Safeguard your Microsoft 365 Environment

using

AdminDroid Alerts

AdminDroid - Microsoft 365 Alerting Solution

It might be quite challenging for an administrator to keep track of day-to-day activities in a Microsoft 365 environment. Here, 'AdminDroid Alerts' comes up with a solution! By utilizing AdminDroid alerts, you can easily monitor and keep track of over 1500 user activities. This will help you stay informed and quickly identify any changes that require prompt action.

Here are some simple steps to deploy AdminDroid alerts in your Microsoft 365 environment.

Create

Create policies for events you want to keep track of.

AdminDroid allows you to create a new alert policy for any activity, regardless of its complexity.

Optimize

Too many alerts will spoil its real purpose.

You can optimize your alert policies by using our broad spectrum of special features.

Engage

Never miss an important alert.

As not all the alerts need the same level of attention, you may customize the alert policies in a way to prioritize the events that matter the most.

Action

Investigate and resolve the alerts.

As a final goal, investigate the triggered alerts and take necessary actions.

CREATE

How to create an alert policy?

You can create AdminDroid alert policies in two ways. Let's see how to deploy an alert policy in a detailed manner.

Default Alert Policies

To help administrators quickly deploy effective alerts, AdminDroid provides a collection of predefined alert policy templates for common monitoring scenarios. These templates are available on the 'Policy Templates' page.

We have classified default alert policies based on two categories,

Severity: It's important to include severity alerts to address serious issues faster. Some alerts require immediate attention while others can be handled later on. AdminDroid's severity levels includes,

Severe | High | Medium | Low | Info

Labels: AdminDroid includes a notable set of default alert labels such as **configuration changes, external sharing, information governance, permission, risky sign-ins, threat management, and traffic monitoring.** You may apply custom labels for easier classification of alert policies.

How to deploy default alert policies?

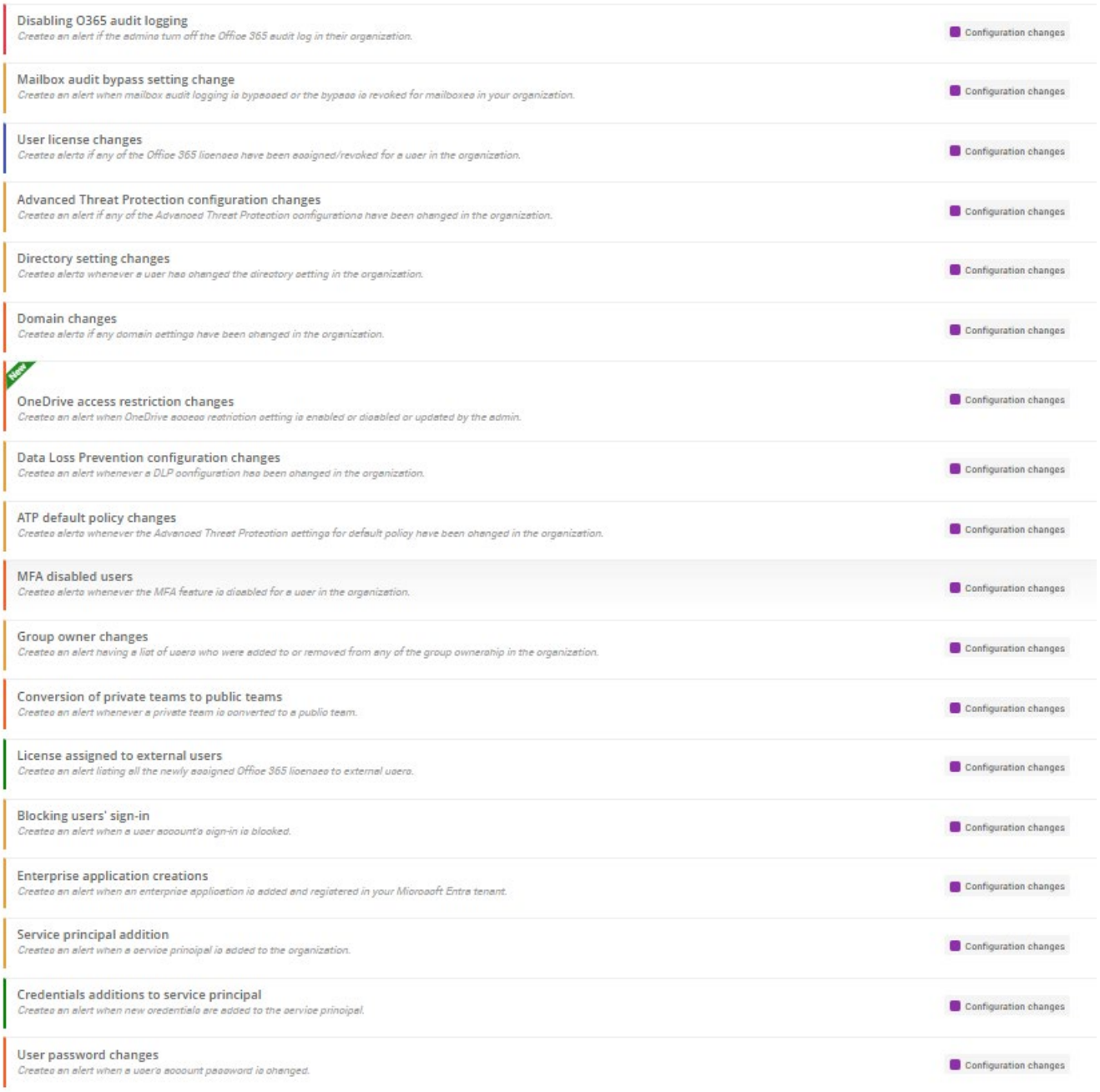
- You can select any one of the 85+ default alert policies you want to deploy on the 'Policy templates' page.
- Click on Preview and Deploy.
- You may change the alert settings, recipients, name, severity, label, etc., and deploy the policy.

Let's see the classification of alert policies based on labels.

- Configuration Changes
- External Sharing
- Traffic Monitoring
- Information Governance
- Permission
- Risky Sign-ins
- Threat Management

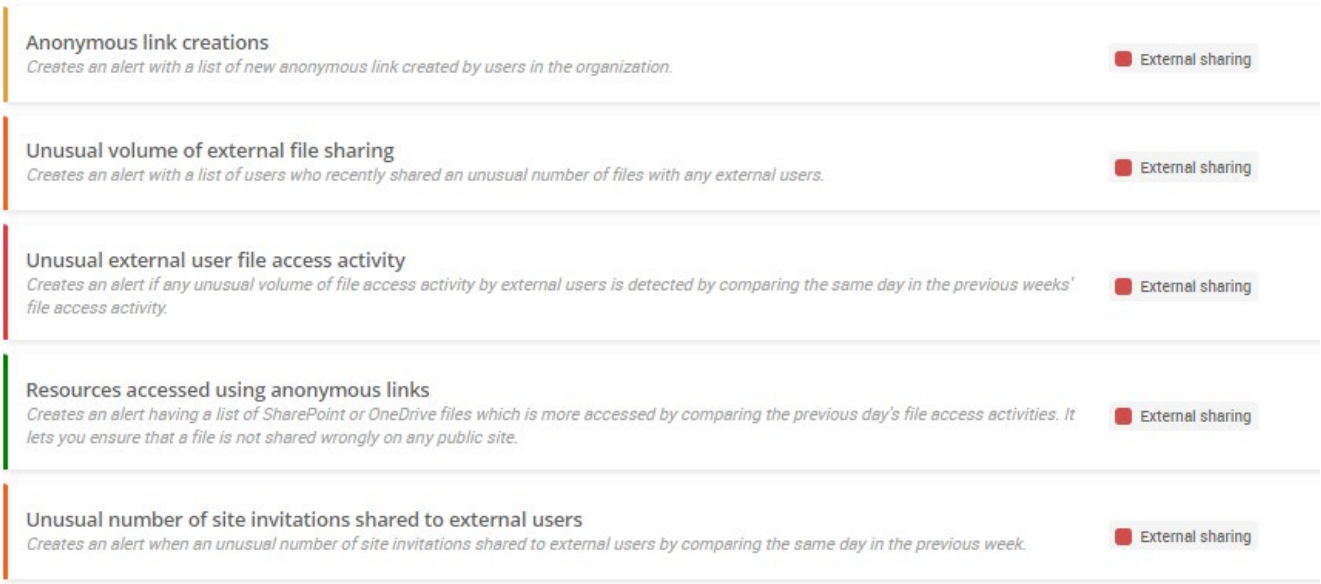
Configuration Changes

Here, policies related to configuration changes are listed. Detailed information on configuration changes, such as user licenses, ATP settings, directory settings, domains, DLP policies, ATP default policies, disabled users with MFA, group owners, and licenses assigned to external users, is available in these reports.



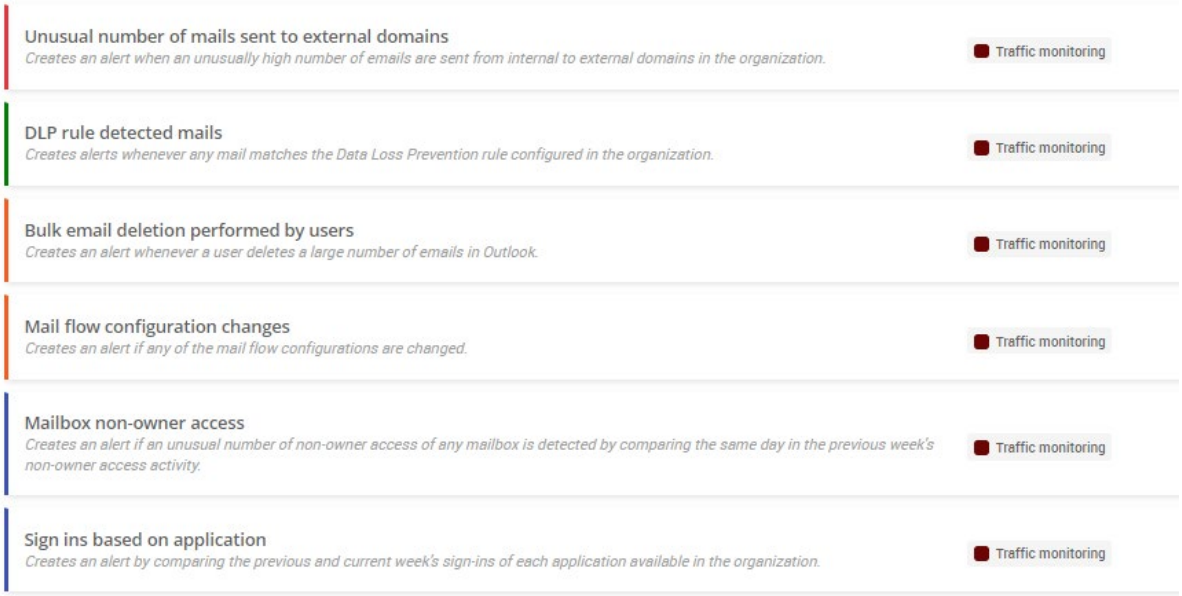
External Sharing

Activities related to external sharing, such as anonymous link creations, unusual volume of external file sharing and external user file access activities, resources accessed using anonymous links, and unusual number of site invitations shared to external users are detailed in these reports.



