BLUE LANCE

LT Auditor+

Windows Assessment Build21 Release

Installation & Configuration Guide

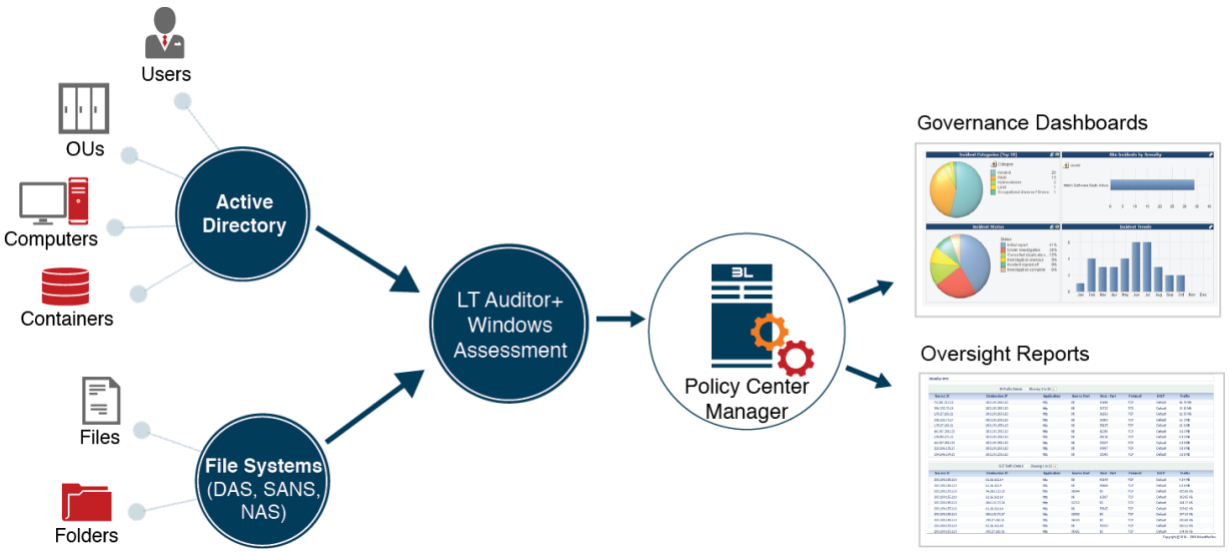
Table of Contents

Chapter 1 – Overview

The LT Auditor+ 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+ framework and can leverage audit data collected with other LT Auditor+ 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

The section provides an overview of how LTWA is installed and configured. Included in this section are systems requirements and prerequisites. Please review “APPENDIX D” for details on what is new in LT Auditor+ Windows Assessment SP3.

System Requirements

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

Prerequisites for the LT Auditor+ Windows Assessment installation

- Must have LT Auditor+ installed.
- PowerShell 3.0 and above.

Installer must have administrative privileges to install LT Auditor+ Windows Assessment.

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

LT Auditor+ Windows Assessment Components

The LT Auditor+ Windows Assessment component is included in the standard LT Auditor+ Build21 release download. After you download and extract the files, the following file should be available for the installation process:

Setup_LT_Assessment_Manager_x64.exe

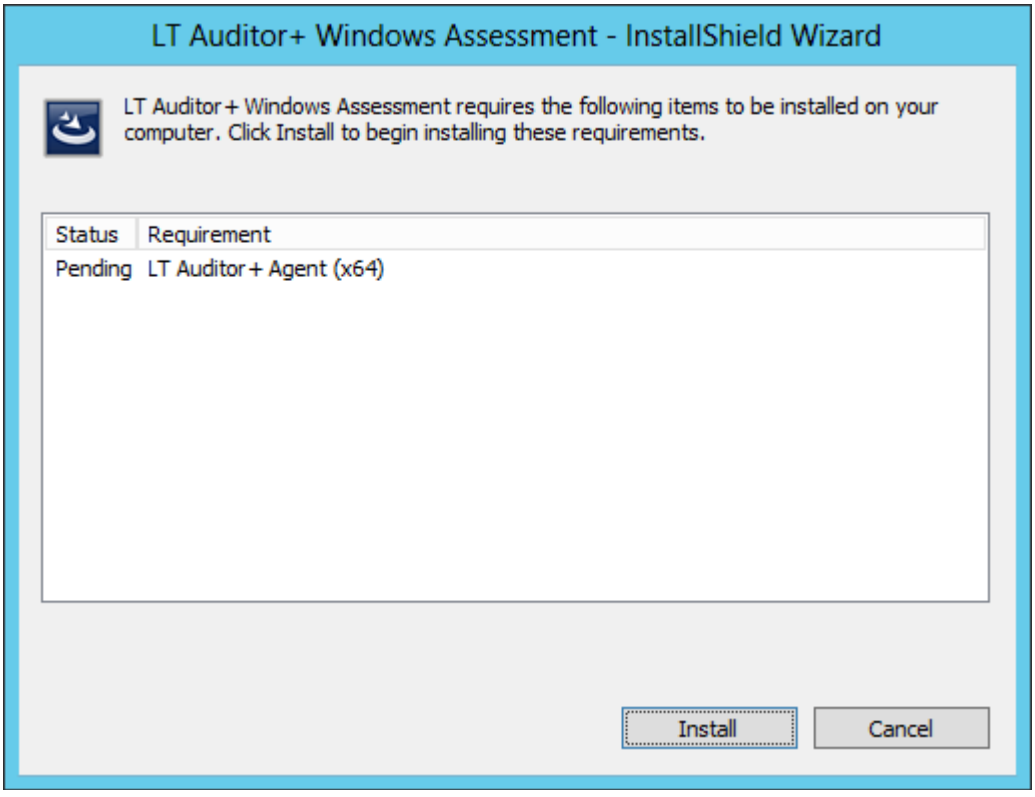
Installation Steps

LT Auditor+ Windows Assessment Manager Component (LTWAMC)

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

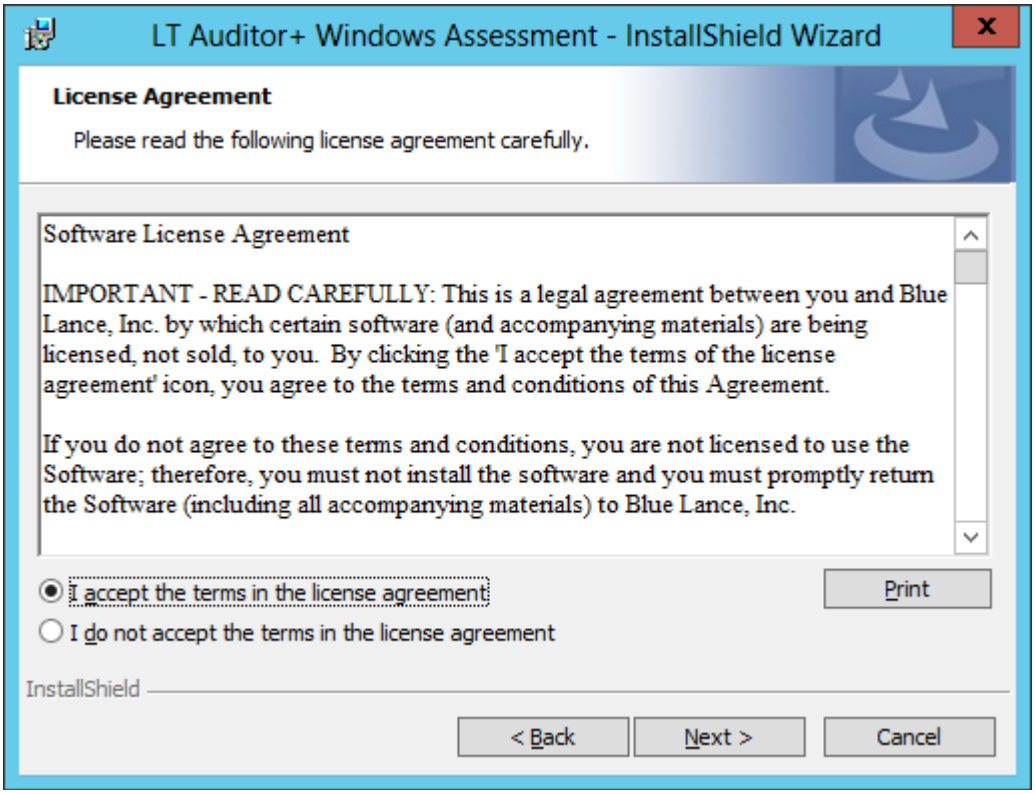
In the following section, the term Setup.exe will be used to refer to **Setup_LT_Assessment_Manager_x64.exe**.

