



USE CASE GUIDE

HOW TO DETECT WHEN AN EMAIL WITH SENSITIVE DATA HAS BEEN SENT

Table of Contents

- 1. Introduction..... 3
- 2. Exchange Server..... 3
- 3. The Lepide Solution 3
- 4. The Potential Data Leakage Threat Model 3
 - 4.1. Prerequisites 3
- 5. The Classified Emails Report 10
 - 5.1. Prerequisites 10
 - 5.2. Running the Classified Emails Report..... 10
 - 5.3. Filtering the Report..... 12
- 6. Support 14
- 7. Trademarks..... 14

1. Introduction

Data breaches are a serious threat to any organization and steps need to be taken to keep the risk of their occurrence to a minimum. The focus at Lepide is to provide visibility over what's happening with your data and through visibility you can take the necessary action to mitigate risk and stay compliant.

2. Exchange Server

Email is an essential element of nearly all business processes within every type of organization and Exchange Server is the standard used to connect with colleagues, customers, and partners to make business decisions and share information.

However, the confidentiality and integrity of email data is an essential element of a security strategy and is as mission critical as Active Directory and Windows Server.

Visibility as to what activity is taking place across your Exchange Server is key to being able to keep your data secure and remain compliant. Once it is evident that sensitive data is being shared improperly, alerts can be triggered, and immediate steps taken to mitigate risk and reduce further damage.

But without a solution in place, keeping track of what is being sent, who sent it, and when can be a complex task.

3. The Lepide Solution

The Lepide Data Security Platform provides a solution to this complexity with the **Potential Data Leakage Threat Model** and the **Classified Emails Report**.

The Threat Model will trigger an alert as soon as sensitive data is sent by email. The report provides detailed information about any emails which have been sent containing sensitive data.


4. The Potential Data Leakage Threat Model

When configured, the Potential Data Leakage Threat Model will generate an alert whenever sensitive data has been leaked or shared with other users via an email exchange.

4.1. Prerequisites

Before configuring the Potential Data Leakage Threat Model, you will need to configure **Data Discovery & Classification for Exchange Online** and choose **On the Fly Classification**. For instructions on how to do this please refer to our [Data Discovery and Classification Configuration Guide](#).

To set up the Potential Data Leakage Threat Model:

- Click the **Alerts** icon  from the left-hand toolbar to display all the Threat Models available.
- To enable the **Potential data leakage Threat Model**, move the slide toggle to the right as shown here:

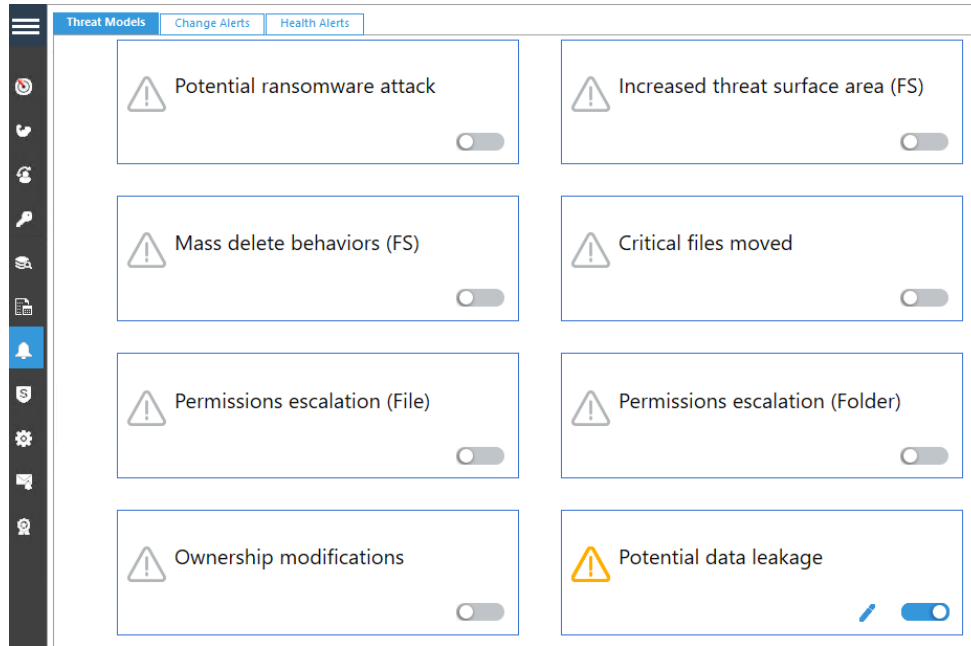


Figure 1: Threat Models

- Click the  icon to configure the alerts and responses you require.

