

Microsoft SQL server.

Configuration guide.

Contents

1	Introduction	2
2	Requirements and Prerequisites	2
2.1	Basic System Requirements	2
2.2	Supported Servers for Auditing	3
2.3	Required User Rights	3
2.4	Required SQL Server Rights	3
2.5	Required Ports	3
3	Add SQL Server	5
3.1	Add SQL Server with Express Configuration	7
3.1.1	SQL Server Details	7
3.1.2	Database Settings	8
3.2	Add SQL Server with Advanced Configuration	10
3.2.1	SQL Health Monitoring	11
3.2.2	Audit Settings	12
3.2.3	Object Settings	14
3.2.4	User Settings	16
3.2.5	Archive Database Settings	18
4	Support	21
5	Trademarks	21

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 6 core processor
 - Recommended 8 core processor
- Required RAM
 - Minimum 16 GB RAM
 - Recommended 32 GB RAM
- Required free disk space
 - Minimum 100 GB
 - Recommended 200 GB
- Any of the following Windows Operating Systems.
 - Windows Server OS: 2016, 2019, 2022 and 2025 (latest)
- Supported SQL Server Options for Storing Auditing Logs:
 - Any of the following SQL Server instances, either local or network hosted.
 - Recommended: Network-hosted SQL Server.
 - Any SQL Server above and including SQL Server 2016 (standard or enterprise)
- .NET Framework 4.6.2 or later



2.2 Supported Servers for Auditing

Audited Servers	Supported Versions
Microsoft SQL Servers	<ul style="list-style-type: none">Microsoft SQL Server 2016 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.

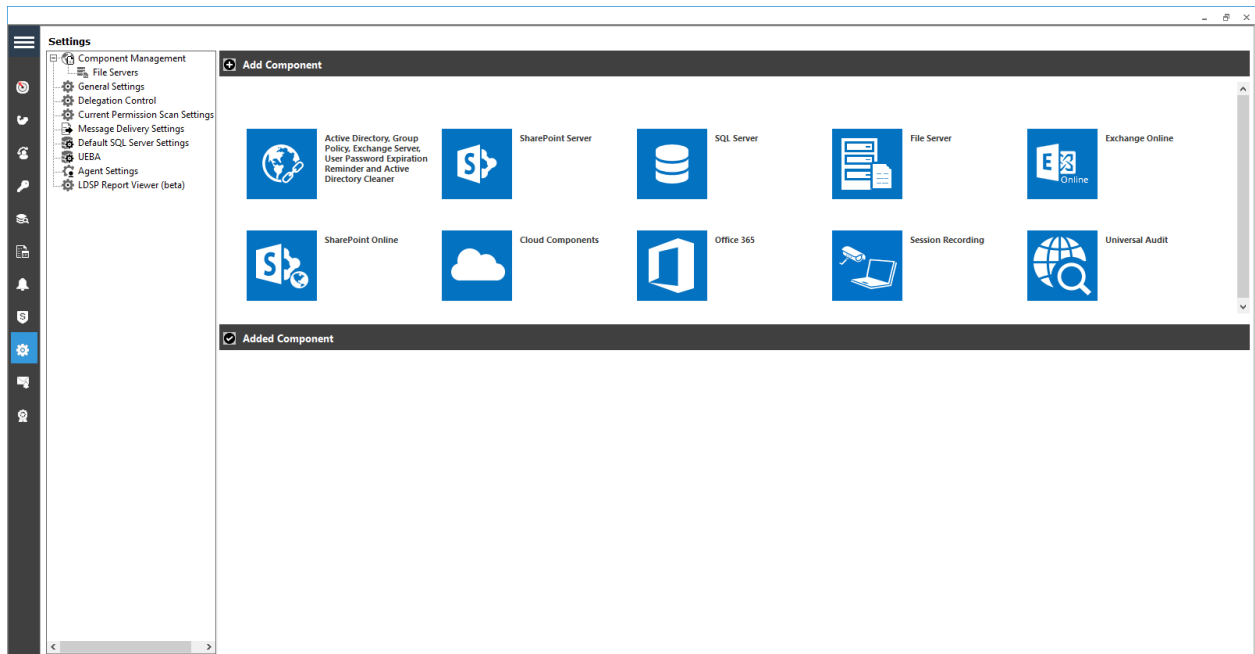
The solution uses the following ports for different purposes.

- Lepide Data Security Platform uses the following ports for communication:
 - Port 389 and Port 636 for LDAP queries.
 - 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 take the following steps:



- Select the SQL Server option in Component Selection dialog box

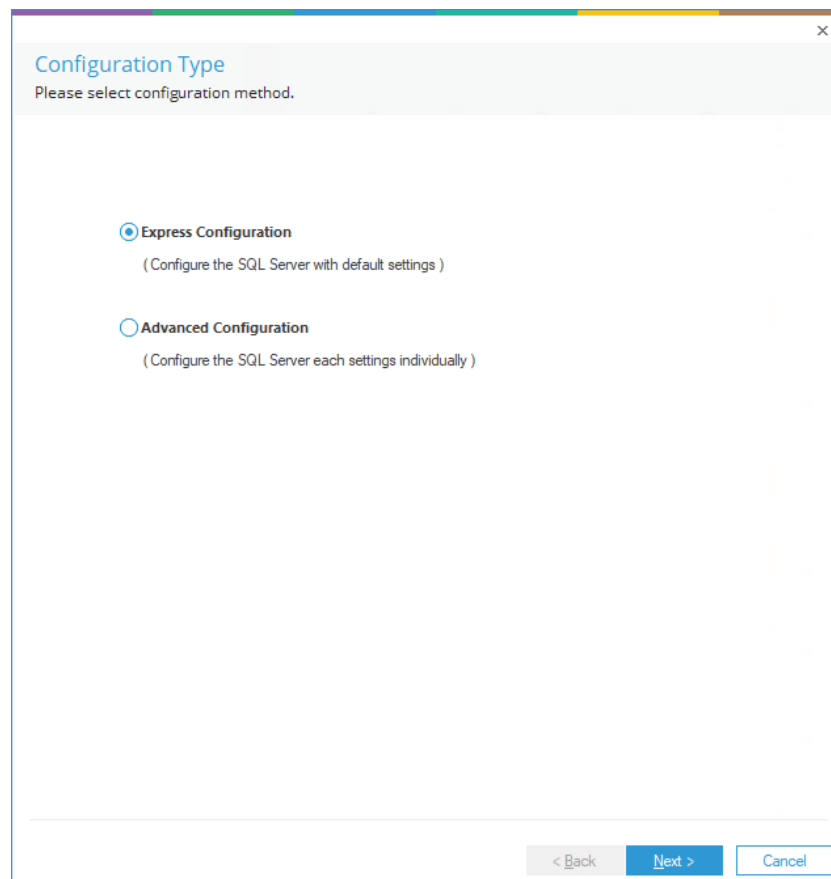


Figure 1: Add SQL Server Wizard

The solution offers two different ways to add SQL Server.

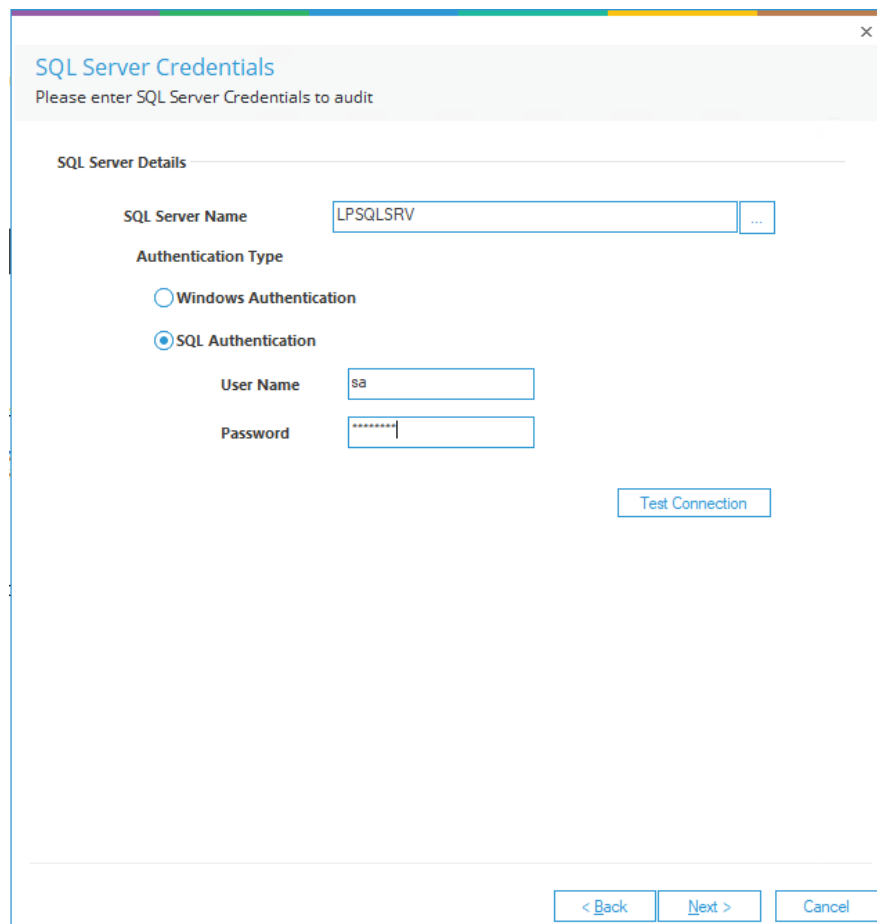
- Express Configuration: Add SQL Server with minimum recommended settings.
- Advanced Configuration: Add SQL Server with the advanced settings to customize the auditing.

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



The screenshot shows a dialog box titled "SQL Server Credentials" with the subtitle "Please enter SQL Server Credentials to audit". The dialog is divided into sections. The "SQL Server Details" section includes a text box for "SQL Server Name" containing "LPSQLSRV". Below this is the "Authentication Type" section, which has two radio buttons: "Windows Authentication" (unselected) and "SQL Authentication" (selected). Under "SQL Authentication", there are text boxes for "User Name" containing "sa" and "Password" containing masked characters. A "Test Connection" button is located to the right of the password field. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

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 SQLServer.

