Lepide Data Security Platform

Installation and Configuration Guide
Table of Contents

1. Introduction ........................................................................................................................................... 5

2. Requirements and Prerequisites ........................................................................................................... 5
   2.1 System Requirements ...................................................................................................................... 5
   2.2 Supported Servers for Auditing .................................................................................................. 6
   2.3 Prerequisites for Health Monitoring ......................................................................................... 8
   2.4 Prerequisites for Web Console ............................................................................................... 8
   2.5 Required User Rights ............................................................................................................... 10
      2.5.1 Service Rights .................................................................................................................. 10
   2.6. Required Ports .......................................................................................................................... 11
   2.7 Prerequisites to Audit Domain ................................................................................................. 12
      2.7.1 Prerequisites to Audit Group Policy Objects .................................................................... 12
      2.7.2 Additional Requirement .................................................................................................... 12
   2.8. Prerequisites to Audit SharePoint .......................................................................................... 17
      2.8.1 Install Microsoft CLR Types .......................................................................................... 18
      2.8.2 Install SQL Management Objects .................................................................................... 19
   2.9. Prerequisites to Audit SQL Server .......................................................................................... 19
      2.10. Prerequisites to Audit NetApp Filers .................................................................................. 19
      2.11. Prerequisites to Audit Exchange Online ............................................................................ 20
   3. Install Lepide Data Security Platform ............................................................................................... 20
   4. Configure Service Credentials ......................................................................................................... 22
   5. Add Server Component ..................................................................................................................... 24
      5.1 Add Domain .............................................................................................................................. 25
         5.1.1 Add Domain with Express Configuration ........................................................................... 27
         5.1.2 Add Domain with Advanced Configuration ....................................................................... 41
         5.1.3 Active Directory Cleaner .................................................................................................. 52
         5.1.4 User Password Expiration Reminder .............................................................................. 62
      5.2 Add SharePoint ............................................................................................................................ 68
         5.2.1 SharePoint Server Details ............................................................................................... 69
         5.2.2 Install SharePoint Auditing Agent .................................................................................... 73
         5.2.3 Site Collection Settings ..................................................................................................... 74
         5.2.4 Database Settings ............................................................................................................... 75
         5.2.5 Archive Database Settings ............................................................................................... 76
8.2.1 Manage SharePoint Agent ........................................................................................................159
8.3. Modify SQL Server ..................................................................................................................162
  8.3.1 Manage SQL Health Monitoring ..........................................................................................164
8.4 Modify Exchange Online Server ..............................................................................................166
9. Remove Component ...................................................................................................................168
  9.1 Remove the listing of Domain ..............................................................................................168
  9.2 Remove the listing of SharePoint ..........................................................................................170
  9.3 Remove the listing of SQL Server ..........................................................................................171
  9.4 Remove the listing of Exchange Online ................................................................................172
10. Uninstall Lepide Data Security Platform ..................................................................................172
11. More Documents ......................................................................................................................173
12. Support ...................................................................................................................................174
13. Copyright ...................................................................................................................................174
14. Warranty, Disclaimers, and Liability Limitations ....................................................................174
15. Trademarks ................................................................................................................................174
1. Introduction

Lepide Data Security Platform provides a comprehensive means of auditing Active Directory, Group Policy, Exchange Server, Exchange Online, SharePoint, SQL Server, Windows File Server, and NetApp Filer. This guide helps you install, configure and manage the solution. It lets you add and manage the following server components.

1. Domain
   a. Active Directory plus Group Policy
   b. Exchange Server
   c. Active Directory Cleaner
   d. User Password Expiration Reminder

2. SharePoint Server

3. SQL Server

4. Exchange Online

Refer to another guide for configuring File Server Auditing. A list of other supportive documents is also provided at the end.

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

Before you start installing Lepide Data Security Platform, make sure that your computer meets the following requirements.

2.1 System Requirements

- Required Processor
  - Minimum dual-core processor
  - Recommended quad-core processor

- Required RAM
  - Minimum 8 GB RAM
  - Recommended 16 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 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

- Any of the following SQL Servers (local or network hosted) for storing auditing logs:
  - SQL Server 2005
  - SQL Server 2008
  - SQL Server 2008 R2
  - SQL Server 2012
  - SQL Server 2014
  - SQL Server 2016
  - SQL Server 2005 Express
  - SQL Server 2008 Express
  - SQL Server 2008 R2 Express
  - SQL Server 2012 Express
  - SQL Server 2014 Express

- .NET Framework 4.0 or later

2.2 Supported Servers for Auditing

<table>
<thead>
<tr>
<th>Audited Servers</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory and Group Policy Objects</td>
<td>- Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2016</td>
</tr>
</tbody>
</table>
## Audited Servers

<table>
<thead>
<tr>
<th>Audited Servers</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Server</td>
<td>• Exchange Server 2003</td>
</tr>
<tr>
<td></td>
<td>• Exchange Server 2007</td>
</tr>
<tr>
<td></td>
<td>• Exchange Server 2010</td>
</tr>
<tr>
<td></td>
<td>• Exchange Server 2013</td>
</tr>
<tr>
<td></td>
<td>• Exchange Server 2016</td>
</tr>
<tr>
<td>Exchange Online</td>
<td>• Office 365</td>
</tr>
<tr>
<td>Non-Owner Mailbox Access Auditing</td>
<td>• Exchange Server 2010</td>
</tr>
<tr>
<td></td>
<td>• Exchange Server 2013</td>
</tr>
<tr>
<td></td>
<td>• Exchange Server 2016</td>
</tr>
<tr>
<td>File Server</td>
<td>Supported Windows File Systems</td>
</tr>
<tr>
<td></td>
<td>• Windows 7</td>
</tr>
<tr>
<td></td>
<td>• Windows 8</td>
</tr>
<tr>
<td></td>
<td>• Windows 8.1</td>
</tr>
<tr>
<td></td>
<td>• Windows 10</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>Supported NetApp Filers</td>
</tr>
<tr>
<td></td>
<td>• NetApp 7-Mode Configuration</td>
</tr>
<tr>
<td></td>
<td>▪ Lepide Data Security Platform for File Server</td>
</tr>
<tr>
<td></td>
<td>successfully audits and report events from NetApp Filer</td>
</tr>
<tr>
<td></td>
<td>with Data ONTAP™ 7.2 or later.</td>
</tr>
<tr>
<td></td>
<td>▪ The recommended version for the availability of all</td>
</tr>
<tr>
<td></td>
<td>features is ONTAP 7.3.4 or later.</td>
</tr>
<tr>
<td></td>
<td>• NetApp Cluster Mode Configuration (CIFS Protocol only)</td>
</tr>
<tr>
<td></td>
<td>▪ 8.2.3 Clustered DataONTAP</td>
</tr>
<tr>
<td></td>
<td>▪ 8.3.0 Clustered DataONTAP</td>
</tr>
</tbody>
</table>
Audited Servers | Supported Versions
--- | ---
| | ▪ 8.3.1 Clustered Data ONTAP
▪ 8.3.2 Clustered Data ONTAP
▪ 8.3.2 RC1 Clustered Data ONTAP
▪ 9.0 Clustered Data ONTAP
▪ 9.1 Clustered Data ONTAP
▪ 9.2 Clustered Data ONTAP

SharePoint Server | • SharePoint Server 2010
• SharePoint Foundation 2010
• SharePoint Server 2013
• SharePoint Foundation 2013
• SharePoint Server 2016

SQL Server | • SQL Server 2005
• SQL Server 2008
• SQL Server 2008 R2
• SQL Server 2012
• SQL Server 2014
• SQL Server 2016

2.3 Prerequisites for Health Monitoring
• WMI Services should be up and running.

2.4 Prerequisites for Web Console
• .NET Framework 4.0 or later for installing Lepide Data Security Platform (Web Console)
• Web Browser is required to open the Web Console.
  ▪ Internet Explorer 8 or later
  ▪ Mozilla Firefox 20.0 or later
  ▪ Apple Safari 4.0 or later
  ▪ Google Chrome
  ▪ Microsoft Edge
2.5 Required User Rights

To install and work with 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.

2.5.1 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
- Manage Service Account object

2.5.2 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 in which 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 the system.
2. If the User Account does not exist on the system, create a new User Account with Administrative rights.

2.5.3 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.

5. 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".

6. 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".

2.6. 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 software 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.

2.7 Prerequisites to Audit Domain

Event Viewer of all domain controllers including the primary domain controller should be accessible. The required user rights to add a domain should meet the requirements that are listed in the steps to add a domain.

Other prerequisites are listed herein below.

2.7.1 Prerequisites to Audit Group Policy Objects

1. Windows PowerShell 2.0 and .NET Framework 4.0 should be installed on the server to be audited.

2. Windows PowerShell 2.0 and .NET Framework 4.0 should be installed on the computer where the software is installed.

3. GPMC should be installed on the computer where the software is installed.

4. Active Directory Module and Group Policy Module should be available in Windows PowerShell on the computer where the software is installed. Group Policy Auditing will not work if the software is installed on a computer where these modules are not available. For example, the Group Policy Auditing will not work at Windows Server 2008 as it does not have both of these modules.

2.7.2 Additional Requirement

You have to define retention method and size of security event logs in Group Policy Management Console on the primary domain controller.

2.8.1.1. Go to “Start Menu” → “All Programs” → “Administrative Tools” → “Group Policy Management”. It opens “Group Policy Management”.

**NOTE:** You can also type “GPMC.msc” in “Run” and press “Enter” key to access it.


2.8.1.3. Select an already existing customized default domain controller policy, which is active and enabled on the domain controller.

**NOTE:** If the auditing of domain is being disabled continuously, then you have to perform these steps in all custom Group Policies in “Domain Controllers” folder and in “Default Domain Controller” policy also. However, if you are not facing this issue, do not alter “Default Domain Controller” policy.

2.8.1.4. If an existing custom policy does not exist, right-click “Domain Controllers” node and click ”Create a GPO in this domain, and Link it here...” option to create a new Custom Group Policy Object. This command also links the newly created Group Policy Object to the domain controller node.
2.8.1.5. Enter the name of new Group Policy Object, for example "EnableAudit".

2.8.1.6. Click "OK" to create the new Group Policy Object and to come back at Group Policy Management Console.

2.8.1.7. Right-click on the existing or newly created custom Group Policy Object and click "Edit" to access “Group Policy Management Editor” for the selected policy.

2.8.1.8. Follow the steps below to modify a Group Policy that stops the Windows Server to override the auditing settings applied by Lepide Data Security Platform. If this policy is not modified as depicted here, the solution may face issues in auditing the server.


2.8.1.8.2. Double-click "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to access its properties.

**Figure 1: Editor of Group Policy Objects**

2.8.1.8.2. Double-click "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to access its properties.
2.8.1.8.3. Make sure that this policy is set to "Not Defined", i.e. "Define this policy setting" should remain unchecked always. Uncheck "Define this policy setting", if it is checked.

2.8.1.8.4. Close the dialog box.

2.8.1.9. Follow the steps below to define the Group Policies related to the storage and retention of the auditing logs. These changes are required to let Lepide Data Security Platform audit your domain. Once these changes are performed in the Default Domain Policy at the Primary Domain Controller hosting Active Directory, they will be applicable to all domain controllers and computers in the domain.

**NOTE:** After adding a domain in the solution, you can visit its properties and select "Domain Credentials" to perform similar settings automatically. You have to select the computers in the domain, on which these settings will be applied manually. [Know more...](#) However, no changes will be done in the Group Policy at the server. If the solution faces any problem in doing it automatically, then you have to perform these steps.

2.8.1.9.2. Double-click “Maximum security log size” policy in the right side to access its properties.

2.8.1.9.3. Check “Define this policy setting” box to enable the policy.
2.8.1.9.4. Enter the size as 2097152 KB (2 GB).

2.8.1.9.5. Click “Apply” and “OK”. It takes you back to “Group Policy Management Editor”, which shows the policies of “Event Log” including the above enabled policy.

2.8.1.9.6. Double-click “Retention method for security log” policy to access its properties.

2.8.1.9.7. Check “Define this policy setting” to enable this policy.

2.8.1.9.8. Select “Overwrite events as needed” option. It lets Event Viewer to overwrite the events once it requires or when the provided disk space to store these events is full.

2.8.1.9.10. Click “Apply” and “OK”. It takes you back to “Group Policy Management Editor”.

2.8.1.11. Close “Group Policy Management Editor”. It takes you back to “Group Policy Management Console”.

2.8.1.12. The left panel shows the newly created or existing Group Policy Object, which you have modified in the previous steps. Select the policy to select the objects like users, groups and computers in the right panel on which this policy will be applied.

2.8.1.13. Click “Add” to display the box to add the objects upon which this policy will be applicable.

2.8.1.14. Type “Everyone” in the text box and click “Check Names”. It selects all objects.

2.8.1.15. Click “OK” to confirm the change. It takes you back to the “Group Policy Management” window, which now displays the newly added group policy.

Figure 5: Properties of “Retention method for security log”
2.8.1.16. Close “Group Policy Management Console”.

2.8.1.17. In “Run” box or at “Command Prompt”, execute the following command to apply the above change.

```
gpupdate /force
```

2.8. Prerequisites to Audit SharePoint

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 Server 2012
- Microsoft SQL Server 2012 Management Objects
- .NET Framework 4.0 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.
2.8.1 Install Microsoft CLR Types

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

2.8.1.18. Go to the server and browse the folder of the computer where Lepide Data Security Platform is installed.

2.8.1.19. Open “Redist” folder, which has different folders. “x64” folder has the setup files for 64-bit Windows Server, whereas “x86” contains the files for 32-bit Windows Server OS.

