cytiva

ÄKTAprocess

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 7

4 Information protection 8

5 System protection 10

6 Remote access 12

7 Personal information collected by the product 13

8 Additional privacy and security considerations 14

1 Introduction

About this manual

This manual describes the privacy and security considerations of the use of the ÄKTAprocess™ system.

Purpose of this manual

This manual describes the privacy and security capabilities of the system, related configuration and use. The intended use of the product is described in *ÄKTAprocess Operating Instructions*.

Scope of this manual

This manual is valid for all variants of standard ÄKTAprocess.

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.

Important user information about intended use of the product

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

ÄKTAprocess requires UNICORN™ control software to operate. Related privacy and security information can be found in the *UNICORN Privacy and Security Manual*.

Contact information

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

2 Privacy and security environment

Privacy and security in the environment

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

- It is strongly recommended that ÄKTAprocess resides in a controlled IT environment.
- The ÄKTAprocess built-in computer is initially configured using a regular user account with auto-logon and therefore opens with user rights to anyone with physical access to the system. The user configuration is the responsibility of the customer.
- All users of UNICORN use their own unique identity (refer to the *UNICORN Privacy and Security Manual*).

3 Privacy and security capabilities

About this chapter

The ÄKTAprocess system and the control software include a broad assortment of capabilities to enable privacy and security. This chapter describes the capability and use of these privacy and security capabilities.

3.1 Access controls

Introduction

The access control on ÄKTAprocess 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.

ÄKTAprocess itself has no identity provisioning apart from the account configuration functionality provided by the Microsoft® Windows® Operating System. UNICORN is used to provide and administrate user accounts. Refer to the *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

User authentication

The user authentication step verifies that the user attempting to access the system is indeed the user associated with the specific account. This section describes the administration of the authentication system.

ÄKTAprocess itself has no user authentication apart from the account configuration provided by the Windows operating system. The access control features of UNICORN include a user authentication system to control access to functionality in the control software. Refer to *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

Assigning access rights

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

ÄKTAprocess itself has no capability of assigning access rights apart from the functionality provided by the Windows operating system. System access can be granted to users in UNICORN, refer to the *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

Patient privacy consent management

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

3.2 Privacy and security audit logging and accountability controls

Introduction

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

No auditing is performed in ÄKTAprocess apart from audit trail functionality provided by the Windows operating system. UNICORN provides audit trail functionality, refer to the *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

4 Information protection

About this chapter

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

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.

Network security

Cytiva strongly recommends that ÄKTAprocess is operated in a network environment that is separated from the general purpose computer network of the owner's organization. There are many effective techniques for isolating ÄKTAprocess 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 ÄKTAprocess.

ÄKTAprocess is operated in a process environment which makes it hard to keep it continuously updated with the latest security fixes and updates. Caution is advised on updating the operating system when the system is running. It is strongly recommended that ÄKTAprocess is operated in a separated protected network environment.

ÄKTAprocess does not provide encryption over PROFIBUS™ DP.

For network and firewall configuration, refer to *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

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 ÄKTAprocess.

ÄKTAprocess does not use wireless communication and is therefore not affected by wireless security. For wireless access to UNICORN, refer to *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

Removable media security

ÄKTAprocess does not require any removable media to operate. UNICORN may produce output that may be desirable to copy to a removable media. However, it is strongly recommended that the company policies related to removable media are applied.

Data at rest security

ÄKTAprocess itself does not store any user or process data. UNICORN is installed on ÄKTAprocess Windows computer and stores data in a persistent storage. UNICORN installs firmware on ÄKTAprocess Control Unit (CU960). ÄKTAprocess Windows operating system disk is not encrypted. For further information, refer to *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

Data integrity capabilities

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

Integrity checks can be performed using UNICORN. For further information, refer to *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

De-identification capabilities

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

No Privacy information (PI) is collected by ÄKTAprocess or UNICORN apart from the user ID performing actions in the system.

Business continuity

Contact Cytiva to retrieve a disaster recovery of the ÄKTAprocess original computer system image.

For UNICORN, refer to *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

Security controls provided by the cloud provider

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

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.

ÄKTAprocess contains a built-in industrial computer with Microsoft Windows operating system. It is recommended to use relevant end-point security and hardening to protect the ÄKTAprocess computer, to serve as an extra protection layer.

Keep the Windows operating system updated with the latest Windows updates and security intelligence updates (for Microsoft Windows Defender). It is recommended to create a recovery point before applying the latest cumulative patch to Windows.

It is strongly recommended not to apply any Windows updates or security fixes during system operation since this will potentially break running processes.

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.

Refer to the *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess for details on system and network security.

Server and/or workstation security

ÄKTAprocess contains additional features to improve local operational security.

ÄKTAprocess contains a built-in computer running Microsoft Windows. ÄKTAprocess is operating in a customer controlled environment, hence the customer is responsible for local operational security.

System change management

The customer is responsible for maintaining the ÄKTAprocess Windows 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.

Any installed malware protection software must be maintained by the customer. This maintenance includes management of patches, upgrades, configuration change, and routine maintenance. Malware protection may impact the performance of the UNICORN software. For more information refer to section "Malicious Software Protection" in the *UNICORN Privacy and Security Manual*.

ÄKTAprocess is serviced by Cytiva. Questions or incident reports regarding cyber security related to ÄKTAprocess can be done via the appointed Cytiva Key Account Manager. Contact Cytiva in case of the following issues:

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

6 Remote access

Introduction

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

ÄKTAprocess is not initially set up with remote access. The system can be set up to enable remote access and control of the system from an external UNICORN client. For more details, refer to *UNICORN Privacy and Security Manual* for the UNICORN version used with ÄKTAprocess.

7 Personal information collected by the product

Personal information

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

No personal information is collected by ÄKTAprocess apart from the accounts used to authenticate and authorize the user on the system computer. Accounts in Windows can be monitored through the default Windows audit trail, hence it is possible to identify who the originating user is.

UNICORN uses the user ID to authenticate and authorize the user, which leaves an audit trail. Refer to *UNICORN Privacy and Security Manual* for further details.

8 Additional privacy and security considerations

Introduction

ÄKTAprocess has been designed with privacy and security functionality integrated into the core design. However, there exist privacy and security residual risks that must be mitigated once ÄKTAprocess is integrated into the work environment. This section describes some risks that should be imported into the risk assessment of the deployment of the ÄKTAprocess for proper mitigation.

Other security considerations

Privacy and security risks have to be considered when integrating the ÄKTAprocess into the work environment. For functionality regarding security provided by UNICORN, which is the control software used with ÄKTAprocess, see relevant version of *UNICORN Privacy and Security Manual*, available from UNICORN 7.3 and higher.

The operating system is running Windows Enterprise Long Time Servicing Branch / Channel, refer to computer description for exact version. The operating system is not hardened although some security features are configured on delivery (e.g. firewall, update of Windows with the latest updates and security patches). See *UNICORN Privacy and Security Manual* for further details.

Regarding Account Configurations, the ÄKTAprocess with Windows LTSC 2019 and later versions are pre-configured with a regular User Account set to auto-logon and an administrator account that forces the user to set password on first logon.

Older versions of ÄKTAprocess running Windows LTSB 2016 are initially configured with a single administrator account set to auto-logon.

The user is responsible for the configuration and maintenance of User Accounts on the ÄKTAprocess Windows computer.

Page intentionally left blank

cytiva.com

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

29655016 AA V:4 12/2020