Bio-Plex Manager 4.0 Security Edition

Configuration Setup Guide

For technical service, call your local Bio-Rad office,
or in the US, call 1-800-4BIORAD (1-800-424-6723)

Part no. 10000528 Rev A

Table of Contents

Introduction

Bio-Plex Manager Security Edition works in conjunction with the built-in security features of the Microsoft® Windows® 2000 and Windows® XP Professional operating systems to provide a secure environment for the maintenance, verification, and tracking of all electronic records generated by the application. These records include Protocol and Results files, and the Calibration, Validation, and Instrument Operations Logs. The tools provided in the software include:

- Access controls and authority checks via the use of user identification codes and passwords
- Electronic record security via the use of protected directories
- Time- and date-stamped audit trails
- Electronic signature of electronic records (user authentication)

When properly configured and administered, these tools ensure compliance with the rules for secure handling of electronic records as outlined in Title 21, Part 11 of the Code of Federal Regulations (CFR).

The Bio-Plex Manager Security Edition security model is layered on top of the Windows 2000 and XP Professional security model. If the Windows operating system is not properly configured, the Bio-Plex Manager Security Edition system will not be secure, and therefore will not be in compliance. This document provides guidelines for a Windows system administrator to properly configure and maintain the Windows security environment for use with Bio-Plex Manager Security Edition.

Note: Bio-Rad makes no claim that Bio-Plex Manager Security Edition is CFR compliant in and of itself, nor does it guarantee compliance for the user. The organization implementing and using Bio-Plex Manager Security Edition must establish policies and standard operating procedures that work in conjunction with the tools provided by Bio-Rad to ensure compliance with 21 CFR Part 11.

Background on 21 CFR Part 11

Effective August 20, 1997, the United States Food and Drug Administration (FDA) released Part 11 "Electronic Records; Electronic Signatures" of title 21 of CFR. This rule states the conditions under which the FDA considers electronic signatures and electronic records to be trustworthy, reliable, and equivalent to traditional handwritten signatures.

Bio-Plex Manager Security Edition is designed to enable organizations and institutions using the Bio-Plex System to comply with the rules laid out under 21 CFR Part 11. It enables system administrators to ensure that Bio-Plex Manager operates in compliance with 21 CFR Part 11 within a "closed system." A closed system is defined as "*an environment in which system access is controlled by the persons who are responsible for the content of electronic records that are on the system*" (Section 11.3 (b) (4)).

Note on This Document

The document provides general guidelines for configuring the built-in security features of the Windows 2000 and XP Professional operating systems. Systems may vary depending on the version of the operating system, local versus network domain account settings, or other differences. This document cannot cover all possible variations, and it assumes a certain level of knowledge and expertise on the part of the Windows system administrator.

Also, certain procedures and policies will by their nature need to be implemented by the user of the software and are the responsibility of the user. This document will identify these areas and make suggestions for policies and procedures.

Standard Mode Versus Secure Mode

Bio-Plex Manager Security Edition can run in standard mode, in which all the security and audit trail features are disabled and the software functions like the standard version of Bio-Plex Manager, or it can run in Secure Mode, with the security functions enabled.

Security Edition Hardware Protection Key (HPK)

Bio-Plex Manager Security Edition is shipped with a special Security Edition hardware protection key (HPK, also known as a HASP key). In the case of the Workstation or Desktop versions of the software, the HPK must be attached to a USB port on the computer running the software. In the case of the Network Desktop version, it must be attached to a USB port on the network file server computer.

Windows Users and Groups

Bio-Plex Manager Security Edition uses Windows user groups to establish security levels within Bio-Plex Manager and Windows user accounts to create user names and passwords. It is essential that these Windows groups and accounts be correctly configured to enable the security features of Bio-Plex Manager Security Edition.

User Groups

The following six Windows user groups must be set up on the system. These groups can be located either locally or on a network domain.

Note: The user groups you create must be named *exactly* as below.

- **BP_Admin** – Users at this level can enable or disable Secure Mode. Administrator-level users

also can view log files. Access to all other features and functions of the software is restricted.

