Which Security Tool When?

A Guide To Microsoft Collaboration Security

September 2021

Microsoft
Partner
Microsoft

Gold Application Development
Gold Collaboration and Content
Gold Cloud Productivity
Gold Messaging
Gold Datacenter

Collaborate with Confidence

Accessible content is available upon request.

We Are AvePoint

Leader in Microsoft 365 data management solutions

AvePoint is headquartered in Jersey City, NJ, with approximately 1,500 employees across 29 offices, 14 countries, and five continents.

25%	7M	88	7
Fortune 500	Cloud Users	Countries	Continents

Microsoft Partner

Microsoft

5x

Partner of the Year Award Winner

AVPT

NASDAQ

Let's connect!

John Peluso

CTO, AvePoint Public Sector

Chief Product Officer

AvePoint Inc.

Jersey City, NJ

Microsoft
Regional Director

john.peluso@avepoint.com

in/johnpeluso

@JohnConnected

https://johnpeluso.me

John Hodges

SVP of Product Strategy

AvePoint, Inc.

Hilo, HI

john.hodges@avepoint.com

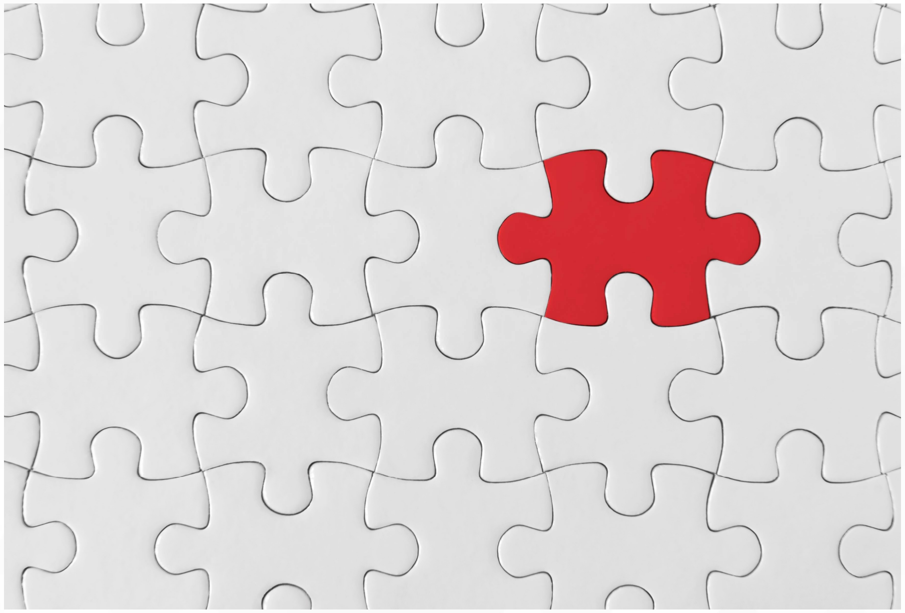
in/johndhodges

https://www.avepoint.com/blog/author/john-hodgesavepoint-com/

So What Are We Talking About Today?

How the “layers” of security in M365 fit together… and where they don’t!

- Securing *Identity*
- Securing *Data*
- Securing *Workspaces*
- Putting it all together…



A5
A6

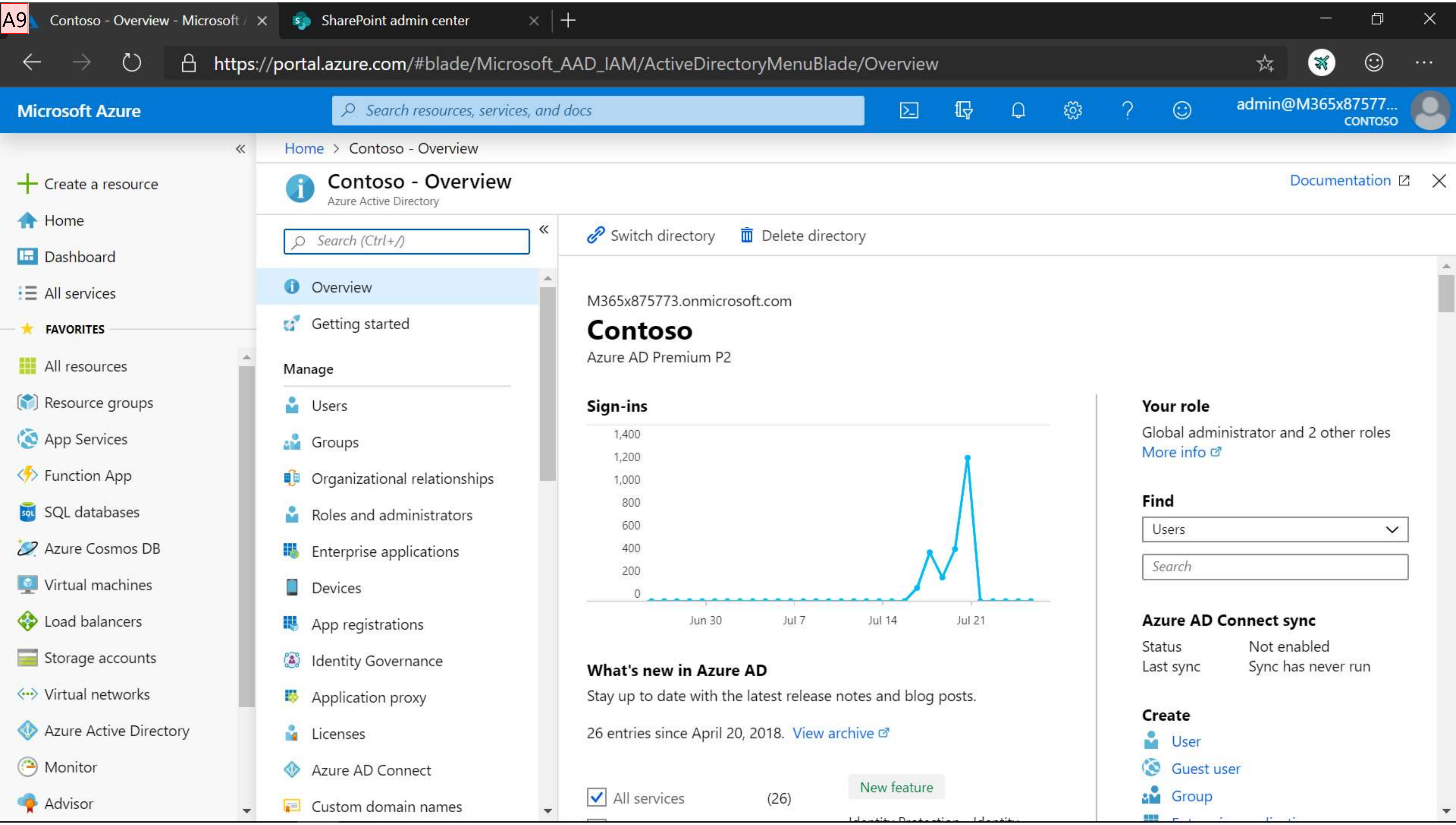
Establishing “Identity” with Azure AD

Slide 7

A5 Changed this to third person to be consistent with rest of click through.
Author, 8/29/2019

A6 I've rewritten this to keep Deana as the hero to match the previous section.
Author, 8/29/2019

A9



M365x875773.onmicrosoft.com

Contoso

Azure AD Premium P2

Your role

Global administrator and 2 other roles

More info

Azure AD Connect sync

Status	Not enabled
Last sync	Sync has never run

What's new in Azure AD

Stay up to date with the latest release notes and blog posts.

26 entries since April 20, 2018. View archive

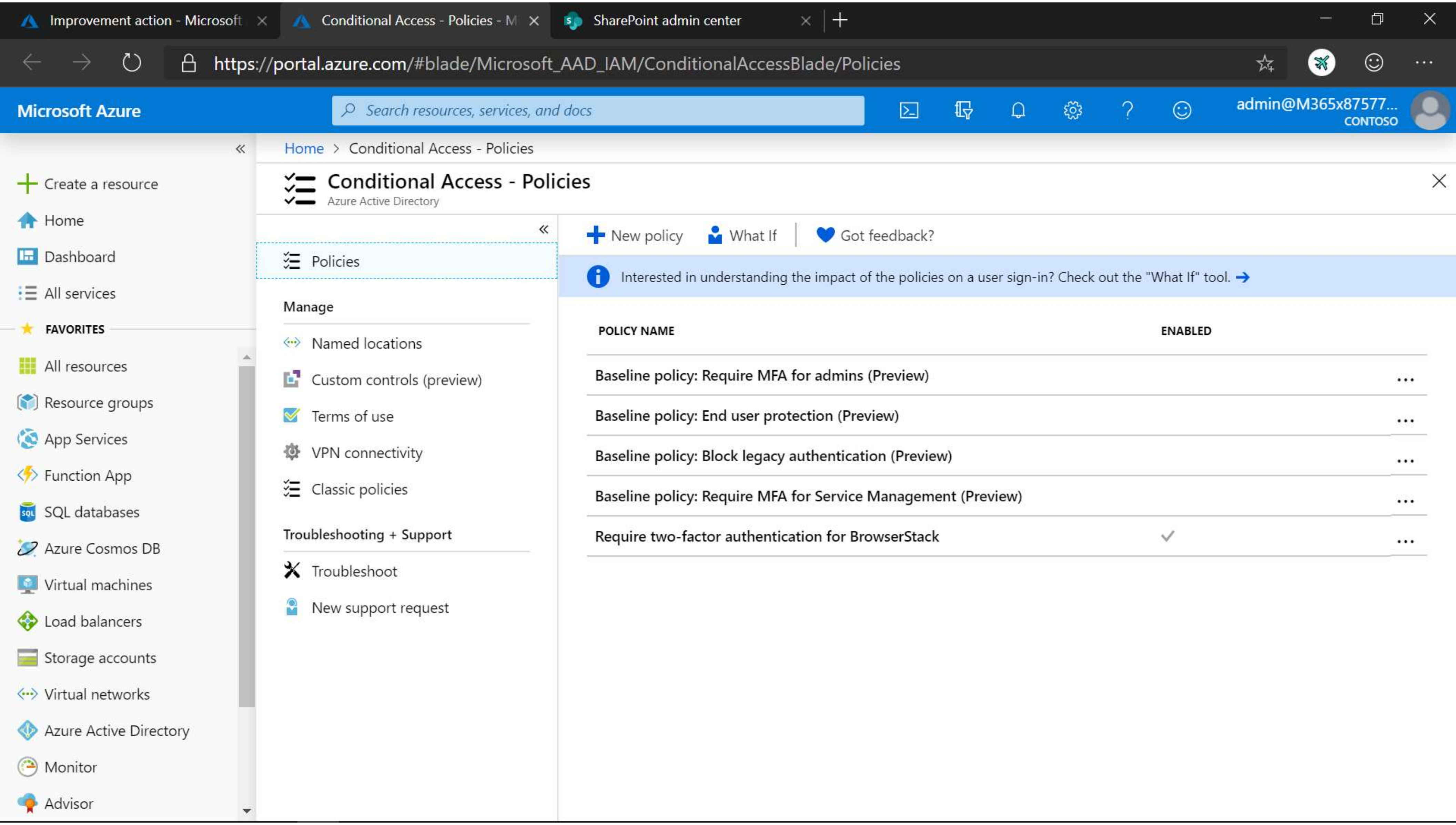
☑ All services (26)

Slide 8

A9 This is just feature bullets. I've rewritten to match tone with the other slides. Please confirm this accurately describes the scenario.

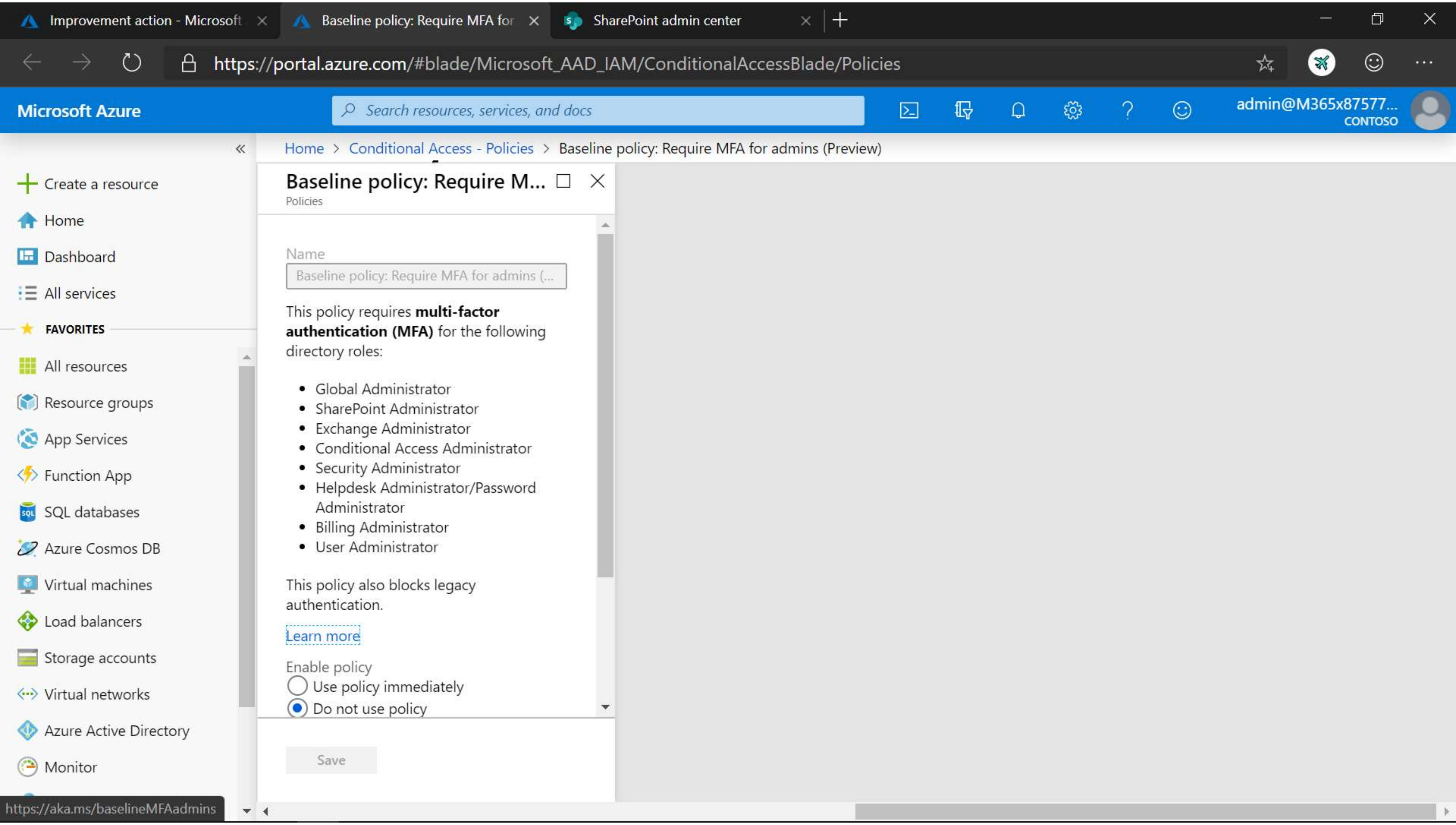
Author, 8/29/2019

Conditional Access



Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)		...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...


Improvement action - Microsoft
Baseline policy: Require MFA for
SharePoint admin center
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies
Microsoft Azure
Search resources, services, and docs
admin@M365x87577...
CONTOSO
Home > Conditional Access - Policies > Baseline policy: Require MFA for admins (Preview)
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
https://aka.ms/baselineMFAadmins

Baseline policy: Require M...

Policies

Name: Baseline policy: Require MFA for admins (...

This policy requires **multi-factor authentication (MFA)** for the following directory roles:

- Global Administrator
- SharePoint Administrator
- Exchange Administrator
- Conditional Access Administrator
- Security Administrator
- Helpdesk Administrator/Password Administrator
- Billing Administrator
- User Administrator

This policy also blocks legacy authentication.

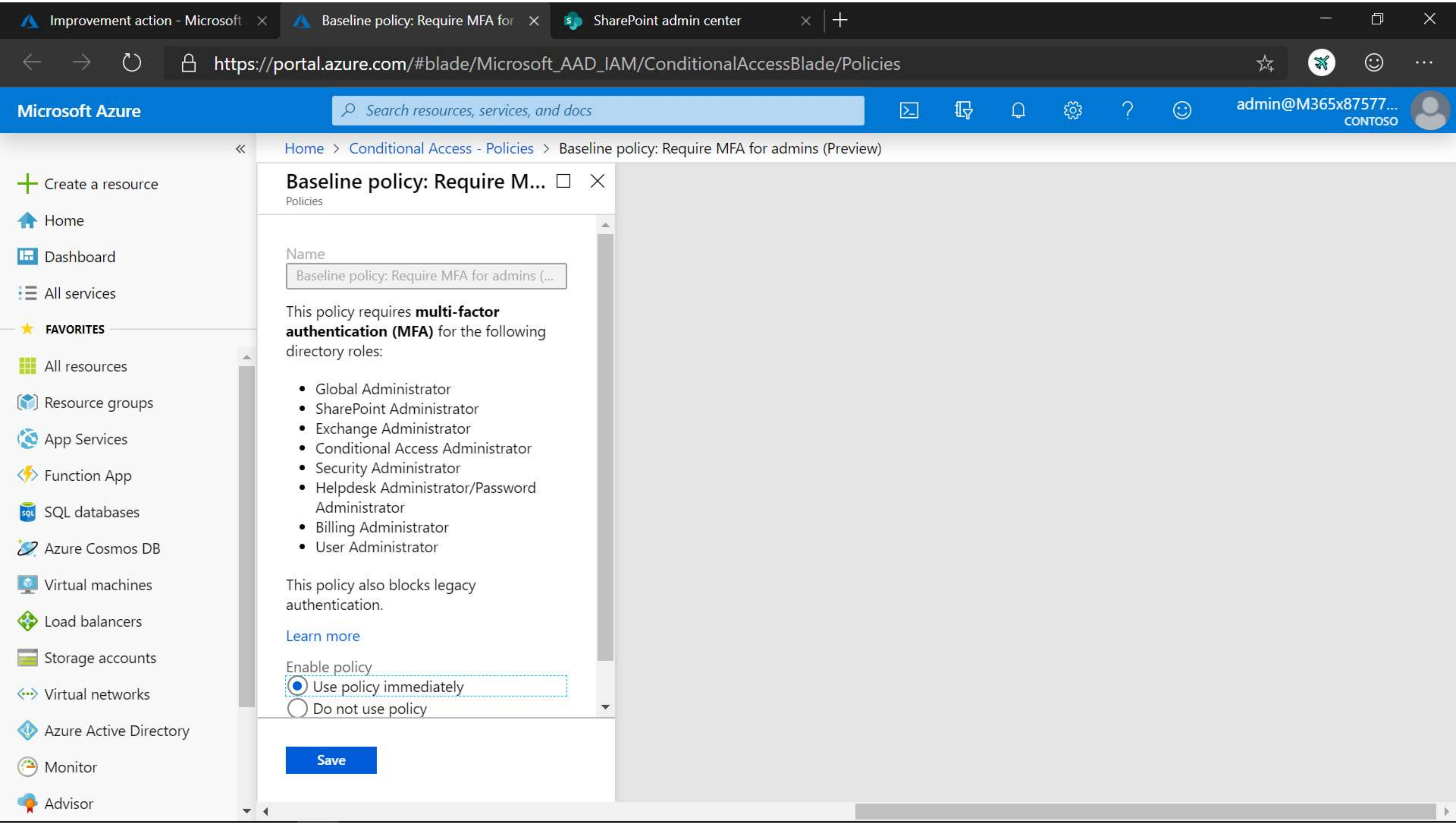
Learn more

Enable policy

○ Use policy immediately

● Do not use policy

Save



Name

Baseline policy: Require MFA for admins (...

This policy requires **multi-factor authentication (MFA)** for the following directory roles:

- Global Administrator
- SharePoint Administrator
- Exchange Administrator
- Conditional Access Administrator
- Security Administrator
- Helpdesk Administrator/Password Administrator
- Billing Administrator
- User Administrator

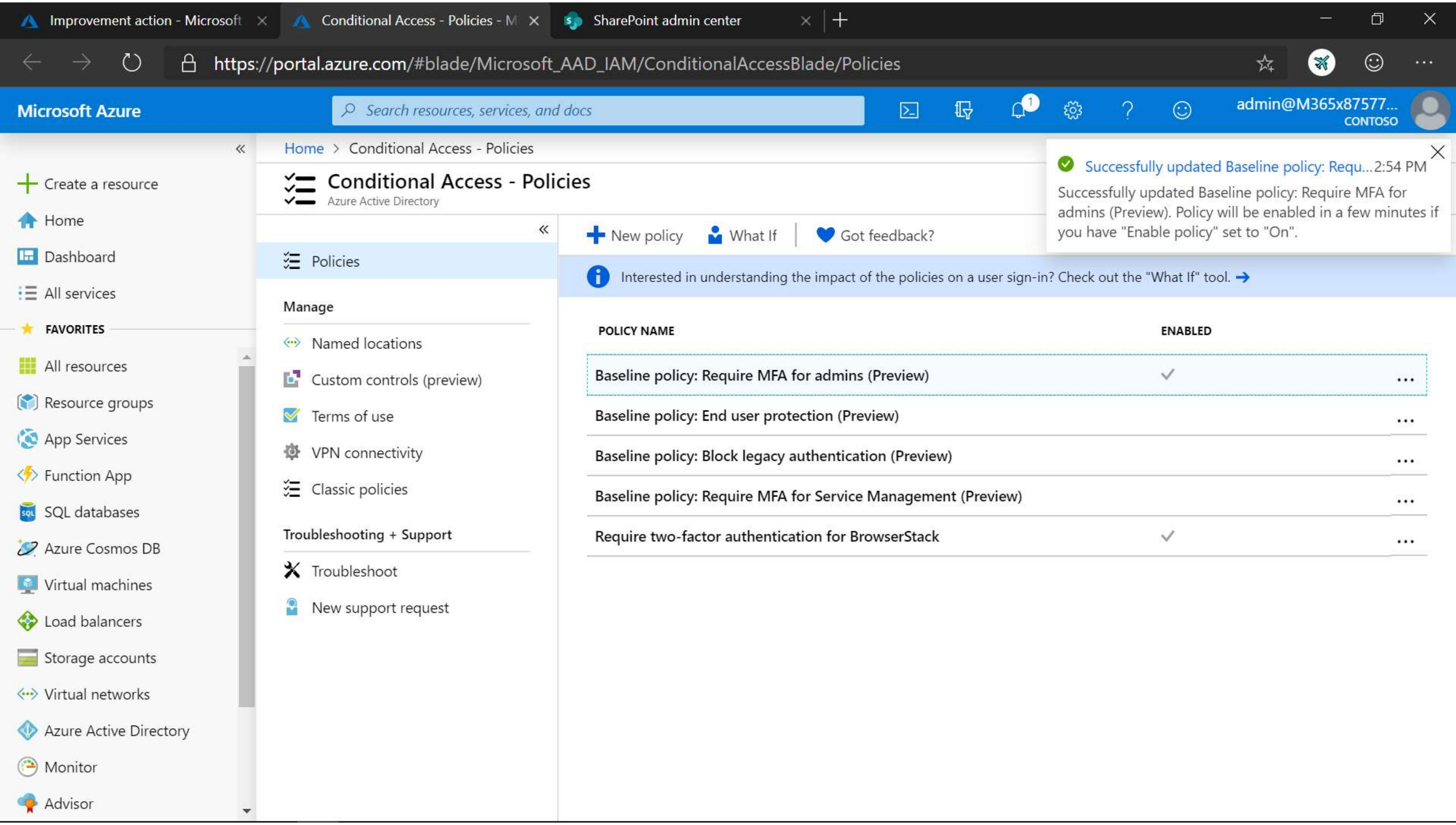
This policy also blocks legacy authentication.

Learn more

Enable policy

● Use policy immediately

○ Do not use policy

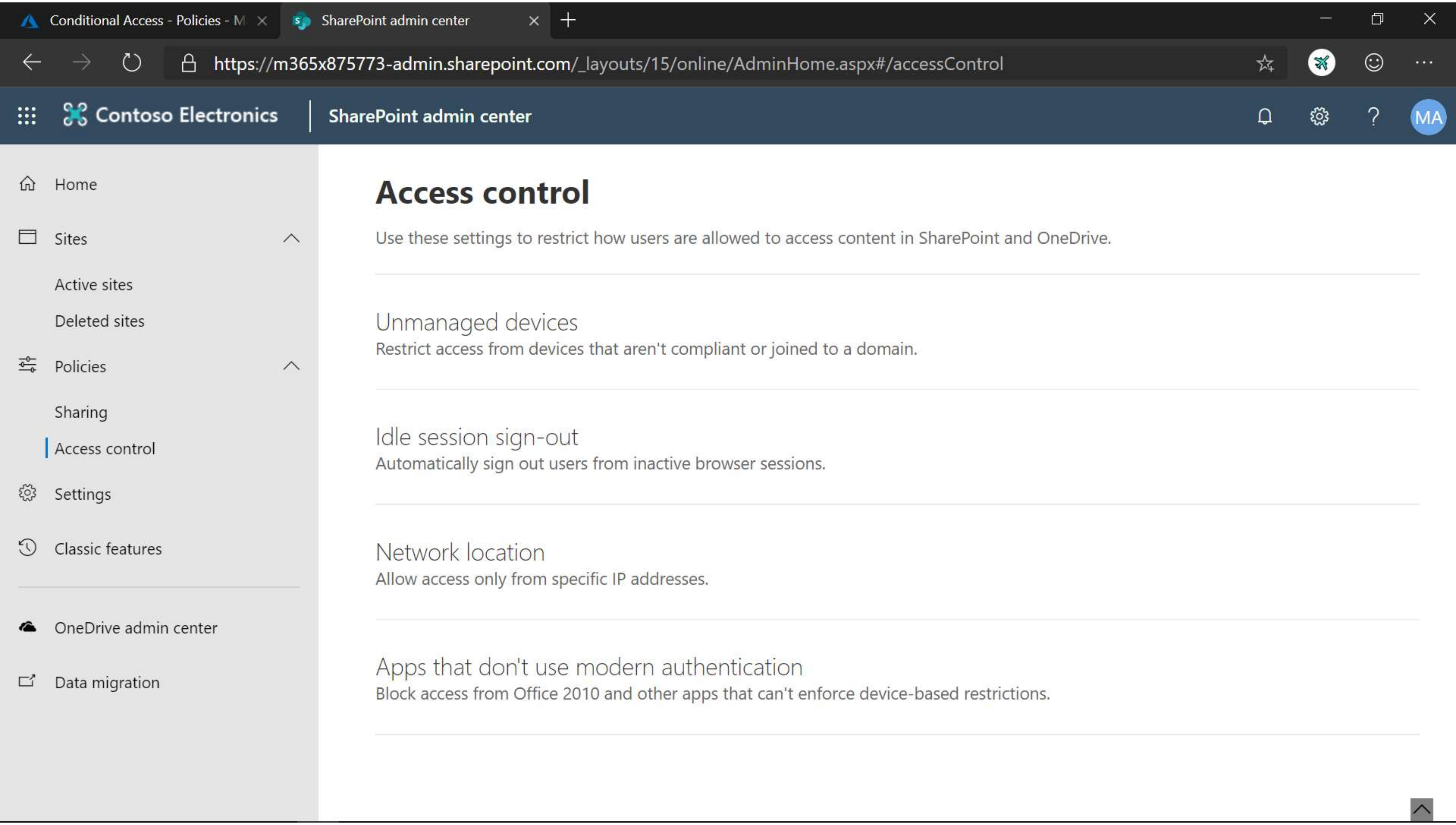


Successfully updated Baseline policy: Requ... 2:54 PM

Successfully updated Baseline policy: Require MFA for admins (Preview). Policy will be enabled in a few minutes if you have "Enable policy" set to "On".

Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED
Baseline policy: Require MFA for admins (Preview)	✓
Baseline policy: End user protection (Preview)	
Baseline policy: Block legacy authentication (Preview)	
Baseline policy: Require MFA for Service Management (Preview)	
Require two-factor authentication for BrowserStack	✓



Access control

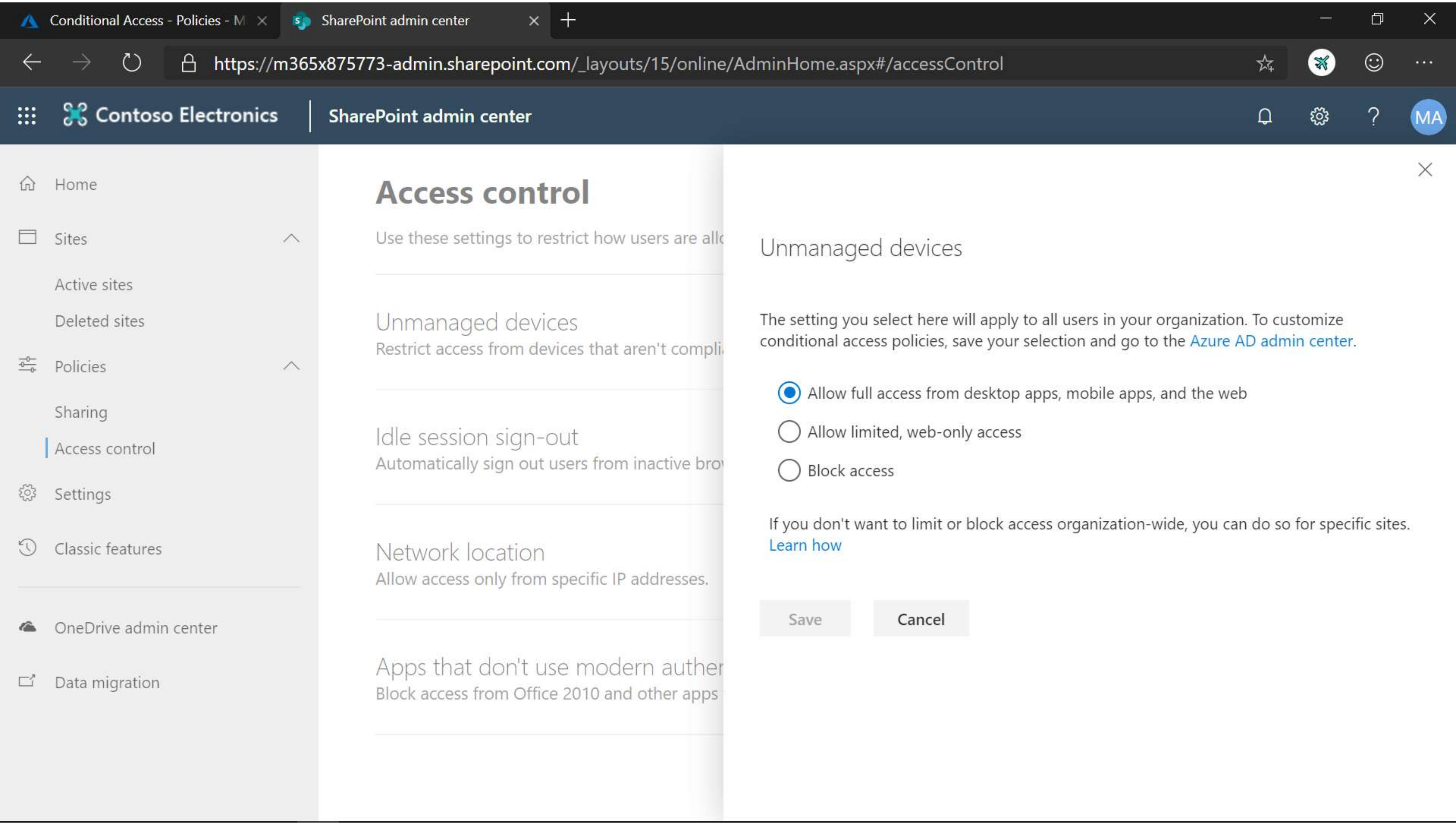
Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

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.

Apps that don't use modern authentication
Block access from Office 2010 and other apps that can't enforce device-based restrictions.



Access control

Use these settings to restrict how users are allo

Unmanaged devices
Restrict access from devices that aren't compli

Idle session sign-out
Automatically sign out users from inactive bro

Network location
Allow access only from specific IP addresses.

Apps that don't use modern auther
Block access from Office 2010 and other apps

Unmanaged devices

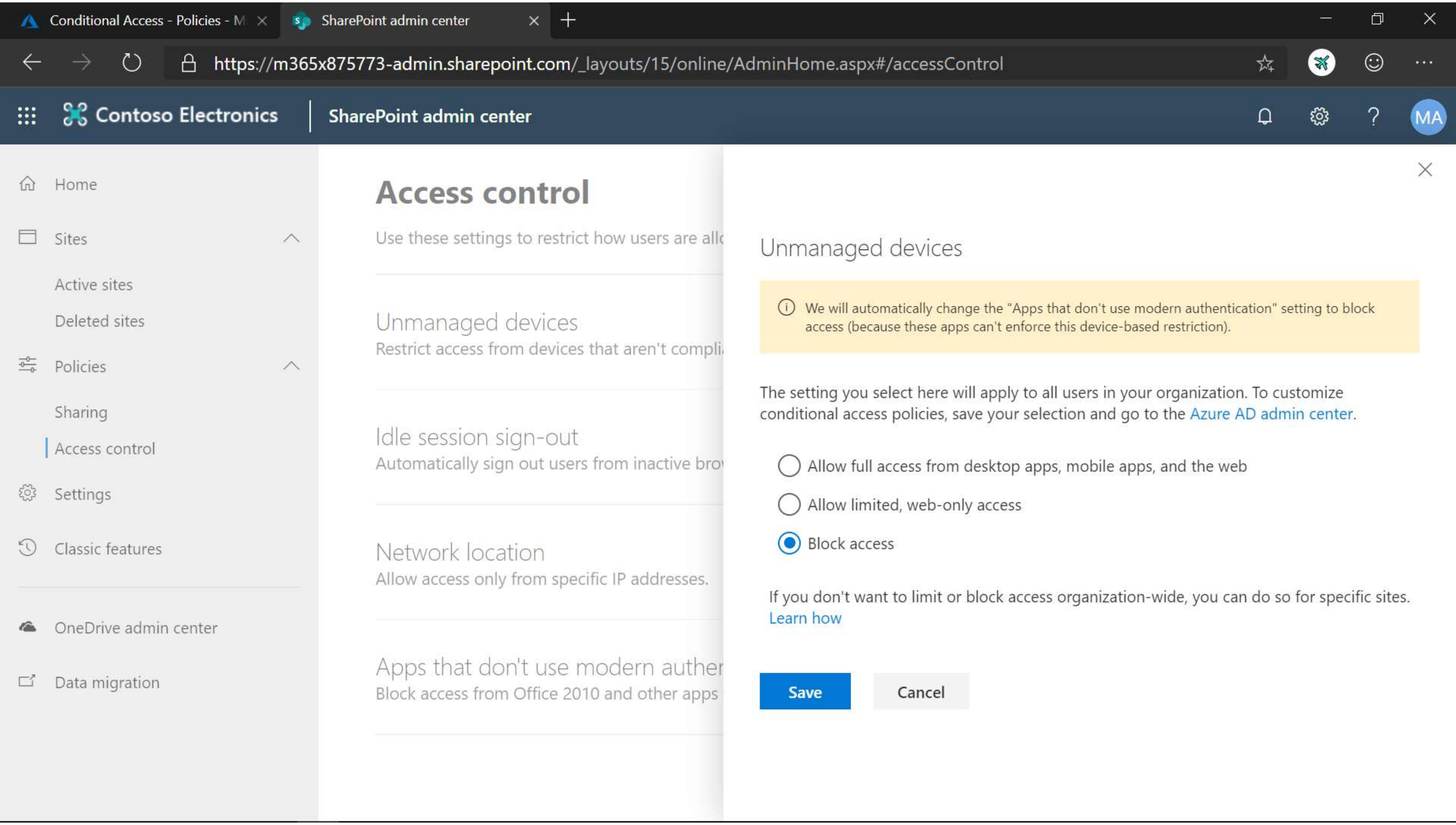
The setting you select here will apply to all users in your organization. To customize conditional access policies, save your selection and go to the Azure AD admin center.

● 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 for specific sites. Learn how



Access control

Use these settings to restrict how users are allo

Unmanaged devices
Restrict access from devices that aren't compli

Idle session sign-out
Automatically sign out users from inactive bro

Network location
Allow access only from specific IP addresses.

Apps that don't use modern authen
Block access from Office 2010 and other apps

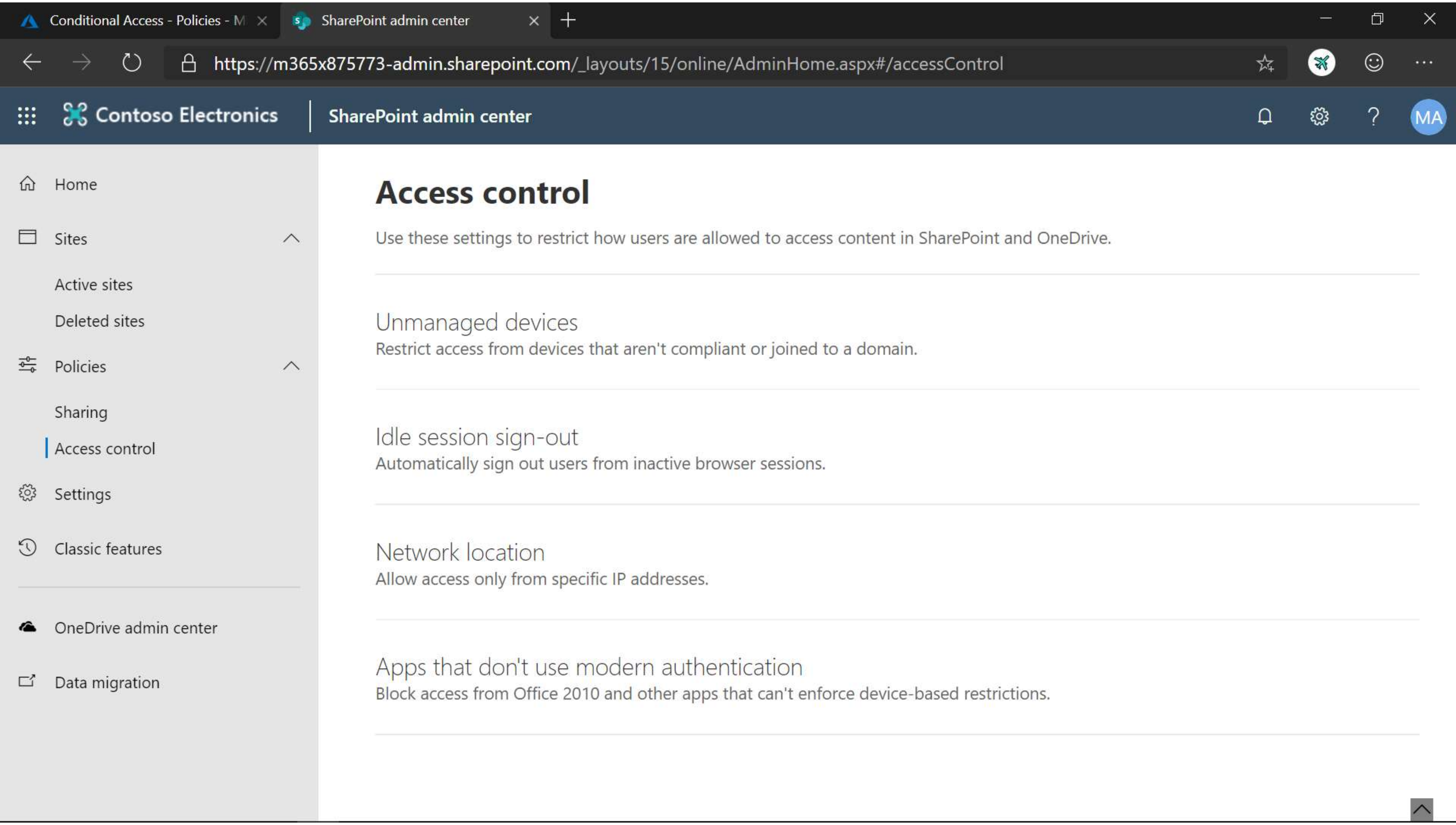
Unmanaged devices

ⓘ We will automatically change the "Apps that don't use modern authentication" setting to block access (because these apps can't enforce this device-based restriction).

