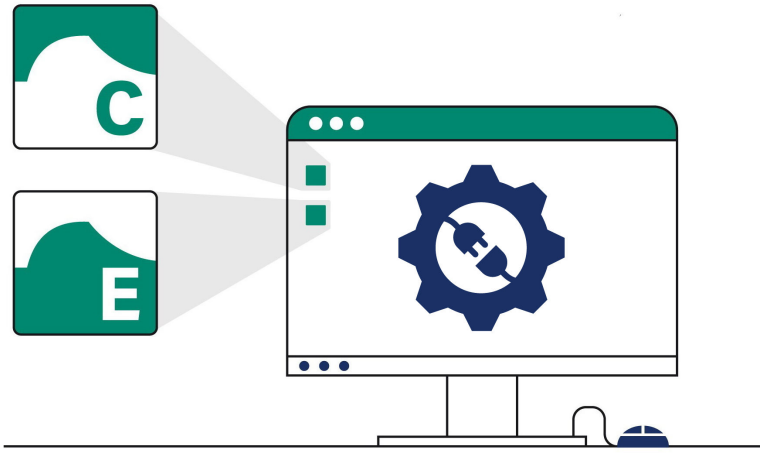
cytiva

Biacore™ Insight API

Installation and Management Guide



cytiva.com

Table of Contents

1 Introduction

About this document

This document is intended for personnel that install and configure Biacore™ Insight API Server, and personnel that integrate with Biacore Insight API.

The document applies to Biacore systems with Biacore Insight Software version 6.0 or later.

Note: *Information in this document is not required by personnel using Biacore systems for label-free interaction analysis.*

Biacore Insight API overview

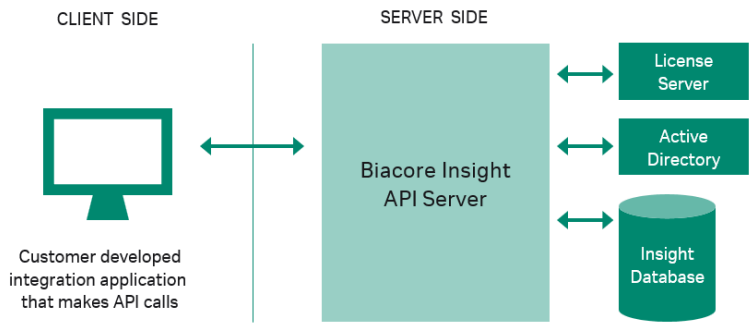
This section provides a brief overview of Biacore Insight API and its role in Biacore Insight Software. For more information, see also *Chapter 8 About Biacore Insight API Server,*

An Application Programming Interface (API) allows different software to communicate and share data with each other. Biacore Insight API enables automated export of run data and evaluated data from Biacore Insight Software. The purpose of the export can be to:

- Centralize data management, in a Laboratory Information Management System (LIMS) or similar.
- Perform data evaluation in company-specific software.
- Create reports and archive data.

Biacore Insight Software consists of five separate components:

Component	Function
Biacore Insight Control Software	Controls the connected instrument and saves its produced data into the database.
Biacore Insight Evaluation Software	Evaluates data saved in the database.
Biacore Insight Database	Stores and controls access to data.
Biacore Insight API Server	Enables automated access to run data and evaluated data for third-party applications.
Cytiva Software Licensing Server	Manages the floating licenses that give access to the software.



Biacore Insight API Server, that hosts the API, is an on-premises solution that connects to the existing Biacore Insight Database, Licensing Server, and Active Directory. An active Data Integration extension is required to access data via the Biacore Insight API. The API client is a customer developed integration application that makes data requests.

2 Installation overview

The table below presents an overview of the installation and configuration of Biacore Insight API.

Step	Action
1	Make sure that prerequisites are met. See *Chapter 3 Prerequisites, on page 6*.
2	Set up necessary Windows user accounts with corresponding database roles. See *Chapter 4 Set up users, on page 8*.
3	Install an SSL/TLS certificate on the server and client side. See *Chapter 5 Handle certificates, on page 12*.
4	Download the Biacore Insight API Server installation file and install it. See *Chapter 6 Install the API server, on page 18*.
5	Configure the API server, including basic authentication. See *Chapter 7 Configure the API server, on page 19*.
6	Develop an API client that makes data requests via the API. This is done outside the Biacore software. For relevant information, see *Chapter 8 About Biacore Insight API Server, on page 21* and *Chapter 9 Develop an API client, on page 22*.

3 Prerequisites

Prior knowledge

The person responsible for installation and configuration of the API server must be familiar with users and roles configuration in Windows Active Directory and SQL Server. Knowledge about firewall configuration is also required.

The person responsible for integration with the API must be familiar with the HTTP(S) protocol and web technology in the programming language of choice.

Computer requirements

The computer that hosts the API server must comply with the requirements listed below:

- CPU with at least four cores, 2 GHz or faster.
- At least 16 GB internal memory.
- At least 200 GB free hard disk space.
- One of the below operating systems, English version:
  - 64-bit Microsoft Windows Server 2022
  - 64-bit Microsoft Windows 10 Enterprise
  - 64-bit Microsoft Windows 10 Professional
  - 64-bit Microsoft Windows 11 Enterprise
  - 64-bit Microsoft Windows 11 Professional

Note: *The functionality of Biacore Insight Software and Biacore Insight API is verified using an English version of Windows. Other languages than English can cause issues.*

Database

Biacore Insight Database must either pre-exist or be installed prior to the API server installation. For instructions, see *Biacore Insight Database Installation and Management Guide (29287249)*.

After installation of a new database, you must first log into it once with Biacore Insight Evaluation Software, before you can connect to the database with the API server. This is to ensure the database is updated to the installed Biacore Insight software version.

Similarly, if you want to log into an existing database with a new version of the API server and evaluation software, you must first log in once with Biacore Insight Evaluation Software.

License handling

The Cytiva Software Licensing Server must be installed prior to the API server installation. For instructions, see *Biacore eLicensing Guide (29287250)*. A ***Data integration*** extension license is required on the API server to enable export via the API. Other extensions might be required to generate certain data, but not for export of already created data via the API.

SSL/TLS Certificate

It is recommended to use HTTPS protocol for communication with the API server, rather than HTTP. HTTPS uses certificates and the Transport Layer Security (TLS) protocol for encryption and server authentication.

To enable HTTPS, make sure that you have a valid SSL/TLS certificate installed on the server. For more information, see *Chapter 5 Handle certificates, on page 12*.