- **BP_Supervisor** – Users at this level have full access to all features and functions of the software, except that they cannot enable or disable Secure Mode.

- **BP_Service** – Users at this level have full access to all features and functions of the software, except that they cannot enable or disable Secure Mode.

- **BP_Clinician_2** – Users at this level can perform instrument operations, run existing protocols, and view Protocol files, Results files, and log files. They can also change the number of unknown samples in the plate format (using the **Set Number of Unknown Samples** command) and enter sample descriptions. All other access is restricted.

- **BP_Clinician_1** – Users at this level can perform instrument operations, run protocols, and view Protocol files, Results files, and log files, but cannot change any settings. All other access is restricted.

- **BP_Reviewer** – Users at this level can view and sign Protocol and Results files, and can view log files. All other access is restricted.

The tools for setting up Windows user groups are located in different places, depending on whether you are setting them up on a local computer or on a network server.

User Accounts

To give users access to Bio-Plex Manager Security Edition, you can create new Windows user accounts or add existing user accounts to the user groups that you create.

Note the following:

- A user account can have any name or password. See the section on Password Security later in this document for information on setting passwords for maximum security.
- Each user can belong to only one Bio-Plex Manager user group. For example, a user cannot belong to both the BP_Admin group and the BP_Supervisor group.

Configuring Users and Groups on a Local Computer

To set up users and groups on a local computer, go to the Windows **Control Panel**, select **Administrative Tools**, and then select **Computer Management**.

In the *Computer Management* window, expand the *System Tools* folder, and then expand the *Local Users and Groups* folder.

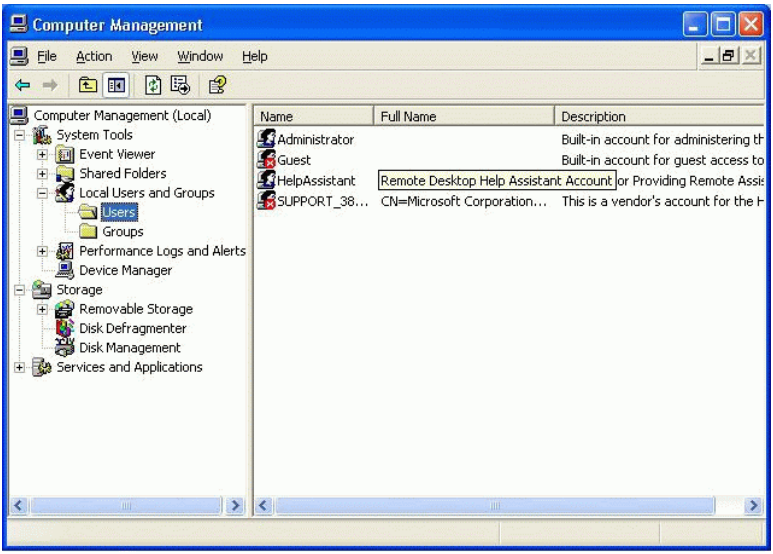

Figure 1. Computer Management screen: Local computer.

To create a new user on a local computer:

Click on the *Users* folder to open it and select **New User** from the *Action* menu or the right-click context menu.

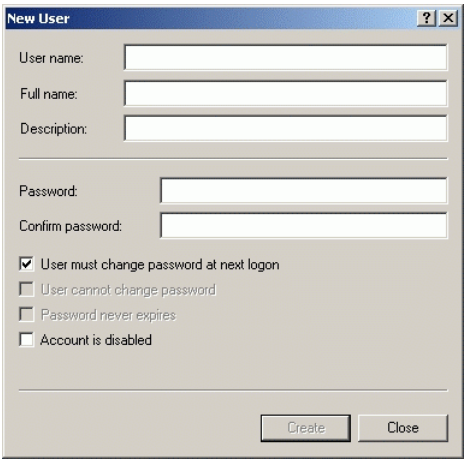

Figure 2. New User dialog: Local computer.

Fill out all the fields:

- **User Name** – The user name must be unique.
- **Full Name** - The Full Name field must be filled out and unique. We recommend using the user's actual full name, as this name will be shown in the audit trail and all the log reports. This is a requirement of 21 CFR 11.50a.
- **Description** – This field must also be filled out. We recommend entering the user's title as the description.

