Introduction

Effective August 20, 1997, the United States Food and Drug Administration released its Code of Federal Regulations (CFR) Title 21 Part 11: Electronic Records; Electronic Signatures (21 CFR Part 11). This regulation provides standards for data security and integrity, electronic record keeping and submissions, and electronic signatures.

The security model for The Discovery Series software is layered on top of the Windows security model, and a system not properly configured will not be secure and therefore will not be in compliance. This document provides guidelines for a system administrator to properly configure and maintain the Windows security environment for use with TDS.

Note: Bio-Rad makes no claim that The Discover Series software is CFR compliant in and of itself, nor does it guarantee compliance for the user. An organization must establish policies and procedures that work in conjunction with the tools provided in The Discovery Series software to ensure compliance with 21 CFR Part 11.

Setting up and maintaining system security requires the expertise of a system administrator. This document cannot be all-inclusive, as there may be differences in specific procedures depending on operating system version, local versus network domain account settings, or other differences

By their nature, certain procedures and policies are the responsibility of the software user. This document will identify these areas and make suggestions for policies and procedures.

Activating the CFR Module License

Before you can use a The Discovery Series application in CFR mode, you must first activate your license. Contact your local sales representative to confirm you have received the CFR module package. Please be ready to provide the system ID for which the license was purchased (this will be needed to generate the permanent license). Within 2–3 business days you should be able to activate the CFR module in your application.

To activate the CFR module, open an application. If the software license screen does not open, click Register from the Help menu. If you are connected to the Internet, click Check License. The application checks the license for the application itself. If the CFR license has been activated, a CFR authorization displays to indicate that your CFR license status has changed.

If you had requested to receive your CFR module password by e-mail or fax, you must enter the password manually. If you are not currently in the software license screen, click Register in the Help menu. Click Enter Password, and enter the password in the CFR Password field. With the correct password, the OK button next to the password field will change to green. Click Done. A CFR authorization displays to indicate that your CFR license status has changed.

After you have activated the CFR module and correctly configured your users and groups (see next section), go to the Security tab of the Preferences dialog box and select **Enable 21 CFR Part 11 mode**. See the application user guide or online help for further information.

Configuring Users and Groups

In order to comply with 21 CFR Part 11, user accounts must be correctly configured. To be correctly configured, user accounts must have a number of attributes set. Either new accounts can be used or existing accounts can be checked against the following requirements and updated as necessary.

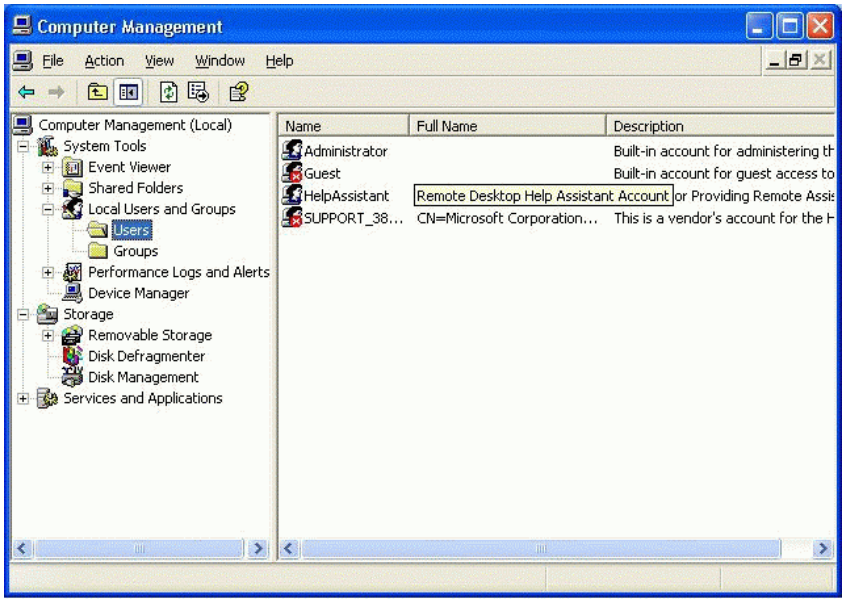
The following four groups must exist on the system. These groups can be located either locally or on a network domain.

