

Manage and monitor Security
Dashboard using Microsoft 365
Defender Portal

- The Security & Compliance Center at <https://protection.office.com> enables your organization to manage data protection and compliance.
- Security Dashboard enables you to review your Threat Protection Status, as well as view and act on security alerts.
- You must be a global administrator, a security administrator, or a security reader to view the Security Dashboard. Some widgets require additional permissions to view.

Microsoft 365 admin center

Search (Alt + S)

Contoso

- Billing
- Support
- Settings
- Setup
- Reports
- Health

Admin centers

- Security
- Compliance
- Endpoint Manager

Install Office

Add domain

Add users

Connect domain

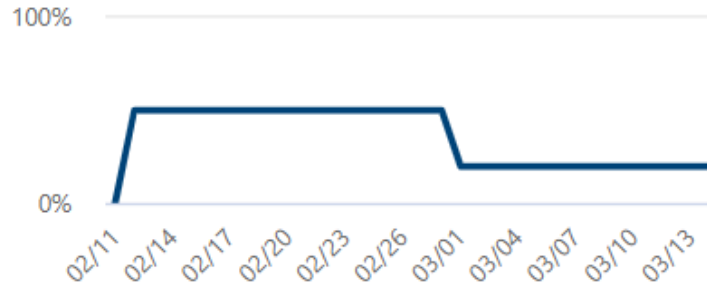
+ Add cards

Secure Score: 19.7%

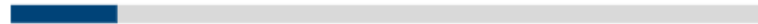
13/66 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 03/14



Identity **14.29%**



Apps **50%**



[Improve your score](#) [View history](#)

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Applied filters:


[Export](#)

18 items

[Filter](#)

[Group by](#) ▾

Rank ↑	Improvement action	Score impact	Points achieved	Status	Regressed	Have license?	Category	Product	Last synced	Microsoft update	Notes
1	Require MFA for administrative roles	+15.15%	0/10	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
2	Ensure all users can complete multi-factor authentication for s...	+13.64%	0/9	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
3	Enable policy to block legacy authentication	+12.12%	0/8	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
4	Turn on user risk policy	+10.61%	0/7	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
5	Turn on sign-in risk policy	+10.61%	0/7	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
6	Do not allow users to grant consent to unmanaged applications	+6.06%	0/4	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
7	Configure which users are allowed to present in Teams meetin...	+3.03%	0/2	<input type="radio"/> To address	No	Yes	Apps	Microsoft Teams	3/6/2022	None	None
8	Only invited users should be automatically admitted to Teams ...	+3.03%	1/2	<input type="radio"/> To address	No	Yes	Apps	Microsoft Teams	3/6/2022	None	None
9	Enable self-service password reset	+1.52%	0/1	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
10	Turn on customer lockbox feature	+1.52%	0/1	<input type="radio"/> To address	No	Yes	Apps	Exchange Online	3/15/2022	None	None

11	Use limited administrative roles 	+1.52%	0/1	<input type="radio"/> To address	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
12	Restrict anonymous users from joining meetings	+1.52%	0/1	<input type="radio"/> To address	No	Yes	Apps	Microsoft Teams	3/6/2022	None	None
13	Do not expire passwords	+12.12%	8/8	<input checked="" type="checkbox"/> Completed	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
14	Remove TLS 1.0/1.1 and 3DES dependencies	+1.52%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Apps	Exchange Online	3/15/2022	None	None
15	Designate more than one global admin	+1.52%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Identity	Azure Active Directory	3/15/2022	None	None
16	Restrict dial-in users from bypassing a meeting lobby	+1.52%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Apps	Microsoft Teams	3/6/2022	None	None
17	Limit external participants from having control in a Teams me...	+1.52%	1/1	<input checked="" type="checkbox"/> Completed	No	Yes	Apps	Microsoft Teams	3/6/2022	None	None

Use limited administrative roles

To address

 Edit status & action plan  Manage tags

General Implementation History (0)

Description

Limited administrators are users who have more privileges than standard users, but not as many privileges as global admins. Leveraging limited administrator roles to perform required administrative work reduces the number of high value, high impact global admin role holders you have. Assigning users roles like Password Administrator or Exchange Online Administrator, instead of Global Administrator, reduces the likelihood of a global administrative privileged account being breached.

Implementation status

You have 0 users with limited administrative roles.

User impact

Admins who have been designated alternate roles will lose some of the privileges that they had before (although they might keep some privileges depending on the role). Make sure that these users have enough privileges to complete their day-to-day work.

