Lepide

USE CASE GUIDE

HOW TO MONITOR NON-OWNER MAILBOX ACCESS

Table of Contents

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

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 Configure Mailbox Access Auditing Guide.

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**

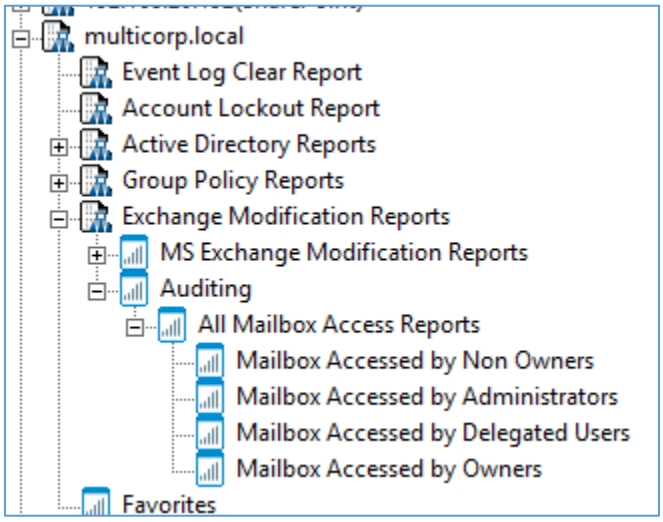

Figure 1: Exchange Server Folder Structure

For **Exchange Online:**

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

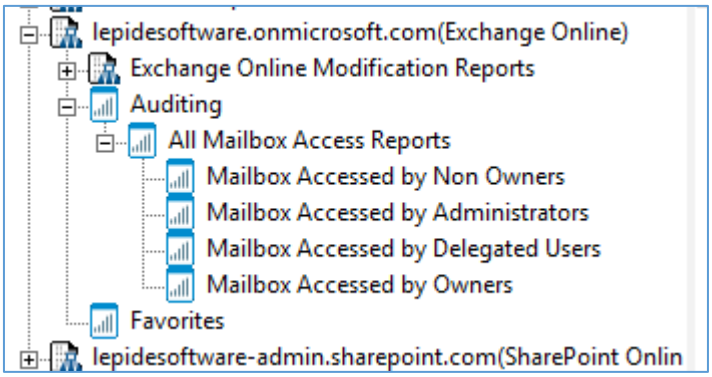

Figure 2: Exchange Online File Structure

The **Mailbox Accessed by Non Owners** screen is displayed:

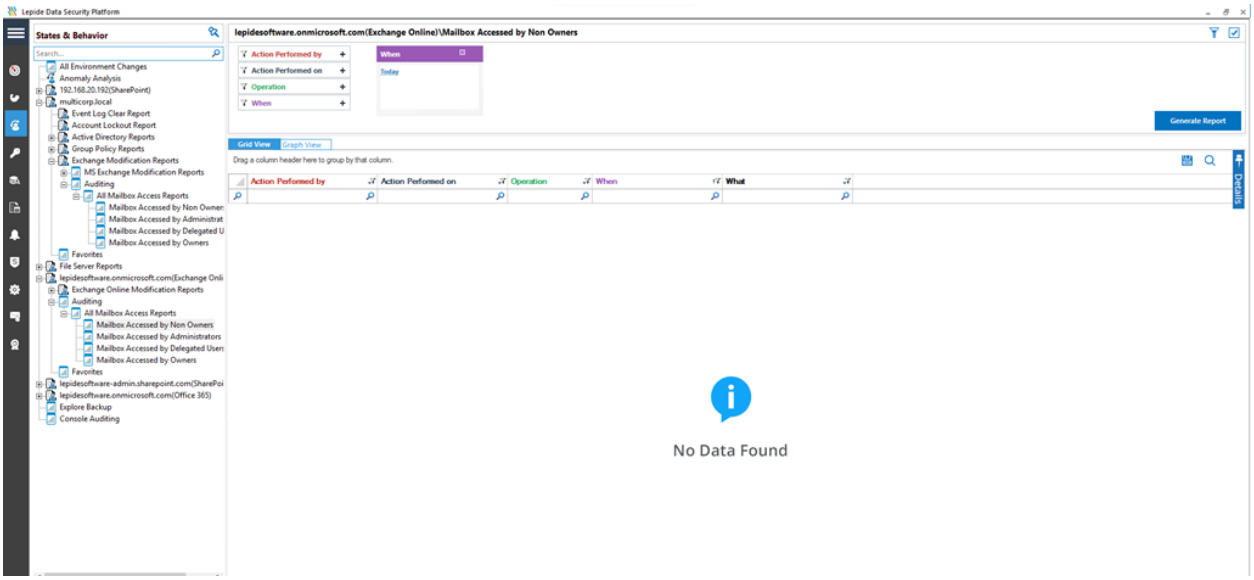

Figure 3: Mailbox Accessed by Non Owners Report

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:

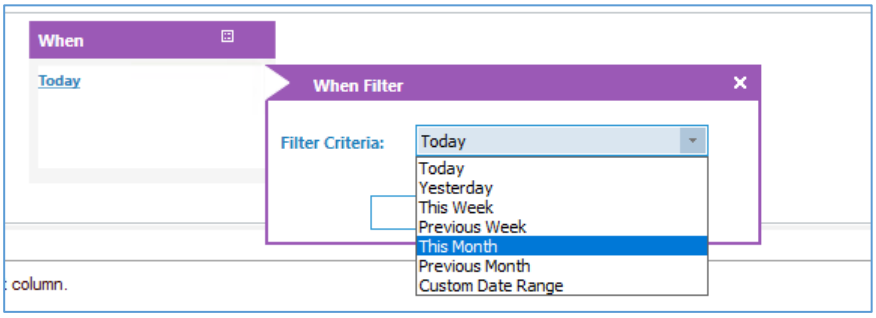

Figure 4: When Filter

- 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:

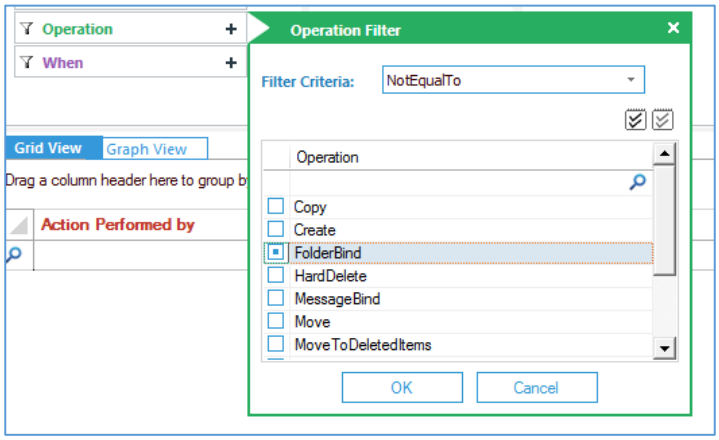

Figure 5: Operation Filter

- 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**

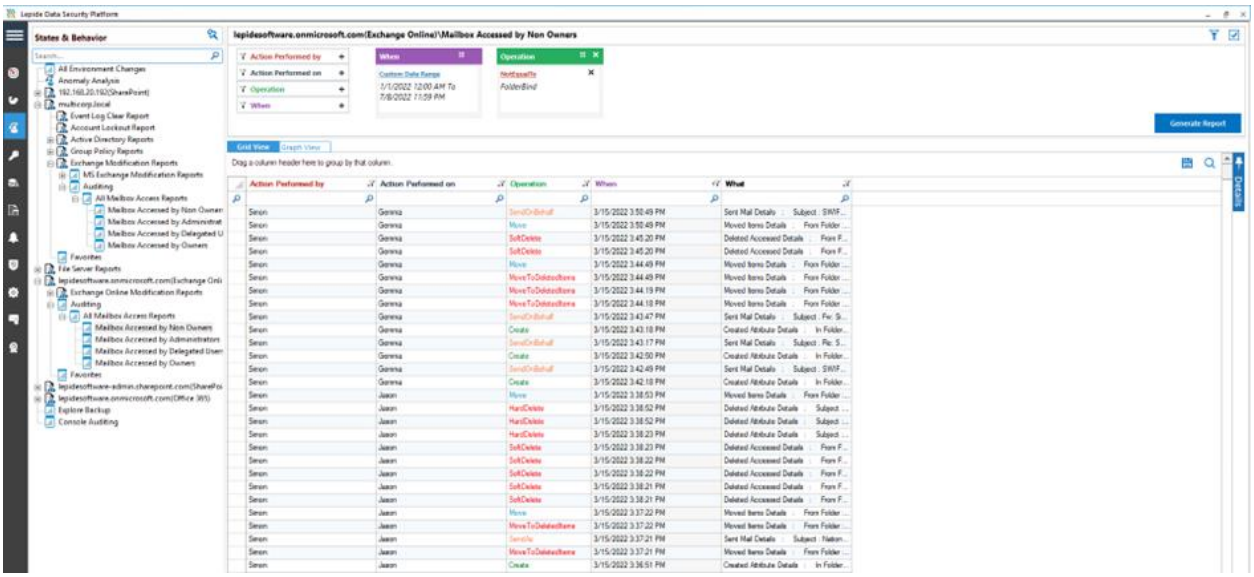

Figure 6: The Generated Report

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:

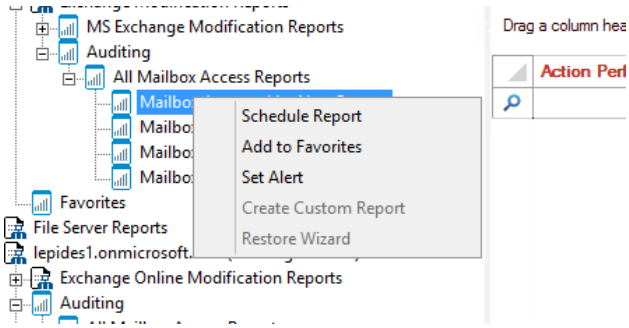

Figure 7: Report Menu

- Choose **Set Alert**

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

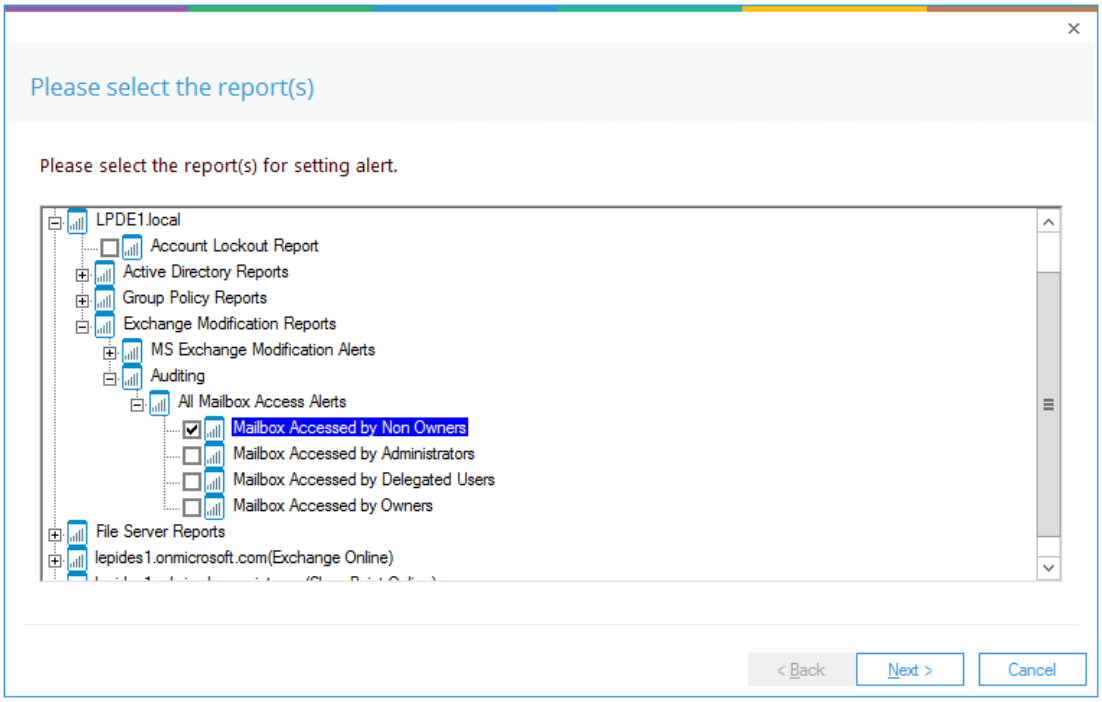

Figure 8: Select Report(s)

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:

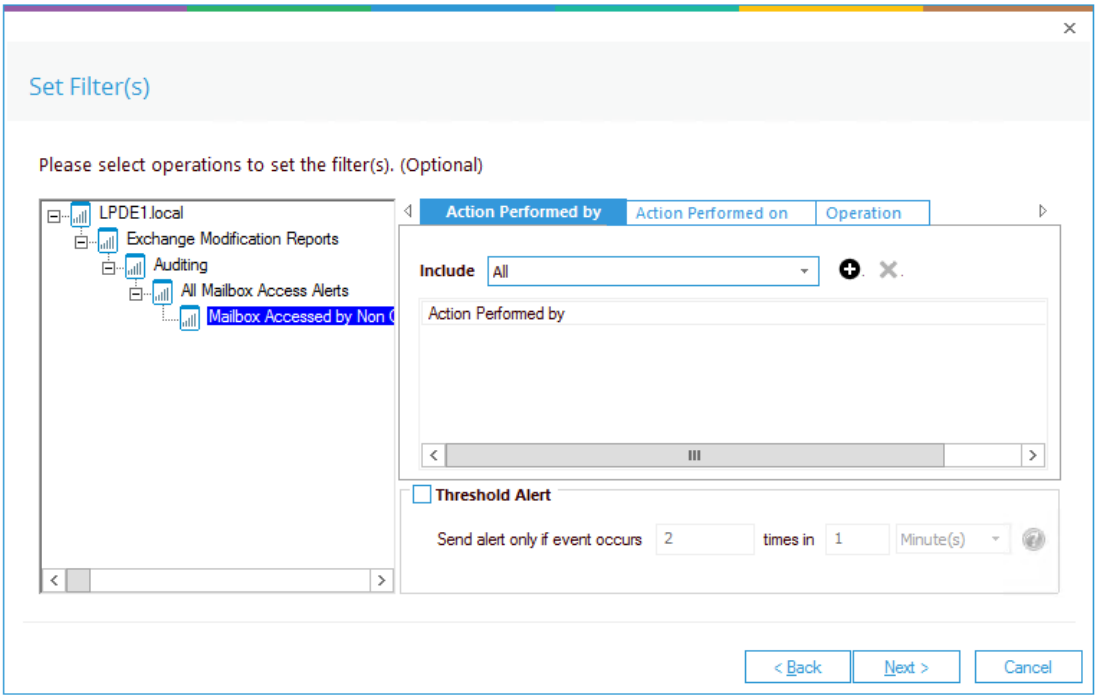

Figure 9: Set Filter(s)

