Lepide Data Security Platform for File Server

Installation and Configuration Guide
# Table of Contents

1. Introduction ........................................................................................................................................... 4  
2. Requirements and Prerequisites ........................................................................................................... 4  
   2.1 Basic System Requirements ............................................................................................................. 4  
   2.2 Supported Servers for Auditing ....................................................................................................... 5  
2.3 Prerequisites to Audit NetApp 7-Mode ................................................................................................. 6  
   2.3.1 Auditing Flow of NetApp 7-Mode; ............................................................................................... 6  
   2.3.2 Agent Installation for NetApp 7-Mode ....................................................................................... 7  
   2.3.3 Recommended Settings for NetApp 7-Mode .............................................................................. 8  
   2.3.4 Limitations to audit 7-Mode with Lepide ................................................................................... 9  
   2.3.5 Connection Types for NetApp 7-Mode ...................................................................................... 9  
2.4 Prerequisites to audit NetApp Cluster Mode ..................................................................................... 9  
   2.4.1 Recommendations for NetApp Cluster Mode ............................................................................ 9  
   2.4.3 Auditing flow for NetApp Cluster Mode ..................................................................................... 10  
   2.4.3 Recommended Versions of NetApp Cluster Mode ...................................................................... 10  
   2.4.4 Limitations to Audit Cluster Mode with LE[ode ........................................................................ 10  
3. Required User Rights ......................................................................................................................... 11  
   3.1 Service Rights ................................................................................................................................. 11  
   3.2 Local System Rights ....................................................................................................................... 11  
4. Install Lepide Data Security Platform ............................................................................................... 11  
5. Configure Service Credentials ............................................................................................................. 13  
6. Add File Server ..................................................................................................................................... 16  
   6.1 Add Windows File Server ............................................................................................................... 17  
   6.2 Add NetApp Filer ............................................................................................................................ 22  
   6.2.1 Add NetApp 7-Mode .................................................................................................................. 22  
   6.2.2 Add NetApp Cluster Mode ........................................................................................................ 28  
   6.3 Steps after adding File Server ........................................................................................................ 34  
1. Audit Rule Management ....................................................................................................................... 36
1. Introduction

This guide helps you install, configure and manage Lepide Data Security Platform for File Server. The solution provides a comprehensive means of auditing Windows File Server and NetApp Filers (both 7-Mode and Cluster Mode).

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.

A list of supporting documentation is also provided at the end.

2. Requirements and Prerequisites

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

2.1 Basic System Requirements

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

- **Required RAM**
  - Minimum 4 GB RAM
  - Recommended 8 GB RAM

- **Required free disk space**
  - Minimum 1 GB
  - Recommended 2 GB

- **Any of the following 32-bit or 64-bit Windows Operating Systems.**
  - Windows 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 Edition
- 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>Windows File System</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>
</tbody>
</table>
Audited Servers | Supported Versions
---|---
NetApp Filer | • NetApp 7-Mode Configuration
  ▪ Lepide Data Security Platform for File Server successfully audits and reports events from NetApp Filer with Data ONTAP™ 7.2 or later.
  ▪ The recommended version for the availability of all features is ONTAP 7.3.4 or later.
• NetApp Cluster Mode Configuration (CIFS Protocol only)
  ▪ 8.2.3 Clustered Data ONTAP
  ▪ 8.3.0 Clustered Data ONTAP
  ▪ 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

2.3 Prerequisites to Audit NetApp 7-Mode

- The agent to audit NetApp Filer can be installed on any client system or domain controller, 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.

2.3.1 Auditing Flow of NetApp 7-Mode;

Lepide uses the CIFS Auditing mode, which allows it to access changes made on NetApp Filers through Windows devices and successfully audit and reports them. It uses the assigned “File policy” or “FPolicy” to capture events and audit changes within the File Server. The auditing process for NetApp Filer is displayed hereinbelow.
The steps involved in the above image are:

1. The system where Lepide is installed connects to the agent computer for event collection.
2. The agent computer connects with the NetApp Filer and tracks the events as per the assigned “fpolicy”.
3. The NetApp Filer sends live events for any changes made within the file server.
4. The agent sends this event to the location where the solution is installed.
5. Lepide connects to the SQL database and stores these events for report generation.
6. The solution displays the reports as per the created audit rules and policies to display all changes within the File Servers.

2.3.2 Agent Installation for NetApp 7-Mode

- We recommend not to install multiple agents on the same server for monitoring multiple NetApp Filers with Data ONTAP versions lower than 7.3.
- The agent can be installed on any client system or domain controller. We recommend not to install it on a workgroup system.
- To install the agent for NetApp Filer, provide the credentials only of a local administrator of NetApp.
2.3.3 Recommended Settings for NetApp 7-Mode

- Verify the settings on the NetApp Filer before installing the agent. Ensure that `httpd.admin.enable` option is on. It is "ON" by default, but we still recommend you to check it first before installing the agent.
- Ensure that the NetApp Filer time is synced with the time on the agent system to get precise report timings.
- In the Agent system GPO Settings, change the required settings as displayed below.

Follow the steps below to perform these settings:

1. Type `gpmc.msc` in "Run" or search in Start Menu. Press ENTER key to open Group Policy Management.
2. Under the forest, navigate to Domains → local domain → Default Policy.
3. Right-click on it and select ‘Edit’. “Group Policy Management Editor” window opens up.
5. Click on Security Options. In this section, make the following policy settings:
   i. Network Access: Do not allow anonymous enumeration of SAM accounts → Disabled
   ii. Network Access: Do not allow anonymous enumeration of SAM accounts and shares → Disabled
   iii. Network Access: Do not allow storage of passwords and credentials for network authentication → Disabled

![Figure 2: Highlighting Group Policies for NetApp Filer](image-url)
iv. Network Access: Let Everyone permissions apply to anonymous users → Enabled

v. Double-click Network Access: Named pipes that can be accessed anonymously and select the checkbox to define policy settings. Type "NTAPVSRQ" and click apply.

vi. Network Access: Restrict anonymous access to Named Pipes and Shares → Disabled

2.3.4 Limitations to audit 7-Mode with Lepide

- Events will not be generated for the changes made from the agent server.
- ONTAP 7.3 or later version is required to monitor security settings event reports (Owner, SACL, and DACL).
- SACL (Audit) change events are reported, but event details will not be shown in the reports.

