



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:

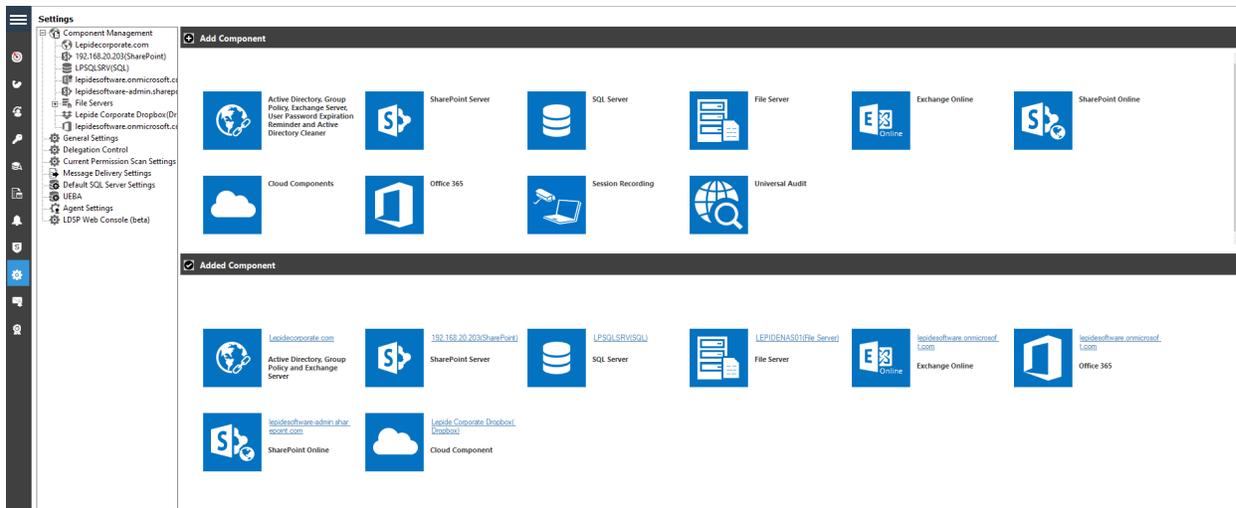


Figure 1: Component Screen

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

The following screen will be displayed:

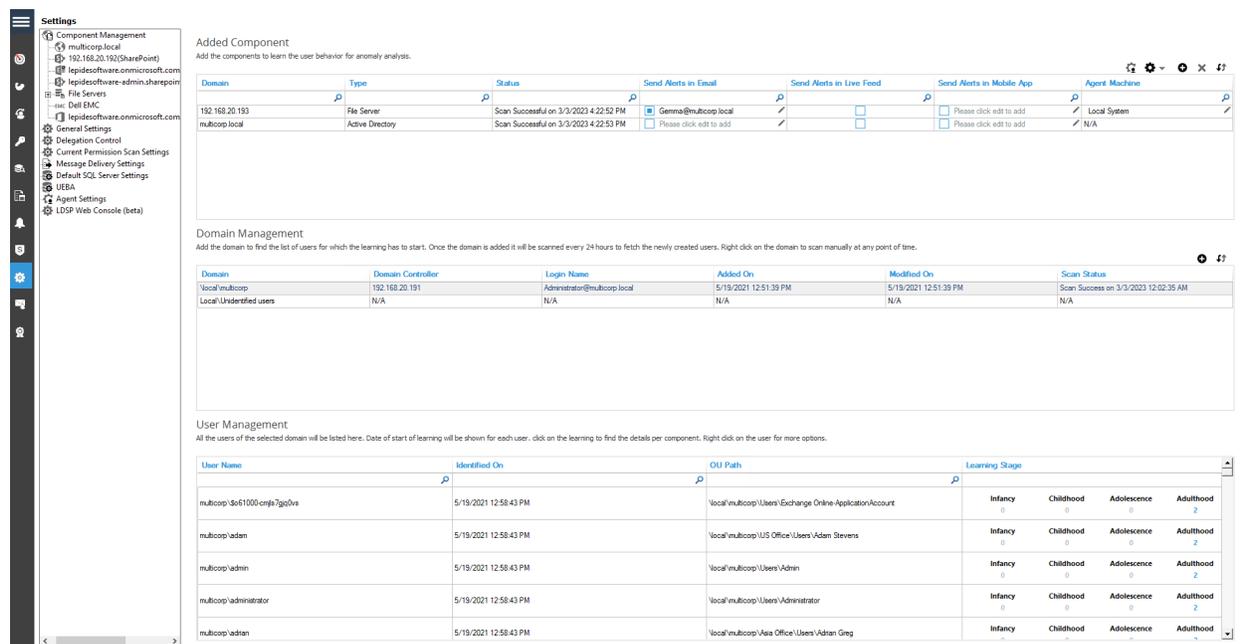


Figure 2: UEBA Screen

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.

