do not support all functionalities.

To create a POC device configuration

1. Choose the **POC device management** tab and choose a POC device type.
2. Choose the **Device configuration** tab.
3. Choose the **Create** button.
4. From the **Firmware version** drop-down list, choose the POC device firmware version that is used for the configuration and choose the **Confirm** button.
5. Enter the required fields in all accordions.
   Mandatory accordions are indicated.
6. Choose the **Save** button.
   ➔ A confirmation message is displayed.
7. Choose the **Generate QR code** button.
   ➔ A confirmation message is displayed listing the entered configuration.
8. Check the correctness of the configuration and choose the **Confirm** button at the end of the window.
   ➔ The QR code is displayed.

Editing a POC device configuration

Editing a POC device configuration can be done any time. Each accordion item is edited separately.

For a detailed explanation of all configuration items, refer to the relevant Roche device* User Assistance, chapters *Initial configuration* and *General configuration*.
*Some Roche devices do not support all functionalities.

To edit a POC device configuration

1. Choose the **POC device management** tab and choose a POC device type.
2. Choose the **Device configuration** tab.
3. In the row of the appropriate configuration, choose the › button.
4. Choose the appropriate accordion item, and then choose the ✎ button.
5. Make the edits.
6. Choose the **Save** button.
7. If necessary, edit other accordion items.
8. Choose the **Generate QR code** button.
   ➔ A confirmation message is displayed listing the entered configuration.
9. Check the correctness of the configuration and choose the **Confirm** button at the end of the window.
   ➔ The QR code is displayed.

Duplicating a POC device configuration

When the new configuration is similar to an existing one, duplicating a configuration is the fastest way to create a configuration.

For a detailed explanation of all configuration items, refer to the relevant Roche device* User Assistance, chapters *Initial configuration* and *General configuration*.
*Some Roche devices do not support all functionalities.

To duplicate a POC device configuration

1. Choose the **POC device management** tab and choose a POC device type.
2. Choose the **Device configuration** tab.
3. In the row of the appropriate configuration, choose the button.
4. Enter a new configuration name.
5. If required, make further edits.
6. Choose the **Save** button.
   ➔ A confirmation message is displayed.
7. Choose the **Generate QR code** button.
   ➔ A confirmation message is displayed listing the entered configuration.
8. Check the correctness of the configuration and choose the **Confirm** button at the end of the window.
   ➔ The QR code is displayed.

Scanning a QR code for a POC device configuration

At the end of a POC device configuration, a QR code is generated. This code can be displayed any time to load the configuration into POC devices.

To scan a QR code for a POC device configuration

1 Choose the **Primary care provider** tab and navigate to the organization.

2 Choose the **POC device management** tab and choose a POC device type.

3 Choose the **Device configuration** tab.

4 In the row of the appropriate configuration, choose the button.

➔ The QR code is displayed.

5 On your Roche device, go to the relevant barcode reading area.

- For example, on the **cobas® pulse** device, tap **> Configuration by barcode**.

6 If prompted, enter the setup password and tap the **Confirm** button.

7 Scan the QR code.

➔ When the QR code has been scanned successfully the device emits a beep and a confirmation dialog box is displayed.

Deleting a POC device configuration

Deleting a POC device configuration cannot be undone.

To delete a POC device configuration

1 Choose the **POC device management** tab and choose a POC device type.

2 Choose the **Device configuration** tab.

3 Choose the configurations being deleted.

4 Choose the **Delete** button.

➔ A confirmation message is displayed.

Page intentionally left blank.

Software management

In this chapter 9

Page intentionally left blank.

About software management

Software management only applies for new generation Roche POC devices which are connected to the service interface.

Scheduled software distribution allows the distribution of POC device software packages and 3rd party applications from POC module for **navify**® Integrator to the POC devices.

In some cases, the distribution of POC device software is limited to customers located within certain countries. These limitations can be the result of the export control and compliance regulations that Roche has to follow.

Software distribution can be managed in two ways:

- Managed in POC module for **navify**® Integrator:
  Schedule the software updates manually in the POC module for **navify**® Integrator centralized management system. The POC devices get updated automatically.
- Managed in the POC device:
  POC module for **navify**® Integrator creates the software schedule automatically (if required, software updates can also be manually scheduled). The POC device prompts the user to execute the software update. Software updates on the POC device itself can be done only by the POC device administrator.

The software will be managed on the POC device (device-managed) if the following criteria are met:

- The device supports device-managed software updates.
- The service provider has the **Software distribution managed on the device** toggle button enabled.

Only specific devices support device-managed software updates.