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

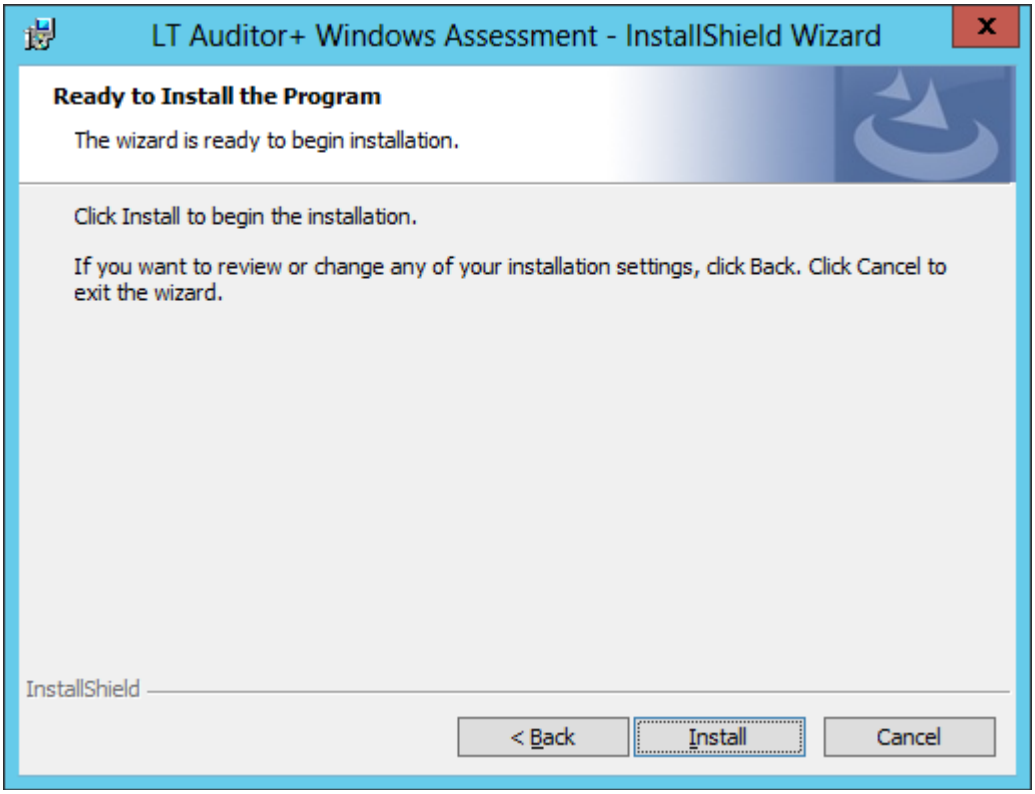


2. Click Install to bring up the following screen.

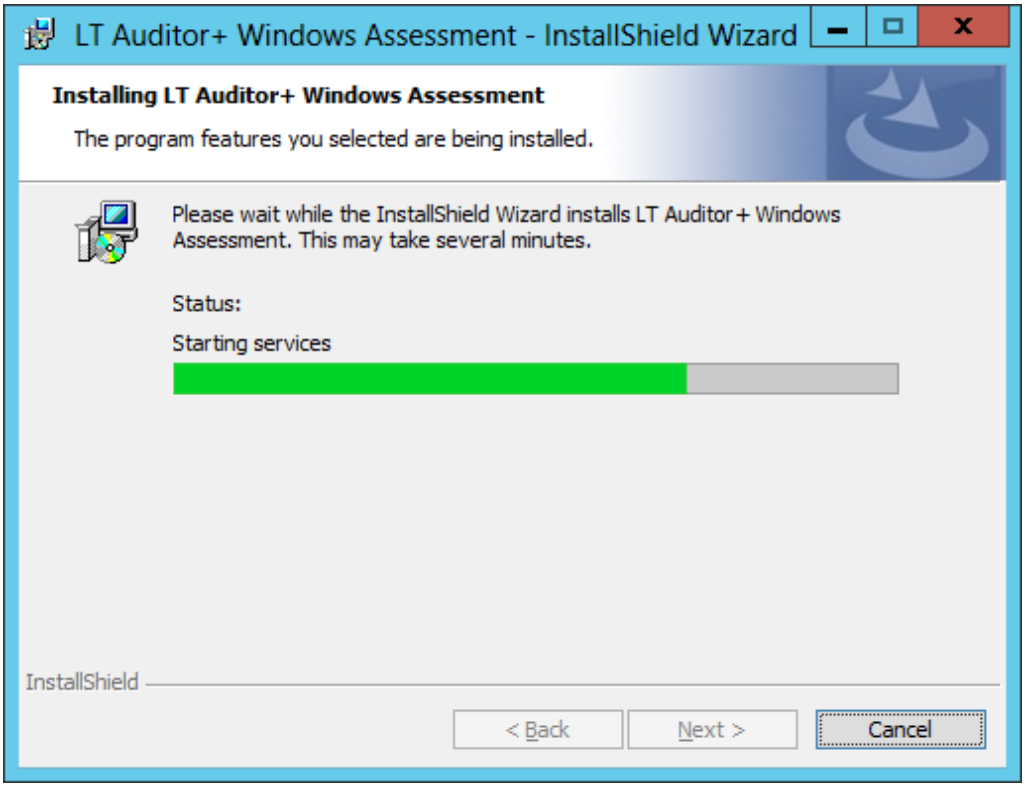
3. Click Next to bring up the License Agreement screen.

