BLUE LANCE

LT Auditor+

Configuration Guide

Intellectual Property

Special Conventions

The following special icons are used in this document to alert the reader to important pieces of information:

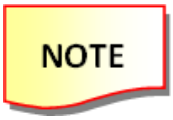
Icons	Description
	**WARNING: Alerts the reader to a potential action, practice or situation that can result in major damage to data or the system. Damage is permanent and irreversible. Results may be contrary to what is expected or intended.**
	**CAUTION: Alerts the reader to a potential action, practice or situation that can result in minor damage to data or the system. Results may be contrary to what is expected or intended.**
	**NOTE: Extra or supplementary information that needs to be emphasized to the reader. Can provide further context, instructions or understanding**
	**TIP: Useful tips or pointers that can help the reader while they are using the product or this document.**

Table of Contents

Chapter 1 – About the Document

This chapter provides a general overview of this document and contains the following major subsections:

- Document Purpose
- Document Audience
- Document Scope
- Using this Document
- Getting Technical Support

Document Purpose

This document is intended to serve as a document that best describes the procedures and steps for Installing LT Auditor+. It focuses on the prerequisites, system requirements and pre-installation of LT Auditor+.

Document Audience

This document is intended for the following users:

Team or person responsible for using the LT Auditor+ application
Team or person entrusted with deploying LT Auditor+ in the environment

Document Scope

The scope of this document includes information that will help you understand the functionalities of LT Auditor+.

The scope includes the following major topics:

- Description of key features
- Details on configuring and using LT Auditor+

Using this Document

This section explains the installation and configuration of the LT Auditor+.

Document Structure

The document is divided into the following chapters:

Chapter	Description
About the Document	Provides information about this document, including what it is used for, who should read it, what it contains, how it is presented and how it is used.
About LT Auditor+ Configuration Guide	Provides information about LT Auditor+ configuration, deployment and management of audit policies.

Chapter 2 – LT Auditor+ Workspace

This section will provide detailed steps to show you how to use LT Auditor+ Security Management Console to configure your workspace.

Connecting to the Workspace

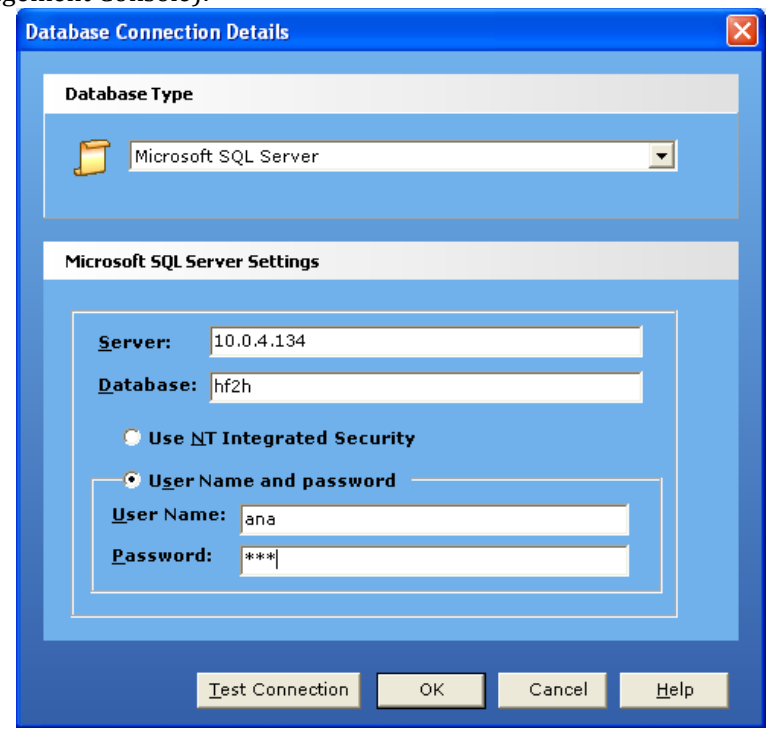
1. To launch the Security Management Console click Start → All Programs → Blue Lance, Inc → Management Console.

The first screen prompts you for the database connection information. This lets you connect to the workspace that you need to configure.

NOTE

You must be authenticated to (have credentials to access) the workspace.

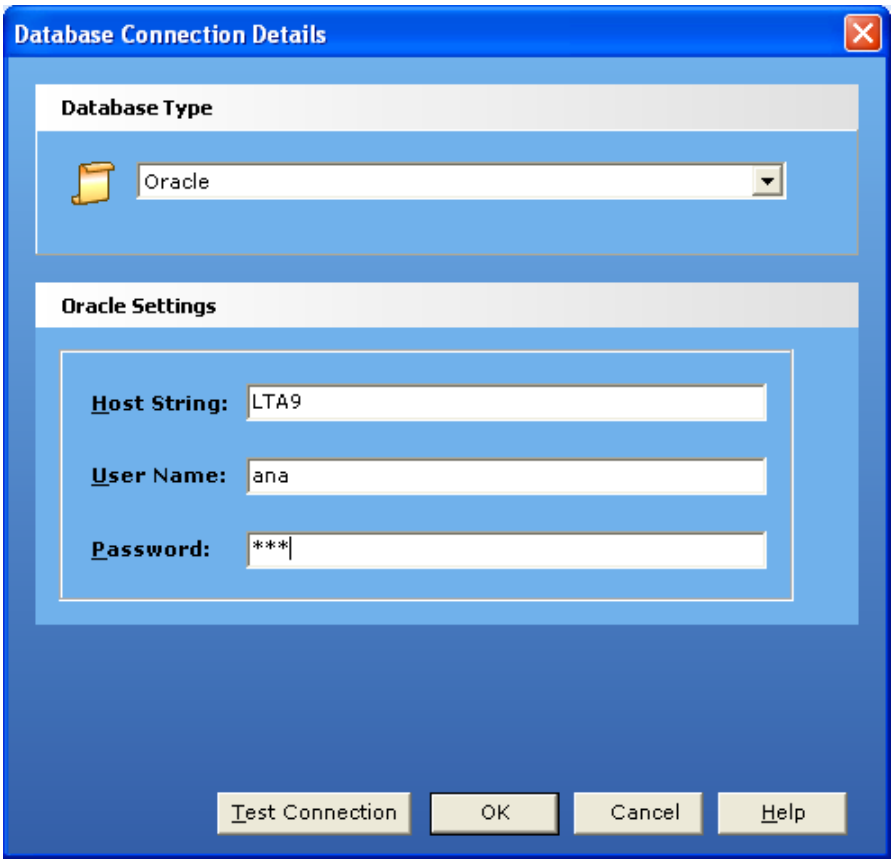
For SQL (Management Console):



2. Select Microsoft SQL Server for database type.
3. Provide Server ID.

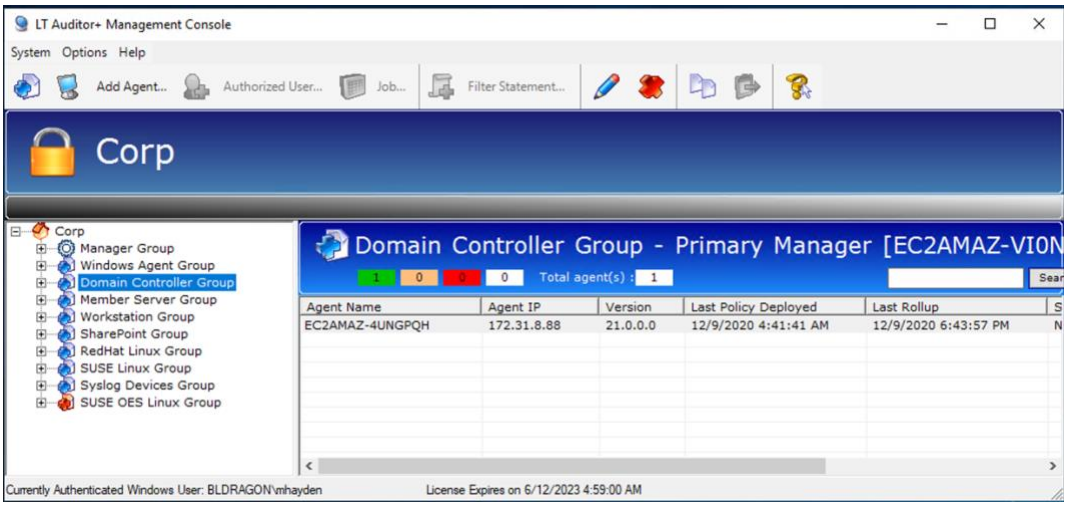
4. Provide Database Name.
5. Select Use NT Integrated Security or User Name and Password.
6. If User Name and Password is selected, provide the username and the password.
7. Click OK.

For Oracle (Management Console):



1. Select Oracle for database type.
2. Provide host string.
3. Provide username
4. Provide password.
5. Click OK.

The Management Console will be launched as soon as you are authenticated to the workspace as displayed in the screen below:



The Management Console is divided into two views. The left pane shows the currently configured workspace with the workspace name as the root node of the tree. Below the root nodes are the manager groups and agent groups of the workspace. The right pane displays the details of each node highlighted on the left side.

Select the workspace root node in the tree to display all the manager groups and agent groups in the pane on the right side.

Manager Groups

Manager groups cannot be created using the Management Console. These groups are created when you install the LT Auditor+ Manager as discussed in the LT Auditor+ Installation Guide. A workspace can contain more than one manager residing in more than one manager group.

NOTE

You need to place managers in different manager groups if you intend to have different policies for each manager.

Creating Agent Groups

New agent groups are created from the Management Console. To create a new Windows agent group, choose one of the following:

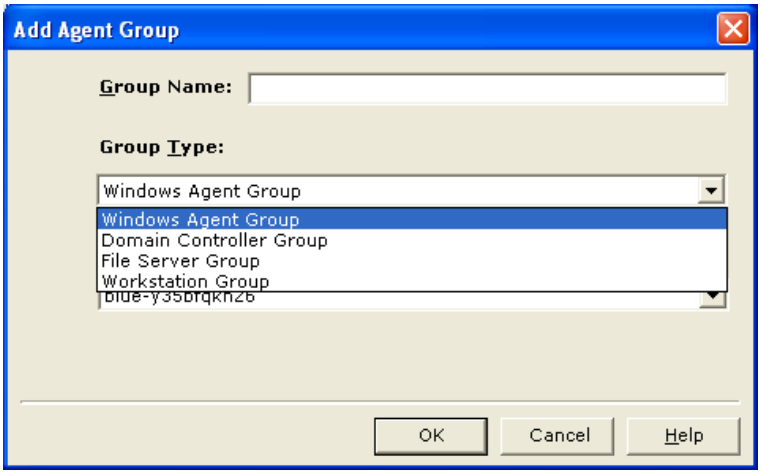
1. Click on System → New → Windows Agent Group OR
2. Click on the toolbar icon Windows Agent Group OR
3. Right-click on the Workspace.
4. Click Windows Agent Group.

When creating a new agent group in the Management Console, the user must determine the type of agent group being created. There are four types of agent groups available for creation in LT Auditor+ for Windows; these include:

- **Windows Agent Group** – This group type is intended for backward compatibility with older versions of LT Auditor+. It may contain machines of any type.
- **Domain Controller Group** – This group type may only contain domain controller machines.
- **Member Server Group** – This group type may only contain member server machines.
- **Workstation Group** – This group type may only contain nonserver machines in the domain.

To create a new agent group:

1. Right-click on the root node of the workspace in the left pane of the Management Console.
2. Select Agent Group (Windows/SUSE Linux or any other application)
3. The new form for agent group creation appears as below:



The selection of domain and group type will determine which agent machines are available in the workspace for addition to the new agent group.

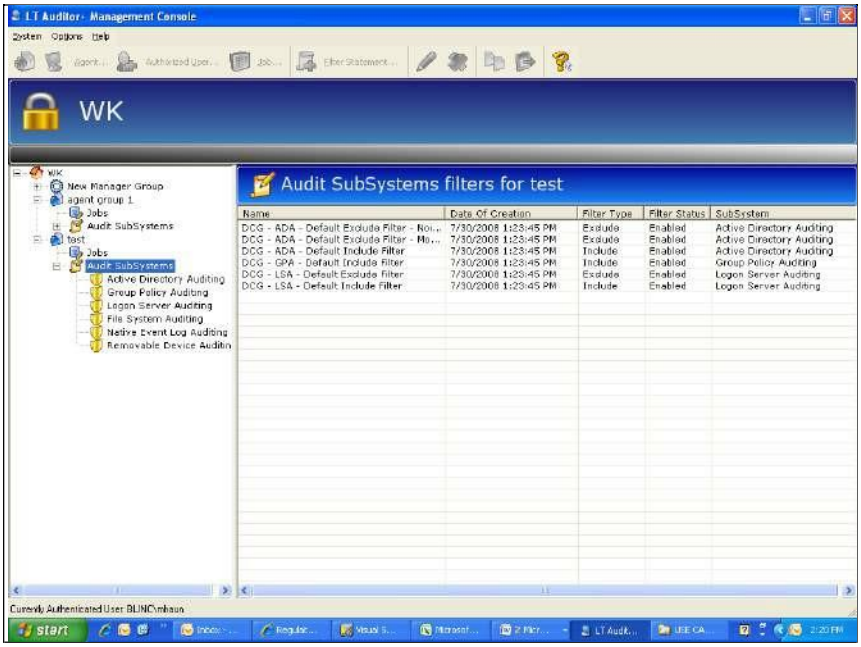
A primary manager is responsible for deploying policies that change within that group. Also, all agents within that group will attempt data transfer with the primary manager first, before attempting to transfer to any other manager in the workspace.

Default Filter Statement

Default filter statements will now be set for each agent group upon creation and will vary according to group type as is appropriate. Default filter statements may be modified in any way to suit specific auditing needs and may be restored to their original configuration at any time by selecting the Restore Default Settings option in the menu.

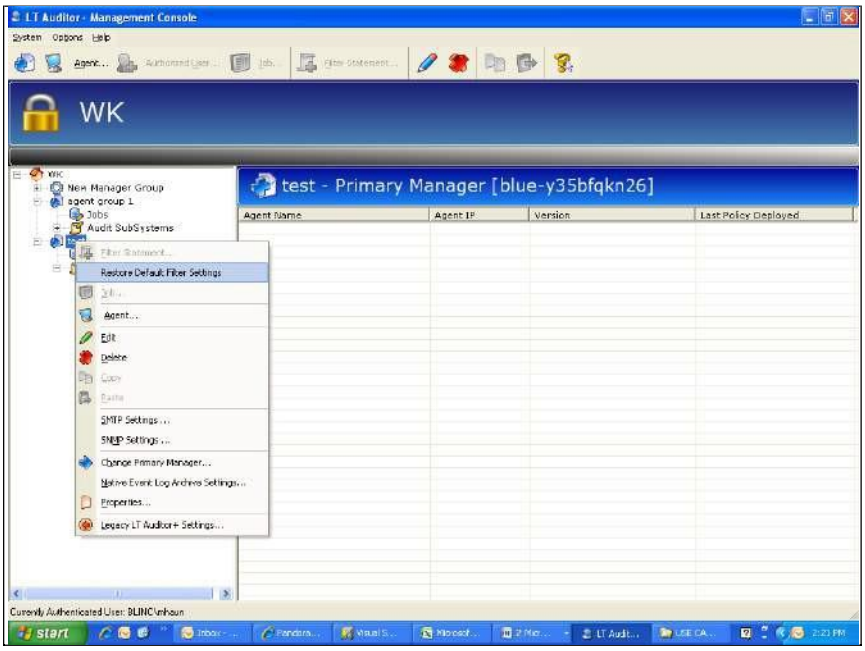
To view default filters:

1. Highlight the agent group or a specific audit subsystem whose filters you would like to view in the left pane of the Management Console.
   The default filters will appear in the right pane list view.



To restore the default settings after reconfiguration:

2. Right-click on the agent group
3. Select Restore Default Filter Settings from the menu. Restoring default filter settings may only be done for all audit subsystems within an agent group simultaneously.
   Default settings may not be restored for an individual subsystem.



The default filters for each group type are listed below:

Domain Controller Groups

Active Directory:

Exclude Noise Users Statement – Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*

a. Exclude Modify Object Statement – Excludes the "modify object" operation
b. Include Statement – Includes all operations

Group Policy:

a. Include Statement – Includes all operations

Logon Server:

a. Exclude Noise Users Statement - Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*
b. Include Statement – Includes operations Interactive Logon, Remote Interactive Logon, All Directory Authentications, All Failed Logons

Member Server Groups

Logon Server:

a. Exclude Noise Users Statement - Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*

b. Include Statement: Includes the operations Interactive Logon, Remote Interactive Logon, All Failed Logons

Removable Device:

a. Exclude Noise Events Statement: Excludes the operation – Write Attribute
b. Include Statement: Includes all operations

SAM:

a. Exclude Noise Users Statement - Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*

    a. Exclude Modify Object Statement – Excludes the Modify Object operation
    b. Include Statement – Includes all operations

Workstation Groups

Logon Server:

a. Exclude Noise Users Statement – Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*

b. Include Statement – Includes the operations Interactive Logon, Remote Interactive Logon, All Failed Logons

Removable Device:

a. Exclude Noise Events Statement – Excludes the operation Write Attribute
b. Include Statement – Includes all operations

SAM:

a. Exclude Noise Users Statement – Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*

b. Exclude Modify Object Statement – Excludes the Modify Object operation
c. Include Statement – Includes all operations

Windows Agent Groups

Active Directory:

a. Exclude Noise Users Statement - Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*

b. Exclude Modify Object Statement – Excludes the Modify Object operation
c. Include Statement – Includes all operations

Group Policy:

a. Include Statement – Includes all operations

Logon Server:

a. Exclude Noise Users Statement – Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*

b. Include Statement – Includes the operations Interactive Logon, Remote Interactive Logon, All Directory Authentications, All Failed Logons

Removable Device:

a. Exclude Noise Events Statement – Excludes the operation Write Attribute
b. Include Statement – Includes all operations

Manager Groups

Active Directory:

a. Exclude Noise Users Statement – Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*

b. Exclude Modify Object Statement – Excludes the Modify Object operation
c. Include Statement – Includes all operations

Group Policy:

a. Include Statement – Includes all operations

Logon Server:

a. Exclude Noise Users Statement – Excludes Users: *$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*

b. Include Statement – Includes the operations Interactive Logon, Remote Interactive Logon, All Directory Authentications, All Failed Logons

Removable Device:

a. Exclude Noise Events Statement – Excludes the operation Write Attribute
b. Include Statement – Includes all operations

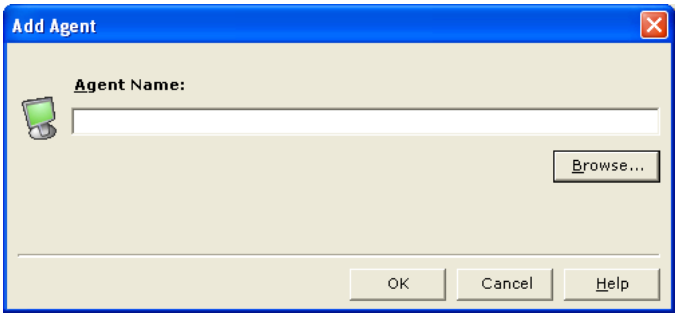
Adding Agents to Agent Groups

Use this option if the LT Auditor+ Agent is already installed on agent being added to Agent Group. To add an agent to a Windows agent group, choose one of the following:

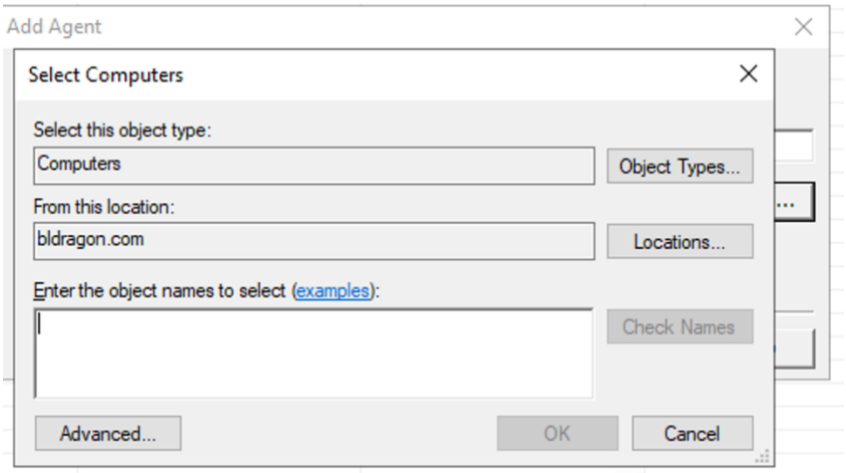
1. Click on System →New → Agent OR
2. Click on the toolbar icon Agent OR
3. Right-click on Agent Group.
4. Click Agent.
5. Provide the IP address or the machine name of the agent that needs to be added.
6. The machine must already have the agent installed, be running, and be a free agent in order to be added to an agent group.

To browse for agents:

1. Right-click on the agent group to which you would like to add a gents.
2. Select Agent from the menu. The following form will appear:



3. Click the Browse button. The following selection form will appear:



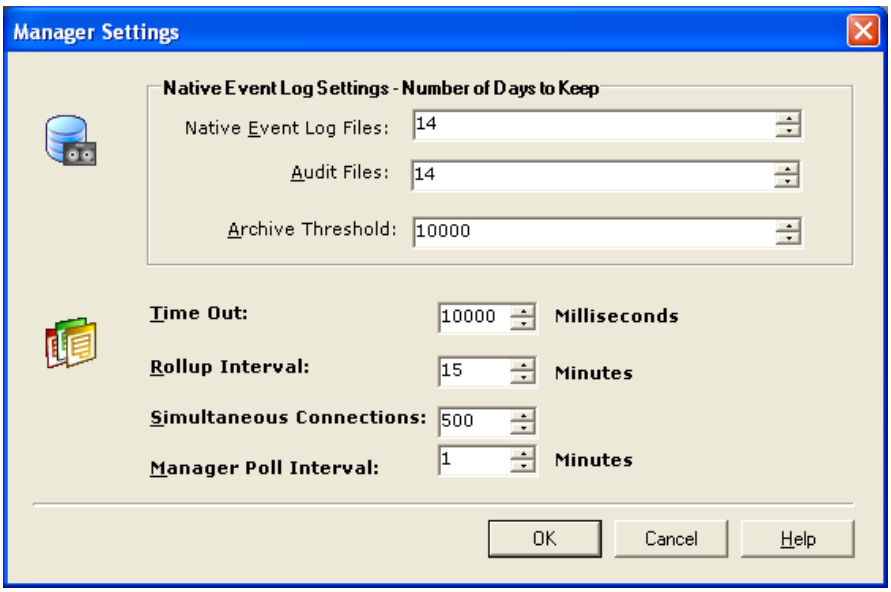
4. Type a machine name or click Advanced to browse Active Directory for machines to install.
5. Click OK.
6. The agents will be added to the chosen agent group.

Renaming agent groups:

1. To rename a group, right-click on the group.
2. Click Edit.
3. Provide the new name for the group and click Enter.

Modifying Manager Group Settings

1. Right-click on Manager Group.
2. Click Manager Settings.



Number of Days to Keep Native Event Logs: This setting is used by the manager to decide how long to keep the archived native event logs of the manager and agents. The default setting is 14 days. The minimum setting is 0 days, and the maximum setting is 90 days.

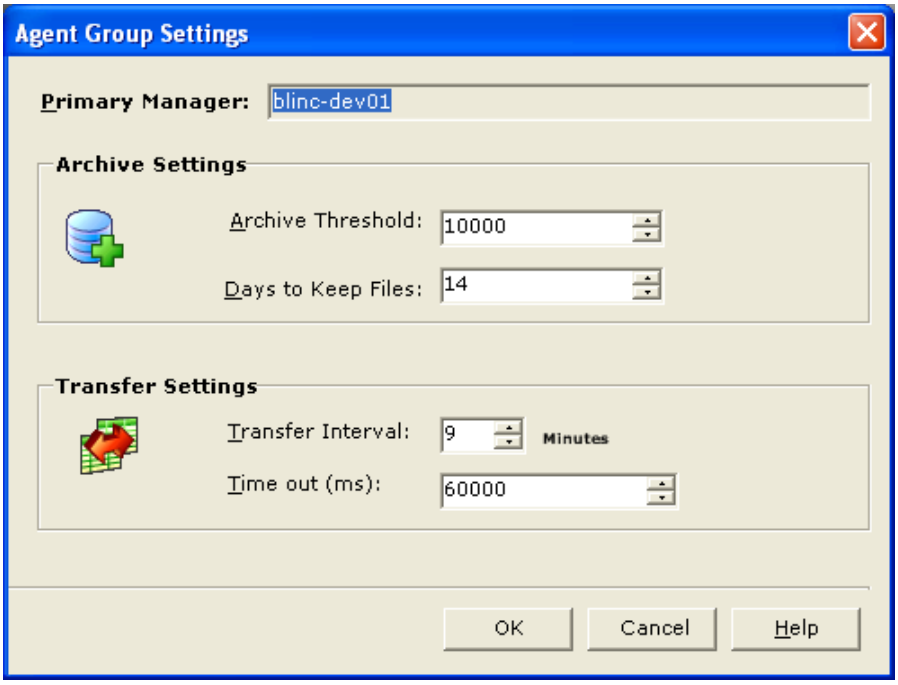
Rollup Interval: This setting is used by the manager to determine the time that elapses between rollups. The default setting is 15 minutes. The minimum setting is 0 minutes, and the maximum setting is 59 minutes.

Simultaneous Connections: This setting is used by the manager as a threshold of connections. The manager will reject all connections exceeding this setting. This setting is used by the manager for load balancing. The default setting is 500 connections. The minimum setting is 1 connection. There is no maximum setting.

Manager Polling Interval: The manager uses this interval to check with the workspace database to see if there are any policy changes for itself as well as the agents that it manages. The default setting is 1 minute. The minimum setting is 0 minutes, and the maximum setting is 15 minutes.

Modifying Agent Group Settings

1. Right-click on the agent group.
2. Click Properties.



Archive Threshold: The agent machine will create an archived file as soon as it reaches this threshold. The default setting is 10,000 records. The minimum setting is 1,000 records, and the maximum setting is 10,000 records.

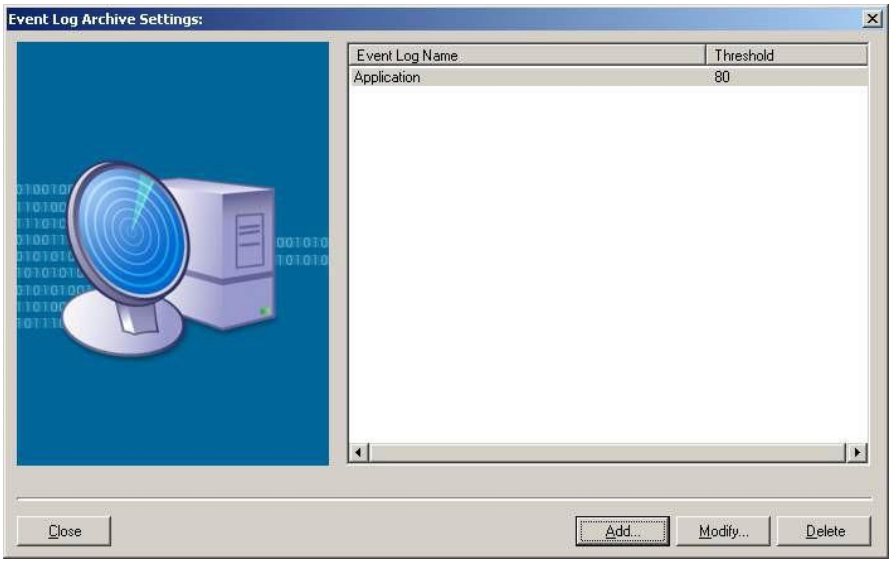
Days to Keep File: The agent machine backs up archived files after they are sent over to the manager. This setting decides how many days the agent will continue to store the backed-up files on the agent machine. The default setting is 14 days. The minimum setting is 0 days, and the maximum setting is 90 days.

