Lepide

CONFIGURATION GUIDE

SHAREPOINT SERVER AUDITING

Table of Contents

1 Introduction

The Lepide Data Security Platform provides a comprehensive way to provide visibility across Active Directory, Group Policy, Exchange on-premises, M365, SharePoint, SQL Server, Windows File Server, NetApp Filer and every platform which can provide an integration with Syslogs and RestAPI.

This guide takes you through the process of standard configuration of the Lepide Data Security Platform for SharePoint. For information on installation, please see our Installation and Prerequisites Guide.

If you have any questions at any point in the process, you can contact our Support Team. The contact details are listed at the end of this document.

2 Requirements and Prerequisites

2.1 Prerequisites to Audit SharePoint

The following are the prerequisites to add a SharePoint Server (any version) for auditing

- Connectivity and accessibility to the instance of SQL Server, which is interlinked with SharePoint Server
- Microsoft System CLR Types for SQL Server2012
- Microsoft SQL Server 2012 ManagementObjects
- .NET Framework 4.6 should be installed on both the server to be monitored and the computer where software is installed.

NOTE: You can add a SharePoint Server in Lepide Data Security Platform for auditing only when you have installed Microsoft System CLR Types for SQL Server 2012 and Microsoft SQL Server 2012 Management Objects on the server computer running SharePoint. The setup files to install these two add-ons comes with the compressed setup file of the solution.

The required user rights to add SharePoint for auditing is listed in Section 3 Add a SharePoint Component.

2.1.1 Install Microsoft CLR Types on SP Server

Follow the steps below to install Microsoft System CLR Types for SQL Server 2012:

1. Go to the server and browse the folder of the computer where the Lepide Data Security Platform is installed.
2. Open the **Redist** folder, which has different folders. **x64** folder has the setup files for 64-bit Windows Server, and **x86** contains the files for 32-bit Windows Server OS.
3. Open the required folder.

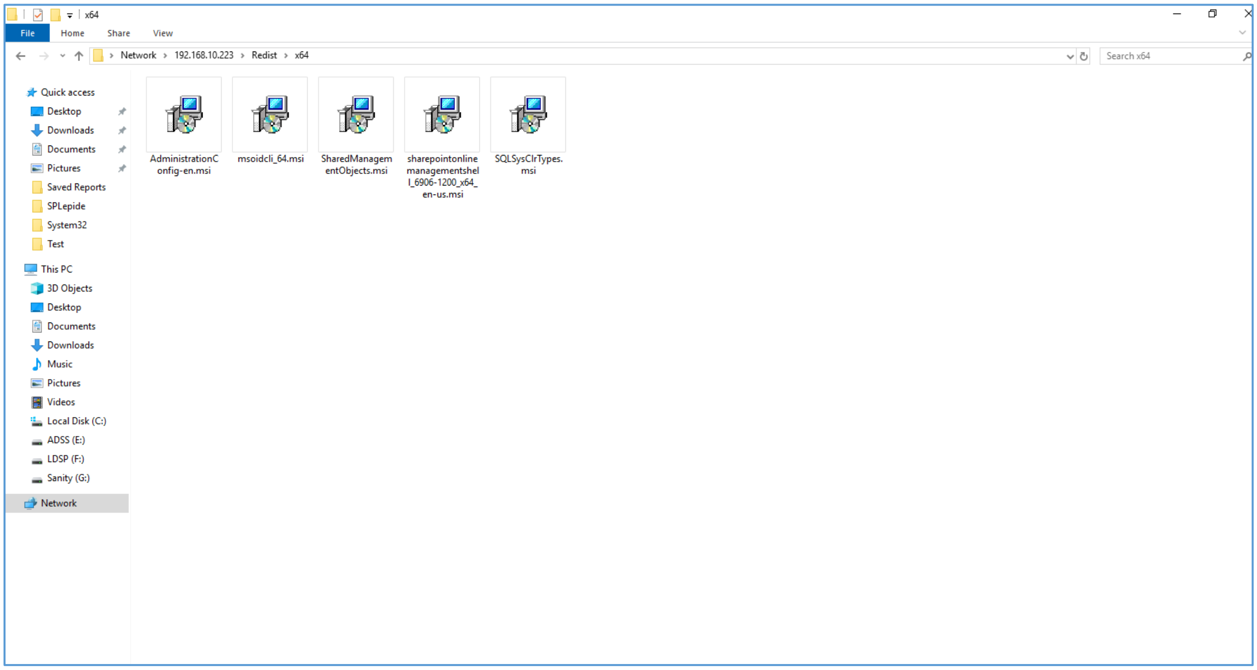


Figure 1: x64 Folder of Redist Folder

4. Copy these files to the SP Server and Run the setup file **SQLSysClrTypes.msi** to install Microsoft System CLR Types for SQL Server 2012.