2.8.1.20. Open the required folder.

2.8.1.21. 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 this warning message does not appear.

2.8.1.22. Click “Run”. It shows “Windows Installer”.

2.8.1.23. Once Windows Installer is initialized, it shows the installation wizard.

2.8.1.24. Click "Next". The next step displays the license agreement of Microsoft Corporation.

2.8.1.25. 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".

2.8.1.26. Click "Next" to proceed. The module is now ready to be installed.

2.8.1.27. Click "Install" to start the installation.

2.8.1.28. Once Microsoft System CLR Types is installed, the successful message appears in the wizard.

2.8.1.29. Click "Finish" to complete the process and to close the wizard.
2.8.2  Install SQL Management Objects

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

2.8.1.30. Go to the server and browse the folder of the computer where Lepide Data Security Platform is installed.

2.8.1.31. Open "Redist" folder, which contains two sub-folders. "x64" folder has the setup files for 64-bit Windows Server, whereas "x86" contains the files for 32-bit Windows Server OS.

2.8.1.32. Open the required folder

2.8.1.33. Run the setup file "SharedManagementObjects.msi" to install SQL Management Objects.

If you are running the setup file after copying it to the Local File System, then this warning message will not appear.

2.8.1.34. Click "Run". It shows "Windows Installer".

2.8.1.35. Once Windows Installer is initialized, it shows the installation wizard.

2.8.1.36. Click "Next". The next step displays the license agreement of Microsoft Corporation.

2.8.1.37. 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".

2.8.1.38. Click "Next" to proceed. The module is now ready to be installed.

2.8.1.39. Click "Install" to start the installation.

2.8.1.40. Once SQL Management Objects is installed, the successful message appears in the wizard.

2.8.1.41. Click "Finish" to complete the process and to close the wizard.

2.8.1.42. Close "Redist" folder.

2.9.  Prerequisites to Audit SQL Server

Following are the required prerequisites to audit SQL Server.

- The selected SQL Server should be in the same forest network.
- The computer, on which it is installed, should be a member of the domain instead of a workgroup.
- You cannot monitor a single SQL Server instance from two different installations of Lepide Data Security Platform. In any such case, the auditing in any installation of Lepide Data Security Platform will not work.

In addition to above, make sure to meet the required user rights to add the supported SQL Server. The rights to add a SQL Server for auditing are listed in the steps to add a SQL Server for auditing.

2.10.  Prerequisites to Audit NetApp Filers

- The agent to audit NetApp Filer can only be installed on any client system, but it requires GPMC.MSC (Group Policy Management Console) for installation.

- If you need the Permission Analysis of NetApp Filer, then we recommend to use synchronous mode to connect to NetApp Filer.
2.11. Prerequisites to Audit Exchange Online

- .NET Framework 4.0 or later
- Windows PowerShell 3.0 or later

3. Install Lepide Data Security Platform

To install Lepide Data Security Platform, you can download the installer file from [http://www.lepide.com/Lepide Data Security Platform/download.html](http://www.lepide.com/Lepide Data Security Platform/download.html). Make sure your computer meets the system requirements and the logged on user has the required rights as discussed in the above section. Extract the downloaded file and run "setup.exe" to start the installation.

**NOTE:** If the sufficient space to install the solution is not available, then it shows the following error.

![Figure 8: Error to install the solution](image)

**NOTE:** The solution can throw this error even after installation in case of insufficient space. Free at least 500 MB space on the disk drive where the solution is installed.

You have to follow the onscreen instructions to install the solution. The installation procedure is same as you follow to install general applications on Windows OS; still, the common steps are listed herein below for your ready reference.

1. At the first step, you have to click "Next".
2. The next step shows the license agreement. We recommend to read the license agreement carefully before installing the solution.
3. If you agree to the license agreement and want to continue the installation, then check "I accept the agreement" and click "Next".
4. It displays the step that lets you modify the installation location.

**NOTE:** The default destination is %ProgramFiles%\Lepide Data Security Platform for 32-bit and %ProgramFiles(x86)%\Lepide Data Security Platform for 64-bit Windows OS.

5. If you want to modify the installation location, then click "Browse" and select the desired location.
6. Click "Next" once you are done. At the next step, you can customize the location of the shortcuts folder in the Start Menu.
7. Click "Browse" and select a different location to modify the location of the shortcuts folder in the Start Menu.

8. Click "Next" to use the default or customized shortcuts folder. It takes you to the next step, where you can perform the additional tasks like creating a desktop and quick launch icon.

9. Check the boxes titled "Create a desktop icon", or "Create a Quick Launch icon", or both, if required.

10. Click "Next". Now, the solution is ready to install.

11. Click "Install" to begin the installation. When the installation process is completed, a message for successful installation appears in the wizard.

12. Click "Finish" to complete the process. If you have checked "Launch Lepide Data Security Platform ", it will close the installation wizard and starts to launch the solution.

Welcome Screen appears once the solution is launched for the very first time.
4. Configure Service Credentials

You can configure this option to select the User Account with which you want to create and run the Windows Service of Lepide Data Security Platform. This setting appears on the Welcome Screen when you are running the solution for the very first time.

Perform the following steps to configure this option.

13. It contains the following two options.
   A. Local System Account: Select this option to install and run the Lepide Data Security Platform service using the local system account.
   B. This account: Select this option to install and run the Lepide Data Security Platform service using the provided user account.

14. Select "This Account" for installing and running the service with a customized account.

**NOTE:** You can also right-click on "Component Management" node in "Settings" tab to access the option to configure the service credentials.

![Figure 11: Configure the credentials](image1)

![Figure 12: Option to access Service Credentials](image2)
15. You can either type the username manually or click "Browse" to select a user account or Manage Service Account object from Active Directory.

![Select Users or Service Accounts](image)

**Figure 13: Select User from Active Directory**

**NOTE:** You should use any of the following user account or object.

- A local system administrator
- A member of Domain Admins Group
- Manage Service Account object

16. You can type the name of user or Service Account and click "Check Names" to verify. Once verified, the name is depicted with an underline.

17. Click "OK" to select the user or Service Account. It takes you back to the previous dialog box.

18. Enter the password for the selected user. If you have selected a Manage Service Account, then leave the password text box blank.

19. Click "OK". The solution configures the services.

20. If the rights required to configure the service are not available to the user on the current system, then following message box appears onscreen.

![LepideAuditor Suite](image)

**Figure 14: Message box asking to assign right**
21. Click "Yes" to assign the rights. The following box is displayed when the service is configured and running with the provided credentials of the selected user.

![Lepide Auditor Suite](Image)

*Figure 15: Successfully configured the service*

Click "OK" to complete the process. Now, "Component Selection" dialog box appears.

![Component Selection](Image)

*Figure 16: Select Component*

Select the type of component and add it for auditing.

## 5. Add Server Component

You can add the following components. There are different configuration wizards for each of these components.

- Active Directory, Exchange Server, Group Policy, Active Directory Cleaner, and User Password Expiration Reminder
- Exchange Online
- SQL Server
- SharePoint Server
- File Server

You can use any of the following methods to get a wizard to adding a component.
22. In Component Selection dialog box, select a component and click “OK”.

23. In “Add Component” section of Component Management, you can click any button.

24. Alternatively, you can right-click on the root node of “Component Management” and go to “Add” sub-menu to access the options to add a component.

5.1. Add Domain

Select “Active Directory, Exchange Server, Group Policy, Active Directory Cleaner, and User Password Expiration Reminder” option in any of the above methods.

You can add a domain with any of the following procedures:

A. Agent-based Auditing: Agents are installed on the server to enable audit at the domain level and to audit these components: Active Directory, Group Policy, Exchange Server, Non-Owner Mailbox Access, and Logon/Logoff. These agents run continuously on the server and consume its resources. Health Monitoring is always agentless even in agent-based monitoring as it is the default option to add the domain; however, you are free to select another option.

2. Agentless Auditing: No agent will be installed for auditing Active Directory, Group Policy, and Exchange Server on the server. Hence, they do not consume the server resources. However, the following agents are still be deployed.

   A. An agent is deployed for Non-Owner Mailbox Access Auditing.
   B. An agent is required to collect logon/logoff events and to send them to the solution for auditing.
   C. A temporary agent to enable audit at domain level are installed on the server, but are removed after enabling the audit.

**NOTE:** In both agentless and agent-based auditing, you have to perform the following steps on any domain controller of the domain.

- Generate "Logon.exe" from the solution, while adding or modifying the domain, and create a Group Policy to assign it. It will collect logon and logoff events and passes them to Logon/Logoff Audit Module.
- Install Logon/Logoff Audit Module, which will process logon/logoff events and send it to the solution for display.

Both of these modules should run continuously at the server for collecting logon/logoff events.

Without deploying this "logon.exe" and "Logon/Logoff Audit Module", logon/logoff events will not be monitored and audited. [Click here to know more about Logon/logoff monitoring and its module.](#)

Before proceeding, make sure that prerequisites to audit the domain are met. [Know more...](#)

To add the domain, you need to perform various steps, which include:
You can add a domain using any of the following methods. While adding the domain, you can also configure Active Directory Cleaner and User Password Expiration Reminder.

1. Express Configuration: Add domain with minimal recommended settings.
5.1.1 Add Domain with Express Configuration

The wizard starts with two different configuration options available for adding a domain.

5.1.1.1 Domain Settings

In this section, you need to provide details of the domain to be added.
It contains the following options:

1.1.1.1.  IP Address or Name of Domain: Enter the domain name or its IP Address. Click icon to let the solution discover the current domain in which it is installed. It auto fills its name in the text box.

1.1.1.2.  User Name: Enter the username in the format 'Username@domain.com'. Ensure you provide the complete username with the domain name.

**NOTE:** The provided user should have any of the following "User Account Privileges".

a.  Minimum Rights – User should be a member of “Administrators” and “Domain Admins” groups to audit Active Directory, Group Policy and Exchange Server. However, with these rights, the auditing of schema and domain configuration will not enabled automatically. In this case, you have to enable their auditing manually.

b.  Required Rights – User should be a member of “Administrators”, “Domain Admins”, “Group Policy Creator Owners”, “Enterprise Admins”, and “Schema Admins” to enable the automatic auditing of schema and domain configuration by the solution.
NOTE: After enabling the audit at domain level, you may switch from above “Required Rights” to “Minimum Rights” by removing the membership of the user account from “Group Policy Creator Owners”, “Enterprise Admins”, and “Schema Admins”.

Follow the steps below to provide the rights mentioned above:

i. Go to “Administrative Tools”.

ii. Open “Active Directory Users and Computers”.

iii. Select “User Properties”.

iv. Go to “Member Of” → “Add Group”.

v. Select any of the following groups as per the above requirements.
   - Administrators
   - Domain Admins
   - Group Policy Creator Owners
   - Enterprise Admins
   - Schema Admins.

vi. Click “Apply” and “OK”.

1.1.1.13. **Password**: Enter the correct password for the selected user.

1.1.1.14. Select any of the following radio buttons for "Auditing Method".

1.1.1.1.14.1. With Agent: Click this button to install the following agents on the server. It is the default option to add the domain.

   1.1.1.1.14.1.1. An agent for enabling auditing

   1.1.1.1.14.1.2. Auditing agents for auditing Active Directory, Group Policy, Exchange Server, and Non-owner Mailbox Access

1.1.1.1.14.2. Without Agent: In this case, agents for auditing Active Directory, Group Policy, and Exchange Server will not be installed. Steps to add the domain with/without an agent will be same as discussed here.

Even in agentless auditing, following agents will be deployed to the server.

1.1.1.1.14.2.1. A temporary agent will also be installed to enable the auditing at the domain level on the server but will be removed after enabling the auditing.

1.1.1.1.14.2.2. One agent is required to monitor non-owner mailbox access in Exchange Server.

**NOTE:** In both agentless and agent-based auditing, you have to deploy "logon.exe" and install a Logon/Logoff Audit Module to enable the auditing of logon/logoff events. Without them, logon/logoff events will not be monitored and audited. [Click here to know more about Logon/logoff monitoring and its module.]

Click “Next” once you have provided the details. The software connects to the domain. If auditing is not enabled at the domain level, the following dialog box appears onscreen.
Figure 20: Enable Auditing

You can click the button. It displays the following dialog box.

Figure 21: Enable Auditing
Enter either IP Address of the primary domain controller or name of the domain. Select any of the following options.

1. **Create New Policy (Recommended):** Select it to create a new Domain Controller Policy. Once selected, you have to provide the name of new Group Policy to be created.

   ![Group Policy Object Selection](image1)

   **Figure 22: Creating new Group Policy**

   Click "OK" to create a new Group Policy at the domain to enable the auditing.

2. **Use Selected Domain Controller Policy:** This option lets you select a domain controller policy to enable the auditing. Select this option to enable the adjoining section.

   ![Group Policy Object Selection](image2)

   **Figure 23: Select a Group Policy Object**
Perform the following steps to select an existing Group Policy.

A. If a Group Policy is not listed here, you can click icon to rescan the domain for listing the updated set of Group Policies.

B. You cannot select "Default Domain Controller Group Policy" or "Default Domain Group Policy" to enable the auditing using Lepide Data Security Platform. If you try, the following error message appears on the screen.

C. Select a custom Group Policy created at the Domain Level or Domain Controller Level upon which the auditing setting has to be applied.

