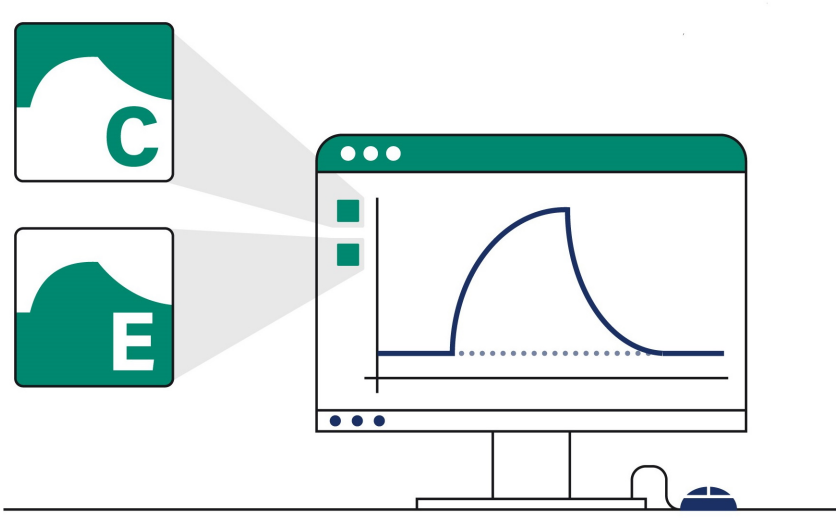
cytiva

Biacore™ Insight software

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™ Insight Control Software and Biacore Insight Evaluation Software, which are dependent on the Biacore Insight Database. The two applications are referred to as Biacore Insight software in this document. Biacore 1K, Biacore 1K+, and Biacore 1S+ are collectively referred to as the Biacore 1 series. Biacore 8K and Biacore 8K+ are collectively referred to as the Biacore 8 series.

This manual also covers the optional Biacore Insight API Server.

Purpose of this manual

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

Scope of this manual

The document is valid for Biacore Insight Control Software, Biacore Insight Evaluation Software , and Biacore Insight API versions 6.0 and higher, and for Biacore Insight Database versions 2.3 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

Biacore 1 series and Biacore 8 series are systems for real-time label-free analysis of molecular interactions.

The systems consist of an instrument from either the Biacore 1 series or the Biacore 8 series, as well as Biacore Insight software. The software can be installed on multiple computers that are connected to a common database server with the Biacore Insight Database installed. Biacore 1 series and Biacore 8 series can share the same database.

Biacore Insight Evaluation Software is also sold separately for analysis to be used together with Biacore T200 and Biacore S200. The run files from these instruments can be imported into Biacore Insight Database.

With the GxP extension, a GxP workflow is supported. Based on three different user roles, the GxP extension manages regulated procedures, regulated runs, and regulated evaluations. For more information, refer to *Biacore Insight GxP User Manual, 29312548*.

Note: *Neither Biacore Insight software nor any of its associated Biacore instruments are medical devices, and shall not be used in any clinical procedures or for diagnostic purposes.*

Biacore Insight API server

The Biacore Insight API enables automated export of run data and evaluated data from the Biacore Insight database. The Biacore Insight API server that hosts the API is an on-premise solution that interconnects to the existing Biacore Insight database, license server, Active Directory and the customer developed API client.

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*.

Abbreviations and definitions

The following terms and abbreviations are used in this manual:

Term/Abbreviation	Definition
DRP	disaster recovery plan

2 Privacy and security in the environment

Biacore Insight 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 Insight software will be used:

- The Biacore Insight software is designed to reside on computers that are members of Microsoft Active Directory in the customer network.
- For network database installations, all users of the Biacore Insight software must be members of Active Directory. For local database installations the application depends on either Active Directory or local Windows accounts. It is recommended to use a central database as this provides higher security, possibility to share data between systems, and larger storage capacity. The local database is intended primarily for service purposes.
- Access to the Biacore Insight software is gained through membership in one of the Biacore Insight Database roles.
- Biacore Insight software users shall not have Windows administrator privileges as this enables the user to bypass security configurations.
- Biacore Insight API Server is running as a Windows Service, which is run by a dedicated user account. This user account has a local user profile folder on the computer where the service is running. The user profile folder shall be protected from unauthorized access, since API access tokens are persisted here.

