BLUE LANCE

LT Auditor+ 2013

Windows Assessment SP1 Installation & Configuration Guide

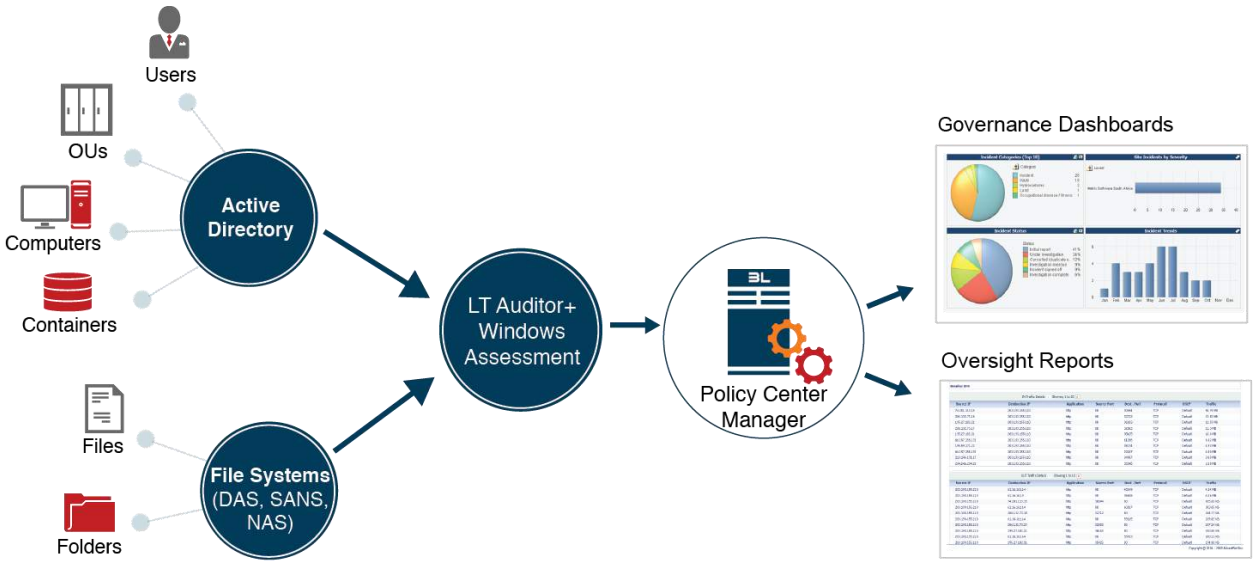
Table of Contents

Chapter 1- Overview

The LT Auditor+ 2013 Windows Assessment (LTWA) application can be used to collect and record information on configuration settings, vulnerabilities and permissions on the following entities:

- Active Directory Users, Groups, and other objects;
- Windows (NTFS) File Systems such as DAS (Direct Attached Storage), SAN (Storage Area Networks) and NAS (Network Attached Storage) systems;

LTWA integrates into the LT Auditor+ 2013 framework and therefore can leverage audit data collected with other LT Auditor+ 2013 modules. Insights can now be gained on who has the rights to access critical file shares while documenting who does access these file systems. The architecture diagram below shows how the LTWA integrates into the LT Auditor+ ecosystem.



Chapter 2 - Install LT Auditor+ Windows Assessment SP1 Components

The section provides an overview on how LTWA is installed and configured. Included in this section are systems requirements, pre-requisites. Please review APPENDIX D for details on what is new in LT Auditor+ Windows Assessment SP1.

System Requirements

- Meet the same systems requirement to install an LT Auditor+ Windows agent as described in the LT Auditor+ 2013 Installation Guide.

Pre-requisites for the LT Auditor+ Windows Assessment installation

- Must have LT Auditor+ 2013 (Framework version HF 1302) installed.
- Must have LT Auditor+ 2013 Syslog Processor installed.
- PowerShell 2.0 and above.
- Installer must have administrative privileges to install LT Auditor+ Windows Assessment.

Note: Please review the HF1302 Installation Guide for documentation on installation or upgrade to LT Auditor+ 2013 HF1302.

LT Auditor+ Windows Assessment Components

After you download and extract the LT_Auditor+_Windows_Assessment.zip file, the following files should be available for the installation process:

1. Setup_LT_Assessment_Manager_x64.exe (Manager component)(
2. Setup_LT_Assessment_Agent_x64.exe (Agent component)
3. Setup_LT_Assessment_Manager_x32.exe (Manager component)
4. Setup_LT_Assessment_Agent_x32.exe (Agent component)

Installation Steps

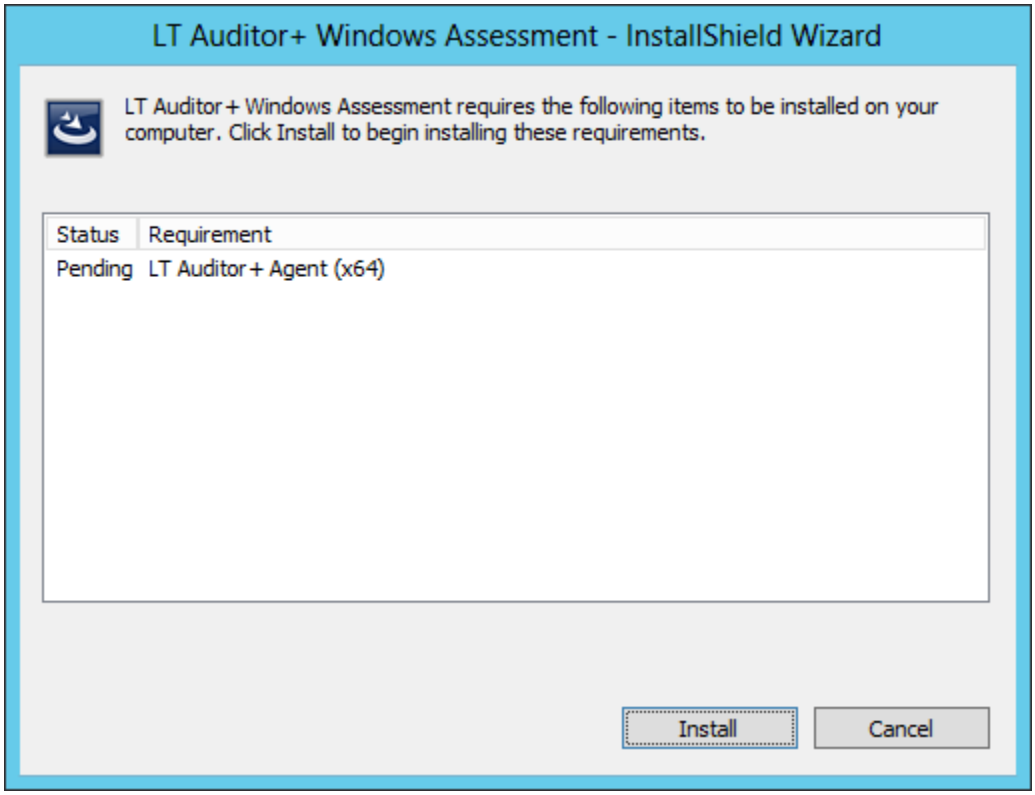
LTWA will require the installation of a Manager component as well as an agent component on target Windows servers to be scanned.

LT Auditor+ Windows Assessment Manager Component (LTWAMC)

The Manager component (LTWAMC) can be installed on any machine as long as the pre-requisite requirements are met. Blue Lance recommends that LTWAMC be installed on the machine that hosts the LT Auditor+ Manager.

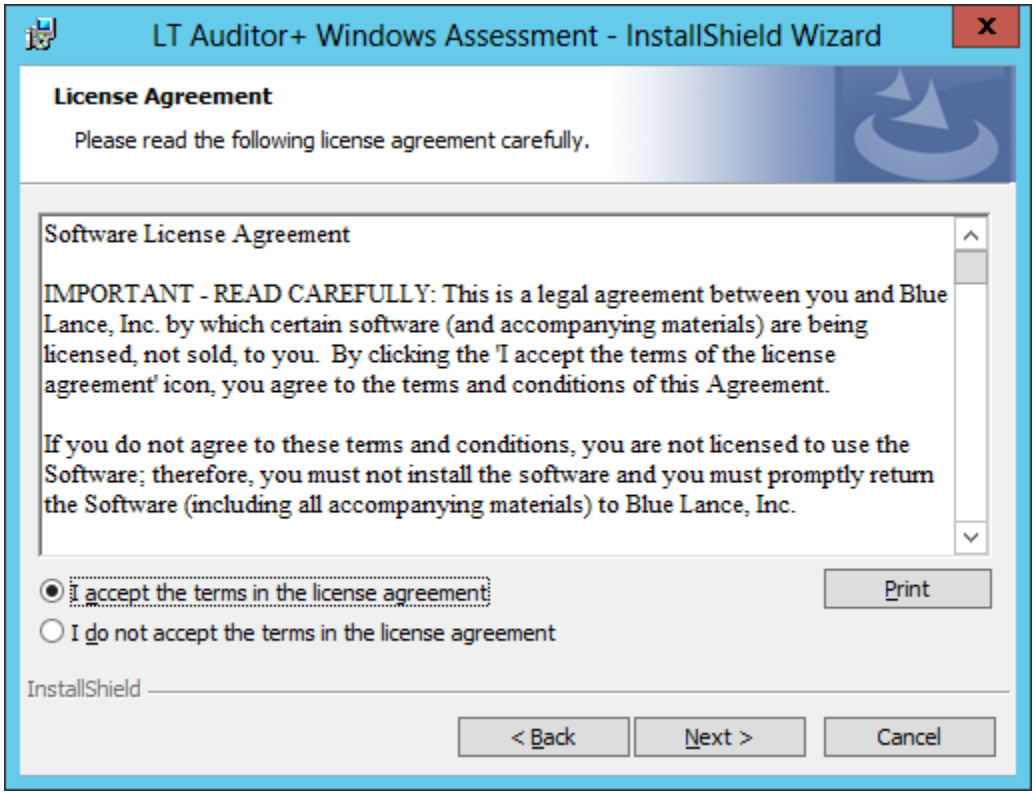
In following section, the term Setup.exe will used to refer to either Setup_LT_Assessment_Manager_x64.exe or Setup_LT_Assessment_Manager_x32.exe based on the operating system selected.

