



LT Auditor+ Build21 Release

Upgrade Guide

Table of Contents

Overview	3
Prerequisites	3
Upgrading the LT Auditor+ Manager	5
Upgrading the LT Auditor+ Database	15
Microsoft SQL Servers	15
Oracle	16
Directly Upgrading the LT Auditor+ Management Console	17
Directly Upgrading the LT Auditor+ Reporting Console	21
Upgrading LT Auditor+ Windows Agents	24
APPENDIX A – What is New in Build21	27
LT Auditor+ Best Practices Panels	27
Auditing of EMC Isilon Network Attached Storage (NAS) Devices	27
Auditing GPO Policy Preferences	27
Enhanced Access Control to LT Auditor+ Consoles	27
Enhanced Active Directory Auditing Capability	27
Enhanced Email Support	27
Splunk Integration	27
APPENDIX B – Enhanced Active Directory Notifications	28
Notification with Additional Attributes	28
APPENDIX C – Installing LT Auditor+ App for Splunk	33
Single Instance	34
Distributed Environment	42
Deploy LT Auditor+ App for Splunk Add-on to Peer Nodes	42
Deploy LT Auditor+ App to Search Heads	42

Deploy LT Auditor+ Add-on to Heavy Forwarder:44

Overview

Build21 introduces new enhancements with powerful reporting capabilities, and these details are discussed in [APPENDIX A](#). This document provides instructions on how to upgrade to Build21 and involves upgrading the following LT Auditor+ components:

1. LT Auditor+ Manager
2. LT Auditor+ Database
3. Updating all instances of the LT Auditor+ Management Console
4. Updating all instances of the LT Auditor+ Reporting Console
5. LT Auditor+ Windows Agents in the environment

Prerequisites

- LT Auditor+ 2013 – An upgrade to Build21 is only permitted if your current version is LT Auditor+ 2013 or newer. If you are on a prior version, either upgrade to LT Auditor+ 2013 or please contact Blue Lance for other options.
- Database Rights – To upgrade the database the user must have 'dbo' or full rights on the LT Auditor+ production and archive databases.
- System Rights – The user performing the upgrade on the LT Auditor+ Manager must have administrative rights.

Build21 Components

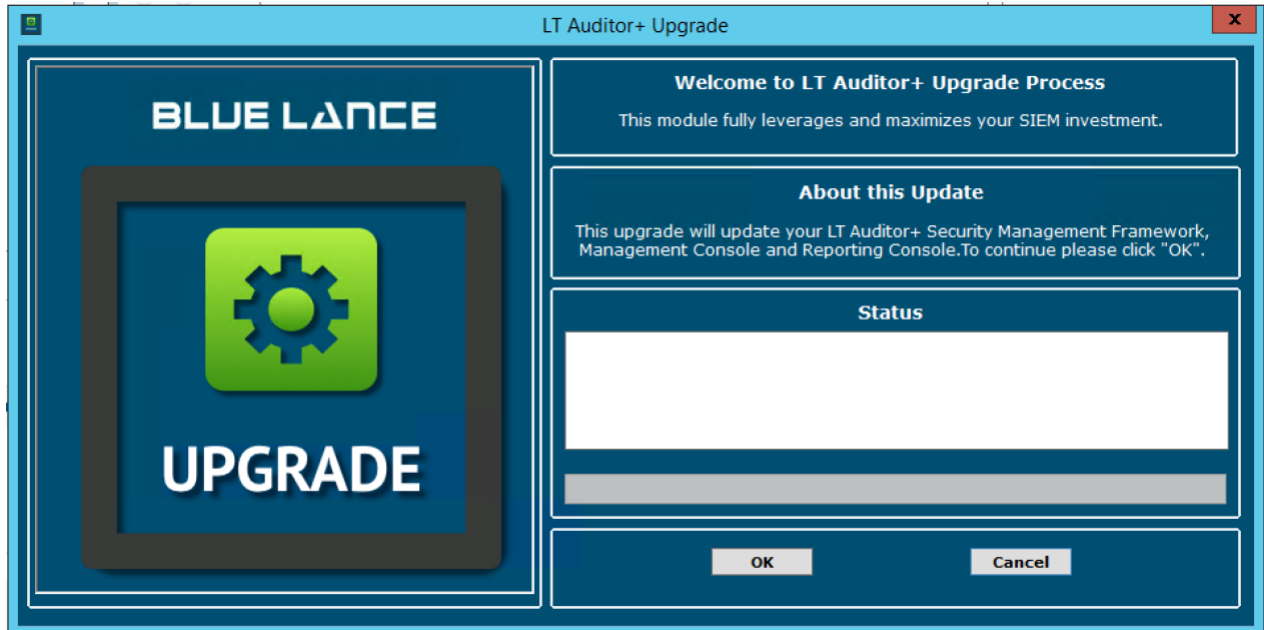
When you download and extract the Build21.zip file, please make sure that the following files and folders exist.

Component	Description
Database Scripts	Database Scripts Folder
Setup_MC_x64.exe	Management Console (64 bit)
Setup_RC_x64.exe	Reporting Console (64 bit)
Setup_SMF_x64.exe	Security Management Framework (64 bit)

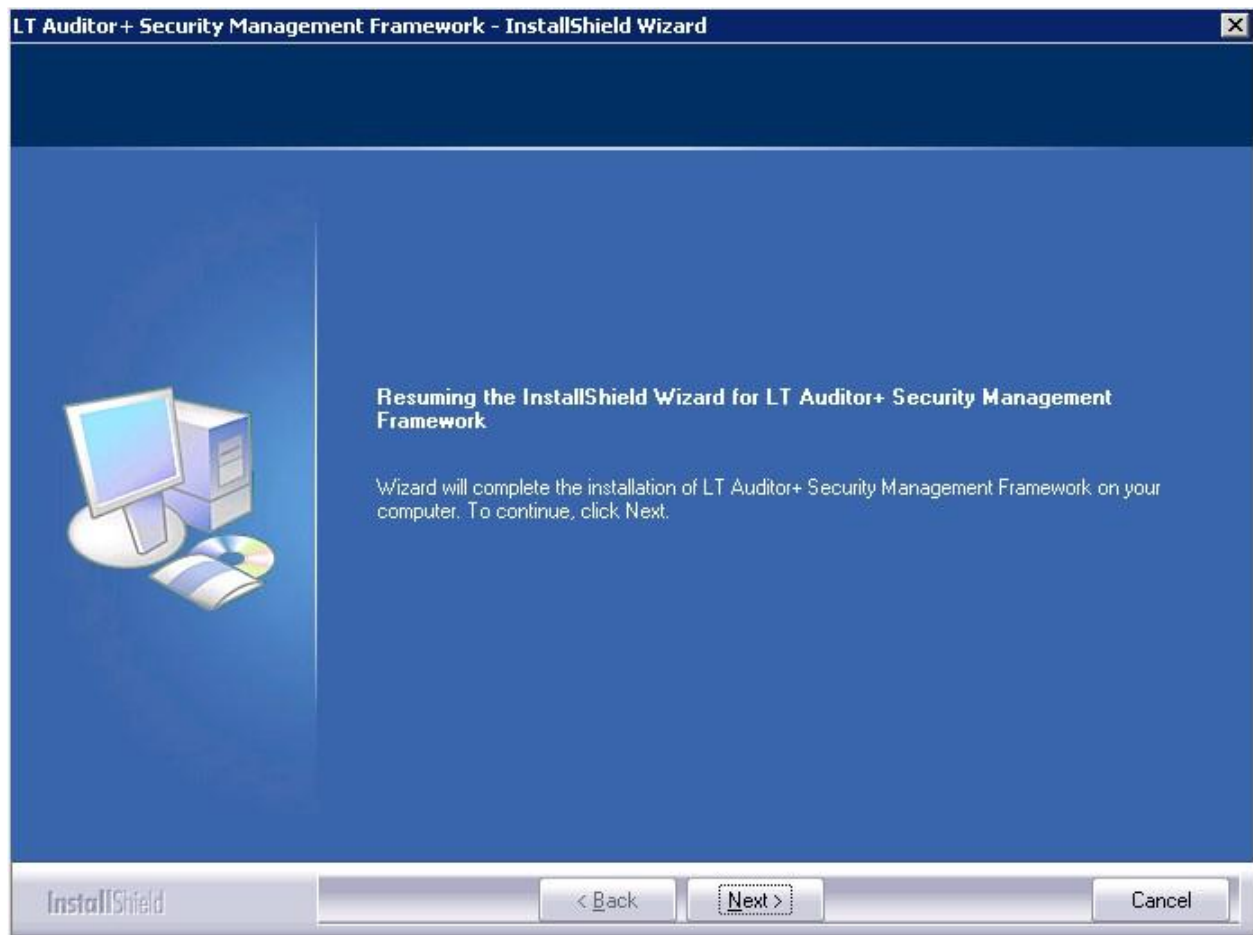
Upgrading the LT Auditor+ Manager

Follow the steps below to upgrade LT Auditor+ Manager.

1. Copy the Build21 component files to a temporary folder on the LT Auditor+ Manager machine.
2. Run LTUpgrade.exe to launch the following screen.

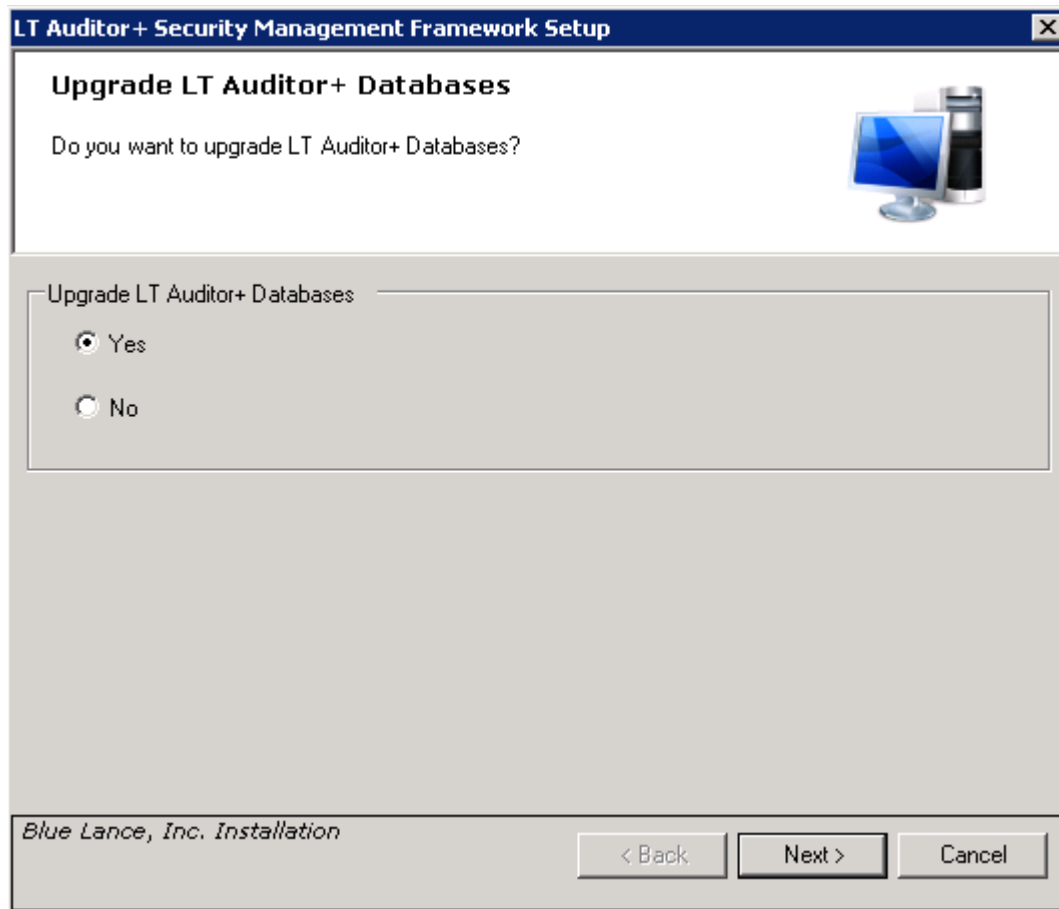


3. Click OK to start the upgrade process and update the LT Auditor+ Manager. The user will be prompted for further input from the following screens.

