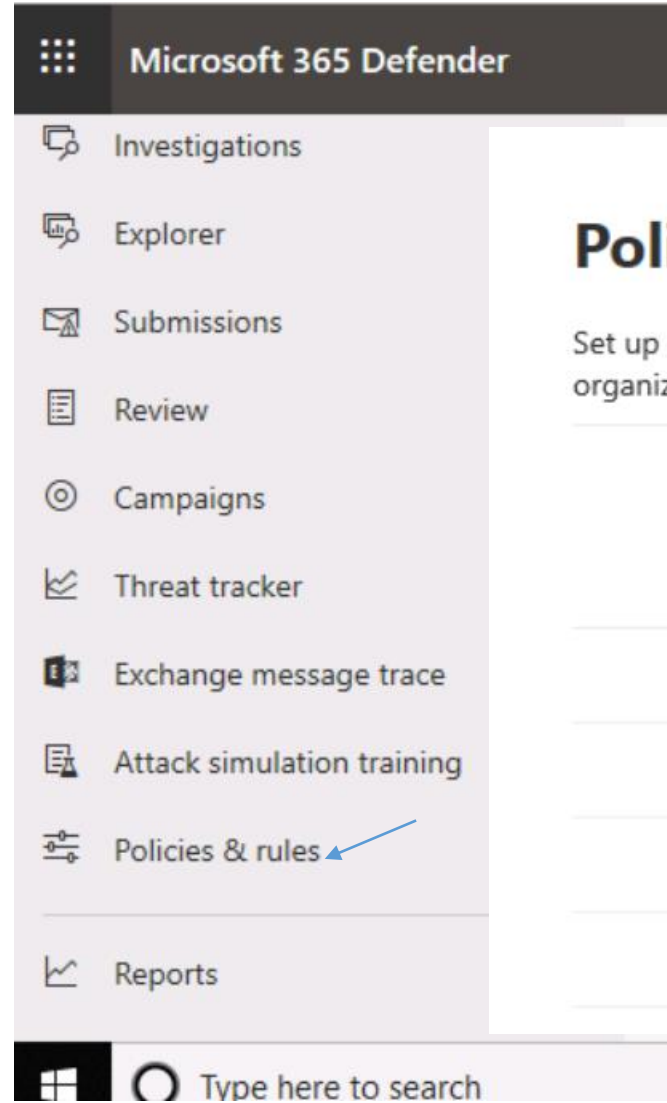
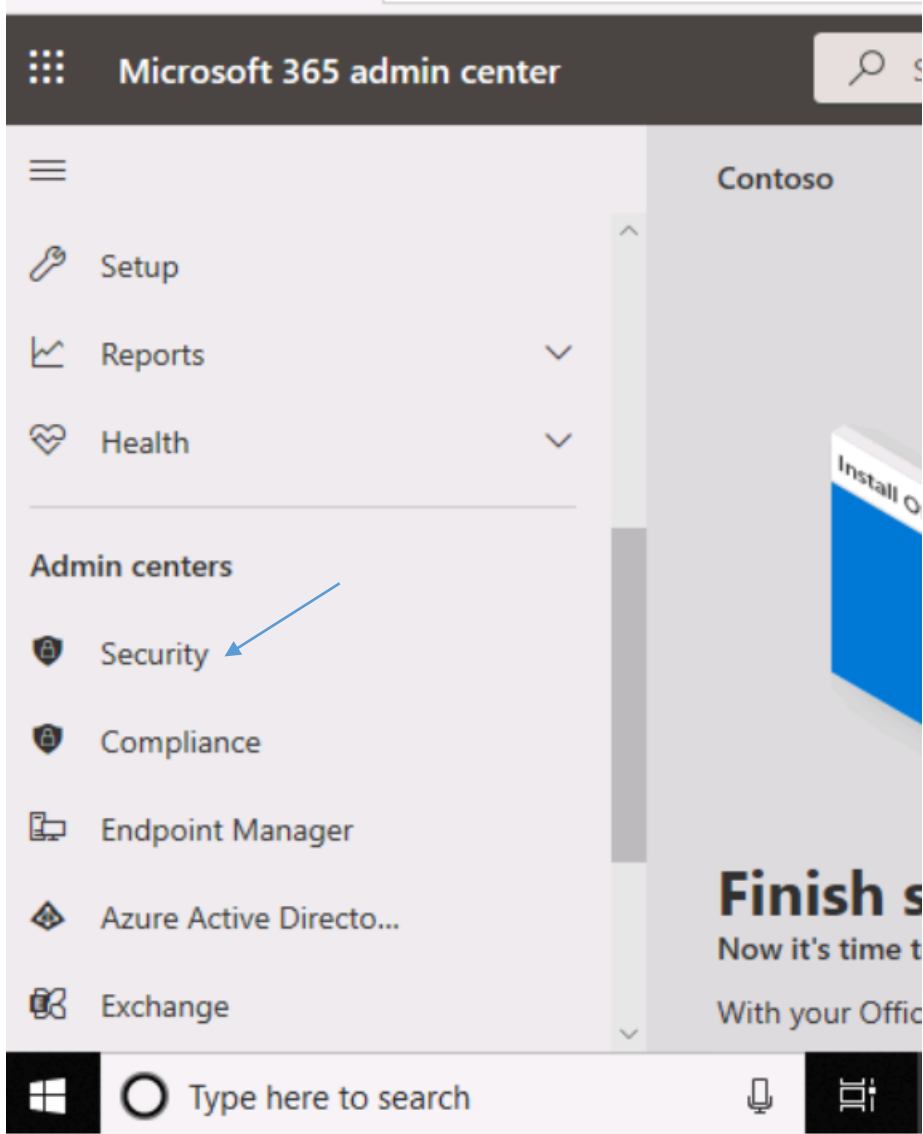


