



USE CASE GUIDE

HOW TO REPORT ON ACTIVITY OUTSIDE OF BUSINESS HOURS

Table of Contents

- 1. Introduction..... 3
- 2. Compromised User Accounts 3
- 3. The Activity Outside of Business Hours Report 3
 - 3.1. Prerequisites 3
 - 3.2. Running the Activity Outside of Business Hours Report..... 3
 - 3.3. Filtering the Report..... 5
- 4. Responding to a Threat..... 6
 - 4.1. Creating an Alert..... 6
- 5. Support 18
- 6. Trademarks 18

1. Introduction

Data within an organization needs to be protected from unauthorized access, modification, or deletion but still be available to anyone who needs access to it. This protection of data from cyber threats is critical within any organization and is fundamental to a zero-trust practice.

The focus at Lepide is to provide visibility over what's happening with your data and through visibility you can take the necessary action to mitigate risk and stay compliant.

2. Compromised User Accounts

A user account is compromised when an attacker gains access to credentials to perform actions on behalf of the targeted user. There are several ways in which potentially compromised user accounts can be detected however, without a solution in place, this can be a complex and time-consuming process. It is essential to not only be able to track potentially compromised users but also to react quickly enough to mitigate any damage.

One indication of a compromised user account is if the user logs on outside of business hours, or outside of their normal working pattern. This could happen because either their account has been compromised or they plan to act maliciously. There are, of course, situations when users have legitimate reasons to logon out of hours but by having visibility over all out of hours activity, anomalies can be detected which trigger alerts and the threat mitigation process initiated.


3. The Activity Outside of Business Hours Report

Within the Lepide Data Security Platform, the summary of activity outside of business hours is provided using the **Activity Outside of Business Hours Report**. This report will show all out of business hours activity within a selected time scale and can be further filtered to focus on whatever data is required. Alerts can be configured to run with this report so that if suspicious activity is detected, an alert is sent, and a manual or automated response activated to reduce any damage and stop any further malicious activity.

3.1. Prerequisites

Before reporting and alerting on outside of business hours activity you will need to have added and configured to enable auditing at least one component.

3.2. Running the Activity Outside of Business Hours Report

- Click the **Permission & Privileges**  icon
- Expand **Risk Analysis** (from the tree structure to the left side of the screen)

- Click on **Activity Outside of Business Hours** to display the **Activity Outside of Business Hours Report**

