BLUE LANCE

LT Auditor+

Installation Guide

Release Build21

Intellectual Property

Special Conventions

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

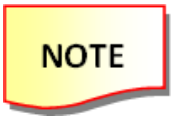
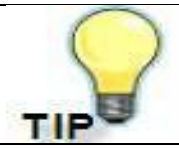
Icons	Description
	**WARNING: Alerts the reader to a potential action, practice or situation that can result in major damage to data or the system. Damage is permanent and irreversible. Results may be contrary to what is expected or intended.**
	**CAUTION: Alerts the reader to a potential action, practice 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 following major subsections.

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

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:

- System requirements for LT Auditor+.
- Installation of LT Auditor+.

Using this Document

This section explains the installation and configuration of the LT Auditor+ 9.

Document Structure

The document is divided into the following chapters:

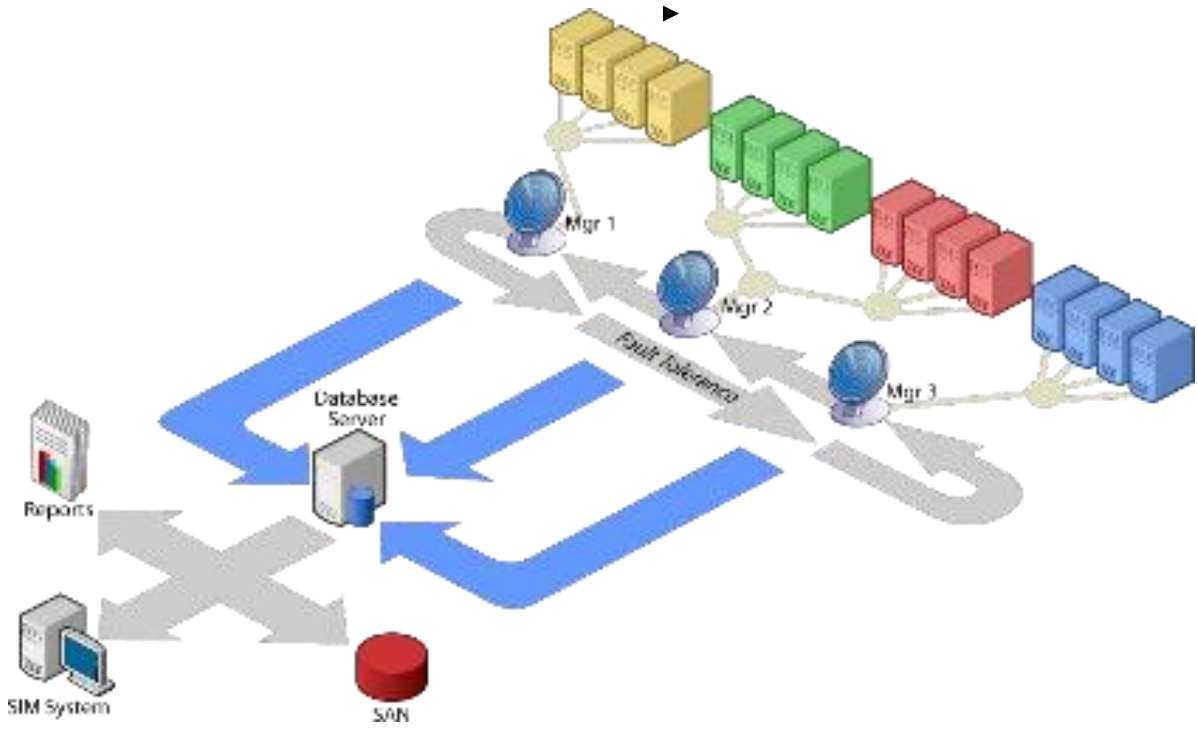
Chapter	Description
About the Document	Provides information about this document, including what it is used for, who should read it, what it contains, how it is presented and how it is used.
About LT Auditor+ Installation Guide	Provides information about LT Auditor+ and its components. Provides the details on how to install LT Auditor+.

TERMS

Components	Description
Workspace	An LT Auditor+ workspace is created in a Microsoft SQL or Oracle database. It contains all the required configuration information to host a working implementation of LT Auditor+ within an enterprise. The configuration information includes the agents that are configured within the setup, the manager machines that will consolidate the data collected by agents and all required LT Auditor+ policy information used to collect and report on the audit data.
Manager	A manager machine performs two major roles within the workspace. It deploys agent group policies to all the agents within the group that it services. It also performs the function of consolidating data received from the agents into the database.
Manager Group	A manager group is an administrative group consisting of one or more managers. They contain policies that define its consolidation of data from the agents and audit policies pertaining to the manager.
Windows Agent	An agent is a Microsoft Windows server/workstation in which LT Auditor+ is installed for auditing purposes. The LTA agent can be configured to collect audit data from the event logs on that machine. Windows agents reside in a Windows agent group that is configured and managed by a manager in that workspace.
Windows Agent Group	An agent group is an administrative group consisting of one or more Windows agents that contain audit policies and settings pertaining to those agents. The Windows agent group is assigned a primary manager from the workspace, which handles policy deployment to and data consolidation from agents in that group.
Event Log	An event log is a database that maintains information about program, security and system events on your computer. There are three standard event logs created on Windows operating systems: • Application • System • Security
Jobs	An event viewer is an application that allows you to view and configure event logs on the computer system. Tasks are scheduled to run at a specified time such as daily, weekly or monthly. LT Auditor+ includes the following jobs: ➢ **Transfer Job** — Creates files that contain events collected from the system and transfers these files to the manager. It also manages logs to ensure that transferred files are backed up, and old backed up files that are no longer required are deleted from the system. ➢ **Rollup Job** — Transfers rolled up or files merged into a

	consolidated database defined by the manager settings on the system. Files can be rolled up to high-end relational databases or data files such as: • Microsoft SQL • Oracle • XML This job is performed on the manager. ➢ **Scan Job** — this job, performed by the Agent Status Monitoring Utility, monitors agents in regard to availability, group membership assignment, data transfer, and version information. This feature can also be configured to send the gathered information via email alerts. Real-time alerts are sent using this feature.
SysLog	
Daemon Settings	Daemon Settings in SUSE Linux are the settings to change the services through the given properties.
LDAP Settings	LDAP setting is modified to get information regarding eDirectory.
Shared Folder	A Shared folder is created by service during first polling. Its format is **Machine name_linux**. User has to provide shared folder settings, which is a primary user due to which shared folder is created.
SUSE Linux Agent Group	SUSE Linux agent group is an administrative group consisting of one or more SUSE Linux agent(s) that contain audit policies and settings pertaining to those agents. This agent group is assigned a primary manager from the workspace, which handles policy deployment to and data consolidation from agents in that group.

Architectural Workflow



The above graphic depicts the LT Auditor+ architecture in three tiers. The first tier represents all audited agents, namely Windows servers/workstations, SUSE Linux servers, NAS devices and any audited device. The second tier represents the LT Auditor+ Manager. Bidirectional communication between the managers and agents is encrypted and secure. Audit policies are deployed from the manager to agents, while audit data is sent from agents to the manager. The third tier represents the database that stores all the configurations and audit data. The manager is tasked with inserting audit data received from agents into the database and also monitor for policy configuration updates that need to be deployed to agents.

Chapter 2 – Install LT Auditor+

This section provides an overview of how the LT Auditor+ is installed and configured. Included in this section are systems requirements, prerequisites and steps required to install LT Auditor+.

Systems Requirements

System requirements for LT Auditor+ components are provided below:

LT Auditor+ Database

Supported databases

- Microsoft SQL 2014, 2016, 2017, 2019
- Microsoft SQL 2017 & 2019 Express Editions (supported only for evaluation)
- Oracle 9i, 10g,11g, 12

Please visit the vendor website for hardware requirements for the database.

LT Auditor+ Manager

Operating system

- Microsoft Windows Server 2012R2, 2016 or 2019 with latest service packs

Hardware

- RAM: 4 GB RAM
- Hard Disk: 200+ GB

Software

- Microsoft .NET 4.0

LT Auditor+ Manager Console

Operating system

- Windows 10, Windows Server 2012R2, 2016, 2019

Hardware

- RAM: 4GB RAM
- Hard Disk: 5+ GB

Software

- Microsoft .NET 4.0

LT Auditor+ Report Console

Operating system

- Windows 10, Windows Server 2012R2, 2016, 2019

Hardware

- RAM: 4 GB RAM
- Hard Disk: 10+ GB

Software

- Microsoft .NET 4.0

LT Auditor+ Agents

Microsoft Windows Agents

- Windows 10, Windows Server 2012R2, 2016, 2019
- Minimum 2GB of RAM
- .NET 4.0
- 500 MB of disk space

SUSE Linux Agents

- OES201515 and OES2018 with latest updates
- 512 MB RAM
- 500 MB of disk space

LT Auditor+ Installation Overview

The following items have to be installed to implement LT Auditor+.

- Create LT Auditor+ databases.
- Install the LT Auditor+ Manager.
- Install LT Auditor+ Manager Console
- Install LT Auditor+ Report Console
- Install LT Auditor+ Agents.

Create LT Auditor+ Databases

LT Auditor+ databases can be created either on Microsoft SQL Server or Oracle. Two databases need to be created, namely Production and Archive. For Microsoft SQL Server, users have an option of creating the databases automatically during the installation of the LT Auditor+ Manager. However, for Oracle, the databases must be created using the scripts provided. Scripts have also been provided to create databases on Microsoft SQL Server directly if customization is required.

For detailed instructions on directly creating LT Auditor+ databases, please refer to **Appendix A.**

Installing the LT Auditor+ Manager

Prerequisites for the LT Auditor+ Manager installation

- Meet the system requirements outlined above.
- Have access to either a Microsoft SQL Server or Oracle database.
- Installer must have administrative privileges to install LT Auditor+.
- For the Windows platform, Windows auditing policies must be set up as per guidelines in Configuration Guide.
- Firewall setting on all machines must be checked to ensure that port 2877 is open.

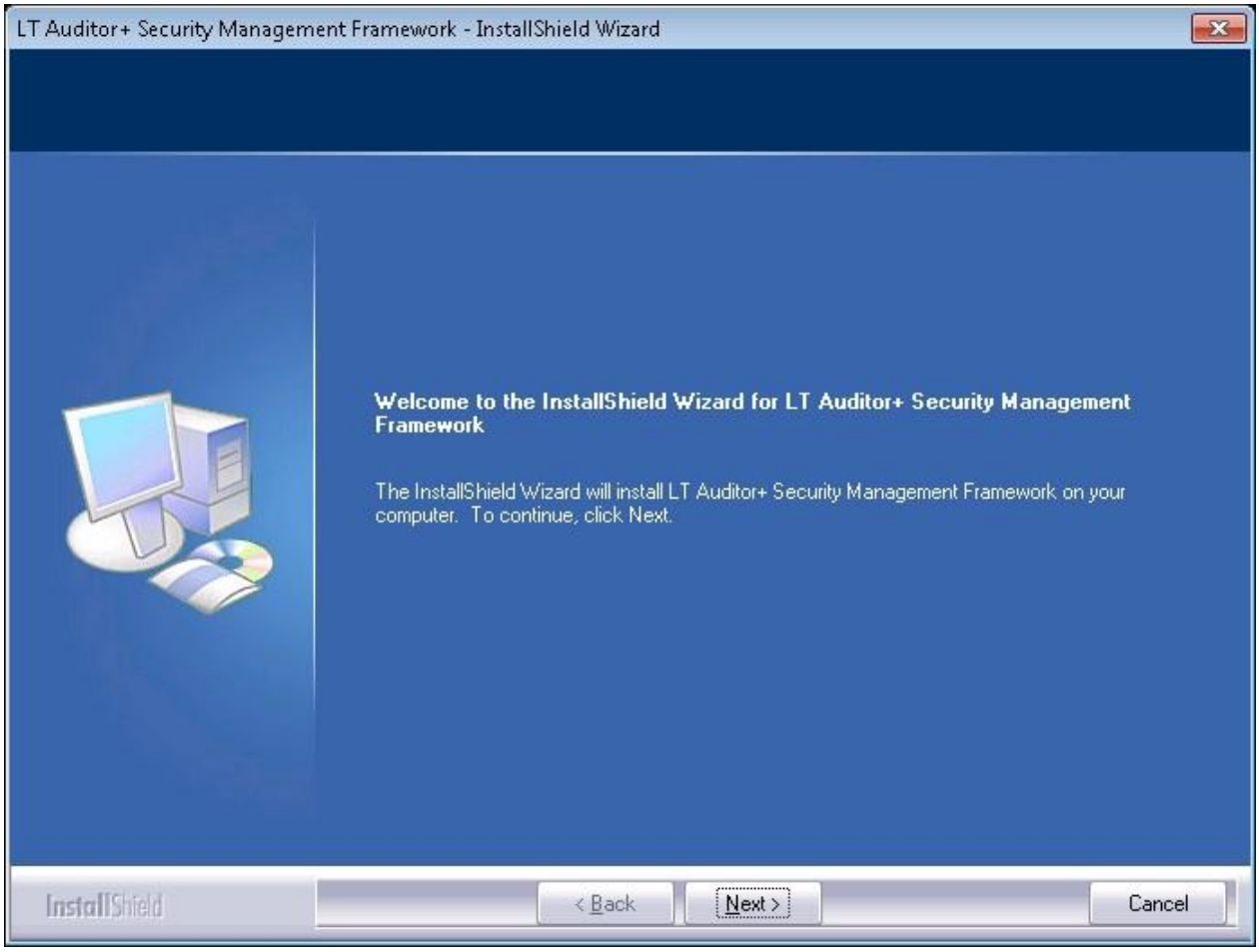
Installation Steps

To install the LT Auditor+ Manager, use the following executable file:

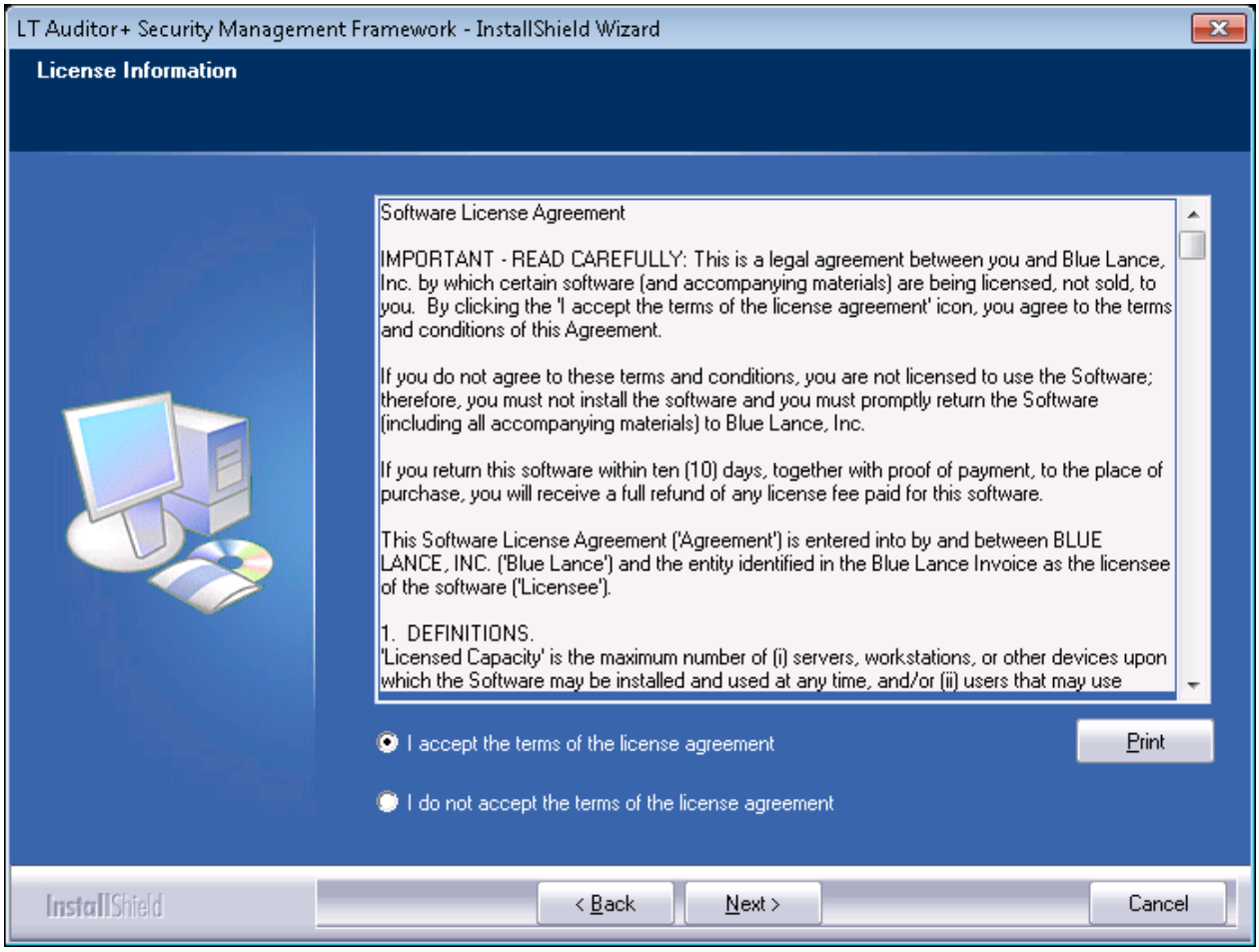
- **Setup_SMF_x64.exe** —Windows 64-bit operating systems

In this section, the term Setup.exe will be used to refer to Setup_SMF_64.exe or Setup_SMF_x86.exe.

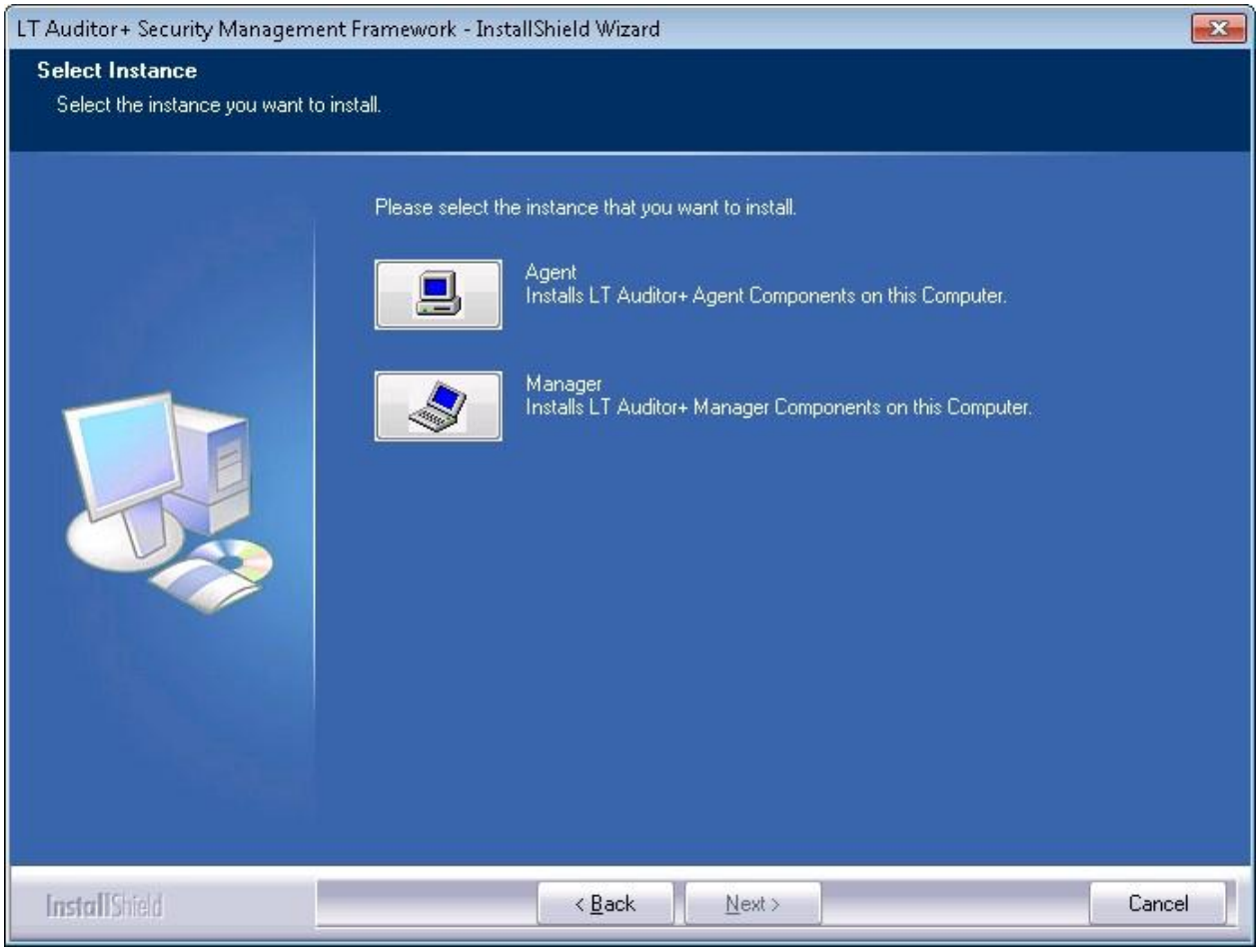
1. Run Setup.exe file from the root of the installation folder to launch the installation of the LT Auditor+ Manager.



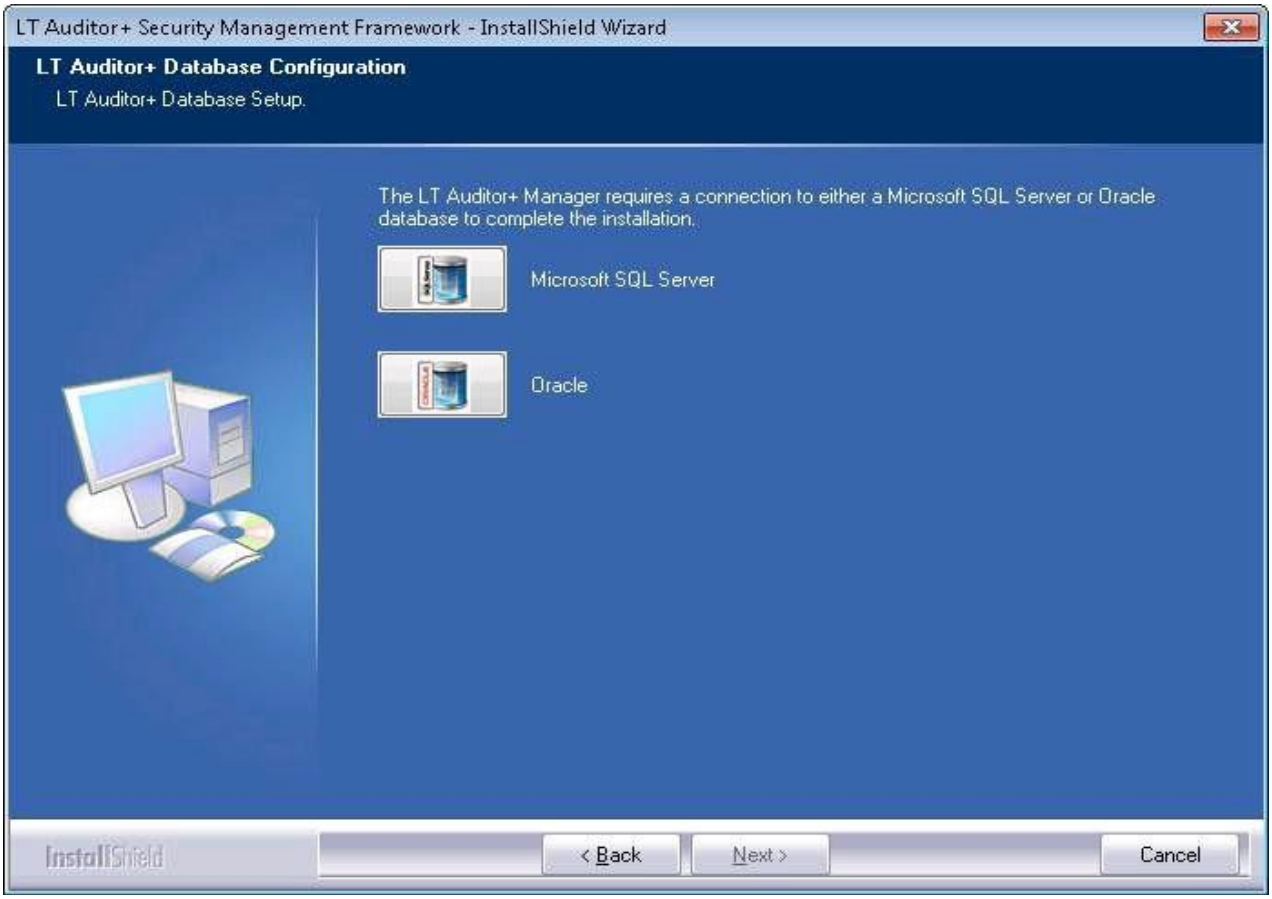
2. Click Next to bring up the License Information screen.



3. Please read the license and if acceptable click on "I accept the terms of the license agreement."
4. Click Next to proceed. There will be a prompt to select installation of a manager or agent on the machine.

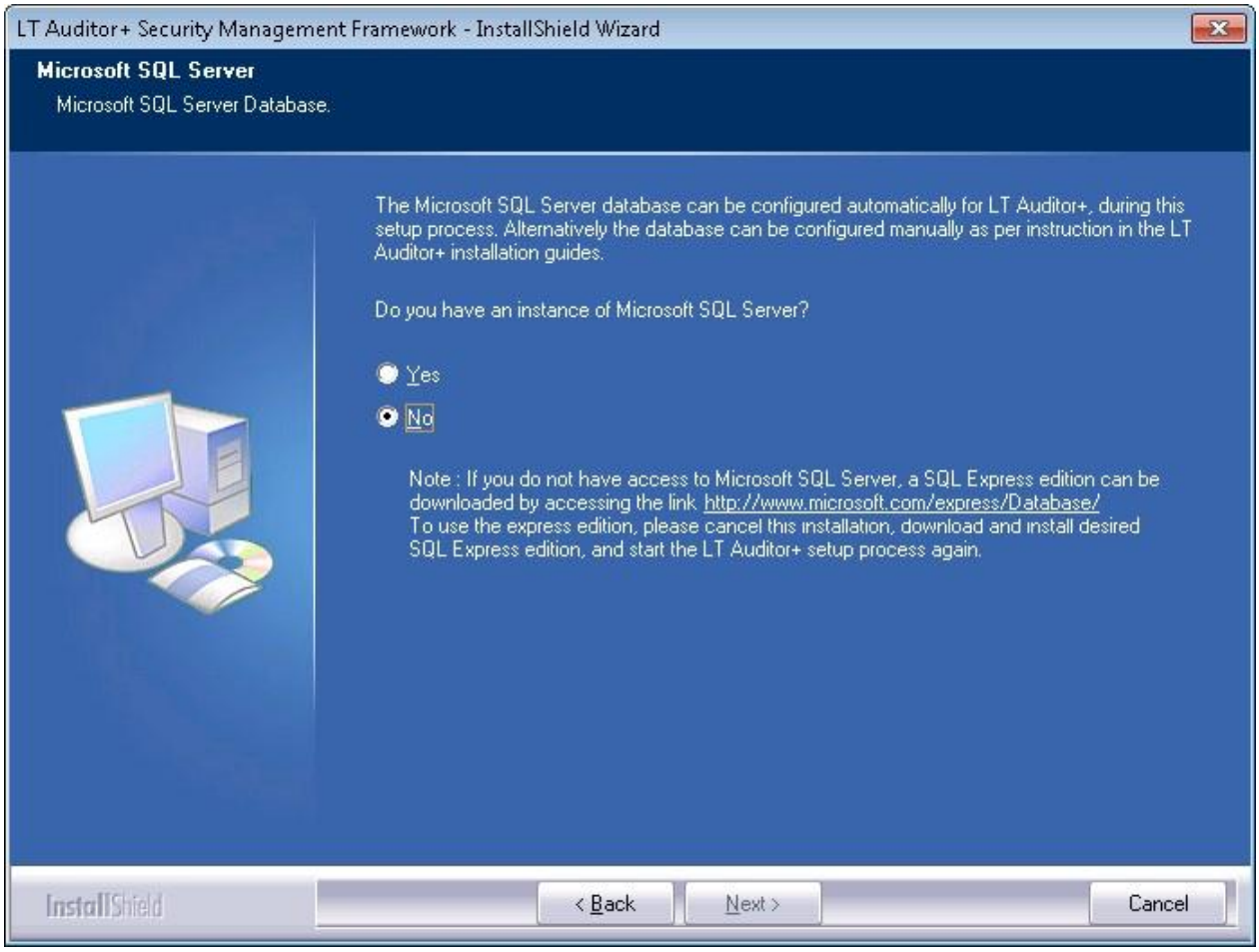


5. Click Manager to display the database setup screen.



6. Select a database for the LT Auditor+ Manager and click Next to continue. This manual will assume that Microsoft SQL Server has been selected.

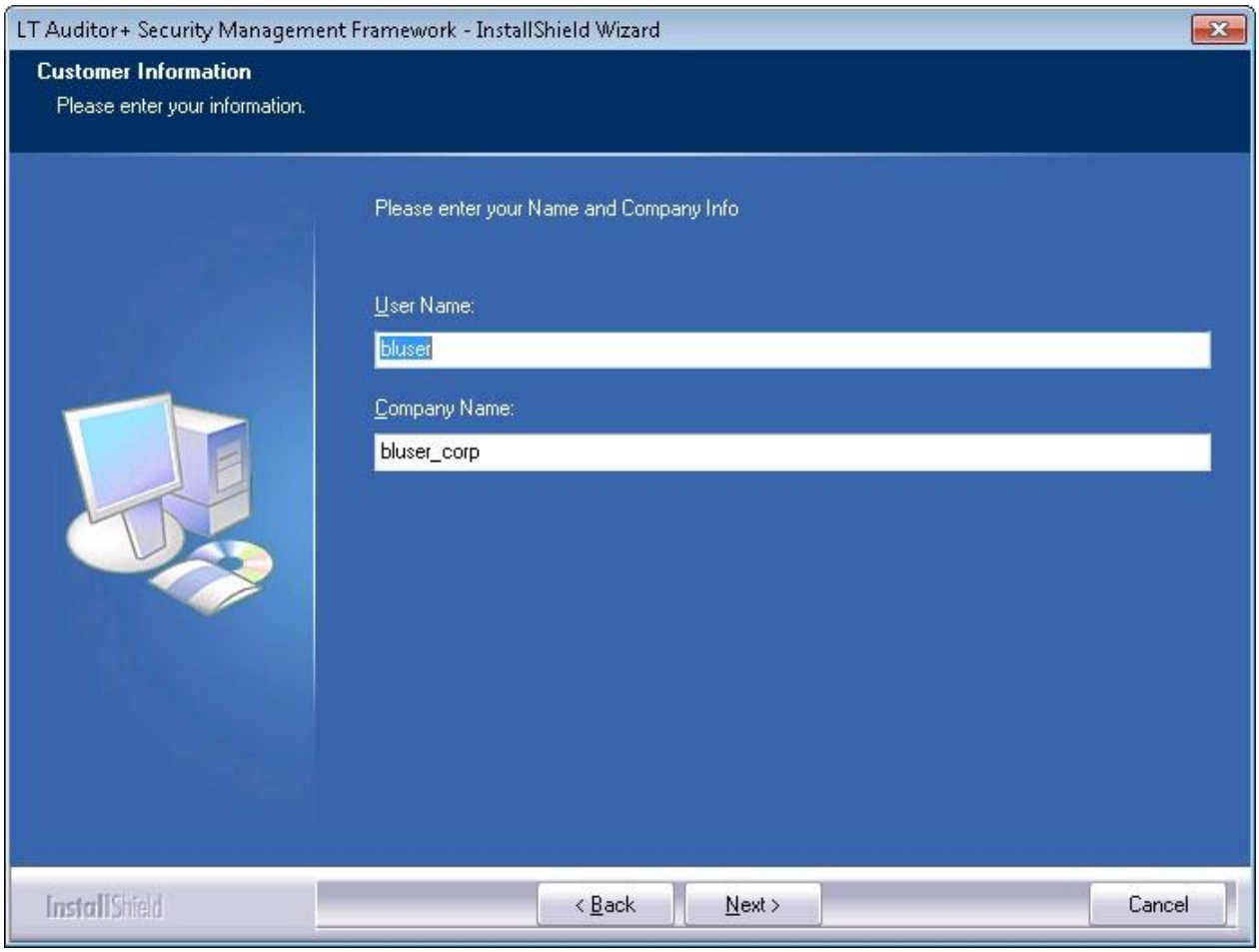
NOTE For Oracle, please ensure that the LT Auditor+ Database has been created, as outlined in "Appendix A," prior to clicking on the Next button.



