LT Assessment for SUSE

User Guide

BLUE LANCE
COMPUTER SECURITY SOFTWARE

CONTACT INFORMATION

Blue Lance, Inc.
410 Pierce St, Suite 303
Houston, TX 77002
Phone number: 713-255-4800
Fax number: 713-650-0090
Web address: **http://www.bluelance.com**

COPYRIGHT © 2010 Blue Lance, Inc.

Blue Lance, LT Assessment for SUSE are registered trademarks of Blue Lance, Inc.

Microsoft, Windows 2003, Windows 2008, SQL Server 2005/2008 and Access are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Novell and SUSE are registered trademarks of Novell, Inc in the United States and other countries.

Intel and Pentium are registered trademarks of Intel Corporation.

Blue Lance shall not be held accountable for technical or editorial errors within this document. This document is provided “as is” without warranty of any kind and is subject to change without notice.

Contents

Chapter 1 — Architecture

Terms and Concepts 2
Architecture 6

Chapter 2 — Installing LT Assessment for SUSE

Overview 1
Installation Requirements 1
Installing LT Assessment for SUSE 2
Modifying, Repairing, and Uninstalling LT Assessment for SUSE 11
Modifying LT Assessment for SUSE 11
Repairing LT Assessment for SUSE 12
Uninstalling LT Assessment for SUSE 12

Chapter 3 — Using LT Assessment for SUSE

Overview 1
LT Assessment for SUSE Components 2
Displaying the LT Assessment for SUSE Window 5
Menu Bar 6
System 6
Edit 7
Help 7
Standard Toolbar 8
Locking and Unlocking the LT Assessment for SUSE Window 9
Address Bar 12
Connecting to a Remote Machine 12
Category Shortcut Window 13
Assessment Category Window 14
Target Profiles for Scans 15
Network Scans 21
Selecting a Target Profile from the Scan Details Window 23
Selecting a Specific Container from the Scan Details Window 25
Selecting a Specific Volume from the Scan Details Window 28
Selecting a Specific Folder or File from the Scan Details Window 31
Gathering File System Trustee Assignments 41
Selecting a Specific Container from the File System Trustee Assignments Scan Details Window 43

Report Queries 47
Creating a New Report Query 50
Deleting a Report Query 53
Modifying an Existing Report Query 54
Modifying Your Database and E-Mail Settings 70
Calendar 74
Creating a New Job 74
Reviewing the Status of a Job 81
Modifying Existing Jobs 82
Deleting an Existing Job 82
Reviewing Previously Run Jobs 82
Scenarios 83
Scenario 1 83
Solution 1 83
Scenario 2 84
Solution 2 84
Scenario 3 85
Solution 3 85

Appendices

Appendix A — Rules
Appendix B — Report Types

LT Assessment for SUSE
Chapter 1 — Architecture

Controlling access to information and data on a network is critical to ensure the confidentiality and integrity of intellectual property in an organization. To mitigate risk or to reduce the potential for loss of intellectual property, security controls are implemented on networks. Controls also provide accountability for individuals accessing sensitive information through access control mechanisms and auditing. These controls must be in accordance with and accurately represent the organization's security policy. Security assessment is performed to ensure that controls are in compliance with the security policy.

LT Assessment for SUSE is a software application that can be used to perform a security assessment on Novell's eDirectory networks.

LT Assessment for SUSE can be used to:

- Determine the current state of security controls defined on the network to ensure compliance with security policies.
- Identify eDirectory/SUSE/NetWare Directory Services (NDS) vulnerabilities that pose significant threats to an organization.
- Provide administrators with disk utilization analysis reports to help manage data stored on the network.

This chapter will focus on eDirectory and LT Assessment for SUSE terms and concepts.

Terms and Concepts

Understanding important network or systems management terms and concepts is the first step toward using LT Assessment for SUSE most advantageously.

The following are eDirectory terms:

- **eDirectory** — Highly scalable, high performance, secure directory service created by Novell, Inc. The eDirectory can store and manage millions of objects. It is also used to control access to network resources and build relationships between those resources.
- **Objects** — Represent network entities such as users, groups, file servers, and printers. The NDS eDirectory tree is made up of objects.
- **Object Attributes** — All objects contain a list of attributes. Each attribute contains information about the object. Objects are classified based on their attributes. Some objects are classified by the number of attributes they contain.
- **Users** — A class of objects with specific attributes in the eDirectory.

  Example

  Every individual in an organization is associated with a user object that identifies that individual. Users will log in to the eDirectory to access resources in that directory.
- **Groups** — A class of objects that contain user objects as members.

  Example

  If a group is assigned rights to a specific resource in the directory, all users in that group automatically have access to that resource.
- **Containers** — A class of objects that contain other objects.

  Example

  Examples of container objects in the eDirectory include:

  - Country
  - Organization
  - Organizational Unit

  The root of the directory or top of the directory tree is created by default when SUSE/NetWare is installed.

- **File Servers** — A class of objects that denote file servers in the tree. File servers host most of the resources that are shared by other objects.
- **Volumes** — Storage objects that represent the SUSE/NetWare file system. Volumes are associated with file servers. Rights can be assigned for users or groups to any file or directory.
- **Trustee Assignments** — Specific SUSE/NetWare rights assigned to trustees of a resource in a directory.
- **Directory Name Context** — An object's name context represents its position in the NDS eDirectory tree. The context is a list of containers separated by periods. This list of containers traces the object's path back to the [Root]. NDS eDirectory locates an object by its path from the [Root].

The following terms are used in the LT Assessment for SUSE application:

- **Network Scan** — Specifies the scope of data to be collected from the eDirectory.
- **Job** — Schedules a network scan to collect eDirectory or file server data and records this information to a database.
- **Rules —** Type of query to be used for reporting specific eDirectory attributes, from the database. It hides eDirectory complexities from the end-user ensuring user-friendly reporting capability.

  Examples

  The following list includes examples of rules:

  - Query users that have never logged in
  - User's password minimum length less than five
  - Users that do not require a password to log in
- **Statements** — Consists of multiple rules and allows for the creation of complex queries for granular reporting.

  Examples

  Statement: Users not logged in for last sixty days

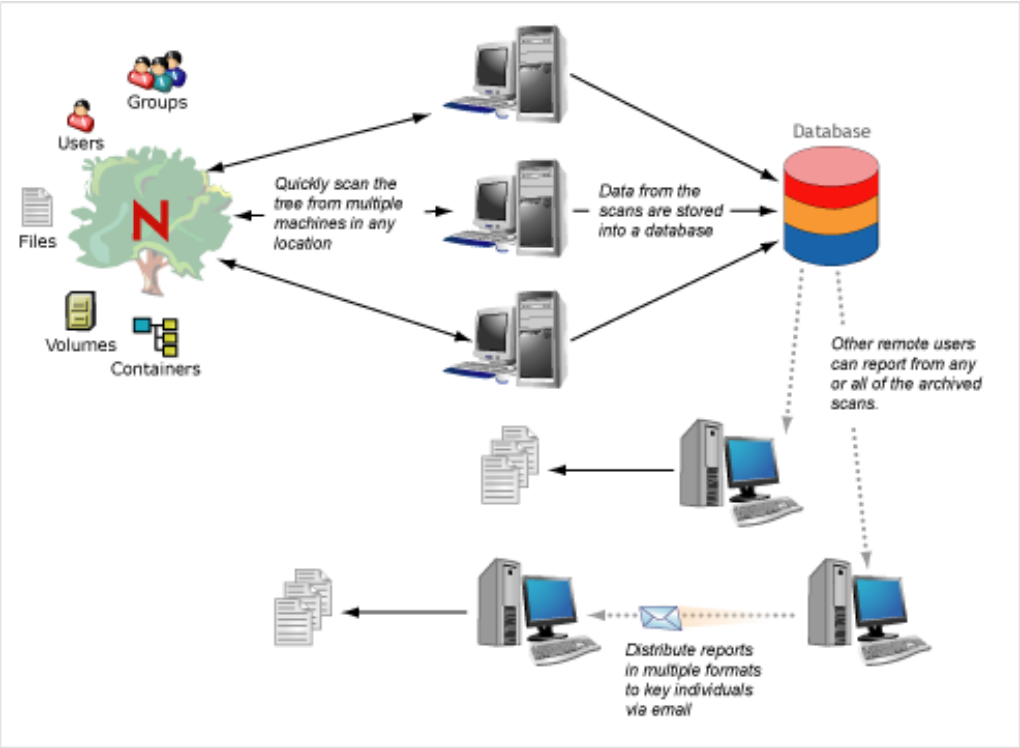
  Rules associated with this statement are:

  1. User last login date is not in the last <60> days [AND]
  2. Users that are not disabled

- **Report Query** — Contain the statements needed to query the database for specific information. It defines the format as well as the output for the report, such as printer, file, and e-mail.
- **Reports** — The process of running a Report Query to retrieve an output.
- **LT Assessment for SUSE console** — This console is launched with LT Assessment for SUSE and used to configure, manage, and report on security assessments for Novell's eDirectory.
- **Assessment Categories** — LT Assessment for SUSE includes the following assessment categories based on the data set of information collected from eDirectory:
  - **User Assessment** — Collects data and reports on user objects in the eDirectory. Some of the reports that can be generated in this category include:
    - Users that have no login activity for a specified period
    - User accounts that do not require a password
    - User accounts with security equivalences equal to administrator
    - Trustee assignments on sensitive files and folders
  - **Group Assessment** — Gathers information on group objects. Some of the reports that can be generated in this category include:
    - Listing of user members for all groups
    - Group trustee assignments
    - Group summary information in eDirectory
  - **Container Assessment** — Collects data on eDirectory container objects. Some of the reports that can be generated in this category include:
    - Incorrect intruder detection settings
    - Object summary information
    - Container trustee assignments
  - **Volume Assessment** — Collects and reports on volume utilization. Some of the reports that can be generated in this category include:
    - Available disk space on specific volumes
    - Summary of disk space utilization on volumes

- **File Assessment** — Collects information about files and folders on file servers in the network. Some of the reports that can be generated in this category include:
  - Which users occupy the most disk space
  - Which directories host the largest files on the network
  - Files that have not been modified over a specified period of time
  - Which users store MPEG, MP3, AVI or other file types
- **Profile Assessment** — Collects all the information needed for a user to log in. Some of the reports that can be generated in this category include:
  - Object entry rights
  - Profile creation modification
- **Application Assessment** — Controls whether network and server applications are available to users. Some of the reports that can be generated in this category include:
  - Application creation modification
  - Applications marked for install only
  - Applications marked to run once after install
- **Template Assessment** — Contains a template of a user's account information allowing you to create multiple accounts with common characteristics. Some of the reports that can be generated in this category include:
  - Template users security equivalent to administrator
  - Template user with grace logins set to more than five
  - Template users with minimum password length not defined
- **File System Trustee Assignment** — Collects all the trustee assignments on SUSE/NetWare servers in the network. Some of the reports that can be generated in this category include:
  - File system trustee report — Grouped by files
  - File system trustee report — Grouped by server
  - File system trustee report — Grouped by trustee
  - File system trustee tabular report

Architecture



Use LT Assessment for SUSE to access the eDirectory

LT Assessment for SUSE can be installed on a single workstation or multiple workstations. Once installed, you can then use the LT Assessment for SUSE console to create a scan capturing assessment data from your eDirectory and SUSE/NetWare file servers. The assessment data is collected and stored to a database. You can then access the data locally or remotely and generate a report from any workstation.

To successfully configure LT Assessment for SUSE to collect and report on eDirectory assessment data, perform the following steps:

1. Setup a network scan to scan the eDirectory for all assessment categories, such as User Assessment, Group Assessment, Container Assessment, Volume Assessment, File Assessment, Profile Assessment, Application Assessment, and Template Assessment. These scans will determine the area of the directory to be scanned as well as the scope of each scan.
2. Build report queries to report on the organization's security assessment requirements as per security policies. LT Assessment for SUSE ships with several report queries that can easily be used or serve as templates to create complex queries. Samples of existing report queries include:
   - User Assessment Report Queries
     - Disabled user accounts
     - Users security equivalent to administrator
     - Users with grace logins set to less than two
   - Group Assessment Report Queries
     - Group summary reports
     - Inheritance mask
   - Volume Assessment Report Queries
     - Free disk space available on volumes
     - Purgeable space on volumes
     - User space restrictions on volumes
   - File Assessment Report Queries
     - File information grouped by folder
     - File ownerships
     - Hidden files
   - Container Assessment Report Queries
     - Inheritance mask
     - Property rights
     - Container object summary report

- Profile Assessment Report Queries
  - Profile creation modification
  - Object entry rights
- Application Assessment Report Queries
  - Applications marked for install only
  - Application creation modification
- Template Assessment Report Queries
  - Template group membership
  - Template user with grace logins set to more than five
  - Template users with minimum password length less than five characters
- File System Trustee Assignment
  - File system trustee group by file folder
  - File system trustee group by server
  - File system trustee group by trustee

Requirements such as how your report is displayed (email, printer, or file) and exported (.XLS, .DOC, or .HTML) must be selected.

3. Setup jobs to run network scans and the associated report queries. Jobs can be scheduled to run during off peak hours and the process can be completely automated.

Every time a job runs, a new table is created in the database allowing reports to be run anytime on data collected from earlier scans. This could prove invaluable for forensic analysis and investigation on the network. As the data has already been collected, security administrators need not rescan the network every time they need a report.

The design allows for a single job to run multiple network scans as well as multiple report queries. This means that data can be collected and reported across multiple eDirectory trees in the enterprise.

LT Assessment for SUSE
Chapter 2 — Installing LT Assessment for SUSE

Overview

This chapter contains instructions for installing LT Assessment for SUSE. This application can only be installed on computers with a Microsoft Windows operating system installed.

Installation Requirements

The minimum requirements for installing SP1A on a Windows workstation or server include:

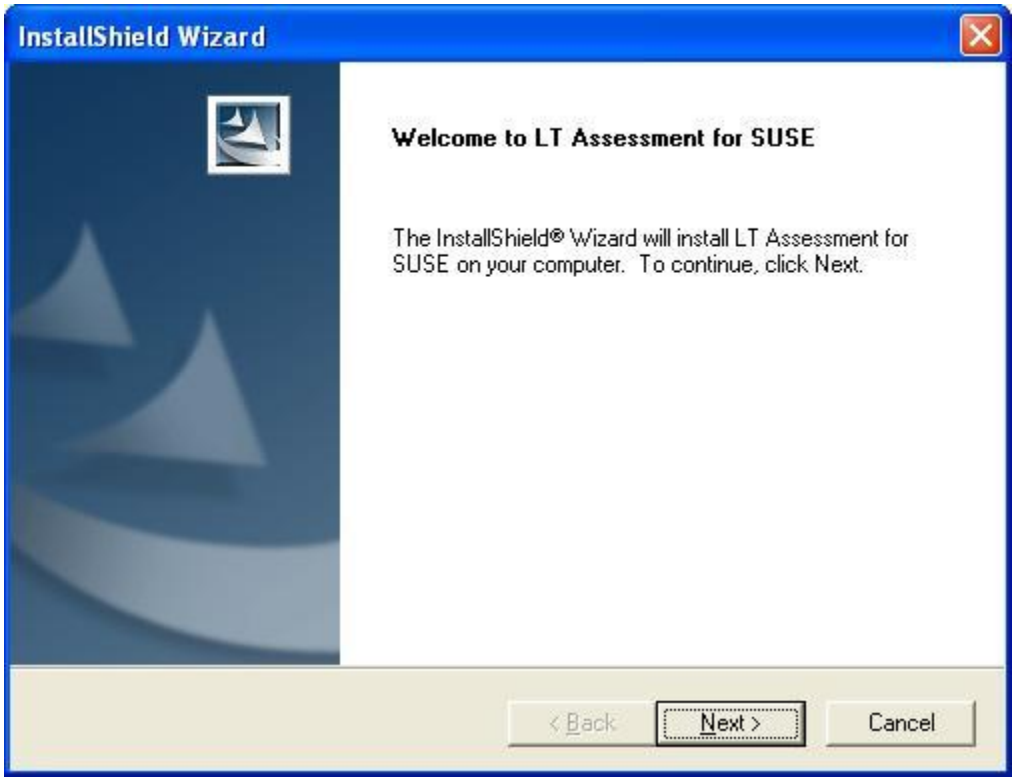
- One of the following operating systems:
  - Windows 2003/2008
  - Windows XP
  - Windows 7
- Novell Client 4.9x or higher for Windows
- 256 MB of RAM recommended

Network scans can only be performed on Novell SUSE-OES/NetWare file server's version 4.x and later.

Installing LT Assessment for SUSE

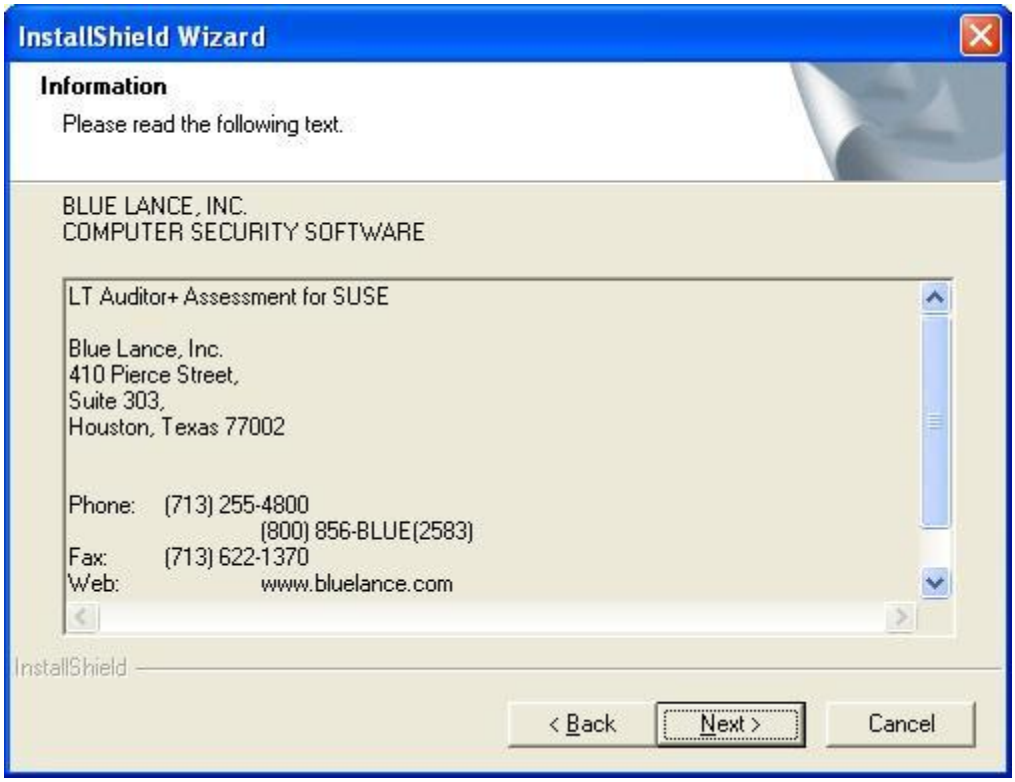
To install LT Assessment for SUSE on a server or workstation, complete the following steps:

1. Insert the LT Assessment for SUSE CD into the CD drive of the server or workstation.
2. If Autorun is enabled, the LT Auditor+ Assessment for NetWare Setup will prepare the InstallShield Wizard. If Autorun is not enabled, execute *Setup.exe* from the root of the LT Auditor+ Assessment for NetWare CD.
3. The InstallShield Wizard displays a Welcome message. Click *Next* to continue.

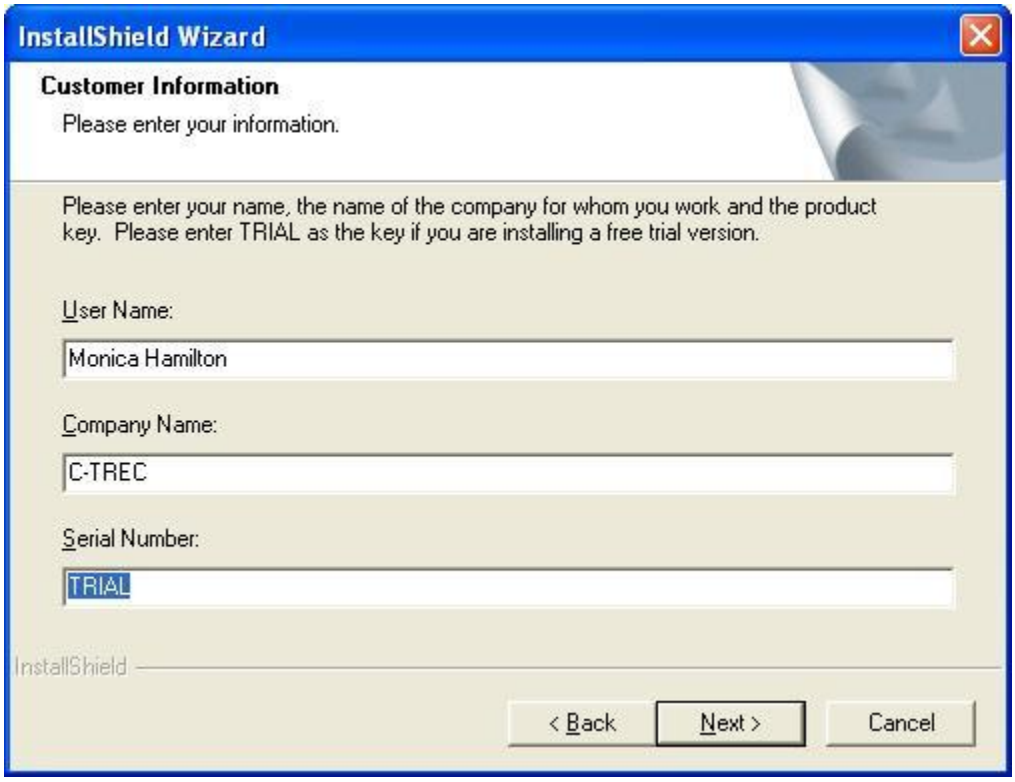


4. The License Agreement screen displays. Scroll down to read the entire license agreement. Click *Yes* to accept the terms of the agreement. If you click *No*, an Exit Setup window will display. Click *Yes* to exit Setup. Click *No* to return to the InstallShield Wizard.

5. The Information screen displays the Blue Lance contact information. Click *Next* to continue.

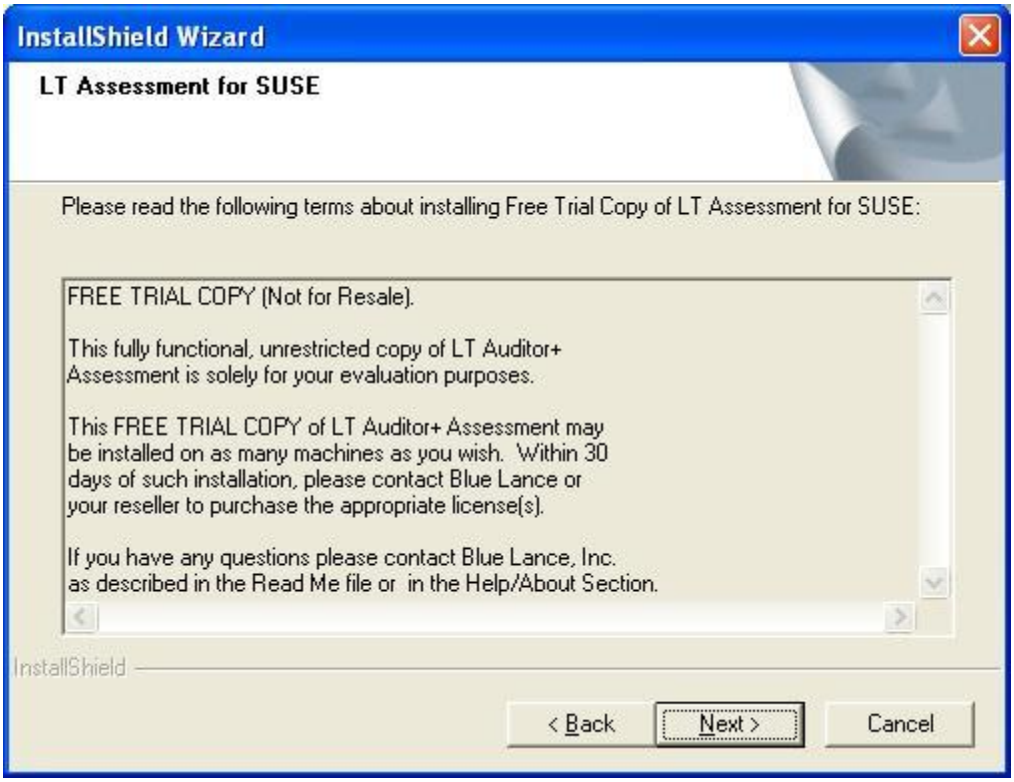

InstallShield Wizard
Information
Please read the following text.
BLUE LANCE, INC.
COMPUTER SECURITY SOFTWARE
LT Auditor+ Assessment for SUSE
Blue Lance, Inc.
410 Pierce Street,
Suite 303,
Houston, Texas 77002
Phone: (713) 255-4800
(800) 856-BLUE(2583)
Fax: (713) 622-1370
Web: www.bluelance.com
InstallShield
< Back
Next >
Cancel

6. The Customer Information screen displays. Enter your user name, company name, and serial number. Click *Next* to continue.

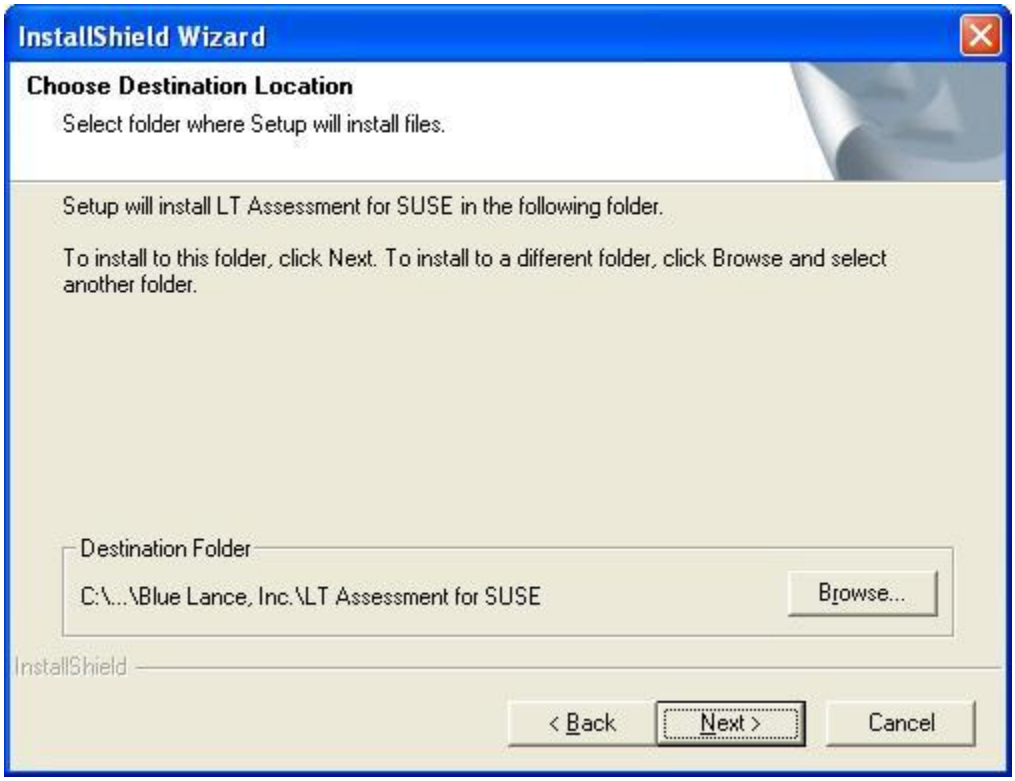


Note
If you entered a serial number, bypass step 7 and go directly to step 8.

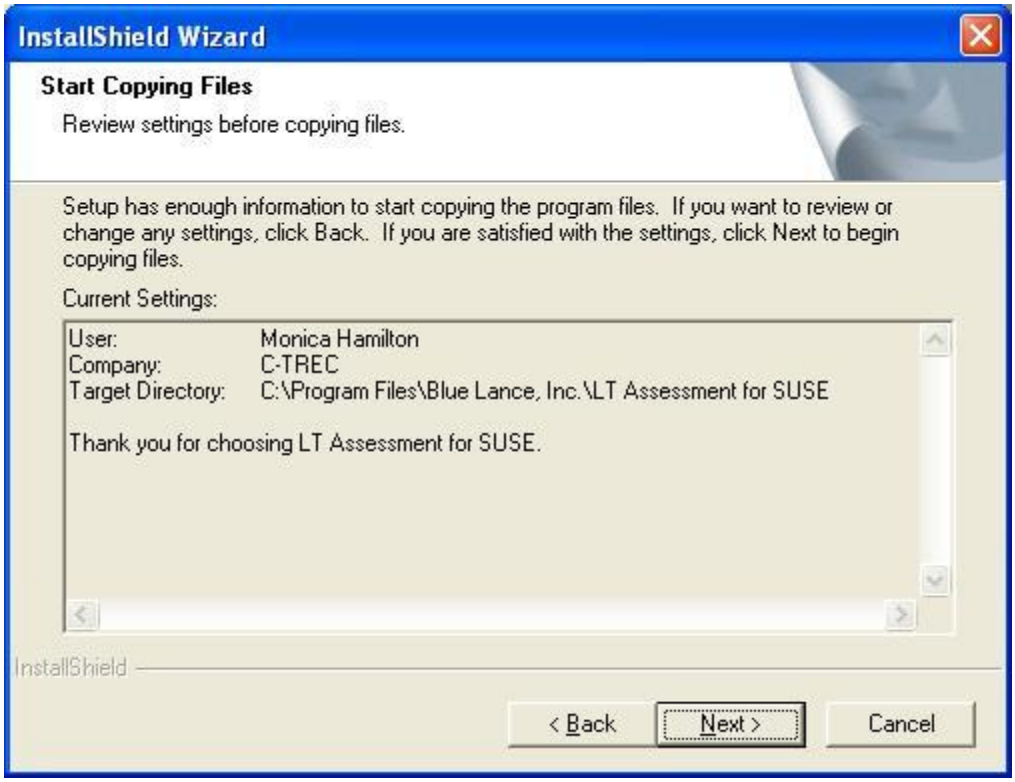
7. If you are installing a trial version of LT Auditor+ Assessment for NetWare, enter *Trial* in the Serial Number field. The LT Auditor+ Assessment for NetWare trial screen will display. Click *Next* to accept the terms and conditions of this trial installation.