Transfer Interval: The agent machine can send archived data files over to the manager on a regular interval. This setting is used to decide this interval. A setting of 0 disables the interval-based data transfer and relies totally on job-based data file transfers. The default setting is 15 minutes. The minimum setting is 0 minutes and the maximum setting is 59 minutes.

Time out: This setting determines the interval of time an agent will attempt to establish a connection with the manager. The default setting is 60,000 milliseconds. The minimum setting is 10,000 milliseconds and the maximum setting is 120,000 milliseconds.

Native Event Log Archive Settings

1. Right-click on the manager or agent group
2. Click on Native Event Log Archive Settings to show a list of all Native Event Logs that need to be archived at a specific percentage of their maximum settings.



To add a new Native Event Log archive setting, choose one of the following:

1. Click Add.
2. Choose appropriate name from list OR
3. Type in the name.
4. Click OK.

To modify a NEL archive setting:

1. Select the Event Log Name.
2. Click Modify.
3. Change the data.
4. Click OK.

To delete an NEL archive setting:

1. Select the Event Log Name
2. Click Delete. The system will ask for confirmation.
3. Click Yes.

Archive Threshold: Provide the threshold percentage. The default setting is 80 percent. The minimum setting is 15 percent, and the maximum setting is 95 percent.

Modify the Threshold: Choose the event log, click Modify, change the threshold.

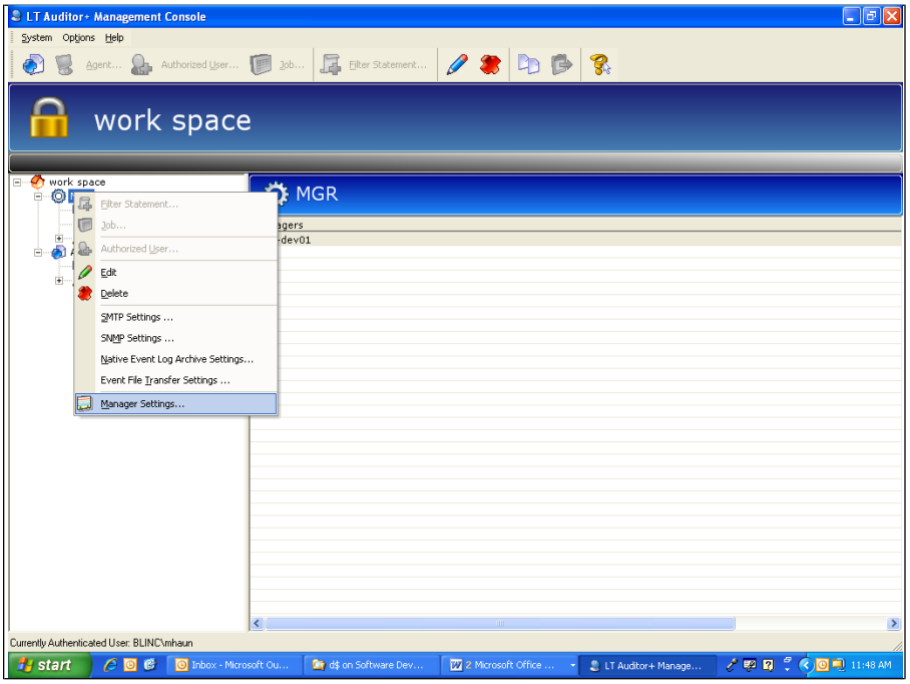
Delete the Threshold: Choose the event log, click Delete, and confirm by clicking Yes.

Event Log Threshold

This setting allows for the archiving of event logs based on specified thresholds. Archiving of event logs will create a local copy of the log, which will then be processed by LT Auditor+. For extremely busy servers, setting a threshold to force archives should be considered to not lose audit data due to standard event log overwrite settings.

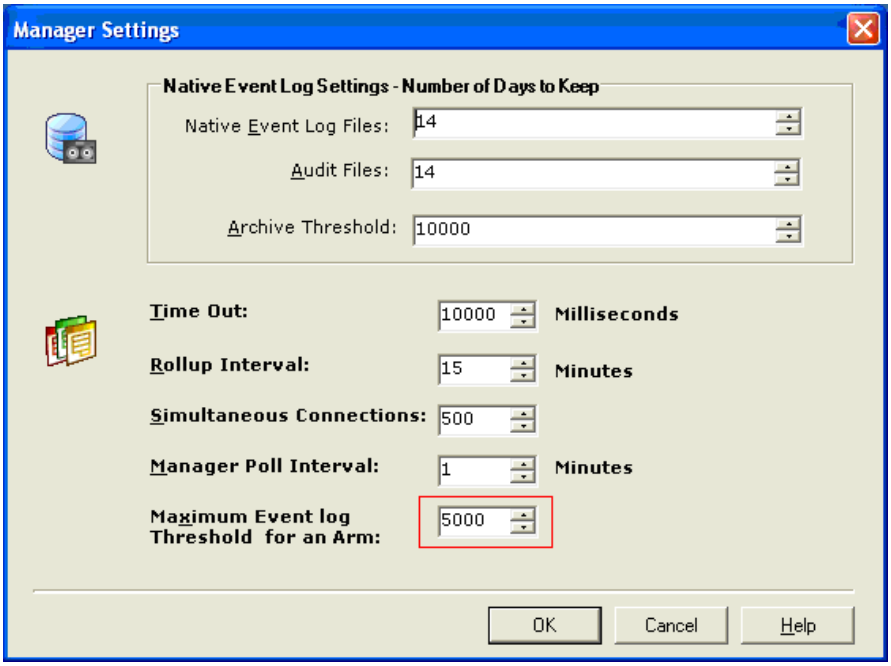
To apply threshold limitations through the Manager:

a. Right-click on the Manager node in the left pane of the Management Console.
b. Select Manager Settings from the drop-down menu.



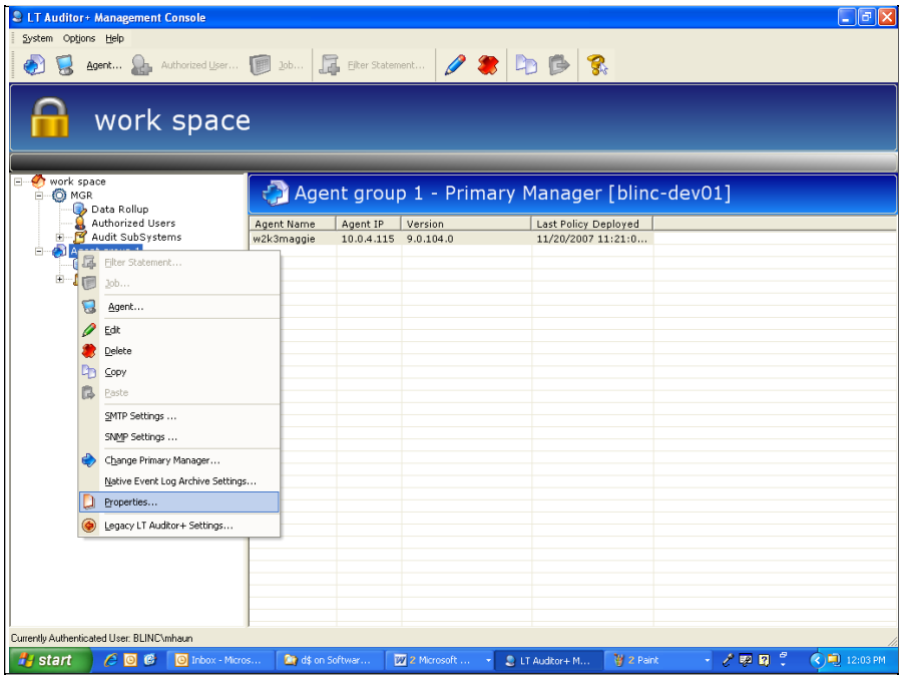
c. Provide a number of events in the Maximum Event Log Threshold for an Arm field. The default setting is 5,000 events. The minimum setting is 5,000 events, and the maximum setting is 100,000 events.
d. Click OK once the desired setting has been entered.

The settings will take effect the next time the manager polls the database for policy changes. This is dependent on the "Poll Interval" setting.



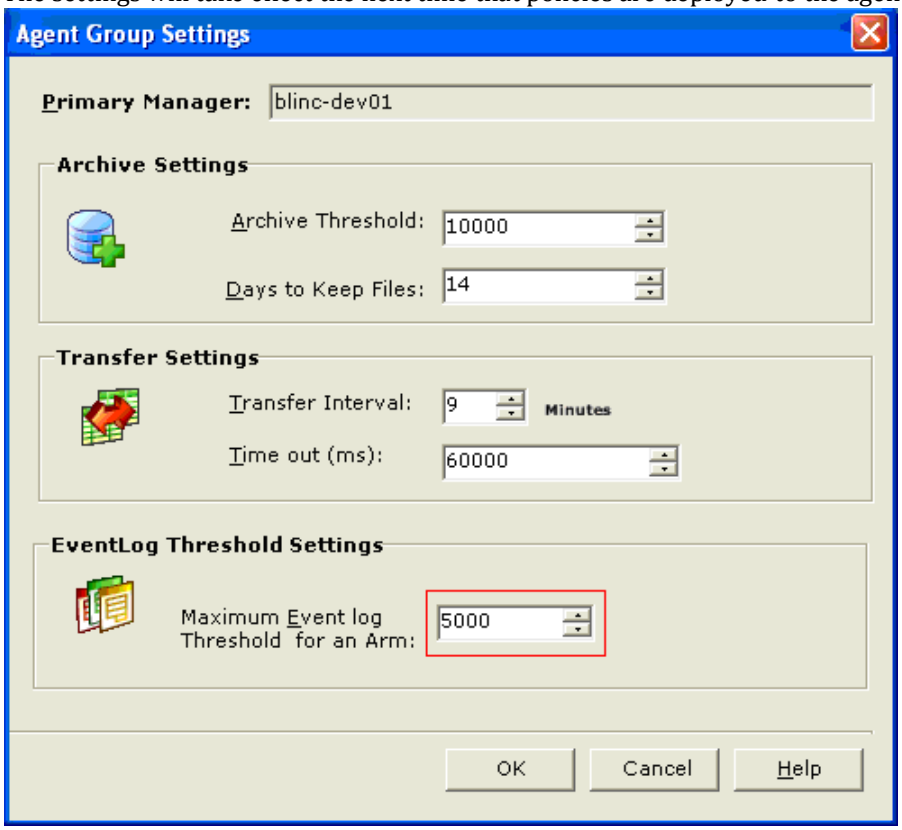
To apply threshold limitations through an agent group:

1. Right-click on the Agent Group node in the left pane of the Management Console.
2. Select Properties from the drop-down menu.



3. Provide a number of events in the Event Log Threshold Settings field. The default setting is 5,000 events. The minimum setting is 5,000 events and, the maximum setting is 100,000 events.
4. Click OK once the desired setting has been entered.

The settings will take effect the next time that policies are deployed to the agents.



Event File Transfer Settings

LT Auditor+ has the capability to archive native event logs onto a local disk through agents/managers. Given that the size of archive data is not limited, there is an increasing probability of issues resulting in a filled disk or not enough disk space. Event file transfer allows the ability to compress and move this data to another physical location. The manager has the capability to compress and move these backup files onto another file server or shared folder. This feature should be configurable in terms of shared folder path and user's credentials to access this folder. Data will be archived whenever rollup occurs.

To launch the Event File Transfer Settings:

1. Click on Options → Event File Transfer Settings. The following screen will be displayed.

2. To activate transfer settings, check Activate Backup.

Backup Folder: The user should designate the backup folder in which the files will reside once transferred.
User Name and Password: This is the username and password that the user enters to connect to the shared folders or network.

Chapter 3 – Audit Policies

Configuring LT Auditor+ Audit Policies

Common Filter Settings

To create any new Active Directory filter, Group Policy filter, file system filter, logon server filter, or Native Event Log filter, begin by highlighting the chosen subsystem in the left pane of the Management Console. Then select one of the following:

1. Click System → New → Filter Statement

   OR

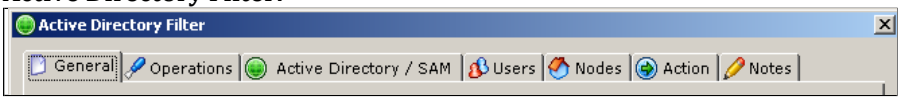
2. Click Filter Statement on the toolbar icon

   OR

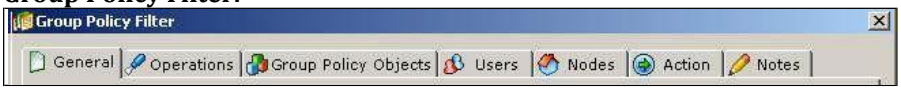
3. Right-click on the chosen subsystem, then click Filter Statement.

Given below are the samples of the tabs for the various auditing filters:

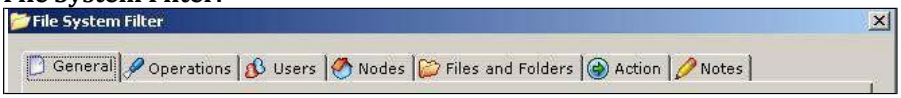
Active Directory Filter:



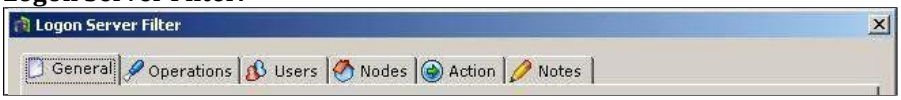
Group Policy Filter:



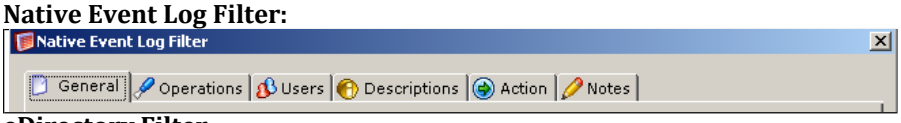
File System Filter:



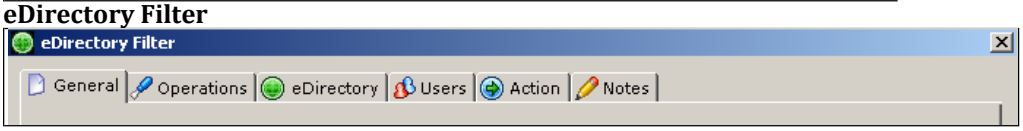
Logon Server Filter:



Native Event Log Filter:



eDirectory Filter



Logon Server Filter

General Settings

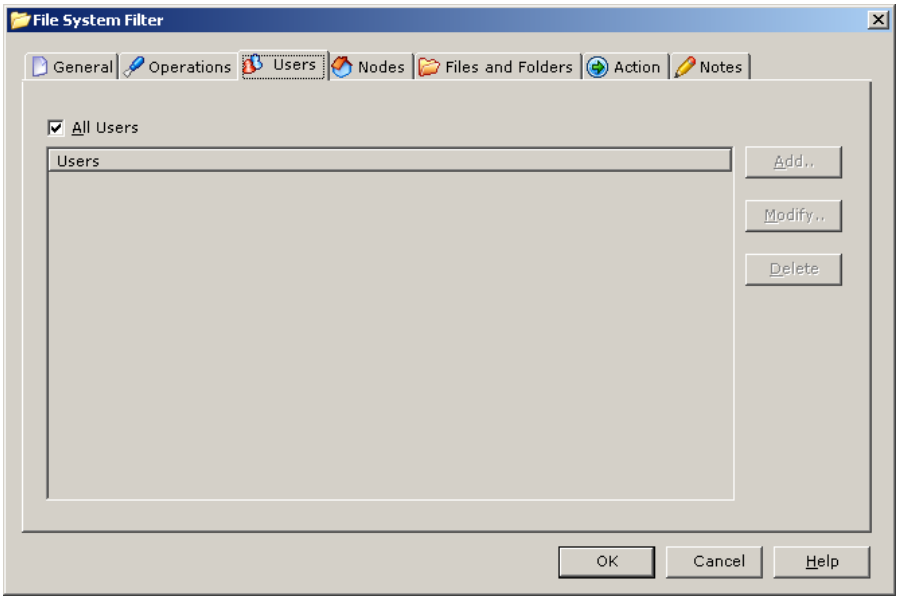
Filter Name: Provide a name to identify the filter statement from a collection of filters that have been created.

Filter Statement Type: Include Statement audits a particular operation only if all of the filter criteria are met. Exclude Statement rejects a particular operation and does not audit if any of filter criteria are met.

All Day: Each filter statement can be modified with a time the statement would be active. Select All Day to have filter statement active for the entire day, or select a specific start time and end time to determine when the filter statement will be active.

Enable Filter: To completely disable the filter settings, uncheck the Enable Filter**.**

User Settings



All Users:

To audit all users performing any active directory operation:

1. Select All Users.
2. To monitor specific user accounts, uncheck All Users.
3. Click Add. Provide the usernames to be audited.

NOTE

A wildcard (*) may be used.

4. Click OK.

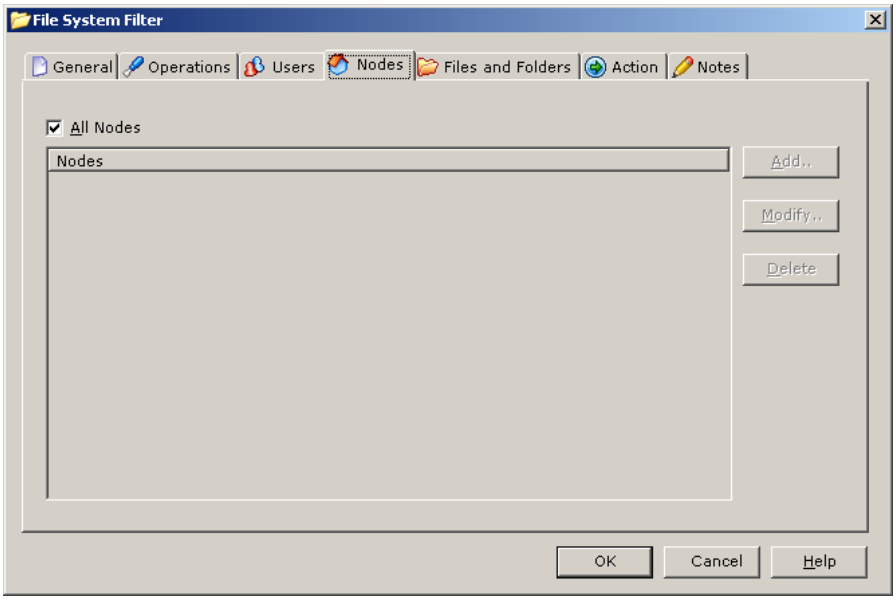
To modify a user:

5. Highlight the user, click Modify.
6. Change the user data, click OK.

To delete a user:

7. Highlight the user.
8. Click Delete. The system will ask you for confirmation.
9. Click Yes.

Node Settings



All Nodes:
To audit all specific workstations from which active directory operations are performed:

1. Select All Nodes.
2. To monitor specific nodes, uncheck All Nodes.
3. Click Add.
4. Provide the specific nodes to be audited.
5. Click OK.

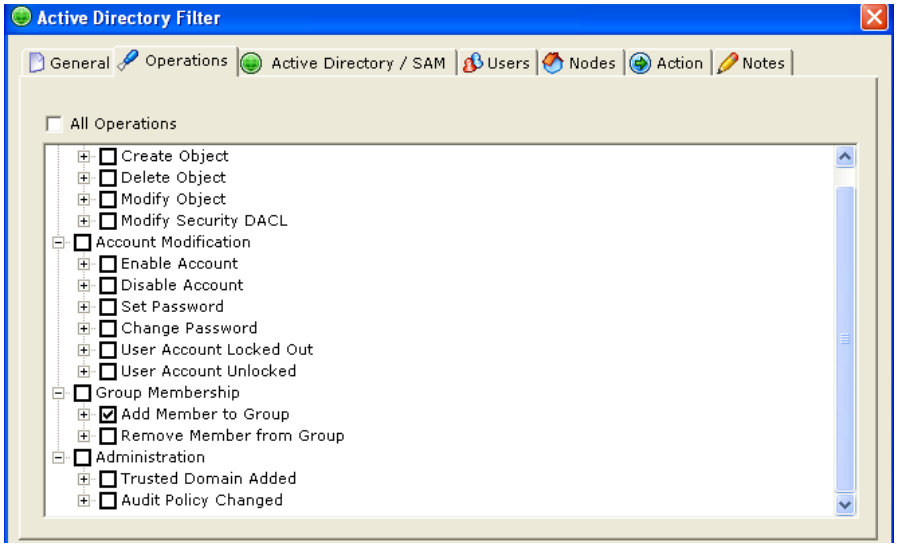
To modify a Node:

1. Highlight the node.
2. Click Modify.
3. Change the node data.
4. Click OK.

To delete a Node:

1. Highlight the node.
2. Click Delete. The system will ask you for confirmation.
3. Click Yes.

Operations Settings

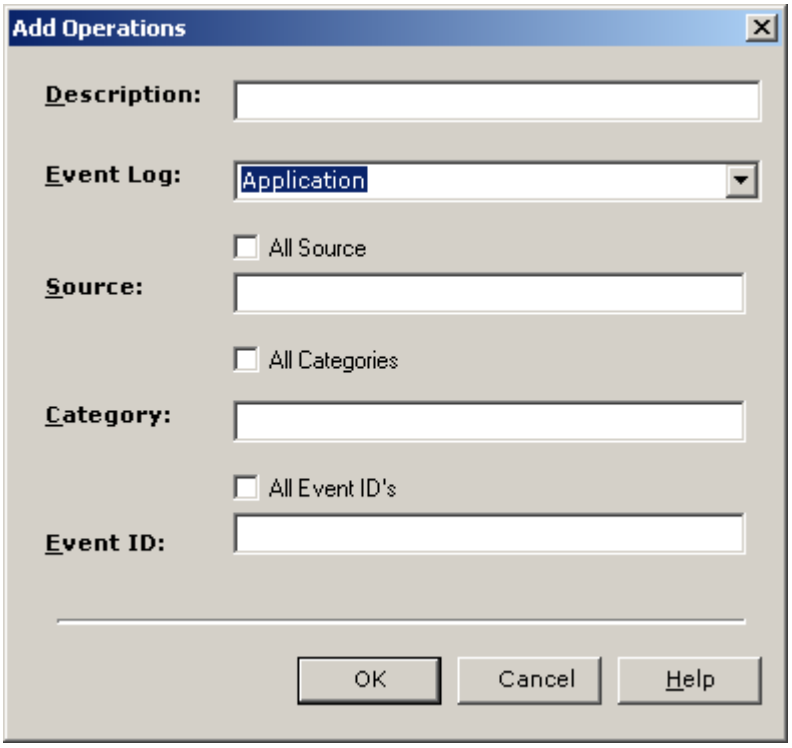


1. Select All Operations to audit all subsystem operations.
2. To select specific operations of interest, uncheck All Operations.
3. Select the appropriate operation(s) to audit.

NOTE Operations will vary between subsystems, but the method of selection will remain the same in all subsystems with the exception of the Native Event Log operations filter, whose method is described below.

Native Event Log Operations:

1. Select the appropriate event to be monitored. A single filter can monitor from any of the six standard event logs in Windows or any newly created event log on the machine.
2. Click Add to add a new Native Event Log operation. The following screen will open:

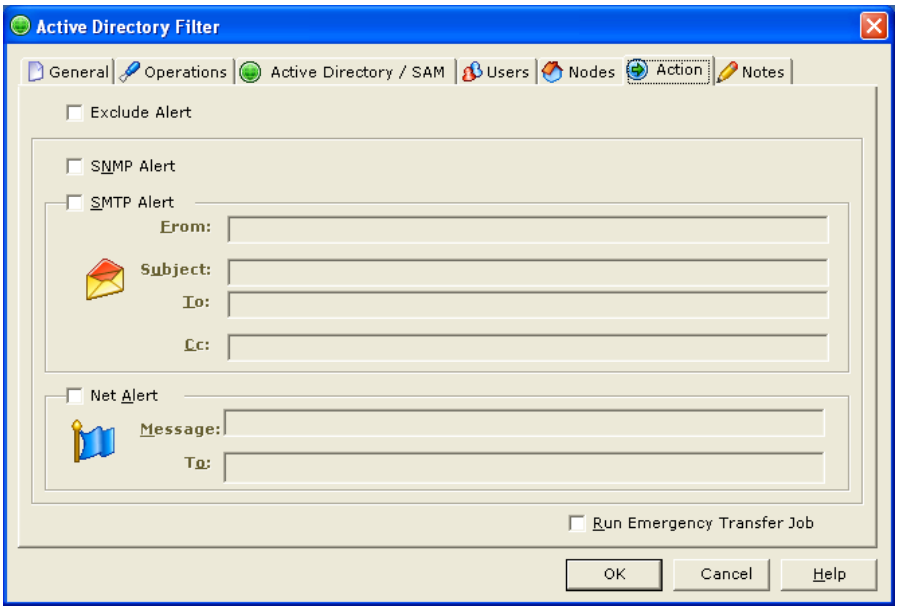


Each Native Event Log operation is made of the event log name, source name, category of the event and the actual event number.

Provide a description of the new event:

1. Select a Native Event Log type.
2. Select either All Source or provide the name of the source to be audited.
3. Select either All Categories or provide a name of the category to be audited.
4. Select either All Event IDs or provide the specific event ID to be audited.

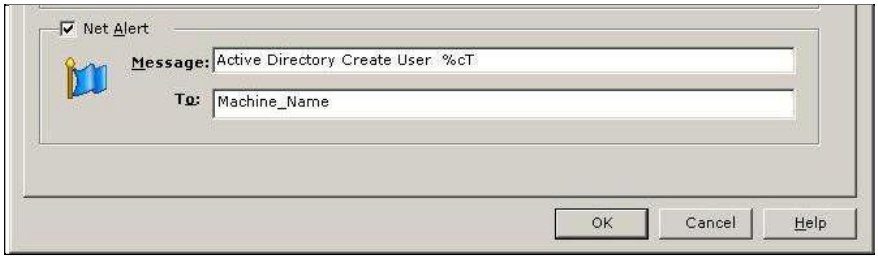
Action Settings



Each included filter statement can be configured to send out real-time alerts if the filter criteria are met in the form of SNMP messages, email alerts or regular Windows messages. By checking the Exclude Alert box, specific users can be excluded from receiving alerts for the same event, which is defined for all users.

