Lepide

USE CASE GUIDE

HOW TO DETECT & RESPOND TO A RANSOMWARE ATTACK USING LEPIDE

Table of Contents

1. Introduction

Ransomware is a serious threat to the security of any IT environment. Even though endpoint protection is highly effective it can never fully protect against every form of attack and so ransomware can still get through.

With the knowledge that attacks can and will happen, it's crucial to look at what can be done to contain any damage and ensure that the risk and spread of an attack is mitigated.

The focus at Lepide is to provide visibility over what's happening with your data. Through visibility, you can speed up the detection of potential ransomware and automate your response. The Lepide Solution supports a wide array of enterprise data stores.

This guide is in two parts. The first explains the ways in which you can use Lepide Data Security Platform to detect and respond to a threat. The second section gives step-by-step instructions on how to configure the Ransomware Threat Model which includes alert and response settings.

2. Detecting a Potential Attack

The immediate detection of any suspicious change activity is crucial to containing a ransomware attack. With the Lepide Data Security Platform, detection is in real time and involves threshold alerting, anomaly spotting and the use of threat models.

2.1. Threshold Alerting

Typical ransomware attacks 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 ransomware attacks can be identified in motion and immediate action taken.

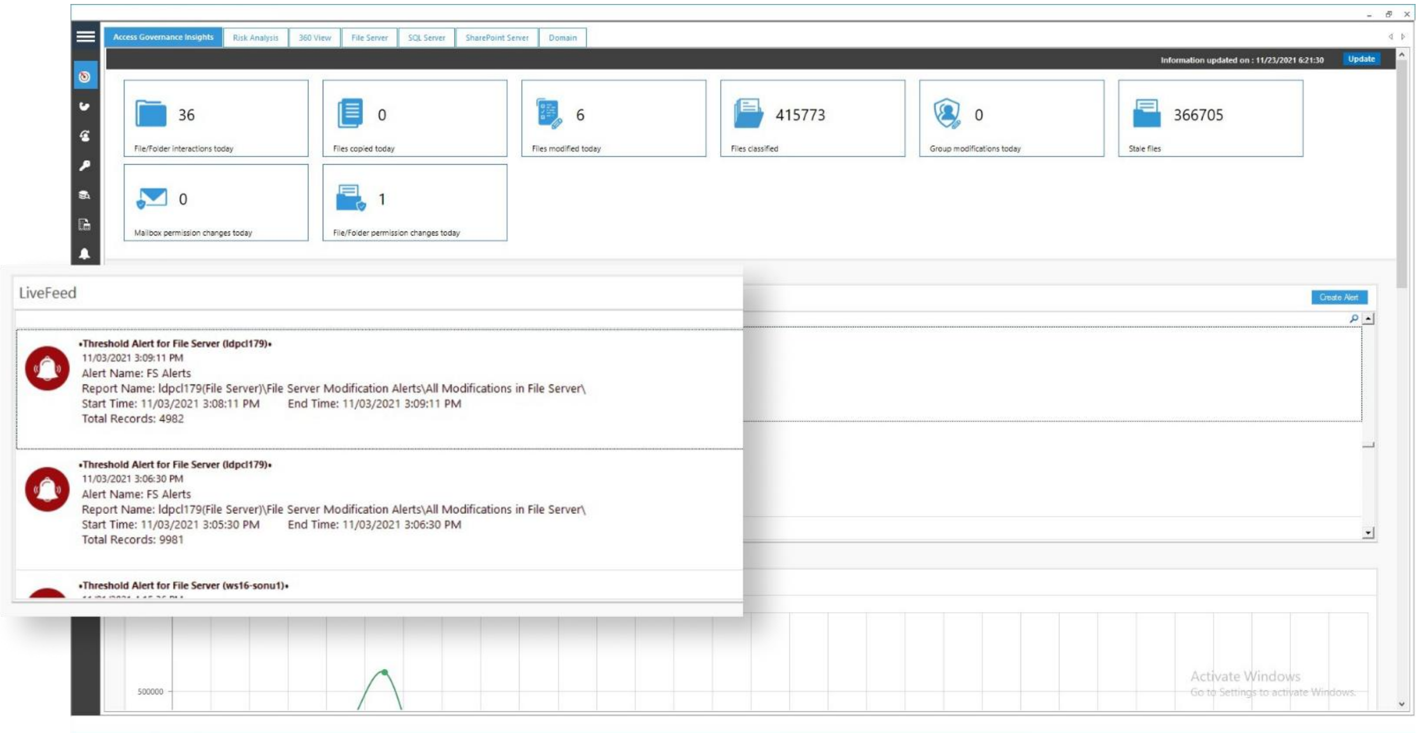
For example, if a large number of files are being renamed within a short time this is a trend that could indicate the start of a ransomware attack. This suspicious activity would trigger an alert, the activity would then be investigated, and the appropriate action taken. For critical alerts, responses 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 **renamed** 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.



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

LiveFeed

•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)•

Below is an example of a Threshold alert on the Lepide Dashboard:

Figure 1: Threshold Alert

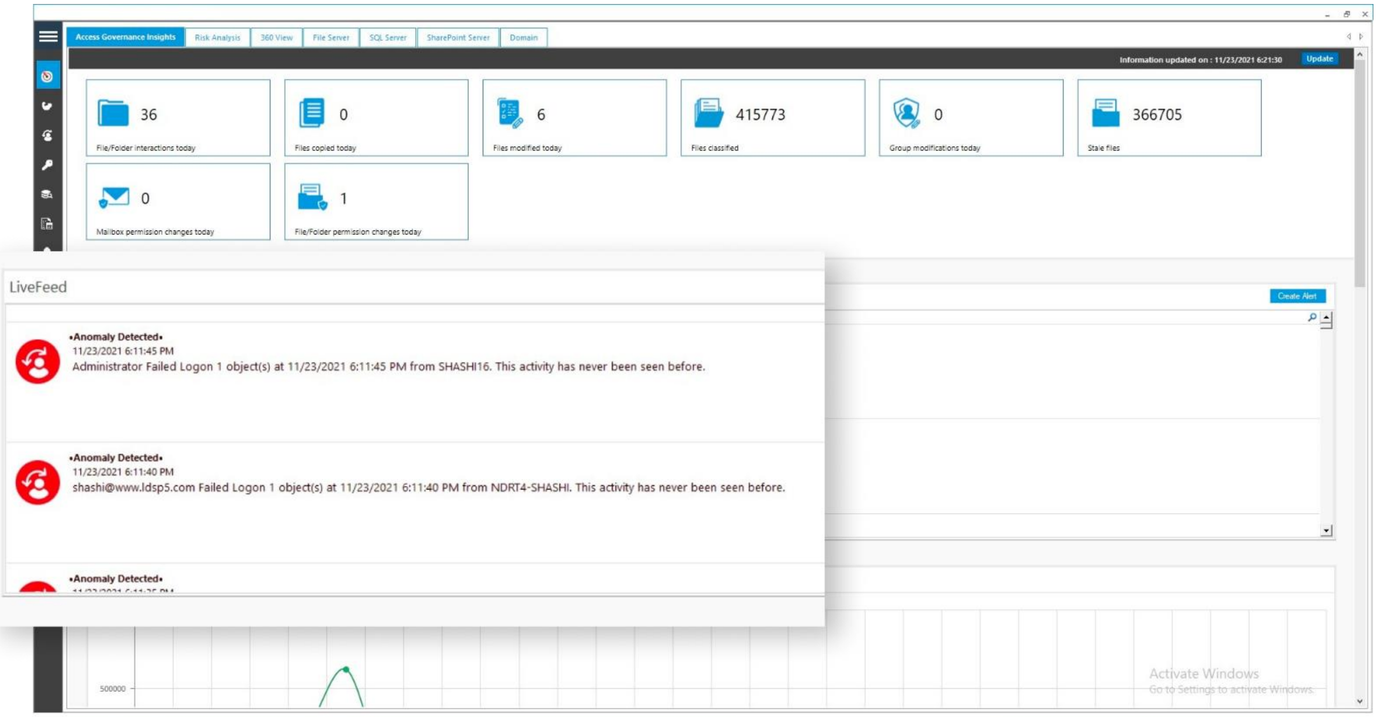
2.2. Anomaly Spotting

The Lepide anomaly detection technology allows you to spot and react to anomalous or unique user behavior. This machine learning establishes a baseline for normal user behavior and then alerts are generated whenever this behavior deviates from this norm. Even single point anomalies can be detected.

Once an anomaly has been identified, automated threat responses can take effect to contain threats before they cause irreparable damage.

Examples of anomalies in user behavior include copying files with sensitive data, logging onto the server out of hours, or simply acting strangely based on learned behavior.

Below is an example of an Anomaly 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

LiveFeed

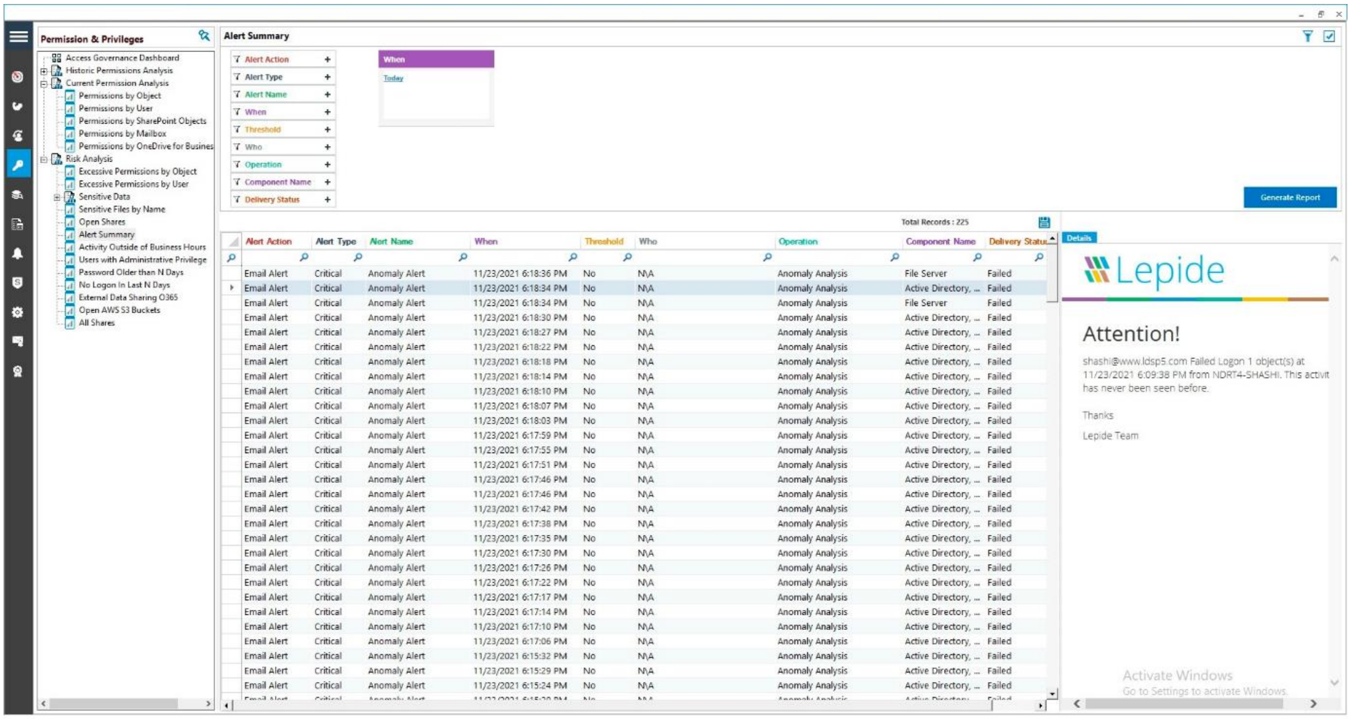
•Anomaly Detected•
11/23/2021 6:11:45 PM
Administrator Failed Logon 1 object(s) at 11/23/2021 6:11:45 PM from SHASHI16. This activity has never been seen before.

