Xcalibur®

Administrator's Guide:
Configuring Xcalibur Software for Compliance with 21 CFR Part 11

XCALI-97108 Revision D April 2007

Analyze • Detect • Measure • Control™

Thermo SCIENTIFIC

Revision D in April 2007.
Xcalibur 2.0.6

Thermo
ELECTRON CORPORATION

WEEE Compliance

This product is required to comply with the European Union's Waste Electrical & Electronic Equipment (WEEE) Directive 2002/96/EC. It is marked with the following symbol:

Thermo Electron has contracted with one or more recycling/disposal companies in each EU Member State, and this product should be disposed of or recycled through them. Further information on Thermo Electron's compliance with these Directives, the recyclers in your country, and information on Thermo Electron products which may assist the detection of substances subject to the RoHS Directive are available at www.thermo.com/WEEERoHS.

WEEE Konformität

Dieses Produkt muss die EU Waste Electrical & Electronic Equipment (WEEE) Richtlinie 2002/96/EC erfüllen. Das Produkt ist durch folgendes Symbol gekennzeichnet:

Thermo Electron hat Vereinbarungen mit Verwertungs-/Entsorgungsfirmen in allen EU-Mitgliedsstaaten getroffen, damit dieses Produkt durch diese Firmen wiederverwertet oder entsorgt werden kann. Mehr Information über die Einhaltung dieser Anweisungen durch Thermo Electron, über die Verwerter, und weitere Hinweise, die nützlich sind, um die Produkte zu identifizieren, die unter diese RoHS Anweisung fallen, finden sie unter www.thermo.com/WEEERoHS.

Thermo
ELECTRON CORPORATION

Conformité DEEE

Ce produit doit être conforme à la directive européenne (2002/96/EC) des Déchets d'Equipements Electriques et Electroniques (DEEE). Il est marqué par le symbole suivant:

Thermo Electron s'est associé avec une ou plusieurs compagnies de recyclage dans chaque état membre de l'union européenne et ce produit devrait être collecté ou recyclé par celles-ci. Davantage d'informations sur la conformité de Thermo Electron à ces directives, les recycleurs dans votre pays et les informations sur les produits Thermo Electron qui peuvent aider la détection des substances sujettes à la directive RoHS sont disponibles sur www.thermo.com/WEEERoHS.

Contents

Preface

About This Guide

Welcome to Xcalibur®! Xcalibur is the Thermo Scientific mass spectrometry data system.

Related Documentation

In addition to this guide, Thermo Scientific provides the following documents for Xcalibur:

- *Getting Productive: Processing Setup and the Analysis of Quantitation Data*
- *Getting Productive: Quantitative Analysis*
- *Getting Productive: Qualitative Analysis*
- *Getting Productive: Designing and Generating Custom Reports with XReport*
- *Getting Productive: Creating and Searching Libraries*
- Help available from within the software

Safety and Special Notices

Make sure you follow the precautionary statements presented in this guide. The safety and other special notices appear in boxes.

Safety and special notices include the following:

CAUTION Highlights hazards to humans, property, or the environment. Each CAUTION notice is accompanied by an appropriate CAUTION symbol.

IMPORTANT Highlights information necessary to avoid damage to software, loss of data, invalid test results, or information critical for optimal performance of the system.

Note Highlights information of general interest.

Tip Helpful information that can make a task easier.

Contacting Us

There are several ways to contact Thermo Scientific.

Assistance

For new product updates, technical support, and ordering information, contact us in one of the following ways:

Visit Us on the Web

www.thermo.com/finnigan

Contact Technical Support

Phone: 1-800-685-9535
Fax: 1-561-688-8736
E-mail: techsupport.finnigan@thermofisher.com

Find software updates and utilities to download at
http://mssupport.thermo.com

Contact Customer Service

In the US and Canada for ordering information:
Phone: 1-800-532-4752
Fax: 1-561-688-8731
Web site: www.thermo.com/finnigan

Changes to the Manual and Online Help

To suggest changes to this guide or to the online Help, use either of the following methods:

- Fill out a reader survey online at www.thermo.com/lcms-techpubs
- Send an e-mail message to the Technical Publications Editor at techpubs.finnigan-lcms@thermofisher.com

Chapter 1 Introduction

Xcalibur®is the Thermo Scientific mass spectrometry data system. This Administrator's Guide discusses how to configure specific Xcalibur software applications to help an organization become compliant with the Electronic Records and Electronic Signatures Rule, published by the United States Food and Drug Administration as 21 CFR Part 11.[1]

It must be stressed that compliance with 21 CFR Part 11 requires both technical and procedural compliance. To achieve technical compliance, the organization must use software that contains the required security features and functions. To achieve procedural compliance, the organization must establish standard operating procedures and policies that define how to use processes and systems in a compliant manner.

This chapter contains the following sections:

[1]Code of Federal Regulations, Title 21, Food and Drugs, Part 11 "Electronic Records: Electronic Signature Final Rule", Federal Register 62 (54) 1997, 13429-13466. The final rule is also available electronically at http://www.fda.gov/ora/compliance_ref/part11/.

Major Requirements of 21 CFR Part 11

In August 1997, the United States Food and Drug Administration published a rule for electronic records and electronic signatures under the current good manufacturing practice (cGMP) regulations in the Code of Federal Regulations (21 CFR Part 11). The rule provides criteria under which electronic records and electronic signatures can be considered equivalent to paper records and handwritten signatures. It also permits the widest possible use of electronic technology.

An important implication in 21 CFR Part 11 is that organizations must implement rules to confirm that proper methods, procedures, and controls are in place. Therefore, certain issues must be addressed, such as the following:

- Prevention of Data Falsification
- Data Reconstruction
- System Security

Prevention of Data Falsification

Electronic data can be falsified in several ways: it can be modified directly; it can be modified indirectly by deleting records; or it can be modified indirectly by using readily available tools.

To prevent falsification, a number of controls must be implemented. These controls can be procedural in nature or can be functionally implemented within the system generating the electronic records. Normally, a system combines both methods to achieve compliance.

To help prevent data falsification, Xcalibur software (designed for compliance with 21 CFR Part 11) uses audit trails and system security.

Data Reconstruction

Although it is important to demonstrate that data has not been falsified, it is just as important to show how it has been generated. Raw data cannot be reconstructed; however, it is possible to regenerate all other records derived from the original raw data files.

An efficient and comprehensive audit trail can confirm that all electronic records generated from the raw data can be regenerated. To do this, audit trail entries must be made for all events and actions that are required to regenerate the records. In addition, new audit trail entries must be added only to existing records; they must not overwrite or obstruct other records. Finally, the user must not have any control on the audit trail records or be able to modify the configuration of the audit trail. The audit trails created by Xcalibur software meet these requirements.

System Security

Most organizations implement strict security procedures for their computer networks to prevent unauthorized access to data. In this context, unauthorized access means:

- Access by an individual (external or internal to the organization) who has not been granted the authority to use, manipulate, or interact with the system.
- Access through the use of the identity of another individual, for example, by using a colleague's username and password.

The 21 CFR Part 11 rule defines a number of controls to confirm that the systems that generate electronic records can be accessed only by individuals who have some level of responsibility towards those records. The rule includes both procedural controls and functionality controls.

Xcalibur software (designed for compliance with 21 CFR Part 11) implements some of these controls directly and relies on the security functions in the Microsoft®Windows®XP Professional operating system for other parts.

For example:

- The Finnigan Security Server controls secure file operations.
- The administrator restricts user access through the Xcalibur Authorization Manager (a Thermo Fisher-supplied administrative tool).
- The administrator controls software feature access through the Xcalibur Authorization Manager.
- Windows XP Professional security functions manage user authentication.
- The Windows XP Professional security functions and, in particular, the NTFS permission rights maintain electronic record security.

Xcalibur Software and Compliance with 21 CFR Part 11

Xcalibur incorporates security features and functions to enable Xcalibur software applications to comply with 21 CFR Part 11. It is crucial that the laboratory administrator configures the software properly to fully implement these security features.

This section contains the following topics:

- Configuring Software Applications
- Security Features Within the Software

Configuring Software Applications

Configuring Xcalibur software applications for compliance with 21 CFR Part 11 involves three steps as follows:

- Configuring the Auditing Database
- Protecting Records
- Setting Up User Access Controls

Configuring the Auditing Database

The auditing database is critical in enabling Xcalibur applications to comply with 21 CFR Part 11. The database confirms that data cannot be deleted or altered without a record being kept, and keeps an audit log of parameter changes made in Xcalibur applications.

See **Chapter 2: Using the Database Configuration Manager** for the procedure for configuring the auditing database.

Protecting Records

To establish secure file operations, the laboratory administrator must grant access permissions for specific folders, files, and registry keys. The permissions must be set so that only an administrator can delete or alter security related records, such as the Authorization Manager and Database Configuration settings. These settings ensure that unauthorized users cannot alter the security settings for Xcalibur applications.

See **Chapter 3: Establishing Secure File Operations** **for** the procedure for creating protected folders, files, and registry keys.

Setting Up User Access Controls

To control user access, the laboratory administrator must define secure user groups and grant access permissions for each group. The administrator can restrict defined groups of users from performing various functions within the application software. This restriction can range from complete

prohibition, through several levels of password-required access, to no restrictions. User access controls are set through the Xcalibur Authorization Manager.

After the security settings are defined for at least one group, users who are not in a secure group are denied access to the application. However, when no secure groups are defined, all features of the software are accessible by all users!

See **Chapter 4: Defining Secure User Groups and Adding Users** for the procedure for defining user groups and granting access permissions.

Security Features Within the Software

After the appropriate file protections and user access controls are in place, Xcalibur applications use a number of built-in features to confirm the security of the data and to meet 21 CFR Part 11 requirements.

Xcalibur includes a file tracking system that maintains a database of the files created in or used by Xcalibur applications. The file tracking system uses the file journaling features of the Windows XP operating system, recording all changes or deletions made to files stored in the database, even if the changes are made using a non-Xcalibur application such as Windows Explorer.

A comprehensive audit trail confirms that all electronic records generated from the raw data can be regenerated. The audit trail consists of two parts: the history log and the event log. The history log contains information about every parameter change that a user has made within the application. The event log contains information about all of the events that have occurred within the application, such as the creation of a sequence or the saving of a file.

Use the CRC Validator to perform Cyclic Redundancy Checks (CRCs) to protect against malicious changes to data files. A CRC can detect file corruption and attempted changes to data files outside of Xcalibur applications. The CRC calculates checksums for sets of data using mathematical formulas and stores the value in auditing database. When data are modified or processed within the application, new checksums are calculated and stored. The stored checksums can be compared with checksums calculated from the files stored on the disk using the CRC Validator application. A mismatch between the stored and computed checksums might indicate file corruption or tampering.

How to Use This Administrator's Guide

Read this Administrator's Guide carefully and complete the procedures that are outlined in Table 1 and described in detail in the following chapters. If you do not perform certain tasks, the software application might not be fully compliant with 21 CFR Part 11.

This guide provides the following information:

- How to configure the auditing database
- How to establish secure file operations
- How to define secure user groups and add users

The following checklist summarizes the major tasks that the laboratory administrator must carry out to configure Xcalibur software applications for compliance with 21 CFR Part 11.

Table 1. Checklist of tasks for configuring Xcalibur software applications for compliance with 21 CFR Part 11

Task	See Topic	Completed?
Install the latest version of Xcalibur core software.		
Install the layered software applications.		
If necessary, install the Oracle client and server software on the appropriate workstations. (Only when Oracle is used for the auditing database.)	Appendix A, "Installing an Oracle Database"	
Configure the auditing database.	"Using the Database Configuration Manager" on page 7	
Confirm that the Finnigan Security Server is set up properly and is running.	"Confirming the Properties of System Services" on page 22	
Restrict access to the folder that contain security files.	"Configuring the Security Settings for the Security Folder" on page 28	
Restrict access to the registry key for the auditing database.	"Configuring Security Settings for the Database Registry Key" on page 39	
Decide how many and what type of user groups you need.	"Planning User Groups" on page 46	
Define user groups in the Authorization Manager.	"Defining User Groups" on page 48	
Set permission levels for software features for each user group.	"Setting Permissions" on page 51	
Save the configuration settings.	"Saving the Security Settings" on page 56	

Chapter 2 Using the Database Configuration Manager

This chapter describes how to use the Database Configuration Manager to configure your compliance database. The compliance database keeps a record of auditable events and changes made to files created by or managed by Xcalibur. Until you run the Database Configuration manager, all applications run without auditing, and the system is not 21 CFR Part 11 compliant.

Use the Database Configuration manager to configure either a Microsoft Access database on your local computer or an Oracle database on a remote computer. To use an Oracle database, confirm that the following tasks have been completed:

- An Oracle database has been installed on an accessible remote server. See **Appendix A** or consult your Oracle database administrator for more information.
- The Oracle client software has been installed on your local computer. See **Appendix A** or consult your Oracle database administrator for more information.
- Make sure that you know the User Name, Password, and Oracle Net Service Name of your Oracle database. Obtain this information from your Oracle database administrator.

Note Confirm that no other Xcalibur applications are running when running the Database Configuration manager. Auditing of Xcalibur applications cannot take place while the Database Configuration manager is running.

To use to Database Configuration manager to configure your auditing database

1. From the Windows taskbar, choose **Start > All Programs > Xcalibur > Database Configuration**. The Auditing Database Configuration Manager dialog box appears (see Figure 1).

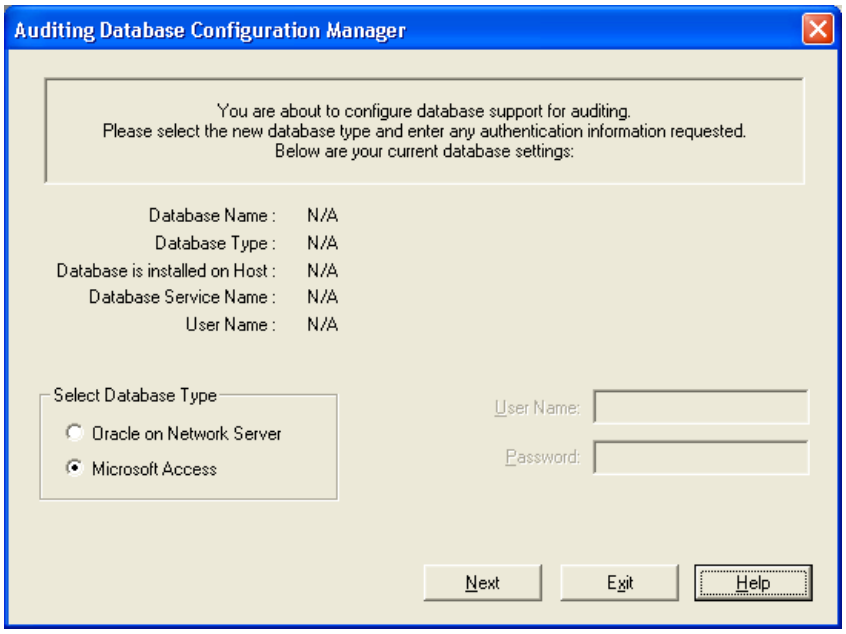

Figure 1. Auditing Database Configuration Manager dialog box

2. Select the database type in the Select Database Type area:

   - When using a Microsoft Access database, select the Microsoft Access option and go on to **step 4**.
   - When using an Oracle database, select the Oracle on Network Server option and go on to **step 3**.

3. When using an Oracle database, specify the Oracle database parameters:

   a. Enter the database user name in the User Name box.

   b. Enter the database password in the Password box.

   c. Select the Oracle Net Service Name for your database in the Oracle Net Service Name list.

   IMPORTANT Be sure to use the Oracle user name and password provided by your Oracle database administrator.

4. Click **Next**. The DatabaseConfigManager dialog box appears (see Figure 2).

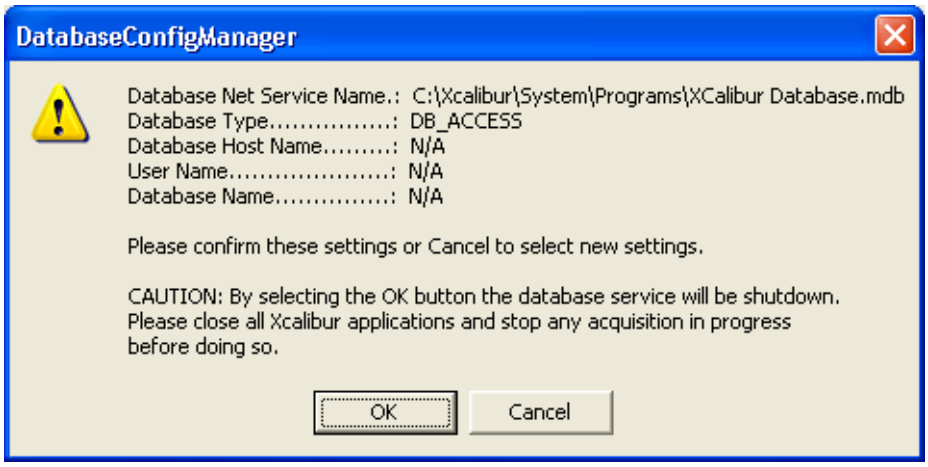

Figure 2. DatabaseConfigManager dialog box

5. Confirm that the settings are correct and click **OK**.

6. The appearance of the Auditing Database Configuration Manager dialog box should be similar to that shown in Figure 3.

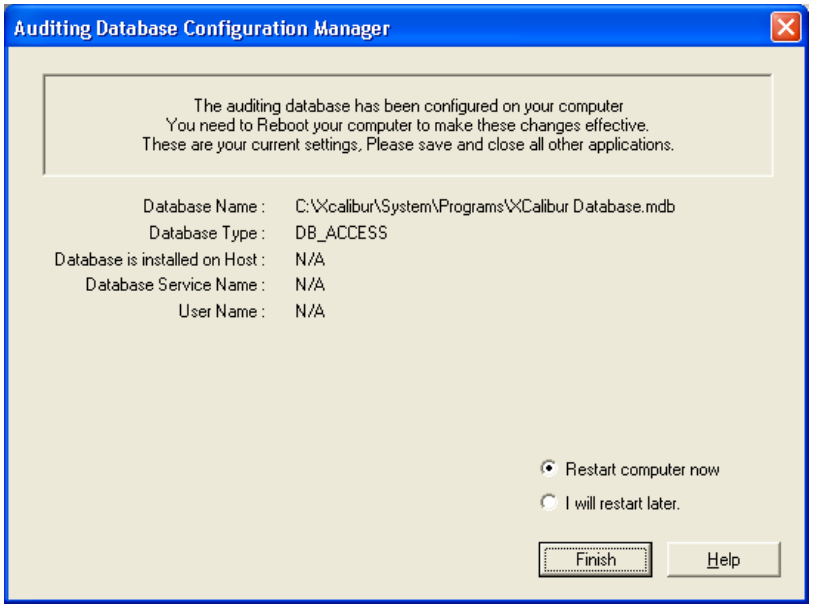

Figure 3. Auditing Database Configuration Manager dialog box, showing restart settings

Click a restart option:

- Click the **Restart Computer Now** option to have the computer restart automatically once you click **Finish**.
- Click the **I Will Restart Later** option to restart the computer manually at a later time.

IMPORTANT The changes you make in the Database Manager do not take effect until you restart the computer.

7. Click **Finish** to save your settings and close the Auditing Database Configuration Manager dialog box.

Chapter 3 Establishing Secure File Operations

The 21 CFR Part 11 rule requires that previously recorded information cannot be obscured by record changes. It also requires that records be protected to enable their accurate and ready retrieval. To comply with these requirements, standard operating procedures must be established for precise and systematic record archiving.

This chapter describes required operating system security settings to configure to confirm that the auditing database, authorization manager, and other security features of Xcalibur operate correctly.

This chapter contains the following sections:

Applying the Security Template

The Security Template is a preconfigured set of security and permission settings for a Windows XP computer. Applying the Security Template to a Windows XP computer changes the status of normal users to enhanced users so that they can access the registry and run Xcalibur. Without the Security Template, all normal users would be unable to run Xcalibur.

We recommend applying this Security Template to all Windows XP computers in a 21 CFR Part 11-compliant environment.

To apply the Security Template to a Windows XP computer

1. Log on to the computer as an Administrator.

2. From the Windows XP taskbar, choose **Start > Run**. The **Windows Run** dialog box appears (see Figure 4).

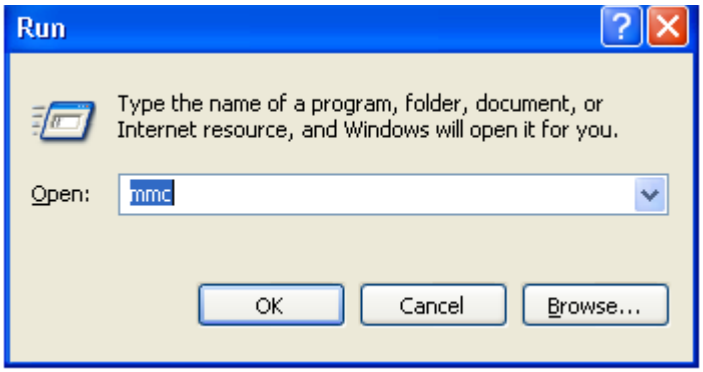

Figure 4. Windows Run dialog box

3. Type “mmc”, and click **OK**. The **Windows Console** menu appears (see Figure 5).

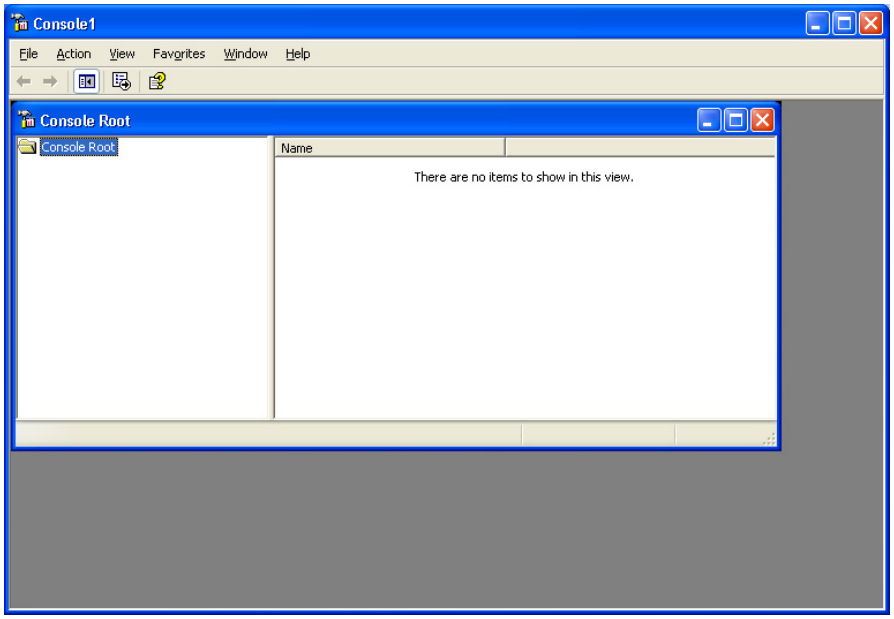

Figure 5. Windows Console menu

4. Choose **File > Add/Remove Snap-In**. The **Add/Remove Snap-in** window appears (see Figure 6).

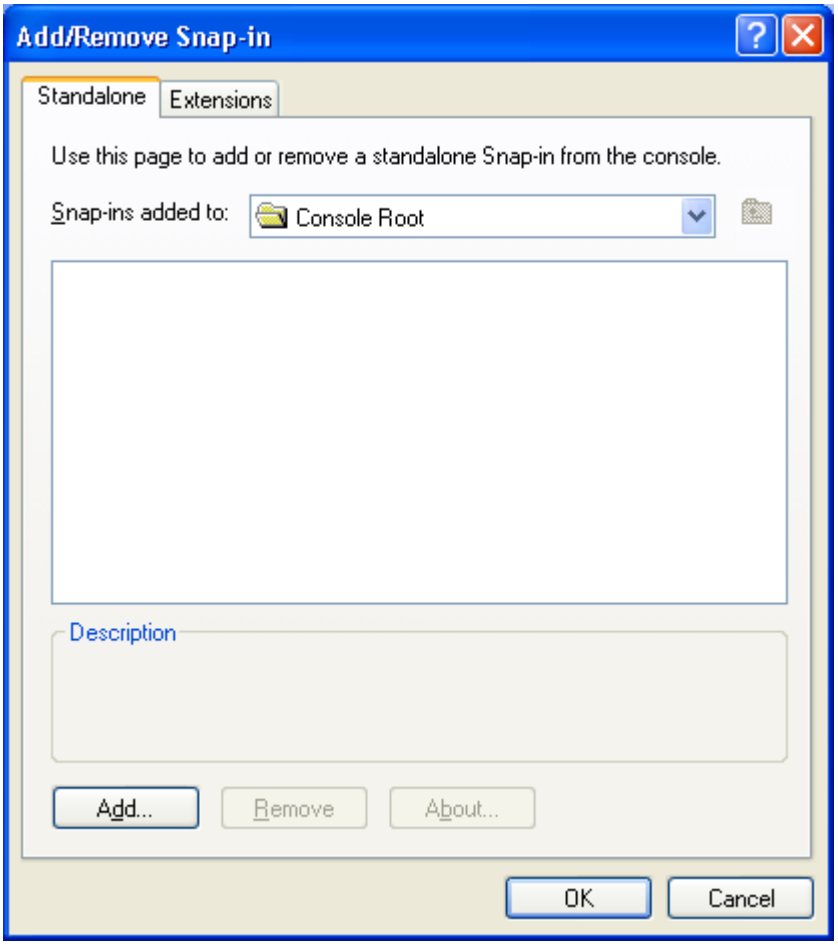

Figure 6. Add/Remove Snap-In window

5. Click **Add**. The **Add Standalone Snap-in** window appears (see Figure 7).

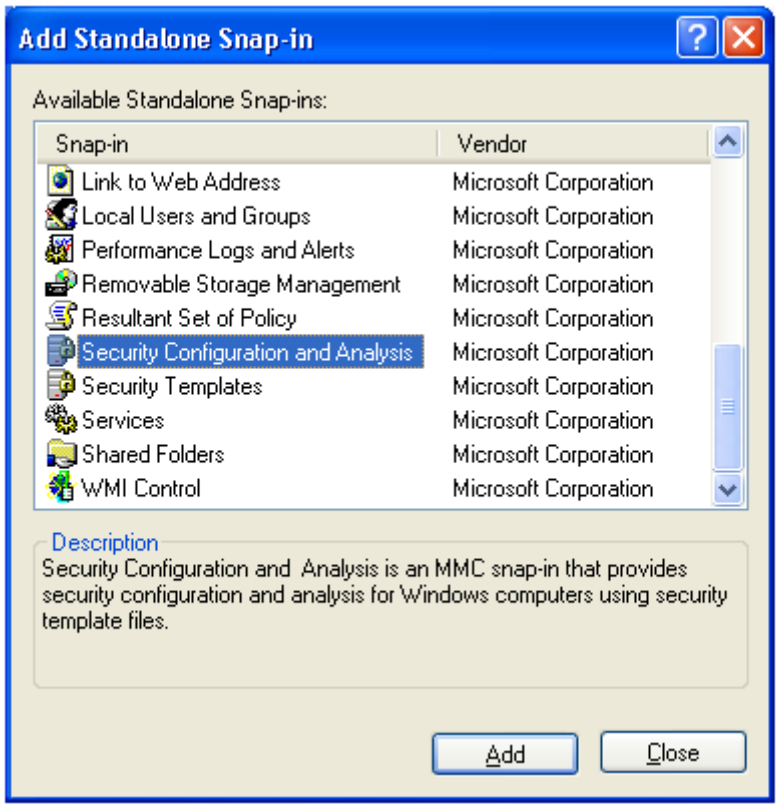

Figure 7. Add Standalone Snap-In window

6. Choose the **Security Configuration and Analysis** option in the scroll menu (see Figure 7).

7. Click **Add** and click **Close** to close the **Add Standalone Snap-in** dialog box. The **Add/Remove Snap-in** window appears, with **Security Configuration and Analysis** in the console window (see Figure 8).

