# Security Addendum to Ventana System Software (VSS) Version 14.x


**F. Hoffmann-La Roche Ltd**
Grenzacherstrasse 124
4070 Basel
Switzerland

Roche Diagnostic Solutions
1910 Innovation Park Drive
Tucson, AZ
85755

www.roche.com

## Contacting Roche to report a cybersecurity event

In the event of a suspected cybersecurity event with Tissue Diagnostics products or services, customers should contact their local affiliate support center (For the United States, contact Roche at 1-800-227-2155).

## Cybersecurity Event Detection

Cybersecurity events are greatly reduced due to the Roche installation methodology. The system includes a mandatory hardware firewall as the outer perimeter. The system's control unit employs a hardened operating system with an Operating System (OS) firewall enabled and locked. Additionally, all removable disk drives are encrypted using Bitlocker. The hardened OS uses whitelisting to determine which applications are acceptable or trustworthy. The medical device is delivered allowing only Roche authorized software to execute. The lab operator and system users have no administrator privileges on the operating system to install or modify the applications on the OS or change the whitelist. These protections, along with scanning by antivirus software, will both prevent and detect unwanted software from being executed. When an application is attempting to be launched, Windows Defender will inform the system user that this is not possible due to permissions.

## Responding to a cybersecurity event

When an individual contacts the Roche support center to report a cybersecurity concern, Roche will follow the Roche support case handling process. A support case will be opened, information collected, and an investigation will be started. In compliance with the Roche support case process, Roche may escalate the concern to ensure the proper Roche experts are engaged, and a complete root cause analysis is performed. If a customer reports a cybersecurity or privacy issue, the appropriate Roche resources are included in the escalation. Roche customer support may advise customers to take specific action and engage their IT department to assist with these activities while an investigation and analysis of the threat is underway.Our post-market quality team will follow the security vulnerability management and incident response process outlined within Roche and provide the outcome of the investigation.

## Recovering from a cybersecurity event

All cybersecurity events are treated as unique events, and Roche aims to restore the lab to operational status as quickly and safely as possible. Roche leverages our Complaint Management System to document a customer concern and provide the required tracking, reporting, auditing, and resolution

documentation. Roche strives to address a customer's reported concern quickly while focusing on patient safety. Once the investigation is complete, the customer will be informed of the outcome and how to proceed.

## Maintaining device cybersecurity

Roche delivers the Ventana System Software (VSS) host computer with a hardened OS which both limits and prevents what instrument operators can do on the computer. Roche delivers the hardened OS with the Microsoft whitelisting and antivirus. The whitelisting allowance is fingerprinted by the Roche/Ventana manufacturer. Since the system is a Class 2 medical device, customers are required to provide strict physical access controls (biohazard) to the lab hosting the system. Only properly trained staff have access to the instrument and the software. Roche will provide the medical device system updates for all components after/pending validation from the system manufacturer and formal Roche launch. As a general rule, Roche will provide and install software patches for the medical device system based on the risk to the patient and the pre-mitigation provided by the Roche installation methodology and segmentation requirements.

Additionally, the system is delivered with a physical hardware firewall in a deny-by-default posture, and this configuration prevents unauthorized access via the customer's network. The firewall is configured for each installation allowing only specific pinholed traffic to the appropriate resources. The firewall denies common risky traffic, thus mitigating the potential for the spread of malware/viruses via the network. In addition to these protections, Roche recommends the following:

- Ensure other computers and services on the network are properly secured and protected against malicious software and unauthorized access.
- Laboratory IT is responsible for the security of their local area network, especially in protecting it against malicious software and attacks. This protection might include measures, such as an additional customer-provided firewall, to separate the device from uncontrolled networks, as well as measures that ensure that the connected network is free of malicious code.
- Restrict physical access to the system and all attached IT infrastructure (computer, cables, network equipment, and so on).
- Make sure that system backups and archive files are protected from any unauthorized access and disaster. This includes: remote storage locations, disaster recovery sites, and secure transfer of backup files.
- Use encrypted communication channels, such as TLS or SSL, between authenticated nodes.
- Access to application files and folders on any computer should be restricted only to authorized personnel.
- Users should secure their login credentials at all times to prevent unauthorized access to the application.
- Store the backups securely; that is, save them on independent disks, separated from the main server, on a different server, and so on.
- Perform regular backup restores on a test environment.
- After restoring a backup, check the source and the integrity of the data.