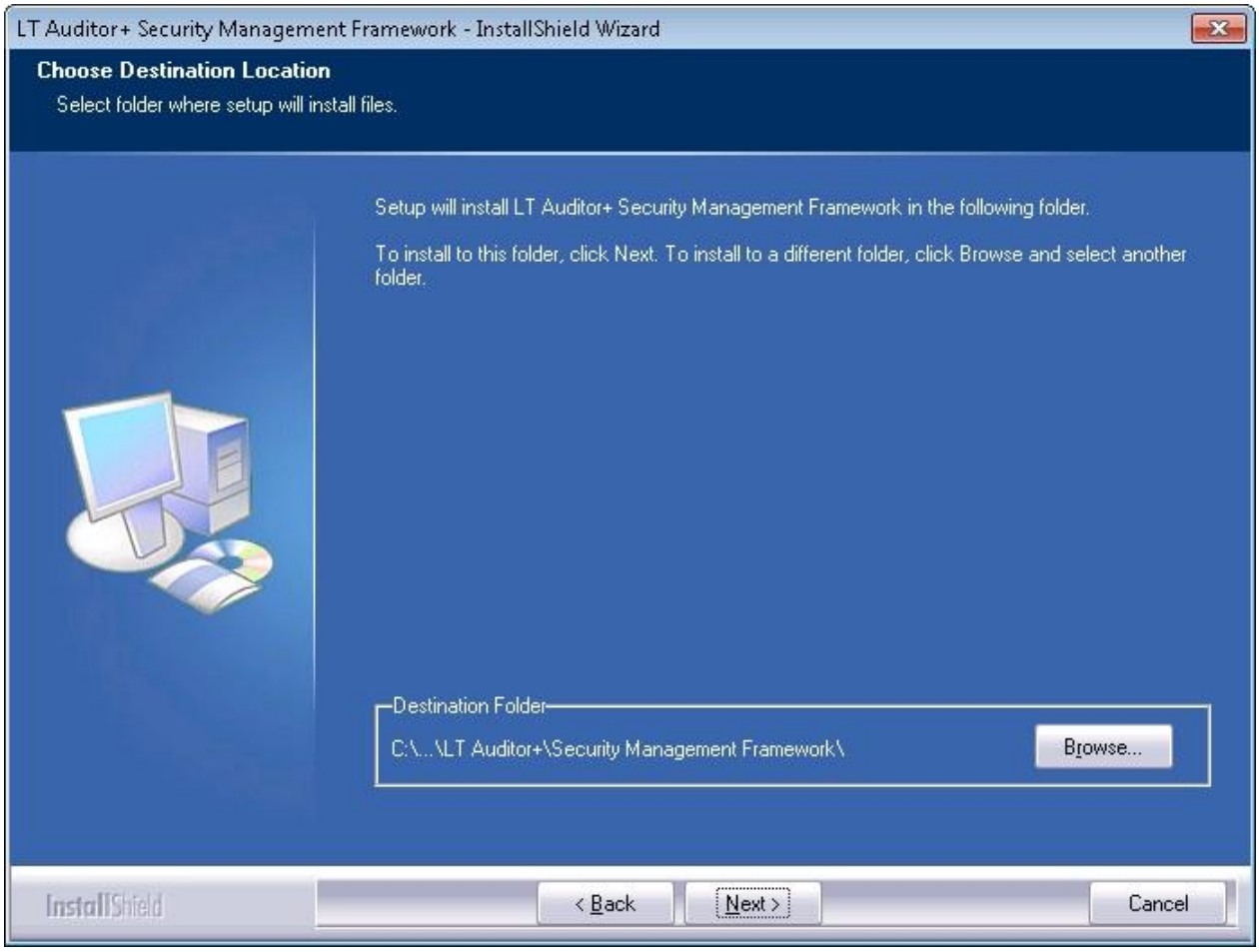
7. Click Yes to proceed to the Customer Information screen.

NOTE If an instance of Microsoft SQL Server is not available, a free Microsoft SQL express edition can be downloaded from http:/www.microsoft.com/express/Database/

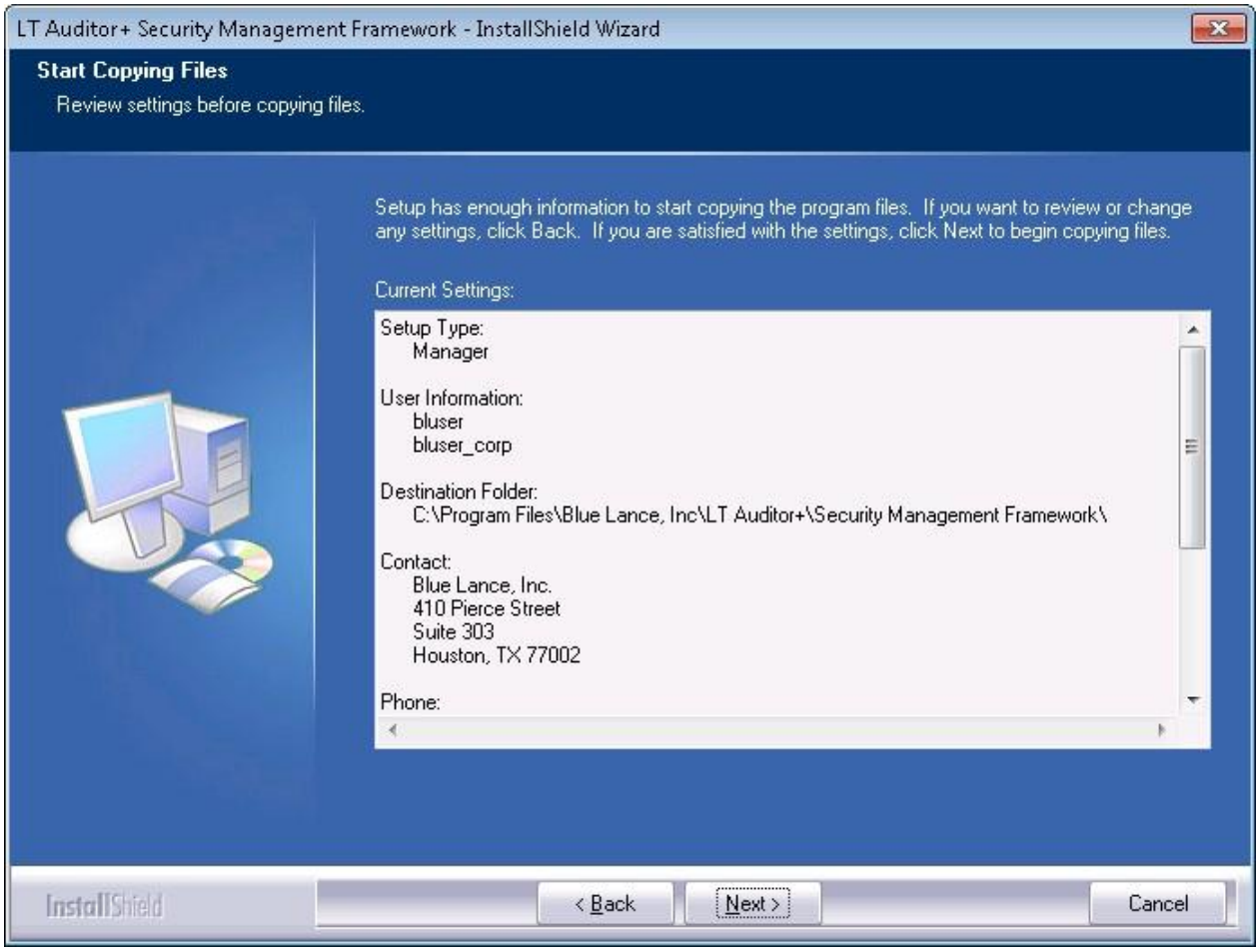
We do not recommend that the express edition be used for production due to limitations in the size of the database growth permitted.



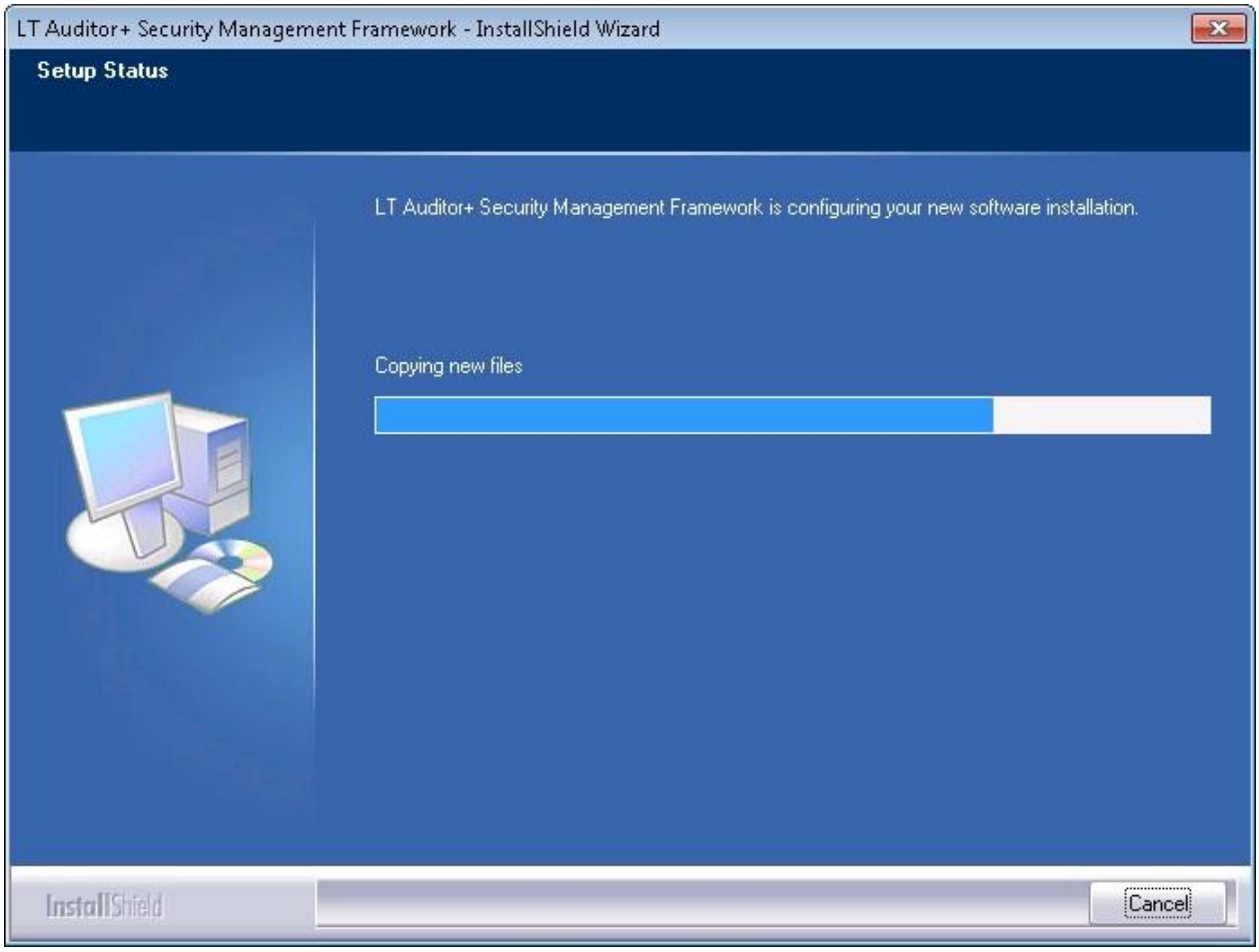
8. Enter your name and company information.
9. Click Next.



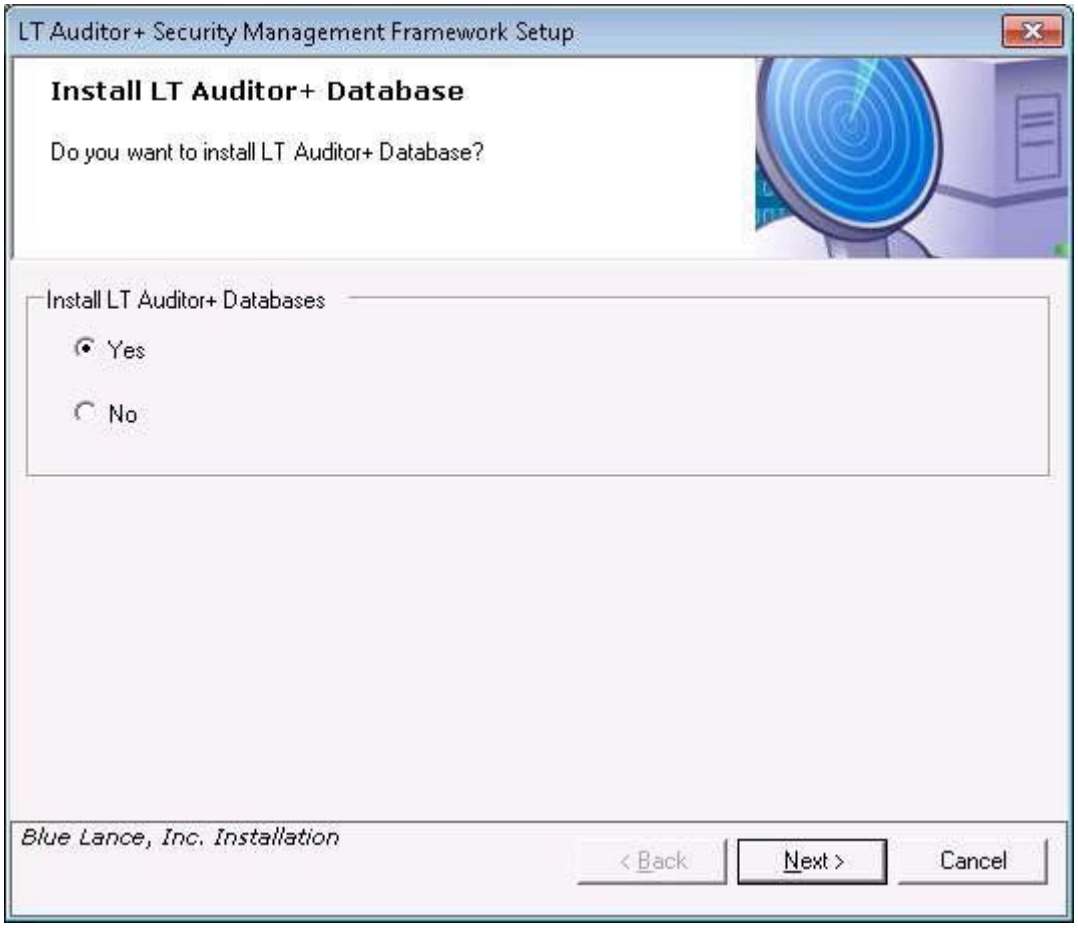
10. Click Next if the destination location is satisfactory; otherwise, click Browse to select a new location.



11. Review the specified settings.
12. Click Back to make any changes; otherwise, click Next.



13. Progress will be shown as the files are copied to the selected location. After the files have been copied, the installation progresses to the database setup screens.

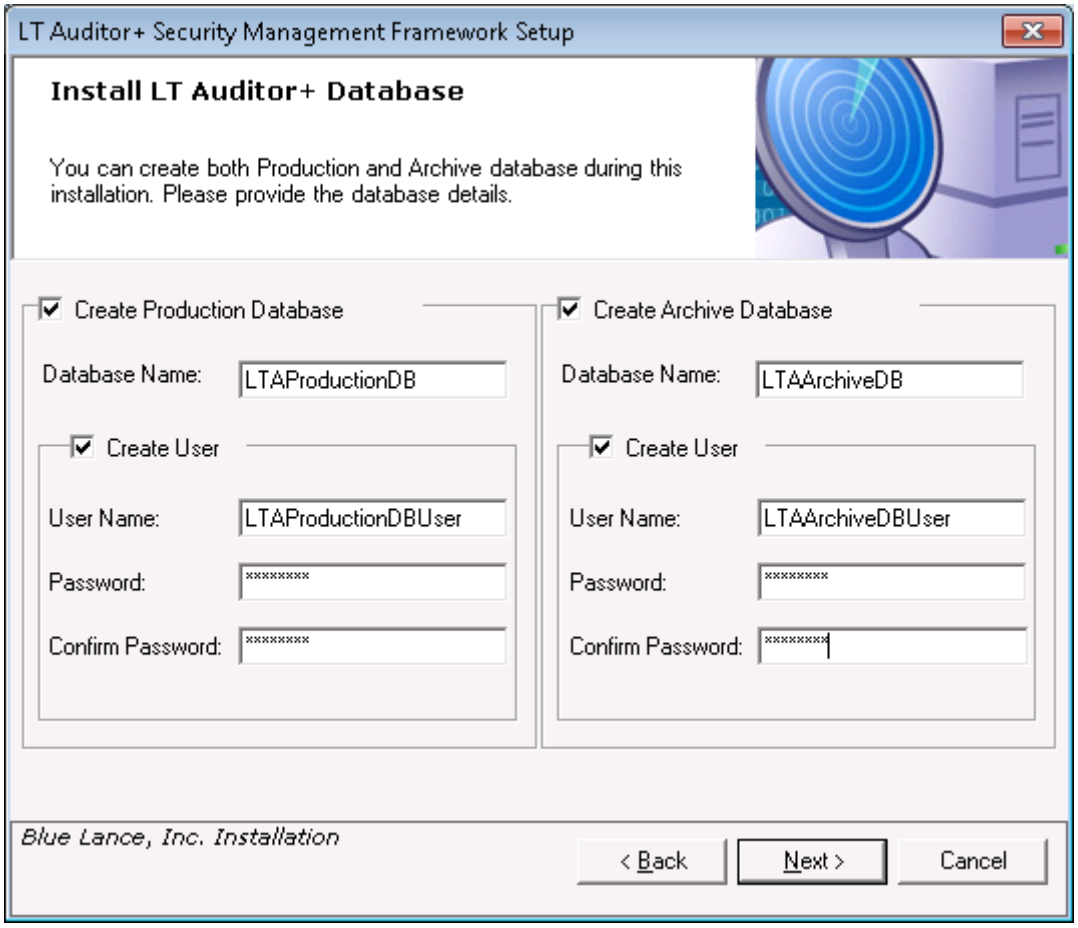


14. Select No if the LT Auditor+ databases have already been created and proceed to step 23 for setting up Database Connection Information. Select Yes if you want to create the LT Auditor+ databases (for Microsoft SQL Server only). The next screens deal with connecting to the Microsoft SQL Server and creating these databases.

NOTE

For Oracle, the databases must be created manually prior to this installation process. For Microsoft SQL Server, the LT Auditor+ databases can also be created manually, as specified in "APPENDIX A," or through this setup program by clicking Yes above.

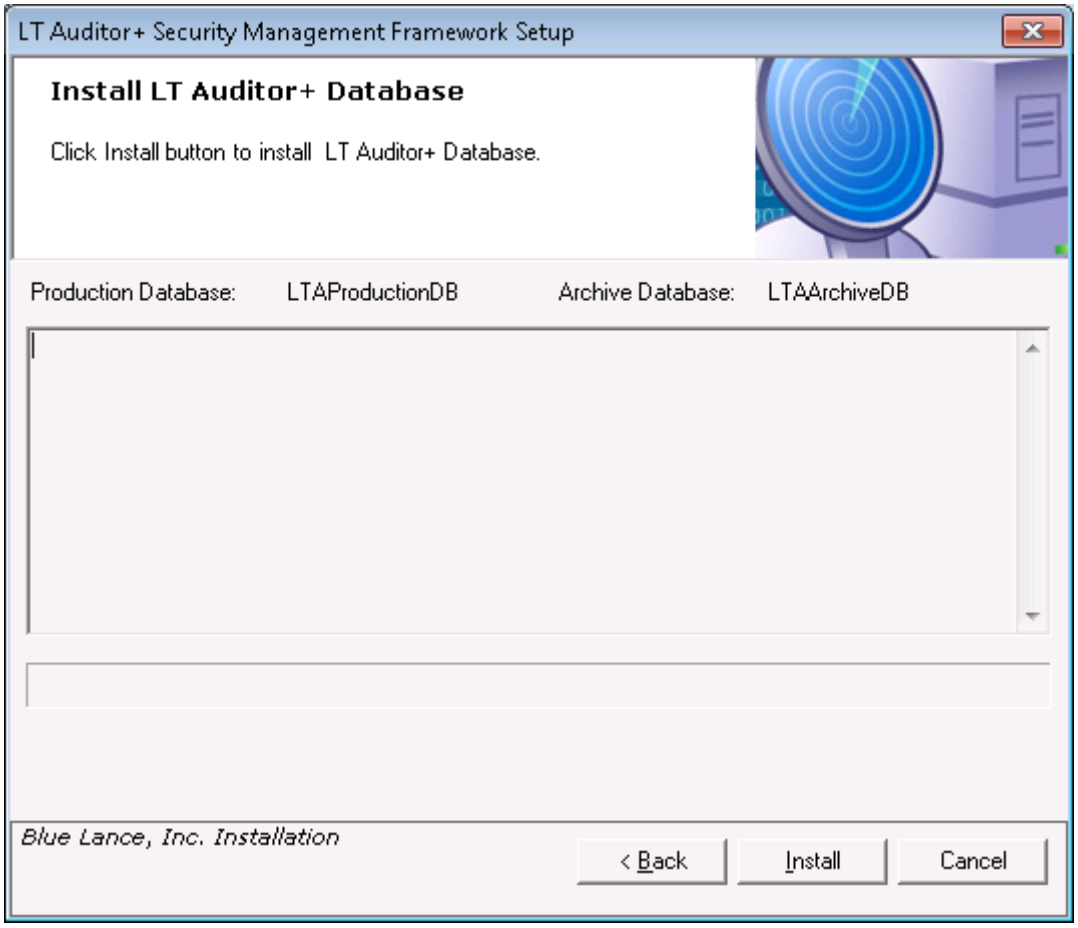
15. Specify the database server name.
16. The connection mode. For Windows authentication, the current user should have the appropriate credentials on the SQL server; otherwise, select a database user. Use the Test Connection button to check the credentials.
17. Click Next to proceed.



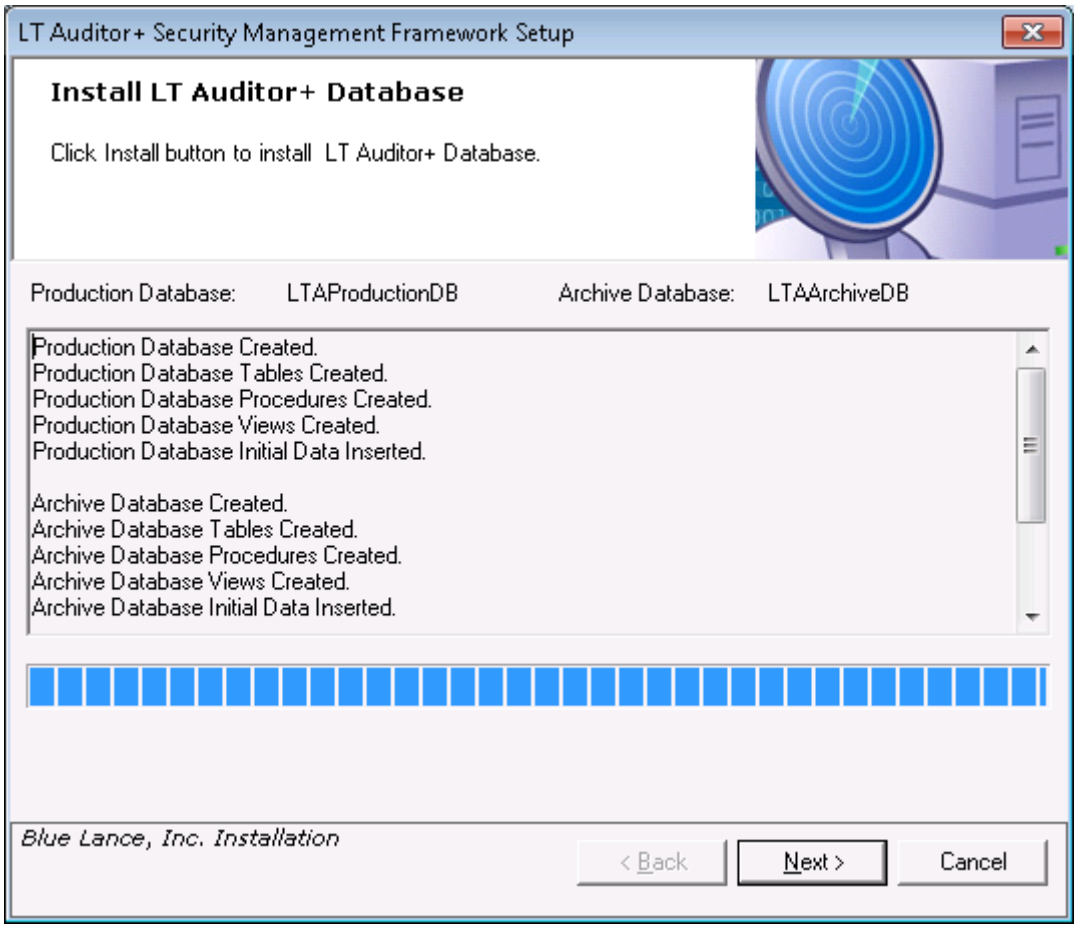
18. If you choose to create a database user for each LT Auditor+ database, enter a password. It is not necessary to have a database user created, and if you choose not to, uncheck the Create User check boxes.
19. Click Next to proceed.

NOTE

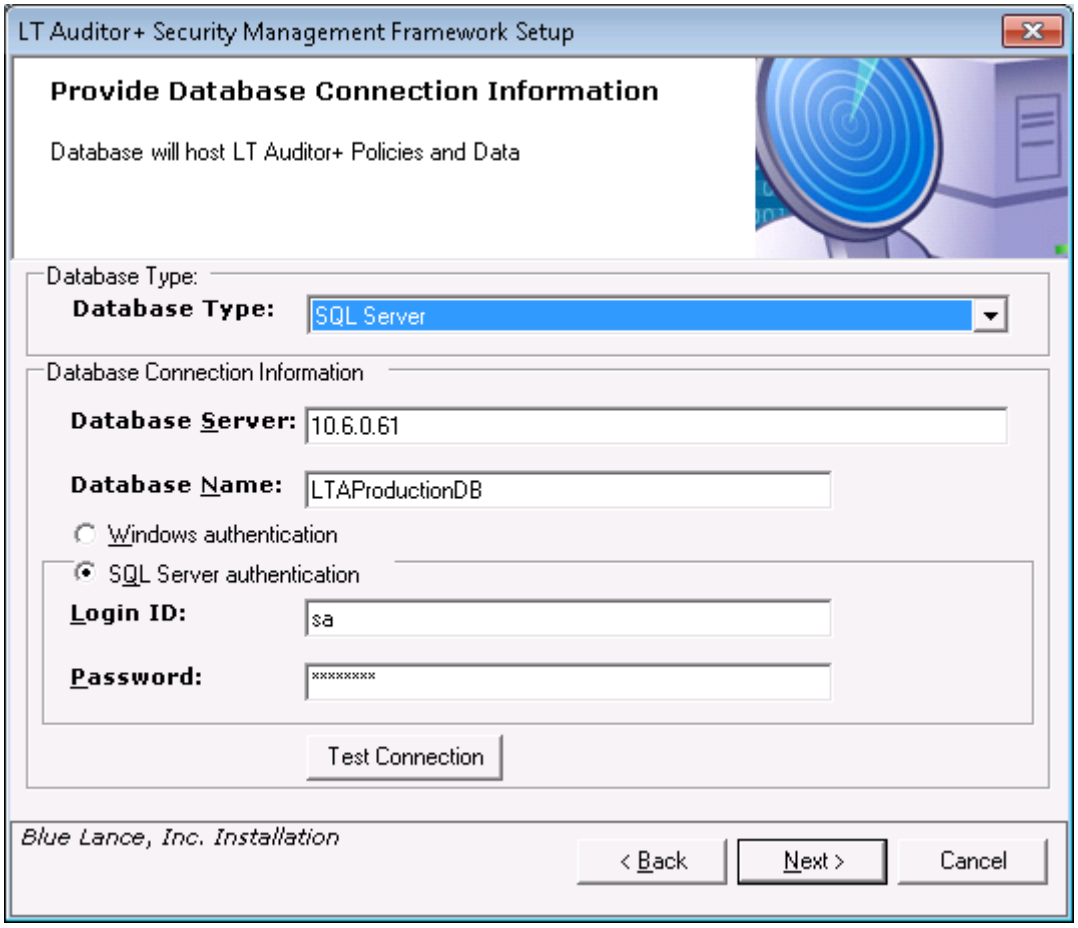
Password complexity requirements may have to be met.



20. Click Install to create the LT Auditor+ databases as shown below.

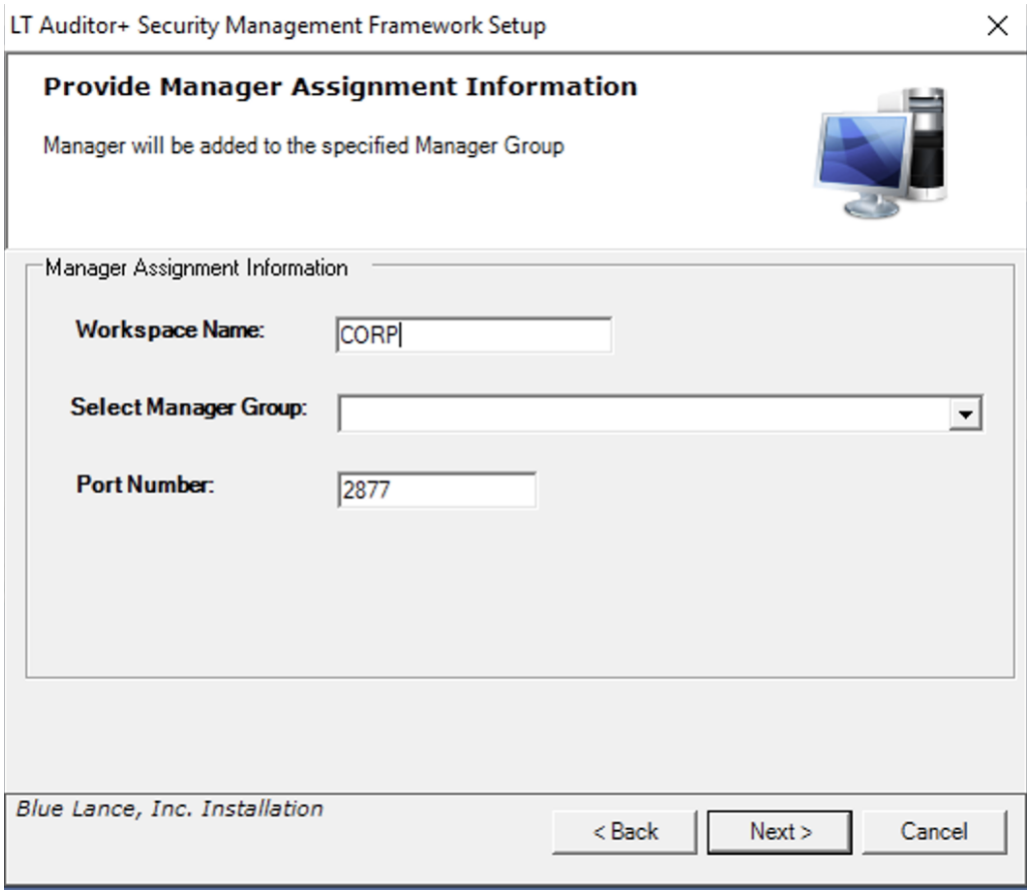


21. Click Next to proceed to the Database Connection Window.

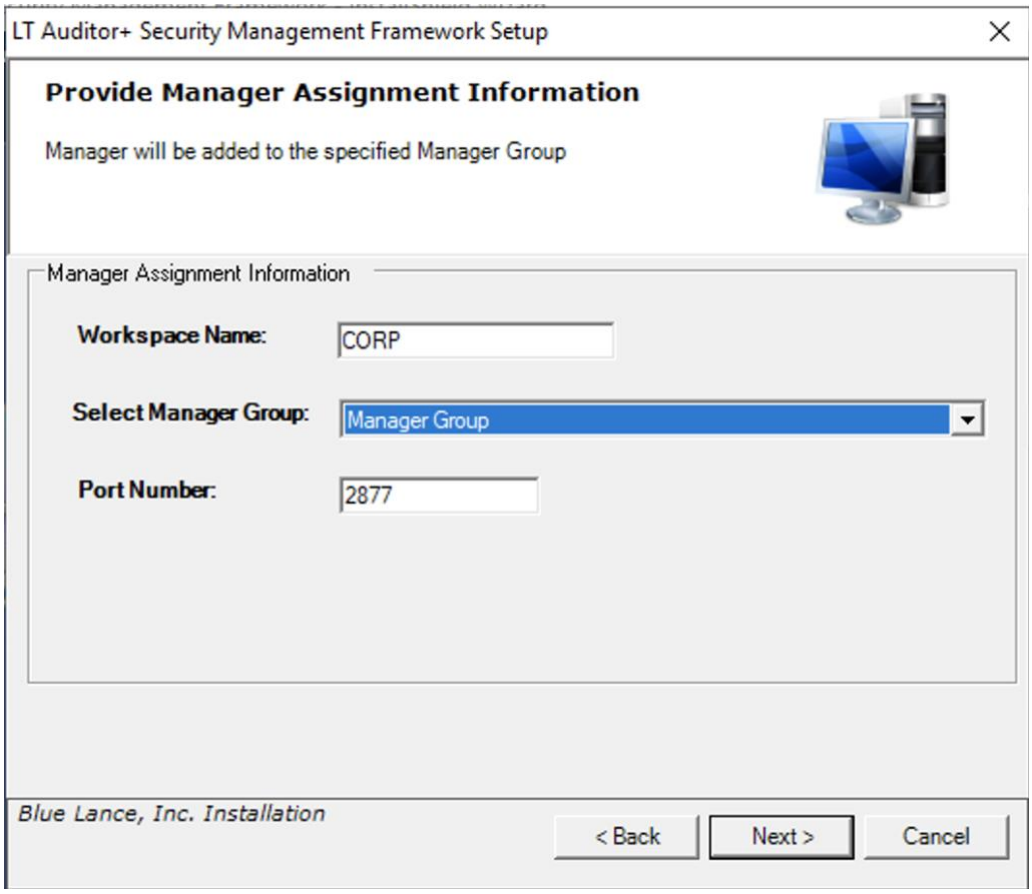


22. Select the Database Type.
23. Select the Database Server.
24. Select the name of the primary LT Auditor+ database. The default is LTAProductionDB.
25. Select the mode of database authentication.
26. If using a database user, enter the login username and password.
27. Click Test Connection to ensure that there is a valid connection.
28. Click Next to continue.

NOTE For database type selection of Oracle, you will be prompted to enter the host string, username and password. The credentials used here will be used by the LT Auditor+ Manager Windows service to connect to the LT Auditor+ database.



29. Enter a workspace name. (Please review the Terms section above for description of workspace.)
30. Select a manager group. If this is the first LT Auditor+ Manager, click New to add a new manager group and enter a new group name.
31. Type in 2877 for the port number.
32. Enter the serial number or click on the Trial check box as shown below.