The setting you select here will apply to all users in your organization. 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 for specific sites. Learn how



Access control

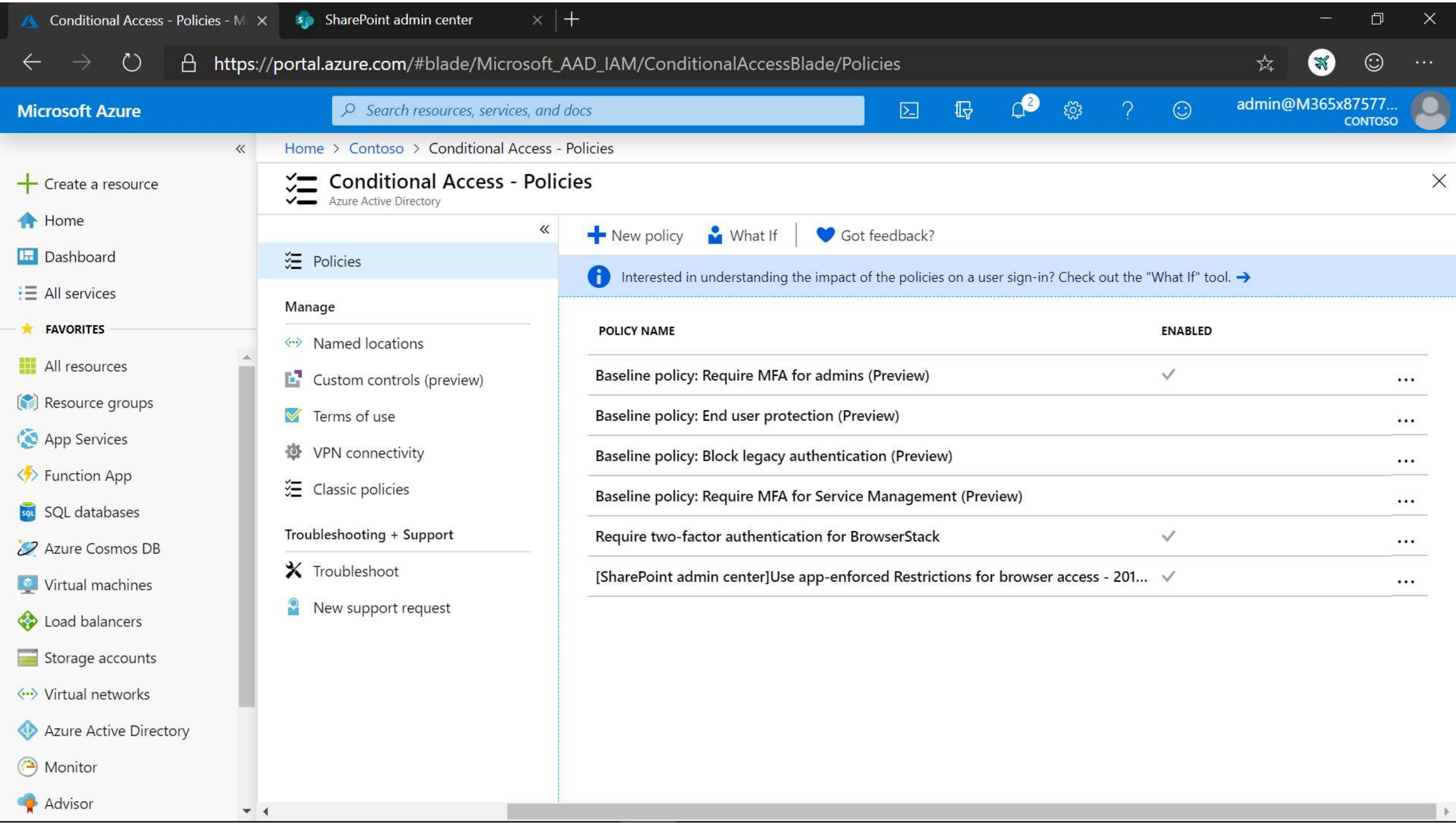
Use these settings to restrict how users are allowed to access content in SharePoint and OneDrive.

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.

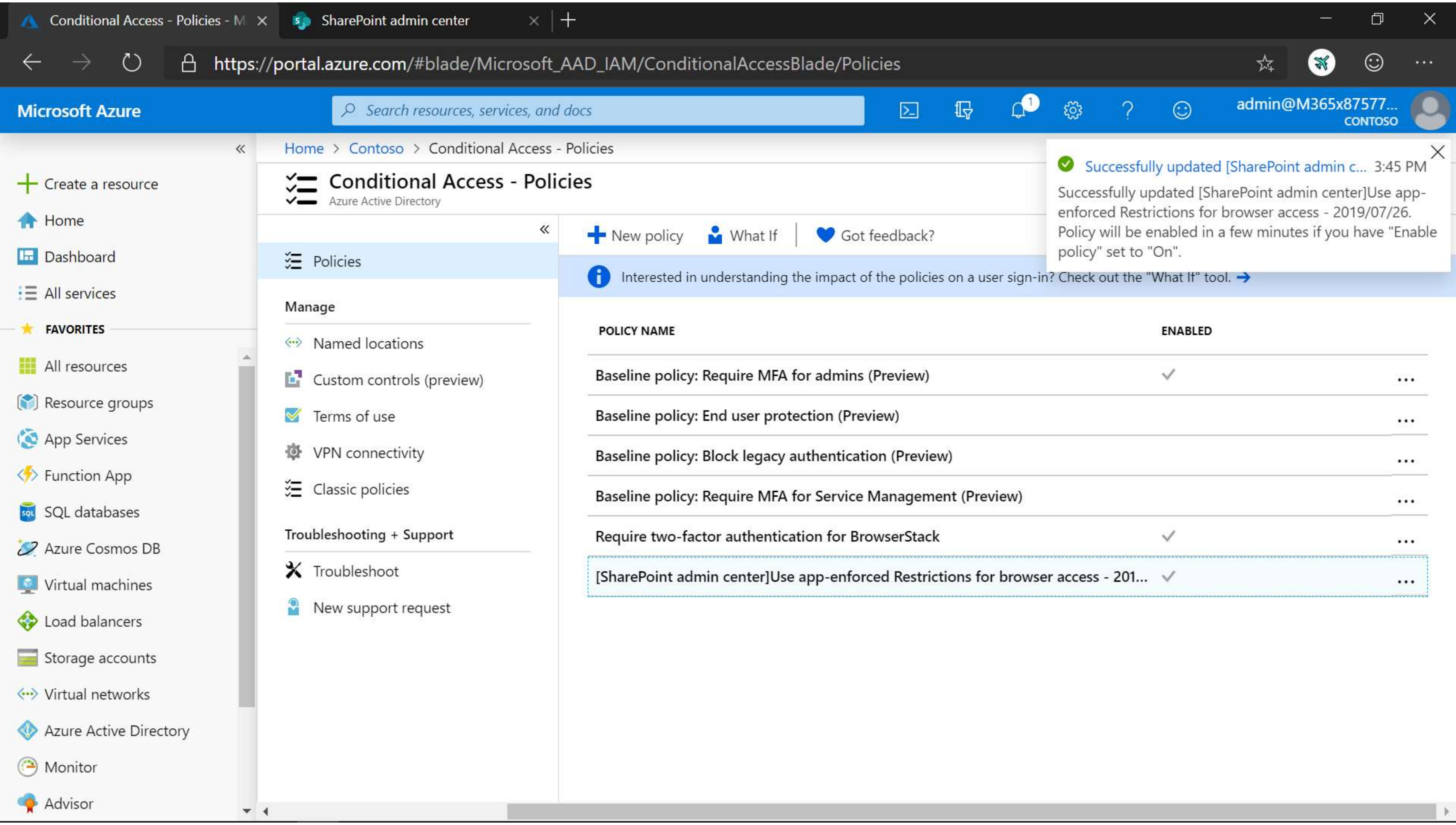
Network location
Allow access only from specific IP addresses.

Apps that don't use modern authentication
Block access from Office 2010 and other apps that can't enforce device-based restrictions.



Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...

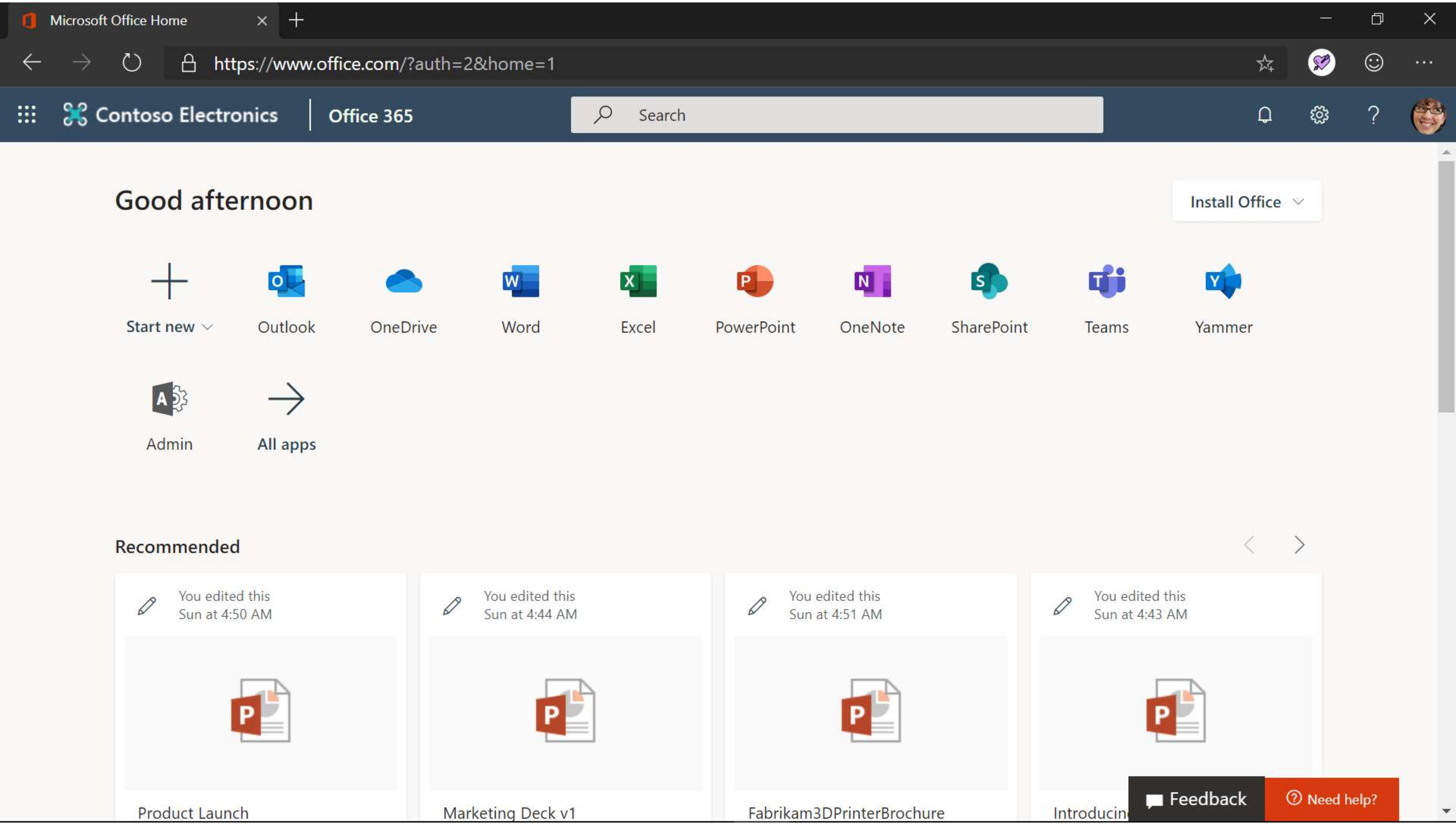


Successfully updated [SharePoint admin c... 3:45 PM

Successfully updated [SharePoint admin center]Use app-enforced Restrictions for browser access - 2019/07/26. Policy will be enabled in a few minutes if you have "Enable policy" set to "On".

Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...

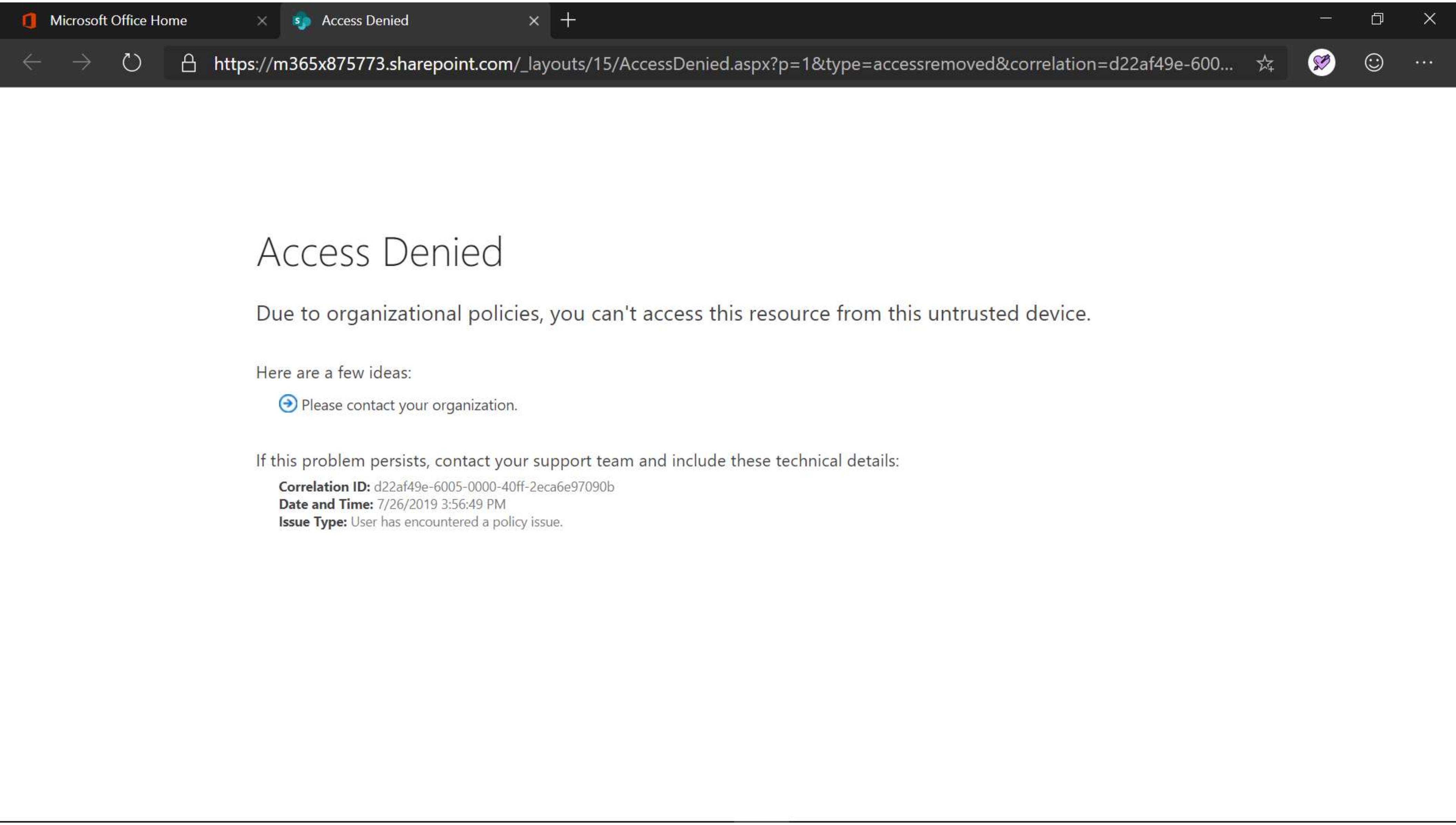


You edited this
Sun at 4:50 AM
Product Launch

You edited this
Sun at 4:44 AM
Marketing Deck v1

You edited this
Sun at 4:51 AM
Fabrikam3DPrinterBrochure

You edited this
Sun at 4:43 AM
Introducin


Microsoft Office Home
Access Denied
https://m365x875773.sharepoint.com/_layouts/15/AccessDenied.aspx?p=1&type=accessremoved&correlation=d22af49e-600...

Access Denied

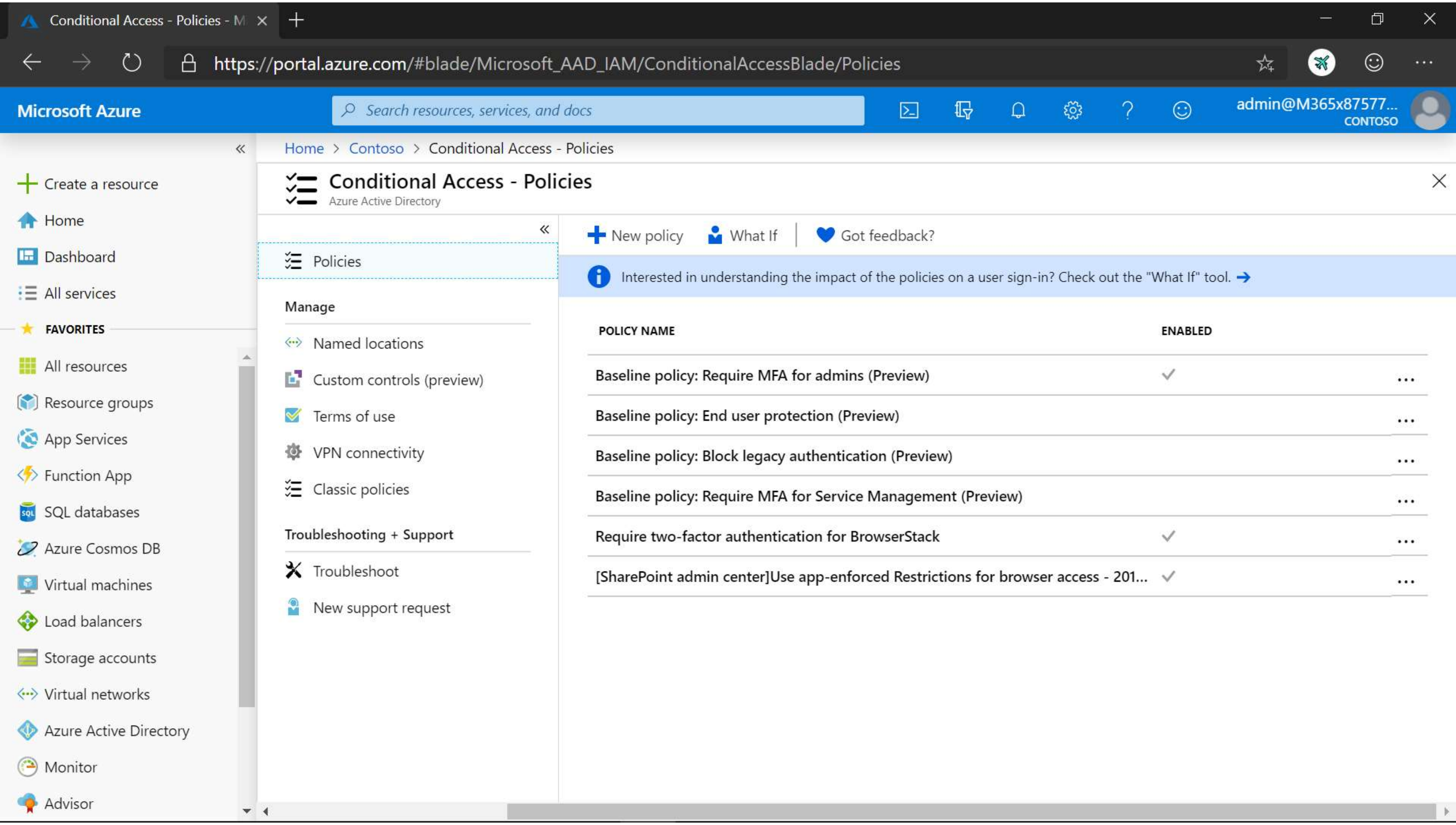
Due to organizational policies, you can't access this resource from this untrusted device.

Here are a few ideas:

- Please contact your organization.

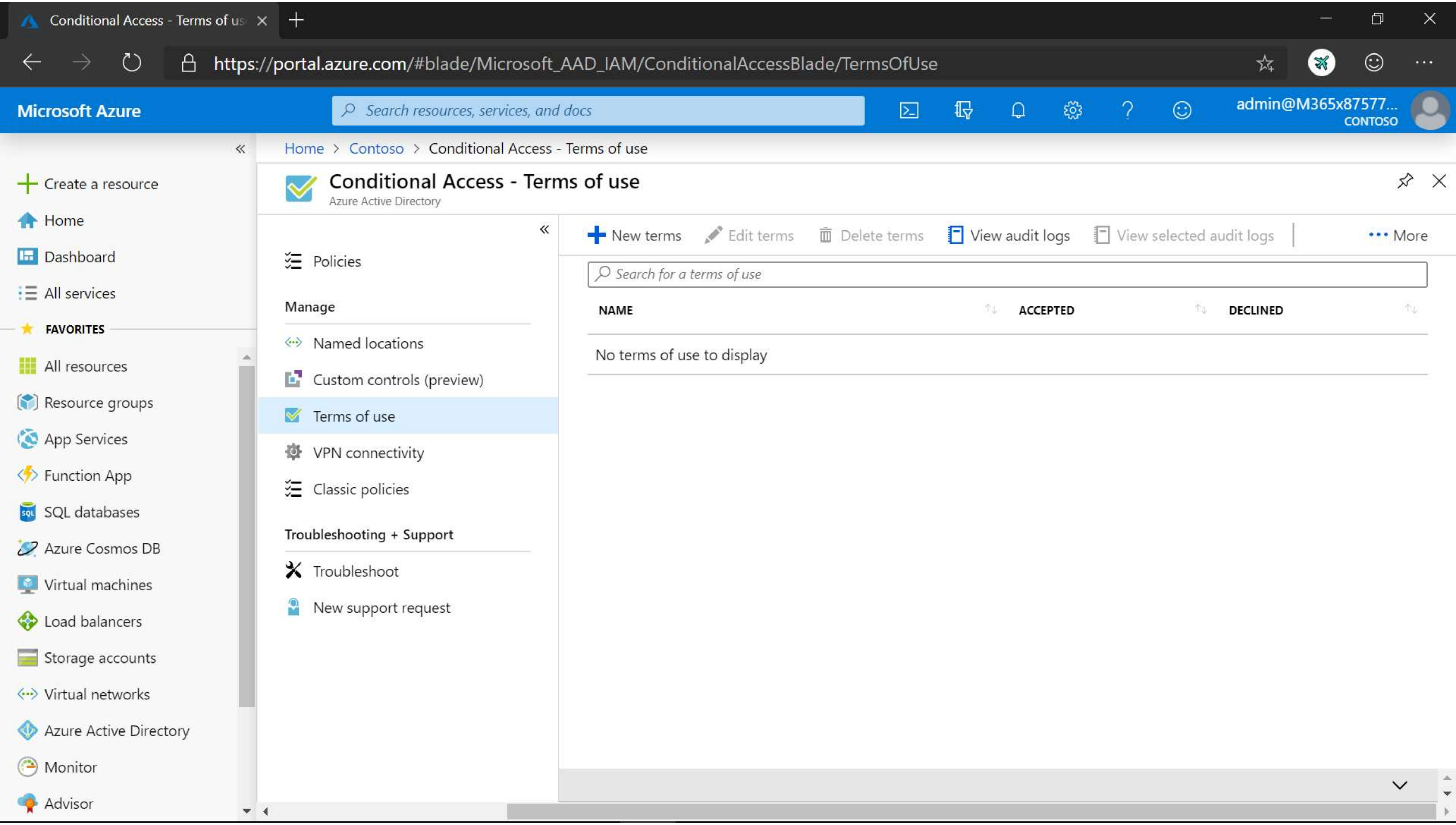
If this problem persists, contact your support team and include these technical details:

Correlation ID: d22af49e-6005-0000-40ff-2eca6e97090b
Date and Time: 7/26/2019 3:56:49 PM
Issue Type: User has encountered a policy issue.

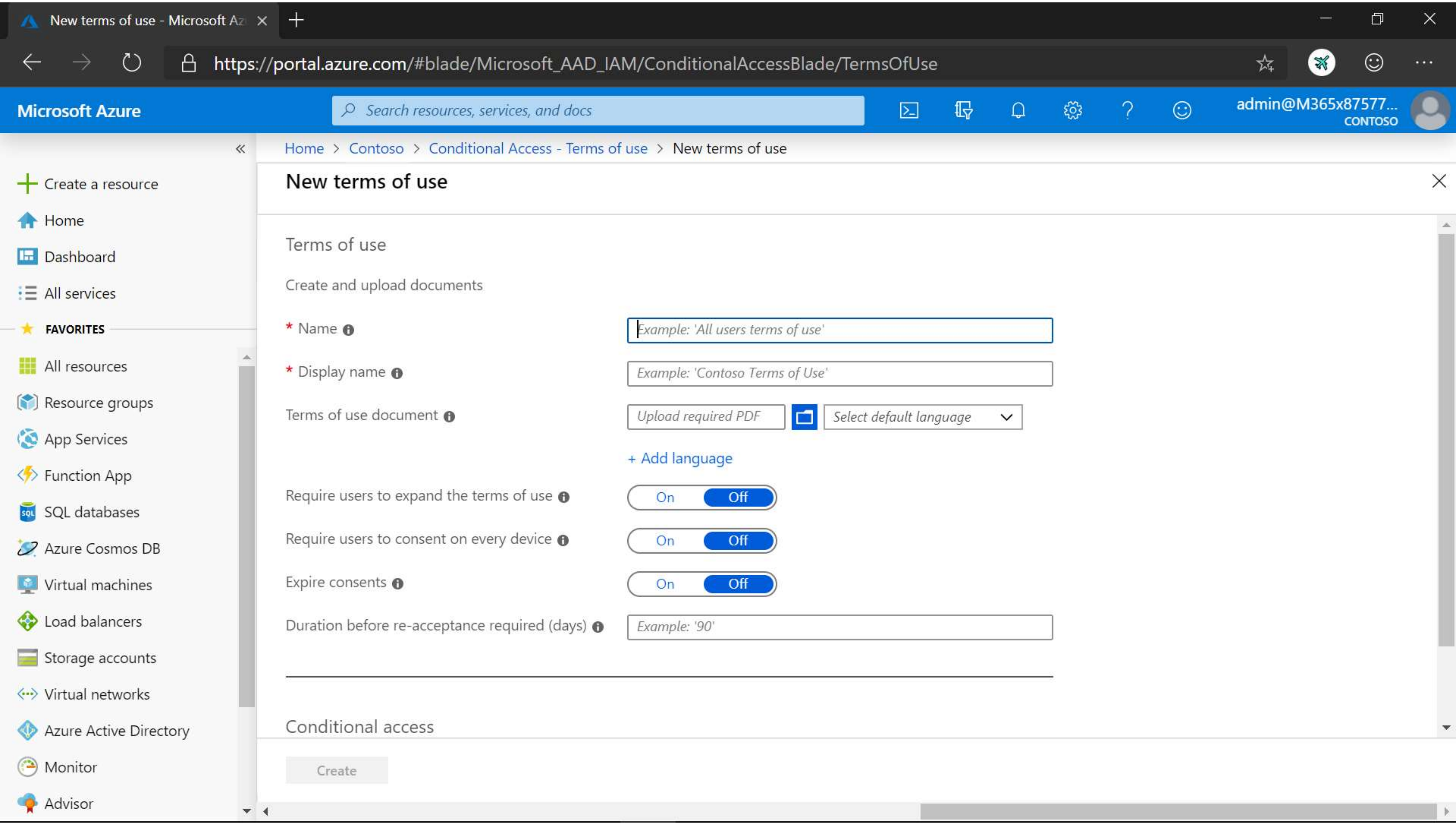


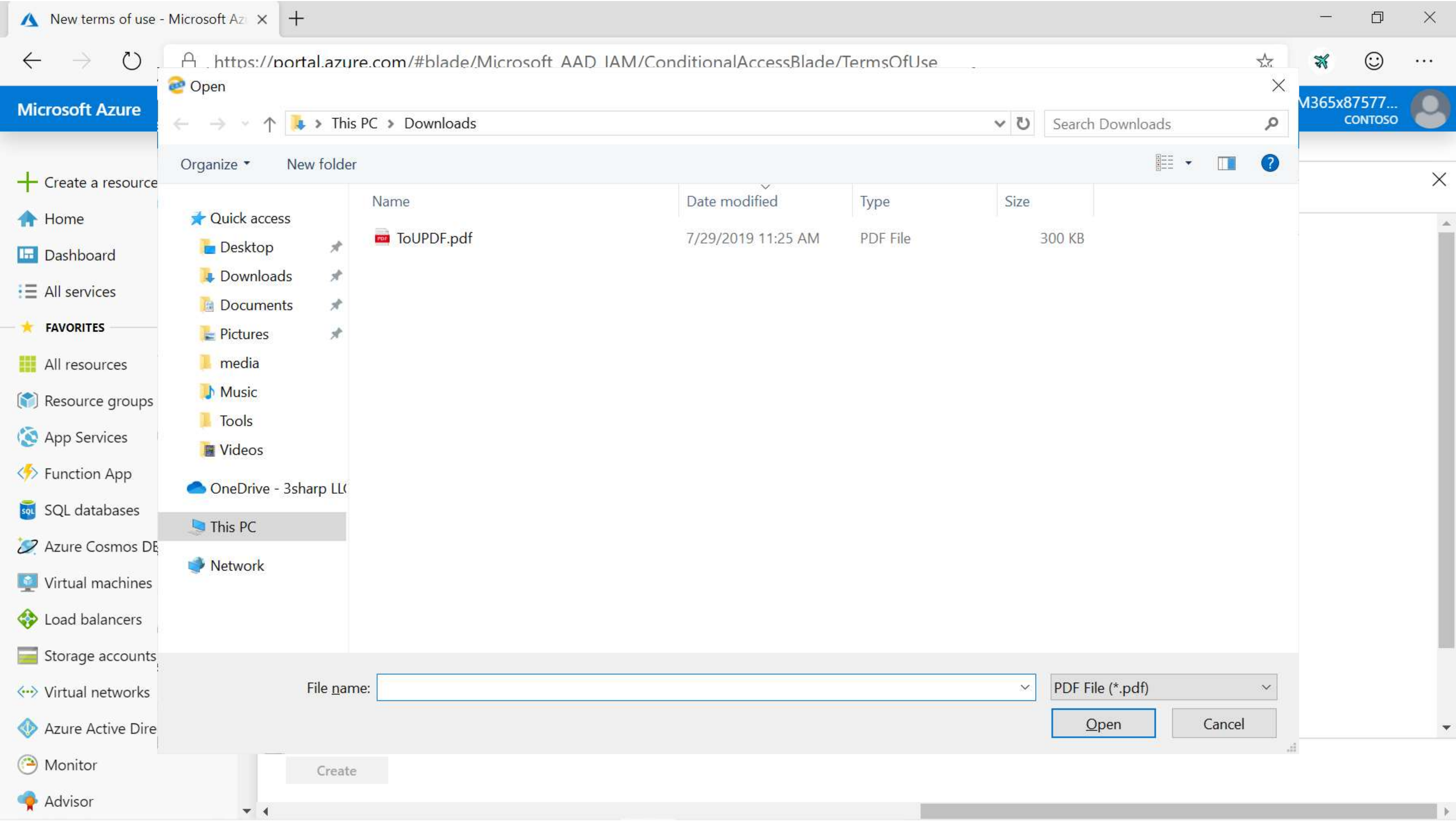
Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

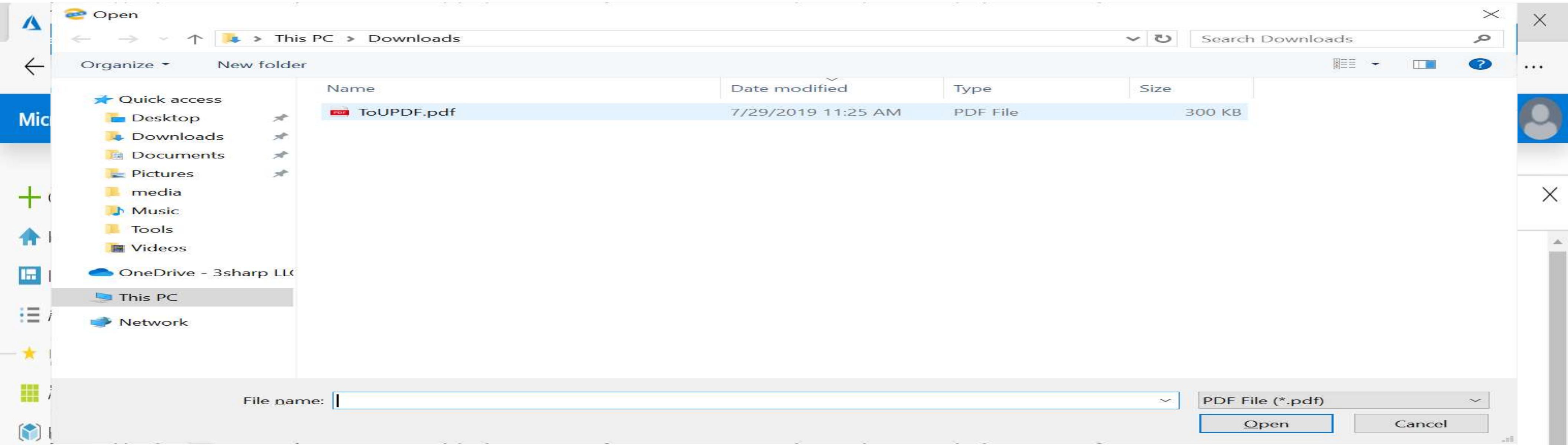
POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...



No terms of use to display

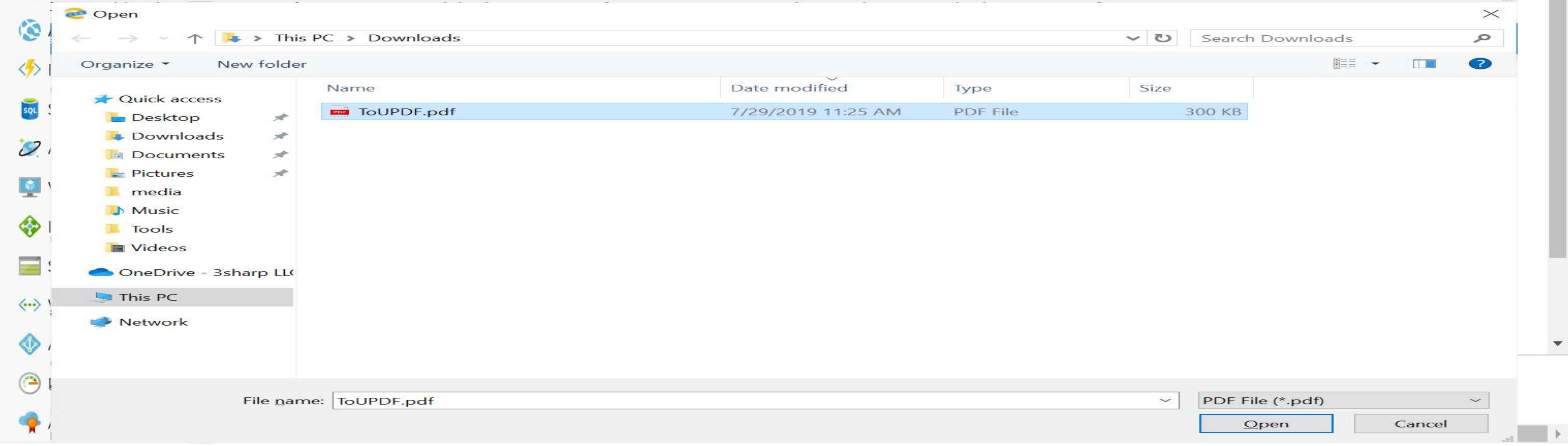



New terms of use - Microsoft Az
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/TermsOfUse
Microsoft Azure
M365x87577...
CONTOSO
Open
This PC > Downloads
Search Downloads
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
media
Music
Tools
Videos
OneDrive - 3sharp LL
This PC
Network
Name
Date modified
Type
Size
ToUPDF.pdf
7/29/2019 11:25 AM
PDF File
300 KB
File name:
PDF File (*.pdf)
Open
Cancel
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Dire
Monitor
Advisor
Create



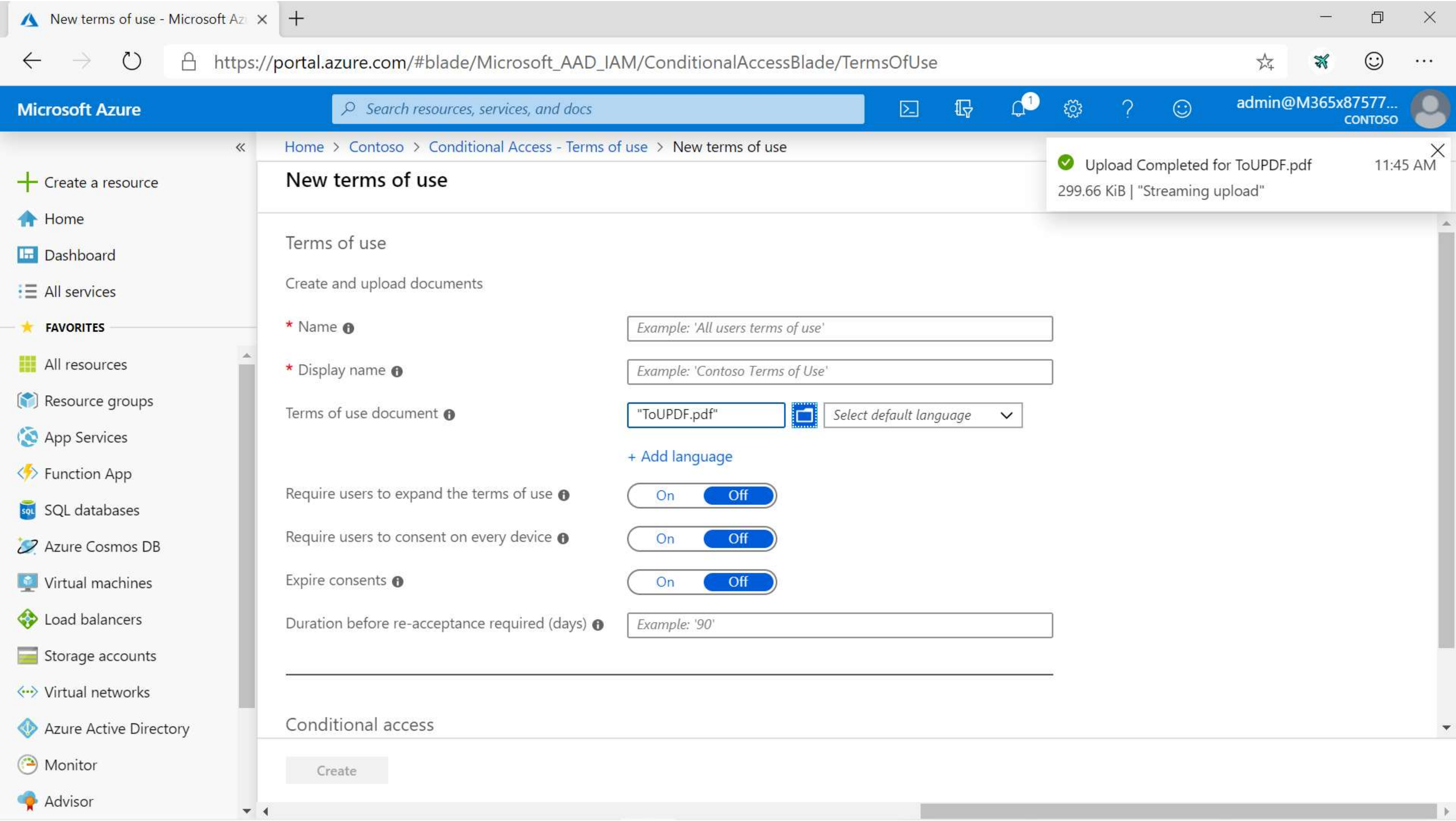
Name	Date modified	Type	Size
ToUPDF.pdf	7/29/2019 11:25 AM	PDF File	300 KB

File name:



Name	Date modified	Type	Size
ToUPDF.pdf	7/29/2019 11:25 AM	PDF File	300 KB

File name: ToUPDF.pdf



Upload Completed for ToUPDF.pdf 11:45 AM
299.66 KiB | "Streaming upload"

New terms of use

Terms of use

Create and upload documents

* Name: Example: 'All users terms of use'

* Display name: Example: 'Contoso Terms of Use'

Terms of use document: "ToUPDF.pdf" | Select default language

+ Add language

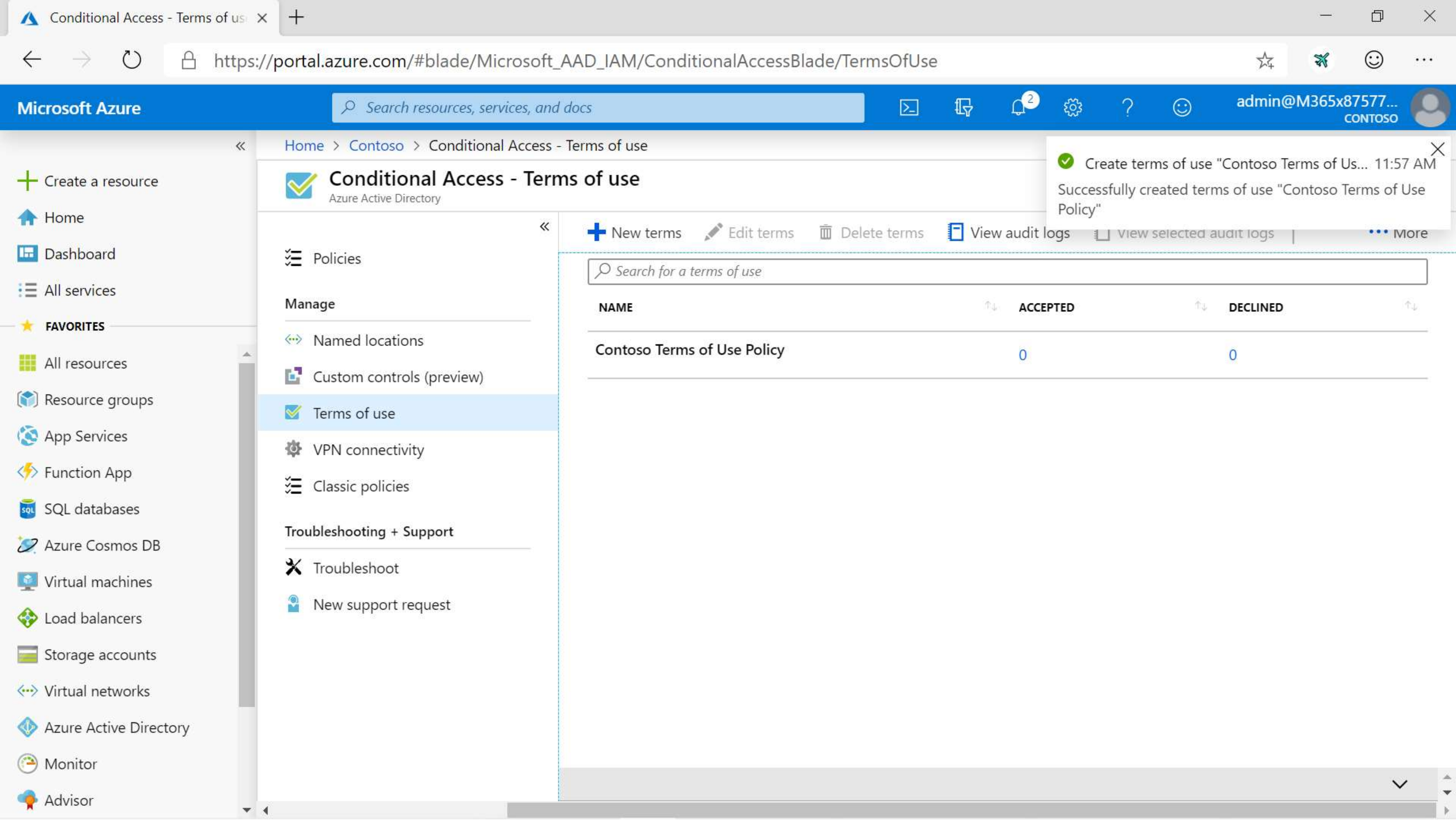
Require users to expand the terms of use: On [✓ Off]

