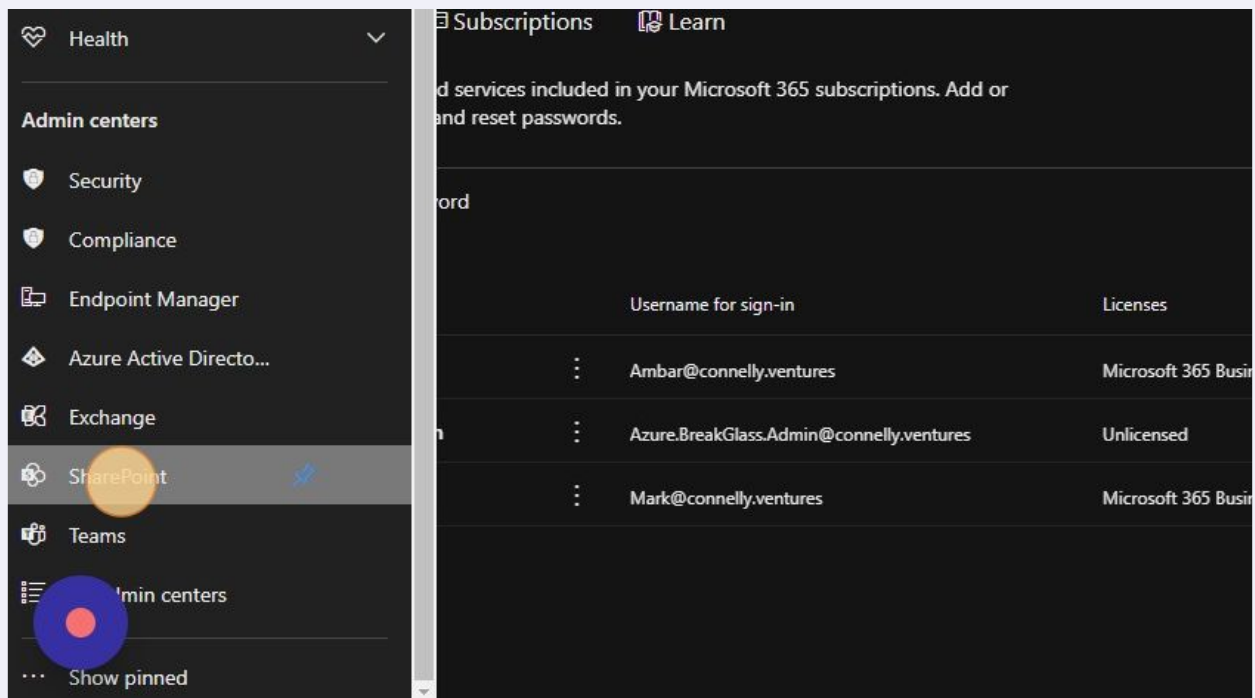


How to Configure SharePoint Online Access Control Policies

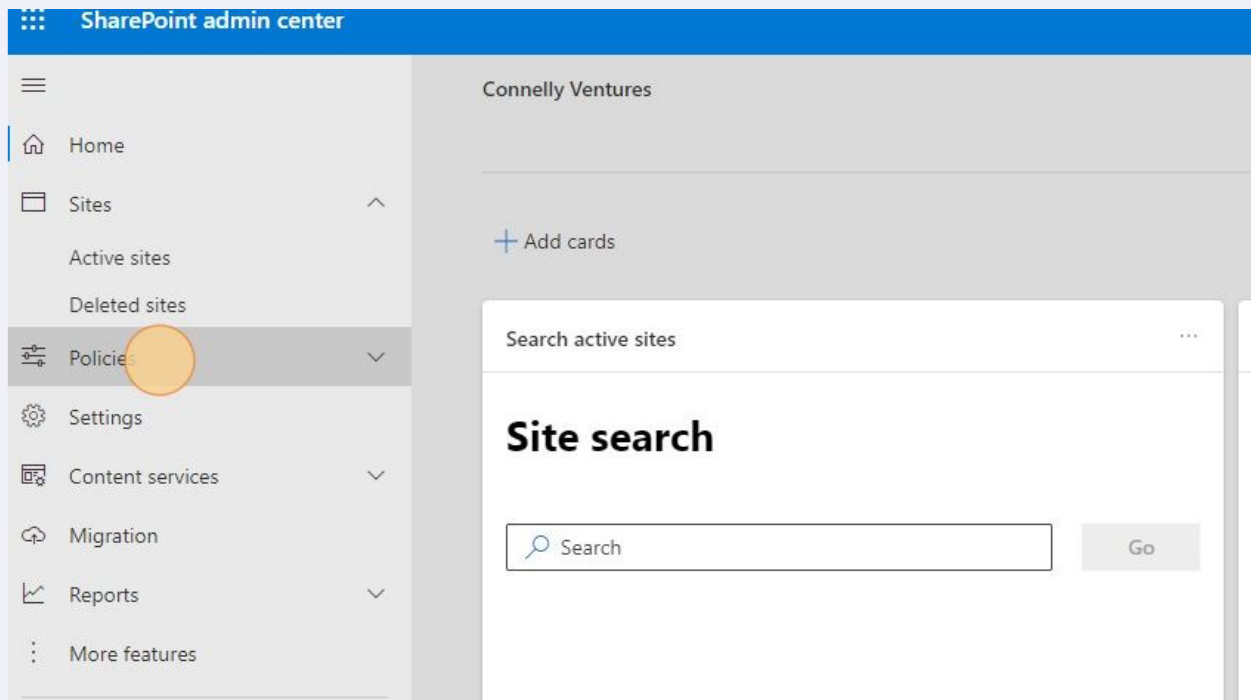
In this guide, we walk through the process of configuring SharePoint Online access control policies.
This guide satisfies the Microsoft Secure Score Recommendation:
Sign out inactive users in SharePoint Online