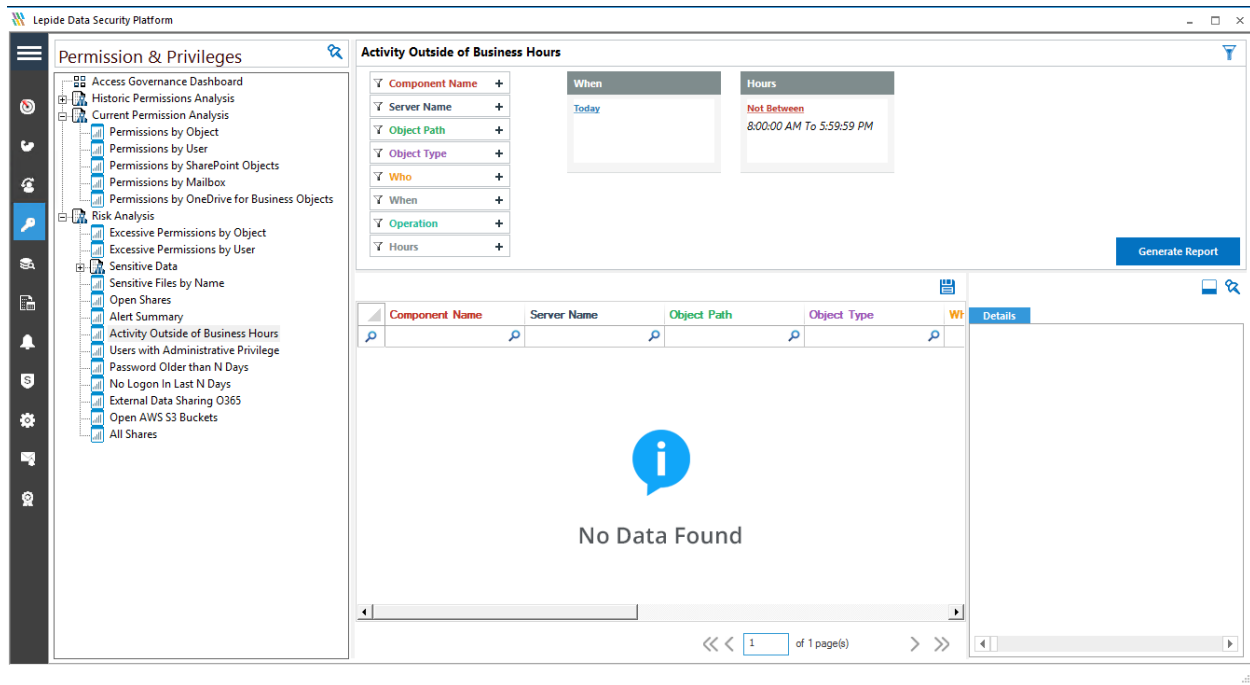


Figure 1: Activity Outside of Business Hours Report

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:

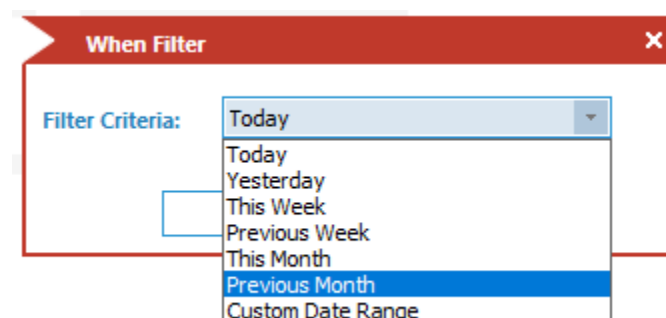


Figure 2: Date Range Filter

- Select a date range from the list

- Click **OK** and you will return to the Activity Outside of Business Hours screen
- Click **Generate Report**

Component Name	Server Name	Object Path	Object Type	Who	When	Operation	What	Where
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:55 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:55 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:50 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:45 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:45 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:40 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:40 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	david	4/30/2022 7:59:36 AM	Login Attempt Failed	Bad password	192.168.20.192
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:35 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:35 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:30 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:30 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:25 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:25 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:20 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:20 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:15 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:10 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:10 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	david	4/30/2022 7:59:06 AM	Login Attempt Failed	Bad password	192.168.20.192
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:05 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:05 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:59:00 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:58:55 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:58:55 AM	Login Attempt Failed	Account is currently dis...	FS001
Active Directory	multicorp.local	N/A	User	luke	4/30/2022 7:58:50 AM	Login Attempt Failed	Account is currently dis...	FS001

Figure 3: The Generated Report

The report runs and shows information including who logged in, when they logged in and what their activity was.

3.3. 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:



Figure 4: Filter Area

In the example below, the report has been filtered to show both data for **David**:

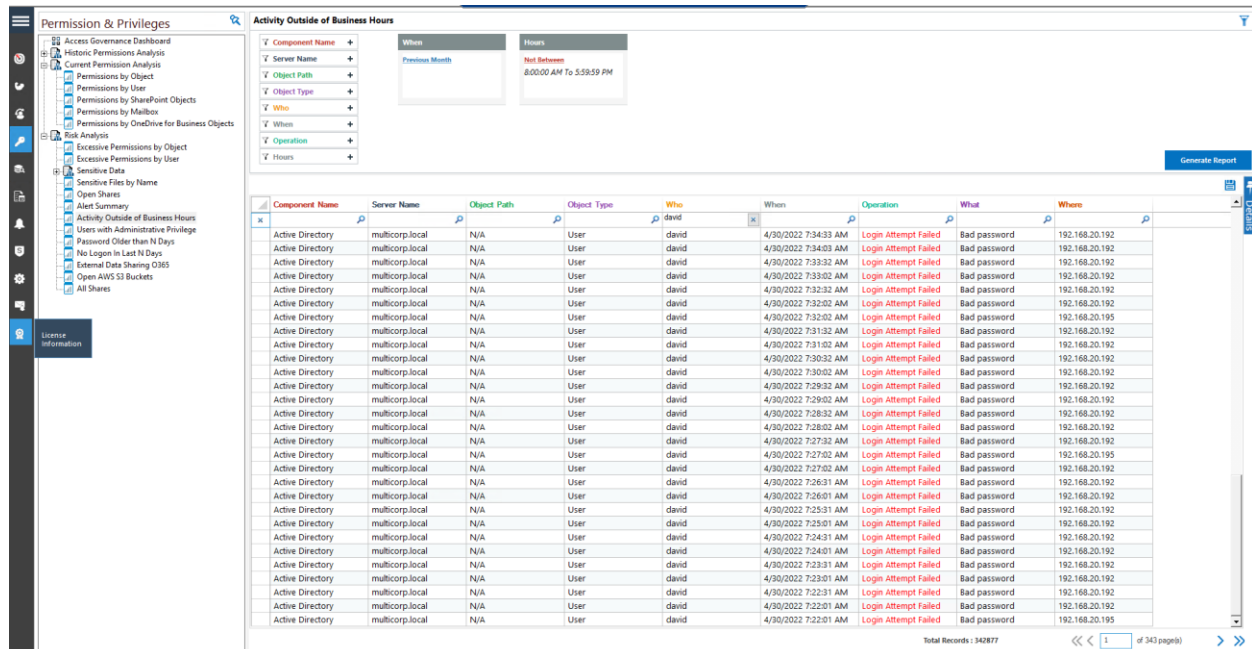


Figure 5: Activity Outside of Business Hours Report with Filtered Data

The report can be scheduled, saved, and exported.

4. 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.

4.1. Creating an Alert

If you want to be notified about out of hours activity you can set up an automated alert on the Activity Outside of Business Hours Report.

To set up an alert:

- Click the **Permission & Privileges**  icon
- A list of reports is displayed in a tree structure on the left-hand side of the screen
- Expand **Risk Analysis** (from the tree structure to the left side of the screen)
- Click on **Activity Outside of Business Hours** to display the **Activity Outside of Business Hours Report**
- Right click on the **Activity Outside of Business Hours Report** to display the context menu:

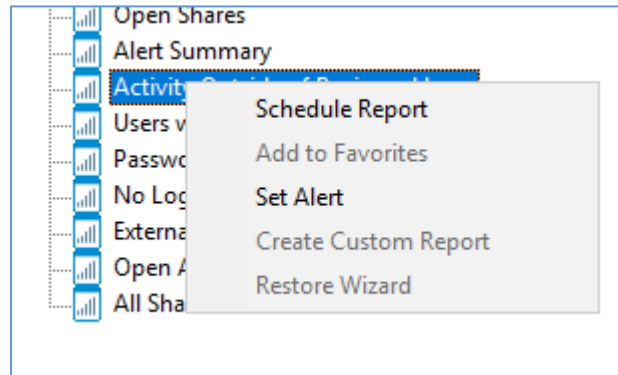


Figure 6: Context Menu

- Choose **Set Alert**

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

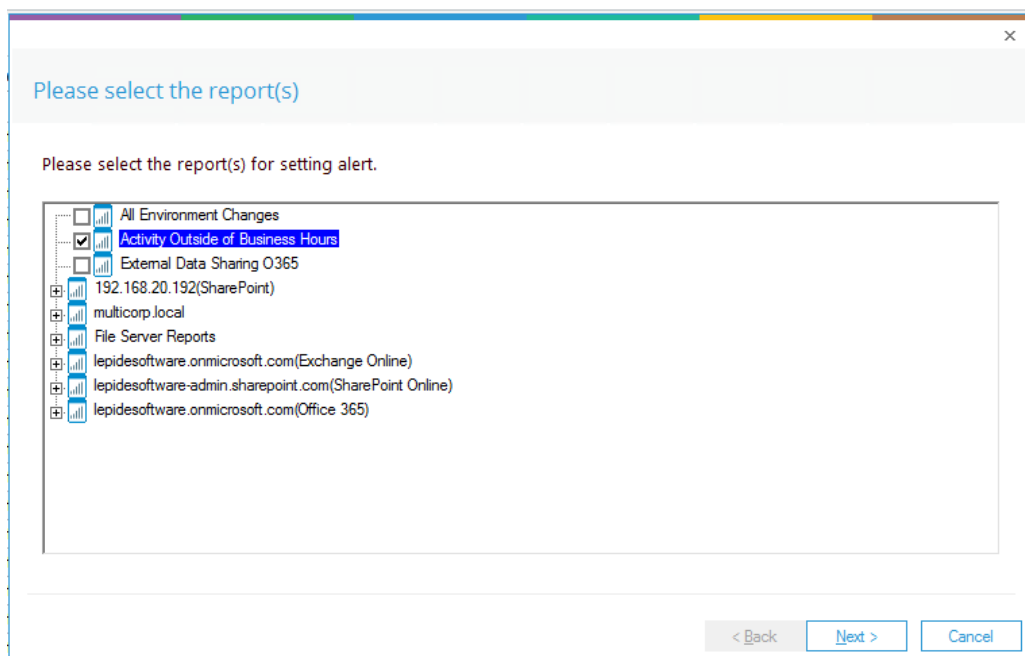


Figure 7: Select Reports

Ensure that the report on which you want to set an alert is checked. In this case, it is the Activity Outside of Business Hours Report.

