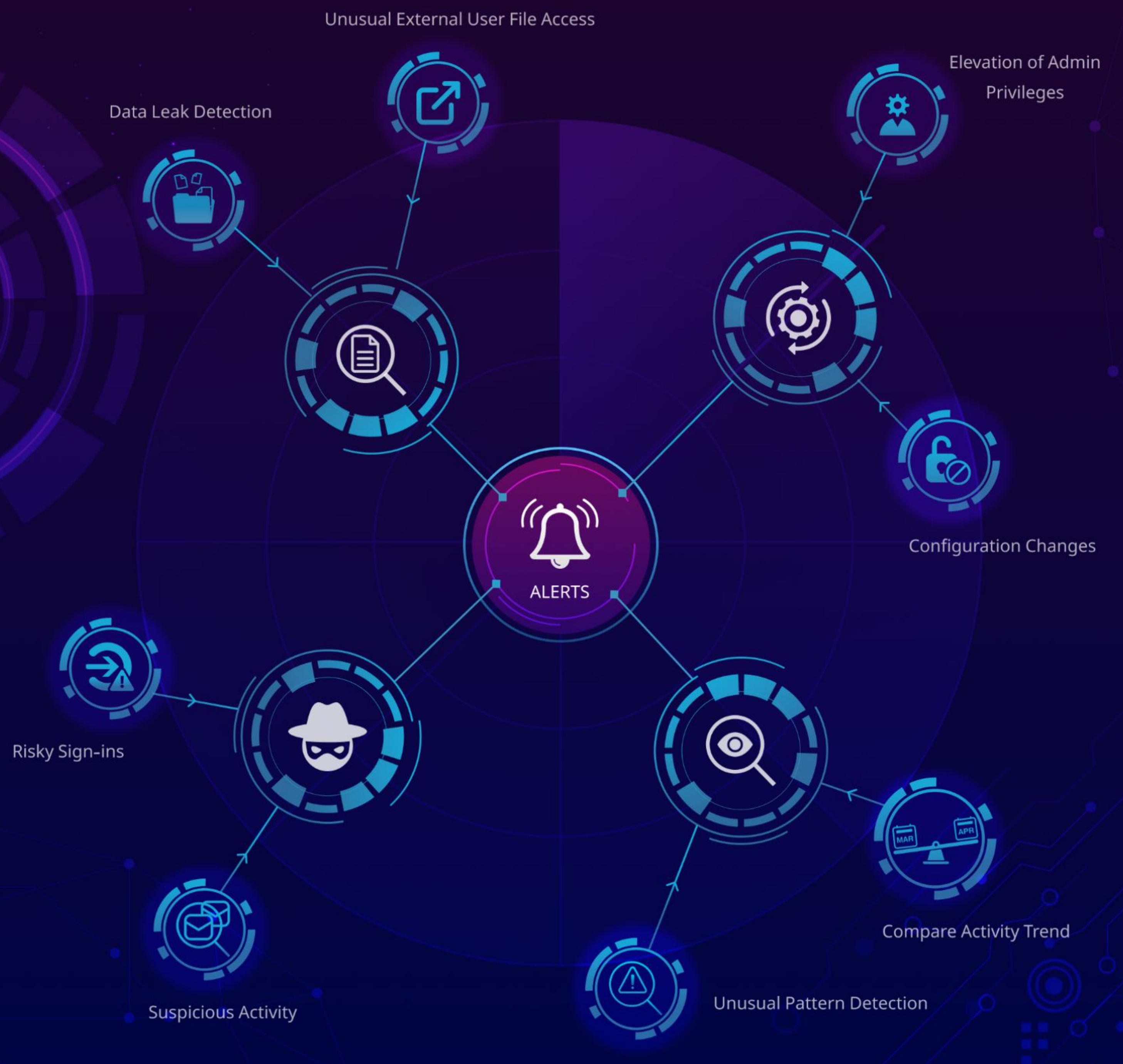
Safeguard your Microsoft 365 Environment

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

Out of 1500+ user activity reports, administrators would have a difficult time deploying high-level alert policies. As a result, AdminDroid has created a set of dominant default policies under each label to make administrators' jobs easier. You can view all the default alert policies 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?

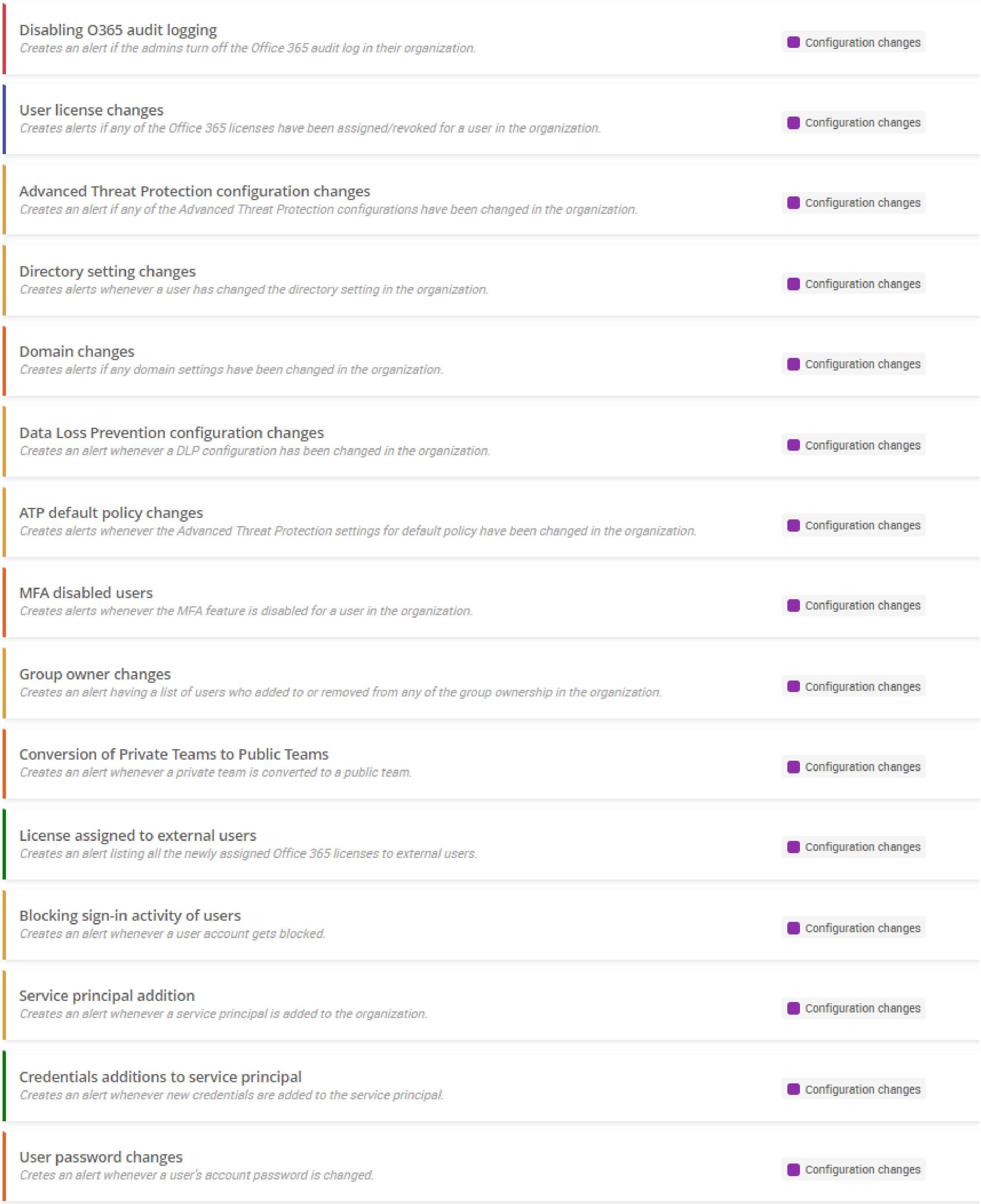
- You can select any one of the 75 default policies you want to deploy on the 'Policy templates' page.
- Click on Preview and deploy.
- You may change the alert settings, recipients, name, severity, label, etc., and deploy the policy.

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

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

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.



Disabling O365 audit logging
Creates an alert if the admins turn off the Office 365 audit log in their organization.
Configuration changes

User license changes
Creates alerts if any of the Office 365 licenses have been assigned/revoked for a user in the organization.
Configuration changes

Advanced Threat Protection configuration changes
Creates an alert if any of the Advanced Threat Protection configurations have been changed in the organization.
Configuration changes

Directory setting changes
Creates alerts whenever a user has changed the directory setting in the organization.
Configuration changes

Domain changes
Creates alerts if any domain settings have been changed in the organization.
Configuration changes

Data Loss Prevention configuration changes
Creates an alert whenever a DLP configuration has been changed in the organization.
Configuration changes

ATP default policy changes
Creates alerts whenever the Advanced Threat Protection settings for default policy have been changed in the organization.
Configuration changes

MFA disabled users
Creates alerts whenever the MFA feature is disabled for a user in the organization.
Configuration changes

Group owner changes
Creates an alert having a list of users who added to or removed from any of the group ownership in the organization.
Configuration changes

Conversion of Private Teams to Public Teams
Creates an alert whenever a private team is converted to a public team.
Configuration changes

License assigned to external users
Creates an alert listing all the newly assigned Office 365 licenses to external users.
Configuration changes

Blocking sign-in activity of users
Creates an alert whenever a user account gets blocked.
Configuration changes

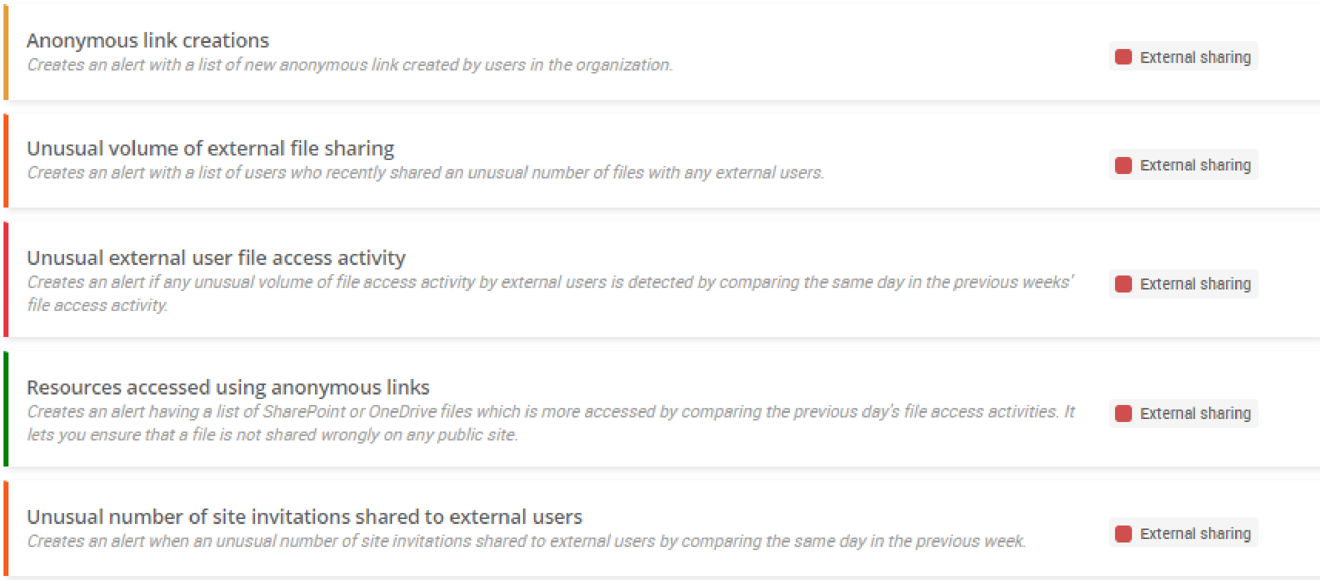
Service principal addition
Creates an alert whenever a service principal is added to the organization.
Configuration changes

Credentials additions to service principal
Creates an alert whenever new credentials are added to the service principal.
Configuration changes

User password changes
Cretes an alert whenever a user's account password is changed.
Configuration changes

External Sharing

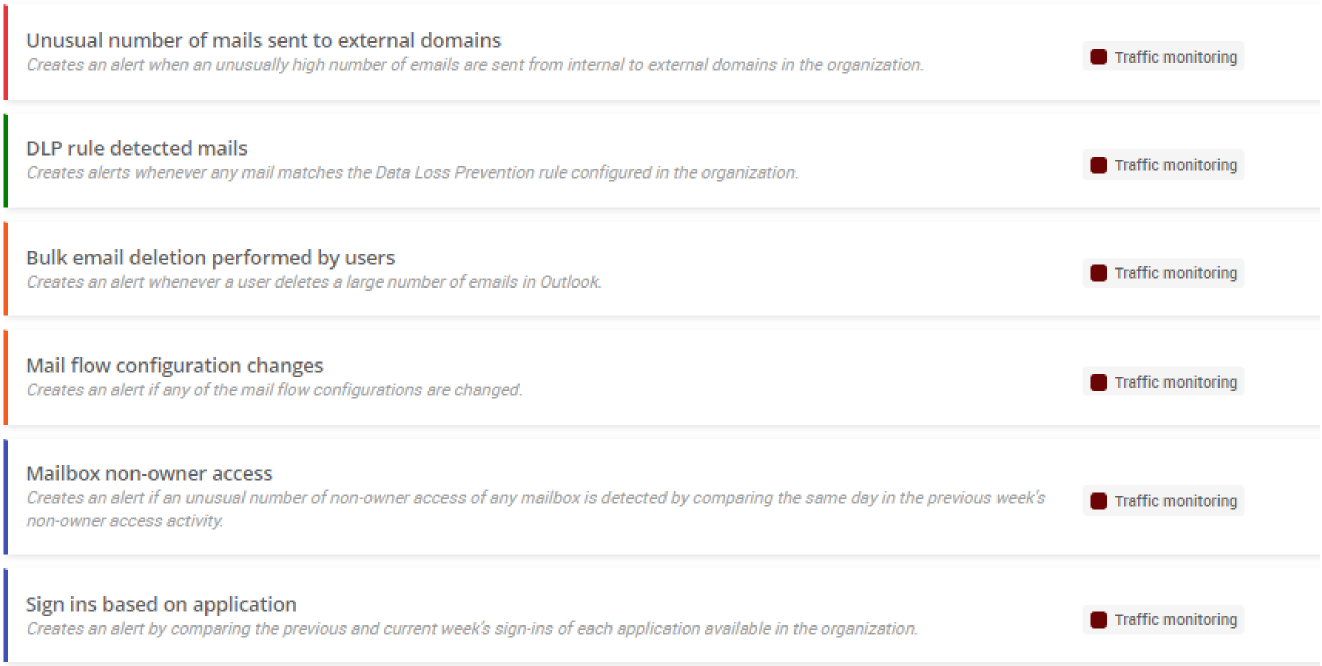
Activities related to external sharing, such as anonymous link creations, unusual volume of external file sharing and external user file access activities, resources accessed using anonymous links, and unusual number of site invitations shared to external users are detailed in these reports.



