



Biacore™ T200

**RECOMMENDED CONFIGURATION OF OPERATING SYSTEM
FOR
21 CFR PART 11 COMPLIANCE**

TABLE OF CONTENTS

1.	Introduction	3
2.	Requirements	3
3.	Biacore T200 user groups	3
3.1	Creating new users	3
3.2	Assignment to user groups.....	3
4.	Password settings	4
4.1	Password Procedure	4
5.	Screen saver settings	5
5.1	Screen Saver Procedure	5
6.	Audit trail settings	5
6.1	Audit Trail Procedure.....	5
6.2	Enabling of auditing of failed file operations	5
6.3	View audit trail of failed file operations.....	6
7.	Folder settings	6
7.1	Methods and Templates folder	6
7.2	Published Procedures folder	7
7.3	Results folder	9
7.4	Backup folder	11
8.	Security Information & recommendations	13
8.1	System Administrator	13
8.2	BIAadministrator	13
9.	References	13
	Appendix 1	14
	Appendix 2 Integration issues	15

1. Introduction

This document describes a recommendation for how to configure the operating systems **Windows 10 Professional edition and Windows 10 Enterprise edition** to facilitate compliance with 21 CFR Part 11 requirements (1). For more information, see www.fda.gov where detailed requirements for electronic signatures and records can be found. This procedure refers to Biacore T200 system controller as a local installation (stand-alone unit) and does not involve network installation settings.

2. Requirements

The IT responsible person(s) together with the system owner should configure the system to meet internal policy and procedure requirements.

This document is written for Biacore T200 GxP Software version 3.2.1.

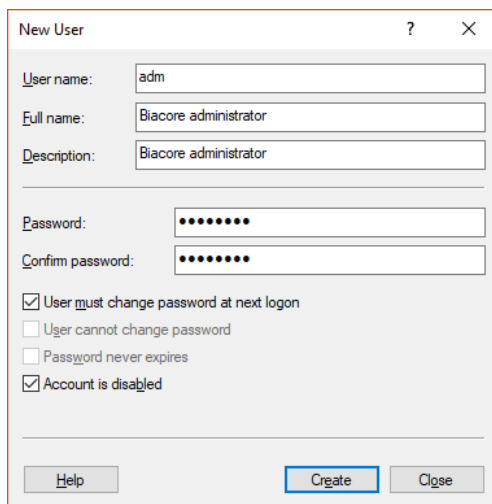
People performing the configuration of the settings must be logged on as a System Administrator unless stated otherwise.

3. Biacore T200 user groups

Ensure that the Biacore T200 Software and Biacore T200 GxP Package are installed, if not install them. Biacore T200 Software with the GxP Package adds three user groups to the Windows Users and Groups security system: BIAadministrator, BIAdeveloper and BIAuser. These groups have different access levels and authorization within the control and evaluation software, which is described in the Biacore T200 GxP Handbook (2).

3.1 Creating new users

1. Start Computer Management in the following way:
In All Apps view, start the **Run** app. Type **compmgmt.msc** and click **OK**. If a User Account Control message box appears, click **Continue**.
2. Select **Local Users and Groups – Users** and click **Action – New User**.



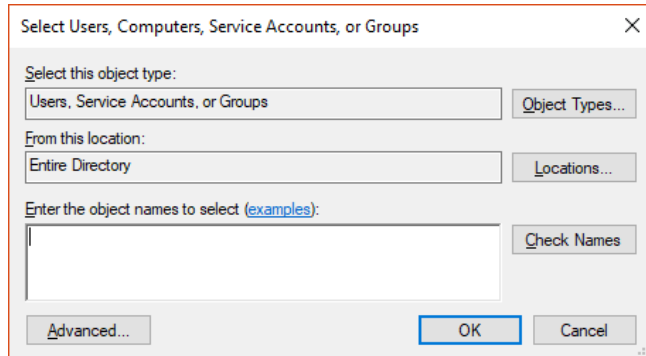
3. Enter user details as required and click **Create**.
4. Repeat step 3 for all users of the system.
5. Click **Close** and close Computer Management.

3.2 Assignment to user groups

The different users of Biacore T200 Software must have a user account that is member of an appropriate user group. The three different Biacore user groups (BIAuser, BIAdeveloper and BIAadministrator) are created automatically by the Biacore T200 GxP Package installation program but the users and the user group assignment must be made manually.

Note! Each user only has to be member of one user group. A member of the BIAdeveloper user group automatically has rights to perform everything that members of the BIAuser group can and thus does not need membership of that user group. See further Biacore T200 GxP Handbook, reference 2.

1. Start Computer Management in the following way:
In All Apps view, start the Run app. Type **compmgmt.msc** and click **OK**. If a User Account Control message box appears, click **Continue**.
2. Select **Local Users and Groups – Groups**.
3. Double-click **BIAadministrator** and click **Add**.



