

POC module for **navify**® Integrator

POC service provider user

User Guide


Publication version 5.0

Software version 3.0



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 and higher	November 2024	 What is new in publication version 5.0 (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	© 2019-2024, F. Hoffmann-La Roche Ltd. All rights reserved.
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



10404094001

Table of contents

Revision history	2
Contact address	4
Intended use	7
Symbols and abbreviations	8
What is new in publication version 5.0	10

Safety

1 Safety information

Safety classifications	15
System safety	16
Data security	17
Checking website certificates	20

System description

2 Overview of the system

About the system	25
Where to find information about the different offerings	27
About Roche backend systems	28
List of technical requirements	29
List of user roles and permissions	38
Overview of the user interface	40

Operation

3 Centralized management system operation

Logging on for the first time	45
Logging on	46
Logging off	47
About user account and password	48
Changing passwords	49
Changing profile settings	50

4 Monitoring

About monitoring	53
Monitoring POC service providers	54
Monitoring DMS gateways	55
Monitoring primary care providers	56
Monitoring POC device gateways	57
Monitoring POC devices	58

5 Lot management

About lot management	61
Adding a test strip lot to a Roche device	62

Glossary

Index

Page intentionally left blank.

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	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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:

Symbols used in system

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

Symbol	Explanation
REF	Catalog number
GTIN	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
MSMQ	Microsoft Message Queuing
POC	Point of Care
RAM	Random access memory
RVA	Roche Vanilla Agent
SSL	Secure Sockets Layer
USB	Universal Serial Bus
WAN	Wide area network

☐ Abbreviations

What is new in publication version 5.0

Product name updates

The product names have been updated to POC module for **navify**® Integrator and **navify**® Connector for Community.

Safety

1	Safety information	13
---	--------------------------	----

Page intentionally left blank.

Safety information

In this chapter

1

Safety classifications	15
System safety	16
Data security	17
Checking website certificates.....	20

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

Incorrect or corrupt data due to unauthorized access

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

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

Monitor the system for suspicious activity and report suspected compromise

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

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

2	Overview of the system	23
---	------------------------------	----

Page intentionally left blank.

Overview of the system

2

In this chapter

About the system	25
Where to find information about the different offerings	27
About Roche backend systems	28
List of technical requirements	29
General requirements	29
navify ® Connector for Community requirements	32
POC module for navify ® Integrator requirements	35
List of user roles and permissions	38
Overview of the user interface	40

Table of contents

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.

