

Integrate GFI MailEssentials

EventTracker v8.x and above

Abstract

This guide provides instructions to integrate GFI MailEssentials with EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and GFI MailEssentials.

Audience

IT Admins, GFI MailEssentials administrators and EventTracker users who wish to integrate GFI MailEssentials with EventTracker.

The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2018 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

- Abstract 1
- Scope 1
- Audience..... 1
- Overview..... 3
- Prerequisites..... 3
- Integrate GFI MailEssentials with EventTracker 3
 - GFI MailEssentials Report configuration:..... 3
 - Configure DLA in EventTracker:..... 9

Overview

GFI MailEssentials detects and blocks phishing emails, and adds email management tools to your mail server, including disclaimers, mail monitoring, Internet mail reporting, list server, server-based auto replies and POP3 downloading.

In Microsoft® Exchange environments, GFI MailEssentials also scans the Microsoft® Exchange Information Store.

- Powerful business anti-spam
- Multiple antivirus engine protection
- Enforce email protection content policy

EventTracker consumes the pdf reports configured in GFI MailEssentials and display them in report dashboard.

Prerequisites

- EventTracker v8.x or above should be installed.
- Exchange mail server should be installed.
- GFI MailEssentials must be installed on Mail server.

Integrate GFI MailEssentials with EventTracker

GFI MailEssentials Report configuration:

You can follow the below steps to schedule the custom reports on GFI MailEssentials:

1. To access Reporting, login to the GFI MailEssentials web console and go to

GFI MailEssentials > Reporting.

2. To enable the Reporting
 - a. Go to **Reporting > Settings.**

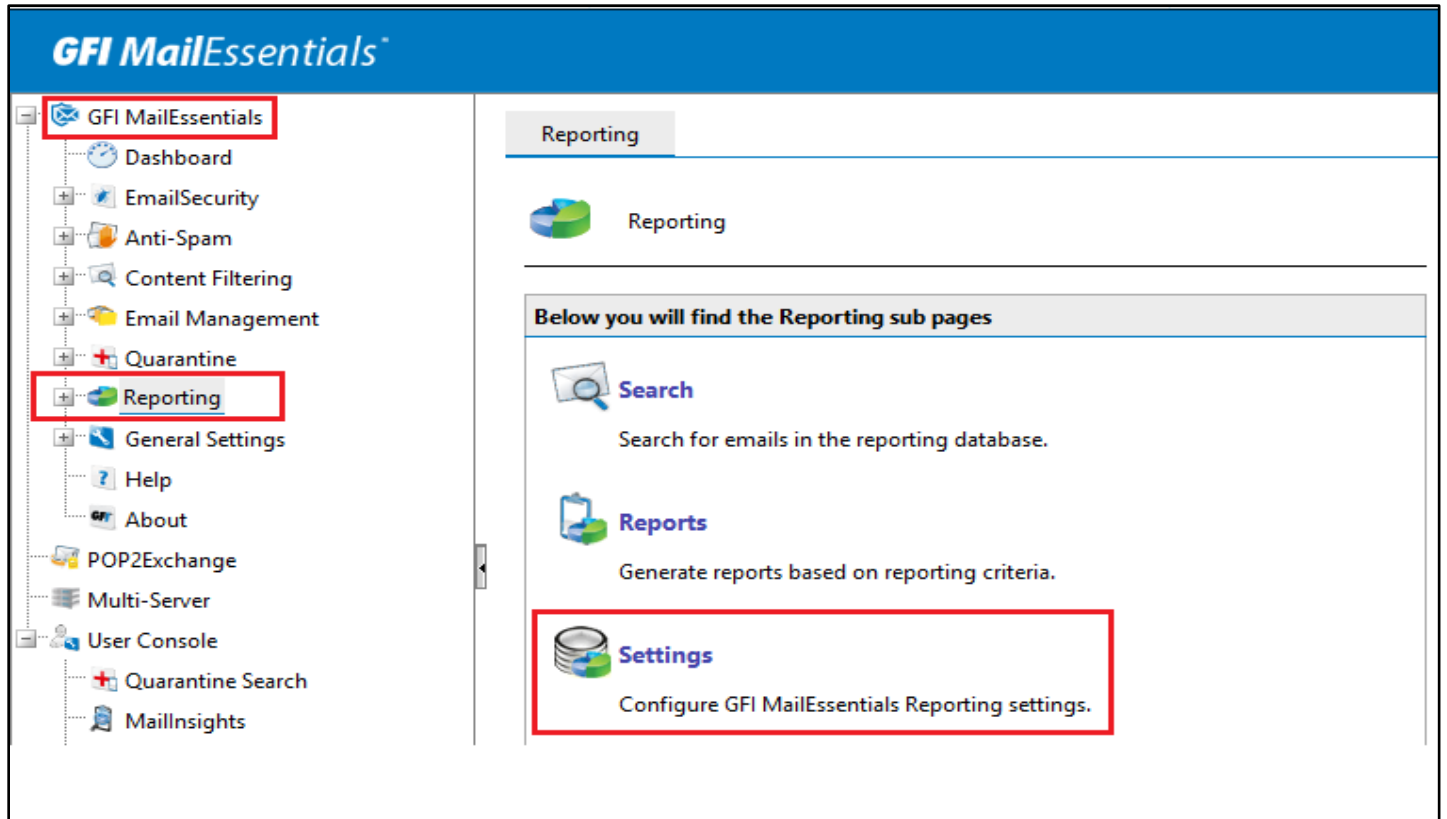


Figure 1

- b. In the **Settings** page, check the **Enable Reporting** option to enable reporting.
- c. To save the changes, click **Apply**.