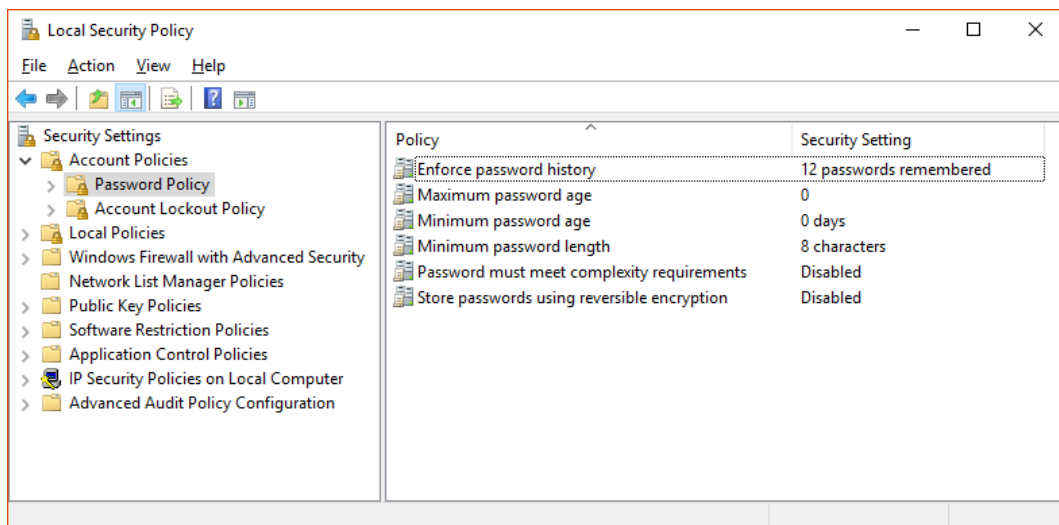
4. Type the names of the users that are to become members of the BIAadministrator group, separating each username with a semicolon (;) and click **OK** twice.
5. Repeat steps 3-4 and add members to the **BIAdeveloper** and **BIAuser** groups.
6. Close Computer Management.

4. Password settings

This section describes how to set specifications of passwords used for controlling access to the computer and programs.

4.1 Password Procedure

1. Start the Local Security Settings editor in the following way:
In All Apps view, start the Run app. Type **secpol.msc** and click **OK**. If a User Account Control message box appears, click **Continue**.



2. Locate **Security Settings – Account Policies – Password Policy** and specify suitable settings as explained in the table below.

Setting	Result
Enforce password history	To require unique passwords over time.
Maximum password age	To force changing of passwords periodically.
Minimum password age	To prevent changing passwords a number of times and then back to the original again.
Minimum password length	To require that at least a specific number of characters are used in the passwords.

3. Close the Local Security Settings editor.

5. Screen saver settings

This section describes how to set the screen saver for controlling access to the computer and programs during unattended operation.

5.1 Screen Saver Procedure

1. Right click on the desktop, click **Personalize** and click **Lock screen** to reach **Screen saver settings**.
2. Select any screen saver and set an appropriate time depending on system use.
3. Check the **On resume, display logon screen** checkbox.

Note! If the system is to be left unattended without the screen saver activated, it is recommended to lock the screen manually by pressing **Ctrl-Alt-Delete** and **Lock**.

6. Audit trail settings

6.1 Audit Trail Procedure

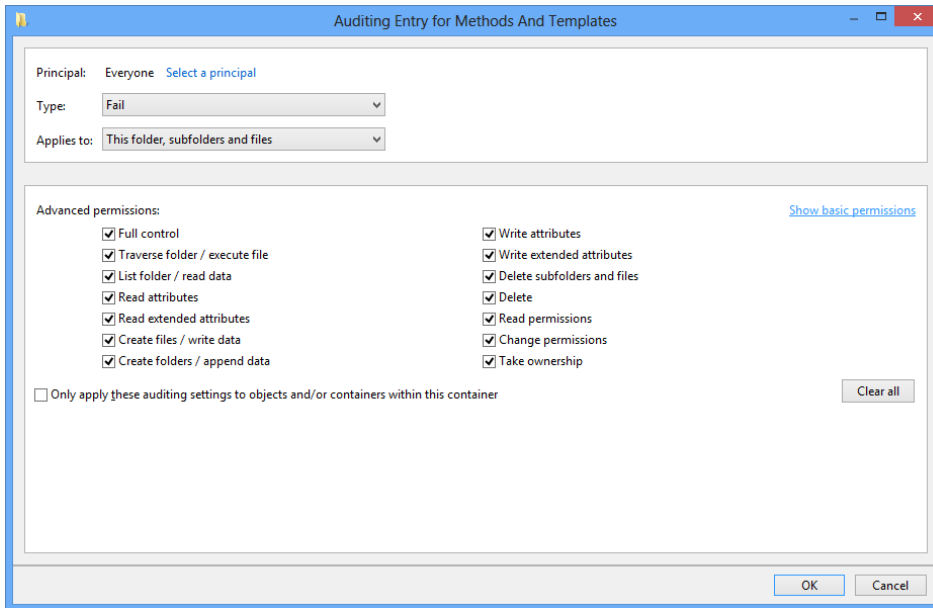
This section describes how to set the audit trail for controlling and audit object access.

1. Start the Local Security Settings editor in the following way:
In All Apps view, start the Run app. Type **secpol.msc** and click **OK**. If a User Account Control message box appears, click **Continue**.
2. Locate **Local Policies – Audit Policy**, double-click **Audit object access** and check **Failure**.
3. Click **OK** and close the Local Security Settings editor.

6.2 Enabling of auditing of failed file operations

This section describes how to activate folder audit trail and view the audit log in the operating system software.
Note: To perform these settings you need to be a System Administrator and have full control to the security permissions of current folders.

1. Log on to the system as a System Administrator.
2. Create a **Results** folder and a **Backup** folder in the **C:\Bia Users** folder using **Windows Explorer**.
3. Right click on the **C:\Bia Users\Methods and Templates** folder, click **Properties** and select the **Security** tab.
4. Click **Advanced** and select the **Auditing** tab.
5. Click **Continue**. If a User Account Control message box appears, click **Continue**.
6. Click **Add** and then **Select a principal**. Type **Everyone** and click **OK**.
7. Make sure that **Type** is set to **Fail**. Make sure that the **Apply to** combo box is set to **This folder, subfolders and files**.
8. Make sure that **Show Advanced permissions** is selected. Check the permission checkboxes according to the picture below.



