File Access Manager

Alerts

Version: 8.3 Revised: March 29, 2022

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices.

Copyright © 2022 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

“SailPoint,” “SailPoint & Design,” “SailPoint Technologies & Design,” “Identity Cube,” “Identity IQ,” “IdentityAI,” “IdentityNow,” “SailPoint Predictive Identity” and “SecurityIQ” are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. https://www.sailpoint.com/patents

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce’s Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

Alerts Introduction

Alert Rules define activity-based criteria for generating system alerts, including notifications and customized responses, such as email, SysLog, or UserExit.

Compliance > Alert Rules – Defining alert rules

Examples of alert rules:

- A file under \\FileStorageApplication\HR is deleted by a user who is not a member of the HR department.
- A specific user reads more than 1000 files in one minute (considered a suspicious activity, regardless of whether the user or malware initiated the activity).

Viewing Existing Alerts

To view existing alert rules:

1. Navigate to **Compliance > Alert Rules**.
   All alerts, including alerts in the Resources section, display in this screen.
2. Click **Include Resource-based Rules** to view alerts from Resources.
3. You can filter the screen by:
   - Rule Name
   - Status - Activate or deactivate an alert rule from the main screen – there is no need to access the rule.

Managing Alert Rules

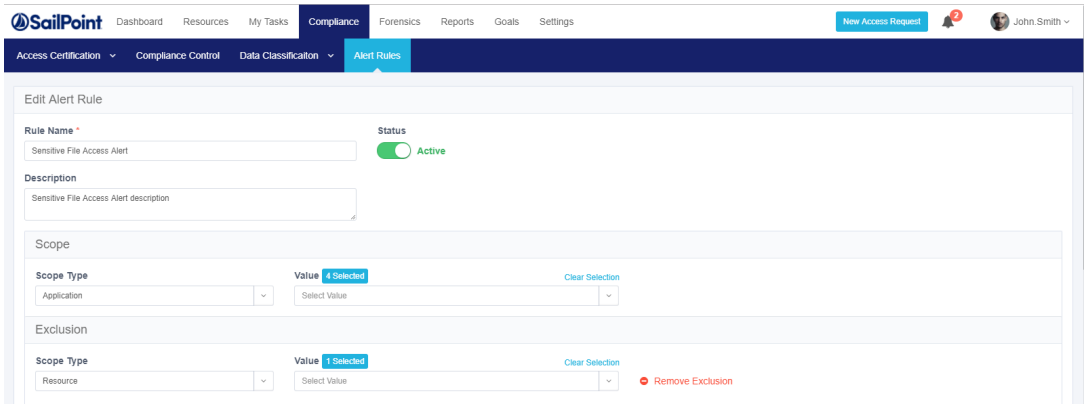
To access the alert rules, Navigate to **Compliance > Alert Rules**.

To open an alert rule for edit, double click the alert rule to edit.

To edit an alert rule:

1. Make changes to the relevant parameters of the General, Scope, Filters, Triggers, and Response sections of the Rule Criteria section, as appropriate.

> An Administrator can define and customize response options in the administrative client.



To duplicate an alert rule:

1. Click **Duplicate** from *Actions* in the alert rule to be edited.
2. The Duplicate Alert Rule screen displays, with all the definitions of the duplicated rule already filled in.
3. Make any required modifications.

> Duplicate a discard rule to create a new rule with definitions that resemble those of an existing discard rule.

To delete an alert rule:

1. Click **Delete** from *Actions* in the alert rule to be deleted.
2. A delete confirmation question displays.

Scope

Use Scope to select a relevant running target.

- Scope inclusion enables users to specify application type, application, or specific business resource to run an alert rule.
- Scope exclusion allows users to avoid running a rule on an irrelevant application type, application, or specific business resource.
- If the same resource is selected for both inclusion and exclusion, the resource will be excluded since exclusions always overrule inclusions.
- Resource scope selection allows users to select or unselect a subfolder to run a rule by checking the “Including subfolders” checkbox:

  For example, if the business resource “Sensitive folder” has a sub-folder, called “Non sensitive folder” if the user deselects the “Including subfolders” checkbox, the rule will only run on the main resource, which is “Sensitive folder”.

Filters

> If an application has a Data Enrichment Collector (DEC), the attributes of that DEC also display. However, you select more than one application from same application type, and the applications share the same DEC, only the DEC attributes common to all of the applications' DECs display. If there are no DECs in common, only attributes relevant to the application type of the selected applications display.

Filter criteria allows users to specify suspicious behavior, based on the selected filter criteria parameters.

The available filter criteria attributes depend on the scope selected.