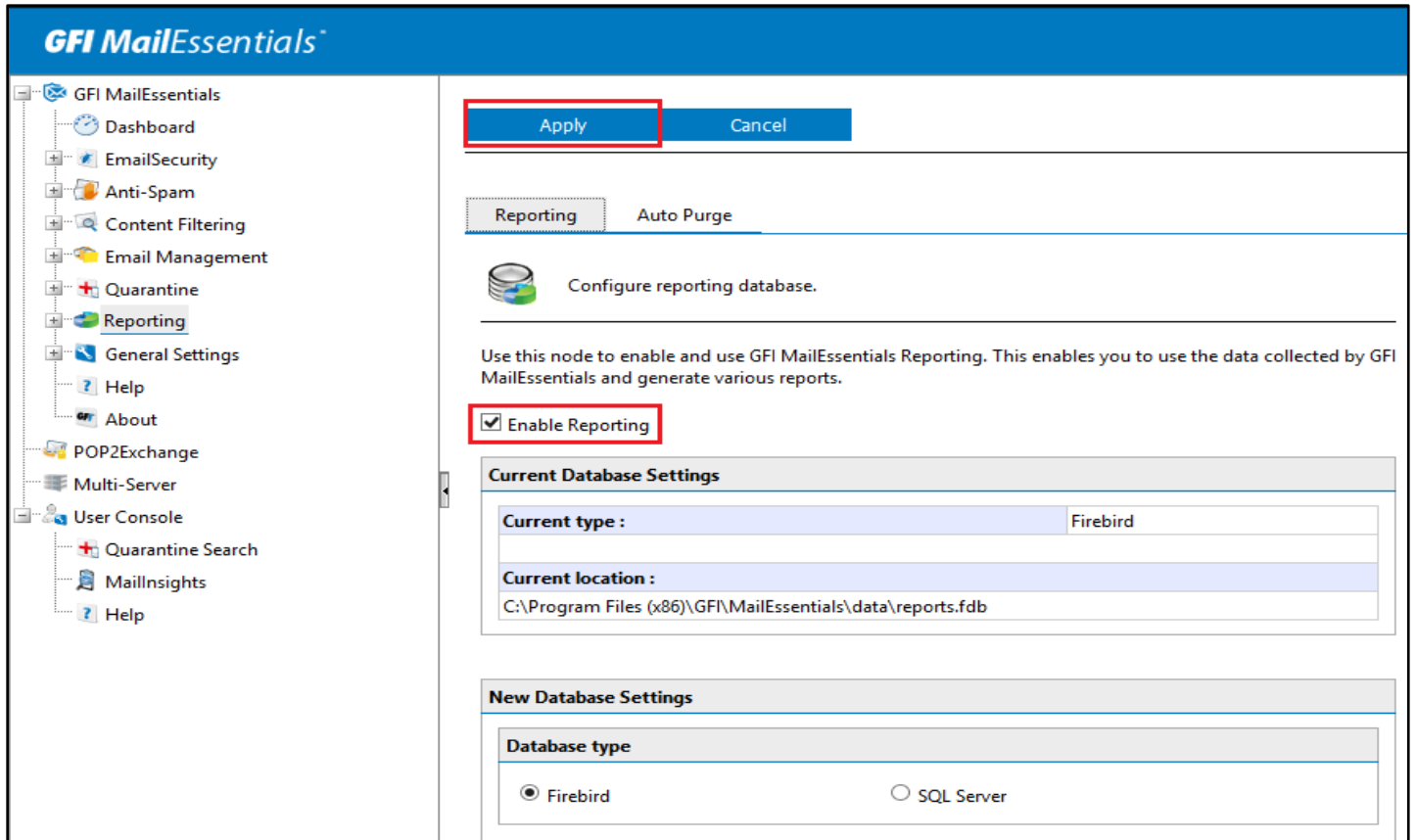


Figure 2

3. To generate custom report,
 - a. Go to **Reporting > Reports > Custom Reports** tab.
 - b. Click **New** to create a new custom report.