9. Close any remaining windows by clicking **OK** repeatedly.
10. Repeat 4–9 for the **Published Procedures**, **Backup** and **Results** folders.

Note!

All failed file operations, such as denied attempts to delete or modify a file, are now logged by an operating system audit trail.

6.3 View audit trail of failed file operations

1. Log on to the system as a System Administrator.
2. Start Computer Management in the following way:
In All Apps view, start the Run app. Type **compmgmt.msc** and click **OK**. If a User Account Control message box appears, click **Continue**.
3. Open the audit trail under **System tools – Event Viewer – Windows Logs – Security**.

7. Folder settings

This section describes how to set the folder security settings for controlling access to files and folders.

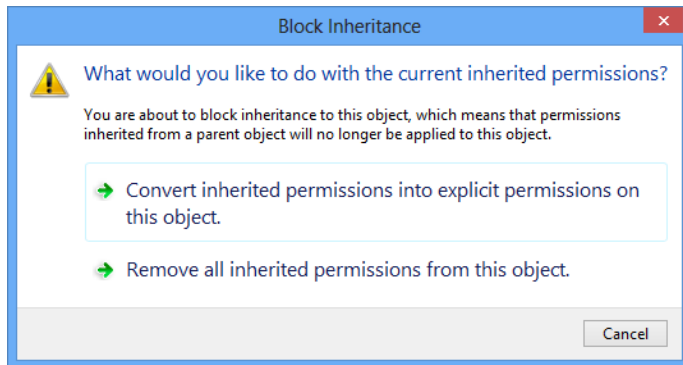
Managing access control can be simplified considerably by using command-line utilities from Microsoft® called **icacls.exe**. Examples of command files that creates the required folder structure and invokes command-line utilities to assign access control restrictions to the folders is found in appendix 1 and appendix 2.

Note! Microsoft has created a tool called **icacls.exe** that supports Windows 10. The information concerning the use of **icacls.exe** is provided as general guidelines only. Cytiva cannot take any responsibility whatsoever for the consequences of using this tool.

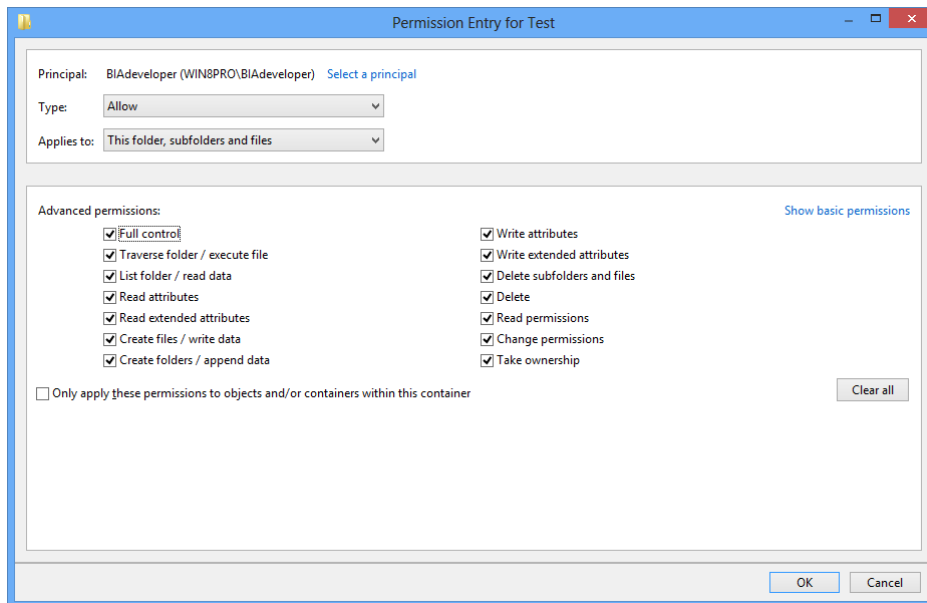
7.1 Methods and Templates folder

1. Start **Windows Explorer**.
2. Right click on the **Bia Users – Methods and Templates** folder and select **Properties**. Select the **Security** tab and click **Advanced**.
3. Click the **Change Permissions** button if it is available. The button will only exist if the folder is owned by another user than the one logged in.
Check the **Replace all child object permission entries with inheritable permission entries from this object** checkbox. Press the **Disable inheritance** button (changes name to **Enable inheritance**).

- Click **Remove all inherited permissions from this object** in the message box that appear.



- Click **Add**, and then click the link **Select a principal**. Type **BIAdeveloper** and click **OK**
- Make sure the **Apply to** combo box is set to **This folder, subfolders and files** and that **Type** is **Allow**.
- Make sure that **Show Advanced permissions** is selected. Check **Full Control** and click **OK**.



- Repeat the steps 5–7 for **BIAadministrator**.
- Click **OK** and click **Yes** in the warning message that appears.
- Click **OK** to close any remaining windows.

Note!

