Lepide

USE CASE GUIDE

HOW TO PERFORM AN INVESTIGATION ON A PRIVILEGED USER

Table of Contents

1 Introduction

Users who have administrative privileges are the most important users within your organization, but they also represent the biggest risk to your data security.

Administrative rights are essential to the efficient running of any IT system as they enable trusted users to perform essential tasks like installing software, adding new accounts, creating passwords and the many other system modifications needed to do their job.

The flip side of this, however, is that admin rights provide the user with the 'keys to the kingdom' and therefore present a huge risk to the security of an organization's data.

2 Privilege Abuse

When a user, either intentionally or accidentally, misuses legitimate privileges they have been granted it is known as privilege abuse. Despite these privileges being legitimately granted, users may access resources or perform actions that compromise data security.

Whether privilege abuse occurs through users purposefully mishandling data, or through employee carelessness, it is a security threat that must be taken seriously.

To be able to monitor any potential threat, it is essential for an organization to have complete visibility over the actions of their privileged users. But without a solution in place, tracking user activity can be a complex and time-consuming task.

3 Why Investigate a Privileged User?

The following scenario of a disgruntled employee is an example of why you might want to track a specific privileged user:

> Jill is an administrator of a company and has worked there for just over 15 years. She has always been a very loyal and diligent employee and there has never been any cause to doubt her integrity.
>
> Recently a new managerial job has been created within the company which Jill thinks she is perfect for. Because of her loyalty and hard work, she assumes she will get this position. She goes through the interview process thinking it's just a formality and has her heart set on this new job with more responsibility but with a higher salary and other additional financial benefits.
>
> But Jill does not get the job. A candidate from outside the company is selected and Jill is devastated.
>
> Jill feels angry and resentful of her employers and decides she will resign rather than work for this new manager.

As Jill has admin privileges, she could potentially cause a lot of damage to the company and put their IT systems at a high level of risk. Without a solution in place, it would be almost impossible to track everything that Jill has done and so any malicious activity would go unnoticed until it caused a problem.

4 The Lepide Solution

The Lepide Data Security Platform offers a solution to this scenario. It has functionality to enable you to report on all activities for a particular user over a specified time-period and across all installed components.

In the scenario described in Section 3 above, the company can track all activity for Jill in the weeks leading up to her resignation. If there is any suspicious activity, it can be investigated, and then remedial action taken to mitigate risk and reduce any damage.

5 How to Track the Actions of a Privileged User

All user actions are tracked using the **All Environment Changes Report**

This is a holistic approach whereby all changes are reported across the different components including File Server, Active Directory and Microsoft 365.

5.1 Running the Report

Follow the steps below to run the **All Environment Changes Report**:

- Click the **User and Entity Behavior Analytics**  icon
- The All Environment Changes screen is displayed
- From the tree structure on the left-hand side, click on **All Environment Changes** to display the **All Environment Changes Report:**

