thermoscientific

Thermo

TraceFinder

Administrator Console User Guide

Software Version 5.1

XCALI-98094 Revision A • December 2019

DOCUMENTATION SURVEY

ThermoFisher SCIENTIFIC

Release history: Revision A, December 2019

Software version: Microsoft Windows 7 Professional SP1 or Windows 10 x64 IoT Enterprise 2016 LTSB; (Thermo) Foundation 3.1 SP7, Xcalibur 4.3

For Research Use Only. Not for use in diagnostic procedures.

Contents

Preface

This guide discusses the features of the Thermo TraceFinder™ Administrator Console. This console is available to any user with Admin Console permission.

When Security is not enabled, all users have full TraceFinder application permissions when they log in. The first user to log in to the Administrator Console and the Windows Administrators group (either local or domain) is given Security permissions. See Role Permission Defaults.

IMPORTANT The Thermo TraceFinder Workflow Service requires that users log on to the computer with a Windows password. If you attempt to access this service on a computer without password protection, an error message prompts you to create a Windows password, reboot, and log on with the password.

Tip (Animation) To view "Administrator Console Overview," choose **Help > Animations**.

Contents

❖ **To suggest changes to the documentation or to the Help**

Complete a brief survey about this document by clicking the button below. Thank you in advance for your help.

Accessing Documentation

The TraceFinder application includes Help and these manuals as PDF files:

- *TraceFinder User Guide*
- *TraceFinder Lab Director User Guide*
- *TraceFinder Administrator Console User Guide*

- *TraceFinder Acquisition Quick Reference Guide*
- *TraceFinder Analysis Quick Reference Guide*
- *TraceFinder Shortcut Menus Quick Reference Guide*

❖ To view TraceFinder documents using the Start menu

From the Microsoft™ Windows™ taskbar choose **Start > All Programs > Thermo TraceFinder 5.1 > Manuals**.

❖ To view user documentation from the Thermo Fisher Scientific website

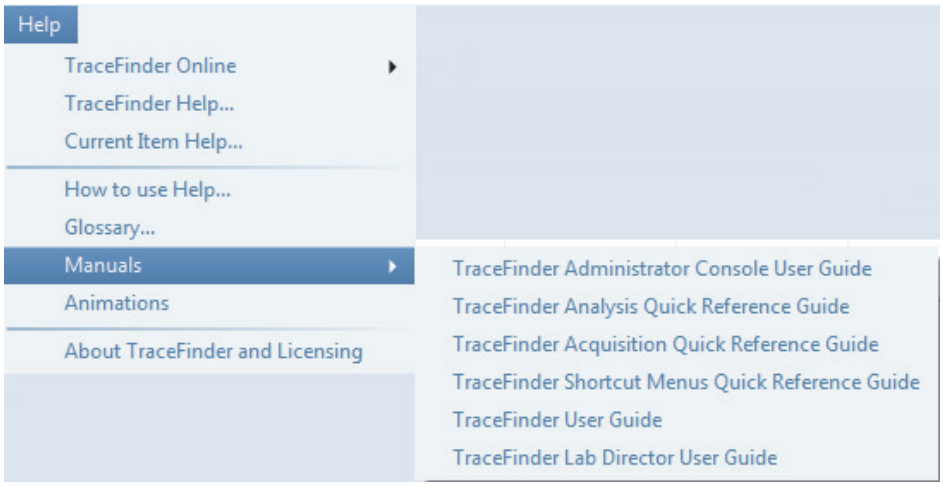
1. Go to thermofisher.com.
2. Click the **Services & Support** tab.
3. On the right, click **Manuals & Protocols**.
4. In the Refine Your Search box, search by the product name.
5. From the results list, click the title to open the document in your web browser, save it, or print it.

   To return to the document list, click the browser **Back** button.

❖ To open TraceFinder Help and access related documents from the application

1. Open the TraceFinder application and choose **Help > TraceFinder Help.**
   - To find a particular topic, use the Contents or Search panes.
   - To create your own bookmarks, use the Favorites pane.
2. To view the user guides or the quick reference guides, choose **Help > Manuals > *PDF file***.

Figure 1. PDF files available from the Help menu



The PDF file of the selected document opens in a new window.

Special Notices

This guide includes the following types of special notices:

IMPORTANT Highlights information necessary to prevent damage to software, loss of data, or invalid test results; or might contain information that is critical for optimal performance of the system.

Note Highlights information of general interest.

Tip Highlights helpful information that can make a task easier.

Contacting Us

Contact	Email	Telephone	QR Code[a]
U.S. Technical Support	us.techsupport.analyze@thermofisher.com	(U.S.) 1 (800) 532-4752	
U.S. Customer Service and Sales	us.customer-support.analyze@thermofisher.com	(U.S.) 1 (800) 532-4752	
Global support	❖ **To find global contact information or customize your request** 1. Go to thermofisher.com. 2. Click **Contact Us**, select the country, and then select the type of support you need. 3. At the prompt, type the product name. 4. Use the phone number or complete the online form. ❖ **To find product support, knowledge bases, and resources** Go to thermofisher.com/us/en/home/technical-resources. ❖ **To find product information** Go to thermofisher.com/us/en/home/brands/thermo-scientific.		

Note To provide feedback for this document, go to surveymonkey.com/s/PQM6P62 or send an email message to Technical Publications (techpubs-lcms@thermofisher.com).

[a] You can use your smartphone to scan a QR Code, which opens your email application or browser.

Accessing the Administrator Console

The Administrator Console is available from the Tools menu in any TraceFinder application window or from the Windows™ Start menu when you install the TraceFinder application.

Follow these procedures:

- To log in to the Administrator Console when user security is not enabled
- To log in to the Administrator Console when user security is enabled

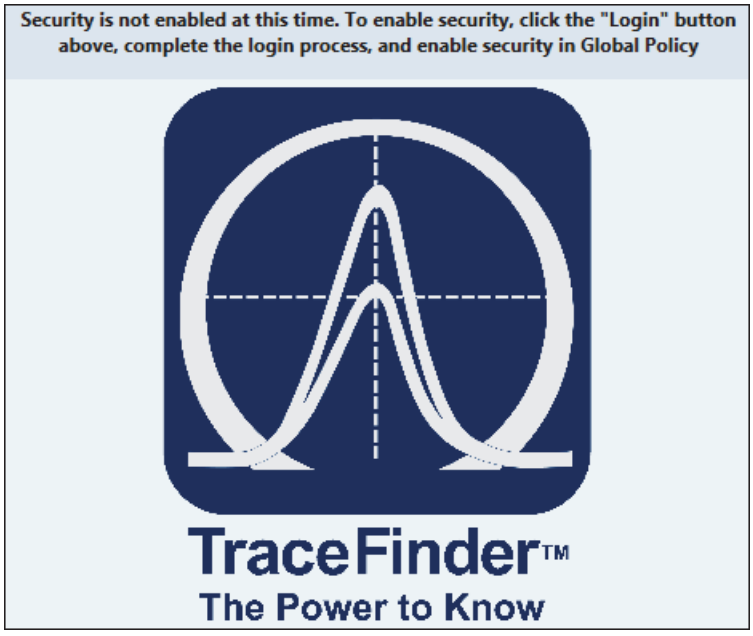
❖ To log in to the Administrator Console when user security is not enabled

1. Do one of the following:
   - Choose **Start > All Programs > Thermo TraceFinder 5.1 > TraceFinder Administration Console**.
   - From the TraceFinder main menu, choose **Tools > Administrator Console**.

   –or–

   - On your desktop, double-click the **TraceFinder 5.1 Administration Console** icon,  .

   The TraceFinder Administrator Console window opens, notifying you that user security is not enabled.

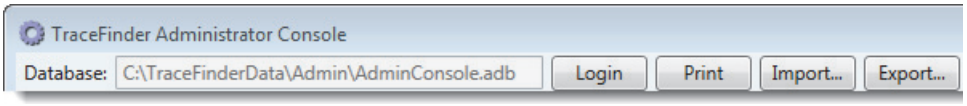


You can proceed without enabling user security and still have access to all Administrator Console features except the security features.

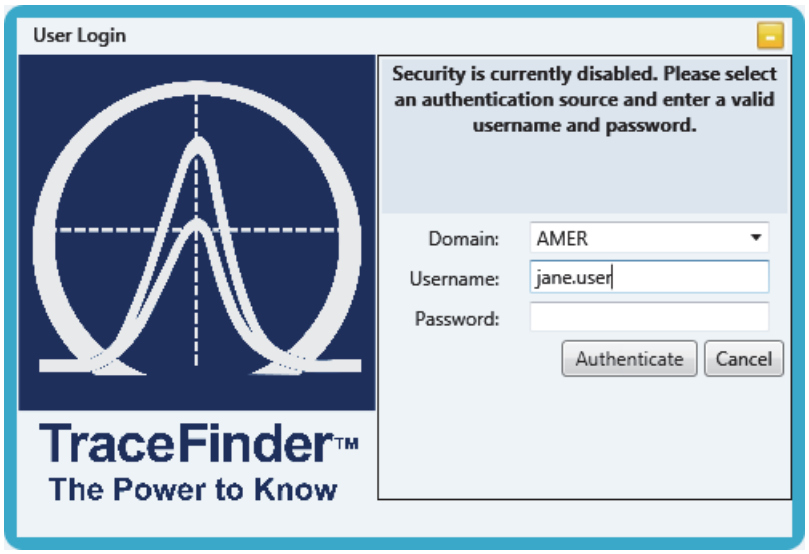
Note You must enter a valid Windows user name and password before you can access the security features.

