Lepide Data Security Platform

Current Permission Report
Table of Contents

Table of Contents .................................................................................................................................................. 2

1. Introduction ...................................................................................................................................................... 3

2. Current Permission Scan Settings .................................................................................................................. 3
   2.1 Configure SQL Server .................................................................................................................................. 3
   2.2 Stale Object Settings ................................................................................................................................... 5
   2.3 Available Options to manage the data set .................................................................................................. 6
       2.3.1 Add Data Set .................................................................................................................................. 6
       2.3.2 Scan Permissions Now ....................................................................................................................... 14
       2.3.3 Modify Data Set ................................................................................................................................ 14
       2.3.4 Remove Data Set .............................................................................................................................. 17

   3.2 Steps to Generate Current Permission Report ............................................................................................ 18
       3.2.1 Row Filter .......................................................................................................................................... 19
       3.2.2 Sorting ............................................................................................................................................ 20
       3.2.3 Manual Scan of Permissions ............................................................................................................ 20
       3.2.4 Permission Report of User Only ....................................................................................................... 21
   3.3 Account Filter .............................................................................................................................................. 21

3.4 Effective Permissions ....................................................................................................................................... 22

3.5 Analyze Current Permissions ......................................................................................................................... 23

3.6 Explore Group Membership ............................................................................................................................ 24

3.7 Investigate Permissions ................................................................................................................................... 25

3.8 Other Reports .................................................................................................................................................... 25

4. Support ............................................................................................................................................................... 26

5. Copyright ............................................................................................................................................................ 26

6. Warranty, Disclaimers, and Liability Limitations .............................................................................................. 26

7. Trademarks ......................................................................................................................................................... 27
1. Introduction

Lepide Data Security Platform provides a comprehensive means of auditing on-premise and cloud platforms.

This document is focused on the Current Permission Report of File Server. It shows how to configure Current Permission Scan Settings, create Data Set, scan the permissions, and generate the Current Permission Report.

2. 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.

![Figure 1: Current Permission Scan Settings](image)

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

2.1 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.

   ![Configure SQL Server Settings](image)
2. The software 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 access a dialog box, which enumerates all SQL Servers in a list.

3. Click icon to expand the listings for local and network servers. You can click icon to collapse the list.

4. Select a server and click "OK" to go back to the "SQL Server Settings" box, which now shows the selected SQL Server.

5. You have to select any of the following authentication types.
   a. **Windows Authentication**: It lets the software 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.

6. You have to provide a database name in the text box saying "Database". If you are reinstalling the software, 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.
7. Click **Test Connection** to test the connection between the software 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 successful](image)

*Figure 3: The connection to SQL Server is successful.*

**NOTE:** You can click ![icon] to save the current SQL Server Settings as default in "Default SQL Server Settings".

8. 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.

![Data Set Management](image)

*Figure 4: Selected SQL Server and its database*

### 2.2 Stale Object Settings

Stale Objects are those that are not accessed for a period of time. You can use the drop-down menu to define the time limit after which an object can be defined as a Stale Object. The drop-down menu contains the following options, whichever you select will be applied on all Data Sets.

1. 30 days
2. 90 days
3. 180 days
4. More than 365 days
If all objects are being displayed as Stale Objects or the status of the stale objects is not being displayed correctly, then it means that the date/time of the last access or modification to a file/folder has not been 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 accurate 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:
   ```
   fsutil behavior set disablelastaccess 0
   ```

![Figure 5: Execute the command to update the last access time](image)

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

### 2.3 Available Options to manage the data set

#### 2.3.1 Add Data Set

Click icon to create a Data Set using the following wizard. The database you configured above is not created until you add a Data Set and start its scanning.
Follow the steps below.

1. Enter the name and description for 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.

*Figure 7: Add the folders*
Figure 8: Add Folders in a Data Set

b. Select the File Server from the drop-down menu. It lists the folders in the left column "File Server folders".

NOTE: Do not add the shared folders of the file servers of the different domains in a Data Set. It is recommended 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 in the selected folder as well.

f. To remove an added folder from the Data Set, select the folder in the right column and click \( < \) button.

g. Click "OK".
It takes you back to the previous wizard, which shows the added folder. The current permissions of the added folders will be monitored.

![Add Data Set](image)

**Figure 9: A folder has been selected.**

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. Check “Schedule Permission Scan” box to activate the subsequent section. Follow the steps below,

   i. Click “Change Schedule” button to access the following dialog box.

   ![Figure 10: Options to scan the permissions](image-url)
Figure 11: Options to schedule the scan

It contains the following options.

- **Daily**: Select this option to scan the folders on a daily basis for updating the permissions. After selecting it, 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" after 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 software also fetches the permissions from any Domain Controller, which hosts Active Directory.

The software, at first, uses the login credentials that are provided while adding a File Server. If these credentials fail to authenticate the request, then the software 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-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 software collects the nested group membership and permissions using the provided credentials.

7. Click “Finish” after 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.
2.3.2 Scan Permissions Now

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

2.3.3 Modify Data Set

Select a Data Set in the list and click icon to modify the selected Data Set with the following dialog box.
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 already added folder and add new folders.

**Figure 15: Wizard to modify the Data Set**
Figure 16: Change 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.

Figure 17: Scanning Options
Click "OK" at any option to save the changes in a Data Set.

2.3.4 Remove Data Set

If the data set is deleted, the software 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.

NOTE: There is no other way to retrieve it back.

Follow the steps below to remove a Data Set.

