Lepide

CONFIGURATION GUIDE

MICROSOFT SQL SERVER

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 Microsoft SQL Servers.

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. Basic System Requirements

- Required Processor
  - Minimum dual-core processor
  - Recommended quad-core processor
- Required RAM
  - Minimum 4 GB RAM
  - Recommended 8 GB RAM
- Required free disk space
  - Minimum 1 GB
  - Recommended 2 GB
- Any of the following 32-bit or 64-bit Windows Operating Systems.
  - Windows Server OS: Any Server above and including 2008 R2
- Any of the following SQL Servers (local or network hosted) for storing auditing logs:
  - Any SQL Server above and including SQL Server 2005 (standard or enterprise)
- .NET Framework 4.6 or later

2.2. Supported Servers for Auditing

Audited Servers	Supported Versions
Microsoft SQL Servers	• Microsoft SQL Server 2005 and above (Standard or Enterprise)

2.3. 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 the SQL server.

To configure the Lepide Data Security Platform for auditing Microsoft SQL Server, the service account requires the following rights:

- Member of Domain Admins Group in Active Directory.
- This account should have Sysadm rights over the SQL databases. An SQL account with the mentioned privileges can also be used.

2.4. Required SQL Server Rights

- **For Windows Authentication:** A login for the currently logged on Windows User should exist in SQL Server with the assigned role of **dbcreator** in SQL server.
- **For SQL Authentication**: A local SQL account with **dbcreator** permission.

2.5. Required Ports

NOTE: For using SQL authentication, the SQL server should be set to mixed authentication mode..

The software uses the following ports for different purposes.

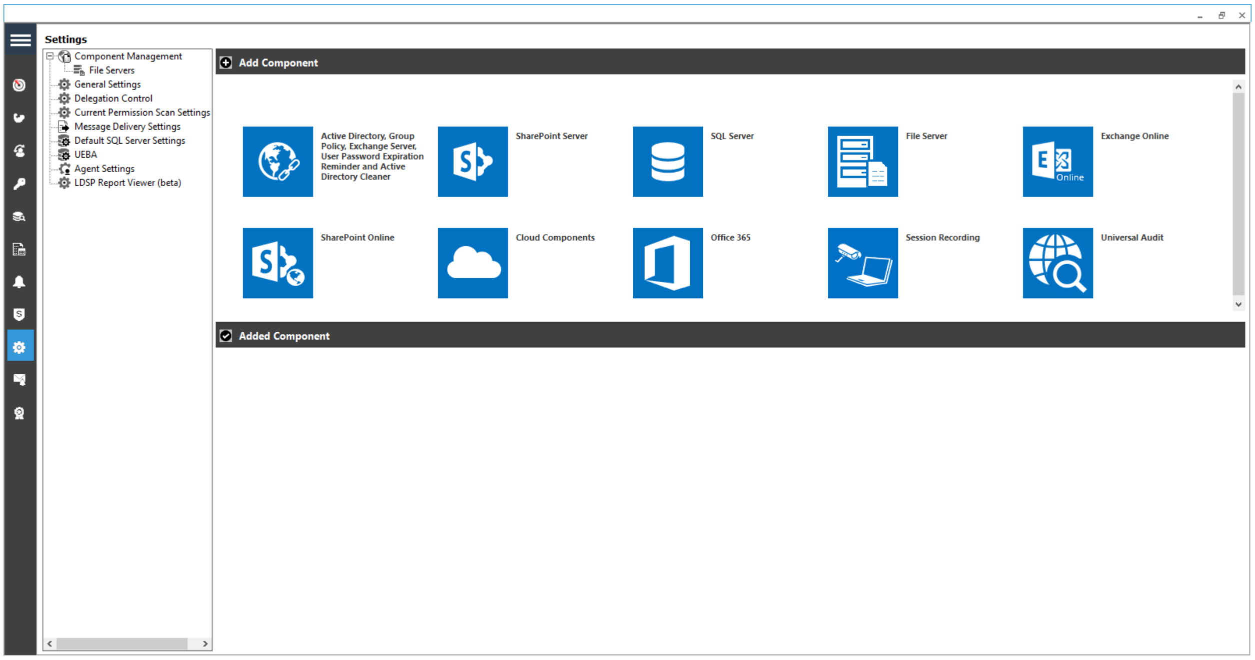
1. Lepide Data Security Platform uses the following ports for communication:
    a. Port 389 and Port 636 for LDAP queries.
    b. Port 135 for WMI (Windows Management Instrumentation)

   c. Default Port for SQL Server Communication. In most cases, the default port for SQL is 1433.

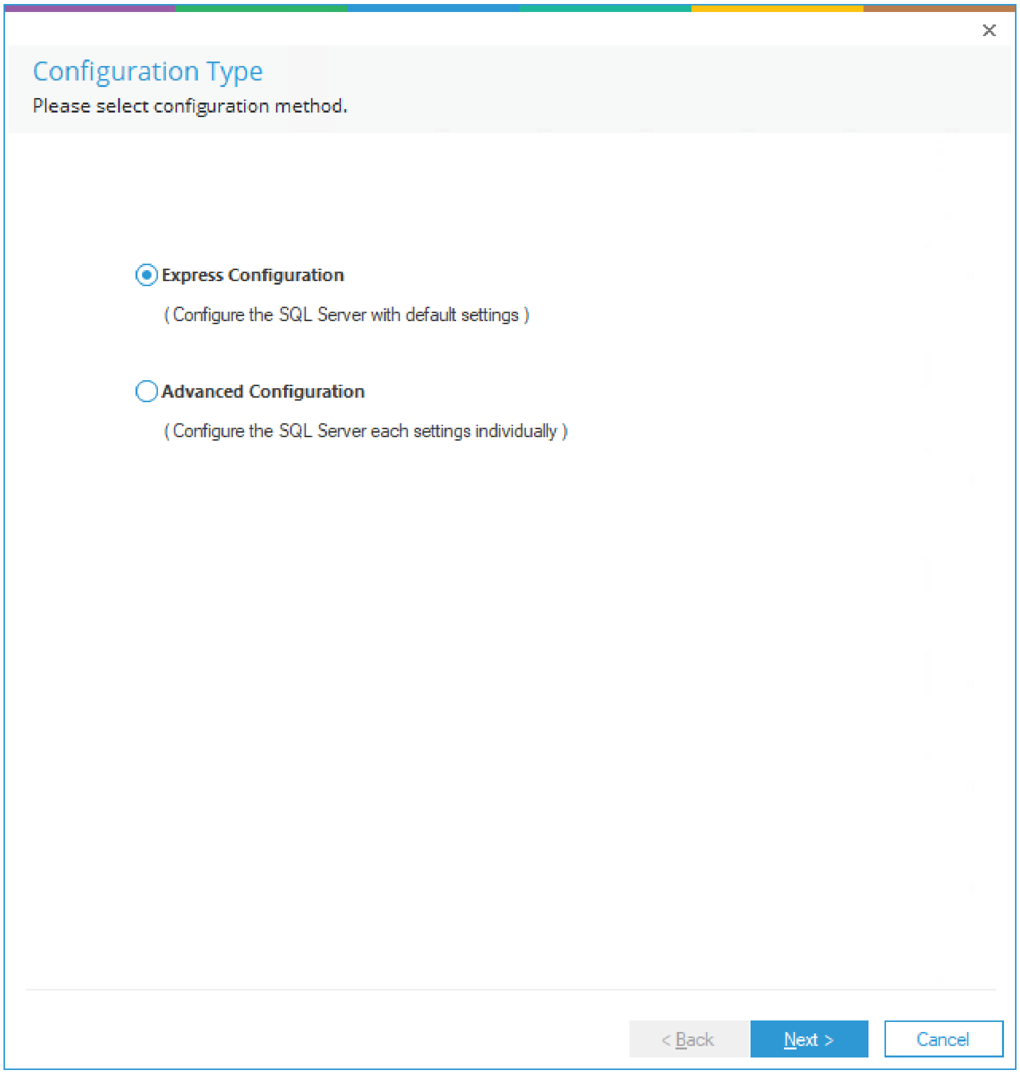
2. Lepide Data Security Platform Web Console uses Port 7779 (HTTP).
3. Lepide Data Security Platform App uses Port 1051.