If you did not select a scope, or if you select an application type, or if you select applications from a different application type, only the following default attributes are available:

- Action Type
- Category
- Domain
- Event Date
- Event Time
- Path
- User Name

However, if you select a specific application type or a single application, or if you select multiple applications from a single application type, only the attributes relevant to the selected application type display.

Users can use queries saved in **Forensics > Activities** queries by clicking on **Load Query**, to display a list of all saved queries.

When the query is loaded, all the information in the Rule Criteria section (Scope and Filters) is overridden by the loaded query filters. If a query cannot be loaded, an error message displays.

The following queries are not available:

- Queries on alerts (since only existing queries on activities can be loaded)
- Mismatched queries
- Queries involving users from more than one domain

Response

The Response section allows users to define a response for an alert.

For example, when a new permission is added to a sensitive resource, all the Data Owners of that resource can receive an email, notifying them that a new permission was added.

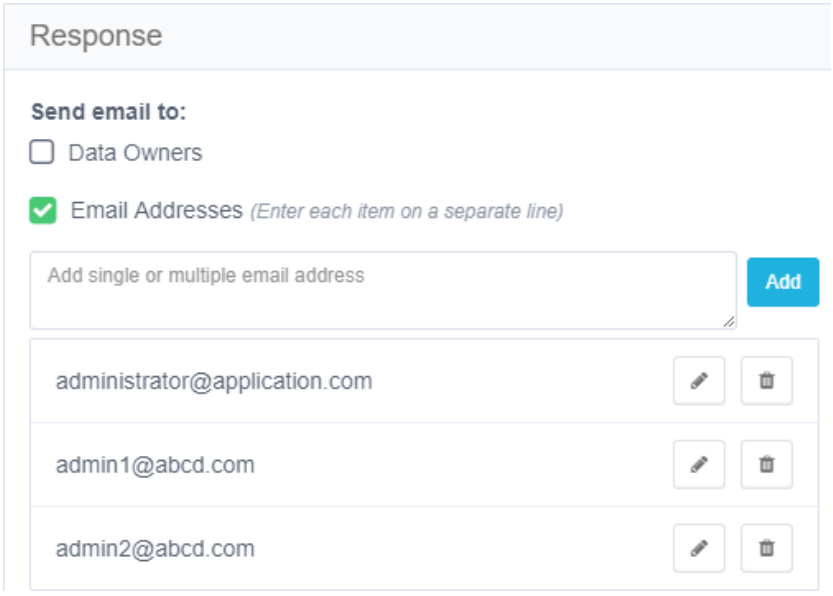
A Response may be one of the following:

- Email to specific email addresses, and/or to the Data Owners who own the resource.

  > Currently, the Data Owners option is available for Single Activity Alerts, but not for Threshold Alerts.

- Syslog
- User Exit

1. A Response object is created / edited in the File Access Manager Administrative Client.



2. Click **Advanced Settings** to select additional option responses.

> Use the File Access Manager Administrative Client to define and customize response options.

> File Access Manager Alert Response is an automatic default, since it retains the alert in the database. A user cannot opt out of the File Access Manager Alert Response.

Resource-based Alert Rules

Data Owners can activate Resource-Based Alert Rules (out-of-the-box alert rules) in the **Resource > Alerts** screen.

Administrators can navigate to **Compliance > Alert Rules** to perform the following operations on Resource-Based rules that were created by Data Owners:

- View the rule
- Change the rule's name/description
- Change the rule's status (active/inactive)
- Delete the rule

Threshold Alert Rules

Architecture and Flow

The Activity Analytics service is responsible for the threshold calculation and issuing threshold-based alerts.

Activities are evaluated against threshold alert rules by the Event Manager during the processing of the activities, and if they match, they are marked as candidates for a threshold calculation.

The Activity Analytics queries the Elasticsearch every defined interval to bring activities candidate for threshold alerts. It then aggregates the activities and when the threshold is met, issues an alert and a response according to the definition in the threshold alert rule.

Limitations

Activities received more than 15 minutes after the Activity time (as the result of a temporary disconnection between the Activity Monitoring and the Event Manager) will be kept in the Database with the original Activity time, but will not be included in the Threshold Alert Rules calculation. However, if an Alert has already been created, the Activities that originated in the Alert timeframe, but were received after the 15-minute time window, will be updated in the relevant existing Alert record. (As a result, the total number of Activities in the existing Alert record will increase.)

The 15-minute time window helps limit the memory required for the Threshold Alert Rules calculation.

Please review the Compass forum for best practices. If required, the PS team can change the time window in the Database.

