UNICORN™ 7.5

Privacy and Security Manual

gelifesciences.com

Table of Contents

1 Introduction

About this manual

This manual describes the privacy and security considerations of the use of UNICORN 7.5.

Purpose of this manual

This manual describes the expected intended use of UNICORN, the privacy and security capabilities included, and how the product is configured, maintained, 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 UNICORN.

Important user information

UNICORN 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.gelifesciences.com/contact*.

2 Privacy and security environment

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

- It is strongly recommended that the computer(s) hosting UNICORN server reside(s) in a controlled server environment.
- Parts of the internal communication in UNICORN use encrypted protocols.
- All users of UNICORN 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

About this chapter

UNICORN 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

3.1 Access controls

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

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 from the UNICORN ***Administration*** module by invoking the ***User Setup*** dialog box. The dialog box contains fields for user name, a full name, a job title, and an email field. A user must belong to an access group which is also defined in this dialog. A temporary password is required for the user to be able to log on to UNICORN. The user is asked to enter a new password at the first time logon.

A user account can also be associated with a password used as digital signatures. This is also a part of the ***User Setup*** dialog and is administratively treated in the same way as the logon password.

A password can be any combination of letters, numbers, and special characters that fulfill the current password rules. The rules, for example, minimum password length, required and allowed characters in a password etc., are defined in the Password Policy in UNICORN ***User Setup***.

A user account can be locked for logon either by a defined expiration time or manually by a system administrator. A locked account does not have access to UNICORN until it is unlocked. A user with the access group ***User Setup*** access level can lock and unlock user accounts. A user account can be deleted via the ***User Setup*** dialog box.

Note: *Methods and results for a deleted user are kept in the system.*

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 UNICORN is done by comparing a hash of the password and a salt with the corresponding hash stored in the UNICORN database when the user setup indicates that the user is a `local user`. SHA256 is used to create hashes. UNICORN 7.4, and earlier versions, stored encrypted passwords in the database using 3DES. A stored password is replaced by a salted hash the next time the user log in into UNICORN.

- Authentication to UNICORN is done via LDAP when the user setup indicates that the user is a `network user`.
- There is a default account for UNICORN with a default password that has unrestricted access to all UNICORN functions. UNICORN requires that default passwords are changed at first log on. It is recommended to delete this user when regular user profiles have been created.

Assigning access rights

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

An access right is defined by access groups, all assigned to various levels of access to UNICORN. For practical reasons, it is recommended to only use a limited number of groups that correspond to different job descriptions in your organization. Some access groups are predefined, for example the Administrators group.

User access rights are defined from UNICORN ***Administration*** module by invoking the User Setup dialog box. The dialog box allows adding members to and removing members from specific access groups.

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.

UNICORN 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 the UNICORN database. It contains information about granted access for users as well as their usage of the system.

4 Information protection

About this chapter

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

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.

In this chapter

4.1 Network security

GE strongly recommends that UNICORN and ÄKTA™ systems are operated in a secure network environment that is protected from unauthorized intrusion. There are many effective techniques for isolating and protecting UNICORN installations, including implementing firewall protection, and Virtual Local Area Networks (VLANs).

To assist in secure network design, the following network profile outlines the required network services for UNICORN.

The following terminologies are used in this section:

Terminology	Description
UNICORN Client	A software consisting of the ***Administration***, ***Method Editor***, ***Evaluation***, and ***System Control*** modules.
UNICORN Instrument Server	A collection of processes that controls an ÄKTA system or some other system that is supported by UNICORN. For some deployments, the UNICORN Instrument Server processes are divided in different hardware, for example, the UNICORN control PC and the Real-Time Unit. An HTTP/WebSocket API can also be enabled to view and control the Instrument Server.
UNICORN User Server	A collection of processes enabling an HTTP API to fetch results and authenticate. For some deployments, it is possible to colocate the UNICORN User Server with the UNICORN Instrument Server.
Griffin	A software developed by GE Healthcare and used by GE Healthcare service persons to test the ÄKTA system hardware components.
OPC	An industry standard for data-exchange in the industrial automation space. OPC defines the interface between clients and servers including access to real-time data, monitoring of alarms and events, and access to historical data.
OPC HDA	A historian according to the industry standard for OPC.
OPC Server	UNICORN Instrument Server implements OPC interfaces and acts as an OPC server.