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

![Figure 18: Warning before you delete a Data Set](image)

2. Click "Yes" to remove the selected Data Set

3. File Server Current Permission Report

Select File Server under "Current Permission Report" to access the current permission report of the Shared Folders and its files & folders. You have to configure "Current Permission Scan Settings" to start analyzing the permissions.

*Know more...*
3.2 Steps to Generate Current Permission Report

Follow the steps below to view the permission changes and compare the permission of files and folders.

1. Click the **Generate Report** button in the Top Section to generate the report of Permission Analysis. If no changes in permission on the selected File Server are detected, then "No Changes Detected" message will be displayed in “Permission Section”.

2. In the left pane of Right Panel, select the file server and expand its nodes to select the desired folder.

3. Select a folder and its contents will be displayed in Object Section.

4. Permission details of the selected folder of Left Pane or the selected file in Object Section are displayed in “Permission Section”.

5. You can use the Top Filter Section to apply any or multiple of the following filters.

6. You can view the analysis report in "Permission" tab with or without applying filters.
7. Left Pane and Object Section in the Right Panel contain the following icons.
   a. Icon: It shows that permission is assigned to everyone.
   b. Icon: It indicates that the permission inheritance is broken at this level.
   c. Icon: It shows that the selected object is a stale object. If all objects are appearing as stale, then make sure that stale object settings on the server is set correctly.
   d. Icon: It shows that the object, which is accessing the selected object, is a group.

**NOTE:** If the status of stale objects is not displaying correctly, then it means that the date/time of the last access or modification to a file/folder is not updated. Refer to Section 2.2 Stale Object Settings to know more.

3.2.1 Row Filter
8. The top row of both "Objects Section" and "Reports Section" is the filter row. In any cell, you can type a word to filter their content.
3.2.2 Sorting

9. You can click any column header in "Object Section" or "Reports Section" to sort the content in the ascending or descending order.

3.2.3 Manual Scan of Permissions

10. In "Object Section", you can right click on any folder to access the following context menu.

It contains the following options.

a. **Scan this folder only**: Select this option to scan the permissions for the selected folder only.
b. **Scan this folder and sub folders:** Select this option to scan the permissions for the selected folder and its sub-folders.

### 3.2.4 Permission Report of User Only

11. There are two tabs in the Reports section.
   a. **Permission:** It displays the current permissions of the selected object.
   b. **Permission by User:** It displays the Current Permissions sorted by the users. Here, only the permissions of the users are displayed.

![Permission Report of User Only](image)

*Figure 23: Permission By User Report of "Shared 1" folder*

### 3.3 Account Filter

You can type the name of User Account in "Account Filter" text box to filter the report of the current tab as per the user account.

![Account Filter](image)

*Figure 24: Applied "Account Filter" for "Administrators" keyword on Direct Permission Report of "Shared 1" folder*

You can click icon, which is next to the textbox, to remove the account filter.
3.4 Effective Permissions

Effective Permissions are the final resultant permissions on an object, which are calculated after analyzing the NTFS and Share Permissions on it. Here, the drop-down menu lists all permissions for a file or folder. You can check any of these permissions to view the account, which have the selected permission on an object. The following table lists the different permissions and their icons that represent them in the Current Permission Report.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Icon in Header Row</th>
<th>Icon in Report</th>
<th>Color in Permission Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List folder / read data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create files / write data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create folders / append data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read extended attributes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write extended attributes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traverse folder / execute</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete subfolders and files</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read attributes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write attributes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td></td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Read permissions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change permissions</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 3.5 Analyze Current Permissions

The icon appears with the object in "Current Permission Report". Click it to view the source, from where the effective permission comes to the selected object. Effective Share Permissions are those, which are applied in the "Sharing" tab of the shared folder, whereas the NTFS Permissions are those, which are applied in the Access Control Lists of the shared folder.

![Effective Permissions Diagram]

*Figure 25: Effective Permissions*

Each permission has a different color. Table 1 lists the name and color of permissions. Here, you can analyze the permission flow for an object. You can scroll down to see the detailed report.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Icon in Header Row</th>
<th>Icon in Report</th>
<th>Color in Permission Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take ownership</td>
<td></td>
<td></td>
<td>![Gray Icon]</td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 1: List of the Effective Permissions, their icons and colors in Permission Calculation*
3.6 Explore Group Membership

If you have selected "Scan Nested Group Membership and Permission", then an icon appears with the Groups listed in the Permission Report. Click this icon to view the group memberships in the following dialog box.

![Displaying Group Memberships](image)

**Figure 26: Displaying Group Memberships**

You have to modify the Data Set and apply "Scan Nested Group Membership and Permission" Settings and then scan the permissions to access this group membership dialog box. Refer to Section 2.3.3 Modify Data Set to know the steps.

The icon appears in Permission Report or in "Explore Group Membership" for the groups. You can click it to view the permissions of a group.

![Explore Group Permissions](image)

**Figure 27 Explore Group Permissions**
3.7 Investigate Permissions

Click icon to investigate the changes in the permissions of the selected object. It displays "Historical Permission Analysis" for the selected object to let the Administrator investigates how the permissions are changed.

![Figure 28: Investigate Permission](image)

3.8 Other Reports

There are different icons on the top right corner as displayed in the image.

1. Click icon to sort the report as per the inherited permissions.
2. Click icon to sort the report as per the direct permissions.
3. Click icon to sort the report as per the indirect permissions.
4. Click icon to save the report.

4. 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/)

5. 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.

6. 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.

7. 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 US and/or other countries.