Roche performs penetration testing with a trusted 3rd party provider at regular intervals. We address the findings with maintenance software releases.

## Implementing security actions

Roche is committed to ensuring the utmost security and integrity of our medical devices and software solutions. In line with this commitment, we wish to remind you of several critical cybersecurity principles and practices that are essential for safeguarding sensitive patient data and ensuring the reliable operation of our systems:

1. Comprehensive Security Training: We strongly recommend that your personnel, including those in laboratory settings, receive thorough training in cybersecurity principles. This training should encompass awareness of potential social engineering tactics that malicious actors might employ to compromise system security.
2. Rigorous Password Management: The strength and confidentiality of passwords are paramount. Weak passwords pose a significant risk and could lead to unauthorized access, potentially resulting in the display of erroneous data or the exposure of sensitive information. We advise the following practices:
    - Regularly update passwords.
    - Avoid reusing passwords across different systems or applications.
    - Never share your login credentials.
    - Refrain from writing down passwords.
    - Ensure that passwords are changed upon initial system access.
3. Controlled Information Dissemination: Exercise caution in handling information pertaining to your organization's cybersecurity measures. This includes:
    - Not disclosing default passwords.
    - Restricting access to documentation detailing cybersecurity practices to authorized individuals only.
    - Ensuring sensitive information is not left in areas where unauthorized personnel might gain access.
4. Restricted Access to Sensitive Data: Access to confidential or sensitive information should be strictly limited to personnel who have the necessary authorization. This is vital for maintaining the confidentiality and integrity of patient data.
5. Network Security and Traffic Control: We advise implementing a robust network security framework. This should involve segmenting the medical device within the network and adopting a zero-trust methodology, where all network traffic is denied by default and only necessary, specific traffic is permitted. Roche collaborates with customers to identify and authorize requisite network traffic. However, the responsibility for allowing, controlling, and monitoring this traffic rests with you, our customer.

Adhering to these guidelines is critical for the security of our medical devices and the protection of patient data. Roche is dedicated to working alongside you to ensure these standards are met and maintained.

## Network and connection dependencies

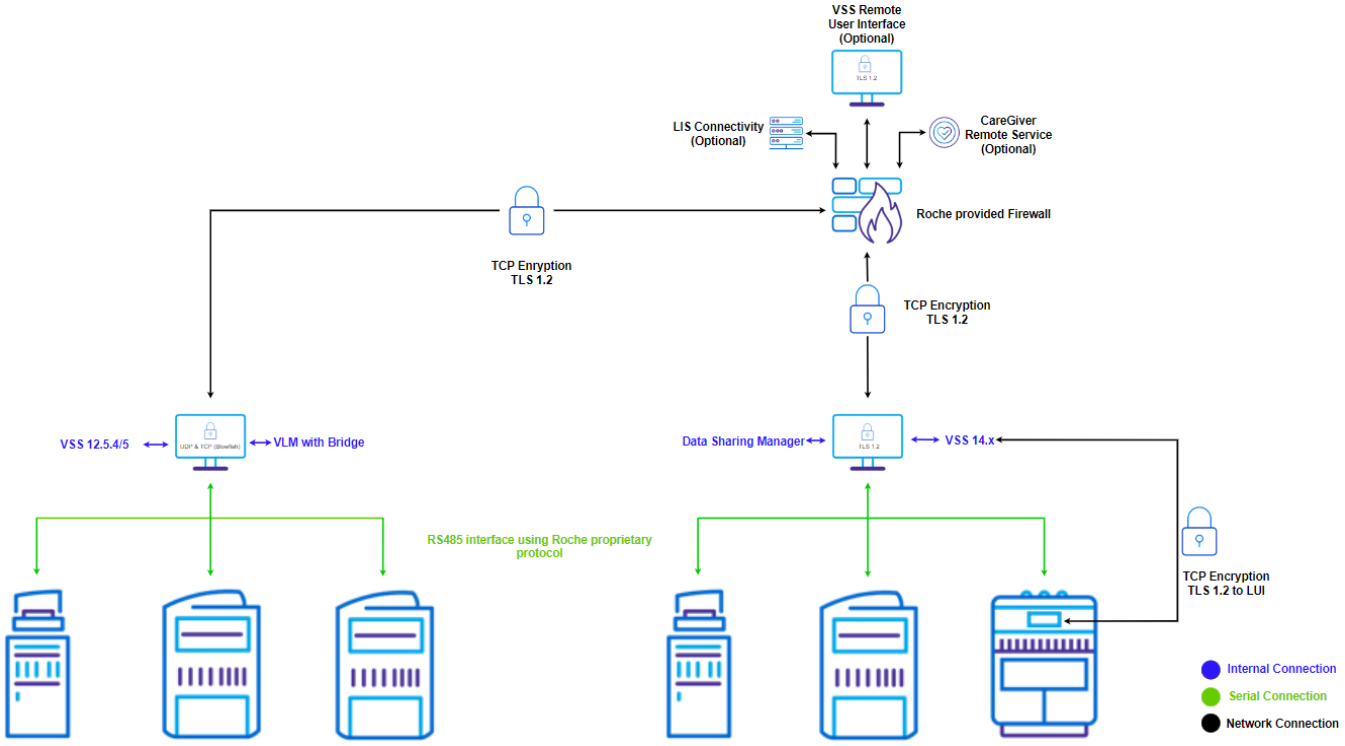
The Roche installation and operational methodology requires defense in depth from a default deny-all standpoint. The VSS system computer and networking interface is delivered with a hardened configuration. The design is for only known traffic to the Roche-provided hardware firewall and upstream systems. This system requires a Roche-provided hardware firewall to provide the mandatory

