%Lepide

USE CASE GUIDE

HOW TO REPORT AND ALERT ON FILES BEING COPIED

Table of Contents

1.	Introduction	.3
2.	Why Monitor the Copying of Files?	.3
3.	The Solution	.3
	3.1. The File Copy Report	.3
	3.2. The Mass Data Copy Threat Model	.3
4.	Configuring File Copy Reporting and Alerting	.4
	4.1. Prerequisites	.4
	4.2. Running the File Copied Report	.4
	Specify a Date Range	.5
	Specify a File Server	.5
	Filtering the Report	.6
	4.3. Threat Models	.7
	Responding to a Threat	.8
	4.4. How to Enable and Configure the Mass Data Copy Threat Model	.8
4. Su	pport	21
5. Tra	ademarks	21

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 <u>Windows File Server</u> 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

💥 Lepide Data Security Platform							- 0 ×
🚍 States & Behavior 🔍	File Server Reports\File Copies	d					¥ 🗹
Access Acce	T Wes ● T Server Name ● T Object Path ● T Process Name ● D Object Object Path ● Ø Wess *** Ø Wess *** Ø Wess ***	hd olune.	2017 Name 135, 486,83,53 X (Clippet Name P	े (Gues Part) P	af Queration P	\vec{x} Process Name \vec{x} From \vec{p} \vec{p}	Consult Report
States & Behavior Benalatore Compliance							
Restore	4				Total Records : 0	<< 1 of 1 page(b)	> >>
a 2 0 😂 🖬 🌖 💥						- .	4 912 PM

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:



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:

Server Na	me Filter		×
Select Server :	102 168 20 102	-	
	192.100.20.195		
Include this :	server :		
	OK Cased		
	OK Cancel		