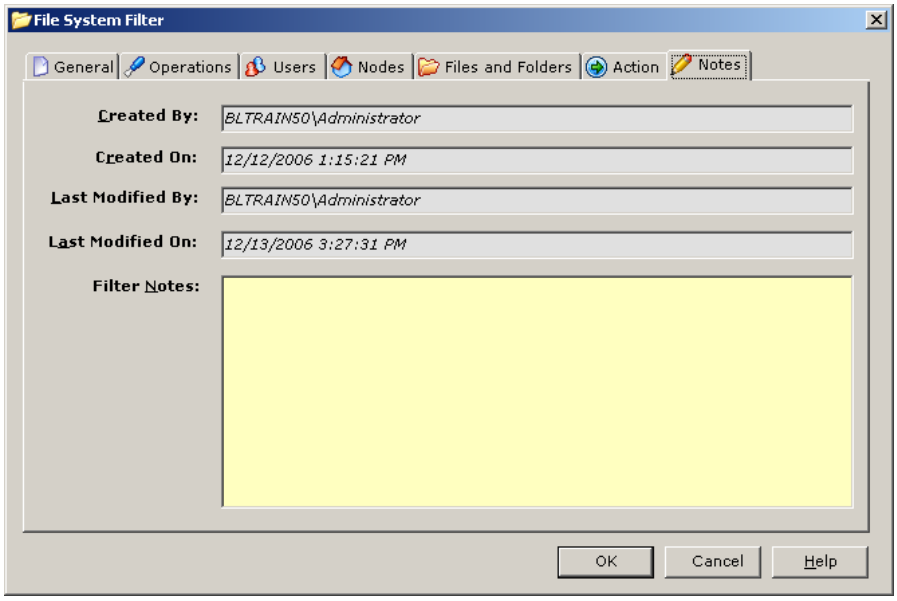
- To send SNMP messages, check SNMP Alert.
- To send email alerts, check SMTP Alert.

Provide the following information in the SMTP form: From, Subject (of the message), To and CC. The To and the CC lists of addresses should be separated by semicolons.



To send a Windows Messenger Alert, check Net Alert (Net Alert works only for Windows XP and Windows 2003).
Provide the following information in the Net Alert form: Message is customized text followed by **%cT** (see example above); To is the machine name or IP address the Net Alert should be sent to.

Notes



The program will automatically keep track of the filter creator, date, filter modifier and date it was modified. The Filter Notes field is provided for the user to track why the filter was created or modified.

Filter Settings Specific to a Subsystem

To create a new filter statement for a category specific to a subsystem (i.e., Active Directory/SAM, eDirectory), highlight your chosen auditing arm in the audit subsystem tree in the left pane of the Management Console, then select one of the following:

1. Click System → New → Filter Statement

   OR

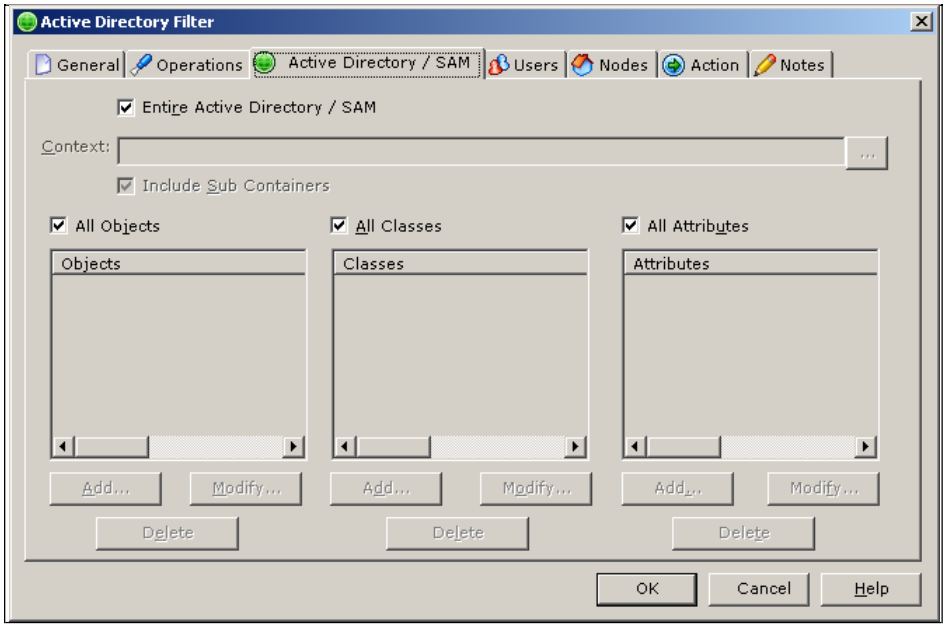
2. Click Filter Statement on the toolbar icon.

   OR

3. Right-click on the Active Directory Subsystem, and then click Filter Statement.

Select the tab specific to that subsystem and follow the instructions below to configure that setting.

Active Directory / SAM Settings – Active Directory Filter



Entire Active Directory / SAM:

To audit the entire active directory on a domain controller or to audit the local Windows accounts on a stand-alone machine, select Entire Active Directory / SAM.

Context: If the Entire Active Directory / SAM option is not checked, the context field will become active. Select the ellipsis **[…]** to browse for the container in the active directory forest that needs to be monitored.

Include Subcontainers: If this is selected, LT Auditor+ will monitor the container specified in the context field and all the subcontainers within it. To monitor only the container specified, but not the subcontainers, uncheck this option.

Objects:

1. To audit all objects, select All Objects.
2. To audit specific objects, uncheck All Objects.
3. Click Add.
4. Provide description of the object(s) to be audited. Utilizing a wildcard '*' will specify any part of the object name. For example, **cn=john*** will audit any object containing the string **cn=john**.
5. Click OK.

To modify the object:

1. Highlight the object in the list.
2. Click Modify.
3. Edit the object data. Click OK.

To delete the object:

1. Highlight the object in the list.
2. Click Delete. The system will ask you for confirmation.

3. Click Yes.

Classes:

To audit all classes:

1. Select All Classes.
2. To audit specific classes within the active directory, uncheck All Classes.
3. Click Add.
4. Provide the description of the class to be audited. A wildcard '*' can be used.
5. Click OK.

To modify the class:

1. Highlight the class in the list.
2. Click Modify.
3. Edit the class data.
4. Click OK.

To delete the class:

1. Highlight the class in the list.
2. Click Delete. The system will ask you for confirmation.
3. Click Yes.

Attributes:

To audit all attributes:

1. Select All Attributes.
2. Uncheck All Attributes to audit specific attributes within the active directory.
3. Click Add.
4. Provide the description of the attribute(s) to be audited. A wildcard '*' can be used.
5. Click OK.

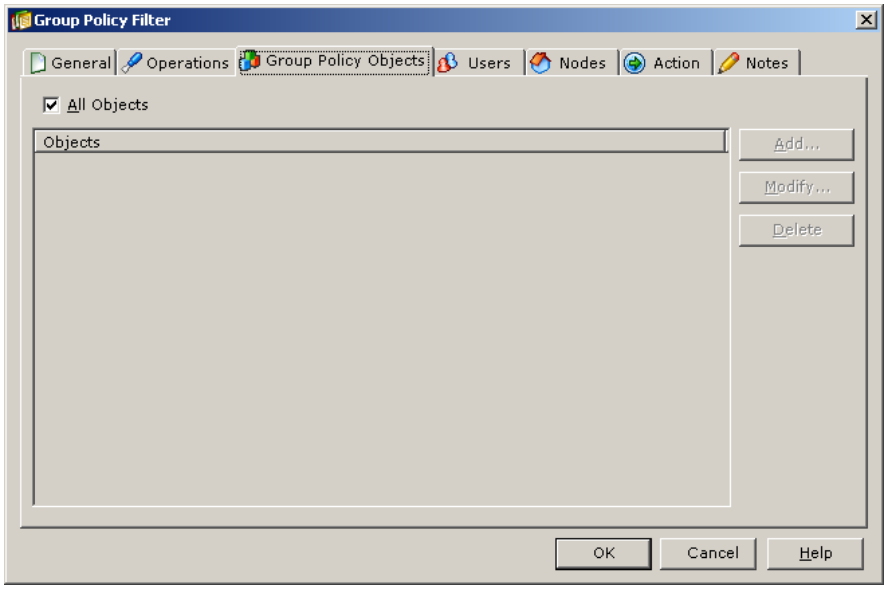
To modify the attribute:

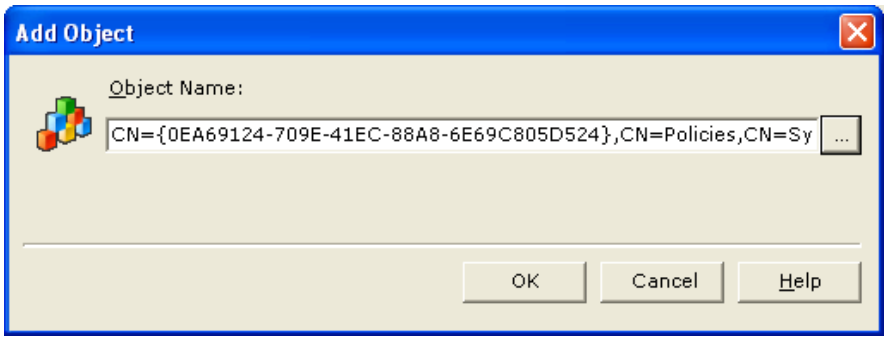
1. Highlight the attribute in the list, click Modify.
2. Edit the attribute data.
3. Click OK.

To delete the attribute:

1. Highlight the attribute in the list.
2. Click Delete when prompted for confirmation.
3. Click Yes.

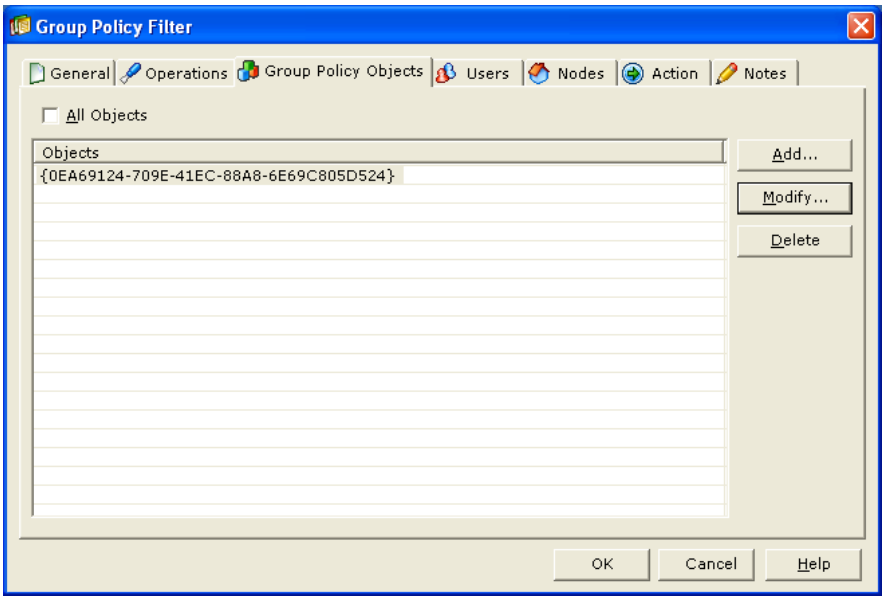
Group Policy Objects Settings – Group Policy Filter





All Objects:

1. To audit all the Group Policy objects within the Active Directory, select All Objects.
2. To audit specific Group Policy objects within the Active Directory, uncheck All Objects.
3. Click Add.
4. Browse through the Active Directory to locate Group Policy objects within the Active Directory.
5. Click OK.



To modify Group Policy Objects:

1. Highlight the object.
2. Click Modify.

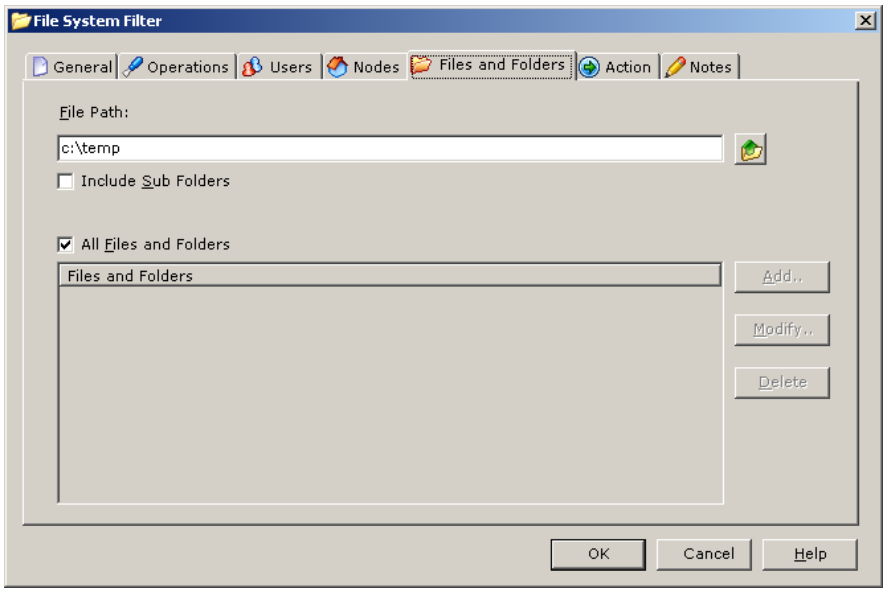
To edit the Group Policy Object data:

1. Highlight the object.
2. Click OK.

To delete Group Policy Objects:

1. Highlight the object.
2. Click Delete.
3. The system will ask you for confirmation. Click Yes.

File / Folders Settings – File System Filter



File Path: Select the file system folder path to be monitored.

Include Sub Folder: To include all subfolders, select Include Sub Folders. To monitor only the folders specified, but not the subfolders, uncheck this option.

Files and Folders:

To audit all files and folders within the specified file path:

1. Check All Files and Folders.
2. To audit specific files or folders from the file path, select Add.
3. Provide the complete addresses of the files or folders to be audited.

NOTE

A wildcard (*) may be used

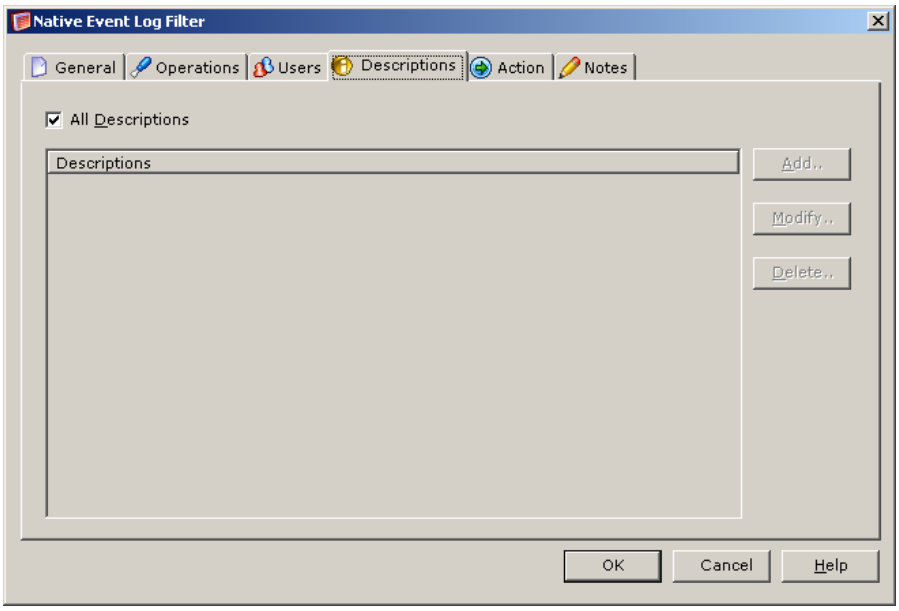
To modify a file or folder:

1. Highlight the file or folder.
2. Click Modify.
3. Change the file or folder data.
4. Click OK.

To delete a file or folder:

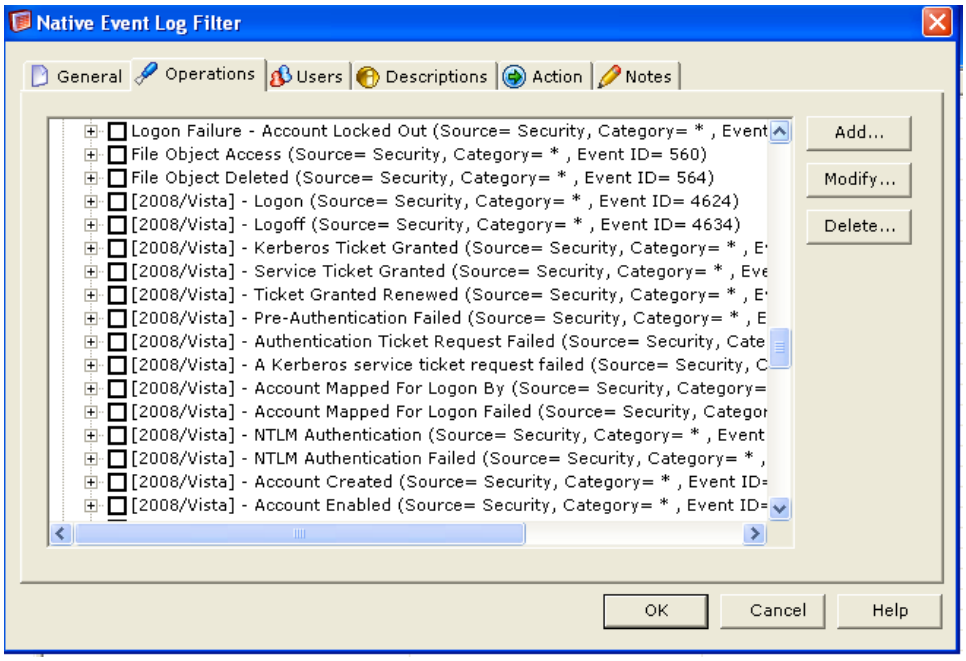
1. Highlight the file or folder.
2. Click Delete.
3. The system will ask you for confirmation.
4. Click Yes.

Description Settings – Native Event Log Filter



Operation Settings – Native Event Log

1. Select All Operations to audit all subsystem operations.
2. To select specific operations of interest, uncheck All Operations.
3. Select the appropriate operation(s) to audit.



All Descriptions

To monitor all the description strings from the event log:

1. Select All Descriptions.

To monitor specific events from the event log with certain description strings in them:

1. Uncheck All Descriptions.
2. Click Add.
3. Provide the description strings.
4. Click OK.

NOTE

A wildcard (*) may be used. For example, if you wanted to audit all failed applications, you would type failed applications *.

To modify a description:

1. Highlight the description.
2. Click Modify.
3. Change the description data.
4. Click OK.

To delete a description:

1. Highlight the description.
2. Click Delete.
3. The system will ask you for confirmation.
4. Click Yes.

Chapter 4 – Configuring Manager and Agent Jobs

This section will provide detailed steps to show you how to use the LT Auditor+ Management Console to configure the agents to send data over to the manager, and to configure the manager to consolidate the data into the database.

Manager Data Rollup Job

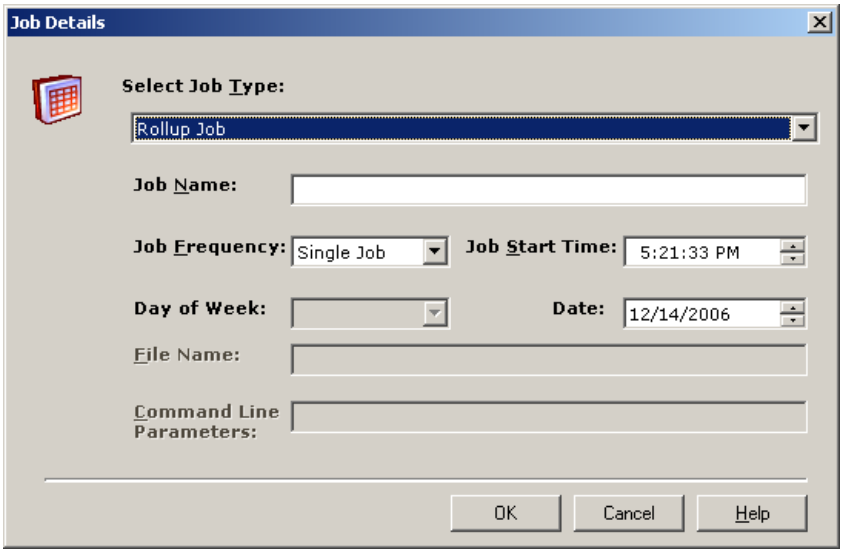
In addition to automated rollup settings described in the section Modified Group Settings, rollup jobs can be scheduled to transfer audit data to the LT Auditor+ database. Each manager can be configured to perform multiple data rollup jobs, scheduled to run at a specific time and frequency.

To create a new data rollup job:

1. Click Data Rollup node in a Windows Manager Group.
2. Select one of the following:

    - Click System → New → Job.

- Click Job on the toolbar.
- Right-click on Data Rollup and click Job.



Job Name: Provide the description of the job.

Job Frequency: Provide how often to run the job. Selection options are single, daily or weekly.

Job Start Time: Specify the time to start the job.

To set up a custom job:

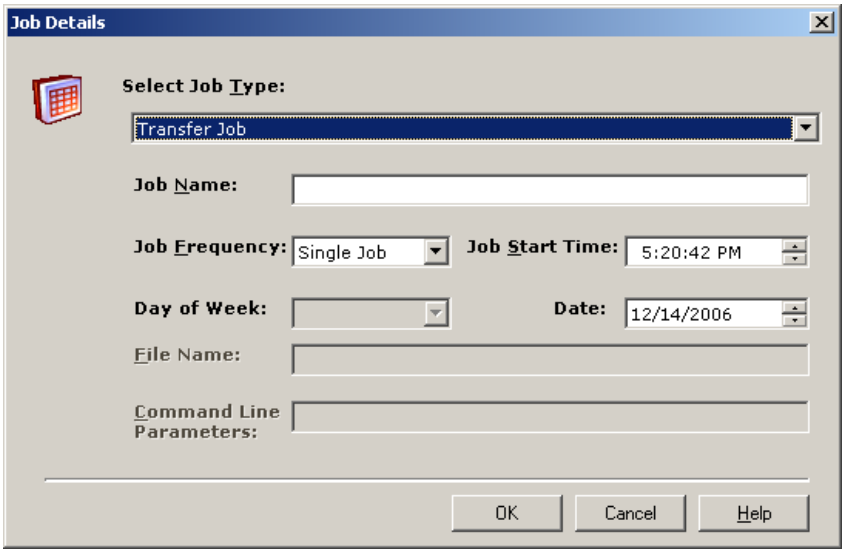
1. Select Custom from the drop-down menu.
2. Select options to suit needs as necessary.

Agent Data Transfer Job

In addition to automated transfer settings described in the section Agent Group Setting, jobs can be configured to transfer audit data to the manager. Each agent group can be configured to perform multiple data transfer jobs, scheduled to run at a specific time and frequency.

To create a new Data Transfer Job:

1. Click Data Transfer node in a Windows agent group.
2. Select one of the following:
   - Click System → New → Job.
   - Click Job on the toolbar.
   - Right-click on Data Transfer.
   - Click Job.



Job Name: Provide the description of the job.

Job Frequency: Provide how often to run the job. Selection options are single, daily or weekly.

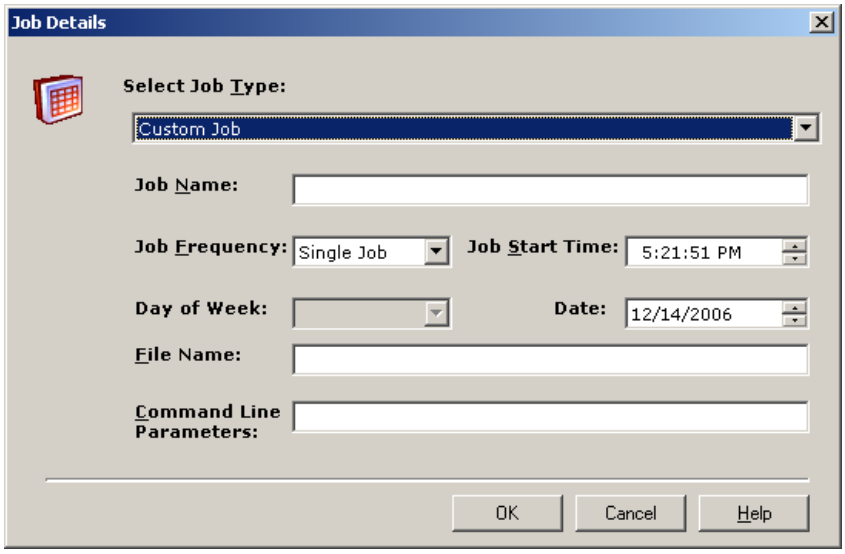
Job Start Time: Specify the time to start the job.

Custom Job

Custom jobs can be set up to perform unique tasks like transferring miscellaneous files to the manager.

To create a new Custom Data Transfer Job:

1. Click Data Transfer node in a Windows agent group.
2. Select one of the following:
   - Click System → New →Custom Job.
   - Click Custom Job on the toolbar.
   - Right-click on Data Transfer. Click Custom Job.



Job Name: Provide the description of the job.

Job Frequency: Determine how often to run the job. Selection options are single, daily or weekly.
Job Start Time: Specify the time to start the job.
File Name: Provide the complete application name, i.e., **C:\directory\filename**.
Command line: Provide the required parameters for the application.

NOTE

Run custom jobs under service privileges. Custom jobs should not require user input and should exit after completing the task.

Chapter 4 – Configure the LT Auditor+ Report Console

This section will provide detailed steps to show you how to use LT Auditor+ Report Console to create report queries and run reports on the consolidated data collected in the workspace.

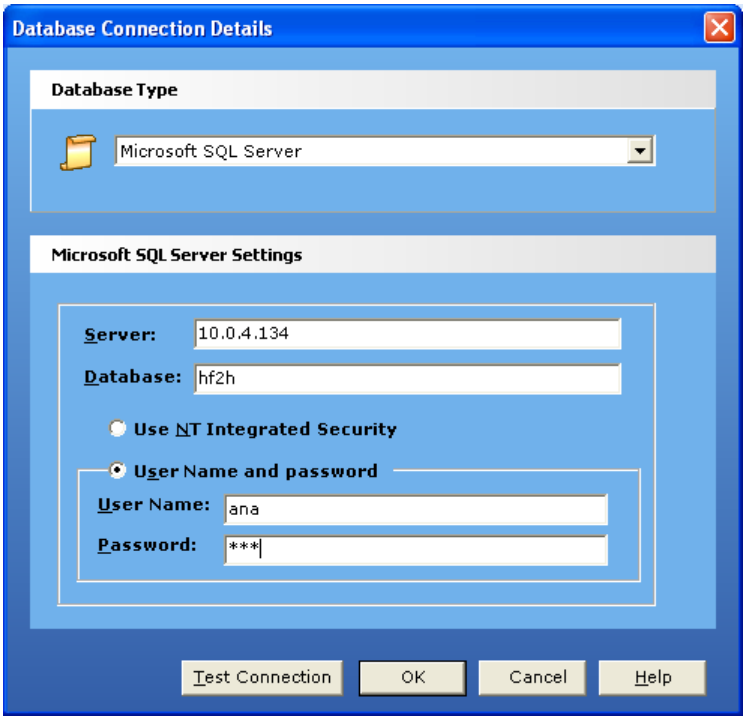
NOTE

To access the Report Console, you must first be certain to be authenticated to the workspace with which you want to work.

Starting the Report Console

1. Click Start → All Programs → Blue Lance, Inc → Reporting Console**.** The following screen gets displayed.
2. It will prompt you for the database connection information.