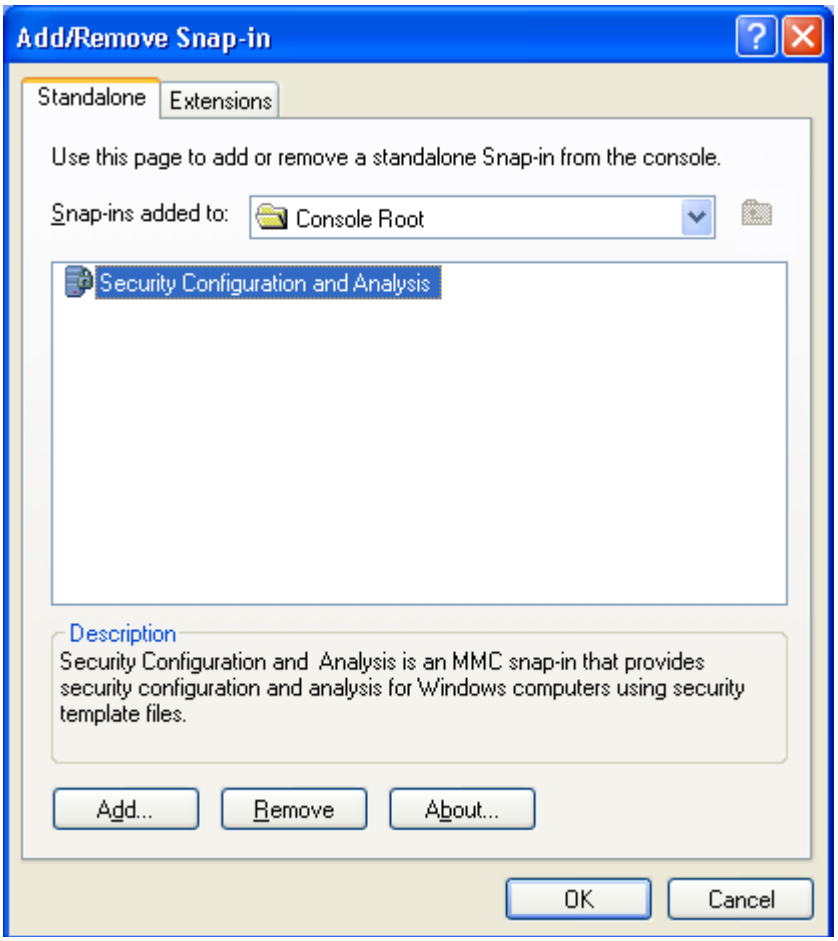

Figure 8. Add/Remove Snap-In window, with Security Configuration and Analysis option

8. Click **OK** to return to the **Console Root** window (see Figure 9).

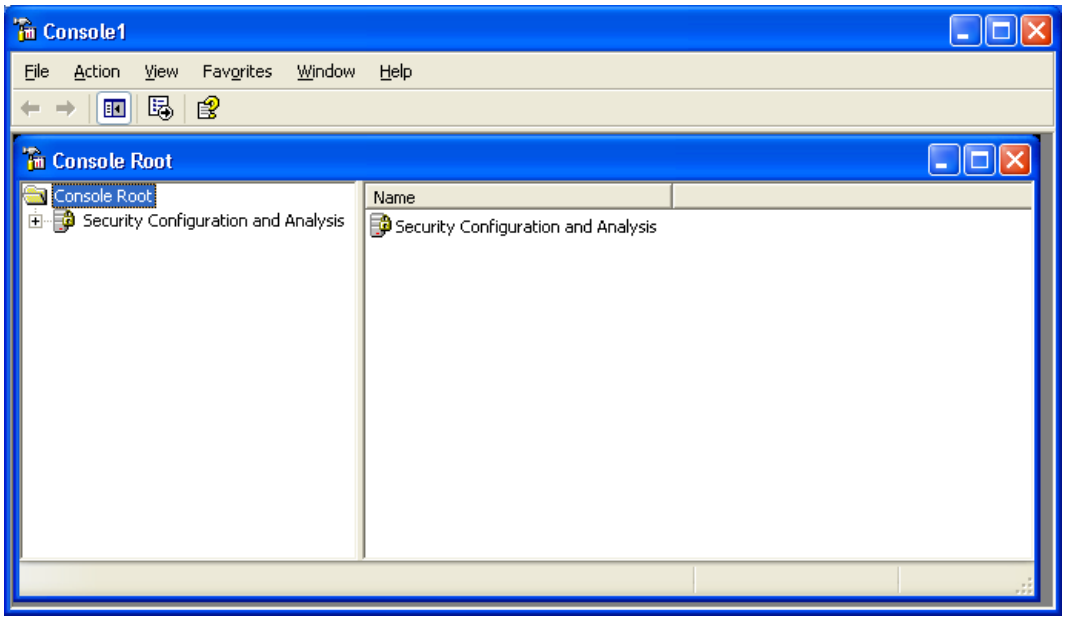

Figure 9. Console Root window, with Security Configuration and Analysis option

9. Double-click **Security Configuration and Analysis**. The **Security Configuration and Analysis** information appears in the right-hand side of the **Console** window (see Figure 10).

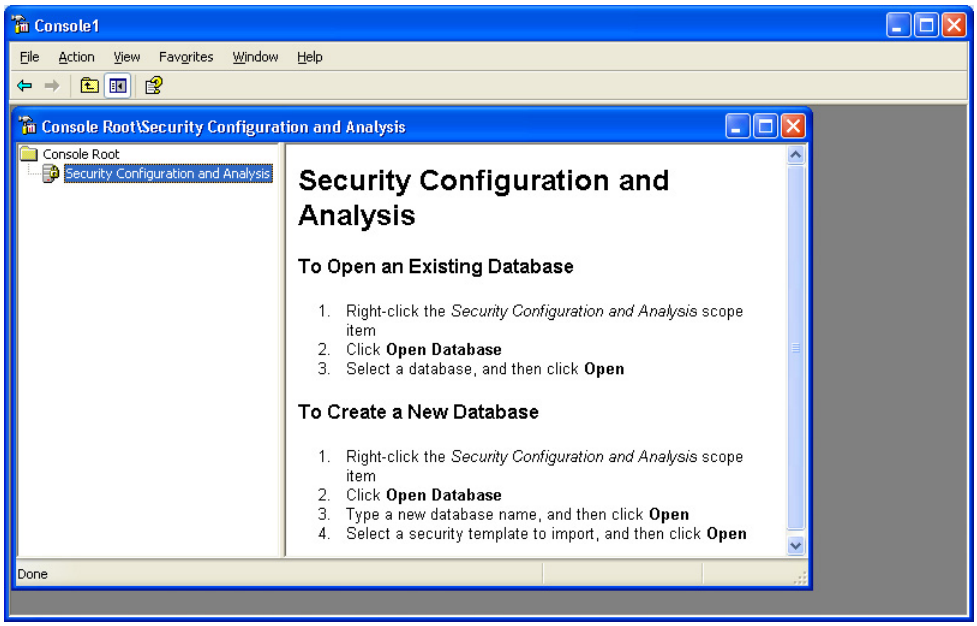

Figure 10. Console Root\Security Configuration and Analysis window

10. Right-click **Security Configuration and Analysis** in the **Console** tree in the left-hand side of the **Console** window, and choose **Open Database** from the shortcut menu.

11. The **Open Database** dialog box appears (see Figure 11).

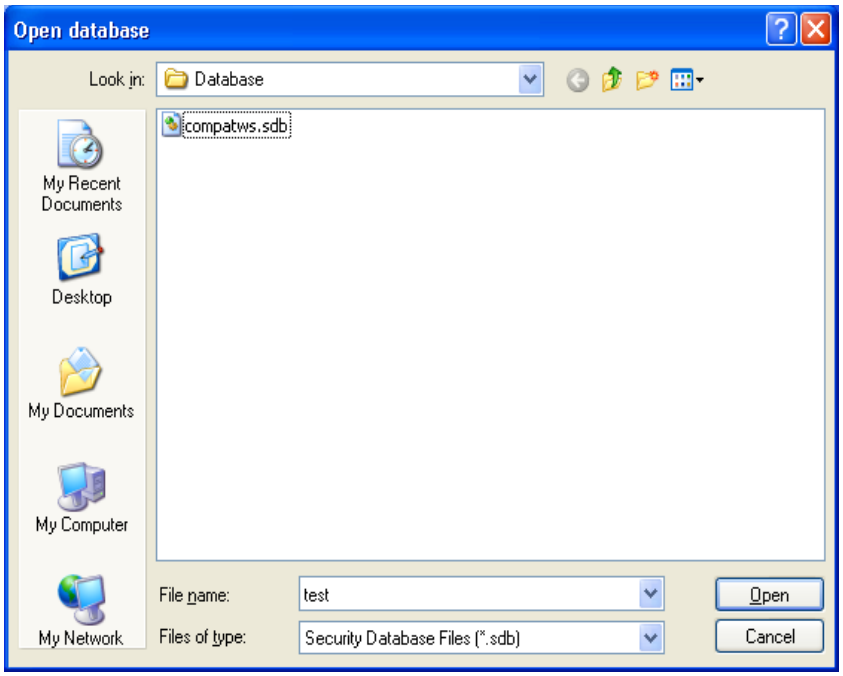

Figure 11. Open Database dialog box

12. Type a name for the security database (the security database is temporary) in the **File** name box and click **Open**. The **Import Template** dialog box appears (see Figure 12).

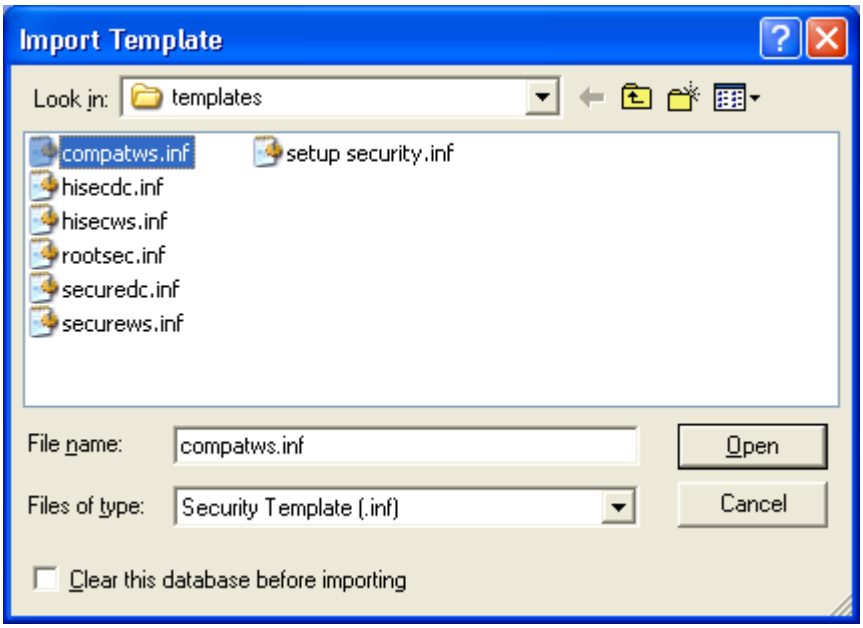

Figure 12. Import Template dialog box

13. Click the compatws.inf template (a template for low-level security settings for Windows XP Professional) in the **Import Template** dialog box to import it.

14. Click **Open**. The **Console Root\Security Configuration and Analysis** dialog box appears (see Figure 13).

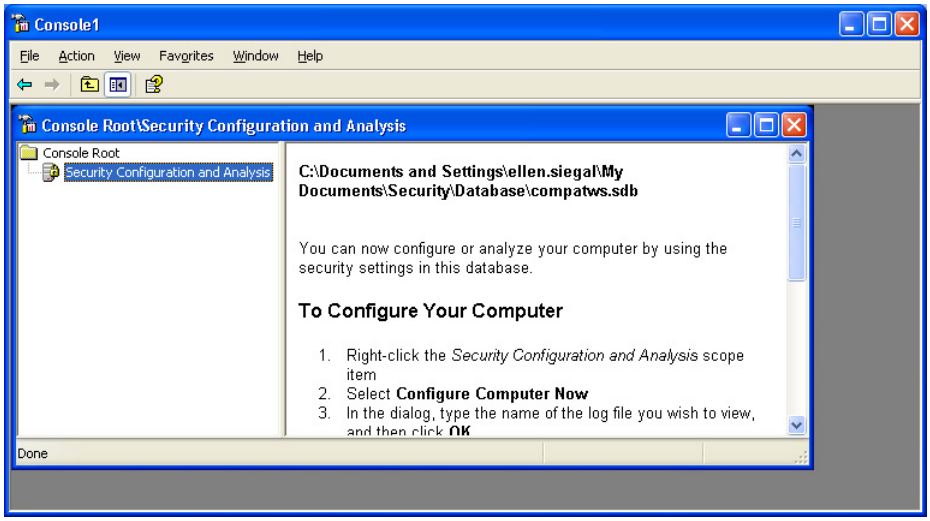

Figure 13. Console Root\Security Configuration and Analysis dialog box

15. Right-click the **Security Configuration and Analysis** option in the console tree to open the short cut menu, and choose **Configure Computer Now.** The **Configure System** dialog box appears (see Figure 14).

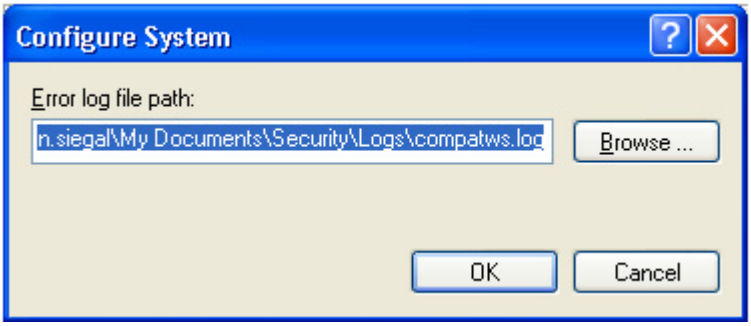

Figure 14. Configure System dialog box

16. Click **Browse**. Select the directory for the error log file and click **OK**.

17. The **Configuring Computer Security** status box tracks the progress of configuring the system.

    Your system settings are now configured to those recommended by the template.

18. Choose **File > Exit** to close the **Console** menu. The **Microsoft Management Console** window appears (see Figure 15).

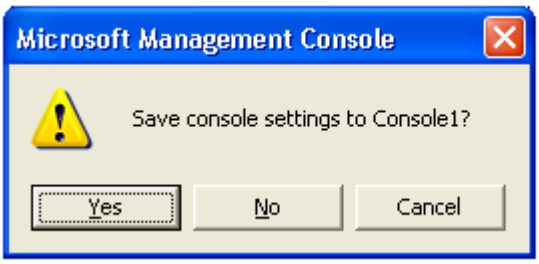

Figure 15. Microsoft Management Console window

Click **Yes** to save the **Console** settings. The software saves **Console** settings and adds the **Security** settings to the computer.

Confirming the Properties of System Services

The authorization and auditing functions of Xcalibur applications rely on two Finnigan system services: the Finnigan Security Server and the Finnigan Database Server. These services are installed when the administrator installs the application software. They are configured to start automatically every time the workstation is restarted.

The main function of the Finnigan Security Server is user authentication. If authentication is selected for certain events, user names and passwords are verified by the Finnigan Security Server whenever they are entered.

The Finnigan Database Service permits Xcalibur applications to access the auditing database and make auditing entries.

To confirm that the properties of the Finnigan Security Server and Finnigan Database Service are set correctly

1. Open the Services window:

    a. Choose **Start > Settings > Control Panel** from the Windows XP taskbar.

    b. Double-click **Administrative Tools**.

    c. Double-click **Services**.

2. Confirm properties for the Finnigan Security Server:

   a. Right-click **Finnigan Security Server**, and choose **Properties** from the shortcut menu to open the Finnigan Security Server Properties dialog box (see Figure 16).

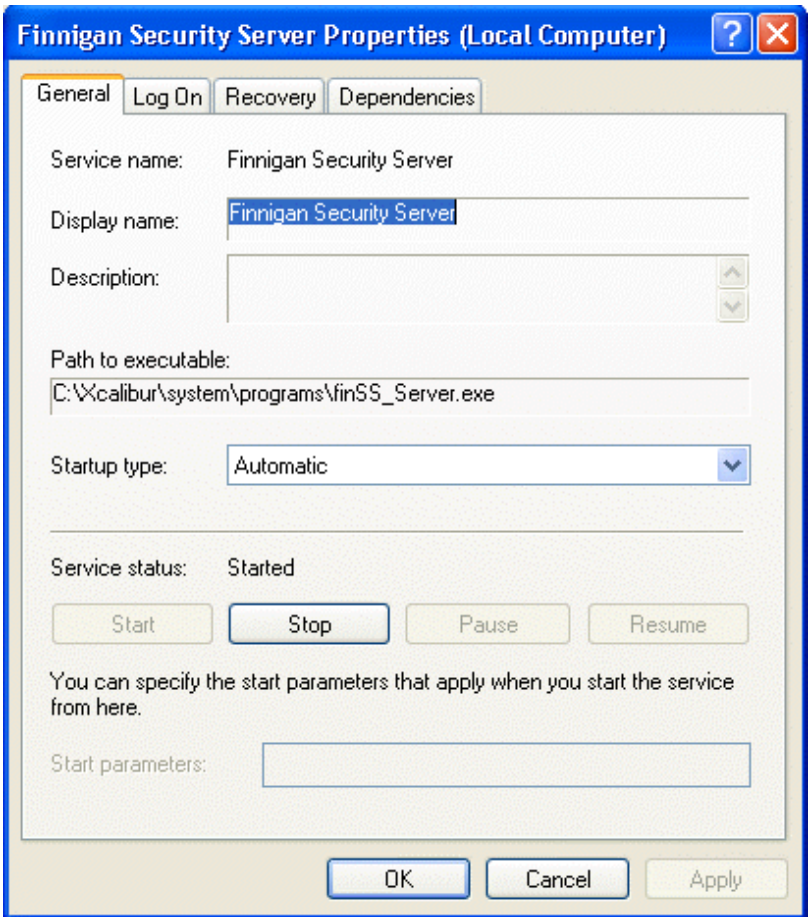

Figure 16. Finnigan Security Server Properties dialog box – General page

   b. Confirm that Startup Type is set to *Automatic* on the General page.

   c. Confirm that the Service Status reads *Started*.

d. Click the **Log On** tab to display the Log On page (see Figure 17).

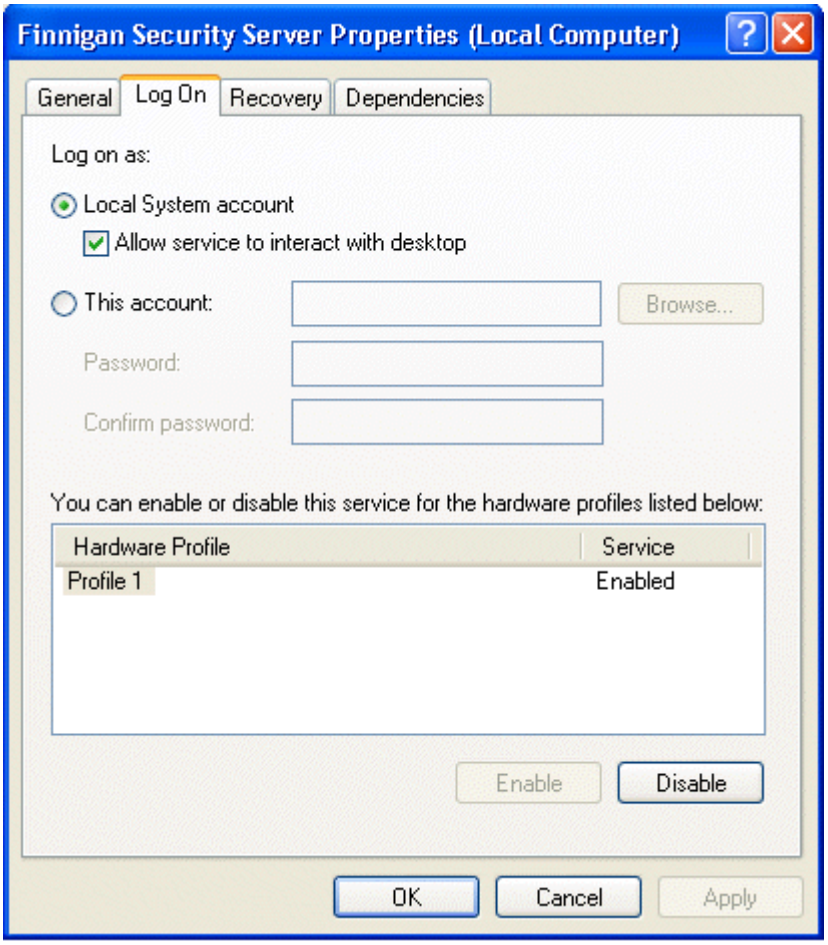

Figure 17. Finnigan Security Server Properties dialog box, showing the Log On page

e. Confirm that the Log On As: Local System Account option is selected.

f. Confirm that the Allow Service To Interact With Desktop check box is checked.

g. Click **OK** to close the dialog box.

3. Confirm properties for the Finnigan Database Service:

   a. Right-click *Database Service*, and choose **Properties** from the shortcut menu to open the Finnigan Database Service Properties dialog box (see Figure 18).