Figure 3: Server Name Filter

- Click OK
- Click Generate Report



States & Behavior	File Server Reports\File	Copied							
Search	V When	+ When	G Server Na	me					
All Environment Changes	V Server Name	· Castors Data Ka	192, 168, 20	192					
Anomaly Analysis	7 100-	4 6/1/2021 12:00	AM To						
(a 192.168.20.192(SharePoint)	10.000	7/31/2021 120	ND AM						
P File Securities	¥ Object Name	•							
File Server Modification Reports	T Chevit Path	*							
All Modifications in File Server	V Operation	 (*) 							
- All Modifications in Shared File and Folder	2 Process Name	+							
All Modifications in Long File Path File Copied Read Successful Read Failed									Generate
- File and Folder Created	Grid View Graph View								
File and Folder Creation Failed	Drag a column header here to	group by that column.							H
- File and Folder Renamed	al When	17 Server Name	J Who J	7 Object Name	J Direct Path	J Operation	J Process Name	of From	3
File and Folder Moved	9	0	0 0	2	P	9	Ø	0	Q
Permission Reports	7/19/2021 8:02 12 PM	192 168 20 193	MULTICORP Adventuation	Regional apita viex	E 'Multicop'/Government'Confidential	File Copy	System	192,168,20,197	
Shared Folder Created and Deleted	7/12/2021 2 26 01 PM	192 168 20 193	MULTICORP & Corportor	RRAS Servers of	E \Muticop\Technolog\JT\Network Data	File Copy	System	192,168,20,192	
Di Custom Report	7/12/2021 2:26:01 PM	192 168 20 193	MULTICORP-Ext_Contractor	Renote Users docx	E \Muticop\Technolog/\JT\Network Data	File Copy	System	192 168 20 192	
Repidesoftware.onmicrosoft.com(Eschange Online)	7/12/2021 2:26:01 PM	192 168 20 193	MULTICORP.Ext_Contractor	Switches.alpr	E \Muticop\Technolog\/JT-Network Data	File Copy	System	192.168.20.192	
lepidesoftware-admin.sharepoint.com(SharePoint Onlir	7/12/2021 2:26:01 PM	192.168.20.193	MULTICORP-Ext_Contractor	Routers door	E \Muticop\Technolog\\T\Network Data	File Copy	System	192 168 20 192	
kpidesoftware.onmicrosoft.com(Office 365)	7/12/2021 2:26:01 PM	192 168 20 193	MULTICORP-Ed_Contractor	Computerendex	E \Mu8cop\Technolog\\T\Network Data	File Copy	System	192 168 20 192	
Explore Backup	7/12/2021 2:26:00 PM	192.168.20.193	MULTICORP-Ext_Contractor	Designa potx	E-\Muticop\Technolog/\JT\Network Data	File Capy	System	192 168 20 192	
Console Auditing	7/12/2021 2:26:00 PM	192 168 20 193	MULTICORP Ext_Contractor	Hardware bit	E-Muticop\Technolog/JT/Network Data	File Copy	System	192 168 20 192	
	7/12/2021 2-26:00 PM	192.168.20.193	MULTICORP-Ed_Contractor	IP Addresses.xtsx	E:\Muticop\Technolog\UTVNetwork Data	File Copy	System	192 168 20 192	
	7/12/2021 2:26:00 PM	192 168 20 193	MULTICORP.Ed_Contractor	License Details.stor	E:\Muticop\Technolog\UT\Network Data	File Copy	System	192.168.20.192	
	7/12/2021 2:26:00 PM	192 168 20 193	MULTICORP-Ext_Contractor	Passwords.txt	E-\Muticorp\Technolog\VT\Network Data	File Copy	System	192.168.20.192	
	7/12/2021 2:25:00 PM	192 168 20 193	MULTICORP Ed_Contractor	Parters dock	E \Muticorp\Technolog\UT\Network Data	File Copy	System	192 168 20 192	
	7/12/2021 2:29:00 PM	192 168 20 193	MULTICORP Ext_Contractor	Frewall Settings doox	E-Muticop\Technolog\UTVNetwork Data	File Copy	System	192,168,20,192	
	7/12/2021 2 25:00 PM	192 168 20 193	MULTICORP.Ed_Contractor	Network Design.bmp	E 'Muticop\Technolog/UT\Network Data	File Copy	System	192,168,20,192	
	7/8/2021 1:55 18 PM	192.168.20.193	MULTICORPVillan	Resident lats dock	E.\Muticop\Government\Confidential	File Copy	System	192.168.20.197	
	7/8/2021 1 19:36 PM	192.168.20.193	MULTICORPVNen	Client portfolio New potx	E.\Muticop\Financial Services\Finance	File Copy	System	192.168.20.197	
	7/8/2021 12:28:04 PM	192 168 20 193	MULTICORP View	Part time visis	E \Multicorp\Education\Students	File Copy	System	192 168 20 197	
	7/8/2021 12:05:20 PM	192 168 20 193	MULTICORPURat	Customer list pots	E:/Muticop/Vinancial Services/Finance	File Copy	System	192 168 20 197	
	7/b/2021 11:54:57 AM	192.168.20.193	MULTICORPURen	Client portfolio New pptx	E-Multicop/Financial Services/Finance	File Copy	System	192.168.20.197	
	7/6/2021 11:54:56 AM	192 168 20 193	MULTICORP Vian	Client portfolio pptx	E 'Muticop/Financial Services/Finance	File Copy	System	192.168.20.197	
	7/8/2021 11:49:11 AM	192 168 20 193	MULTICORP Vien	Policies poly	E Multicop/Healthcare/Patients	File Copy	Sydwin	192.168.20.197	
	7/7/2021 6:29:48 PM	192 168 20 193	MULTICORPVAIM	Doctor contact details also	E 'Muticop'/Heathcare/Patients	File Copy	System	192.168.20.197	
	6/24/2021 10:10:28 AM	192 168 20 193	MULTICORP-Paul	Payment bd encrypt	E 'Muticop'Heathcare'Accounts'/Payroli	File Copy	System	192 168 20 195	
1 (AAAAAA)	6/24/2021 10:18:28 AM	192.168.20.193	MULTICORP'/Paul	Paseword bit encrypt	E 'Mullcop Vieathcare'Accounts'/Payrol	File Copy	System	192,168,20,195	
	6/24/2021 10:18:28 AM	152.168.20.193	MULTICOMPIPaul	tmatAddresses til encrypt	E: Muticop Vieathcare Accounts Payol	File Copy	System	192.168.20.195	
States & Behavior	6/24/2021 10 17 17 AM	182 168 20 193	MULTUOHPVPau	Password bit encrypt	E Multicop Viestricare Viccounts/Payrol	File Copy	System	192 168 20 195	
	6/24/2021 10:17:17 AM	192.168.20.193	MULTICORP'Pad	Payment bit encrypt	E Indicop visaticale viccourts Payos	File Copy	System	192 168 20 195	
Angunatory Compliance	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	146.160.20.100	AND I COMPANY	Fride registered of evolution	 In many vesticare veccure insystemeters 	The Copy	Skaren	132 190 20 195	
O Restore						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:

Who	-7
Gemma	×
Firmer Fr Filter Area	

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):



rtes & Behavior 😵	File Server F	ieports\All M	Indifications in File 1	lerver									1
nh. p	7 When		+ When	10	Server Na	-							
All Environment Changes	T Server No	-	* Caston De	in Gerge	192,558,21	191							
Anomaly Analysis	7 1000		+ 6/1/2021	1200 AM To									
Stor His 20, 19(2) Arene (19)	T Count to	-	1/31/2021	12:00 AM									
File Server Reports	T. Ospertin												
File Server Modification Reports	a commenter		-										
All Modifications in File Server	V Content 1	Abs	*										
Al Modifications in Long File Bath	¥ Complian	et.	+										
File Copied	7 Monetary	Walae	+										
Read Successful	T Operation		+										
Read Failed	V Event Sta	hin :	+										
Ela and Folder Created	7 Process N	and a											
Permission Reports Shared Folder Created and Deleted File and Folder Property Change Guttom Report	Grid View Drag a column h	Graph View	true by that column.									8	1
lepidesoftware.onmicrosoft.com(Exchange Online)			J Server Name	J Who	6	Chievel Name	J Cligant Fully	of Content Type	J Fisk Level	of Complement	of Monstary Value	J Operation	
lepidesoftware-admin.sharepoint.com/SharePoint Onlo	*		P	,o Gennal	18		9	,p am	×	Q	P	P	
lepidesoftware.onmicrosoft.com(Office 365)	6/23/2021	82152 PM	192.168.20.193	MULTICORPIGer	1014	Confidential pdf	E-Mutcop/Inancial Ser	w. 55N	1512	GLBA + NPPI	\$2472	File Field	
Explore Backup Console Audition	6/23/2021	8.21.52.PM	192 168 20 193	MULTICORP.Ger	ana -	Confidential pdf	E'Multicop/Feancial Ser	w SSN	1512	OLEA + NPPI	\$ 2472	File Copy	
Country Participa	6/23/2021	82152PM	152.168.20.193	MULTICORP-Get	nna .	Experses.xtsr	E.'Muticop/Financial Ser	vi SSN + Names	708	GLEA + NPP1	\$ 2124	File Flead	
	6/23/2021	#21:52 PM	192 166 20 193	MULTICORP.Ger	nna	Expenses vise	E: Wutkcorp Financial Ser	v. SSV + Names	708	GLEA + NPPI	\$ 2124	File Copy	
	6/23/2021	8.21.52 PM	152 168 20 193	MULTICORP Ger	ana .	investments pptx	E'Muticog/Financial Ser	w. SSN	459	GLEA + NPPI	\$ 1105	File Field	
	6/23/2021	8.21.52.PM	192 168 20 193	MULTICORP Ger	wna .	investments ppts	E.'Mutoop:Friancial Ser	w. SSN	459	GLEA + NPPI	\$ 1105	File Copy	
	6/23/2021	8.21.52 PM	192,168,20,193	MULTICORP/Ger	whe .	Legal.bt	E'Muticog/Financial Ser	w	864	GLBA + NPPI	\$ 2080	Re Read	
	6/23/2021	821.52 PM	152 168 20 193	MULTICORP Ger	whet .	Legal bit	E-'Multicorp'/Pinancial Ser	v. 55N	864	GLEA + NPPI	\$ 2080	File Copy	
	6/23/2021	821.52 PM	192 168 20 193	MULTICORP\Ger	nne .	Passport crokes.pdf	E (Multicorp) Financial Ser	w. SSN	1404	GLBA + NPPI	\$ 3380	File Read	
	6/23/2021	8.21.52.PM	132 168 20 193	MULTICORP\Ger	inte .	Passpot copies pdf	E'Mutcop/Financial Ser	w. SSN	1404	GLEA + NPPI	\$ 3380	File Copy	
	4/23/2021	8-21-52 PM	152 168 20 793	MULTICORP Ger	NT4	Investments.pptx	E'Muticop/Priancial Ser	vi	459	GLEA + NPPI	\$ 1105	File Copy	
	6/23/2021	8.21.52 PM	132 168 20 193	MULTICORP Gen	ana .	Legal bit	E.'Muticop'/inancial Ser	v. 55V	564	GLEA + NPPI	\$ 2080	File Copy	