D. Make sure to check "Create a backup of selected Group Policy Object before enable auditing" box if you are enabling the auditing on an existing Group Policy. This backup allows you to restore the previous default Domain Controller Policy if any issue persists after enabling the auditing.

   To avoid such an issue, create a new Domain Controller Policy to enable the auditing.

E. Click "OK". The software tries to enable the auditing and create the backup of the selected group policy on the server in "%systemdrive%\Windows\Lepide\GPOBKP_24-01-2017 18_13_35" folder. Here, 24-01-2017 will be replaced with the date and 18_13_35 will be replaced with the time when you have clicked "OK" to enable auditing on the selected policy.

   If you face any issue in future, you can use this backup to restore the policy to the earlier state. Refer to the guide to enable audit manually at the domain level to restore the group policy.

F. You have to wait until the auditing is enabled.

If the solution faces any problem in enabling the audit, you may receive the following or another error message.

![Figure 24: Error message while enabling auditing at Default Domain Controller Policy](image)

![Figure 25: Error message](image)
In the case of above error or other problem, you have to enable the auditing settings manually on the Windows Server. Kindly refer to the guide to enable audit manually at the domain level.

Once auditing is enabled, the solution displays the next step to configure the auditing.

5.1.1.2 Advanced Domain Configuration

All domain controllers in the domain will be listed here. Here, you can configure the domain auditing by enabling or disabling the following options.

1.1.1.5. **Enable Auditing**: Check/uncheck the following options to enable/disable auditing, backup snapshots, and Health Monitoring.

*Figure 26: Advanced Domain Configuration*
d. Non-owner Mailbox Auditing: Enable/disable the mailbox access auditing of non-owner users and owners.


f. Active Directory Backup: Enable/disable the backup snapshot feature to create snapshots of Active Directory.

g. Group Policy Backup: Enable/disable the backup snapshot feature to create snapshots of Group Policy Objects.

1.1.1.6. **Options for Domain Controllers:** Each domain controller will have the following options. Check/uncheck these options to enable/disable features and install/uninstall their corresponding agents for the target domain controller.

a. Change Auditing: Check it to enable Change Auditing for a component and install its corresponding agent. Auditing agents will not be installed in the agentless auditing mode.

b. Health Monitoring: Check it to enable Health Monitoring for Active Directory & Exchange component, and to install its corresponding agent.

c. Non-Owner Mailbox Auditing: Check it to enable Non-Owner Mailbox Access Auditing for the selected Exchange Server and to install its agent on the server.

1.1.1.7. The following options are unchecked by default.

a. Active Directory Backup

b. Group Policy Backup

c. Health Monitoring

d. Non-Owner Mailbox Auditing

e. Active Directory Cleaner

f. User Password Expiration Reminder

1.1.1.8. You have to check these options to enable them. We have selected all these options in this test case.
1.1.1.9. Click icon of "Non-Owner Mailbox Auditing" to configure the auditing options of Exchange Mailbox Accesses for both owner and non-owner users. You can refer to enable non-owner mailbox auditing guide for more information.

1.1.1.10. Click icon for "Active Directory Cleaner" to configure its options. Know more...

1.1.1.11. Click icon for "User Password Expiration Reminder" to configure its options. Knowmore...

1.1.1.12. Click icon for "Active Directory Backup" to configure its options using the following dialog box. Select "Daily", "Weekly", or "Monthly" option in the dialog box. You can customize the time in "Daily" settings. Upon selecting "Weekly at", you can specify the days on which backup snapshots will be captured.
If "Monthly at" option is selected, you can specify the time and day options. Click "OK" to apply the settings.

1.1.1.13. Similarly, you click icon for "Group Policy Backup" and use above steps to configure the Group Policy Backup.

1.1.1.14. You can click icon to restore the default options for this step.

1.1.1.15. Click icon to rescan the domain and to load the updated information.

Click "Next" to proceed further.
5.1.1.3 IP Settings

Here, you have to verify the IP Address resolved by the solution. If IP Address is blank or wrong, double click the cell containing IP Address to make this field editable. Enter the correct IP Address and press “ENTER” key.

You can click icon to restore the default options for this step.

You can also select the preferred domain controller, to which the calls related to auditing, data collection, and backup snapshots will be sent. The selected domain controller should be located nearby so that the actions related to these calls can be performed at the earliest. You can also select a domain controller, which is comparatively idle or has less load.

If there is a long list of domain controllers, then you can use the top filtration row to filter for the required domain controllers that have to be modified. The following image shows such a list.
Type the keyword in the first cell of the domain controller to filter this list.

Once done, you can click “Next” to proceed further.

5.1.1.4 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 to a locally hosted or networked SQL Server.
To perform database settings, follow the steps below:

1.1.1.16. Enter the SQL Server name manually or click button to enumerate all SQL Servers and select any one from the list.

1.1.1.17. Authenticate the SQL Server configuration by either way:

a. Windows Authentication: Choose this option to allow the solution to access SQL Server using the credentials with which the user is currently logged in.

b. SQL Server Authentication: Select this option to access SQL Server with the credentials of an SQL Server user. We recommend to select this option.

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

NOTE: Here, the selected user should have "sysAdmin" role in SQL Server. Know more...

1.1.1.18. Provide database name where Lepide Data Security Platform have to store the auditing logs.
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.

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

Click 'Test Connection' button. It displays either an error if failed to connect or the following message confirming the successful connection.

![Test connection successful](image)

*Figure 33: Test Connection is successful*

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

1.1.1.20. You can change the default path to save the complete and reference backup snapshots. Refer to 8.1.1 Move Backup Snapshot Data section to know more.

Click 'Finish' to add the domain with the above settings.

A message box to restart the solution appears on the screen.
5.1.2 Add Domain with Advanced Configuration

You can use this method to define the advanced auditing options while adding the domain. The wizard starts with two different configuration options.

Select “Advanced Configuration” option and click “Next”.

The following four steps appear next in the above wizard. They have been discussed earlier in the Express Configuration section. You can click the links below to know more about them.

- 5.1.1.1 Domain Details
- 5.1.1.2 Advanced Domain Configuration
- 5.1.1.3 IP Settings
- 5.1.1.4 Database Settings

Click “Next” once you have configured the database settings.
5.1.1.1 Organizational Unit Settings

In this step, you can select the Organizational Units that you wish to audit.

Use “Audit” drop-down menu to select any of the following options.

1. All Organizational Units: Select this option to audit all Organizational Units. By default, ‘Audit All Organizational Units’ option is selected. If you wish to audit all OUs then just click “Next” to proceed.

2. Only selected Organizational Units: Select this option to audit only selected Organizational Units. You need to select OUs to customize their auditing.

To add Organizational Units manually, enter the name of the new Organizational Unit in “Add New” box and click ‘+’ button.

Press and hold CTRL key to select the multiple organizational units to be audited and click ‘>’ button to add the selected organizational units to “Selected OU Path” list.
The selected OUs will be listed in the table. Click 'Next' to proceed.
5.1.1.1 Object Class and other Settings

In this step, you can select the Object classes that you wish to audit.

![Object Classes and Other Settings](image)

By default, 'Audit All Object Classes' option is selected. If you want to audit the particular object classes, then you can select those manually. This section is divided into two parts:

1. **Object Classes**: In this section, you can choose any of the following two options.
   a. **All Object Classes**: Select this option to audit all Object Classes of both Active Directory and Exchange Server.
   b. **Only selected Classes**: Select this option to audit only the selected Object Classes of Active Directory and Exchange Server.
   c. **All but excluding selected classes**: Select this option to audit all Active Directory and Exchange Server Object Classes except the selected classes. It is the default option while adding the domain. It means the following 13 object classes remains excluding from the auditing by default. You have to uncheck these classes in "All but excluding selected classes" or select "All Object Classes" to start their auditing.
      - CRLDistributionPoint
      - CrossRef
Perform the following steps below to customize the auditing of object classes.

1. Select “Only Selected Classes” or “All but excluding selected classes” option for the Audit drop-down menu. It lists the object classes listed in two columns – “Active Directory Object Classes” and “Exchange Server Object Classes” – will be activated for selection.

![Selecting Object Classes and other auditing settings](image-url)

*Figure 38: Selecting Object Classes and other auditing settings*
ii. In the case of “Only selected Object Classes”, check the object classes from the list which you want to audit and uncheck those, which you do not want to audit.

iii. In the case of “All but excluding selected object classes”, select the object classes which you do not want to audit. These object classes will not be audited.

iv. To sort any list, click its column header to sort the list alphabetically.

v. You can also type a keyword in the top search row to filter the list as per the keyword.

2. Other Audit Settings: In this section, you can choose settings for the domain auditing. It contains the following options:

   a. Audit Failed Logon: Select this option to audit all failed login attempts.

   b. Audit Successful Logon/Logoff: Select this option to audit all logon/logoff attempts. These events will not be collected until the user manually creates a Group Policy Object on the targeted server.

5.1.2.2.1 Generate Logon/Logoff Script

Lepide Data Security Platform needs the Administrator to generate a logon/logoff executable file from solution and add it using a Group Policy Object at the domain controllers of which logon/logoff events have to be monitored. Once “Audit Successful Logon/Logoff” option is enabled, you have to perform the following steps.

1. Click icon to show the following dialog box.

   ![Figure 39: Dialog box to generate logon/logoff script](image)

2. Enter "IP Address" of the domain controller on which you have installed Logon/Logoff Audit Module.

3. Click icon to select a location, on the server, to save the script file.
We recommend to save the executable file in the shared folder on the server, of which logon/logoff events you want to monitor.

4. Select the folder and click "OK".

5. It takes you back to the previous dialog box, which now shows the selected folder.

6. Click "OK" to generate the executable file and to save at the specified location. You receive the following message box confirming the same.

7. Click "Please follow the link" to know the steps to be performed at the server. It opens an HTML file in the default Web Browser.
Refer to the enable logon/logoff monitoring guide to know the steps that have to be performed on a domain controller.

5.1.2.3 Archive Database Settings

Here, you can configure and schedule the automatic archiving of auditing logs stored in the main database. Database archiving can also be performed manually at any moment by right clicking on the domain and selecting 'Archive Now' option.

In both cases, you can also set to preserve or remove the archived logs in the main database.
To perform Archive Database Settings, follow the steps mentioned below:

1. Select the 'Archive Audit Data' checkbox.

**NOTE:** Click icon to load the database settings from “Default SQL Server Settings”.

2. Now select SQL Server by using “Browse” button or enter its name manually.
3. Select either Windows Authentication or SQL Authentication. We recommend to select SQL Authentication and provide the username and password of a SQL user.

**NOTE:** Here, the selected user should have "sysAdmin" role in SQL Server. [Know more...]

4. Provide the name of the database where archived logs will be stored.
5. Test SQL Server connectivity to ensure successful archiving.
6. Now select the schedule for automatic archiving. Choose from:
   a. Monthly: Select dates to run the archive process on the specified dates in a month.
   b. Weekly: Select days to run the archive process on the specified days in a week.
7. Select the archive start time.
8. Provide the age of the log, in days, after which the log will be eligible for archiving.
9. Select ‘Delete records from production database after archiving’ checkbox to remove the archived logs from the main database after archiving. It helps to limit the size of the main database.

Once you have completed all the steps to add the domain through Express or Advanced Configuration, you can click “Finish” at the end to complete this process. A message box to restart the solution appears on the screen.

Click ‘Yes’ to restart the solution. After restarting the solution, both “Radar” and “Health Monitoring” Tabs shows a new tab for the newly added domain. Following is a screenshot of Domain Radar Tab.

Switch to ‘Settings’ tab and click ‘Component Management’. The added domain is listed in the tree in the right panel.
Domain Management lets you manage and remove the listing of the domains. Here, you can uninstall the auditing agent, configure the auditing, reinstall the auditing agent, and manage health monitoring.

Figure 46: Domain Management in Settings Tab
5.1.3 Active Directory Cleaner

While adding a domain or modifying an already added domain, the option of "Active Directory Cleaner" is available in "Advanced Domain Configuration".

You have to enable "Active Directory Cleaner" to activate this feature. Once enabled, you can click the adjacent icon to open its settings.
You can click the "Advanced Server Settings" link to select the domain controllers for which you want to enable Active Directory Cleaner.
Check the box of domain controllers to enable the cleanup feature for them. Uncheck the domain controllers where this feature is not required.

Click "OK" to apply the settings. It takes you back to the same wizard. Here, you have to provide the following details.

1. **Organizational Unit**: You have to select the Organizational Units for which the alerts will be generated. You can select "All" to select all Organizational Units.

   ![Figure 50: Option to select Organizational Unit](image)

   Click the icon to select the Organizational Units.
You can check the boxes of Organizational Units to enable the cleanup for them. Uncheck the OUs where this feature is not required.

Click "OK" to apply the settings. It takes you back to the previous wizard, which now displays the selected Organizational Units.

2. **Set Time**: Select the time at which either the action is performed, or the notification through email will be sent.

3. **Notification Settings**: This section lets you configure the notification settings. It contains the following options.
   a. **Sender’s Email Account**: Select the email account from which you want to send the alert emails. The added email accounts of "Message Delivery Settings" will be listed here in the drop-down menu. You can also click the icon to add another account.
   b. **Recipient Email Address**: Enter the email addresses of the recipients to which you want to send the notifications about the inactive accounts, their inactive period, and actions taken on inactive accounts.
4. **Action Settings**: Here, you can configure the action settings.

   a. **Select Action Template**: It allows you to perform some actions such as random password setting, disabling accounts, moving accounts to a particular OU, and deleting accounts, after specified number of days. You can also set notifications to inform administrator as and when the application automatically performs these actions.

   i. **Create Action Template**: By default, "Do not perform any action" is selected here. You can click + icon to add a new action template using the following dialog box.

