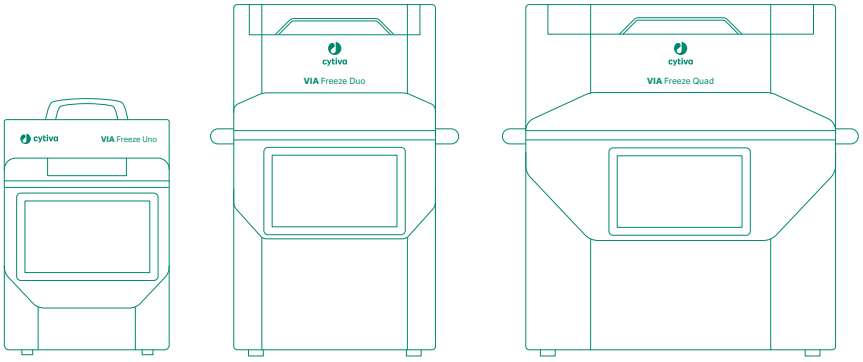
VIA Freeze™

Privacy and Security Manual



cytiva.com

Table of Contents

1 Introduction

About this manual

This manual describes the privacy and security considerations of the use of VIA Freeze™.

Purpose of this manual

This manual describes the expected intended use of VIA Freeze, the privacy and security capabilities included, and how these capabilities are configured.

Scope of this manual

This manual covers the VIA Freeze range of controlled rate freezer instruments, running software version 3.3.x and above.

There are three models available:

- VIA Freeze Uno,
- VIA Freeze Duo, and
- VIA Freeze Quad.

Introduction to privacy and security

This manual assumes that the reader understands the concepts of privacy and security. Security protects both system and information from risks to confidentiality, integrity, and availability. Security and privacy work together to help reduce risk to an acceptable level. In healthcare, the privacy, security, and safety must be balanced, relating to the intended use of the product.

The customer is encouraged to use risk management procedures to assess and prioritize privacy, security, and safety risks. Using the risk management, the customer can determine how to best leverage the capabilities provided within the product.

Product description

The VIA Freeze instruments are intended for controlled rate cooling of biological materials for subsequent cryopreservation as part of research projects or during manufacturing.

The VIA Freeze instruments are intended for research or manufacturing use only. They are not intended for clinical procedures or for diagnostic purposes.

Contact information

For specific privacy and security inquiries, use the contact form found at *cytiva.com/contact*.

Abbreviations and definitions

The following terms and abbreviations are used in this manual:

Term/Abbreviation	Definition
DNS	Domain Name System
HTTPS	Hypertext Transfer Protocol Secure
PHI	Protected Health Information
PI	Personal Information
PII	Personally Identifiable Information
TLS	Transport Layer Security
USB	Universal Serial Bus

Definitions

The following table explains the general concepts used in this manual:

Concept	Description
Chronicle™	Automation software providing an unified digital platform to monitor cell therapy facility manufacturing operations and supply chain logistics. Chronicle automation software is offered as a cloud-based solution or as a local on-premise solution.

2 Privacy and security environment

Privacy and security in the environment

VIA Freeze has been designed for an intended use with the following expectations of privacy and security protection, that should be included in the environment where VIA Freeze will be used:

- The instruments are intended to be used in laboratory environment in the development and manufacture of cell-based therapies, not accessible to the general public.
- The instruments are not intended to be patient facing equipment and are not medical devices.
- The instruments weigh between 20 to 70 kg, therefore may be physically moved out of a secure environment.
- The instruments are able (but not required) to be connected to a network in order to connect to Chronicle.

3 Authentication, authorization and audit logging

About this chapter

VIA Freeze includes a broad assortment of capabilities to enable privacy and security. This chapter describes the ability and use of these privacy and security capabilities.

In this chapter

3.1 Access controls

Introduction

The access control on VIA Freeze is used to help control access to customer information on the system. Access control includes user account creation, assigning the privileges, and other features.

Identity provisioning

The provisioning of user accounts requires the steps of account creation, maintenance, and removal of the account when it is no longer needed. A user account is created to be used by a specific individual. This user account is associated with access rights, and is recorded in system security log files.

User accounts are created by any user with ***Admin*** access level via the ***User Management*** page.

User accounts can also be created through Chronicle, and these users are synchronized to the VIA Freeze instruments. Access roles on the instruments are inherited from Chronicle.

To create an account the following information is required:

- Username, which has to be unique (including suspended and deleted accounts).

  Note: *Usernames are case-insensitive and have a maximum length of 255 characters.*

- First/last name of the user and email address for the account (optional).

User accounts can be deactivated, either permanently (delete) or temporarily (suspend), by any user with ***Admin*** access level.

The VIA Freeze instruments are delivered with a single, default ***Admin*** access level account. The default account can be deleted when at least one additional ***Admin*** level account has been created.