- **Password** – Enter and confirm a password for the user. Be sure to select the **User must change password at next logon** checkbox. This prevents the Windows system administrator from knowing the passwords of the users.

Note: If you select the **User must change password at next logon** checkbox, the user must actually log on to Windows and change their password before using Bio-Plex Manager Security Edition. Otherwise, Security Edition will not recognize the user.

To create a new group on a local computer:

Open the *Groups* folder and select **New Group** from the *Action* menu or right-click menu.

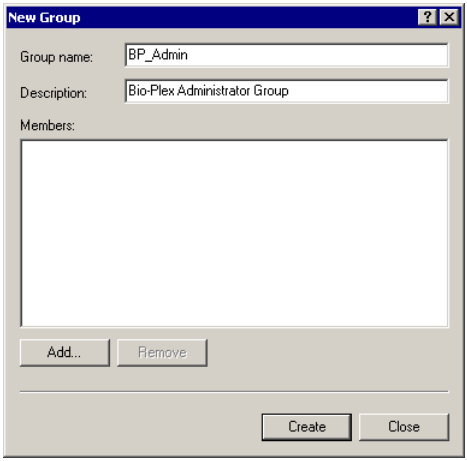

Figure 3. New Group dialog: Local computer.

In the *New Group* dialog **Group Name** field, enter one of the group names specified on page 4 (BP_Admin, BP_Supervisor, BP_Service, BP_Clinician_2, BP_Clinician_1, BP_Reviewer). You can also enter any description you want in the **Description** field.

The group does not need to have any special operating-system level privileges.

To add a user to a group on a local computer:

In the *New Group* dialog, click on the **Add** button. Alternatively, double-click on an existing group in the *Groups* folder to open its *Properties* dialog, and click on the **Add** button. The *Select Users* dialog will open.

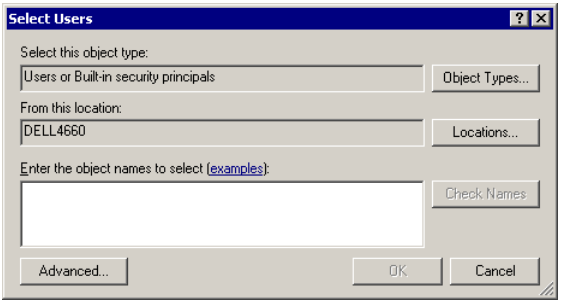

Figure 4. Select Users dialog: Local computer.

Click on the **Advanced** button to expand the dialog.

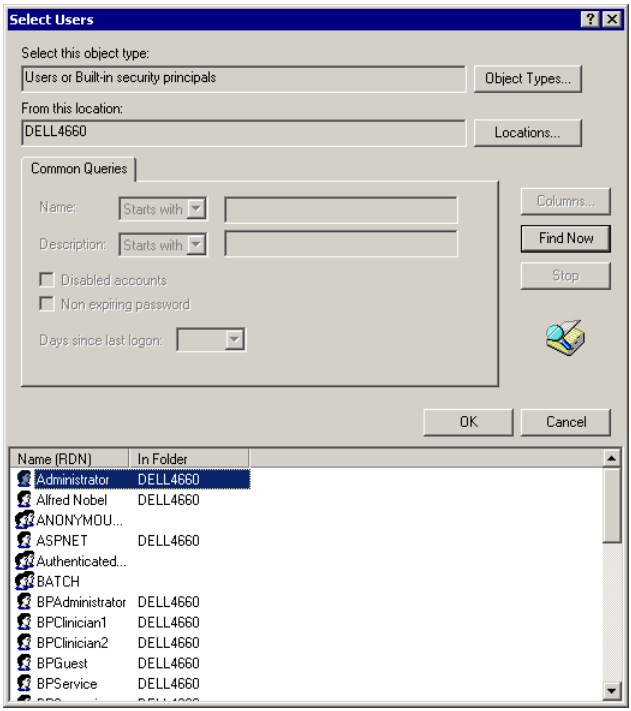

Figure 5. Select Users dialog, expanded: Local computer.