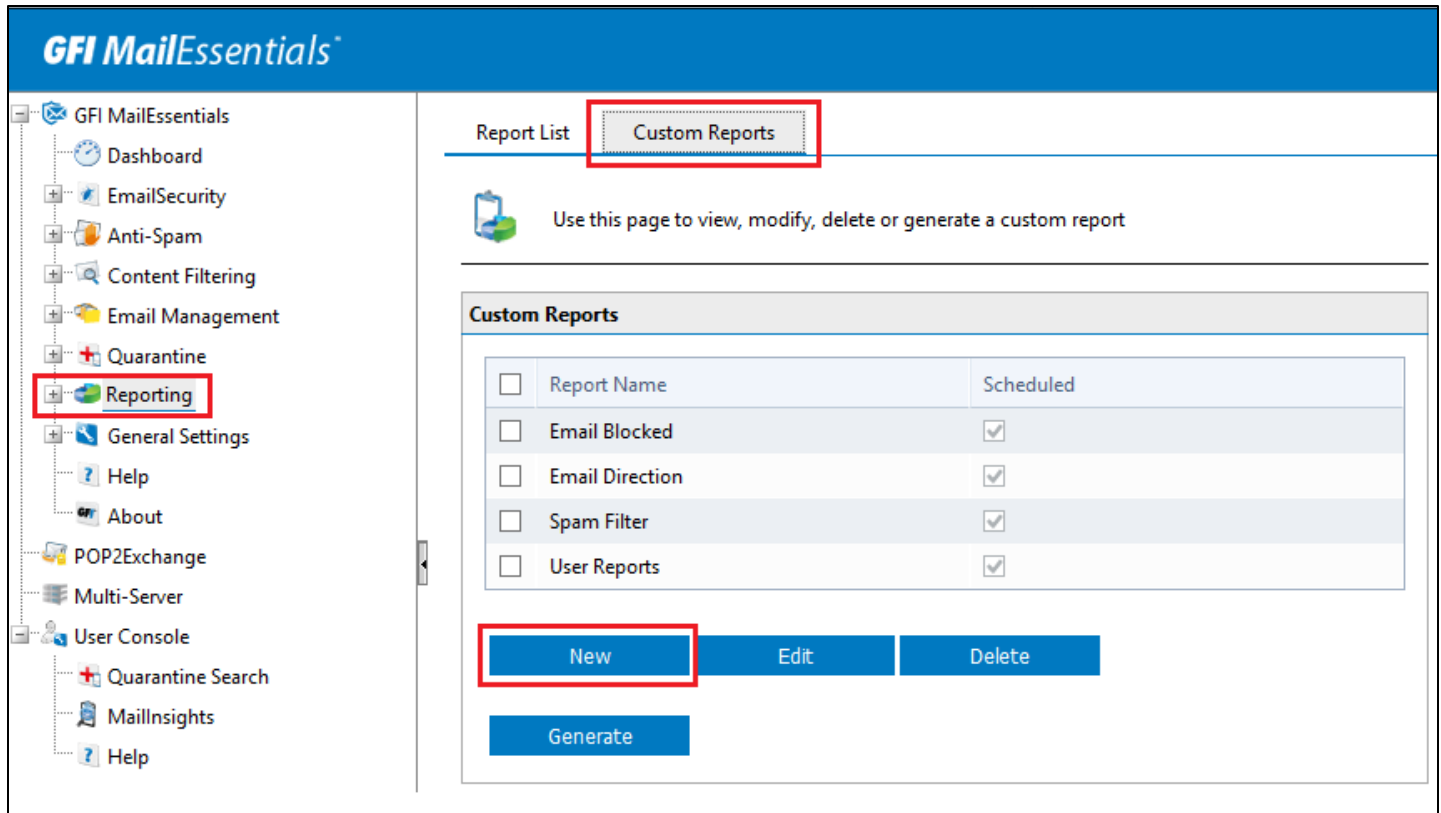


Figure 3

c. In the **Custom report** page,

- **Report Name:** Please mention the report name of the custom report.
- **Reports lists:** Select the type of report that you want to generate.
 - i. **Email Direction** - shows total emails processed for each email direction - Inbound, Outbound and Internal.
 - ii. **Emails Blocked** - shows total emails blocked by anti-spam and anti-malware filters for each email direction (Inbound, Outbound and Internal) out of all emails processed.
 - iii. **Spam Filter** - shows the total number of emails blocked by each anti-spam filter.
 - iv. **User Report** - shows the number of blocked and allowed emails for each email address.

NOTE: For **Emails blocked** and **Spam Filter** report, you must configure anti-spam and anti-malware rule on GFI MailEssentials.

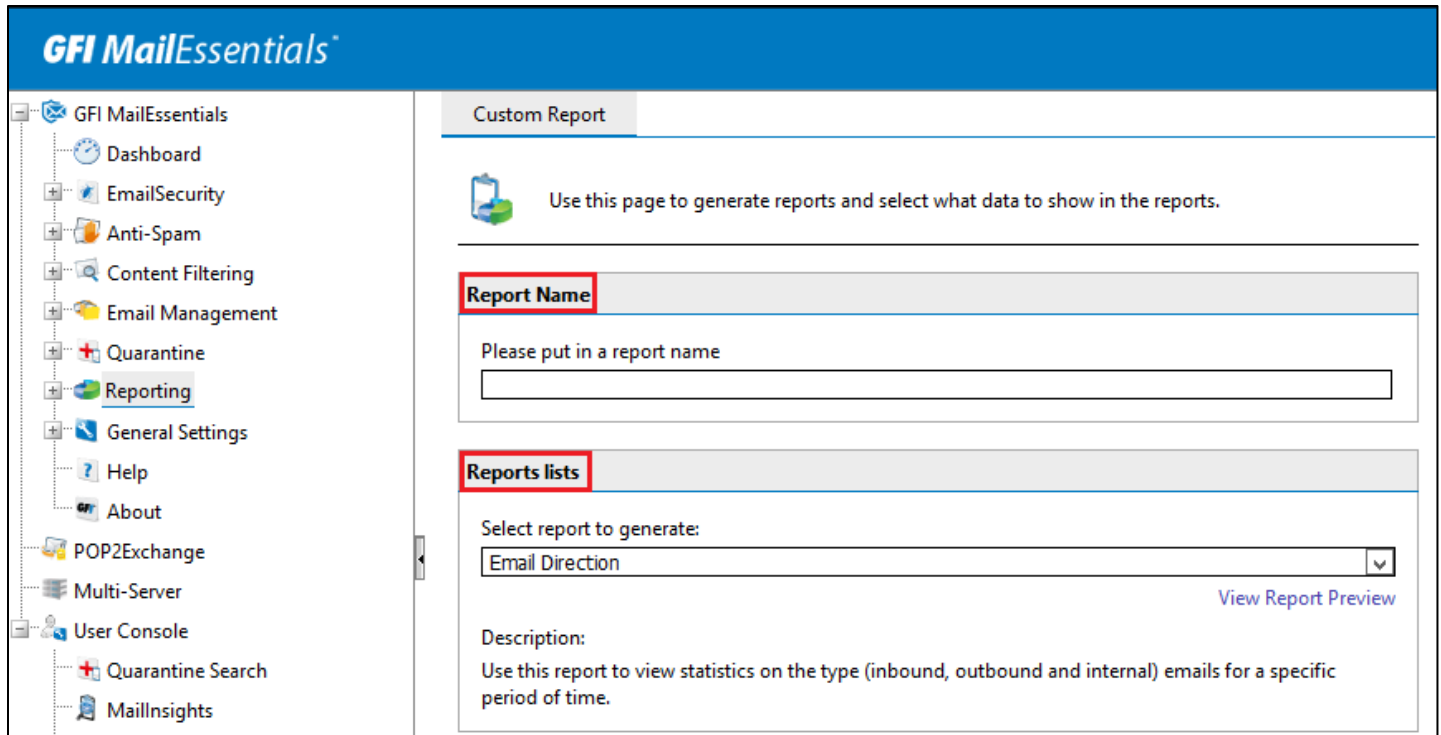


Figure 4

- **Reporting Filtering:**
 - i. For **Date Filtering**, select report date range and when selecting **Custom date range**, specify the period to display data for, from the **Custom from date** and **Custom to date** calendar controls.
 - ii. For **Email direction filtering**, select an email direction to display data for or select all email directions (inbound, outbound, internal) to display data for all directions.
 - iii. For **Email address filtering**, Key in an email address to display report information for that email address only.
- **Reporting grouping:** Specify how to group the data in custom report.