The VIA Freeze instruments:

- Do not contain guest accounts.
- Do not allow methods to identify inactive user accounts other than manual inspection.
- Support Emergency access via a service account that requires service authorization.

Passwords

By default, a user's password is forced to be changed upon first login.

The following restrictions apply to the passwords:

- Password minimum length is 8 characters.
- Password must contain the following categories:
  - English uppercase letters A through Z

  - English lowercase letters a through z
  - Numbers 0 through 9
- The last 10 previously used passwords cannot be reused.
- The user account is locked out after 5 failed logon attempts with incorrect passwords.

  Note: *The lockout time for repeated password failure is 10 minutes. It is not possible to inactivate the lockout time.*

User authentication

The user authentication step verifies that the user attempting to access the system is indeed the user associated with the specific account.

User Authentication is enabled by default and requires a user to enter the password for their account in order to gain access. Successive failed attempts to login will result in a lockout and an audit event being logged.

It is possible for an ***Admin*** level account to disable user authentication by enabling a feature called ***Automatic Login***. To enable the ***Automatic Login*** feature confirmation is required, as well as logging an audit event. The user that is automatically logged in is an ***Admin*** level user.

The VIA Freeze instruments:

- Do not support Single Sign On (SSO) login.
- Do not support Two Factor Authentication.

Assigning access rights

Assigning access rights is the administrative process for connecting permissions with user accounts.

The VIA Freeze instruments have user accounts with two roles:

- ***Operator***
- ***Admin***

The default role is ***Operator***.

Consider the following aspects when assigning access rights on the VIA Freeze instruments:

- It is not possible to create additional roles on the instruments and a user with an ***Admin*** level account is able to assign a role to other user accounts.
- It is possible to provide emergency access via use of service account, which can also reset passwords for other accounts.
- Users with any access level are able to export records off the instruments, but exporting audit logs requires an ***Admin*** account.
- The access control system operates in a fail – deny mode. The access control system is part of the main database and as such if that fails then most other functionality (starting protocols and accessing records) would also fail.

3.2 Audit logging and accountability controls

Introduction

Privacy and security information logging and control provide accountability through security surveillance, auditable records, and reporting.

The information logged is not configurable and information logging cannot be disabled.

VIA Freeze provides audit logging of: the following events:

- Successful and unsuccessful login attempts
- Modification of user privilege
- Creating/modifying/deleting users
- Creation and deletion of records
- Creation and deletion of protocols
- Chronicle synchronization:
  - Users
  - Protocols
  - Records
- Export of data (record, audit logs) to removable media. Success and failure.
- Export of data (record, audit logs) via email. Success and failure.
- Accessing the service screens.
- Holding a running protocol. Success and failure.
- Aborting a running protocol. Success and failure.
- Resuming a running protocol. Success and failure.
- Starting a protocol. Success and failure.
- Shutting down. Success and failure.
- System administration:
  - Autologin
  - Session timeout
  - Software update
- Starting remote service tool.

The audit log contains the following details of the event:

- Date/time of the event
- User who was logged in at time of the event

Logs are stored on the instruments in a MySQL database. It is not possible to alter the logs on the instruments.

No PHI is stored on the instruments, therefore there are no reports regarding its exposure.

3.3 Patient privacy consent management

Patient privacy

VIA Freeze does not handle (create, transfer, or store) patient data, therefore the patient privacy consent is not applicable to VIA Freeze.

4 Information protection

About this chapter

This chapter describes privacy and security operations, and contains guidelines for the preparation of a secure environment for VIA Freeze.

Defense in depth

Security operations are best implemented as part of an overall "defense in depth" information assurance strategy. This strategy is used throughout an information technology system that addresses personnel, physical security, and technology. The layered approach of defense in depth limits the risk that the failure of a single security safeguard allows the system to be compromised.

In this chapter

4.1 Network security

System interconnections

The table below describes the system interconnections available for VIA Freeze. None of the connections described is required for normal functionality of the instruments.

Source/Destination	Network Service	Description
VIA Freeze / Chronicle (optional)	HTTPS	Record upload, event upload, protocol download, user download, software updates download
VIA Freeze	SMTP	Records export
VIA Freeze / Remote support	TCP/UDP	Remote service
VIA Freeze / DNS server	DNS	DNS resolution for Chronicle

