Filter by title

Microsoft Defender for Cloud Apps documentation
- Overview
- Deploy Defender for Cloud Apps
- Cloud app discovery
- Security posture
- Threat protection
  - Control cloud apps with policies
  - Configure threat protection
    - Detect suspicious user activity with UEBA
    - Create activity policies
    - **Create anomaly detection policies**
    - Create OAuth policies
    - Common threat protection policies
  - Configure access and session protection
  - Investigate threats
  - Investigate alerts
  - Respond to threats
- Information protection
- App governance
- Operations guide
- REST API
- Resources
- Microsoft Defender XDR Docs

Create Defender for Cloud Apps anomaly detection policies

Article • 02/28/2024 • 16 contributors

Feedback

In this article

Anomaly detection policies
Enable automated governance
Tune anomaly detection policies
Scope anomaly detection policies
Show 3 more

The Microsoft Defender for Cloud Apps anomaly detection policies provide out-of-the-box user and entity behavioral analytics (UEBA) and machine learning (ML) so that you're ready from the outset to run advanced threat detection across your cloud environment. Because they're automatically enabled, the new anomaly detection policies immediately start the process of detecting and collating results, targeting numerous behavioral anomalies across your users and the machines and devices connected to your network. In addition, the policies expose more data from the Defender for Cloud Apps detection engine, to help you speed up the investigation process and contain ongoing threats.

The anomaly detection policies are automatically enabled, but Defender for Cloud Apps has an initial learning period of seven days during which not all anomaly detection alerts are raised. After that, as data is collected from your configured API connectors, each session is compared to the activity, when users were active, IP addresses, devices, and so on, detected over the past month and the risk score of these activities. Be aware that it may take several hours for data to be available from API connectors. These detections are part of the heuristic anomaly detection engine that profiles your environment and triggers alerts with respect to a baseline that was learned on your organization's activity. These detections also use machine-learning algorithms designed to profile the users and sign in pattern to reduce false positives.

Anomalies are detected by scanning user activity. The risk is evaluated by looking at over 30 different risk indicators, grouped into risk factors, as follows:

- Risky IP address
- Login failures
- Admin activity
- Inactive accounts
- Location
- Impossible travel
- Device and user agent
- Activity rate

Based on the policy results, security alerts are triggered. Defender for Cloud Apps looks at every user session on your cloud and alerts you when something happens that is different from the baseline of your organization or from the user's regular activity.

In addition to native Defender for Cloud Apps alerts, you'll also get the following detection alerts based on information received from Microsoft Entra ID Protection:

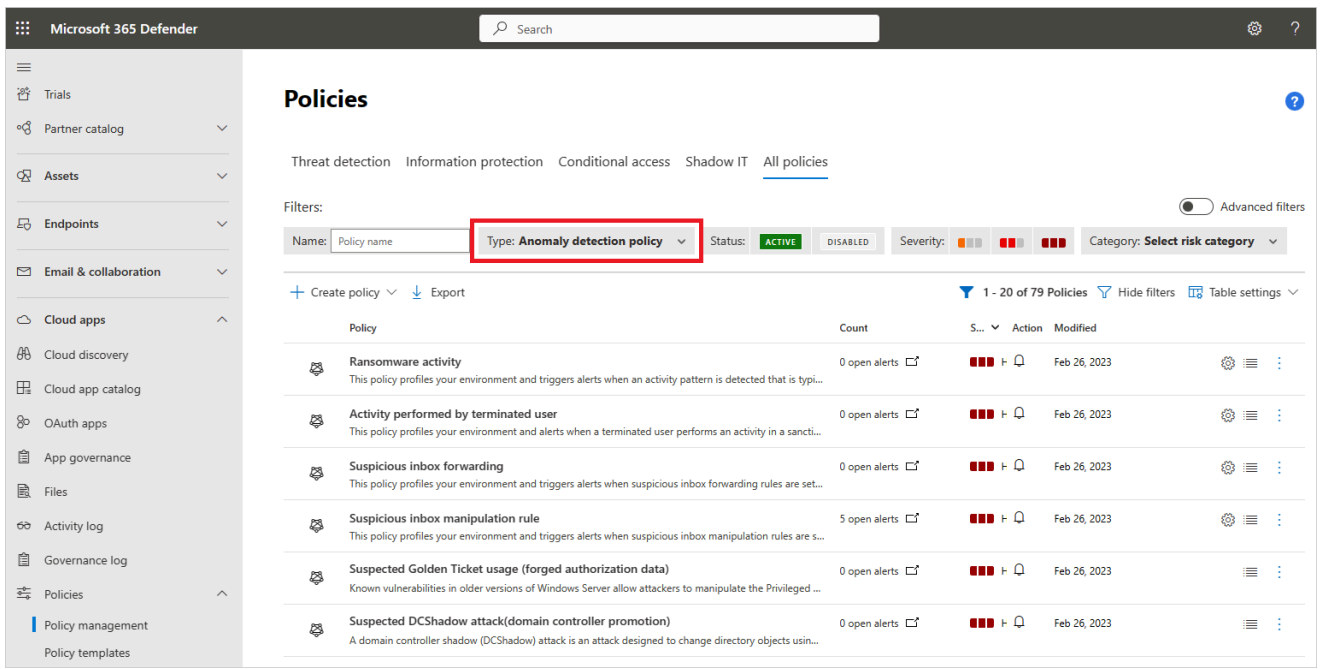
Download PDF

- Leaked credentials: Triggered when a user's valid credentials have been leaked. For more information, see Microsoft Entra ID's Leaked credentials detection.
- Risky sign-in: Combines a number of Microsoft Entra ID Protection sign-in detections into a single detection. For more information, see Microsoft Entra ID's Sign-in risk detections.

These policies will appear on the Defender for Cloud Apps policies page and can be enabled or disabled.

Anomaly detection policies

You can see the anomaly detection policies in the Microsoft Defender Portal, by going to **Cloud Apps** -> **Policies** -> **Policy management**. Then choose **Anomaly detection policy** for the policy type.



The following anomaly detection policies are available:

Impossible travel

- This detection identifies two user activities (in a single or multiple sessions) originating from geographically distant locations within a time period shorter than the time it would have taken the user to travel from the first location to the second, indicating that a different user is using the same credentials. This detection uses a machine-learning algorithm that ignores obvious "false positives" contributing to the impossible travel condition, such as VPNs and locations regularly used by other users in the organization. The detection has an initial learning period of seven days during which it learns a new user's activity pattern. The impossible travel detection identifies unusual and impossible user activity between two locations. The activity should be unusual enough to be considered an indicator of compromise and worthy of an alert. To make this work, the detection logic includes different levels of suppression to address scenarios that can trigger false positive, such as VPN activities, or activity from cloud providers that don't indicate a physical location. The sensitivity slider allows you to affect the algorithm and define how strict the detection logic is. The higher the sensitivity level, fewer activities will be suppressed as part of the detection logic. In this way, you can adapt the detection according to your coverage needs and your SNR targets.

> **Note**
> - When the IP addresses on both sides of the travel are considered safe and sensitivity slider is not set to **High**, the travel is trusted and excluded from triggering the Impossible travel detection. For example, both sides are considered safe if they are tagged as corporate. However, if the IP address of only one side of the travel is considered safe, the detection is triggered as normal.

- The locations are calculated on a country/region level. This means that there will be no alerts for two actions originating in the same country/region or in bordering countries/regions.

Activity from infrequent country

- This detection considers past activity locations to determine new and infrequent locations. The anomaly detection engine stores information about previous locations used by the user. An alert is triggered when an activity occurs from a location that wasn't recently or never visited by the user. To reduce false positive alerts, the detection suppresses connections that are characterized by common preferences to the user.

