Lepide

USE CASE GUIDE

HOW TO REPORT ON SECURITY SETTING CHANGES IN GROUP POLICY USING LEPIDE

Table of Contents

1.Introduction

Group Policy Objects are an integral part of Active Directory, as they enable the IT Administrator to centralize the management of computers on a network without having to configure each computer individually. However, problems begin to arise when multiple Administrators can change Group Policy Objects without proper change tracking mechanisms in place. Whether it's inadvertent or deliberate, changes in the Group Policy configuration can impact compliance and create security risks, paving the way for significant damage.

This guide looks at what Group Policy is and how to manage the change process using the Lepide Data Security Platform.

2.What is Group Policy?

Group Policy is primarily a security tool which can be used to apply security settings to users and computers. It provides administrators with a secure and stable platform to establish and manage settings for users and computers. For example, group policy can determine whether a user has rights to install software or to change system settings, or whether a user is authorized to take remote control of other computers in the network. Any decision whatsoever regarding the rights of users can be applied through Group Policy Objects.

However, if these changes are not tracked, the security of the entire network is at significant risk. It is essential to have a process in place to pro-actively track changes to Group Policy Objects so that reports can be generated, and regular notifications received whenever changes in Group Policies occur. Tracking can be achieved with native Group Policy auditing, but this can be a complex and time consuming process.

3.The Lepide Solution

The Lepide Data Security Platform facilitates change tracking and auditing of multiple domains from a centralized location. Using the Security Policy Modified Report, you can see who made the change, when the change was made and where the change occurred and by configuring real time and threshold alerts you can be notified whenever suspicious changes in Group Policy Objects are detected.

The following is an example of the Security Policy Modified Report:

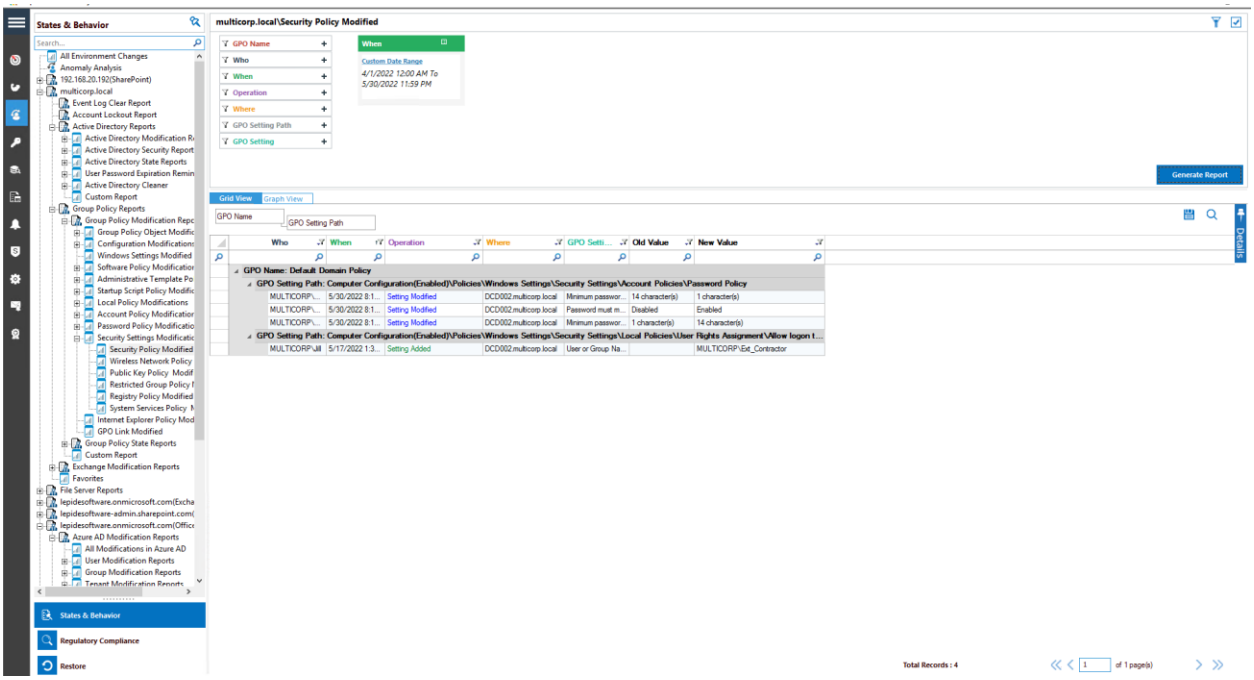

Figure 1: Security Policy Modified Report

The report is grouped by GPO Name and then GPO Setting Path.

The first row of the report, in this example, shows the Operation of Setting Modified, Where the change was made, the minimum password length changed from the Old Value of 14 characters to the New Value of 1 character.

4. The Security Policy Modified Report

The following steps explain how to run the report:

- Click the User & Entity Behavior Analytics icon 

The States & Behavior screen will be displayed:

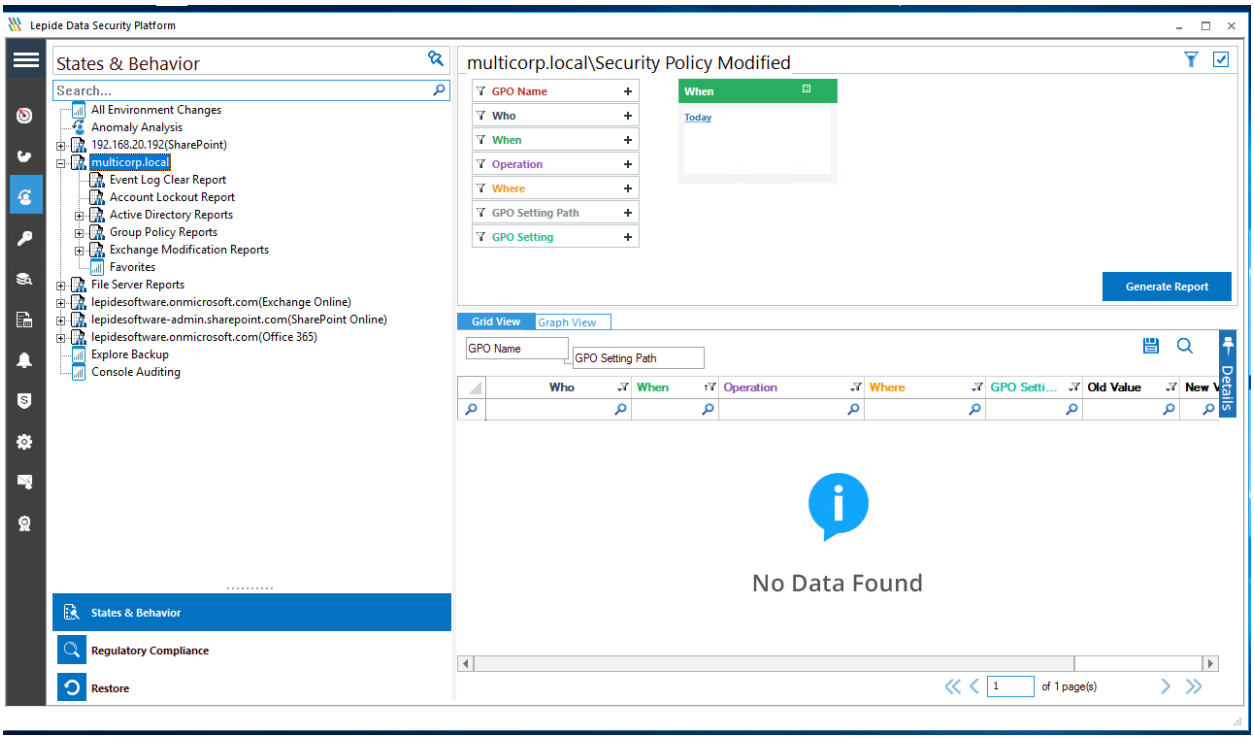

Figure 2: States & Behavior Screen

From the left-hand tree structure:

- Expand **Group Policy Reports**
- Expand **Group Policy Modification Reports**
- Expand **Security Settings Modifications**
- Click on **Security Policy Modified** to display the **Security Policy Modified Report:**

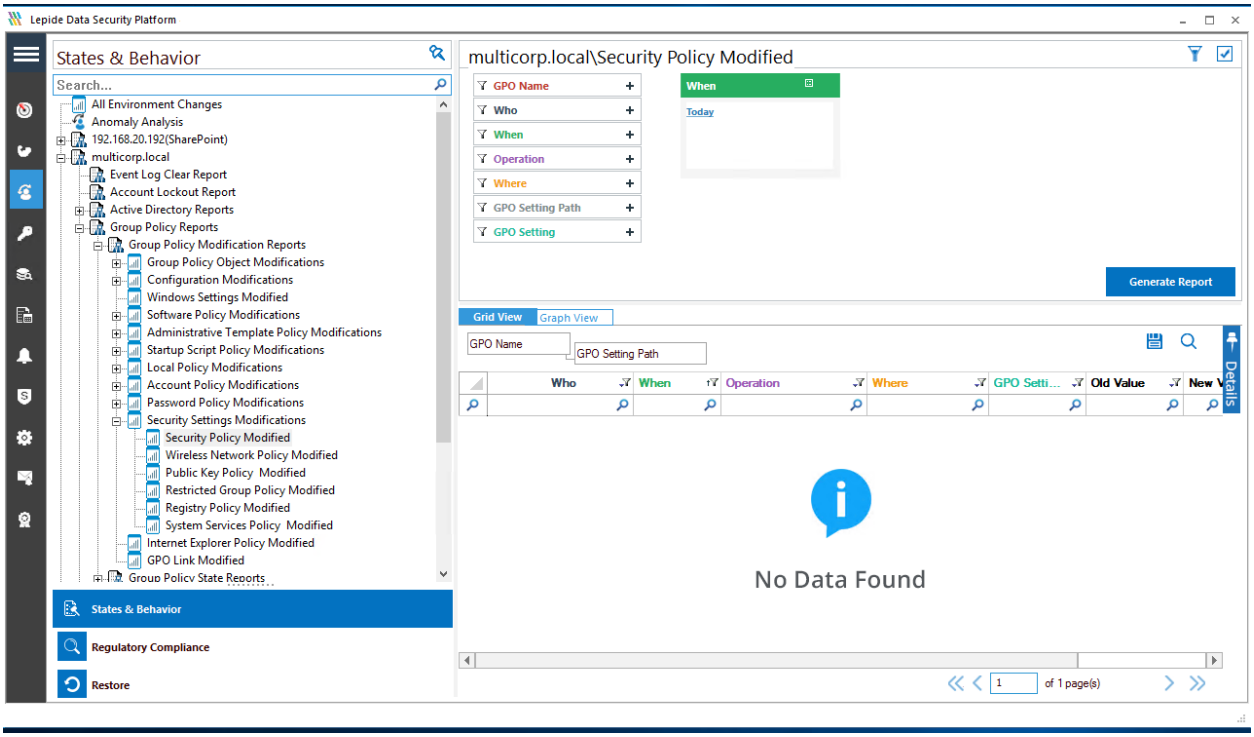

Figure 3: Security Policy Modified Report

4.1. Specify a Date Range

- From the top of the screen, under **When** click **Today** to choose a date range for the report

The following dialog box is displayed:

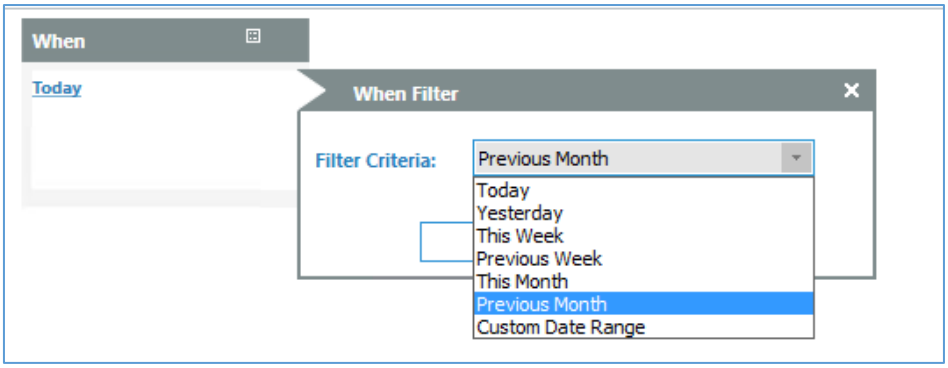

Figure 4: Date Range Filter

- Select a date range from the list
- Click **OK** and you will return to the **Security Policy Modified** screen
- Click **Generate** Report
- The report runs and shows any Group Policy Changes for the time period specified:

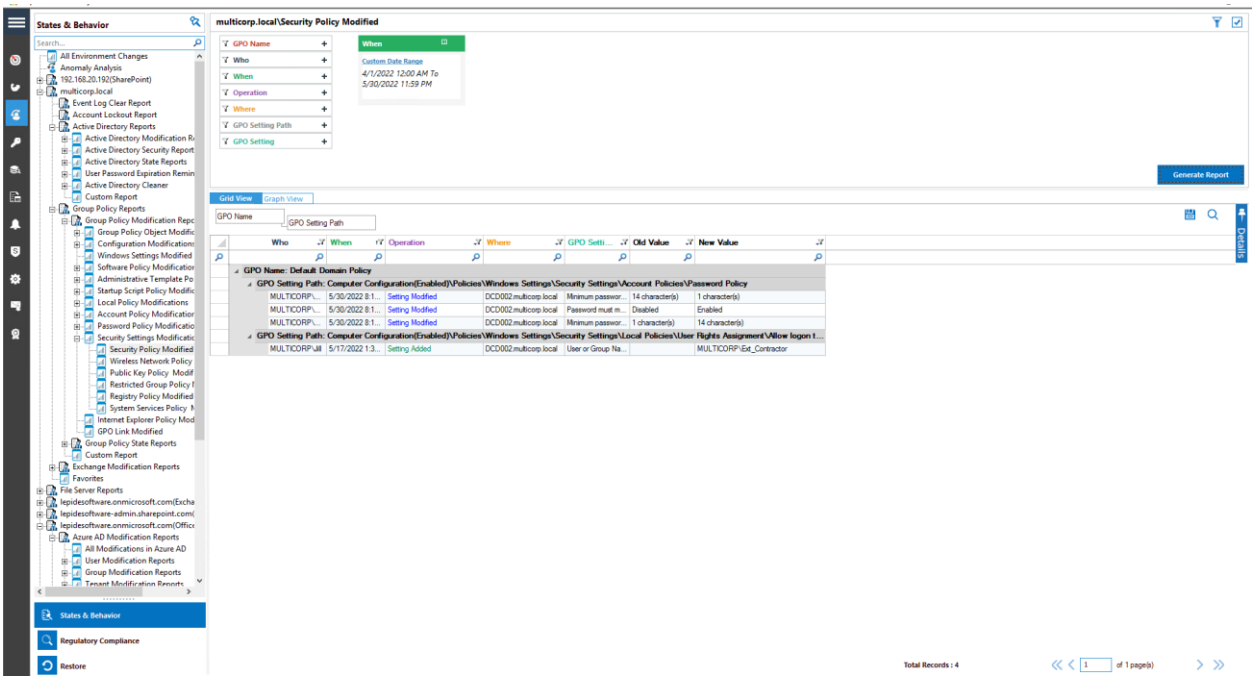

Figure 5: Generated Security Policy Modified Report

5. Creating an Alert

From the States & Behavior screen:

- Right click on **Security Policy Modified** to display the context menu:

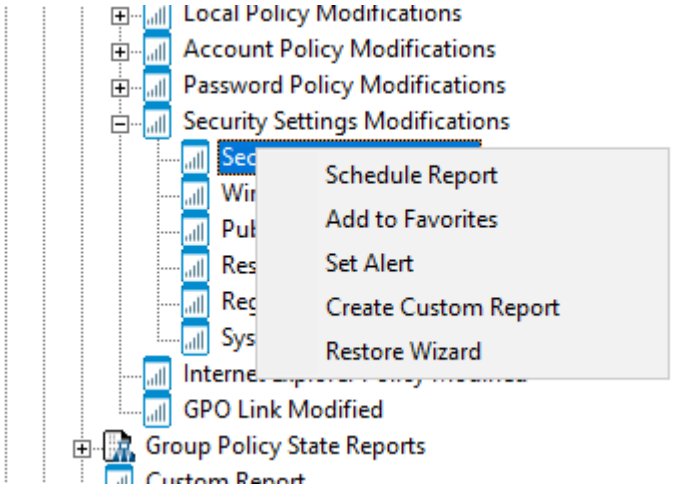

Figure 6: Context Menu

- Choose **Set Alert**

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

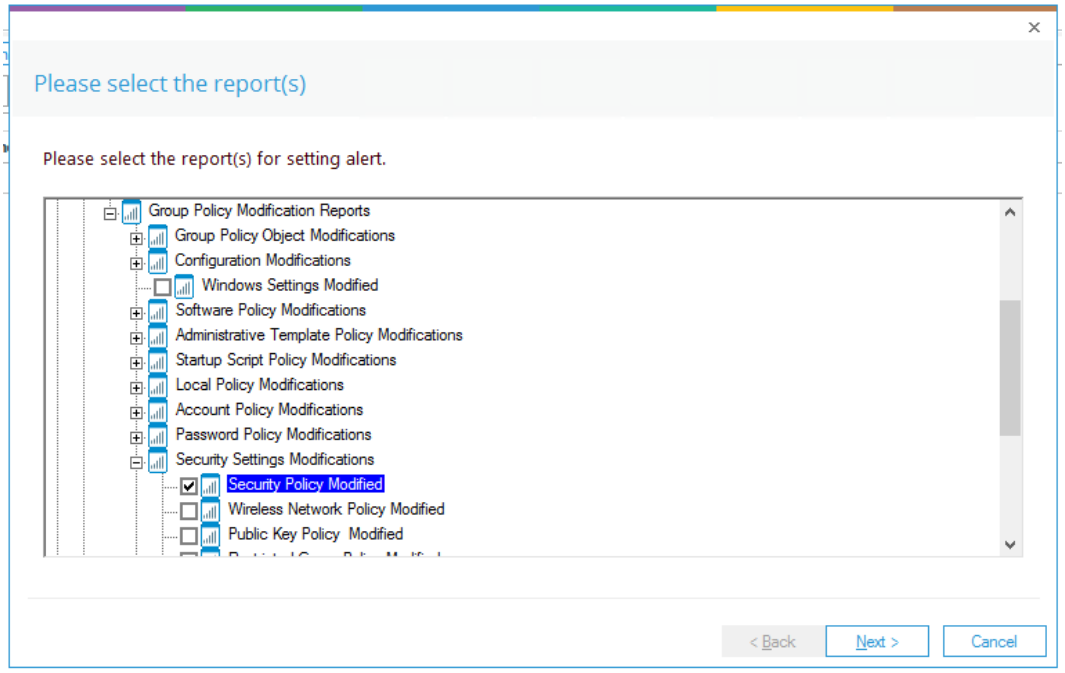

Figure 7: Select Reports

- Click **Next** to display the Set Filter(s) dialog box:

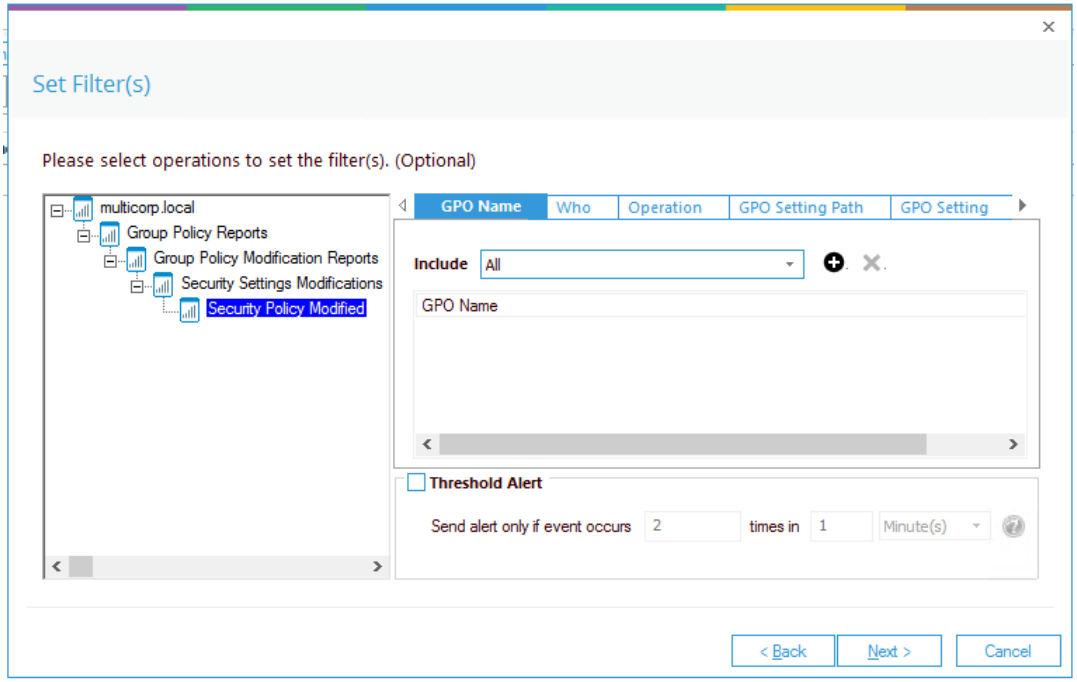

Figure 9: Set Filter(s)

On the left of this dialog box, you can see the report you are working on which in this case is **Security Policy Modified**.

There are options to apply filters for **GPO Name, Who, Operation, GPO Setting Path and GPO Setting** using the tabs at the top of this dialog box.

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:

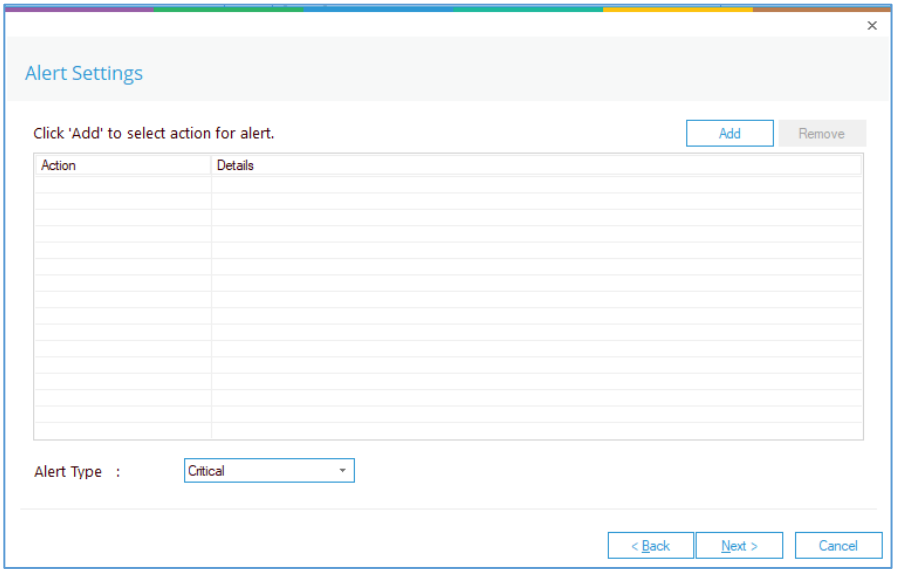

Figure 10: Alert Settings

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** here.