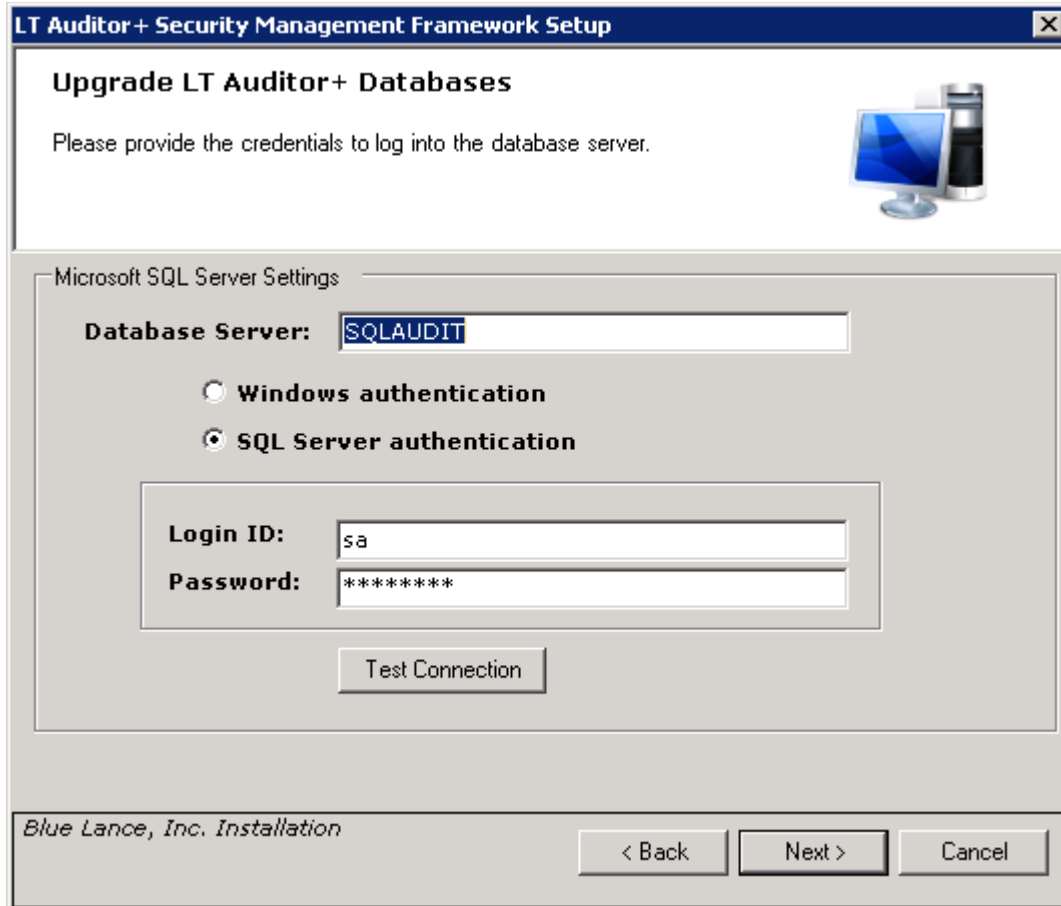


4. Click Next to continue.

5. After the update, the following screen will appear to prompt for the database upgrade. (This screen will only appear for Microsoft SQL databases.)



6. Select Yes and click on Next.



LT Auditor+ Security Management Framework Setup

Upgrade LT Auditor+ Databases

Please provide the credentials to log into the database server.

Microsoft SQL Server Settings

Database Server:

☐ Windows authentication

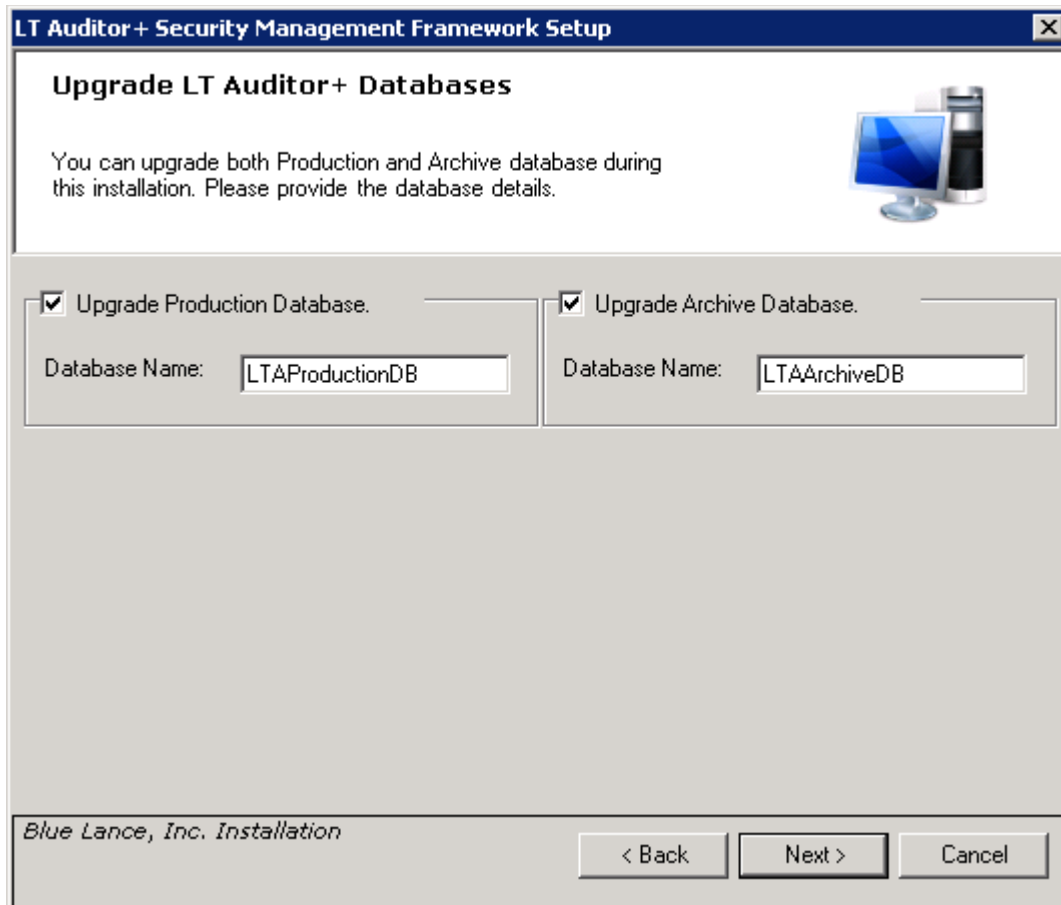
☒ SQL Server authentication

Login ID:

Password:

Blue Lance, Inc. Installation

Please provide the credentials to the database and click Next.



LT Auditor+ Security Management Framework Setup

Upgrade LT Auditor+ Databases

You can upgrade both Production and Archive database during this installation. Please provide the database details.

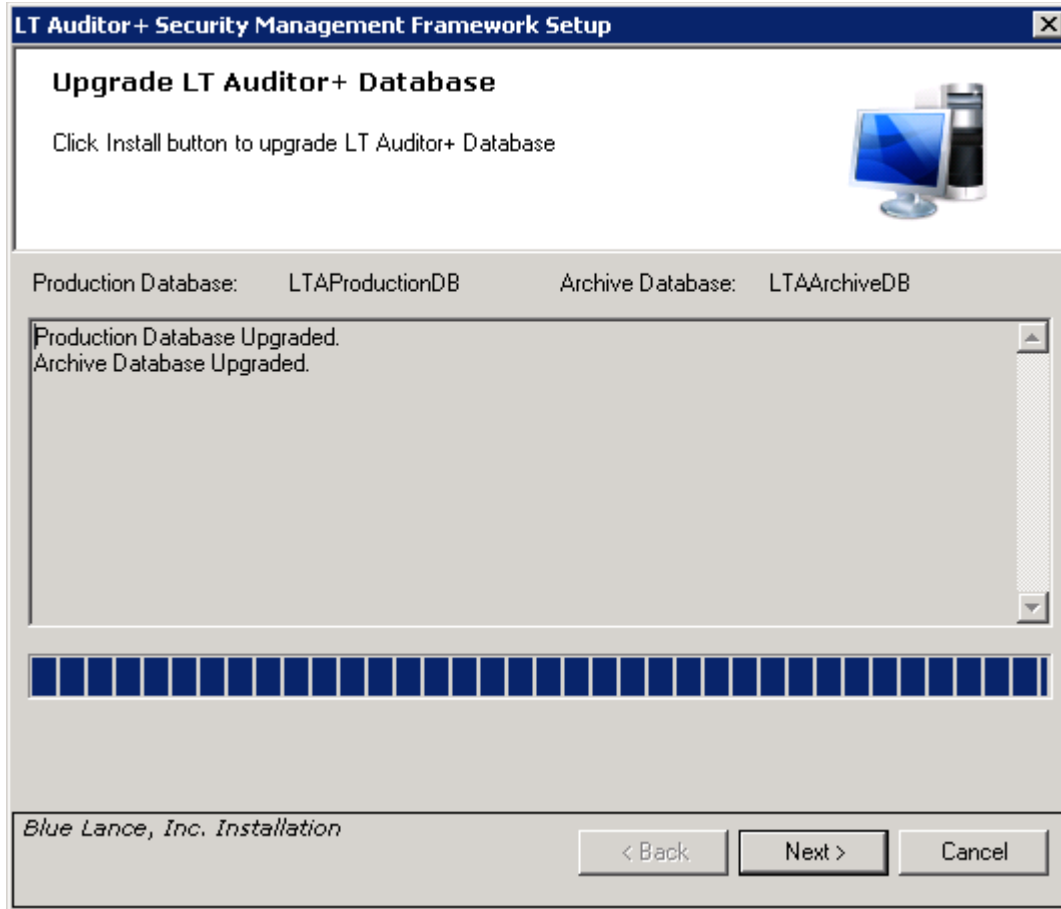
☒ Upgrade Production Database. Database Name:

☒ Upgrade Archive Database. Database Name:

Blue Lance, Inc. Installation

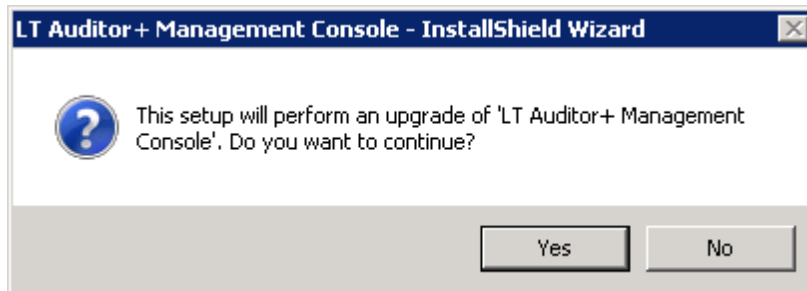
< Back Next > Cancel

7. Ensure that the production and archive database names are correct and click Next to upgrade the databases.

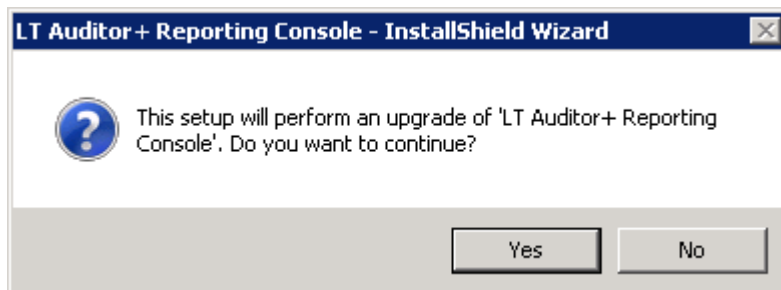


8. Click Next and then Finish to complete the upgrade.

9. If the LT Auditor+ Management Console is installed, a prompt will appear to approve the upgrade as shown below.



10. Click Yes to continue and follow instructions on screen to complete the upgrade.
11. If the LT Auditor+ Reporting Console is installed, a prompt will appear to approve the upgrade as shown below.