2. To access the security features, do the following:

   a. Click **Login**.



   The User Login dialog box opens.



   b. Select a domain, either your Windows Active Directory™ domain or your local Windows computer name.

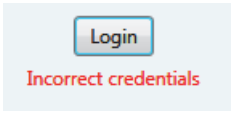
   c. Type your user name.

   d. Type your password.

   e. Click **Authenticate**.

      The application authenticates your login and password and opens the TraceFinder Administrator Console.

      If the authentication fails, the application displays Incorrect Credentials.



      The error might be with any of the login parameters. Enter your user name and password again, or contact your system administrator.

3. To turn on user security, requiring all users to log in each time they start the TraceFinder application, see To enable security.

❖ To log in to the Administrator Console when user security is enabled

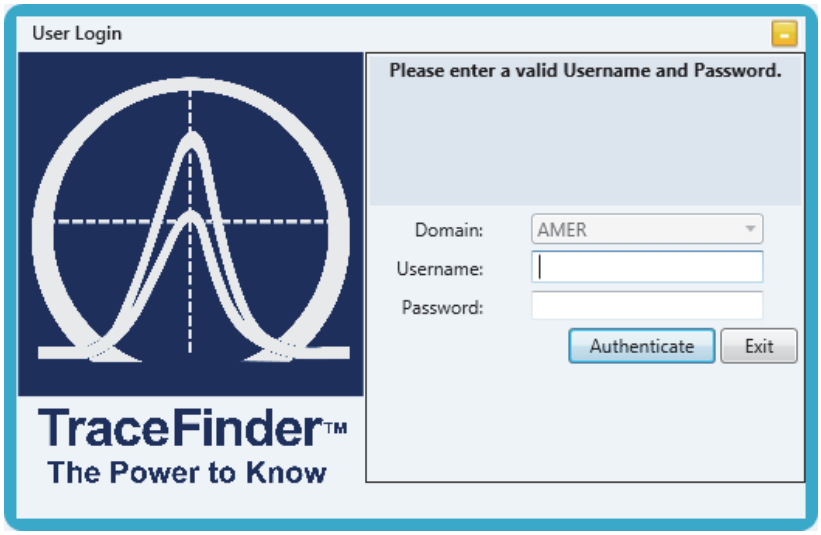
1. Do one of the following:

   - Choose **Start > All Programs > Thermo TraceFinder 5.1 > TraceFinder Administration Console**.
   - From the TraceFinder main menu, choose **Tools > Administrator Console**.

   –or–

   - On your desktop, double-click the **TraceFinder 5.1 Administration Console** icon,  .

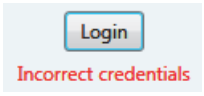
   The TraceFinder Administrator Console window opens to the User Login page.



2. Select a domain, either your Windows Active Directory domain or your local Windows computer name.
3. Type your user name.
4. Type your password.
5. Click **Authenticate**.

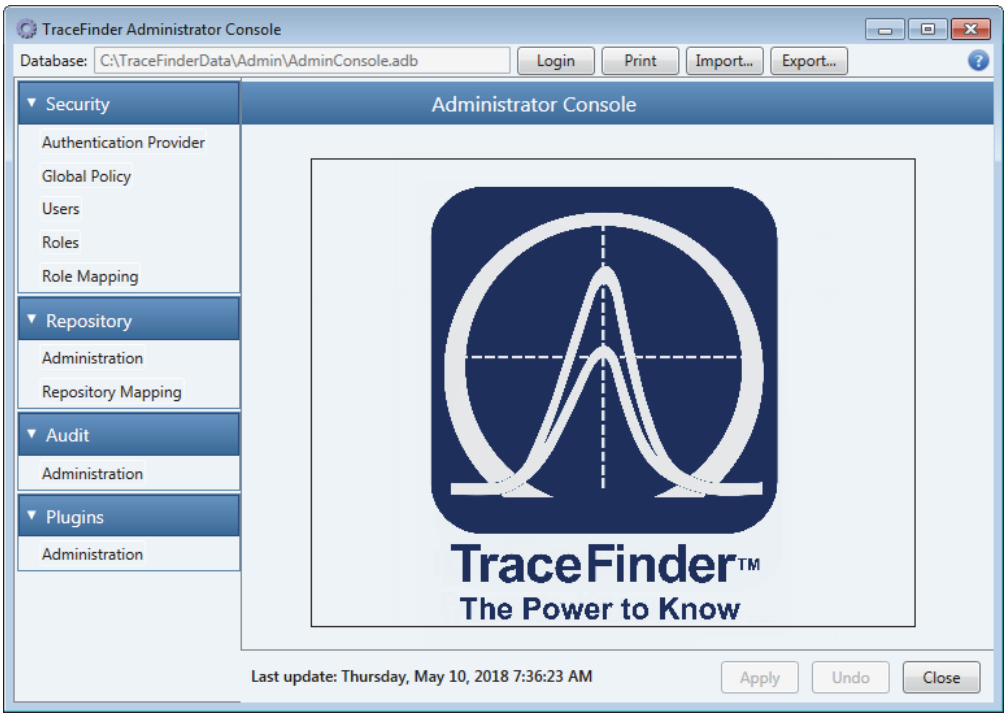
   The application authenticates your login and password and opens the TraceFinder Administrator Console.

   If the authentication fails, the application displays Incorrect Credentials.



   The error might be with any of the login parameters. Enter your user name and password again, or contact your system administrator.

Administrator Console



You can access the following functions of the Administrator Console from the left navigation pane and the top menu bar.

Function	Description
Security	Use the Security view to specify how the application manages authentication, to create and manage users, to map groups to roles and roles to users, or to select specific permissions for all user roles. See Using the Security View.
Repository	Use the Repository view to specify repositories for batches, methods, or templates that you create. See Using the Repository View.
Audit	Use the Audit view to specify the events that are audited, that require confirmation, or that require a sample authorization. See Using the Audit View.
Plugins	Use the Plugins view to configure available plugins for the TraceFinder application. See Using the Plugins View.
Login	Use the Login button to access the security features.
Print	Use the Print button to save your administrator settings to a PDF file. See Printing the Administrator Settings.
Import Export	Use the Import button to import saved security settings to your current Administrator Console. Use the Export button to save your current security settings to a file. See Importing and Exporting Administrator Settings.

1

Using the Security View

When you enable security, a user with Security permission can choose authentication providers, specify how the application manages authentication, create and manage users, map groups to roles and roles to users, and select specific permissions for all user roles.

Tip (Animation) To view "Using Security Features," choose **Help > Animations**.

Contents

Authentication Provider

Use the features on the Security – Authentication Provider page to select a method for authenticating user security.

❖ **To specify how user authentication is implemented**

1. Click **Authentication Provider** in the navigation pane.

   The Security – Authentication Provider page opens. The application displays the current authentication provider.

- **Local Windows**: Uses the local Windows user login and password to allow access to the TraceFinder application. To be allowed access, users must have a Windows user account on the local machine.
- **Active Directory Domain**: Uses the selected Active Directory domain to allow access to the TraceFinder application. To be allowed access, users must be members of the selected domain.

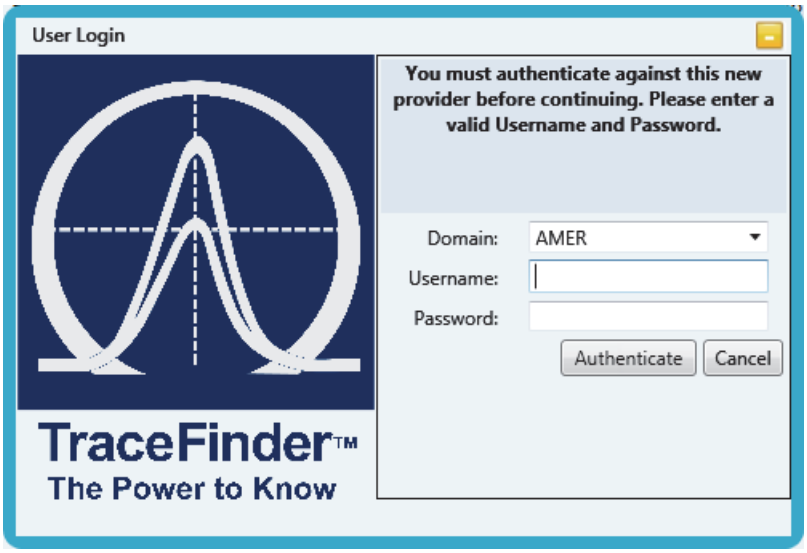
IMPORTANT

- If a user's computer is part of a Windows Active Directory and the TraceFinder security features specify the Active Directory as the authentication provider, you must change the authentication provider to a local Windows account before removing the computer from the Active Directory domain.
- Ensure that the user has sufficient security permissions to open the Administrator Console before you remove their computer from the domain. Otherwise, the user cannot run the TraceFinder application.

To activate these options for user authentication, you must enable security on the Security – Global Policy page.

2. To choose a different authentication provider, click **Select**.

   The User Login dialog box opens.



3. Select a domain.
4. Type your user name and password for the selected domain.
5. Click **Authenticate**.

   The application authenticates the specified domain, user name, and password. If the authentication fails, enter your user name and password again or click **Cancel** to remain logged in to the current domain.

Global Policy

Use the features on the Security – Global Policy page for controlling user security, automatic logoff, and access to the TraceFinder application.