Require users to consent on every device: On [✓ Off]

Expire consents: On [✓ Off]

Duration before re-acceptance required (days): Example: '90'

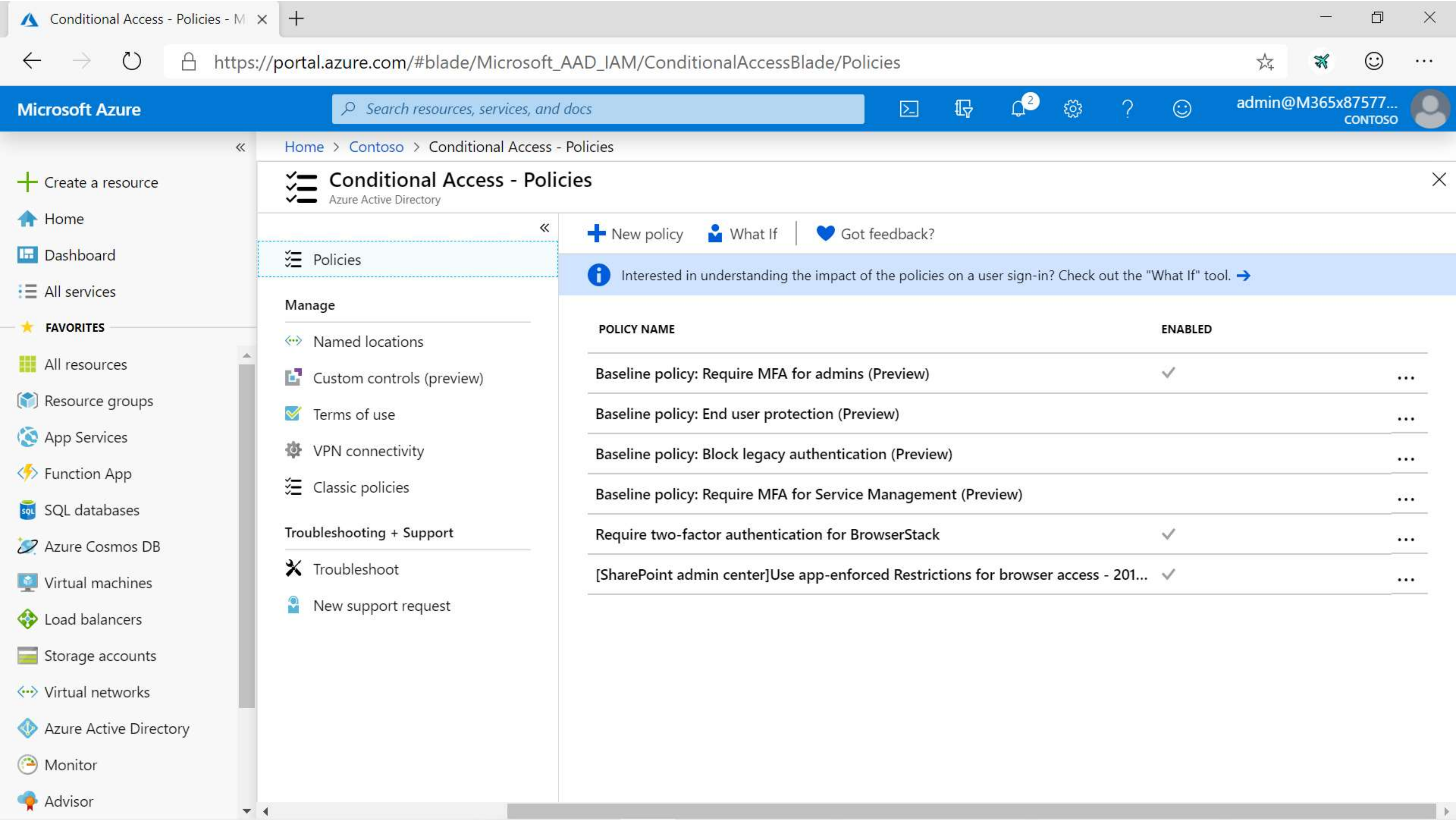
Conditional access



Create terms of use "Contoso Terms of Us... 11:57 AM

Successfully created terms of use "Contoso Terms of Use Policy"

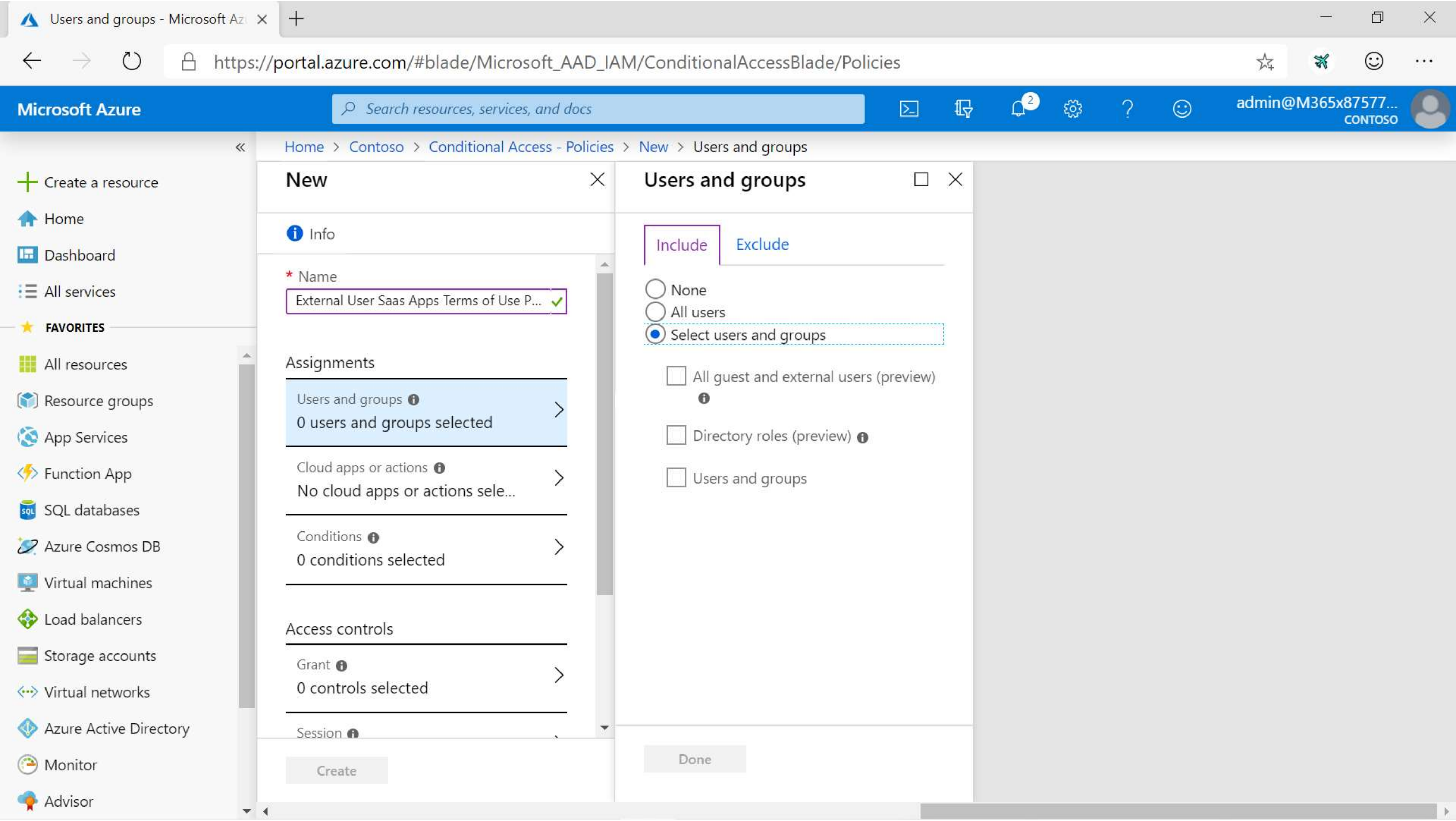
NAME	ACCEPTED	DECLINED
Contoso Terms of Use Policy	0	0



https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies

Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...



* Name: External User Saas Apps Terms of Use P... ✓

Users and groups: 0 users and groups selected

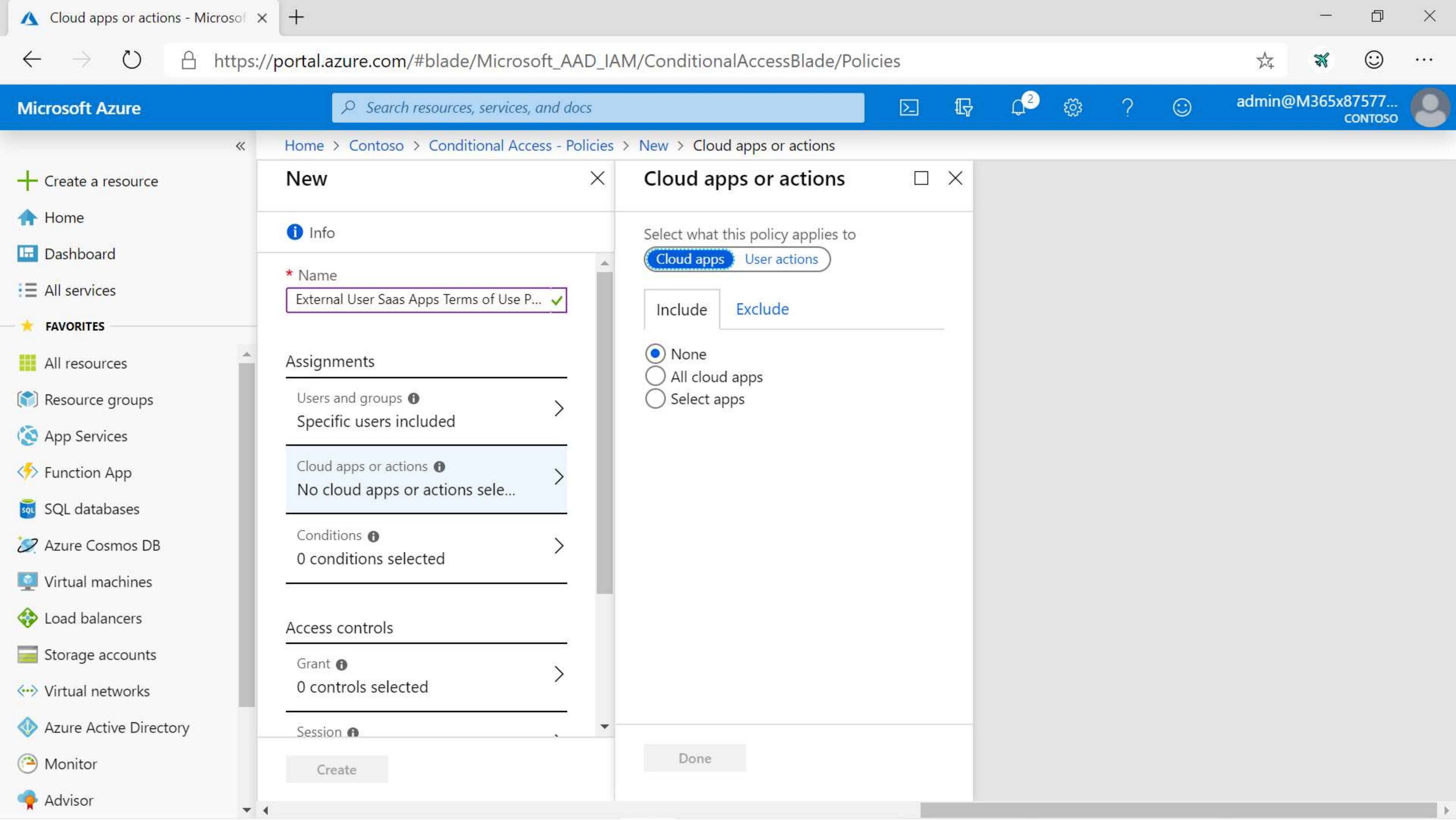
Cloud apps or actions: No cloud apps or actions sele...

Conditions: 0 conditions selected

Grant: 0 controls selected

Include:

○ None
○ All users
● Select users and groups
  ☐ All guest and external users (preview)
  ☐ Directory roles (preview)
  ☐ Users and groups



* Name: External User Saas Apps Terms of Use P... ✓

Users and groups: Specific users included

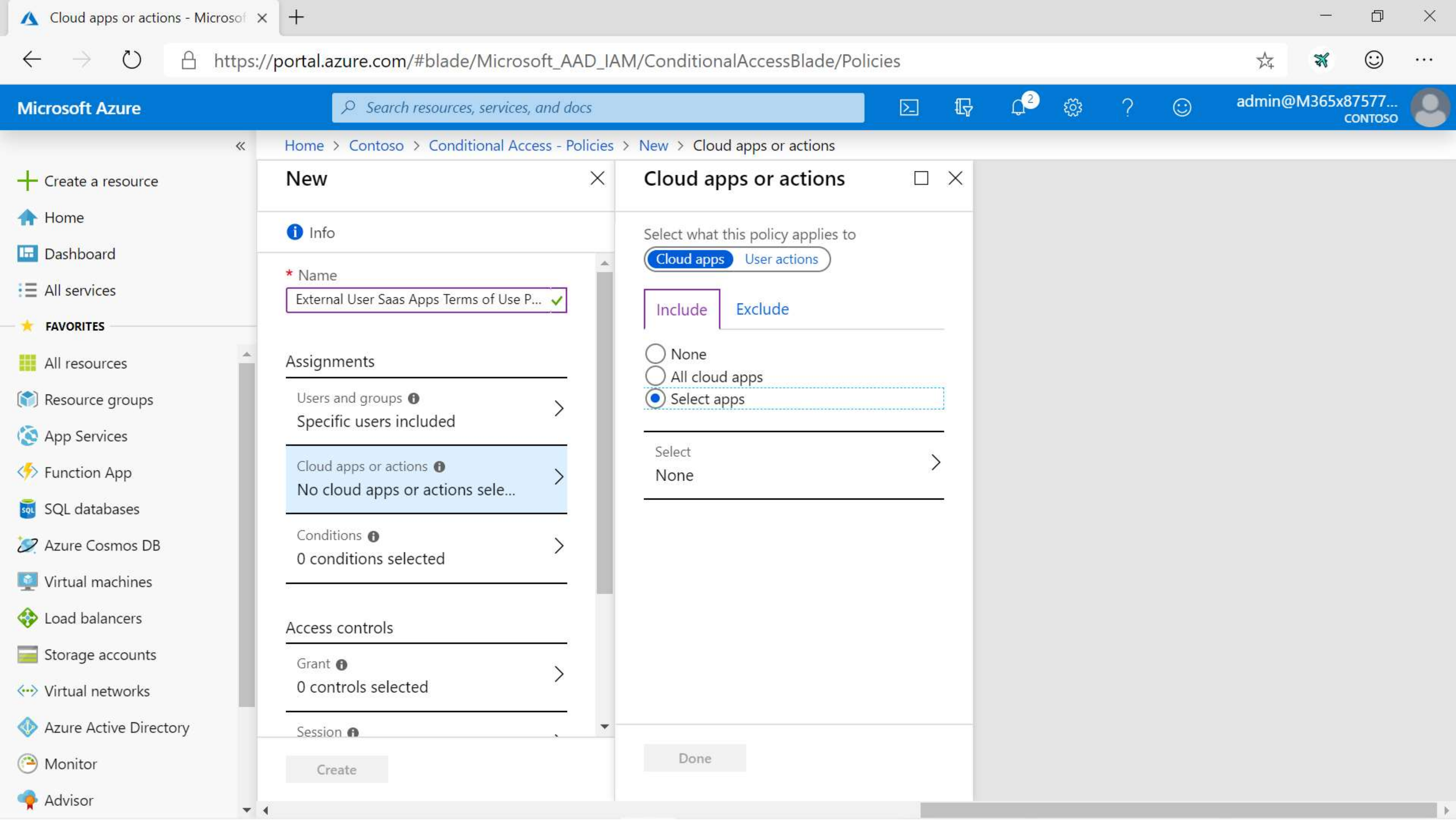
Cloud apps or actions: No cloud apps or actions sele...

Conditions: 0 conditions selected

Grant: 0 controls selected

Select what this policy applies to: Cloud apps

Include:
● None
○ All cloud apps
○ Select apps



New

* Name: External User Saas Apps Terms of Use P... ✓

Assignments

- Users and groups: Specific users included
- Cloud apps or actions: No cloud apps or actions sele...
- Conditions: 0 conditions selected

Access controls

- Grant: 0 controls selected
- Session

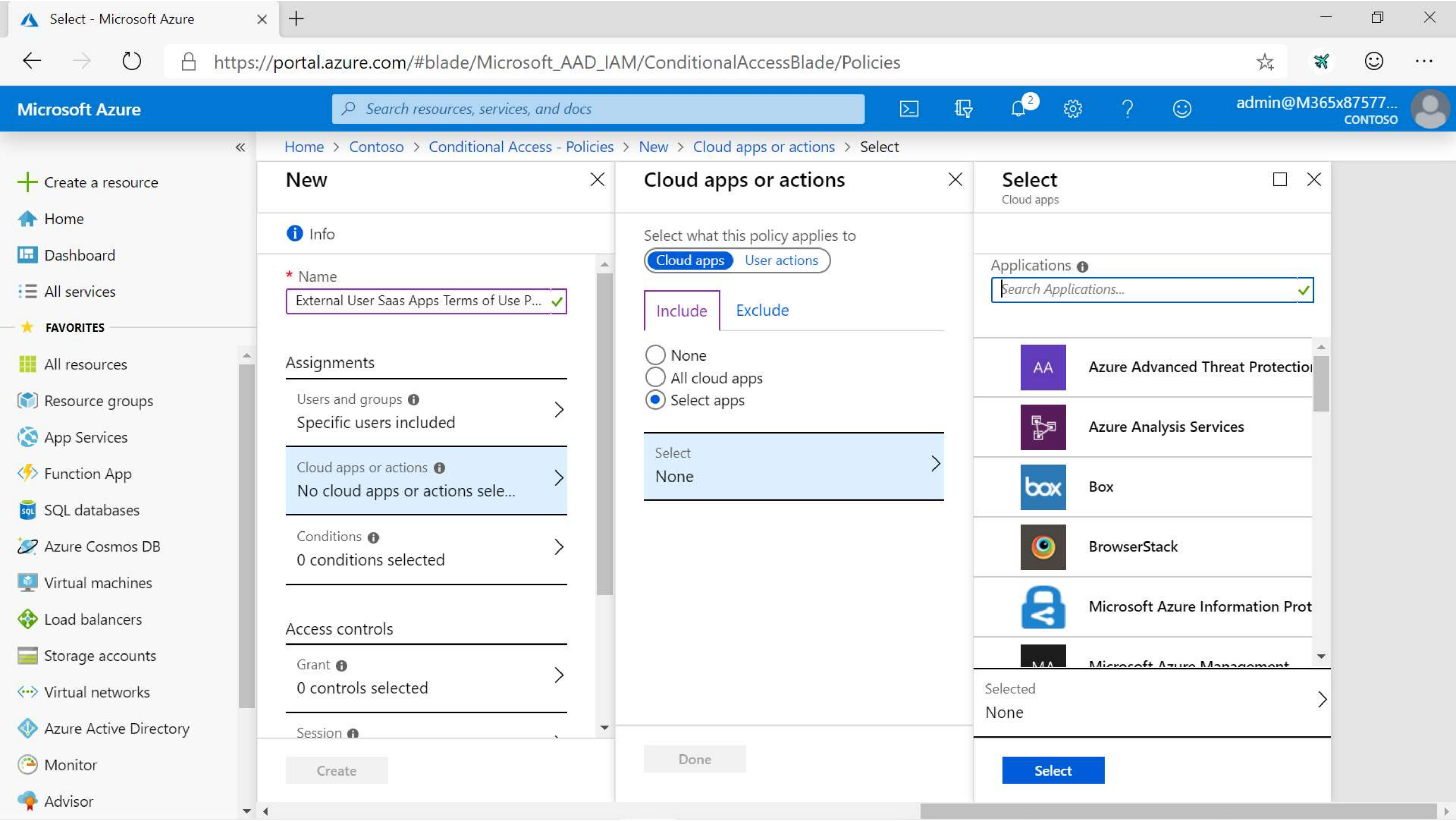
Cloud apps or actions

Select what this policy applies to: [✓ Cloud apps] User actions

Include | Exclude

○ None
○ All cloud apps
● Select apps

Select: None



New

Info

* Name: External User Saas Apps Terms of Use P... ✓

Assignments

- Users and groups: Specific users included
- Cloud apps or actions: No cloud apps or actions sele...
- Conditions: 0 conditions selected

Access controls

- Grant: 0 controls selected
- Session

Cloud apps or actions

Select what this policy applies to: Cloud apps | User actions

Include | Exclude

○ None
○ All cloud apps
● Select apps

Select: None

Select

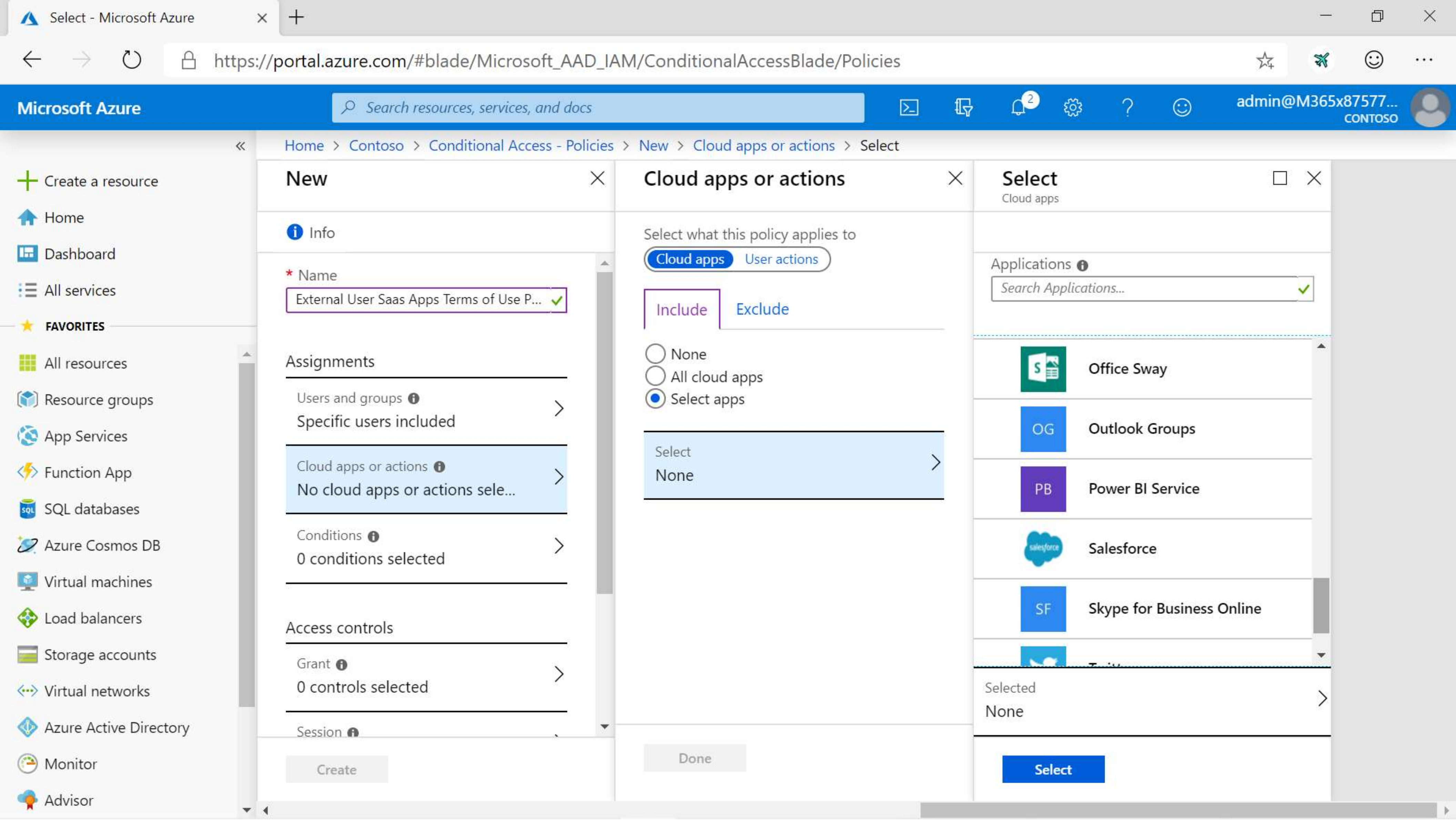
Cloud apps

Applications

Search Applications...

- Azure Advanced Threat Protectio
- Azure Analysis Services
- Box
- BrowserStack
- Microsoft Azure Information Prot
- Microsoft Azure Management

Selected: None



https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies

* Name: External User Saas Apps Terms of Use P...

Users and groups: Specific users included

Cloud apps or actions: No cloud apps or actions sele...

Conditions: 0 conditions selected

Grant: 0 controls selected

Session

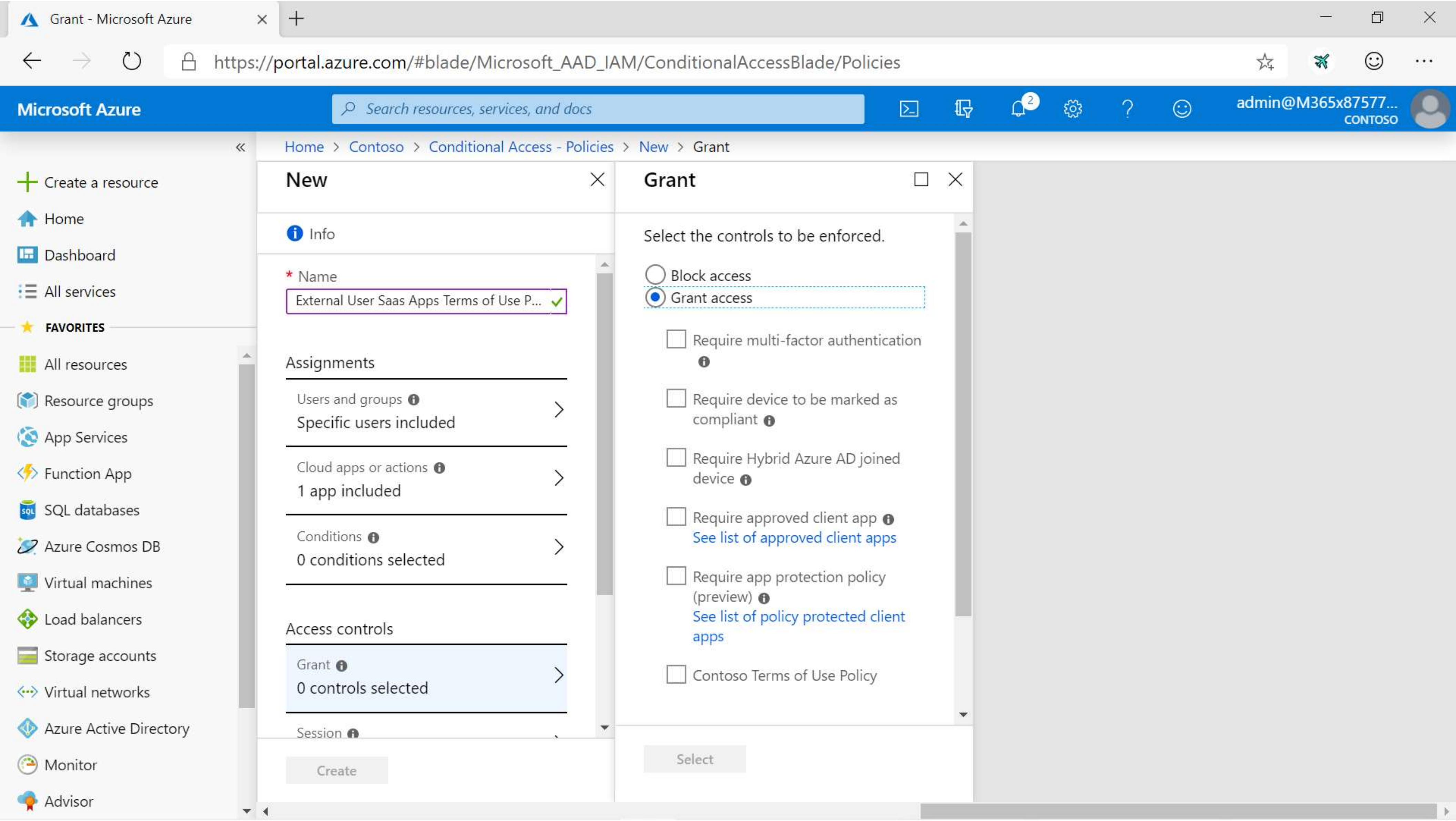
Select what this policy applies to: Cloud apps | User actions

Include | Exclude

○ None
○ All cloud apps
● Select apps

Select: None

Selected: None



Home > Contoso > Conditional Access - Policies > New > Grant

New

Info

* Name: External User Saas Apps Terms of Use P... ✓

Assignments

- Users and groups: Specific users included
- Cloud apps or actions: 1 app included
- Conditions: 0 conditions selected

Access controls

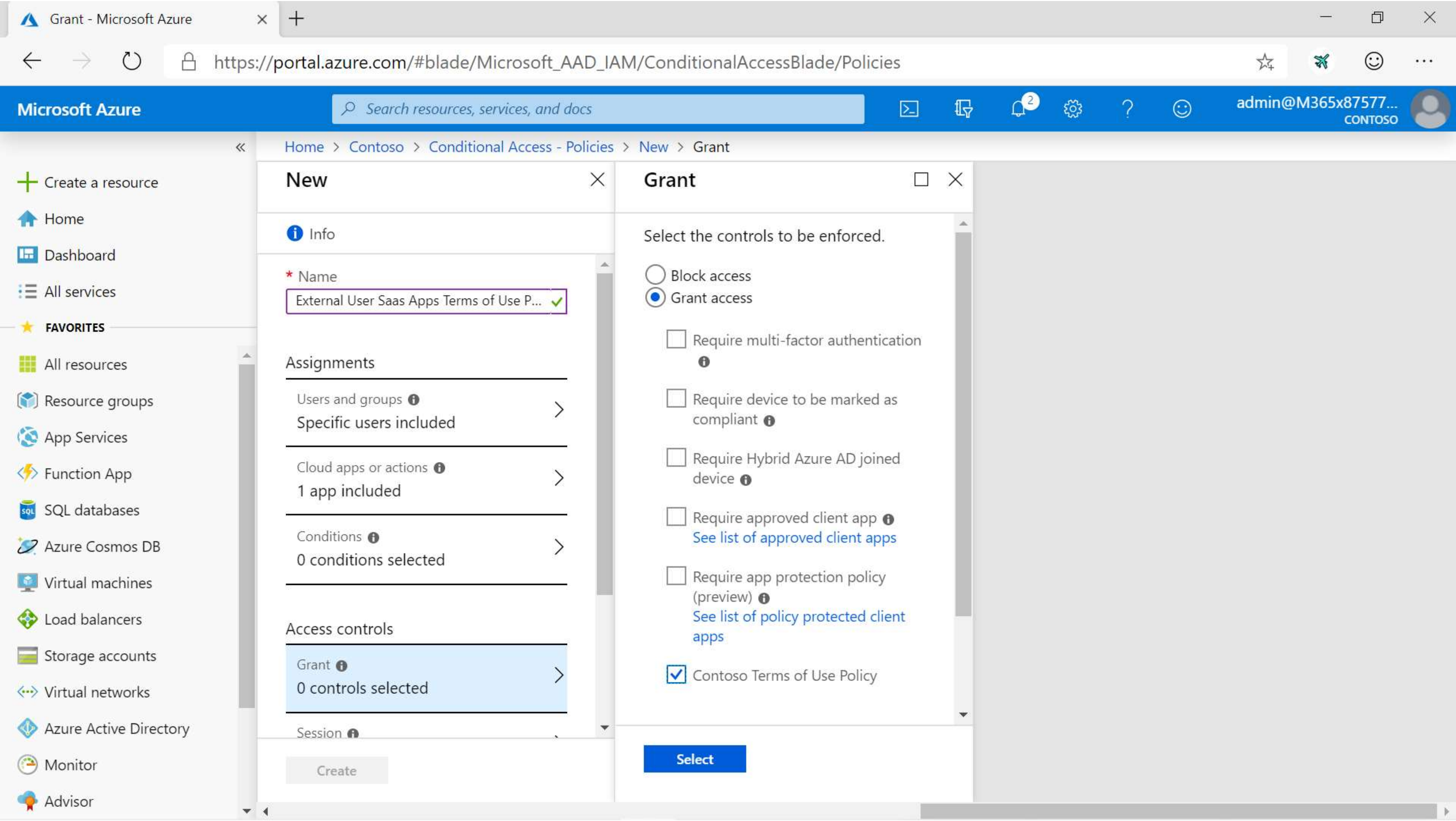
- Grant: 0 controls selected
- Session

Grant

Select the controls to be enforced.

○ Block access
● Grant access

☐ Require multi-factor authentication
☐ Require device to be marked as compliant
☐ Require Hybrid Azure AD joined device
☐ Require approved client app
See list of approved client apps
☐ Require app protection policy (preview)
See list of policy protected client apps
☐ Contoso Terms of Use Policy



* Name: External User Saas Apps Terms of Use P... ✓

Users and groups: Specific users included

Cloud apps or actions: 1 app included

Conditions: 0 conditions selected

Grant: 0 controls selected

Select the controls to be enforced.

○ Block access

● Grant access

☐ Require multi-factor authentication

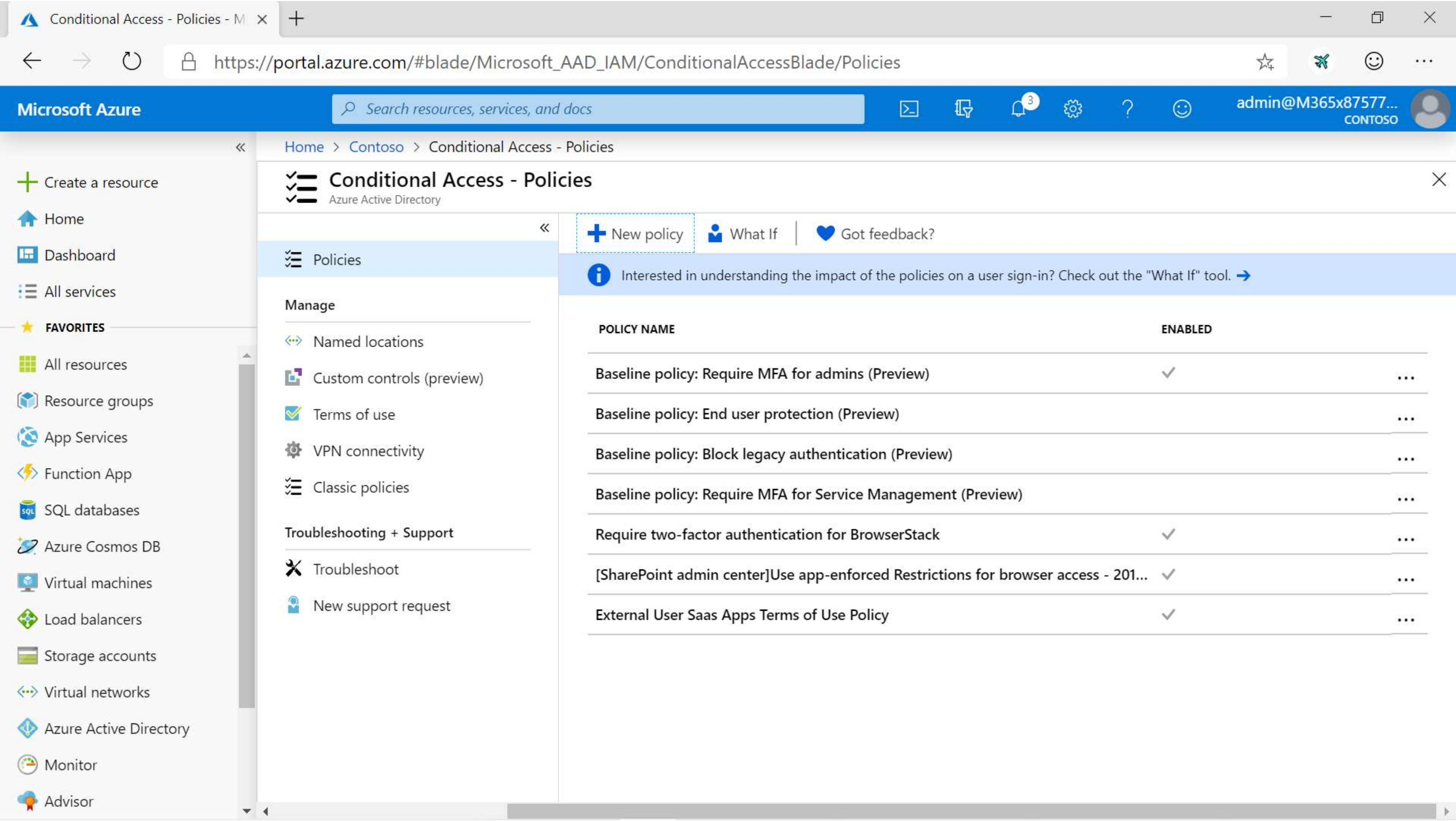
☐ Require device to be marked as compliant

☐ Require Hybrid Azure AD joined device

☐ Require approved client app
See list of approved client apps

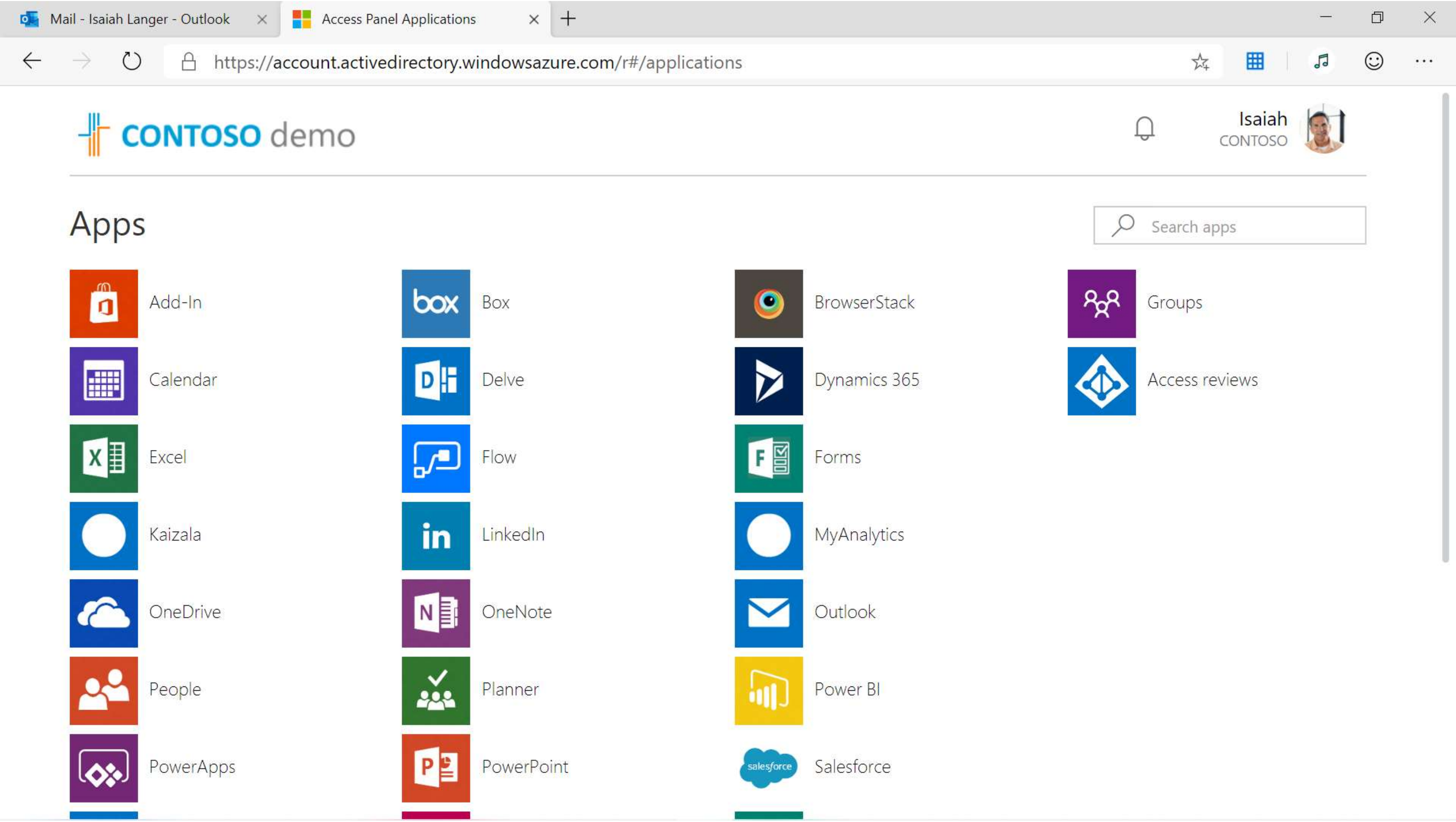
☐ Require app protection policy (preview)
See list of policy protected client apps

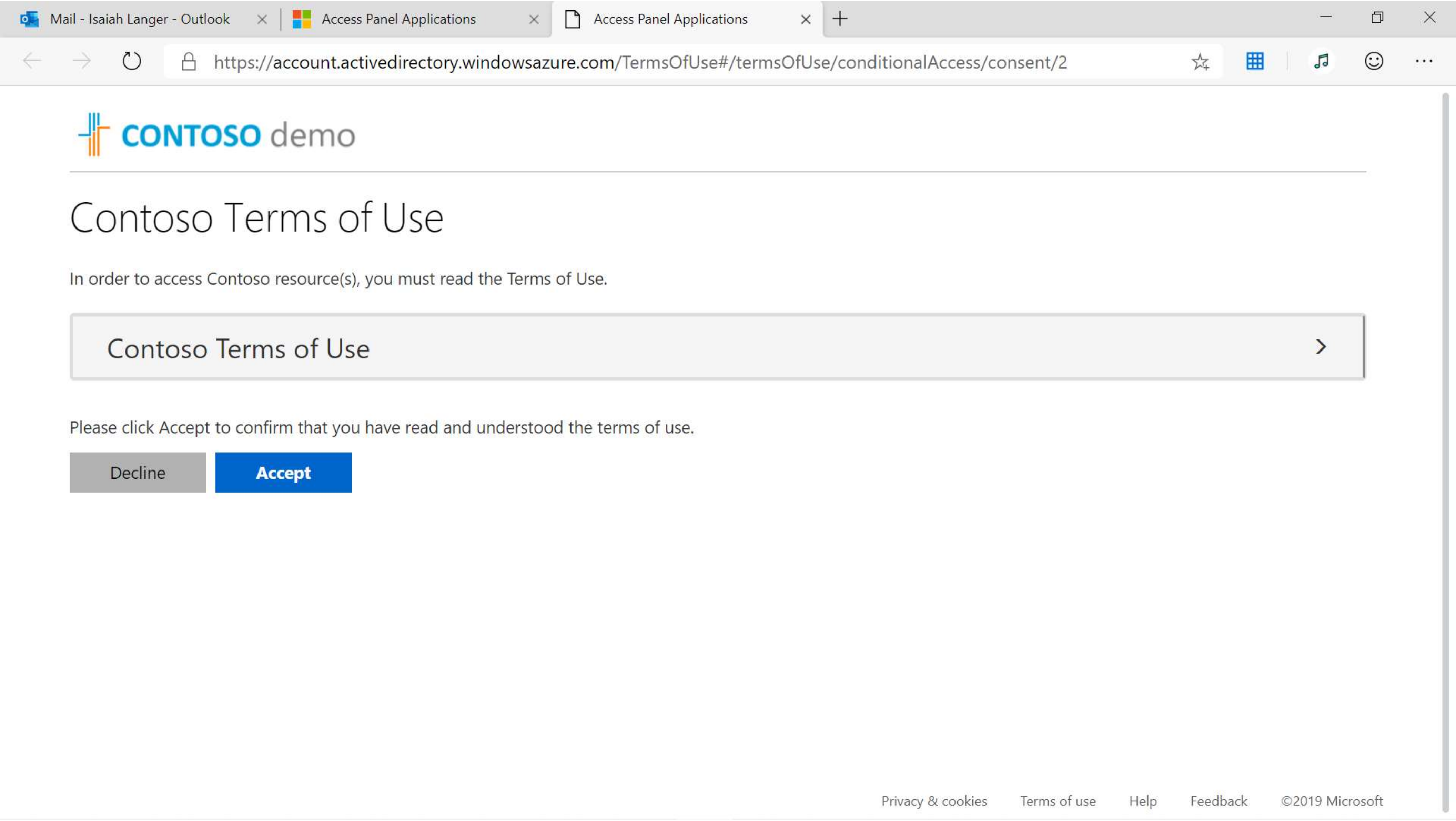
☑ Contoso Terms of Use Policy



Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool. →

POLICY NAME	ENABLED	
Baseline policy: Require MFA for admins (Preview)	✓	...
Baseline policy: End user protection (Preview)		...
Baseline policy: Block legacy authentication (Preview)		...
Baseline policy: Require MFA for Service Management (Preview)		...
Require two-factor authentication for BrowserStack	✓	...
[SharePoint admin center]Use app-enforced Restrictions for browser access - 201...	✓	...
External User Saas Apps Terms of Use Policy	✓	...