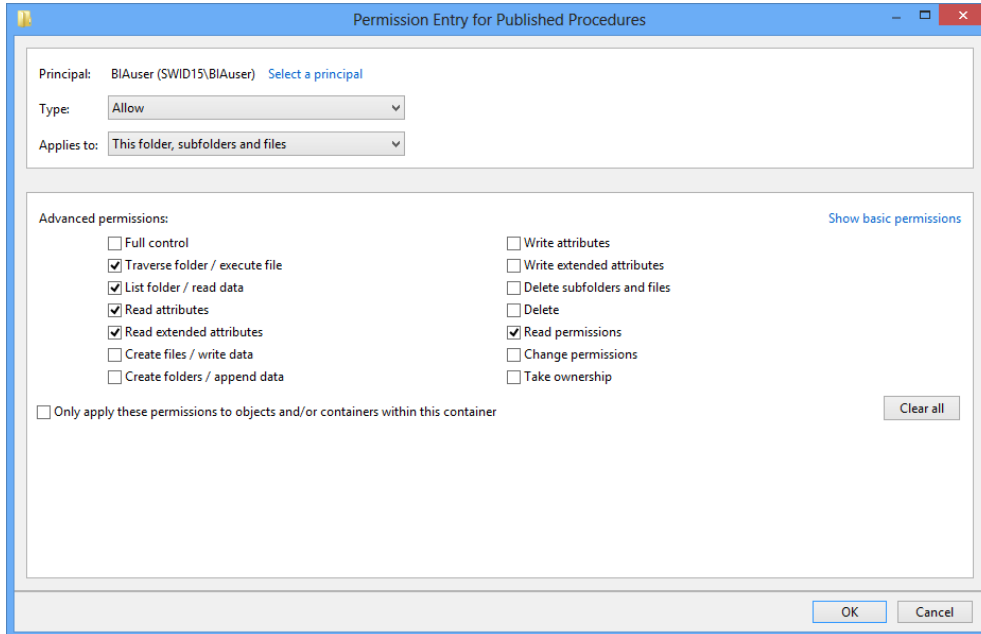
Members of the **BIAuser** group are not allowed to create, modify or delete files in the **Methods and Templates** folder.

Members of the **BIAdeveloper** and **BIAadministrator** groups have full access and other users have no access.

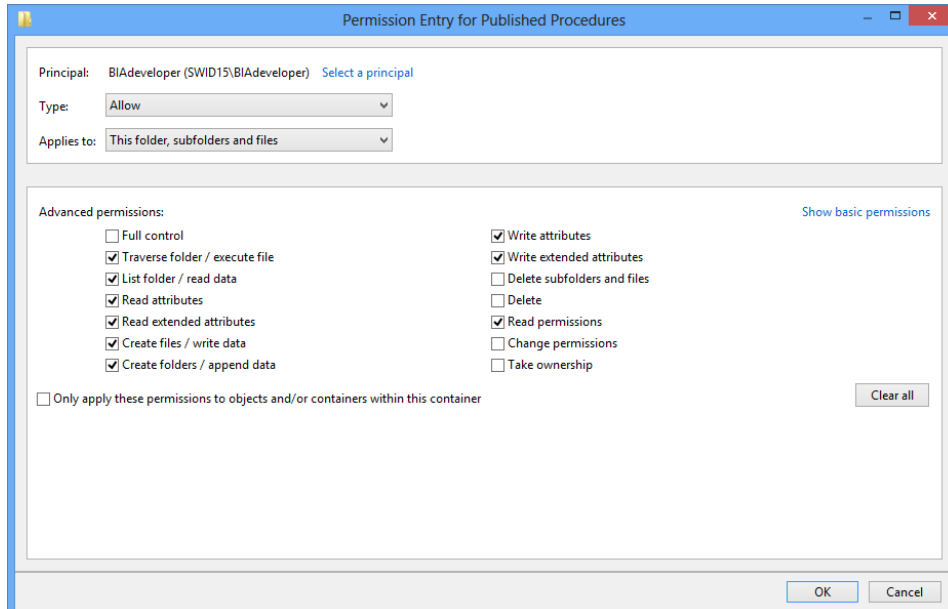
7.2 Published Procedures folder

- Start **Windows Explorer**.
- Right click on the **Bia Users – Published Procedures** folder and click **Properties**. Select the **Security** tab and click **Advanced**.
- Under the **Permissions** button if existing. Will only exist if folder is owned by another user than the one logged in. Check the **Replace all child object permission entries with inheritable permission entries from this object** and press the **Disable inheritance** button.

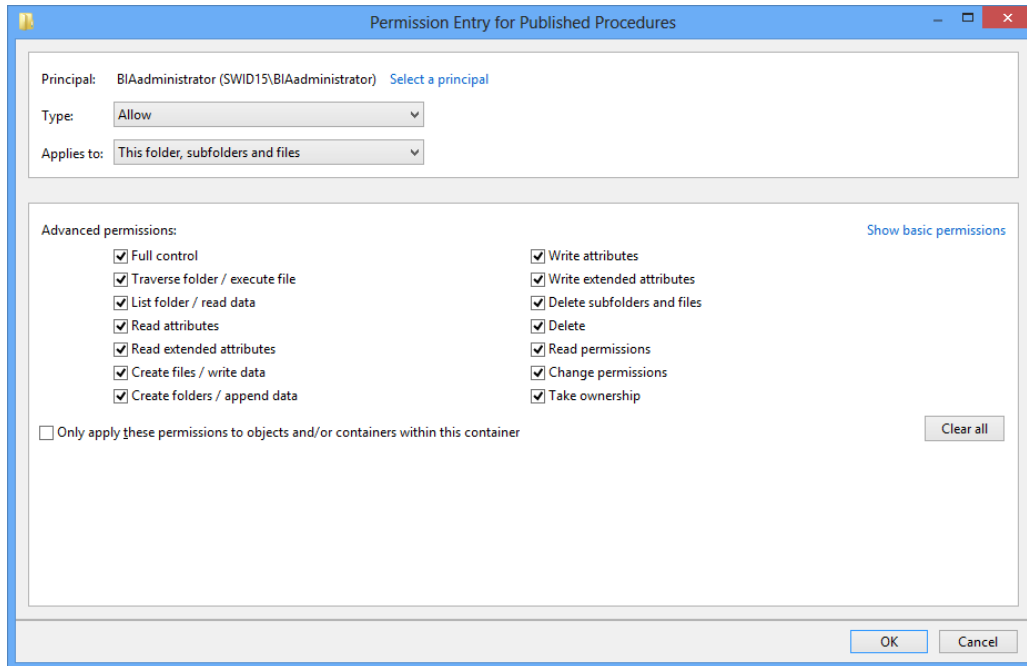
4. Click **Remove all inherited permissions from this object** in the message box that appear.
5. Click **Add**, and then click the link **Select a principal**. Type **BIAuser** and click **OK**.
6. Make sure the **Applies to** combo box is set to **This folder, subfolders and files** and that **Type** is **Allow**.
7. Make sure that **Show Advanced permissions** is selected. Check the five checkboxes in the **Advanced permissions** list as shown in the figure below:



8. Click **OK**.
9. Repeat steps 5–8 for the **BIAdeveloper** group using settings as shown in the figure below.



10. Click **OK**.
11. Repeat steps 5–8 for the **BIAadministrator** group using settings as shown in the figure below:



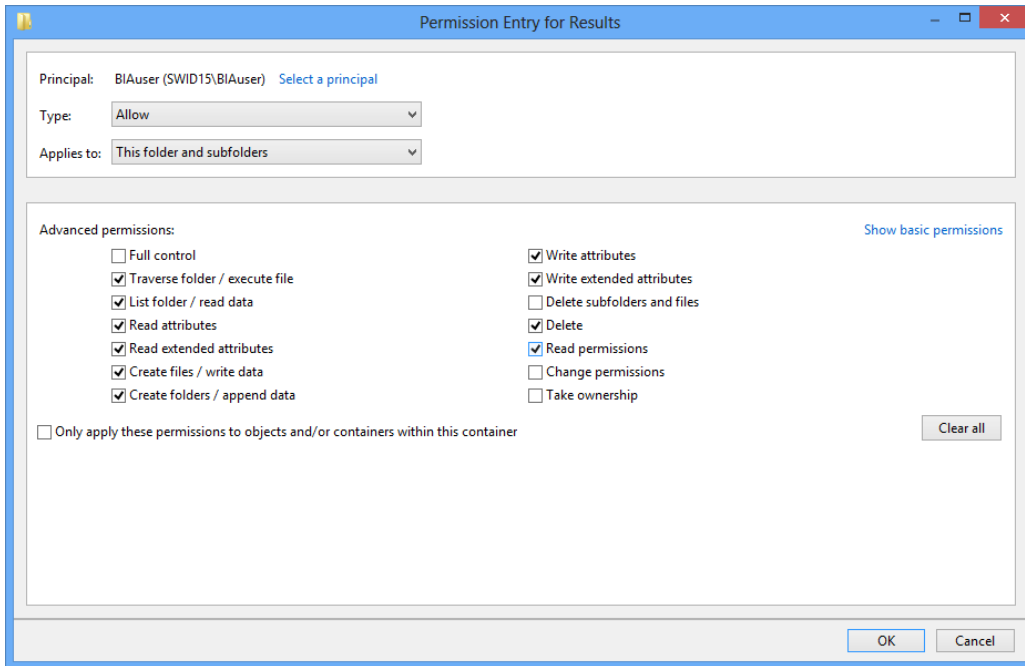
12. Click **OK** and click **Yes** in the warning message that appears.
13. Click **OK** to close any remaining windows.

Note!

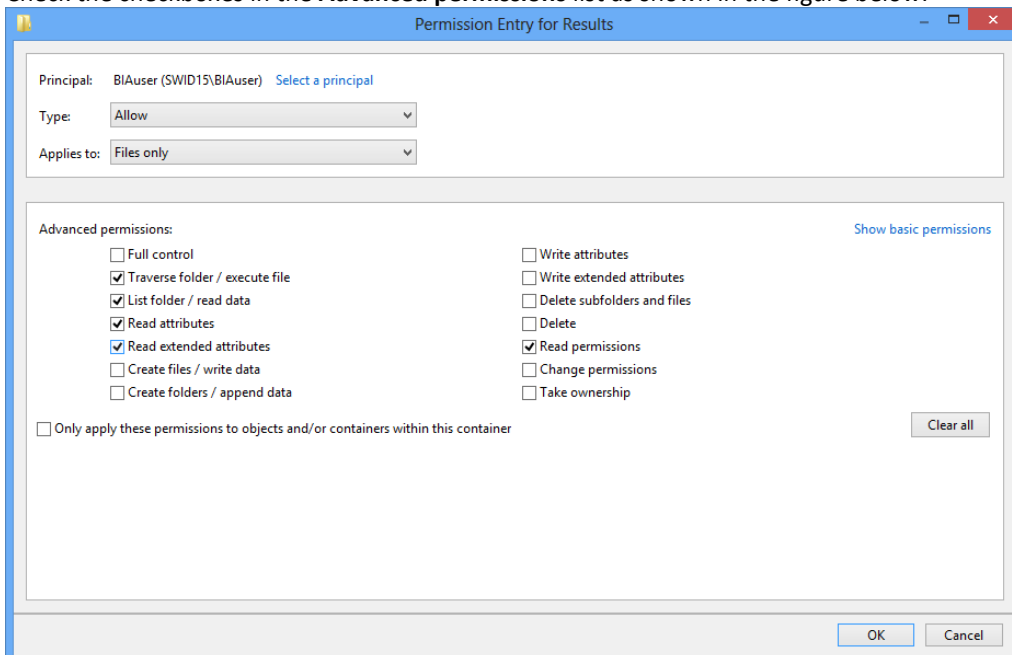
Members of the **BIAuser** group are not allowed to create, modify or delete files and members of the **BIAdeveloper** group are not allowed to delete files in the **Published Procedures** folder. Members of the **BIAadministrator** group have full access and other users have no access.