1. Run Setup.exe file from the root of the installation folder to launch the installation of the LTWAMC.

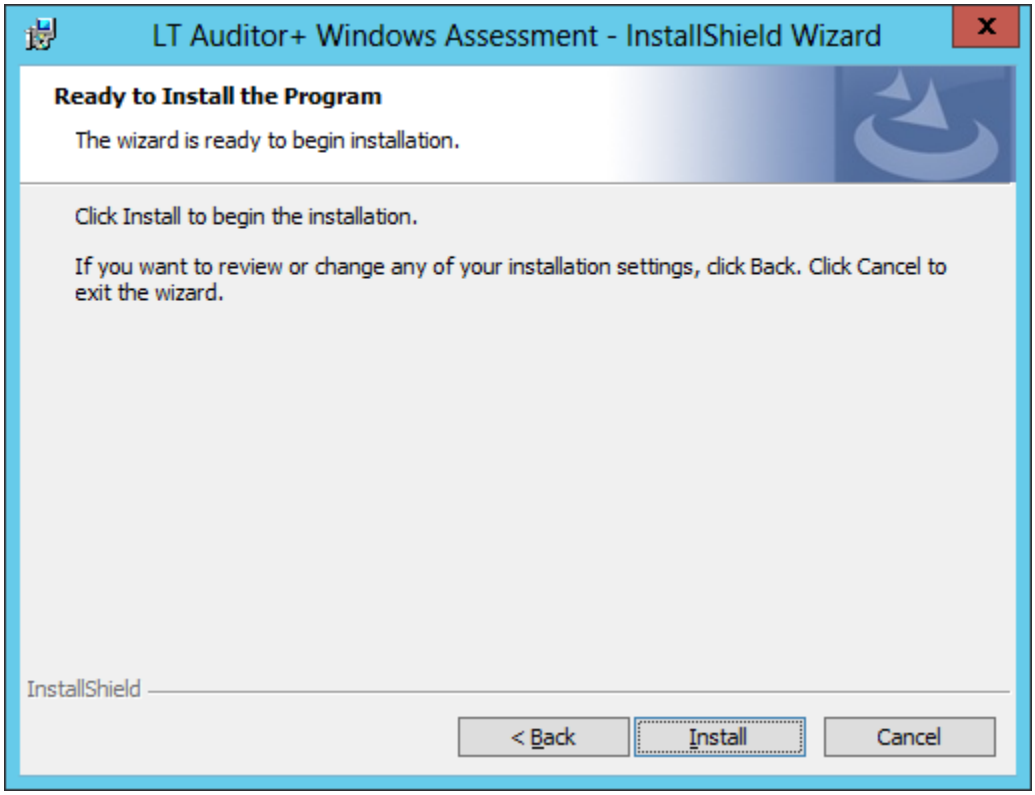


2. Click Install to being up the following screen.

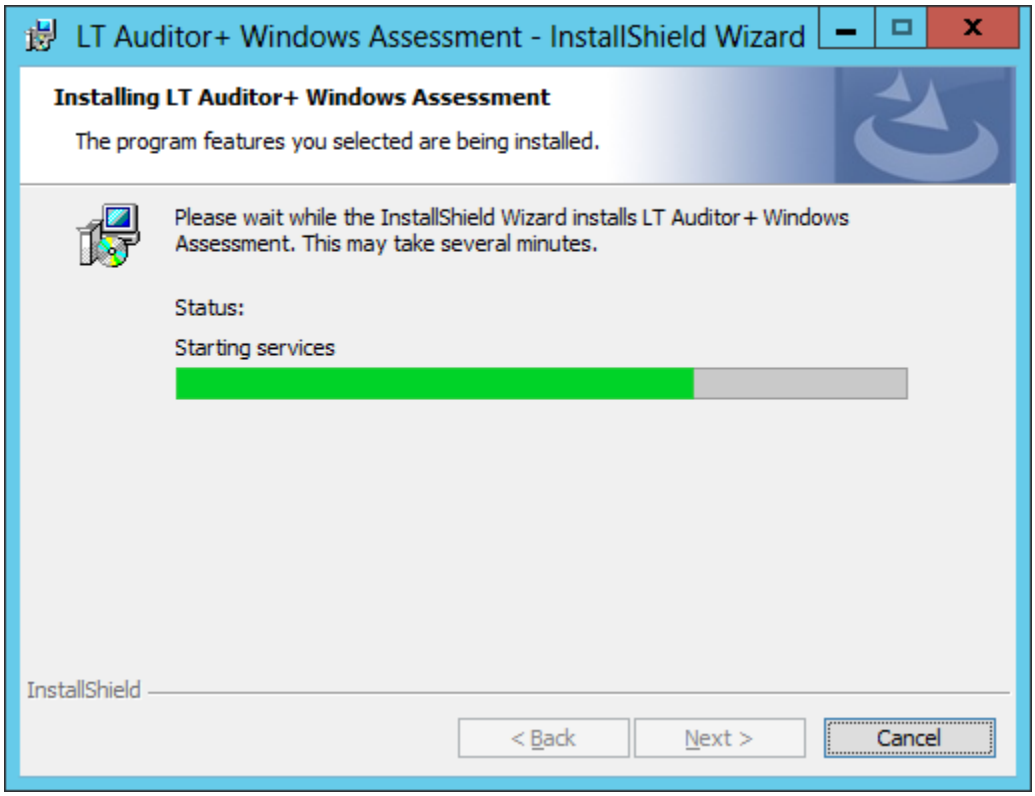
3. Click Next to bring up the License information screen.

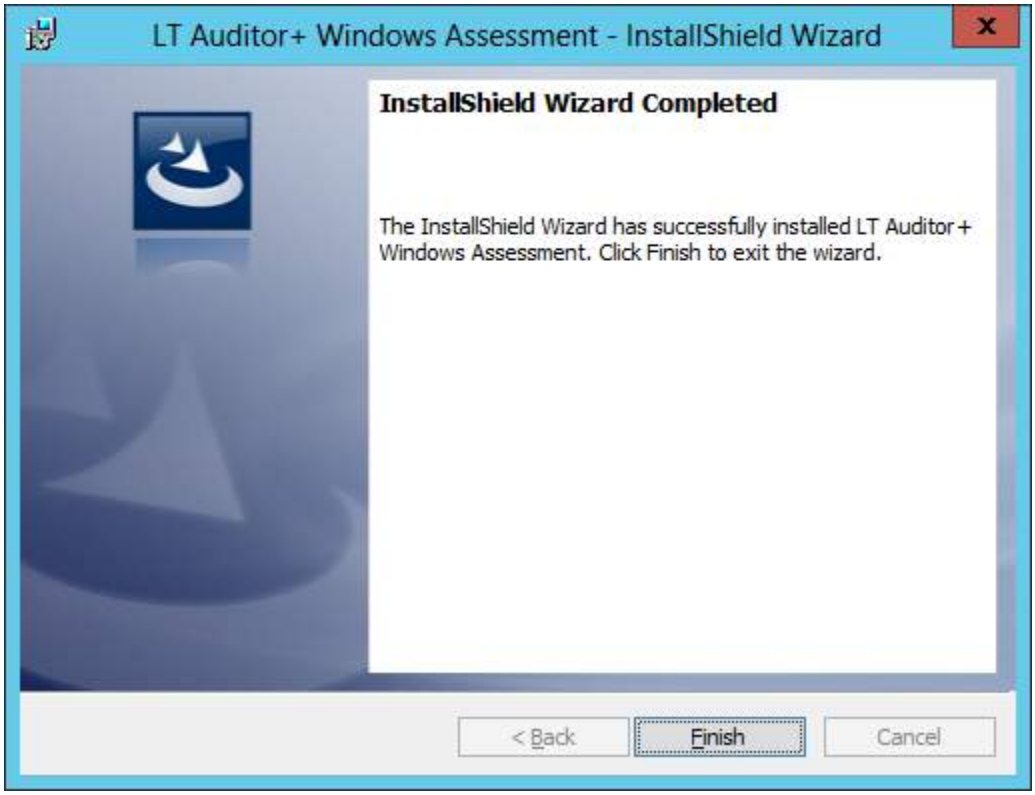


4. Read the Software License Agreement, and if acceptable, click on ‘I accept the license terms in the license agreement’ and click Next.



5. Click Install to start the installation.





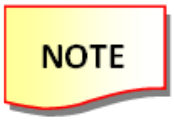
6. Click Finish to complete the installation of the LTWAMC.

NOTE LTAWMC is installed to the LT Auditor+ folder that hosts the LT Auditor+ SMF installation.

LT Auditor+ Windows Assessment Agent Component (LTWAAC)

The Agent component (LTWAAC) has to be installed on Windows machines and following table can be used as a guideline.

