My Instruments 1.2

Privacy and Security Manual

cytiva.com

Table of Contents

1 Introduction 3

2 Privacy and security environment 4

3 Privacy and security capabilities 5

3.1 Access controls 6

3.2 Privacy and security audit logging and accountability controls 9

4 Information protection 10

4.1 Network security 12

4.2 Wireless security 14

4.3 Removable media security 15

4.4 Data at rest security 16

4.5 Data integrity capabilities 17

4.6 De-identification capabilities 18

4.7 Business continuity 19

4.8 Security controls provided by the cloud provider 20

5 System protection 21

5.1 Protection from malicious attacks 22

5.2 Server and/or workstation security 23

5.3 System change management 24

6 Remote service 25

7 Personal information collected by the product 26

1 Introduction

About this chapter

This manual describes the privacy and security considerations of the use of the My Instruments.

Purpose of this manual

This manual describes the expected intended use of My Instruments, the privacy and security capabilities included, and how the product is configured and used appropriately.

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 protects privacy, but also protects more broadly against these risks. Privacy requires security. In the working environment one must balance privacy, security, and safety. Most of the time there is no conflict between these three domains of risk. The customer is encouraged to use risk management procedures to assess and prioritize privacy, security, and safety risks. Through the use of risk management one can determine how to best leverage the capabilities provided in My Instruments.

Important user information

My Instruments is not a medical device and shall not be used in any clinical procedures or for diagnostic purposes.

Contact information

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

2 Privacy and security environment

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

- It is strongly recommended that the computer hosting My Instruments server resides in a controlled server environment.
- All communications with My Instruments use encrypted protocols.
- All users of My Instruments use their own unique identity.
- Mobile devices used outside of the secured environment must be protected by the customer cyber security policies.

3 Privacy and security capabilities

My Instruments includes a broad assortment of capabilities to enable privacy and security. This chapter describes the capability and use of these privacy and security capabilities.

In this chapter

Section		See page
3.1	Access controls	6
3.2	Privacy and security audit logging and accountability controls	9

3.1 Access controls

The access control features of My Instruments can be used to control access to sensitive information. Access control includes user account creation and assigning privileges.

My Instruments is installed with a default user which must be changed after the installation for better access control.

Identity provisioning

The provisioning of user accounts includes the steps of account creation, maintenance, and suspension of the account when it is no longer needed. A user account is created for a specific individual and is associated with access rights and is recorded in security audit logging.

User accounts are created by adding users to the configuration files for the adapters residing in My Instruments. A password generator tool is included as a part of My Instruments installation. This password generator assists with creating hashed version of passwords. However, the colon (:) and the quotation (") characters are not allowed in usernames.

Even though the password generator does not require a certain type of password by default, there is an optional flag `-V` which validates the password. The password:

- must have 8 to 10 characters,
- must contain lower case letters,
- must contain at least 2 digits,
- must begin and end with a letter,
- must not contain the username.

The credentials for an inactive user is removed by removing the corresponding user account from the configuration file.

Note: *Any changes in the configuration files require a restart of the My Instruments.*

User authentication

The User Authentication step verifies that the user attempting to use the system is indeed the user associated with the account given. This section covers the administration of the authentication systems to be used.

- Authentication to My Instruments is done using a challenge-response sequence where the transferred data uses the one-way hash function SHA256 to make sure that it is not possible to recreate the data.
- There is no root/admin account for My Instruments.

- In a validated environment, the ***Save Password*** functionality needs to be deactivated and it is recommended that the user logs out from the application when leaving.

5.2.1 X.509 digital certificates

My Instruments uses an installed certificate with the following RFC 5280 compliant X.509 digital certificates:

- Root certificate with the subject name `UNICORN Public Root SSL CA`.
- Separate server certificate for each instrument server, signed by the above mentioned root certificate, with subject name `UNICORN Public SSL Certificate`.