Wired network security

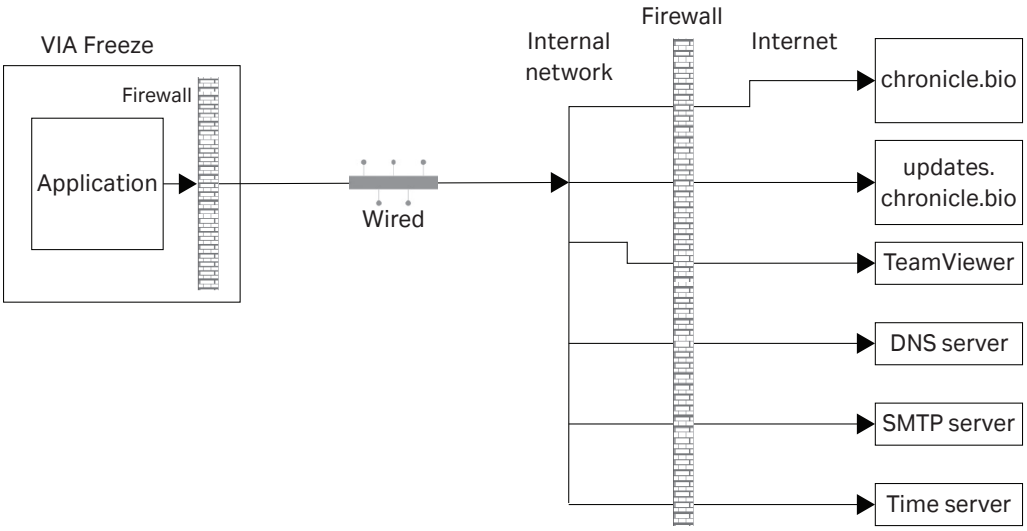
Cytiva strongly recommends that VIA Freeze is operated in a network environment that is separated from the general purpose computing network of the owner's organization. There are many effective techniques for isolating VIA Freeze on a secure subnetwork, including implementing firewall protection, demilitarized zones (DMZs), virtual local area networks (VLANs), and network enclaves.

To assist in secure network design, the following sections describe the required network services for VIA Freeze.

MAC and IP address are visible on the engineering screen of the VIA Freeze instruments.

Network connection

The following illustration shows recommended ways to connect the VIA Freeze instruments to the customer network, using a wired network.



Consider the following aspects when connecting the VIA Freeze instruments to the customer network, using a wired network:

- The firewall of the instruments is software based and is managed using iptables.
- Communication with Chronicle is done via HTTPS across the wired connection.
- Time synchronization is done via time server of Ubuntu™ using NTP.

Network profile and required network services

The following table shows the network profile and required network services for VIA Freeze.

Port	Protocol	Direction	Network Service	Source/Destination
443	tcp	Inbound/ Outbound	Proprietary protocol over sockets for conversation with Chronicle	Data transfer to/from the Chronicle server. The Chronicle server is a Cytiva-hosted server (for example, *https://pre-gmp.chronicle.bio*).
443	tcp	Inbound/ Outbound	Proprietary protocol over sockets for download of software updates	*https://updates.chronicle.bio*
443	tcp	Inbound/ Outbound	HTTPS	TeamViewer™[1]
443	WSS	Inbound/ Outbound	HTTPS	***Link*** mode support

Port	Protocol	Direction	Network Service	Source/Destination
53	udp/tcp	Inbound/ Outbound	DNS	DNS Server for resolving the Chronicle and updates.chronicle.bio servers.
587	tcp	Inbound/ Outbound	SMTP	User configured email server
123	udp	Inbound/ Outbound	NTP	Time server
5938	udp/tcp	Inbound/ Outbound	Remote service	TeamViewer

[1] TeamViewer is the remote-support software in use on the system. Sessions are opt-in by a local user and can be terminated by a local user at any time.

Wireless network security

Radio signals are used in a wireless network communication, therefore wireless devices require special security consideration. Effective techniques and tools exist for improving the security of wireless communication. This section describes the characteristics for wireless connections for VIA Freeze.

The VIA Freeze instruments do not support wireless networking.

4.2 Removable media security

Removable media

VIA Freeze provides the possibility to use removable media, for example USB storage media.

USB ports are enabled and freely accessible. USB ports are used for:

- Exporting of records via USB flash drive.
- Use with accessory and/or input devices (e.g., keyboard, barcode scanner, mouse etc).

Use of the USB ports is not privileged although export of privileged information (e.g. audit log) is only possible for users with ***Admin*** access level.

No PII/PHI is collected in the audit log.

Serial ports are internal to the instruments and require tools to access. They are used by service during some servicing procedures and access is not privileged.

Booting from removable media

Booting from removable media requires access to the serial port which is internal to the instruments.

AutoPlay disabled

Autorunning from removable media is disabled.

4.3 Data storage and encryption

Encryption of data at rest

Fields in the database that may contain PII are encrypted at rest (first name, last name, email address, record name).

Removable media is not encrypted as it is not supplied with the instruments.

Database backups are not encrypted.

Data in transit security

Internal data transit is local to the app and not remotely viewable. Data is uploaded to Chronicle via HTTPS.