Database Settings
Please enter SQL server details to store data

Configure SQL Server

SQL Server :



Authentication

Windows Authentication

SQL Authentication

User Name :

Password :

Select Database :

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.

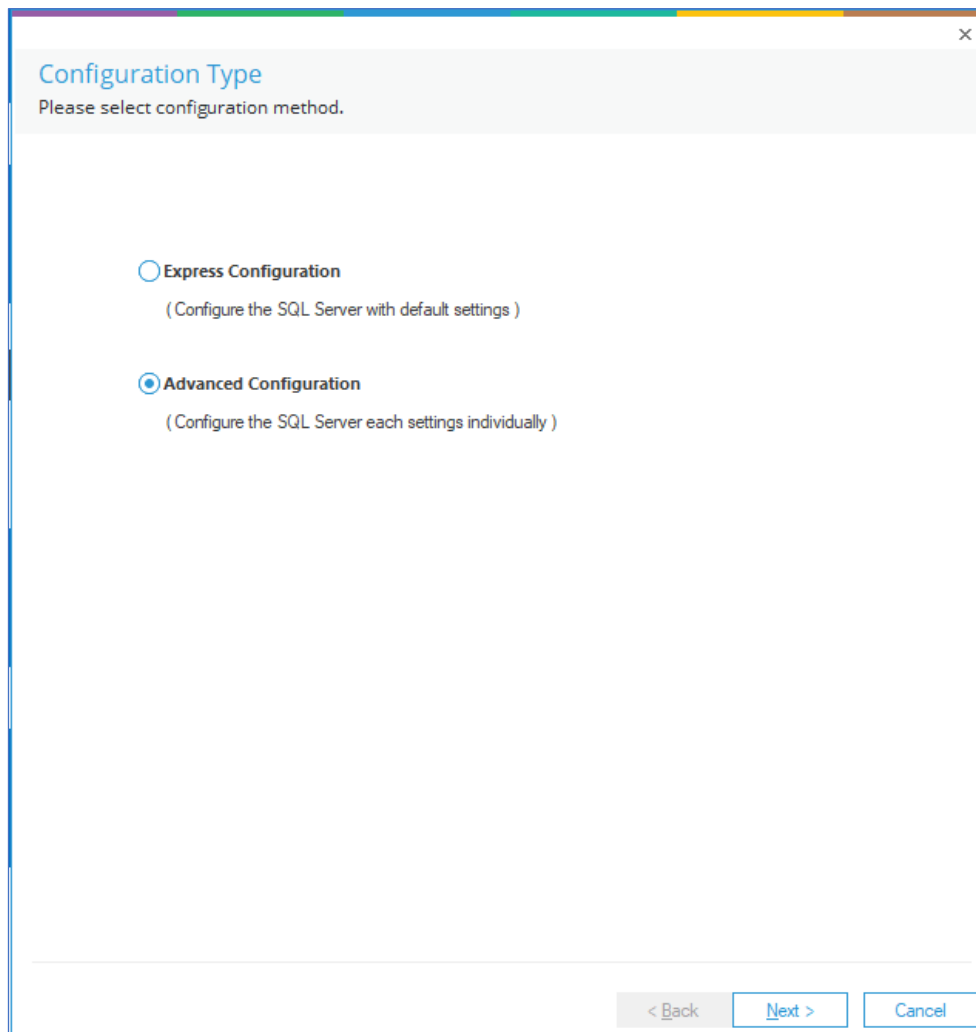


Figure 4: Adding SQL Server with Advanced Configuration

2. Click **Next**.

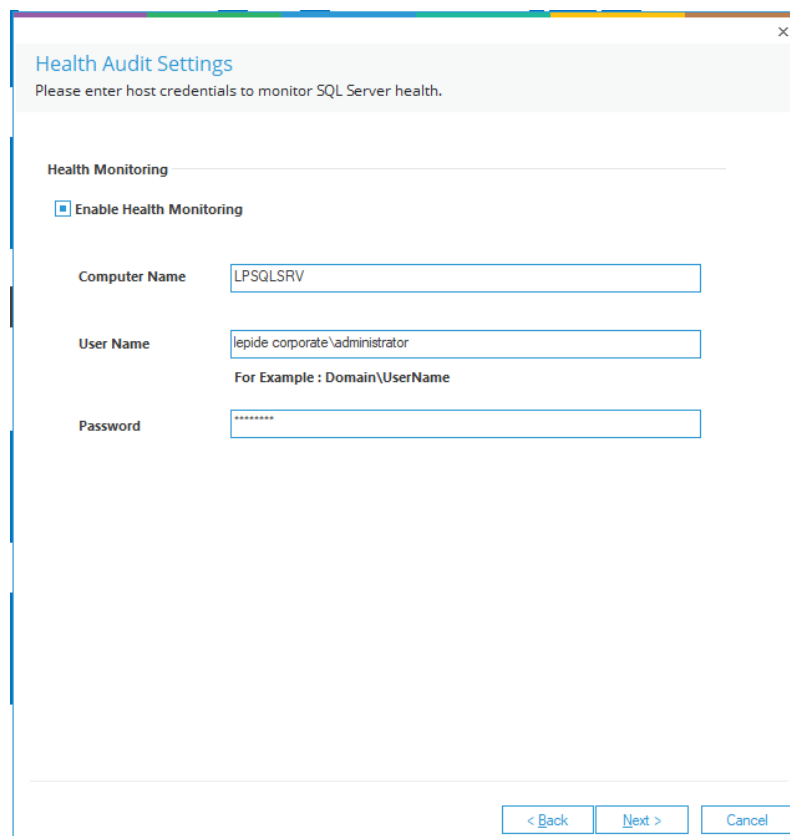
The following steps are the same as when adding SQL Server using Express Configuration and have previously been discussed in this guide. Click the following links to return to these topics:

- 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

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



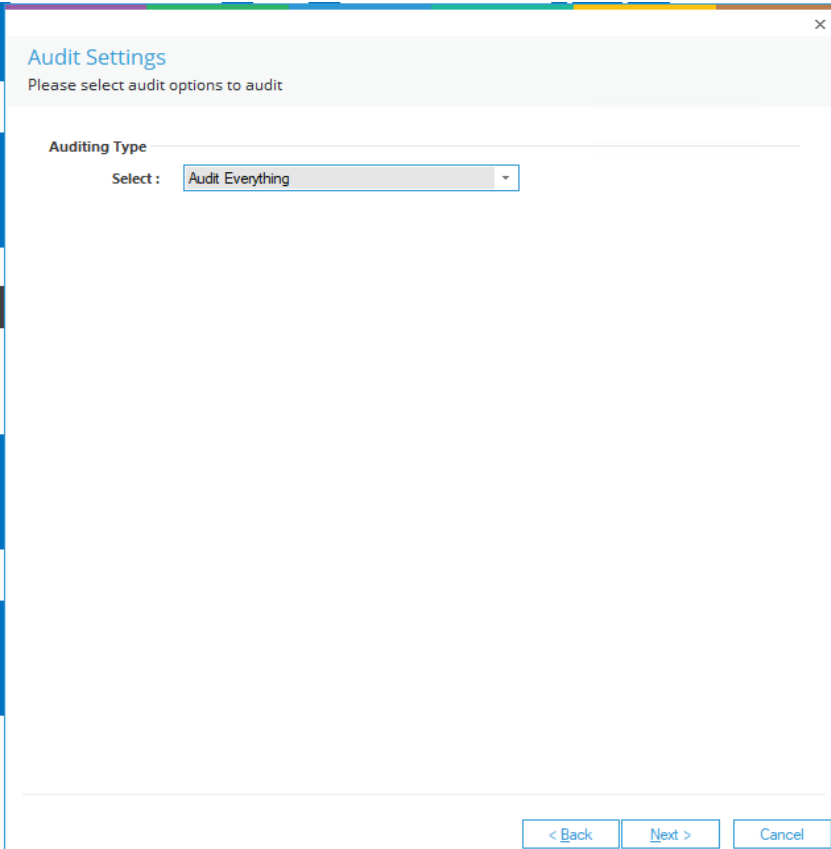
The screenshot shows a dialog box titled "Health Audit Settings" with a close button (X) in the top right corner. Below the title bar, it says "Please enter host credentials to monitor SQL Server health." The main area is titled "Health Monitoring" and contains a checkbox labeled "Enable Health Monitoring" which is checked. Below this are three input fields: "Computer Name" with the value "LPSQLSRV", "User Name" with the value "lepide corporate\administrator", and "Password" with a masked value "*****". A small text note below the User Name field reads "For Example : Domain\UserName". At the bottom right of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Figure 5: SQL Server Health Monitoring Settings

4. 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.
5. Click **Next** to proceed.

The next step displays **Audit Settings**.

3.2.2 Audit Settings



The screenshot shows a window titled "Audit Settings" with a close button (X) in the top right corner. Below the title bar, the text "Please select audit options to audit" is displayed. Under the heading "Auditing Type", there is a "Select:" label followed by a dropdown menu currently showing "Audit Everything". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

Figure 6: Audit Settings

6. Here, you need to specify the auditing type. The following options are available:
- Audit Everything:** Everything at SQL Server including all server objects and databases will be audited.
 - Audit Server:** Only Server objects will be audited, whereas databases will not be audited.
 - 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.