Mail - Isaiah Langer - Outlook
Access Panel Applications
https://account.activedirectory.windowsazure.com/r#/applications
CONTOSO demo
Isaiah
CONTOSO
Apps
Search apps
Add-In
Box
BrowserStack
Groups
Calendar
Delve
Dynamics 365
Access reviews
Excel
Flow
Forms
Kaizala
LinkedIn
MyAnalytics
OneDrive
OneNote
Outlook
People
Planner
Power BI
PowerApps
PowerPoint
Salesforce


Mail - Isaiah Langer - Outlook
Access Panel Applications
Access Panel Applications
https://account.activedirectory.windowsazure.com/TermsOfUse#/termsOfUse/conditionalAccess/consent/2
CONTOSO demo

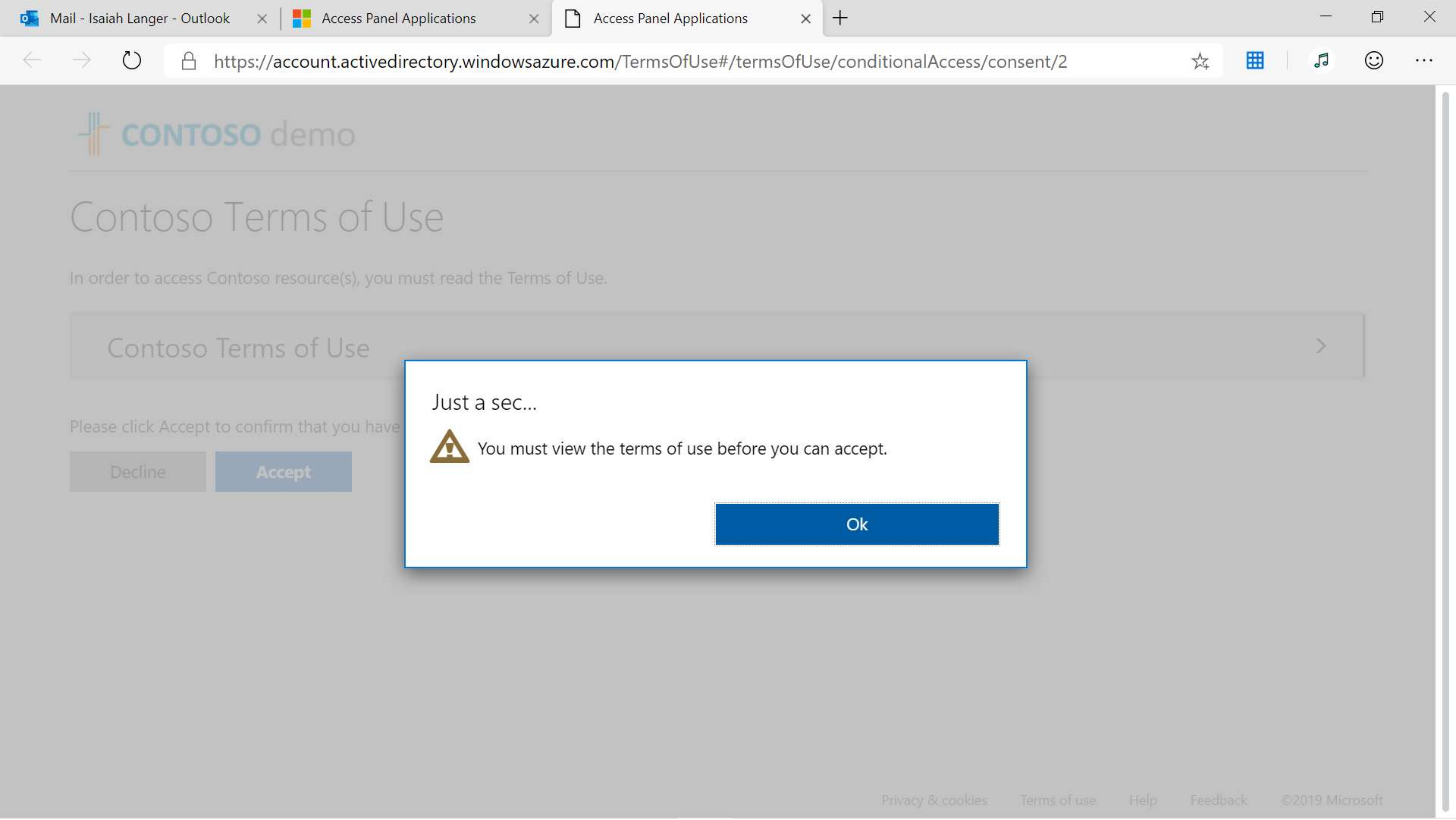
Contoso Terms of Use

In order to access Contoso resource(s), you must read the Terms of Use.

Contoso Terms of Use >

Please click Accept to confirm that you have read and understood the terms of use.

Decline
Accept
Privacy & cookies
Terms of use
Help
Feedback
©2019 Microsoft



Mail - Isaiah Langer - Outlook
Access Panel Applications
Access Panel Applications
https://account.activedirectory.windowsazure.com/TermsOfUse#/termsOfUse/conditionalAccess/consent/2
CONTOSO demo

Contoso Terms of Use

In order to access Contoso resource(s), you must read the Terms of Use.

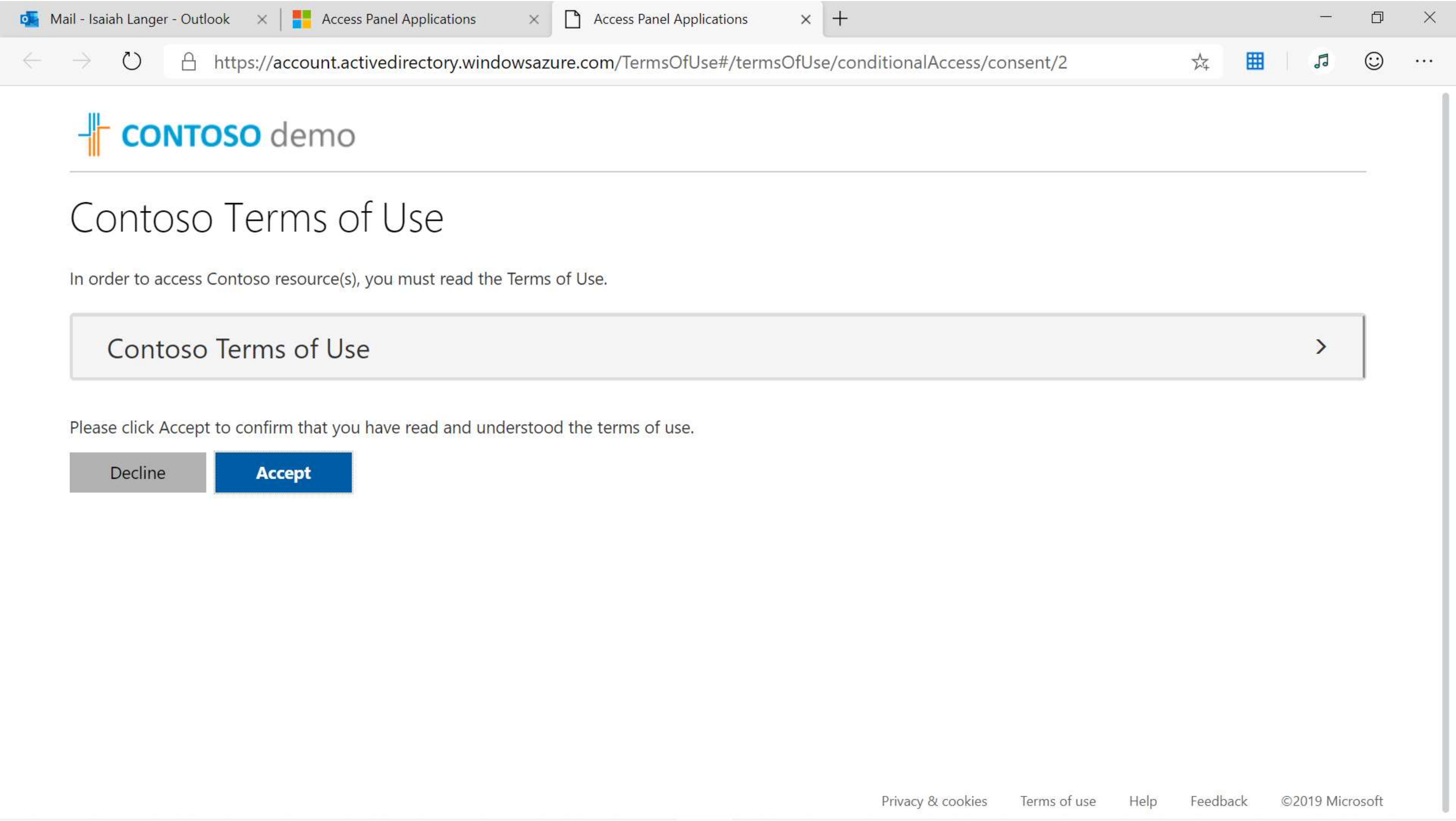
Contoso Terms of Use

Please click Accept to confirm that you have

Just a sec...

You must view the terms of use before you can accept.

Ok
Privacy & cookies
Terms of use
Help
Feedback
©2019 Microsoft

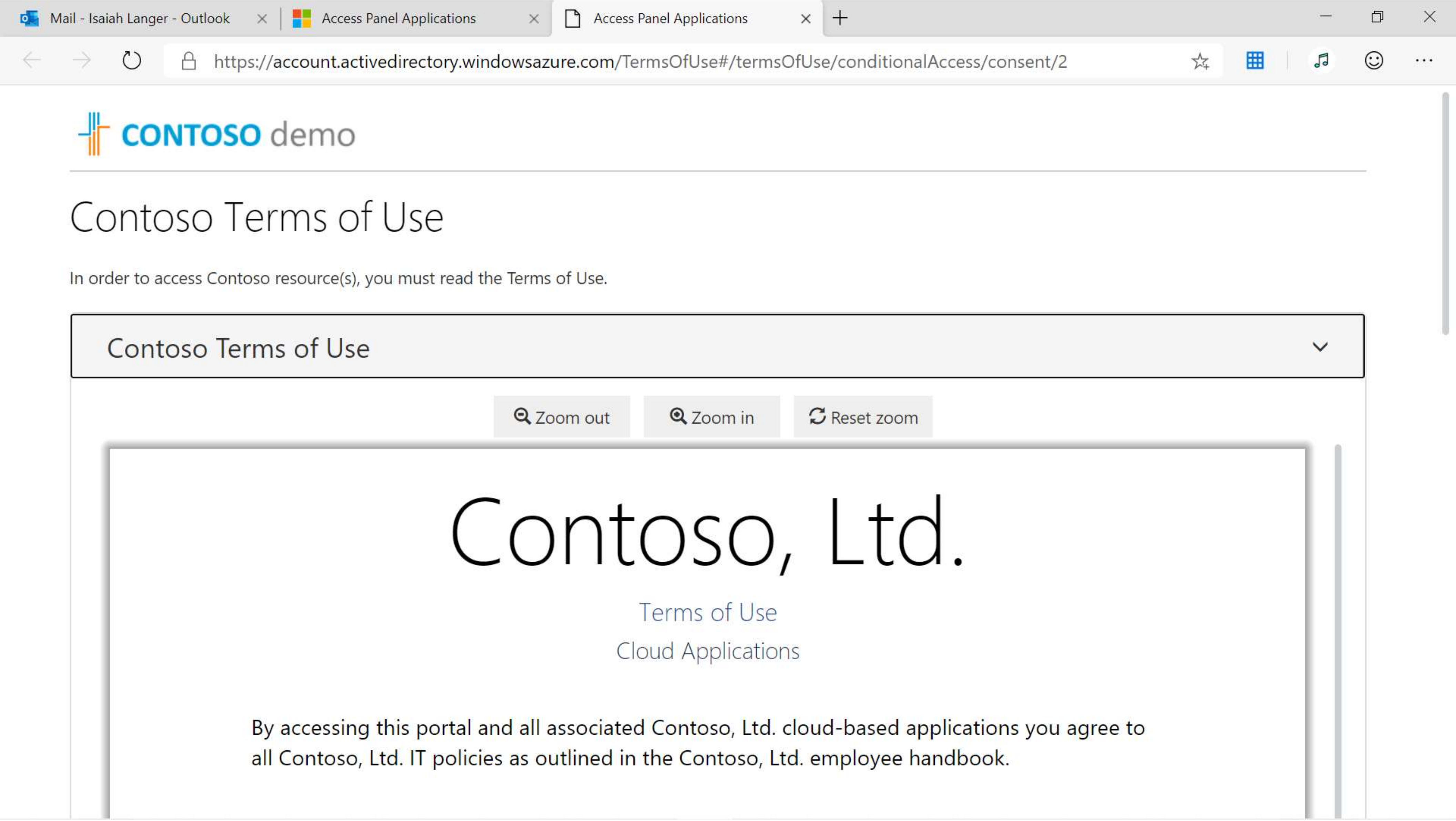

Mail - Isaiah Langer - Outlook
Access Panel Applications
Access Panel Applications
https://account.activedirectory.windowsazure.com/TermsOfUse#/termsOfUse/conditionalAccess/consent/2
CONTOSO demo
Decline
Accept
Privacy & cookies
Terms of use
Help
Feedback
©2019 Microsoft

Contoso Terms of Use

In order to access Contoso resource(s), you must read the Terms of Use.

Contoso Terms of Use >

Please click Accept to confirm that you have read and understood the terms of use.


Mail - Isaiah Langer - Outlook
Access Panel Applications
Access Panel Applications
https://account.activedirectory.windowsazure.com/TermsOfUse#/termsOfUse/conditionalAccess/consent/2
CONTOSO demo

Contoso Terms of Use

In order to access Contoso resource(s), you must read the Terms of Use.

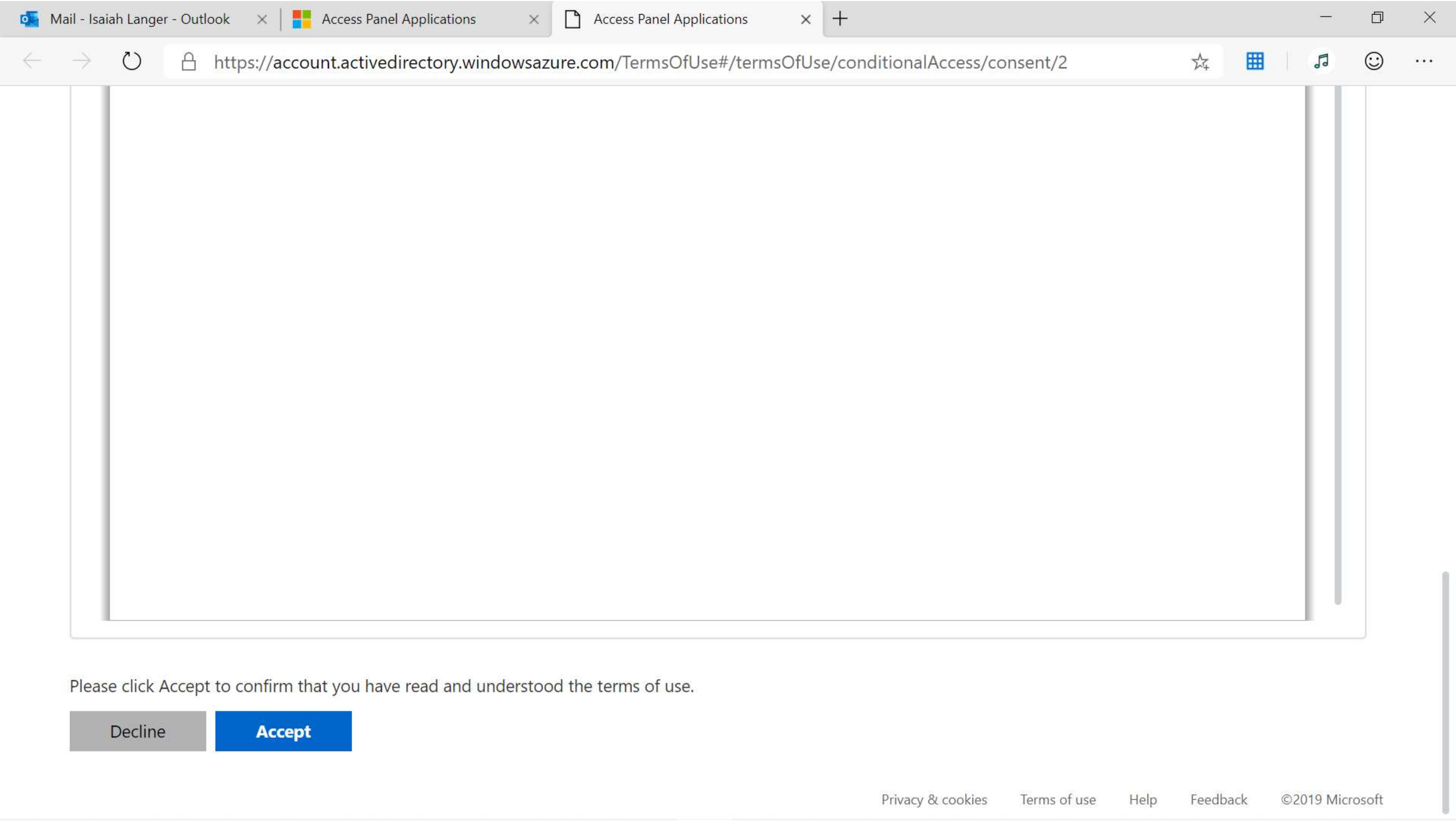
Contoso Terms of Use
Zoom out
Zoom in
Reset zoom

Contoso, Ltd.

Terms of Use

Cloud Applications

By accessing this portal and all associated Contoso, Ltd. cloud-based applications you agree to all Contoso, Ltd. IT policies as outlined in the Contoso, Ltd. employee handbook.

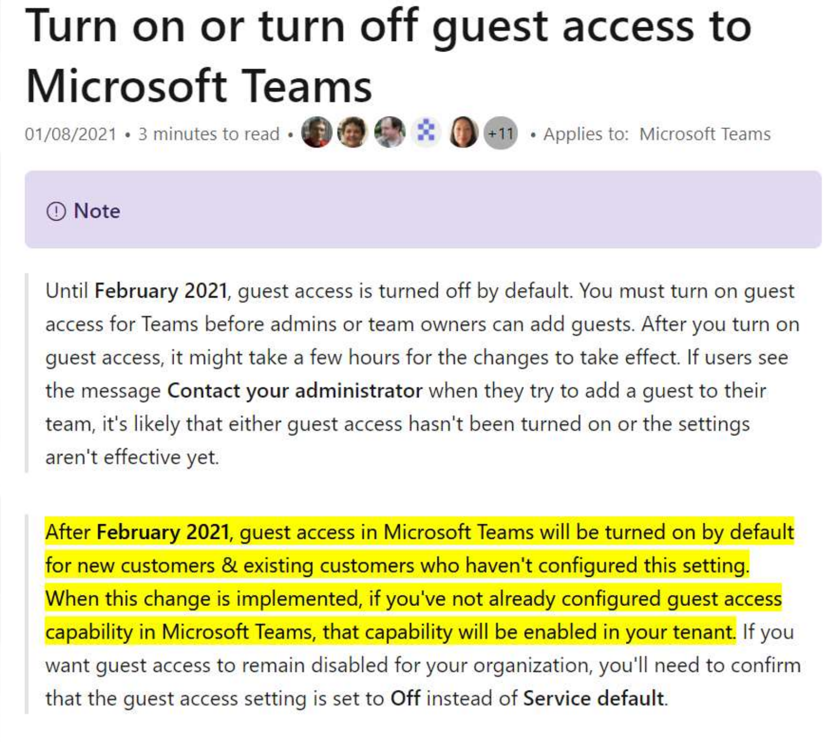

Mail - Isaiah Langer - Outlook
Access Panel Applications
Access Panel Applications
https://account.activedirectory.windowsazure.com/TermsOfUse#/termsOfUse/conditionalAccess/consent/2

Please click Accept to confirm that you have read and understood the terms of use.

Decline
Accept
Privacy & cookies
Terms of use
Help
Feedback
©2019 Microsoft

What is Azue AD B2B and "External Identities"?

External access to SharePoint, Groups and Teams is "on by default" in M365 and "*open* for business"



Turn on or turn off guest access to Microsoft Teams

01/08/2021 • 3 minutes to read • +11 • Applies to: Microsoft Teams

ⓘ Note

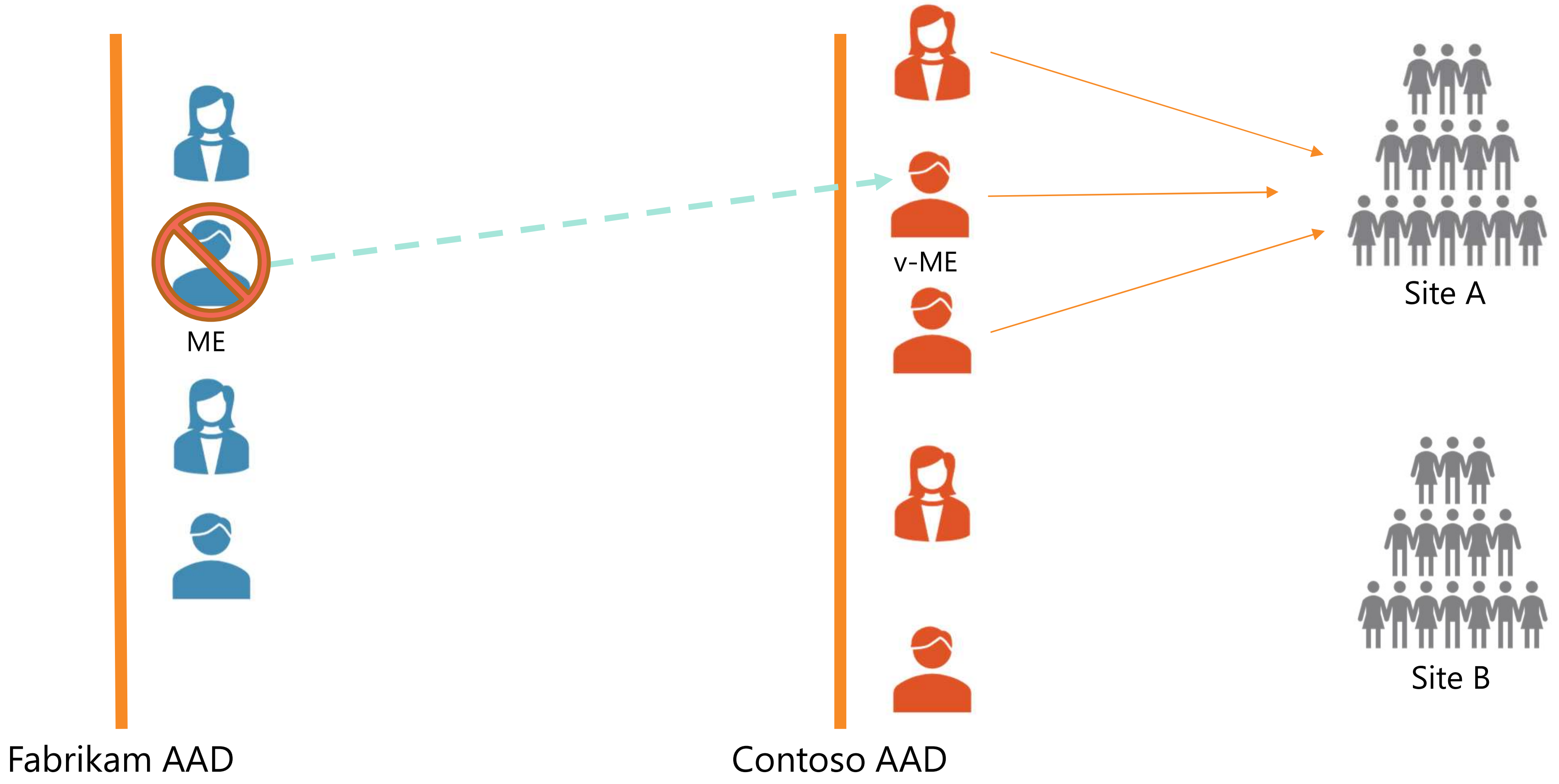
Until **February 2021**, guest access is turned off by default. You must turn on guest access for Teams before admins or team owners can add guests. After you turn on guest access, it might take a few hours for the changes to take effect. If users see the message **Contact your administrator** when they try to add a guest to their team, it's likely that either guest access hasn't been turned on or the settings aren't effective yet.

After **February 2021**, guest access in Microsoft Teams will be turned on by default for new customers & existing customers who haven't configured this setting. When this change is implemented, if you've not already configured guest access capability in Microsoft Teams, that capability will be enabled in your tenant. If you want guest access to remain disabled for your organization, you'll need to confirm that the guest access setting is set to **Off** instead of **Service default**.

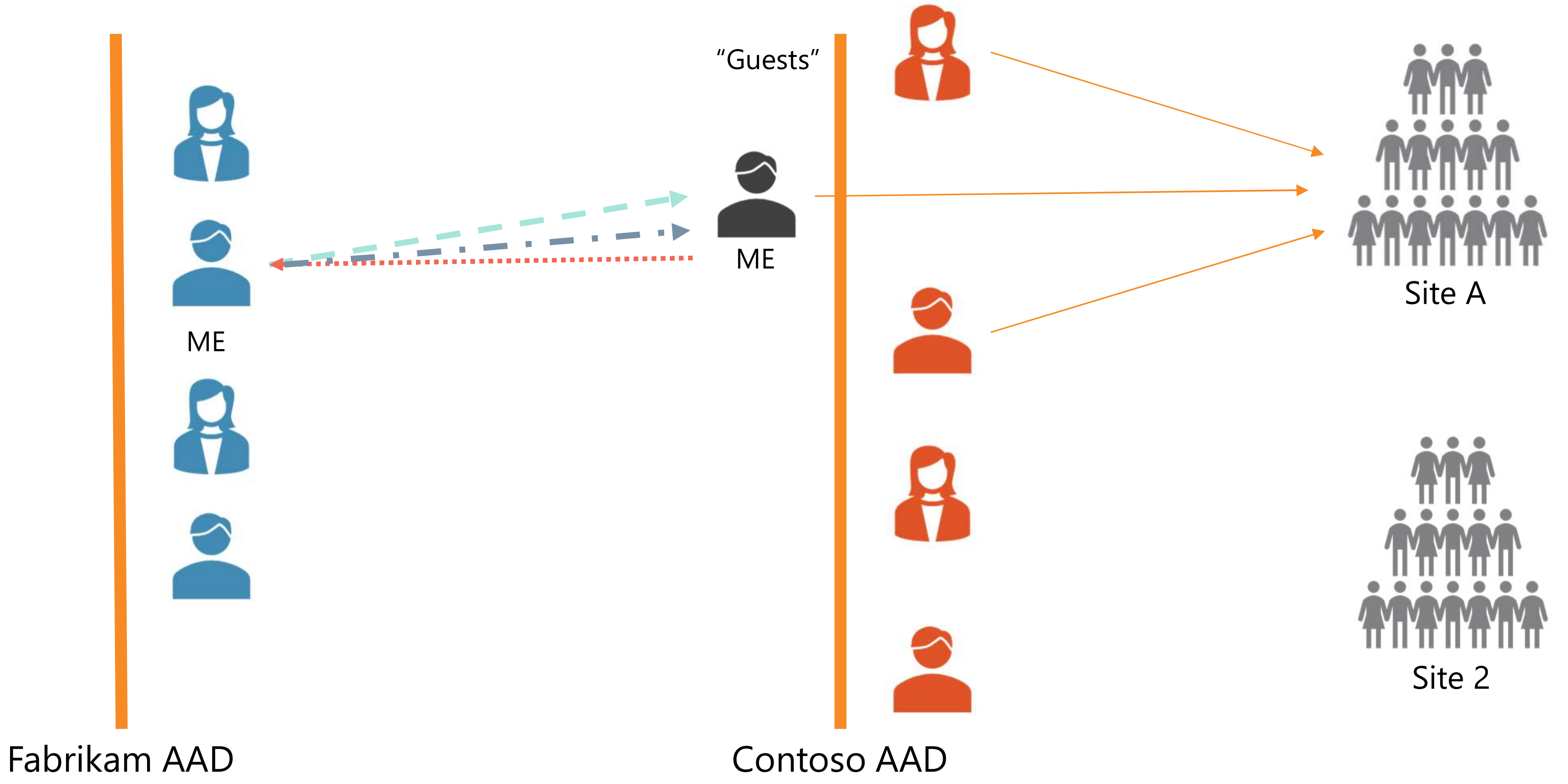
Understanding the Azure AD “Guest” Model

The foundation of external collaboration in Teams

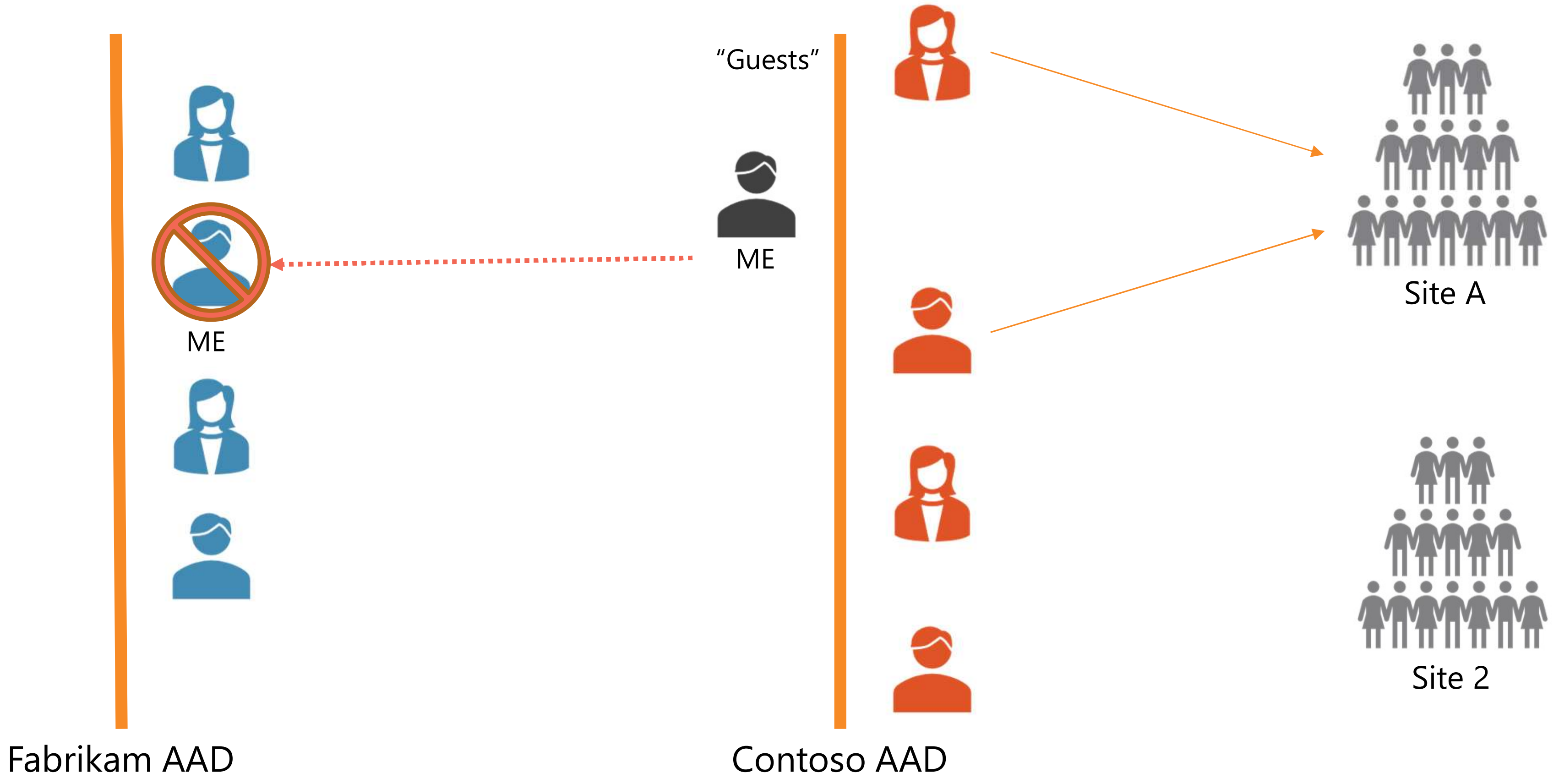
"In the beginning…"



The Azure B2B Guest Model



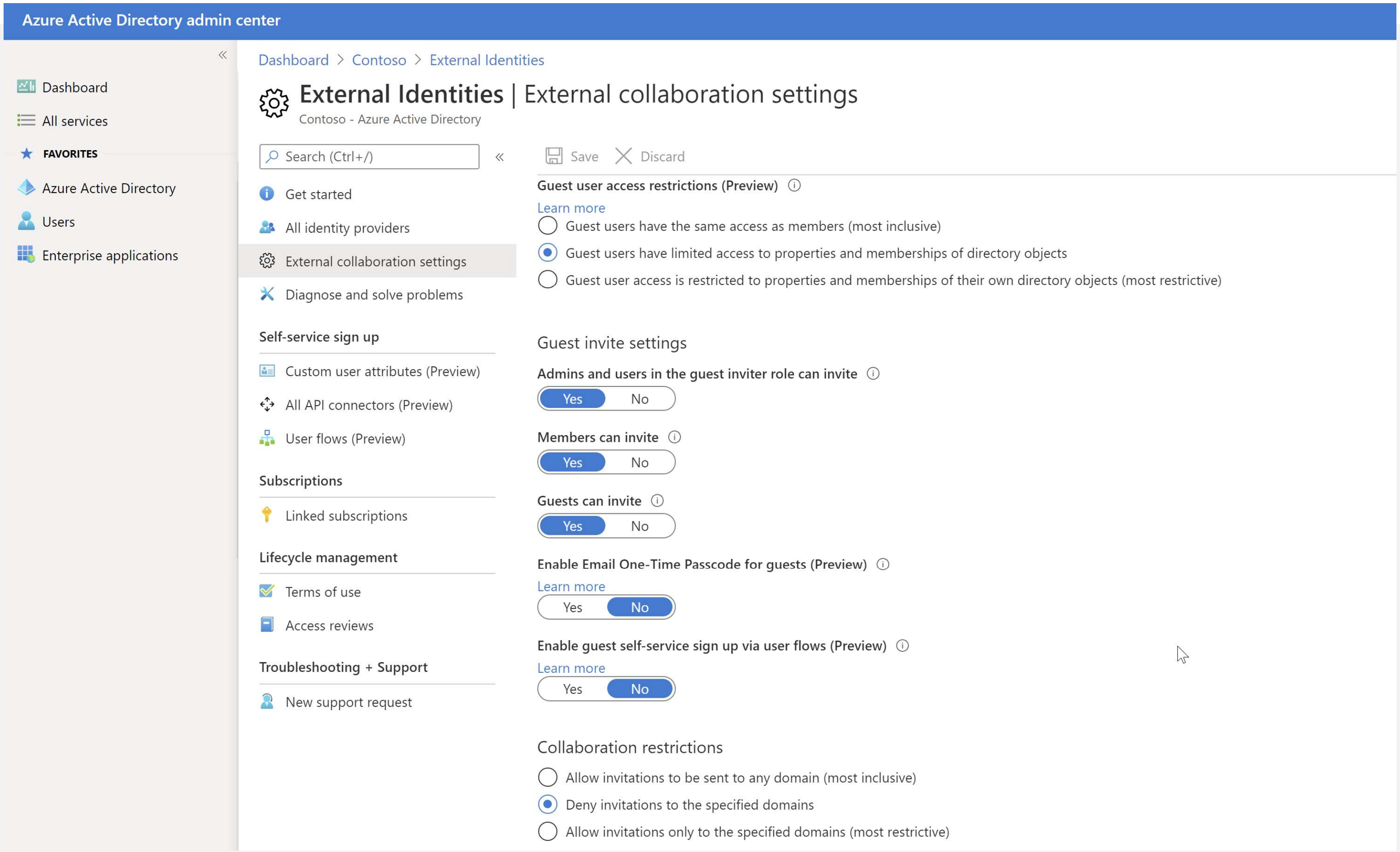
The Azure B2B Guest Model



Benefits of the AAD B2B approach?