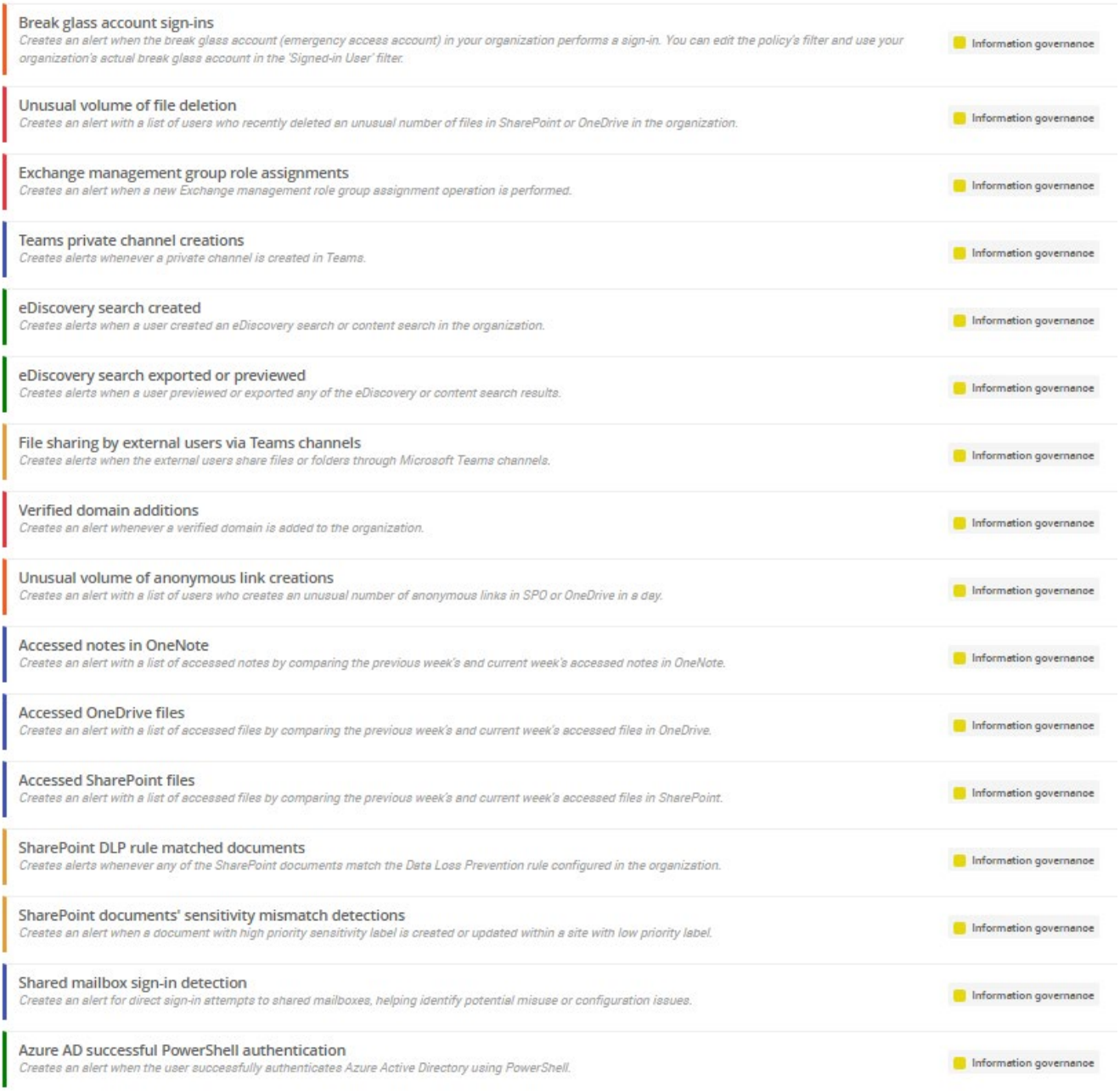
Traffic Monitoring

Reports on mail traffic enable admins to identify unusual email activities and follow appropriate procedures to reduce security risks and stay in compliance. Events related to traffic monitoring such as DLP rule matched mails, mail flow configuration changes, mailbox non–owner access, and sign-ins based on application are listed under this label.



Information Governance

Under information governance, admins can track events, such as unusual volume of file deletions, Teams private channel creations, eDiscovery search creations & exportations, accessed OneDrive files, SharePoint DLP rule matched documents, etc.



Permission

Configuration changes related to permission, such as elevation of administrative privileges, admin consent to applications, teams channel ownership changes, and re-enabling blocked user accounts are listed in these reports.

Elevation of Global admin privilege *Creates an alert when a user is added to the global admin role in the organization.*	Permission
External user addition *Creates an alert whenever an external user is added to the organization.*	Permission
Elevation of Exchange admin privilege *Creates alerts if a user gets added to the Exchange admin role in the organization.*	Permission
OneDrive site collection admin added *Creates an alert if an admin is provided access to a user's OneDrive site collection. You can use this to identify unauthorized or unexpected data accesses if any.*	Permission
Granted mailbox permission *Creates an alert whenever an administrator grants mailbox permissions to a user.*	Permission
Admin consent to applications *Creates an alert having a list of consents given to any applications by the admins in the organization.*	Permission
Elevation of administrative privilege *Creates alerts when a user gets added to any of the admin roles in the organization.*	Permission
Users removed from admin role permission *Creates an alert whenever admin role permissions are revoked from the users in the organization.*	Permission
Teams channel ownership changes *Creates an alert with a list of newly changed ownership in the Teams channels.*	Permission
SharePoint sharing policy changes *Creates alerts whenever changes are made to the organization's SharePoint sharing policy.*	Permission
Site permission level changes in SharePoint *Creates an alert by comparing the changes in site-level permissions between the previous and current week in SharePoint.*	Permission
Re-enabling blocked user accounts *Creates an alert when an admin enables any of the previously sign-in disabled user accounts in the organization.*	Permission
Owner addition to service principal *Creates an alert when a new owner is added to the service principal within the organization.*	Permission
App role assignment grants to users *Creates an alert when an app role assignment is granted to a user.*	Permission

Risky Sign-ins

Risky sign-in activities, such as an unusual volume of sign-ins blocked by access policies, an unusual volume of admin login failures, sign-ins from anonymous IP addresses, and all failed activities are listed in this report.

Unusual volume of sign Ins blocked by Access Policy *Creates an alert if an unusual number of sign-ins blocked due to access policy by comparing the same day in the previous week's blocked sign-ins.*	Risky sign-ins
Account lockouts due to incorrect sign-in attempts *Creates an alert whenever account lockouts occur due to users' incorrect sign-in attempts.*	Risky sign-ins
High level risky sign ins *Creates alerts if a high-level risky sign-in is detected for a user in the organization.*	Risky sign-ins
Unusual volume of admins' login failures *Creates an alert whenever an unusual volume of admins' login failures has been detected when compared to the same day in the previous week's failed logins.*	Risky sign-ins
Unusual volume of user login failures *Creates an alert when the user logins fail unusual number of times in the organization.*	Risky sign-ins
Users failed to pass MFA challenge *Creates an alert whenever users fail an unusually high number of times to pass the MFA challenge while signing into the organization.*	Risky sign-ins
Unlikely travel risk detections *Creates alerts if an impossible travel risk is detected for any users in the organization.*	Risky sign-ins
Sign ins from anonymous IP address *Creates alerts when a user sign-in from an anonymous IP address risk is detected in the organization.*	Risky sign-ins
Admin confirmed user compromised *Creates alerts whenever admins confirmed a risky user as compromised in Azure Active Directory.*	Risky sign-ins
All confirmed risky sign-ins *Creates an alert when the risky sign-ins are confirmed as remediated, dismissed, and compromised.*	Risky sign-ins
Users' risky sign-ins with detailed Info *Creates an alert whenever risks are detected in user sign-ins in the organization.*	Risky sign-ins

Threat Management

> Threat-causing events, such as the creation of external forwarded rules, admins-forced user password resets, unusual anonymous user file activities, resolved risky sign-ins of users, blocked user login attempts, and more can be managed from these alert policies.

Customized Alert policies

You can create your own new alert policies for activities that you want to track in your organization.

AdminDroid supports both Activity-based alerts and Property-based alerts to help you monitor your Microsoft 365 environment effectively.

Activity-based alerts monitor user and administrative actions across Microsoft 365. The **New Events, Threshold, and Comparison** alert types help you detect new activities, identify unusual activity volumes, and compare activity trends over time.

New Events

Stay informed of any crucial activities happening in your organization by configuring **New Events**.

Threshold

You can define a **Threshold** to alert you when the occurrence of events falls within your threshold. Say when a user's login fails more than 10 times in a minute.

Comparison

Analyze activities over past periods with the **Comparison** alert type. The past period includes daily, weekly, and same day comparisons from the previous week and month.

Property-based alerts monitor changes to important Microsoft 365 attributes and configurations. The **New Change** alert type helps you track updates to critical properties and receive notifications whenever a monitored value changes or matches specified conditions

New Change

Never miss important property updates using the **New Change** alert type. Receive notifications when a monitored property value changes or meets the defined criteria.

When Can We Use New Events?

New event alerts will notify you of critical activities happening in your organization. You can stay on top of all suspicious activities such as admin role changes, malware emails, license changes, high-risk logins, and so on.

Customization Available:

Further, you can customize how you get alerts for important events.

Single alert:

Get one alert for all new activities grouped together.

Separate alerts:

Receive individual alerts for each new activity.

Explore advanced customization

Few Use Cases:

User added to Global/any administrator role:

The global administrator role holds the highest level of privileges within an organization. It enables one to manage, control, and monitor access to critical resources. Taking care of role changes from a user to a global or any domain admin is necessary. Configure this alert policy to get notified when a user is added to the global/any admin role in the organization.

License changes:

As you know, users will require the appropriate licenses to access Microsoft 365 services. This policy will trigger alerts when any of the Microsoft 365 licenses have been assigned/revoked for a user in the organization.

High-level risky users sign-ins:

High risky sign-ins denote a sign-in attempt may be malicious or associated with compromised credentials. By configuring this policy, admins can get informed when high-level risky sign-in is detected for a user in the organization.

When Can We Use Threshold?

You can specify the number of times an action can happen before an alert is raised. If the actions surpass the given Activity measurement, then you will get notified. Activities such as bulk file deletions, an unusual amount of external file sharing, anonymous link creation, and so on can be captured with ease.

Customization Available:

Activity measurement:

You can set activity measurement when you are configuring threshold and comparison alerts. Here, you can specify the increment/decrement of event count along with time measurement.

Single/Separate alerts:

Same as 'New Events'. While configuring the 'Threshold' alert type, you can choose between receiving a single alert or separate alerts.

Scope:

Scope lets you target alerts based on specific properties instead of evaluating events across the entire organization. Say for example, you can track failed sign-ins for individual users rather than counting all failed sign-ins organization-wide.

Explore advanced customization

Few Use Cases:

Unusual file deletion:

You may notify admins when a large number of files are removed in SharePoint/OneDrive by setting up a threshold alert. Include 'deleted by' as the scope to figure out who caused the unusual activity.

Higher number of files/folders sharing with external users:

When a user shares a large number of files/folders with external users, there is a high risk of information leakage. Configure threshold alert along with 'operation performer' as scope to list the users who performed external file/folder sharing.

Unusual anonymous sharing link creations:

In most cases, not all content in an organization is suitable for anonymous sharing. Configuring a threshold along with the 'Link created User' will display the users who have created unusually high numbers of anonymous sharing links.

Spike in failed user sign-ins:

If you find an increasing number of failed user sign-in attempts, it indicates the signs of threat. Configure threshold alert along with ‘logged in user’ as scope to determine which user account is involved in high failure attempts.

When Can We Use Comparison Alerts?

Comparison alert is an intelligent technique used for past trend reports and gives out the best outcome when it is combined with the scope feature. Comparison alerts can be used for both reporting and alerting purposes.

Customization Available:

Activity measurement:

You can set Activity measurement when you are configuring threshold and comparison alerts. Here, you can specify the increment/decrement of event count along with time measurement.

For advanced customization:

Same as ‘New Events’. While configuring the ‘Threshold’ alert type, you can choose between receiving a single alert or separate alerts.

Scope:

Scope refers to fine-tuned alerting, triggered by specified attributes that allow targeted alerts instead of org-wide ones.