•Anomaly Detected•
11/23/2021 6:11:40 PM
shashi@www.ldsp5.com Failed Logon 1 object(s) at 11/23/2021 6:11:40 PM from NDRT4-SHASHI. This activity has never been seen before.

•Anomaly Detected•

Figure 2: Anomaly Alert

Once an alert has been received, an Alert Summary is available to provide information about the potential attack. The details of the activity triggering the alert can then be further investigated using the **All Modifications in File Server** report.



Alert Action	Alert Type	Alert Name	When	Threshold	Who	Operation	Component Name	Delivery Status
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:36 PM	No	N\A	Anomaly Analysis	File Server	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:34 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:34 PM	No	N\A	Anomaly Analysis	File Server	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:30 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:27 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:22 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:18 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:14 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:10 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:07 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:18:03 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:59 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:55 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:51 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:46 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:46 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:42 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:38 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:35 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:30 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:26 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:22 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:17 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:14 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:10 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:17:06 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:15:32 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:15:29 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed
Email Alert	Critical	Anomaly Alert	11/23/2021 6:15:24 PM	No	N\A	Anomaly Analysis	Active Directory, ...	Failed

Lepide

Attention!

shashi@www.ldsp5.com Failed Logon 1 object(s) at 11/23/2021 6:09:38 PM from NDRT4-SHASHI. This activit has never been seen before.

Thanks

Lepide Team

Figure 3: Alert Summary

2.3. Threat Model for Ransomware

Real time alerts are generated whenever a potential threat is detected by enabling one of many 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:

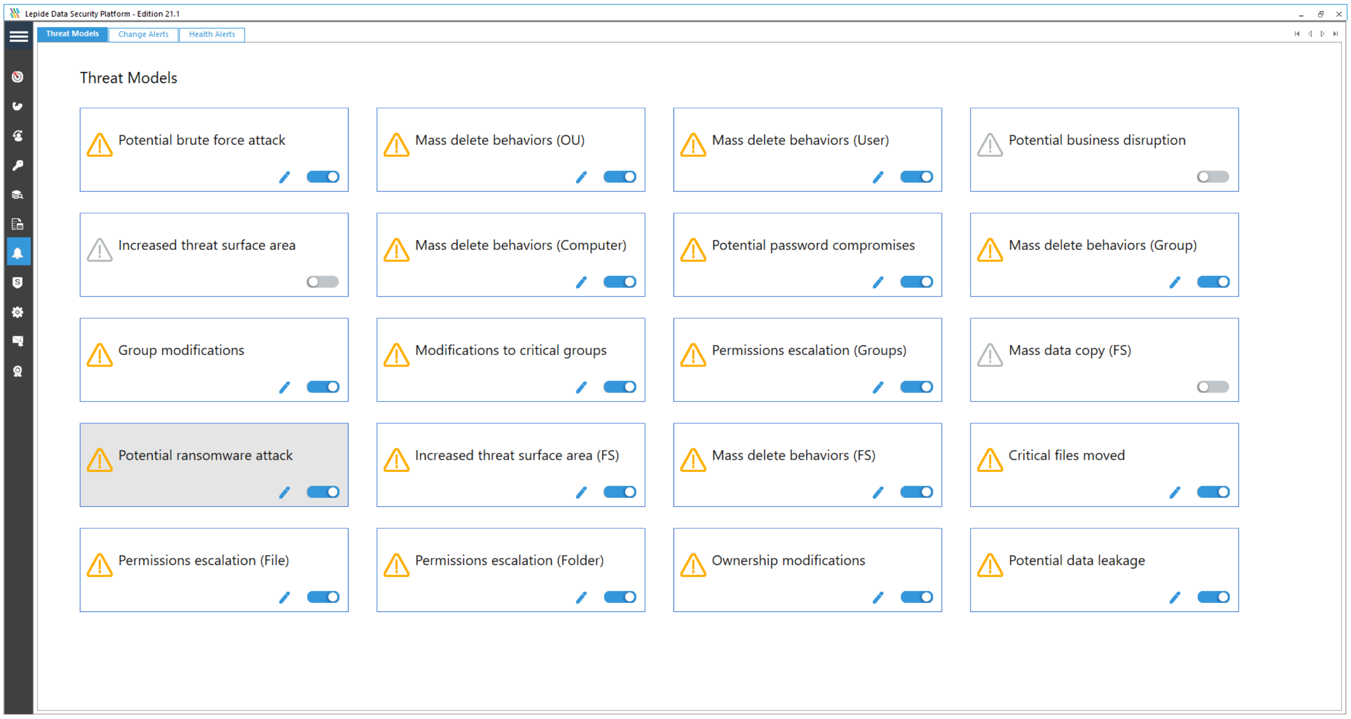

Lepide Data Security Platform - Edition 21.1
Threat Models
Change Alerts
Health Alerts
Threat Models
Potential brute force attack
Mass delete behaviors (OU)
Mass delete behaviors (User)
Potential business disruption
Increased threat surface area
Mass delete behaviors (Computer)
Potential password compromises
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 4: Threat Models

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

3. Responding to a Potential Attack

Once alerts have 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 malware from spreading.

With a detailed and complete audit trail of all changes being made to your data, permissions and systems, the Lepide Data Security Platform can provide your security operations team with the information they need to investigate incidents faster and more efficiently.

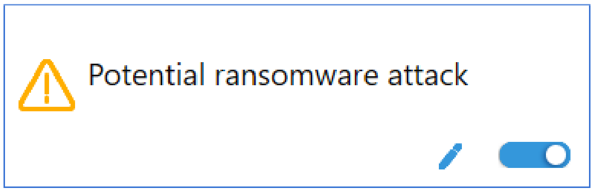
Improve Incident Response and Integrate with your SIEM

The Lepide Data Security Platform can integrate with any SIEM solution to simplify your ransomware response. The Solution can be configured to send specific events to your SIEM and give more context to the raw audit data.

