%Lepide

CONFIGURATION GUIDE

User and Entity Behavior Analytics

Table of Contents

1.	Introduction	3
2.	Purpose of this Document	3
3.	How to Configure UEBA	3
	3.1. Learning Stages	5
	3.2. Learning Information	5
	3.3. Reset or Extend Learning	6
4.	How to Report on Anomalies	7
	4.1. The Anomaly Analysis Report	7
5.	Support1	1
6.	Trademarks1	1

1. Introduction

Welcome to the User and Entity Behavior Analytics (UEBA) guide for the Lepide Data Security Platform.

With the Lepide Solution, you can identify single point anomalies to gain an understanding of when users are doing something that is outside of their normal behavior. The UEBA analysis within the Lepide Data Security Platform allows you to determine exactly why something has been flagged as unusual based upon a number of factors including, time, event criticality, operation, and location.

User behavior is analyzed based upon a predefined learning period to accurately identify potential insider threats.

2. Purpose of this Document

The purpose of this document is to explain how to configure User and Entity Behavior Analytics in the Lepide Data Security Platform and how to run the Anomaly Analysis report to help you understand any deviations in user behavior and then take appropriate action.

3. How to Configure UEBA

From the Component screen:

	Settings									
	🕀 😭 Component Management	Add Componen								
	5 Lepidecorporate.com	Mad componen								
0										^
	LPSQLSRV(SQL)									
6	-Uff lepidesoftware.onmicrosoft.co									
	Epidesoftware-admin.sharepi		Active Directory, Group	SharePoint Server	SQL Server	 File Server		Exchange Online	SharePoint Online	
æ	## Lepide Corporate Drophov(Dr		Policy, Exchange Server,				- 20			
	lepidesoftware.opmicrosoft.cr		Reminder and Active				E S			
	- 10 General Settings	10	Directory Cleaner				Online			
	- Delegation Control									
	- Current Permission Scan Settings									
84	- 🔂 Message Delivery Settings									
	- 🔂 Default SQL Server Settings		Cloud Components	Office 365	Session Recording	Universal Audit				
100	- G UEBA									
	- G Agent Settings									
-										
13										~
۹		~								
25		Added Compo	nent							
~										
0					 _				 _	
×			Lepidecorporate.com	192.168.20.203(SharePoint)	LPSQLSRV(SQL)	LEPIDENAS01(File Server)		lepidesoftware.onmicrosof	lepidesoftware.onmicrosof	
							E 20	Loom	Loom	
		Sel Contraction	Active Directory, Group Policy and Exchange	SharePoint Server	SQL Server	File Server		Exchange Online	Office 365	
			Server				Online			
			lenidesoftware-admin shar	Lepide Comorate Drophov(
			epoint.com	Dropbox)						
			Charao Darlant Carllon	Claud Company						
			SharePoint Online	cioud component						

Figure 1: Component Screen

- Click the Settings icon
- Choose UEBA from the tree structure on the left-hand side

The following screen will be displayed:

Setti	Settings ① Component Management ① multicorp.local ④ 192.168.20.192(SharePoint) ● lepidesoftware.onmicrosoft.com	Added Component Add the components to learn the user behavior	or anomaly analysis.									G Ø-	O X II		
6	Epidesoftware-admin.snarepoin Eile Senvers	Domain	lype	Status Send Werts in Em			mail Send Alerts in Live Feed Se			end Alerts in Mobile App	Ag	ent Machine			
	-mag rife servers	م		م م		_	<u>р</u>		٩		Q		Q		
3	I lepidesoftware.onmicrosoft.com	192.168.20.193	File Server	Scan Successf	ul on 3/3/2023 4:22:52 PM	Gemma@multic	orp.local			Please click edit to add	/ La	scal System	/		
✓	© General Settings © Delegation Control © Current Permission Scan Settings ■ Message Delivery Settings © UEBA © UEBA © 4 Agent Settings © LDSP Web Console (beta)	Domain Management	nun unun	Joan Jocobe	1011372065 142.551 H			L	<u> </u>						
Ş		Add the domain to find the last if uses for which the learning has to start. Once the domain is added it will be scanned every 24hours to field the newly created users. Right click on the domain to scan manually at any point of time.													
-		Domain	Domain Controller	Login Name			Added On Modified On				Scan Sta	Scan Status			
~		Vocal/multicorp	192.168.20.191			5/19/2021 12:51:39 PM 5/			19 PM	Scan Succ	Scan Success on 3/3/2023 12:02:35 AM				
-		Local/Unidentified users	N/A	N/A		N/A		N/A			N/A				
Υ.															
		User Management All the users of the selected domain will be listed	here. Date of start of learning wil	be shown for each user. dic	k on the learning to find the de	als per component. F	ight click on the user for	more options.							
		User Name		Identified On			OU Path			Learning Stage			<u> </u>		
			م			م				Q					
		multicorp\\$o61000-cmils7gjq0vs		5/19/2021 12:58:43 PM			Vocal/multicorp/Users/Exchange Online-Application/Account			Infancy 0	Childhood 0	Adolescence 0	Adulthood 2		
		multicorp \adam	5/19/2021 12:58:43 PM		Vocal/multicorp/US Office/Users/Adam Stevens				Infancy 0	Childhood 0	Adolescence 0	Adulthood 2			
		multicorp/admin		5/19/2021 12:58:43 PM			\local\muticorp\Users\Admin			Infancy 0	Childhood 0	Adolescence 0	Adulthood 2		
		multicorp/administrator		5/19/2021 12:58:43 PM			Vocal/wulticorp/Users/Vidministrator			Infancy 0	Childhood 0	Adolescence 0	Adulthood 2		
	< >>	multicorp/ladiam 5/13/2021 12:58:43 PM Vicosl*/multicorp/Vaio Office*/Libers/Adram Greg Neilancy Childhood Addelevence											Adulthood		