- **TDS_Administrator** – These users have full privileges to the software and can make changes to the CFR preferences located on the Security tab of the Preferences dialog box
- **TDS_User** – These users have full privileges to the software
- **TDS_Tech** – These users have the same privileges as a user of the software in basic mode
- **TDS_Guest** – These users only have viewing privileges. No changes can be made to data or to the analysis of data

Users and groups are located in different places depending on whether The Discovery Series is installed on a local machine (single computer) or server (network).

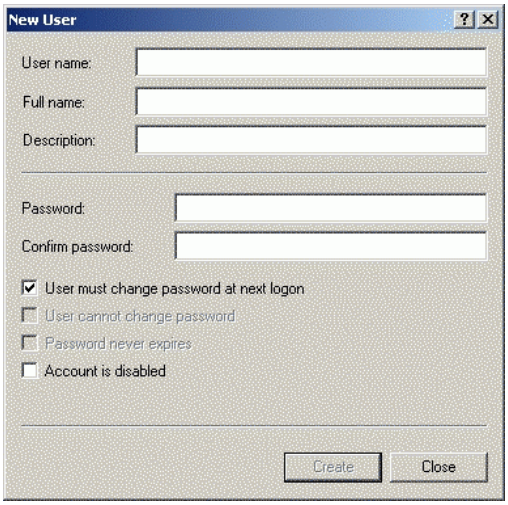
Configuring Users and Groups on a Local Computer

To find users and groups on a local computer (Windows 2000 or Windows XP operating system), go to Control Panel and select Administrative Tools, then select Computer Management.



Expand the Local Users and Groups folder. The Users folder lists the users, while the Groups folder lists the groups.

To create a new user, open the Users folder and click **New User** in the Action menu or right-click to open the context menu and click **New User**.



Fill in the fields, following these rules:

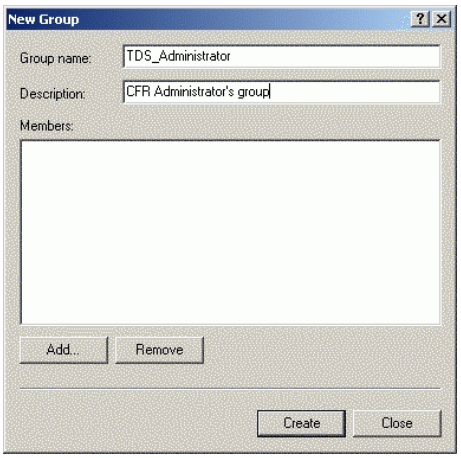
User name – The user name must be unique

Full name – The field is required and the full name must be unique. The Discovery Series will use this name for events logged in the audit report. The CFR (Part 11.50a) requires that the user's actual full name be used

Description – This field is also required. It is recommended that the user's job title be used as the description

Password – Enter and confirm a password for the user, and then check **User must change password at next logon**. This keeps the administrator from knowing the passwords of the users

To create a new group on a local computer, open the Groups folder and select **New Group** in the Action menu or in the right-click context menu.



The groups do not need to have any special operating system level privileges. However, each user who wants to use the software in CFR mode must belong to one of these groups. Each group has all of the rights of the group inferior to it, so it is not necessary to add a user to multiple groups. For example, a member of the TDS_User group does not have to be added to the TDS_Tech or TDS_Guest group.