Cloud App security

To deploy Cloud App Security, you must follow these steps to set up and get started investigating your applications:

- Step 1 - Set up Cloud Discovery
- Step 2 - Set instant visibility, protection, and governance actions for your apps
- Step 3 - Control cloud apps with policies
- Step 4 - Personalize your experience
- Step 5 - Organize the data according to your needs



Policies & rules

Set up policies to manage devices, protect against the organization. [Learn more](#)

Name
Threat policies
Alert policy
Manage advanced alerts
Activity alerts

Manage advanced alerts



Your subscription allows you to use Office 365 Cloud App Security!

Take advantage of features such as:

- Behavioral analytics (UEBA) - Detect, investigate, and remediate advanced threats such as compromised users, insider threats, exfiltration, and ransomware using best-of-class machine learning algorithms
- Cloud discovery - Identify Shadow IT and gain instant visibility into how Office 365 and other productivity cloud services are used in your organization
- OAuth apps - Detect malicious apps, identify overprivileged apps, investigate and control suspicious apps in your Office 365 environment
- Conditional Access App Control - Get real-time session monitoring and control for your Office 365 apps

[Go to Office 365 Cloud App Security](#)

[Learn more about Office 365 Cloud](#)

App Security

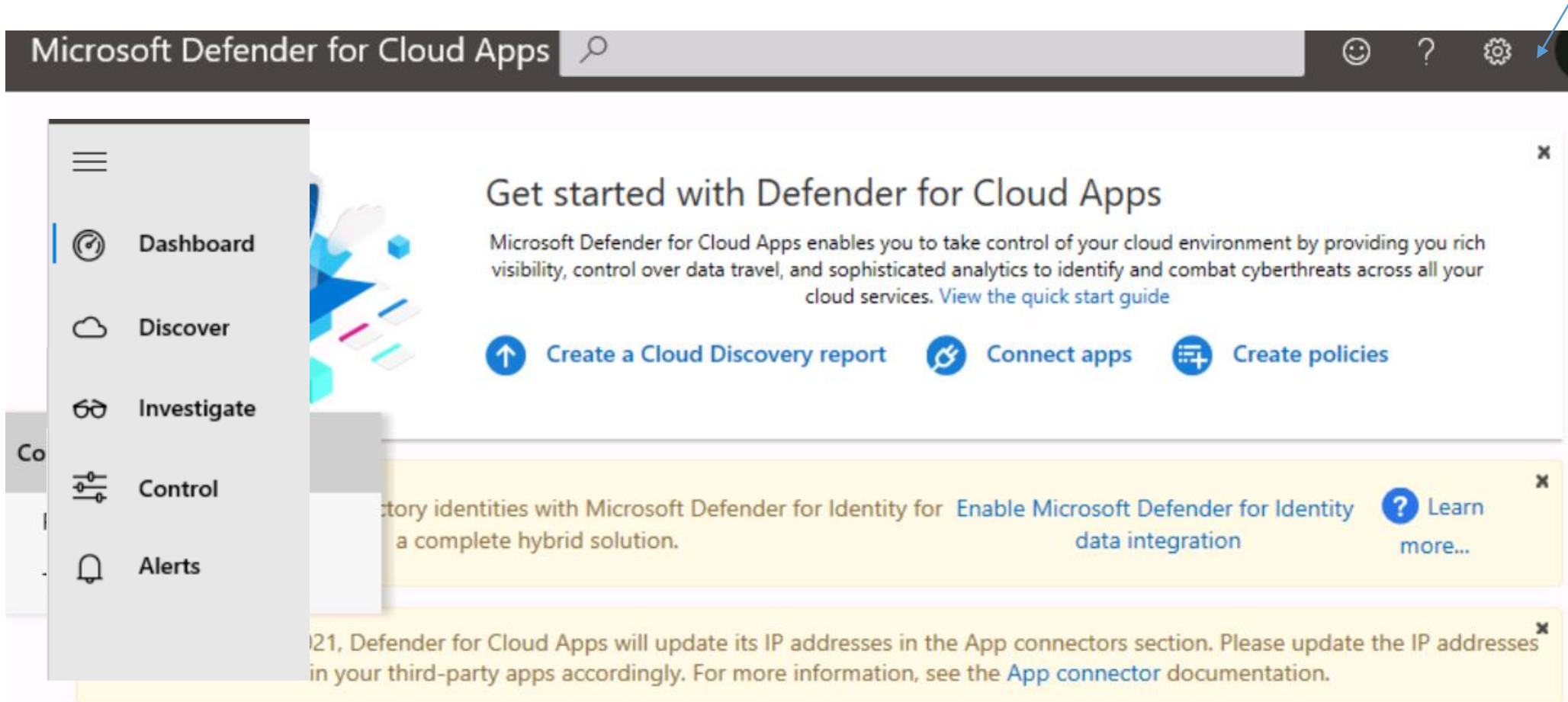
Office 365 Cloud App Security is powered by Microsoft Defender for Cloud Apps service which is a separate online service

- [Privacy & Cookies](#)
- [Terms](#)



STEP 1

The following steps allow you to configure Cloud Discovery logs: 1. In the Cloud App Security dashboard <https://portal.cloudappsecurity.com>, from the settings cog, select Settings. 2. Choose Automatic log upload. 3. On the Data sources tab, add your sources. 4. On the Log collectors tab, configure the log collector