2.3.5 Connection Types for NetApp 7-Mode

Lepide provides two types of connections with the NetApp Filer from the agent:

- Asynchronous: This option is quick, but it cannot capture security details. It captures the security events but does not show details.
- Synchronous: This option captures security details, but the process slightly slows down the performance of the Filer. We recommend to select “Synchronous” connection type if you want to perform the Permission Analysis of NetApp Filer

Select the appropriate connection type while adding the File Server.

2.4 Prerequisites to audit NetApp Cluster Mode

- Please verify settings on the NetApp Cluster Mode before installing the agent.
- Ensure that the time on NetApp Cluster Mode is synchronized with the time on the computer where the solution is installed to get precise report timings.
- When you install agent for NetApp Cluster Mode, use only NetApp domain user.

2.4.1 Recommendations for NetApp Cluster Mode

In NetApp, the auditing framework is provided by Data ONTAP. It is similar to the auditing performed on Windows® Servers. This feature was available from the early versions of Data ONTAP, but NetApp itself recommends using Data ONTAP version 8.2.3 or higher, that is the same as what we recommend.

Auditing can be enabled on either CIFS shares or NFS exports.

- CIFS Auditing: It refers to auditing access events from NetApp filers through Windows clients/Mac OS, which allows to access data on the storage system using the CIFS protocol.
- NFS Auditing: It refers to auditing access events from NetApp filers through UNIX/Linux® clients, which allows to access data on the storage system using the NFS protocol.
2.4.3 Auditing flow for NetApp Cluster Mode

Lepide Data Security Platform for File Server uses the CIFS Auditing mode for Cluster Mode. It uses event log file to capture events and audit changes within the File Server. Our solution audits NetApp Cluster Mode as per the following flowchart.

![NetApp Cluster Mode Auditing Flow](image)

*Figure 3: NetApp Filer Cluster Mode Auditing Flow*

The auditing flow of NetApp Cluster Mode involves the following steps:

1. The computer where the solution is installed connects to NetApp Cluster Mode for event collection.
2. The NetApp Cluster Mode sends immediate events for any change made within the file server.
3. The agent sends this event to the computer where the solution is installed.
4. The solution connects to the SQL database and stores this events for report generation.
5. The solution displays reports as per the audit rules and policies to display all changes within the File Servers.

2.4.3 Recommended Versions of NetApp Cluster Mode

- Lepide Data Security Platform for File Server successfully audits and report events from NetApp file server with Data ONTAP™ 8.2.3 or later.
- The recommended version for complete feature availability is ONTAP 8.2.3 or later.

2.4.4 Limitations to Audit Cluster Mode with LE[ode]

SACL (Audit), creating and removing Share folder, copying file - these change events will not be shown in the reports.
3. Required User Rights

To install and work with Lepide, you need to have appropriate rights to the system where it will be installed. You will also need to have appropriate rights to access Active Directory, SQL Server, Windows File System, and NetApp Filer.

3.1 Service Rights

To run the service of Lepide after installation, you can select any of the following object or user.

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

3.2 Local System Rights

The user should have the following permissions on the local computer where the software 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 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.

4. Install Lepide Data Security Platform

To install Lepide Data Security Platform, download the installer file from [http://www.lepide.com/start-free-trial.html](http://www.lepide.com/start-free-trial.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.
You have to follow the onscreen instructions to install the software. 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 software.
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%\LepideAuditor` for 32-bit and `%ProgramFiles(x86)%\LepideAuditor` 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" after 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 software 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 Lepide Data Security Platform ", it will close the installation wizard and starts to launch the software.

---

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

![Figure 4: Error to install the software](image)

The software can throw this error even after installation in case of insufficient space. Free at least 500 MB space on the disk drive where the software is installed.
Welcome Screen appears after the software is launched for the very first time.

![Welcome Screen](image)

**Figure 5: Welcome Screen**

5. Configure Service Credentials

This setting appears on the Welcome Screen when you are installing the software for the very first time.
You can configure this option to select the User Account with which you want to create and run the Windows Service of Lepide. Follow the steps below to configure this option.

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

2. 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.

3. You can either type the username manually or click "Browse" to select a user account or Manage Service Account object from Active Directory.
4. You can type the name of user or Service Account and click "Check Names" to verify. After verification, the name is depicted with an underline.

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

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

7. Click "OK". The software configures the services.

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

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

9. Click "Yes" to assign the rights. The following message box appears on the screen when the service is configured and running with the provided credentials of the selected user.
Click “OK” to complete the process. Now, “Component Selection” dialog box appears.

Select the type of component and add it for auditing.

6. Add File Server

After you have installed the software and configured Lepide service to run with administrative credentials, you can add a File Server for auditing. You can use any of the following methods to get a wizard for adding a component.

You can select “Click here to configure File Server” link on “Component Selection dialog box to start adding the File Server. You can also click “File Server” button in “Add Component” section of Component Management in Settings Tab. Alternatively, you can right-click on “Component Management” node in “Settings Tab”, go to “Add” and click “File Server”.
If you follow any of the above methods, then it displays a dedicated console for managing File Server Auditing.

Here, you can click “Add File Server” option on the toolbar to add any of the following file servers.

1. Windows File System
2. NetApp Filer

6.1 Add Windows File Server

Follow the steps below to add Windows File System.

1. Click “Add File Server” button on the toolbar and click “Windows File Server”.

![Figure 12: Right-click “Component Management” node in Settings Tab](image1)

![Figure 13: File Server Auditor Console](image2)
You can also click icon in the Right Panel and select “Windows File Server”.