4. How to Enable and Configure the Ransomware Attack 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.

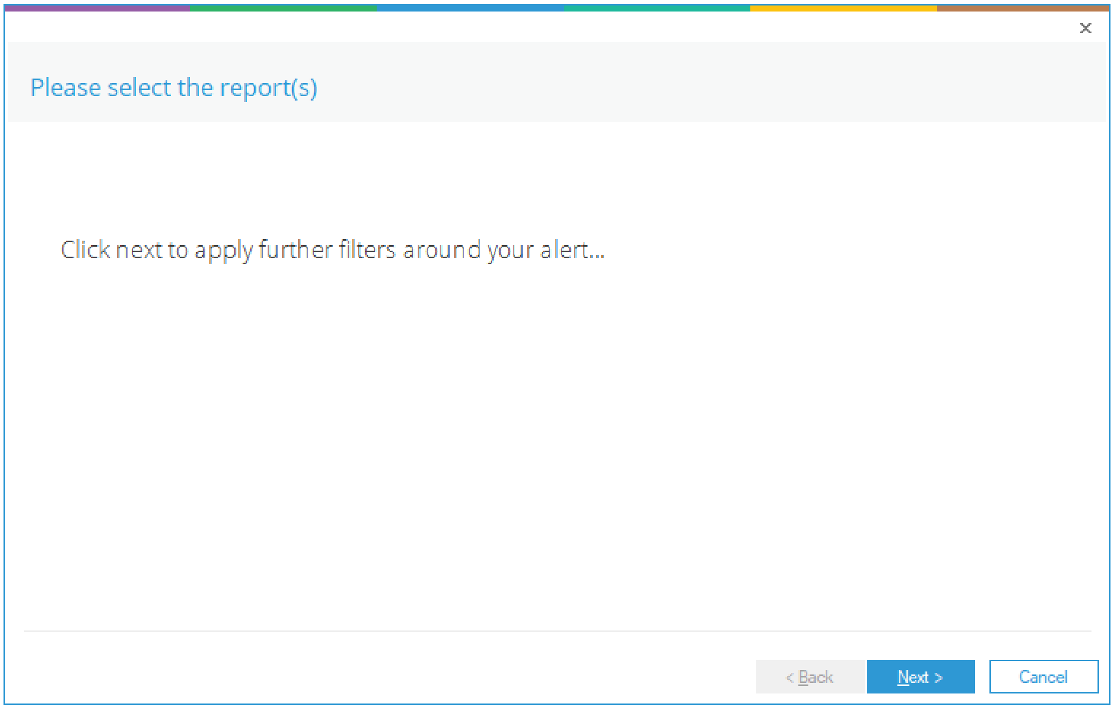


Potential ransomware attack

Figure 5:Enable the Potential Ransomware Attack Threat Model

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

This will start a wizard:

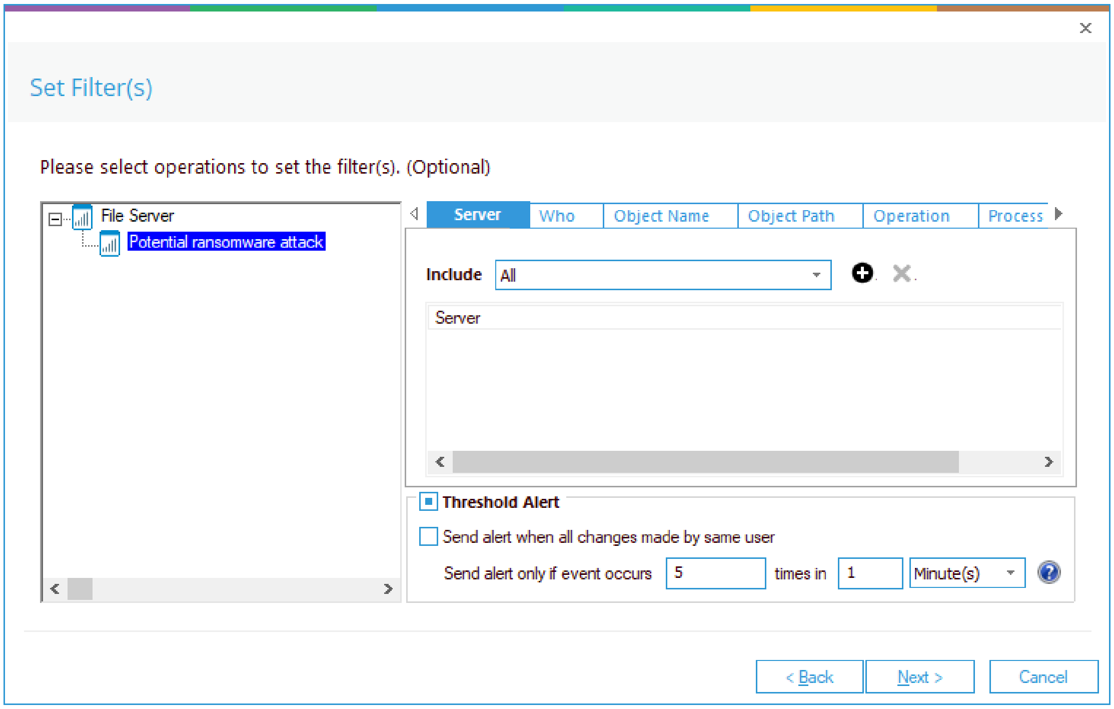


Please select the report(s)

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

Figure 6: Wizard to Configure Alerts

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



Set Filter(s)

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

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 7: 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**.

