



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies

Microsoft Ignite

Nov 19–22, 2024

Register now >



Learn

Discover ▾

Product documentation ▾

Development languages ▾

Topics ▾



Sign in

Microsoft Defender

Microsoft Defender products & services ▾

Security resources ▾



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

Overview

Learn / Microsoft Defender for Cloud Apps /



Defender for Cloud Apps policy templates

Article • 09/23/2024 • 11 contributors

Feedback

In this article

[Policy template highlights](#)

[View the full list of policy templates](#)

[Next steps](#)

Supported policy templates

Troubleshoot policies


- > Configure threat protection
- > Configure access and session protection

 Download PDF

We recommend that you simplify policy creation by starting with existing templates whenever possible. This article lists several policy templates available with Microsoft Defender for Cloud Apps.

For the full list of templates, check the Microsoft Defender Portal.

Policy template highlights

 Expand table

| Risk category | Template name | Description |
|-----------------|------------------------------------|--|
| Cloud discovery | Collaboration app compliance check | Alert when new collaboration apps are discovered that aren't compliant with SOC2 and SSAE 16, and are used by more than 50 users with a total daily use of more than 50 MB. |
| Cloud discovery | Cloud storage app compliance check | Alert when new cloud storage apps are discovered that aren't compliant with SOC2, SSAE 16, ISAE 3402 and PCI DSS, and are used by more than 50 users with total daily use of more than 50 MB. |
| Cloud discovery | CRM app compliance check | Alert when new CRM apps are discovered that aren't compliant with SOC2, SSAE 16, ISAE 3402, ISO 27001 and HIPAA, and are used by more than 50 users with a total daily use of more than 50 MB. |
| Cloud discovery | New cloud storage app | Alert when new cloud storage apps are discovered that are used by more than 50 users with total daily use of more than 50 MB. |
| Cloud discovery | New code hosting app | Alert when new code hosting apps are discovered that are used by more than 50 users with total daily use of more than 50 MB. |

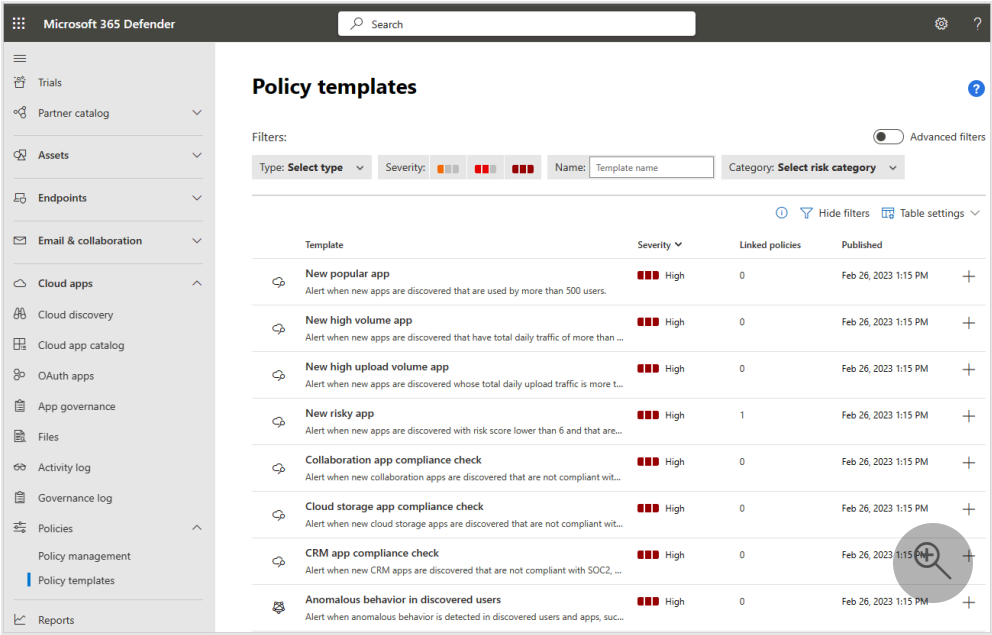
| | | |
|-----------------|-----------------------------------|--|
| Cloud discovery | New collaboration app | Alert when new collaboration apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB. |
| Cloud discovery | New CRM app | Alert when new CRM apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB. |
| Cloud discovery | New high volume app | Alert when new apps are discovered that have total daily traffic of more than 500 MB. |
| Cloud discovery | New high upload volume app | Alert when new apps are discovered whose total daily upload traffic is more than 500 MB. |
| Cloud discovery | New Human-Resource Management app | Alert when newly discovered Human-Resource Management apps are used by more than 50 users with a total daily use of more than 50 MB. |
| Cloud discovery | New online meeting app | Alert when new online meeting apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB. |
| Cloud discovery | New popular app | Alert when new apps are discovered that are used by more than 500 users. |
| Cloud discovery | New risky app | Alert when new apps are discovered with risk score lower than 6 and that are used by more than 50 users with a total daily use of more than 50 MB. |
| Cloud discovery | New sales app | Alert when new sales apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB. |
| Cloud discovery | New vendor management system apps | Alert when new vendor management system apps are discovered that are used by more than 50 users with a total daily use of more than 50 MB. |