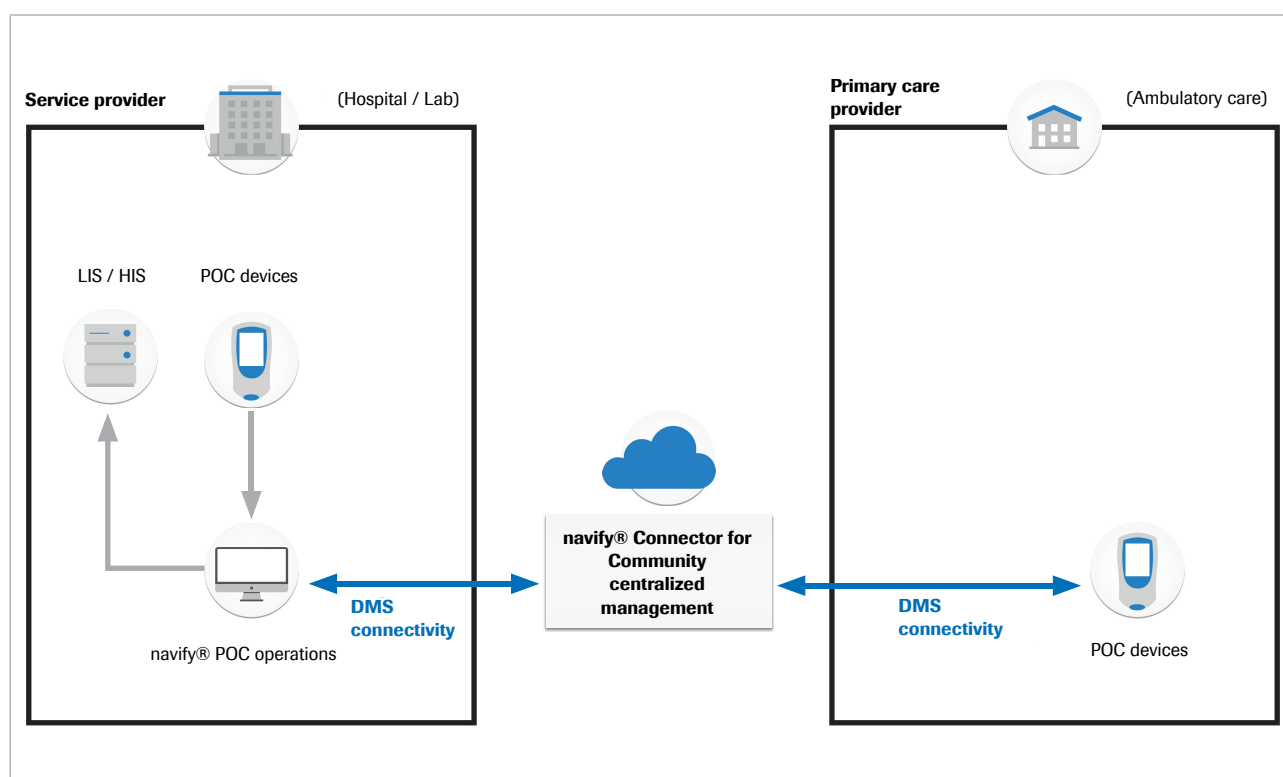
The following offerings are available

- **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:



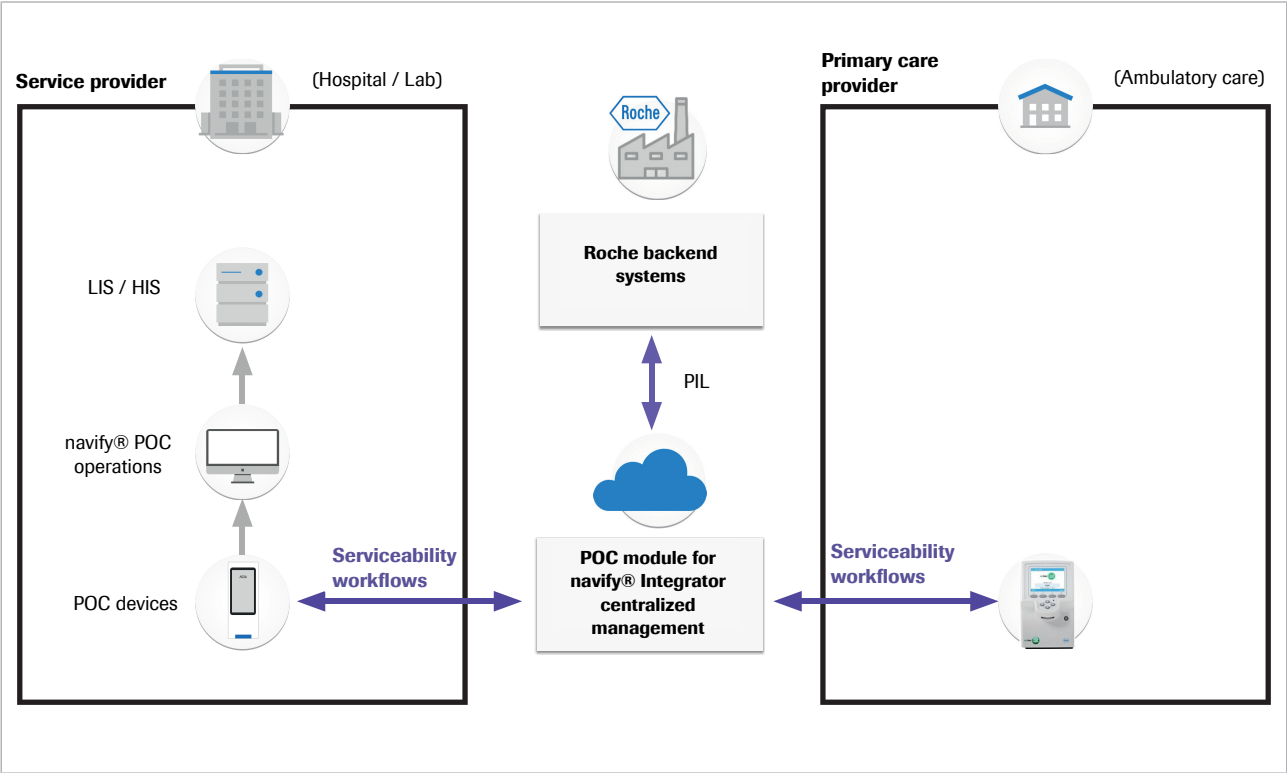
 **navify**® Connector for Community offering (DMS connectivity)