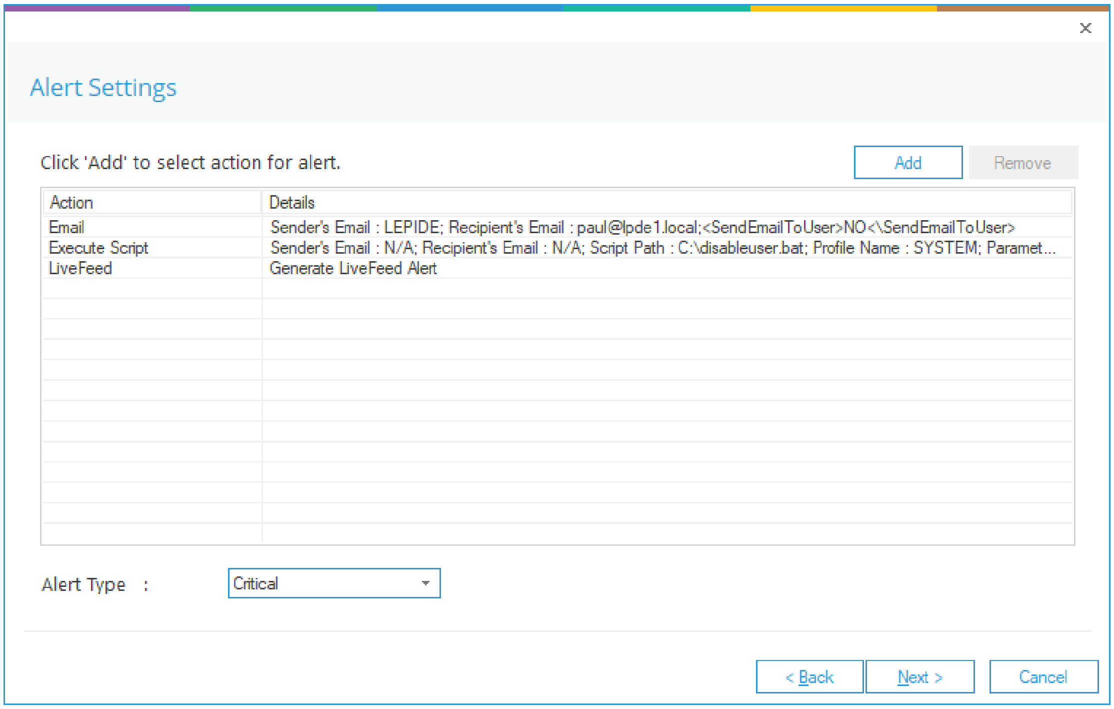
There are options to change the settings for **Server, User, Object Name, Object Path, Operation, Process and From** using the tabs at the top of this dialog box. The default setting for all these options is **All**.

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:



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

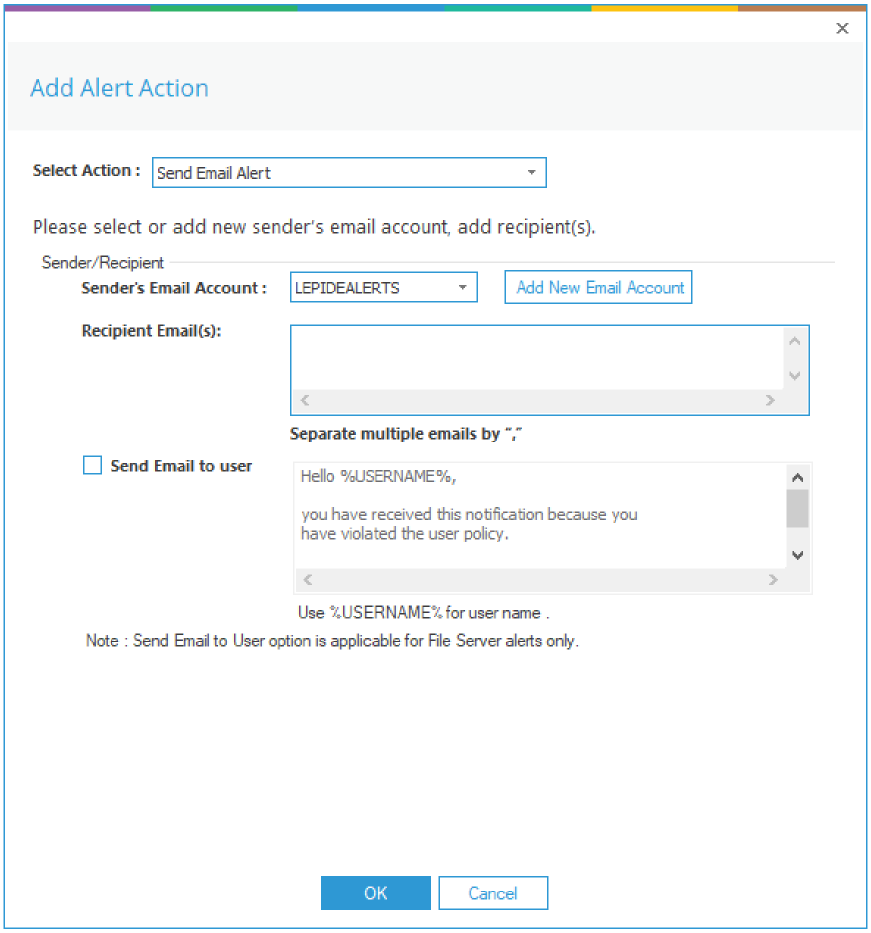
Alert Type : Critical

Figure 8: Add 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%,

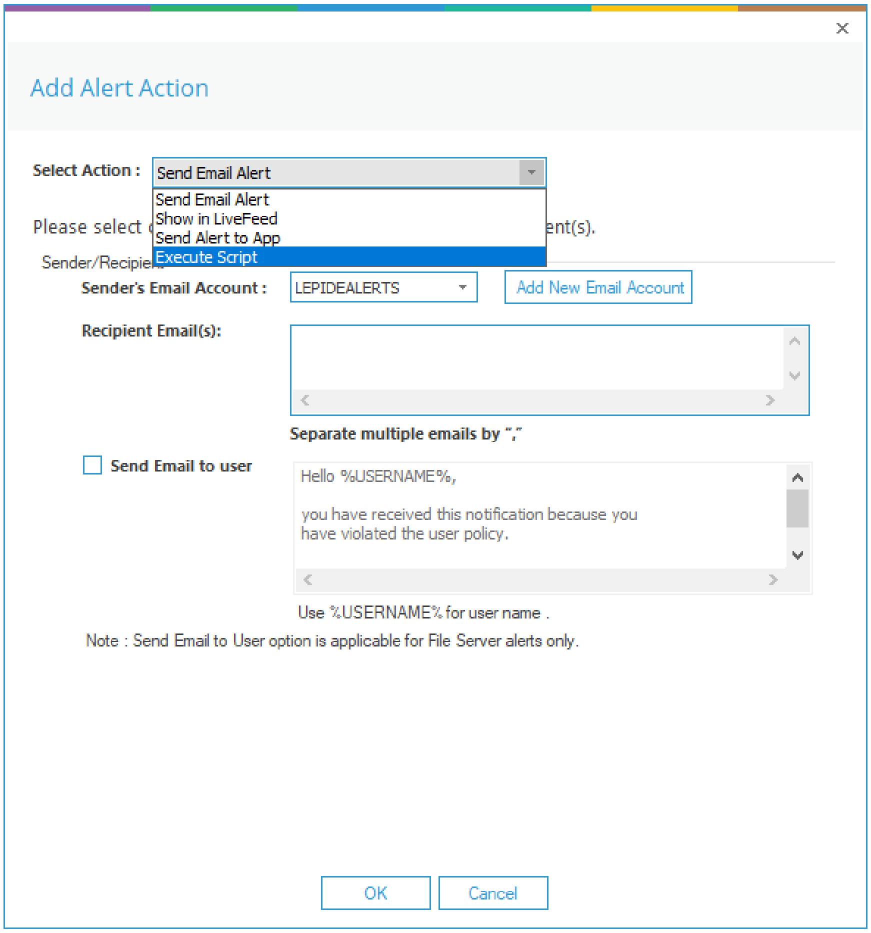
you have received this notification because you have violated the user policy.

