Lepide

USE CASE GUIDE

# HOW TO CONFIGURE A REAL TIME ALERT

# Table of 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.

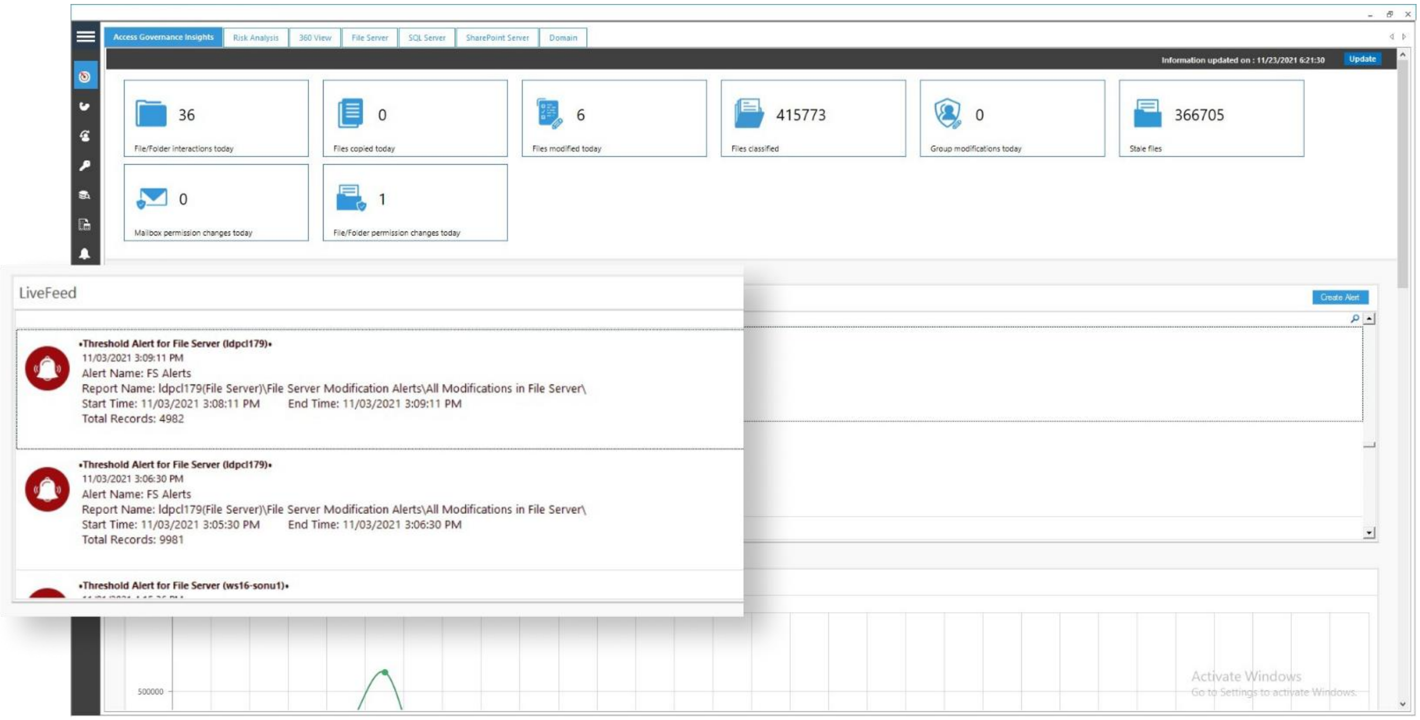
Three different criteria are used to define threshold alerts:

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 Threshold Alert on the Lepide Dashboard:



Information updated on : 11/23/2021 6:21:30

36 File/Folder interactions today

0 Files copied today

6 Files modified today

415773 Files classified

0 Group modifications today

366705 Stale files

0 Mailbox permission changes today

1 File/Folder permission changes today

•Threshold Alert for File Server (ldpcl179)•
11/03/2021 3:09:11 PM
Alert Name: FS Alerts
Report Name: ldpcl179(File Server)\File Server Modification Alerts\All Modifications in File Server\
Start Time: 11/03/2021 3:08:11 PM End Time: 11/03/2021 3:09:11 PM
Total Records: 4982

•Threshold Alert for File Server (ldpcl179)•
11/03/2021 3:06:30 PM
Alert Name: FS Alerts
Report Name: ldpcl179(File Server)\File Server Modification Alerts\All Modifications in File Server\
Start Time: 11/03/2021 3:05:30 PM End Time: 11/03/2021 3:06:30 PM
Total Records: 9981

•Threshold Alert for File Server (ws16-sonu1)•

*Figure 1: Threshold 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

- Click the **User and Entity Behaviour Analytics** icon
- Expand **File Server Reports** (from the tree structure to the left side of the screen)
- Expand **File Server Modification Reports**
- Click on **File Copied** to display the **File Copied Report**

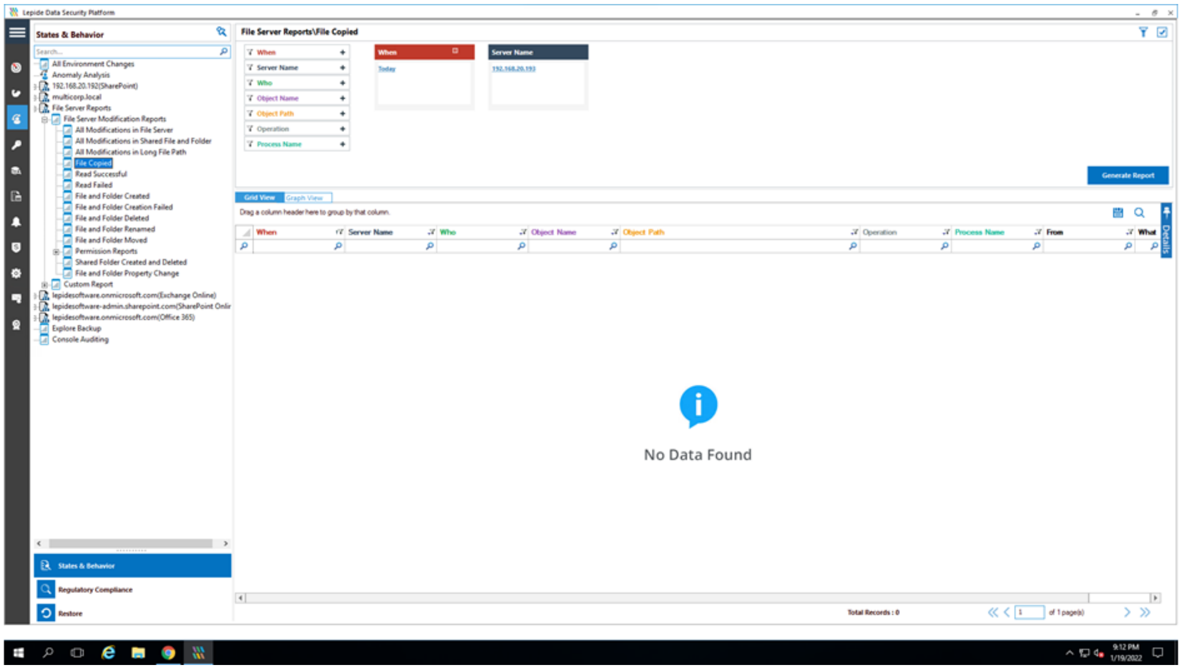
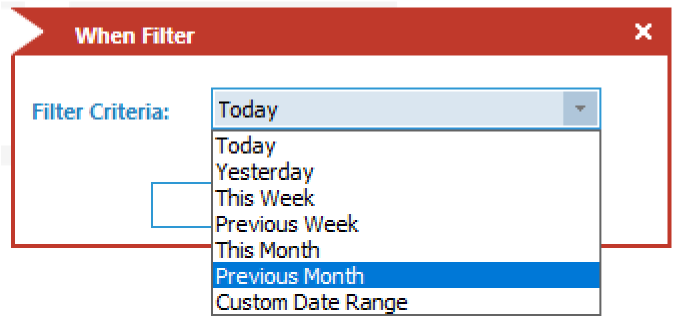


*Figure 2: File Copied Report*

## 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:



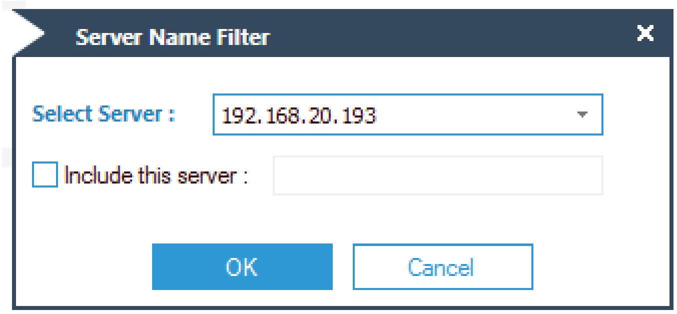
Filter Criteria: Today

*Figure 3: Date Range Filter*

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

## Specify a File Server

- From the top of the screen under **File Server**, click to select the required file server:

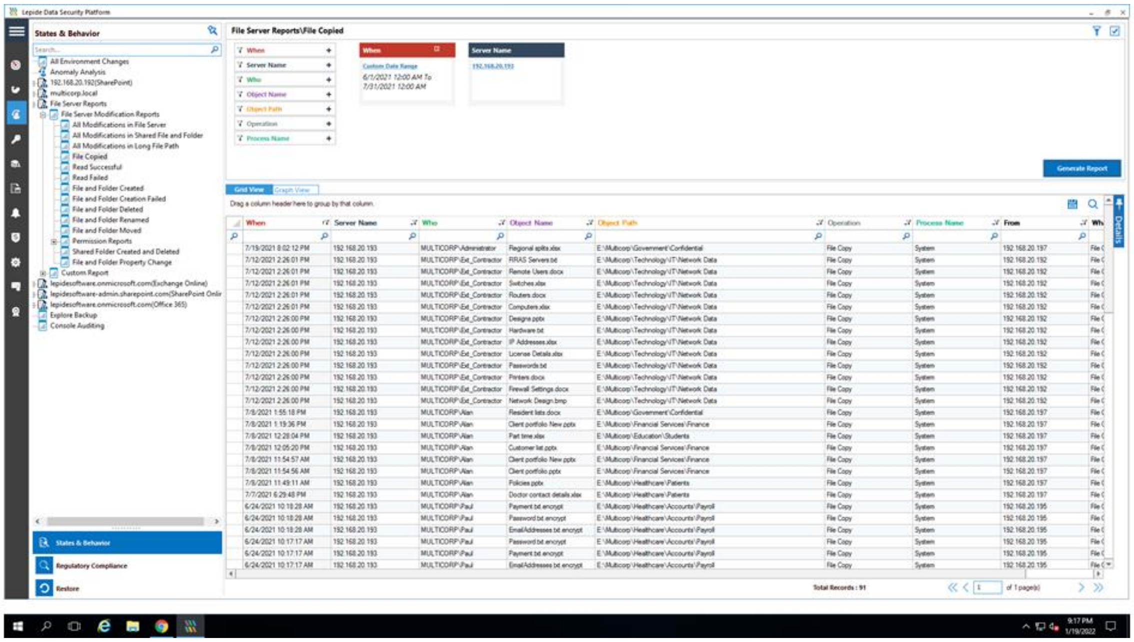


Select Server : 192.168.20.193

☐ Include this server :

*Figure 4: Server Name Filter*

- Click **OK**
- Click **Generate Report**


Lepide Data Security Platform
States & Behavior
Search...
All Environment Changes
Anomaly Analysis
192.168.20.192(SharePoint)
multicorp.local
File Server Reports
File Server Modification Reports
All Modifications in File Server
All Modifications in Shared File and Folder
All Modifications in Long File Path
File Copied
Read Successful
Read Failed
File and Folder Created
File and Folder Creation Failed
File and Folder Deleted
File and Folder Renamed
File and Folder Moved
Permission Reports
Shared Folder Created and Deleted
File and Folder Property Change
Custom Report
lepidesoftware.onmicrosoft.com(Exchange Online)
lepidesoftware-admin.sharepoint.com(SharePoint Onlir
lepidesoftware.onmicrosoft.com(Office 365)
Explore Backup
Console Auditing
States & Behavior
Regulatory Compliance
Restore
File Server Reports\File Copied
When
Server Name
Who
Object Name
Object Path
Operation
Process Name
Generate Report
Grid View
Graph View
Details
9:17 PM
1/19/2022

When: Custom Date Range 6/1/2021 12:00 AM To 7/31/2021 12:00 AM

Server Name: 192.168.20.193

Drag a column header here to group by that column.

| When | Server Name | Who | Object Name | Object Path | Operation | Process Name | From | Wh |
|---|---|---|---|---|---|---|---|---|
| 7/19/2021 8:02:12 PM | 192.168.20.193 | MULTICORP\Administrator | Regional splits.xlsx | E:\Multicorp\Government\Confidential | File Copy | System | 192.168.20.197 | File C |
| 7/12/2021 2:26:01 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | RRAS Servers.txt | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:01 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Remote Users.docx | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:01 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Switches.xlsx | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:01 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Routers.docx | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:01 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Computers.xlsx | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:00 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Designs.pptx | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:00 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Hardware.txt | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:00 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | IP Addresses.xlsx | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:00 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | License Details.xlsx | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:00 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Passwords.txt | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:00 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Printers.docx | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:00 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Firewall Settings.docx | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/12/2021 2:26:00 PM | 192.168.20.193 | MULTICORP\Ext_Contractor | Network Design.bmp | E:\Multicorp\Technology\IT\Network Data | File Copy | System | 192.168.20.192 | File C |
| 7/8/2021 1:55:18 PM | 192.168.20.193 | MULTICORP\Alan | Resident lists.docx | E:\Multicorp\Government\Confidential | File Copy | System | 192.168.20.197 | File C |
| 7/8/2021 1:19:36 PM | 192.168.20.193 | MULTICORP\Alan | Client portfolio New.pptx | E:\Multicorp\Financial Services\Finance | File Copy | System | 192.168.20.197 | File C |
| 7/8/2021 12:28:04 PM | 192.168.20.193 | MULTICORP\Alan | Part time.xlsx | E:\Multicorp\Education\Students | File Copy | System | 192.168.20.197 | File C |
| 7/8/2021 12:05:20 PM | 192.168.20.193 | MULTICORP\Alan | Customer list.pptx | E:\Multicorp\Financial Services\Finance | File Copy | System | 192.168.20.197 | File C |
| 7/8/2021 11:54:57 AM | 192.168.20.193 | MULTICORP\Alan | Client portfolio New.pptx | E:\Multicorp\Financial Services\Finance | File Copy | System | 192.168.20.197 | File C |
| 7/8/2021 11:54:56 AM | 192.168.20.193 | MULTICORP\Alan | Client portfolio.pptx | E:\Multicorp\Financial Services\Finance | File Copy | System | 192.168.20.197 | File C |
| 7/8/2021 11:49:11 AM | 192.168.20.193 | MULTICORP\Alan | Policies.pptx | E:\Multicorp\Healthcare\Patients | File Copy | System | 192.168.20.197 | File C |
| 7/7/2021 6:29:48 PM | 192.168.20.193 | MULTICORP\Alan | Doctor contact details.xlsx | E:\Multicorp\Healthcare\Patients | File Copy | System | 192.168.20.197 | File C |
| 6/24/2021 10:18:28 AM | 192.168.20.193 | MULTICORP\Paul | Payment.txt.encrypt | E:\Multicorp\Healthcare\Accounts\Payroll | File Copy | System | 192.168.20.195 | File C |
| 6/24/2021 10:18:28 AM | 192.168.20.193 | MULTICORP\Paul | Password.txt.encrypt | E:\Multicorp\Healthcare\Accounts\Payroll | File Copy | System | 192.168.20.195 | File C |
| 6/24/2021 10:18:28 AM | 192.168.20.193 | MULTICORP\Paul | EmailAddresses.txt.encrypt | E:\Multicorp\Healthcare\Accounts\Payroll | File Copy | System | 192.168.20.195 | File C |
| 6/24/2021 10:17:17 AM | 192.168.20.193 | MULTICORP\Paul | Password.txt.encrypt | E:\Multicorp\Healthcare\Accounts\Payroll | File Copy | System | 192.168.20.195 | File C |
| 6/24/2021 10:17:17 AM | 192.168.20.193 | MULTICORP\Paul | Payment.txt.encrypt | E:\Multicorp\Healthcare\Accounts\Payroll | File Copy | System | 192.168.20.195 | File C |
| 6/24/2021 10:17:17 AM | 192.168.20.193 | MULTICORP\Paul | EmailAddresses.txt.encrypt | E:\Multicorp\Healthcare\Accounts\Payroll | File Copy | System | 192.168.20.195 | File C |

Total Records : 91

1 of 1 page(s)

*Figure 5: The Generated File Copy Report*

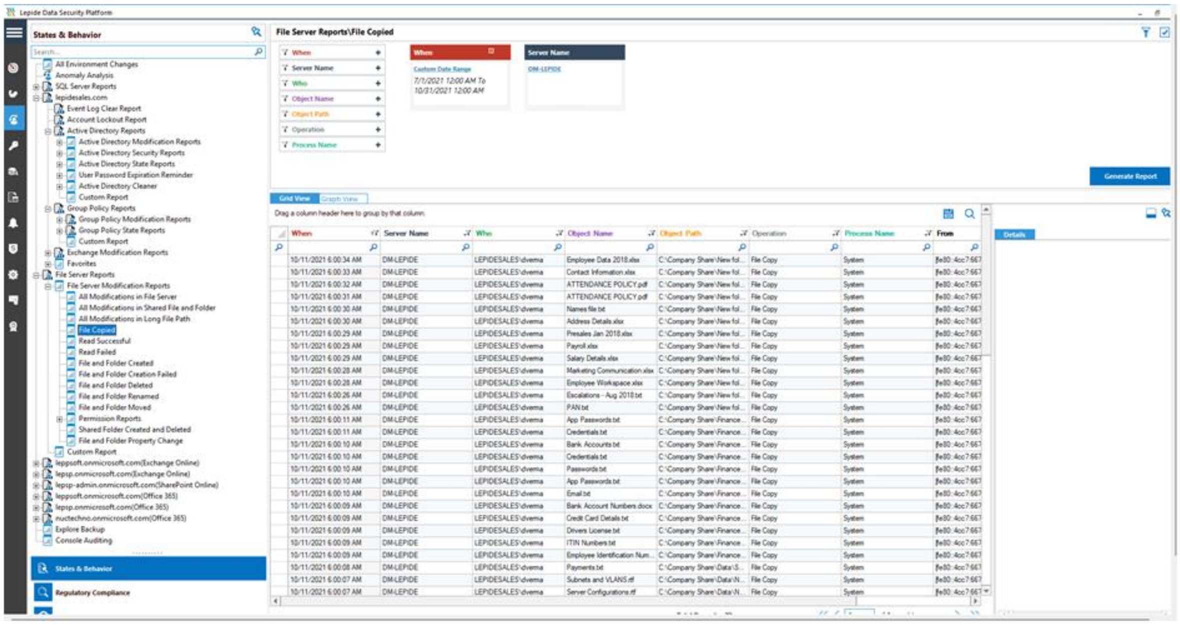
The report runs and shows information including who copied the file, what was copied and the location of the file.

