



USE CASE GUIDE

# HOW TO TROUBLESHOOT ACCOUNT LOCKOUTS

# Table of Contents

1	Introduction.....	3
2	Common Causes of Account Lockouts .....	3
3	How to Resolve Account Lockouts.....	4
4	The Lepide Solution.....	4
4.1	The Account Lockout Report.....	4
4.2	Account Lockout Investigator.....	5
5	Generating the Account Lockout Report .....	5
5.1	Unlock Accounts and Reset Passwords .....	7
	Unlock Account .....	7
	Reset Password.....	8
6	The Lepide Account Lockout Investigator Tool.....	9
6.1	Using the Lepide Account Lockout Investigator Tool.....	9
7	Support .....	11
8	Trademarks .....	23

# 1. Introduction

Active Directory auditing is an important part of ensuring compliance and the security of the IT environment. However, a common problem that Active Directory administrators face is how to identify the source of account lockouts. If a user account gets locked out for any reason, for example they may try and login with the wrong username, this can result in downtime, and it can often be a time consuming and frustrating process to find the source of the lockout and get the account re-enabled.

In this guide, we will look at some of the root causes of the account lockouts and ways to simplify the troubleshooting process.

## 2. Common Causes of Account Lockouts

Account lockouts are a common occurrence, and they can happen for several different reasons which is why finding the root cause can be very time consuming and challenging. Here are some of the common causes:

- Mapped drives using old credentials

Mapped drives can be configured to use user-specified credentials to connect to a shared resource. Afterwards, the user may change the password without updating the credentials in the mapped drive. The credentials may also expire, which will lead to account lockouts.
- Systems using old, cached credentials

Some users are required to work on multiple computers. As a result, a user can be logged on to more than one computer simultaneously. These other computers may have applications that are using old, cached credentials which may result in locked accounts.
- Applications using old credentials

On the user's system, there may be several applications which either cache the users' credentials or explicitly define them in their configuration. If the user's credentials are expired and are not updated in the applications, the account will become locked.
- Windows Services using expired credentials

Windows services can be configured to use user-specified accounts which are known as service accounts. The credentials for these user-specified accounts may expire and Windows services will continue using the old, expired credentials; leading to account lockouts.
- Scheduled Tasks

The Windows task scheduler requires credentials to run a task whether the user is logged in or not. Different tasks can be created with user-specified credentials which can be domain credentials. These user-specified credentials may expire, and Windows tasks will continue to use the old credentials.

### 3. How to Resolve Account Lockouts

Microsoft offers the Account Lockout Status (LockoutStatus.exe) tool to simplify the process of determining the account lockout status. This is a blend of command-line and graphical tools, but it is complex to use and can be time consuming.

## 4. The Lepide Solution

Lepide's Account Lockout capabilities simplify the process of identifying the account lockout status. The Lepide Solution ensures you can easily identify which accounts have been locked out, when the lockout occurred and examine which machine the account lockout has come from by generating the Account Lockout Report.

Once this report has been generated, the Lepide Investigator tool can be used to determine exactly what may have caused the lockout. With its built-in remote management capability, you can immediately unlock the account or reset the password.

This whole process makes it very easy to administer and maintain the status of user and service accounts within Active Directory – especially in crucial, time sensitive situations.

### 4.1. The Account Lockout Report

If a user does something to create an account lockout, for example they may try and login with the wrong username, this event is generated on the domain controllers. The Lepide Solution reads it from the domain controller and gives all the details for the lockout in the **Account Lockout Report**:

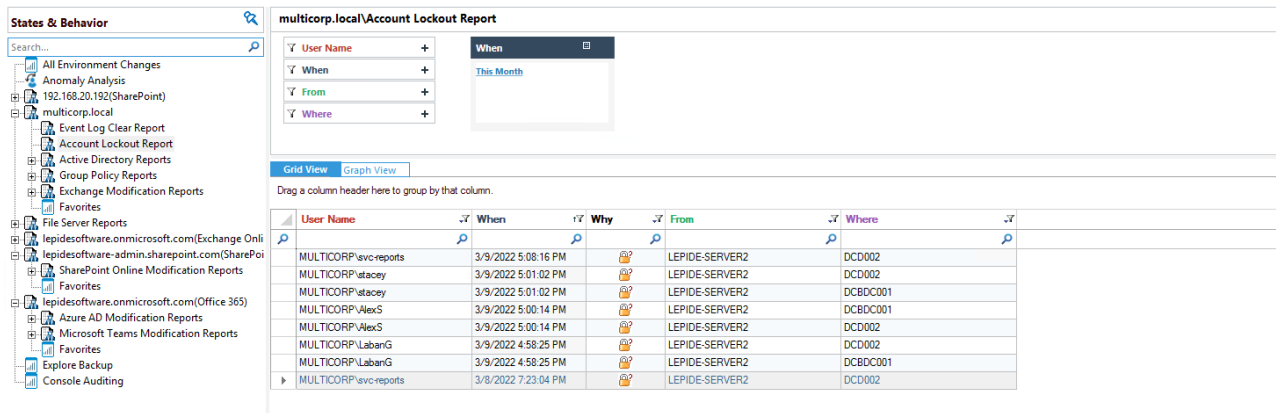


Figure 1: Account Lockout Report

## 4.2. Account Lockout Investigator

The Lepide Data Security Platform has a built-in module called the **Account Lockout Investigator** which you can use to find out the cause of any lockouts.

