%Lepide

USE CASE GUIDE

HOW TO MONITOR NON-OWNER MAILBOX ACCESS

Table of Contents

1	Introduction	3
2	Mailbox Access Auditing	3
3	The Lepide Solution	3
	3.1 The Mailbox Accessed by Non-Owners Report	3
	3.2 Prerequisites	3
	3.3 Running the Report	4
	3.4 Creating an Alert	7
4	Support	20
5	Trademarks	20



1 Introduction

Shared mailboxes are a great way for a specific group of people to perform certain tasks from a common account. However, having shared mailboxes introduces a high risk of security incidents. With non-owners having privileged rights to access shared mailboxes, there's always a chance that they might wrongly handle emails with sensitive information.

Whether it is done accidentally or maliciously, a message could be deleted, sent to a wrong recipient, or moved to another location and any of these situations may result in data loss or leaks. To avoid any security incidents, it is highly recommended that users regularly monitor non-owner access to shared mailboxes.

2 Mailbox Access Auditing

There are many situations where employees may need to give other people access to their mailboxes, examples include the case of an employee with a personal assistant or teams of people that might use shared mailboxes to communicate better. Whatever the reason, it's important that proper auditing is maintained on shared mailboxes to avoid unwanted changes going unnoticed. This, however, can be a complex and time-consuming task without a proper solution in place.

3 The Lepide Solution

Using the Lepide Data Security Platform, you can audit mailboxes based on specific user access and instantly get alerts and receive regular reports showing you who, what, when and where a specific mailbox was accessed and what actions were taken.

3.1 The Mailbox Accessed by Non-Owners Report

The Mailbox Accessed by Non Owners Report identifies mailboxes that have been accessed by somebody other than the mailbox owner, and the actions that were taken.

This report is available for both Exchange Server and Exchange Online.

3.2 Prerequisites

You will need to have installed the following components:

- For Exchange Server, you will need an Active Directory component. For information on how to install and configure this, please refer to the <u>Active Directory Quick Start Guide</u>.
- For Exchange Online, you will need an Exchange Online component. For information on how to install and configure this, please refer to the <u>Microsoft 365 Quick Start Guide</u>.

For Exchange Online, Non-Owner mailbox auditing is enabled automatically when the component is installed.

For Exchange Server, Non-Owner mailbox auditing can be enabled either during installation of the component or after installation via Properties, Advanced Domain Configuration. For more information, please refer to the <u>Configure Mailbox Access Auditing Guide.</u>

3.3 Running the Report

Click the User Behavior & Analytics icon

The report is found in the tree structure on the left-hand side:

For Exchange Server:

- Expand the Active Directory name
- Expand Exchange Modification Reports
- Expand Auditing
- Expand All Mailbox Access Reports
- Click on Mailbox Accessed by Non Owners



Figure 1: Exchange Server Folder Structure

For Exchange Online:

- Expand Exchange Online
- Expand Auditing
- Expand All Mailbox Access Reports
- Click on Mailbox Accessed by Non Owners



Figure 2: Exchange Online File Structure

The Mailbox Accessed by Non Owners screen is displayed:



Figure 3: Mailbox Accessed by Non Owners Report

The example above is an Exchange Online Report but the Exchange Server Report works in the same way.

• From the top of the screen, click **Today**

The following dialog box is displayed:

When	:				
Today		When Filter			×
		Filter Criteria:	Today Today Yesterday This Week Previous Week	¥	
olumn.			This Month Previous Month Custom Date Range		

Figure 4: When Filter

• Select a date range and click **OK**

You will return to the Mailbox Accessed by Non Owners screen

• Click on **Operation**

The following dialog box is displayed:

▼ Operation +	Operation Filter	×
থ When +	Filter Criteria: NotEqualTo •]
Grid View Graph View	Operation	
Drag a column header here to group b		o
Action Performed by	Copy Create	
Q	FolderBind	
	Hard Delete Message Bind	
	Move	
	MoveToDeletedItems	-
	OK Cancel	

Figure 5: Operation Filter

- Change the Filter Criteria to **Not EqualTo**
- Check FolderBind

FolderBind will show every time the mailbox is accessed so it is better to filter this out to reduce unnecessary data being retrieved by the report.