Category	Scan Information	Target
Active Directory	To scan for Active Directory Users, Groups or any other AD objects	LTWAAC should be installed on one Domain Controller in the environment
File System	To scan for files and folders	LTWAAC should be installed on any File Server where there is a requirement to scan for information on the local file system.



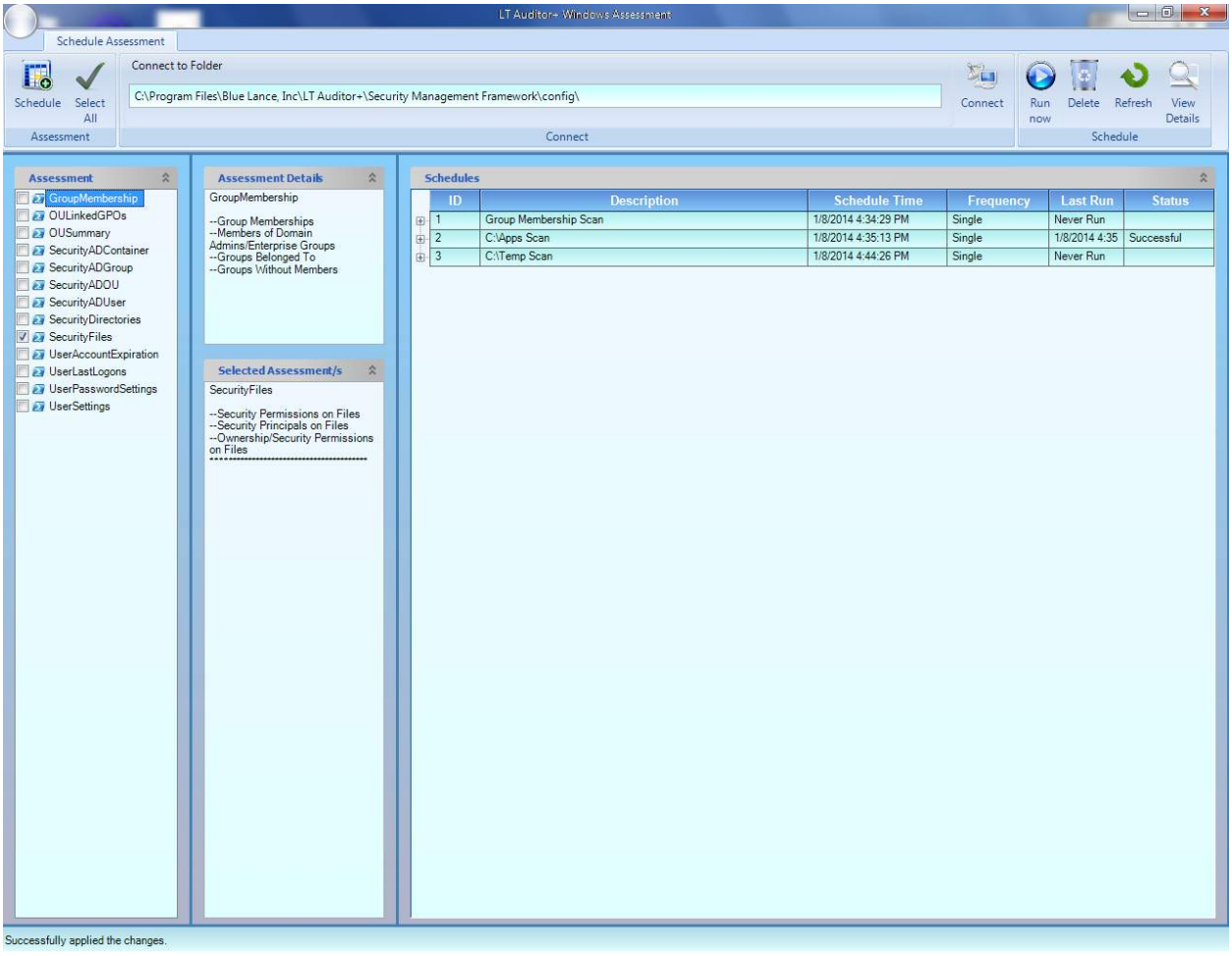
If the LTWAMC (Manager Component) is installed on a Domain Controller then there is no need to install the LTWAAC on any other Domain Controller.

To install LTWAAC copy the Setup_LT_Assessment_Agent_x64.exe or Setup_LT_Assessment_Agent_x32.exe to the target Windows machine and run the executable. The installation steps are identical to the steps described in the section above for the LTWAMC.

Chapter 3 – Setup Scans with LT Auditor+ Windows Assessment (LTWA)

This section provides instructions on how to use the LT Auditor+ Windows Assessment Console (LTWAC) to schedule scans. This application is installed on the machine where the LTWAMC was installed.

To launch the LTWAC click Start → All Programs → Blue Lance, Inc. → Windows Assessment Console to bring up the following window.



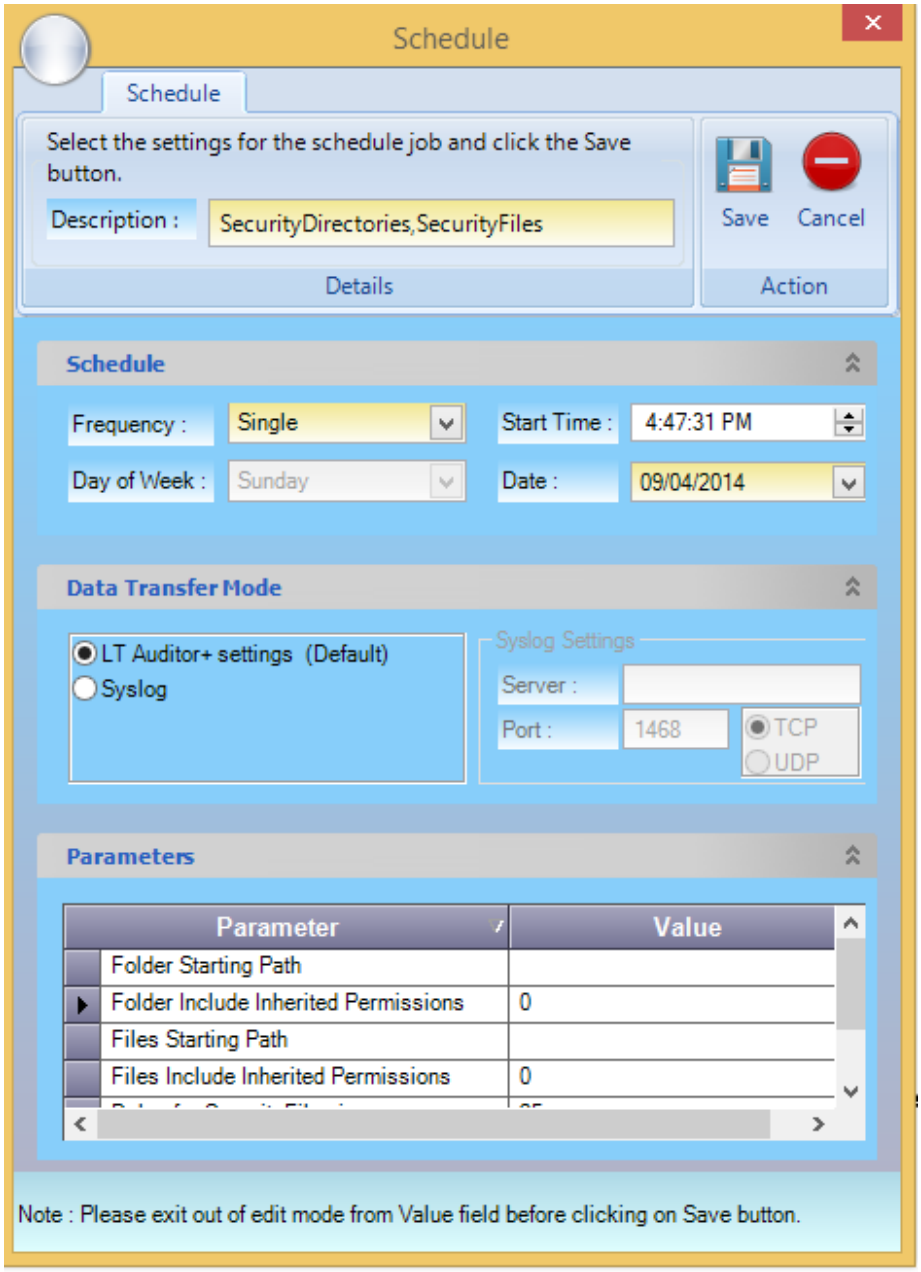
The left pane (*Assessment Pane*) displays a list of scripts that be selected for any scan job. Click on any script to display the possible reports that be generated in the *Assessment Details* pane.

The following events can be performed with the LTWAC.

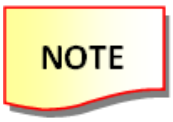
Schedule Scan Jobs

To schedule a scan job:

1. Select one or more scripts listed in the *Assessment* pane.
2. Click the *Schedule*  button to bring up the Schedule window



3. Select the desired Frequency for the job.
4. Select Data Transfer Mode. The default data transfer mode leverages LT Auditor+'s communication protocols to transfer data to the LT Auditor+ Manager. This is the recommended approach, however customers can choose to transfer using a Syslog server. To use Syslog:
    a. Select Syslog and enter the IP Address of the server where the LT Auditor+ Syslog Processor has been installed.
    b. Select the protocol to use for sending data collected during the scan to the Syslog server.



Please review Appendix B for additional configuration information when using Syslog.