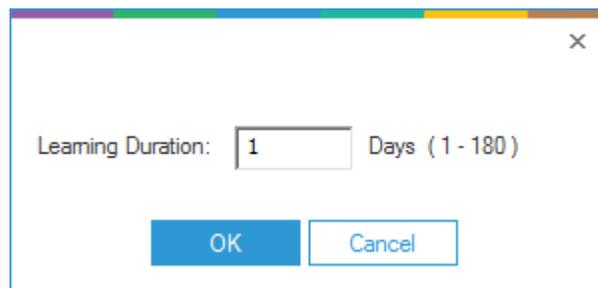
All the users of the selected domain will be listed here. The start date of learning will be shown for each user together with the OU Path and the Learning Stage.

## 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:



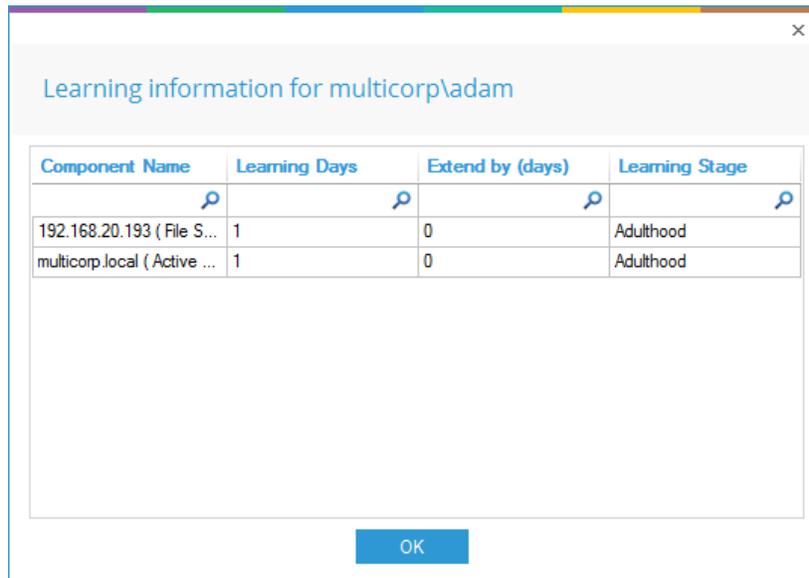
**Figure 3: Learning Duration**

- 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:



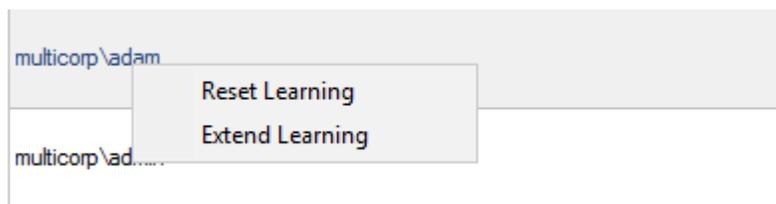
Component Name	Learning Days	Extend by (days)	Learning Stage
192.168.20.193 (File S...	1	0	Adulthood
multicorp.local (Active ...	1	0	Adulthood