3. Add SQL Server

To add a Microsoft SQL Server, you need to perform the following steps:



- Select the **SQL Server** option in **Component Selection** dialog box



Configuration Type

Please select configuration method.

● Express Configuration

(Configure the SQL Server with default settings)

○ Advanced Configuration

(Configure the SQL Server each settings individually)

Figure 1: Add SQL Server Wizard

The solution offers two different ways to add SQL Server.

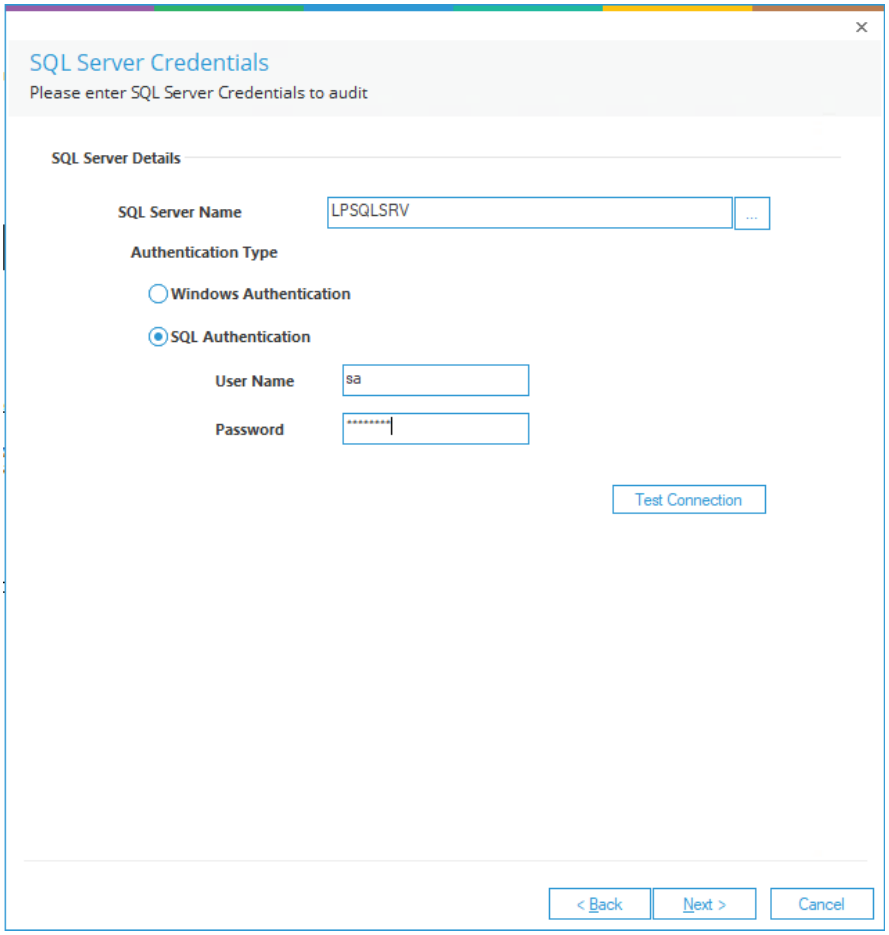
- Express Configuration: Add SQL Server with minimum recommended settings.
- Advanced Configuration: Add SQL Server with the advanced settings to customize the auditing.

3.1. Add SQL Server with Express Configuration

Perform the below steps at the **Add SQL Server** wizard:

1. Select **Express Configuration** at the wizard.
2. Click **Next**. It asks you to provide the details of SQL Server to be added.

3.1.1.SQL Server Details



SQL Server Credentials

Please enter SQL Server Credentials to audit

SQL Server Details

SQL Server Name: LPSQLSRV

Authentication Type

○ Windows Authentication

● SQL Authentication

User Name: sa

Password: ********

Figure 2: Asking for SQL Server Details

3. The solution lets you add a local or networked SQL Server. You can enter the name of SQL Server manually in the text box. Alternatively, you can click the … icon to enumerate all SQL Servers in a list, from which you can select the required server.
4. You need to select either Windows Authentication or SQL Server Authentication. We recommend that you select the latter option.
5. Enter the name and password of a SQL Server user.

NOTE: The selected user should be assigned the role of sysadmin in SQL Server. If you are using a local system administrator or domain administrator to run Lepide Data Security Platform Service, then its login with Windows Authentication and sysAdmin role should exist in SQL Server.

6. Click **Next** to proceed. The next step shows **Database Settings**.

3.1.2. Database Settings

Perform the following steps to configure the database settings.