- Click **Next**

The Set Filter(s) dialog box is displayed:

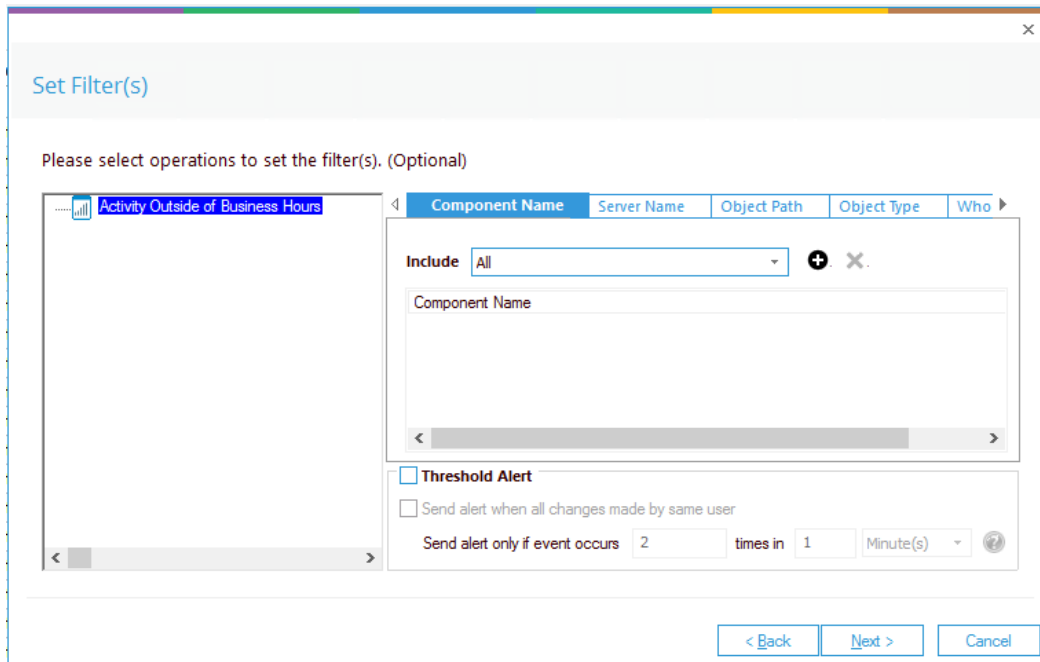


Figure 8: Set Filters

On the left of the dialog box, you can see the report you are working on which in this case is **Activity Outside of Business Hours**.

There are options to change the settings for **Component Name, Server Name, Object Path, Object Type, Who, Operation, and Hours** using the tabs at the top of this dialog box.

The threshold alert options can be customized as follows:

Threshold Alert: Check this box to switch threshold alerting on

Send alert 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:

[illegible]

Figure 9: 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 : JILL Add New Email Account

Recipient Email(s):

Separate multiple emails by ","

☐ Send Actions for past Days

Report Format

☐ CSV ☐ MHT ☐ PDF

OK Cancel

Figure 10: 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 **Send Email Alert**

Sender/Recipient **Show in LiveFeed**

Send Alert to App

Execute Script

ent(s).

Sender's Email Account : **JILL** **Add New Email Account**

Recipient Email(s):

Separate multiple emails by ","

☐ Send Actions for past Days

Report Format

☐ CSV ☐ MHT ☐ PDF

OK **Cancel**

Figure 11: Alert Action Options

The Alert Actions are:

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

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

1. Send Email Alert

The screenshot shows a dialog box titled "Add Alert Action" with a close button (X) in the top right corner. Inside the dialog, the "Select Action" dropdown menu is set to "Send Email Alert". Below this, a prompt reads "Please select or add new sender's email account, add recipient(s)". The "Sender/Recipient" section includes a "Sender's Email Account" dropdown menu currently showing "JILL" and an "Add New Email Account" button. The "Recipient Email(s)" section features a large text input area with scrollbars. Below the input area, a note states "Separate multiple emails by ','". Further down, there is a checkbox labeled "Send Actions for past" followed by a text input field for "Days". At the bottom, the "Report Format" section has three radio button options: "CSV", "MHT", and "PDF". The "CSV" option is selected. At the very bottom of the dialog are "OK" and "Cancel" buttons.