2. Add File Server wizard opens up.

3. Enter the name or IP Address of the server along with its domain or Workgroup name.

4. Instead of typing manually, you can click “Add” button to scan the domain network and select the required file servers.
5. You can select the domain name in the drop-down menu or type its name.

6. Click “Find” button to list its computers in the blank area.

7. Select the computer you want to audit and click “OK”. It takes you back to the previous wizard, which now displays the selected File Server.

8. Now, you have to select the user with which you want to add the File Server.

9. If you are logged in as a user that has above rights, then you can select “Current User”.

**NOTE:** The provided user should be a member of “Administrators”, “Domain Admins”, “Group Policy Creator Owners”, “Enterprise Admins”, and “Schema Admins” groups to enable the auditing of File Server.

If the above rights are not assigned to the user, then follow the steps below.

a. Go to “Administrative Tools”.

b. Open “Active Directory Users and Computers”.

c. Select “User Properties”.

d. Go to “Member Of” → “Add Group”.

e. Select any of the following groups as per the above requirements.

   (i) Administrators   (ii) Domain Admins   (iii) Group Policy Creator Owners
   (iv) Enterprise Admins   (v) Schema Admins

f. Click “Apply” and “OK”
10. If the logged in user does not have the required rights, then you have to select “Following User” option and provide the login credentials of a user who has the required rights.

11. After entering the details, click “Next”. At the next step, you have to provide the details of SQL Server.

12. Click “Server Name” dropdown to select the desired SQL Server.

13. There are two authentication options under it.
a) Windows Authentication: This mode can be selected if SQL Server is installed on the same computer where Lepide is installed.

b) SQL Server Authentication: Select this mode if SQL Server is installed on a remote machine or the local machine. We recommend to select this option.

Provide the username and password of an SQL User, which has sufficient rights to create a new database.

14. Enter a database name in the database name field to create a new database. You can also select an existing database created by Lepide or another application.

15. Click “Next” to start installing the auditing agent at Windows File Server.

16. After the agent is installed, you reach the following step.
17. Click “Finish” to complete the process.

6.2 Add NetApp Filer

You can add NetApp 7-Mode and NetApp Cluster Mode for auditing.

6.2.1 Add NetApp 7-Mode

Follow the steps below to add NetApp 7-Mode for auditing.

1. Click “Add File Server” button on the toolbar and click “NetApp Filer”.

You can also click icon in the Right Panel, go to “NetApp Filer” sub-menu and click “7-Mode”.

3. Either enter the name or IP Address of NetApp Filer Name manually or click “Add” to select a NetApp Filer from the network.

4. Here, you can select a domain name and click “Find” to list the available Filers in it.
5. Select a NetApp Filer and click “OK”.
6. After the required NetApp Filer is selected, enter the login credentials of a NetApp Administrator to add it.
7. Click “Next” to go to the next step, where you have to provide the details of SQL Server to create a database for storing auditing logs.

![SQL Server Information](image)

Figure 24: SQL Server Details to add NetApp Filer

18. Click “Server Name” dropdown to select the desired SQL Server.
19. There are two authentication options under it.
   a) Windows Authentication: This mode can be selected if SQL Server is installed on the same computer where the solution is installed.
   b) SQL Server Authentication: Select this mode if SQL Server is installed on a remote or local computer. We recommend to select this option. Provide the username and password of a SQL user, who has sufficient rights to create the database.
20. Enter a database name in the database name field to create a new database. You can also select an existing database created earlier by Lepide or another application.
21. Click “Next”, after you have entered the details. At the next step, you have to provide the details of the system where you wish to install the agent to collect the changes from NetApp Filer.
22. Enter the name or IP address of the agent system.

23. Provide username and password of an administrator of the agent system to allow access to the software to install the agent.

**NOTE:** You can install the agent on another system apart from NetApp Filer. However, it is important to note that the agent can only be installed on any client system or the domain controller. We recommend not to install it on workgroup computers. We install the agent only on the connected Windows Computer and not on NetApp.

**NOTE:** The provided user should be a member of “Administrators”, “Domain Admins”, “Group Policy Creator Owners”, “Enterprise Admins”, and “Schema Admins” groups, at the agent system, to enable the auditing of NetApp Filer. If the above rights are not assigned to the user, then follow the steps below.

a. Go to “Administrative Tools”.

b. Open “Active Directory Users and Computers”.

c. Select “User Properties”.

d. Go to “Member Of” → “Add Group”.

e. Select any of the following groups as per the above requirements.

   (i) Administrators  
   (ii) Domain Admins  
   (iii) Group Policy Creator Owners  
   (iv) Enterprise Admins  
   (v) Schema Admins

f. Click “Apply” and “OK”
24. Now you need to choose the Connection Type. Lepide provides the following two types of connections with the NetApp Filer from the agent:

   a. Asynchronous: This option is quick, but it cannot capture security details. It captures the security events but does not show details.

   b. Synchronous: This option captures security details, but the process slightly slows down the performance of the Filer.

   **NOTE**: If you need the Permission Analysis of NetApp Filer, we recommend to use synchronous mode to connect to NetApp Filer.

25. Certain changes are required in the Local Security Policies to allow the software to audit Filers. The software provides a checkbox to make such changes automatically from its end.

26. If you do not want to go for automatic changes or facing any error in applying these changes automatically, then uncheck this option and make these manually. To know more, refer to Section 9.4 Recommended Settings.

27. Click the checkbox to make the changes automatically. The software displays the list of required changes in the next screen and reconfirms it.

![NetApp Agent Information](image)

*Figure 26: List of changes to be made for auditing NetApp Filer*

28. Click “Yes” to make these changes and to install the agent.

   If you click “No”, then the changes will not be made, but still, the agent will be installed. Because of no agent installation, the audit reports will not be generated in this case.