For SQL (Report Console):



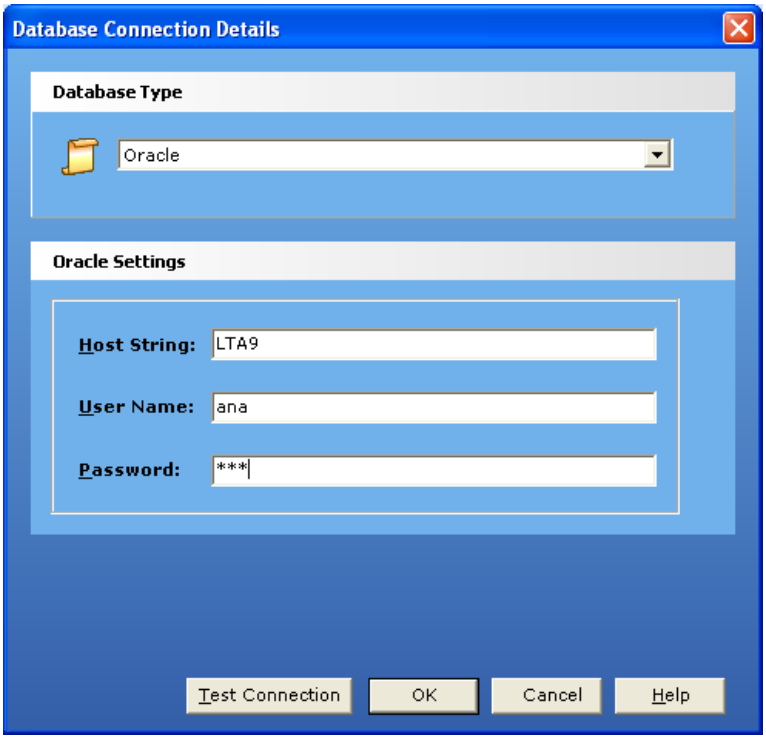
Select Microsoft SQL Server for Database Type.

1. Provide server ID.
2. Provide database name.
3. Select Use NT Integrated Security OR User Name and Password.
4. If User Name and Password is selected, provide the username and the password.
5. Click OK.

For Oracle (Report Console):

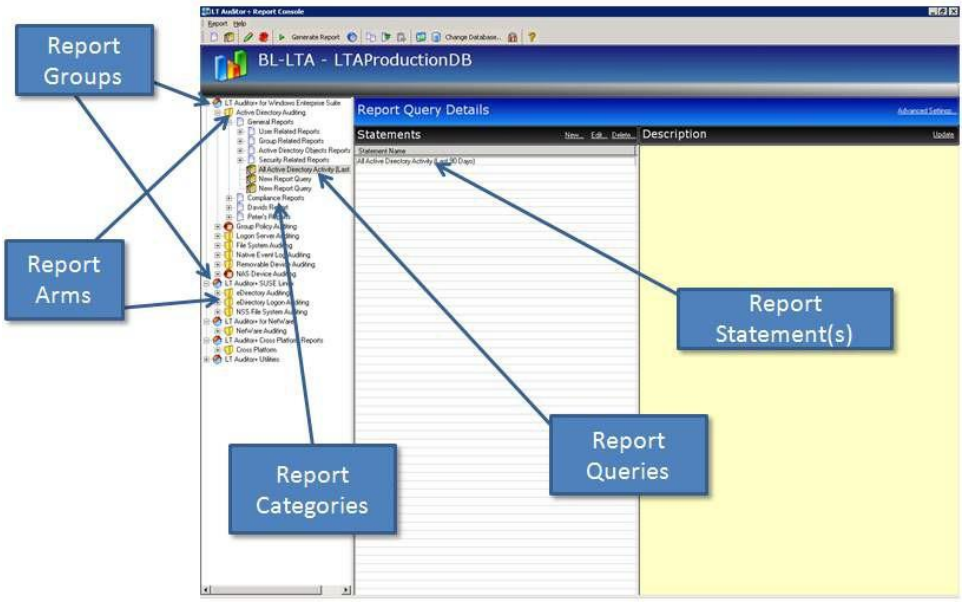
NOTE

Oracle client tools are needed to connect to the database using the Report Console.



1. Select Oracle for database type.
2. Provide host string.
3. Provide username.
4. Provide password.
5. Click OK.

The Report Console will be launched as soon as you are authenticated to the workspace. The Report Console screen is shown in the following screen:



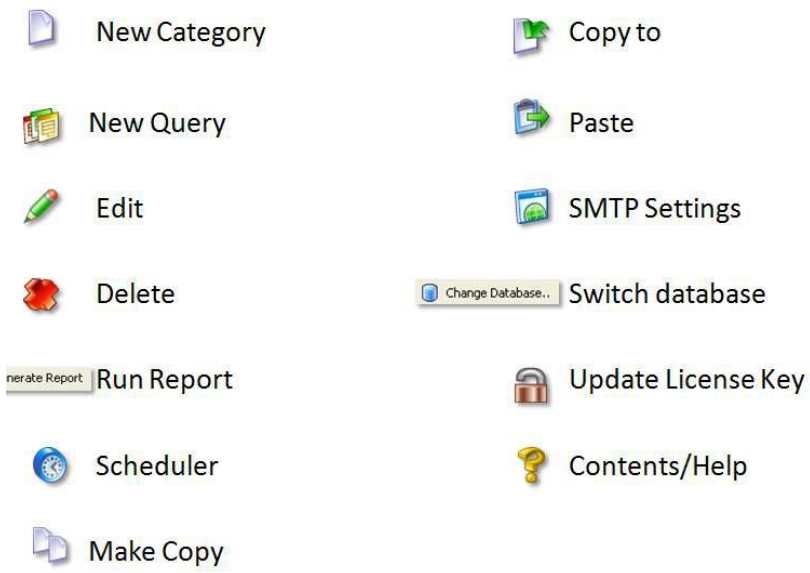
The Report Console is divided into two views:

- The left pane shows all the report groups available for reporting.
- The right pane provides detailed information about each selected entity on the left.

Each reporting group has report arms that relate to Blue Lance products or tools. Reporting arms can have multiple report categories within them. Each report category can further have subcategories or actual report queries within them. Each report query is made up of one or more report query statements.

Report Icons

The icons used in the LT Auditor+ Report Console are listed below:



Report Groups and Report Arms

The following table lists report groups and report arms available with LT Auditor+.

Report Group	Report Arms	Description
LT Auditor+ for Window Enterprise Suite	Active Directory Auditing	Reports for Active Directory Changes.
	Group Policy Auditing	Report for Group Policy changes.
	Logon Server Auditing	Reports for authentications.
	File System Auditing	Reports for access to files and Folders.
	Native Event Log Auditing	Reports on Windows event logs.
	Removable Media Auditing	Reports on access to flash drives and other removable media.
	NAS Devices Auditing	Reports for access on devices like NetApp and EMC Isilon.
LT Auditor+ Windows Assessment	Windows Assessment	Reports for Active Directory Users, Groups, OUs, Computers, Object permissions (ACLs) and File/Folder permissions.
LT Auditor+ for SUSE Linux	eDirectory Auditing	Report on eDirectory changes.
	eDirectory Logon Auditing	Reports on authentications to eDirectory.
	NSS File System Auditing	Reports on access to NSS file systems on SUSE Linux systems.
LT Auditor+ for Syslog Devices	Syslog Device Auditing	Reports on data received from Syslog-enabled devices using LT

		Auditor+ Syslog Server.
LT Auditor+ Compliance Reports	Compliance Reports	Mappings to FFIEC, PCI-DSS, HIPAA, NIST and SOX .
LT Auditor+ Cross Platform Reports	Cross Platform Reports	Reports that can be consolidated across any of the report arms.

LT Auditor+ Utilities	Audit the Auditor	Reports on configuration and status changes made within LT Auditor+.
	Rollup Status Monitoring	Reports on status of audit data inserted into the LT Auditor+ Database.

Report Categories

Report Categories hosts groups of report queries that allow users the option to group similar queries under a single category for ease of access and use.

Create a new report category:

1. Highlight the appropriate report arm:

   - Click Report → New Report Category
     OR
   - Click New Report Category on the toolbar.

2. Provide a name for the report category.
3. Press Enter.

Modify a report category:

Select the report category and one of the following:

- Click Report, click Edit
  OR
- Click Edit on the toolbar.

Delete a report category:

1. Select the report category and one of the following:
   - Click Report, click Delete
     OR
   - Click Delete on the toolbar.
2. The system will ask you for confirmation.
3. Click Yes.

Creating a Report Query

Report queries determine how data is retrieved from the database for reporting. Every report query is comprised of one or more query statements. The following steps outline how to create a report query with one report query statement.

1. Select the report arm category in the left pane of the Report Console.
2. Select one of the following:

    - Highlight the report category.
    - Click on the Create Report Query icon.

A new report query is made up of one or more report query statements. A report statement is created when creating a report query. Each query can be configured in terms of desired output, format of report and additional parameters by selecting Advanced Setting, which will be discussed later in this session.

Report Statements

A report query statement contains a set of parameters that specifies how data is retrieved from the database on executing the query. A statement is comprised of multiple tabs that allow users to define the database query.

There are common tabs for all report arms as well as tabs specific to each arm.

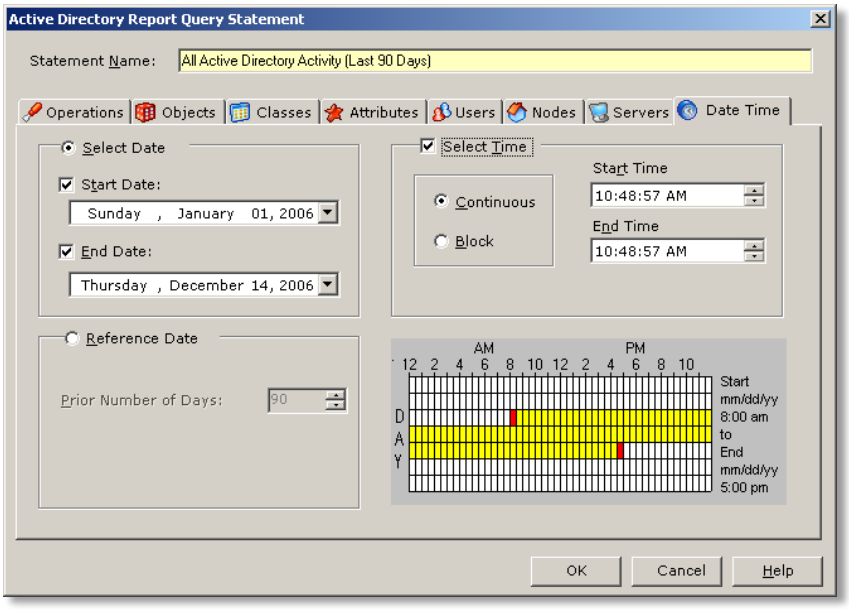
Common Report Statement Tabs for All Report Arms

The common tabs on report statements for all report arms are:

- Date &Time
- Users
- Nodes
- Servers
- Operations – Though this tab is common, its content varies for each report arm. We will discuss the Operations tab for each report arm in the "Specific Tabs" section.

Date & Time

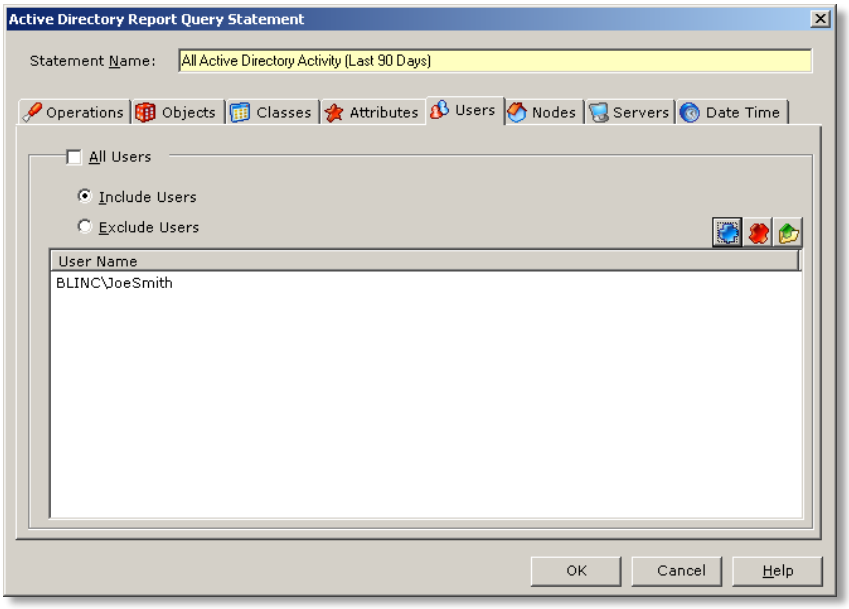
This tab is used to specify date range for retrieval of data.



- **Select Date** – runs reports between a start date and an end date.
- **Reference Date** – runs reports from prior days up to present date
- **Select Time** – runs reports for a specific time.
- **Continuous Time** – This option reports activity from the start date and start time to the end date and end time.
- **Block of Time** – This option reports activity from the start date to the end date and all operations that fall within the specified start time and end time.

Users

Specifies what users are to be reported on.



Wild card characters are accepted. For example, to report on all users that contain the words admin, type in *admin*.

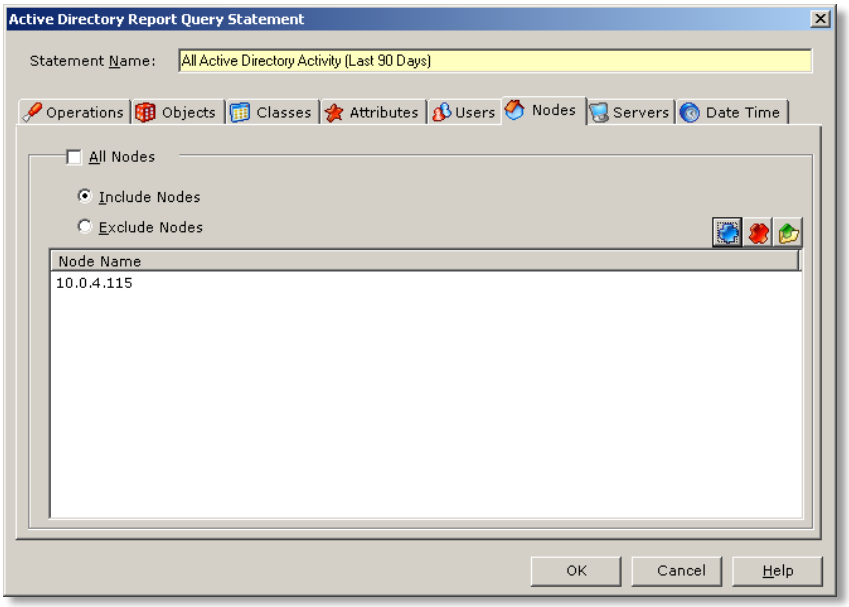
NOTE

Actions common for all tabs

- Include/Exclude selection criteria.
  - All query statement tabs, with the exception of the Date & Time tab, provide the choice of including or excluding the selection criteria specified in that tab.
  - Selecting Include will produce reports containing criteria selected in the tabs.
  - Selecting Exclude will produce reports containing all audited data except those items selected in the tabs.
  - Wild card characters are accepted.
- Adding , Deleting , and Browsing within tabs
  - In most tabs, when selecting specific items rather than all items for reporting, you may use the Add, Delete, and Browse icons to modify the items for which you would like to report.

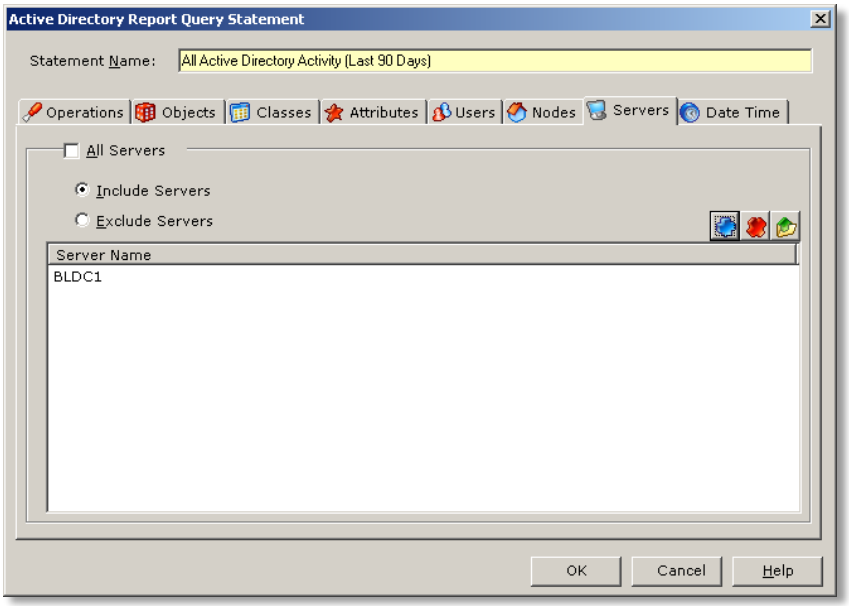
Nodes

Specifies what nodes are to be reported on.



Servers

Specifies what servers are to be reported on.

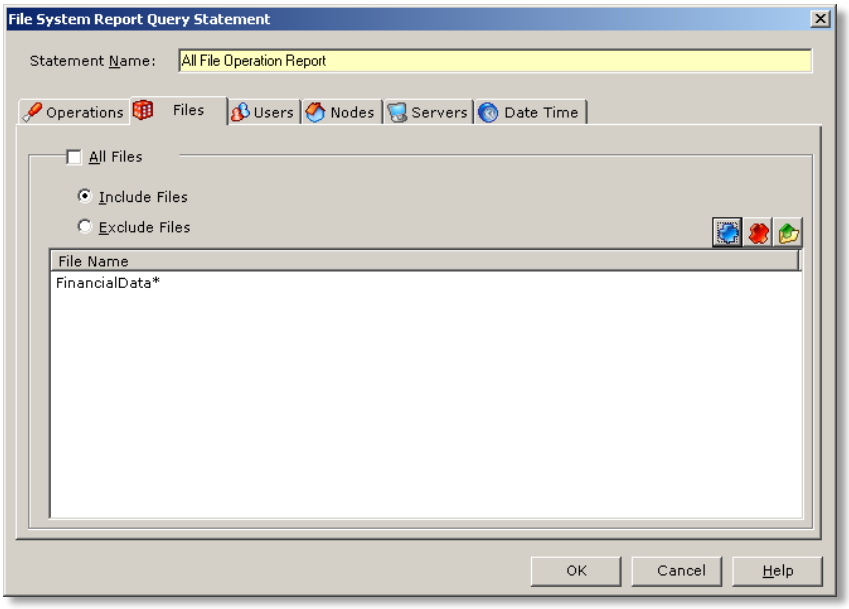


Report Statement Tabs for File System, Removable Devices, NAS Devices and NSS File Systems Report Arms

For these report arms, the following tabs are applicable for enhanced querying.

Files

Specifies what files and folders are to be reported on.

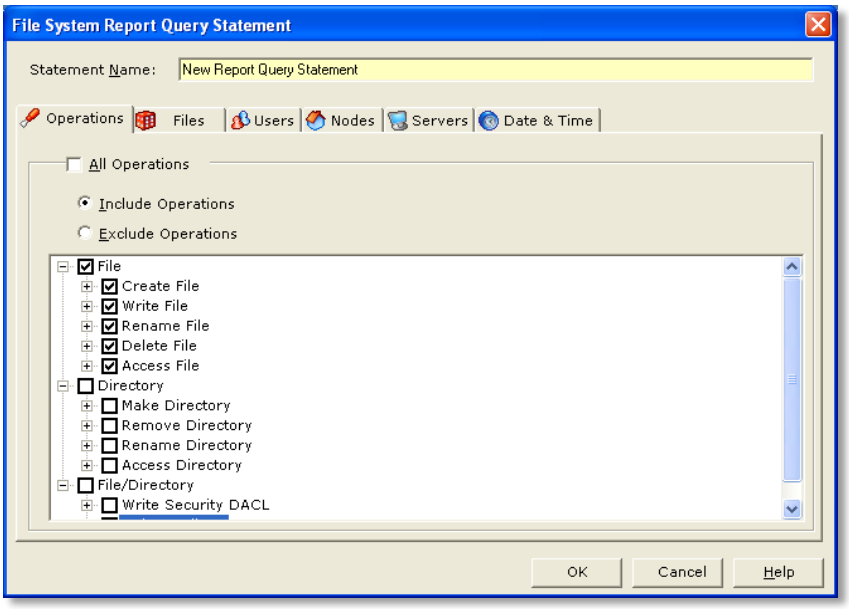


Example:

- Including ***.xlsx** will report on all files with the .xlsx extension.
- Excluding ***.tmp** will report on all files except files with the extension of .tmp

Operations

Species file operations to query for in the report.



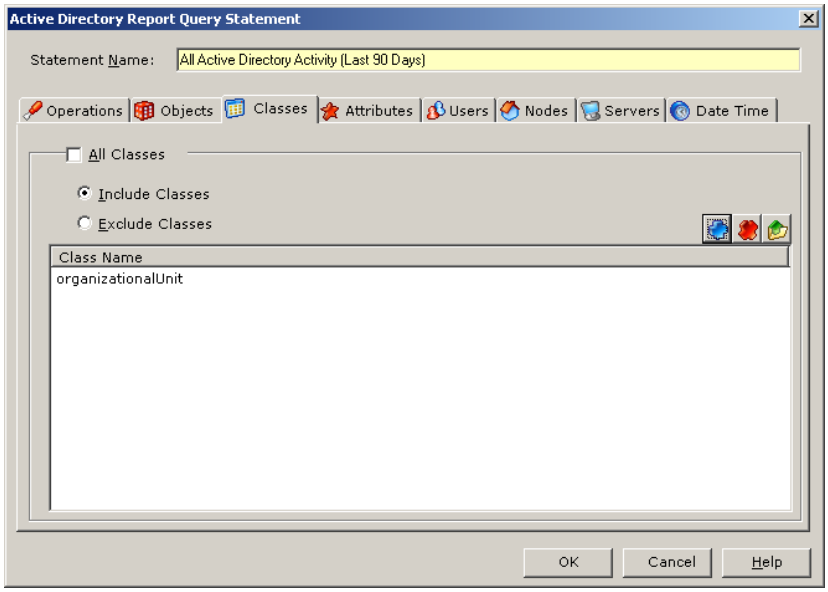
Operations are grouped into the following sections:

- File Operations – Create, Write, Rename, Delete and Access
- Directory Operations – Make, Remove, Rename and Access
- File & Directory Operations – Write Security DACL/Write Attribute

Report Statement Tabs for the Active Directory, eDirectory and NetWare Report Arms

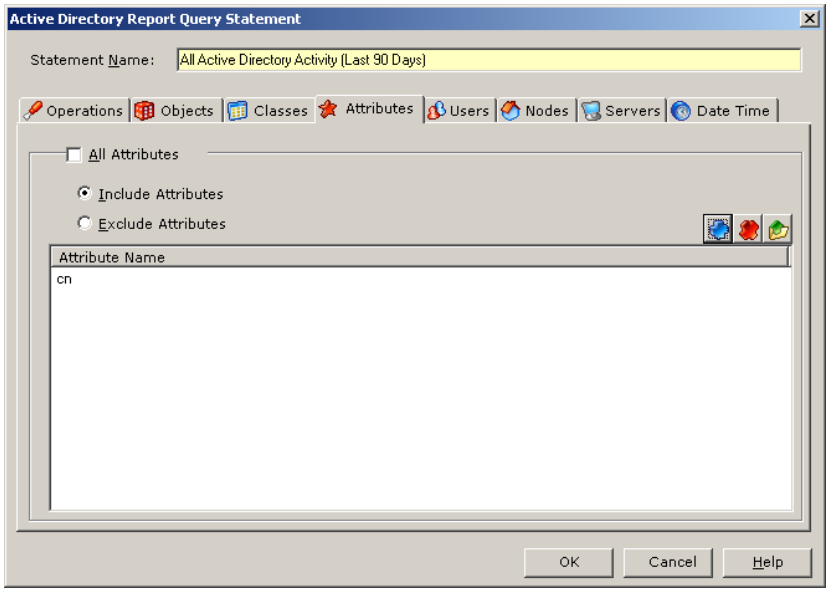
Classes

Classes are a group of objects defined by a certain set of attributes. Classes can include users, groups, organizational units, computers and any others defined in the Active Directory/eDirectory environment. Select the classes to report on in this tab.



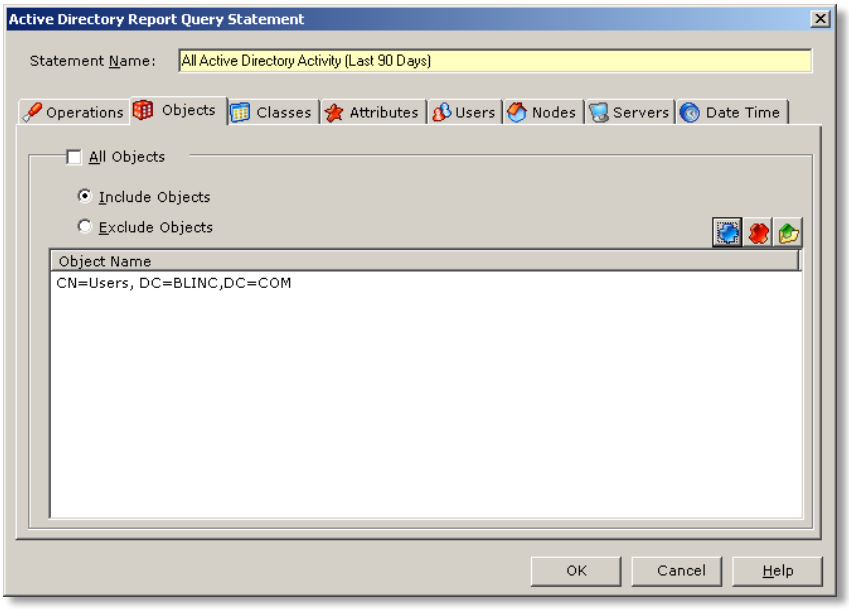
Attributes

Attributes are any properties that define an object. Report on specific attributes like DACL, description and surname. Reports can also be generated on values given to attributes.



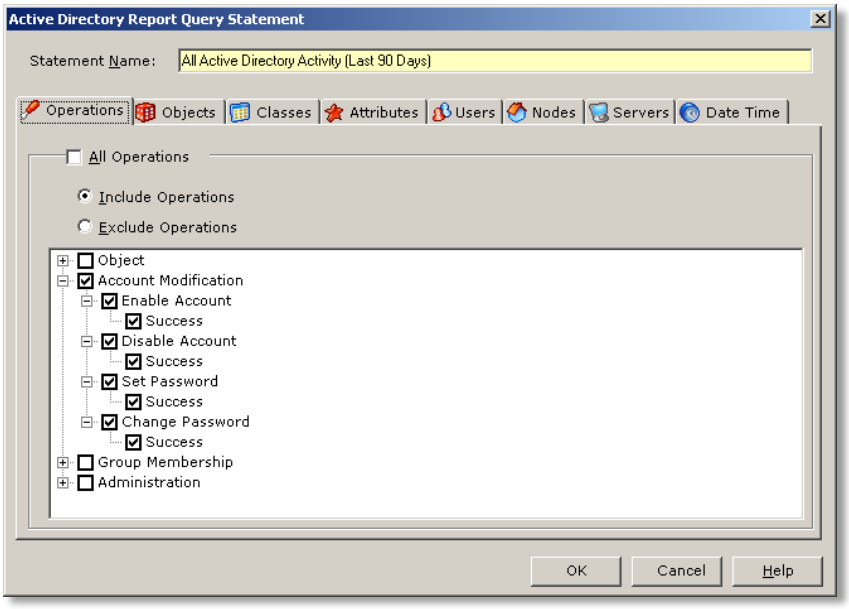
Objects

Objects are entities in the directory. Specific objects to report on are in this tab.



Operations

The operations available for reporting in a Directory query are actions related to changes in objects, accounts, group membership and administration.

