Lepide

How to configure a real time alert.

Use case guide.

Contents

1 Introduction

Real time alerts for all significant security changes are an essential tool to enable organizations to quickly detect and respond to potential attacks. Alerts provide timely information about current security issues, vulnerabilities, and activities. Once an alert has been triggered, immediate action can be taken to reduce risk and mitigate damage.

The focus at Lepide is to provide visibility over what's happening with your network and through visibility you can take the necessary steps to reduce risk and stay compliant. Once an alert has been generated within the Lepide Data Security Platform, the administrator will be aware that there is a problem, and necessary action can be taken to resolve the issue.

2 What is an Alert?

Using the Lepide Data Security Platform, you can select the specific events for which you want to create alerts instead of being notified of every change in the system. The administrators, or selected recipients, can receive these alerts as email notifications, LiveFeed updates and as push-notifications on our mobile-based application.

Alerts can be generated based on several factors. These could be:

- a single event
- pre-defined criteria (such as time and date)
- threshold-based criteria

2.1 Threshold Alerting

Typical security breaches display characteristics which can be picked up by the Lepide threshold alerting capability. This ability to detect and alert on file activity which may be suspicious means that potential data breaches can be identified in motion and immediate action taken.

For example, if a large number of files are being copied within a short time this is a trend that could indicate the start of a ransomware attack. This suspicious activity would trigger an alert, the activity would then be investigated, and the appropriate action taken. For critical alerts, responses can be automated to provide immediate action which could be to shut down a server or revoke user access rights.

Three different criteria are used to define threshold alerts:

1. Number of events
2. Type of event
3. Time period

So, for example, if **100** files were **copied** within **20** seconds, an alert would be activated as this indicates the start of a ransomware attack. These different criteria options can be set by the User to suit their requirements.

All alerts are real time and are delivered either to the Lepide Dashboard, via email or directly to any iOS or Android mobile device.

Below is an example of a Live Feed Alert:

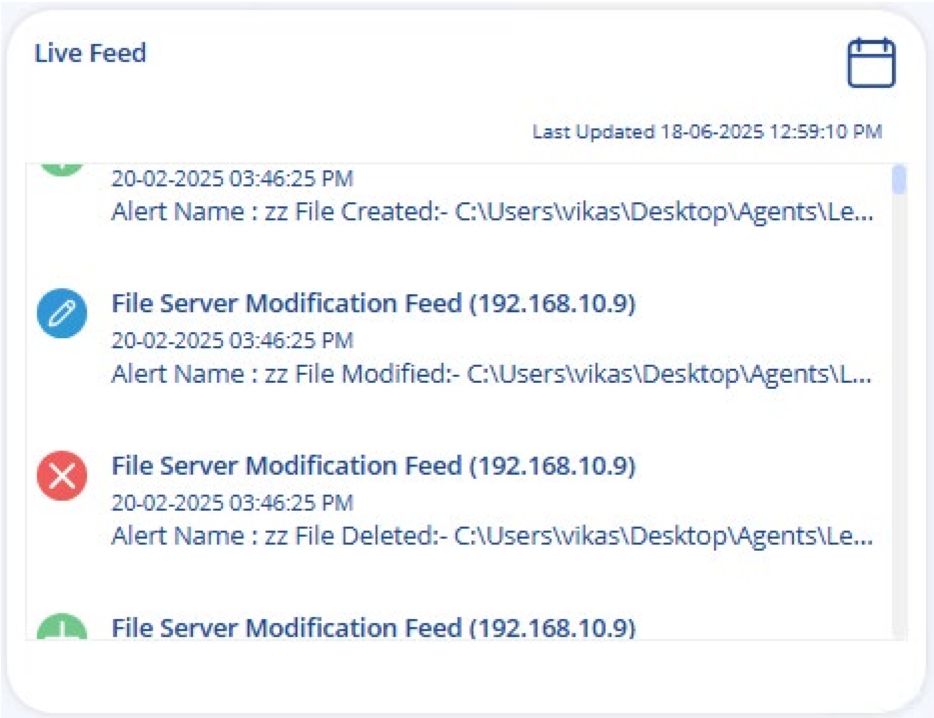


Figure 1: Live Feed Alert

2.2 Automated Response

The Lepide Data Security Platform can be configured to execute a customized script whenever a selected change is detected. Scripts can be of the following types:

- VB Script
- PowerShell Script
- Batch File

Using custom script execution, you can shut down users, servers and take other actions to mitigate the effects of a security breach.

3 To Create an Alert

An alert can be created from any of the reports within the Lepide Data Security Platform. For this example, we will look at creating an alert from the File Copied Report.

As described previously, if there is a situation where many files are being copied within a short space of time, this could indicate the start of a ransomware attack so creating an alert on file copying is essential to mitigate this risk.

To see the file copied data, the first step is to run the File Copied Report:

3.1 Run the File Copied Report

- From the Web Console Home Screen, choose **Lepide Auditor**, **Reports**
- Expand **File Server Reports** (from the tree structure to the left side of the screen)
- Select **Files Copied**

The Files Copied report is displayed:

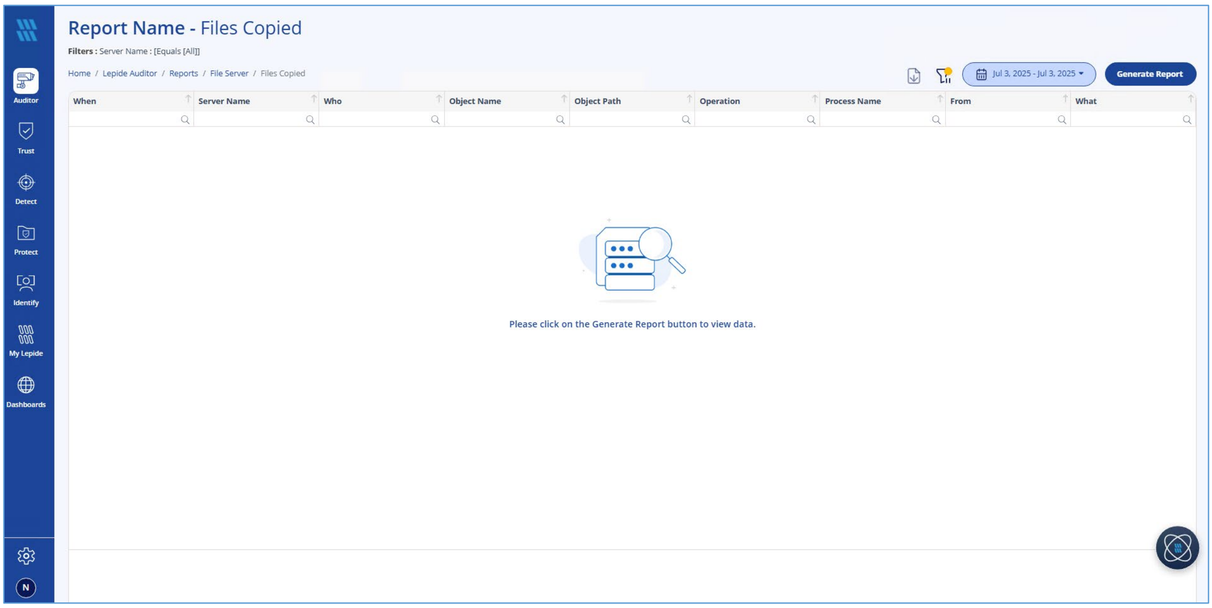


Figure 2: Files Copied Report

3.1.1 Specify a Date Range

- From the top of the screen, click on the date to choose a date range for the report

The following dialog box is displayed:

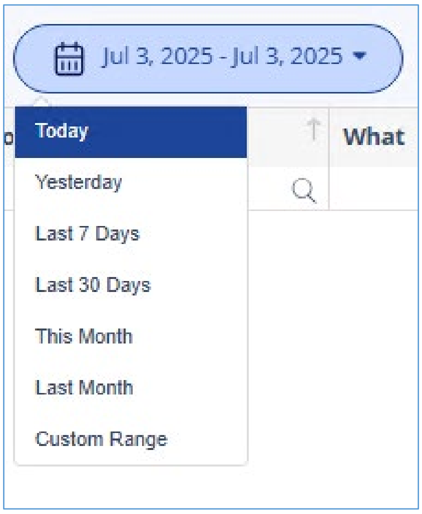


Figure 3: Date Range Filter

- Select a date range from the list
- Click **OK** and you will return to the File Copied screen
- Click **Generate Report**