Figure 12: Add Alert Action - Send Email Alert

This option allows you to send an email once an alert has been triggered. The elements of the dialog box are as follows:

- | | |
|--------------------------------|--|
| Sender's Email Account: | The Sender's email account will be displayed here if it has been selected. Click Add New Email Account to enter a new Sender's Email Account |
| Recipient Email(s): | Add recipient emails by typing the email addresses into the box. If there are multiple email addresses, separate them with a ',' |
| Send Actions for past xx days: | This option allows you to see everything that this user has done over the last number of specified days. For example, if an alert is triggered because permissions have been changed for a sensitive document, you may want to see |

what else has been happening for that account. Check this box and specify the number of days and an email will be sent with an attachment listing everything that the user has done over the specified number of days.

The attachment will contain a report and the format(s) can be specified by checking the relevant box. The formats are CSV, MHT and PDF.

- Click **OK** to save the alert action.

2. Show in LiveFeed

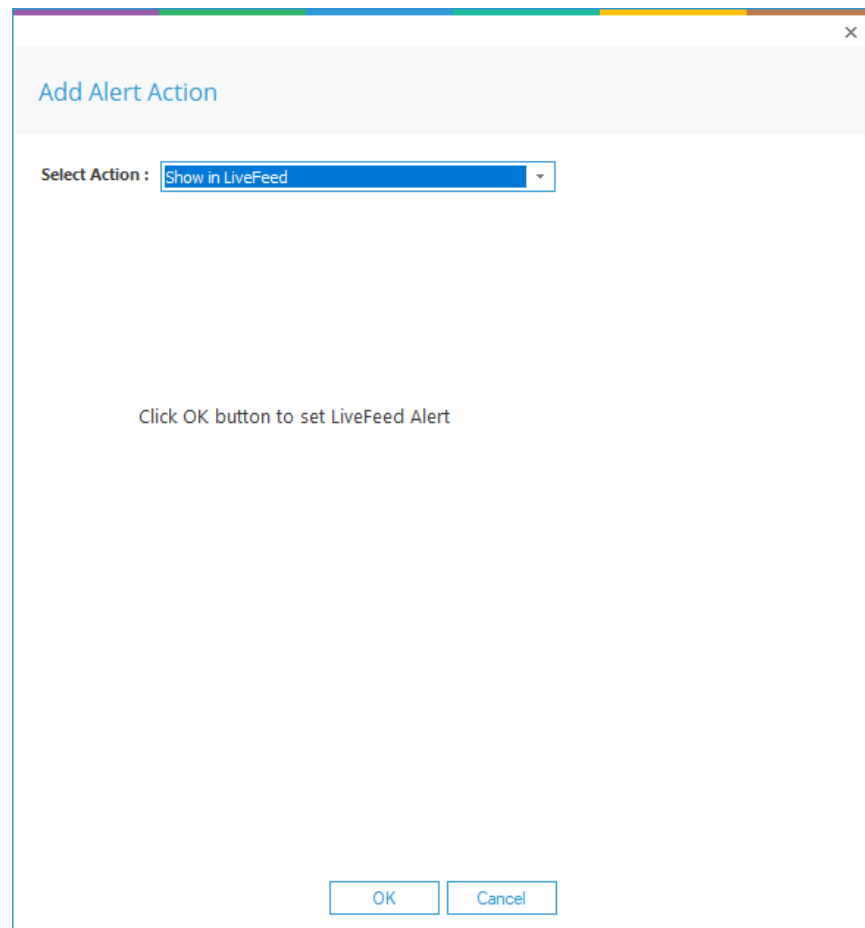
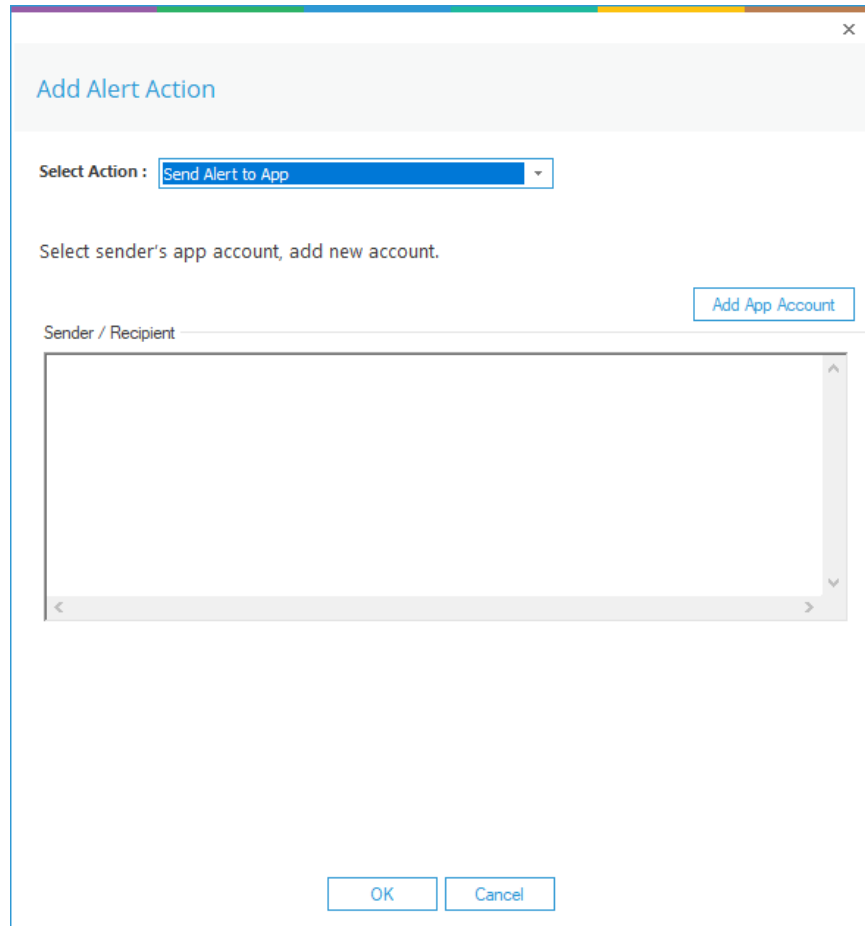