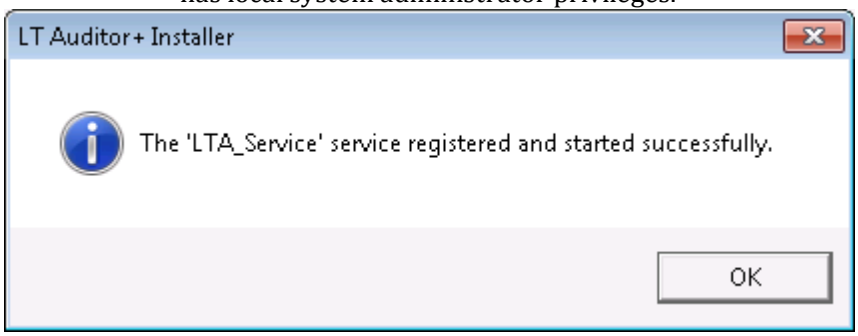


33. Click Next to continue.

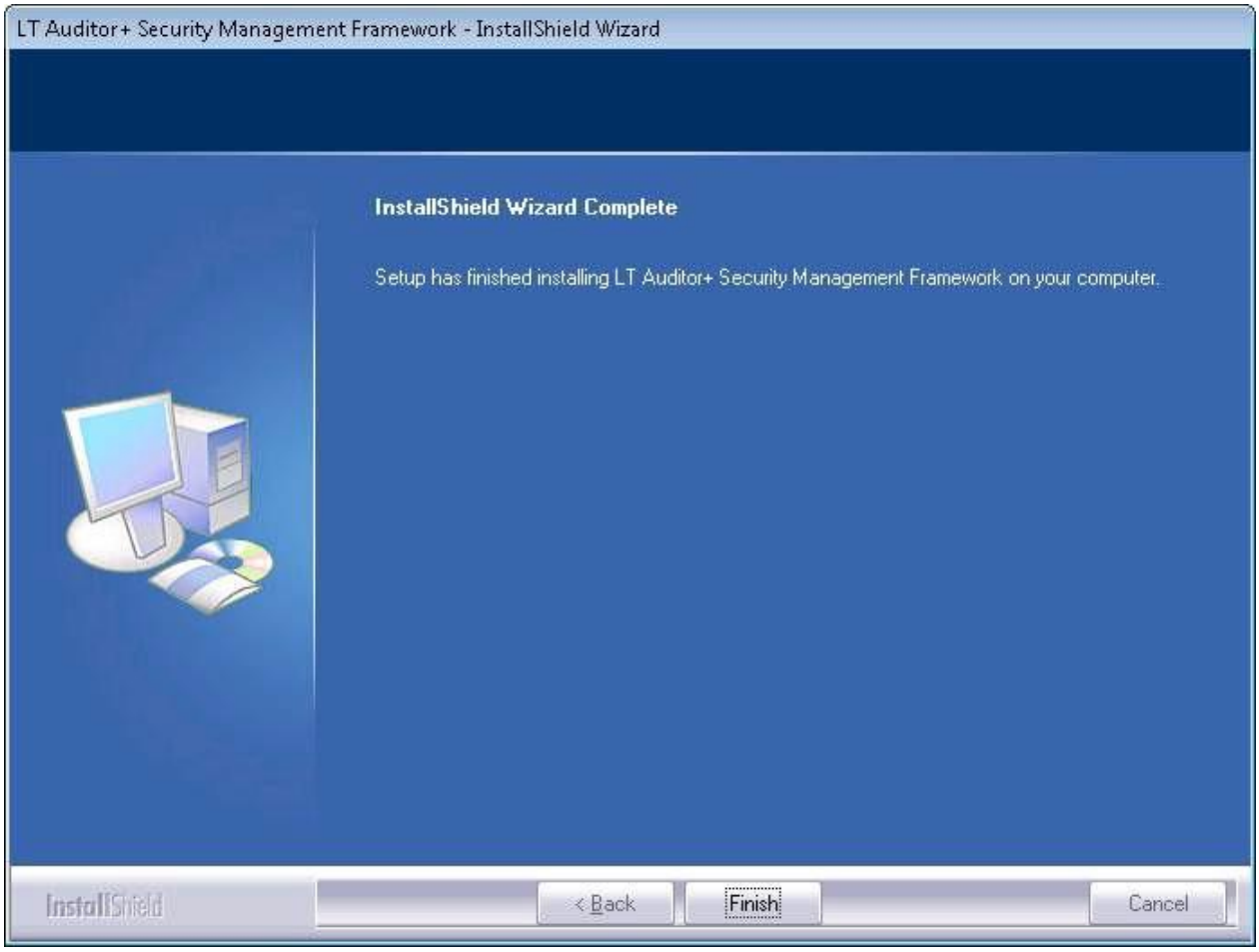
34. Click Local System Account for the LT Auditor+ service to use the local system account; otherwise, enter credentials to log on as a specified account.
35. Click Next for service registration.

NOTE

When the LT Auditor+ service uses a specific account, it is recommended that this account has local system administrator privileges.



36. Click OK to continue to the Wizard Complete screen.



37. Click Finish to complete the installation of the LT Auditor+ Manager.

Installing LT Auditor+ Manager Console

The LT Auditor+ Manager Console or Management Console is the application used to configure policies and manage Windows agents. It can be installed on any Windows workstation or server. Please review the Configuration Guide for instructions on how to use this application.

Prerequisites for the LT Auditor+ Manager Console Installation

- Meet the system requirements outlined above.
- Installer must have administrative privileges to install on Windows machine.

Installation Steps

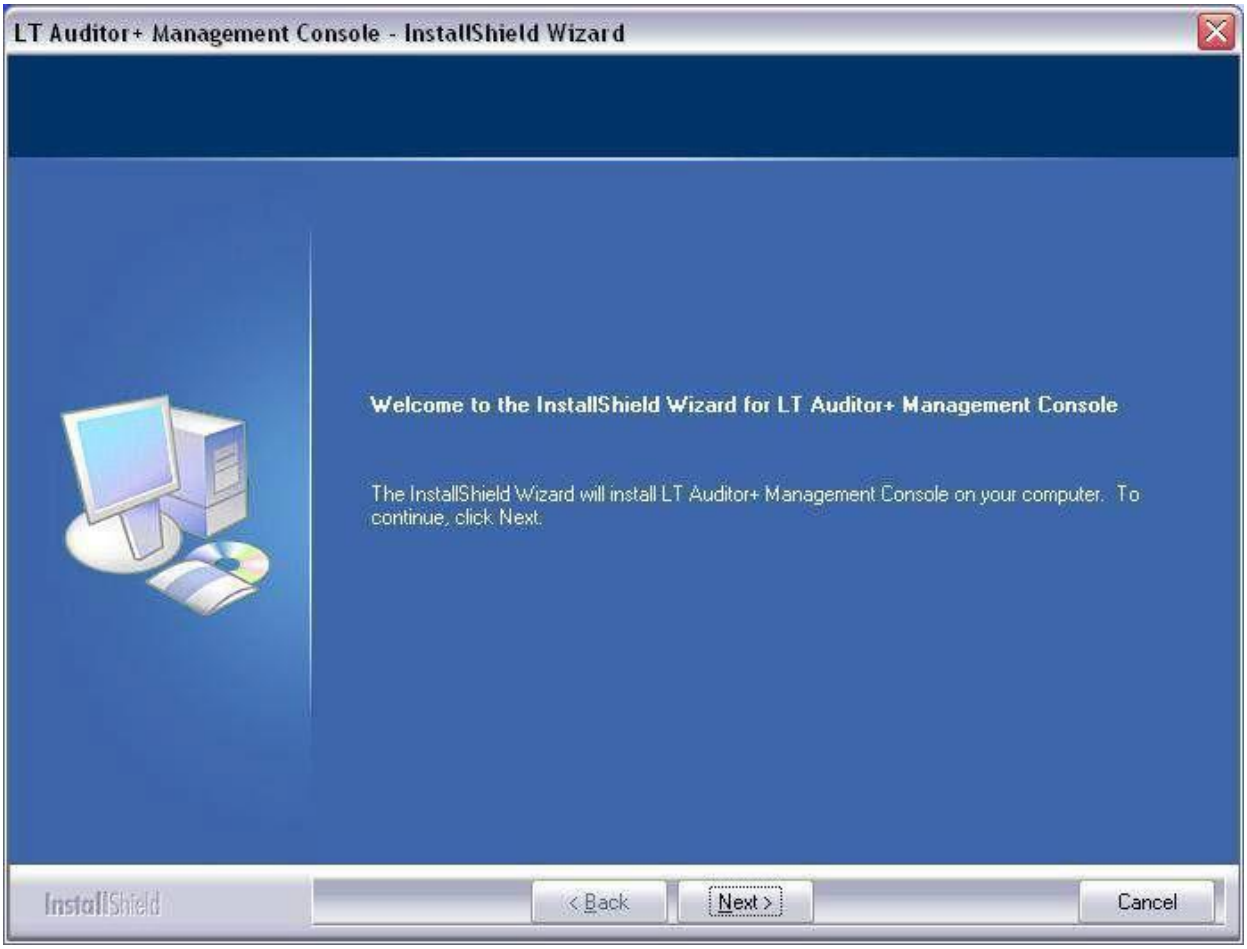
To install the LT Auditor+ Manager Console, use the following executable file

- Setup_MC_x64.exe - Windows 64bit operating systems

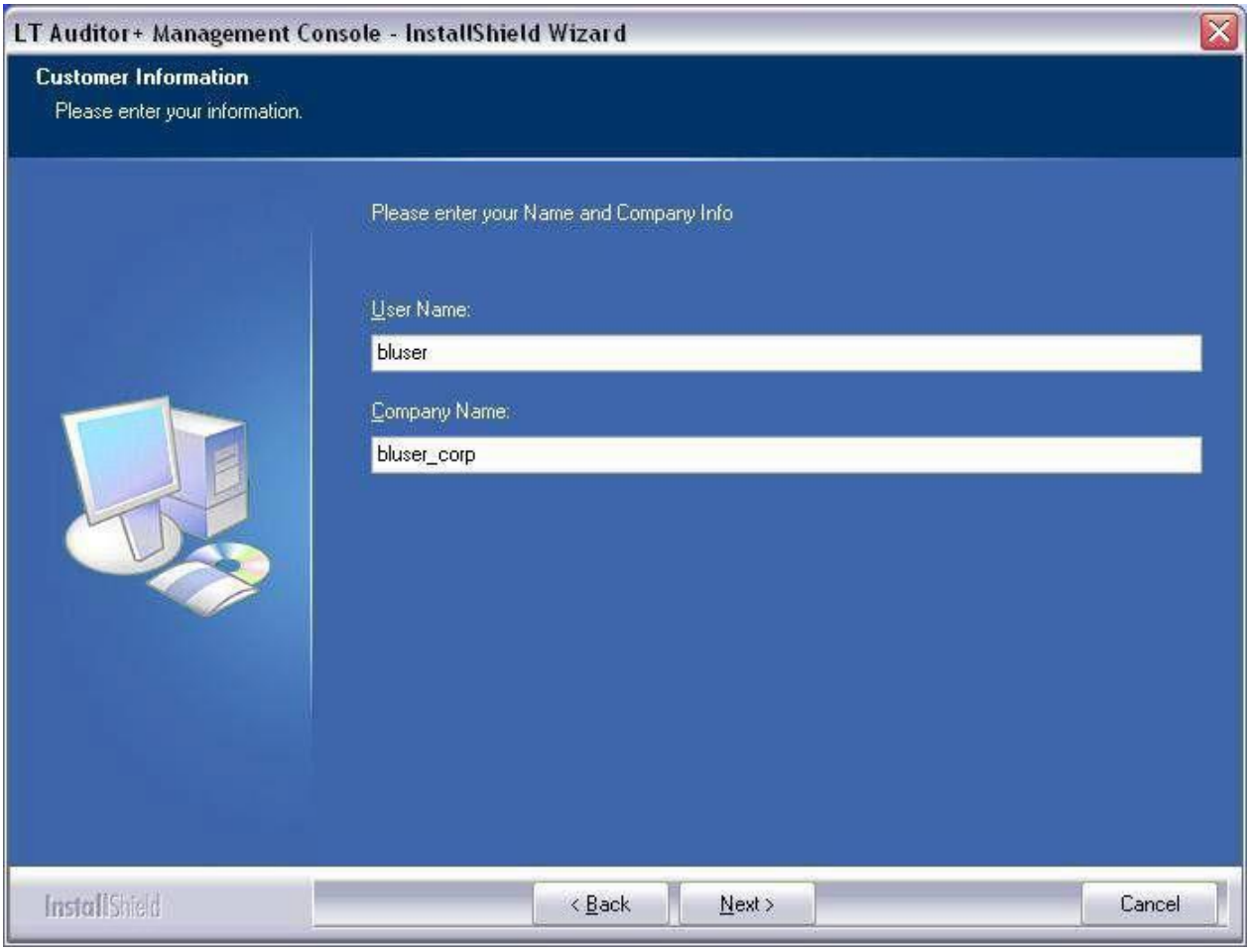
In this section, the term Setup.exe will be used to refer to Setup_MC_64.exe.

1. Run Setup.exe file from the root of the installation folder to launch the installation of the LT Auditor+ Manager Console.

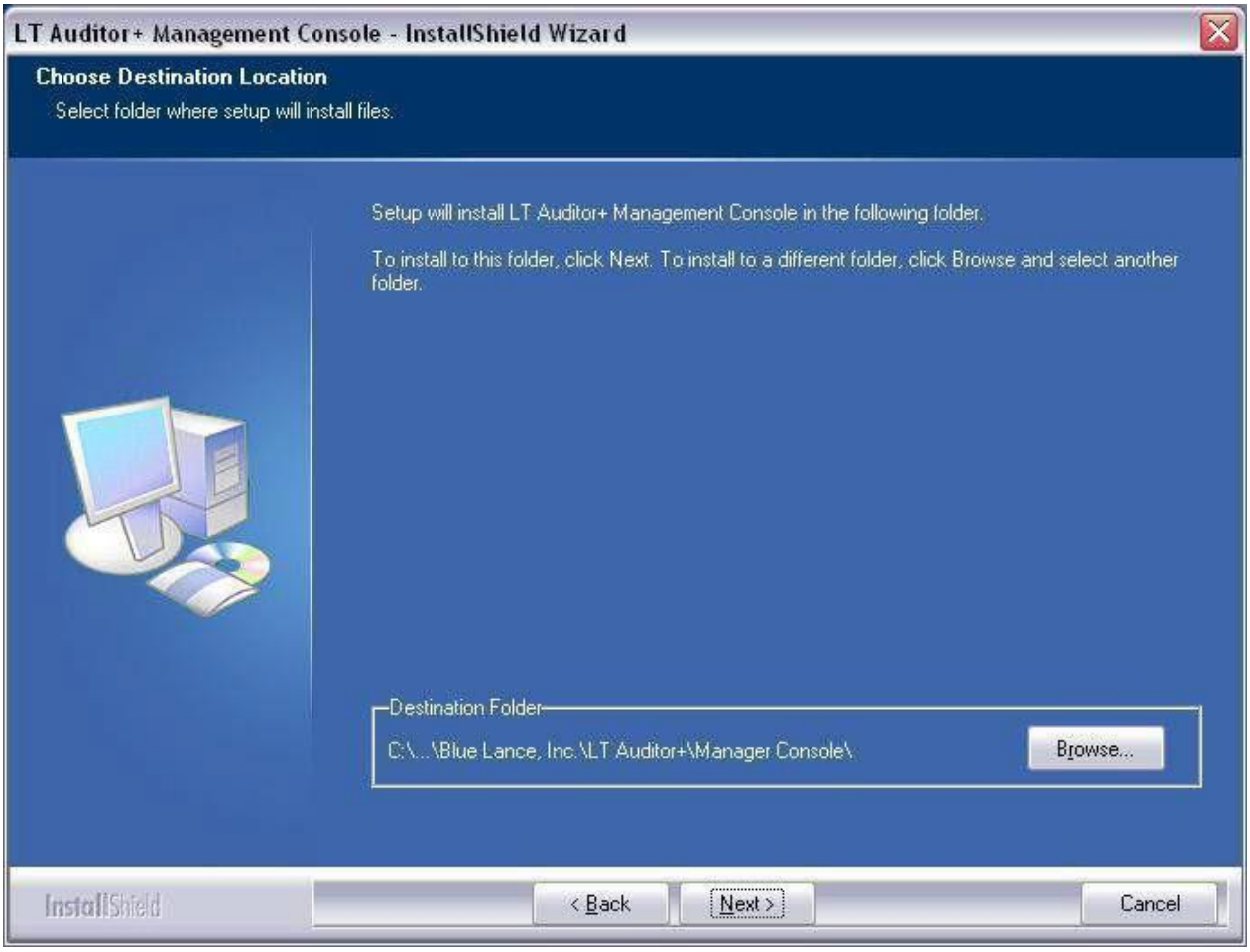
If the application detects that Microsoft .NET 4.0 is not installed on the machine, the wizard will prompt you with a message to install. After Microsoft .NET 4.0 is installed, the welcome screen will be shown.



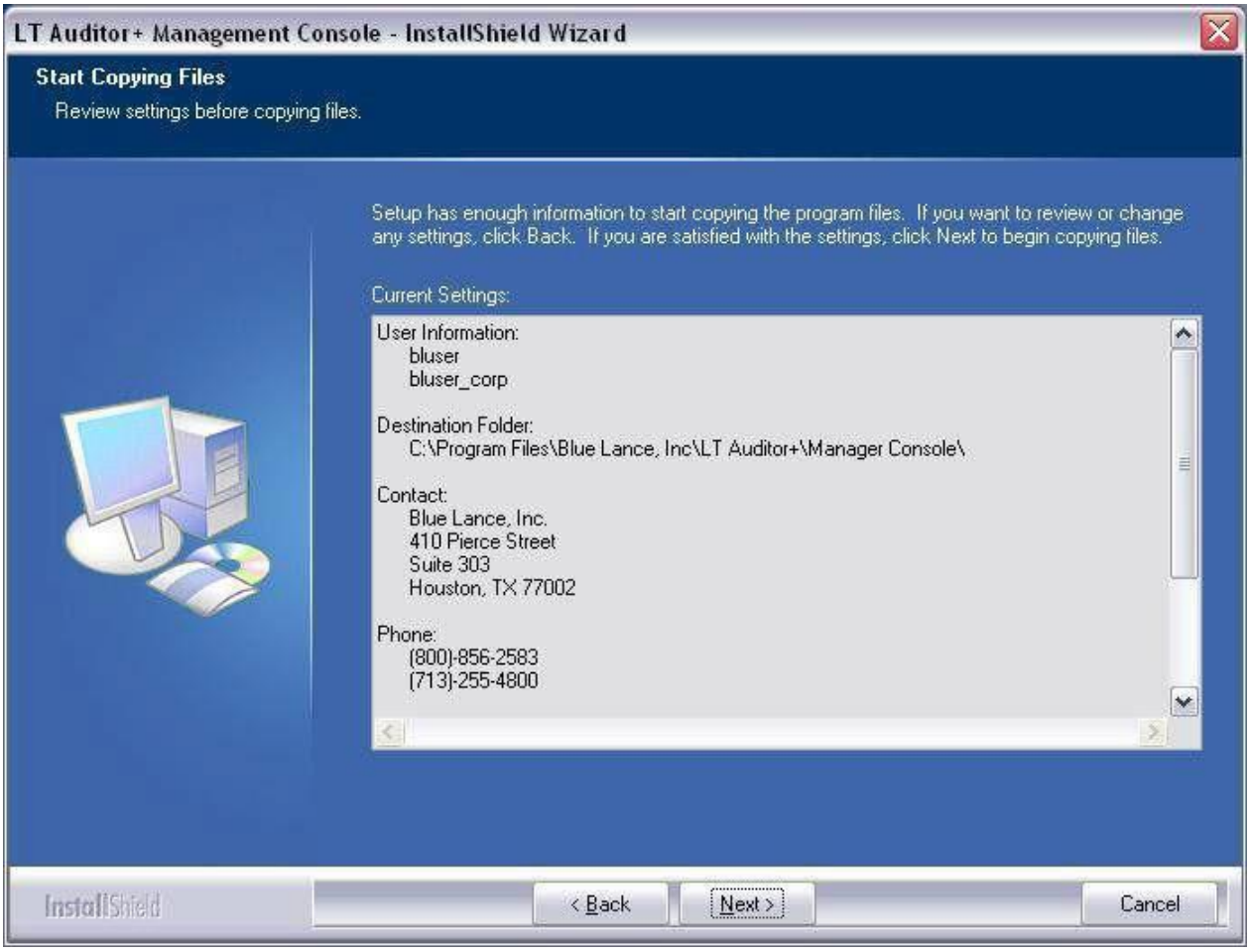
2. Click Next to continue to Customer Information screen.



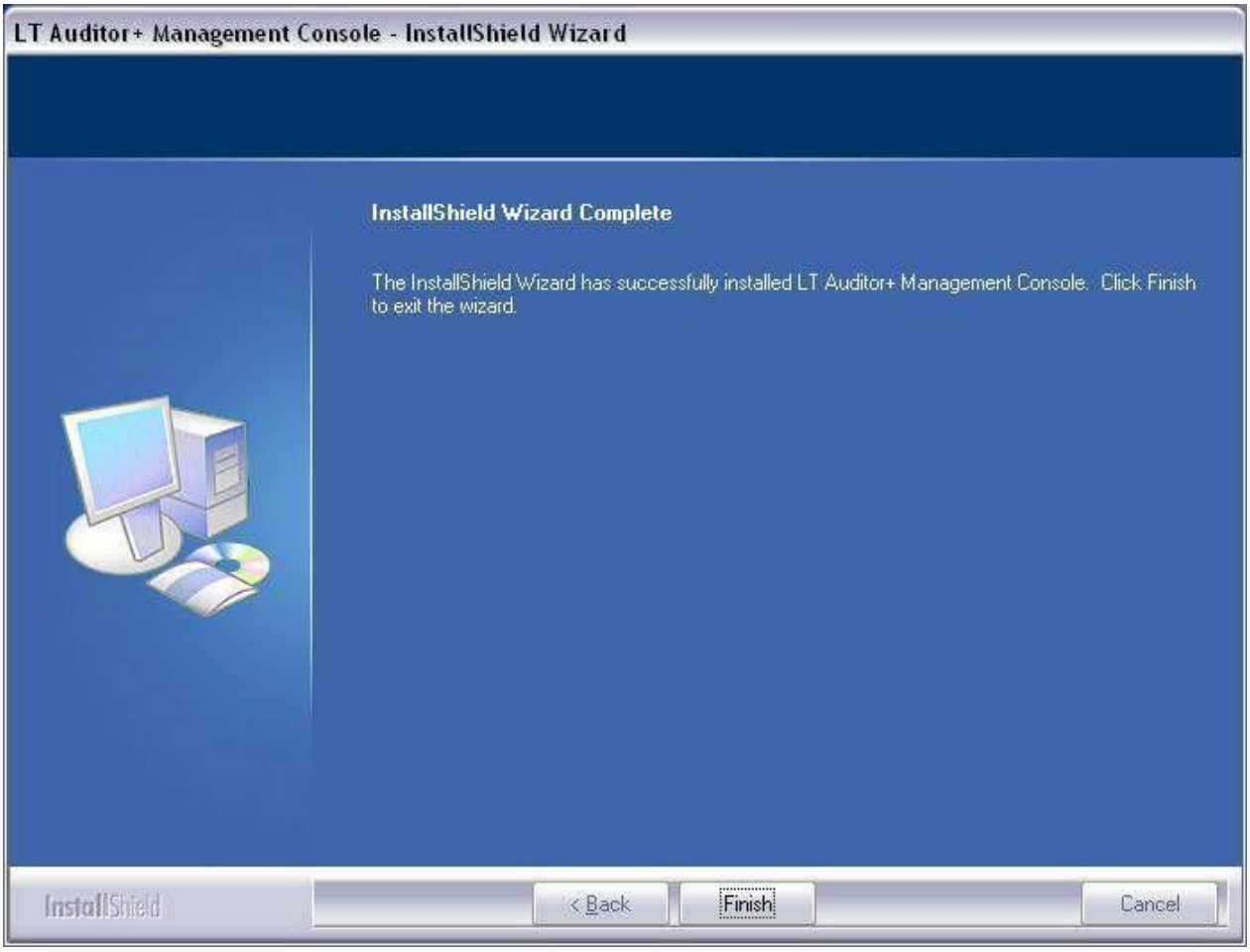
3. Enter your name and company information.
4. Click Next.
5. This will display Choose Destination Location as shown below.



6. By default, the product will be installed in the folder C:\Program Files\Blue Lance, Inc.\LT Auditor+\Manager Console\
7. Click Browse to change the install path.
8. Click Next. The review creen will be displayed as shown below.



9. Review the information selected.
10. If there are any changes that need to be made, click Back and make corrections. Otherwise, click Next to start copying files onto the machine.



11. Click Finish to complete installation of the Manager Console.

Installing LT Auditor+ Report Console

The LT Auditor+ Report Console, or Reporting Console, is the application used to report on audit data collected using LT Auditor+.

Prerequisites for the LT Auditor+ Report Console Installation

- Meet the system requirements outlined above.
- Installer must have administrative privileges to install on Windows machine.

Installation Steps

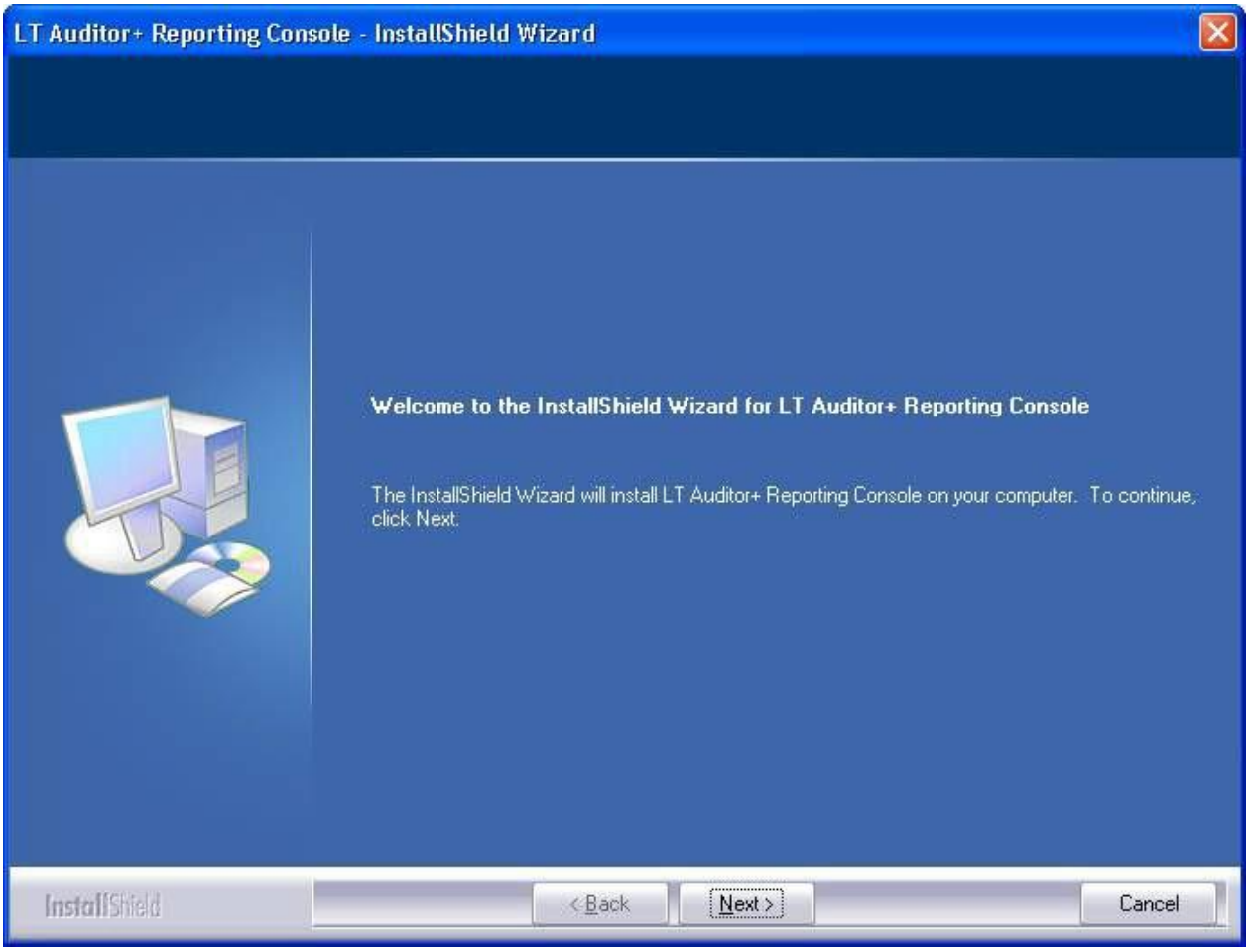
To install the LT Auditor+ Report Console, use the following executable file:

- Setup_RC_x64.exe – Windows 64-bit operating systems

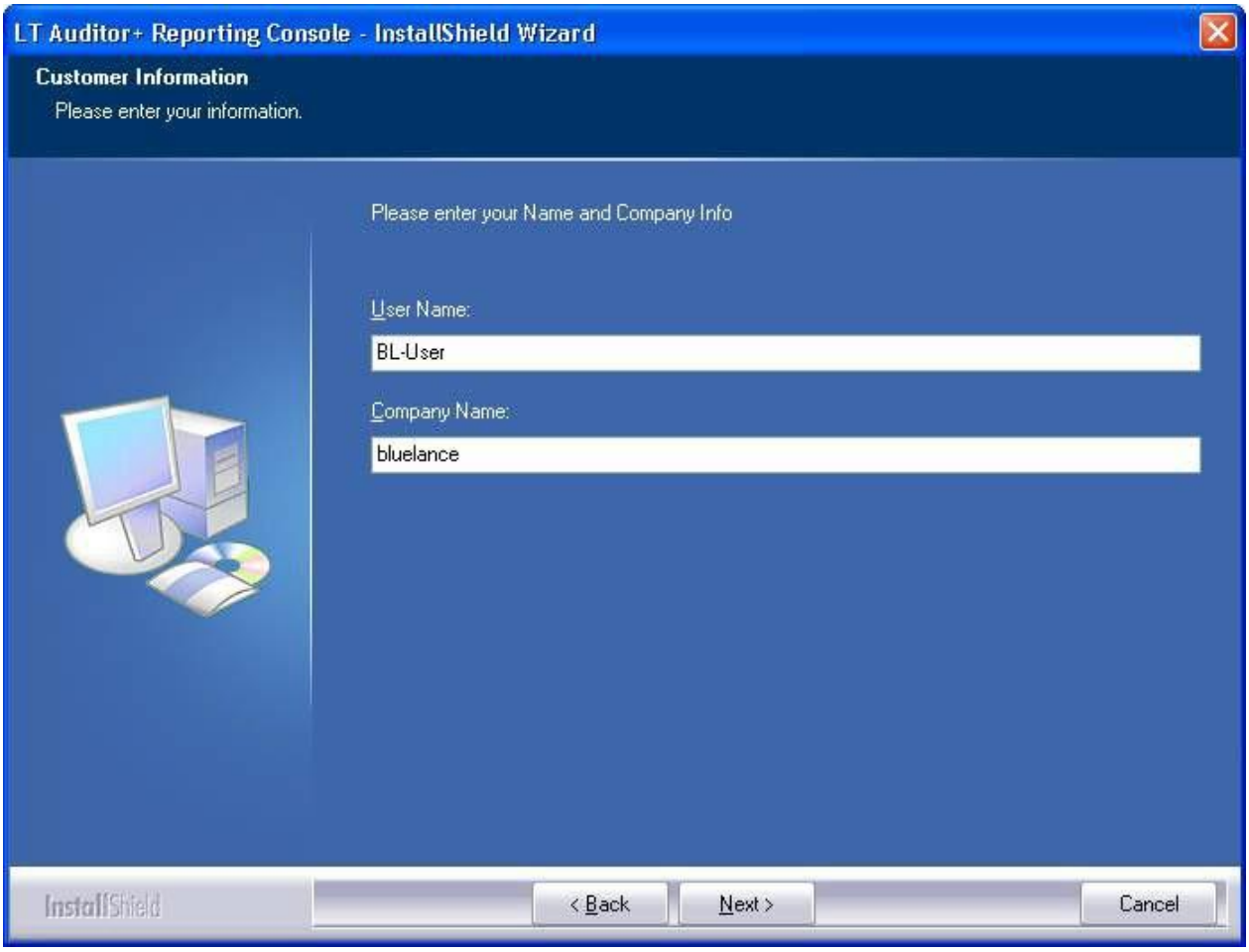
In this section, the term Setup.exe will be used to refer to Setup_RC_64.exe.

1. Run Setup.exe file from the root of the installation folder to launch the installation of the LT Auditor+ Report Console.

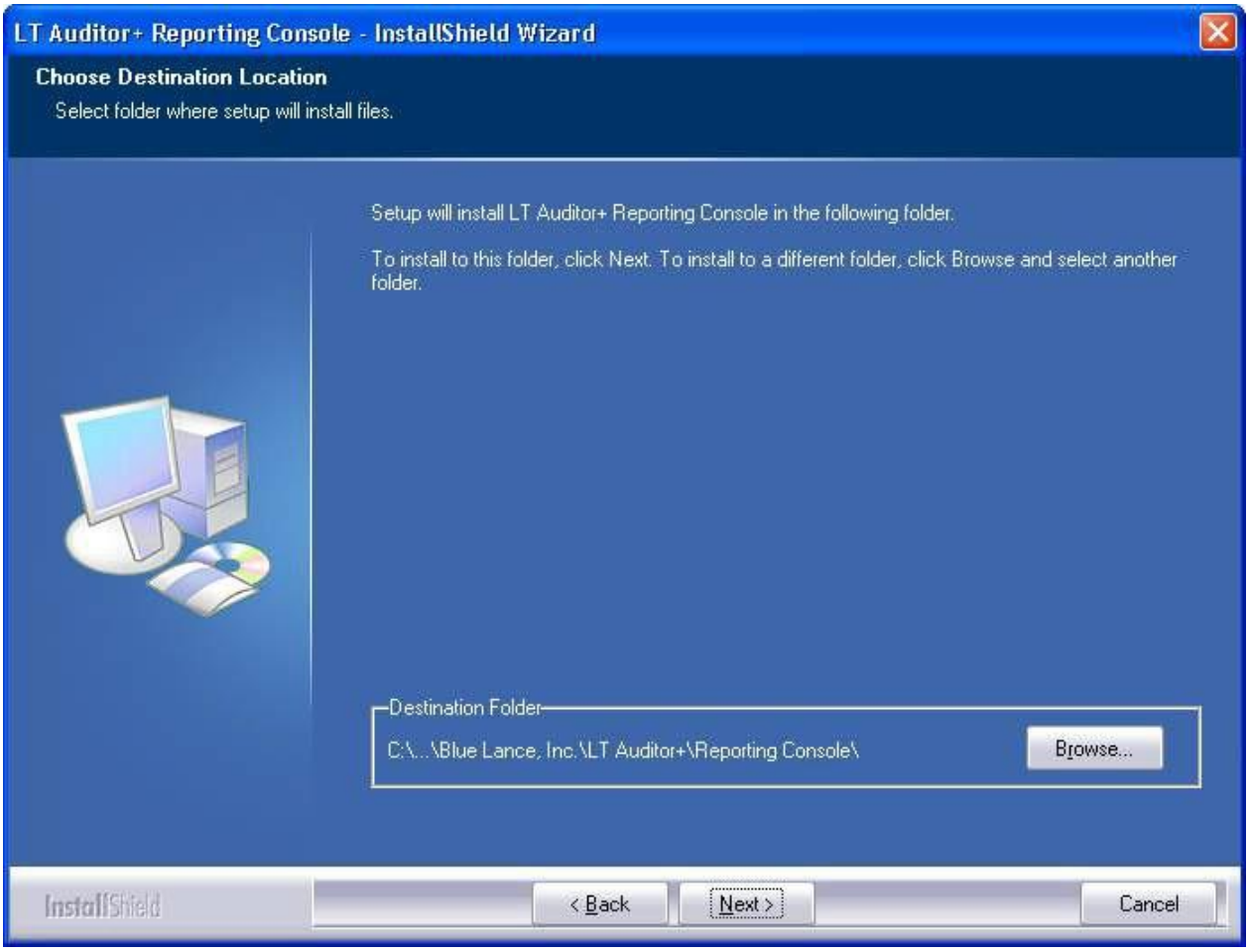
If the application detects that Microsoft .NET 4.0 is not installed on the machine, the wizard will prompt you with a message to install. After Microsoft .NET 4.0 is installed the welcome screen will be shown.