The following applies for installation of digital certificates:

- The root certificate and its public key is installed in the trusted root certificate store on the local computer during the installation of My Instruments. It is valid for two years from its creation date, which is not necessarily the same as the installation date.
- The server certificate is generated during the installation of My Instruments. It is valid for two years from its creation. It is stored in the personal certificate store on the local computer. The private and public keys are locally stored. The private key is exportable for users that have access to the certificate store.

The following applies for removal of digital certificates:

- Do not remove the ROOT certificate as it can be shared between several Cytiva products.
- The generated SSL certificates can be removed if My Instruments is uninstalled or if the user has changed the certificates to their own certificates.
- The certificates can be removed by manually deleting them from the personal certificates folder in the local computer store on the computer where My Instruments has been installed. Depending on what has been installed there can be several certificates with the same subject name. Make sure that the correct certificate is removed. Do not remove all of them.

The following applies for renewal of server certificates:

- To renew the supplied certificates before the expiration date 15 October 2021, reinstall My Instruments. When reinstalling My Instruments, new certificates are generated. See *My Instruments Installation Guide* for information on how to renew the certifiace without reinstalling My Instruments.

Installation of certificates registered for the customer domain is encouraged, but it does not remove the original certificates automatically, this has to be done manually. For detailed information, see the My Instruments installation manual.

The included certificates are self-signed and not meant to be used in an environment that needs correct certificate authorities. The user is therefore encouraged to install their own certificate.

Assigning access rights

The assigning of access rights is the administrative process to associate permissions with user accounts.

My Instruments requires each user to have at least one role and one privilege. It is installed with default role ***system*** and privilege ***system*** which should be changed for better protection.

For instruments sending data to My Instruments require that they have the role ***system*** and the privilege ***dashboard***. User accessing the dashboard for monitoring the instruments are required to have the role ***dashboard*** and the privilege ***dashboard*** (in public areas) or ***control*** (in private areas) for elevated user rights. The instrument accounts reside in the configuration file for the Data Source Adapter (DSA) and the user accounts in the configuration file for the Client Adapter (CA). Any account without proper access rights is not able to access My Instruments

Patient privacy consent management

Patient privacy consent management is the process of supporting the patient expressing their privacy requirements. This is distinct from other forms of consent such as the consent to treat.

My Instruments does not create, transfer, or store patient data, therefore the patient privacy consent is not applicable.

3.2 Privacy and security audit logging and accountability controls

Privacy and security audit logging and accountability controls supports Security surveillance and privacy investigations and reporting.

The audit log resides in the server hosting My Instruments. It contains information about granted access for users and instruments as well as failed connection attempts. General information about startup, shutdown, and performance alerts can also be found in this log. The log file is located at `C:\ProgramData\Cytiva\My Instruments\Logs`

4 Information protection

This chapter focuses on privacy and security operations, and contains information to guide in the preparation of a secure environment for My Instruments.

In this chapter

Section		See page
4.1	Network security	12
4.2	Wireless security	14
4.3	Removable media security	15
4.4	Data at rest security	16
4.5	Data integrity capabilities	17
4.6	De-identification capabilities	18
4.7	Business continuity	19
4.8	Security controls provided by the cloud provider	20

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 to compromise the system.

IMPORTANT

My Instruments encrypts certain connections using the TLS protocol. TLS 1.0 and TLS 1.1 are not considered secure anymore and hence only TLS 1.2 or higher must be used. My Instruments uses certificates for encryption that are located in Windows Certificate Store. As a limitation of Windows 10, it is currently neither possible to allow certain versions of TLS nor to reject others using this solution. Therefore, it is recommended to block the use of TLS 1.0 and TLS 1.1 on operating system level instead. Please refer to Microsoft Windows documentation for instructions on how to block specific TLS versions. **Not allowing TLS 1.0 and TLS 1.1 on operating system level will affect all applications running on the computer**.

4.1 Network security

Cytiva strongly recommends that My Instruments is operated in a network environment that is protected from unauthorized intrusion.

