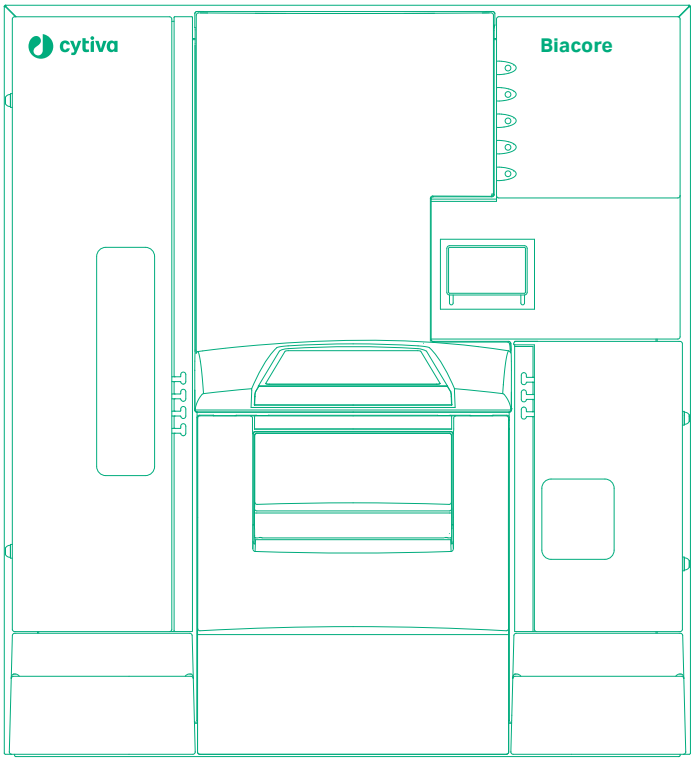
cytiva

Biacore™ S200 and Biacore T200

Privacy and Security Manual



cytiva.com

Table of Contents

1 Introduction

About this manual

This manual describes the privacy and security considerations of the Biacore™ S200 and Biacore T200 Control Software and the Biacore S200 and Biacore T200 Evaluation Software. These are referred to collectively in this manual as the Biacore S200 and Biacore T200 Software.

The privacy and security considerations of the Biacore T200 Software also apply to the Kinetics Summary applications, as well as to the Biacore T200 Software with and without the Biacore T200 GxP package.

Purpose of this manual

This manual describes the expected intended use, the Privacy & Security capabilities included, and how they are configured and used appropriately.

Scope of this manual

This manual is valid for Biacore S200 and Biacore T200.

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 protects privacy, but also protects more broadly against these risks. Privacy requires security. In the working environment one must balance privacy, security, and safety. Most of the time there is no conflict between these three domains of risk. The customer 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 Biacore S200 and Biacore T200.

Important information about intended use of the product

Biacore S200 and Biacore T200 are not medical devices and must not be used in any clinical procedures.

Contact information

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

2 Privacy and security environment

Privacy and security in the environment

The Biacore S200 and Biacore T200 Software has been designed for an intended use with the following expectations of privacy and security protections, that must be included in the environment where Biacore S200 and Biacore T200 are used:

- The Biacore S200 and Biacore T200 Software is designed to reside on a computer that is maintained from a security perspective by the customer.

If using Biacore T200 in a GxP environment, the following additional requirements also apply:

- The user logged on to the computer must be member of one of the GxP user groups.
- Access control to the folders where published procedures, results, and evaluation files are stored should be setup according to the recommendations, see *Biacore T200 GxP Handbook (28976881)*.

3 Privacy and security capabilities

About this chapter

Biacore S200 and Biacore T200 include a broad assortment of capabilities to enable privacy and security. This chapter describes the capability and the use of these privacy and security capabilities.

In this chapter

3.1 Access controls

Introduction

The access control features of Biacore S200 and Biacore T200 can be used to help control access to sensitive information. Access control includes user account creation, assigning privileges and other features.

This section provides information about controlling the user access to information.

User authentication

The Biacore S200 and Biacore T200 Software use the Windows ***User Authentication*** system to identify the user logged in to the operating system. This user is considered as the user running Biacore S200 and Biacore T200 Software. The name of the user is logged in result and evaluation files. No further user authentication is required to access Biacore S200 and Biacore T200 Software.

Assigning access rights

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

The Biacore S200 and Biacore T200 Software can be run by any user that can log in to the computer where the Biacore S200 and Biacore T200 Software is installed. Thus, access to Biacore S200 and Biacore T200 Software is assigned by granting access to the computer.

If the Biacore T200 GxP package is installed, the user logged on to Windows needs to be member in one of the Biacore GxP user groups to be able to run the Biacore T200 Software. Membership to these user groups is managed by the administrator through Windows users and groups configuration.

The different Biacore GxP user groups are listed below. These roles are described in detail in the *Biacore T200 GxP Handbook (28976881)*.

- ***BIAadministrator***
- ***BIAdeveloper***
- ***BIAuser***

Note: *Normal use of Biacore S200 and Biacore T200 software should not be performed using Windows users that has Windows administrator privileges as these users may circumvent important security settings.*

3.2 Audit logging and accountability controls

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

The Biacore S200 and Biacore T200 Software does not have built in privacy and security audit logs.

4 Patient privacy consent management

Patient privacy

Biacore S200 and Biacore T200 Software does not handle (create, transfer, or store) patient data, therefore the patient privacy consent is not applicable to Biacore S200 and Biacore T200 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 S200 and Biacore T200 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 to compromise the system.