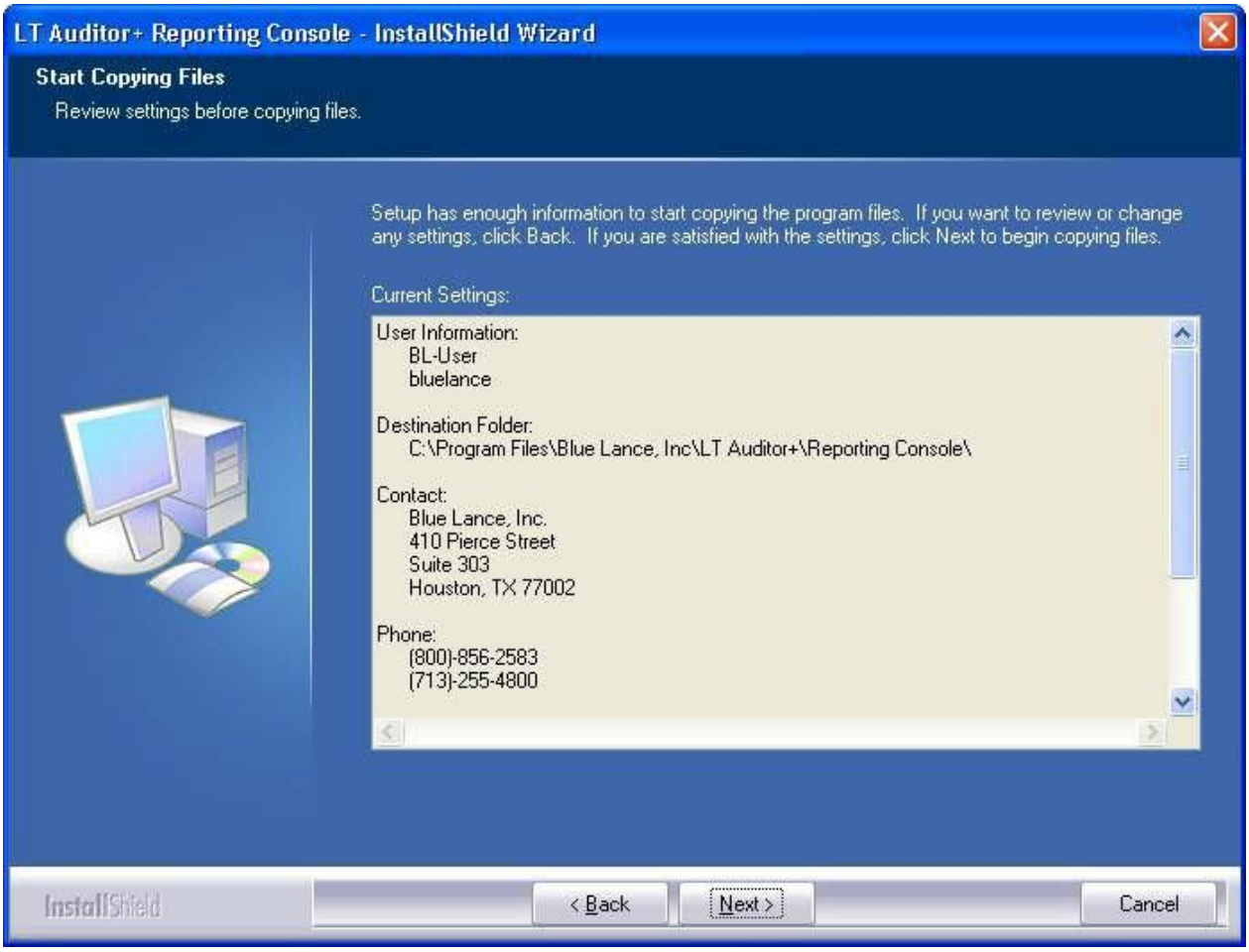
2. Click Next to continue to Customer Information screen.



3. Enter the username and company name under which this product will be registered.
4. Click Next to display Choose Destination Location as shown below.



5. By default, the product will be installed in the folder "C:\Program Files\Blue Lance, Inc.\LT Auditor+\Report Console\"
6. Click Browse to change install path.
7. Click Next to proceed to the Review screen.



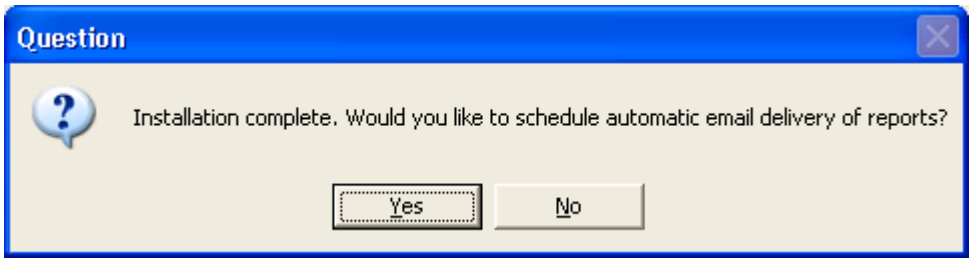
8. Review the information selected.
9. Click Back to make changes and corrections; otherwise, click Next to start copying files onto the machine.

With a new LT Auditor+ installation, certain reports containing commonly queried data can be generated and sent regularly via email as a default setting. These default reports may be deleted or modified at any time. The database and email settings will be determined upon installation of the Report Console. The following reports may be scheduled:

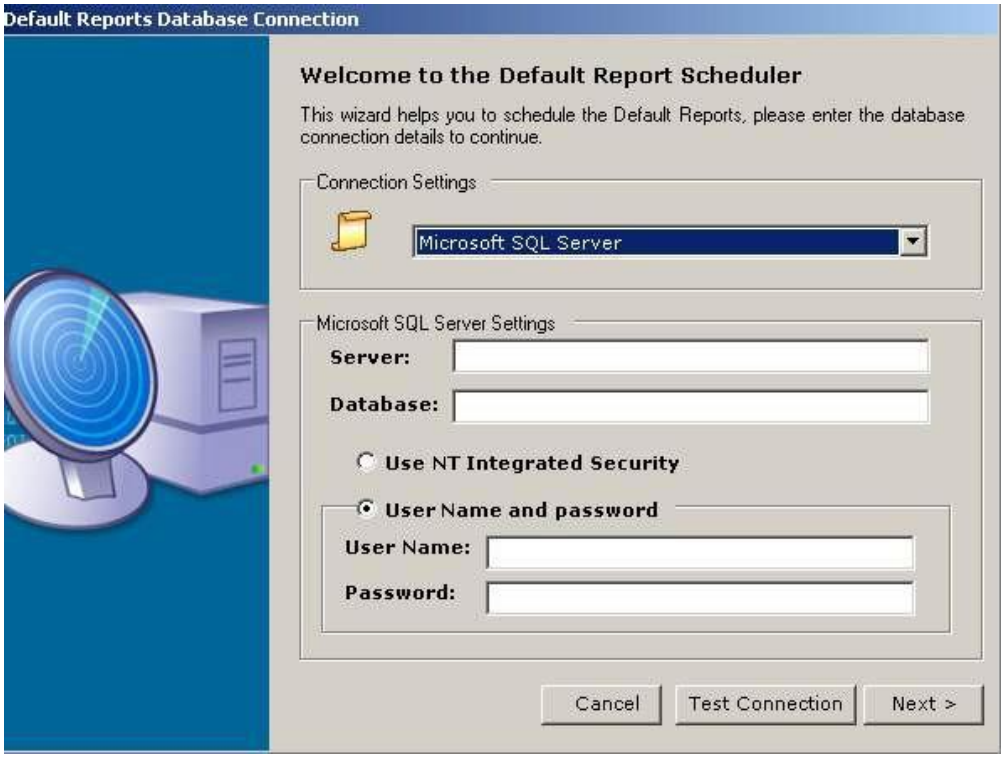
- Failed Login Report
- Users Created Report
- Users Deleted Report
- Users who were made members of the Enterprise Admin Group
- Users who were made members of the Domain Admin Group
- Accounts Enabled or Disabled Report
- User Accounts Change Password Report
- All Group Policy Modifications Report

When installing the Report Console, the Installation Wizard will now guide the user to determine database connection settings and SMTP settings needed to generate and send the default reports. The user will be prompted during installation to determine whether or not default reporting will be enabled. If the user chooses not to enable default reporting, the default reports will still be stored in the Report Console but will not be generated or emailed. They may be accessed for scheduling at a later time.

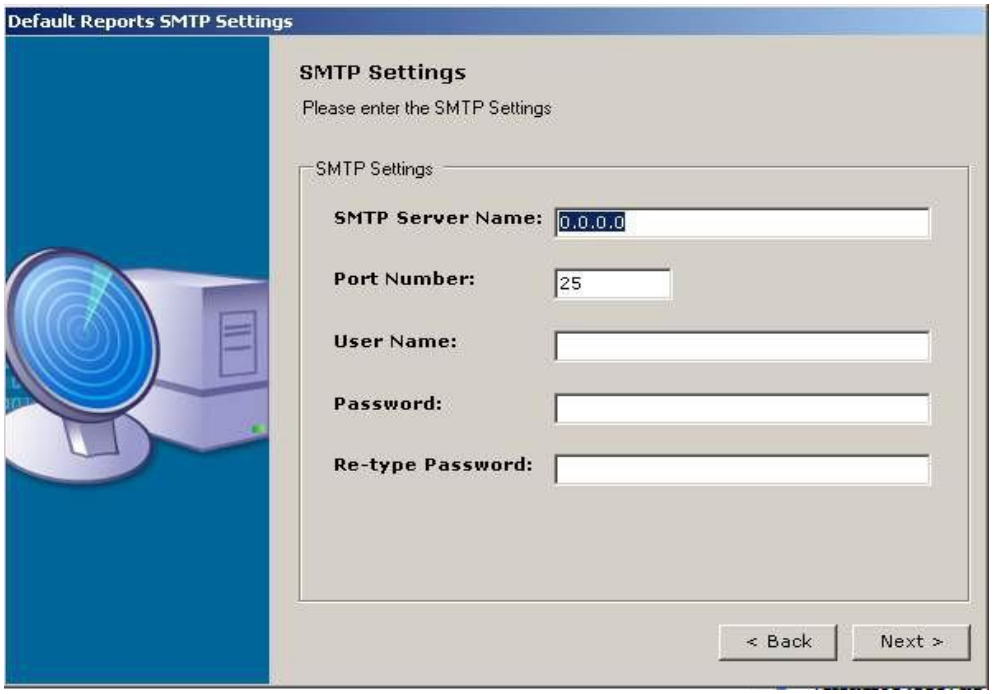
After installation of the Report Console, the following window will appear:



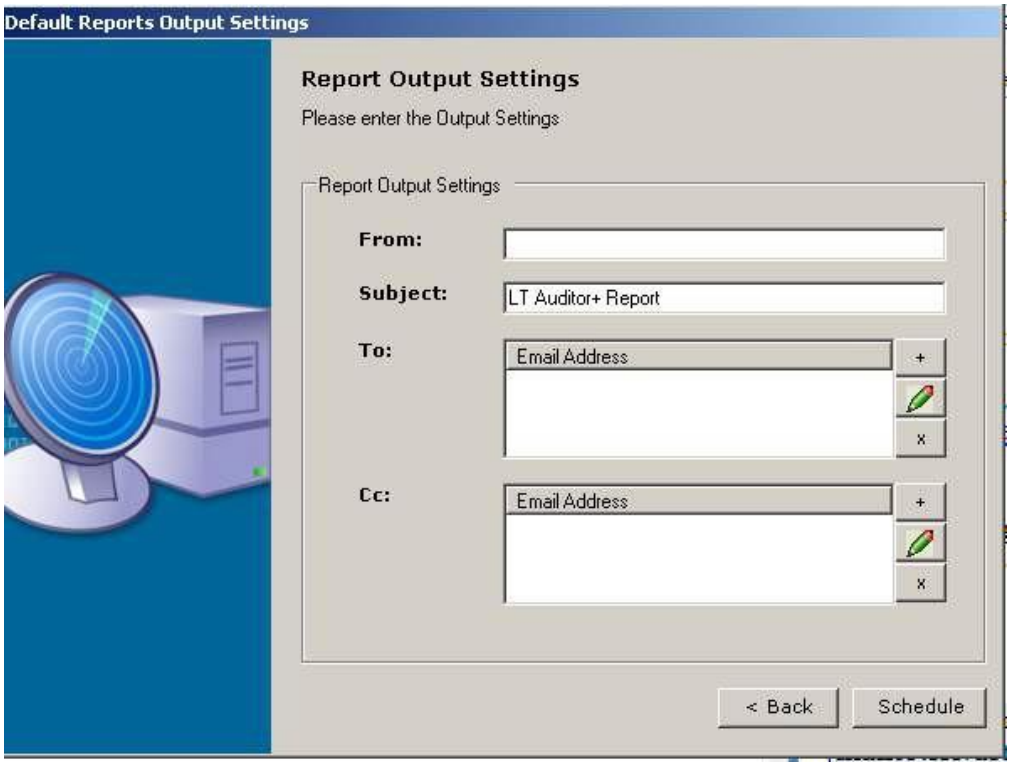
Should the user want to schedule default reports at this time, click Yes. All default reports must be installed at once; however, unneeded reports can be deleted later. Default reports may be scheduled after installation is complete through a menu option in the Report Console, as shown in the following image:



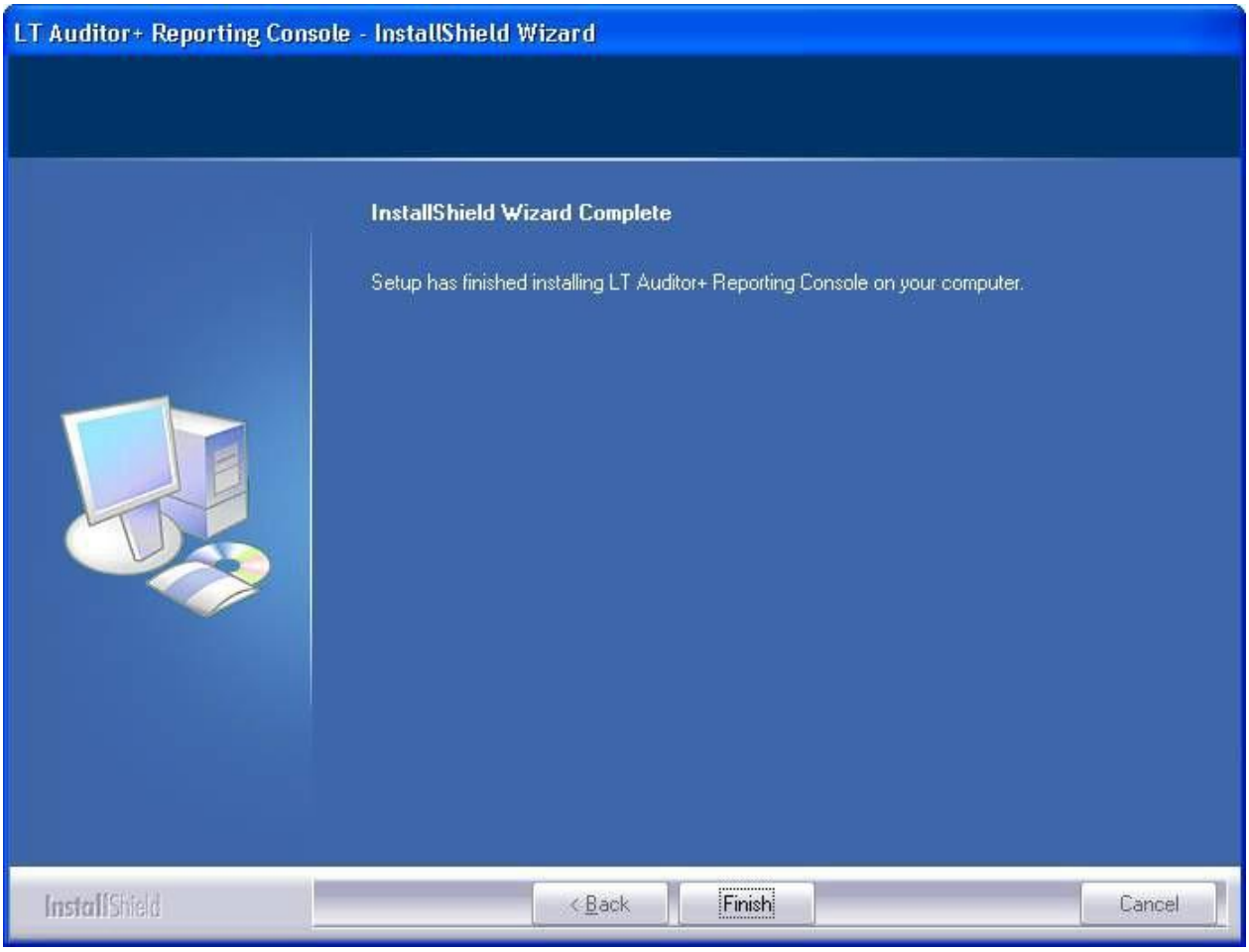
10. Enter credentials to connect with the LT Auditor+ database.



11. Enter the credentials required to connect to the SMTP server.
12. Click Next.



13. Enter information to enable users to receive automated email messages from LT Auditor+.
14. Click Schedule.



15. Click Finish to complete installation.

Installing LT Auditor+ Agents

LT Auditor+ agents have to be installed on operating systems to audit and monitor user activity. LT Auditor+ agents can be loaded on the following operating systems:

- Windows 2012R2/2016, 2019 Windows 7, Windows 10 systems
- SUSE Linux (SLES 10, 11, 12 with OES2, OES2015, OES2018)

The table below lists the machines that need to be installed with LT Auditor+ agents for each of the Blue Lance products or solutions.

LT Auditor+ Product Name	Target Operating Systems	LT Auditor+ Agents
LT Auditor+ for Active Directory	Windows 2012R2/Windows 2016, Windows 2019	Agents should be installed on all Active Directory Domain Controllers
LT Auditor+ for Group Policies	Windows 2012R2/Windows 2016, Windows 2019	Agents should be installed on Active Directory Domain Controllers
LT Auditor+ for Windows Servers	Windows 2012R2/Windows 2016, Windows 2019	Agents should be installed on Windows Application or Member Servers
LT Auditor+ for Windows Workstations	Windows 7 and Windows 10	Agents should be installed on all workstations or laptops that are to be audited
LT Auditor+ for SUSE Linux for eDirectory	SLES 10, 11, 12 with OES2, OES2015, OES2018	Agents should be installed on all SUSE servers that host eDirectory replicas
LT Auditor+ for SUSE Linux for NSS File Systems	SLES 10, 11, 12 with OES2, OES2015, OES2018	Agents should be installed on all SUSE servers that host NSS file systems

This section will cover the installation of LT Auditor+ agents on Windows and SUSE Linux operating systems.

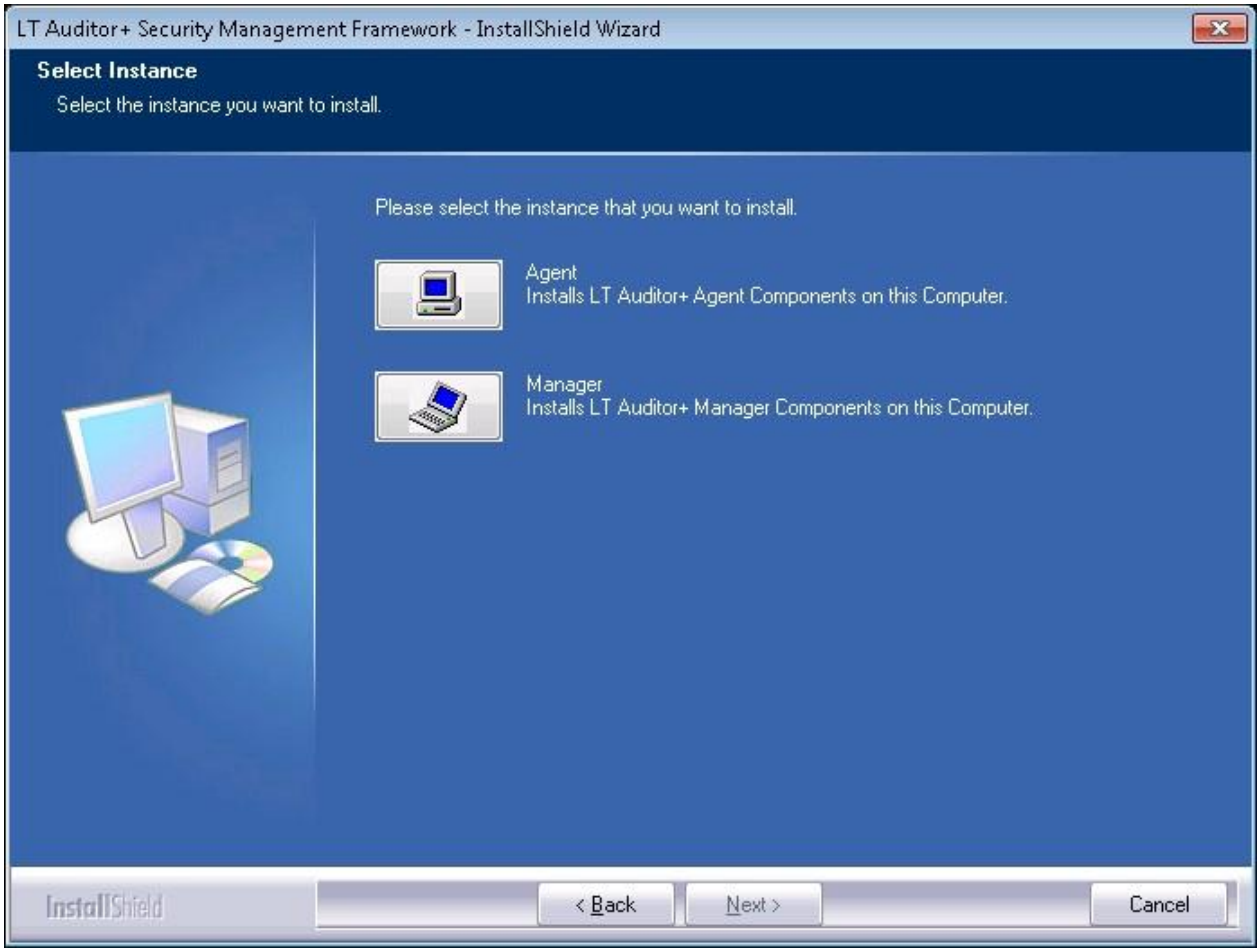
Installation of Windows Agents

LT Auditor+ agents can be installed on Windows servers and workstations either locally or remotely. For local installation, a user has to be logged on interactively on the target machine. Remote installation can only be done from a machine where the LT Auditor+ Manager Console has been installed.

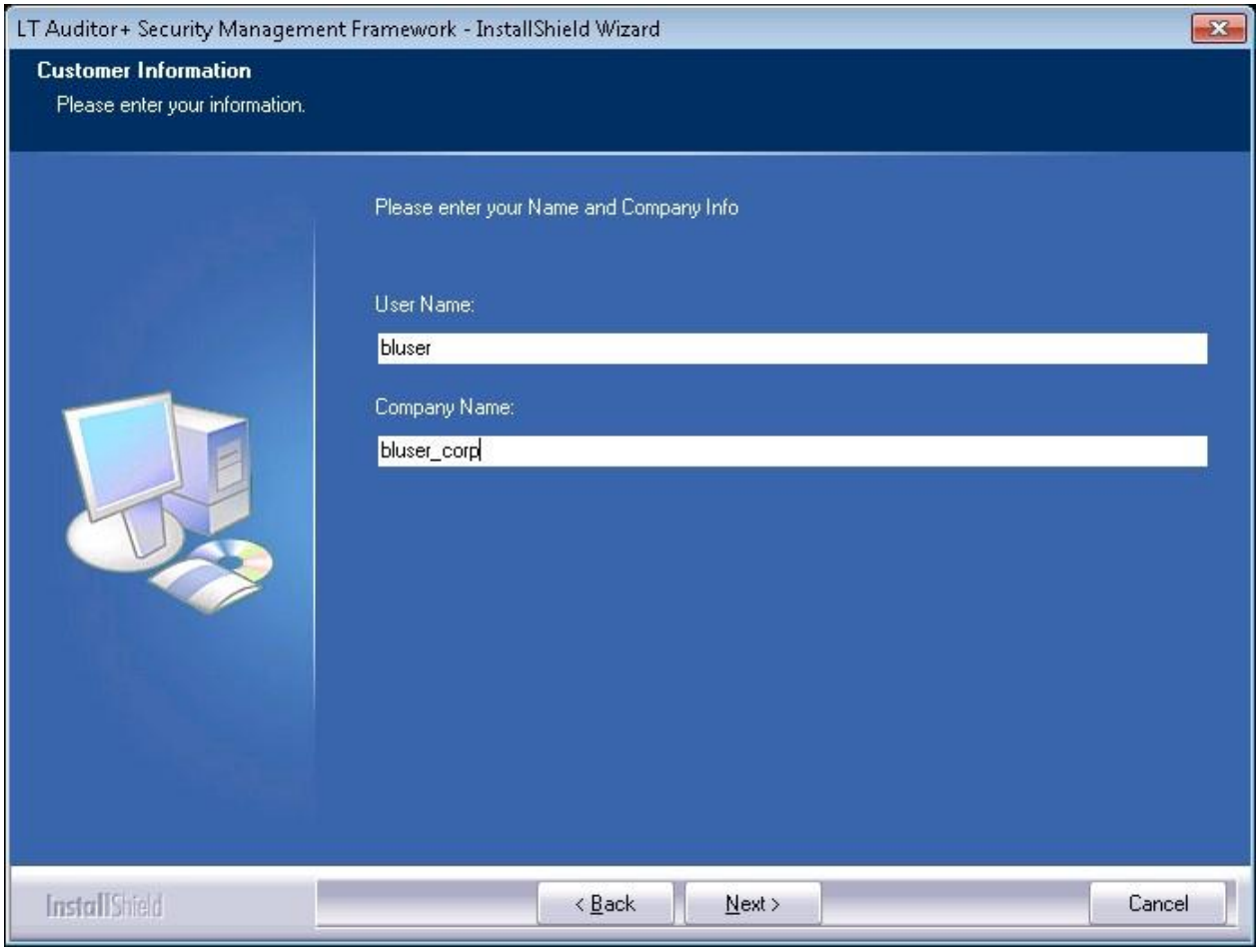
The following sections describe how to perform local and remote installations.

Local Installation

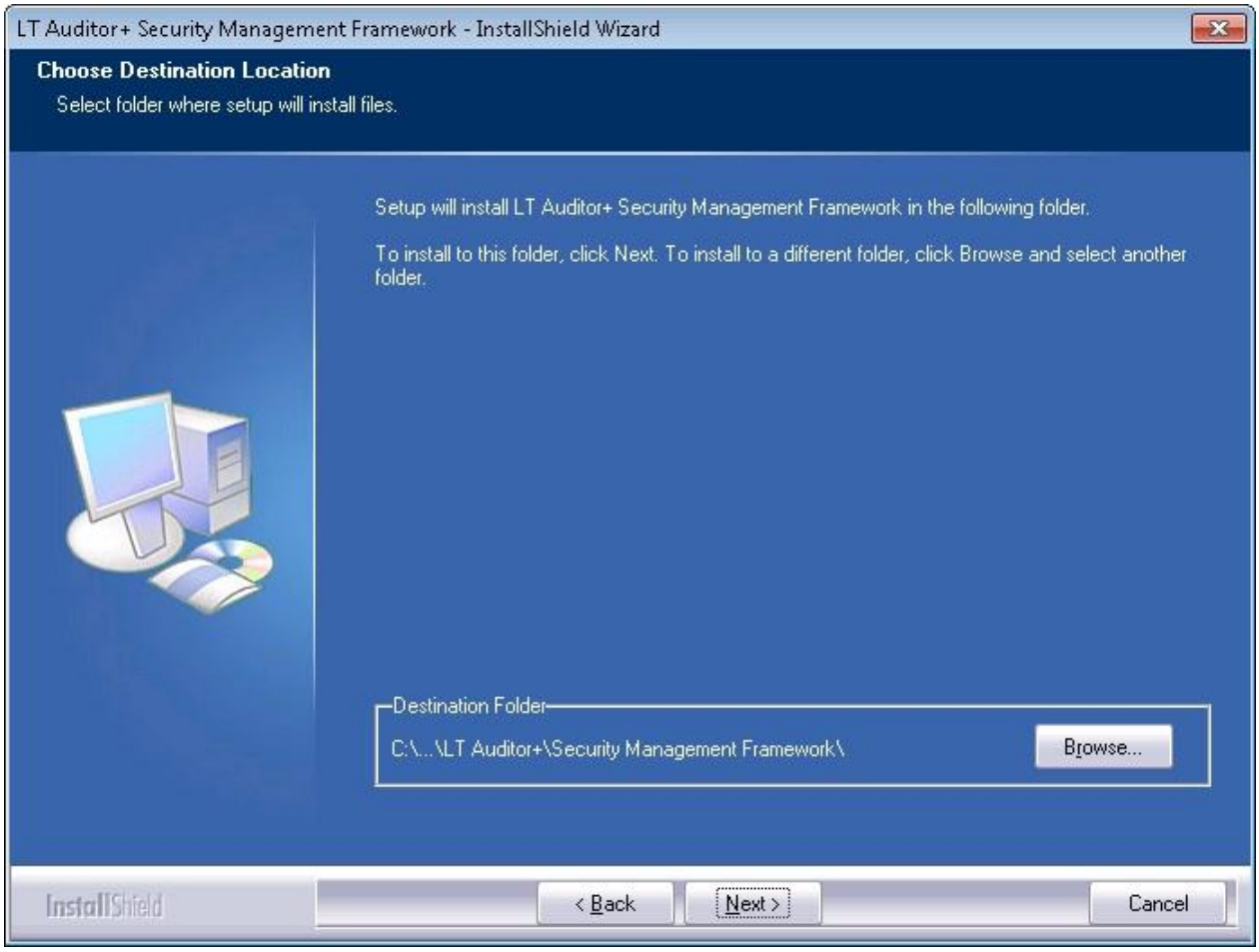
1. Follow all steps up to step #5 for installing the LT Auditor+ Manager, discussed above, to display the following screen.



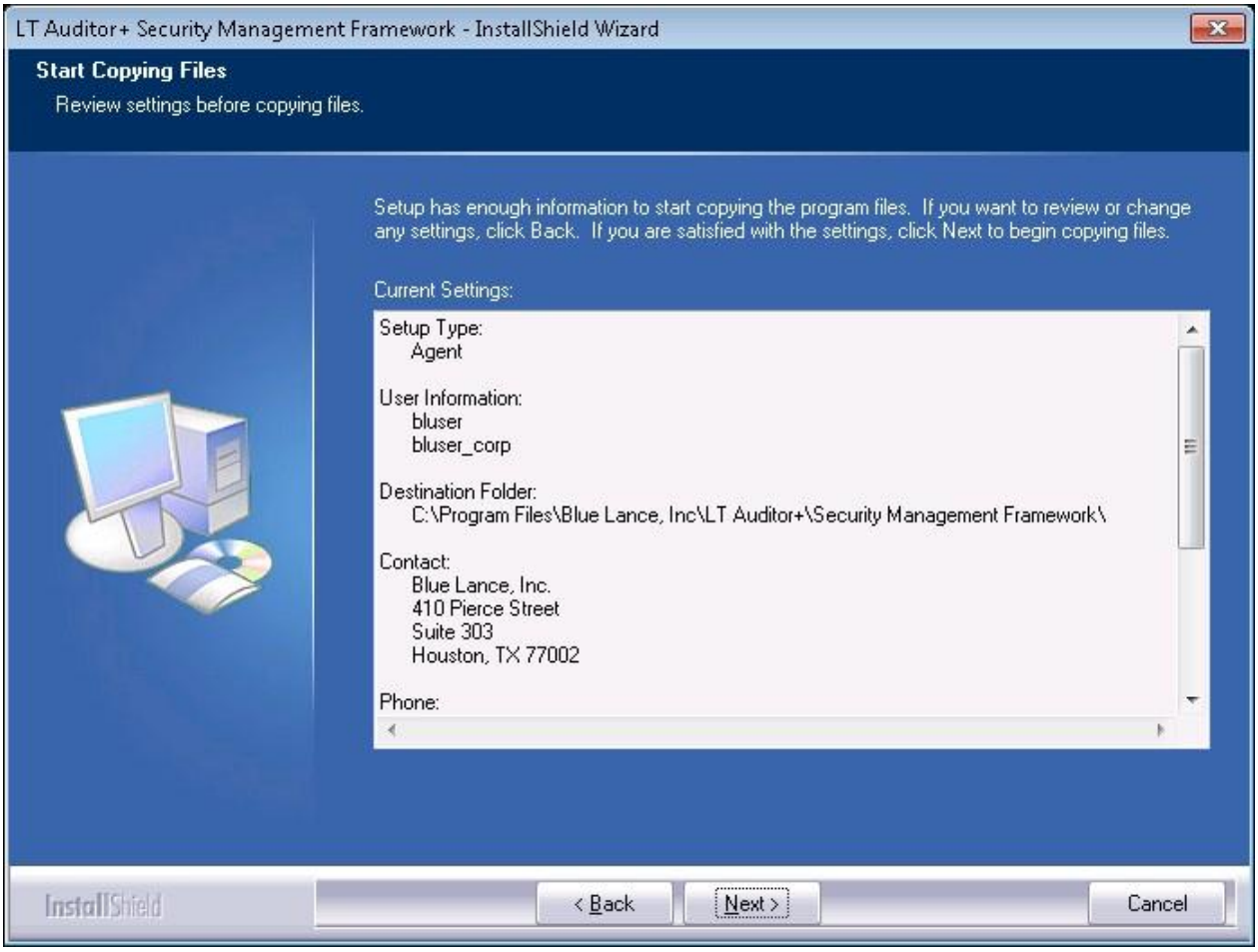
2. Select Agent and click Next to proceed to the Customer Information window.