Follow these procedures:

- To enable security
- To enable automatic screen locking
- To allow access without logging in
- To restrict access only to users created in TraceFinder
- To change the security account

❖ To enable security

1. Select the **Enable Security** check box.

   The application enables the features on the Global Policy page.

2. Click **Apply**.

   When you enable user security, users must log in with their user name and password. The application uses the authentication method you specify to authenticate the user name and password.

   IMPORTANT Clearing the Enable Security check box disables the password requirement in the audit Confirm Changes dialog box. See Esignatures.

❖ To enable automatic screen locking

1. Select the **Lock Client That Has No Interaction for *x* Minutes** check box.

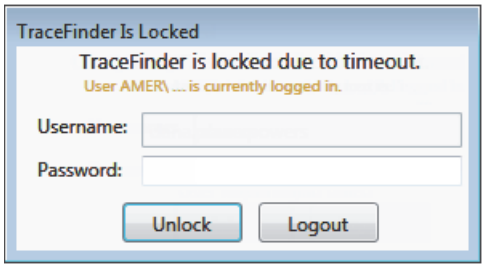
   Note This feature is available only when you select the Enable Security check box.

   Note You cannot use this feature with the Silent Authentication features.

2. In the Minutes box, type the number of minutes of inactivity before the application locks the screen and prompts the user to reenter the password.

   You can enter a number between 1 and 999 minutes (999 minutes = ~16 hours).

After the specified number of minutes elapses with no activity from a user, the TraceFinder application displays a lock screen with a login box.



While the password-protected lock screen is active, the TraceFinder application continues to perform all functions in the queue: analysis, acquisition, processing, and reporting.

3. When you have completed all your changes to the Security – Global Policy page, click **Apply**.

❖ To allow access without logging in

1. Select the **Silent Authentication** check box.

Note This feature is available only when you select the Enable Security check box.

Note You cannot use this feature with the Lock Client … feature.

IMPORTANT Enabling Silent Authentication disables the password requirement in the audit Confirm Changes dialog box.

2. Click **Apply**.

A TraceFinder user who is currently logged in to Windows can access the TraceFinder application without logging in again, even with user security enabled. The TraceFinder application authenticates the user and starts without requiring a user name and password.

IMPORTANT When a user is assigned to multiple roles, the user must choose which role they want to use for the session.

IMPORTANT This feature allows access only to verified TraceFinder users. See Users.

❖ To restrict access only to users created in TraceFinder

1. Select the **Authenticate Explicit Users Only** check box.

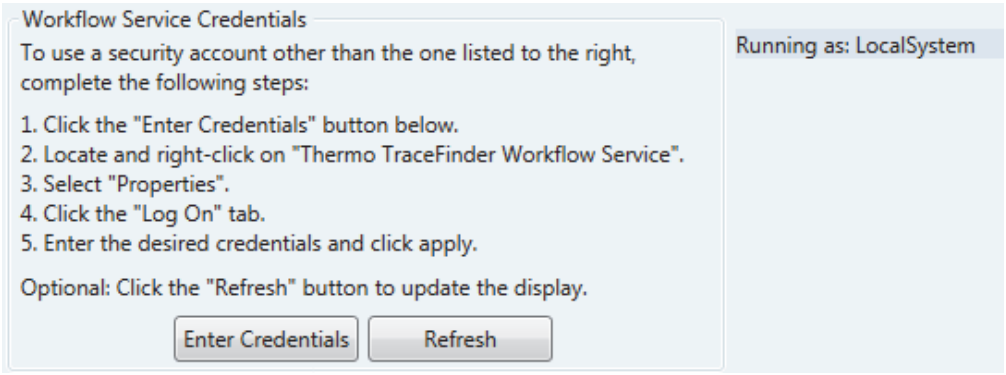
Note This feature is available only when you select the Enable Security check box.

2. Click **Apply**.

The only users who can access the TraceFinder application are those listed in the Users list on the Users page. See Users. Users cannot access the application if their user permissions are granted only through group membership.

❖ To change the security account

IMPORTANT When you use network repositories, you must use a custom workflow service account to specify an Active Directory Domain. You cannot use the default Local System account. See Chapter 2, "Using the Repository View."



1. Click **Enter Credentials**.

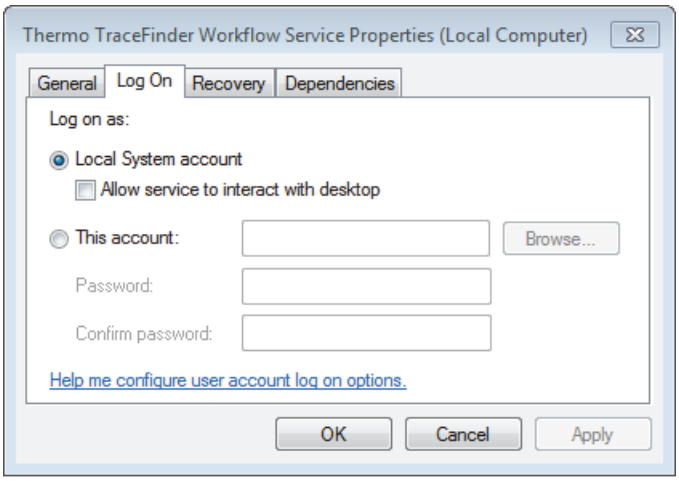
   The Services window opens.

2. Widen the Name column to see the entire workflow name.
3. Locate and right-click **Thermo TraceFinder Workflow Service.**
4. Choose **Properties** from the menu.

   The Thermo TraceFinder Workflow Service Properties dialog box opens.

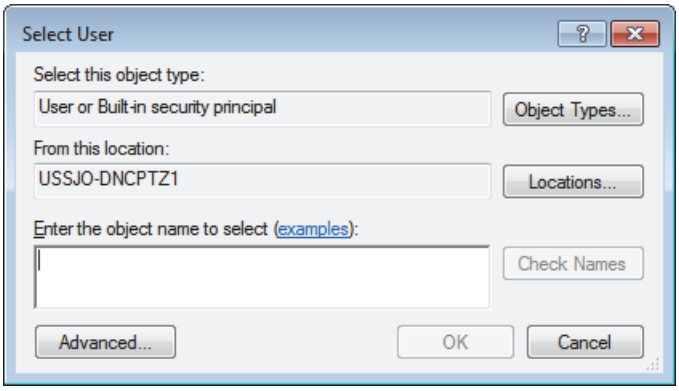
5. Click the **Log On** tab.

Figure 2. Thermo TraceFinder Workflow Service Properties dialog box



6. To change from a custom account to the default local account, select the **Local System Account** option and then click **OK**.
7. To change from the default local system account to an account that you identify, do the following:
   a. Select the **This Account** option.
   b. Click **Browse**.

      The Select User dialog box opens, where you can identify new accounts.



   c. In the Enter the Object Name to Select box, type an identifier for the account.

      Use the following syntax:

      - DisplayName (example: **FirstName LastName**)
      - ObjectName (example: **Computer1**)
      - UserName (example: **User1**)
      - ObjectName@DomainName (example: **User1@Domain1**)
      - DomainName\ObjectName (example: **Domain1\User1**)

      Note For example, to identify an account for your user login, use the following syntax: **jane.user@thermofisher.com**.

   d. To verify the account, click **Check Names**.

      The system confirms the object name you entered.

   e. Click **OK**.
   f. In the Thermo TraceFinder Workflow Service Properties dialog box, type the password and confirming password for the account.
   g. Click **OK**.
   h. In the Services dialog box, right-click **Thermo TraceFinder Workflow Service** and choose **Restart** from the menu.

      The application does not apply the new account until you restart the workflow service.

i. Close the Services dialog box.

j. If the TraceFinder Administrator Console displays Running as: LocalSystem instead of the account you selected, click **Refresh**.

8. Click **Apply**.

IMPORTANT The Thermo TraceFinder Workflow Service requires that users log on to the computer with a Windows password. If you attempt to access this service on a computer without password protection, an error message prompts you to create a Windows password, reboot, and log on with the password.

Security – Global Policy Page

From the Security – Global Policy page, you can set parameters for user security, automatic logoff, and access to the TraceFinder application.

Figure 3. Security – Global Policy page

Table 1. Security – Global Policy page parameters (Sheet 1 of 2)

Function	Description
Enable Security	Turns on the application security features in the Administrator Console.

Table 1. Security – Global Policy page parameters (Sheet 2 of 2)

Function	Description
Lock Client that Has No Interaction…	Specifies the number of minutes before an idle TraceFinder session displays a password-protected lock screen and, unless the user enters a user name and password, automatically logs off the user. Range: 1 through 999 minutes Default: 5 minutes
Silent Authentication	With user security enabled, a TraceFinder user who is currently logged in to Windows may access the TraceFinder application without logging in again.
Authenticate Explicit Users Only	Allows login access to only users listed in the Users list on the Users page.
Workflow Service Credentials	Specifies the TraceFinder workflow services security account.

Users

With security enabled, use the features on the Security – Users page to create users, assign roles to users, and map Active Directory groups to TraceFinder roles.

Follow these procedures:

- To add a new user
- To remove a user
- To verify a user's group membership

❖ To add a new user

1. Click the **Add User** icon,  .

   The Add User to Security List dialog box opens.

2. Type the login name of the new user and click **Add**.

   The application adds the new, unverified, user to the Users list.

   - A green check,  , indicates verified users.
   - A red X,  , indicates unverified users.

3. To verify that the users in the list are members of the current authentication group, click the **Verify Users** icon,  .