Users affected

All of your Microsoft 365 global administrators

Details

Points achieved 0/1

History

0 events

Category

Identity

Product

Azure Active Directory

Protects against






[Account Breach](#), [Elevation of Privilege](#),
[Malicious Insider](#)

 [Manage in Microsoft Azure](#)

 Share 

Active users

Recommended actions (1)

 Add a user  User templates  Add multiple users  Multi-factor authentication  Delete a user  Refresh ...  Filter

<input type="checkbox"/>	Display name ↑		Username	Licenses
<input type="checkbox"/>	Alex Wilber	⋮	AlexW@M365x16621225.OnMicrosoft.com	Office 365 E5 , Enterprise Mobility + Security E5
<input type="checkbox"/>	Allan Deyoung	⋮	AllanD@M365x16621225.OnMicrosoft.com	Office 365 E5 , Enterprise Mobility + Security E5
<input type="checkbox"/>	Diego Siciliani	⋮	DiegoS@M365x16621225.OnMicrosoft.com	Office 365 E5 , Enterprise Mobility + Security E5
<input type="checkbox"/>	Isaiah Langer	⋮	IsaiahL@M365x16621225.OnMicrosoft.com	Office 365 E5 , Enterprise Mobility + Security E5



[View last 30 days](#)

Sign-out ⓘ

Sign this user out of all Office 365 sessions.

[Sign out of all sessions](#)

Groups

[Manage groups](#)

Manager

Megan Bowen

[Edit manager](#)

Contact information

Display name

Isaiah Langer

Phone number

Alternate email address

None provided

[Add address](#)

Roles

Global Administrator

[Manage roles](#)



First name

Isaiah

Last name



Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

- Global Administrator ⓘ
- Exchange Administrator ⓘ
- Global Reader ⓘ
- Helpdesk Administrator ⓘ
- Service Support Administrator ⓘ
- SharePoint Administrator ⓘ
- Teams Administrator ⓘ
- User Administrator ⓘ

Help & support

Show all by category



Global readers have read-only access to admin centers, while Global admins have unlimited access to edit all settings. Users assigned other roles are more limited in what they can see and do.

- Global Administrator ⓘ
- Exchange Administrator ⓘ
- Global Reader ⓘ
- Helpdesk Administrator ⓘ
- Service Support Administrator ⓘ
- SharePoint Administrator ⓘ
- Teams Administrator ⓘ
- User Administrator ⓘ

Help & support

Show all by category

Alternate email address

None provided

[Add address](#)

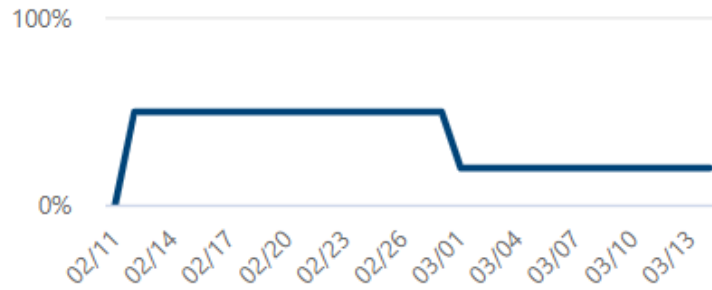
Save changes

Secure Score: 19.7%

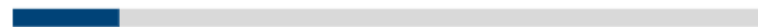
13/66 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 03/14