Anonymous link creations *Creates an alert with a list of new anonymous link created by users in the organization.*	🟥 External sharing
Unusual volume of external file sharing *Creates an alert with a list of users who recently shared an unusual number of files with any external users.*	🟥 External sharing
Unusual external user file access activity *Creates an alert if any unusual volume of file access activity by external users is detected by comparing the same day in the previous weeks' file access activity.*	🟥 External sharing
Resources accessed using anonymous links *Creates an alert having a list of SharePoint or OneDrive files which is more accessed by comparing the previous day's file access activities. It lets you ensure that a file is not shared wrongly on any public site.*	🟥 External sharing
Unusual number of site invitations shared to external users *Creates an alert when an unusual number of site invitations shared to external users by comparing the same day in the previous week.*	🟥 External sharing

Traffic Monitoring

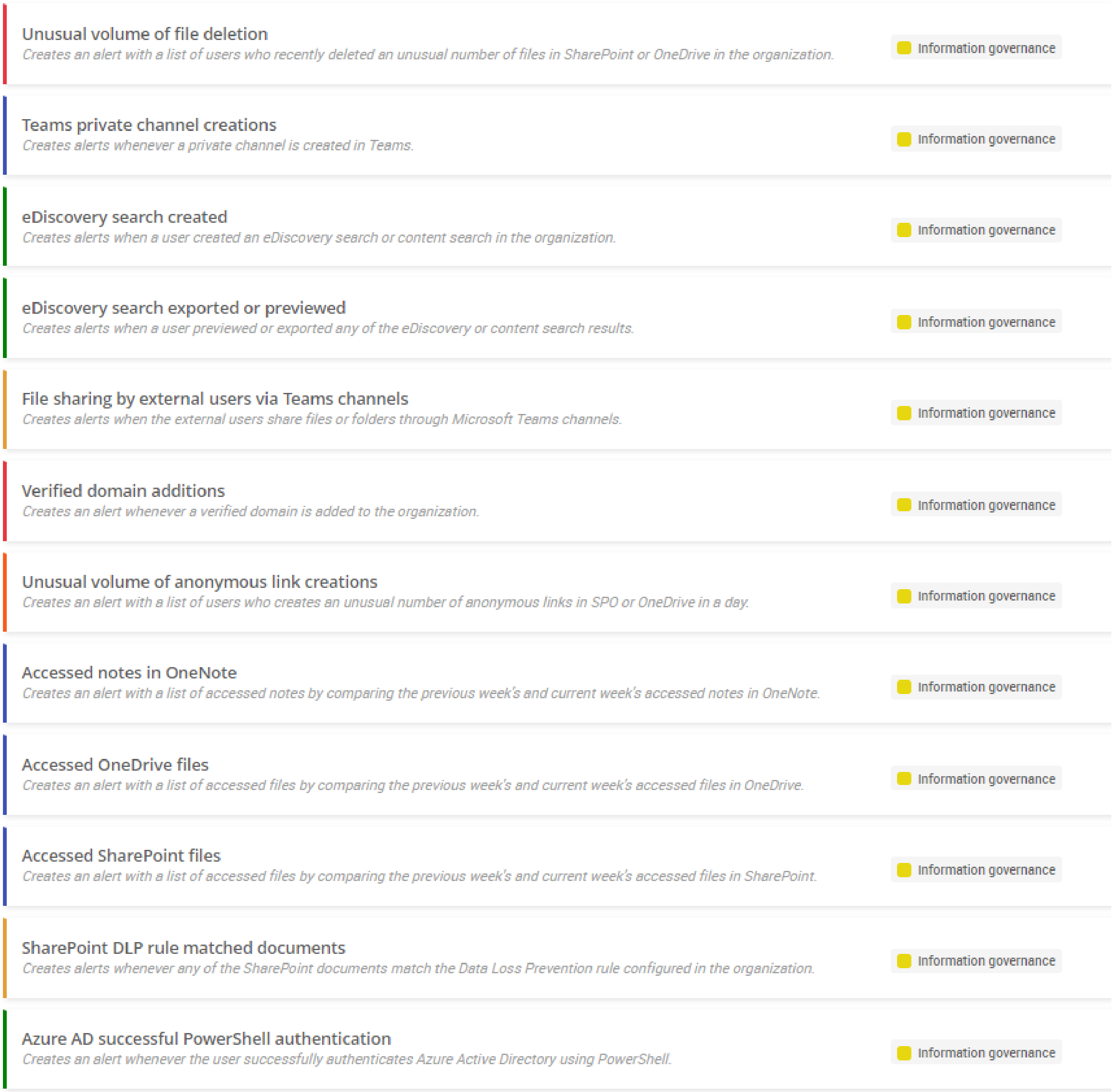
Reports on mail traffic enable admins to identify unusual email activities and follow appropriate procedures to reduce security risks and stay in compliance. Events related to traffic monitoring such as DLP rule matched mails, mail flow configuration changes, mailbox non–owner access, and sign-ins based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



Unusual number of mails sent to external domains *Creates an alert when an unusually high number of emails are sent from internal to external domains in the organization.*	🟥 Traffic monitoring
DLP rule detected mails *Creates alerts whenever any mail matches the Data Loss Prevention rule configured in the organization.*	🟥 Traffic monitoring
Bulk email deletion performed by users *Creates an alert whenever a user deletes a large number of emails in Outlook.*	🟥 Traffic monitoring
Mail flow configuration changes *Creates an alert if any of the mail flow configurations are changed.*	🟥 Traffic monitoring
Mailbox non-owner access *Creates an alert if an unusual number of non-owner access of any mailbox is detected by comparing the same day in the previous week's non-owner access activity.*	🟥 Traffic monitoring
Sign ins based on application *Creates an alert by comparing the previous and current week's sign-ins of each application available in the organization.*	🟥 Traffic monitoring

Information Governance

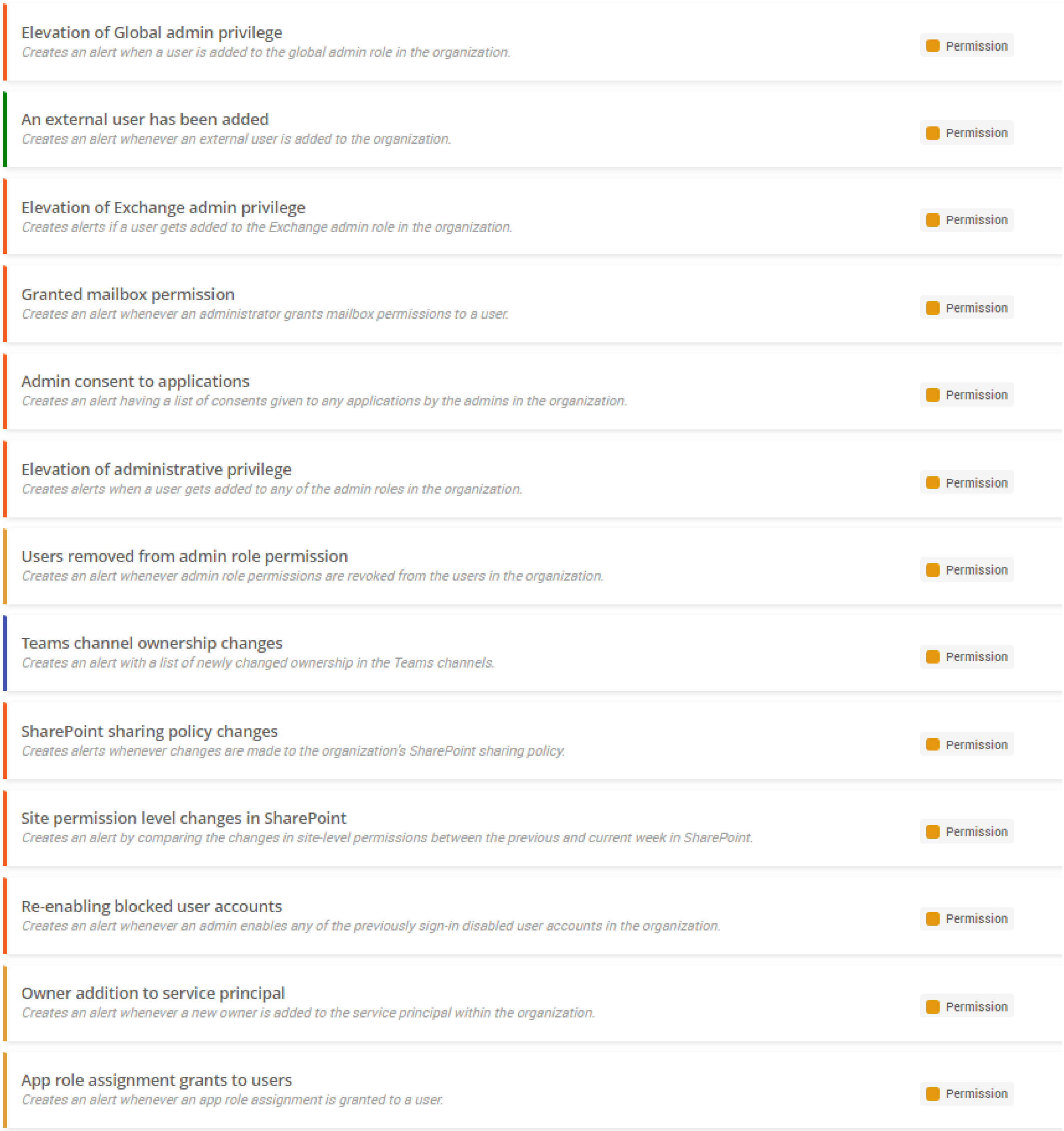
> Under information governance, admins can track events, such as unusual volume of file deletions, Teams private channel creations, eDiscovery search creations & exportations, accessed OneDrive files, SharePoint DLP rule matched documents, etc.



Unusual volume of file deletion *Creates an alert with a list of users who recently deleted an unusual number of files in SharePoint or OneDrive in the organization.*	🟨 Information governance
Teams private channel creations *Creates alerts whenever a private channel is created in Teams.*	🟨 Information governance
eDiscovery search created *Creates alerts when a user created an eDiscovery search or content search in the organization.*	🟨 Information governance
eDiscovery search exported or previewed *Creates alerts when a user previewed or exported any of the eDiscovery or content search results.*	🟨 Information governance
File sharing by external users via Teams channels *Creates alerts when the external users share files or folders through Microsoft Teams channels.*	🟨 Information governance
Verified domain additions *Creates an alert whenever a verified domain is added to the organization.*	🟨 Information governance
Unusual volume of anonymous link creations *Creates an alert with a list of users who creates an unusual number of anonymous links in SPO or OneDrive in a day.*	🟨 Information governance
Accessed notes in OneNote *Creates an alert with a list of accessed notes by comparing the previous week's and current week's accessed notes in OneNote.*	🟨 Information governance
Accessed OneDrive files *Creates an alert with a list of accessed files by comparing the previous week's and current week's accessed files in OneDrive.*	🟨 Information governance
Accessed SharePoint files *Creates an alert with a list of accessed files by comparing the previous week's and current week's accessed files in SharePoint.*	🟨 Information governance
SharePoint DLP rule matched documents *Creates alerts whenever any of the SharePoint documents match the Data Loss Prevention rule configured in the organization.*	🟨 Information governance
Azure AD successful PowerShell authentication *Creates an alert whenever the user successfully authenticates Azure Active Directory using PowerShell.*	🟨 Information governance

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

An external user has been added
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

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

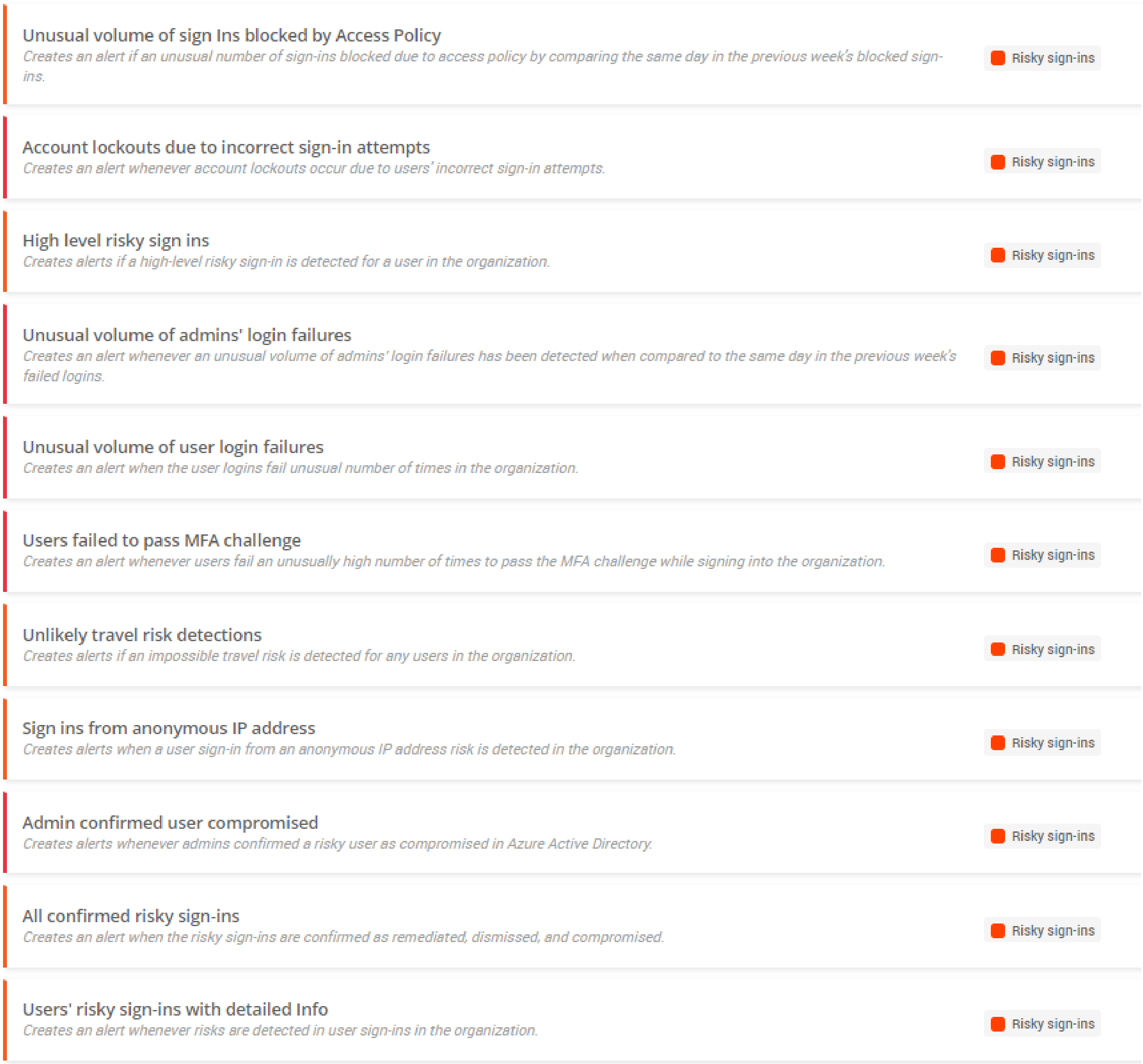
Re-enabling blocked user accounts
Creates an alert whenever an admin enables any of the previously sign-in disabled user accounts in the organization.
Permission