12. Click Yes to continue and follow instructions on screen to complete the upgrade.
13. After the installation, the following window will be displayed where the user has the choice to set up a connection with a SIEM system. If a connection is set up, audit data generated by LT Auditor+ will be sent to the SIEM system in real time.

LT Auditor+ SIEM Integration

LT Auditor+ fully leverages and maximizes your SIEM investment
To configure and setup integration with your SIEM system, please follow the steps below

BLUE LANCE

SIEM Systems

- 1. Select SIEM System**
SIEM System :
- 2. Download LT Auditor+ SIEM Integration Package**
Download the LT Auditor+ SIEM package file
[View instructions to install the LT Auditor+ app](#)
- 3. Configure SIEM Settings**
SIEM Server Name / IP Address:
TCP Port :
- 4. Deploy LT Auditor+ SIEM Update**
Please follow your organization's change control processes to deploy this update to all LT Auditor+ Windows agents
[View instructions to update the LT Auditor+ Windows agents](#)
- 5. Activate Smart Connector**
Click on "Activate" to send audit data to SIEM Server

Copyright(c) 1985-2017, Blue Lance, Inc. All Rights Reserved.
All other brand names, product names, or trademarks belong to their respective owners.

14. To connect to a SIEM system, please follow instructions in the table below:

Selection	Action	Remarks
Select SIEM	Select Splunk or any other SIEM system	LT Auditor+ can send data to any SIEM system. By selecting Splunk, Blue Lance provides enhanced dashboards for analytics and reporting.

SIEM Integration package	Download the LT Auditor+ package or app for the SIEM	This is currently only available for Splunk. Users can download the LT Auditor+ App for Splunk and follow instructions in the link
--------------------------	--	--

		to install the app. Details are also provided in APPENDIX C
Configure SIEM settings	Provide the SIEM Server Name or IP address and port to send audit data.	Currently the LT Auditor+ App for Splunk only accepts TCP packets. Please contact Blue Lance if another form of communication is required.
Deploy LT Auditor+ update to Agent machines	Remotely update LT Auditor+ Agents using the LT Auditor+ Management Console.	LT Auditor+ audit data is sent to the SIEM system in real time. To ensure that this happens, all agent machines need to be updated with HF 13.3.0.8. Instructions are provided in section. Upgrading LT Auditor+ Windows Agents.
SIEM smart connectors	Activate	Activating the smart connectors will configure the LT Auditor+ filters and settings to automatically send audit data to the SIEM.

15. After completion the following screen will be displayed:

LT Auditor+ SIEM Integration

LT Auditor+ fully leverages and maximizes your SIEM investment
To configure and setup integration with your SIEM system, please follow the steps below

BLUE LANCE

SIEM Systems

- 1. Select SIEM System**
SIEM System : **Splunk**
- 2. Download LT Auditor+ SIEM Integration Package**
Download the LT Auditor+ SIEM package file **Download**
View [instructions](#) to install the LT Auditor+ app
- 3. Configure SIEM Settings**
SIEM Server Name / IP Address: **WINSIEMSVR** **Test**
TCP Port : **1468**
- 4. Deploy LT Auditor+ SIEM Update**
Please follow your organization's change control processes to deploy this update to all LT Auditor+ Windows agents
View [instructions](#) to update the LT Auditor+ Windows agents
- 5. Activate Smart Connector**
Click on "Activate" to send audit data to SIEM Server
Activate
Smart Connector activated successfully

Copyright(c) 1985-2017, Blue Lance, Inc. All Rights Reserved.
All other brand names, product names, or trademarks belong to their respective owners.

OK

Upgrading the LT Auditor+ Database

Microsoft SQL Servers

The Microsoft SQL database is upgraded during upgrade of the LT Auditor+ Manager discussed above. If you choose to upgrade the database manually, you can run the following scripts under the Database Scripts folder for the production and archive databases respectively.

- **Database Scripts\Microsoft SQL\Production Database Script\ Update Script - ObjectCreation 2013.sql**
- **Database Scripts\Microsoft SQL\Archive Database Script\ Update Script - ArchiveObjectCreation 2013.sql**

Oracle

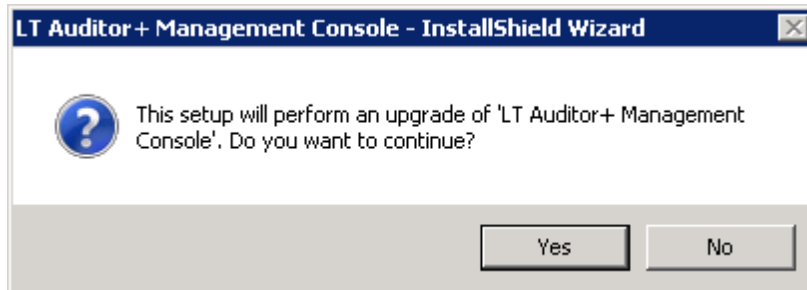
Updates on the LT Auditor+ Oracle database have to be performed manually. The following scripts under the Database Scripts folder should be used for the production and archive databases respectively.

- **Database Scripts\Oracle\Production Database Script\ Update Script - ObjectCreation 2013.sql**
- **Database Scripts\Oracle\Archive Database Script\ Update Script - ArchiveObjectCreation 2013.sql**

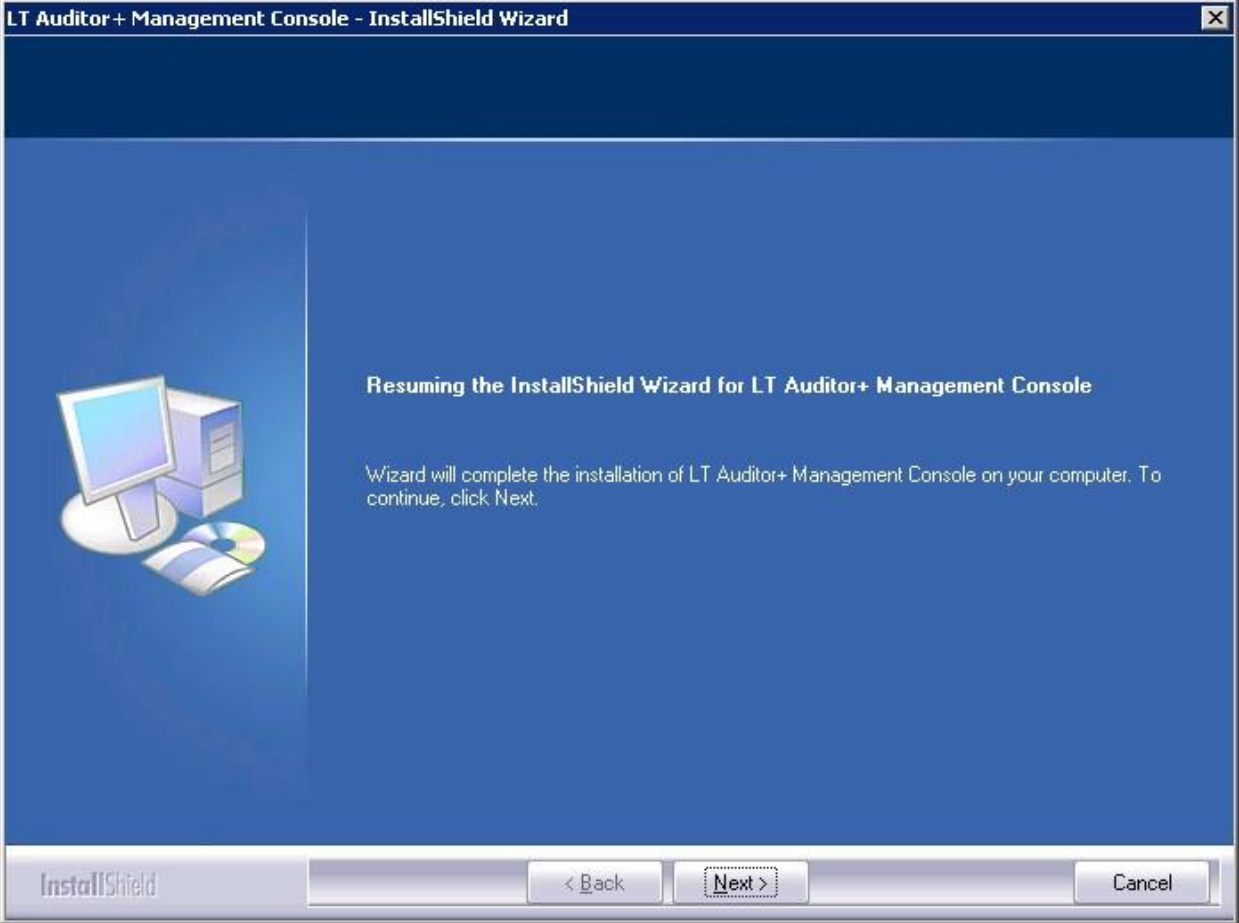
Directly Upgrading the LT Auditor+ Management Console