Identity **14.29%**



Apps **50%**



Improve your score

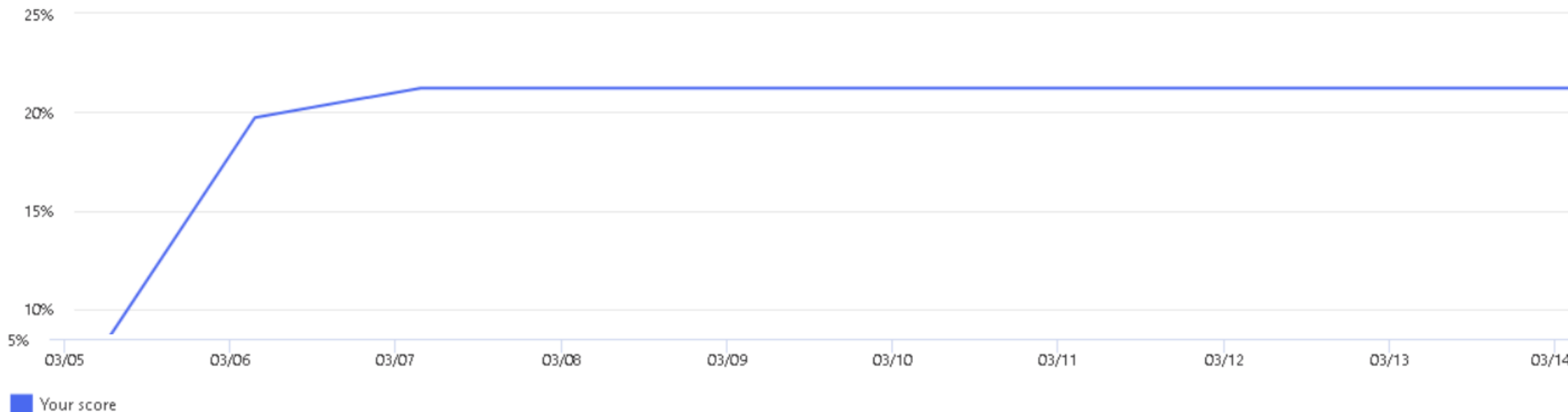
View history



Microsoft Secure Score

Overview Improvement actions **History** Metrics & trends

▲ 14.17%



Applied filters:

Export

3 items

Search

90 days

Filter

Group by

Date/Time	Activity	Resulting points	Category	Attributed to
Mar 7, 2022 4:00 PM	Enable Password Hash Sync if hybrid was removed because it is no longer relevant. Your score ...	0/-5	Identity	System
Mar 6, 2022 4:00 PM	1.00 points gained by completing Designate more than one global admin. Great work!	1/1	Identity	System
Mar 6, 2022 4:00 PM	8.00 points gained by completing Do not expire passwords. Great work!	8/8	Identity	System

Devices with active malware




No affected devices

Intune-managed devices with active, unresolved malware




NA


■ Active ■ No Active Malware

 [View details](#)

Reports > Devices with malware detections

Ensure your devices don't have active, unremediated malware. Check if users have allowed malware to run or if the devices have pending restarts, rescans, or other manual cleanup actions.

0 items  Filter  Group by 

Filters: Malware state: Active 

Device name	Malware state	Active malware	Malware detections	Management status	OS platform	OS version	User	Last update
-------------	---------------	----------------	--------------------	-------------------	-------------	------------	------	-------------



Data isn't available right now

0% noncompliant

Intune device compliance status



- Compliant
- In grace period
- Noncompliant
- Not evaluated

[View details](#)



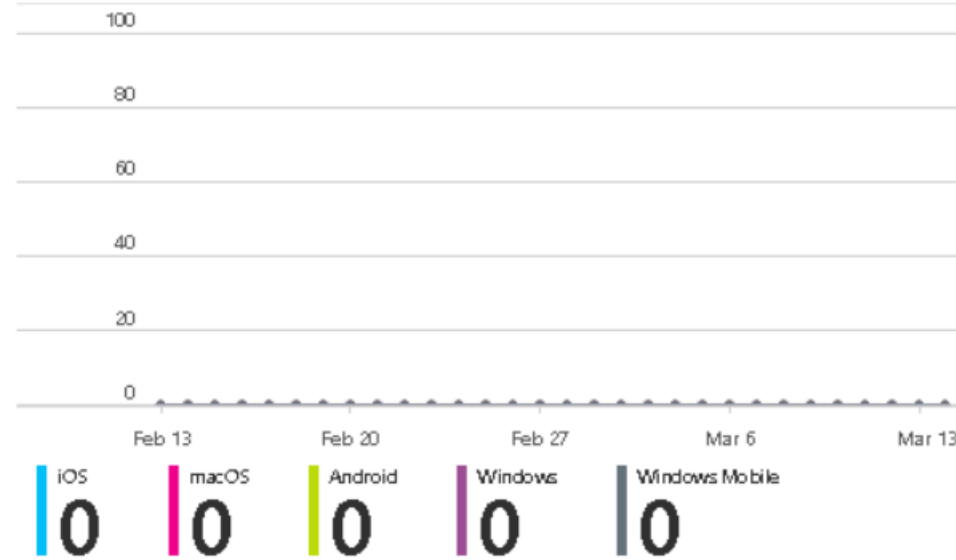
- Enrollment status**
- Enrollment alerts
- Compliance status
- Configuration status
- Software update status

Intune enrolled devices

LAST UPDATED 3/15/22, 2:34 PM

Platform	Devices
Windows	1
Android	0
iOS/iPadOS	0
macOS	0
Windows Mobile	0
Total	1