Use %USERNAME% for user name .

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

Figure 9: 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/Recipie

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.

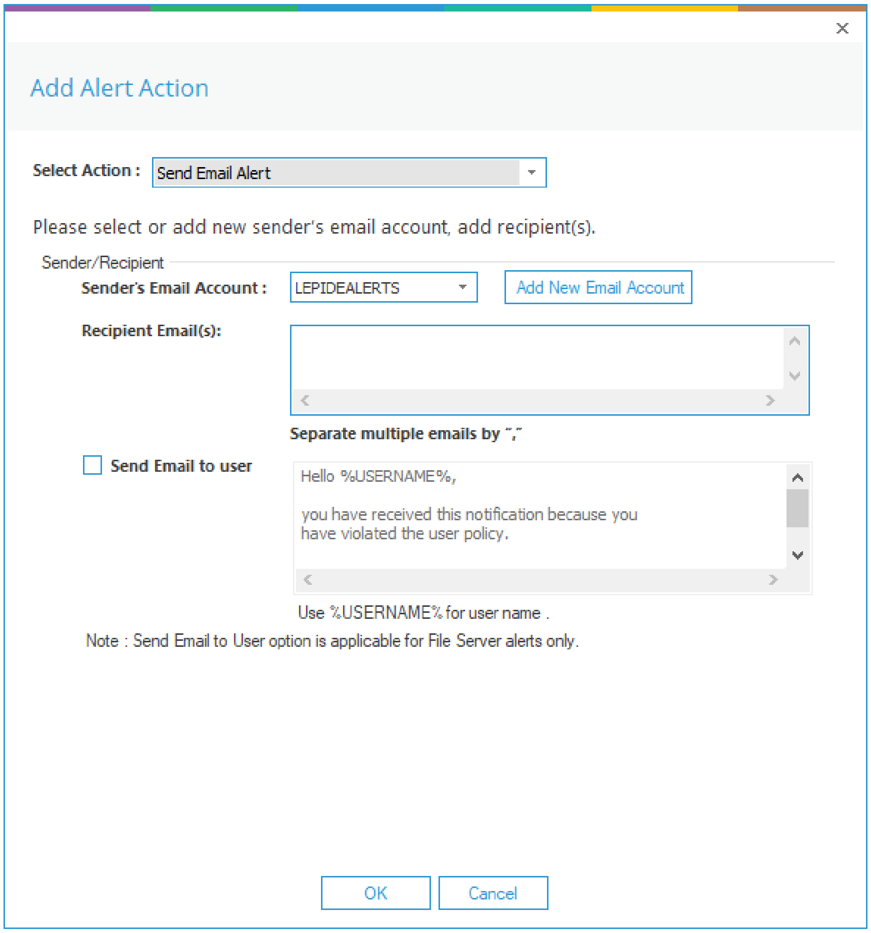
Figure 10: Add Alert Action Options

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 11: 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:

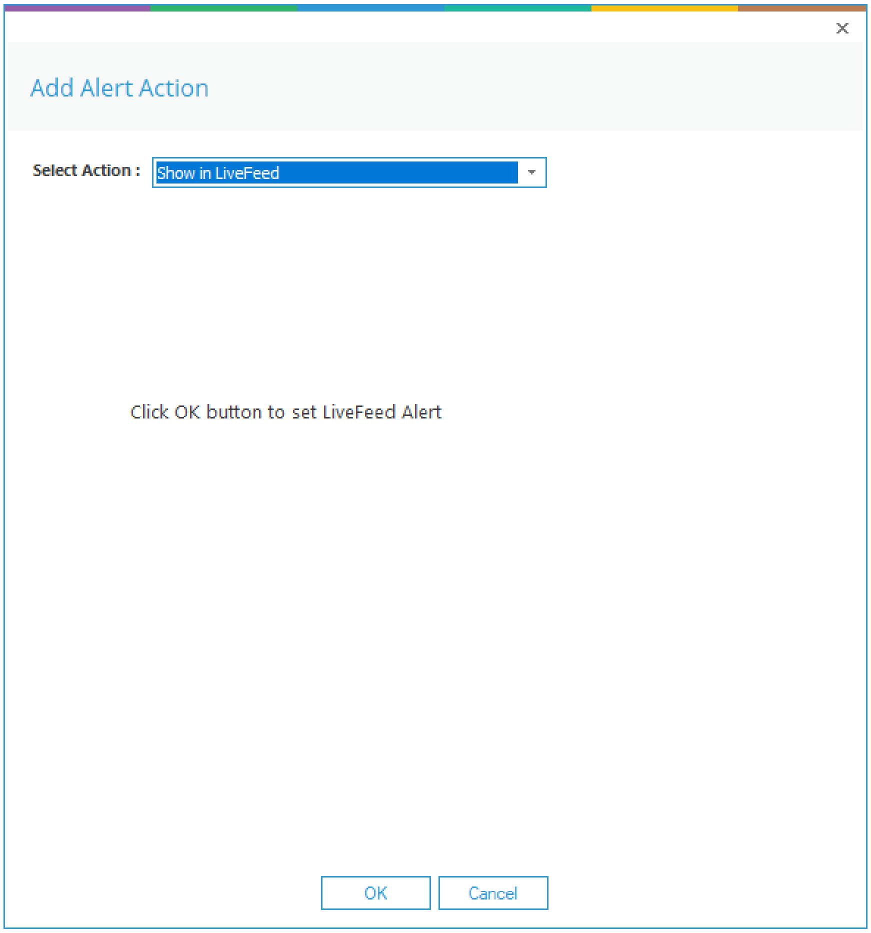
Sender's Email Account: The Sender's email account will be displayed here if it has been selected. Click **Add New Email Account** to enter a new Sender's Email Account