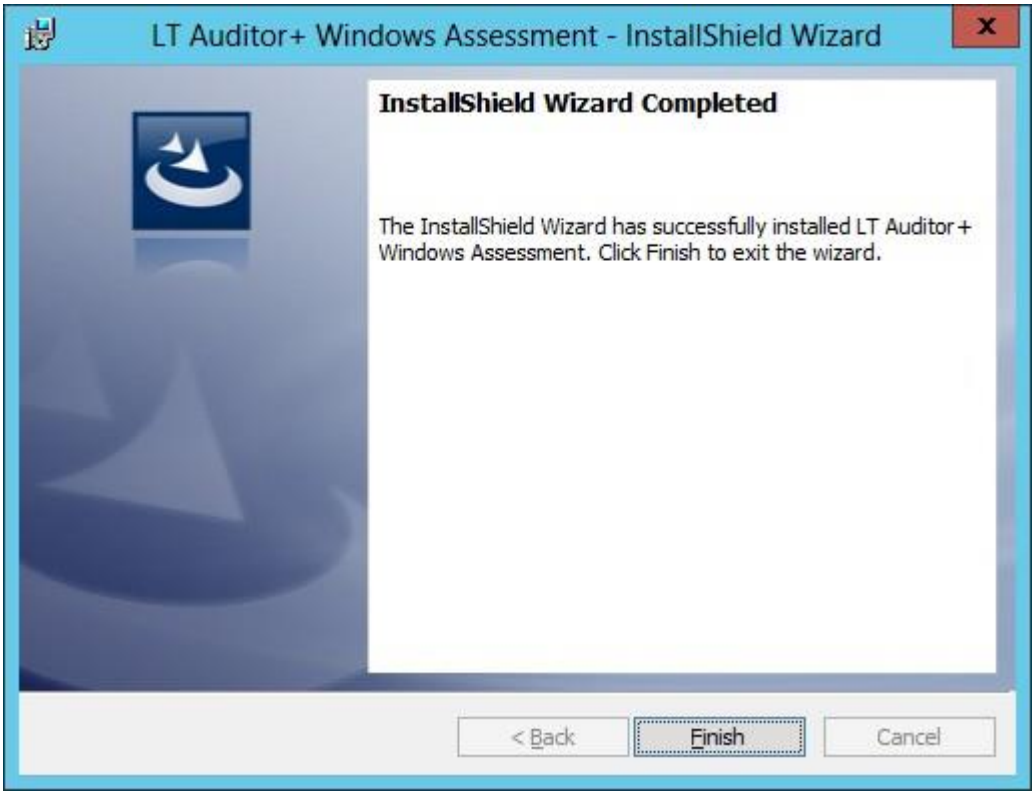


Read the Software License Agreement, and if acceptable, click on “I accept the license terms in the license agreement” and click Next.



4. Click Install to start the installation.





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

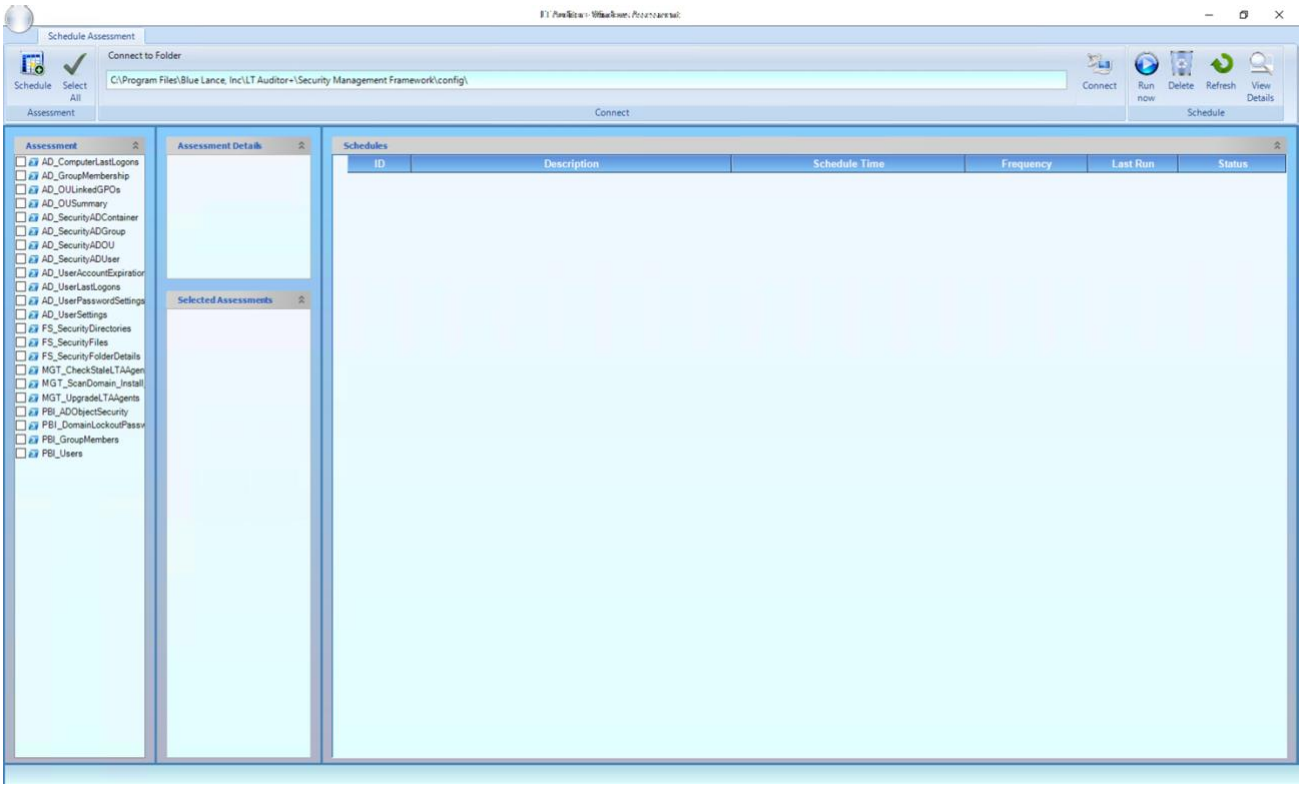
NOTE

LTAWMC is installed to the LT Auditor+ folder that hosts the LT Auditor+ SMF installation. The same module can be installed on other Windows machines in the environment as long as an LT Auditor+ Agent is on the machine.

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.



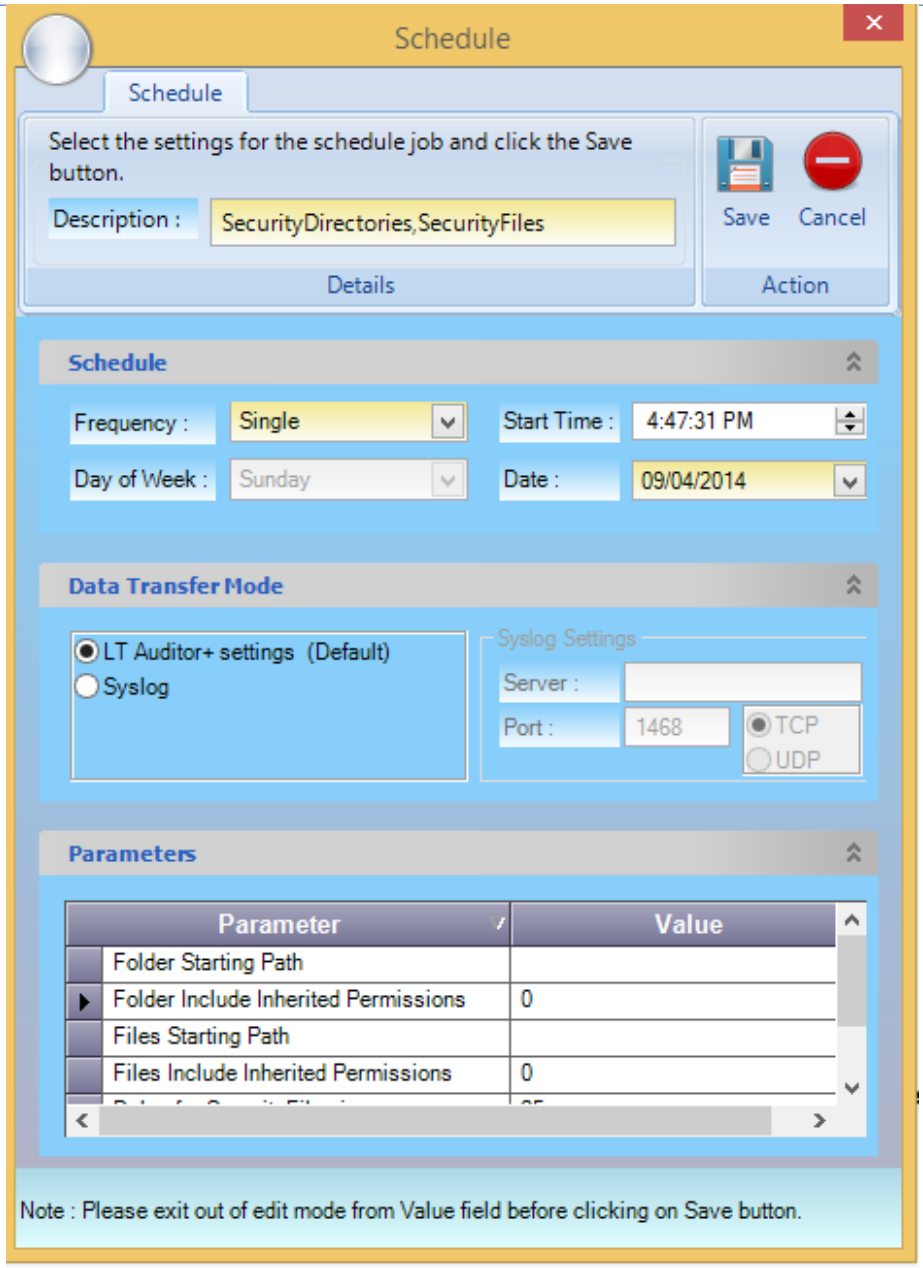
The left pane (Assessment Pane) displays a list of scripts that can be selected for any scan job. Click on any script to display the possible reports that be generated in the Assessment Details pane.