   ![Action Template Settings](image)

   **Figure 52: Creating an Action Template**

   Follow the steps below to create a new template.

   - Select “New” in “Select Action Template” drop-down menu.
   - Provide a name for the Action Template in "Template Name" textbox.
   - Select the account types to apply the action on them.
     - **User/Computer**: Select it to apply the action on both user and computer accounts.
     - **User Only**: Select it to apply the action only on user accounts.
     - **Computer Only**: Select it to apply the action only on computer accounts.
Follow the steps below to exclude the accounts from the action.

- List the accounts that have to be excluded from cleanup operations. "Administrator" is by default excluded from the cleanup.
- You can click + icon to add other accounts.

![Select Account to Exclude](image)

*Figure 53: Excluding the Users from AD Cleanup*

- All user and computer accounts are listed in the left column "Account Name". You can select the accounts to be excluded from the inactive list and button.
You can click \[
\text{\textless} \ \text{\textgreater}
\]
to remove the selected account from the exclusion list.

Click “OK” to apply the settings.

Select any of the following actions. You have to specify the inactivity period to some days for each option.

- Set Random Password After: Select this option to apply a random password to the inactive account.
- Disable Account After: Select this option to disable the inactive account.
- Move to OU After: Select this option to move the inactive account to an Organizational Unit. You can select the Organizational Unit where the account will be moved.
- Delete Account After: Select this option to delete the inactive accounts.

Click \[
\text{\ldots}
\]
icon to access a dialog box for selecting the Organizational Unit where the inactive accounts will be moved.
Here is a screenshot of an action template.

**NOTE:** For each action, you can select “Notify Administrator” option to send notification to Administrator about the action taken on inactive account.

![Action Template Settings](image)

*Figure 56: Creating a new template*

i. **Edit Action Template:** Click icon to modify the selected action template using the following dialog box. You can change the actions to be taken on inactive accounts and set them for users, computers, or both. You cannot change the template name.

iii. **Delete Action Template:** Click icon to remove the selected template.

5. **Send Daily Reports:** Check this option to send the daily reports of inactive accounts. Unchecking it lets the solution not to send any inactivity reports. You can check this option to access its following settings.

a. **Inactivity Period:** In the option “Select Account Inactivity Period”, you have to provide the number of days after which an account will be termed as "Inactive Account".

b. **Email Template:** Here, you have to specify the email template using which the alert email will be sent to the recipients. You can use the default email template, modify it, or create a new custom one.
i. Create Email Template: Click \( + \) icon to add a new email template using the following dialog box.

![Add Template Settings](image)

Create or modify alert template by selecting the information to be included in the alert emails.

- **Template Name**: 
- **Select**: Column Name
  - SAM Account Name
  - Account Type
  - Distinguished Name
  - E-Mail
  - Last Logon Time
  - Inactivity Time (In days)
  - Account Age (In days)

![Figure 57: Adding new Alert Email Template](image)

Follow the steps below to add a new email template.

- Provide a name for the template.
- The bottom part lets you select the columns, which will be added in the email.
- Check the boxes of information that has to be included, whereas you can uncheck the boxes to exclude them.
- Click "OK" to add the template.

ii. Modify Email Template: Select a template from the drop-down menu and click \( \penknife \) icon to modify it. You can change the columns to be included in the email template.

iii. Delete Email Template: Click \( \times \) icon to remove the email template.

Following is a screenshot of the sample details filled in "Active Directory Cleaner Settings."
Click "Apply" to apply the Active Directory Cleaner Settings. The following message box appears to confirm the successful configuration.

Click "OK" to complete the process of configuring the Active Directory Cleaner.
5.1.4 User Password Expiration Reminder

While adding a domain or modifying an already added domain, the option of "User Password Expiration Reminder" is available in "Advanced Domain Configuration".

You have to enable "User Password Expiration Reminder" to activate this feature. Once enabled, you can click the adjacent icon to access its settings.
Follow the steps below to configure this setting.

1. Select Organizational Units: Here, you have to specify organizational units on which this configuration will be applied. The default value is "All".
   
   Click icon to select the organization unit on which you want to apply the password expiration reminder. The following dialog box appears.
Check the boxes of Organizational Units for which you want to enable this feature. You can uncheck the boxes to exclude them.

Click "OK" to go back to the previous wizard.

2. Select Time: You can select the time at which you want to send the password expiration reminder alerts to the users.

3. Notify Administrator: In this section, you have to specify the settings to notify the administrator. Select the number of days in which the passwords of users are going to expire.
Enter the email addresses of the recipients, who have to be notified about the list of users whose passwords are going to expire.

You can select the alert email template for the administrator. It contains the following options.

A. Click \+ icon to add a new email template using the following dialog box.

Perform the steps below to configure the email template:

i. Enter the name for the new template.

ii. The bottom part lets you select the columns, which will be added in the email. Check the boxes of information that has to be included, whereas you can uncheck the boxes to exclude them.

iii. Click "OK" to add the template and go back to the previous wizard.

B. You can select an email template and click \- icon to modify it.
You can change the columns to be included in the email template. Click "Modify" to apply the changes.

C. Click \( \times \) icon to remove the selected email template.

4. Notify Users: Here, you can configure the settings to notify the users whose passwords are going to expire.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyday if password expires in:</td>
<td>14 days</td>
</tr>
<tr>
<td>Send first notification when password expires in:</td>
<td>14 days</td>
</tr>
<tr>
<td>Send second notification when password expires in:</td>
<td>7 days</td>
</tr>
<tr>
<td>Send last notification when password expires in:</td>
<td>3 days</td>
</tr>
<tr>
<td>Only when password expires in:</td>
<td>1 day</td>
</tr>
</tbody>
</table>

**User Notification Text:**

Hi %USERNAME%,

Your password will expire in %DAYS%. Please change the password as soon as possible to prevent further logins.

Thanks,

Administrator

---

Note: Use %USERNAME% for user name and %DAYS% for password expiration days.

*Figure 65: Options to notify the user*

It contains the following options.

a. Everyday if password expires in: Select this option to send the notifications every day to the users whose password is going to expire in the specified number of days.

b. Send Notifications: Select this option to send only three notifications to the users at different intervals. It has the following options.
   i. Send first notification when password expires in: First notification will be sent when the password is going to expire in the specified number of days.
   ii. Send second notification when password expires in: Second notification will be sent when the password is going to expire in the specified number of days.
   iii. Send last notification when password expires in: Third and last notification will be sent when the password is going to expire in the specified number of days.

c. Only when password expires in: Select this option to send a notification only when the password is going to expire in the specified number of days.

d. User Notification Text: It contains the text, which will be sent to the users in the notifications. You can modify the text as per the requirement. Use %USERNAME% code for usernames and %DAYS% for the number of days after which the password is going to expire.

Following is a screenshot of the configured settings.
Click “Apply” to apply User Password Expiration Reminder settings. The following message box appears to confirm the successful configuration.

Click “OK” to go back to the previous wizard of adding or modifying the domain.
5.2 Add SharePoint

Before going ahead, make sure that the prerequisites to add SharePoint Server are met. [Know more...]

To add a SharePoint Server for auditing, you need to perform various steps, which include:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharePoint Server</td>
<td>Provide the details of SharePoint Server and the credentials of a user who have required privileges</td>
</tr>
<tr>
<td>Interlinked SQL Server</td>
<td>Provide the details of SQL Server, that is interlinked with SharePoint, and the credentials of a user who have required privileges in SQL Server</td>
</tr>
<tr>
<td>(Optional) Site Collection Settings</td>
<td>Select the sites or Central Administration to be audited</td>
</tr>
<tr>
<td>Database Settings</td>
<td>Provide SQL Server details</td>
</tr>
<tr>
<td>(Optional Step) Archive Database Settings</td>
<td>Turn on archiving and configure its options</td>
</tr>
</tbody>
</table>

*Figure 68: Steps to add a SharePoint Server for auditing*

Select “SharePoint” option in “Component Selection” dialog box or “Add” submenu in the right-click upon “Component Management” node. You can also click “SharePoint” button in “Add Component” section of “Component Management”.

Follow any of the above methods to access “Add SharePoint Server” wizard.
5.2.1 SharePoint Server Details

1. This step has two sections:
   a) SharePoint Details: In the SharePoint Details section, provide Central Administration URL, IP Address, username and password.
      Provide the username in this format - ‘Domain\User’ or ‘Workgroup\User’.
Refer to the following note for 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” link.
   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.
2. 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 box.
6. Type the username and click "Check Names" button to validate the entry.
7. Click "OK" to add the user. It takes you back to the policy properties.
8. Click "Apply" and "OK".
b) SQL Server Details: Enter SQL Server Name manually or click 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.

2. We recommend to click “Test Connection” button to check if a successful connection to SQL Server can be established or not.
3. Click "Next" once you are done.

5.2.2 Install SharePoint Auditing Agent

4. The solution starts installing the agent on SharePoint Server for auditing.

![Figure 70: 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. Kindly install them both from "Redist" folder of program installation folder.

![Figure 71: Error in connecting to SharePoint]

**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 sysadmin role is not assigned to it.

Create the login of SharePoint User with Windows Authentication and sysadmin role in SQL Server for the content database.
5.2.3 Site Collection Settings

5. Here, the list of all Sites on SharePoint is displayed. You can select the sites that you want to audit.

6. **Site Selection**: This drop down menu has the following options.
   - **All**: Select this option if you want to audit all Site Collection(s).
   - **Exclude**: Select this option if you want to audit all but few Site Collection(s).
   - **Include**: Select this option if you want to audit a few SiteCollections.

   Follow the steps below.
   
   a. Selecting include or exclude option enables the section to select the sites for auditing.
   
   b. Check the boxes of the sites in “Include” that has to be included in the auditing. Similarly, you can select the sites in “Exclude” to exclude them from auditing.

   Alternatively, you can click [ icon to select all sites, whereas click [ icon to deselect all sites.

   You can click [ icon to refresh the list of all sites at SharePoint Server.

5.2.4 Database Settings

8. Enter the name of SQL Server in which you want to configure your database.

You can also click icon to enumerate all local and remote SQL Servers in the network and then select an SQL Server.

9. Authenticate the SQL Server configuration by either way:
   • Windows Authentication: Choose this option to allow the solution to access SQL Server using the credentials with which the user is currently logged in.
   • SQL Server authentication: Provide SQL server username and password to allow the solution to access the server using SQL authentication.

   **NOTE:** Here, the selected user should have “sysAdmin” role in SQL Server. **Know more...**

   We recommend to select “SQL Server Authentication.”

10. Click “Test Connection” to check the connection status.
11. Enter database name to store the audit logs.

12. Click “Next” to proceed.

5.2.5 Archive Database Settings

13. You can skip this optional step if you do not want to archive the audit data.

We have already discussed this configuration in the section to add a domain. Refer to 5.1.2.3 Archive Database Settings to know more.

The solution asks for your permission to restart the solution.
Click “Yes” to restart the solution.

After the restart, a new tab for SharePoint Server is created in “Radar” Tab.

Once added, you can switch to “Settings” Tab → “Component Management” to manage the added SharePoint Server.
SharePoint Server Management lets you manage and remove the listing of SharePoint Server. Here, you can uninstall the auditing agent, configure the auditing, and reinstall the auditing agent.

### 5.3 Add SQL Server

Before adding a SQL Server for auditing, make sure its prerequisites are met. Know more...

To add a SQL Server, you need to perform various steps, which include:
Select "SQL Server" option in "Component Selection" dialog box or "Add" submenu in the right-click upon "Component Management" node in "Settings" tab. You can also click "SQL Server" button in "Add Component" section of "Component Management".

Follow any of the above methods to access this 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.

### 5.3.1 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.
5.3.1.1 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 have to select either Windows Authentication or SQL Server Authentication. We recommend to select the latter option.
5. Enter the name and password of an 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.

**Case 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 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 local system administrator or domain administrator, with which you are running Lepide Data Security Platform Service.
i. Switch to “Server Roles” and select “sysAdmin”.
j. Click “OK”.

**Case 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 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 Status page, select Grant and Enabled.
k. Click “OK”.

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

Perform the following steps to configure the database settings.

1. 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.
2. Select the authentication type, preferably “SQL Authentication”.
3. Enter the login credentials of an SQL administrative user.

**NOTE:** Here, the selected user should have “sysAdmin” role in SQL Server. Know more...

4. Enter the name of the database in which the auditing logs will be stored. You can provide the name of the same database used earlier to store the auditing logs of the domain or SharePoint. Following screenshot displays the sample details.

![Sample Details for Database Settings](image)

**Figure 81: Sample Details for Database Settings**

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

5. Click “Test Connection” to test the connection to SQL Server.
6. Click “Finish”.

© 2020 Lepide Software Pvt. Ltd. Page 83
5.3.2 Add SQL Server with Advanced Configuration

In the following wizard, you have to select “Advanced Configuration” option.

Click “Next”.

The following steps are common in adding SQL Server using Express Configuration and Advanced Configuration. They have earlier been discussed in Express Configuration section. You can click the following links to know more.