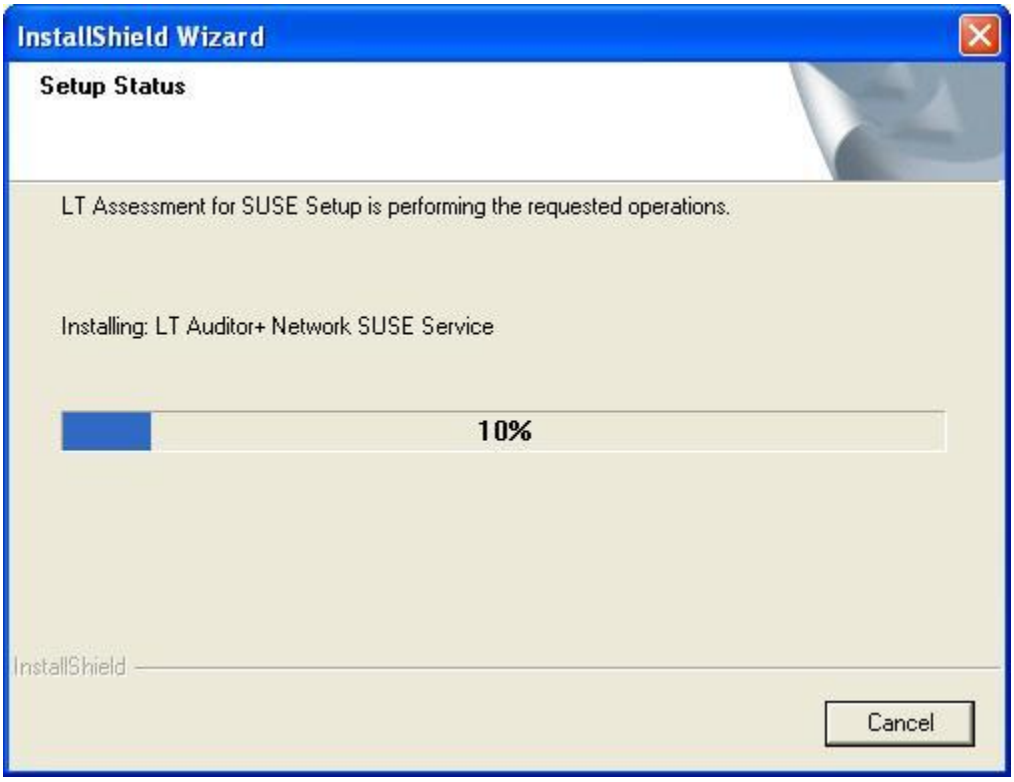
8. The Choose Destination Location screen displays. If you want to save the files to a folder other than the default destination folder, click *Browse* to select a folder. Click *Next* to accept the default destination folder.



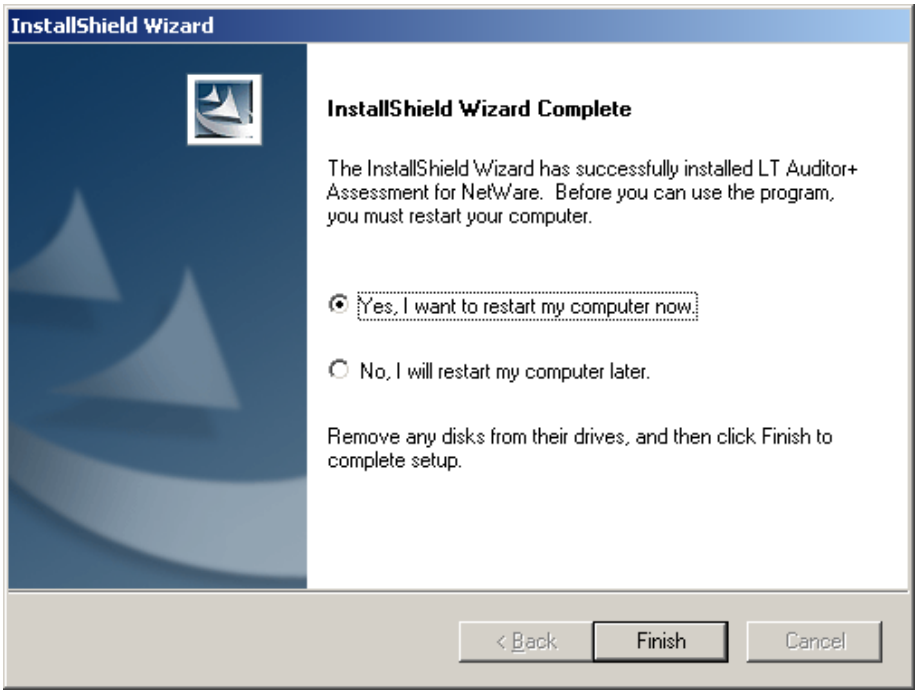
9. The Start Copying Files screen displays the user name and company name entered in the Customer Information window. It also displays the destination path of the application. Click *Next* to begin the installation.


InstallShield Wizard
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
User: Monica Hamilton
Company: C-TREC
Target Directory: C:\Program Files\Blue Lance, Inc.\LT Assessment for SUSE
Thank you for choosing LT Assessment for SUSE.
InstallShield
< Back
Next >
Cancel

10. The Setup Status screen shows the progress of the installation process. You can click *Cancel* at any time to terminate the installation.



11. After all files have been copied and installed, the InstallShield Wizard Complete screen displays. By default, the *Yes, I want to restart my computer now* radio button is selected. Click *Finish* to restart your computer.



!

Important

Before you can use the LT Assessment for SUSE software, you must restart your computer.

Modifying, Repairing, and Uninstalling LT Assessment for SUSE

InstallShield Wizard provides a single method for modifying, repairing, and uninstalling LT Auditor+ Assessment for NetWare on Windows machines. To display the InstallShield Wizard, from the Control Panel window click *Add/Remove Programs* → *LT Auditor+ Assessment for NetWare* → *Change/Remove*.

Modifying LT Assessment for SUSE

Use the Modify option to add new program components. To modify LT Auditor+ Assessment for NetWare, perform the following steps:

1. From the InstallShield Wizard Welcome screen, click *Modify* → *Next*.

2. The Setup Status window displays showing the progress of the modification process.
3. When setup is complete, the Maintenance Complete screen displays. Click *Finish* to exit the InstallShield Wizard window.

Repairing LT Assessment for SUSE

Files can become corrupted if they are accidentally modified. The InstallShield Wizard Repair feature allows you to repair corrupted LT Auditor+ Assessment for NetWare files.

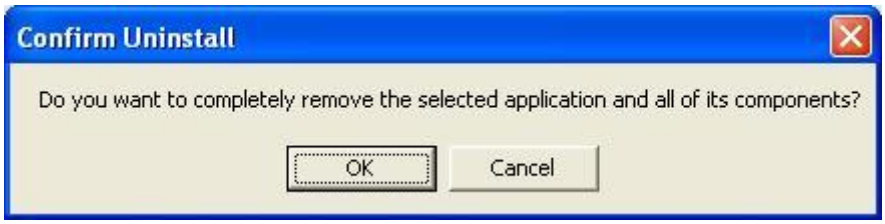
To repair LT Auditor+ Assessment files, perform the following steps:

1. From the InstallShield Wizard Welcome screen, click *Repair* → *Next*. The Setup Status window displays.
2. The InstallShield Wizard automatically finds and repairs corrupted files. When the repair is complete, the InstallShield Wizard Complete screen displays. By default, the *Yes, I want to restart my computer now* radio button is selected. Click *Finish* to exit the InstallShield Wizard window and automatically restart your system.

Uninstalling LT Assessment for SUSE

To remove LT Assessment for SUSE from a machine, perform the following steps:

1. From the InstallShield Wizard Welcome screen, click *Remove* → *Next*.
2. The Confirm Uninstall window displays. Click *OK* to continue the process.



3. The Setup Status window displays. When the Maintenance Complete window displays, LT Assessment for SUSE is deleted. Click *Finish* to exit the InstallShield Wizard window.

LT Assessment for SUSE

Chapter 3 — Using LT Assessment for SUSE

Overview

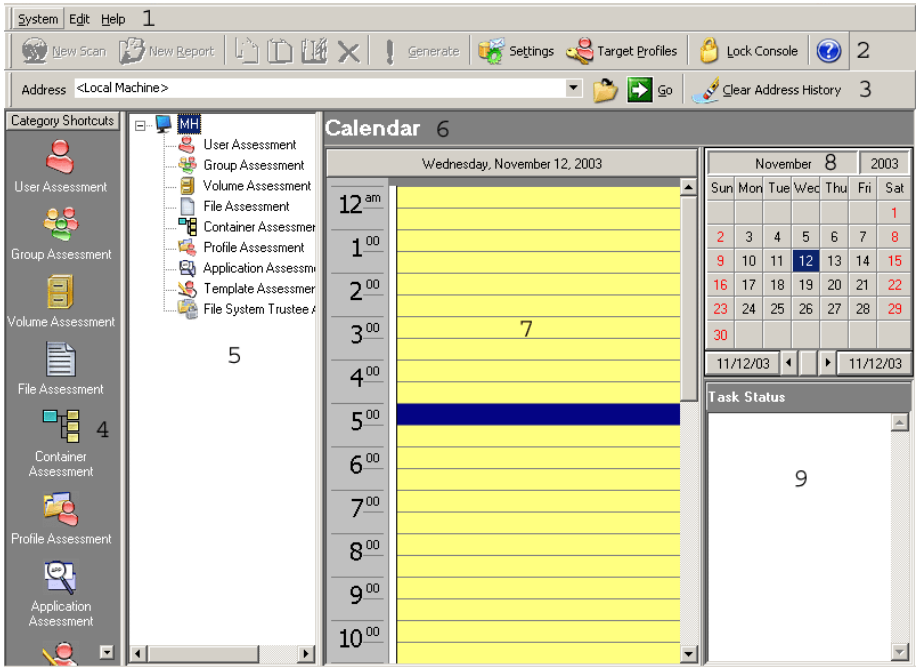
Security assessment of a network is a process by which an audit is performed to determine whether the configurations and settings are compliant with the security policies and practices of the organization.

LT Assessment for SUSE allows you to perform a security assessment of your network by capturing a snapshot of your eDirectory and NetWare servers and checking for vulnerabilities.

In this chapter, you will learn how to use the LT Assessment for SUSE window to:

- Create new scans and report queries.
- Configure e-mail and database settings.
- Create a password that allows you to lock and unlock the console window.
- Create authenticated user profiles.
- Generate reports.

LT Assessment for SUSE Components



LT Assessment for SUSE

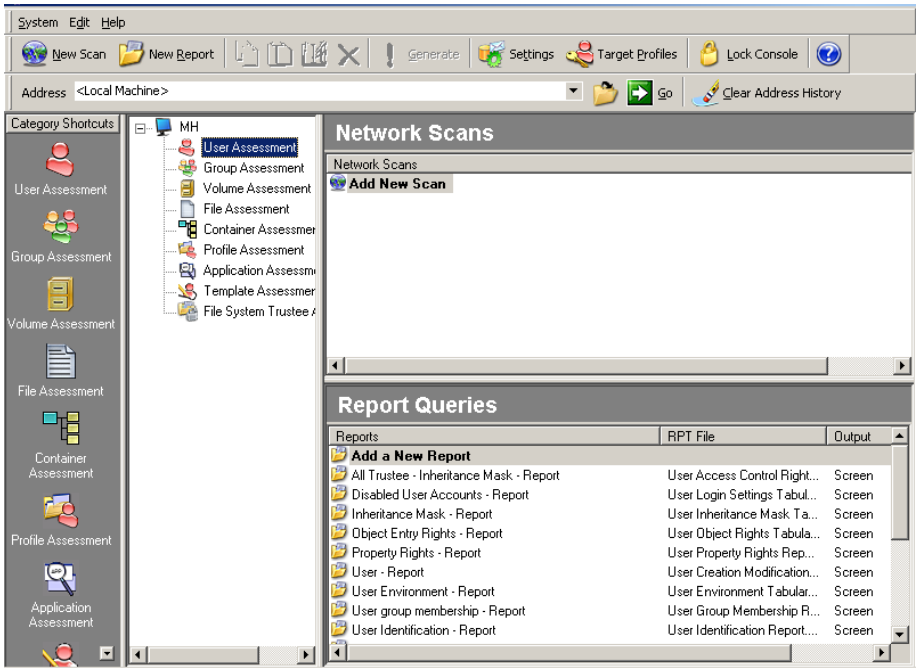
The LT Assessment for SUSE window consists of the following components:

1. **Menu bar** — Provides a variety of options that enable you to:
   - Create new scans and report queries.
   - Copy, paste, and modify existing scans.
   - Configure e-mail and database settings.
   - Create a password that allows you to lock and unlock the console window.
   - Generate reports.
   - View the LT Assessment for SUSE help files and version information.
   - Manage user authentications.
2. **Standard toolbar** — Provides a variety of options that enable you to configure the LT Assessment for SUSE window.

3. **Address bar** — Allows you to connect to remote machines with LT Assessment for SUSE already installed and deploy scans and report queries across multiple networks.
4. **Category Shortcuts window** — Displays the Network Scans and Report Queries panes associated with the selected button.
5. **Assessment Category window** — Lists the Microsoft Windows server or workstation to which you are currently connected and contains the following assessment categories:
   - User Assessment
   - Group Assessment
   - Volume Assessment
   - File Assessment
   - Container Assessment
   - Profile Assessment
   - Application Assessment
   - Template Assessment
   - File System Trustee Assignment Assessment
6. **Calendar** — Allows you to:
   - Create a new job
   - Review the status of your job
   - Delete or modify existing jobs
   - Review jobs previously run

   The Calendar includes the following windows:

   7. **Job Scheduler window** — Allows you to schedule jobs or select a previously existing job to review.
   8. **Calendar window** — Allows you to:
      - Select a specific date for your new job.
      - Select a date to review existing jobs.
   9. **Task Status window** — Displays the status of the selected job in the Job Scheduler window.



If an assessment category is selected, the LT Assessment for SUSE window displays the following sections:

- **Network Scans** — Allows you to create a scan by selecting a specific target profile.
- **Report Queries** — Allows you to modify existing report queries and create new report queries for the assessment categories.

Displaying the LT Assessment for SUSE Window

To display the LT Assessment for SUSE window, select *Start* → *Programs* → *LT Auditor+* → *LT Assessment for SUSE* → *Assessment Console*.

Assessment for NetWare License Agreement Window

If you entered Trial in the Serial Number field during installation, the LT Assessment for SUSE License Agreement window displays. From this screen you can, perform one of the following tasks:

- Enter a license key and click the *Apply License* button. Click *OK* after the license key is successfully registered. Next time the Assessment Console is launched you can deselect the *Show license key at startup* check box to prevent the LT Assessment for SUSE License Agreement window from displaying.
- Click *Close* to continue to evaluate the trial copy of LT Assessment for SUSE.

Menu Bar

From the Menu bar, you can select the following options:

- System
- Edit
- Help

System

The options on the System menu allow you to:

- Create new scans and report queries.
- Configure e-mail and database settings.
- Create a password that allows you to lock and unlock the console window.
- Create user authentications.
- Generate reports.

From the System menu, you can select:

- **New Scan** — Displays the Scan Details window
- **New Report** — Displays the Report Query window
- **Settings** — Displays the E-mail and Database Settings window
- **Security** — Displays the Setup a password window
- **Target Profiles** — Displays the Target Profiles for Scans window
- **Generate** — Runs a report based on the selected report query
- **Exit** — Closes the LT Assessment for SUSE window

Edit

Features on the Edit menu allow you to copy, paste, modify, and delete an existing scan or a report query. From the Edit menu you can select:

- **Copy** — Copies network scans and report queries from one LT Assessment for SUSE to a remote LT Assessment for SUSE
- **Paste** — Pastes network scans and report queries from one LT Assessment for SUSE to a remote LT Assessment for SUSE
- **Modify** — Displays the window of the selected object, allowing you to modify that object
- **Delete** — Deletes the currently selected object

Help

Features on the Help menu allow you to review the LT Assessment for SUSE help files and version information. From the Help menu you can select:

- **Contents** — Displays a list of help files
- **About LT Assessment for SUSE** — Displays current version information

Standard Toolbar

The Standard Toolbar provides a variety of options that enable you to configure the LT Assessment for SUSE window. The buttons on the Standard toolbar are described in the following table.

Button	Icon	Function
New Scan	New Scan	Displays the Scan Details window
New Report	New Report	Displays the Report Query window
Copy		Allows you to copy the selected object
Paste		Allows you to paste a copied object to a remote LT Assessment for SUSE
Modify		Displays the window of the selected object so that you can modify that object
Delete		Deletes the currently selected object
Generate	Generate	Runs the selected query
Settings	Settings	Displays the E-mail and Database Settings window
Target Profiles	Target Profiles	Displays the Target Profiles for Scans window
Lock Console	Lock Console	Displays the Enter password window
Contents		Displays the Help file

Locking and Unlocking the LT Assessment for SUSE Window

The LT Assessment for SUSE window includes a security feature that allows you to lock and unlock the console window.

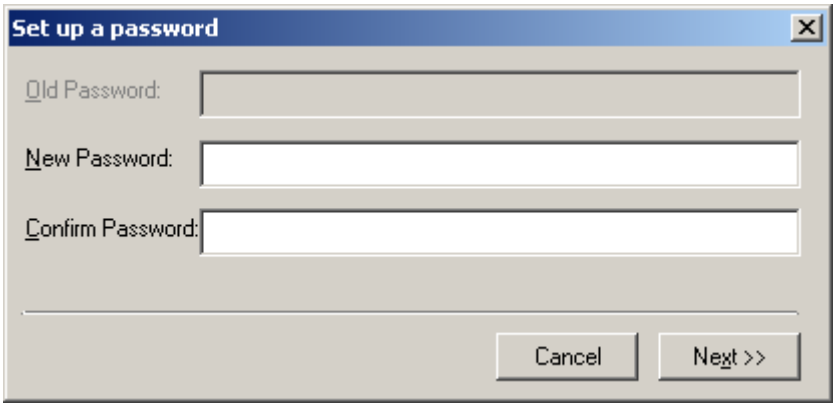
! **Important**

If you create a new password, you will be unable to disable this security feature.

Creating a Password

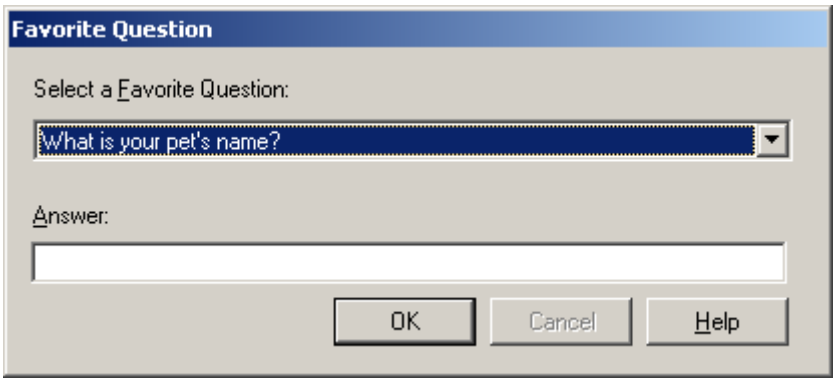
To create a password for locking and unlocking the LT Assessment for SUSE window, perform the following steps:

1. From the System menu on the Menu bar, click *Security*. The Set up a password window displays.

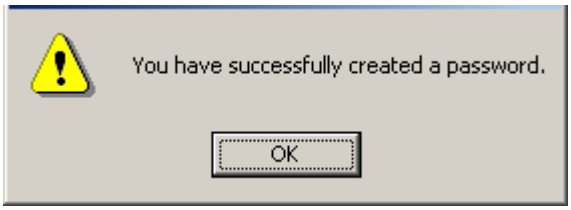


2. Enter a password in the New Password and Confirm Password fields. Click *Next* to continue.

3. The Favorite Question window displays. From the Select a Favorite Question drop-down menu, select one of the following questions:
   - What is your pet's name?
   - What was the name of your high school?
   - What is your mother's maiden name?
   - What is the name of the city you were born?



4. In the Answer field, enter an answer for the question you selected.
5. Click *OK*. A window displays stating that you have successfully created a new password. Click *OK* to exit this window.

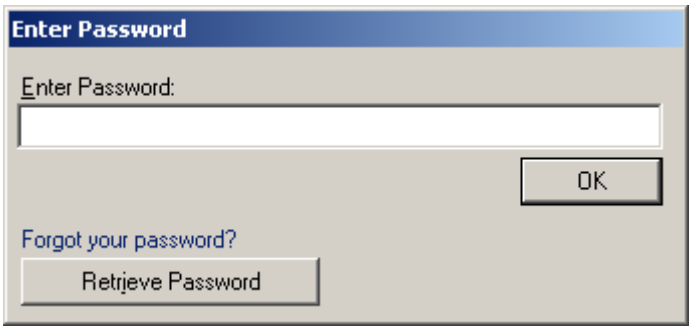


! **Important**
After you create a password, the password must be entered each time you launch the LT Assessment for SUSE application.

Locking the LT Assessment for SUSE Window

To lock the LT Assessment for SUSE window, perform the following steps:

1. From the Standard toolbar, click the *Lock Console* button. The following window displays.



2. The LT Assessment for SUSE window will remain locked until the correct password is entered in the Enter Password field.

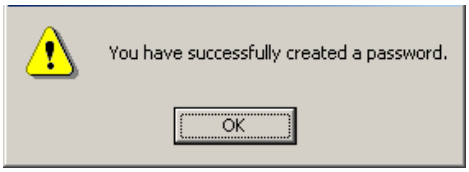
Unlocking the LT Assessment for SUSE window

To unlock the LT Assessment for SUSE window, perform the following steps:

1. In the Enter Password field, enter the password you created to unlock the console window.
2. Click *OK* to unlock the machine.

If you forget your password, perform the following steps:

1. From the Enter Password window, click the *Retrieve Password* button. The Favorite Question window displays.
2. Enter an answer for the security question you previously selected and click *OK*.
3. If you wish to reset your password, click *Yes* to display the Set up a password window.
4. Enter a password in the New Password and Confirm Password fields. Click *Next*.
5. Click *OK* to accept the selected question and answer. A window displays stating that you have successfully created a new password. Click *OK* to exit this window.



Address Bar

The Address bar allows you to connect to remote machines with LT Assessment for SUSE already installed. This feature enables administrators to set up jobs and create scans on the selected remote machines allowing you to manage multiple machines in an environment.

Note
A mapped drive to the remote computer must exist on your local computer.

The directories of machines previously configured are stored in the address history field. They can be accessed by clicking the Address Bar drop-down arrow, selecting the required path, and clicking *Go*.

To remove all address history information, click the *Clear Address History* button.

The options on the Address bar are described in the following table.

Button	Icon	Function
Address bar		Allows you to enter a directory and map to a remote computer
Browse		Allows you to browse to a remote computer
Go		Connects to the entered or selected computer
Clear Address History		Clears the address history of all selected computers

Connecting to a Remote Machine

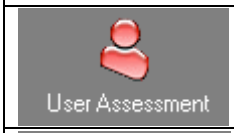
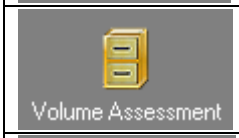
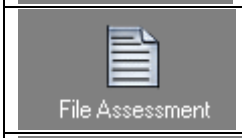
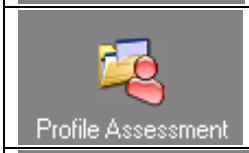
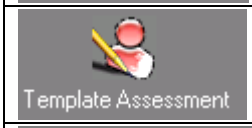
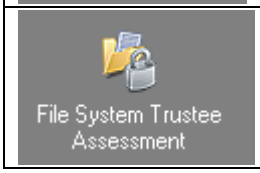
If you have network authentication to a remote computer and want to configure the LT Assessment for SUSE application on that machine, provide the complete path to the LTAudit.iif file located in the installation folder on the remote machine.

Enter the path of the LTAudit.iif file into the Address Bar field or click the *Browse* button on the Address Bar to locate a specific path. After the entire path is provided, click *Go* to connect to the remote computer.

From the Address bar, select the local machine by clicking <*Local Machine*> → *Go*.

Category Shortcut Window

Each security assessment features its own network scans and report queries. Use the Category Shortcut window to display the panes associated with the selected button. These buttons are described in the following table.

Icon	Function
	Displays existing User Assessment network scans and report queries
	Displays existing Group Assessment network scans and report queries
	Displays existing Volume Assessment network scans and report queries
	Displays existing File Assessment network scans and report queries
	Displays existing Container Assessment network scans and report queries
	Displays existing Profile Assessment network scans and report queries
	Displays existing Application Assessment network scans and report queries
	Displays existing Template Assessment network scans and report queries
	Displays existing File System Trustee Assessment network scans and report queries

Assessment Category Window

The Assessment Category window lists all of the available category assessments in a tree structure. Selecting the root of the tree structure displays the Calendar.

Note
The Calendar will be discussed later in this chapter.

Right-clicking on the root of the tree structure displays a drop-down menu where you can select *Settings* to modify the e-mail and database settings.

Note
The E-mail and Database Settings window will be discussed later in this chapter.

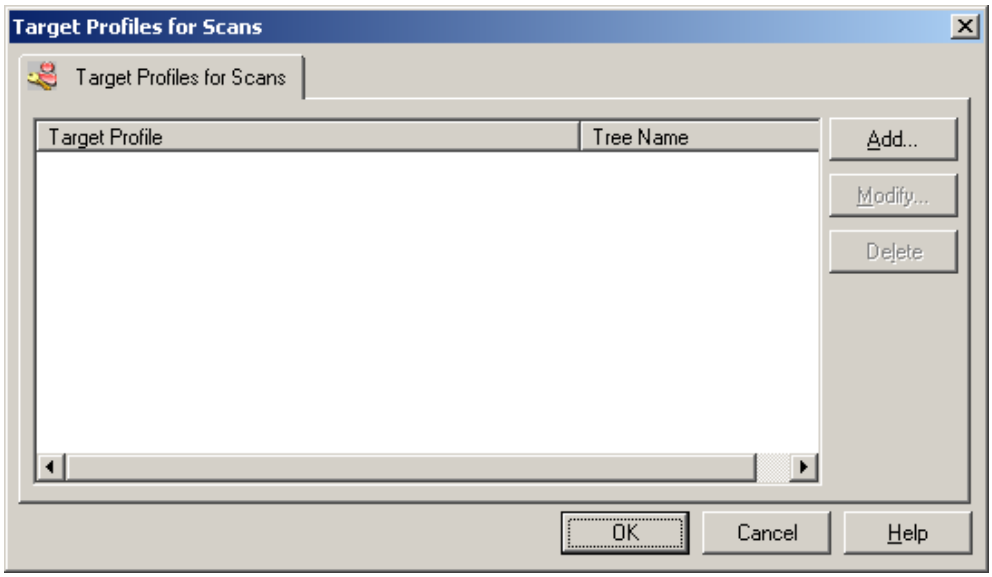
The main directory contains the following assessment categories:

- User Assessment
- Group Assessment
- Volume Assessment
- File Assessment
- Container Assessment
- Profile Assessment
- Application Assessment
- Template Assessment
- File System Trustee Assessment

Right-click on any of the assessment categories to display a drop-down menu, which allows you to select the following options:

- **New Scan** — Displays the Scan Details window
- **New Report** — Displays the Report Query window
- **Copy** — Allows you to copy the selected object
- **Paste** — Allows you to paste a copied object to a remote LT Assessment for SUSE
- **Modify** — Displays the selected object's window so that you can modify that object
- **Delete** — Deletes the currently selected object
- **Generate** — Runs a report based on the selected report query
- **Settings** — Displays the E-mail and Database Settings window

Target Profiles for Scans



Using the Target Profiles for Scans window, you can create an authenticated user profile. To display the Target Profiles for Scans window, perform one of the following steps:

- From the System menu on the Menu bar, click *Target Profiles*.
- From the Standard toolbar, click the *Target Profiles* button.

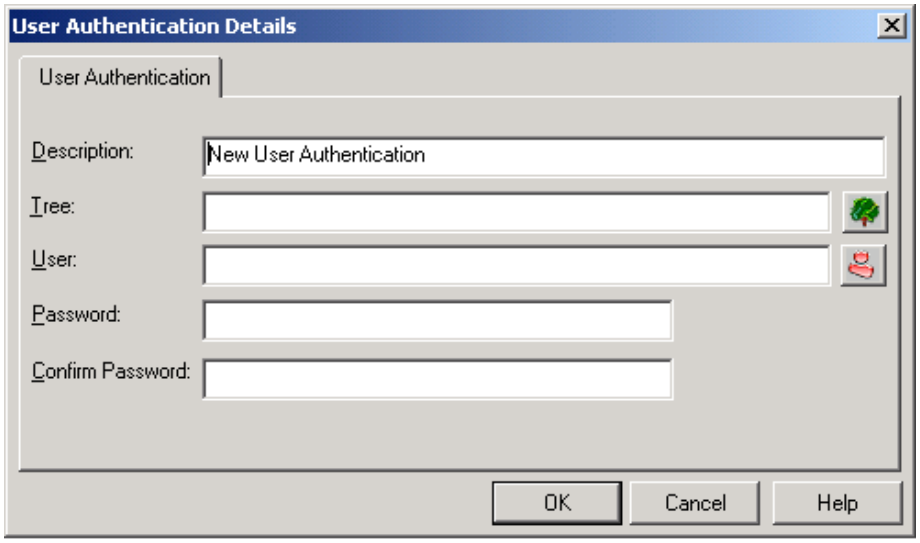
!

