

LepideAuditor

USER AND ENTITY
BEHAVIOR ANALYTICS

Table of Contents

1. Introduction.....	2
2. Purpose of this Document.....	2
3. Configuring the Module.....	2
Select the Component	3
Define a Learning Period.....	3
Select the Analysis Period	3
Select the user to be analyzed.....	4
Generate Report.....	4
4. Support.....	5
5. Trademarks	6

1. Introduction

Welcome to the User and Entity Behavior Analytics document for LepideAuditor.

With LepideAuditor, you can identify single point anomalies to easily understand when users are doing something that is outside of normal behavior. The UEBA section within LepideAuditor allows you to determine exactly why something has been flagged as unusual based upon numerous factors including, time, event criticality, operation and location.

Analyze user behavior based upon a predefined learning period to accurately identify potential insider threats.

2. Purpose of this Document

The purpose of this document is to take you through the configuration of User and Entity Behavior Analytics in LepideAuditor and give you a glimpse of how the User and Entity Behavior Analytics can help you solve business problems.

3. Configuring the Module

User and Entity Behavior Analytics can be configured by following the below steps:



3.1 Select the Component

Select the component in this filter as per your requirement. There are 2 choices available: File Server and Active Directory.

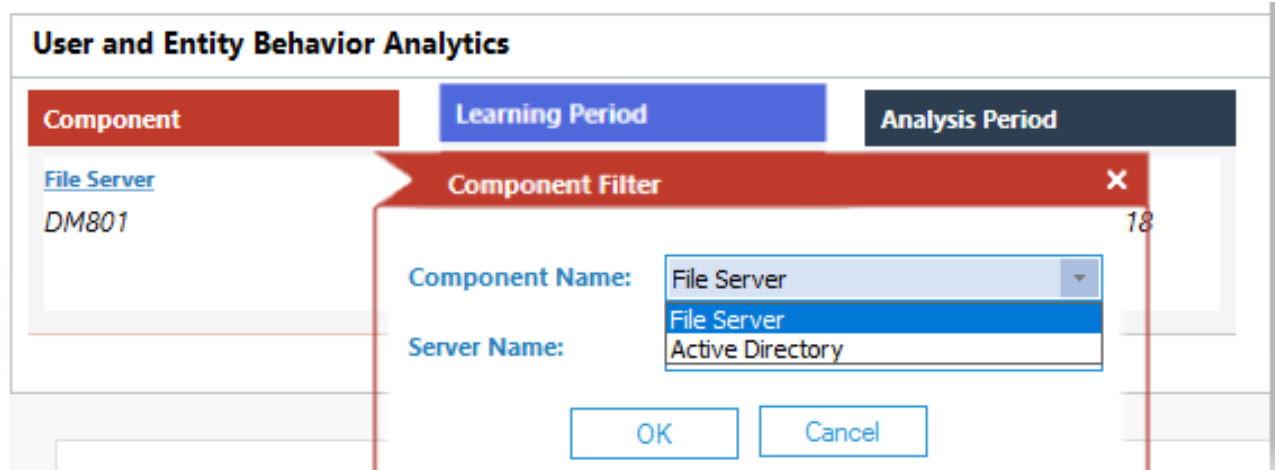


Figure 1: Selecting the component

3.2 Define a Learning Period

In this step, define a learning period for the solution to study the changes and the trends from your environment. We recommend to keep this period as long as you can. The more time the solution will get to study, the more accurately it can spot the anomalies in the components.

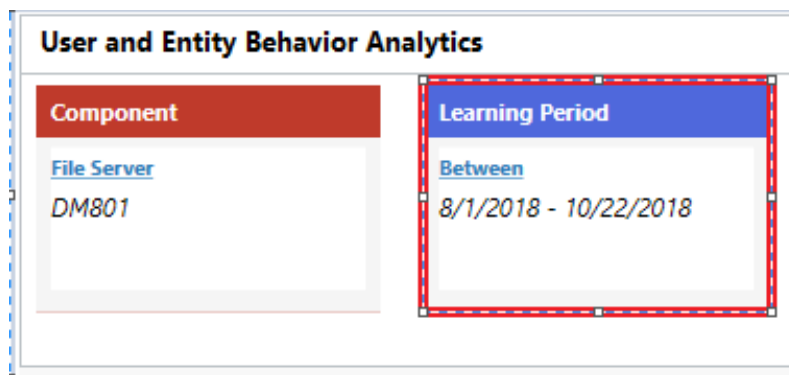


Figure 2: Defining a learning period

3.3 Select the Analysis Period

Now, select the period in which you want the solution to spot the anomalies for you. The solution will look for any unfamiliar events in this period and report back to you all the changes which have never been seen before.

