Lepide

USE CASE GUIDE

HOW TO REPORT AND ALERT ON FILES BEING COPIED

Table of Contents

1. Introduction

Data breaches are a serious threat to any organization and so appropriate action must to be taken to keep the risk of these threats to a minimum. The focus at Lepide is to provide visibility over what's happening with your data and through visibility you can take the necessary steps to mitigate risk and stay compliant.

This guide is in two parts. The first explains the ways in which you can use Lepide Data Security Platform to reduce the chance of a data breach in the case of files being copied. The second section gives step-by-step instructions on how to configure the solution to meet your requirements.

2. Why Monitor the Copying of Files?

The ability to copy files is an essential requirement to many job roles within an organization.

However, when this functionality is misused and file copying activity is done for the wrong reasons, data security is compromised, and appropriate remedial action needs to be taken. To combat this ever-increasing insider threat of a data breach, it is essential to monitor all file activities, especially file copy actions, to spot malicious activity at the initial stages. While the constant monitoring of user behavior is achievable, it can be complex and time consuming without the right solution in place.

3. The Solution

The Lepide Data Security Platform provides a solution to this. It works in real time and allows you to view a summary of employee activity within a given timeframe to see which files have been copied.

It also provides the ability to set up real-time alerts so that immediate action can be taken. For example, if a certain number of files are copied in quick succession, this could indicate the start of a data breach. In this case, an alert would be triggered, and an immediate response implemented.

Once there is visibility is in place to warn of potential threats, action can be taken to reduce risk and remain compliant.

3.1. The File Copy Report

The summary of user file copy activity is provided using the File Copy Report. This report will show file copying activity within a given time scale and can be further filtered to focus on whatever data is required.

3.2. The Mass Data Copy Threat Model

This Threat Model can be activated and then customized to meet specific requirements. As well as providing an alert to suspicious activity, it can also be configured to respond to an event which could be, for example, to shut down a file server or revoke a user's permissions.

4. Configuring File Copy Reporting and Alerting

4.1. Prerequisites

Before reporting and alerting on files being copied, you will need to have added and configured Windows File Server to enable auditing.

Once this has been configured, you will immediately see all file copy events as the Lepide Data Security Platform provides alerting and reporting in real time.

4.2. Running 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**

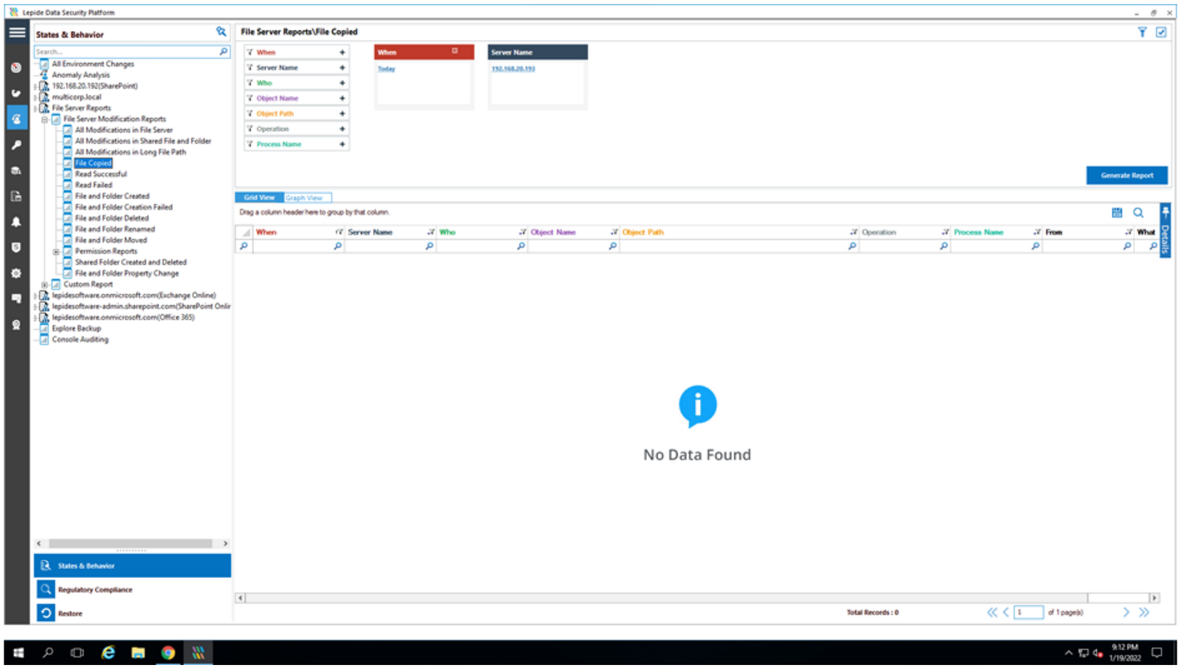
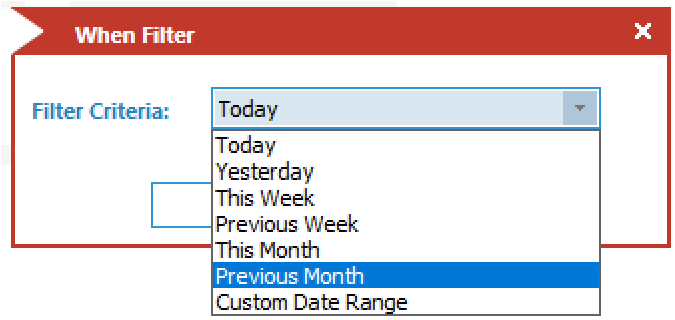


Figure 1: File Copied Report

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:



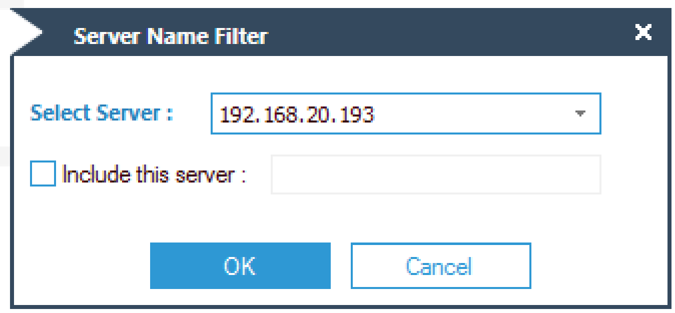
Filter Criteria: Today

Figure 2: 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:

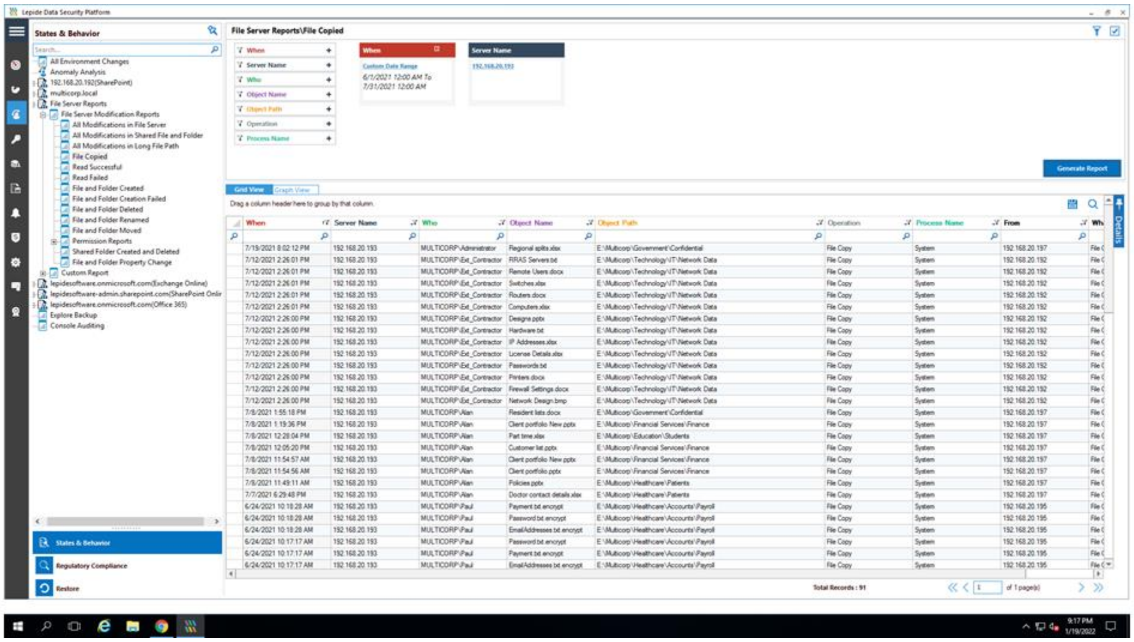


Select Server : 192.168.20.193

□ Include this server :

Figure 3: 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)

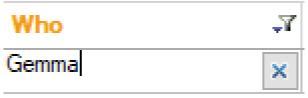
Figure 4: The Generated File Copy Report

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

Filtering the Report

To add filters to the data, click on the filter area above the relevant column and type in the information you want to see.

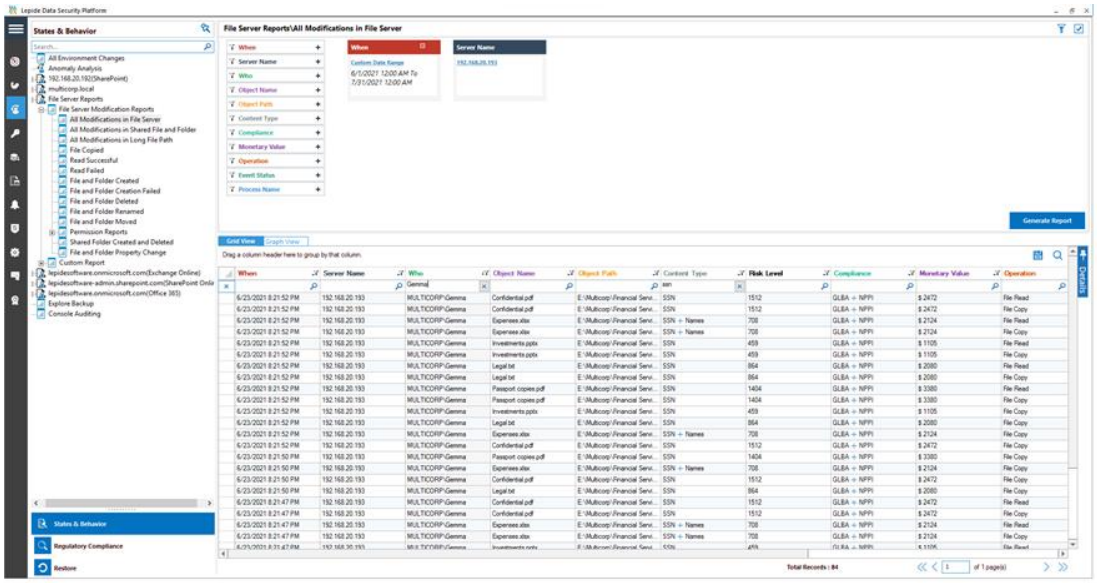
For example, you may want to see data for a particular user - so click at the top of the Who column and type in the username:



Gemma

Figure 5: Filter Area

In the example below, the report has been filtered to show both data for Gemma and where the content includes SSN (Social Security Numbers):