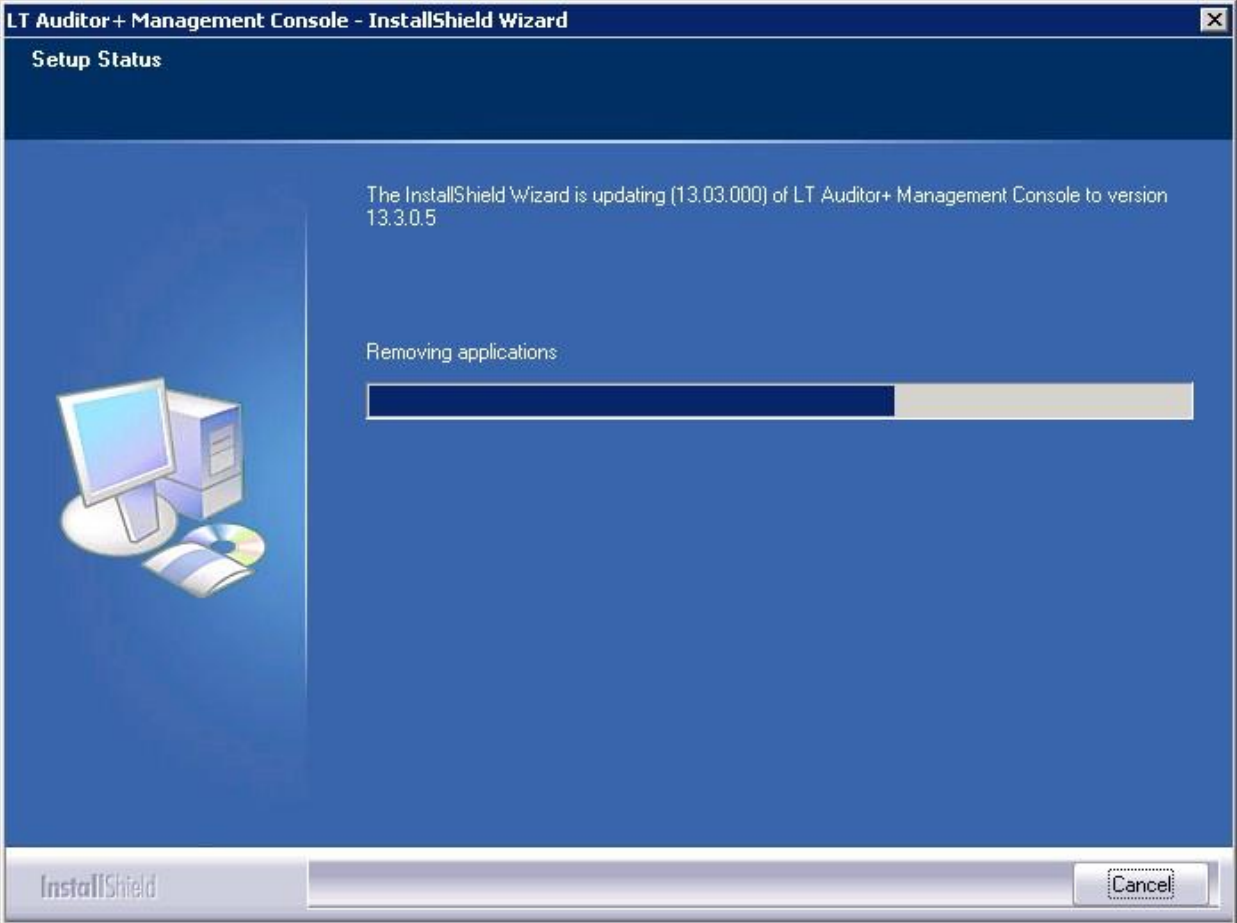
Follow listed steps to upgrade LT Auditor+ Management Console without using the LTUpgrade.exe tool.

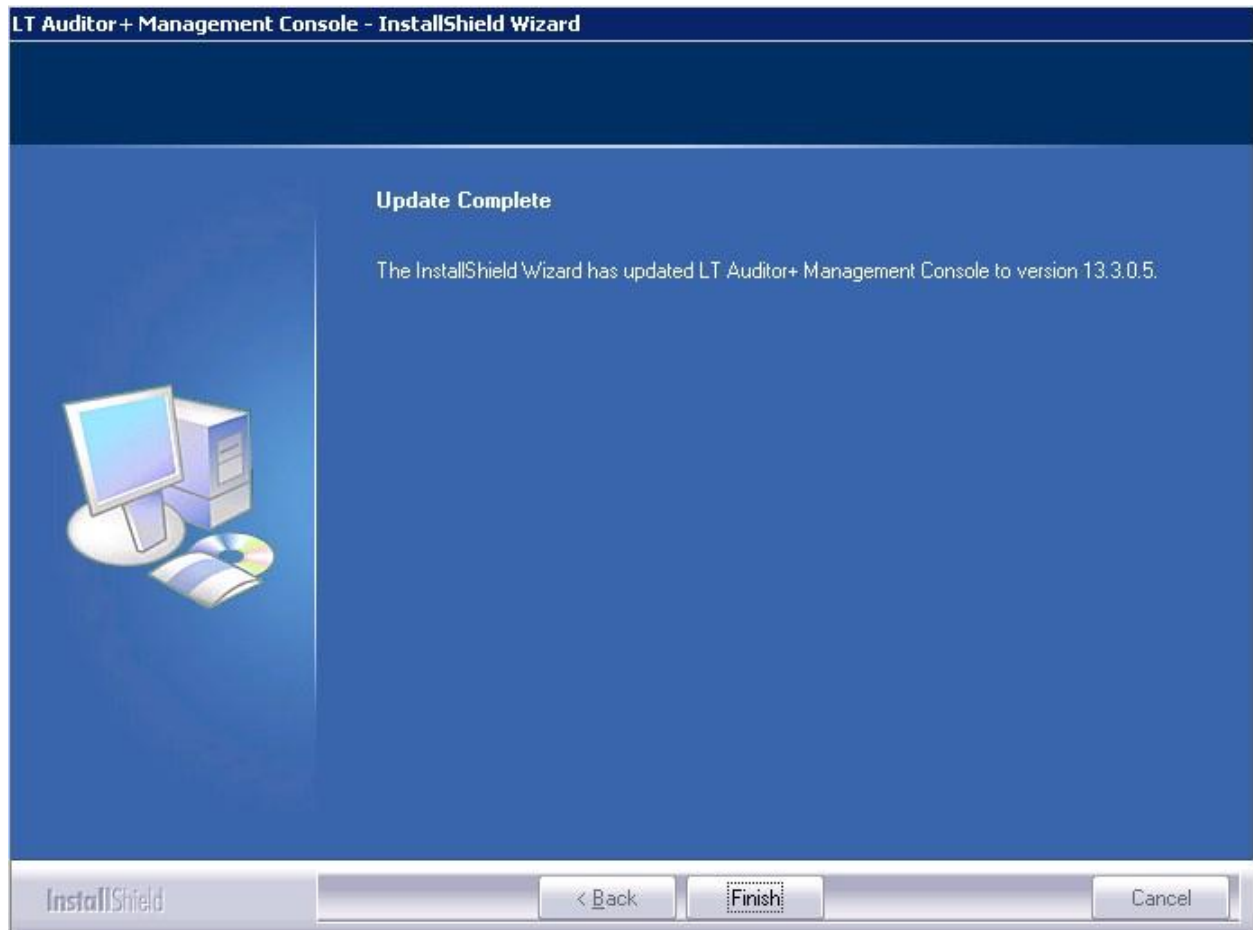
1. Right-click on Setup_MC_x64.exe and run as Administrator.



2. Click Yes to continue.





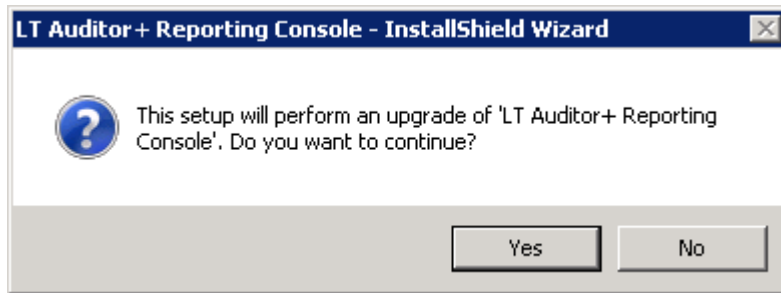


3. Click Finish to complete upgrade.

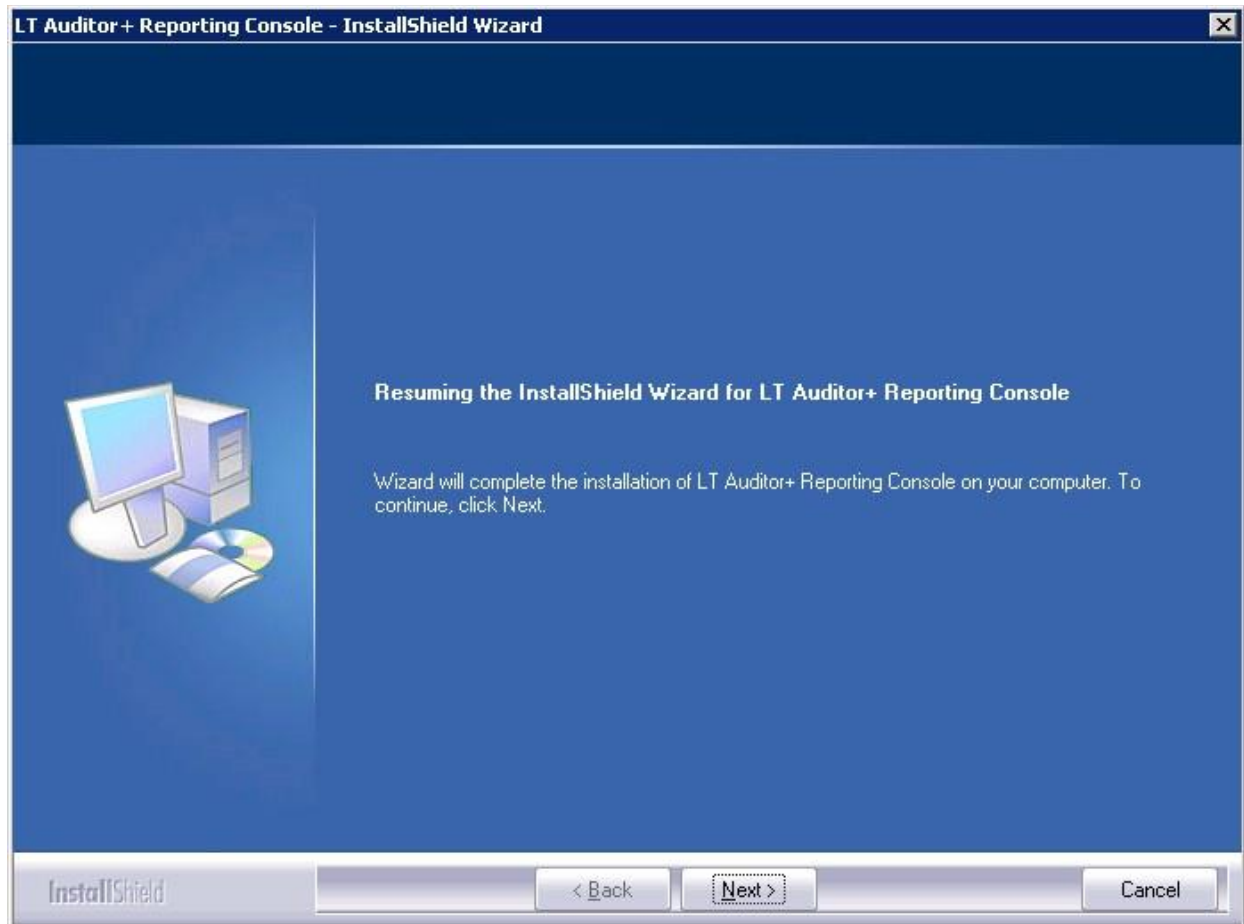
Directly Upgrading the LT Auditor+ Reporting Console

Follow listed steps to upgrade LT Auditor+ Reporting Console without using the LTUpgrade.exe tool.

