Alert policies in the security and compliance center

To view contributors to this article access the link below

https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide

In this article

1. How alert policies work
2. Alert policy settings
3. Default alert policies
4. Viewing alerts
5. RBAC permissions required to view alerts
6. Managing alerts
7. Viewing Cloud App Security alerts

You can use the new alert policy and alert dashboard tools in the Office 365 and Microsoft 365 security and compliance centers to create alert policies and then view the alerts generated when users perform activities that match the conditions of an alert policy.

Alert policies build on and expand the functionality of activity alerts by letting you categorize the alert 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. There's also a **View alerts** page in the security and compliance center where you can view and filter alerts, set an alert status to help you manage alerts, and then dismiss alerts after you've addressed or resolved the underlying incident. We've also expanded the type of events that you can create alerts for. For example,

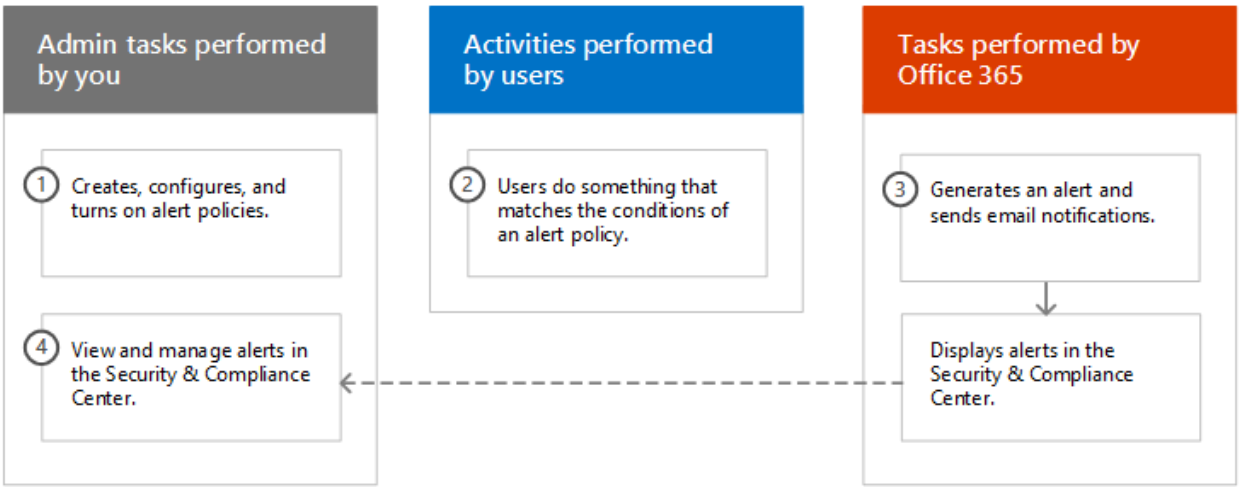
you can create alert policies to track malware activity and data loss incidents. We've also included several default alert policies that help you monitor activities such as assigning admin privileges in Exchange Online, malware attacks, phishing campaigns, and unusual levels of file deletions and external sharing.

Note

Alert policies are available for organizations with a Microsoft 365, Office 365 Enterprise, or Office 365 US Government E1/F1/G1, E3/G3, or E5/G5 subscription. Advanced functionality is only available for organizations with an E5/G5 subscription, or for organizations that have an E1/F1/G1 or E3/G3 subscription and an Office 365 Advanced Threat Protection (ATP) P2 or a Microsoft 365 E5 Compliance or Microsoft 365 E5 eDiscovery and Audit add-on subscription. The functionality that requires an E5/G5 or add-on subscription is highlighted in this topic. Also note that alert policies are available in Office 365 GCC, GCC High, and DoD US government environments.

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.