Important

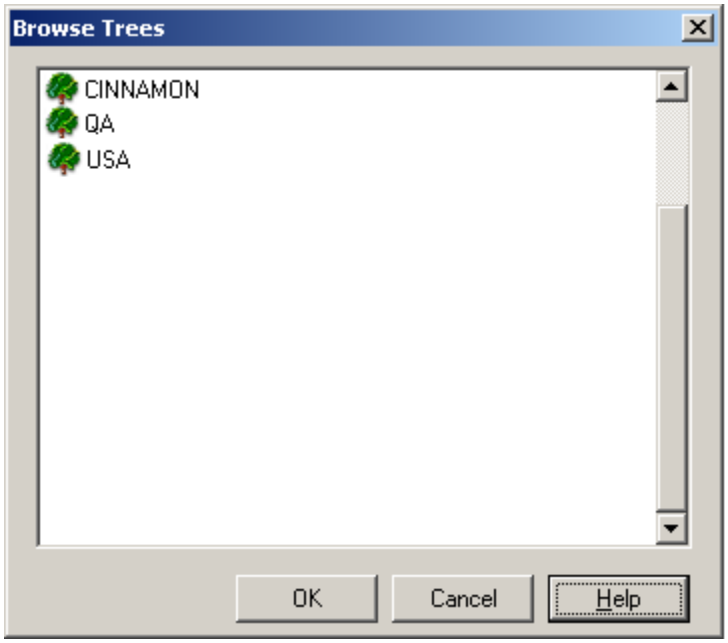
You must create a target profile before using the Scan Details window. The Scan Details window will be discussed later in this chapter.

To save an authenticated user profile, perform the following steps:

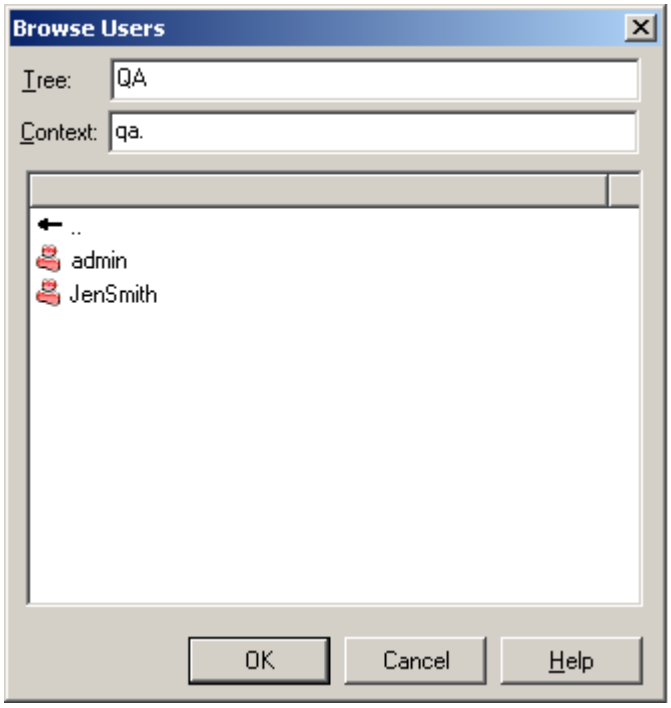
1. Display the Target Profiles for Scans window.
2. Click the *Add* button. The following window displays.



3. In the Description field, enter a name or description to help identify the specific user. If you do not enter a name for this field, the name entered in the User field will automatically be inserted into the Description field.
4. In the Tree field, enter a Novell Directory Service (NDS) tree name. To browse for a specific tree, click the button located to the right of the Tree field. The following window displays.



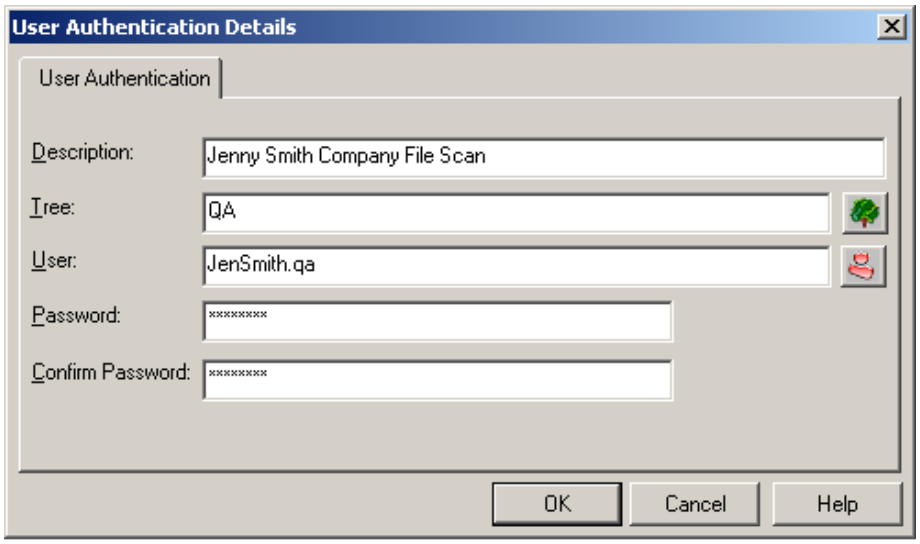
5. Select a tree name and click *OK* to return to the User Authentication Details window. The tree name you selected now displays in the Tree field.
6. In the User field, enter a user name. To browse for a specific user name, click the button located to the right of the User field. The following window displays.



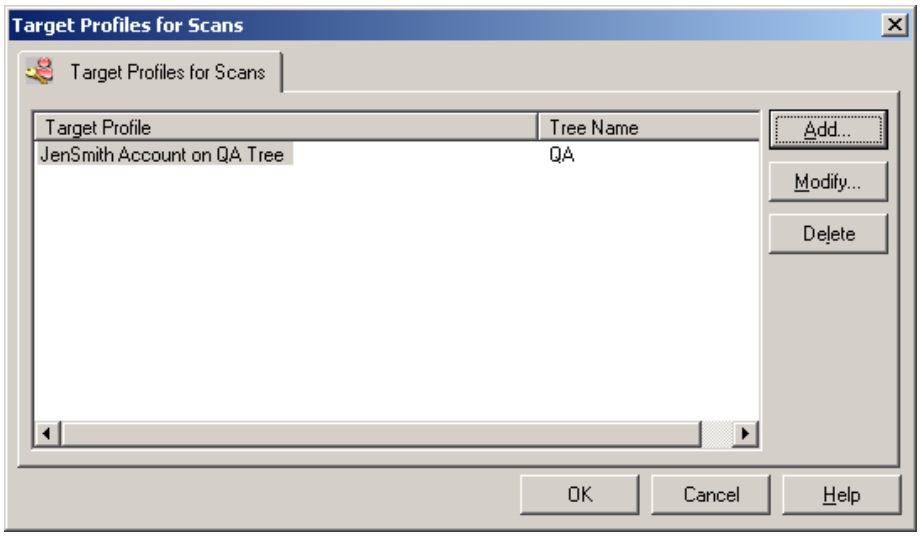
! **Important**
The user name that you enter or select must have browse rights enabled.

7. Select a user name and click *OK* to return to the User Authentication Details window. The user name you selected now displays in the User field.

8. In the Password and Confirm Password fields, enter the password that allows you to authenticate to the selected network.

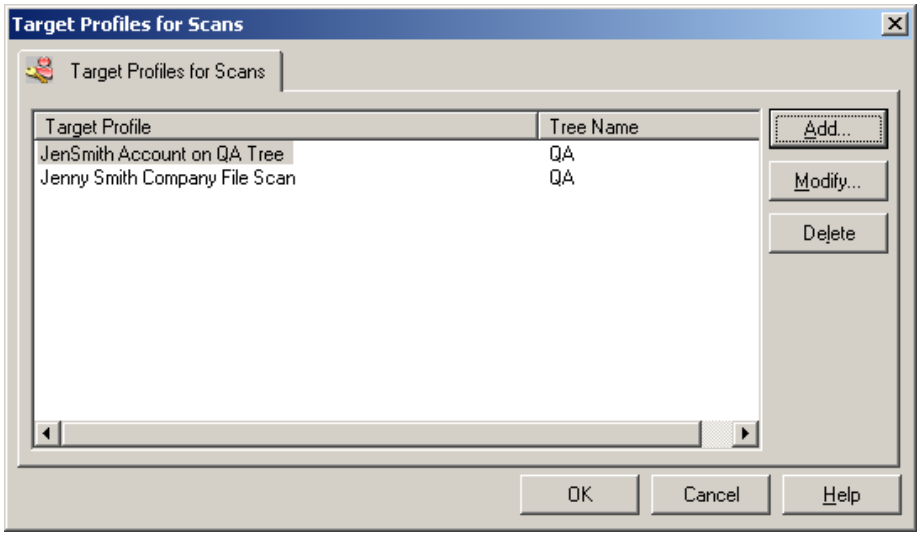


9. Click *OK* to save your changes and exit the User Authentication Details window. The new authenticated user profile displays in the Target Profiles for Scans window.



To delete an existing profile, perform the following steps:

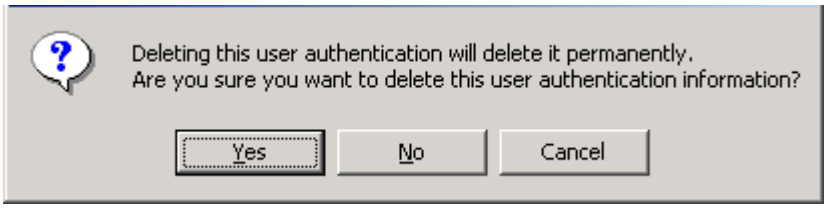
1. Display the Target Profiles for Scans window.
2. From the Target Profiles for Scans tab, select the name of the user profile you want to delete.



Important

Target profiles that are being used for an existing scan cannot be deleted. You must delete the scan or remove the target profile from the scan before you can delete the selected target profile.

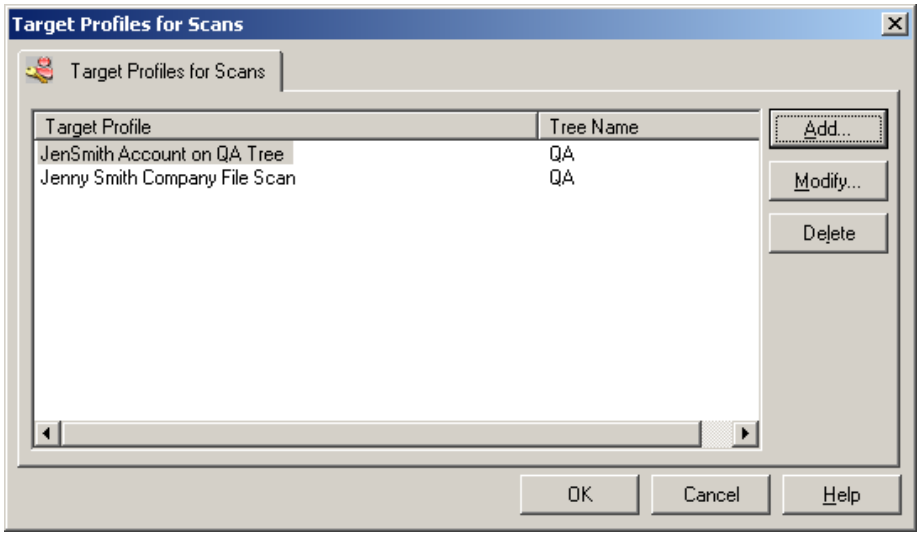
3. Click *Delete*. The following window displays stating that the user authentication profile will be permanently deleted. Click *Yes* to confirm the deletion.



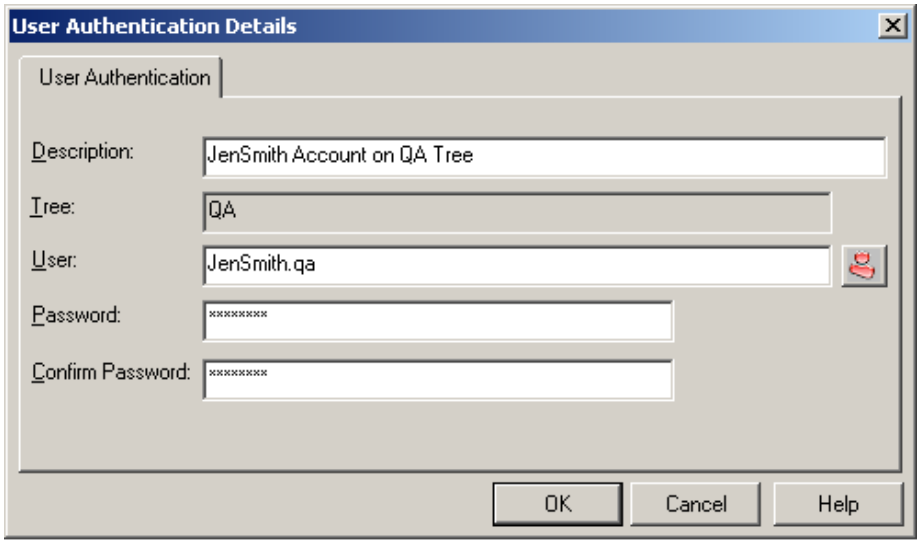
4. Click *OK* to exit the Target Profiles for Scans window.

To modify an existing user profile, perform the following steps:

1. Display the Target Profiles for Scans window.
2. From the Target Profiles for Scans tab, select the name of the profile you want to modify.

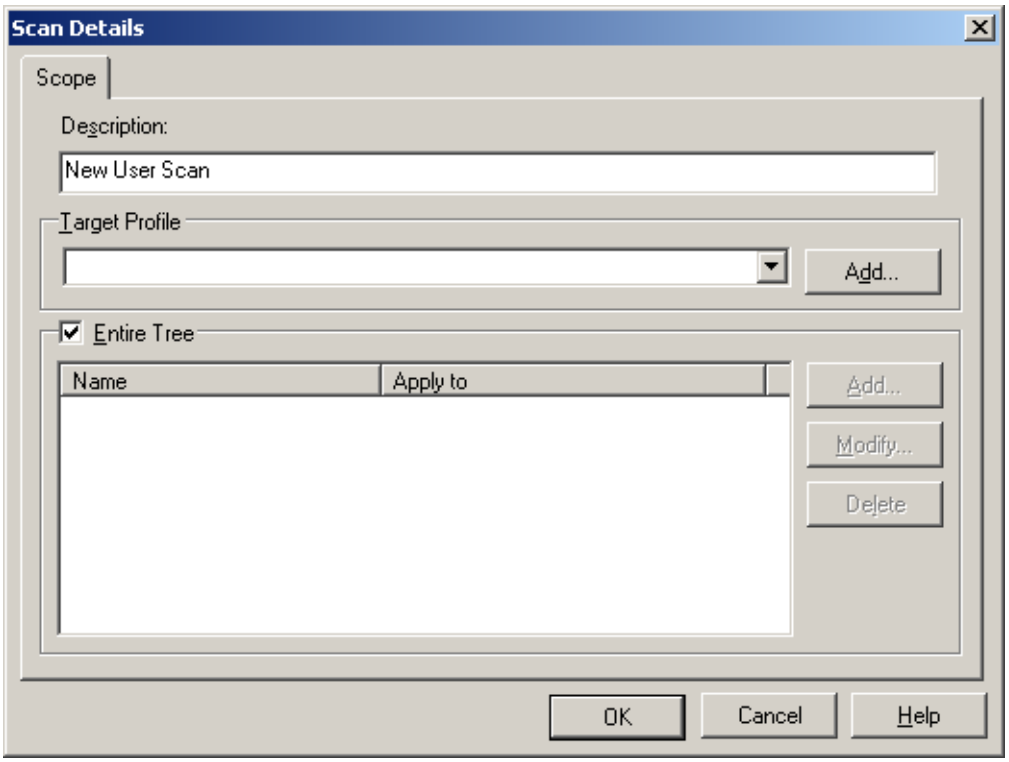


3. Click *Modify*. The following window displays.



4. After you have modified the existing profile, click *OK* to save your changes and exit the User Authentication Details window.
5. Click *OK* to exit the Target Profiles for Scans window.

Network Scans



A network scan specifies the scope of data to be collected from the eDirectory. The Scan Details window allows you to select a target profile. Based on the assessment category you select, you can select a specific:

- Container in the tree to be scanned (User Assessment, Group Assessment, Container Assessment, Profile Assessment, Application Assessment, and Template Assessment).
- Volume to be scanned (Volume Assessment).
- File and folder to be scanned (File Assessment).
- Container in the tree to be scanned (File System Trustee Assessment).

Using the Job Details window, you can select the scan that you created to perform a snapshot of the current configuration of your network.

Note
The Job Details window will be discussed later in this chapter.

From the Assessment Category window, select one of the nine assessment categories to display the Network Scans pane.

To display the Scan Details window, use any of the following methods:

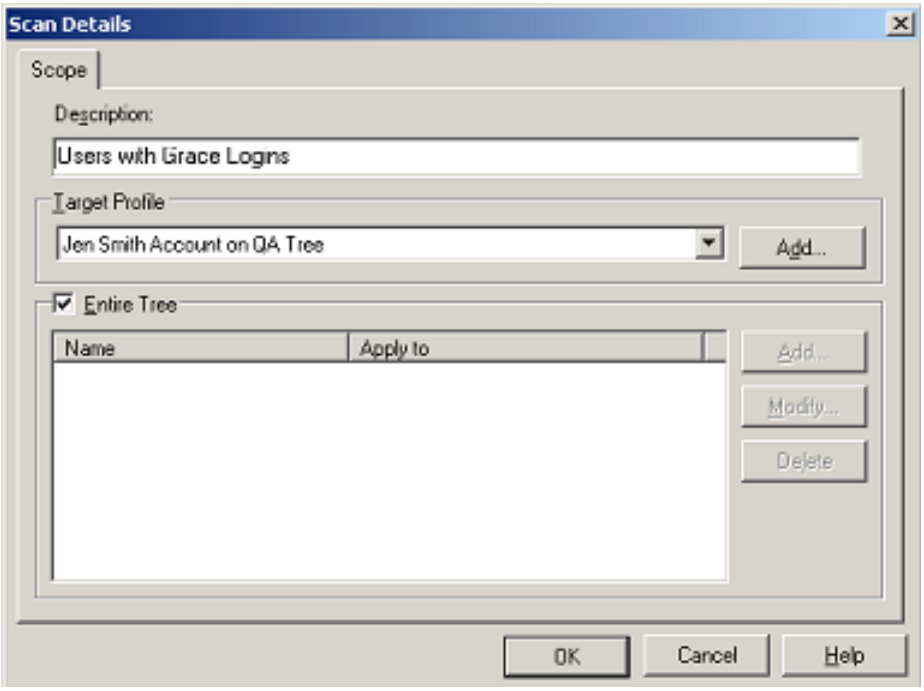
- From the System menu on the Menu bar, click *New Scan*.
- From the Standard toolbar, click the *New Scan* button.
- From the Assessment Category window, right-click to display the drop-down menu. From this menu, select *New Scan*.
- From the Network Scans pane in the LT Assessment for SUSE window, right-click and select *New Scan* from the drop-down menu.
- From the Network Scans pane in the LT Assessment for SUSE window, double-click *Add New Scan*.

Selecting a Target Profile from the Scan Details Window

To modify the Scan Details window, perform the following steps from the Scans Details window:

1. In the Description field, enter a name or description to help identify the individual scan.
2. Select the Target Profiles drop-down arrow. Select a preexisting target profile. To create a new target profile, perform the following steps:
   a. From the Scan Details window, click *Add*. The Target Profiles for Scans window displays.
   b. Click *Add*. The User Authentication Details window displays.
   c. In the Description field, enter a name or description to help identify the specific user. If you do not enter a name for this field, the name entered in the User field will automatically be inserted into the Description field.
   d. In the Tree field, enter a NDS tree name or click the button to the right of the Tree field to browse for a specific tree.
   e. In the User field, enter a user name or click the button located to the right of the User field to browse for a specific user name.
   f. In the Password and Confirm Password fields, enter the password that allows you to authenticate to the selected network.
   g. Click *OK* to exit the User Authentication Details window.
   h. From the Target Profiles for Scans window, select the newly created user profile. Click *OK* to exit the Target Profiles for Scans window and return to the Scan Details window.

3. A description for the target profile you selected displays in the Target Profiles field.



4. Based on the assessment category you selected to display the Network Scans pane, you can select a specific container in a tree, a specific volume, or file/folder.

Note

If you selected the User Assessment, Group Assessment, Container Assessment, Profile Assessment, Application Assessment, or Template Assessment, continue to page 3-25 of this user guide for complete instructions for selecting a container.

If you selected the Volume Assessment category, continue to page 3-28 of this user guide for complete instructions for selecting a volume.

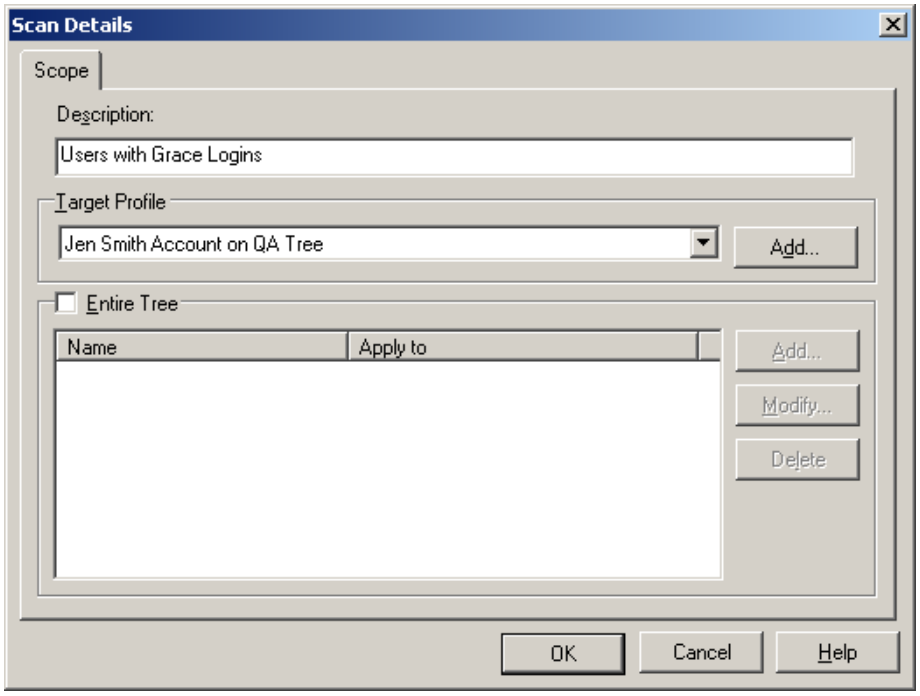
If you selected the File Assessment category, continue to page 3-31 of this user guide for complete instructions for selecting a file.

If you selected the File System Trustee Assessment category, continue to page 3-42 of this user guide for complete instructions for selecting a file.

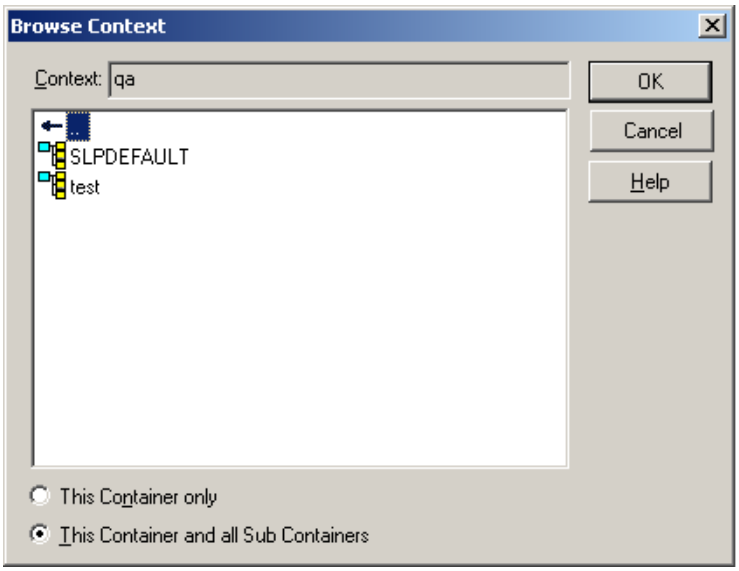
Selecting a Specific Container from the Scan Details Window

If you selected the User Assessment, Group Assessment, Container Assessment, Profile Assessment, Application Assessment, or Template Assessment, by default the *Entire Tree* check box is selected. To scan a specific container of the tree, perform the following steps:

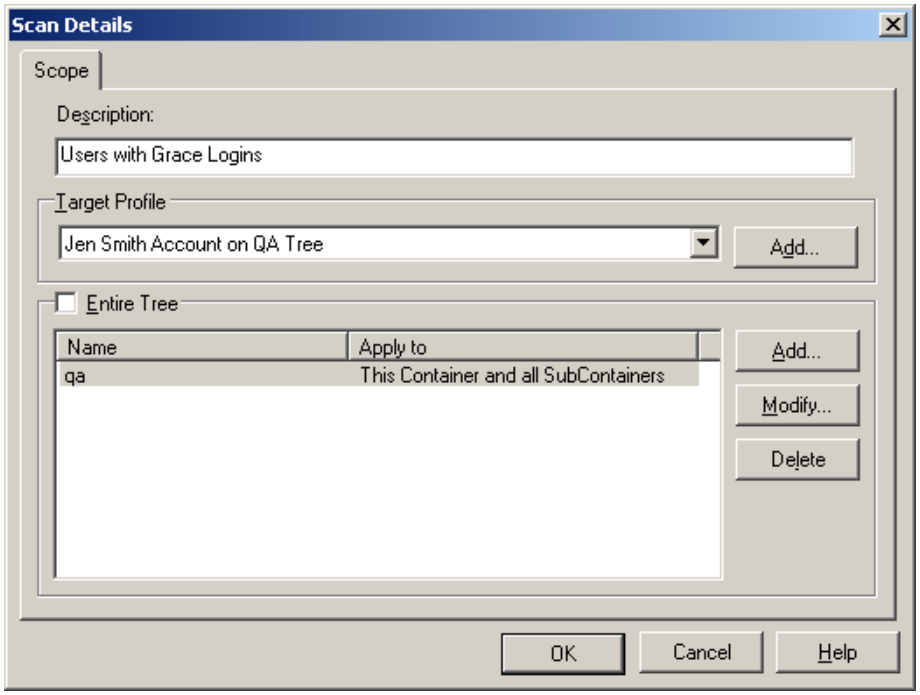
1. Deselect the *Entire Tree* check box.



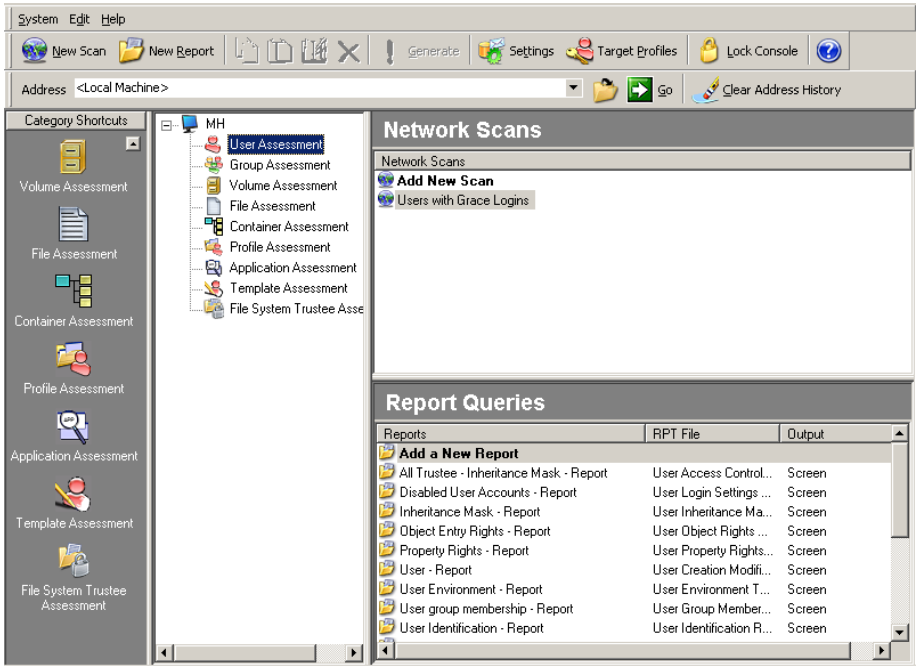
2. Click the *Add* button. The Browse Context window displays.



3. Select a container. Your selection displays in the Context field.
4. By default the *This Container and all Sub Containers* radio button is selected. To scan only the selected container, click *This Container only*. Click *OK* to exit the Browse Context window.
5. The selected container now displays in the Name column of the Scan Details window.



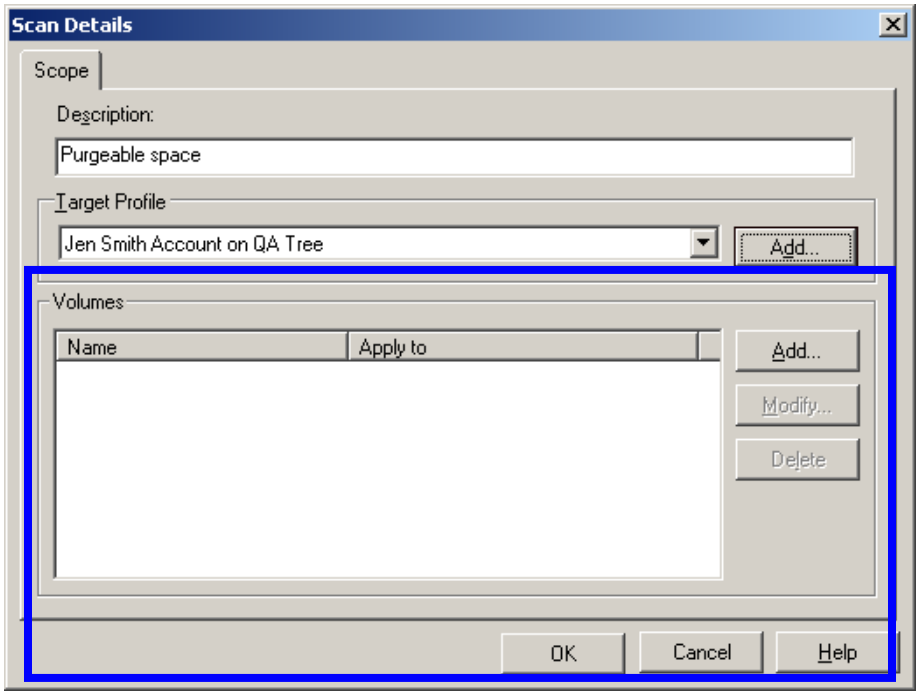
6. Click *OK* to save your changes and exit the Scan Details window. Your new scan displays in the Network Scans column of the LT Assessment for SUSE window.