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

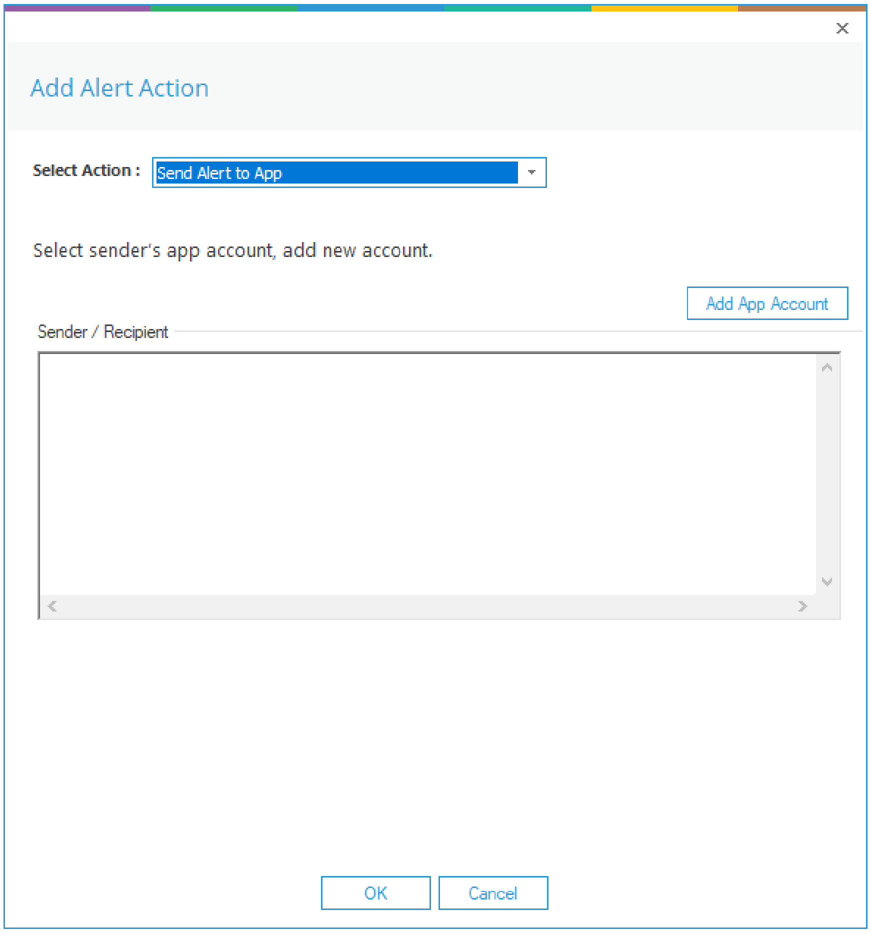
Click OK button to set LiveFeed Alert

Figure 12: 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

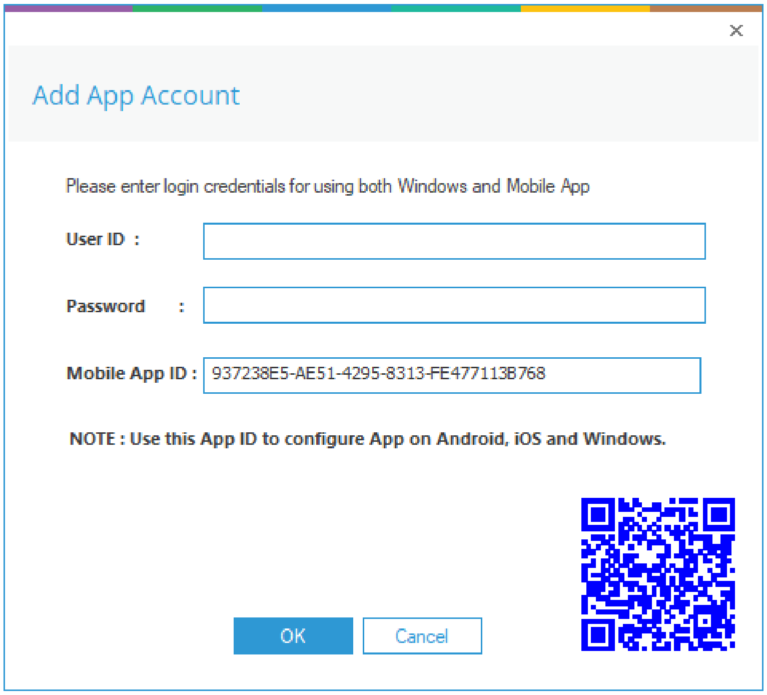
Select Action : Send Alert to App

Select sender's app account, add new account.

Figure 13: 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.