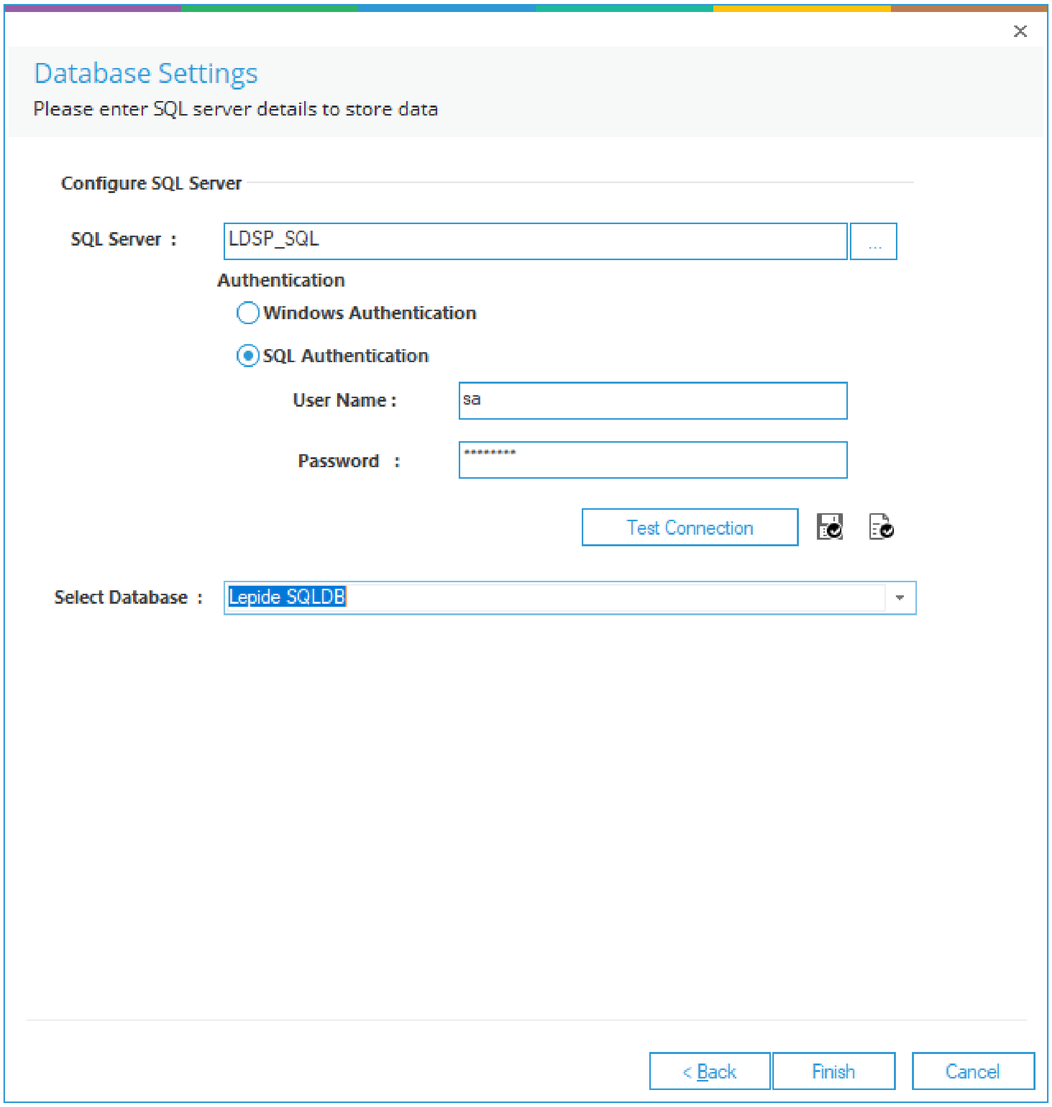
7. Enter the name of an SQL Server. You can also click … icon to enumerate the list of all SQL Servers, from which you can select the desired one.
8. Select the authentication type, preferably **SQL Authentication**.
9. Enter the login credentials of an SQL administrative user.

NOTE: Here, the selected user should have **dbcreator** role in SQL Server, where the audit data must be stored.

10. Enter the name of the database in which the auditing logs will be stored. Following screenshot displays the sample details.

NOTE: Click the 💾 icon to save the current SQL Server Settings as default in **Default SQL Server Settings**.

11. Click **Test** Connection to test the connection to SQL Server.



Database Settings

Please enter SQL server details to store data

Configure SQL Server

SQL Server : LDSP_SQL

Authentication

○ Windows Authentication

● SQL Authentication

User Name : sa

Password : ********

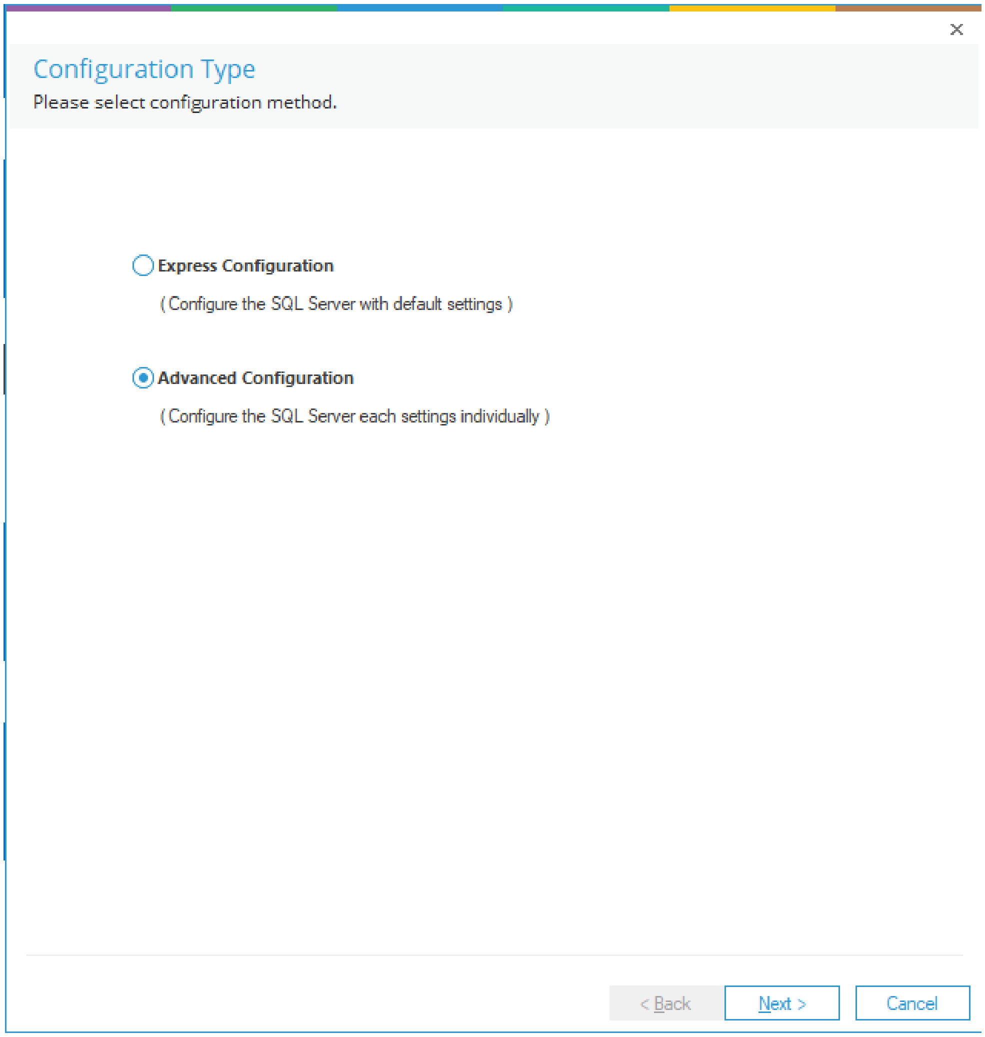
Select Database : Lepide SQLDB

Figure 3: Database Settings

12. Click **Finish**.

3.2. Add SQL Server with Advanced Configuration

1. In the following wizard, you need to select the **Advanced Configuration** option.



Configuration Type

Please select configuration method.