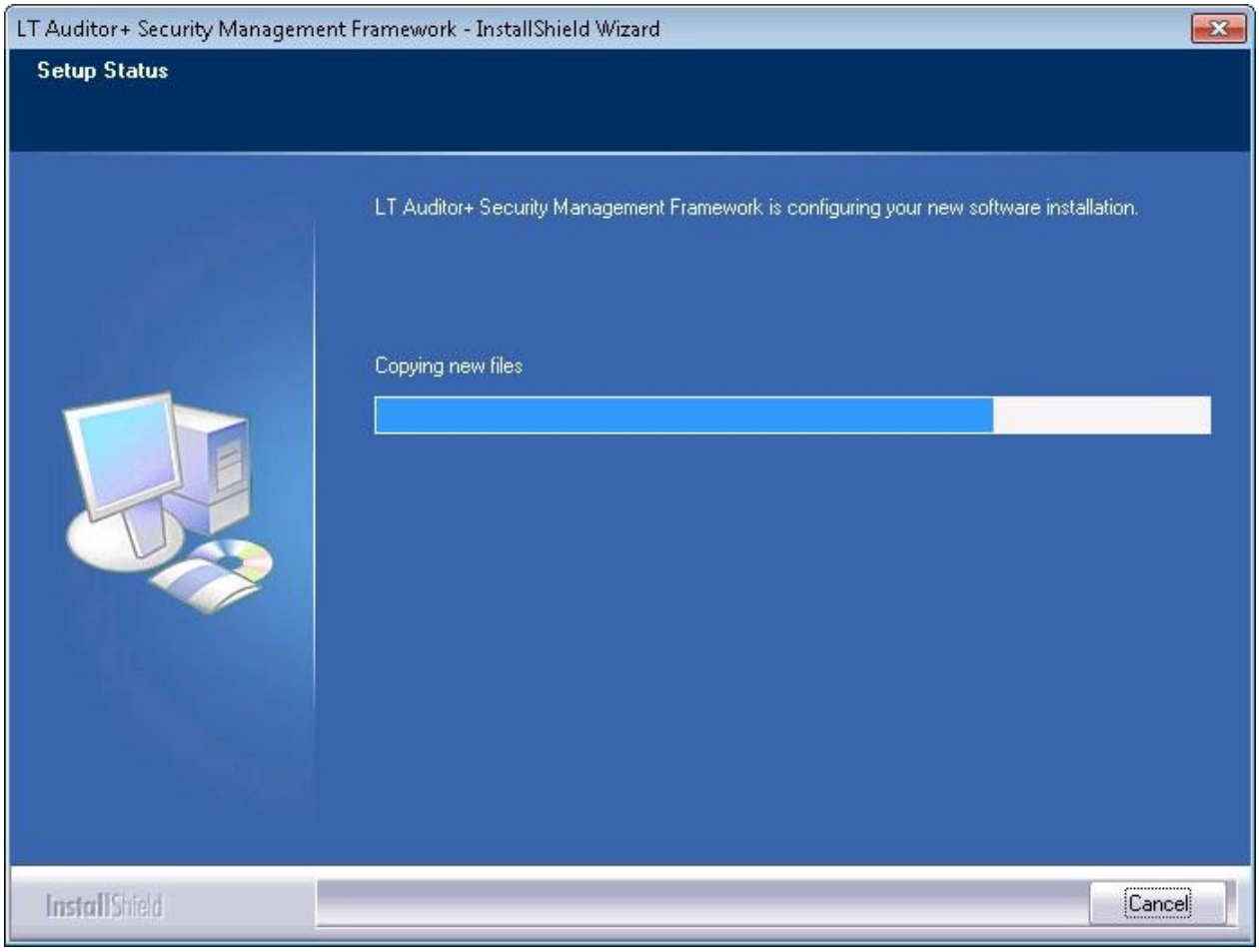
3. Enter your name and company information.
4. Click Next.



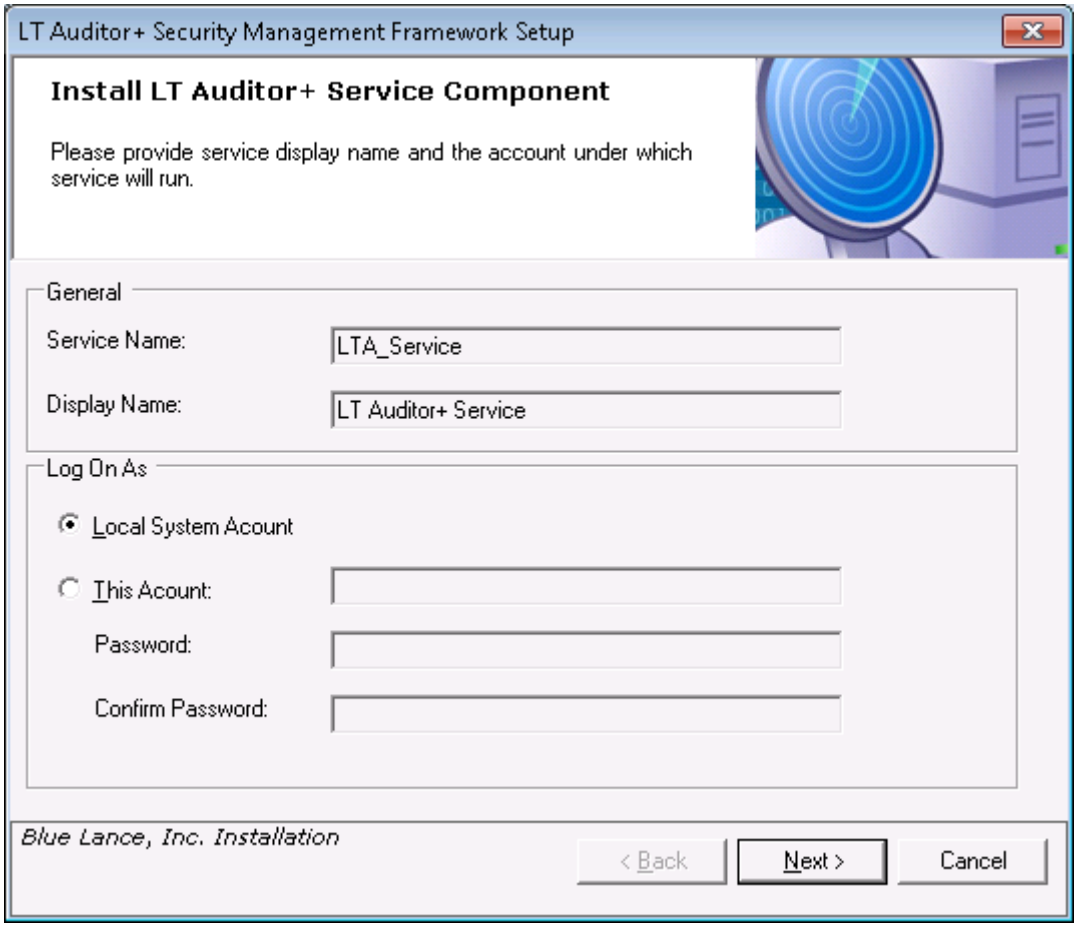
5. Click Next if the destination location is satisfactory; otherwise, click Browse to select new location.



6. Review the specified settings.
7. Click Back to make any changes; otherwise, click Next.



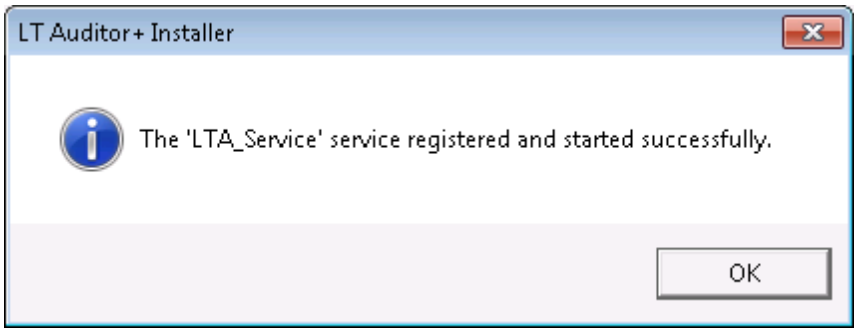
8. Progress will be shown as the files are copied to the selected location. After the files have been copied, the installation progresses to the setting up for the LT Auditor+ Windows service screen.



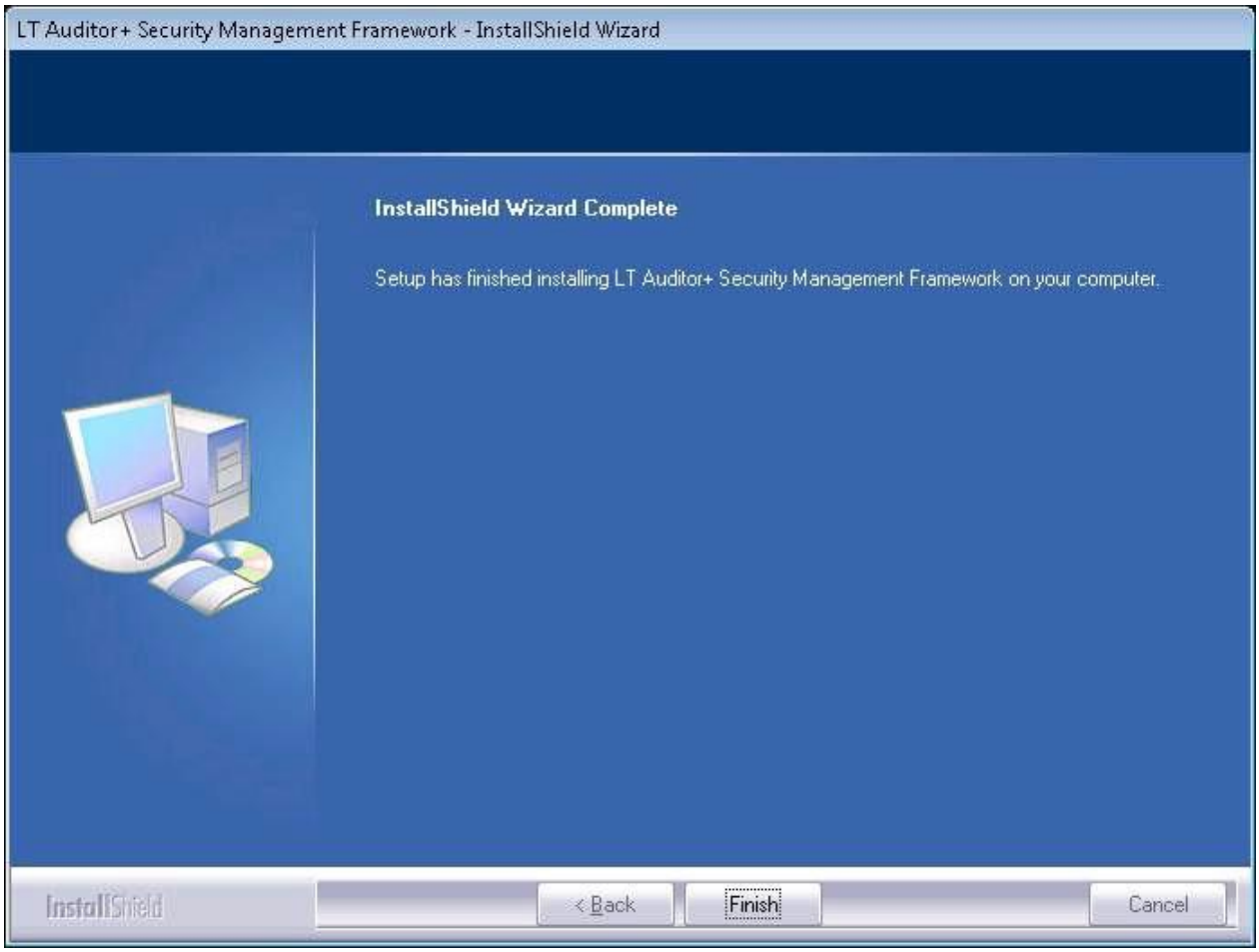
9. Click Local System Account for the LT Auditor+ service to use the local system account. Otherwise, enter credentials to log on as a specified account.
10. Click Next for service registration.

NOTE

When the LT Auditor+ service uses a specific account, it is recommended that this account has local system administrator privileges.



11. Click OK to continue to the Wizard Completion screen.



Click Finish to complete the installation.

NOTE

After a Windows agent has been installed, this agent will have to be added to a group setup using the LT Auditor+ Manager Console. Please refer to the Configuration Guide for instructions on adding agents to LT Auditor+ groups.

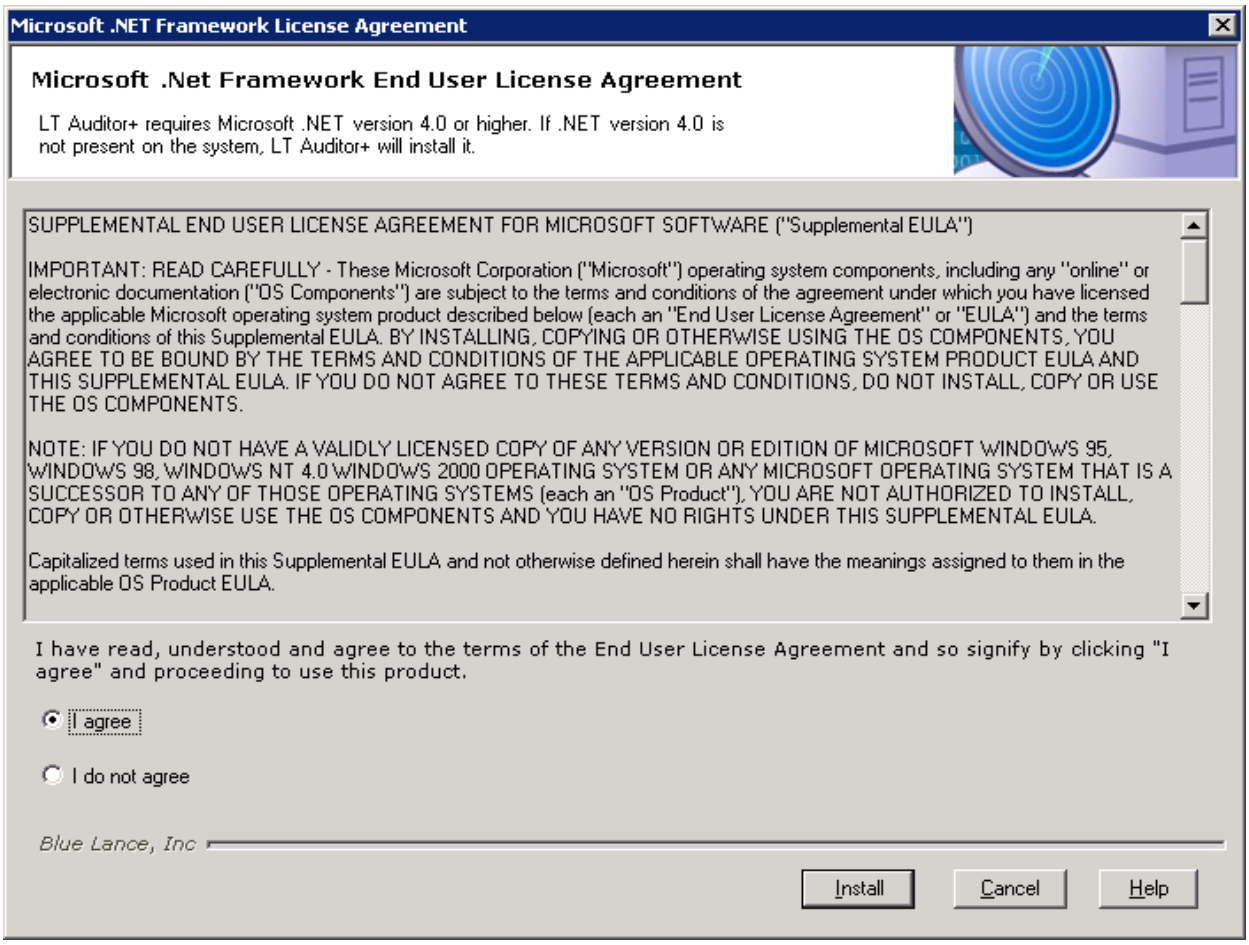
Remote Installation of the Agent

Prerequisites for the LT Auditor+ Agent Installation

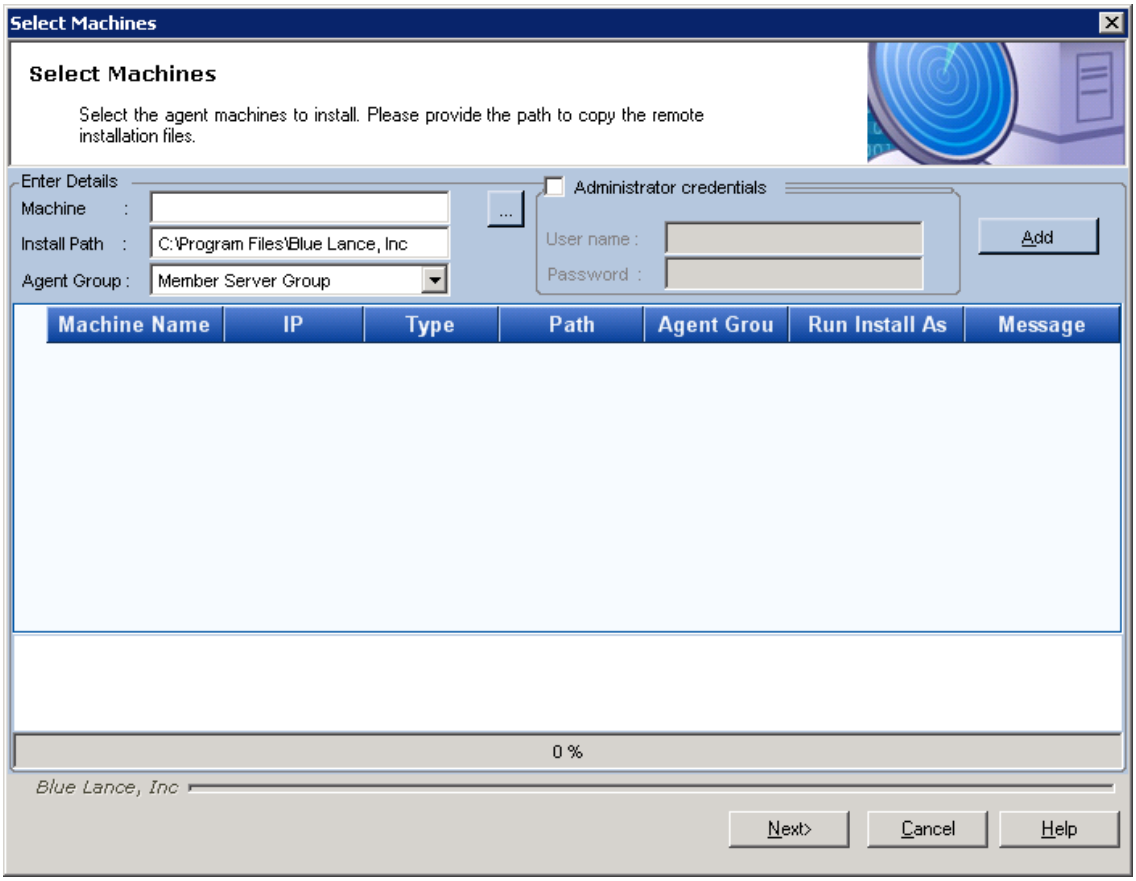
- Meet the system requirements outlined above.
- The LT Auditor+ Manager Console must have been installed to perform remote installation.
- Installer must have administrative privileges to install on agent machine.
- Firewall setting on all target machines must be checked to ensure that port 2877 is open.

Remote Installation Steps

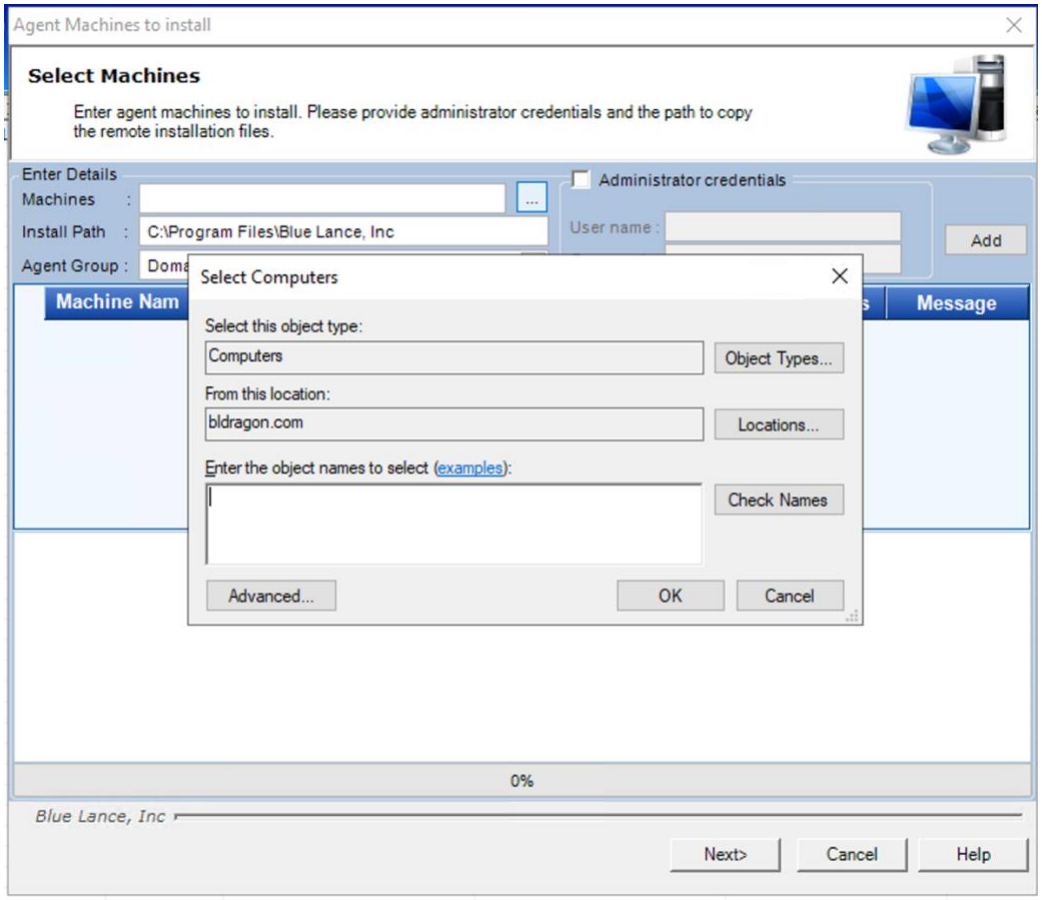
1. From the Manager Console, select Options → Remote Install.
2. Windows .Net Framework License Agreement will open.



3. Select "I agree."
4. Click Install.
5. A Select Machines screen is displayed as shown below.



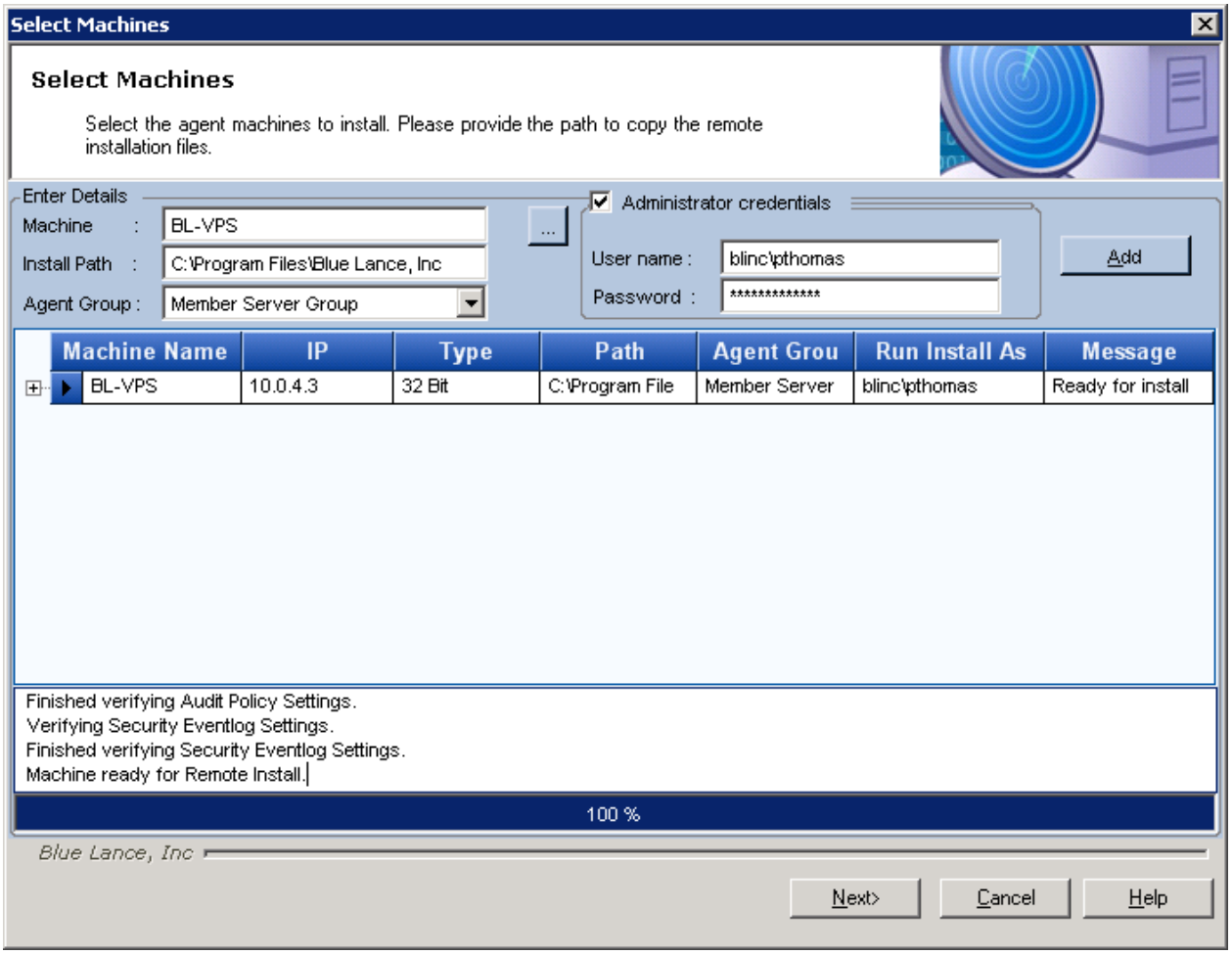
6. Click on Browse button and browse for the networked machines, or type the machine name or the IP address of the destination server in the Machine field.
7. Change the Install Path, if desired; the default path will automatically populate the field.
8. Select an Agent Group name from the drop-down.
9. Check the Administrative Credentials check box to use credentials to authenticate to the target machine.



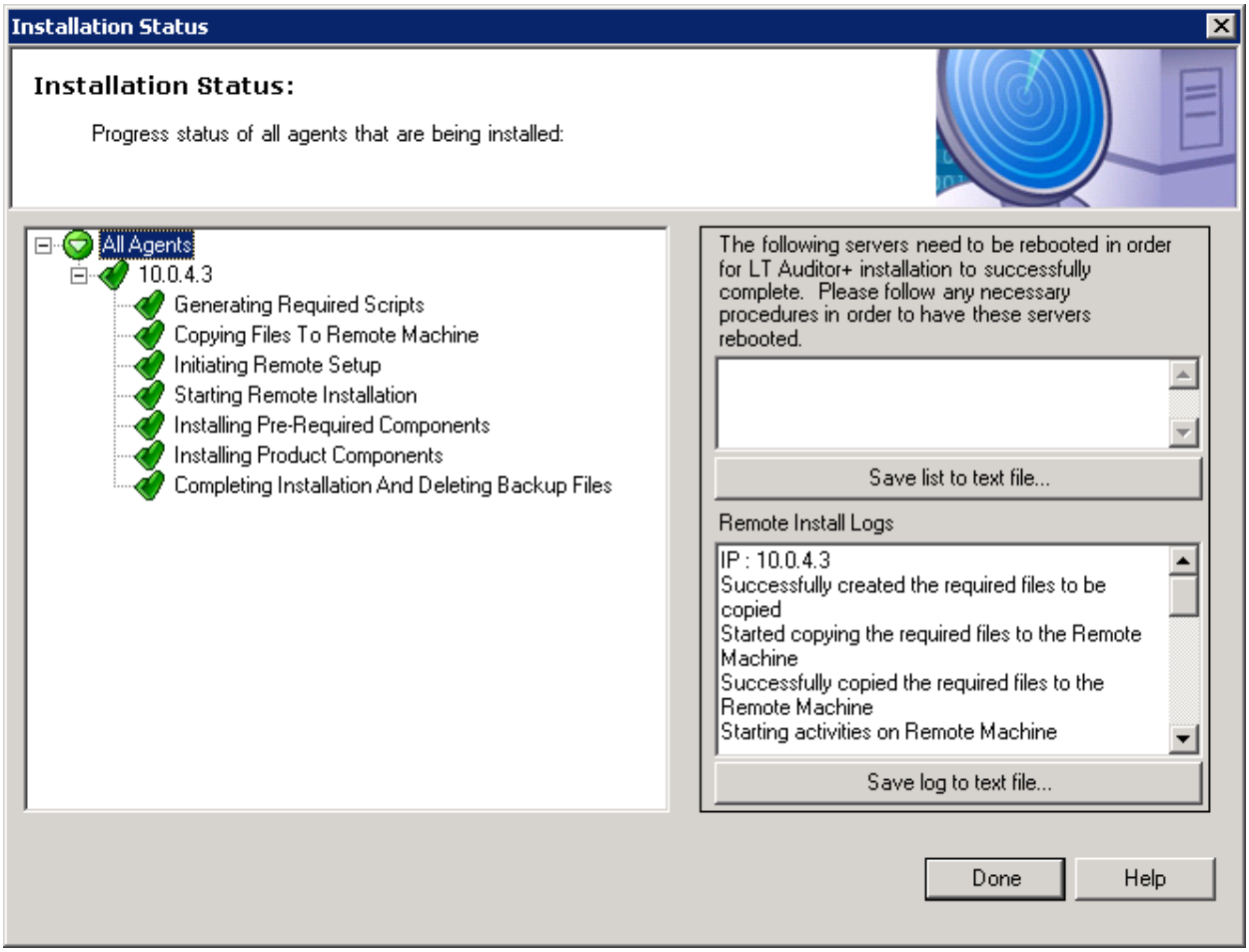
NOTE

If the target machine is within the same domain, and if the installer had domain admin privileges, you would not need to check the Administrative Credentials check box. If target machine is not in the same domain or if the installer is not a Domain Administrator, it is recommended that credentials for a user that has administrative privileges on the target machine be entered.

10. Click on the Add button and the application will perform checks to ensure that the LT Auditor+ can be installed on the target machine. If errors are found, click on the "plus sign" by the machine name to view reasons for error. If all checks pass, the message "Ready to install" will be displayed in the message column as shown.



11. Continue to add agents until desired remote agents have been selected.
12. Click Next.
13. The Installation Status window will open as displayed.



14. When the install is complete, any servers that need to be rebooted will be listed in the panel to the right.
15. To save the list to a text file, click Save List to Text File.
16. If there were any errors during the installation, a file called **RemoteInstallLog.txt** will get created in the Program Files' **\Blue Lance, Inc.\LT Auditor +\Manager Console\Install** folder.
17. Click Done to finish the installation and close the communication loop(s) with the remote installs.
18. The new agent will now be added to the agent group selected.