This will start a wizard:

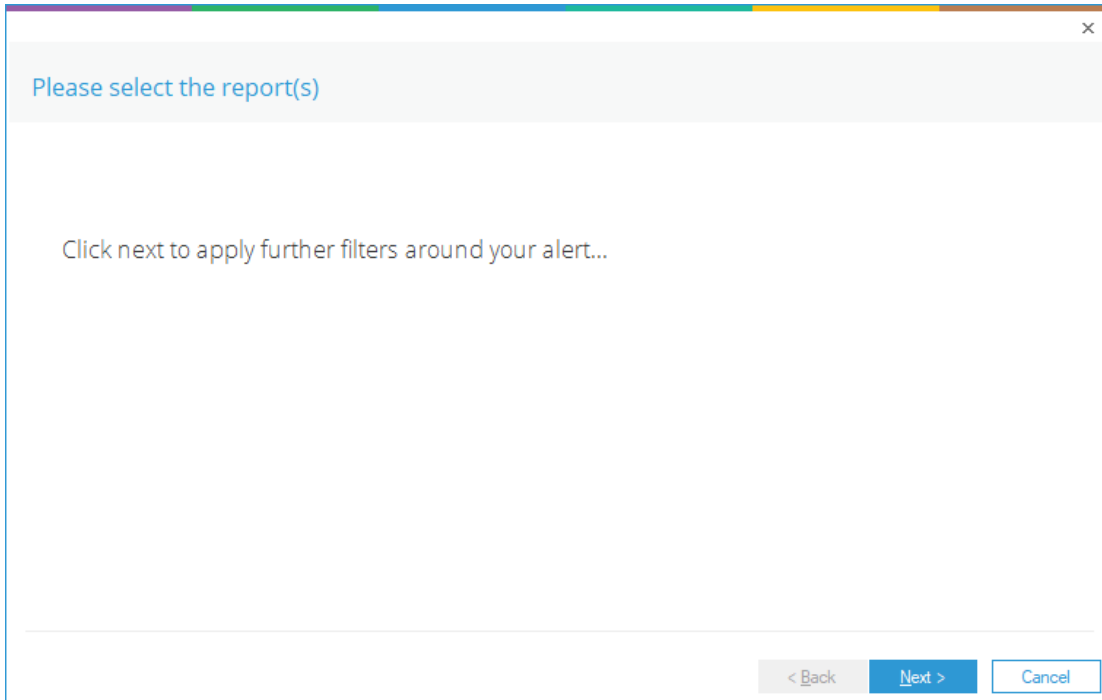


Figure 2: Wizard to Configure Alerts

- Click **Next** to display the Set Filter(s) dialog box:

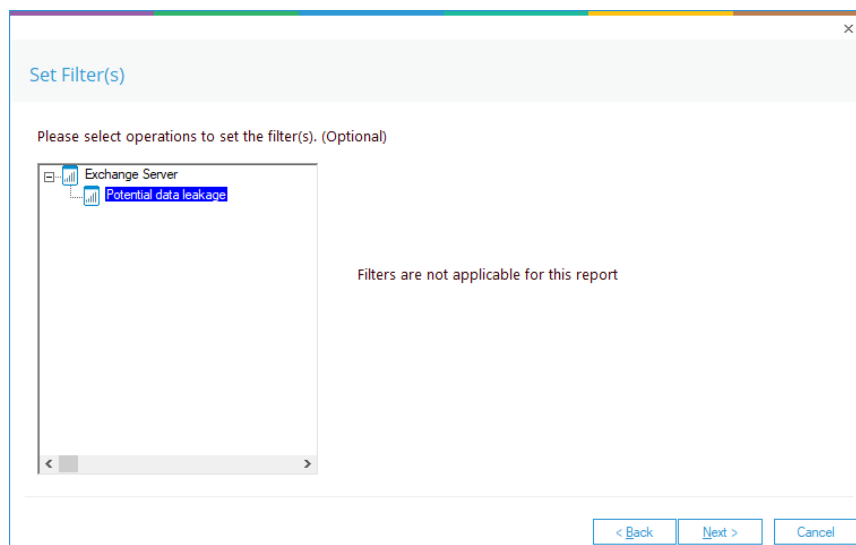


Figure 3: Set Filters

- There are no filters needed for this report, so click **Next** to continue

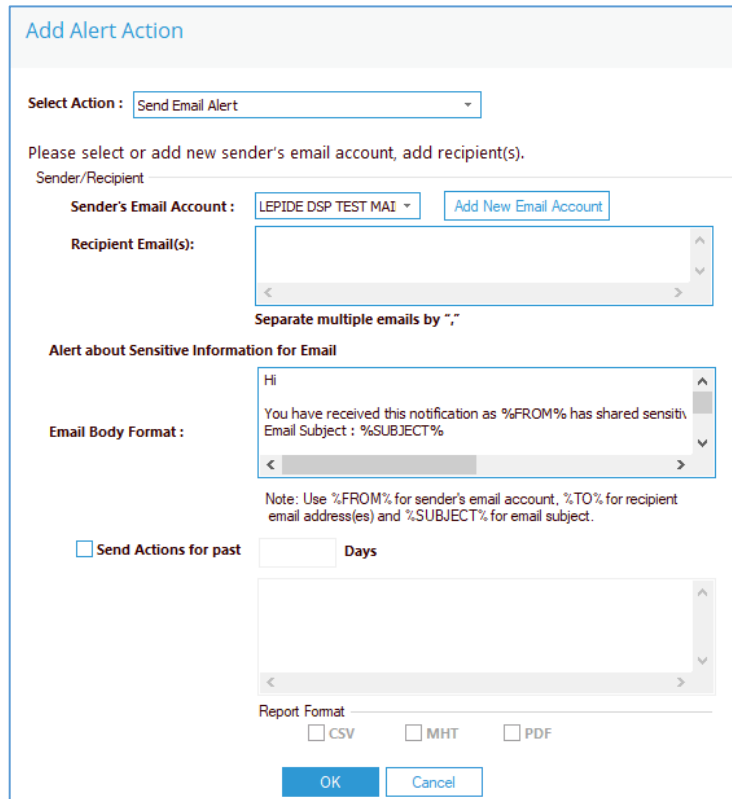


Figure 5: Add Alert Action

This option allows you to send an email once an alert has been triggered. The elements of the dialog box are as follows:

Sender's Email Account: The Sender's email account will be displayed here if it has been selected. Click **Add New Email Account** to enter a new Sender's Email Account

Recipient Email(s): Add recipient emails by typing the email addresses into the box. If there are multiple email addresses, separate them with a ','

Send Actions for past xx days: This option allows you to see everything that this user has done over the last number of specified days. For example, if an alert is triggered because an email with sensitive data has been sent, you may want to see what else has been happening for that account. Check this box and specify the number of days and an email will be sent with an attachment listing everything that the user has done over the specified number of days.

The attachment will contain a report and the format(s) can be specified by checking the relevant box. The formats are CSV, MHT and PDF.

- Click **OK** to save the alert action.

You will return to the Alert Settings dialog box and any alert you have set will now be displayed here:

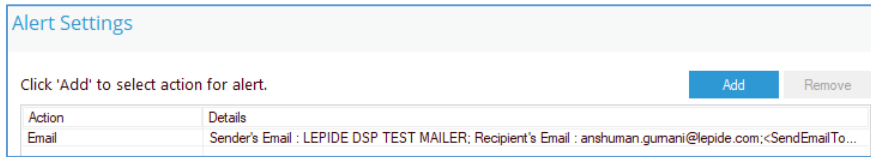


Figure 6: Alert Settings with an Alert Added

- Click **Next**

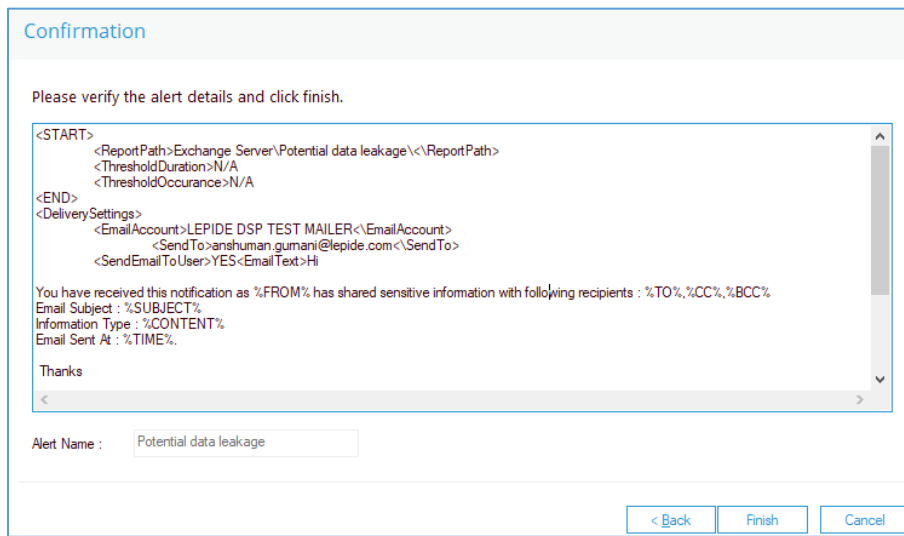


Figure 7: Confirmation

The Alert is now setup. As soon as an email exchange takes place, the Lepide Data Security Platform will invoke the Alert settings and send an email to the recipient as shown below:

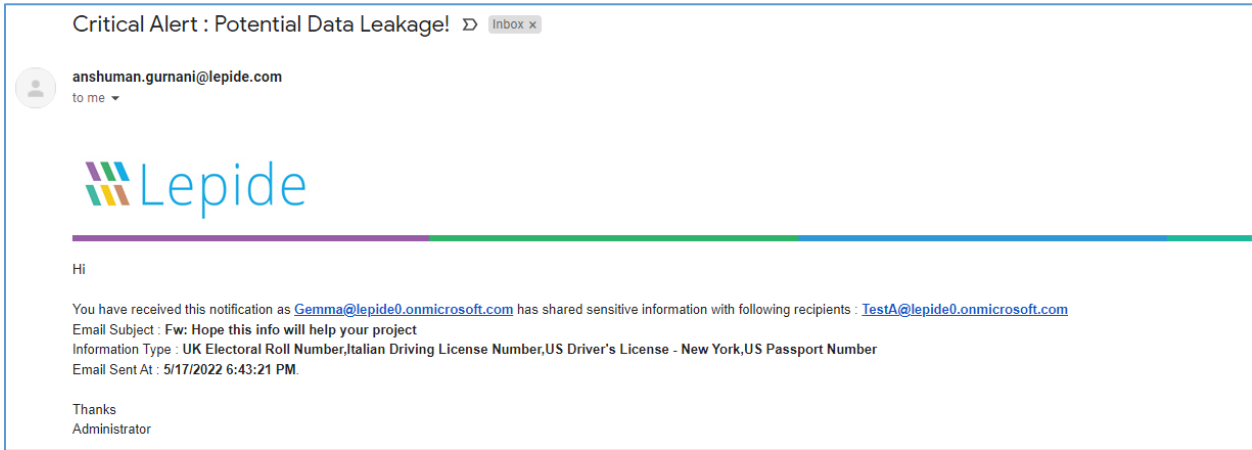


Figure 8: Alert Notification Email

The Alert notification can also be seen in the Alert Summary Report.

To run the Alert Summary Report:

- Click the **Permissions & Privileges**  icon
- Expand **Risk Analysis** (from the tree structure to the left side of the screen)
- Click on **Alert Summary** to display the **Alert Summary Report**