   To generate the audit reports after clicking “No”, you have to make these changes manually now. To know more, refer to Section 9.4 Recommended Settings.
29. After completing the installation, "Finish" button will be activated.

30. Click "Finish" to complete the process.
6.2.2 Add NetApp Cluster Mode

Follow the steps below to add NetApp Cluster Mode for auditing.

1. Click “Add File Server” button on the toolbar and click “NetApp Filer”.

You can also click icon in the Right Panel, go to “NetApp Filer” sub-menu and click “Cluster Mode”.

2. Wizard to add “NetApp Cluster Mode” opens up on the screen. Here, you have to provide the information of that domain where NetApp Cluster Mode exists.

3. Here, you have to provide the following details.
   
   A. Domain Name: Enter the name or IP Address of the domain, where NetApp Cluster Mode is located, in “Domain” text field.
   
   B. User Name: Enter the name of a user, who is a member of “Domain Admins” group.
   
   C. Password: Enter the password of the selected user.

4. Click “Next” to proceed. “Add File Server” page is displayed.
5. Here, you have to provide the following details.
   A. **File Server Name/IP**: Enter the name or IP Address of NetApp Filer.
   B. **User Name**: Enter the name of a user, who have vsadmin role.
   C. **Password**: Enter the password of the selected user.
   D. **Audit Configuration**: Here, you have to select “Manual Auditing” or “Automatic Auditing”. Please refer to the following points to understand it better and to make your selection.

**NOTE: What Auditing should be preferred?**

You can select Automatic Auditing option to enable the auditing settings automatically without giving any user input. However, you should prefer Manual Auditing when you

- are receiving errors in enabling Automatic Auditing
- want to allocate 2 GB to 3 GB (not less than 2 GB and not more than 3 GB) space to a volume for auditing
- want to allocate more than 3 GB space to a volume for auditing

**Prerequisites of Manual Auditing**

a. Make sure that any existing manual auditing should meet the following prerequisites.

b. Auditing should be enabled.

c. The minimum Log File Size (rotate-size) should be 1 MB.

d. The format of auditing should be XML.

e. The size of selected volume should be at least 2 GB.
NOTE: Steps to create Manual Auditing on NetApp Cluster Mode

If manual auditing does not exist already or does not meet the above prerequisites, you have to add and enable an Audit Setting manually on the selected Storage Virtual Machine (SVM). Perform the following steps:

A. Execute the following commands to configure auditing manually at NetApp Cluster Mode.

```
vserver audit create -vserver <Name_SVM> -destination "/<Name_Volume>" -format XML -rotate-size <XX><XB>
```

B. Change the following values.

- `<Name_SVM>`: Name of SVM
- `<Name_Volume>`: Name of Volume

**WARNING:** The minimum size of the selected volume should be 2 GB.

- `<XX>`: Value in numbers. It is the size of Log File.
- `<XB>`: Measurement of the file size. It can be in KB, MB, GB, TB, or PB.

**NOTE:** The minimum Log File Size (rotate-size) must be 1MB.

C. After creating the auditing setting, you can execute the following command to view the auditing setting created for an SVM.

```
vserver audit show
```

D. Execute the following command to enable the auditing setting.

```
vserver audit enable -vserver <Name_SVM>
```

Replace `<Name_SVM>` with the name of SVM.

E. After enabling the auditing setting, execute the following command to view the status of added auditing.

```
vserver audit show
```

**Figure 32:** Commands to set auditing and show its status

**Figure 33:** Commands to enable auditing and show its status
I. Manual Auditing: In "Audit Configuration Section", click "Manual" option to enable its options. If the manual auditing is already configured on the selected Storage Virtual Machine (SVM) and if it meets the above-listed prerequisites, you can click "Detect" button to find and add it here.

NOTE: Old log files existing in the log volume generated before adding the file server in the solution will be moved to "Back Up" folder in the log volume. The following message box appears on the screen in this case.

![Add File Server](image)

*Figure 35: Message about Audit Log*

![Add File Server](image)

*Figure 34: Selected the manual auditing.*

II. Automatic Auditing: Select this option if you have not already configured auditing. You have to provide the following inputs.

- Volume Name
- Aggregate Name

Click "Next" to proceed. The solution enables auditing with following settings:
- Log Volume Size: 3 GB
- Log format: XML
- Log File Size: 1 MB

**NOTE:** LepideAuditor needs at least 3 GB of free space at the selected aggregate to enable the auditing automatically.

![Add File Server](image)

*Figure 36: Selected Automatic Auditing for NetApp*

**NOTE:** The following error message may appear when you try to apply Automatic Auditing option.

![Add File Server](image)

*Figure 37: Error message while enabling Automatic Auditing*

To solve this issue, add the aggregate in the Vserver’s list by the following command:

```
vserv modify -vserver <server_name> -aggr-list <aggregate_value>
```

To see whether the aggregate has been added to the list, use the following command:

```
vserv show -fields aggr-list
```
6. Click “Next” after providing all details and selecting the audit configuration. The next page asks for “SQL Server Information”, where you have to provide the details of SQL Server to create a database for storing auditing logs.

![SQL Server Information](image)

NOTE: If you do not have SQL Server installed then click this link to download SQL Express edition.

31. Click “Server Name” dropdown to select the desired SQL Server.

32. There are two authentication options under it.
   
   c) Windows Authentication: This mode can be selected if SQL Server is installed on the same computer where the solution is installed.
   
   d) SQL Server Authentication: Select this mode if SQL Server is installed on a remote or local computer. We recommend to select this option.

   Provide the username and password of a SQL user, who has sufficient rights to create the database.

33. Enter a database name in the database name field to create a new database. You can also select an existing database created earlier by Lepide or another application.

34. Click “Next”, after you have provided the details. At the next page, the installation of agent starts.
35. After installing the agent, “Finish” button gets activated.
36. Click “Finish” to complete the process.