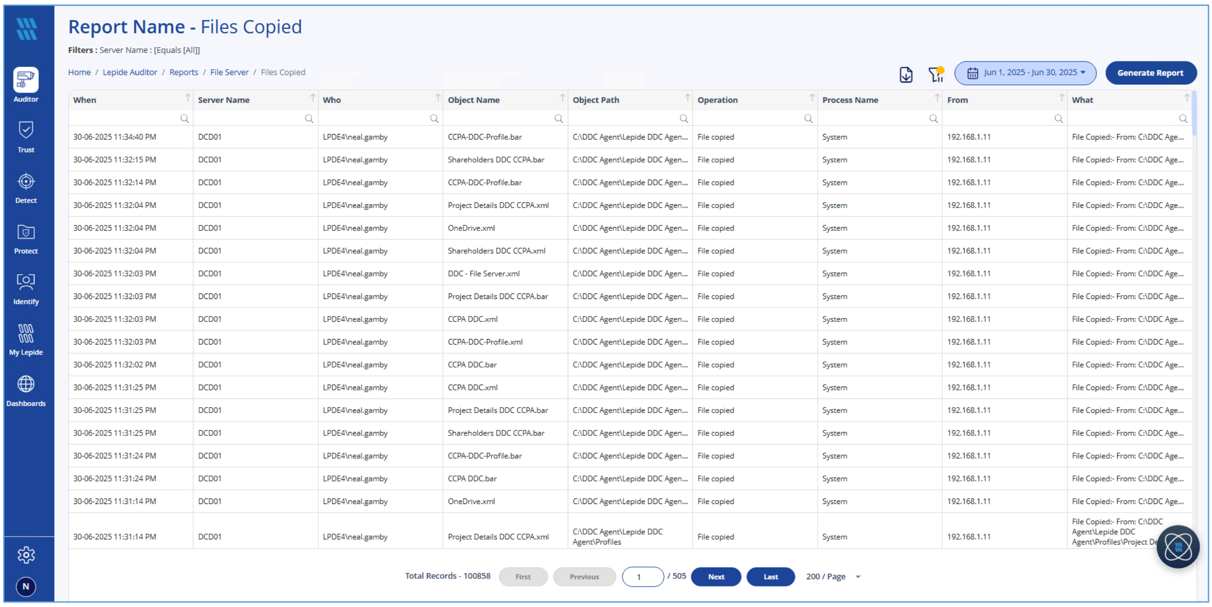


Figure 4: The Generated Files Copy Report

The report runs and shows information including who copied the file, what was copied and the location of the file.

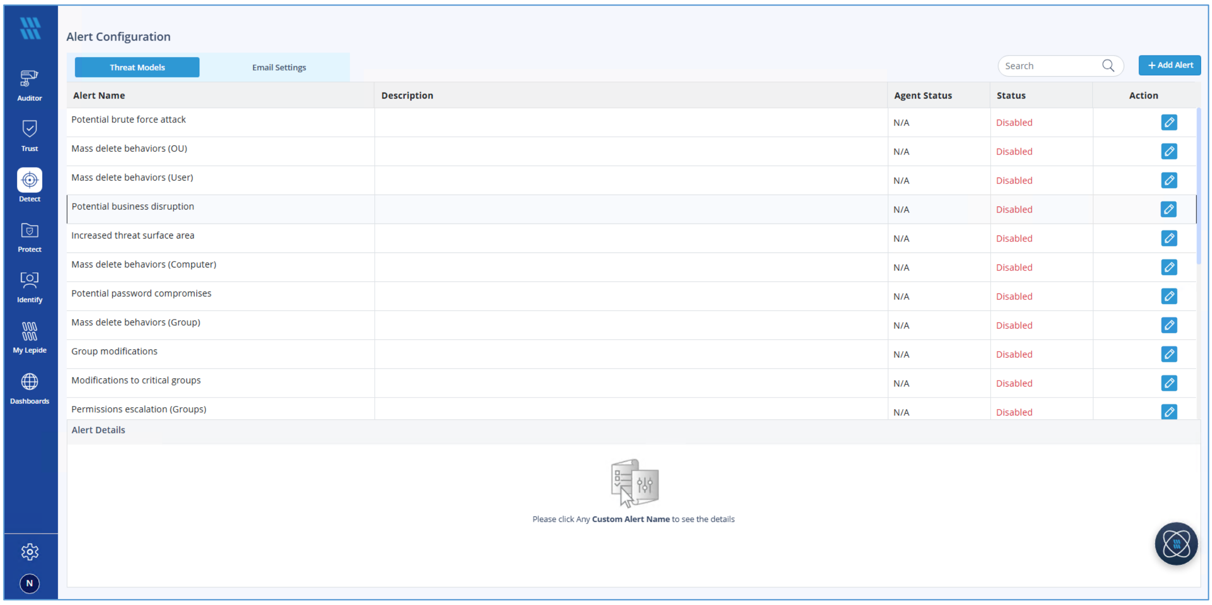
The report can be scheduled, saved, and exported.

3.2 To Create an Alert on the File Copied Report

An alert is created in the same way for all the Lepide Data Security Platform reports. Here, the Files Copied report is used as an example.

From the Web Console Home Page, select **Detect**

The **Alert Configuration** screen will be displayed:



- Click the **Add Alert** button

The **Add Alert** wizard starts:

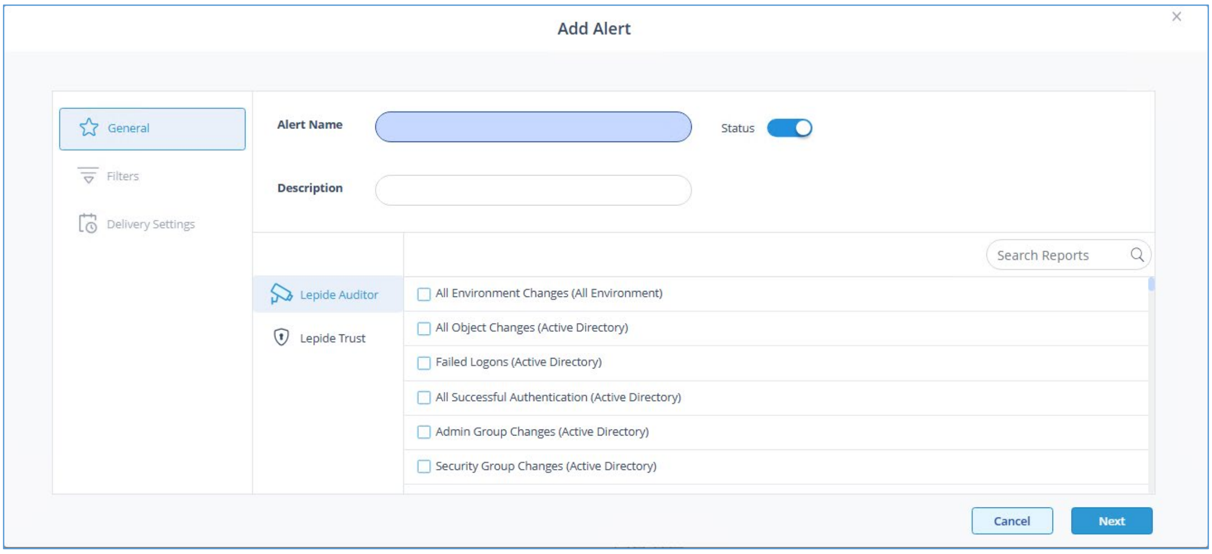


Figure 5: Add Alert Wizard

- Type a name for the alert in the **Alert Name** box
- Add an optional **Description**
- Select the report to add an alert to. In this example we will choose the **Files Copied (File Server) Report**
- Click **Next**