1. SQL Server Details
2. Database Settings
3. Install SQL Auditing Agent

The remaining steps are discussed in detail hereby.
5.3.2.1 SQL Health Monitoring

The next step displays the SQL Server Health Monitoring Settings.

![Image of SQL Health Monitoring Settings]

Check the box "Enable Health Monitoring" to enable the health monitoring of SQL Server. You have to provide the following details of the computer where SQL Server is installed.

1. **Computer Name**: Enter the name or IP Address of the computer where SQL Server is installed.
2. **User Name**: Provide the name of an administrator user of that computer.
3. **Password**: Enter the password for the above user.

Click "Next" to proceed.

The next step displays "Audit Settings".
5.3.2.2 Audit Settings

At this step, 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 be audited.

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

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

Figure 84: Audit Settings
Check the boxes for the databases to be audited. Unchecked databases will not be audited or monitored.

Click the list button once you are done. The next step shows “Object Settings”.

*Figure 85: Listing all databases to audit*
5.3.2.3 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. Further, 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.

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

2. It will show an arrow. Click the down arrow to access the list of operations.
3. Uncheck the operations that you do not want to audit.

4. Click "OK" to modify the selection of operations for "Login" object.

Click button to proceed. The next page displays "User Settings".
5.3.2.4 User Settings

It has the following options.

1. Audit All Users: Select this option to audit all users.
2. Audit Selected Users: Select this option to enable the "Users" section and enumerate all SQL users in it.
Here, you can check the users to be audited and uncheck others to exclude from auditing. Click “Next” once you are done with User Settings. The next page displays database settings.

5.3.2.5 Archive Database Settings

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.
We have already discussed this configuration in the process to add the domain. You can refer to 9.1.2.3 Archive Database Settings section. 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.

Click “Yes” to restart the solution.

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.
SQL Server Settings are displayed in “Settings” Tab under “Component Management”.

Figure 95: SQL Server Tab in Radar

Figure 96: 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.
5.4 Add Exchange Online

Before going ahead, make sure that the prerequisites to add and audit Exchange Online are met. [Know more...]

To add an Exchange Online Server for auditing, you need to perform various steps, which include:

- **Exchange Online Details**
  - Provide the credentials of a user who have required privileges.

- **(Optional) Mailbox Settings**
  - Select the mailboxes to be audited

- **(Optional) Object Settings**
  - Select the objects to be audited

- **Database Settings**
  - Provide SQL Server details
  - Database created with Platform is preferred
  - Configure interval to collect changes

- **(Optional Step) Archive Database Settings**
  - Turn on archiving and configure its options

![Diagram: Steps to add an Exchange Online Server for auditing](image)

Select “Exchange Online” option in “Component Selection” dialog box or in “Add” submenu of context menu that appears after right clicking upon “Component Management” node. You can also click “Exchange Online” button in “Add Component” section of “Component Management”.

Follow any of the above methods to access “Add Exchange Online” wizard.
5.4.1 Exchange Online Details

It contains the following options:

1. User Name: This field is divided into the following two parts.
   a. User ID: Enter the user ID of your Exchange Online, that comes before "@" character.
   b. Server Name: Enter the name of Exchange Online Serve that comes after "@" character.

**NOTE:** The provided user should be “Exchange Administrator” or “Global Administrator”. If the selected user does not have any of these rights, perform the following steps.

1. Login at Office 365 portal and open Admin Center.
2. Go to “Users”.
3. Either create a new user or edit an existing user.
4. Click "Roles" to change the use role.
5. To make the user global administrator, select "Global Administrator". To make the user Exchange Administrator, select "Customized Administrator" and then select "Exchange Administrator".
6. Click "Save".
2. **Password:** Enter password of the selected user.

Click "Next" to proceed to the next page. The solution tries to verify the user credentials and to connect to Exchange Online. In case of any issue, an error message may appear on the screen. If it successfully connected to Exchange Online using provided credentials of the user, the next page appears on the screen.

### 5.4.2 Select Mailboxes

The next page shows the option to select those mailboxes which you want to audit.

![Option to select mailboxes](image)

In the drop-down menu, you have to select any of the following options.

1. **All Mailboxes:** Click it to audit all mailboxes.
2. **Selected only:** Click it to select only those mailboxes, which you want to audit.
3. **All but Excluding Selected:** Click it to select those mailboxes, which you do not want to audit. All other mailboxes will be audited.

Selecting “Selected Only” or “All but Excluding Selected” lists all available mailboxes. Once any of these options is selected, you have to select those mailboxes can be either included in auditing or excluded from auditing.
Click “Next” after adding all or selected mailboxes for auditing.

5.4.3 Select Objects

The next page shows the option to select those objects which you want to audit.
In the drop-down menu, you have to select any of the following options.

1. All Objects: Click it to audit all objects.
2. Selected only: Click it to select only those objects, which you want to audit.
3. All but Excluding Selected: Click it to select those objects, which you do not want to audit. All other objects will be audited.

Selecting “Selected Only” or “All but Excluding Selected” lists all available objects. Once any of these option is selected, you have to select those objects can be either included in auditing or excluded from auditing.
Click “Next” after adding all or selected objects for auditing.

5.4.4 Database Settings

After selecting the mailboxes and objects to be audited, you have to configure the settings of database to store the audit data.
Perform the following steps here.

1. Enter the name of SQL Server in which you want to configure your database.
   
   You can also click icon to enumerate all local and remote SQL Servers in the network and then select an SQL Server.

2. Authenticate the SQL Server configuration by either way:
   
   • Windows Authentication: Choose this option to allow the solution to access SQL Server using the credentials with which the user is currently logged in.
   
   • SQL Server authentication: Provide SQL server username and password to allow the solution to access the server using SQL authentication.

   **NOTE:** Here, the selected user should have “sysAdmin” role in SQL Server. [Know more...](#)

   We recommend to select “SQL Server Authentication.”

3. Click “Test Connection” to check the connection status.

4. Enter the minutes after which the changes will be collected. The minimum event collection interval is 5 minutes.
5. Enter database name to store the audit logs.
6. Click “Next” to proceed.

5.4.5 Archive Database Settings

Once database settings is configured, you can configure the archiving of audit data that will be stored in the database selected above. However, it is an optional step and you can skip it.

![Archive Database Settings](image)

*Figure 104: Archive Database Settings*

We have already discussed this configuration in the section to add a domain. Refer to 5.1.2.3 Archive Database Settings to know more.

The solution asks for your permission to restart the solution.

![Restart Confirmation](image)

*Figure 105: Asking to restart the solution*
Click “Yes” to restart the solution.

After the restart, a new tab for Exchange Online is created in “Radar” Tab.

Figure 106: SharePoint Server Tab in Radar

Once added, you can switch to “Settings” Tab ➔ “Component Management” to manage the added Exchange Online Server.

Figure 107: SharePoint Server Management
Exchange Online Server Management lets you manage and remove the listing of Exchange Online. Here, you can configure the auditing and remove the Exchange Online from the solution.

6. License Activation

You will be provided with a License ID and a Password in an email as soon as the Sales Representative from Lepide registers you on the management portal. There are basically two methods of activating your licenses:

1. Active Online
2. Activate Offline

6.1 Activating Online

Once you have the credentials, please follow the below steps:

1. Go to the Licensing information page, click on Update License.

![Figure 108: Update License Tab](image)

2. Select "Activate Online" and enter the Licensing ID and Password and hit Update License.
3. Once you click on "Update License" it will show up a pop-up saying, "License information updated successfully". Click OK now.
4. Once you click OK, it will give you a pop-up for restarting the software. Please hit "Yes".

Figure 110: License Activation Online

Figure 111: Complete License Activation
5. Once you restart the software, you will see the column “License Type” is changed to the mode of license you have opted for. This shows your license is active now.

![License Activated Successfully](image)

6.2 Activating Offline

This mode is helpful in activating the license when you don't have an active internet connection on the machine where Lepide Data Security Platform is installed.

1. Go to the Licensing information page, click on Update License.

2. Now select “Activate Offline” and enter the Licensing ID and Password and hit “Generate Request”.

![Update License Tab](image)
3. You will get a pop-up saying, “License request file generated successfully at: Your Desktop”. Just hit “OK”.
4. Now you have two options, either send the file to sales@lepide.com and wait for the activation file. Or, you can activate the licenses yourself. For that, please copy this request file to a computer where internet is available. Open this url: https://secure.softwarekey.com/solo/customers/ManualRequest.aspx You have two options now:
   i. Either paste the content of the license request file into the “Copy and Paste Request” Pane and hit “Submit”.
   ii. Or, you can simply upload the file in the “Upload Request File” pane.

5. Once you click on “Submit”, you will redirected to the following page:
6. Just copy the text from the “Response” pane, or you can also download this content in a file, which you can transport to the Lepide machine and copy the contents. Now paste these contents in the “Response” pane of the solution and hit “Activate”.

Figure 117: License Portal
7. You will be presented with the screen saying, "License Information updated Successfully".

---

**Figure 118: Activate License**
8. Once you click OK, it will give you a pop-up for restarting the software. Please hit "Yes".

Figure 119: License Information Update

© 2020 Lepide Software Pvt. Ltd.
9. Once you restart the software, you will see the column “License Type” is changed to the mode of license you have opted for. This shows your license is active now.
7. Settings

“Settings Tab” is the centralized control panel of Lepide Data Security Platform, which allows you to perform all required settings to configure and use the solution. Its settings are divided into the following categories.

- Component Management
  - Domain Settings
    - Active Directory plus Group Policy Objects
    - Exchange Server
    - User Password Expiration Reminder
    - Active Directory Cleaner
  - SharePoint Server Settings
  - SQL Server Settings
  - File Server Settings – It opens a separate dedicated console to add and manage File Server.
  - Exchange Online Settings
  - Console Auditing Settings
- General Settings
- Delegation Control
- Current Permission Scan Settings
- Delivery Message Settings
  - App Profile Management
  - Alert Profile Management
  - Email Account Management
- Default SQL Server Settings
7.1 Component Management

Here, you can add/remove/modify the added server components, and configure/install/uninstall their auditing agents. There is also an option to uninstall the auditing agent from a not added component.

You can add and manage the domain, SQL Server, SharePoint, and Exchange Online. However, a separate dedicated console is also added to add and manage File Server Auditing of Windows File Server and NetApp Filer. You can refer to the different dedicated guide for configuring File Server Auditing.

![Component Management](image)

Figure 122: Component Management

This tab’s interface is divided into two sections – “Add Component” to add a new component and “Added Component” to manage already added components.

We have already discussed the steps to add the server components. You can refer to the following sections to modify and remove the added server components.

a. Modify Component

b. Remove Component

7.1.1 Console Auditing Settings

Console Auditing lets you audit the user actions performed on the console of Lepide Data Security Platform. A separate report named “Console Auditing” has been added in “Audit Reports” Tab. It throws the following error message if its settings are not configured.
You have to perform the following steps to enable and configure the Console Auditing.

1. Right-click "Component Management" node in "Settings" Tab.

2. Click "Console Auditing" to access the following dialog box.
3. Check the box of “Enable Console Auditing” to enable the next section of database settings.

NOTE: You can click icon to load the settings from "Default SQL Server Settings".

4. The solution lets you connect to a local or networked SQL Server. You can either enter the name of SQL Server manually in the text box or click icon to enumerate all SQL Servers in a list and select the desired one.

5. You have to provide the following inputs.
   A. Authentication Type: Select any of the following authentication types.
      I. Windows Authentication: It lets the solution login at SQL Server using the credentials of that user with which you are logged into the computer currently.
      II. SQL Server Authentication: It lets the solution login to SQL Server using the credentials of an SQL user.

      We recommend to use the SQL Server Authentication.
   B. Login Credentials: Provide the name and password of an SQL user in case of SQL Authentication.

      NOTE: Here, the selected user should have "sysAdmin" role in SQL Server. Know more...
   C. Database Name: Provide a database name that will store the console auditing logs. If you are reinstalling the solution, then you can reuse the earlier database.

6. Click button to test the connection between the solution and the selected SQL Server using the provided details. It either displays an error if failed to connect or shows the following message confirming the successful connection.

    ![Test Connection Success](image)

    Figure 126: The connection to SQL Server is successful

7. Click "OK" to save the settings.

Once, Console Auditing is enabled; you can go to "Audit Reports" section to view its report.
7.2 General Settings

You can configure the general settings to customize the solution.
General Settings is divided into the following three sections:

7.2.1 Display Settings

i. Maximum Records per Page: Select the maximum number of records that you wish to be displayed on each page of the report.

ii. Date/Time Format: Specify the date and time format from the available options in the drop-down list.

iii. Dashboard Refresh Interval: It specifies the refresh interval, after which the Radar Tab recollects the changes made in the server components and updates its graph widgets and views accordingly.

7.2.2 Retention Settings

This section lets you define the interval after which the relevant records will be deleted. These retention settings are quite necessary to keep the space free on the disk drive where the software is installed or where the software is saving the backup snapshots.

1. Schedule/Alert Report Retention Settings: It defines the interval after which the records of already sent alerts and schedule reports will be deleted from the software. Check this option to enable it. Once enabled, you have to define the select its value from the following options.

   a. 7 days
   b. 15 days
   c. 30 days
   d. 60 days
   e. 90 days

   **NOTE:** The records of alert and schedule report will be marked for retention either after three hours of its creation or whenever Lepide Data Security Platform Service restart. Once this service is running, the software scans for the age of these records every three hours and enables the retention for the eligible records.