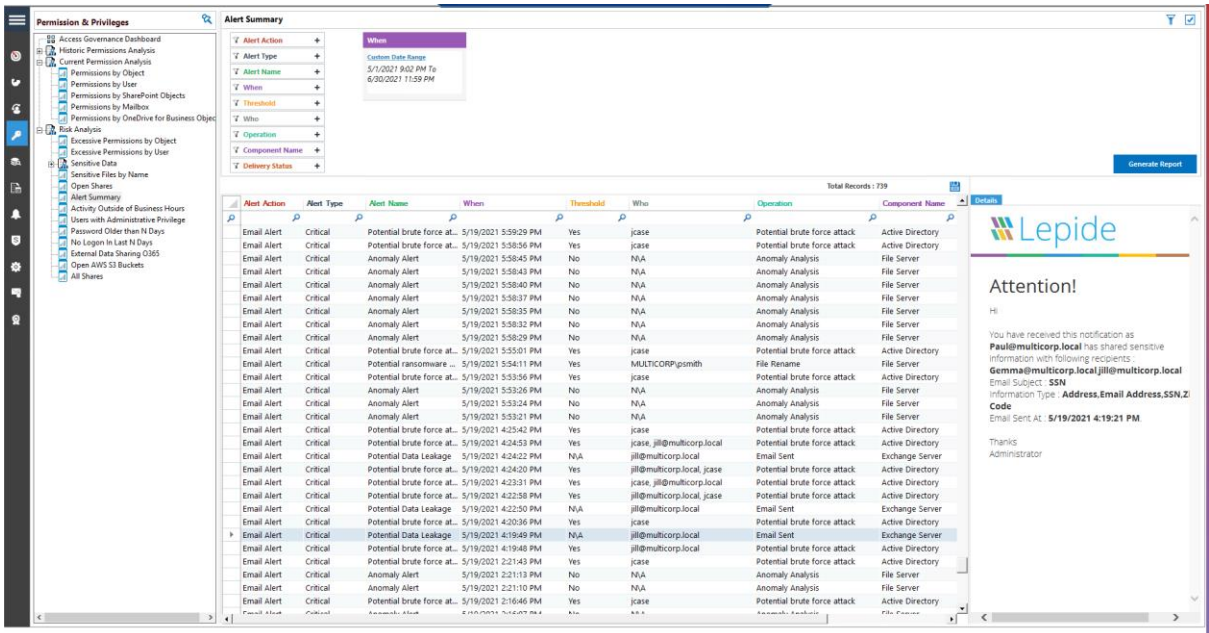


Figure 9: Alert Summary Report


When you click on a particular row it will show the content of the alert email in the details window to the right-hand side of the screen.

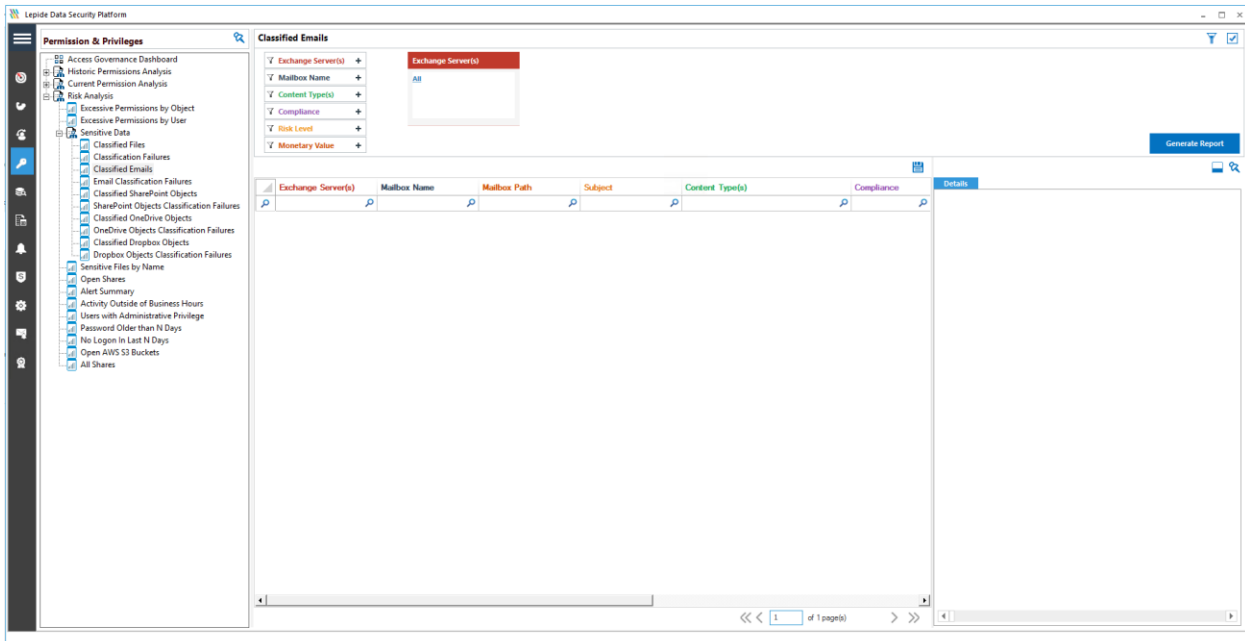
5. The Classified Emails Report

5.1. Prerequisites

Before running the classified emails report you will need to configure Data Discovery & Classification for Exchange Online. For information on how to do this, please refer to the [Data Discovery and Classification Configuration Guide](#).