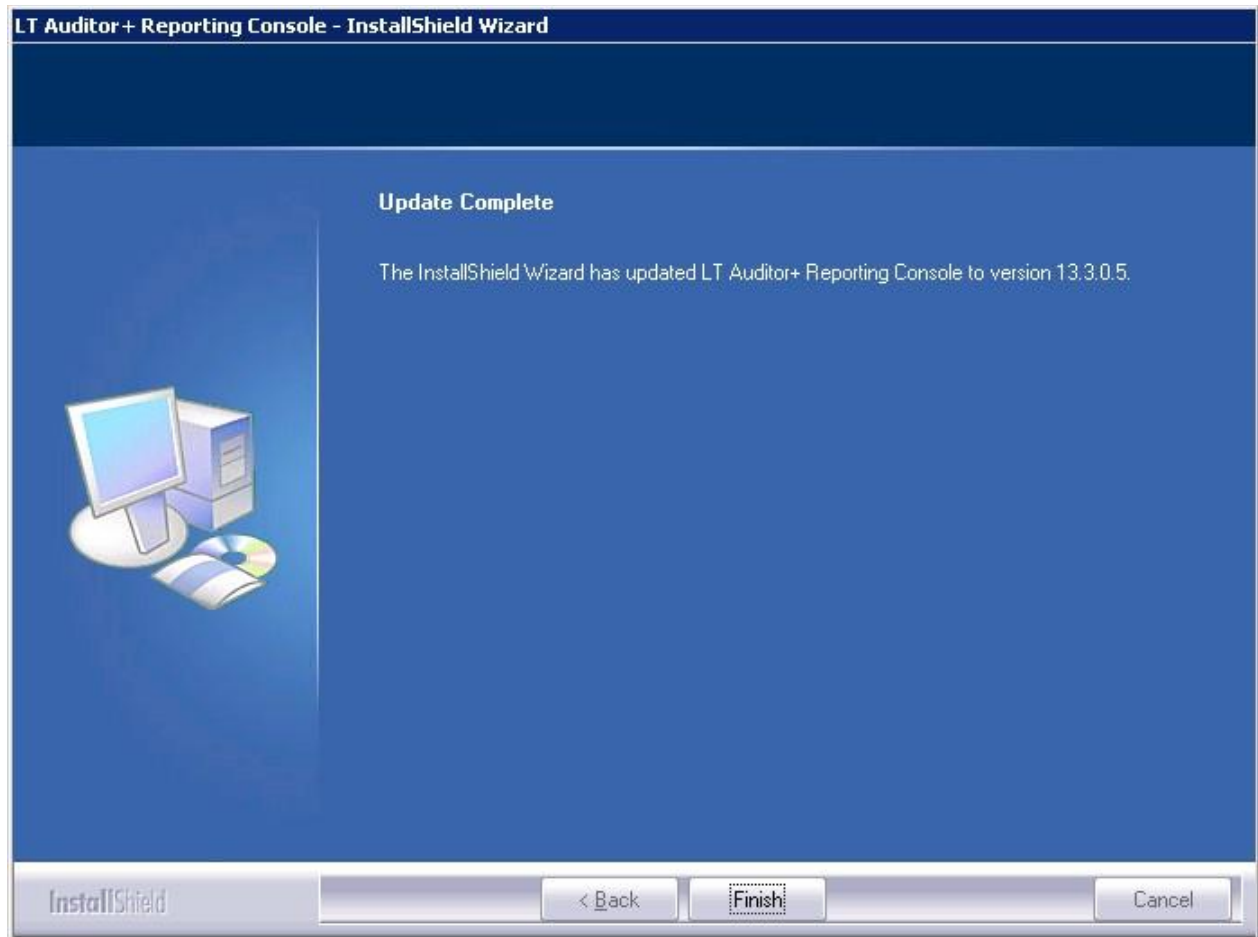
1. Right-click on Setup_RC_x64.exe and run as Administrator.



1. Click Yes to continue.



2. Click Next to continue.

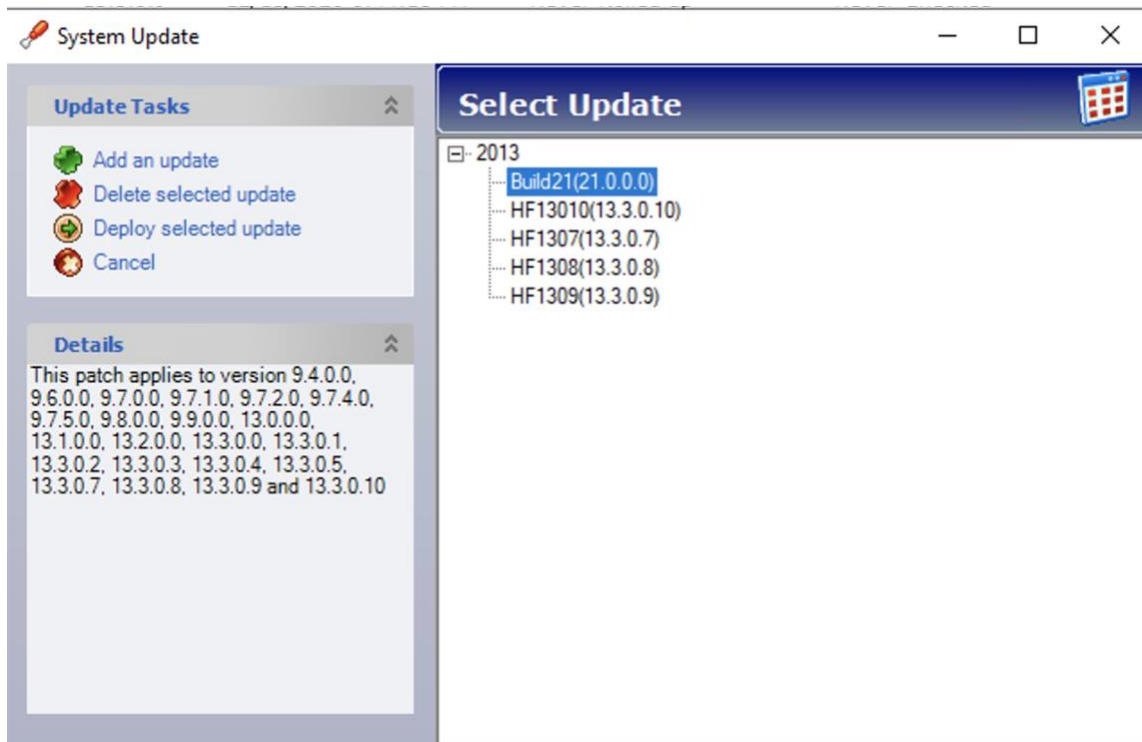


3. Click Finish to complete the upgrade.

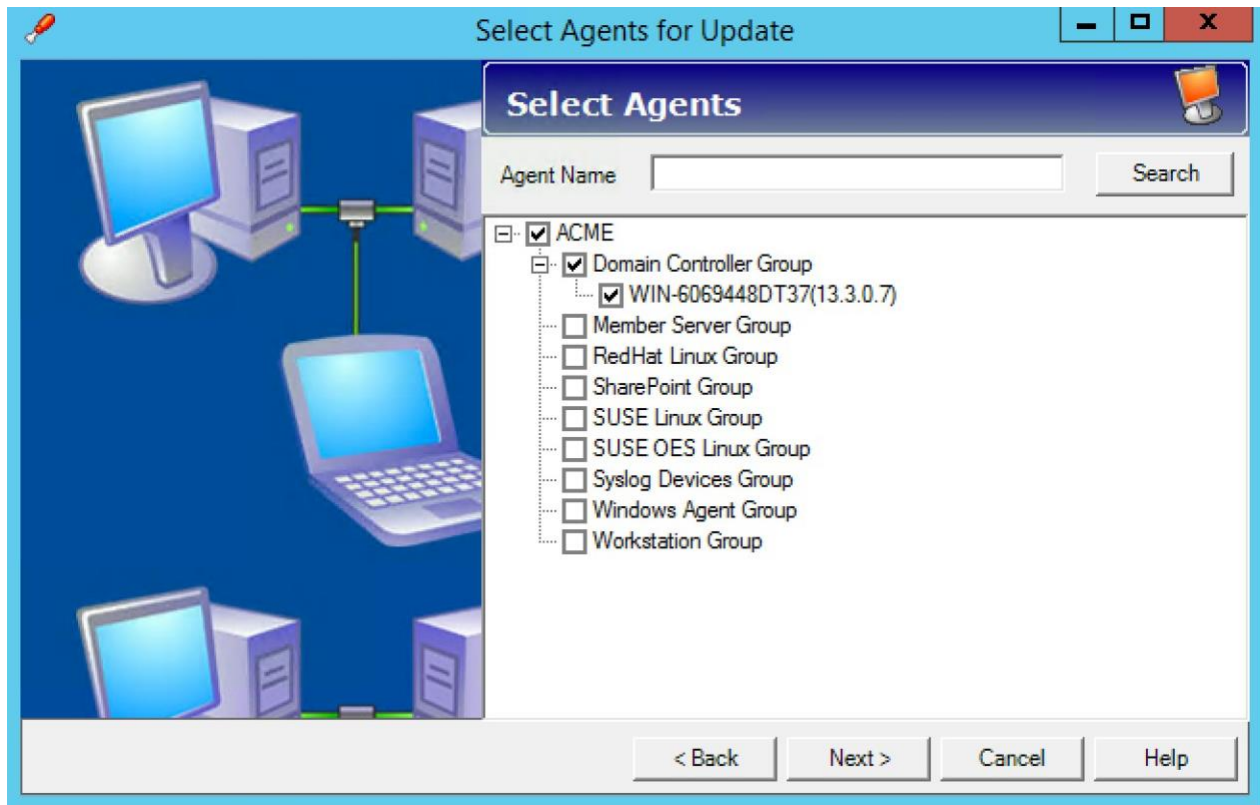
Upgrading LT Auditor+ Windows Agents

Follow the steps outlined below to update all Windows agents to Build21.

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



2. Select the Build21 (21.0.0.0) 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.

Agent Analysis

Agent Machines Available for Deployment

Agent	IP	Version	Description
WIN-6069448D...	10.1.2.173	13.3.0.7	Ready to be updated

Agent Machines Not Available for Deployment

Agent	IP	Version	Reason

View Error

< Back

Next >

Cancel

Help

- 4. Click Next to start the upgrade process. Each agent will be upgraded. This window can be closed during the upgrade process.
- 5. Click Close to complete the upgrade process.

APPENDIX A – What is New in Build21

LT Auditor+ Best Practices Panels

Introducing a set of powerful dashboard panels that highlight network activity captured with LT Auditor+, encapsulated into intelligent, easy to use portals that assist organizations with improving cybersecurity practices and hygiene.

Auditing of EMC Isilon Network Attached Storage (NAS) Devices

Introducing new capabilities to audit and monitor Isilon NAS devices. LT Auditor+ can effectively handle monitoring of detailed file activity on petabytes of storage.

Auditing GPO Policy Preferences

This release can now comprehensively audit changes to GPO Policy Preferences. Group Policy Preferences are a collection of Group Policy client-side extensions of administrative configuration choices deployed to desktops and servers in an Active Directory domain.

Enhanced Access Control to LT Auditor+ Consoles

Build21 release makes it quicker and easier to grant permissions to access LT Auditor+ by allowing Active Directory groups to be added as authorized entities. Members inherit permissions configured for the group, making it a breeze to manage multiple users with common access needs and privileges. Nested grouping is also supported.

Enhanced Active Directory Auditing Capability

Complete support of Microsoft Server 2019 and capability to audit configurations such as User Passwords set to Never Expire and Unconstrained Delegations granted to computers on the network.

Enhanced Email Support

Build21 fully supports sending LT Auditor+ email messages in real time or via scheduled report to Office 365.

Splunk Integration

Build21 has built integration into Splunk. The LT Auditor+ App for Splunk can ingest data from LT Auditor+ and provides dashboards and portals to fully leverage audit data generated with LT Auditor+.

