Forcepoint Data Security Posture Management

Powered by Getvisibility

Emails Configuration

Forcepoint

Report

Forcepoint
April 23, 2024

Table of Contents

Introduction

This user guide details the steps required for configuring email notifications as part of the Forcepoint DSPM feature. Email notifications are a crucial component of data control management, enabling specified users to receive alerts when data control rules are triggered.

Prerequisites

- Administrative access to the Forcepoint DSPM tenant.
- Email API credentials were obtained from support.forcepoint.com

Steps :

1. Obtain API Credentials

   Before configuring email notifications, you must acquire the necessary API credentials from Forcepoint. Use support.forcepoint.com to request these credentials. Your request should include:

   - Your account details.
   - The purpose of the API credential request (i.e., setting up Forcepoint DSPM email notifications).

   Note: Only the individual responsible for deploying the software should perform this step to ensure security compliance.

2. Configuring email notifications in Forcepoint DSPM portal

   a) Access the **Administration** Panel

      Log in to your Forcepoint DSPM account and navigate to the **Administration** section from the top bar menu. This allows you to manage various administrative settings, including email configurations.
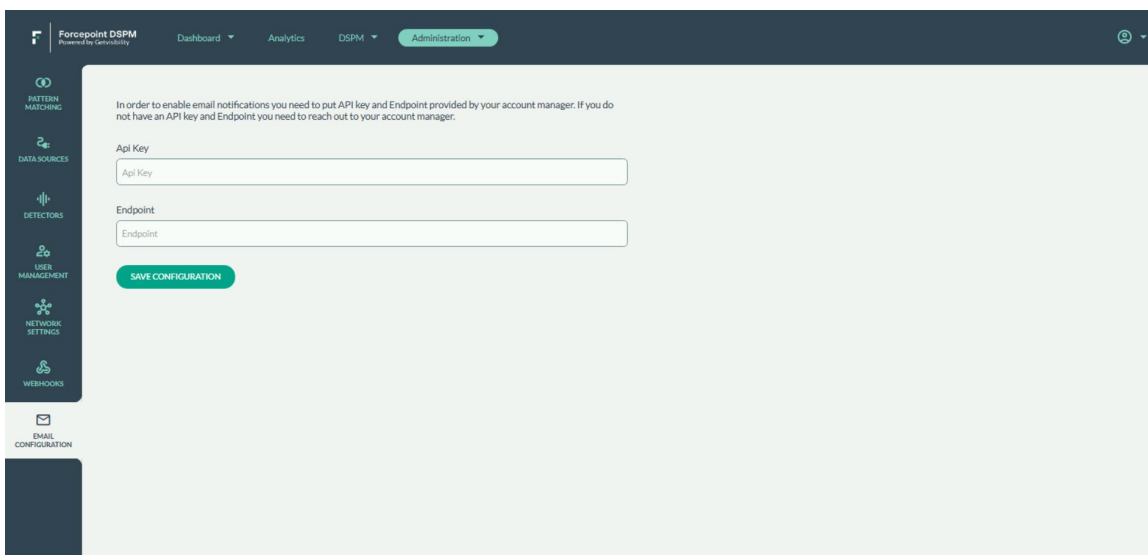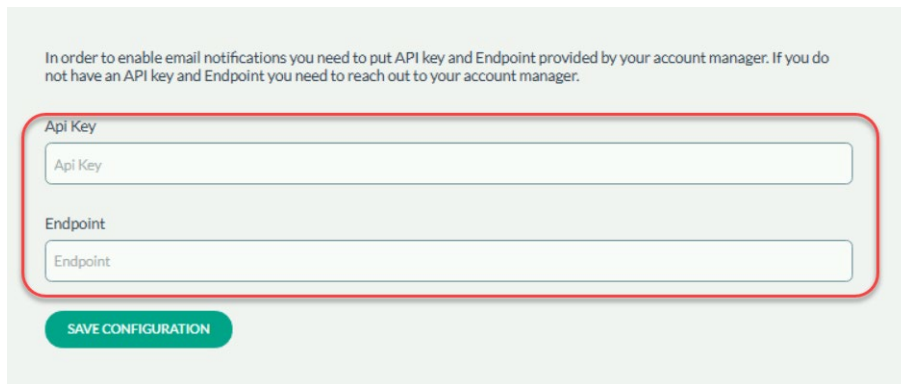

Figure 1.

   b) Enter API Credentials:

In the **Email Configuration** section, you will see fields for **API Key** and **Endpoint**. Enter the Api key and endpoint provided by us in the respective fields.