Malware detection

This detection identifies malicious files in your cloud storage, whether they're from your Microsoft apps or third-party apps. Microsoft Defender for Cloud Apps uses Microsoft's threat intelligence to recognize whether certain files that match risks heuristics such as file type and sharing level are associated with known malware attacks and are potentially malicious. This built-in policy is disabled by default. After malicious files are detected, you can then see a list of **Infected files**. Select the malware file name in the file drawer to open a malware report that provides you with information about the type of malware the file is infected with.

Use this detection to control file uploads and downloads in real time with session policies.

File Sandboxing

By enabling file sandboxing, files that according to their metadata and based on proprietary heuristics to be potentially risky, will also be sandbox scanned in a safe environment. The Sandbox scan may detect files that were not detected based on threat intelligence sources.

Defender for Cloud Apps supports malware detection for the following apps:

- Box
- Dropbox
- Google Workspace

Note

- Proactively sandboxing will be done in third party applications (*Box*, *Dropbox* etc.). In *OneDrive* and *SharePoint* files are being scanned and sandboxed as part of the service itself.
- In *Box*, *Dropbox*, and *Google Workspace*, Defender for Cloud Apps doesn't automatically block the file, but blocking may be performed according to the app's capabilities and the app's configuration set by the customer.
- If you're unsure about whether a detected file is truly malware or a false positive, go to the Microsoft Security Intelligence page at https://www.microsoft.com/wdsi/filesubmission and submit the file for further analysis.

Activity from anonymous IP addresses

- This detection identifies that users were active from an IP address that has been identified as an anonymous proxy IP address. These proxies are used by people who want to hide their device's IP address, and may be used for malicious intent. This detection uses a machine-learning algorithm that reduces "false positives", such as mis-tagged IP addresses that are widely used by users in the organization.

Ransomware activity

- Defender for Cloud Apps extended its ransomware detection capabilities with anomaly detection to ensure a more comprehensive coverage against sophisticated Ransomware attacks. Using our security research expertise to identify behavioral patterns that reflect ransomware activity, Defender for Cloud Apps ensures holistic and robust protection. If Defender for Cloud Apps identifies, for example, a high rate of file uploads or file deletion activities it may represent an adverse encryption process. This data is collected in the logs received from connected APIs and is then combined with learned behavioral patterns and threat intelligence, for example, known ransomware extensions. For more information about how Defender for Cloud Apps detects ransomware, see Protecting your organization against ransomware.

Activity performed by terminated user

- This detection enables you to able to identify when a terminated employee continues to perform actions on your SaaS apps. Because data shows that the greatest risk of insider threat comes from employees who left on bad terms, it's important to keep an eye on the activity on accounts from terminated employees. Sometimes, when employees leave a company, their accounts are de-provisioned from corporate apps, but in many cases they still retain access to certain corporate resources. This is even more important when considering privileged accounts, as the potential damage a former admin can do is inherently greater. This detection takes advantage of the Defender for Cloud Apps ability to monitor user behavior across apps, allowing identification of the regular activity of the user, the fact that the account was deleted, and actual activity on other apps. For example, an employee whose Microsoft Entra account was deleted, but still has access to the corporate AWS infrastructure, has the potential to cause large-scale damage.

The detection looks for users whose accounts were deleted in Microsoft Entra ID, but still perform activities in other platforms such as AWS or Salesforce. This is especially relevant for users who use another account (not their primary single sign-on account) to manage resources, since these accounts are often not deleted when a user leaves the company.

Activity from suspicious IP addresses

- This detection identifies that users were active from an IP address identified as risky by Microsoft Threat Intelligence. These IP addresses are involved in malicious activities, such as performing password spray, Botnet C&C, and may indicate compromised account. This detection uses a machine-learning algorithm that reduces "false positives", such as mis-tagged IP addresses that are widely used by users in the organization.

Suspicious inbox forwarding

- This detection looks for suspicious email forwarding rules, for example, if a user created an inbox rule that forwards a copy of all emails to an external address.