○ Express Configuration

(Configure the SQL Server with default settings)

● Advanced Configuration

(Configure the SQL Server each settings individually)

Figure 4: Adding SQL Server with Advanced Configuration

13. Click **Next**.

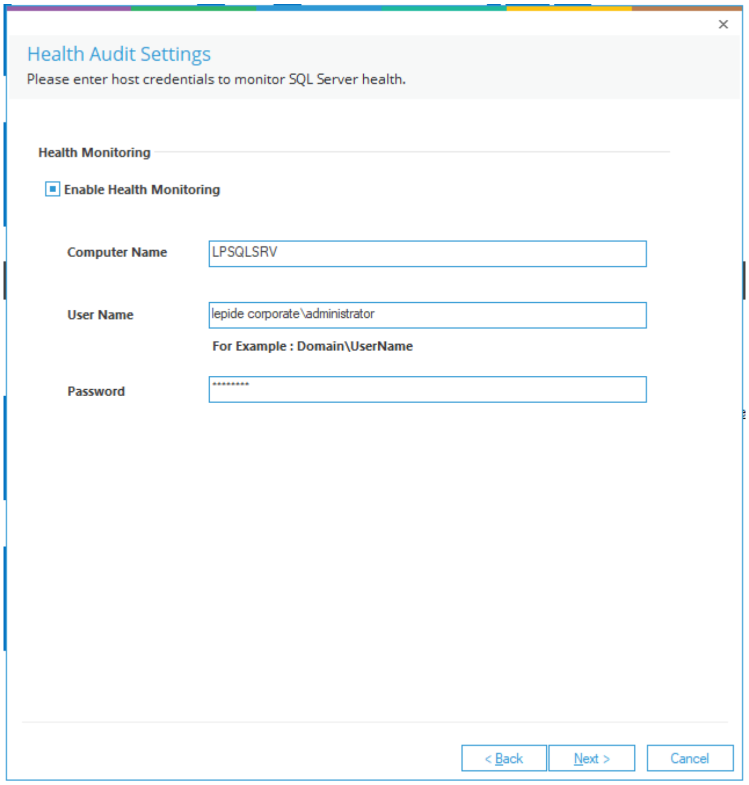
    The following steps are the same as when adding SQL Server using Express Configuration and have previously been discussed in this guide. Click the following links to return to these topics:

    - Section 3.1.1 SQL Server Details
    - Section 3.1.2 Database Settings

    The remaining steps are discussed in detail as follows:

3.2.1.SQL Health Monitoring

14. The next step displays the SQL Server Health Monitoring Settings.



Health Audit Settings

Please enter host credentials to monitor SQL Server health.

Health Monitoring

☑ Enable Health Monitoring

Computer Name: LPSQLSRV

User Name: lepide corporate\administrator

For Example : Domain\UserName

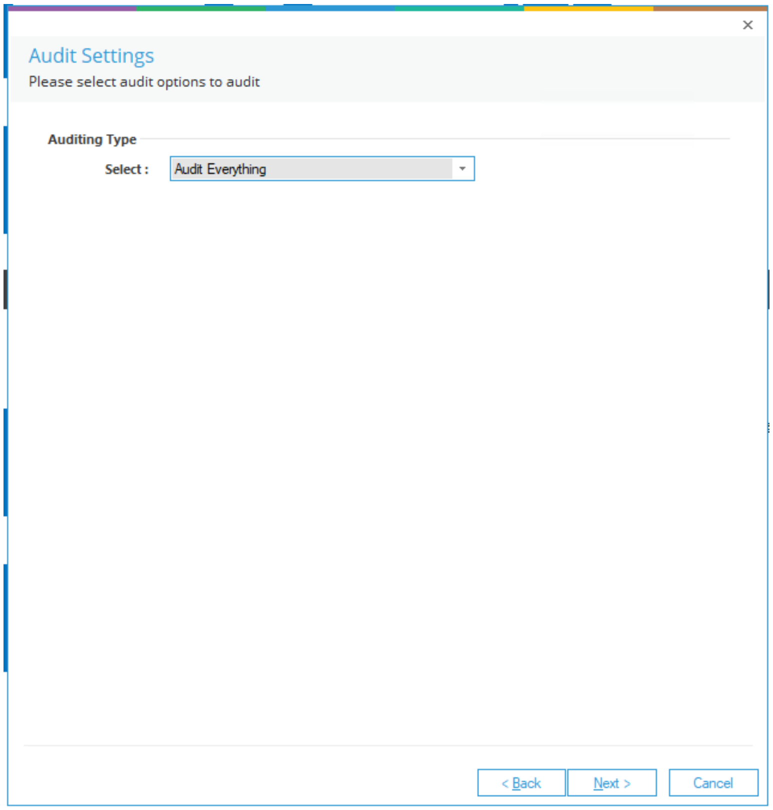
Password: ********

Figure 5: SQL Server Health Monitoring Settings

15. Check the box **Enable Health Monitoring** to enable the health monitoring of SQL Server. You must provide the following details of the computer where SQL Server is installed.
    a. **Computer Name:** Enter the name or IP Address of the computer where SQL Server is installed.
    b. **User Name:** Provide the **name** of an administrator user of that computer (It can be the domain admin user as well).
    c. **Password**: Enter the password for the above user.
16. Click **Next** to proceed.

The next step displays **Audit Settings**.

3.2.2.Audit Settings



Audit Settings

Please select audit options to audit

Auditing Type

Select : Audit Everything

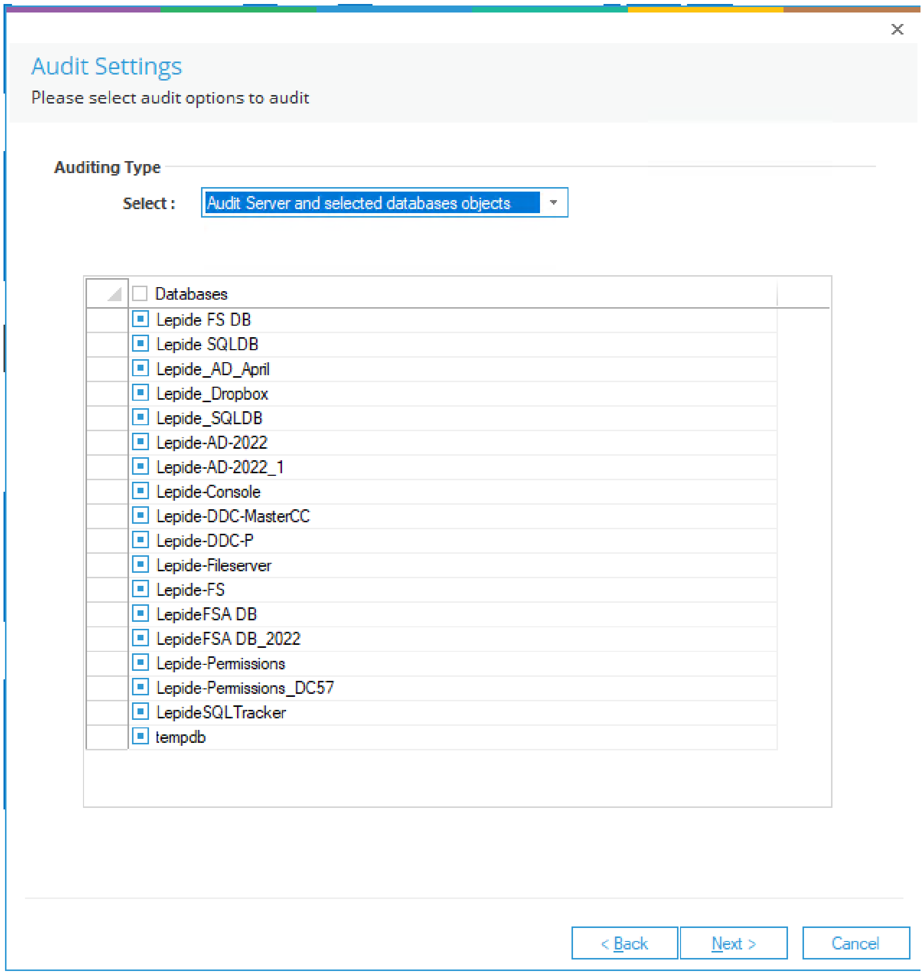
Figure 6: Audit Settings

17. Here, you need to specify the auditing type. The following options are available:

    a. **Audit Everything**: Everything at SQL Server including **all** server objects and databases will beaudited.

    b. **Audit Server**: Only Server objects will be audited, whereas databases will not beaudited.

    c. **Audit Server with Selected Databases:** All server objects and only selected database objects will be audited. If you select this option, then you must select which databases you want to audit.



