ReadyToProcess WAVE™ 25 and Xuri™ Cell Expansion System W25 EPC

Privacy and Security Documentation

Original instructions

Table of Contents

1 Introduction 3

2 Privacy and security environment 5

3 Privacy and security capabilities 6

3.1 Access controls 7
3.2 Privacy and security audit logging and accountability controls 9

4 Information protection 10

5 System protection 13

5.1 Malicious software protection 14
5.2 Server and/or workstation security 15
5.3 System (product) change management 17

1 Introduction

About this manual

This manual describes the privacy and security considerations for the Embedded Personal Computer (EPC).

Purpose of this manual

The purpose of this manual is to describe the intended use of the EPC, the available privacy and security capabilities, and how they are configured and used.

Scope of this manual

This *Privacy and Security Manual* covers the EPC in the ReadyToProcess WAVE™ 25 and the Xuri™ Cell Expansion System W25.

Important user information

The EPC is not a medical device.

Introduction to privacy and security

This manual assumes that the reader understands the concepts of privacy and security:

- Privacy is the protection of personal and private interests of users.
- Security protects both system and information from breaches of confidentiality, integrity, and availability.

Security protects privacy but also protects more broadly 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. Through the use of risk management, one can determine how to best leverage the capabilities provided in UNICORN™.

2 Privacy and security environment

Intended use of the EPC

The EPC has been designed for use in an environment with the following expectations of privacy and security protections:

- It is recommended that the EPC is placed in a controlled environment.
- Any communication with software running on the EPC must use encrypted protocols. The only exception is communication from Griffin, a software used by GE service personnel.

3 Privacy and security capabilities

About this chapter

The EPC incorporates 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 features of the EPC can be used to help control access to sensitive information by the user. Access control includes secure connection to the EPC.

Overview of the EPC

The EPC is a computer with a locked down Windows® Embedded Standard 7, running two components of UNICORN. These are the Remote Deployment Service (RDS) and the UNICORN instrument server processes. RDS is preinstalled and the instrument server processes is deployed by UNICORN.

Identity provisioning

User accounts are unnecessary since the users do not directly interact with the EPC. UNICORN provides account creation, maintenance, and suspension of the account when it is no longer needed. A user account is created for the use by a specific individual. This user account is associated with access rights, and is recorded in security audit logging. Access rights include system access that indirectly controls the possibility to use the EPC.

User authentication

The user authentication step verifies that the user is associated with the account. This section covers the administration of the authentication system.

User accounts are created by adding users to the configuration files for UNICORN. The accounts and passwords are internal for UNICORN and are not associated with any real user. The deployment is initiated by the UNICORN instrument server. The account information is encrypted and obfuscated in the UNICORN instrument server and the UNICORN service tool.

Assigning access rights

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

There is only one level of access rights for UNICORN running on the EPC and that is to allow connection to services.

Patient privacy consent management

Patient privacy consent management is the process of supporting the patient's needs for privacy. This is distinct from other forms of consent such as the consent to treat.

The EPC is not a medical device and no patient data is managed by the product.

3.2 Privacy and security audit logging and accountability controls

Introduction

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

Audit logging and accountability controls

No auditing is performed since the communication with the EPC does not involve user interaction directly except for GE service personnel. All other log files are related to debugging and error handling. These log files are included when generating UNICORN error reports.

4 Information protection

About this chapter

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

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 compromise the system.

Network security

GE strongly recommends that UNICORN and ReadyToProcess WAVE 25/Xuri Cell Expansion System W25 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 networking profile outlines the required network services for the EPC.

Networking profile

The EPC is part of ReadyToProcess WAVE 25/Xuri Cell Expansion System W25 and comes as a separate board. An EPC is a separate hardware in the system between the computer with the UNICORN client and the ICU (Instrument Control Unit) system.

UNICORN deploys necessary software to control the ReadyToProcess WAVE 25 and the Xuri Cell Expansion System W25. The software may differ depending on UNICORN version. The UNICORN instrument server is deployed at the time of installation of UNICORN.

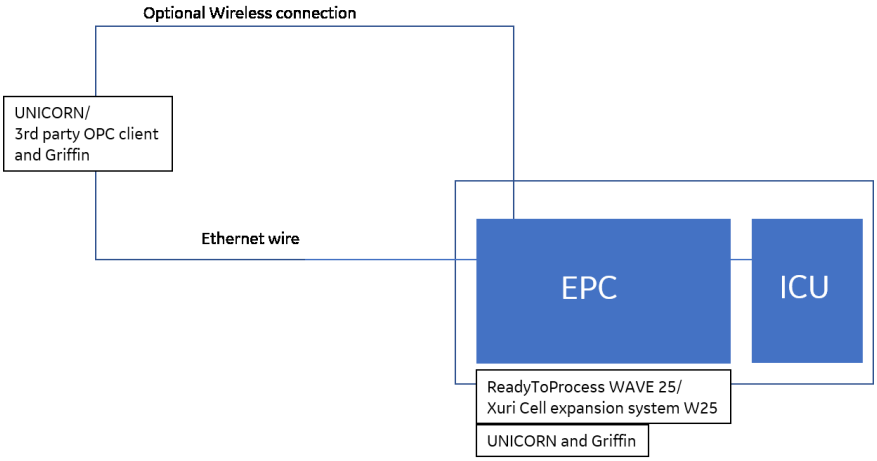
Firewall

The Windows firewall is enabled in the EPC and is set to block all incoming and outgoing traffic by default. For information about UNICORN related security and firewall settings, see *Privacy and Security Manual - UNICORN* and *Privacy and Security Manual - Griffin*.