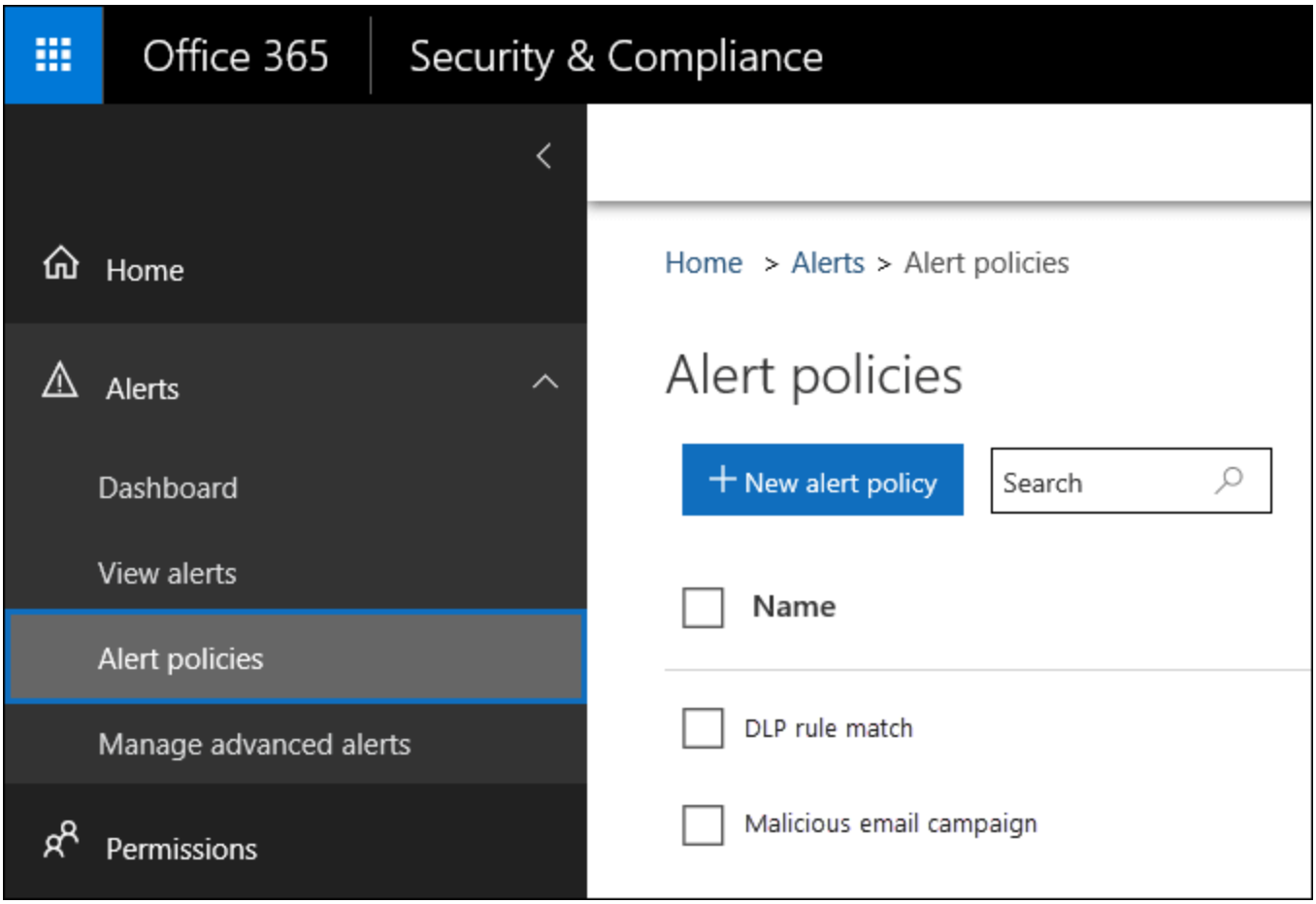


1. An admin in your organization creates, configures, and turns on an alert policy by using the **Alert policies** page in the security and compliance center. You can also create alert policies by using the **New-ProtectionAlert** cmdlet in Security & Compliance Center PowerShell. To create alert policies, you have to be assigned the Manage Alerts role or the Organization Configuration role in the security and compliance center.
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. Office 365 generates an alert that's displayed on the **View alerts** page in the security and compliance center. Also, if email notifications are enabled for the alert policy, Office 365 sends a notification to a list of recipients. The alerts that an admin or other users can see that on the View alerts page is determined by the roles assigned to the user. For more information, see the RBAC permissions required to view alerts section.
4. An admin manages alerts in the security and compliance center. 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 security and compliance center. 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, go to https://protection.office.com and then select **Alerts** > **Alert policies**.