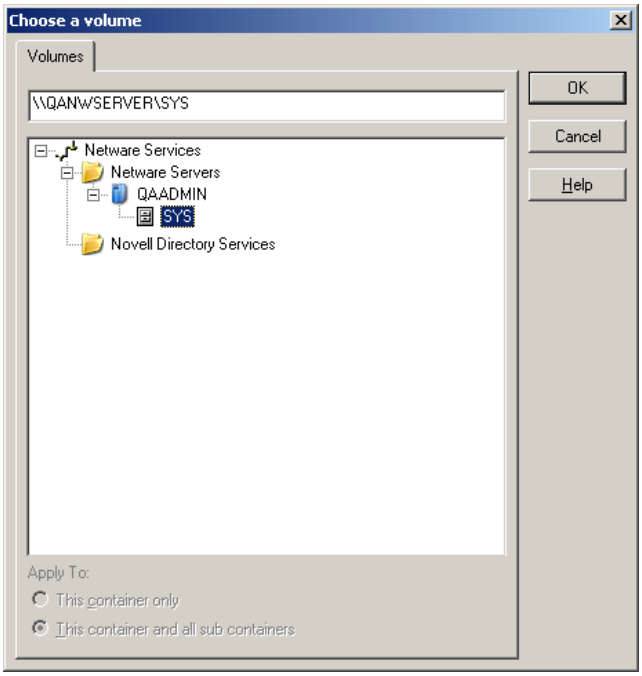
Selecting a Specific Volume from the Scan Details Window

If you selected the Volume Assessment category, you can add a particular volume by performing the following steps:

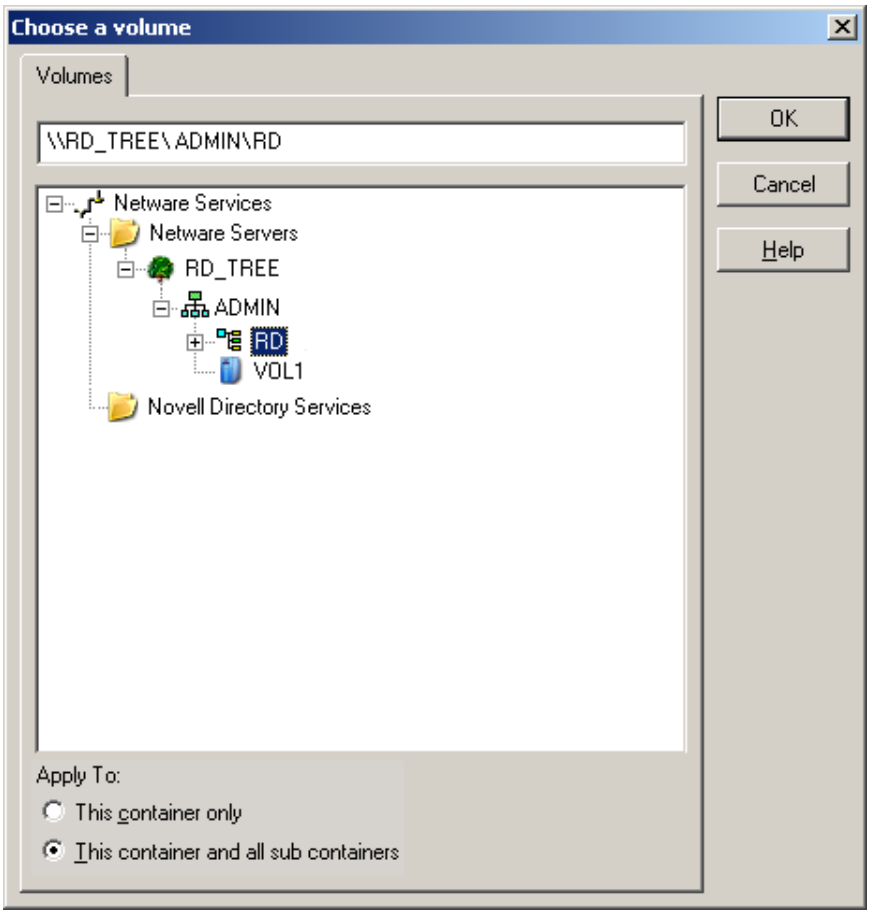
1. Locate the Volumes section of the Scan Details window.



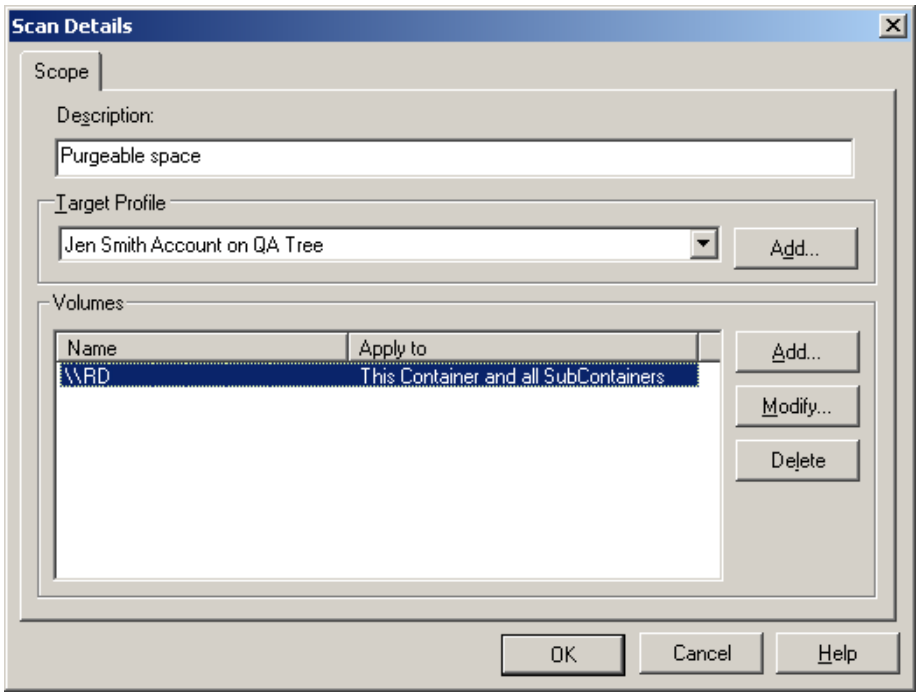
2. Click the *Add* button. The Choose a volume window displays.



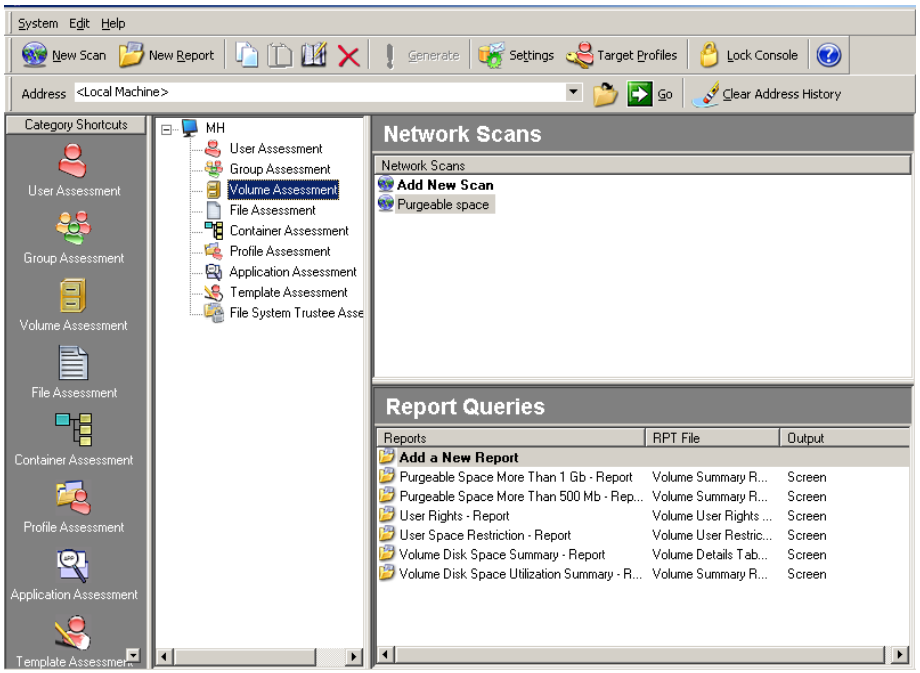
3. Select a volume. If you selected an organizational unit, organization, or container, the Apply to section will be enabled. By default the *This container and all sub containers* radio button is selected. Click *This container only* to scan only the containers in the selected object. Click *OK* to return to the Scan Details window.



4. The selected volume now displays in the Volumes section of the Scan Details window. Click *OK* to save your changes and exit the Scan Details window.



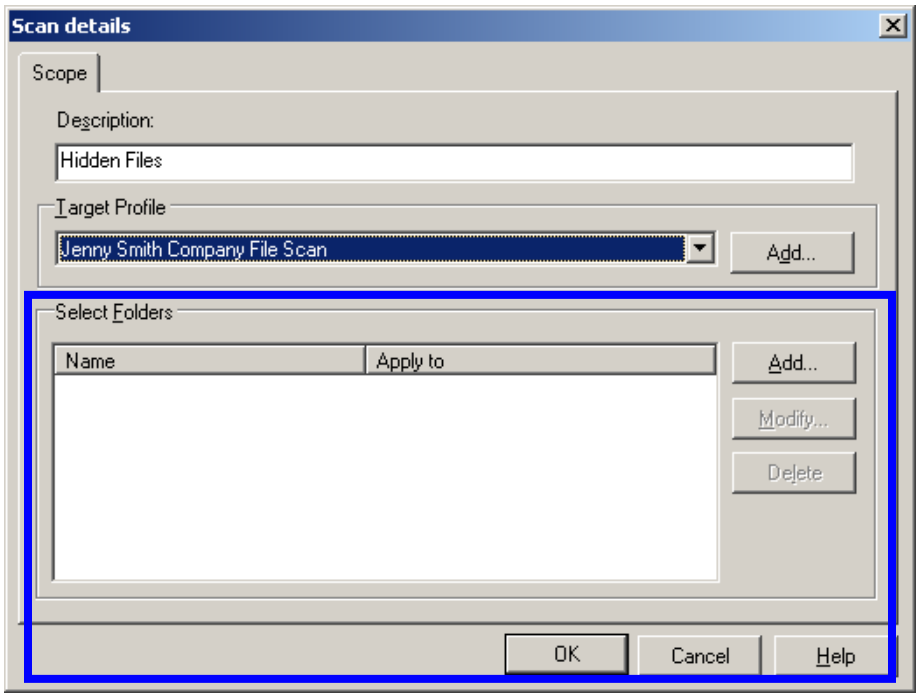
5. Your new scan displays in the Network Scans column of the LT Assessment for SUSE window.



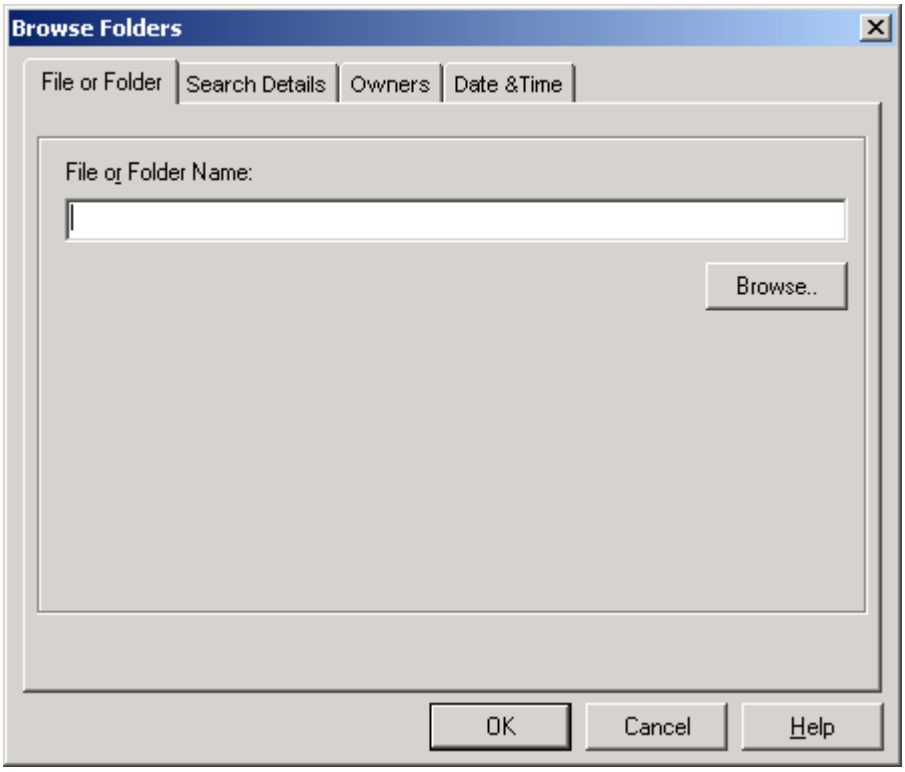
Selecting a Specific Folder or File from the Scan Details Window

If you selected the File Assessment category, you can select a specific folder or file to scan by performing the following steps:

1. From the Scan Details window, locate the Select Folders section.

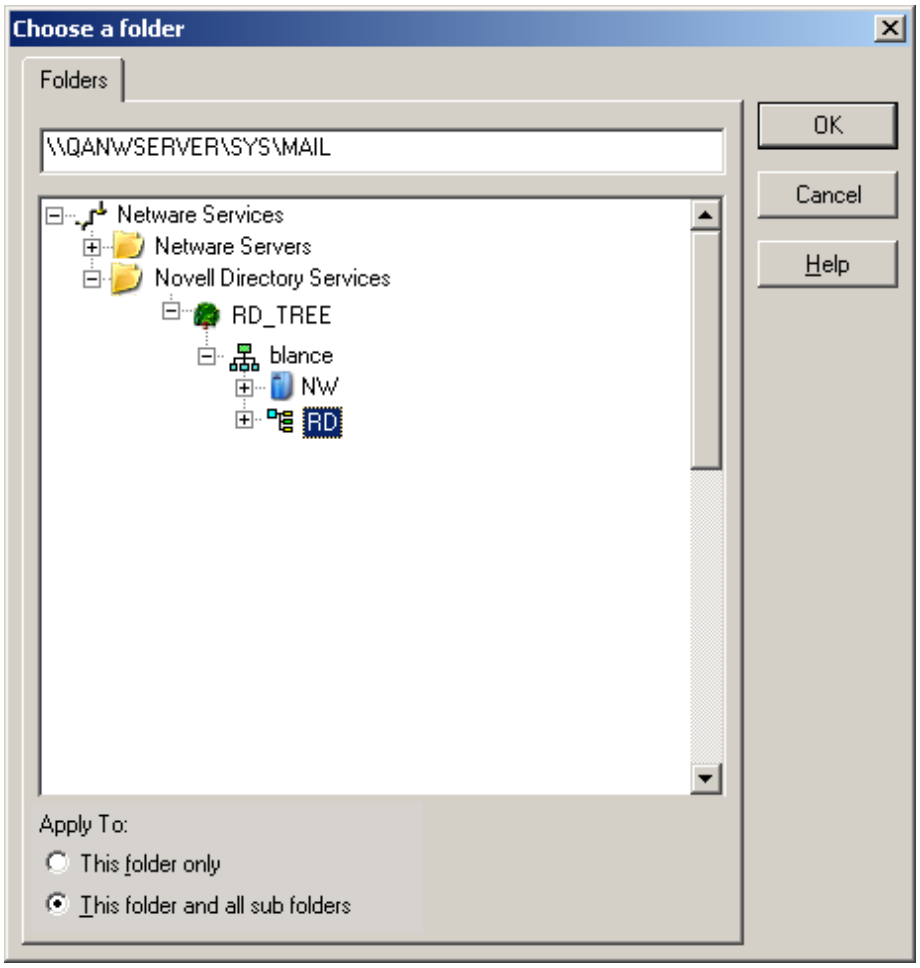


2. Click the *Add* button. The following window displays.



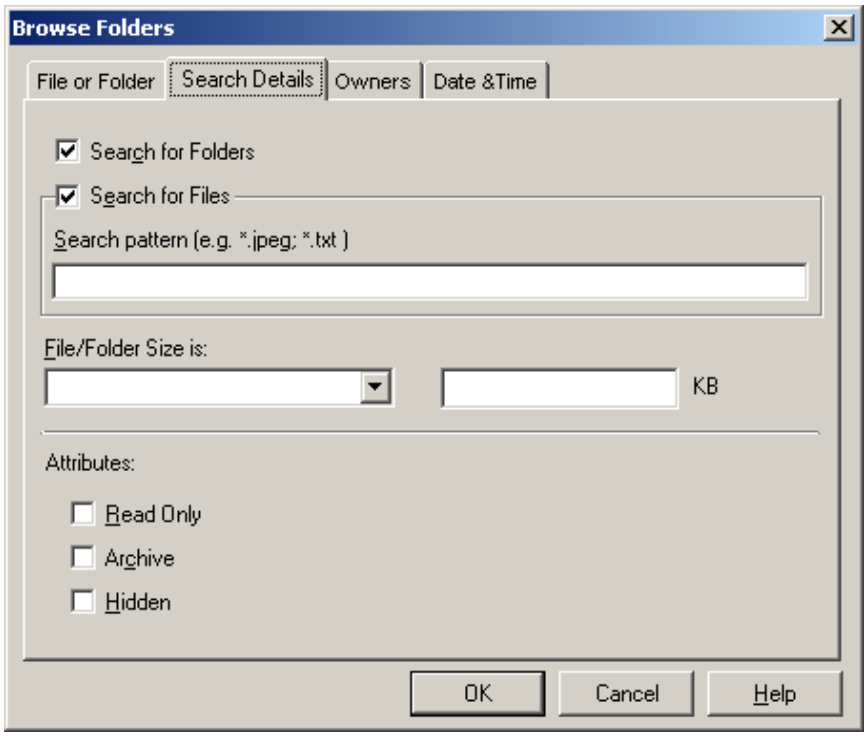
3. Click the *File or Folder* tab.
4. In the File or Folder Name field, enter a file or folder name. To select a specific file or folder, click the *Browse* button. The Choose a folder window displays.

5. Select an object. If you selected an organizational unit, organization, or container, the Apply to section will be enabled. By default the *This folder and all sub folders* radio button is selected. Click the *This folder only* radio button to scan only the files or folder in the selected object. Click *OK* to return to the Browse Folders window.



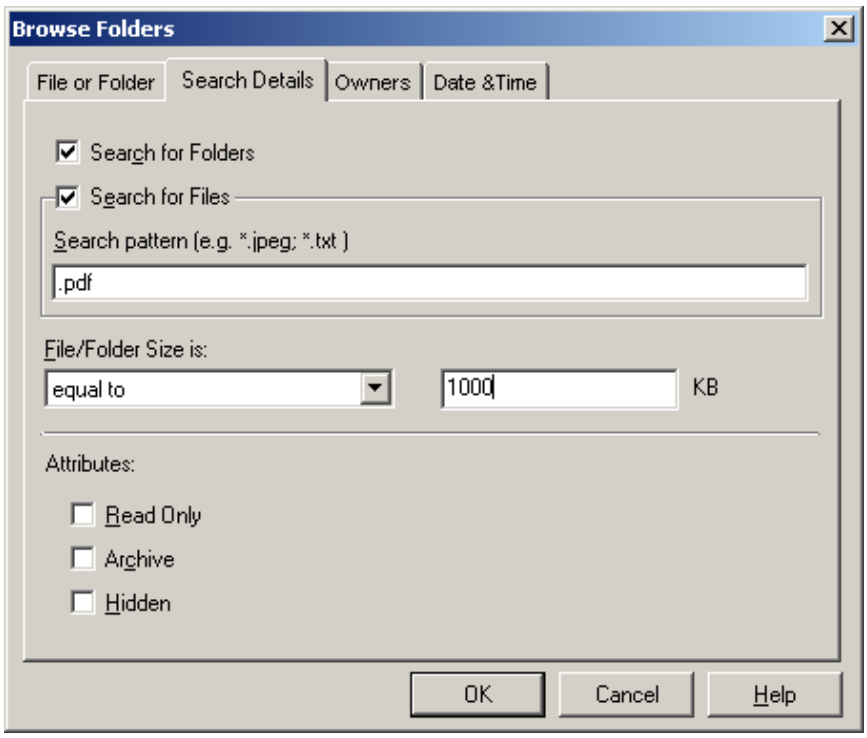
6. Click *OK* to exit the Browse Folders window or click the *Search Details* tab to modify specific details for your file or folder search.

7. By default, *the Search for Folders* and *Search for Files* check boxes are selected.



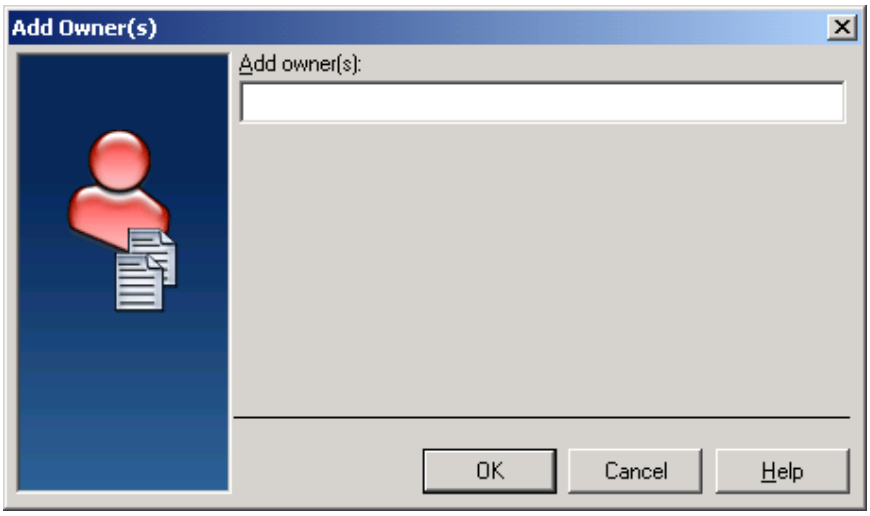
8. To narrow your scan, enter a specific file extension, such as .pdf, .doc, or .jpeg, in the Search pattern field.
9. You can determine a file to scan by specifying a range of sizes. Select one of the following parameters from the File/Folder Size is drop-down menu:
   - **Equal to** — Scans files that are equivalent to the specified size
   - **Greater than** — Scans files that are larger than the specified size
   - **Greater than or equal to** — Scans files that are larger than or equivalent to the specified size
   - **Less than** — Scans files that are smaller than the specified size
   - **Less than or equal to** — Scans files that are smaller than or equivalent to the specified size

10. In the KB field, enter a number in kilobytes for the file size.

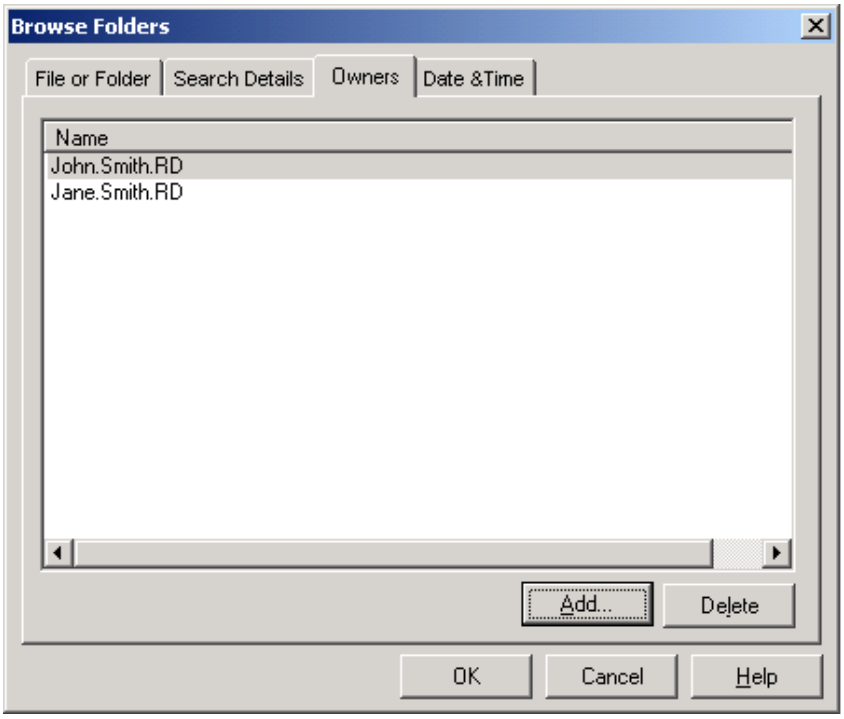


11. In the Attributes section, select any of the following:
    - **Read Only** — Scans read-only files
    - **Archive** — Scans archived files
    - **Hidden** — Scans hidden files
12. Click *OK* to exit the Browse Folders window or click the *Owners* tab to select a specific owner for the file you want to scan.

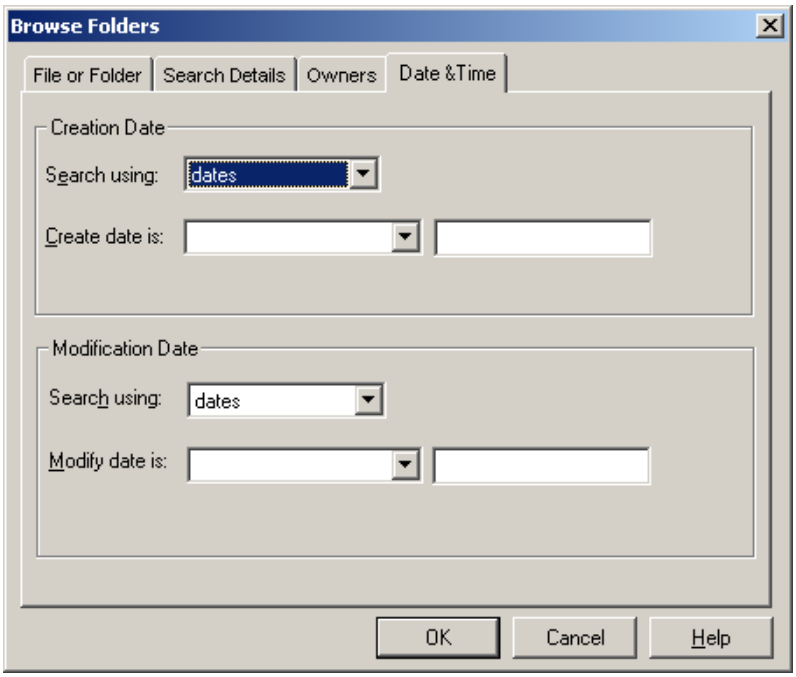
13. If you selected the Owners tab, click the *Add* button to display the following window.



14. In the Add owner(s) field, enter the name of the owner of the file you want to scan. To enter multiple names, enter a semi-colon (;) after each name entered.
15. Click *OK* to return to the Owners tab. The name you entered displays in the Name column.



16. Click *OK* to exit the Browse Folders window or click the *Date & Time* tab to select a creation and modification date for the file you want to scan.
17. In the Creation Date section, click the Search using drop-down arrow and select one of the following options:
    - **Days** — Allows you to scan files that were created in a specified number of days before or after the current day.
    - **Dates** — Allows you to scan files that were created on a specified date.



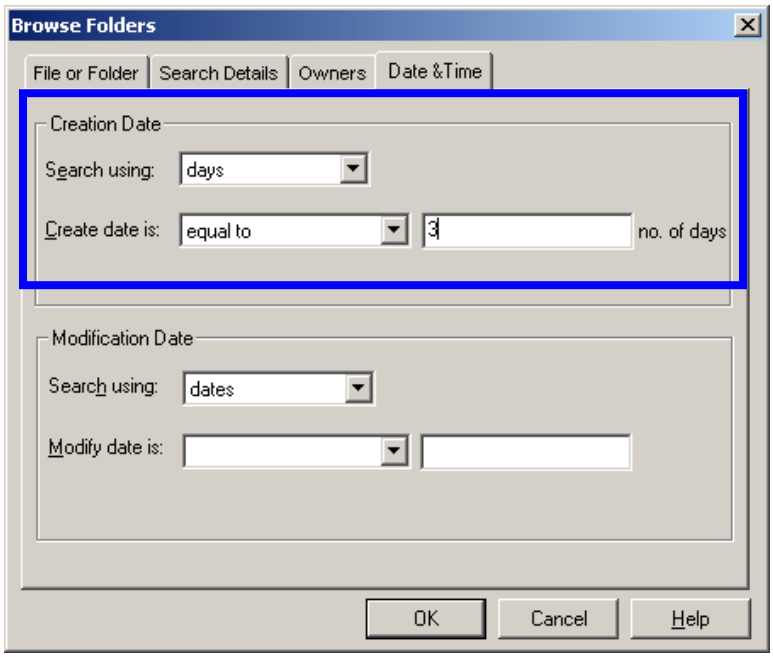
18. From the Creation date is drop-down menu, select one of the following:
    - **Equal to** — Allows you to scan files that were created on the specified day or date
    - **Greater than** — Allows you to scan files that were created after the specified day or date
    - **Greater than or equal to** — Allows you to scan files that were created on or after the specified day or date
    - **Less than** — Allows you to scan files that were created before the specified day or date
    - **Less than or equal to** — Allows you to scan files that were created on or before the specified day or date

19. If you selected days, enter the amount of days in the no. of days field. If you selected dates, enter a date in the text field.

    Example

    To scan a file that was created three days ago, perform the following steps from the Date & Time tab:

    1. In the Creation Date section, select *days* from the Search using drop-down menu.
    2. From the Creation date is drop-down menu, select *equal to*.
    3. In the no. of days field, enter *3*.