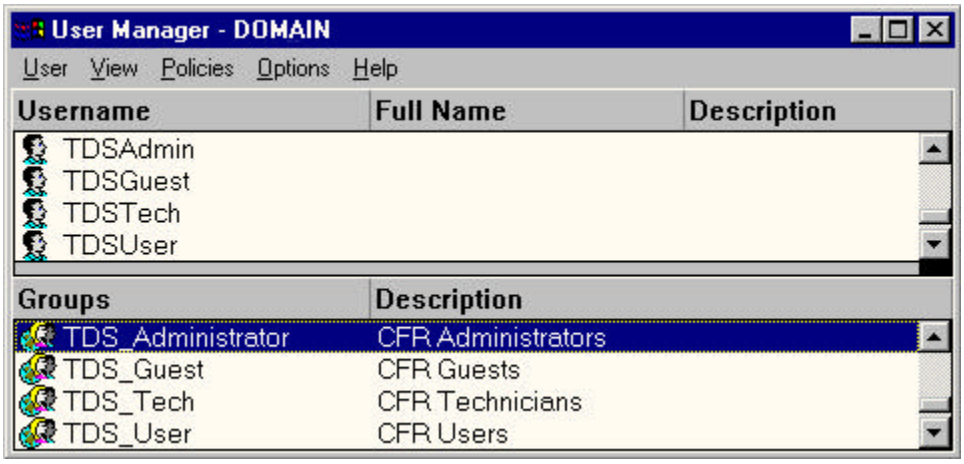
Note: A user in the CFR group must also belong to the Users, Power Users, or Administrators group.

Configuring Users and Groups on a Network Domain

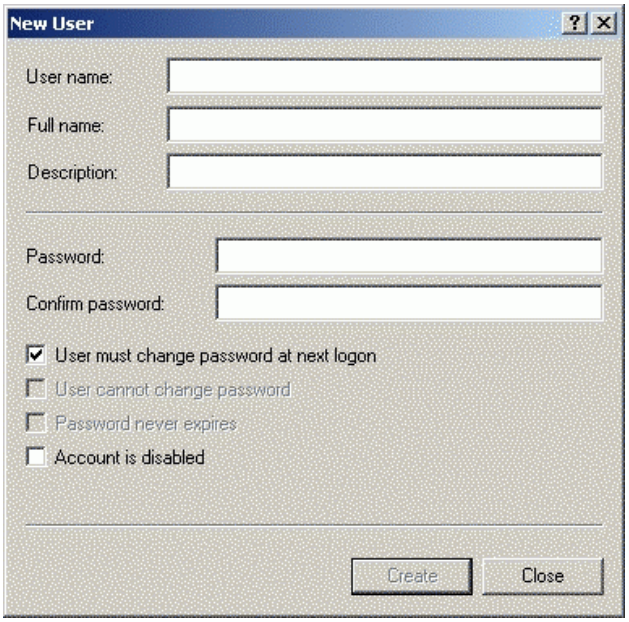
The CFR module is supported on Windows NT and Windows 2000 servers.

Windows NT Server

To find users on a Windows NT server, go to Administrative Tools and select User Manager for Domains. This opens the User Manager dialog box.



The User Manager lists current users in the top screen and the groups in the bottom screen. To create a new user, click New User in the User menu.



Fill in the fields, following these rules:

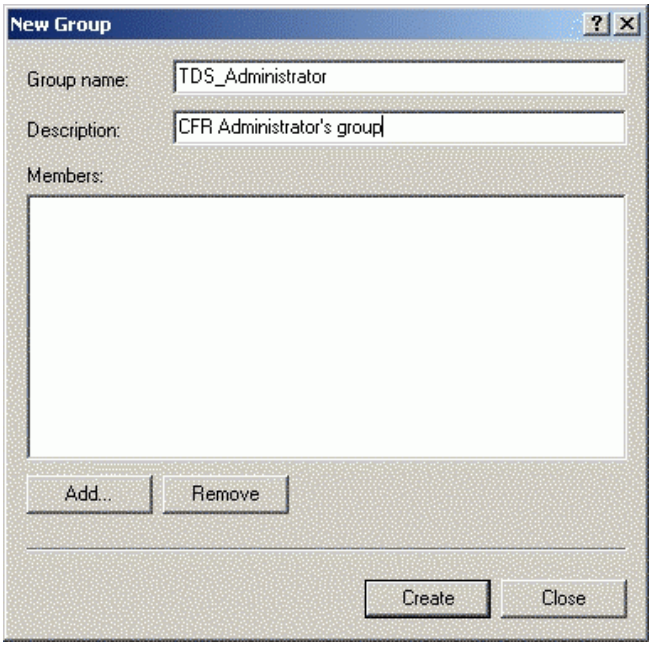
User name – The user name must be unique