An alert policy consists of the following settings and conditions.

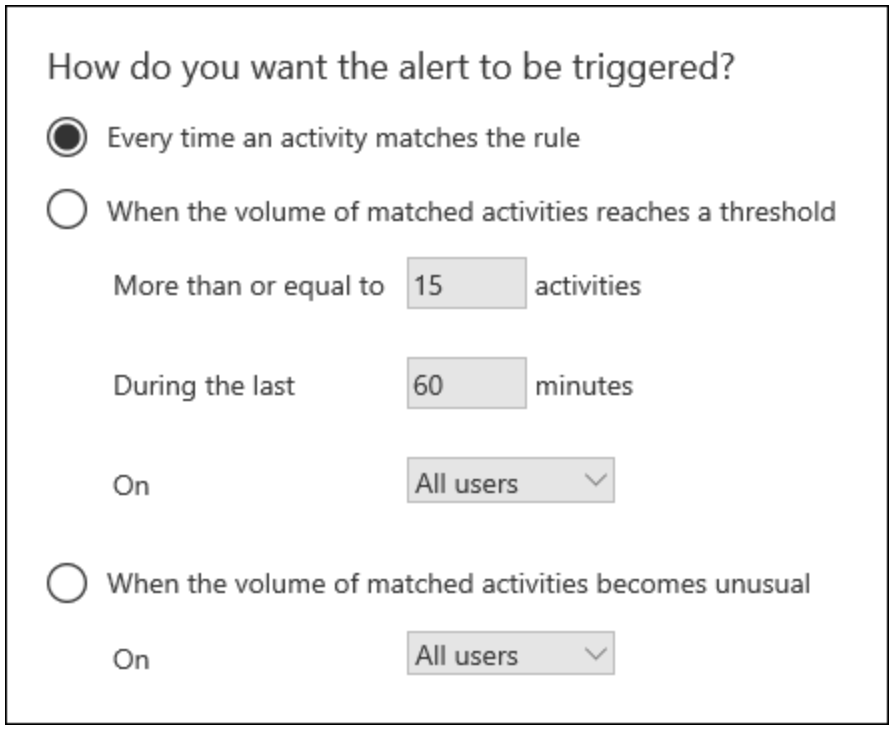
- **Activity the alert is tracking** - You create a policy to track an activity or in some cases a few related activities, such a sharing a file with an external user by sharing it, assigning access permissions, or creating an anonymous link. When a user performs the activity defined by the policy, an 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/G3 subscription with an Office 365 Advanced Threat Protection 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.
- **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, Office 365 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 won't be 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/G3

subscription with an Office 365 ATP P2, Microsoft 365 E5 Compliance, or Microsoft 365 eDiscovery and Audit add-on subscription. Organizations with an E1/F1/G1 and E3/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 alert that's generated 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 **View alerts** page in the security and compliance center 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 **View 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.

- **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 has been 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 **View alerts** page. Consider enabling email notifications for alert policies of a specific category or that have a higher severity setting.

Default alert policies

Office 365 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 table lists and describes 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 View alerts page. For more information, see the RBAC permissions required to view alerts section.

The table also indicates 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/G3 subscription.

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
A potentially malicious URL click was detected	Generates an alert when a user protected by Office 365 ATP Safe Links in your organization clicks a malicious link. This event is triggered when URL verdict changes are identified by Office 365 ATP or when users override the Office 365 ATP Safe Links pages (based on your organization's Office 365 ATP Safe Links policy).	Threat management	E5/G5 or Office 365 ATP P2 add-on subscription

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	This alert policy has a **High** severity setting. For Office 365 ATP P2, E5, G5 customers, this alert automatically triggers automated investigation and response in Office 365. For more information on events that trigger this alert, see Set up Office 365 ATP Safe Links policies.		
Admin Submission result completed	Generates an alert when an Admin Submission completes the rescan of the submitted entity. An alert will be 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	Threat management	E1/F1, E3, or E5

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	reported messages to get the latest policy check and rescan verdicts, and help you determine if the filtering policies in your organization are having the intended impact. This policy has a **Low** severity setting.		
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. This policy has	Threat management	E1/F1/G1, E3/G3, or E5/G5