APPENDIX B – Enhanced Active Directory Notifications

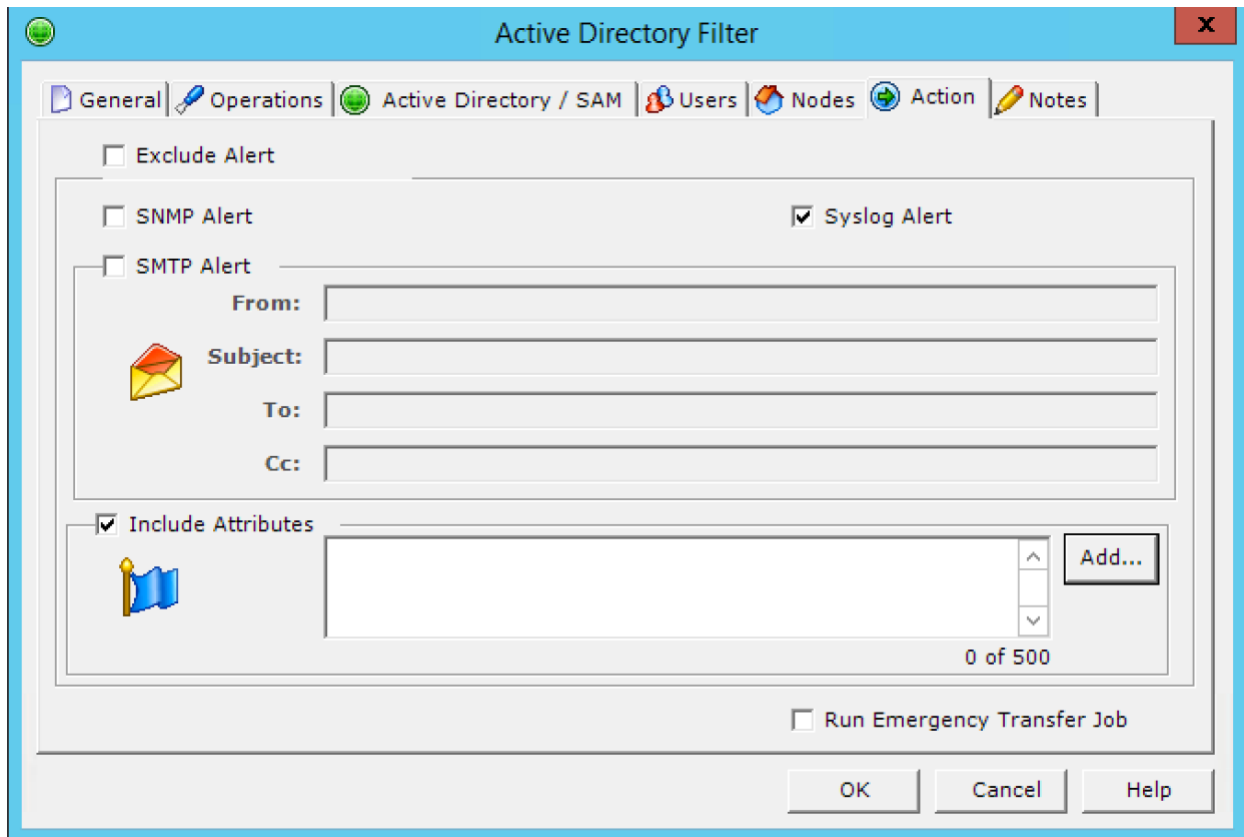
Notification with Additional Attributes

Build21 provides the capability to alert on additional Active Directory attributes for specified events. This is useful as it gives users more information about an alerted event.

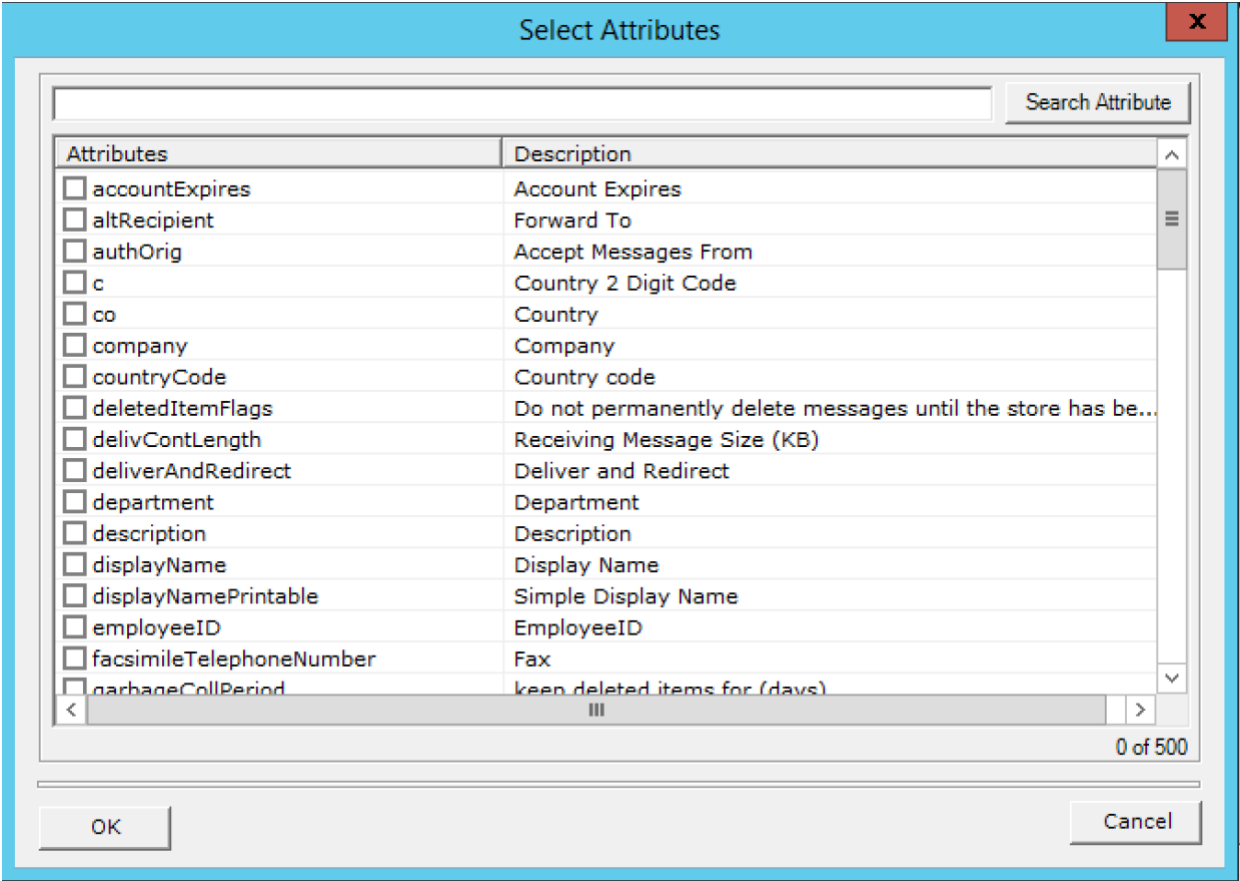
For example, if a security administrator is alerted when a user is made a member of a group or is disabled, additional details like the user's full name or employee ID or the user's manager, etc. can be included in the alert message.

These additional attributes can be selected in the Alert tab for the Active filter.

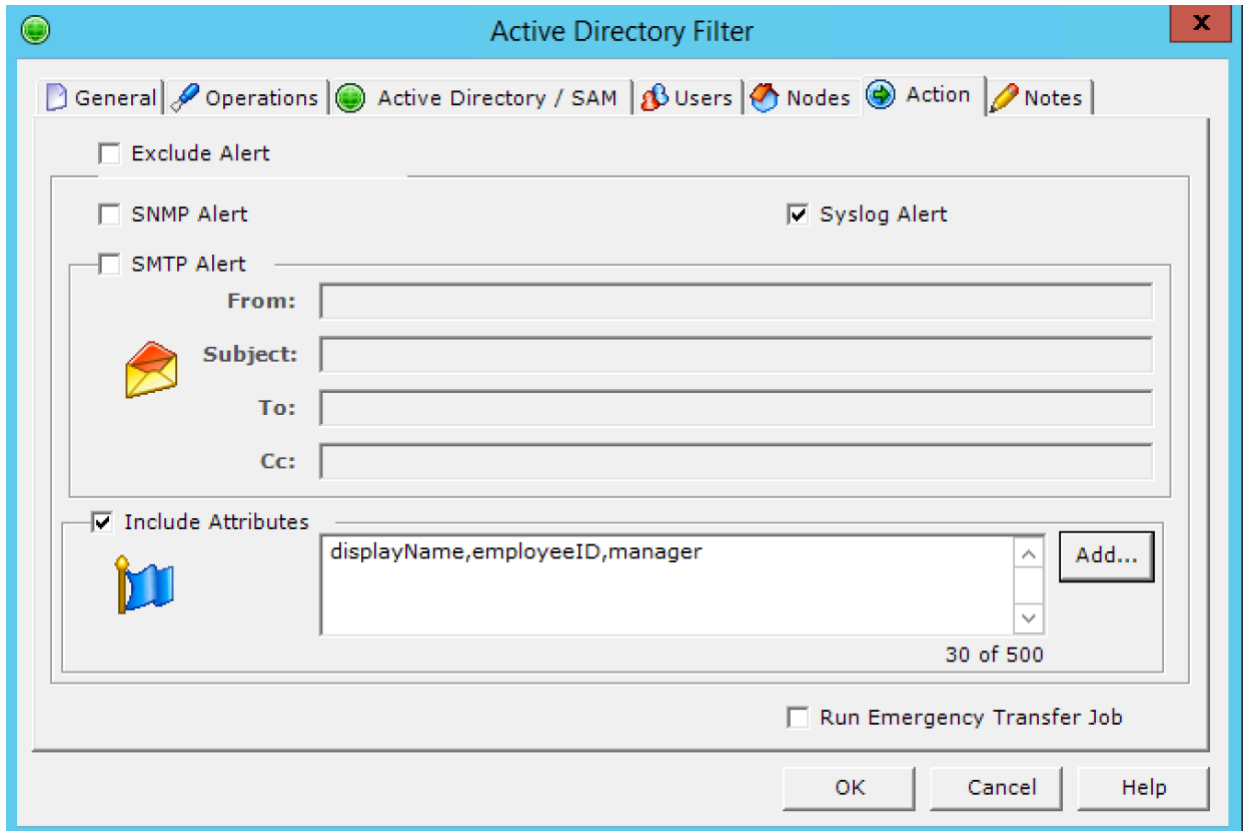
This tab now includes a section called Include Attributes as shown below:



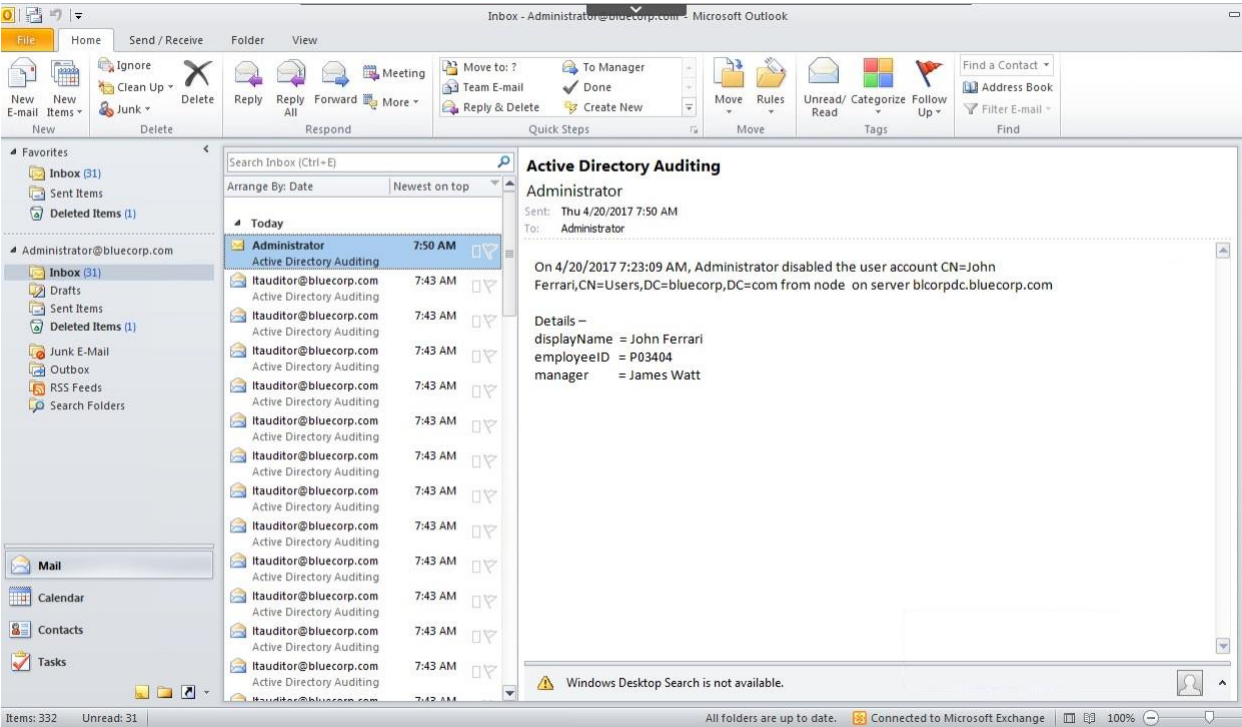
To add attributes, check the Include Attributes check box and click on the Add button to bring up a list of attributes as shown below:



Select the desired attributes and click OK.