Full name – The field is required and the full name must be unique. The Discovery Series will use this name for events logged in the audit report. The CFR (Part 11.50a) requires that the user's actual full name be used

Description – This field is also required. It is recommended that the user's job title be used as the description

Password – Enter and confirm a password for the user, and then check **User must change password at next logon**. This keeps the administrator from knowing the passwords of the users

To create a new group on the NT server, click **New Group** in the User menu or in the right-click context menu.

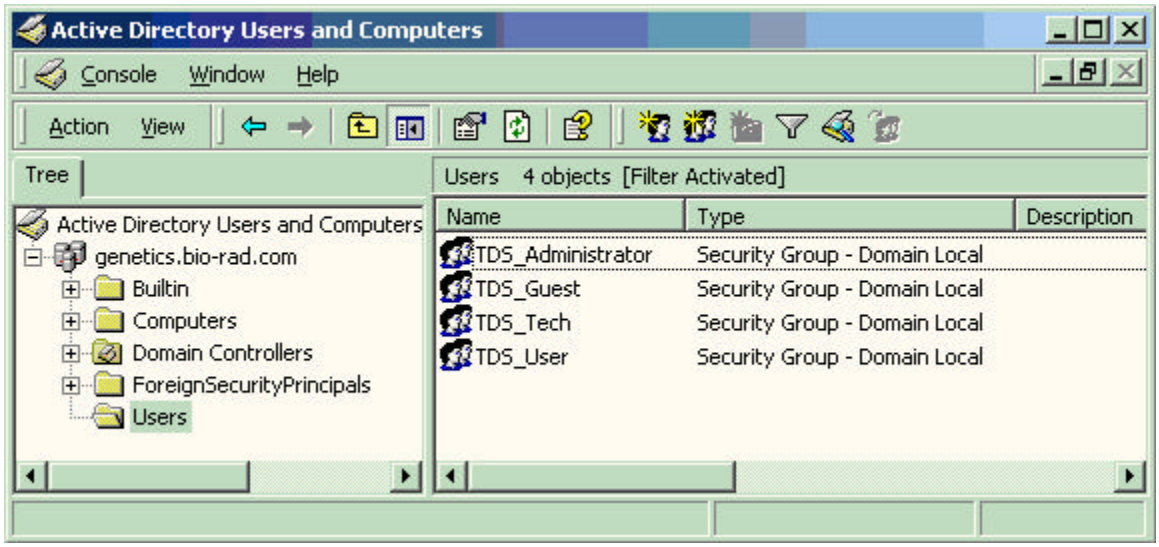


The groups do not need to have any special operating system level privileges. However, each user who wants to use the software in CFR mode must belong to one of these groups. Each group acquires all of the rights of the group inferior to it, so it is not necessary to add a user to multiple groups. For example, a member of the TDS_User group does not have to be added to the TDS_Tech or TDS_Guest group.

Note: A user in the CFR group must also belong to the Users, Power Users, or Administrators group.

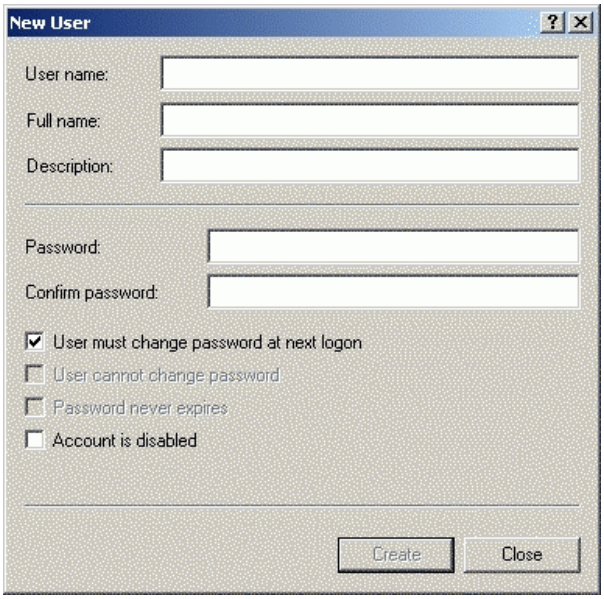
Windows 2000 Server

To locate users on a Windows 2000 server, go to Administrative Tools and select Active Directory.