Figure 2: UEBA Screen

The top area of the screen shows Added Components.

- Add components here to learn the user behavior for anomaly analysis
- You can specify here where you want anomaly alerts to be sent. One or more of the following options can be selected: Email, Live Feed and Mobile App
- To Add a new component, click the 🔁 icon to the top right of the screen

The middle area of the screen shows Domain Management.

- Add a domain here to find the list of users for which the learning has to start. Once a domain has been added it will be scanned every 24 hours to fetch the newly created users.
- Right click on the domain to do a manual scan at any point in time.
- To add a new domain, click the 🔁 icon

The bottom of the screen shows User Management.

All the users of the selected domain will be listed here. The start date of learning will be shown for each user together with the OU Path and the Learning Stage.

3.1. Learning Stages

The Learning Stages are called Infancy, Childhood, Adolescence and Adulthood and these are based on the number of days specified in the learning duration which is found under the settings icon at the top right of the screen. To specify the Learning Duration:

Click the settings icon and choose Learning Duration

The Learning Duration dialog box is displayed:

	×
Learning Duration: 1	Days (1-180)
ок	Cancel

Figure 3: Learning Duration

- Specify the number of days over which the learning should take place. It is recommended that this is at least 3 months (90 days) but it can be any number up to 180 days.
- Click **OK**

The Learning Stages (Infancy, Childhood, Adolescence and Adulthood) are calculated based on the Learning Duration. The number of days is divided by 4 to determine each of the four learning stages. For example, if the Learning Duration was set to 80 days, then each of the learning stages would be 20 days.

3.2. Learning Information

From the UEBA screen, click on the learning stage for a particular user to find the Learning Information details for that user by component:



Component Name	Learning Days	Extend by (days)	Learning Stage	
Q	Q	Q		P
192.168.20.193 (File S	1	0	Adulthood	
multicorp.local (Active	1	0	Adulthood	

Figure 4: Learning Information

This shows the learning information for the user Adam. The learning stage for both the File Server and Active Directory components is Adulthood. These could be at different learning stages if the components had been installed at different times.

3.3. Reset or Extend Learning

• From the UEBA Screen, right click on a username for more options:

Reset Learning	am
	Reset Learning
Extend Learning	Extend Learning

Figure 5: Reset or Extend Learning Options for a User

These options are to:

- Reset Learning to start the learning again for that user
- Extend Learning to increase the number of days of learning for that user



4. How to Report on Anomalies

Once anomaly analysis has been configured it needs to run for enough time for the Solution to be able to spot anomalous behavior. It will start finding anomalies immediately, but the longer it runs the better as it will be able to establish a pattern of normal user behavior and then spot anything unusual and flag it as an anomaly.