The following events can be performed with the LTWAC.

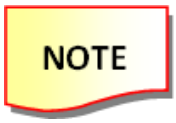
Schedule Scan Jobs

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

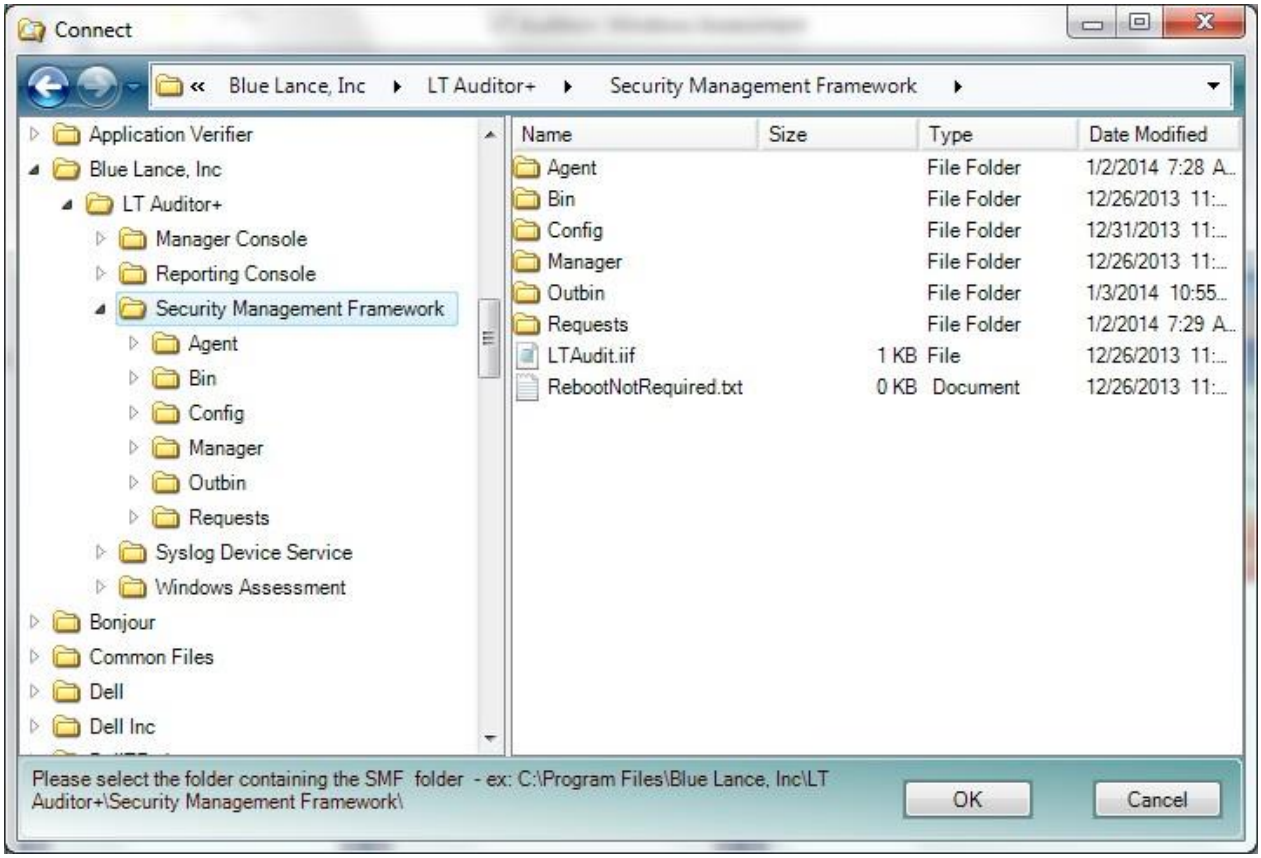
To run a job immediately:

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. Set up 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 – Scan Scripts

The following table describes the scans that can be scheduled to run with the LTWAMC. Periodic scans can be run for the following categories:

Active Directory Scans (Prefix AD_)

Active Directory scans can be scheduled to collect information on Users, Groups, Organization Units and Computers.

Purpose	Scripts
Group Membership Information	AD_GroupMembership.ps1
Information on Users, Password Settings and Last Logon Activity	AD_UserAccountExpiration.ps1 AD_UserLastLogons.ps1 AD_UserPasswordSettings.ps1 AD_UserSettings.ps1
Computer Information	AD_ComputerLastLogons.ps1
Data on permissions (DACLS) assigned to Active Directory Objects	AD_SecurityADContainer.ps1 AD_SecurityADGroup.ps1 AD_SecurityADOU.ps1 AD_SecurityADUser.ps1
Information on OUs	AD_OULinkedGPOs.ps1 AD_OUSummary.ps1

Prior versions of LT Auditor+ Windows Assessment scans did not have any prefix in the name. If those files have been scheduled to run, please delete schedules and files and proceed to set up new scheduled scans.

File System Scans (Prefix FS_)

File system scans can be scheduled to collect information on permissions assigned to principals for scanned files and folders.

Purpose	Scripts
Scan Folders	FS_SecurityDirectories.ps1 FS_SecurityFolderDetails.ps1
Scan Files	FS_SecurityFiles.ps1

Scans for LT Auditor+ Power BI Panels (Prefix PBI_)

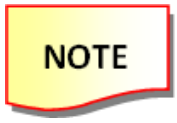
File system scans can be scheduled to collect information on permissions assigned to principals for scanned files and folders.

Purpose	Scripts
Scans required for LT Auditor+ Power BI panels	PBI_ADObjectSecurity.ps1 PBI_DomainLockoutPasswordPolicy.ps1 PBI_GroupMembers.ps1 PBI_Users.ps1

Scans for LT Auditor+ Maintenance (Prefix MGT_)

These scans can be scheduled to install, update and maintain LT Auditor+ Agents in the environment.