20. In the Modification Date section, click the Search using drop-down arrow and select one of the following options:

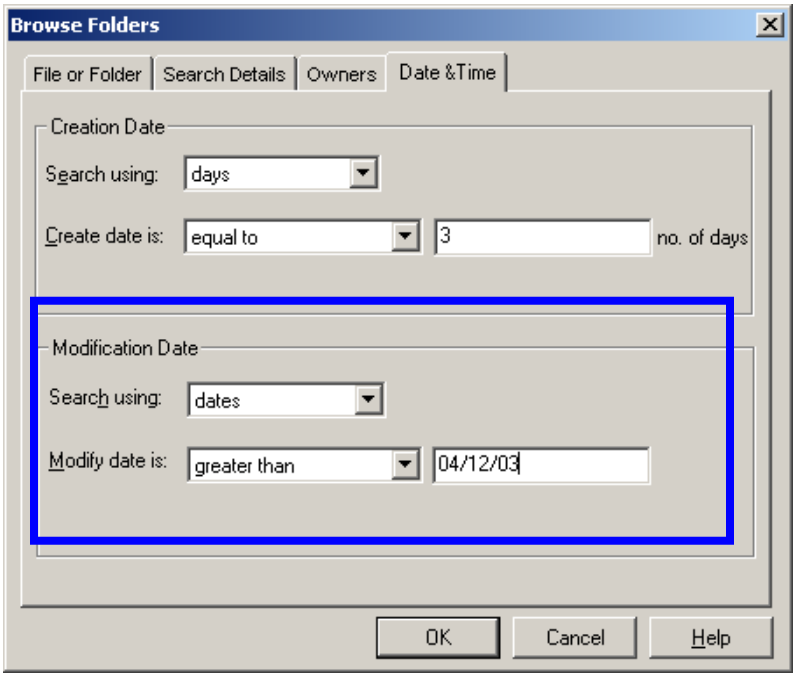
    - **Days** — Allows you to scan files that were modified in a specified number of days before or after the current day.
    - **Dates** — Allows you to scan files that were modified on a specified date.

21. From the Modify date is drop-down menu, select one of the following:
    - **Equal to** — Allows you to scan files that were modified on the specified day or date
    - **Greater than** — Allows you to scan files that were modified after the specified day or date
    - **Greater than or equal to** — Allows you to scan files that were modified on or after the specified day or date
    - **Less than** — Allows you to scan files that were modified before the specified day or date
    - **Less than or equal to** — Allows you to scan files that were modified on or before the specified day or date
22. If you selected days, enter the amount of days in the no. of days field. If you selected dates, enter a date in the text field.

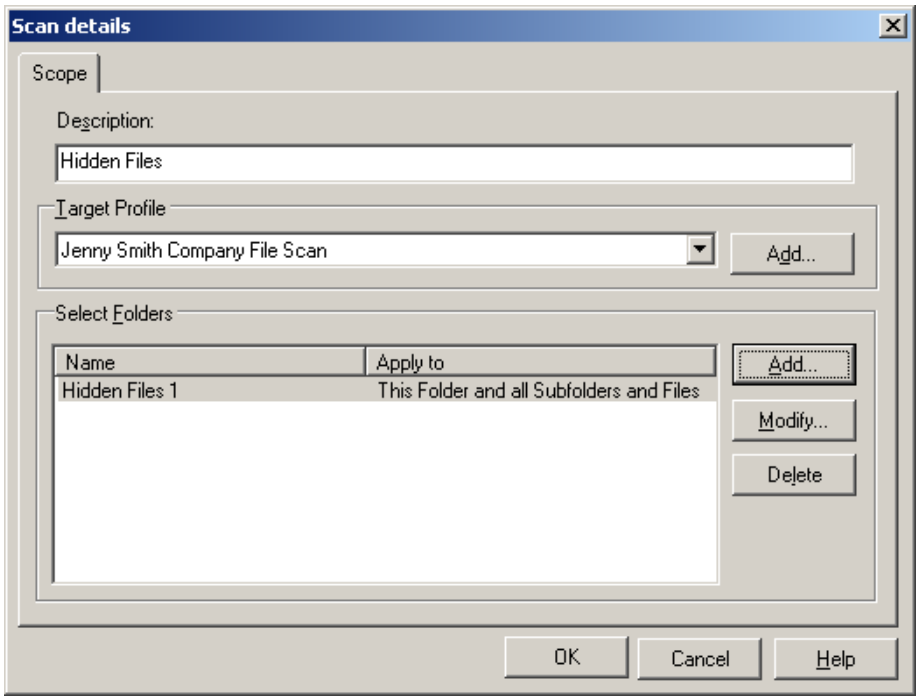
    Example

    To scan files that were modified after 04/12/03, perform the following steps:

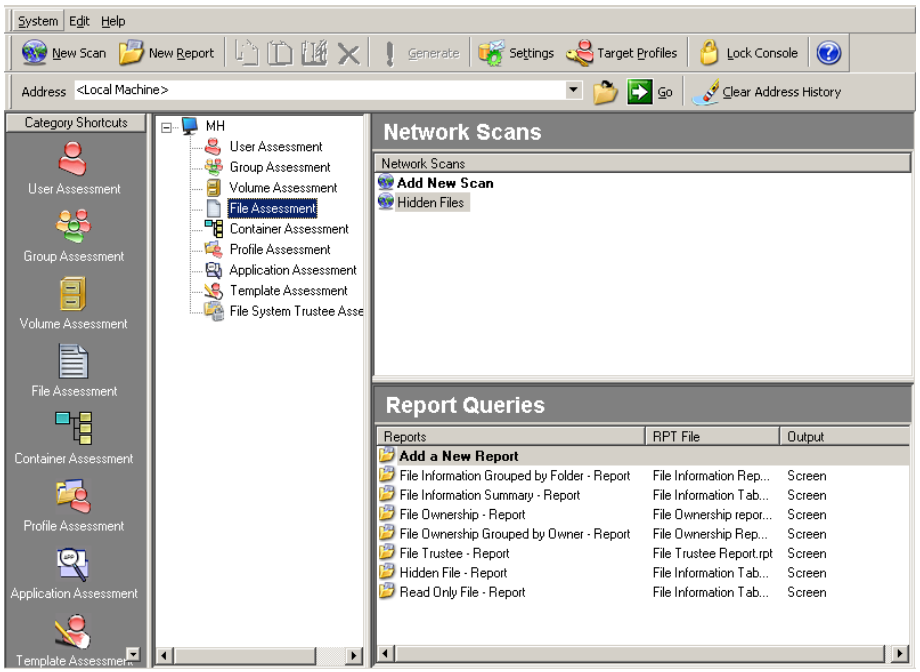
    1. In the Modification Date section, select *dates* from the Search using drop-down menu.
    2. From the Modify date is drop-down arrow, select *greater than*.
    3. In the text field, enter *04/12/03*.



23. Click *OK* to exit the Browse Folders window. The folder you selected displays in the Name column of the Scan Details window.



24. Click *OK* to save your changes and exit the Scan Details window. Your new scan displays in the Network Scans column of the LT Assessment for SUSE window.



Gathering File System Trustee Assignments

In order to scan for trustee assignments, we will first have to run utility on the SUSE-OES/NetWare server. For SUSE, a module called METAMIG must be run and on NetWare, the module TRUSTEE.NLM must run. These modules have to be run on all servers, in your network, that are to be scanned. The METAMIG/TRUSTEE.NLM module scans all folders and files, on all volumes, and gathers trustee assignments, which are stored to a XML or text file.

Both METAMIG and TRUSTEE.NLM are distributed by Novell and can be downloaded from **http://support.novell.com/filefinder/**

SUSE-OES Servers

Running METAMIG

LT Assessment for SUSE supports the following switches in METAMIG.

- t — Trustee information

The module is located in the following folder:

/opt/novell/nss/sbin

The typical syntax for usage is:

metamig save <Volume Name> -m t >/media/nss/<Volume name>/trustee.xml;

This command will save a file called trustee.xml at the root of the volume. If you desire a different path, redirect the command to a different folder on the volume.

Example

metamig save VOL1 -m t >/media/nss/VOL1/trustee.xml;

We recommend running the following command after the metamig command to ensure that the XML file created has no errors.

sed –i ‘s/&/&/g’ /media/nss/VOL1/trustee.xml”

Both commands can be executed together as shown below:

metamig save VOL1 -m t >/media/nss/VOL1/trustee.xml;sed –i ‘s/&/&/g’ /media/nss/VOL1/trustee.xml

NetWare Servers

Running TRUSTEE.NLM

LT Assessment for SUSE supports the following switches in TRUSTEE.NLM.

- /ET — Trustee information
- /EI — Inherited rights mask (IRM) information

The default settings in the TRUSTEE.NCF file are:

LOAD SYS:SYSTEM\TRUSTEE /ET /EI /D SAVE ALL SYS:TRUSTEE.TXT

/D indicates that only directories will be scanned. If the requirement is to scan all files, remove this parameter.

The path defined in the default settings is SYS:TRUSTEE.TXT. This means that the TRUSTEE.TXT file will be created at the root of the SYS volume. If you desire a different path, modify the default settings.

Example

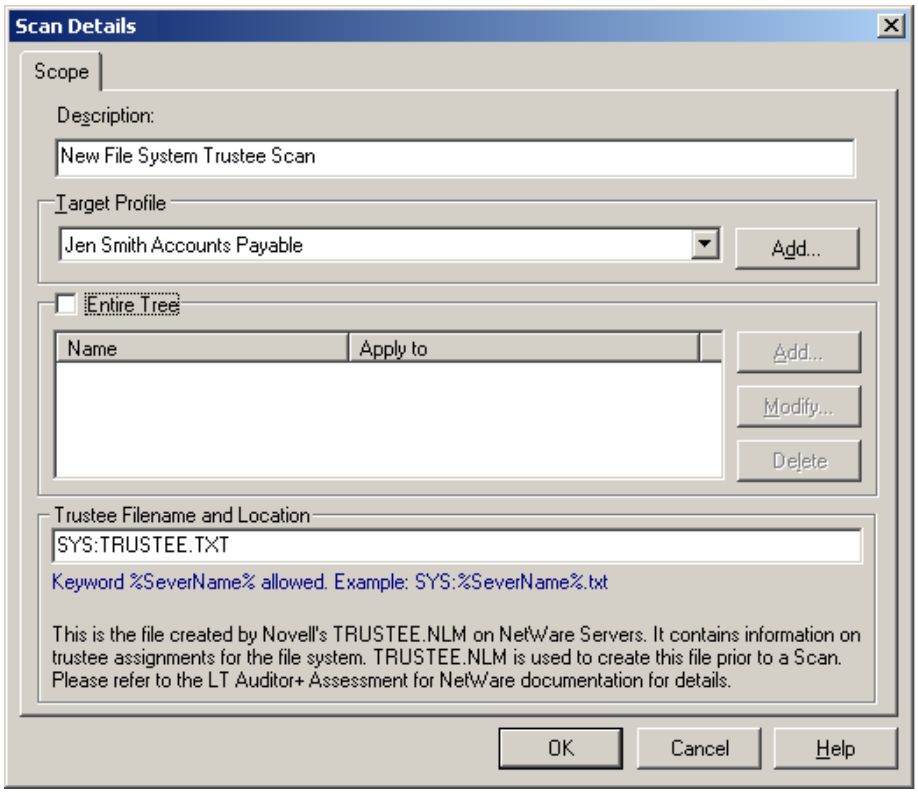
LOAD SYS:SYSTEM\TRUSTEE /ET /EI /D SAVE ALL VOL1:LTAUDIT\TRUSTEE.TXT

It is important that this path name is uniform for all NetWare servers in the environment. LT Assessment for SUSE will search for this specific file as setup in the Scan Details window of the File System Trustee Assessment network scan.

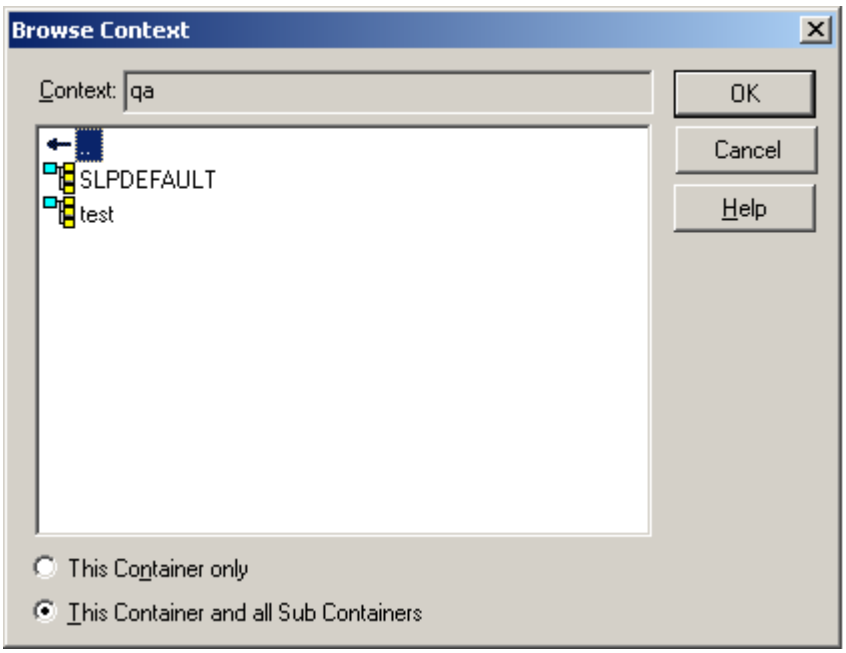
Selecting a Specific Container from the File System Trustee Assignments Scan Details Window

If you selected the File System Trustee Assignments, by default the *Entire Tree* check box is selected. To scan a specific container of the tree, perform the following steps:

1. Deselect the *Entire Tree* check box.

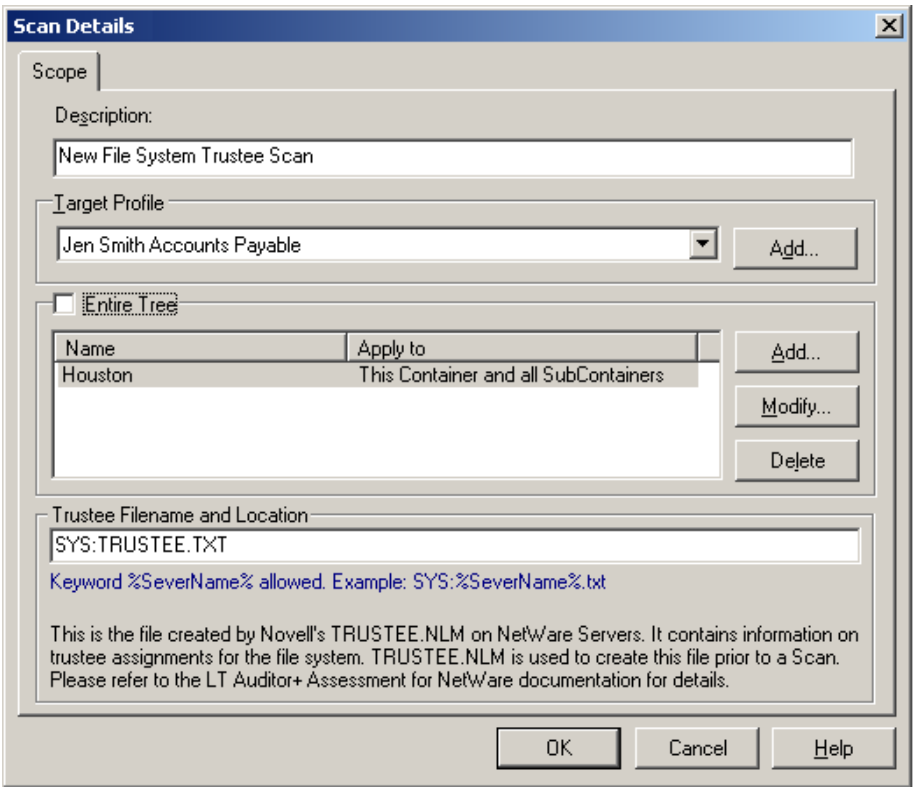


2. Click the *Add* button. The Browse Context window displays.



3. Select a container. Your selection displays in the Context field.
4. By default the *This Container and all Sub Containers* radio button is selected. To scan only the selected container, click *This Container only*. Click *OK* to exit the Browse Context window.

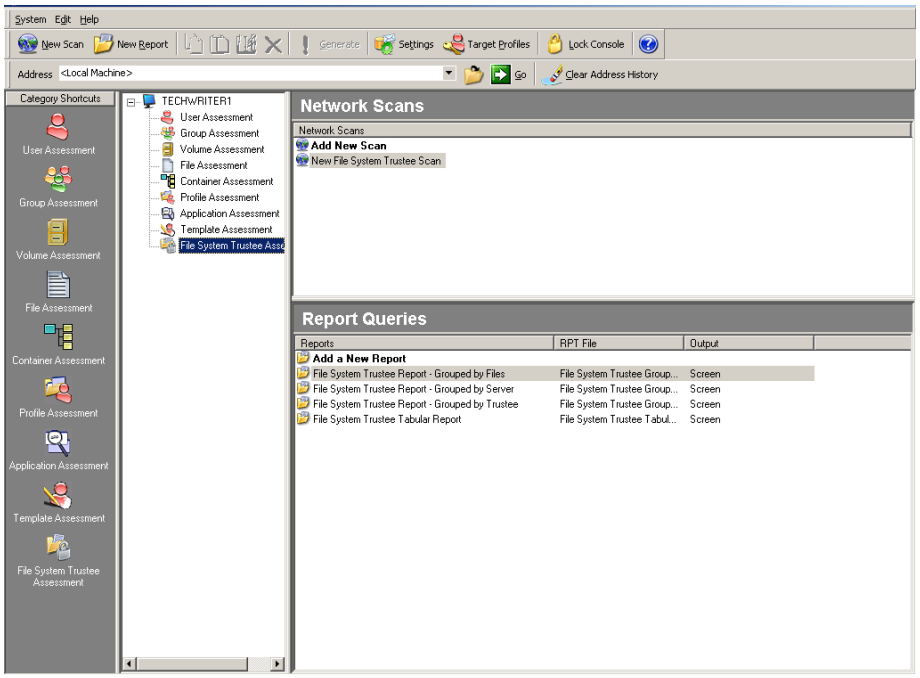
5. The selected container now displays in the Name column of the Scan Details window.



6. In the Trustee Filename and Location field, enter the directory on the server (s) to which the text file created by METAMIG/TRUSTEE.NLM is located.

> **!** **Important**
> METAMIG/TRUSTEE.NLM enables you to scan your network for trustee assignments. METAMIG/TRUSTEE.NLM must run on all SUSE/NetWare servers from which you want to scan file system trustee assessment data. METAMIG/TRUSTEE.NLM creates a file on the server, which is used by LT Assessment for SUSE during a Scan. An assumption is made that the file created by METAMIG/TRUSTEE.NLM contains the latest information on current Trustee assignments. TRUSTEE.XML/TRUSTEE.TXT will be created after METAMIG/TRUSTEE.NLM is run.

7. Click *OK* to save your changes and exit the Scan Details window. Your new scan displays in the Network Scans column of the LT Assessment for SUSE window.



Report Queries

From the Assessment Category window, select one of the nine assessment categories to display the Report Queries pane.

Report queries contain the statements needed to query the databases for specific information. The LT Assessment for SUSE software ships with a variety of report queries that can be customized to fit specific criteria for each assessment category.

In addition to modifying existing report queries, you can also create new queries for the assessment categories. By default, LT Assessment for SUSE provides several queries for each assessment category:

- User Assessment Report Queries
  - All trustee — Inheritance mask
  - Disabled user accounts
  - Inheritance mask
  - Object entry rights
  - Property rights
  - User
  - User environment
  - User group membership
  - User identification
  - Users with concurrent connections set to more than five
  - Users not logged in for last thirty days
  - Users security equivalent to administrator
  - Users that are not allowed to change their password
  - Users that do not require a password
  - Users with grace logins set to more than five
  - Users with minimum password length less than five characters
  - Users with minimum password length not defined
  - Users with more than five incorrect login attempts

- Group Assessment Report Queries
  - All trustee — Inheritance mask
  - Group creation modification
  - Group identification
  - Group member
  - Group report
  - Group summary
  - Inheritance mask
  - Object entry rights
  - Property rights
- Volume Assessment Report Queries
  - Purgeable space more than 1 Gb
  - Purgeable space more than 500 Mb
  - User rights
  - User space restriction
  - Volume disk space summary
  - Volume disk space utilization summary
- File Assessment Report Queries
  - File information grouped by folder
  - File information summary
  - File ownership
  - File ownership grouped by owner
  - File trustee
  - Hidden file
  - Read only file

- Container Assessment Report Queries
  - All trustee — Inheritance mask
  - Container object summary
  - Container object summary report
  - Containers intrusion detection not set
  - Inheritance mask
  - Intruder detection settings
  - Object entry rights
  - Property rights
- Profile Assessment Report Groups
  - Object entry rights
  - Profile Identification
  - Profile report
- Application Assessment Report Groups
  - Application creation modification
  - Application report
  - Applications marked for install only
  - Applications marked to run once after install
  - Object entry rights
- Template Assessment Report Groups
  - All trustee — Inheritance mask
  - Inheritance mask
  - Object entry rights
  - Property rights
  - Template group membership
  - Template users security equivalent to administrator
  - Template users that are not allowed to change their password
  - Template users that do not require a password
  - Template users with concurrent connections set to more than five
  - Template users with grace logins set to more than five
  - Template users with minimum password length less than five characters
  - Template users with minimum password length not defined

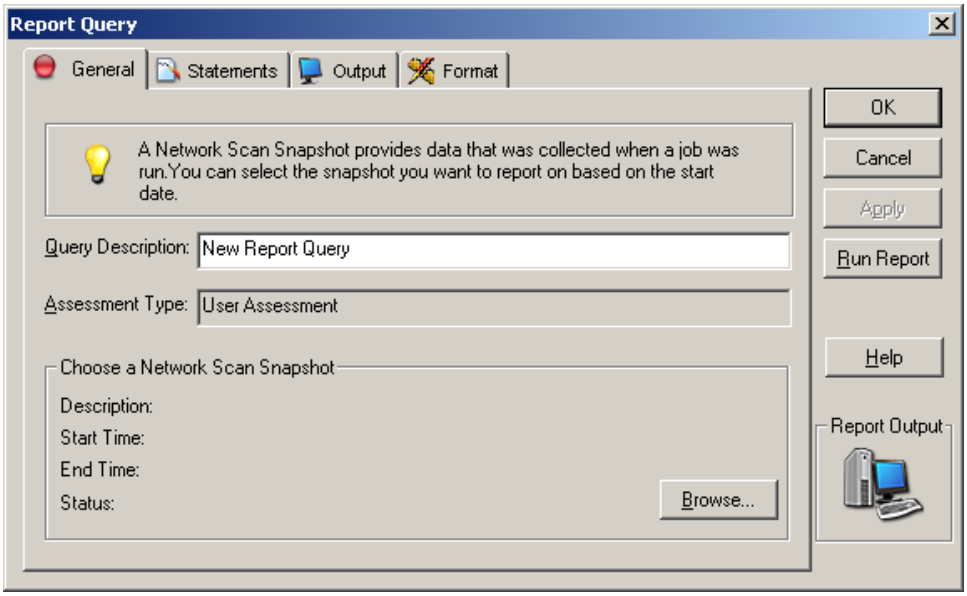
- File System Trustee Assessment Report Groups
  - File system trustee report — Grouped by files
  - File system trustee report — Grouped by server
  - File system trustee report — Grouped by trustee
  - File system trustee tabular report

Creating a New Report Query

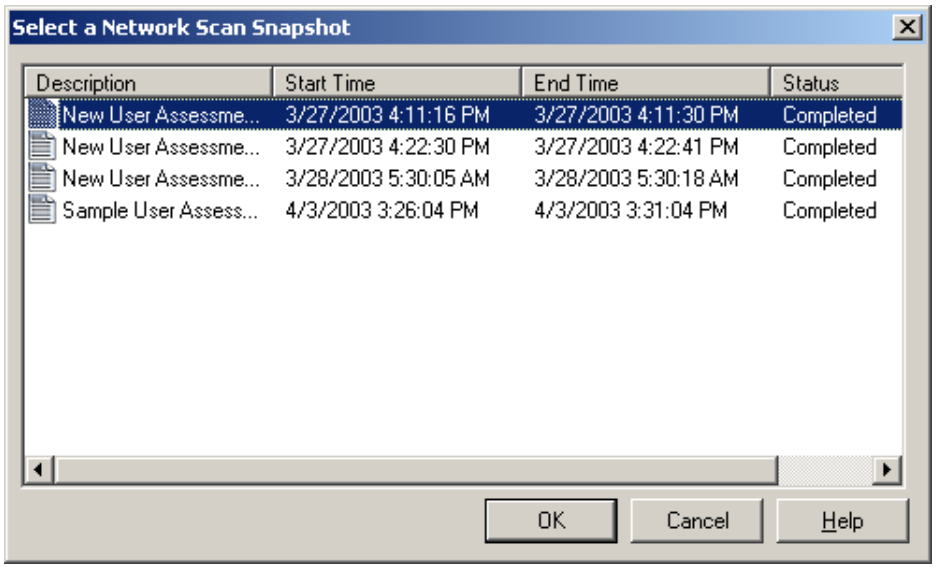
A report query allows you to query the data that was collected with a scan.

To create a new report query, perform the following steps:

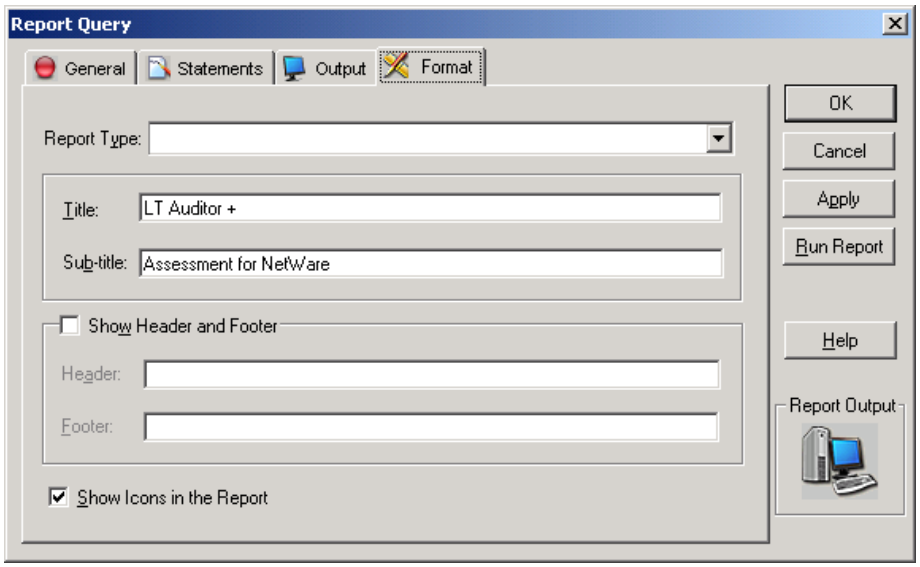
1. Select the assessment category to which you would like to add a new report query.
2. To display the Report Query window, use any of the following methods:
   - From the System menu on the Menu bar, select *New Report*.
   - From the Standard toolbar, click the *New Report* button.
   - From the Assessment Category window, right-click to display the drop-down menu. From this menu, select *New Report*.
   - From the Report Queries pane in the LT Assessment for SUSE window, right-click to display the drop-down menu. From this menu, select *New Report*.
   - From the Report Queries pane in the LT Assessment for SUSE window, double-click *Add a New Report*.
3. From the Report Query window, click the *General* tab and enter a description for this query in the Query Description field.



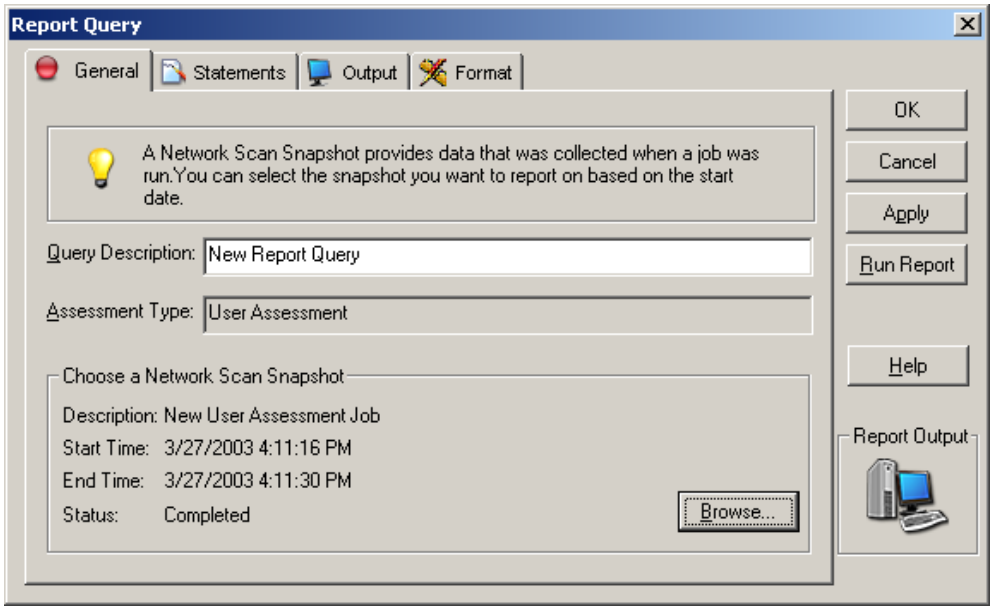
4. Click the *Browse* button to select a previously existing scan.
5. The Select a Network Scan Snapshot window lists previously existing snapshots. Select a snapshot and click *OK*.



6. Click the *Format* tab. Click the drop-down arrow in the Report Type field and select a report type.



7. Click *Apply* → *OK* to save the query to the selected assessment category or click *Run Report* to execute a report immediately.