Owner addition to service principal
Creates an alert whenever a new owner is added to the service principal within the organization.
Permission

App role assignment grants to users
Creates an alert whenever an app role assignment is granted to a user.
Permission

Risky Sign-ins

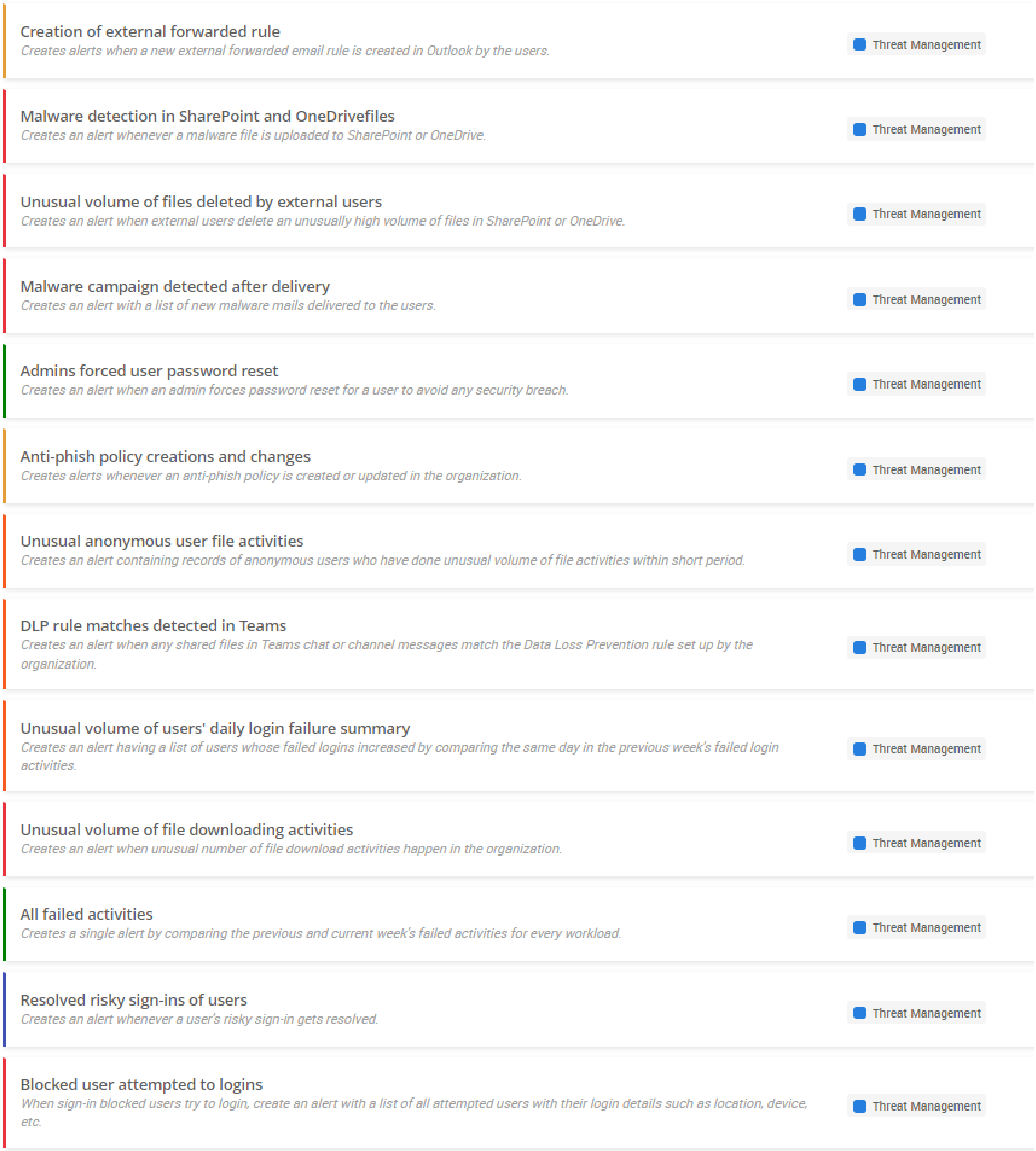
Risky sign-in activities, such as an unusual volume of sign-ins blocked by access policies, an unusual volume of admin login failures, sign-ins from anonymous IP addresses, and all failed activities are listed in this report.



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.



Creation of external forwarded rule
Creates alerts when a new external forwarded email rule is created in Outlook by the users.
Threat Management

Malware detection in SharePoint and OneDrivefiles
Creates an alert whenever a malware file is uploaded to SharePoint or OneDrive.
Threat Management

Unusual volume of files deleted by external users
Creates an alert when external users delete an unusually high volume of files in SharePoint or OneDrive.
Threat Management

Malware campaign detected after delivery
Creates an alert with a list of new malware mails delivered to the users.
Threat Management

Admins forced user password reset
Creates an alert when an admin forces password reset for a user to avoid any security breach.
Threat Management

Anti-phish policy creations and changes
Creates alerts whenever an anti-phish policy is created or updated in the organization.
Threat Management

Unusual anonymous user file activities
Creates an alert containing records of anonymous users who have done unusual volume of file activities within short period.
Threat Management

DLP rule matches detected in Teams
Creates an alert when any shared files in Teams chat or channel messages match the Data Loss Prevention rule set up by the organization.
Threat Management

Unusual volume of users' daily login failure summary
Creates an alert having a list of users whose failed logins increased by comparing the same day in the previous week's failed login activities.
Threat Management

Unusual volume of file downloading activities
Creates an alert when unusual number of file download activities happen in the organization.
Threat Management

All failed activities
Creates a single alert by comparing the previous and current week's failed activities for every workload.
Threat Management

Resolved risky sign-ins of users
Creates an alert whenever a user's risky sign-in gets resolved.
Threat Management

Blocked user attempted to logins
When sign-in blocked users try to login, create an alert with a list of all attempted users with their login details such as location, device, etc.
Threat Management

Customized Alert policies

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

AdminDroid comes with three types of alerting mechanism to identify new risks, detect unusual activities, and compare activity trends.

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.

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 Office 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 made by someone who is not the authorized owner of the account. 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 refers to fine-tuned alerting, triggered by specified attributes that allow targeted alerts instead of org-wide ones.

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

Explore Advanced Customization

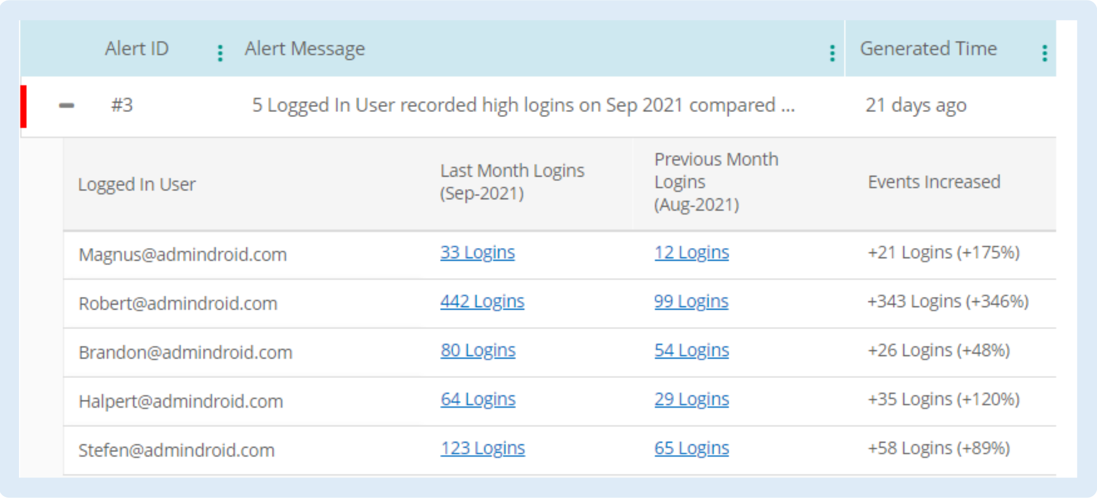
Reporting Use Cases:

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.

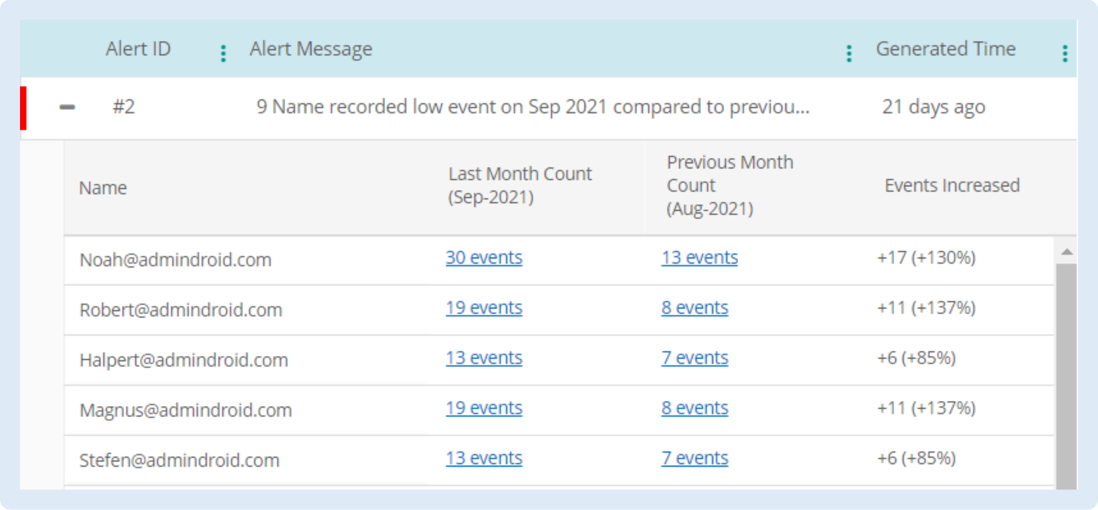


Alert ID	Alert Message	Generated Time
#3	5 Logged In User recorded high logins on Sep 2021 compared ...	21 days ago

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.

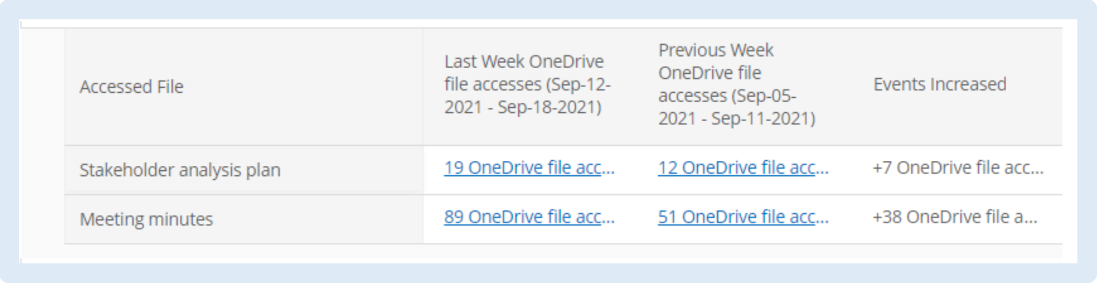


Alert ID	Alert Message	Generated Time
#2	9 Name recorded low event on Sep 2021 compared to previou...	21 days ago

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.



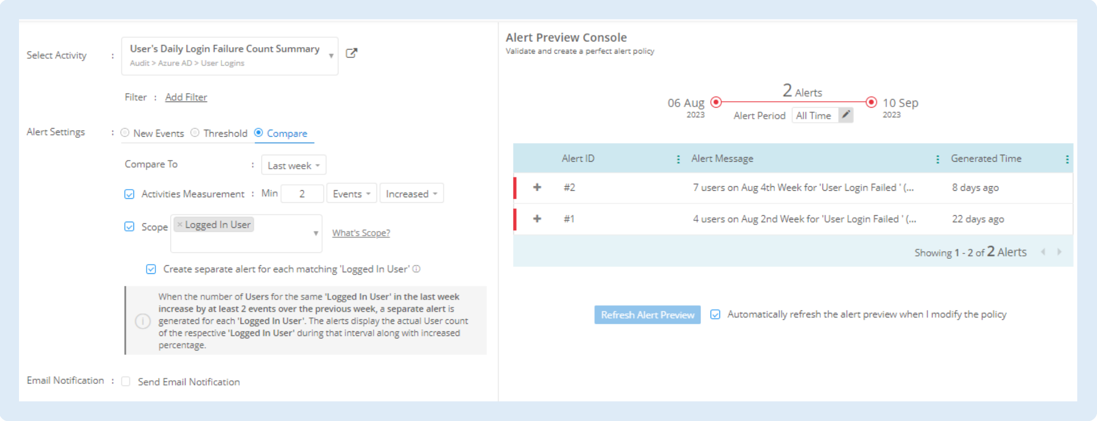
Accessed File	Last Week OneDrive file accesses (Sep-12-2021 - Sep-18-2021)	Previous Week OneDrive file accesses (Sep-05-2021 - Sep-11-2021)	Events Increased
Stakeholder analysis plan	19 OneDrive file acc...	12 OneDrive file acc...	+7 OneDrive file acc...
Meeting minutes	89 OneDrive file acc...	51 OneDrive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



Select Activity : User's Daily Login Failure Count Summary
Audit > Azure AD > User Logins

Filter : Add Filter

Alert Settings : ○ New Events ○ Threshold ● Compare

Compare To : Last week

☑ Activities Measurement : Min 2 Events Increased

☑ Scope × Logged In User What's Scope?