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 \(53\)](#)

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

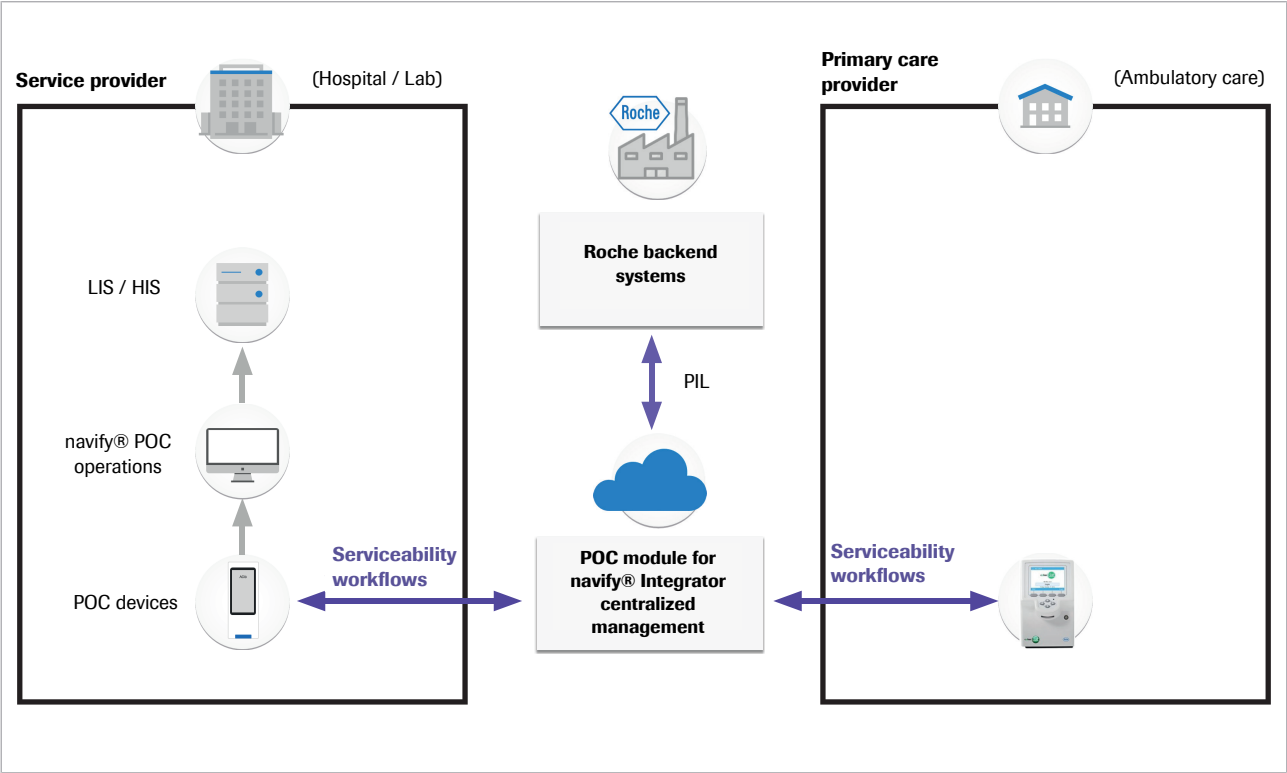
- POC device configuration
- Software management
- Lot management

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 (29)

navify® Connector for Community requirements (32)

POC module for **navify**® Integrator requirements (35)

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

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 able 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
DPS:		
https://global.azure-devices-provisioning.net	443	https & AMQP
https://dps-euprod-icconnect.azure-devices-provisioning.net	443	https
IoT Hub:		
https://iothub-euprod-icconnect.azure-devices.net	443	https
Storage accounts:		
☒ Gateway connectivity requirements (EU Instance)		

URL	Port	Protocol
https://swidextractstorageeuprod.blob.core.windows.net	443	https
https://stpilpackagestorageprod.blob.core.windows.net	443	https
https://servicedatastorageeuprod.blob.core.windows.net	443	https
https://appauditlogseuprod.blob.core.windows.net	443	https
https://euprodgatewaydriverfile.blob.core.windows.net	443	https
https://euprodgwmsgstore.blob.core.windows.net	443	https
https://euprodinstrumentdrivers.blob.core.windows.net	443	https
Others:		
https://euapi.cobas-infinity-edge.com/gwapi	443	https
https://eu.cobas-infinity-edge.com	443	https
http://crl-pki-rd.roche.com	80	http
🏠 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 Instance):

