cytiva

UNICORN 5.31

Privacy and Security Manual

cytiva.com

Table of Contents

1 Introduction

About this manual

This manual describes the privacy and security considerations for UNICORN™ 5.31.

Purpose of this manual

The purpose of this manual is to describe the expected intended use of UNICORN 5.31, the available privacy and security capabilities of this product, and how these capabilities are configured and used.

Introduction to privacy and security

This manual assumes that the reader understands the concepts of privacy and security. Privacy is the property of protecting the personal private interests of users. Security protects both system and information from risks to confidentiality, integrity, and availability. Security protects privacy but also protects widely against these risks. Privacy requires security. One must balance privacy, security, and safety. Most of the time there is no conflict between these three domains of risk. The organization is encouraged to use risk management procedures to assess and prioritize privacy, security, and safety risks. Using risk management, one can determine how to best leverage the capabilities provided in UNICORN 5.31.

Important user information

UNICORN 5.31 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.cytivalifesciences.com/contact*.

2 Privacy and security environment

The Cytiva UNICORN 5.31 has been designed for an intended use with the following expectations of privacy and security protections included in the environment where this product can be used:

The assumption for UNICORN 5.31 related to Privacy and Security elements is as follows:

- It is recommended that the computer hosting UNICORN 5.31 resides in a controlled environment.
- All users of UNICORN 5.31 use their own unique identity.
- ***Windows® 10 Operating System should be installed on the computer hosting UNICORN 5.31***.

Note: *Parts of the internal communication in UNICORN 5.31 use unencrypted protocols.*

3 Privacy and security capabilities

About this chapter

The Cytiva UNICORN 5.31 includes a range of capabilities to enable privacy and security. This section describes the capability and use of these privacy and security capabilities.

In this chapter

3.1 Access controls

The access control features of UNICORN 5.31 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 5.31 ***Administration*** module by invoking the ***User Setup*** dialog box. The dialog box contains fields for user name, a full name, and a job title. 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 5.31 . 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 and numbers with a minimum size and it can also have an expiration time. This is defined in the Password Policy in UNICORN 5.31 ***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 5.31 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 and can be manually deleted.*

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 5.31 is undertaken by comparing the password with the corresponding password stored in a persistent storage.
- There is a default account for UNICORN 5.31 with a default password that has unrestricted access to all UNICORN 5.31 functions. 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 5.31. 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 5.31 ***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 5.31 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

The audit log resides in the log files under the UNICORN 5.31 installation folder. It contains information about granted access for users and 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 UNICORN 5.31.

Defense in depth

Security operations are best implemented as part of an overall *defense in depth* information assurance strategy that 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 will allow the system to be compromised.

Network security

Cytiva 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 5.31.

The following terminologies are used in this section:

Terminology	Description
UNICORN 5.31	A software consisting of the ***Administration, Method Editor, Evaluation***, and ***System Control*** modules.
UNICORN 5.31 Server	A collection of processes that controls an ÄKTA system or some other system that is supported by UNICORN 5.31. For some deployments, the UNICORN 5.31 Instrument Server processes are divided in different hardware, for example, the UNICORN 5.31 control PC and the Control Unit.
OPC (OLE for Process Control)	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 (Historical Data Access)	A historian according to the industry standard for OPC.
OPC Client	Any software that implements the client part of the OPC specification.

UNICORN 5.31 can be deployed in many ways but a fully networked solution consists of several parts. There are also 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 5.31 there can be OPC clients. This section only describes the network environment for UNICORN 5.31.

Note: *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 (exception for the UNICORN installation folder). If a simpler installation is used then some of the communication will only take place on the 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
OPC	OPC client
ÄKTA system	ÄKTA system
ÄKTA classic system	ÄKTA classic system (CU950/960 based)

Common communication scenarios:

Description	
Control an ÄKTA system with UNICORN 5.31	UPC1 -> ÄKTA classic system
Connecting OPC client to OPC HDA server	OPC -> UPC1

Note:
- *Processes must be allowed to communicate on local machines.*

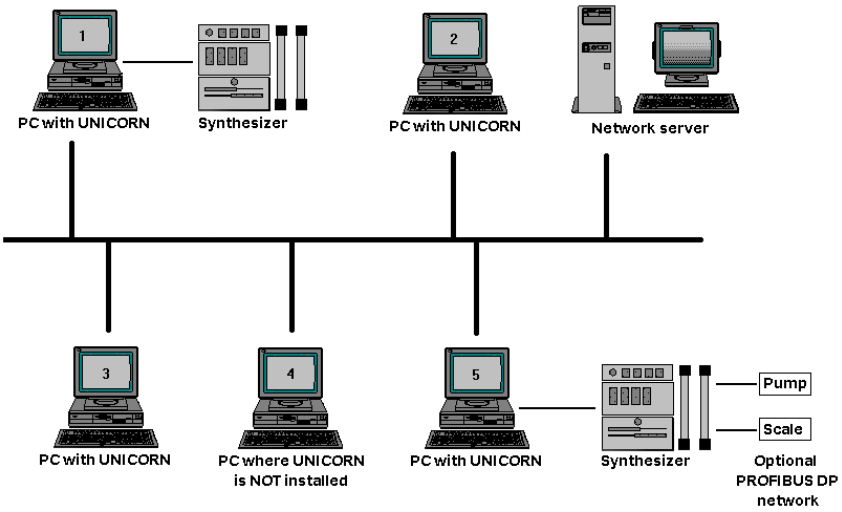
Firewall settings for UPC1

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

Outbound traffic from UNICORN 5.31.