4 Set up users

Introduction

Before configuration of the API server, Windows users must be set up, and corresponding database roles must be assigned to allow specific operations. The table below shows relevant database roles:

Role	Description
BiacoreAPIServerRunner	Allowed to run Biacore Insight API Server.
BiacoreAPIClient	Allowed to query API server for data.
BiacoreAPIServerAdministrator	Allowed to get log files and test if server is running.
BiacoreUsersReadOnly	Allowed to read normal data from database.
BiacoreGxPreadOnly	Allowed to read GxP data from database.

Note: *To be able to set up logins to the database you need to have system administrator rights to the database instance.*

Recommended role configurations

For security reasons, three role configurations are recommended with responsibility for different tasks, see the table below.

User description	Required database roles for database login	Other requirements
User that runs the Biacore Insight API service and has right to read data from the database.	• BiacoreAPIServerRunner • BiacoreUsersReadOnly • BiacoreGxPreadOnly • Public	Must have the ***Logon as a service*** right to be allowed to run the API service. Make sure the user has write access to the log files folder: `%ProgramData%\Biacore\Insight`
User or users allowed to query the API server for data.	• BiacoreAPIClient • Public	N/A
User allowed to test if server is running and read log files generated by the API.	• BiacoreAPIServerAdministrator • Public	N/A

SQL server supports both logins for specific users and Windows groups. Both local and Active Directory groups are supported. Using groups is preferred because it simplifies administration and addition of new users.

Example of user setup

Follow the steps below to create users, groups, and logins for groups with different roles mapped.

Step	Action
1	Create the users. Example: • *APIServerRunnerUser* (user that is allowed to run the API service). • *APIClientUser* (allowed to query the API service). • *APIAdministratorUser* (allowed to monitor the API).
2	Create the groups. Example: • *APIServerRunnerGroup* (with *APIServerRunnerUser* as member). • *APIClientGroup* (with *APIClientUser* as member). • *APIAdministratorGroup* (with *APIAdministratorUser* as member).
3	Log in to the database instance with system administrator rights using SQL Server Management Studio and create logins for the groups with correct roles mapped. Example: • *APIServerRunnerGroup*. The login has the database role *BiacoreAPIServerRunner*, *BiacoreUsersReadOnly*, and *BiacoreGxPreadOnly* mapped. • *APIClientGroup*. The login has *BiacoreAPIClient* mapped. • *APIAdministratorGroup*. The login has *BiacoreAPIServerAdministrator* mapped. For an example on how to create logins, see section *6.2 Set up database logins* in *Biacore Insight Database Installation and Management Guide (29287249)*.
4	Give the *APIServerRunnerGroup* the ***Log on as a service*** right, so the members of the group are able to run the API service. ***Note:*** *To change this setting, you must have local administrator rights.* a. Open the Windows start menu and search for ***secpol.msc***. The search results are either ***secpol.msc*** or ***Local Security Policy***; click either of them to start the ***Local Security Policy*** program.

Step	Action

b. In the left pane, click ***Security Settings*** →***Local Policies*** →***User Rights Assignments***.

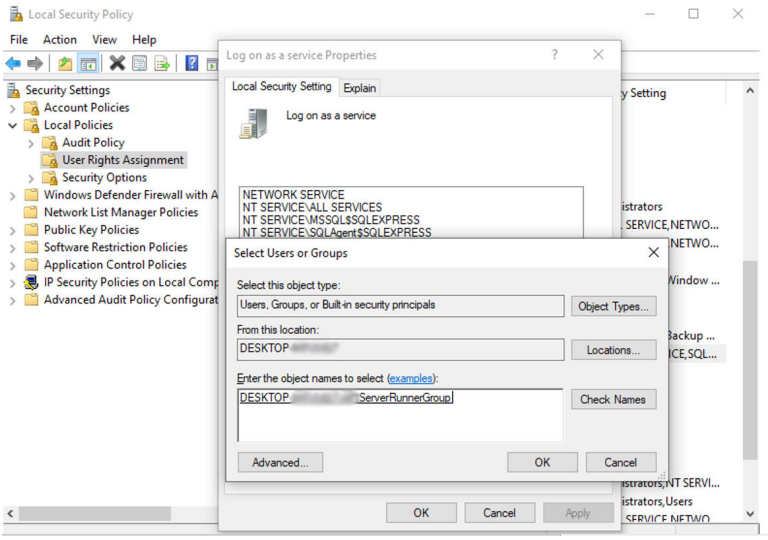
c. In the right-hand pane, find the policy ***Log on as a service***.

d. Right-click ***Log on as a service***, and then click ***Properties***.

e. In the ***Properties*** box, add the *APIServerRunnerGroup*, then click ***OK***.

Note:
When you add a group, you might need to press the ***Object Types...*** *button, then select the* ***Groups*** *object type to make it possible to add a group.*

Note:
Local Security Policies might be overridden by Group Security Policies. If the policy setting is not visible or read-only, this is probably the case.



5 Give all groups (*APIServerRunnerGroup* AND *APIClientGroup* AND *APIAdministratorGroup*) the ***Allow log on locally*** right, required for verification of roles in the Biacore Insight database.

Note:
To change this setting, you must have local administrator rights.

a. Open the Windows start menu and search for ***secpol.msc***. The search results are either ***secpol.msc*** or ***Local Security Policy***; click either of them to start the ***Local Security Policy*** program.

b. In the left pane, click ***Security Settings*** →***Local Policies*** →***User Rights Assignments***.

Step	Action

c. In the right-hand pane, find the policy ***Allow log on locally***.

d. Right-click ***Allow log on locally***, and then click ***Properties***.

e. In the ***Properties*** box, add the groups and click ***OK***.

Note:
When you are adding a group, you might need to press the ***Object Types...*** *button, then select the* ***Groups*** *object type to make it possible to add a group.*

IMPORTANT
As this policy allows users to log on to the server, it is recommended to disable remote desktop connections for these users. It is also recommended to use a separate user for server administration.

5 Handle certificates

Introduction

To enable secure communication and server authentication using HTTPS, an SSL/TLS certificate with its corresponding private key must be installed on the API server. This chapter walks you through the manual steps that are required to install such a certificate both on the API server side and the API client side. It does not guide you how to obtain a certificate, as the process can vary depending on your environment and security requirements. This chapter presents minimum recommendations, your organization might have other demands.

Contact your IT organization or relevant authorities for more detailed information on how to obtain and handle certificates.