> **Note**
>
> Defender for Cloud Apps only alerts you for each forwarding rule that is identified as suspicious, based on the typical behavior for the user.

Suspicious inbox manipulation rules

- This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user's inbox. This may indicate that the

user's account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.

Suspicious email deletion activity (Preview)

- This policy profiles your environment and triggers alerts when a user performs suspicious email deletion activities in a single session. This policy may indicate that a user's mailboxes may be compromised by potential attack vectors such as command-and-control communication (C&C/C2) over email.

> **Note**
>
> Defender for Cloud Apps integrates with Microsoft Defender XDR to provide protection for Exchange online, including URL detonation, malware protection, and more. Once Defender for Microsoft 365 is enabled, you'll start seeing alerts in the Defender for Cloud Apps activity log.

Suspicious OAuth app file download activities

- Scans the OAuth apps connected to your environment and triggers an alert when an app downloads multiple files from Microsoft SharePoint or Microsoft OneDrive in a manner that is unusual for the user. This may indicate that the user account is compromised.

Unusual ISP for an OAuth App

- This policy profiles your environment and triggers alerts when an OAuth app connects to your cloud applications from an uncommon ISP. This policy may indicate that an attacker tried to use a legitimate compromised app to perform malicious activities on your cloud applications.

Unusual activities (by user)

These detections identify users who perform:

- Unusual multiple file download activities
- Unusual file share activities
- Unusual file deletion activities
- Unusual impersonated activities
- Unusual administrative activities
- Unusual Power BI report sharing activities (preview)
- Unusual multiple VM creation activities (preview)
- Unusual multiple storage deletion activities (preview)
- Unusual region for cloud resource (preview)
- Unusual file access

These policies look for activities within a single session with respect to the baseline learned, which could indicate on a breach attempt. These detections leverage a machine-learning algorithm that profiles the users log on pattern and reduces false positives. These detections are part of the heuristic anomaly detection engine that profiles your environment and triggers alerts with respect to a baseline that was learned on your organization's activity.

Multiple failed login attempts

- This detection identifies users that failed multiple login attempts in a single session with respect to the baseline learned, which could indicate on a breach attempt.

Data exfiltration to unsanctioned apps

- This policy is automatically enabled to alert you when a user or IP address uses an app that is not sanctioned to perform an activity that resembles an attempt to exfiltrate information from your organization.

Multiple delete VM activities

- This policy profiles your environment and triggers alerts when users delete multiple VMs in a single session, relative to the baseline in your organization. This might indicate an attempted breach.

Enable automated governance

You can enable automated remediation actions on alerts generated by anomaly detection policies.

1. Select the name of the detection policy in the **Policies** page.
2. In the **Edit anomaly detection policy** window that opens, under **Governance actions** set the remediation actions you want for each connected app or for all apps.
3. Select **Update**.

Tune anomaly detection policies

To affect the anomaly detection engine to suppress or surface alerts according to your preferences:

- In the Impossible Travel policy, you can set the sensitivity slider to determine the level of anomalous behavior needed before an alert is triggered. For example, if you set it to low or medium, it will suppress Impossible Travel alerts from a user's common locations, and if you set it to high, it will surface such alerts. You can choose from the following sensitivity levels:
  - **Low**: System, tenant, and user suppressions
  - **Medium**: System and user suppressions
  - **High**: Only system suppressions

Where:

Expand table

Suppression type	Description
System	Built-in detections that are always suppressed.
Tenant	Common activities based on previous activity in the tenant. For example, suppressing activities from an ISP previously alerted on in your organization.
User	Common activities based on previous activity of the specific user. For example, suppressing activities from a location that is commonly used by the user.

> **Note**
>
> Impossible travel, activity from infrequent countries/regions, activity from anonymous IP addresses, and activity from suspicious IP addresses alerts don't apply on failed logins and non-interactive logins.