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 File Copied report is used as an example.

From the States & Behavior screen:



File Server Reports\File Copied

When: Custom Date Range 7/1/2021 12:00 AM To 10/31/2021 12:00 AM

Server Name: DM-LEPIDE

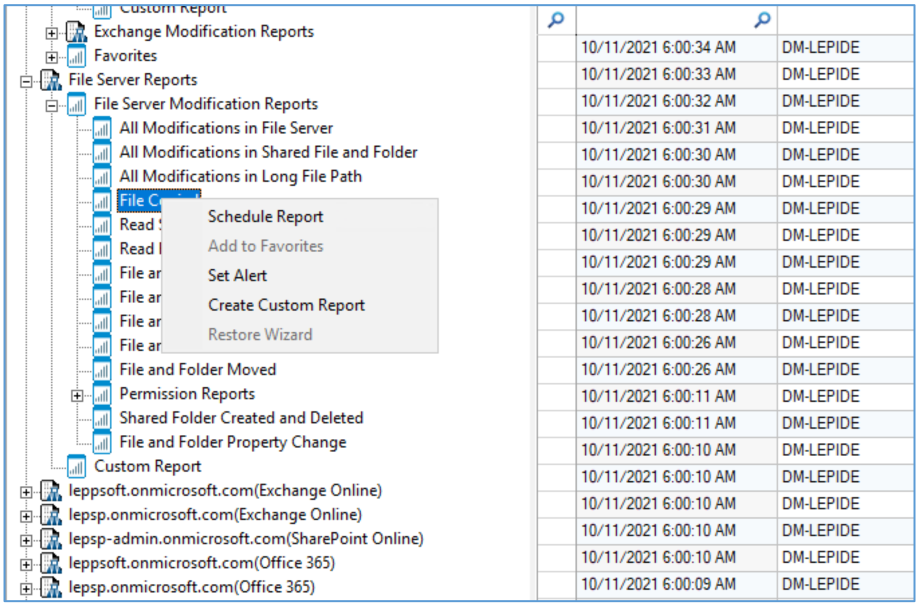
Drag a column header here to group by that column.

| When | Server Name | Who | Object Name | Object Path | Operation | Process Name | From |
|---|---|---|---|---|---|---|---|
| 10/11/2021 6:00:34 AM | DM-LEPIDE | LEPIDESALES\dverma | Employee Data 2018.xlsx | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:33 AM | DM-LEPIDE | LEPIDESALES\dverma | Contact Information.xlsx | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:32 AM | DM-LEPIDE | LEPIDESALES\dverma | ATTENDANCE POLICY.pdf | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:31 AM | DM-LEPIDE | LEPIDESALES\dverma | ATTENDANCE POLICY.pdf | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:30 AM | DM-LEPIDE | LEPIDESALES\dverma | Names file.txt | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:30 AM | DM-LEPIDE | LEPIDESALES\dverma | Address Details.xlsx | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:29 AM | DM-LEPIDE | LEPIDESALES\dverma | Presales Jan 2018.xlsx | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:29 AM | DM-LEPIDE | LEPIDESALES\dverma | Payroll.xlsx | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:29 AM | DM-LEPIDE | LEPIDESALES\dverma | Salary Details.xlsx | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:28 AM | DM-LEPIDE | LEPIDESALES\dverma | Marketing Communication.xlsx | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:28 AM | DM-LEPIDE | LEPIDESALES\dverma | Employee Workspace.xlsx | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:26 AM | DM-LEPIDE | LEPIDESALES\dverma | Escalations - Aug 2018.txt | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:26 AM | DM-LEPIDE | LEPIDESALES\dverma | PAN.txt | C:\Company Share\New fol... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:11 AM | DM-LEPIDE | LEPIDESALES\dverma | App Passwords.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:11 AM | DM-LEPIDE | LEPIDESALES\dverma | Credentials.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:10 AM | DM-LEPIDE | LEPIDESALES\dverma | Bank Accounts.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:10 AM | DM-LEPIDE | LEPIDESALES\dverma | Credentials.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:10 AM | DM-LEPIDE | LEPIDESALES\dverma | Passwords.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:10 AM | DM-LEPIDE | LEPIDESALES\dverma | App Passwords.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:10 AM | DM-LEPIDE | LEPIDESALES\dverma | Email.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:09 AM | DM-LEPIDE | LEPIDESALES\dverma | Bank Account Numbers.docx | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:09 AM | DM-LEPIDE | LEPIDESALES\dverma | Credit Card Details.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:09 AM | DM-LEPIDE | LEPIDESALES\dverma | Drivers License.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:09 AM | DM-LEPIDE | LEPIDESALES\dverma | ITIN Numbers.txt | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:09 AM | DM-LEPIDE | LEPIDESALES\dverma | Employee Identification Num... | C:\Company Share\Finance... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:08 AM | DM-LEPIDE | LEPIDESALES\dverma | Payments.txt | C:\Company Share\Data\S... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:07 AM | DM-LEPIDE | LEPIDESALES\dverma | Subnets and VLANS.rtf | C:\Company Share\Data\N... | File Copy | System | fe80::4cc7:667 |
| 10/11/2021 6:00:07 AM | DM-LEPIDE | LEPIDESALES\dverma | Server Configurations.rtf | C:\Company Share\Data\N... | File Copy | System | fe80::4cc7:667 |

*Figure 6: States & Behavior Screen*

- **Right click** on the **File Copied** report.

  A menu is displayed:

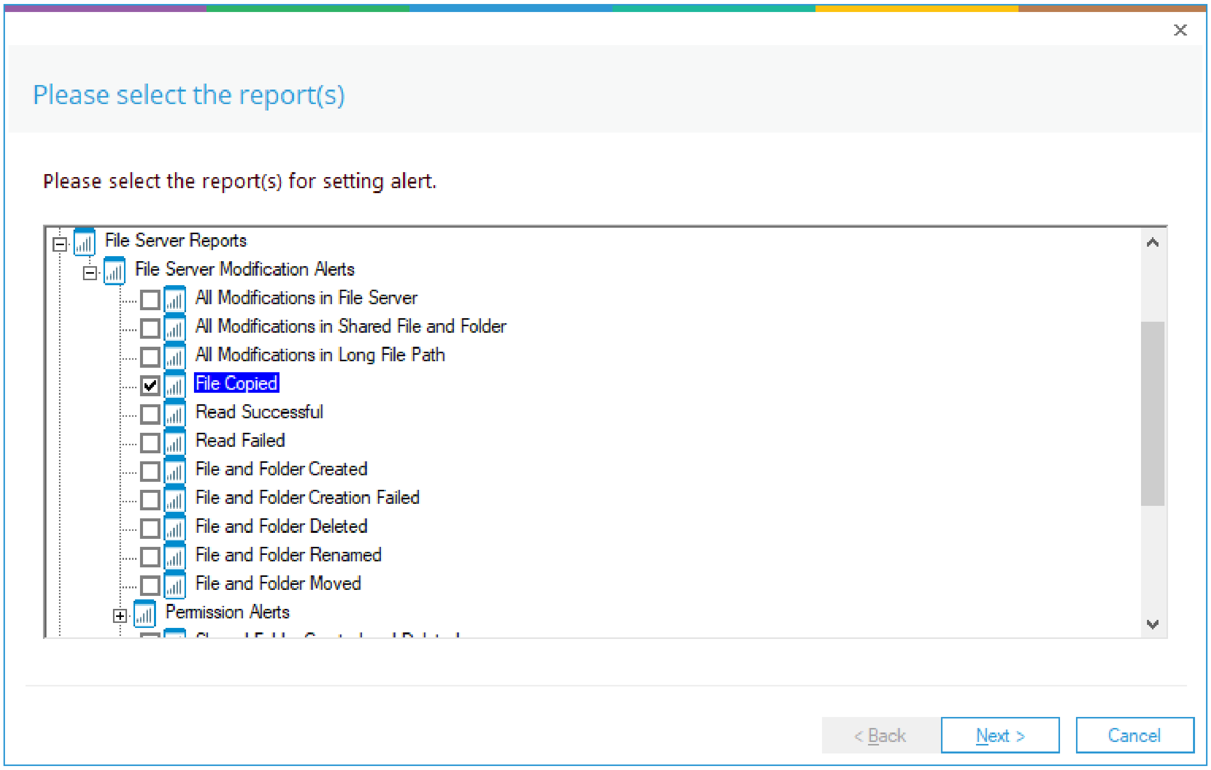

Custom Report
Exchange Modification Reports
Favorites
File Server Reports
File Server Modification Reports
All Modifications in File Server
All Modifications in Shared File and Folder
All Modifications in Long File Path
File C
Read S
Read I
File ar
File ar
File ar
File ar
File and Folder Moved
Permission Reports
Shared Folder Created and Deleted
File and Folder Property Change
Custom Report
leppsoft.onmicrosoft.com(Exchange Online)
lepsp.onmicrosoft.com(Exchange Online)
lepsp-admin.onmicrosoft.com(SharePoint Online)
leppsoft.onmicrosoft.com(Office 365)
lepsp.onmicrosoft.com(Office 365)
Schedule Report
Add to Favorites
Set Alert
Create Custom Report
Restore Wizard

| | |
|---|---|
| 10/11/2021 6:00:34 AM | DM-LEPIDE |
| 10/11/2021 6:00:33 AM | DM-LEPIDE |
| 10/11/2021 6:00:32 AM | DM-LEPIDE |
| 10/11/2021 6:00:31 AM | DM-LEPIDE |
| 10/11/2021 6:00:30 AM | DM-LEPIDE |
| 10/11/2021 6:00:30 AM | DM-LEPIDE |
| 10/11/2021 6:00:29 AM | DM-LEPIDE |
| 10/11/2021 6:00:29 AM | DM-LEPIDE |
| 10/11/2021 6:00:29 AM | DM-LEPIDE |
| 10/11/2021 6:00:28 AM | DM-LEPIDE |
| 10/11/2021 6:00:28 AM | DM-LEPIDE |
| 10/11/2021 6:00:26 AM | DM-LEPIDE |
| 10/11/2021 6:00:26 AM | DM-LEPIDE |
| 10/11/2021 6:00:11 AM | DM-LEPIDE |
| 10/11/2021 6:00:11 AM | DM-LEPIDE |
| 10/11/2021 6:00:10 AM | DM-LEPIDE |
| 10/11/2021 6:00:10 AM | DM-LEPIDE |
| 10/11/2021 6:00:10 AM | DM-LEPIDE |
| 10/11/2021 6:00:10 AM | DM-LEPIDE |
| 10/11/2021 6:00:10 AM | DM-LEPIDE |
| 10/11/2021 6:00:09 AM | DM-LEPIDE |

*Figure 7: Report Menu*

- 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.