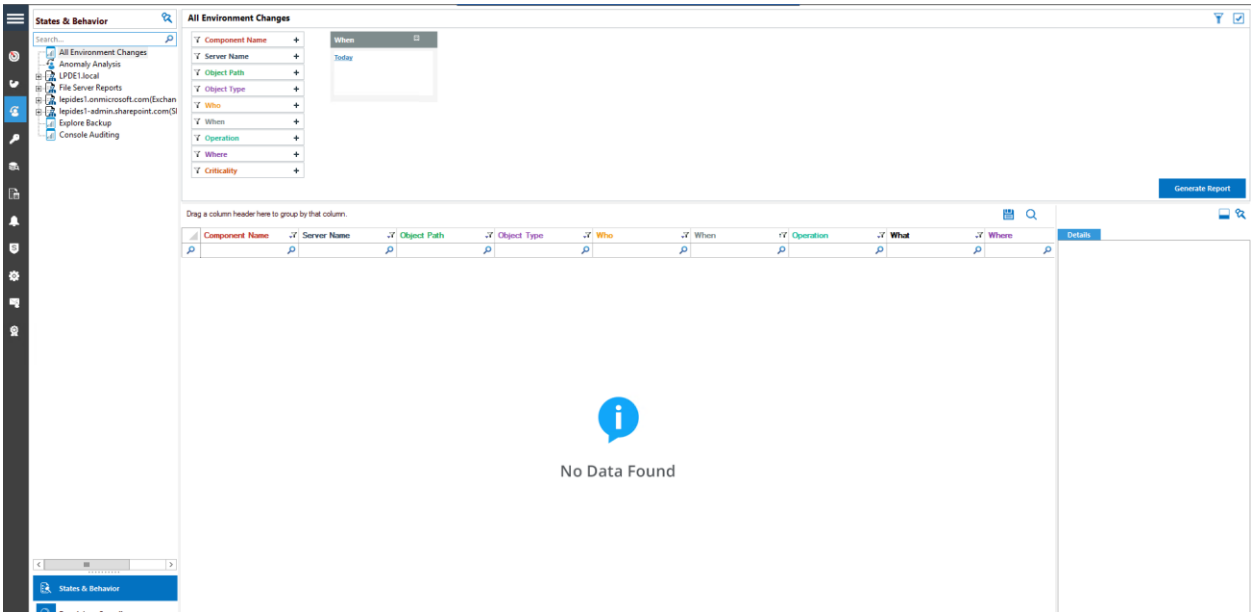


Figure 1: The All Environment Changes Report

5.1.1Specify 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:

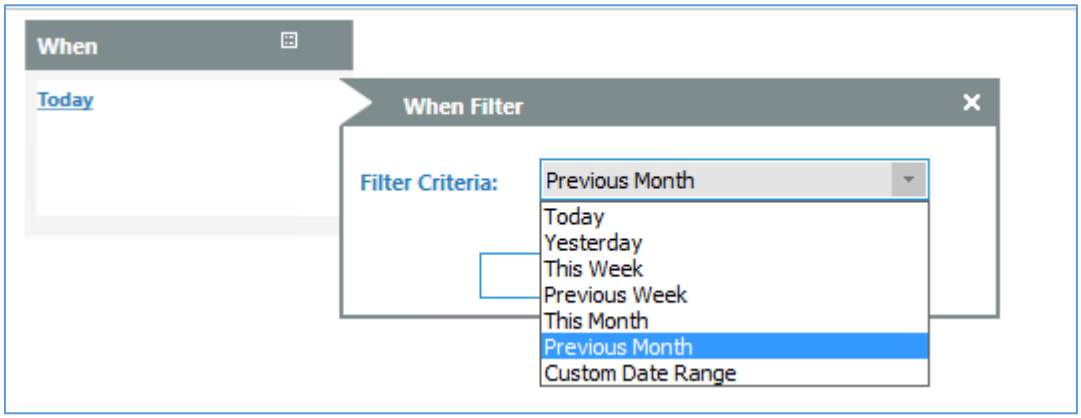


Figure 2: Date Range Filter

- Select a date range from the list
- Click **OK** and you will return to the **All Environment Changes** screen

5.1.2Specify the User

From the list of filter options, click **Who**

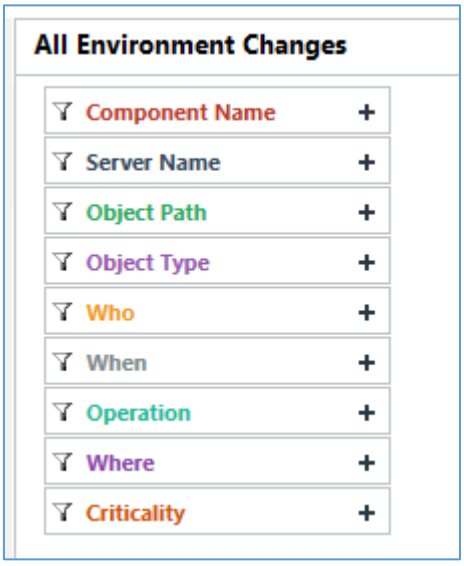


Figure 3: Filter Options

The Who Filter dialog box is displayed:

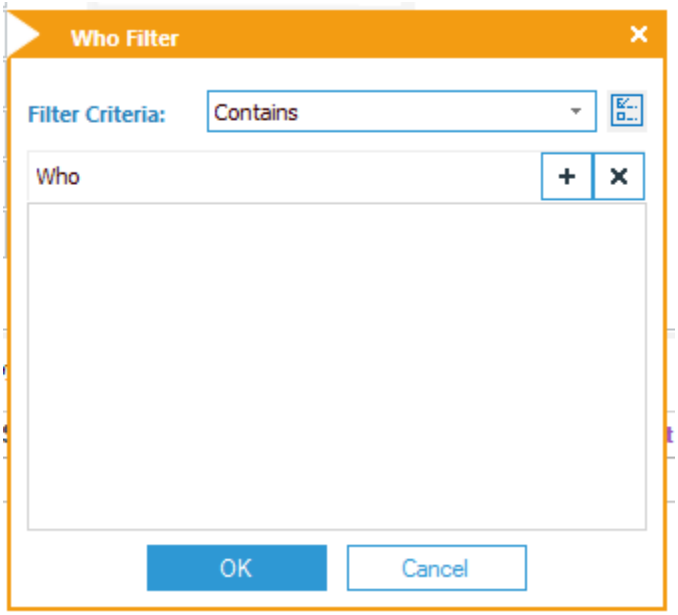


Figure 4: Who Filter

- Click the + button to add the name you want to filter by
- Click **OK**
- Click **Generate Report**

In the example below, the report has been filtered on **Previous Month** and **Jill**:

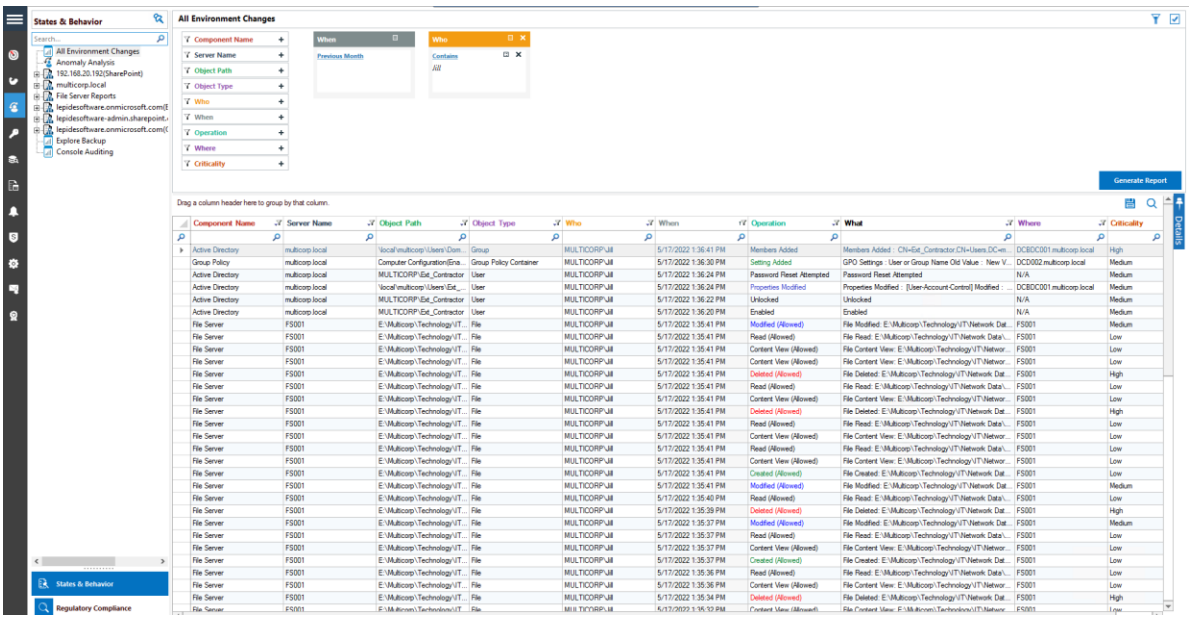
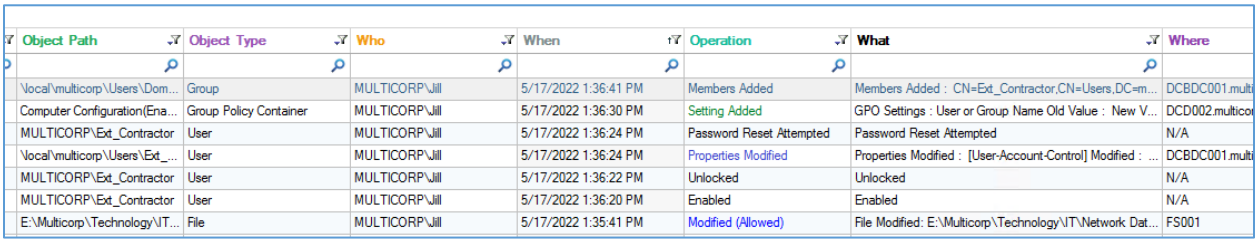


Figure 5: All Environment Changes Report with Filters

The report shows all system activity for **Jill** in **May** and includes some actions that require further investigation.