Scope anomaly detection policies

Each anomaly detection policy can be independently scoped so that it applies only to the users and groups you want to include and exclude in the policy. For example, you can set the Activity from infrequent county detection to ignore a specific user who travels frequently.

To scope an anomaly detection policy:

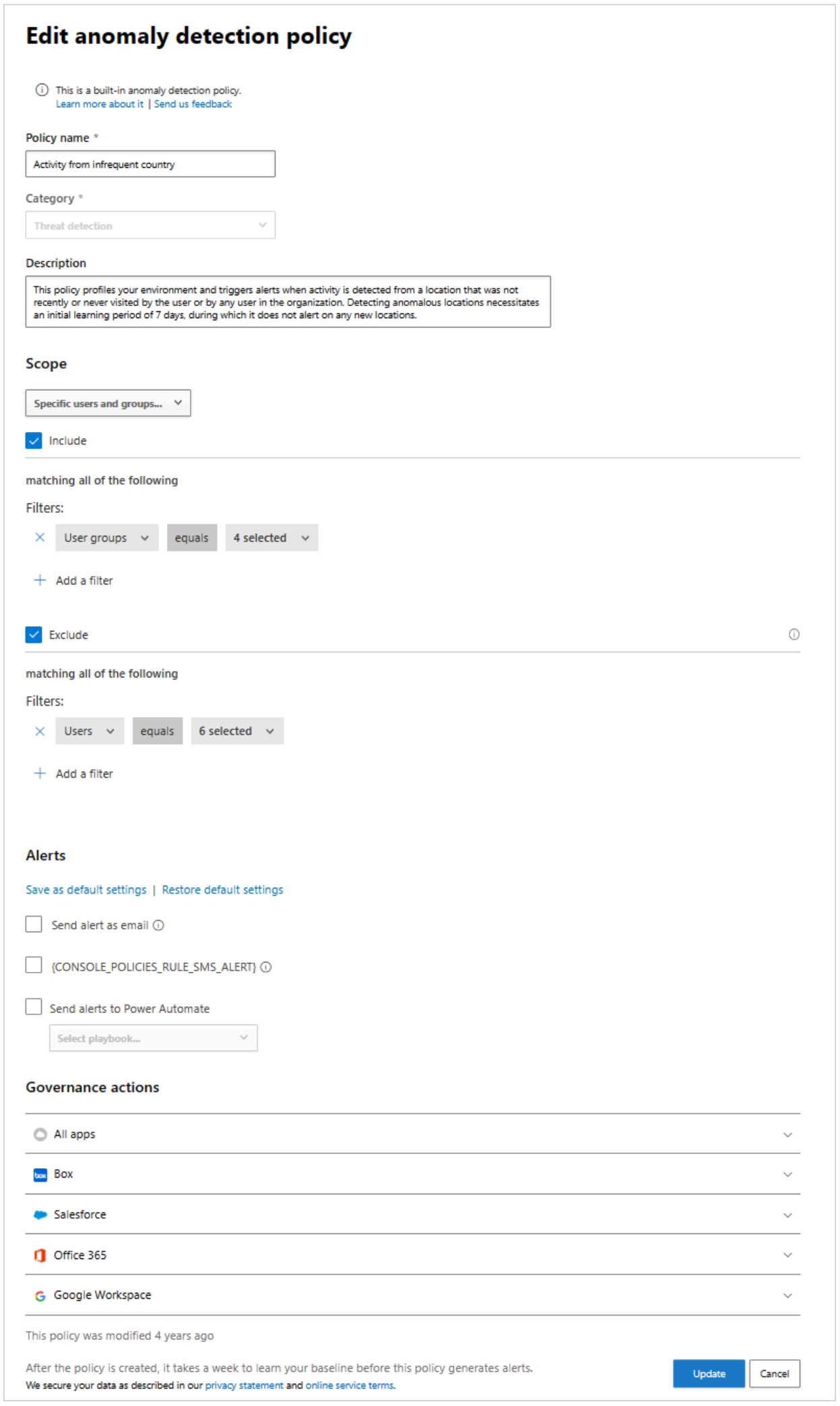
1. In the Microsoft Defender Portal, go to **Cloud Apps** -> **Policies** -> **Policy management**. Then choose **Anomaly detection policy** for the policy type.