3 Authentication, authorization and audit logging

About this chapter

Biacore Insight 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.

3.1 Access controls

Introduction

The access control on Biacore Insight software is used to help control access to customer information on the system. Access control includes user account creation, assigning the privileges, and other features, such as assigning privileges to Active Directory users in Biacore Insight Database.

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 Insight 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 early discover any computer security compromises.

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 the Biacore Insight software, the user must log on to the application with the username and password for an Active Directory or Windows user account.
- Make sure that the Password Policy Settings configuration meets the recommended security standards.
- Only members of one of the BiacoreUsers roles in the Biacore Insight Database can log on to the applications. For information about BiacoreUsers roles, refer to *Biacore Insight Database Installation and Management Guide, 29287249*.
- A successful logon to the Biacore Insight software results in the application process being run as the user that logged on. The logon event is also registered in the Action History functionality of the Biacore Insight software when the GxP extension is applied.
- The database connection string does not contain any username or password, database access is based on the Active Directory users access rights to the specified database.

Assigning access rights

Assigning access rights is the administrative process for connecting permissions with user accounts. This is performed by a database administrator or Active Directory administrator who can assign users to different database roles for the Biacore Insight Database.

Active Directory users who are not members of any of the BiacoreUsers database roles do not have read or write access to the database.

Biacore Insight API access control

Biacore Insight API uses role-based access control in the same way as the Biacore Insight software, together with a timed access token that is to be used for authentication in the calls to the data retrieving API-endpoints.

Credentials are a username/password pair that correspond to a user with the ***BiacoreAPIClient*** and/or ***BiacoreAPIServerAdministrator*** database role.

The retrieved access token has different authorization scopes depending on the role(s) of the authenticated user in the database. The access token should be treated as a password or corresponding secret, as it provides access to the data retrieving API-endpoints.

Note: *Make sure that the API publicity is limited by the network accessibility and security level.*

3.2 Audit logging and accountability controls

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

Biacore Insight software has limited built-in privacy and security audit logs. For runs, run methods, evaluations, and evaluation methods the actions create, move, rename, and delete are logged in the Action history. The Action history is available for all users. When the GxP extension is enabled additional events are logged, such as user logon, logout, and actions on regulated items, including regulated procedures. Audit logs can be created using Active Directory audit functionality as well as using Microsoft SQL Server audit functionality.

Biacore Insight Database is expected to be accessed only from Biacore Insight software. After enabling relevant logs, make sure to monitor entries indicating access from other applications.

4 Patient privacy consent management

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

5.1 Network security

Introduction

Cytiva strongly recommends that Biacore Insight 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 Insight 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 Insight software.

System interconnections

The Biacore Insight software has the following system interconnections on the network:

- Biacore Insight Database
- Cytiva Software Licensing Server
- Active directory
- File servers
- Biacore Insight API Server (optional)

It is a recommended approach to encrypt the network communication.

Biacore Insight Database	The communication to the database has "in transit" encryption enabled by default.
Cytiva Software Licensing Server	The communication between the Biacore Insight software and the Cytiva license server is handled by a third party solution from Revenera.
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.
Biacore Insight API Server	The Biacore Insight API Server has the same system interconnections as the Biacore Insight software, and an additional connection to the customer developed API-client. The communication to the API-client uses the HTTP protocol and exposes the Biacore API as an HTTP(S) REST JSON API. The API uses RPC-like endpoints with JSON payloads as parameters. All responses are returned as JSON.