In the expanded dialog, click on **Find Now** to populate the bottom field with all the users on the local computer. Click on a user name in the list to select it, or hold down the Control key and click on multiple users to select them.

When you have selected all the users to add to the group, click on **OK**, and **OK** again to close the *Select Users* dialog.

Then click on **Create** to close the *New Group* dialog and create the group, or click on **OK** to close the existing group's *Properties* dialog and accept the changes.

Configuring Users and Groups on a Network Domain

Bio-Plex Manager Security Edition is supported on Windows NT Server and Windows 2000 Server.

Windows NT Server

To locate the users and groups on a Windows NT Server, go to **Administrative Tools** and select **User Manager for Domains**. This opens the *User Manager* dialog.

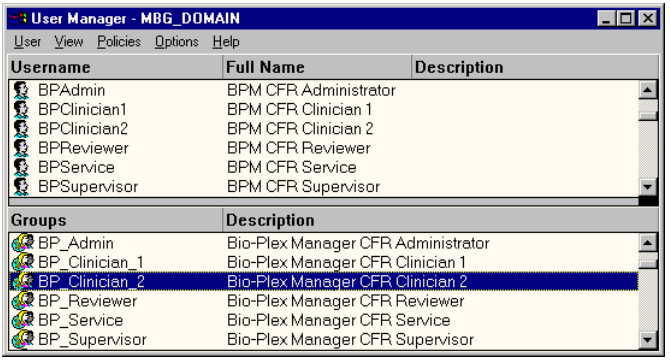

Figure 6. User Manager dialog: Windows NT Server.

In the dialog, the current users are listed in the top field and groups are listed below.

To create a new user on a Windows NT Server:

In the *User Manager* dialog, select **New User** from the *User* menu.

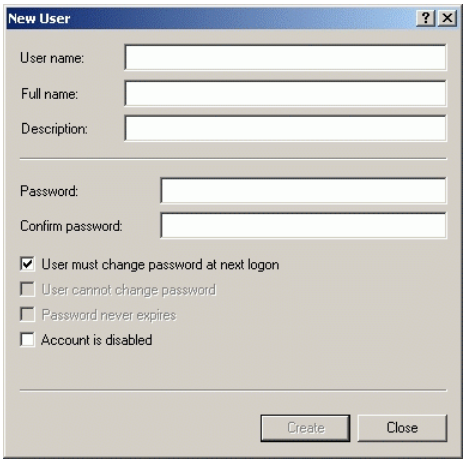

Figure 7. New User dialog: Windows NT Server.

Fill out all the fields:

- **User Name** – The user name must be unique.
- **Full Name** - The Full Name field must be filled out and unique. We recommend using the user's actual full name, as this name will be shown in the audit trail and all the log reports. This is a requirement of 21 CFR 11.50a.
- **Description** – This field must also be filled out. We recommend entering the user's title as the description.
- **Password** – Enter and confirm a password for the user. Be sure to select the **User must change password at next logon** checkbox. This prevents the Windows system administrator from knowing the passwords of the users.

Note: If you select the **User must change password at next logon** checkbox, the user must actually log on to Windows and change their password before using Bio-Plex Manager Security Edition. Otherwise, Security Edition will not recognize the user.

To create a new group on a Windows NT Server:

In the *User Manager* dialog, select **New Group** from the *User* menu or right-click menu.

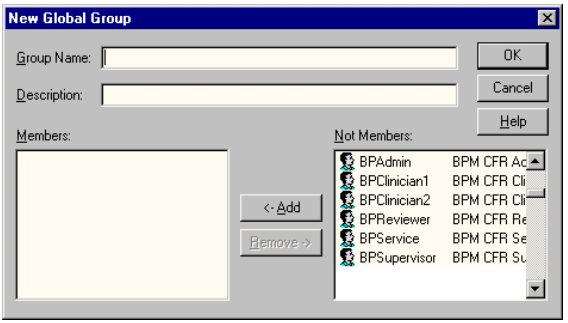

Figure 8. New Group dialog: Windows NT Server.