URL	Port	Protocol
DPS:		
https://global.azure-devices-provisioning.net	443	https
https://dps-usprd-iconnect.azure-devices-provisioning.net	443	https
IoT Hub:		
https://iothub-usprd-iconnect.azure-devices.net	443	https
Storage accounts:		
https://swidextractstorageeuprod.blob.core.windows.net	443	https
https://stpilpackagestorageprod.blob.core.windows.net	443	https
https://servicedatastorageeuprod.blob.core.windows.net	443	https
https://appauditlogsusprd.blob.core.windows.net	443	https
https://usprdgatewaydriverfile.blob.core.windows.net	443	https
https://usprdgwmsgstore.blob.core.windows.net	443	https
https://usprdinstrumentdrivers.blob.core.windows.net	443	https
Others:		
https://usapi.cobas-infinity-edge.com/gwapi	443	https
https://us.cobas-infinity-edge.com	443	https
http://crl-pki-rd.roche.com	80	http
🏠 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
https://liat.tepi.navify.com	443	https
https://hbm.tepi.navify.com	443	https
https://b123.tepi.navify.com	443	https

(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

Minimum security requirements

When installing a POC gateway, the Roche Vanilla Agent (RVA) is also installed. The Roche Vanilla Agent provides secure connectivity to the ServiceLink enterprise and does not connect to any other system. All communications are authenticated and encrypted.

In summary, the Roche Vanilla Agent requires:

- Access to limited number of IP addresses only
- Outgoing TCP connections only
- One outbound port, specifically port 443 (SSL)

It is recommended that systems using the Roche Vanilla Agent should continue to adhere to IT security best practices and guidelines for application and database servers including:

- Controlled and limited access to the internet

- Use of software or hardware firewall protection
- Installation of anti-virus software that provides continuous inspection of network traffic
- Regular application of operating system and drivers updates, especially security related

This can be implemented either by software firewalls in the client computer, by hardware firewalls, or both.

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)	4 GB	2 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.
- MSMQ and 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.