4.1. The Anomaly Analysis Report

The Anomaly Analysis Report identifies any anomalous behavior 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

• Click on **Anomaly Analysis** and the report will be displayed:



Figure 6: Anomaly Analysis Report

From the top of the screen, set the filters as follows:

- Click **Component** to select the components required or leave as all
- Click Analysis Period to select a date range for the report
- Click **User** to select the users required or leave as all
- Click Analyze

The report will run and will display anomalies for the selected components, the specified time period and selected users:

	States & Behavior 🛛 🔍	Anomaly Analys	sis						
	Search P	Component	Anal	vsis Period	User				
	All Environment Changes								
•	Anomaly Analysis	01	4/1/	2022 - 4/3/20	22				
60	In the second								
<u> </u>	Image: Second Seco							_	
æ	lepidesoftware.onmicrosoft.com/E								Analyze
	E lepidesoftware-admin.sharepoint.								
0	Iepidesoftware.onmicrosoft.com((Hear	Component(a)	Total & A					
·		0.00			Short/Hide Series				
8 A	Console Auditing	m dicom loand	File Server	121					
		multicom\simon	File Server	99					
B.		multicorp\russel	File Server Active Dir	109					
		multicorp\administr	File Server, Active Dir	101					
A		multicorp\ext_cont	File Server	47					
		multicorp/yill	File Server, Active Dir	41					
5		multicorp\gemma	File Server	10					
		fs001\administrator	File Server	1					
ø		david	Active Directory	1144705					
		luke	Active Directory	599186					
1		administrator	Active Directory	117942					
		sign in m: multicorp	Active Directory	21314			No Data Found		
2		multicorp	Active Directory	20834					
		admin	Active Directory	5961					
		administrador	Active Directory	2212					
		test	Active Directory	2129					
		user	Active Directory	676					
		guest millicom local/kike	Active Directory	645					
		usuario	Active Directory	628					
		support	Active Directory	612				(1 or i page(s)	1 11
		server	Active Directory	541					
		scanner	Active Directory	510	Anomalu		Anomaly Details		
		user1	Active Directory	489	Anomary		Anomary Details		
		asp.net	Active Directory	459	Date Time	Details			
		exd001\$	Active Directory	446					
		scan	Active Directory	434					
		administrateur	Active Directory	418					
		suporte	Active Directory	334					
		servidor	Active Directory	295					
	<>	user2	Active Directory	2/8					
	California & Rehaudor	houser	Active Directory	104					
	EX Junes & Denamor	student	Active Directory	162					
	C Regulatory Compliance	test1	Active Directory	160					
		defaultaccount	Active Directory	153 -1					
	O Restore	•		ن ا					

Figure 7: Anomaly Analysis Report

• To see anomalies for a specific user, click on the username from the list of users in the middle section of the screen:

	States & Behavior 🛛 🕅	Anomaly Analy	sis					
	Search 🔎	Component	Ana	lysis Period		User		
8) 6-	All Environment Changes - C Anomaly Analysis 9 2 192.168.20.192(SharePoint) 9 2 multicoro.local	All	Bets 4/1,	/2022 - 4/3/20	123	All		
6	File Server Reports Grade Server Reports Grade Server Reports Grade Server Reports							Analyze
	🗄 🔝 lepidesoftware-admin.sharepoint.							
	Epidesoftware.onmicrosoft.com(1 heres	Comment(s)	T-1-1 6 *				
		User	Component(s)	Total A	shor /Hi	de Series		Anomaly (121)
	Console Auditing		· · · · · ·	<u>д</u>	20 -	19		
~		muticorp/paul	He Server	121		•		
EN .		multicorp\simon	File Server	99				
63		multicorp/russell	File Server, Active Dir	109				
		multicorp\administr.	. File Server, Active Dir	101	15 -			
+		multicorp/ext_cont.	. File Server	47				
_		multicorp/jill	File Server.Active Dir	41				
8		multicorp/gemma	File Server	10				
		fs001\administrator	File Server	1	10 -	- 1		
۵		david	Active Directory	1144705				
		luke	Active Directory	599186				
- N		administrator	Active Directory	117942				
		sign in m: multicorp	Active Directory	21314	5 -			
۵		multicorp	Active Directory	20834			_	
*		admin	Active Directory	5961				
		administrador	Active Directory	2212				
		test	Active Directory	2129	0.			
		user	Active Directory	1784		· · · · · · · · ·		
		quest	Active Directory	676	C 100 10000			
		multicorp.local/luke	Active Directory	645	5/20/2022	1:35:41 PM 5/26/2022 2:	20:56 PM 5/20/2022 2:27:14 PM 5/20/2022 2:27:41	M 5/26/2022 2:21:51 PM //12/2022 10:51:45 AM //12/2022 10:38:19 AM //12/2022 10:39:01 AM //12/2022 10:39:19 AM //12/2022 11:01:14 AM
		usuario	Active Directory	628				
		support	Active Directory	612				IOGAI RECORDS : 121 (1 01 (page 8) / //
		aerver	Active Directory	541				
		scanner	Active Directory	510				
		user1	Active Directory	489	Anomaly			Anomaly Details
		aso net	Active Directory	459	Date Time	8	Details	
		avd0015	Active Directory	446	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 48 file(s) at 5. 	
		scan	Active Directory	434	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 51 folder(s) a 	
		administrateur	Active Directory	418	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 48 file(s) at 5. 	
		rupote	Active Directory	334	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 51 folder(s) a 	
		rapidor	Active Directory	295	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 48 file(s) at 5. 	
		11007	Active Directory	278	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 51 folder(s) a 	
	< >>	optone	Active Directory	235	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 48 file(s) at 5. 	
	B. marine and second	hunges	Anthre Directory	104	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 51 folder(s) a 	
	EX States & Benavior	ilpuser student	Active Directory	109	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 48 file(s) at 5. 	
	C Regulatory Compliance	stopers.	Active Directory	102	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 51 folder(s) a 	
	Regulatory compliance	defer the second	Active Directory	160	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 48 file(s) at 5. 	
	O Bastara	uer aux account	Acave Directory	100 -	5/20/2022	1:35:41 PM	 multicorp\paul changed permissions of 1 folder(s) at 	
	Nexure .	1		>			· · · · · · · · · · · · · · · · · · ·	