Deleting a Report Query

Perform the following steps to delete a report query:

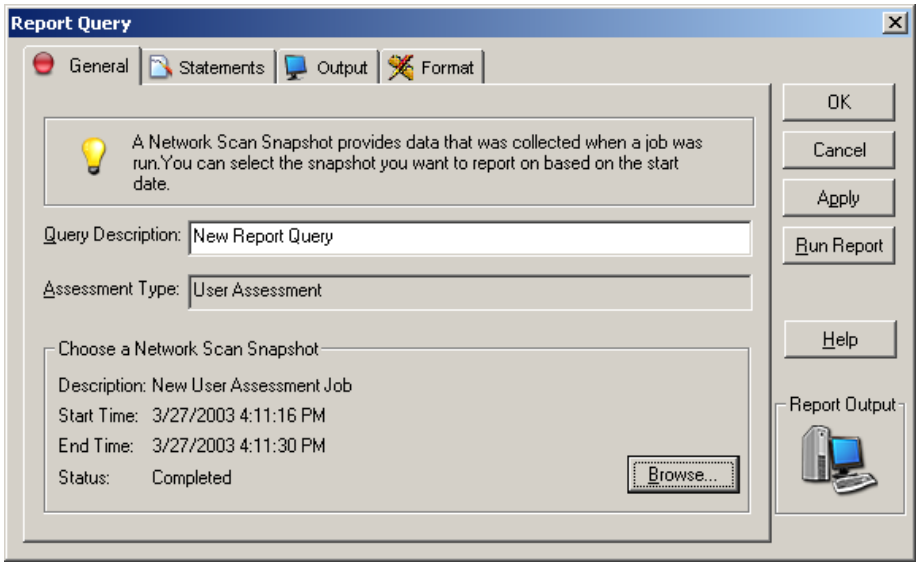
1. From the LT Assessment for SUSE window, highlight the desired report query's assessment category. All report queries in this assessment category are displayed in the bottom right-hand pane.
2. From the Report Query pane, highlight the report query to be deleted.
3. To delete the report query, use any of the following methods:
   - From the Edit menu on the Menu bar, click *Delete*.
   - From the Standard toolbar, click the *Delete* button.
   - From the Assessment Category window, right-click to display a drop-down menu. From this menu, select *Delete*.
4. Click *Yes* to confirm the deletion of the report query.

Modifying an Existing Report Query

To modify an existing report query, perform the following steps:

1. From the Assessment Category window, select one of the following assessment categories:
   - User Assessment
   - Group Assessment
   - Volume Assessment
   - File Assessment
   - Container Assessment
   - Profile Assessment
   - Application Assessment
   - Template Assessment
   - File System Trustee Assessment
2. From the Report Queries pane, highlight the desired report query.
3. To display the Report Query window, use any of the following methods:
   - From the Edit menu on the Menu bar, click *Modify*.
   - From the Standard toolbar, click the *Modify* button.
   - From Report Queries pane, right-click to display a drop-down menu. From this menu, select *Modify*.
   - From the Report Queries pane, double-click the selected query.
4. Selecting one of the following tabs provides additional options for modifying the report query:
   - General
   - Statements
   - Output
   - Format

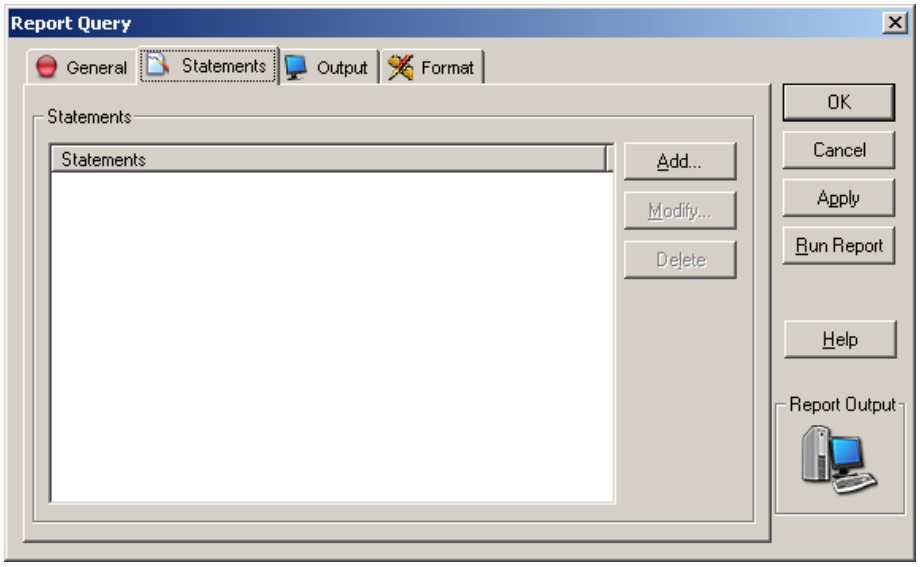
General



From the General tab, you can enter a query description and select a network scan snapshot. The General tab contains the following fields:

- **Query Description** — Enter a name or description to identify individual queries.
- **Assessment Type** — The assessment category for which the query is designed displays in this field.
- **Choose a Network Scan Snapshot** — Select a previously created snapshot of your network configuration.

Statements

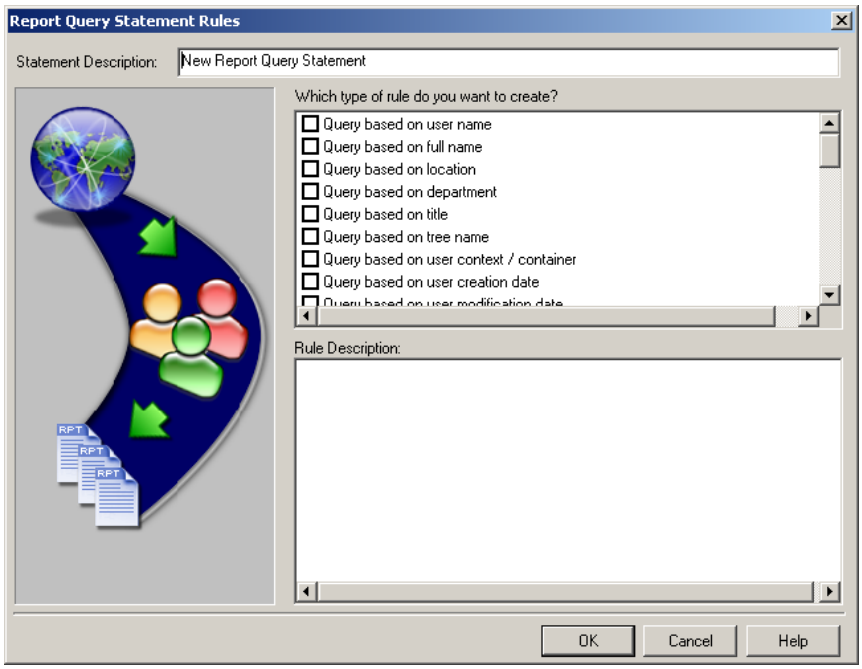


Rules are specific attributes that can be customized to query only the information that is important to your organization. A statement consists of multiple rules and allows the creation of complex queries for granular reporting.

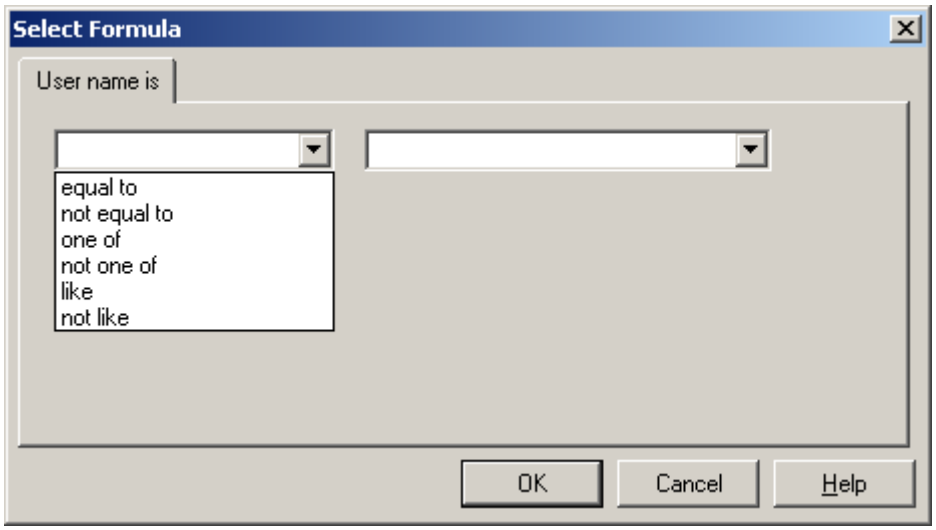
Adding a Report Query Statement and Creating a Customized Rule

To add a report query statement, perform the following steps from the Report Query window:

1. Click the *Statements* tab.
2. Click the *Add* button to display the Report Query Statements Rules window.



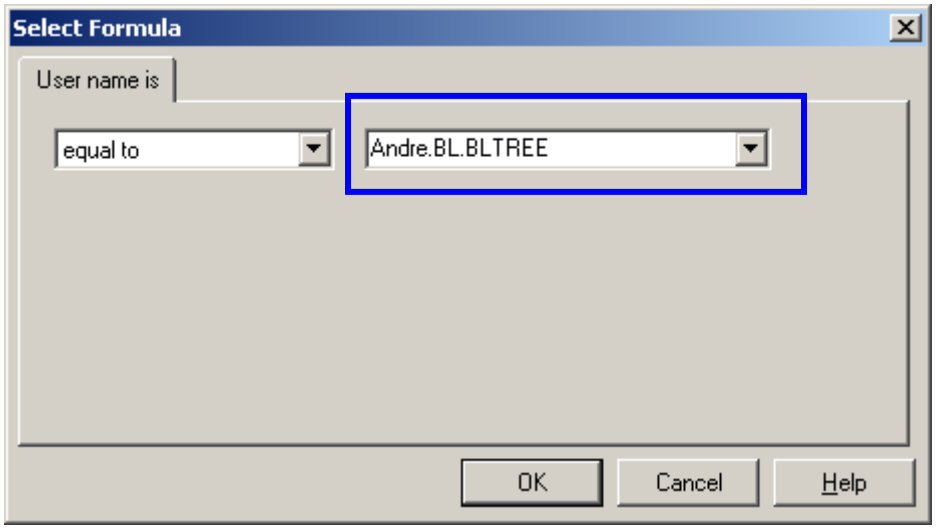
3. In the Statement Description field, enter a name or description to identify the individual statement.
4. Select one rule or multiple rules from the section named Which type of rule do you want to create?
5. Based on your selection, a description of the rule will display in the Rule Description section of the Report Query Statements Rule window. If the rule you selected is customizable, <*Define*> will display at the end of the description statement. Click the rule to display the Select Formula window.
6. The rule you selected displays on the tab of the Select Formula window. To list the parameters for this rule, click the drop-down arrow to the field on the left. The parameters display in the drop-down window. Select a parameter from the list that displays in the drop-down window.



Note

For a complete list of parameters, their definitions, and examples on how they can be used, refer to the table in Appendix A of this user guide.

7. After you have selected a parameter, enter an attribute for your parameter in the text field or click the drop-down arrow of the text field to select from multiple attributes.

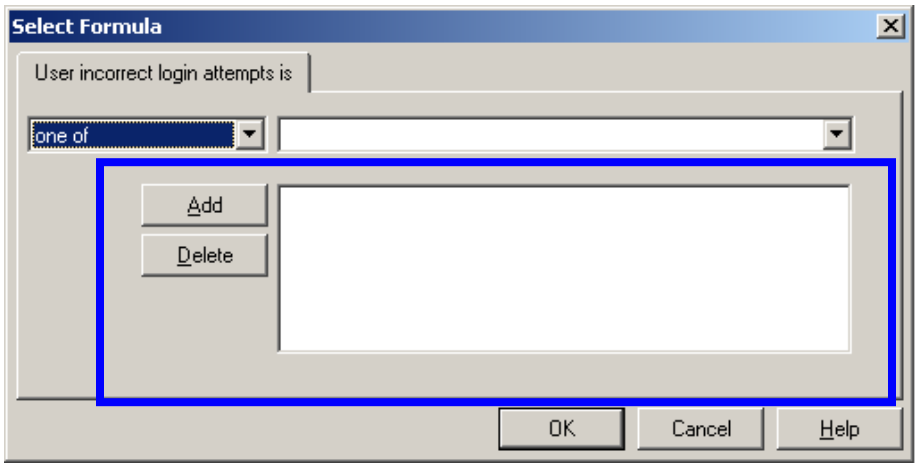


If you select *one of* or *not one of*, enter an attribute in the text field and click the *Add* button to add your attribute to the list box. At any time you can remove an attribute from the list box by selecting the attribute and clicking the *Delete* button.

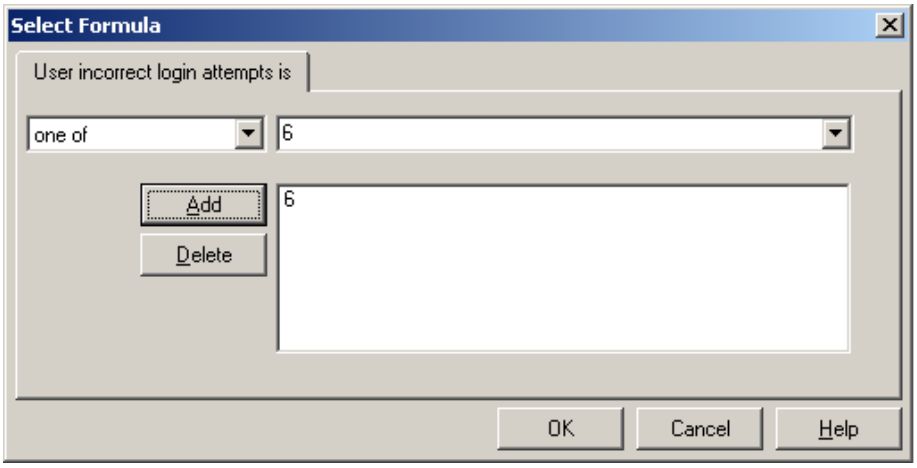
If you select *between* or *not between*, you must enter an attribute in each text field (a starting number or date and an ending number or date).

Example 1 — Rule: Query based on user incorrect login attempts

If you click the rule description *User incorrect login attempts is* and select the *one of* option, a list box displays in the window.

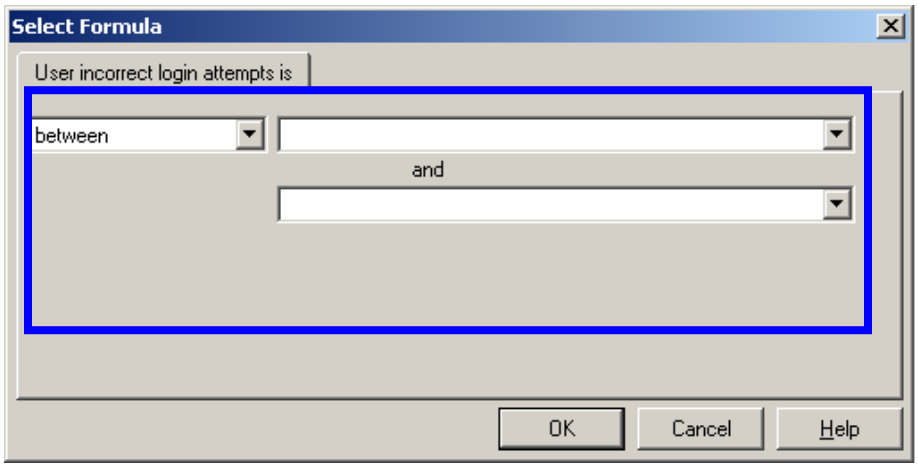


If you enter the number *6* in the text field, click *Add* to add the number to the list box. All computers with six incorrect login attempts will be queried.



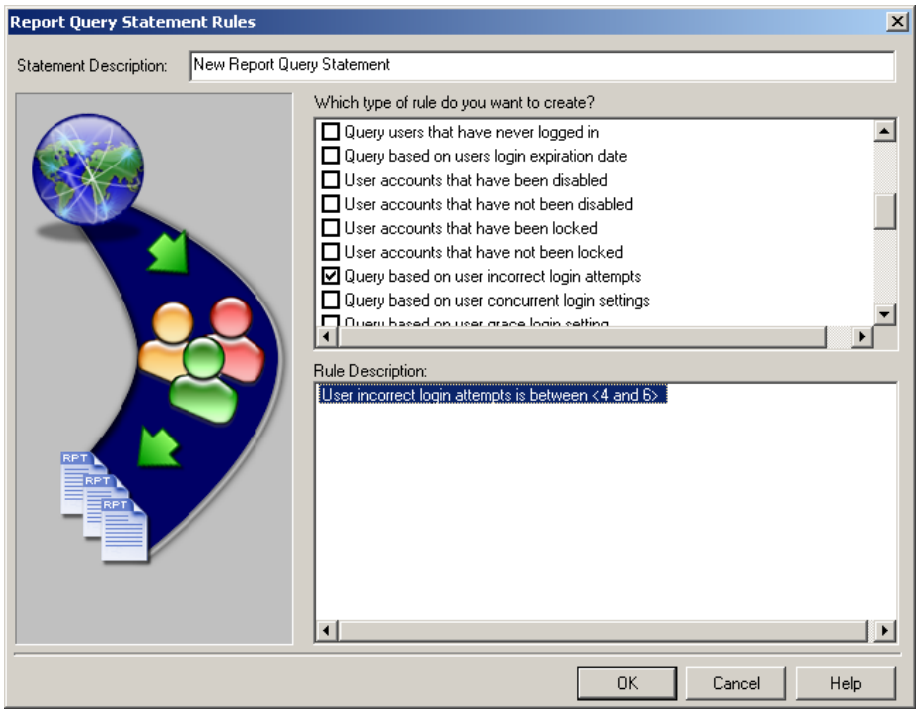
Example 2 — Rule: Query based on user incorrect login attempts

If you click the rule description *User incorrect login attempts is* and select the *between* option, the window displays the following text fields.



Enter *4* and *6* to query all computers with four, five, or six incorrect login attempts.

8. Click *OK* to exit the Select Formula window. The rule you selected and attributes you entered display in the Rule Description section.

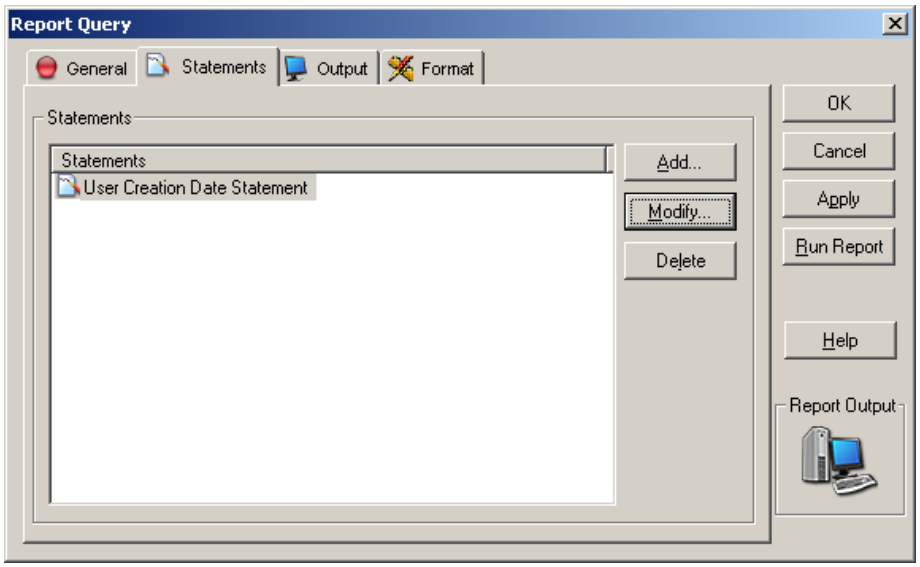


!

Important

If you initially selected multiple rules, if applicable, click the rule description statement and customize the rule based on your specific criteria. Parameters must be selected and attributes must be added to all selected customizable rule statements before exiting the Report Query Statement Rules window.

9. Click *OK* to exit the Report Query Statement Rules window. The newly created report query statement displays in the Statements column.



!

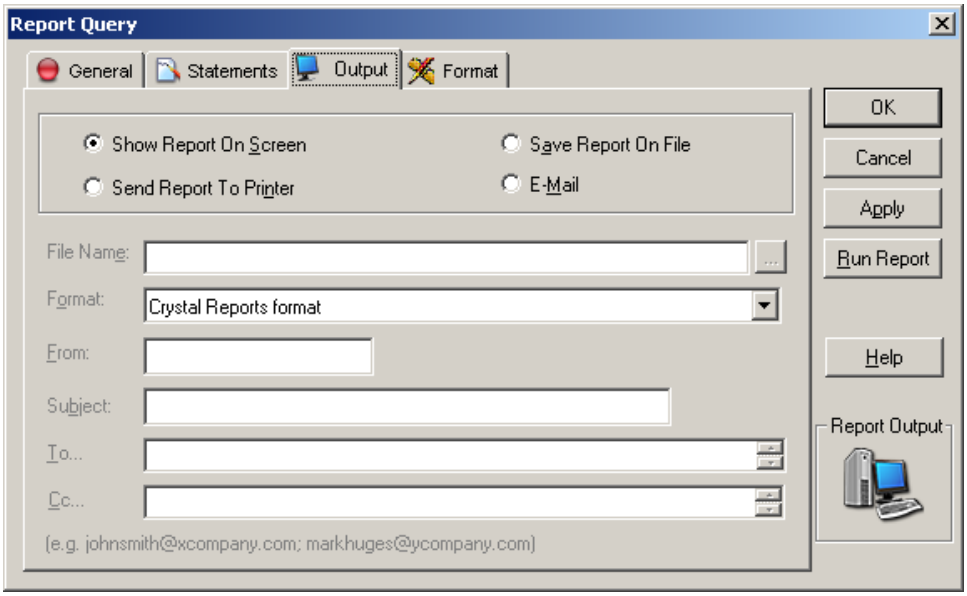
Important

If only one statement is added to your report query, a report will be generated with data that matches the criteria for **all** rules in that statement.

If multiple statements are added to the report query, a report will be generated with data that matches the criteria for **any** of the rules in either statement.

10. Click the *Output* tab to select more criteria for your query.

Output



You can click the *Output* tab to select more criteria for your query. Use the Output tab to specify how and where your report is displayed.

1. Select a report output by clicking the desired radio button:
   - **Show Report On Screen** — Displays the report on the screen.

     Important
     If you want to use this report query to run a job in the future, do not select the Show Report On Screen option. This option is not a valid option in the Job Details window.

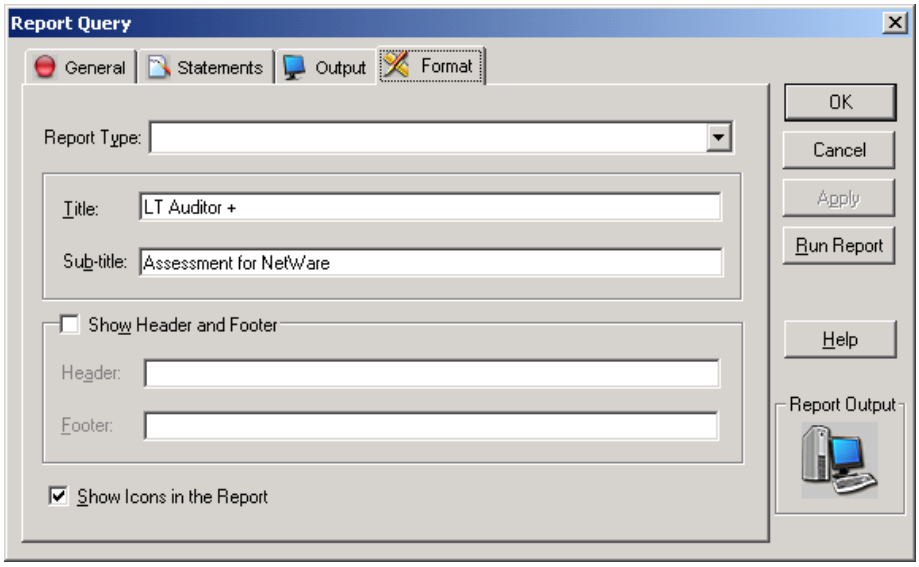
   - **Send Report To Printer** — Generates the report directly to the default printer.
   - **Save Report On File** — Exports the report to a file or to another disk media.
   - **E-Mail** — Sends an exported report to an SMTP e-mail address.

     Note
     Ensure that SMTP parameters are set properly for delivery of e-mail.

2. Enter a file name to specify a destination for the report file. This is required when saving reports to a file or when e-mailing reports.

3. If you selected the Save Report on File or the Email radio button, click the drop-down arrow to select a format for the report. The list contains the following possible export formats.
   - Crystal Reports
   - Data Interchange Format (.dif)
   - Web page (.html)
   - Portable Document Format (.pdf)
   - Report Definition format
   - Record format
   - Rich text Format (.rtf)
   - Comma separated descriptions format
   - Text format (.txt)
   - Lotus 1-2-3 format
   - Microsoft Word for Windows
   - Extensible Markup Language format (.xml)
   - Microsoft Excel for Windows
4. If you selected the E-mail radio button, in the From field enter the e-mail address of the sender.
5. If you selected the E-mail radio button in the Subject field, enter a subject for the e-mail.
6. If you selected the E-mail radio button, designate an e-mail address where the report will be sent by entering the address into the To and the optional CC field. Ensure that the correct e-mail address has been entered, because LT Assessment for SUSE does not validate this information.
7. Click the *Format* tab to select more criteria for your query.

Format



The Format tab allows you to select:

- A report type for your report query.
- A title, subtitle, header description, or footer description for your final report.

To add specific details to your query, perform the following steps on the Format tab:

1. Click the drop-down arrow in the Report Type field to select a report type. This list displays the following report types:
   - User Assessment
     - User Access Control Rights Report
     - User Account Restriction Tabular Report
     - User Creation Modification Report
     - User Creation Modification Tabular Report
     - User Environment Tabular Report
     - User Group Membership Report
     - User Identification Report
     - User Identification Tabular Report
     - User Inheritance Mask Report
     - User Inheritance Mask Tabular Report
     - User Invalid Login Information Report

- User Invalid Login Tabular Report
- User Login Information Report
- User Login Information Tabular Report
- User Login Settings Report
- User Login Settings Tabular Report
- User Network Restriction Report
- User Object Rights Report
- User Object Rights Tabular Report
- User Password Settings Report
- User Password Settings Tabular Report
- User Property Rights Report
- User Security Equivalence Report

▪ Group Assessment

- Group Creation Modification Report
- Group Creation Modification Tabular Report
- Group Description Report
- Group Identification Report
- Group Inheritance Mask Report
- Group Inheritance Mask Tabular Report
- Group Member Report
- Group Object Rights Report
- Group Object Rights Tabular Report
- Group Property Rights Report
- Group Summary Report
- Group Summary Tabular Report
- Group Trustee Report

- Volume Assessment
  - Volume Creation Modification Report
  - Volume Creation Modification Tabular Report
  - Volume Details Tabular Report
  - Volume Summary Report
  - Volume User Restriction Report
  - Volume User Rights Report
- File Assessment
  - File Information Report Grouped by Folder
  - File Information Report
  - File Information Tabular Report
  - File Ownership Report Grouped by Owner
  - File Ownership Report
  - File Ownership Summary Tabular Report
  - File Trustee Report (All Files)
  - File Trustee Report
- Container Assessment
  - Container Group Report
  - Container Inheritance Mask Report
  - Container Inheritance Mask Tabular Report
  - Container Intruder Detection Settings Report
  - Container Intruder Detection Settings Tabular Report
  - Container Invalid Login Information Report
  - Container Login Settings Report
  - Container Login Settings Tabular Report
  - Container Network Restriction Report
  - Container Object Rights Report
  - Container Object Rights Tabular Report
  - Container Object Summary Report

  - Container Object Summary Tabular Report
  - Container Password Setting Report
  - Container Password Setting Tabular Report
  - Container Property Rights Report
  - Container Trustee Report
- Profile Assessment
  - Profile Creation Modification Report
  - Profile Description Report
  - Profile Identification Report
  - Profile Object Rights Tabular Report
- Application Assessment
  - Application Creation Modification Report
  - Application Object Rights Tabular Report
  - Application Settings Tabular Report
- Template Assessment
  - Template Access Control Rights Report
  - Template Creation Modification Tabular Report
  - Template Description Report
  - Template Equivalent to Me Report
  - Template Group Membership Report
  - Template Identification Report
  - Template Inheritance Mask Tabular Report
  - Template Login Settings Tabular Report
  - Template Network Restriction Report
  - Template New Object DS Rights Report
  - Template New Object Self Rights Report
  - Template New Object Trustee Report

- Template Object Rights Tabular Report
- Template Password Settings Tabular Report
- Template Property Rights Report
- Template Security Equivalence Report

▪ File System Trustee Assessment

- File System Trustee Group by File Folder Report
- File System Trustee Group by Server Report
- File System Trustee Group by Trustee Report
- File System Trustee Tabular Report

2. In the Title field, enter a title to display in the report.
3. In the Sub-title field, enter a subtitle to display in the report.
4. To enable the Header and Footer fields, check the *Show Header and Footer* check box. In the Header field, enter a header to display in the report. In the Footer field, enter a footer to display in the report.
5. Select the *Show Icons in the Report* check box to display the user, group, volume, file, container, profile, application, and template icons in your final report.

Note
If you select the Save Report on File or E-mail options on the Output tab, by default the icons will not display in the final report.