2. Active Directory/Group Policy Backup Retention Settings: It defines the interval after which the complete backup of the state of Active Directory Objects and Group Policy Objects will be deleted. Check this option to enable it. Once enabled, you have to define the select its value from the following options.

   a. 3 Months
   b. 1 Year
   c. 2 Years
   d. 3 Years
   e. 4 Years
   f. 5 Years
   g. 6 Years
7.2.3 Other Settings

This section contains the following settings.

3. Maximum number of concurrent session (Active Directory): This setting is applicable only for Active Directory and Exchange Online. There can be one session for one domain controller (in the added domain) or one instance of Exchange Online (added to software). If multiple instances of domain controllers and Exchange Online are added, then number of concurrent sessions should be equal to those number of domain controllers/Exchange Online instances, which is larger.

For example, if there are 15 domain controllers and 5 instances of Exchange Online are added, then number of concurrent sessions will be equal to 15 instead of (15+5=)20.

4. Maximum File Size of Logon/Logoff Database: Lepide Data Security Platform creates a SQL Server Database in the installation folder to retain the raw format of the logon/logoff events received from Lepide Logon/Logoff Audit Module. Once stored in this database, the software processes these logs and saves them permanently in the provided auditing database.

Here, the user can define the maximum size of Logon/Logoff Database that stores raw formats of logon/logoff events. Once the maximum size is reached, the software removes the old logs at 12:00 AM on the first Saturday of every month. If WMI runs successfully, then the software removes all logs except the event logs of current active logon/logoff sessions. If WMI does not run, then the software removes 90% of the specified maximum size including that 25% of logs, which was collected within the last 30 days.

5. Do not send scheduled reports, if blank: Select this checkbox if you do not want scheduled report recipients to receive a blank report without any data.

6. Don't capture “From” information (Active Directory): You can check this option to disable the capturing of "From" field while auditing Active Directory.

Unchecking this option enables the capturing of this particular field in Active Directory auditing logs.

7. Encrypt the data in the Archive Database: You can enable this option to enhance the security of logs stored in the archive database.

8. Allow multiple instances of the console: Check this option to run multiple instances of Lepide Data Security Platform either by the same logged on user or by different users logged on at the same computer. If you want to run only one instance of the solution at a time, then uncheck this option.

7.3. Delegation Control

Web Console of Lepide Data Security Platform lets the domain users access the audit reports from anywhere in a domain's network.

"Delegation Control" lets the administrator create accounts for the domain users to access Web Reports and select what reports they can access.
Here, the Administrator can add, edit, delete, enable, and disable the user accounts, using which domain users can access Web Report Console.

Follow the below steps to add a new delegation account.

1. Click the + icon to create a new account. It shows the following wizard.

2. Enter the account name in the textbox.
3. Click the icon to add the user(s) who can use this account to login to Web Report Console. It shows the following dialog box.

![Add User Dialog Box](image1.jpg)

*Figure 131: Dialog box to add the users*

4. Click the button to select the users from Active Directory. It shows the following dialog box.

![Select Users Dialog Box](image2.jpg)

*Figure 132: Dialog box to select the users from Active Directory*

5. Enter the name of the user to be added. You can type multiple usernames separated with ; (semicolon).

6. You can also click "Advanced" to search in Active Directory and select the users.

7. Click "Check Names" to validate the entered username(s).

8. Click "OK" once you have added the required users. It takes you back to "Add Users" box that now shows selected AD user.

![Add User Dialog Box](image3.jpg)

*Figure 133: Showing the user to be added*

9. Click "OK" to add the selected user in the list. It takes you back to "Add Delegate Account" wizard.
To remove a user from the list, select it and click the icon. It displays a warning message, where you have to click "Yes" to delete its name from the list.

10. Click "Next" to proceed ahead. The next step gives you the option to select the reports for which you want to authorize the account.

11. "Delegate" drop-down menu has the following options.
A. All Reports: Select this option to authorize the new account to access all audit reports.
B. Only Selected Reports: Select this option to choose what reports the new account can access and what cannot.

![Select Report(s)](image)

**Figure 136: Select the reports for which account will be authorized**

12. Select the reports, which are divided into three different categories.

A. SQL Server: It shows the auditing reports for SQL Server.
B. SharePoint: It shows the auditing reports for SharePoint Server.
C. Domain: It displays the reports for the domain. It is further divided into the following categories.

   I. Active Directory Reports: It shows the following reports of Active Directory.
      a. Active Directory Modification Reports
      b. Active Directory Security Reports
      c. Active Directory Custom Report
   II. Group Policy Reports: It displays the following reports of Group Policy.
      a. Group Policy Modification Reports
      b. Group Policy Custom Reports
   III. Exchange Server Reports: It displays the auditing reports of Exchange Server.

13. Select the reports for which you want to provide access to the delegation account.
14. Click "Finish" to create the account.

You can follow the above steps to create multiple accounts. Delegation Control displays all created accounts in the list.
In addition to create an account, the following are other options available in "Delegation Control".

- Use this icon to remove an added delegation account.
- Use this icon to modify details in a delegation account. Just select the account from the list and click this icon. Change the required values and click "OK" to apply the changes.
- Use this icon to refresh changes and display the latest changes in the Delegation Account list, if any.
- Use this icon to disable an existing delegation account.
- Use this icon to enable an existing delegation account.
7.4. Current Permission Scan Settings

You can use Current Permission Scan Settings to create the Data Set containing those folders, of which current permissions you want to monitor.

After configuring SQL Server, Administrator can add, edit and delete the object lists.

7.4.1 Configure SQL Server

Follow the steps below to configure SQL Server Settings for accessing Current Permissions.

1. Click icon to configure the server. It displays the following dialog box.
2. The solution lets you connect to a local or networked SQL Server. You can either enter the name of SQL Server manually in the text box or click ⋮ icon to enumerate all SQL Servers in a list and select the desired one.

3. You have to select any of the following authentication types.
   a. Windows Authentication: It lets the solution login at SQL Server using the credentials of that user with which you are logged into the computer currently.
   b. SQL Server Authentication: It lets you provide the username and password of an SQL Server user.

NOTE: Here, the selected user should have "sysAdmin" role in SQL Server. 

4. You have to provide a database name in the text box saying “Database”. If you are reinstalling the solution, then you can reuse the earlier database.

NOTE: The software does not create this database until you add a Data Set and start its scanning.

5. Click Test Connection to test the connection between the solution and the selected SQL Server using the provided details. It either displays an error if failed to connect or shows the following message confirming the successful connection.
6. Click "Apply" to save the database settings. It takes you back to "Current Permission Scan Settings" that shows the details of selected SQL Server and database.

7.4.2 Stale Object Settings

Stale Objects are those objects, which are not accessed for a long time. You can use the drop-down menu to define the time limit after which a not accessed object can be defined as a Stale Object. The drop-down menu contains the following options. You can select anyone of them. The selected option is applicable on all Data Sets.

- 7. 30 days
- 8. 90 days
- 9. 180 days
- 10. More than 365 days

If all objects are being displayed as Stale Objects or status of stale objects is not being displayed correctly, then it means that the date/time of the last access or modification to a file/folder is not updated. File Server does not modify the last access date and time of the modified/accessed files and folders, by default. You have to enable a certain property to get this information precisely.

Follow the steps below to modify this system property and to get the exact last access date and time.

1. Run the Command Prompt as Administrator.
2. Click "Yes" if "User Access Control" dialog box appears.

3. Execute the following command at the Command Prompt.

   \texttt{fsutil behavior set disablelastaccess 0}

Here, value '0' is provided to disable the last access. You can provide '1' to enable the last access.

### 7.4.3 Available Options

Let us have a look at the available options to manage the data set.
7.4.3.1 Add Data Set

Click icon to create a Data Set using the following wizard.

NOTE: Database, configured above, will not be created until you add a Data Set and start its scanning.

Follow the steps below.

1. Enter the name and description of the Data Set.

2. Click "Next". The next step displays the options to add the shared folders, of which current permissions you want to monitor.
3. The default component is File Server, which is already selected in the drop-down menu.

4. You can perform the following steps to add folders.
   a. Click icon to add the folders using the following dialog box.

   ![Add Data Set Dialog Box](image)
b. Select the File Server from the drop-down menu. It lists the folders in the left column "File Server folders".

**NOTE**: Please do not add the shared folders of the file servers of the different domains in a Data Set. We recommend to create a Data Set from the file server(s) of a single domain only.

c. You can expand the nodes to select the folders.

**NOTE**: The user, using which File Server is added in the software, should have "Full Control" or at least "Read" rights to read the permissions of the shared folders and its content. If that user did not have even these privileges, then the scanning to read the rights will fail with an error.

d. Select a folder and click > button to add it.

e. Check "Include child objects" to monitor the permissions of sub-folders and files of the selected folder as well.
To remove an added folder from the Data Set, select the folder in the right column and click the button.

Click "OK" once you are done.

It takes you back to the previous wizard, which shows the added folder. The current permissions of the added folders will be monitored.
5. Click "Next". The next step displays the options to scan the permissions of the selected objects.
6. It contains the following options.
   a. **Scan Permissions Now**: Select this option to scan the permissions now.
   b. **Schedule Permission Scan**: Select this option to schedule the scanning of permissions on different periodic intervals. Once “Schedule Permission Scan” box is checked, it activates the subsequent section. Follow the steps below,
      i. Click “Change Schedule” button to access the following dialog box.
It contains the following options.

- **Daily**: Select this option to scan the folders on a daily basis for updating the permissions. Once selected, you have to select the start date and time, from which the scheduling will be created.

- **Weekly**: Select this option to scan the folders on a weekly basis. You have to select the start date from which the scheduling will be started. Select the days and time at which the scan will run.

- **Monthly**: Select this option to scan the folders on a monthly basis. You have to select the start date from which the scheduling will be started. Provide the time at which the scan will run. Select the months and their days when the scanning has to be scheduled.

ii. Select any of the above options and provide the required inputs.

iii. Click "OK" once you have defined the schedule. It takes you back to the previous wizard, which displays the scheduled days and timings for the scan.
c. **Login Credentials:** The solution also fetches the permissions from any Domain Controller, which hosts Active Directory.

   The solution, at first, uses the login credentials that are provided while adding a File Server. If these credentials fail to authenticate the request, then the solution uses the credentials provided here.

   Enter the name of the domain controller.

   If you have selected “This user” while adding the File Server, then the provided login credentials are reflected here as-it-is.

   Otherwise, you have to enter the login credentials of an administrative user manually. The provided user should be a member of “Domain Admins” group.
The solution collects the nested group membership and permissions using the provided credentials.

7. Click “Finish” once you have selected the option to scan the permissions. It creates a new Data Set.

You can follow the above steps to create multiple Data Sets.
7.4.3.2 Scan Permissions Now

Right-click on a data set and click “Scan Now”. It lets you scan the permissions of the selected Data Set.

![Figure 155: Option to scan the permissions](image)

7.4.3.2 Modify Data Set

Select a Data Set in the list and click icon to modify the selected Data Set with the following dialog box.

![Figure 156: Wizard to modify the Data Set](image)

The steps to modify a Data Set is the same as you have performed while adding it. It contains the following options.

1. **Data Set Information**: You can change the description of the Data Set; however, you cannot change its name.
2. **Select Object(s)**: Click this link in the left panel to access its settings. You can remove the listing of the already added folder and add new folders.
3. **Permission Scanning Options**: Click this link in the left panel to access its settings. You can change the update method and modify the scheduling of permission scan.

Click "OK" at any option to save the changes in Data Set.
7.4.3.3 Remove Data Set

If the data set is deleted, the solution does not show the current permissions of the folders and its content added in the data set. The information of Data Set and its scanning from the SQL Server Database is also removed. And there is no other way to retrieve it back.

Follow the steps below to remove a Data Set.

4. Select a Data Set from the list and click the icon to remove the selected Data Set. The solution displays the following warning message.

```
LepideAuditor Suite

Do you want to delete selected data set?

Yes  No
```

*Figure 159: Warning before you delete a Data Set*

5. Click “Yes” to remove the selected Data Set

7.5 Message Delivery Settings

This setting allows you to define the medium of sending delivery notifications like auditing alerts’ messages, health monitoring alerts’ messages and scheduled reports.

*Figure 160: Message Delivery Settings*
There are two methods to send the delivery notifications and the third one lets you select the user account to run the customized script.

1. Email Account: It lets you send the alerts through email.
3. Alert Profile Account: It lets you provide the credentials of a user account with which the user-selected customized script will run.

### 7.5.1 Email Account

The solution lets you add email accounts, modify existing accounts and remove email accounts. The added email account(s) are used to send real-time alerts and scheduled reports.

To add an email account, click the button.

![Figure 161: Option to add an email account](image)

Select “Add Email Account” option to access the following dialog box.
Enter the following details:

1. Display Name: Provide a name that will be used as the profile name.
2. Sender's Email ID: Enter the email address that will be used to send emails.
3. Requires authentication: Uncheck this option if your Exchange Server does not require authentication.
   You can check this option if the SMTP Server requires authentication. Once checked, you have to provide the following login credentials.
   a. Logon Name: Enter the login name for your email address. This name will be used by the solution, on your behalf, to login to the provided Email Server.
   b. Password: Provide the required password for the provided logon name.
4. Server Name: Enter the server name or IP Address of your email ID. The solution will use this value to find out the email server and ping it.
5. Port: Enter the port number for SMTP connection (the default port number is 25). The solution will try to connect to SMTP Server at this port.
6. Requires a secure connection (SSL): Check this box if you want the solution to connect to your email server using SSL.
7. Send Test Email: Use this option to send a test mail to check the authenticity of the details provided here. We recommend to perform this step before moving ahead.
7.5.2 App Account

An App Account sends the delivery notifications to Lepide Data Security Platform App, mobile application available for Android and Apple devices. The solution lets you add, modify and delete app accounts. To add an app account, click the button.