Note that in the Active Directory, the Users folder lists Groups as well.

To create a new user, open the Users folder and click **New User** in the Action menu or right-click to open the context menu and click **New User**.



Fill in the fields, following these rules:

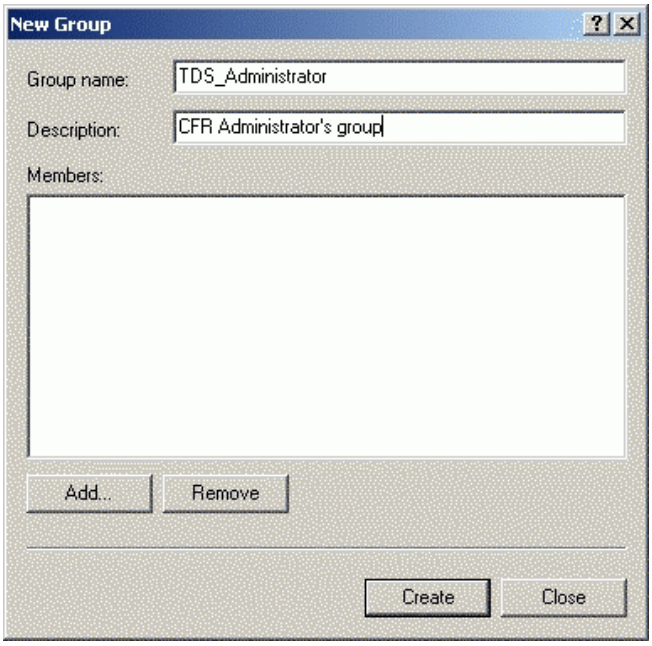
User name – The user name must be unique

Full name – The field is required and the full name must be unique. The Discovery Series will use this name for events logged in the audit report. The CFR (Part 11.50a) requires that the user's actual full name be used

Description – This field is also required. It is recommended that the user's job title be used as the description

Password – Enter and confirm a password for the user, and then check **User must change password at next logon**. This keeps the administrator from knowing the passwords of the users

To create a new group on a Windows 2000 server, select **New Group** in the Action menu or in the right-click context menu.



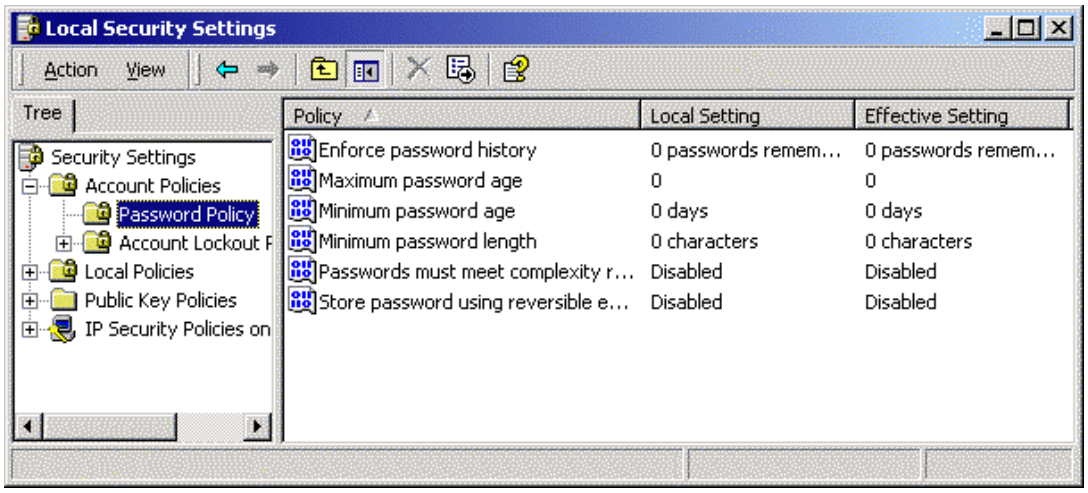
The groups do not need to have any special operating system level privileges. However, each user who wants to use the software in CFR mode must belong to one of these groups. Each group has all of the rights of the group inferior to it, so it is not necessary to add a user to multiple groups. For example, a member of the TDS_User group does not have to be added to the TDS_Tech or TDS_Guest group.