The Investigator tool notifies IT administrators about Active Directory account lockout issues. It helps to simplify and speed up investigations into the root cause of lockouts and provides the ability to unlock user accounts from within the tool itself.

### Key Features

- Detect account lockouts in real time
- Speed up investigation into the root cause
- Quickly unlock accounts through an intuitive interface
- Take the strain off your IT help desk
- Demonstrate compliance with your Active Directory lockout policy
- Fulfill SLAs by identifying lockouts to service accounts

## 5. Generating the Account Lockout Report


### 5.1. Prerequisites

Before reporting and alerting on account lockouts, you will need to have added and configured [Active Directory](#) to enable auditing.

Once this has been configured, you will be able to see all account lockout events as the Lepide Data Security Platform provides alerting and reporting in real time.

### 5.2. How to Run the Account Lockout Report

The Account Lockout Report identifies any account lockouts for a particular time-period. The report is generated as follows:

- Click the **User Entity & Analytics** icon  to display the **States & Behavior** window  
A list of reports is displayed in a tree structure on the left-hand side of the screen
- Expand the Active Directory node
- Click on the **Account Lockout Report**:

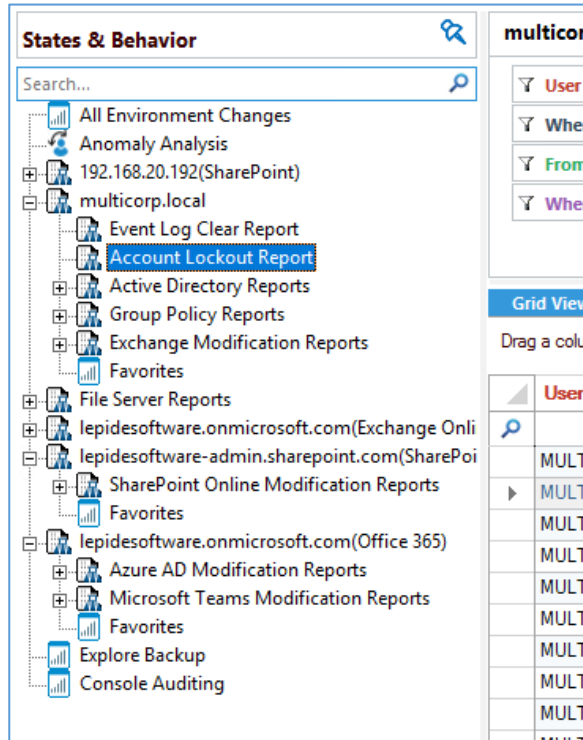


Figure 2: List of Reports

Click the **When** box and select a Date Range for the Report

- Click **Generate** to run the report

The Account Lockout Report is generated, and each row displays complete information about the lockout:

User Name	When	Why	From	Where
MULTICORP\svc-reports	3/9/2022 5:08:16 PM		LEPIDE-SERVER2	DCD002
MULTICORP\stacey	3/9/2022 5:01:02 PM		LEPIDE-SERVER2	DCD002
MULTICORP\stacey	3/9/2022 5:01:02 PM		LEPIDE-SERVER2	DCBDC001
MULTICORP\NexS	3/9/2022 5:00:14 PM		LEPIDE-SERVER2	DCBDC001
MULTICORP\NexS	3/9/2022 5:00:14 PM		LEPIDE-SERVER2	DCD002
MULTICORP\LabanG	3/9/2022 4:58:25 PM		LEPIDE-SERVER2	DCD002
MULTICORP\LabanG	3/9/2022 4:58:25 PM		LEPIDE-SERVER2	DCBDC001
MULTICORP\svc-reports	3/8/2022 7:23:04 PM		LEPIDE-SERVER2	DCD002

Figure 3: Account Lockout Report

The report includes the following:

- User Name**     The name of the user who’s account is locked out
- When**             The date and time of when the lockout occurred
- Why**                The reason why the lockout happened. Clicking the icon in this column takes you to the Investigator which is described below
- From**                The source machine where the account is being used to authenticate against the Active Directory
- Where**                The address of the domain controller where the authentication request is received

### 5.3. Unlock Accounts and Reset Passwords

Accounts can be unlocked, and passwords reset from within the Lepide solution. This can be done using the context menu:

- Right-click on a row to display the context menu relating to that specific row. This will give you the following options: Unlock, Reset Password and Investigate.