☑ Create separate alert for each matching 'Logged In User'

When the number of Users for the same **'Logged In User' in the last week increase by at least 2 events over the previous week, a separate alert is** generated for each **'Logged In User'**. The alerts display the actual User count of the respective **'Logged In User'** during that interval along with increased percentage.

Email Notification : □ Send Email Notification

Alert Preview Console

Validate and create a perfect alert policy

06 Aug 2023 — 2 Alerts — 10 Sep 2023

Alert Period All Time

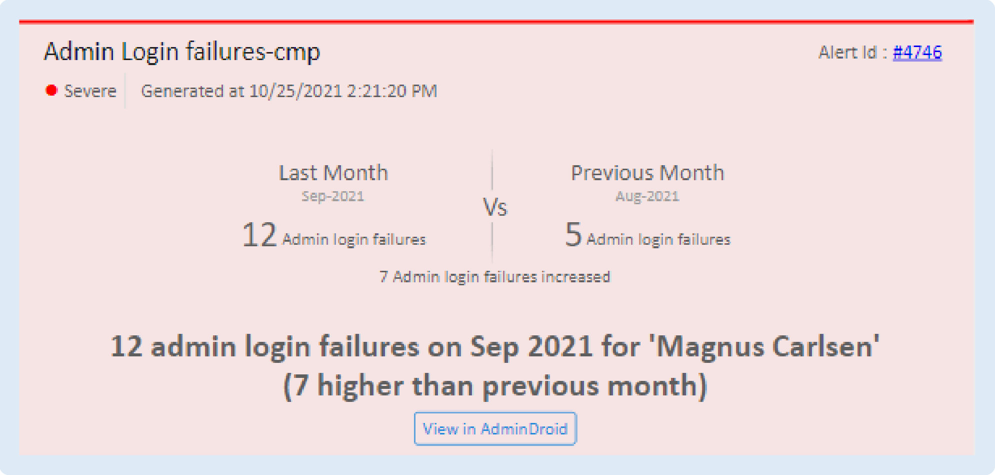
	Alert ID	Alert Message	Generated Time
+	#2	7 users on Aug 4th Week for 'User Login Failed ' (...	8 days ago
+	#1	4 users on Aug 2nd Week for 'User Login Failed ' (...	22 days ago

Showing **1 - 2** of **2** Alerts

☑ Automatically refresh the alert preview when I modify the policy

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.



Admin Login failures-cmp

Alert Id : #4746

● Severe | Generated at 10/25/2021 2:21:20 PM

Last Month
Sep-2021
12 Admin login failures

Vs

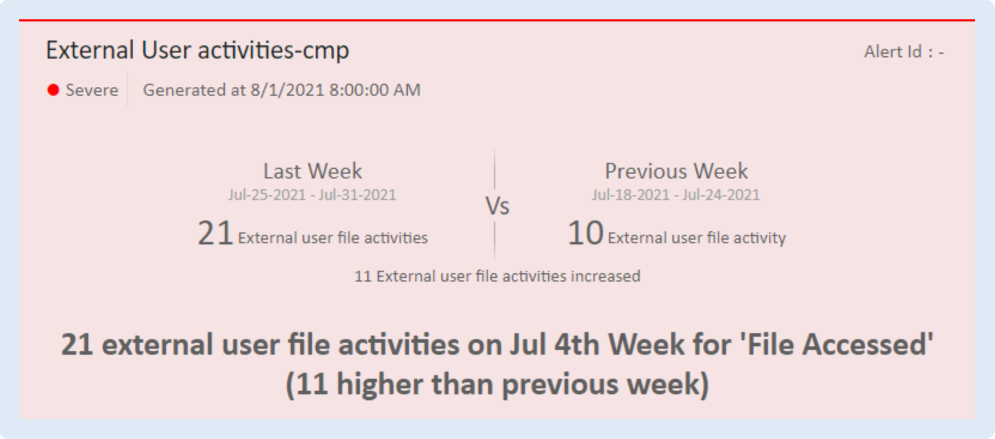
Previous Month
Aug-2021
5 Admin login failures

7 Admin login failures increased

12 admin login failures on Sep 2021 for 'Magnus Carlsen' (7 higher than previous month)

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.



External User activities-cmp

Alert Id : -

● Severe | Generated at 8/1/2021 8:00:00 AM

Last Week
Jul-25-2021 - Jul-31-2021
21 External user file activities

Vs

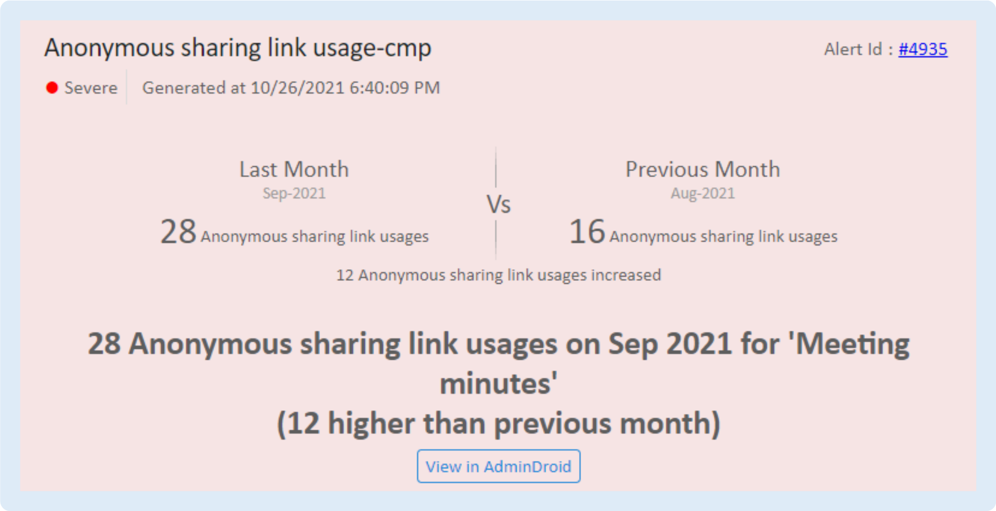
Previous Week
Jul-18-2021 - Jul-24-2021
10 External user file activity

11 External user file activities increased

21 external user file activities on Jul 4th Week for 'File Accessed' (11 higher than previous week)

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.



Anonymous sharing link usage-cmp

Alert Id : #4935

● Severe | Generated at 10/26/2021 6:40:09 PM

Last Month
Sep-2021
28 Anonymous sharing link usages

Vs

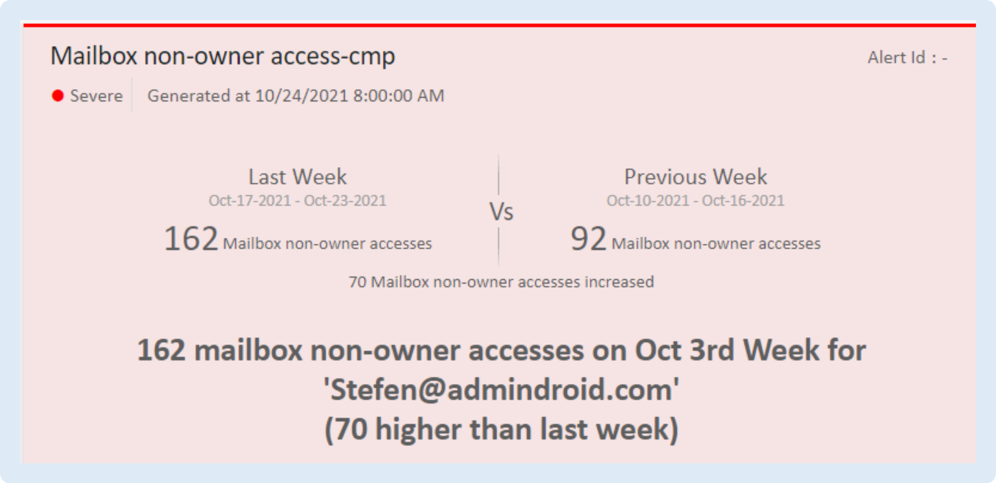
Previous Month
Aug-2021
16 Anonymous sharing link usages

12 Anonymous sharing link usages increased

28 Anonymous sharing link usages on Sep 2021 for 'Meeting minutes'
(12 higher than previous month)

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.



Mailbox non-owner access-cmp

Alert Id : -

● Severe | Generated at 10/24/2021 8:00:00 AM

Last Week
Oct-17-2021 - Oct-23-2021
162 Mailbox non-owner accesses

Vs

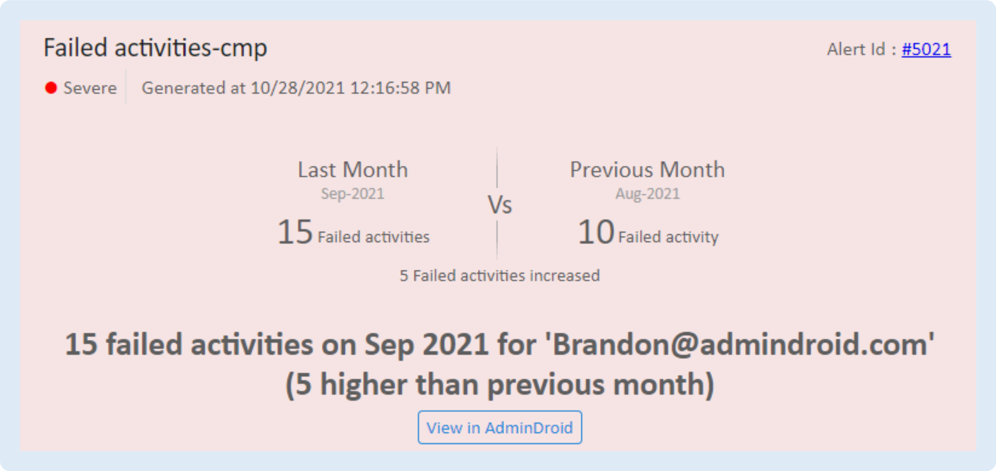
Previous Week
Oct-10-2021 - Oct-16-2021
92 Mailbox non-owner accesses

70 Mailbox non-owner accesses increased

162 mailbox non-owner accesses on Oct 3rd Week for 'Stefen@admindroid.com'
(70 higher than last week)

Failed activities:

If you notice failed operations occurring regularly in a specific Office 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.



Failed activities-cmp

Alert Id : #5021

● Severe | Generated at 10/28/2021 12:16:58 PM

Last Month
Sep-2021
15 Failed activities

Vs

Previous Month
Aug-2021
10 Failed activity

5 Failed activities increased

15 failed activities on Sep 2021 for 'Brandon@admindroid.com' (5 higher than previous month)

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.

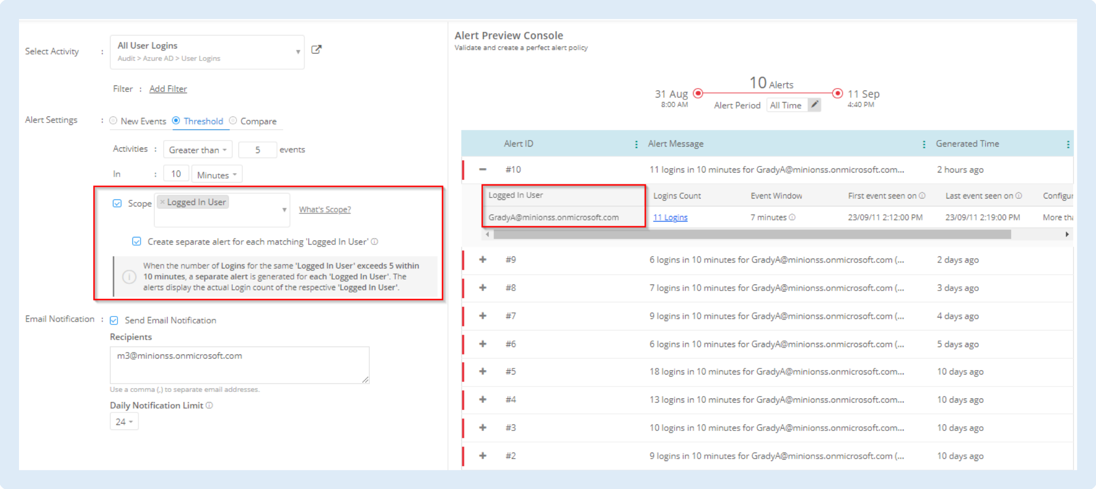
When Can We Use Scope?

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.



Select Activity : All User Logins
Audit > Azure AD > User Logins

Filter : Add Filter

Alert Settings : ○ New Events ● Threshold ○ Compare

Activities : Greater than 5 events

In : 10 Minutes

☑ Scope × Logged In User What's Scope?

☑ Create separate alert for each matching 'Logged In User'

When the number of Logins for the same 'Logged In User' exceeds 5 within 10 minutes, a separate alert is generated for each 'Logged In User'. The alerts display the actual Login count of the respective 'Logged In User'.

Email Notification : ☑ Send Email Notification

Recipients

m3@minionss.onmicrosoft.com

Use a comma (,) to separate email addresses.