Scheduling a POC device software update

The POC device software or a 3rd party application can be updated for all or for selected POC devices in an organization. The selected POC devices can be scheduled for immediate update, or at a specific date and time.

An update retry window can be defined during which the system attempts to update the POC device software.

The list of POC devices can be filtered for the following criteria:

- Software type
- Current version
- Software status
- Location
- Scheduled start and end date
- Free search text

The software will be managed on the POC device (device-managed) if the following criteria are met:

- The device supports device-managed software updates.
- The service provider has the **Software distribution managed on the device** toggle button enabled.

To schedule a POC device software update

1. Choose the **POC device management** tab and choose a POC device type.
2. Choose the **Software update** tab.
   → A list of POC devices with their software status is displayed.
3. If necessary, apply the appropriate filters.
4. Select the check box for each POC device a software update has to be scheduled.
   - If necessary, choose the POC device to display the POC device details.
5. Choose the **Schedule update** button.
6. Enter the required fields.
7. Choose the **Schedule** button.
   → A confirmation message is displayed.

Rescheduling a POC device software update

A scheduled POC device software or 3rd party application update can be rescheduled.

Rescheduling is only possible as long as the scheduled POC device software update has not yet been started.

For the **cobas® pulse** system, the application does not support the scheduling of multiple software updates at the same time. If you need to install multiple software packages, it is recommended to schedule the software updates with a time difference of e.g. 1 hour.

To reschedule a POC device software update

1 Choose the **POC device management** tab and choose a POC device type.

2 Choose the **Software update** tab.
   ➔ A list of POC devices with their software status is displayed.

3 If necessary, apply the appropriate filters.

4 Select the check box for each POC device a software update has to be rescheduled.
   • If necessary, choose the POC device to display the POC device details.

5 Choose the **Reschedule update** button.

6 Enter the required fields.

7 Choose the **Reschedule** button.
   ➔ A confirmation message is displayed.

Cancelling a POC device software update

A scheduled POC device software or 3rd party application update can be cancelled.

If the POC device software update has already begun, you cannot cancel it.

To cancel a POC device software update

1 Choose the **Primary care provider** tab and navigate to the organization.

2 Choose the **POC device management** tab and choose a POC device type.

3 Choose the **Software update** tab.
➔ A list of POC devices with their software status is displayed.

4 If necessary, apply the appropriate filters.

5 Select the check box for each POC device a software update has to be cancelled.
- If necessary, choose the POC device to display the POC device details.

6 Choose the **Cancel update** button.
➔ A confirmation message is displayed.

Lot management

In this chapter 10

Page intentionally left blank.

About lot management

Lot information of test strip containers is automatically distributed from POC module for **navify**® Integrator to the POC device via the service interface when the barcode of the strip lot container is scanned on the device.

If a POC device is not connected to the service interface, the QR code of a specific strip lot can directly be scanned in POC module for **navify**® Integrator.

Scanning a QR code of a test strip lot on a Roche device

Strip lot QR codes can be displayed any time to load them into POC devices.

This procedure may not be applicable to all Roche devices.

To scan a QR code of a test strip lot on a Roche device

1 Choose the **Primary care provider** tab and navigate to the organization.

2 Choose the **POC device management** tab and choose a POC device type.

3 Choose the **Lot management** tab.

4 In the row of the appropriate strip lot number, choose the button.

➔ The QR code is displayed.

5 Use the Roche device to scan the strip lot.

Adding a test strip lot to a Roche device

You must add a new test strip lot to your device in order to be able to use the test strips from that lot.

The distribution of test strips from a new lot will depend on the best practice of your healthcare facility.

The device can be configured to perform a QC test the first time a test strip from a new lot is inserted into the device.

This procedure is only applicable to the **cobas® pulse** instrument.

⚠ CAUTION!

Device is not connected to POC module for navify® Integrator

If the device is not connected to POC module for **navify®** Integrator you cannot add a test strip lot as described in this task.

- You must scan the QR code generated in the POC module for **navify®** Integrator portal using the ⚙ > **Configuration by barcode** option.
  The new strip lot is then added to the **Lot management** screen.