- Home domain authenticates user
- Guest domain can leverage AAD conditional access policies
- Centralized identity in guest means centralized reporting or memberships

Configuring B2B settings in AAD…



External Identities | External collaboration settings

Contoso - Azure Active Directory

Guest user access restrictions (Preview)

Learn more

○ Guest users have the same access as members (most inclusive)

● Guest users have limited access to properties and memberships of directory objects

○ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Admins and users in the guest inviter role can invite

[✓ Yes] No

Members can invite

[✓ Yes] No

Guests can invite

[✓ Yes] No

Enable Email One-Time Passcode for guests (Preview)

Learn more

Yes [✓ No]

Enable guest self-service sign up via user flows (Preview)

Learn more

Yes [✓ No]

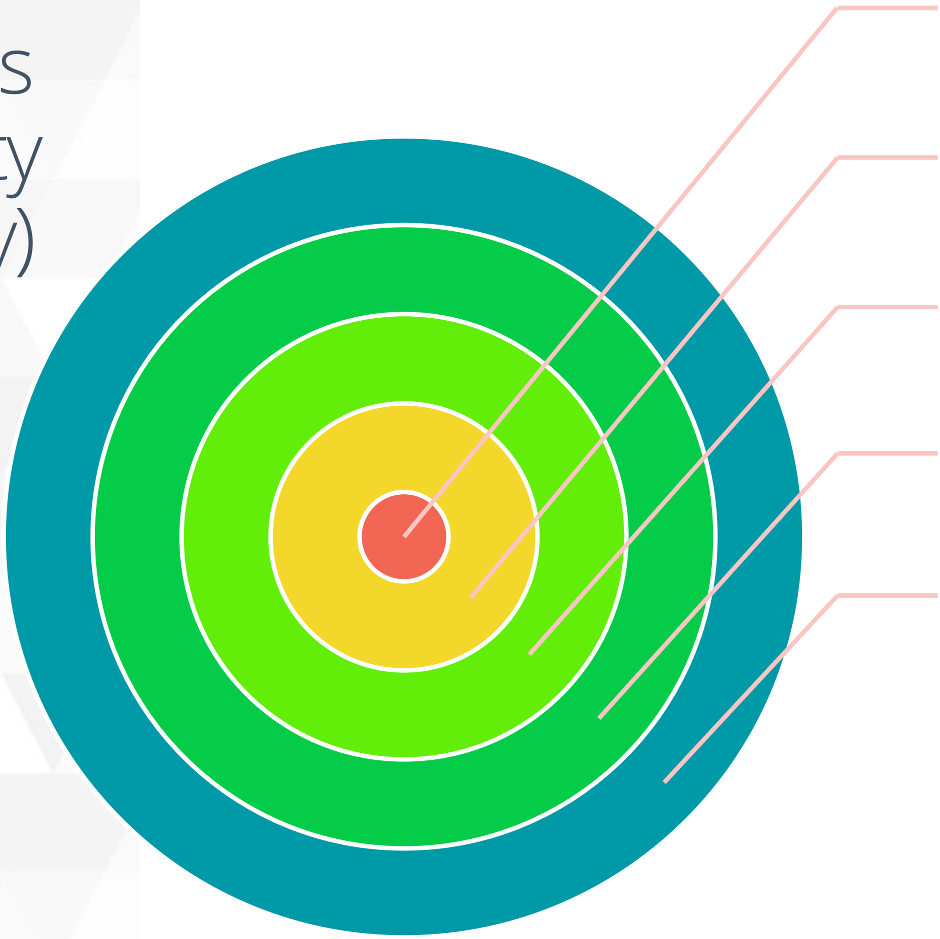
Collaboration restrictions

○ Allow invitations to be sent to any domain (most inclusive)

● Deny invitations to the specified domains

○ Allow invitations only to the specified domains (most restrictive)

Layered settings provide flexibility (and complexity)



AAD Settings

- *Lots of options*

O365 Security and Privacy Setting

- *On/Off*

Group Settings

- *2 Options*

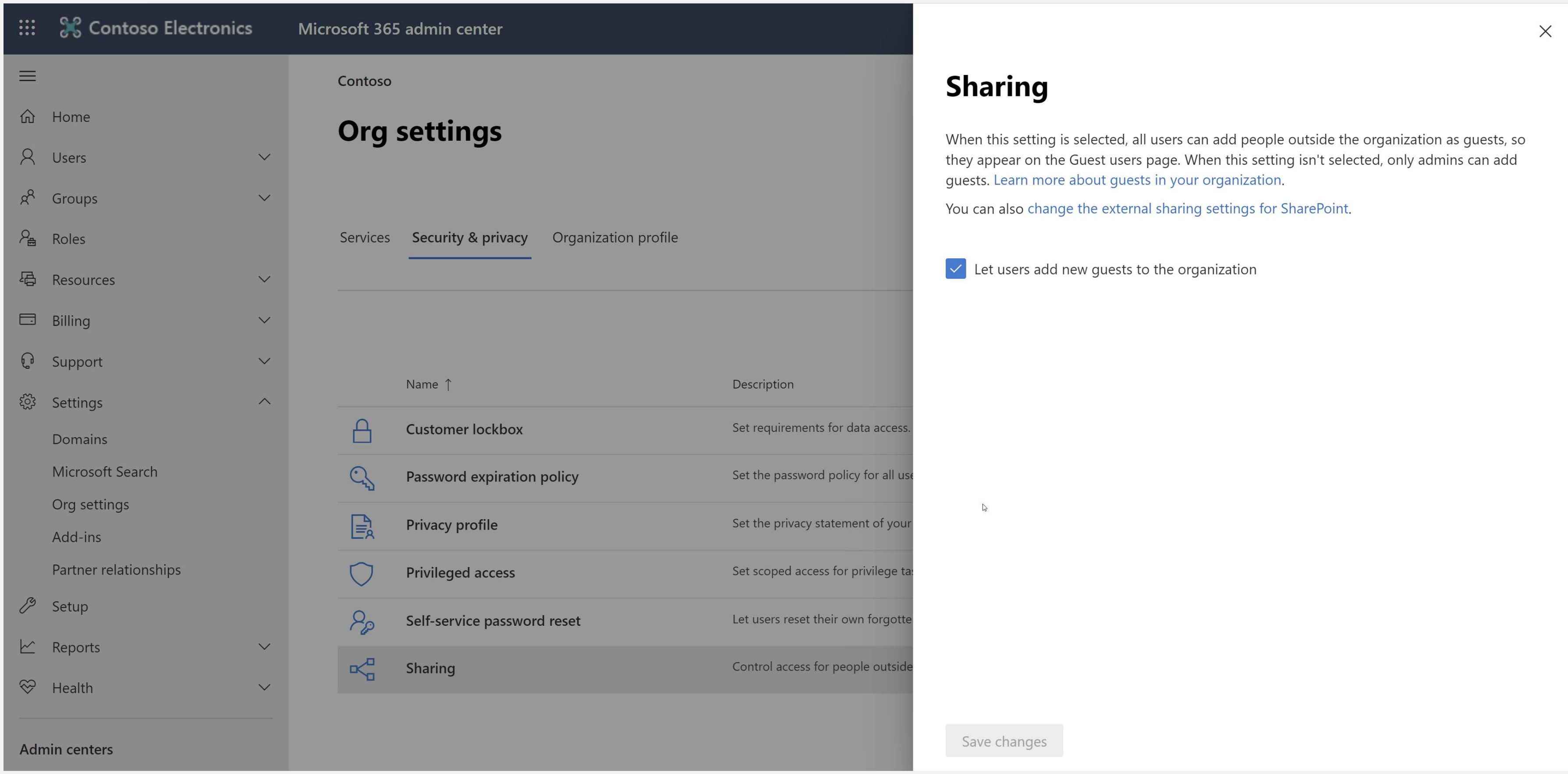
SharePoint setting

Teams Settings

- *Many options*

https://docs.microsoft.com/en-us/microsoftteams/guest-access-checklist

O365 *Tenant wide:* Owners can invite *new* guests?



Name ↑	Description
Customer lockbox	Set requirements for data access.
Password expiration policy	Set the password policy for all use
Privacy profile	Set the privacy statement of your
Privileged access	Set scoped access for privilege ta
Self-service password reset	Let users reset their own forgotte
Sharing	Control access for people outside

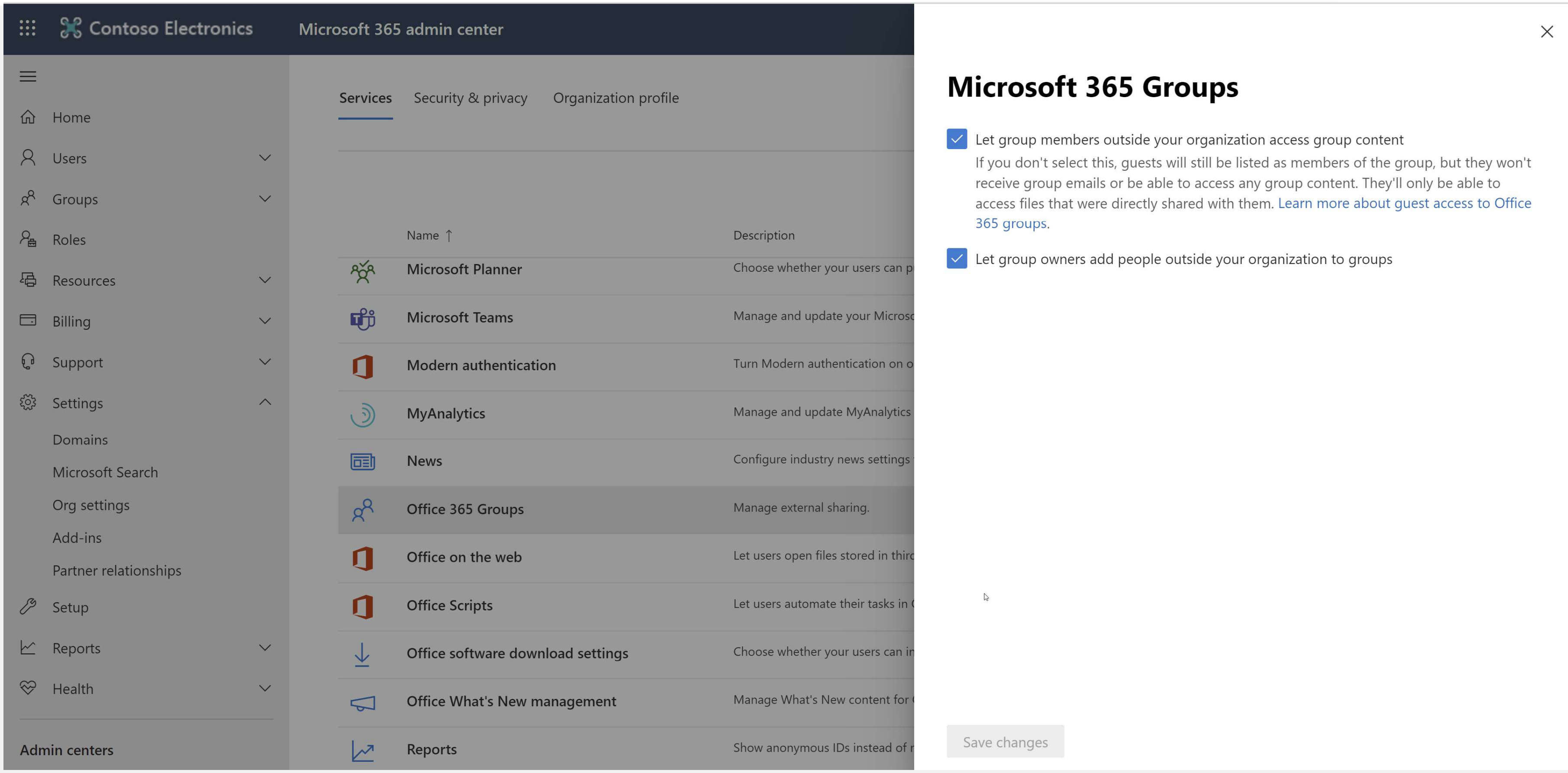
Sharing

When this setting is selected, all users can add people outside the organization as guests, so they appear on the Guest users page. When this setting isn't selected, only admins can add guests. Learn more about guests in your organization.

You can also change the external sharing settings for SharePoint.

☑ Let users add new guests to the organization

O365 *Groups*: Owners can *add* guests?



Name ↑	Description
Microsoft Planner	Choose whether your users can p
Microsoft Teams	Manage and update your Microso
Modern authentication	Turn Modern authentication on o
MyAnalytics	Manage and update MyAnalytics
News	Configure industry news settings
Office 365 Groups	Manage external sharing.
Office on the web	Let users open files stored in thirc
Office Scripts	Let users automate their tasks in (
Office software download settings	Choose whether your users can ir
Office What's New management	Manage What's New content for (
Reports	Show anonymous IDs instead of r

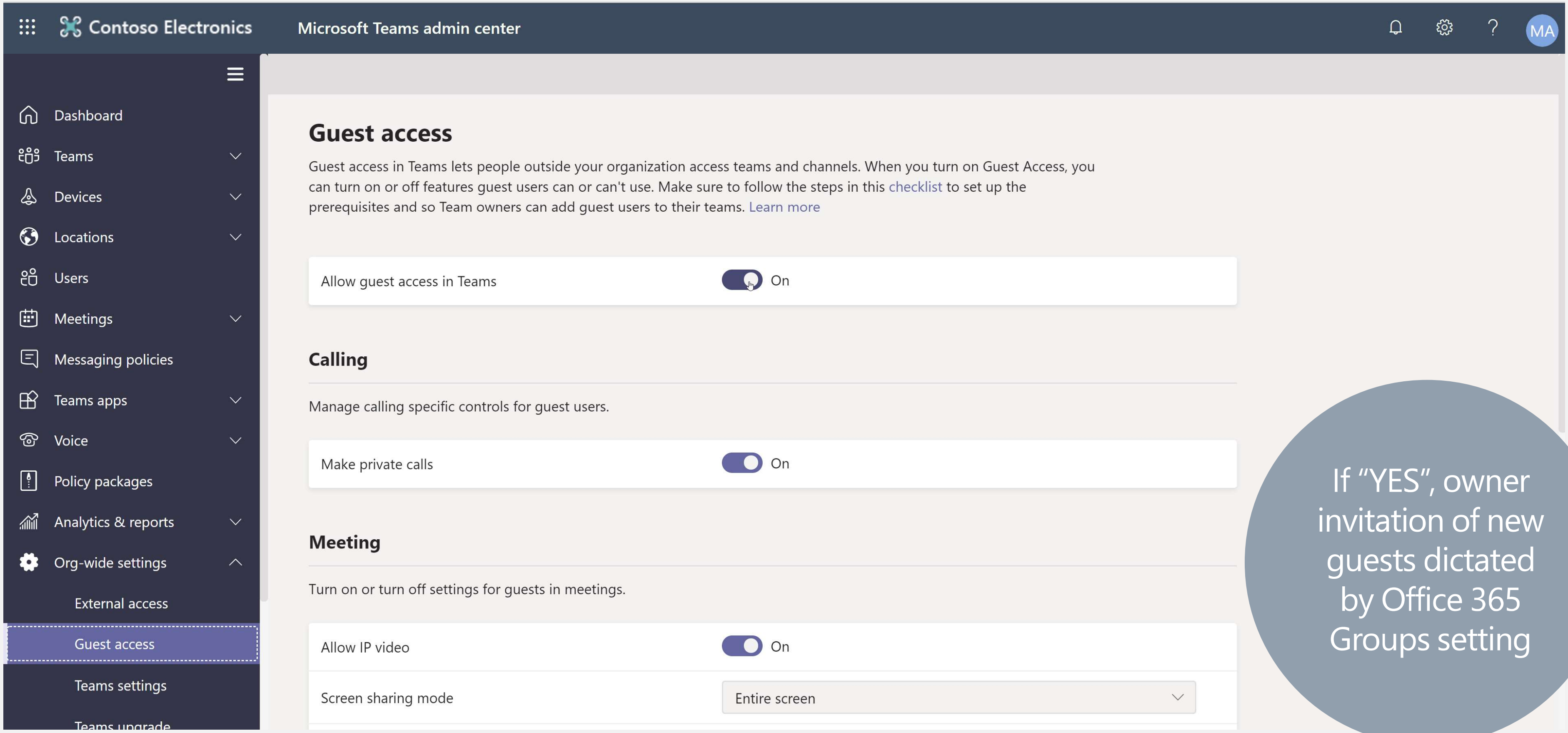
Microsoft 365 Groups

☑ Let group members outside your organization access group content

If you don't select this, guests will still be listed as members of the group, but they won't receive group emails or be able to access any group content. They'll only be able to access files that were directly shared with them. Learn more about guest access to Office 365 groups.

☑ Let group owners add people outside your organization to groups

Microsoft Teams: Are *guests* allowed in Teams?



Guest access

Guest access in Teams lets people outside your organization access teams and channels. When you turn on Guest Access, you can turn on or off features guest users can or can't use. Make sure to follow the steps in this checklist to set up the prerequisites and so Team owners can add guest users to their teams. Learn more

Allow guest access in Teams: On

Calling

Manage calling specific controls for guest users.

Make private calls: On

Meeting

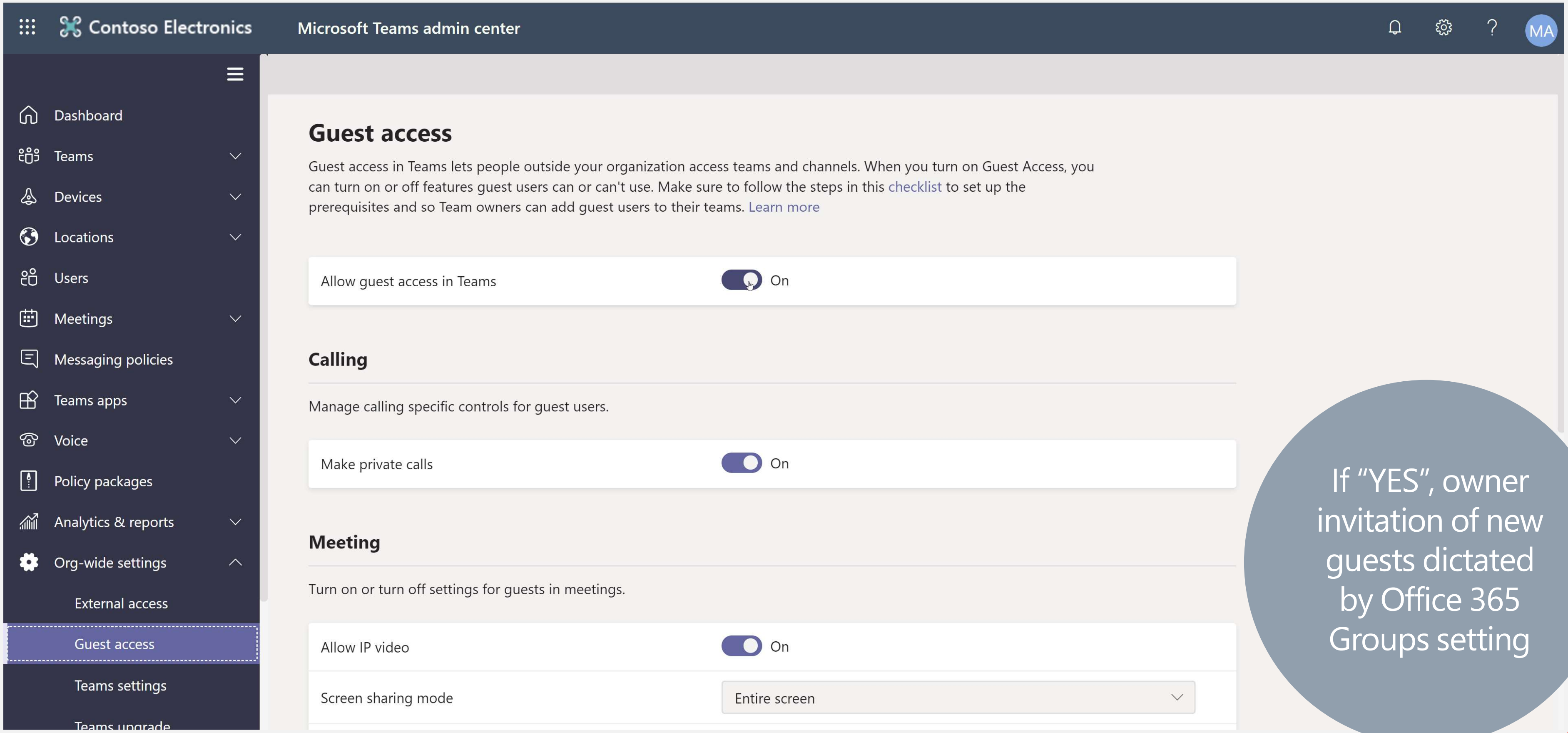
Turn on or turn off settings for guests in meetings.

Allow IP video: On

Screen sharing mode: Entire screen

If "YES", owner invitation of new guests dictated by Office 365 Groups setting

Microsoft Teams: Are *guests* allowed in Teams?



Guest access

Guest access in Teams lets people outside your organization access teams and channels. When you turn on Guest Access, you can turn on or off features guest users can or can't use. Make sure to follow the steps in this checklist to set up the prerequisites and so Team owners can add guest users to their teams. Learn more

Allow guest access in Teams: On

Calling

Manage calling specific controls for guest users.

Make private calls: On

Meeting

Turn on or turn off settings for guests in meetings.

Allow IP video: On

Screen sharing mode: Entire screen

If "YES", owner invitation of new guests dictated by Office 365 Groups setting

Going Further – Microsoft *Information Barriers*

Leveraging our *AAD properties* and segments to create hard divisions that block sharing and communications *within a tenant*.

This group…	…can't talk to this group…	…because…
Investment Banking	Research	FINRA Regulations
Lawyer for Client A	Lawyer for Client B	Conflict of interest within a firm
Professional Services	Off-shore Development	Government contracts
US Weapons Developers	Overseas Subsidiaries	ITAR Compliance

Jefferies

Customer:
Jefferies

Industry:
Banking & Capital Markets

Size:
3,900 employees

Country:
United States

Products and services:
Microsoft 365
Microsoft Teams
Microsoft OneDrive

Microsoft SharePoint
Microsoft 365 Information Barriers
Microsoft 365 Multi-Geo

Microsoft Information Protection

Microsoft Defender Antivirus

Read full story here

Microsoft

> “We were pleased that the information barriers feature was already ‘baked in’ to Microsoft 365. By implementing information barriers we were able to successfully deploy Teams, OneDrive, and SharePoint Online.”
>
> —Jitesh Mandalia, Senior Vice President, Jefferies

Situation:

The global, independent investment banking, capital markets and alternative asset management firm Jefferies wanted its employees to collaborate using Microsoft Teams, OneDrive, and SharePoint. It needed to be sure it complied with banking and investment regulations.

Solution:

The company adopted information barriers, which is included in its Microsoft 365 E5 license, and was able to establish barriers between its investment banking and research divisions. Users across those divisions cannot digitally see or contact each other.

Impact:

In deploying information barriers, Jefferies could quickly get employees collaborating using Teams, OneDrive, and SharePoint. Even while transitioning to the cloud-based platform while 98 percent of the company worked remotely, it had a successful quarter.

Going Further – Microsoft *Information Barriers*

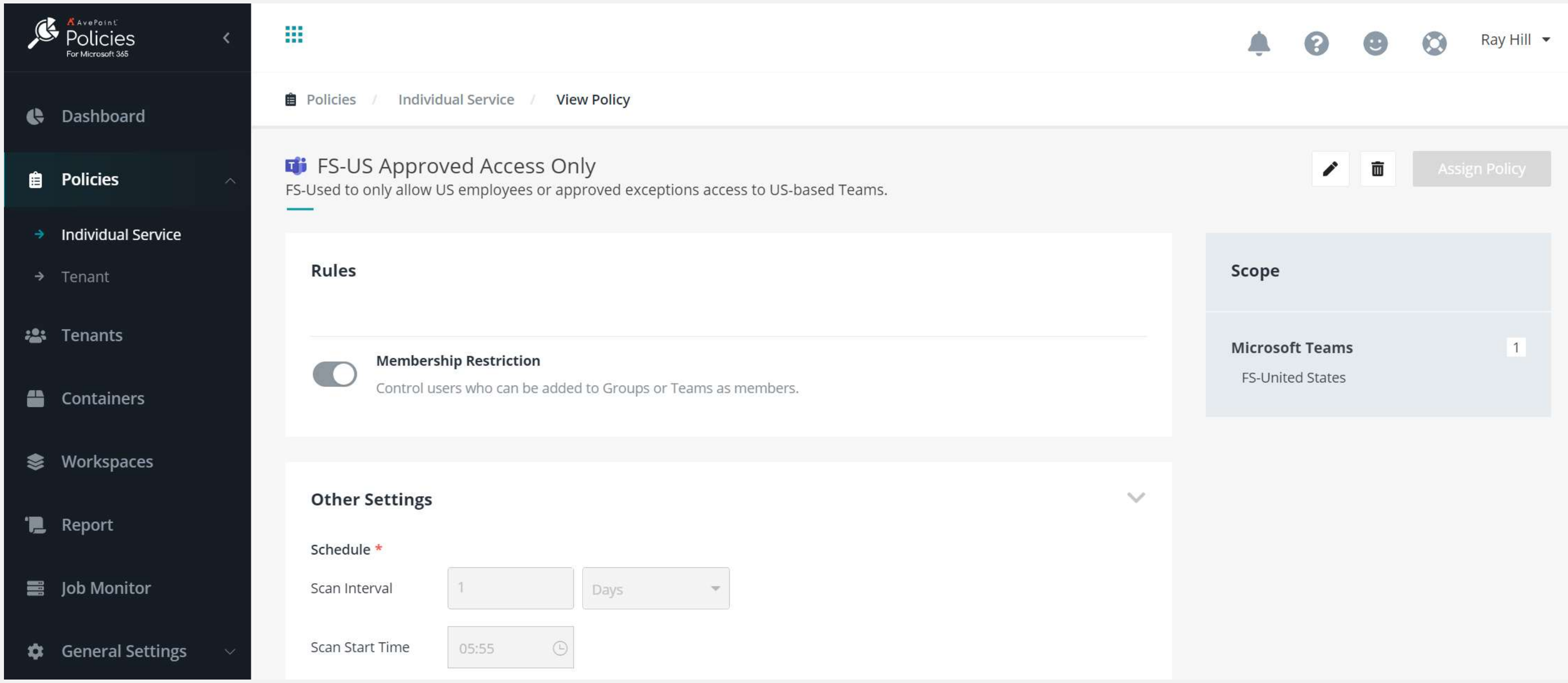
Leveraging our *AAD properties* and segments to create hard divisions that block sharing and communications *within a tenant*.

This group…	…can't talk to this group…	…because…
Investment Banking	Research	FINRA Regulations
Lawyer for Client A	Lawyer for Client B	Conflict of interest within a firm
Professional Services	Off-shore Development	Government contracts
US Weapons Developers	Overseas Subsidiaries	ITAR Compliance

But… what if this isn't *always* true in a shared tenant?

Right-sizing Governance – *AvePoint Policies*

For the *sometimes* scenarios – let’s combine the AAD classifications with our Teams and Groups Memberships!



FS-US Approved Access Only

FS-Used to only allow US employees or approved exceptions access to US-based Teams.

Rules

Membership Restriction

Control users who can be added to Groups or Teams as members.

Scope

Microsoft Teams 1

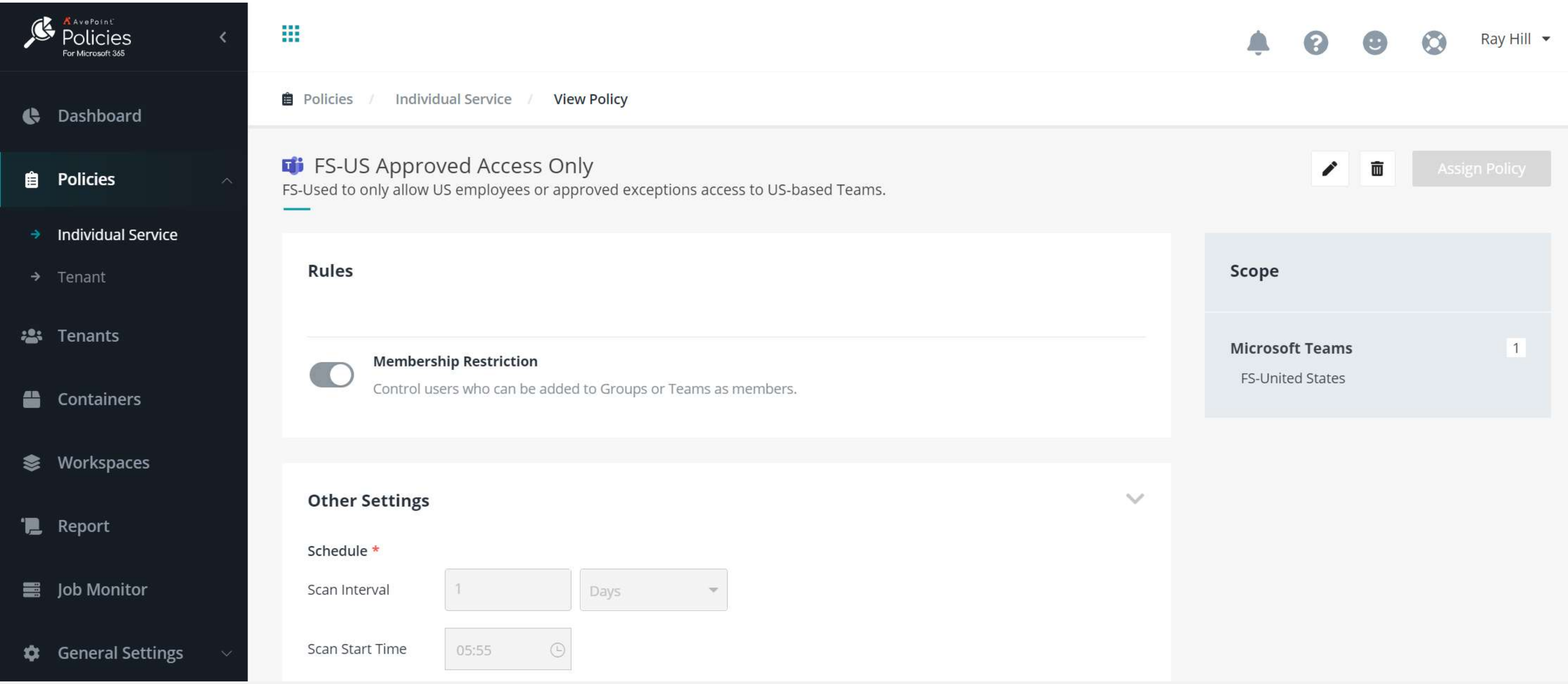
FS-United States

Other Settings

Schedule *

Scan Interval: 1 Days

Scan Start Time: 05:55



FS-US Approved Access Only

FS-Used to only allow US employees or approved exceptions access to US-based Teams.

Rules

Membership Restriction

Control users who can be added to Groups or Teams as members.

Scope

Microsoft Teams 1

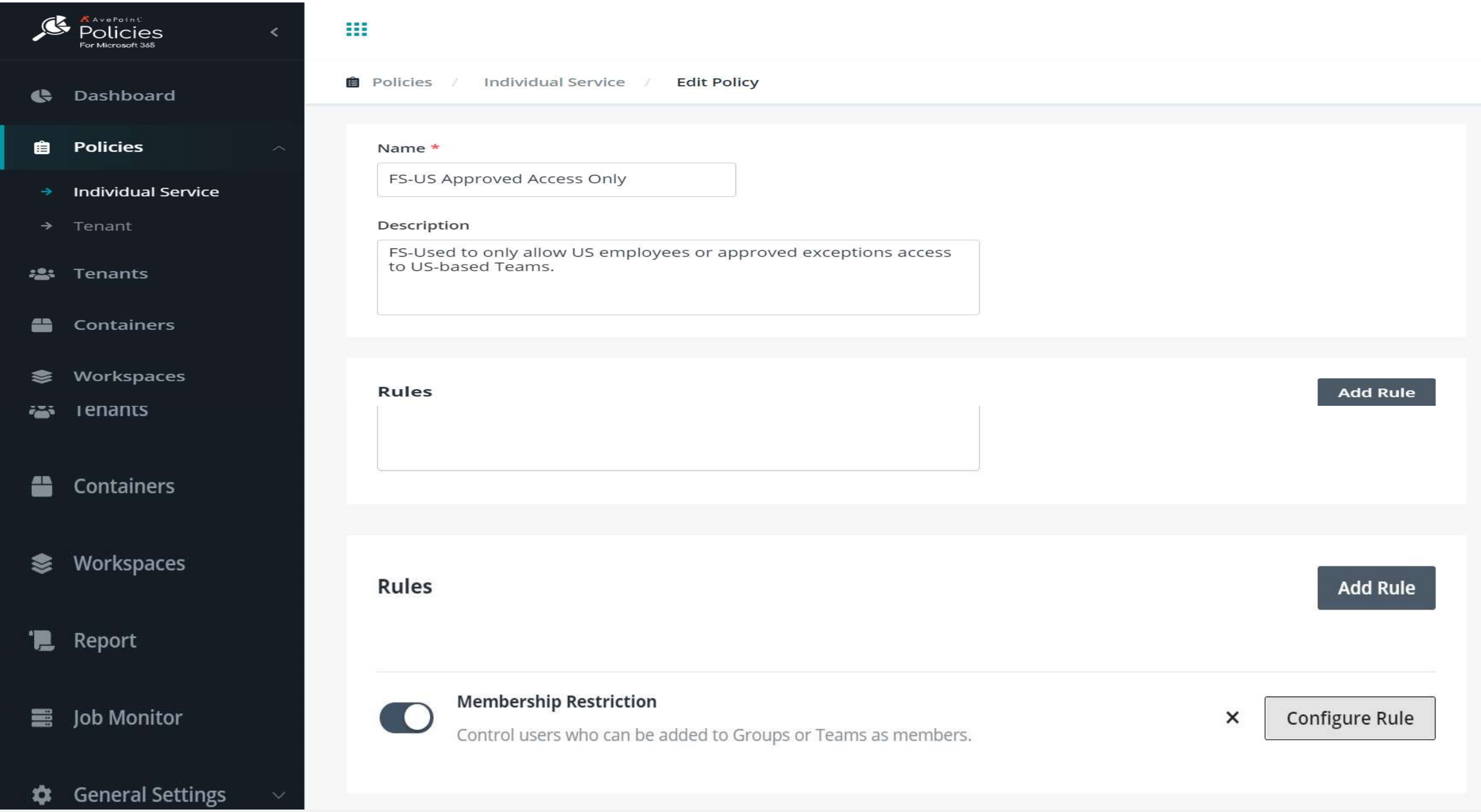
FS-United States

Other Settings

Schedule *

Scan Interval: 1 Days

Scan Start Time: 05:55



Name *

FS-US Approved Access Only

Description

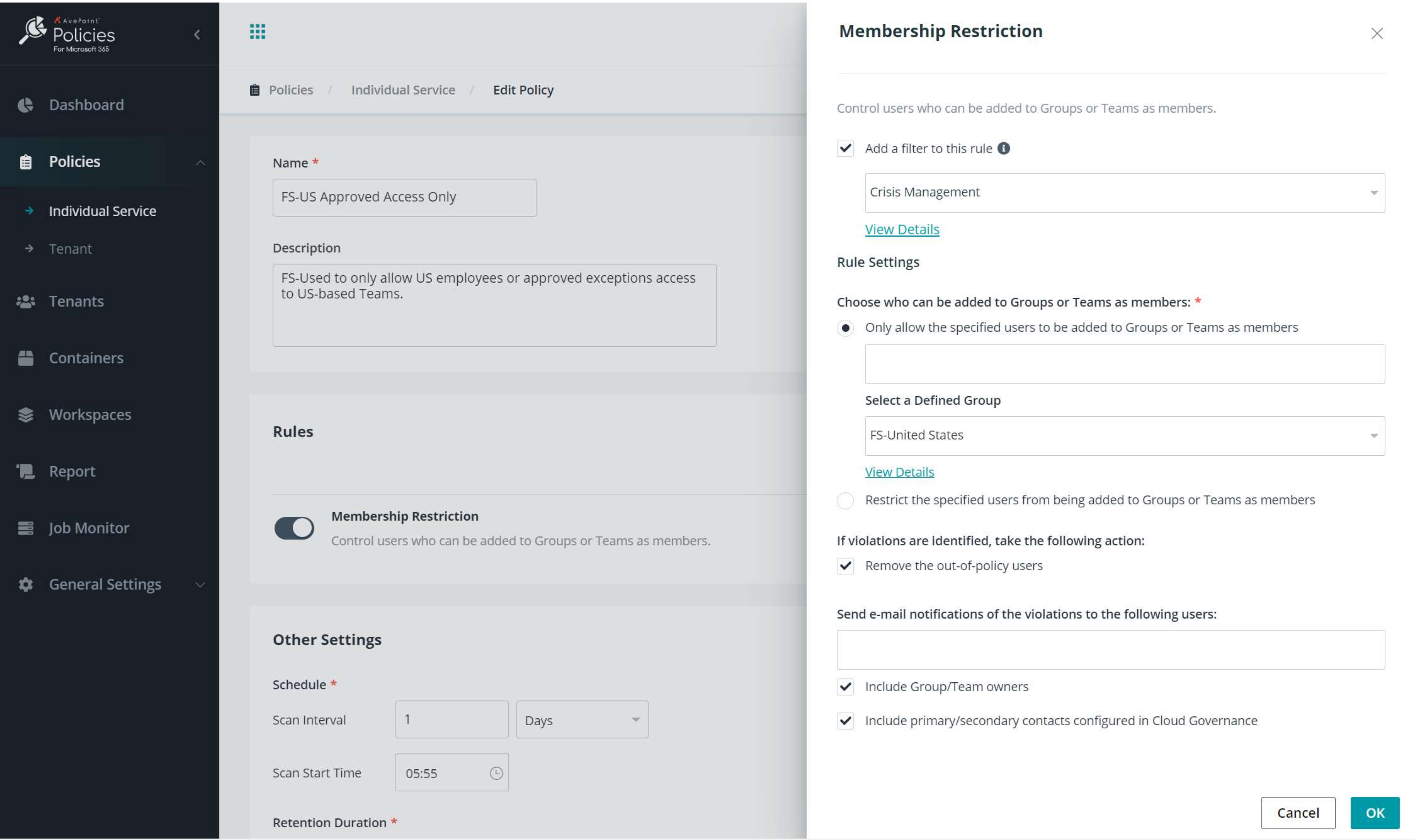
FS-Used to only allow US employees or approved exceptions access to US-based Teams.

Rules

Rules

Membership Restriction

Control users who can be added to Groups or Teams as members.



Name *

FS-US Approved Access Only

Description

FS-Used to only allow US employees or approved exceptions access to US-based Teams.

Rules

Membership Restriction
Control users who can be added to Groups or Teams as members.

Other Settings

Schedule *

Scan Interval: 1 Days

Scan Start Time: 05:55

Retention Duration *

Membership Restriction

Control users who can be added to Groups or Teams as members.

☑ Add a filter to this rule

Crisis Management

View Details

Rule Settings

Choose who can be added to Groups or Teams as members: *

● Only allow the specified users to be added to Groups or Teams as members

Select a Defined Group

FS-United States

View Details

○ Restrict the specified users from being added to Groups or Teams as members

If violations are identified, take the following action:

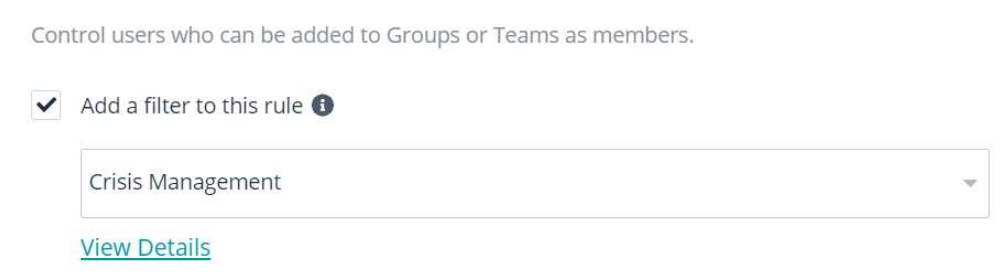
☑ Remove the out-of-policy users

Send e-mail notifications of the violations to the following users:

☑ Include Group/Team owners

☑ Include primary/secondary contacts configured in Cloud Governance

Right-Sizing Governance Controls

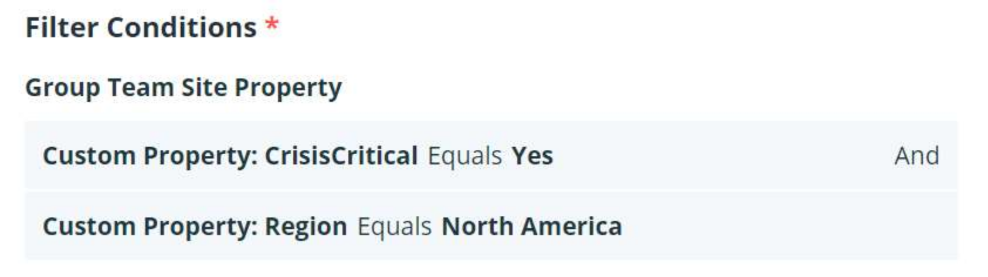


Control users who can be added to Groups or Teams as members.