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	a **Low** severity setting. 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.		
eDiscovery search started or exported	Generates an alert when someone uses the Content search tool in the Security and compliance center. 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	Threat management	E1/F1/G1, E3/G3, or E5/G5

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	Alerts are also triggered when the previous content search activities are performed in association with an eDiscovery case. This policy has a **Medium** severity setting. For more information about content search activities, see Search for eDiscovery activities in the Office 365 audit log.		
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. This policy has a **Low** severity setting.	Permissions	E1/F1/G1, E3/G3, or E5/G5

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
Email messages containing malware removed after delivery	Generates an alert when any messages containing malware are delivered to mailboxes in your organization. If this event occurs, Office 365 removes the infected messages from Exchange Online mailboxes using Zero-hour auto purge. This policy has an **Informational** severity setting and automatically triggers automated investigation and response in Office 365.	Threat management	E5/G5 or Office 365 ATP P2 add-on subscription
Email messages containing phish URLs removed after delivery	Generates an alert when any messages containing phish are delivered to mailboxes in your organization. If this event occurs, Office 365 removes the infected messages from Exchange	Threat management	E5/G5 or Office 365 ATP P2 add-on subscription

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	Online mailboxes using Zero-hour auto purge. This policy has an **Informational** severity setting and automatically triggers automated investigation and response in Office 365.		
Email reported by user as malware or phish	Generates an alert when users in your organization report messages as phishing email using the Report Message add-in. This policy has an **Informational** severity setting. For more information about this add-in, see Use the Report Message add-in. For Office 365 ATP P2, E5, G5 customers, this alert automatically triggers automated investigation and	Threat management	E1/F1/G1, E3/G3, or E5/G5

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	response in Office 365.		
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 may be compromised. This policy has a **Medium** severity setting. If you get an alert generated by this alert policy, it's a good idea to check whether the user account is compromised.	Threat management	E1/F1/G1, E3/G3, or E5/G5
Messages have been delayed	Generates an alert when Office 365 can't deliver email messages to your on-premises organization or a partner server by using a	Mail flow	E1/F1/G1, E3/G3, or E5/G5

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	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. This policy has a **High** severity setting.		
Malware campaign detected after delivery	Generates an alert when an unusually large number of messages containing malware are delivered to mailboxes in your organization. If this event occurs, Office 365 removes the infected messages from Exchange Online mailboxes. This policy has a **High** severity setting.	Threat management	E5/G5 or Office 365 ATP P2 add-on subscription
Malware campaign	Generates an alert when	Threat	E5/G5 or

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
detected and blocked	someone has attempted to send an unusually large number of email messages containing a certain type of malware to users in your organization. If this event occurs, the infected messages are blocked by Office 365 and not delivered to mailboxes. This policy has a **Low** severity setting.	management	Office 365 ATP P2 add-on subscription
Malware campaign detected in SharePoint and OneDrive	Generates an alert when an unusually high volume of malware or viruses is detected in files located in SharePoint sites or OneDrive accounts in your organization. This policy has a **High** severity setting.	Threat management	E5/G5 or Office 365 ATP P2 add-on subscription
Phish delivered due	Generates an alert when	Threat	E5/G5 or

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
to tenant or user override[1]	Office 365 detects an admin or user override allowed the delivery of a phishing message to a mailbox. Examples of overrides include an inbox or mail flow rule that allows messages from a specific sender or domain, or an anti-spam policy that allows messages from specific senders or domains. This policy has a **High** severity setting.	management	Office 365 ATP P2 add-on subscription
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 may indicate that the	Threat management	E1/F1/G1, E3/G3, or E5/G5

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	account is compromised, but not severe enough to restrict the user. This policy has a **Medium** severity setting. Although it's rare, an alert generated by this policy may be an anomaly. However, it's a good idea to check whether the user account is compromised.		
Tenant restricted from sending email	Generates an alert when most of the email traffic from your organization has been 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	Threat management	E1/F1/G1, E3/G3, or E5/G5