File Server Reports\All Modifications in File Server

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	Content Type	Risk Level	Compliance	Monetary Value	Operation
		Gemma			ssn				
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Confidential.pdf	E:\Multicorp\Financial Servi...	SSN	1512	GLBA + NPPI	$ 2472	File Read
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Confidential.pdf	E:\Multicorp\Financial Servi...	SSN	1512	GLBA + NPPI	$ 2472	File Copy
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Expenses.xlsx	E:\Multicorp\Financial Servi...	SSN + Names	708	GLBA + NPPI	$ 2124	File Read
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Expenses.xlsx	E:\Multicorp\Financial Servi...	SSN + Names	708	GLBA + NPPI	$ 2124	File Copy
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Investments.pptx	E:\Multicorp\Financial Servi...	SSN	459	GLBA + NPPI	$ 1105	File Read
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Investments.pptx	E:\Multicorp\Financial Servi...	SSN	459	GLBA + NPPI	$ 1105	File Copy
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Legal.txt	E:\Multicorp\Financial Servi...	SSN	864	GLBA + NPPI	$ 2080	File Read
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Legal.txt	E:\Multicorp\Financial Servi...	SSN	864	GLBA + NPPI	$ 2080	File Copy
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Passport copies.pdf	E:\Multicorp\Financial Servi...	SSN	1404	GLBA + NPPI	$ 3380	File Read
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Passport copies.pdf	E:\Multicorp\Financial Servi...	SSN	1404	GLBA + NPPI	$ 3380	File Copy
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Investments.pptx	E:\Multicorp\Financial Servi...	SSN	459	GLBA + NPPI	$ 1105	File Copy
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Legal.txt	E:\Multicorp\Financial Servi...	SSN	864	GLBA + NPPI	$ 2080	File Copy
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Expenses.xlsx	E:\Multicorp\Financial Servi...	SSN + Names	708	GLBA + NPPI	$ 2124	File Copy
6/23/2021 8:21:52 PM	192.168.20.193	MULTICORP\Gemma	Confidential.pdf	E:\Multicorp\Financial Servi...	SSN	1512	GLBA + NPPI	$ 2472	File Copy
6/23/2021 8:21:50 PM	192.168.20.193	MULTICORP\Gemma	Passport copies.pdf	E:\Multicorp\Financial Servi...	SSN	1404	GLBA + NPPI	$ 3380	File Copy
6/23/2021 8:21:50 PM	192.168.20.193	MULTICORP\Gemma	Expenses.xlsx	E:\Multicorp\Financial Servi...	SSN + Names	708	GLBA + NPPI	$ 2124	File Copy
6/23/2021 8:21:50 PM	192.168.20.193	MULTICORP\Gemma	Confidential.pdf	E:\Multicorp\Financial Servi...	SSN	1512	GLBA + NPPI	$ 2472	File Copy
6/23/2021 8:21:50 PM	192.168.20.193	MULTICORP\Gemma	Legal.txt	E:\Multicorp\Financial Servi...	SSN	864	GLBA + NPPI	$ 2080	File Copy
6/23/2021 8:21:47 PM	192.168.20.193	MULTICORP\Gemma	Confidential.pdf	E:\Multicorp\Financial Servi...	SSN	1512	GLBA + NPPI	$ 2472	File Read
6/23/2021 8:21:47 PM	192.168.20.193	MULTICORP\Gemma	Confidential.pdf	E:\Multicorp\Financial Servi...	SSN	1512	GLBA + NPPI	$ 2472	File Copy
6/23/2021 8:21:47 PM	192.168.20.193	MULTICORP\Gemma	Expenses.xlsx	E:\Multicorp\Financial Servi...	SSN + Names	708	GLBA + NPPI	$ 2124	File Read
6/23/2021 8:21:47 PM	192.168.20.193	MULTICORP\Gemma	Expenses.xlsx	E:\Multicorp\Financial Servi...	SSN + Names	708	GLBA + NPPI	$ 2124	File Copy
6/23/2021 8:21:47 PM	192.168.20.193	MULTICORP\Gemma	Investments.pptx	E:\Multicorp\Financial Servi...	SSN	459	GLBA + NPPI	$ 1105	File Read

Total Records : 84

1 of 1 page(s)

Figure 6: File Copy Report with Filtered Data

The report can be scheduled, saved, and exported.

4.3. Threat Models

Real time alerts can be generated whenever a potential threat is detected by enabling one of many pre-defined Threat Models within the Lepide Data Security Platform.

To see all the threat models available, click the **Alerts** icon 🔔 and the following screen will be displayed:

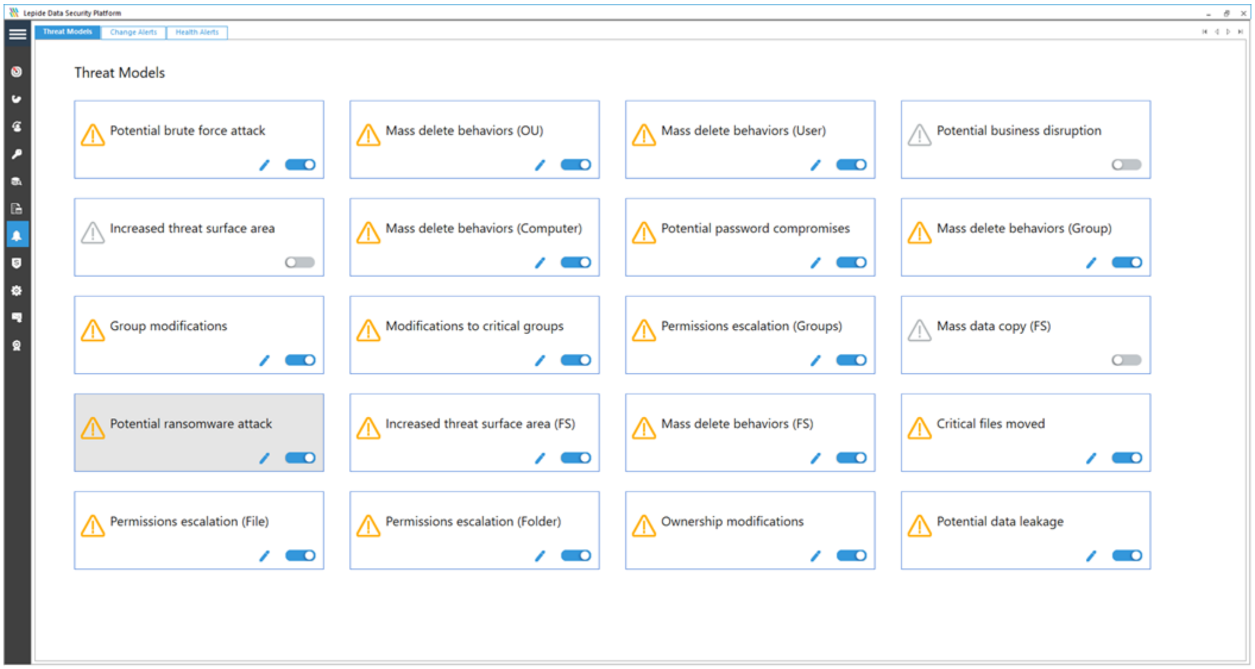

Lepide Data Security Platform
Threat Models
Change Alerts
Health Alerts
Threat Models
Potential brute force attack
Mass delete behaviors (OU)
Mass delete behaviors (User)
Potential business disruption
Increased threat surface area
Mass delete behaviors (Computer)
Potential password compromises
Mass delete 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 7: Threat Models

The Threat Models can be enabled as needed. They can then be configured to generate an alert and respond to a threat.

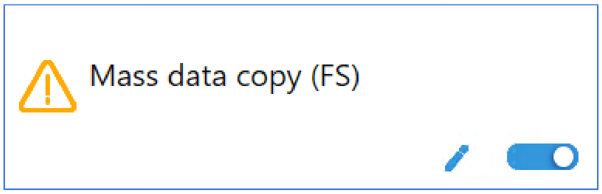
Responding to a Threat

Once an alert has been received, automated scripts can be executed to speed up the response time and address any threats immediately. Using custom script execution, user accounts and/or file servers can be shut down and other actions taken to prevent a potential data breach.

4.4. How to Enable and Configure the Mass Data Copy Threat Model

Click the **Alerts** icon 🔔 from the left-hand toolbar to display all the Threat Models available.

To enable the **Mass data copy (FS) Threat Model,** move the slide toggle to the right.