Daily Notification Limit

24

Alert Preview Console
Validate and create a perfect alert policy

31 Aug 8:00 AM — 10 Alerts — 11 Sep 4:40 PM
Alert Period All Time

	Alert ID	Alert Message	Generated Time
−	#10	11 logins in 10 minutes for GradyA@minionss.onmicrosoft.com...	2 hours ago

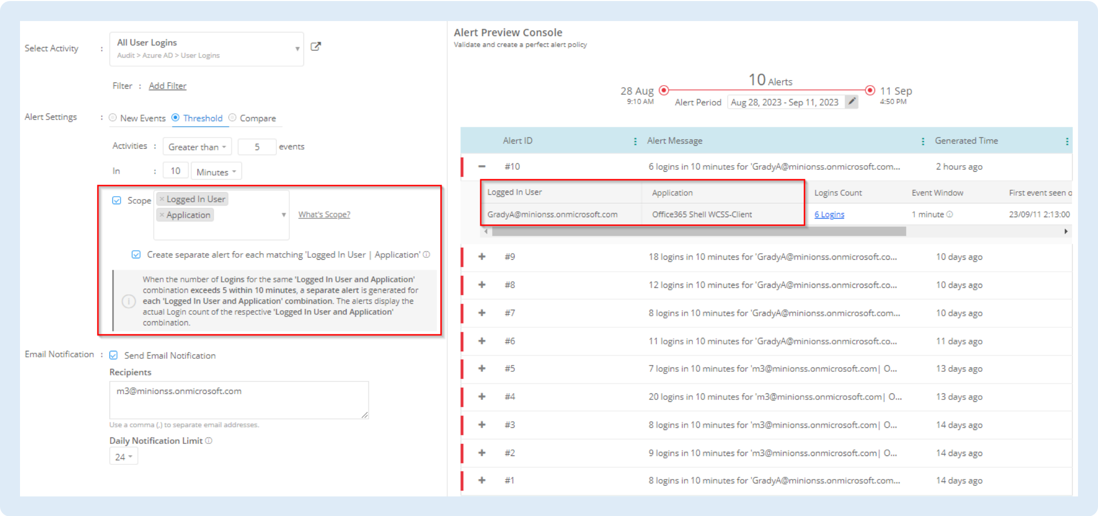
Logged In User	Logins Count	Event Window	First event seen on	Last event seen on	Configur
GradyA@minionss.onmicrosoft.com	11 Logins	7 minutes	23/09/11 2:12:00 PM	23/09/11 2:19:00 PM	More tha

	Alert ID	Alert Message	Generated Time
+	#9	6 logins in 10 minutes for GradyA@minionss.onmicrosoft.com (...	2 days ago
+	#8	7 logins in 10 minutes for GradyA@minionss.onmicrosoft.com (...	3 days ago
+	#7	9 logins in 10 minutes for GradyA@minionss.onmicrosoft.com (...	4 days ago
+	#6	6 logins in 10 minutes for GradyA@minionss.onmicrosoft.com (...	5 days ago
+	#5	18 logins in 10 minutes for GradyA@minionss.onmicrosoft.com...	10 days ago
+	#4	13 logins in 10 minutes for GradyA@minionss.onmicrosoft.com...	10 days ago
+	#3	10 logins in 10 minutes for GradyA@minionss.onmicrosoft.com...	10 days ago
+	#2	9 logins in 10 minutes for GradyA@minionss.onmicrosoft.com (...	10 days ago

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



Select Activity : All User Logins
Audit > Azure AD > User Logins

Filter : Add Filter

Alert Settings : ○ New Events ● Threshold ○ Compare

Activities : Greater than 5 events

In : 10 Minutes

☑ Scope × Logged In User × Application What's Scope?

☑ Create separate alert for each matching 'Logged In User | Application'

When the number of Logins for the same 'Logged In User and Application' combination exceeds 5 within 10 minutes, a separate alert is generated for each 'Logged In User and Application' combination. The alerts display the actual Login count of the respective 'Logged In User and Application' combination.

Email Notification : ☑ Send Email Notification

Recipients

m3@minionss.onmicrosoft.com

Use a comma (,) to separate email addresses.

Daily Notification Limit

24

Alert Preview Console
Validate and create a perfect alert policy

10 Alerts
28 Aug 9:10 AM — 11 Sep 4:50 PM
Alert Period Aug 28, 2023 - Sep 11, 2023

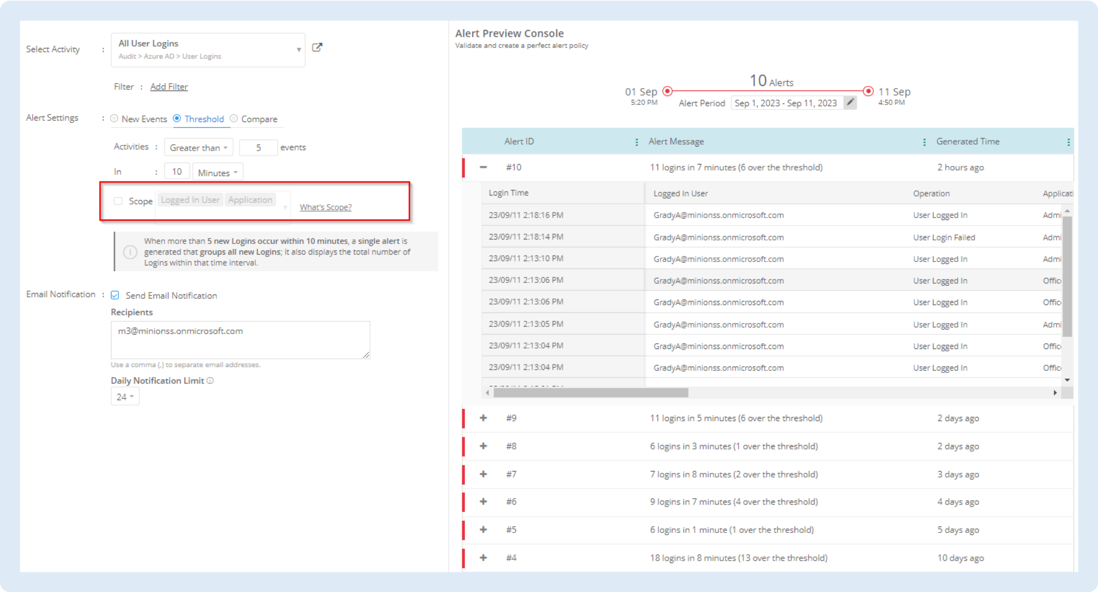
Alert ID	Alert Message	Generated Time
#10	6 logins in 10 minutes for 'GradyA@minionss.onmicrosoft.com...	2 hours ago

Logged In User	Application	Logins Count	Event Window	First event seen o
GradyA@minionss.onmicrosoft.com	Office365 Shell WCSS-Client	6 Logins	1 minute	23/09/11 2:13:00

Alert ID	Alert Message	Generated Time
#9	18 logins in 10 minutes for 'GradyA@minionss.onmicrosoft.co...	10 days ago
#8	12 logins in 10 minutes for 'GradyA@minionss.onmicrosoft.co...	10 days ago
#7	8 logins in 10 minutes for 'GradyA@minionss.onmicrosoft.com...	10 days ago
#6	11 logins in 10 minutes for 'GradyA@minionss.onmicrosoft.co...	11 days ago
#5	7 logins in 10 minutes for 'm3@minionss.onmicrosoft.com| O...	13 days ago
#4	20 logins in 10 minutes for 'm3@minionss.onmicrosoft.com| O...	13 days ago
#3	8 logins in 10 minutes for 'm3@minionss.onmicrosoft.com| O...	14 days ago
#2	9 logins in 10 minutes for 'm3@minionss.onmicrosoft.com| O...	14 days ago
#1	8 logins in 10 minutes for 'GradyA@minionss.onmicrosoft.com...	14 days ago

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.



Select Activity : All User Logins
Audit > Azure AD > User Logins

Filter : Add Filter

Alert Settings : ○ New Events ● Threshold ○ Compare

Activities : Greater than 5 events

In : 10 Minutes

□ Scope Logged In User Application What's Scope?

When more than 5 new Logins occur within 10 minutes, a single alert is generated that groups all new Logins; it also displays the total number of Logins within that time interval.

Email Notification : ☑ Send Email Notification

Recipients

m3@minionss.onmicrosoft.com

Use a comma (,) to separate email addresses.

Daily Notification Limit

24

Alert Preview Console
Validate and create a perfect alert policy

10 Alerts
01 Sep 5:20 PM — 11 Sep 4:50 PM
Alert Period Sep 1, 2023 - Sep 11, 2023

Alert ID	Alert Message	Generated Time
#10	11 logins in 7 minutes (6 over the threshold)	2 hours ago

Login Time	Logged In User	Operation	Applicati
23/09/11 2:18:16 PM	GradyA@minionss.onmicrosoft.com	User Logged In	Admi
23/09/11 2:18:14 PM	GradyA@minionss.onmicrosoft.com	User Login Failed	Admi
23/09/11 2:13:10 PM	GradyA@minionss.onmicrosoft.com	User Logged In	Admi
23/09/11 2:13:06 PM	GradyA@minionss.onmicrosoft.com	User Logged In	Offic
23/09/11 2:13:06 PM	GradyA@minionss.onmicrosoft.com	User Logged In	Offic
23/09/11 2:13:05 PM	GradyA@minionss.onmicrosoft.com	User Logged In	Admi
23/09/11 2:13:04 PM	GradyA@minionss.onmicrosoft.com	User Logged In	Offic
23/09/11 2:13:04 PM	GradyA@minionss.onmicrosoft.com	User Logged In	Offic

Alert ID	Alert Message	Generated Time
#9	11 logins in 5 minutes (6 over the threshold)	2 days ago
#8	6 logins in 3 minutes (1 over the threshold)	2 days ago
#7	7 logins in 8 minutes (2 over the threshold)	3 days ago
#6	9 logins in 7 minutes (4 over the threshold)	4 days ago
#5	6 logins in 1 minute (1 over the threshold)	5 days ago
#4	18 logins in 8 minutes (13 over the threshold)	10 days ago

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.

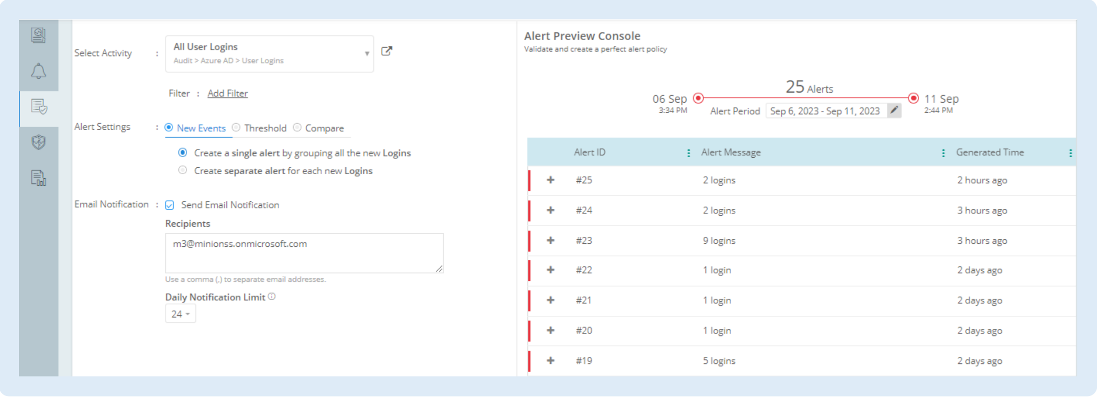
Separate Alert: Separate alerts feature is used to trigger individual alerts for every activity.

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.



Select Activity : All User Logins
Audit > Azure AD > User Logins

Filter : Add Filter

Alert Settings : ● New Events ○ Threshold ○ Compare

● Create a **single alert** by grouping all the new **Logins**
○ Create **separate alert** for each new **Logins**

Email Notification : ☑ Send Email Notification

Recipients
m3@minionss.onmicrosoft.com
Use a comma (,) to separate email addresses.

Daily Notification Limit ⓘ
24

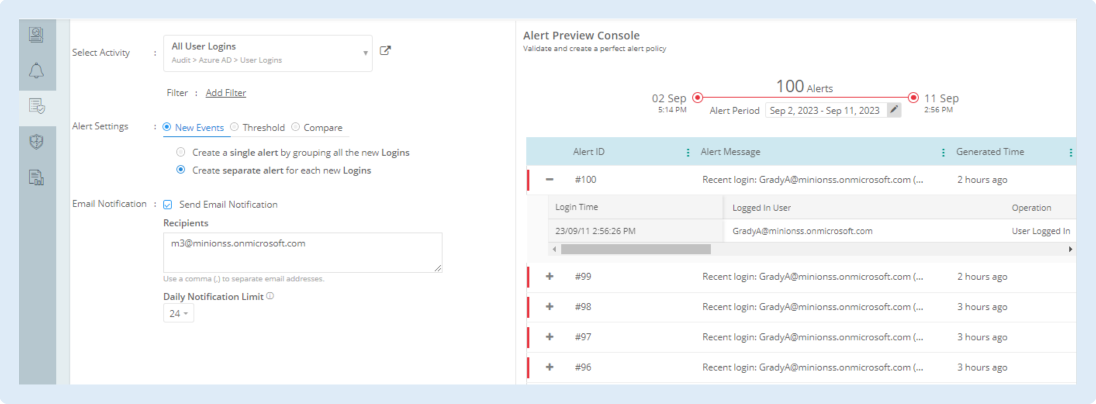
Alert Preview Console
Validate and create a perfect alert policy

06 Sep 3:34 PM — 25 Alerts — 11 Sep 2:44 PM
Alert Period Sep 6, 2023 - Sep 11, 2023

	Alert ID	Alert Message	Generated Time
+	#25	2 logins	2 hours ago
+	#24	2 logins	3 hours ago
+	#23	9 logins	3 hours ago
+	#22	1 login	2 days ago
+	#21	1 login	2 days ago
+	#20	1 login	2 days ago
+	#19	5 logins	2 days ago

- **Separate Alert:**

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



Select Activity : All User Logins
Audit > Azure AD > User Logins

Filter : Add Filter

Alert Settings : ● New Events ○ Threshold ○ Compare

○ Create a **single alert** by grouping all the new **Logins**
● Create **separate alert** for each new **Logins**

Email Notification : ☑ Send Email Notification

Recipients
m3@minionss.onmicrosoft.com
Use a comma (,) to separate email addresses.

Daily Notification Limit ⓘ
24

Alert Preview Console
Validate and create a perfect alert policy

02 Sep 5:14 PM — 100 Alerts — 11 Sep 2:56 PM
Alert Period Sep 2, 2023 - Sep 11, 2023

	Alert ID	Alert Message	Generated Time
−	#100	Recent login: GradyA@minionss.onmicrosoft.com (...	2 hours ago

Login Time	Logged In User	Operation
23/09/11 2:56:26 PM	GradyA@minionss.onmicrosoft.com	User Logged In

	Alert ID	Alert Message	Generated Time
+	#99	Recent login: GradyA@minionss.onmicrosoft.com (...	2 hours ago
+	#98	Recent login: GradyA@minionss.onmicrosoft.com (...	3 hours ago
+	#97	Recent login: GradyA@minionss.onmicrosoft.com (...	3 hours ago
+	#96	Recent login: GradyA@minionss.onmicrosoft.com (...	3 hours ago

How Do Single/Separate Alerts Work in Threshold Alert Type?