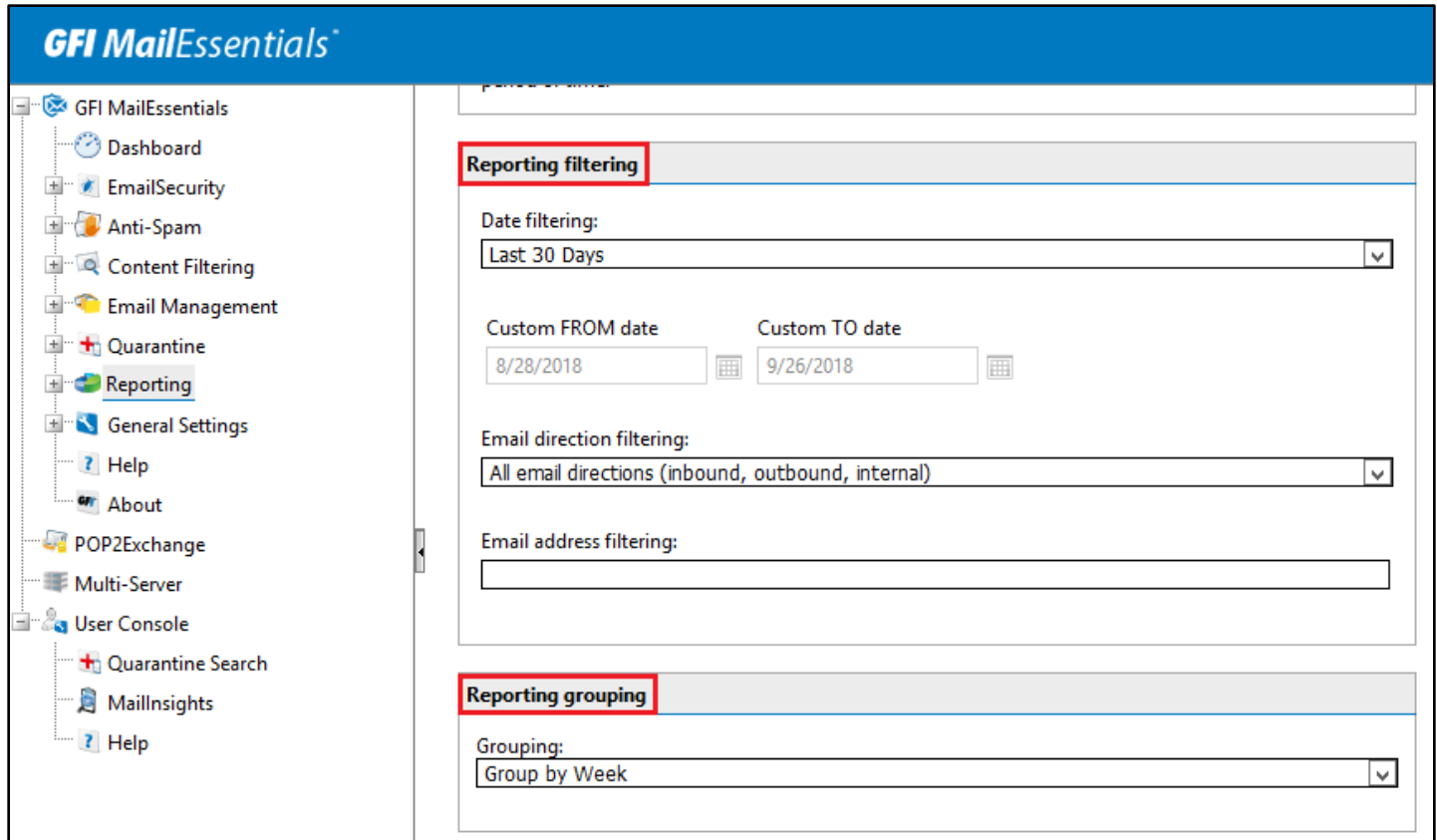


Figure 5

- **Report Scheduling:** Enable **Send every** checkbox to scheduling reports and configure a date/time combination to have the report generated at a specific date and time. Click **Add Rule** to save report generation time. Once you add the rule, it displays in the box.
- **Custom Report Output:** To save report locally, select **Save to Disk** and **specify a location** where report file will be saved. Select the **pdf** format of the report in the **File Type** box.
- Click **Save** to save the custom report.