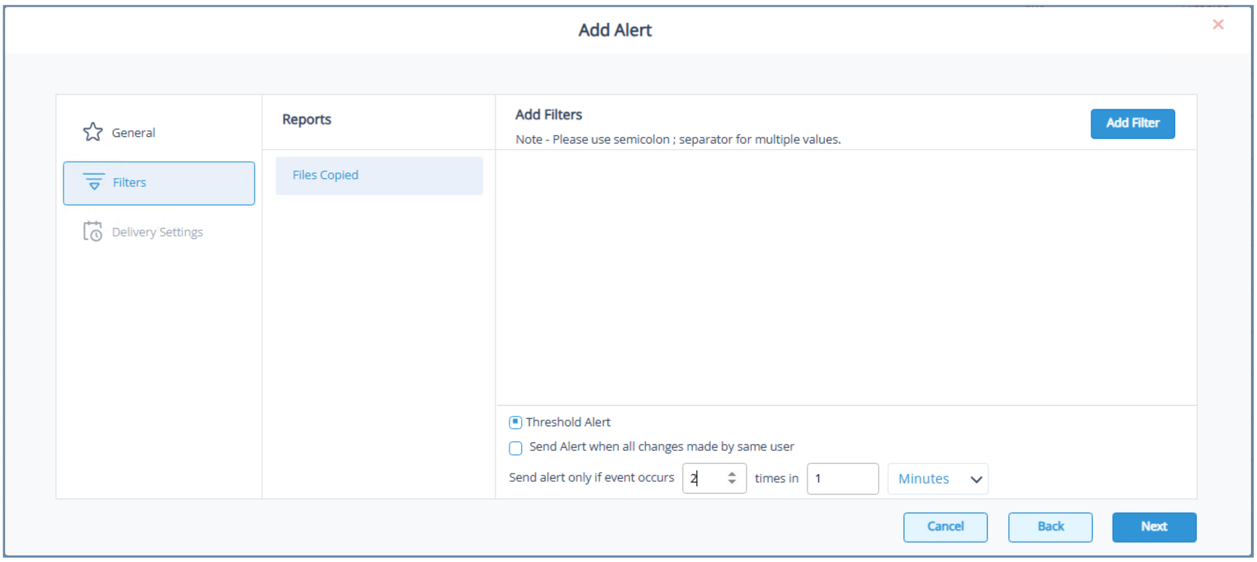


Figure 6: Add Alert Wizard – Filters

- On the left of the dialog box, you can see the report you are working on which in this case is **Files Copied**.
- Click the **Add Filter** button to add a filter if required. This will add filter options to the dialog box:

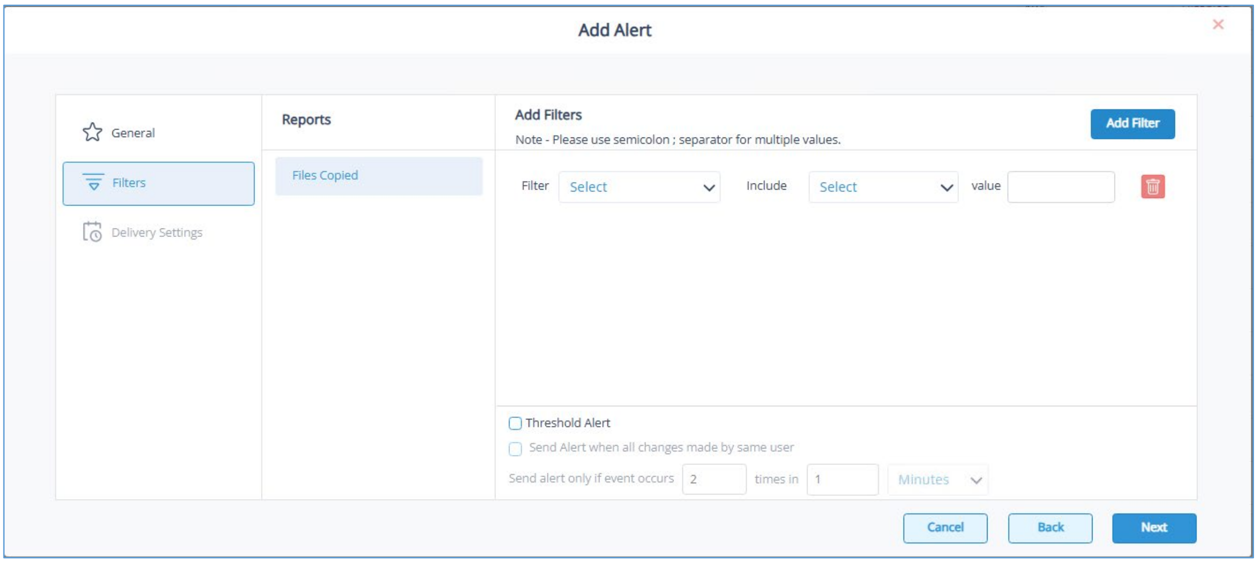


Figure 7: Filter Options Displayed

- Click the drop-down arrow next to **Filter** to select from the following options:

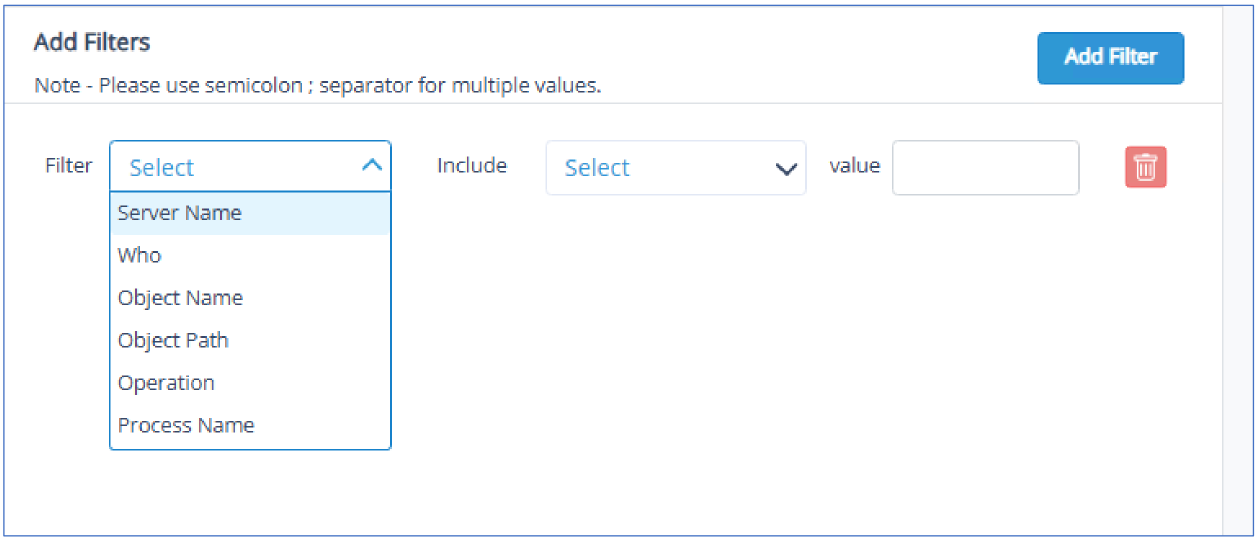


Figure 8: Filter Options

- Click the drop-down arrow next to Include to select from the following options:

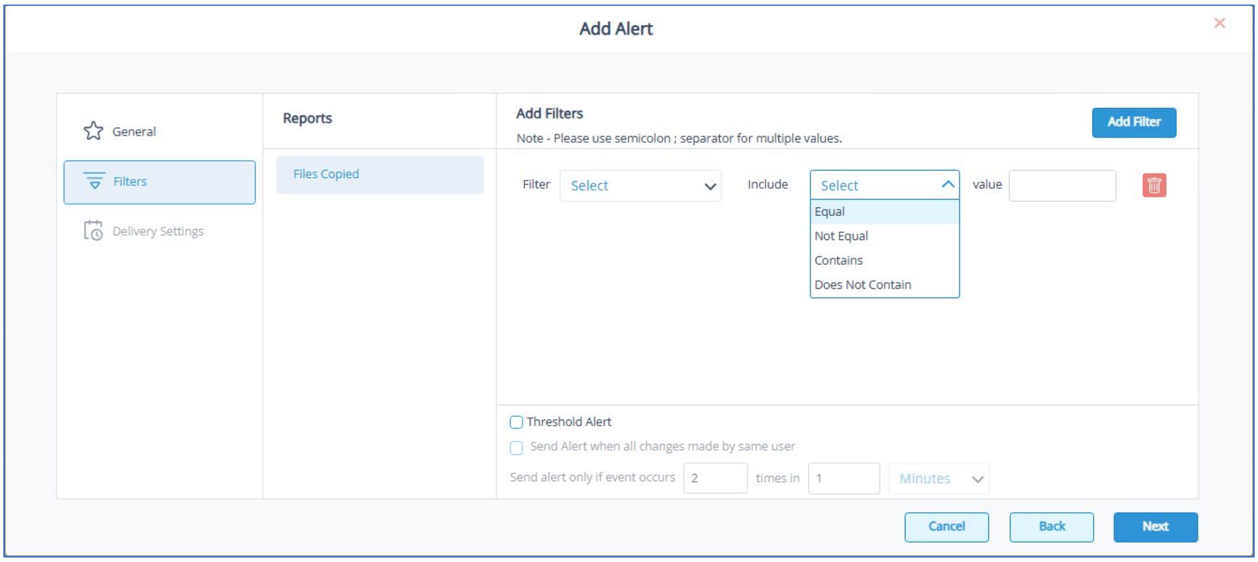


Figure 9: Include Options

- Type a value into the **Value** box

The threshold alert options can be customized as follows:

Threshold Alert:	Check this box to switch threshold alerting on
Send alert when all changes made by same user:	Check this if you want an alert to be sent when all changes have been made by a single user
Send alert only if event occurs:	Enter the number of times the event occurs, the time value and time-period here. This option is only available if the Threshold Alert button has been checked.