Terminology	Description
OPC Client	Any software that implements the client part of the OPC specification.

UNICORN can be deployed in many ways but a fully networked solution consists of several parts. UNICORN itself can be distributed into UNICORN clients, UNICORN Instrument Servers, UNICORN User Server, UNICORN database, and GE Healthcare license server. Optionally, Real-Time Unit can be used for a robust operation of ÄKTA systems. ÄKTA systems shall always be connected to a network adapter on the control PC or a network adapter on a Real-Time Unit. ÄKTA systems shall not be directly connected to the LAN.

There are two different technologies for communicating with ÄKTA systems, one is software based and the other is hardware based in the form of CU950/960. In addition to UNICORN there can be OPC clients, an Active Directory server, an email server, Griffin clients, and My Instruments. This section describes only the network environment for UNICORN.

The information in this section is based on a full-scale network solution that may not be applicable for small scale installations. It is also assumed that a firewall is active on every computer. The firewall blocks both inbound and outbound communication unless there are firewall rules allowing it. If a simpler installation is used then some of the communication will only take place on local host.

The following computers are used in a full-scale network solution:

Id	Description
UPC1	PC with UNICORN Client, optionally with a running OPC HDA server
UPC2	PC with UNICORN Instrument Server (without Real-Time Unit)
UPC3	PC with UNICORN Instrument Server (using an Real-Time Unit)
UPC4	PC with UNICORN Instrument Server (using CU950/960)
UPC5	PC with UNICORN User Server
UPC6	PC with HTTP/WebSocket client
Real-Time Unit	Real-Time Unit (hardware)
LS	GE Healthcare license server

Id	Description
DB	Microsoft® SQL Server (database in data center or installed by UNICORN installation program)
GPC	PC with Griffin
AD	Active Directory
ES	Email server
OPC	OPC client
ÄKTA system	ÄKTA system
ÄKTA classic system	ÄKTA classic system (CU950/960 based)

Common communication scenarios:

Description	Computer connection(s)
Control an ÄKTA system with UNICORN	UPC1 -> UPC3 -> ÄKTA system
Control an ÄKTA system with UNICORN	UPC1 -> UPC2 -> Real-Time Unit -> ÄKTA system
Control an ÄKTA system with UNICORN	UPC1 -> UPC4 -> ÄKTA classic system
Starting UNICORN Client	UPC1 -> LS and UPC1 -> DB and optionally UPC1 -> AD
Connecting OPC client to OPC HDA server	OPC -> UPC1
Connecting OPC client to UNICORN Instrument Server	OPC -> UPC2, UPC3 or UPC4
Connecting an HTTP/WebSocket client to UNICORN Instrument Server	UPC6 -> UPC2, UPC3 or UPC4
Connecting an HTTP client to UNICORN User Server	UPC6 -> UPC5
Sending E-mail	UPC1 or UPC2 or UPC3 or UPC4 -> ES

Description	Computer connection(s)
Database access in general	UPC1 or UPC2 or UPC3 or UPC4 -> DB
Testing an ÄKTA system with Griffin (no Real-Time Unit)	GPC -> UPC2
Testing an ÄKTA system with Griffin (with Real-Time Unit)	GPC -> UPC3 followed by GPC -> Real-Time Unit

Note:

- *Processes in general must be allowed to communicate on local machine.*
- *If firewall rules are restricted to specific applications, the paths to executables can differ between UNICORN versions.*

Firewall settings for UPC1

Inbound traffic from OPC clients (if OPC HDA server is used)

Outbound traffic to UNICORN Instrument Server, database, Active Directory (if LDAP is used), email-server.