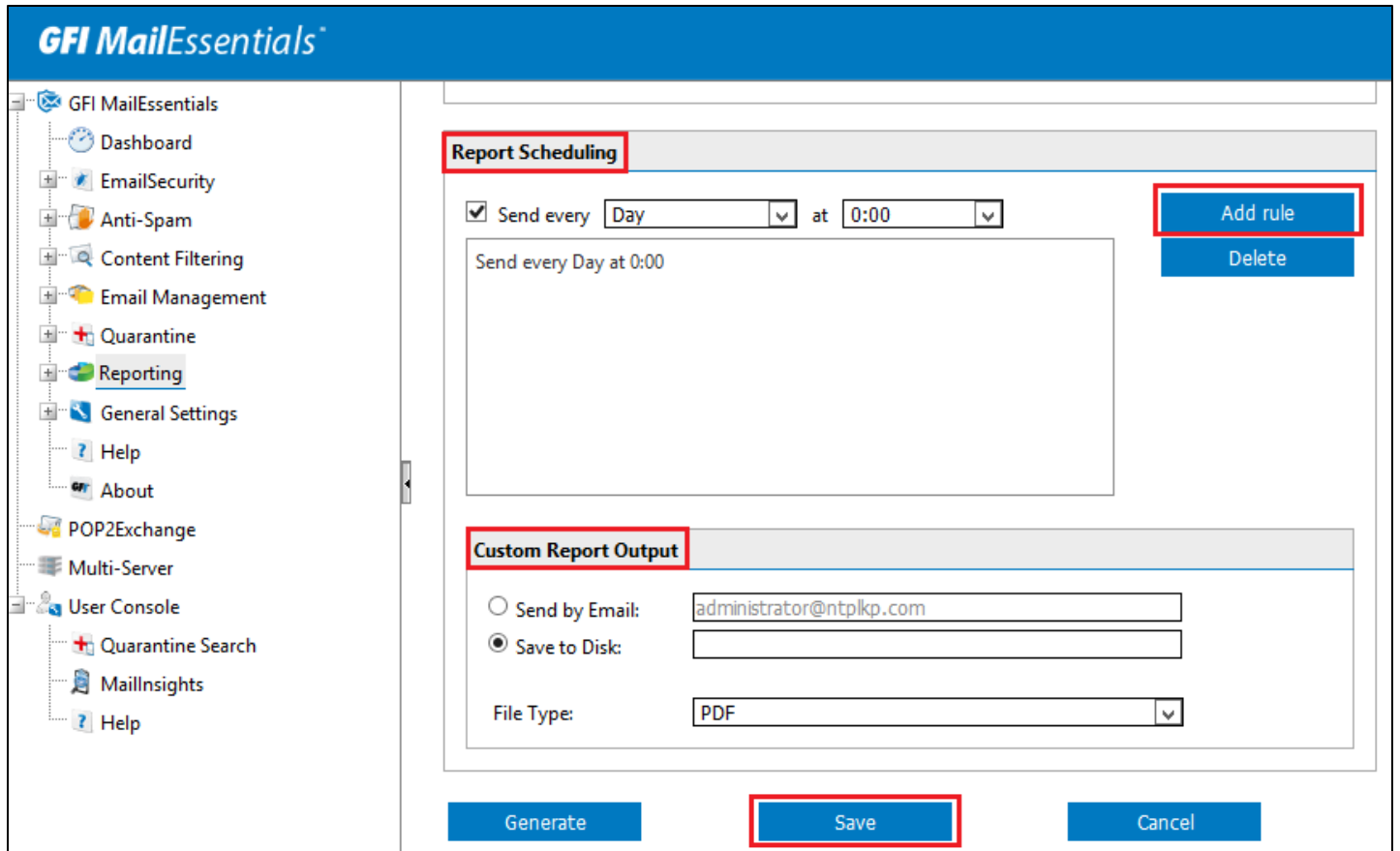


Figure 6

Configure DLA in EventTracker:

1. Logon to EventTracker Manager Console.
2. Under the **Admin** drop-down, select **Manager**.

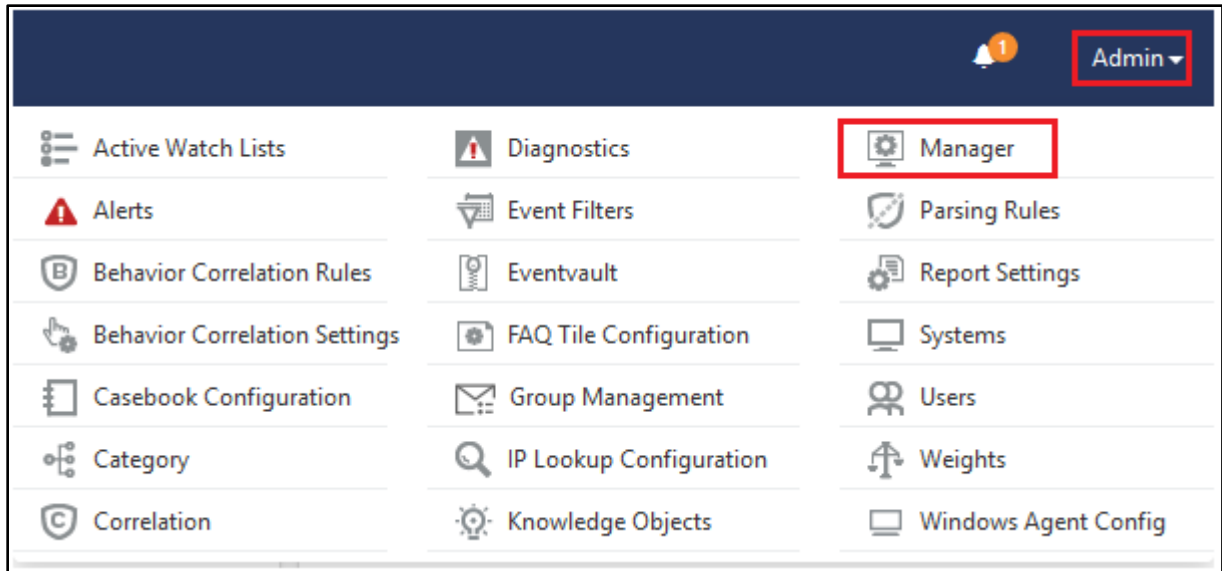


Figure 7

3. Select the **Direct Log Archiver** tab and click the **Add** button to configure DLA.

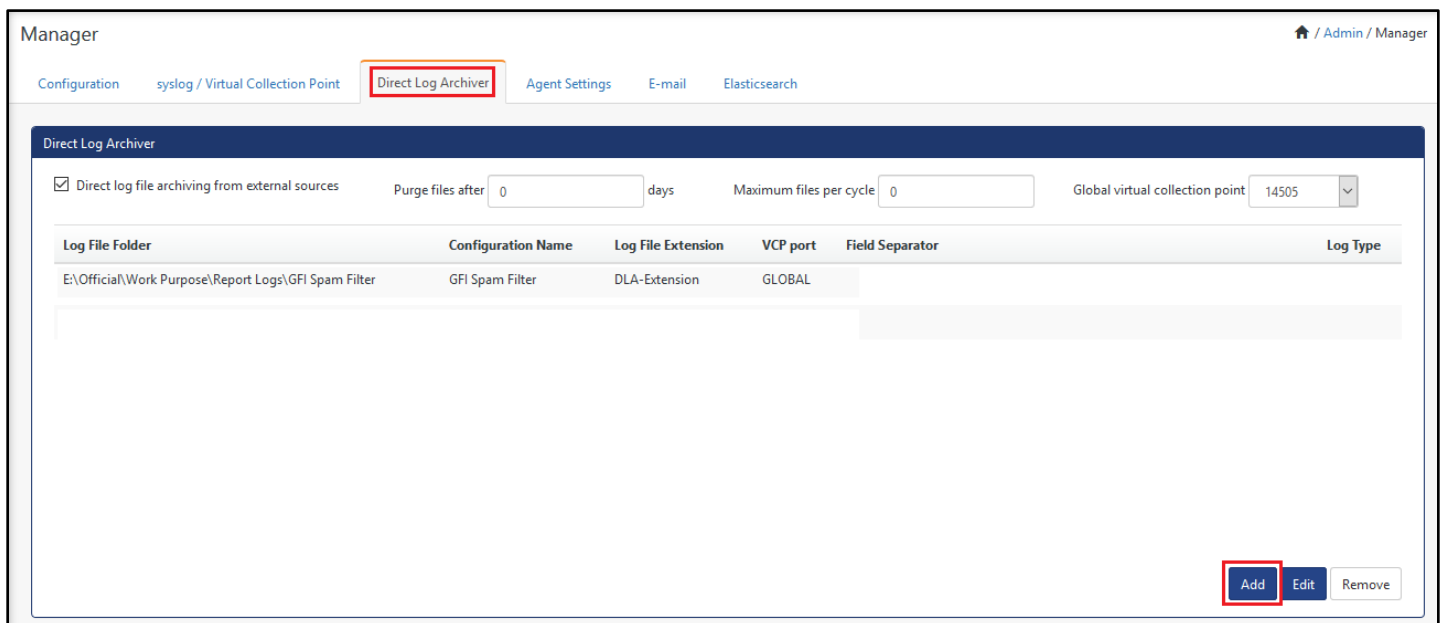
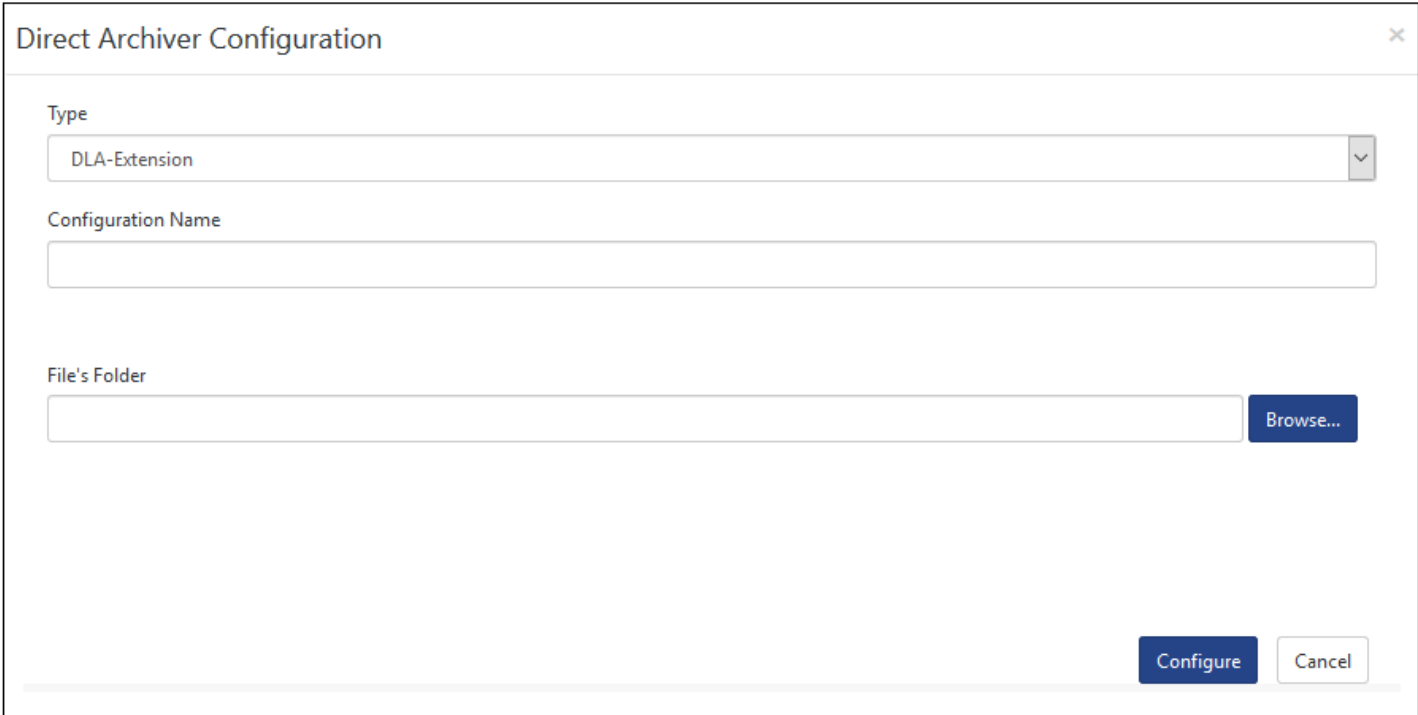