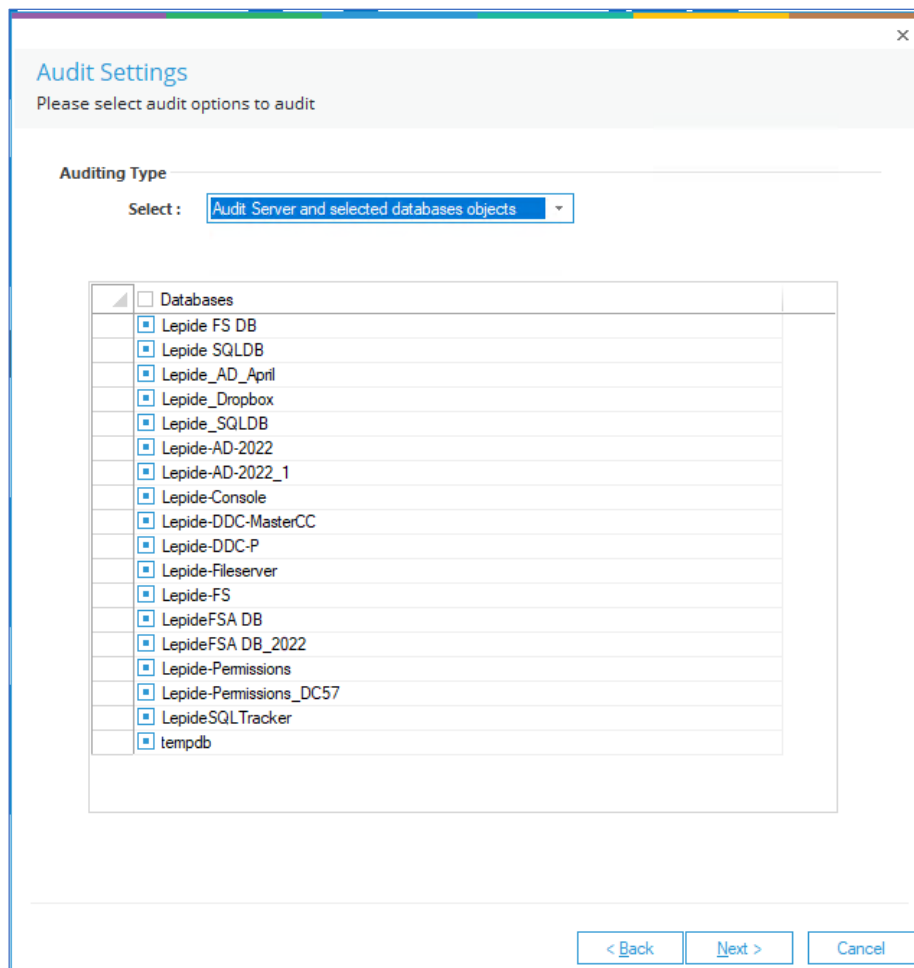


Figure 7: Listing all Databases to Audit

7. 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

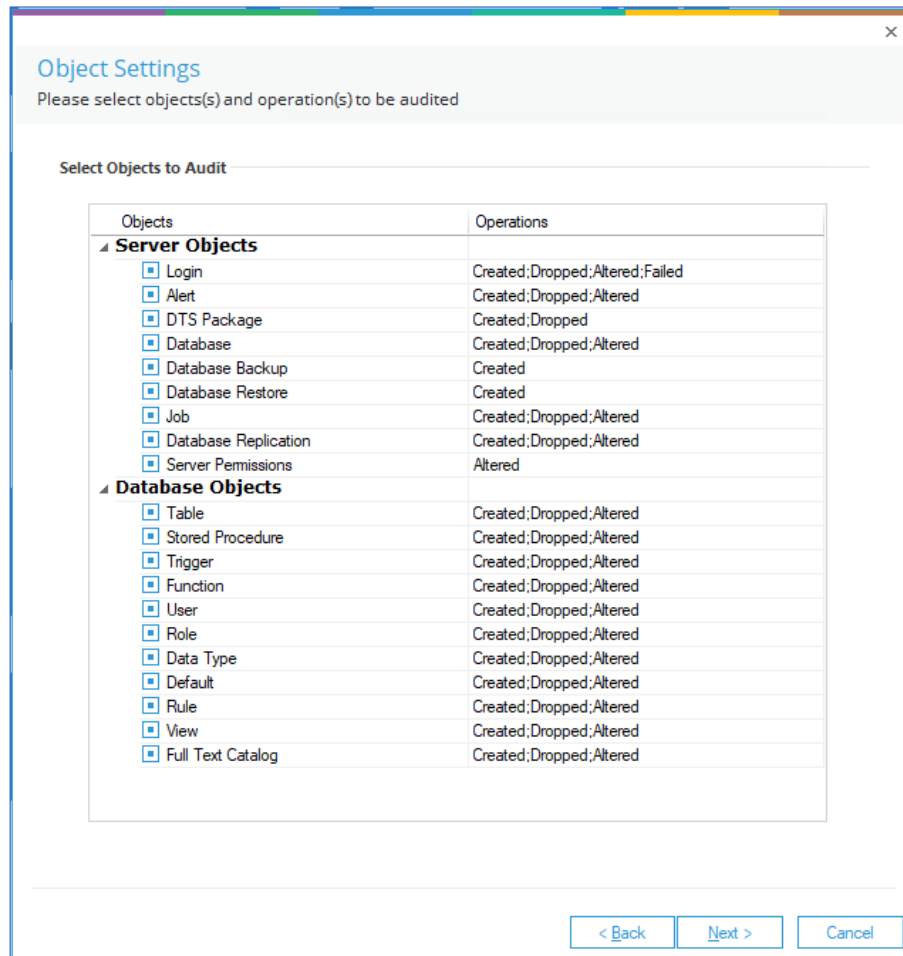


Figure 8: Object Settings

- 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.