Explore advanced customization

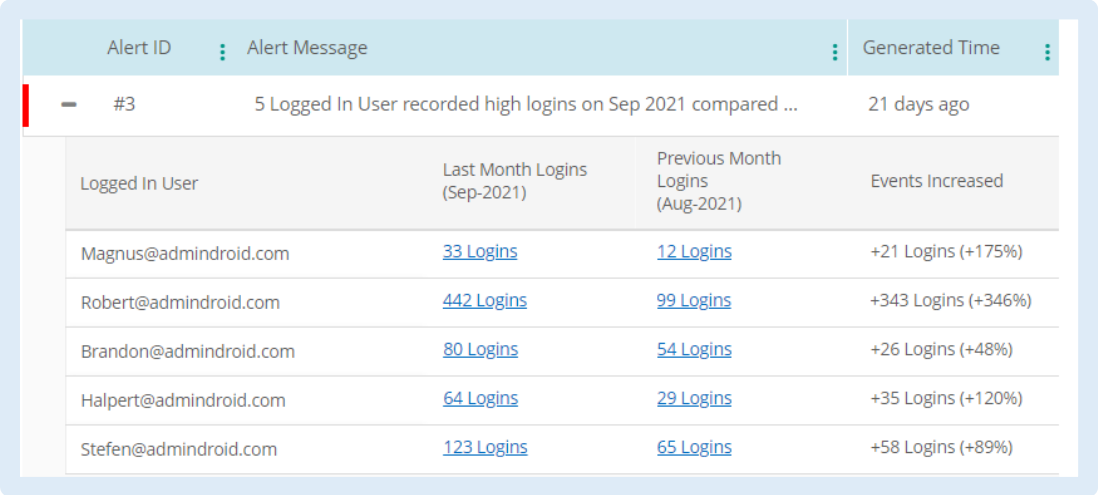
Reporting Use Cases:

Comparison of events between past periods is possible. A detailed summary of events such as user logins, email traffic, file accesses, and so on for every day/week/month will hit your respective emails. Include scope to boost the power of comparison alerts.

> Activities measurement is not required for reporting purposes

User logins trends:

To avoid unusual sign-in activities, it’s important to monitor who is logging in and how often. Configure comparison alerts to analyze the differentiation of user activity count with past behavior activities. Include ‘Logged-in user’ as the scope to know which user logins differ from the past period.

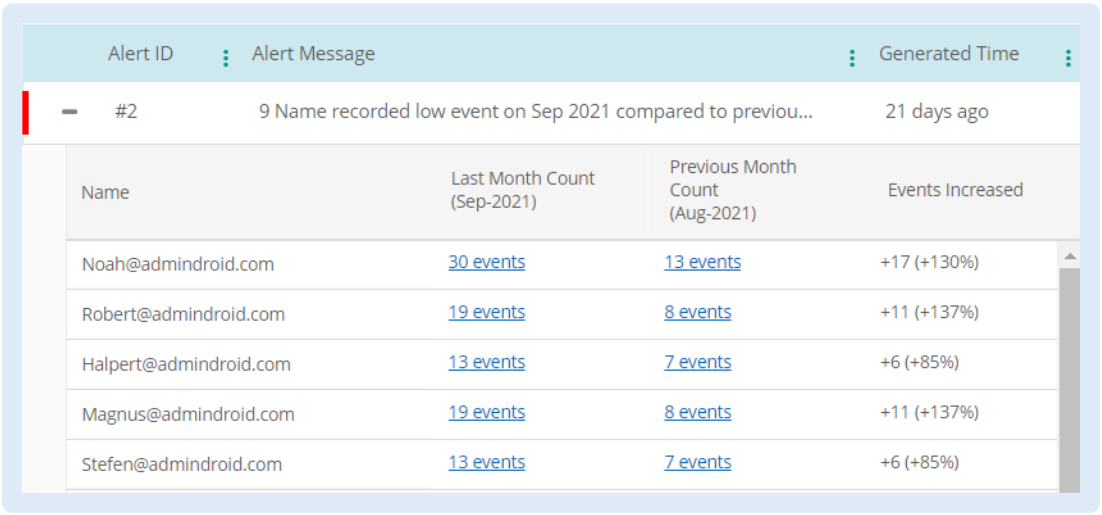


Alert ID	Alert Message	Generated Time
#3	5 Logged In User recorded high logins on Sep 2021 compared ...	21 days ago

Logged In User	Last Month Logins (Sep-2021)	Previous Month Logins (Aug-2021)	Events Increased
Magnus@admindroid.com	33 Logins	12 Logins	+21 Logins (+175%)
Robert@admindroid.com	442 Logins	99 Logins	+343 Logins (+346%)
Brandon@admindroid.com	80 Logins	54 Logins	+26 Logins (+48%)
Halpert@admindroid.com	64 Logins	29 Logins	+35 Logins (+120%)
Stefen@admindroid.com	123 Logins	65 Logins	+58 Logins (+89%)

Email traffic:

Email traffic must be tracked by organizations that rely heavily on email communication. Mailbox traffic reports provide crucial details such as the volume of spam entering your organization's mailboxes, the users who send and receive the most mail, and the users who receive the most junk and malware. Configure comparison alerts to analyze the differences in email traffic with past behavior.

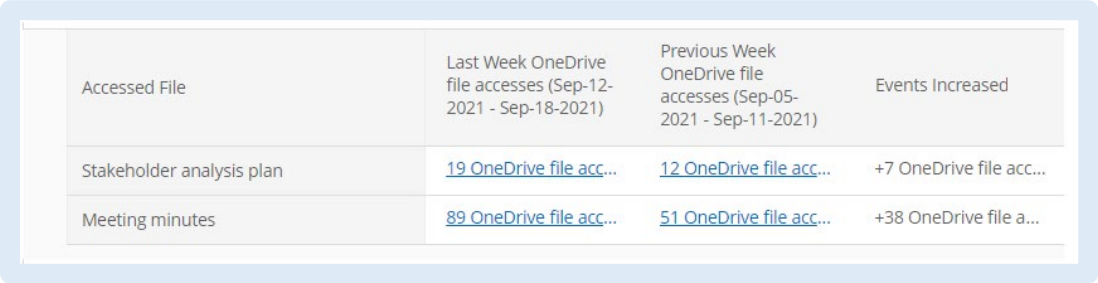


Alert ID	Alert Message	Generated Time
#2	9 Name recorded low event on Sep 2021 compared to previou...	21 days ago

Name	Last Month Count (Sep-2021)	Previous Month Count (Aug-2021)	Events Increased
Noah@admindroid.com	30 events	13 events	+17 (+130%)
Robert@admindroid.com	19 events	8 events	+11 (+137%)
Halpert@admindroid.com	13 events	7 events	+6 (+85%)
Magnus@admindroid.com	19 events	8 events	+11 (+137%)
Stefen@admindroid.com	13 events	7 events	+6 (+85%)

Accessed SharePoint/OneDrive files:

Admins can manage the traffic analysis by tracking the files accessed from SharePoint/OneDrive. Configure comparison alerts to analyze the traffic of SharePoint/OneDrive access entries with past period activities. Include 'Accessed file' as scope to know which file access activity differs from the past period.



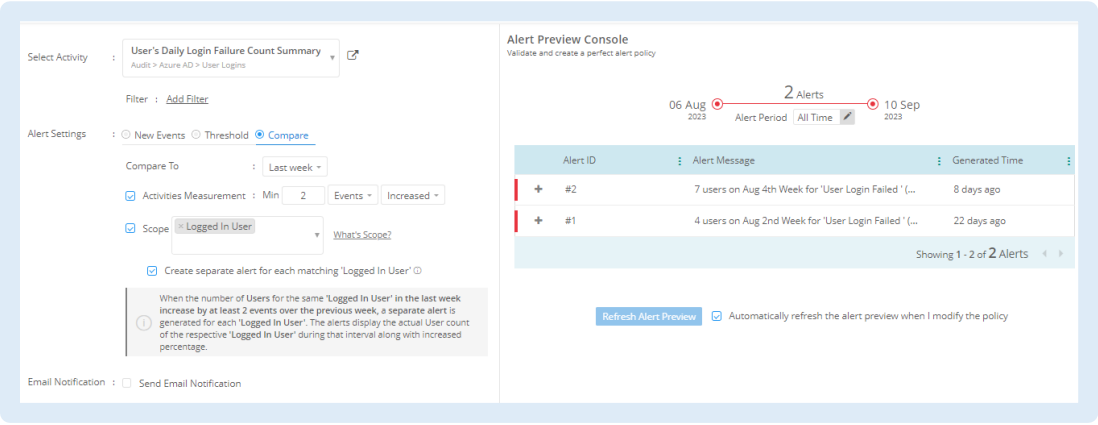
Accessed File	Last Week OneDrive file accesses (Sep-12-2021 - Sep-18-2021)	Previous Week OneDrive file accesses (Sep-05-2021 - Sep-11-2021)	Events Increased
Stakeholder analysis plan	19 OneDrive file acc...	12 OneDrive file acc...	+7 OneDrive file acc...
Meeting minutes	89 OneDrive file acc...	51 OneDrive file acc...	+38 OneDrive file a...

Alerting Use Cases:

If you find an unusual rise or fall in the number of events compared to the past period, then you can trigger comparison alerts. By doing so, complications in manually defining a threshold condition are reduced. Here are a few use cases in which using **Comparison Alerts** may be quite beneficial.

> Activities measurement is required for alerting purposes to include necessary conditions

Comparison of events between past periods is possible. A detailed summary of events such as user logins, email traffic, file accesses, and so on for every day/week/month will hit your respective emails. Include scope to boost the power of comparison alerts.

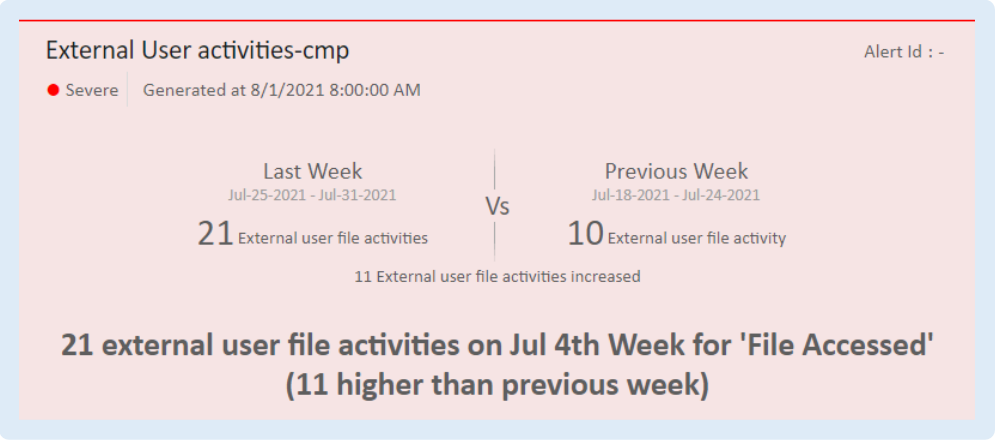


Spike in admin login failures:

When admin login failures are happening often lately in your organization, you may want to track the activity measurement of such suspicious events. In that case, you can opt for comparison alerts to monitor whether the failure count is increasing or decreasing over past periods. Include ‘Attempted Admin Account’ as scope to precisely find alerts for the respective admin accounts that match the policy condition.

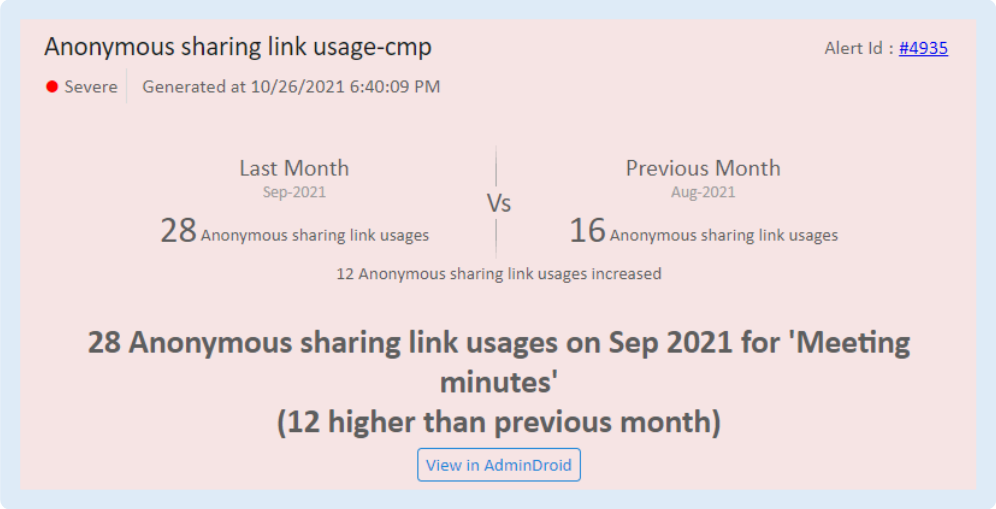
Increase in external user activities:

As the services having external user permissions are at high risk of being involved in security breaches, it is important to have a close watch. Here you can opt for a comparison alert to monitor the frequency of an external user’s access to a targeted file/site/mailbox. Include ‘File accessed’ as scope to identify the targeted file location where the external user activities differ from the past period.