Port	Protocol	Direction	Program	Source/Destination
135	TCP	Inbound		DCOM for OPC
Any	Any	Inbound	OPCEnum.exe	DCOM calls to OPCEnum
Any	Any	Outbound	OPCEnum.exe	DCOM calls from OPCEnum
Any	Any	Inbound	UNICORN HDA Service.exe	DCOM calls to OPC HDA Service
Any	Any	Outbound	UNICORN HDA Service.exe	DCOM related to OPC
1433	TCP	Outbound	UNICORN-Client.exe	UNICORN Client -> database
1434	UDP	Outbound	UNICORN-Client.exe	UNICORN Client -> database

Port	Protocol	Direction	Program	Source/Destination
40500–40502	TCP	Outbound	UNICORN-Client.exe	UNICORN Client -> UNICORN Instrument Server
40511	TCP	Outbound	UNICORN-Client.exe	UNICORN Client -> UNICORN Instrument Server
40511	TCP	Outbound	SystemInstallation.exe	UNICORN Installer -> UNICORN Instrument Server
9920	TCP	Outbound	UNICORN-Client.exe	UNICORN Client -> UNICORN Instrument Server
###	Any	Outbound	UNICORN-Client.exe	UNICORN Client -> email server
636	TCP	Outbound	UNICORN-Client.exe	UNICORN Client -> Active Directory (encrypted)
389	TCP	Outbound	UNICORN-Client.exe	UNICORN Client -> Active Directory (no encryption)
139	TCP	Inbound		NetBIOS to enable OPC Client -> OPC communication with UNICORN Instrument Server
445	TCP	Inbound		SMB to enable OPC Client -> OPC communication with UNICORN Instrument Server
27000–27009	TCP	Outbound	UNICORN-Client.exe	UNICORN Client -> License Server (gehealth.exe)
Any (dynamic)	TCP	Outbound	UNICORN-Client.exe	UNICORN Client -> License Server (lmgrd.exe)

Network discovery must be enabled in firewall to allow computer name resolution. This can be restricted to the following predefined rules found in the Windows® firewall:

Windows firewall rule	Direction
FPS-NB_Datagram-In-UDP	Inbound

Windows firewall rule	Direction
FPS-NB_Name-In-UDP	Inbound
FPS-LLMNR-In-UDP	Inbound
FPS-NB_Datagram-Out-UDP	Outbound
FPS-NB_Name-Out-UDP	Outbound
FPS-LLMNR-Out-UDP	Outbound

Note:

- *Select one of the rules for LDAP communication with Active Directory, either encrypted or non-encrypted depending on how UNICORN is configured.*
- *Rules related to OPC can be omitted if OPC is not used.*
- *### = Remote port number depends on customer installation.*
- *Additional firewall rules can be needed if extensions are installed in UNICORN Client. Check necessary firewall rules.*

Firewall settings for UPC2

Inbound traffic from UNICORN Clients, OPC clients, HTTP/WebSocket clients, and Griffin.

Outbound traffic to Real-Time Unit, database, and email-server.

Port	Protocol	Direction	Program	Source/Destination
40500-40502	TCP	Inbound	UNICORN Instrument Server.exe	UNICORN Instrument Server
50000-50003	UDP	Outbound	VIDmain.exe	UNICORN Instrument Server-> ÄKTA system
40504-40510	UDP	Inbound	VIDmain.exe	ÄKTA system -> UNICORN Instrument Server
40503	TCP	Inbound	VIDmain.exe	Griffin -> UNICORN Instrument Server
9920	TCP	Inbound	UNICORN Support Service.exe	UNICORN Instrument Server