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

The **Add Alert Action** dialog box will be displayed:

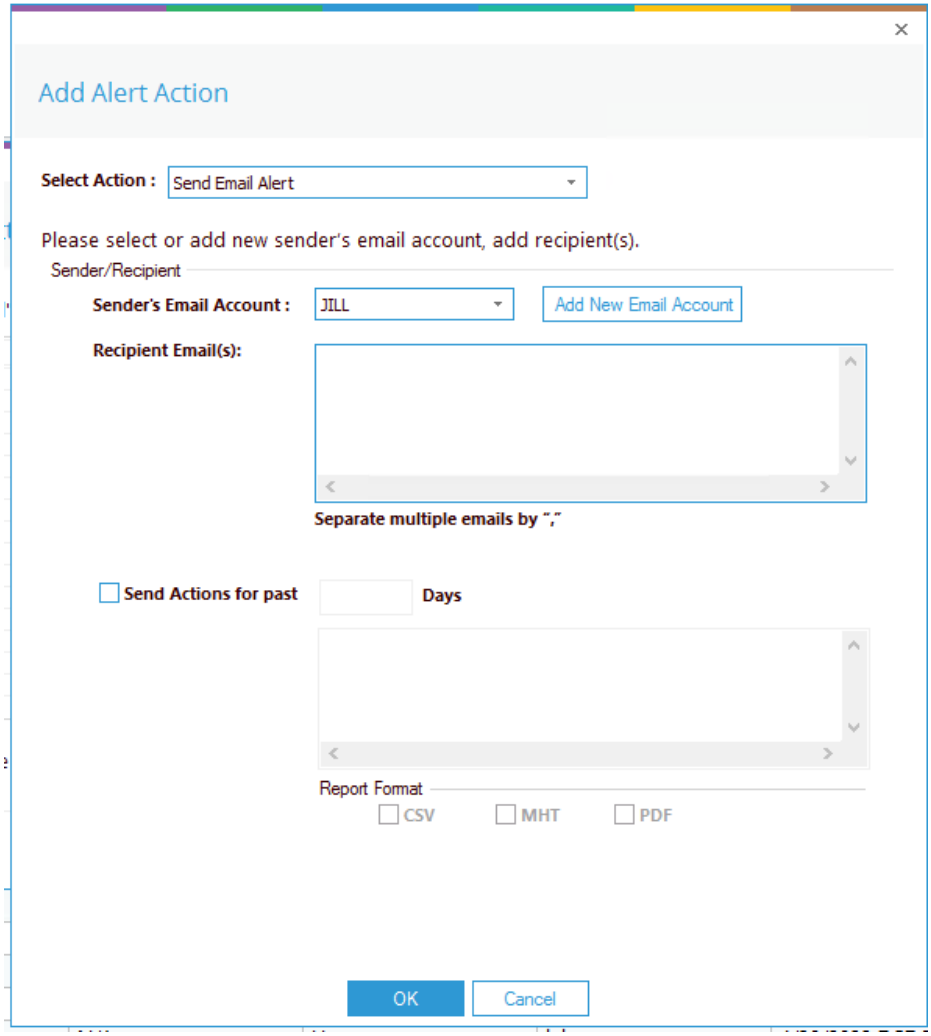

Figure 11: Add Alert Action

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

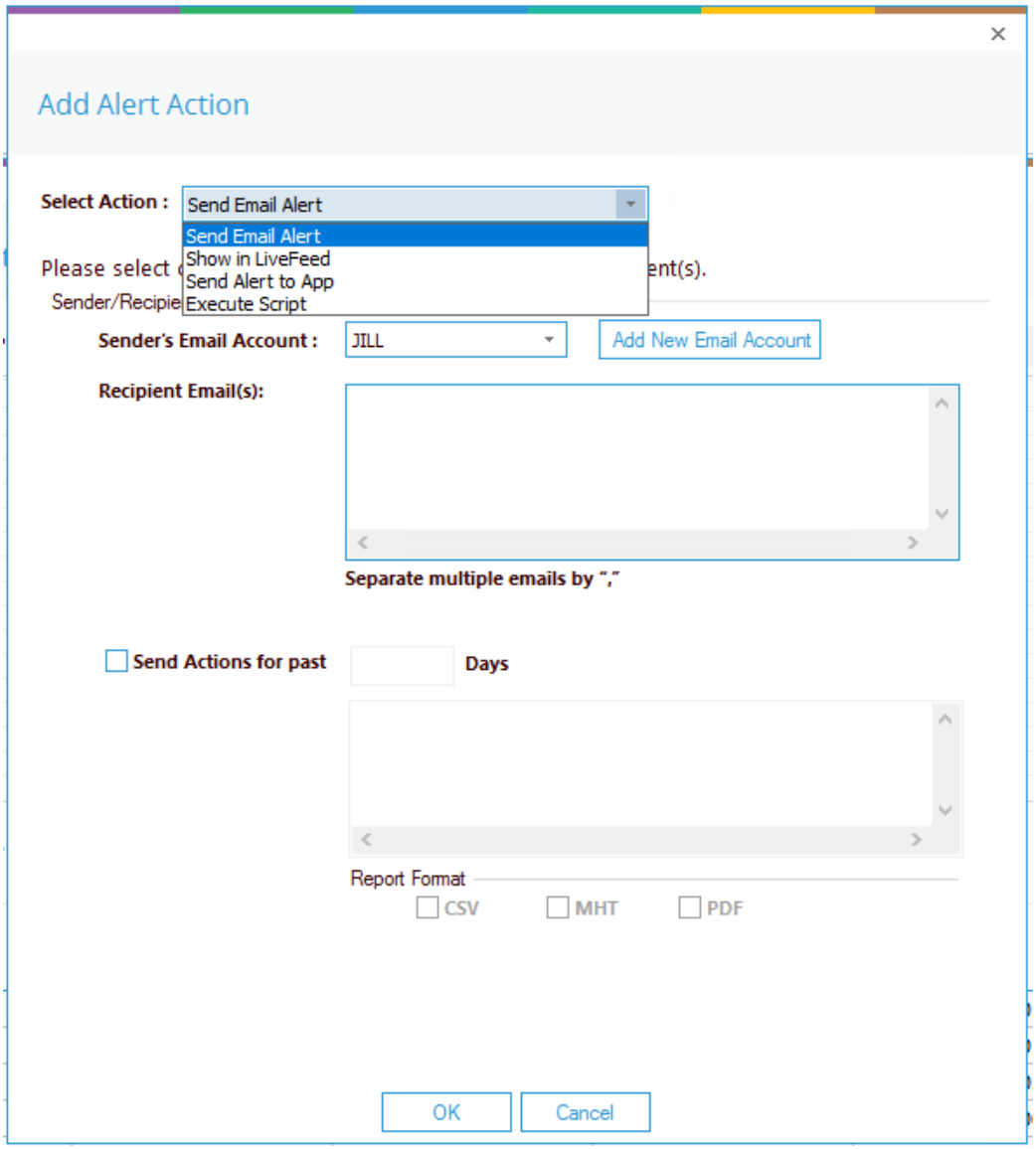

Figure 12: Alert Action Options

The Alert Actions are:

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