Note: *It is strongly recommended to use the HTTPS protocol for communication with the Biacore Insight API Server, since HTTPS encrypts the transferred data. HTTPS requires usage of certificates, see Biacore Insight API Installation and Management Guide 29751155.*

If HTTP is used, note that it transfers the data without encryption, including credentials used for authentication.

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 Insight software.

Apply the appropriate company policies when accessing the Biacore Insight Database via a wireless connection.

Removable media security

Biacore Insight 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 Cytiva license server

The following firewall settings are used for Cytiva license server:

- Inbound traffic from Biacore Insight software clients
- No outbound traffic initiated by license server

Note: *The Cytiva license server installation program automatically opens the firewall ports.*

Port	Protocol	Direction	Program	Source/Destination
Any	TCP	Inbound	BIOPHARM.exe[1]	Biacore Insight software client/Cytiva license server
27000–27009	TCP	Inbound	lmgrd.exe[1]	Biacore Insight software client/Cytiva license server

[1] Full file path: `C:\Program Files (x86)\Cytiva\eLicense server\Bin\`

An Biacore Insight software client initiates a license request with lmgrd.exe, which in turn communicates with BIOPHARM.exe, and then Biacore Insight software client sends the request to BIOPHARM.exe on a dynamically assigned port.

Firewall settings for database server

Use the following settings for the Biacore Insight Database server host for inbound traffic from Biacore clients. No outbound traffic is initiated.

The settings are the default ones, but they can be altered.

Port	Protocol	Direction	Network service	Destination
1433	TCP	Inbound		Microsoft SQL Server
1434	UDP	Inbound		Microsoft SQL Server Browser
Any	Any	Outbound	Sqlservr.exe	N/A

Firewall settings on Biacore Insight software client computer

If the outgoing network traffic is blocked, apply the firewall rules as listed in the table below for the Biacore Insight software computer. The rules must be applied to the following software:

- `C:\Program Files\Biacore\Biacore Insight Control Software\Biacore.Insight.Control.exe`
- `C:\Program Files\Biacore\Biacore Insight Control Software\Biacore.Insight.LogOn.exe`
- `C:\Program Files\Biacore\Biacore Insight Evaluation Software\Biacore.Insight.Evaluation.exe`
- `C:\Program Files\Biacore\Biacore Insight Evaluation Software\Biacore.Insight.LogOn.exe`

Port	Protocol	Direction	Destination
Any	TCP	Out	Cytiva license server
1433	TCP	Out	Database server
1434	UDP	Out	Database server

Note: *The defined database server ports are the default ports used by Microsoft SQL Server. These can be changed by the database administrator and if so, the ports opened in the firewall need to be adapted.*

Firewall settings on Biacore Insight API Server computer

Biacore Insight API Server communicates with the client software (developed by the customer) via a configurable network port.

Port	Protocol	Direction	Destination
50000	HTTP(S)	In/Out	API client

Note: *The default is port 50000, but it can be changed in the Biacore Insight API Server configuration tool, see Biacore Insight API Installation and Management Guide 29751155.*

If the default port is changed, the port opened in the firewall needs to be adapted.

If the outgoing network traffic is blocked, apply the firewall rules as listed in the table below for the Biacore Insight API Server computer. The rules must be applied to the following software:

`C:\Program Files\Biacore\Biacore Insight API Server \Biacore.Insight.Evaluation.exe`

Port	Protocol	Direction	Destination
Any	TCP	Out	Cytiva license server
1433	TCP	Out	Database server
1434	UDP	Out	Database server

Note: *The defined database server ports are the default ports used by Microsoft SQL Server. These can be changed by the database administrator, and if so, the ports opened in the firewall need to be adapted.*

5.2 Data storage and encryption

Data at rest security

Biacore Insight software stores data in a persistent storage. This includes methods, results, log files, and system data. The persistent storage consists of one or more Microsoft SQL Server databases. The communication to the Microsoft SQL Server is protected by encryption, but the Biacore Insight Database is not encrypted by default. It is recommended that the database administrator enables encryption at rest on the Microsoft SQL Server databases.