Port	Protocol	Direction	Program	Source/Destination
40511	TCP	Inbound	RemoteDeploymentService.exe	UNICORN Client -> UNICORN Instrument Server
40513	TCP	Inbound	UNICORN Instrument Server.exe	HTTP/WebSocket Client -> UNICORN Instrument Server
40514	TCP	Inbound	UNICORN Instrument Server.exe	HTTP/WebSocket Client ->UNICORN Instrument Server
Any	Any	Outbound	UNICORN Instrument Server.exe	DCOM, UNICORN Clients, Email server, My Instruments etc.
135	TCP	Inbound		DCOM for OPC
Any	Any	Inbound	OPCEnum.exe	DCOM calls to OPCEnum
Any	Any	Outbound	OPCEnum.exe	DCOM calls from OPCEnum
Any	Any	Inbound	UNICORN Instrument Server.exe	DCOM calls to UNICORN Instrument Server
	ICMPv4	Inbound		Ping, used by UNICORN Clients
139	TCP	Inbound		NetBIOS to enable OPC Client -> OPC communication with UNICORN Instrument Server
445	TCP	Inbound		SMB to enable OPC Client -> OPC communication with UNICORN Instrument Server

Network discovery share must be enabled in firewall to allow computer name resolution. This can be restricted to the following predefined rules found in the Windows firewall:

Windows firewall rule	Direction
FPS-NB_Datagram-In-UDP	Inbound

Windows firewall rule	Direction
FPS-NB_Name-In-UDP	Inbound
FPS-LLMNR-In-UDP	Inbound
FPS-NB_Datagram-Out-UDP	Outbound
FPS-NB_Name-Out-UDP	Outbound
FPS-LLMNR-Out-UDP	Outbound

Note: *Rules related to OPC can be omitted if OPC is not used.*

Firewall settings for UPC3

Inbound traffic from UNICORN Clients, OPC clients, HTTP/WebSocket clients, and Griffin.

Outbound traffic to ÄKTA system, database, and email-server.

Port	Protocol	Direction	Program	Source/Destination
40500-40502	TCP	Inbound	UNICORN Instrument Server.exe	UNICORN Instrument Server
40512	TCP	Outbound	UNICORN Instrument Server.exe	UNICORN Instrument Server -> Real-Time Unit
9920	TCP	Inbound	UNICORN Support Service.exe	UNICORN Instrument Server
40511	TCP	Inbound	RemoteDeploymentService.exe	UNICORN Client -> UNICORN Instrument Server
40513	TCP	Inbound	UNICORN Instrument Server.exe	HTTP/WebSocket client -> UNICORN Instrument Server
40514	TCP	Inbound	UNICORN Instrument Server.exe	HTTP/WebSocket client -> UNICORN Instrument Server

Port	Protocol	Direction	Program	Source/Destination
Any	Any	Outbound	UNICORN Instrument Server.exe	DCOM, UNICORN Clients, Email server, My Instruments etc.
135	TCP	Inbound		DCOM for OPC
Any	Any	Inbound	OPCEnum.exe	DCOM calls to OPCEnum
Any	Any	Outbound	OPCEnum.exe	DCOM calls from OPCEnum
Any	Any	Inbound	UNICORN Instrument Server.exe	DCOM calls to UNICORN Instrument Server
	ICMPv4	Inbound		Ping, used by UNICORN Clients
139	TCP	Inbound		NetBIOS to enable OPC Client -> OPC communication with UNICORN Instrument Server
445	TCP	Inbound		SMB to enable OPC Client -> OPC communication with UNICORN Instrument Server

Network discovery share must be enabled in firewall to allow computer name resolution. This can be restricted to the following predefined rules found in the Windows firewall:

Windows firewall rule	Direction
FPS-NB_Datagram-In-UDP	Inbound
FPS-NB_Name-In-UDP	Inbound
FPS-LLMNR-In-UDP	Inbound
FPS-NB_Datagram-Out-UDP	Outbound
FPS-NB_Name-Out-UDP	Outbound
FPS-LLMNR-Out-UDP	Outbound

Note: *Rules related to OPC can be omitted if OPC is not used.*

Firewall settings for UPC4

Inbound traffic from UNICORN Clients, OPC clients, HTTP/WebSocket clients, and Griffin.

Outbound traffic to Real-Time Unit, database, and email-server.