In the *New Group* dialog **Group Name** field, enter one of the group names specified on page 4 (BP_Admin, BP_Supervisor, BP_Service, BP_Clinician_2, BP_Clinician_1, BP_Reviewer). Be careful to type the name exactly as specified. You can also enter any description you want in the **Description** field.

The group does not need to have any special operating-system level privileges.

To add a user to a group on the Windows NT Server:

In the *New Group* dialog, click on the **Add** button. Alternatively, double-click on an existing group in the *User Manager* folder to open its *Properties* dialog, and click on the **Add** button. The *Select Users* dialog will open.

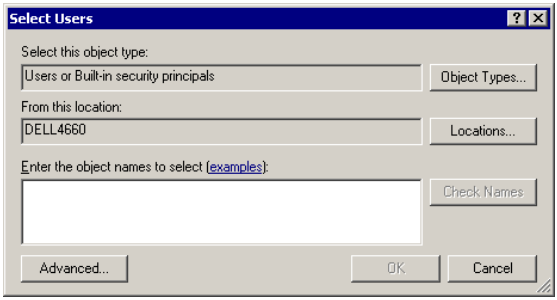

Figure 9. Select Users dialog: Windows NT Server.

Click on the **Advanced** button to expand the dialog.

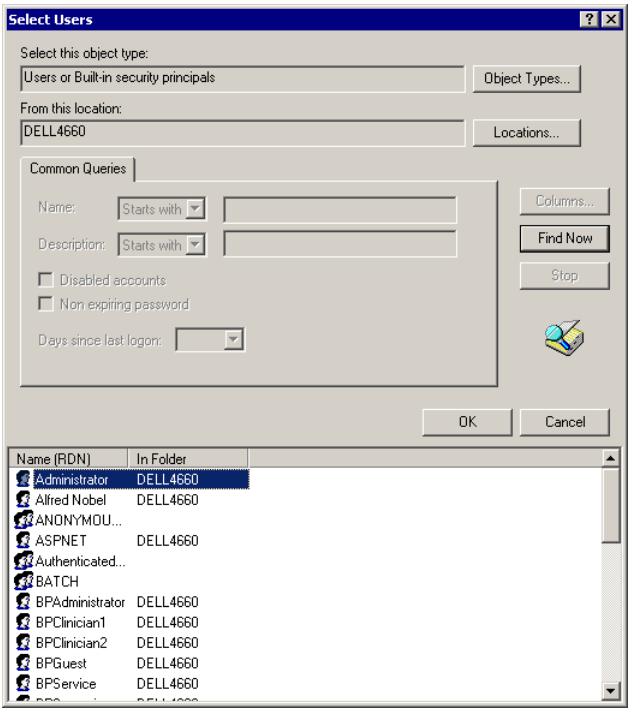

Figure 10. Select Users dialog, expanded: Windows NT Server.

In the expanded dialog, click on **Find Now** to populate the bottom field with all the users. Click on a user name in the list to select it, or hold down the Control key and click on multiple users to select them.

When you have selected all the users to add to the group, click on **OK**, and **OK** again to close the *Select Users* dialog.

Then click on **Create** to close the *New Group* dialog and create the group, or click on **OK** to close the existing group's *Properties* dialog and accept the changes.

Windows 2000 Server

To locate the users and groups on a Windows 2000 Server, go to **Administrative Tools** and select **Active Directory**.

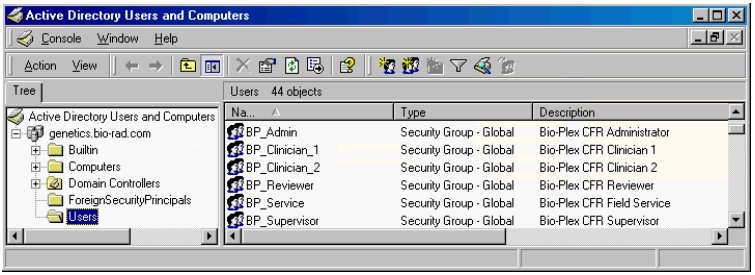

Figure 11. Active Directory window: Windows 2000 Server.