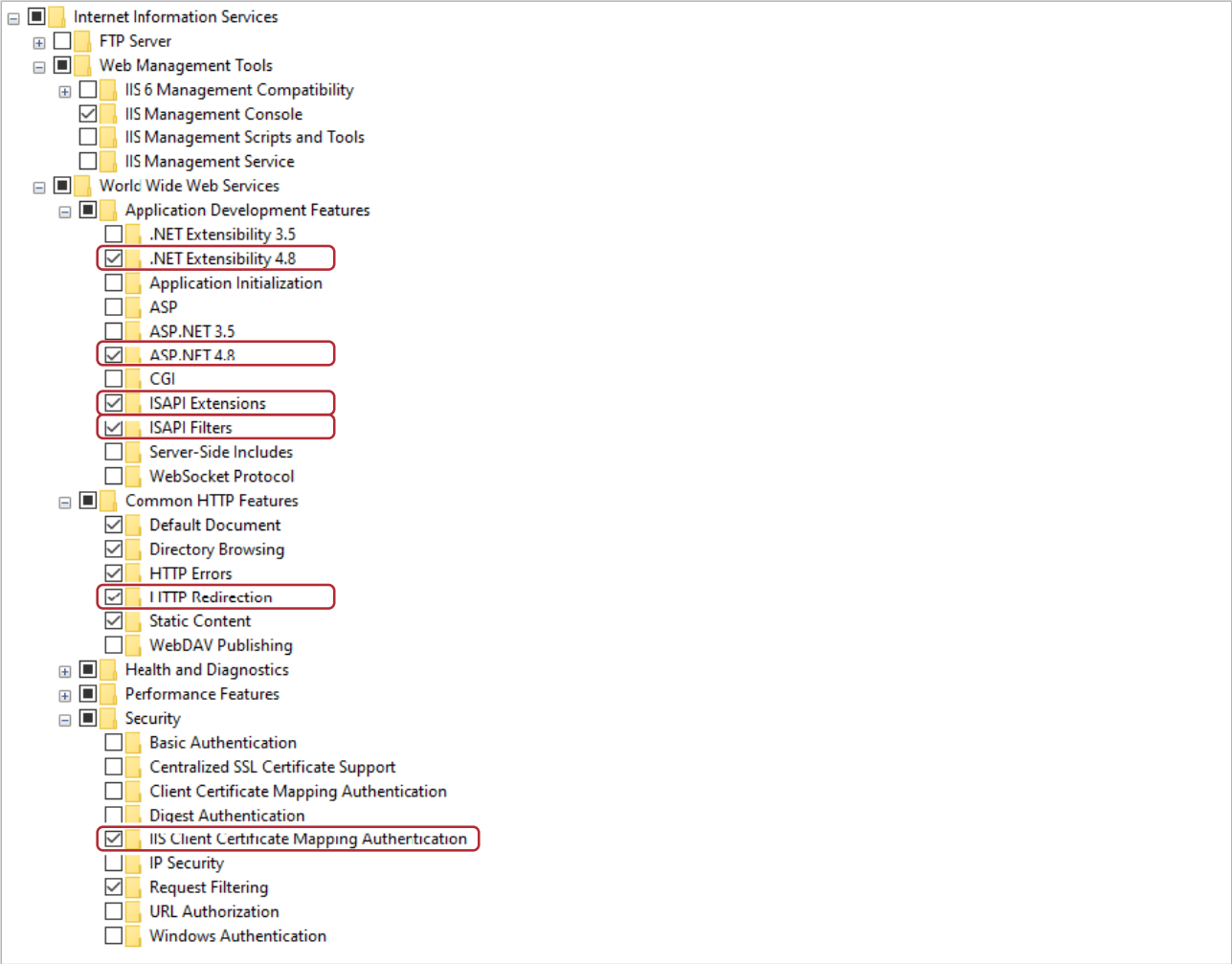
	Minimum requirements	Responsible for installation
Supported operating systems	<ul style="list-style-type: none"> • Windows 10 Professional or Enterprise edition (64 bit) • Windows 11 Professional or Enterprise edition (64 bit) 	Customer
.NET	8.0	Customer
.NET Framework version	.NET 4.8.3928.0 or higher	Customer
IIS subcomponents	See image below	Customer
MSMQ subcomponents	See image below	Customer
Communication server	1.21.0.10909	Gateway installer

 Minimum POC device gateway software requirements

	Minimum requirements	Responsible for installation
Driver framework	4.3.0.13634	Gateway installer

☰ Minimum POC device gateway software requirements

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



☰ Minimum IIS subcomponents for POC device gateways



☰ Minimum MSMQ 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	<ul style="list-style-type: none"> • 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
MSMQ 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.