**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:



**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.

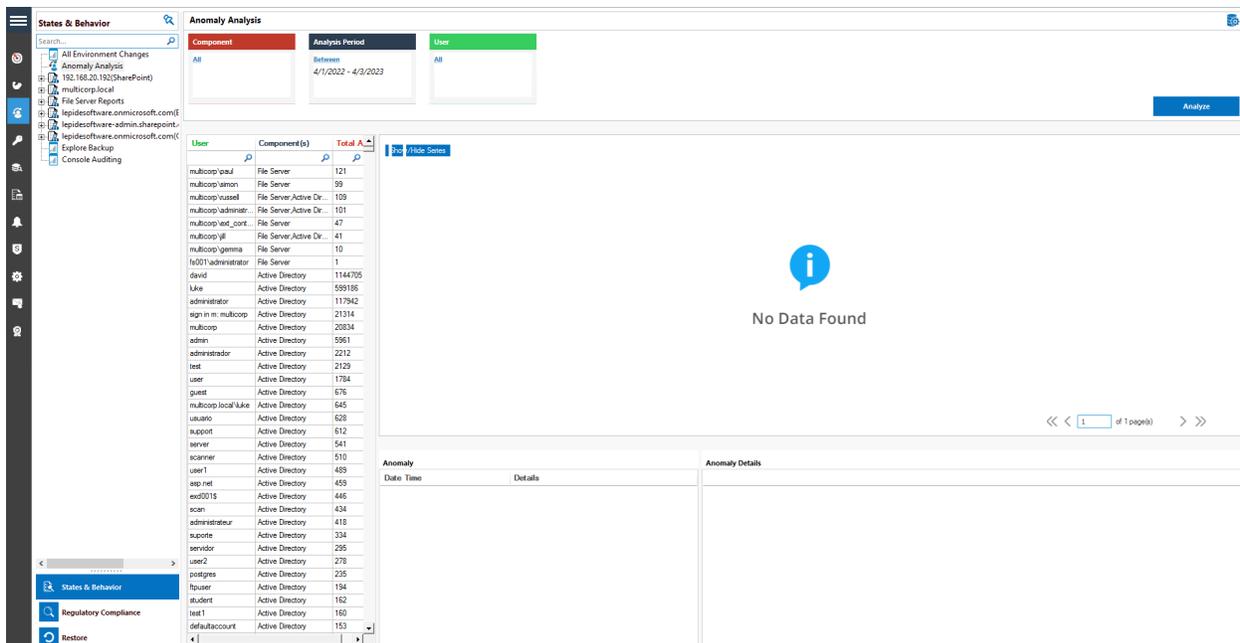
### 4.1. The Anomaly Analysis Report

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:



The screenshot shows the 'States & Behavior' window with the 'Anomaly Analysis' report selected. The report is filtered by Component (All), Analysis Period (Between 4/1/2022 - 4/3/2023), and User (All). The table below shows the results of the analysis:

User	Component(s)	Total A
multicorp\paul	File Server	121
multicorp\amom	File Server	99
multicorp\usnell	File Server,Active Dir.	109
multicorp\adminstr	File Server,Active Dir.	101
multicorp\and_cort	File Server	47
multicorp\ill	File Server,Active Dir.	41
multicorp\gemma	File Server	10
fs001\administrator	File Server	1
david	Active Directory	1144705
lake	Active Directory	559105
administrator	Active Directory	117542
sign in m. multicorp	Active Directory	21314
multicorp	Active Directory	20834
admin	Active Directory	5961
administrator	Active Directory	2212
test	Active Directory	2139
user	Active Directory	1704
guest	Active Directory	676
multicorp.local\lake	Active Directory	645
usuarlo	Active Directory	628
usupost	Active Directory	612
server	Active Directory	541
scanner	Active Directory	510
user1	Active Directory	489
esp.net	Active Directory	459
esp0018	Active Directory	446
scan	Active Directory	434
administratur	Active Directory	418
supote	Active Directory	334
servidor	Active Directory	295
user2	Active Directory	278
pastrges	Active Directory	225
flpuser	Active Directory	194
student	Active Directory	162
test1	Active Directory	160
defaultaccount	Active Directory	153