   If you are running the setup file after copying it to the Local File System, then the warning message does not appear.
5. Click Run. It shows Windows Installer.
6. Once Windows Installer is initialized, it shows the installation wizard.
7. Click **Next**. The next step displays the license agreement of Microsoft Corporation.
8. Read the license agreement carefully. The license and terms to install Microsoft CLR Types will be between you and Microsoft. If you agree, then click I accept the terms in the license agreement.

9. Click **Next** to proceed. The module is now ready to be installed.
10. Click **Install** to start the installation.
11. Once Microsoft System CLR Types is installed, the successful message appears in the wizard.
12. Click **Finish** to complete the process and to close the wizard.

2.1.2 Install SQL Management Objects on SP Server

Follow the steps below to install Microsoft SQL Server 2012 Management Objects Setup.

1. Go to the server and browse the folder of the computer where the Lepide Data Security Platform is installed.
2. Open **Redist** folder, which contains two sub-folders. **x64** folder has the setup files for 64-bit Windows Server, and **x86** contains the files for 32-bit Windows Server OS.
3. Open the required folder
4. Copy the files to the SP Server and Run the setup file **SharedManagementObjects.msi** to install SQL Management Objects.
5. Click **Run**. It shows Windows Installer.
6. Once Windows Installer is initialized, it shows the installation wizard.
7. Click **Next**. The next step displays the license agreement of Microsoft Corporation.
8. Read the license agreement carefully. The license to install Microsoft SQL Server 2012 Management Objects will be between you and Microsoft. If you agree, then click **I accept the terms in the license agreement**.
9. Click **Next** to proceed. The module is now ready to be installed.
10. Click **Install** to start the installation.
11. Once SQL Management Objects is installed, the successful message appears in the Wizard.
12. Click **Finish** to complete the process and to close the wizard.
13. Close **Redist** folder.

2.2 Required User Rights

To install and work with the Lepide Data Security Platform, you need to have appropriate rights to the system where it will be installed. Also, you need to have appropriate rights to access Active Directory, Exchange Server, SQL Server and SharePoint Server.

2.2.1 Service Rights

To run the service of Lepide Data Security Platform after installation, you can select any of the following objects or users.

- A local system administrator
- A member of Domain Admins Group

2.2.2 Local System Rights

The user should have the following permissions on the local computer where the solution is installed:

- Full access permission on the drive where the Operating System is installed
- Read/Write permissions in the Registry

Follow the steps below to assign these permissions.

1. Go to Control Panel and select **User Accounts**.
2. Select the User and select **Change Account Type**.
3. Make user an **Administrator**.
4. Click **Save**.

NOTE:

1. Steps mentioned above may vary depending on the Windows version installed on thesystem.
2. If the User Account does not exist on the system, create a new User Account with Administrative rights.

2.2.3 Required SQL Server Rights for Audit Database

The provided user to create or access a database for auditing logs should have a login with the assigned role of **sysadmin** in SQL Server.

If you are using **Windows Authentication**, then a login for the currently logged on Windows user should exist in SQL Server. Perform the following steps.