Minimum software requirements for POC device gateways

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

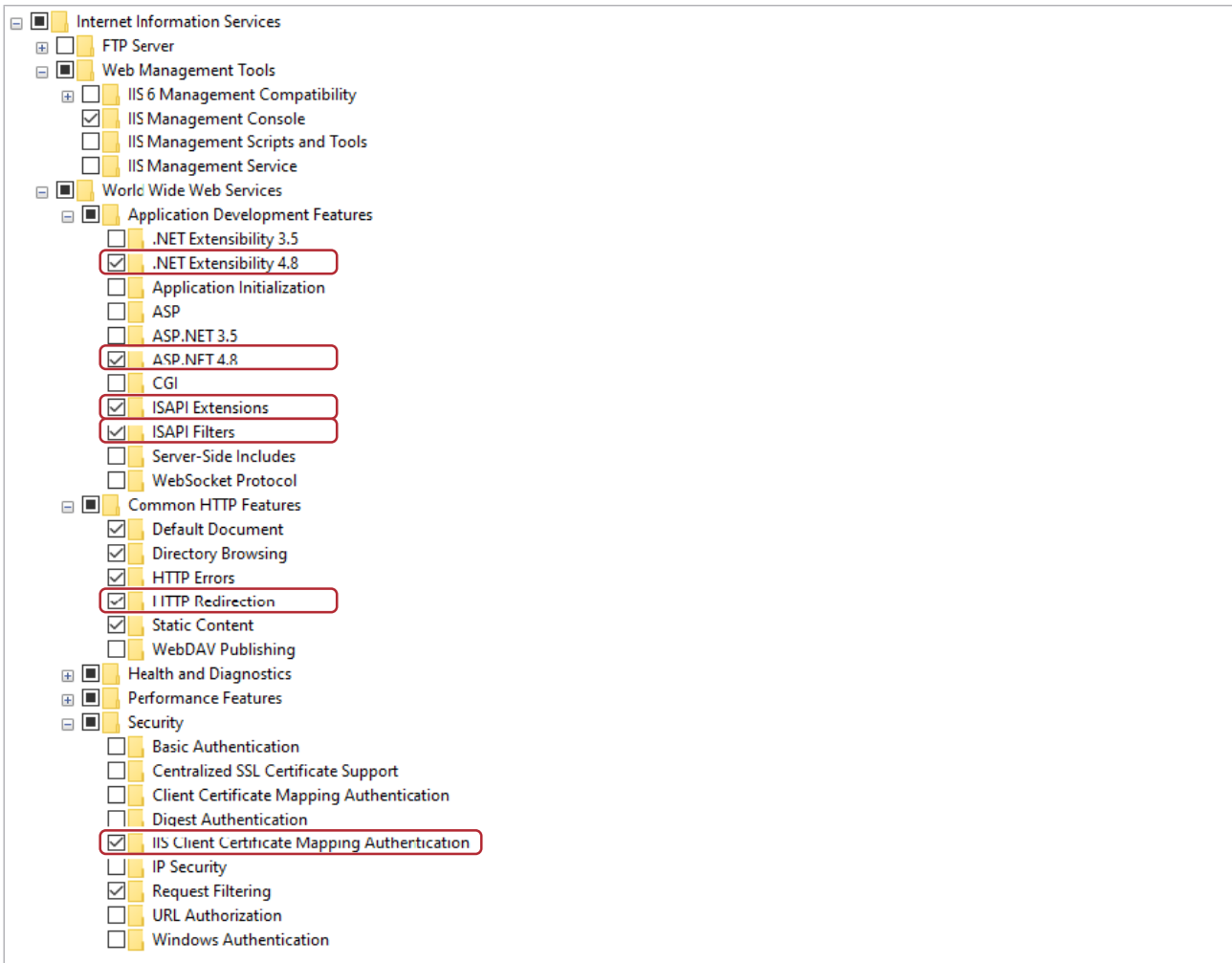
☰ Minimum POC device gateway hardware requirements

- 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.

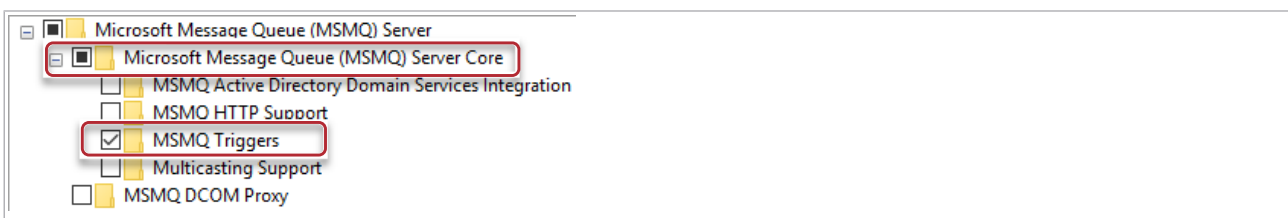
	Minimum requirements	Responsible for installation
Supported operating systems	<ul style="list-style-type: none">• Windows 10 Professional or Enterprise edition (64 bit)• Windows 11 Professional or Enterprise edition (64 bit)• Windows Server 2012 R2 (64 bit)• Windows Server 2016 (64 bit)• Windows Server 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
MSMQ subcomponents	See image below	Customer

☰ Minimum POC device gateway software requirements

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



Minimum IIS subcomponents for POC device gateways



Minimum MSMQ 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	POC service provider user	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	POC service provider user	Primary care provider administrator	Primary care provider user
Monitoring POC service providers	✓	X	X
Monitoring DMS gateways	✓	X	X
Monitoring primary care providers	✓	✓	✓