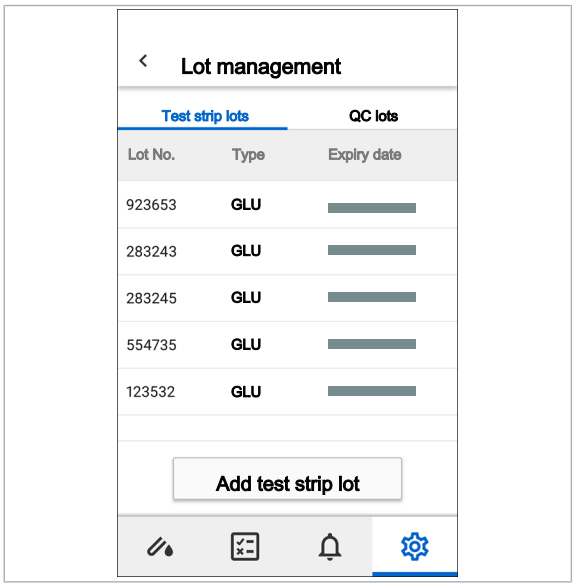
As required

- ☐ Test strip container and test strips from the new lot

- ☐ The new lot has been uploaded to the DMS
- ☐ Connection to POC module for **navify®** Integrator

To add a test strip lot to the device

1 In the Glucose app, tap ⚙ > **Lot management**.



2 In the **Lot management** screen on the **Test strip lots** tab, tap the **Add test strip lot** button.

3 Using the **Scan lot barcode** screen, scan the barcode of the new test strip lot container.

➔ A message confirms that the new lot has been added. The new lot is added to the **Test strip lots** tab.

4 Do one of the following:

- If you are not prompted to perform a QC test, you can start using the test strips from the new lot.
- If prompted, perform a QC test using the new test strip lot.
  After performing the QC test successfully you can start using the test strips from the new lot.

User management

In this chapter 11

Page intentionally left blank.

About user management

Only users with an administrator role can perform user management actions. These actions can only be performed on users of the same or lower level as the administrator performing the actions.

The user groups in the system are organized from the highest permissions level to the lowest as follows:

- Roche global administrator
- Roche affiliate administrator
- Roche affiliate user
- POC service provider administrator
- POC service provider user
- Primary care provider administrator
- Primary care provider user

Users that belong to one of the three Roche user groups must have an e-mail in the roche.com domain and have to login using their Roche credentials.

Non-Roche users are managed in the POC module for **navify**® Integrator system. They get an initial on-boarding email after their user account has been created in the system. New non-Roche users have to change the password after first logon.

Viewing users

Administrators can see a list of active and inactive users for all organizations that they have administrative rights over.

To view users

1 Choose the **Primary care provider** tab and navigate to the organization.

2 Choose the **Users** tab.

3 To see additional information about a user, choose the > button in the row of the user.
➔ The user details screen is displayed.

Related topics

- Creating additional users (129)
- Deleting users (130)

Creating additional users

The following user types can be created:

- Primary care provider administrator
- Primary care provider user

To create an additional user

1 Choose the **Primary care provider** tab and navigate to the organization.

2 Choose the **Users** tab.

3 Choose the **Create** button.

4 Enter the required fields.

5 Choose the **Next** button.

6 Select the check box for each organization the user is assigned to.

7 Choose the **Save** button.
➔ A confirmation message is displayed.

Related topics

- Changing organization primary contact (65)

Deleting users

Deleting a user will permanently remove all information about that user from the system. Once deleted, the user will no longer have access to the system.

The following user types can be deleted:

- Primary care provider administrator
- Primary care provider user

☐ The user is not the primary contact for any organization they are assigned to.

To delete a user

1 Choose the **Primary care provider** tab and navigate to the organization.

2 Choose the **Users** tab.

3 In the row of the user being deleted, choose the › button.

4 Choose the **Delete** button.

➔ A message asking to confirm the action is displayed.

5 Choose the **Confirm** button.

➔ A confirmation message is displayed.

Related topics

- Changing organization primary contact (65)

Editing user details

The user role and contact details can be edited. Changing the user role will impact what actions the user is able to perform in the system.

The user details of the following user types can be edited:

- Primary care provider administrator
- Primary care provider user

☐ The user role cannot be changed if the user is the primary contact of an organization.

To edit user details

1. Choose the **Primary care provider** tab and navigate to the organization.
2. Choose the **Users** tab.
3. In the row of the user being edited, choose the › button.
4. On the **User** accordion item, choose the ✎ button.
5. Make the edits.
6. Choose the **Save** button.
   ➔ A confirmation message is displayed.

Related topics

- Editing organizations a user is assigned to (132)

Editing organizations a user is assigned to

A user can only be assigned to an organization that is at the same level as the user. For example, a primary care provider administrator can only be assigned to primary care providers.

This action can be performed on the following user roles:

- Primary care provider administrator
- Primary care provider user

- ☐ A user must be assigned to at least one organization.
- ☐ If removing the user from an organization, the user cannot be the primary contact of that organization.