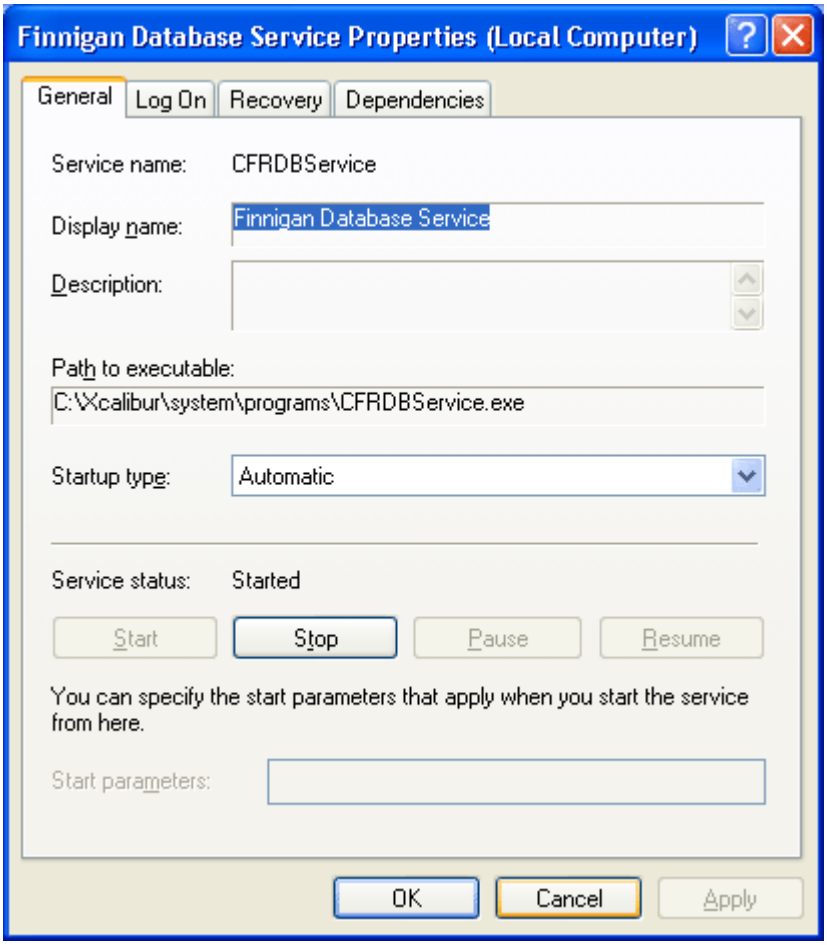

Figure 18. Finnigan Database Service Properties dialog box – General page

b. Confirm that Startup Type is set to *Automatic* on the General page.

c. Confirm that the Service Status Reads *Started*.

d. Click the **Log On** tab to display the Log On page (see Figure 19).

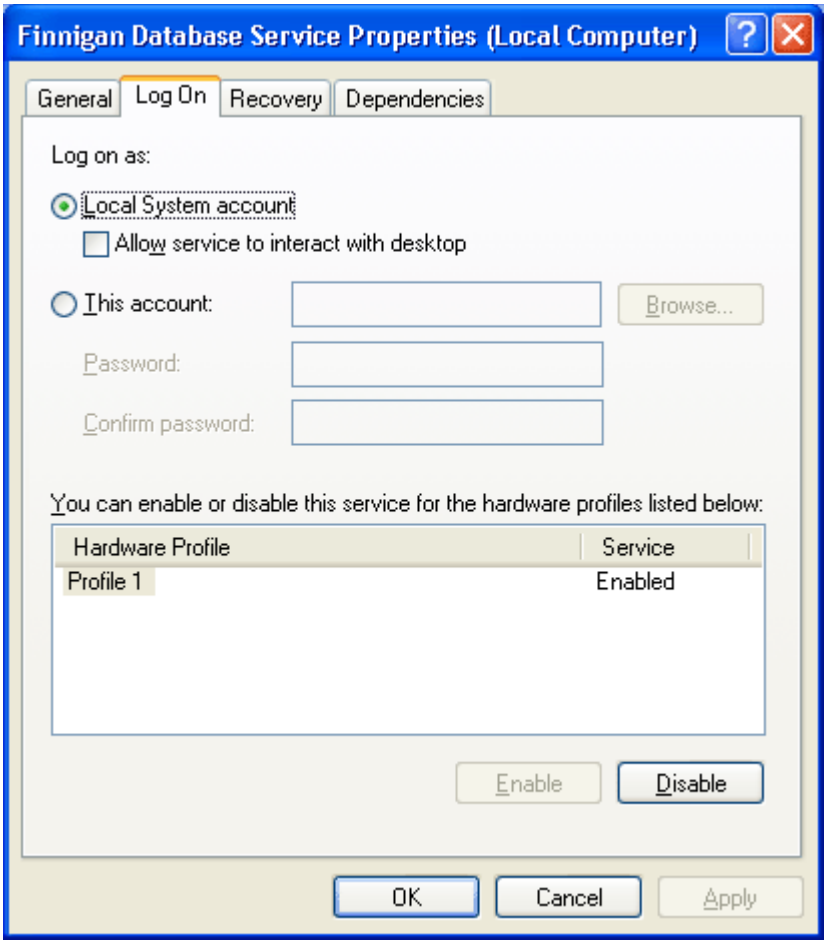

Figure 19. Finnigan Database Service Properties dialog box – Log On page

e. Confirm that the **Log On As: Local System Account** option is selected.

f. Confirm that the Allow Service To Interact With Desktop check box is not checked.

g. Click **OK** to close the dialog box.

4. Close the Services window and close the Administrative Tools window.

You have now confirmed that the services are set up properly.

Configuring Security Settings for Folders and Files

To confirm the security of your data, restrict access to the folder named *security* (located by default in C:\Xcalibur\system) that contains the configuration files. Because the Authorization Manager reads the controlled feature information from the configuration files, prohibit access to these files by non-administrators.

Set the access permissions for folders and files for specific user groups using the NTFS file system (an advanced file system used within the Windows XP operating system). When you set up permissions, specify the level of access for user groups, for example:

- Permit members of one user group to read the contents of a file
- Permit members of another user group to make changes to the file
- Prevent members of all other user groups from accessing the file

Folder permissions are inherited by new subfolders and files. Existing subfolders and files can be made to inherit new permissions that are applied to the parent folder by using the Properties dialog box for the folder. (See "Configuring the Security Settings for the Security Folder" on page 28.)

After appropriate permissions are set, it is not possible for an unauthorized user to maliciously or accidentally alter the contents of the folder using such utilities as the Windows Explorer.

In the procedures that follow, add an administrative user (or administrative group) and the *Everyone* group to the Security page Group Or User Names list. Grant the administrator full access to the *security* folder and read-only access to everyone else.

Tip When you require more restricted access to folders and files, grant access to only specific user groups. To do this, set up appropriate user groups, as described in the next chapter. Then, perform the procedures that follow, but use your specific user groups instead of the *Everyone* group.

Continue with the following subtopics:

Configuring the Security Settings for the Security Folder

To configure settings for the security folder

1. Log on to the workstation as a user with administrative privileges.
2. Choose **Start > Programs > Accessories > Windows Explorer** to open the Windows Explorer.
3. Choose **Tools > Folder Options** to open the Folder Options dialog box, and click the **View** tab.
4. Use the scroll bar in the Advanced Settings box to scroll to the bottom of the list.
5. Clear the Use Simple File Sharing check box (see Figure 20).

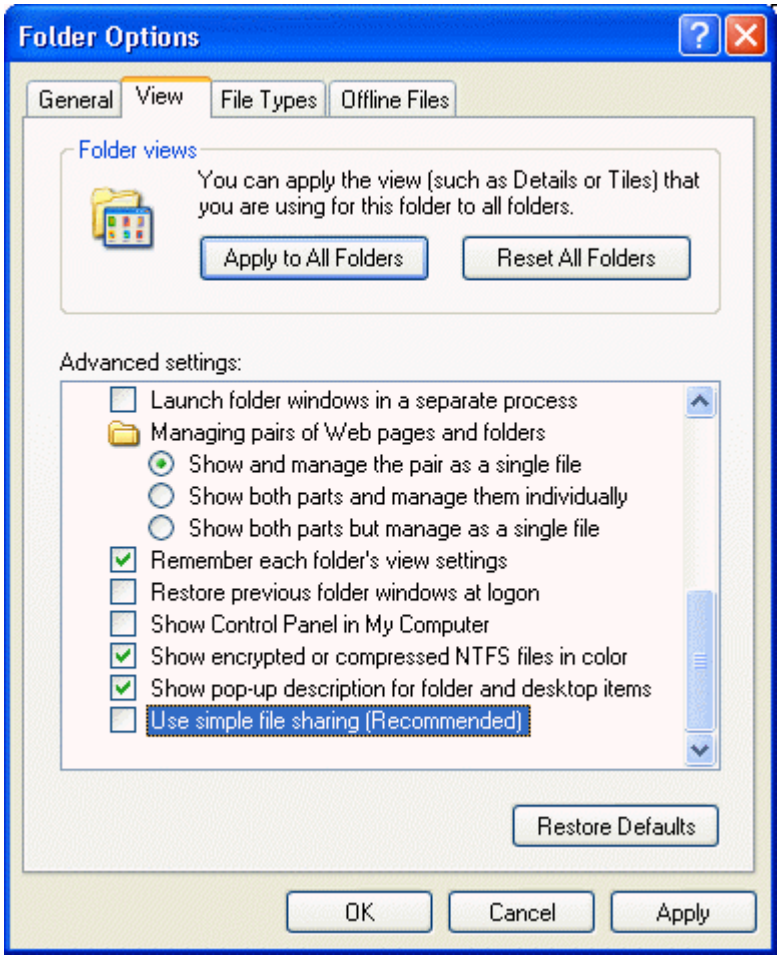

Figure 20. Folder Options dialog box, showing setting for Use Simple File Sharing check box.

6. Click **OK** to save the change and close the dialog box.

7. Locate the *security* folder in the Windows Explorer. (The default path for this folder is C:\Xcalibur\system\security.)

8. Right-click the *security* folder and choose **Properties** from the shortcut menu to open the Properties dialog box for the folder.

9. Click the **Security** tab to display the Security page (see Figure 21).

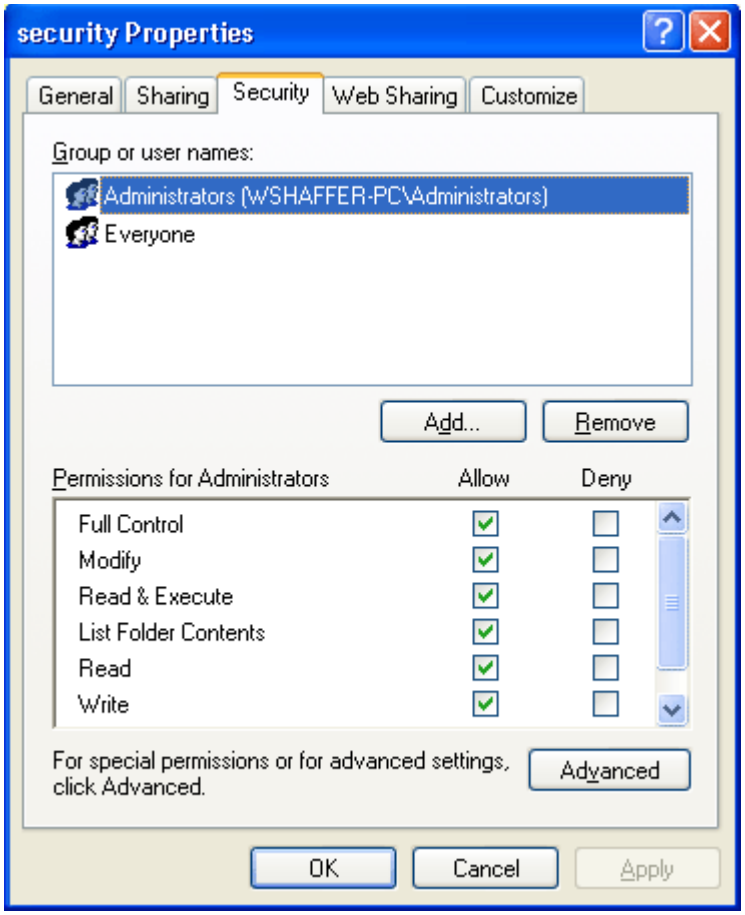

Figure 21. Properties dialog box – Security page

IMPORTANT When you create a new folder, the permissions from the parent folder automatically propagate to the new folder. This is indicated by the following:

- The check boxes in the Permissions list are shaded
- In the Advanced Security Settings dialog box, the Inherit From Parent The Permission Entries That Apply To Child Objects check box is selected

Normally, do not permit your *security* folder to inherit permissions from the parent folder. Prevent this inheritance by clearing the Inherit From Parent The Permission Entries That Apply To Child Objects check box in the next steps. Then correct the permissions in the topic "Setting Permissions" on page 34.

10. Click **Advanced** to open the Advanced Security Settings dialog box for the folder (see Figure 22).

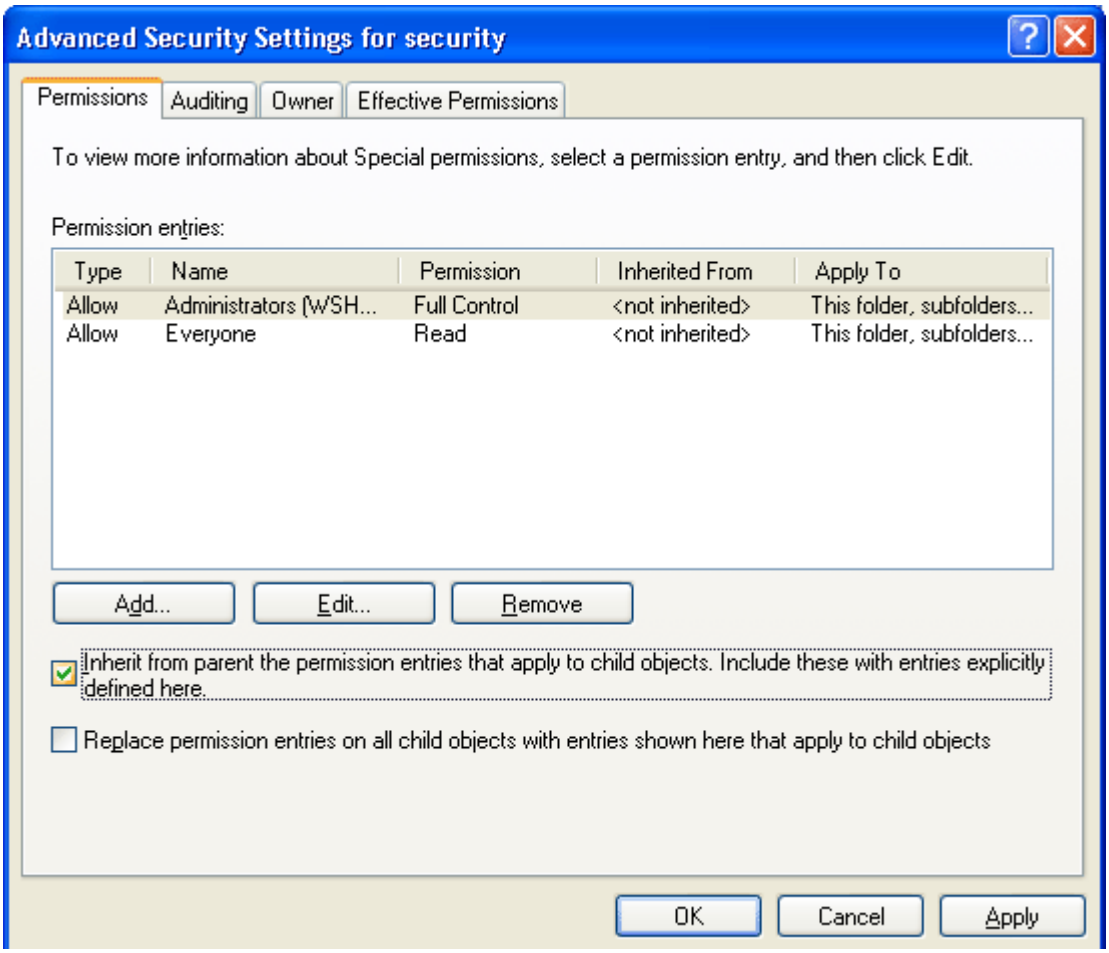

Figure 22. Advanced Security Settings dialog box

11. Clear the Inherit From Parent The Permission Entries That Apply To Child Objects check box. The Security dialog box appears (see Figure 23).

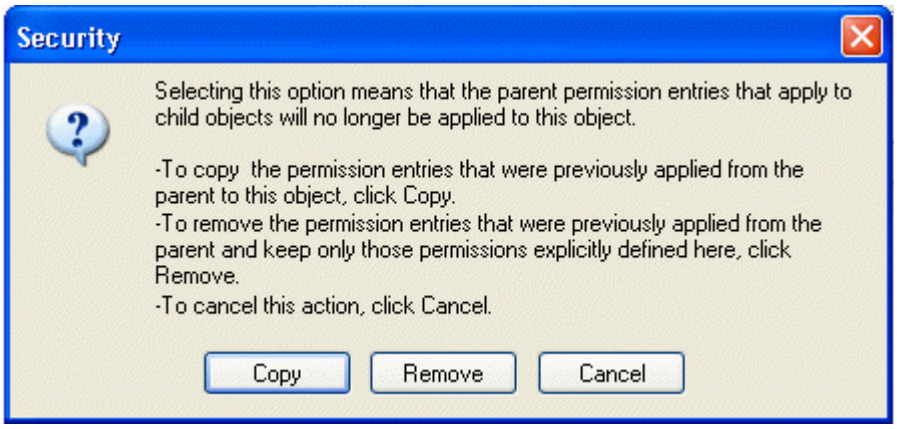

Figure 23. Security dialog box

12. Click **Copy** to copy the inherited permissions to the new folder and click **OK** to close the Advanced Security Settings dialog box.

    Correct the permission settings later (see "Setting Permissions" on page 34).

    Note After you clear the Inherit From Parent The Permission Entries That Apply To Child Objects check box and copy the inherited permissions to the new folder, the *security* folder no longer inherits permissions from the parent folder. As a result of this action, if someone changes the permission settings of the parent folder, the permission settings of the *security* folder does not change.

    However, any subfolders that are created under the *security* folder still inherit the permissions from it.

13. Examine the Group Or User Names list in the Properties dialog box and note what groups or users appear in the list. Only the *Everyone* group and the name of the administrator (or the name of the administrator group) should appear in this list.

    - If either is missing from the list, go to the next topic **Adding Users**.
    - If both appear in the list but additional groups or users also appear in the list, go to "Removing Users" on page 34.
    - If both appear in the list and no additional groups or users appear, go to "Setting Permissions" on page 34.

Adding Users

To prepare for setting permission levels for a folder or registry key, you might need to add users and groups to the Groups Or User Names list on the Security page.

To add users and groups

1. Click **Add** in the Properties dialog box – Security page to open the Select Users Or Groups dialog box (see Figure 24).

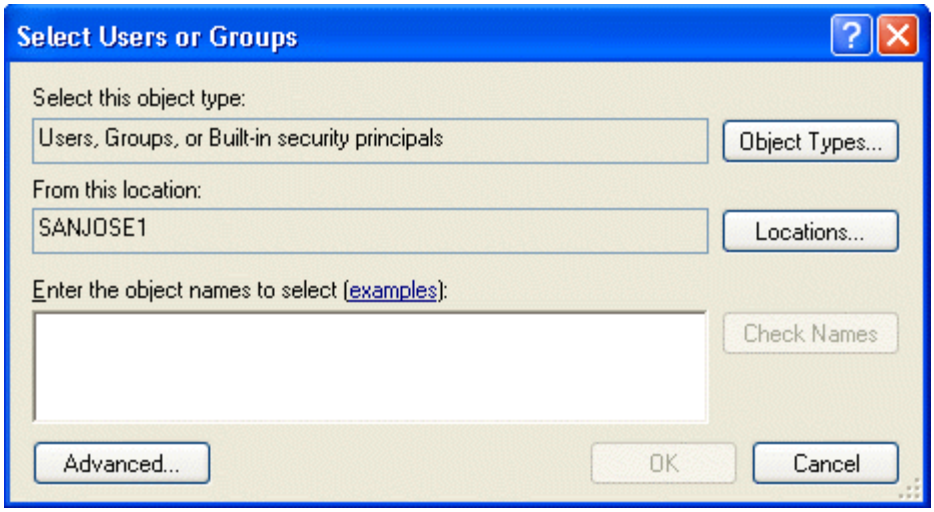

Figure 24. Select Users Or Groups dialog box

2. Confirm that the Select This Object Type box lists the object types that you require (*Users*, *Groups*, *Built-In Security Principals*).

   To change the list, click **Object Types** to open the Object Types dialog box and add or remove object types as needed.

3. Confirm that the From This Location box lists the root location that contains your users and groups.

   To change where to search, click **Locations** to open the Locations dialog box and specify a new location.

4. Enter the users or groups in the Enter The Object Names To Select box to add:

   - If the *Everyone* group was missing from the Group Or User Names list on the Security page, type **Everyone**.

- If the user name of the administrator (or the name of the administrator group) was missing from the Group Or User Names list on the Security page, type the appropriate user name or group name.

  Tip To enter multiple object names at the same time, separate the names with a semicolon.

5. Click **Check Names** to search for users or groups with the names that you specified in the box. All similar or matching object names that were found appear underlined in the box (see Figure 25).

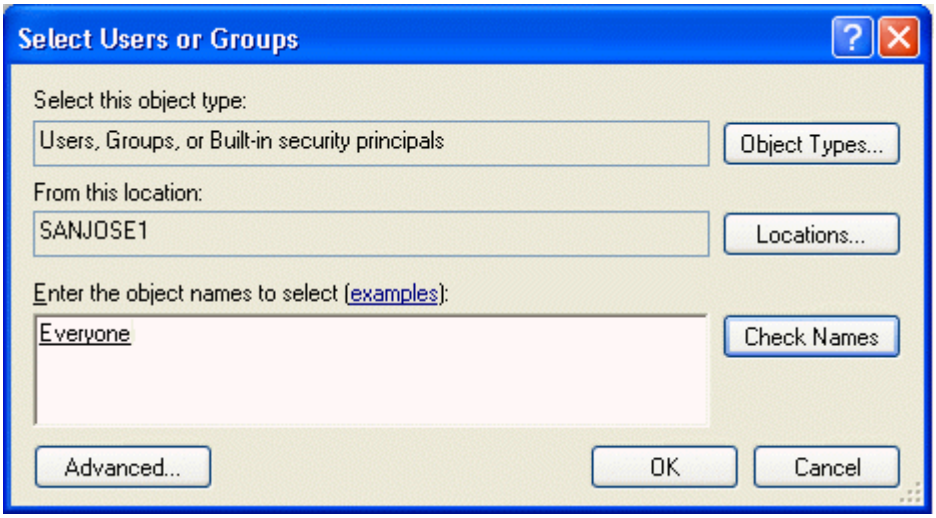

Figure 25. Select Users Or Groups dialog box, showing the *Everyone* group

6. Confirm that only the correct object name (or names) is listed in the box and click **OK** to close the dialog box and to return to the Properties dialog box.

7. Examine the Group Or User Names list on the Security page of the Properties dialog box again. The *Everyone* group and the name of the administrator are now available in the list.

   - When additional groups or users appear in the Group Or User Names list, go to the next topic, Removing Users.

   - If no additional groups or users appear, go to "Setting Permissions" on page 34.

Removing Users

To remove users or groups from the Group Or User Names list on the Security page

1. Select the name of the user or group.
2. Click **Remove** to remove the selected user or group.
3. Repeat these steps to remove any other users or groups.

You are now ready to set the permission levels for your users and groups.

Setting Permissions

After the correct users and groups are in the Group Or User Names list on the Security page of the Properties dialog box, set the permissions as follows:

1. Select the administrator (or the administrator group) in the Group Or User Names list.
2. Select the **Allow** check box in the Permissions list for the Full Control option. All of the other check boxes in the Allow column are automatically selected (see Figure 26).

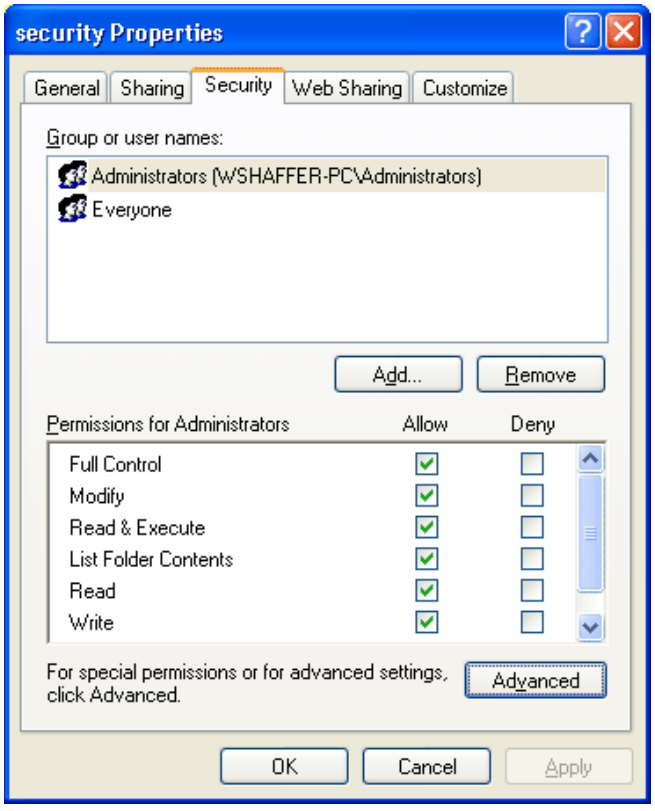

Figure 26. Properties dialog box – Security page, showing the correct settings in the Permissions list for an administrator

Note Groups or users granted Full Control for a folder can delete files and subfolders within that folder regardless of the permissions protecting the files and subfolders.