Data integrity capabilities

VIA Freeze has capabilities to make sure that the data is not accidentally or maliciously modified.

Data from sensors is checked via CRC to ensure integrity; data that fails the check is discarded.

It is not possible to directly edit data stored in the database and previous versions are maintained.

De-identification capabilities

VIA Freeze is not a medical device and does not handle (create, transfer, or store) patient data. Therefore VIA Freeze does not contain de-identification (anonymization and pseudonymization) capabilities.

Business continuity

If VIA Freeze is networked and connected to Chronicle, records are automatically uploaded.

Performing local backups is a manual process which is possible for ***Admin*** level users through the user interface to a USB drive. The backup consists of just the database and is unencrypted. Restoring the database is a service procedure along with restoring software in the event of a complete loss.

As the database is local to the instruments, in the event of drive failure, standard data retrieval methods may be able to get data off the drive.

Storage is on an internal SSD; no RAID or SAN are possible. Storage and encryption of the backups is a choice of the user, e.g. offsite or cloud storage.

4.4 External connections

Security controls provided by the cloud provider

VIA Freeze is not hosted on a third party cloud environment. Cloud security controls are not applicable.

VIA Freeze is able to interface with Chronicle automation software. The privacy and security aspects of Chronicle are outside the scope of this document. For more information, contact your local Cytiva representative.

5 System protection

Introduction

This chapter describes the guidelines for how to configure and maintain the product in a way that continuously protects privacy and security.

Protection from malicious attacks

The computing environment is increasingly hostile, and threats continue to grow from denial of service attacks and malicious software, including computer viruses, worms, Trojan horses, and other malware. Vigilant defense on many levels is required to keep the systems free from intrusion by malicious software. In most cases, effective protection requires cooperation between Cytiva and our customers.

The VIA Freeze instruments are single purpose (dedicated) instruments that have controlled intended use, and thus can be hardened. A hardening approach is employed to maximize security. This approach focuses on locking down the instruments to eliminate vulnerabilities with OS configuration and host-based firewalls versus the signature-based detection technique used by common off-the-shelf anti-malware solutions.

The following are justifications for not including 3rd Party Anti-Malware software:

- No operating system facilities allowing installation, modification or running of additional software are available.
- Cytiva provides antimalware capabilities through whitelisting or the equivalent instead of installing and executing Anti-Malware software.
- Anti-Malware does not protect against insider threats, zero-day attacks, or misuse by organizational staff; whitelisting provides better protection against threats.
- Utilizing whitelisting or otherwise preventing installation, modification, or execution of any additional software negates the need for run-time Anti-Malware software with its attendant requirements of connectivity and frequent updating.
- The installed software image is scanned for malware at the time of build and carefully controlled throughout installation ensuring that the executable is free from malware at execution time.
- Maintaining appropriate firewall settings and limiting physical access to the system reduces the possibility of introducing malicious software to the system.

Server and workstation security

VIA Freeze contains additional features to improve local operational security:

- The instruments are single self-contained units and the only access points are via the physical touchscreen and the physical USB port.
- A login session will expire and logoff after a period of inactivity which is configurable by administrators.

- Multiple successive failed login attempts cause the account to be locked for a period of time.
- Database fields that contain PII are encrypted at rest.
- The firewall blocks all incoming connections with exceptions for functionality listed in section *Section 4.1 Network security, on page 12*.

Patch management practices

Cytiva patches instruments using a risk-based model, where vulnerabilities go through a risk assessment process and patch deployment occurs according to the severity of the risk determined in the assessment.

Vulnerabilities are identified and new releases are created to provide any updates. The customer chooses whether to install updates, and installation is performed by service personnel. Any risks are communicated through customer change notifications.

The following applies to software installation on VIA Freeze:

- Installation of additional software requires physical root access to the machine.
- To update the VIA Freeze software it is required an ***Admin*** level or service user to authenticate and trigger a software update.
- It is possible to install software updates over the network via Chronicle.

6 Remote access

Introduction

Often the most efficient and cost-effective ways for Cytiva to provide service is to connect to VIA Freeze remotely. Every effort is made to make sure that this connection is as secure as possible. This chapter describes the security measures for remote access connections.

VIA Freeze uses TeamViewer as remote support software. Sessions are opt-in by a local ***Admin*** user and can be terminated by a local user at any time.

7 Personal information collected by the product

Personal information

VIA Freeze is not a medical device and does not handle (create, transfer, or store) patient data. VIA Freeze does not collect personal information.

8 Product security supplemental documents

Software Bill of Materials (SBOM)

SBOM is available for VIA Freeze upon request. Contact the sales representative for a copy of SBOM.

Page intentionally left blank

cytiva

cytiva.com

For local office contact information, visit cytiva.com/contact

29443719 AA V:3 02/2022