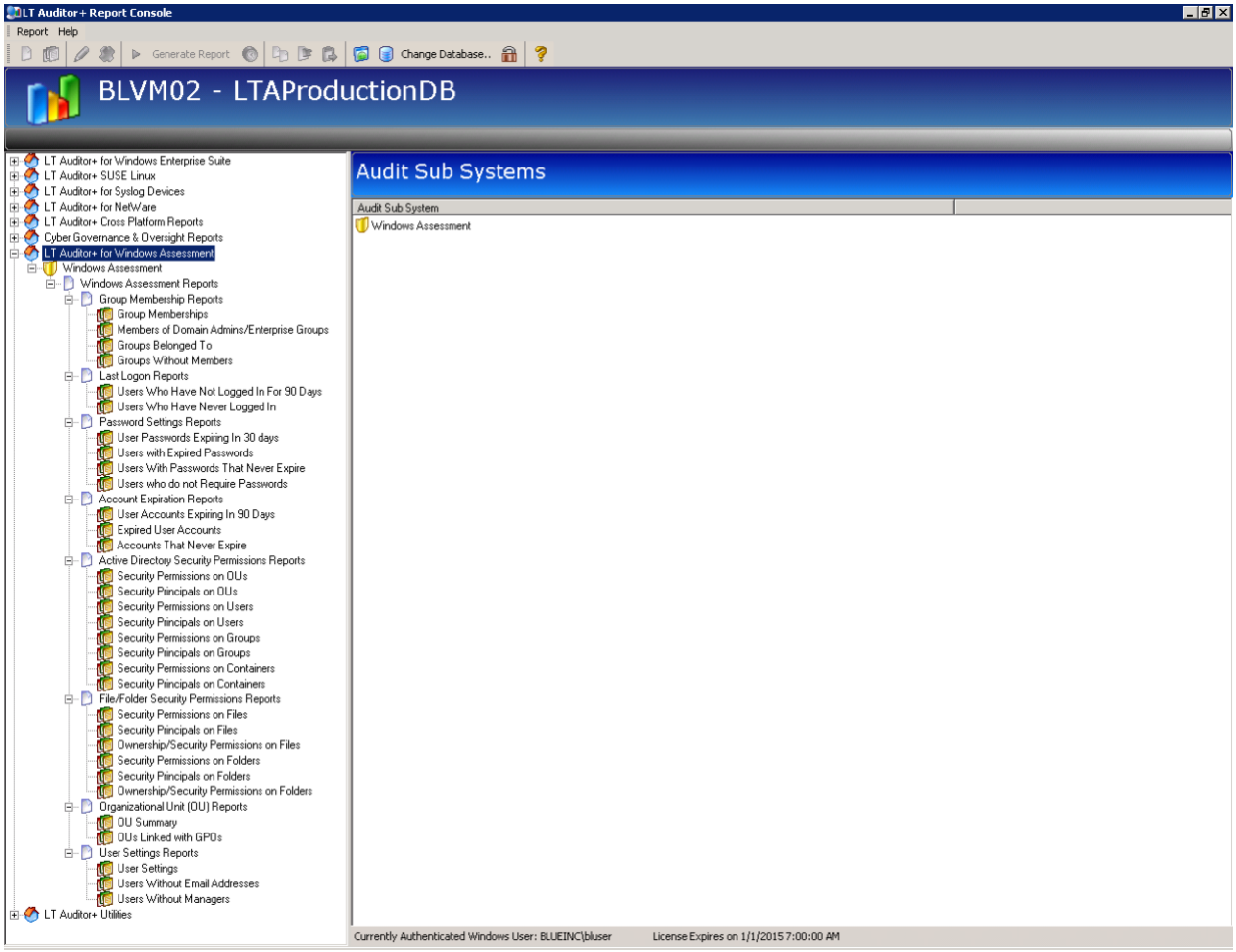
Purpose	Scripts
Scan to check status of LT Auditor+ Agents. Can be configured to delete stale agents, update IP Addresses and restart LT Auditor+ services on agents that are not active.	MGT_CheckStaleLTAAgents.ps1
Scan to check Active Directory domain for new computers (Workstations or Servers) that do not have LT AUDITOR+ installed. If such systems are discovered, the script proceeds to install LT Auditor+ Agent on these machines to ensure organizational auditing and compliance policies are met.	MGT_ScanDomain_Install_LTA_Agents.ps1
Scan to upgrade LT Auditor+ Agents with the latest updates.	MGT_UpgradeLTAAgents.ps1



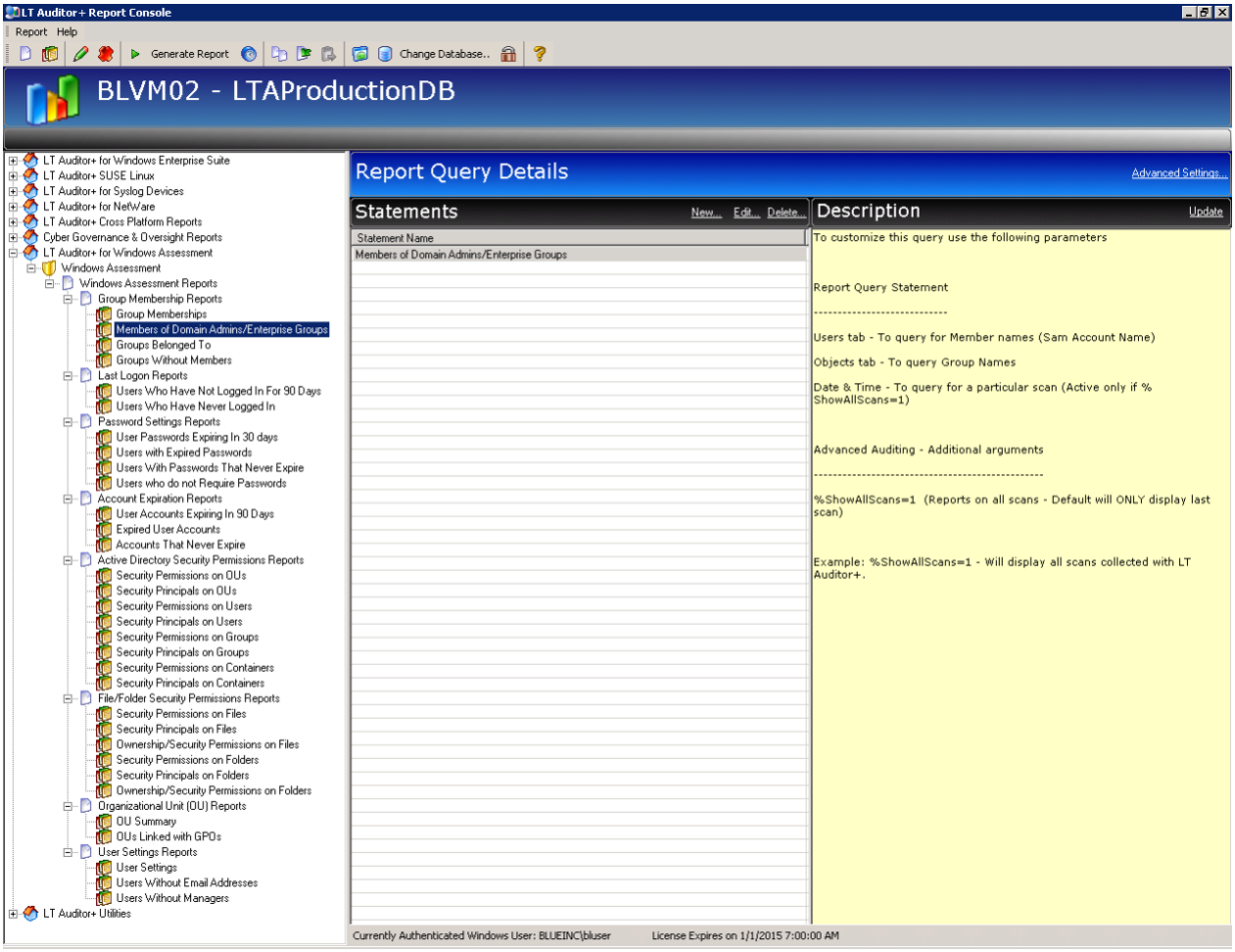
For maintenance scripts, the Windows Assessment service must be started with an account that has permissions to install LT Auditor+ on remote machines, as well as have access to read and update the LT Auditor+ database.

Chapter 5 – 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 reports, and details on how to query a report are provided in the description field.