3. Select *Everyone* in the Group Or User Names list.
4. Select the **Allow** check box in the Permissions list for the Read option, and clear the Allow check box for all other actions in the list.

Note Setting these permissions confirms that none of the files in the folder can be deleted by using the Windows Explorer.

5. Confirm that the inheritance setting is correct:
   a. Click **Advanced** to open the Advanced Security Settings dialog box.
   b. Confirm that the Inherit From Parent The Permission Entries That Apply To Child Objects check box is cleared.
   c. Click **OK** to close the dialog box and to return to the Security page of the Properties dialog box.
6. Click **OK** to close the Properties dialog box and to save the permission assignments.

You have configured the security settings for the *security* folder.

Setting Permissions for Xcalibur Folders

When you are configuring a system with multiple users and those users work with files created by other users, set the permissions for Xcalibur files and folders so that all users who work with them have the necessary permissions. If these permissions are not set correctly, users might not be able to open or modify files created by other users.

In the procedure that follows, add the *Everyone* group to the Security page Group or User Names list and grant appropriate access to that group.

Tip When you require more restricted access to folders and files, grant access to only specific user groups. To do this, set up appropriate user groups, as described in the next chapter. Then, perform the procedures that follow, but use specific user groups instead of the *Everyone* group.

To set permissions for Xcalibur folders

1. Locate the *Xcalibur* folder in the Windows Explorer. (The default path is C:\Xcalibur.)

2. Right-click the Xcalibur folder and choose **Properties** from the shortcut menu to open the Properties dialog box for the folder.

3. Click the **Security** tab to display the Security page (see Figure 27).

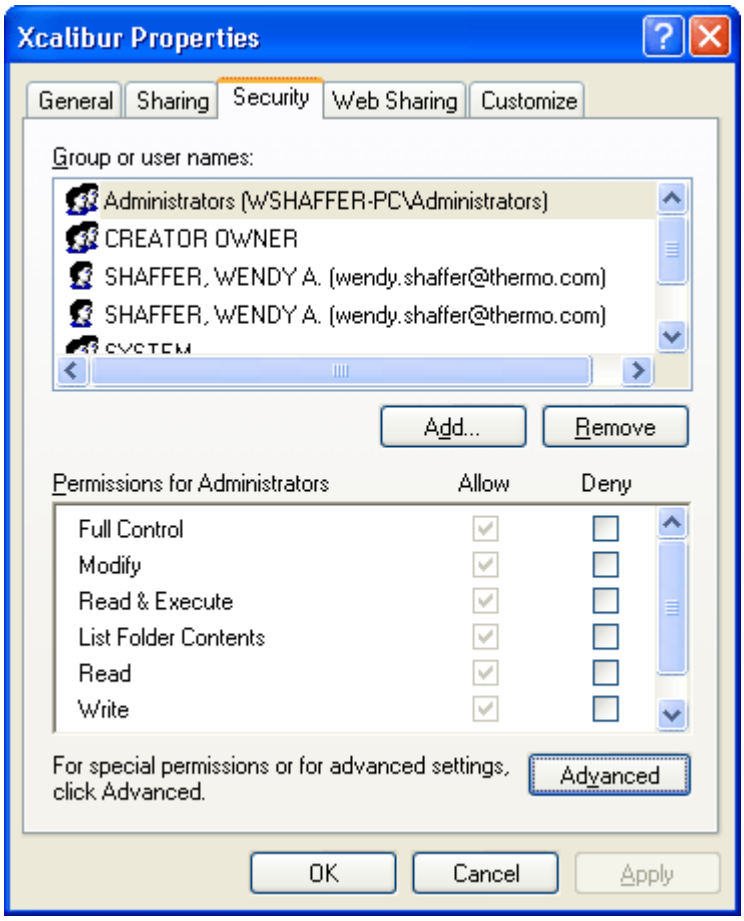

Figure 27. Properties dialog box – Security page

4. Click **Advanced** to open the Advanced Security Settings dialog box for the folder (see Figure 28).

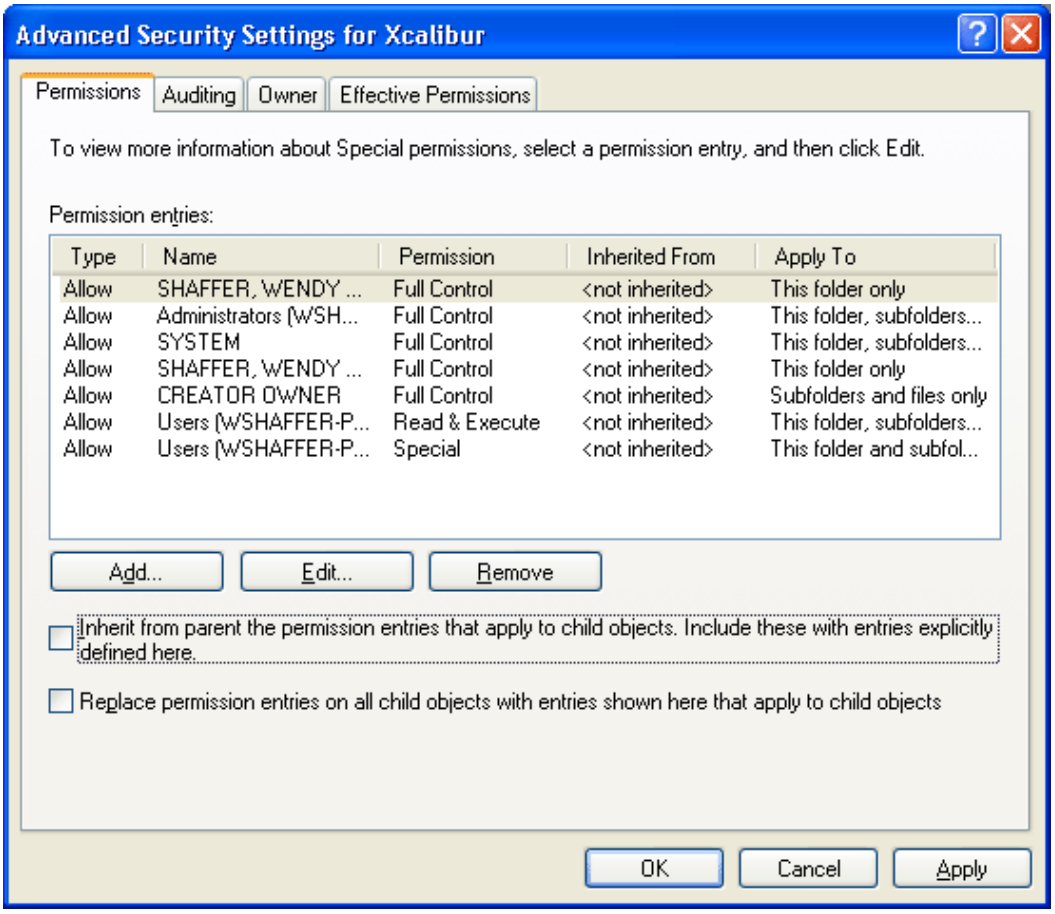

Figure 28. Advanced Security Settings dialog box – Permissions page

5. Clear the Inherit From Parent the Permission Entries That Apply to Child Objects check box. The Security dialog box appears.

6. Click **Copy** to copy the inherited permissions to the new folder and click **OK** to close the Advanced Security Settings dialog box.

   Correct the permission settings later (see "Setting Permissions" on page 34).

7. Examine the Group or User Names list in the Properties dialog box and make sure that the *Everyone* group appears in the list. If it does not appear in the list, add it. (See "Adding Users" on page 32.)

8. Select *Everyone* in the Group or User Names list.

9. Confirm that the Allow check boxes are checked for the following settings:
    - Modify
    - Read and Execute
    - List Folder Contents
    - Read
    - Write
10. Click **OK** to close the Properties dialog box and to save the permission assignments.
11. Repeat steps 1 to 10 for any additional folders not in the *Xcalibur* folder hierarchy used to store Xcalibur data.

Configuring Security Settings for the Database Registry Key

When the administrator runs the Database Configuration tool for the first time, the tool creates a Windows XP registry key that stores information about the database. To confirm the security of the auditing database, the security settings for this registry key must be set so that only the workstation administrator can make changes to the key.

To configure the security settings for the database registry key

1. From the Windows XP taskbar, choose **Start > Run** to open the Run dialog box.

2. Type ***regedit*** and click **OK**. The Registry Editor dialog box appears (see Figure 29).

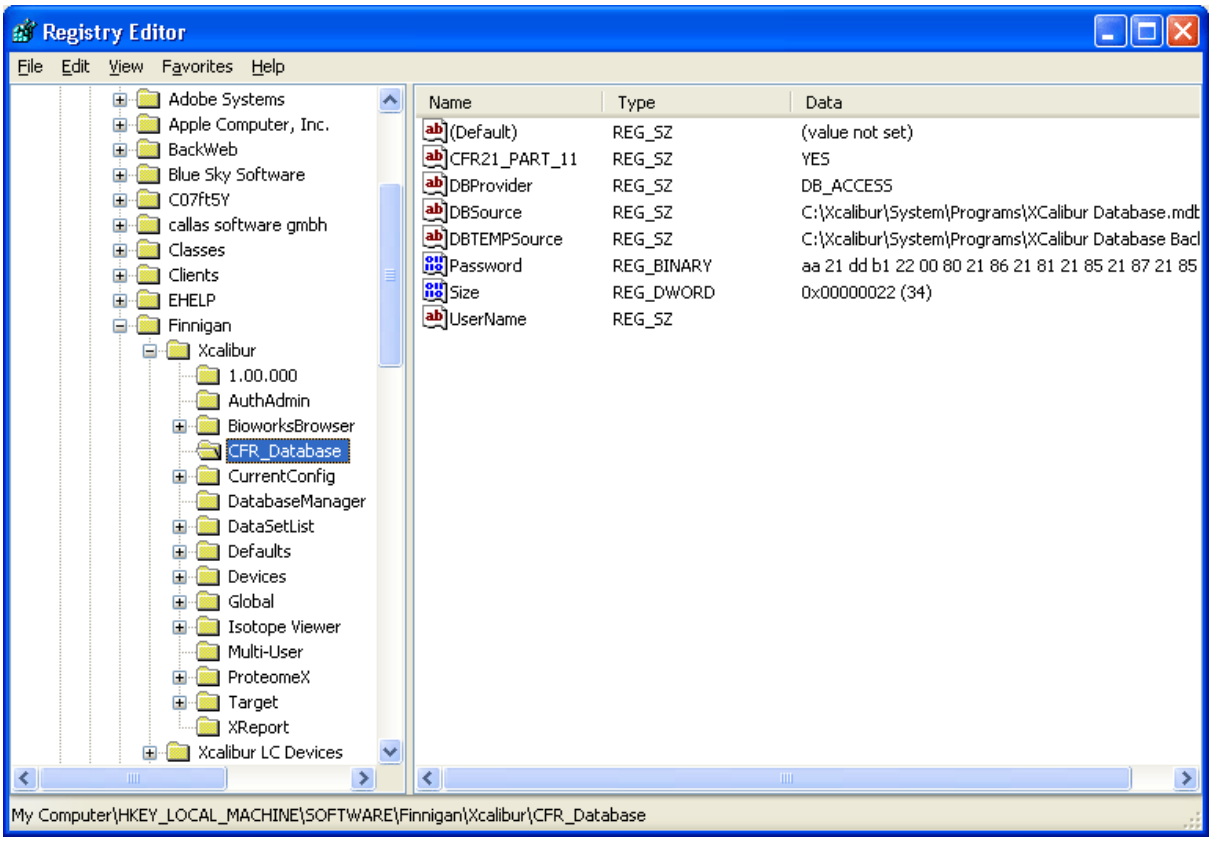

Figure 29. Registry Editor dialog box, showing CFR_Database key selected

3. Locate the My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Finnigan\Xcalibur\CFR_Database folder in the left-hand pane of the Registry Editor dialog box.

4. Right-click the CFR_Database folder and choose Permissions from the shortcut menu to open the Permissions dialog box for this registry key.

5. Click **Advanced** to open the Advanced Security Settings dialog box (see Figure 30).

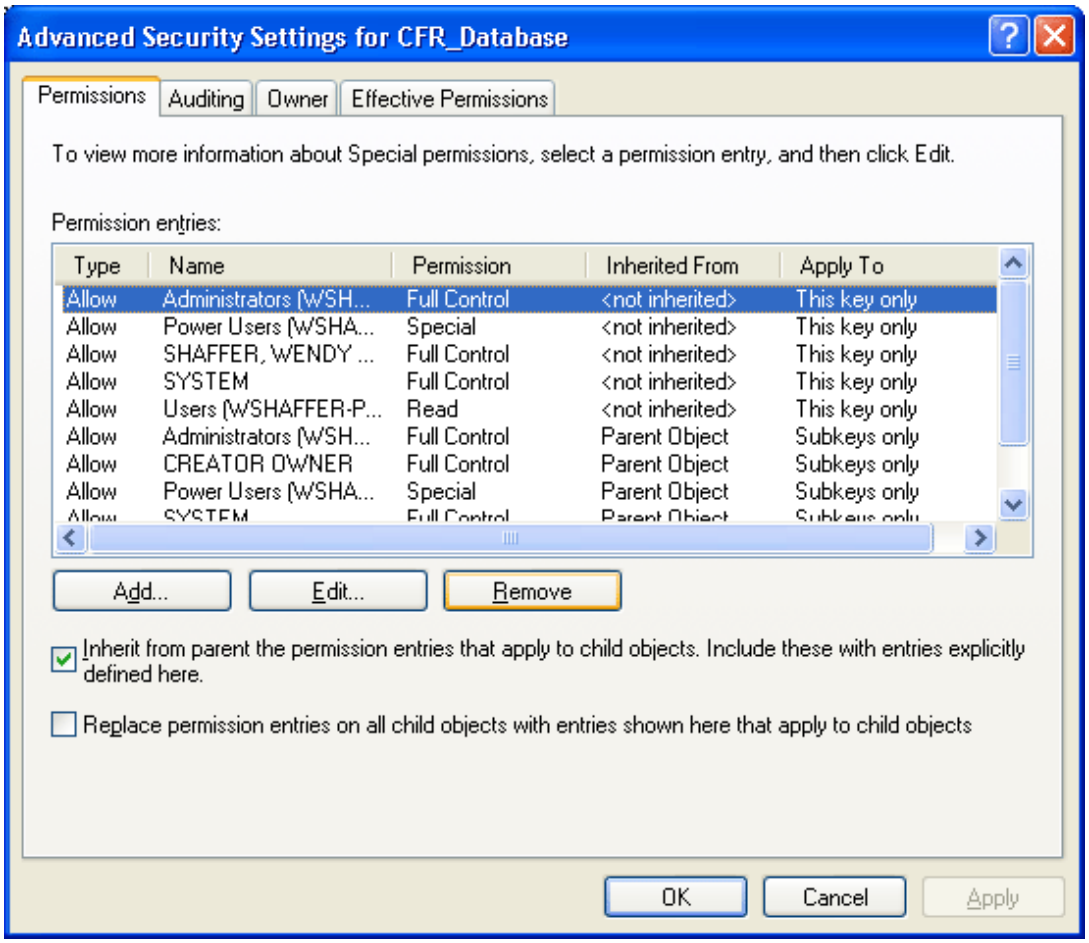

Figure 30. Advanced Security Settings dialog box

6. Clear the Inherit From Parent the Permission Entries That Apply to Child Objects check box. The Security dialog box appears (see Figure 31).

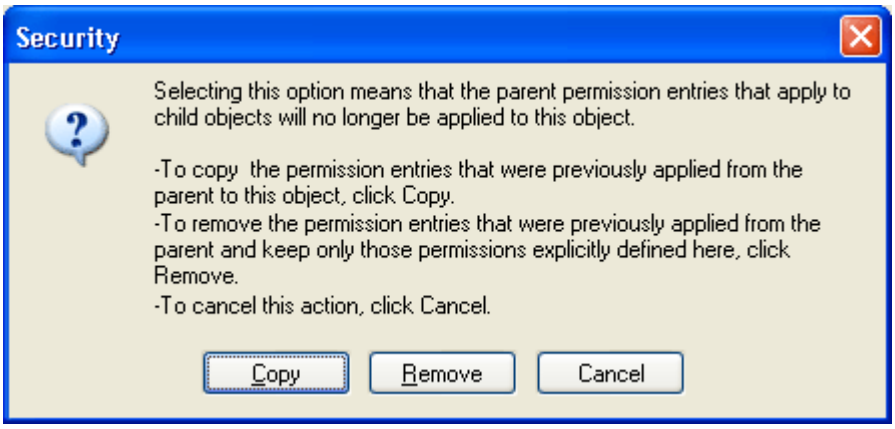

Figure 31. Security dialog box

7. Click **Copy** to copy the inherited permissions to the CFR_Database registry key and click **OK** to close the Advanced Security Settings dialog box.

8. Examine the Group or User Name list in the Properties dialog box and note what groups or users appear in the list. Only the name of the administrator (or the administrator group) and the *Everyone* group should appear in this list.

   - If the administrator (or the administrator group) does not appear in the list, add it (see "Adding Users" on page 32.)
   - If the *Everyone* group does not appear in the list, add it (see "Adding Users" on page 32.)
   - If other users or groups appear in the list, remove them (see "Removing Users" on page 34.)

9. Set the permissions for the registry key:

    a. Select the administrator (or the administrator group) in the Group or User Name list.

    b. Select the **Allow** check box in the Permissions list for the Full Control option. The Read check box in the Allow column is automatically selected (see Figure 32).

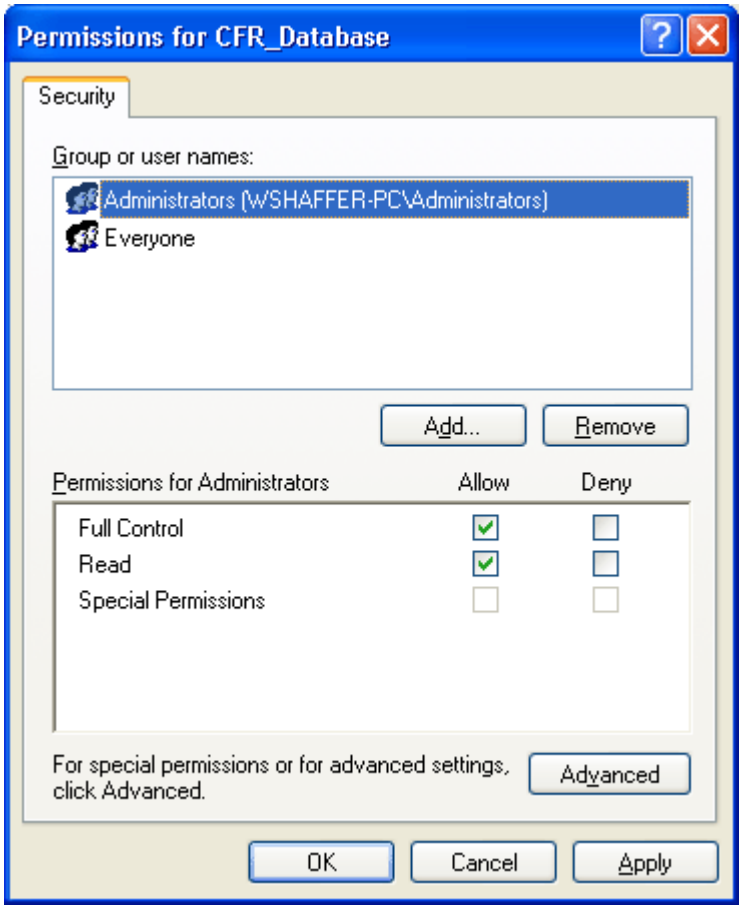

Figure 32. Permissions dialog box for CFR_Database, showing permission settings for the Administrators group

    c. Select *Everyone* in the Group or User Name list.

    d. Select the **Allow** check box in the Permissions list for the Read option. Clear the Allow check box for all other actions in the list.

10. Click **OK** to close the Permissions dialog box and save the permission settings.

11. Choose **File > Exit** to close the Registry Editor.

Specifying the Way Users Log On and Off

On computers that are not members of a network domain, the Windows XP Professional operating system permits you to switch between users without actually logging off from the computer. This feature, called Fast User Switching, can be turned off so that the current user must log off before another user logs on.

To maintain secure file operations, turn off Fast User Switching on computers that are not members of a network domain as follows:

1. From the Windows XP taskbar, choose **Start > Settings > Control Panel** to open the Control Panel.
2. Double-click *User Accounts* to open the User Accounts window.
3. Under Pick A Task, click **Change The Way Users Log On And Off** to open the Select Logon And Logoff Options page.
4. Clear the Use Fast User Switching check box.
5. Click **Apply Options**.
6. Close the User Accounts page.
7. Close the Control Panel.

When a user logs off, the computer automatically shuts down any programs that were running.

Removing and Archiving Files

To be fully compliant with 21 CFR Part 11, an organization must have proper procedures in place for long-term archiving and retrieving of electronic records, including raw data, processed data, and metadata. It is also necessary to have a procedure for ensuring that retrieval records can be read. Generally, this requires the organization to convert records to a new format or to keep and maintain the tools for reading the records in their current format.

To archive files, use third-party software designed for this purpose. In addition, develop and implement standard operating procedures for archiving files and security procedures to protect the archived data.

Chapter 4 Defining Secure User Groups and Adding Users

Control access to certain features of the Xcalibur software application by defining secure user groups and granting these groups appropriate permission levels. By design, every member of a secure user group holds the same rights and permissions. Use the Xcalibur Authorization Manager to create new groups and define permission levels.

After you define secure user groups and set permission levels, only those users who are in a secure user group can access the application. All others are prohibited access.

This chapter contains the following sections:

Planning User Groups

Before you begin, decide how many user groups you require or, equivalently, how many levels of access to grant to your users. For example, consider a laboratory in which both scientists and technicians work. The standard operating procedures for this laboratory state that technicians cannot perform certain operations with the software. There are no restrictions on what operations the scientists can perform. In this case, the laboratory administrator needs to create at least two user groups—one for scientists and one for technicians.

There is no limit to the number of user groups defined. For simplicity, if all users are to have the same privileges, define a single user group.

IMPORTANT If there are no user groups in place, there is no security for the software application!

A user group can be either a pre-existing Windows XP domain logon group or a private group:

- Windows XP domain logon groups must be created and managed by the domain administrator. Contact your domain administrator for help with domain logon groups.
- Private groups can be created and managed by the workstation administrator. However, before the workstation administrator can add a user to a private group, the user must be a member of a domain group. If an intended user is not a user on the domain, grant a domain account for that person. Contact your domain administrator for help in completing this task.

A single user can belong to more than one user group. If the groups have different permission levels, the most lenient permission level applies to the user.

Using the Authorization Manager

The topics contained in this section explain how to use the Authorization Manager:

- Defining User Groups
- Editing User Groups
- Setting Permissions
- Specifying Predefined Comments
- Viewing the Authorization Manager History Log
- Printing the Security Settings
- Saving the Security Settings

Note Shut down all Xcalibur applications before running the Authorization Manager. If you make changes to permissions for an application when the application is open, the changes might not take effect until the program is shut down and restarted.

Defining User Groups

To define user groups

1. From the Windows XP taskbar, choose **Start > Programs > Xcalibur > Authorization Manager** to open the Authorization Manager (see Figure 33).