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	Support to unblock your organization. This policy has a **High** severity setting. For more information about why organizations are blocked, see Fix email delivery issues for error code 5.7.7xx in Exchange Online.		
Unusual external user file activity	Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a **High** severity setting.	Information governance	E5/G5, Office 365 ATP P2, or Microsoft 365 E5 add-on subscription
Unusual volume of	Generates an alert when an	Information	E5/G5, Office

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
external file sharing	unusually large number of files in SharePoint or OneDrive are shared with users outside of your organization. This policy has a **Medium** severity setting.	governance	365 ATP P2, or Microsoft 365 E5 add-on subscription
Unusual volume of file deletion	Generates an alert when an unusually large number of files are deleted in SharePoint or OneDrive within a short time frame. This policy has a **Medium** severity setting.	Information governance	E5/G5, Office 365 ATP P2, or Microsoft 365 E5 add-on subscription
Unusual increase in email reported as phish	Generates an alert when there's a significant increase in the number of people in your organization using the Report Message add-in in Outlook to report messages as phishing mail. This	Threat management	E5/G5 or Office 365 ATP P2 add-on subscription

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
	policy has a **High** severity setting. For more information about this add-in, see Use the Report Message add-in.		
User impersonation phish delivered to inbox/folder[1,2]	Generates an alert when Office 365 detects that an admin or user override has allowed the delivery of a user impersonation phishing message to the inbox (or other user-accessible folder) of a mailbox. Examples of overrides include an inbox or mail flow rule that allows messages from a specific sender or domain, or an anti-spam policy that allows messages from specific senders or domains. This policy has a **Medium** severity setting.	Threat management	E5/G5 or Office 365 ATP P2 add-on subscription

Table 1			
Default alert policy	**Description**	**Category**	**Office 365 Enterprise subscription**
User restricted from sending email	Generates an alert when someone in your organization is restricted from sending outbound mail. This typically results when an account is compromised, and the user is listed on the **Restricted Users** page in the Security & Compliance Center. (To access this page, go to **Threat management > Review > Restricted Users**). This policy has a **High** severity setting. For more information about restricted users, see Removing a user, domain, or IP address from a block list after sending spam email.	Threat management	E1/F1/G1, E3/G3, or E5/G5

Note

[1] We've temporarily removed this default alert policy based on customer feedback. We're working to improve it, and will replace it with a new version in the near future. Until then, you can create a custom alert policy to replace this functionality by using the following settings:

* Activity is Phish email detected at time of delivery
* Mail is not ZAP'd
* Mail direction is Inbound
* Mail delivery status is Delivered
* Detection technology is Malicious URL retention, URL detonation, Advanced phish filter, General phish filter, Domain impersonation, User impersonation, and Brand impersonation

For more information about anti-phishing in Office 365, see Set up anti-phishing and anti-phishing policies.