If a filter was configured to generate an SMTP alert when a user is disabled, with the additional attributes of displayName, employeeID and manager, then the person receiving the SMTP alert will get a message as shown below:



APPENDIX C – Installing LT Auditor+ App for Splunk

The first step to installing the LT Auditor+ App for Splunk is to download the app from

http://bldownloads.blob.core.windows.net/release/LT_Auditor_App_For_Splunk.zip.

Extraction of this zip file will reveal the following folders and files:

Folder Name	Files	Comments
Single Instance	LT_Auditor.spl	LT Auditor+ App
	TA-LT_Auditor.spl	LT Auditor+ Splunk Add-on
Distributed Environment	LT_Auditor.tar.tz	LT Auditor+ App
	TA-LT_Auditor.tar.tz	LT Auditor+ Splunk Add-on

Splunk has the following types of deployments:

1. Single Instance
2. Distributed Environment

Details to install the LT Auditor+ App for Splunk for each type of configuration are listed below.

Single Instance

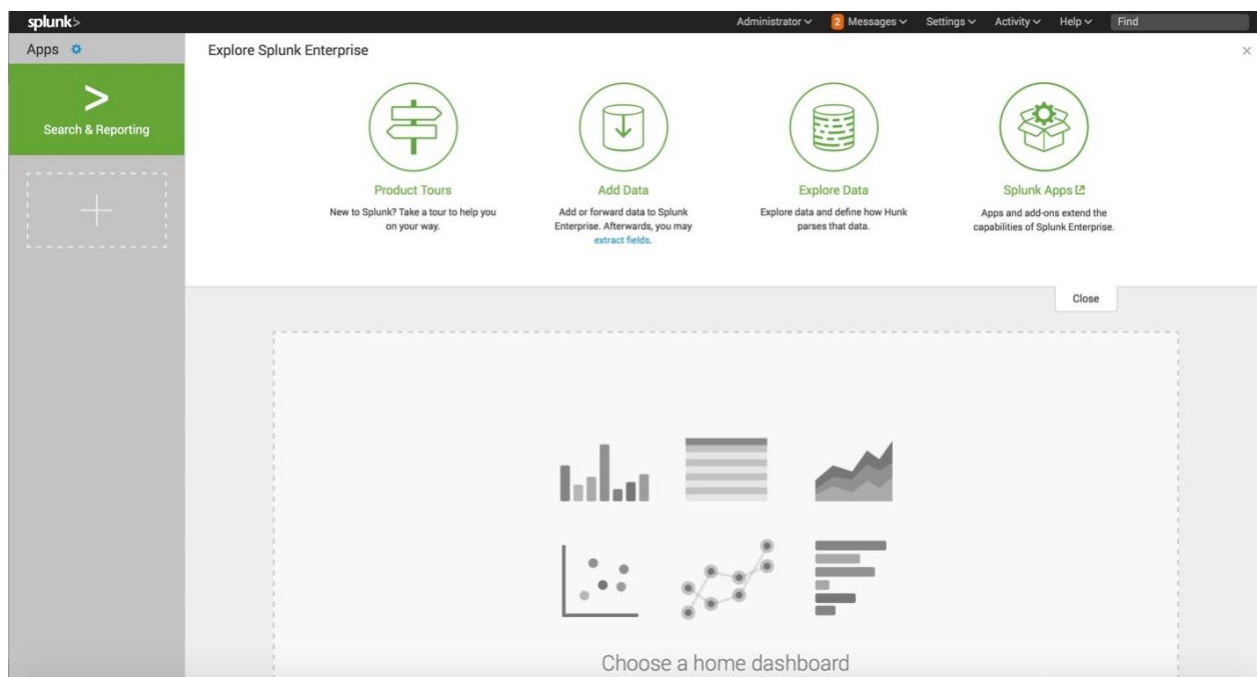
A Single Instance of Splunk is one server providing all Splunk-related functionality, namely license server, indexer and search head. This type of deployment is used in smaller environments.

To install the LT Auditor+ App for Splunk, please follow the steps outlined below:

1. Log in to your Splunk console.



2. Access the Splunk home page.



3. Click on the Apps icon to open Apps screen as shown below:

splunk> Apps

Administrator 2 Messages Settings Activity Help Find

Apps

Browse more apps

Install app from file

Create app

Showing 1-18 of 18 items

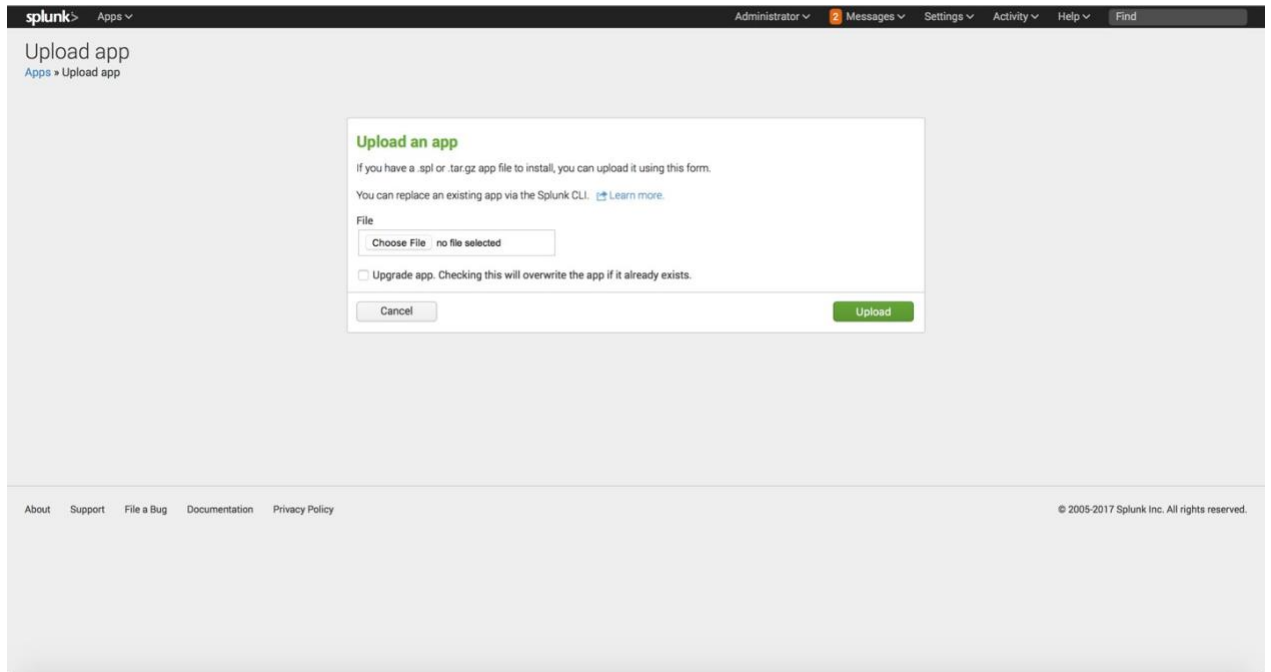
Results per page 25

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Log Event Alert Action	alert_logevent	6.5.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	6.5.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	6.5.0	Yes	No	App Permissions	Enabled	Edit properties View objects
framework	framework		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Getting started	gettingstarted	1.0	Yes	Yes	App Permissions	Disabled Enable	
introspection_generator_addon	introspection_generator_addon	6.5.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
marketplace-confs	marketplace-confs	1.0.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	
Search & Reporting	search	6.5.0	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects View details on SplunkApps
splunk_httpinput	splunk_httpinput		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Instrumentation	splunk_instrumentation	1.0	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Monitoring Console	splunk_monitoring_console	6.5.0	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects

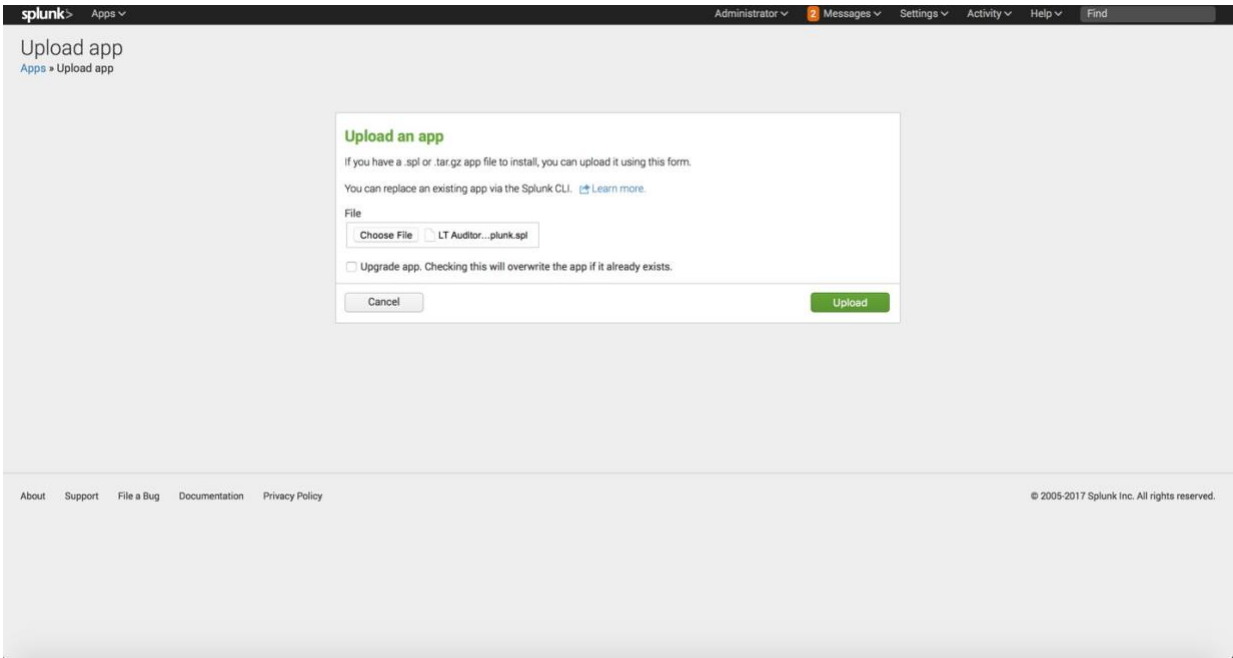
AboutSupportFile a BugDocumentationPrivacy Policy

© 2005-2017 Splunk Inc. All rights reserved.