5. Input parameters that can be passed for certain scan jobs. If a selected script requires parameters, the Parameters section will display the default parameters that can be modified. Details on parameters are discussed in APPENDIX A
6. Click the Save  button to save the scan job.

Job Status

The status of any job is displayed by clicking the + symbol that prefixes all scheduled jobs. Details are available on whether the job ran successfully or failed.

Delete Scan Jobs

To delete a scan job:

1. Click on the desired scan job to delete in the *Schedule* pane.
2. Right-click and select Delete or click the Delete  button.

Run Now

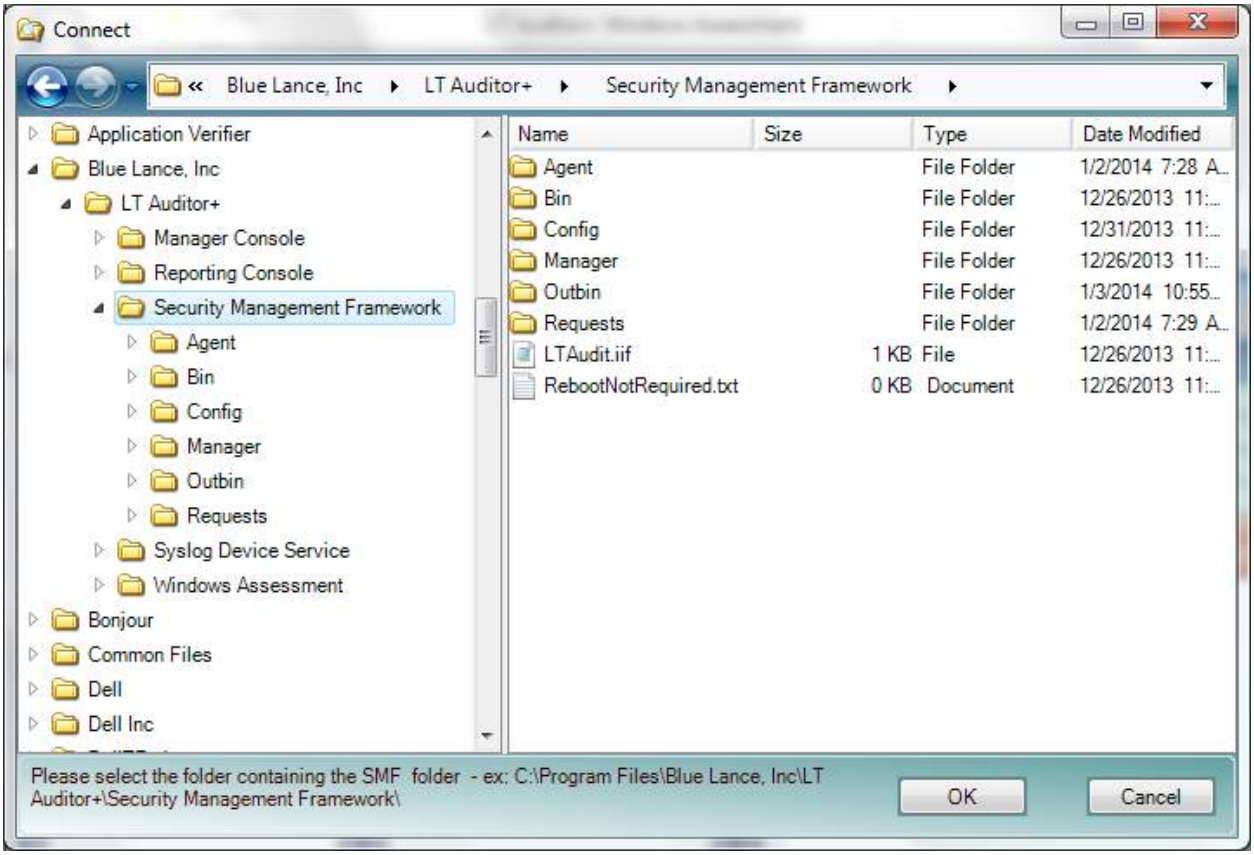
To run a job immediately:

1. Click on the desired scan job in the *Schedule* pane.
2. Right-Click and select Run now or click on the Run now  button.

Connect to a Remote Server

To schedule jobs on remote machines:

1. Click the Connect  button and browse to the 'Security Management Framework' (SMF) folder where LT Auditor+ has been installed.