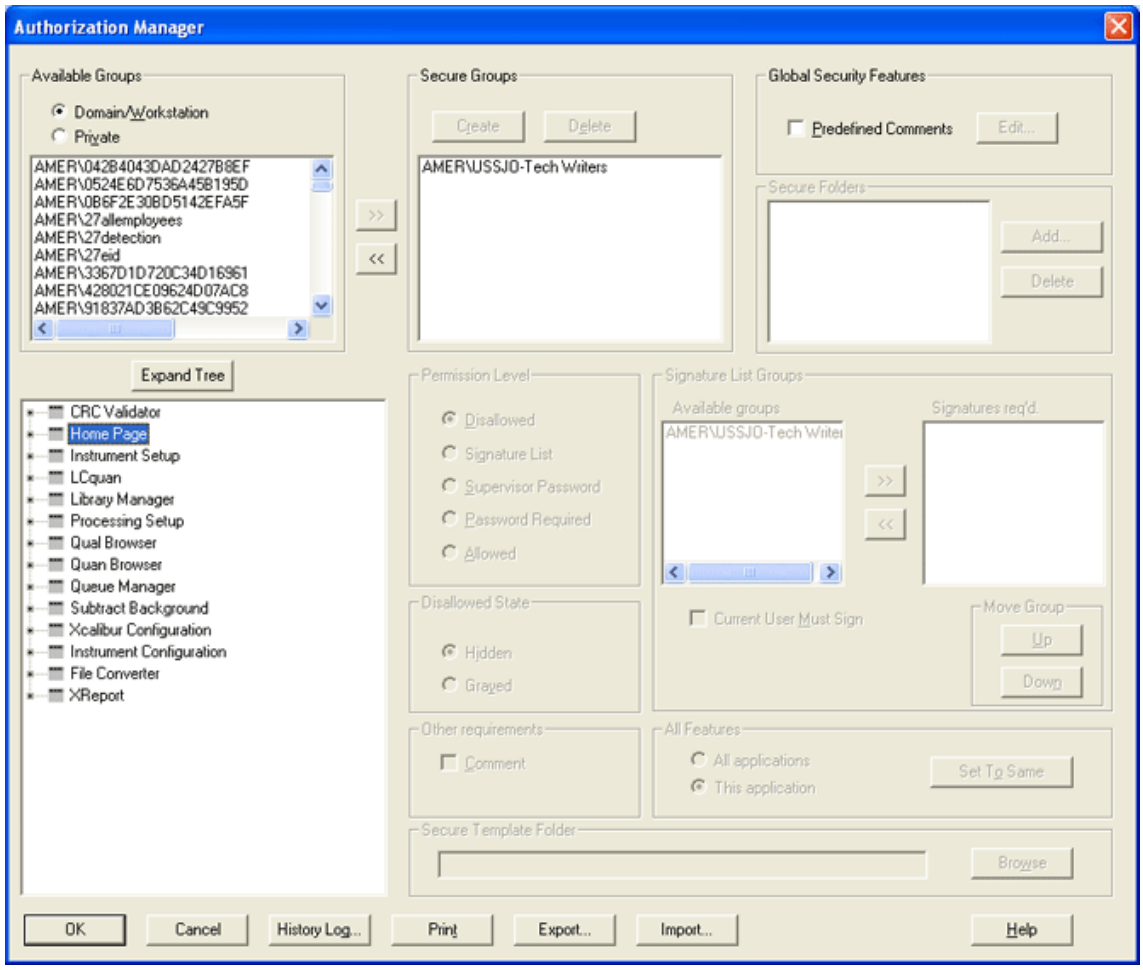

Figure 33. Xcalibur Authorization Manager

Note The Secure Template Folder, as shown in Figure 33, is only available in LCQuan.

2. Click the appropriate Available Groups option to specify the type of user group:

   - Click the **Domain/Workstation** option to use pre-existing Windows XP logon groups. Contact your domain administrator to create or change logon groups.

     Continue with step 3.

   - Click the **Private** option to use (or to create) a local user group. The administrator of the workstation can create private groups.

     Skip to step 4.

3. Define secure domain/workstation logon groups:

   a. Select a group in the Available Groups list to define as a secure group and click the right arrow button. The group appears in the Secure Groups list.

   

   b. To define more groups as secure, repeat this process. When you have created all needed groups, go to the next topic "Editing User Groups" on page 50.

4. Define secure private groups:

   a. Click **Create** in the Secure Groups area to open the Create Private Group dialog box (see Figure 34).

   b. Type a name in the Group Name box for the group.

   c. Select a domain in the System Group list. The domain user accounts appear in the Users Not In Private Group list.

   d. Select a user account and click the left arrow button to add it to the new private group. The user account appears in the Users In Private Group list.

   

   e. To add users in other domains to the private group, repeat steps c and d. If not, click **OK**. The new private group appears in the Secure Groups list.

   f. To create additional private groups, repeat steps a-e. If you have created all needed private groups, continue with the next topic.

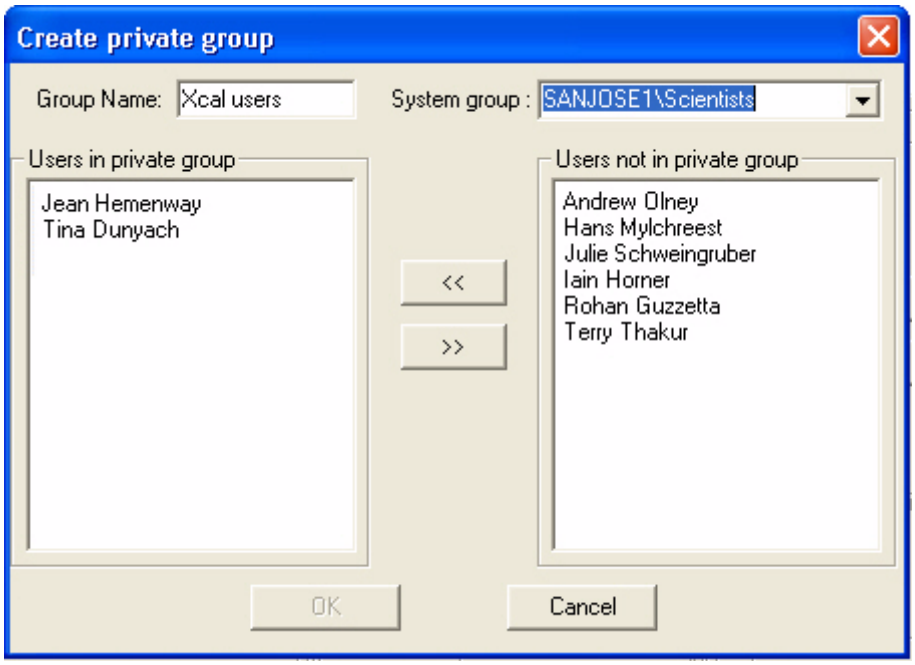

Figure 34. Create Private Group dialog box, showing two users in the new private group, Xcal Users

Editing User Groups

After defining a secure user group, view and (for private groups only) edit the members of the group. To do this, right-click the user group in the Secure Groups list and select **Members** from the shortcut menu.

- If the group is a private group, the Edit User List Of Private Group dialog box appears. Add or remove names from the user group by using the arrow keys.
- If the group is a domain/workstation logon group, the Modify Users In Group dialog box appears. Because membership in these groups is controlled by the domain administrator, the lists in the Modify Users In Group dialog box are read-only (see your domain administrator to make changes to domain/workstation logon groups.

Setting Permissions

For each secure user group, set the permission levels for certain features in the software application. Set permissions in the Permission Level area.

The available permission levels are listed in Table 2. All new secure user groups, whether domain/workstation groups or private groups, have all features set to *Disallowed*.

Table 2. Permission levels and descriptions

Permission Level	Description
Disallowed	Not permitted. Specify whether the user interface control for the disallowed operation is hidden or grayed out.
Signature List	The names and passwords of everyone on the signature list must be entered to perform the action. A series of dialog boxes (one for each signature) appears when a user attempts to perform this action in the software application.
Supervisor Password	The supervisor name and password must be entered to perform the action. A dialog box for the supervisor signature appears when a user attempts to perform this action in the software application.
Password	The user password must be entered to perform the action. A dialog box for the user password appears when a user attempts to perform this action in the software application.
Allowed	No restrictions.

Set permission levels in the following ways:

- By changing the permission level of an individual feature
- By setting all permissions to the same level
- By inheriting permissions from other secure user groups
- By importing permission lists from other workstations

Changing the Permission Level of an Individual Feature

To change the permission level of an individual feature

1. Select a user group in the Secure Groups list.
2. Select the name of your software application in the list in the lower left of the Authorization Manager.
3. Click **Expand Tree** to show the entire list of controlled features for the application.
4. From the list, select a feature to change the permission level.

Note Set permissions only for individual features, not subgroups. After selecting a feature, the Permission Level options are active. If they are unavailable, you probably selected a subgroup, not a feature.

5. Select one of the Permission Level options:
   - Disallowed
   - Signature List
   - Supervisor Password
   - Password Required
   - Allowed

   Tip To define the permission level of a feature, right-click the feature and select the permission level from the shortcut menu.

6. If you selected **Permission Level: Disallowed**, specify the appearance of the user interface control for the disallowed state:
   - If you do not want the user interface control to appear at all, click the **Disallowed State: Hidden** option.
   - To gray out the user interface control, click the **Disallowed State: Grayed** option.

7. When you selected Permission Level: Signature List, use the Signature List Groups area to define the signature list groups:

   Note When a feature with a permission level of Signature List is chosen in the software application, a series of password dialog boxes appear, one for each signature (name and password of a member of the designated group).

   The order of the groups shown in the Signature List Groups: Available Groups list defines the order of appearance for the password dialog boxes.

   a. Select a user group in the Available Groups list and click the right arrow key. The group appears in the Signature Required list.
   b. Add other groups to the signature list in the same manner as needed.

c. To require that the current user of the software application be placed on the signature list, select the **Current User Must Sign** check box.

d. If necessary, rearrange the order of the groups in the signature list by selecting a group and clicking on the Move Group buttons: **Up** or **Down**.

8. To permit the user to enter a comment after performing the action, select the **Comment** check box. (This option is available for all permission settings, except *Disallowed*.)

   When a comment is entered, it appears in the audit log for the software application.

9. Set the permission levels for any or all of the remaining features:

   - To set the permission level of an individual feature, repeat steps 4 to 8.

   - To set all of the other features for this application to the same permission level that you just set, click the **This Application** option and click **Set To Same**.

     The Permission Level setting, the Disallowed State setting (if applicable), and the Comment setting are copied to all of the other features for the currently selected application.

   - To set all other features for all applications to the permission level that you just set, click the **All Applications** option and click **Set to Same**.

     The software copies the Permission Level setting, the Disallowed State setting (if applicable), and the Comment setting to all other features for all application.

10. To set the permission levels for other user groups in the Secure Groups list, repeat steps 1 to 9.

IMPORTANT Permission level settings are retained when you move a user group out of the Secure Groups list and into the Available Groups list. When you move the group back into the Secure Groups list, the permission settings remain intact.

However, when you delete a user group from the Secure Groups list, all permission settings are lost.

Setting All Permissions

Set every feature to the same permission level in either of two ways:

- After you set the permission level for one feature, click **Set To Same** (as described in step 9 of the procedure above).
- Right-click the user group name in the Secure Groups list, and choose **Globally Set To > [Permission Level]** from the shortcut menu.

Inheriting Permissions

Copy a complete set of permission levels from one secure user group to another secure user group as follows:

1. Select the user group in the Secure Groups list that is to receive the set of permission levels.
2. Right-click the selected group and choose **Inherit From** from the shortcut menu.

   The Choose Secure Group dialog box appears and displays a list of the secure groups (minus the current one).
3. Select the group containing the permission levels to copy and click **OK**.

Both user groups now have the same set of permission levels.

Exporting and Importing Permissions

Import the permission list that contains the user groups and permissions from another workstation. This action saves time when you have more than one workstation in your lab and plan to provide access to all stations to users. Instead of setting up identical user groups on each workstation, copy the permission list from a workstation that has the user groups and access permissions that you require.

IMPORTANT To maintain the security of the permission list, export it to a secure location. The *security* folder (with proper security settings) on the current workstation is an ideal location.

To export and import the permission list

1. On the workstation where the correct users and permission levels are set, start the Authorization Manager and click **Export**. The Save As dialog box appears.

2. Save the permission list in the *security* folder as a file with the .eperm extension. (The default path for this folder is C:\Xcalibur\system\security; the default file name is permissions.eperm.)

3. Copy the file into the *security* folder on the new workstation.

4. On the new workstation, start the Authorization Manager and click **Import**. The Open dialog box appears.

5. Locate the permission list file (.eperm file) and click **Open**. The user groups and permission levels appear in the Authorization Manager.

6. Confirm that the user groups and permissions are correct and click **OK** to save the settings and close the Authorization Manager.

Specifying Predefined Comments

As an option, require users to select comments from a predefined list rather than typing in comments when they use features that require comment entry. To do this, select the Predefined Comments check box in the Global Security Features area. When predefined comments are active, a dialog box appears whenever a user performs an action that requires a comment. The user must select a comment from a drop down list before proceeding.

To define comments

1. Confirm that the Predefined Comments check box is selected.

2. Click **Edit**. The Edit Comment List dialog box appears.

3. Click **Add New Comment**. The New Comment dialog box appears.

4. Type comment text and click **OK**.

5. Repeat steps 3 and 4 to add each predefined comment.

6. Make any additional changes to the comment list:

   - To delete a comment from the list, select the comment and click **Remove Comment**.

   - To move a comment up or down in the list, select it and click **Move Up** or **Move Down**.

7. Click **OK** to save your changes and close the dialog box.

Viewing the Authorization Manager History Log

The Authorization Manager automatically maintains a history log to record all changes made to the security settings. The following events are logged:

- The creation of a private group
- The addition or deletion of members from a group
- A change in group permissions
- A switch between private and domain/workstation groups
- The manipulation of the signature list

To display the history log for the Authorization Manager, click **History Log**.

Each entry in the history log contains the time and date, the user ID and full name, and a description of the event. Sort and filter the entries in the history log by field (for example, sort and filter by date and time) or print the log.

Printing the Security Settings

Print a report of the security settings for each secure user group by clicking **Print**. The report contains a listing of the members of the group, the controlled feature information for each application, and the names of any secure folders for each application.

Saving the Security Settings

After you have defined your user groups, set the appropriate permission levels, and specified the type of application auditing, click **OK** to save your settings and exit the Authorization Manager.

The controlled feature information is saved in a configuration file in system\security. (The default path for this file is C:\Xcalibur\system\security.) Prohibit non-administrator access to this folder by properly setting the security for this folder. If you have not already done this, see the previous chapter, Establishing Secure File Operations.

Chapter 5 Using the CRC Validator

The CRC Validator compares the cyclic redundancy check (CRC) value stored in the database for a file with the CRC value computed from the file stored on the hard disk. If the stored CRC value and the computed CRC value do not match, the file might have been corrupted or altered since an Xcalibur application saved it.

This chapter describes how to use the CRC Validator to check your files. It contains the following sections:

Note Close any open Xcalibur applications before running the CRC Validator.

Checking Files With the CRC Validator

To use the CRC Validator

1. From the Windows taskbar, Choose **Start > All Programs > Xcalibur > CRC Validation** to launch the CRC Validator (see Figure 35).

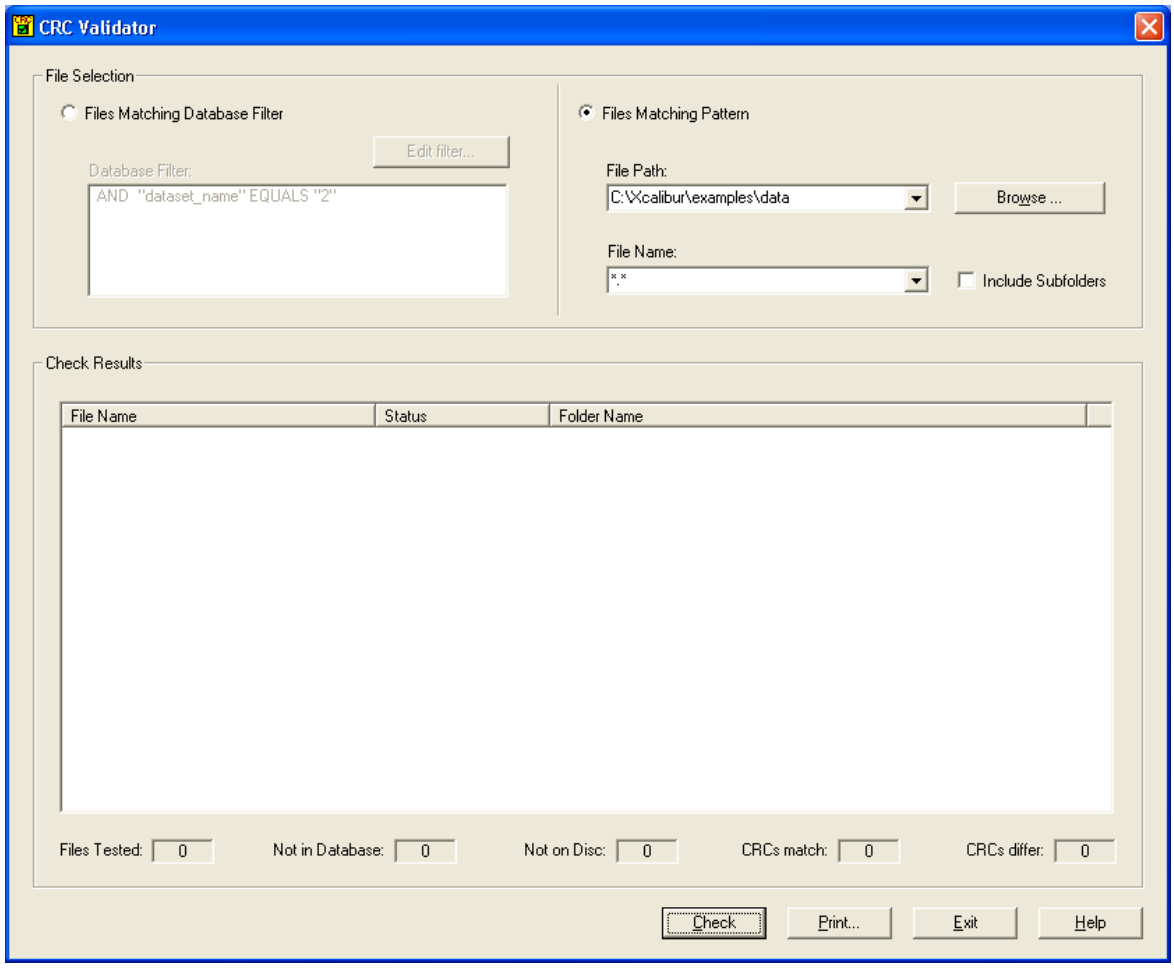

Figure 35. CRC Validator

2. Select a method for selecting files for validation in the File Selection area:

   - To select files matching a database filter, see "Selecting Files Using Database Filters" on page 60.
   - To select files matching a pattern, see "Selecting Files Using a Pattern" on page 62.

3. Click **Check** to check the selected files.

4. Examine the results displayed in the Check Results area. The status column in the file list indicates the status of each file as described in Table 3.

5. Click **Exit** to close the CRC Validator.

Table 3. Status values for CRC Validation

Status	Description
CRCs Match	The CRC stored in the database matches the CRC just calculated for the file.
CRCs Do Not Match	The CRC stored in the database does not match the CRC just calculated for the file. Most likely, the file has been modified since the tracking record was created.
File Not In Database	The file was found on the hard disk, but not in the database. It might not be a tracked file.
File Not On Disk	The file was found in the database, but not on the hard disk. The file might have been archived or deleted.

Selecting Files Using Database Filters

When you select files using database filters, select files for validation based on information about those files that is stored in the auditing database. For example, select files created by a particular Xcalibur application or select files created or modified at certain times.

Create two types of filters: non-date filters and date filters. Non-date filters are based on fields from the auditing database. Use them to select files based on characteristics such as the application used to create the file or the name of the user who created the file. Use date filters to select files based on the date when they were created or last modified.

Combine multiple non-date filters using the AND and OR operators. The default filter is the most recently selected dataset name.

To select files using a database filter

1. Click the **Files Matching Database Filter** option in the File Selection area.

2. Click **Edit Filter** to open the Filters dialog box (see Figure 36).

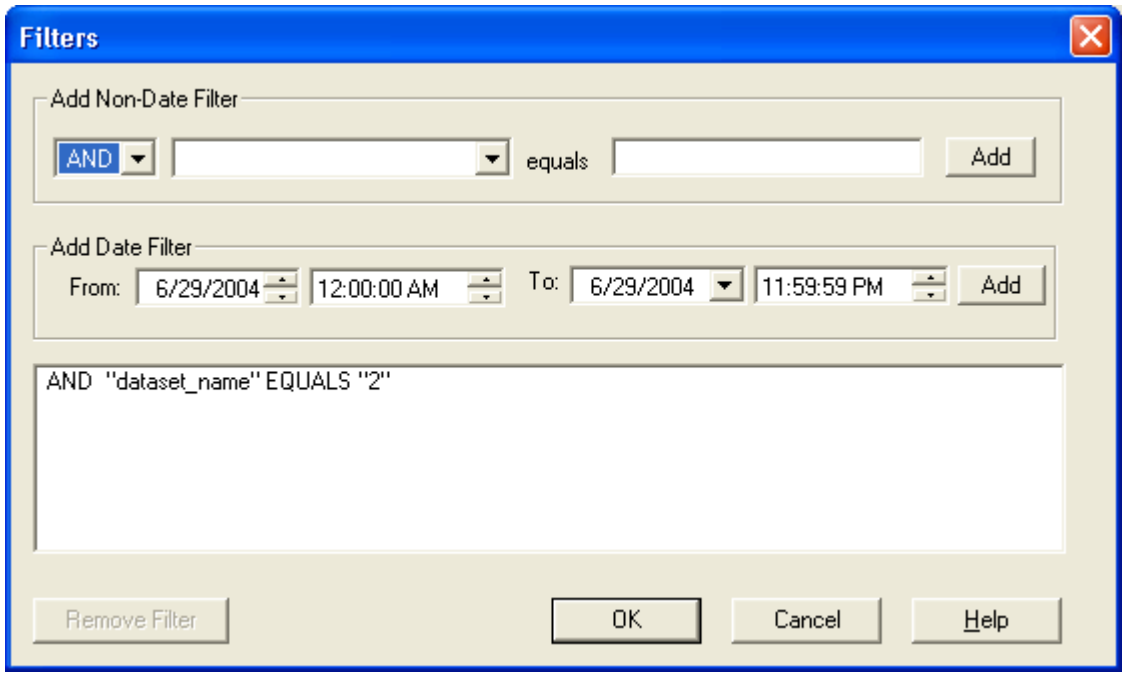

Figure 36. Filters dialog box

3. To add a non-date filter, do the following:

    a. Select AND or OR from the first list in the Add Non-Date Filter area.

    b. Select the database key to filter on from the second list.

    c. Type the value for the database key in the Equals box. For example, if you selected *Application Name* in the second list, you might enter Home Page or Qual Browser in the Equals box.

    d. Click **Add** to add this filter to the list of current filters.

    e. Repeat steps a through d to add other non-date filters.

4. To add a date filter, do the following:

    a. Enter the starting date and time for your filter in the Add Date Filter area in the From combo boxes.

    b. Enter the ending date and time for your filter in the To combo boxes.

    c. Click **Add** to add this filter to the list of current filters.

5. If necessary, remove unwanted filters from the filter list:

    a. Select the filter to remove by clicking on the filter name in the list.

    b. Click **Remove Filter** to remove the filter from the list.

6. When you have made all needed changes, click **OK** to close the dialog box and save your changes.

Selecting Files Using a Pattern

When selecting files using a pattern, specify the folder containing the files and the format type of the files (for example, a .raw file). To select files using a pattern, do the following:

1. Click the **Files Matching Pattern** option in the File Selection area.
2. Enter the path in the File Path combo box to the folder containing the files to check, or click **Browse** to browse to the folder.
3. Select the file extension of the files to check in the File Name list.
4. Select the **Include Subfolders** check box to have the CRC Validator check files in subfolders of the selected folder.

Appendix A Installing an Oracle Database

This chapter describes the procedure used by Thermo Scientific to install the Oracle Server and Client software. Consult your Oracle database administrator for advice and instructions on how to install this software for your application.

The installation information in this chapter is a supplement to the documentation provided by Oracle and does not replace it. See your documentation from Oracle for installation and configuration details.

Note The procedures contained in this chapter describe the installation of the Oracle9*i* Database. The installation procedures for other versions or releases of the database might differ from those described here.

This chapter contains the following sections:

Installing the Oracle Server

Install the Oracle Server as follows:

1. Insert the Oracle Database compact disc. The Autorun installation program should start automatically. If the installation program does not start automatically, locate and double-click the setup.exe file.

2. Click **Install/Deinstall Products** in the installation program. The Oracle Universal Installer: Welcome page appears (see Figure 37).