7.3 Results folder

1. Right click on the **Results** folder and click **Properties**. Select the **Security** tab and click **Advanced**.
 Click the **Change Permissions** button if it is available. The button only exists if the folder is owned by another user than the one logged in.
 Check the **Replace all child object permission entries with inheritable permission entries from this object** and press the **Disable inheritance** button.
2. Click **Remove all inherited permissions from this object** in the message box that appear.
3. Click **Add**, and then click the link **Select a principal**. Type **BIAuser** and click **OK**.
4. Make sure that **Applies to** combo box is set to **This folder and subfolders** and that **Type** is **Allow**.
5. Check the checkboxes in the **Advanced permissions** list as shown in the figure below:

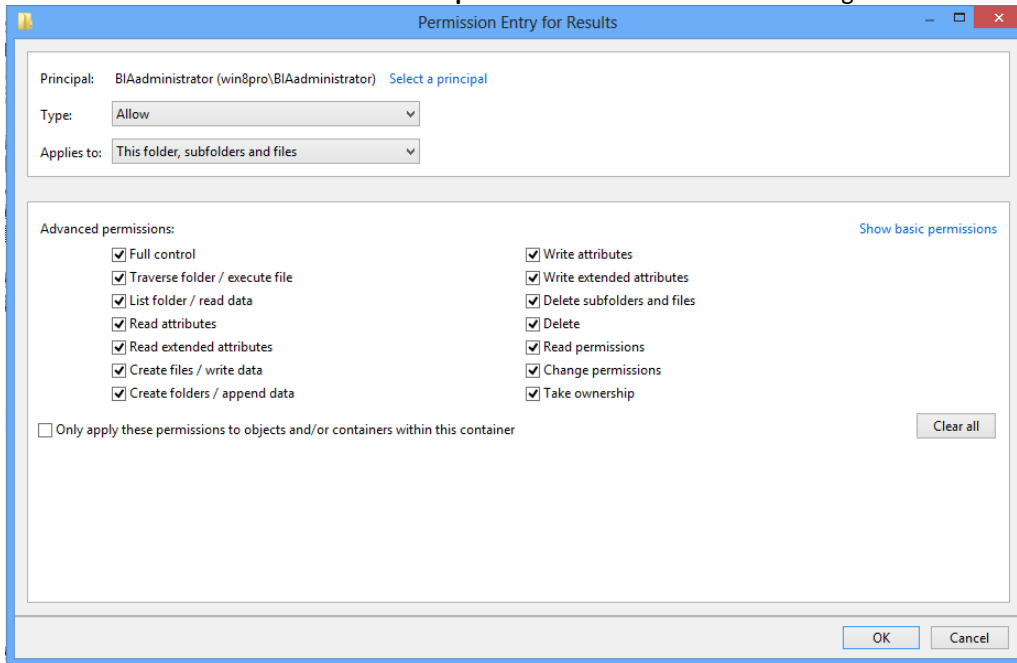


6. Click **OK**.
7. Click **Add**, type **BIAuser** (again) and click **OK**.
8. Make sure the **Apply to** combo box is set to **Files only**.
9. Check the checkboxes in the **Advanced permissions** list as shown in the figure below:



10. Click **OK**.
11. Repeat steps 3–10 for the user group **BIAdeveloper**.
12. Click **Add**, and then click the link **Select a principal**. Type **BIAadministrator** and click **OK**.
13. Make sure the **Apply to** combo box is set to **This folder, subfolders and files** and that **Type** is **Allow**.

14. Check the checkboxes in the **Advanced permissions** list as shown in the figure below and click **OK**:



15. Click **OK** and click **Yes** in the warning message that appears.
16. Click **OK** to close any remaining windows.

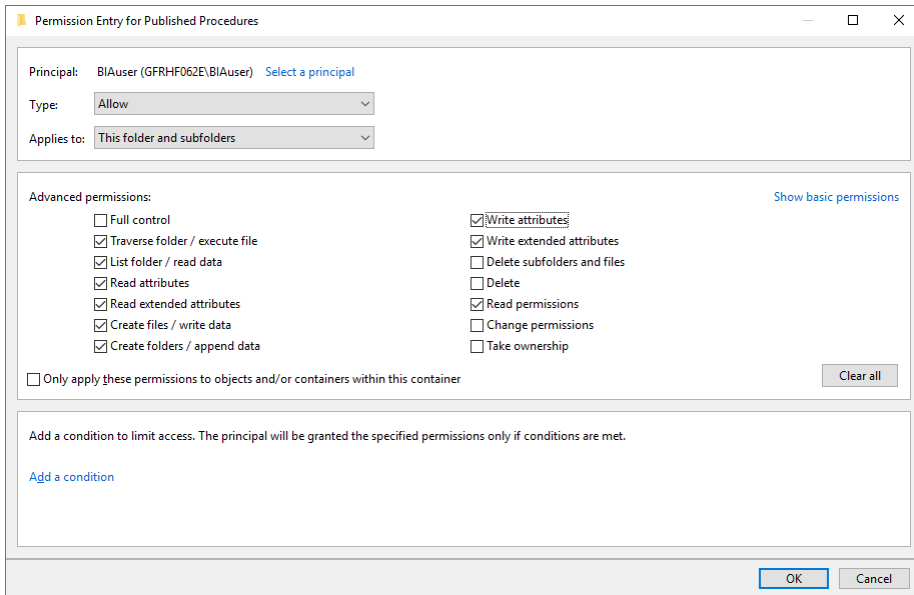
Note!