If Windows activities have more than one shared path, the system will send duplicate activities for a threshold alert calculation. For example, if Folder1 can be accessed by \\MyServer\Folder1 and by \\MyServer\C$\Main\Folder1, each activity performed in Folder1 will appear twice in the Database, each time, with a different shared path.

To prevent duplicate activities from being calculated in the total number of activities required to create a threshold alert, select “Windows” as the application type in the scope, and set the following filter in the **Alert Rule > Rule Criteria Filter** section:
Attribute = Original Access Path (OAP)
Operator = Empty

All duplicated Activities have the OAP field as part of the original path. Adding this filter causes the Threshold Alert Rule to ignore all duplicated Activities and to calculate only the original Activity.

Create/Edit a Threshold Alert Rule

See for information on creating a Threshold Alert rule.

Only administrators (not data owners) can view threshold alerts in Activity Forensics or in Reports.

Troubleshooting Activities

The best way to troubleshoot activities is to follow their activity trail.

Use a specific Collector Installation and Configuration Guide to troubleshoot a specific monitoring issue for that Activity Monitor.

The lists below are suggestions of what to look for in the various services.

Application

- All prerequisites were completed successfully.
- Activities are generated when relevant. For example, check that relevant activities are generated in the Event Log in Active Directory or that they are included in the Exchange Audit log.

Activity Monitor Log

- The log has errors.
- Events were received (by viewing the Monitor Statistics file).
- Events were monitored, but not sent (by checking the monitoring mode – full, semi, and discard) .

Event Manager

- New events were entered (by viewing Event Collector statistics) and then moved to the memory queue.
- Events were saved in the Event Manager (one Connector at a time, or through a dedicated Event Manager).
- The Event Manager log has errors.

Events Backup

File Access Manager includes a backup mechanism for events streaming into the Event Manager. Incoming events are serialized to disk as compressed bulk events.

- This backup mechanism allows for re-streaming the backed-up event bulks into the event manager in case of a failure in the events processing flow.
- A separate file is created daily, containing the bulk events received that day.

The behavior of the Events Backup mechanism is defined by several parameters under the <appSettings> tag in the Event Manager's app.config files:

```
<add key="BackupEvents" value="true"/>

<add key="WaitForBackupSeconds" value="5"/>

<add key="BackupEventsDir" value="EventsBackup"/>

<add key="RestoreBackedupEvents" value="false"/>

<add key="BackupRetentionDays" value="7"/>

<add key="CleanOldBackups" value="true"/>
```

Parameter	Type	Description	Default
BackupEvents	True/ False	Enables / Disabled the Events Backup mechanism	True
WaitForBackupSeconds	Number	Number of seconds the Event Managers service waits for the backup process to finish serializing in-memory events, on service shutdown, before it terminates the process	5 (seconds)
BackupEventsDir	Text	Directory path for the event backup files	EventsBackup in the service home dir
RestoreBackedupEvents	True/False	Activates backed up events restore on service startup	False
BackupRetentionDays	Number	Number of days to retain events backup files, before backup files are deleted.	7 (days)
CleanOldBackups	True/False	Enables/Disables automatic cleanup of expired backup files (older than *BackupRetentionDays*)	True

To Enable Events Backup

- Set the *BackupEvents* to **True** (default). This will cause the Backup mechanism to start.
- The *BackupEventsDir* by default will be set to EventsBackup in the service's home directory. This folder will be created by the service if it is not already there. If you wish events to be backed up to another location, change the *BackupEventsDir* parameter accordingly before the service is started, or restart it after the change. Make sure the drive containing the backup folder has enough space. (Space requirements depend on events traffic).
- Make sure the *RestoreBackedupEvents* parameter is set to false – if you don't wish to restore existing backups.
- Ensure all other parameters suit your needs, or configure accordingly.

To Restore events from previous backup

- Set the *RestoreBackedupEvents* to True before you start the service, or restart it after the change.
- Once the service is running with *RestoreBackedupEvents* set to True, it will attempt to restore all backup files, and will stream all backed up events, back to the Event Manager, to be processed and stored in File Access Manager.
- If you do not wish to restore all the backup files, but only specific files (days), you should copy the unnecessary files to another location.
- In case restoring the events fails, a new file contained the un-restored events will be created, with the *.recreated* suffix, indicating this file contains events that failed to be restored, and will not be re-attempted.

To Retain backups for specific dates or longer periods:

- Either disable the automatic cleanup of backup files, by setting the *CleanOldBackups* parameter to **True**, or modify the *BackupRetentionDays* parameter to suit the retention policy you wish to configure.
- When modifying app.config parameters, changes will take place only the next time the service is started, as app.config parameters are read on service startup.