To edit the organizations a user is assigned to

1. Choose the **Primary care provider** tab and navigate to the organization.
2. Choose the **Users** tab.
3. In the row of the user being edited, choose the › button.
4. Choose the second accordion item.
5. Choose the ✎ button.
6. Do one or both of the following:
   - Select the check box of each parent organization being added to the user profile.
   - Clear the check box of each parent organization being removed from the user profile.
7. Choose the **Save** button.
   ➔ A confirmation message is displayed.

Related topics

- Editing user details (131)
- Changing organization primary contact (65)

Resetting user password

Resetting a user password sends an email to that user with a one-time password that allows them to enter the system and update their password.

The user password can be reset for the following user types:

- Primary care provider administrator
- Primary care provider user

To reset a user password

1. Choose the **Primary care provider** tab and navigate to the organization.
2. Choose the **Users** tab.
3. In the row of the user being edited, choose the › button.
4. On the **User** accordion item, choose the **Reset password** button.
   ➔ A message asking to confirm the action is displayed.
5. Choose the **Reset** button.
   ➔ A confirmation message is displayed.

Page intentionally left blank.

Troubleshooting

Page intentionally left blank.

Troubleshooting

In this chapter 12

Page intentionally left blank.

Viewing logs

All events logged by the system can be viewed at any time.

The list of **Centralized management system** logs can be filtered for the following criteria:

- Log type
- The user who triggered the log
- Log time
- Date range

The list of **Gateway** logs can be filtered for the following criteria:

- Gateway type
- Log type
- Organization type
- Date range

The list of **Edge and PIL** logs can be filtered for the following criteria:

- Communication type
- Message
- Status
- Date range
- POC service provider

The list of **Events** logs can be filtered for the following criteria:

- Roche affiliate
- POC service provider
- Primary care provider
- Event
- Event type
- Date range

The list of **Audit trail** logs can be filtered for the following criteria:

- Roche affiliate
- POC service provider
- Primary care provider
- Event
- Date range

To view logs

1. Choose the **Logs** tab.
2. Choose the **Centralized management system**, **Gateway**, **Edge and PIL**, **Events**, or **Audit trail** tab.

3 To find a specific log, apply the appropriate filters.
➔ A list of logs and their high-level descriptions is displayed.

4 In the row of the appropriate log, choose the › or ☁ button.
➔ A detailed description of the log is displayed.

Exporting log files to CSV

A CSV export of the log files can be downloaded at any time.

To export log files to CSV

1 Choose the **Logs** tab.

2 Choose the **Centralized management system**, **Edge and PIL**, or **Audit trail** tab.

3 If necessary, apply the appropriate filters.

4 Choose the **Export to CSV** button.

➔ A message stating that the CSV log file is exported to the local downloads folder is displayed.

Exporting gateway log files to CSV

A CSV export of gateway log files can be downloaded at any time. The local logs are moved to the centralized management system once every 24 hours. When logs are downloaded from the gateway, only the items logged since the last transfer are downloaded.

To export gateway log files to CSV

1 On the desktop, double-click the gateway icon.
➔ The gateway user interface is displayed.

2 Choose the **Download log file** button.
➔ The logs are downloaded

Restarting gateways from the centralized management system

Restarting a gateway will temporarily disable communication between POC device, the system, and the data management system.

To restart a gateway from the centralized management system

1 Choose the **Primary care provider** tab and navigate to the organization.

2 In the row of the appropriate organization, choose the › button.

3 Choose the **Software** accordion item.

4 In the row of the appropriate gateway, choose the › button.

5 Choose the **Gateway software** accordion item.

6 Choose the **Restart** button.

➔ A confirmation message is displayed.

Restarting gateways from the gateway

Restarting a gateway will temporarily disable communication between POC device, the system, and the data management system.

To restart a gateway from the gateway

1 On the desktop, double-click the gateway icon.
➔ The gateway user interface is displayed.

2 Choose the **Restart** button.
➔ A confirmation message is displayed.

Glossary

centralized management system

Combination of different cloud services that are used to establish communication, to provide a secure exchange of messages, to manage users, and in general to operate and maintain a whole system.

data management system

System that facilitates the creation, organization, retrieval, maintenance, and use of an electronic database.

gateway

Functional unit or node on a network that serves as an entrance to another network.

GLU

Parameter that provides information about the concentration of glucose in a sample.

POC service provider

Service provider that brings POC-related services to primary care providers.

primary care provider

Healthcare provider who is the first point of contact for a patient.

Roche affiliate

Roche organization that is responsible for the marketing, sales, and service of Roche products and solutions in a specific country.

Page intentionally left blank.

Index

M

O

P

R

S

T

U

V

W

Published by

Roche Diagnostics International Ltd
CH-6343 Rotkreuz
Switzerland

www.roche.com