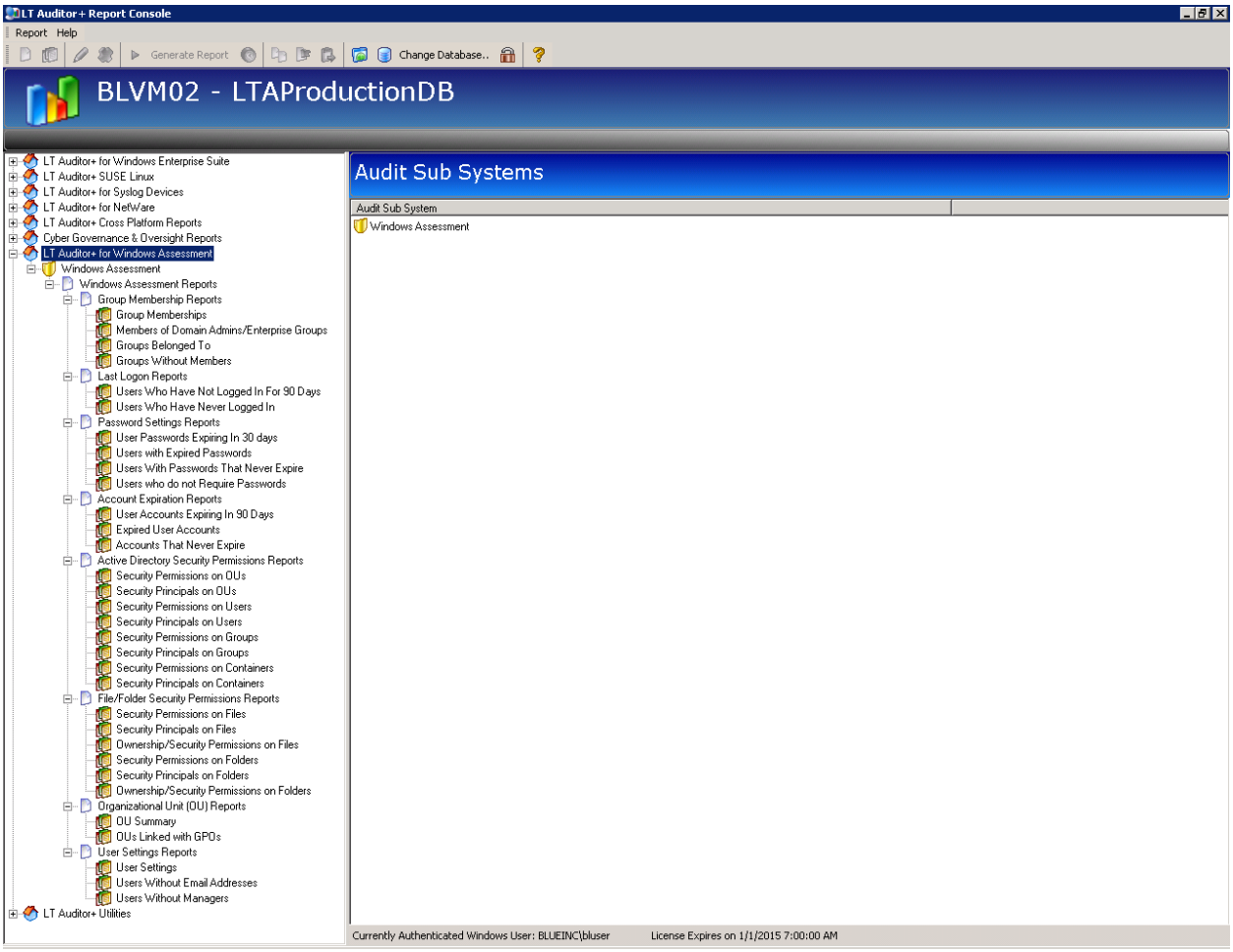


2. Setup a Scan job as described above,

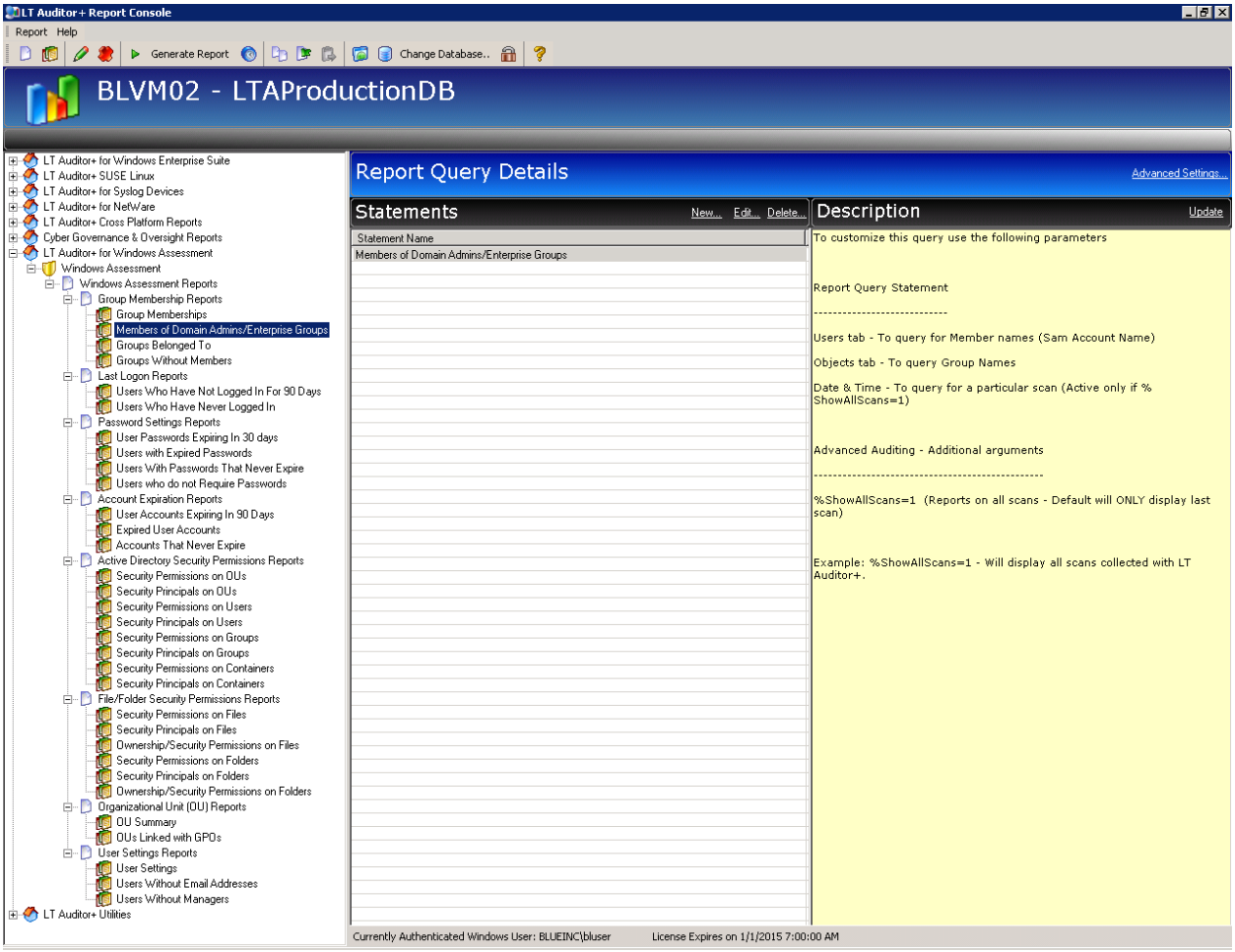
NOTE Prior to clicking the Connect button, please ensure that you have a drive mapped to the target agent machine.

Chapter 4 – Reporting for LT Auditor+ Windows Assessment

The default reports are created under the Windows Assessment reporting group as shown below:



Click on any of the report and details on how to query a report are provided in the description field.

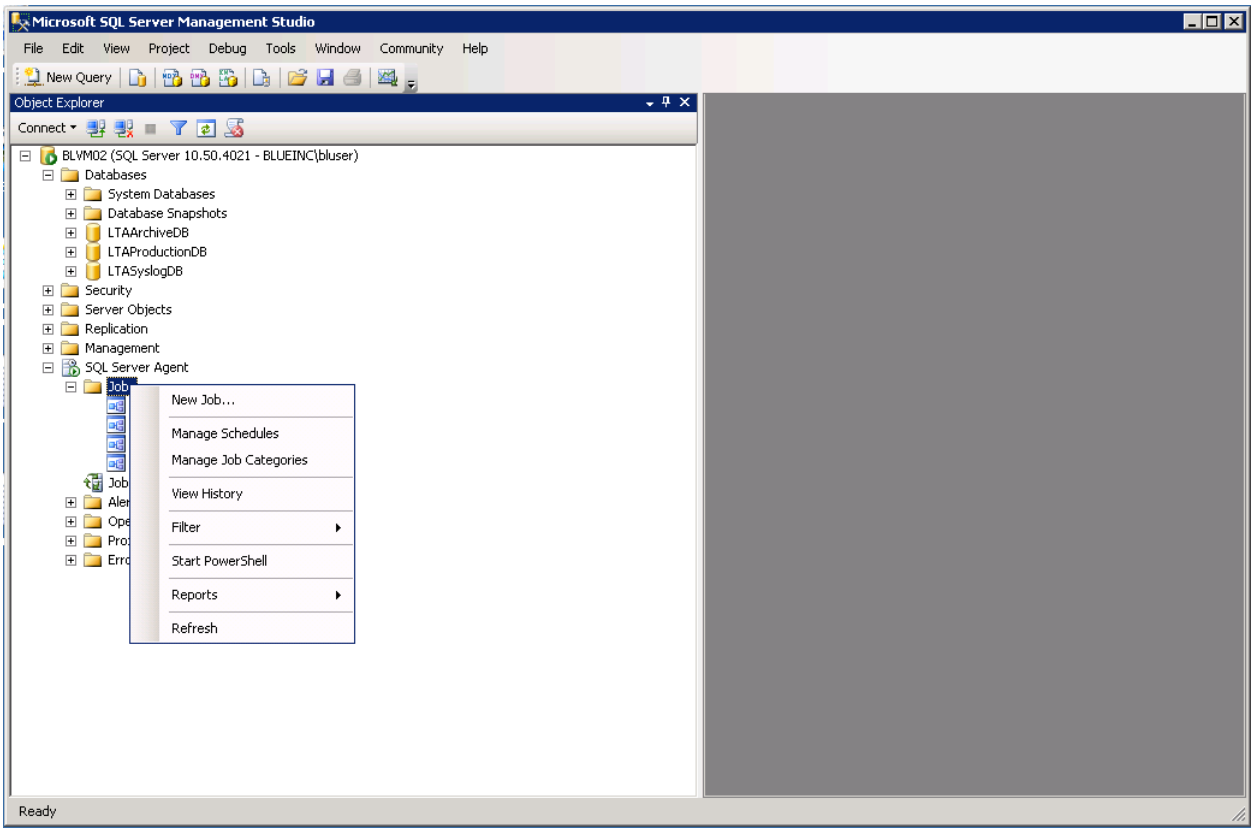


Please review the LT Auditor+ 2013 Configuration guide for details on configuring and scheduling reports.

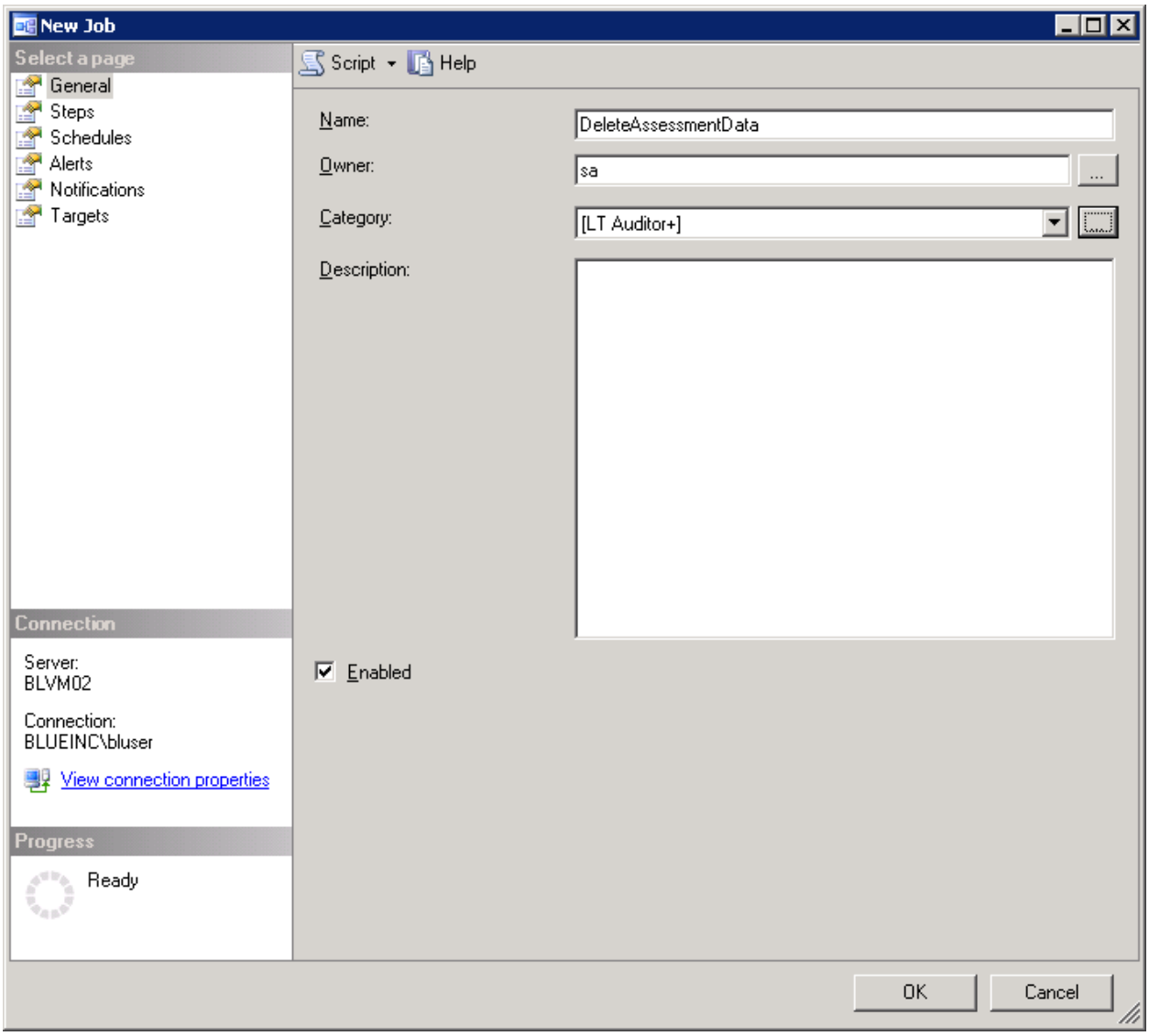
Chapter 5 – Setting up deletion job

Scheduling the deletion of Windows Assessments from the database is done by following these steps

Step 1. Login to the Microsoft SQL Server Management Studio and navigate to the section “Jobs”. Right click and select “New Job…” to create a new job.