1 Navigate to admin.microsoft.com

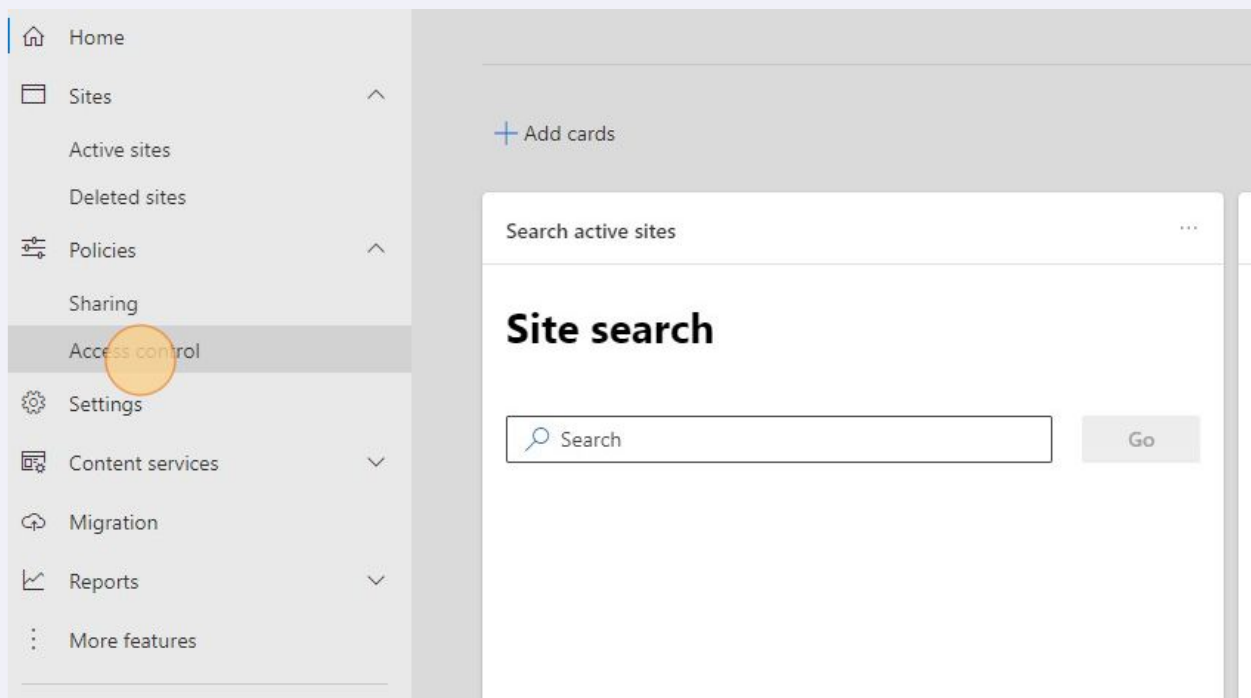
2 Click "SharePoint"



