Alert policies in Microsoft 365

Article • 04/15/2024 • 4 contributors

Feedback

In this article

You can use alert policies and the alert dashboard in the Microsoft Purview compliance portal or the Microsoft Defender portal to create alert policies and then view the alerts generated when users perform activities that match the conditions of an alert policy. There are several default alert policies that help you monitor activities such as assigning admin privileges in Exchange Online, malware attacks, phishing campaigns, and unusual levels of file deletions and external sharing.

Tip

Go to the **Default alert policies** section in this article for a list and description of the available alert policies.

Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered. There's also a **Alerts** page where you can view and filter alerts, set an alert status to help you manage alerts, and then dismiss alerts after you address or resolve the underlying incident.

Note

Alert policies are available in the following organizations:

- Microsoft 365 Enterprise.
- Office 365 Enterprise.
- Office 365 U.S. Government E1/F1/G1, E3/F3/G3, or E5/G5.

Advanced functionality is available only in the following organizations:

- E5/G5.

- E1/F1/G1 or E3/F3/G3 and one of the following add-on subscriptions:
  - Microsoft Defender for Office 365 Plan 2.
  - Microsoft 365 E5 Compliance.
  - E5 eDiscovery and Audit add-on.

Advanced functionality that requires E5/G5 or an add-on subscription is highlighted in this article.

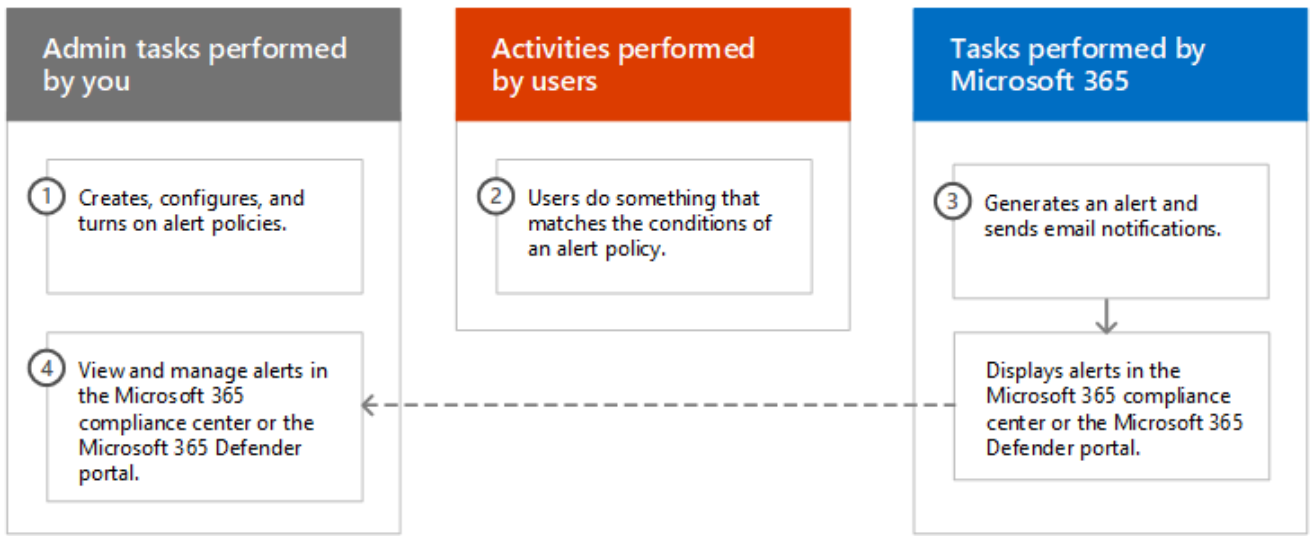
Alert policies are available in U.S. Government organizations (Office 365 GCC, GCC High, and DoD).

Tip

If you're not an E5 customer, use the 90-day Microsoft Purview solutions trial to explore how additional Purview capabilities can help your organization manage data security and compliance needs. Start now at the Microsoft Purview compliance portal trials hub. Learn details about signing up and trial terms.

How alert policies work

Here's a quick overview of how alert policies work and the alerts that are triggers when user or admin activity matches the conditions of an alert policy.



1. An admin in your organization creates, configures, and turns on an alert policy by using the **Alert policies** page in the compliance portal or the Microsoft Defender portal. You can also create alert policies by using the New-ProtectionAlert cmdlet in Security & Compliance PowerShell.

   To create alert policies, you have to be assigned the Manage Alerts role or the Organization Configuration role in the compliance portal or the Defender portal.

   Note

   It takes up to 24 hours after creating or updating an alert policy before alerts can be triggered by the policy. This is because the policy has to be synced to the alert detection engine.

2. A user performs an activity that matches the conditions of an alert policy. In the case of malware attacks, infected email messages sent to users in your organization trigger an alert.

3. Microsoft 365 generates an alert that's displayed on the **Alerts** page in compliance portal or Defender portal. Also, if email notifications are enabled for the alert policy, Microsoft sends a notification to a list of recipients. The alerts that an admin or other users can see that on the Alerts page is determined by the roles assigned to the user. For more information, see RBAC permissions required to view alerts.

4. An admin manages alerts in the Microsoft Purview compliance portal. Managing alerts consists of assigning an alert status to help track and manage any investigation.