1. If such a user login does not exist already, then follow the steps below to create it.
    a. Open SQL Server Management Studio.
    b. Select SQL or Windows Authentication.
    c. Enter the username and password of an SQL Server Administrator in the case of SQL authentication.
    d. Click **Connect**.
    e. In the left tree panel, go to **Security** → **Logins**.
    f. Right click on **Logins** and select **New Login**.
    g. **Login - New** wizard appears onscreen.
    h. Enter the same login name as that of currently logged-on user, with which you are running Lepide Data Security Platform.
    i. Switch to **Server Roles** and select **sysAdmin**.
    j. Click **OK.**
2. If the user exists, but no such rights are assigned, then follow these steps to assign the required rights.
    a. Open SQL Server Management Studio.
    b. Select SQL or Windows Authentication.
    c. Enter the username and password of an SQL Server Administrator in the case of SQL authentication.
    d. Click **Connect**.
    e. In the left tree panel, go to **Security** → **Logins**.
    f. Expand **Logins** and select the required user.
    g. Right-click on the user and select **Properties**.
    h. Switch to **Server Roles** and select **sysAdmin**.
    i. Click **OK.**
    j. Go to the Status page, select Grant and Enabled.
    k. Click **OK**.

2.3 Required Ports

The software uses the following ports for different purposes:

1. Lepide Data Security Platform uses the following ports for communication:
   a. Port 389 and Port 636 for LDAP queries.
   b. Port 445 for RPCSS (Remote Procedure Call Services)
   c. Port 135 for communication to Event Logs
   d. TCP/5985 (HTTP) and TCP/5986(HTTPS) for Remote PowerShell Communication
   e. Default Port for SQL Server Communication. In most cases, the default port for SQL is 1433.

2. The Solution uses the following Microsoft functions, which uses different ports:
   a. OpenEventLog, which uses Port 445 and Port 135
   b. ReadEventLogt, which uses Port 445 and Port 135
   c. AdsOpenObject, which uses Port 389 and Port 636
3. Lepide Data Security Platform Web Console uses Port 7778 (HTTP). You can change the Port Number.
4. Lepide Data Security Platform App uses Port 1051.

3 Add a SharePoint Component

Before going ahead, make sure that the prerequisites to add SharePoint Server are met. To find out more about prerequisites, refer to Section 2.1 Prerequisites to Audit SharePoint

To add a SharePoint Component

From the **Add Component** section of the Component Management window, click on the icon which says **SharePoint Server** to add this component to the solution.