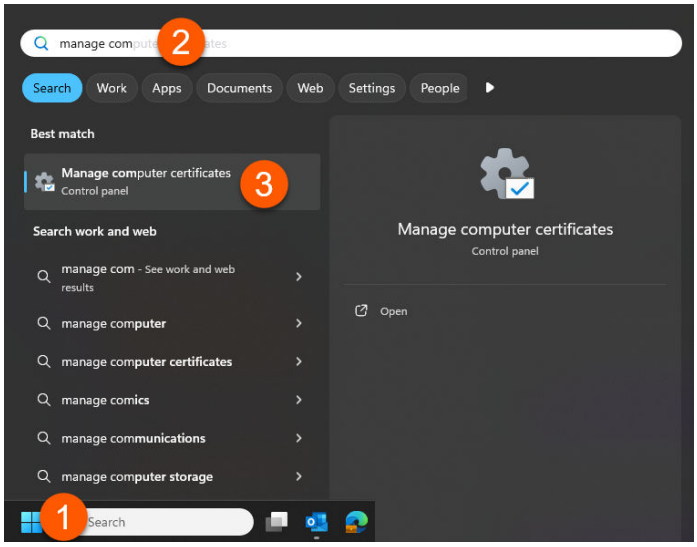
Certificate recommendations

- Self-signed certificates are **not** recommended.
- It is recommended to use a certificate chain of trust where all API clients trust a certificate higher in the chain. This enables renewal of an expired or compromised certificate on the server without requiring certification renewal on all API clients.
- The certificate must be issued for the Biacore Insight API Server's public computer name, domain, or IP address. A Fully Qualified Domain Name (FQDN) is recommended. For example, certificates issued to `localhost` does not work when connecting from a remote computer, but certificates issued to the FQDN `mycomputername.mydomain.org` works.

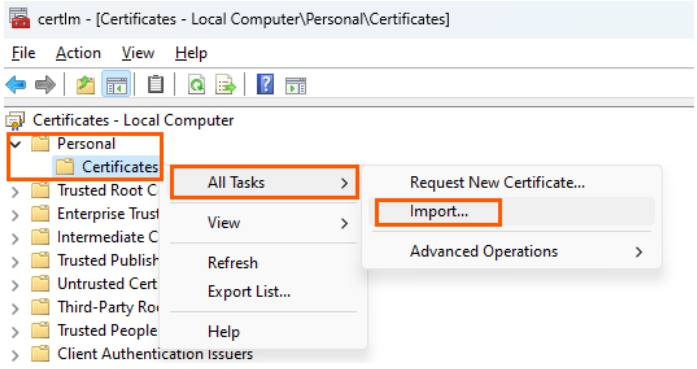
Add or renew API server certificate

Follow the steps below to add a new certificate, or renew an expiring certificate, on the server.

Step	Action
1	Open the Windows ***Start*** menu, or the Windows ***Search*** box.



2	Search for the program ***Manage computer certificates*** and run it.
3	Open the ***Personal*** folder, right-click ***Certificates***, then click ***All Tasks →Import***.



4	Follow the instructions and select your certificate file.

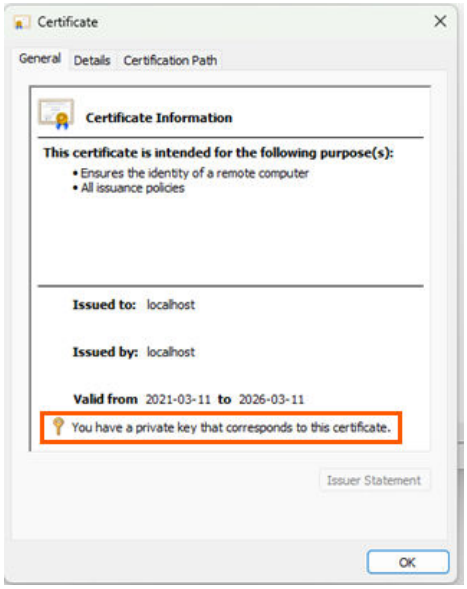
Note:
Choose any additional applicable options depending on security level. If you are uncertain, use the default settings.

Step	Action

IMPORTANT
Do not enable ***strong private key protection***.

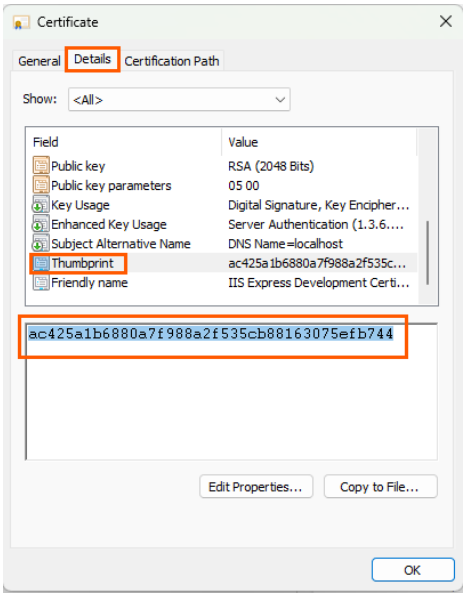
5 Complete the import.

6 Double-click the imported certificate in the view. Verify that you have the private key that corresponds to the certificate. (See screenshot below.)



IMPORTANT
If you do not have the private key that corresponds to the certificate, make sure you imported the correct certificate and repeat the previous steps.

Step	Action
7	Click the ***Details*** tab and find the ***Thumbprint***. Copy the thumbprint from the text box.



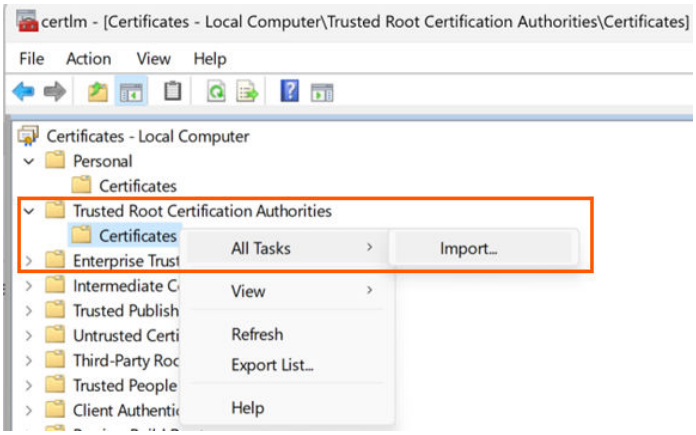
8	(Only if renewing certificate) Open a Windows administrator command prompt and type the following command, replacing ***<biacore_server_port>*** with the configured port of the Biacore Insight API Server: `netsh http delete sslcert ipport=0.0.0.0:<biacore_server_port>`
9	Open a Windows administrator command prompt and type the following command, replacing ***<biacore_server_port>*** with the configured port of the Biacore Insight API Server, and ***<thumbprint_of_certificate>*** with the thumbprint copied in the previous step: `netsh http add sslcert ipport=0.0.0.0:<biacore_server_port> certhash=<thumbprint_of_certificate> appid={8CA40661-52AB-44AE-9293-49EBA7C52D20}`
10	The certificate is now available for the API server to use. The server service might need to be restarted if it was configured and started before a valid certificate was in place. Renewing or adding an additional certificate can generally be done without a restart.