Audit Settings

Please select audit options to audit

Auditing Type

Select : Audit Server and selected databases objects

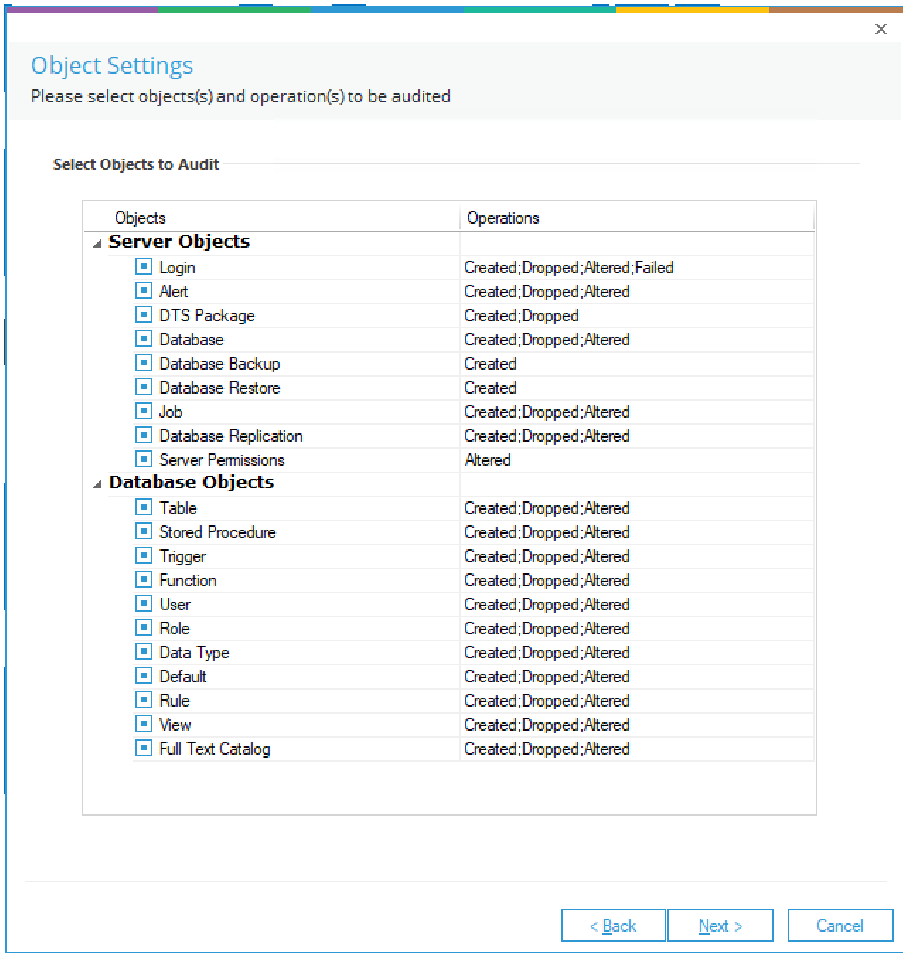
□ Databases
- ▣ Lepide FS DB
- ▣ Lepide SQLDB
- ▣ Lepide_AD_April
- ▣ Lepide_Dropbox
- ▣ Lepide_SQLDB
- ▣ Lepide-AD-2022
- ▣ Lepide-AD-2022_1
- ▣ Lepide-Console
- ▣ Lepide-DDC-MasterCC
- ▣ Lepide-DDC-P
- ▣ Lepide-Fileserver
- ▣ Lepide-FS
- ▣ LepideFSA DB
- ▣ LepideFSA DB_2022
- ▣ Lepide-Permissions
- ▣ Lepide-Permissions_DC57
- ▣ LepideSQLTracker
- ▣ tempdb

Figure 7: Listing all Databases to Audit

18. Check the boxes for the databases to be audited. Unchecked databases will not be audited or monitored. Click **Next**

    The next step is **Object Settings**.

3.2.3.Object Settings



Object Settings

Please select objects(s) and operation(s) to be audited

Select Objects to Audit

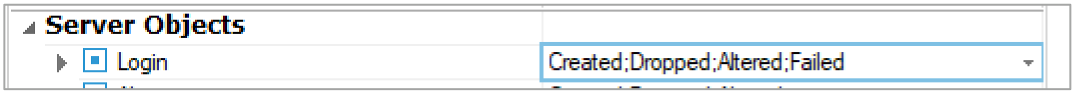
Objects	Operations
Server Objects	
▣ Login	Created;Dropped;Altered;Failed
▣ Alert	Created;Dropped;Altered
▣ DTS Package	Created;Dropped
▣ Database	Created;Dropped;Altered
▣ Database Backup	Created
▣ Database Restore	Created
▣ Job	Created;Dropped;Altered
▣ Database Replication	Created;Dropped;Altered
▣ Server Permissions	Altered
Database Objects	
▣ Table	Created;Dropped;Altered
▣ Stored Procedure	Created;Dropped;Altered
▣ Trigger	Created;Dropped;Altered
▣ Function	Created;Dropped;Altered
▣ User	Created;Dropped;Altered
▣ Role	Created;Dropped;Altered
▣ Data Type	Created;Dropped;Altered
▣ Default	Created;Dropped;Altered
▣ Rule	Created;Dropped;Altered
▣ View	Created;Dropped;Altered
▣ Full Text Catalog	Created;Dropped;Altered

Figure 8: Object Settings

19. In this step, you can specify the server objects, database objects, and operations for auditing. You can check the box for the object that has to be monitored. Also, you can click the operation list for an object to select which operations have to be included in or excluded from auditing.

    Follow the steps below to select the operations for an object.

- Select an operation cell for an object either server or database.

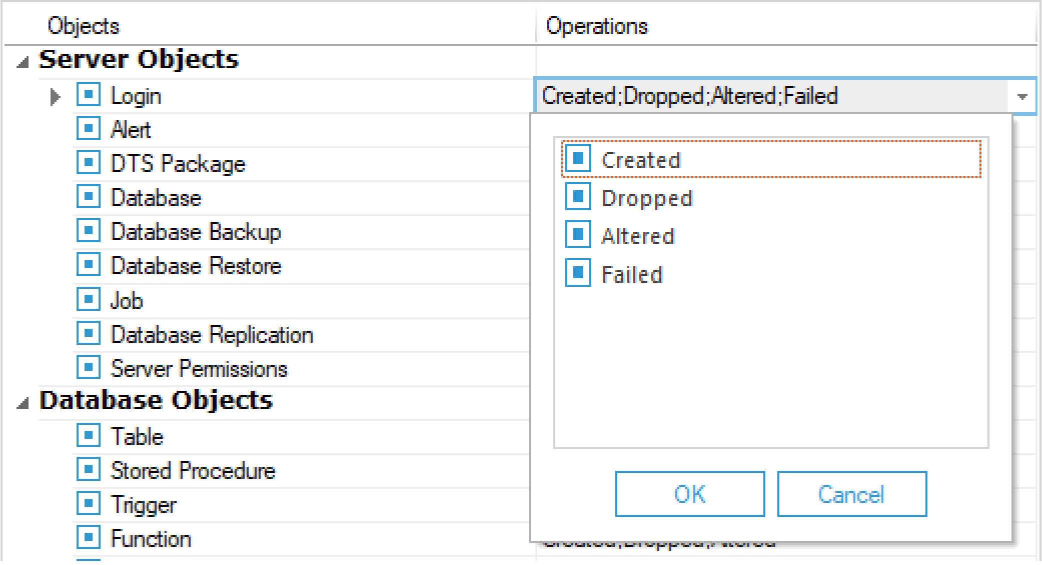


Server Objects

Objects	Operations
■ Login	Created;Dropped;Altered;Failed

Figure 9: Enabled Operations for an Object

- It will show ▾ arrow. Click the down arrow to access the list of operations.