The screenshot shows the Microsoft Defender for Cloud Apps dashboard. At the top, there is a dark header with the text "Microsoft Defender for Cloud Apps" and a search icon. To the right of the header are icons for a smiley face, a question mark, and a gear (settings), with a blue arrow pointing to the gear icon. A settings menu is open on the left side, listing the following options: Dashboard, Discover, Investigate, Control, and Alerts. The main content area features a "Get started with Defender for Cloud Apps" section with a sub-header and a paragraph of text. Below this are three buttons: "Create a Cloud Discovery report", "Connect apps", and "Create policies". There are also two yellow notification banners at the bottom of the page.

Microsoft Defender for Cloud Apps

Get started with Defender for Cloud Apps

Microsoft Defender for Cloud Apps enables you to take control of your cloud environment by providing you rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services. [View the quick start guide](#)

[Create a Cloud Discovery report](#) [Connect apps](#) [Create policies](#)

...ory identities with Microsoft Defender for Identity for [Enable Microsoft Defender for Identity](#) [Learn more...](#)

...21, Defender for Cloud Apps will update its IP addresses in the App connectors section. Please update the IP addresses in your third-party apps accordingly. For more information, see the [App connector](#) documentation.

Microsoft Defender for Cloud Apps

Get started with Defender for Cloud Apps

Microsoft Defender for Cloud Apps enables you to take control of your cloud services. [View the quick start guide](#)

[Create a Cloud Discovery report](#) [Connect apps](#)

① Protect your Azure Directory identities with Microsoft Defender for Identity for [Enable Microsoft Defender for Identity](#) a complete hybrid solution.