6.3 Steps after adding File Server

After you have added a Windows File System or NetApp Filer, the application asks you if you want to create a new rule for File Server.

Click “Yes” to add a new rule.

NOTE: You need an Audit Rule to start monitoring of the newly added File Server. If you have to skip the step of creating rule, then you have to click "NO". However, the audit reports will not be generated until you create an Audit Rule and update the agent. It is necessary to “Update Agent” if you are creating or modifying an Audit Rule.

After the Audit Rule is created, or you clicked “NO” in above step, the following dialog box appears on the screen.
Click “OK”. Now, close the console of File Server Auditor and restart the software.

After the restart, the software displays "File Server" tab in Radar Tab and a node under "Component Management" in "Settings" Tab.

You can click "File Server" node under "Component Management" to manage the added File Server.

Click “click here” link to access the console of File Server Auditor.
1. Audit Rule Management

After you have added the File Server to the application, you have to create an audit rule for that File Server. In the audit rule, you can base your auditing on:

- Objects such as Directories, Drives, Events, Files, Monitoring Time, and Processes that you want to audit.
- Users/ User Groups actions which you want to audit.

7.1 Create Audit Rule

Follow the steps below to create a new Audit Rule. If you had selected “Yes” in the last step of the Add File Server Wizard, “Add Rule to the File Server” wizard starts automatically.

Alternatively, you can navigate to the “Audit Rules” section in the left pane and click + icon in the “Select Rule” section of the right pane to start this wizard. You can also click + in “Rules Management” in File Server page to start adding an audit rule.

1. Select Create New Rule radio button under “Add Rule” section.
2. Enter a rule name and select the File Server for which you want to create the rule if it is not already selected in the “File Servers” drop-down menu. You can select multiple file servers to apply the audit rule.
3. Click “Next”. The next step displays the audit policies.

4. Select the policy type from the following options:

   Lepide allows you to link Audit policy to both – a User and a User Group.

   a) Individual User Policy: In this case, the data will be collected as per the specified users only. Data will not be collected if the changes are made by other users, which are not listed.

   b) Group Policy: In this case, data will be collected as per the Group's policy no matter which User of the Group has logged in. That is, the policy associated with the user will be overridden by the group's policy.

   A few possible scenarios, here, are listed below.

   i. We have added four Users each of which belongs to same Group and they have same or different audit policy. Moreover, here we select "Individual User Policy". In this case, audit data will be collected as per each User's policy.

   ii. We have added four Users each of which belongs to different Groups, and they have same or different audit policy. Moreover, here we select "Individual User Policy". In this case, audit data will be collected as per each User's policy.

   iii. We have added four Users each of which belongs to same Group and they have same or different audit policy. Moreover, here we select "Group Policy". In this case, audit data will be collected as per Group's policy.
iv. We have added four Users, each of which belongs to a different group, and they have same or different audit policy. Moreover, here we select “Group Policy”. In this case, the audit data will be collected as per the policy applied on groups of each user.

Selecting Individual User policy and Group Policy will not generate report here as we have not yet created any User Group in the application. These policies can be selected only if you have pre-defined groups in the application.

c) Selected Policy: It has four options under it. The first three are pre-defined policies while the fourth one can be configured.

- **Audit All**: Audit all Files and Folders accesses to the File Server.
- **Audit Shares Only**: Audit only shared files and folders.
- **Audit all but Shares**: Audit all Files and Folders accesses except shared files and folders.
- **Create New Policy**: Create new policy where you can define what all Objects you want to audit.

**NOTE**: In this example, we are creating an audit rule with predefined policy. To create auditing rule with a user-configured policy refer to 13.1 Create a New Audit Policy section.

We are selecting Audit All policy for now.

<table>
<thead>
<tr>
<th>Policy Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Policy Type</td>
</tr>
<tr>
<td><strong>Selected Policy</strong>: Audit All</td>
</tr>
<tr>
<td><strong>Individual User Policy</strong></td>
</tr>
<tr>
<td><strong>Group Policy</strong></td>
</tr>
</tbody>
</table>

*Figure 45: Select Policy Type*

5. Click “Next” to proceed.
6. Here, you can select any of the following options to define the users.
   a. All users: The selected rule will be applicable to all users.
   b. Include Selected Users: The rule will be applicable to the selected users only. Other users will be excluded from the rule.
   c. Exclude Selected Users: The rule will not be applicable to the selected users, whereas it will be applied to all other users.

Selecting “Include Selected Users“ or “Exclude Selected Users“ enables the subsequent section. Now, you can execute the steps below to add the selected users.
   a. Perform the following steps to add the selected or all users.
      i. You can click “Add User“ button to add the users.
ii. If no user is listed here, then it means no user group has been created in the software. Refer to Section 14.1 Add User Group to know the steps to create a user group.

iii. You can also click “Add User” button here to create a new user group and add the user to it.

iv. After adding and listing the users in the dialog box, you can check the boxes of the users to include them and uncheck others to exclude them.
v. Click “OK”. It takes you back the previous wizard that now shows the list of selected users.

d. Click “Add Group” button to add the group.

![Add User Group to Rule](image)

*Figure 49: Add Group to the rule*

If no group is listed here, then it means that you have not added any group. Refer to Section 14.1 Add User Group to know more. You can also click “Add new user group list” button to add a new group.

e. Select the group and click “OK”. It takes you “Add Rule” wizard, which now shows the list of users added from the selected group.

![Select User/Group](image)

*Figure 50: Added users*
f. You can select any user here and click “Remove” button to remove it from the list.
   We are not selecting any user and applying the rule to all users in this test case.

7. Click “Next” to proceed, after you have selected the required users. The next step displays the summary.

![Rule Summary](image)

**Figure 51: Audit Rule Summary**

8. Click “Finish” to complete the process. Newly added audit rule is displayed in the list.

9. Click ‘Update Agent on all File Servers to apply new Settings’ notification and follow the onscreen instructions to update the agent.