Note that in the *Active Directory* window, the *Users* folder lists groups as well.

To create a new user on a Windows 2000 Server:

With the *Users* folder open, select **New User** from the *Action* menu or right-click context menu.

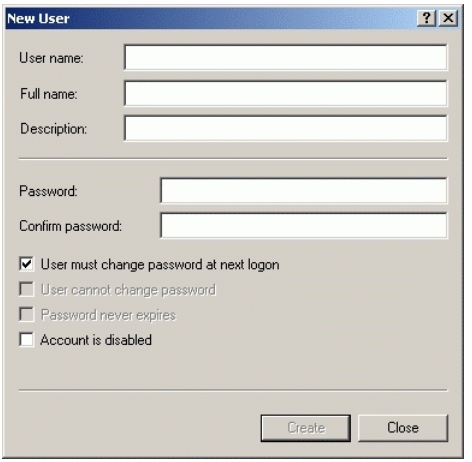

Figure 12. New User dialog: Windows 2000 Server.

Fill out all the fields:

- **User Name** – The user name must be unique.
- **Full Name** - The Full Name field must be filled out and unique. We recommend using the user's actual full name, as this name will be shown in the audit trail and all the log reports. This is a requirement of 21 CFR 11.50a.
- **Description** – This field must also be filled out. We recommend entering the user's title as the description.

- **Password** – Enter and confirm a password for the user. Be sure to select the **User must change password at next logon** checkbox. This prevents the Windows system administrator from knowing the passwords of the users.

Note: If you select the **User must change password at next logon** checkbox, the user must actually log on to Windows and change their password before using Bio-Plex Manager Security Edition. Otherwise, Security Edition will not recognize the user.

To create a new group on a Windows 2000 Server:

With the *Users* folder open, select **New Group** from the *Action* menu or right-click menu.

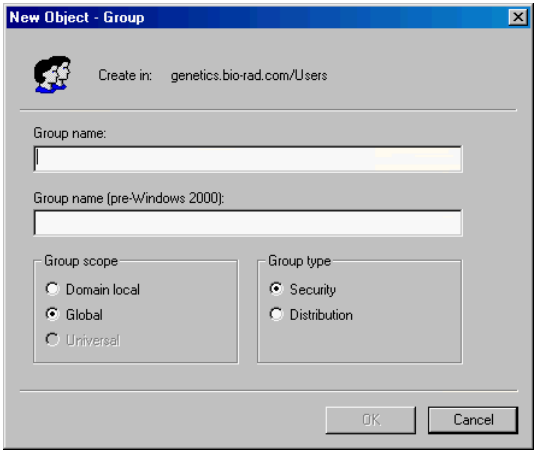

Figure 13. New Group dialog: Windows 2000 Server.

In the *New Group* dialog **Group Name** field, enter one of the group names specified on page 4 (BP_Admin, BP_Supervisor, BP_Service, BP_Clinician_2, BP_Clinician_1, BP_Reviewer). Be careful to type the name exactly as specified. You can also enter any description you want in the **Description** field.

The group does not need to have any special operating-system level privileges.

To add a user to a group on a Windows 2000 Server:

In the *New Group* dialog, click on the **Add** button. Alternatively, double-click on an existing group in the *User Manager* folder to open its *Properties* dialog, and click on the **Add** button. The *Select Users* dialog will open.

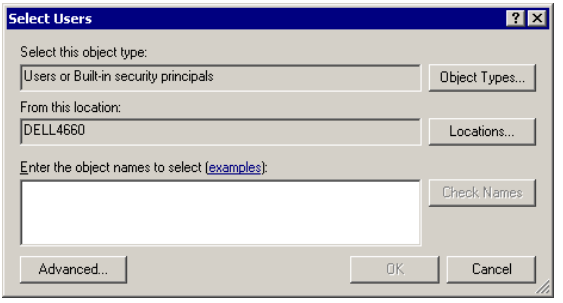

Figure 14. Select Users dialog: Windows 2000 Server.

Click on the **Advanced** button to expand the dialog.