Figure 8

4. In Direct Archiver Configuration,

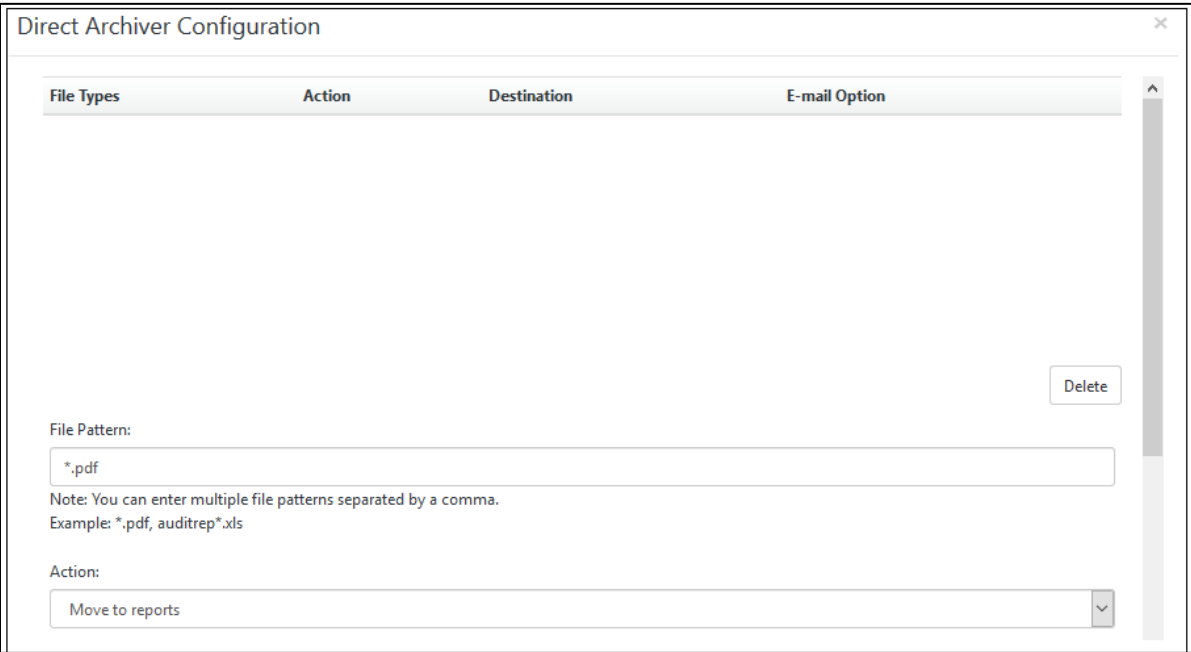
- **Type:** Select the DLA-Extension as type.
- **Configuration Name:** Provide the name of DLA configuration.
- **File's Folder:** Specify the folder path using **Browse** option to monitor the report files.
- Select **Configure** to save the changes.



The image shows a 'Direct Archiver Configuration' dialog box. It has a title bar with a close button (X). The main area contains three input fields: 'Type' with a dropdown menu showing 'DLA-Extension', 'Configuration Name' with an empty text box, and 'File's Folder' with an empty text box and a 'Browse...' button to its right. At the bottom right, there are two buttons: 'Configure' and 'Cancel'.

Figure 9

- **File Pattern:** Type *.pdf for pdf report file.
- **Action:** Under the drop-down, select “Move to reports” option to show the reports in EventTracker’s Report Dashboard.



The image shows the 'Direct Archiver Configuration' dialog box with a table and additional fields. The table has four columns: 'File Types', 'Action', 'Destination', and 'E-mail Option'. Below the table is a 'Delete' button. There are also fields for 'File Pattern' (containing *.pdf), a note about multiple file patterns, and an 'Action' dropdown menu (containing Move to reports).

File Types	Action	Destination	E-mail Option
------------	--------	-------------	---------------