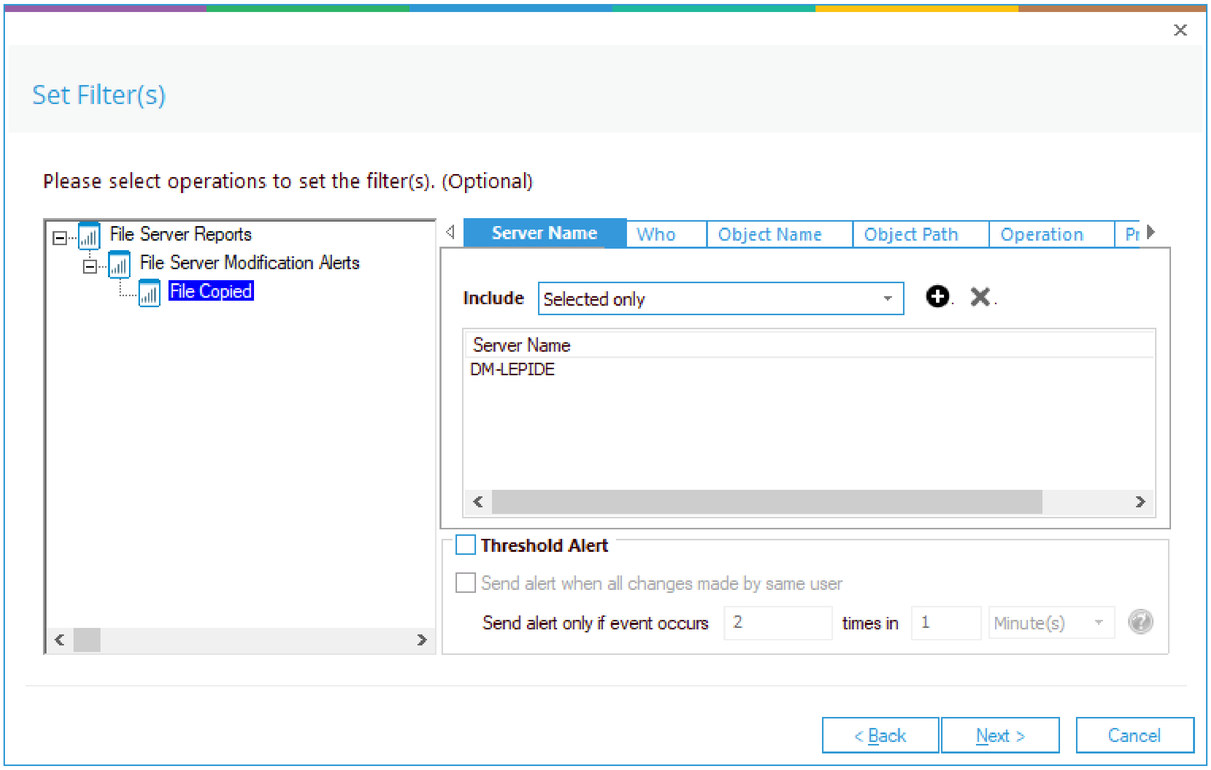
- File Server Reports
  - File Server Modification Alerts
    - □ All Modifications in File Server
    - □ All Modifications in Shared File and Folder
    - □ All Modifications in Long File Path
    - ☑ File Copied
    - □ Read Successful
    - □ Read Failed
    - □ File and Folder Created
    - □ File and Folder Creation Failed
    - □ File and Folder Deleted
    - □ File and Folder Renamed
    - □ File and Folder Moved
  - Permission Alerts

*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 File Copied report.

- Click Next

The Set Filter(s) dialog box is displayed:



Set Filter(s)

Please select operations to set the filter(s). (Optional)

Include: Selected only

| Server Name |
|---|
| DM-LEPIDE |

□ Threshold Alert

□ Send alert when all changes made by same user

Send alert only if event occurs 2 times in 1 Minute(s)

*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 File Copied.

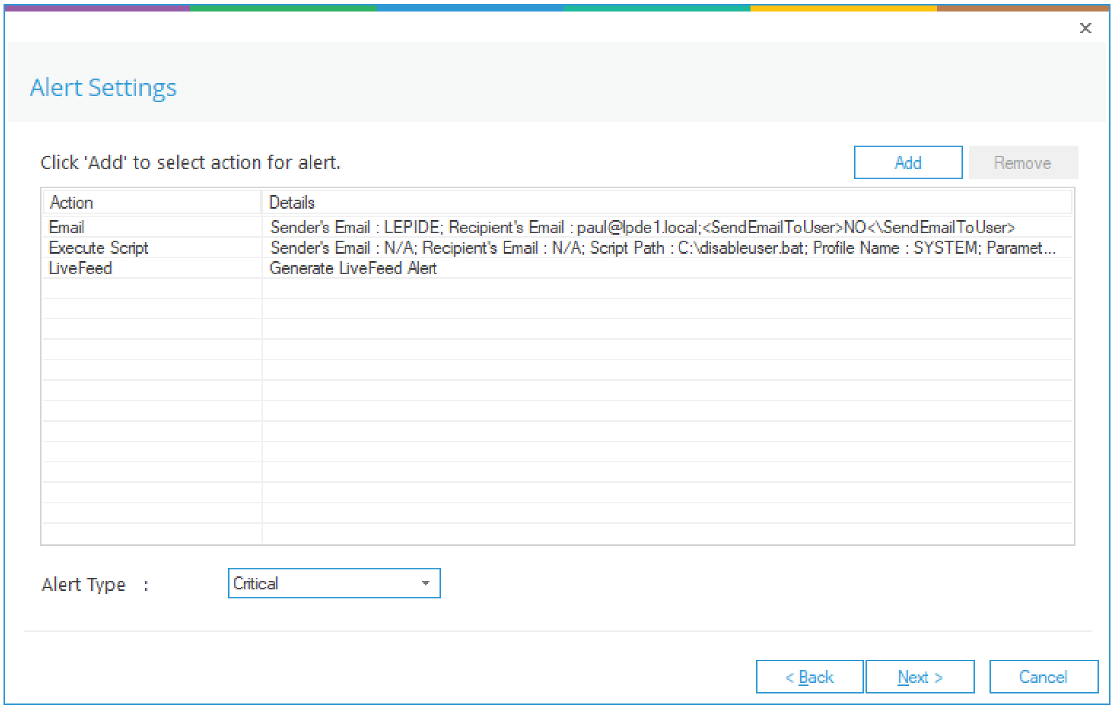
There are options to change the settings for Server, User, Object Name, Object Path, Operation, Process and From using the tabs at the top of this dialog box. The default setting for all these options is All.

The threshold alert options can be customized as follows:

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

- Click Next

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



Alert Settings

Click 'Add' to select action for alert.

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

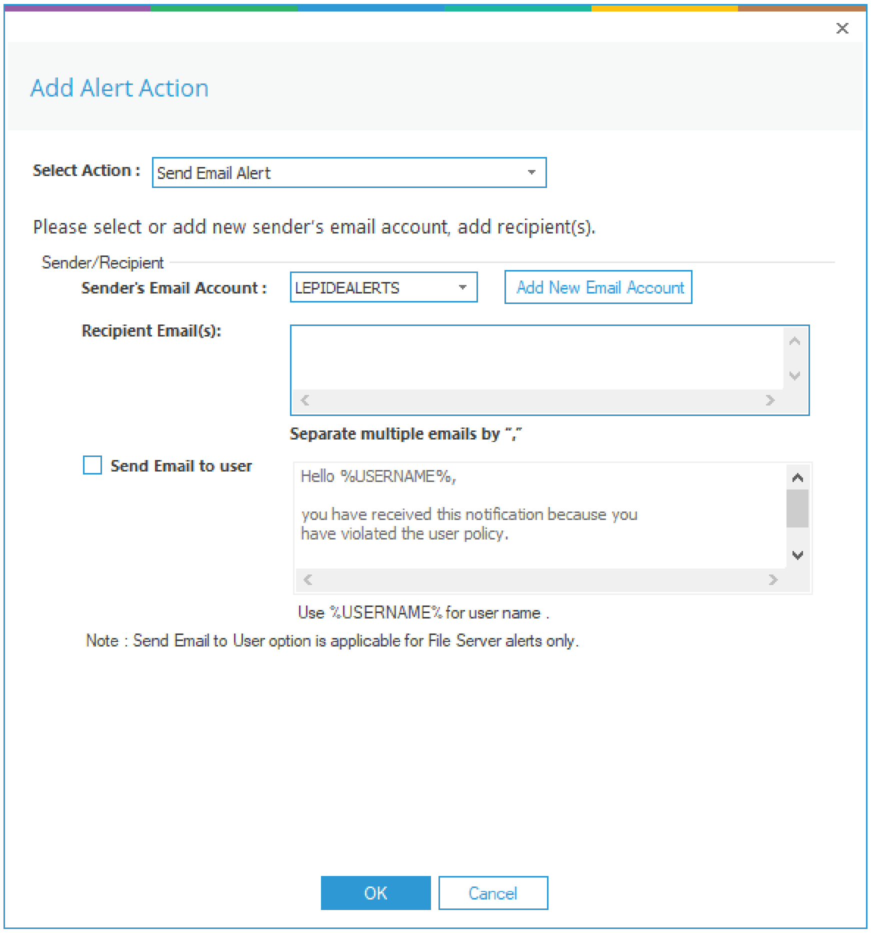
Alert Type : Critical

*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 will be displayed:



Add Alert Action

Select Action : Send Email Alert

Please select or add new sender's email account, add recipient(s).