**NOTE:** It is necessary to update the agent each time you change the applied Audit Rule. If not updated, the auditing will not be updated and the reports will not be generated as per the new modifications.

After you have created the auditing rules, you can go to “Audit Reports” Tab in the main panel to view the reports.

### 7.1.1 Common Issues of Reports

If you cannot view, the reports after doing the configuration try the following:

1. Navigate the root node of File Server Console, which displays the list of all added File Servers. Here, you have to check if the agent on File Server is properly installed and working. For the selected File Server, “Agent Status” should be “Installed” and “Auditing Status” should be started.

2. If the agent status is not installed, then install the agent and start the auditing. If the auditing status is stopped, but agent status is installed, then you should start the auditing.
3. If the agent is properly installed, check the Rule and Policy if they have been properly applied or not. Check Rule Name (box should be filled), Rule Status (it should be enabled) and Assigned Policies (policy name should display) under File Server in the left pane.

4. It is advised to use SQL authentication even if SQL Server is installed on the local system. If you cannot use SQL authentication for any reason and using Windows authentication, try the following:
   
i. Type services.msc in “RUN” and press “Enter” to access the Windows Services, on the system where the software is installed.
   
ii. Double click Lepide FSA Service, go to “Logon” tab and select “This Account”.
   
iii. Browse the username by which you have logged into the system.
   
iv. Provide the password in the given field.
   
v. In case, the username is already selected re-enter the password in the given field.
   
vi. Click “Apply” and “OK”.
   
vii. Again right-click on Lepide FSA Service and select “Restart” in the pop-up menu.

7.2 Change Priority of Audit Rule

Follow the steps below to change the priority of Audit Rule.

1. Navigate to “File Servers” section from the left panel and go to “Rules Management”.

2. In Rules Management, click ⬆ icon. It displays the following dialog box.
3. Select an audit rule and click icon to decrease its priority.
4. Select an audit rule and click icon to increase its priority.
5. Click “OK”.

NOTE: After you have created an audit rule, you can follow the similar steps to modify it. You can also delete an audit rule.

8. Create Audit Policy

By creating a new audit policy, you can ensure that you audit only the required objects such as only specified Files, Folders, Directories, Events, and Processes.

There are three default policies.

- Audit All: Select this policy to audit all objects on the File Server.
- Audit Shares Only: Select this policy to audit the shared folders only.
- Audit All but Shares: Select this policy to audit all except shared folders.

For customized auditing, you need to create an audit policy with the desired object monitoring list. While creating a policy, an administrator can set the priority of policy rules to streamline the audit report further.

Perform the following steps to create new audit policy. Then you can associate it with an audit rule to audit only selected objects.

1. Navigate to the Audit Policies in the left pane.
2. In the right-pane, go to the Policy Name section and click the + icon.

![Add New Policy Wizard]

*Figure 55: Add New Policy Wizard*
3. Enter the Policy Name and description.

4. Now, select the type of object list from the drop-down menu.
   a. Directory
   b. File Mask
   c. Process
   d. Event
   e. Monitoring Time

5. There are different ways to add each object list. Let us have a look at each of the different methods.
   a. **Add Directory**: Follow the steps below to add a directory.
      i. Select Directory and click “Add” to open the following dialog box.

      ![Add Directory dialog box](image)

      **Figure 56: Add Directory box**

      If you wish to add all directories, check “All Directories” box. You have to uncheck this option to add a customized list of directories.

      ii. Can click “Add” button to access the following options to add the directories.

         * Manually: Select this option to add a directory manually with its name. It displays the following dialog box.
Enter the name of the directory and click “OK”. It takes you back to “Add Directory” dialog box, which now displays the name of the added directory.

- Scan: Select this option to scan the File Server and select the directories from the list.

In “Scan and Add” dialog box, you have to select the name of File Server from the drop-down menu. It lists all directories in a tree structure on the File Server in the
Left Panel. You have to expand the nodes to access the directories. Select a directory and click icon to add it.

In the Right Panel, you can uncheck the directories which you do not want to add.

To remove a directory from the added list, select it and click icon to remove it.

After you have selected the directories, you can click "OK" button. It takes you back to "Add Directory" wizard.

- Default: You can select this option to add the selected default directories on the File Server. It displays the following dialog box.

![Add Default Directory](Figure 59: Add the default user directories)

Select the desired default directories and click "OK" It takes you back to "Add Directory" wizard.

iii. You can add the directories using any of the above methods. The added directories are listed in the dialog box.
iv. To delete a directory, you can select it and click “Remove” button.

v. Click “OK” after you have added the required directories. It takes you back to “Add New Policy” wizard, where all added directories are listed in the section as a separate category named – “Directories”.

*Figure 60: Displaying the added directories*
You can expand or collapse “Directories” categories.

vi. You can click “Include” radio button to include the list of added directories in the auditing, which means that only the listed directories will be audited.

vi. Click “Exclude” radio button to exclude the list of added directories from auditing.

After adding the directories, if you click “Add” button again for adding further directories, then “Modify Directory” dialog box appears onscreen. You have to follow the same steps as listed above to add or remove the directories.

b. Add File Mask: You can mention the name or extension of the files to be monitored in File Masks. Follow the steps below to add the File Masks.

i. Select “File Mask” in the drop-down menu of “Objects” and click “OK”. It displays “Add File Mask” dialog box.
If you have checked “All Files” option, then all files on the File Server will be added. However, you have to uncheck this option to add a customized list of files.

ii. The process to add File Mask is same as we have followed in adding directories except “Default” option. Click “Add” button to access the following options.

- Manually: Click this option to add a file mask manually by providing its name. Provide the name or extension of the file and click “OK”. It adds the file mask and takes you back to “Add File Mask” dialog box.
- Scan: Select this option to scan the File Server and add the selected files.
Select the files in the left panel and click the icon to add the file mask. In the Right Panel, you can uncheck the files which you do not want to add. To remove a file from the added list, select it and click the icon to remove it.