Wired network security

Cytiva strongly recommends that the Biacore S200 and Biacore T200 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 the Biacore S200 and Biacore T200 Software 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 Biacore S200 and Biacore T200.

The Biacore S200 and Biacore T200 Software may be operated standalone, without any network connection. However, for access to the diffusion coefficient calculator that is linked from Biacore T200 Software, an Internet connection is required.

Wireless network security

Radio signals are used in a wireless network communication, therefore wireless devices require special security considerations. Effective techniques and tools exist for improving the security of wireless communication. This section describes the characteristics for wireless connections for the Biacore S200 and Biacore T200 Software.

If a network storage is used using a wireless connection, apply the appropriate company policies when accessing Biacore S200 and Biacore T200 via a wireless connection. For example, use WPA2 for network transmission encryption and mutually authenticated TLS for transport control security. MAC address filtering is something that can be considered for enhancing security as well as limited transmission power range and no SSID broadcasting.

Removable media security

The Biacore S200 and Biacore T200 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.

Data at rest security

Results, evaluations, and methods are not encrypted and are stored as files on a drive connected to the computer. It is the customer's responsibility to set up the access rights to these folders so that unauthorized access to the data and computer is prohibited.

Several recommendations are made to set up folder security if using Biacore T200 in a GxP environment. Refer to the *Biacore T200 GxP Handbook (28976881)* for more information.

Exported files in Microsoft Excel format, XML format and TXT format are not encrypted. It is the customer's responsibility to establish appropriate file management procedures.

Data integrity capabilities

Biacore S200 and Biacore T200 use binary file formats to store data, but these are not designed to prevent or detect all types of modification. It is the customer responsibility to establish appropriate file access restrictions to reduce the risk for data integrity losses due to accidental or malicious modifications in the data.

De-identification capabilities

Biacore S200 and Biacore T200 are not medical devices and do not handle patient data. Therefore, Biacore S200 and Biacore T200 Software does not contain de-identification (anonymization and pseudonymization) capabilities.

Business continuity

Backup and disaster recovery routines for the files generated by the Biacore S200 and Biacore T200 Software are the responsibility of the administrator.

The system must be configured and maintained in a way that continuously protects privacy and security.

Security controls provided by the cloud provider

Biacore S200 and Biacore T200 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. The use and configuration of antivirus software is recommended.

Server and/or workstation security

The Biacore S200 and Biacore T200 Software is deployed in a customer-controlled environment, therefore the customer is responsible for local operational security.

System change management

Cytiva provides system updates for the Biacore S200 and Biacore T200 Software.

Biacore system users can subscribe to change control notifications. This service provides information on changes in accordance with our change control processes. To register and for more information, visit *http://cytiva.com/rsf*.

Software updates after system delivery

The customer is responsible for manually updating the software with Microsoft Operating System security patches and critical patches that are released by Microsoft. The updates should be done by a user with an Administrator account. Most Microsoft updates require a reboot of the system. To avoid an impact on Biacore S200 and Biacore T200 performance, install the updates only when Biacore S200 or Biacore T200 are not in use.

The customer is responsible for maintaining the computer hosting the Biacore S200 and Biacore T200 Software. This maintenance includes the following:

- Applying operating system patches/updates
- Applying operating system upgrades
- Applying operating system configuration changes
- Applying operating system routine maintenance

- Applying Biacore S200 and Biacore T200 Software upgrades

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.

Updates to virus protection software

Malware protection software installed must be maintained by the customer. This maintenance includes management of patches, upgrades, configuration changes, and routine maintenance. For more information about how to apply malicious software protection, see *Protection from malicious attacks, on page 11*.

Questions or incident reports regarding cyber security related to the Biacore S200 and Biacore T200 Software can be done via the appointed Cytiva Key Account Manager or the Cytiva Service Personnel. Cytiva can assist with the following:

- A security enhancement request in the Biacore S200 and Biacore T200 Software
- A security incident related to the usage of the Biacore S200 and Biacore T200 Software
- General questions about the availability of online material

7 Remote access

Remote connection

Remote connection to the product is not applicable.

8 Personal information collected by Biacore S200 and Biacore T200 Software

Personal information

No personal information is collected by the Biacore S200 and Biacore T200 Software during normal use apart from the name and ID of the user performing actions in the system. The user name and ID can be used to identify a user.

The audit trail[1], results, and so on include the user name and ID, therefore it is possible to identify who the originating user is. The Biacore S200 and Biacore T200 Software has free text input fields that can be considered personal information depending on what is entered by the user. The most widely used free text input fields are the notebooks in runs and evaluations that could be used to enter personal information.

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

1 Available only for the Biacore T200 GxP package.

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 S200 and Biacore T200 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?	Computers hosting Biacore S200 and Biacore T200 control and evaluation software.
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 S200 and Biacore T200 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?	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 S200 and Biacore T200 control and evaluation software. Contact your local service representative for more information.
How far back is Cytiva able to recover a failed component (restore to last working configuration)?	Cytiva is able to restore Biacore S200 and Biacore T200 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.

Responsibilities	Objectives
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. The backup should contain all files and subdirectories in the directory `C:\BIA Users` and any other directory where files related to Biacore S200 and Biacore T200 have been saved. Backup data should be collected from all computers having Biacore S200 and Biacore T200 installed.

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 S200 and Biacore T200 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 Product security supplemental documents

Software Bill of Materials (SBOM)

SBOM, a list of third-party software components used, is available for Biacore S200 and Biacore T200 Software upon request. Contact the sales representative for a copy of SBOM.

Page intentionally left blank

Give feedback on this document

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

cytiva.com/biacore

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

29388876 AE V:9 12/2024