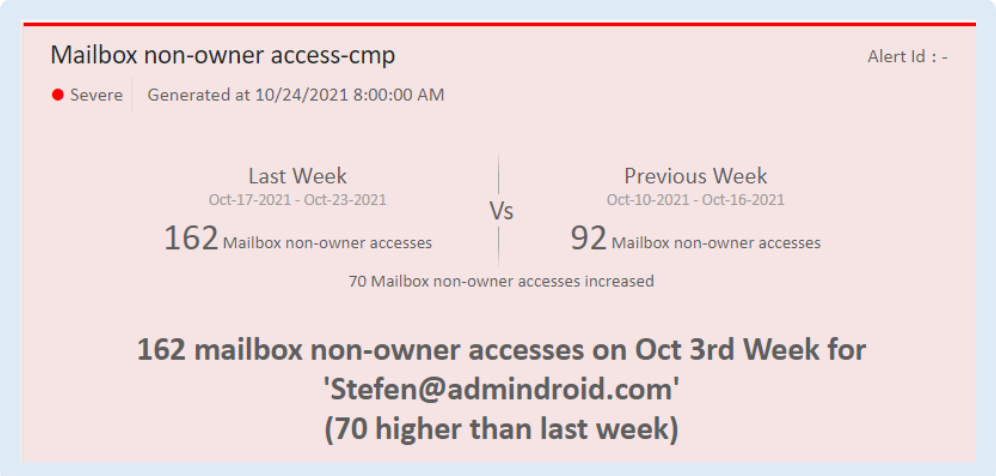
Unusual numbers in anonymous sharing link usage :

Public access links have a major risk of allowing unrestricted access to sensitive data. Here you can opt for a comparison alert to get notified if anonymous link accesses continue to increase day by day. Include 'Shared file' as a scope to get informed when access to the same shared file differs from the previous period.



Excess mailbox non-owner access:

As non-owner mailbox access activities might involve fraudulent activity, it's important to examine if non-owner mailbox access events fit the business context to detect anomalies. To help you with this, you can set up a comparison alert that triggers when there is an increase in non-owner access activity compared to the usual count. Include ‘Accessed by’ as scope to get informed about the mailbox accessibility of non-owners that differs from the previous period.



Failed activities:

If you notice failed operations occurring regularly in a specific Microsoft 365 service, it could indicate an underlying issue that needs to be addressed. Here you can opt for a comparison alert so that whenever the failed activities increase than the normal number, you will get notified. Configure 'Performed by' as scope to know whose activities differ from the past period.

When Can We Use New Change?

New Change alerts help admins monitor the changes made to critical properties, such as sign-in status, location, phone number, MFA device details, user type, display name, storage quota, and more.

You can receive alerts whenever a property's value changes or matches a configured value.

Customization Available:

Further, you can customize how you get alerts for important events.

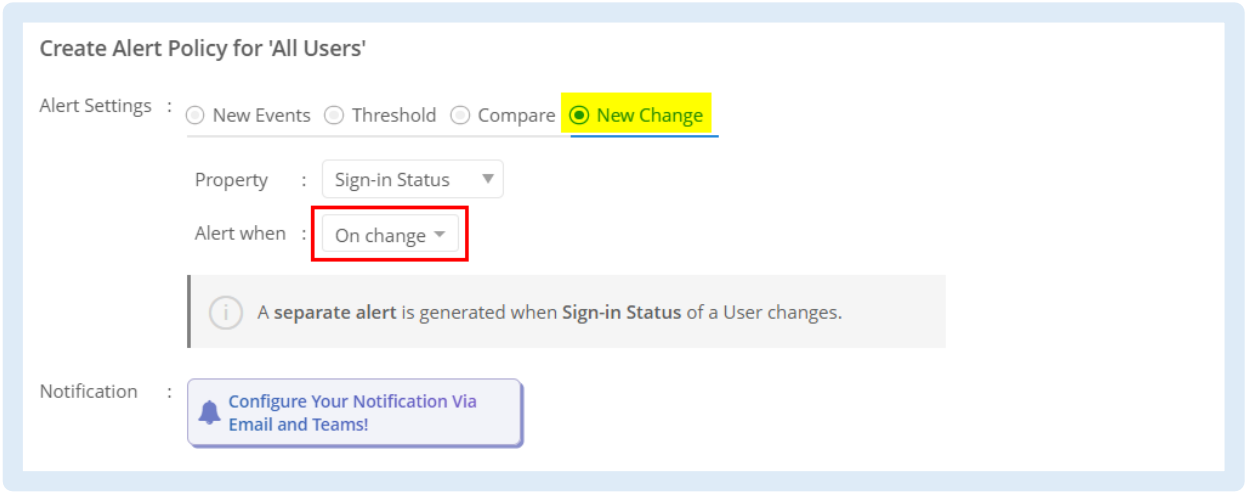
Property changes:

You can select the property you want to monitor and receive alert notifications when its value changes.

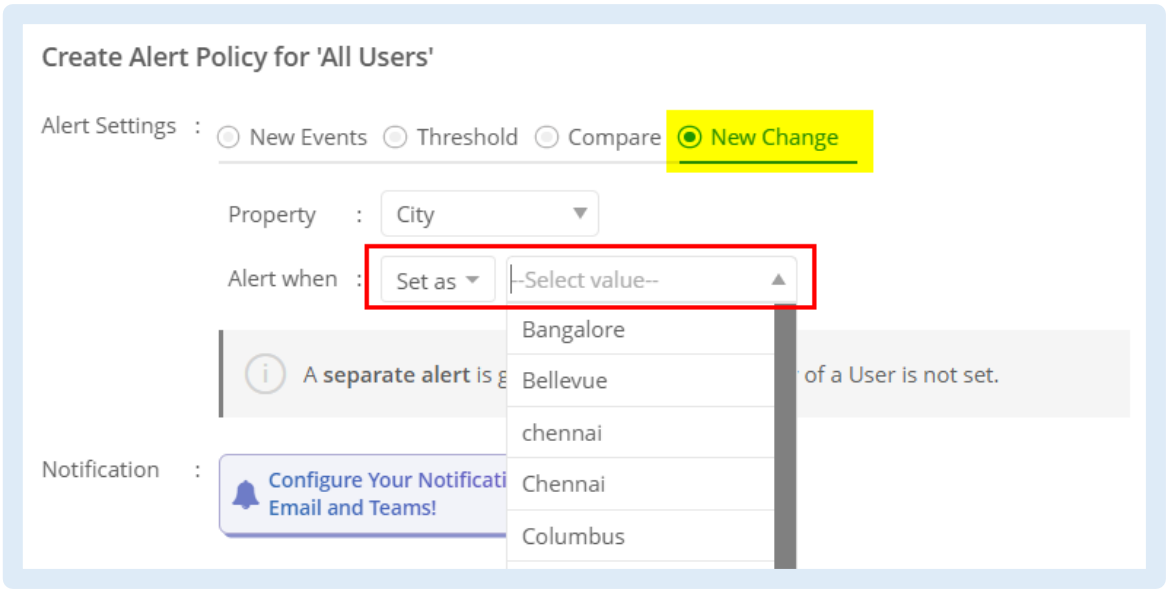
When to be alerted:

Choose how the alert should be triggered. You can either get alerted when the property's value changes or matches the value you specify.

- **Property changed:** Receive an alert whenever the selected property's value is modified/changed.



- **"Set as" value matched:** Receive an alert when the property's value matches the specified condition or value that was set.



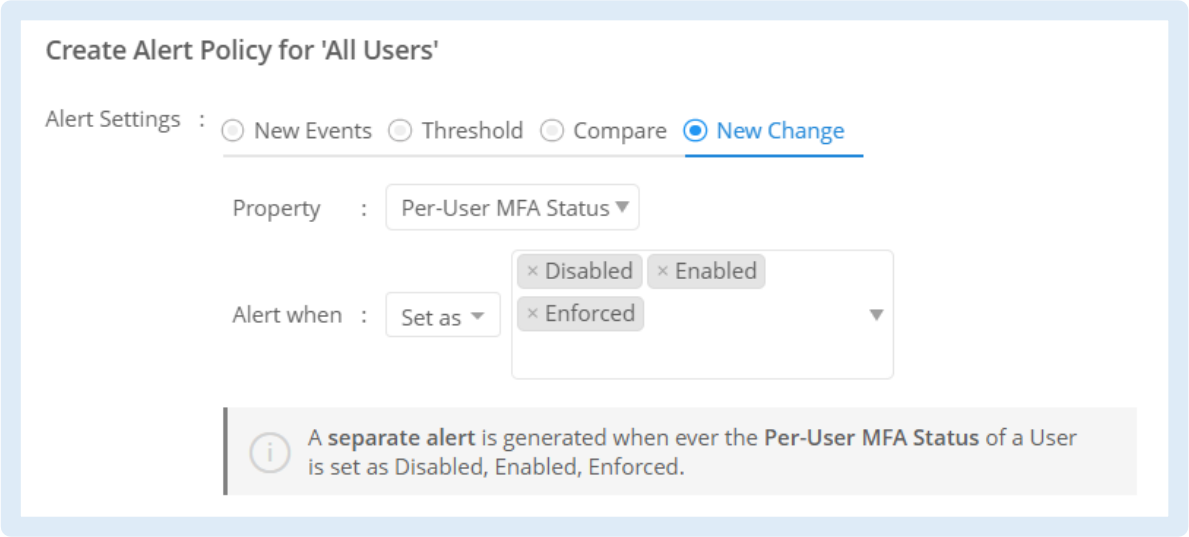
Separate alerts:

A separate alert is generated whenever there is a new change on the selected property. This helps admins to track individual changes with greater precision.

Few Use Cases:

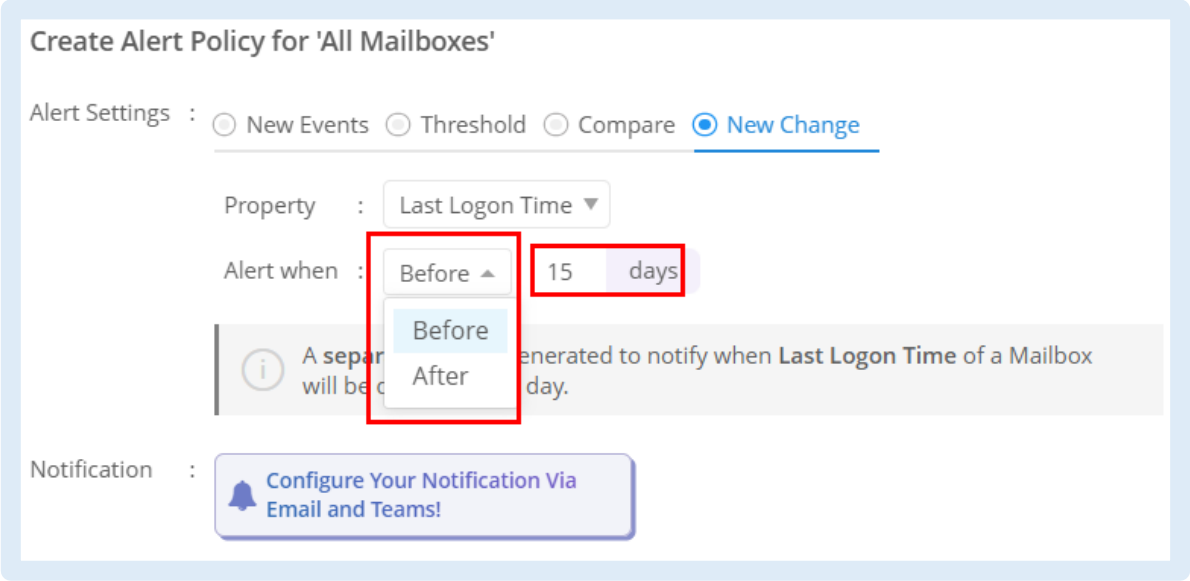
1. **Per-User MFA enforcement status changes**

   Disabling Per-User MFA can increase the risk of unauthorized access, unless MFA is enforced through another policy. Configure this alert type to get notified whenever per-user MFA is disabled for a user, allowing admins to quickly identify the changes.