Sender/Recipient

Sender's Email Account : LEPIDEALERTS

Recipient Email(s):

Separate multiple emails by ","

□ Send Email to user

Hello %USERNAME%,

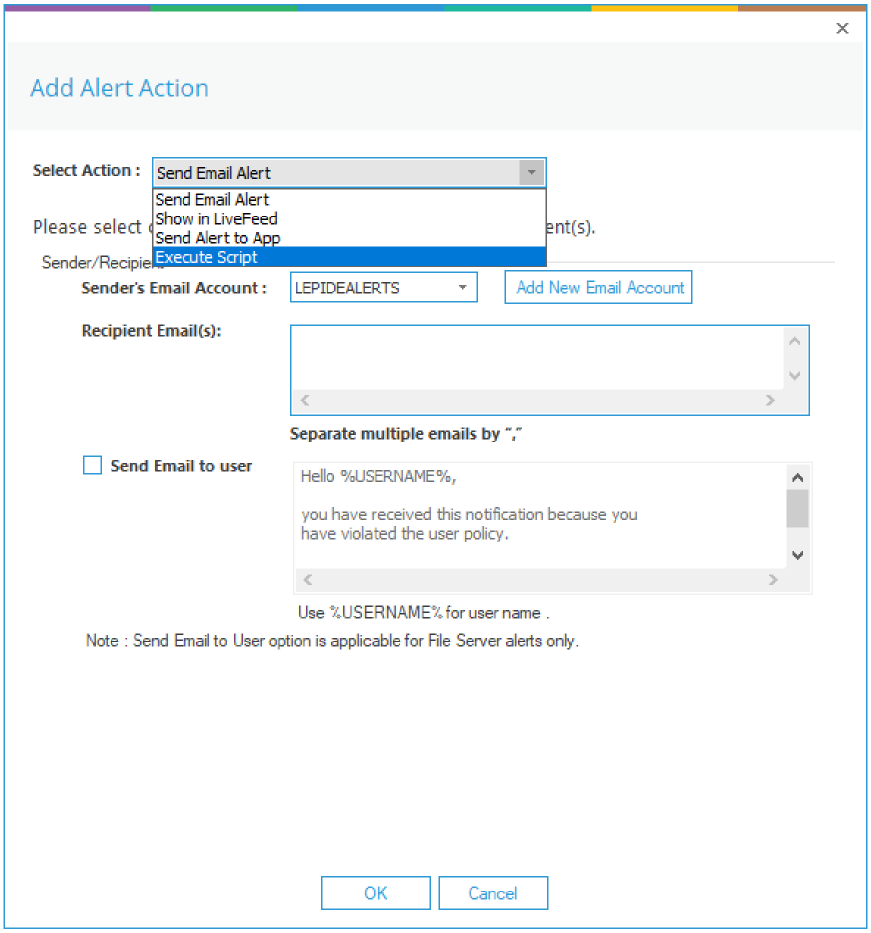
you have received this notification because you have violated the user policy.

Use %USERNAME% for user name .

Note : Send Email to User option is applicable for File Server alerts only.

*Figure 11: Add Alert Action*

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



Add Alert Action

Select Action : Send Email Alert

Please select ... ent(s).

Sender/Recipient

Sender's Email Account : LEPIDEALERTS

Recipient Email(s):

Separate multiple emails by ","

□ Send Email to user

Hello %USERNAME%,

you have received this notification because you have violated the user policy.

Use %USERNAME% for user name .

Note : Send Email to User option is applicable for File Server alerts only.

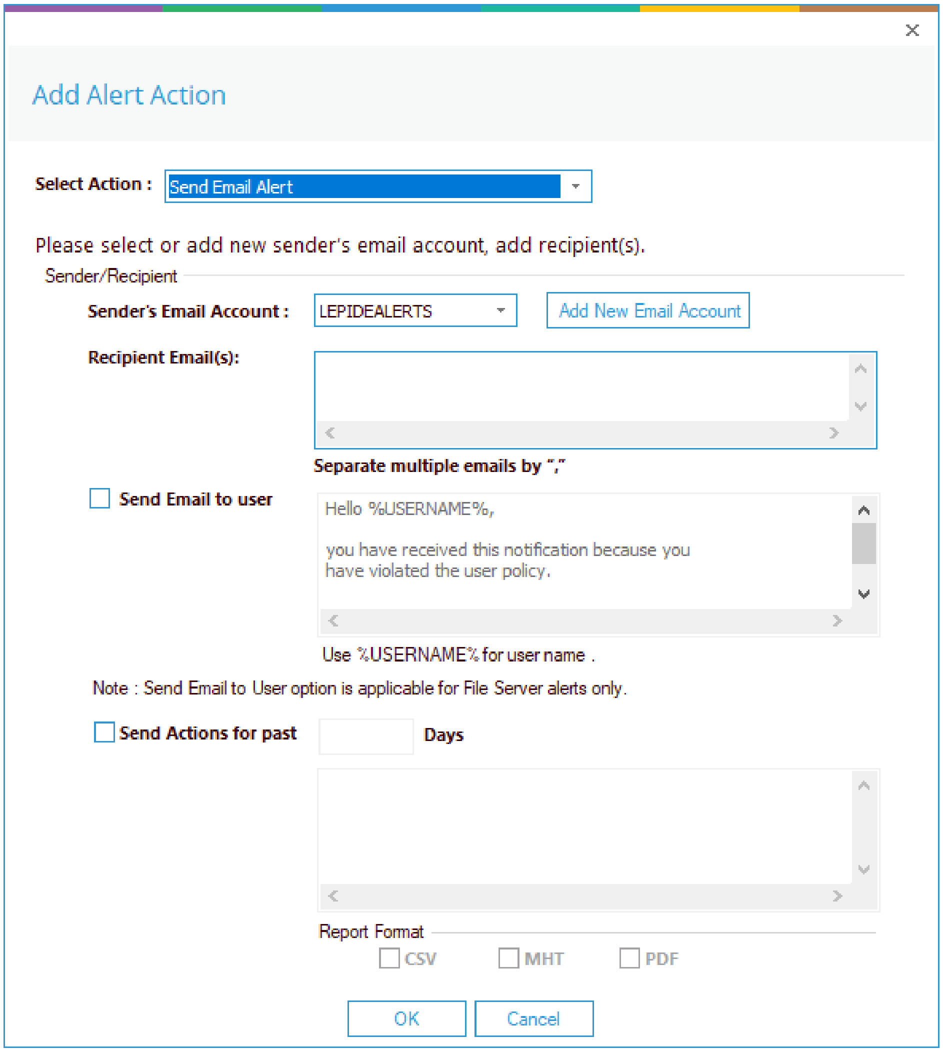
*Figure 12: Add Alert Action Options*

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 sender's email account, add recipient(s).

Sender/Recipient

Sender's Email Account : LEPIDEALERTS

Recipient Email(s):

Separate multiple emails by ","

□ Send Email to user

Hello %USERNAME%,

you have received this notification because you have violated the user policy.

Use %USERNAME% for user name .

Note : Send Email to User option is applicable for File Server alerts only.

□ Send Actions for past Days

Report Format

□ CSV □ MHT □ PDF

*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 ','

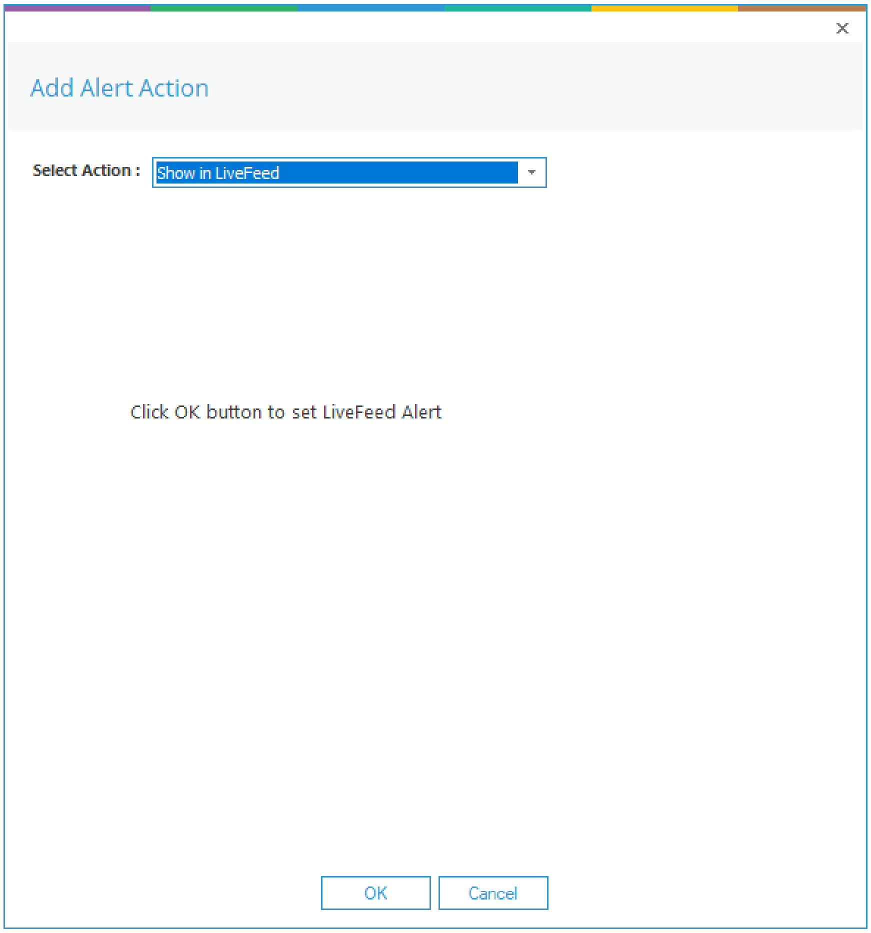
Send Email to user: Check this box to send an email to the user. The content of the email can be typed into the text box. To include the username within the content, use the variable %USERNAME%. Note that this option is only applicable to File Server alerts.