Click "Add App Account to access the following dialog box.

Enter the following details and click "OK".

1. User ID: Provide a user ID with which you will create a profile in Mobile Application.
2. Password: Enter the password for the user ID with which you will login in Mobile Application.
3. Mobile App ID: Note down the Application ID and use it to create the profile in a mobile application.

You can add more app accounts for apps installed on multiple devices. However, one account should be used for only one application.
7.5.3 Alert Profile Account

An Alert Profile Account stores the credentials (username and password) of an Active Directory user account that lets you run the script. Lepide Data Security Platform uses the created alert profile to use the credentials for executing a script associated with an alert, in which any script is selected to execute whenever the selected change is detected. For this purpose, the user is first required to add an alert profile in the software. The solution lets you add, modify and delete app accounts. To add an app account, click button.

![Option to add an App Account](image)

Click "Add Alert Profile" to access the following dialog box.

![Dialog box to add an App Account](image)

Enter the following details and click "OK".

4. **Profile Name**: Enter the name of profile that stores the provided login credentials.
5. **User Name**: Enter the name of a domain user in the following format.
**Domain\Username**

**NOTE:** Please make sure that the provided user have full rights to run the script and to perform actions mentioned in the script. If the provided user does not have required rights, the action mentioned in the script will not be displayed.

6. **Password:** Enter the password of above user.

You can add more app accounts for apps installed on multiple devices. However, one account should be used for only one application.

### 7.5.4 Other Options

Following are other available options to manage App or email account.

- ✕ Use this icon to remove an added account
- ✏️ Use this icon to modify details in an existing account. Just select the account from the list and click on this button. Change the required values and click "OK."
- 🔁 Use this icon to refresh changes and display the latest changes in the account list, if any.
- 🌐 Click this icon to configure the App Server Settings.

![LepideAuditor App Data Settings](image)

**Figure 167: App Data Settings**

Here, you have to enter the public IP Address of the system, where you have installed Lepide Data Security Platform App Server. Make sure to allow Port 1051 for all incoming and outgoing connections in Firewall, on the system where Lepide Data Security Platform App Server is installed. [Know more]...
7.6 Default SQL Settings

This setting lets you configure the default SQL Server for storing the auditing logs.

Follow the steps below to configure this setting,

1. The solution lets you connect to a local or networked SQL Server. You can either enter the name of SQL Server manually in the text box or click ▼ to enumerate all SQL Servers in a list and select the desired one.
2. You have to select any of the following authentication types.
   a. Windows Authentication: It lets the solution login to SQL Server using the credentials of that user with which you are logged in to the computer currently.
   b. SQL Server Authentication: It lets you provide the username and password of an SQL Server user.

   **NOTE:** Here, the selected user should have "sysAdmin" role in SQL Server. [Know more...]

3. Click "Test Connection" to test the connection between the solution and the selected SQL Server with the provided details. It displays either an error if failed to connect or the following message confirming the successful connection.
4. The bottom section deals with the connectivity timeout period between the solution and SQL Server. You can use its buttons to increase/decrease the values or provide a manual value for it.

```
Connection Time-Out : 15    Seconds
```

*Figure 170: Connection time-out setting*

5. Following is a snapshot of the dialog box containing the sample details, where we have selected to login with SQL Server Authentication mode.

*Figure 171: Default SQL Server*

### 7.6.1 Usage of the Default SQL Server Settings

At a screen where you have to provide the details of SQL Server for storing or retrieving auditing logs, you will receive either anyone or both of the following buttons.
1. ▶ Click it to save the current Database Settings as the default SQL Server, which will be displayed as default in "SQL Server Settings".

2. ▶ Click it to load the Database Settings from the default SQL Server configured in "SQL Server Settings".

8  Modify Component

8.1.  Modify Domain

Right click on any domain node under “Component Management” and click “Properties”. It displays the domain properties.

**NOTE:** You can also click the domain node and then click “Properties” link in “Actions” pane.

![Domain Properties](image)

*Figure 172: Domain Properties*

The procedure to modify the domain properties is exactly same as that of adding a new domain with Advanced Configuration and involves the same steps. All the settings are listed as links in the left panel. At any point, you can click “OK” to apply the modified settings.
1. Domain Credentials: Here, you can change the login credentials of domain administrator to let the solution access and audit the domain.

   NOTE: These login credentials are saved in encrypted format in the solution, and you can only see the username in domain properties.

You can click “Enable Audit” button to enable the audit at the domain level. Click “Set Event Log Properties” to configure the storage and retention options of the event logs on the selected domain controllers and computers in the domain. It is necessary to set the Event Log Properties at the domain controllers, to audit the Windows Server properly. If you have not set this property manually, then you can use this button. Follow the steps below to set this property.

   Follow the steps below.

   a. Click button to access the following wizard.

   b. Select the domain controllers in the middle section, on which you want to apply this property. You have to select those domain controllers, which you want to audit. If this property is not applied, then the solution faces issues in auditing the domain.

   c. Select the maximum size of event logs to be stored at the domain controller. The available options are listed herein below.

   Figure 173: Wizard to set the Event Log Properties
i. 512 MB
ii. 1 GB
iii. 2 GB

d. In "When maximum event log size is reached" section, select any of the following options.
   i. **Overwrite event as need**: Select this option to overwrite the old logs when the event log size is reached.
   ii. **Archive the log when full, do not overwrite**: Select this option to archive the log when full. It saves the event logs from being overwritten.

e. Click "Next" once you have selected the options.

f. It processes to apply the properties on the selected domain controllers. Once done, the successful message appears in the wizard.

f. Click "Finish" to complete the process. It closes the wizard and takes you back to the domain properties.

If you face any issue in performing these log storage settings, then you have to configure these settings manually. [Know more...](#)

Here, you can also switch between agentless and agent-based auditing. If you are switching from “With Agent” to “Without Agent”, then "Uninstall Agent" wizard will appear.

If you are switching from “Without Agent” to “With Agent” or modifying the properties after uninstalling the agent, then agents will be installed silently.

2. **Advanced Domain Configuration**: Here, you can enable/disable the following components and configure their settings.
   i. Auditing of Active Directory, Group Policy, and Exchange Server
   ii. Backup of Active Directory and Group Policy
   iii. Health Monitoring of Active Directory and Exchange Server
   iv. Non-owner Mailbox Access Auditing
   v. Active Directory Cleaner
   vi. User Password Expiration Reminder

3. **IP Settings**: You can resolve the IP Addresses of all domain controllers in the domain. You can also change the preferred domain controllers to which the calls for collecting domain auditing will be sent.

4. **Database Settings**: You can change the database settings such as SQL Server and database to store the auditing logs.
   You can also change the backup settings such as location to save the complete and reference backup snapshots. Refer to the section herein below for more details.

5. **Organizational Unit Settings**: You can select the organizational units that you want to audit. Deselect others not to be audited.

6. **Object Classes and Other Settings**: You can select the object classes to be audited or not to be audited. You can even enable or disable the logon/logoff events.
7. **Archive Settings:** You can enable/disable the archiving of auditing logs and change the auditing schedule.

### 8.1.1 Move Backup Snapshot Data

You can modify the path of both Reference Backup and Complete Backup. If you are modifying their paths, then you have to use "Move Data" utility to move the backup from the previous location to the new location.

Follow the steps below to modify the path of Reference Backup or Complete Backup.

1. Click ![icon](image1) icon to access the following dialog box for selecting the new folder to save the Active Directory or Group Policy Backup.

   ![Set Backup Location](image2)

   *Figure 174: Dialog box to set/modify the backup location*

2. You can further click ![icon](image3) icon to select the new backup folder.

   ![Browse For Folder](image4)

   *Figure 175: Dialog box to select the folder*

3. Select a folder and click "OK". It takes you back to the same dialog box, which now shows the selected folder.
4. Click "OK". It shows "Move Data Utility" to move the backup data from the old location to the newly selected location.

5. Click "Next". It starts to move the data.
6. Once backup data is moved successfully, the following message box appears onscreen.

![Figure 178: Moving data of backup snapshots](image)

7. Click "Finish" to close the wizard. It takes you back to the Advanced Domain Configuration step of adding or modifying domain.

![Figure 179: Data has been moved successfully](image)
8. Click “Apply” at the bottom to apply the settings.

NOTE: You can also click Move Data button to move the data with above steps.

8.1.2 Manage Domain Agent

You can perform the following actions to manage the domain-auditing agent:

- Switch between agentless and agent-based auditing
- Uninstall auditing agent
  - Uninstall agent from a not added domain
  - Uninstall agent from an added domain
- Install auditing agent

8.1.2.1. Switching Auditing Modes

You can follow the steps below to switch between agentless and agent-based auditing.

1. Go to “Settings” tab → “Component Management” and access the domain properties.

![Figure 180: Dialog box to modify the domain](image)
2. Here, you can select "With Agent" in "Auditing Method" section to switch to agent-based auditing, which installs an agent for Active Directory, Group Policy, and Exchange Server. If you are switching from agentless to agent-based auditing, the agent will be installed.

3. You can select "Without Agent" option to choose agentless auditing, where no agent will be installed and run on the domain. If you are switching from agent-based auditing to agentless auditing here, then "Uninstall Agent" wizard appears.

8.1.2.2 Uninstall Agent from an added Domain

Follow the steps below to uninstall agent from a domain.

1. Right-click "Domain" node in “Settings” Tab and click ‘Uninstall Agent’ option. It displays the following dialog box.

![Uninstall Agent dialog box]

2. Select the relevant options from where you want to uninstall the agents.
   a. Active Directory, Exchange Server, Group Policy: Select this option to uninstall the auditing agent from Active Directory, Group Policy, and Exchange Server.
   b. Group Policy (Applicable for version 15.4 and before): Select this option to uninstall Group Policy auditing agent installed by Lepide Data Security Platform version 15.4 or earlier.
   c. Non-Owner: Select this option to uninstall the agent of non-owner mailbox access auditing from Exchange Server. This agent is installed on the server in both cases of “with agent” and “without agent” auditing mode.

3. Select the agents to be removed.

4. Click "Next". It lists all domain controllers available in the domain.
5. Select the domain controllers from which you want to uninstall the agent. You can click icon to select all listed domain controllers or click icon to deselect all selected items.

6. If "IP Address" cell of the select domain controller(s) does not display no or wrong IP Address, double click this cell to access a dialog box. Enter the correct IP Address of the selected domain controller and click "OK". Now, the wizard displays the entered IP Address.

7. Click "Next" to start the uninstall agent process.

8. Once the agent is uninstalled, the following message appears.
8.1.2.3 Uninstall Agent from a not added Domain

To uninstall agent over domain controllers whose domain is not added or whose details are not available in the solution, simply follow the steps below.

1. Right-click “Component Management” node; go to “Uninstall Agent”.
2. Click "Active Directory, Exchange Server and Group Policy". It shows the following box.
3. Enter the following details.
   a. Name or IP Address of Domain from which the agents have to be uninstalled.

9. Click “Finish” to complete the process.
b. Name of an administrative user.

c. Password of the above user.

4. Click "OK". It displays the following wizard.

![Image of Uninstall Agent wizard]

Figure 185: Listing available domain controllers

5. Select the domain controllers from which you want to uninstall the agent.

   Click [ ] icon to select all listed domain controllers or click [ ] icon to deselect all selected items.

6. Click "IP Address" cell of the selected domain controller. It displays the dialog box to enter the IP Address of the target domain controller.

![Image of IP Address dialog box]

Figure 186: Enter IP Address

7. Enter the correct IP Address of the selected domain controller.

8. Click "OK" to come back to the previous wizard, which now displays the entered IP Address for the domain controller.
9. Click "Next" to start the uninstall agent process.
10. Once the agent is uninstalled, you receive a message to confirm the same.
8.1.2.4 Reinstall Domain Agent

Follow the steps below to reinstall the auditing agent on a domain.

11. Select the domain and click "Advanced Domain Configuration" link in "Actions" pane. It shows the following settings.

**NOTE:** You can also access the domain properties and then switch to “Advanced Domain Configuration”.

12. Check the options to reinstall their agents to re-enable their auditing.

Figure 189: Domain Controllers Excluded from Auditing
13. Click "OK" to apply the settings.

While applying the settings, the solution installs the auditing agent on the server for the selected components. Then the domain is added to the list of changes collection, which means its auditing is re-enabled.

8.1.3 Manage Domain Health Monitoring

You can exclude or include the selected domain controllers or entire domain from health monitoring.

8.1.3.1 Exclude Domain Controllers from Health Monitoring

Follow the steps below to exclude the domain controllers from health monitoring.

1. In the left panel of Domain Properties, click "Advanced Domain Configuration" settings.
2. To disable Health Monitoring for the complete domain, including its all domain controllers, uncheck "Health Monitoring" at the top.

3. To disable Health Monitoring for selected domain controllers, uncheck boxes under "Health Monitoring" for the servers.
4. Click "OK". It displays a warning message.

5. Click "Yes".

8.1.3.2 Include Domain Controllers in Health Monitoring

1. In the left panel of Domain Properties, click "Advanced Domain Configuration" settings.
2. Check the box for "Health Monitoring" to enable the health monitoring for the entire domain.