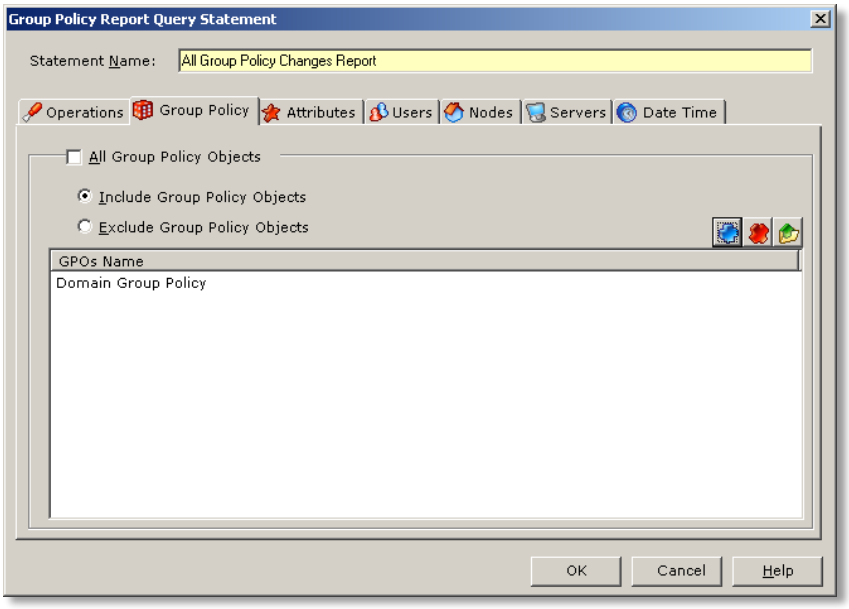


The operations available for reporting include object creation, modification, and deletion; account modification; changes in group membership; password changes and changes in administration.

Report Statement Tab for the Group Policy Report Arm

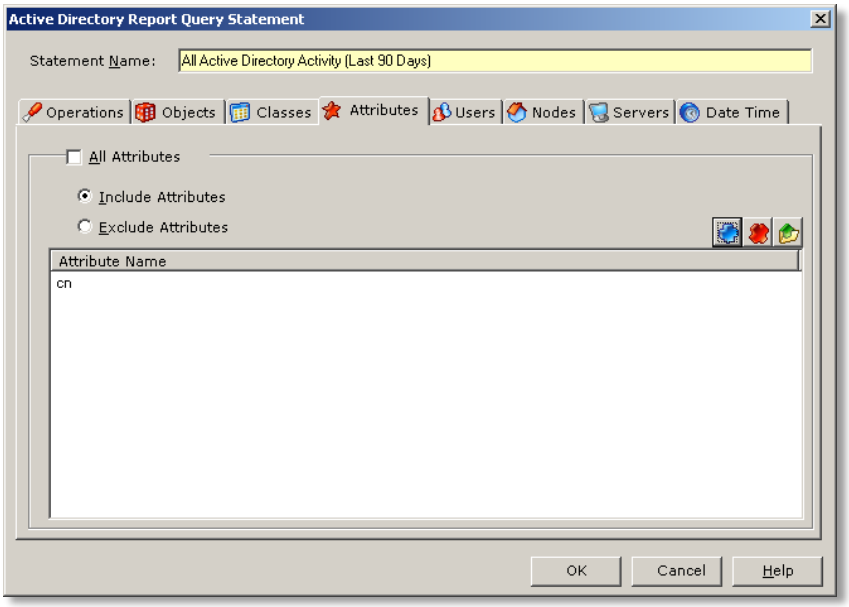
Objects

In Group Policy, a group policy object is a container where policy settings are stored.



Attributes

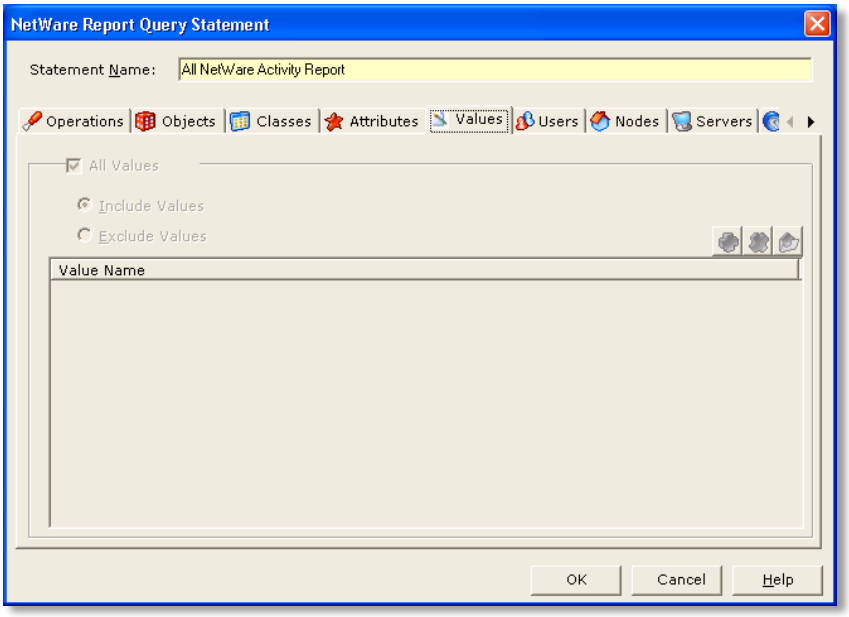
Attributes are properties that define the group policy and LT Auditor+ allows for granular reporting.



Report Statement Tab for the NetWare Report Arm

Values

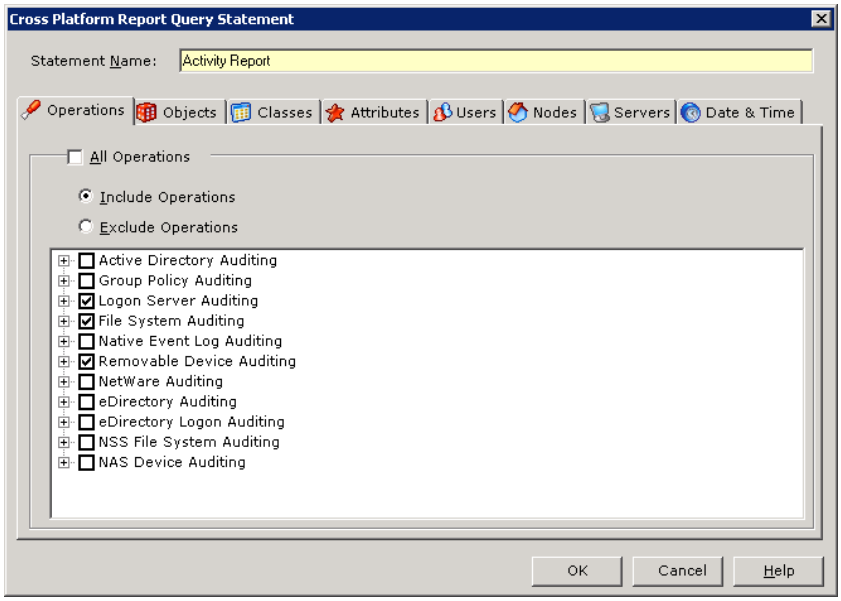
Values assigned to attributes can be queried for in this tab.



Report Statement Tab for the Cross-platform Report Arm

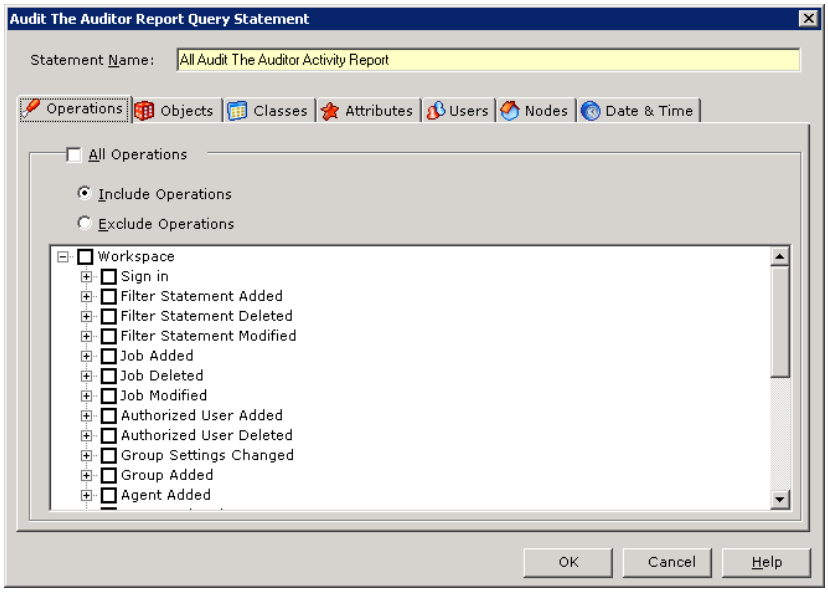
The cross-platform reports allow users to report consolidated information across all report arms. For example, if a single report of Active Directory, eDirectory and NetWare activity was required, one can do so with cross-platform reports. Another example would be a query for a particular user's entire activity across everything, audited with LT Auditor+.

A cross-platform report statement contains a combination of all tabs discussed above as shown below.



Report Statement Tab for the Audit the Auditor Report Arm

Audit the Auditor reports display information on modifications made to configurations and policies within LT Auditor+. It is important to audit the activity of LT Auditor+ administrators. The screen below displays the standard tabs available for querying.

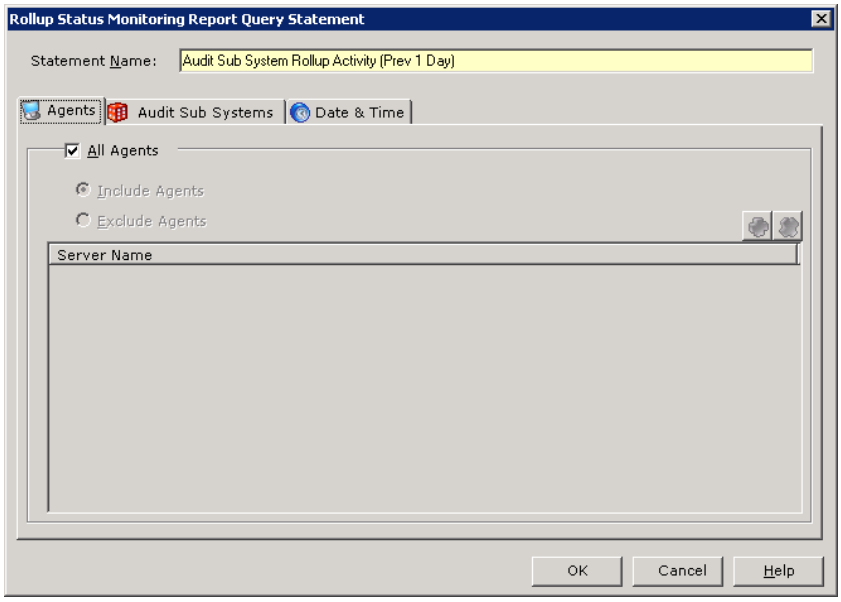


Report Statement Tab for the Rollup Status Monitoring Report Arm

The rollup status monitoring reports provide information on the status of data inserted into the LT Auditor+ database. Users can get information such as:

- How many records were inserted per agent.
- How many agents did not send data.
- Patterns for volume of audit data collected over time.

The following screen displays tabs available to query for rollup information.



Advanced Settings

The Advanced Settings option in the Report Console allows users the following options:

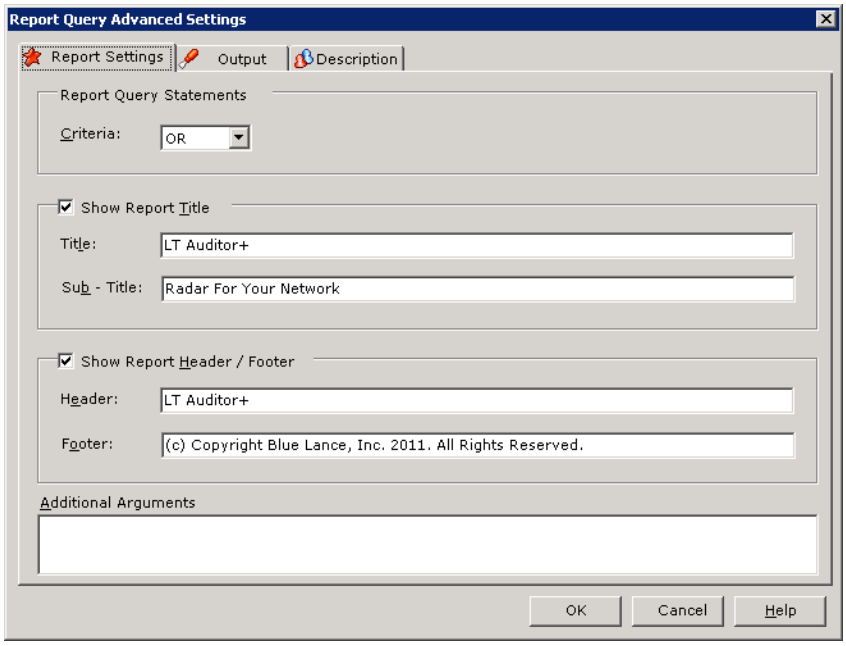
- Choose the report output type (email, send to printer, etc.).
- Choose the type of report (chronological columnar, etc.).
- Determine whether multiple statements will be linked by "AND" or "OR."
- Give the report a description.

To access Advanced Settings:

1. Select the report query statement.
2. Click Advanced Settings in the top right pane.

The Advanced Settings window has multiple tabs discussed below.

Report Settings



Criteria – Used when combining multiple query statements within a query, they may be linked by either the logical phrase "AND" or the logical phrase " OR."

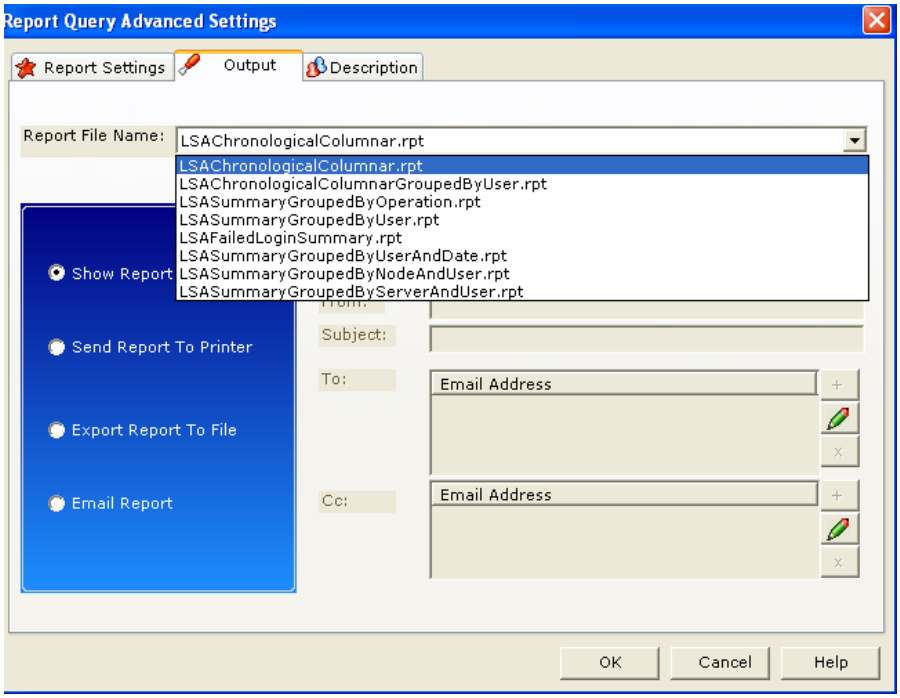
- AND – Using the phrase AND to link query statements will return only the data that applies to the parameters of all statements.
- OR – Using the phrase OR to link query statements will return data that applies to the parameters of any statement in a query, not necessarily all statements.

Show Report Title and Subtitle – In this field you may choose to show, hide or change the report's title and subtitle.

Show Report Header and Footer – In this field you may choose to show, hide or change the report's header and footer.

Additional Arguments – This field is used to write in additional information necessary to run specific types of reports.

Output – Under the Output tab, you will be able to select how you would like to organize the report and where you would like it to be viewed.



You may have it shown on screen, sent to a printer, exported to a file or sent in an email. If you choose to send the report in an email, you may enter the email settings as desired in the right portion of this window. You must give the report a file name and format when sending it to a file or via email.

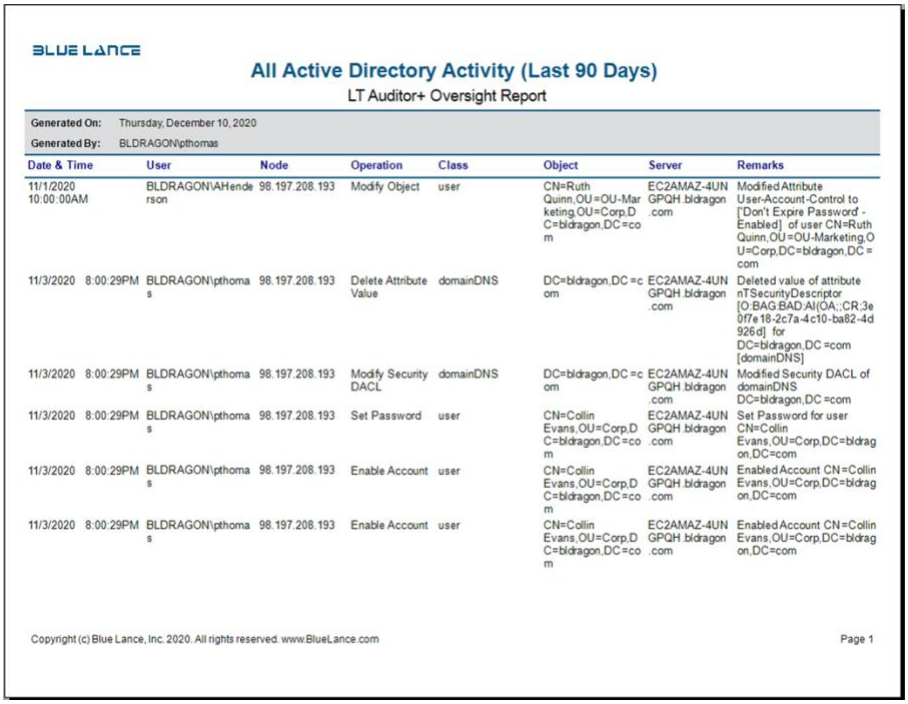
NOTE

Choosing to show the report on screen will prevent you from being able to schedule the report, so it should only be used when generating a single report.

Selection of a Report File Name determines the format of the report. There are multiple report formats defined based on the report arm selected. Some are displayed below:

Chronological Columnar

This report output type is the default setting for most reports generated. It is viewed in columns of text with the data listed from least to most recent.



BLUE LANCE

All Active Directory Activity (Last 90 Days)

LT Auditor+ Oversight Report

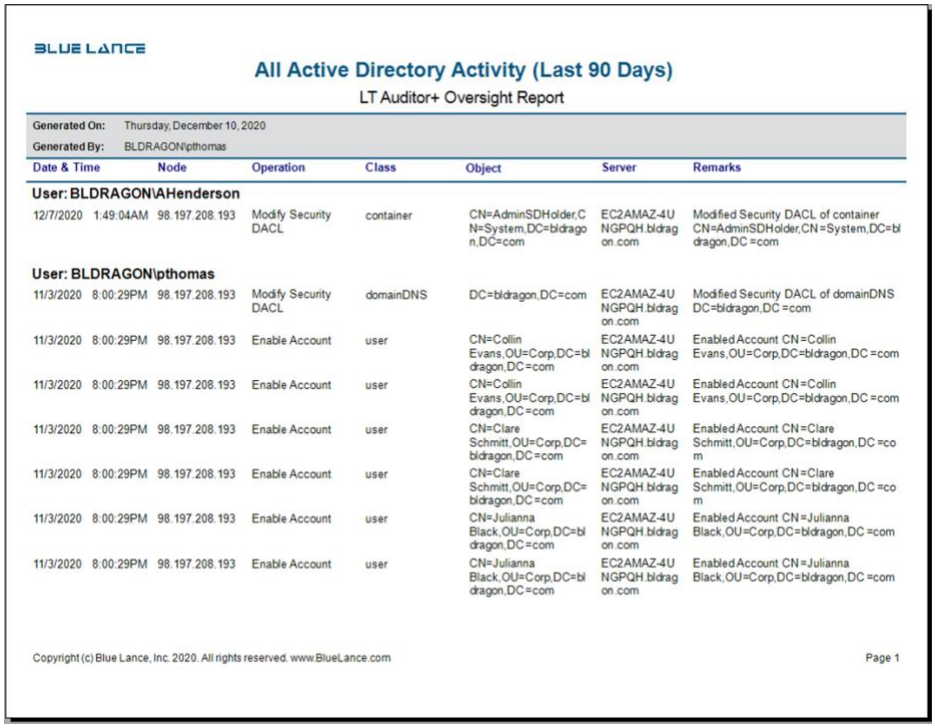
Generated On: Thursday, December 10, 2020
Generated By: BLDRAGON\pthomas

Date & Time	User	Node	Operation	Class	Object	Server	Remarks
11/1/2020 10:00:00AM	BLDRAGON\AHenderson	98.197.208.193	Modify Object	user	CN=Ruth Quinn,OU=OU-Marketing,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Modified Attribute User-Account-Control to ['Don't Expire Password' - Enabled] of user CN=Ruth Quinn,OU=OU-Marketing,OU=Corp,DC=bldragon,DC=com
11/3/2020 8:00:29PM	BLDRAGON\pthomas	98.197.208.193	Delete Attribute Value	domainDNS	DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Deleted value of attribute nTSecurityDescriptor [O:BAG:BAD:AI(OA;;CR;3e0f7e18-2c7a-4c10-ba82-4d926d] for DC=bldragon,DC=com [domainDNS]
11/3/2020 8:00:29PM	BLDRAGON\pthomas	98.197.208.193	Modify Security DACL	domainDNS	DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Modified Security DACL of domainDNS DC=bldragon,DC=com
11/3/2020 8:00:29PM	BLDRAGON\pthomas	98.197.208.193	Set Password	user	CN=Collin Evans,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Set Password for user CN=Collin Evans,OU=Corp,DC=bldragon,DC=com
11/3/2020 8:00:29PM	BLDRAGON\pthomas	98.197.208.193	Enable Account	user	CN=Collin Evans,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Enabled Account CN=Collin Evans,OU=Corp,DC=bldragon,DC=com
11/3/2020 8:00:29PM	BLDRAGON\pthomas	98.197.208.193	Enable Account	user	CN=Collin Evans,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Enabled Account CN=Collin Evans,OU=Corp,DC=bldragon,DC=com

Copyright (c) Blue Lance, Inc. 2020. All rights reserved. www.BlueLance.com Page 1

Chronological Columnar Grouped by User

This report output type is similar to the one prior, but data is grouped by user. It is then listed in chronological form from least to most recent data within each user's group of data.



BLUE LANCE

All Active Directory Activity (Last 90 Days)

LT Auditor+ Oversight Report

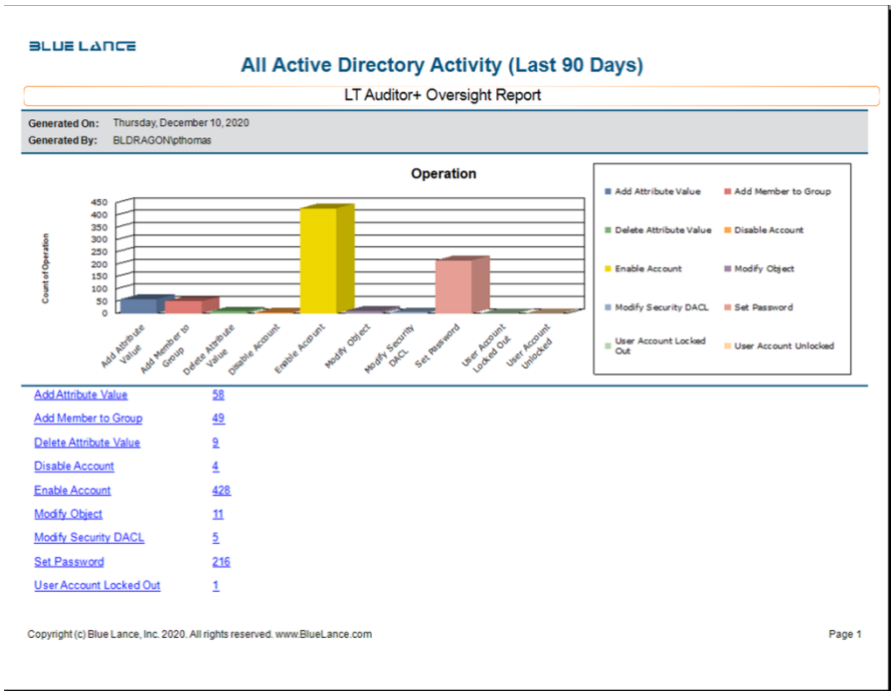
Generated On: Thursday, December 10, 2020
Generated By: BLDRAGON\pthomas

Date & Time	Node	Operation	Class	Object	Server	Remarks
User: BLDRAGON\AHenderson						
12/7/2020 1:49:04AM	98.197.208.193	Modify Security DACL	container	CN=AdminSDHolder,CN=System,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Modified Security DACL of container CN=AdminSDHolder,CN=System,DC=bldragon,DC=com
User: BLDRAGON\pthomas						
11/3/2020 8:00:29PM	98.197.208.193	Modify Security DACL	domainDNS	DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Modified Security DACL of domainDNS DC=bldragon,DC=com
11/3/2020 8:00:29PM	98.197.208.193	Enable Account	user	CN=Collin Evans,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Enabled Account CN=Collin Evans,OU=Corp,DC=bldragon,DC=com
11/3/2020 8:00:29PM	98.197.208.193	Enable Account	user	CN=Collin Evans,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Enabled Account CN=Collin Evans,OU=Corp,DC=bldragon,DC=com
11/3/2020 8:00:29PM	98.197.208.193	Enable Account	user	CN=Clare Schmitt,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Enabled Account CN=Clare Schmitt,OU=Corp,DC=bldragon,DC=com
11/3/2020 8:00:29PM	98.197.208.193	Enable Account	user	CN=Clare Schmitt,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Enabled Account CN=Clare Schmitt,OU=Corp,DC=bldragon,DC=com
11/3/2020 8:00:29PM	98.197.208.193	Enable Account	user	CN=Julianna Black,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Enabled Account CN=Julianna Black,OU=Corp,DC=bldragon,DC=com
11/3/2020 8:00:29PM	98.197.208.193	Enable Account	user	CN=Julianna Black,OU=Corp,DC=bldragon,DC=com	EC2AMAZ-4UNGPQH.bldragon.com	Enabled Account CN=Julianna Black,OU=Corp,DC=bldragon,DC=com

Copyright (c) Blue Lance, Inc. 2020. All rights reserved. www.BlueLance.com Page 1

Summary Grouped by Operation

This report output type is shown in graph form. Each audited operation being reported will represent one bar in the graph. The number of times that operation was performed will be shown by the height of each bar. The specific counts for each operation will be listed in text format below the graph.
This report also permits the user to drill down into the details.