When using a specific certificate on a central database, we recommend to remove ***TrustServerCertificate=True*** in the connection string. To do that, the connection string to the central database must be edited directly in the `Biacore Insight connections.config` file.

For all exported files it is the responsibility of the customer to establish appropriate file management procedures. All exported files are accessible using standard tools, except for exported runs, evaluations, run methods, and evaluation methods, which can only be imported to Biacore Insight Database using Biacore Insight software.

Recommendations for central network database installation

The recommendation is to use a central database. If a local database is used, note that the local Biacore Insight Database is configured by default for high accessibility, but with lower security. Refer to *Biacore Insight Database Installation and Management Guide (29287249)* for further details.

Data integrity capabilities

Biacore Insight software has capabilities to prevent the data from being accidentally or maliciously modified.

In a correctly configured Biacore Insight Database the user has the necessary access rights to database tables with the help of the BiacoreUsers roles.

The data for runs, regulated procedures, and regulated evaluations cannot be updated, and are thereby protected from manipulation. Users granted delete rights, if any, can however delete both runs and regulated evaluations, but not regulated procedures.

However, the database administrator has full access to the database contents and may perform changes that cannot be detected by Biacore Insight 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 Insight software is not a medical device and does not handle (create, transfer, or store) patient data. Therefore Biacore Insight software does not contain de-identification (anonymization and pseudonymization) capabilities.

Business continuity

Backup and disaster recovery routines for the Biacore Insight 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.

5.3 External connections

Connection to an external computer

See *System interconnections, on page 12* for more information.

Security controls provided by the cloud provider

Biacore Insight 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/or workstation security

Biacore Insight software is deployed in a customer controlled environment, hence the customer is responsible for local operational security.

Computer hardening

Our recommendation is to disable all unnecessary operating system (OS), system, and application services which are not necessary for the functionality of the product. For more information about computer hardening, see *https://www.cisecurity.org/*. Also, search for *Security baselines guide* on *https://learn.microsoft.com/*.

For further security adjustments, search for *Application Control for Windows* on *https://learn.microsoft.com/*.

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 Insight software. This maintenance includes at least the following:

- If a Biacore Insight Database is installed, make sure that the option to receive updates for other Microsoft products is enabled when updating Windows. This ensures that security updates for the installed version of Microsoft SQL Server is applied automatically. However, upgrades to newer versions of Microsoft SQL Server must be monitored and installed manually on a regular basis to make sure that all available security updates are applied.
- Applying updates to computer firmware and drivers.
- Applying operating system configuration changes.
- Applying operating system routine maintenance.
- Applying Biacore Insight software upgrades.
- Applying Biacore Insight 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 19*.

Questions or incident reports regarding cyber security related to Biacore Insight software can be done via the appointed Cytiva Key Account Manager or the Cytiva Service Personnel. Cytiva can aid with the following:

- A security enhancement request in Biacore Insight software
- A security incident related to the usage of Biacore Insight software
- General questions about the availability of online material such as documentation and similar

7 Remote access

Biacore Insight does not include any built-in support for remote access connections.

If any other software is used for remote access, refer to that software's documentation for privacy and security considerations.

8 Personal information collected by the product

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

Information stored in the database (such as run results, evaluations, methods, and the audit trail) includes the username and ID, which is required for the designed traceability features of Biacore Insight software.

Biacore Insight 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 Disaster recovery considerations

Disaster recovery plan (DRP)

Cytiva recommends that customers create a disaster recovery plan for their organization, and test the functionality of the plan. This plan should include the elements outlined in the following sections.

Asset management

The customer should undertake the following tasks:

1. Identify critical asset.

   This may be facilities, systems, equipment which – if destroyed, degraded, or otherwise rendered unavailable – would influence the reliability or operability of your product.

   If Biacore Insight software is considered to be a critical asset of the organization, the following items have been identified by Cytiva as critical components.