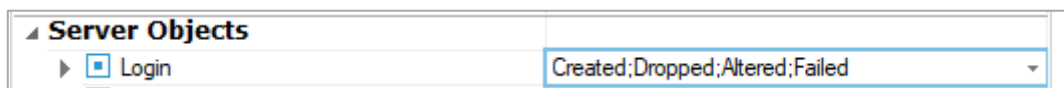



Figure 9: Object Settings

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

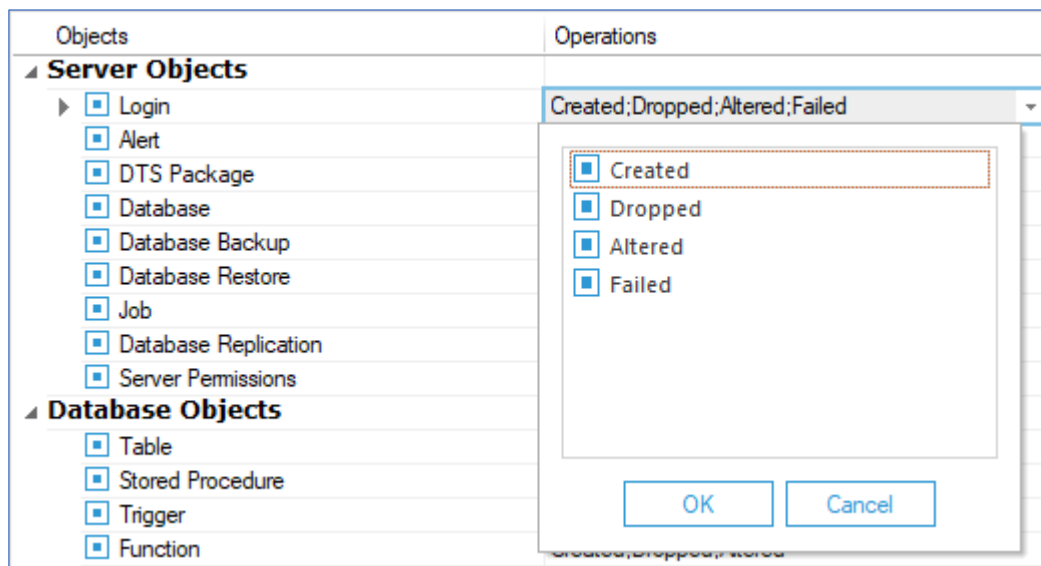


Figure 10: Listing all Operations for an Object

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

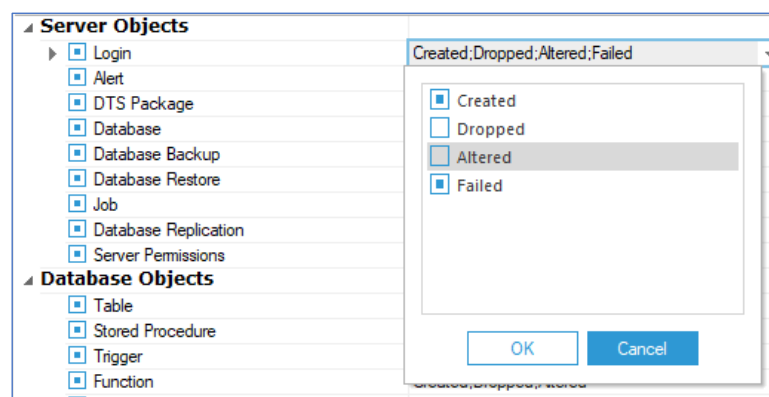


Figure 11: Modifying the Selection of Operations

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

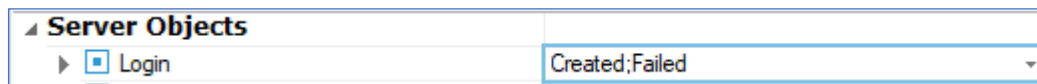


Figure 12: Selected Different Operations

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

NOTE: DML changes event are not being captured.