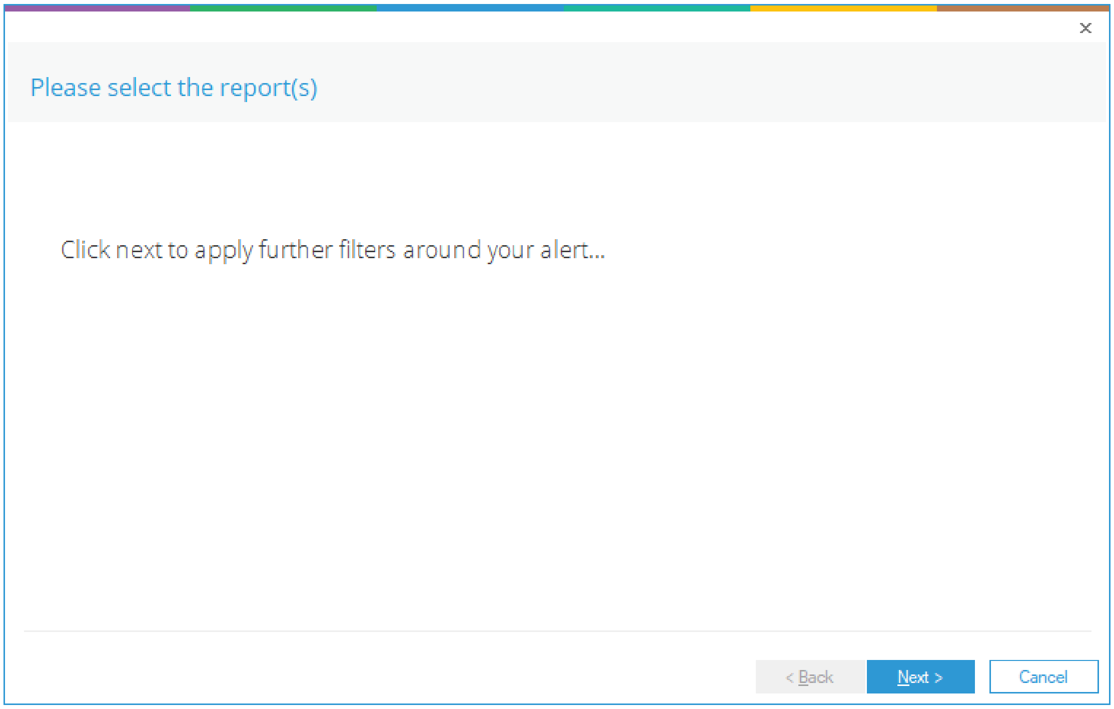


Mass data copy (FS)

Figure 8: Mass Data Copy Threat Model

Click the ✎ icon to configure the alerts and responses you require.

This will start a wizard:

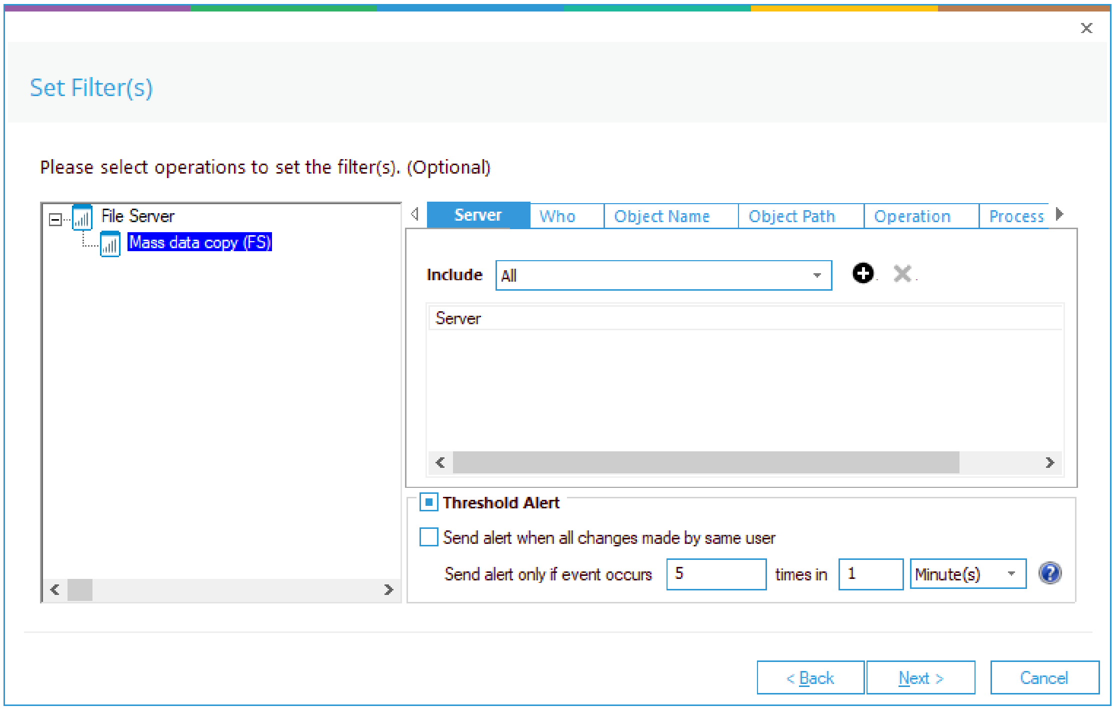


Please select the report(s)

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

Figure 10: Threat Model Wizard

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



Set Filter(s)

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

File Server
Mass data copy (FS)

Include: All

Server

☑ Threshold Alert

□ Send alert when all changes made by same user

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

Figure 11: 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 Mass data copy (FS).

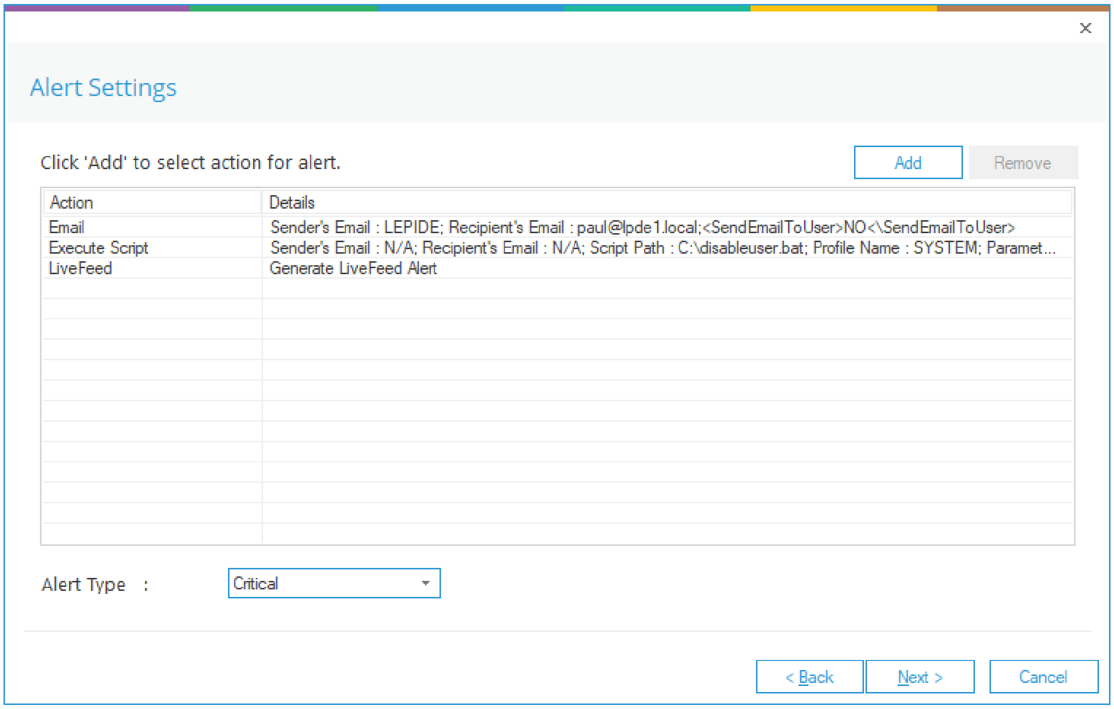
There are options to change the settings for Server, User, Object Name, Object Path, Operation, Process and From using the tabs at the top of this dialog box. The default setting for all these options is All.