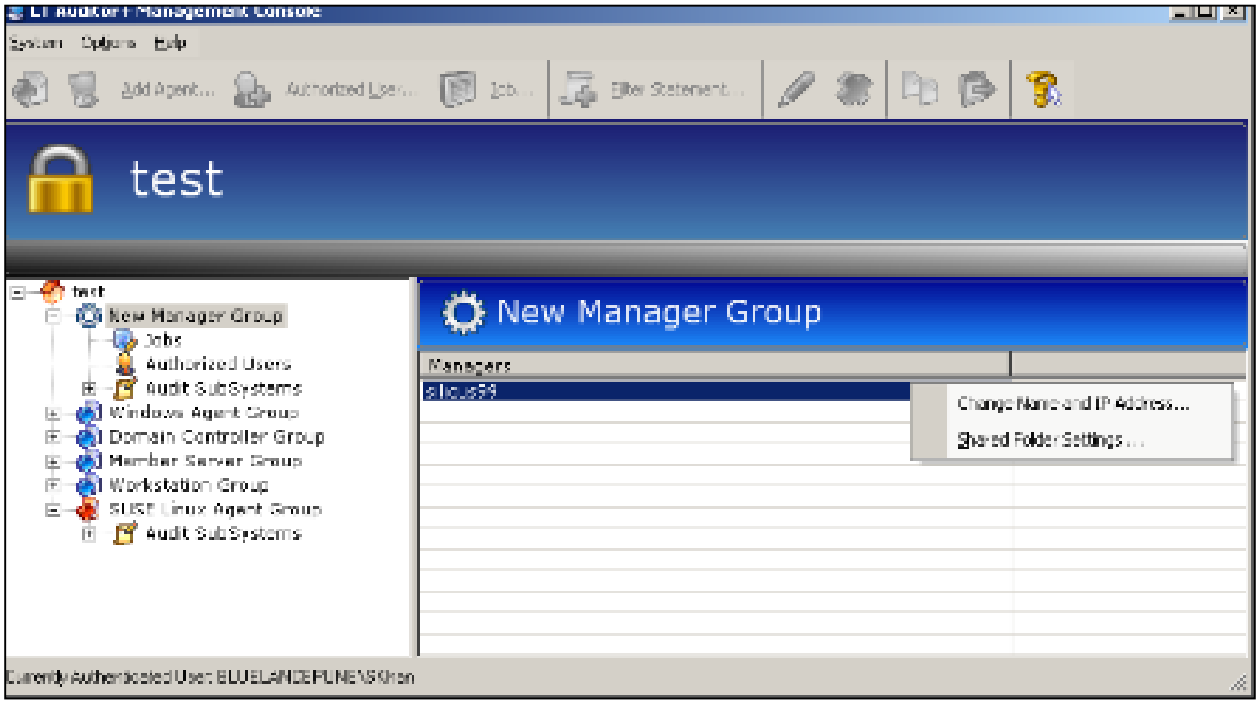
Installation of SUSE Linux Agents

Prior to installing the SUSE Linux agents, a Windows share folder needs to setup on the machine hosting the LT Auditor+ Manager.

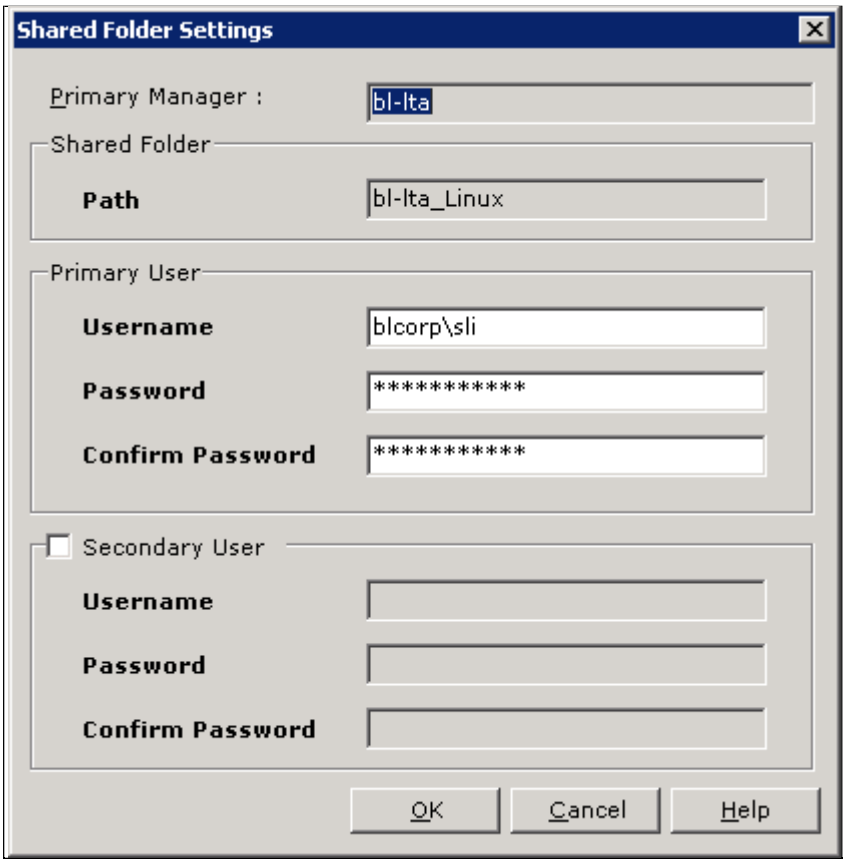
Setting up a Windows Share Folder for SUSE Linux Agents

A Windows Shared folder will be used to deploy all policies and configurations for all SUSE Linux agents. The SUSE Linux agents will also use this shared folder to transfer audit data to the LT Auditor+ Manager. The steps outlined below provide detail on how the Share Folder setting can be configured.

1. Launch the LT Auditor+ Manager Console.
2. Click on any manager group.
3. Right-click on the pane. The options to change Name and IP Address and Shared Folder appear as shown below.



1. Click on the Share Folder Settings option to display the Shared Folder Settings windows shown below:



1. Enter the username prefixed with the domain name or machine name.
2. Enter Password.
3. Click OK.

NOTE

The shared folder displayed in the path will be created. This folder will always have the name of the manager machine concatenated with '_Linux' as the name.

If the manager is in a domain, on clicking OK, LT Auditor+ will assign the necessary permissions for the user specified. If the manager is not in a domain, and if the user entered does not exist, the user will be created on the local machine and appropriate rights will assigned to the shared folder.

Installation of LT Auditor+ on SUSE Linux Machine

In order to install agents, we would need to install the RPM package. Do the following to install the RPM package:

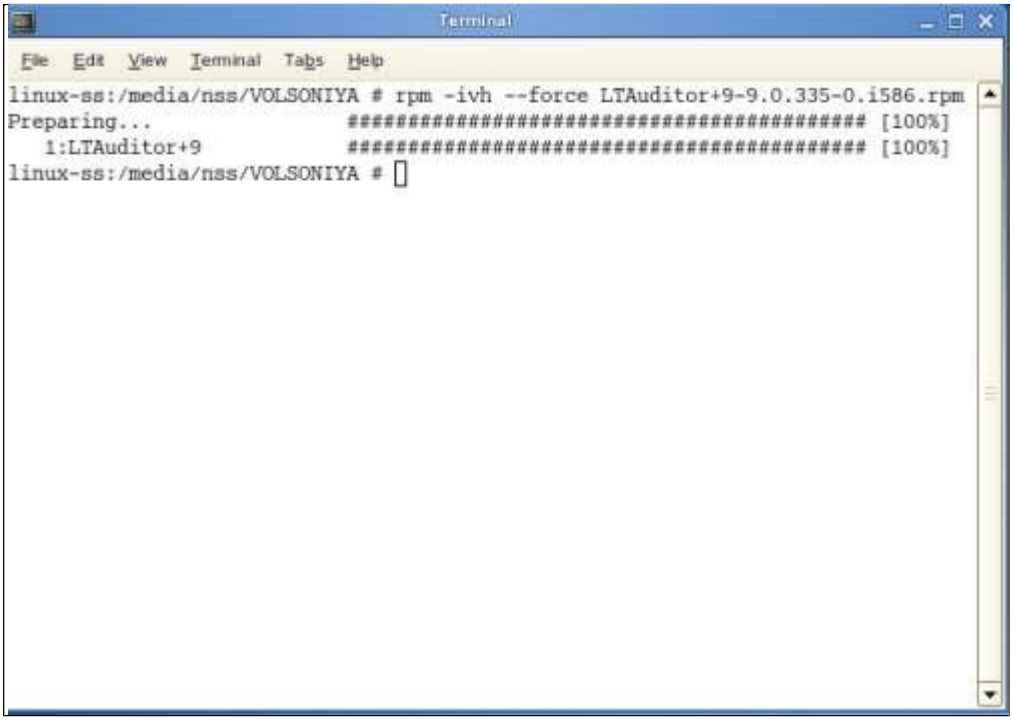
1. Copy and paste the installation RPM package to the SUSE Linux server. This package can also be put on a NSS volume associated with the SUSE server as shown below:

2. Go to file and click on Open in Terminal and run the following command: **rpm –ivh LTAuditor+OESYYYY—xx.x.x.m-0.x86_64.rpm.**

NOTE

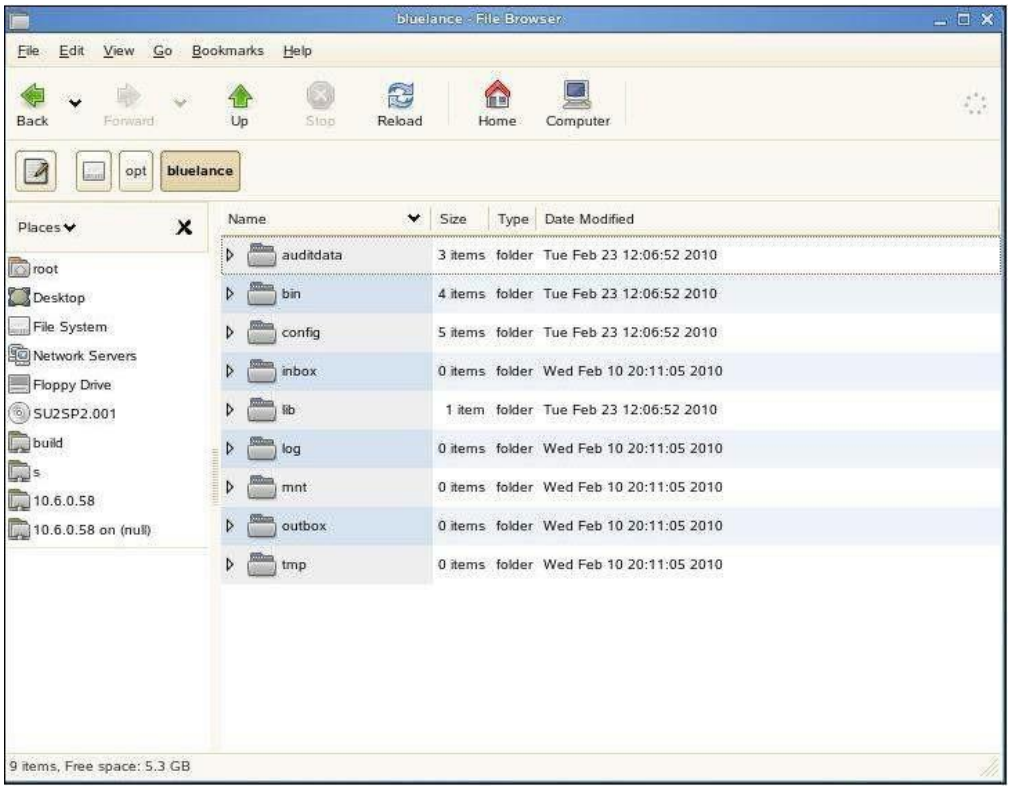
The **yyyy** represents OES version supported. Example: **3015** or **2018**
xx.x.x.m represents version
e – represents LT Auditor+ engine
LTAuditor+OES2018-18.0.3.0-0.x86_64.rpm (Installs both eDirectory and NSS engines)
LTAuditor+OES2018-18.0.3.3-0.x86_64.rpm (Installs NSS audit engine only)
LTAuditor+OES2018-18.0.3.4-0.x86_64.rpm (Installs NSS audit engine only)

5. Click enter.



After the installation of the RPM package, **/opt/bluelance** folder is created along with following subfolders:

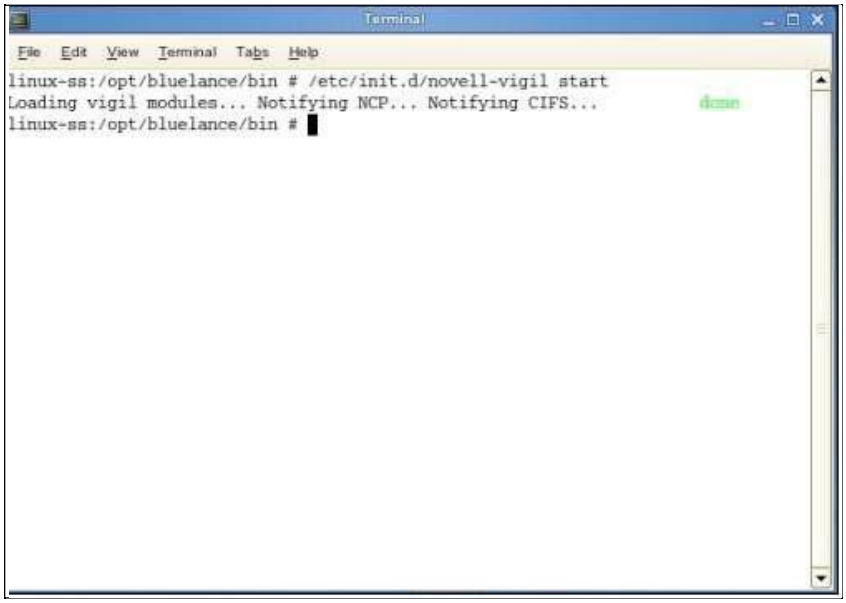
- **/opt/bluelance/config**
- **/opt/bluelance/bin**
- **/opt/bluelance/lib**
- **/opt/bluelance/log**
- **/opt/bluelance/inbox**
- **/opt/bluelance/mnt**
- **/opt/bluelance/temp**
- **/opt/bluelance/outbox**



NOTE

When using LT Auditor+ for NSS File System, please ensure that that the Novell Auditing Engine (Vigil) has been started. If the Vigil module has not been loaded, use the following command to activate Vigil.

/etc/init.d/novell-vigil start



Starting LT Auditor+ Daemons on SUSE Linux

Run the following command.

/etc/init.d/ltaudit.rc start

Starting LT Auditor+ SUSE Agents on SUSE Linux Server for the First Time

When starting for the first time, the LT Auditor+ agents on SUSE Linux will need to:

- Establish a connection to the LT Auditor+ Manager.
- Agent needs to be added to a SUSE Linux agent group on the LT Auditor+ Manager.

Establish a connection to the LT Auditor+ Manager

When starting the LT Auditor+ daemons, for the first time, the user will be prompted for connection information as described below:

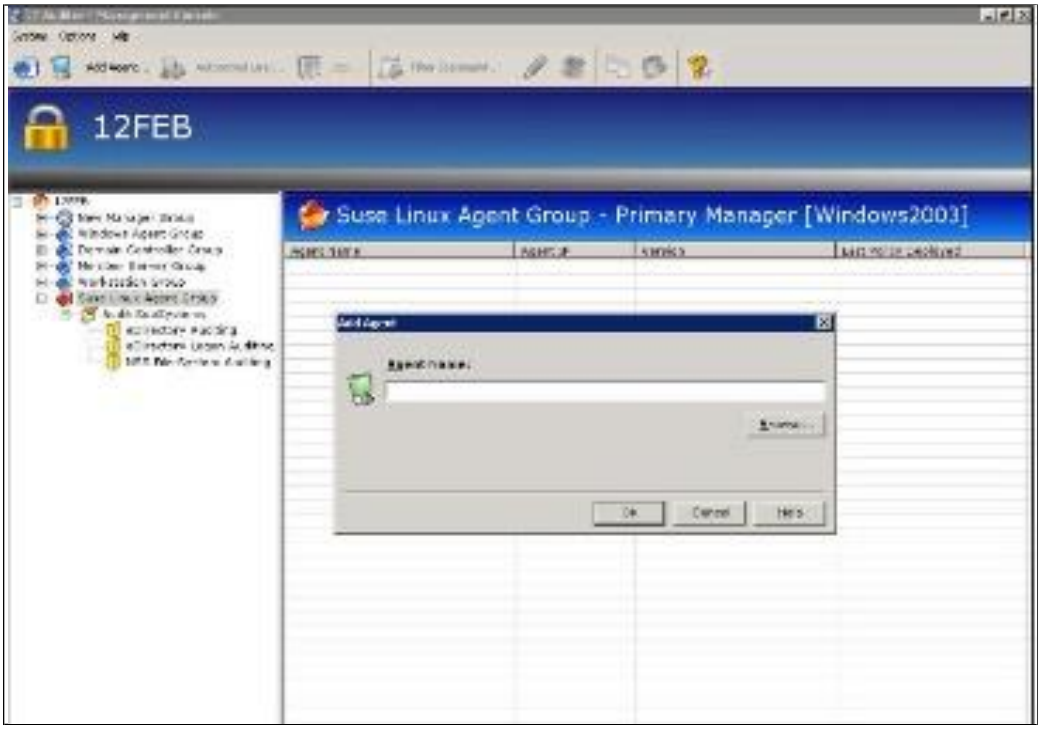
1. Enter LT Auditor+ Windows Manager IP Address: <Please enter the IP address only of the LTA Manager (e.g., 10.0.3.4).>
2. Enter LT Auditor+ Windows Manager Share Name: <Enter the name of the share as discussed above (e.g., machinename_Linux).
3. Enter LT Auditor+ Windows Manager Domain Name: <Enter the Domain name of the manager. If the manager is not in a domain enter the machine name (e.g., BLMANGER).>
4. Enter Username to Access Windows Share: <Enter Username to connect.>
5. Enter Password for User: <Password>

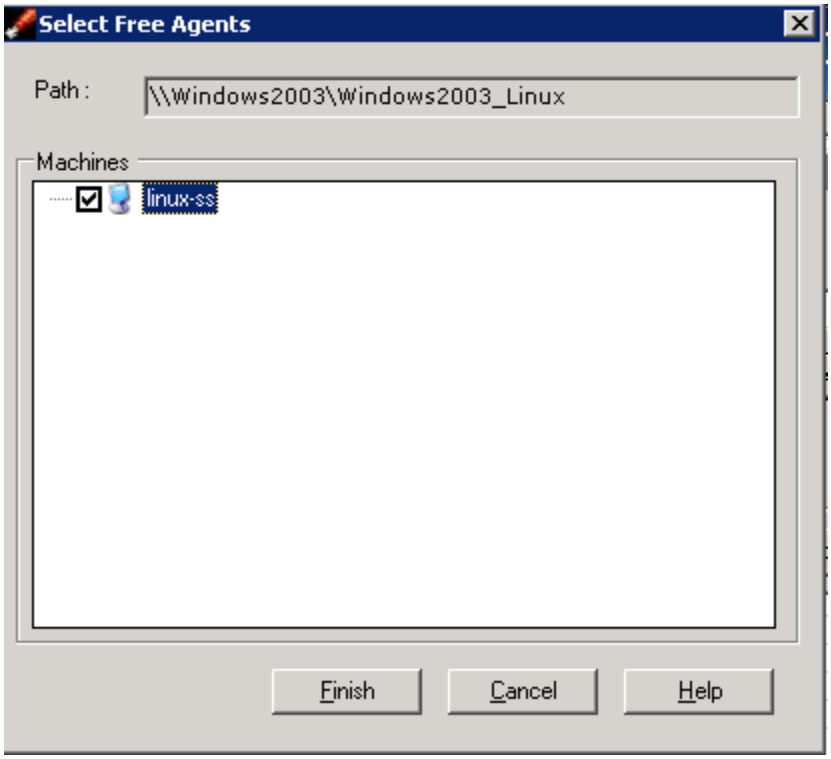
This agent is now ready to be added to the SUSE Linux agent group on the LT Auditor+ Manager.

Add LT Auditor+ SUSE Linux Agent to Agent Group on LT Auditor+ Manager

To add agents to SUSE Linux Agent Group, choose one of the following:

1. Click on System → New → Add Agent OR
1. Click on the toolbar icon: Add Agent OR
2. Right-click on summary view → Add Agent
3. Right-click on SUSE Linux Agent Group, click Add Agent. The Agent window will be displayed.
4. Click on the Browse button. The Select Free Agents window will open.

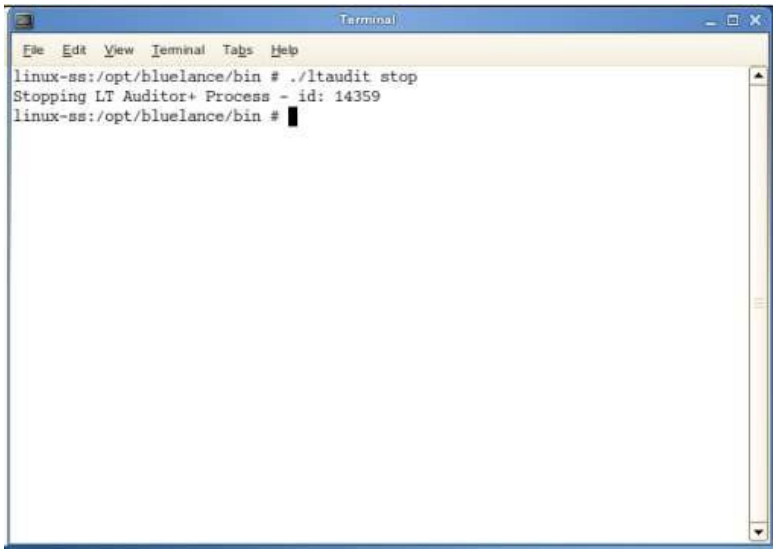




Stopping the LT Auditor+ Daemons

Run the following command to stop the LT Auditor+ daemons:

/etc/init.d/ltaudit.rc stop

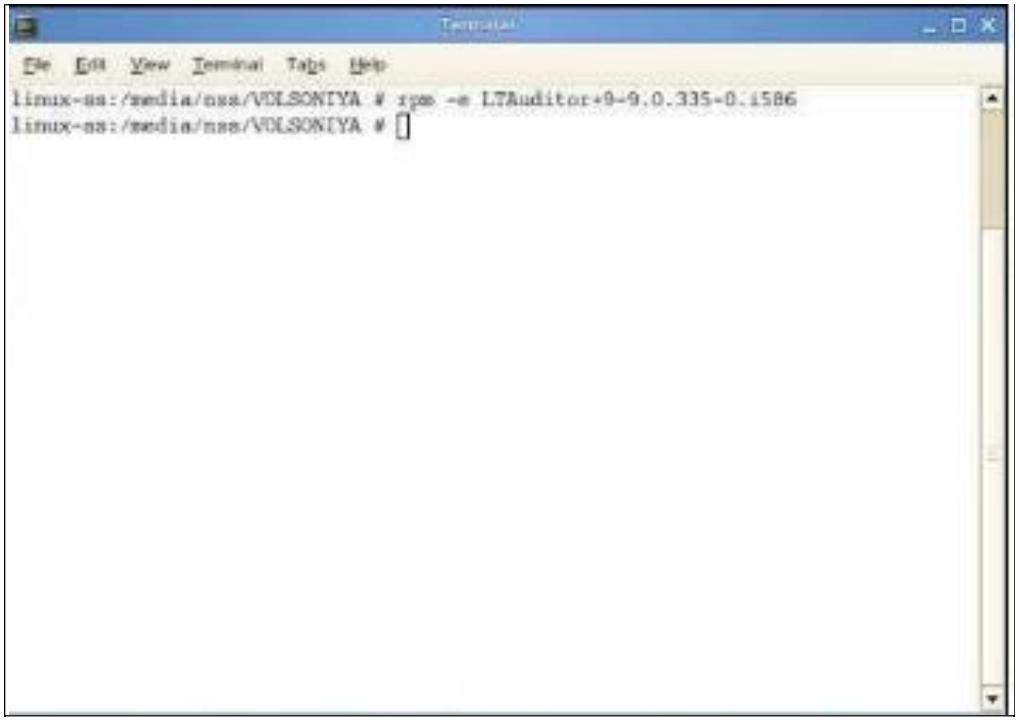


Uninstalling LT Auditor+ SUSE Linux Package

Run the following command to uninstall:

- **Rpm –e LTAuditor+OESYYYY-xx.x.x.m-0.x86_64**

NOTE **YYYY-xx.x.x.m** here denotes the current version of LT Auditor+ SUSE Linux installed.



APPENDIX A

Creating a Database

Overview

This appendix is intended to help LT Auditor+ users create the two databases necessary to run LT Auditor+. These step-by-step instructions do not encompass all available information on database creation. Should you need more information on SQL database creation, please access the following link: http://support.microsoft.com. For more information on creating an Oracle database, access: http://www.orafaq.com. You may also contact Blue Lance customer care services with questions or concerns.

LT Auditor+ supports the following databases:

- Microsoft SQL (2014/2016/2017/2019)
- Oracle (9i, 10g,11g,12)

Creating and configuring an LT Auditor+ Database is done in the following four stages:

1. Creating the database
2. Creating database objects
3. Setting access permissions
4. Setting up database maintenance jobs

Two databases will have to be created for LT Auditor+. We call these the production database and the archive database. The production database hosts audit data for a period of time, usually 30 days, after which older data is moved to the archive database. The archive database hosts audit data for a longer period of time, usually 60 days. The number of days each database can hold data is configurable.

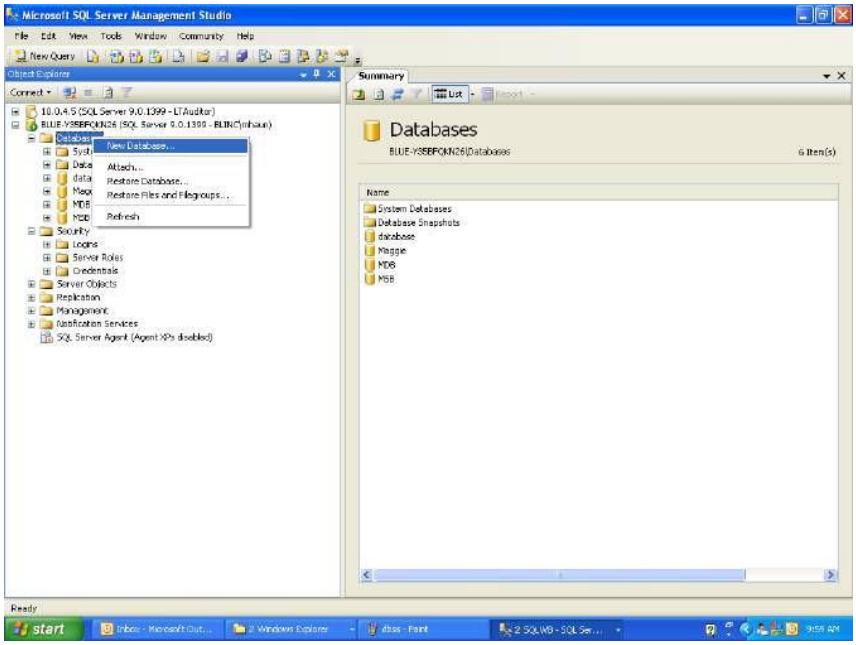
*NOTE MSSQL Server Agent must be configured for auto-start to ensure archive job can run.

LT Auditor+ Database on Microsoft SQL Server

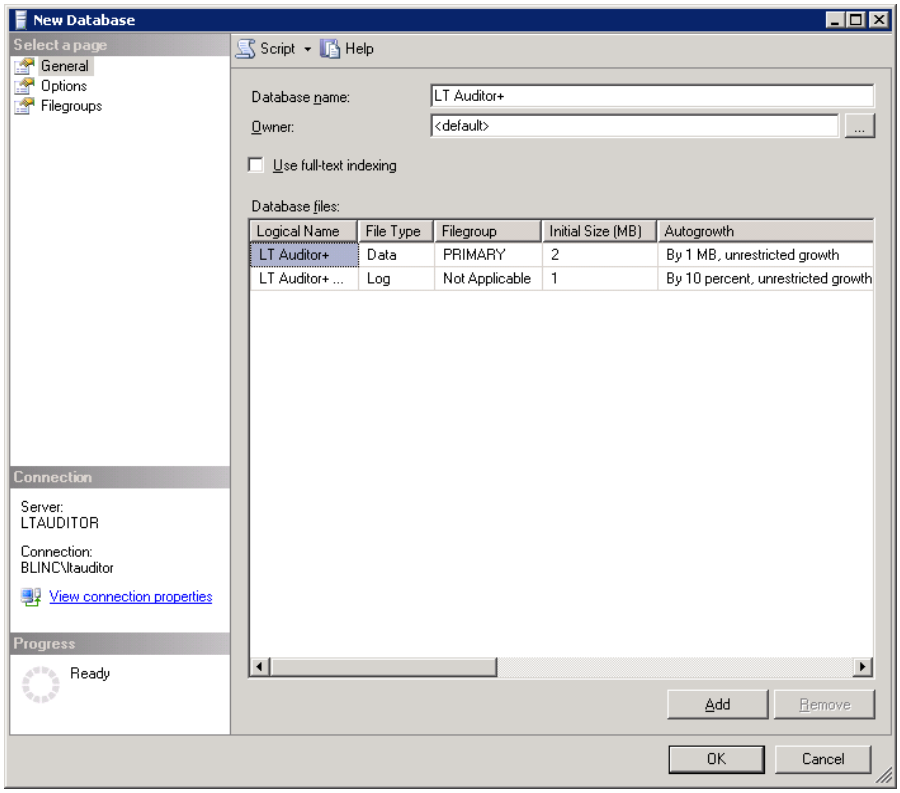
Creating a Microsoft SQL Database

1. From the Start menu, select Programs → Microsoft SQL Server → SQL Server Management Studio. SQL will prompt you to connect to the database engine.
2. Click Connect.

3. Once you have accessed the Management Studio, right-click on the database node in the left pane of the studio.



4. Select New Database.



To configure the database, specify:

- Name of the database
- Owner – Set as <default> unless you would like to specify otherwise.
- Initial size (MB) – Blue Lance recommends the following guidelines to determine the initial database size:

Number of Audited Servers	Database Size	Log File (1/5th database size)
< 25 Servers	500MB	100MB
> 25 Servers	1 – 5 GB	200MB – 1GB

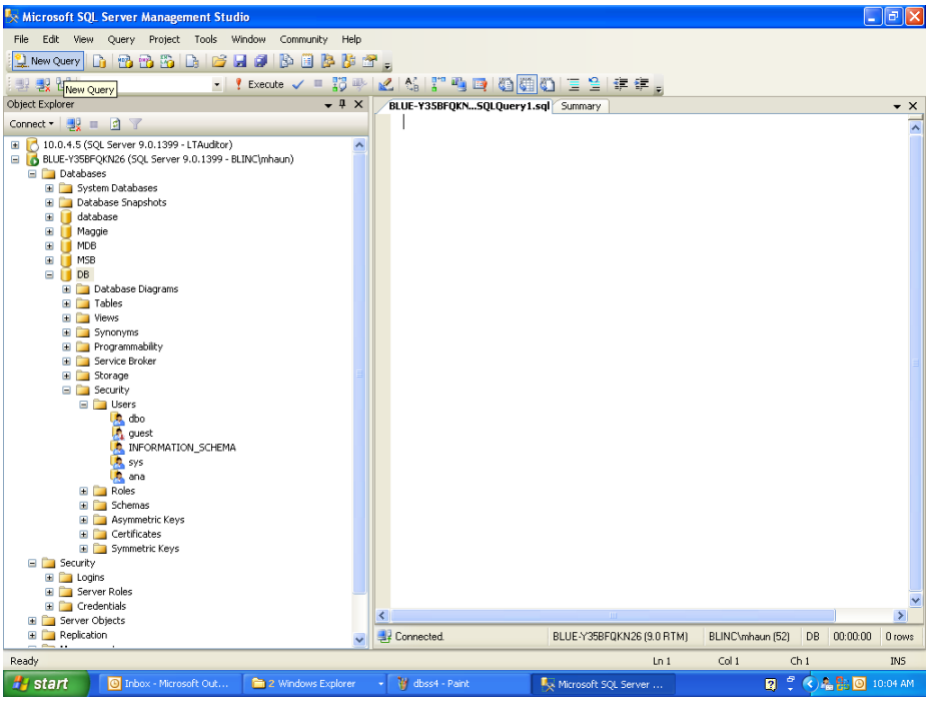
- Auto growth – Leave the default setting (10%)
- Path – Check with your DBA to select a path for data files other than the default path.

5. Click OK to create the database. Your new database should be displayed in the left pane of the studio.

Creating Database Objects

To create database objects for the LT Auditor+ database, the object creation script that ships with LT Auditor+ will have to be run. This script will need to be run using the SQL Query Analyzer as described below.

1. Select New Query in the toolbar seen in the upper left corner of the Microsoft SQL Management Studio.

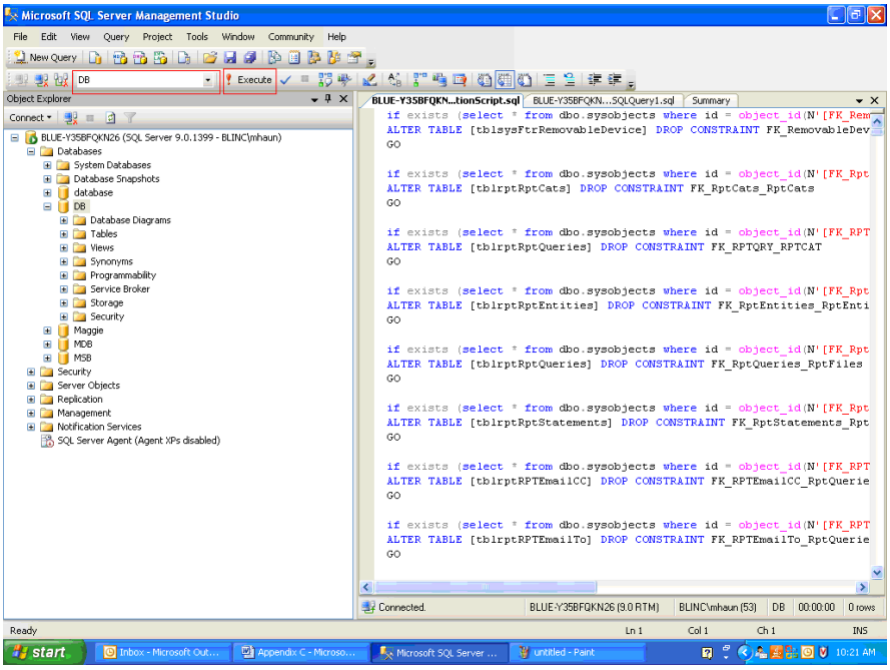


2. Locate the object creation script if you are creating the production database or the archive object creation script if you are creating the archive database. These scripts can be found in the LT Auditor+ CD or from www.bluelance.com.
3. Open the production database script from the following folder:
   \Database Scripts\Microsoft SQL\Production Database Scripts\ObjectCreationScript .sql
   – OR –
   Open the archive database script from the following folder:
   \Database Scripts\Microsoft SQL\Archive Database Scripts\ArchiveObjectCreationScript.sql
4. After selecting the proper script, SQL will prompt you to connect to the database engine again. Click Connect.

5. From the top left corner of the studio screen, select the new LT Auditor+ Database from the drop-down list next to the Execute button.

Note: Please be sure to select your new database from the drop-down menu before running the script. SQL will revert this setting to master after opening the file containing the script, but it must be set to your new database in order to properly run the script.