Members of the **BIAuser** and **BIAdeveloper** groups are not allowed to modify or delete files in the **Results** folder.

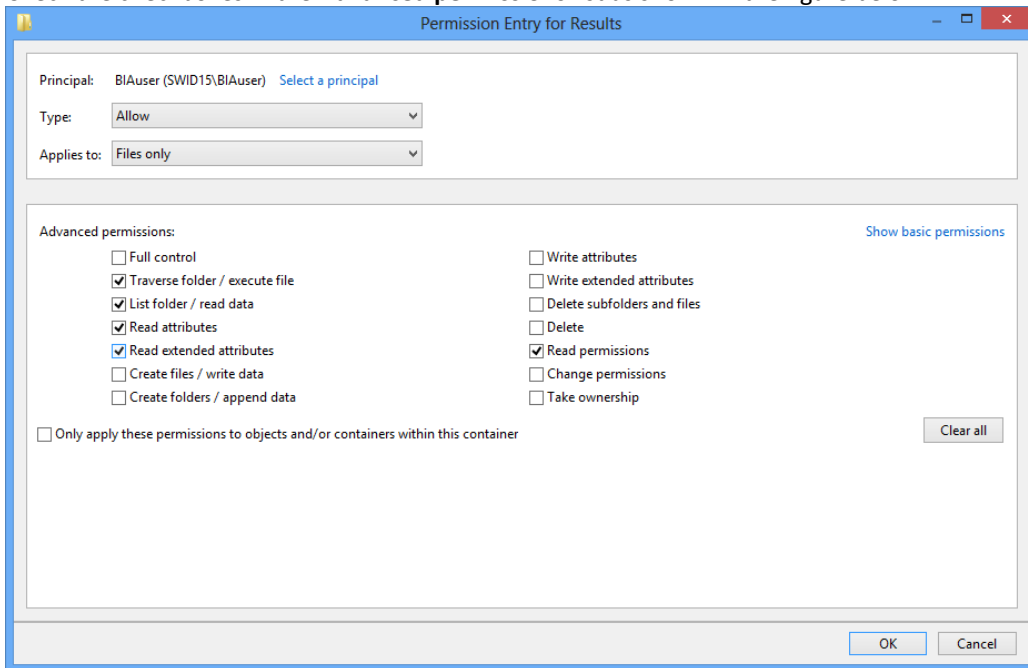
Members of the **BIAadministrator** group have full access and other users have no access.

7.4 Backup folder

1. Right click on the **Backup** folder and click **Properties**. Select the **Security** tab and click **Advanced**.
2. Click the **Change Permissions** button if it is available. The button only exists if the folder is owned by another user than the one logged in.
Check the **Replace all child object permission entries with inheritable permission entries from this object** and press the **Disable inheritance** button.
3. Click **Remove all inherited permissions from this object** in the message box that appear
4. Click **Add**, and then click the link **Select a principal**. Type **BIAuser** and click **OK**
5. Make sure that **Applies to** combo box is set to **This folder and subfolders** and that **Type** is **Allow**.
6. Check the checkboxes in the **Advanced permissions** list as shown in the figure below:

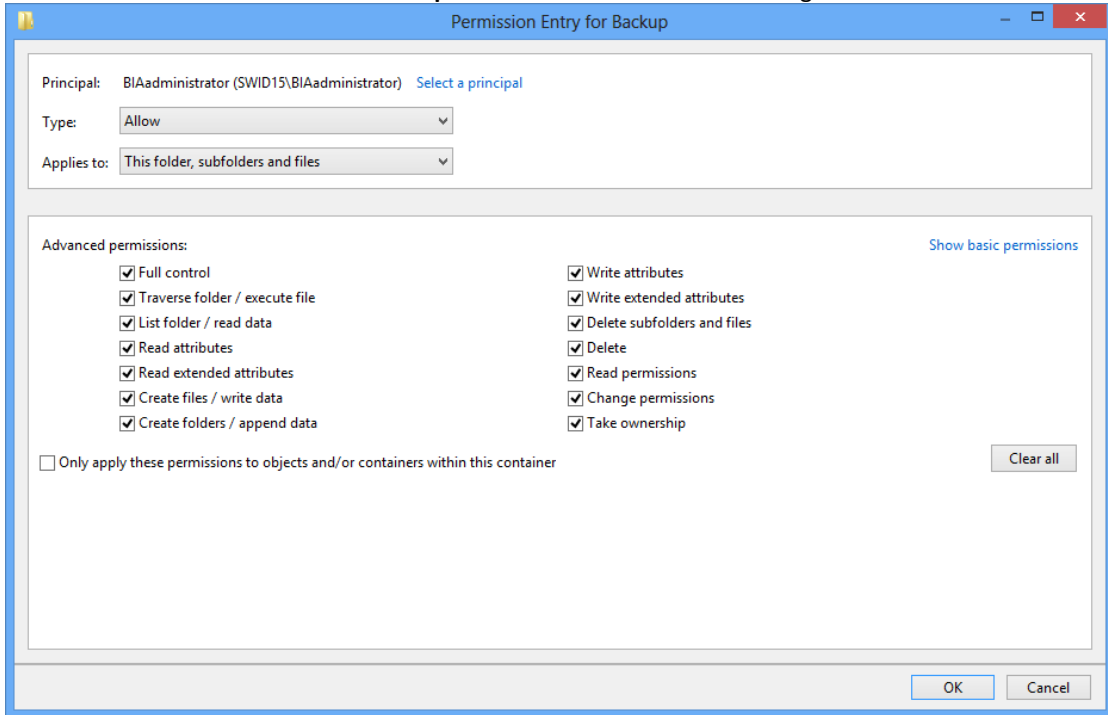


7. Click **OK**.
8. Click **Add**, type **BIAuser** (again) and click **OK**.
9. Make sure the **Apply to** combo box is set to **Files only**.
10. Check the checkboxes in the **Advanced permissions** list as shown in the figure below:



11. Click **OK**.
12. Repeat steps 4–11 for the user group **BIAdeveloper**.
13. Click **Add**, and then click the link **Select a principal**. Type **BIAadministrator** and click **OK**.
14. Make sure the **Apply to** combo box is set to **This folder, subfolders and files** and that **Type** is **Allow**.

15. Check the checkboxes in the **Advanced permissions** list as shown in the figure below and click **OK**:



16. Click **OK** and click **Yes** in the warning message that appears.

17. Click **OK** to close any remaining windows.

Note!

Members of the **BIAuser** and **BIAdeveloper** groups are not allowed to modify or delete files in the **Backup** folder.

Members of the **BIAadministrator** group have full access and other users have no access.

8. Security Information & recommendations

The following section is general information and recommendations on how to control system audit trail and result file handling.

8.1 System Administrator

By following the previously described actions, the **System Administrator** can now read the created operating system audit trail.

However, the **System Administrator** can also delete the created audit trail, without creating an audit trail of that action. It is therefore recommended that deletion of the operating system audit trail is controlled by a company specific routine.

8.2 BIAadministrator

Following the previously recommended procedures, the **BIAadministrator** can now move and delete files from the **Results, Published Procedures** or **Backup** folders, but cannot view the operating system audit log.

It is therefore recommended that deletion of result files is controlled by a company specific routine.

9. References

1. Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures (US Food and Drug Administration)
2. Biacore T200 GxP Handbook, 28976881, Cytiva Sweden AB

Appendix 1

In this appendix an example of a command file is provided, that automates the creation of the folders needed and the assignment of access control restrictions to the respective folders that is described in chapter 7. The command file invokes *icacls.exe*, a command-line utility tool, which is included in Windows 10.

Copy the commands below and save them in a command file ('.bat' file), and then execute the command file as administrator.

```
md "c:\BIA Users\Published Procedures"
md "c:\BIA Users\Backup"
md "c:\BIA Users\Results"
md "c:\BIA Users\Methods and Templates"

icacls "c:\BIA Users\Published Procedures" /inheritance:r
icacls "c:\BIA Users\Published Procedures" /grant:r BIAuser:(OI)(CI)(GR,GE) /T
icacls "c:\BIA Users\Published Procedures" /grant:r BIAdeveloper:(OI)(CI)(GR,GW,GE) /T
icacls "c:\BIA Users\Published Procedures" /grant:r BIAadministrator:(OI)(CI)F /T

icacls "c:\BIA Users\Backup" /inheritance:r
icacls "c:\BIA Users\Backup" /grant:r BIAuser:(CI)(GR,GW,GE) /T
icacls "c:\BIA Users\Backup" /grant:r BIAuser:(OI)(IO)(GR,GE) /T
icacls "c:\BIA Users\Backup" /grant:r BIAdeveloper:(CI)(GR,GW,GE) /T
icacls "c:\BIA Users\Backup" /grant:r BIAdeveloper:(OI)(IO)(GR,GE) /T
icacls "c:\BIA Users\Backup" /grant:r BIAadministrator:(OI)(CI)F /T

icacls "c:\BIA Users\Results" /inheritance:r
icacls "c:\BIA Users\Results" /grant:r BIAuser:(CI)(GR,GW,GE,D) /T
icacls "c:\BIA Users\Results" /grant:r BIAuser:(OI)(IO)(GR,GE) /T
icacls "c:\BIA Users\Results" /grant:r BIAdeveloper:(CI)(GR,GW,GE,D) /T
icacls "c:\BIA Users\Results" /grant:r BIAdeveloper:(OI)(IO)(GR,GE) /T
icacls "c:\BIA Users\Results" /grant:r BIAadministrator:(OI)(CI)F /T

icacls "c:\BIA Users\Methods and Templates" /inheritance:r
icacls "c:\BIA Users\Methods and Templates" /grant:r BIAdeveloper:(OI)(CI)F /T
icacls "c:\BIA Users\Methods and Templates" /grant:r BIAadministrator:(OI)(CI)F /T

pause
```

Appendix 2 Integration issues

The instructions in this document support the setup of users and folder permissions. The following issues with integration of Biacore T200 GxP software with Windows have been found.

- In some cases, not possible to save Kinetic Summary Files. This is linked to the fact that Kinetic Summary is not part of the GxP package.
- Errors reported when trying to open files from non-existing (re-named) folders. This may happen if results are not forced to a specific folder as recommended.



cytiva.com

Cytiva and the Drop logo are trademarks of Global Life Sciences IP Holdco LLC or an affiliate.

Biacore is a trademark of Global Life Sciences Solutions USA LLC or an affiliate doing business as Cytiva.

All other third-party trademarks are the property of their respective owners.

© 2021 Cytiva

All goods and services are sold subject to the terms and conditions of sale of the supplying company operating within the Cytiva business. A copy of those terms and conditions is available on request. Contact your local Cytiva representative for the most current information.

For local office contact information, visit [cytiva.com/contact](https://www.cytiva.com/contact)