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:

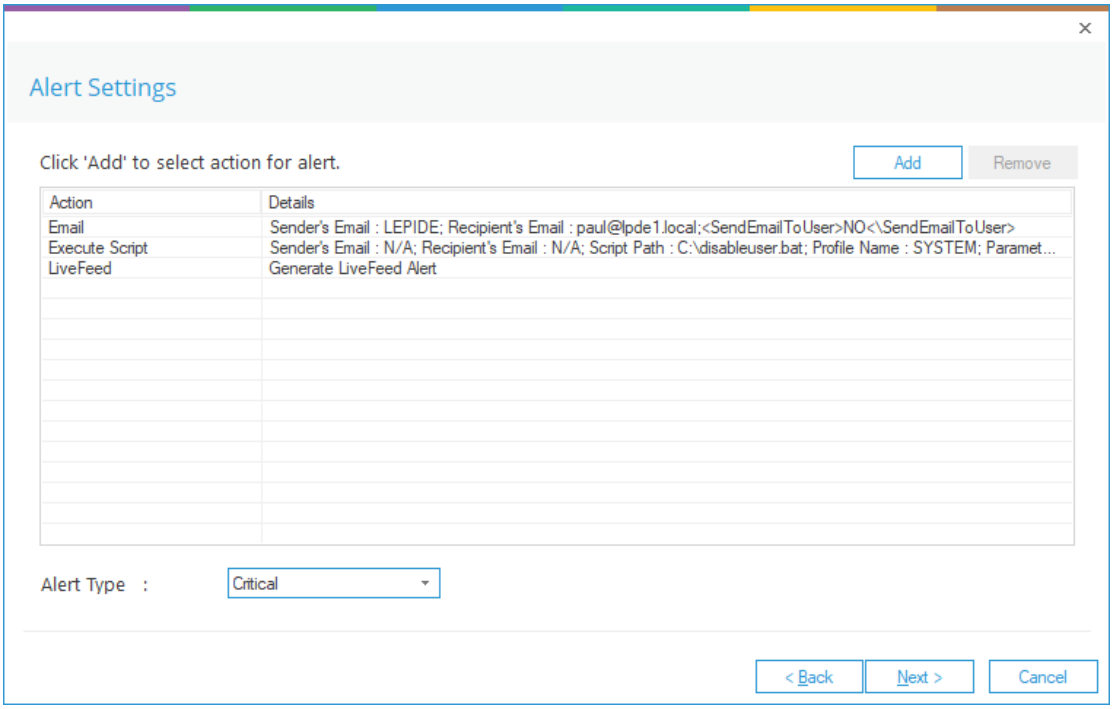

Figure 10: Alert Settings

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:

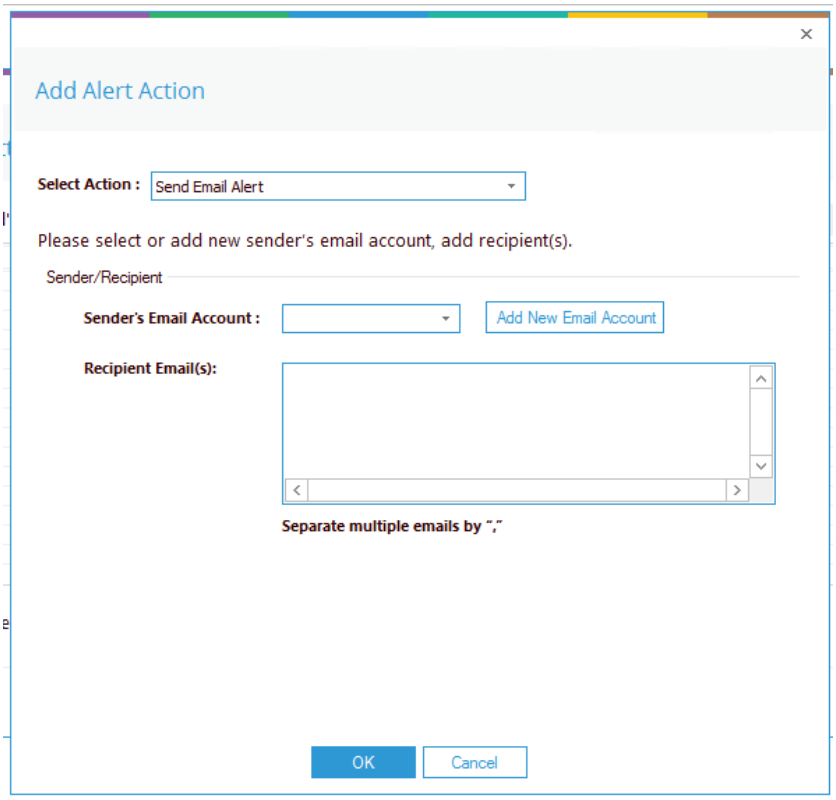

Figure 11: Add Alert Action

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

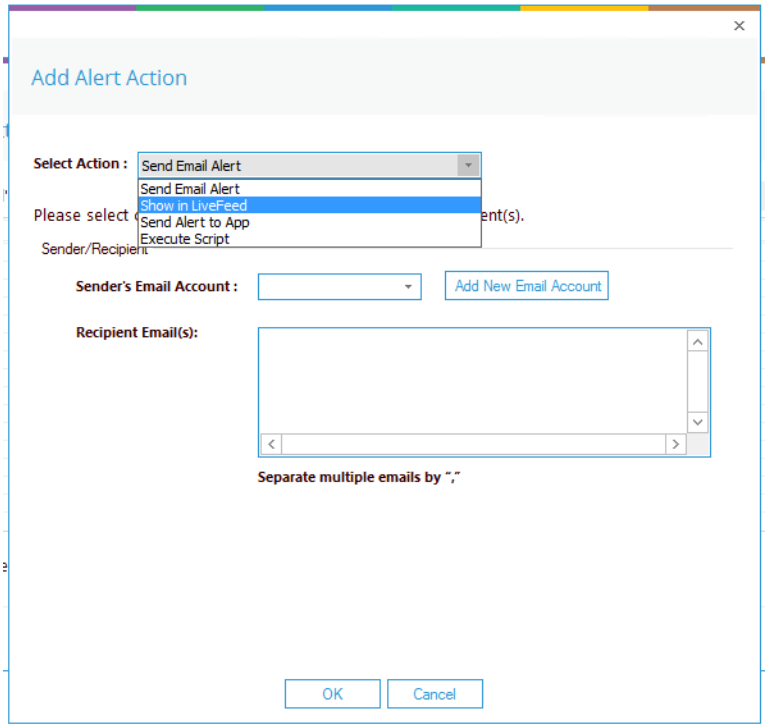

Figure 12: Add Alert Action Options

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

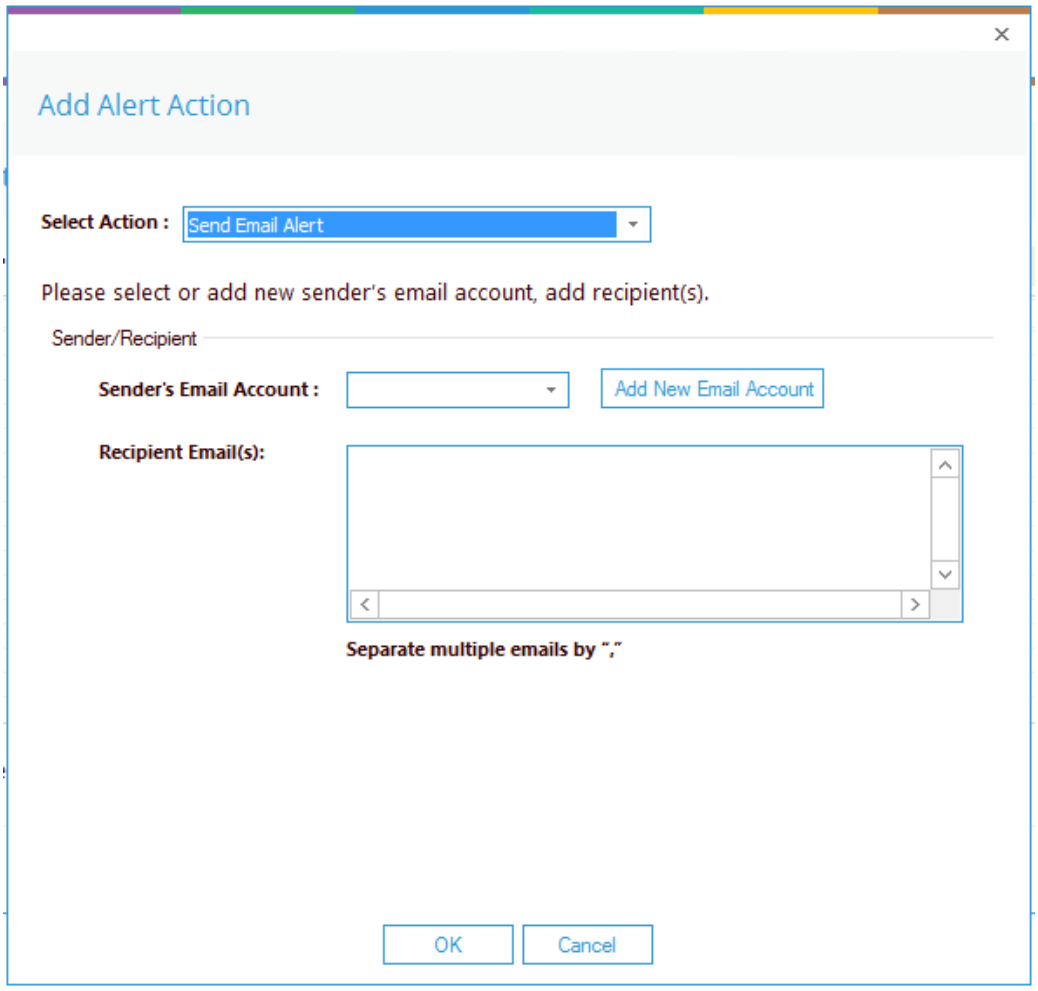

Figure 13: Add Alert Action – Send Email Alert

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. Click **Add New Email Account** to 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