	6/23/2021	8-21-52 PM	152.168.20.153	MULTICORP-Gen	nte .	Expenses xits	E.'Mubcop/Financial Ser	vi. SSN + Names	708	GLEA + NPPI	\$ 2124	File Copy	
	6/23/2021	0.21.52.PM	192 168 20 193	MULTICORP Gen	nne .	Confidential pdf	E'Muticop'Friancial Ser	w. 55%	1512	GLEA + NPPI	\$2672	File Copy	
	6/23/2021	8.21.50 PM	192,168,20,193	MULTICORP Ger	what .	Passpot copies pdf	E 'Muticoty' Financial Ser	v. \$94	1404	GLEA + NPPI	1 3000	File Copy	
	5/23/2021	#2150 FM	192.168.20.193	MULTICORP Ger	what is	Experiees Xisk	E. Mutoop Financial Ser	v. SSN + Names	708	GLEA + NPPI	8 2124	File Copy	
	a dia make	THE REPORT OF LAND	192.168.20.193	MULTICORP Ger	what .	Contownarpdf	E. Mutoop Snandal Ser	N. 224	1942	ULEA + NPPI	12472	He Colly	
	6/23/2021			INT & TICORP Gas	where the	Legalise	E. Muticorp Financial Ser	W. 53W	864	ULBA + NPPI	12080	The Copy	
	6/23/2021	8.21.50 PM	192 168 20 193						15.12	DLEA = NPPI	\$ 24/2	File Field	
•	6/23/2021 6/23/2021 6/23/2021	82150 PM 82147 PM	192 168 20 193 192 168 20 193	MULTICORP/Ger	nne .	Confidential pdf	E 'Muticoty'/Inancel Ser	M_ 55N	inter a		a 21/21		
	6/23/2021 6/23/2021 6/23/2021 6/23/2021	8 21.50 PM 8 21.47 PM 8 21.47 PM	192 168 20 193 192 168 20 193 192 168 20 193	MULTICORP Ger MULTICORP Ger	nne me	Confidential pdf	E 'Mutcop' Prancel Ser E 'Mutcop' Prancel Ser	w 55% w 55%	1512	GLEA + NPPI	\$ 3472	File Copy	
States & Behavior	6/23/2021 6/23/2021 6/23/2021 6/23/2021 6/23/2021	8 21 50 PM 8 21 47 PM 8 21 47 PM 8 21 47 PM 8 21 47 PM	192 168 20 193 192 168 20 193 192 168 20 193 192 168 20 193 192 168 20 193	MULTICORP Ger MULTICORP Ger MULTICORP Ger	nne me me	Confidential pdf Confidential pdf Expenses sta	E 'Muticop' Prancel Ser E 'Muticop' Prancel Ser E 'Muticop' Prancel Ser	w. SSN w. SSN w. SSN + Namen	1512	GLBA + NPPI GLBA + NPPI	\$ 3472 \$ 2134	File Copy File Read	
, States & Behavior	6/23/2021 6/23/2021 6/23/2021 6/23/2021 6/23/2021 6/23/2021 6/23/2021	8/21:50 PM 8/21:47 PM 8/21:47 PM 8/21:47 PM 8/21:47 PM	192 168 20 193 192 168 20 193 192 168 20 193 192 168 20 193 192 168 21 193 192 168 20 193	MULTICORP Ger MULTICORP Ger MULTICORP Ger MULTICORP Ger	nna nna nna	Confidential pdf Confidential pdf Expenses star Expenses star	E Multicop Prancel Ser E 'Multicop Prancel Ser E 'Multicop Prancel Ser E 'Multicop Prancel Ser	M 55N M 55N M 55N + Names M 55N + Names	1512 708 708	GLEA + NPPI GLEA + NPPI GLEA + NPPI GLEA + NPPI	\$ 3472 \$ 2124 \$ 2124	File Copy File Filead File Copy	
, Shite & Bohavio Regulatory Congliance	6/23/2021 6/23/2021 6/23/2021 6/23/2021 6/23/2021 6/23/2021 6/23/2021	82150 PM 82147 PM 82147 PM 82147 PM 82147 PM 82147 PM 82147 PM	192 168 20 193 192 168 20 193	MULTICORP Ger MULTICORP Ger MULTICORP Ger MULTICORP Ger MULTICORP Ger	974 974 974 974 974	Confidential pdf Confidential pdf Expenses atte Expenses atte Investments note	E Multicop Francel Ser E Multicop Francel Ser	M. 55% M. 55% M. 55% + Names M. 55% + Names M. 55% + Names	1512 708 708 4%	GLBA + NPPI GLBA + NPPI GLBA + NPPI GLBA + NPPI GLBA + NPPI	8 3472 8 2134 8 2134 8 2134 4 1136	File Copy File Read File Copy Elle Reet	