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:



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

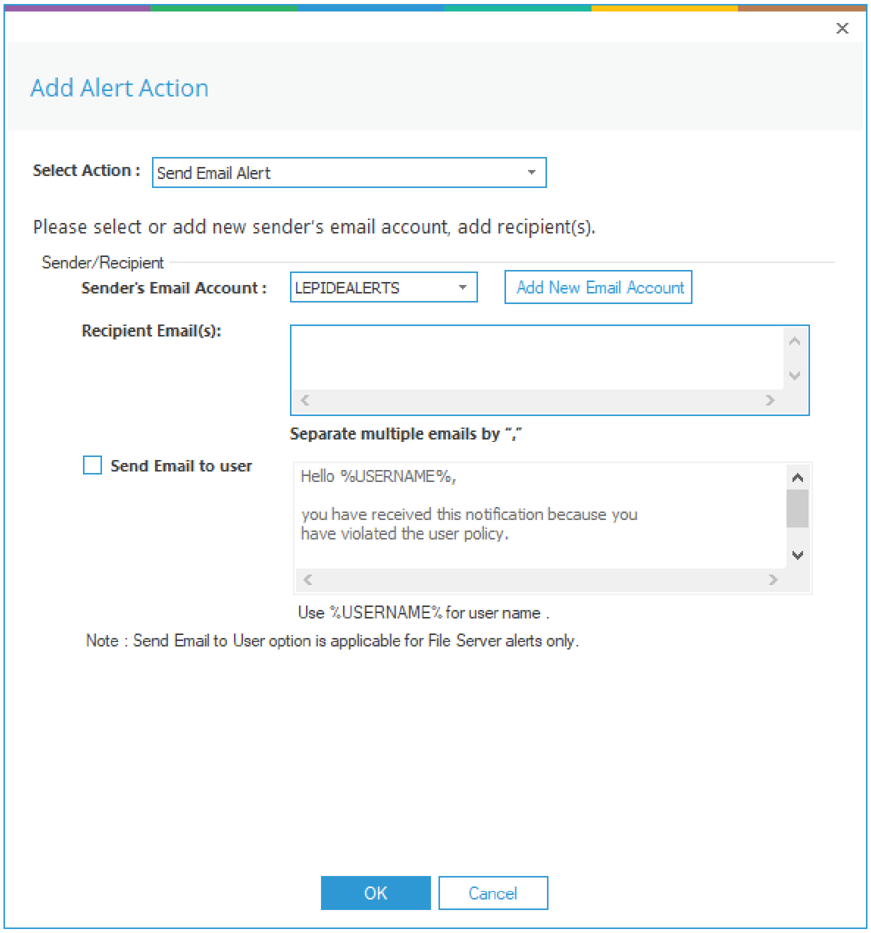
Alert Type : Critical

Figure 12: Add Alert Settings

This dialog box allows you to set up responses to occur when an alert has been triggered and it 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%,

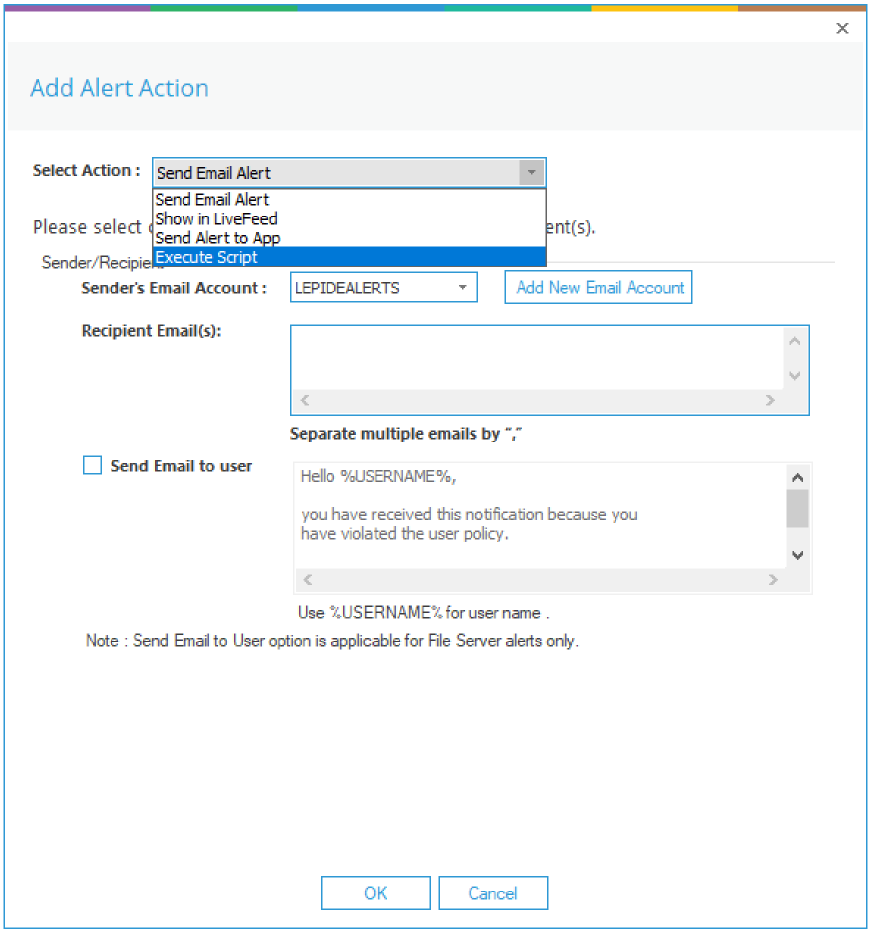
you have received this notification because you have violated the user policy.