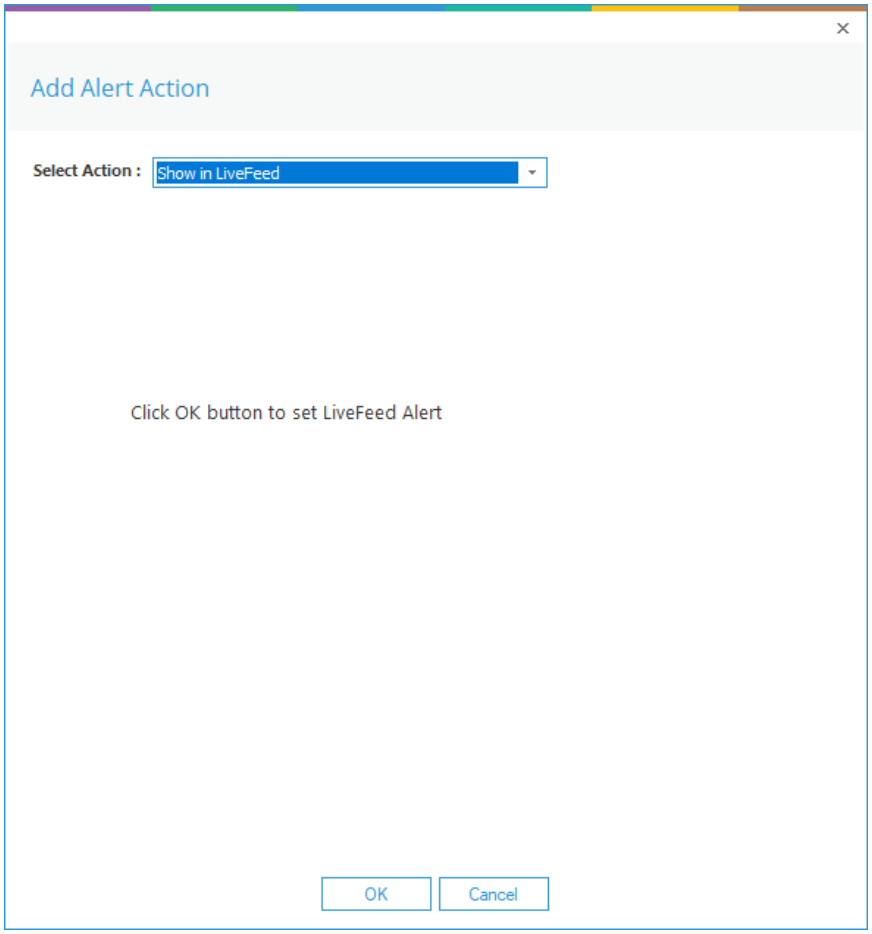

Figure 14: Add Alert Action – Show in LiveFeed

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

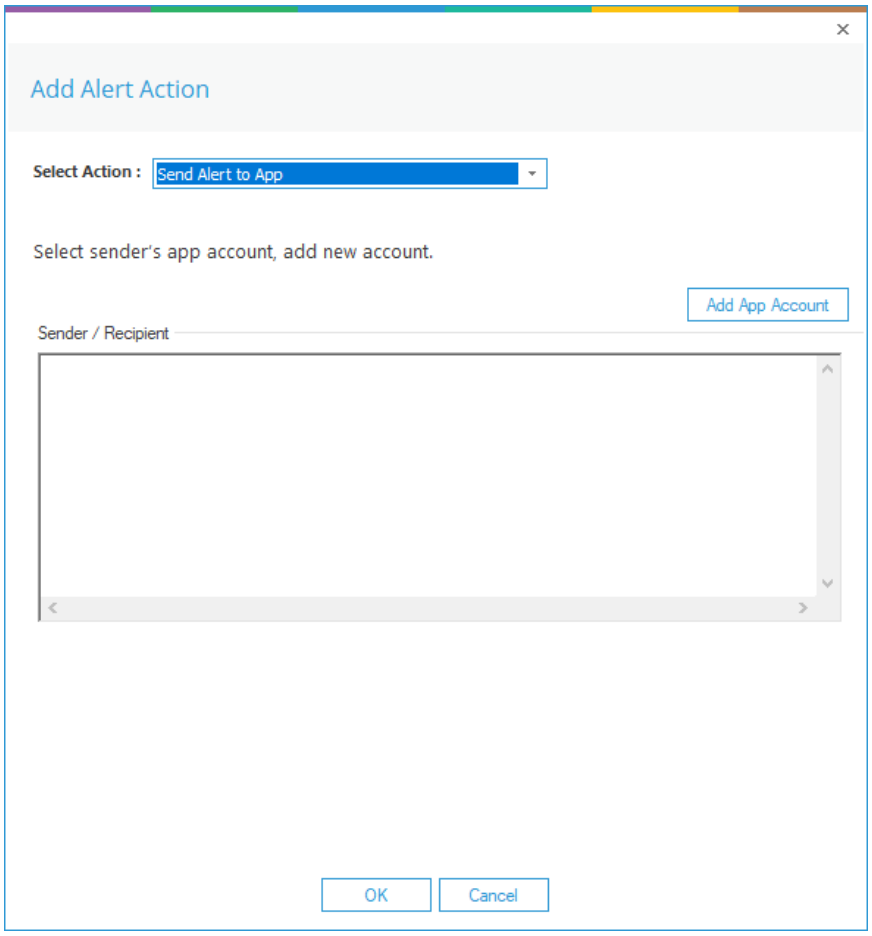

Figure 15: Add Alert Action – Send Alert to App

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:

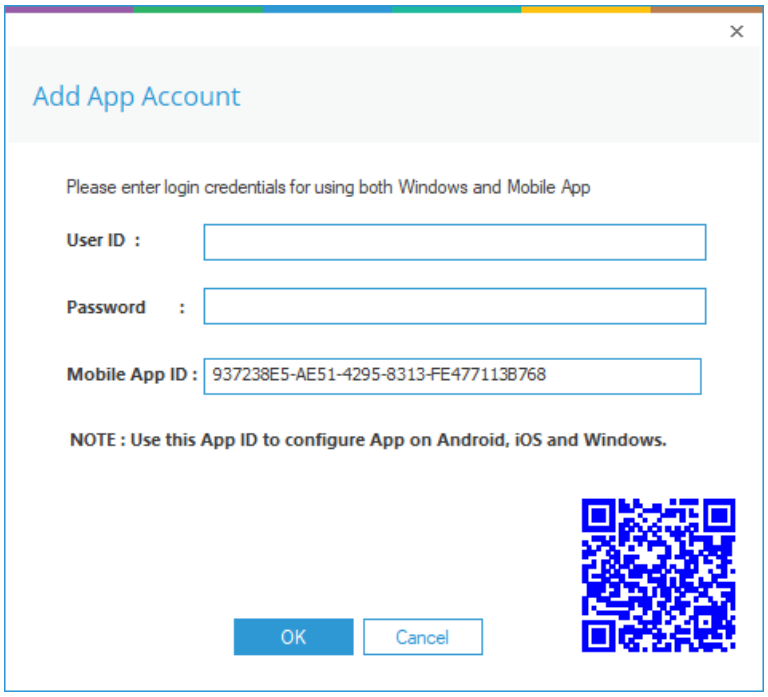

Figure 16: Add App Account

- 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

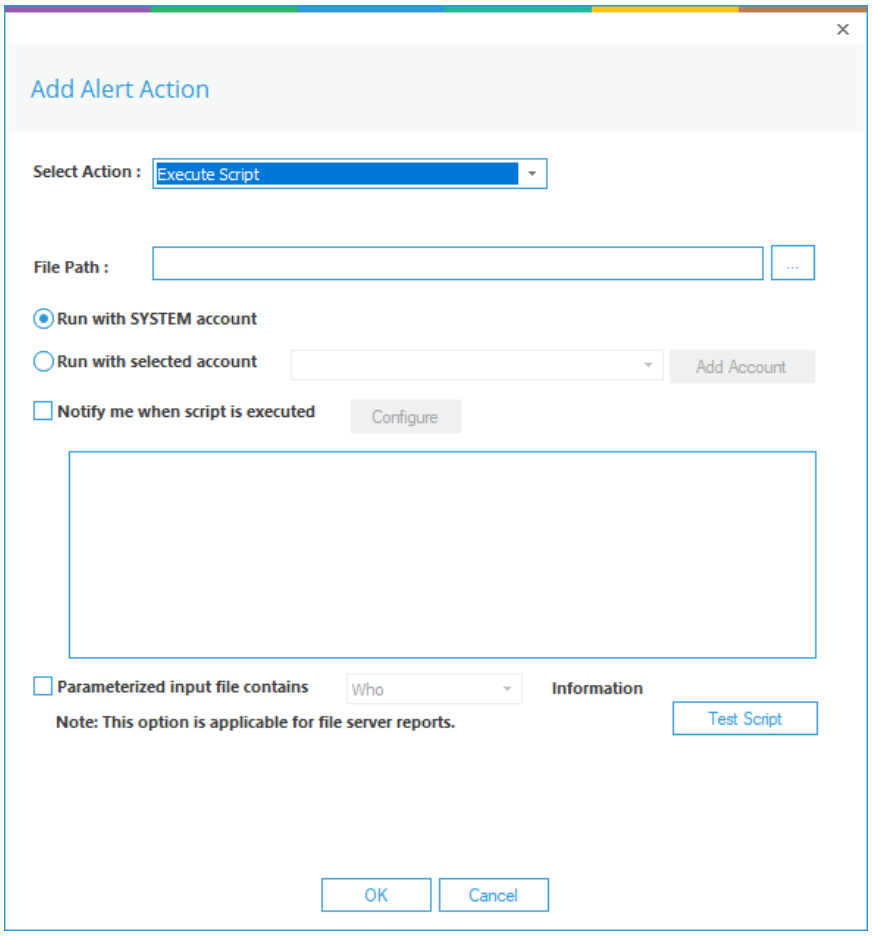

Figure 17: Add Alert Action – Execute Script

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:

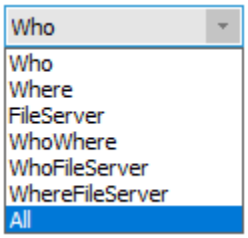

Figure 18: List of Variables