Step 2. Enter the details as shown below.

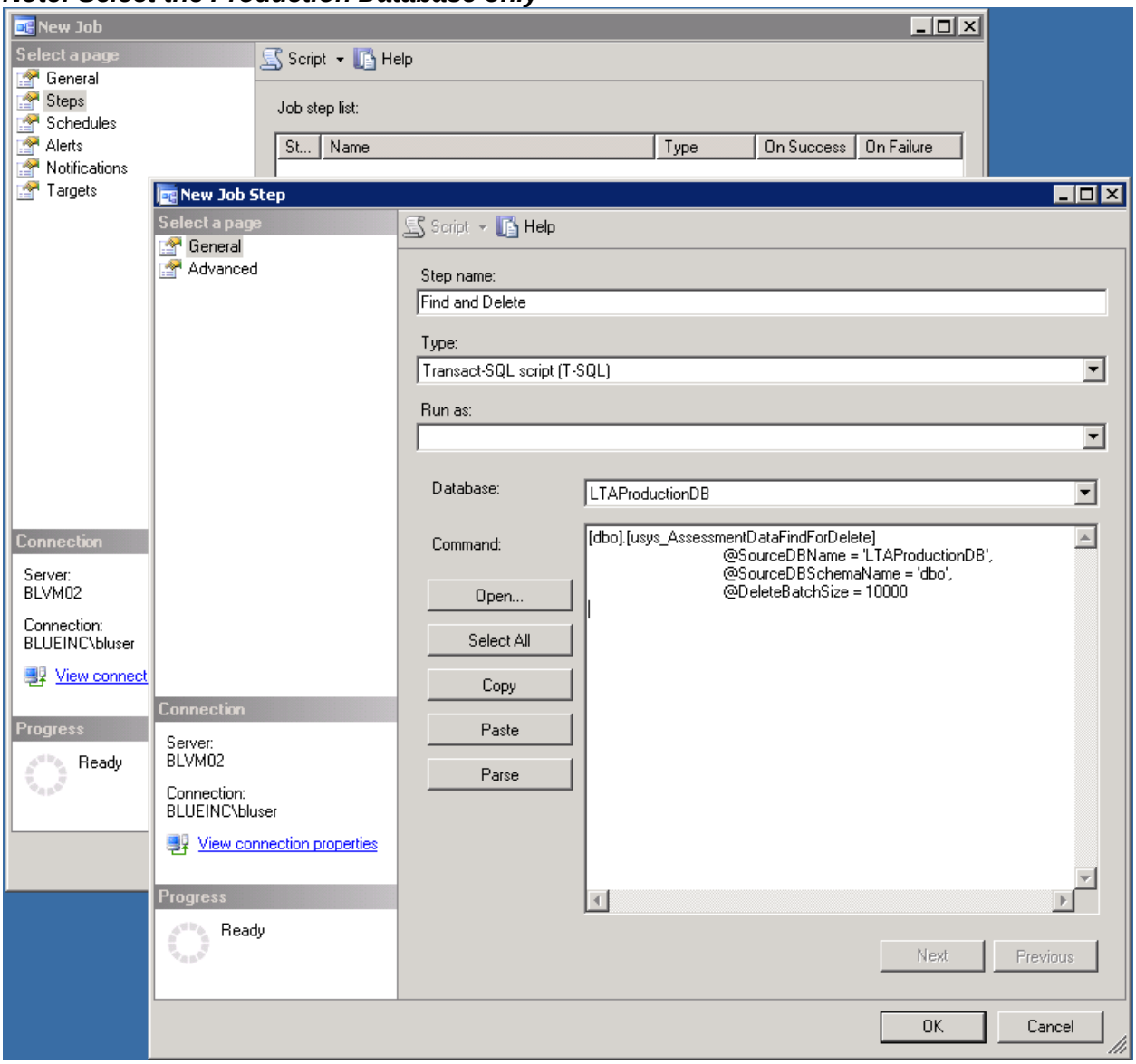


Step 3. Select “Steps” and click on “New” to create a new step and enter the following details –

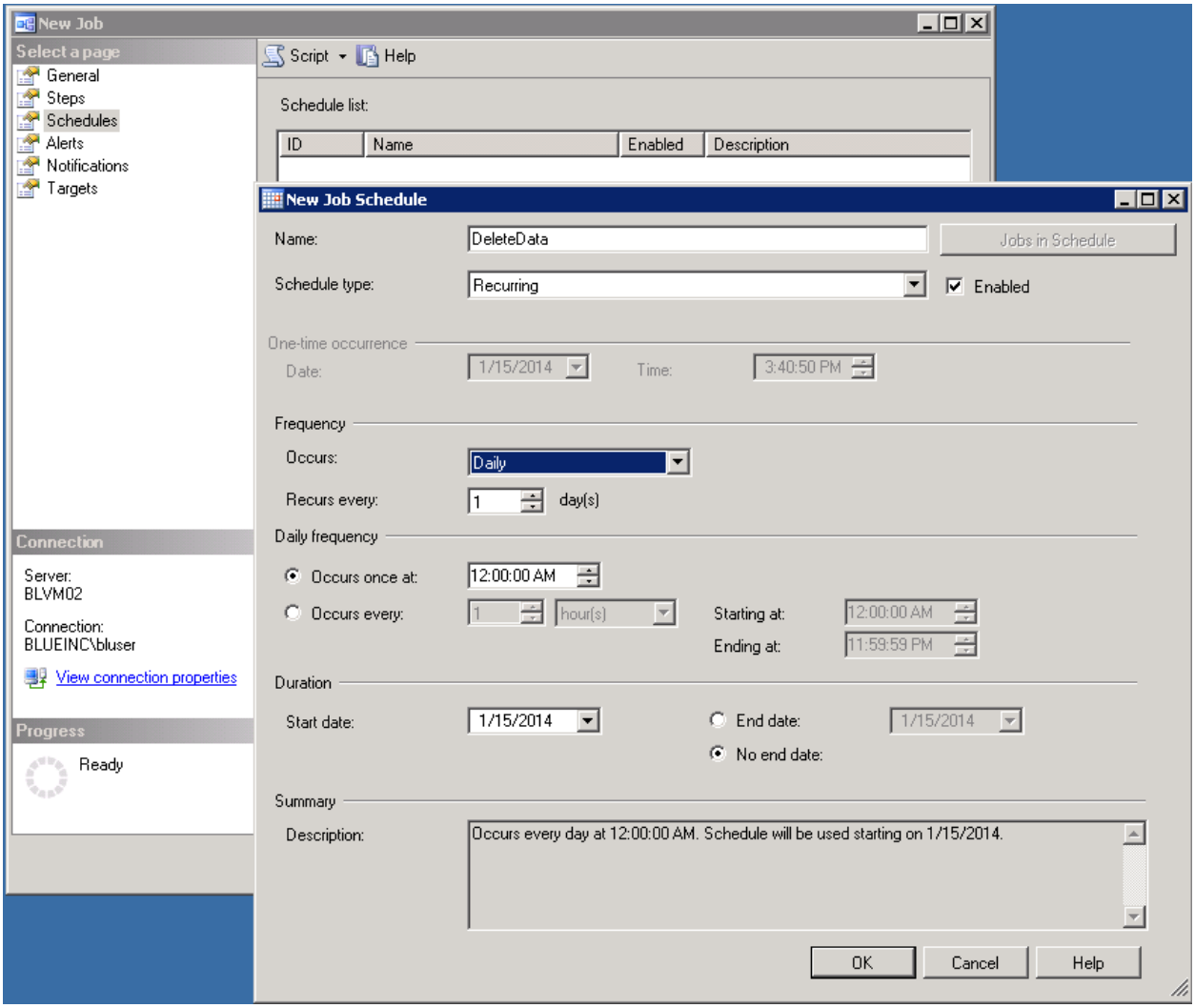
```
[dbo].[usys_AssessmentDataFindForDelete]
                @SourceDBName = 'LTAProductionDB',
                @SourceDBSchemaName = 'dbo',
```

@DeleteBatchSize = 10000

Note: Select the Production Database only



Step 4. Select “Schedules” and enter the details as shown below.



Step 5. Click on “OK” to save the details.

NOTE The deletion job retains the last assessment run and all older jobs are deleted for each category.

APPENDIX A – PowerShell Scripts

LT Auditor+ Windows Assessment uses PowerShell scripts to perform scans. The following table describes the available scripts and the parameters than are accepted for each script.