4. In the Roles Granted Directly area, select the roles that you want to assign to this user.

5. When you have completed all your changes, click **Apply**.

❖ **To remove a user**

1. Select the user name in the Users list.
2. Click the **Delete User** icon,  .

   The application immediately removes the selected user.

❖ **To verify a user's group membership**

1. Select the user name in the Users list.
2. Click the **Refresh Groups** icon,  , in the Roles Via Group Membership area.

   The application displays all Windows security groups to which the selected user belongs.

Roles

Use the features on the Security – Roles page to define the roles that are available for users and assign permissions to these roles. This topic describes the default responsibilities for the following default user roles created in the TraceFinder application: Security, LabDirector, ITAdmin, Supervisor, Technician, and QAQC. Each role has default permissions. See Role Permission Defaults. If your team has changed these default permissions, your access might be different. You must also activate user security for these user roles to take effect.

A user in either the default LabDirector or the ITAdmin role assigns you to a role that provides access to specific modes and features of the TraceFinder application. When you log in, the navigation pane displays links to only the modes, interface areas, and features that you have permission to access. For multiple role assignments, you must select which role to use for the TraceFinder session.

IMPORTANT User roles are in effect only when user security is enabled. When user security is not enabled, all users have access to all permissions except Security.

These are the default user roles:

- Security
- LabDirector
- ITAdmin
- Supervisor
- QAQC
- Technician

Security

In the Security role, you can access only the Security features in the Administrator Console; you cannot access the TraceFinder application.

LabDirector

In the default LabDirector role, you review graphically applicable data and manipulate data, batches, methods, and instruments.

A laboratory director is responsible for these tasks:

- Creating or editing methods for new levels of detection or adding new compounds to the existing database
- Reviewing data from the mass spectrometer
- Running samples and reviewing data collected by others
- Reporting the data
- Understanding the results and giving final approval of the released data before archiving

ITAdmin

In the default ITAdmin role, you set security, manage users into their roles, and manipulate the various databases. You are responsible for adding compounds into the compound databases.

An IT administrator is responsible for these tasks:

- Handling the databases
- Applying roles to users
- Understanding security, users, and groups
- Creating local users and network groups

Supervisor

In the default Supervisor role, you are responsible for setting up the instrument samples and using previously built batches and methods for processing and acquiring data. You also develop and edit methods for processing and acquiring data, review the data, and distinguish between the need to rerun samples or pass reports up to the laboratory director for final review. On a daily basis, you establish the priority for a list of samples to run and create the sequence of events.

A supervisor is responsible for these tasks:

- Submitting samples
- Creating and submitting batches

- Reporting the data to management
- Creating or editing methods for new levels of detection or adding new compounds to the existing compound database
- Reviewing data from the mass spectrometer
- Understanding the results, who ran the batch, and who passed along the results before giving intermediate approval and sending the data to management
- Modifying new compounds or adjusting methods for specific result sets

QAQC

In the default QAQC role, you review graphically applicable data and interpret the data, but you do not manipulate the data.

A QAQC technician is responsible for these tasks:

- Reviewing data from the mass spectrometer
- Understanding the results, reviewing who ran and passed along the results before giving intermediate approval, and sending the data to management
- Receiving instructions for new sets of samples for the TraceFinder application to analyze after finishing the current analysis

Note In the QAQC role, you have access only to the Analysis mode.

Technician

In the default Technician role, you are responsible for setting up the instrument samples and using previously built sequences and methods for processing and acquiring data. You also edit existing methods for processing and acquiring data, review collected data, and distinguish between the need to rerun samples or pass reports up to the supervisor. On a daily basis, you are responsible for gathering the list of samples to run and creating the sequence of events.

A technician is responsible for these tasks:

- Submitting samples
- Creating and submitting batches
- Creating data to be reviewed by management
- Receiving instructions for new sets of samples for the TraceFinder application to analyze after finishing the current analysis
- Reviewing data from the mass spectrometer
- Understanding the resulting data, making integration changes, and passing those changes up for further approval

Using the Roles Page

Use the Security – Roles page to create new roles, change the permissions assigned to roles, or delete roles.

Follow these procedures:

- To add a role
- To remove a role
- To change permissions for a role

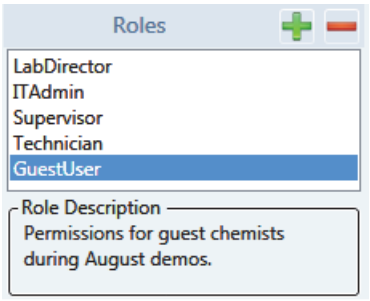
❖ To add a role

1. Click **Add Role** in the Roles area.

   The Add New Role dialog box opens.

2. In the Role Name box, type a name for the new role.
3. (Optional) In the Description box, type a description for the new user role.

   The application displays the description for a selected role below the Roles list on the Security – Roles page, as in this example:



4. Click **OK**.
5. On the Security – Roles page, select the permissions for the new role.
6. When you have made all your changes, click **Apply**.

Note You cannot open a different page in the Administrator Console while these changes are pending.

❖ To remove a role

IMPORTANT Be careful before deleting the LabDirector or ITAdmin roles. These are the only default roles that can control user security. You must have at least one user role that can control security.

1. Select the role in the Roles list.
2. Click the **Delete Role** icon,  .

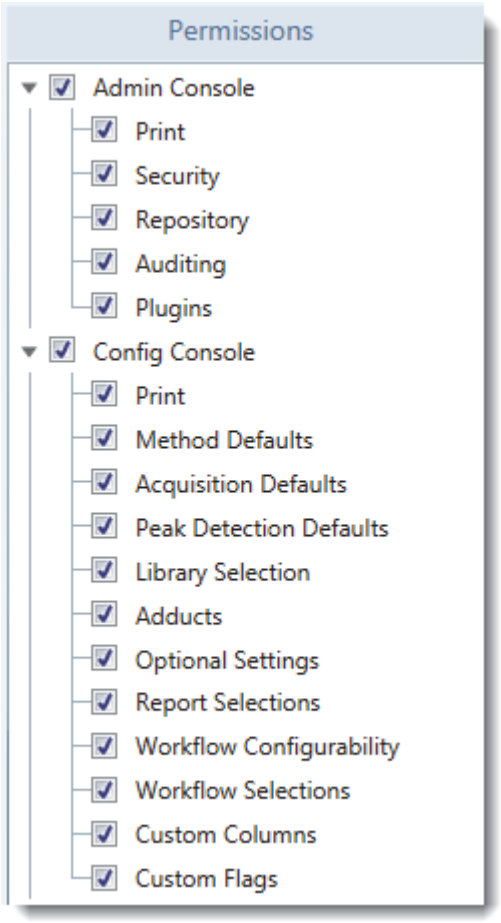
3. When prompted to confirm this action, click **Yes**.

   The application immediately deletes the specified role. There is no undo for this action.

❖ To change permissions for a role

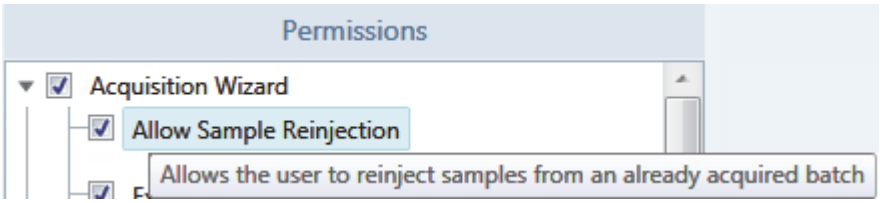
1. Select the role in the Roles list.

   The Permissions list indicates all the permissions assigned to the selected role. The following example shows some of the default permissions for the LabDirector role.



2. Select the check box for each permission that you want to assign to the selected role, or clear the check box for each permission that you do not want to assign to the role.

3. To see additional information about a permission, point to it in the Permissions list.



4. To reset all the permissions that were specified before you made changes, click **Undo**.

   The applications discards all pending changes to all the roles.

5. When you have made all your changes, click **Apply**.

   The application saves all pending changes to all the roles.

Security – Roles

Use the features on the Security – Roles page to create new roles, change the permissions assigned to roles, or delete roles.

Figure 4. Security – Roles page

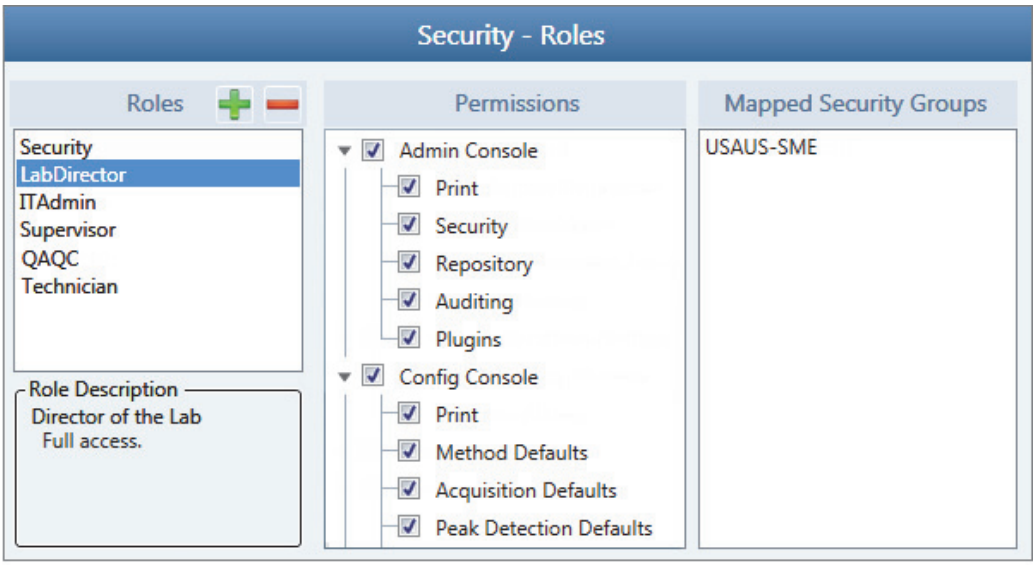


Table 2. Roles page

Function	Description
Roles	Displays all available roles.
Role Description	User-defined description of the selected role.
Permissions	Displays all permissions allowed for the selected role.
Mapped Security Groups	Displays all Windows security groups that are mapped to the selected role. The group inherits all permissions of the roles to which it is mapped. To map a security group to a role, see Role Mapping.