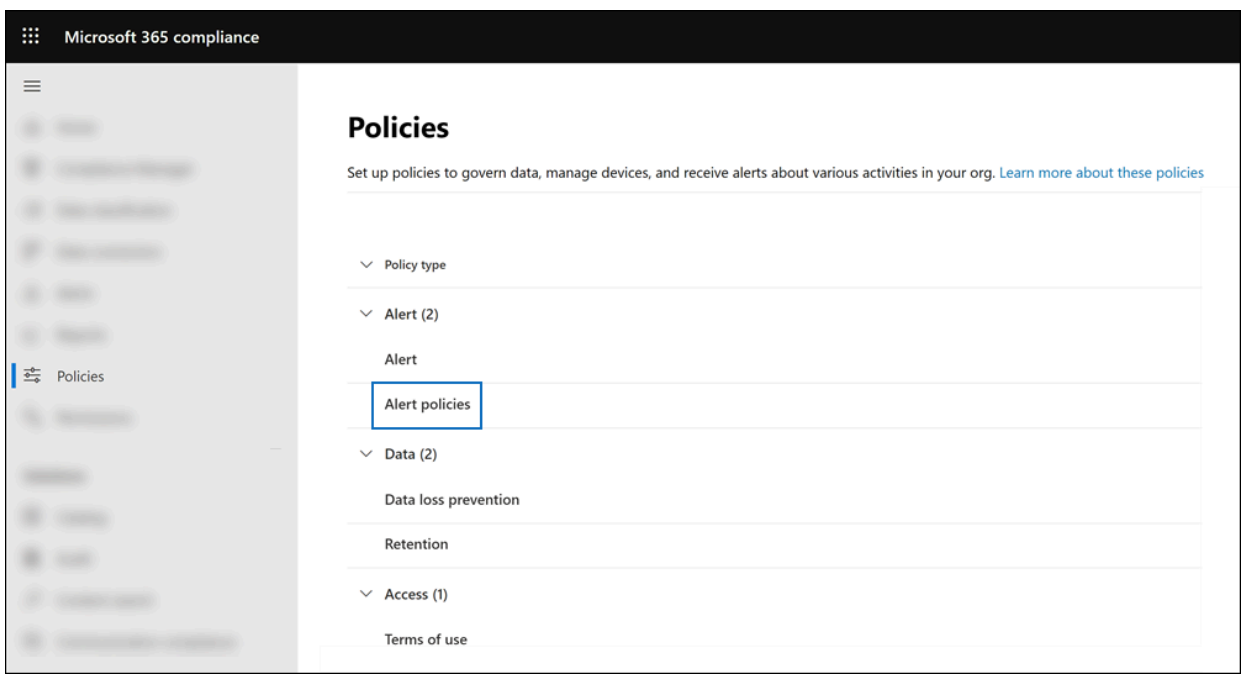
Alert policy settings

An alert policy consists of a set of rules and conditions that define the user or admin activity that generates an alert, a list of users who trigger the alert if they perform the activity, and a threshold that defines how many times the activity has to occur before an alert is triggered. You also categorize the policy and assign it a severity level. These two settings help you manage alert policies (and the alerts that are triggered when the policy conditions are matched) because you can filter on these settings when managing policies and viewing alerts in the Microsoft Purview compliance portal. For example, you can view alerts that match the conditions from the same category or view alerts with the same severity level.

To view and create alert policies:

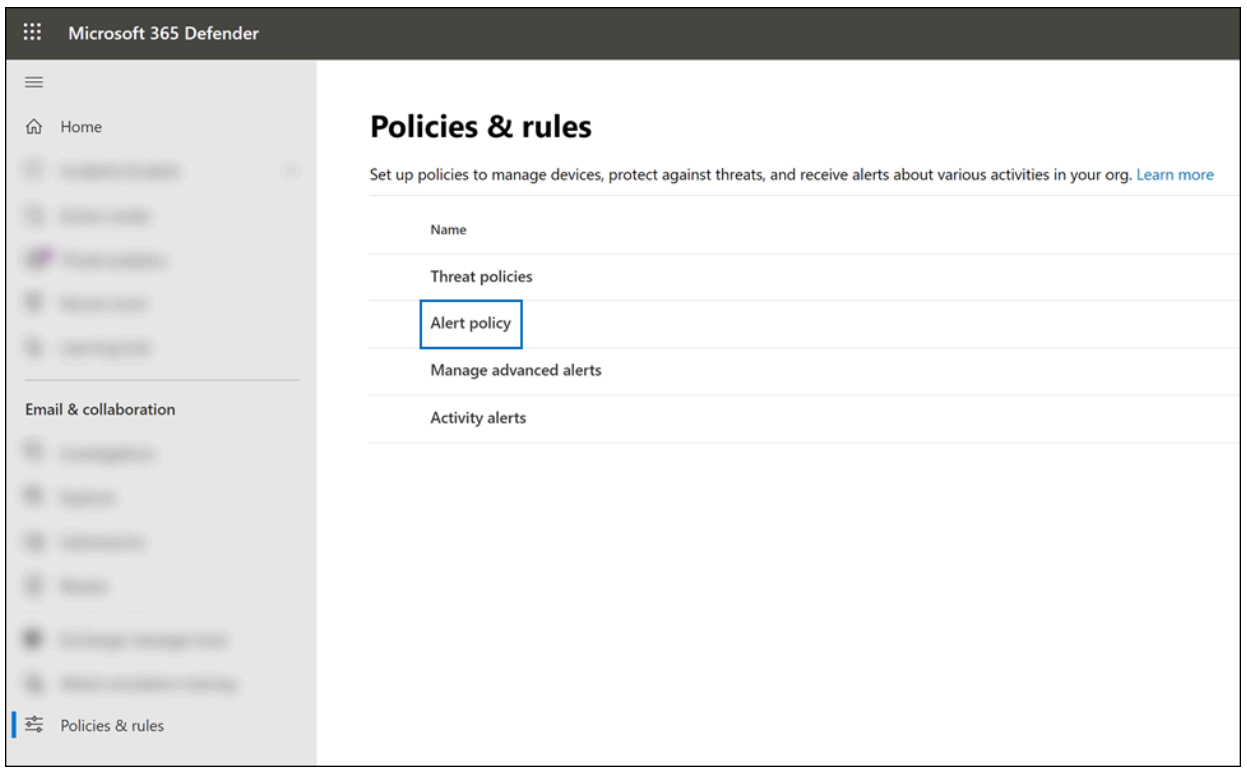
- **Microsoft Purview compliance portal**:

  Go to the compliance portal, and then select **Policies** > **Alert** > **Alert policies**.



- **Microsoft Defender portal**:

  Go to the Microsoft Defender portal and under **Email & collaboration** select **Policies & rules** > **Alert policy**. Alternatively, you can go directly to https://security.microsoft.com/alertpolicies.



> **Note**
>
> You have to be assigned the View-Only Manage Alerts role to view alert policies in the Microsoft Purview compliance portal or the Microsoft Defender portal. You have to be

assigned the Manage Alerts role to create and edit alert policies. For more information, see Permissions in the Microsoft Purview compliance portal.

An alert policy consists of the following settings and conditions.

- **Activity the alert is tracking**. You create a policy to track an activity or in some cases a few related activities, such a sharing a file with an external user by sharing it, assigning access permissions, or creating an anonymous link. When a user performs the activity defined by the policy, an alert is triggered based on the alert threshold settings.

  > ⓘ **Note**
  >
  > The activities that you can track depend on your organization's Office 365 Enterprise or Office 365 US Government plan. In general, activities related to malware campaigns and phishing attacks require an E5/G5 subscription or an E1/F1/G1 or E3/F3/G3 subscription with an Defender for Office 365 Plan 2 add-on subscription.

- **Activity conditions**. For most activities, you can define additional conditions that must be met to trigger an alert. Common conditions include IP addresses (so that an alert is triggered when the user performs the activity on a computer with a specific IP address or within an IP address range), whether an alert is triggered if a specific user or users perform that activity, and whether the activity is performed on a specific file name or URL. You can also configure a condition that triggers an alert when the activity is performed by any user in your organization. The available conditions are dependent on the selected activity.

You can also define user tags as a condition of an alert policy. This definition results in the alerts triggered by the policy to include the context of the impacted user. You can use system user tags or custom user tags. For more information, see User tags in Microsoft Defender for Office 365.

- **When the alert is triggered**. You can configure a setting that defines how often an activity can occur before an alert is triggered. This allows you to set up a policy to generate an alert every time an activity matches the policy conditions, when a certain threshold is exceeded, or when the occurrence of the activity the alert is tracking becomes unusual for your organization.

If you select the setting based on unusual activity, Microsoft establishes a baseline value that defines the normal frequency for the selected activity. It takes up to seven days to establish this baseline, during which alerts aren't generated. After the baseline is established, an alert is triggered when the frequency of the activity tracked by the alert policy greatly exceeds the baseline value. For auditing-related activities (such as file and folder activities), you can establish a baseline based on a single user or based on all users in your organization; for malware-related activities, you can establish a baseline based on a single malware family, a single recipient, or all messages in your organization.

> ⓘ **Note**

> The ability to configure alert policies based on a threshold or based on unusual activity requires an E5/G5 subscription, or an E1/F1/G1 or E3/F3/G3 subscription with a Microsoft Defender for Office 365 P2, Microsoft 365 E5 Compliance, or Microsoft 365 eDiscovery and Audit add-on subscription. Organizations with an E1/F1/G1 and E3/F3/G3 subscription can only create alert policies where an alert is triggered every time that an activity occurs.