Script Name	Reports for this script	Parameters
GroupMembership	Group Memberships	
	Members of Domain Admins/Enterprise Groups	
	Groups Belonged To	
	Groups Without Members	
UserLastLogons	Users Who Have Not Logged In For 90 Days	
	Users Who Have Never Logged In	
UserPasswordSettings	User Passwords Expiring In 30 days	
	Users with Expired Passwords	
	Users With Passwords That Never Expire	
	Users who do not Require Passwords	
userAccountExpiration	User Accounts Expiring In 90 Days	
	Expired User Accounts	
	Accounts That Never Expire	
SecurityADOU	Security Permissions on OUs	
	Security Principals on OUs	
SecurityADUser	Security Permissions on Users	
	Security Principals on Users	
SecurityADGroup	Security Permissions on Groups	
	Security Principals on Groups	
SecurityADContainer	Security Permissions on Containers	
	Security Principals on Containers	
SecurityFiles	Security Permissions on Files	FilesIncludeInherited, FilesStartPath
	Security Principals on Files	
	Ownership/Security Permissions on Files	
SecurityDirectories	Security Permissions on Folders	FolderIncludeInherited, FolderStartPath
	Ownership/Security Permissions on Folders	
OUSummary	OU Summary	
OULinkedGPOs	OUs Linked with GPOs	
UserSettings	User Settings	
	Users With no Email Addresses	
	Users With no Managers	

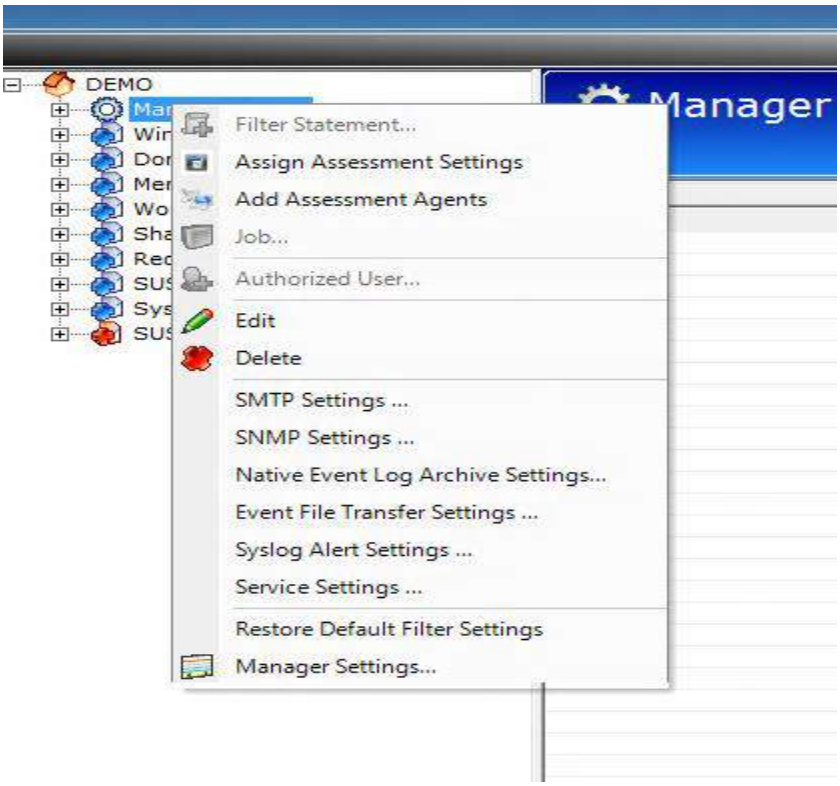
APPENDIX B – LT Auditor+ settings when using Syslog

The following steps outline how to configure LT Auditor+ to use the Syslog server.

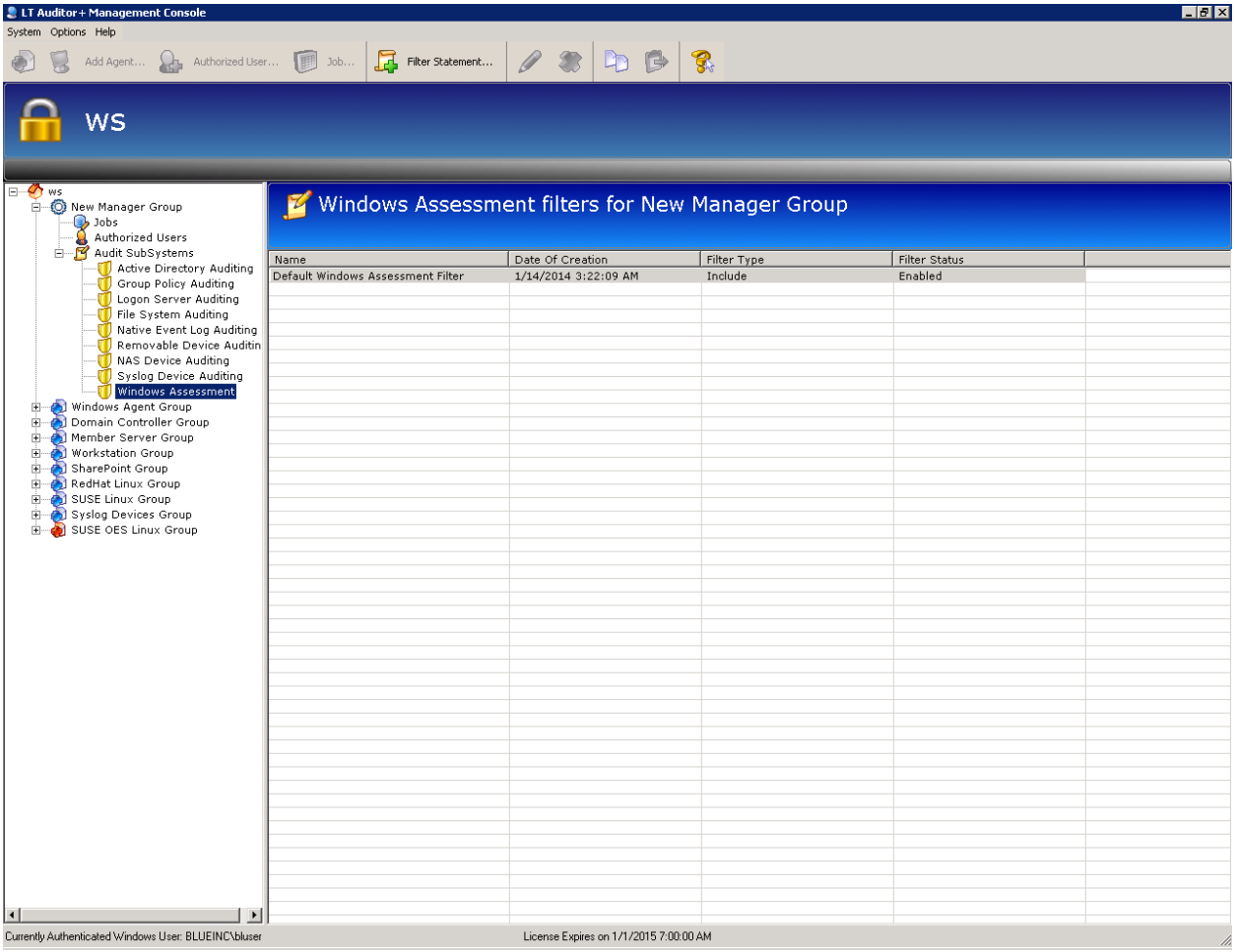
Setup LT Auditor+ Windows Assessment (LTWA)

LT Auditor+ Windows Assessment is an add-on module for LT Auditor+ 2013. LTWA requires:

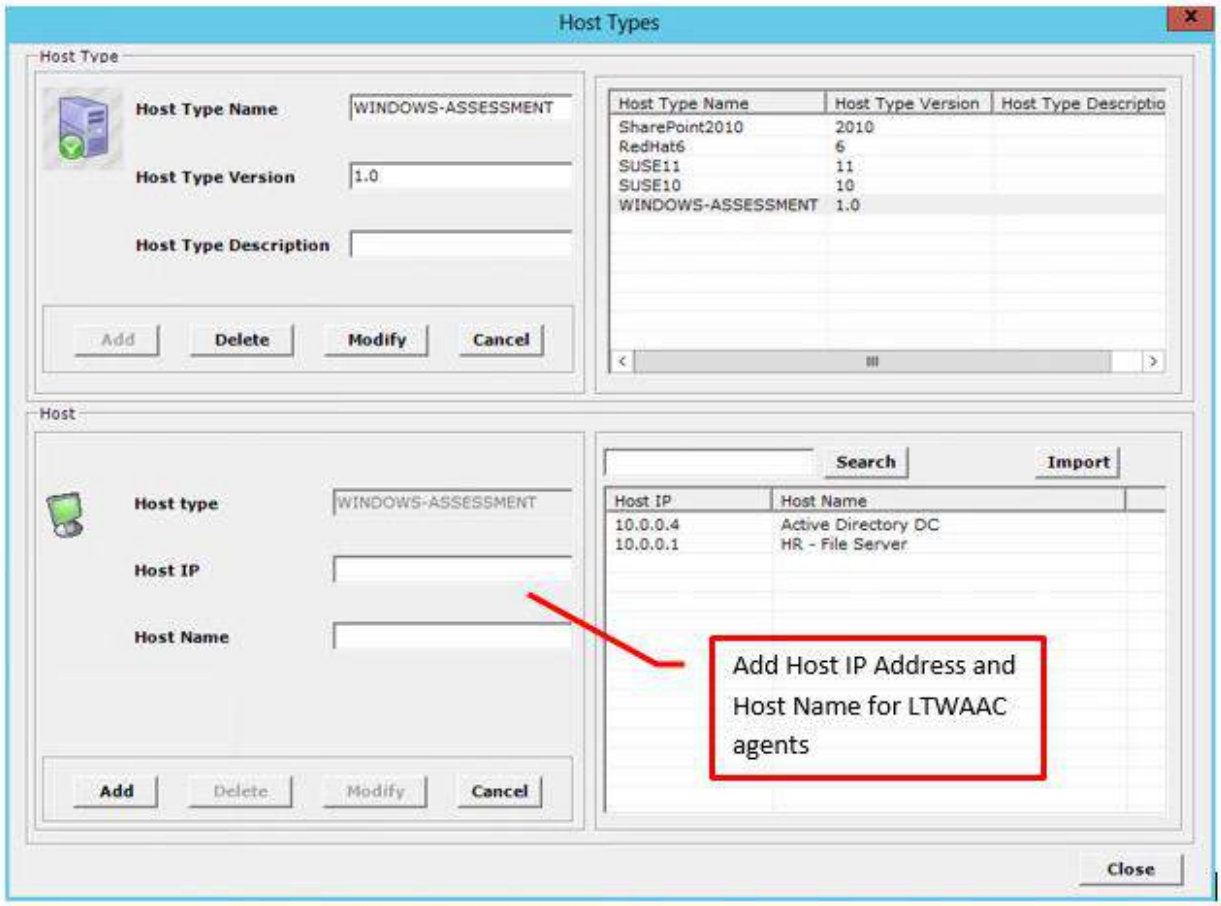
1. LT Auditor+ 2013 HF1302 (or higher) installed and configured in your environment. (For installing and configuring LT Auditor+ 2013 HF1302 please review the HF1302 installation and configuration documentation.
2. The LT Auditor+ 2013 Syslog Processor installed either on the LT Auditor+ Manager machine or any other Windows server.
3. On the LT Auditor+ Group (Manager/Agent) that hosts your Syslog Server Right-Click on the Group and select *Assign Assessment Settings* to set the default filter and rules. This rules will apply to the new Windows Assessment auditing arm. For example if your Syslog server is hosted on the same machine as the LT Auditor+ Manager follow these steps:
    a. Right click on the Manager Group and select Assign Assessment Settings