To assist in secure network design, the following network profile outlines the required network services for the My Instruments. The table below contains information about the network ports that must be accessible on the server hosting My Instruments:

IMPORTANT
The following are the default ports used during the My Instruments installation and can be reconfigured by the user. All firewall exception handling must be done by the user except the default ports for Windows firewall.

Port	Protocol	Direction	Network Service	Source/Destination
9000	https	Inbound	Instrument data publish	Instrument data publish
8080	https	Inbound	HTML5 Web App	HTML5 Web App

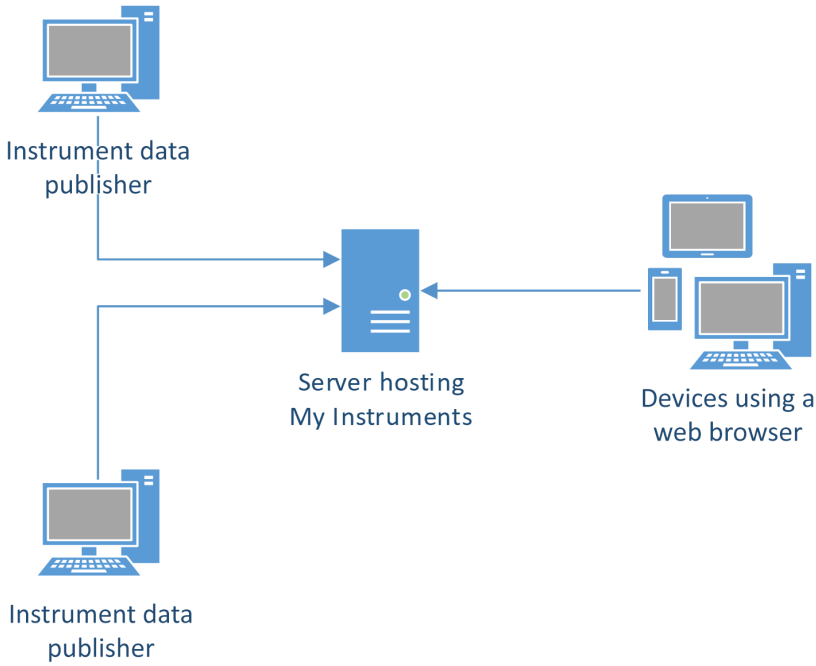
The servers hosting the Instrument Servers requires the following network profile to be able to reach the server hosting the My Instruments:

Port	Protocol	Direction	Network Service	Source/Destination
Any	https	Outbound	Instrument data publish	Server hosting My Instruments

Computers hosting a web browser intended to access My Instruments requires the following network profile to be able to reach the server hosting My Instruments:

Port	Protocol	Direction	Network Service	Source/Destination
Any	https	Outbound	HTML5 Web App	Server hosting My Instruments

The following illustration gives a schematic overview of My Instruments installation:



4.2 Wireless 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 My Instruments.

Apply the appropriate company policies when accessing My Instruments via a wireless connection. For example, use WPA2 for network transmission encryption and mutually authenticated TLS for transport control security. MAC address filtering is also something that can be considered for enhancing security as well as limited transmission power rage and no SSID broadcasting.

4.3 Removable media security

My Instruments does not require any removable media to operate. However, it is strongly recommended that the company policies related to removable media are applied to the computer hosting My Instruments.

4.4 Data at rest security

No information related to instrument state and status is stored in a persistent storage. User credentials are stored locally in the configuration file using the SHA256 hash algorithm.

4.5 Data integrity capabilities

My Instruments contains capabilities to make sure that data are not inappropriately modified either accidently or maliciously. Any state or status originating from the instruments are stored untouched in RAM of the server hosting My Instruments. The web application that fetches and displays data does not modify the data and displays the data in its original form.

4.6 De-identification capabilities

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

My Instruments contains no de-identification (anonymization and pseudonymization) capabilities to limit privacy and security risks to sensitive information.

