



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. Support 11
- 6. Trademarks 11

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:

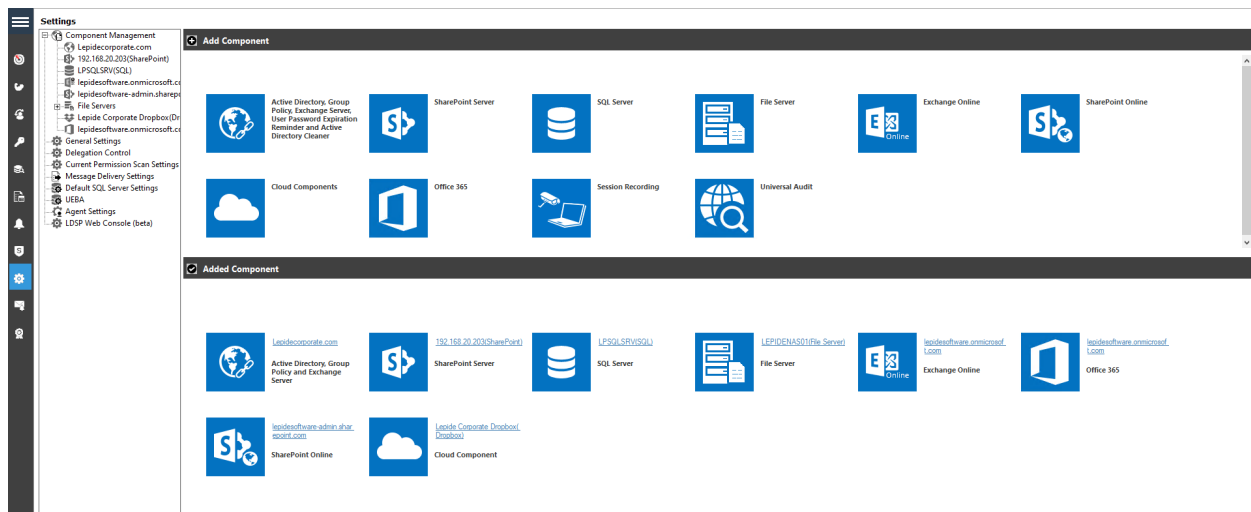



Figure 1: Component Screen

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

The following screen will be displayed:

Settings

- Component Management
 - multicorp.local
 - 192.168.20.192(SharePoint)
 - lepidesoftware.onmicrosoft.com
 - lepidesoftware-admin.sharepoint
 - File Servers
 - Dell EMC
 - lepidesoftware.onmicrosoft.com
- General Settings
- Delegation Control
- Current Permission Scan Settings
- Message Delivery Settings
- Default SQL Server Settings
- UEBA
- Agent Settings
- LDSP Web Console (beta)

Added Component

Add the components to learn the user behavior for anomaly analysis.

Domain	Type	Status	Send Alerts in Email	Send Alerts in Live Feed	Send Alerts in Mobile App	Agent Machine
192.168.20.192	File Server	Scan Successful on 3/3/2023 4:22:52 PM	<input checked="" type="checkbox"/> Gemma@multicorp.local	<input type="checkbox"/>	<input type="checkbox"/> Please click edit to add	Local System
multicorp.local	Active Directory	Scan Successful on 3/3/2023 4:22:53 PM	<input type="checkbox"/> Please click edit to add	<input type="checkbox"/>	<input type="checkbox"/> Please click edit to add	N/A

Domain Management

Add the domain to find the list of users for which the learning has to start. Once the domain is added it will be scanned every 24 hours to fetch 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 Status
local/multicorp	192.168.20.191	Administrator@multicorp.local	5/19/2021 12:51:39 PM	5/19/2021 12:51:39 PM	Scan Success on 3/3/2023 12:02:36 AM
Local\Unidentified users	N/A	N/A	N/A	N/A	N/A

User Management

All the users of the selected domain will be listed here. Date of start of learning will be shown for each user; click on the learning to find the details per component. Right click on the user for more options.