☑ Add a filter to this rule

Crisis Management

View Details

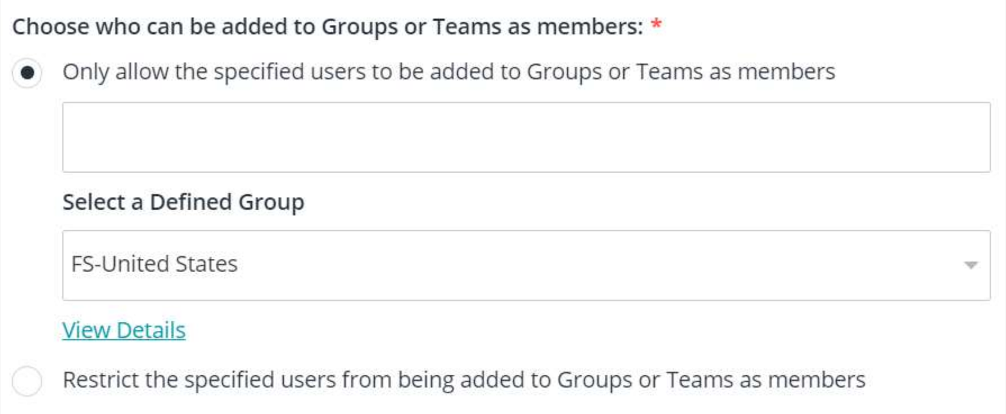


Filter Conditions *

Group Team Site Property

Custom Property: CrisisCritical Equals **Yes** And

Custom Property: Region Equals **North America**



Choose who can be added to Groups or Teams as members: *

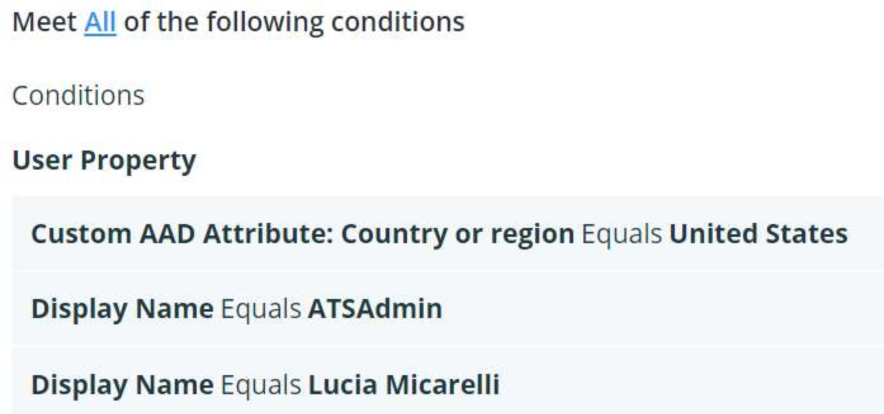
● Only allow the specified users to be added to Groups or Teams as members

Select a Defined Group

FS-United States

View Details

○ Restrict the specified users from being added to Groups or Teams as members



Meet All of the following conditions

Conditions

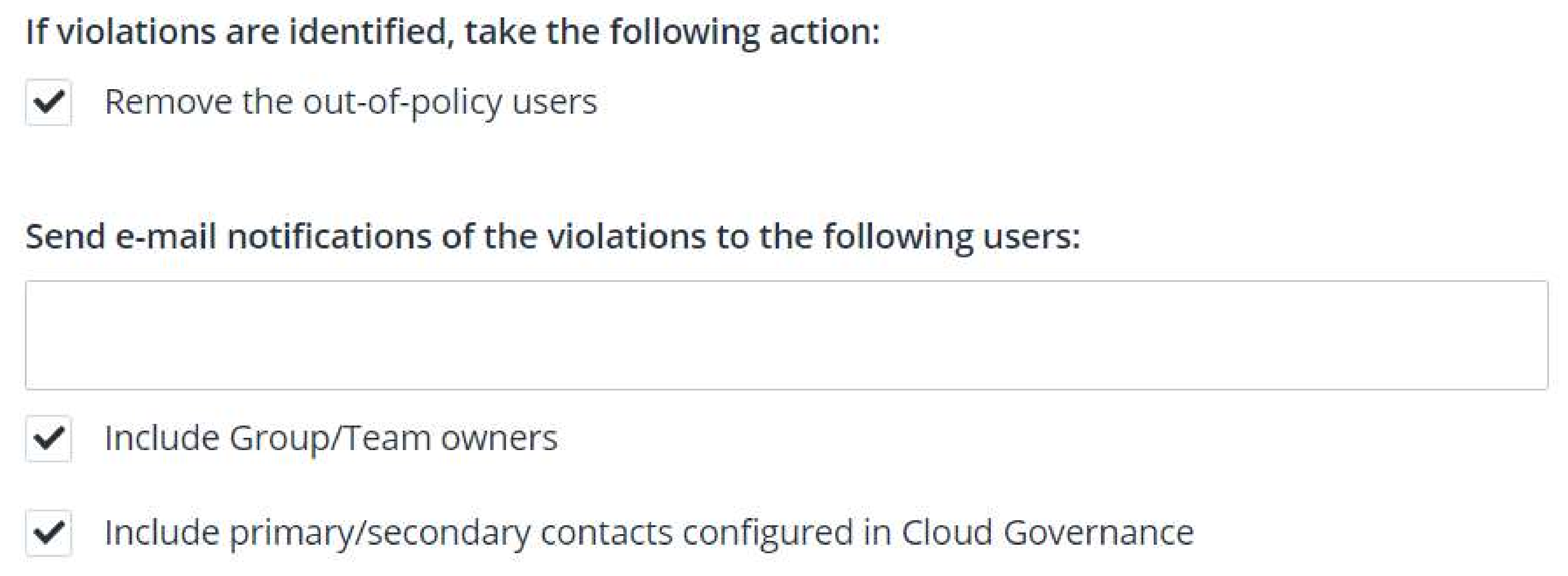
User Property

Custom AAD Attribute: Country or region Equals **United States**

Display Name Equals **ATSAdmin**

Display Name Equals **Lucia Micarelli**

Right-Sizing Governance Controls



If violations are identified, take the following action:

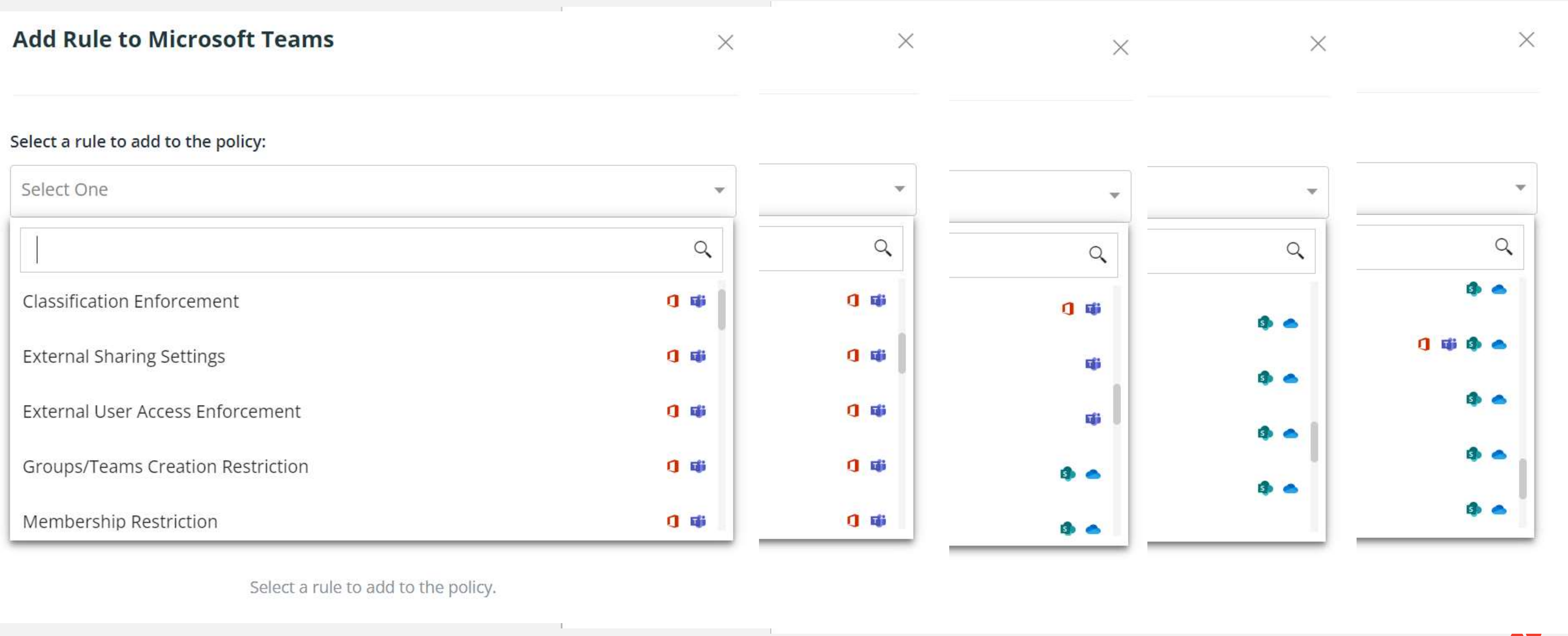
☑ Remove the out-of-policy users

Send e-mail notifications of the violations to the following users:

☑ Include Group/Team owners

☑ Include primary/secondary contacts configured in Cloud Governance

Building Blocks for Microsoft Policies



Add Rule to Microsoft Teams

Select a rule to add to the policy:

Select One

Classification Enforcement

External Sharing Settings

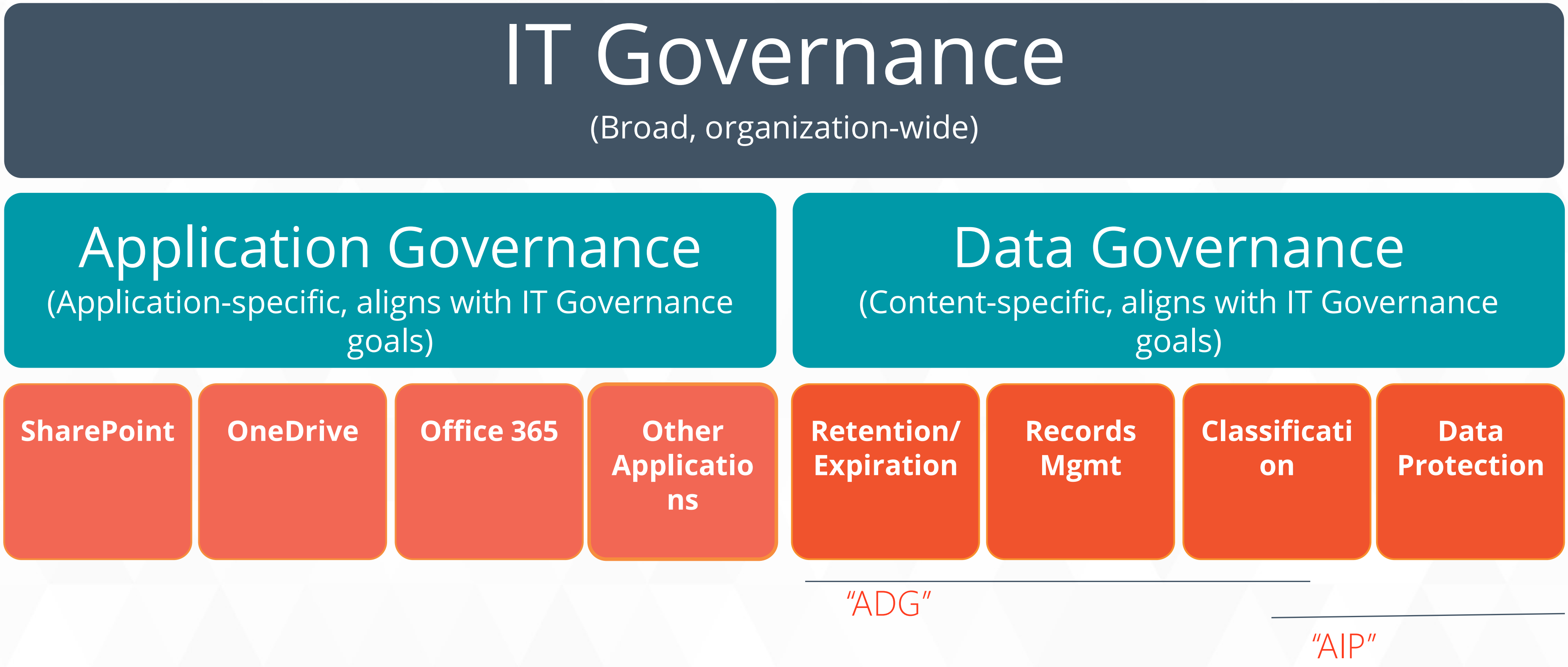
External User Access Enforcement

Groups/Teams Creation Restriction

Membership Restriction

Select a rule to add to the policy.

Where does this conversation fit in…



IT Governance

(Broad, organization-wide)

Application Governance

(Application-specific, aligns with IT Governance goals)

- **SharePoint**
- **OneDrive**
- **Office 365**
- **Other Applications**

Data Governance

(Content-specific, aligns with IT Governance goals)

- **Retention/ Expiration**
- **Records Mgmt**
- **Classification**
- **Data Protection**

"ADG"

"AIP"

Out-of-box sensitive info types

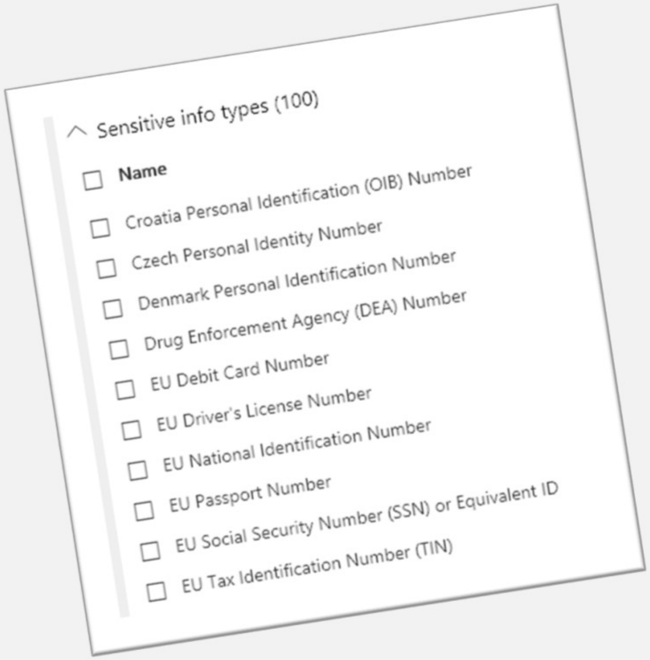
Core activity

Microsoft 365 includes hundreds of sensitive info types
For different countries, industries or by information type

Sensitive information comes in many forms
Financial data, Personally Identifiable Information (PII)

Examples

- Croatia Personal Identification (OIB) Number
- EU Debit Card Number
- EU Passport Number
- US Drivers License Number
- Social Security Number



Sensitive info types (100)

☐ **Name**
☐ Croatia Personal Identification (OIB) Number
☐ Czech Personal Identity Number
☐ Denmark Personal Identification Number
☐ Drug Enforcement Agency (DEA) Number
☐ EU Debit Card Number
☐ EU Driver's License Number
☐ EU National Identification Number
☐ EU Passport Number
☐ EU Social Security Number (SSN) or Equivalent ID
☐ EU Tax Identification Number (TIN)

Customer specific sensitive info types

Core activity

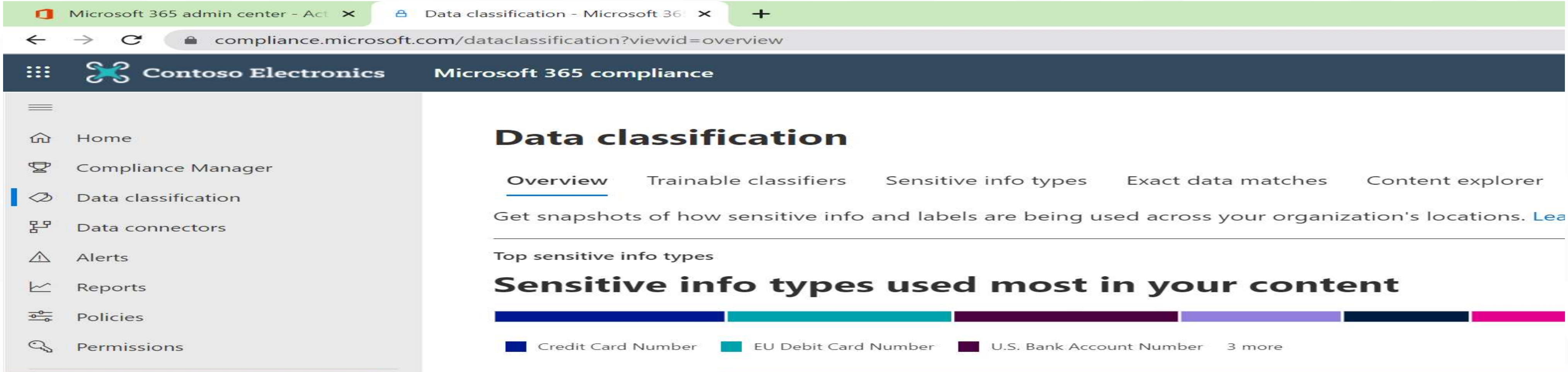
Business intellectual property
Business plans, product designs, confidential projects

Employee or customer information
HR Information, resumés, employment records, salary information

Highly confidential information
Mergers and Acquisition, workforce reduction

Examples

- Employee or customer numbers *Technology: RegEx*
  - <EMP-nnnnn>
  - <CUST-nnnnnn-NL>
- Specific keywords *Technology: Static Keywords*
  - <Project Enigma>
  - <Highly Confidential>
  - <Internal only>

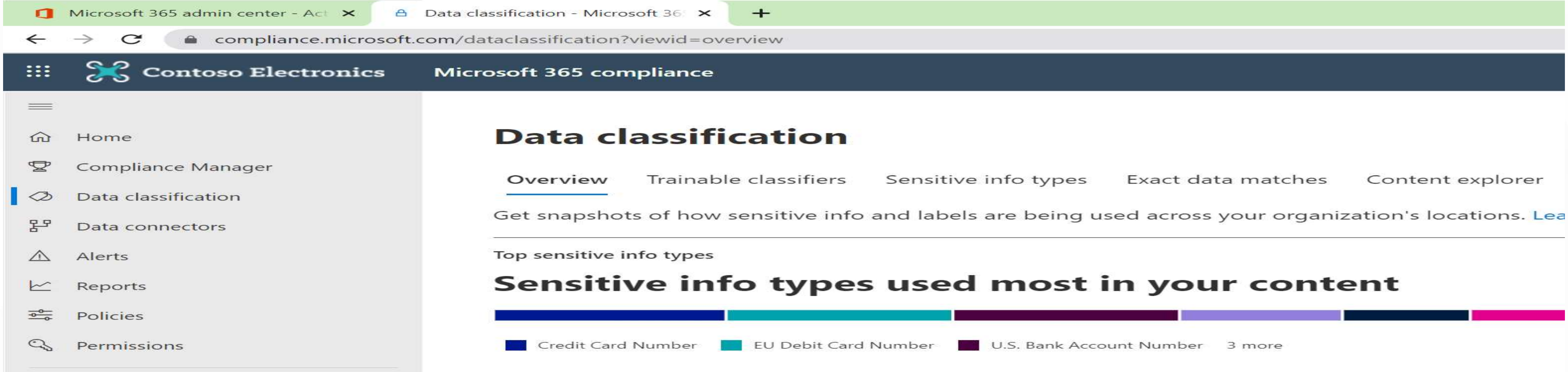


Data classification

Get snapshots of how sensitive info and labels are being used across your organization's locations. Lea

Top sensitive info types

Sensitive info types used most in your content


Data classification

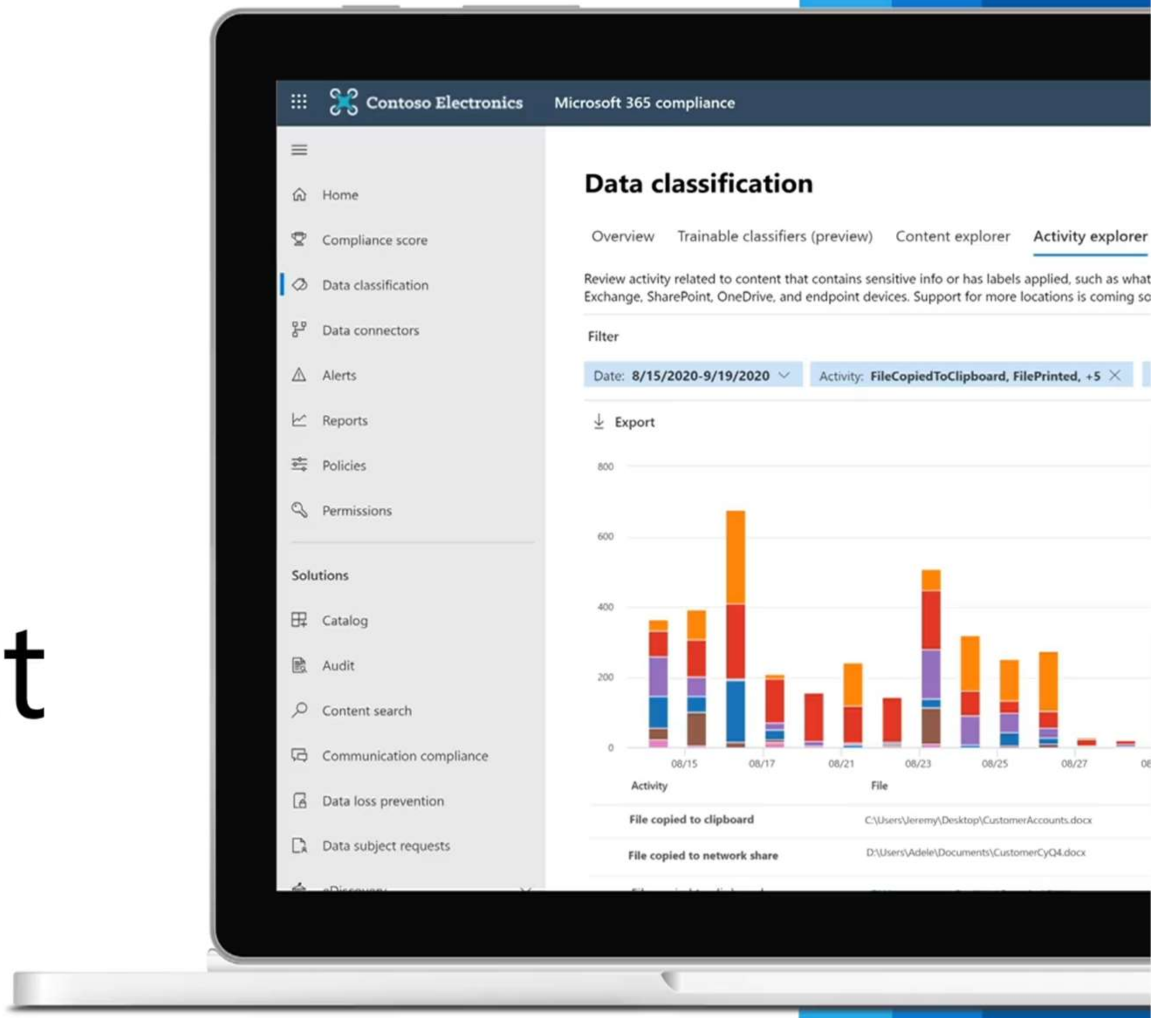
Get snapshots of how sensitive info and labels are being used across your organization's locations. Lea

Top sensitive info types

Sensitive info types used most in your content

Microsoft Security

Protecting sensitive information using Endpoint DLP



Review activity related to content that contains sensitive info or has labels applied, such as what
Exchange, SharePoint, OneDrive, and endpoint devices. Support for more locations is coming so

Activity	File
File copied to clipboard	C:\Users\Jeremy\Desktop\CustomerAccounts.docx
File copied to network share	D:\Users\Adele\Documents\CustomerCyQ4.docx

Microsoft's information protection solutions help you protect sensitive data throughout the lifecycle – inside and outside the organization

Microsoft Information Protection

Protect your sensitive data – wherever it lives or travels

Discover

Classify

Protect

Monitor

Across

Devices

Apps

Cloud services

On-premises

SENSITIVITY LABELS PERSIST WITH THE DOCUMENT

Document labeling – what is it?

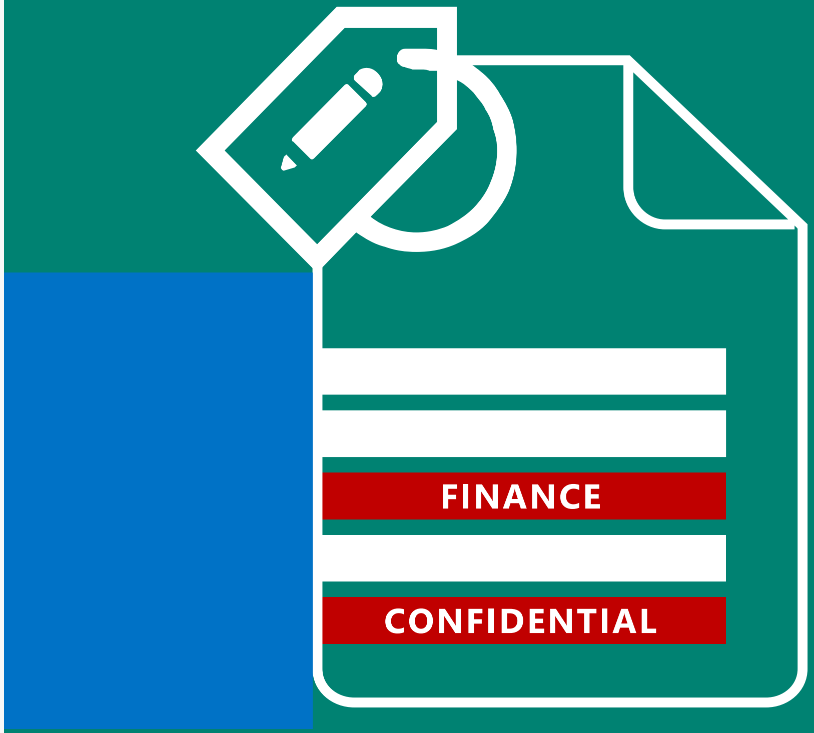
Metadata written into document files

Travels with the document as it moves

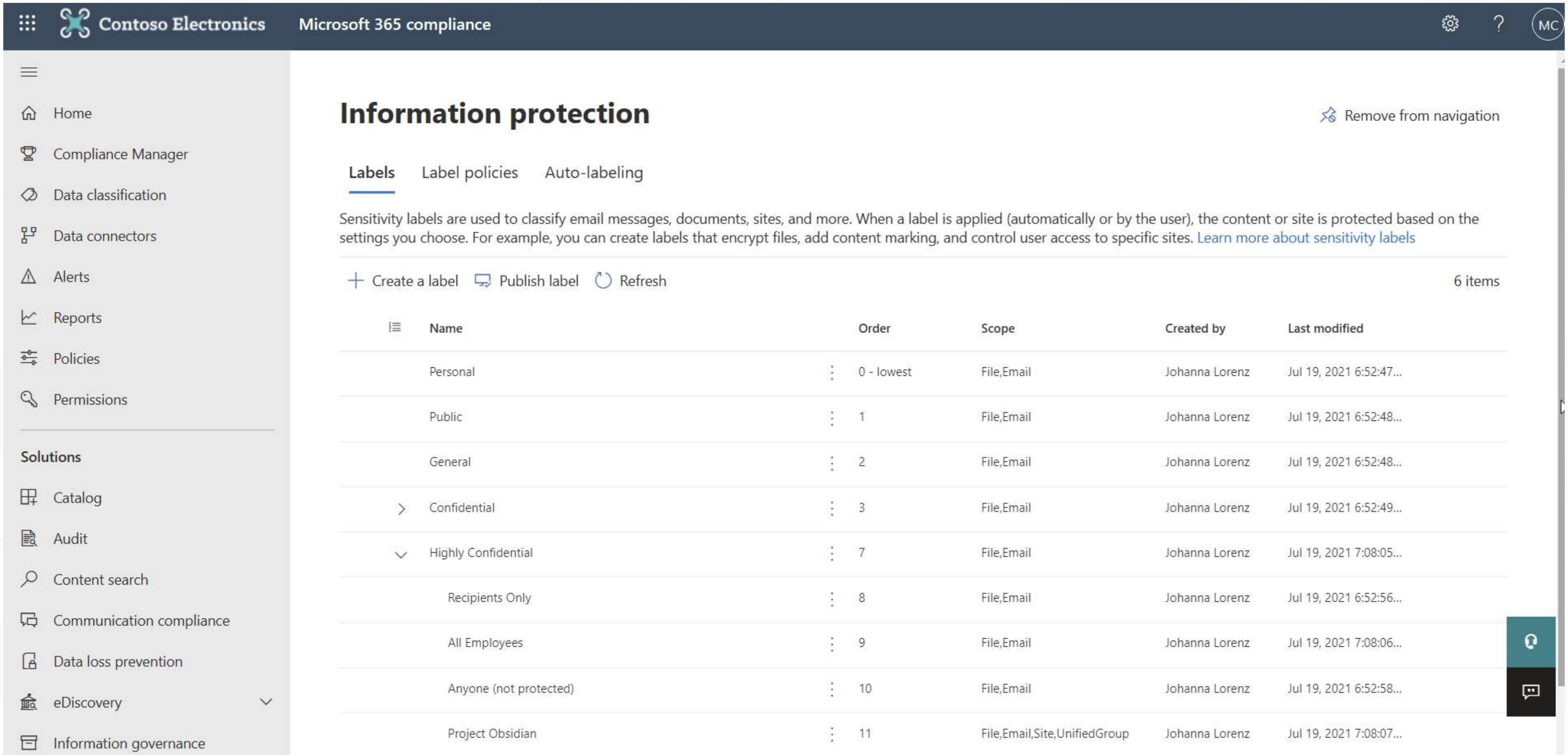
In clear text so that other systems can read it

Can be used to apply a protection action or data governance action

Can be customized per the organization’s needs



Creating “Sensitivity Labels” in the S&C Center

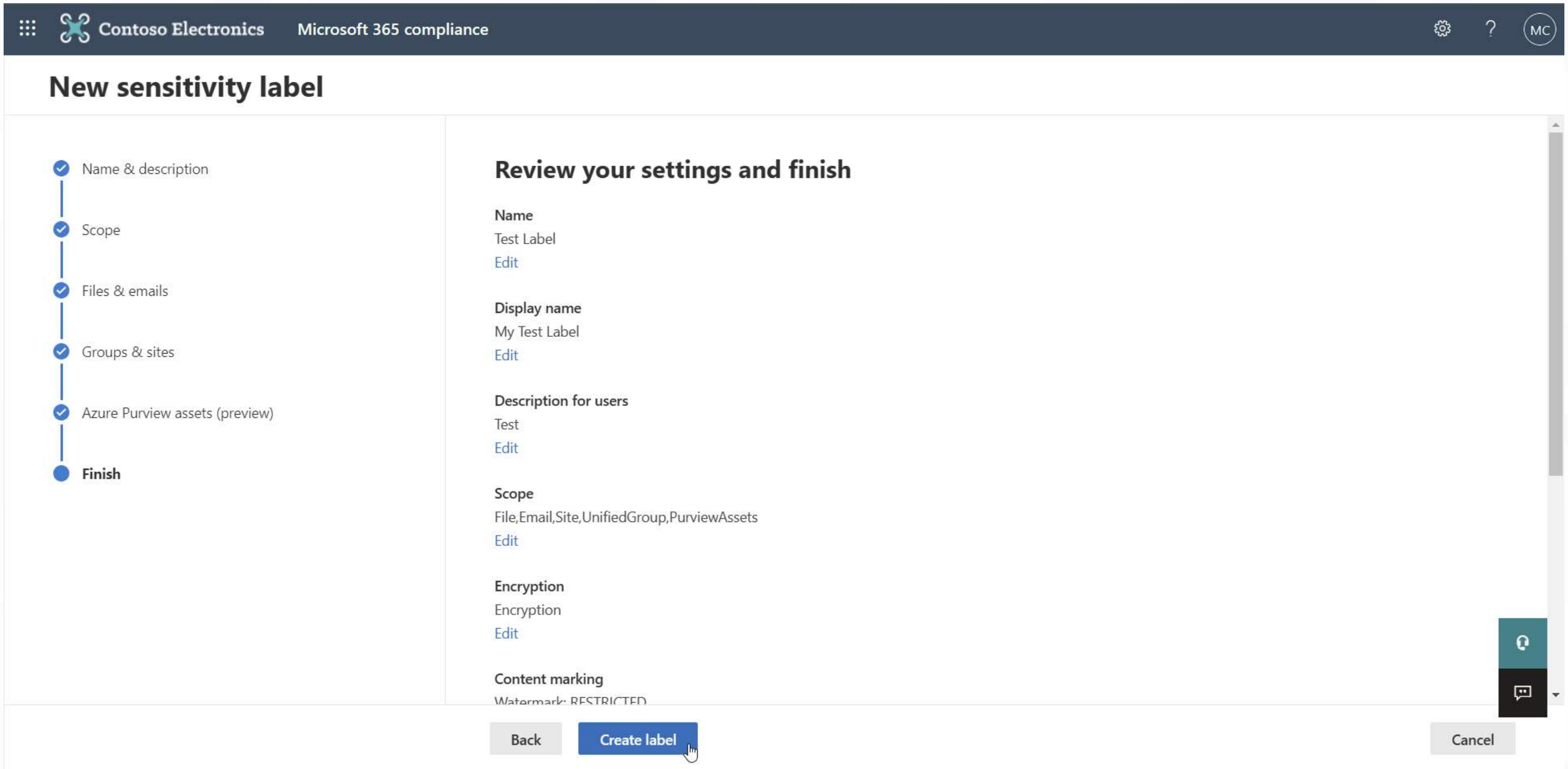


Information protection

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Name	Order	Scope	Created by	Last modified
Personal	0 - lowest	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:47...
Public	1	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:48...
General	2	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:48...
Confidential	3	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:49...
Highly Confidential	7	File,Email	Johanna Lorenz	Jul 19, 2021 7:08:05...
Recipients Only	8	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:56...
All Employees	9	File,Email	Johanna Lorenz	Jul 19, 2021 7:08:06...
Anyone (not protected)	10	File,Email	Johanna Lorenz	Jul 19, 2021 6:52:58...
Project Obsidian	11	File,Email,Site,UnifiedGroup	Johanna Lorenz	Jul 19, 2021 7:08:07...

Building Your Sensitivity Labels



Review your settings and finish

Name
Test Label
Edit

Display name
My Test Label
Edit

Description for users
Test
Edit

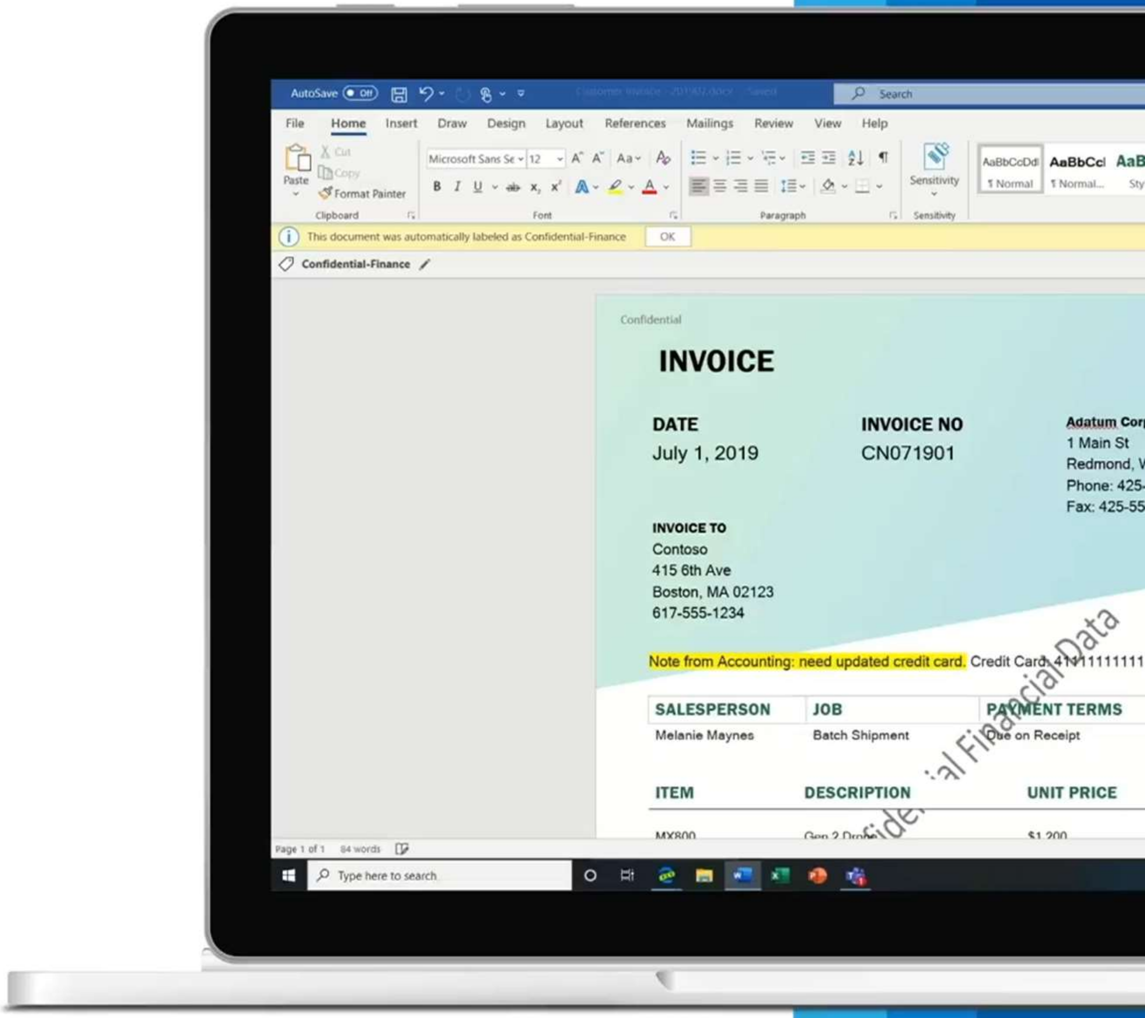
Scope
File,Email,Site,UnifiedGroup,PurviewAssets
Edit

Encryption
Encryption
Edit

Content marking
Watermark: RESTRICTED

Microsoft 365 Security

Automatic document classification



This document was automatically labeled as Confidential-Finance OK

Confidential-Finance

Confidential

INVOICE

DATE
July 1, 2019

INVOICE NO
CN071901

Adatum Cor
1 Main St
Redmond, W
Phone: 425-
Fax: 425-55

INVOICE TO
Contoso
415 6th Ave
Boston, MA 02123
617-555-1234

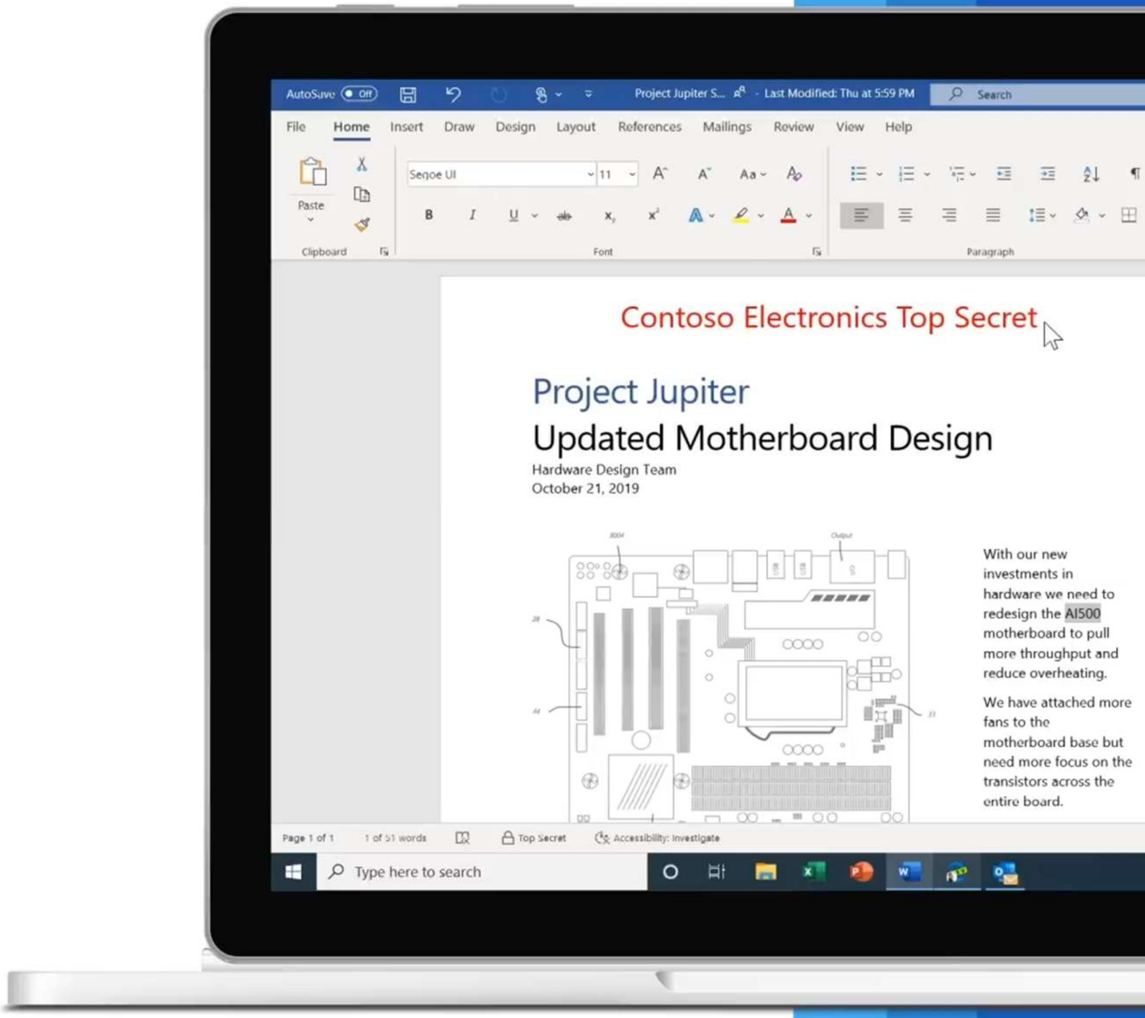
Note from Accounting: need updated credit card. Credit Card: 41111111111

SALESPERSON	JOB	PAYMENT TERMS
Melanie Maynes	Batch Shipment	Due on Receipt

ITEM	DESCRIPTION	UNIT PRICE
MX800	Gen 2 Dro	$1,200

Microsoft 365 Security

Automatic classification of content



Contoso Electronics Top Secret

Project Jupiter

Updated Motherboard Design

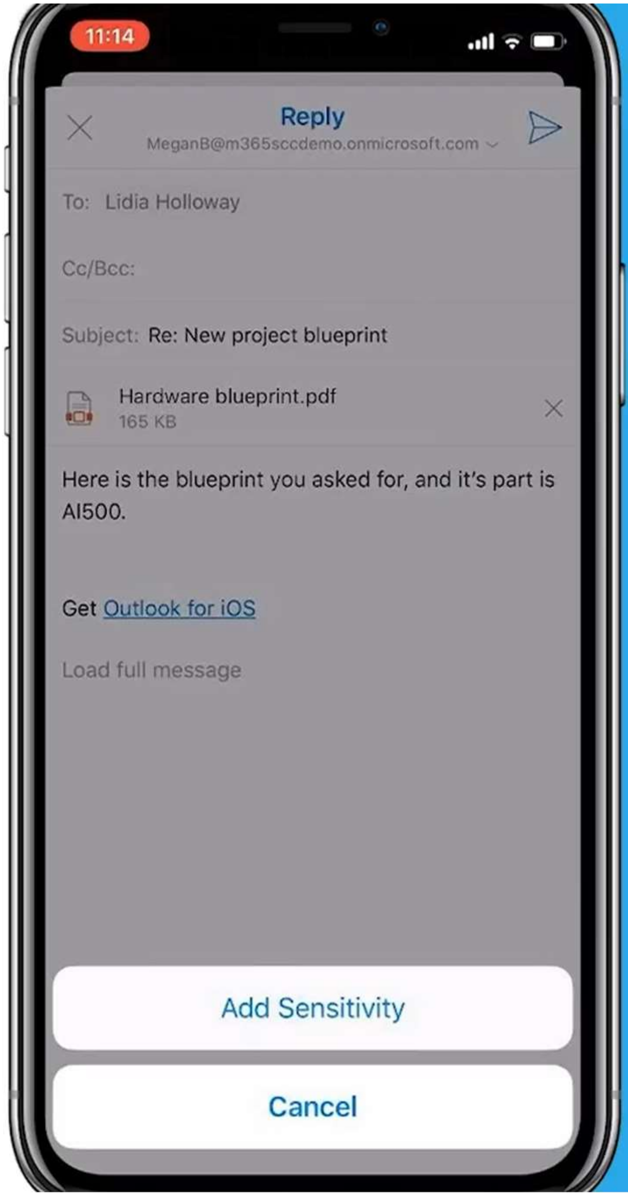
Hardware Design Team
October 21, 2019

With our new investments in hardware we need to redesign the AI500 motherboard to pull more throughput and reduce overheating.