BLUE LANCE

All Active Directory Activity (Last 90 Days)

LT Auditor+ Oversight Report

Generated On: Thursday, December 10, 2020
Generated By: BLDRAGON\pthomas

Operation

Count of Operation

450 400 350 300 250 200 150 100 50 0

Add Attribute Value | Add Member to Group | Delete Attribute Value | Disable Account | Enable Account | Modify Object | Modify Security DACL | Set Password | User Account Locked Out | User Account Unlocked

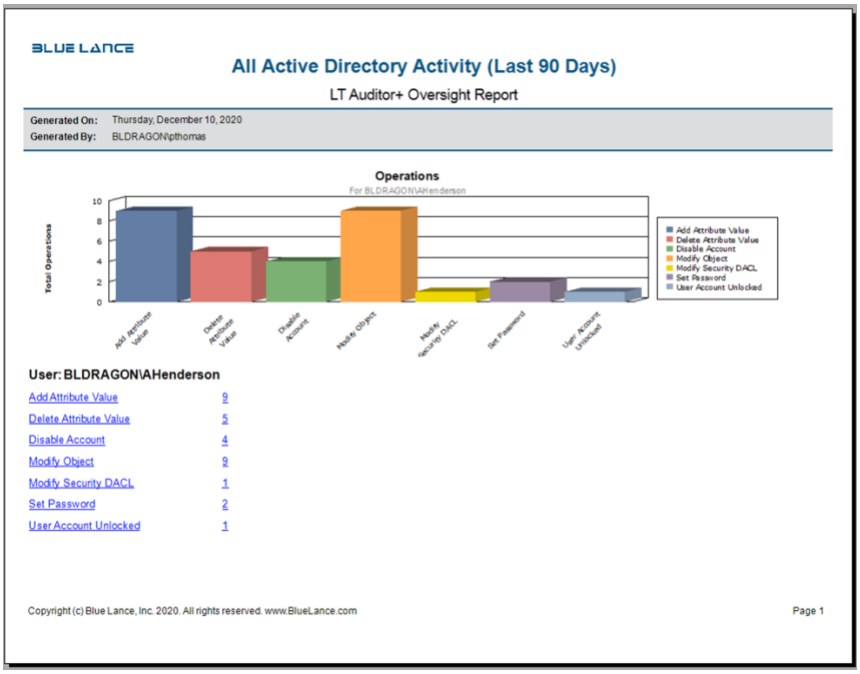
Add Attribute Value	58
Add Member to Group	49
Delete Attribute Value	9
Disable Account	4
Enable Account	428
Modify Object	11
Modify Security DACL	5
Set Password	216
User Account Locked Out	1

Copyright (c) Blue Lance, Inc. 2020. All rights reserved. www.BlueLance.com

Page 1

Summary Grouped by User

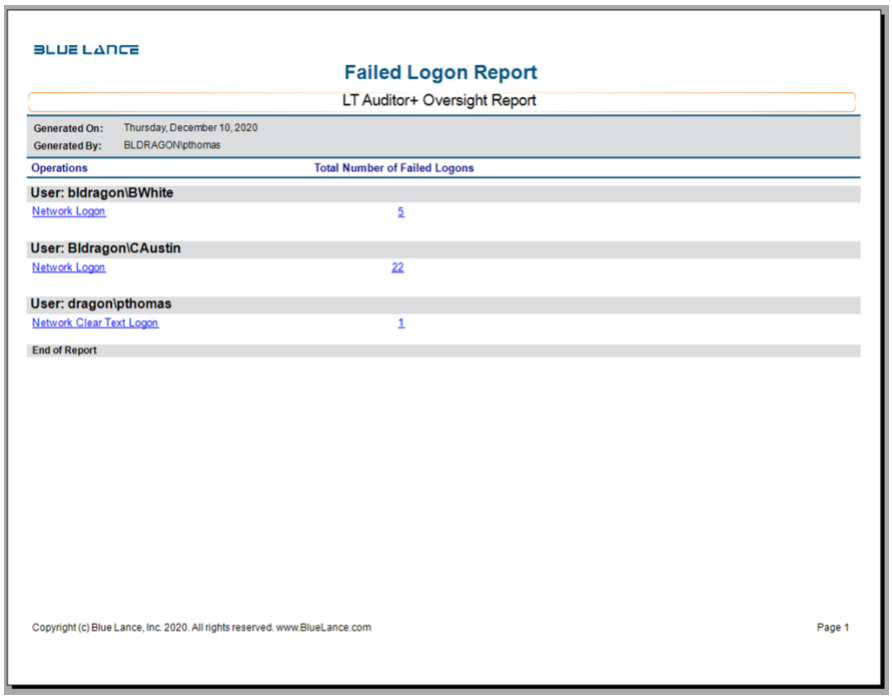
This report output type is shown in graph form. Each audited operation being reported will represent one bar in the graph. The number of times that operation was performed will be shown by the height of each bar. The specific counts for each operation will be listed in text format below the graph.



Failed Logon Summary Report

This is a report containing failed login data categorized by user and specified by a threshold of a minimum number of failed login attempts.

When selecting this type of report, return to the Report Settings tab and under Additional Arguments, enter **%T=n**, where "n" is the minimum number of failed login attempts by any one user to be generated in the report.



BLUE LANCE

Failed Logon Report

LT Auditor+ Oversight Report

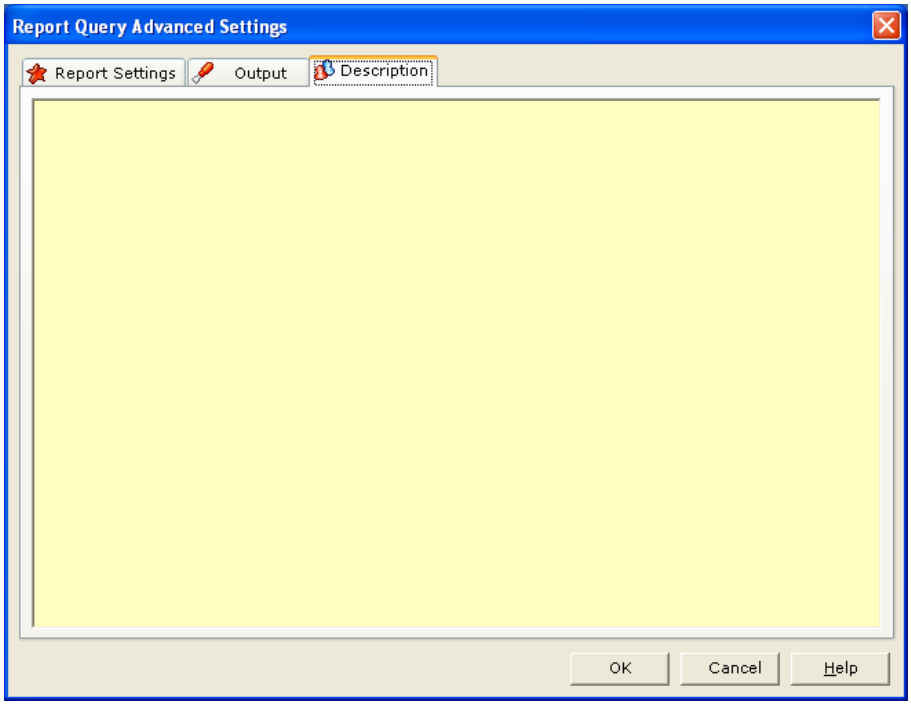
Generated On: Thursday, December 10, 2020
Generated By: BLDRAGON\pthomas

Operations	Total Number of Failed Logons
User: bldragon\BWhite	
Network Logon	5
User: Bldragon\CAustin	
Network Logon	22
User: dragon\pthomas	
Network Clear Text Logon	1
End of Report	

Copyright (c) Blue Lance, Inc. 2020. All rights reserved. www.BlueLance.com Page 1

Description

Under the tab you can create a description of your query. You may choose to include any information regarding the purpose of the query, how it is configured, when it is scheduled to run and in what form it will be viewed.


Report Query Advanced Settings
Report Settings
Output
Description
OK
Cancel
Help

Creating additional report query statements:

3. Select the report query statement.
4. Click New in the right pane displaying all the report query statements for the specific report query.

Modify a report query statement:

1. Select the report query statement.
2. Click Edit in the right pane, which displays all the report query statements for that report query.
3. Modify the report query statement data.
4. Click OK.

Delete a report query statement:

1. Select the report query statement.
2. Click Delete in the right pane, which displays all the report query statements for that report query.
3. Click Yes when prompted for confirmation.

Modify a Report Query:

1. Select the report query and select one of the following:

2. Click Report → Edit in the menu
   OR
   Click Edit on the toolbar.

3. Modify the report query data.
4. Click OK.

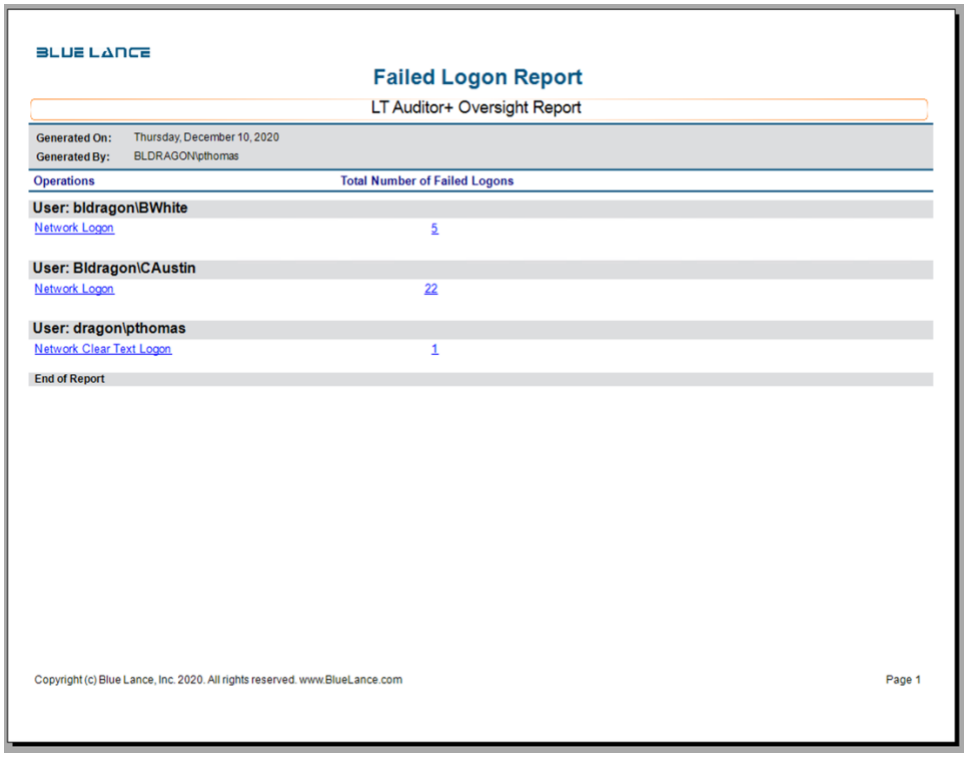
Delete a report query:

1. Select the report query.
2. Select one of the following:

   Click Report → Delete in the menu
   OR
   Click Delete on the toolbar.
3. Click Yes when prompted for confirmation.

Generate a report:

1. Select the report query.
2. Select Generate Report from the Report Console toolbar. A sample report is shown below.



BLUE LANCE

Failed Logon Report

LT Auditor+ Oversight Report

Generated On: Thursday, December 10, 2020
Generated By: BLDRAGON\pthomas

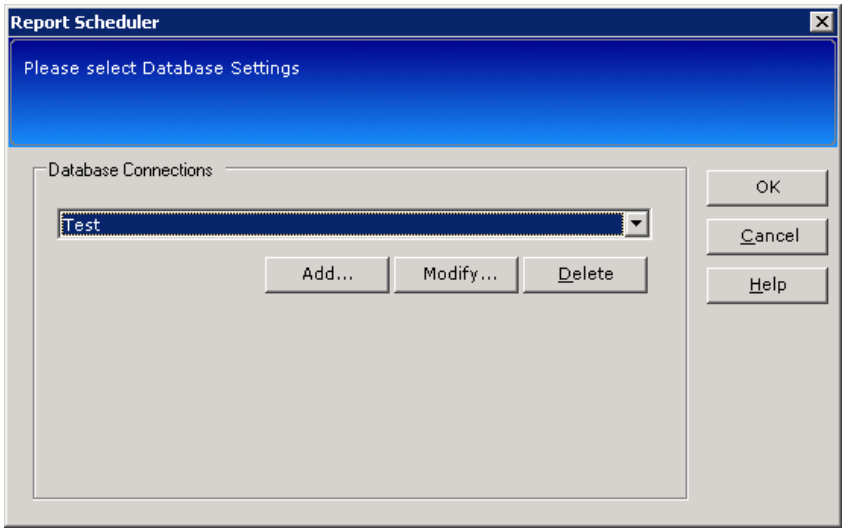
Operations	Total Number of Failed Logons
User: bldragon\BWhite	
Network Logon	5
User: Bldragon\CAustin	
Network Logon	22
User: dragon\pthomas	
Network Clear Text Logon	1
End of Report	

Page 1

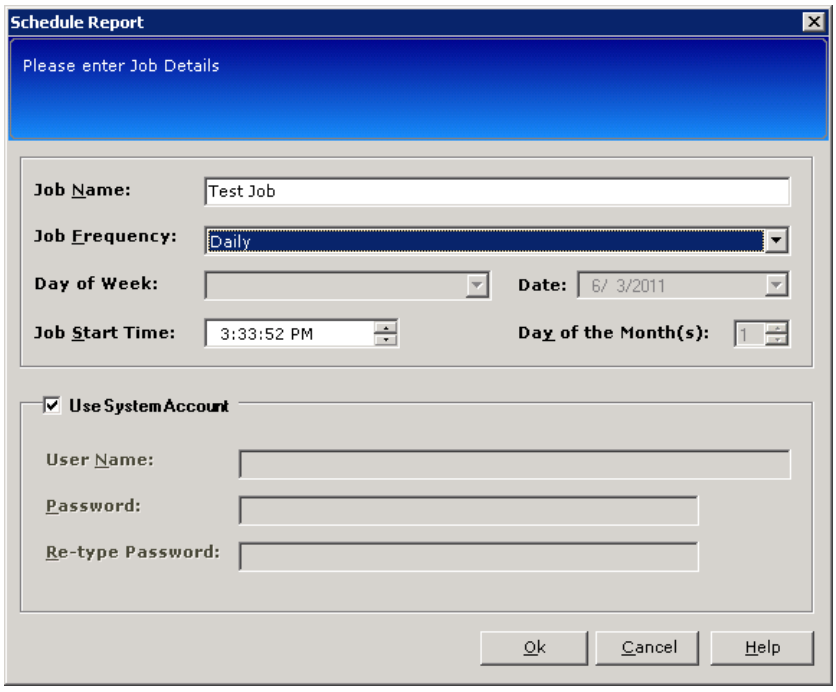
Scheduling a Report

Scheduling a report in the Report Console is made simple by the Report Scheduler. Highlight the query you would like to schedule and click Report → Report Scheduler, or click on the schedule icon in the toolbar.

The Report Console will prompt you for database connection information.

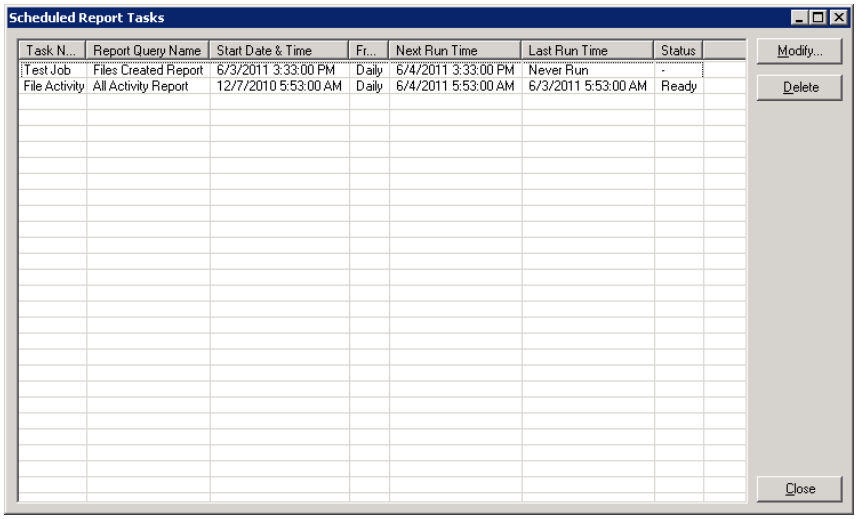


Select your database from the drop-down box, or choose to create a new connection. Once you are connected, the Job Details window will appear.



Enter the job name, job frequency, date and start time as necessary. When properly configured, click OK. You will receive reports with the frequency you requested in the output format previously configured in the Advanced Settings window.

A list of all scheduled reports can be viewed by clicking on the menu Report → View Scheduled Reports.



Chapter 5 – Securing LT Auditor +

Authenticating to the Workspace

There are several areas in LT Auditor+ that require authentication to access.

- Security Management Console
- Manager Console
- Report Console
- Remote Install for Agents

There are two levels of security for LT Auditor+. Level 1 security defines the users authorized to access the workspace. Level 2 securities define users authorized to access the managers.

LT Auditor+ Security Level 1

Authorized users will access the workspace by authentication. For example, LT Auditor+ for Windows will access the workspace through a Microsoft SQL server or through an Oracle server. The first level 1 user is added during the initial installation.

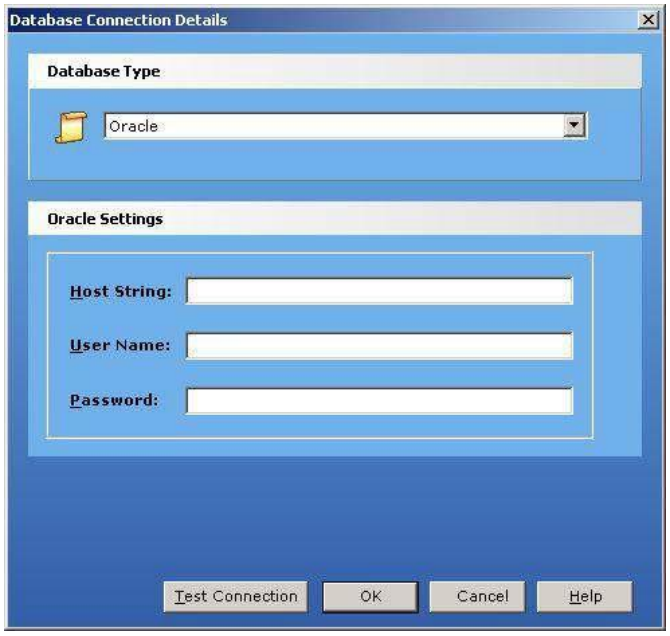
To launch the Security Management Console:

1. Click Start → All Programs →Blue Lance, Inc → Management Console.
2. The screen displayed below prompts for the database connection information.
3. Connect to the workspace to add authorized users.

For SQL:

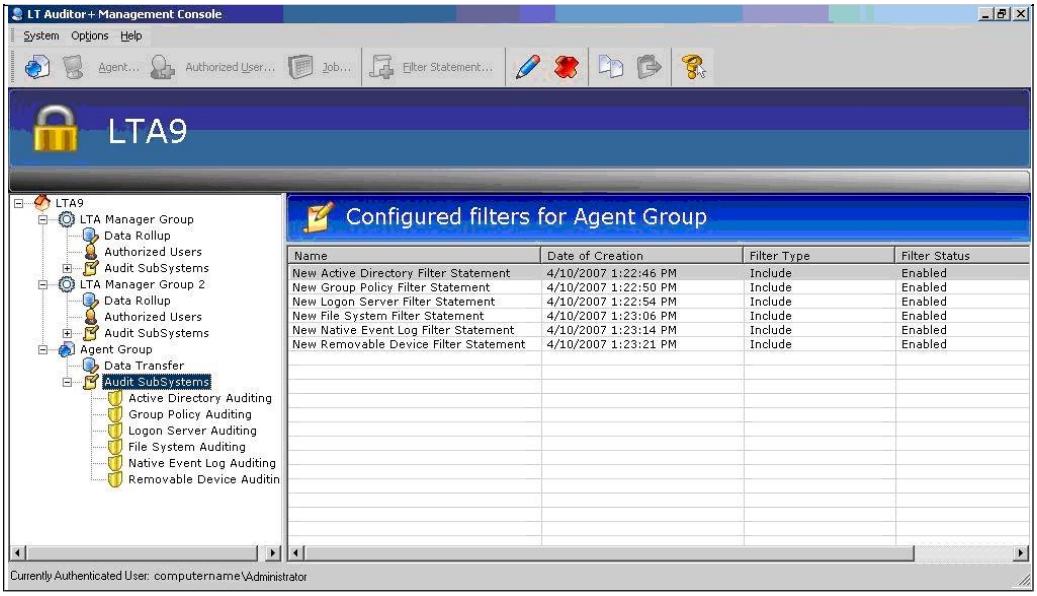
1. Select Microsoft SQL Server for Database Type information.
2. Provide Server ID.
3. Provide Database Name.
4. If NT Integrated Security was enabled during installation, you should be signed in with your Windows password. If User Name and Password was selected, provide the username and the password.
5. Click OK.

For Oracle:



1. Select Oracle for database type.
2. Provide host string.
3. Enter username.
4. Enter password.
5. Click OK.

The Management Console gets launched as soon as the user is authenticated to the workspace. The Management Console screen is shown in the following figure:



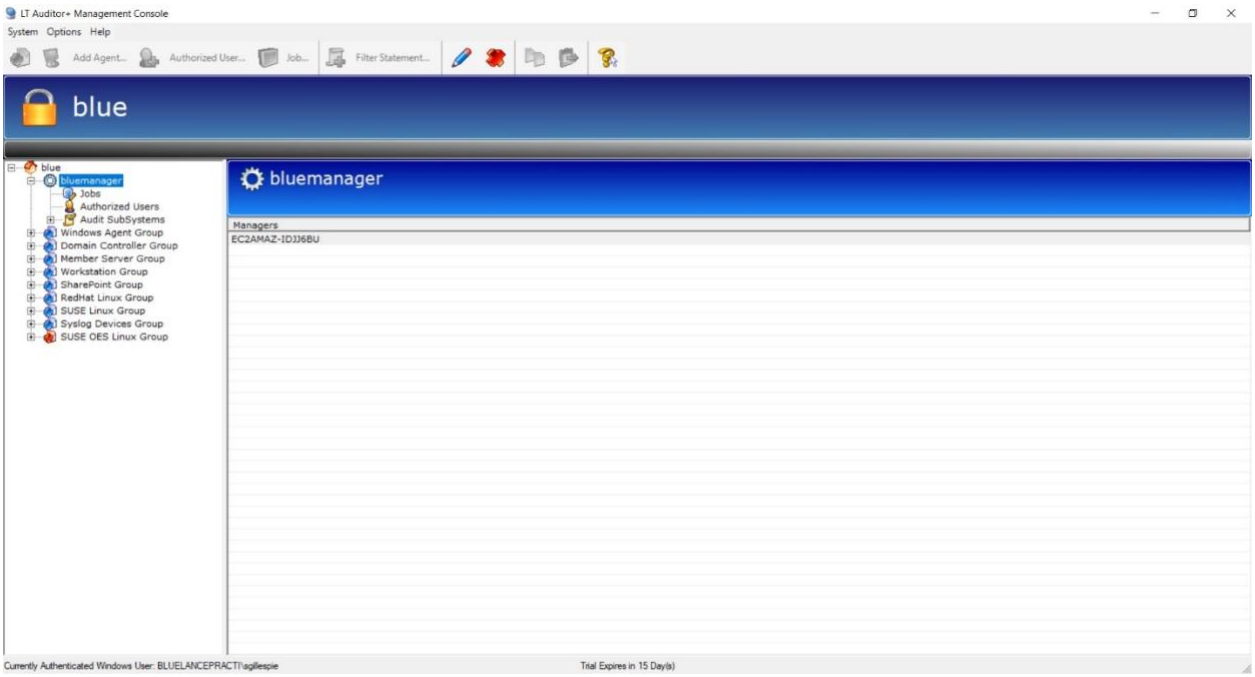
The Management Console is divided into two views. The left pane shows all of the currently configured workspace with the workspace name as the root node of the tree. Below the root nodes are the manager groups and agent groups of the workspace. The right pane displays the details of each node highlighted on the left side.

Select the workspace root node in the tree to display all the manager groups and agent groups in the pane on the right side.

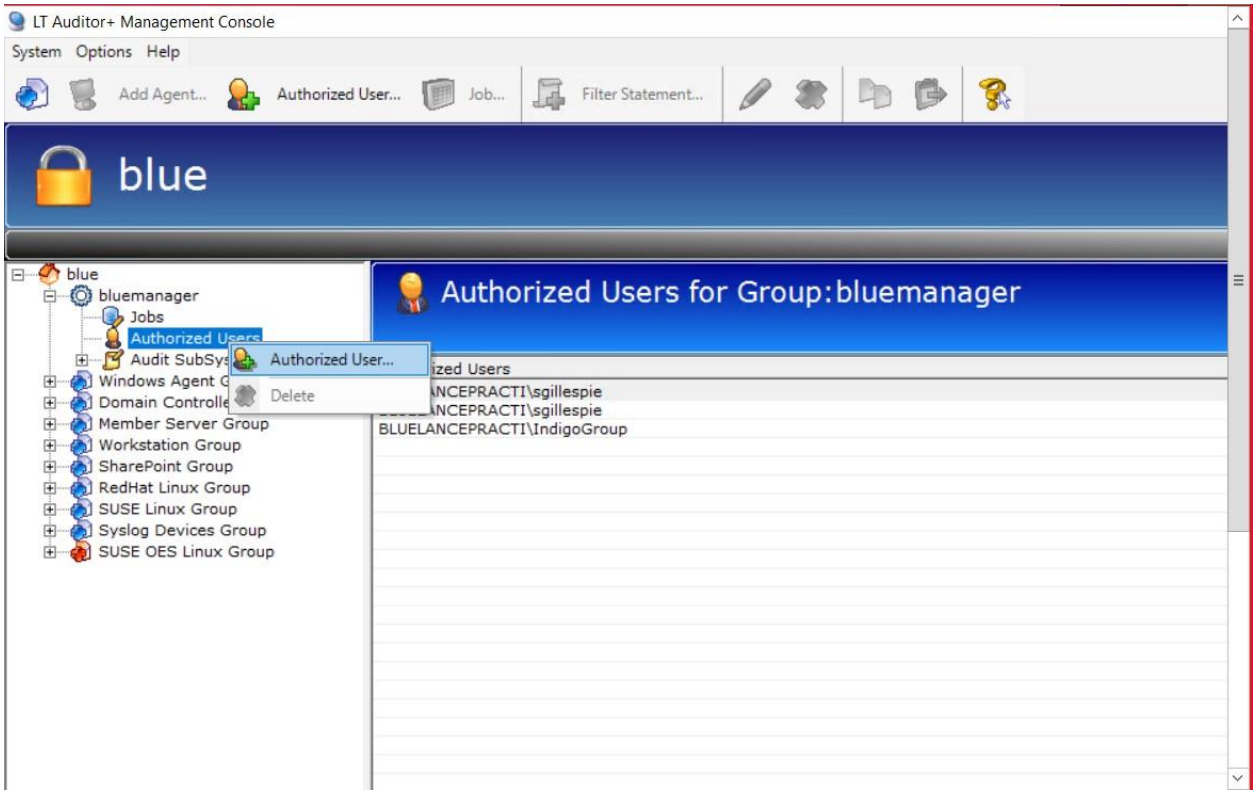
LT Auditor+ Security Level 2

Adding Authorized Users and Groups to the LT Auditor+ Management Console

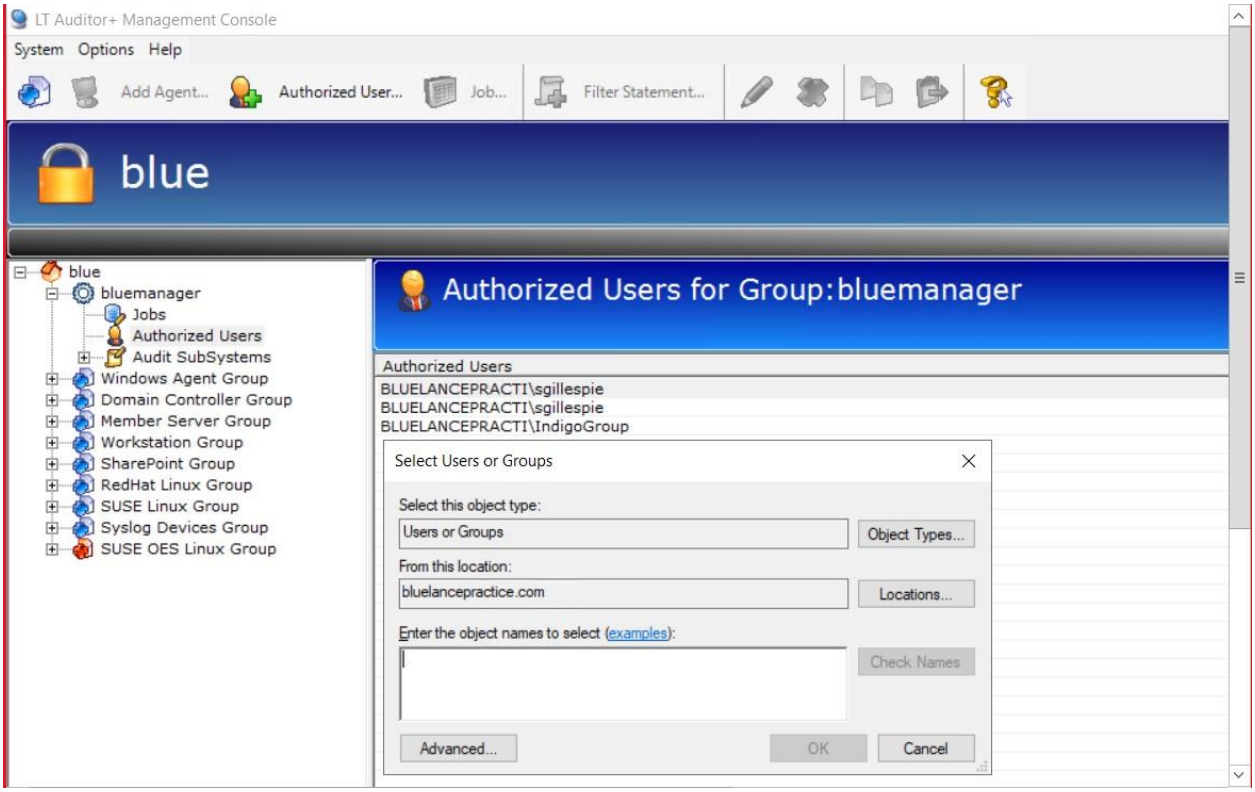
1. Open LT Auditor+ Management Console and navigate to Management Group directly under your Domain in the left panel.