After you have selected the file masks, you can click “OK” button. It takes you back to “Add File Mask” dialog box, which displays the list of all added File Masks.
iii. To delete a File Mask, you can select it and click “Remove” button.

iv. Click “OK” after you have added the required file masks. It takes you back to “Add New Policy” wizard, where all added File Masks are listed in the section as a separate category named – “File Masks”.
Figure 66: List of added file masks

You can expand or collapse “File Masks” categories.

v. You can click “Include” radio button to include the list of added file masks in the auditing, which means that only the listed file masks will be audited.

vi. Click “Exclude” radio button to exclude the list of added file masks from auditing.

After adding the file masks, if you click “Add” button again for adding further file masks then “Modify File Mask” dialog box appears onscreen. You have to follow the same steps as listed above to add or remove the file masks.

c. **Add Process**: Follow the steps below to add the processes.

   i. Select “Process” in the drop-down menu of “Objects” and click “OK”. It displays “Add Process” dialog box.
If you have checked “All Processes” option, then all processes running on the File Server will be added. However, you have to uncheck this option to add a customized list of processes.

ii. Click “Add” button to access the following options to add the processes.
   - Manually: Click this option to add a process manually by providing its name. Provide the name of the process and click “OK”. It adds the process and takes you back to “Add Process” dialog box.
   - Default: Select this option to choose the processes from a predefined list.
Check the boxes of those processes, which want to add. Click “OK” after you have made your selection. It takes you back to “Add Process” dialog box that now shows the list of added processes.
vii. To delete a process, you can select it and click “Remove” button.

viii. Click “OK” after you have added the required processes. It takes you back to “Add New Policy” wizard, where all added Processes are listed in the section as a separate category named – “Processes”.

![Add New Policy](image)

*Figure 71: List of added processes*

You can expand or collapse “Processes” categories.

ix. You can click “Include” radio button to include the list of added processes in the auditing, which means that only the listed processes will be audited.

x. Click “Exclude” radio button to exclude the list of added processes from auditing.

After adding the processes, if you click “Add” button again for processes, then “Modify Process” dialog box appears onscreen. You have to follow the same steps as listed above to add or remove the processes.

d. **Add Event**: Follow the steps below to add events.
   
i. Click “Add” button to access the following dialog box, which has two tabs.
ii. In both tabs, you can check the boxes of the events to be added.

iii. You can uncheck the events, which you do not want to add.

iv. Click “OK” after you have selected the required events. It takes you back to “Add New Policy” wizard, where all added events are listed in the section as a separate category named – “Events”.

Figure 72: Add File Event

Figure 73: Add Folder Event
Figure 74: List of added events

You can expand or collapse “Events” categories.

v. You can click “Include” radio button to include the list of added events in the auditing, which means that only the listed events will be audited.

vi. Click “Exclude” radio button to exclude the list of added events from auditing.

After adding the events, if you click “Add” button again for events, then “Modify Event” dialog box appears onscreen. You have to follow the same steps as listed above to add or remove the events.

e. Add Monitoring Time: Follow the steps below to add monitoring time.

i. Select “Monitoring Time” in “Objects” drop-down menu and click “Add” button to access the following dialog box.
ii. You have to select any of the following options in the drop-down menu.

- Always: Select this option to audit always.
- Daily: Select this option to audit daily. You have to provide the start and end time for the auditing.

Figure 75: “Add Monitoring” Time dialog box

Figure 76: Add Daily monitoring time
- **Weekly**: Select this option to audit on a weekly basis. Define the start and date time. Select the days on which the auditing will be performed.

- **Monthly**: Select this option to audit on a monthly basis.
Define the start and end time for auditing. Select the months and define the day on which the auditing will be performed.

- **One Time Only**: Select this option to run the auditing only once at the selected date and time.

iii. Select the required option and provide the necessary input for it as explained above.

iv. Click “OK” to add the selected monitoring time. It takes you back to “Add New Policy” wizard, which now shows the added monitoring time.

6. After you have added the required objects of the different categories such as directories, file masks, processes, and events, you can now select whether to include the entire category in the auditing or not.
7. The defined monitoring time specifies when the auditing will be done.
8. You can select a category and click “Remove” button to remove it from the auditing list.
9. Click “OK” to create the new audit policy.
10. If the notification appears, then you have to update the agent as well.

NOTE: You can follow the above similar steps to modify an existing user-created audit policy. The software also allows you deleting an audit policy.
9. Add User Group

You can create “Users Groups” of the selected users in an organization to apply similar policies over the groups. With the User Groups Section, you can create a group of individual users. The users of the user group are assigned a common policy and the users added to the User Group List are by default added to the User List.

Click “User Group” option on the Left Panel to add, modify, or delete the user group.

Follow the steps below to add a new user group.

1. Click icon, “Add New User Group” dialog appears.
2. Enter the name and description of the new user group.

   ![Add User dialog box]

   *Figure 81: Add User dialog box*

3. Click “Add” button and select any of the following options to add the users.
a. **From AD**: Select this option to obtain the users from Active Directory to form a user group. It contains the following options.

   i. **Users**: You can select this option to add the users of Active Directory.

   Follow the steps below to add the users.

   - Select the domain from the drop-down menu or type a domain name manually.
   - Click “Find” to list all available users.
• You can tap and hold CTRL button to select multiple users.

• Click "OK" to add the users.

It takes you back to “Add User” wizard, which now shows the list of added users.

ii. Groups: You can select this option to add the users from a group.

Follow the steps below to select the group. All users in the selected group will be added.

- Select the domain from the drop-down menu or type a domain name manually.
- Click “Find” to list all available groups.
- You can tap and hold “CTRL” key to select the multiple groups.
- Click “OK” to add the groups.