Port	Protocol	Direction	Program	Source/Destination
139	TCP	Inbound	UNICORN	UNICORN 5.31
Any	Any	Inbound	UNICORN OCI	OCI
Any	Any	Inbound	UNICORN P950_drv	P950_drv
Any	Any	Inbound	UNICORN Clstorage	Clstorage

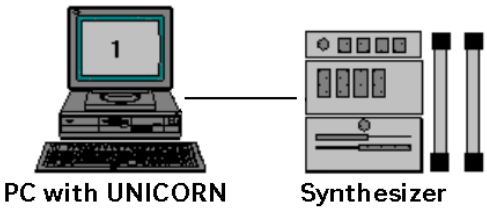
Schematic diagram of UNICORN 5.31 network installation



Key to the network illustration:

- PCs 1 and 5 are local stations: they have UNICORN installed and are directly connected to synthesizers. To have a synthesizer accessible remotely, the local station must be switched on and logged on to the network.
- PCs 2 and 3 are remote stations: they have UNICORN installed but are not directly connected to synthesizers. Via the network, the remote stations can control the synthesizers that are connected to the local stations.
- PC 4 does not have UNICORN installed and therefore cannot control any synthesizers although it is connected to the network.
- The network server does not have UNICORN installed and is not involved in the synthesizer control process as such.
- UNICORN 5.31 does not provide encryption over Profibus. If connected, the user should prevent access to the PROFIBUS DP network.

UNICORN 5.31 standalone installation



The network options settings are ignored for a stand-alone installation. If you perform a stand-alone installation and later want to connect the system to a network, uninstall the software and reinstall with the appropriate settings.

Wireless security

Due to the broadcast nature of wireless communication, wireless devices require special security consideration. There are effective techniques and tools for improving the security of wireless communication devices.

Apply the appropriate company policies when accessing UNICORN 5.31 via a wireless connection.

Removable media security

UNICORN 5.31 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 5.31 .

Data at rest security

UNICORN 5.31 stores data in a persistent storage, this includes methods, results, log files, system, and user data.

Data integrity capabilities

UNICORN 5.31 does not contain capabilities to make sure that data are not inappropriately modified accidentally or maliciously.

De-identification capabilities

UNICORN 5.31 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 5.31 apart from the user id performing actions in the system.

Note: *The user id can possibly be used to identify a user.*

Business continuity

A data recovery of UNICORN 5.31 is performed by creating regular backups of methods, results, and logs. In case of network installation, result files from an ongoing run can be saved automatically at preset intervals to minimize data loss if the system fails. The results are saved locally if the network communication fails and after the communication is restored the data is stored at appropriate locations.

Security controls provided by the cloud provider

UNICORN 5.31 is not deployed on the cloud.

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 Malicious software protection

The computing environment is increasingly hostile, and threats continue to grow from malicious software, including computer viruses, worms, Trojan horses, denial of service attacks, and other malware. Vigilant defense on many levels is required to keep systems free from compromise by malicious software.

UNICORN 5.31 can 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 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 workstation security

UNICORN 5.31 is deployed in a customer controlled environment, hence the customer is responsible for local operational security.

5.3 System (Product) change management

The customer is responsible for maintaining the computer hosting UNICORN 5.31. 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 5.31 configuration changes
- Applying UNICORN 5.31 routine maintenance

Furthermore, any malware protection software installed must also be maintained by the customer. This maintenance includes management of patches, upgrades, configuration changes, and routine maintenance.

Questions or incident reports regarding cyber security related to UNICORN 5.31 can be performed via the appointed Cytiva Key Account Manager. The appointed Cytiva personnel will take care of the customer case and forward it to the organization within Cytiva responsible for UNICORN 5.31. The case can be of one or more of the following categories:

- A security enhancement is requested in UNICORN 5.31.
- A security incident has occurred related to the usage of UNICORN 5.31.
- A general question about the existence of security related patches for UNICORN 5.31.
- A general question about the availability of online material such as documentation and similar.

6 Remote service

UNICORN 5.31 does not provide support for remote service.

7 Personal information collected by the product

No PI is collected by UNICORN 5.31 apart from the user id performing actions in the system. The user id 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 5.31 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.

8 Additional privacy and security considerations

UNICORN 5.31 has not been designed with recent privacy and security standards. The privacy and security residual risks must be mitigated once UNICORN 5.31 is integrated into the work environment and should be imported into the risk assessment of the deployment of UNICORN 5.31 for proper mitigation.

Page intentionally left blank

cytiva

cytiva.com/unicorn

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

29329084 AB V:3 10/2020