- **Alert category**. To help with tracking and managing the alerts generated by a policy, you can assign one of the following categories to a policy.
  - Data loss prevention
  - Information governance
  - Mail flow
  - Permissions
  - Threat management
  - Others

  When an activity occurs that matches the conditions of the alert policy, the generated alert is tagged with the category defined in this setting. This allows you to track and manage alerts that have the same category setting on the **Alerts** page in the Microsoft Purview portal because you can sort and filter alerts based on category.

- **Alert severity**. Similar to the alert category, you assign a severity attribute (**Low**, **Medium**, **High**, or **Informational**) to alert policies. Like the alert category, when an activity occurs that matches the conditions of the alert policy, the alert that's generated is tagged with the same severity level that's set for the alert policy. Again, this allows you to track and manage alerts that have the same severity setting on the **Alerts** page. For example, you can filter the list of alerts so that only alerts with a **High** severity are displayed.

  > **Tip**
  >
  > When setting up an alert policy, consider assigning a higher severity to activities that can result in severely negative consequences, such as detection of malware after delivery to users, viewing of sensitive or classified data, sharing data with external users, or other activities that can result in data loss or security threats. This can help you prioritize alerts and the actions you take to investigate and resolve the underlying causes.

- **Automated investigations**. Some alerts trigger automated investigations to identify potential threats and risks that need remediation or mitigation. In most cases these alerts are triggered by detection of malicious emails or activities, but in some cases the alerts are triggered by administrator actions in the security portal. For more information about automated investigations, see Automated investigation and response (AIR) in Microsoft Defender for Office 365.

- **Email notifications**. You can set up the policy so that email notifications are sent (or not sent) to a list of users when an alert is triggered. You can also set a daily notification limit so that once the maximum number of notifications is reached, no more notifications are sent for the alert during that day. In addition to email notifications, you or other administrators can view the alerts that are triggered by a policy on the **Alerts** page. Consider enabling email notifications for alert policies of a specific category or that have a higher severity setting.

Default alert policies

Microsoft provides built-in alert policies that help identify Exchange admin permissions abuse, malware activity, potential external and internal threats, and information governance risks. On the **Alert policies** page, the names of these built-in policies are in bold and the policy type is

defined as **System**. These policies are turned on by default. You can turn off these policies (or back on again), set up a list of recipients to send email notifications to, and set a daily notification limit. The other settings for these policies can't be edited.

The following tables list and describe the available default alert policies and the category each policy is assigned to. The category is used to determine which alerts a user can view on the Alerts page. For more information, see RBAC permissions required to view alerts.

The tables also indicate the Office 365 Enterprise and Office 365 US Government plan required for each one. Some default alert policies are available if your organization has the appropriate add-on subscription in addition to an E1/F1/G1 or E3/F3/G3 subscription.

> **Note**
>
> The unusual activity monitored by some of the built-in policies is based on the same process as the alert threshold setting that was previously described. Microsoft establishes a baseline value that defines the normal frequency for "usual" activity. Alerts are then triggered when the frequency of activities tracked by the built-in alert policy greatly exceeds the baseline value.

Information governance alert policies

> **Note**
>
> The alert policies in this section are in the process of being deprecated based on customer feedback as false positives. To retain the functionality of these alert policies, you can create custom alert policies with the same settings.

Expand table

Name	Description	Severity	Automated investigation	Subscription
Unusual volume of external file sharing	Generates an alert when an unusually large number of files in SharePoint or OneDrive are shared with users outside of your organization.	Medium	No	E5/G5 or Defender for Office 365 Plan 2 add-on subscription.

Mail flow alert policies

Expand table

Name	Description	Severity	Automated investigation	Required subscription
Messages have been delayed	Generates an alert when Microsoft can't deliver email messages to your on-premises organization or a partner server by using a connector. When this happens, the message is queued in Office 365. This alert is triggered when there are 2,000 messages or more that have been queued for more than an hour.	High	No	E1/F1/G1, E3/F3/G3, or E5/G5
Reply-all storm detected	This alert is triggered when a reply-all storm is detected and at least one reply-all to the mail thread was blocked. For more information, see the Reply-all storm protection report.	High	No	E1/F1/G1, E3/F3/G3, or E5/G5

Permissions alert policies

Expand table

Name	Description	Severity	Automated investigation	Required subscription
Elevation of Exchange admin privilege	Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.	Low	No	E1/F1/G1, E3/F3/G3, or E5/G5

Threat management alert policies

Expand table

Name	Description	Severity	Automated investigation
A potentially malicious URL click was detected	Generates an alert when a user protected by Safe Links in your organization clicks a malicious link. This alert is generated when a user clicks on a link and this event triggers a URL verdict change identification by Microsoft Defender for Office 365. It also checks for any clicks in the past 48 hours from the time the malicious URL verdict is identified, and generates alerts for the clicks that happened in the 48-hour timeframe for that malicious link. This alert automatically triggers automated investigation and response in Defender for Office 365 Plan 2. For more information on events that trigger this alert, see Set up Safe Links policies.	High	Yes
A Tenant Allow Block List entry has been found malicious	Generates an alert when Microsoft determines that the admin submission corresponding to an allow entry in the Tenant Allow/Block List is found to be malicious. This event is triggered as soon as the submission is analyzed by Microsoft. The allow entry will continue to exist for its stipulated duration. For more information on events that trigger this alert, see Manage the Tenant Allow/Block list.	Informational	No
A user clicked through to a potentially malicious URL	Generates an alert when a user protected by Safe Links in your organization clicks a malicious link. This event is triggered when user clicks on a URL (which is identified as malicious or pending validation) and overrides the Safe Links warning page (based on your organization's Microsoft 365 for business Safe Links policy) to continue to the URL hosted page / content. This alert automatically triggers automated investigation and response in Defender for Office 365 Plan 2. For more information on events that trigger this alert, see Set up Safe Links policies.	High	Yes
Admin submission result completed	Generates an alert when an Admin Submission completes the rescan of the submitted entity. An alert is triggered every time a rescan result is rendered from an Admin Submission. These alerts are meant to remind you to review the results of previous submissions, submit user reported messages to get the latest policy	Informational	No

	check and rescan verdicts, and help you determine if the filtering policies in your organization are having the intended impact.		
Admin triggered manual investigation of email	Generates an alert when an admin triggers the manual investigation of an email from Threat Explorer. For more information, see Example: A security administrator triggers an investigation from Threat Explorer. This alert notifies your organization that the investigation was started. The alert provides information about who triggered it and includes a link to the investigation.	Informational	Yes
Admin triggered user compromise investigation	Generates an alert when an admin triggers the manual user compromise investigation of either an email sender or recipient from Threat Explorer. For more information, see Example: A security administrator triggers an investigation from Threat Explorer, which shows the related manual triggering of an investigation on an email. This alert notifies your organization that the user compromise investigation was started. The alert provides information about who triggered it and includes a link to the investigation.	Medium	Yes
Creation of forwarding/redirect rule	Generates an alert when someone in your organization creates an inbox rule for their mailbox that forwards or redirects messages to another email account. This policy only tracks inbox rules that are created using Outlook on the web (formerly known as Outlook Web App) or Exchange Online PowerShell. For more information about using inbox rules to forward and redirect email in Outlook on the web, see Use rules in Outlook on the web to automatically forward messages to another account.	Informational	No
eDiscovery search started or exported	Generates an alert when someone uses the Content search tool in the Microsoft Purview portal. An alert is triggered when the following content search activities are performed: • A content search is started. • The results of a content search are exported. • A content search report is exported. Alerts are also triggered when the previous content search activities are performed in association with an eDiscovery case. For more information about content search activities, see Search for eDiscovery activities in the audit log.	Informational	No
Email messages containing malicious file removed after delivery	Generates an alert when any messages containing a malicious file are delivered to mailboxes in your organization. If this event occurs, Microsoft removes the infected messages from Exchange Online mailboxes using Zero-hour auto purge. This policy automatically triggers automated investigation and response in Office 365. For more information on this new policy, see New alert policies in Defender for Office 365.	Informational	Yes
Email messages containing malicious URL removed after delivery	Generates an alert when any messages containing a malicious URL are delivered to mailboxes in your organization. If this event occurs, Microsoft removes the infected messages from Exchange Online mailboxes using Zero-hour	Informational	Yes