We have attached more fans to the motherboard base but need more focus on the transistors across the entire board.

Microsoft 365 Security

Manually classify content on mobile



MeganB@m365sccdemo.onmicrosoft.com

To: Lidia Holloway

Cc/Bcc:

Subject: Re: New project blueprint

Hardware blueprint.pdf
165 KB

Here is the blueprint you asked for, and it's part is AI500.

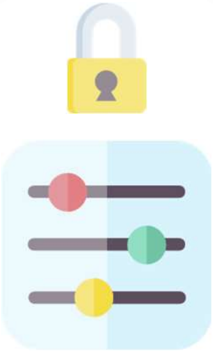
Get Outlook for iOS

Load full message

Sensitive data in a “free and open sharing” system?

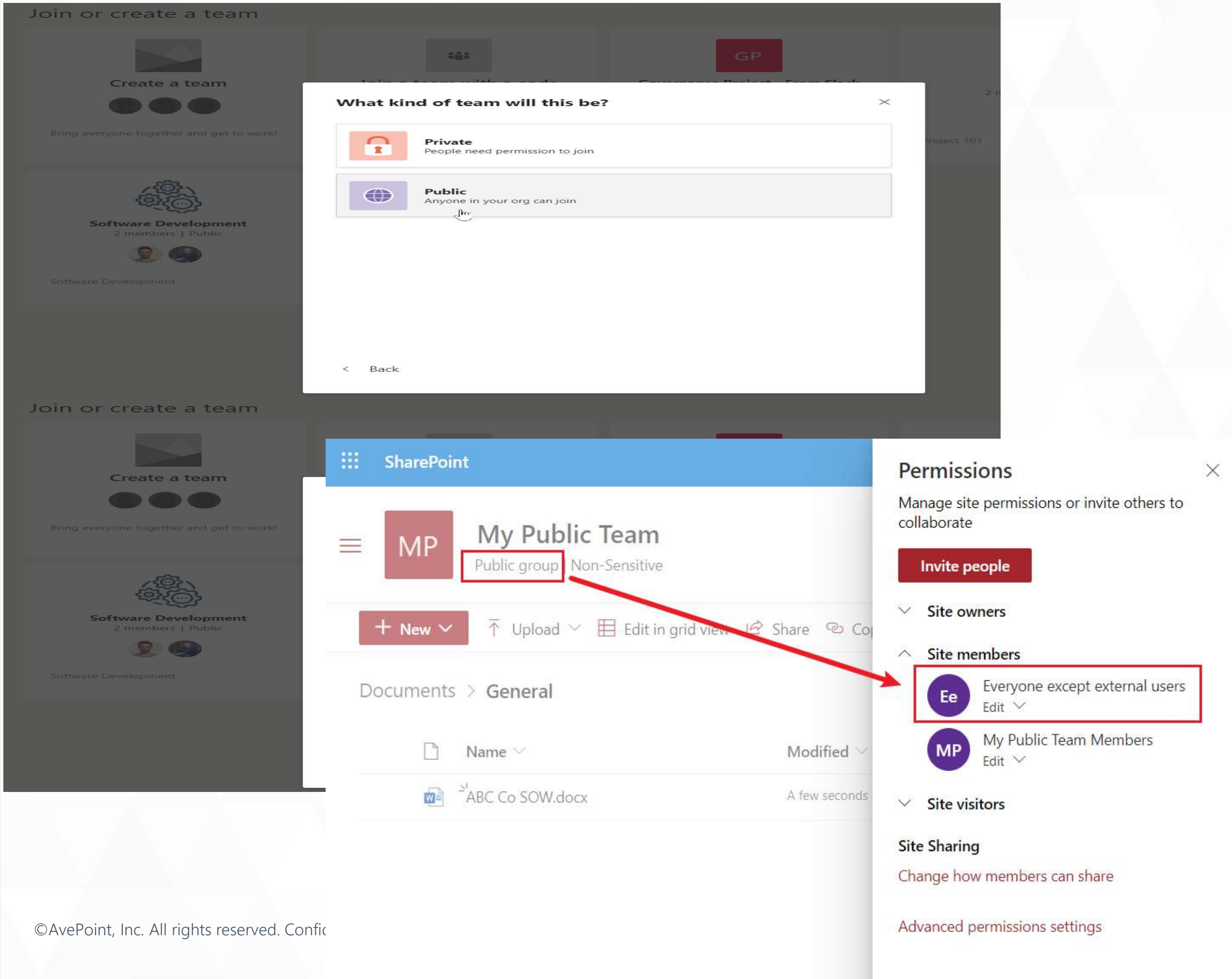
Office 365 gives “Owners” significant privilege

Anyone can be an owner, but even members can share content



THE ANSWER: Right-sizing control based on risk

Understanding the impact of Public/Private for Groups and Teams...



Join or create a team

What kind of team will this be?

Private
People need permission to join

Public
Anyone in your org can join

< Back

SharePoint

My Public Team
Public group Non-Sensitive

Permissions

Manage site permissions or invite others to collaborate

Invite people

Site owners

Site members

Everyone except external users
Edit

My Public Team Members
Edit

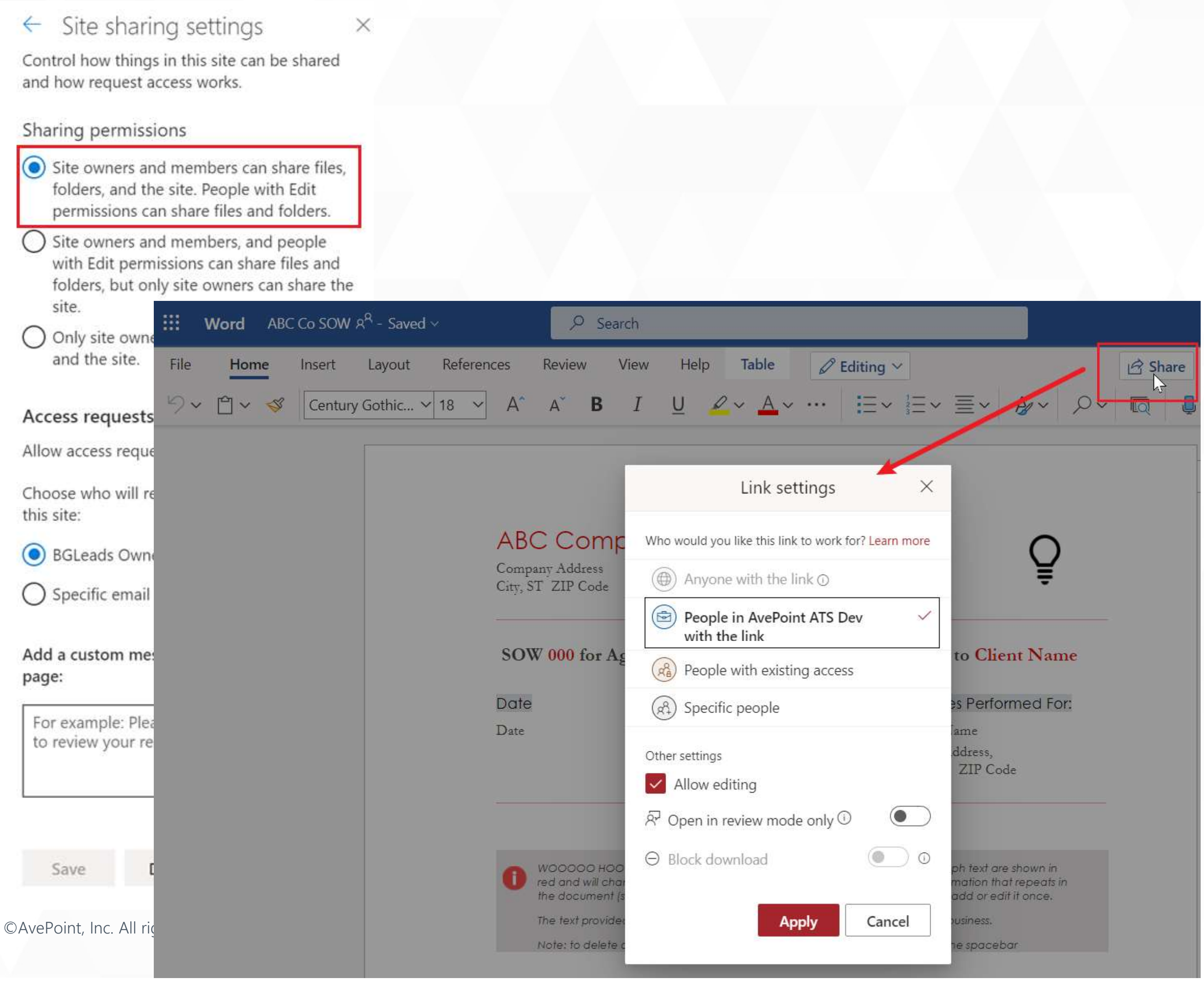
Site visitors

Site Sharing

Change how members can share

Advanced permissions settings

Understanding the default sharing options for all SharePoint sites…



Site sharing settings

Control how things in this site can be shared and how request access works.

Sharing permissions

● Site owners and members can share files, folders, and the site. People with Edit permissions can share files and folders.

○ Site owners and members, and people with Edit permissions can share files and folders, but only site owners can share the site.

○ Only site owne
and the site.

Access requests

Allow access reque

Choose who will re
this site:

● BGLeads Own

○ Specific email

Add a custom me
page:

For example: Plea
to review your re

Save

©AvePoint, Inc. All ri

Link settings

Who would you like this link to work for? Learn more

- Anyone with the link
- People in AvePoint ATS Dev with the link ✓
- People with existing access
- Specific people

Other settings

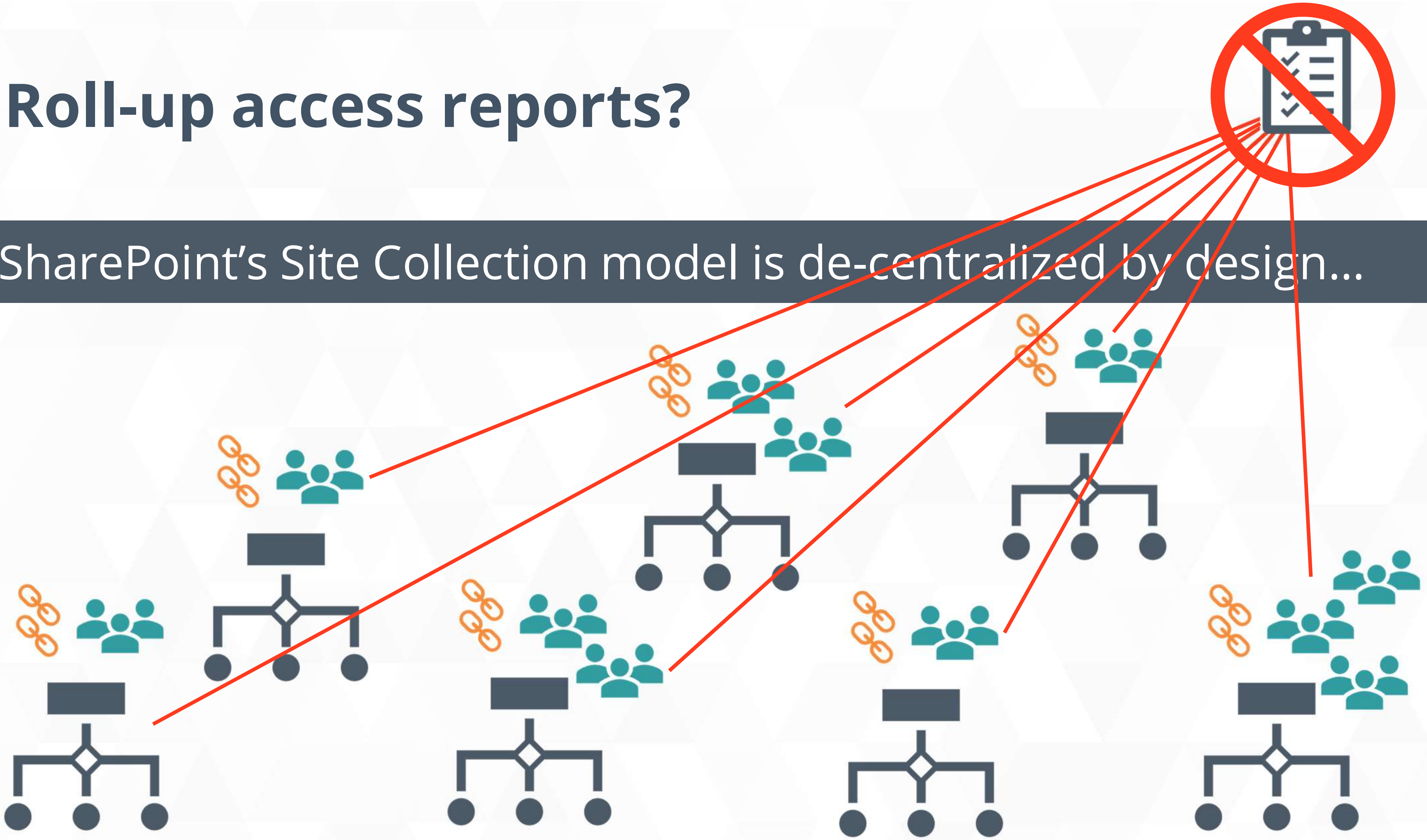
☑ Allow editing

Open in review mode only ○

Block download ○

Roll-up access reports?

SharePoint's Site Collection model is de-centralized by design…



How do you manage security settings?

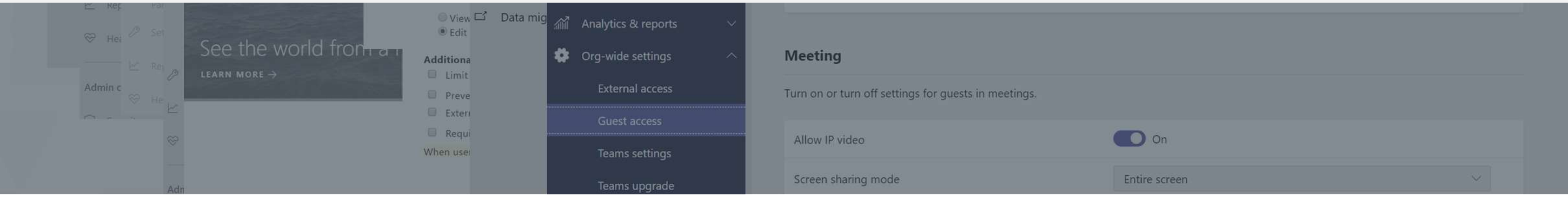
M365 Access Reviews and Admin Settings don’t tell the whole story.

Marco still does not have a top-down view.

He can't identify who has access to what information.

Not enough context to tailor policies for audiences and purpose.

Marco is exhausted.



Meeting

Turn on or turn off settings for guests in meetings.

Allow IP video: On

Screen sharing mode: Entire screen

AvePoint
Policies & Insights

+

Microsoft / Office 365

With PI, organizations can unleash user adoption and the power of Microsoft 365 sensitive information types and security controls, without becoming a security expert. PI guides admins towards appropriate controls with prioritized insights. Set robust controls from one place, that get enforced automatically.

TAP INTO VALUABLE M365 DATA TO PRIORITIZE INSIGHTS

We aggregate sensitive information types and data from Microsoft's own activity feed to keep you focused on what matters

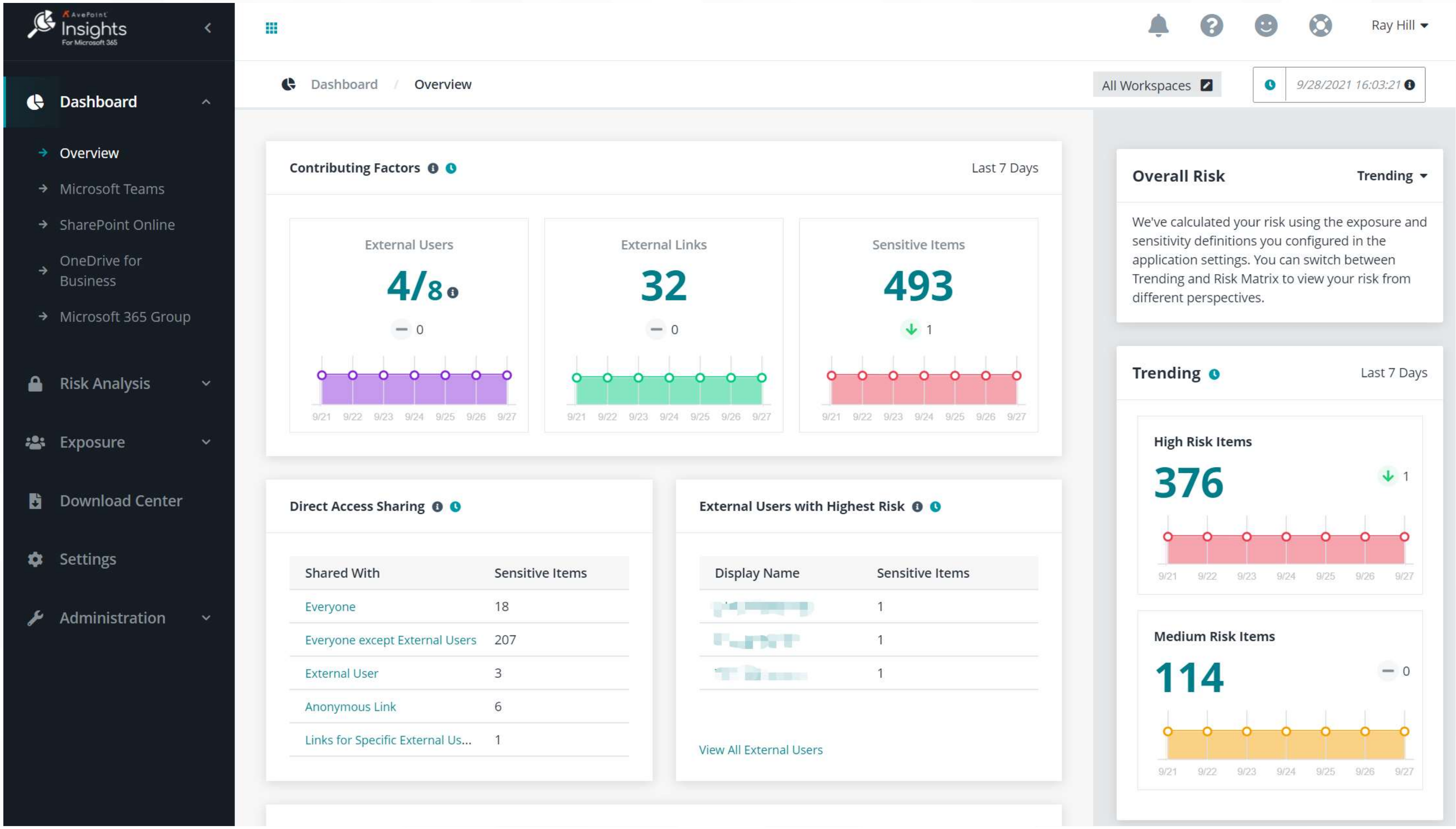
PUT MICROSOFT SECURITY CONTROLS TO WORK

With central access to critical configurations for guest access, sharing, and more – we make it easy to get the control you need

REDUCE IT WORKLOAD FOR ONGOING MANAGEMENT

Prevent configuration drift with policies that get enforced automatically. We enable control, without impeding user adoption

Drawing Your Attention to *Higher Levels*



Overall Risk

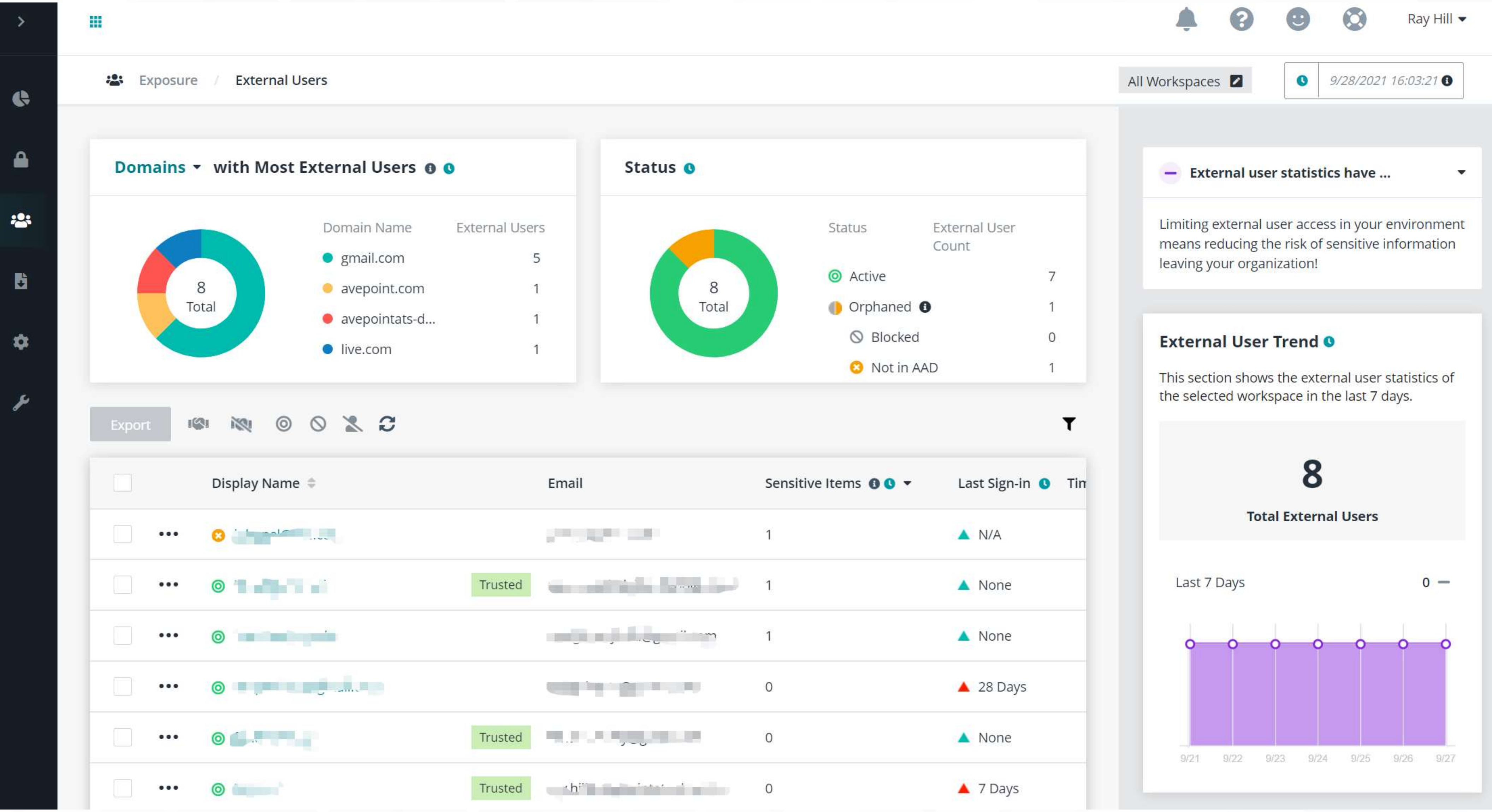
We've calculated your risk using the exposure and sensitivity definitions you configured in the application settings. You can switch between Trending and Risk Matrix to view your risk from different perspectives.

Direct Access Sharing

Shared With	Sensitive Items
Everyone	18
Everyone except External Users	207
External User	3
Anonymous Link	6
Links for Specific External Us...	1

External Users with Highest Risk

Display Name	Sensitive Items
[redacted]	1
[redacted]	1
[redacted]	1



Ray Hill

Exposure / External Users

All Workspaces

9/28/2021 16:03:21

Domains with Most External Users

8 Total

Domain Name	External Users
● gmail.com	5
● avepoint.com	1
● avepointats-d...	1
● live.com	1

Status

8 Total

Status	External User Count
Active	7
Orphaned	1
Blocked	0
Not in AAD	1

Export

☐		Display Name		Email	Sensitive Items	Last Sign-in	Tim
☐	•••	[redacted]		[redacted]	1	N/A	
☐	•••	[redacted]	Trusted	[redacted]	1	None	
☐	•••	[redacted]		[redacted]	1	None	
☐	•••	[redacted]		[redacted]	0	28 Days	
☐	•••	[redacted]	Trusted	[redacted]	0	None	
☐	•••	[redacted]	Trusted	[redacted]	0	7 Days	

External user statistics have ...

Limiting external user access in your environment means reducing the risk of sensitive information leaving your organization!

External User Trend

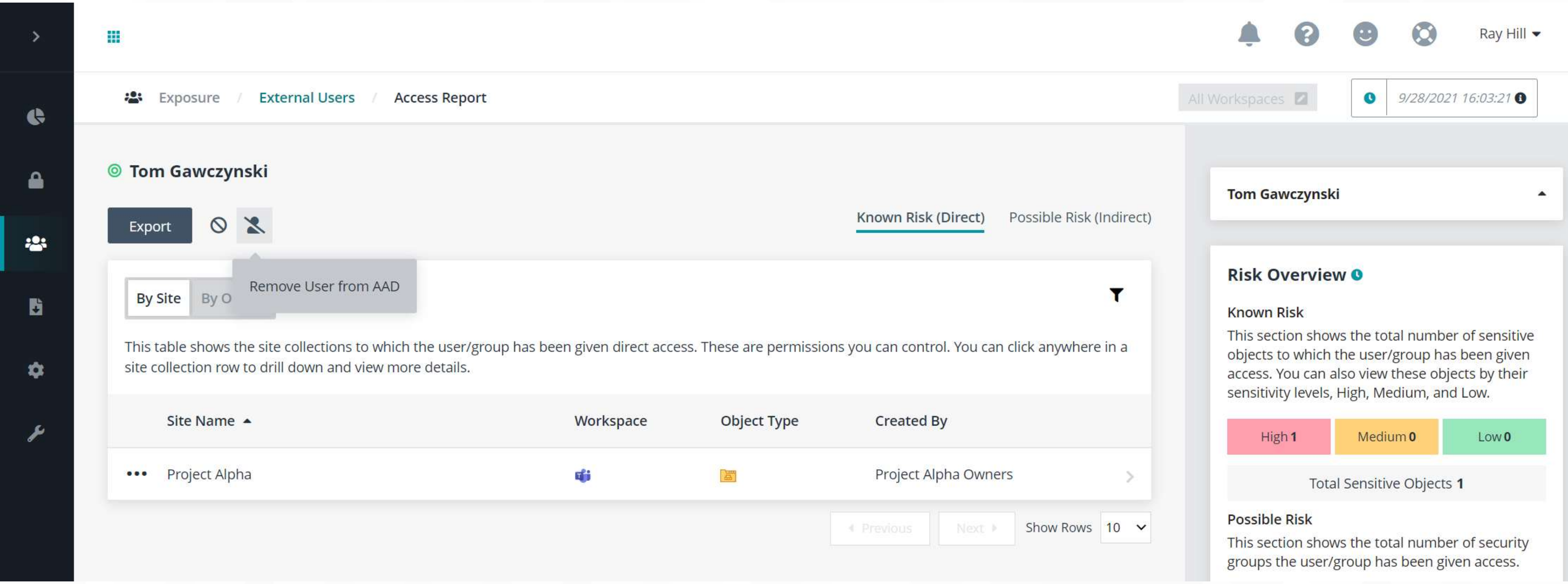
This section shows the external user statistics of the selected workspace in the last 7 days.

8

Total External Users

Last 7 Days 0

User-Level Insights Across our Tenants



Tom Gawczynski

This table shows the site collections to which the user/group has been given direct access. These are permissions you can control. You can click anywhere in a site collection row to drill down and view more details.

Site Name	Workspace	Object Type	Created By
Project Alpha			Project Alpha Owners

Show Rows 10

Tom Gawczynski

Risk Overview

Known Risk

This section shows the total number of sensitive objects to which the user/group has been given access. You can also view these objects by their sensitivity levels, High, Medium, and Low.

High	Medium	Low
1	0	0

Total Sensitive Objects 1

Possible Risk

This section shows the total number of security groups the user/group has been given access.

INCORPORATED 1961

Customer success: City of Port St. Lucie

> When we first ran Policies and Insights, it came up with thousands of links that were shared incorrectly. We hit a button and it basically fixed all the links and that risk was instantly mitigated.
>
> ***Hannah Melton****, Assistant Director IT*

ENABLE REMOTE WORK IN COVID-19 RESPONSE

Migrated to Microsoft 365 with AvePoint within 12 hours. Leveraging AvePoint's governance, security, and backup solutions, was able to drive adoption and minimize risk.

COMPLY WITH LOCAL REGULATIONS

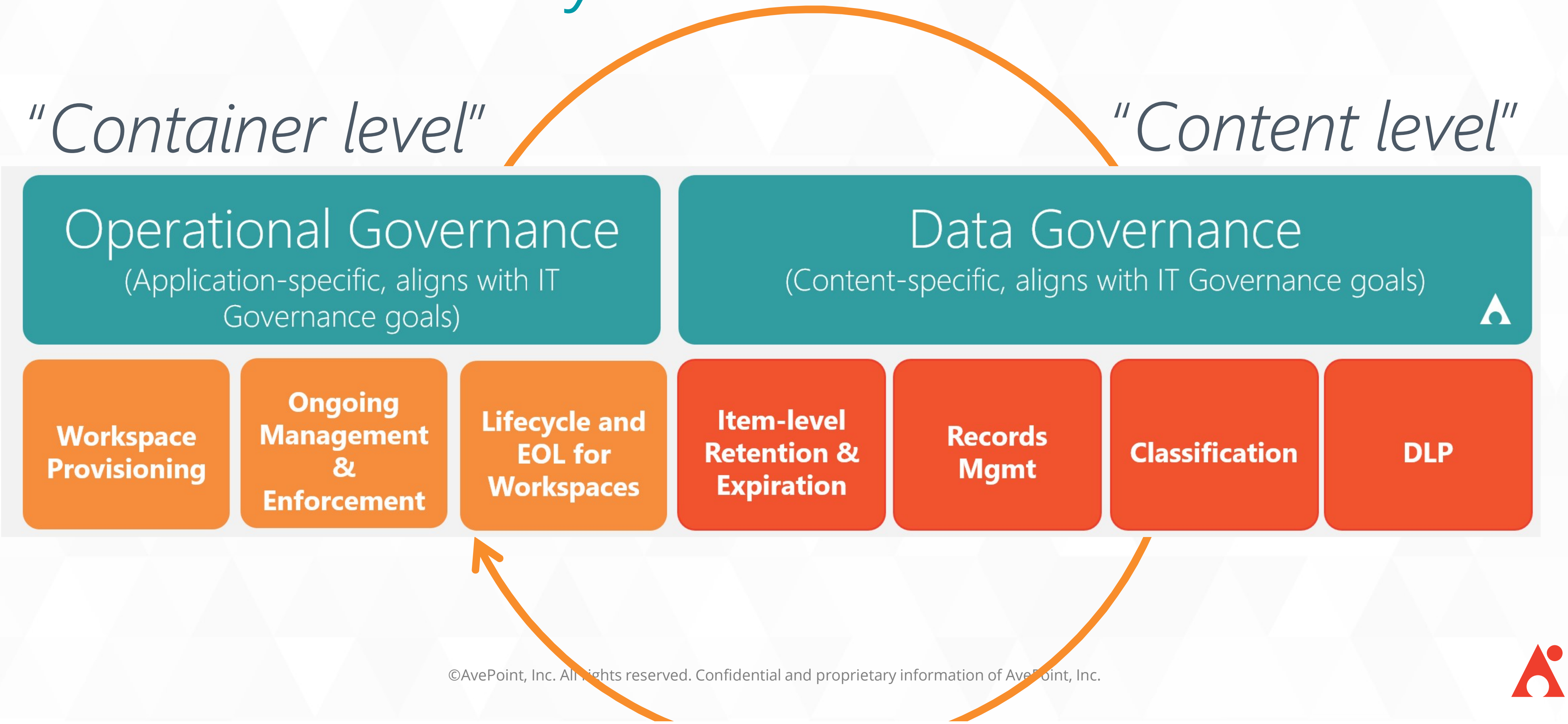
Monitor access to sensitive documents, automatically remediate policy violations for guest access. Security dashboards provide actionable insights. Paired with AvePoint's granular backup and restore, meet "Sunshine State" protection laws.

REDUCE MANUAL IT WORK TO ROLL-OUT & MANAGE TEAMS

Reduce Teams provisioning process by 600%, automatically fix links that are shared incorrectly, and prevent configuration drift with governance + PI capabilities. No more manual configuration and membership checks to validate access!

Top-down, and bottom-up…

You can't chase every document!



"Container level"

"Content level"

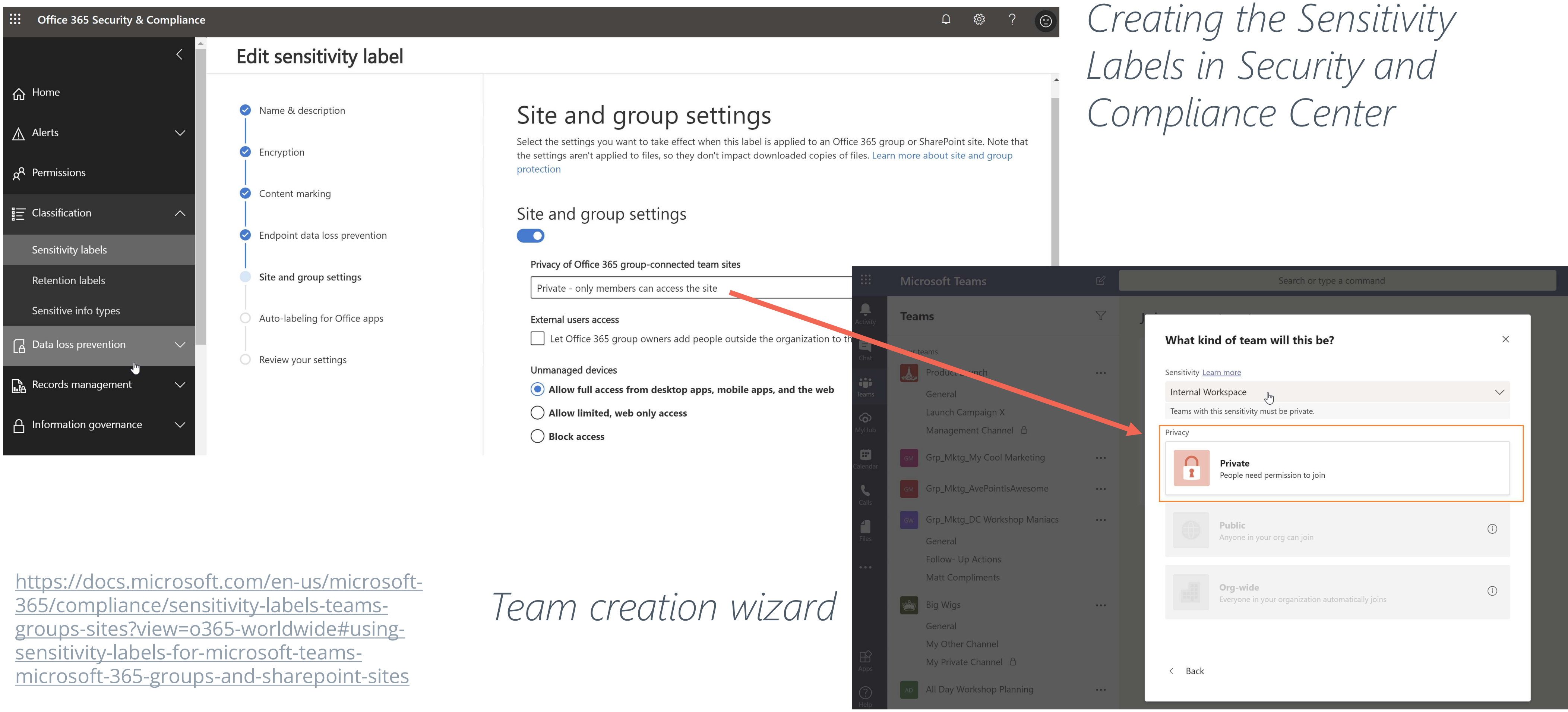
Operational Governance
(Application-specific, aligns with IT Governance goals)

Data Governance
(Content-specific, aligns with IT Governance goals)

- **Workspace Provisioning**
- **Ongoing Management & Enforcement**
- **Lifecycle and EOL for Workspaces**
- **Item-level Retention & Expiration**
- **Records Mgmt**
- **Classification**
- **DLP**

Sensitivity Labels for teams, groups and sites

Creating the Sensitivity Labels in Security and Compliance Center



Office 365 Security & Compliance

Edit sensitivity label

Site and group settings

Select the settings you want to take effect when this label is applied to an Office 365 group or SharePoint site. Note that the settings aren't applied to files, so they don't impact downloaded copies of files. Learn more about site and group protection

Site and group settings

Privacy of Office 365 group-connected team sites: Private - only members can access the site

External users access

☐ Let Office 365 group owners add people outside the organization to th

Unmanaged devices

● **Allow full access from desktop apps, mobile apps, and the web**

○ **Allow limited, web only access**

○ **Block access**

Microsoft Teams

What kind of team will this be?