- Click **Next**

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

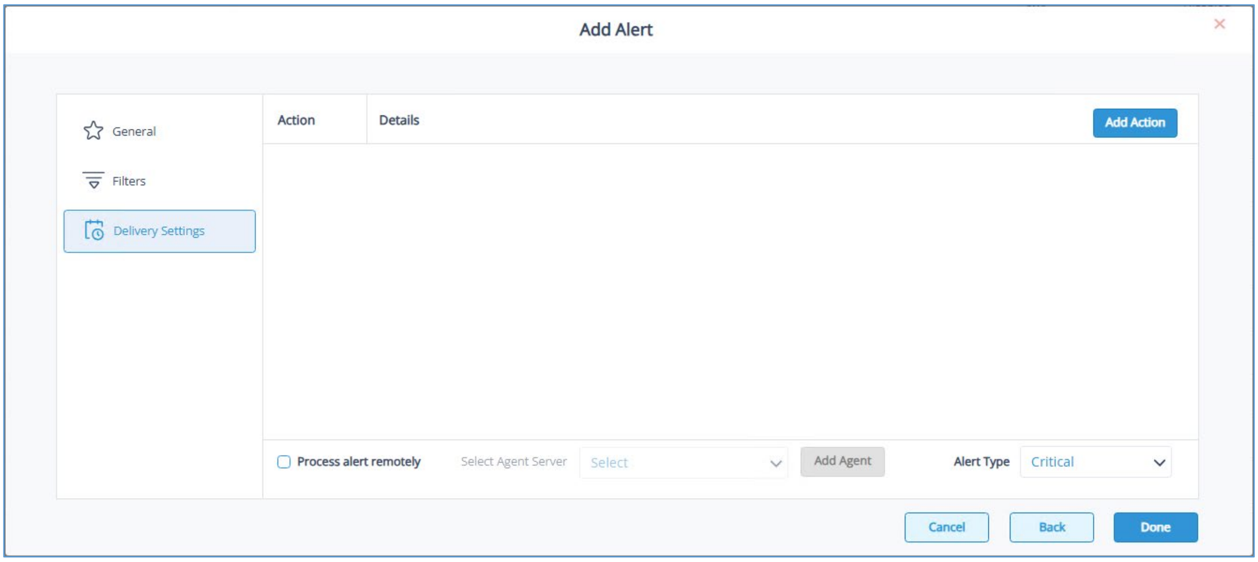


Figure 10: Alert Settings

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 select the following:

Alert Type: alert types are **Critical, Warning or Normal**

Process alert remotely: check this box and select an **Agent Server** from the drop-down menu to use an agent for processing the alert

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

The **Configure Report Delivery Action** dialog box will be displayed:

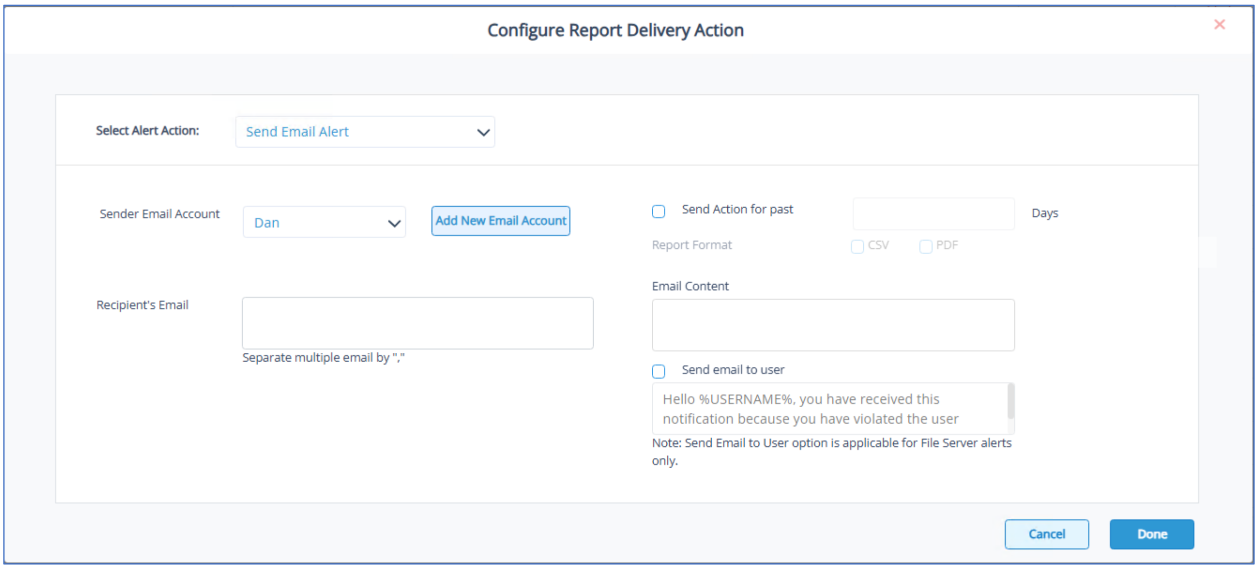


Figure 11: Configure Report Delivery Action

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

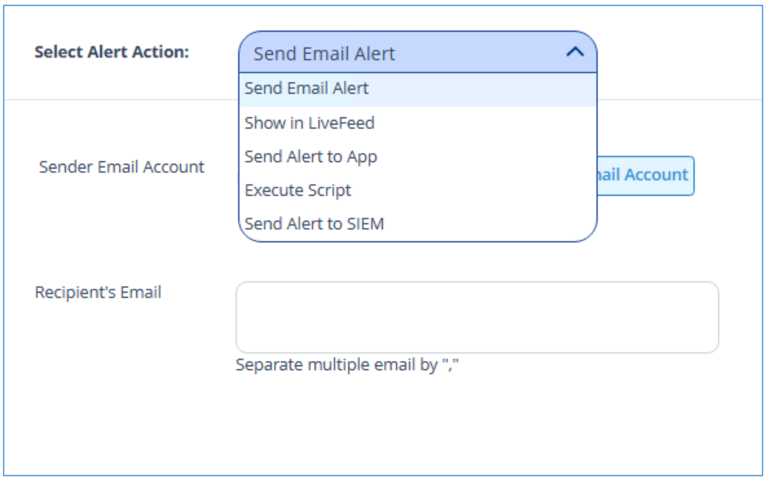


Figure 12: Alert Actions

The Alert Actions are as follows:

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

The configuration of each of these actions is explained below:

1. Send Email Alert

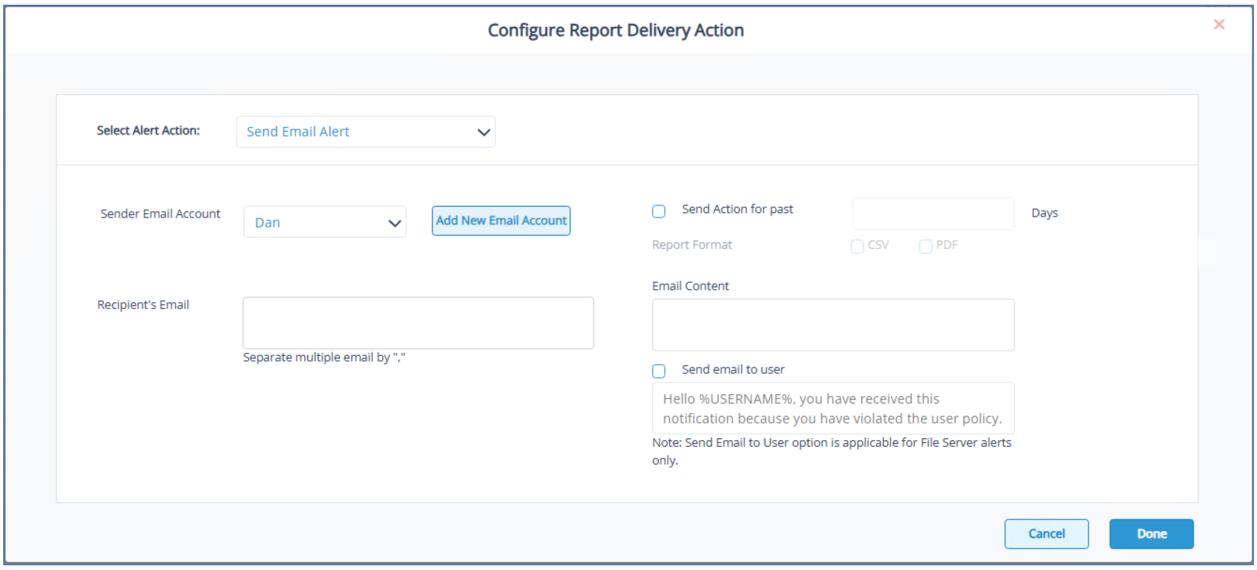


Figure 13: Add Alert Action – Send Email Alert

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. Further information on how to add a new email accounts is shown in Section 3.2.1 of this guide.
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 Email to user:	Check this box to send an email to the user. The content of the email can be typed into the text box. To include the username within the content, use the variable %USERNAME%. **Note** that this option is only applicable to File Server alerts.
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 they have been copying files, then you may want to see what else they have been doing. 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.

3.2.1 Add an Email Account

- Select **Add Email Account** from the menu

The following dialog box is displayed:

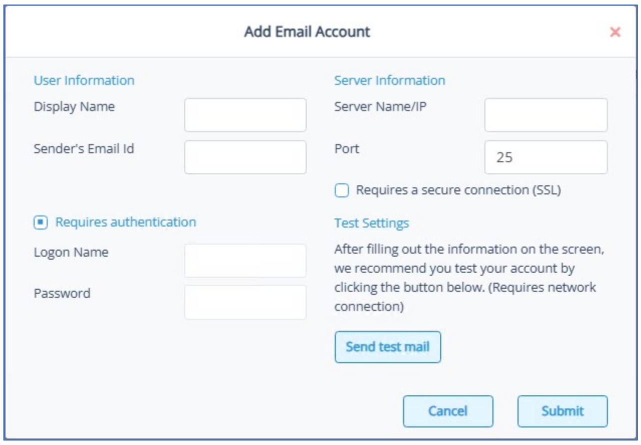


Figure 14: Add Email Account

- Add the following information:
  - Display Name
  - Sender's Email Id
  - Check the **Requires authentication** box if required
  - Logon Name
  - Password
  - Server Name/IP
  - Port
  - Check the **Requires a secure connection (SSL)** if required
- Select **Send a Test Email** to check that all the settings have been added correctly
- Click **Done** when finished
- You will return to the Configure Report Delivery Action dialog box
- Select the **Sender Email Account**
- Click **Done** when finished