6. Click *Apply* → *OK* to save your query or click *Run Report* to generate a report.

Modifying Your Database and E-Mail Settings

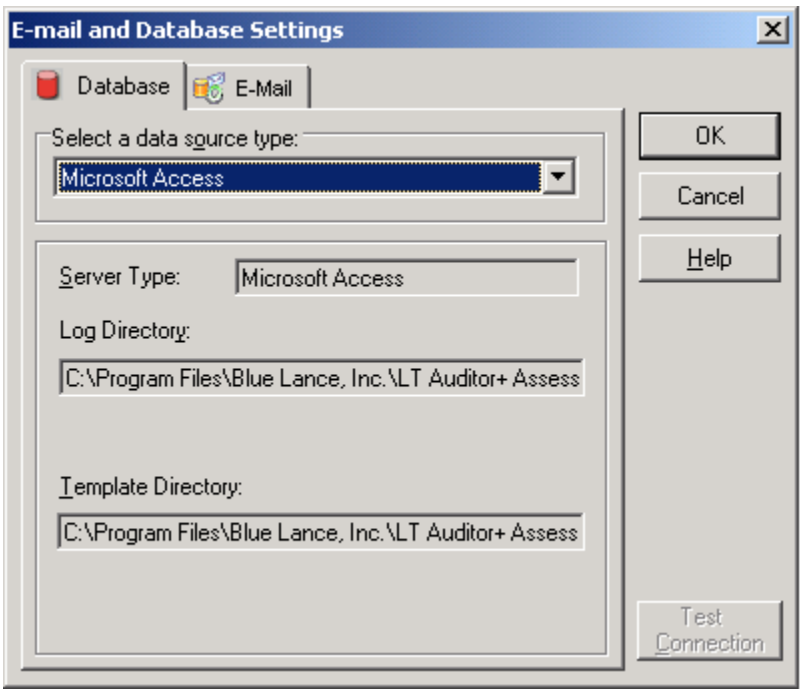
By default when LT Assessment for SUSE is installed, it is automatically set up to record assessment data to a Microsoft Access database.
LT Assessment for SUSE also supports recording assessment data to a Microsoft SQL database. However, you must configure the E-Mail and Database Settings window to connect to the appropriate data source file.

Access the E-mail and Database Settings window by using any of the following methods:

- From the *System* menu on the Menu bar, select *Settings*.
- From the Standard toolbar, click the *Settings* button.
- From the Assessment Category window, right-click to display a drop-down menu. From this menu, select *Settings*.
- From the Calendar section of the LT Assessment for SUSE window, right-click to display a drop-down menu. From this menu, select *Settings*.
- From the Network Scans section of the LT Assessment for SUSE window, select a scan and right-click to display a drop-down menu. From this menu, select *Settings*.
- From the Report Queries pane of the console window, select a report query and right-click to display the drop-down menu. From this menu, select *Settings*.

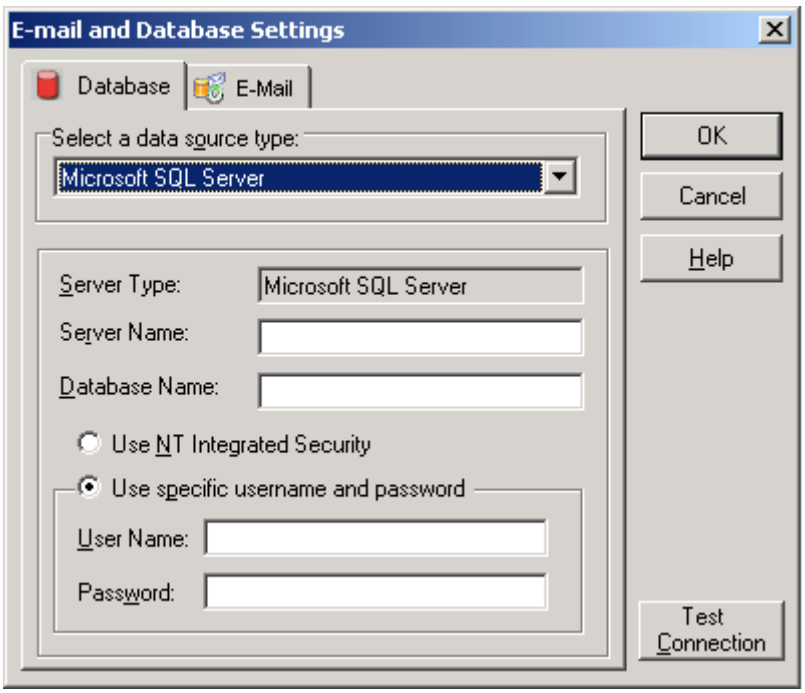
From the Select a database source type section, use the drop-down arrow to select an Access or SQL Server database.

Microsoft Access



If you selected Microsoft Access for your database, the log and template directories are named and created by default.

Microsoft SQL Server

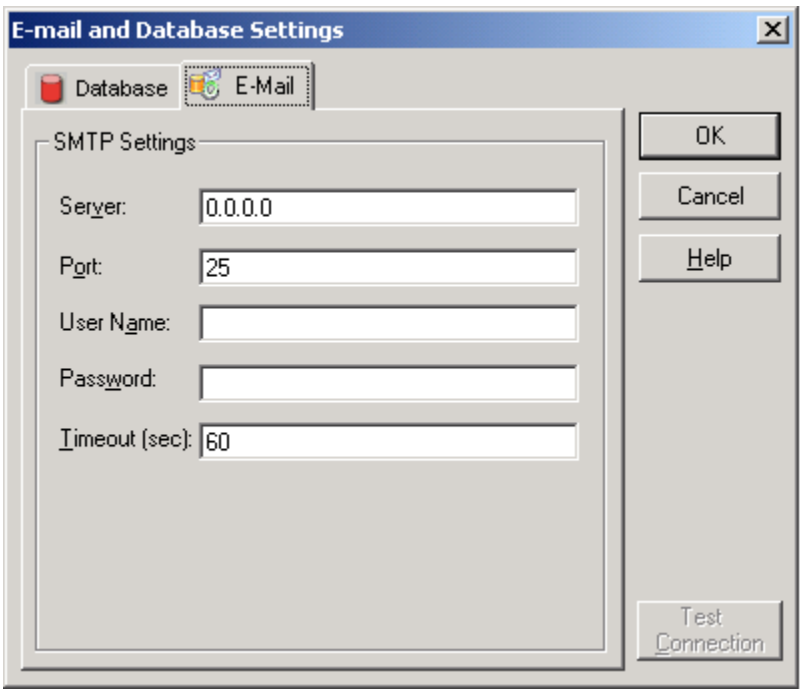


If you select Microsoft SQL Server, a warning message displays stating that if you change databases the data source will invalidate all the scans selected in each query. You will have to create new scans based on your current database settings. Click *Yes*. The preceding graphic displays.

Perform the following steps to ensure that you connect to the appropriate data source file. This data source file will be used by LT Assessment for SUSE to gather data for your report queries.

1. In the Server Name field, enter the SQL Server name.
2. In the Database Name field, enter the SQL Server database name.
3. Select either *Use NT Integrated Security* or *Use specific username and password*. If *Use specific username and password* is selected, enter the user name and password in the designated fields.
4. Click the *Test Connection* button to verify that you have a valid connection to the selected database.
5. Click *OK* to save your changes or *Cancel* to exit without saving.

E-Mail Settings



The E-mail tab defines the SMTP settings used by the computer to e-mail reports to servers. You can enter information into the following fields:

- **Server** — The name or IP address of the machine that hosts the e-mail services.
- **Port** — The number of the port used to send SMTP messages.
- **User Name** (if applicable) — The user name used to log into the e-mail server.
- **Password** (if applicable) — The password used to log into the e-mail server.
- **Timeout (sec)** — The amount of time that the application will attempt to connect to the server before stopping.

Calendar

The Calendar allows you to:

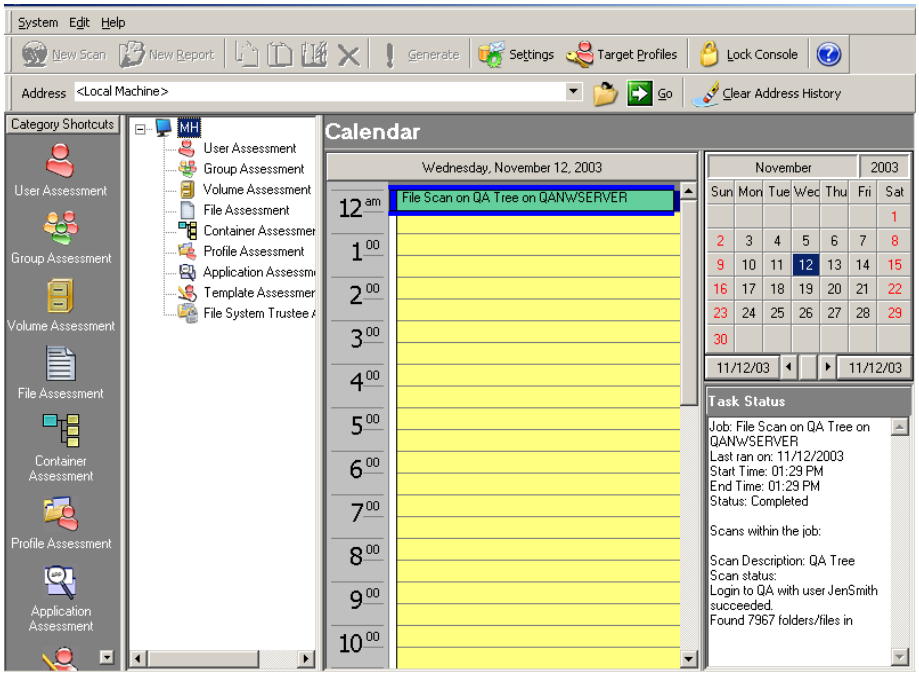
- Create a new job
- Review the status of your job
- Delete or modify existing jobs
- Review jobs previously run

Creating a New Job

A job schedules a network scan to collect eDirectory or file server data and records this information to a database. You can also configure a job to run a report based on the collected data.

If you want to schedule a job, perform the following steps:

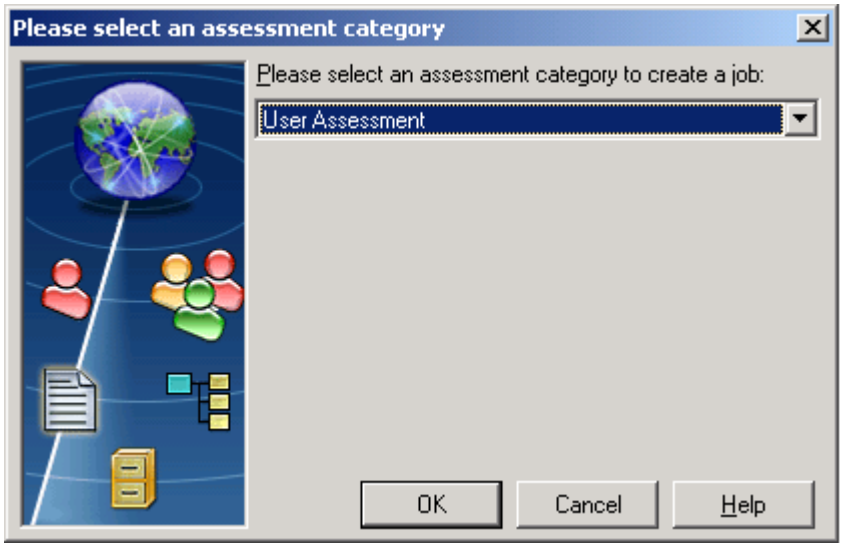
1. In the Assessment Category window, click the root of the tree structure. The Calendar displays.



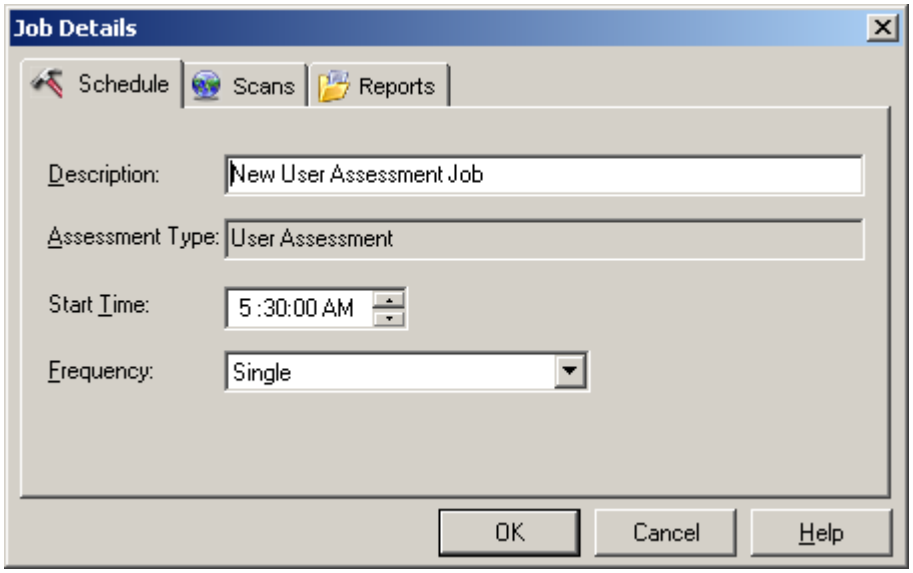
2. From the Calendar window, select a date to run your job. The Calendar window allows you to schedule jobs up to ninety days in advance.
3. Select a time in the Job Scheduler window.

4. To select a assessment category, perform one of the following steps:
   - From the Job Scheduler window, right-click the time you selected to display the drop-down menu. Select *Add New Job*.
   - From the Job Scheduler window, double-click the time you selected.

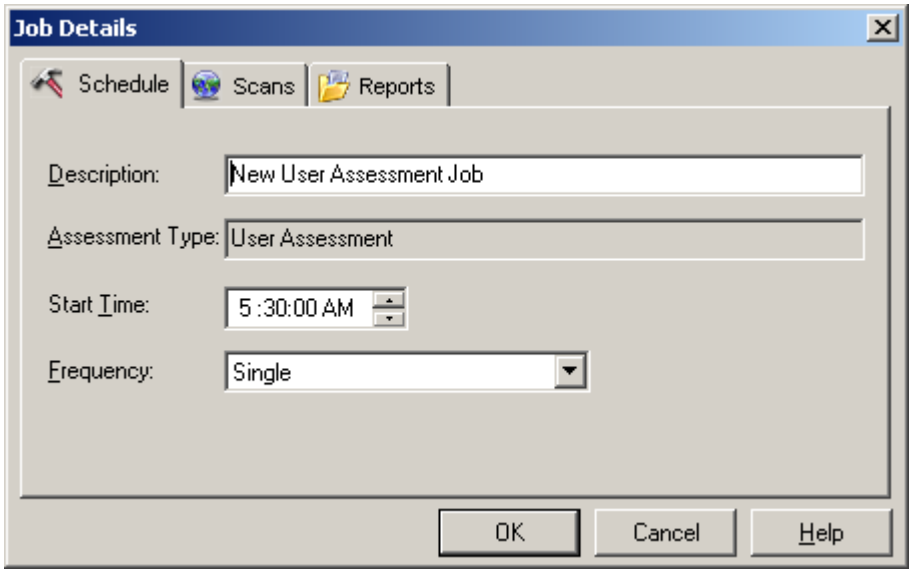
   The Please select an assessment category window displays.



5. Click the drop-down arrow and select an assessment category. Click *OK*. The Job Details window displays.



Providing the Job Details



The Job Details window includes the following tabs:

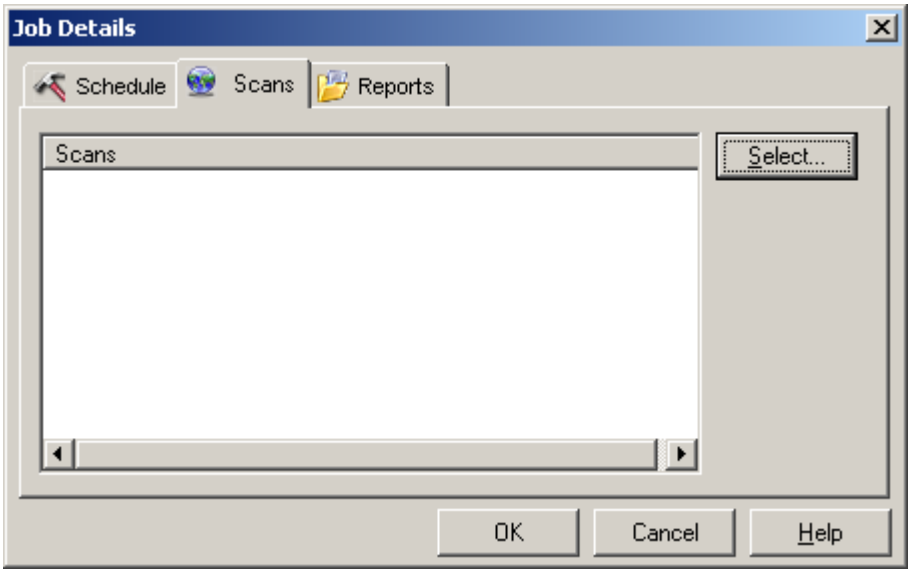
- **Schedule** — Allows you to select a name, time, and frequency to execute your job.
- **Scans** — Allows you to select a previously created network scan and create a snapshot based on the container, volume, or file you selected within that scan.
- **Reports** — Allows you to select preexisting queries based on the selected assessment type.

Schedule

On the Schedule tab, you can complete the following fields:

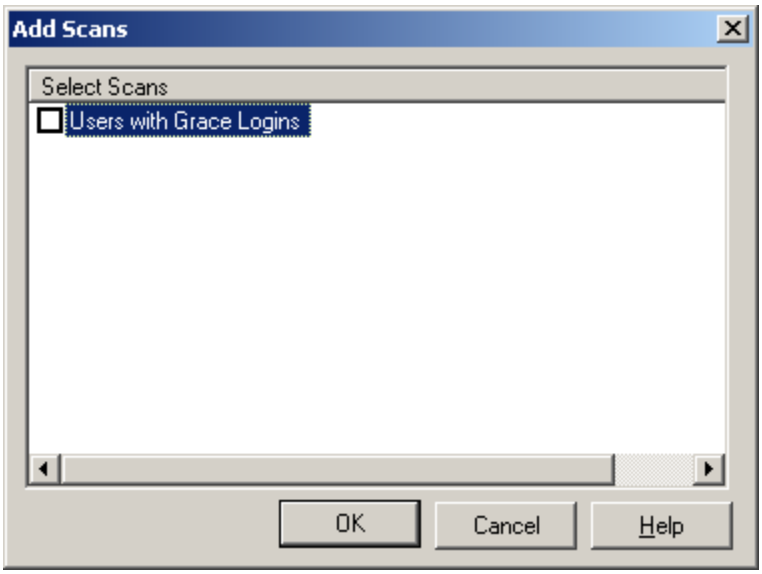
- **Description** — Enter a name for your job.
- **Assessment Type** — The assessment category for which the job is designed displays in this field.
- **Start Time** — Select the time when the job will be executed.
- **Frequency** — Select one of the following to determine how often the job will be executed:
  - Single
  - Daily
  - Weekly
  - Monthly

Scans



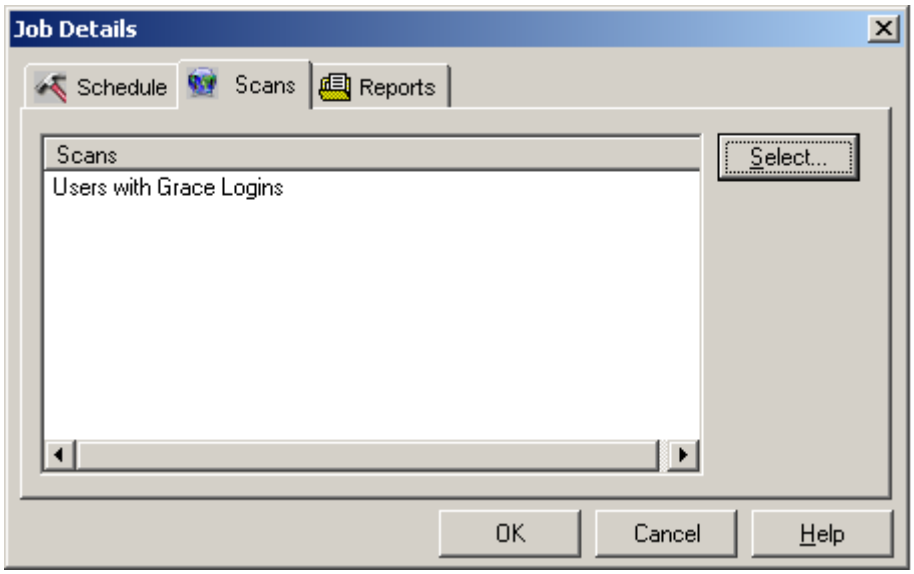
When scheduling a report, you must select a scan. The Scans tab allows you to select any network scans that were previous created. To select a specific network scan, perform the following steps:

1. From the Scans tab, click the *Select* button. The following window displays.

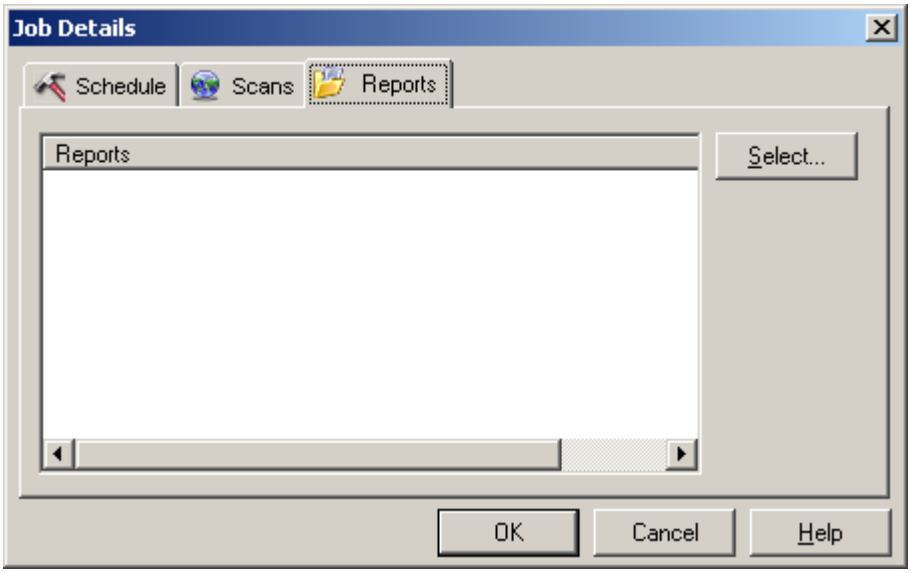


2. From the Add Scans window select the check box to the left of the network scan you would like to use. You can select one or multiple scans. This option allows you to scan more than one tree. Click *OK* to save your changes and return to the Job Details window.

3. The scans you selected now display. Click the *Reports* tab to select a specific report or click *OK* to run your job.

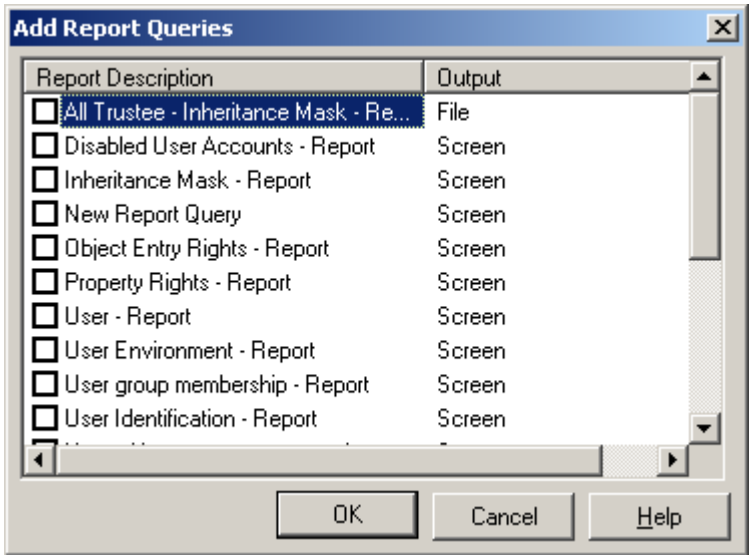


Reports



Select a report query from the Reports tab by performing the following steps:

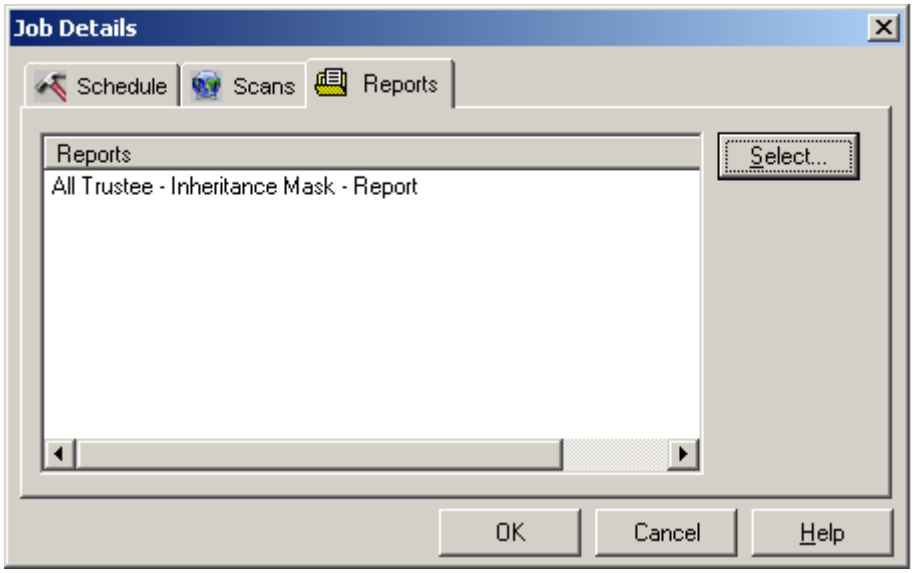
1. From the Reports tab, click the *Select* button. The following window displays the report queries of the assessment category you previously selected.



! **Important**

Clicking on a report that outputs to the screen is not a permissible action.

2. Click the check box to the left of the report query or queries that you want to run. This option allows you to run multiple report queries based on the selected scans. Click *OK* to return to the Job Details window.
3. The report query or queries that you selected display in the Reports column.



4. Click *OK* to save your changes and exit the Job Details window. The newly created job displays in the Calendar.

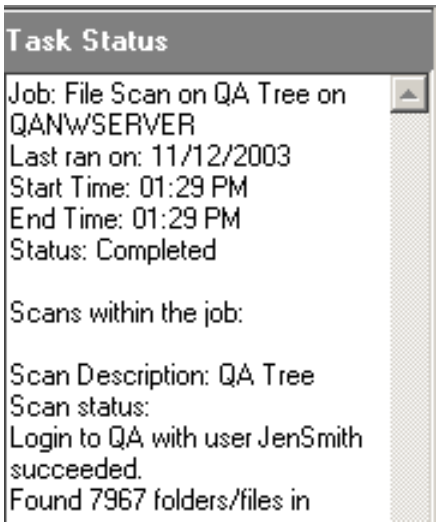
Reviewing the Status of a Job

After you have created a job, it displays in the Job Scheduler window. You can identify the status of a job by performing the following:

- Verifying the color of the square in the Job Scheduler window.
- Reviewing the information in the Task Status window.

The following colors will help you to determine the status of your job:

- **Gray** — Job history was not detected and job is currently in an idle state
- **Green** — Job completed
- **Red** — Job failed



You can use the Task Status window to identify the status of the job. From the Job Scheduler window, click the job and review the following information in the Task Status window:

- Job name
- Date job ran last
- Time the job was executed
- Time the job ended
- Status of the job

The Task Status window also lists the scans that were selected for the job.

Modifying Existing Jobs

Using LT Assessment for SUSE, you can modify existing jobs that are executed daily, weekly, or monthly. To modify an existing job, perform the following steps:

1. From the Calendar, select a day.
2. From the Job Scheduler window, select a job.
3. From the Job Scheduler window, right-click the job you want to modify. From the drop-down menu, click *Modify*.
4. When the Job Details window displays, you can modify your job's criteria. Click *OK* to save your changes and execute the job.

Deleting an Existing Job

To delete a job, perform the following steps:

1. From the Job Scheduler window, select the job you want to delete.
2. From the Job Scheduler window, right-click the job you want to delete. From the drop-down menu, click *Delete*.

> **!** **Important**
> Before you select the Delete button, verify that the appropriate job is selected.

3. Click *Yes* to confirm your deletion.

Reviewing Previously Run Jobs

You can review the status of previously run jobs by performing the following steps:

1. From the calendar select a past date.
2. From the Job Scheduler window, select a job.
3. Review the status of the job in the Task Status window.

Scenarios

This section includes three scenarios that you can use to compare with your LT Assessment for SUSE environment.

Scenario 1

You have been instructed by your administrator to ensure the security of your network. To ensure that user accounts are not violated, you want to perform a scan of your entire network and run a query on those users with a minimum password length fewer than five characters.

Solution 1

To use LT Assessment for SUSE to create a scan of the NetWare tree and run a report querying only users with passwords with less than five characters, perform the following steps:

1. From the LT Assessment for SUSE, select the *User Assessment* button. The Network Scans and Report Queries panes display.
2. From the Network Scans pane, double-click *Add New Scan*.
3. Select an existing target profile.
4. Click *OK* to exit the Add Scan window.
5. From the Report Queries pane, double-click the *Users with minimum password length below 5 characters* report query. The Report Query window displays.
6. Select the tabs and modify your criteria as needed.
7. Click *Run Report* to run the report immediately.
8. Click the *x* located at the top right corner of the LT Assessment for SUSE window to return to the Report Query window.
9. Click *Apply* → *OK* to save your changes and exit the Report Query window.

Scenario 2

You want to run a report based on an existing network scan. You want to query groups that were created on a specific date.

Solution 2

To accomplish this task, perform the following steps:

1. From the LT Assessment for SUSE, select the *Group Assessment* button. The Network Scans and Report Queries panes display.
2. From the Report Queries pane, double-click *Add a New Report*. The Report Query window displays.
3. From the General tab, enter a description for your report.
4. From the Choose a Network Scan Snapshot section, click the *Browse* button.
5. Select a snapshot and click *OK* to return to the Report Query window.
6. Click the *Statements* tab.
7. Click the *Add* button.
8. From the Report Query Statement Rules window *Query based on group creation date*.
9. From the Description section, click *Creation time is <Define>*.
10. From the Select Formula window, click the drop-down arrow and select *equal to*.
11. In the text field, enter a specific date and time.
12. Click *OK* → *OK* to return to the Report Query window.
13. Click the *Format* tab. From the Report Type drop-down menu, select *Group Summary Tabular Report*.
10. Click *Run Report* to run the report immediately.
11. Click the *x* located at the top right corner of the LT Assessment for SUSE window to return to the Report Query window.
14. Click *Apply* → *OK* to save your changes and exit the Report Query window.

Scenario 3

You have been instructed to use an existing scan to query user accounts that have been disabled. This query must be performed on a daily basis.