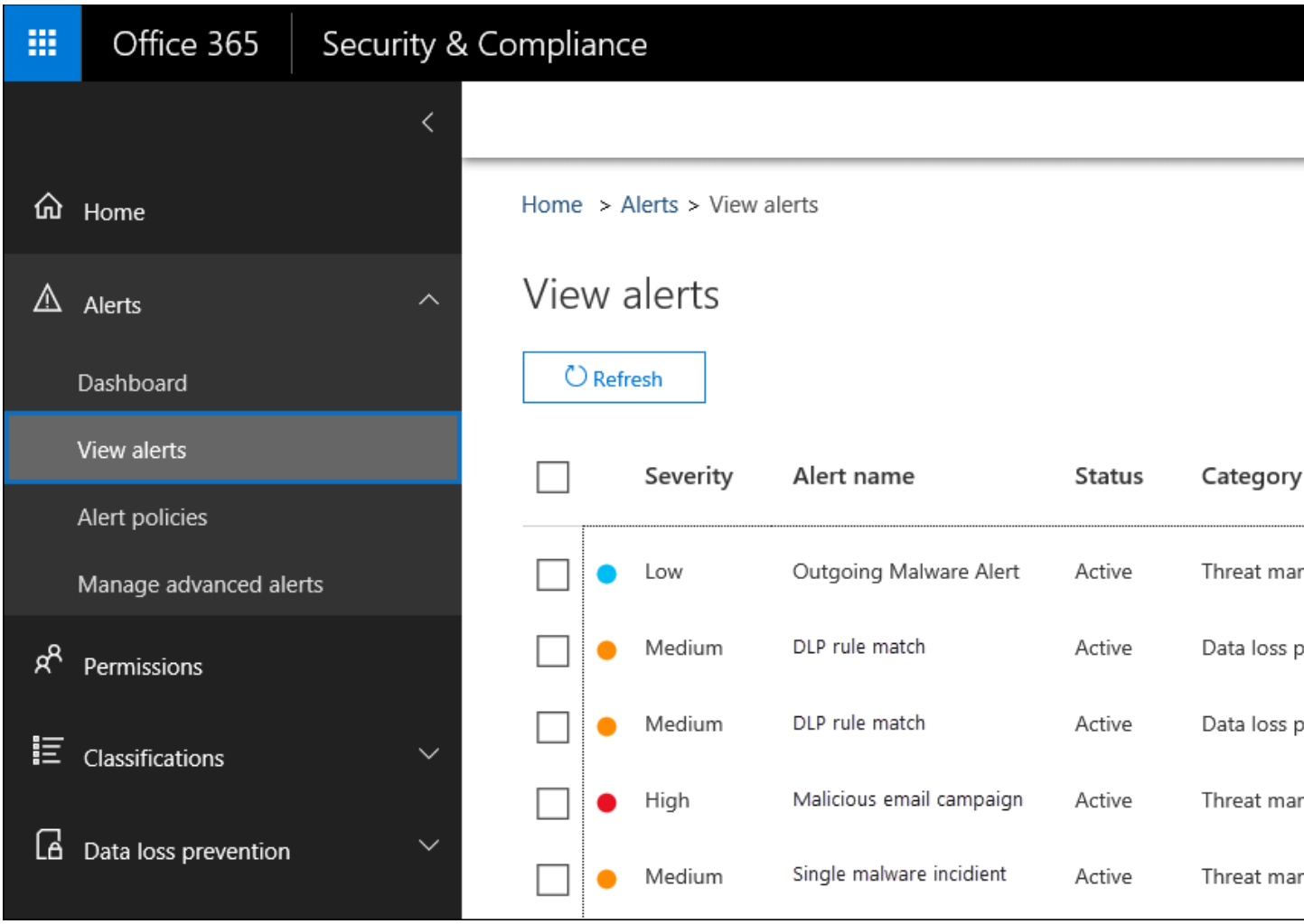
[2] To recreate this alert policy, follow the guidance in the previous footnote, but choose User impersonation as the only Detection technology.

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. Office 365 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.

Viewing 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 **View alerts** page in the security and compliance center. 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 **View 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 the Managing alerts section.

To view alerts, go to https://protection.office.com and then select **Alerts** > **View alerts**.



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

- **Status.** Use this filter to show alerts that are assigned a particular status. The default status is **Active**. You or other administrators can change the status value.
- **Policy.** Use this filter to show alerts that match the setting of one or more alert policies. Or you can display all alerts for all alert policies.
- **Time range.** Use this filter to show alerts that were generated within a specific date and time range.

- **Severity.** Use this filter to show alerts that are assigned a specific severity.
- **Category.** Use this filter to show alerts from one or more alert categories.
- **Source.** Use this filter to show alerts triggered by alert policies in the security and compliance center or alerts triggered by Office 365 Cloud App Security policies, or both. For more information about Office 365 Cloud App Security alerts, see the Viewing Cloud App Security alerts section.

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 **View alerts** page. How is this accomplished? The management roles assigned to users (based on their membership in role groups in the Security & Compliance Center) determine which alert categories a user can see on the **View 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. The first column in the tables lists all roles in the Security & Compliance Center. A check mark indicates that a user who is assigned that role can view alerts from the corresponding alert category listed in the top row.