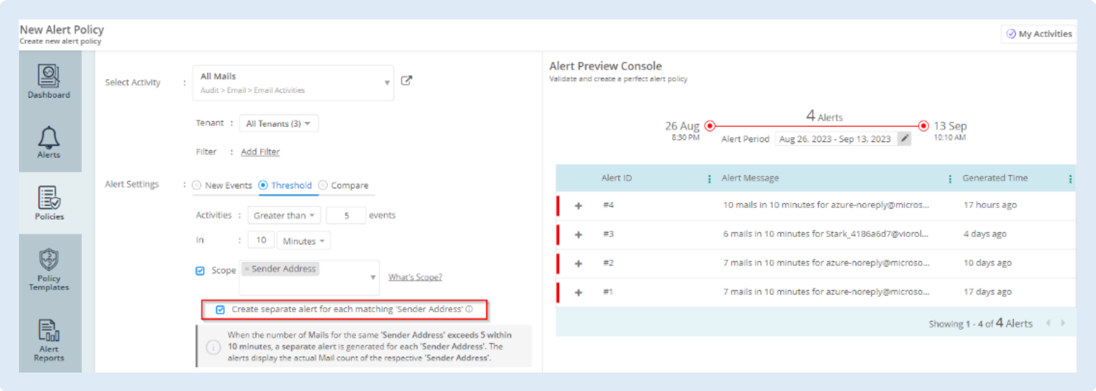
Let's say you want to create a threshold alert for all mail activities whenever a user sends 5 emails within a ten-minute window, you can refer to the **All Mails** report inside AdminDroid.

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.



New Alert Policy
Create new alert policy

Select Activity : All Mails (Audit > Email > Email Activities)

Tenant : All Tenants (3)

Filter : Add Filter

Alert Settings : ○ New Events ● Threshold ○ Compare

Activities : Greater than 5 events

In : 10 Minutes

☑ Scope × Sender Address What's Scope?

☑ Create separate alert for each matching 'Sender Address'

When the number of Mails for the same 'Sender Address' exceeds 5 within 10 minutes, a separate alert is generated for each 'Sender Address'. The alerts display the actual Mail count of the respective 'Sender Address'.

Alert Preview Console
Validate and create a perfect alert policy

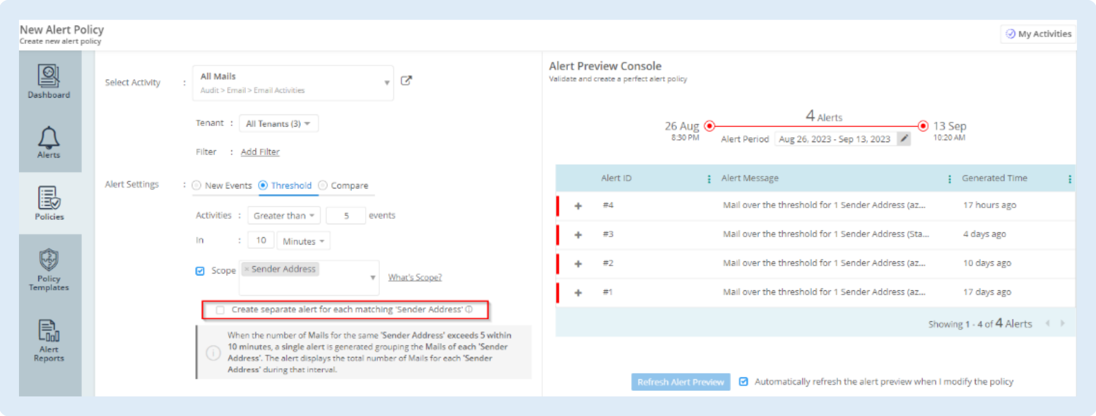
4 Alerts
26 Aug 8:30 PM – 13 Sep 10:10 AM
Alert Period Aug 26, 2023 - Sep 13, 2023

Alert ID	Alert Message	Generated Time
#4	10 mails in 10 minutes for azure-noreply@micros...	17 hours ago
#3	6 mails in 10 minutes for Stark_4186a6d7@viorol...	4 days ago
#2	7 mails in 10 minutes for azure-noreply@microso...	10 days ago
#1	7 mails in 10 minutes for azure-noreply@microso...	17 days ago

Showing 1 - 4 of 4 Alerts

▶ 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.



New Alert Policy
Create new alert policy

Select Activity : All Mails (Audit > Email > Email Activities)

Tenant : All Tenants (3)

Filter : Add Filter

Alert Settings : ○ New Events ● Threshold ○ Compare

Activities : Greater than 5 events

In : 10 Minutes

☑ Scope × Sender Address What's Scope?

□ Create separate alert for each matching 'Sender Address'

When the number of Mails for the same 'Sender Address' exceeds 5 within 10 minutes, a single alert is generated grouping the Mails of each 'Sender Address'. The alert displays the total number of Mails for each 'Sender Address' during that interval.

Alert Preview Console
Validate and create a perfect alert policy

4 Alerts
26 Aug 8:30 PM – 13 Sep 10:20 AM
Alert Period Aug 26, 2023 - Sep 13, 2023

Alert ID	Alert Message	Generated Time
#4	Mail over the threshold for 1 Sender Address (az...	17 hours ago
#3	Mail over the threshold for 1 Sender Address (Sta...	4 days ago
#2	Mail over the threshold for 1 Sender Address (az...	10 days ago
#1	Mail over the threshold for 1 Sender Address (az...	17 days ago

Showing 1 - 4 of 4 Alerts

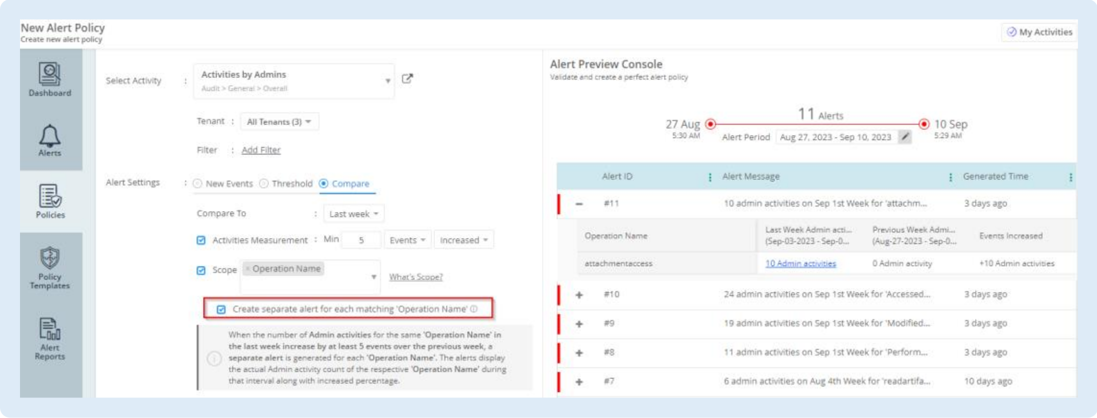
☑ Automatically refresh the alert preview when I modify the policy

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.



New Alert Policy
Create new alert policy

Select Activity : Activities by Admins
Audit > General > Overall
Tenant : All Tenants (3)
Filter : Add Filter
Alert Settings : ○ New Events ○ Threshold ● Compare
Compare To : Last week
☑ Activities Measurement : Min 5 Events Increased
☑ Scope × Operation Name What's Scope?
☑ Create separate alert for each matching 'Operation Name'

When the number of **Admin activities** for the same **'Operation Name'** in the last week increase by at least 5 events over the previous week, a separate alert is generated for each **'Operation Name'**. The alerts display the actual Admin activity count of the respective **'Operation Name'** during that interval along with increased percentage.

Alert Preview Console
Validate and create a perfect alert policy

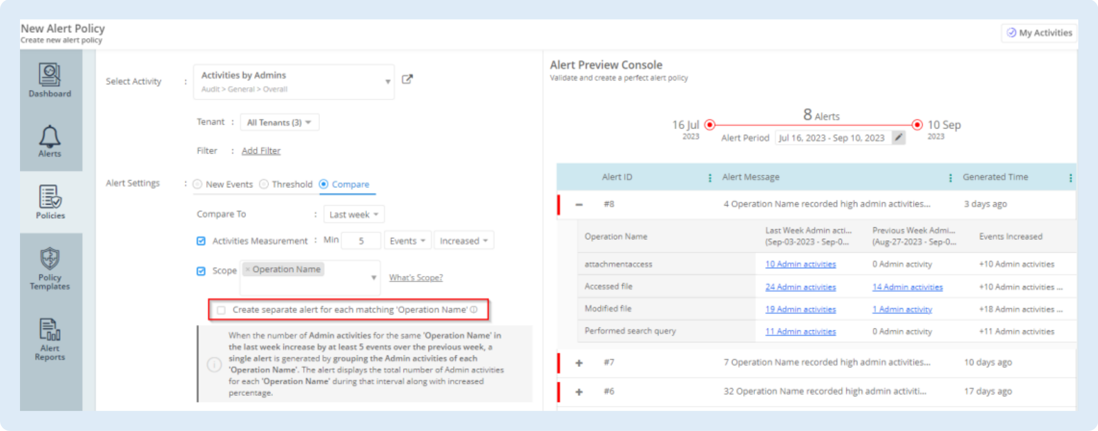
27 Aug 5:30 AM — 11 Alerts — 10 Sep 5:29 AM
Alert Period Aug 27, 2023 - Sep 10, 2023

	Alert ID	Alert Message	Generated Time
−	#11	10 admin activities on Sep 1st Week for 'attachm...	3 days ago

Operation Name	Last Week Admin acti... (Sep-03-2023 - Sep-0...	Previous Week Admi... (Aug-27-2023 - Sep-0...	Events Increased
attachmentaccess	10 Admin activities	0 Admin activity	+10 Admin activities

	Alert ID	Alert Message	Generated Time
+	#10	24 admin activities on Sep 1st Week for 'Accessed...	3 days ago
+	#9	19 admin activities on Sep 1st Week for 'Modified...	3 days ago
+	#8	11 admin activities on Sep 1st Week for 'Perform...	3 days ago
+	#7	6 admin activities on Aug 4th Week for 'readartifa...	10 days ago

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



New Alert Policy
Create new alert policy

Select Activity : Activities by Admins
Audit > General > Overall
Tenant : All Tenants (3)
Filter : Add Filter
Alert Settings : ○ New Events ○ Threshold ● Compare
Compare To : Last week
☑ Activities Measurement : Min 5 Events Increased
☑ Scope × Operation Name What's Scope?
□ Create separate alert for each matching 'Operation Name'

When the number of **Admin activities** for the same **'Operation Name'** in the last week increase by at least 5 events over the previous week, a single alert is generated by grouping the Admin activities of each 'Operation Name'. The alert displays the total number of Admin activities for each **'Operation Name'** during that interval along with increased percentage.

Alert Preview Console
Validate and create a perfect alert policy

16 Jul 2023 — 8 Alerts — 10 Sep 2023
Alert Period Jul 16, 2023 - Sep 10, 2023

	Alert ID	Alert Message	Generated Time
−	#8	4 Operation Name recorded high admin activities...	3 days ago

Operation Name	Last Week Admin acti... (Sep-03-2023 - Sep-0...	Previous Week Admi... (Aug-27-2023 - Sep-0...	Events Increased
attachmentaccess	10 Admin activities	0 Admin activity	+10 Admin activities
Accessed file	24 Admin activities	14 Admin activities	+10 Admin activities ...
Modified file	19 Admin activities	1 Admin activity	+18 Admin activities ...
Performed search query	11 Admin activities	0 Admin activity	+11 Admin activities

	Alert ID	Alert Message	Generated Time
+	#7	7 Operation Name recorded high admin activities...	10 days ago
+	#6	32 Operation Name recorded high admin activiti...	17 days ago

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.

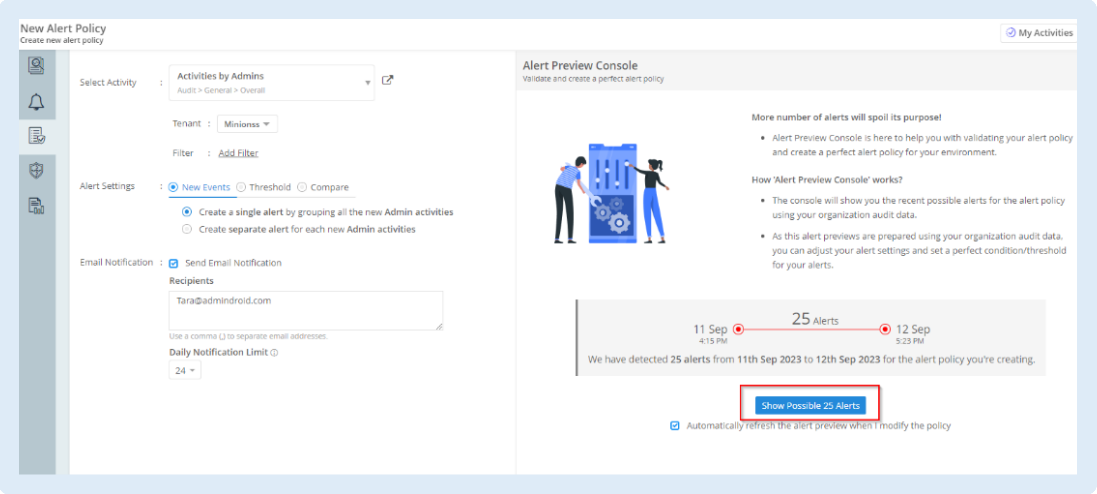
You may alter your alert settings and establish a perfect condition/threshold for your alerts since this alert preview is based entirely on your organization's audit data.

> 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.



New Alert Policy
Create new alert policy

Select Activity : Activities by Admins
Audit > General > Overall

Tenant : Minionss

Filter : Add Filter

Alert Settings : ● New Events ○ Threshold ○ Compare

● Create a **single alert** by grouping all the new **Admin activities**
○ Create **separate alert** for each new **Admin activities**

Email Notification : ☑ Send Email Notification

Recipients
Tara@admindroid.com
Use a comma (,) to separate email addresses.