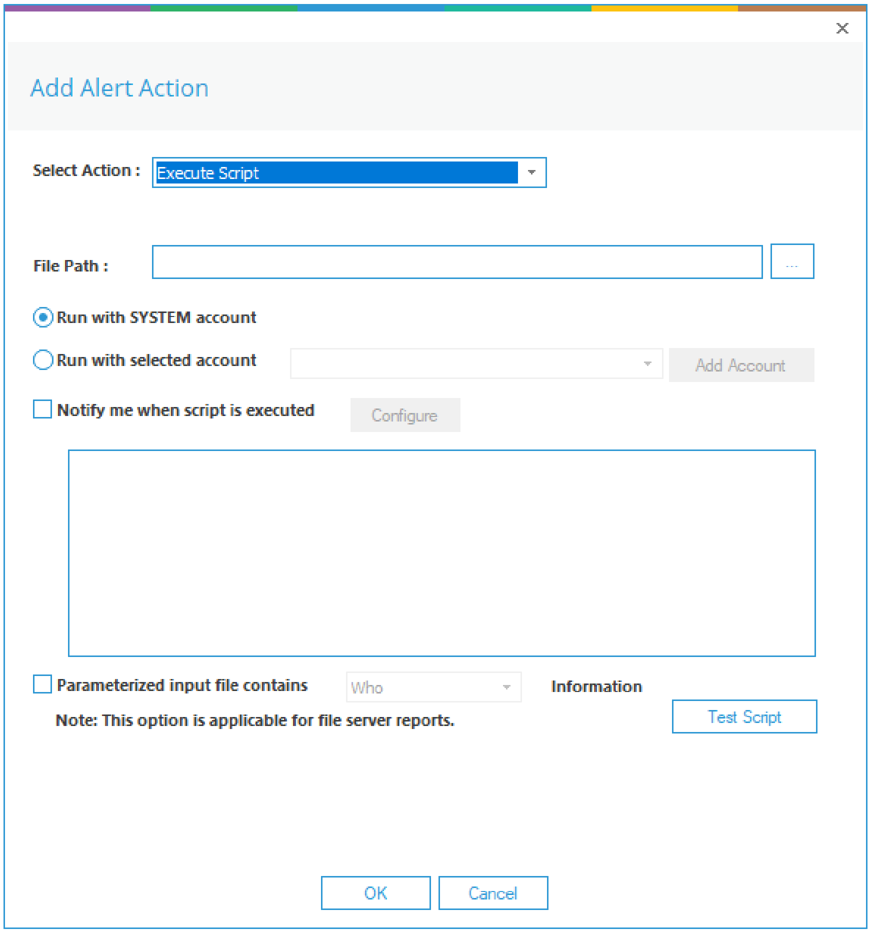
Figure 14: Add App Account

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 15: 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

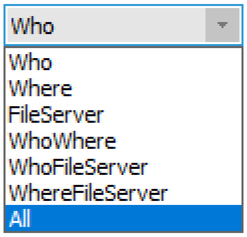
Run with selected account.

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:



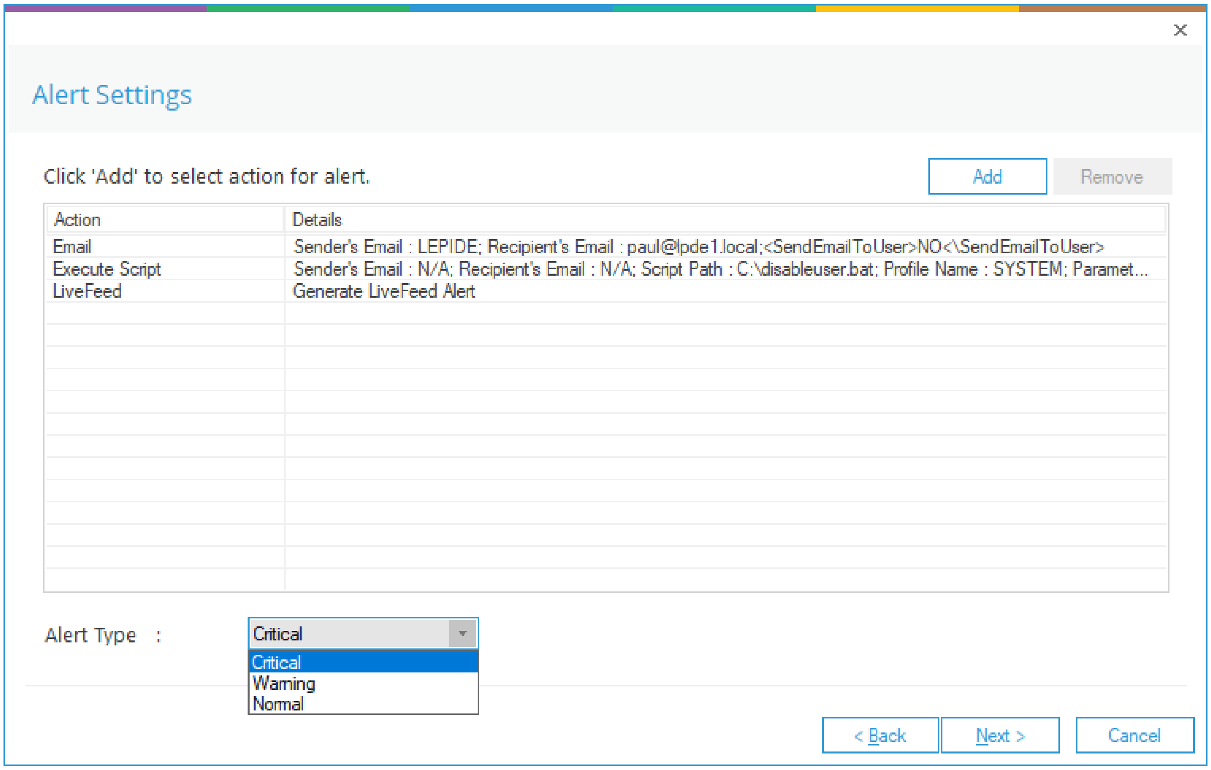
Who

- Who
- Where
- FileServer
- WhoWhere
- WhoFileServer
- WhereFileServer
- All

Figure 16: 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 17: 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 Threat Models screen.

5. Support

If you are facing any issues whilst installing, configuring or using the solution, you can connect with our team using the below contact information.

Product Experts	Technical Gurus
USA/Canada: +1(0)-800-814-0578	USA/Canada: +1(0)-800-814-0578
UK/Europe: +44 (0) -208-099-5403	UK/Europe: +44 (0) -208-099-5403
Rest of the World: +91 (0) -991-004-9028	Rest of the World: +91(0)-991-085-4291

Alternatively, visit https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

6. Trademarks

Lepide Data Security Platform, 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.