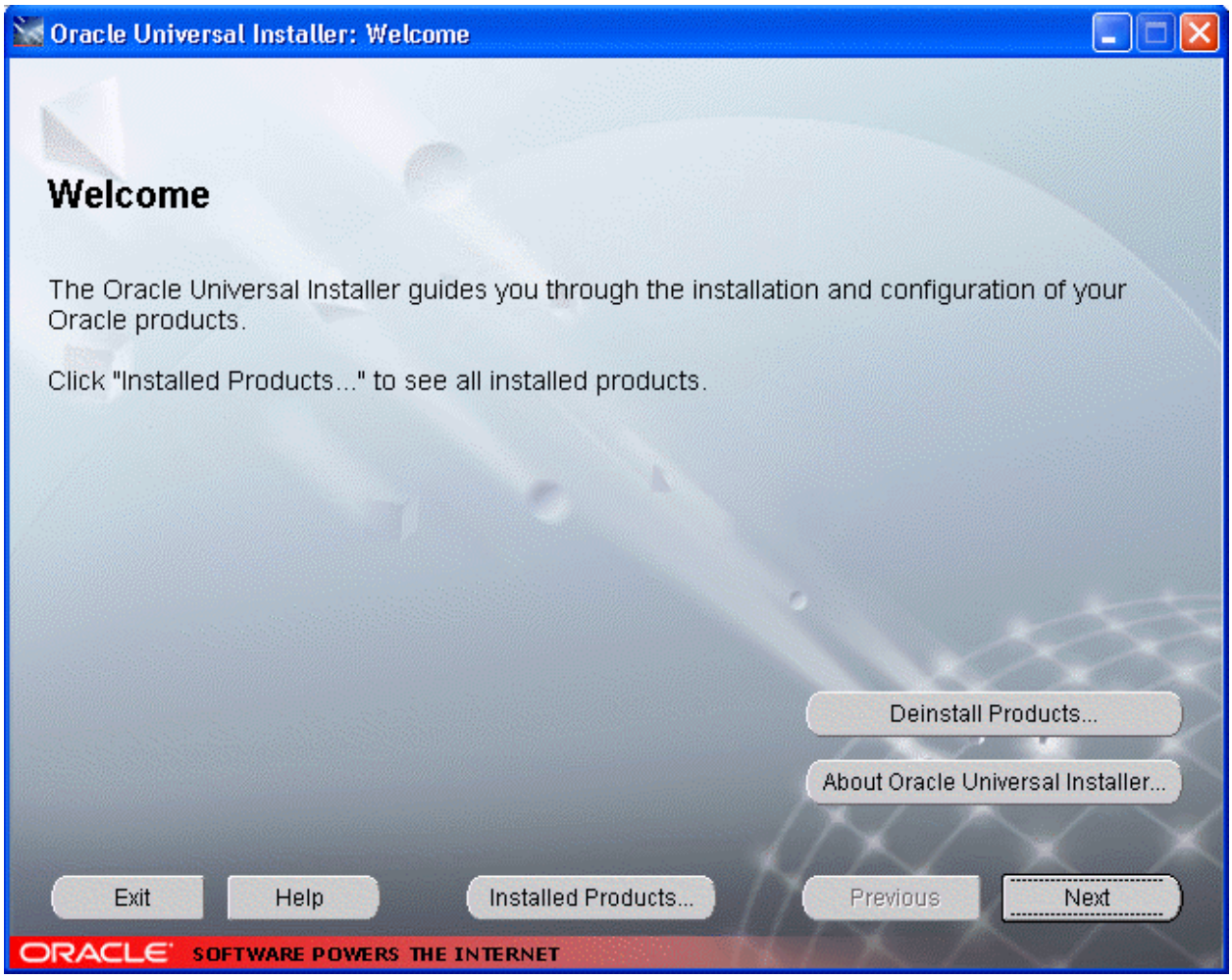

Figure 37. Oracle Universal Installer: Welcome page

IMPORTANT Do not install Oracle software into an existing Oracle home that contains another installation of Oracle software. Deinstall any previous versions before installing a new version. If you have data in the other database, ***back up your data*** and migrate it to the new database during or after the installation by using the Oracle Data Migration Assistant. See your documentation from Oracle for more information

3. To remove a previous version of Oracle software before proceeding with this installation, click **Deinstall Products** to open the Inventory dialog box, select the previous version from the list, and click **Remove**.

4. Click **Next** in the Welcome page. The File Locations page appears (see Figure 38).

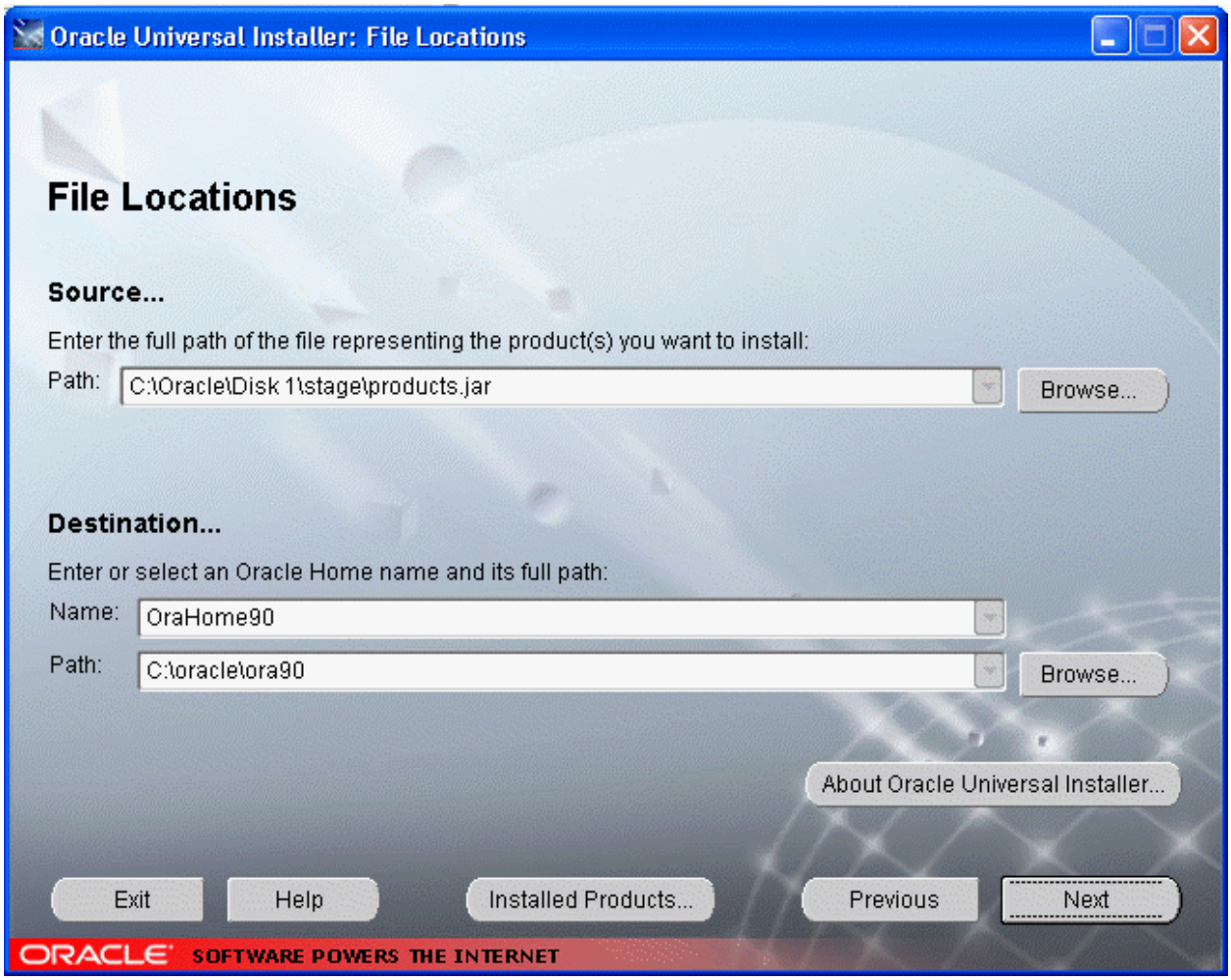

Figure 38. Oracle Universal Installer: File Locations page

IMPORTANT The Source Path combo box is filled in automatically with the location of the installation files. Do not change the path.

5. Enter the Oracle Home name and its full path:

   a. Enter or select a name for the Oracle Home in the Destination Name combo box.

   b. Enter or select the location for the Oracle components in the Destination Path combo box.