**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:

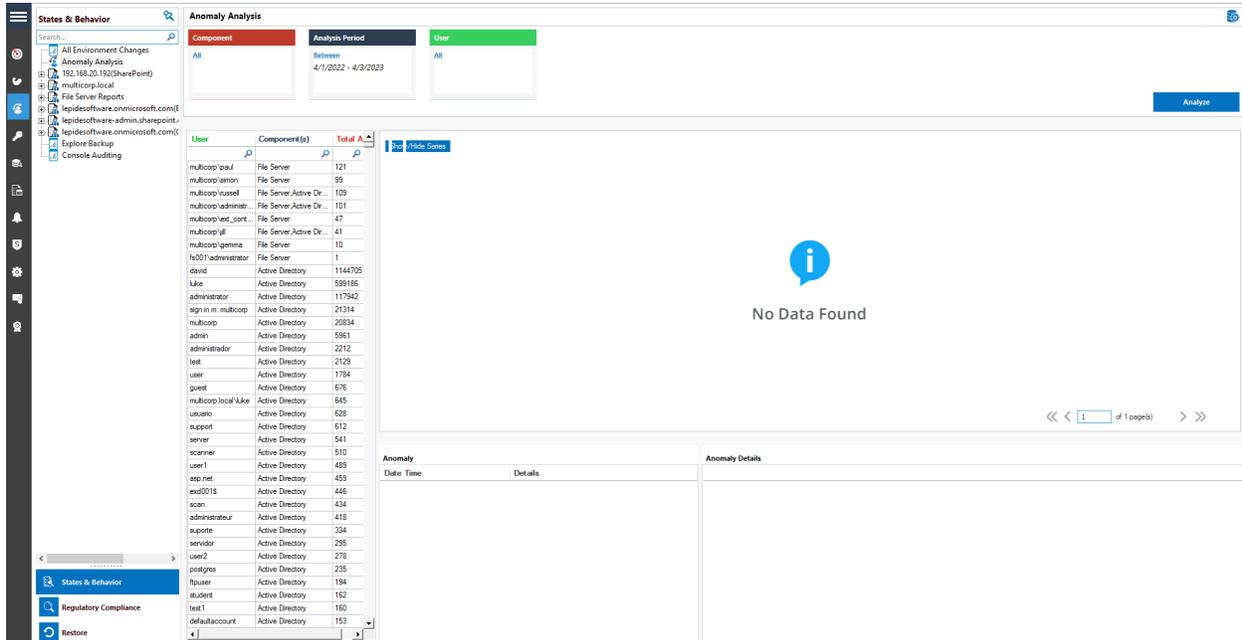


Figure 7: Anomaly Analysis Report

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

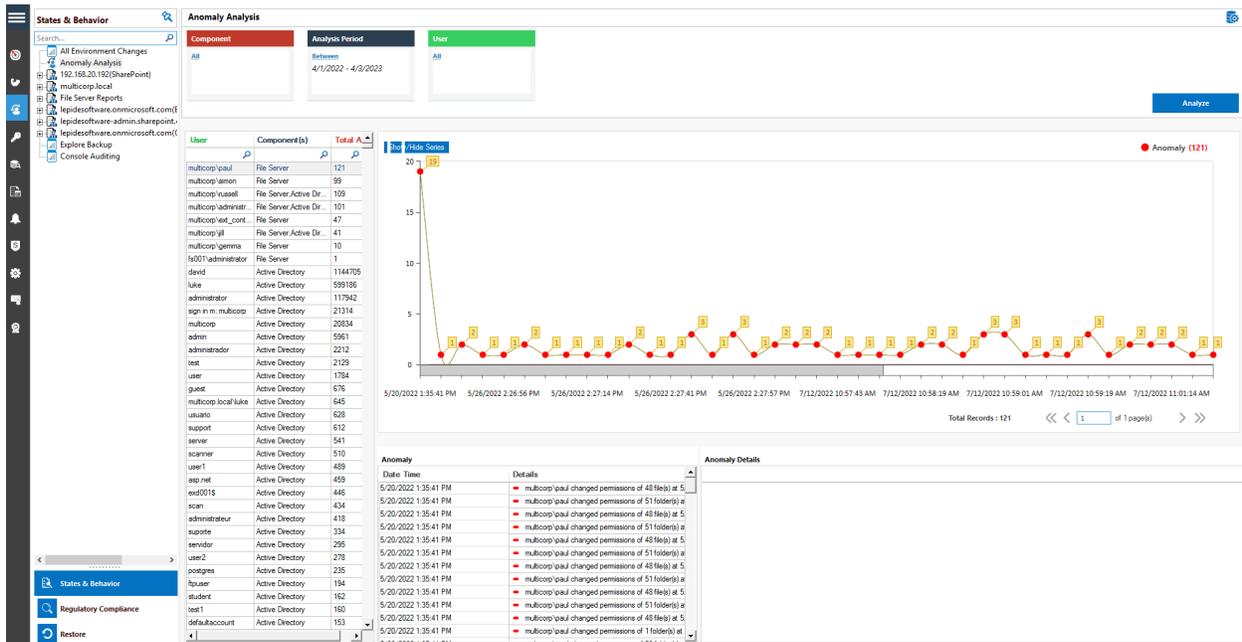


Figure 8: Anomaly Analysis for a Specific User

- 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:

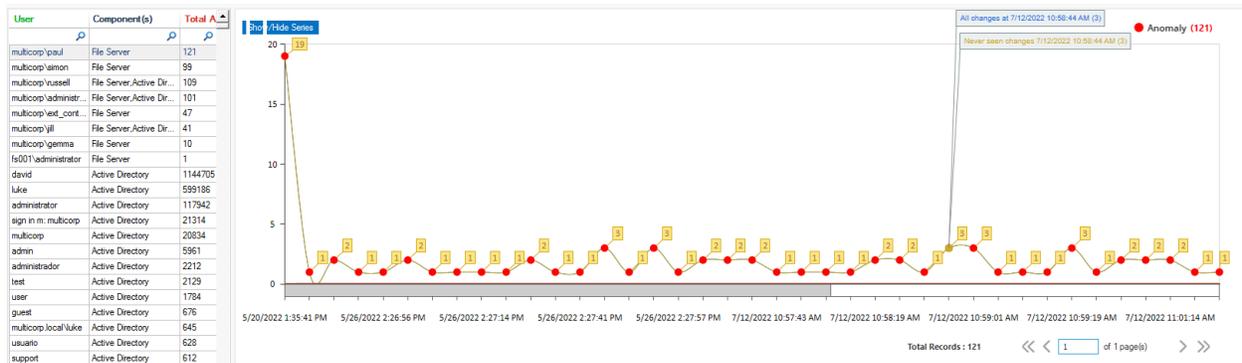


Figure 9: Anomaly Graph

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

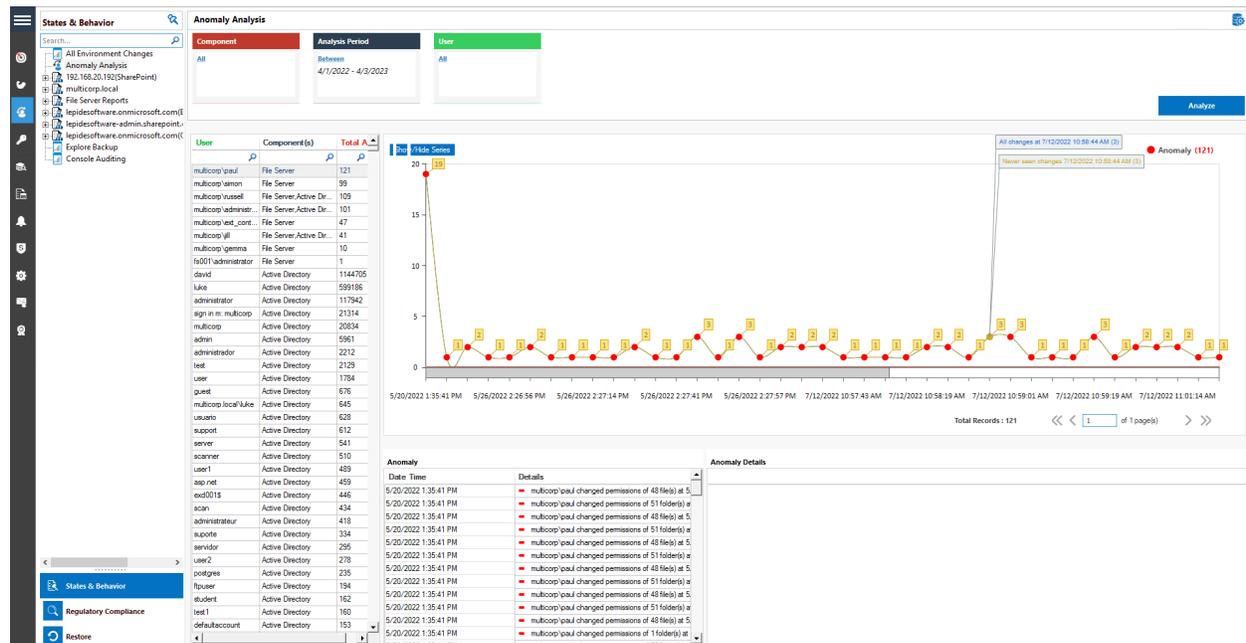


Figure 10: List of Anomalies

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

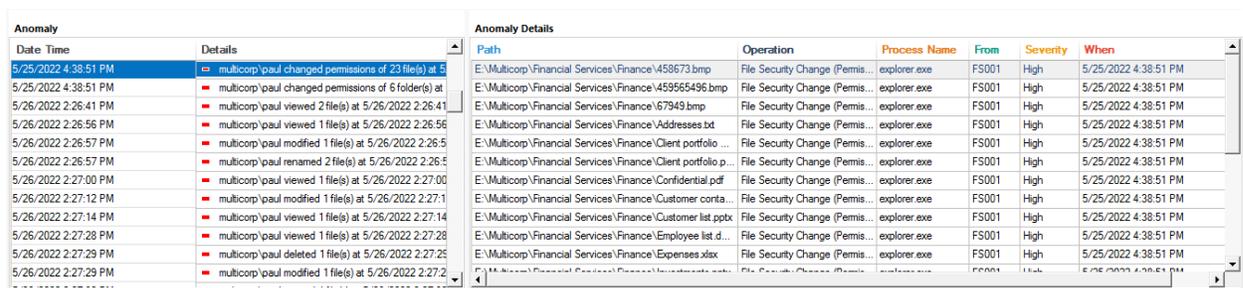


Figure 11: Anomaly Details

- 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](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/>.

## 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.