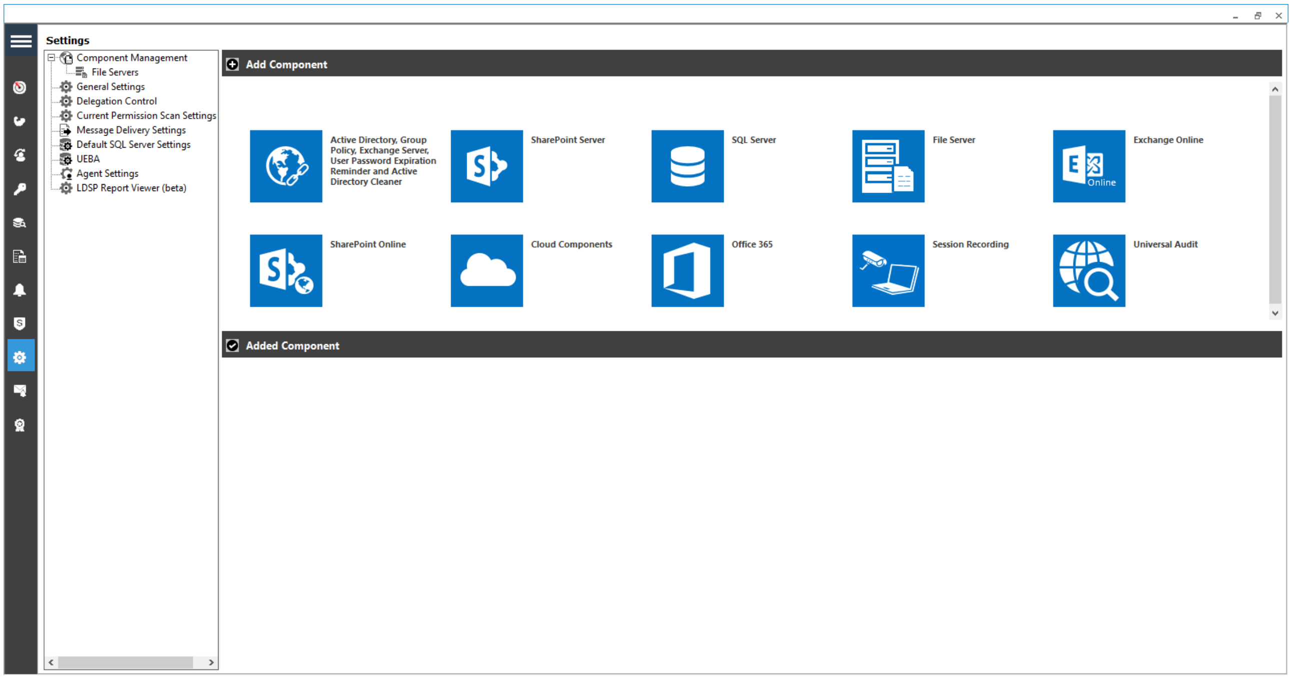
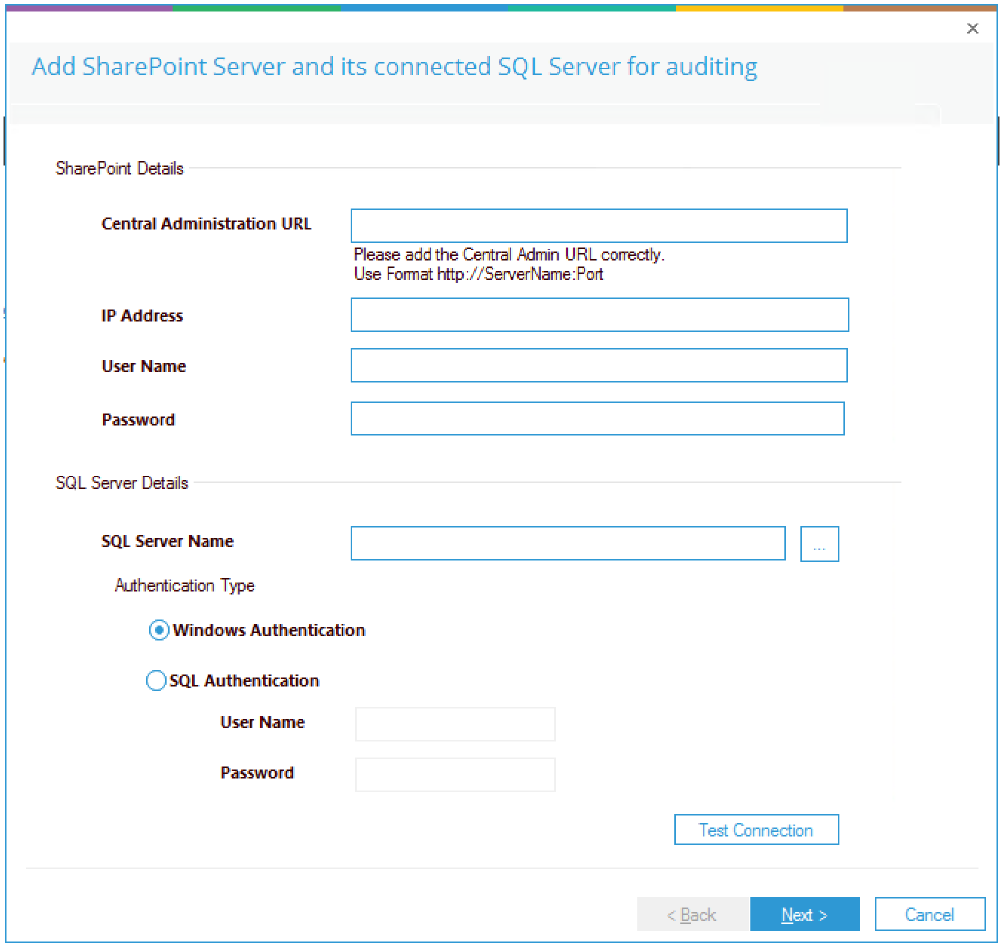


Figure 2: Component Management Window

The **Add SharePoint Server** wizard will start:



Add SharePoint Server and its connected SQL Server for auditing

SharePoint Details

Central Administration URL

Please add the Central Admin URL correctly.
Use Format http://ServerName:Port

IP Address

User Name

Password

SQL Server Details

SQL Server Name

Authentication Type

● Windows Authentication

○ SQL Authentication

User Name

Password

Figure 3: Add SharePoint Server

3.1 SharePoint Server Details

1. This step has two sections:

   a) SharePoint Details: In the SharePoint Details section, you will need to provide **Central Administration URL, IP Address, User Name and Password.**

      Provide the username in this format - **Domain\User** or **Workgroup\User**.