3. Check the boxes in "Health Monitoring" column for all domain controllers, whose Health Monitoring you want to enable.

4. Click "OK" to apply the change and enable health monitoring for selected servers.

8.2. Modify SharePoint Server

Perform any of the following methods to access the wizard to modify the listing of SharePoint Server.

1. Right-click any SharePoint Node under “Component Management” and click “Properties”.

   **NOTE:** You can also click “Properties” link in “Actions” pane for the selected SharePoint Server.
The available settings to modify the listing of a SharePoint Server are listed in the left panel. You can click them to modify their options and click “OK” at any point to apply the modified settings.

1. **SharePoint Server Settings**: Here, you can modify the settings related to SharePoint Server and its linked SQL Server.

2. **Site Collection Settings**: It lets you modify the auditing settings of Site Collections. Here you can select the site collections to be included or excluded in the auditing. The excluded sites will not be monitored and audited by Lepide Data Security Platform. You have to remove the excluded sites from “Exclude” list to start their monitoring.

3. **Database Settings**: You can modify the SQL Server database settings. You can select a different SQL Server, authentication mode, and database to store the auditing logs.

4. **Archive Database Settings**: Here, you can modify the archive database settings.

### 8.2.1 Manage SharePoint Agent

You can uninstall and reinstall SharePoint Auditing Agent.

#### 8.2.1.1 Uninstall SharePoint Auditing Agent

Follow the steps below to uninstall auditing agent from an already added SharePoint Server.
1. Right click on a SharePoint Server node and click “Uninstall Agent”. You can also click “Uninstall Agent” link in “Actions” pane for the selected SharePoint.

2. It shows the following warning message.

![Warning to uninstall the agent](image1)

3. Click “Yes” to start the process of uninstalling the agent.

![Uninstalling the SharePoint Agent](image2)

4. With the completion of the process, the agent will be uninstalled from SharePoint Server.

**8.2.1.2 Uninstall Agent from not added SharePoint**

Lepide Data Security Platform lets you uninstall agent from not added SharePoint Server. It helps you to remove the agent installed by an outdated version of Lepide Data Security Platform or Lepide Data Security Platform for SharePoint. Follow the steps below,

5. Go to “Settings” tab; right-click on "Component Management".

6. Go to “Uninstall Agent” sub-menu and click "SharePoint". It shows the following wizard.

![Wizard to uninstall SharePoint Agent](image3)
7. Enter the following details.
   - Name or IP Address of Domain Controller
   - Username and Password of an administrative user

8. Click "OK". It shows the following warning message.

![Warning to uninstall agent](image)

9. Click "Yes" to start the process to uninstall the agent.

![Uninstalling the SharePoint Agent](image)

8.2.1.3 Reinstall SharePoint Auditing Agent

Follow the steps below to reinstall the agent for a SharePoint Server.

10. Right-click SharePoint Server node under Component Management and click "Properties".
You can also click “Properties” link in “Actions” pane for the selected SharePoint.

11. Click "OK". It starts installing the agent.

8.3. Modify SQL Server

Right-click any SQL Server node and click "Properties".

NOTE: In component management, you can also click “Properties” link in “Actions” pane.
SQL Server properties appear on the screen.

![SQL Server properties](image)

*Figure 203: Wizard to modify the listing of SQL Server*

All the settings to add SQL Server with Advanced Configuration are listed as the links in the left panel. You can click these links to modify the settings. At any point, you can click “OK” to apply the modified settings. You cannot change the name or IP Address of SQL Server.

Here, you can change the following settings.

1. **SQL Server Credentials**: Here, you can change the following options.
   a. Authentication Type: You can select either Windows authentication or SQL Server authentication.
   b. Username and Password for SQL Server Authentication

2. **Health Audit Settings**: It lets you modify the health auditing of SQL Server. Checking the box enables SQL Health Monitoring whereas unchecking the box disables it. You can modify its options as well.

3. **Audit Settings**: It lets you modify the auditing settings of SQL Server. Clicking it shows the audit types, which you can select to enable/disable their auditing.

4. **Object Settings**: You can specify what database objects, server objects, operations, and users have to be audited or excluded from auditing.

5. **User Settings**: Select the option "Select Users" in the section - "Select User(s) to audit". It enables the list of users in the adjoining area, where you can select the users to include or exclude them in auditing.
6. **Database Settings**: You can modify the database settings. You can select a different SQL Server, authentication mode, and database.

7. **Archive Database Settings**: Here, you can modify the archive database settings for the domain.

### 8.3.1 Manage SQL Health Monitoring

You can go to Settings Tab → Component Management and browse Properties of an SQL Server to manage its health monitoring by excluding and including the server(s).

#### 8.3.1.1 Disable Health Monitoring

Follow the steps below to disable the health monitoring of SQL Server.

1. In the left panel of SQL Server Properties, click "Health Auditing".

2. To disable Health Monitoring for SQL Server, uncheck "Enable Health Monitoring".

![Figure 204: Modifying Health Auditing Settings](image-url)
3. Click "OK" to save the changes in SQL listing.

### 8.3.1.2 Enable SQL Server Health Monitoring

Follow the steps below to enable the Health Monitoring of SQL Server.

4. In the left panel of SQL Server Properties, click "Health Auditing".
5. Check the box labeled "Enable Health Monitoring."

6. You have to provide the details of the computer where SQL Server is installed.
   - Computer Name: Enter the name or IP Address of the computer, where SQL Server is installed.
   - User Name: Provide the name of an administrator user of that computer.
   - Password: Enter the password for the above user.

7. Click "OK" to save the changes and enable the health monitoring of SQL Server.

8.4 Modify Exchange Online Server

Right-click any Exchange Online node under "Component Management" and click "Properties".

**NOTE:** You can also click “Properties” link in “Actions” pane for the selected Exchange Online.
The available settings to modify the listing of an Exchange Online are listed in the left panel. You can click them to modify their options and click "OK" at any point to apply the modified settings.

1. **Credentials**: Here, you can modify the changed user credentials with which Exchange Online is added. You can change the name and password of the user, however, you cannot change the name of Exchange Online.

2. **Site Collection Settings**: It lets you modify the auditing settings of Site Collections. Here you can select the site collections to be included or excluded in the auditing. The excluded sites will not be monitored and audited by Lepide Data Security Platform. You have to remove the excluded sites from "Exclude" list to start their monitoring.

3. **Mailbox Configuration**: You can modify the mailbox audit settings. Select the mailboxes that has to be audited and uncheck others to disable their auditing.

4. **Object Configuration**: You can modify the object audit settings. Select the objects that has to be audited and uncheck others to disable their auditing.

5. **Database Settings**: You can modify the SQL Server database settings. You can select a different SQL Server, authentication mode, and database to store the auditing logs.

6. **Archive Database Settings**: Here, you can modify the archive database settings.

Click “OK” at any step to apply the modifications.
9. Remove Component

9.1 Remove the listing of Domain

To delete an already added domain from the auditing list, follow the steps below:

1. Right-click on domain node under "Component Management" and click "Remove" option.

**NOTE:** You can also click “Remove” link in “Actions” pane for the selected domain.

2. It displays the following warning message.

![Warning to remove the domain's listing](image)

3. Click "Yes". It displays “Uninstall Agent” box.

![“Uninstall Agent” box](image)
4. If you do not want to add the domain again, then it is required to uninstall the agent.

**NOTE:** In some cases, the domain controllers of the removed domain are still being monitored, therefore, we recommend to uninstall the agents while removing the domain from the auditing listing.

5. Check the boxes for the domain controllers, from which you want to uninstall the agents.
   
   You can click [ ] icon to select all domain controllers in the list or click [ ] icon to deselect all.

6. Click "Next" to start the agent uninstallation process.

![Uninstall Agent](image)

*Figure 210: Uninstalling the agent*

7. The wizard confirms once the agent uninstallation is completed successfully.
8. Click "Close" to close the dialog box. Now, it asks to restart the solution.

![Figure 211: Uninstalled Agent while removing the listing of domain](image)

9. Click "Yes" to restart the solution.

![Figure 212: Asking to restart the solution](image)

### 9.2 Remove the listing of SharePoint

Follow the steps below to remove the listing of an already added SharePoint Server.

1. Right-click any SharePoint node and click "Remove".

   **NOTE:** You can also click “Remove” in “Actions” pane for the selected SharePoint Server.

2. It displays the following warning message.
3. Click "Yes". It displays the following message box asking you to restart the solution.

![Warning before deleting SharePoint's listing](image1)

Figure 213: Warning before deleting the SharePoint's listing

4. Click "Yes" to restart the solution.

![Message to restart solution](image2)

Figure 214: Message to restart the solution

### 9.3 Remove the listing of SQL Server

You can remove the listing of an SQL Server from Lepide Data Security Platform. After this, the solution will not monitor and audit that SQL Server. Follow the steps below,

1. Right-click "SQL Server" node under "Component Management" and click "Remove".

   **NOTE:** You can also click "Remove" link in "Actions" pane for the selected SQL Server.

2. It displays the warning message.

![Warning before deleting SQL Server's listing](image3)

Figure 215: Warning before deleting the listing of an SQL Server
3. Click "Yes". After the restart, SQL Server will be removed from the auditing list.

9.4 Remove the listing of Exchange Online

Follow the steps below to remove the listing of an already added Exchange Online Server.

1. Right-click any Exchange Online node and click “Remove”.

   **NOTE:** You can also click “Remove” in “Actions” pane for the selected Exchange Online Server.

2. It displays the following warning message.

   ![Figure 216: Warning before deleting the listing of Exchange Online](image)

3. Click "Yes". It displays the following message box asking you to restart the solution.

   ![Figure 217: Message to restart the solution](image)

4. Click "Yes" to restart the solution.

10. Uninstall Lepide Data Security Platform

There can be a situation when you need to uninstall Lepide Data Security Platform. Make sure to close the solution before uninstalling it. Follow the steps below to uninstall it.

1. There are two ways to start the uninstallation.
   a. Go to Start → “All Programs” → "Lepide Data Security Platform “, click "Uninstall Lepide Data Security Platform ".
   b. Click Start → Control Panel. Its window appears. Launch "Programs and Features". Select "Lepide Data Security Platform" and click "Uninstall".
2. Following any of the above methods displays a warning message.
3. Click "Yes" to start the uninstallation process.
4. Once uninstalled, the message box confirming the successful uninstallation appears onscreen.
5. Click "OK" to finish the process.

After following the above steps, Lepide Data Security Platform is uninstalled successfully from your computer. By default, the solution is configured to retain the license file, auditing for the server, data of backup snapshots, and other settings in the program installation folder. To remove the remaining elements, delete its program installation folder manually and then empty the Recycle Bin as well.

Do not delete this folder if you want to retain the license file, or have to reinstall the same/upgraded version of the solution.

%ProgramFiles%\Lepide Data Security Platform – for 32-bit OS
%ProgramFiles(x86)%\Lepide Data Security Platform – for 64-bit OS

If above folders are deleted, the snapshot data captured by the solution will also be removed (if you have not provided other path to store the snapshots) and there is no way to recover them back. So do not remove the installation folder to retain the application logs, license files, backup snapshots, and other settings.

11. More Documents

You can refer to the following documentation for Lepide Data Security Platform.

<table>
<thead>
<tr>
<th>Other Document</th>
<th>URL</th>
</tr>
</thead>
</table>
12. Support

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

**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 [http://www.lepide.com/contactus.html](http://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 [http://www.lepide.com/](http://www.lepide.com/)

13. Copyright

LepideAuditor, LepideAuditor App, LepideAuditor App Server, LepideAuditor (Web Console), LepideAuditor Logon/Logoff Audit Module, any and all components, any and all accompanying software, files, data and materials, this guide, and other documentation are copyright of Lepide Software Private Limited, with all rights reserved under the copyright laws. This user guide cannot be reproduced in any form without the prior written permission of Lepide Software Private Limited. No Patent Liability is assumed, however, on the use of the information contained herein.

© Lepide Software Private Limited, All Rights Reserved.

14. Warranty, Disclaimers, and Liability Limitations

LepideAuditor, LepideAuditor App, LepideAuditor App Server, LepideAuditor (Web Console), LepideAuditor Logon/Logoff Audit Module, any and all components, any and all accompanying software, files, data, and materials are distributed and provided AS IS and with no warranties of any kind, whether expressed or implied. In particular, there is no warranty for any harm, destruction, impairment caused to the system where these are installed. You acknowledge that good data processing procedure dictates that any program, listed above, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of LepideAuditor and the above listed accompanying programs covered by this License. This disclaimer of warranty constitutes an essential part of this License.

In no event does Lepide Software Private Limited authorize you or anyone else to use LepideAuditor and the above listed accompanying programs in applications or systems where LepideAuditor and the above listed accompanying programs’ failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any
such use is entirely at your own risk, and you agree to hold Lepide Software Private Limited harmless from any and all claims or losses relating to such unauthorized use.

15. Trademarks


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. We have compiled a list of such trademarks, but it may be possible that a few of them are not listed here.


Apple® and Safari® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

Google®, Android™ and Chrome™ are registered trademarks of Google Inc.

Mozilla® and Firefox® are registered trademarks of The Mozilla Foundation.

NetApp, NetApp Filer, Data ONTAP®, and Clustered Data ONTAP® are trademarks of NetApp, Inc., registered in the U.S. and/or other countries.