Use %USERNAME% for user name .

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

Figure 13: 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.

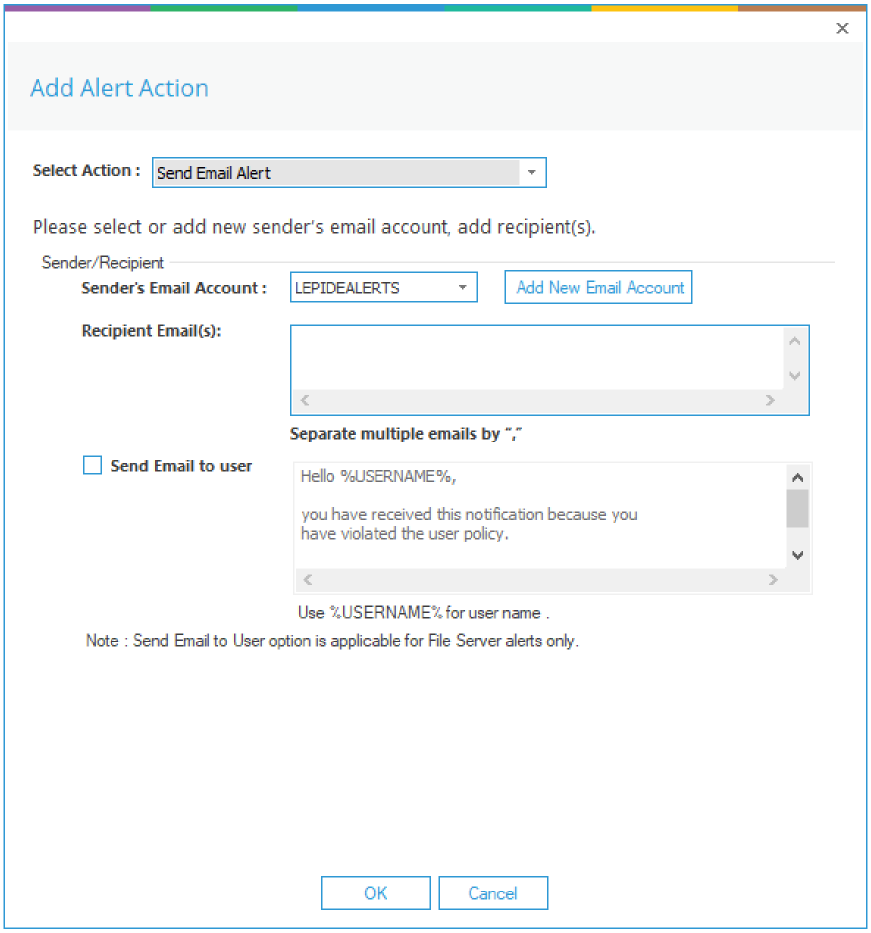
Figure 14: Add Alert Action Options

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.

Figure 15: 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:

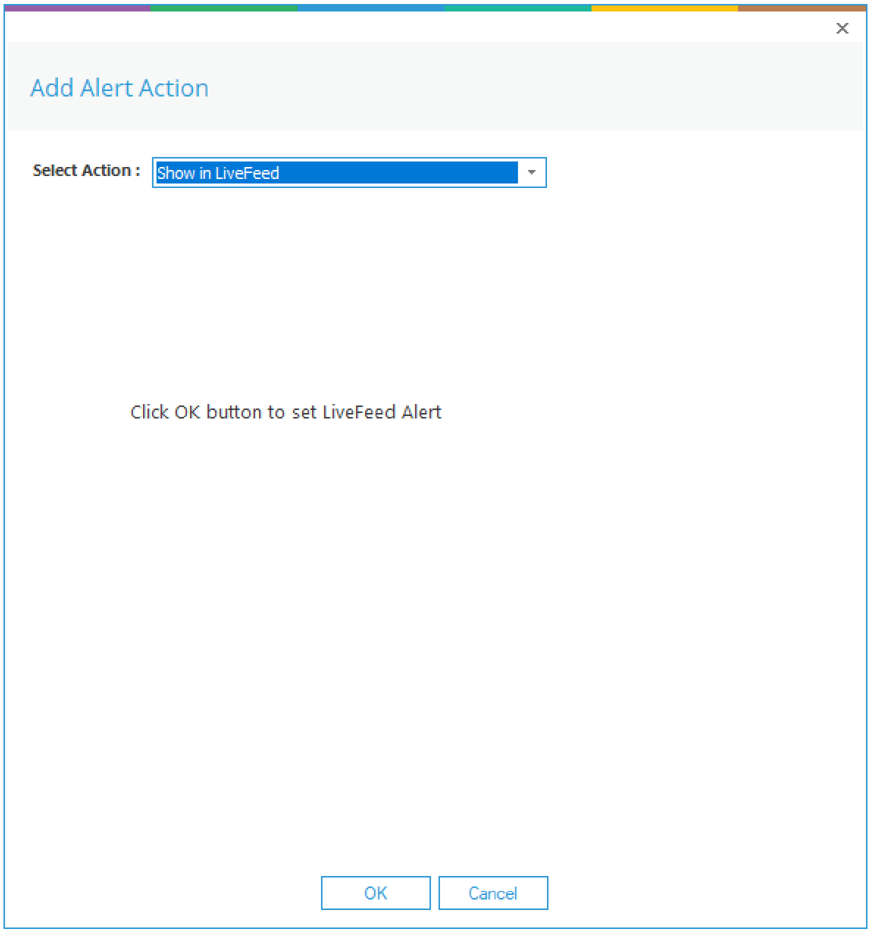
Sender's Email Account: The Sender's email account will be displayed here if it has been selected. Click Add New Email Account to enter a new Sender's Email Account

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.

Click OK to save the alert action.