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

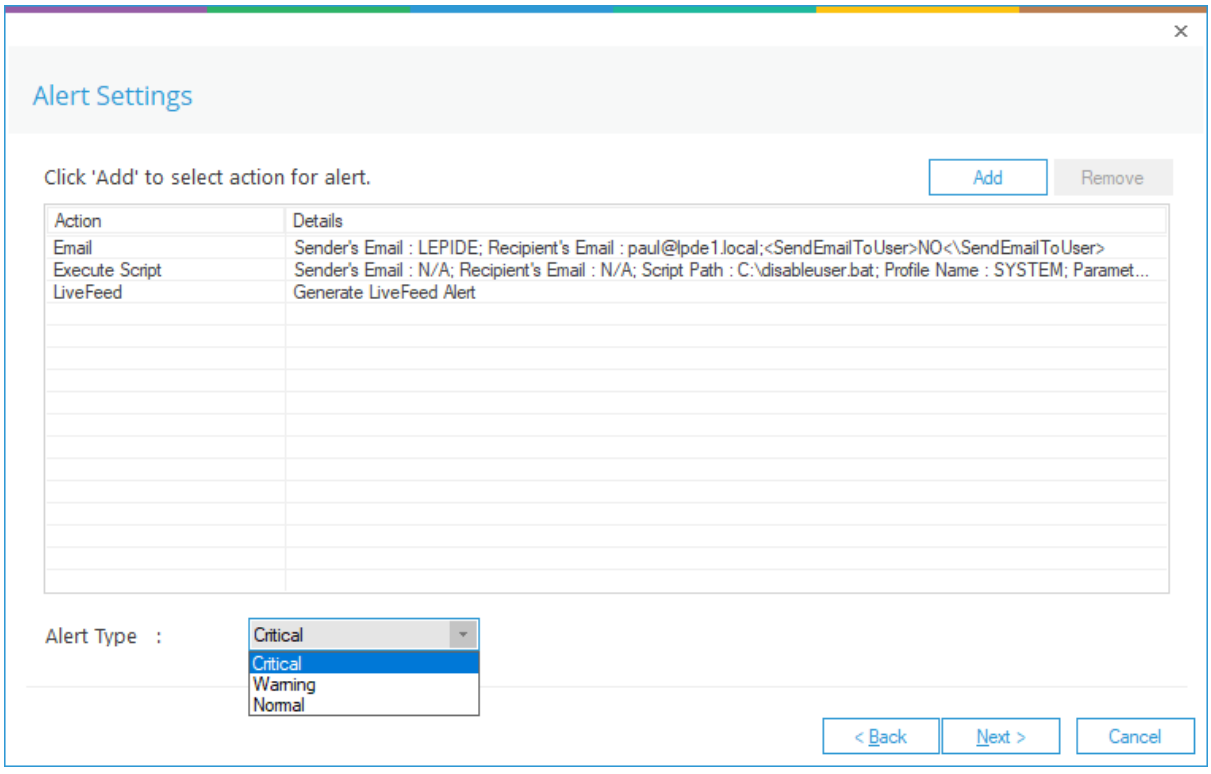

Figure 19: Alert Settings - Alert Type Options

- 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 https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

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

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.