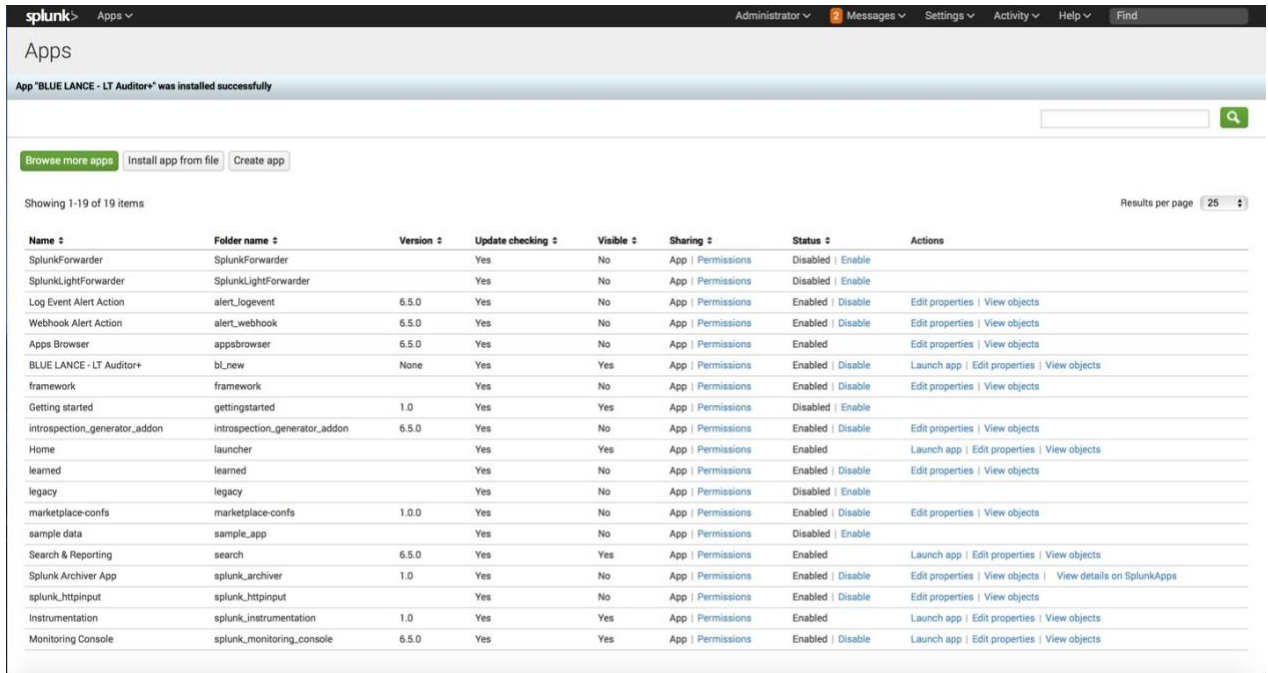
- Click “Install app from file” to open the screen “Upload an app”:



- Browse to the file “Single Instance\LT_Auditor.spl” and select Upload.



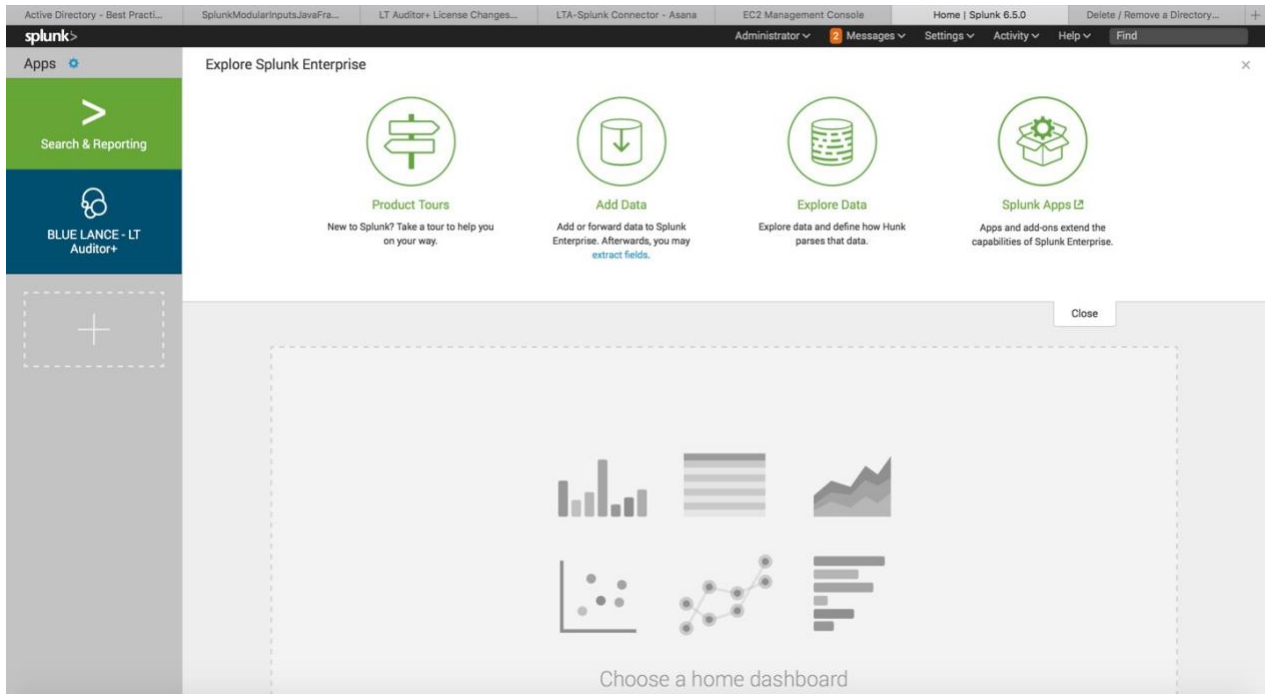
6. Repeat steps four to six to install the add-on “Single Instance\TA- LT_Auditor.spl”
7. You will now see the LT Auditor+ App for Splunk and LT Auditor+ Add-on for Splunk installed as shown below:



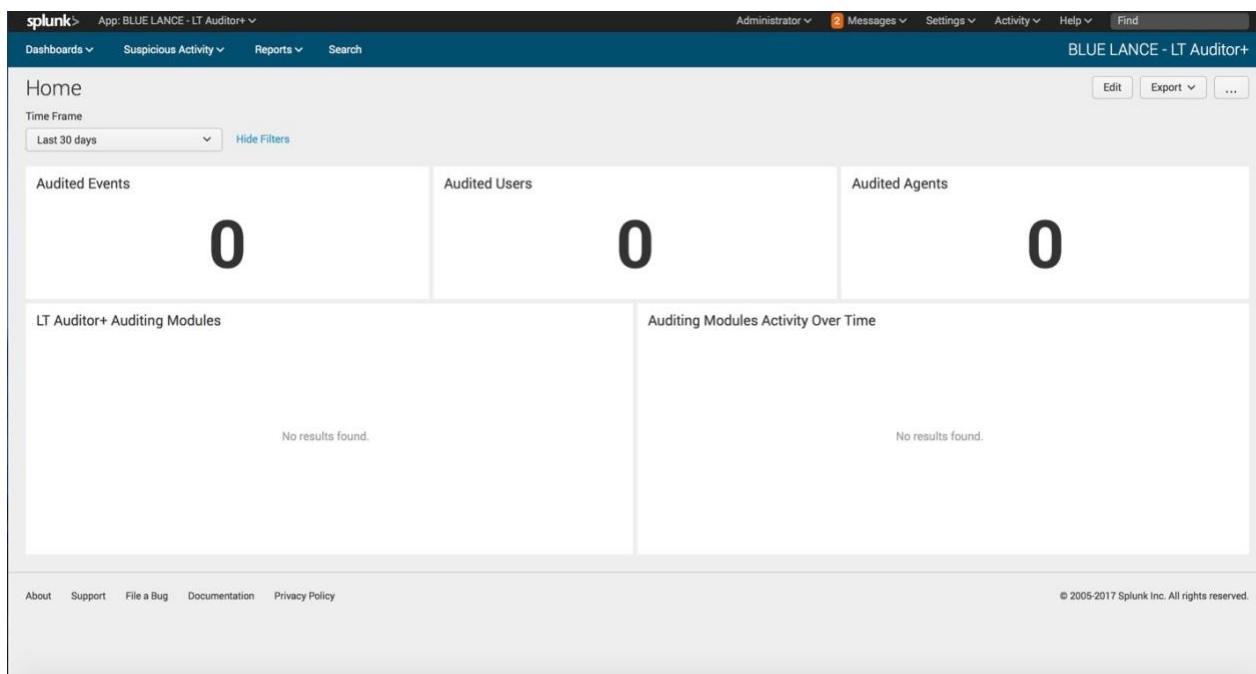
The screenshot shows the Splunk Apps page. At the top, a message states: "App 'BLUE LANCE - LT Auditor+' was installed successfully". Below this, there are buttons for "Browse more apps", "Install app from file", and "Create app". A search bar is also present. The main content area displays a table of installed apps, showing 1-19 of 19 items. The table has columns for Name, Folder name, Version, Update checking, Visible, Sharing, Status, and Actions. The "BLUE LANCE - LT Auditor+" app is listed with a version of "None" and is currently "Enabled".

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Log Event Alert Action	alert_logevent	6.5.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	6.5.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	6.5.0	Yes	No	App Permissions	Enabled	Edit properties View objects
BLUE LANCE - LT Auditor+	bl_new	None	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects
framework	framework		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Getting started	gettingstarted	1.0	Yes	Yes	App Permissions	Disabled Enable	
introspection_generator_addon	introspection_generator_addon	6.5.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
marketplace-confs	marketplace-confs	1.0.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	
Search & Reporting	search	6.5.0	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects View details on SplunkApps
splunk_httpinput	splunk_httpinput		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Instrumentation	splunk_instrumentation	1.0	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Monitoring Console	splunk_monitoring_console	6.5.0	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects

8. Click the Splunk icon to switch to the homepage, and you will now see the new app — LT Auditor+ App for Splunk.



9. Click on LT Auditor+ App for Splunk to get to the LT Auditor+ home screen as shown below:



Congratulations! You have successfully installed the LT Auditor+ App for Splunk.

Distributed Environment

A distributed deployment of Splunk consists of several instances working together to provide indexing and search head duties. Both the search heads and indexers could be clustered as well.

Deploy LT Auditor+ App for Splunk Add-on to Peer Nodes

1. Connect to the master node.
2. Extract the contents of the file “Distributed Environment\TA-LT_Auditor.tar.gz” to the folder “/opt/splunk/etc/master-apps”
3. Run the command “/opt/splunk/bin/splunk” to apply cluster-bundle to deploy to all peer nodes.

The LT Auditor+ Add-on uses a custom index called lt_auditor_idx. Please take steps to ensure that this index is replicated across all peer servers.

Deploy LT Auditor+ App to Search Heads

1. Connect to search head machine.
2. For nonclustered search heads, extract the contents of the file “Distributed Environment\LT_Auditor.tar.gz” to the folder “/opt/splunk/etc/apps”
3. For clustered search heads:
 - a. Extract the contents of the file “Distributed Environment\LT_Auditor.tar.gz” to the folder “/opt/splunk/etc/shcluster/apps”
 - b. Run the command “/opt/splunk/bin/splunk” to apply shcluster- bundle -target https://<master-node>:8089 -

force true

Deploy LT Auditor+ Add-on to Heavy Forwarder:

1. Connect to Heavy Forwarder machine.
2. Extract the contents of the file “Distributed Environment\TA-LT_Auditor.tar.gz” to the folder “/opt/splunk/etc/apps.”
3. If there are multiple forwarders, use a deployer to distribute the Add-on “TA-LT_Auditor.tar.gz” to all forwarders.