	auto purge. This policy automatically triggers automated investigation and response in Office 365. For more information on this new policy, see New alert policies in Defender for Office 365.		
Email messages containing malware removed after delivery	**Note**: This alert policy was replaced by **Email messages containing malicious file removed after delivery**. This alert policy will eventually go away, so we recommend disabling it and using **Email messages containing malicious file removed after delivery** instead. For more information, see New alert policies in Defender for Office 365.	Informational	Yes
Email messages containing phish URLs removed after delivery	**Note**: This alert policy was replaced by **Email messages containing malicious URL removed after delivery**. This alert policy will eventually go away, so we recommend disabling it and using **Email messages containing malicious URL removed after delivery** instead. For more information, see New alert policies in Defender for Office 365.	Informational	Yes
Email messages from a campaign removed after delivery	Generates an alert when any messages associated with a Campaign are delivered to mailboxes in your organization. If this event occurs, Microsoft removes the infected messages from Exchange Online mailboxes using Zero-hour auto purge. This policy automatically triggers automated investigation and response in Office 365. For more information on this new policy, see New alert policies in Defender for Office 365.	Informational	Yes
Email messages removed after delivery	Generates an alert when any malicious messages that don't contain a malicious entity (URL or File), or associated with a Campaign, are delivered to mailboxes in your organization. If this event occurs, Microsoft removes the infected messages from Exchange Online mailboxes using Zero-hour auto purge. This policy automatically triggers automated investigation and response in Office 365. For more information on this new policy, see New alert policies in Defender for Office 365.	Informational	Yes
Email reported by user as junk	Generates an alert when users in your organization report messages as junk using the built-in Report button in Outlook or the Report Message add-in. For more information about the add-ins, see Use the Report Message add-in.	Low	No
Email reported by user as malware or phish	Generates an alert when users in your organization report messages as phishing using the built-in Report button in Outlook or the Report Message or Report Phishing add-ins. For more information about the add-ins, see Use the Report Message add-in. For Defender for Office 365 Plan 2, E5, G5 customers, this alert automatically triggers automated investigation and response in Defender for Office 365 Plan 2.	Low	Yes

Email reported by user as not junk	Generates an alert when users in your organization report messages as not junk the built-in Report button in Outlook or the Report Message add-in. For more information about the add-ins, see Use the Report Message add-in .	Low	No
Email sending limit exceeded	Generates an alert when someone in your organization has sent more mail than is allowed by the outbound spam policy. This is usually an indication the user is sending too much email or that the account might be compromised. If you get an alert generated by this alert policy, it's a good idea to check whether the user account is compromised.	Medium	No
Failed exact data match upload	Generates an alert when a user receives the following error when uploading an exact data match based sensitive information type: New sensitive information failed to upload. Try again later.	High	No
Form blocked due to potential phishing attempt	Generates an alert when someone in your organization is restricted from sharing forms and collecting responses using Microsoft Forms due to detected repeated phishing attempt behavior.	High	No
Form flagged and confirmed as phishing	Generates an alert when a form created in Microsoft Forms from within your organization is identified as potential phishing through Report Abuse and confirmed as phishing by Microsoft.	High	No
Malware not zapped because ZAP is disabled	Generates an alert when Microsoft detects delivery of a malware message to a mailbox because Zero-Hour Auto Purge for Phish messages is disabled.	Informational	No
Messages containing malicious entity not removed after delivery	Generates an alert when any message containing malicious content (file, URL, campaign, no entity), is delivered to mailboxes in your organization. If this event occurs, Microsoft attempted to remove the infected messages from Exchange Online mailboxes using Zero-hour auto purge, but the message wasn't removed due to a failure. Additional investigation is recommended. This policy automatically triggers automated investigation and response in Office 365.	Medium	Yes
MIP AutoLabel simulation completed	Generates an alert when anservice-side auto-labeling policy in simulation mode has completed.	Low	No
Phish delivered due to an ETR override[1]	Generates an alert when Microsoft detects an Exchange transport rule (also known as a mail flow rule) that allowed delivery of a high confidence phishing message to a mailbox. For more information about Exchange Transport Rules (Mail flow rules), see Mail flow rules (transport rules) in Exchange Online.	Informational	No
Phish delivered due to an IP allow policy[1]	Generates an alert when Microsoft detects an IP allow policy that allowed delivery of a high confidence phishing message to a mailbox. For more information about the IP allow policy (connection filtering), see Configure the default connection filter policy - Office 365.	Informational	No
Phish not zapped because ZAP is disabled[1]	Generates an alert when Microsoft detects delivery of a high confidence phishing message to	Informational	No

	a mailbox because Zero-Hour Auto Purge for Phish messages is disabled.		
Potential nation-state activity	Microsoft Threat Intelligence Center detected an attempt to compromise accounts from your tenant.	High	No
Purview policy simulation completed	Generates an alert to notify admins when simulation is complete for any Purview policy that supports simulation mode.	Low	No
Remediation action taken by admin on emails or URL or sender	**Note**: This alert policy wasn replaced by **Administrative action submitted by an Administrator**. This alert policy will eventually go away, so we recommend disabling it and using **Administrative action submitted by an Administrator** instead. This alert is triggered when an admin takes remediation action on the selected entity	Informational	Yes
Removed an entry in Tenant Allow/Block List	Generates an alert when an allow entry in the Tenant Allow/Block List is learned from by filtering system and removed. This event is triggered when the allow entry for the affected domain or email address, file, or URL (*entity*) is removed. You no longer need the affected allow entry. Email messages that contain the affected entities are delivered to the Inbox if nothing else in the message is determined to be bad. URLs and files will be allowed at time of click. For more information on events that trigger this alert, see Manage the Tenant Allow/Block list.	Informational	No
Retention Auto-labeling policy simulation completed	Generates an alert when a retention auto-labeling policy simulation has completed.	Low	No
Successful exact data match upload	Generates an alert after a user successfully uploads an exact data match based sensitive information type.	Low	No
Suspicious connector activity	Generates an alert when a suspicious activity is detected on an inbound connector in your organization. Mail is blocked from using the inbound connector. The admin receives an email notification and an alert. This alert provides guidance on how to investigate, revert changes, and unblock a restricted connector. To learn how to respond to this alert, see Respond to a compromised connector.	High	No
Suspicious email forwarding activity	Generates an alert when someone in your organization has autoforwarded email to a suspicious external account. This is an early warning for behavior that might indicate the account is compromised, but not severe enough to restrict the user. Although it's rare, an alert	High	No