The following note gives further information about required user rights:

NOTE:

Required User Rights in Active Directory

The selected user should be a member of Administrators and Domain Admins group. Moreover, the user with which you are logged on to the computer running SharePoint and Auditing Agent, should be a member of Domain Admins group.

If the user is not having these rights, follow the given steps to assign the rights:

1. Go to Administrative Tools.
2. Open Active Directory Users and Computers.
3. Select User Properties.
4. Click Member Of.
5. Click Add Group.
6. Select the following Groups:
    a. Administrators
    b. Domain Admins
7. Click Apply and OK.

Required User Rights in SharePoint

1. The selected user should be a member of Farm Administrator Group in SharePoint. Perform the following steps to add the user in Farm Administrator Group.
    a. Go to Central Administration → Security.
    b. Click Manage the farm administrators group link under Users.
    c. Check if the selected user is already added in the Farm Administrator Group or not.
    d. If the selected user is not listed here, click New .
    e. In Share 'Central Administration' pop-up, type the username. Once typed, SharePoint Server will recognize the name and show a list.
    f. Select the username in the appeared list.
    g. Click Share to add the user in Farm Administrator group.

1. The selected user must have the administrative rights over each Site Collection to be audited. For this, the user either should be the Site Collection Administrator or should have full control over the Web App.

   a. Perform the following steps to add the user in Site Collection Administrators:

      i. Open the Site Collection in the Web Browser, for which you need to enable the auditing.

      ii. Click **Settings** icon on the top right corner and click **Site Settings**.

      iii. In Site Settings, click Site Collection Administrators under Users and Permissions.

      iv. Check whether the selected user is listed as **Site Collection Administrator** or not.

      v. If it is not listed, add the user.

   If you want to enable the auditing of new sites that will be created in future, add the selected user as Primary or Secondary Site Collection Administrator while creating a new site.

   b. Perform the following steps to assign the Full Control over Web App:

      i. Go to Central Administration → Application Management → Manage Web Applications

      ii. Select the required Web Application.

      iii. Click **User Policy** button on the ribbon.

      iv. Select **All Zones** and click **Next**

      v. Select Full Control - Has full control and click Next

      vi. Click **Finish** to complete the process.

   Once these rights are assigned, the user attains the administrative rights over each Site Collection in the Web App.

Required User Rights in Local Security Policy

The selected user should be added in the security right of **Log on as a service** in Local Security Policy. If the user does not have this right, then follow the steps below on the Server computer, where SharePoint Server is installed, to assign the same.

1. Go to Administrative Tools → Local Security Policy.
2. In the left panel, go to **Security Settings** → **Local Policies** → **User Rights Assignment**. It displays the different policies in the right panel.
3. Select **Log on as a service** and double click on it to access its properties.
4. Make sure that the selected user is listed in **Local Security Setting** tab of **Properties** window.
5. If the selected user is not added, then click **Add User or Group** button. It shows **Select Object** dialog

Required User Rights in SP SQL Server

A login of the selected SharePoint User with Windows Authentication and sysadmin role should exist in SQL Server for SharePoint Content Database.

Case 1: If the user login does not exist already, then follow the steps below to create it.

1. Open **SQL Server Management Studio**.
2. Select SQL or Windows Authentication.
3. Enter the name and password of an SQL Administrator in case of SQL Authentication.
4. Click **Connect**.
5. In the left tree panel, go to **Security → Logins**.
6. Right click on **Logins** and select **New Login**.
7. **Login – New** wizard appears onscreen.
8. Enter the same login name as that of SharePoint user with which you are adding SharePoint Server for auditing.
9. Switch to **Server Roles**.
10. Select both **sysAdmin** and **dbcreator** roles.
11. Click **OK**.