Roche-side zero-trust segmentation. The Roche firewall operates from a deny-all by default.  Under a zero-trust methodology, Roche works with each customer to ensure the concept of least networking privilege is leveraged for system operation.

The following is the controlled network traffic allowed from the Roche system:

- HL7 staining orders via 80 (HTTP) or 443 (HTTPS) from the IP address of the customer's middleware
- HL7 staining status messages via 80 (HTTP)or 443 (HTTPS) to the IP address of the customer's middleware
- UDP 53 (DNS) to the customer's internal trusted DNS server
- 443 (HTTPS) to the 4 Roche remote diagnostics IP addresses for the country/region
- Deny all other traffic.

## Interfaces and communication protocols




### VSS Host

The VSS Host is deployed on Roche hardware and shall reside standalone or in the customer network. The hardened OS includes a host-based firewall configuration that blocks all outbound and inbound traffic except for the specified ports. Traffic is not restricted based on source and destination. This VSS Host has its own certificate used for node authentication. Communication between the VSS Host and Ventana Connect will occur using SOAP  messaging over http or https. Authentication and data encryption between client and server is done over TLS v1.2 with use of the Open SSL library. All communication between the VSS Server that resides in the host and the VSS Client that resides on the Remote User Interface (RUI) is over RemObjects Super TCP channel on port 8095. Mutual authentication and data encryption between client and server is done over TLS v1.2 with use of the Open SSL library. All communication between the CareGiver server and the CareGiver agent is via a certificate-based HTTPS tunnel. The Roche CareGiver agent initializes this connection using port 443. All other ports are closed.

### VSS Local User Interface (Instrument Computer)

The VSS Local User Interface (LUI) runs an instance of the VSS Client. The VSS LUI is deployed on Roche hardware and shall reside behind the firewall. The hardened OS includes a host-based firewall configuration that blocks all outbound and inbound traffic except for the specified ports. Traffic is not restricted based on source and destination. This machine has a certificate used for node authentication. All communication between the VSS Server that resides in the host and the VSS Client that resides on the LUI over a RemObjects Super TCP channel on port 8095. Mutual authentication and data encryption between client and server is done over TLS v1.2 with use of the Open SSL library. All other ports are closed.

### VSS Remote User Interface (RUI)

The VSS RUI is a computer owned by the customer and shall reside in the customer network. This machine has a certificate used for node authentication that is the same as the VSS Host. All communication between the VSS Server that resides in the host and the VSS Client that resides on the RUI is over RemObjects Super TCP channel on port 8095. Mutual authentication and data encryption between client and server is done over TLS v1.2 with use of the Open SSL library.