It takes you back to “Add User” wizard, which now shows the list of users added from the selected group.

iii. Containers/OUs: You can select this option to add the users from a container or organizational unit.
Follow the steps below to select the container of which all users will be added.

- Select the domain from the drop-down menu or type a domain name manually.
- Click “Find” to list all available containers or Organizational Units.
- Check the boxes of containers or organizational units, from which you want to add the users.
- Click “OK”.

It takes you back to “Add User” wizard, which now shows the list of users added from the selected container.

b. **Manually**: Select this option to add the user manually by providing its username and name of its domain or computer.
Follow the steps below to add a user manually.

i. Enter the username.

ii. Enter the name of the domain or computer.

iii. Select whether it is a local user or a domain user.

iv. Click “OK” to add the user. It takes you back to “Add User” wizard that shows the added user.

c. **Local User**: Select this option to add the local users.
Follow the steps below to add the local user.

i. Select the domain from the drop-down menu or type a domain name manually.
ii. Click “Find” to list all available computers and their local users.
iii. Check the boxes of the users, which you want to add.
iv. Click “OK”. It takes you back to “Add User” wizard, which now shows the list of added users.

![Add User Window]

Figure 88: List of added users

4. To remove the user(s), you can select the user(s) and click “Remove” button.
5. You can use the drop-down menu of “Apply Policy” to select the audit policy applicable for the added users. It lists three default audit policies (Audit all, audit shares only, and audit all but shares) and all customized audit policies created in the software.
6. Click “OK”. It creates the user group for the selected policy.
7. The notification appears on screen to update the agent. You have to update the agent to make the modifications in the auditing of the File server.

NOTE: Perform the same steps, mentioned above, to modify an existing user group. The software also allows you deleting a user group.
10. 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

10.1. Activating Online

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

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

2. Select "Activate Online" and enter the Licensing ID and Password and hit Update License.
Activation

- **Activate Online**
- **Activate Offline**

License ID: [Enter License ID]  
Password: [Enter Password]

Response: [Enter Response]

![Figure 90: License Activation Tab](image)

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 92: 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.

**Figure 93: License Activated Successfully**

10.2 Activating Offline

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

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

**Figure 94: Update License Tab**

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

---

© 2020 Lepide Software Pvt. Ltd.
3. You will get a pop-up saying, “License request file generated successfully at: Your Desktop”. Just hit “OK”.

*Figure 95: License Activation Offline*
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 98: Manual Request**

![Image of Manual Request screenshot]

<?xml version="1.0" encoding="utf-8"?>
<GetLicenseFile>
  <EncryptedData Id="PrivateData" Type="http://www.w3.org/2001/04/xmlenc#Element" xmlns="http://www.w3.org/2001/04/xmlenc#">
    <CipherData>
      <CipherValue>Y2k1PcNJNeqPX6Nl0m0tR4QPUNr8qAoELJPI1y351F1qG+FYrAYfHDXyptMQ+S9xtT5ury/Tbdt1992+FeJgznM5tk57o74+efjgk465fWxCu3S4Gxa35E6LDPaEUFCfDWz9XYpovcW78jQSNKZ57HvQSLE/cm0xSdp/tIe3YspHggHSCItD67vS123v+OzAy/jH9v1h3gJcDP7djPM9OaAhjJY19MB44FCgljijZ1l2pKvKwFbKLEuFC13tmjuVnXixQtw8bhN82gYdtyg/17vq/j9F1wpX/11U+TWe0TR7dp8Afe9/iBYyq/j</CipherValue>
    </CipherData>
  </EncryptedData>
</GetLicenseFile>
7. You will be presented with the screen saying, “License Information updated Successfully”. 

Figure 99: Activate License
Activation

- Activate Online
- Activate Offline

License ID: 63493198
Password: [Field]

License information updated successfully.

Response:
```xml
<?xml version="1.0" encoding="utf-8"?>
<GetLicenseFile>
  <EncryptedData Id="PrivateData" Type="http://www.w3.org/2001/04/xmlenc#Element" xmlns="http://www.w3.org/2001/04/xmlenc#">
    <CipherData/>
  </EncryptedData>
</GetLicenseFile>
```

8. Once you click OK, it will give you a pop-up for restarting the software. Please hit “Yes”.

Figure 100: License Information Update
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.

<table>
<thead>
<tr>
<th>Component</th>
<th>License Type</th>
<th>Valid for</th>
<th>Valid Upto</th>
<th>Support Valid Upto</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Online Server</td>
<td>Subscription</td>
<td>300 Mailboxes</td>
<td>02/27/2018 11:59:59 PM</td>
<td>02/27/2018 11:59:59 PM</td>
</tr>
<tr>
<td>SharePoint Server</td>
<td>Subscription</td>
<td>300 Concurrency</td>
<td>02/27/2018 11:59:59 PM</td>
<td>02/27/2018 11:59:59 PM</td>
</tr>
<tr>
<td>SharePoint Online</td>
<td>Subscription</td>
<td>100 Unsubscribed</td>
<td>02/27/2018 11:59:59 PM</td>
<td>02/27/2018 11:59:59 PM</td>
</tr>
<tr>
<td>SQL Server</td>
<td>Subscription</td>
<td>15 Concurrency</td>
<td>02/27/2018 11:59:59 PM</td>
<td>02/27/2018 11:59:59 PM</td>
</tr>
</tbody>
</table>

Figure 101: License Updated

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.
11. Uninstall Lepide Data Security Platform

Make sure to close the software before uninstalling it. Follow the steps below to uninstall it.

1. There are two ways to start the uninstallation.
   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. After uninstallation, the dialog box confirming the successful uninstallation appears onscreen.

5. Click “OK” to finish the process.
After following the above steps, Lepide will be uninstalled successfully from your computer. By default, the software 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.

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

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](mailto:sales@Lepide.com)
- [support@Lepide.com](mailto:support@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.


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

UNIX® is a registered trademark of The Open Group.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.