Port	Protocol	Direction	Program	Source/Destination
40500-40502	TCP	Inbound	UNICORN Instrument Server.exe	UNICORN Instrument Server
60030-60033	TCP	Outbound	p950_drv.exe	UNICORN Instrument Server -> ÄKTA system (CU1)
60130-60133	TCP	Outbound	p950_drv.exe	UNICORN Instrument Server -> ÄKTA system (CU2)
60230-60233	TCP	Outbound	p950_drv.exe	UNICORN Instrument Server -> ÄKTA system (CU3)
60330-60333	TCP	Outbound	p950_drv.exe	UNICORN Instrument Server -> ÄKTA system (CU4)
9920	TCP	Inbound	UNICORN Support Service.exe	UNICORN Instrument Server
40511	TCP	Inbound	RemoteDeploymentService.exe	UNICORN Client -> UNICORN Instrument Server
40513	TCP	Inbound	UNICORN Instrument Server.exe	HTTP/WebSocket client ->UNICORN Instrument Server
40514	TCP	Inbound	UNICORN Instrument Server.exe	HTTP/WebSocket client ->UNICORN Instrument Server
Any	Any	Outbound	UNICORN Instrument Server.exe	DCOM, UNICORN Clients, Email server, My Instruments etc.
135	TCP	Inbound		DCOM for OPC
Any	Any	Inbound	OPCEnum.exe	DCOM calls to OPCEnum
Any	Any	Outbound	OPCEnum.exe	DCOM calls from OPCEnum

Port	Protocol	Direc-tion	Program	Source/Destination
Any	Any	Inbound	UNICORN Instru-ment Server.exe	DCOM calls to UNICORN In-strument Server
	ICMPv4	Inbound		Ping, used by UNICORN Cli-ents
139	TCP	Inbound		NetBIOS to enable OPC Client -> OPC communication with UNICORN Instrument Server
445	TCP	Inbound		SMB to enable OPC Client -> OPC communication with UNICORN Instrument Server

Network discovery share must be enabled in firewall to allow computer name resolution. This can be restricted to the following predefined rules found in the Windows firewall:

Windows firewall rule	Direction
FPS-NB_Datagram-In-UDP	Inbound
FPS-NB_Name-In-UDP	Inbound
FPS-LLMNR-In-UDP	Inbound
FPS-NB_Datagram-Out-UDP	Outbound
FPS-NB_Name-Out-UDP	Outbound
FPS-LLMNR-Out-UDP	Outbound

Note: *Rules related to OPC can be omitted if OPC is not used.*

Firewall settings for UPC5

Inbound traffic from HTTP/WebSocket clients

Outbound traffic to database, Active Directory (if LDAP is used), email server.

Port	Protocol	Direction	Program	Source/Destination
1433	TCP	Outbound	UNICORNUserServer.exe	UNICORN User Server -> database
1434	UDP	Outbound	UNICORNUserServer.exe	UNICORN User Server -> database
###[1]	Any	Outbound	UNICORNUserServer.exe	UNICORN User Server -> email server
636	TCP	Outbound	UNICORNUserServer.exe	UNICORN User Server -> Active Directory (encrypted)
389	TCP	Outbound	UNICORNUserServer.exe	UNICORN User Server -> Active Directory (no encryption)
443	TCP	Inbound	UNICORNUserServer.exe	HTTP Client-> HTTP communication with UNICORN User Server
40516	TCP	Inbound	UNICORNUserServer.exe	HTTP Client -> HTTP communication with UNICORN User Server

[1] Remote port number depends on customer installation.