User Name	When	Why	From	Where
MULTICORP\svc-reports	3/9/2022 5:08:16 PM		LEPIDE-SERVER2	DCD002
MULTICORP\stacey	3/9/2022 5:01:02 PM		LEPIDE-SERVER2	DCD002
MULTICORP\stacey	3/9/2022 5:01:02 PM		LEPIDE-SERVER2	DCBDC001
MULTICORP\AlexS	3/9/2022 5:00:14 PM		LEPIDE-SERVER2	DCBDC001
MULTICORP\AlexS	3/9/2022 5:00:14 PM		LEPIDE-SERVER2	DCD002
MULTICORP\LabanG	3/9/2022 4:58:25 PM		LEPIDE-SERVER2	DCD002
MULTICORP\LabanG	3/9/2022 4:58:25 PM		LEPIDE-SERVER2	DCBDC001
MULTICORP\svc-reports	3/8/2022 7:23:04 PM		LEPIDE-SERVER2	DCD002

Figure 4: The Context Menu

### Unlock Account

- Click on this option to unlock the chosen user account. Once unlocked, it shows the following message:

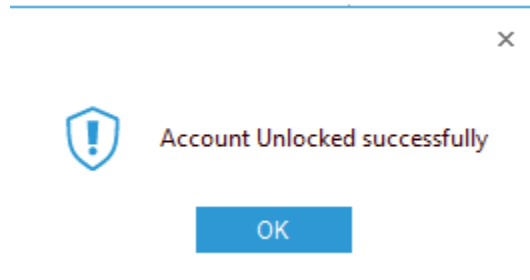


Figure 5: Account Unlocked Successfully

## Reset Password

To reset the users' password:

- Right click on the row of the user where the password needs to be reset.
- Click on **Reset Password** from the context menu.
- Enter the new password and then confirm it.
- Select the **User must change password at the next logon** option to force the user to change the password on the next logon.

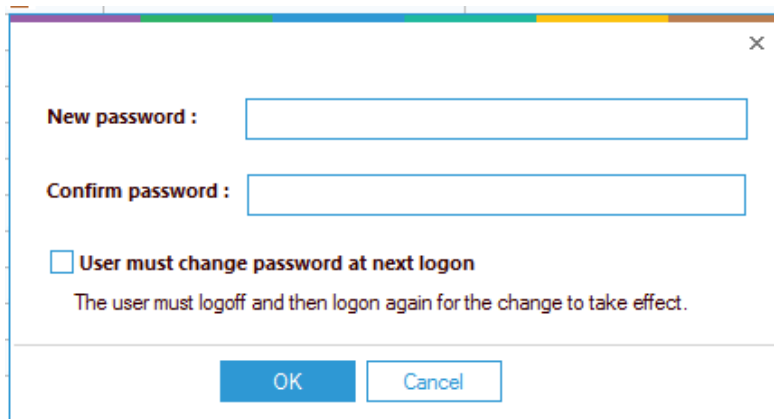


Figure 6: Reset Password



## 6. The Lepide Account Lockout Investigator

The Account Lockout Report gives you all the details for those accounts that are locked out. But you may also want to know what's causing the account lockouts. For this you can use the Lepide Account Lockout Investigator.

### 6.1. Using the Lepide Account Lockout Investigator

To use the Investigator Tool:

- From the context menu (right-click on a row to display this), choose **Investigate**  
A dialog box is displayed
- Click **Generate Report** to generate the report to view the reason behind the account lockout:

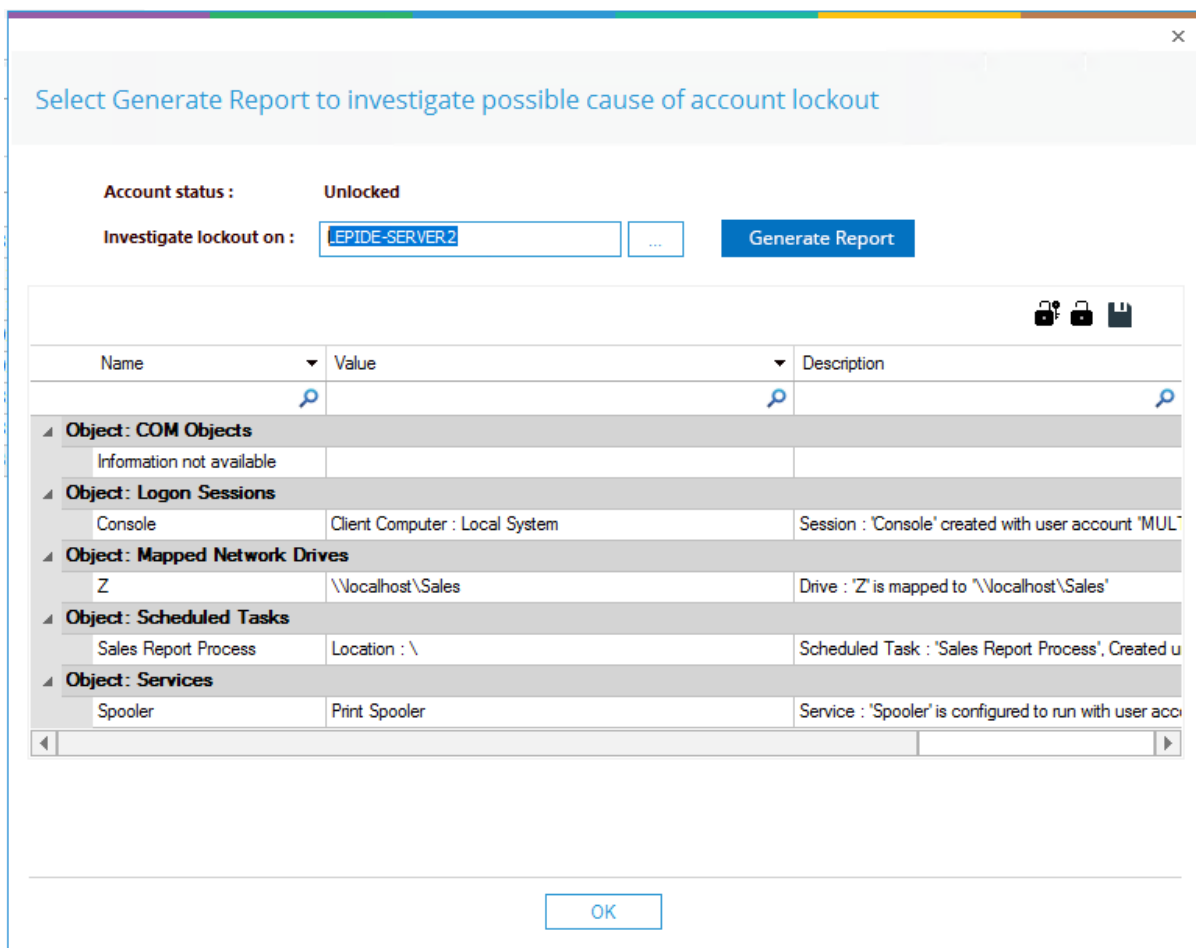





Figure 7: Lockout Investigator

The solution will look at the following 5 areas to find out where the account lockout has taken place:

- **Computer Objects:** Any computer objects which relate to those credentials
- **Mapped Network Drives:** Whether there is a mapped network drive with that user account on that machine
- **Services:** Any Services which are present on those machines which are using those credentials to logon
- **Scheduled Tasks:** Any scheduled tasks which are configured to run on a daily, weekly, or monthly basis which are using those credentials. Maybe an old password is being used and this will cause an account lockout.
- **Logon Sessions:** Whether there are any active logon sessions with those credentials


From the Lockout Investigator dialog box, you can do the following:

- Click the Unlock Account icon  to unlock the account
- Click the Reset Password  icon to reset the password
- Click the Save Report icon  to save the report.  
When you select this option, a dialog box is displayed. You can choose where to save the report and the file format to save it in which can be .pdf, .csv and .mht.

## 7. Creating an Alert on the Account Lockout Report

If you want to be notified as soon as an account has been locked out, you can set up an automated alert on the Account Lockout Report.

To set up an alert:

- Click the **User Entity & Analytics** icon  to display the **States & Behavior** window  
A list of reports is displayed in a tree structure on the left-hand side of the screen
- Expand the Active Directory node
- Right click on the **Account Lockout Report** to display the context menu  
The context menu is displayed:

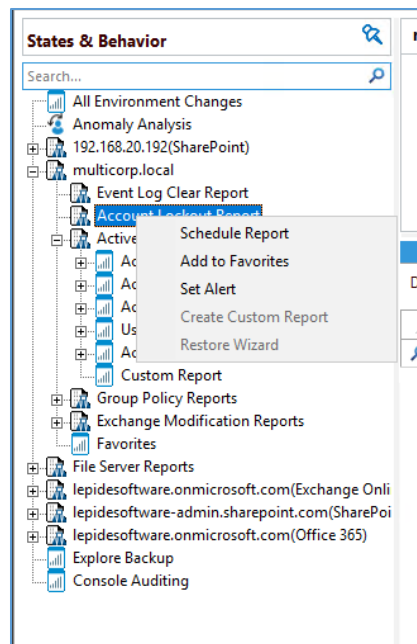


Figure 8: Context Menu

- Choose **Set Alert**

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

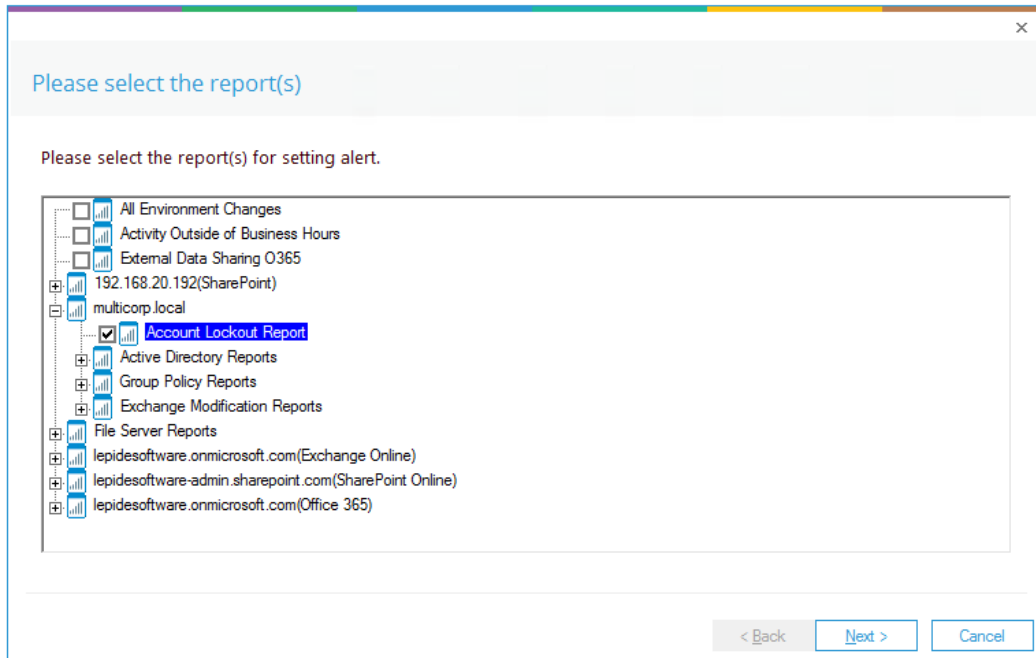


Figure 9: Select Report(s)

Ensure that the report on which you want to set an alert is checked. In this case, it is the Account Lockout Report.

- Click **Next**

The Set Filter(s) dialog box is displayed:

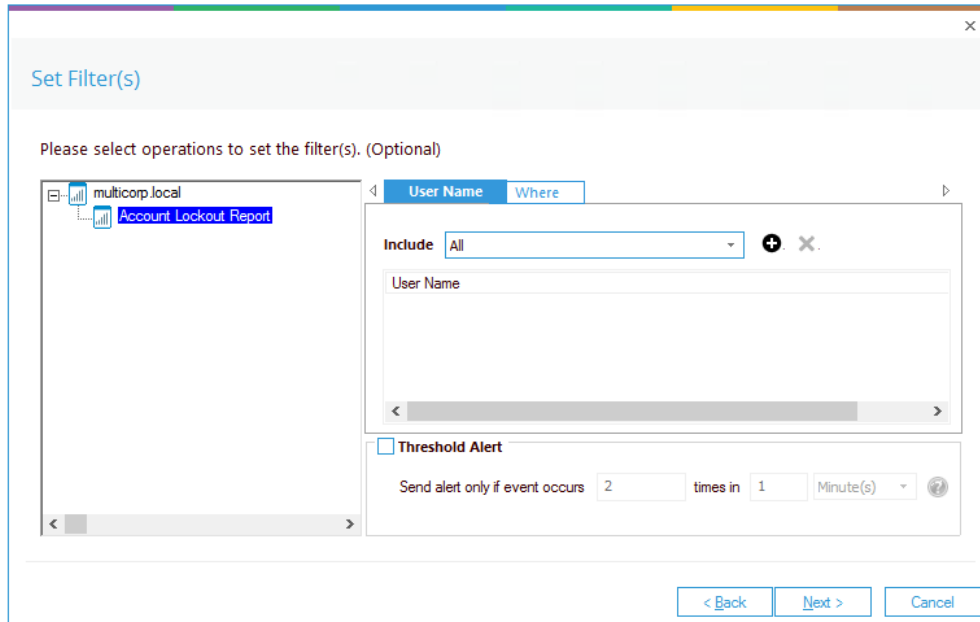


Figure 10: Set Filter(s)

On the left of the dialog box, you can see the report you are working on which in this case is **Account Lockout**. There are options to change the settings for **User Name** and **Where** using the tabs at the top of this dialog box. The default setting for both options is **All**.

The threshold alert options can be customized as follows:

- Threshold Alert:** Check this box to switch threshold alerting on
- Send alert only if event occurs:** Enter 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.

Add Remove

Action	Details

Alert Type : Critical

< Back Next > Cancel

Figure 11: 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:

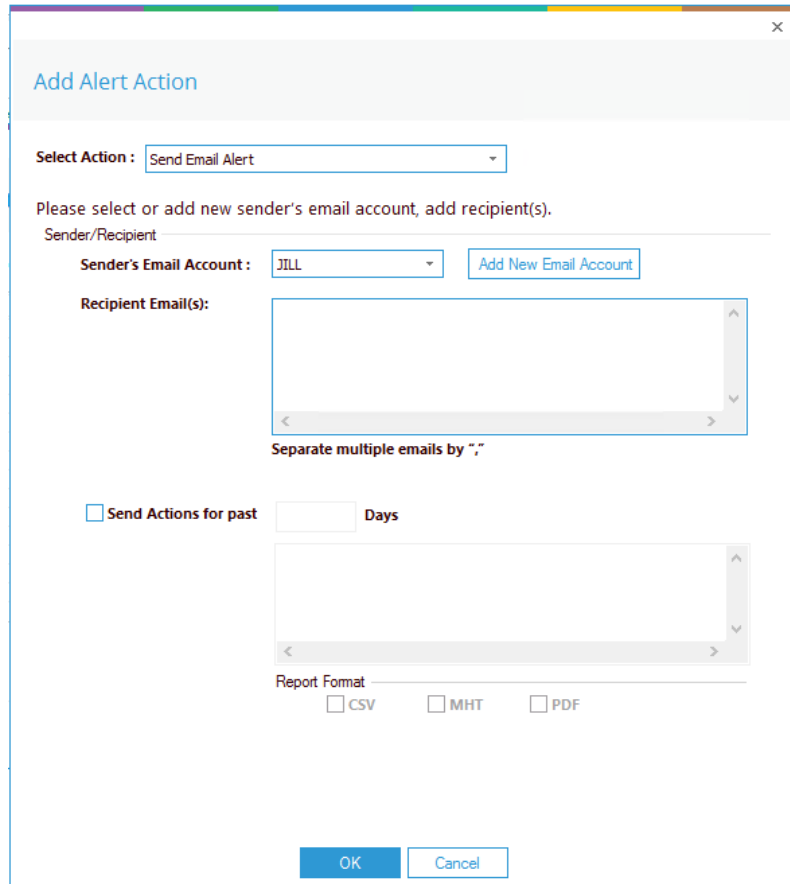


Figure 12: Add Alert Action

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

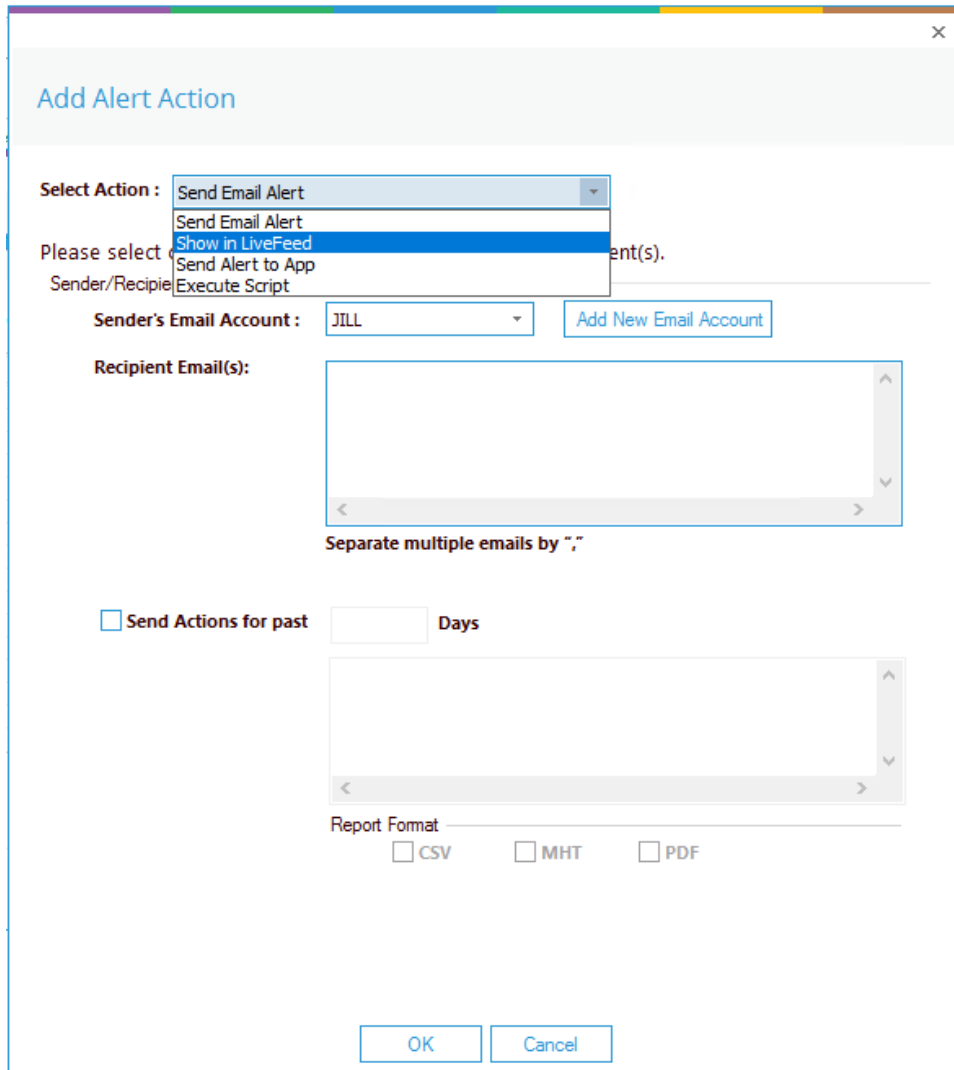


Figure 13: Add Alert Action Options

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

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

Figure 14: 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 ','