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.

2. Show in LiveFeed



Add Alert Action

Select Action : Show in LiveFeed

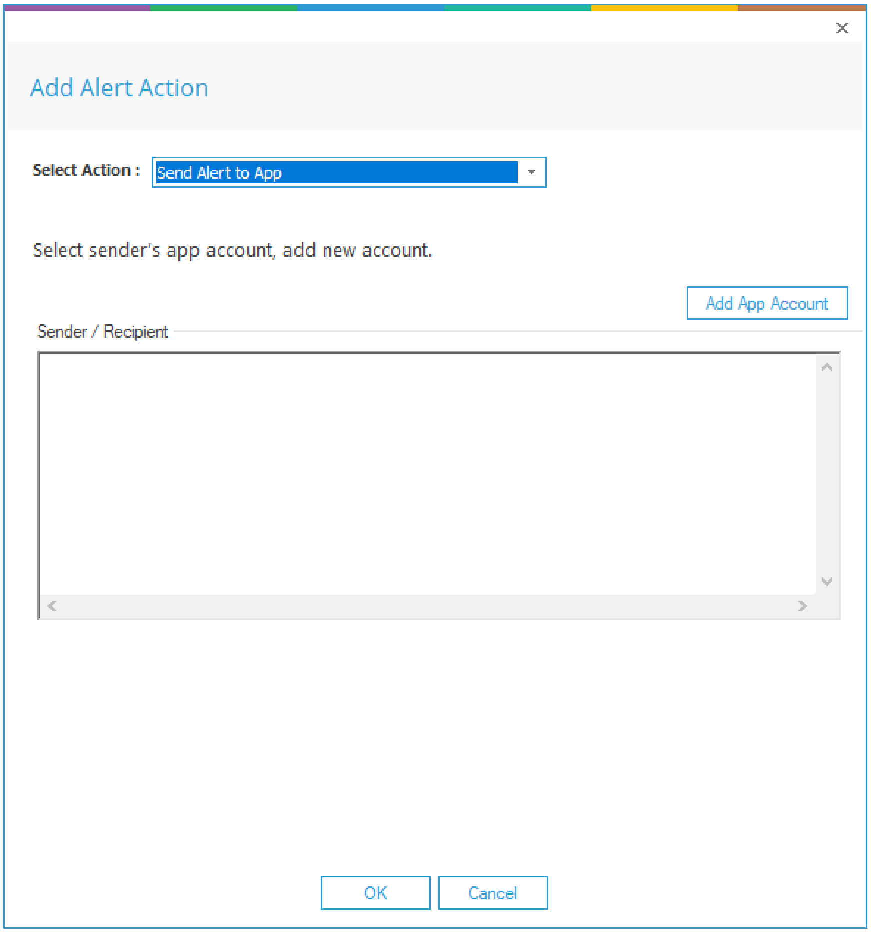
Click OK button to set LiveFeed Alert

*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

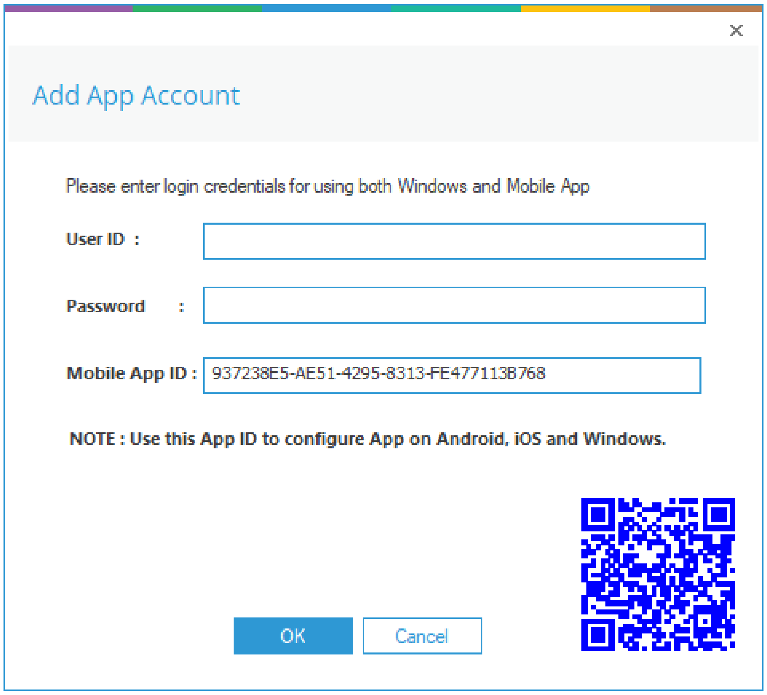
Select Action : Send Alert to App

Select sender's app account, add new account.

*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 :

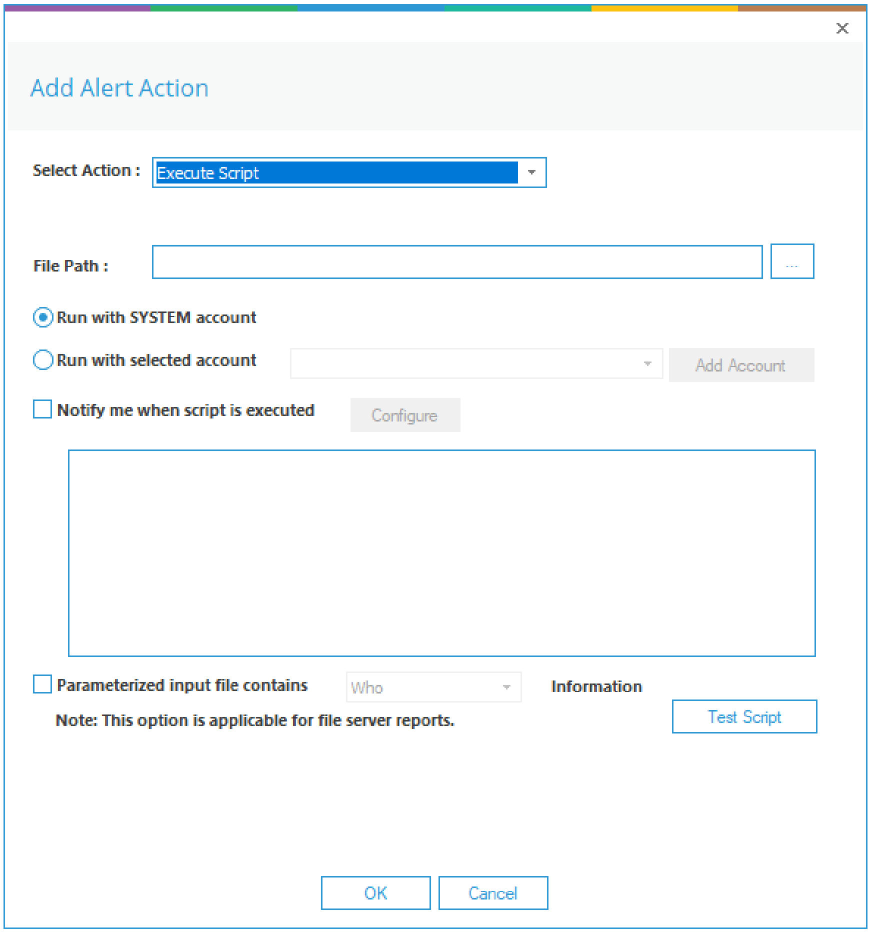
Mobile App ID : 937238E5-AE51-4295-8313-FE477113B768

NOTE : Use this App ID to configure App on Android, iOS and Windows.

*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

○ Run with selected account

□ Notify me when script is executed

□ Parameterized input file contains Who Information

Note: This option is applicable for file server reports.