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

Table 2

	Information governance	**Data loss prevention**	**Mail flow**	**Permissions**	**Threat management**	**Others**
Audit Logs						
Case Management						
Compliance Administrator	✓	✓		✓		✓
Compliance Search						

Table 2						
	Information governance	**Data loss prevention**	**Mail flow**	**Permissions**	**Threat management**	**Others**
Device Management						
Disposition Management						
DLP Compliance Management		✓				
Export						
Hold						
Manage Alerts						✓
Organization Configuration						✓
Preview						
Record Management	✓					
Retention Management	✓					
Review						
RMS Decrypt						
Role Management				✓		

Table 2						
	Information governance	**Data loss prevention**	**Mail flow**	**Permissions**	**Threat management**	**Others**
Search And Purge						
Security Administrator		✓		✓	✓	✓
Security Reader		✓		✓	✓	✓
Service Assurance View						
Supervisory Review Administrator						
View-Only Audit Logs						
View-Only Device Management						
View-Only DLP Compliance Management		✓				

Table 2						
	Information governance	**Data loss prevention**	**Mail flow**	**Permissions**	**Threat management**	**Others**
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 Center PowerShell:

PowerShell

```
$RoleGroups = Get-RoleGroup
```

PowerShell

```
$RoleGroups | foreach {Write-Output -InputObject
`r`n,$_.Name,"----------------------"; Get-RoleGroup
$_.Identity | Select-Object -ExpandProperty Roles}
```

You can also view the roles assigned to a role group in the Security & Compliance Center. Go to the **Permissions** page, and select a role group. The assigned roles are listed on the flyout page.

Managing alerts

After alerts have been generated and displayed on the **View alerts** page in the security and compliance center, you can triage, investigate, and resolve them. 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: name of the actual operation that triggered the alert (such as a cmdlet), a description of the activity that triggered the alert, the user (or list of users) who triggered the alert, and the name (and link to) of the corresponding alert policy.
    - 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 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 may not match that actual number of related alerts listed on the View alerts page because more alerts may 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 actual operation (such as "FileDeleted"), and 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 to) 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, Office 365 won't send notifications when activities or events that match the conditions of the alert policy. 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 **View alerts** page.

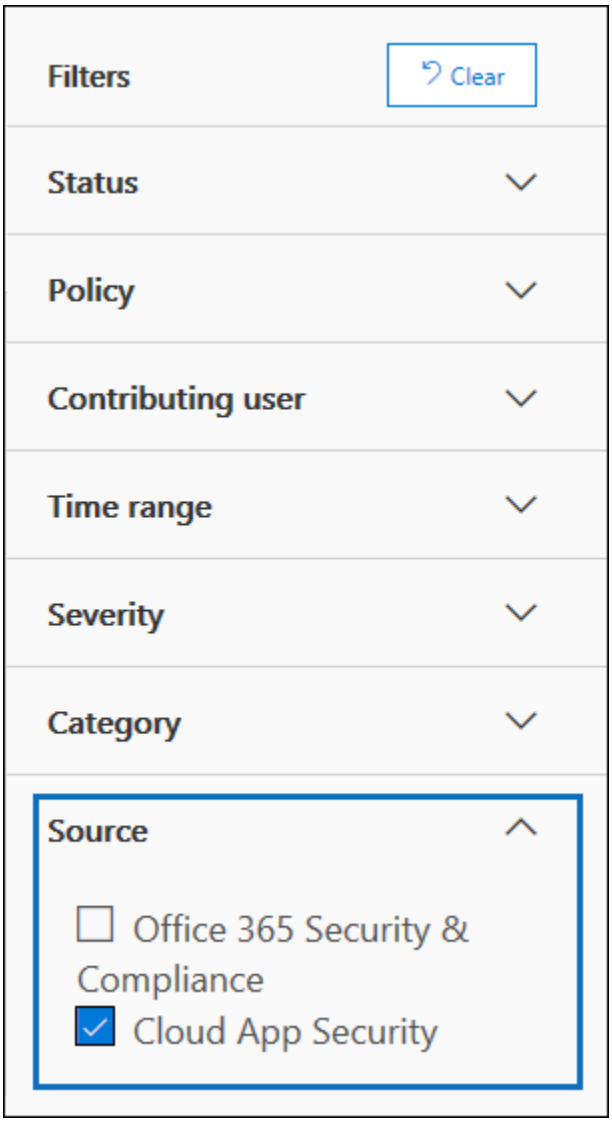
Viewing Cloud App Security alerts

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

Organizations that have Microsoft Cloud App Security as part of an Enterprise Mobility + Security E5 subscription or as a standalone service can also view Cloud