Role Permission Defaults

The following table shows the default permissions assigned to each of the default user roles.

Table 3. Permission defaults (Sheet 1 of 5)

Permission	LabDirector	Supervisor	ITAdmin	QAQC	Technician
Admin Console					
Print	✓	✓	✓		
Security	✓		✓		
Repository	✓	✓	✓		
Auditing	✓		✓		
Plugins	✓	✓	✓		
Config Console					
Print	✓	✓			
Method Defaults	✓	✓			
Acquisition Defaults	✓	✓			
Peak Detection Defaults	✓	✓			
Library Selection	✓	✓			
Adducts	✓	✓			
Optional Settings	✓	✓			
Report Selections	✓	✓			
Custom Columns	✓	✓			
Custom Flags	✓	✓			
Miscellaneous					
Real Time Viewer - Edit	✓	✓			
Online Access	✓	✓		✓	✓
Help Desk	✓	✓			
Instrument Method Editor	✓	✓			
Instrument Method Per Sample	✓	✓			✓
Override Batch Ownership	✓	✓			
Tools					
Qual Explorer	✓	✓			
Library Browser	✓	✓			
Legacy Data Converter	✓	✓			

Table 3. Permission defaults (Sheet 2 of 5)

Permission	LabDirector	Supervisor	ITAdmin	QAQC	Technician
Quick Acquisition	✓	✓			
Audit Viewer	✓	✓			
Method Development					
Unknown Screening	✓	✓			
Update from Local Method	✓	✓			
Create New Master Method from Local	✓	✓			
Update Instrument Method	✓	✓			
Compound Database	✓	✓			
Analysis					
Batch View	✓	✓			
Print Batch	✓	✓			
Archive Batch	✓	✓			
Import Batch	✓	✓			
Save Batch	✓	✓			
Save Batch As	✓	✓			
Move Batch	✓	✓			
Extended Calibration	✓	✓			✓
Update from Master Method	✓	✓			
Select New Master Method	✓	✓			
Submit for Acquisition	✓	✓			✓
Submit for Processing	✓	✓			
Submit for Reporting	✓	✓			
Auto TSRM Update	✓	✓			
Auto Samples	✓	✓			
Reference Samples	✓	✓			
Threshold Samples	✓	✓			
Sample List	✓	✓			
Add Sample	✓	✓			
Insert Sample	✓	✓			
Insert Copy Sample	✓	✓			
Reinject Selected Samples	✓	✓			

Table 3. Permission defaults (Sheet 3 of 5)

Permission	LabDirector	Supervisor	ITAdmin	QAQC	Technician
Remove Selected Samples	✓	✓			
Import Samples	✓	✓			
Browse In Rawfiles (Move)	✓	✓			
Browse In Rawfiles (Copy)	✓	✓			
Map Rawfiles	✓	✓			
Copy/Paste/Export Samples	✓	✓			
Modify Columns	✓	✓			
Sample Weight Calculation	✓	✓			
Data Review	✓	✓			
Sample View	✓	✓			
Compound View	✓	✓			
Comparative View	✓	✓			
Qual View	✓	✓			
Adjust Views	✓	✓			
Modify Columns	✓	✓			
Adjust Calibrations	✓	✓			
Toggle Calibration Points	✓	✓			
Activate/Deactivate Compounds	✓	✓			
Export Results	✓	✓			
Edit	✓	✓			✓
Peak	✓	✓			
Delete Peak	✓	✓			
Send the Peak's RT Method	✓	✓			
Manual Integration	✓	✓			✓
User Integration	✓	✓			✓
Local Method Integration	✓	✓			✓
Survey View Enforcement					
Strict Survey View Enforcement					
Report View	✓	✓			
Print	✓	✓			
Template Archiving	✓	✓			

Table 3. Permission defaults (Sheet 4 of 5)

Permission	LabDirector	Supervisor	ITAdmin	QAQC	Technician
Template Editing	✓	✓			
Generate Reports	✓	✓			
Local Method	✓	✓			
Print	✓	✓			
Edit Acquisition Components	✓	✓			
Edit Quantitation Components	✓	✓			
Edit Report Components	✓	✓			
Associate a Rawfile	✓	✓			
Adjust Retention Times	✓	✓			
Acquisition Wizard					
Create Batch	✓	✓			
Submit Prepared Batch	✓	✓			
Reinject Samples	✓	✓			
Batch Templates	✓	✓			
Submission	✓	✓			
Select Batch Folder	✓	✓			
Select Method Information	✓	✓			
Report Selection	✓	✓			
System Startup Method	✓	✓			✓
System Shutdown Method	✓	✓			✓
Auto TSRM Update	✓	✓			✓
Extended Calibration	✓	✓			✓
Submit for Acquisition	✓	✓			
Submit for Processing	✓	✓			
Submit for Reporting	✓	✓			
Sample List	✓	✓			
Add Sample	✓	✓			
Insert Sample	✓	✓			
Insert Copy Sample	✓	✓			
Reinject Selected Samples	✓	✓			
Remove Selected Samples	✓	✓			

Table 3. Permission defaults (Sheet 5 of 5)

Permission	LabDirector	Supervisor	ITAdmin	QAQC	Technician
Import Samples	✓	✓			
Copy/Paste/Export Samples	✓	✓			
Modify Columns	✓	✓			
Sample Weight Calculation	✓	✓			

IMPORTANT The Security role has access only to the security features in the Administrator Console. Users who are assigned only to this role cannot access other features in the TraceFinder Administrator Console or in the main TraceFinder application.

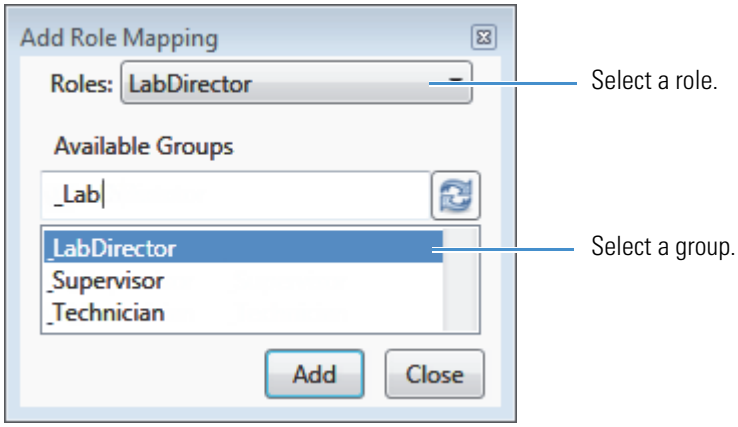
Role Mapping

Use the features on the Security – Role Mapping page to assign Windows security groups to the default roles or the roles you defined for the TraceFinder application.

❖ **To create a new mapping**

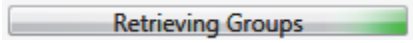
1. Click the **Create Mapping** icon,  .

   The Add Role Mapping dialog box opens.



2. If the Available Groups list is not populated, click the **Retrieve Groups** icon,  .

   The dialog box displays a progress bar until it finishes searching the Windows Active Directories and displays all the available groups defined for your organization.



   - A user in the default LabDirector role who also has administrator privileges on the local machine can create groups and assign users to those groups.
   - A user in the default LabDirector role who also has administrator privileges on the network can create groups in the Windows Active Directories.

3. Select a role from the Roles list.
4. Select a group from the Available Groups list.

   Tip This list can be very long. To quickly jump to the group you want, begin typing the group name in the text field. The list scrolls to the first matching text string. The search is not case sensitive.

5. Click **Add**.

   The application immediately creates the mapping and closes the Add Role Mapping dialog box.

6. Click **Close**.

Using the Repository View

Use the features in the Repository view to specify repositories for batches, methods, and templates that you create.

Tip (Animation) To view "Using Repository Features," choose **Help > Animations**.

IMPORTANT When you use network repositories, you must also use a custom workflow service account. See how to specify a custom account in the Global Policy topic in Chapter 1, "Using the Security View."

Contents

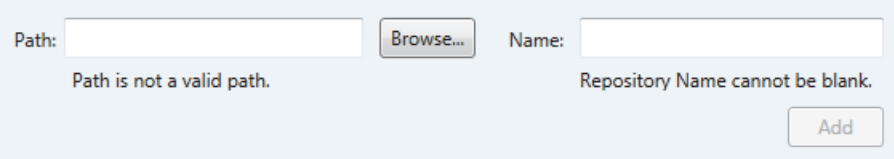
Administration

Use the features on the Repository – Administration page to create and manage repositories.