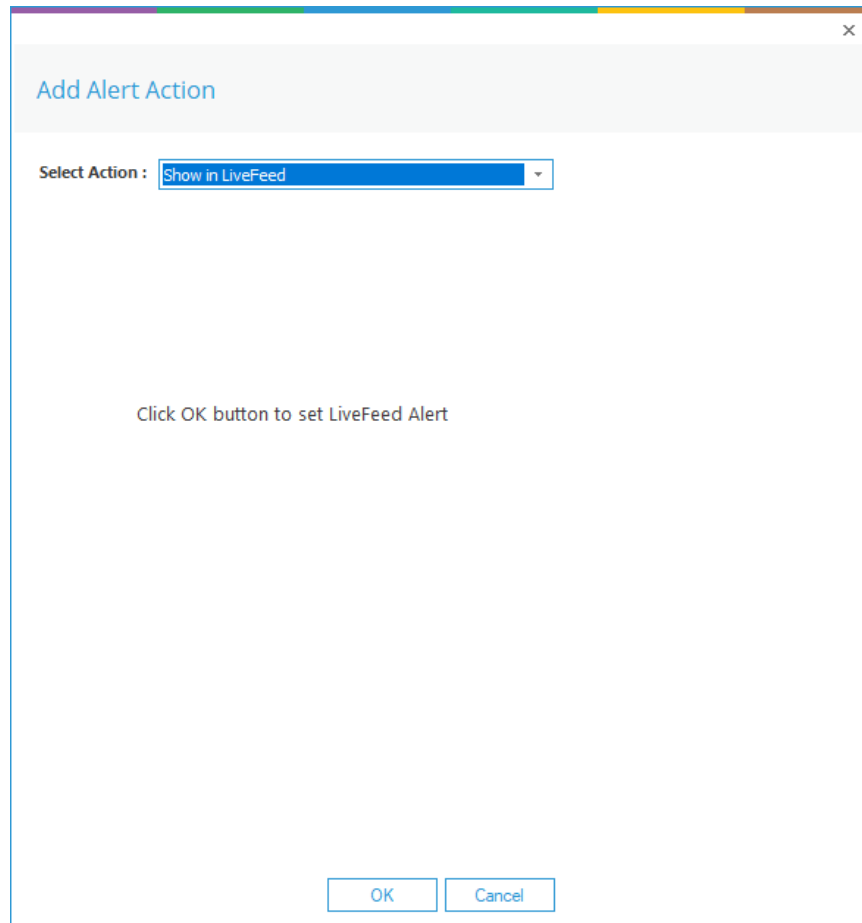
**Send Actions for past xx days:** This option allows you to see everything that this user has done over the last number of specified days. For example, if an alert is triggered because an account has been locked out, then you may want to see what else has been happening for that account. Check this 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

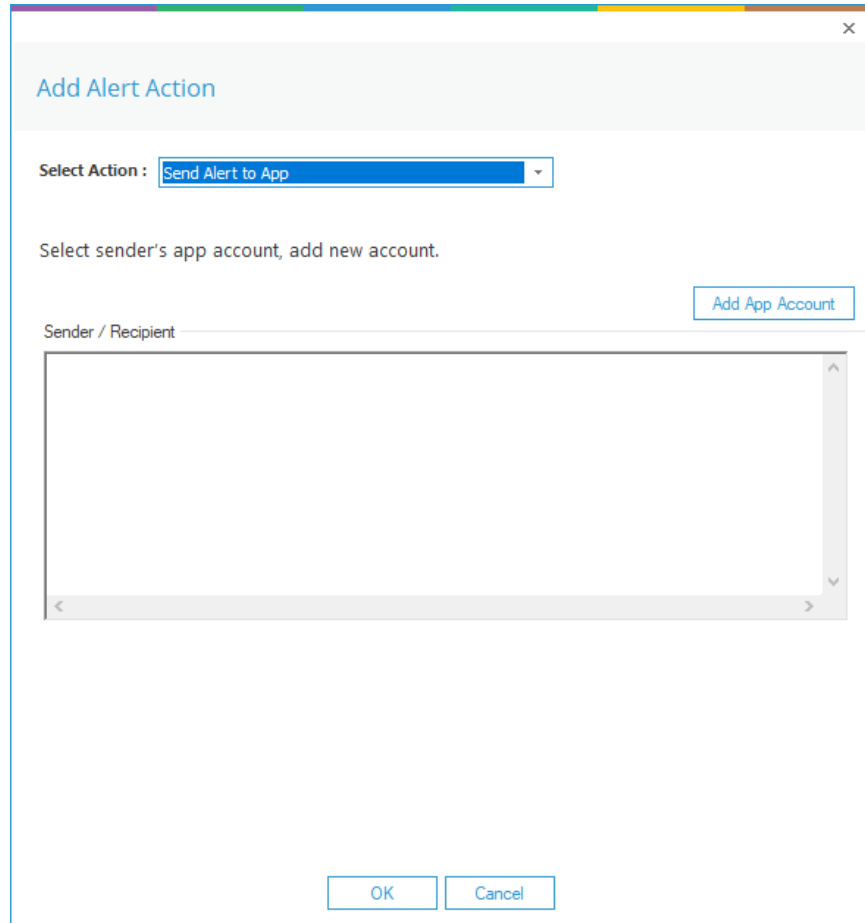


**Figure 15: Add Alert Action – Show in LiveFeed**

**Show in LiveFeed** means that the alert will be sent to the Lepide dashboard.

- Click **OK** to switch the **LiveFeed** alert on.