Figure 13: Add Alert Action – Show in LiveFeed

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.

Add App Account

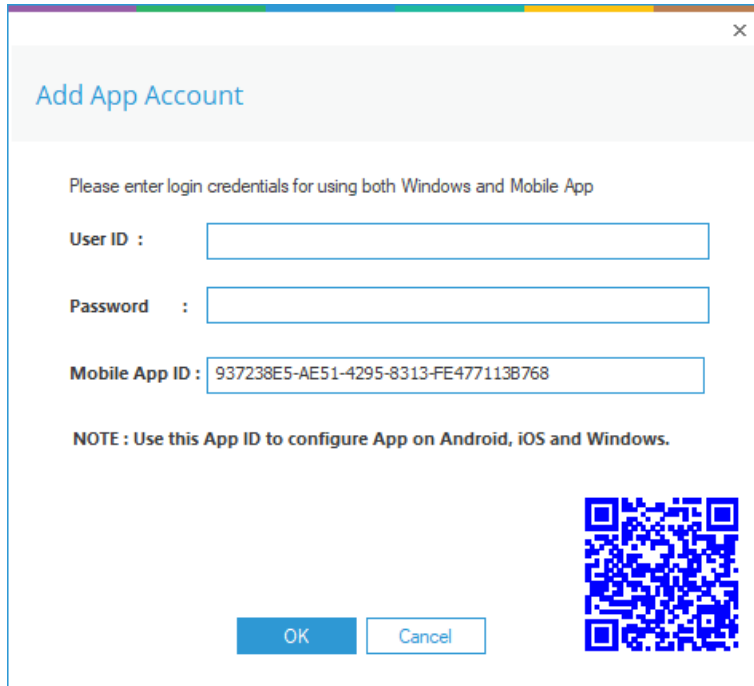
Sender / Recipient

OK Cancel

Figure 14: 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:



The image shows a software dialog box titled "Add App Account". It contains a header bar with the title and a close button (X). Below the header, there is a text prompt: "Please enter login credentials for using both Windows and Mobile App". This is followed by three input fields: "User ID :", "Password :", and "Mobile App ID :". The "Mobile App ID" field is pre-filled with the value "937238E5-AE51-4295-8313-FE477113B768". Below these fields is a note: "NOTE : Use this App ID to configure App on Android, iOS and Windows." At the bottom left are two buttons: "OK" and "Cancel". At the bottom right is a square QR code.