Case 2: If the user exists, but no such rights are assigned, then follow these steps to assign the required rights:

1. Open **SQL Server Management Studio**.
2. Select SQL or Windows Authentication.
3. Enter the name and password of an SQL Server Administrator in case of SQL Authentication.
4. Click **Connect**.
5. In the left tree panel, go to **Security → Logins**.
6. Expand **Logins** and select the required user.
7. Right click on the user and select **Properties**.
8. Switch to **Server Roles**.
9. Select both **sysAdmin** and **dbcreator** roles.
10. Click **OK**.

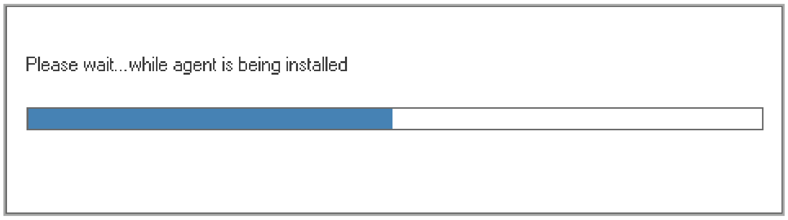
b) **SQL Server Details:** Enter the SQL Server Name manually or click the ... icon to enumerate all local and remote SQL Servers and select one from the list.

Select the authentication type and provide the credentials for the user.

1. Click the **Test Connection** button to check for a successful connection to SQL Server.
2. Click **Next**.

3.2 Install SharePoint Auditing Agent

3. The Solution starts installing the agent on SharePoint Server for auditing.

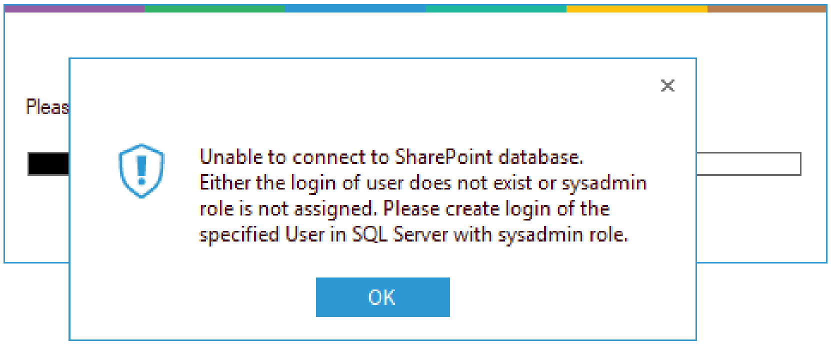


Please wait...while agent is being installed

Figure 4: Installing Agent on SharePoint Server

NOTE: You may receive an error at this stage if you have not installed Microsoft System CLR Types for SQL Server 2012 and Microsoft SQL Server 2012 Management Objects Setup at the server. Install them both from the Redist folder of program installation folder.