Daily Notification Limit
24

Alert Preview Console
Validate and create a perfect alert policy

More number of alerts will spoil its purpose!

- Alert Preview Console is here to help you with validating your alert policy and create a perfect alert policy for your environment.

How 'Alert Preview Console' works?

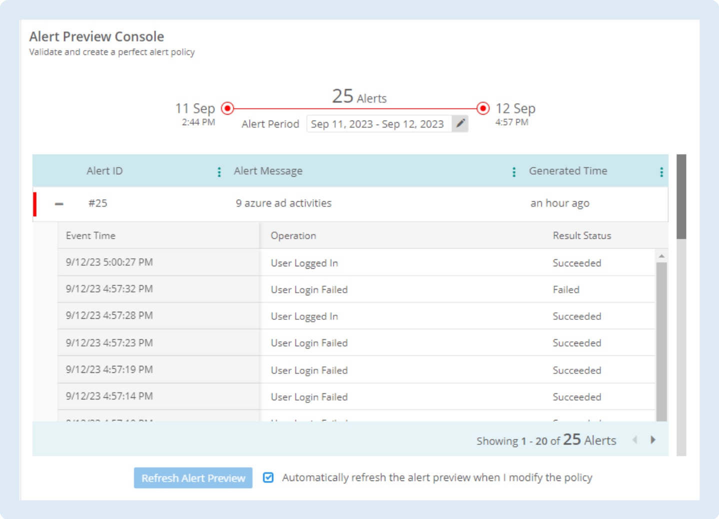
- The console will show you the recent possible alerts for the alert policy using your organization audit data.
- As this alert previews are prepared using your organization audit data, you can adjust your alert settings and set a perfect condition/threshold for your alerts.

11 Sep 4:15 PM — 25 Alerts — 12 Sep 5:23 PM

We have detected **25 alerts** from **11th Sep 2023** to **12th Sep 2023** for the alert policy you're creating.

☑ Automatically refresh the alert preview when I modify the policy

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.



Alert Preview Console
Validate and create a perfect alert policy

11 Sep 2:44 PM — 25 Alerts — 12 Sep 4:57 PM

Alert Period Sep 11, 2023 - Sep 12, 2023

Alert ID	Alert Message	Generated Time
#25	9 azure ad activities	an hour ago

Event Time	Operation	Result Status
9/12/23 5:00:27 PM	User Logged In	Succeeded
9/12/23 4:57:32 PM	User Login Failed	Failed
9/12/23 4:57:28 PM	User Logged In	Succeeded
9/12/23 4:57:23 PM	User Login Failed	Succeeded
9/12/23 4:57:19 PM	User Login Failed	Succeeded
9/12/23 4:57:14 PM	User Login Failed	Succeeded

Showing **1 - 20** of 25 Alerts

☑ Automatically refresh the alert preview when I modify the policy

ENGAGE

With AdminDroid, you can engage in three different ways.

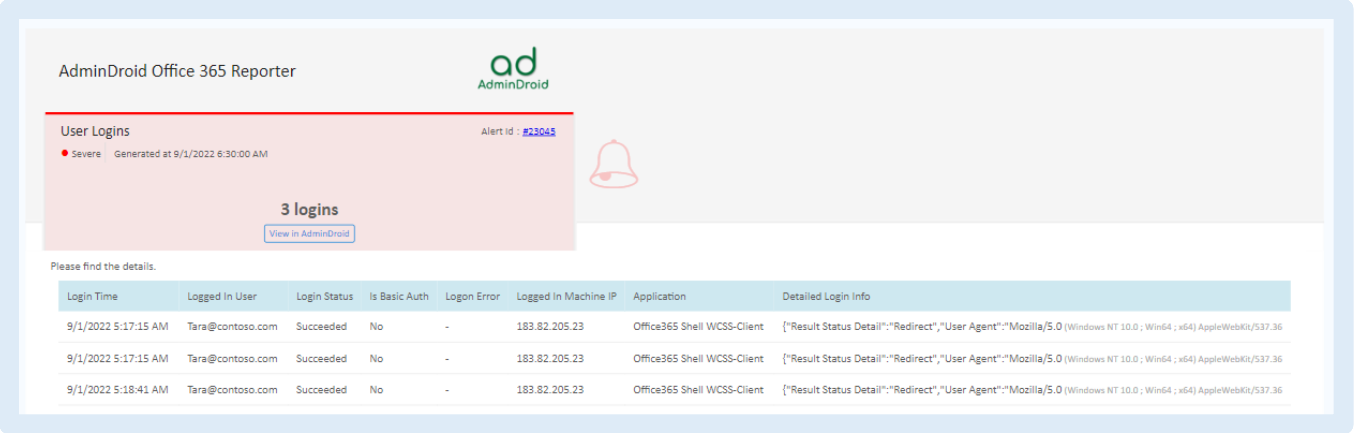
These are the ways you can engage via

- Emails
- Alert Reports
- Alert Dashboard

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.



AdminDroid Office 365 Reporter

User Logins

Alert Id : #23045

● Severe | Generated at 9/1/2022 6:30:00 AM

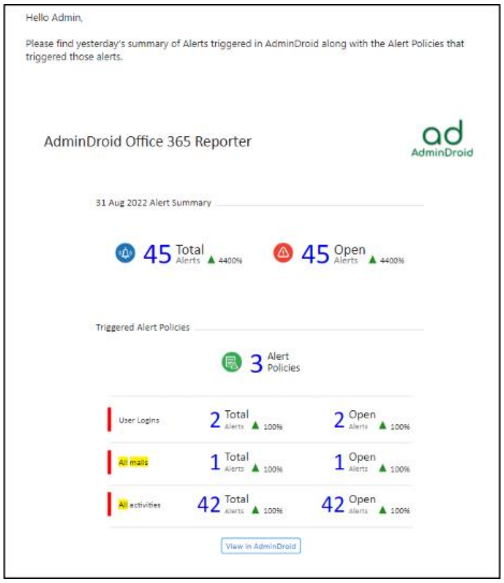
3 logins

View in AdminDroid

Please find the details.

Login Time	Logged In User	Login Status	Is Basic Auth	Logon Error	Logged In Machine IP	Application	Detailed Login Info
9/1/2022 5:17:15 AM	Tara@contoso.com	Succeeded	No	-	183.82.205.23	Office365 Shell WCSS-Client	{"Result Status Detail":"Redirect","User Agent":"Mozilla/5.0 (Windows NT 10.0 ; Win64 ; x64) AppleWebKit/537.36
9/1/2022 5:17:15 AM	Tara@contoso.com	Succeeded	No	-	183.82.205.23	Office365 Shell WCSS-Client	{"Result Status Detail":"Redirect","User Agent":"Mozilla/5.0 (Windows NT 10.0 ; Win64 ; x64) AppleWebKit/537.36
9/1/2022 5:18:41 AM	Tara@contoso.com	Succeeded	No	-	183.82.205.23	Office365 Shell WCSS-Client	{"Result Status Detail":"Redirect","User Agent":"Mozilla/5.0 (Windows NT 10.0 ; Win64 ; x64) AppleWebKit/537.36

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.



Hello Admin,

Please find yesterday's summary of Alerts triggered in AdminDroid along with the Alert Policies that triggered those alerts.

AdminDroid Office 365 Reporter

31 Aug 2022 Alert Summary

45 Total Alerts ▲ 4400%

45 Open Alerts ▲ 4400%

Triggered Alert Policies

3 Alert Policies

User Logins	2 Total Alerts ▲ 100%	2 Open Alerts ▲ 100%
All mails	1 Total Alerts ▲ 100%	1 Open Alerts ▲ 100%
All activities	42 Total Alerts ▲ 100%	42 Open Alerts ▲ 100%

View in AdminDroid

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

Daily Notification limit:

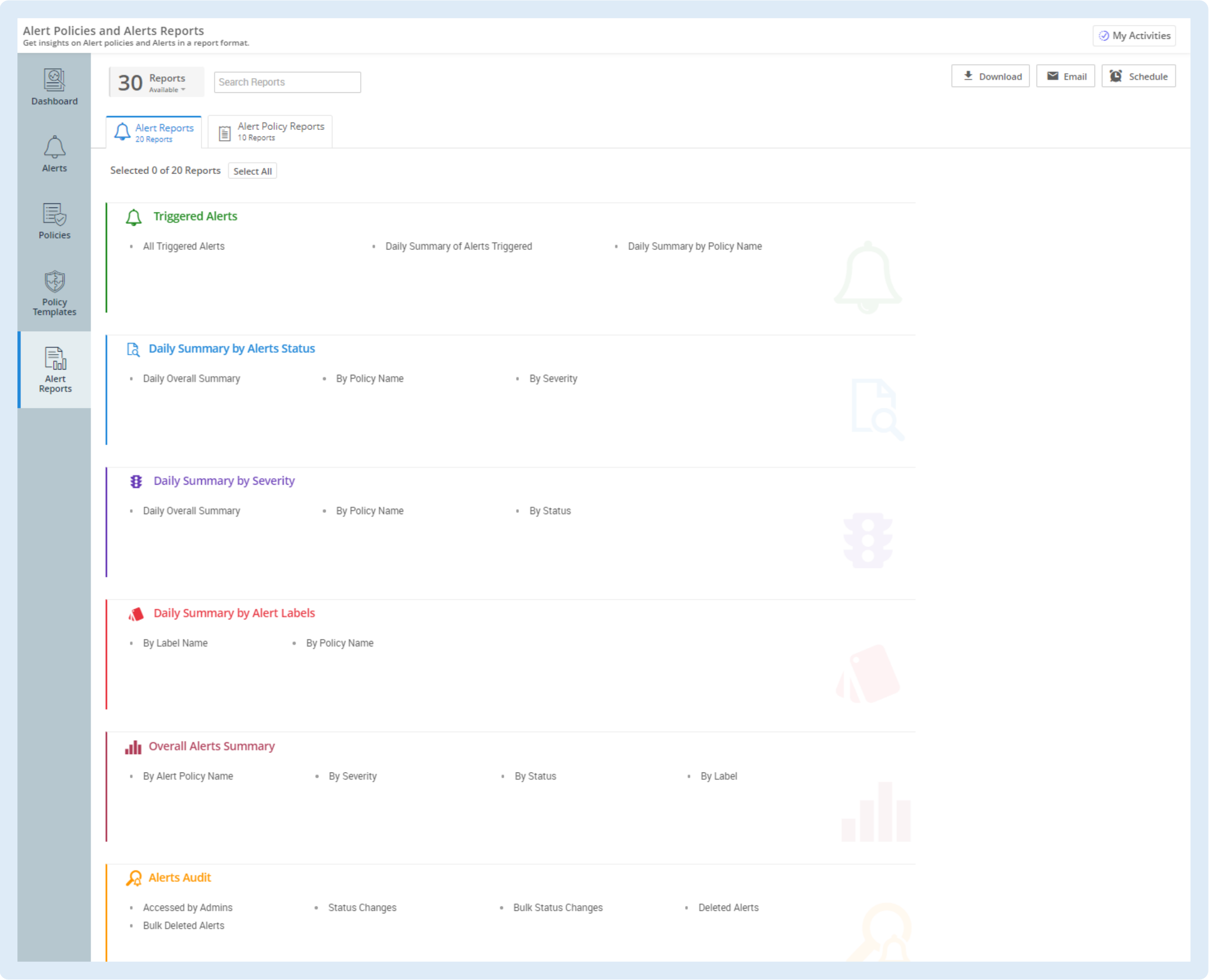
You can set how many email notifications you want to receive for each alert policy per day. However, it does not affect the number of alerts that can be generated.

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 Policies and Alerts Reports
Get insights on Alert policies and Alerts in a report format.

Selected 0 of 20 Reports

Triggered Alerts
- All Triggered Alerts
- Daily Summary of Alerts Triggered
- Daily Summary by Policy Name

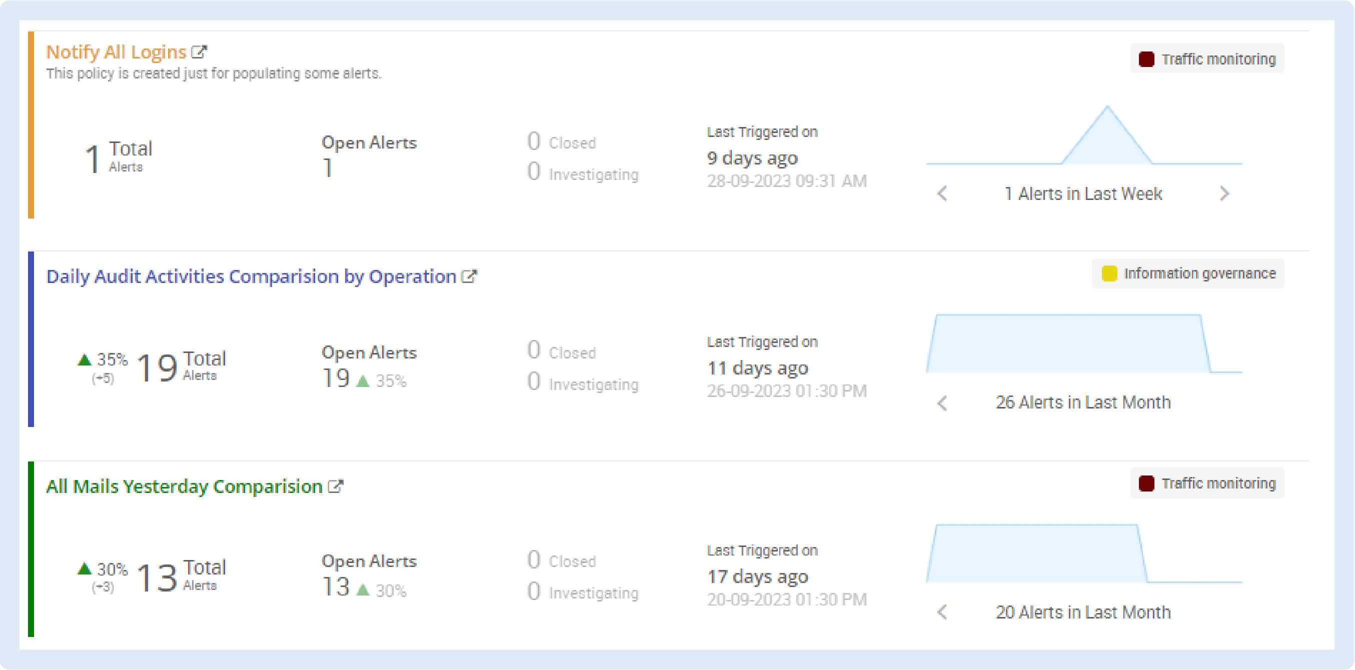
Daily Summary by Alerts Status
- Daily Overall Summary
- By Policy Name
- By Severity

