cytiva

Biacore™ X100

Privacy and Security Manual

cytiva.com

Table of Contents

1 Introduction

About this manual

This manual describes the privacy and security considerations of the use of the Biacore™ X100 Control Software and Biacore X100 Evaluation Software, which are dependent on the Biacore X100 database. The two applications and the database are collectively referred to as Biacore X100 Software in this document.

Purpose of this manual

This manual describes the expected intended use of Biacore X100 Software, the privacy and security capabilities included, and how these capabilities are configured.

Scope of this manual

This document is valid for Biacore X100 Control Software, and Biacore X100 Evaluation Software versions 2.1 and higher, and for the Biacore X100 database versions 2.1 and higher.

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.

Product description

Neither Biacore X100 Software nor the Biacore X100 instrument are medical devices, and shall not be used in any clinical procedures or for diagnostic purposes.

Biacore X100 is a system for real-time label-free analysis of molecular interactions.

The system consists of a Biacore X100 instrument, as well as Biacore X100 Software. Biacore X100 Software, including the Biacore X100 database, is installed on the same computer. One additional installation of the Biacore X100 Evaluation Software is allowed on a second computer that connects to the database on the first computer.

Safety notices

This user documentation contains safety notices concerning the safe use of the product. See the definition below.

NOTICE

NOTICE indicates instructions that must be followed to avoid damage to the product or other equipment.

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

Biacore X100 Software has been designed for an intended use with the following expectations of privacy and security protection, that should be included in the environment where Biacore X100 Software will be used:

- Biacore X100 Software is designed to reside on computers that are members of Microsoft Active Directory in the customer network, or local Windows accounts.
- Access to Biacore X100 Software is gained through membership in one of the Biacore X100 database roles connected to the Biacore X100 Windows user groups.
- Biacore X100 Software users shall not have Windows administrator privileges, as this enables the user to bypass security configurations. An exception to this rule is for the user(s) changing the backup settings in Biacore X100 Backup & Restore, which requires Windows administrator privileges.

3 Authentication, authorization and audit logging

About this chapter

Biacore X100 Software includes a broad assortment of capabilities to enable privacy and security. This chapter describes the ability and use of these privacy and security capabilities.

In this chapter

3.1 Access controls

Introduction

The access control on Biacore X100 Software is used to help control access to customer information on the system. Access control includes user account creation, assigning the users to the Windows user groups predefined for the Biacore X100 database access, and other features, such as removing Windows administrator privileges for the standard Biacore X100 users.

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.

For Biacore X100 Software, the provisioning of users is performed through Active Directory for domain accounts, and through Windows for local accounts. Use of Active Directory is recommended as it provides higher security. Active Directory and Windows provide event logs. Monitoring of these event logs is recommended to detect any computer security breaches early.

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.

- When starting Biacore X100 Software, the user must log in to the application with the username and password for an Active Directory or Windows user account.
- Only user accounts that are members of one of the Biacore X100 user groups can log in to the applications. For information about Biacore X100 user groups, refer to *Biacore X100 Software v2.1 Installation Instructions, 29288193*.
- Biacore X100 Software application is run with the credentials of the user that logged in to Biacore X100 Software.
- The database connection string does not contain any username or password. Instead, the database access is based on the Biacore X100 user groups.

Assigning access rights

Assigning access rights is the administrative process for connecting permissions with user accounts. This is performed by a user with administrator rights on the computer where the database is installed, who can assign users to different Biacore X100 roles by adding them to the Biacore X100 user groups in Windows.

Windows users or Active Directory users who are not members of any of the Biacore X100 user groups do not have access to the Biacore X100 database.

3.2 Audit logging and accountability controls

Introduction

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

Biacore X100 audit logs

Biacore X100 Software has no built-in privacy and security audit logs.

Audit logs can be created using Windows or Active Directory audit functionality as well as using Microsoft SQL Server audit functionality.

The Biacore X100 database is expected to be accessed only from Biacore X100 Software. After enabling relevant logs, make sure to monitor entries indicating access from other applications.