Enrollment failures by OS



Top enrollment failures this week

Failures	Count
----------	-------

No data to display

Enrollment status

Enrollment alerts

Compliance status

Configuration status

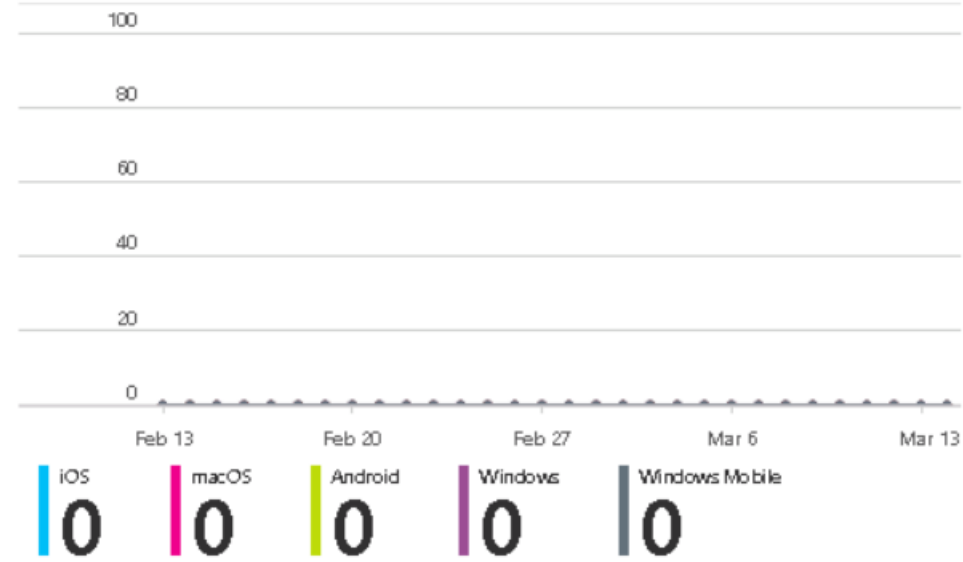
Software update status

Intune enrolled devices

LAST UPDATED 3/15/22, 2:34 PM

Platform	Devices
Windows	1
Android	0
iOS/iPadOS	0
macOS	0
Windows Mobile	0
Total	1

Enrollment failures by OS



Users with threat detections




Users with threat detections

User

Alerts

Show more



Filter by app: All apps 

 Send feedback

Alerts



Phew, there are no open alerts

Over the last 30 days

[View all alerts](#)

Discovered apps



No discovered apps

Over the last 30 days

Updated on Mar 15, 2022, 2:44 PM

[View all discovered apps](#)

Top users to investigate



Investigate Risky Users

Identify and investigate risky users and protect your organization from the threat they pose. Connect apps to get started. [Learn how to investigate risky users](#)

[Connect apps](#)



Monitor and manage user activities

Gain instant visibility into user activities and enhance your security using our anomaly detections, threat protection, DLP scanning, collaboration control, and automated governance actions. [Learn how to protect connected apps](#)

[Connect apps](#)



Something went wrong



Identify suspicious OAuth apps

Investigate and monitor OAuth app permissions granted by your users, and revoke permissions for risky apps. [Learn how to investigate risky OAuth apps](#)

[Connect apps](#)

Conditional Access App Control



Configure access and session controls

Enable real-time monitoring of your organization's business-critical apps. [Learn how to protect connected apps](#)

Users at risk



0 users at risk

■ High Risk ■ Medium Risk ■ Low risk

[View all users](#)

[Home](#) >


Risky users

 [Learn more](#) |  [Download](#) |  [Select all](#) |  [Confirm user\(s\) compromised](#) |  [Dismiss user\(s\) risk](#) |  [Refresh](#) |  [Columns](#) |  [Got feedback?](#)

Auto refresh : **Off**

Show dates as : **Local**

Risk level : **Low, Medium, High**

 [Add filters](#)

User ↑↓

Risk state ↑↓

Risk level ↑↓

Risk last updated ↑↓

No risky users found

0 privileged OAuth apps

Apps that users gave permissions to. Discovered by Defender for Cloud Apps

High Medium Low

App Permission level

Show more



Manage OAuth apps

The OAuth page displays information about app permissions in your connected apps. Manage OAuth apps is available only after connecting one or more of the supported platforms - Office 365, Google Workspace, or Salesforce. Once connected, the OAuth apps menu option will appear under Investigate.