	generated by this policy might be an anomaly. It's a good idea to check whether the user account is compromised.		
Suspicious email sending patterns detected	Generates an alert when someone in your organization has sent suspicious email and is at risk of being restricted from sending email. This is an early warning for behavior that might indicate that the account is compromised, but not severe enough to restrict the user. Although it's rare, an alert generated by this policy might be an anomaly. However, it's a good idea to check whether the user account is compromised.	Medium	Yes
Suspicious tenant sending patterns observed	Generates an alert when Suspicious sending patterns have been observed in your organization, which might lead to your organization being blocked from sending emails. Investigate any potentially compromised user and admin accounts, new connectors, or open relays to avoid tenant exceed threshold blocks. For more information about why organizations are blocked, see Fix email delivery issues for error code 5.7.7xx in Exchange Online.	High	No
Teams message reported by user as security risk	This alert is triggered when users report a Teams message as a security risk.	Low	No
Tenant Allow/Block List entry is about to expire	Generates an alert when an allow entry or block entry in the Tenant Allow/Block List entry is about to be removed. This event is triggered seven days before the expiration date, which is based on when the entry was created or last updated. For both allow entries and block entries, you can extend the expiration date. For more information on events that trigger this alert, see Manage the Tenant Allow/Block list.	Informational	No
Tenant restricted from sending email	Generates an alert when most of the email traffic from your organization is detected as suspicious and Microsoft has restricted your organization from sending email. Investigate any potentially compromised user and admin accounts, new connectors, or open relays, and then contact Microsoft Support to unblock your organization. For more information about why organizations are blocked, see Fix email delivery issues for error code 5.7.7xx in Exchange Online.	High	No
Tenant restricted from sending unprovisioned email	Generates an alert when too much email is being sent from unregistered domains (also known as *unprovisioned* domains). Office 365 allows a reasonable amount of email from unregistered domains, but you should configure every domain that you use to send email as an accepted domain. This alert indicates that all users in the organization can no longer send email. For more information about why organizations are blocked, see Fix email delivery issues for error code 5.7.7xx in Exchange Online.	High	No
User requested to release a quarantined message	Generates an alert when a user requests release for a quarantined message. To request the release of quarantined messages, the **Allow recipients to request a message to be released from quarantine** (*PermissionToRequestRelease*) permission is required in the quarantine policy (for example, from the **Limited access** preset permissions group). For more information, see	Informational	No

	Allow recipients to request a message to be released from quarantine permission.		
User restricted from sending email	Generates an alert when someone in your organization is restricted from sending outbound mail. This alert typically indicates a compromised account where the user is listed on the **Restricted entities** page at https://security.microsoft.com/restrictedentities. For more information about restricted users, see Remove blocked users from the Restricted entities page.	High	Yes
User restricted from sharing forms and collecting responses	Generates an alert when someone in your organization is restricted from sharing forms and collecting responses using Microsoft Forms due to detected repeated phishing attempt behavior.	High	No

[1] This alert policy is part of the replacement functionality for the **Phish delivered due to tenant or user override** and **User impersonation phish delivered to inbox/folder** alert policies that were removed based on user feedback. For more information about anti-phishing in Office 365, see Anti-phishing policies.

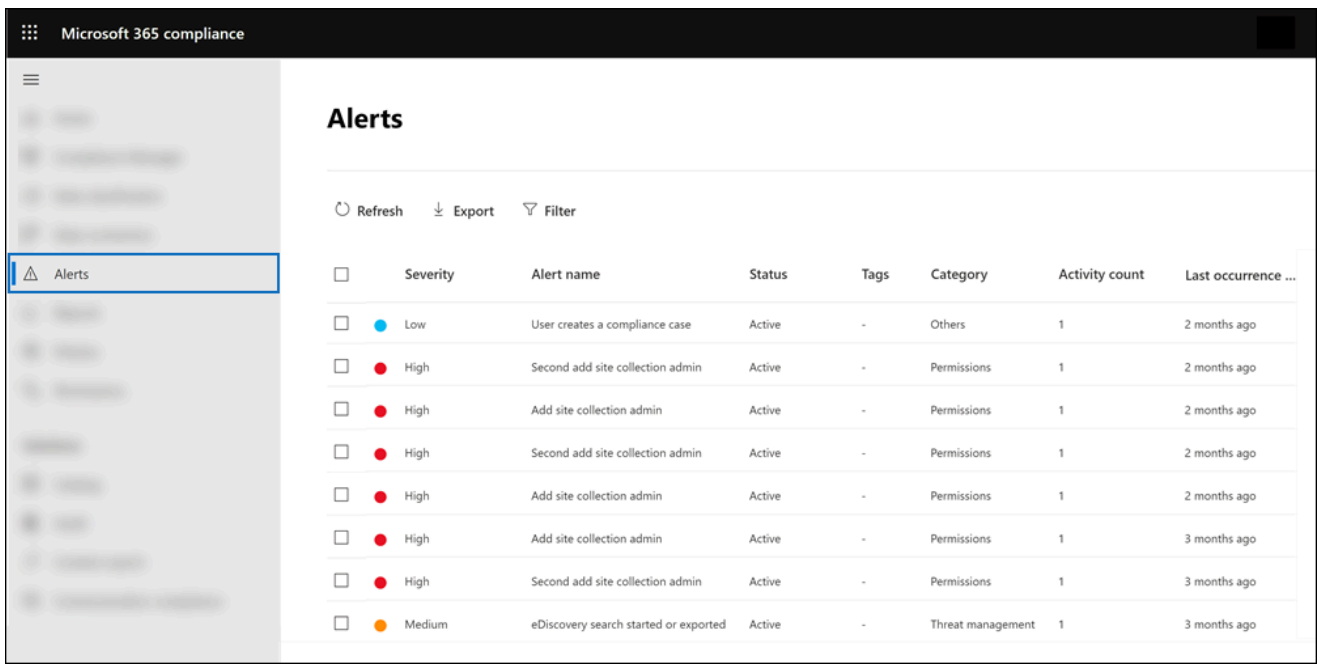
View alerts

When an activity performed by users in your organization matches the settings of an alert policy, an alert is generated and displayed on the **Alerts** page in the Microsoft Purview portal or the Defender portal. Depending on the settings of an alert policy, an email notification is also sent to a list of specified users when an alert is triggered. For each alert, the dashboard on the **Alerts** page displays the name of the corresponding alert policy, the severity and category for the alert (defined in the alert policy), and the number of times an activity has occurred that resulted in the alert being generated. This value is based on the threshold setting of the alert policy. The dashboard also shows the status for each alert. For more information about using the status property to manage alerts, see Managing alerts.