- Click **OK**
- Click Generate Report

	the second second second		-			
States & Behavior	lepidesoftware.onmicrosoft.	.com(Exchange Online)\Mailbox Ar	cessed by Non Owners			Ŷ
teanh	Y Action Performed by +	When II	Operation	E . K		
All Environment Changes	7 Action Performed on +	Cutton Date Earon	Netfanalle	×		
Anomaly Analysis	7 Augustus	1/1/2022 12:00 AM To	FolderBind			
[] [] 110.16L20.192(SharsPoint]		7/8/2022 11:59 PM				
Contraction Class Resort	• When •					
Account Lockout Report						Generale Report
E 🔐 Active Directory Reports						
🗄 🎑 Group Policy Reports	COLUMN CONTRACTOR					
E Exchange Modification Reports	Drag a outures header here to group t	by that column.				B Q .
IR La MS Exchange Modelsetten Reports	Active Performed by	37 Action Performed on	of Operation	J When	17 What J	
E All Malkov Access Reports	Ø	P	0	0	0	
Malbox Accessed by Non Owne	n Smin	Gerana	Indiated	3/15/2022 3 50-49 PM	Sent Mail Details Subject SWAF	
T Mailton Accessed by Administra	A Seco	German	Man	3/15/2022 3:50 49 PM	Woord Inne Details From Follow	
 Melbox Accessed by Delegated 	U Secon	Genna	ToltCelete	3/15/2022 3 45 20 PM	Deleted Accessed Datals Free F	
Multer Accessed by Camera	Smon	Germa	SoltCalate	3/15/2022 3 45 20 PM	Deleted Accessed Datala Fices F	
C favortes	Seon	Germa	Here	3/15/2022 3.44.49 FM	Moved tions Datails From Fulder	
(i) Construction and the second se	Sean	Garwa	Neve ToDistandaria	3/15/2022 3.44.49 PM	Moved Items Datails	
1 Exchange Online Modification Reports	Seron	Gerria	Move To Deletecherra	3/15/2022 3 44.19 PM	Moved Items Datals . From Folder	
in 🔄 Auditing	ting Seen Germa MoveTuDetractione 3/15/2022 3.44.18 PM MoveTuDetractione	Moved Items Datails . From Folder				
11 Al Malbos Access Reports	Seron	n General Switch Brief 3/15/2522 3 43 47 PM See Mal Datals - Subject Fer S-				
Mailbox Accessed by Non Duners	Smon	Genna	Create	3/15/2022 3.43.18 PM	Created Adubuter Details In Felder	
Malbox Accented by Administrator	Seen	Gerena	Development.	3/15/2022 3:43:17 PM	Sent Mal Detals Subject : Re: 5	
Marbox Accessed by Delegated Use	5mon	Germa	Onde	3/15/2022 3.42.50 PM	Created Atsteate Details In Folder	
Tavortes	Seon	Genna	SendOrithd	3/15/2022 3.42.49 PM	Serk Mal Details Subject : SWIF	
a D lepidetoffware-admin.charepoint.com/SharePo	s Serien	Germa	Osate	3/15/2022 3:42:18 PM	Created Attribute Databa In Folder	
in Ca. lepidesoftware.onmicrosoft.com/Office 385	Sevin	Jason	Marre	3/15/2022 3 38:53 PM	Moved Items Datals From Folder	
Diplore Backup	Seon	Jaaon	HardCelety	3/15/2022 3.38.52 PM	Deleted Atstate Details Subject	
Console Auditing	Sean	Jacon	HasExiste	3/15/2022 3 38:52 PM	Deleted Atribute Details Subject	
	Seen	Junori	HartExiste	3/15/2022 3 38 23 PM	Deleted Athleute Details Subject	
	Seen	Jacon	SelfCedate	1/15/2022 3 38 23 PM	Deleted Accessed Details From F	
	Seron	Januari	DeliCentry	3/15/2022 3 38 22 PM	Debited Accessed Debute Prov F	
	Smon	Janur	Solition	3/15/2022 3.30 22 PM	Updated Accessed Database Prov F	
	Seen	- Annon	Deficients D.A.D. State	5/15/2022 3 38 21 PM	Debuted Accessed Debute Pres F	
	2000		DORL BRID	Sector and a 30 21 PM	Manual Accessing Longing Control Party	
	fame	have	March To The State Street	3/15/2012 3 3/22 PM	Marcal Anton Parlament Press Parlament	
	in the second seco	12.5	inch.	1/16/2022 3 27.24 PM	See Hall Details . School Materia	
	Seco	here	Marco To Todate officers	3/16/3022 3 37 21 FM	Moved here Datale Free Folder	
		1.000	Conde	LAL MAN S M C IN	Constant Restricts - Deside - In Galder	

Figure 6: The Generated Report

The Report is displayed and shows who performed the action, the owner of the mailbox the action was performed on, what was done, when it was done and more detail what the activity was.