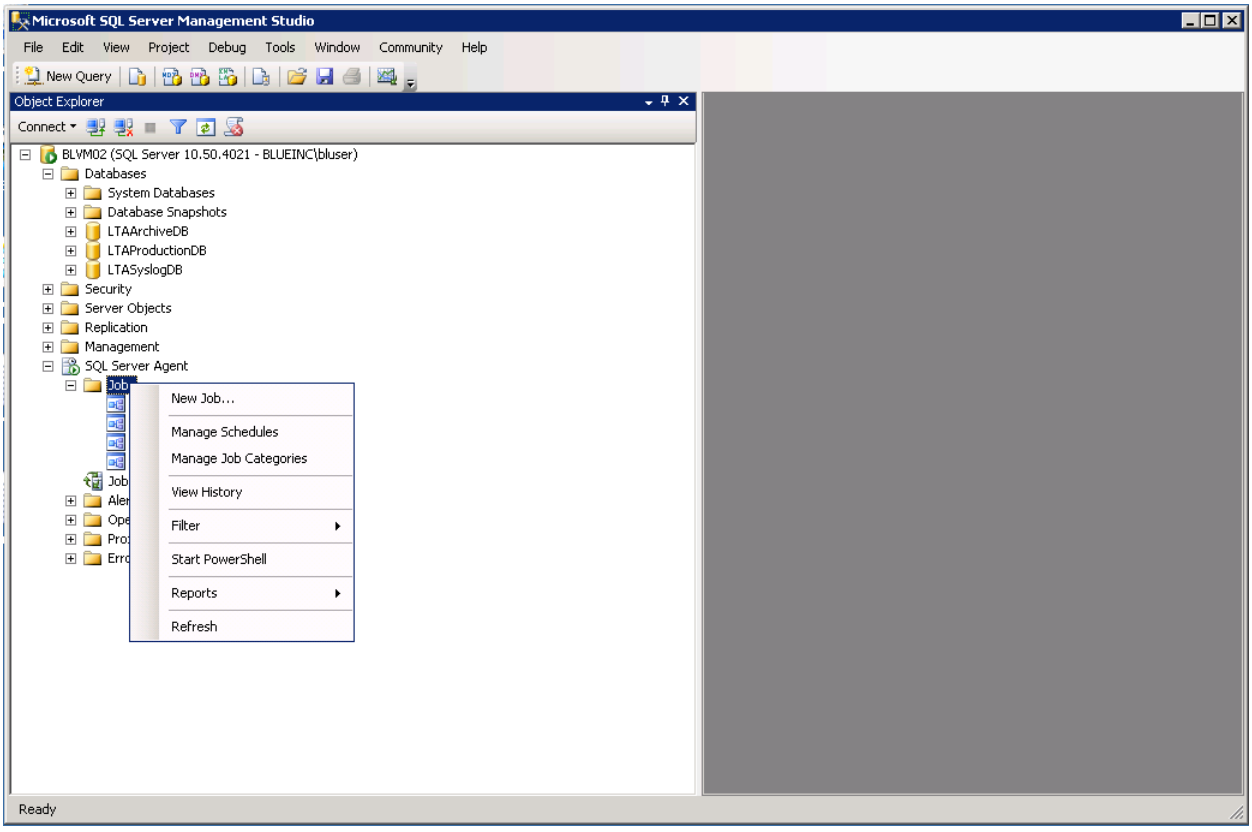


Please review the LT Auditor+ Configuration Guide for details on configuring and scheduling reports.