To view alerts:

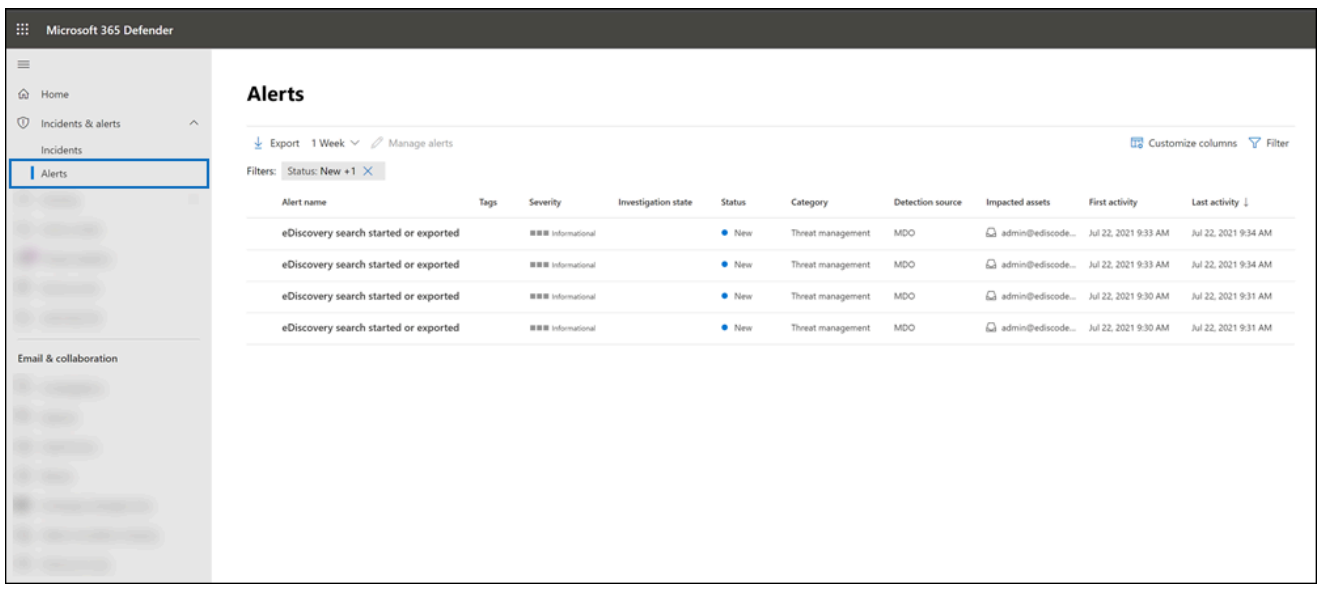
Microsoft Purview compliance portal

Go to https://compliance.microsoft.com and then select **Alerts**. Alternatively, you can go directly to https://compliance.microsoft.com/compliancealerts.



Microsoft Defender portal

Go to https://security.microsoft.com and then select **Incidents & alerts** > **Alerts**. Alternatively, you can go directly to https://security.microsoft.com/alerts.



You can use the following filters to view a subset of all the alerts on the **Alerts** page:

- **Status**: Show alerts that are assigned a particular status. The default status is **Active**. You or other administrators can change the status value.
- **Policy**: Show alerts that match the setting of one or more alert policies. Or you can display all alerts for all alert policies.
- **Time range**: Show alerts that were generated within a specific date and time range.
- **Severity**: Show alerts that are assigned a specific severity.
- **Category**: Show alerts from one or more alert categories.
- **Tags**:Show alerts from one or more user tags. Tags are reflected based on tagged mailboxes or users that appear in the alerts. See User tags in Defender for Office 365 to learn more.
- **Source**: Use this filter to show alerts triggered by alert policies in the Microsoft Purview portal or alerts triggered by Microsoft Defender for Cloud Apps policies, or both. For more information about Defender for Cloud Apps alerts, see the View Defender for Cloud Apps alerts section in this article.

> **Important**
>
> Filtering and sorting by user tags is currently in Public Preview, and might be substantially modified before it's generally available. Microsoft makes no warranties, express or implied, with respect to the information provided about it.

Alert aggregation

When multiple events that match the conditions of an alert policy occur with a short period of time, they're added to an existing alert by a process called *alert aggregation*. When an event triggers an alert, the alert is generated and displayed on the **Alerts** page and a notification is sent. If the same event occurs within the aggregation interval, then Microsoft 365 adds details about the new event to the existing alert instead of triggering a new alert. The goal of alert aggregation is to help reduce alert "fatigue" and let you focus and take action on fewer alerts for the same event.

The length of the aggregation interval depends on your Office 365 or Microsoft 365 subscription.

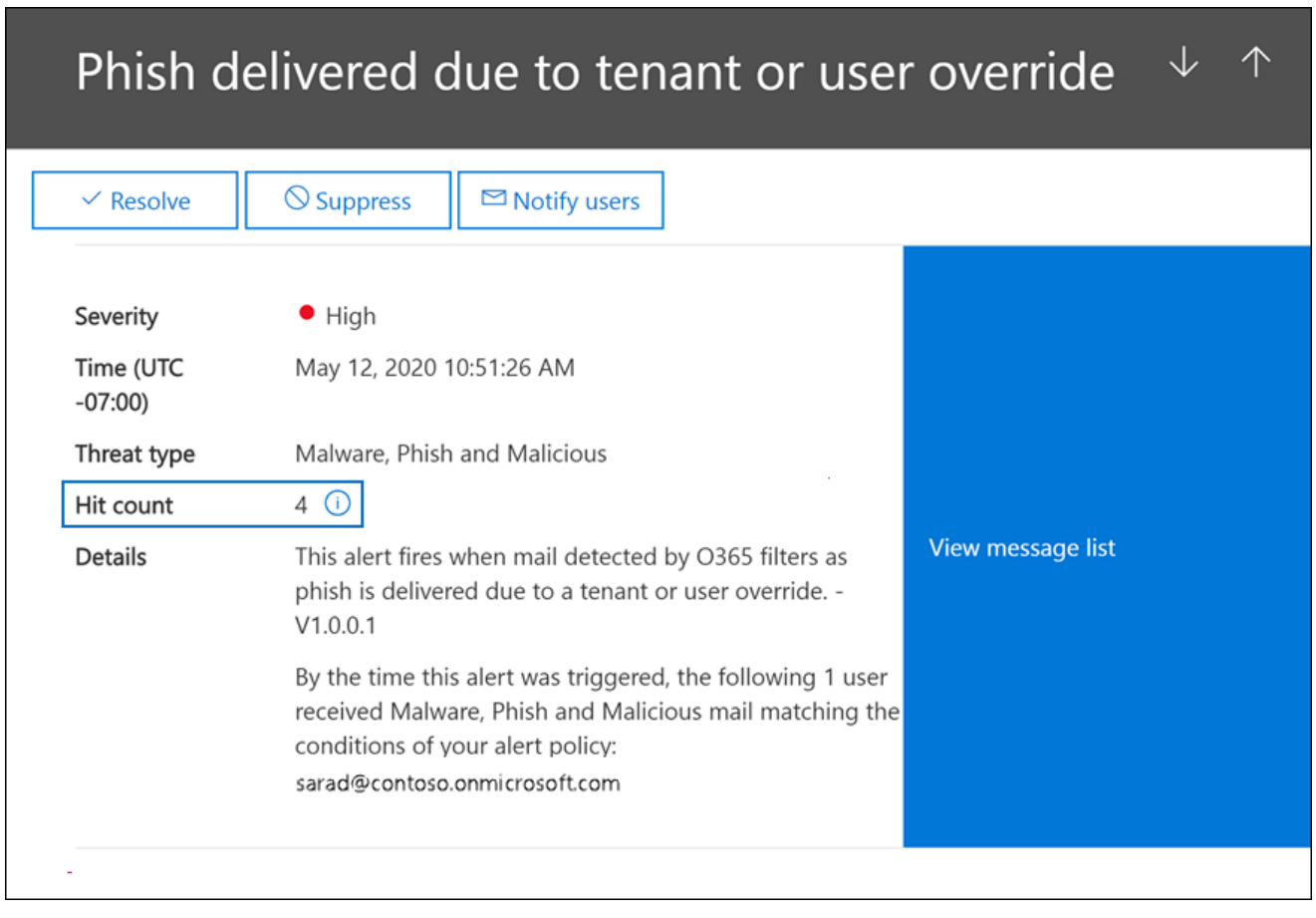
Expand table

Subscription	Aggregation interval

Office 365 or Microsoft 365 E5/G5	1 minute
Defender for Office 365 Plan 2	1 minute
E5 Compliance add-on or E5 Discovery and Audit add-on	1 minute
Office 365 or Microsoft 365 E1/F1/G1 or E3/F3/G3	15 minutes
Defender for Office 365 Plan 1 or Exchange Online Protection	15 minutes