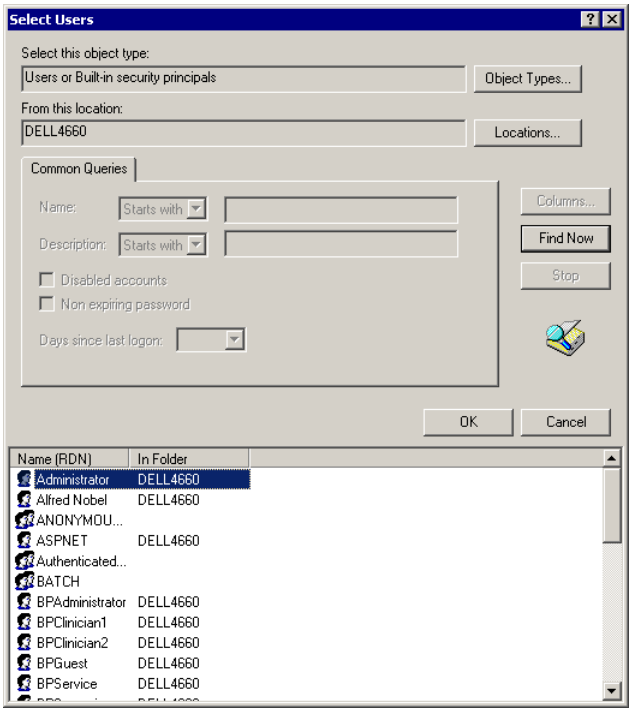

Figure 15. Select Users dialog, expanded: Windows 2000 Server.

In the expanded dialog, click on **Find Now** to populate the bottom field with all the users. Click on a user name in the list to select it, or hold down the Control key and click on multiple users to select them.

When you have selected all the users to add to the group, click on **OK**, and **OK** again to close the *Select Users* dialog.

Then click on **Create** to close the *New Group* dialog and create the group, or click on **OK** to close the existing group's *Properties* dialog and accept the changes.

Password Security

21 CFR 11.300 (b) requires that passwords be "periodically checked, recalled, or revised." The following password policies are therefore recommended, although the exact numbers are up the judgment of the system administrator/organization. For example, it is required that the maximum password age be set to enforce password changes, but the exact number of days between changes is flexible.

To locate the password policies on your local computer, go to the Windows **Control Panel** and select **Administrative Tools**, then select **Local Security Policy**.

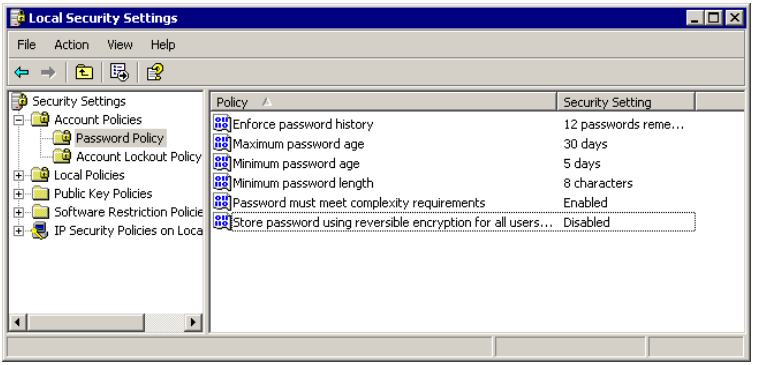

Figure 16. Local Security Settings window: Local computer.

To locate the password policies on your Windows NT Server, go to **Administrative Tools**, select **Administrative Tools**, and then select **Account Policy**.

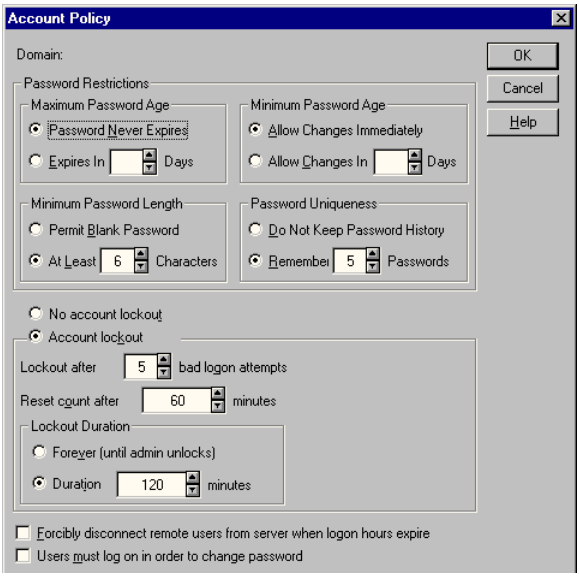

Figure 17. Account Policy dialog: Windows NT Server.