| | | |
|------------------|---|--|
| DLP | Externally shared source code | Alert when a file containing source code is shared outside your organization. |
| DLP | File containing PCI detected in the cloud (built-in DLP engine) | Alert when a file with payment card information (PCI) is detected by the Microsoft Defender for Cloud Apps built-in data loss prevention (DLP) engine in a sanctioned cloud app. |
| DLP | File containing PHI detected in the cloud (built-in DLP engine) | Alert when a file with protected health information (PHI) is detected by the Microsoft Defender for Cloud Apps built-in data loss prevention (DLP) engine in a sanctioned cloud app. |
| DLP | File containing private information detected in the cloud (built-in DLP engine) | Alert when a file with personal data is detected by the Microsoft Defender for Cloud Apps built-in data loss prevention (DLP) engine in a sanctioned cloud app. |
| Threat detection | Administrative activity from a non-corporate IP address | Alert when an admin user performs an administrative activity from an IP address that isn't included in the corporate IP address range category. First configure your corporate IP addresses by going to the Settings page, and setting IP address ranges . |
| Threat detection | Log on from a risky IP address | Alert when a user signs into your sanctioned apps from a risky IP address. By default, the Risky IP address category contains addresses that have IP address tags of Anonymous proxy, TOR, or Botnet. You can add more IP addresses to this category in the IP address ranges settings page. |
| Threat detection | Mass download by a single user | Alert when a single user performs more than 50 downloads within 1 minute. |
| Threat detection | Multiple failed user sign-in attempts to an app | Alert when a single user tries to sign in to a single app and fails more than 10 times within 5 minutes. |

| | | |
|------------------|---|--|
| Threat detection | Potential ransomware activity | Alert when a user uploads files to the cloud that might be infected with ransomware. |
| Sharing control | File shared with personal email addresses | Alert when a file is shared with a user's personal email address. |
| Sharing control | File shared with unauthorized domain | Alert when file is shared with an unauthorized domain (such as your competitor). |
| Sharing control | Shared digital certificates (file extensions) | Alert when a file containing digital certificates is publicly shared. Use this template to help govern your AWS storage. |
| Sharing control | Publicly accessible S3 buckets (AWS) | Alert when an AWS S3 bucket is publicly shared. |

View the full list of policy templates

To see the full list of policy templates, in the Microsoft Defender Portal, under **Cloud Apps**, go to **Policies -> Policy templates**. For example:



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](#)

 English (United States)

 Your Privacy Choices


 Theme 

[Manage cookies](#)


[Previous Versions](#)

[Blog](#) 

[Contribute](#)

[Privacy](#) 

[Terms of Use](#)

[Trademarks](#) 

© Microsoft 2024