When events that match the same alert policy occur within the aggregation interval, details about the subsequent event are added to the original alert. For all events, information about aggregated events is displayed in the details field and the number of times an event occurred with the aggregation interval is displayed in the activity/hit count field. You can view more information about all aggregated events instances by viewing the activity list.

The following screenshot shows an alert with four aggregated events. The activity list contains information about the four email messages relevant to the alert.



Keep the following things in mind about alert aggregation:

- Alerts triggered by the **A potentially malicious URL click was detected** default alert policy aren't aggregated. This behavior occurs because alerts triggered by this policy are unique to each user and email message.
- At this time, the **Hit count** alert property doesn't indicate the number of aggregated events for all alert policies. For alerts triggered by these alert policies, you can view the aggregated events by clicking **View message list** or **View activity** on the alert. We're working to make the number of aggregated events listed in the **Hit count** alert property available for all alert policies.

RBAC permissions required to view alerts

The Role Based Access Control (RBAC) permissions assigned to users in your organization determine which alerts a user can see on the **Alerts** page. How is this accomplished? The management roles assigned to users (based on their membership in role groups in the compliance portal or the Microsoft Defender portal) determine which alert categories a user can see on the **Alerts** page. Here are some examples:

- Members of the Records Management role group can view only the alerts that are generated by alert policies that are assigned the **Information governance** category.
- Members of the Compliance Administrator role group can't view alerts that are generated by alert policies that are assigned the **Threat management** category.

- Members of the eDiscovery Manager role group can't view any alerts because none of the assigned roles provide permission to view alerts from any alert category.

This design (based on RBAC permissions) lets you determine which alerts can be viewed (and managed) by users in specific job roles in your organization.

The following table lists the roles that are required to view alerts from the six different alert categories. A check mark indicates that a user who is assigned that role can view alerts from the corresponding alert category listed in the title row.

To see which category a default alert policy is assigned to, see the tables in Default alert policies.

> **Tip**
>
> For information about permissions in **Microsoft Defender XDR Unified role based access control (RBAC)**, see **Alert policies in the Microsoft Defender portal**.

Expand table

Role	Information governance	Data loss prevention	Mail flow	Permissions	Threat management	Others
Compliance Administrator	✓	✓		✓		✓
DLP Compliance Management		✓				
Information Protection Admin		✓				
Information Protection Analyst		✓				
Information Protection Investigator		✓				
Manage Alerts						✓
Organization Configuration						✓
Privacy Management						
Quarantine						
Record Management	✓					
Retention Management	✓					
Role Management				✓		
Security Administrator		✓		✓	✓	✓
Security Reader		✓		✓	✓	✓
Transport Hygiene						
View-Only DLP Compliance Management		✓				
View-Only Configuration						
View-Only Manage Alerts						✓
View-Only Recipients			✓			

View-Only Record Management	✓
View-Only Retention Management	✓

Tip

To view the roles that are assigned to each of the default role groups, run the following commands in Security & Compliance PowerShell:

PowerShell Copy

```
$RoleGroups = Get-RoleGroup

$RoleGroups | foreach {Write-Output -InputObject `r`n,$_.Name,("-"*25); Get-
```

You can also view the roles assigned to a role group in the compliance portal or the Microsoft Defender portal. Go to the **Permissions** page, and select a role group. The assigned roles are listed on the flyout page.

Manage alerts

After alerts are generated and displayed on the **Alerts** page in the Microsoft Purview portal, you can triage, investigate, and resolve them. The same RBAC permissions that give users access to alerts also give them the ability to manage alerts.

Here are some tasks you can perform to manage alerts.

- **Assign a status to alerts**: You can assign one of the following statuses to alerts: **Active** (the default value), **Investigating**, **Resolved**, or **Dismissed**. Then, you can filter on this setting to display alerts with the same status setting. This status setting can help track the process of managing alerts.

- **View alert details**: You can select an alert to display a flyout page with details about the alert. The detailed information depends on the corresponding alert policy, but it typically includes the following information:
  - The name of the actual operation that triggered the alert, such as a cmdlet or an audit log operation.
  - A description of the activity that triggered the alert.
  - The user (or list of users) who triggered the alert. This is included only for alert policies that are set up to track a single user or a single activity.
  - The number of times the activity tracked by the alert was performed. This number might not match that actual number of related alerts listed on the Alerts page because more alerts might have been triggered.
  - A link to an activity list that includes an item for each activity that was performed that triggered the alert. Each entry in this list identifies when the activity occurred, the name of the actual operation (such as "FileDeleted"), the user who performed the activity, the object (such as a file, an eDiscovery case, or a mailbox) that the activity was performed on, and the IP address of the user's computer. For malware-related alerts, this links to a message list.
  - The name (and link) of the corresponding alert policy.

- **Suppress email notifications**: You can turn off (or suppress) email notifications from the flyout page for an alert. When you suppress email notifications, Microsoft won't send notifications when activities or events that match the conditions of the alert policy occur. But alerts will be triggered when activities performed by users match the conditions of the alert policy. You can also turn off email notifications by editing the alert policy.