Follow these procedures:

- To create a new repository
- To delete a repository

❖ To create a new repository



1. In the Path box, either browse to a folder for the new repository or type a URL.

IMPORTANT The folder name for the repository cannot include any of the following special characters: / \ : * ? " < > |

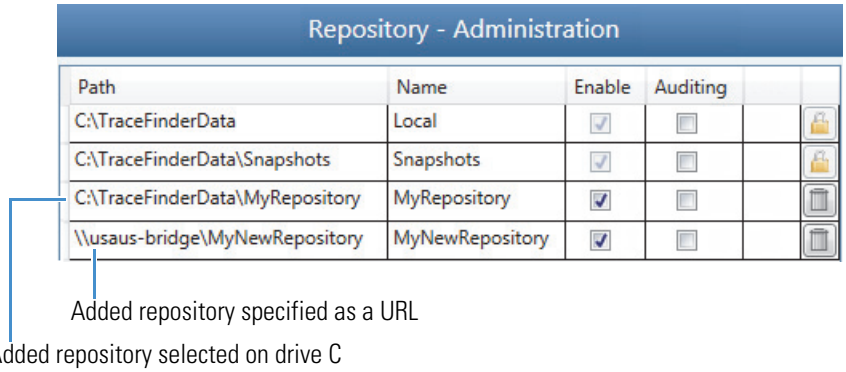
2. In the Name box, type a name for the new repository.

IMPORTANT The name for the repository must be unique. Repository names are case insensitive. For example, *MyRepository* is the same as *myrepository*.

3. Click **Add**.

The application adds the new repository to the repository list. The trashcan icon indicates that you can change or delete this repository, unlike the locked repositories.

IMPORTANT You cannot change a repository name because the name is associated with the batch and method data you create. The name is read-only, but you can change the repository Path to redirect the repository to different location.



4. To specify that the repository is available to users, select the **Enable** check box.

The application enables all added repositories by default.

5. To specify that the application create an audit trail for the repository, select the **Auditing** check box.

To specify the actions to be audited, see Chapter 3, "Using the Audit View."

IMPORTANT When multiple TraceFinder installations access the same repository, each of the TraceFinder applications must use the same setting to enable or not enable Auditing. Failure to use the same setting can result in incorrect audit trails.

6. When you have made all your changes, click **Apply**.

❖ To delete a repository

Click the **Remove Repository** icon,  , for the repository that you want to delete.

The application immediately removes the repository from the list. There is no confirmation. This action does not delete the folder from the computer; it only removes the repository from this list.

Note Using the Undo function does not necessarily return a deleted repository. The Undo function returns the Repository – Administration page to the state when you first opened it or to the state immediately after the last Apply.

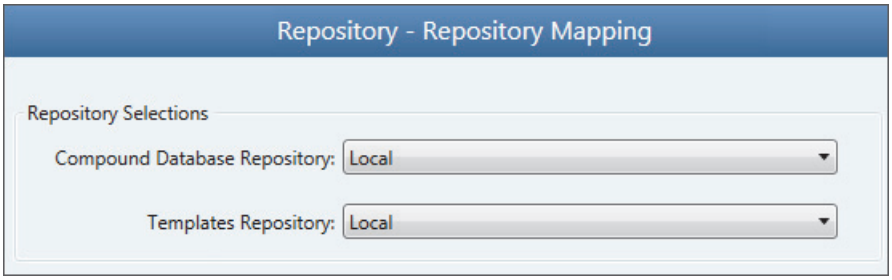
Repository Mapping

Use the repository mapping features to change the repository where you store your data folders, such as batch, method, template, and compound database folders (the default location is C:\TraceFinderData).

❖ To select the repositories for storing data folders

1. Click **Repository Mapping** in the Repository navigation pane.

   The Repository – Repository Mapping page opens.



2. Select a Compound Database Repository where you want to save compound databases.

   The dropdown list displays the default repository and all available repositories that you added. See To create a new repository.

   By default, the TraceFinder application saves compound databases to the following folder:

   C:\TraceFinderData\CompoundDatabases

   When you save a new compound database in the application, it creates a file (.cdb extension) in the specified repository.

3. Select a Templates Repository where you want to save batches, methods, and templates.

   The dropdown list displays the default repository and all available repositories that you added. See To create a new repository.

   By default, the application saves batches, methods, and templates to the following folders:

   C:\TraceFinderData\Projects

   C:\TraceFinderData\Methods

   C:\TraceFinderData\Templates

   When you create any of these items in the application, it creates Projects, Methods, and Templates folders in your specified repositories.

3

Using the Audit View

Use the features in the Audit view to specify the events that are audited or that require confirmation. You can also specify a list of default reasons for a specific event and whether a user can submit a custom reason.

An event describes a specific action, such as opening or saving a batch, method, or template. Each event can include multiple actions. For example, an "edit" event includes all the changes to the data since the last time the user saved the data.

The TraceFinder application records all user access, including logging in, logging out, data creation and editing (batches, methods, and templates), and manual integration. As a user with Auditing permission, you can configure the auditing service by specifying the events to be logged, the events requiring confirmation, and those that can have custom reasons. In the TraceFinder application, all users can use the Audit Viewer to view the resulting log files to track user access and modifications to the data.

IMPORTANT When multiple TraceFinder installations access the same repository, each of the TraceFinder applications must use the same setting to enable or not enable Auditing. Failure to use the same setting can result in incorrect audit trails.

Tip (Animation) To view "Using Audit Features," choose **Help > Animations**.

Contents

Audit Logs

The application creates the following audit trail log files:

- Application: Records all user access, such as starting and stopping the application, logging in, logging out, accessing or saving data in batches and methods. The log file with this data is saved in C:\TraceFinderData\Admin\AuditLog.adb.
- Master Method: Records all user interactions with master methods, such as creating, opening, or editing a master method. The log file with this data is saved in C:\TraceFinderData\Methods*MasterMethodName*\5.1\AuditLog.adb.
- Batch: Records all user interactions with batches, such as creating, opening, editing, acquiring, processing, or generating reports for a batch. The log file with this data is saved in C:\TraceFinderData\Projects*SubFolder**BatchName*\Batch\5.1\AuditLog.adb.

Event Maps

An event map defines which auditing parameters the application uses for each audited event.

Use the following procedures:

- To create an event map
- To edit an event map

❖ To create an event map

1. Do one of the following:
   - Click the **Create New Map** icon,  .

     The application adds a new audit map named *NewMap_1* to the audit map list. The application sets all parameters in the new audit map to the default.

   –or–

   - Select an audit map and click the **Copy** icon,  .

     The application copies the selected map and adds a new audit map named *OriginalName*_1 to the audit map list. The application copies all parameter values from the selected map.
2. (Optional) Edit any of the following parameters:
   - Select the audit map name in the Name column, and rename the new audit map.
   - In the Selected Map pane, type information for the new audit map.
   - In the Events pane, edit the parameter values for the new audit map.

❖ To edit an event map

1. In the Audit Maps pane, select the audit map that you want to edit.

   The application displays the parameter values for the selected map in the Events pane.

   Tip The active audit map is not necessarily the selected one. See Distinguishing Active from Selected Maps.

2. Select or clear the check box for each of the following parameters that you want to edit.

   - **Audit**: Writes information about the event to the audit log. Available for all event types.
   - **Challenge**: Prompts the user to enter a reason before completing the event. Available for only immediate event types.
   - **Custom Reason**: Lets the user enter a reason other than the default reasons defined for the event. Available for only immediate event types.
   - **ESignature**: Prompts the user to enter a password before completing the event. Available for only immediate event types.

     IMPORTANT You must also select the Enable Security check box to enable the password requirement in the audit Confirm Changes dialog box. Follow the instructions To enable security.

     IMPORTANT Enabling Silent Authentication grays out Esignatures in the audit Confirm Changes dialog box.

3. In the Reason 1–6 columns, enter or change the text.

   This parameter is available for only immediate event types.

4. Click **Apply**.

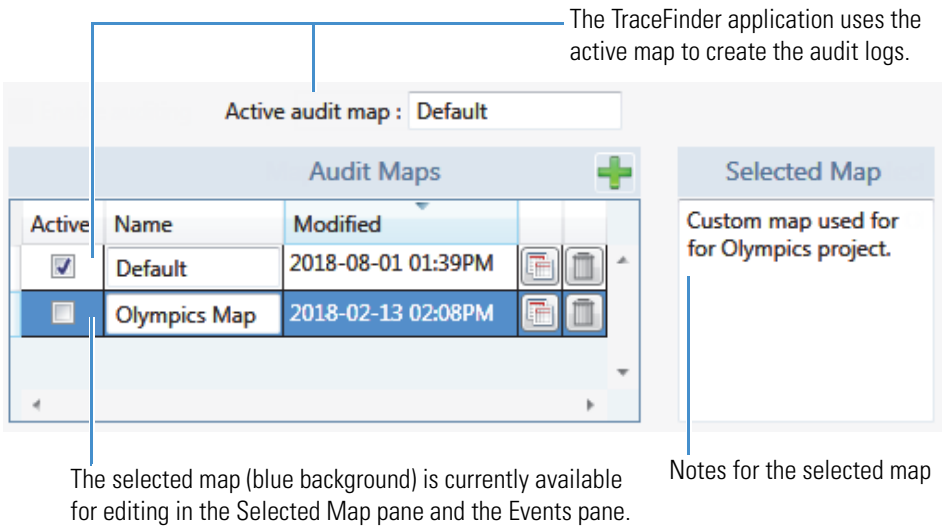
   The application saves your changes to the audit map. When this map is selected as the Active map, the application applies these audit parameter settings to all user interactions. To be sure you know which audit map is the active one, see Distinguishing Active from Selected Maps.