User and Entity Behavior Analytics

Component File Server DM801	Learning Period Between 8/1/2018 - 10/22/2018	Analysis Period Between 4/1/2018 - 10/22/2018
--	--	--

Figure 3: Selecting the Analysis Period

3.4 Select the User to be Analyzed

In this section, you need to select the user whose behavior is to be analyzed by the solution. The solution will give you a list of users who have done changes in the learning period and you would need to select a user from the list.

User and Entity Behavior Analytics

Component File Server DM801	Learning Period Between 8/1/2018 - 10/22/2018	Analysis Period Between 4/1/2018 - 10/22/2018	Selected User LPDE8\administrator
--	--	--	---

Figure 4: Selecting the user to be analyzed

3.5 Generate Report

Click on the generate report option now to enable the solution to trace all the changes and report back with the anomalies if they are found.

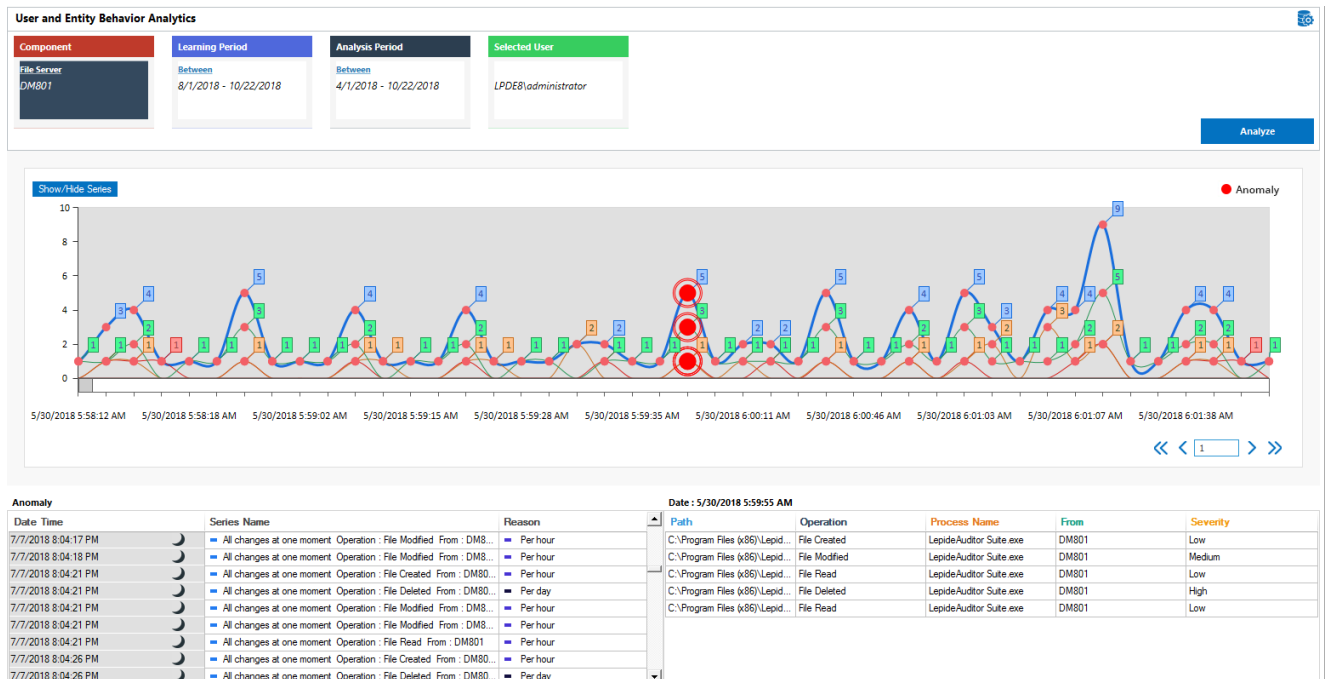


Figure 5: Generate a report

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 <http://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 <http://www.lepide.com/lepideauditor/>.

5. Trademarks

LepideAuditor, LepideAuditor App, LepideAuditor App Server, LepideAuditor (Web Console), LepideAuditor Logon/Logoff Audit Module, LepideAuditor for Active Directory, LepideAuditor for Group Policy Object, LepideAuditor for Exchange Server, LepideAuditor for SQL Server, LepideAuditor 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.