3.2.4 User Settings

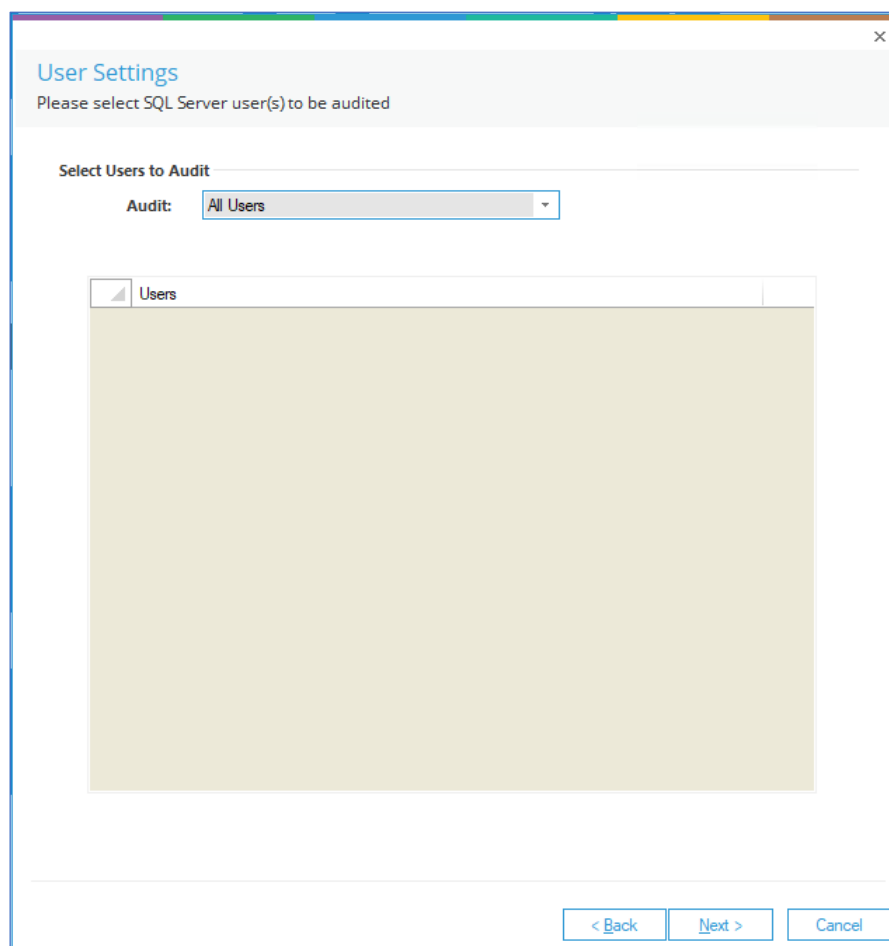


Figure 13: User Settings

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.

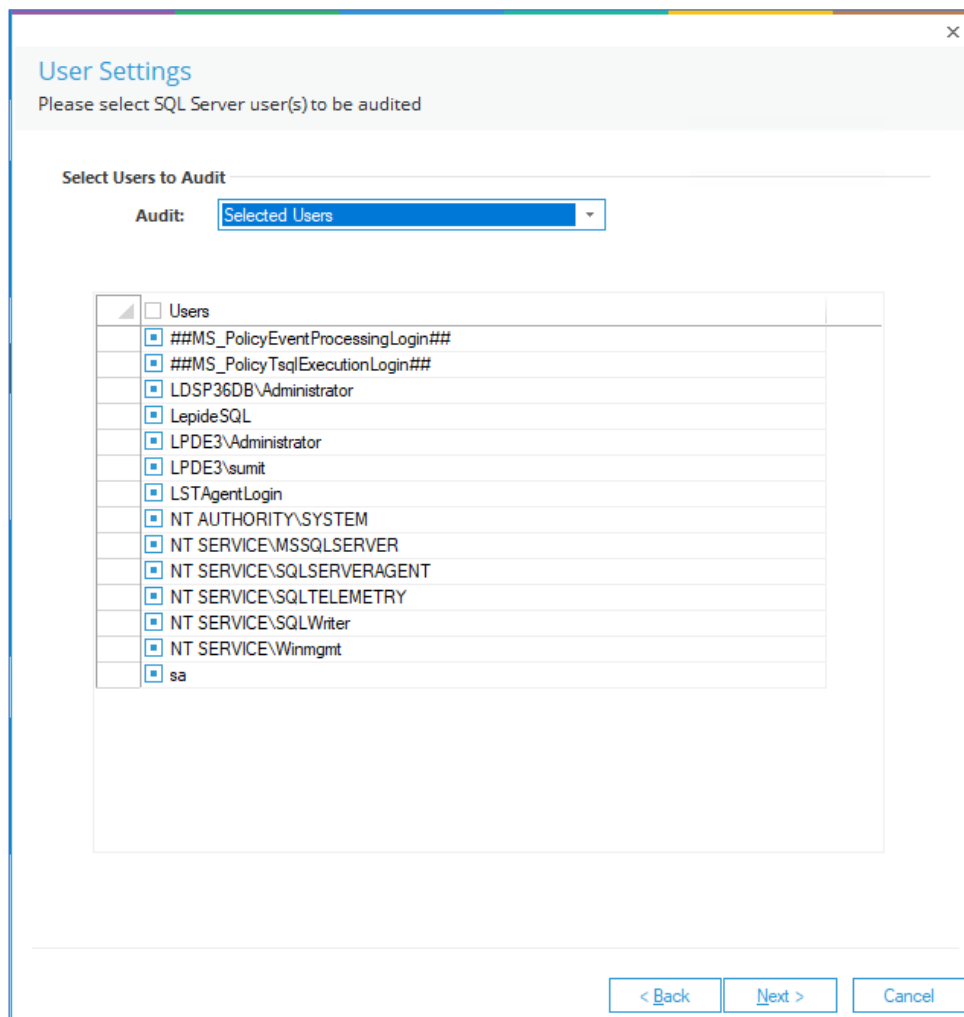


Figure 14: Listing all SQL Server Users

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

3.2.5 Archive Database Settings

16. 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 :

Test Connection

Database Name :

Schedule

Weekly Monthly

Archive Older than Days

Delete records from current database after archiving

< Back Finish Cancel

Figure 15: Archive Database Settings to Add SQL Server

17. 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](#).