In order to enable email notifications you need to put API key and Endpoint provided by your account manager. If you do not have an API key and Endpoint you need to reach out to your account manager.

Api Key

Api Key

Endpoint

Endpoint

SAVE CONFIGURATION

Figure 2.

c)   Send Test Email

After entering the API credentials, click the **Send Test Email** button. This action will trigger a test email to verify that the email automation setup is functioning correctly. Ensure that you check the inbox of the configured recipient to confirm receipt of the test email.
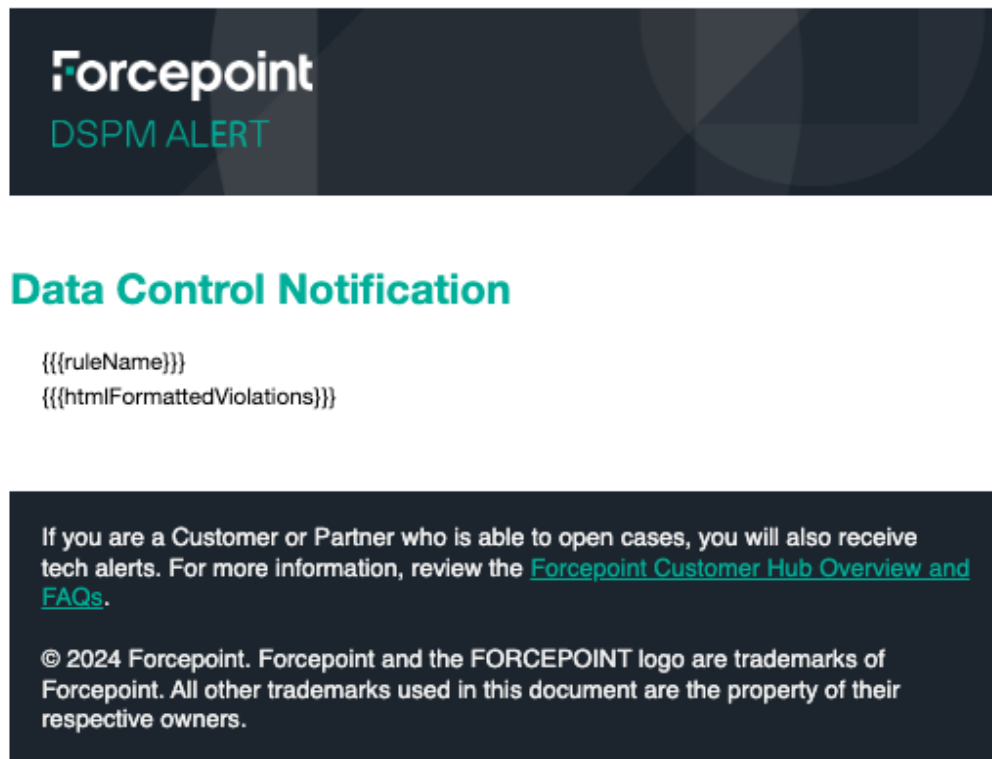
Forcepoint
DSPM ALERT

Data Control Notification

{{{ruleName}}}
{{{htmlFormattedViolations}}}

If you are a Customer or Partner who is able to open cases, you will also receive tech alerts. For more information, review the Forcepoint Customer Hub Overview and FAQs.

© 2024 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.

Figure 3.

d)   Save Configuration.

Once the test email has been successfully sent and received, click the **Save Configuration** button to apply the settings. This action will enable email notifications for all data control rules that have an email action set up.