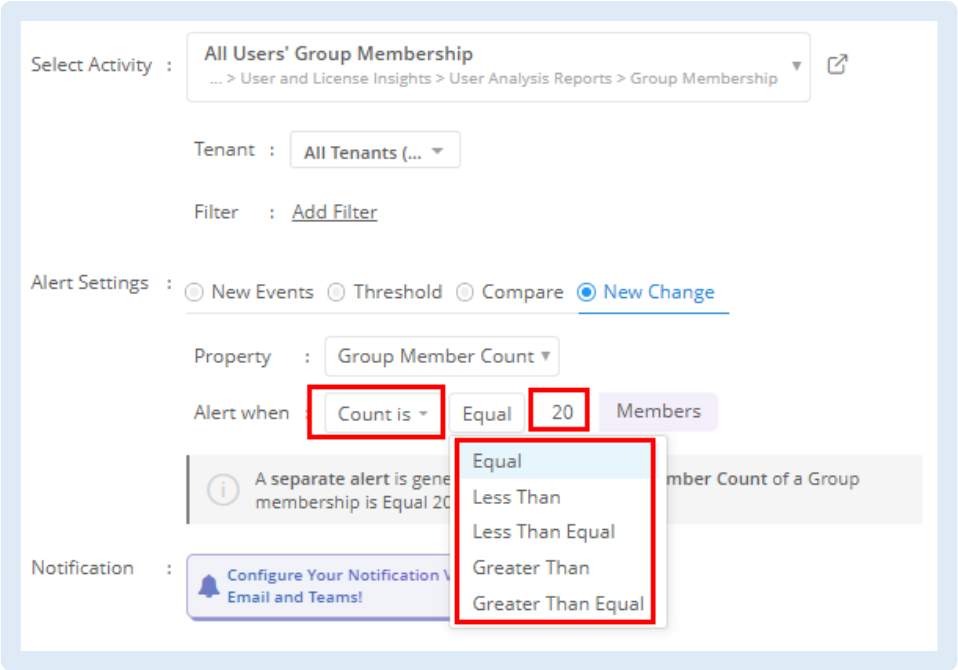
2. **Last logon activity**

Get alerted when user accounts become inactive for longer than expected or crosses a specified threshold, helping you identify stale or dormant accounts that need attention.



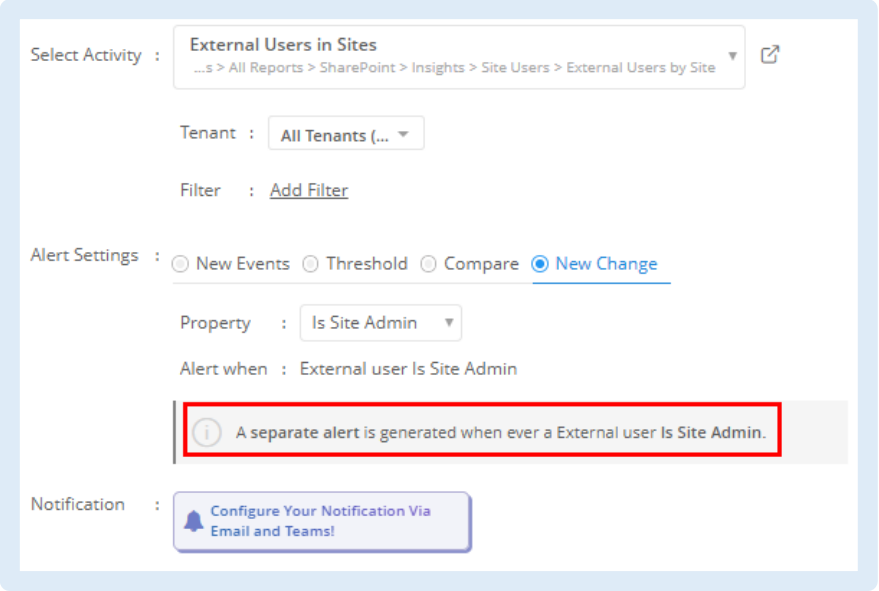
3. **Sudden increase in group members count**

You can use this alert type to get notified when a group's membership exceeds a specified limit. For example, you can configure an alert to trigger whenever a group grows beyond 20 members.



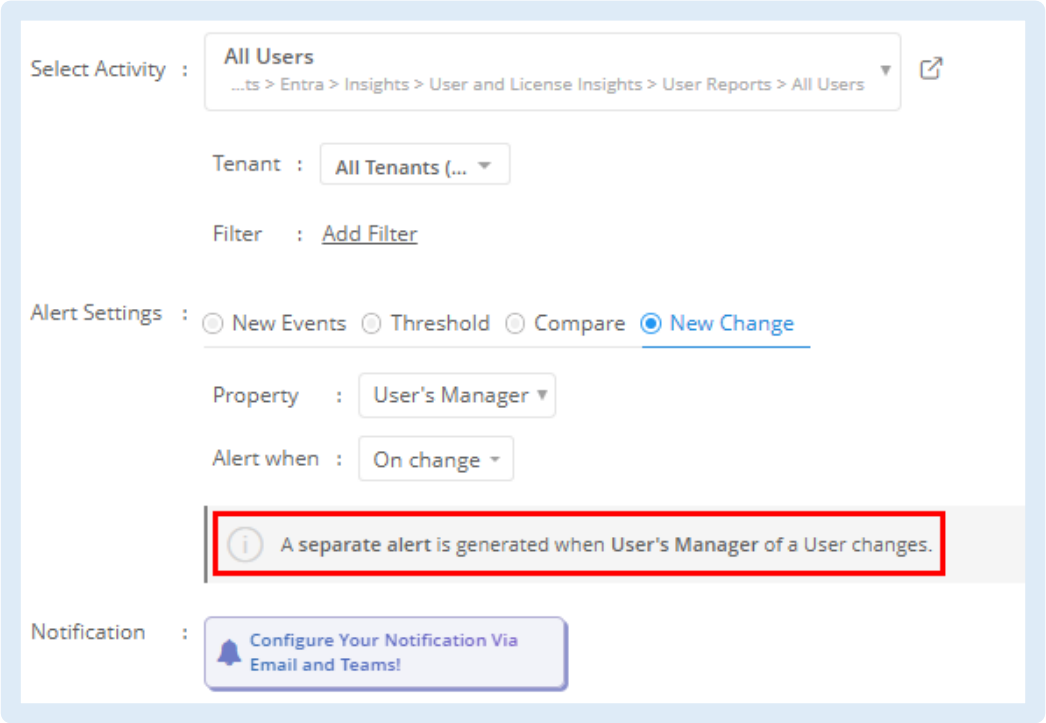
4. **Granted site admin access to external user**

Granting site administrator privileges to external users can provide broad control over a SharePoint site. Configure this alert to receive notifications whenever an external user is assigned site admin rights.



5. **Manager changed for a user**

A user's manager is often used in approval workflows, organizational hierarchy, performance management, and access governance processes. Configure this alert type to get notified whenever a user's manager is assigned, updated, or removed.



OPTIMIZE

How can you optimize your alert policies?

When the number of alerts generated increases, managing them becomes more challenging. This is where your alert policies need to be optimized. To optimize your alert policies, AdminDroid has included some unique features such as:

- **Scope**
- **Group Similar Alerts**
- **Alert Preview Console**

Scope

> Scope - Granular alerting based on the attributes you specify

Instead of sending out organization-wide alerts, you can use Scope to accomplish focused alerting that raises alerts based on the attributes you define. If you don't specify any attribute, then the scope of the alert policy will get considered as the entire organization.

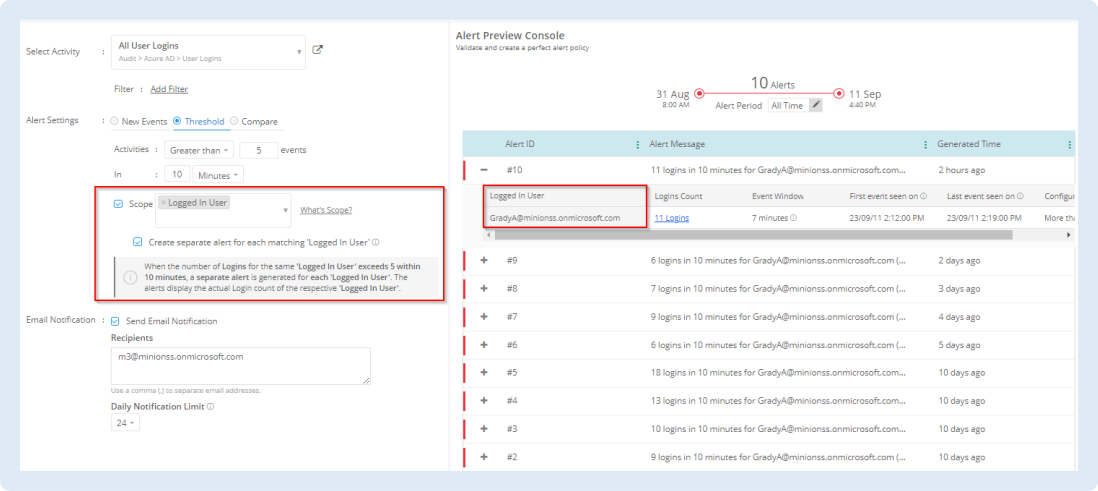
When Can We Use Scope?

Say you need to monitor the user sign-in attempts when it reach a threshold of 5 logins in 10 minutes, you can refer to the **All User Logins** report inside AdminDroid.

With Scope:

Based on a single property:

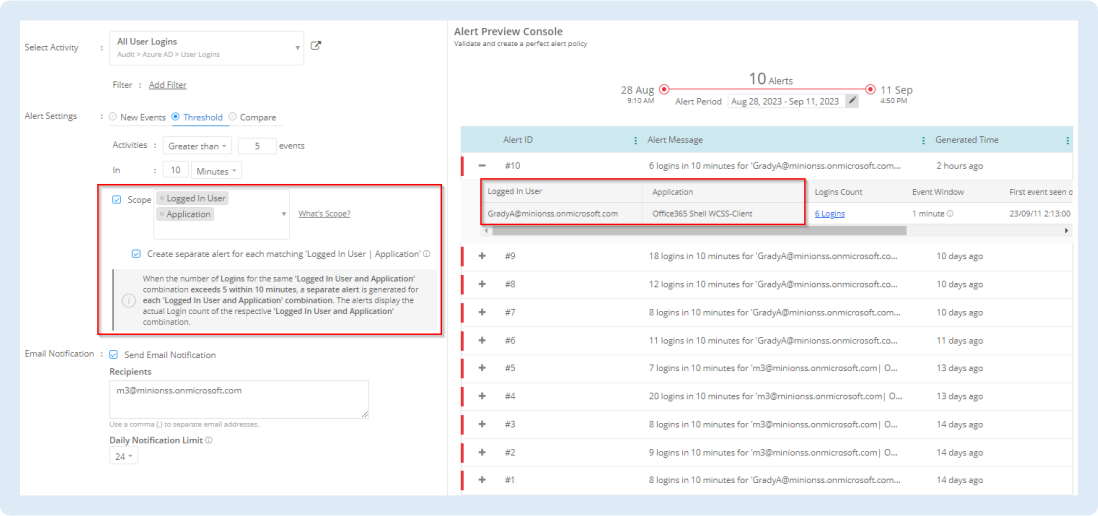
In this case, if you define 'Logged in user' as scope, alerts will get generated for each logged in user.