Step	Action
11	(Optional) If you want to test the connection to the server from the server itself, add the certificate as a ***Trusted Root Certification Authority*** by performing steps 1-6 in the ***Trusted Root Certification Authority →Certificates*** folder.

API client certificate

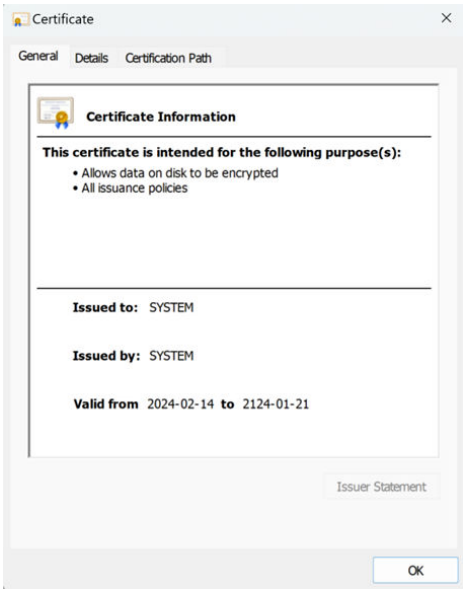
The computer running the API client must trust the Biacore Insight API Server's certificate to enable communication between the two computers. If the server certificate is signed by an already trusted certificate, no further action is needed.

However, if the certificate is not signed by a trusted certificate or is self-signed, perform the following steps:

Step	Action
1	From the start menu, search for the program ***Manage computer certificates*** and run it. For detailed instructions, see steps 1-3 in *Add or renew API server certificate, on page 13*. ***Note:*** *If you want to reduce attack surface areas and know that only a certain user will connect to the Biacore Insight API Server, you can instead search for and start* ***Manage user certificates****.*
2	In the folder ***Trusted Root Certification Authorities →Certificates***, right click and select ***All Tasks →Import***. 
3	Follow the on-screen instructions and select your certificate file. Choose any additional options desired, depending on security level. If you are uncertain, use the default settings.

Step	Action
4	Double-click the imported certificate in the view.

IMPORTANT
Make sure that you do **not** have the private key corresponding to the certificate. If you do, you have likely imported the full certificate and not only the public part. If the dialog below mentions the private key, consider removing the certificate and re-importing only the public part, as this may be a security issue.

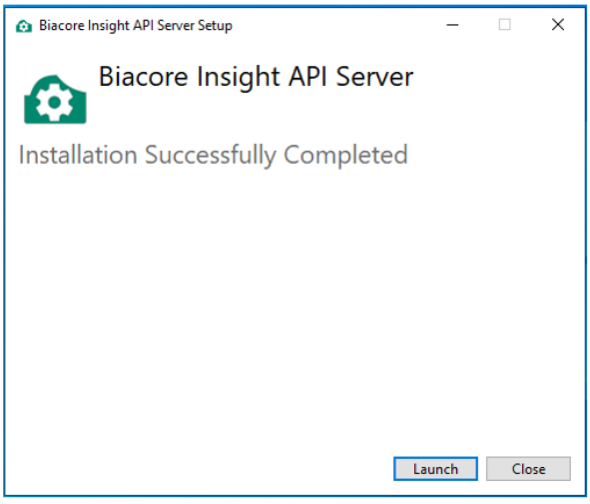


5	If required, repeat steps 1-4 to add the certificate in the folder ***Intermediate Certification Authority*** →***Certificates*** depending on how the certificate was issued. You can see which part of a certificate chain is not trusted by opening the ***Certification Path*** tab.
6	If you are not allowed to alter the ***Trusted Root Certification Authorities*** store due to security requirements, you can place the API client certificate in other places. For more information, search for and open the ***Certificate Directory*** page on the Microsoft website to read about the ***Certificate Stores.***

6 Install the API server

Follow the steps below to install Biacore Insight API Server.

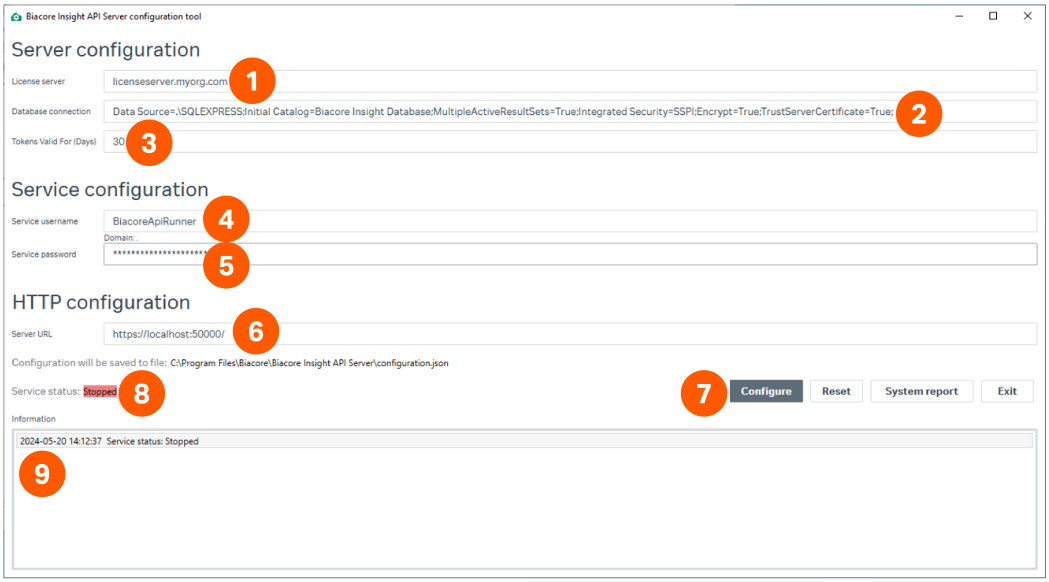
Note: *Local administrator rights are required to complete the installation.*

Step	Action
1	Download the Biacore Insight API installation package. It can be downloaded in either of two ways • From the eDelivery Portal *https://cytiva.com/eDelivery* using the Activation ID. • From *https://cytiva.com/support/software/biacore-downloads* after registration.
2	Double-click the `Biacore Insight API Server Setup.exe` file to start the installation.
3	Read the license terms and conditions, select the ***I agree to the license terms and conditions*** checkbox, and click the ***Install*** button.
4	When the installation is completed, you can either click ***Close*** to close the installation wizard and continue with the configuration later, or click ***Launch*** to start the configuration right away. For details on how to configure the Biacore Insight API Server, see *Chapter 7 Configure the API server, on page 19*. 