On December 20, 2021, Defender for Cloud Apps will update its IP addresses in the App connectors section in your third-party apps accordingly. For more information, see the [App connectors](#)

Dashboard

- SYSTEM
 - Settings
 - Governance log
 - Security extensions
 - Manage admin access
 - Exported reports
 - Scoped deployment and privacy
- SOURCES
 - Log collectors
 - App connectors
 - Conditional Access App Control
- DATA ENRICHMENT
 - IP address ranges
 - User groups



System

Organization details

Mail settings

Export settings

Automatic sign out

Activity privacy

Cloud Discovery

Score metrics

Snapshot reports

Continuous reports

Automatic log upload



Organization details

Configure your organization's details

Organization display name ⓘ

Environment name ⓘ

Organization logo ⓘ

Managed domains ⓘ



Search

System

Organization details

Mail settings

Export settings

Automatic sign out

Activity privacy

Cloud Discovery

Score metrics

Snapshot reports

Continuous reports

Automatic log upload

Automatic log upload



Data sources

Log collectors

Create and manage your organization's data sources.

[Terms](#) | [Privacy statement](#)



+ Add data source...

No data sources found

Table settings

N..	S...	R	Uploaded logs	Last data received	Modified date
-----	------	---	---------------	--------------------	---------------

Add data source

Name *


Source *

[View sample of expected log file](#), and compare it with yours

Receiver type *

Anonymize private information
Store and display only encrypted usernames.

Comment



Search

System

Organization details

Mail settings

Export settings

Automatic sign out

Activity privacy

Cloud Discovery

Score metrics

Snapshot reports

Continuous reports

Automatic log upload

Automatic log upload



Data sources Log collectors

Create and manage your organization's data sources.

[Terms](#) | [Privacy statement](#)



+ Add data source...

1 - 1 of 1 data sources Table settings

N..	S..	R	Uploaded logs	Last data received	Modified date	
	B	0		—	Dec 22, 2021	⋮

Search

System

Organization details

Mail settings

Export settings

Automatic sign out

Activity privacy

Cloud Discovery

Score metrics

Snapshot reports

Continuous reports

Automatic log upload



Data sources **Log collectors**

Automatically sanitize, compress and transmit log data to the portal.

To use this feature a log collector machine needs to be deployed.

[Terms](#) | [Privacy statement](#)



+ Add log collector...

No log collectors found [Table settings](#) ▾

Name	Linked data sources	Last data received	Modified date
------	---------------------	--------------------	---------------

Create log collector

Name

Host IP address or FQDN ⓘ

Data source(s)

Create

Close

Next steps:

1. Follow the [deployment guide](#) to install the log collector on your host
2. On the hosting machine, import the collector configuration using:

```
(echo ae8830e83e9fbed99e86418e13cdb52bee0bd6eb6e1a855a0a42f2792ae615c5) | docker run --name Logcollector_hq -p 601:601
```

3. Configure exports from data sources (in your network) to the log collector according to the following:

Export

1 - 1 of 1 data sources Table settings

Name

Barracuda

FTP user:



Remember to copy the command

Make sure you copy the command below - it will not be saved:

```
(echo ae8830e83e9fbed99e86418e13cdb52bee0bd6eb6e1a855a0a42f2792ae615c5) | docker run --name Logcollector_hq -p
```

Close

What do you want to do with
2021-12-22_discovery_data_sources_config.csv?
From: m365x76990664.us3.portal.cloudappsecurity.com

Open

Save

Cancel

System

- Organization details
- Mail settings
- Export settings
- Automatic sign out
- Activity privacy

Cloud Discovery

- Score metrics
- Snapshot reports
- Continuous reports
- Automatic log upload**
- App tags

Data sources **Log collectors**

Automatically sanitize, compress and transmit log data to the portal.

To use this feature a log collector machine needs to be deployed.
[Terms](#) | [Privacy statement](#)



+ Add log collector...