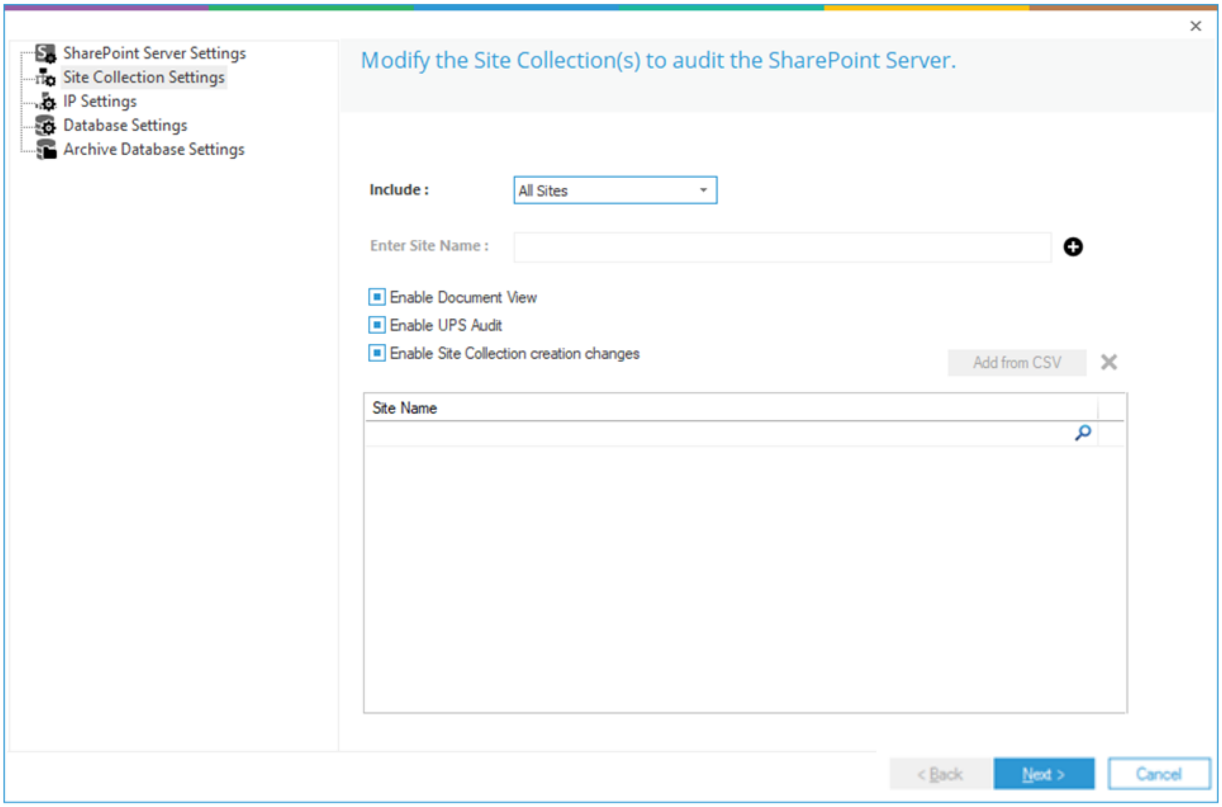
NOTE: If the following error appears on screen while trying to connect to SharePoint, then it means either the login of SharePoint user does not exist, or the sysadmin role is not assigned to it.



Unable to connect to SharePoint database.
Either the login of user does not exist or sysadmin role is not assigned. Please create login of the specified User in SQL Server with sysadmin role.

Figure 5: Error in Connecting to SharePoint

3.3 Site Collection Settings



Modify the Site Collection(s) to audit the SharePoint Server.

Include : All Sites

Enter Site Name :

■ Enable Document View

■ Enable UPS Audit

■ Enable Site Collection creation changes

Figure 6: Site Collection Settings

4. In this dialog box, the list of all Sites on SharePoint is displayed. You can select the sites that you want to audit.
5. **Include**: this drop-down menu has the following options:
    a. **All**: Select this option if you want to audit all Site Collection(s).
    b. **Exclude**: Select this option if you want to audit all except the selected Site Collection(s).
    c. **Include**: Select this option if you want to audit the selected Site Collections.

Follow the steps below to choose the site name(s)**:**

a. Selecting the include or exclude option enables you to select the sites for auditing.

b. To add the site name directly, click the ⊕ icon and type the name into the Site Name box.

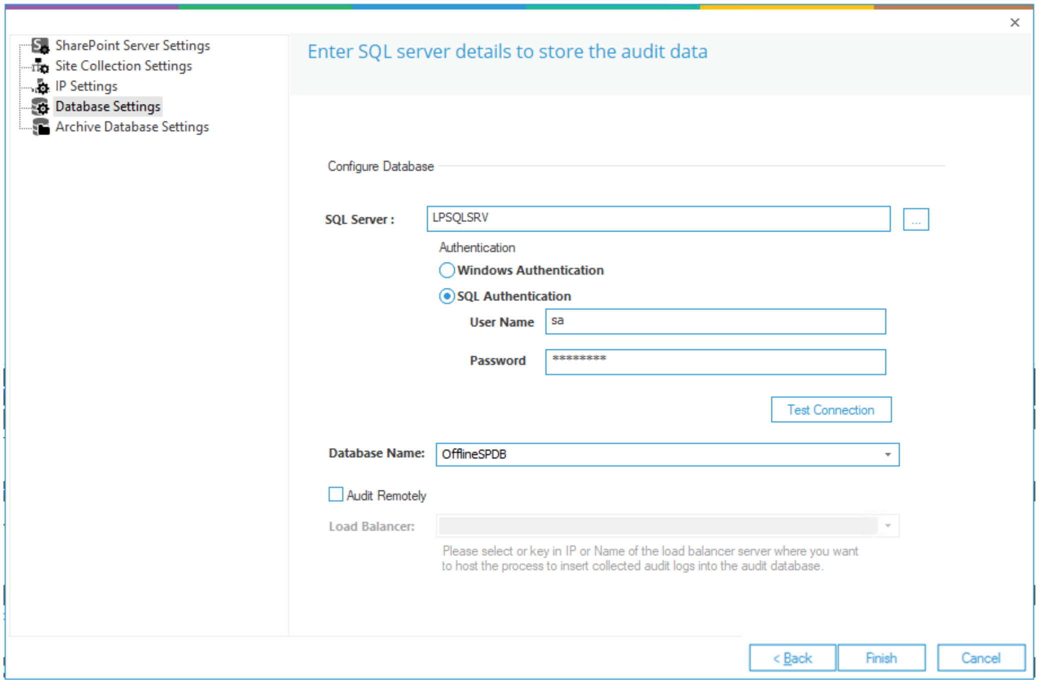
c. Click the ⊕ icon and check the boxes of the sites to **Include** or **Exclude** depending on the option selected in the drop-down box