6. Click the Execute button to run the script.



This completes the creation of database objects for the LT Auditor+ Database.

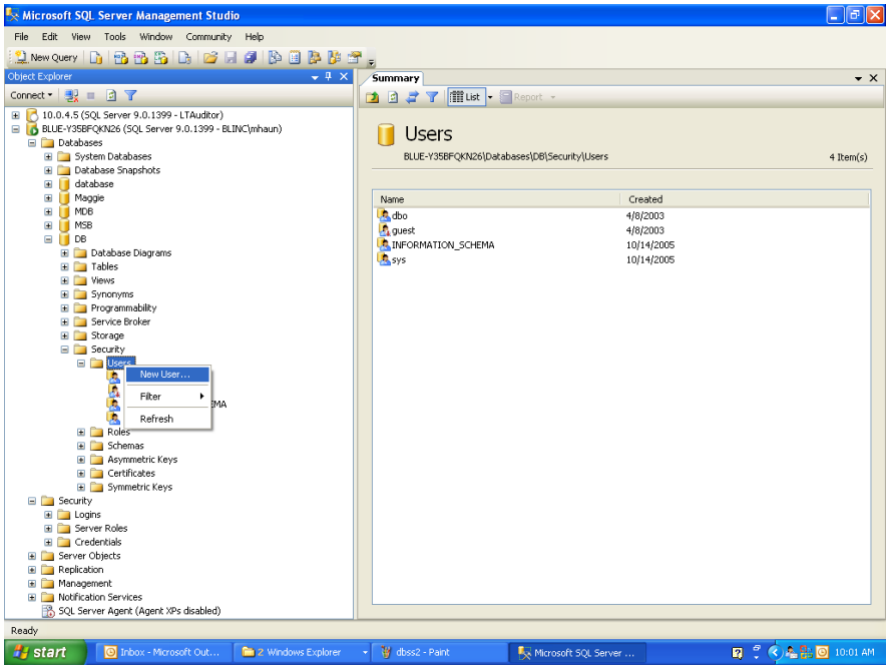
Setting Access Permissions

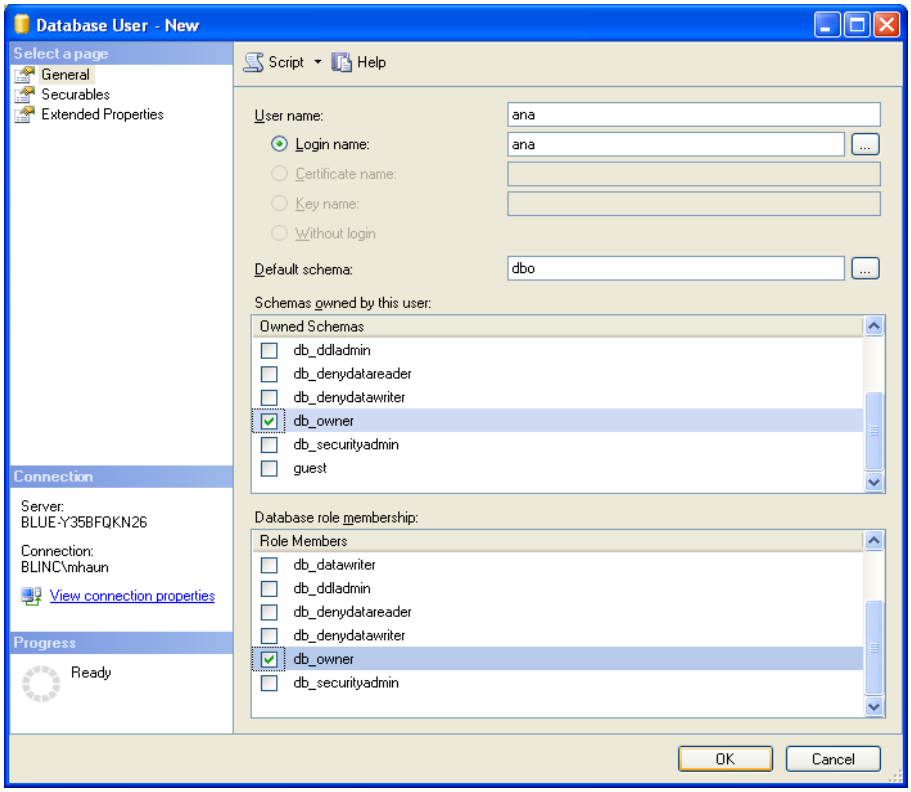
Database access permissions are needed for the following LT Auditor+ applications:

- LT Auditor+ Manager – Permissions are required to insert audit data into the database
- LT Auditor+ Report Generator – Permissions to run reports
- LT Auditor+ Manager Console – Permissions to configure LT Auditor+ settings

The following steps describe how to set up permissions for all LT Auditor+ applications:

1. Expand your New Database node, and then expand the Security node. RRight-click on the Users node. Select New User.

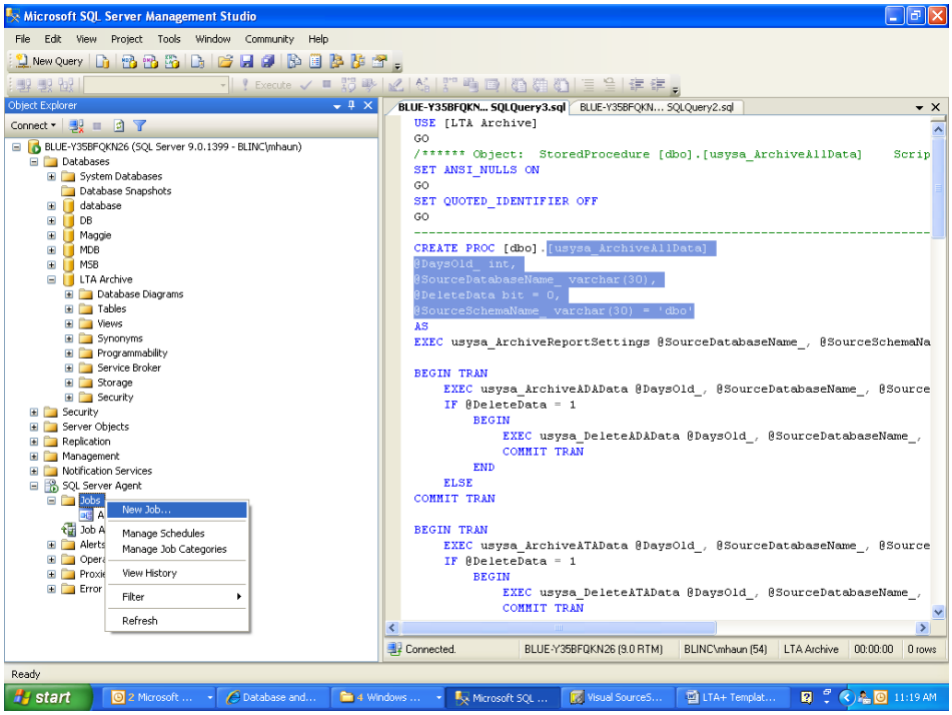




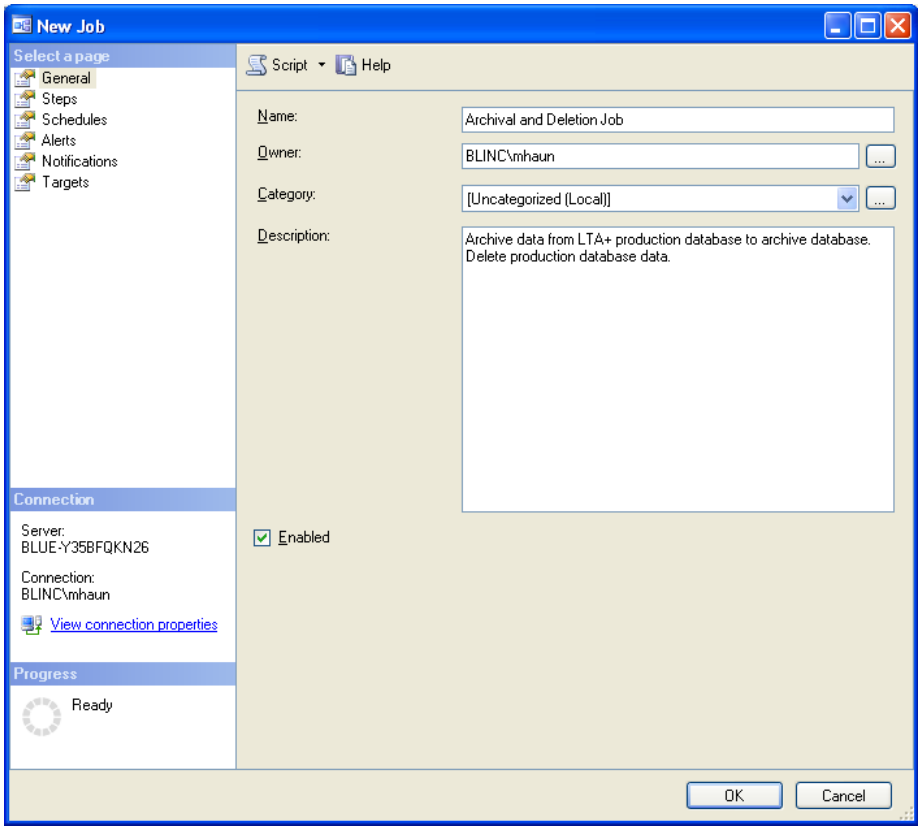
2. Fill in the username and login name. If you want to give this new user full permission to access LTA+, set the default schema to DBO. Then, in the field labeled Schemas owned by this user, check the box next to db_owner. In the field labeled “Database role membership,” check the box next to db_owner.
3. Click OK.

Configuring Maintenance Jobs

1. Under the SQL Server Agent node in the left pane of the SQL Management Studio, right-click on Job and select New Job.



2. The General page will be the first to open in the New Job window. Specify the name of the new job and its owner. Leave the category as default. Write a description of the new job in the description box.



3. Next, click on the Steps page in the "Select a page" area of the job properties box. Click New.
4. In the Job Step Properties window, name the step you are about to create. Leave the type as Transact SQL script (T-SQL). Under Database, select the archive database that you have already created from the drop-down menu. In the command window, begin by typing in the following:

   EXEC usysa_ArchiveAllData

   @DaysOld_= * — In place of the asterisk, enter the number of days old the data you are archiving should be before it is moved from the production database.

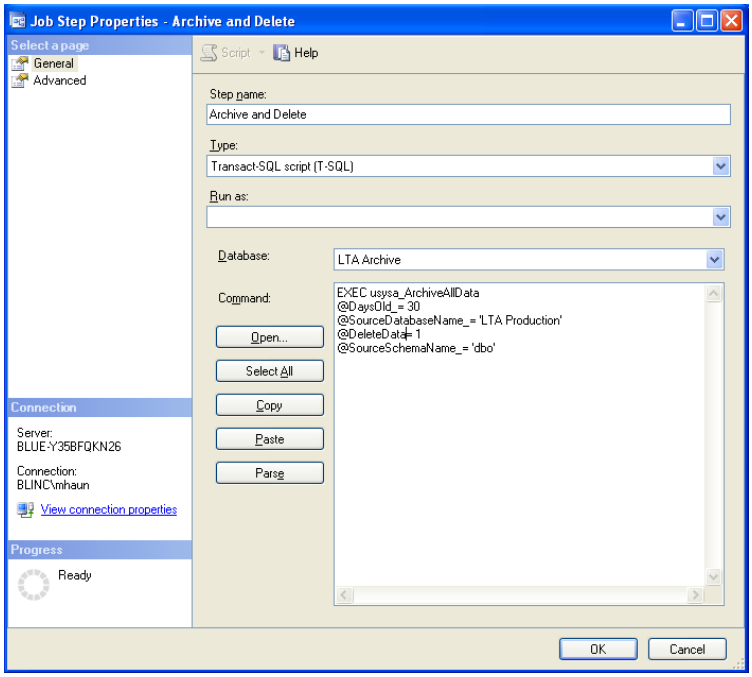
   @SourceDatabaseName_= ' * ' — Instead of the asterisk in the single quotes, type the name of your LTA+ production database.

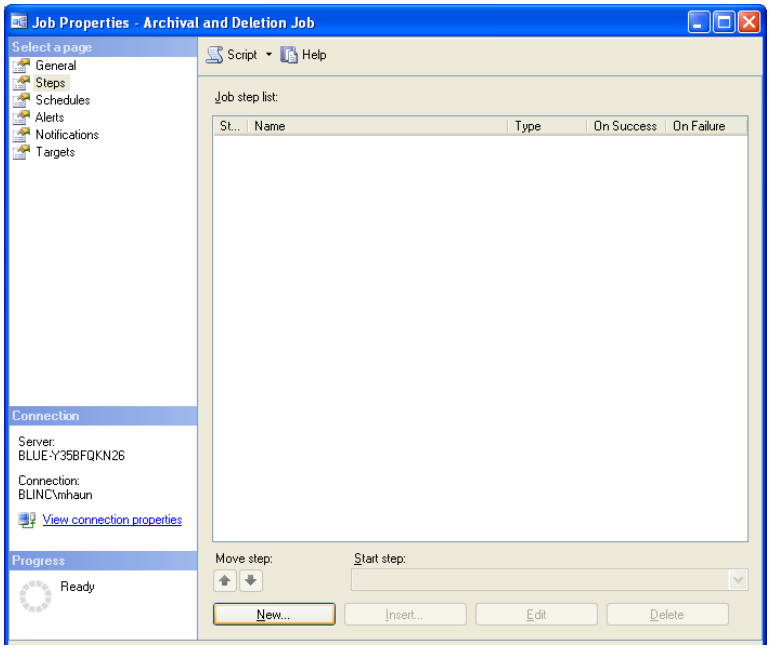
   @DeleteData= * — If you were to enter 1 in this field in place of the asterisk, the data archived would then be deleted from the production database. If 0 were entered, no would be deleted.

   @SourceSchemaName_= ' * ' — Instead of this asterisk, type the name of your database schema.

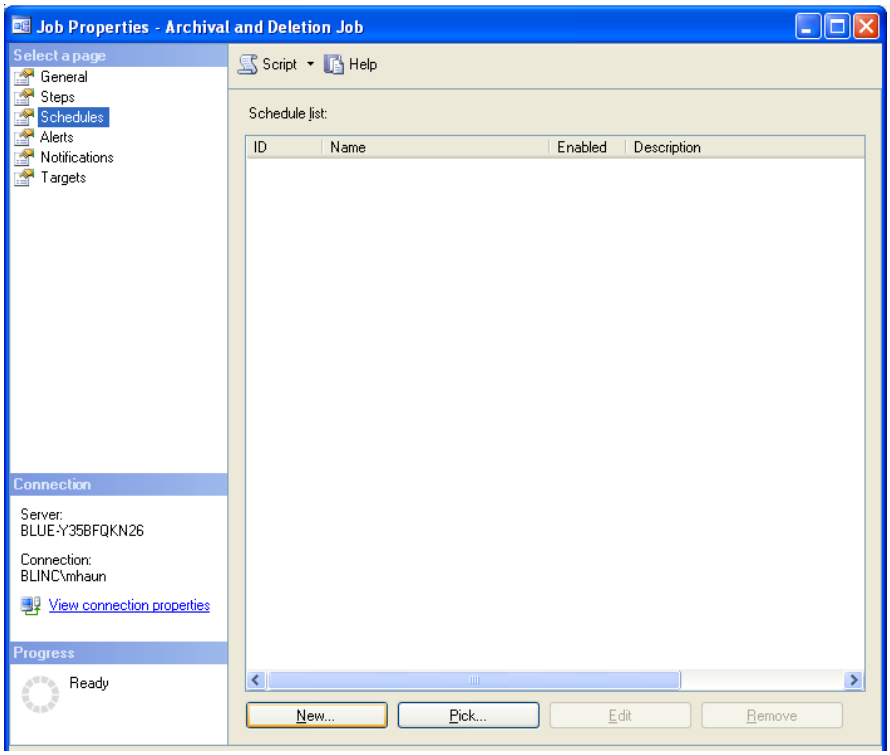
An example of this sequence with all of the fields filled in with common values is as follows:

EXEC usysa_ArchiveAllData
@DaysOld_=30,
@SourceDatabaseName_= 'LTA Production',
@DeleteData= 1,
@SourceSchemaName_= 'dbo'



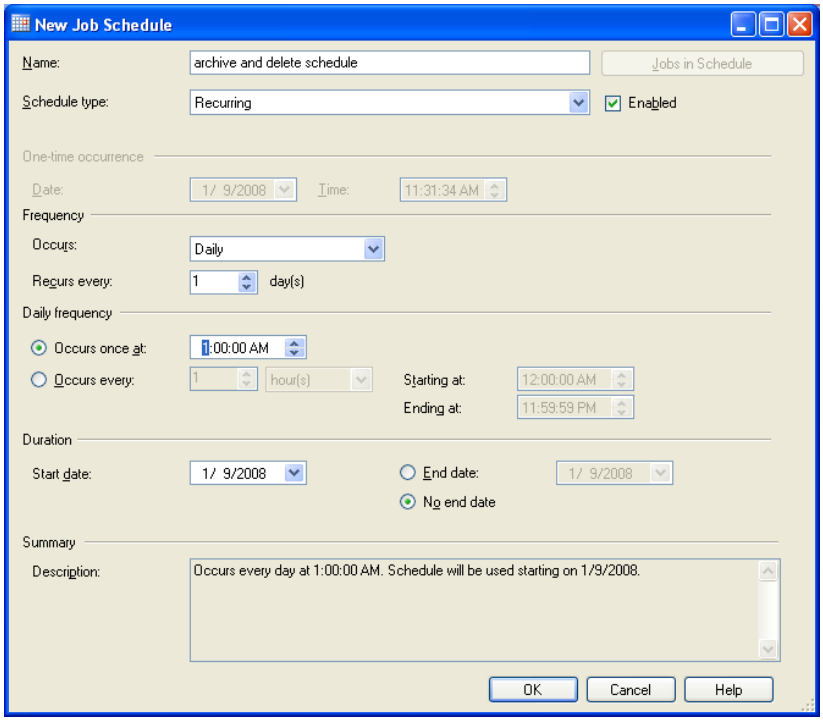


5. Click OK. Then, under the Job Properties window, select the Schedules page. Click New.

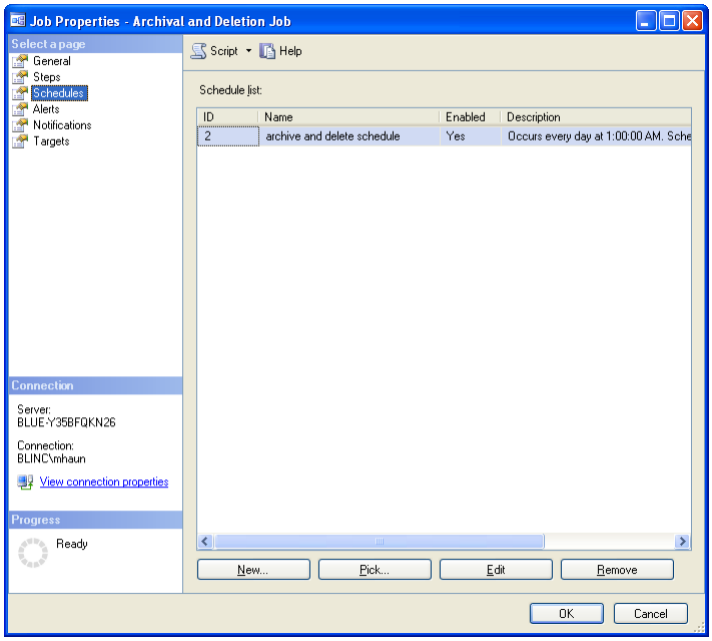


The Schedules page would contain the following:

1. Name your new job schedule.
2. Choose Recurring as the Schedule type if you want this job to run automatically at a scheduled interval.
3. Choose the frequency with which you would like the job to occur.
4. When selecting a daily frequency, you may choose to have the job run either every one day, every two days and so on by changing the number in the box next to "Recurs every."
5. Under the "Daily frequency" section, you may choose to run the job once a day or once every several hours, starting and ending at chosen times depending on your company's needs.
6. When running the job once daily, most users choose to configure this job to run at a time when there is little to no activity in the enterprise.
7. A verbal description of the schedule you have configured will show in the bottom of this window under the heading Summary. Once the job schedule has been configured to your needs, click OK.



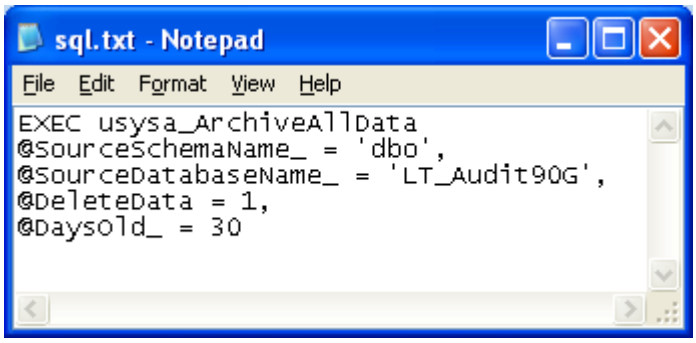
8. In the Job Properties window, click OK. The new job will take a moment to be saved, and the window will close. In the Management Studio, your new job should appear in the left pane under the Jobs node.


Job Properties - Archival and Deletion Job
Select a page
General
Steps
Schedules
Alerts
Notifications
Targets
Script
Help
Schedule list:
ID
Name
Enabled
Description
2
archive and delete schedule
Yes
Occurs every day at 1:00:00 AM. Sche
Connection
Server:
BLUE-Y35BFQKN26
Connection:
BLINC\mhaun
View connection properties
Progress
Ready
New...
Pick...
Edit
Remove
OK
Cancel

Configuring Maintenance Jobs Using SQL Server Express

To configure a scheduled maintenance job in SQL Server Express, you must create a batch file that will be run by Windows Scheduler. This process begins by creating a text file that includes the job information necessary to archive data from the production database to the archive database and delete from the production database if desired. You will then create a batch file containing that sequence of switches necessary to run the stored procedure in the text file in SQL Express through a command prompt. That batch file can then be configured to run on a regular basis through Windows Scheduler, thus regularly running the maintenance job.

1. Create a text file named **sql.txt** in the Notepad application.



SQL.TXT

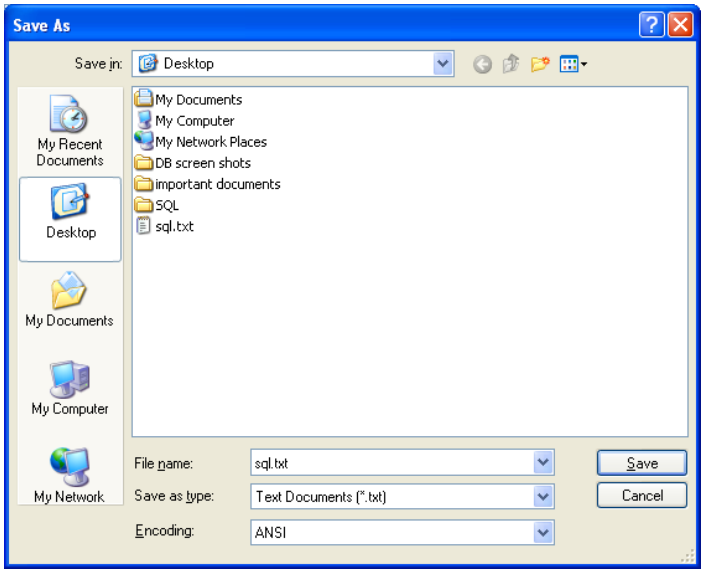
The **sql.txt** file should contain the following information:

EXEC usysa_ArchiveAllData

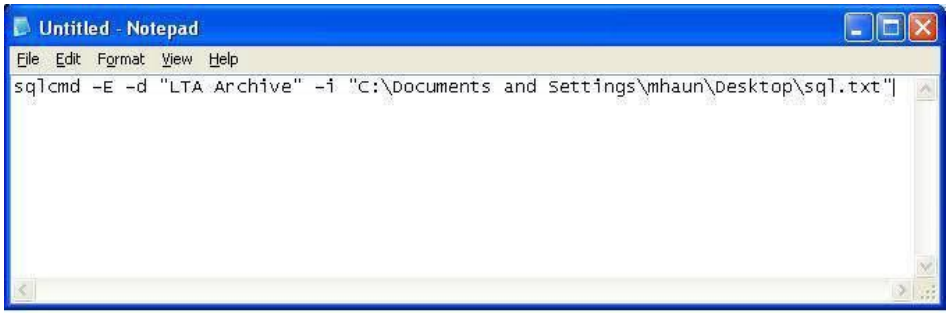
- **@SourceSchemaName_= ' * '** — Instead of this asterisk, type the name of your database schema.
- **@SourceDatabaseName_= ' * '** — Instead of the asterisk in the single quotes, type the name of your LTA+ production database.
- **@DeleteData= *** — If you were to enter 1 in this field in place of the asterisk, the data archived would then be deleted from the production database. If 0 were entered, no data would be deleted.
- **@DaysOld_= *** — In place of the asterisk, enter the number of days old the data you are archiving should be before it is moved from the production database.

An example of this sequence with all of the fields filled in with common values is as follows:

EXEC usysa_ArchiveAllData
@SourceSchemaName_= 'dbo',
@SourceDatabaseName_= 'LTA Production',
@DeleteData= 1,
@DaysOld_=30



2. Create a batch file named **sql.bat** in the Notepad application.



SQL.BAT

This is the sequence of switches for the SQL batch program:

sqlcmd -E -Sblue-labsqlexp01 -dlt_archive90 -ic:\sql.txt

Individually, these switches are as follows:

sqlcmd — This is the command that runs the process.

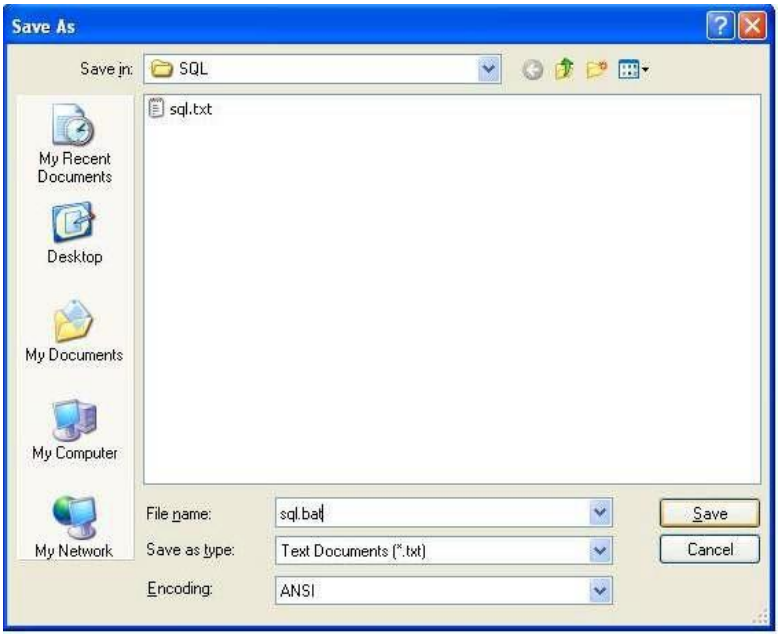
-E — This is the command that runs the process with NT Integrated security so no username or password is required. Should you want to use username and password security, substitute the switches –U and –P, followed by your username and password respectively.

-SSQLserverName — Enter -S then your sql server name using no spaces.

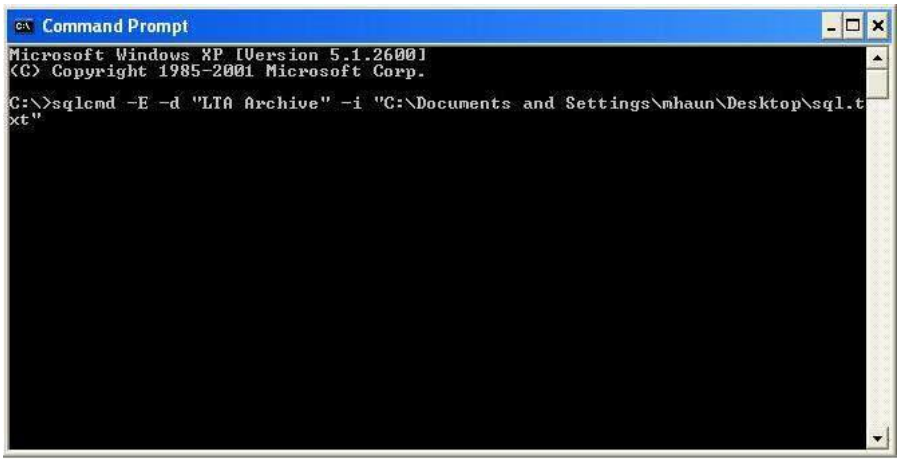
-dDatabaseName — Enter -d then the database name using no spaces.

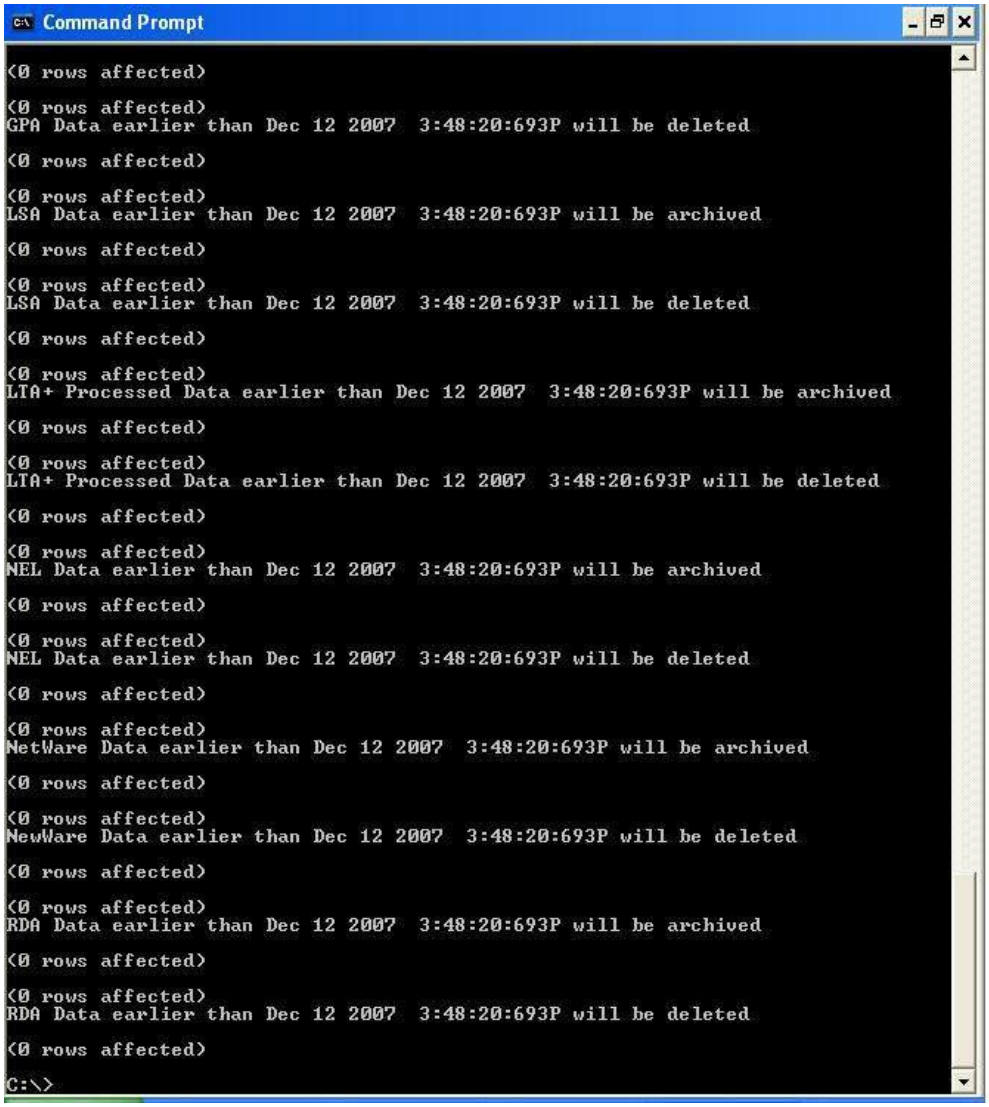
-IC:\SQL.TXT —This is the path for the text file (sql job script).

Enter -I then the path using no spaces. Blue Lance recommends keeping the path very simple.