If we analyze the extract below, we can see a pattern of suspicious behavior:

- We can see that an external contractor account was enabled, and the account was then unlocked
- Immediately after this, we can see the password was reset on the account
- Following this, the accounts privileges have been escalated by adding it to the domain admins group
- Finally, we can see a modification to the security settings of a Group Policy object whereby the account has now been given remote login rights.



Object Path	Object Type	Who	When	Operation	What	Where
\local\multicorp\Users\Dom...	Group	MULTICORP\Jill	5/17/2022 1:36:41 PM	Members Added	Members Added : CN=Ext_Contractor,CN=Users,DC=m...	DCBDC001.multi
Computer Configuration(Ena...	Group Policy Container	MULTICORP\Jill	5/17/2022 1:36:30 PM	Setting Added	GPO Settings : User or Group Name Old Value : New V...	DCD002.multico
MULTICORP\Ext_Contractor	User	MULTICORP\Jill	5/17/2022 1:36:24 PM	Password Reset Attempted	Password Reset Attempted	N/A
\local\multicorp\Users\Ext_...	User	MULTICORP\Jill	5/17/2022 1:36:24 PM	Properties Modified	Properties Modified : [User-Account-Control] Modified : ...	DCBDC001.multi
MULTICORP\Ext_Contractor	User	MULTICORP\Jill	5/17/2022 1:36:22 PM	Unlocked	Unlocked	N/A
MULTICORP\Ext_Contractor	User	MULTICORP\Jill	5/17/2022 1:36:20 PM	Enabled	Enabled	N/A
E:\Multicorp\Technology\IT...	File	MULTICORP\Jill	5/17/2022 1:35:41 PM	Modified (Allowed)	File Modified: E:\Multicorp\Technology\IT\Network Dat...	FS001

Figure 6: Extract of Report

5.1.3Details Window

To see more information about a particular event in the report, select the row containing the event and click Details to display the details window:

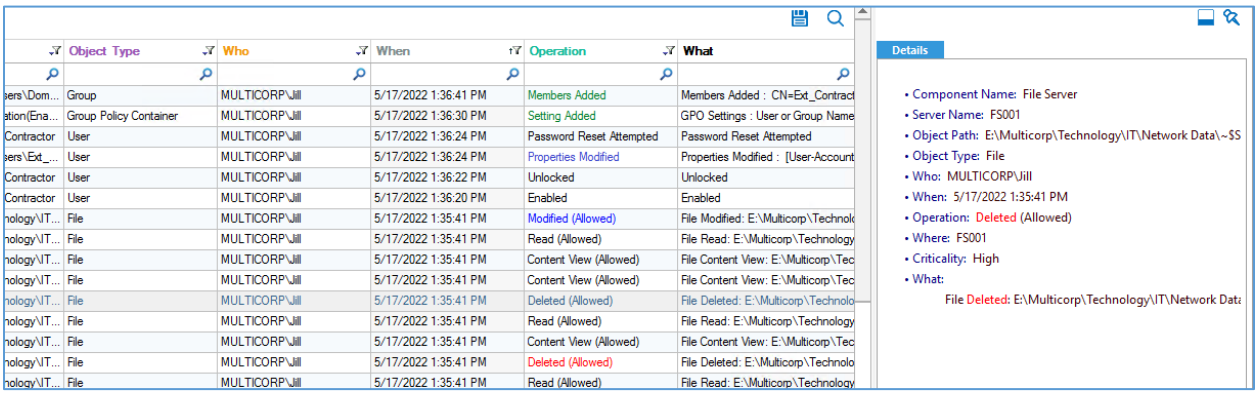


Figure 7: Report with Details Window Displayed

6 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/.

7 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.