*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:

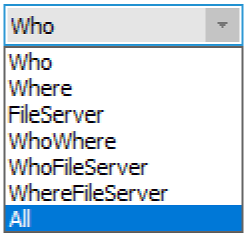
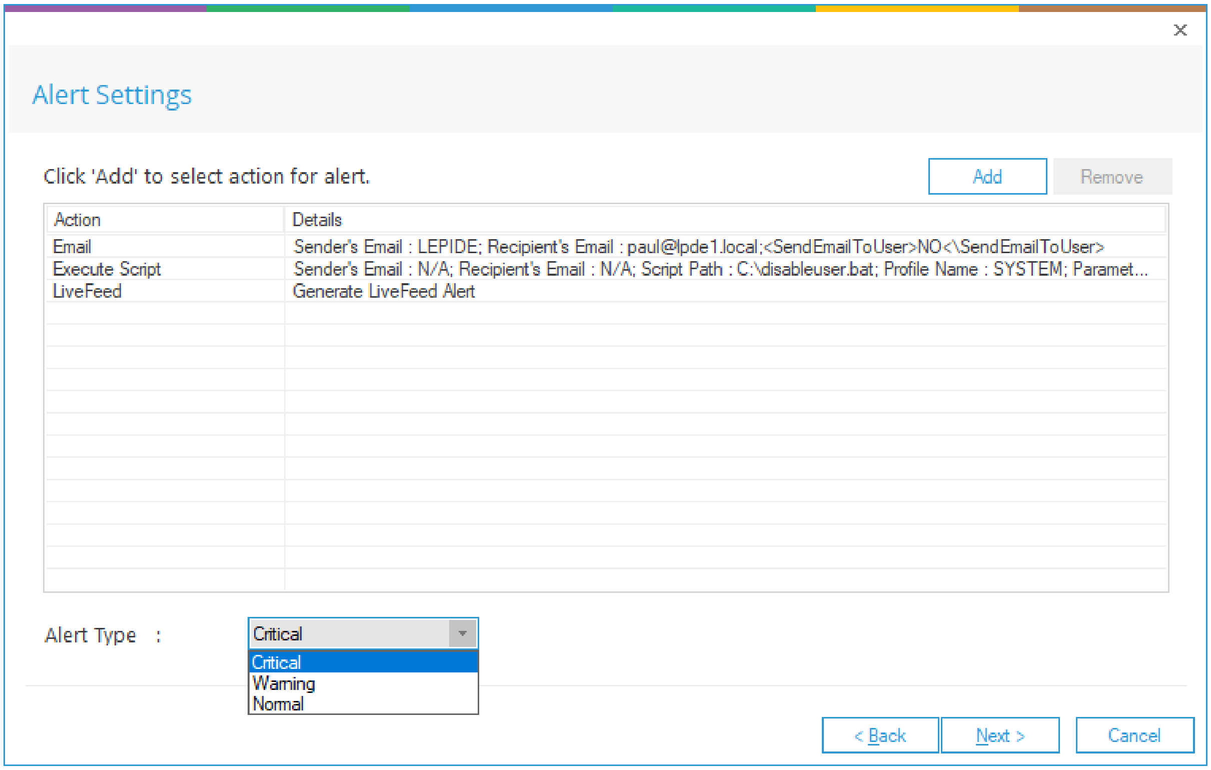


*Figure 18: List of Variables*

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



Alert Settings

Click 'Add' to select action for alert.

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

Alert Type : Critical

*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. Threat Models

Another way to configure an alert is to enable one of the many 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 pre-defined threat models.

To see all the threat models available within the Lepide Data Security Platform, click the Alerts icon and the following screen will be displayed:

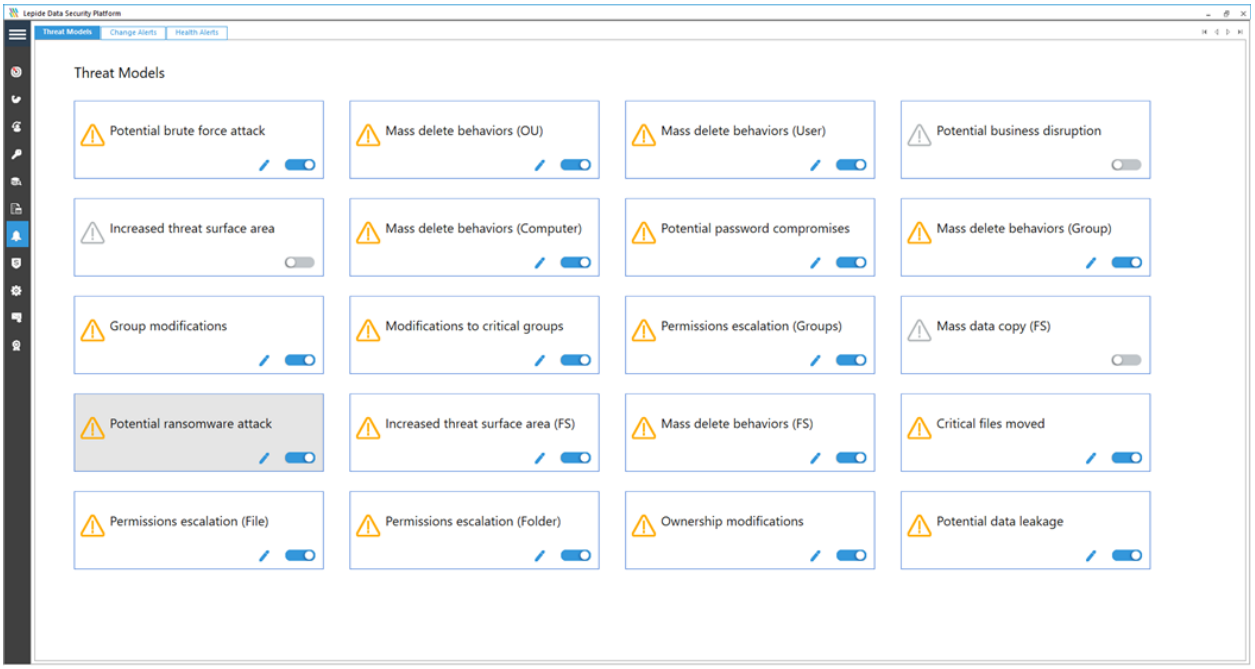
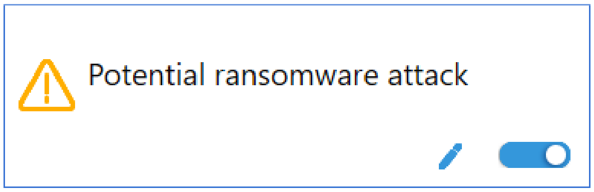

Lepide Data Security Platform
Threat Models
Change Alerts
Health Alerts
Threat Models
Potential brute force attack
Mass delete behaviors (OU)
Mass delete behaviors (User)
Potential business disruption
Increased threat surface area
Mass delete behaviors (Computer)
Potential password compromises
Mass delete behaviors (Group)
Group modifications
Modifications to critical groups
Permissions escalation (Groups)
Mass data copy (FS)
Potential ransomware attack
Increased threat surface area (FS)
Mass delete behaviors (FS)
Critical files moved
Permissions escalation (File)
Permissions escalation (Folder)
Ownership modifications
Potential data leakage

*Figure 20: 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

- Click the **Alerts** icon 🔔 from the left-hand toolbar to display all the Threat Models available.
- To enable the **Potential Ransomware Attack Threat Model,** move the slide toggle to the right.

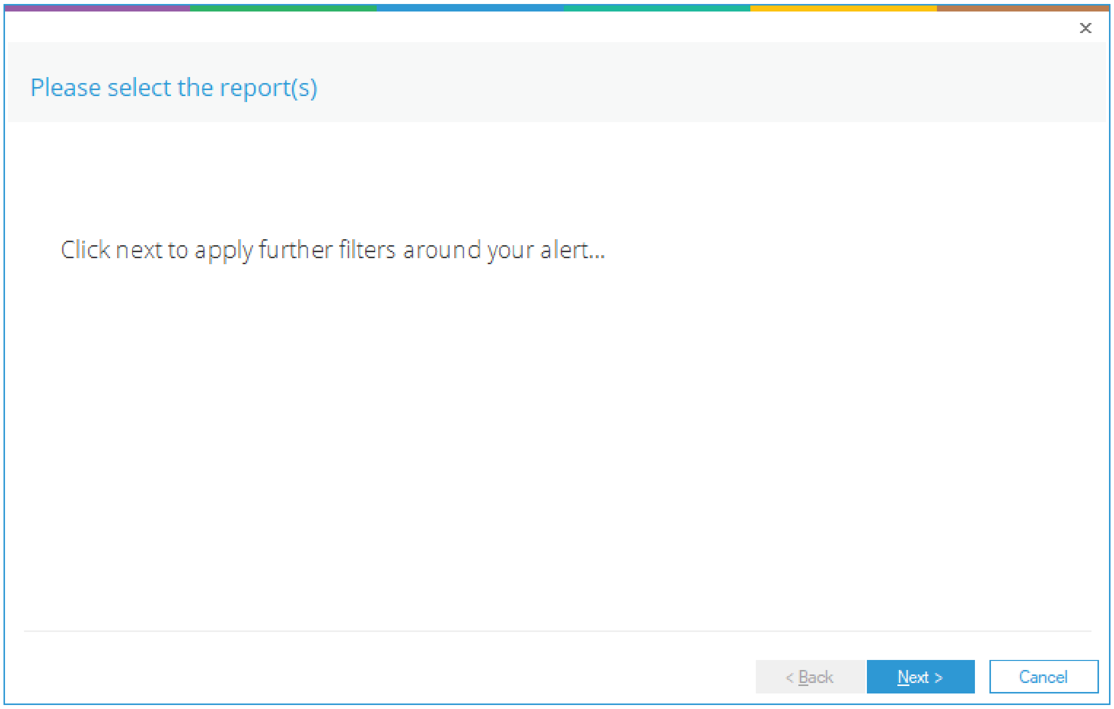


Potential ransomware attack

*Figure 21:Enable the Potential Ransomware Attack Threat Model*

- Click the ✏ icon to configure the alerts and responses you require.