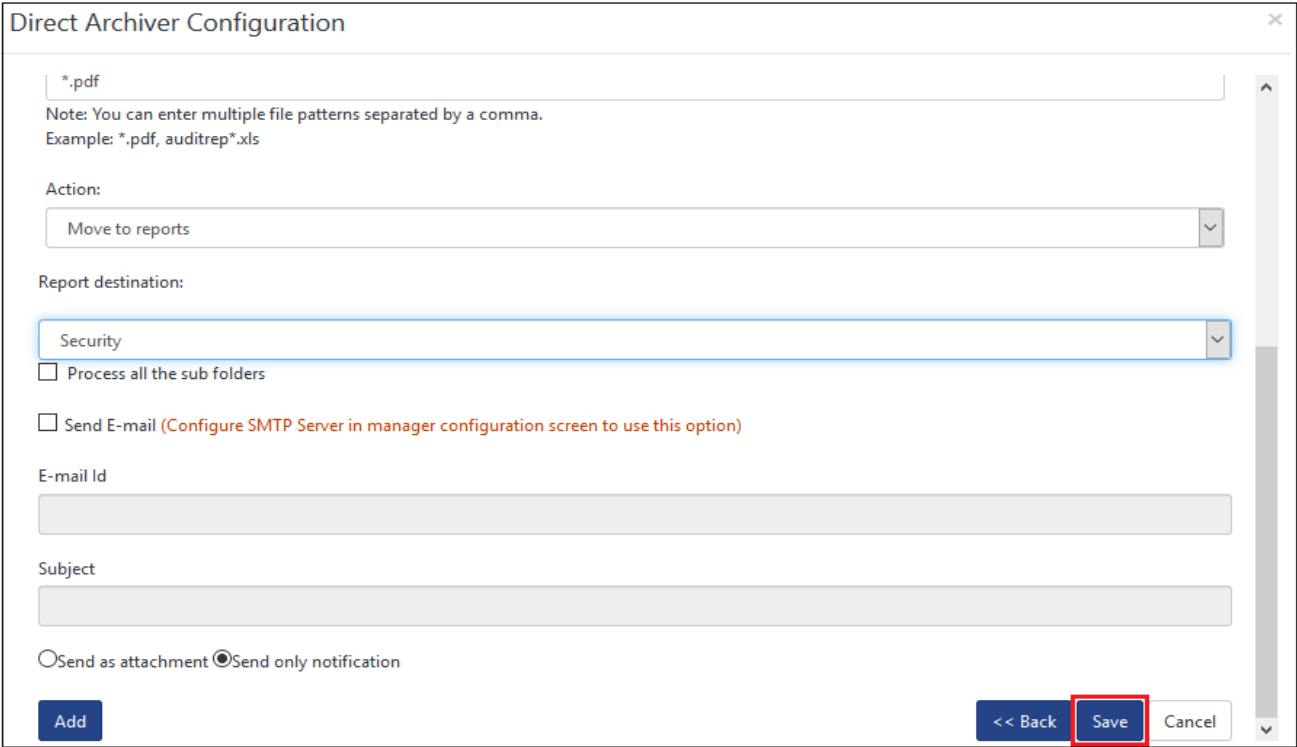
File Pattern: *.pdf

Note: You can enter multiple file patterns separated by a comma.
Example: *.pdf, auditrep*.xls

Action: Move to reports

Figure 10

- **Report Destination:** Under the drop-down, select **Security** option.

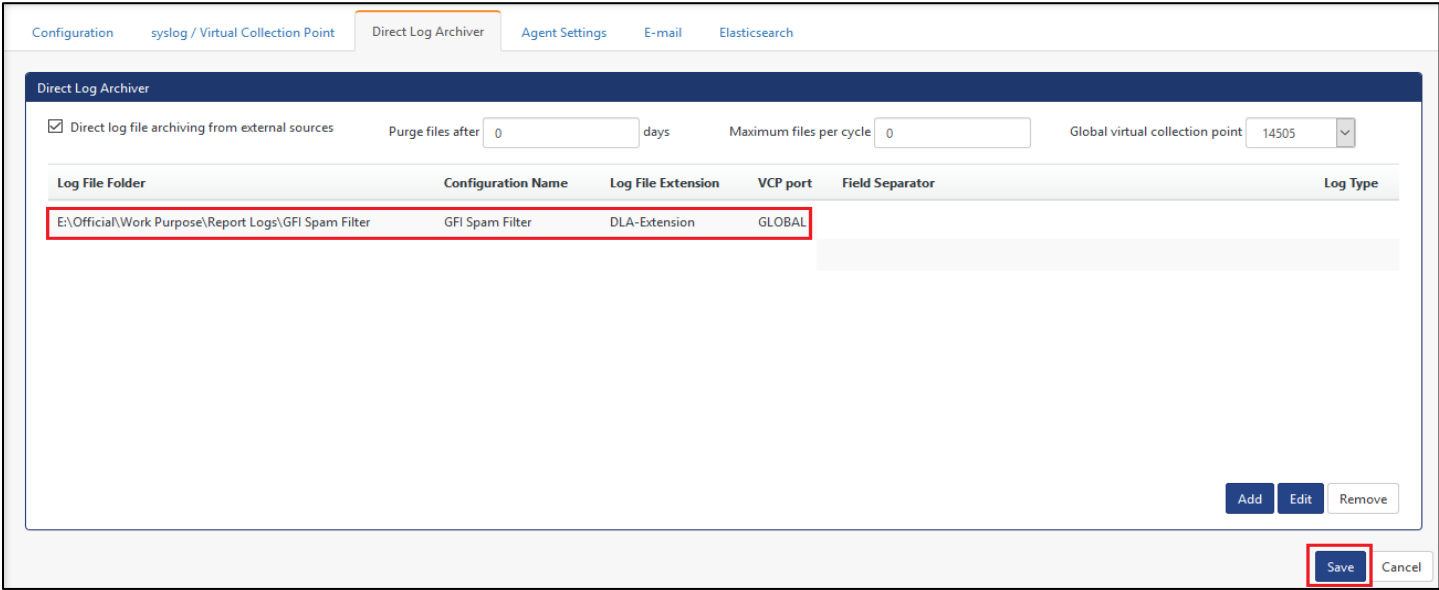


The image shows a 'Direct Archiver Configuration' dialog box. It contains several fields and options: a file pattern field with '*.*pdf', a note about multiple file patterns, an 'Action' dropdown set to 'Move to reports', a 'Report destination' dropdown set to 'Security', and checkboxes for 'Process all the sub folders' and 'Send E-mail'. There are also fields for 'E-mail Id' and 'Subject', and radio buttons for 'Send as attachment' and 'Send only notification'. At the bottom, there are 'Add', '<< Back', 'Save', and 'Cancel' buttons. The 'Save' button is highlighted with a red box.

Figure 11

- Click **Save** to configure the DLA.

Next EventTracker displays the below page. Click **Save** to save the changes.



The image shows the 'Direct Log Archiver' configuration page in EventTracker. It includes a navigation bar with 'Configuration', 'syslog / Virtual Collection Point', 'Direct Log Archiver', 'Agent Settings', 'E-mail', and 'Elasticsearch'. The main content area has a table with columns: 'Log File Folder', 'Configuration Name', 'Log File Extension', 'VCP port', 'Field Separator', and 'Log Type'. A table row is highlighted with a red box, showing 'E:\Official\Work Purpose\Report Logs\GFI Spam Filter', 'GFI Spam Filter', 'DLA-Extension', and 'GLOBAL'. At the bottom right, there are 'Add', 'Edit', 'Remove', 'Save', and 'Cancel' buttons. The 'Save' button is highlighted with a red box.

Log File Folder	Configuration Name	Log File Extension	VCP port	Field Separator	Log Type
E:\Official\Work Purpose\Report Logs\GFI Spam Filter	GFI Spam Filter	DLA-Extension	GLOBAL		

Figure 12