User Name	Identified On	OU Path	Learning Stage
multicorp\661000-cmjh7gdlvs	5/19/2021 12:58:43 PM	'local/multicorp\Users\Exchange Online Application\Account	<div> <div>Infancy</div> <div>Childhood</div> <div>Adolescence</div> <div>Adulthood</div> </div>
multicorp\adam	5/19/2021 12:58:43 PM	'local/multicorp\US Office\Users\Adam Stevens	<div> <div>Infancy</div> <div>Childhood</div> <div>Adolescence</div> <div>Adulthood</div> </div>
multicorp\admin	5/19/2021 12:58:43 PM	'local/multicorp\Users\Admin	<div> <div>Infancy</div> <div>Childhood</div> <div>Adolescence</div> <div>Adulthood</div> </div>
multicorp\administrator	5/19/2021 12:58:43 PM	'local/multicorp\Users\Administrator	<div> <div>Infancy</div> <div>Childhood</div> <div>Adolescence</div> <div>Adulthood</div> </div>
multicorp\adrian	5/19/2021 12:58:43 PM	'local/multicorp\Asia Office\Users\Adrian Greg	<div> <div>Infancy</div> <div>Childhood</div> <div>Adolescence</div> <div>Adulthood</div> </div>

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:

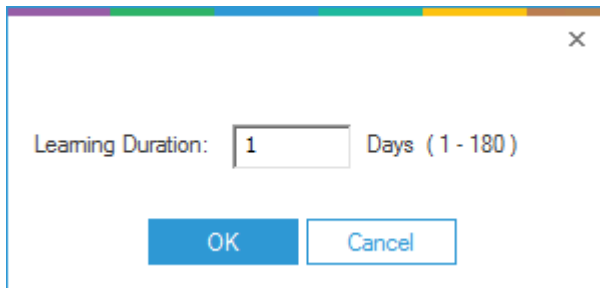
A dialog box titled "Learning Duration" with a close button (X) in the top right corner. It contains a text input field with the value "1" and the label "Days (1 - 180)". Below the input field are two buttons: "OK" and "Cancel".

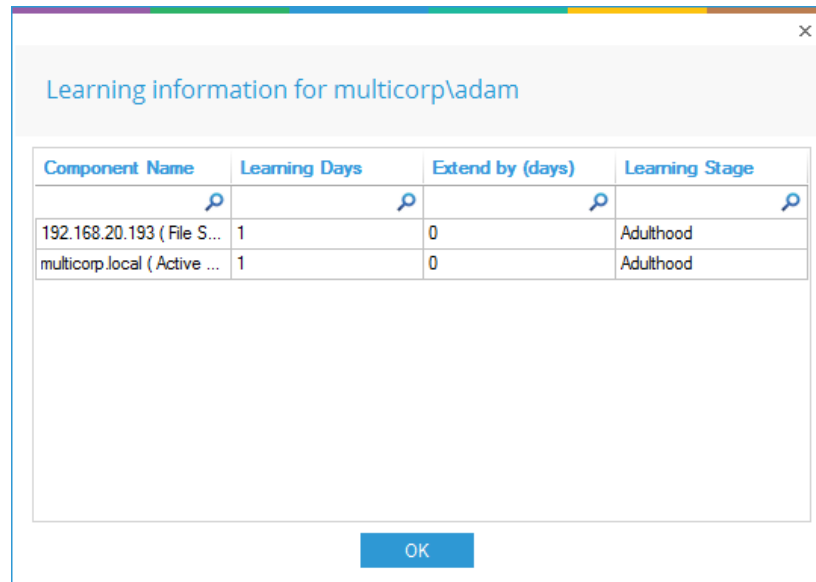
Figure 3: Learning Duration

- 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:



Learning information for multicorp\adam

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

OK

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:

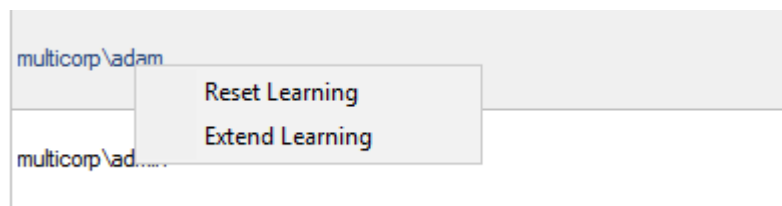


Figure 5: Reset or Extend Learning Options for a User

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:

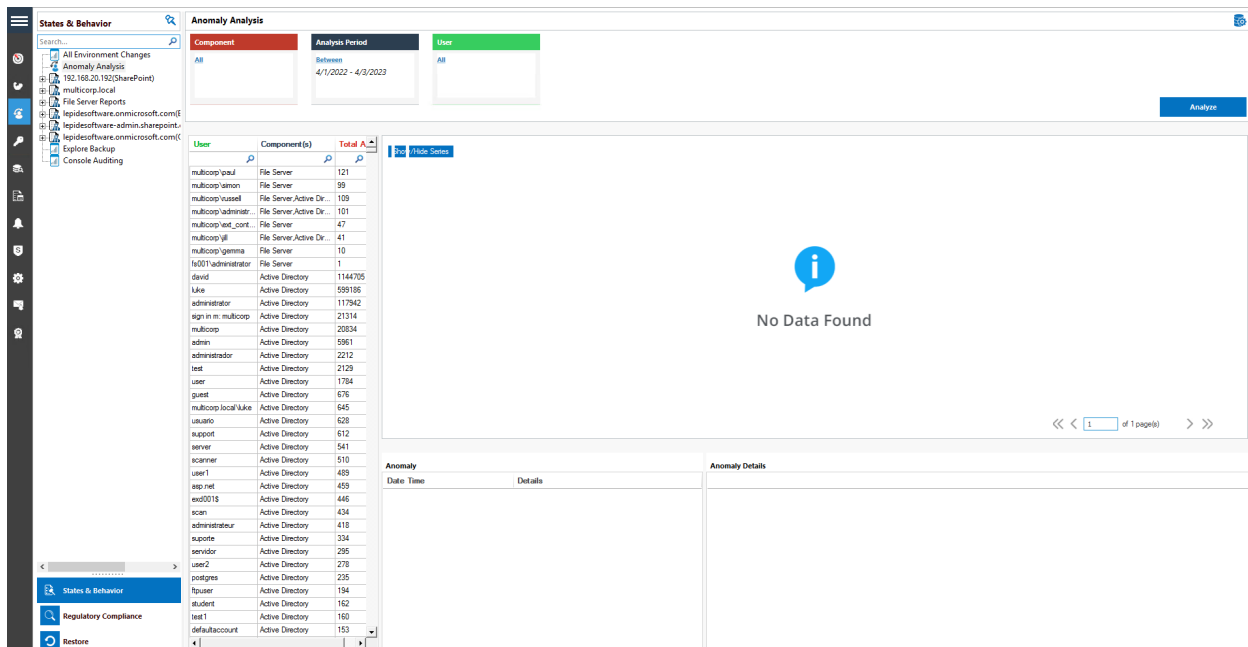


Figure 6: Anomaly Analysis Report

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:

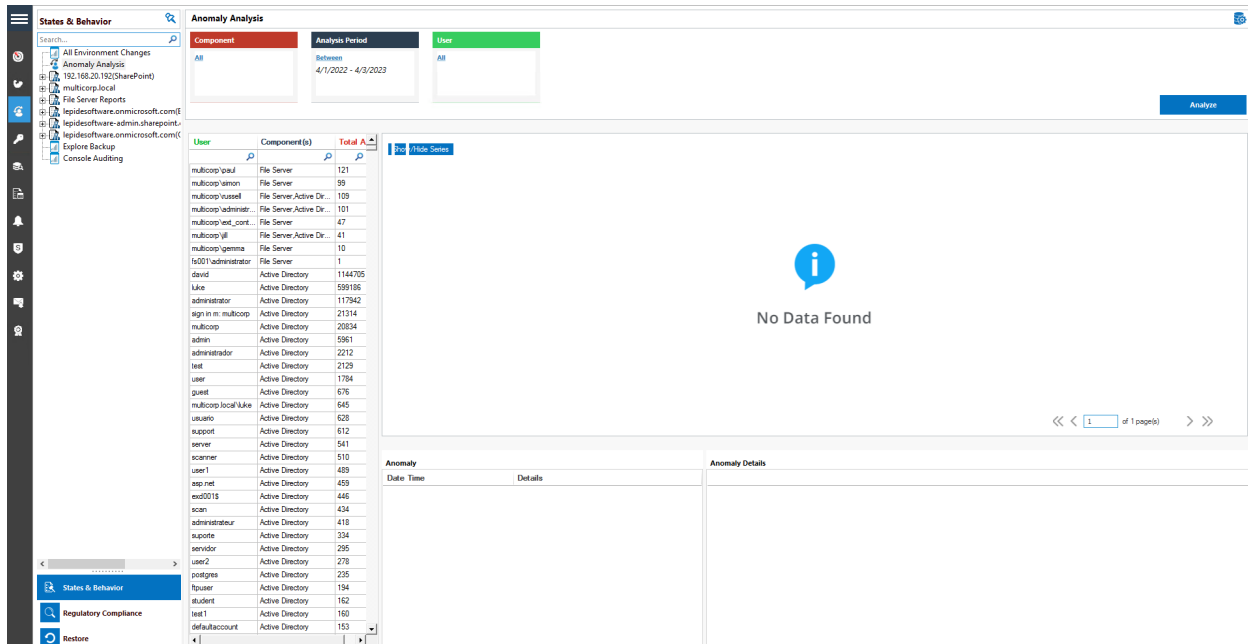


Figure 7: Anomaly Analysis Report

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

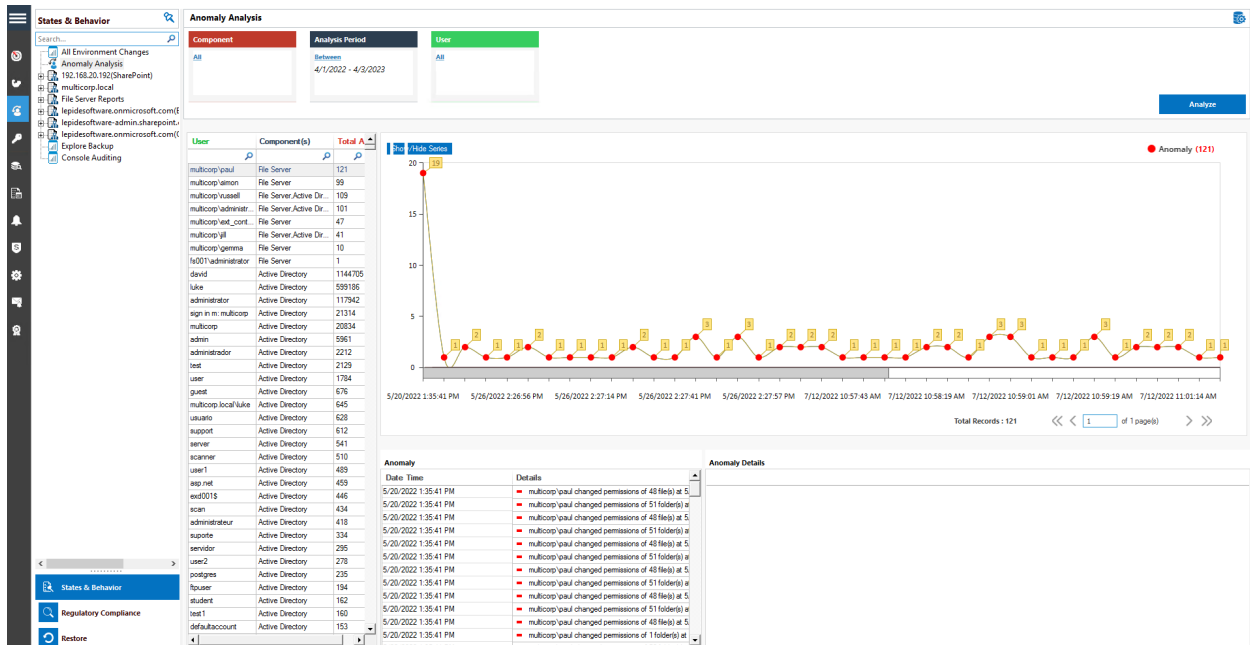


Figure 8: Anomaly Analysis for a Specific User

- 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:

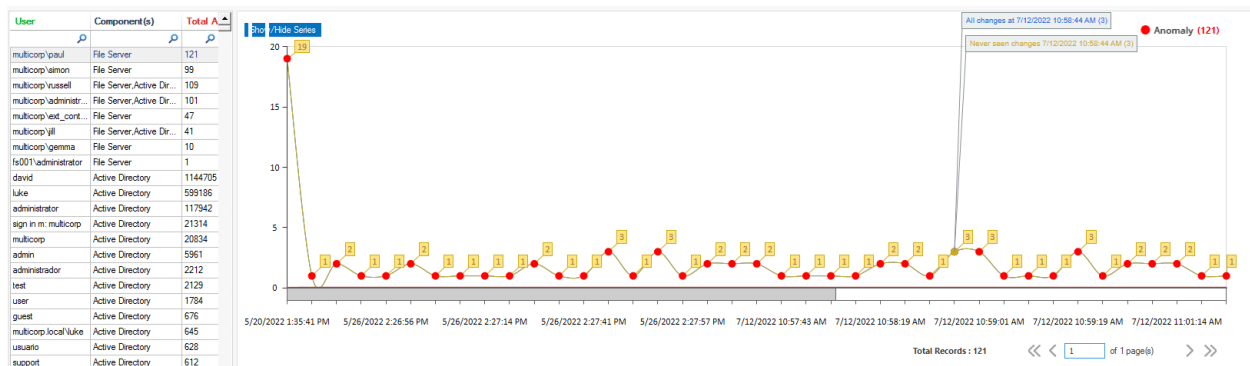


Figure 9: Anomaly Graph

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

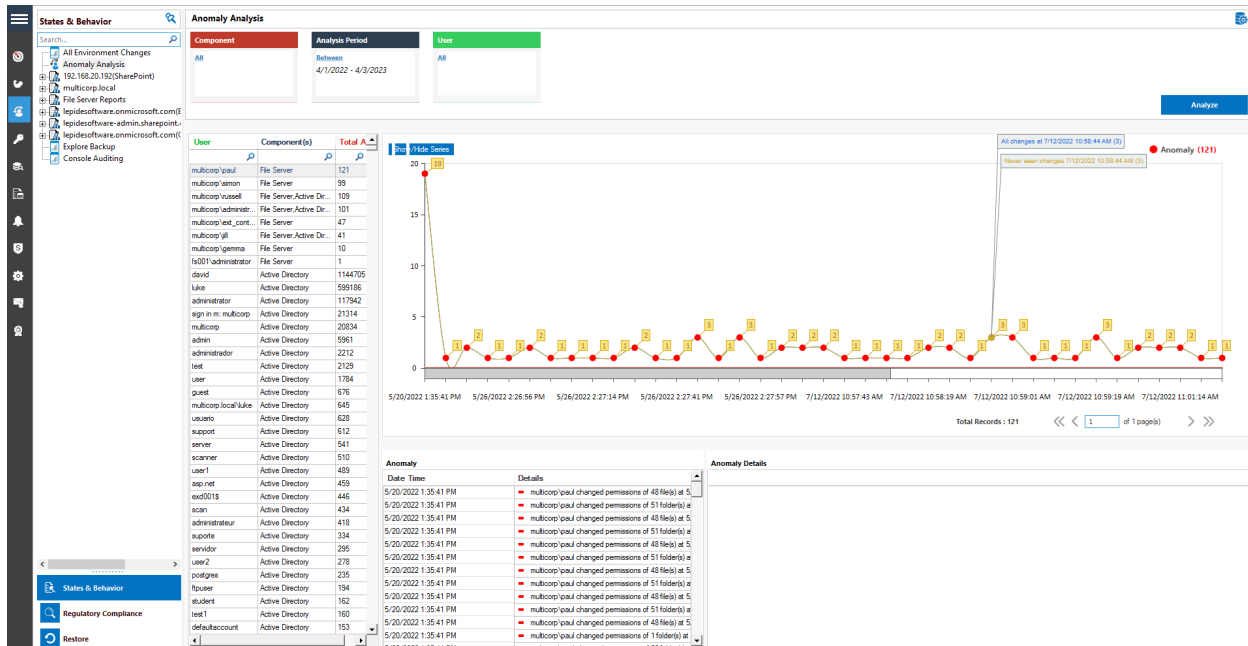


Figure 10: List of Anomalies

- 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 5/25/2022 4:38:51 PM	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 5/25/2022 4:38:51 PM	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 PM	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 PM	E:\Multicorp\Financial Services\Finance\Addresses.bt	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 2:26:57 PM	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 2:26:57 PM	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 PM	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 2:27:12 PM	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 PM	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 PM	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 2:27:29 PM	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 2:27:29 PM	E:\Multicorp\Financial Services\Finance\Expense...	File Security Change (Permis...	explorer.exe	FS001	High	5/25/2022 4:38:51 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 <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.