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

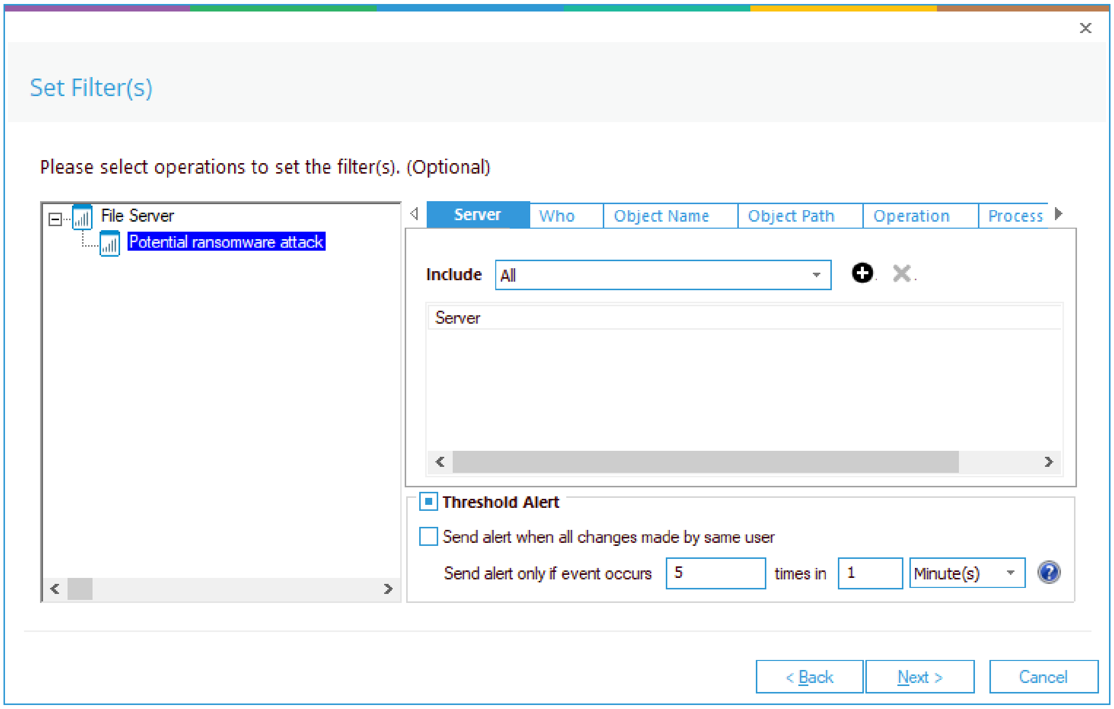


Please select the report(s)

Click next to apply further filters around your alert...

*Figure 22: Wizard to Configure Threat Models*

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



Set Filter(s)

Please select operations to set the filter(s). (Optional)

Include: All

☑ Threshold Alert

☐ Send alert when all changes made by same user

Send alert only if event occurs 5 times in 1 Minute(s)

*Figure 23: Set Filters for the Threat Model*

The Set Filter(s) dialog box enables you to set up an alert.

On the left of the dialog box, you can see the Threat Model you are working on which is Potential ransomware attack.

There are options to change the settings for Server, User, Object Name, Object Path, Operation, Process and From using the tabs at the top of this dialog box. 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 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: | Change the number of times the event occurs, the time value and time-period here |

- Click Next

The Alert Settings dialog box is displayed.

- Follow the instructions given previously on page 11 to continue working through the Wizard and complete the configuration of the Threat Model.

# 5. To Modify an Alert

- Click the 🔔 icon to display the Threat Models screen
- Click on the Tab at the top of the screen called Change Alerts.
- The center left of this screen has a section called Manage Alerts. Here the Alerts which have been set up are displayed in a list:

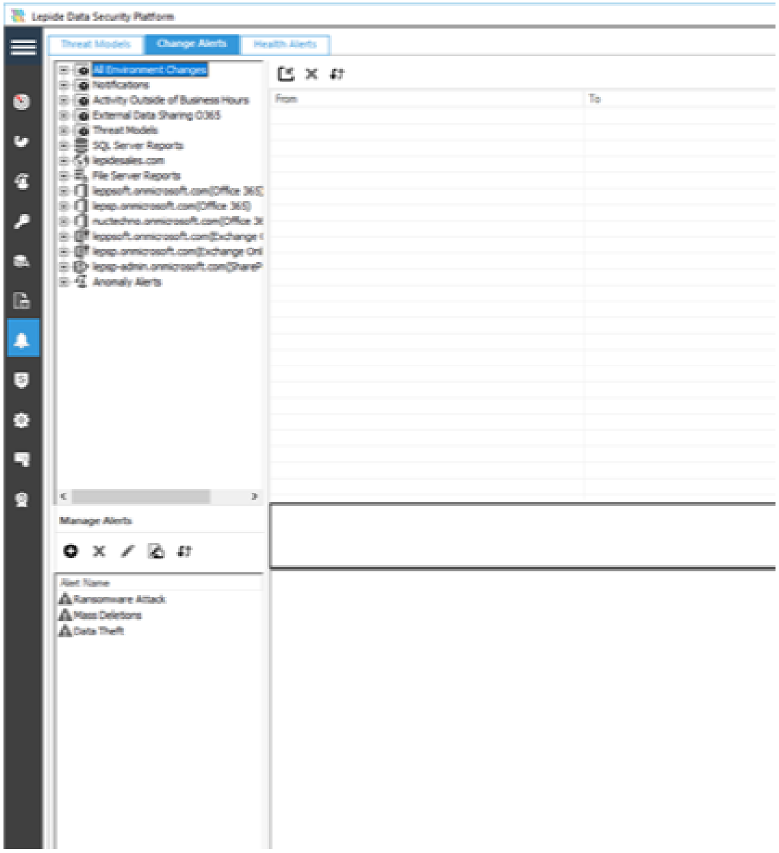
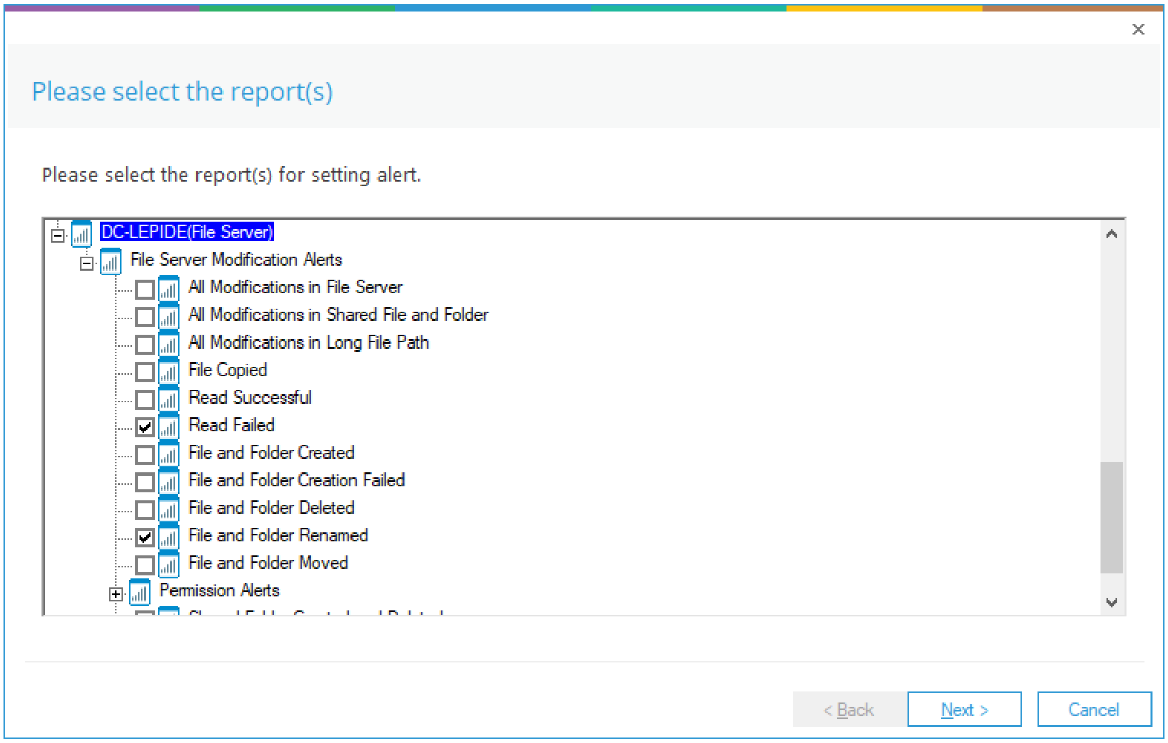

Lepide Data Security Platform
Threat Models
Change Alerts
Health Alerts
All Environment Changes
Notifications
Activity Outside of Business Hours
External Data Sharing O365
Threat Models
SQL Server Reports
lepidesales.com
File Server Reports
leppsoft.onmicrosoft.com(Office 365)
lepsp.onmicrosoft.com(Office 365)
nuctechno.onmicrosoft.com(Office 3
leppsoft.onmicrosoft.com(Exchange
lepsp.onmicrosoft.com(Exchange Onl
lepsp-admin.onmicrosoft.com(ShareP
Anomaly Alerts
From
To
Manage Alerts
Alert Name
Ransomware Attack
Mass Deletions
Data Theft

*Figure 24: Manage Alerts*

- Select the Alert you want to modify
- Click the 🔧 icon

The Alerts Wizard will start and display the Select Reports dialog box:



Please select the report(s)

Please select the report(s) for setting alert.

- DC-LEPIDE(File Server)
  - File Server Modification Alerts
    - ☐ All Modifications in File Server
    - ☐ All Modifications in Shared File and Folder
    - ☐ All Modifications in Long File Path
    - ☐ File Copied
    - ☐ Read Successful
    - ☑ Read Failed
    - ☐ File and Folder Created
    - ☐ File and Folder Creation Failed
    - ☐ File and Folder Deleted
    - ☑ File and Folder Renamed
    - ☐ File and Folder Moved
  - Permission Alerts

*Figure 25: Select Reports*

- Ensure that the report(s) on which you want to set an alert is checked
- Click Next

The Set Filter(s) dialog box is displayed.

- Follow the instructions given previously on page 10 to continue working through the Wizard making changes to the Alert as needed.

# 4. 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/.

# 5. Trademarks

Lepide Data Security Platform, 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.