Network discovery must be enabled in firewall to allow computer name resolution. This can be restricted to the following predefined rules found in the Windows firewall:

Windows firewall rule	Direction
FPS-NB_Datagram-In-UDP	Inbound
FPS-NB_Name-In-UDP	Inbound
FPS-LLMNR-In-UDP	Inbound
FPS-NB_Datagram-Out-UDP	Outbound
FPS-NB_Name-Out-UDP	Outbound
FPS-LLMNR-Out-UDP	Outbound

Note: *Select one of the rules for LDAP communication with Active Directory, either encrypted or non-encrypted depending on how UNICORN is configured.*

Firewall settings for UPC6

Outbound traffic from HTTP/WebSocket clients

Outbound traffic to UNICORN Instrument Server and UNICORN User Server

Port	Proto-col	Direction	Program	Source/Destination
443	TCP	Outbound	HTTP Client	HTTP Client -> UNICORN User Server
40513	TCP	Outbound	WebSocket Client	WebSocket Client -> UNICORN Instrument Server
40514	TCP	Outbound	HTTP Client	HTTP Client -> UNICORN Instrument Server
40516	TCP	Outbound	HTTP Client	HTTP Client -> UNICORN User Server

Network discovery must be enabled in firewall to allow computer name resolution. This can be restricted to the following predefined rules found in the Windows firewall:

Windows firewall rule	Direction
FPS-NB_Datagram-In-UDP	Inbound
FPS-NB_Name-In-UDP	Inbound
FPS-LLMNR-In-UDP	Inbound
FPS-NB_Datagram-Out-UDP	Outbound
FPS-NB_Name-Out-UDP	Outbound
FPS-LLMNR-Out-UDP	Outbound

Firewall settings for GE Healthcare License Server

Inbound traffic from UNICORN Clients

No outbound traffic initiated by license server.

Port	Proto-col	Direction	Program	Source/Destination
Any	TCP	Inbound	gehealth.exe	UNICORN Client -> GE Healthcare license server
27000–27009	TCP	Inbound	lmgrd.exe	UNICORN Client -> GE Healthcare license server

A UNICORN Client initiates a license request with lmgrd.exe. lmgrd.exe communicates with gehealth.exe and then UNICORN Client sends the request to gehealth.exe on a dynamically assigned port.

Firewall settings for UNICORN Database (SQL Server)

Inbound traffic from UNICORN Clients, OPC HDA, and UNICORN Instrument Servers.

No outbound traffic is initiated by SQL Server to UNICORN.

Port	Protocol	Direction	Program	Source/Destination
1433	TCP	Inbound		SQL Server
1434	UDP	Inbound		SQL Server Browser
Any	Any	Outbound	Sqlservr.exe	SQL Server outbound

Note: *These corresponds to the Windows firewall rules created by the SQL Server installation program.*

Optional - Computers using UNICORN Service Tool

UNICORN Service Tool is usually used locally on a computer to service the installation in terms of adjusting configuration files, checking running processes, and versions. There is also some functionality for connectivity tests. The following rules are required on UPC1, UPC2, UPC3, and UPC4 to be able test a database connection using UNICORN Service Tool.

Port	Protocol	Direction	Program	Source/Destination
1433	TCP	Outbound	UNICORNSrv-Tool.exe	UNICORN Service Tool -> database
1434	UDP	Outbound	UNICORNSrv-Tool.exe	UNICORN Service Tool -> database

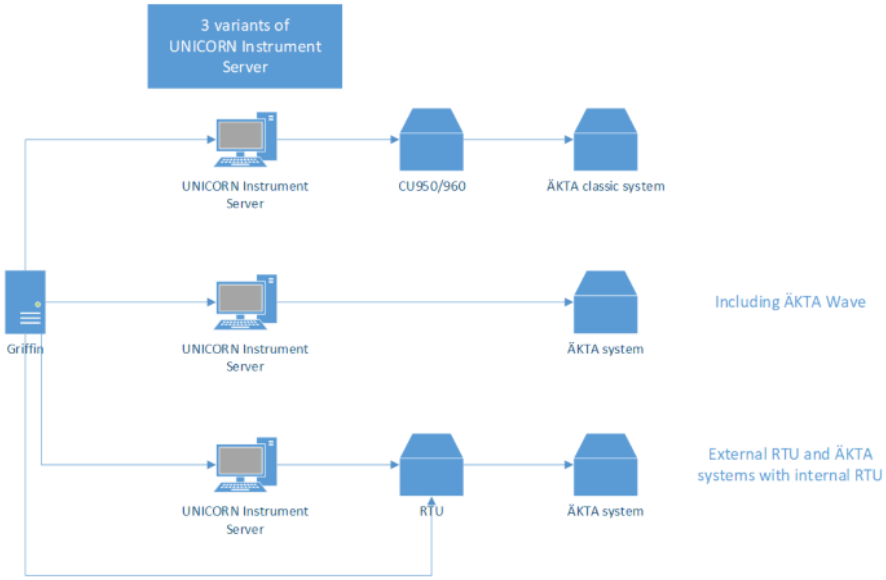
Additional rules can be required if UNICORN Service Tool is used for port checking since many firewall rules may have been restricted to specific applications.