7 Configure the API server

Follow the steps below to configure Biacore Insight API Server.

Step	Action
1	Configure the Biacore Insight API Server by using the Biacore Insight API server configuration tool. Start the tool by double-clicking the `Biacore Insight API Server Configuration.exe` file, or by clicking on the ***Launch*** button at the end of the installation of the Biacore Insight API Server. ***Note:*** *To be able to start the API server, certain users need to be set up, see Chapter 4 Set up users, on page 8.*
2	Fill in the required information in the Biacore Insight Server Configuration window, see (1) to (6) in the below image and table.
3	Click the ***Configure*** (7) button to configure and to start the Biacore Insight API Server. Review the status of the API server in the ***Service status*** (8) field. Relevant information messages are displayed in the ***Information*** (9) field.



Label	Instruction
License server (1)	Enter the address of the license server. If the license server is installed on the same computer as the API server, enter *local-host*. For more details, see *Biacore eLicensing Guide (29287250)*.
Database connection (2)	Enter a valid connection string, used for connecting to the SQL server database. Example: *Data Source=.\SQLEXPRESS;Initial Catalog=Biacore Insight Database;MultipleActiveResultSets=True;Integrated Security=SSPI;Encrypt=True;TrustServerCertificate=True* The most important settings are: • ***Data Source***: The full name of the SQL Server instance with the syntax `ComputerName\ShortInstanceName` • ***Initial Catalog***: The database in the SQL server instance to connect to.
Token Valid for (Days) (3)	The maximum number of days an access token will be valid for.
Service username (4)	Enter the username of the user that will start the service. For more details, see *Chapter 4 Set up users, on page 8*. If the user is a local Windows user, enter the username. If the user is a domain user, enter *DOMAIN\username*
Service Password (5)	Enter the password of the user that will start the service. For more details, see *Chapter 4 Set up users, on page 8*.
Server URL (6)	An example URL is *https://biacoreapi.myorg.com:50000/*. By using "https", the secure encrypted HTTPS-protocol is used, which is recommended. This requires certificates, see *Chapter 5 Handle certificates, on page 12*. For test purposes, the http protocol can be used. Be aware that data, such as user credentials, is then transferred unencrypted. *:50000* in the example indicates that port 50000 will be used for the communication with Biacore Insight API Server. To avoid conflicts, make sure that the port is not already in use. If so, select another port. To be able to access the port from the API client, make sure that the selected port is opened in the firewall.
Configure (7)	Click to configure and to start the Biacore Insight API Server.
Service status (8)	Displays the status of the API server.
Information (9)	Displays relevant information messages.

8 About Biacore Insight API Server

Introduction

Biacore Insight API Server is an on-premises web API server that is run in a Windows Service. The name of the Windows Service is *BiacoreInsightApiServer*, and its display name is *Biacore Insight API Server*.

The API server uses token-based authentication to provide security. The token makes a snapshot of the claims when it is created.

For a general software overview, see *Chapter 1 Introduction,*

Available endpoints

The table below shows all endpoints available via the API.

Endpoint	Description
Get Token	Retrieves a token for a given user.
Assay Item Search	Searches the database for specific items, enumerated as a list.
Assay Tree Search	Searches the database for specific items, returning the matching items as a filtered database folder tree.
Get Run Data	Retrieves all run data from a run.
Get Evaluation Data	Retrieves all data from an evaluation.
Get Heartbeat	Examines the availability and reachability of the API server by checking its heartbeat.
Get Log Files	Retrieves log files that help troubleshooting issues with obtaining the API server to start or with getting data from the API server.

Concurrent request limit

The API server has a concurrent request limit functionality, used to control the rate of requests from the network. It prevents cyber security attacks.

In the API Server, the concurrency limit setting is set to a value of maximum concurrent requests. Additionally, queue functionality exists that makes sure that only one evaluation request is processed at a time.

If the concurrency limit is exceeded, an error message is shown with the standard HTTP status code 429 (Too Many Requests).

It is also logged in the API server logfile that the limit is exceeded, and the request is ignored. The actual value for the concurrency limit is included in the log message.

9 Develop an API client

Introduction

This chapter contains information useful when developing an API client. The Biacore Insight API Server conforms to the design principles of the representational state transfer (REST) architectural style using the HTTP protocol. The API client can be developed in any language and environment that supports HTTP REST and token-based authentication.

For detailed JSON schema of requests and responses, see **Developer resources - DTO Documentation** and the Swagger examples available by navigating to the Biacore Insight API Server's configured URL in a browser.

API workflow

The following table describes the normal workflow to get data through the API.

Step	Action
1	Get a token by requesting a new one from the API or by using an existing token.
2	Perform a search using criteria defined by your use case.
3	Use the search result to retrieve run data or evaluation data.

Calling an endpoint

The API server exposes several endpoints to the API client. All endpoints function much like remote procedure calls in the following way:

- All endpoints only respond to POST requests.
- A JSON object that contains all request parameters is always expected as the body of the request.
- A JSON object is always returned in the body of a successful response.
- For certain types of errors, the returned object must be examined for more details. The normal HTTP error codes apply in other cases.
- An Authorization header is required to call all except one endpoint, see *Authentication,* for details.

Authentication

The API server uses token-based authorization. To obtain a token, call the ***Get Token*** endpoint with the credentials of a Windows User that has been assigned at least one of the ***BiacoreAPIClient*** or ***BiacoreAPIServerAdministrator*** roles in the database. See *Get Token,* for more details.

The token must be included in a standard HTTP Authorization header as follows:

Authorization: basic <base64_encoded_token>

This header must be included in calls to all endpoints except ***Get Token***.