Distinguishing Active from Selected Maps

When you work with event maps, you can edit parameters for the selected map; however, the selected map is not necessarily the active map that the TraceFinder application is using. A selected Active check box indicates an active map; a blue background indicates a selected map.

Use the following graphic to be sure you know the difference.

Figure 5. Difference between active and selected maps



Administration Page

Use the features on the Audit – Administration page to specify which events are audited and which auditing parameters you want to use for each audited event.

Figure 6. Administration page

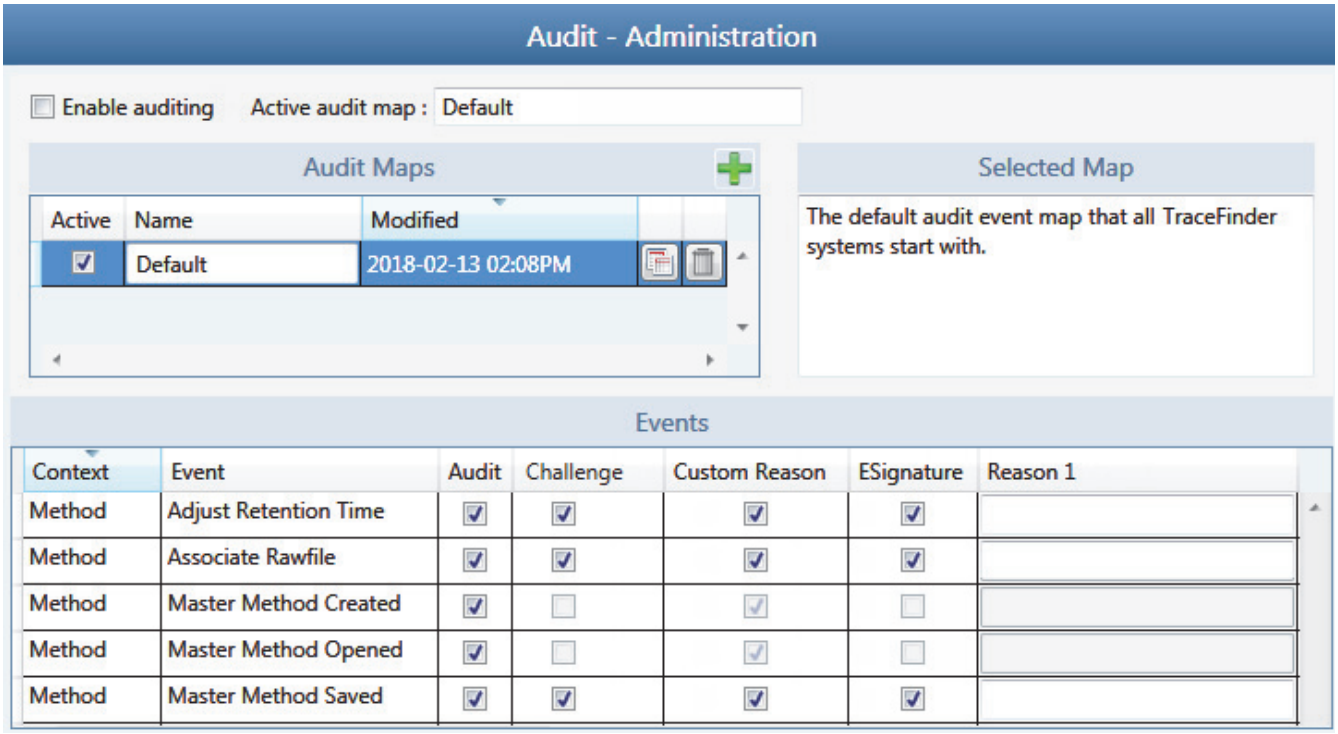


Table 4. Administration page parameters (Sheet 1 of 2)

Parameter	Description
Enable Auditing	Turns on the auditing features in the TraceFinder application.
	IMPORTANT When multiple TraceFinder installations access the same repository, each of the TraceFinder applications must use the same setting to enable or not enable auditing. Failure to use the same setting can result in incorrect audit trails.
Active Audit Map	The name of the currently selected audit map.
Audit Maps	
Active	Makes the selected map the currently used map.
Name	Name of the audit map.
Modified	The last date the audit map was edited.
Copy	Copies this audit map to a new name. The default name is *OriginalName*_1.
Delete	Removes the audit map from the list of available audit maps.

Table 4. Administration page parameters (Sheet 2 of 2)

Parameter	Description
Selected Map	Editable description of the currently selected map.
Events	
Context	Events are grouped into application-level, batch-level, template-level, or method-level contexts.
Event	An action that triggers an entry in the audit log. There are three types of events: automatic, immediate, and queued. For a detailed list of events that the application logs, see Events. • For automatic events, the Challenge, Custom Reason, Reason *n*, and ESignature features are not available. • For immediate events, all Events features are available. • Queued events—unsaved edits to a batch or method that are recorded in the audit log—require no confirmation, reason, or authorization.
Audit	Writes this event to the audit log.
Challenge	Requires that the user enter a reason before completing the event.
Custom Reason	Allows a custom reason for the event. When prompted to confirm the event, the user can select a reason from the list of default reasons or type a custom reason in the Confirm Changes dialog box.
ESignature	Requires that the user enter a password before completing the event. Disabling Security or enabling Silent Authentication disables the password requirement in the audit Confirm Changes dialog box.
Reason 1–6	Reasons that you define for an event. When prompted to confirm the event, the user can select a reason from the list of default reasons in the Confirm Changes dialog box.

Table 5. Events (Sheet 1 of 5)

Parameter	Description
Application	All Application events are automatic events. The Challenge, Custom Reason, Reason *n*, and ESignature features are not available for these events.
Application Configuration Changed	Makes an entry in the audit log each time a user makes a change in the Configuration Console.
Application Start	Makes an entry in the audit log each time a user logs on to the TraceFinder application.
Application Stop	Makes an entry in the audit log each time a user logs off the TraceFinder application.
Cdb (Database) Updated	Makes an entry in the audit log each time a user updates the compound database.
Help Desk Snapshot	Makes an entry in the audit log each time a user creates a snapshot from the Help Desk.
Batch	
A batch related file was exported	Makes an entry in the audit log each time a user exports a batch-related file.

Table 5. Events (Sheet 2 of 5)

Parameter	Description
A batch related file was imported	Makes an entry in the audit log each time a user imports a batch-related file.
Acquisition	Makes an entry in the audit log each time a user performs an acquisition.
Adjust Retention Time	Makes an entry in the audit log each time a user modifies the retention time in the local method for any compound in any sample in the batch. To modify the retention times for a single compound in a batch or to modify the retention times for all compounds in a local method. This is an automatic event.
Associate Rawfile	Makes an entry in the audit log each time a user associates a raw data file with a local method for a batch.
Batch Archived	Makes an entry in the audit log each time a user archives a batch.
Batch Closed	Makes an entry in the audit log each time a user closes a batch.
Batch Created	Makes an entry in the audit log each time a user creates a new batch. This is an automatic event. The Challenge, Custom Reason, Reason *n*, and ESignature features are not available for this event.
Batch Exported	Makes an entry in the audit log each time a user exports a batch.
Batch Imported	Makes an entry in the audit log each time a user imports a batch.
Batch Moved	Makes an entry in the audit log each time a user saves a batch to a new project folder.
Batch Opened	Makes an entry in the audit log each time a user opens a batch. This is an automatic event. The Challenge, Custom Reason, Reason *n*, and ESignature features are not available for this event.
Batch Saved	Makes an entry in the audit log each time a user saves a batch.
Batch Saved As	Makes an entry in the audit log each time a user saves a batch to a new name. This is not the same as the entry for "Batch Moved" in which a batch is saved to a different project folder, even though it might also be saved to a new name in the new project folder.
Batch Submitted	Makes an entry in the audit log each time a user submits a batch for acquisition, processing, or reporting.
Clear Extended Calibration	Makes an entry in the audit log each time a user clears the Extend Calibration feature when submitting a batch.
Copy User Peak to Local Method	Makes an entry in the audit log each time a user copies a user-defined peak to a local method.
Create Master Method from Local Method	Makes an entry in the audit log each time a user saves a local method as a master method.
Edit Local Peak Settings	Makes an entry in the audit log each time a user modifies the local peak detection settings.

Table 5. Events (Sheet 3 of 5)

Parameter	Description
Edit User Peak Settings	Makes an entry in the audit log each time a user modifies the user-defined peak detection settings.
Extended Calibration	Makes an entry in the audit log each time a user selects the Extend Calibration feature when submitting a batch.
	IMPORTANT Both the method and the batch must be on either a local repository or a network repository; otherwise, the application cannot save the calibration history to the audit log file.
Help Desk Batch Snapshot	Makes an entry in the audit log each time a user creates a Help Desk snapshot that includes batch data.
Manual Integration	Makes an entry in the audit log each time a user changes the manual integration settings on the Data Review page in the Analysis mode.
Peak Added	Makes an entry in the audit log each time a user adds a quantitation or confirming ion peak on the Data Review page in the Analysis mode.
Peak Deleted	Makes an entry in the audit log each time a user removes a quantitation or confirming ion peak on the Data Review page in the Analysis mode.
Queue	Makes an entry in the audit log each time a user modifies a queue on the Real Time Status – Queues page.
Select a New Master Method	Makes an entry in the audit log each time a user opens a method in the Analysis mode.
Take Ownership of a Locked Batch	Makes an entry in the audit log each time a user overrides ownership of a locked batch.
Toggle Integration Mode	Makes an entry in the audit log each time a user toggles the integration mode between method, manual, or user integration.
Update Local Instrument Method	Makes an entry in the audit log each time a user updates a local instrument method from the master method.
	Note Before you can audit edits to instrument methods, you must set up the Foundation instrument audit trail to work with TraceFinder. Refer to the *Foundation Administrator Guide* or to the Foundation online Help.
Update Local Method from Master Method	Makes an entry in the audit log each time a user updates a local method from a master method in the Batch View in the Analysis mode.
Update Master Instrument Method	Makes an entry in the audit log each time a user updates a master instrument method from the local instrument method.
	Note Before you can audit edits to instrument methods, you must set up the Foundation instrument audit trail to work with TraceFinder. Refer to the *Foundation Administrator Guide* or to the Foundation online Help.
Update Master Method from Local Method	Makes an entry in the audit log each time a user updates a master method in the Local Method view in the Analysis mode.