The configuration of each of these actions is explained as follows:

1. Send Email Alert

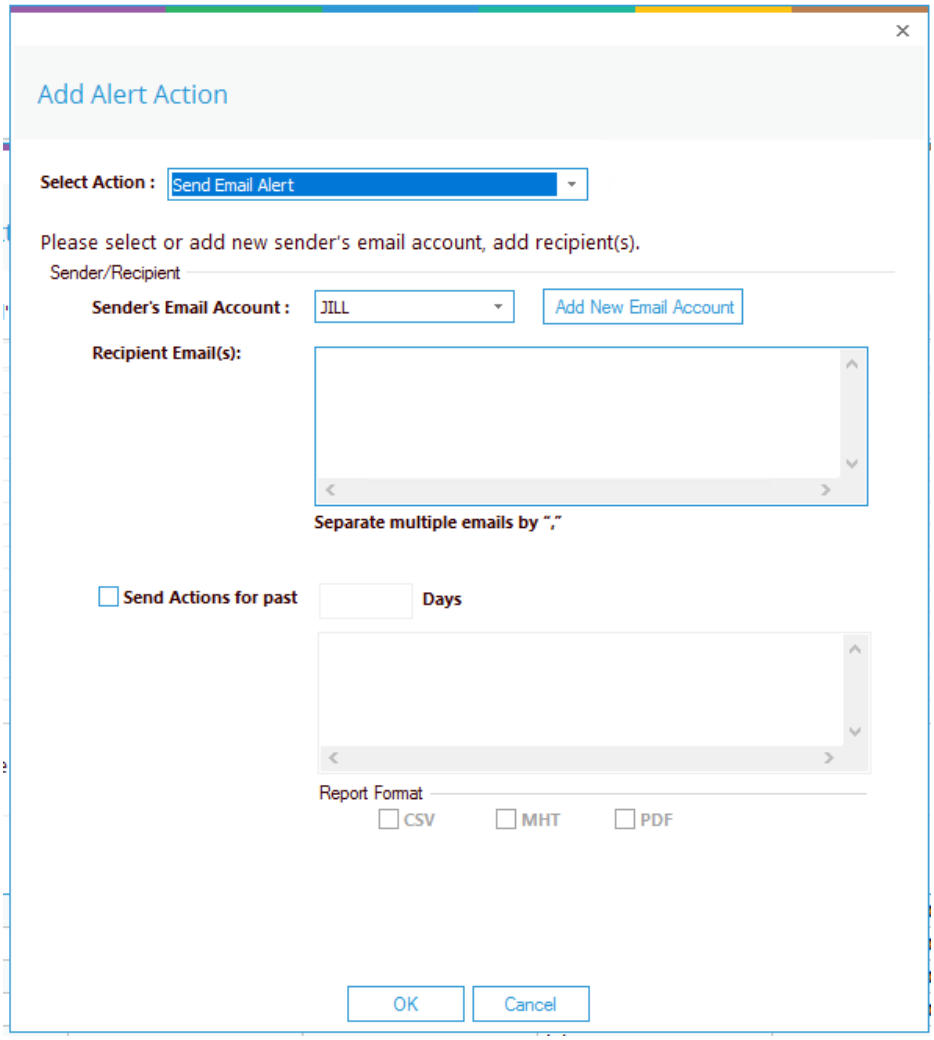

Figure 13: Add Alert Action - Send Email Alert

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 ','
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

permissions have been changed for a sensitive document, 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