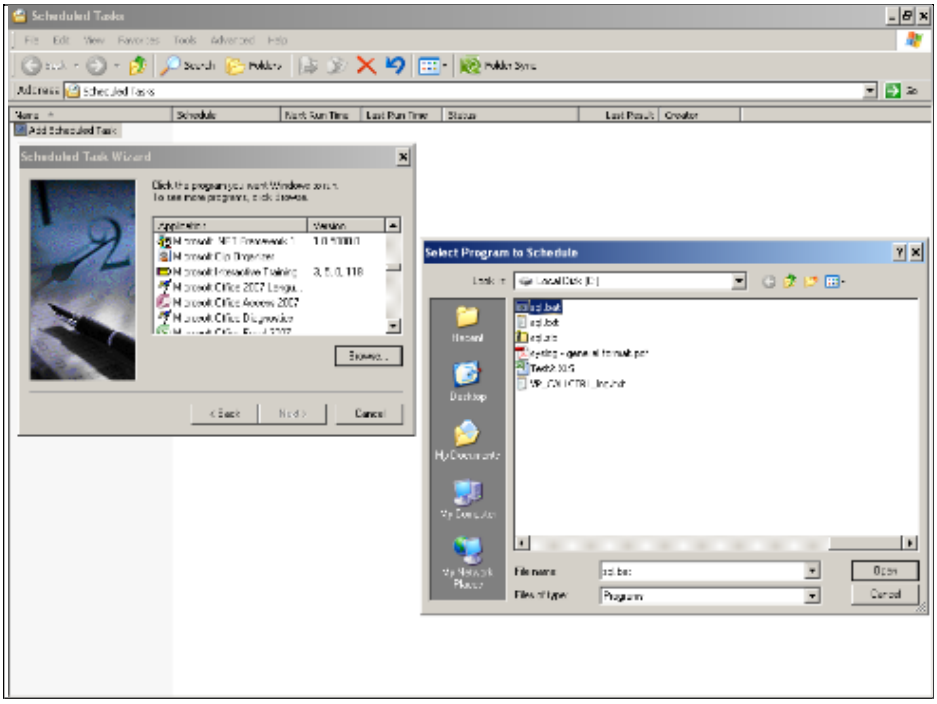


3. This sequence will be run from the command prompt window, so to test for syntax errors and ensure that the sequence runs properly, copy the sequence from your batch file and paste it into the command prompt.
4. Press enter to run the sequence. The following should appear, if the sequence is entered, and run properly:

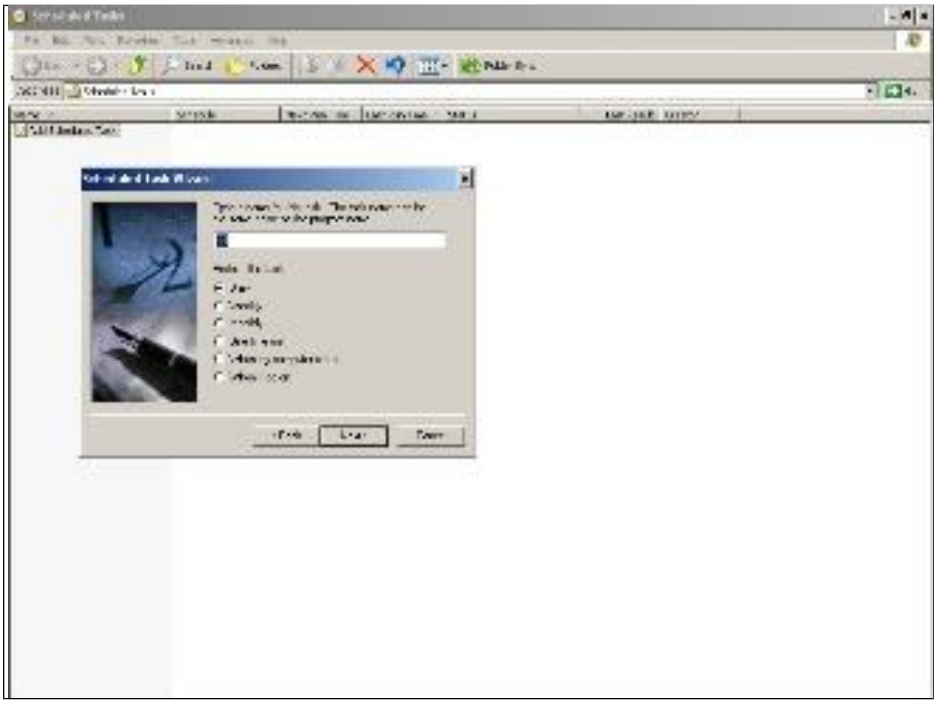




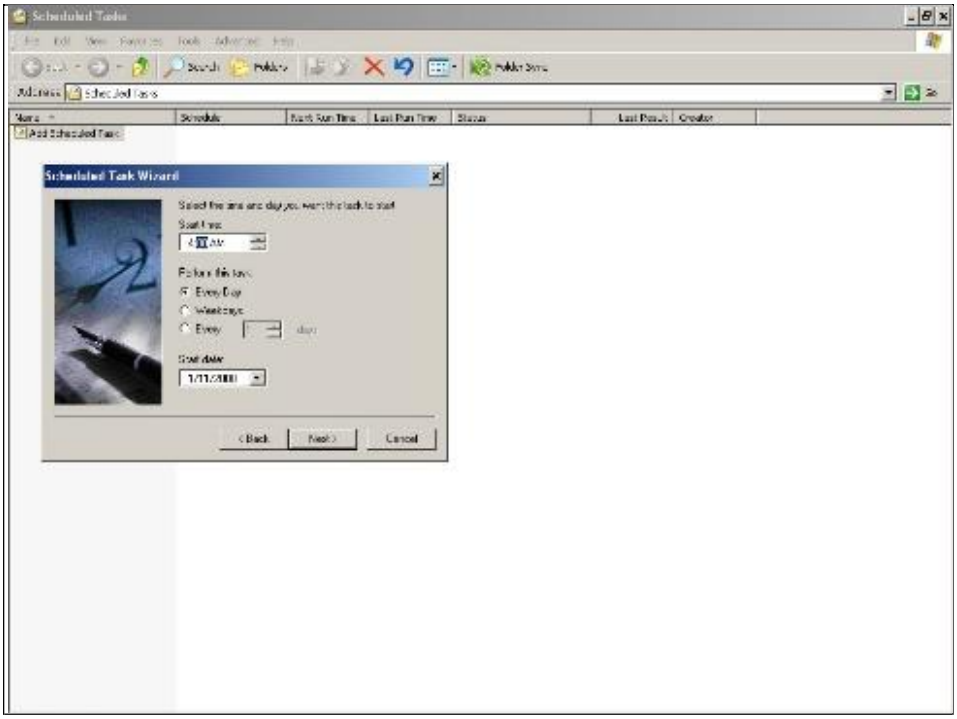
5. Once you have created both batch and text files successfully, open Windows scheduled tasks. Double-click on Add New Task to start the wizard. Open the file name for the SQL batch program.



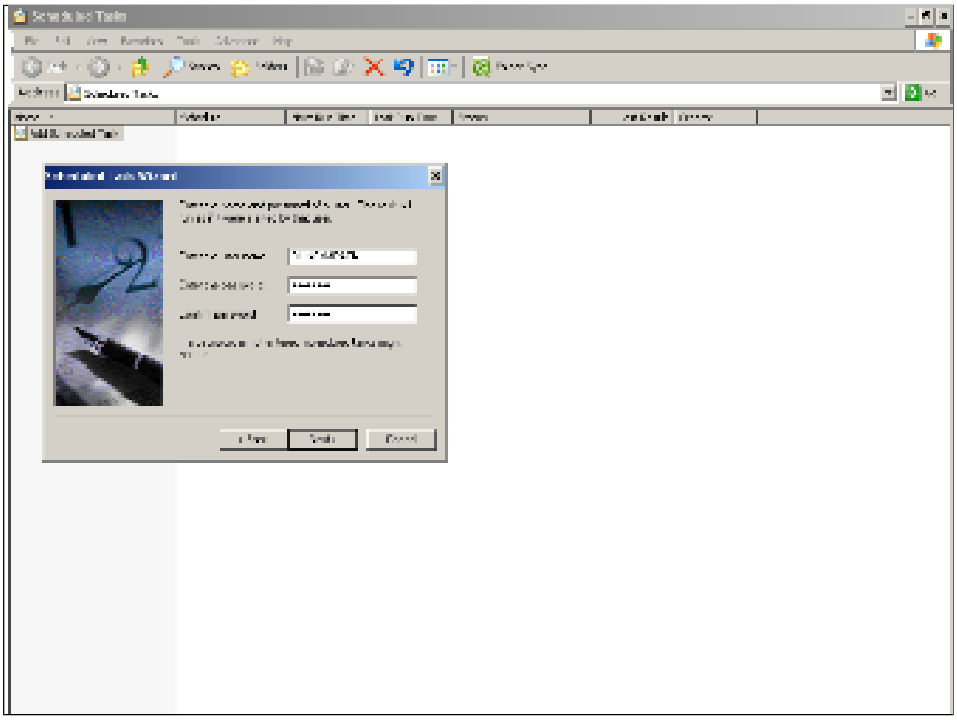
6. Name the job and select the frequency with which you will configure how often the batch is run.



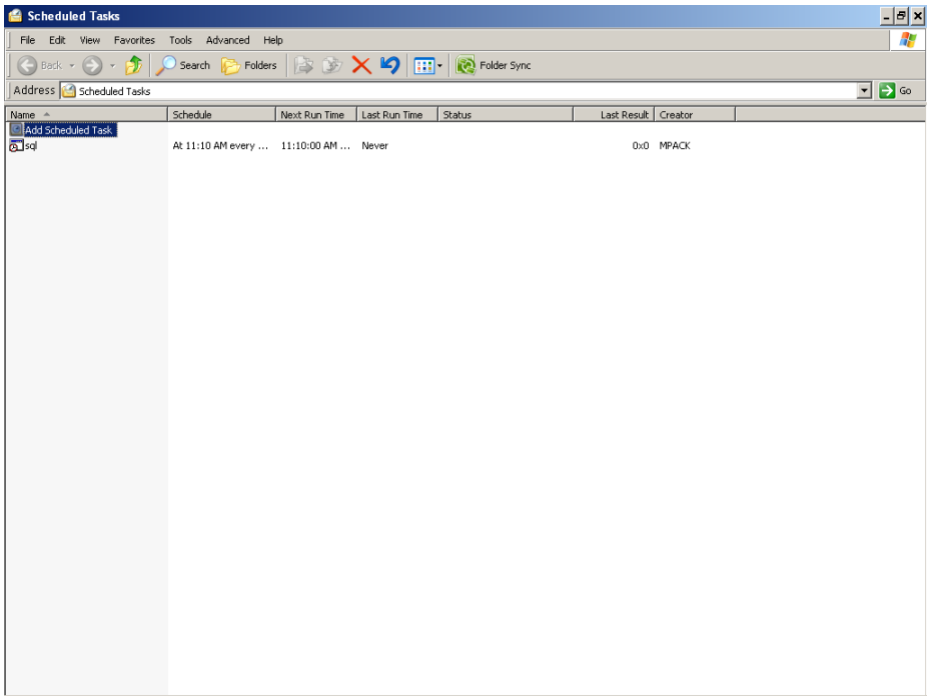
7. Select the time the batch will run. Click Next.



8. Enter a valid username and password that will allow access to the batch file.



9. If created correctly you should see a scheduled job entry as shown in the window below.



Oracle

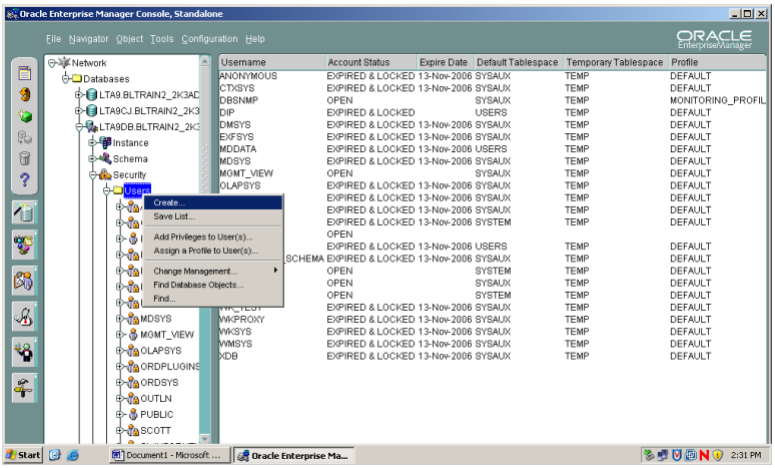
Create the database that will be used for LT Auditor+ for Windows 9.0 using the Database Configuration Assistant. For help, please contact your Oracle DBA.

Setting Access Permissions

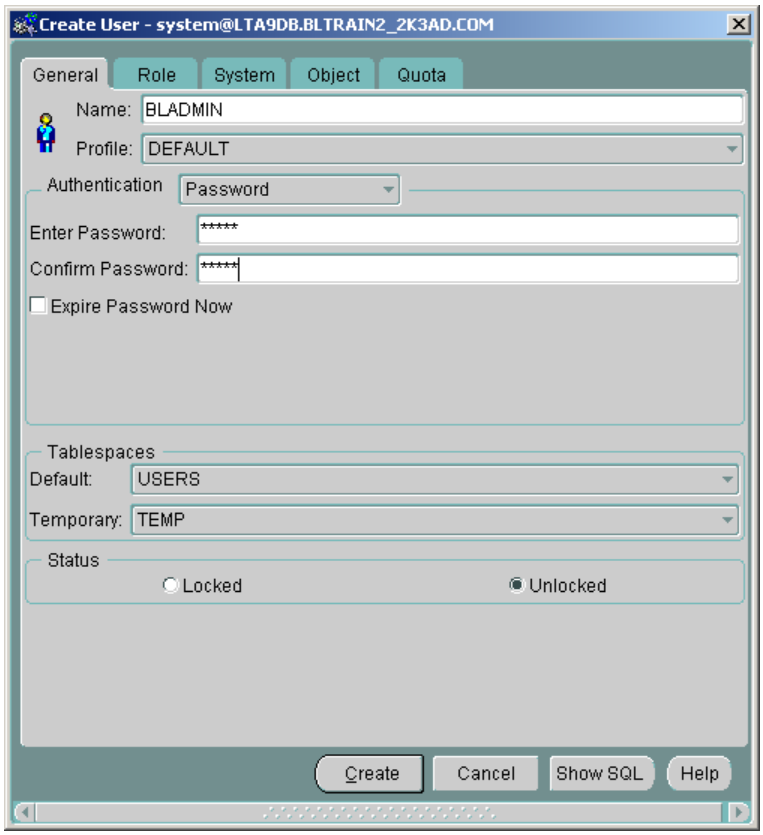
1. Click on the database. The following screen will pop up:

2. Connect to the database using the System account and connect as SYSDBA.

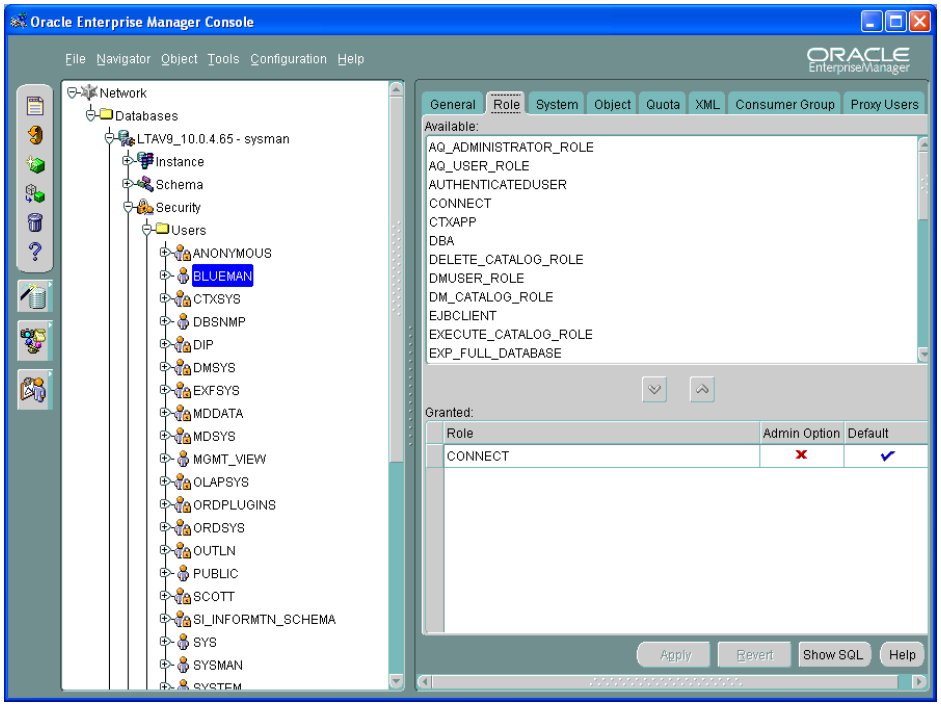
3. Click on the database; go to Security → Users → Create.



4. Enter the name and password for the user you would like to create.

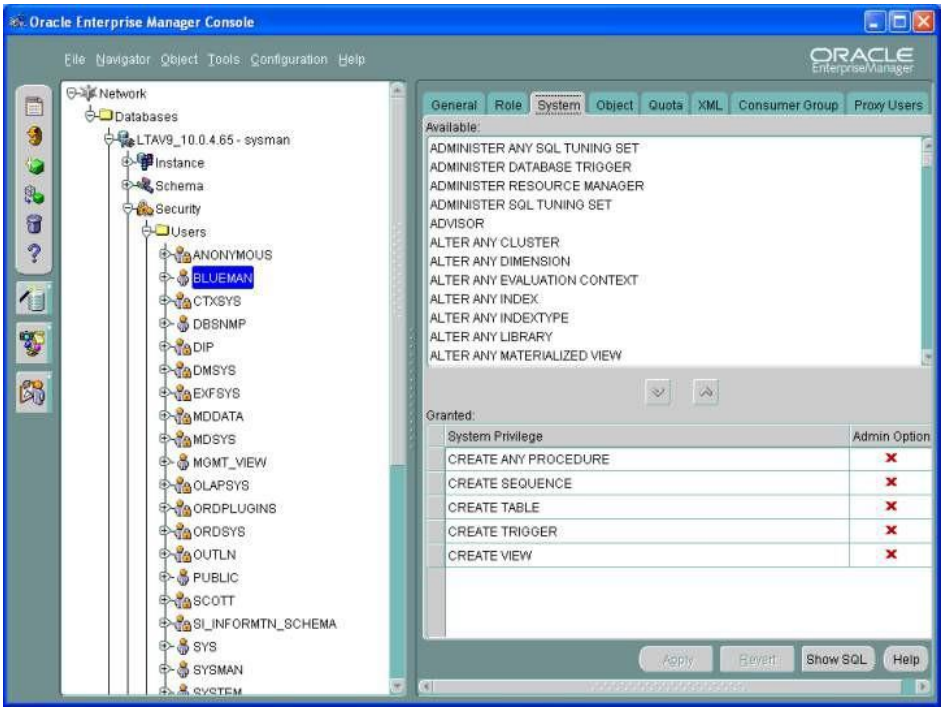


5. Go to the Role tab and give the user the “Connect" role.

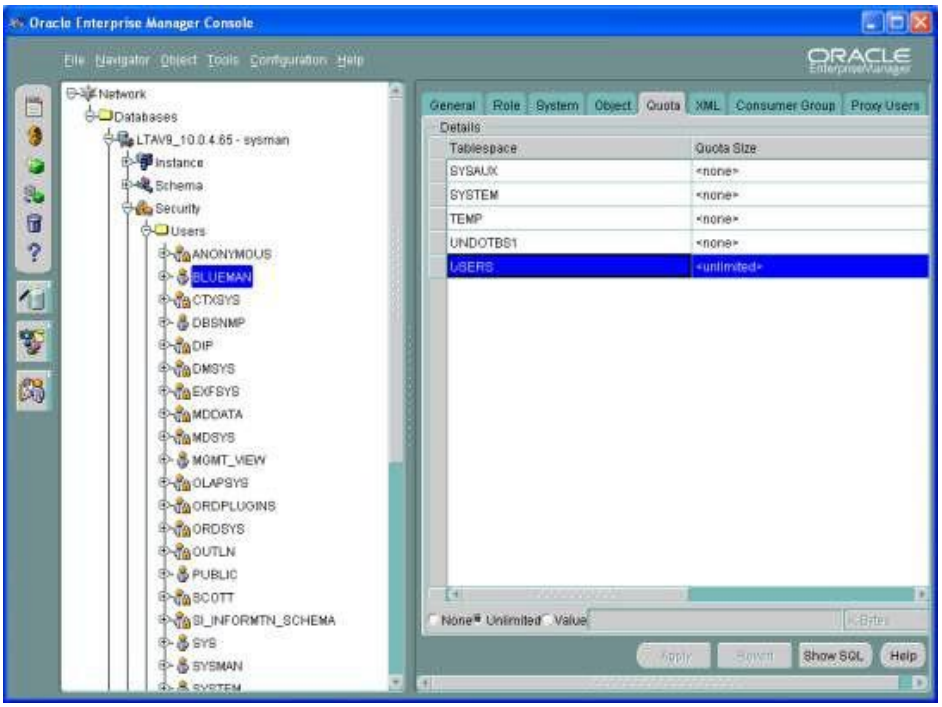


6. Go to the System tab and give the user the following permissions:

   - Create any procedure
   - Create sequence
   - Create table
   - Create trigger
   - Create view



7. Under the Quota tab assign values, should you choose to set size limitations.

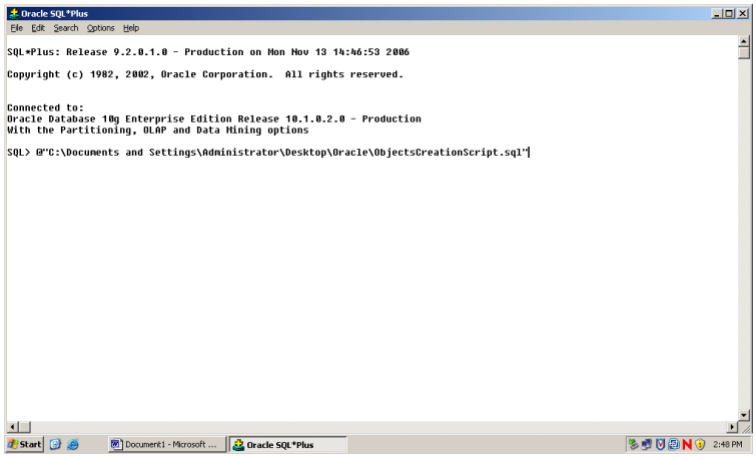


8. Go to SQL Plus and log in.

Once the database is created, run the script from the following location on the CD:

\Database Scripts\Oracle\ObjectScripts.sql

Running this script will create all the necessary tables, stored procedures and views required by LT Auditor+.

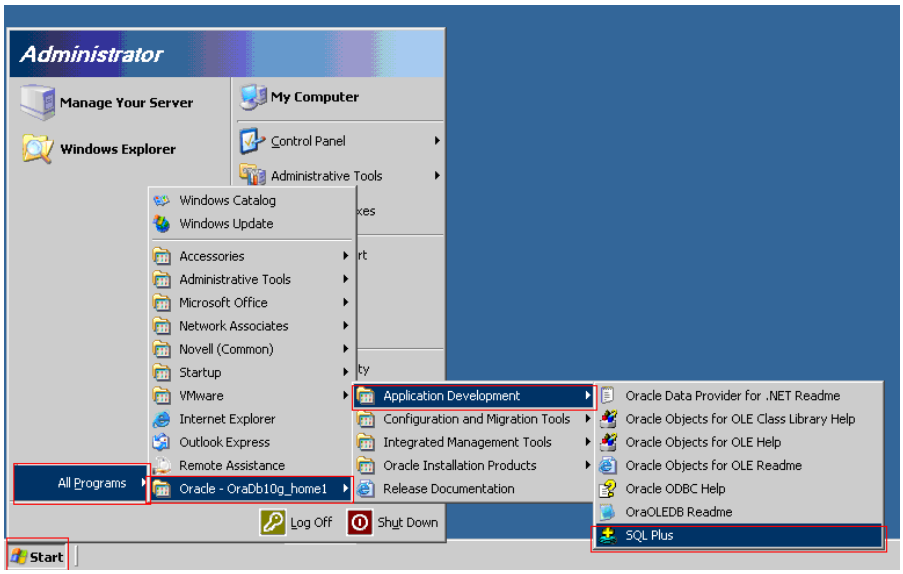


Configuring Maintenance Jobs

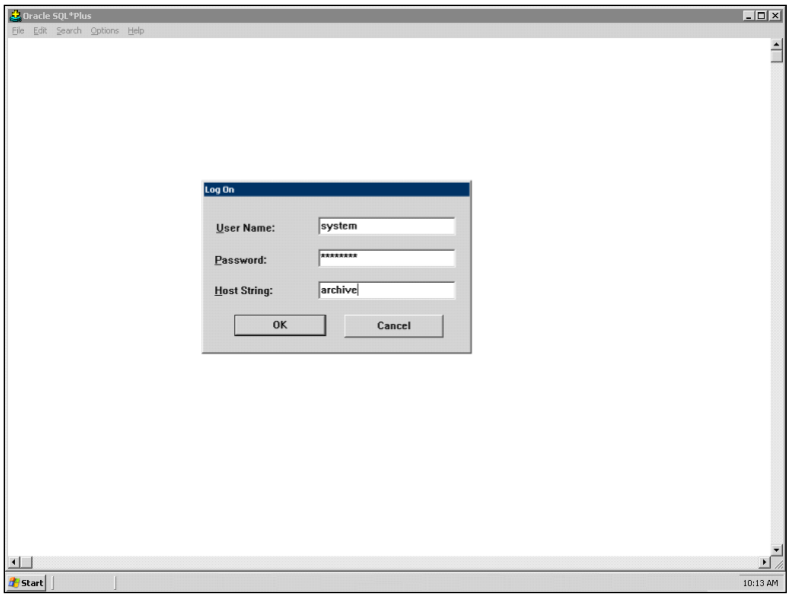
The following steps show the processes of running the data archive and deletion script and the delete archive data script using Oracle 9i or 10g. The archive and deletion script may be run using a set date range. Please note that when running that script, a public database link must first be created in the archive database that points to the production database. Alternatively, the database link may be pointed to the production schema in the same database as the archive schema. You may enter a start date and end date to specify the archive and deletion parameters. For instance, you may enter the start date as 1/1/2000 and the end date as 7/1/2000; the archive or deletion will begin on your specified start date at exactly 12:00:00 a.m. and will terminate on your specified end date at exactly 11:59:59 p.m. The delete archive data script deletes archived data when it reaches a certain number of days old as specified in the executable script.

To run either script on Oracle 10g, please follow the sequence of steps below:

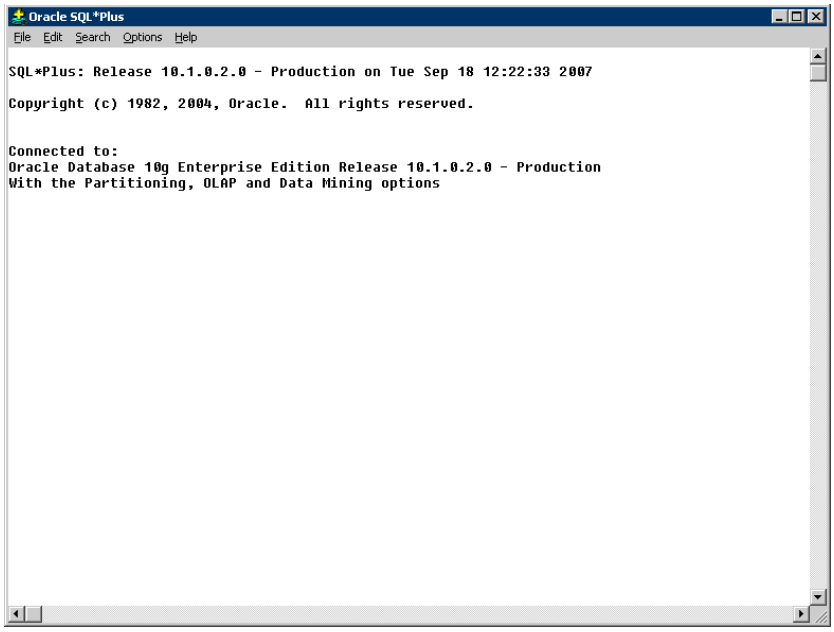
1. Go to Start → All Programs → Oracle – OraDb10g_home1 → Application Development → SQL Plus



2. This will direct you to the Log On screen, where you will need to enter the username, password and host string that has privileges to the schema.

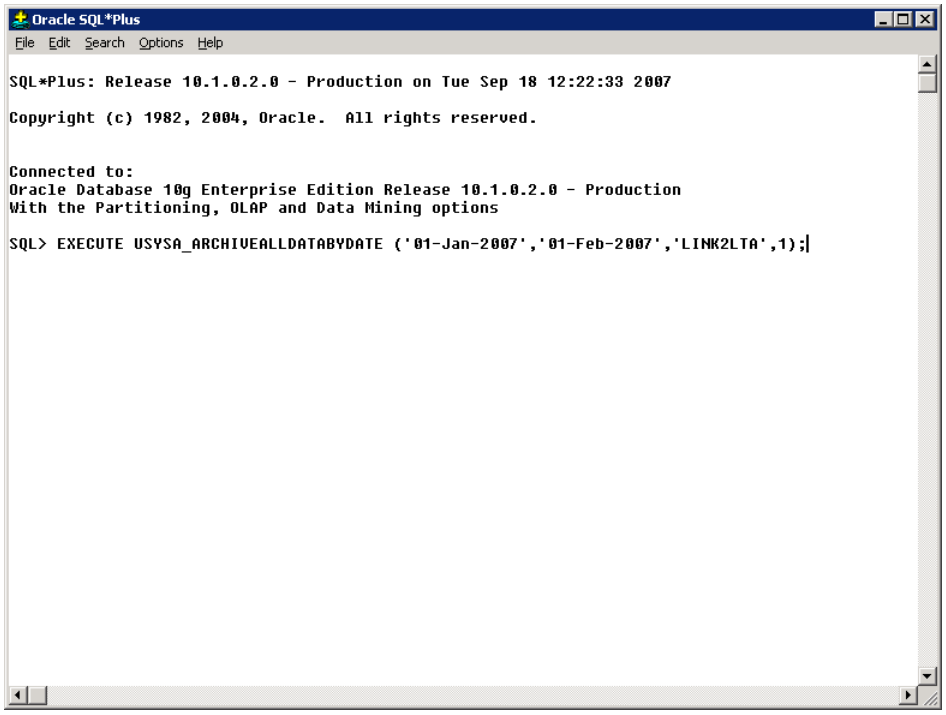


3. Once you have logged on successfully, SQL Plus will connect to the database and allow you to type in the executable procedure that will run the archive and deletion script.



4. Type in this executable procedure to copy data from the production database to the archive database and delete the copied data from the production database:

EXECUTE USYSA_ARCHIVEALLDATABYDATE ('01-Jan-2007', '01-Feb-2007','LINKTOLTA',1);



To perform the same function using age of data as the defining parameter, type in the following executable procedure:

EXEC usysa_ArchiveAllData

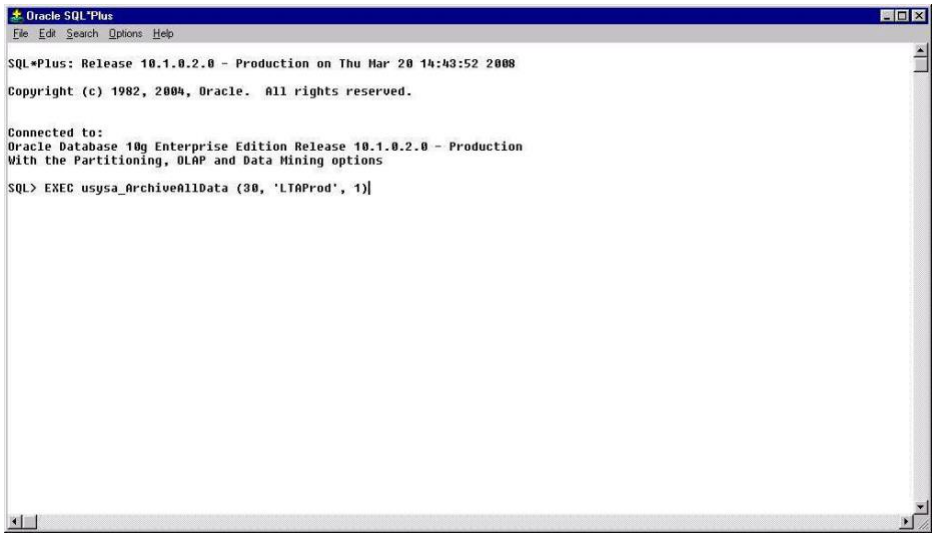
DaysOld_=>* , — In place of the asterisk, enter the number of days old the data you are archiving should be before it is moved from the production database.

SourceDatabaseName_=>‘ * ’ , — Instead of the asterisk in the single quotes, type the name of your LTA+ production database link.

DeleteData=>* — If you were to enter 1 in this field in place of the asterisk, the data archived would then be deleted from the production database. If 0 were entered, no data would be deleted.

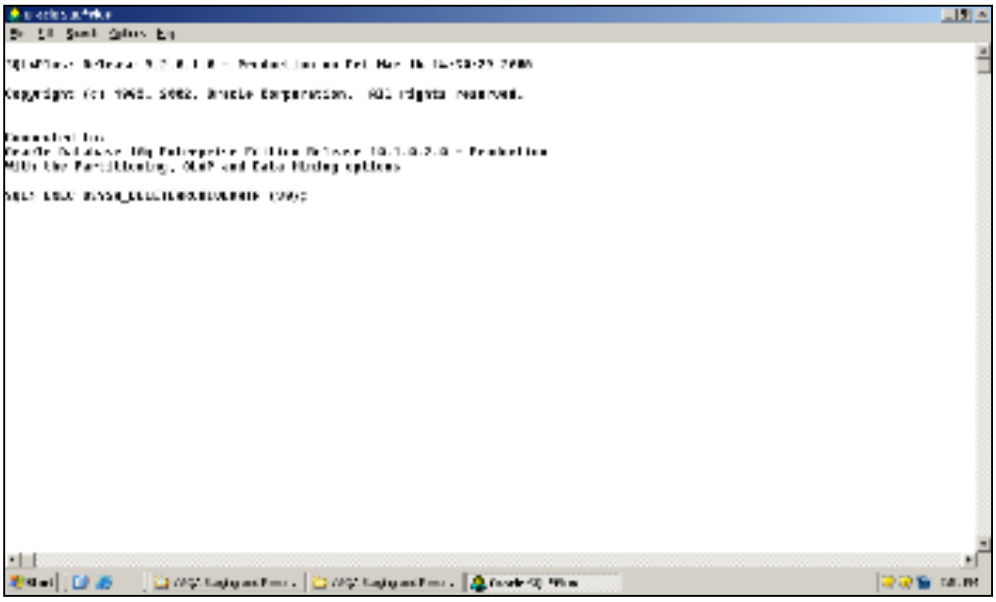
These parameters may be entered in the list style as shown above or as a string of parameters separated by commas without their parameter named listed, as shown below:

EXEC usysa_ArchiveAllData (30 , ’LTAProd’ , 1)



To delete data that is a certain number of days old from the archive database, type in the following executable procedure:

EXEC usysa_DeleteArchiveData (*) — The asterisk represents the number of days that data must have been stored in the database before it may be deleted.



Getting Technical Support

If at any time you require technical support on the product, or you have technical support questions that this document does not cover, you can contact Blue Lance.

CONTACT METHOD	ADDRESS OR NUMBER	DESCRIPTION
Phone	800-856-BLUE or 800-856-2583 in USA +1 713-255-4800 outside USA	Technical support hours are Monday – Friday 8:30 a.m. to 5:50 p.m. CST.
Email	support@bluelance.com	

Blue Lance, Inc.
410 Pierce St
Suite 300
Houston, TX 77002
800-856-2583
+1 713-255-4800