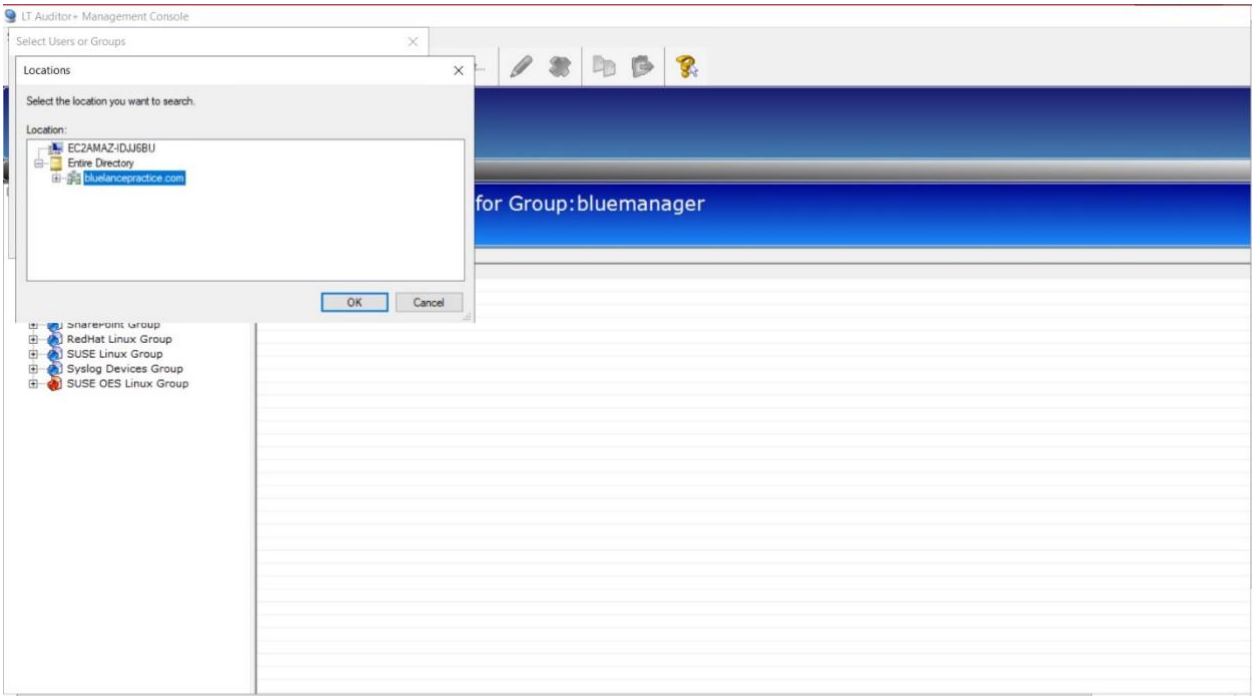


2. Click on Manager Group to expand and view Authorized Users.

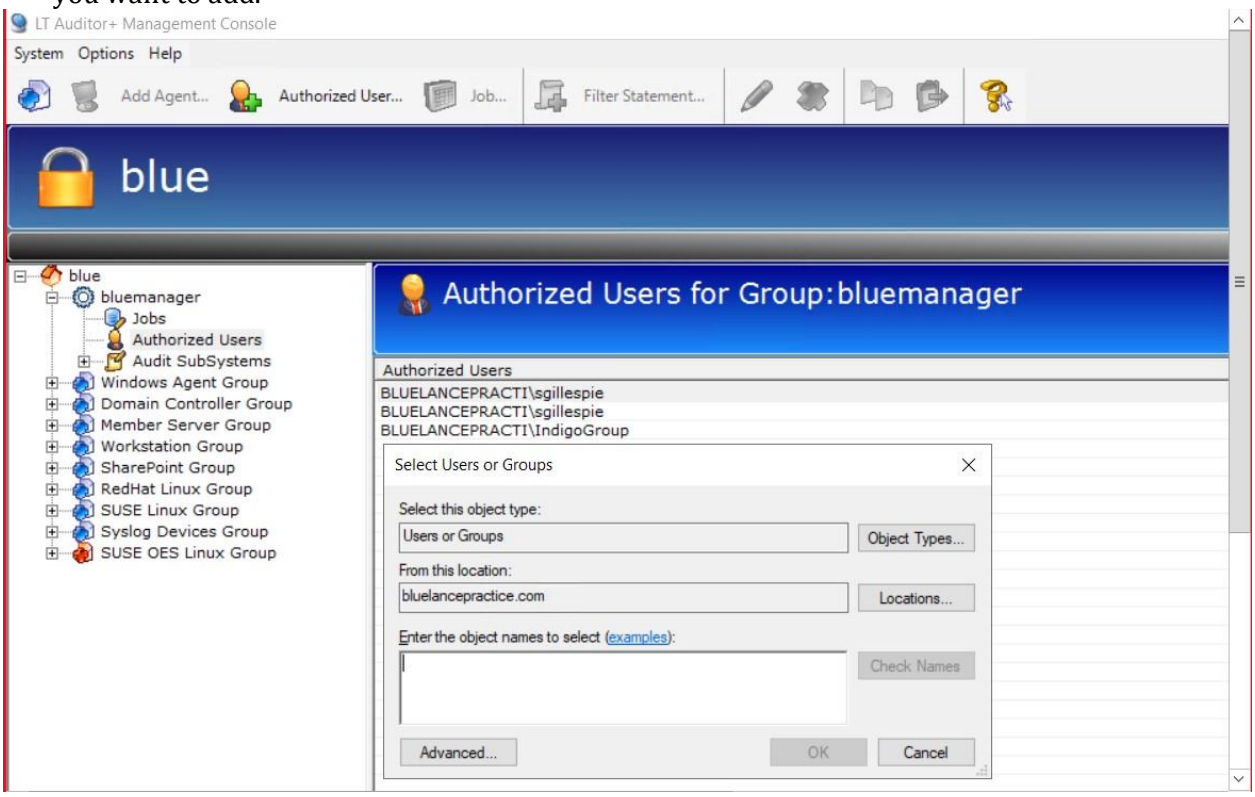


3. Right-click on Authorized Users and select the Add Authorized User option.





4. If needed, click on the Locations button to navigate to the domain that contains users or groups you want to add.

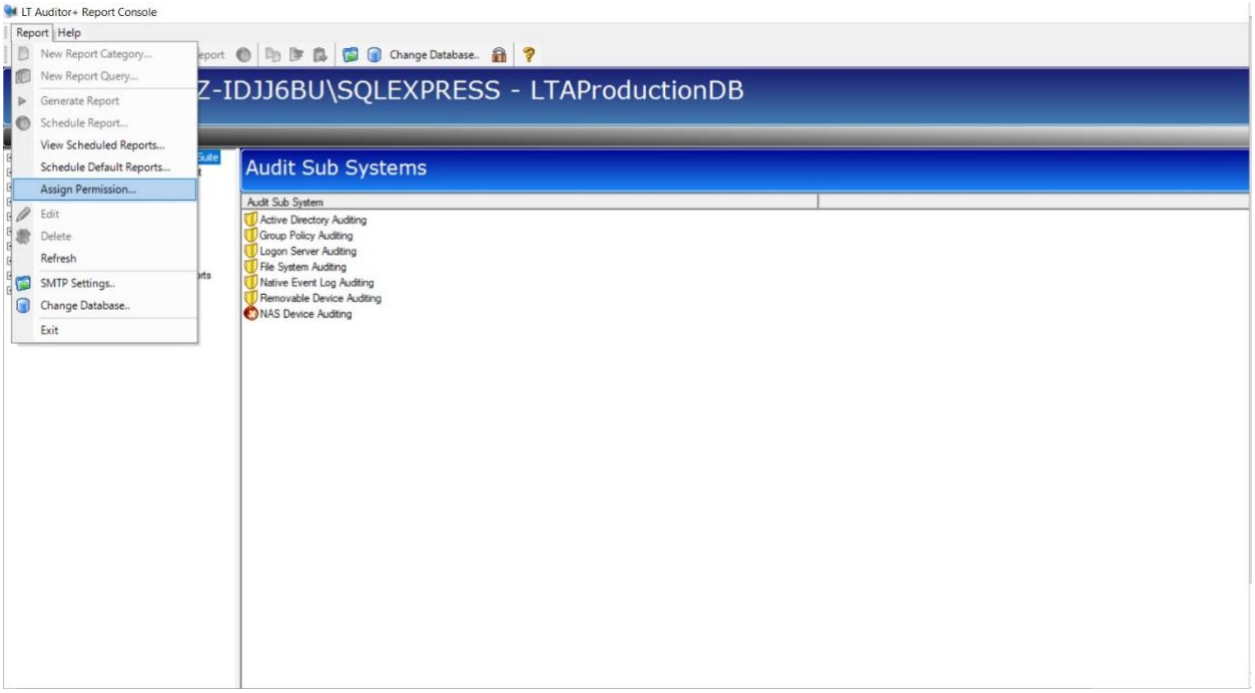


5. With the desired domain location selected, enter name(s) of user(s) and/or group(s) to authorize.
6. After adding the desired users and/or groups, click the Check Names button to confirm.

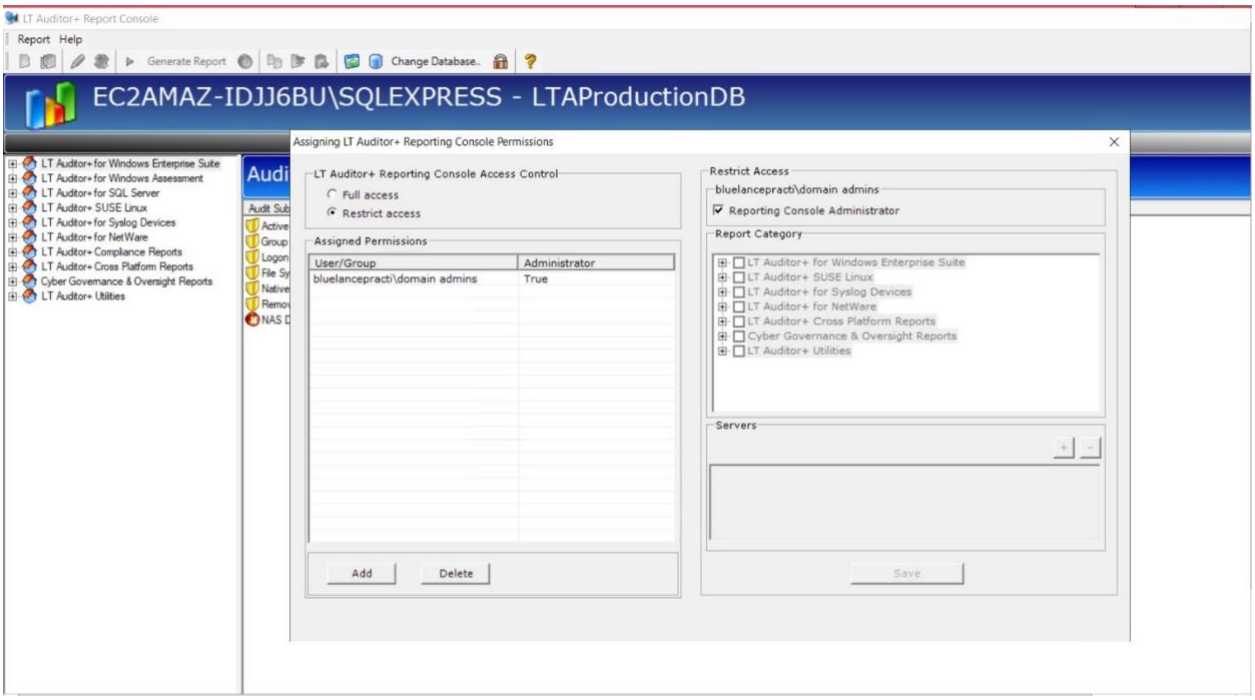
7. Click the OK button, and the user/group path(s) will show up under Authorized Users.

Adding Authorized Users or Groups to the LT Auditor+ Reporting Console

1. Open the LT Auditor+ Reports Console and click on the Report tab.
2. Select the Assign Permissions option.

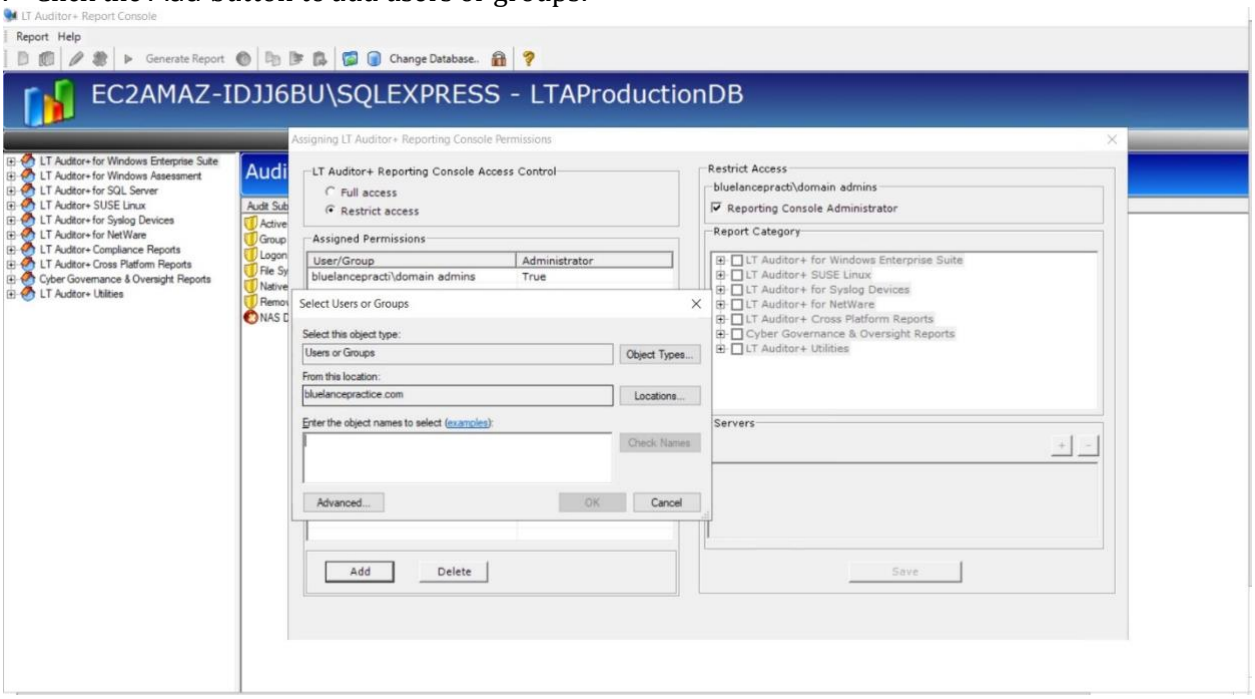


3. To add permissions for individual users or groups, click the Restrict Access option.

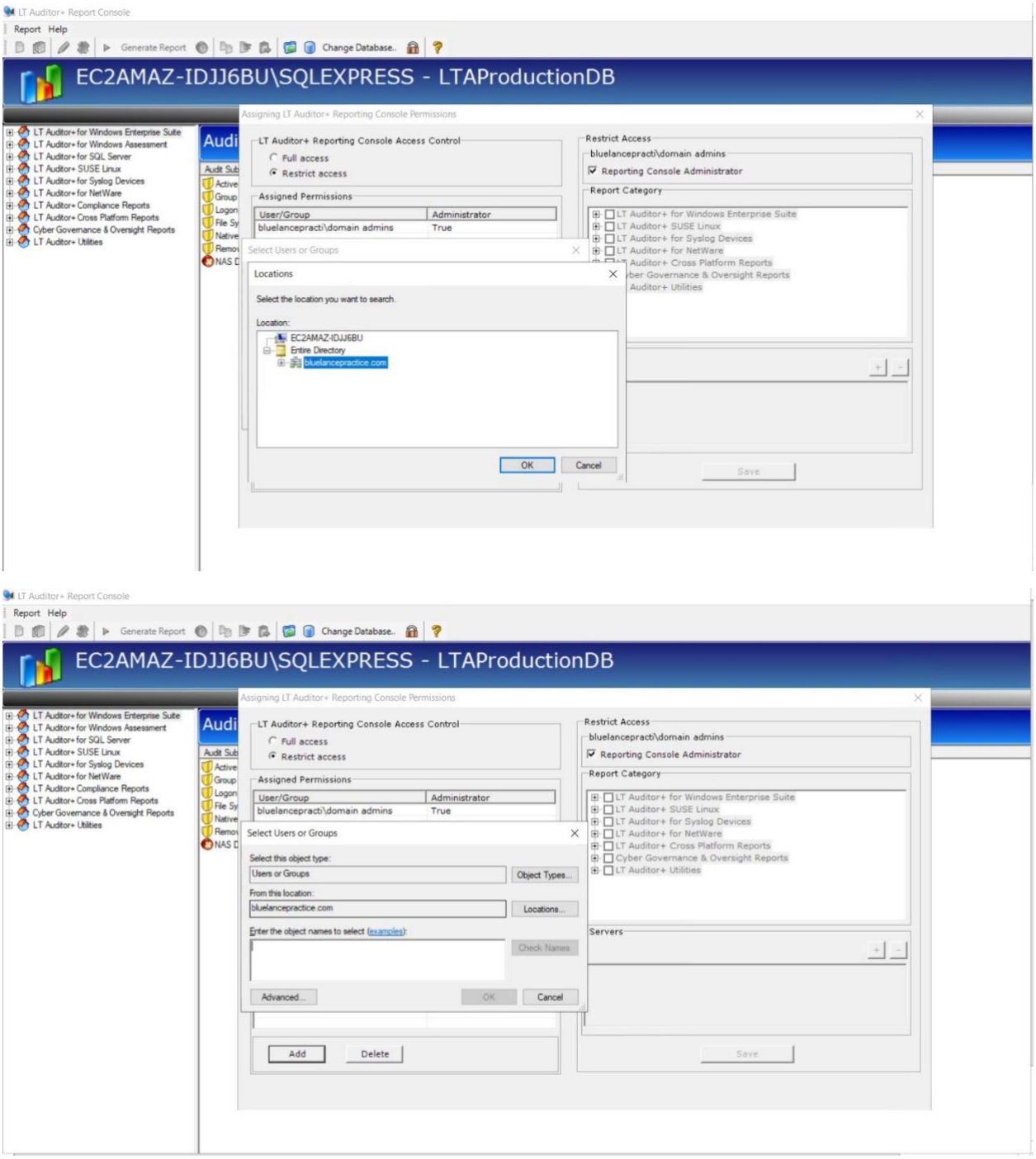


Note: if the Full Access option is selected, then anyone with access to the LT Auditor+ Reporting Console will be able to use the application.

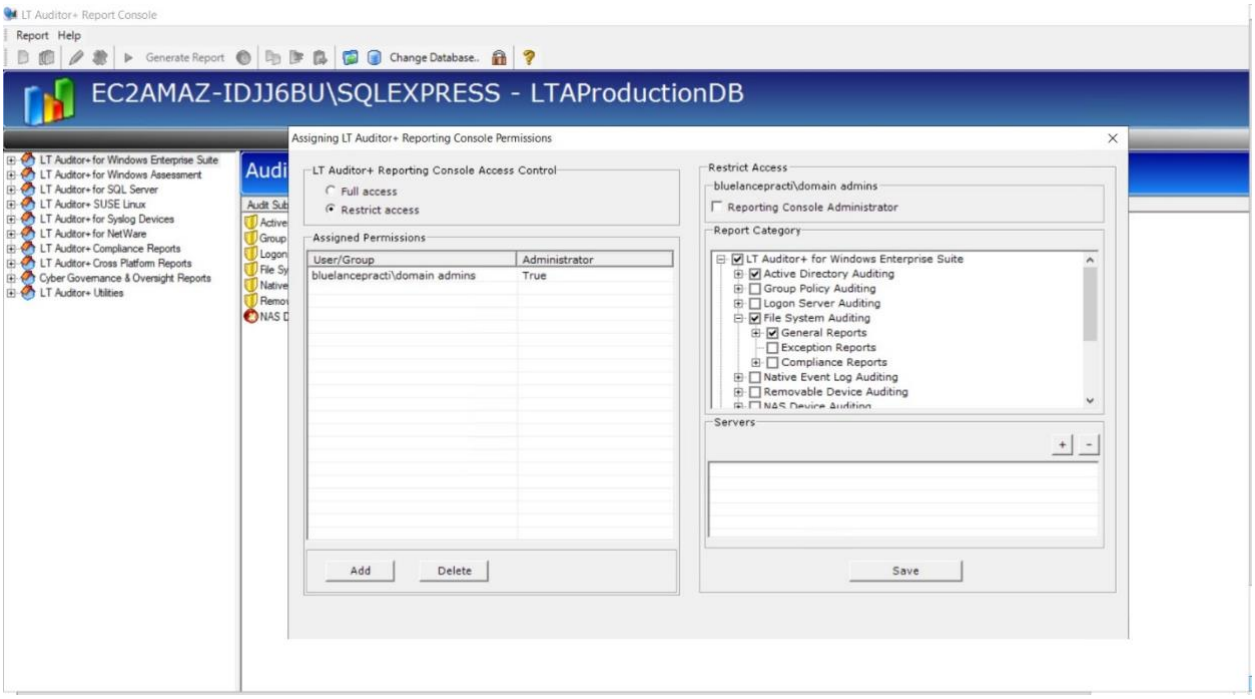
4. Click the Add button to add users or groups.



5. If needed, click on the Location(s) button to navigate to the domain where you want to assign users or groups.



6. Enter name(s) of user(s) and/or group(s) you want to authorize.
7. After adding the desired users and/or groups, click the Check Names button to confirm.
8. Click the OK button and the user/group path(s) will show up under Authorized Users.



9. To add Restrictions to specific report categories, select the user or group under the Assigned Permissions table, and check the boxes for the needed accessibility rules under Report Category. If the user or group needs access to all report categories, check the Reporting Console Administrator check box.
10. Select the Save option when finished and exit the Assign Permissions console.

APPENDIX A

Update Agents

Overview

The purpose of the Update Agents Utility is to automatically upgrade patches remotely on LT Auditor+ Agents from a manager machine hosting LT Auditor+.

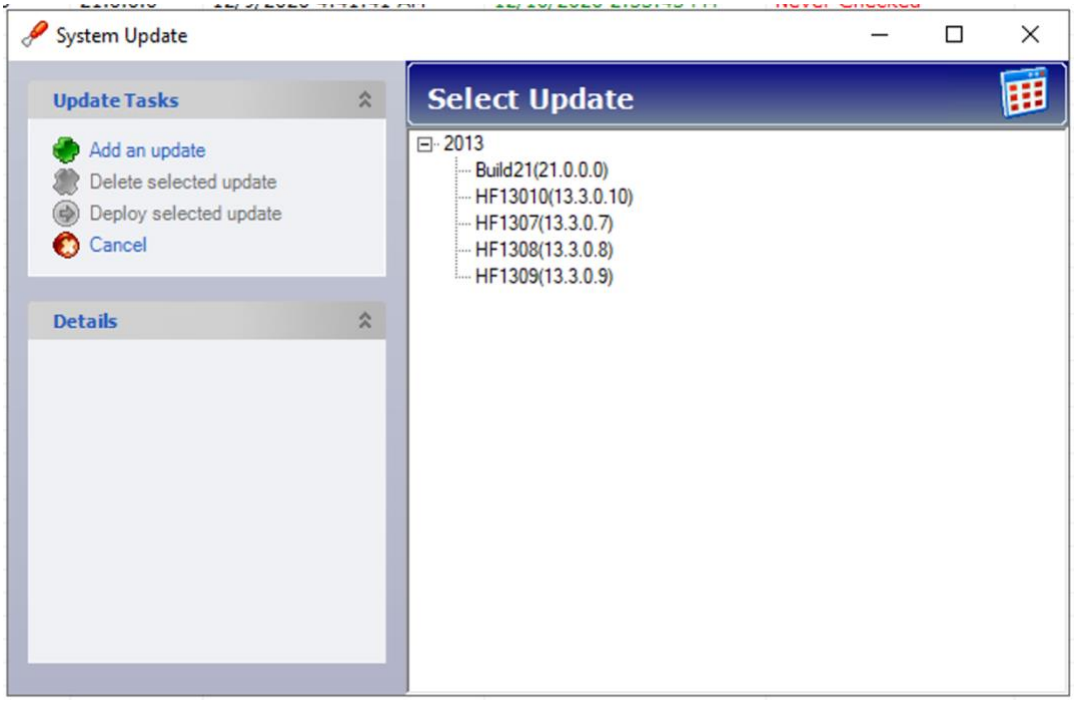
Blue Lance will periodically release patches for LT Auditor+. These patches can be downloaded from the Blue Lance support website at www.bluelance.com/support.
Following the patch download, the Update Agents Utility can be used to ensure that you have installed and deployed a patch across your environment for optimal performance.