2. Show in LiveFeed

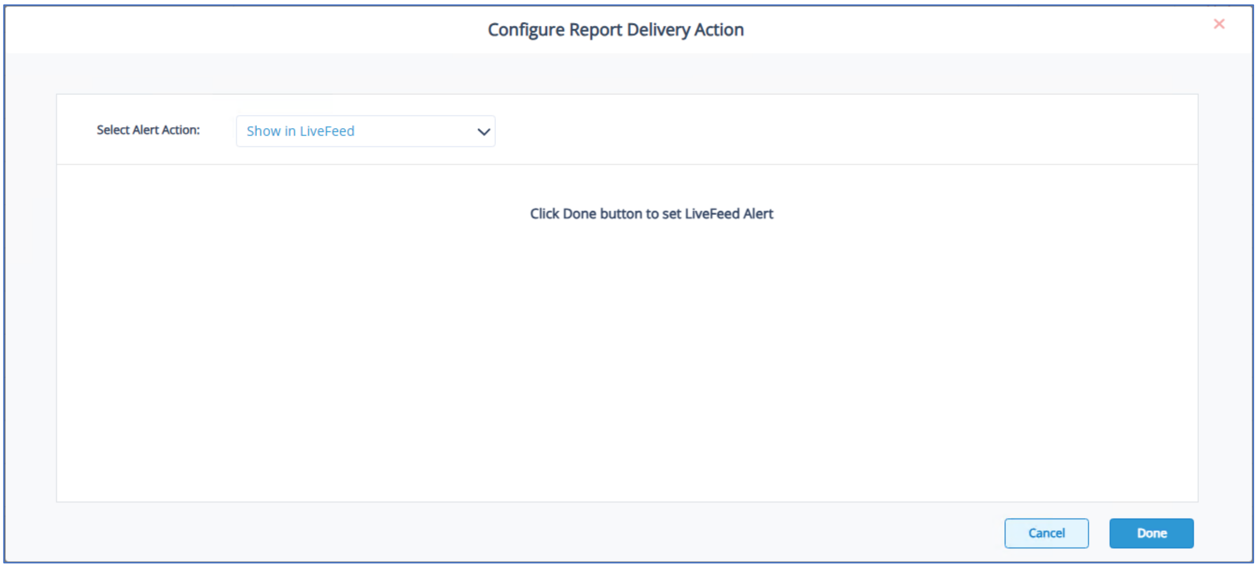


Figure 15: Add Alert Action – Show in LiveFeed

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

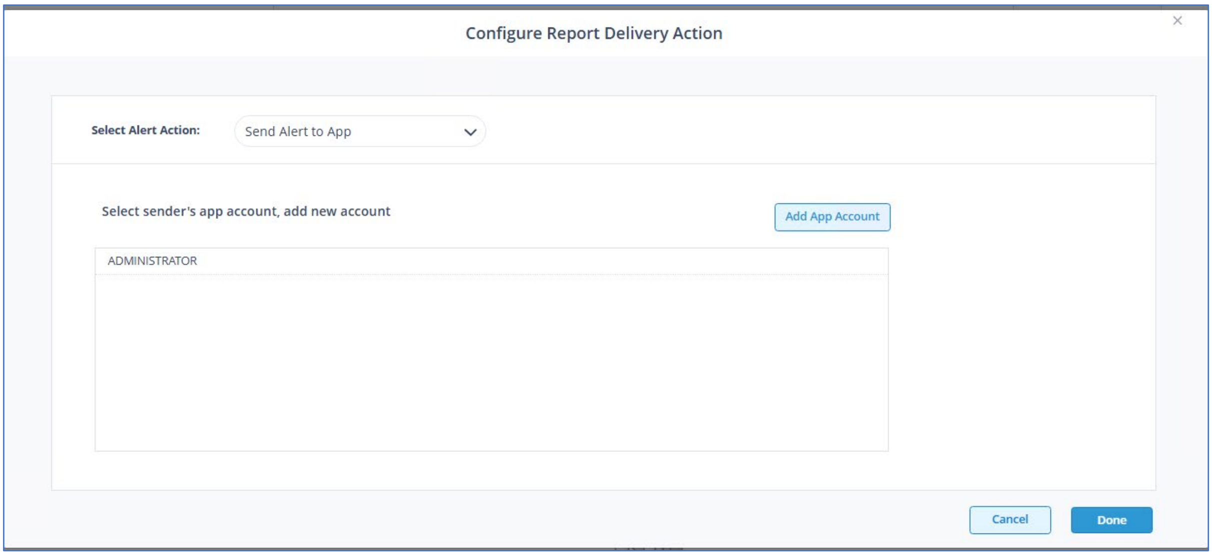


Figure 16: Add Alert Action – Send Alert to App

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

3.2.2 Add an App Account

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

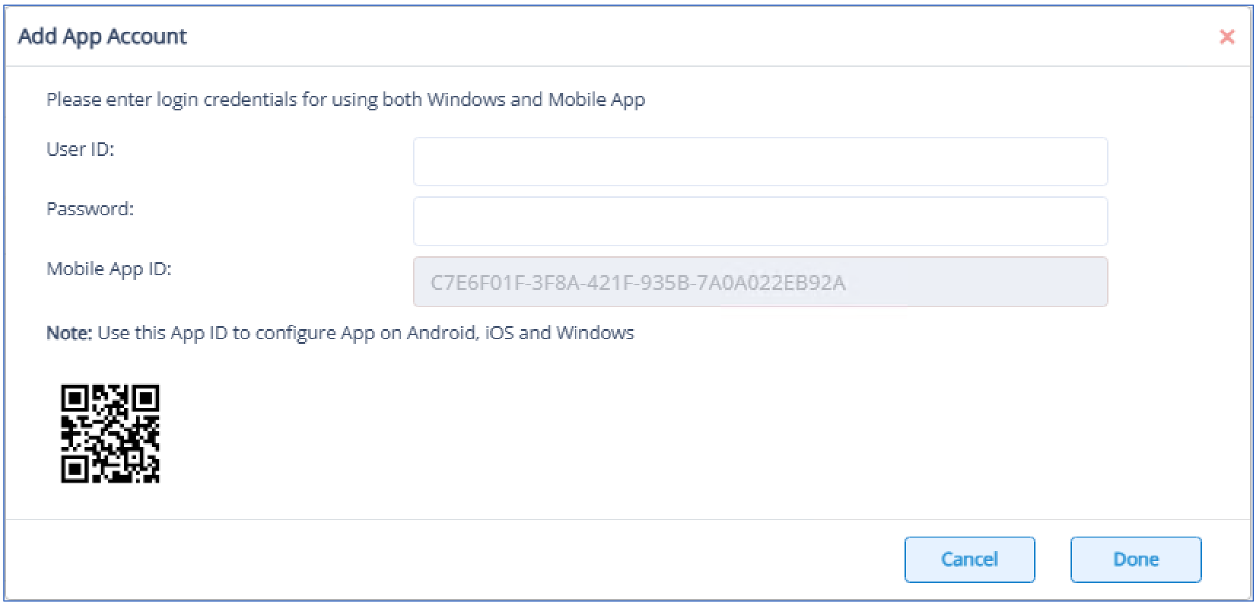


Figure 17: Add App Account

- 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 **Done** when you have finished adding the account. You will return to the Configure Report Delivery Action screen
- Select the newly added account from the list
- Click **Done** when finished

4. Execute Script

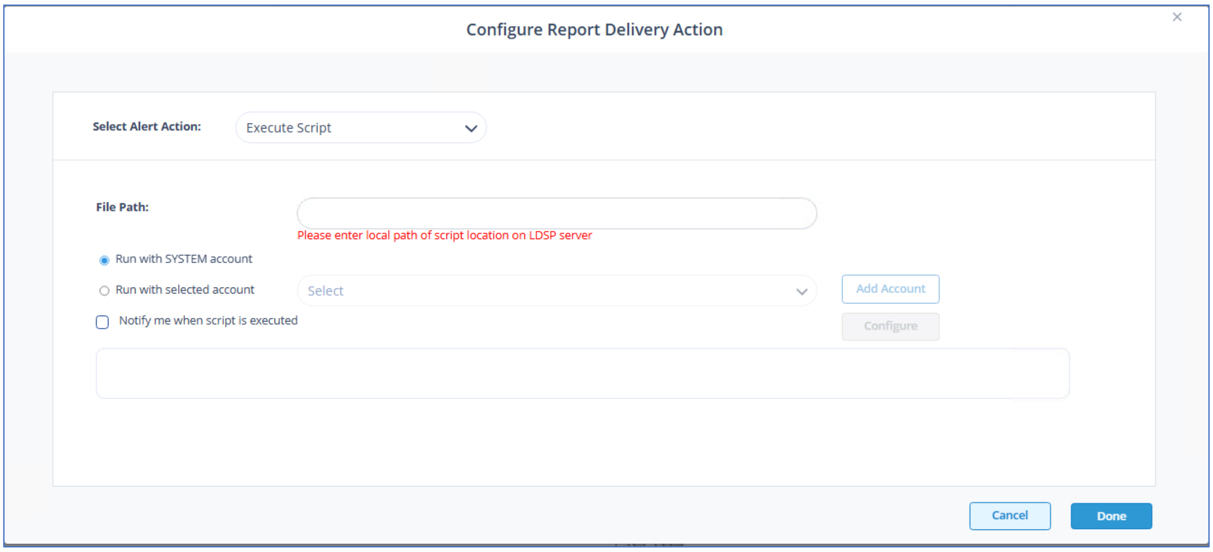


Figure 18: Add Alert Action – Execute Script

Execute Script gives 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:

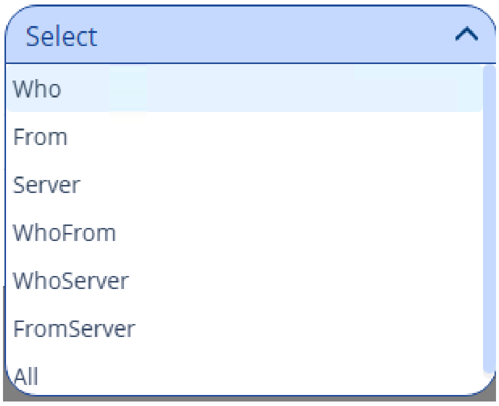


Figure 19: List of Variables

- Click **Test Script** to test that the specified script runs with no errors.

5. Send Alert to SIEM

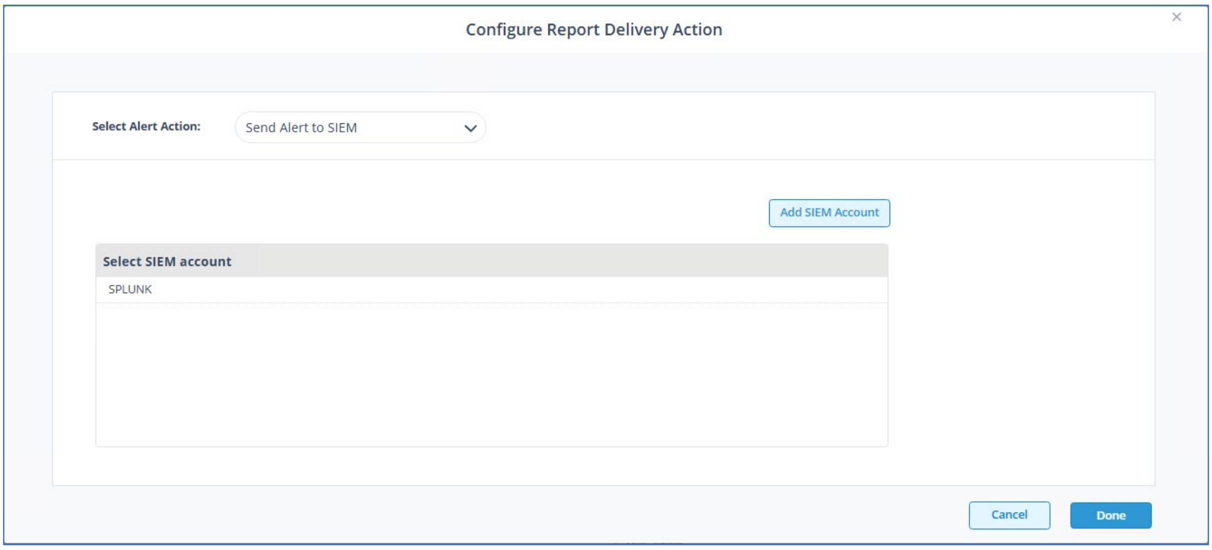


Figure 20: Add Alert Action - Send Alert to SIEM

- The Send Alert to SIEM option allows you to add a SIEM account and send an alert to the SIEM

3.2.3 Add a SIEM Account:

- Click the **Add SIEM Account** button to add details of your SIEM account

  The following dialog box is displayed:

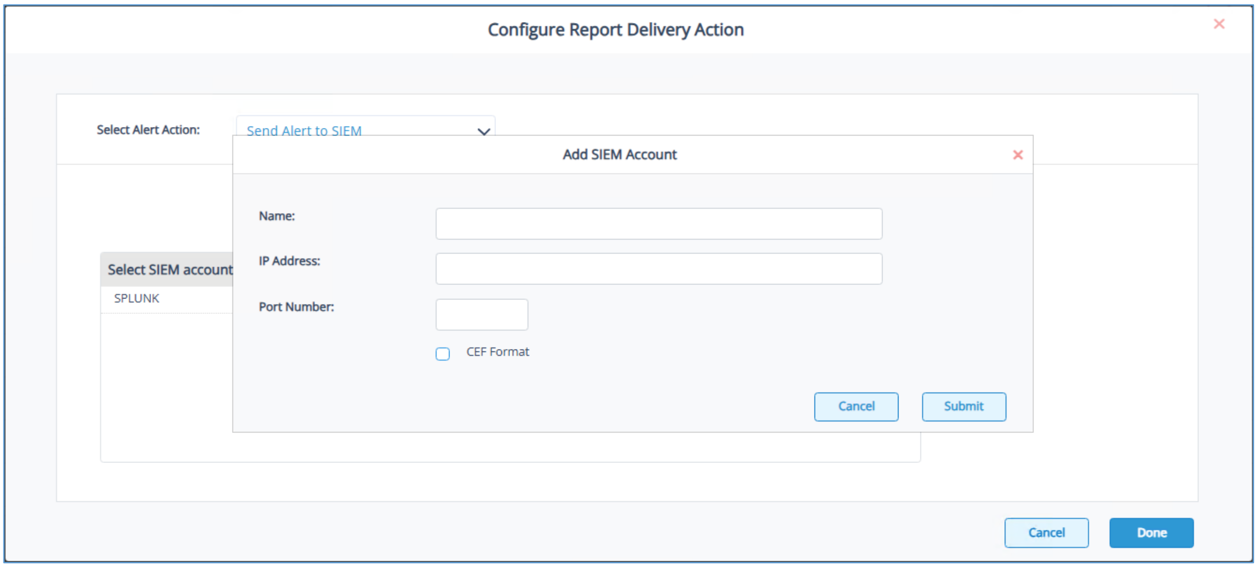


Figure 21: Add SIEM Account

- Add the **Name, IP Address and Port Number** for the SIEM account
- Check the **CEF Format** box if required
- Click **Submit**

  This will take you back to the Configure Report Delivery Action screen.
- Select the **SIEM** account and click **Done** when finished
- Click **Done** to return to **Add Alert** dialog box and details of the alert will be displayed
- Click **Done** when finished and the alert will be created

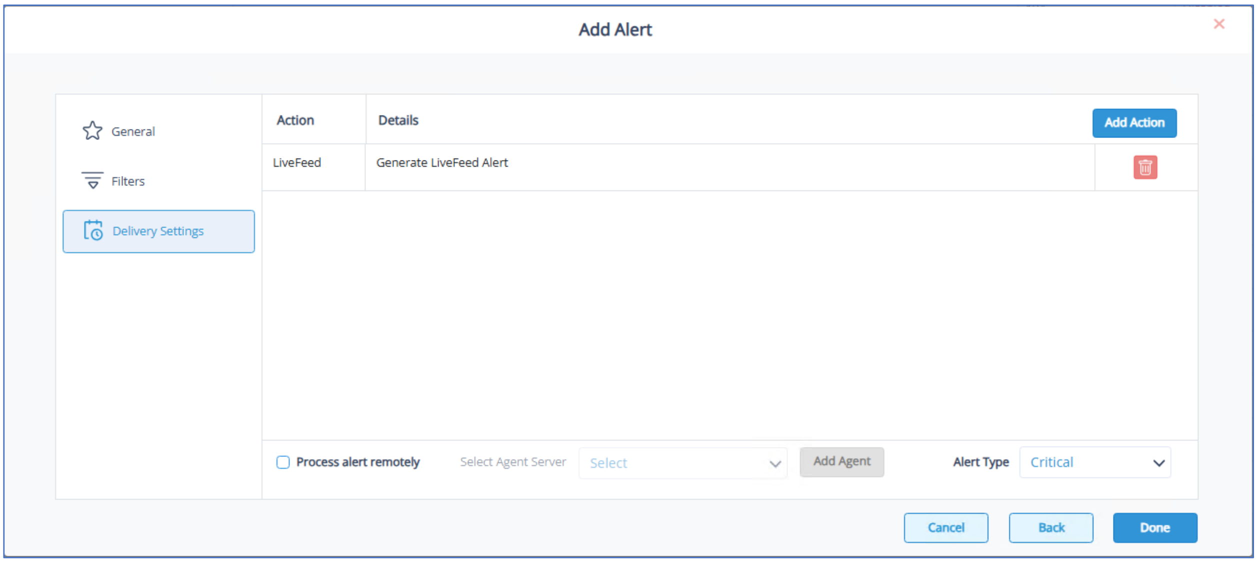


Figure 22: Alert Listed

- Click **Done** when finished to return to the Alert Configuration screen

4 Threat Models

Another way to configure an alert is to enable one of the many pre-defined Threat Models which are included with the Lepide Data Security Platform. A threat model is a predefined alert for a particular scenario, for example a potential ransomware attack, or files copied. Real time alerts are generated whenever a potential threat is detected by enabling one of these predefined threat models.

- To display a list all the Threat Models available within the Lepide Data Security Platform, select Lepide Identify, Alert Configuration:

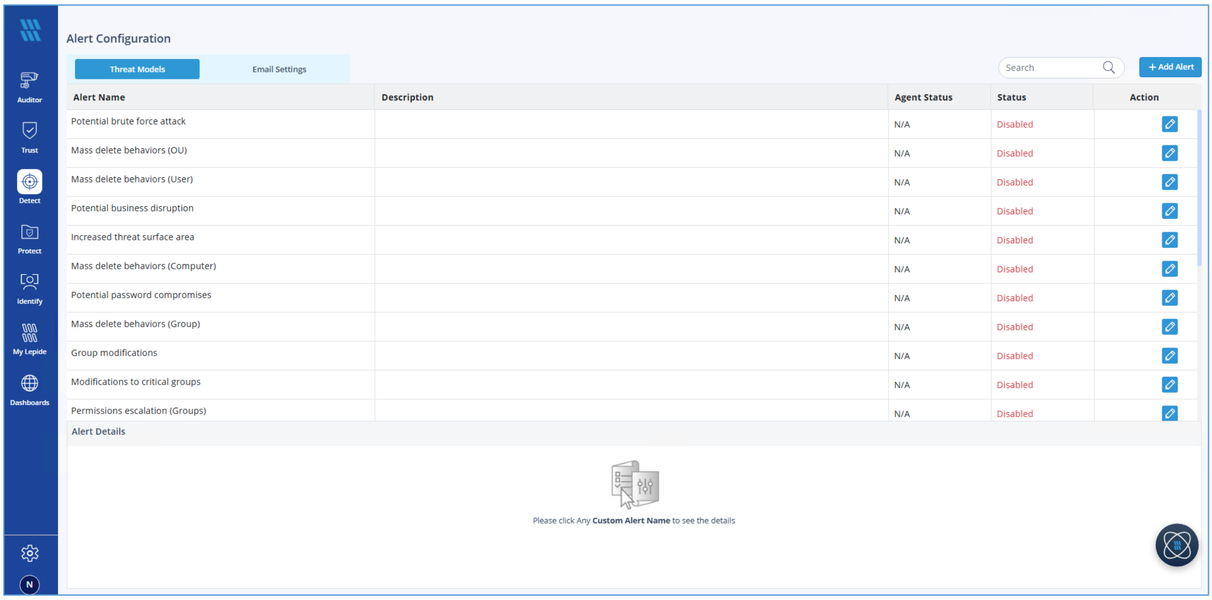


Figure 23: Threat Models

The Threat Models can be enabled as needed. They can then be configured to generate an alert and respond to a threat. The example below explains how to enable the **Potential Ransomware Attack Threat Model**.