To locate the password policies on your Windows 2000 Server, go to **Administrative Tools**, and then select **Domain Controller Security Policy**.

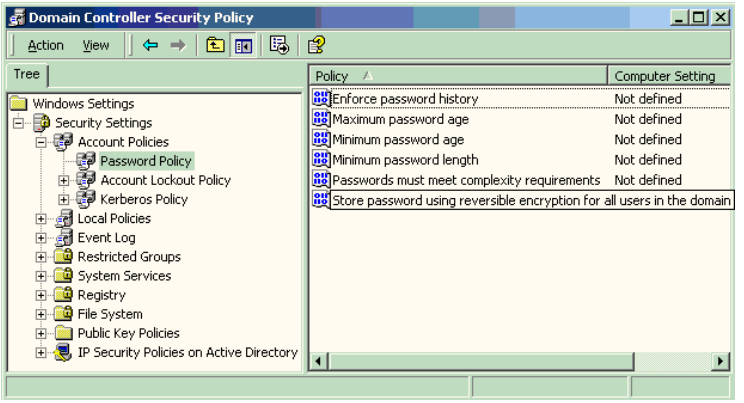

Figure 18. Domain Controller Security Policy window: Windows 2000 Server.

Password Policy:

- Enforce password history: 12 passwords remembered
- Minimum password age: 5 days
- Maximum password age: 30 days
- Minimum password length: 8 characters
- Password must meet complexity requirements: Enabled

Account Lockout Policy:

- Account lockout duration: 0 (The account is locked out until the administrator unlocks it.)
- Account lockout threshold: 3 logon attempts

Auditing Windows Event Logs

Some global auditing information is stored in the Windows Event Logs. It is a requirement of 21 CFR Part 11 that these logs be archived. However, by default, Windows systems automatically remove this data without warning. It is therefore critical that the event log be reconfigured to generate and preserve all necessary log data. Regular manual intervention is also required to preserve this data.

To open the **Event Properties Log**, go to **Administrative Tools** and click **Event Viewer.** Right-click on each log and select **Properties**. Select **Do Not Overwrite Events** and substantially increase the maximum size of the event log to cover any possible messages. The smaller the maximum size of the Event Log, the more often the manual process of viewing, archiving, and clearing the log must occur.

Auditing information generated by the operating system is recorded in the **Security Log**. Logon failures in Bio-Plex Manager Security Edition will be recorded in this log.

The Security Log should be reviewed, archived, and cleared periodically by the system administrator. During the review process, the log should be examined for attempted breaches of security, such as a series of failed logon attempts. To avoid the risk of losing data, the size should be very large and this inspection/archive process should occur daily.

The **Audit Policy** should be set as follows:

- Audit account logon events - Failure should be checked at a minimum.

- Audit account management - Both Success and Failure should be checked.

- Audit logon events - Failure should be checked at a minimum.

- Audit policy change - Both Success and Failure should be checked.

Misc. Security Measures

We recommend taking advantage of the built-in protections that Windows 2000 and XP Professional offer to protect the computer while the user is absent. It should be standard operating procedure for users to lock the computer when they step away by pressing Ctrl-Alt-Delete and then clicking on **Lock computer**. As a backup measure, we also recommend configuring the screen saver to require a password.

To configure the screen saver, open the Windows **Display** control panel and click the **Screen Saver** tab. Check the **Password Protected** checkbox. Note that this setting only applies to the current user and should be set for every user that logs onto the computer.

Note: Microsoft is continually updating its operating systems in response to security issues. **It is critical to keep all components of the Windows operating system, especially any domain controllers, up to date.**