3.4 Creating an Alert

You may want to create an alert for non owner mailbox access so you are notified as soon as a particular event occurs. For example you may want to be notified if a message is moved to deleted items by a particular user.

An alert can be created from the Exchange Server Non Owner Mailbox Report within the Lepide Data Security Platform as follows:

• Right click on the Mailbox Accessed by Non Owners Report



A menu is displayed:

• Choose Set Alert

A Wizard will start, and the Select Reports dialog box is displayed:

		×
Please select the report(s)		
Please select the report(s) for setting alert.		
Imit LPDE Llocal Imit Lockout Report Imit Lockout Report Imit Lockout Report Imit Lockout Report		
Group Policy Reports Exchange Modification Reports Giran MS Exchange Modification Alerts		
in Auditing in All Mailbox Access Alerts in In Mailbox Accessed by Non Owners		=
Image: Mailbox Accessed by Administrators Image: Mailbox Accessed by Delegated Users Image: Mailbox Accessed by Owners		
Image: Server Reports Image: Image: Image: Server Reports Image: Image: Image: Image: Server Reports Image: Image: Image: Image: Image: Image: Image: Server Reports Image:		~
	(Deels Next)	Creat
	< <u>Back</u> <u>N</u> ext >	Cancel

Figure 8: Select Report(s)

Ensure that the report on which you want to set an alert is checked. In this case, it is the Mailbox Accessed by Non Owners report.

• Click Next

The Set Filter(s) dialog box is displayed:



Set Filter(s) Please select operations to set the filter(s), (Optional)	
LPDE1.Jocal E	Action Performed by Action Performed on Operation Include All • •	
< >	III Threshold Alert Send alert only if event occurs 2 times in 1 Minute(s) *	>
	< <u>B</u> ack <u>N</u> ext > Can	icel

Figure 9: Set Filter(s)

On the left of the dialog box, you can see the report you are working on which in this case is **Mailbox Accessed by Non Owner**.

There are options to change the settings for **Action Performed by, Action Performed on and Operation.** The default setting for all these options is **All**.

The threshold alert options can be customized as follows:

Threshold Alert:	Check this box to switch threshold alerting on
Send alert only if event occurs:	Change the number of times the event occurs, the time value and time-period here

• Click Next

The **Alert Settings** dialog box is displayed:

Action	Detaile	
Email Execute Script LiveFeed	Sender's Email : LEPIDE; Recipient's Email : paul@lpde1.local; <sendemailtouser>NO<\Send Sender's Email : N/A; Recipient's Email : N/A; Script Path : C:\disableuser.bat; Profile Name : S Generate LiveFeed Alert</sendemailtouser>	EmailToUser> SYSTEM; Paramet

Figure 10: Alert Settings

This dialog box allows you to set up responses to occur when an alert has been triggered and displays any existing responses which have been set up. You can also change the **Alert Type**.

• To create a new response to an alert, click the **Add** button.

The **Add Alert Action** dialog box is displayed:

X
d Alert Action
Send Email Alert
ase select or add new sender's email account, add recipient(s).
nder/Recipient
Sender's Email Account : Add New Email Account
Decisions Emeral/ch
· · · · · · · · · · · · · · · · · · ·
<
Separate multiple emails by ","
OK Cross
Cancer

Figure 11: Add Alert Action

• Click the **Select Action** drop down arrow to see a list of actions available:

Add Alert Action		
ad meren celon		
Select Action : Send Email Alert	*	
Send Email Alert Show in LiveFeed	pot(s)	
Execute Script) Ent(s).	
Sender/Recipient		
Sender's Email Account :	← Add New Email Account	
Recipient Email(s):		
	,	_
		~
	< >	
	Separate multiple emails by ","	

Figure 12: Add Alert Action Options

The Alert Actions are as follows:

- Send Email Alert
- Show in LiveFeed
- Send Alert to App
- Execute Script



The configuration of each of these actions is explained below:

1. Send Email Alert

		×
Add Alert Action		
Select Action : Send Email Alert	*	
Please select or add new sen	der's email account, add recipient(s).	
Sender/Recipient		—
Sender's Email Account :	→ Add New Email Account	
Recipient Email(s):		
	< >	
	Separate multiple emails by ","	
	OK Cancel	

Figure 13: Add Alert Action – Send Email Alert

This option allows you to send an email once an alert has been triggered. The elements of the dialog box are as follows:

Sender's Email Account:The Sender's email account will be displayed here if it has been selected. ClickAdd New Email Accountto enter a new Sender's Email Account

Recipient Email(s):Add recipient emails by typing the email addresses into the box. If there are
multiple email addresses. separate them with a ','

• Click **OK** to save the alert action.