3. Configure Data Control Rules:

   a) Access Data Controls

   Navigate to the **Data Controls** page from the top bar. Here, you can create and manage data control rules that monitor and protect your sensitive data.
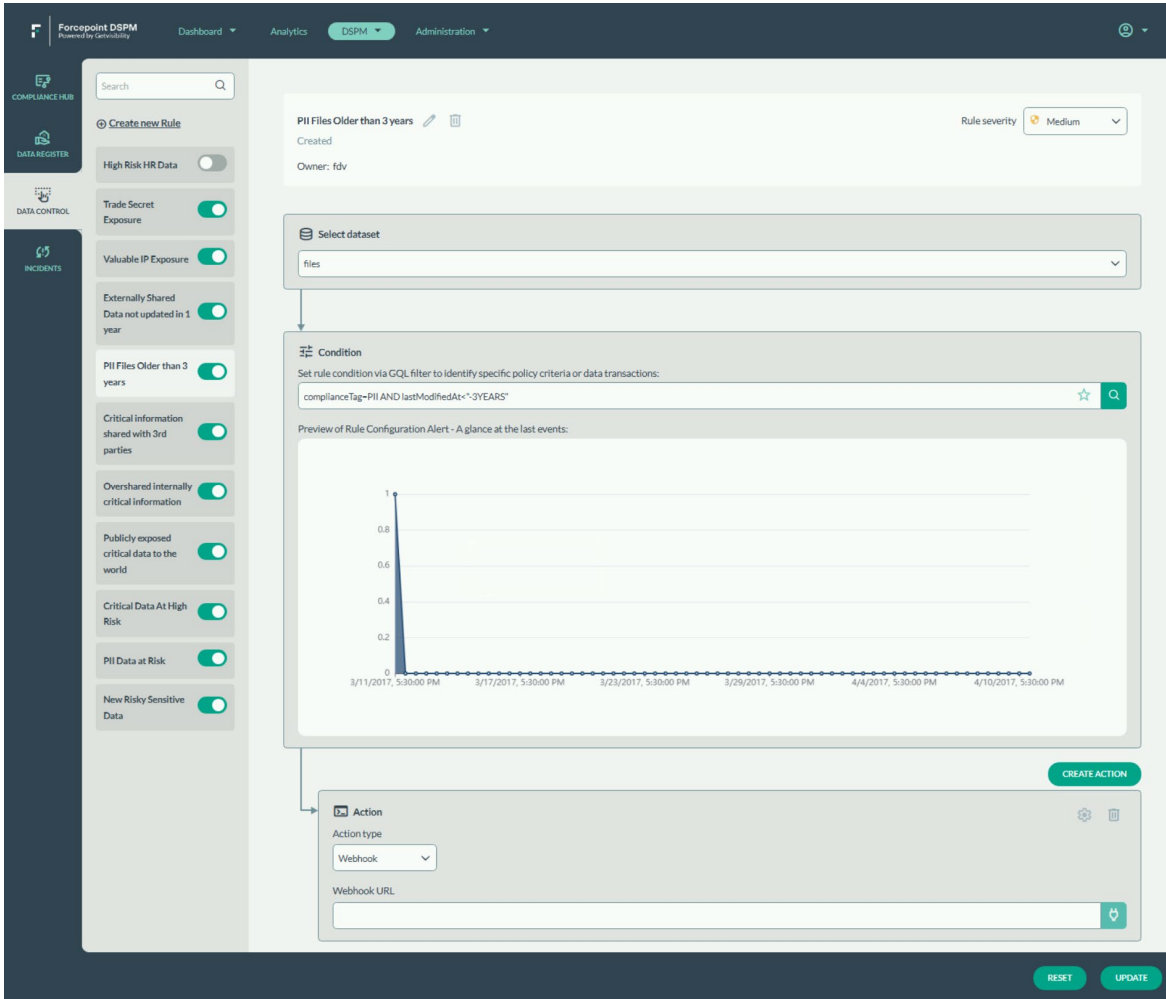

Figure 4.