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 **A** and the following screen will be displayed:



💥 Lepide D	ata Security Platform			- 0 ×
=	reat Models Change Alerts Health Alerts			н сэн
	Threat Models			
	Threat wodels			
U I				
	Potential brute force attack	Mass delete behaviors (OU)	Mass delete behaviors (User)	Potential business disruption
<u> </u>				
	/ 💷	/ 💷		
84				
B				
	Increased threat surface area	Mass delete behaviors (Computer)	A Potential password compromises	A Mass delete behaviors (Group)
*				
а				
				,
۰				
	Group modifications	Modifications to critical groups	Permissions escalation (Groups)	Mass data copy (FS)
ହ				
	/ 💷	/ 💷 /		
	Potential ransomware attack	Increased threat surface area (ES)	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.





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		
	< Back New	t > Cancel
	1 DOOL	Cancer

Figure 10: Threat Model Wizard

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

Set Filter(s)	
Please select operations to set the filt	er(s). (Optional)
Mass data copy (FS)	Include All
	Jeivei
	< >>
<	Send alert only if event occurs 5 times in 1 Minute(s) • 0
	< <u>B</u> ack <u>N</u> ext > Cancel

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:

Astice		nonovo
Email Execute Script LiveFeed	Sender's Email : LEPIDE; Recipient's Email : paul@lpde1.local; <sendemailtouser>NO<\SendEmailToUs Sender's Email : N/A; Recipient's Email : N/A; Script Path : C:\disableuser.bat; Profile Name : SYSTEM; F Generate LiveFeed Alert</sendemailtouser>	er> ⁹ aramet

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:

lect Action : Send Email Alert	• •	
ease select or add new se	nder's email account, add recipient(s).	
ender/Recipient Sender's Email Account :	LEPIDEALERTS Add New Email Account	
Recipient Email(s):		^
		\sim
	<	>
	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	
Send Email Alert Please select (Show in LiveFeed Send Alert to App ent(s).	
Sender/Recipie Execute Script	
Sender's Email Account : LEPIDEALERTS Add New Email Account	
v .	
< >>	
Separate multiple emails by ","	
Send Email to user	
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.	
OK Cancel	

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 ser	ider's email account, add recipient(s).	
Sender/Recipient Sender's Email Account :	LEPIDEALERTS Add New Email Account	
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 o	ption is applicable for File Server alerts only.	
	OK Cancel	

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	
OK Cancel	

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.	
Sender / Recipient	Add App Account
	~
<	>
OK Cancel	

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.	
OK Cancel	

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 selected account	Add Account	
Notify me when script is executed Configure		
Parameterized input file contains Who r Information	Test Cariat	
Note: This option is applicable for file server reports.	Test Script	
OK Cancel		

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:

Who	Ŧ
Who	
Where	
FileServer	
WhoWhere	
WhoFileServer	
WhereFileServer	
All	

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.

Action	Details	
Email Execute Script LiveFeed	Sender's Email : LEPIDE; Recipient's Email : paul@lpde1.local; <sendemailtouser>NO<\SendEmailToUs Sender's Email : N/A; Recipient's Email : N/A; Script Path : C:\disableuser.bat; Profile Name : SYSTEM; P Generate LiveFeed Alert</sendemailtouser>	er> aramet

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:

Confirmation	
<pre></pre> <tart> <reportpath>File Server\Mass data copy (FS)\<\ReportPath> <pre></pre> <pr< th=""><th></th></pr<></reportpath></tart>	
Alert Name : Mass data copy (FS)	
	< <u>B</u> ack Finish Cancel

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 <u>https://www.lepide.com/contactus.html</u> 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.