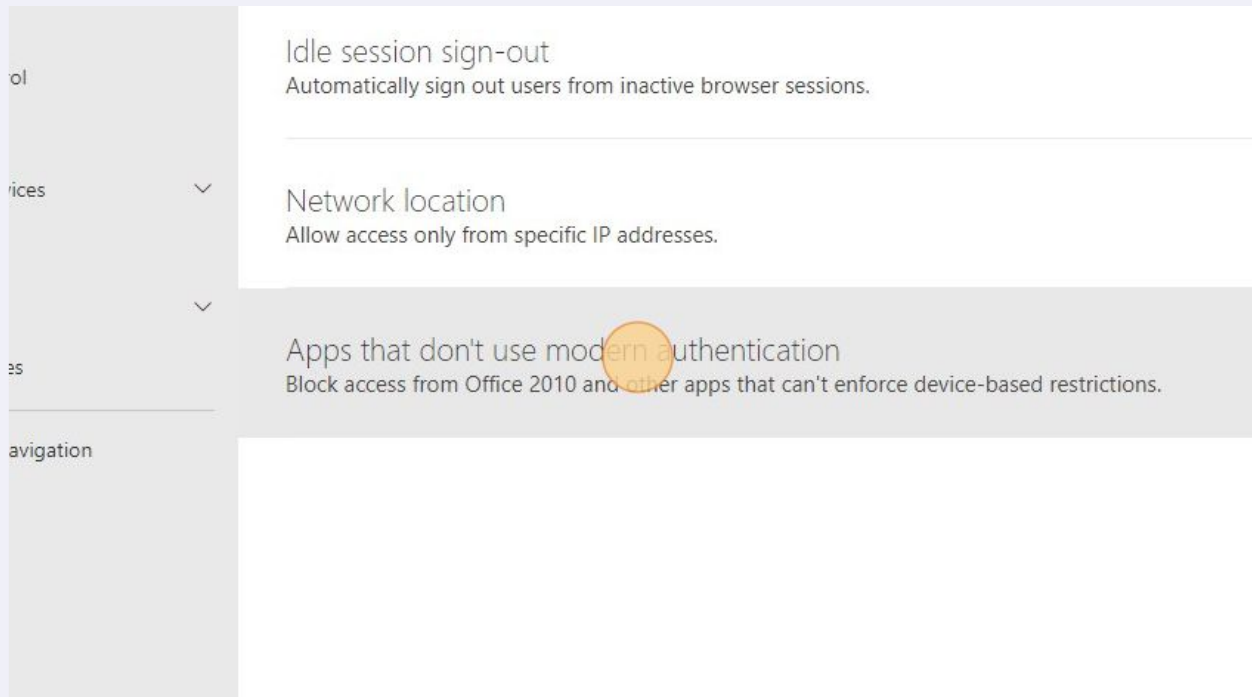
3 Click "Policies"



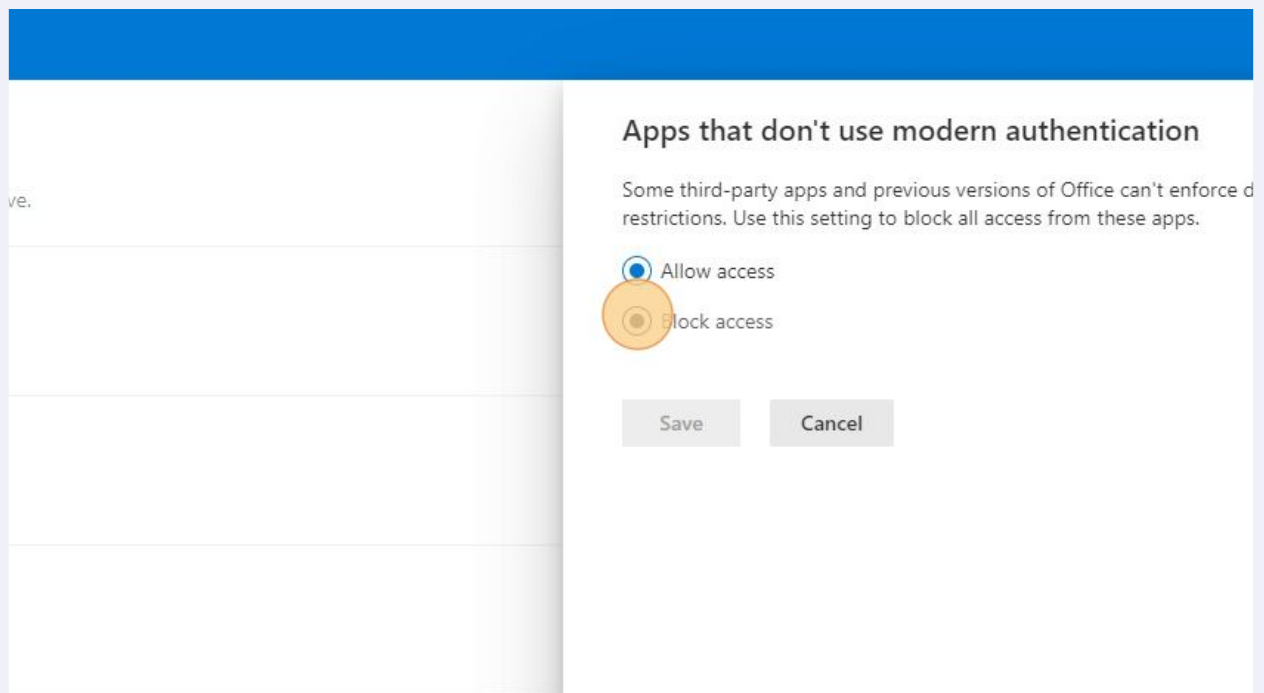
4 Click "Access control"