Based on multiple properties:

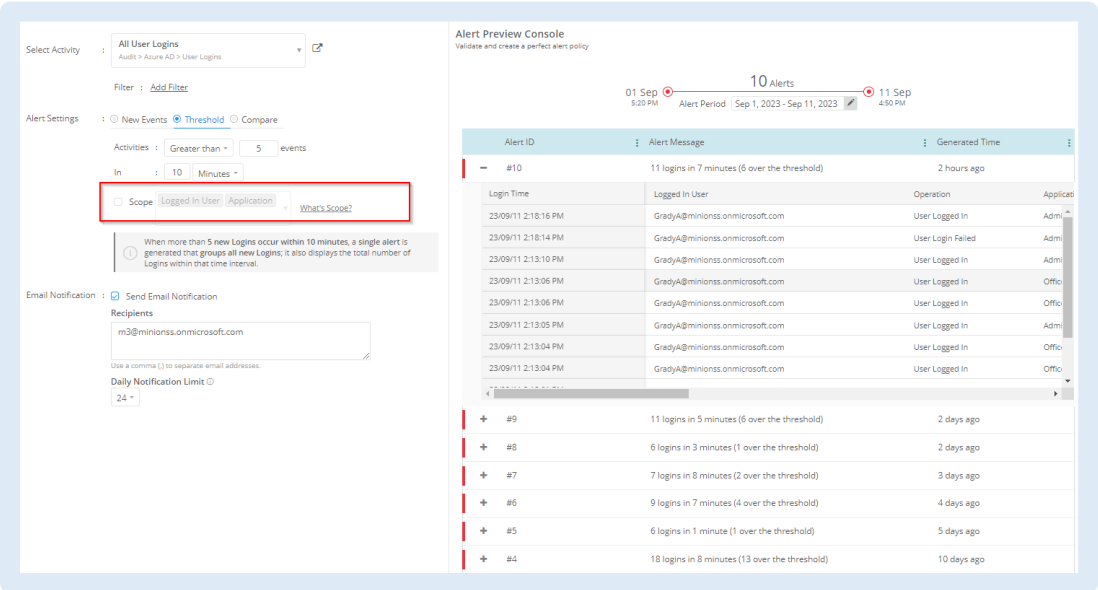
Say you need to monitor the user sign-in attempts for a specific application when a user tries to log in 5 times in 10 minutes. In this case, if you define both 'Logged in user' and 'Application' as scope, alerts will get generated for each logged in user and the application combined.

> Analyze data in multiple dimensions by using multiple scope properties



Without Scope:

In contrast, if you don't define any scope, it will check org-wide, and an alert will get generated grouping all user sign-ins.



Group Similar Alerts

> Specify whether to receive individual alerts or grouped alerts

After customizing your alert settings, you have the option to choose between receiving single or separate alerts for every new activity. The single alert feature groups all the new activities together and triggers a single alert for all of them. On the other hand, the separate alerts feature triggers individual alerts for every new activity.

Single alert: Single alert feature will trigger grouped alerts for all the activities.

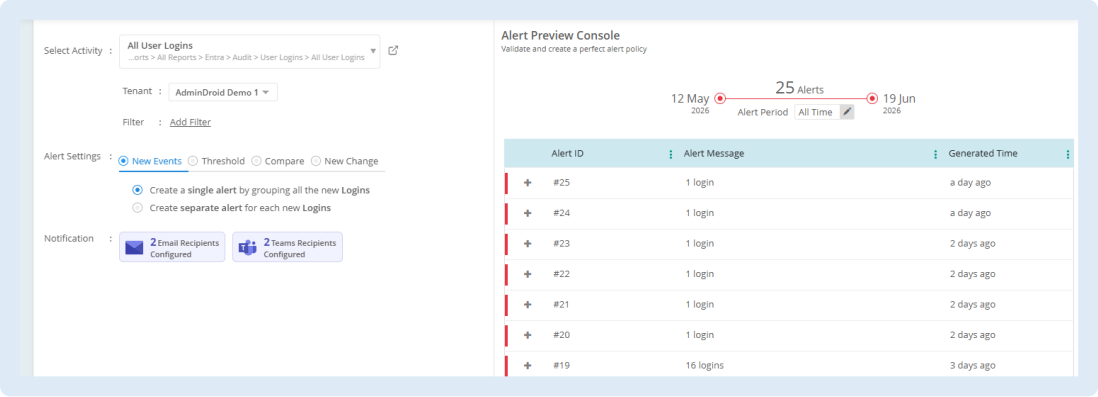
Separate alert: Separate alerts feature is used to trigger individual alerts for every activity.

How do Single/Separate alerts work in New Events alert type?

Let's say you want to monitor all user logins in your organization, you can refer to the **All User Logins** report inside AdminDroid.

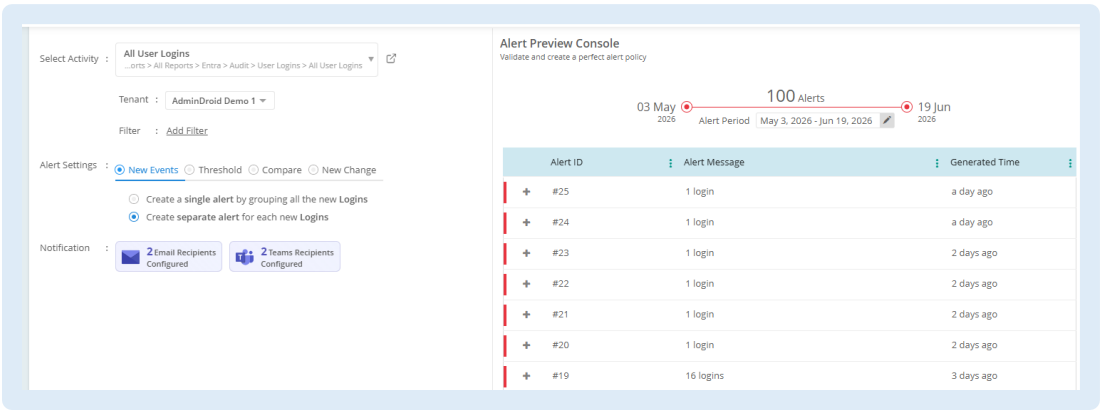
- **Single alert:**

  If you configure a single alert, you will get alerted once for all logins made at the time of alerts.



- **Separate alert:**

  If you configure separate alerts, you will get alerted for individual sign-in.



How do Single/Separate alerts work in Threshold alert type?

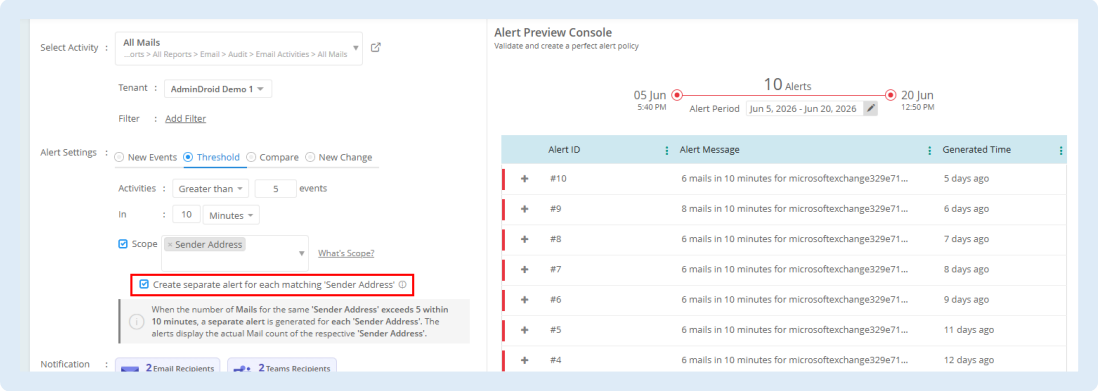
Let's say you want to create a threshold alert for all mail activities whenever a user sends 5 emails within a ten-minute window, you can refer to the **All Mails** report inside AdminDroid.

In this case, you need to configure scope as 'sender address'. So that threshold condition will get applied for each address separately.

> When you include scope, it is possible for users to avail single or Separate alerts. Separate alert is configured by default when scope is added. Checking out the Separate alert box will be considered as a Single alert.

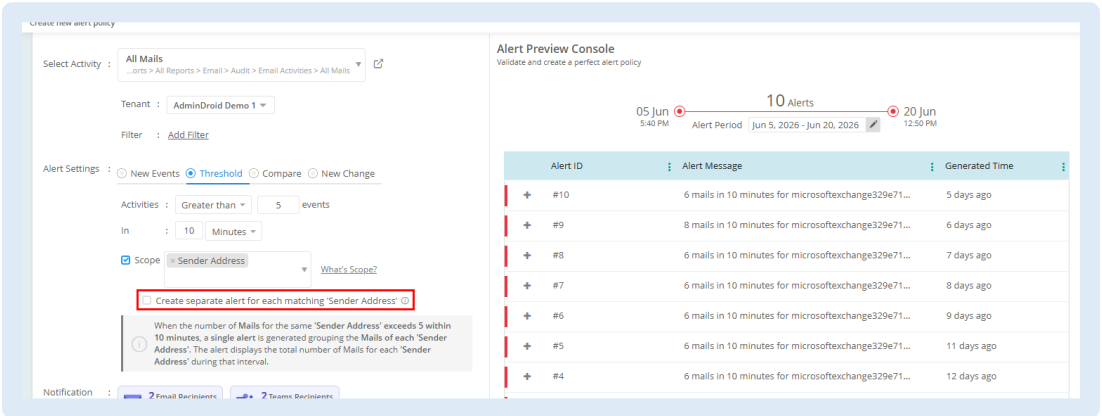
- **Separate alert:**

  You will get separate alerts for each sender who exceeds the threshold limit.



- **Grouped/Single alert:**

  Since you have configured 'sender address' as scope, you will receive single alerts grouping all the senders who exceeded the threshold limit.



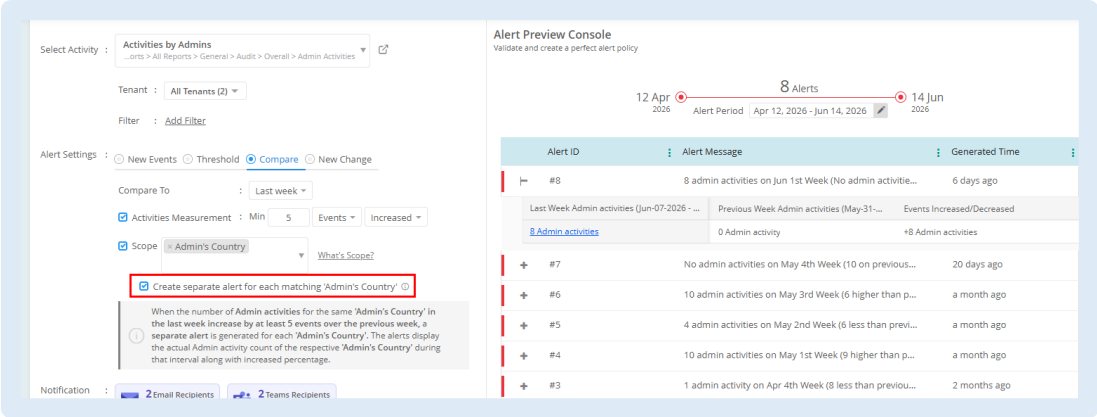
How do Single/Separate alerts work in Comparison alert type?

Let's say you want to monitor the admin activities to get an idea of how frequently they operate compared to the previous month, you can refer to the **Activities by Admins** report inside AdminDroid.

In this case, you may configure 'Operation Name' as scope to find out which operation the admin has performed the most. Here, the triggered alert will contain the differentiation of past period activity counts. (e.g., Last week/previous week)

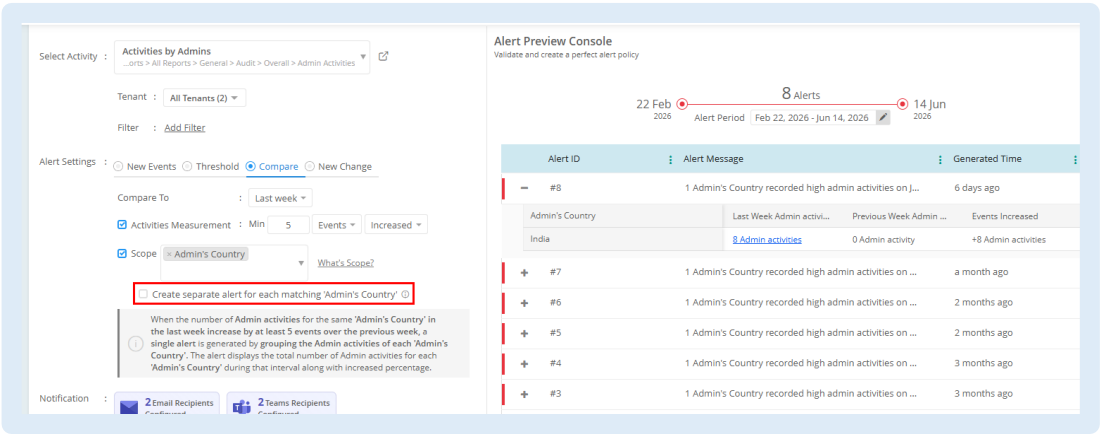
- **Separate alert:**

  Since you have configured 'Operation Name' as scope, you will get separate alerts for each distinct operation.