    b. This will create a filter under the Windows Assessment auditing arm:



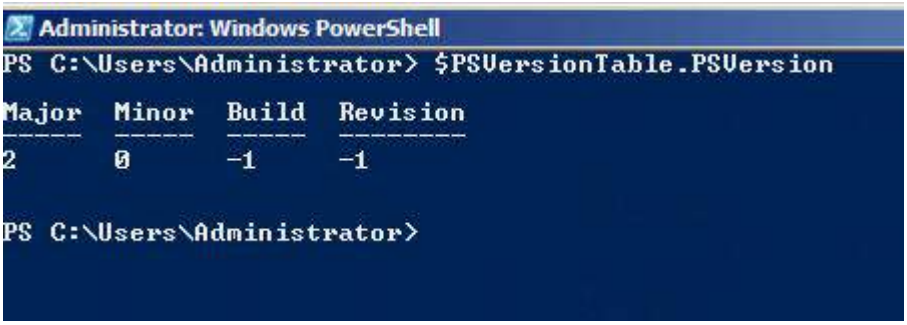
c. After installation of the LTWA components, please ensure that all agent machines are added to the LT Auditor+ Syslog Host and Host-Type tables displayed below. This is achieved with a right-click on the Group and selecting the option *Add Assessment Agents*.


Host Types
Host Type
Host Type Name
WINDOWS-ASSESSMENT
Host Type Version
1.0
Host Type Description
Add
Delete
Modify
Cancel
Host Type Name
Host Type Version
Host Type Descriptio
SharePoint2010
2010
RedHat6
6
SUSE11
11
SUSE10
10
WINDOWS-ASSESSMENT
1.0
Host
Host type
WINDOWS-ASSESSMENT
Host IP
Host Name
Add
Delete
Modify
Cancel
Search
Import
Host IP
Host Name
10.0.0.4
Active Directory DC
10.0.0.1
HR - File Server
Add Host IP Address and Host Name for LTWAAC agents
Close

APPENDIX C – Troubleshooting

Check Points

1. Ensure that scanned data is received by the Kiwi Syslog Server
2. Check PowerShell versions for all agent servers. Supported versions are 2.0 and 3.0. To check launch the PowerShell windows and run the command: *$PSVersionTable.PSVersion* and this should return the version information as shown below:



3. Ensure that you run the scans for Active Directory objects on a Windows Domain Controller

Error messages

Any error messages are logged to the Application log

1.) The term 'Get-ADUser' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

Resolution – Please run the scripts on an Active Directory environment.

2.) Failed. Error trying to send message.
Resolution – Check the connectivity to the Syslog server from the machine running the scripts.
Also check the Application log event id 5005 for detailed error.

APPENDIX D – What is new in LT Auditor+ Windows Assessment SP1

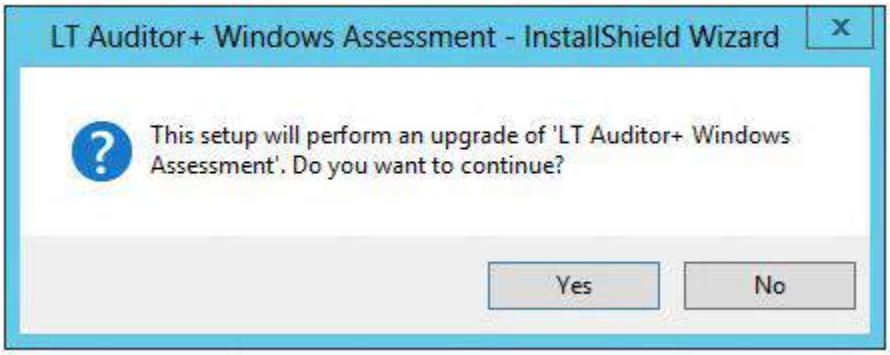
The primary change in LTWA SPI is the ability to transfer assessment data using the standard LT Auditor+ communication engine. The core benefits of using this approach are:

1. Removes requirement to have a Syslog server thereby improving stability and redundancy by eliminating a single point of failure
2. Reducing network traffic and congestion as data is not streamed in real time to the Syslog server.
3. Eliminating bottleneck issues on the Syslog server when receiving high volumes of data.

APPENDIX E – Upgrading to LT Auditor+ Windows Assessment SP1

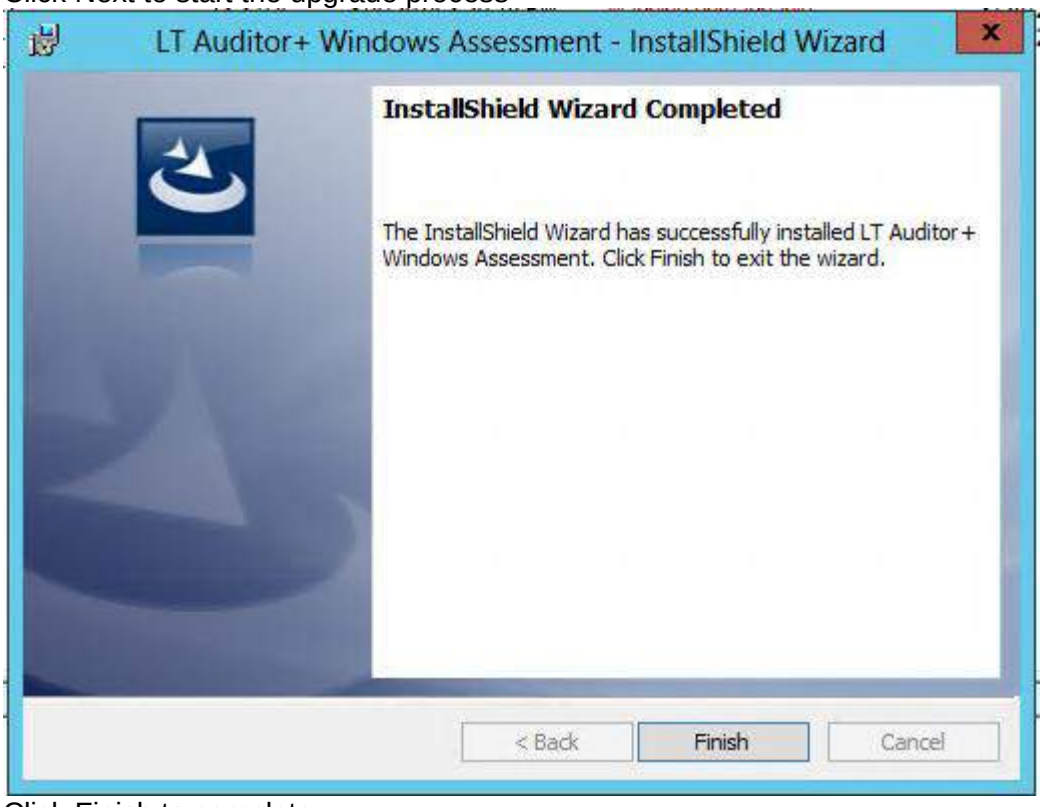
To upgrade to SP1 follow these steps. (Note In following section, the term Setup.exe will used to refer to either Setup_LT_Assessment_Manager_x64.exe or Setup_LT_Assessment_Manager_x32.exe based on the operating system selected.

1. Download LT Auditor+ for Windows Assessment SP1 and extract the zip file.
2. On the Manager machine run Setup.exe to bring the following Window



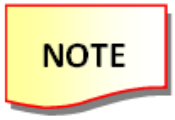
3. Click Yes to start the upgrade process and the following screen will appear

4. Click Next to start the upgrade process



5. Click Finish to complete.

6. Repeat steps 2 to 5 for all agent machines but with the executable ‘Setup_LT_Assessment_Agent’



After the upgrade we recommend that all scheduled jobs be deleted and create new jobs to leverage the new settings.