Table 5. Events (Sheet 4 of 5)

Parameter	Description
Template	
Template Created	Makes an entry in the audit log each time a user creates a new batch template in the Acquisition wizard. This is an automatic event. The Challenge, Custom Reason, Reason *n*, and ESignature features are not available for this event.
Template Opened	Makes an entry in the audit log each time a user opens a batch template. This is an automatic event. The Challenge, Custom Reason, Reason *n*, and ESignature features are not available for this event.
Template Saved	Makes an entry in the audit log each time a user saves a batch template.
Method	
A Method Related File was Exported	Makes an entry in the audit log each time a user exports method-related files, such as a CSV file or mass list of compounds.
A Method Related File was Imported	Makes an entry in the audit log each time a user imports method-related files, such as a CSV or CDB file of compounds.
Adjust Retention Time	Makes an entry in the audit log each time a user modifies the expected retention time for a single compound or for all compounds in the method.
Associate Rawfile	Makes an entry in the audit log each time a user associates a raw data file with a master method.
Help Desk Method Snapshot	Makes an entry in the audit log each time a user creates a Help Desk snapshot that includes method data.
Instrument Setup	Makes an entry in the audit log each time a user modifies parameters on the Instrument Setup window.
Master Method Closed	Makes an entry in the audit log each time a user closes a master method.
Master Method Created	Makes an entry in the audit log each time a user creates a new master method. This is an automatic event. The Challenge, Custom Reason, Reason *n*, and ESignature features are not available for this event.
Master Method Opened	Makes an entry in the audit log each time a user opens a master method. This is an automatic event. The Challenge, Custom Reason, Reason *n*, and ESignature features are not available for this event.
Master Method Overwritten	Makes an entry in the audit log each time a user overwrites a master method.
Master Method Saved	Makes an entry in the audit log each time a user saves a master method.
Master Method Saved As	Makes an entry in the audit log each time a user saves a master method to a new name.
Master Method Lock Override	Makes an entry in the audit log each time a user overrides a locked master method.

Table 5. Events (Sheet 5 of 5)

Parameter	Description
Update Global Instrument Method	Makes an entry in the audit log each time a user updates the global instrument method (in the …\TraceFinderData\InstrumentMethods folder) from the current master method.
Update Master Method Instrument Method	Makes an entry in the audit log each time a user updates the current master method from the global instrument method (in the …\TraceFinderData\InstrumentMethods folder).
Security	
Security Changed	Makes an entry in the audit log each time a user modifies the configuration security settings.
User Lockout	Makes an entry in the audit log each time the application locks out the user.
User Login	Makes an entry in the audit log each time a user logs in to the TraceFinder application.
User Login Failed	Makes an entry in the audit log each time a user enters incorrect credentials when logging in to the TraceFinder application.
User Logout	Makes an entry in the audit log each time a user logs out of the TraceFinder application.

Using the Plugins View

Use the features on the Plugins – Administration page to configure available plugins for the TraceFinder application.

❖ To enable plugins

1. Click **Administration** in the Plugins navigation pane.

   The Plugins – Administration page opens, listing all available plugins.

2. For each plugin that you want to use in the TraceFinder application, select the **Enabled** check box.

3. To configure a plugin, select the plugin and click **Configure**.

   Note You can configure only one plugin at a time. Do not confuse an *enabled* plugin with a *selected* plugin. An enabled plugin shows a check mark; a selected plugin is highlighted in blue.

   A dialog box for the selected plugin opens.

4. In the configuration dialog box, select the options you want to configure and then click **Save**.

5. Click **Apply**.

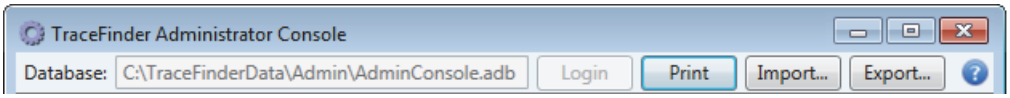
   The enabled plugins become available the next time you start the TraceFinder application.

Printing the Administrator Settings

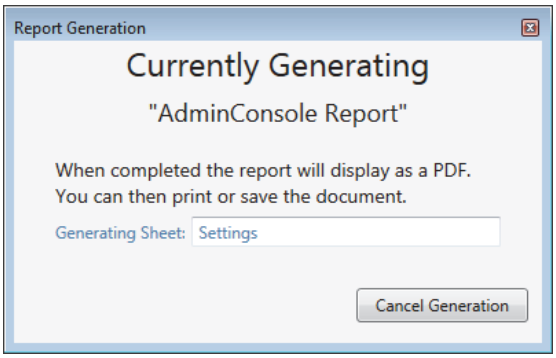
Use the Print button to save the administrator settings to a PDF file.

❖ **To print the current administrator settings**

1. Click **Print**.

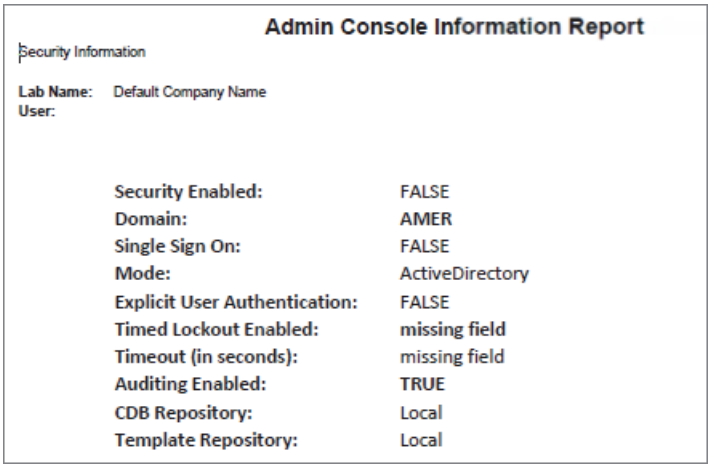


The application confirms that the report is generating.



The resulting report opens as a read-only PDF file.

Figure 7. Example of an Admin Console Information Report



Admin Console Information Report

Security Information

Lab Name: Default Company Name
User:

Security Enabled:	FALSE
Domain:	**AMER**
Single Sign On:	FALSE
Mode:	ActiveDirectory
Explicit User Authentication:	FALSE
Timed Lockout Enabled:	**missing field**
Timeout (in seconds):	missing field
Auditing Enabled:	**TRUE**
CDB Repository:	Local
Template Repository:	Local

B

Importing and Exporting Administrator Settings

Use the Export button to save your current administration settings to a file.

Use the Import button to import saved administration settings to your current Administrator Console.

Tip (Animation) To view "Using Print, Import, and Export Features," choose **Help > Animations**.

Follow these procedures:

- To export settings to a file
- To import settings from a file

❖ To export settings to a file

1. Set and apply all the settings that you want to export.
2. Click **Export**.

   The Browse For Folder dialog box opens.
3. Locate the folder where you want to save the exported file and click **OK**.

   The target folder can be on the local machine, on a network drive, or on a USB drive.

   Tip To create a new folder for the saved data, navigate to a higher level folder, click **Make New Folder**, type the name for the new folder, and click **OK**.

   The application writes the saved administration information to the following file:

   AdminConsole.abd

❖ To import settings from a file

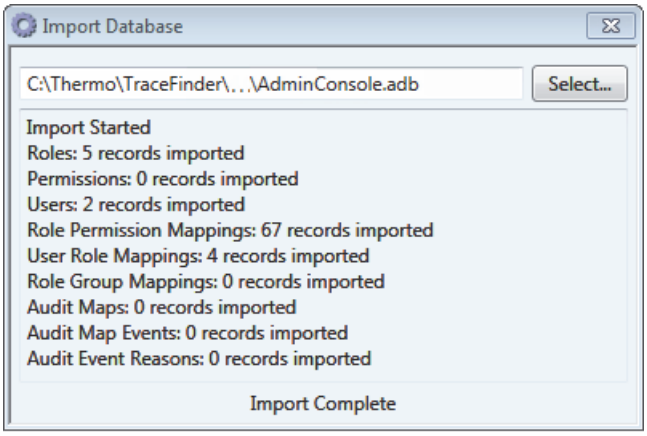
1. Click **Import**.

   The Import Database dialog box opens.
2. Click **Select** and locate a saved administrator database file (.adb) to import.

   The database file can be on the local machine, on a network drive, or on a USB drive.

3. Click **Open**.

   The Import Database dialog box displays the imported records: roles, permissions, users, role mappings, and audit mapping settings.



4. Close the Import Database dialog box.
5. To see the imported changes on your current page, refresh the page.