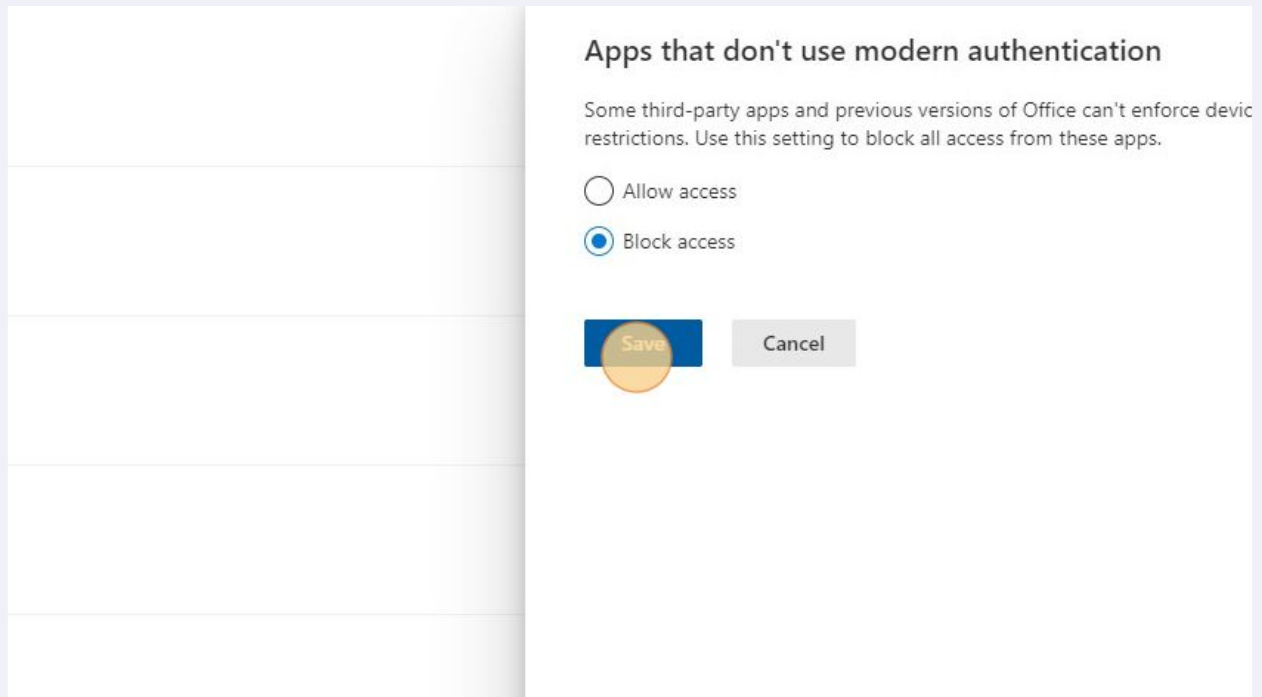
5 Click "Apps that don't use modern authentication"



6 Click "Block access"



7 Click "Save"



Apps that don't use modern authentication

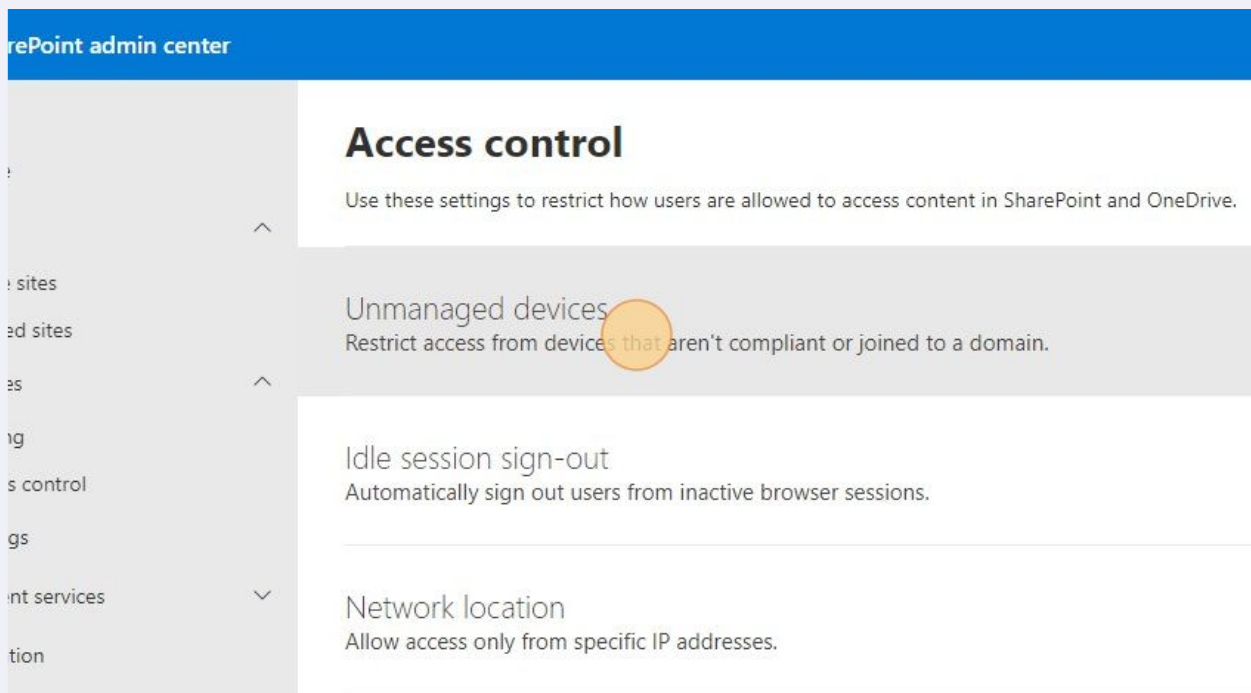
Some third-party apps and previous versions of Office can't enforce device restrictions. Use this setting to block all access from these apps.

