



USER GUIDE

LEPIDE SIEM INTEGRATION

Table of Contents

- 1. Introduction 3
- 2. Why Integrate your SIEM Solution with the Lepide Data Security Platform?..... 3
 - 2.1. Integrate With Any SIEM Solution..... 3
- 3. Prerequisites..... 3
- 4. Configuring Lepide to be used with a SIEM Application..... 4
- 5. Support..... 9
- 6. Trademarks..... 9

1. Introduction

This guide is an introduction to integrating your Security Information and Event Management (SIEM) solution within the Lepide Data Security Platform.

2. Why Integrate your SIEM Solution with the Lepide Data Security Platform?

Many enterprise organizations implement Security Information and Event Management (SIEM) solutions into their IT environment to provide granular audit detail and meet compliance demands.

However, SIEM solutions, whilst being able to generate and analyze huge amounts of audit data, are not always very intuitive when it comes to enabling users to spot and prevent data breaches.

The Lepide Data Security Platform provides a solution to this. It enables you to quickly identify what the SIEM user behavior alerts are trying to say by giving real world context to them.

Once you have context to the raw audit data that is being generated, you can speed up your detection and response to any unwanted or unauthorized changes. You will save yourself both time and money by not having to sift through mountains of indexed data. The Lepide Data Security Platform can do the work for you.

2.1. Integrate With Any SIEM Solution

The Lepide Data Security Platform can integrate with any SIEM solution, **including Splunk, LogRhythm, IBM QRadar, HP ArcSight and more.**

You can also have multiple SIEM integrations running simultaneously through the Lepide Data Security Platform.

3. Prerequisites

You will need to configure the port inside the SIEM solution, to be used by the Lepide Data Security Platform for communication.

4. Configuring Lepide to be used with a SIEM Application

Follow the steps below to configure the Lepide Data Security Platform to be used with a SIEM application:

1. Click on the SIEM  icon to go to the Security Information and Event Management screen

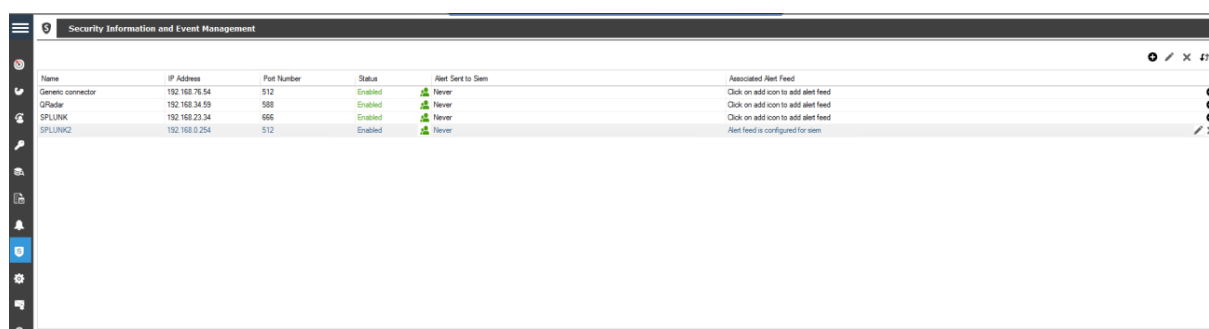

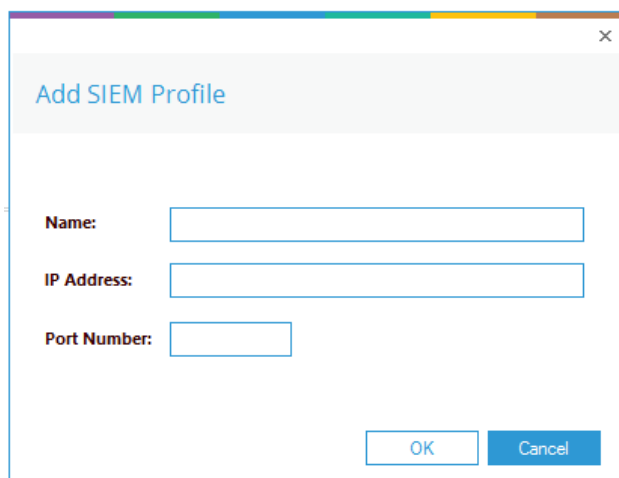


Figure 1: Security Information and Event Management

2. Click on the **Add SIEM Account** icon  at the top right corner of the screen to add a SIEM Account.

The Add SIEM Profile dialog box is displayed:



Add SIEM Profile

Name:

IP Address:

Port Number:

OK Cancel

Figure 2: Add SIEM Profile

3. Fill in the **Name**, **IP Address** and **Port Number**

4. Click **OK**

The Configure Alert Feed message box is displayed:

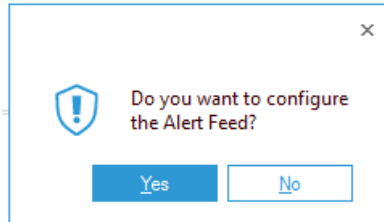


Figure 3: Configure Alert Feed

5. Click **Yes** to configure the Alert Feed.

The Select Report(s) dialog box is displayed:

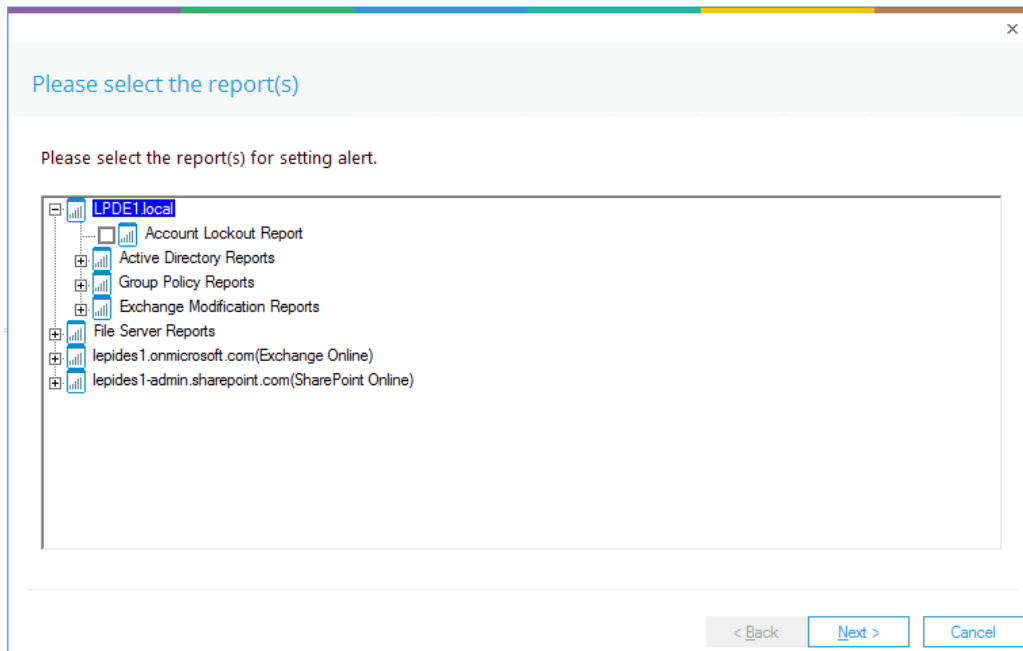


Figure 4: Select Reports

6. Select the reports for which you want to send the alerts
7. Click **Next**

The Set Filter(s) dialog box is displayed:

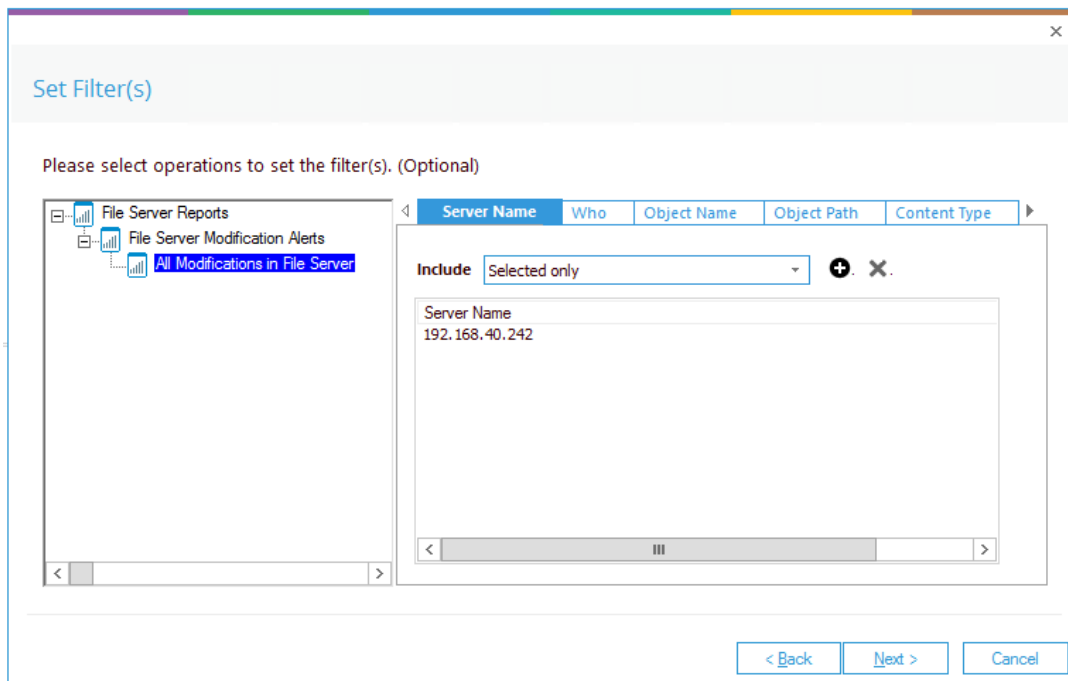


Figure 5: Set Filter(s)

There are options to change the settings for **Server Name**, **Who**, **Object Name**, **Object Path**, **Content Type**, **Compliance**, **Monetary Value**, **Operation**, **Event Status Process Name** and **From** using the tabs at the top of this dialog box.