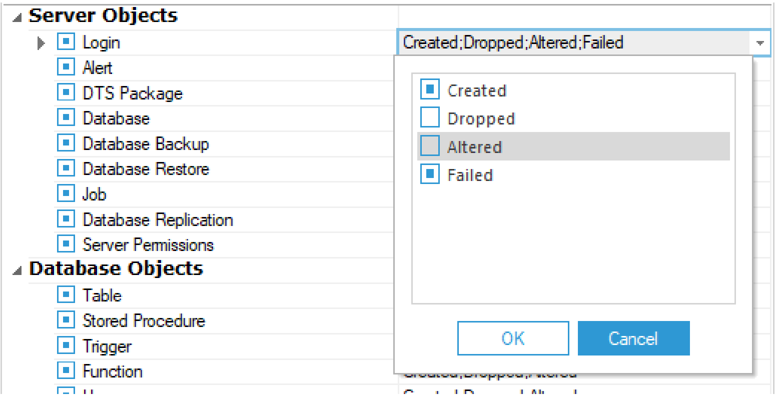


Objects	Operations
Server Objects	
■ Login	Created;Dropped;Altered;Failed
■ Alert	
■ DTS Package	
■ Database	
■ Database Backup	
■ Database Restore	
■ Job	
■ Database Replication	
■ Server Permissions	
Database Objects	
■ Table	
■ Stored Procedure	
■ Trigger	
■ Function	

■ Created
■ Dropped
■ Altered
■ Failed

Figure 10: Listing all Operations for an Object

- Uncheck the operations that you do not want to audit.



Server Objects

- ☑ Login: Created;Dropped;Altered;Failed
- ☑ Alert
- ☑ DTS Package
- ☑ Database
- ☑ Database Backup
- ☑ Database Restore
- ☑ Job
- ☑ Database Replication
- ☑ Server Permissions

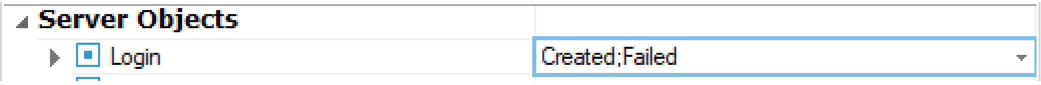
Database Objects

- ☑ Table
- ☑ Stored Procedure
- ☑ Trigger
- ☑ Function

☑ Created
□ Dropped
□ Altered
☑ Failed

Figure 11: Modifying the Selection of Operations

- Click **OK** to modify the selection of operations for **Login** object.



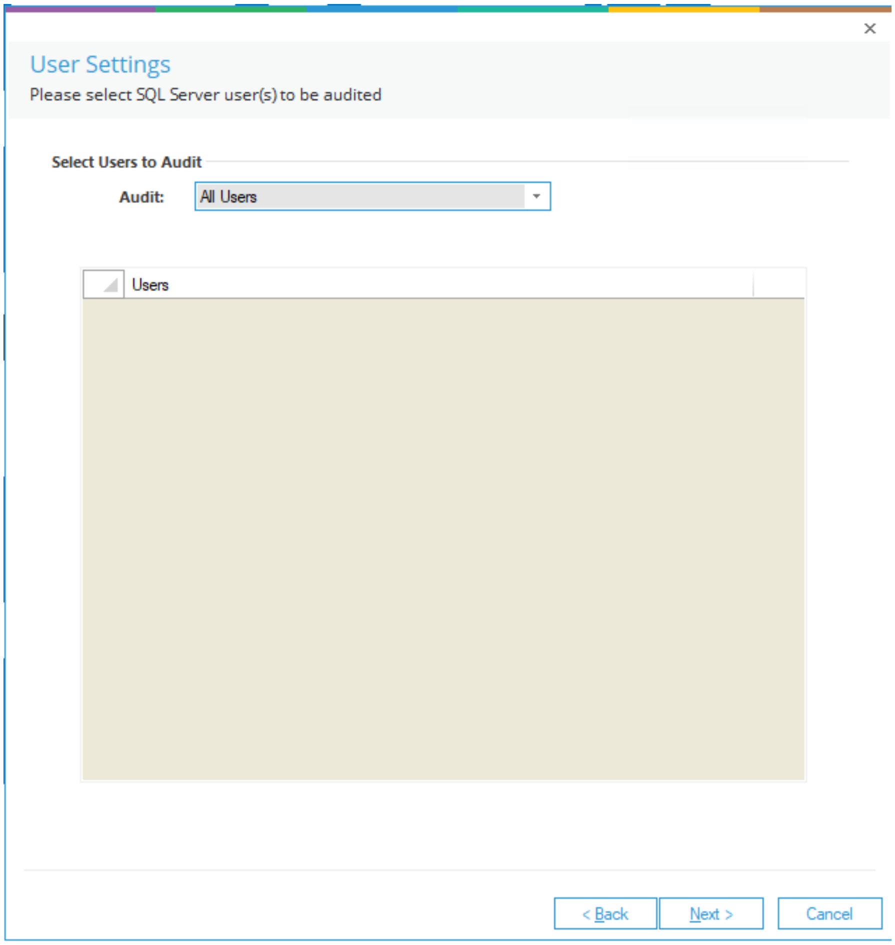
Server Objects

- ☑ Login: Created;Failed

Figure 12: Selected Different Operations

- Click **Next** . The next page displays **User Settings**.