☐ Allow access

☒ Block access

Save Cancel

8 Click "Restrict access from devices that aren't compliant or joined to a domain."



SharePoint admin center

Access control

Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

Unmanaged devices
Restrict access from devices that aren't compliant or joined to a domain.

Idle session sign-out
Automatically sign out users from inactive browser sessions.

Network location
Allow access only from specific IP addresses.

9 Click "Allow limited, web-only access"

The setting you select here will apply to all users in your organization.
[Learn more about controlling access from unmanaged devices](#)

To customize conditional access policies, save your selection and go to the [Azure AD admin center](#)

☒ Allow full access from desktop apps, mobile apps, and the web
☐ Allow limited, web-only access
☐ Block access

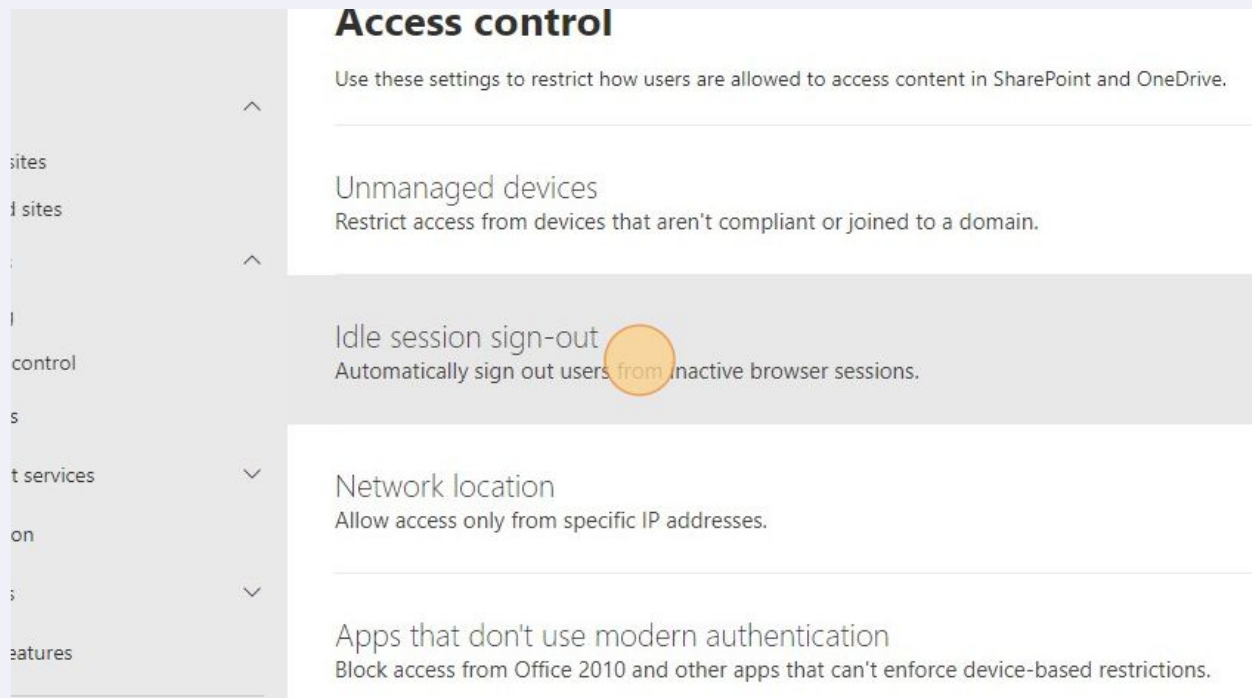
If you don't want to limit or block access organization-wide, you can do so on a per-site basis.
[Learn how to control access to specific sites by using Microsoft PowerShell](#)