☐ Monitoring

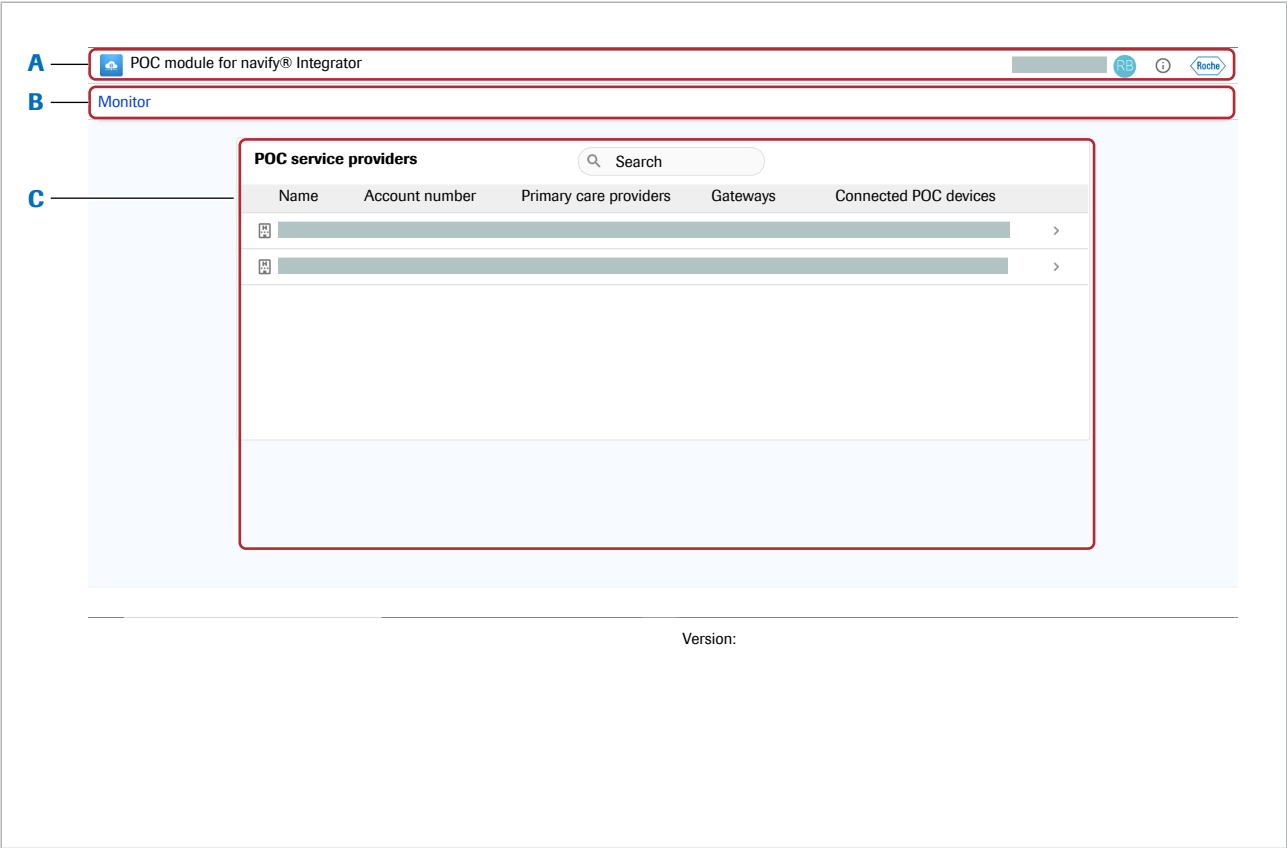
Monitoring task	POC service provider user	Primary care provider administrator	Primary care provider user
Monitoring POC device gateways	✓	✓	✓
Monitoring POC devices	✓	✓	✓

Monitoring

Lot management task	POC service provider user	Primary care provider administrator	Primary care provider user
Adding strip lot to POC device	✓	✓	✓

Lot management

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
- 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

3	Centralized management system operation	43
4	Monitoring.....	51
5	Lot management	59

Page intentionally left blank.

Centralized management system operation

In this chapter

3

Logging on for the first time.....	45
Logging on.....	46
Logging off	47
About user account and password	48
Changing passwords	49
Changing profile settings	50

Table of contents

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 \(48\)](#)

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 \(48\)](#)

Logging off

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

► To log off

- 1 Choose the  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  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 \(48\)](#)

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  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

About monitoring.....	53
Monitoring POC service providers.....	54
Monitoring DMS gateways	55
Monitoring primary care providers	56
Monitoring POC device gateways	57
Monitoring POC devices	58

Table of contents

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:

- POC service provider
- Primary care provider
- DMS gateway
- POC device gateway
- POC devices

Monitoring POC service providers

The following POC service provider attributes can be monitored:

- The number of associate primary care providers and 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 POC service provider by the system.
- The phone number and email address of the primary contact.

