Lepide

USE CASE GUIDE

HOW TO REPORT ON ADMINISTRATIVE GROUP CHANGES

Table of Contents

1. Introduction

Users who have administrative privileges are the most important users within your organization, but they also represent the biggest risk to your data security.

Administrative rights are essential to the efficient running of any IT system as they enable trusted users to perform essential tasks like installing software, adding new accounts, creating passwords and the many other system modifications needed to do their job.

The flip side of this, however, is that admin rights provide the user with the 'keys to the kingdom' and therefore present a huge risk to the security of an organization's data. An attacker who infiltrates a business with access to these rights could do significant harm.

For this reason, particularly in today's world of ever-increasing cyber risk, it is imperative to limit the number of user accounts with administrative privileges to the bare minimum and to have visibility over any changes to administrative groups.

2. Principle of Least Privilege (PoLP)

The Principle of Least Privilege (PoLP) is an information security concept in which a user is given the minimum levels of access needed to perform their job functions. Applying this principle is a highly effective way to greatly reduce the chance of an attack within an organization.

Once the Principle of Least Privilege has been followed within an organization, it is essential to have visibility over any subsequent changes made to these administrative user groups. The adding or removal of admin users needs to be monitored so that the number of users with admin privileges stays at the bare minimum. In this way, companies can remain compliant and reduce the chance of a security breach.

To be able to do this, however, it is essential for organizations to have visibility over these changes. But as organizations grow, and Active Directory structures evolve, being able to keep track of what modifications are happening within the admin user group can become a complex and time-consuming task.

3. The Admin Group Modifications Report

The Lepide Data Security Platform overcomes this complexity and provides visibility in a clear and easy to understand way. By running the Admin Group Modifications Report you can quickly identify all changes within the admin group.

The report can be run immediately and/or scheduled to run on a daily, weekly, or monthly basis therefore providing up-to-date visibility to mitigate the risk of privilege abuse.

Here is an example of the Admin Group Modifications Report:

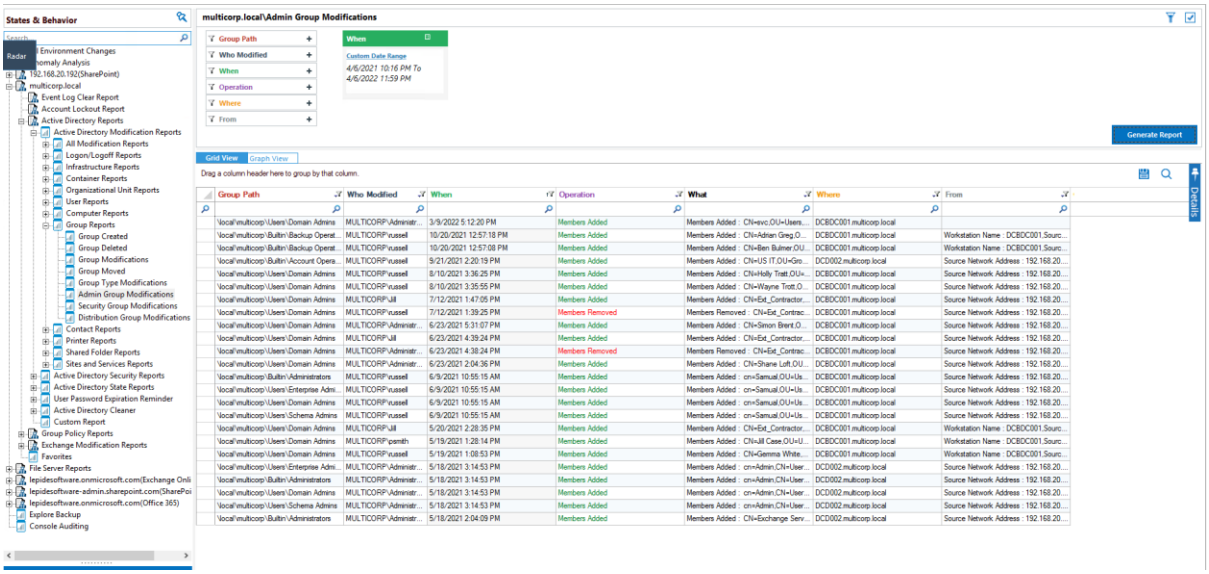

Figure 1: Admin Group Modifications Report Example

The report shows in the Operations column where members of the admin group have been added or removed. Members added are shown in green and members removed shown in red.

3.1. Prerequisites

Before reporting and alerting on admin group modifications, you will need to have added and configured Active Directory to enable auditing.

Once this has been configured, you will be able to see all admin group modification events as the Lepide Data Security Platform provides alerting and reporting in real time.

3.2. How to Run the Admin Group Modifications Report

To view the Admin Group Modifications Report:

- Click the Use & Entity Behavior Analytics  icon:
- Expand **Active Directory Reports** (from the tree structure to the left side of the screen)
- Expand **Group Reports**
- Click on **Admin Group Modifications** to display the **Admin Group Modifications Report:**