Daily Summary by Severity
- Daily Overall Summary
- By Policy Name
- By Status

Daily Summary by Alert Labels
- By Label Name
- By Policy Name

Overall Alerts Summary
- By Alert Policy Name
- By Severity
- By Status
- By Label

Alerts Audit
- Accessed by Admins
- Status Changes
- Bulk Status Changes
- Deleted Alerts
- Bulk Deleted Alerts



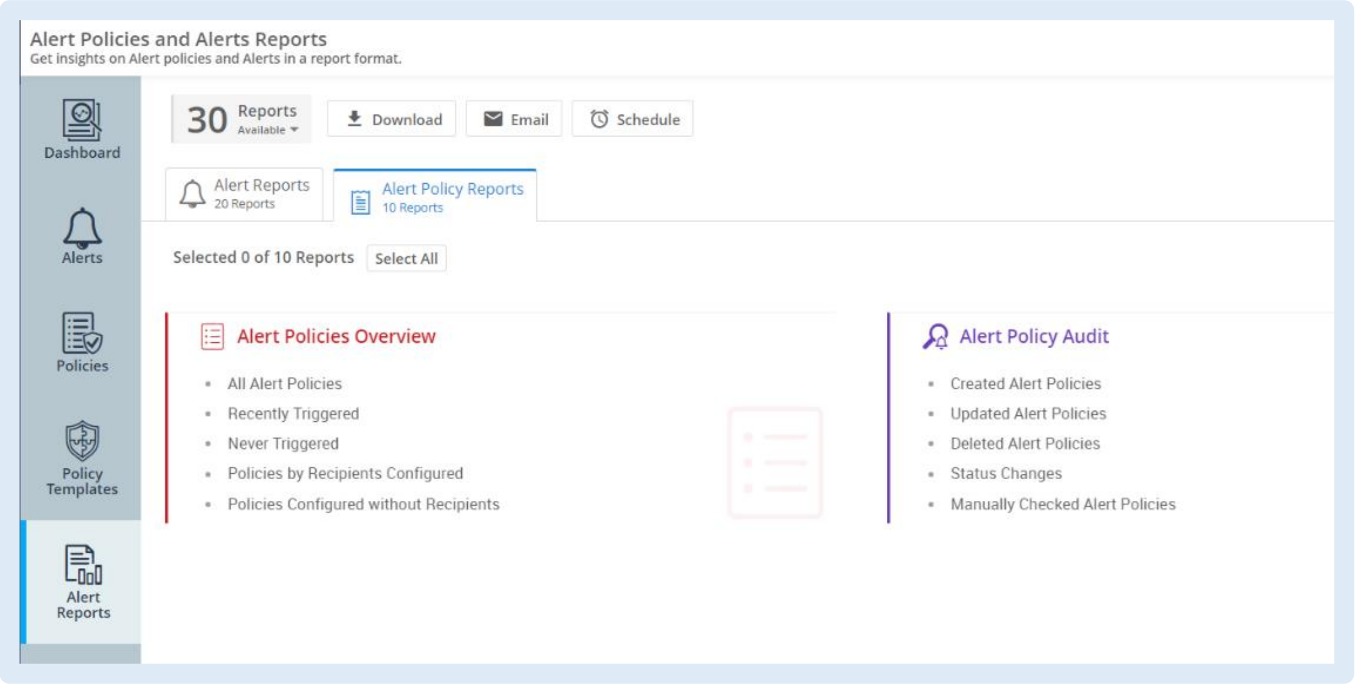
Notify All Logins
This policy is created just for populating some alerts.
🟥 Traffic monitoring
1 Total Alerts
Open Alerts 1
0 Closed
0 Investigating
Last Triggered on
9 days ago
28-09-2023 09:31 AM
1 Alerts in Last Week

Daily Audit Activities Comparision by Operation
🟨 Information governance
▲ 35% (+5) 19 Total Alerts
Open Alerts 19 ▲ 35%
0 Closed
0 Investigating
Last Triggered on
11 days ago
26-09-2023 01:30 PM
26 Alerts in Last Month

All Mails Yesterday Comparision
🟥 Traffic monitoring
▲ 30% (+3) 13 Total Alerts
Open Alerts 13 ▲ 30%
0 Closed
0 Investigating
Last Triggered on
17 days ago
20-09-2023 01:30 PM
20 Alerts in Last Month

Alert policy reports:

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



Alert Policies and Alerts Reports
Get insights on Alert policies and Alerts in a report format.

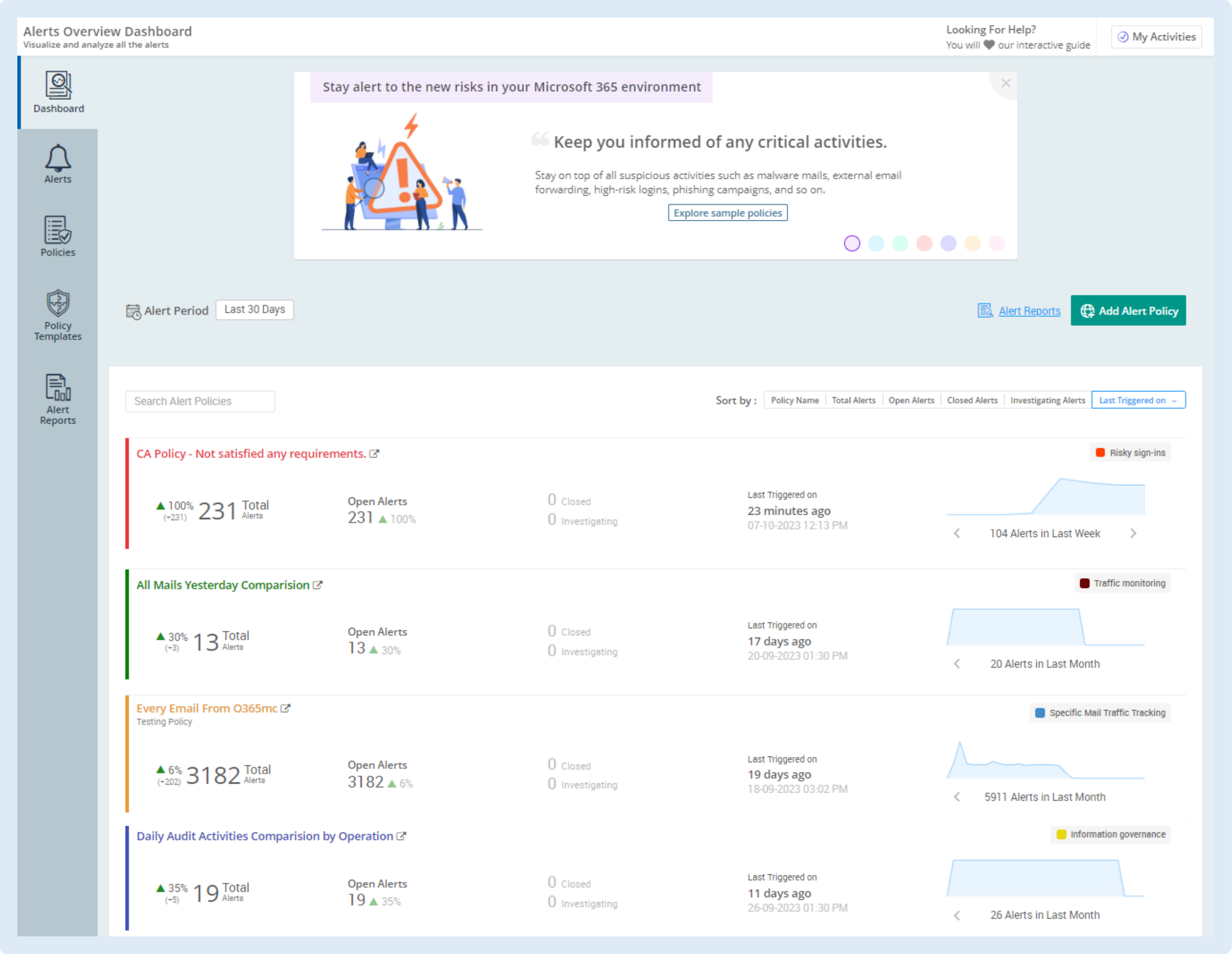
Selected 0 of 10 Reports Select All

Alert Policies Overview
- All Alert Policies
- Recently Triggered
- Never Triggered
- Policies by Recipients Configured
- Policies Configured without Recipients

Alert Policy Audit
- Created Alert Policies
- Updated Alert Policies
- Deleted Alert Policies
- Status Changes
- Manually Checked Alert Policies

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.



Alerts Overview Dashboard
Visualize and analyze all the alerts

Looking For Help?
You will ♥ our interactive guide

Stay alert to the new risks in your Microsoft 365 environment

Keep you informed of any critical activities.

Stay on top of all suspicious activities such as malware mails, external email forwarding, high-risk logins, phishing campaigns, and so on.

Alert Period: Last 30 Days

CA Policy - Not satisfied any requirements.
🟥 Risky sign-ins
▲100% (+231) 231 Total Alerts
Open Alerts 231 ▲ 100%
0 Closed
0 Investigating
Last Triggered on 23 minutes ago 07-10-2023 12:13 PM
104 Alerts in Last Week

All Mails Yesterday Comparision
🟥 Traffic monitoring
▲30% (+3) 13 Total Alerts
Open Alerts 13 ▲ 30%
0 Closed
0 Investigating
Last Triggered on 17 days ago 20-09-2023 01:30 PM
20 Alerts in Last Month

Every Email From O365mc
Testing Policy
🟦 Specific Mail Traffic Tracking
▲6% (+202) 3182 Total Alerts
Open Alerts 3182 ▲ 6%
0 Closed
0 Investigating
Last Triggered on 19 days ago 18-09-2023 03:02 PM
5911 Alerts in Last Month

Daily Audit Activities Comparision by Operation
🟨 Information governance
▲35% (+5) 19 Total Alerts
Open Alerts 19 ▲ 35%
0 Closed
0 Investigating
Last Triggered on 11 days ago 26-09-2023 01:30 PM
26 Alerts in Last Month

- ✓ 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.

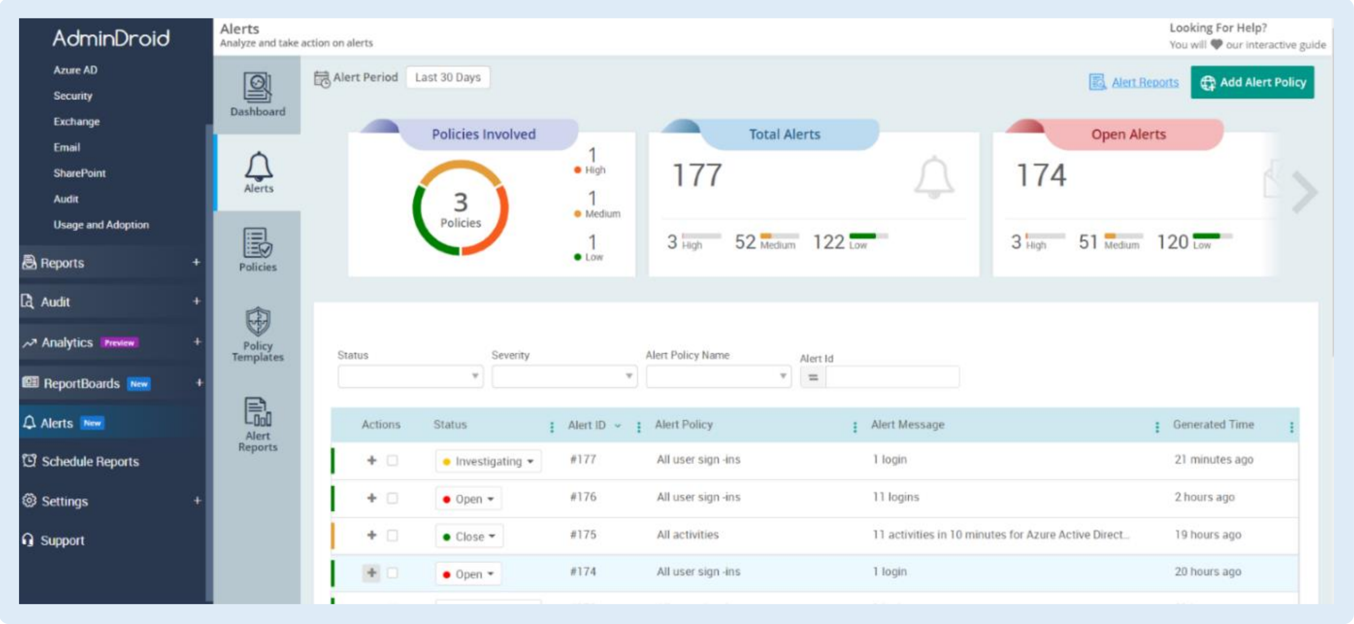
Here let’s see what are all the actions that can be taken on triggered alerts.

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**.

> Set alert status into open, closed, or investigating to resolve incidents quickly



Alerts
Analyze and take action on alerts

Alert Period: Last 30 Days

Policies Involved: 3 Policies — 1 High, 1 Medium, 1 Low

Total Alerts: 177 — 3 High, 52 Medium, 122 Low

Open Alerts: 174 — 3 High, 51 Medium, 120 Low

Status | Severity | Alert Policy Name | Alert Id =

Actions	Status	Alert ID	Alert Policy	Alert Message	Generated Time
+ □	● Investigating	#177	All user sign -ins	1 login	21 minutes ago
+ □	● Open	#176	All user sign -ins	11 logins	2 hours ago
+ □	● Close	#175	All activities	11 activities in 10 minutes for Azure Active Direct...	19 hours ago
+ □	● Open	#174	All user sign -ins	1 login	20 hours ago

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.

Usage & Adoption

Granular Delegation

Precise Auditing

Compliance Management

Robust Reporting

Actionable Insights

Explore >

AdminDroid

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 Microsoft 365 Reporter, visit below.

Live Demo Download

Connect with us

linkedin.com/company/admindroid/

facebook.com/admindroid

github.com/admindroid-community

reddit.com/r/AdminDroid/

youtube.com/admindroid

twitter.com/admiindroid

admindroid.com