Responsibilities	Assets
Which critical assets are necessary for the operation of the product?	• Computer hosting Biacore Insight control and evaluation software. • Biacore Insight database. • Cytiva license server. Depending on configuration, these may also be regarded as critical components: • Active directory. • Biacore Insight API server (Data Integration extension).
Which components is the customer responsible for?	All of the above.
Which components is Cytiva responsible for?	None.
Which components is a third-party company responsible for?	None, unless the customer has transferred part of their responsibility.

2. Identify critical infrastructure.

   This may be existing and proposed systems and assets, whether physical or virtual. The incapacity or destruction of these systems or assets would have a negative impact on security, economic security, public health or safety, or any combination of these matters.

Examples: cloud service provider, internet connection, third-party services, etc.

If Biacore Insight software is considered to be part of the critical infrastructure of the organization, the following items have been identified by Cytiva as critical components.

Responsibilities	Infrastructure
Which critical infrastructure is necessary for the operation of the product?	Local area network for connection to Biacore Insight database and Cytiva license server, and depending on configuration, also to Active directory and Biacore Insight API server. A Biacore instrument is required for instrument related operations such as starting runs and instrument maintenance.
Which components is the customer responsible for?	All of the above.
Which components is Cytiva responsible for?	None.
Which components is a third-party company responsible for?	None, unless the customer has transferred part of their responsibility.

Identifying recovery objectives

It is essential to establish the Recovery Time Objective and Recovery Point Objective. The customer is responsible for establishing both objectives for their products.

- The Recovery Time Objective is a pre-established deadline for a business to recover their systems after an outage. The customer should specify when the system needs to be recovered.

  Examples: day, week, month, year.
- The Recovery Point Objective relates to a business' loss tolerance. This is measured by the amount of data that is deemed acceptable to be lost, before causing major damage to the customer business. The customer should specify to which time point in the past the system needs to be recovered.

  Examples: day, week, month, year.

The following table identifies the responsibilities for recovery.

Responsibilities	Objectives
What parts of the product is Cytiva able to restore back to working order in case of failure?	If wanted, Cytiva can assist in software installations on computers hosting Biacore Insight control and evaluation software. Contact your local service representative for more information.

Responsibilities	Objectives
How far back is Cytiva able to recover a failed component (restore to last working configuration)?	Cytiva is able to restore Biacore Insight control and evaluation software to the same version as installed in the last working configuration.
What data is Cytiva responsible for restoring (if any) in case of failure?	None.
What data is the customer responsible for restoring (if any) in case of failure?	It is a customer responsibility to restore all data using a backup. It is also a customer responsibility to install and configure Biacore Insight database and Cytiva license server, and depending on configuration, also Biacore Insight API Server.

Perform regular testing

The customer should perform regular testing, auditing, and assessment of their DRP to make sure that the plan is effective. It is important to evaluate the DRP routinely and confirm that the processes and procedures are still applicable. The DRP should be updated and improved when applicable.

Cytiva recommends to evaluate the DRP annually.

Additional information

For any disaster recovery support related to Biacore Insight software contact your Cytiva service representative.

For more information for industry best practices about disaster recovery visit the following websites:

- *CISA Disaster Recovery Consultation, Documentation, and Testing*
- *SANS Disaster Recovery Plan Strategies and Processes*

10 Additional privacy and security considerations

Biacore Insight 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 Insight 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 Insight software for proper mitigation.

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

- Biacore Insight software users shall not have Windows administrator privileges.
- Use secure password policy settings in Active Directory for all Biacore Insight Software users.
- Install the Biacore Insight Database on a network server. Do not use a local database installation for routine work.
- Enable relevant database logs.
- Configure database encryption according to the latest Microsoft recommendations. This must be managed by the customer database administrator.
- Monitor the Active Directory event logs to early discover any computer security compromises.

11 Product security supplemental documents

Software Bill of Materials (SBOM)

SBOM, a list of third-party software components used, is available for Biacore Insight 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 Insight software.

cytiva

cytiva.com/biacore

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

29357434 AF V:16 09/2024