4 Patient privacy content management

Patient privacy

Biacore X100 Software does not handle (create, transfer, or store) patient data, therefore the patient privacy consent is not applicable to Biacore X100 Software.

5 Information protection

About this chapter

This chapter describes privacy and security operations, and contains guidelines for the preparation of a secure environment for Biacore X100 Software.

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 the system to be compromised.

In this chapter

5.1 Network security

System interconnections

Biacore X100 Software has the system interconnections on the network listed below.

The recommended approach to encrypt the network communication is described in the table below.

System connection	Communication
Biacore X100 database	The communication to the database has "in transit" encryption enabled by default. Communication to the database occurs on the network only when a second instance of Biacore X100 Evaluation Software is installed on an another computer. Otherwise communication to the database goes through the local host.
Active directory	The communication to the Active directory uses the LDAP protocol.
File servers	Any file server for file sharing is owned by the customer. Connections to file servers for saving exported files must be encrypted. In a Windows environment, make sure that the SMB3 network protocol is enabled.

Wired network security

Cytiva strongly recommends that Biacore X100 Software is operated in a network environment that is separated from the general purpose computing network of the owner's organization. There are many effective techniques for isolating Biacore X100 Software on a secure sub-network, 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 Biacore X100 Software.

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 Biacore X100 Software.

Apply the appropriate company policies when accessing the Biacore X100 database via a wireless connection.

Removable media security

Biacore X100 Software 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 Biacore clients.

Firewall settings for database server

Instructions on how to configure the computer with the Biacore X100 database for remote access are provided in *Biacore X100 Software v2.1 Installation Instructions, 29288193*.

The table below shows default firewall settings for the Biacore X100 database server host for inbound traffic from Biacore clients. No outbound traffic is initiated, but the database server responds to incoming requests.

Note: *If you change the ports in SQL Server, make sure to open the corresponding port in the firewall.*

Port	Protocol	Direction	Network service	Destination
1434	UDP	Inbound	N/A	Microsoft SQL Server Browser
Dynamic	Any	Inbound	Sqlservr.exe	Microsoft SQL Server

5.2 Data storage and encryption

Data at rest security

Biacore X100 Software data at rest storage consists of the Biacore X100 database, which is a Microsoft SQL Server database. The data storage includes methods, results, and system data. The communication to Microsoft SQL Server is protected by encryption, but the Biacore X100 database is not encrypted by default. It is recommended that the database administrator enables encryption at rest on the Microsoft SQL Server databases.

For all exported files, the customer is responsible for establishing appropriate file management procedures. All exported files are accessible using standard tools, except for exported runs, evaluations, and projects, which can only be imported to the Biacore X100 database using Biacore X100 Software.

Data integrity capabilities

Biacore X100 Software has capabilities to make sure that the data is not accidentally or maliciously modified.

Note that the database administrator has full access to the database contents and may perform changes that cannot be detected by Biacore X100 Software. It is therefore important for the data integrity that database administration is covered by well-established routines with data integrity in mind.

De-identification capabilities

Biacore X100 Software is not a medical device and does not handle (create, transfer, or store) patient data. Therefore Biacore X100 Software does not contain de-identification (anonymization and pseudonymization) capabilities.

Business continuity

Backup and disaster recovery routines for the Biacore X100 database is the responsibility of the customer database administrator or other applicable administrator.

The system needs to be configured and maintained in a way that continually protects privacy and security.

Make sure to back up the SQL Server using the provided Biacore X100 backup tool. The backup tool stores the backups locally, so it’s recommended to transfer the backup files to a network drive or similar.

5.3 External connections

Connection to an external computer

See *System interconnections, on page 11* for more information.

Security controls provided by the cloud provider

Biacore X100 Software is not hosted on a third party cloud environment. Cloud security controls are not applicable.

6 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.

This product is designed to be used in an environment where commercial antivirus software is used to detect the presence of malicious software.

Server and workstation security

Biacore X100 Software is deployed in a customer-controlled environment, therefore the customer is responsible for local operational security.