IMPORTANT

Never store a token in clear text nor share it with other people. Tokens should be treated like passwords because tokens grant access to the API.

Database path representation

Paths in the database are represented by a list of strings that represents the discrete path elements, see the example below.

Path: `Root\Folder 1\Subfolder\My Run`

Representation: `[ "Root", "Folder 1", "Subfolder", "My Run" ]`

This format was chosen as it is possible to name folders and items in the database using any character. Unusual characters can lead to ambiguity when specifying paths in normal file system format, while this list of discrete path elements removes that ambiguity.

The *Chapter 10 Endpoints, on page 25* refers to database paths using the normal format for brevity, but the above specified representation is always expected in the API.

JSON data structure

The result of an evaluation is as presented in the Biacore Insight Evaluation Software user interface in, e.g., charts and tables. The result is based on run data, the settings performed by any applied evaluation method and any manual edits performed by the user. The purpose of the JSON export is to reflect the evaluation result, including the applied settings.

The data structure follows the user interface layout of the software to large extent, so an understanding of how the software works will simplify the understanding of the JSON data structure. For more information, refer to *Biacore Insight Evaluation Software User Manual (29287248)*

The general structure of evaluation data returned from the ***Get Evaluation Data*** endpoint is as follows:

- Evaluation data with meta data about the evaluation and the included runs.
  - Evaluation results for each evaluation item organized as below:
    - Curve groups
      - Charts (possible to exclude)
        - Curve data

        - Chart meta data for how the chart is represented in the evaluation software.
    - Tables: The data for the sample and result tables available in the evaluation item.
    - Evaluation item type specific data
        - Settings
        - Specific results
- Run data (optional). Corresponds to the original run data that are loaded into the evaluation software before any data processing has been applied in any evaluation item. The run data includes the following:
    - Used flow cells and channels
    - Chip information
    - Run curve data

The same structure is used for run data returned from the ***Get Run Data*** endpoint, where the result is available in the `RunData` node.

For description of the JSON data structure, see the text about developer resources in the section below.

Developer resources

Available documentation and material helpful when developing an API client is found in the Biacore Insight API installation package. It can be downloaded in either of two ways:

- From the eDelivery portal *https://cytiva.com/eDelivery* using the activation ID.
- From *https://cytiva.com/support/software/biacore-downloads* after registration.

The package includes for example:

Item	Description
JSON Format Description	Description of the JSON data format received as payload from the ***Get Evaluation Data*** endpoint.
Python API Client	A sample API client developed in Python.
DTO Documentation	Documentation generated from Data Transfer Object (DTO) classes for all endpoint requests and responses in html format. Open the `index.html` file in the package to start navigating the annotated object structure. *Chapter 10 Endpoints,* refers to this documentation.

10 Endpoints

Introduction

This chapter lists all endpoints exposed by the server and gives a more detailed description of their usage.

Note: *All URL:s given in this chapter are relative to the base URL configured in previous chapters.*

Explanation of the tables listed under the different endpoints:

Row title	Explanation
Relative URL	The relative URL to the endpoint.
Required role	The required role of the user that owns the token used to connect to the endpoint. If the token is not connected to the required role, an `HTTP 401` error is returned.
Request DTO	The specific data transfer object (DTO) in ***Developer resources →DTO Documentation*** that the endpoint expects in the request body.
Response DTO	The specific DTO in ***Developer resources →DTO Documentation*** that the endpoint expects in the resulting response body.

Get Token

The ***Get Token*** endpoint retrieves a token for a given user.

Note: *The user must have one of the **BiacoreAPIClient** or **BiacoreAPIServerAdministrator** roles in the database.*

Relative URL	`v1/Authenticate/GetToken`
Required role	None[1]
Request DTO	`Biacore.Authentication.Dto.GetTokenRequest`
Response DTO	`Biacore.Authentication.Dto.GetTokenResponse`

[1] But the user must have one of the ***BiacoreAPIClient*** or ***BiacoreAPIServerAdministrator*** roles in the database.

Authentication is performed against Active Directory by Biacore Insight API Server when the token is obtained. If none of the above database roles are configured for the user, the token retrieval fails. If successful, the token takes a snapshot of the claims of the user at the time of retrieval. While the server tries to honor the requested lifetime of the token, the server might return a token with less lifetime at its own discretion.

The token is returned in Base64 form.

Assay Item Search

The ***Assay Item Search*** endpoint searches the database for items matching specified criteria and returns all matching items as a list.

Relative URL	`v1/AssayManagement/SearchAssayItem`
Required role	***BiacoreAPIClient***
Request DTO	`Biacore.Insight.Api.Current.Assay.AssaySearchRequest`
Response DTO	`Biacore.Insight.Api.Current.Assay.AssaySearchResponse`

Several search criteria (`SearchRequestParameter`) are possible to combine when defining the search.

Examples of possible searches:

- runs with a specific name AND specific description
- runs with a specific name OR specific description

The following search parameters can be used with either AND or OR criteria:

- `Name`
- `Description`
- `Ligand`
- `Solution`
- `PublishedProcedure`
- `Guid`
- `CustomVariableName`
- `CustomVariableValue`

The rest of the search criteria are of the AND type if they are defined. More detailed information about the search criteria is found in **Developer resources - DTO Documentation**.

The result for the search query holds basic information about the found items like GUID, name and creation time. For more information see **Developer resources - DTO Documentation**.

Assay Tree Search

The ***Assay Tree Search*** endpoint searches the database for items matching specified criteria and returns all matching items and their containing folders as a tree of folders and items.

Relative URL	`v1/AssayManagement/SearchAssayTree`
Required role	***BiacoreAPIClient***
Request DTO	`Biacore.Insight.Api.Current.Assay.AssayTreeSearchRequest`
Response DTO	`Biacore.Insight.Api.Current.Assay.AssayTreeSearchResponse`

The same search criteria are supported as for ***Assay Item Search***.

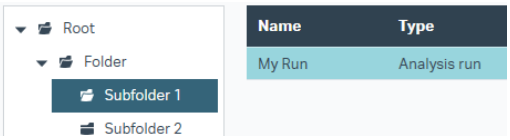
It is also possible to remove empty folders from the result as well as include or exclude the folder path from the root folder when searching only for items within a specified folder and its subfolders.

Get Run Data

The ***Get Run Data*** endpoint gets all run data from a specified run.