Figure 8: Anomaly Analysis for a Specific User

- In the example above, the user Paul has been selected and a graph shows a graphical representation of all anomalies for Paul
- Pausing on any of the points of the graph will show more information about the anomalies:



Figure 9: Anomaly Graph

• Below the graph is a list of all the anomalies for the selected user (Paul) showing **Date**, **Time** and **Details** of the anomaly:



Figure 10: List of Anomalies

• By clicking on an anomaly in this list, you can see details of the selected anomaly in the **Anomaly Details** window to the right:

Anomaly		Anomaly Details						
Date Time	Details	Path	Operation	Process Name	From	Severity	When	-
5/25/2022 4:38:51 PM	 multicorp\paul changed permissions of 23 file(s) at 5. 	E:\Multicorp\Financial Services\Finance\458673.bmp	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/25/2022 4:38:51 PM	 multicorp\paul changed permissions of 6 folder(s) at 	E:\Multicorp\Financial Services\Finance\459565496.bmp	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:26:41 PM	 multicorp\paul viewed 2 file(s) at 5/26/2022 2:26:41 	E:\Multicorp\Financial Services\Finance\67949.bmp	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:26:56 PM	 multicorp\paul viewed 1 file(s) at 5/26/2022 2:26:56 	E:\Multicorp\Financial Services\Finance\Addresses.txt	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:26:57 PM	 multicorp\paul modified 1 file(s) at 5/26/2022 2:26:5 	E:\Multicorp\Financial Services\Finance\Client portfolio	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:26:57 PM	 multicorp\paul renamed 2 file(s) at 5/26/2022 2:26:5 	E:\Multicorp\Financial Services\Finance\Client portfolio.p	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:27:00 PM	 multicorp\paul viewed 1 file(s) at 5/26/2022 2:27:00 	E:\Multicorp\Financial Services\Finance\Confidential.pdf	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:27:12 PM	 multicorp\paul modified 1 file(s) at 5/26/2022 2:27:1 	E:\Multicorp\Financial Services\Finance\Customer conta	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:27:14 PM	 multicorp\paul viewed 1 file(s) at 5/26/2022 2:27:14 	E:\Multicorp\Financial Services\Finance\Customer list.pptx	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:27:28 PM	 multicorp\paul viewed 1 file(s) at 5/26/2022 2:27:28 	E:\Multicorp\Financial Services\Finance\Employee list.d	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:27:29 PM	 multicorp\paul deleted 1 file(s) at 5/26/2022 2:27:25 	E:\Multicorp\Financial Services\Finance\Expenses.xlsx	File Security Change (Permis	explorer.exe	FS001	High	5/25/2022 4:38:51 PM	
5/26/2022 2:27:29 PM	 multicorp\paul modified 1 file(s) at 5/26/2022 2:27:2 	C → M. Minnes \ Dimensional Constant \ Dimensional \ D	Die Commen Channel (Domin		FC001	11.44	E (26 (2022 4-20-61 PM	•

Figure 11: Anomaly Details

• In the example above we have clicked on the first anomaly in the list which showed that the permissions of 23 files had been changed. The Anomaly Details window on the right shows more details about the files which were changed including the filename and path, operation, process name, from which server, severity and when it happened.

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 <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/.

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.