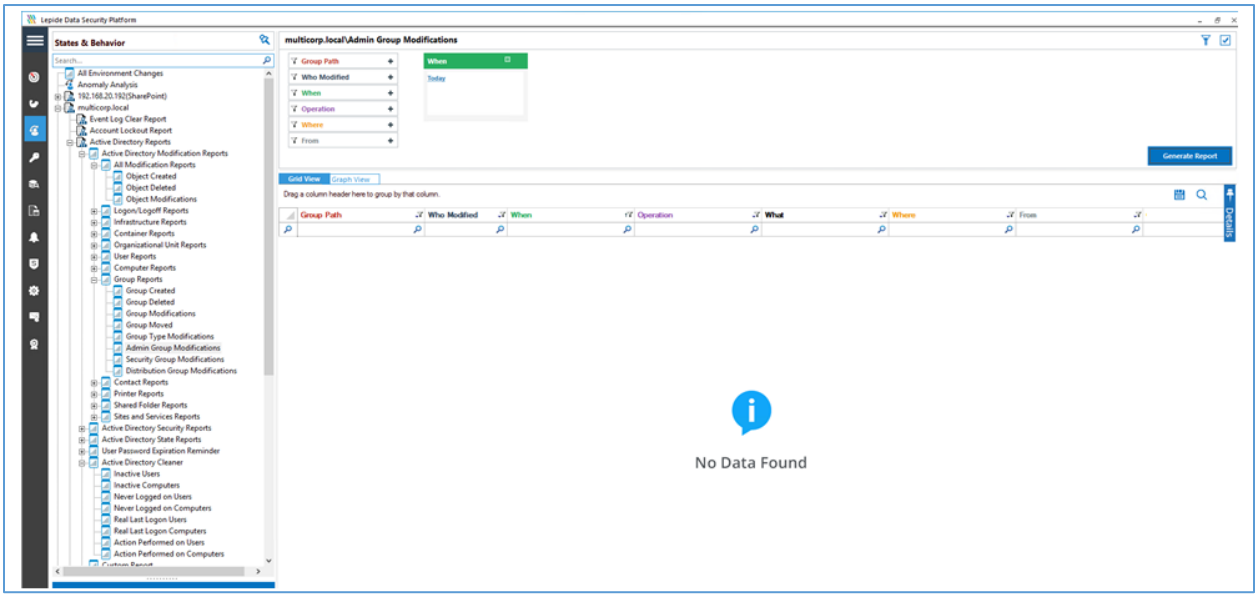

Figure 2: Admin Group Modifications Report

- Click the **When** filter box to add a date range
- Click **Generate** to generate the report

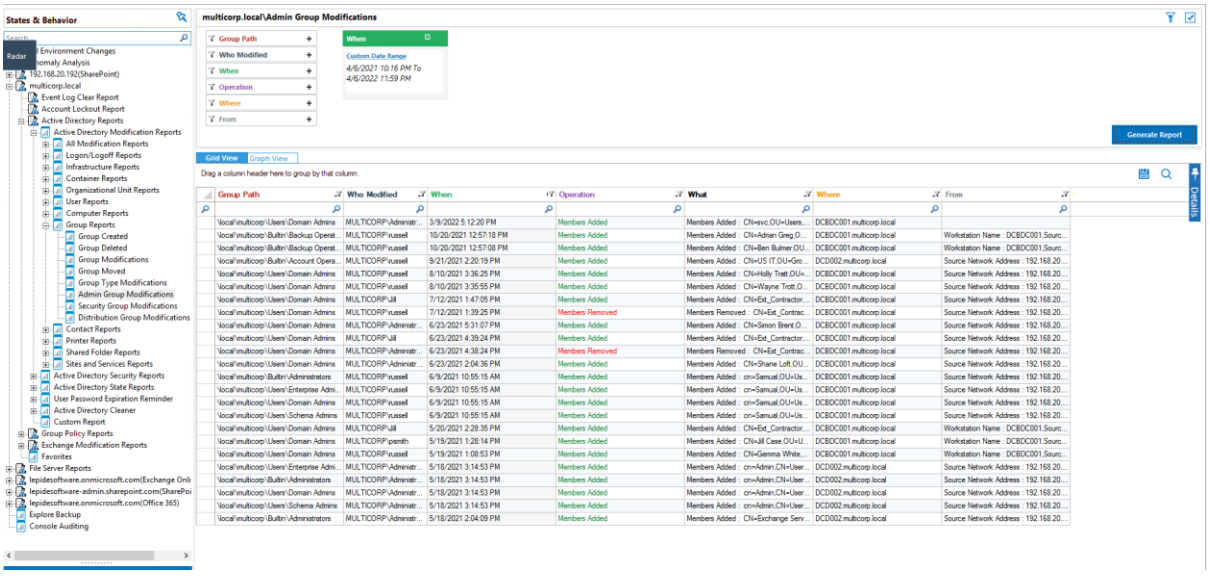

Figure 3: Generated Admin Group Modifications Report

The report displays the following:

- Object Path: The path for the admin group type. For example, Administrator, Domain Admin etc
- Who Modified: The username of the person who modified the group
- When: When the modification occurred
- Operation: What the modification was
- What: More details on exactly what was modified
- Where: The domain controller where the modification was made
- From: The location where the modification was made

4. Creating an Alert on the Admin Group Modifications Report

If you want to be notified as soon as a change has been made, you can set up an automated alert on the Admin Group Modifications Report.