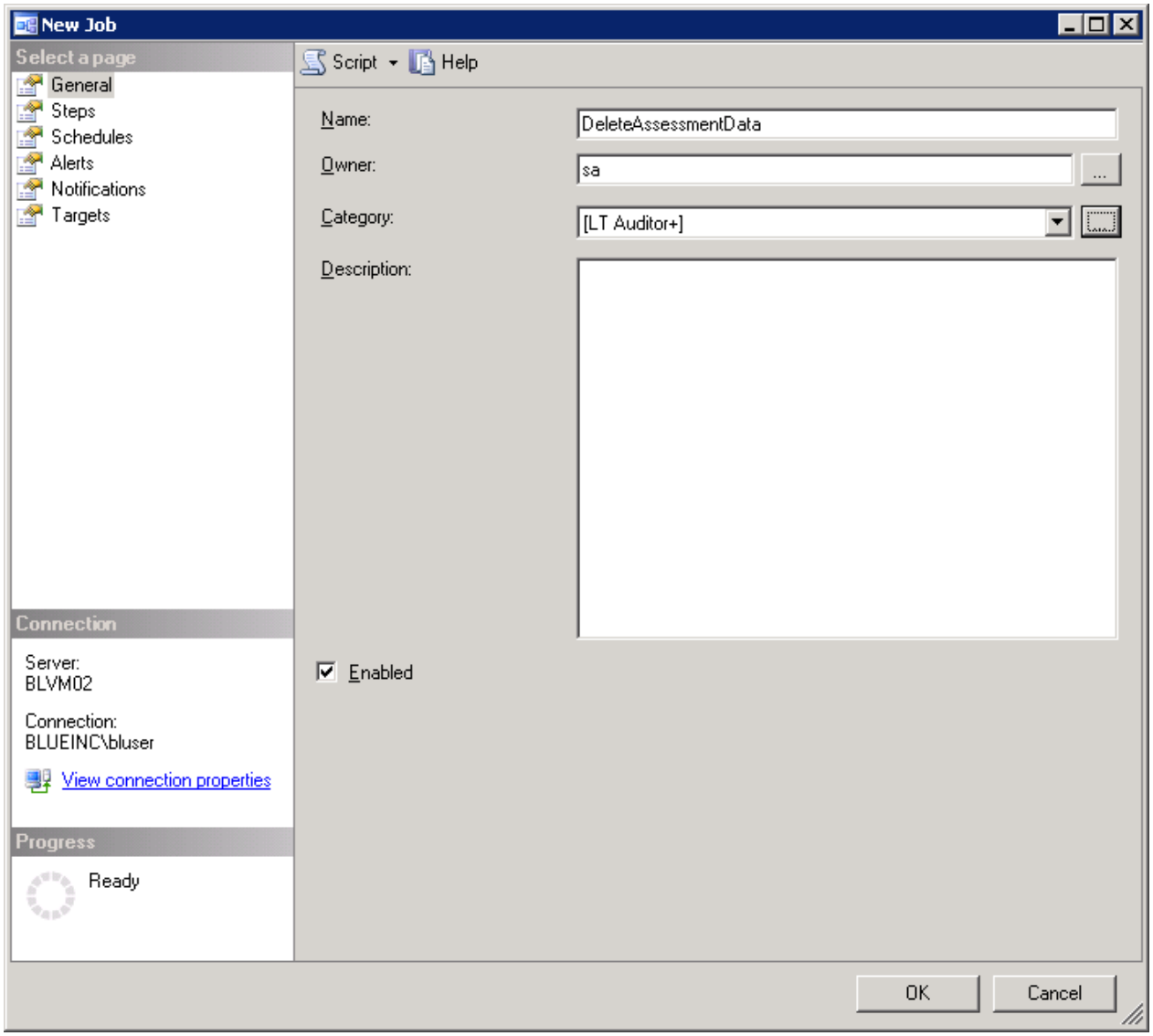
Chapter 6 – Setting Up Deletion Job

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

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



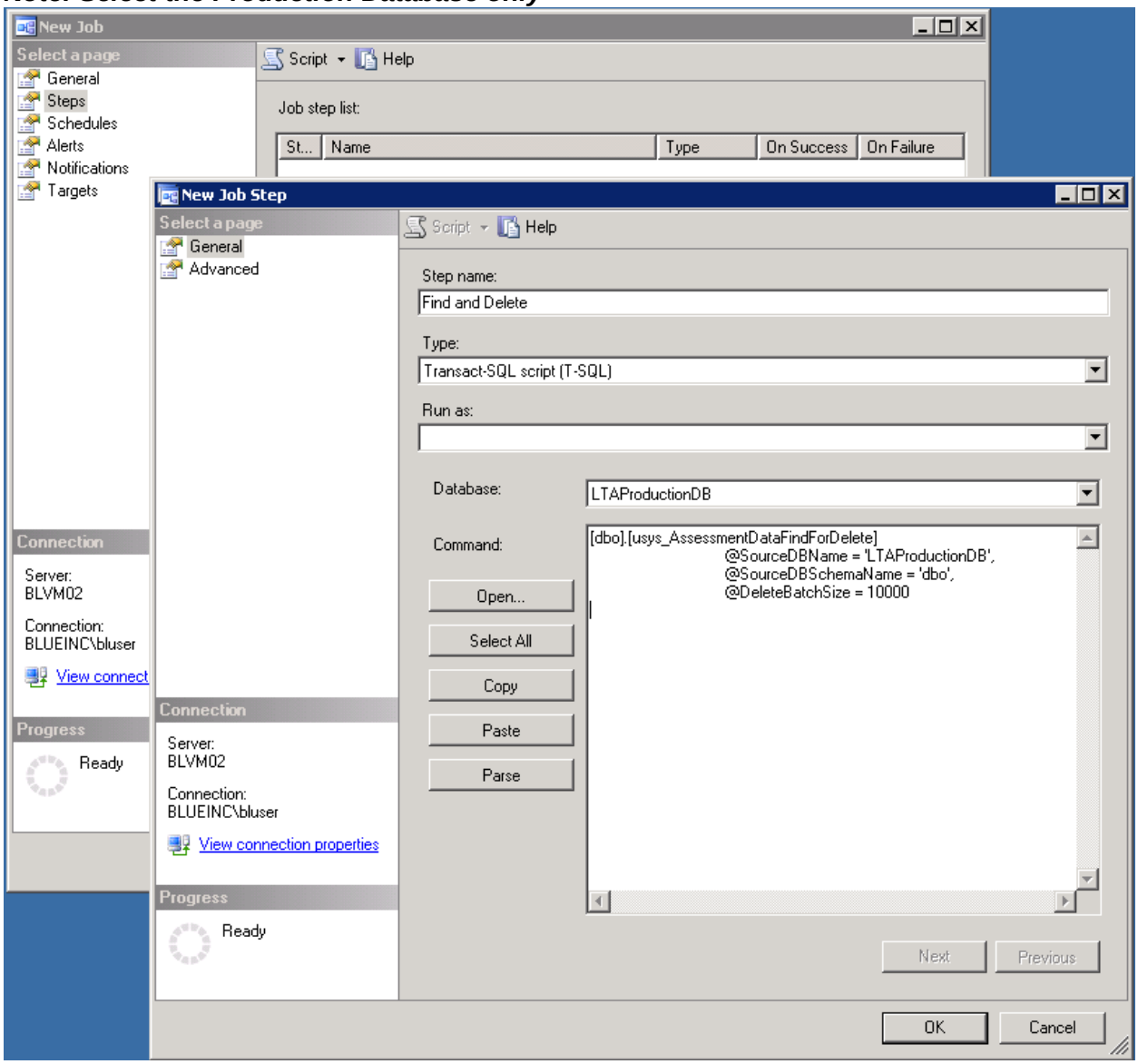
2. Enter the details as shown below.



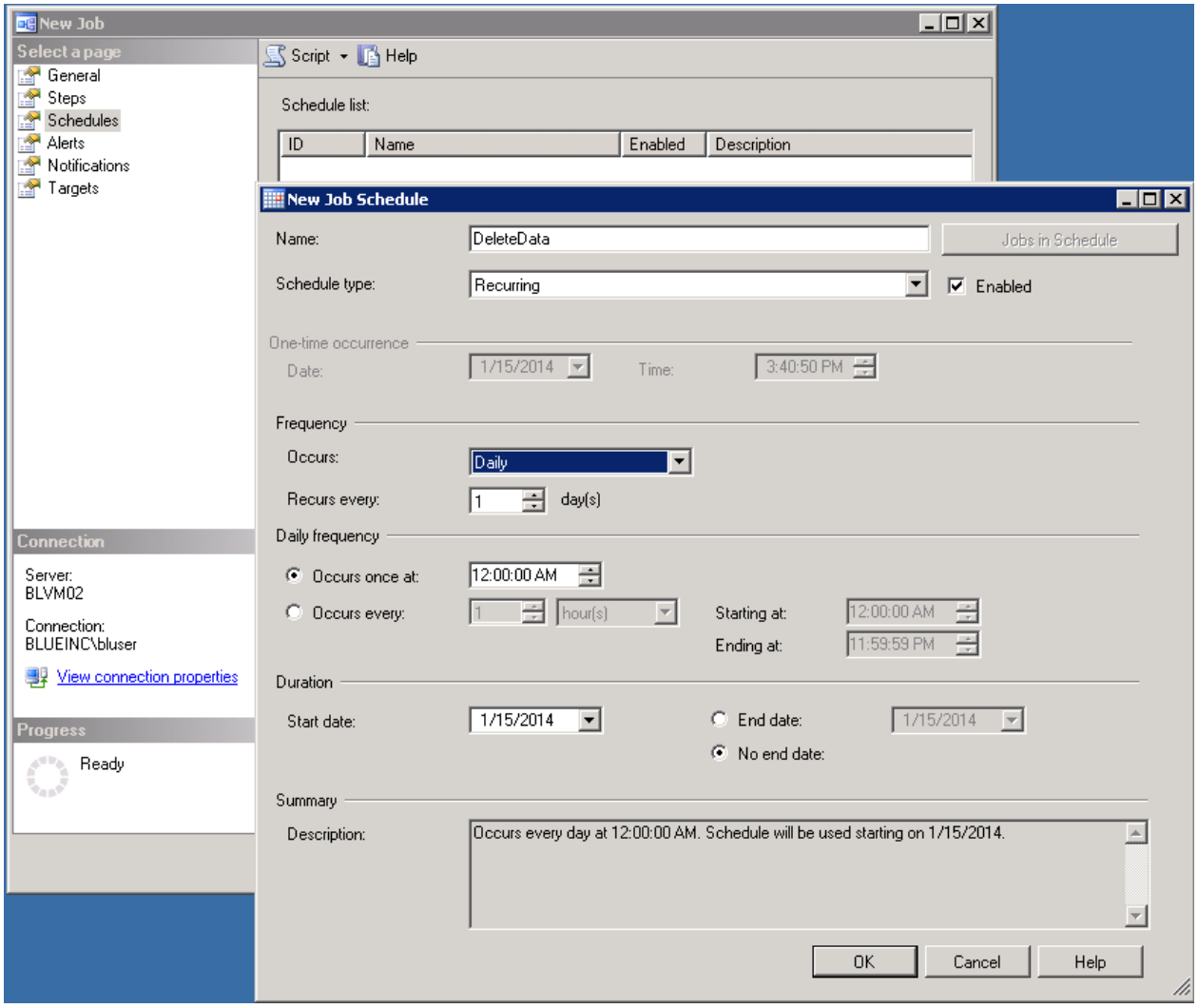
3. Select Steps and click on New to create a new step, and enter the following details: **[dbo].[usys_AssessmentDataFindForDelete]**
@SourceDBName = 'LTAProductionDB',
@SourceDBSchemaName = 'dbo',