2. Show in LiveFeed



Add Alert Action

Select Action : Show in LiveFeed

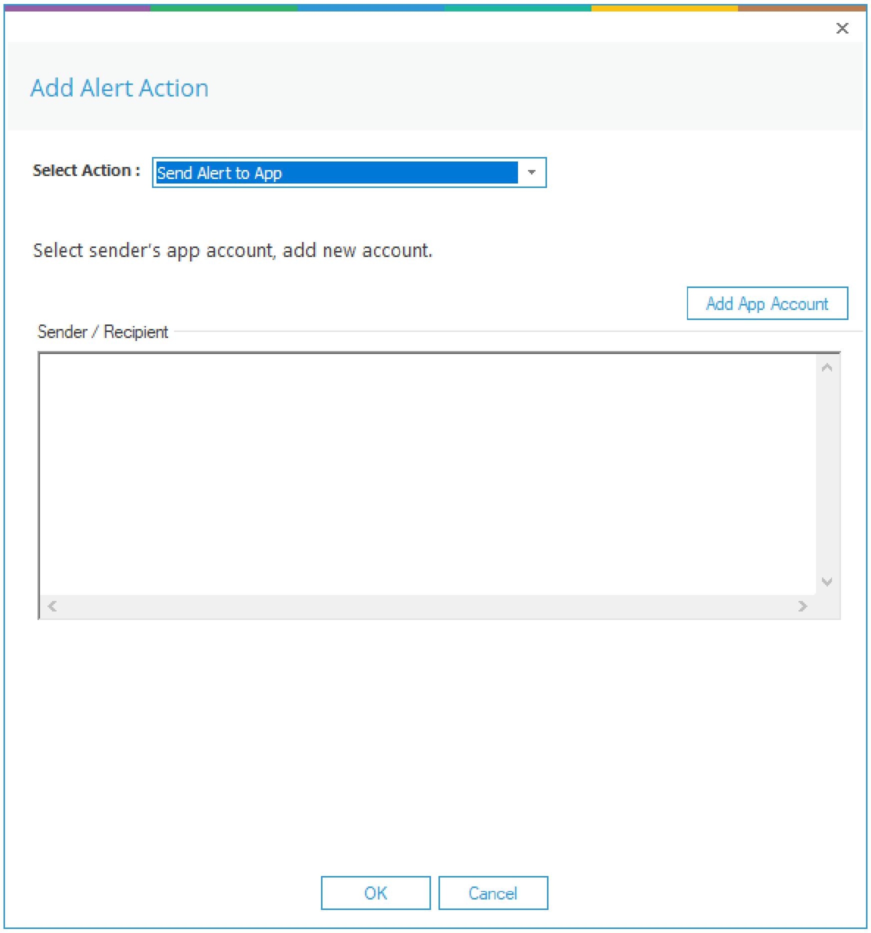
Click OK button to set LiveFeed Alert

Figure 16: 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

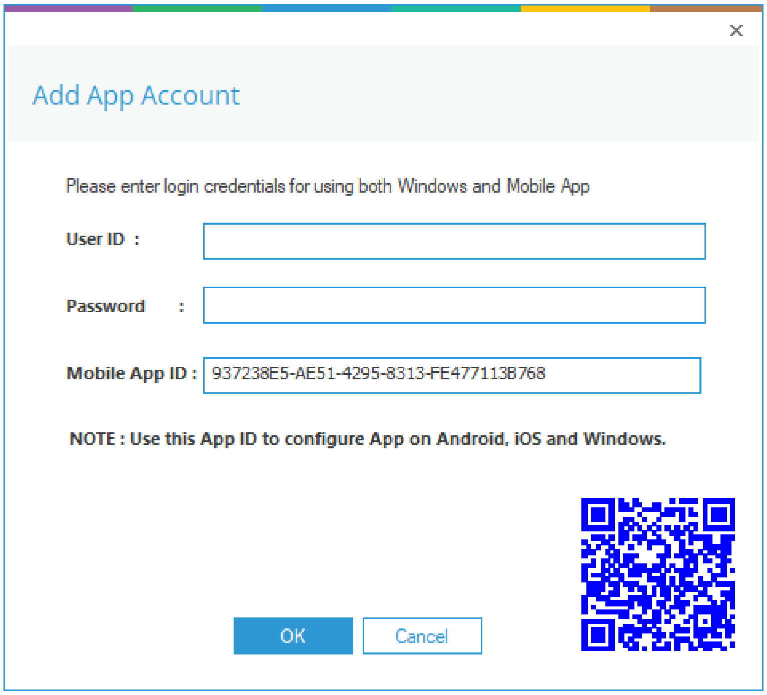
Select Action : Send Alert to App

Select sender's app account, add new account.

Figure 17: 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.

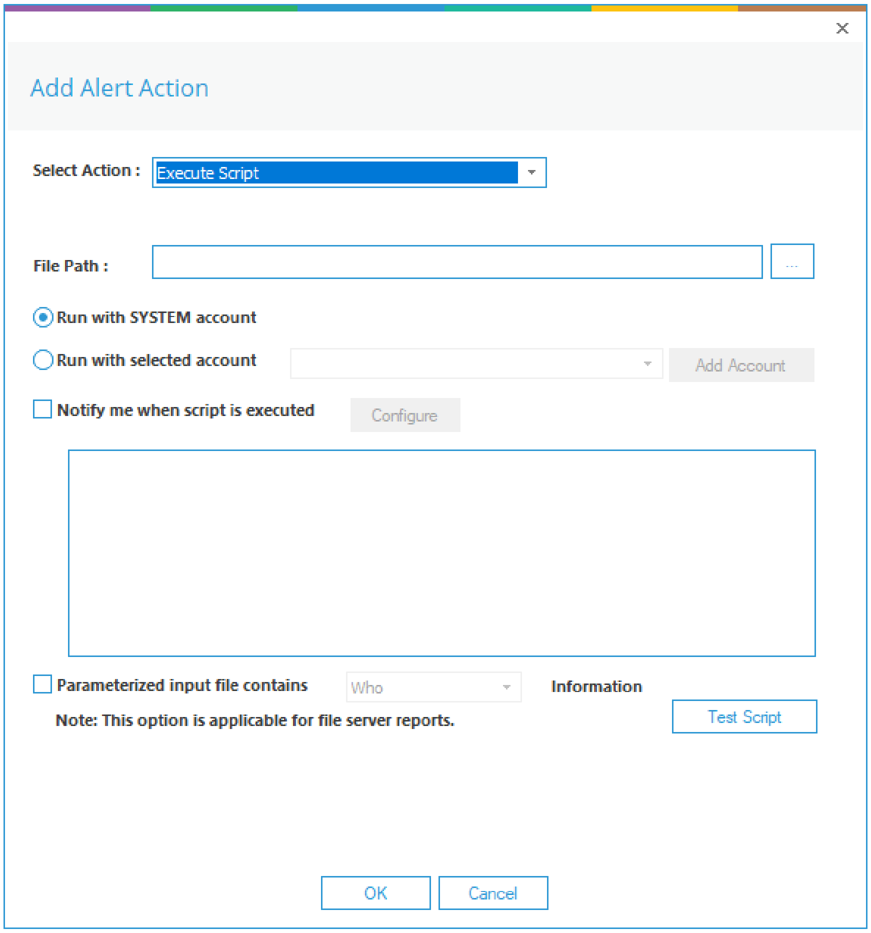
Figure 18: Add App Account

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 19: 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:

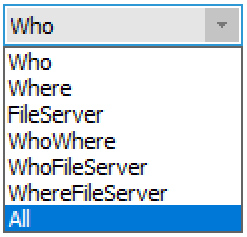
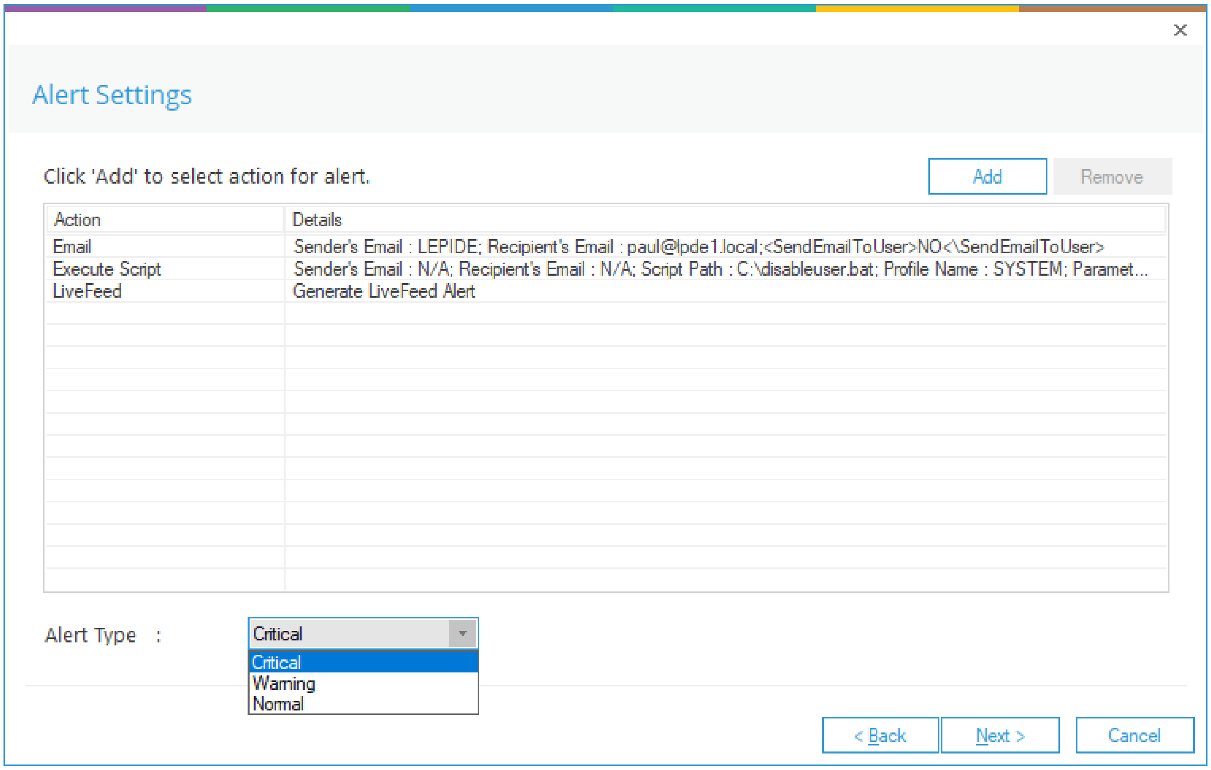


Figure 20: List of Variables

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

Click **OK** to return to the **Alert Settings** dialog box.



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

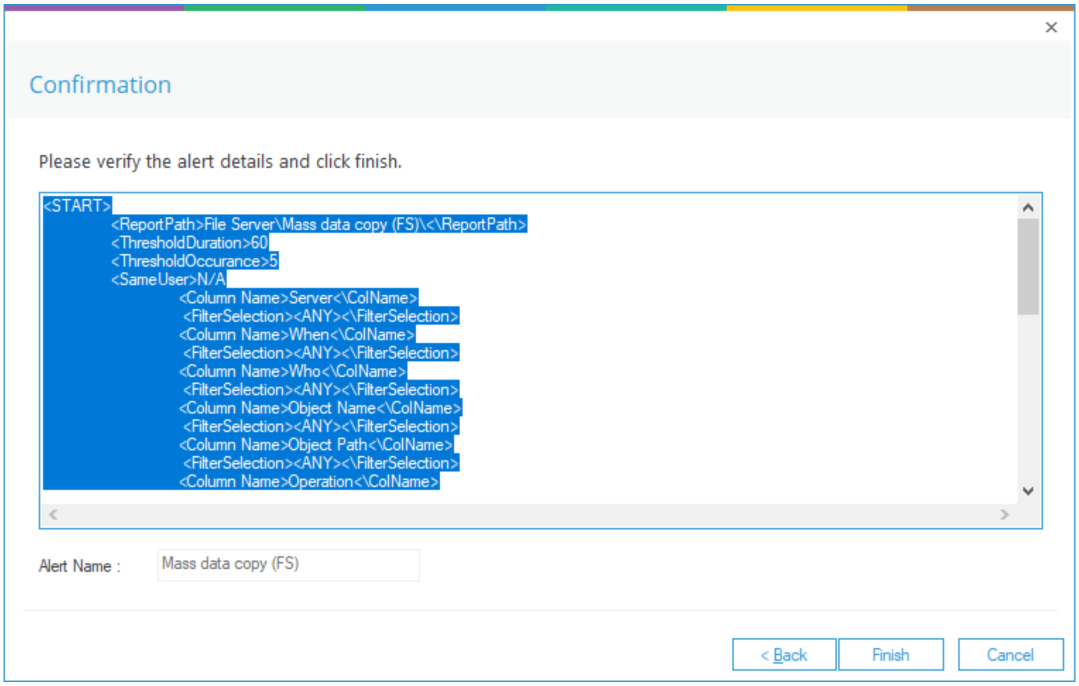
Alert Type : Critical

Figure 21: 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:



Please verify the alert details and click finish.

```
<START>
        <ReportPath>File Server\Mass data copy (FS)\<\ReportPath>
        <ThresholdDuration>60
        <ThresholdOccurance>5
        <SameUser>N/A
                <Column Name>Server<\ColName>
                 <FilterSelection><ANY><\FilterSelection>
                <Column Name>When<\ColName>
                 <FilterSelection><ANY><\FilterSelection>
                <Column Name>Who<\ColName>
                 <FilterSelection><ANY><\FilterSelection>
                <Column Name>Object Name<\ColName>
                 <FilterSelection><ANY><\FilterSelection>
                <Column Name>Object Path<\ColName>
                 <FilterSelection><ANY><\FilterSelection>
                <Column Name>Operation<\ColName>
```

Alert Name : Mass data copy (FS)

Figure 22: Confirmation of Alert Details

Click **Finish** to return to the Threat Models screen.

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.