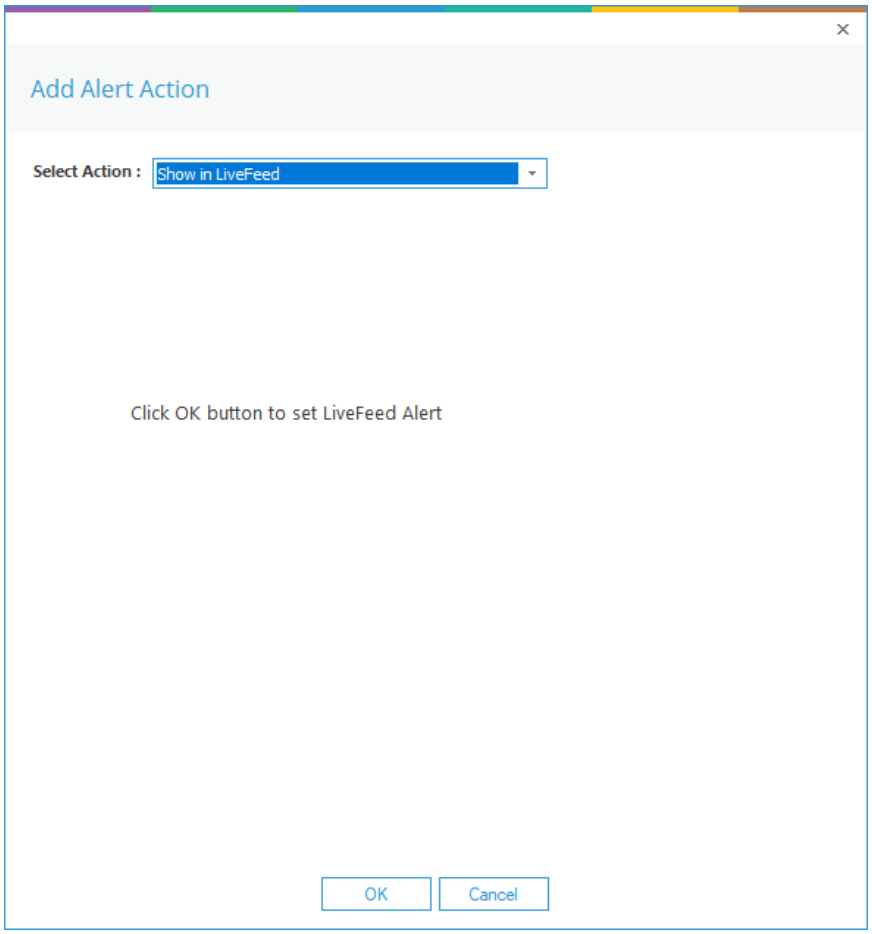

Figure 14: Add Alert Action – Show in LiveFeed

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

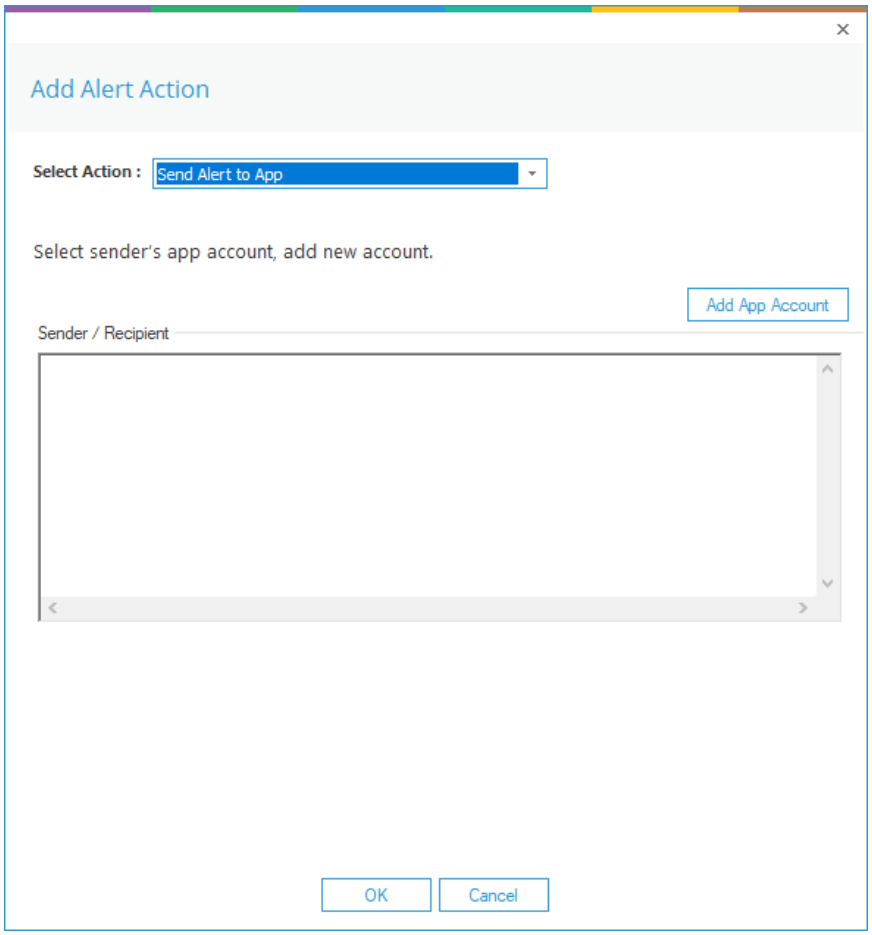

Figure 15: Add Alert Action – Send Alert to App

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:

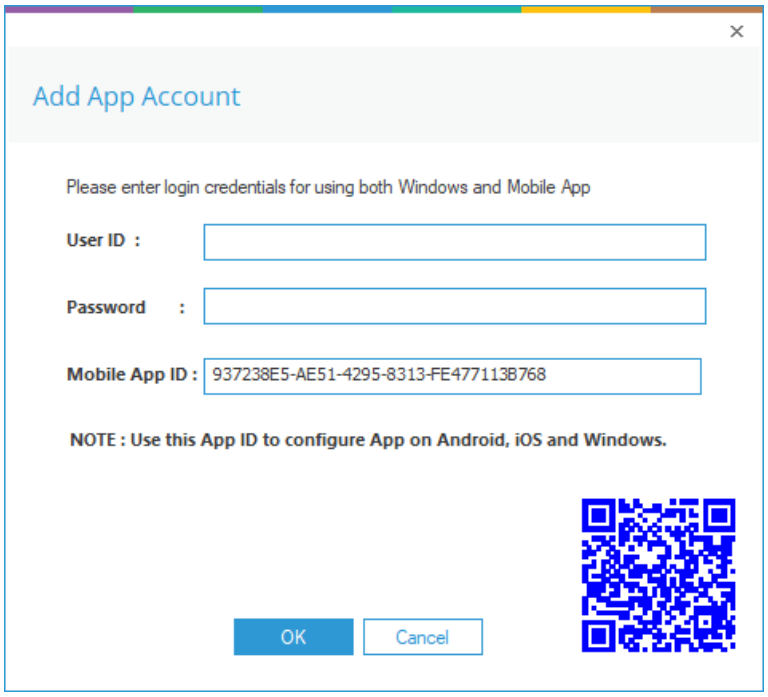

Figure 16: Add App Account

- 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

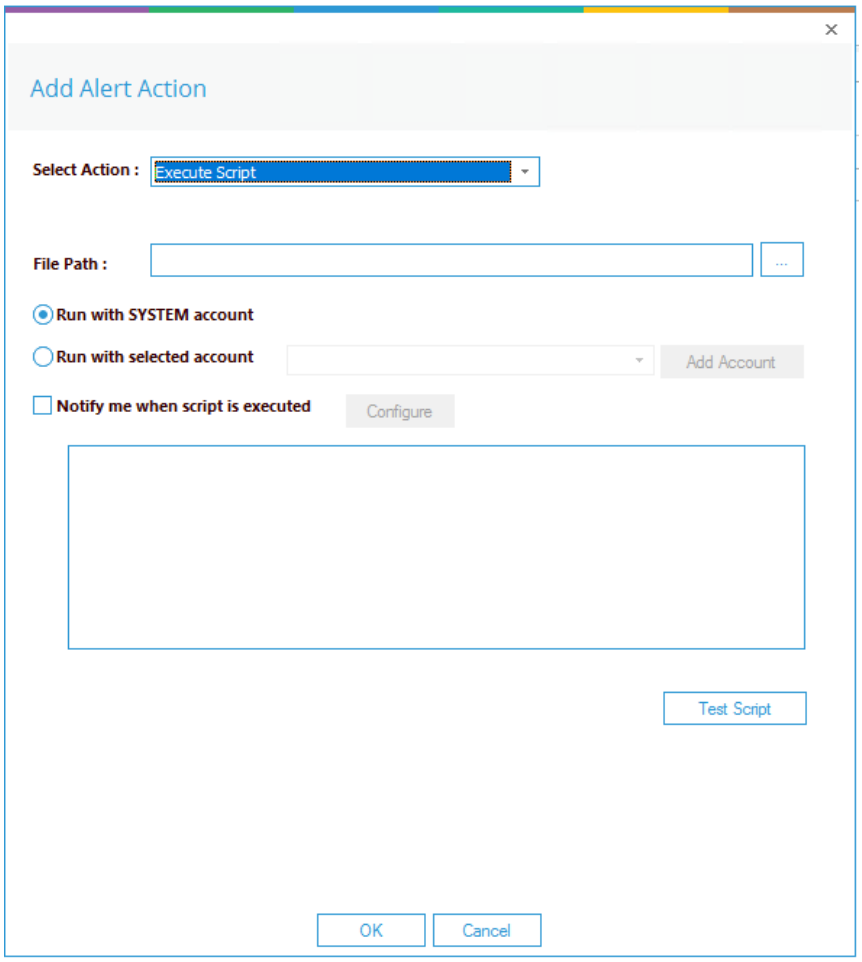

Figure 17: Add Alert Action – Execute Script

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.

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

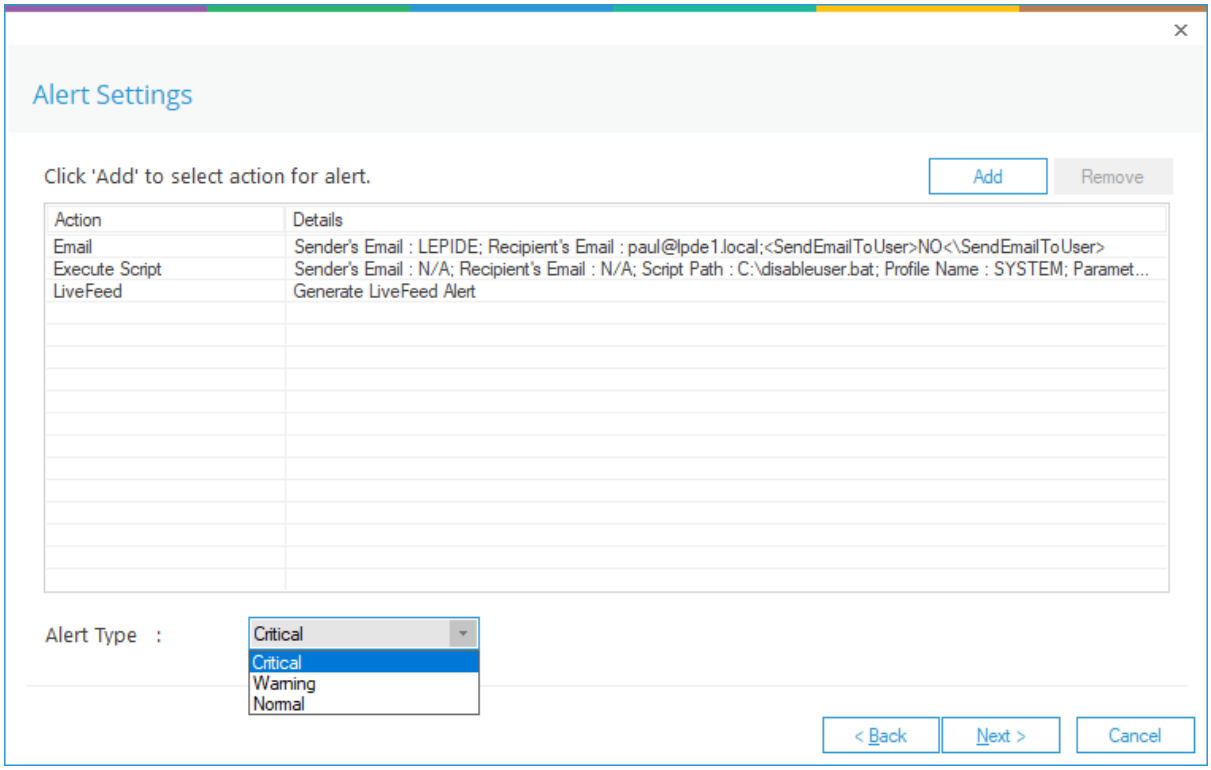

Figure 18: Alert Settings - Alert Type Options

- 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

The Alert is now setup. As soon as an email exchange takes place, the Lepide Data Security Platform will invoke the Alert settings and send an email to the recipient.

6.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/.

7.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.