► To monitor POC service providers

- 1 Choose the **Monitor** tab.
 - High-level details of the POC service providers the user is assigned to are displayed.
- 2 For more detailed information, choose the > button for the appropriate POC service provider.
 - The **Details** and **Primary care providers** of the chosen POC service provider are displayed.

Monitoring DMS gateways

DMS 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
- Gateway software version
- Gateway IP address
- Gateway host name

The connection status of a DMS gateway is **Connected** as long as there is a heartbeat between the DMS 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**.

► To monitor DMS gateways

- 1 Choose the **Monitor** tab.
- 2 On the **POC service providers** panel, choose the > button for the appropriate POC service provider.
- 3 Choose the **DMS gateways** tab.
 - High-level details of the connected DMS gateways are displayed.
- 4 For more detailed information, choose the > button for the appropriate gateway.
 - The **Details** for the chosen gateway are displayed.

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.
- 2 On the **POC service providers** panel, choose the > button for the appropriate POC service provider.
 - High-level details of the primary care providers connected to the POC service provider are displayed.
- 3 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 acknowledgment 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 On the **POC service providers** panel, choose the > button for the appropriate POC service provider.
- 3 Choose the **POC device gateways** tab.
 - High-level details of the connected POC device gateways are displayed.
- 4 For more detailed information, choose the > button for the appropriate gateway.
 - The **Details** and **Connected POC devices** for the chosen gateway are displayed.

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 **POC service providers** panel, choose the > button for the appropriate POC service provider.
- 3 On the **Primary care providers** panel, choose the > button for the appropriate primary care provider.
- 4 On the **POC device gateways** panel, choose the > button for the appropriate POC device gateway.
- 5 Choose the ∨ button in the row of the appropriate POC device.
 - The POC device details accordion item is expanded.

Lot management

In this chapter

5

About lot management.....	61
Adding a test strip lot to a Roche device	62

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.

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

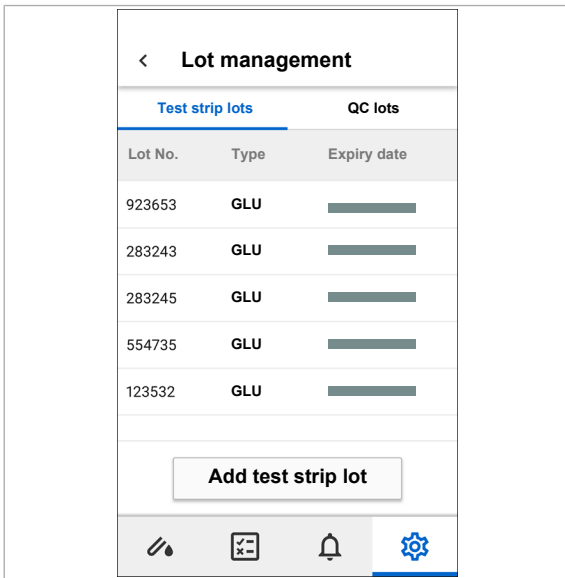


☐ The new lot has been uploaded to the DMS

☐ 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 bottle 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.

Page intentionally left blank.

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.

Page intentionally left blank.

Index

A

About monitoring, 53

C

Changing password, 49

Changing profile settings, 50

Conventions used in this publication

– abbreviations, 9

– symbols used in system, 9

Copyright, 3

D

Data security, 17

Date format, 50

Display language, 50

E

Edition notice, 2

F

Feedback, 3

G

Gateways

– monitoring, DMS, 55

– monitoring, POC device, 57

L

Logging off, 47

Logging on, 45, 46

Logging on for the first time, 45

Lot management

– test strip lot, 62

M

Monitoring

– about, 53

Monitoring DMS gateways, 55

Monitoring POC device gateways, 57

Monitoring POC devices, 58

Monitoring POC service providers, 54

Monitoring primary care providers, 56

Multimedia disclaimer, 3

P

Passwords, 45

– change, 49

– rules, 48

POC devices

– monitoring, 58

POC service providers

– monitoring, 54

Primary care providers

– monitoring, 56

R

Revision history, 2

S

Safety

– data security, 17

– system safety, 16

System safety, 16

T

Test strip lot, 62

Time format, 50

Trademarks, 3

U

User accounts, 48

User names, 45

W

Warranty, 3

Published by

Roche Diagnostics International Ltd
CH-6343 Rotkreuz
Switzerland

www.roche.com