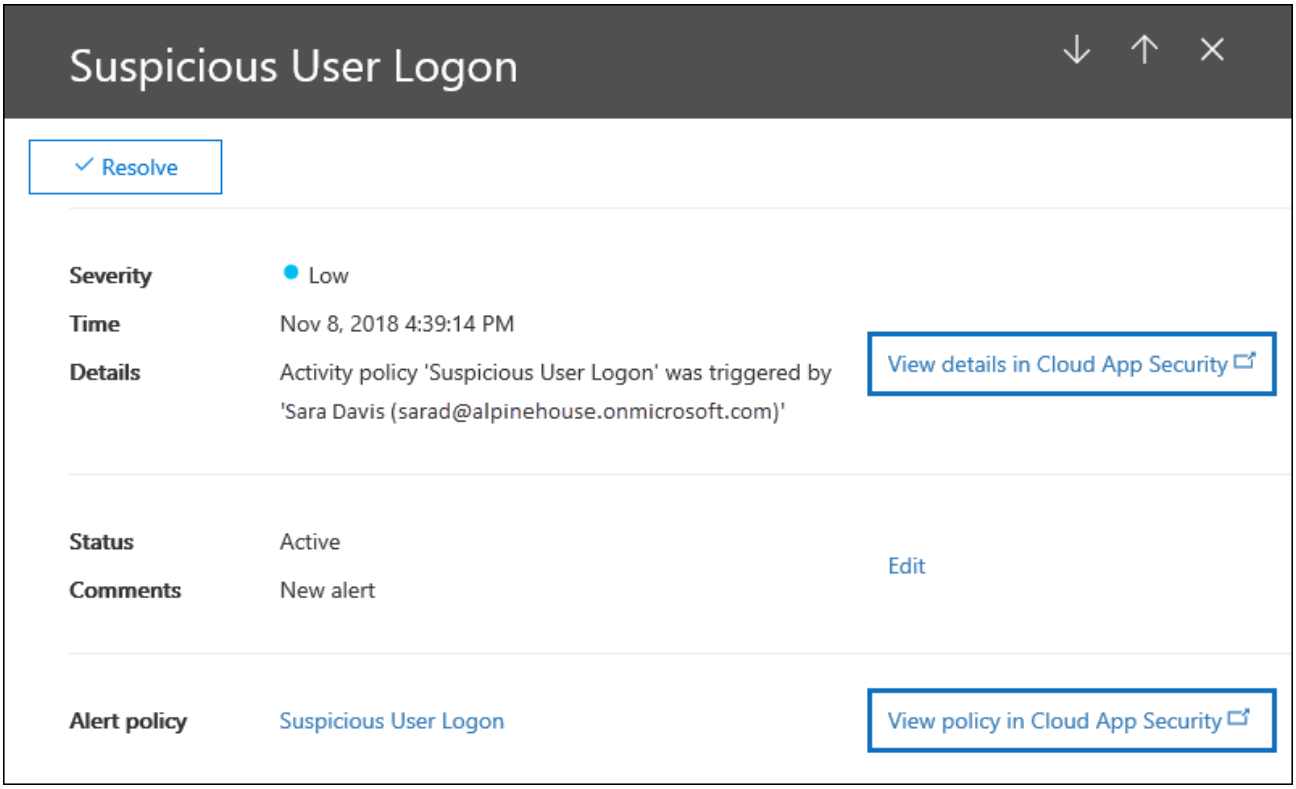
App Security alerts that are related to Office 365 apps and services in the Security & Compliance Center.

To display only Cloud App Security alerts in the security and compliance center, use the **Source** filter and select **Cloud App Security**.



Similar to an alert triggered by an alert policy in the security and compliance center, you can select a Cloud App Security 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 Cloud App Security portal and a link to the corresponding Cloud App Security policy that triggered the alert. See Monitor alerts in Cloud App Security.



Important

Changing the status of a Cloud App Security alert in the security and compliance center won't update the resolution status for the same alert in the Cloud App Security portal. For example, if you mark the status of the alert as **Resolved** in the security and compliance center, the status of the alert in the Cloud App Security portal is unchanged. To resolve or dismiss a Cloud App Security alert, manage the alert in the Cloud App Security portal.