2. Show in LiveFeed

	×
Add Alert Action	
Select Action : Show in LiveFeed	
Click OK button to set LiveFeed Alert	
OK Cancel	

Figure 14: Add Alert Action - Show in LiveFeed

Show in LiveFeed means that the alert will be sent to the Lepide dashboard.

• Click **OK** to switch the **LiveFeed** alert on.



3. Send Alert to App

	×
Add Alert Action	
Select Action : Send Alert to App	
Select sender's app account, add new account.	
Sender / Recipient	Add App Account
	^
	v
×	7
OK Cancel	

Figure 15: Add Alert Action – Send Alert to App

The **Send Alert to App** option sends the alert to a mobile device.

• Click **Add App Account** to add a new mobile account. The following dialog box is displayed:

	×
Add App Account	
Please enter login credentials for using both Windows and Mobile App	
User ID :]
Password :]
Mobile App ID : 937238E5-AE51-4295-8313-FE477113B768]
NOTE : Use this App ID to configure App on Android, iOS and Windows.	
OK Cancel	

Figure 16: Add App Account

- Enter the User ID and Password
- Enter the **Mobile App ID** which is generated by using the mobile device to scan the QR code displayed at the bottom of the dialog box.
- Click **OK**

4. Execute Script

		×
Add Alert Action		
Select Action : Execute Script	•	
File Path :		
Run with SYSTEM account		
ORun with selected account	▼ Ade	d Account
Notify me when script is executed	Configure	
Parameterized input file contains	Who - Information	
Note: This option is applicable for file	server reports.	est Script
	-	
	OK Cancel	

Figure 17: Add Alert Action – Execute Script

The last action from the drop-down menu is **Execute Script**

This sets up the option to execute one of the predefined PowerShell scripts when an alert is triggered.

The elements of the dialog box are as follows:

File Path: Browse to choose the file path of the PowerShell script by clicking

Choose either Run with SYSTEM account or

Run with selected account.

If you choose **Run with selected account**, you can use the drop-down to select the account or click **Add Account** to specify the account to be used.

Choose **Notify me when a script is executed** to send an email on script execution.

When this option is checked, the **Configure** button becomes available. Choose **Configure** to set up the sender's account and recipient's email address.

Choose **Parameterized input file contains** to specify a variable to include in the script. When this option is checked, a drop-down menu becomes available to choose a variable:

Who	*
Who	
Where	
FileServer	
WhoWhere	
WhoFileServer	
WhereFileServer	
All	

Figure 18: List of Variables

- Click **Test Script** to test that the specified script runs with no errors.
- Click **OK** to return to the **Alert Settings** dialog box.

Action		nemove
Email Execute Script	Sender's Email : LEPIDE; Recipient's Email : paul@lpde1.local; <sendemailtouser>NO<\SendEmailToUser>Sender's Email : N/A; Recipient's Email : N/A; Script Path : C:\disableuser.bat; Profile Name : SYSTEM; I</sendemailtouser>	ser> Paramet
LiveFeed	Generate LiveFeed Alert	

Figure 19: Alert Settings - Alert Type Options

- Now choose the **Alert Type** which can be Critical, Warning or Normal
- Click **Next** to continue

- The **Confirmation** dialog box is displayed with the alert details. •
- Click Finish to return to the States & Behavior screen. •



4 Support

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

Product Experts

USA/Canada: +1(0)-800-814-0578 UK/Europe: +44 (0) -208-099-5403 Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578 UK/Europe: +44 (0) -208-099-5403 Rest of the World: +91(0)-991-085-4291

Alternatively, visit <u>https://www.lepide.com/contactus.html</u> to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

5 Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft[®], Active Directory[®], Group Policy Object[®], Exchange Server[®], Exchange Online[®], SharePoint[®], and SQL Server[®] are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.