Relative URL	`v1/Results/Run`
Required role	***BiacoreAPIClient***
Request DTO	`Biacore.Insight.Api.Current.Evaluation.GetRunDataRequest`
Response DTO	`Biacore.Insight.Api.Current.Evaluation.GetRunDataResponse`

In the example below, a run with the name "My Run" exists under the path `Root\Folder\Subfolder 1\`.



With the ***Get Run Data*** endpoint, it is possible to get all run data for this specific run by using the full path of the run: `Root\Folder\Subfolder 1\My Run`, see section Develop API client – Database path representation.

An alternative way to get the run data is to use the GUID of the run. The GUID of the run is part of the search result when using the ***Assay Item Search*** endpoint.

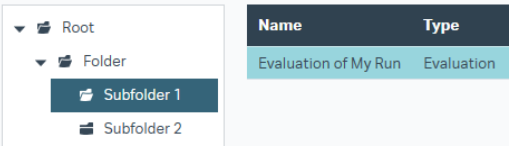
For more information about the response, see **Develop API client - JSON data structure concept for run and evaluations.**

Get Evaluation Data

The ***Get Evaluation Data*** endpoint gets all data from a specified evaluation.

Relative URL	`v1/Results/Evaluation`
Required role	***BiacoreAPIClient***
Request DTO	`Biacore.Insight.Api.Current.Evaluation.GetEvaluationDataRequest`
Response DTO	`Biacore.Insight.Api.Current.Evaluation.GetEvaluationDataResponse`

In the example below, an evaluation with the name "`Evaluation of My Run`" exists under the path `Root\Folder\Subfolder 1`.



With the ***Get Evaluation Data*** endpoint, it is possible to get evaluation data by using the full path name of the evaluation: `Root\Folder\Subfolder 1`, see section *Database path representation, on page 23*.

An alternative way to get the evaluation data is to use the evaluation GUID. The GUID of the evaluation is part of the search result when using the ***Assay Item Search*** endpoint.

Two parameters can be used to specify whether the chart data and the run data are included or excluded by the exported evaluation data:

- The `IsIncludeRunData` parameter specifies whether the run data shall be included or not. By default, this parameter is set to FALSE to reduce transfer data size.
- The `IsExcludeChartData` parameter specifies whether the chart data shall be excluded or not. By default, this parameter is set to FALSE as the chart data is a central part of the result. Set this to TRUE if you are only interested in table data.

For more information about the response, see **Develop API client - JSON data structure concept for run and evaluations**.

Get Heartbeat

The ***Get Heartbeat*** endpoint checks the availability and reachability of the Biacore Insight API Server by checking its heartbeat.

Relative URL	`v1/Observability/Heartbeat`
Required role	***BiacoreAPIServerAdministrator***
Request DTO	`Biacore.Insight.Api.Current.Observability.ObservabilityRequest`[1]
Response DTO	`Biacore.Insight.Api.Current.Observability.HeartbeatResponse`

[1] Note that the endpoint requires an empty JSON object in the request body.

Get Logs

The ***Get Logs*** endpoint gets log files that help troubleshooting issues with starting the Biacore Insight API Server or retrieving data from the Biacore Insight API Server.

Relative URL	`v1/Observability/LogContent`
Required role	***BiacoreAPIServerAdministrator***
Request DTO	`Biacore.Insight.Api.Current.Observability.ObservabilityRequest`
Response DTO	`Biacore.Insight.Api.Current.Observability.LogFileResponse`[1]

[1] Note that the endpoint requires an empty JSON object in the request body. Logs might be truncated to only include the latest messages.

The following log files are retrieved:

Log file	Description
`biacore_insight_api_server_log`	This log file provides information on the status of the Biacore Insight API Server.
`biacore_insight_api_http_protocol_log`	This log file provides information on the Biacore HTTP REST protocol.
`error.log`	This log file provides information on all errors occurring as part of the process of retrieving evaluation and run data.
`common.log`	This log file provides information on the process of retrieving evaluation and run data. It also contains all errors found in `error.log`.

11 Update consideration

Future updates of the Biacore Insight Evaluation Software will require concurrent update of the Biacore Insight API Server.

12 Troubleshooting

Introduction

This chapter presents suggested solutions to some issues that you might encounter. To suggest an addition to the troubleshooting chapter, use the feedback link on the last page of this document.

Initial troubleshooting

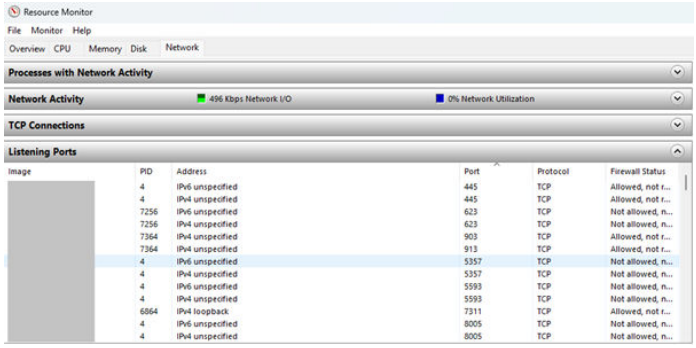
It is recommended to start all troubleshooting by following the steps below, to better understand your specific issue.

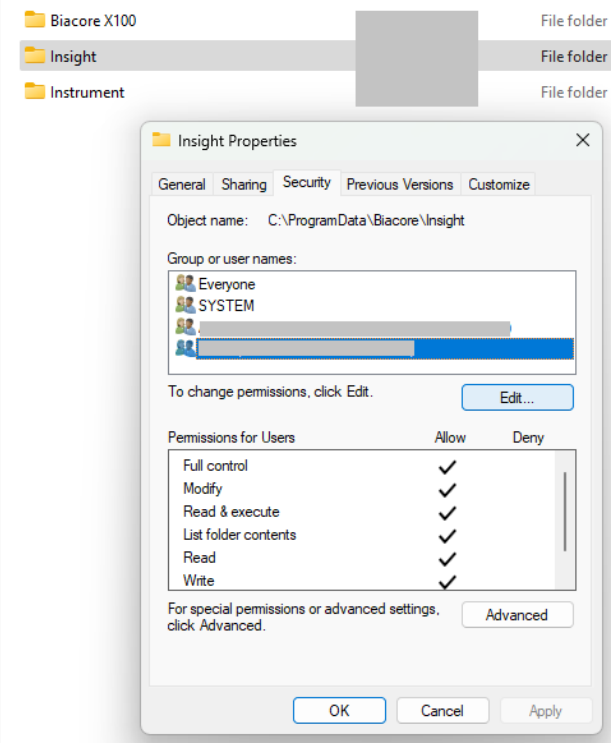
Step	Action
1	If the server fails to start properly during configuration, read the information messages in the configuration application. While the general error message lists everything, the information messages may have specific issues listed.
2	Read the log files in the `%ProgramData%\Biacore\Insight \Server` directory. If there are multiple numbered copies of the same log file, the latest logs are unnumbered. When troubleshooting issues like the server not starting or clients that are unable to connect, refer to the following log files: • `biacore_insight_api_server_log.log` • `Biacore Http REST Protocol \biacore_insight_api_http_protocol_log.log`

Server stops unexpectedly

If the server stops unexpectedly after configuration, follow the instructions in the pop-up window. If you are uncertain where to start, look in the information field of the configuration application for hints. If there are no apparent issues mentioned, follow the steps below to troubleshoot your issue.