3.2.4.User Settings


User Settings

Please select SQL Server user(s) to be audited

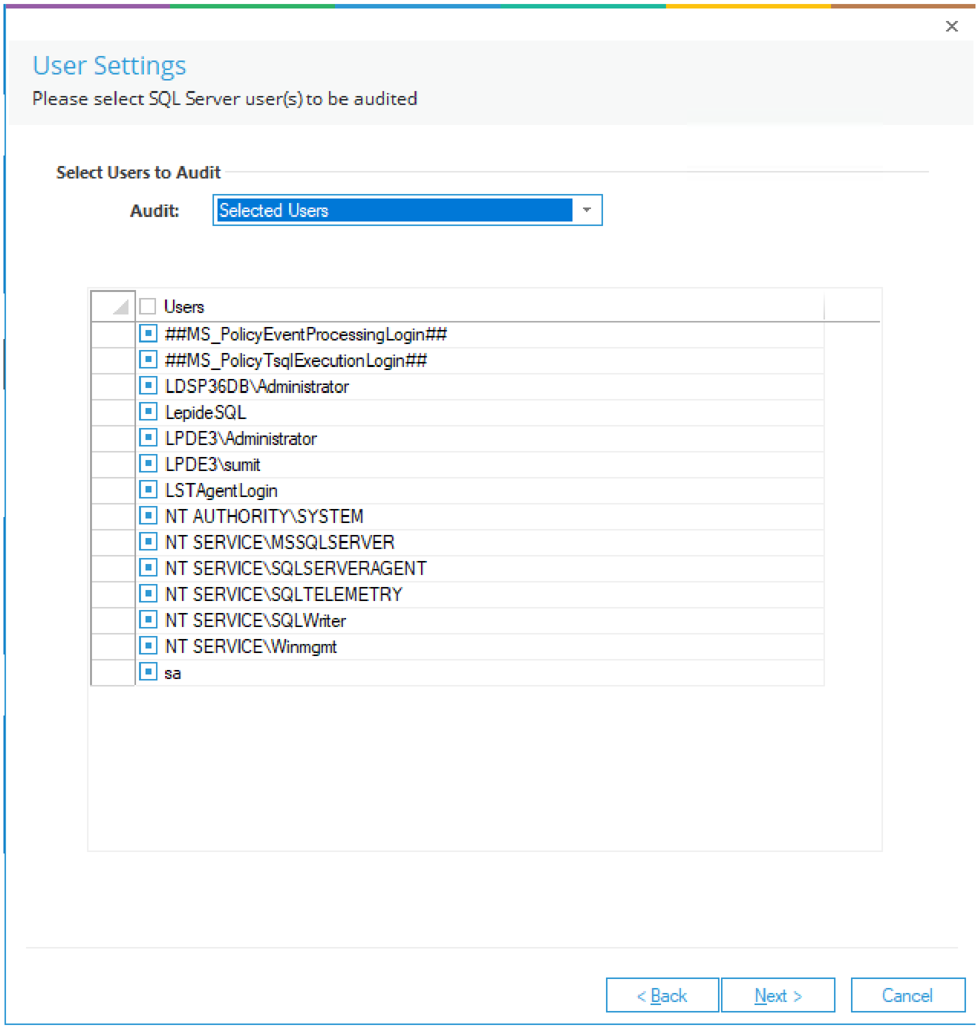
Select Users to Audit

Audit: All Users

Figure 13: User Settings

User Settings has the following options.

- Audit All Users: Select this option to audit all users.
- Audit Selected Users: Select this option to enable the **Users** section and enumerate all SQL users in it.



User Settings

Please select SQL Server user(s) to be audited

Select Users to Audit

Audit: Selected Users

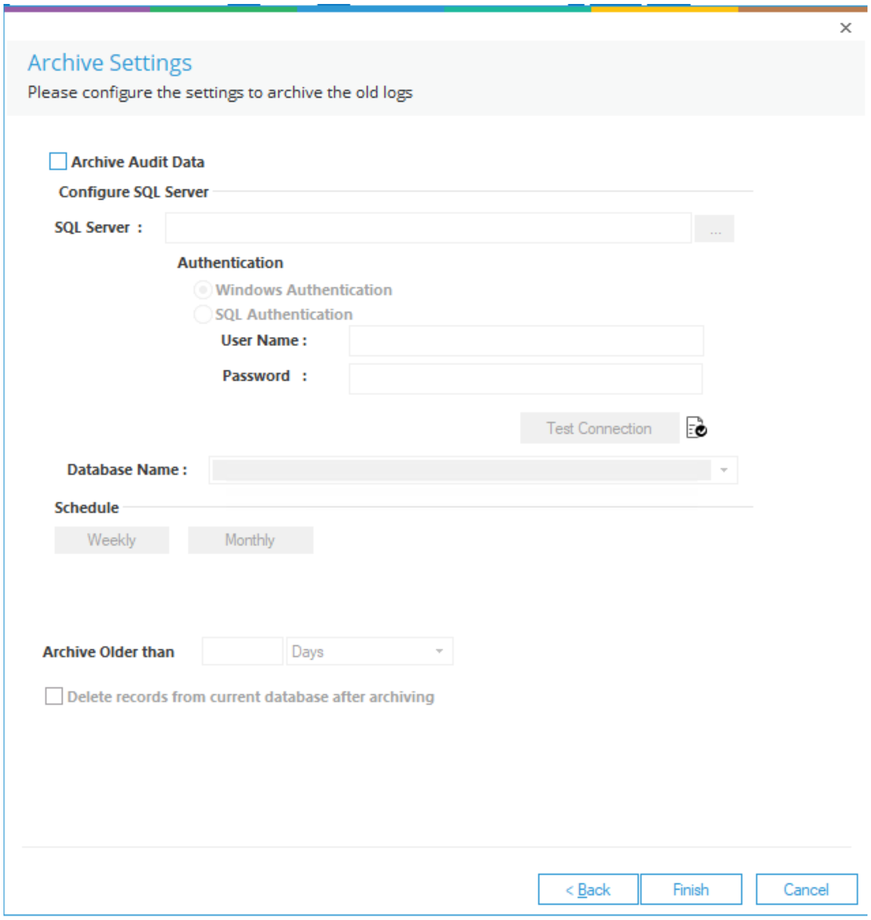
□ Users
- ▣ ##MS_PolicyEventProcessingLogin##
- ▣ ##MS_PolicyTsqlExecutionLogin##
- ▣ LDSP36DB\Administrator
- ▣ LepideSQL
- ▣ LPDE3\Administrator
- ▣ LPDE3\sumit
- ▣ LSTAgentLogin
- ▣ NT AUTHORITY\SYSTEM
- ▣ NT SERVICE\MSSQLSERVER
- ▣ NT SERVICE\SQLSERVERAGENT
- ▣ NT SERVICE\SQLTELEMETRY
- ▣ NT SERVICE\SQLWriter
- ▣ NT SERVICE\Winmgmt
- ▣ sa

Figure 14: Listing all SQL Server Users

20. Here, you can check the users to be audited and uncheck others to exclude from auditing.
21. Click **Next**. The next page displays database settings.

3.2.5.Archive Database Settings

22. In this step, you need to provide archive data details. It is an optional step that you can skip it if you do not want to archive the audit data.



Archive Settings

Please configure the settings to archive the old logs

□ Archive Audit Data

Configure SQL Server

SQL Server :

Authentication

○ Windows Authentication

○ SQL Authentication

User Name :

Password :

Database Name :

Schedule

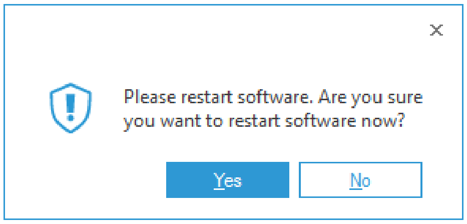
Archive Older than Days

□ Delete records from current database after archiving

Figure 15: Archive Database Settings to Add SQL Server

23. Archive Database Settings are discussed in the process of adding a domain. For further information, please refer to our Advanced Configuration Guide for Active Directory.
24. Click **Finish** to complete the process.