- **Single alert:**

  Since you have configured 'Operation Name' as scope, a single alert will get generated by grouping all operations.



Alert Preview Console

> Too many alerts! Too many spoilers!!

While creating an alert policy, you may find it difficult to define a perfect threshold for your policy. AdminDroid comes with a smart feature called **Alert Preview Console** which helps in validating the necessary conditions required.

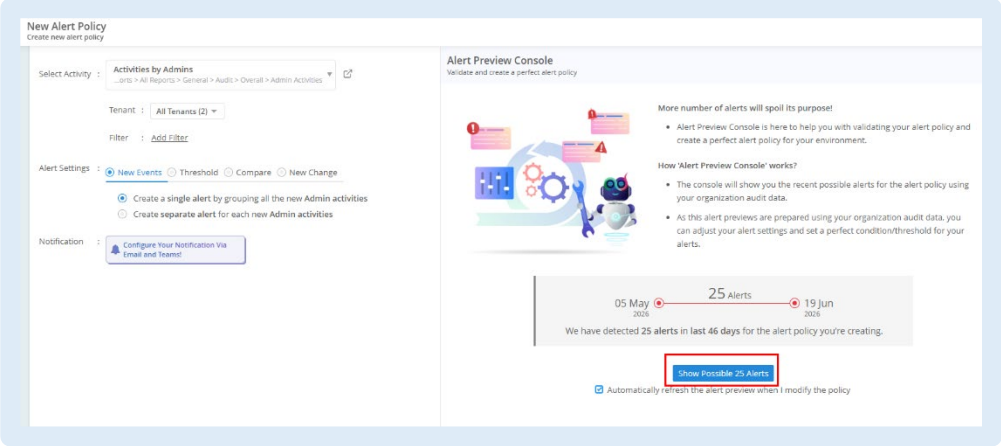
You may alter your alert settings and establish a perfect condition/threshold for your alerts since this alert preview is based entirely on your organization's audit data.

> A validating console where you can preview sample alerts based on past period activities

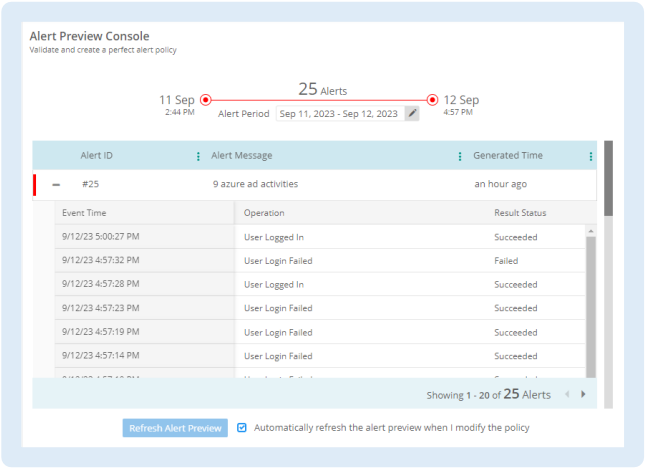
After customizing your alert settings, you have the option to choose between receiving single or separate alerts for every new activity. The single alert feature groups all the new activities together and triggers a single alert for all of them. On the other hand, the separate alerts feature triggers individual alerts for every new activity.

Where can you check for Sample Alerts?

After specifying the required conditions, you can check for sample alerts using the alert preview console.



In the alerts preview console, you receive the alert count along with detailed information such as event time, performed operation, performed user, and so on.



ENGAGE

How can you engage with your alert policies?

Configuring alerts is only the first step. To effectively monitor your Microsoft 365 environment, you need quick access to alert information and actionable insights. AdminDroid provides below ways to view, analyze, and respond to alerts:

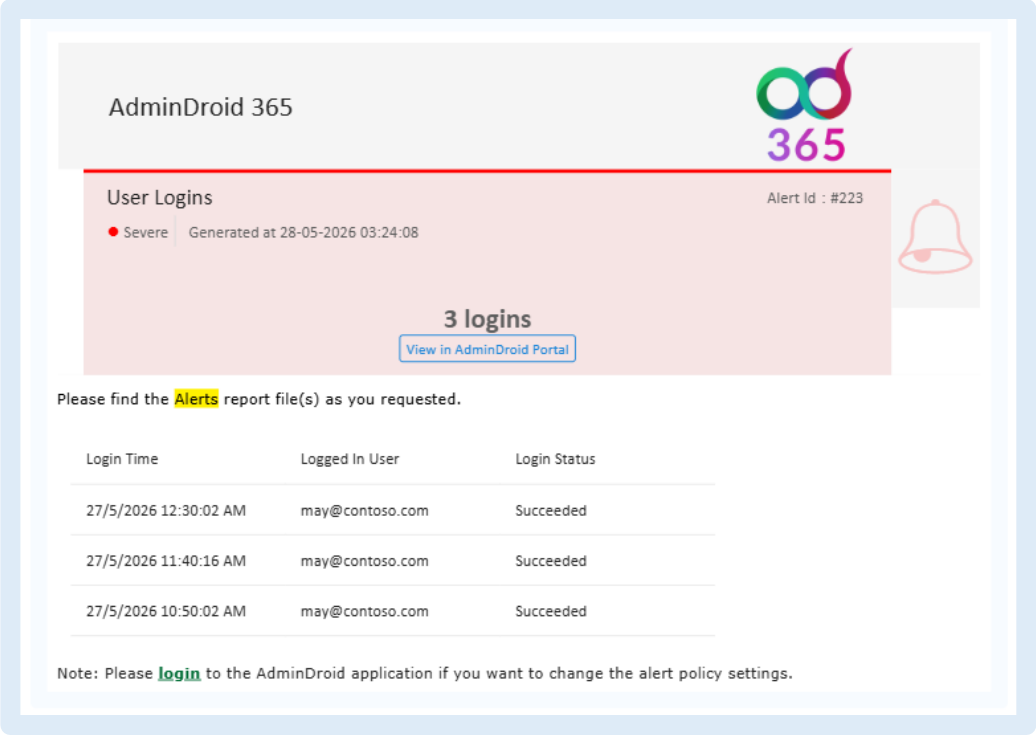
- **Emails**
- **Alert Reports**
- **Alert Dashboard**

These options help admins stay informed, investigate alert activity, and respond promptly to important events.

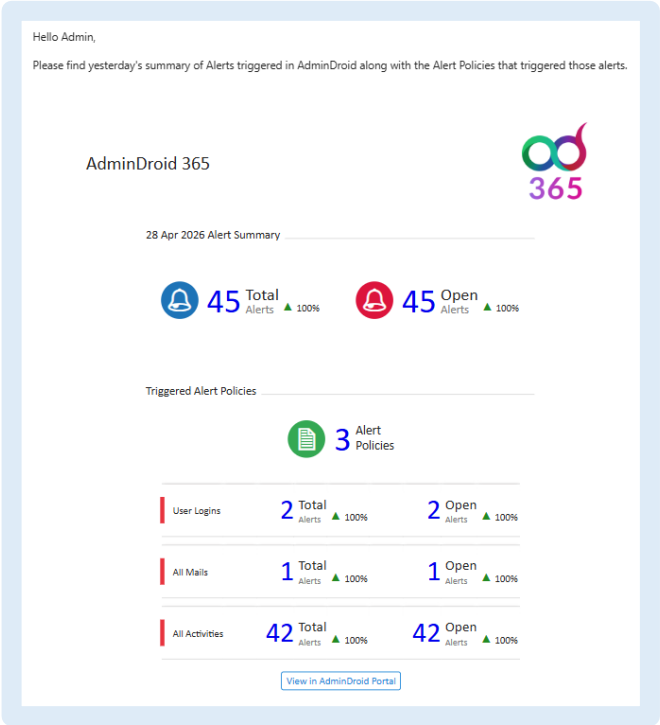
Emails

Email Notifications:

Get notified right away whenever an alert is triggered. Route the alert to the right recipients by setting up an email configuration.



All the configured recipients can view all the triggered alerts for the respective report in emails. Along with the email notification, all selected recipients will receive a summary of events with more details.



Apart from this, you can also include settings related to daily notification limit.

Daily Notification Limit:

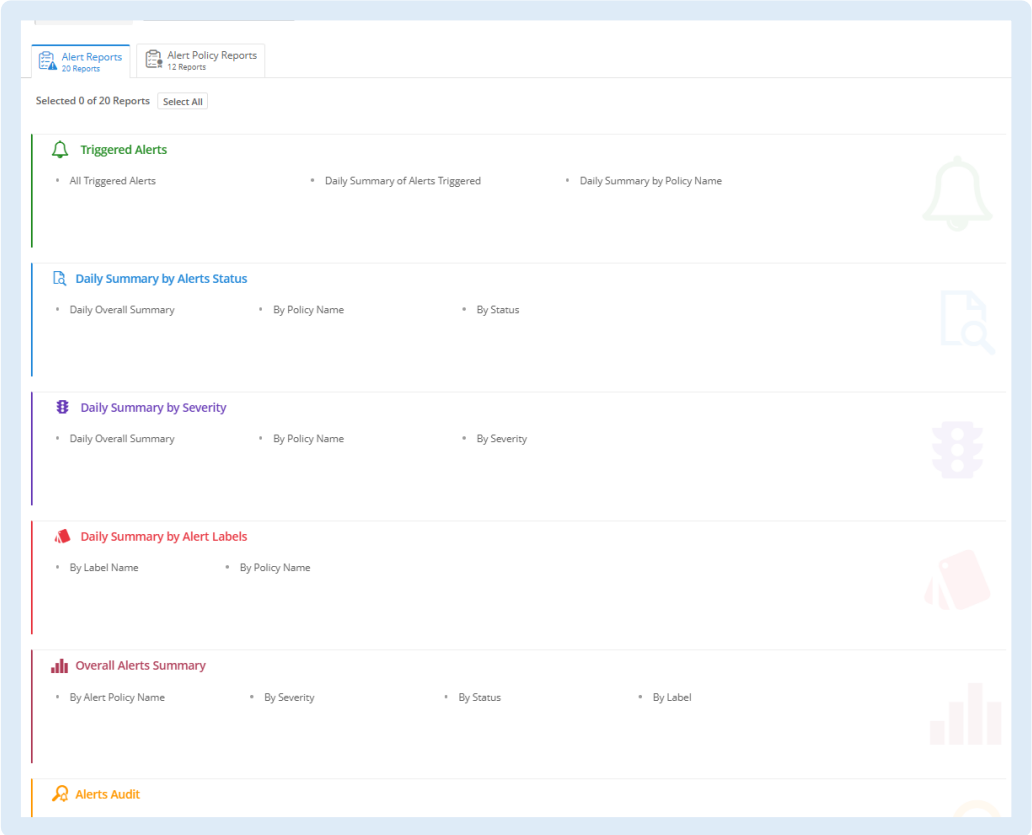
You can set how many email notifications you want to receive for each alert policy per day. However, it does not affect the number of alerts that can be generated.

Alert Reports

AdminDroid Alerts comes up with rich reporting features where you can find separate sections for alert reports and alert policy reports. Reports include interactive dashboards for better insights. To meet your specific requirements, you can create your own custom blend of charts, graphs, and infographics. You can email, download, and schedule all the alert reports from a single location.