Step	Action
1	Verify that all settings were entered correctly.
2	Verify that the server user has the required roles and policies by following the instructions in *Chapter 4 Set up users, on page 8*.
3	Verify that the server user is not a sysadmin or database owner in the SQL database.

Step	Action
4	Make sure that the configured port is not used by another process: **a.** Open the Windows ***Start*** menu and search for ***Resource Monitor***. **b.** Go to the network tab and review the used ports in ***Listening Ports***. **c.** If needed, change port. 
5	Verify that the server user has access to the log folder `%ProgramData%\Biacore\Insight` and its sub folders: Use Windows ***File Explorer*** to view and manage the user access by right-clicking the folder in question and going to ***Properties***.

Step	Action
	
6	Verify that the license server has at least one ***Data Integration*** and one ***Biacore Insight Software*** license available. The server will hold the licenses for as long as it is running.

Client cannot connect to server

If the server is running without any indicated errors but a client cannot access the server at all, follow the steps below to troubleshoot the issue:

Step	Action
1	Verify that the port is open in the server computer's local firewall. The firewall must allow inbound TCP traffic on the configured port for clients to connect.
2	Verify that the server is reachable from the client. Contact your IT organization and ensure that the server's configured port is forwarded or otherwise allowed to communicate through any router and network firewall.

Client cannot receive a token

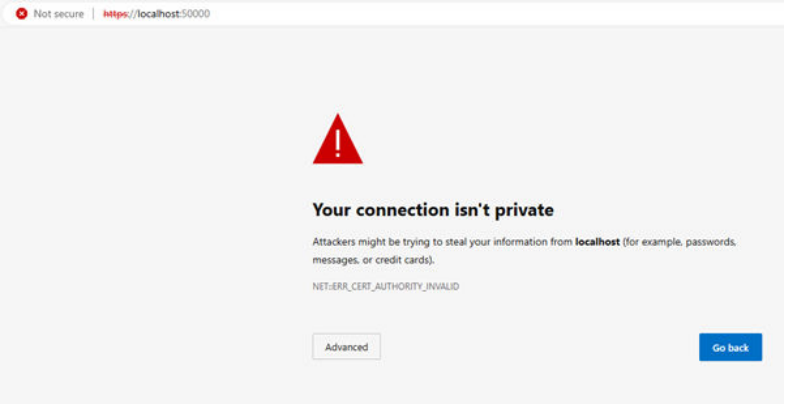
If the client can connect to the server, but the server refuses to return a token despite the credentials looking correct, follow the steps below.

Step	Action
1	Verify that all request characters are correctly escaped. Most JSON serializers handle escaping automatically. However, if you hand-roll your JSON, please ensure characters are properly escaped.
2	Verify that your client user has the required roles and policies by following the instructions in *Chapter 4 Set up users, on page 8*.

Client does not trust server certificate

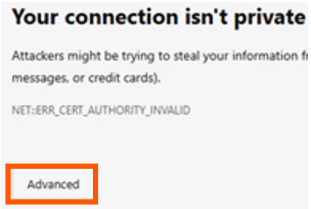
If your API client fails to connect to the Biacore Insight API Server with an error like `Server Certificate is not valid/trusted` or `Server could not be authenticated`, you likely have an issue with your certificate configuration.

To verify that you have a certificate configuration issue, copy the server address into a browser window on the client machine. If the browser warns you about an insecure connection or similar, you have issues with your certificate configuration.



Follow the steps below to troubleshoot a certification configuration issue:

Step	Action
1	Verify that the Biacore Insight API Server's certificate includes its corresponding private key. For more information, see *Add or renew API server certificate, on page 13*.

Step	Action
2	Verify that your server certificate is issued for the server's public name or IP address. For example, a certificate issued for `localhost` is not valid when you connect from a remote API client. For more information, see *Chapter 5 Handle certificates, on page 12*.
3	Verify that the API client machine trusts the server certificate itself or a certificate higher in the chain of trust. For more information, see *API client certificate, on page 16*.
4	Make sure that a server certificate has not expired: Open the same browser, click on ***Advanced*** in the warning message, and find the accessible information on the expiry date of the certificate.  If your certificate has expired, you need to obtain a new certificate, renew it on the server, and renew the trusted certificate on the clients. For more information, see *Chapter 5 Handle certificates, on page 12*.
5	Check if a certificate higher in the chain has been revoked. If so, you might be required to obtain and install a new certificate on the server and renew the trusted certificates on the clients. For more information, see *Chapter 5 Handle certificates, on page 12*.

Client receives 401 (Unauthorized) response

IMPORTANT
If new roles are assigned, you must retrieve a new token for that user before you can connect to the endpoints.

If the client receives a 401 response from the API, ensure your token has not expired. Try to generate a new token.

If the issue is not resolved, verify that the client user has the required roles for the given endpoint. For more information about the required roles for each endpoint, see *Chapter 10 Endpoints, on page 25*.

Failure during import of certificate

If you use Windows 10 operating system or an older version of Windows Server, and there are issues importing an encrypted certificate, the old Windows version might use an unsupported encryption scheme.

Follow the steps below to troubleshoot the issue:

Step	Action
1	Upgrade to a supported operating system. We strongly recommend upgrading the server operating system to one of our supported operating systems for security reasons.
2	If you cannot upgrade to a supported operating system, read and follow the Microsoft recommendations on this, or a similar updated, link from Microsoft: *https://learn.microsoft.com/en-us/troubleshoot/windows-server/certificates-and-public-key-infrastructure-pki/cannot-import-aes256-sha256-encrypted-pfx-certificate*

Page intentionally left blank

cytiva

cytiva.com

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

29751155 AA V:4 09/2024