Solution 3

To create a job that is performed daily, using an existing scan, and querying user accounts that have been disabled, perform the following steps:

1. From the Category Shortcuts window in the LT Assessment for SUSE window, select *User* Assessment.
2. From the Report Queries pane, double-click *Disable User Accounts*. The Report Query window displays.
3. From the Report Query window, click the *Output* tab.
4. Select the *Send Report to Printer* radio button.
5. Click *Apply* → *OK* to save your changes and exit the Report Query window.
6. From the LT Assessment for SUSE window, click the root of the directory on the Assessment Category window.
7. From the calendar, select a date.
8. From the Job Scheduler window, select a time.
9. Double-click the time you selected. The Please select an assessment category window displays.
10. Select *User Assessment* and click *OK*. The Job Details window displays.
11. Enter a description for your job.
12. From the Frequency drop-down menu, select *Daily*.
13. Click the *Scans* tab.
14. Click the *Select* button. The Add a Scan window displays.
15. Select a scan and click *OK* to return to the Job Details window.
16. Click the *Reports* tab.
17. Click the *Select* button. The Add Report Queries window displays.
18. Check the *Disabled User Accounts* check box.

15. Click *OK* → *OK* to execute your job.
16. Click the job and review its status in the Task Status window.

LT Assessment for SUSE
Appendix A — Rules

Overview

LT Assessment for SUSE uses two types of rules:

- **Fixed rules** — A fixed rule cannot be modified.
- **Customizable rules** — A customizable rule allows you to apply certain operators against a given value to query for. A value can be one of the following:
  - Character string
  - Date
  - Number

Character String

The following table lists the operators that can be applied against a character string.

Operators	Definition	Examples
Equal to	An entity equivalent to the character string will be queried.	Query based on user name/User name is ▪ If Andre.ABC is listed in the text field, all user accounts with the name Andre.ABC will be queried.
Not Equal to	All entities, excluding the specified character string, will be queried.	Query based on user name/User name is ▪ If Jane.XYZ is listed in the text field, all accounts except Jane.XYZ are included in the query.
One of	Multiple entities will be queried.	Query based on user name/User name is ▪ If the account names Andre.ABC and Jane.XYZ are added to the list box, both user accounts will be queried.
Not one of	All entities, excluding the character string you entered, will be queried.	Query based on user name/User name is ▪ If the account names Andre.ABC and Jane.XYZ are added to the list box, neither user account will be queried.
Like	All entities containing the characters of the character string you entered will be queried.	Query based on user name/User name is ▪ If Jim is listed in the text field, all user accounts with the characters JIM will be queried. (Example: SHJIM.ABC, JIM.XYZ, and JIMT.ABC).
Not like	All entities containing the characters of the character string you entered will not be queried.	Query based on user name/User name is ▪ If Jim is listed in the text field, all user accounts with the characters JIM will not be queried. (Example: SHJIM.ABC, JIM.XYZ, and JIMT.ABC).

Date

The following tables list the operators that can be applied against a date value.

Operators	Definition	Examples
Equal to	An entity equivalent to the date value will be queried.	Query based on user login expiration date/User login expiration date is ▪ If 09/01/2003 is listed in the text field, all user accounts with login capabilities that expire on the specified date will be queried.
Not equal to	All entities, excluding the specified date value, will be queried.	Query based on user login expiration date/User login expiration date is ▪ If 12/03/2003 is listed in the text field, all user accounts with login capabilities that expire on the specified date will not be queried.
Between	All entities equivalent to a number between the specified date values will be queried.	Query based on user login expiration date/User login expiration date is ▪ If 07/12/03 and 01/15/03 are listed in the text fields, users accounts with login capabilities that expire in that time frame will be queried
Not between	All entities equivalent to a number between the specified date values will not be queried.	Query based on user login expiration date/User login expiration date is ▪ If 07/12/03 and 01/15/03 are listed in the text fields, users accounts with login capabilities that expire in that time frame will not be queried.
Less than	All entities equivalent to a date less than the specified date value will be queried.	Query based on user login expiration date/User login expiration date is ▪ If 03/21/2003 is listed in the text field users accounts with login capabilities that expire before that date will be queried.
Less than or equal to	All entities equivalent to a date less than or equal to the specified date value will be queried.	Query based on user login expiration date/User login expiration date is ▪ If 03/21/2003 is listed in the text field users accounts with login capabilities that expire on and before that date will be queried.
Greater than	All entities equivalent to a date greater than the specified date value will be queried.	Query based on user login expiration date/User login expiration date is ▪ If 11/27/2003 is listed in the text field users accounts with login capabilities that expire after that date will be queried.
Greater than or equal to	All entities equivalent to a date greater than or equal to the specified date value will be queried.	Query based on user login expiration date/User login expiration date is ▪ If 11/27/2003 is listed in the text field users accounts with login capabilities that expire on and after that date will be queried.

Operators	Definition	Examples
In the last	All entities equivalent to the past-specified number of days will be queried.	Query based on user login expiration date/User login expiration date is ▪ If the number 3 is listed in the text field, users accounts with login capabilities that expired in the past three days will be queried.
In the next	All entities equivalent to the next-specified number of days will be queried.	Query based on user login expiration date/User login expiration date is ▪ If the number 20 is listed in the text field, users accounts with login capabilities that expire in the next 20 days will be queried.
Not in the last	All entities equivalent to the past-specified number of days will not be queried.	Query based on user login expiration date/User login expiration date is ▪ If the number 3 is listed in the text field, users accounts with login capabilities that expired in the past three days will not be queried.
Not in the next	All entities equivalent to the next-specified number of days will not be queried.	Query based on user login expiration date/User login expiration date is ▪ If the number 20 is listed in the text field, users accounts with login capabilities that expire in the next 20 days will not be queried.

Number

The following tables list the operators that can be applied against a number value.

Operators	Definition	Examples
Equal to	An entity equivalent to the number value will be queried.	Query based on user password minimum length/ User password minimum length is ▪ If the number 6 is listed in the text field all user accounts whose password equals six characters will be queried.
Not equal to	All entities, excluding the specified number value, will be queried.	Query based on user password minimum length/ User password minimum length is ▪ If the number 9 is listed in the text field all user accounts whose password equals nine characters will not be queried.
One of	Multiple entities will be queried.	Query based on user password minimum length/ User password minimum length is ▪ If 2 and 3 are added to the list box, all user accounts whose password equals two or three characters will be queried.
Not one of	All entities, excluding the number value you entered, will be queried.	Query based on user password minimum length/ User password minimum length is ▪ If 5 and 6 are added to the list box, all user accounts whose password equals five or six characters will not be queried.
Between	All entities equivalent to a number between the specified number values will be queried.	Query based on user password minimum length/ User password minimum length is ▪ If 1 and 2 are added to the text fields, all user accounts whose password equals one and two characters will be queried.
Not between	All entities equivalent to a number between the specified number values will not be queried.	Query based on user password minimum length/ User password minimum length is ▪ If 3 and 5 are added to the text fields, all user accounts whose password equals three, four, or five characters will not be queried.
Less than	All entities equivalent to a number less than the specified number value will be queried.	Query based on user password minimum length/ User password minimum length is ▪ If 4 is entered in the text field, all user accounts whose password equals less than four characters will be queried.
Less than or equal to	All entities equivalent to a number less than or equal to the specified number value will be queried.	Query based on user password minimum length/ User password minimum length is ▪ If 4 is entered in the text field, all user accounts whose password equals or is less than four characters will be queried.
Greater than	All entities equivalent to a number greater than the specified number value will be queried.	Query based on user password minimum length/ User password minimum length is ▪ If 6 is entered in the text field, all user accounts whose password equals or is greater than six characters will be queried.
Greater than or equal to	All entities equivalent to a number greater than or equal to the specified number value will be queried.	Query based on user password minimum length/ User password minimum length is ▪ If 4 is entered in the text field, all user accounts whose password equals or is greater than four characters will be queried.

Rules

The following tables list the rules that are included with the LT Assessment for SUSE application. These tables also list the rule type and value associated with each rule.

User Assessment		
Rule/Rule Description	**Rule Type**	**Value**
Query based on user name/User name is	Customizable	Character string
Query based on full name/Full name is	Customizable	Character string
Query based on location/Location is	Customizable	Character string
Query based on location count/Location count is		
Query based on department/Department is	Customizable	Character string
Query based on department count/Department count is		
Query based on title/Title is	Customizable	Character string
Query based on title count/Title count is	Customizable	Number
Query based on tree name/Tree name is	Customizable	Character string
Query based on user context/container/User context/container is	Customizable	Character string
Query based on user creation date/User create date is	Customizable	Date
Query based on user modification date/User modified date is	Customizable	Date
Query based on network address/Network address is	Customizable	Character string
Query based on network address count/Network address count is	Customizable	Number
Query based on when user logged in/User last login date is	Customizable	Date
Query users that have never logged in	Fixed	N/A
Query based on users login expiration date/User login expiration date is	Customizable	Date
User accounts that have been disabled	Fixed	N/A
User accounts that have not been disabled	Fixed	N/A
User accounts that have been locked	Fixed	N/A
User accounts that have not been locked	Fixed	N/A
Query based on user incorrect login attempts/Users incorrect login attempt	Customizable	Number
Query based on user concurrent login settings/Users concurrent logins is	Customizable	Number
Query based on user grace login setting/Users grace login setting is	Customizable	Number
Query based on user grace login remaining/User grace login remain is	Customizable	Number
Query based on user password minimum length/ User password minimum length is	Customizable	Number
Query based on user password expiration interval/Users password expiration interval is	Customizable	Date
User accounts that are allowed to change their password	Fixed	N/A
User accounts that are not allowed to change their password	Fixed	N/A
User accounts that require a password to login	Fixed	N/A
User accounts that do not require a password to login	Fixed	N/A

User Assessment (continued)		
Rule/Rule Description	**Rule Type**	**Value**
User accounts that require a unique password to login	Fixed	N/A
User accounts that do not require a unique password to login	Fixed	N/A
Query based on user password expiration date/User password expiration date is	Customizable	Date
User accounts that do not have password expiration date	Fixed	N/A
Query based on user group membership/User group membership is	Customizable	Character string
Query based on user group membership count/User group membership count is	Customizable	Number
Query based on user security equivalence/User security equivalence is	Customizable	Character string
Query based on user security equivalence/User security equivalence count is	Customizable	Number
Query based on trustee name/ Trustee name is	Customizable	Character string
Query based on trustee name count/ Trustee name count is	Customizable	Number
Query based on property name	Customizable	Character string

Group Assessment		
Rule/Rule Description	**Rule Type**	**Value**
Query based on tree name/Tree is	Customizable	Character string
Query based on group context/container/Context is	Customizable	Character string
Query based on group name/Group name is	Customizable	Character string
Query based on group department/Group department is	Customizable	Character string
Query based on group department count /Group department count is	Customizable	Number
Query based on group location/Group location is	Customizable	Character string
Query based on group location count/Group location count is	Customizable	Number
Query based on group organization/Group organization is	Customizable	Character string
Query based on group organization count/Group organization count is	Customizable	Number
Query based on group owner/Group owner is	Customizable	Character string
Query based on group owner count/Group owner count is	Customizable	Number
Query based on group creation date/Creation time is	Customizable	Date
Query based on group modification date/Modification time is	Customizable	Date
Query based on group member/Member name is	Customizable	Character string
Query based on group member count/Member count is	Customizable	Number
Query based on trustee name/ Trustee name is	Customizable	Number
Query based on trustee name count/ Trustee name count is	Customizable	Character string
Query based on property name/Property name is	Customizable	Character string

Volume Assessment		
Rule/Rule Description	**Rule Type**	**Value**
Query based on volume name/Volume name is	Customizable	Character string
Query based on server name/Server name is	Customizable	Character string
Query based on volume total space/Total space is	Customizable	Number
Query based on volume used space/Used space is	Customizable	Number
Query based on volume purgeable space/Purgeable space is	Customizable	Number
Query based on volume creation date/Creation time is	Customizable	Date
Query based on volume modification date/Modification time is	Customizable	Date
Query based on user restrictions/User name is	Customizable	Character string
Query based on total space restrictions/Total space is	Customizable	Number
Query based on user's used space/User space is	Customizable	Number
Query based on volume user rights by user/User name is	Customizable	Character string
Query based on volume user rights count	Customizable	Number

File Assessment		
Rule/Rule Description	**Rule Type**	**Value**
Query based on file/folder name/File name is	Customizable	Character string
Query based on file/folder size/File size is	Customizable	Number
Query based on file/folder owner/ Owner is	Customizable	Character string
Query based on file/folder creation time/ Creation time is	Customizable	Number
Query based on file/folder modification time/Modification time is	Customizable	Number
Query based on file/folder last accessed time/Last accessed time is	Customizable	Number
Files that are marked as read only	Fixed	N/A
Files that are not read only	Fixed	N/A
Files marked for archive	Fixed	N/A
Files not marked for archive	Fixed	N/A
Files marked as hidden	Fixed	N/A
Files not marked as hidden	Fixed	N/A
Files marked as purge immediately	Fixed	N/A
File not marked as purge immediately	Fixed	N/A
File marked as copy inhibit	Fixed	N/A
Files not marked as copy inhibit	Fixed	N/A
File marked as rename inhibit	Fixed	N/A
Files not marked as rename inhibit	Fixed	N/A
Files marked as delete inhibit	Fixed	N/A
Files not marked as delete inhibit	Fixed	N/A
Files marked as transactional	Fixed	N/A
Files not marked as transactional	Fixed	N/A
Files marked as sharable	Fixed	N/A
Files not marked as shareable	Fixed	N/A
Files marked as not compressible	Fixed	N/A
Files marked as compressible	Fixed	N/A
Files marked as immediate compress	Fixed	N/A
Files not marked as immediate compress	Fixed	N/A

Container Assessment		
Rule/Rule Description	**Rule Type**	**Value**
Query based on tree name/Tree is	Customizable	Character string
Query based on container name/Container name is	Customizable	Character string
Query based on container context/Context is	Customizable	Character string
Containers set to detect intruder	Fixed	N/A
Containers not set to detect intruder	Fixed	N/A
Query based on incorrect login attempts/Incorrect login attempts	Customizable	Number
Query based on reset interval for intruder attempt/Reset interval is	Customizable	Number
Lockout account after intruder detection is set on	Fixed	N/A
Lockout account after intruder detection is not set	Fixed	N/A
Query based on reset interval after lockout	Customizable	Number
Containers that allow users to change the password	Fixed	N/A
Containers that do not allow users to change the password	Fixed	N/A
Containers that require a password	Fixed	N/A
Containers that do not require a password	Fixed	N/A
Query based on minimum password length/Minimum password length is	Customizable	Number
Query based on the number of days before a password is forced to change/Number of days is	Customizable	Number
Query based on password expiration date/Day and time is	Customizable	Date
Containers that require a unique password	Fixed	N/A
Containers that do not require a unique password	Fixed	N/A
Query based on number of grace logins for a container/Grace Logins are	Customizable	Number
Query based on grace logins remaining/Grace logins remaining are	Customizable	Number
Containers that do not have disabled accounts	Fixed	N/A
Query based on the expiration date of a container/Expiration date is	Customizable	Date
Query based on a container's concurrent connection limit/Concurrent connection limit is	Customizable	Number
Query based on container account balance/Account balance is	Customizable	Number
Query based on user equivalent to me/Container is	Customizable	Character string
Query based on user equivalent to me count/User name count is	Customizable	Number
Query based on container group/Group name is	Customizable	Character string
Query based on container group count /Group name count is	Customizable	Number
Group based on trustee name/Trustee name is	Customizable	Character string
Group based on trustee name count/Trustee name count is	Customizable	Number
Group based on property name/Property name is	Customizable	Character string

Profile Assessment		
Rule/Rule Description	**Rule Type**	**Value**
Query based on tree name/Tree name is	Customizable	Character string
Query based on profile context/container/Profile context/container is	Customizable	Character string
Query based on profile name/Profile name is	Customizable	Character string
Query based on profile department/Profile department is	Customizable	Character string
Query based on profile department count/Profile department count is	Customizable	Number
Query based on profile location/Profile location is	Customizable	Character string
Query based on profile location count/Profile location count is	Customizable	Number
Query based on profile organization/profile organization is	Customizable	Character string
Query based on profile organization count/profile organization count is	Customizable	Number
Query based on profile creation date/Profile creation date is	Customizable	Date
Query based on profile modification date/Profile modification date is	Customizable	Date

Application Assessment		
Rule/Rule Description	**Rule Type**	**Value**
Query based on tree name/Tree name is	Customizable	Character string
Query based on application container/context/Application container/context is	Customizable	Character string
Query based on application name/Application name is	Customizable	Character string
Query based on application creation date/Application creation date is	Customizable	Date
Query based on application modification date/Application modification date is	Customizable	Date
Query based on application version/Application version is	Customizable	Number
Query based on application marked as install only	Fixed	N/A
Query based on applications not marked as install only	Fixed	N/A
Query based on applications marked to run once	Fixed	N/A
Query based on applications not marked to run once	Fixed	N/A
Query based on applications forced to run if installed on a workstation	Fixed	N/A
Query based on applications not forced to run if installed on a workstation	Fixed	N/A

Template Assessment		
Rule/Rule Description	**Rule Type**	**Value**
Query based on tree name/Tree name is	Customizable	Character string
Query based on template container/context/Template container/context is	Customizable	Character string
Query based on template name/Template name is	Customizable	Character string
Query based on template department/Template department is	Customizable	Character string
Query based on template department count/Template department count is	Customizable	Number
Query based on template location/ Template location is	Customizable	Character string
Query based on template location count/ Template location count is	Customizable	Number
Query based on template title/Template title is	Customizable	Character string
Query based on template title count/Template title count is	Customizable	Number
Query based on template creation date/Template creation date is	Customizable	Date
Query based on template modification date/Template modification date is	Customizable	Date
Query based on template with login disabled	Fixed	N/A
Query based on template with login not disabled	Fixed	N/A
Query based on template login expiration date/Template login expiration date is	Customizable	Date
Query based on template maximum simultaneous logins	Customizable	Number
Query based on template accounts that allow password changes	Fixed	N/A
Query based on template accounts that do not allow password changes	Fixed	N/A
Query based on template accounts that require a password change	Fixed	N/A
Query based on template accounts that do not require a password change	Fixed	N/A
Query based on template password minimum length/Template password minimum length is	Customizable	Number
Query based on template password expiration interval/Template password expiration interval is	Customizable	Number
Query based on template password expiration date/Template password expiration date is	Customizable	Date
Query based on template accounts that require a unique password	Fixed	N/A
Query based on template accounts that do not require a unique password	Fixed	N/A
Query based on template grace login limit/Template grace login limit is	Customizable	Number
Query based on template security equivalent to me/Template security equivalent to me is	Customizable	Character string

Template Assessment (continued)		
Rule/Rule Description	**Rule/Rule Description**	**Rule/Rule Description**
Query based on template security equivalent to me count/Template security equivalent to me count is	Customizable	Number
Query based on template group membership/Template group membership is	Customizable	Character string
Query based on template group membership count/Template group membership count is	Customizable	Number
Query based on template members/Template member is	Customizable	Character string
Query based on template members count/Template member count is	Customizable	Number
Query based on template security equivalences/Template security equivalent to	Customizable	Character string
Query based on template security equivalences count/Template security equivalent count is	Customizable	Number

File System Trustee Assessment		
Rule/Rule Description	**Rule Type**	**Value**
Query based on server name/Server name is	Customizable	Character string
Query based on trustee name/Trustee name is	Customizable	Character string
Query based on file/folder name/File/folder name is	Customizable	Character string
Query based on class/Class is	Customizable	Character string
Trustee with [Read] access rights	Fixed	N/A
Trustee without [Read] access rights	Fixed	N/A
Trustee with [Write] access rights	Fixed	N/A
Trustee without [Write} access rights	Fixed	N/A
Trustee with [Create] access rights	Fixed	N/A
Trustee without [Create] access rights	Fixed	N/A
Trustee with [Erase] access rights	Fixed	N/A
Trustee without [Erase] access rights	Fixed	N/A
Trustee with [Modify] access rights	Fixed	N/A
Trustee without [Modify] access rights	Fixed	N/A
Trustee with [File Scan] access rights	Fixed	N/A
Trustee without [File Scan] access rights	Fixed	N/A
Trustee with [Access Control] access rights	Fixed	N/A
Trustee without [Access Control] access rights	Fixed	N/A

LT Assessment for SUSE
Appendix B — Report Types

Overview

This appendix includes a list of report types included with the LT Assessment for SUSE application. It also lists the type of assessment data that can be queried using these report types.

- User Assessment
  - User Access Control Rights Report
    - Trustee/Inheritance mask
    - Property
    - Rights
  - User Account Restrictions Tabular Report
    - User
    - Container
    - Full name
    - Grace login limit
    - Concurrent logins allowed
    - Login expiration time
    - Creation date
    - Password required
    - Password minimum length
    - Password must be unique
    - Password change interval
  - User Creation Modification Report
    - User
    - Container
    - Last Modified On
    - Created On

- User Creation Modification Tabular Report
  - User
  - Container
  - Full name
  - Last modified on
  - Created on
- User Environment Tabular Report
  - User
  - Full name
  - Language
  - Network address
  - Default server
  - Home directory volume
  - Home directory path
- User Group Membership Report — Groups
- User Identification Report
  - Other name
  - Title
  - Location
  - Department
  - Telephone
  - Fax
  - Email address
  - Description

- User Identification Tabular Report
  - User
  - Full name
  - Other name
  - Title
  - Location
  - Department
  - Telephone
  - Fax
  - Email address
- User Inheritance Mask Report
  - User
  - Object/Property
  - Rights
- User Inheritance Mask Tabular Report
  - User
  - Full name
  - Object/Property
  - Rights
- User Invalid Login Information Report
  - User
  - Container
  - Last Login Time
  - Invalid Login attempts
  - Account locked
  - Login reset time
  - Login intruder address

- User Invalid Login Information Tabular Report
  - User
  - Container
  - Full name
  - Last login time
  - Invalid login attempts
  - Account locked
  - Login reset time
  - Login intruder address
- User Login Information Report
  - User
  - Container
  - Last login time
  - Login disabled
- User Login Information Tabular Report
  - User
  - Container
  - Full name
  - Last login time
  - Account disabled
- User Login Setting Report
  - User
  - Container
  - Login disabled
  - Grace login limit
  - Grace login remaining
  - Concurrent logins allowed
  - Login expiration time
  - Account locked

- User Login Settings Tabular Report
  - User
  - Container
  - Full name
  - Account disabled
  - Grace login limit
  - Grace login remaining
  - Concurrent logins allowed
  - Login expiration time
  - Account locked
- User Network Restriction Report — Restricted network address
- User Object Rights Report
  - User
  - Trustee
  - Rights
- User Objects Rights Tabular Report
  - User
  - Full name
  - Trustee
  - Rights
- User Password Settings Report
  - User
  - Container
  - Requires a password
  - Requires a unique password
  - Allowed to change password
  - Minimum password length
  - Password expires on

- User Password Settings Tabular Report
  - User
  - Container
  - Full name
  - Required password
  - Required unique password
  - Allowed to change password
  - Minimum password length
  - Days between change
  - Password expires on
- User Property Rights Report
  - Trustee/Inheritance mask
  - Property
  - Rights
- User Security Equivalence Report — Security equals to

- Group Assessment
  - Group Creation Modification Report
    - Group
    - Context
    - Last modified on
    - Created on
  - Group Creation Modification Tabular Report
    - Group
    - Context
    - Number of users
    - Last modified on
    - Created on
  - Group Description Report — Group description

- Group Identification Report
  - Departments
  - Locations
  - Organizations
  - Other names
  - Owners
- Group Inheritance Mask Report
  - Group
  - Object/property
  - Rights
- Group Inheritance Mask Tabular Report
  - Group
  - Object/Property
  - Rights
- Group Member Report — Group members
- Group Object Rights Tabular Report
  - Group
  - Trustee
  - Rights
- Group Property Rights Report
  - Trustee
  - Property
  - Rights
- Group Summary Report
  - Group
  - Context
  - Total number of members

- Group Summary Tabular Report
  - Group
  - Context
  - Total number of members
- Group Trustee Report
  - Trustee
  - Property
  - Rights

- Volume Assessment
  - Volume Creation Modification Report
    - Volume
    - Last modified on
    - Created on
  - Volume Creation Modification Tabular Report
    - Volume
    - Last modified on
    - Created on
  - Volume Details Tabular Report
    - Volume
    - Total space
    - Used space
    - Free space
    - Purgeable space
  - Volume Summary Report
    - Used space
    - Free space
    - Purgeable space

- Volume User Restrictions Report
  - User
  - Total space
  - Used space
- Volume User Rights Report
  - User
  - Rights

- File Assessment
  - File Information Report Grouped by Folder
    - File name
    - Owner
    - File size
    - Last modified on
    - Last accessed on
    - Created on
    - Attributes
  - File Information Report
    - Folder/File name
    - Owner
    - File size
    - Last modified on
    - Created on
    - Attributes

- File Information Tabular Report
  - Folder/File name
  - Owner
  - File size
  - Last modified on
  - Last accessed on
  - Created on
  - Attributes
- File Ownership Report Grouped by Owner
  - File name
  - Owner
  - File size
  - Last modified on
  - Last accessed on
  - Created on
  - Attributes
- File Ownership Report
  - File name
  - File size
  - Last modified on
  - Last accessed on
  - Created on
  - Attributes
- File Ownership Summary Tabular Report
  - Owner
  - File count
  - Total file size

- File Trustee Report (All Files)
  - Trustee
  - Rights
- All Trustee Report
  - Trustee
  - Rights

- Container Assessment
  - Container Group Report — Group inside the container
  - Container Inheritance Mask Report
    - Container
    - Object/Property
    - Privilege
  - Container Inheritance Mask Tabular Report
    - Container
    - Object/Property
    - Privilege
  - Container Intruder Detection Settings Report
    - Container
    - Detect intruder
    - Incorrect login attempts limit
    - Intruder lockout reset intervals
    - Intruder attempt reset interval
  - Container Intruder Detection Settings Tabular Report
    - Container
    - Users
    - Detect intruder
    - Incorrect login attempts limit
    - Locked by intruder
    - Account locked
    - Intruder lockout reset interval
    - Intruder attempt reset interval

- Container Invalid Login Information Report
  - Container
  - Account locked
  - Intruder lockout reset interval
  - Intruder attempt reset interval
- Container Login Settings Report
  - Container
  - Login disabled
  - Grace login limit
  - Grace login remaining
  - Concurrent logins
  - Login expiration time
  - Account locked
- Container Login Settings Tabular Report
  - Container
  - Login disabled
  - Grace login limit
  - Grace login remaining
  - Concurrent logins
  - Login expiration time
  - Account locked
- Container Network Restriction Report — Restricted network address
- Container Object Rights Report
  - Container
  - Trustee
  - Privilege
- Container Object Rights Tabular Report
  - Container
  - Trustee
  - Rights

- Container Object Summary Report
  - Container
  - Containers
  - Groups
  - Users
  - Volumes
  - Servers
  - Applications
  - Print servers
  - Printers
  - Print queues
  - Other
- Container Object Summary Tabular Report
  - Container
  - Containers
  - Groups
  - Users
  - Volumes
  - Servers
  - Applications
  - Print servers
  - Printers
  - Print queues
  - Other
- Container Password Setting Report
  - Container
  - Allowed to change password
  - Password required
  - Password minimum length
  - Password expiration date
  - Requires unique password

- Container Password Setting Tabular Report
  - Container
  - Allowed to change password
  - Password required
  - Password minimum length
  - Password expiration date
  - Requires unique password
- Container Property Rights Report
  - Trustee
  - Property
  - Rights
- Container Trustee Report
  - Trustee/Inherited mask
  - Property
  - Rights

- Profile Assessment
  - Profile Creation Modification Tabular Report
    - Profile
    - Container
    - Last modified on
    - Created on
  - Profile Description Report — Profile description
  - Profile Identification Report
    - Department
    - Location
    - Organization
    - Other names
  - Profile Object Rights Tabular Report
    - User
    - Trustee
    - Rights

- Application Assessment
  - Application Creation Modification Tabular Report
    - Application
    - Container
    - Version
    - Last modified on
    - Created on
  - Application Object Rights Tabular Reports
    - Application
    - Trustee
    - Rights
  - Application Settings Tabular Report
    - Application
    - Container
    - Version
    - Install only
    - Run once
    - Force run if workstation
    - File path
    - Working path
    - Parameters

- Template Assessment
  - Template Access Control Rights Report
    - Trustee/Inheritance Mask
    - Property
    - Rights
  - Template Creation Modification Tabular Report
    - Template
    - Container
    - Last modified on
    - Created on
  - Template Description Report — Description
  - Template Equivalent To Me Report — Security equal to me
  - Template Group Membership Report — Group
  - Template Identification Report
    - Department
    - Fax
    - Language
    - Location
    - Other name
    - Telephone
    - Title
  - Template Inheritance Mask Tabular Report
    - Template
    - Object/Property
    - Rights
  - Template Login Settings Tabular Report
    - Template
    - Container
    - Account disabled
    - Grace login limit
    - Concurrent logins allowed
    - Login expiration time

- Template Network Restriction Report — Restricted network address
- Template New Object DS Rights Report
  - Object
  - Property
  - Rights
- Template New Object Self Rights Report
  - Property
  - Rights
- Template New Object Trustee Report
  - Trustee
  - Property
  - Rights
- Template Object Rights Tabular Report
  - Template
  - Trustee
  - Rights
- Template Password Settings Tabular Report
  - Template
  - Container
  - Requires password
  - Requires unique password
  - Allowed to change password
  - Minimum password length
  - Password expires on
- Template Property Rights Report
  - Trustee/Inheritance mask
  - Property
  - Rights
- Template Security Equivalence Report — Security equal to

- File System Trustee Assessment
  - File System Trustee Group by File Folder Report
    - Trustee
    - Class
    - Rights
  - File System Trustee Group by Server Report
    - File/Folder
    - Trustee
    - Class
    - Rights
  - File System Trustee Group by Trustee Report
    - Server name
    - File/Folder
    - Rights
  - File System Trustee Tabular Report
    - Server name
    - File/Folder
    - Trustee
    - Class
    - Rights