To set up an alert:

- Click the **User Entity & Analytics** icon  to display the **States & Behavior** window

  A list of reports is displayed in a tree structure on the left-hand side of the screen
- Expand the Active Directory node
- Right click on the **Admin Group Modifications Report** to display the context menu

The context menu is displayed:

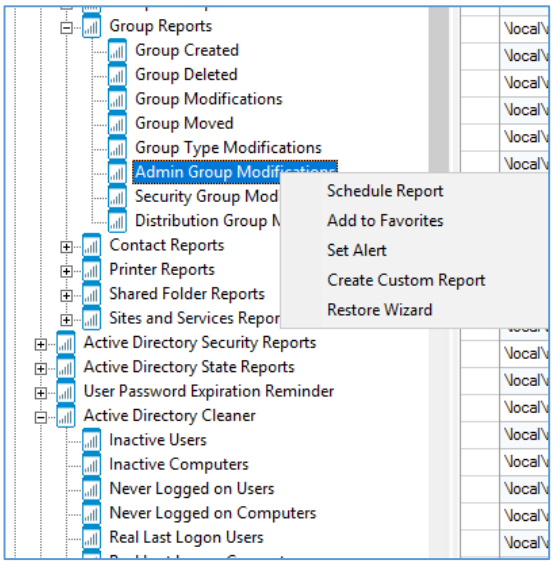

Figure 4: Context Menu

- Choose **Set Alert**

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

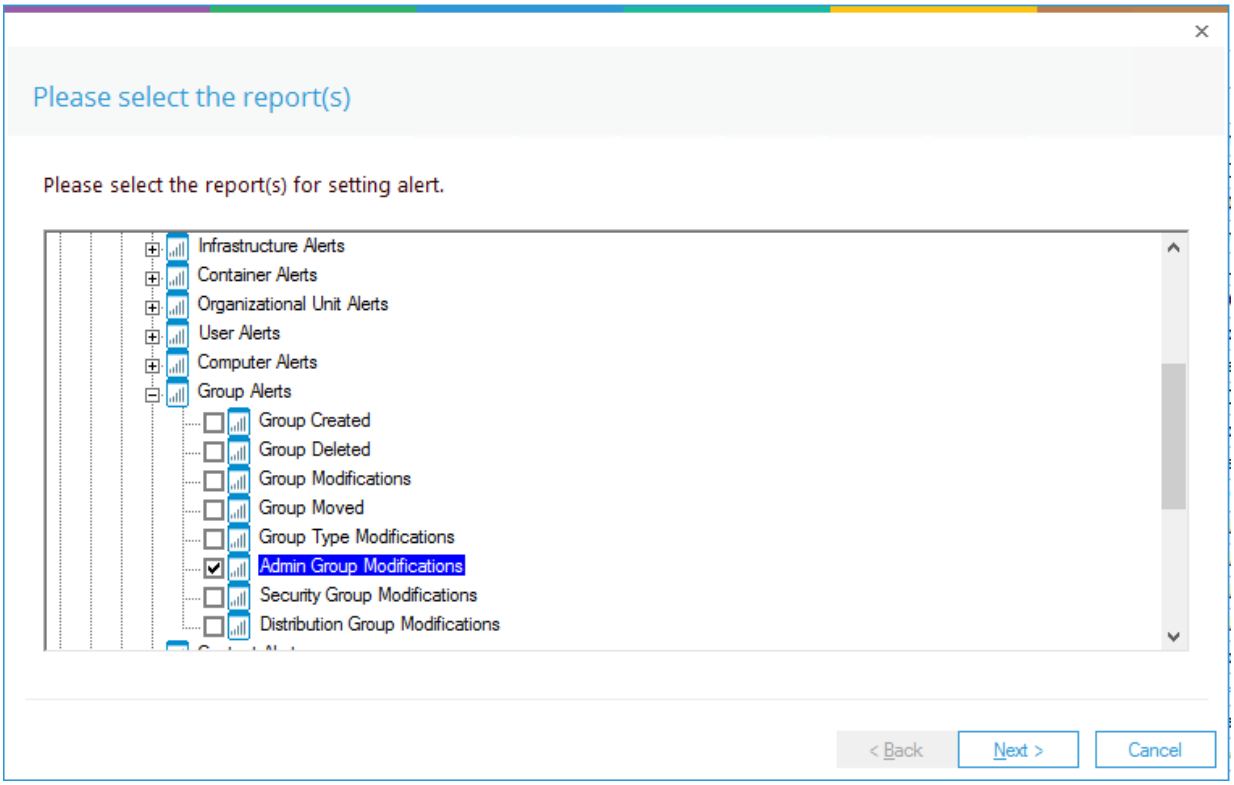

Figure 5: Select Report(s)

Ensure that the report on which you want to set an alert is checked. In this case, it is the Admin Group Modifications Report.

- Click **Next**

The Set Filter(s) dialog box is displayed:

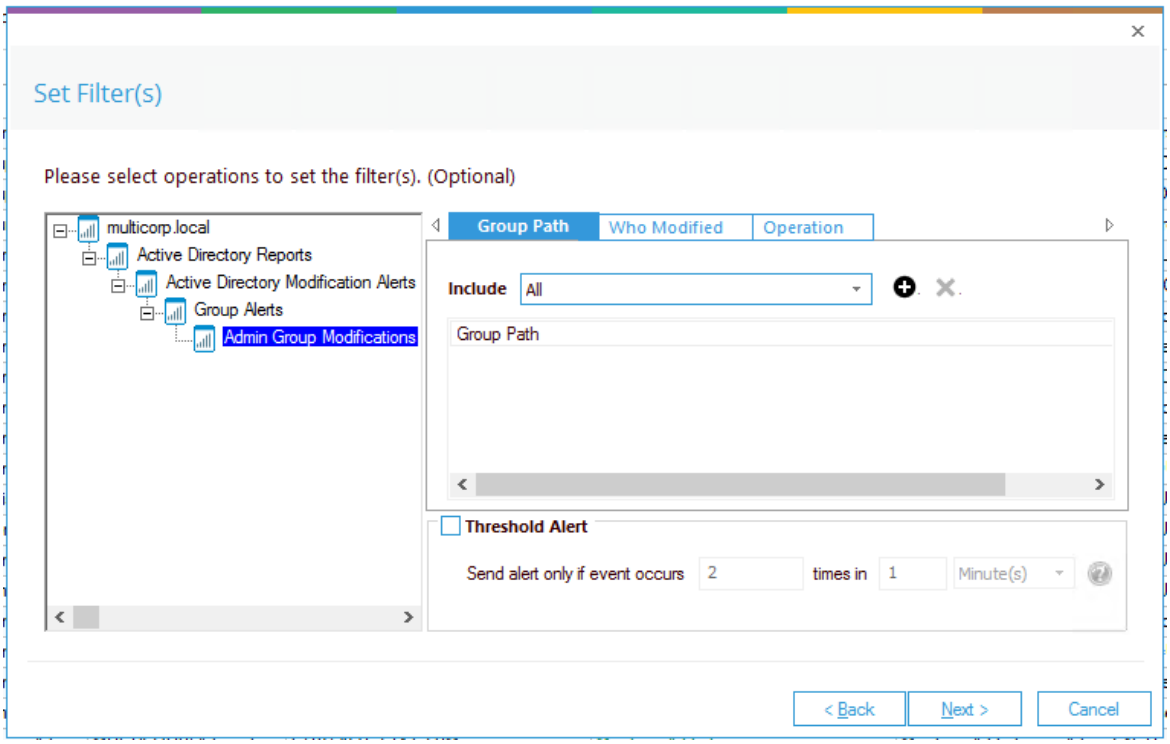

Figure 6: Set Filter(s)

On the left of the dialog box, you can see the report you are working on which in this case is **Admin Group Modifications Report**.

There are options to change the settings for **Group Path, Who Modified** and **Operation** using the tabs at the top of this dialog box. The default setting for both 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: Enter the number of times the event occurs, the time value and time-period here

- Click **Next**

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

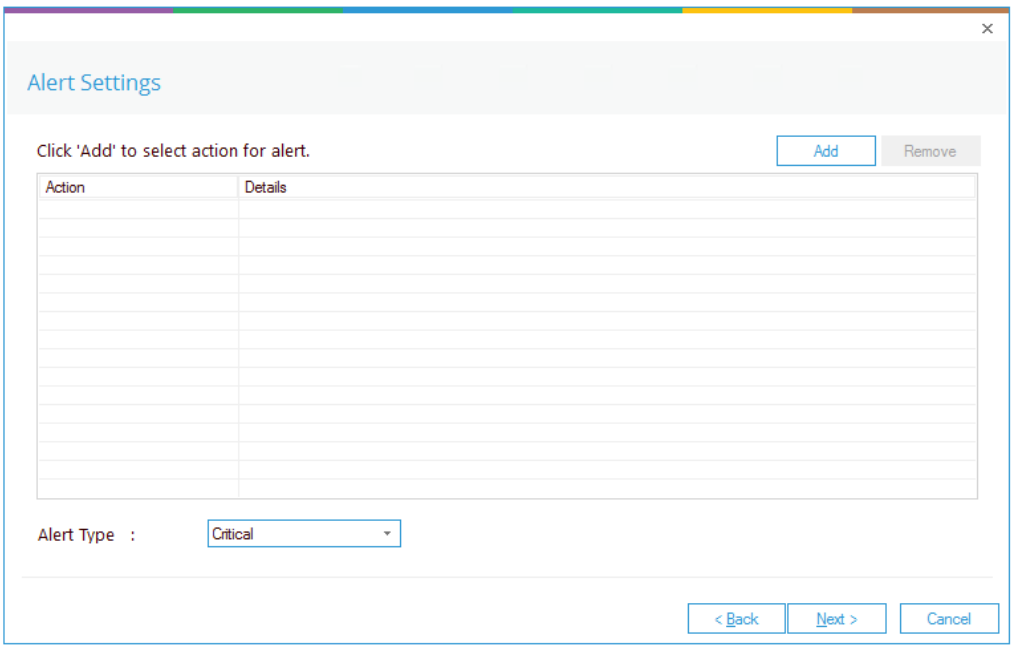

Figure 7: Alert Settings

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 will be displayed:

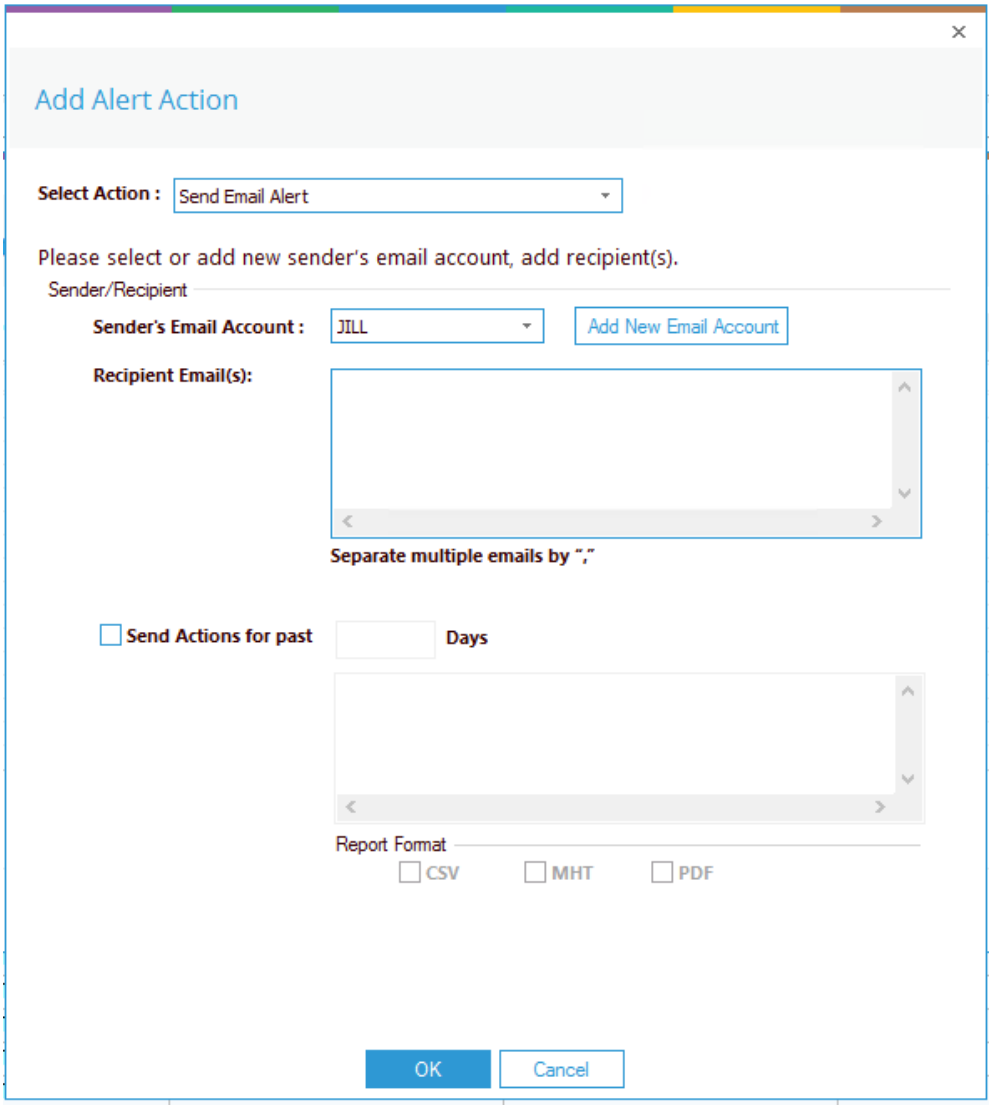

Figure 8: Add Alert Action

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

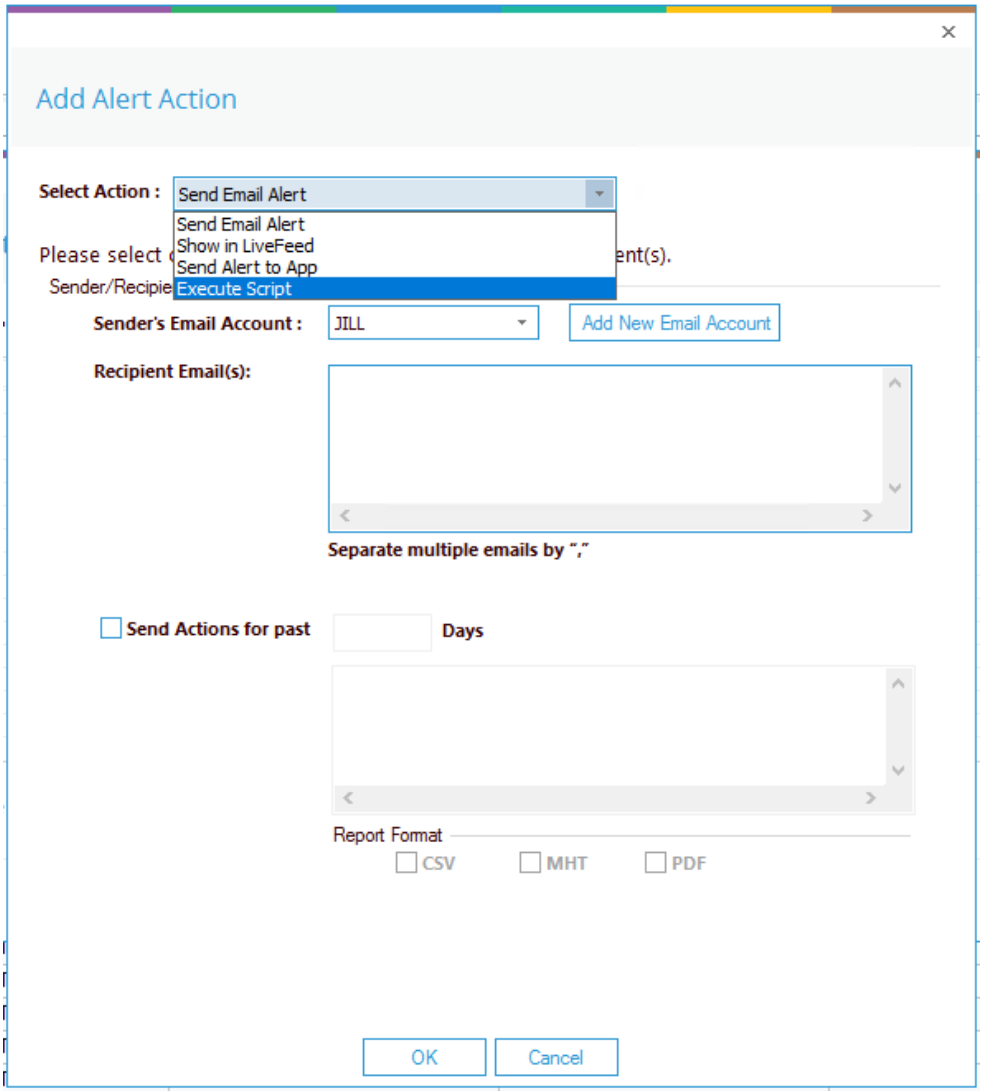

Figure 9: Add Alert Action Options

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

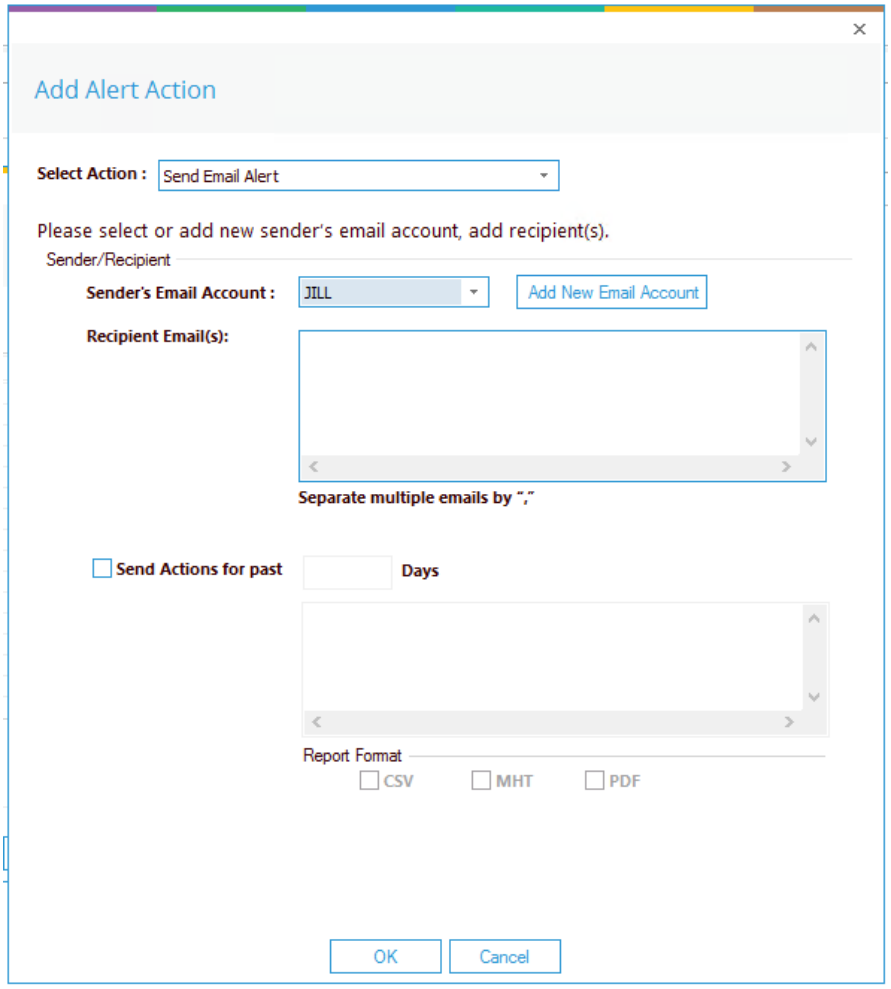

Figure 10: Add Alert Action – Send Email Alert

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 ','

Send Actions for past xx days: This option allows you to see everything that this user has done over the last number of specified days. For example, if an alert is triggered because a user has been added, then you may want to see what else has been happening for that account. Check this box and specify the number of days and an email will be sent with an attachment listing everything that the user has done over the

specified number of days.
The attachment will contain a report and the format(s) can be specified by checking the relevant box. The formats are CSV, MHT and PDF.