1 - 1 of 1 log collectors [Table settings](#) ▾

Name	Linked data sources	Last data received	Modified date
Lo...	1 data source	—	Dec 22, 2021

Step 2 - Set instant visibility, protection, and governance actions for your apps After you connect an app, you can gain deeper visibility by investigating activities, files, and accounts for the apps in your cloud environment. You must perform the following steps to connect an app:

1. In the Cloud App Security dashboard, from the settings cog, select App connectors.
2. Click the plus sign to add an app and select an app.
3. Follow the configuration steps to connect the app



System

- Organization details
- Mail settings
- Export settings
- Automatic sign out
- Activity privacy

Cloud Discovery

- Score metrics
- Snapshot reports
- Continuous reports
- Automatic log upload**
- App tags

Data sources **Log collectors**

Automatically sanitize, compress and transmit log data to the portal.
To use this feature a log collector machine needs to be deployed.
[Terms](#) | [Privacy statement](#)

+ Add log collector... 1

Name	Linked data sources	Last data received
Lo...	1 data source	—

- SYSTEM
 - Settings
 - Governance log
 - Security extensions
 - Manage admin access
 - Exported reports
 - Scoped deployment and privacy
- SOURCES
 - Log collectors
 - App connectors**
 - Conditional Access App Control
- DATA ENRICHMENT
 - IP address ranges
 - User groups

App connectors provide you with greater visibility and control over your cloud apps.



Filters:

Advanced filters

App: **Select apps** ▾ App category: **Select category** ▾ Connected by: **Select users** ▾

+ Connect an app ^

- Amazon Web Services
- Box
- Cisco Webex
- Dropbox
- GitHub
- Google Cloud Platform

No connected apps found ↔ Show details ⚙ Hide filters 📄 Table settings ▾

Status Was connected on Last activity Accounts ▾

There are no connected apps



Connect Box

Connect Box to enable instant visibility, protection and governance actions.

Instance name:

Connect Box

To connect this app, provide your access credentials. We secure your data as described in the [privacy statement](#) | [Terms](#)



Connect Box

Before you connect Box, we highly recommend reviewing the [Box connection guide](#).


Follow these steps in order to connect Box.

Make sure to provide a user with admin privileges for Box, to enable a full scan of your Box app.

Follow the link

Connect as Box administrator and allow the required permissions.

To connect, [follow this link](#)

 It is strongly recommended that you connect Box as an Admin.
Connecting as a co-admin will result in partial data visibility.

Close



Log in to grant access to **Box**

✉ l65x76990664.onmicrosoft.com

🔒 ●●●●●●●●●● | 🔍

Authorize

[Use Single Sign On \(SSO\)](#)

[Forgot password](#)

By granting MICROSOFT CLOUD APP SECURITY - USW2 access to Box, you are agreeing to Box's [Terms of Service](#) and [Privacy Policy](#).

Step 3 - Control cloud apps with policies You can use policies to help monitor trends, see security threats, and generate customized reports and alerts. With policies, you can create governance actions and set data loss prevention and filesharing controls.

To create a policy, you must perform the following steps:

1. In the Cloud App Security dashboard, go to Control > Templates.
2. Select a policy template from the list, and then click (+) Create policy.
3. Customize the policy (select filters, actions, and other settings), and then click Create.
4. On the Policies tab, choose the policy to see the relevant matches (activities, files, alerts). Tip: To cover all your cloud environment security scenarios, create a policy for each risk category.

Microsoft 365 admin center

Contoso

- Setup
- Reports
- Health

Admin centers

- Security
- Compliance
- Endpoint Manager
- Azure Active Directo...
- Exchange

Finish s
Now it's time t
With your Offic

Type here to search

Microsoft 365 Defender

- Investigations
- Explorer
- Submissions
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules
- Reports

Type here to search

Policies & rules

Set up policies to manage devices, protect against the organization. [Learn more](#)

Name
Threat policies
Alert policy
Manage advanced alerts
Activity alerts



Your subscription allows you to use Office 365 Cloud App Security!

Take advantage of features such as:

- Behavioral analytics (UEBA) - Detect, investigate, and remediate advanced threats such as compromised users, insider threats, exfiltration, and ransomware using best-of-class machine learning algorithms
- Cloud discovery - Identify Shadow IT and gain instant visibility into how Office 365 and other productivity cloud services are used in your organization
- OAuth apps - Detect malicious apps, identify overprivileged apps, investigate and control suspicious apps in your Office 365 environment
- Conditional Access App Control - Get real-time session monitoring and control for your Office 365 apps



[Go to Office 365 Cloud App Security](#)

[Learn more about Office 365 Cloud](#)



Dashboard



Discover



Investigate



Control



Alerts

Get started with Defender for Cloud Apps

Microsoft Defender for Cloud Apps enables you to take control of your cloud environment by providing you rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services. [View the quick start guide](#)



Create a Cloud Discovery report



Connect apps



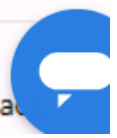
Create policies

...ory identities with Microsoft Defender for Identity for a complete hybrid solution. [Enable Microsoft Defender for Identity data integration](#)



Learn more...