10 Click "Save"

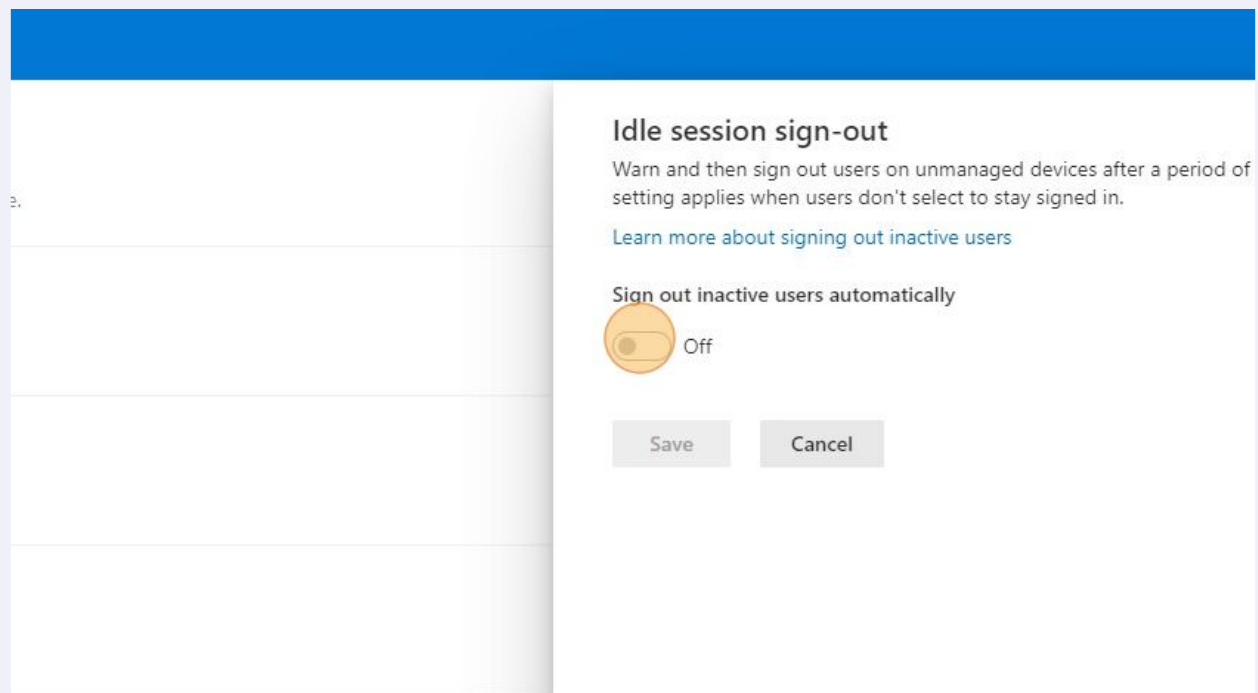
☐ Allow full access from desktop apps, mobile apps, and the web
☒ Allow limited, web-only access
☐ Block access

If you don't want to limit or block access organization-wide, you can do so on a per-site basis.
[Learn how to control access to specific sites by using Microsoft PowerShell](#)

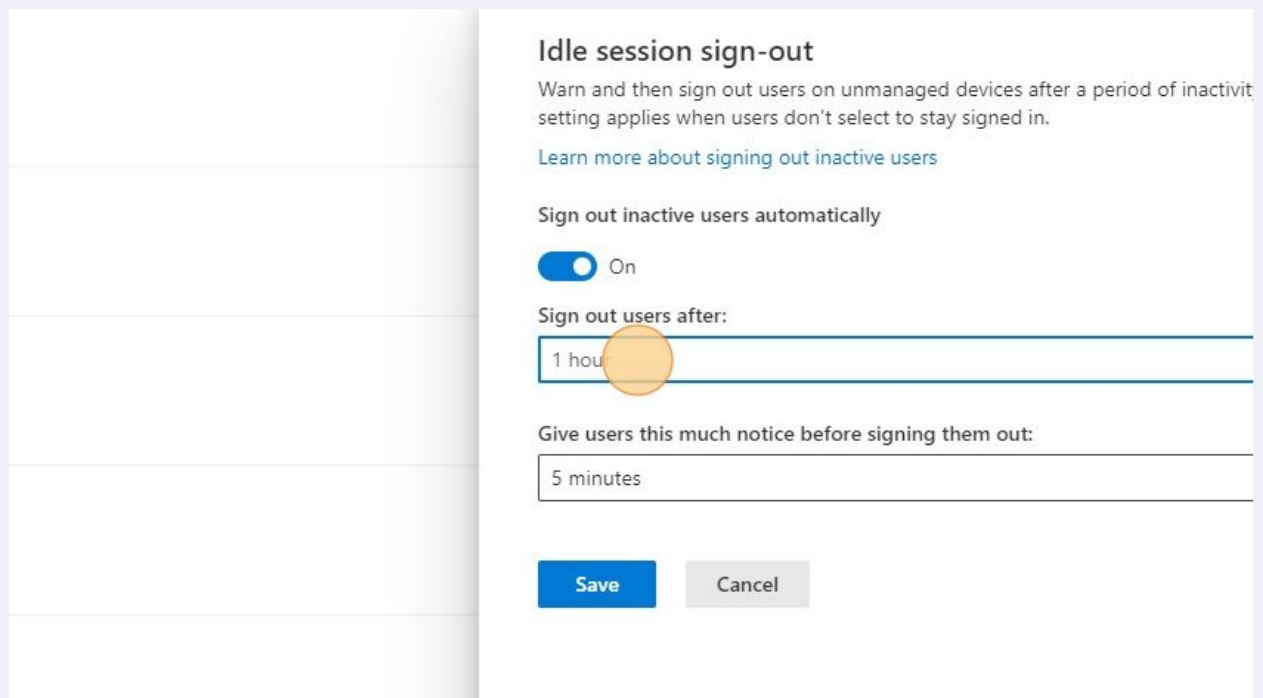
- 11 Click "Automatically sign out users from inactive browser sessions."