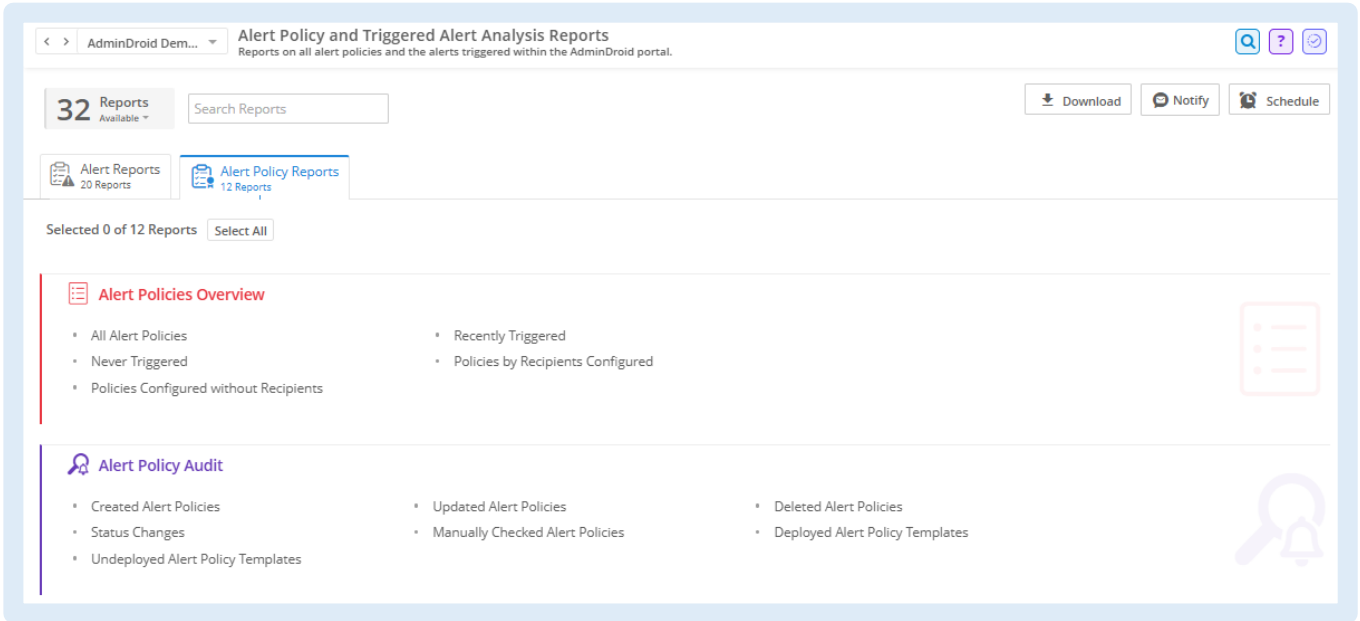
Alert Reports:

Here you can find reports based on categories such as triggered alerts, alert status, severity, labels, overall alerts, alerts audit.



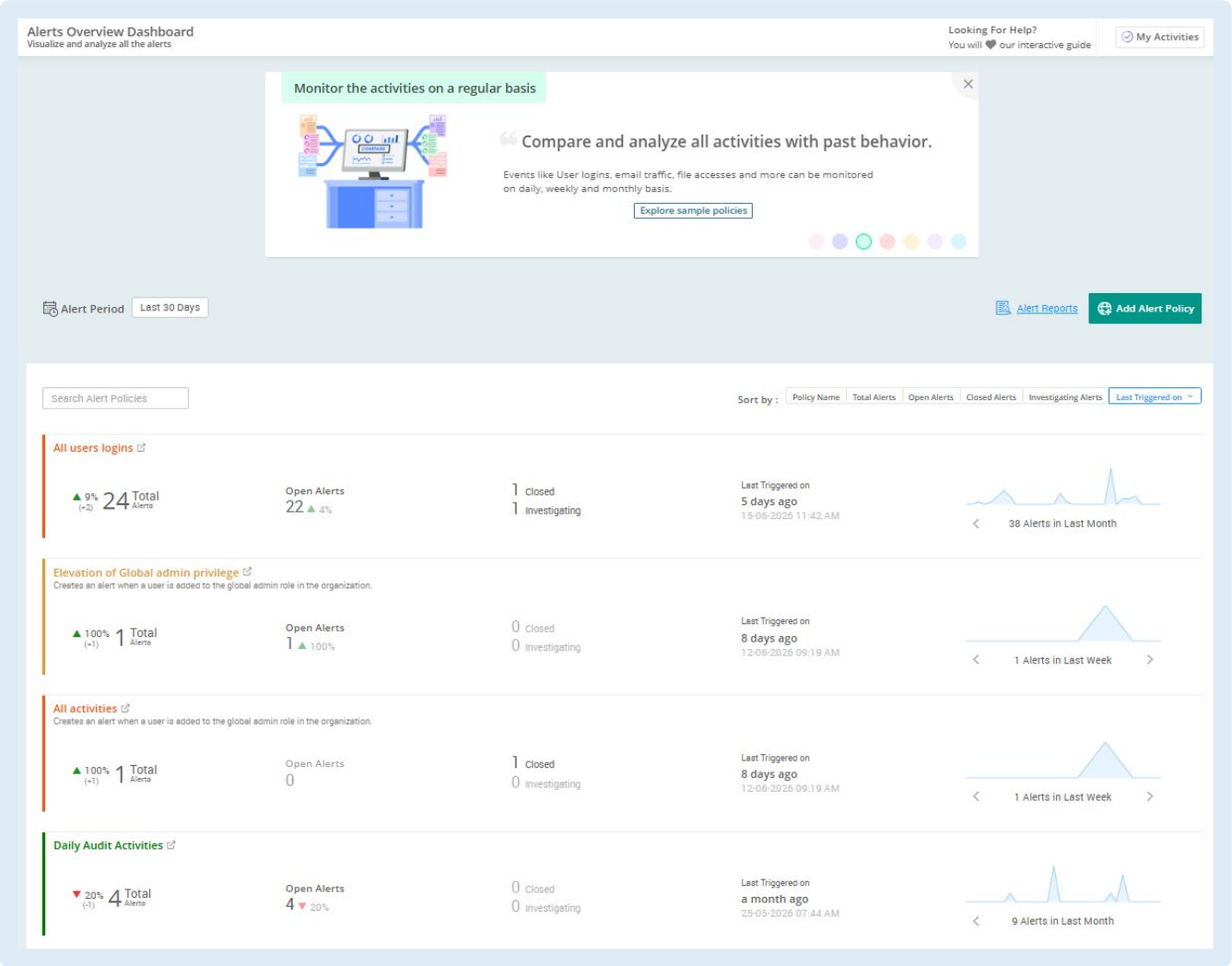
Alert Policy Reports:

Here you can find reports based on categories such as alert policies overview and alert policies audit.



Alert Dashboard

On the Dashboard page, you will see a complete overview of alert trends over time. Graph visualizations will help you to spot variations in the frequency of triggered alerts. You may also look at the most recent triggered alerts. Navigation of respective alert policies is possible with a single click.



- Total alerts generated for the selected time period.
- Total number of alerts with open statuses.
- Count of Closed and investigating alerts among total alerts generated.
- Displays when the last alert was generated, along with the date and time.
- Here are the current alert trends.
- Use the navigation to view past alert trends.

ACTION

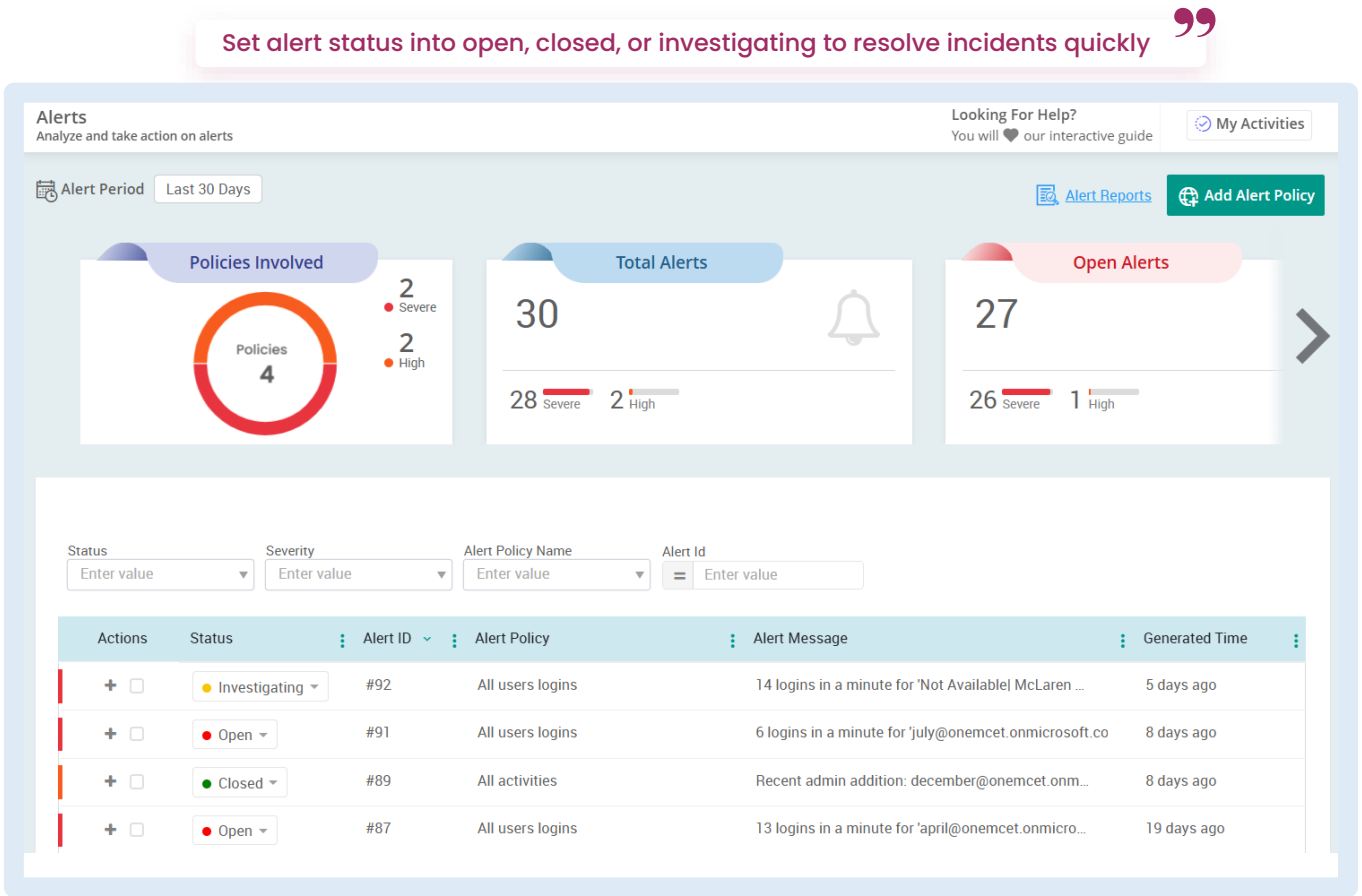
Alerts don't just aim to trigger events, but also to resolve them.

Here let's see what are all the actions that can be taken on triggered alerts.

Alerts Portal

The Alerts page displays all the triggered alerts where you can analyze and take action on alerts. Here you can get a detailed summary of events generated by clicking the '+' icon.

Action - Setting up an alert status assists in identifying the actions taken in response to the triggered events. On the alerts page, you can alter the status of triggered alerts to **open, closed, or investigating**.



How can AdminDroid help to enhance security in the Microsoft 365 environment?

Beyond alerting capabilities, AdminDroid provides a comprehensive array of features that empower organizations to strengthen their security posture.

To proactively safeguard sensitive information and maintain compliance, we have outlined the multifaceted features that every organization can utilize.

AdminDroid

Explore >

Our mission is to solve everyday challenges of IT admins and save their time. We strive to provide admin-friendly software with a user-friendly interface, at a budget-friendly pricing. Try AdminDroid, and you'll love how it simplifies your Microsoft 365 management!

For a live demonstration of our flagship tool, AdminDroid 365, visit below.

Live Demo **Download**

Connect with us

linkedin.com/company/admindroid/
reddit.com/r/AdminDroid/
twitter.com/admiindroid
facebook.com/admindroid
youtube.com/admindroid
admindroid.com
github.com/admindroid-community

© 2026 AdminDroid. All Rights Reserved.