2. Select the policy you want to scope.

3. Under **Scope**, change the drop-down from the default setting of **All users and groups**, to **Specific users and groups**.

4. Select **Include** to specify the users and groups for who this policy will apply. Any user or group not selected here won't be considered a threat and won't generate an alert.

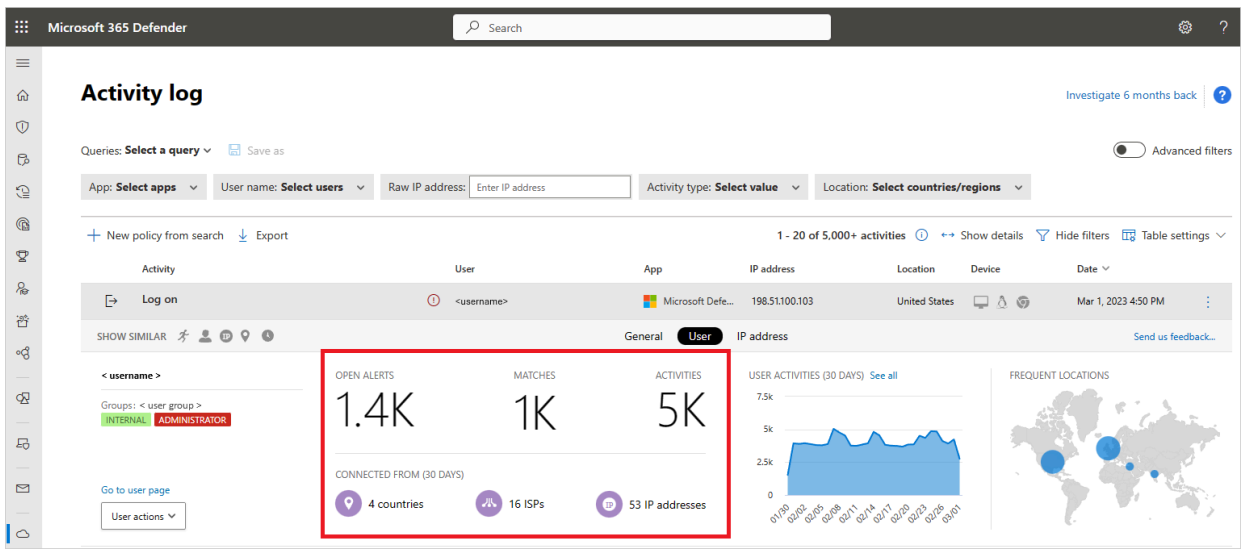
5. Select **Exclude** to specify users for who this policy won't apply. Any user selected here won't be considered a threat and won't generate an alert, even if they're members of groups selected under **Include**.



Triage anomaly detection alerts

You can triage the various alerts triggered by the new anomaly detection policies quickly and decide which ones need to be taken care of first. To do this, you need the context for the alert, so you can see the bigger picture and understand whether something malicious is indeed happening.

1. In the **Activity log**, you can open an activity to display the Activity drawer. Select **User** to view the user insights tab. This tab includes information like number of alerts, activities, and where they've connected from, which is important in an investigation.



2. For malware infected files, After files are detected, you can then see a list of **Infected files**. Select the malware file name in the file drawer to open a malware report that provides you with information about that type of malware the file is infected with.

Related videos

Threat protection webinar

Next steps

Best practices for protecting your organization

If you run into any problems, we're here to help. To get assistance or support for your product issue, please open a support ticket.

Feedback

Was this page helpful? Yes No

Provide product feedback