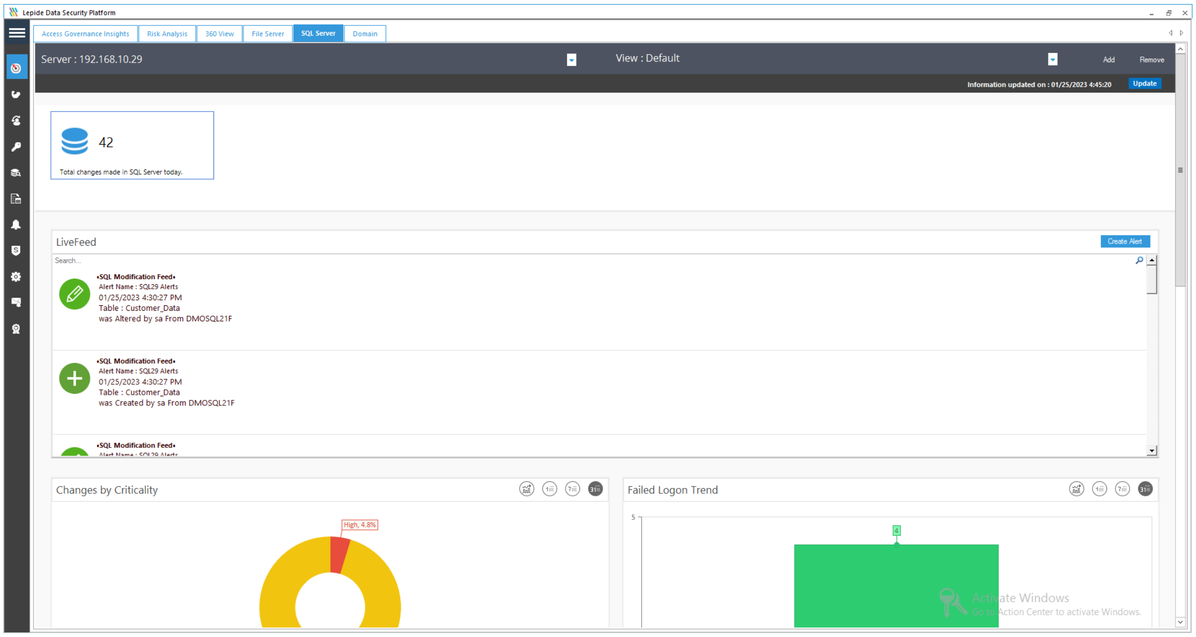
    Once you have performed all steps to add an SQL Server through Express Configuration or Advanced Configuration, a message box appears onscreen that needs the permission to restart the solution.



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

Figure 16: Asking to Restart the Solution

25. Click **Yes** to restart the solution.
26. After the restart, a new tab is created in both **Radar** and **Health Monitoring** Tabs. Once restarted, a new SQL Server tab is created under **Radar** tab.



Server : 192.168.10.29

View : Default

Information updated on : 01/25/2023 4:45:20

42

Total changes made in SQL Server today.

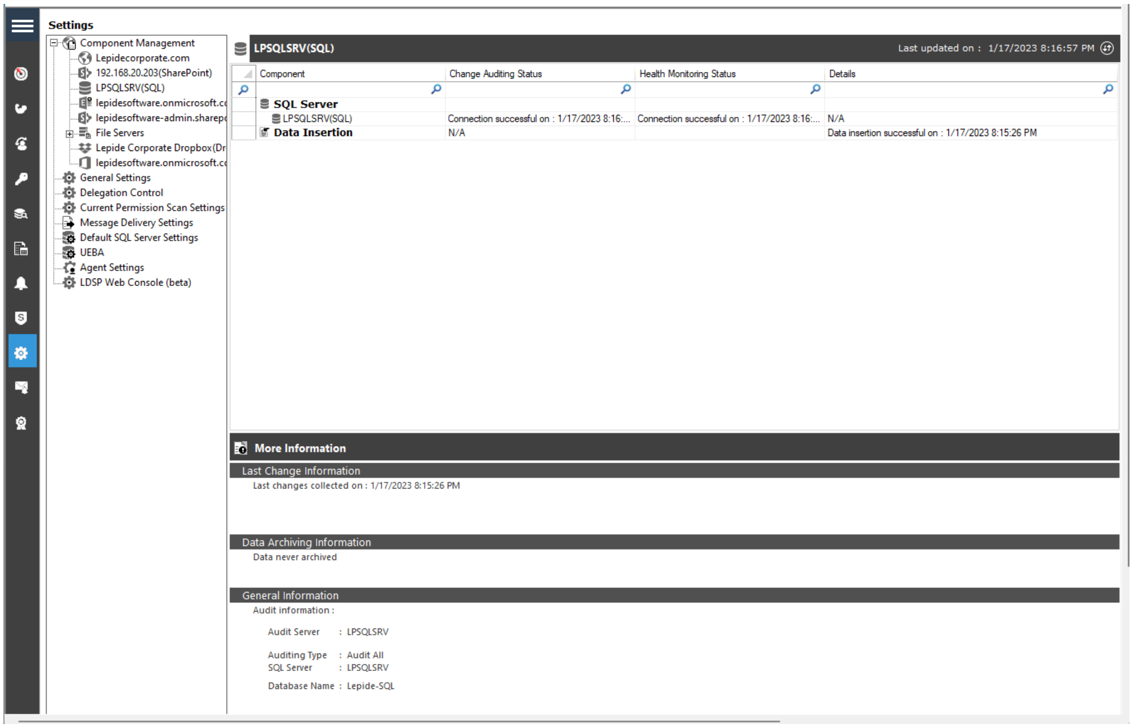
•SQL Modification Feed•
Alert Name : SQL29 Alerts
01/25/2023 4:30:27 PM
Table : Customer_Data
was Altered by sa From DMOSQL21F

•SQL Modification Feed•
Alert Name : SQL29 Alerts
01/25/2023 4:30:27 PM
Table : Customer_Data
was Created by sa From DMOSQL21F

•SQL Modification Feed•

Figure 17: SQL Server Tab in Radar

SQL Server Settings are displayed in **Settings** Tab under **Component Management**.


Settings
Component Management
Lepidecorporate.com
192.168.20.203(SharePoint)
LPSQLSRV(SQL)
lepidesoftware.onmicrosoft.c
lepidesoftware-admin.sharep
File Servers
Lepide Corporate Dropbox(Dr
lepidesoftware.onmicrosoft.c
General Settings
Delegation Control
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Web Console (beta)

LPSQLSRV(SQL) Last updated on : 1/17/2023 8:16:57 PM

Component	Change Auditing Status	Health Monitoring Status	Details
SQL Server			
LPSQLSRV(SQL)	Connection successful on : 1/17/2023 8:16:...	Connection successful on : 1/17/2023 8:16:...	N/A
Data Insertion	N/A		Data insertion successful on : 1/17/2023 8:15:26 PM

More Information

Last Change Information

Last changes collected on : 1/17/2023 8:15:26 PM

Data Archiving Information

Data never archived

General Information

Audit information :

```
Audit Server    :  LPSQLSRV

Auditing Type   :  Audit All
SQL Server      :  LPSQLSRV

Database Name   :  Lepide-SQL
```

Figure 18: SQL Server Management

- SQL Server Management lets you manage and remove the listing of SQL Server. Here, you can uninstall the auditing agent, configure the auditing, reinstall the auditing agent, and manage health monitoring.

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.