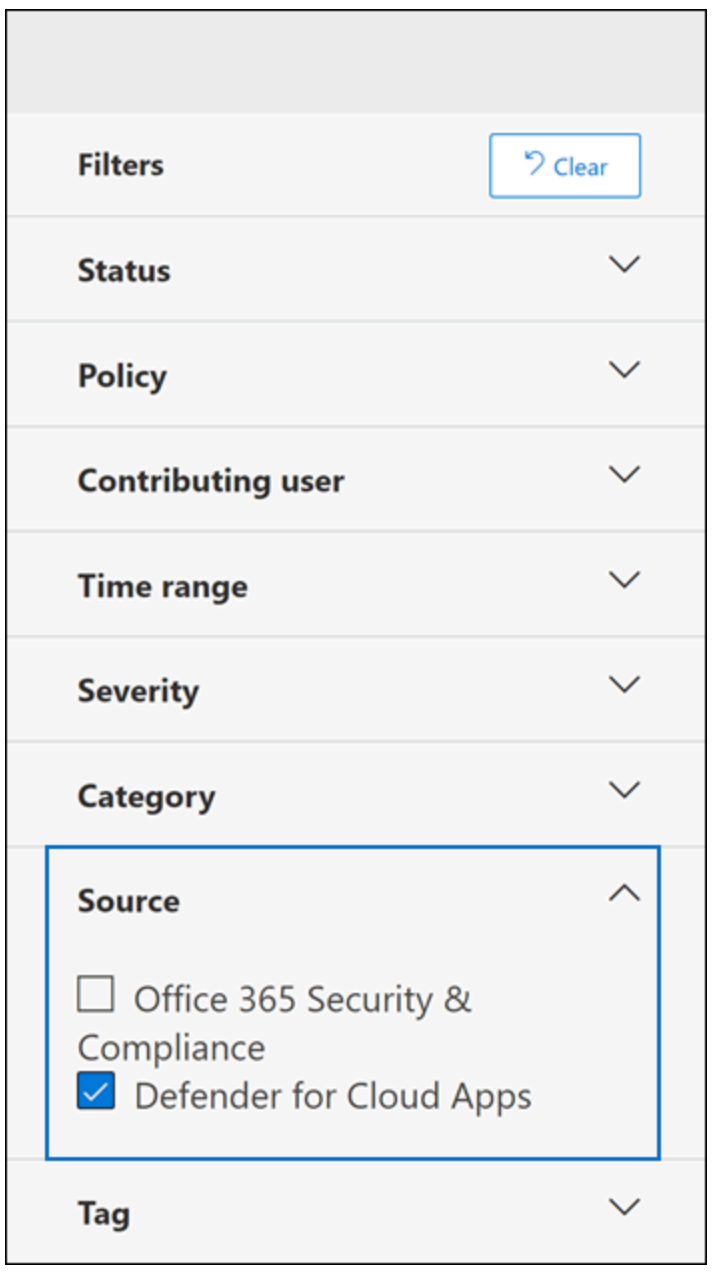
- **Resolve alerts**: You can mark an alert as resolved on the flyout page for an alert (which sets the status of the alert to **Resolved**). Unless you change the filter, resolved alerts aren't displayed on the **Alerts** page.

View Defender for Cloud Apps alerts

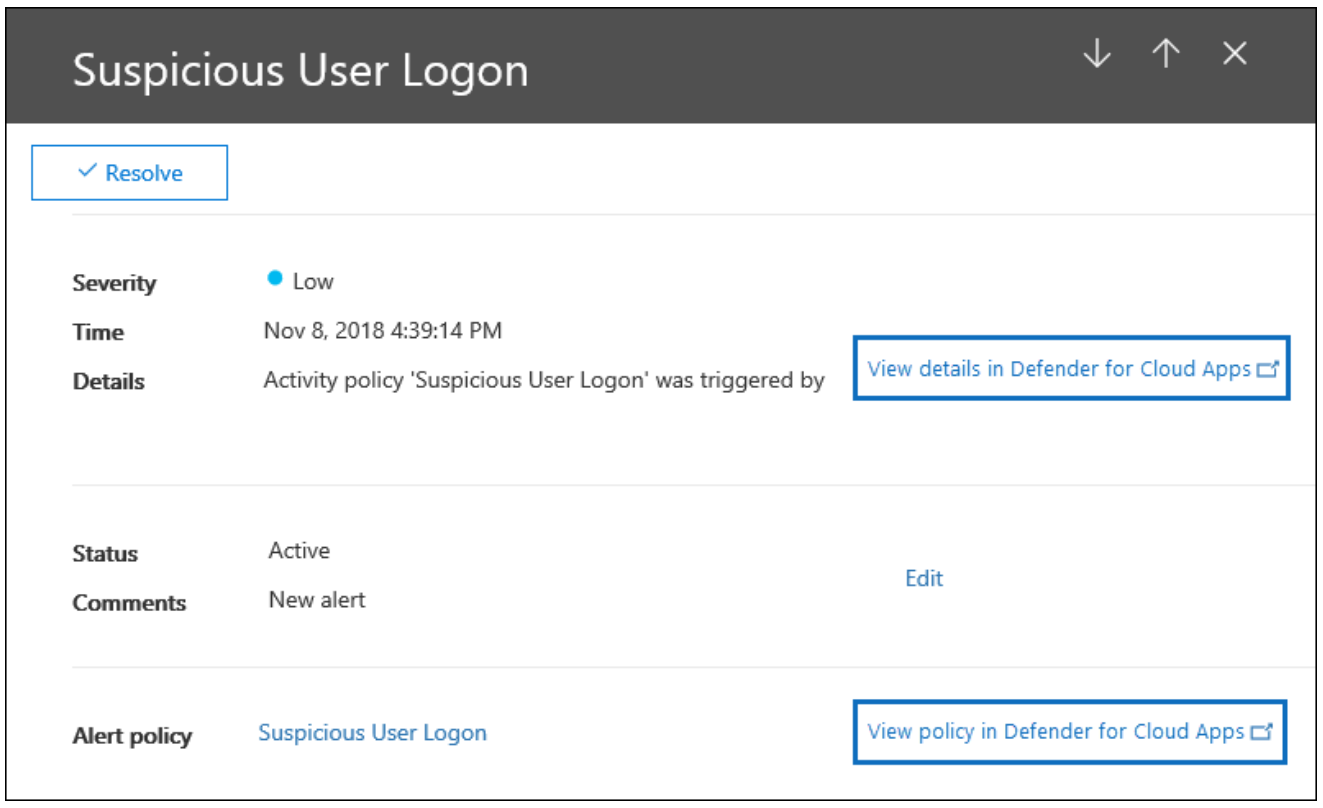
Alerts that are triggered by Defender for Cloud Apps policies are now displayed on the **Alerts** page in the Microsoft Purview portal. This includes alerts that are triggered by activity policies and alerts that are triggered by anomaly detection policies in Defender for Cloud Apps. This means you can view all alerts in the Microsoft Purview portal. Defender for Cloud Apps is only available for organizations with an Office 365 Enterprise E5 or Office 365 US Government G5 subscription. For more information, see Overview of Defender for Cloud Apps.

Organizations that have Microsoft Defender for Cloud Apps as part of an Enterprise Mobility + Security E5 subscription or as a standalone service can also view Defender for Cloud Apps alerts that are related to Microsoft 365 apps and services in the compliance portal or the Microsoft Defender portal.

To display only Defender for Cloud Apps alerts in the Microsoft Purview portal or the Defender portal, use the **Source** filter and select **Defender for Cloud Apps**.



Similar to an alert triggered by an alert policy in the Microsoft Purview portal, you can select a Defender for Cloud Apps alert to display a flyout page with details about the alert. The alert includes a link to view the details and manage the alert in the Defender for Cloud Apps portal and a link to the corresponding Defender for Cloud Apps policy that triggered the alert. See Monitor alerts in Defender for Cloud Apps.



Important

Changing the status of a Defender for Cloud Apps alert in the Microsoft Purview portal won't update the resolution status for the same alert in the Defender for Cloud Apps portal. For example, if you mark the status of the alert as **Resolved** in the Microsoft Purview portal, the status of the alert in the Defender for Cloud Apps portal is unchanged. To resolve or dismiss a Defender for Cloud Apps alert, manage the alert in the Defender for Cloud Apps portal.

Feedback

Was this page helpful? Yes No

Additional resources

Training

Module

Enhance your email protection using Microsoft Defender for Office 365 - Training

This module examines how Microsoft Defender for Office 365 extends EOP protection through various tools, including Safe Attachments, Safe Links, spoofed intelligence, spam filtering policies, and the Tenant Allow/Block List.

Certification

Microsoft Certified: Information Protection and Compliance Administrator Associate - Certifications

Demonstrate the fundamentals of data security, lifecycle management, information security, and compliance to protect a Microsoft 365 deployment.