NOTE

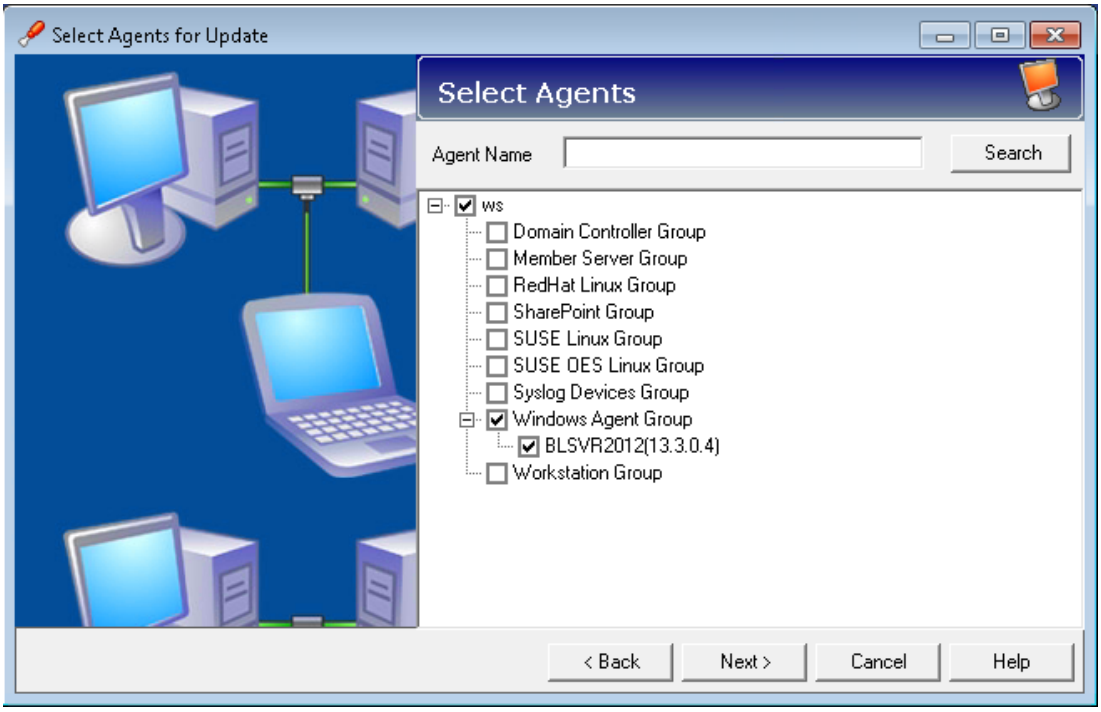
System should be accessed/launched by authorized users from existing Management Console application. No other application or process should be allowed to access or launch this application.

Follow the steps to update all Windows agents.

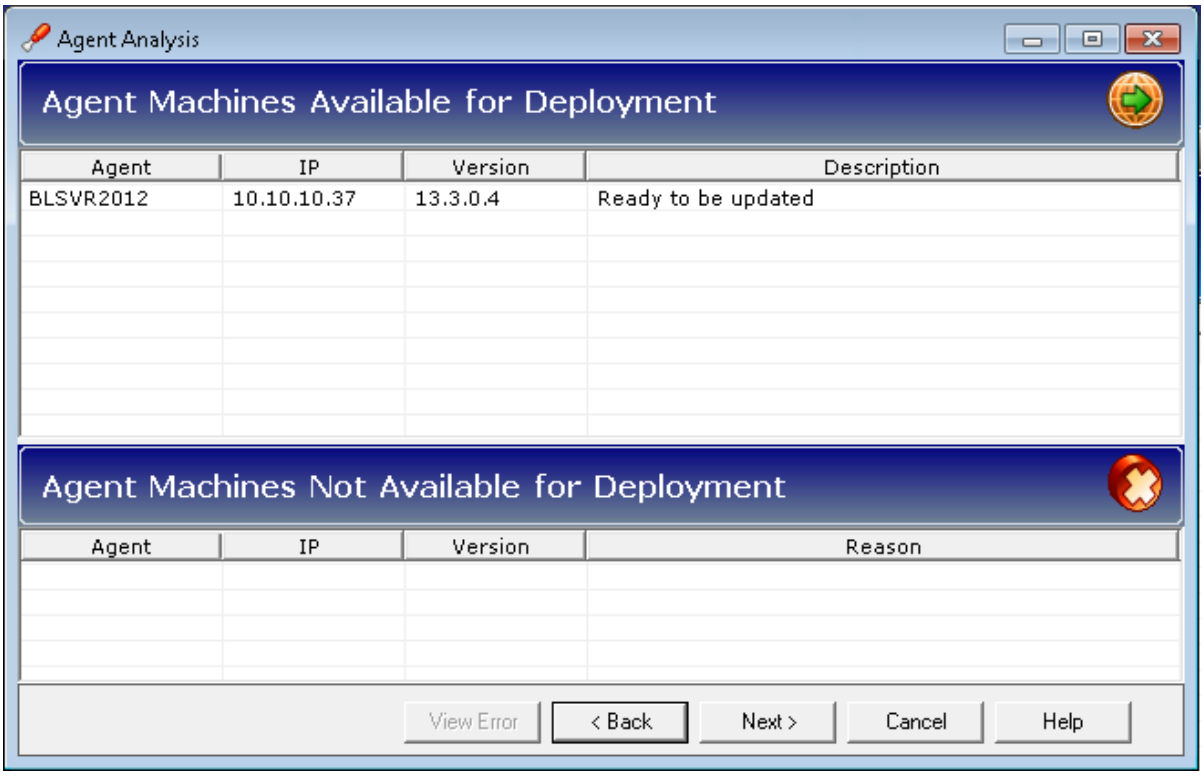
1. Launch the LT Auditor+ Management Console and bring the System Update window by clicking Options →Update Agents.



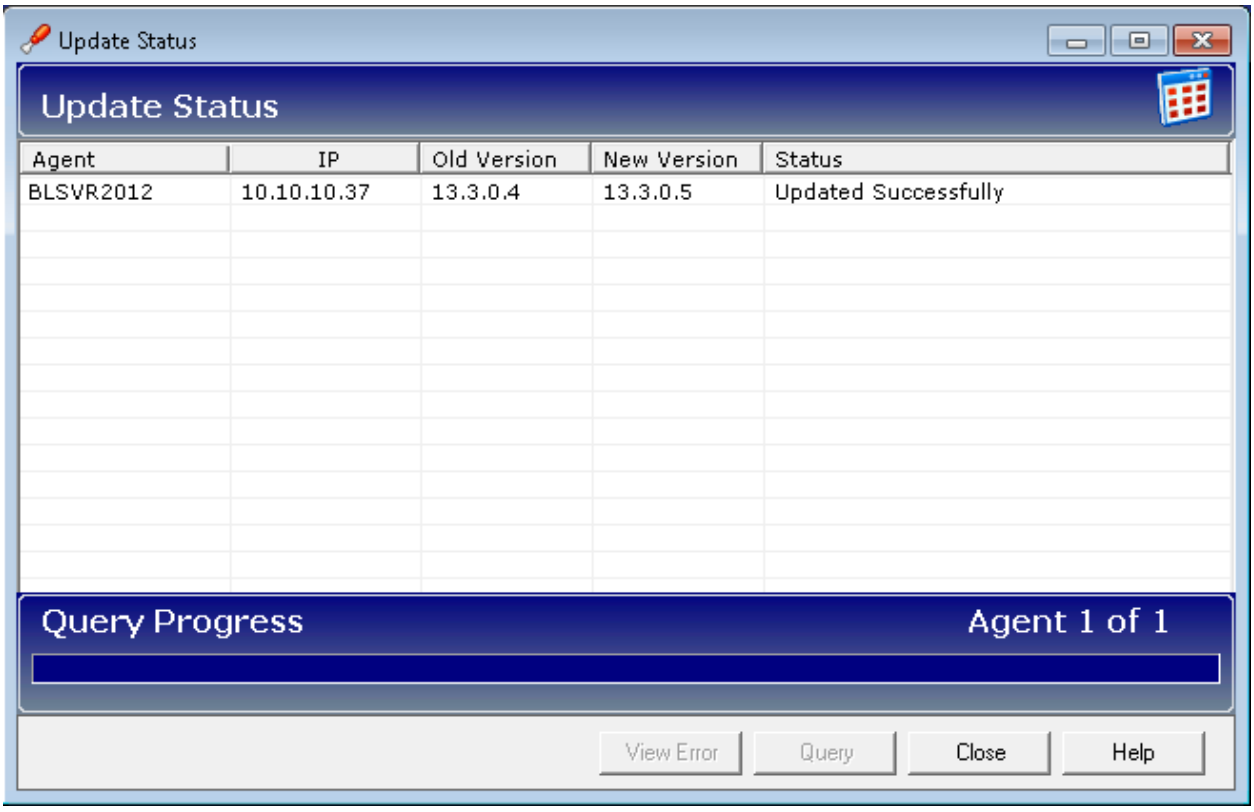
2. Select the latest update and click Deploy Selected update to bring up the following screen.



3. Select the Windows agents to be upgraded and click Next. The system will check each of the selected agents and will confirm if each agent is ready to be updated.



4. Click Next to start the upgrade process. Each agent will be upgraded. This window can be closed during the upgrade process. However, if it is kept active, it will display the status of the update as shown below.



5. Click Close to complete the upgrade process.

APPENDIX B

Auditing EMC Isilon

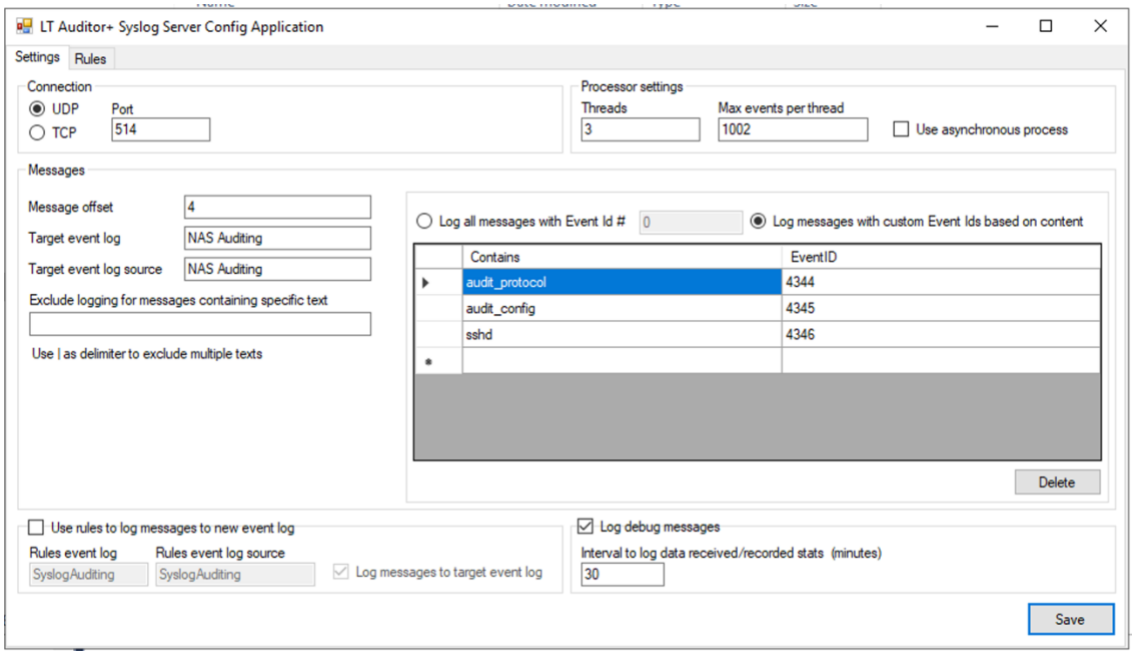
Overview

The purpose of this section is to review steps required for EMC Isilon NAS devices with LT Auditor+.

NOTE

NAS Auditing requires installation and configuration of the LT Auditor+ Syslog Server. Please review documentation on LT Auditor+ Syslog Server prior to undertaking the following steps.

1. Launch the LT Auditor+ Syslog Server and set up the following configurations as shown:



- Target event log must be set to “NAS Auditing.”
- Log Messages must be set to the following event IDs with content message as shown:
  - audit_protocol 4344
  - audit_config. 4345
  - sshd 4346
- Set Message offset to 4. (See explanation below)

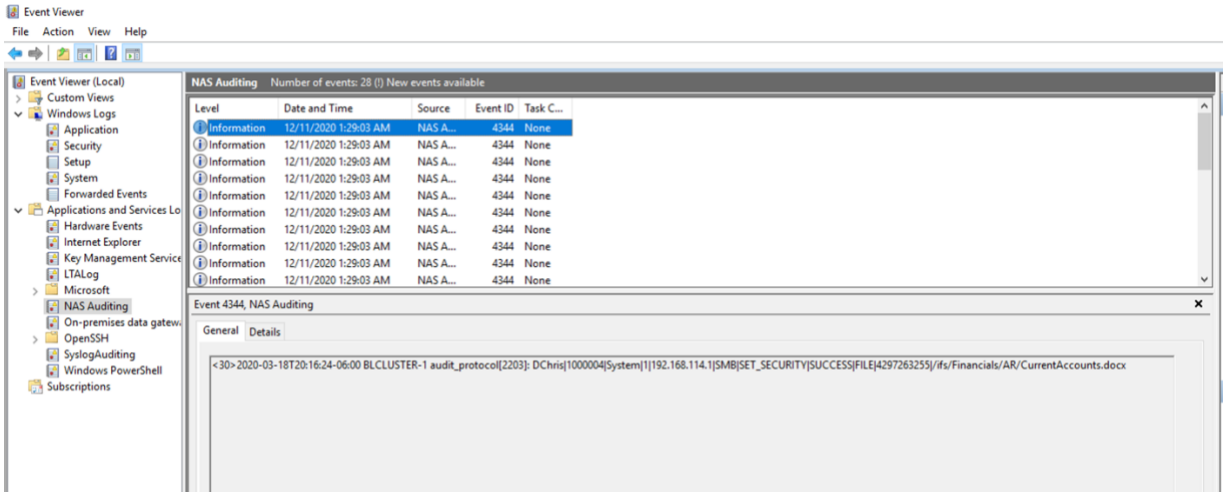
2. Configure the Isilon NAS device to send audit data via Syslog to the LT Auditor+ Syslog Server. Keep in

mind if the port is different from UDP 514, please update LT Auditor+ Syslog Server with the different settings.

NOTE

Isilon is an enterprise class data storage system that can handle petabytes of data. Auditing this device can generate a tremendous volume of data. LT Auditor+ can control what data received from Isilon is recorded or alerted on. However, the LT Auditor+ Syslog Server receives all data; therefore, it is vital that a dedicated instance of LT Auditor+ Syslog Server be used for auditing Isilon devices. In this environment, if auditing is required for other Syslog devices, please use another instance of the LT Auditor+ Syslog Server.

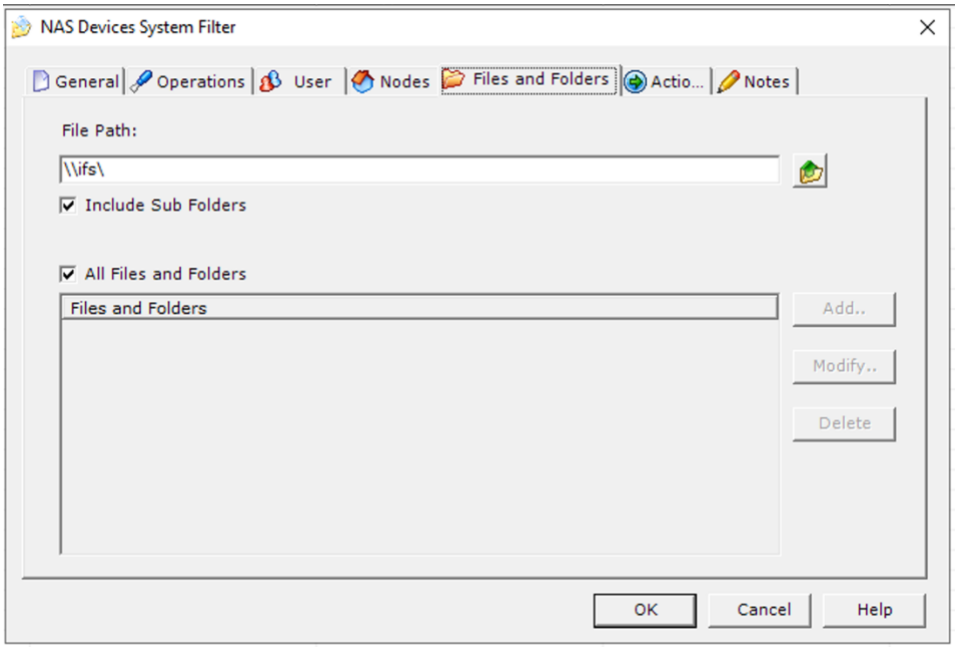
3. Confirm LT Auditor+ Syslog Server is receiving messages from the Isilon device by reviewing the event log NAS Auditing. Messages should become as shown below:



NOTE

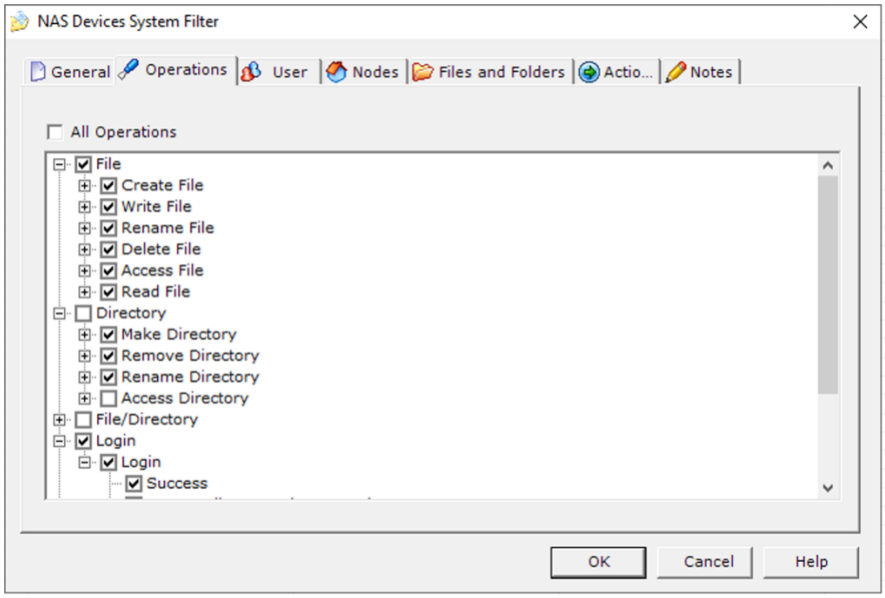
Ensure that Date stamp of event in the log appears after the number of characters specified in the Message Offset. Example: <30>2020-03-18T20:16:24-0600. There are four characters highlighted before the date stamp; therefore, message offset should be set to "4." If the offset value is not correct, LT Auditor+ will not be able to read the time stamp of the event.

4. Setup an LT Auditor+ filter to audit activity received from Isilon via the LT Auditor+ Syslog Server.

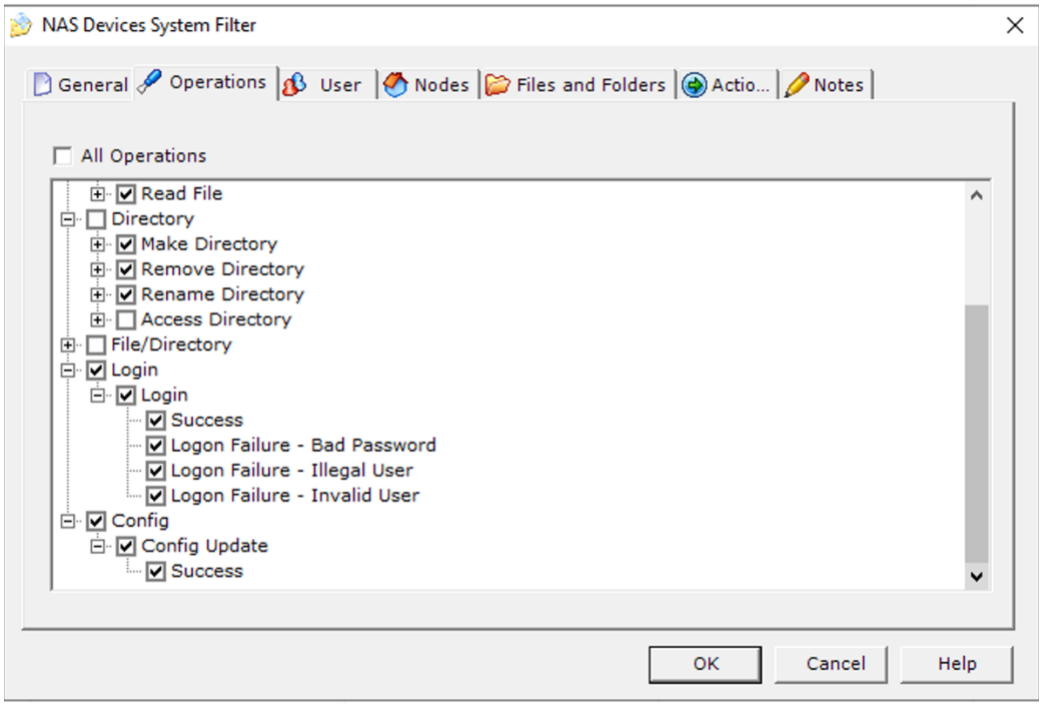


Additional filters can be configured to include or exclude activity.

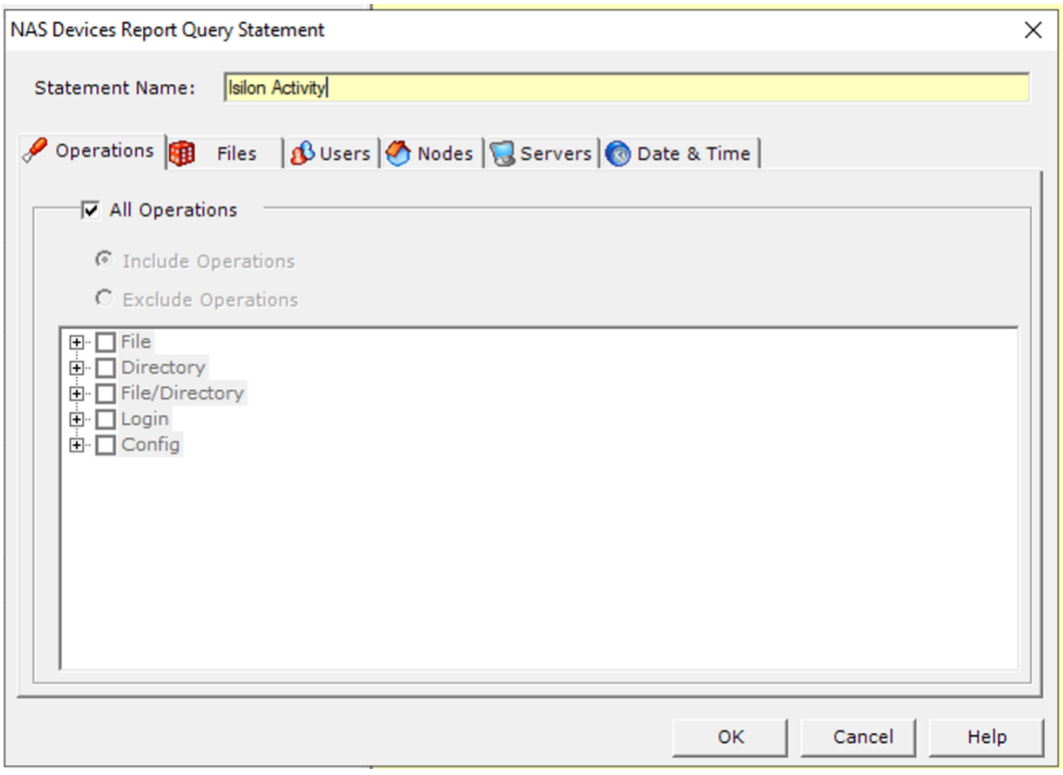
LT Auditor+ audits the following File/Folder Isilon operations as shown:



LT Auditor+ also audits the following config and login Isilon operations as shown:



5. Use similar settings in the LT Auditor+ Report Console to report on Isilon activity.



Reports can be queried based on operations, files, users, and date and time criteria. A sample report is shown below:

Date & Time	User	Node	Operation	File	Server	Remarks
1/2/2020 5:51:50PM	NFS\root	137.15.98.37	Write File	\\ifs\dmnas\data\sapmnt-sap\pr1\global\sapcontrol\1_52013_52014_28_2_20_scspr1-vip	BLCLUSTER-2	Wrote to File \\ifs\dmnas\data\sapmnt-sap\pr1\global\sapcontrol\1_52013_52014_28_2_20_scspr1-vip
1/2/2020 5:51:50PM	NFS\root	137.15.98.37	Write File	\\ifs\dmnas\data\sapmnt-sap\pr1\global\sapcontrol\1_52013_52014_28_2_20_scspr1-vip	BLCLUSTER-2	Wrote to File \\ifs\dmnas\data\sapmnt-sap\pr1\global\sapcontrol\1_52013_52014_28_2_20_scspr1-vip
1/3/2020 5:39:45PM	\hhh	192.15.2.246	Login	: Failed password for invalid user hhh from 192.15.2.246 port 51842 ssh2	BLCLUSTER-2	
1/3/2020 5:39:48PM	\hhh	192.15.2.246	Login	: Failed password for invalid user hhh from 192.15.2.246 port 51842 ssh2	BLCLUSTER-2	
1/3/2020 5:39:50PM	\hhh	192.15.2.246	Login	: Failed password for invalid user hhh from 192.15.2.246 port 51842 ssh2	BLCLUSTER-2	
3/19/2020 2:07:34AM	SMB\JSmith	ip-192-168-114-1.ec2.internal	Create File	\\ifs\Financials\AR\DelinquentAccounts.xlxs	BLCLUSTER-1	Created File \\ifs\Financials\AR\DelinquentAccounts.xlxs
3/19/2020 2:07:34AM	SMB\JSmith	ip-192-168-114-1.ec2.internal	Create File	\\ifs\Financials\AR\DelinquentAccounts.xlxs	BLCLUSTER-1	Created File \\ifs\Financials\AR\DelinquentAccounts.xlxs
3/19/2020 2:10:10AM	SMB\DSam	ip-192-168-114-1.ec2.internal	Delete File	\\ifs\Financials\AR\DelinquentAccounts.xlxs	BLCLUSTER-1	Deleted File \\ifs\Financials\AR\DelinquentAccounts.xlxs
3/19/2020 2:10:10AM	SMB\DSam	ip-192-168-114-1.ec2.internal	Delete File	\\ifs\Financials\AR\DelinquentAccounts.xlxs	BLCLUSTER-1	Deleted File \\ifs\Financials\AR\DelinquentAccounts.xlxs
3/19/2020 2:11:58AM	SMB\HFox	ip-192-168-114-1.ec2.internal	Access File	\\ifs\Financials\AR\CurrentAccounts.docx	BLCLUSTER-1	Accessed File \\ifs\Financials\AR\CurrentAccounts.docx
3/19/2020 2:11:58AM	SMB\HFox	ip-192-168-114-1.ec2.internal	Access File	\\ifs\Financials\AR\CurrentAccounts.docx	BLCLUSTER-1	Accessed File \\ifs\Financials\AR\CurrentAccounts.docx
3/19/2020 2:16:24AM	SMB\DChris	ip-192-168-114-1.ec2.internal	Write Security DACL	\\ifs\Financials\AR\CurrentAccounts.docx	BLCLUSTER-1	Modified Security DACL of \\ifs\Financials\AR\CurrentAccounts.docx