6. To reduce the number of collections returned you can uncheck one or more of the following boxes:
   Enable document View
   Enable UPS Audit
   Enable Site Collection creation changes
7. To add from a CSV file, click **Add from CSV** and choose the CSV file from the list
8. Click **Next**.

The Database Settings dialog box is displayed.

3.3.1 Database Settings

In this step, you need to provide the details of SQL Server and database that will be used to store the audit data. The solution lets you connect both to a locally hosted or a networked SQL Server.



Enter SQL server details to store the audit data

Configure Database

SQL Server : LPSQLSRV

Authentication
○ Windows Authentication
● SQL Authentication
User Name sa
Password ********

Database Name: OfflineSPDB

□ Audit Remotely

Load Balancer:

Please select or key in IP or Name of the load balancer server where you want to host the process to insert collected audit logs into the audit database.

Figure 7: Database Settings

Enter the SQL Server name manually or click the … button to show all SQL Servers on the network

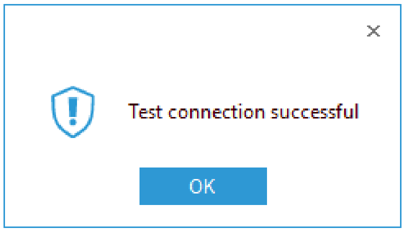
Provide the SQL Server username and password to allow the solution to access SQL using these credentials.

> **NOTE**: Here, the selected user should have **dbcreator** role in SQL Server.

You must test the connection between the solution and the selected SQL Server. This helps to authenticate the database connection.

- Click **Test Connection**.

It displays either an error if failed to connect or the following message confirming the successful connection.



Test connection successful

Figure 8: Test Connection is Successful

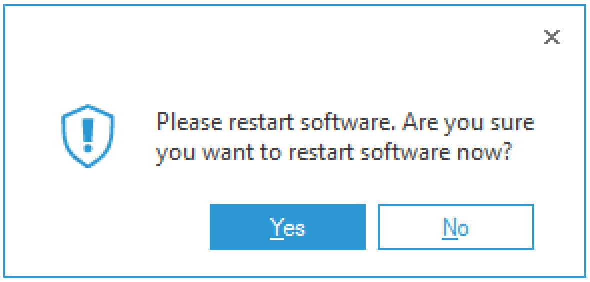
Provide the database name where the Lepide Data Security Platform will store the auditing logs.

> NOTE: Lepide Data Security Platform connects to a database created by the solution itself. The solution alerts when you try to use an existing database.

If you are using the solution for the first time, you can provide a name for the new database that will be created with the solution. In the case of reinstallation, you can use a database created earlier by the solution.

Audit Remotely: Selecting this checkbox allows you to specify a server to host the process to insert the collected audit logs into the audit database.

Click **Finish**



Please restart software. Are you sure you want to restart software now?

Figure 9: Asking to Restart the Solution

4 Support

If you are facing any issues whilst installing, configuring, or using the solution, you can connect with our team using the contact information below.

Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

5 Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.