4.1 How to Enable and Configure a Threat Model

- Select Lepide Identify, Alert Configuration to display the list of Threat Models
- To enable a Threat Model, click the Edit icon next to the Threat Model

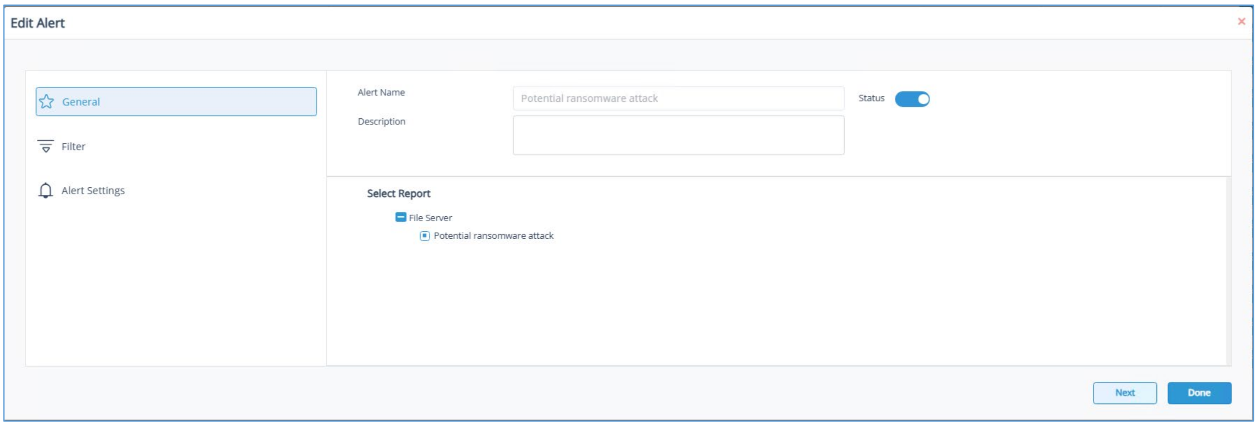


Figure 24: Alert Status

This will start the Alerts Wizard which is the same wizard used for setting up and editing alerts explained earlier in this document.

- Slide the **Status** button to the right to enable the alert
- Continue through the steps of the Wizard making changes as required. Please refer to Section 3.2 of this guide for more information about the steps of the Wizard.
- Click **Done** when finished

5 To Delete or Edit an Alert

- All Alerts are listed within the Threat Models screen which can be found under **Lepide Detect, Alert Configuration**
- Scroll down the list of Threat Models to see the user-defined alerts as these will be listed after the predefined alerts

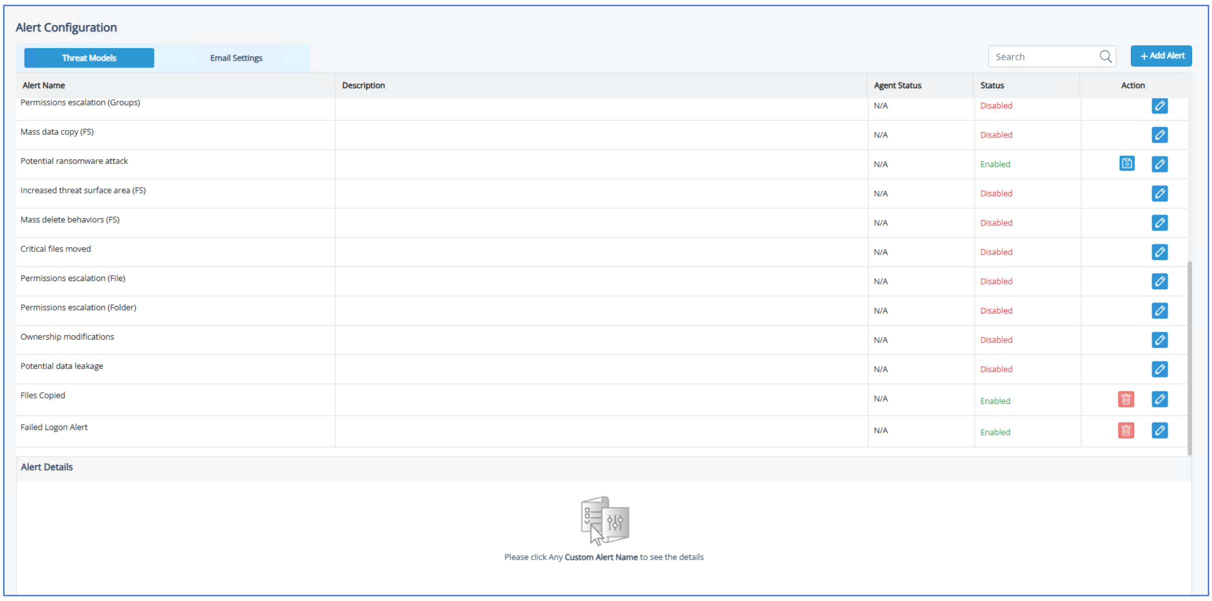


Figure 25: Threat Models

- Next to each alert is a Delete  and an Edit  option. Note that only the user-defined alerts can be deleted or edited. The predefined alerts can only be edited.

To Delete an Alert:

- To delete an alert, click the  icon

  A confirmation message box will be displayed:

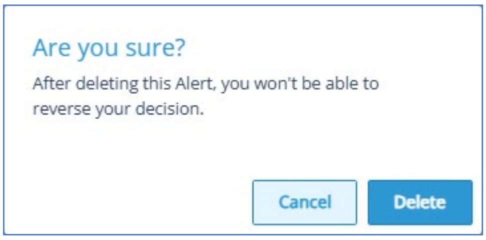


Figure 26: Confirmation to Delete an Alert

- Click **Delete** to confirm deletion of the alert

To edit an alert:

- To edit an alert, click the  icon
- This will take you back to the Alert wizard. Work through the steps of the Wizard making changes as required and click **Done** when finished

6 Email Settings

The email settings screen shows the email configurations for the different accounts which are used when configuring the alerts. These accounts can be added as part of the Alert Wizard or can be set up here by clicking the **Add** button.

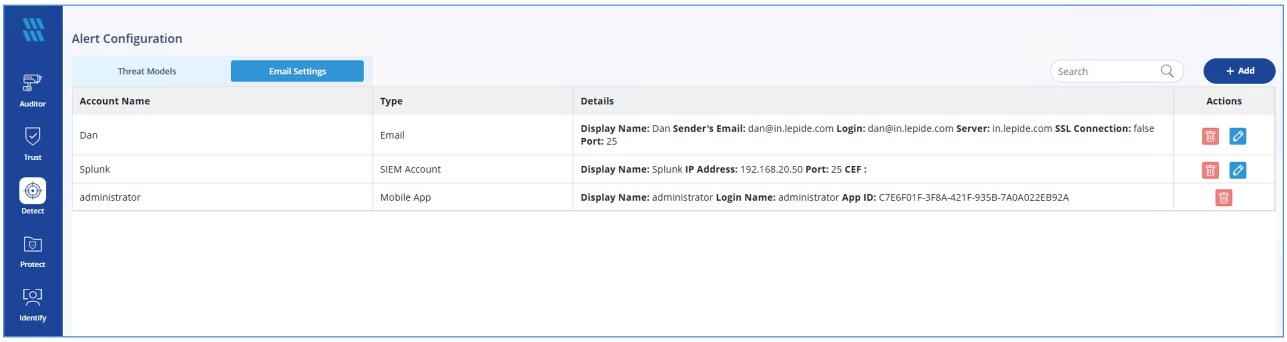


Figure 27: Email Settings

6.1 To Add an Email Account Setting

- Click the **Add** button

The Add drop down menu is displayed:

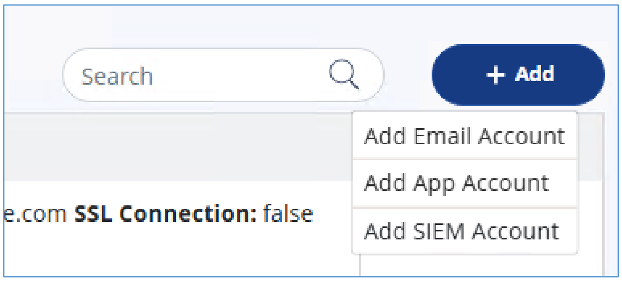


Figure 28: Add Account Menu

- Please refer to section 3.2 of this guide for more information on adding the different account configurations.

6.2 To Edit an Email Account Setting

- Click the Edit button  next to the account to be edited

6.3 To Delete an Email Account Setting

- Click the Delete button  next to the account to be deleted

7 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/.

8 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.