18. 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.

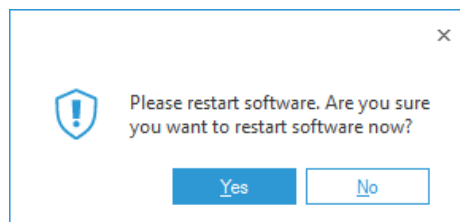


Figure 16: Asking to Restart the Solution

19. Click **Yes** to restart the solution.

20. 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.

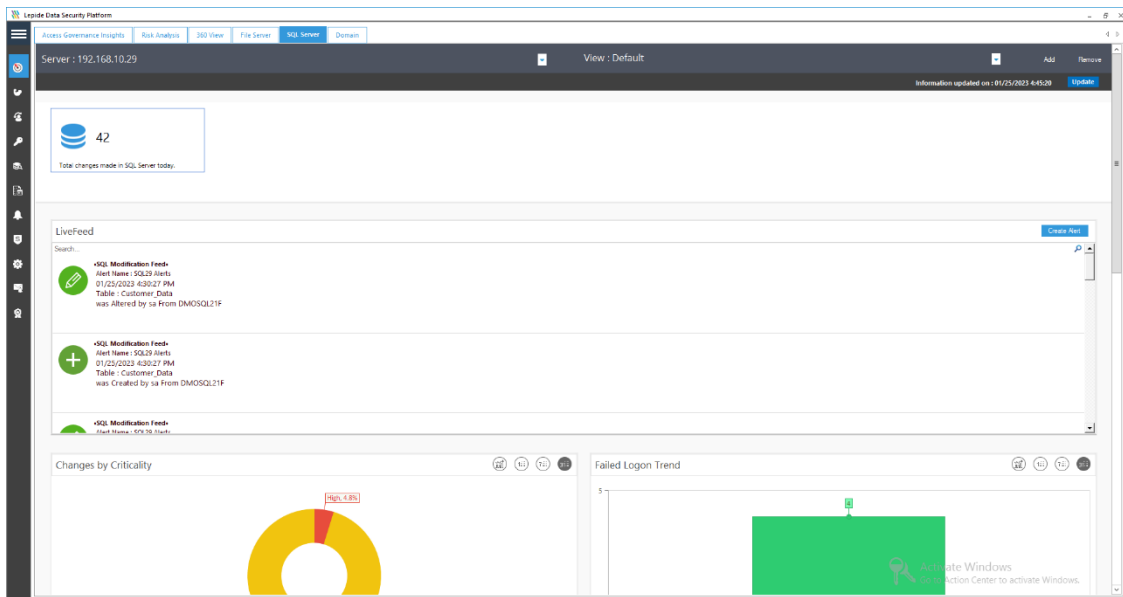


Figure 17: SQL Server Tab in Radar

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

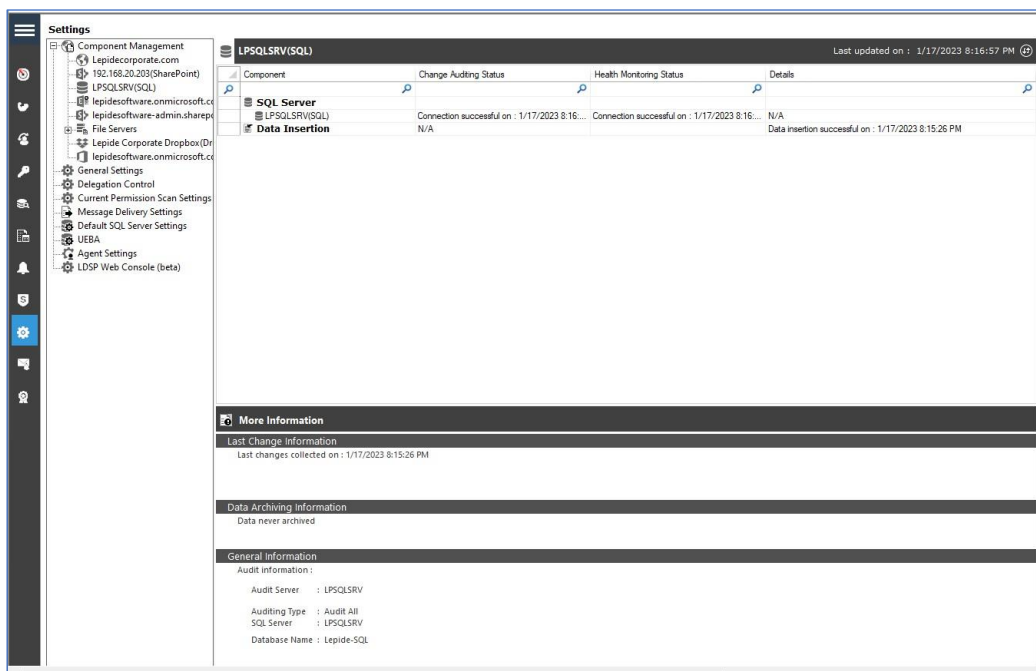


Figure 18: SQL Server Management

21. 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

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/>.

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

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.