Add App Account

Please enter login credentials for using both Windows and Mobile App

User ID :

Password :

Mobile App ID :

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




Figure 15: 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

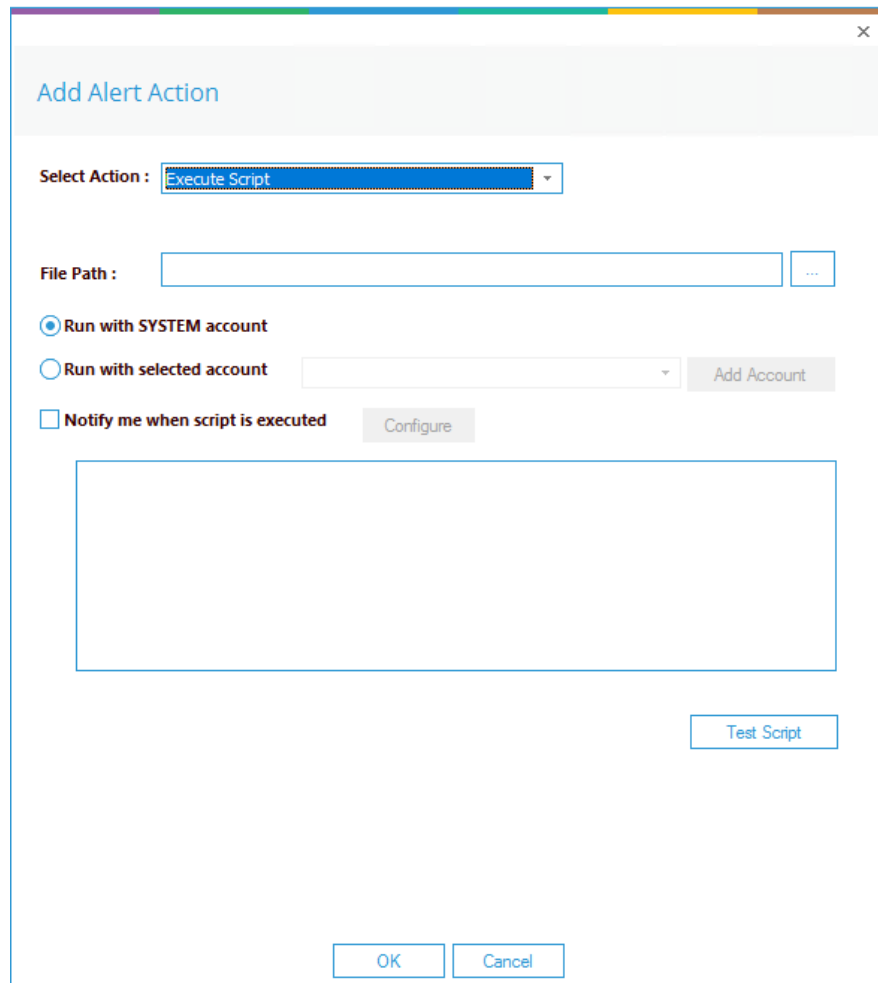

The image shows a Windows-style dialog box titled "Add Alert Action". At the top, there's a header bar with the title. Below it, a dropdown menu labeled "Select Action :" has "Execute Script" selected. Underneath, there's a "File Path :" label followed by a text input field and a browse button (three dots). Below that are two radio buttons: "Run with SYSTEM account" (which is selected) and "Run with selected account" (which is unselected). To the right of the second radio button is another dropdown menu and an "Add Account" button. Below these is a checkbox labeled "Notify me when script is executed" which is unselected, with a "Configure" button next to it. A large empty rectangular box occupies the middle section of the dialog. At the bottom right, there is a "Test Script" button. At the very bottom, there are "OK" and "Cancel" buttons.

Figure 16: Add Alert Action – Execute Script

The last action from the drop-down menu is **Execute Script**

This sets up the option to execute one of the predefined PowerShell scripts when an alert is triggered.