   b) Set Up Email Notification Action

   When creating or editing a data control rule, select **Email** as the action type. Specify the users who should receive notifications by entering their email addresses in the provided field.
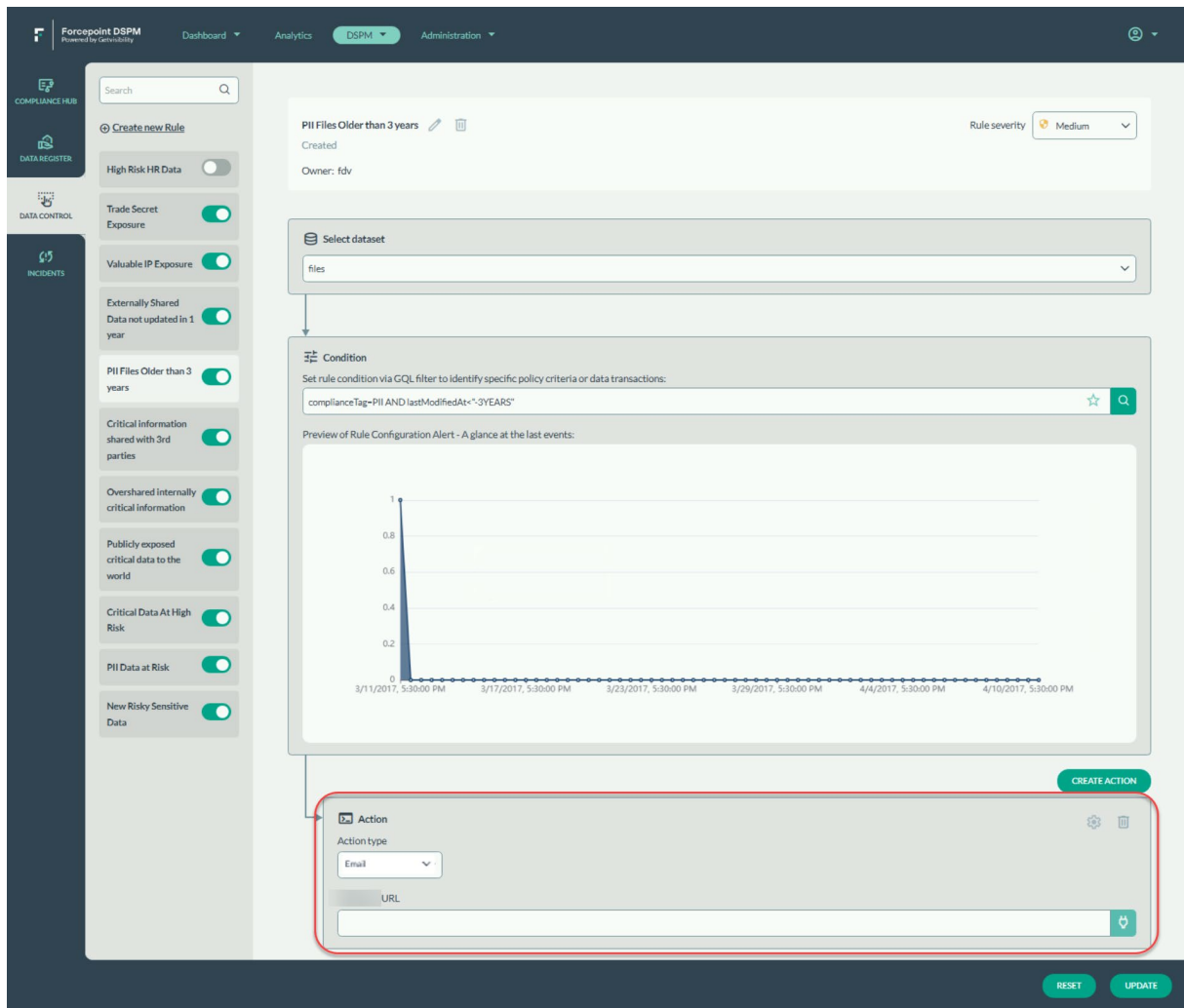
Figure 5.

4.   Confirming Active Notifications

Once the above configurations are complete, the specified users will start receiving email notifications whenever a relevant data control rule is triggered. It is recommended to review the data control rules and notification lists periodically to ensure that the correct individuals are alerted to potential data security events.

Troubleshooting and Support

If at any point you encounter issues with configuring or testing email notifications, please reach out to our support team at support.forcepoint.com for assistance.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.