5.2. Running the Classified Emails Report

- Click the **Permissions & Privileges**  icon
- Expand **Risk Analysis** (from the tree structure to the left side of the screen)
- Expand **Sensitive Data**
- Click on **Classified Emails** to display the **Classified Emails Report**:



The screenshot displays the Lepide Data Security Platform interface. On the left, a navigation tree under 'Permissions & Privileges' is expanded to 'Sensitive Data' > 'Classified Emails'. The main area shows the 'Classified Emails' configuration panel with filters for Exchange Server(s), Mailbox Name, Content Type(s), Compliance, Risk Level, and Monetary Value. Below this is a table with the following columns: Exchange Server(s), Mailbox Name, Mailbox Path, Subject, Content Type(s), and Compliance. The table is currently empty. A 'Generate Report' button is visible in the top right of the configuration area.

Figure 10: Classified Emails Report

- From the top of the screen under Exchange Server(s), click to select the required Exchange Server:

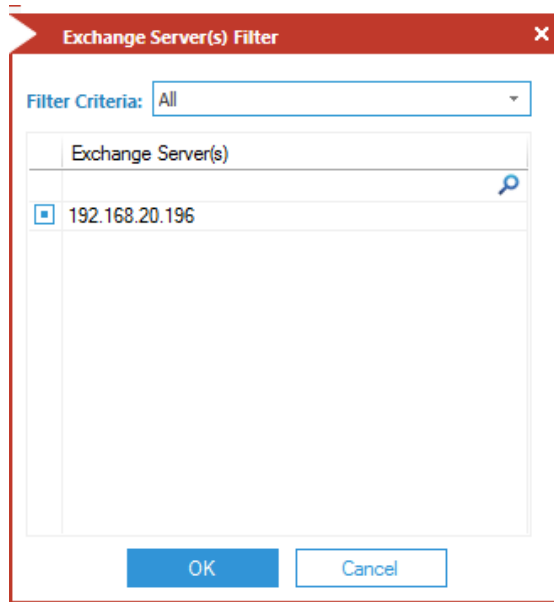


Figure 11: Exchange Server Filter

- Click **Generate Report**

Any sensitive email exchange between any users or their mailboxes within the selected exchange server will be listed in the report:

Exchange Server(s)	Mailbox Name	Mailbox Path	Subject	Content Type(s)	Compliance	Cases	Risk Level	Monetary Value	Classification Date
192.168.20.196	Gemma White	Gemma@multicorp.local	Handling your Email Ad...	Email Address, Addresses Name	GDPR, GLBA	56	553	\$ 1083	12/16/2021 11:12:56
192.168.20.196	Jill Case	jill@multicorp.local	Confidential	Email Address, Addresses Name	PI, Confidential	64	553	\$ 1963	12/16/2021 11:12:56
192.168.20.196	Jill Case	jill@multicorp.local	Confidential Information	Email Address	PI, Confidential	64	1024	\$ 2432	11/16/2021 12:32:10
192.168.20.196	Jill Case	jill@multicorp.local	Confidential	SSN	PI, Confidential	32	1154	\$ 2912	11/16/2021 12:51:28
192.168.20.196	Jill Case	jill@multicorp.local	Zip Codes	Zip Code	PI, Confidential	26	442	\$ 1326	11/16/2021 12:48:19
192.168.20.196	Jill Case	jill@multicorp.local	Email IDs	Email Address	PI, Confidential	55	995	\$ 2605	11/16/2021 12:47:48
192.168.20.196	Jill Case	jill@multicorp.local	Sensitive Information	SSN	PI, Confidential	15	990	\$ 4455	11/16/2021 12:47:28
192.168.20.196	Jill Case	jill@multicorp.local	PI attached	PI	PI, Confidential	30	1674	\$ 7533	11/16/2021 12:44:54
192.168.20.196	Jill Case	jill@multicorp.local	Medicare Information	US Medicare	HIPAA	29	522	\$ 2349	11/16/2021 12:43:34
192.168.20.196	Jill Case	jill@multicorp.local	Medical Details	US Medicare	HIPAA	29	522	\$ 2349	11/16/2021 12:42:07
192.168.20.196	Gemma White	Gemma@multicorp.local	Zip Codes attached	Zip Code	PI, GDPR	42	739	\$ 3402	11/16/2021 12:39:47
192.168.20.196	Gemma White	Gemma@multicorp.local	Customer Details	Email Address	PI, GDPR	36	648	\$ 2916	11/16/2021 12:39:07
192.168.20.196	Gemma White	Gemma@multicorp.local	Customer Details	National Insurance Number	PI, GDPR	36	672	\$ 4356	11/16/2021 12:38:22
192.168.20.196	Russell Clarke	Russell@multicorp.local	Sharing SSN Details	SSN	PCI-DSS	57	969	\$ 6097	11/16/2021 12:34:54
192.168.20.196	Russell Clarke	Russell@multicorp.local	Addresses	Zip Code	PCI-DSS	112	784	\$ 2352	11/16/2021 12:33:53
192.168.20.196	Russell Clarke	Russell@multicorp.local	Email Addresses	Email Address	PCI-DSS	47	1974	\$ 3311	11/16/2021 12:33:13
192.168.20.196	Russell Clarke	Russell@multicorp.local	SSN Details	SSN	PCI-DSS	67	2402	\$ 9133	11/16/2021 12:31:02
192.168.20.196	Russell Clarke	Russell@multicorp.local	Card Details	Credit Card Number	PCI-DSS	53	2226	\$ 5989	11/16/2021 12:30:27
192.168.20.196	Russell Clarke	Russell@multicorp.local	Bank Details	Bank Account Number	PCI-DSS	64	1688	\$ 7232	11/16/2021 12:29:44
192.168.20.196	Jill Case	jill@multicorp.local	Doctor Details	SSN	HIPAA, PI	15	630	\$ 1695	11/16/2021 12:27:21
192.168.20.196	Jill Case	jill@multicorp.local	Patient Contact Details	Address	HIPAA, PI	26	1062	\$ 1716	11/16/2021 12:26:49
192.168.20.196	Jill Case	jill@multicorp.local	Patient Sensitive Infor...	SSN	HIPAA, PI	31	1322	\$ 3472	11/16/2021 12:25:45
192.168.20.196	Jill Case	jill@multicorp.local	Patient Email Address	Email Address	HIPAA, PI	24	1008	\$ 2112	11/16/2021 12:25:01
192.168.20.196	Jill Case	jill@multicorp.local	Patient Health Record	National Drug Code	HIPAA	24	792	\$ 2376	11/16/2021 12:24:10
192.168.20.196	Gemma White	Gemma@multicorp.local	Client Address	Email Address	FSMA, NIST	32	1056	\$ 2112	11/16/2021 12:21:14
192.168.20.196	Gemma White	Gemma@multicorp.local	Client Address	Zip Code	FSMA, NIST	44	4136	\$ 8272	11/16/2021 12:20:28
192.168.20.196	Gemma White	Gemma@multicorp.local	Sharing Customer Det...	SSN	FSMA, NIST	23	2162	\$ 4254	11/16/2021 12:19:48
192.168.20.196	Gemma White	Gemma@multicorp.local	Sharing Customer Det...	Email Address	FSMA, NIST	12	1128	\$ 2256	11/16/2021 12:18:06
192.168.20.196	Gemma White	Gemma@multicorp.local	New Customer Contact	National Insurance Number	GDPR, GLBA	18	832	\$ 1763	11/16/2021 10:45:04
192.168.20.196	Jill Case	jill@multicorp.local	Sharing SSN	SSN	GDPR, GLBA	43	832	\$ 1763	11/16/2021 10:42:53
192.168.20.196	Jill Case	jill@multicorp.local	Customer Phone Num...	Phone Number	GDPR, GLBA	38	832	\$ 1763	11/16/2021 10:42:55