The Biacore X100 database installation program performs the following changes to the computer that might affect the security:

1. The ***Allow Inprocess*** option is enabled for the SQL Server linked server Oracle provider (OraOLEDB.Oracle).
2. The following certificates are added as trusted:
    - **Cytiva**

      Thumbprint: d15a7b19aaa8e0095748278226c8aecbba2721c5

      CN = Cytiva Sweden AB

      OU = Cytiva Sweden AB

      O = Cytiva Sweden AB

      L = Uppsala

      S = Uppsala

      C = SE
    - **Microsoft #1**

      Thumbprint: bc0b6d0d7398035fcfbe8cc1ad8724a23a3a89db

      CN = Microsoft Corporation

      OU = AOC

      O = Microsoft Corporation

      L = Redmond

S = Washington

C = US

- **Microsoft #2**

  Thumbprint: b9eaa034c821c159b05d3521bcf7feb796ebd6ff

  CN = Microsoft Corporation

  OU = MOPR

  O = Microsoft Corporation

  L = Redmond

  S = Washington

  C = US

Patch management practices

Cytiva recommends that the latest updates to the operating system should always be applied.

NOTICE

An operating system update might interrupt the operation. To prevent unexpected equipment operation, the update process should be initiated manually and only performed when the equipment is not in use.

The customer is responsible for maintaining the computer hosting Biacore X100 Software. This maintenance includes at least the following:

- Maintaining Microsoft product updates. For the Biacore X100 database installation, make sure that upgrades to newer versions of Microsoft SQL Server, including cumulative updates, are monitored and installed manually on a regular basis. Regular upgrades make sure that all available security updates are applied. Also, make sure that the option to receive updates for other Microsoft products is enabled when updating Windows. This makes sure that security updates for the currently installed version of Microsoft SQL Server are applied automatically.
- Applying updates to computer firmware and drivers.
- Applying operating system configuration changes.
- Applying operating system routine maintenance.
- Applying Biacore X100 Software upgrades.
- Applying the Biacore X100 database backup and disaster recovery routines.

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 *Protection from malicious attacks, on page 15*.

Questions or incident reports regarding cyber security related to Biacore X100 Software can be done via the appointed Cytiva Key Account Manager or the Cytiva service personnel. Cytiva can aid with the following:

- Security enhancement requests in Biacore X100 Software.
- Security incidents related to the usage of Biacore X100 Software.
- General questions about the availability of online material such as documentation and similar.

7 Remote access

Introduction

Often the most efficient and cost-effective ways for to provide service is to connect to remotely. Every effort is made to make sure that this connection is as secure as possible.

Remote connection

Cytiva provides support for the Biacore instrument by remotely connecting to the customer's computer.

8 Personal information collected by the product

Personal information

No personal information is collected by Biacore X100 Software apart from the name and ID of the user performing actions in the system.

Information stored in the database (such as run and evaluation results) includes the username and ID, which is required for the designed traceability features of Biacore X100 Software.

Biacore X100 Software has text input fields that can be considered personal information depending on what is entered by the user. To avoid unnecessary collection of personal information, establish instructions on how to use the text input fields.

For more information on customer privacy rights and how Cytiva processes personal data, see *Cytiva Privacy Policy*.

9 Additional privacy and security considerations

Additional risks

Biacore X100 Software 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 when Biacore X100 Software is integrated into the work environment. This section describes some risks that should be imported into the risk assessment of the deployment of Biacore X100 Software for proper mitigation.

For full user access control and improved traceability, the following is recommended:

- Make sure that Biacore X100 Software users do not have Windows administrator privileges.
- Enable relevant database logs.
- Configure database encryption according to the latest Microsoft recommendations.
- Monitor the Active Directory event logs to early discover any computer security compromises.

10 Product security supplemental documents

Software Bill of Materials (SBOM)

SBOM, a list of third-party software components used, is available for Biacore X100 Software upon request. Contact the sales representative for a copy of SBOM.

A list of used third-party components is also available in the End-User Licence Agreement, EULA, accessible from the ***About*** dialog in Biacore X100 Software.

Give feedback on this document

Visit cytiva.com/techdocfeedback or scan the QR code.

cytiva.com

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