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

2. Show in LiveFeed

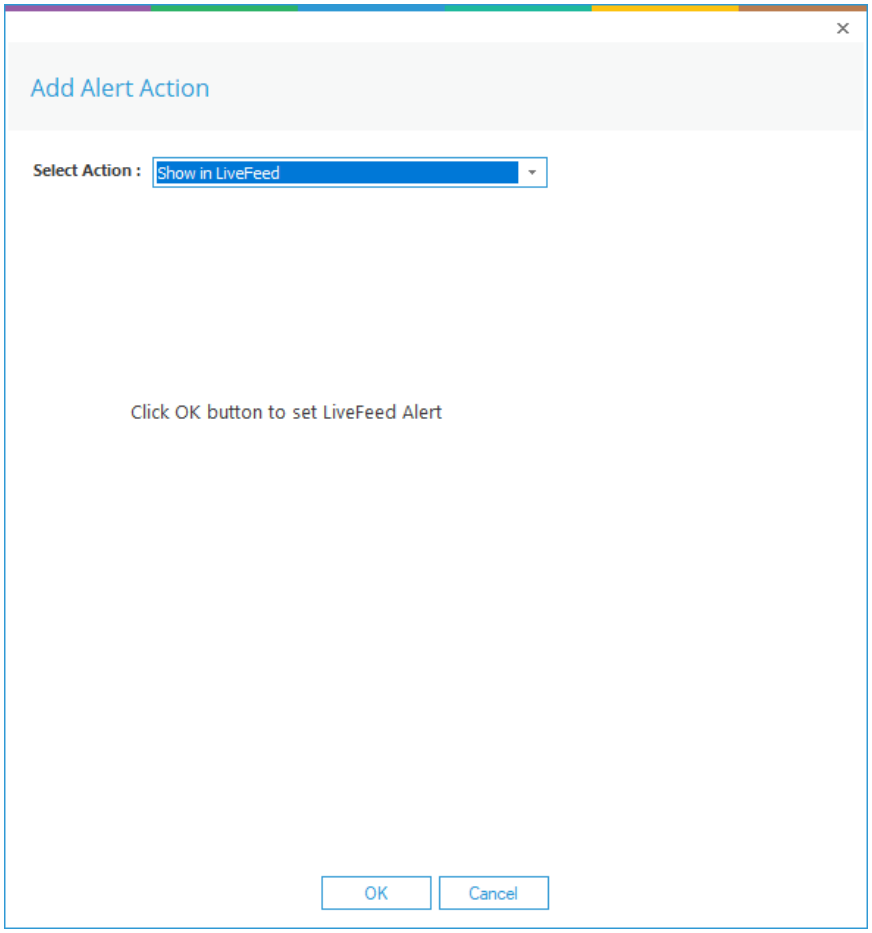

Figure 11: Add Alert Action – Show in LiveFeed

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

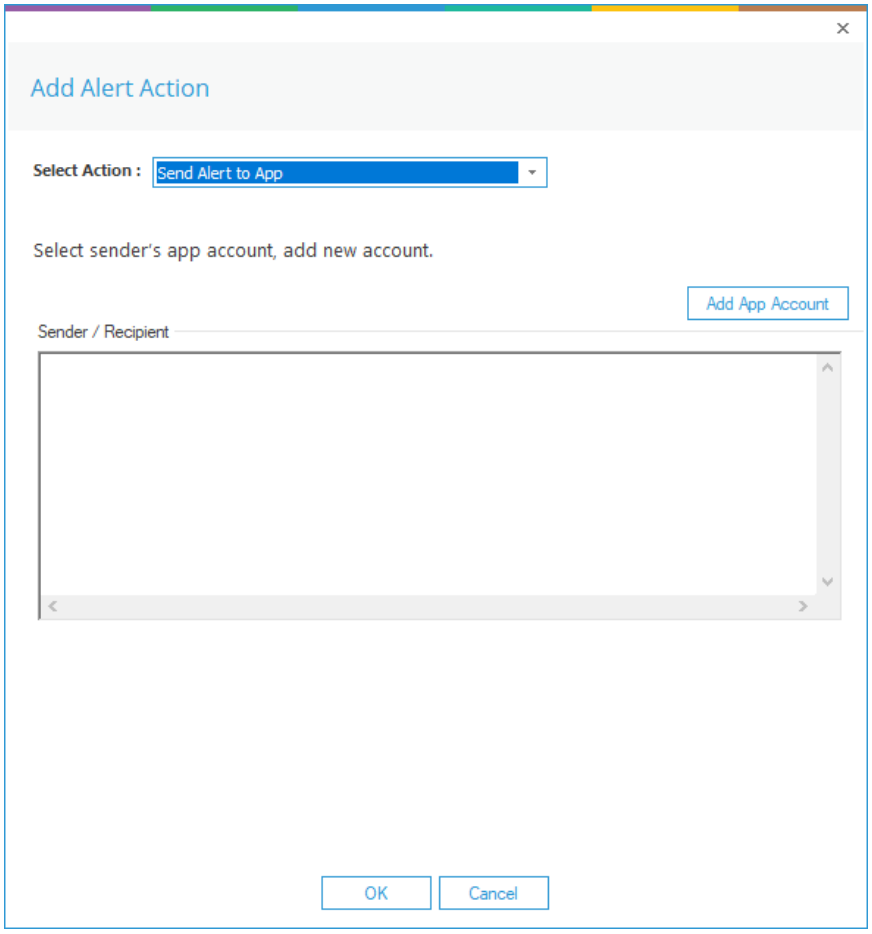

Figure 12: Add Alert Action – Send Alert to App

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:

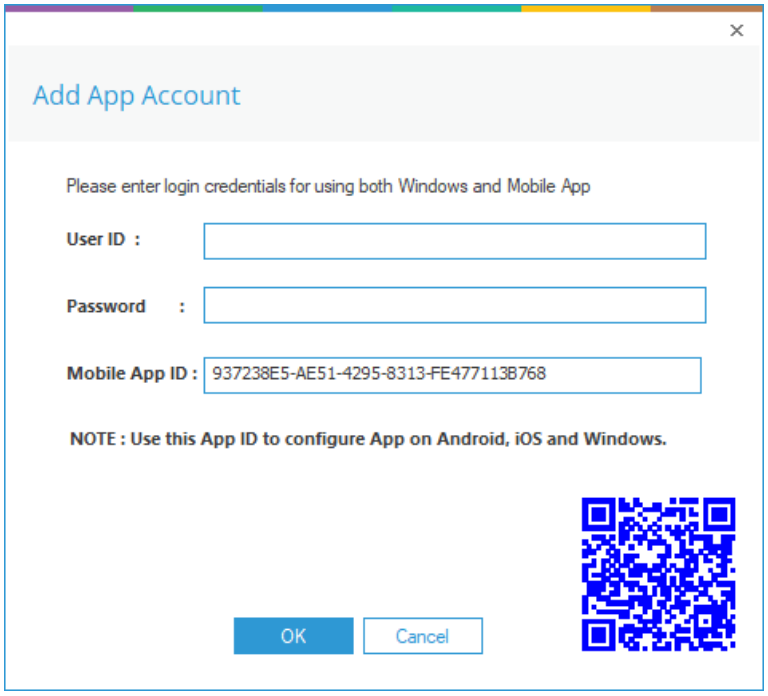

Figure 13: Add App Account

- 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

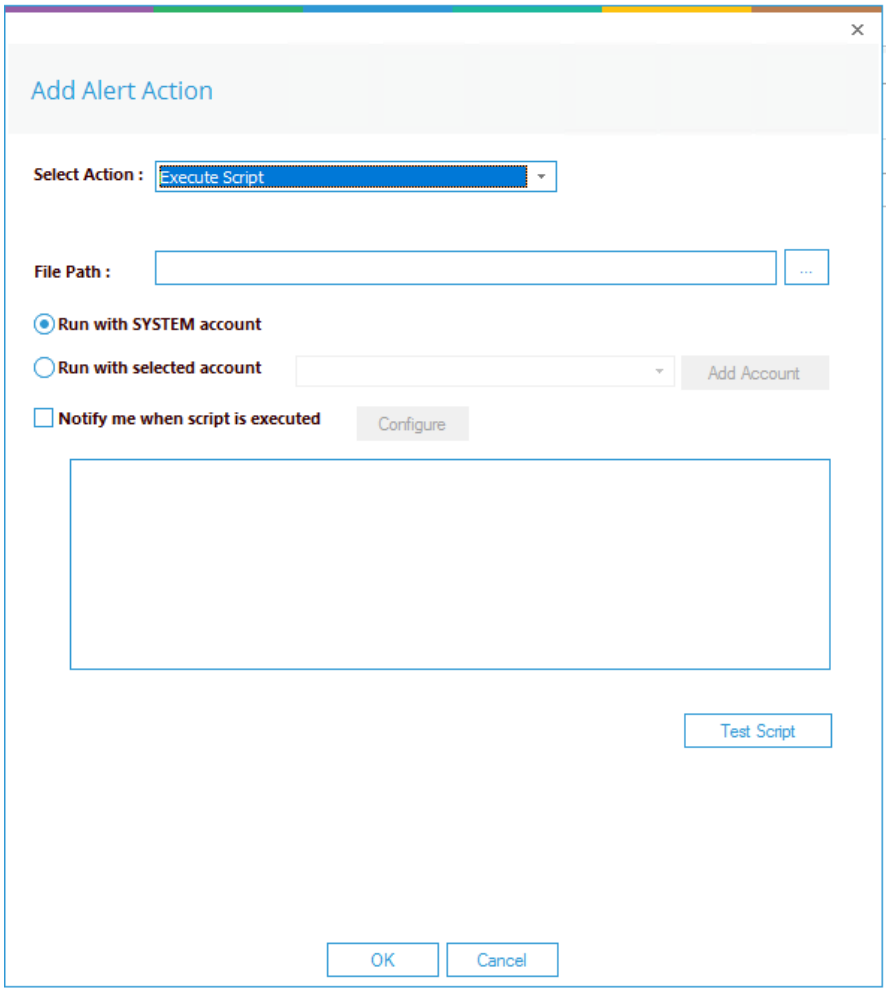

Figure 14: Add Alert Action – Execute Script

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.

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

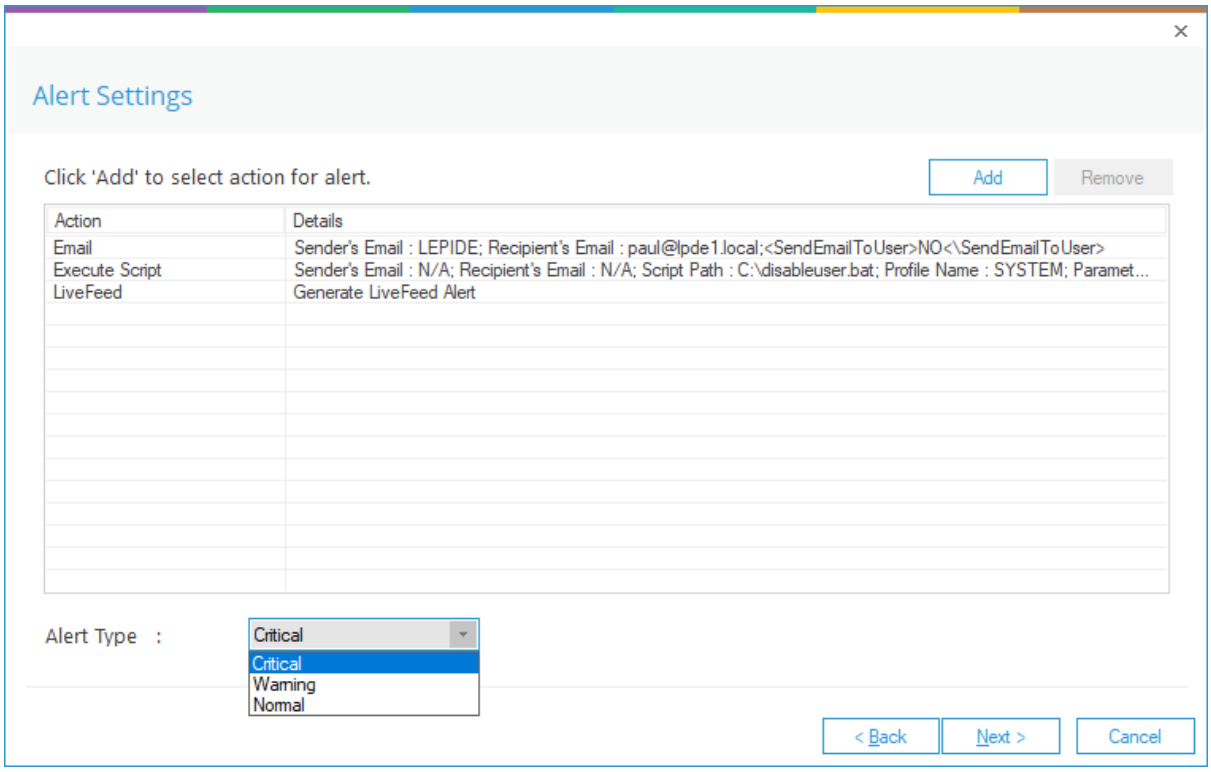

Figure 15: Alert Settings - Alert Type Options

- 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.

5. 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 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/.

6. Trademarks

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.