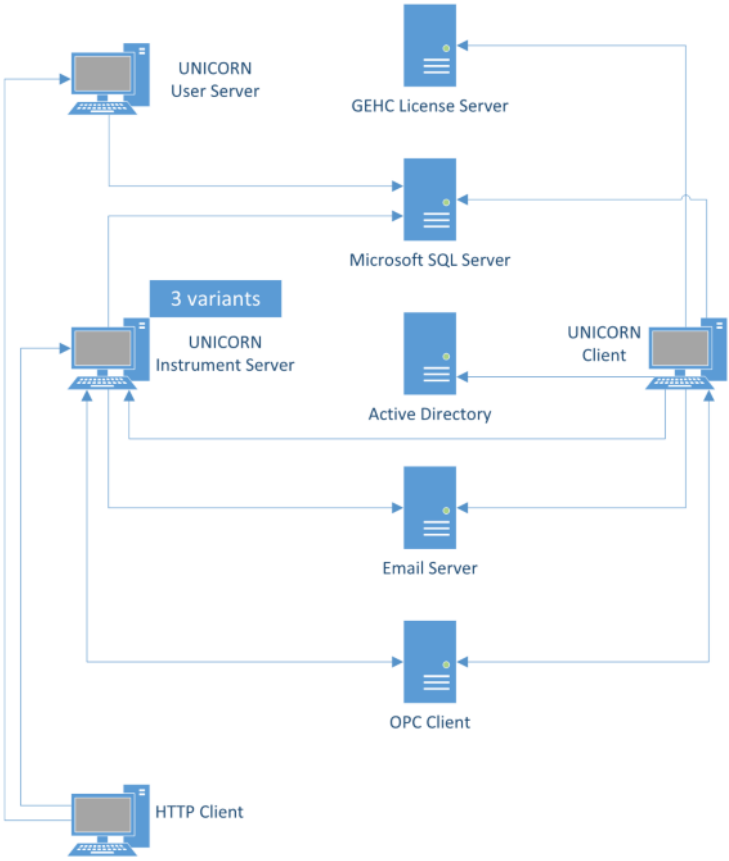
Rules for Real-Time Unit

For firewall settings of the Real-Time Unit, see the *Real-Time Unit Privacy and Security Manual*.

UNICORN network overview

The following is a schematic diagram of a full-scale network solution for UNICORN:





- Communication with Microsoft SQL Server is encrypted by default if installed by the UNICORN installation program.
- Communication with Real-Time Unit is encrypted.
- Communication with Active Directory is encrypted by default.
- Parts of the communication from UNICORN Client to UNICORN Instrument Server are encrypted using SSL/TLS.
- OPC Client communication can be encrypted by enabling encryption for DCOM in Windows. Instructions are available in the UNICORN OPC Manual.
- Communication between HTTP client and UNICORN Instrument and User Server is encrypted using SSL/TLS.
- Other communication is not encrypted.

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 UNICORN.

Apply the appropriate company policies when accessing UNICORN via a wireless connection. For example, use WPA2 or WPA3 for network transmission encryption and mutually authenticated TLS for transport control security. MAC address filtering is something that can be considered for enhancing security as well as limited transmission power range and no SSID broadcasting.

4.3 Removable media security

UNICORN 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(s) hosting UNICORN.