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

Remote desktop connection using RDP is enabled using predefined rules in the Windows firewall.

Illustration of a typical network



All communication to the RDS and EPC is encrypted using SSL/TLS.

Communication from Griffin is not encrypted.

Wireless security

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

The EPC does not include wireless connection. Contact GE Service personnel for information about installation of optional wireless connection.

Removable media security

The EPC does not require any removable media to operate.

Data at rest security

The EPC does not store data in a persistent storage except for log files and temporary data during a run in progress on ReadyToProcess WAVE 25/Xuri Cell Expansion System W25. Log files do not contain any personal information or any passwords.

Data integrity capabilities

UNICORN has capabilities that prevent the accidental or malicious modification of data. Integrity checks can be performed using the UNICORN Administration module by invoking the ***Perform Integrity Check*** functionality for the specific system. Any anomalies found during the check will be reported to the user that may use this information as a base for appropriate action.

De-identification capabilities

EPC contains no de-identification (anonymization and use of pseudonyms) capabilities to limit privacy and security risks to sensitive information. No privacy information is collected by the EPC.

Business continuity

The EPC is serviced by GE service personnel.

Security controls provided by the cloud provider

The EPC is not deployed in a cloud.

5 System protection

About this chapter

The system is configured and maintained in a way that continuously protects privacy and security. The normal case, is to install the EPC behind a customer controlled PC where the EPC has no direct network access.

In this chapter

Section	See page
5.1 Malicious software protection	14
5.2 Server and/or workstation security	15
5.3 System (product) change management	17

5.1 Malicious software protection

Intrtoduction

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. In most cases, effective protection requires cooperation and partnership between GE and our customers.

Windows firewall

Windows firewall comes as a part of Windows Embedded Standard 7 and protects the EPC against malware, viruses, spyware, and other potentially unwanted programs. Signatures are not updated automatically since the EPC has no direct network access. This also prevents the interruption of ongoing runs on ReadyToProcess WAVE 25/Xuri Cell Expansion System W25 by automatic updates.

There are exclusions to some GE specific paths to avoid performance degradation by excessive scanning of runtime backup data and log files.

5.2 Server and/or workstation security

Introduction

The EPC is deployed in a customer controlled environment. The EPC itself is a Windows Embedded Standard 7 installation that has been locked down to prevent any unauthorized applications to run on the system.

Security baseline

A security baseline has been applied on the Windows installation. The security baseline is a collection of settings that have a security impact. This includes Microsoft® recommended values for configuring those settings, along with guidance on the security impact of those settings. These settings are based on feedback from Microsoft's security engineering teams, product groups, partners, and customers.

The security base package (Windows Embedded Standard 7) contains low-level security features that are needed across other security packages such as Credentials and Certificate Management, Credential Roaming Service, and Windows Authorization Manager.

It includes features such as Access Control List (ACL) Editor, Active Directory Domain services APIs, Windows Cryptographic Primitives Library, licenses, and run-time APIs.

Applocker

To install any application in the EPC in the ReadyToProcess WAVE 25, authentication is required. Applocker does not allow the third party application to be installed until the proper credentials are provided.

Applocker is configured to only allow software digitally signed by GE Healthcare Life Sciences or Microsoft to execute. Executing any other program or loading a third party dll-file requires an explicit exception and that exception must be digitally signed by GE Healthcare Life Sciences.

Windows firewall

Windows firewall is configured to block inbound and outbound traffic. All necessary traffic must be allowed using specific firewall rules. Windows firewall is used to avoid third party firewall software that may disconnect network adapters during updates. See *Network security, on page 10* for details about firewall settings.

This package includes functionality that provides network firewall support for other networking functionality of Windows Embedded Standard 7 in the EPC.

PowerShell scripts

PowerShell scripts can only be executed in PowerShell Constrained Language Mode.

Remote desktop and remote service

Since the EPC has no input devices, remote desktop has been enabled. The software used on the EPC, such as the RDS and UNICORN, has been designed to make explicit logon to the system unnecessary, and therefore the GE Service Person and/or the customer has no access to the remote desktop.

UNICORN does not provide support for remote service.

5.3 System (product) change management

The EPC is serviced by GE service personnel.

Questions or incident reports regarding security related to UNICORN shall be directed to the appointed GE key account manager or the GE service personnel. The appointed GE person takes care of the customer case and forwards it to GE. The case can be of one or several of the following categories:

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

For local office contact information, visit
www.gelifesciences.com/contact

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

www.gelifesciences.com/

GE Healthcare Europe GmbH
Munzinger Strasse 5, D-79111 Freiburg, Germany

GE Healthcare UK Limited
Amersham Place, Little Chalfont, Buckinghamshire, HP7 9NA, UK

GE Healthcare Bio-Sciences Corp.
100 Results Way, Marlborough, MA 01752, USA

GE Healthcare Japan Corporation
Sanken Bldg. 3-25-1, Hyakunincho Shinjuku-ku, Tokyo 169-0073, Japan

29323733 AA 05/2018 a924