Figure 12: The Generated Report

- The report shows which mailboxes, email subjects and content types which were part of the email exchange containing sensitive data.
- To the right of this report, you will be able to see more details in the Compliance column showing which data security compliance has been breached as part of this email exchange.
- The risk level posed, its count and monetary value is also reported. This can be critical information used by administrators to take action to stop any further damage.
- The report also shows if the same email was forwarded to other users, as can be seen in Subject column. The Received Time column can be used to establish an understanding of which data source (or the mailbox) acted as source in this sensitive data breach by email incident. This provides essential information for further investigation.
- Please note that you do not need to add the same Exchange Online Server in the Auditing Module of the Lepide Data Security Platform. Just completing the setup for Data Discovery & Classification is sufficient for generating this one-off report.
- However, if you wish to generate the same report in real-time, then you would need to select the **On the Fly Classification** option on the classification server wizard during the **Data Discovery & Classification** configuration.

5.3. Filtering the Report

- To add filters to the data, click on the filter area above the relevant column and type in the information you want to see.

For example, you may want to see data for a particular Mailbox Name - so click at the top of the **Mailbox Name** column and type the name to be filtered on:

Mailbox Name	Mailbox Path
Gemma	
Gemma White	Gemma@mult
Gemma White	Gemma@mult
Gemma White	Gemma@mult
Gemma White	Gemma@mult
Gemma White	Gemma@mult
Gemma White	Gemma@mult

Figure 13: Filter Area

In the example below, the report has been filtered to show data for **Gemma**:

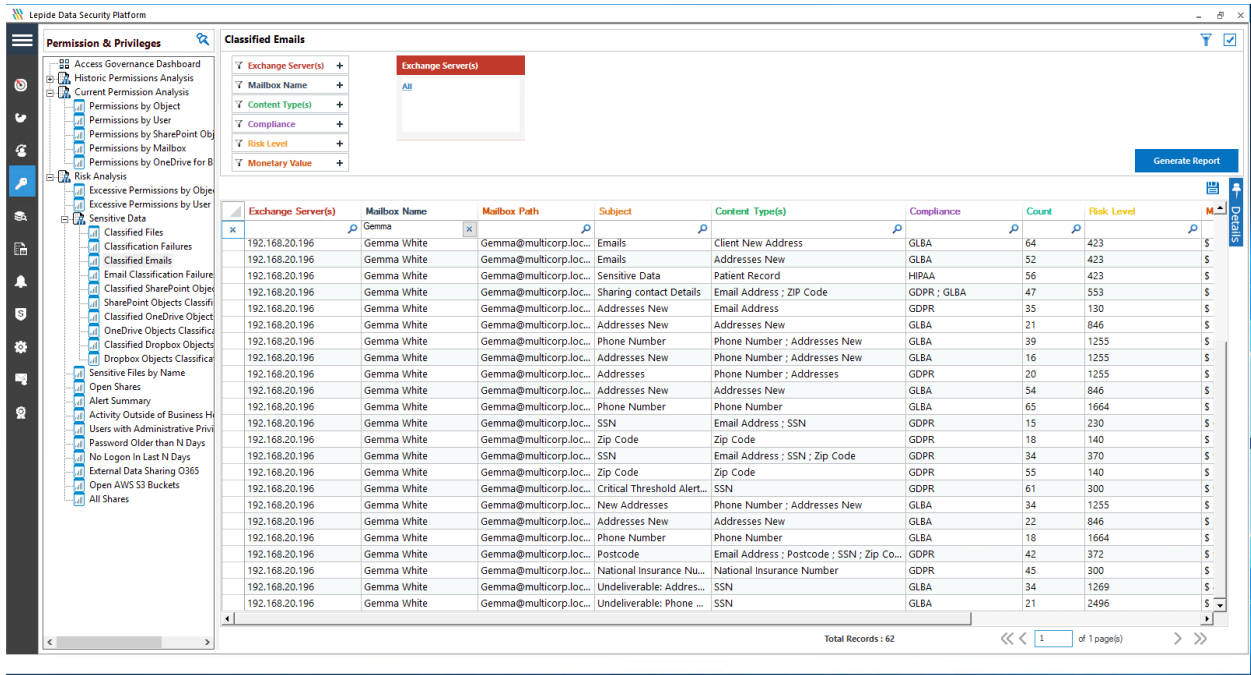


Figure 15: Report Filtered by Mailbox Name

The report can be scheduled, saved, and exported.

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.