4.4 Data at rest security

UNICORN stores data in a persistent storage, this includes methods, results, log files, system, and user data. The persistent storage consists of one or more Microsoft SQL Server Express Edition. The access to the storage is protected by encryption, however the actual database in the standard installation is not encrypted.

When Microsoft SQL Server Express Edition is installed by the UNICORN installation program, the system administrator (sa) password is set to an internal static password. This password is obfuscated using string encryption. For increased SQL Server security it is recommended to do an enterprise installation as described in the UNICORN Database Installation Guide.

UNICORN uses AES to encrypt sensitive information in application configuration files, e.g. account names and passwords used to connect to the UNICORN database.

4.5 Data integrity capabilities

UNICORN contains capabilities to make sure that the installation is not inappropriately modified accidentally or maliciously. Integrity checks can be performed using the UNICORN ***Administration*** module by invoking the ***Perform Integrity Check*** functionality. Any issues found during the check are reported to the user that can use this information as a base for an appropriate action.

4.6 De-identification capabilities

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

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

No Privacy Information (PI) is collected by UNICORN apart from the user id performing actions in the system.

Note: *The user id can be used to identify a user and the email address.*

4.7 Business continuity

A disaster recovery of the UNICORN database is done by restoring a database backup. Hence, it is very important to apply an appropriate schedule for the database backups. However, it is recommended that the database backups are stored on a secured media and are made available whenever a restore of the database is required.

4.8 Security controls provided by the cloud provider

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

5 System protection

About this chapter

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

In this chapter

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 GE Healthcare and our customers.

UNICORN 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.

During virus scans, the performance of UNICORN might be affected and therefore it is highly recommended to do the scans when the UNICORN controlled system is not in use. The current organizational policies and procedures regarding AntiVirus software should be applied with the proper network defenses and similar activated.

5.2 Server and/or workstation security

UNICORN 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 UNICORN. This maintenance includes the following:

- Applying operating system patches
- Applying operating system upgrades
- Applying operating system configuration changes
- Applying operating system routine maintenance
- Applying UNICORN patches
- Applying UNICORN upgrades
- Applying UNICORN configuration changes
- Applying UNICORN 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, on page 34*.

It is important to be aware that UNICORN is a soft real-time system. This means that there are requirements for response time, though not as strict as requirements for hard real-time systems. Other software running on the system control PC can cause delay in response time and in worst case interrupt the run on the system.

It is important to apply necessary security updates to keep the computer secure. However, all security software and computer management software must be configured so that they do not interfere when the system is 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 the system is in use. This includes Windows update and end point protection software. It is known that some endpoint security software suspend 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 UNICORN can be done via the appointed GE Healthcare Key Account Manager.

- A security enhancement is requested in UNICORN.

- A security incident has occurred related to the usage of UNICORN.
- A general question about the existence of security related patches for UNICORN.
- A general question about the availability of online material such as documentation and similar.

6 Remote service

Remote service possibility is not implemented for UNICORN.

7 Personal information collected by the product

No PI is collected by UNICORN apart from the user id performing actions in the system. The user id and email address can be used to identify a user. The audit trail log, methods, results, and so forth includes the user id, hence it is possible to identify who the originating user is. UNICORN has free text input fields that can be considered PI depending on what is entered by the user. The most prominent free text input fields are method, start, run, and evaluation notes. There are other input fields, for example, method and result names, that could be used to enter PI.

UNICORN does not send back any data to GE Healthcare. UNICORN can create error reports where PI may exist, but UNICORN does not send it back to GE Healthcare. This is a manual process that must be explicitly performed by the user.

8 Security updates

UNICORN 7.5 contains a security update to address the following vulnerabilities:

- CVE-2018-20031
- CVE-2018-20032
- CVE-2018-20033
- CVE-2018-20034
- CVE-2016-10395
- CVE-2015-8277

These are related to a vulnerable third party component that is used in the license server.

GE Healthcare Bio-Sciences AB
Björkgatan 30, 751 84 Uppsala Sweden

www.gelifesciences.com/unicorn

29465418 AA V:2 12/2019