@DeleteBatchSize = 10000

Note: Select the Production Database only



4. Select Schedules and enter the details as shown below.



5. Click 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 that are accepted for each script.

Script Name	Reports for this script	Parameters
AD_GroupMembership	Group Memberships	
	Members of Domain Admins/Enterprise Groups	
	Groups Belonged To	
	Groups Without Members	
AD_UserLastLogons	Users Who Have Not Logged In For 90 Days	
	Users Who Have Never Logged In	
AD_Computers Last Accessed	Computers not accessed in the last 90 days Computers that have never been accessed	
AD_UserPasswordSettings	User Passwords Expiring In 30 days	
	Users with Expired Passwords	
	Users With Passwords That Never Expire	
	Users who do not Require Passwords	
AD_UserAccountExpiration	User Accounts Expiring In 90 Days	
	Expired User Accounts	
	Accounts That Never Expire	
AD_SecurityADOU	Security Permissions on OUs	
	Security Principals on OUs	
AD_SecurityADUser	Security Permissions on Users	
	Security Principals on Users	
AD_SecurityADGroup	Security Permissions on Groups	
	Security Principals on Groups	
AD_SecurityADContainer	Security Permissions on Containers	
	Security Principals on Containers	
FS_SecurityFiles	Security Permissions on Files	FilesIncludeInherited, FilesStartPath
	Security Principals on Files	
	Ownership/Security Permissions on Files	
FS_SecurityDirectories	Security Permissions on Folders	FolderIncludeInherited, FolderStartPath
	Ownership/Security Permissions on Folders	
AD_OUSummary	OU Summary	
AD_OULinkedGPOs	OUs Linked with GPOs	
AD_UserSettings	User Settings	
	Users With no Email Addresses	
	Users With no Managers	

APPENDIX B — Setting Up Active Directory Scans on a Machine That Is Not a Domain Controller

To run Active Directory scans on machines that are not Domain Controllers, you will need to install the PowerShell RSAT-AD and GPMC modules. Instructions to install these components are listed below.

Prerequisites:

- Operating System – Windows 2012R2 and above.
- PowerShell version 3.0 and above.
- The Windows machine must be in the Active Directory domain.

Installation:

1. Log in to Windows machine with a domain admin account.

2. Open a PowerShell Window (Run as Administrator) and ensure that you can run PSHELL commands by running the following command:
   Set-ExecutionPolicy Unrestricted

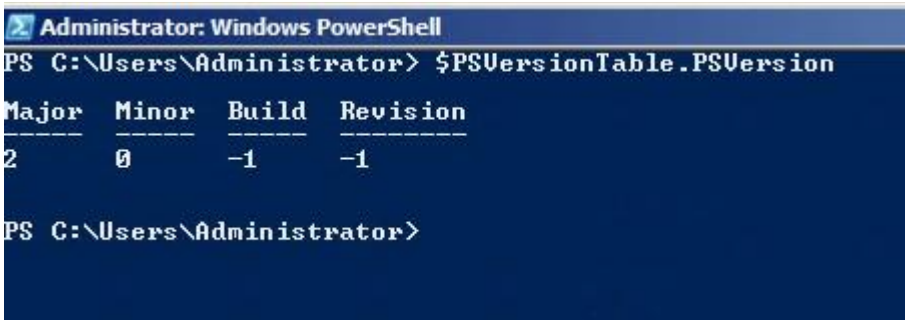
3. Execute the following commands:
   - **Import-Module ServerManager**
   - **Add-WindowsFeature RSAT-AD-PowerShell**
   - **Add-WindowsFeature –Name GPMC**

4. Run **Set-ExecutionPolicy Restricted** to reset PowerShell settings.

APPENDIX C —Troubleshooting

Checkpoints

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.

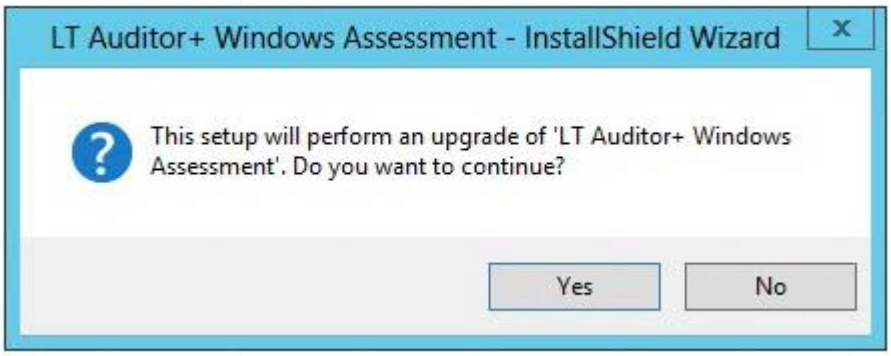
APPENDIX D — What is new in LT Auditor+ Windows Assessment Build21

1. Added scans for LT Auditor+ Power BI panels.
2. Added scan for automating the discovery and installation of LT Auditor+ on new machines in the environment.
3. Added scans to maintain and upgrade LT Auditor+ Agents.

APPENDIX E — Upgrading to LT Auditor+ Windows Assessment BUILD21

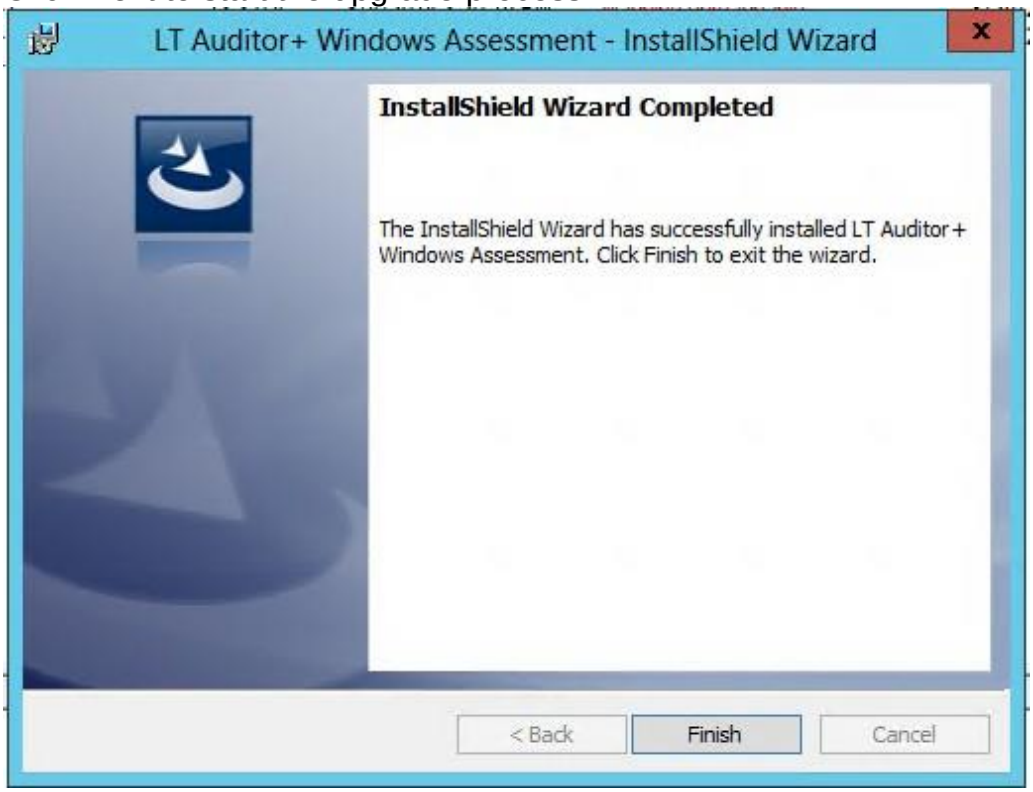
To upgrade to SP3 follow these steps. (Note In the following section, the term Setup.exe will be used to refer to either **Setup_LT_Assessment_Manager_x64.exe** or **Setup_LT_Assessment_Manager_x32.exe** based on the operating system selected.

1. Download LT Auditor+ for Windows Assessment SP3 and extract the zip file.
2. On the manager machine, run Setup.exe to bring the following window.

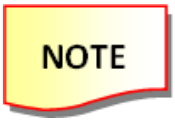


3. Click Yes to start the upgrade process, and the following screen will appear.

4. Click Next to start the upgrade process.



5. Click Finish to complete.



Prior versions of LT Auditor+ Windows Assessment scans did not have any prefix (AD_, FS_) in the name. If those files have been scheduled to run, please delete schedules and files and proceed to set up new scheduled scans.