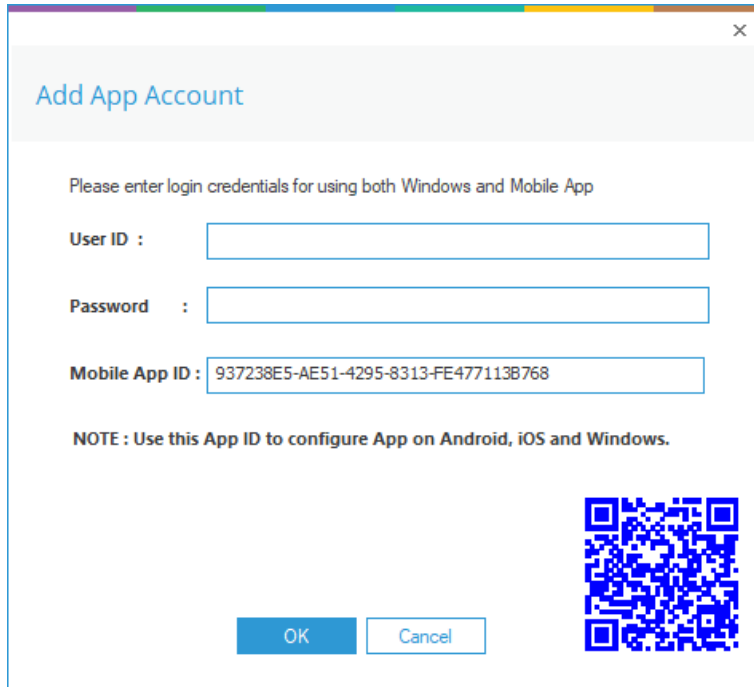
3. Send Alert to App



**Figure 16: Add Alert Action – Send Alert to App**

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

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



**Figure 17: Add App Account**

- Enter the **User ID** and **Password**
- Enter the **Mobile App ID** which is generated by using the mobile device to scan the QR code displayed at the bottom of the dialog box.
- Click **OK**

## 4. Execute Script

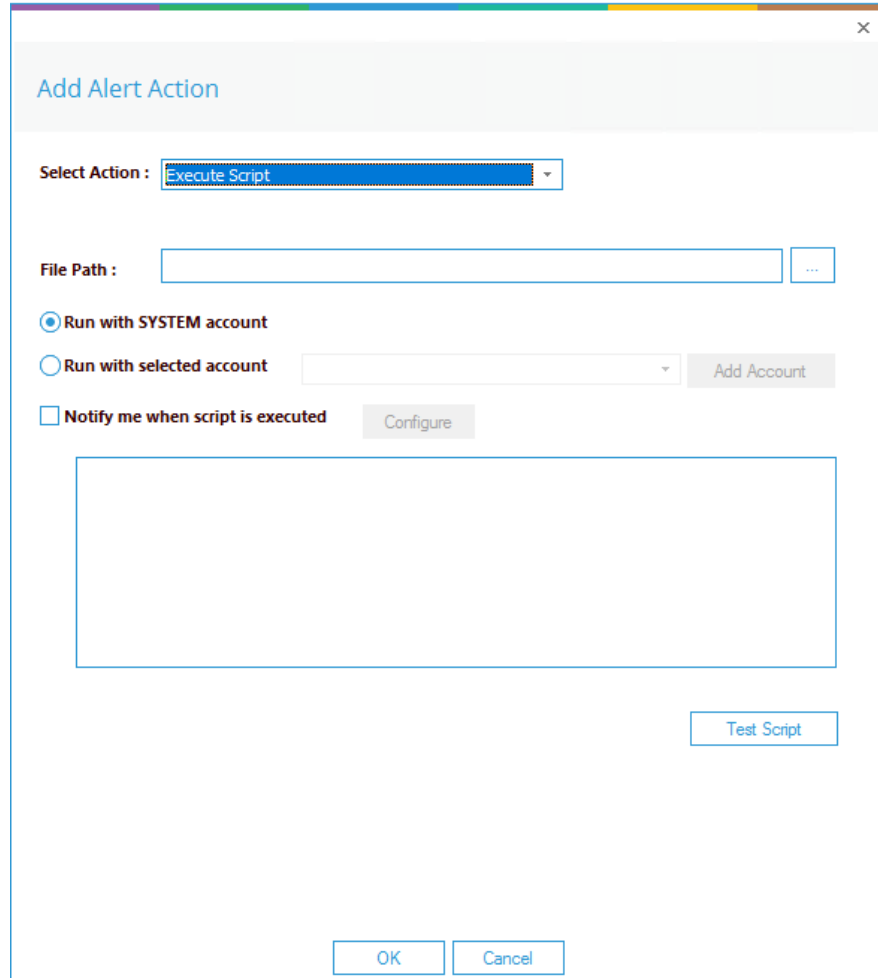


Figure 18: Add Alert Action – Execute Script

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, there is a title bar with a close button (X). Below the title bar, the text 'Alert Settings' is displayed. Underneath, there is a prompt: 'Click 'Add' to select action for alert.' To the right of this prompt are two buttons: 'Add' and 'Remove'. Below this is a table with two columns: 'Action' and 'Details'. The table contains three rows of data:

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

Below the table, there is a label 'Alert Type :' followed by a dropdown menu. The dropdown menu is open, showing three options: 'Critical', 'Warning', and 'Normal'. At the bottom right of the dialog box, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**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.

## 8.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](mailto:sales@Lepide.com)

[support@Lepide.com](mailto:support@Lepide.com)

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

## 9.Trademarks

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.