- 12 Click the toggle to "On"



13 Select "Sign out users after"



Idle session sign-out

Warn and then sign out users on unmanaged devices after a period of inactivity. This setting applies when users don't select to stay signed in.

[Learn more about signing out inactive users](#)

Sign out inactive users automatically

☒ On

Sign out users after:

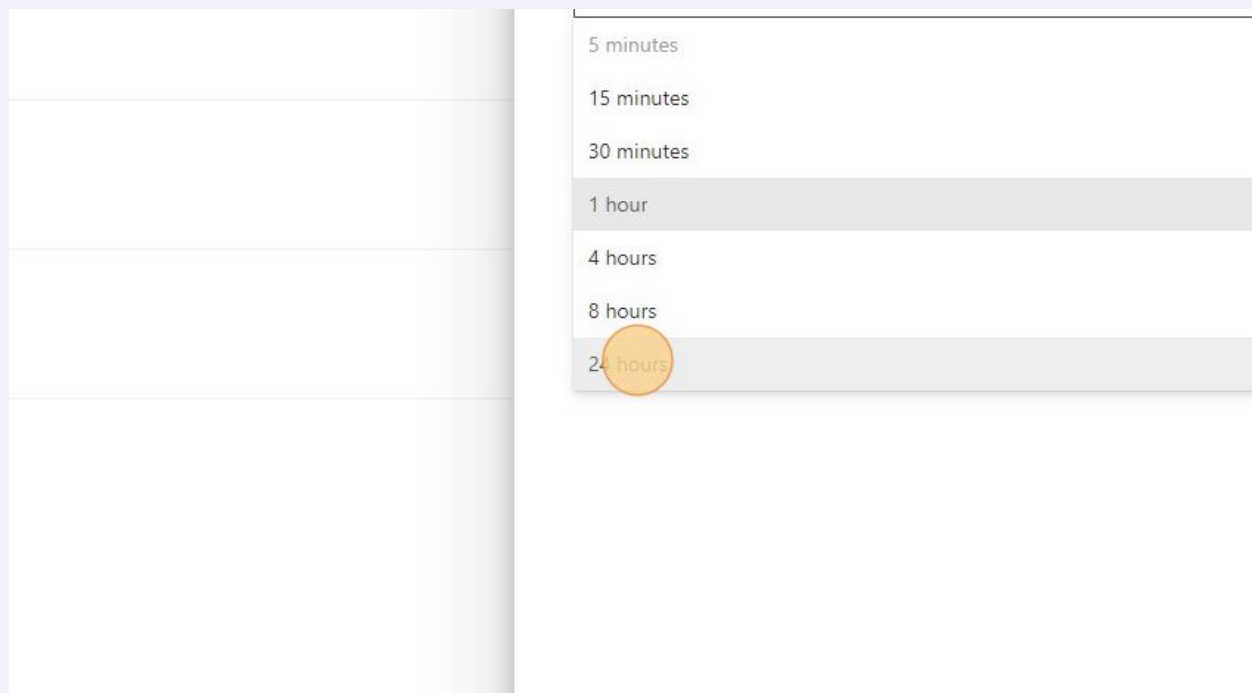
1 hour

Give users this much notice before signing them out:

5 minutes

Save **Cancel**

14 Set it to "24 hours"



5 minutes

15 minutes

30 minutes

1 hour

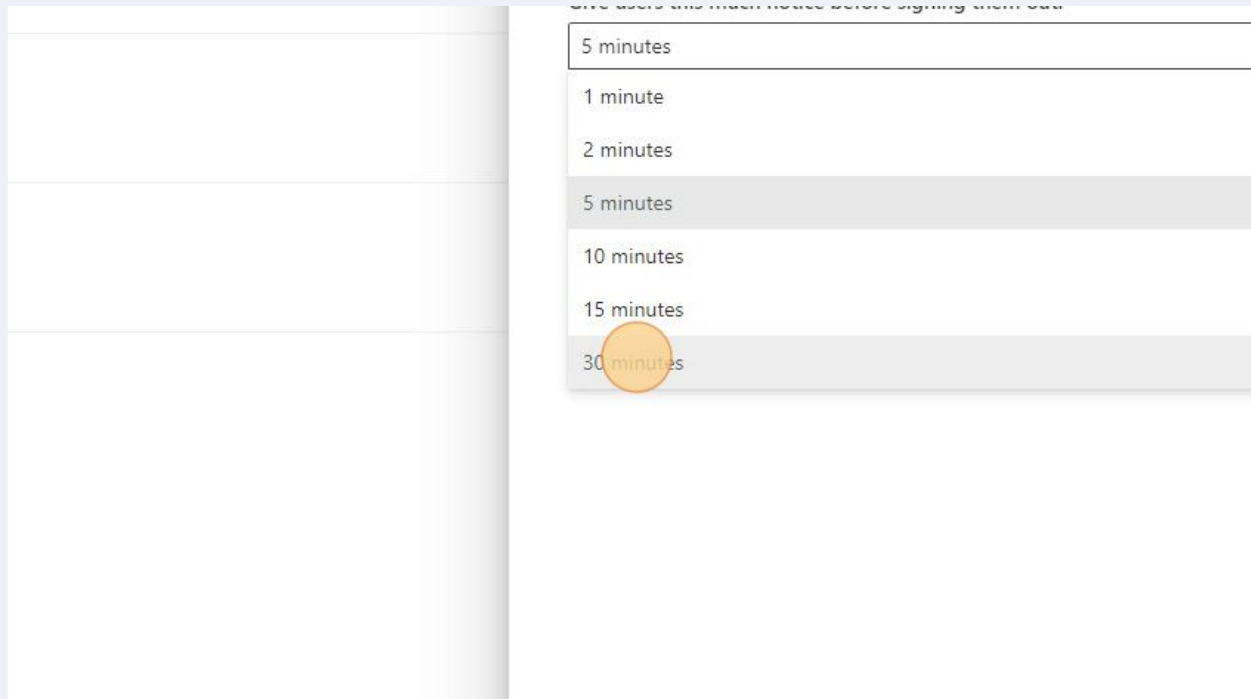
4 hours

8 hours

24 hours

15

Select "Give users this much notice before signing them out"
Set it to "30 minutes"



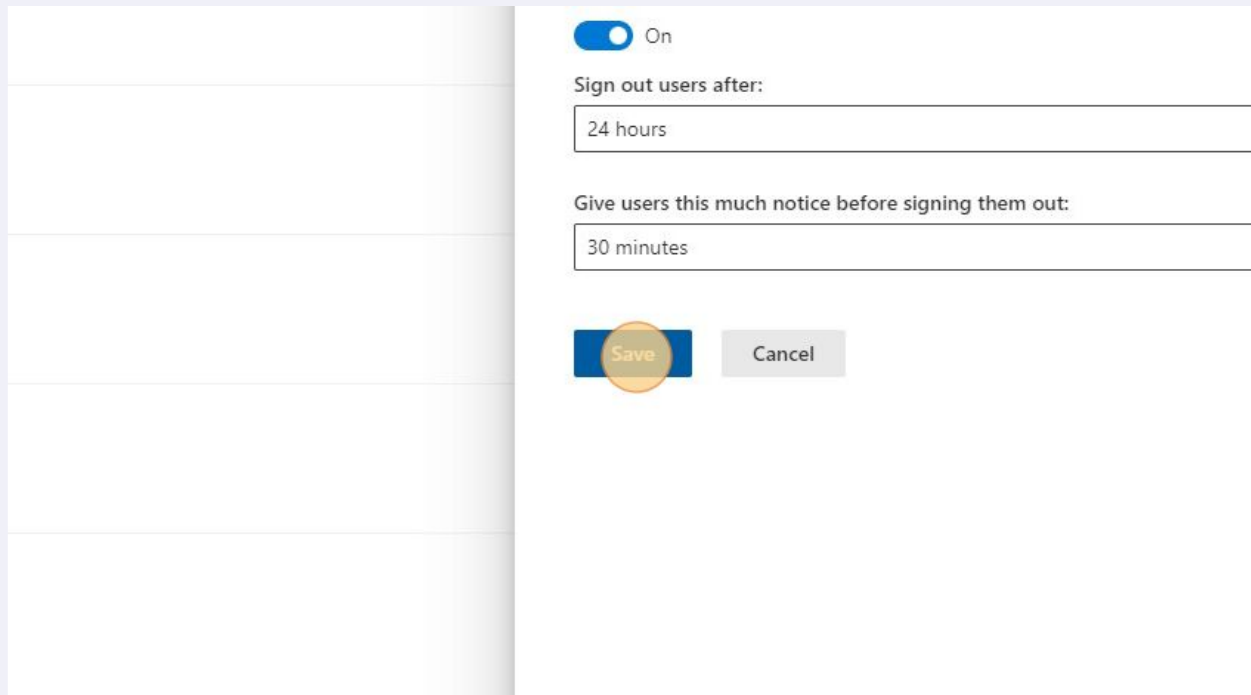
The screenshot shows a settings interface with a list of time intervals for signing out users. The list includes 5 minutes, 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, and 30 minutes. The 30 minutes option is highlighted with a blue background and a yellow circle, indicating it is the selected option.

Give users this much notice before signing them out:

- 5 minutes
- 1 minute
- 2 minutes
- 5 minutes
- 10 minutes
- 15 minutes
- 30 minutes

16

Click "Save"



The screenshot shows the settings page with a toggle switch set to 'On'. Below the toggle, there are two sections: 'Sign out users after:' with a value of '24 hours', and 'Give users this much notice before signing them out:' with a value of '30 minutes'. At the bottom, there are two buttons: 'Save' (highlighted with a yellow circle) and 'Cancel'.

☒ On

Sign out users after:

24 hours

Give users this much notice before signing them out:

30 minutes

Save Cancel