No Privacy Information (PI) is collected by My Instruments apart from the user ID of the user currently logged in to an instrument. This information is available to all users of My Instruments and is visible on the web application. The information is protected by HTTPS (TLS) when transmitted from the instrument to the server hosting My Instruments as well as between the web application and the server.

4.7 Business continuity

A disaster recovery of My Instruments is easy since there is no database or similar that requires backup or restore. However, it is recommended to back up configuration files in a secure media to be used whenever a reinstallation of My Instruments is required.

4.8 Security controls provided by the cloud provider

My Instruments is not hosted on a third party cloud environment. Cloud security controls are not applicable.

5 System protection

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

The System is configured and maintained in a way that protects privacy and security.

In this chapter

Section		See page
5.1	Protection from malicious attacks	22
5.2	Server and/or workstation security	23
5.3	System change management	24

5.1 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.

My Instruments is designed to be used in an environment where commercial Anti-virus software is used to detect the presence of malicious software (virus, Trojan horse, worm, etc). The use and configuration of the specific AntiVirus software is encouraged.

Note: *During virus scans, the performance of My Instruments can be affected and therefore it is highly recommended to do the scans during non-office hours. The current organizational policies and procedures regarding AntiVirus software should be applied with the proper network defenses activated.*

5.2 Server and/or workstation security

My Instruments is deployed in a customer controlled environment, hence the customer is responsible for local operational security.

5.3 System change management

The customer is responsible for maintaining the computer hosting My Instruments. This maintenance includes the following:

- Applying operating system patches.
- Applying operating system upgrades.
- Applying operating system configuration changes .
- Applying operating system routine maintenance.
- Applying My Instruments patches.
- Applying My Instruments upgrades.
- Applying My Instruments configuration changes.
- Applying My Instruments routine maintenance.

Furthermore, any malware protection software installed must also be maintained by the customer. This maintenance includes management of patches, upgrades, configuration change, and routine maintenance. For more information about how to apply malicious software protection, see *Section 5.1 Protection from malicious attacks,* .

It is important to apply necessary security updates to keep the computer secure. However, all security software and computer maintenance software must be configured so that they do not interfere with My Instruments when in use. See the following guidelines:

- No disk defragmentation.
- No full disk scans for malicious software. Only use on file access scan.
- No software inventory scans or other tasks run by endpoint management software.
- No software updates when My Instruments is in use. This includes Windows update and end point protection software. It is known that some end point security software suspends network traffic during the update.
- Create exceptions for UNICORN related processes when data leak prevention software is being used.

Questions or incident reports regarding cyber security related to My Instruments can be done via the appointed Cytiva Key Account Manager.

- A security enhancement is requested in My Instruments.
- A security incident has occurred related to the usage of My Instruments.
- A general question about the existence of security related patches for My Instruments.
- A general question about the availability of online material such as documentation and similar.

6 Remote service

Remote service possibility is not implemented for My Instruments.

7 Personal information collected by the product

No personal information is collected by My Instruments besides the user ID of the user currently logged in to an instrument. This information is not stored persistently and is removed when the server hosting My Instruments is restarted.

Page intentionally left blank

cytiva

cytiva.com

Cytiva and the Drop logo are trademarks of Global Life Sciences IP Holdco LLC or an affiliate.

Windows, Microsoft .NET, and Windows Server are registered trademarks of Microsoft Corporation.

All other third-party trademarks are the property of their respective owners.

© 2020-2021 Cytiva

UNICORN © 2020-2021 Cytiva

Any use of UNICORN is subject to Cytiva Standard Software End-User License Agreement for Life Sciences Software Products. A copy of this Standard Software End-User License Agreement is available on request.

All goods and services are sold subject to the terms and conditions of sale of the supplying company operating within the Cytiva business. A copy of those terms and conditions is available on request. Contact your local Cytiva representative for the most current information.

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

29323950 AD V:7 02/2021