8. Select any filters required
9. Click **Next**

The Confirmation dialog box is displayed:

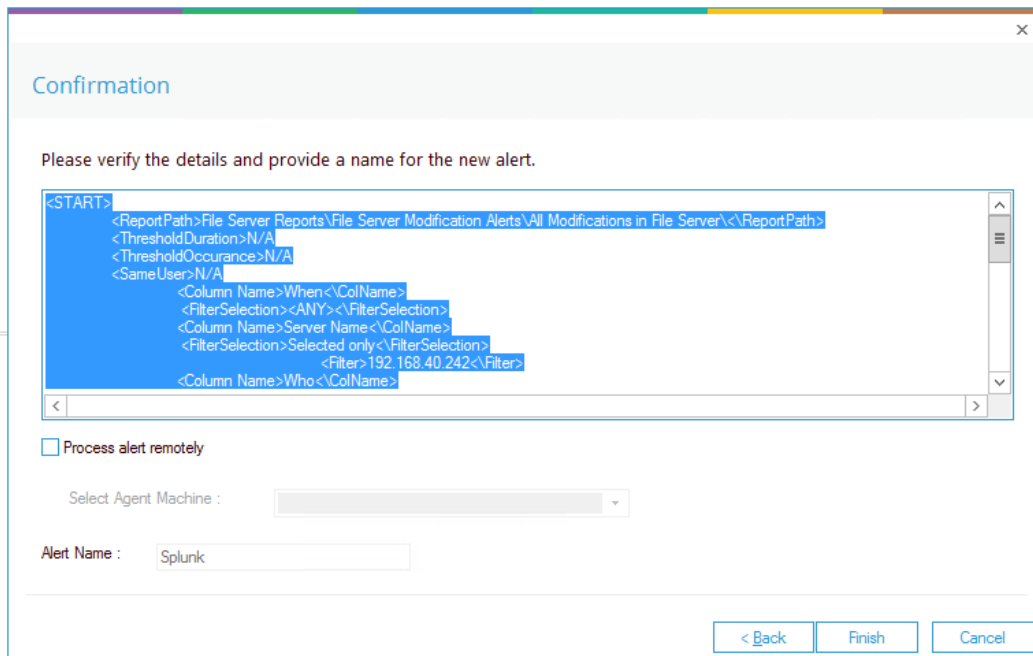


Figure 6: Confirmation

10. Click **Finish**

You will return to the Security information and Event Management screen:

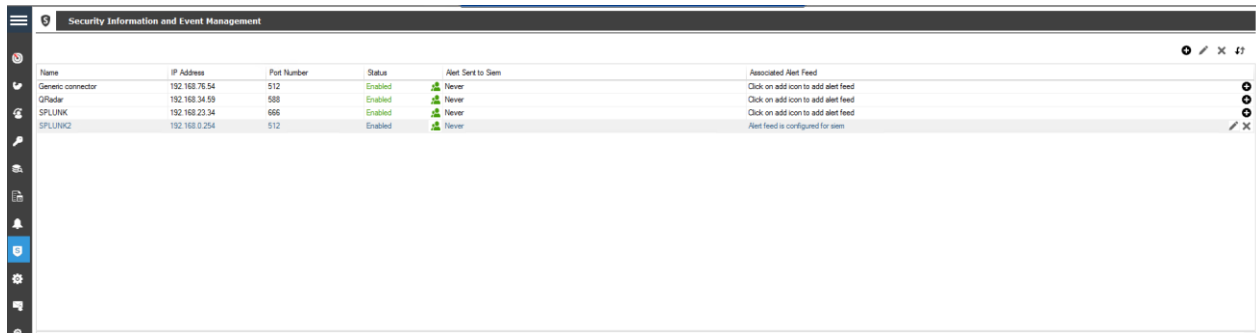


Figure 7: Security Information and Event Management Screen

As soon as the alert is sent, the column **Alert Sent to SIEM** will update with the relevant time stamp. If the connection is broken, it will be shown as **Unsuccessful**.

You can enable or disable the SIEM account at any time by clicking the Status field. The following message box will be displayed:

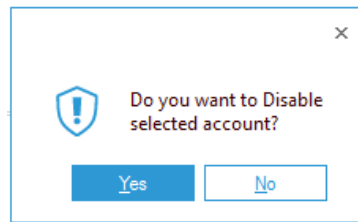




Figure 8: Disable Selected Account

- You can modify the alert by clicking the **Modify Alert** icon 
- You can remove the alert by clicking the **Delete Alert** icon 

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.