[Learn how to manage OAuth apps](#)

Connected apps to get OAuth Usage visibility

Microsoft Defender for Cloud Apps

- Dashboard
- Discover
- Investigate
- Control
- Alerts

Connected apps

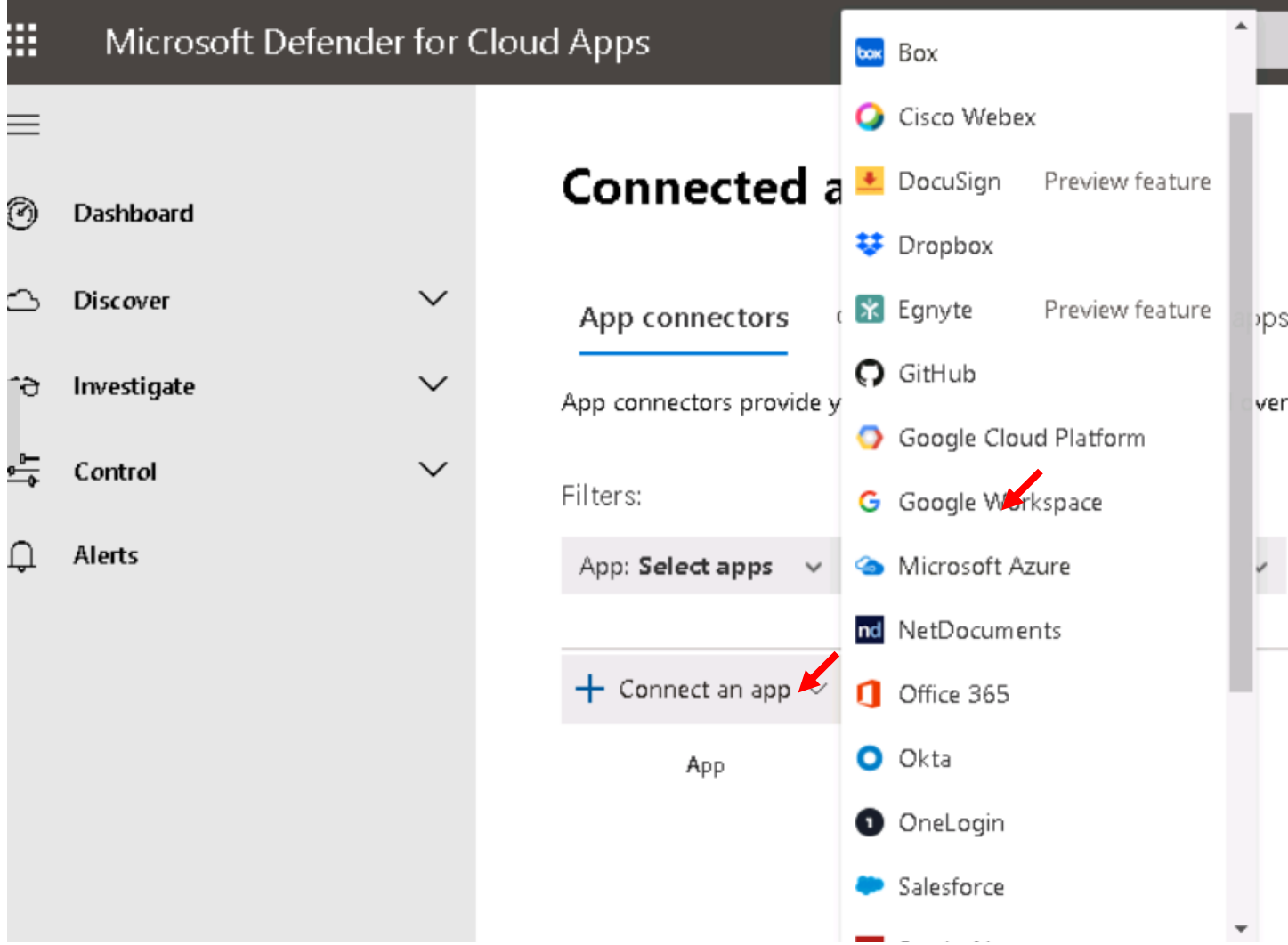
App connectors provide y

Filters:

App: **Select apps**

+ Connect an app

- Box
- Cisco Webex
- DocuSign Preview feature
- Dropbox
- Egnyte Preview feature
- GitHub
- Google Cloud Platform
- Google Workspace
- Microsoft Azure
- NetDocuments
- Office 365
- Okta
- OneLogin
- Salesforce





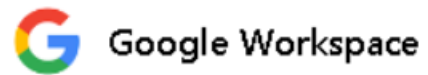
Connect Google Workspace

Connect Google Workspace to enable instant visibility, protection and governance actions.

Instance name:

Connect Google Workspace

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



Connect Google Workspace

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


Follow these steps in order to connect Google Workspace.

1 Add Google key

Service account ID

Project number
(App ID)

Certificate

 Browse

2 Add admin account

Admin account
email

account1@acme.com