The elements of the dialog box are as follows:

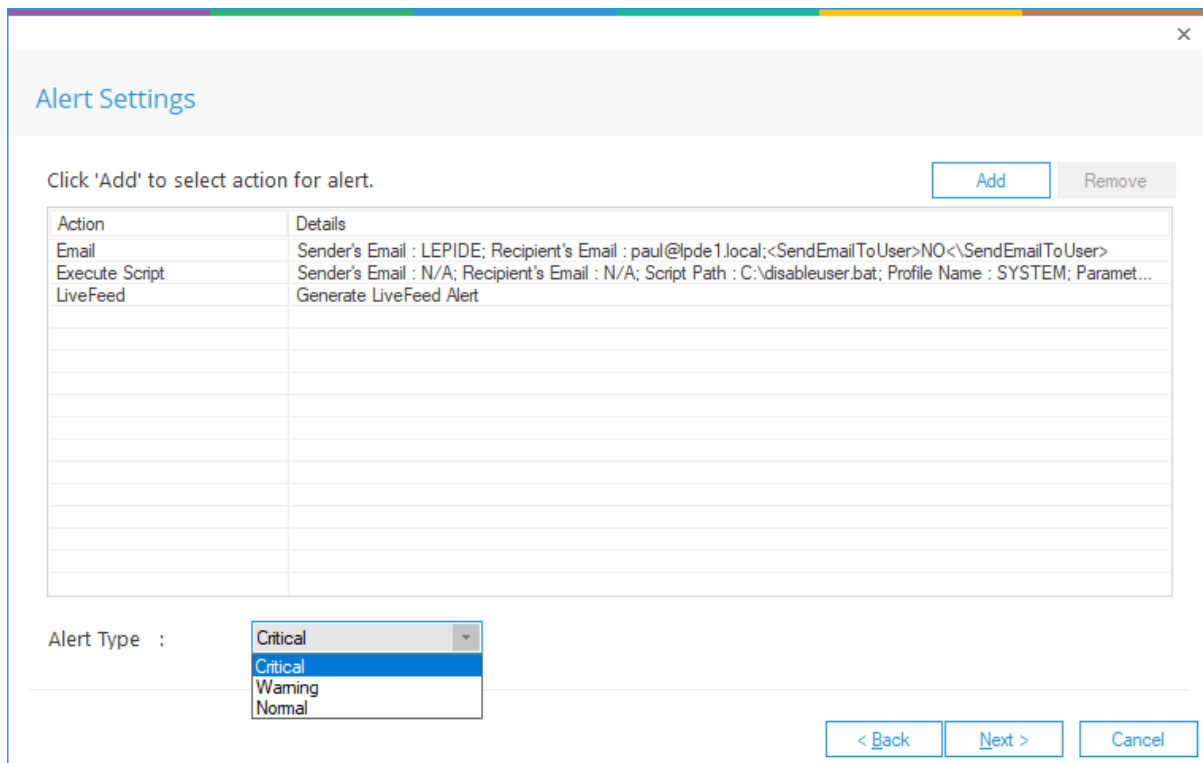
File Path: Browse to choose the file path of the PowerShell script by clicking 
Choose either **Run with SYSTEM account** or
Run with selected account.

If you choose **Run with selected account**, you can use the drop-down to select the account or click **Add Account** to specify the account to be used.

Choose **Notify me when a script is executed** to send an email on script execution.

When this option is checked, the **Configure** button becomes available. Choose **Configure** to set up the sender's account and recipient's email address.

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



The screenshot shows the 'Alert Settings' dialog box. At the top, it says 'Click 'Add' to select action for alert.' with 'Add' and 'Remove' buttons. Below is a table with two columns: 'Action' and 'Details'. The table contains three rows: 'Email' with details 'Sender's Email : LEPIDE; Recipient's Email : paul@lpde1.local;<SendEmailToUser>NO<\SendEmailToUser>', 'Execute Script' with details 'Sender's Email : N/A; Recipient's Email : N/A; Script Path : C:\disableuser.bat; Profile Name : SYSTEM; Paramet...', and 'LiveFeed' with details 'Generate LiveFeed Alert'. Below the table, there is an 'Alert Type' dropdown menu with 'Critical' selected. At the bottom right, there are '< Back', 'Next >', and 'Cancel' buttons.

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

< Back Next > Cancel

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 **Permission & Privileges** screen

5. Support

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

Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

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

sales@Lepide.com

support@Lepide.com

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

6. Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.