6. Click **Next**. The Available Products page appears (see Figure 39).

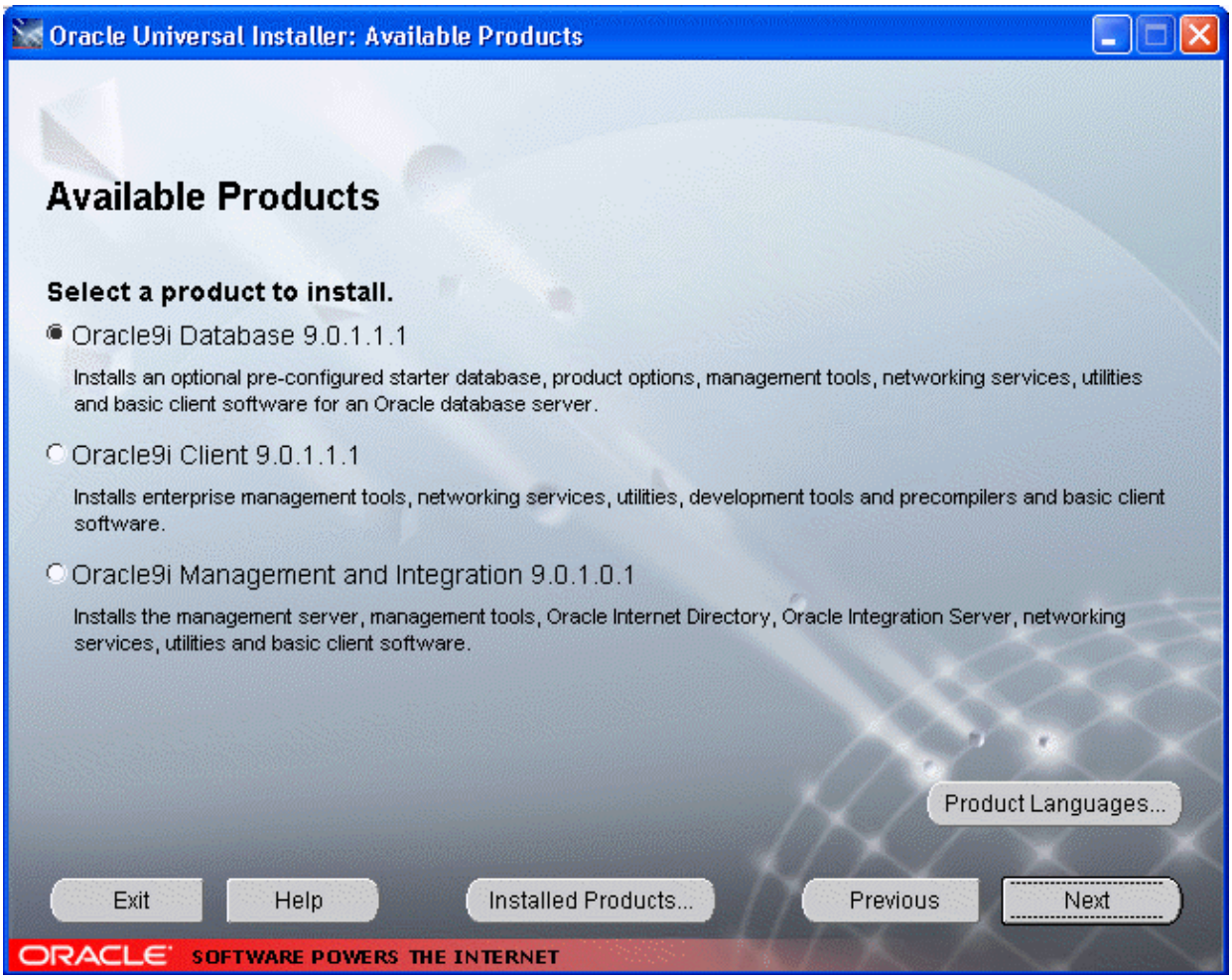

Figure 39. Oracle Universal Installer: Available Products page

7. Select the product to install.

8. Click **Next**. The Installation Types page appears (see Figure 40).

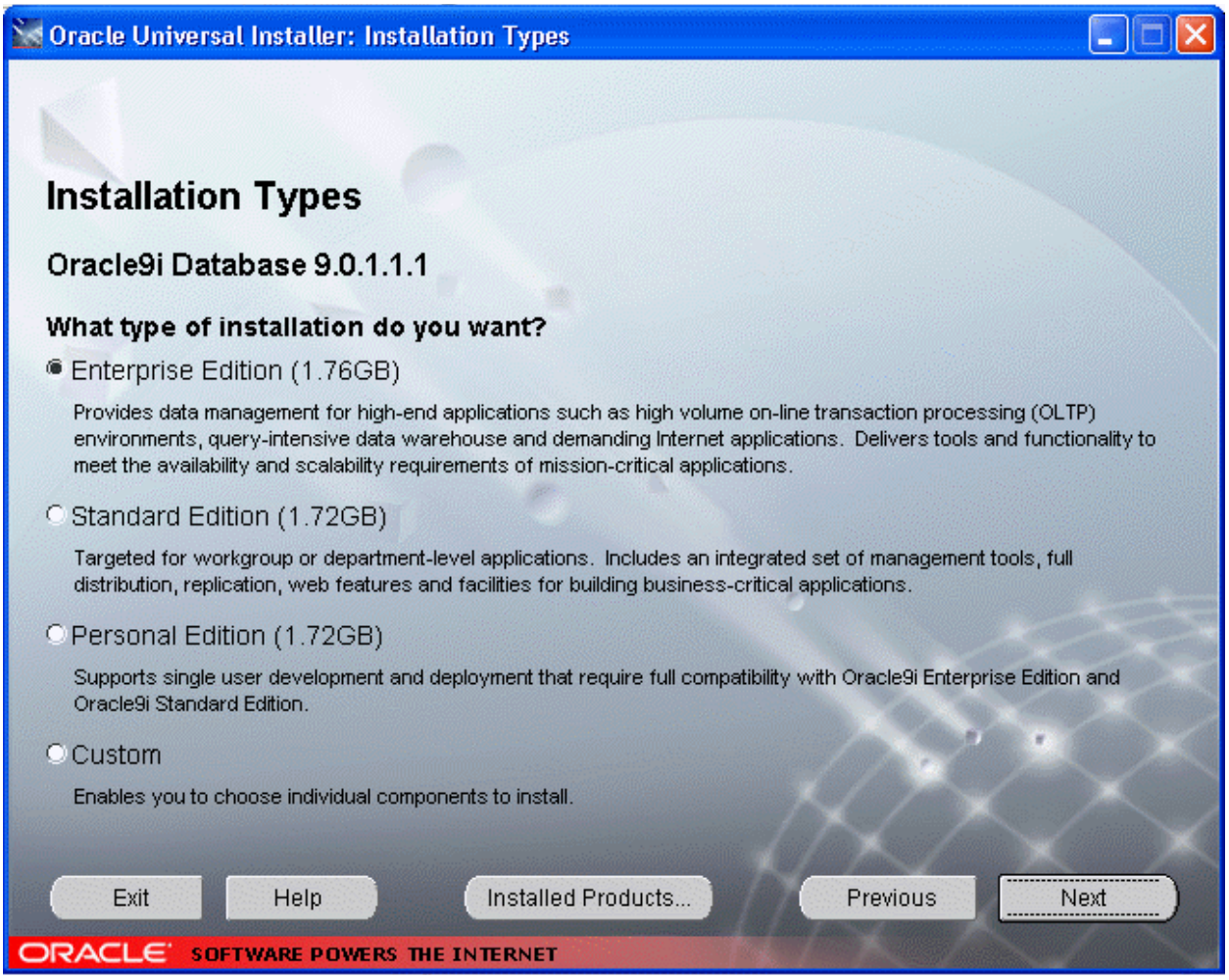

Figure 40. Oracle Universal Installer: Installation Types page

9. Select the type of installation.

10. Click **Next**. The Database Configuration page appears (see Figure 41).

Figure 41. Oracle Universal Installer: Database Configuration page

11. Select a database.

12. Click **Next**. The Database Identification page appears (see Figure 42).

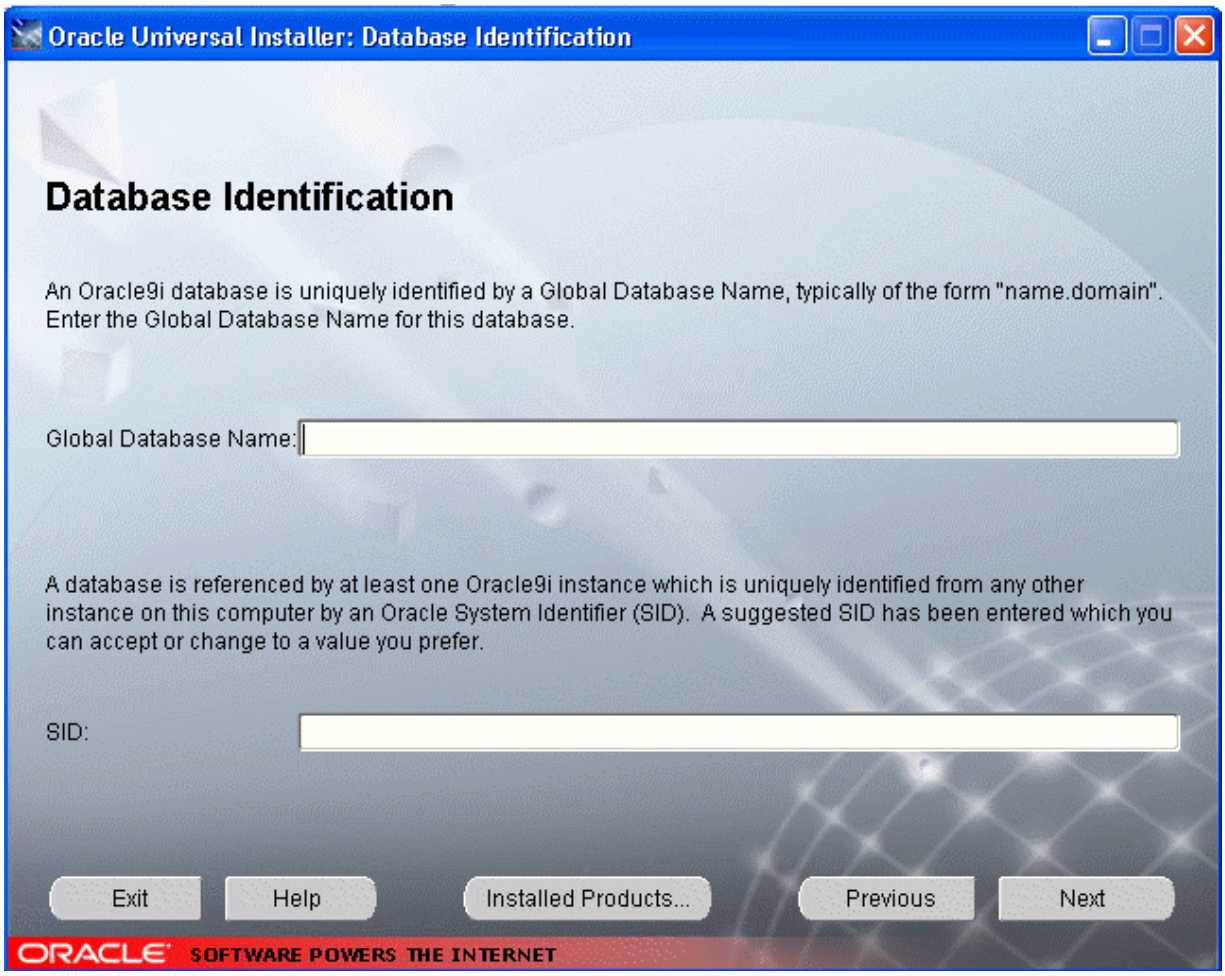

Figure 42. Oracle Universal Installer: Database Identification page

13. Enter the global database name for the database and the Oracle System Identifier (SID) name in the fields provided.

14. Click **Next**. The Database File Location page appears (see Figure 43).

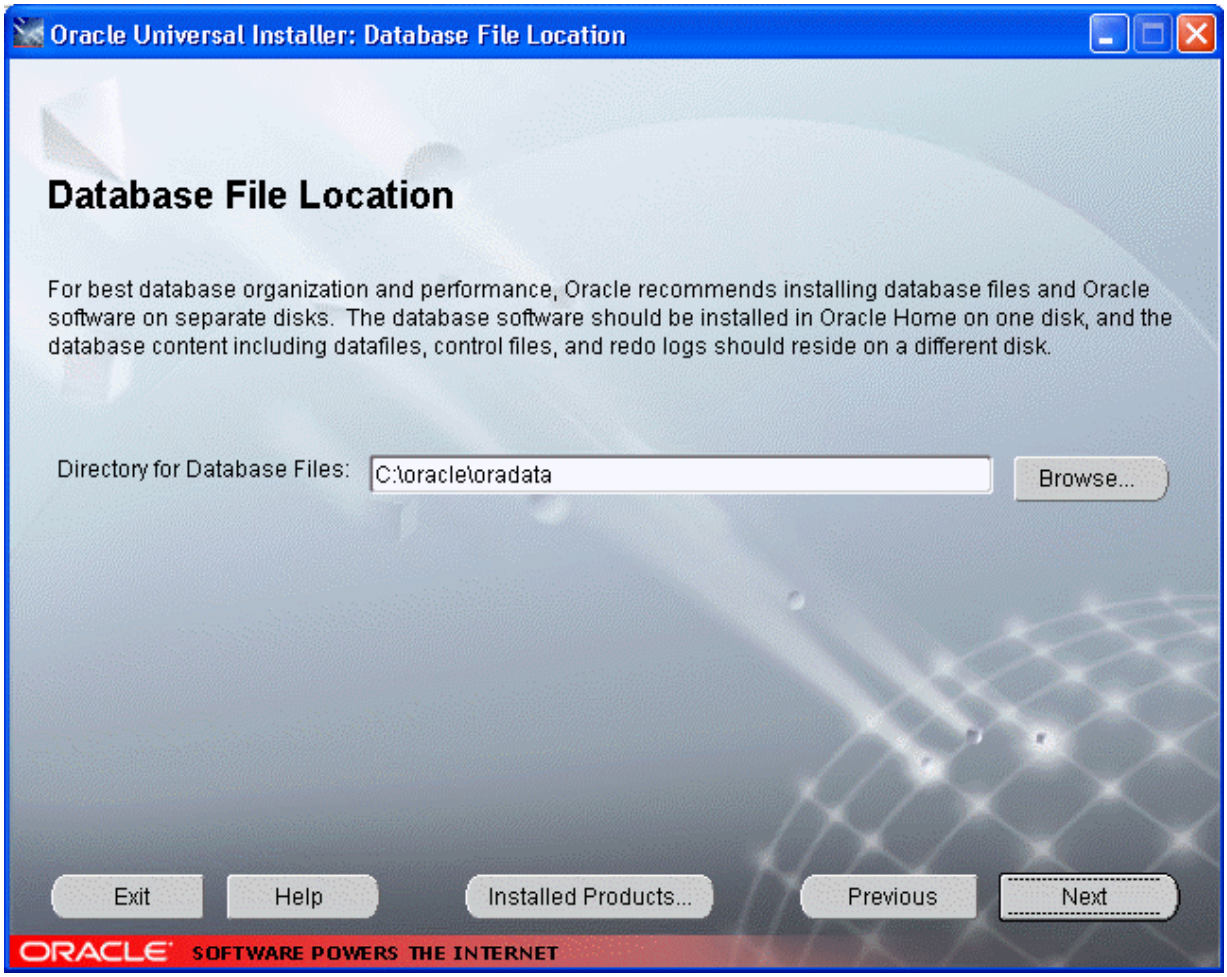

Figure 43. Oracle Universal Installer: Database File Location page

15. Enter the directory location for the database files. The directory location must be a mapped drive.

16. Click **Next**. The Database Character Set page appears (see Figure 44).

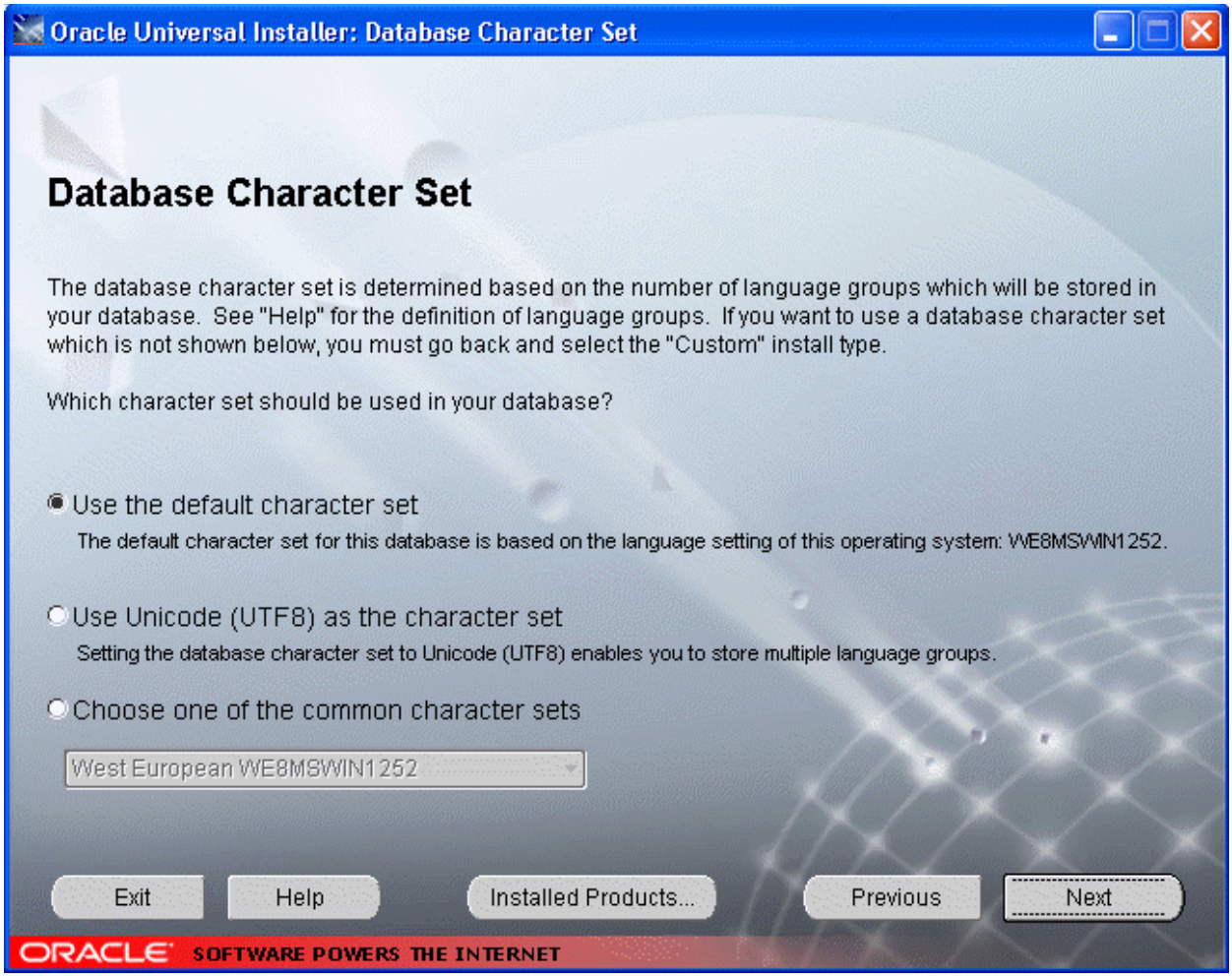

Figure 44. Oracle Universal Installer: Database Character Set page

17. Select the character set to use in your database.

18. Click **Next**. The Summary page appears (see Figure 45).

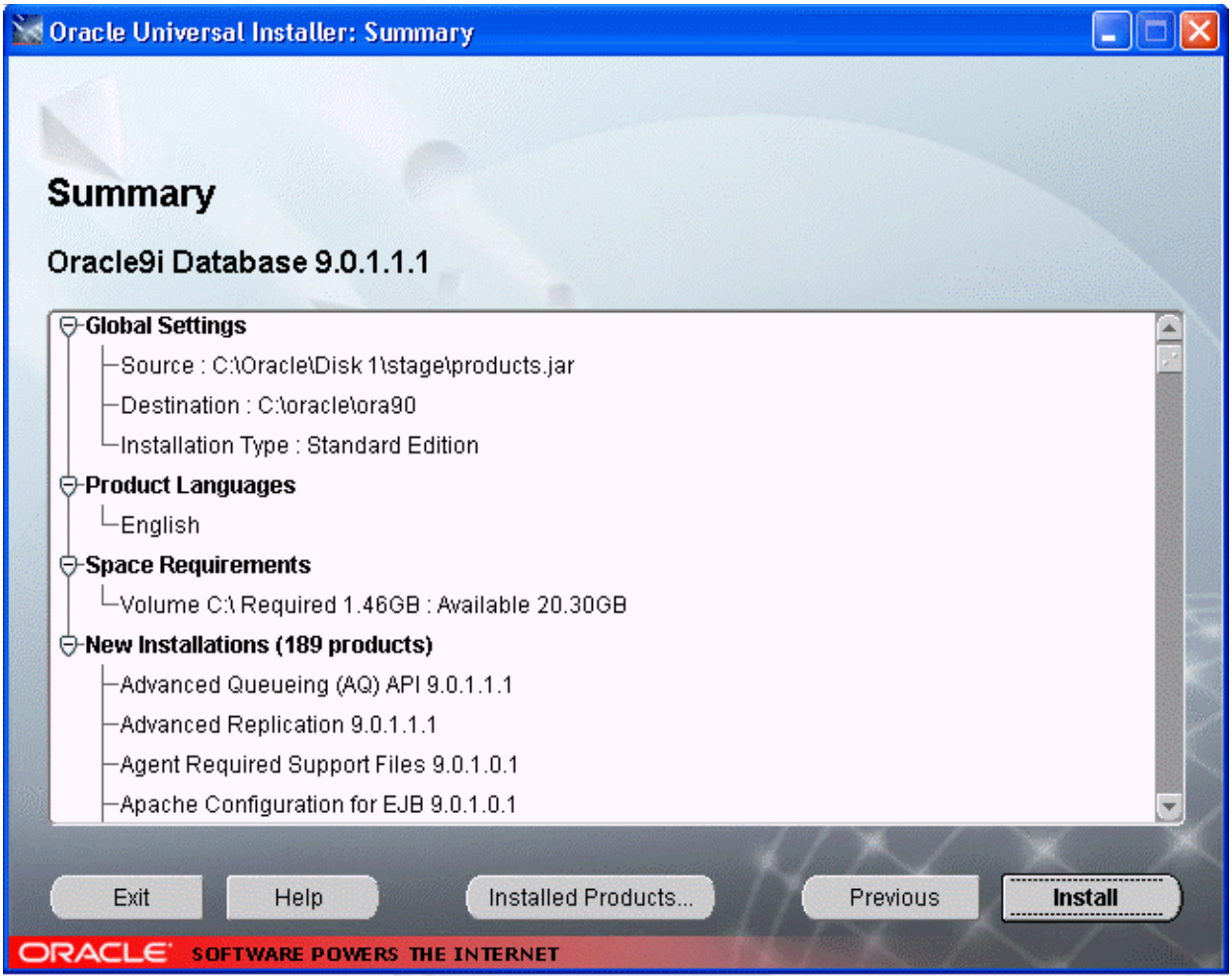

Figure 45. Oracle Universal Installer: Summary page

19. Review the space requirements in the Summary page to confirm that you have enough disk space.

20. Click **Install** to start the installation.

    When the installation is complete, the Configuration Tools page appears and a series of tools starts automatically to create and configure your database and Oracle Net Services environments.The Configuration Tools page displays the results of running these tools (see Figure 46).

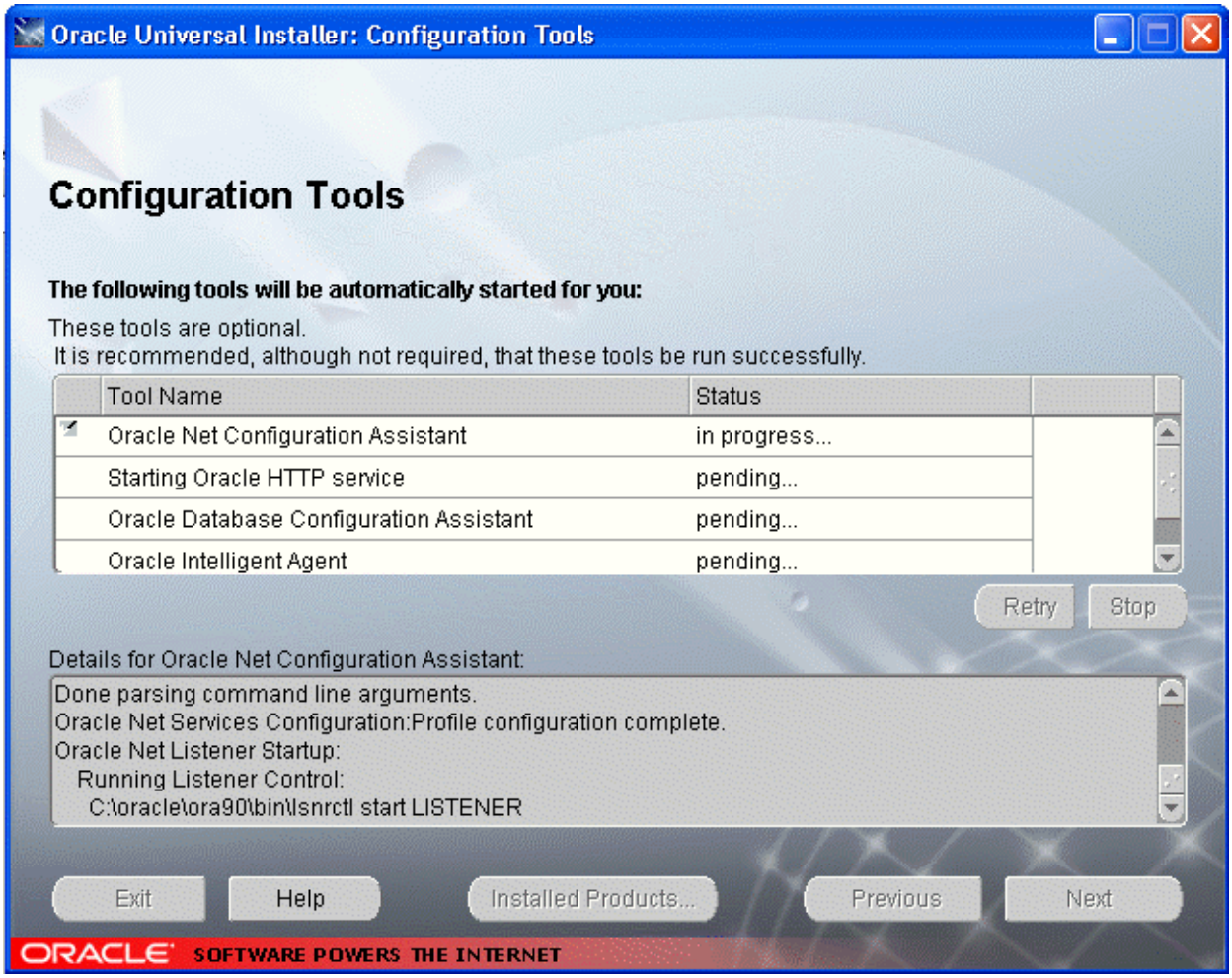

Figure 46. Oracle Universal Installer: Configuration Tools page

- If the Oracle Database Configuration Assistant tool runs, continue with step 21.
- If the Oracle Database Configuration Assistant tool does not run, go to step 22 on page 75.

21. If the Oracle Database Configuration Assistant tool runs, change the default passwords that it sets:

    a. After the tool completes, the Oracle Database Configuration Assistant dialog box opens (see Figure 47). Make of note of the database information that is listed in this dialog box.

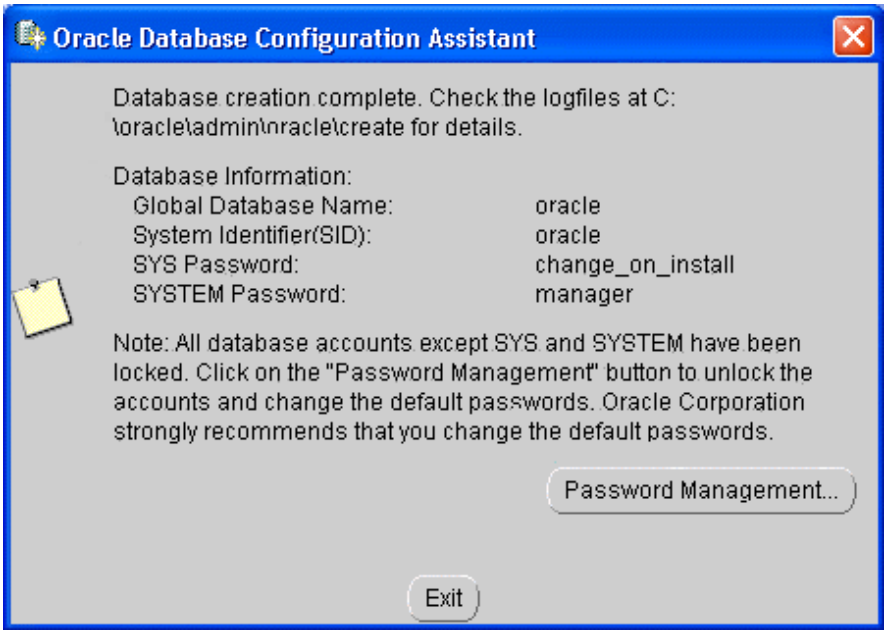

Figure 47. Oracle Database Configuration Assistant dialog box

b. Click **Password Management** to open the Password Management dialog box (see Figure 48).

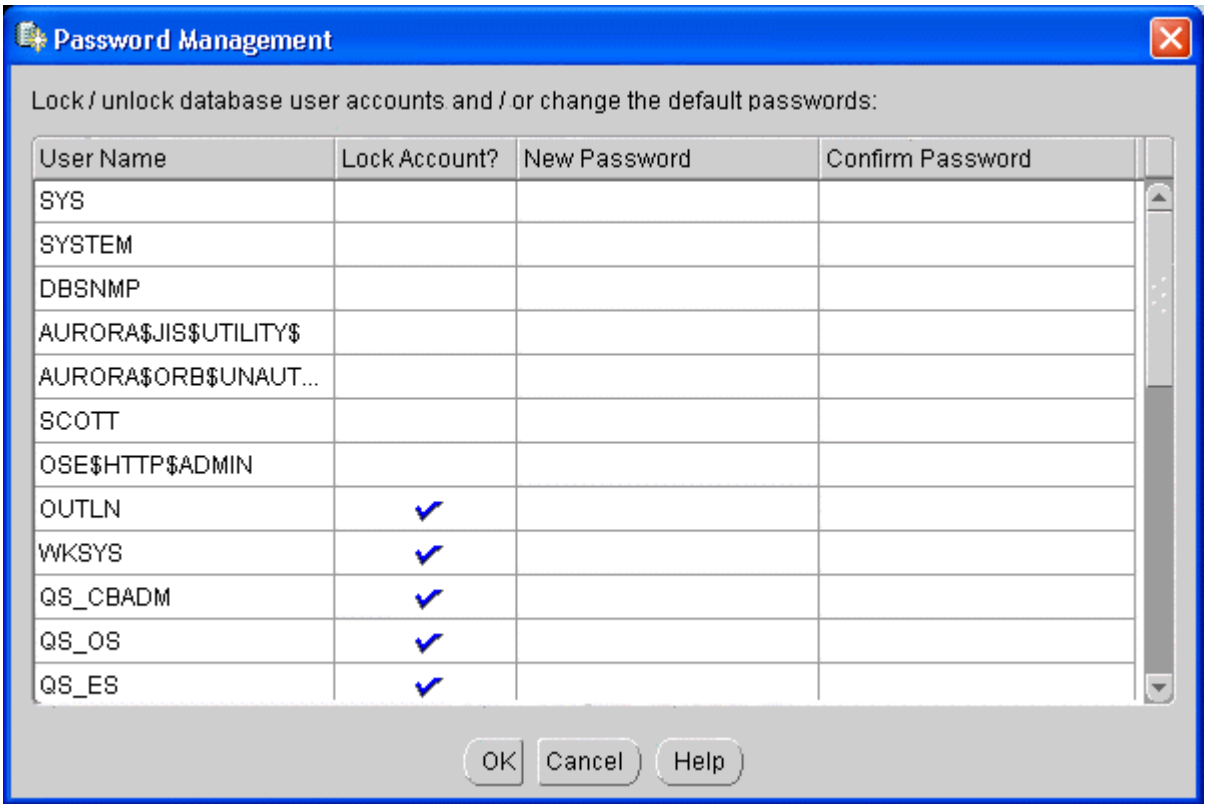

Figure 48. Password Management dialog box

c. Change the default passwords.

d. Lock or unlock the database user accounts as necessary.

e. Click **OK** to save the changes and close the dialog box.

22. When all of the tools in the Configuration Tools page have finished, click **Next**. The End Of Installation page appears.

23. Click **Exit** to exit from the Oracle Universal Installer. The database is installed.

Installing the Oracle Client

Install the Oracle Client software as follows:

1. Insert the Oracle Database Client compact disc. The Autorun installation program should start automatically. If it does not, locate and double-click the setup.exe file.

2. Click **Install/Deinstall Products** in the installation program. The Oracle Universal Installer: Welcome page appears.

   IMPORTANT Do not install Oracle software into an existing Oracle home that contains another installation of Oracle software. Deinstall any previous versions before installing a new version. See your documentation from Oracle for more information.

3. To remove a previous version of Oracle software before proceeding with this installation, click **Deinstall Products** to open the Inventory dialog box, select the previous version from the list, and click **Remove**.

4. Click **Next** in the Welcome page. The File Locations page appears (see Figure 49).

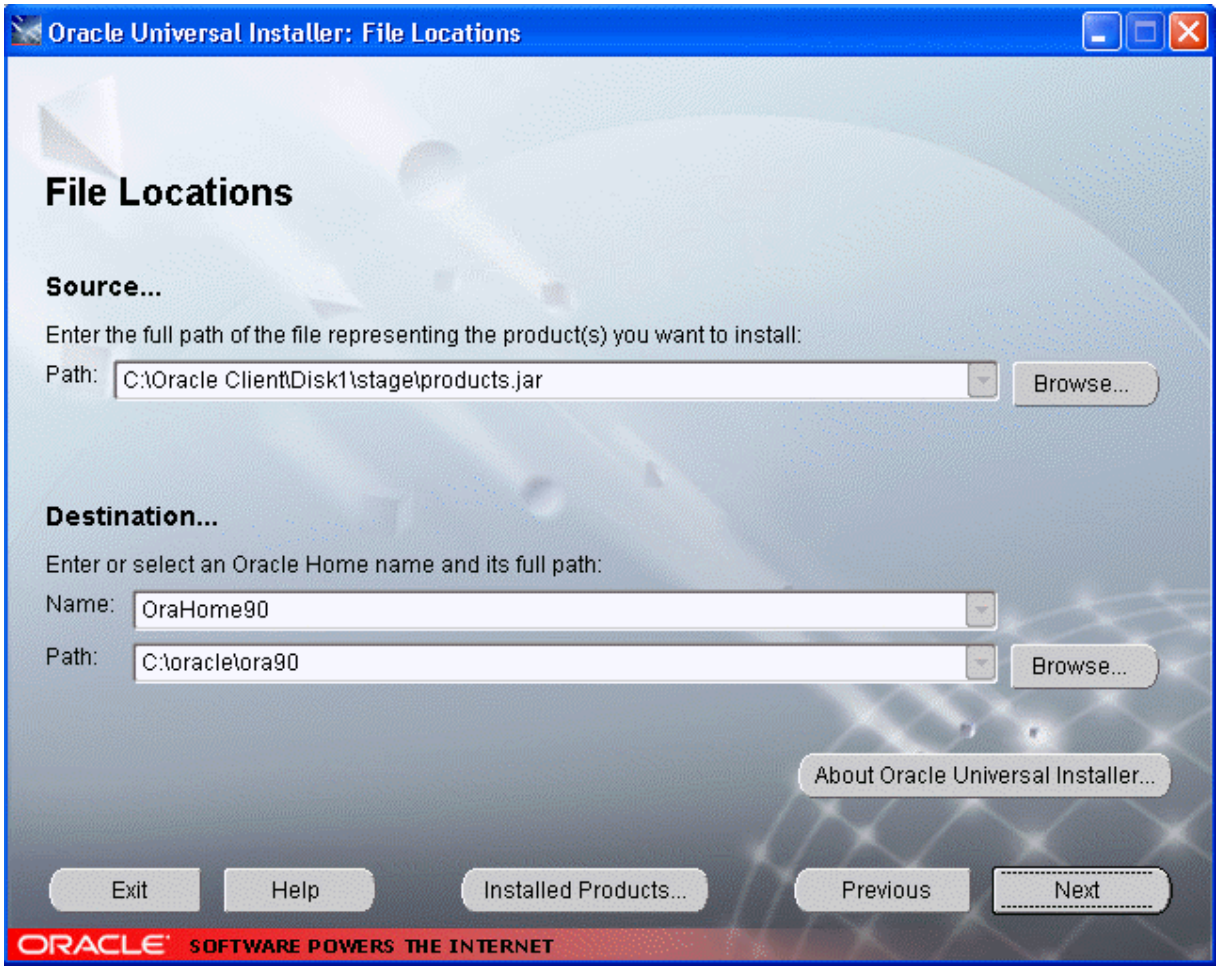

Figure 49. Oracle Universal Installer: File Locations page

IMPORTANT The Source Path combo box is filled in automatically with the location of the installation files. Do not change the path.

5. Enter the Oracle Home name and its full path:

   a. Enter or select a name for the Oracle Home in the Destination Name combo box.

   b. Enter or select the location for the Oracle components in the Destination Path combo box.