...fender for Cloud Apps will update its IP addresses in the App connectors section. Please update the IP addresses of third-party apps accordingly. For more information, see the [App connector](#) documentation.





Dashboard



Discover



Investigate



Control



Policies

Templates



Alerts

Get started with Defender for Cloud Apps

Microsoft Defender for Cloud Apps enables you to take control of your cloud environment by providing you rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services. [View the quick start guide](#)



Create a Cloud Discovery report



Connect apps



Create policies

...tory identities with Microsoft Defender for Identity for [Enable Microsoft Defender for Identity data integration](#) a complete hybrid solution.



Learn more...

...fender for Cloud Apps will update its IP addresses in the App connectors section. Please update the IP addresses of third-party apps accordingly. For more information, see the [App connector](#) documentation.



Type: **Select type** ▾







Severity: ■ ■ ■ ■

Name:

Category: **Select risk category** ▾

Alert when a single user attempts to log on to a single app, and fails more than 10 times within 5 minutes.

1 - 20 of 38 Templates [Hide filters](#) [Table settings](#) ▾

Template	Severity ▾	Linked policies	Published	
 File shared with unauthorized domain Alert when a file is shared with an unauthorized domain (such a...	■ ■ ■	0	Dec 23, 2021, 7:03 ...	+
 Mass download by a single user Alert when a single user performs more than 50 downloads wit...	■ ■ ■	0	Dec 23, 2021, 7:03 ...	+
 Multiple failed user log on attempts to an app Alert when a single user attempts to log on to a single app, an...	■ ■ ■	0	Dec 23, 2021, 7:03 ...	+
 New popular app Alert when new apps are discovered that are used by more tha...	■ ■ ■	0	Dec 23, 2021, 7:03 ...	+
 New high volume app Alert when new apps are discovered that have total daily traffic...	■ ■ ■	0	Dec 23, 2021, 7:03 ...	+
 New high upload volume app Alert when new apps are discovered whose total daily upload tr...	■ ■ ■	0	Dec 23, 2021, 7:03 ...	+

Create activity policy

Policy template *

Multiple failed user log on attempts to an ... ▾

Policy name *

Multiple failed user log on attempts to an app

Policy severity *



Category *

Threat detection ▾

Description

Alert when a single user attempts to log on to a single app, and fails more than 10 times within 5 minutes.

Create filters for the policy

Act on:

Single activity
Every activity that matches the filters

Repeated activity:
Repeated activity by a single user

Minimum repeated activities:

Within timeframe:

minutes

In a single app






Count only unique target files or folders
per user ⓘ








Activities matching all of the following


[👁 Edit and preview results](#)

Activities matching all of the following

 Edit and preview results

 User  From domain  equals  adatum 

 User  Name  is set  as  Any role  

 Add a filter

Alerts

Create an alert for each matching event with the policy's severity

[Save as default settings](#) | [Restore default settings](#)

Send alert as email 

Jane@adatum.com 

Send alert as text message 

- Send alerts to Power Automate
[Create a playbook in Power Automate](#)

Governance actions

All apps



We secure your data as described in our [privacy statement](#) and [online service terms](#).

Create

Cancel

Policies



Threat detection Information protection Conditional access Shadow IT All policies

Filters:

Advanced filters

Name:

Type: **Activity policy** ▾

Status: **ACTIVE**

DISABLED

Severity:




Category: **Select risk category** ▾

[+ Create policy](#) ▾ [↓ Export](#)

1 - 1 of 1 Policies

[Hide filters](#)

[Table settings](#) ▾

Policy	Count	Severity ▾	Action	Modified	
 Multiple failed user log on attempts to an app Alert when a single user attempts to log on to a single ap...	0 open alerts			Dec 23, 2021	