Note: A user in the CFR group must also belong to the Users, Power Users, or Administrators group.

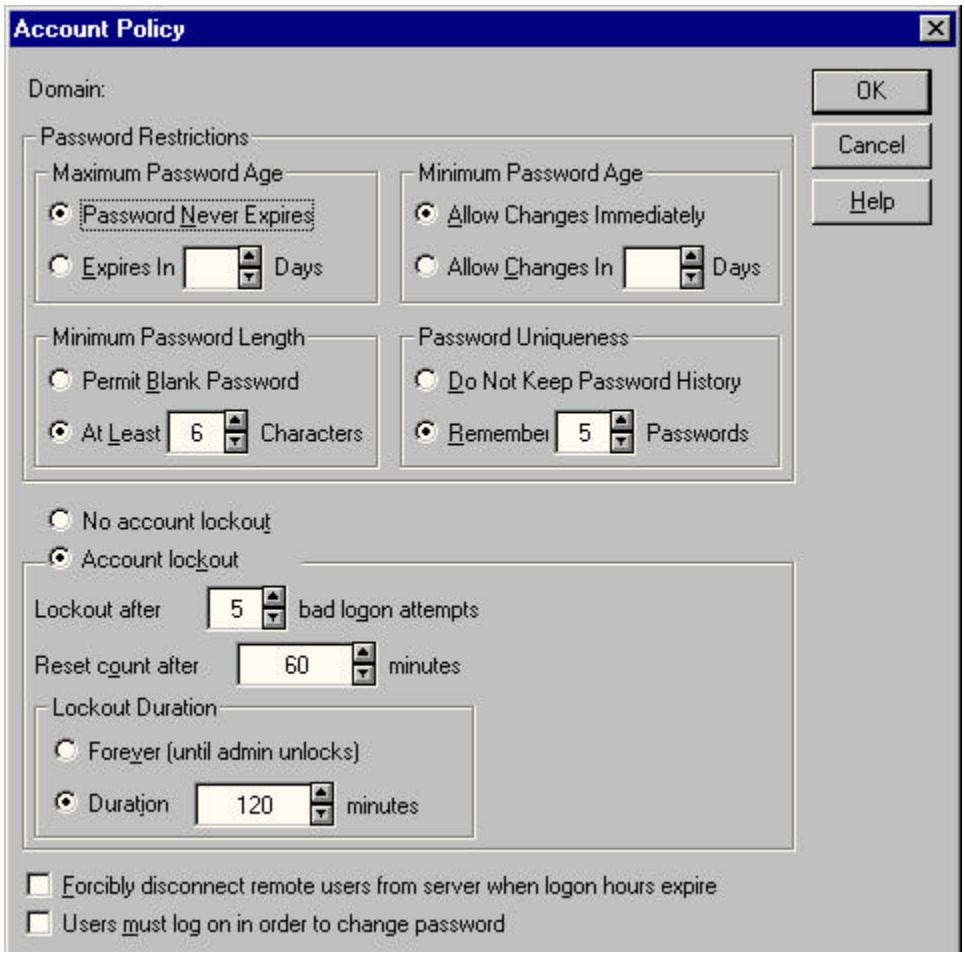
Password Security

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

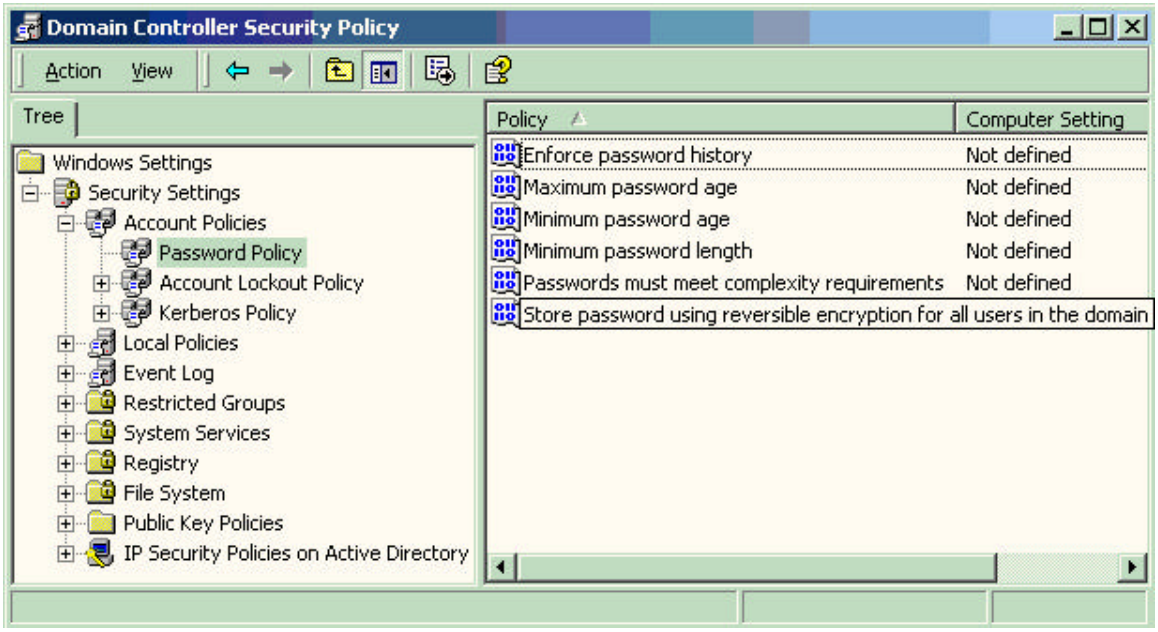
To locate the password policies on your local computer, go to Control Panel and select Administrative Tools, then select Local Security Policy.



To locate the password policies on a Windows NT server, go to Administrative Tools and select select **Account Policy**.



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



Recommended Settings

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. 21 CFR Part 11 requires that these logs be archived. However, by default Windows automatically removes these data without warning. It is therefore critical that the event logs be reconfigured to generate all necessary data, and that the events be logged. Regular manual intervention is required to preserve the data.

To open Event Properties, go to Administrative Tools and click **Event Viewer**. Right-click each log and click 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 log must be manually viewed, archived, and cleared.

Messages generated directly by the application are recorded in the **Application** log with the source set to the name of the product used. Auditing information generated by the operating system is recorded in the **Security** log. In particular, logon failures will be recorded in this log.

Both logs must be reviewed, archived, and cleared periodically by the system administrator. During the review process, the logs should be examined for attempted security breaches such as a series of failed logon attempts. To avoid the risk of losing data, the size should be very large and this inspection/archiving 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

Miscellaneous Security Measures

Although the software does have a lockout capability – after a set number of minutes of inactivity, the password must be reentered – it is advisable to take advantage of the Windows system features that protect the computer while the user is absent. Users should routinely lock the computer when they leave, by pressing Ctrl-Alt-Delete and then clicking **Lock computer**. However, as an added measure against forgetfulness the screen saver should be configured to require a password for reentry.

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

After setting up the CFR mode in the file system, to ensure that a user cannot change CFR settings by manipulating the preference files on the hard disk, protect the files **cfr_oned.cfg** and **cfr_pdquest.cfg** so that only administrators can write to them. See your Windows documentation for information on how to protect files.

Note: Microsoft is continually updating their operating systems to address security issues. It is critical to keep all computers running the Windows operating system up to date, especially any domain controllers.