6. Click **Next**. The Installation Types page appears (see Figure 50) on page 78.

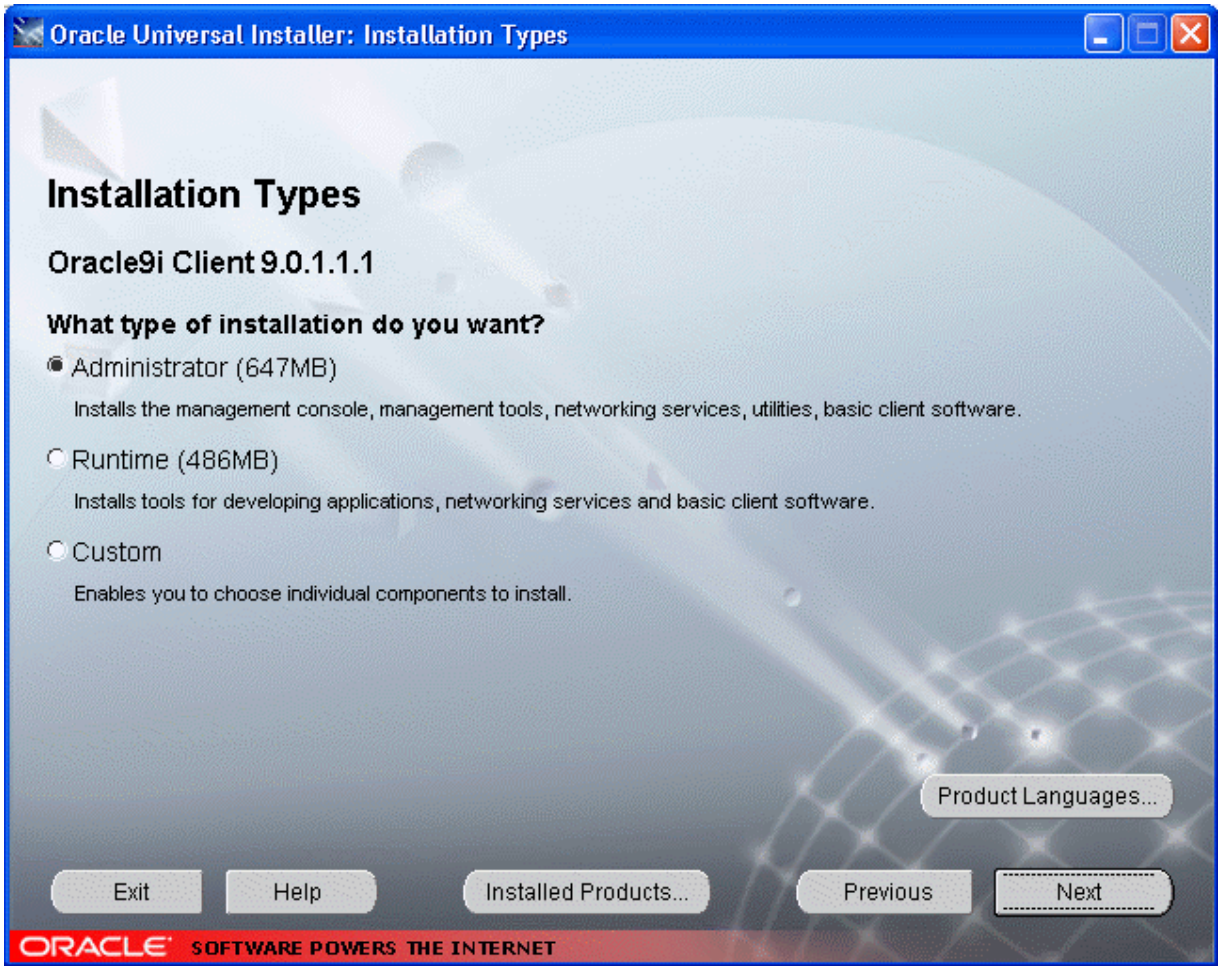

Figure 50. Oracle Universal Installer: Installation Types page

7. Select the type of installation.

8. Click **Next**. The Summary page appears (see Figure 51).

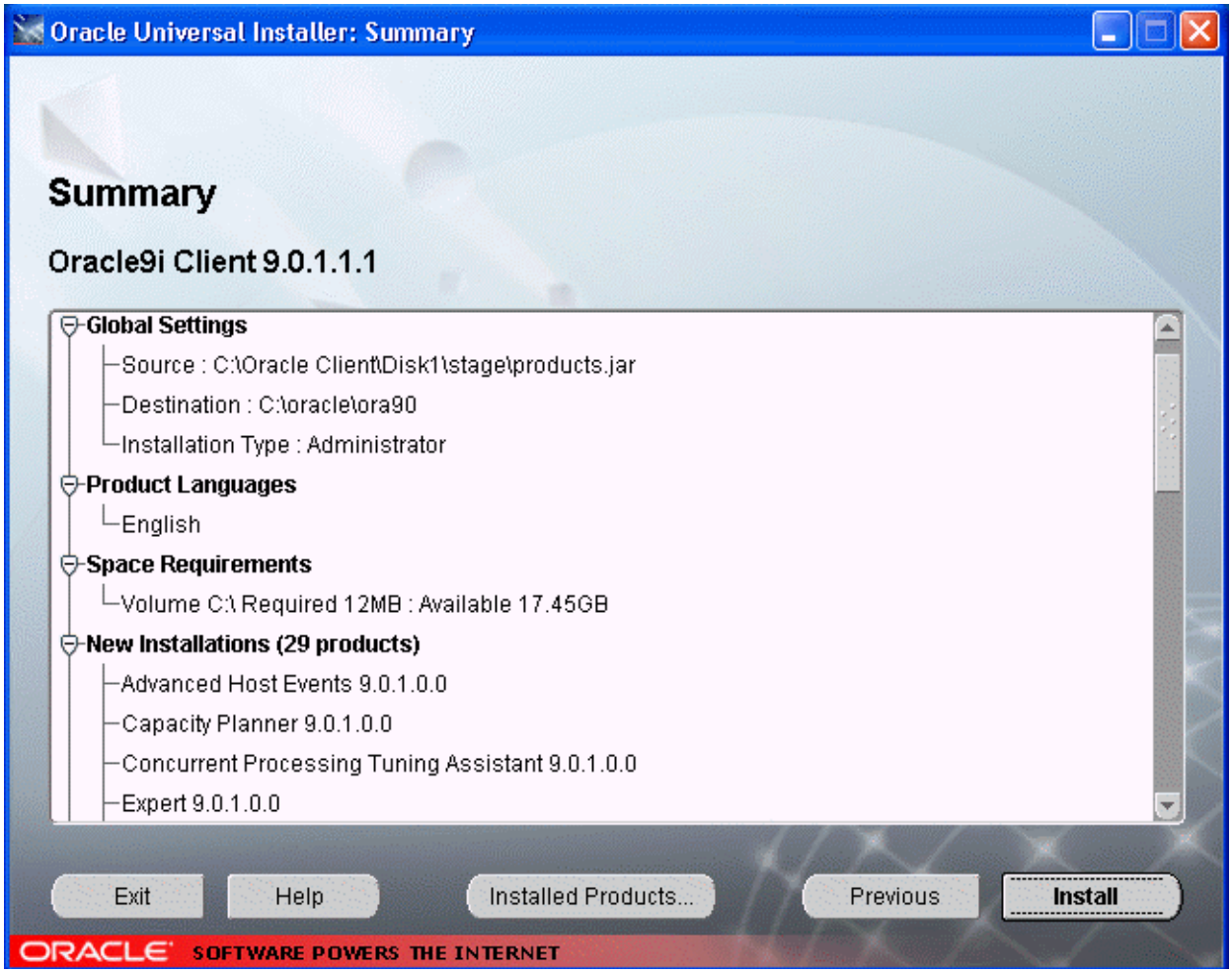

Figure 51. Oracle Universal Installer: Summary page

9. Review the space requirements in the Summary page to confirm that you have enough disk space.

10. Click **Install** to start the installation.

    When the installation is complete, the Configuration Tools page appears and a series of tools automatically starts to create and configure your database and Oracle Net Services environments. The Configuration Tools page displays the results of running these tools (see Figure 52).

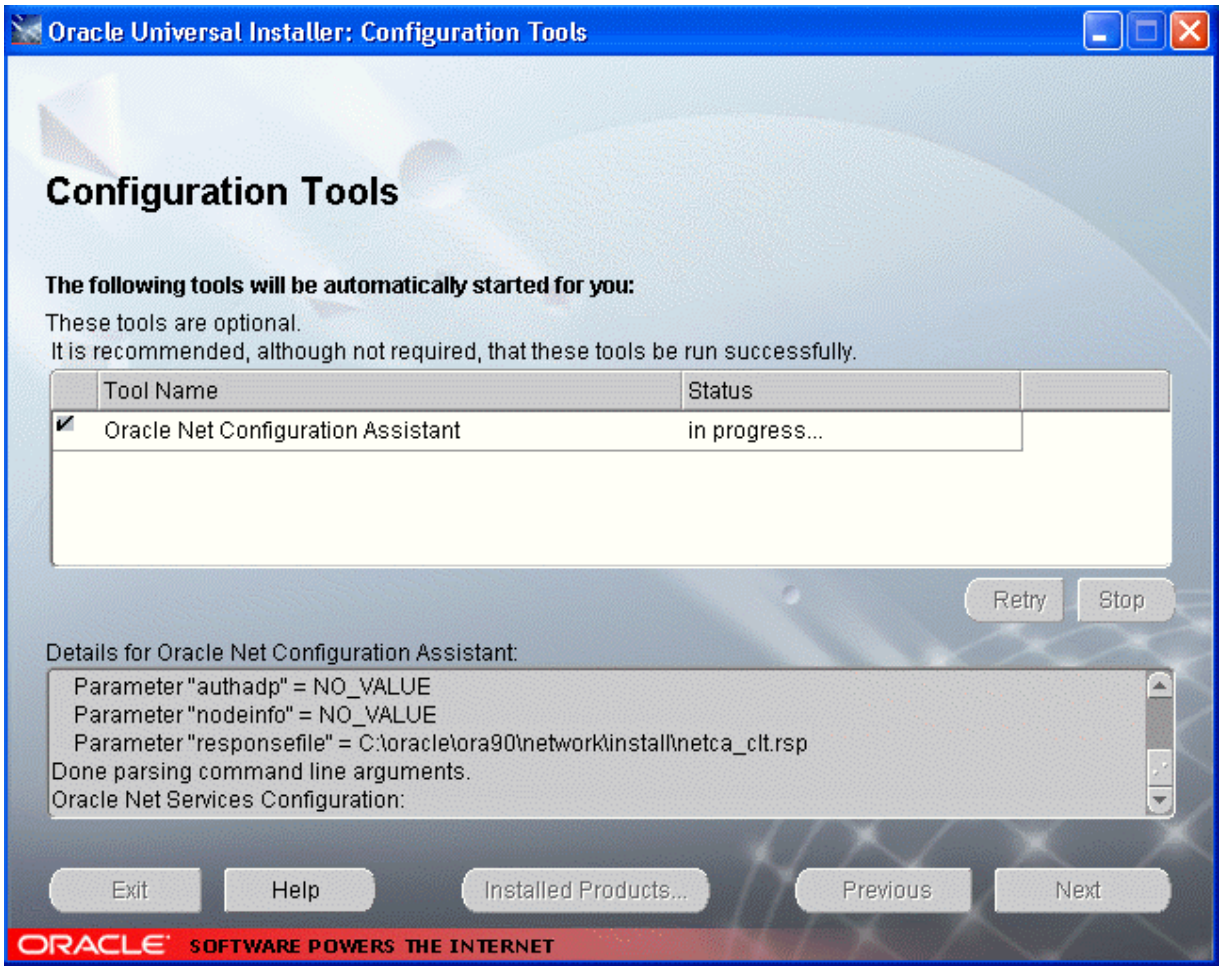

Figure 52. Oracle Universal Installer: Configuration Tools page

- If the Oracle Net Configuration Assistant runs (see Figure 53), continue with step 11.

Figure 53. Oracle Net Configuration Assistant: Welcome page

- If the Oracle Net Configuration Assistant does not run, go to step 24 on page 86.

11. Click the **No, I Will Create Net Service Names Myself** option.

12. Click **Next**. The Net Service Name Configuration, Database Version page appears (see Figure 54).

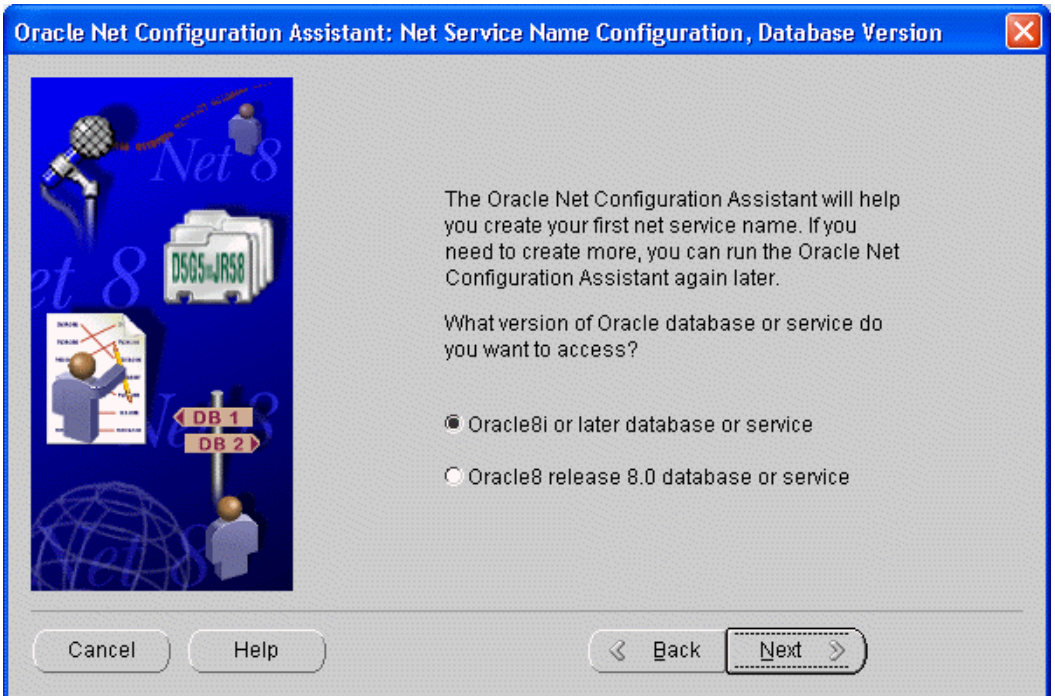

Figure 54. Oracle Net Configuration Assistant: Net Service Name Configuration, Database Version page

13. Click the **Oracle 8i Or Later Database Or Service** option.

14. Click **Next**. The Net Service Name Configuration, Service Name page appears (see Figure 55).

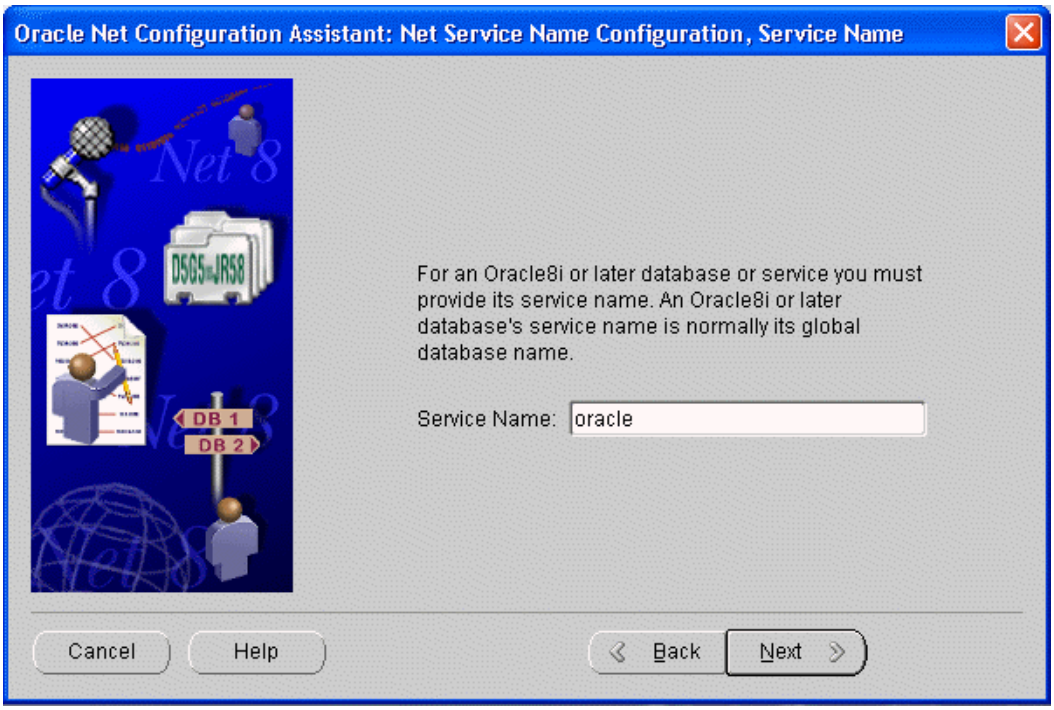

Figure 55. Oracle Net Configuration Assistant: Net Service Name Configuration, Service Name page

15. Enter the global database name.

16. Click **Next**. The Net Service Name Configuration, Select Protocols page appears (see Figure 56).

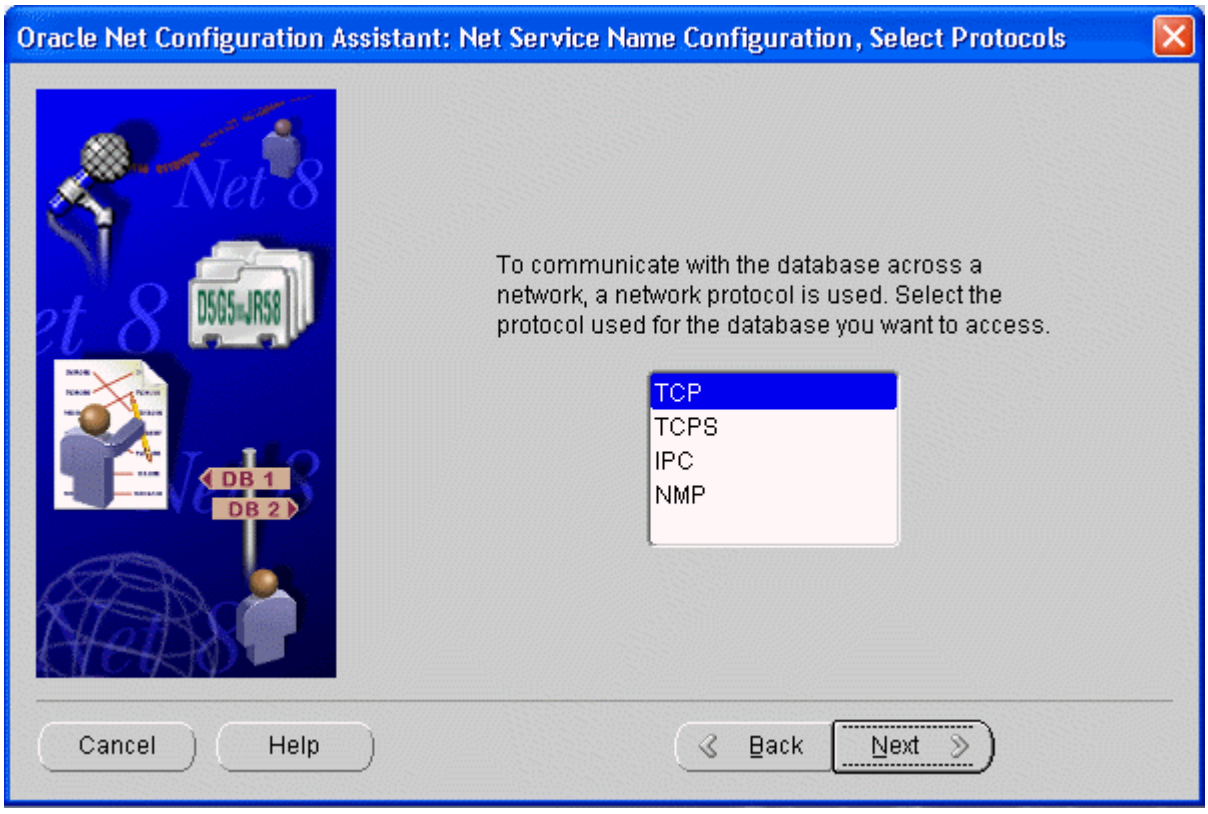

Figure 56. Oracle Net Configuration Assistant: Net Service Name Configuration, Select Protocols page

17. Select the protocol used for the database.

18. Click **Next**. The next page that appears depends on what protocol you selected.

    For example, if you selected the TCP protocol, the Net Service Name Configuration, TCP/IP Protocol page appears (see Figure 57).

19. Based on the choice of protocol, the software requests protocol parameter information. Complete the specification of the protocol and click **Next**.

For example, on the Net Service Name Configuration, TCP/IP Protocol page, type the host name for the computer where the database is located and click the Use Standard Port Number option (see Figure 57).

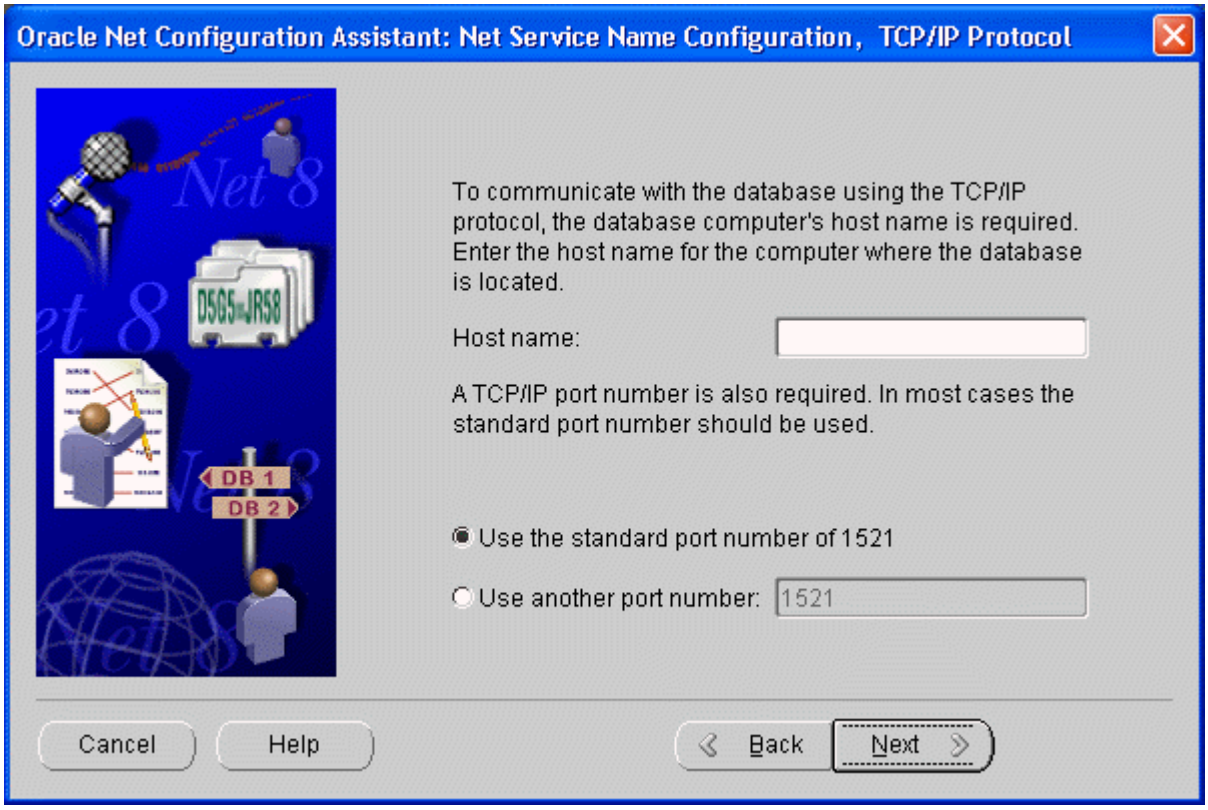

Figure 57. Oracle Net Configuration Assistant: Net Service Name Configuration, TCP/IP Protocol page

The Net Service Name Configuration test page appears.

20. On the Net Service Name Configuration, Test page, click the **Yes, Perform A Test** option and click **Next**. The Net Service Name Configuration, Connecting page appears and a connection test is performed.

    - If the test is successful, click **Next**. The Net Service Name Configuration, Net Service Name page appears (see Figure 58).

    - If the test fails, click **Back** to review the information that you entered. Make any necessary changes and try the test again.

21. On the Net Service Name Configuration, Net Service Name page, accept the default net service name or enter another net service name. The name you enter should be unique to the client.

22. Click **Next**. The Net Service Name Configuration, Another Net Service Name? page appears.

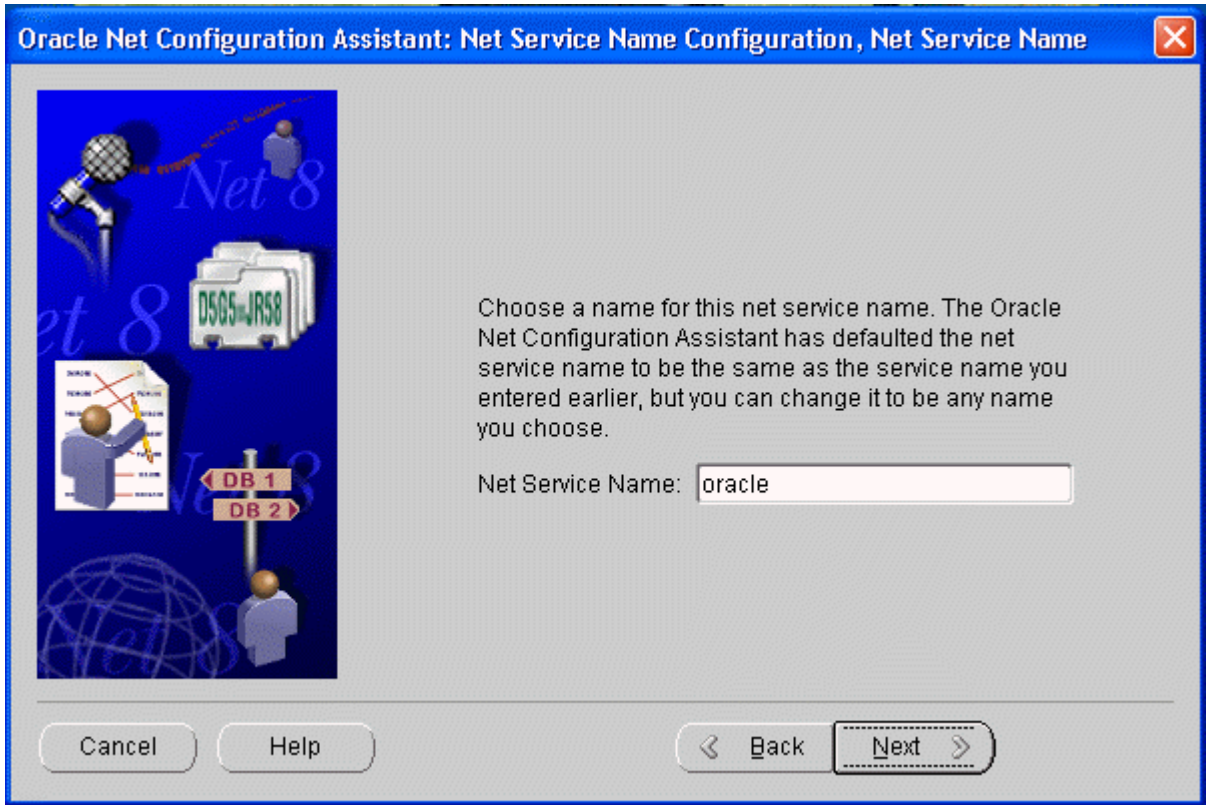

Figure 58. Oracle Net Configuration Assistant: Net Service Name Configuration, Net Service Name page

23. On the Net Service Name Configuration, Another Net Service Name? page, specify whether or not to configure another net service name for this client.

    - When you select Yes and click **Next**, the Oracle Net Configuration Assistant leads you through the process of configuring another net service name.

    - When you select No and click **Next**, the Net Service Name Configuration Done page appears. Click **Next** again and click **Finish** to complete the Oracle Net Configuration Assistant. You are returned to the Oracle Universal Installer: Configuration Tools page. (Figure 52)

24. On the Oracle Universal Installer: Configuration Tools page, click **Next**. The installation is complete.

Index

Numerics

A

C

D

E

F