Sensitivity Learn more: Internal Workspace

Teams with this sensitivity must be private.

Privacy

Private People need permission to join

Public Anyone in your org can join

Org-wide Everyone in your organization automatically joins

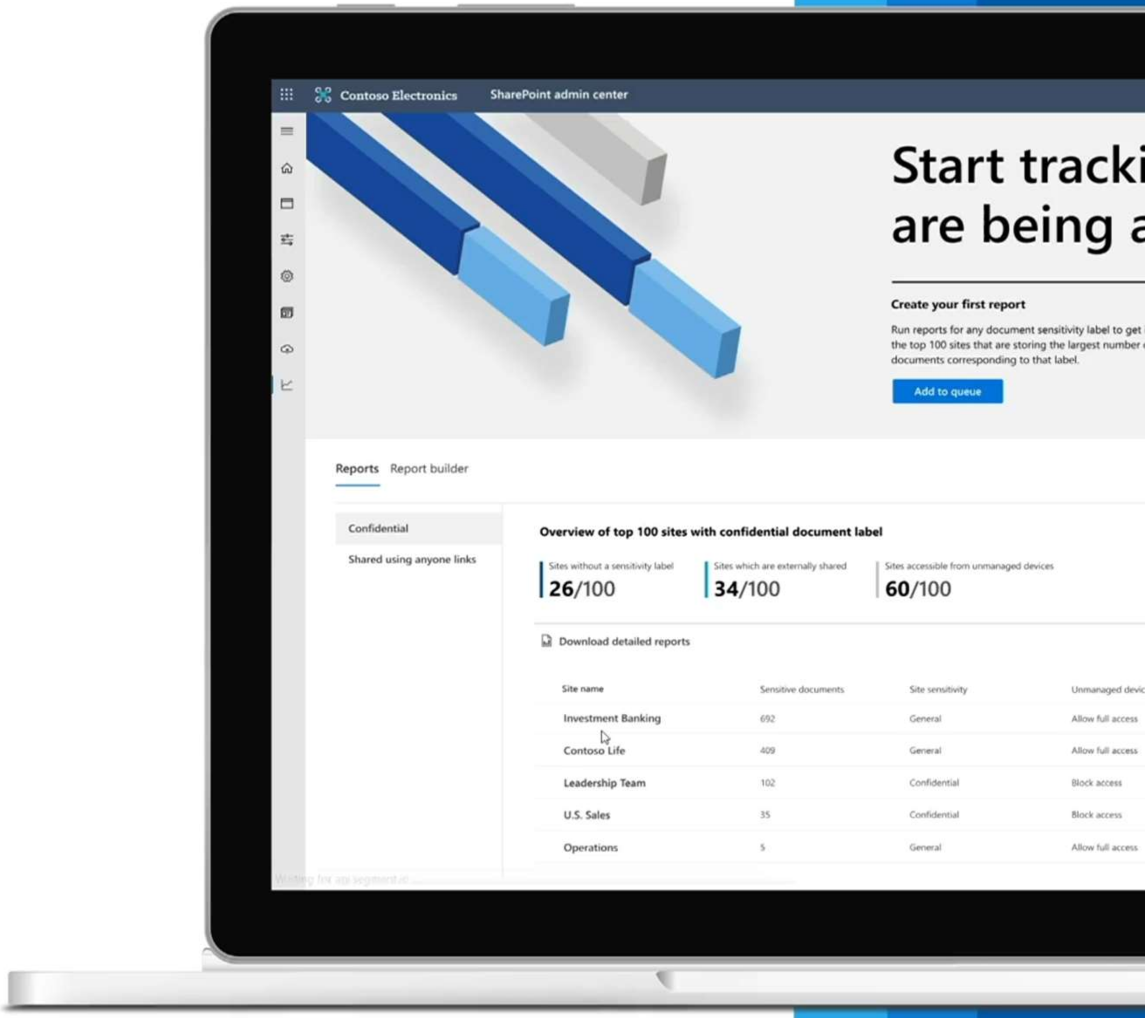
Back

Team creation wizard

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide#using-sensitivity-labels-for-microsoft-teams-microsoft-365-groups-and-sharepoint-sites

Microsoft Security

Protecting sensitive information at the site or team level



Start tracki
are being a

Create your first report

Run reports for any document sensitivity label to get
the top 100 sites that are storing the largest number
documents corresponding to that label.

Overview of top 100 sites with confidential document label

Sites without a sensitivity label **26**/100

Sites which are externally shared **34**/100

Sites accessible from unmanaged devices **60**/100

Site name	Sensitive documents	Site sensitivity	Unmanaged devic
Investment Banking	692	General	Allow full access
Contoso Life	409	General	Allow full access
Leadership Team	102	Confidential	Block access
U.S. Sales	35	Confidential	Block access
Operations	5	General	Allow full access

Advantages of a container-focused approach

- Establishing data ownership
- Workspace level classification
- Collaboration asset inventory
- Attestation/Recertification
- Automated self-service requests
- End-to-end lifecycle management

What is sprawl?

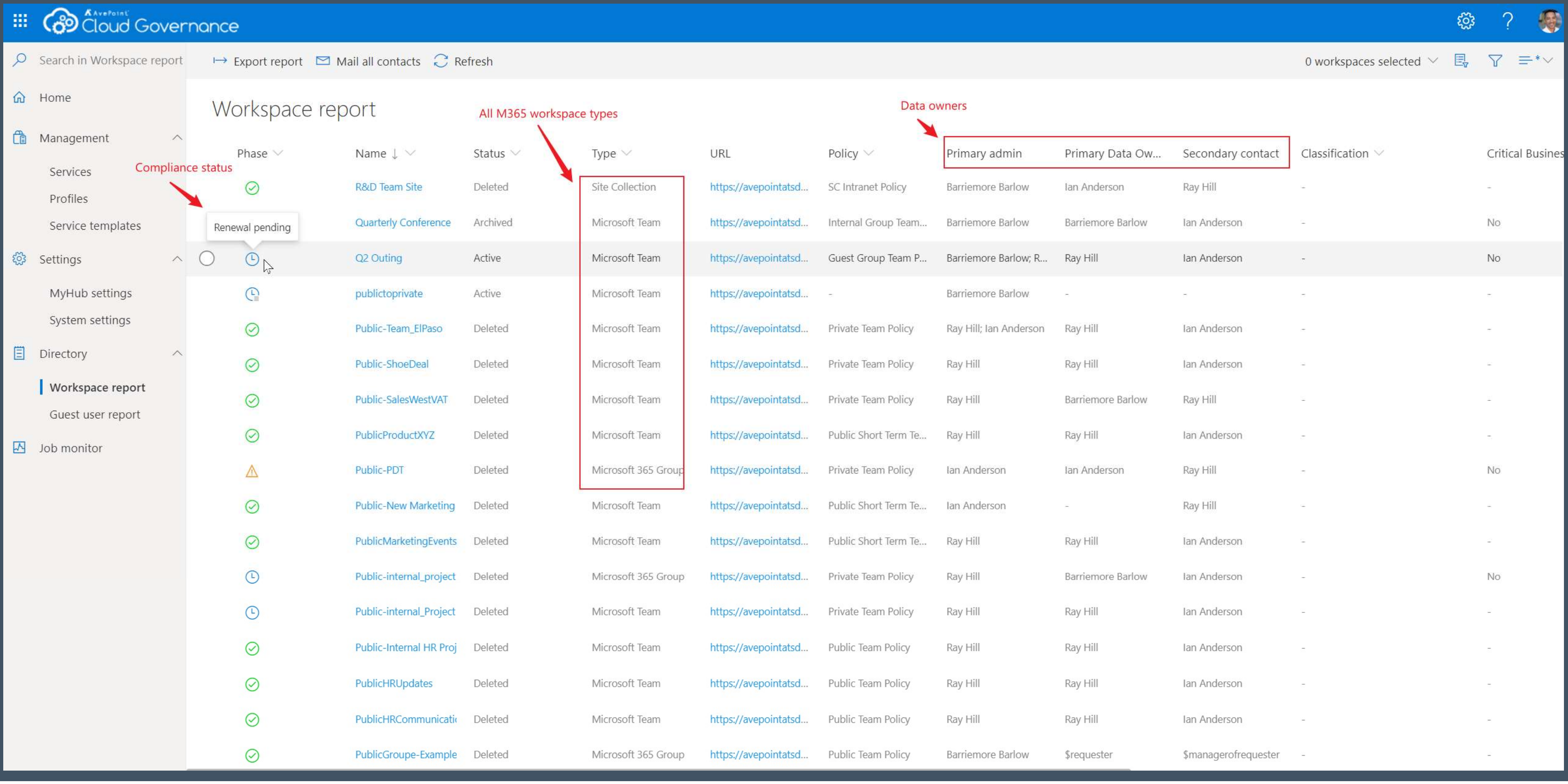
Not a number…

… just more than you can effectively manage

Cutting through the noise…

Maintaining an inventory of your collaborative workspaces

Admins have an “inventory” of all M365 collaborative workspaces



Workspace report

All M365 workspace types

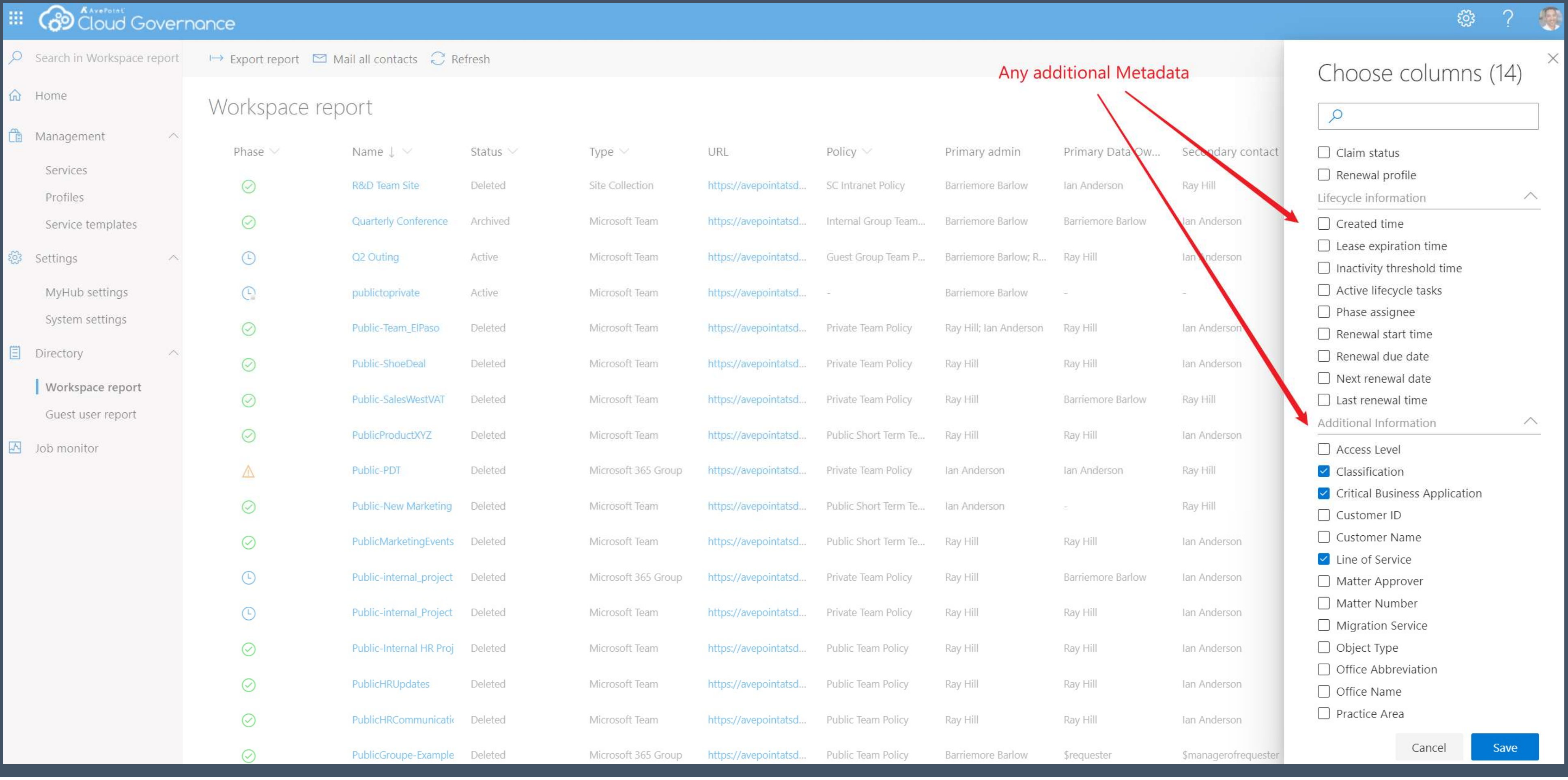
Data owners

Compliance status

Renewal pending

	Phase	Name ↓	Status	Type	URL	Policy	Primary admin	Primary Data Ow...	Secondary contact	Classification	Critical Busines
	✓	R&D Team Site	Deleted	Site Collection	https://avepointatsd...	SC Intranet Policy	Barriemore Barlow	Ian Anderson	Ray Hill	-	-
		Quarterly Conference	Archived	Microsoft Team	https://avepointatsd...	Internal Group Team...	Barriemore Barlow	Barriemore Barlow	Ian Anderson	-	No
○	🕒	Q2 Outing	Active	Microsoft Team	https://avepointatsd...	Guest Group Team P...	Barriemore Barlow; R...	Ray Hill	Ian Anderson	-	No
	🕒	publictoprivate	Active	Microsoft Team	https://avepointatsd...	-	Barriemore Barlow	-	-	-	-
	✓	Public-Team_ElPaso	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill; Ian Anderson	Ray Hill	Ian Anderson	-	-
	✓	Public-ShoeDeal	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill	Ray Hill	Ian Anderson	-	-
	✓	Public-SalesWestVAT	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill	Barriemore Barlow	Ray Hill	-	-
	✓	PublicProductXYZ	Deleted	Microsoft Team	https://avepointatsd...	Public Short Term Te...	Ray Hill	Ray Hill	Ian Anderson	-	-
	⚠	Public-PDT	Deleted	Microsoft 365 Group	https://avepointatsd...	Private Team Policy	Ian Anderson	Ian Anderson	Ray Hill	-	No
	✓	Public-New Marketing	Deleted	Microsoft Team	https://avepointatsd...	Public Short Term Te...	Ian Anderson	-	Ray Hill	-	-
	✓	PublicMarketingEvents	Deleted	Microsoft Team	https://avepointatsd...	Public Short Term Te...	Ray Hill	Ray Hill	Ian Anderson	-	-
	🕒	Public-internal_project	Deleted	Microsoft 365 Group	https://avepointatsd...	Private Team Policy	Ray Hill	Barriemore Barlow	Ian Anderson	-	No
	🕒	Public-internal_Project	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill	Ray Hill	Ian Anderson	-	-
	✓	Public-Internal HR Proj	Deleted	Microsoft Team	https://avepointatsd...	Public Team Policy	Ray Hill	Ray Hill	Ian Anderson	-	-
	✓	PublicHRUpdates	Deleted	Microsoft Team	https://avepointatsd...	Public Team Policy	Ray Hill	Ray Hill	Ian Anderson	-	-
	✓	PublicHRCommunicati	Deleted	Microsoft Team	https://avepointatsd...	Public Team Policy	Ray Hill	Ray Hill	Ian Anderson	-	-
	✓	PublicGroupe-Example	Deleted	Microsoft 365 Group	https://avepointatsd...	Public Team Policy	Barriemore Barlow	$requester	$managerofrequester	-	-

Admins have deep visibility into all built-in and organizational metadata



Any additional Metadata

Workspace report

Phase	Name ↓	Status	Type	URL	Policy	Primary admin	Primary Data Ow...	Secondary contact
✓	R&D Team Site	Deleted	Site Collection	https://avepointatsd...	SC Intranet Policy	Barriemore Barlow	Ian Anderson	Ray Hill
✓	Quarterly Conference	Archived	Microsoft Team	https://avepointatsd...	Internal Group Team...	Barriemore Barlow	Barriemore Barlow	Ian Anderson
🕒	Q2 Outing	Active	Microsoft Team	https://avepointatsd...	Guest Group Team P...	Barriemore Barlow; R...	Ray Hill	Ian Anderson
🕒	publictoprivate	Active	Microsoft Team	https://avepointatsd...	-	Barriemore Barlow	-	-
✓	Public-Team_ElPaso	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill; Ian Anderson	Ray Hill	Ian Anderson
✓	Public-ShoeDeal	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	Public-SalesWestVAT	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill	Barriemore Barlow	Ray Hill
✓	PublicProductXYZ	Deleted	Microsoft Team	https://avepointatsd...	Public Short Term Te...	Ray Hill	Ray Hill	Ian Anderson
⚠	Public-PDT	Deleted	Microsoft 365 Group	https://avepointatsd...	Private Team Policy	Ian Anderson	Ian Anderson	Ray Hill
✓	Public-New Marketing	Deleted	Microsoft Team	https://avepointatsd...	Public Short Term Te...	Ian Anderson	-	Ray Hill
✓	PublicMarketingEvents	Deleted	Microsoft Team	https://avepointatsd...	Public Short Term Te...	Ray Hill	Ray Hill	Ian Anderson
🕒	Public-internal_project	Deleted	Microsoft 365 Group	https://avepointatsd...	Private Team Policy	Ray Hill	Barriemore Barlow	Ian Anderson
🕒	Public-internal_Project	Deleted	Microsoft Team	https://avepointatsd...	Private Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	Public-Internal HR Proj	Deleted	Microsoft Team	https://avepointatsd...	Public Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	PublicHRUpdates	Deleted	Microsoft Team	https://avepointatsd...	Public Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	PublicHRCommunicati	Deleted	Microsoft Team	https://avepointatsd...	Public Team Policy	Ray Hill	Ray Hill	Ian Anderson
✓	PublicGroupe-Example	Deleted	Microsoft 365 Group	https://avepointatsd...	Public Team Policy	Barriemore Barlow	$requester	$managerofrequester

Choose columns (14)

☐ Claim status
☐ Renewal profile

Lifecycle information

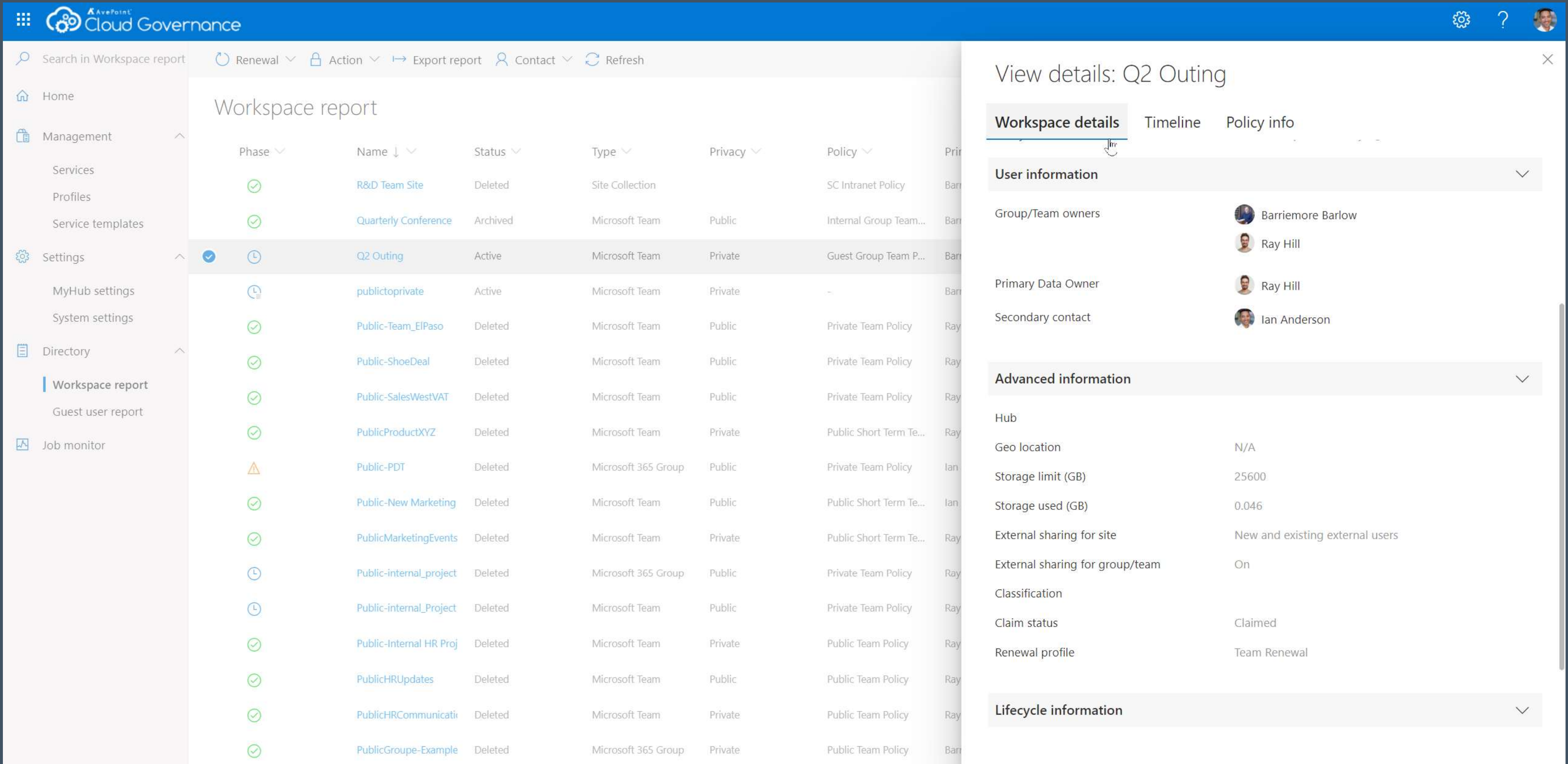
☐ Created time
☐ Lease expiration time
☐ Inactivity threshold time
☐ Active lifecycle tasks
☐ Phase assignee
☐ Renewal start time
☐ Renewal due date
☐ Next renewal date
☐ Last renewal time

Additional Information

☐ Access Level
☑ Classification
☑ Critical Business Application
☐ Customer ID
☐ Customer Name
☑ Line of Service
☐ Matter Approver
☐ Matter Number
☐ Migration Service
☐ Object Type
☐ Office Abbreviation
☐ Office Name
☐ Practice Area

Cancel Save

Admins can drill-down for all details of each workspace



Workspace report

	Phase	Name ↓	Status	Type	Privacy	Policy	Pri
	✓	R&D Team Site	Deleted	Site Collection		SC Intranet Policy	Bar
	✓	Quarterly Conference	Archived	Microsoft Team	Public	Internal Group Team...	Bar
☑	◷	Q2 Outing	Active	Microsoft Team	Private	Guest Group Team P...	Bar
	◷	publictoprivate	Active	Microsoft Team	Private	-	Bar
	✓	Public-Team_ElPaso	Deleted	Microsoft Team	Public	Private Team Policy	Ray
	✓	Public-ShoeDeal	Deleted	Microsoft Team	Public	Private Team Policy	Ray
	✓	Public-SalesWestVAT	Deleted	Microsoft Team	Public	Private Team Policy	Ray
	✓	PublicProductXYZ	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray
	⚠	Public-PDT	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ian
	✓	Public-New Marketing	Deleted	Microsoft Team	Public	Public Short Term Te...	Ian
	✓	PublicMarketingEvents	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray
	◷	Public-internal_project	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ray
	◷	Public-internal_Project	Deleted	Microsoft Team	Public	Private Team Policy	Ray
	✓	Public-Internal HR Proj	Deleted	Microsoft Team	Private	Public Team Policy	Ray
	✓	PublicHRUpdates	Deleted	Microsoft Team	Public	Public Team Policy	Ray
	✓	PublicHRCommunicati	Deleted	Microsoft Team	Private	Public Team Policy	Ray
	✓	PublicGroupe-Example	Deleted	Microsoft 365 Group	Private	Public Team Policy	Bar

View details: Q2 Outing

Workspace details | Timeline | Policy info

User information

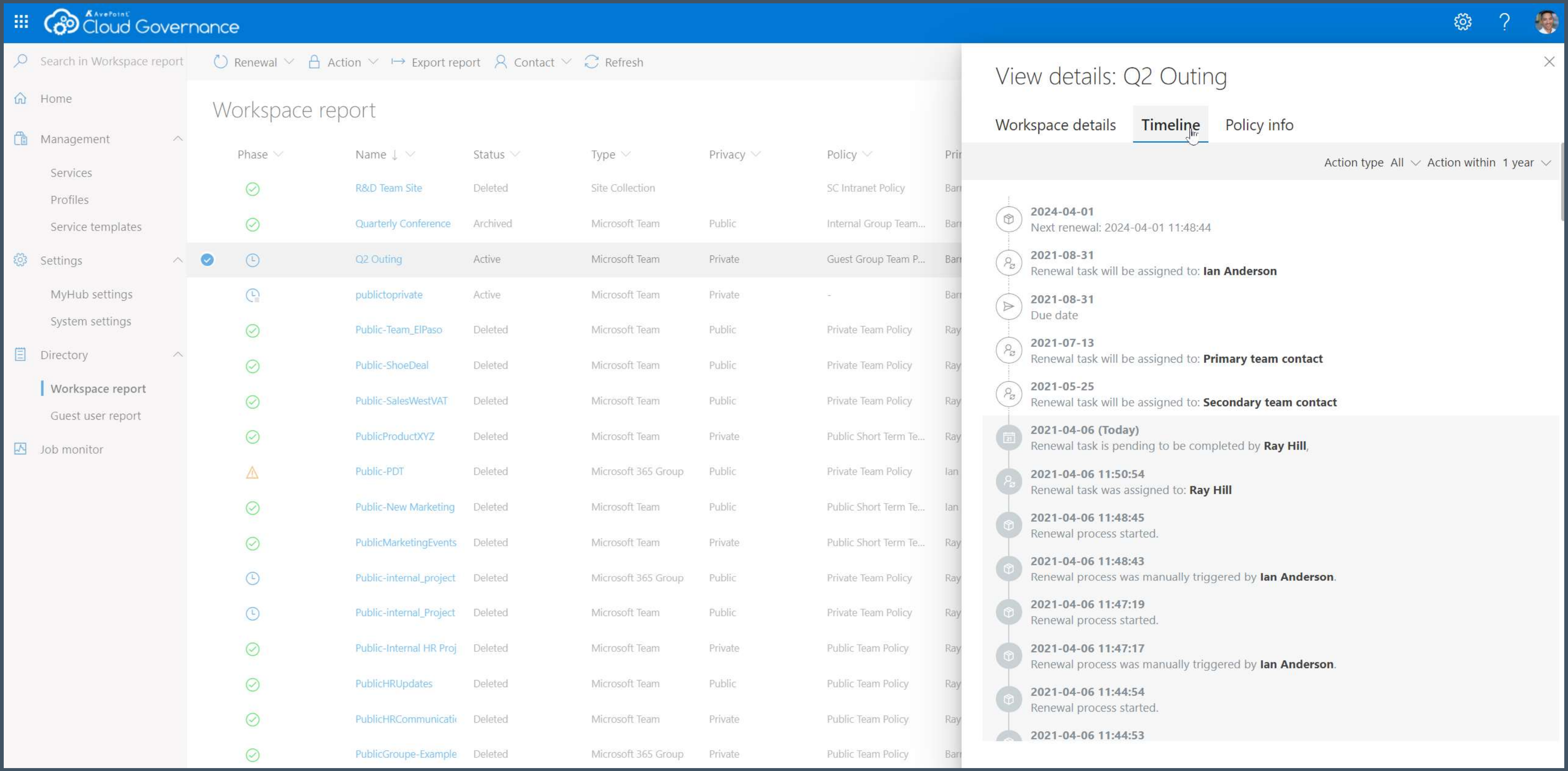
Group/Team owners	Barriemore Barlow Ray Hill
Primary Data Owner	Ray Hill
Secondary contact	Ian Anderson

Advanced information

Hub	
Geo location	N/A
Storage limit (GB)	25600
Storage used (GB)	0.046
External sharing for site	New and existing external users
External sharing for group/team	On
Classification	
Claim status	Claimed
Renewal profile	Team Renewal

Lifecycle information

Admins can drill-down for all details of each workspace



Workspace report

	Phase	Name ↓	Status	Type	Privacy	Policy	Pri
	✓	R&D Team Site	Deleted	Site Collection		SC Intranet Policy	Bar
	✓	Quarterly Conference	Archived	Microsoft Team	Public	Internal Group Team...	Bar
☑	◷	Q2 Outing	Active	Microsoft Team	Private	Guest Group Team P...	Bar
	◷	publictoprivate	Active	Microsoft Team	Private	-	Bar
	✓	Public-Team_ElPaso	Deleted	Microsoft Team	Public	Private Team Policy	Ray
	✓	Public-ShoeDeal	Deleted	Microsoft Team	Public	Private Team Policy	Ray
	✓	Public-SalesWestVAT	Deleted	Microsoft Team	Public	Private Team Policy	Ray
	✓	PublicProductXYZ	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray
	⚠	Public-PDT	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ian
	✓	Public-New Marketing	Deleted	Microsoft Team	Public	Public Short Term Te...	Ian
	✓	PublicMarketingEvents	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray
	◷	Public-internal_project	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ray
	◷	Public-internal_Project	Deleted	Microsoft Team	Public	Private Team Policy	Ray
	✓	Public-Internal HR Proj	Deleted	Microsoft Team	Private	Public Team Policy	Ray
	✓	PublicHRUpdates	Deleted	Microsoft Team	Public	Public Team Policy	Ray
	✓	PublicHRCommunicati	Deleted	Microsoft Team	Private	Public Team Policy	Ray
	✓	PublicGroupe-Example	Deleted	Microsoft 365 Group	Private	Public Team Policy	Bar

View details: Q2 Outing

Action type All
Action within 1 year

2024-04-01
Next renewal: 2024-04-01 11:48:44

2021-08-31
Renewal task will be assigned to: **Ian Anderson**

2021-08-31
Due date

2021-07-13
Renewal task will be assigned to: **Primary team contact**

2021-05-25
Renewal task will be assigned to: **Secondary team contact**

2021-04-06 (Today)
Renewal task is pending to be completed by **Ray Hill**,

2021-04-06 11:50:54
Renewal task was assigned to: **Ray Hill**

2021-04-06 11:48:45
Renewal process started.

2021-04-06 11:48:43
Renewal process was manually triggered by **Ian Anderson**.

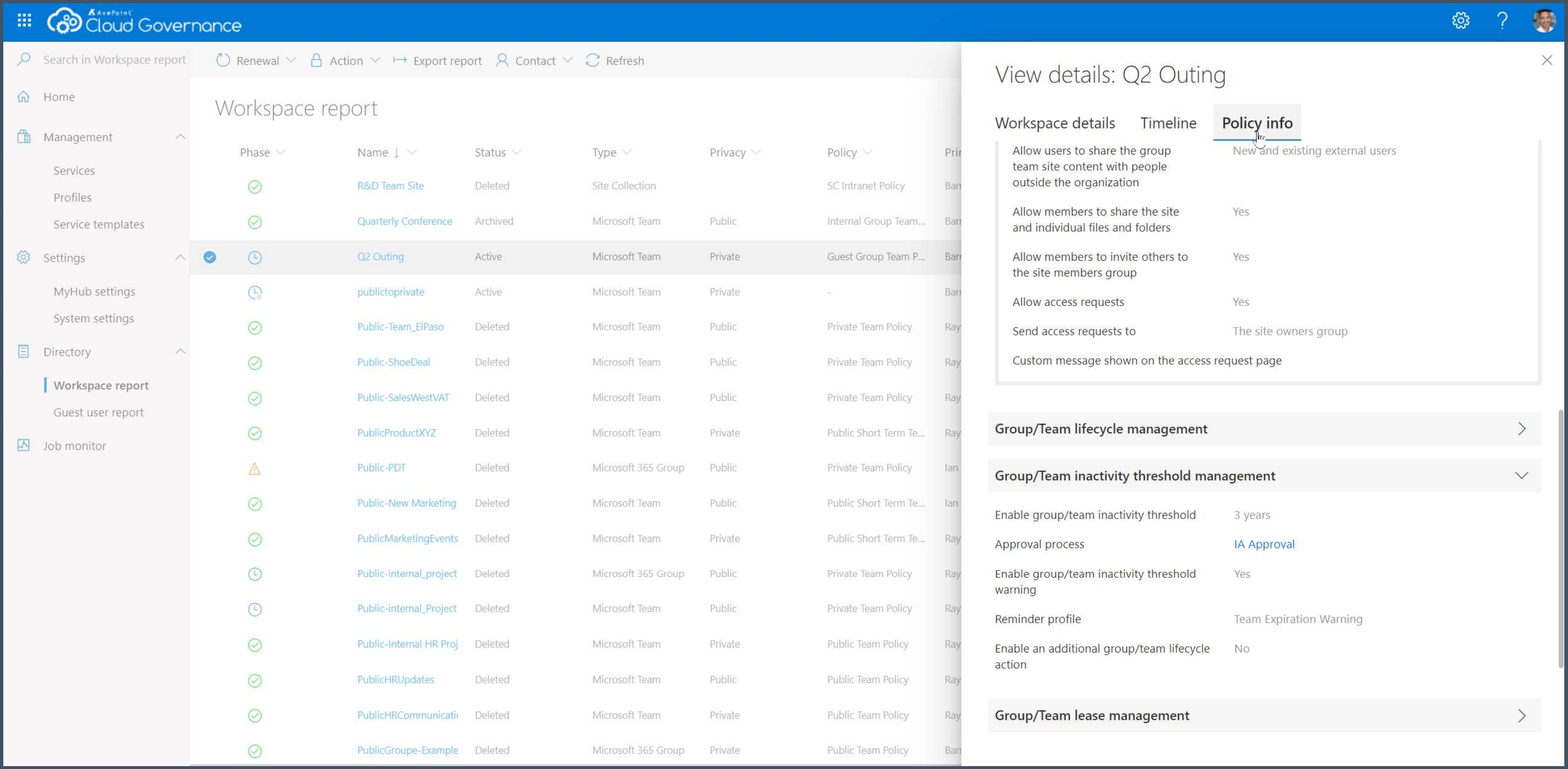
2021-04-06 11:47:19
Renewal process started.

2021-04-06 11:47:17
Renewal process was manually triggered by **Ian Anderson**.

2021-04-06 11:44:54
Renewal process started.

2021-04-06 11:44:53

Admins can drill-down for all details of each workspace



Workspace report

Phase	Name ↓	Status	Type	Privacy	Policy	Pri
✓	R&D Team Site	Deleted	Site Collection		SC Intranet Policy	Bar
✓	Quarterly Conference	Archived	Microsoft Team	Public	Internal Group Team...	Bar
🕒	Q2 Outing	Active	Microsoft Team	Private	Guest Group Team P...	Bar
🕒	publictoprivate	Active	Microsoft Team	Private	-	Bar
✓	Public-Team_ElPaso	Deleted	Microsoft Team	Public	Private Team Policy	Ray
✓	Public-ShoeDeal	Deleted	Microsoft Team	Public	Private Team Policy	Ray
✓	Public-SalesWestVAT	Deleted	Microsoft Team	Public	Private Team Policy	Ray
✓	PublicProductXYZ	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray
⚠	Public-PDT	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ian
✓	Public-New Marketing	Deleted	Microsoft Team	Public	Public Short Term Te...	Ian
✓	PublicMarketingEvents	Deleted	Microsoft Team	Private	Public Short Term Te...	Ray
🕒	Public-internal_project	Deleted	Microsoft 365 Group	Public	Private Team Policy	Ray
🕒	Public-internal_Project	Deleted	Microsoft Team	Public	Private Team Policy	Ray
✓	Public-Internal HR Proj	Deleted	Microsoft Team	Private	Public Team Policy	Ray
✓	PublicHRUpdates	Deleted	Microsoft Team	Public	Public Team Policy	Ray
✓	PublicHRCommunicati	Deleted	Microsoft Team	Private	Public Team Policy	Ray
✓	PublicGroupe-Example	Deleted	Microsoft 365 Group	Private	Public Team Policy	Bar

View details: Q2 Outing

Workspace details | Timeline | **Policy info**

Allow users to share the group team site content with people outside the organization	New and existing external users
Allow members to share the site and individual files and folders	Yes
Allow members to invite others to the site members group	Yes
Allow access requests	Yes
Send access requests to	The site owners group
Custom message shown on the access request page	

Group/Team lifecycle management

Group/Team inactivity threshold management

Enable group/team inactivity threshold	3 years
Approval process	IA Approval
Enable group/team inactivity threshold warning	Yes
Reminder profile	Team Expiration Warning
Enable an additional group/team lifecycle action	No

Group/Team lease management

EXAMPLE

"Policies" are defined and mapped to users, divisions, or purpose

	ITAR/EAR Protected Workspace	General Purpose Workspace	CAS Protected Workspace
Team Owner	Service Account	Business User	Service Account
EXPIRATION/ RETENTION	3 Months after last accessed	3 Months after last accessed	12 Months after last accessed
MEMBER SHARING SETTINGS	Not Allowed	Allowed	Not Allowed
RECERTIFY ACCESS	after 3 Months	after 6 Months	after 12 Months

How do you get there from here?

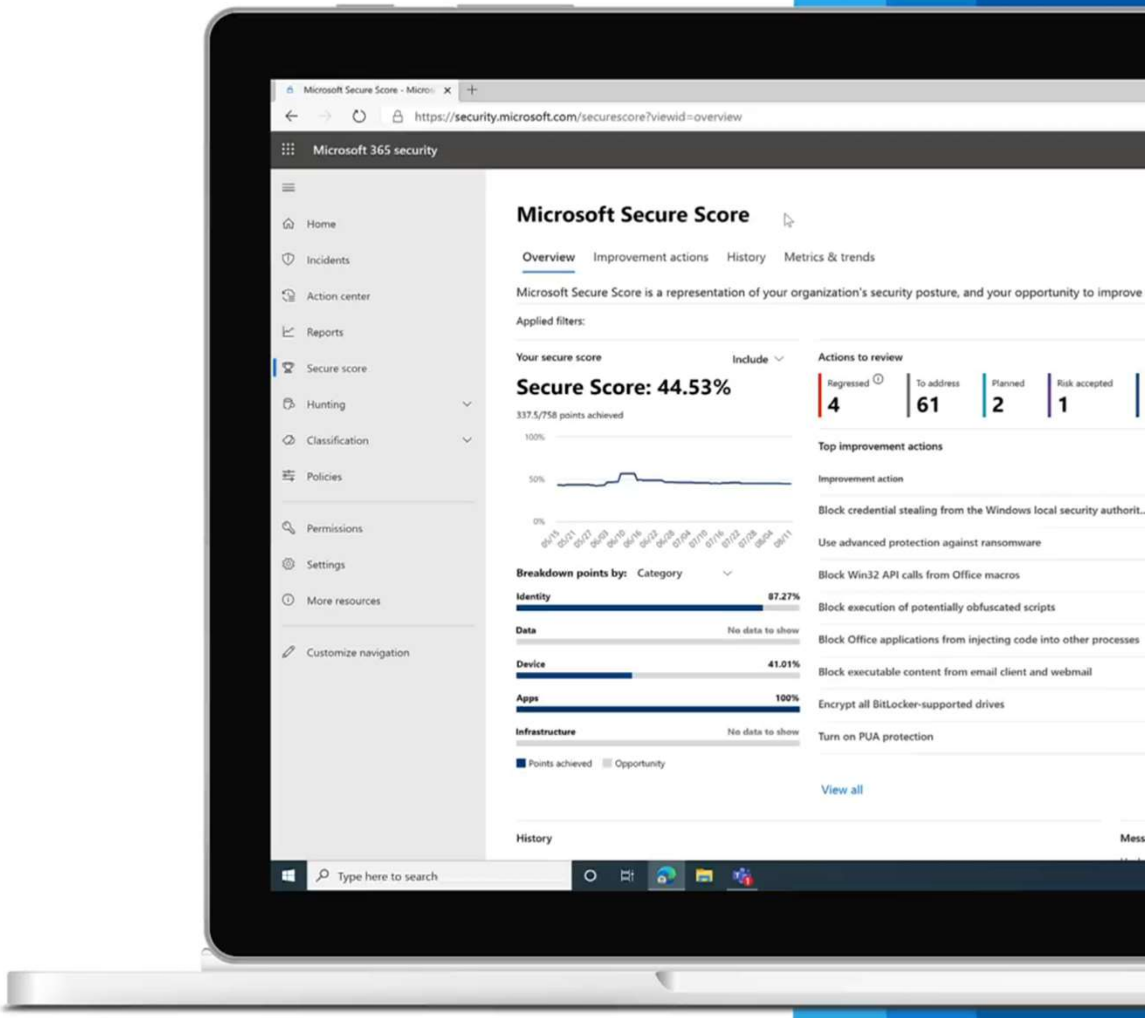
Managed provisioning or import of collaborative workspaces

How do you keep this information current over time?

Periodic review and confirmation of permissions, access, ownership and key governance attributes

Microsoft Secure Score

Strengthen your security posture



Microsoft Secure Score

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

Applied filters:

Your secure score

Secure Score: 44.53%

337.5/758 points achieved

Breakdown points by: Category

Identity	87.27%
Data	No data to show
Device	41.01%
Apps	100%
Infrastructure	No data to show

Actions to review

Regressed	To address	Planned	Risk accepted
4	61	2	1

Top improvement actions

Improvement action

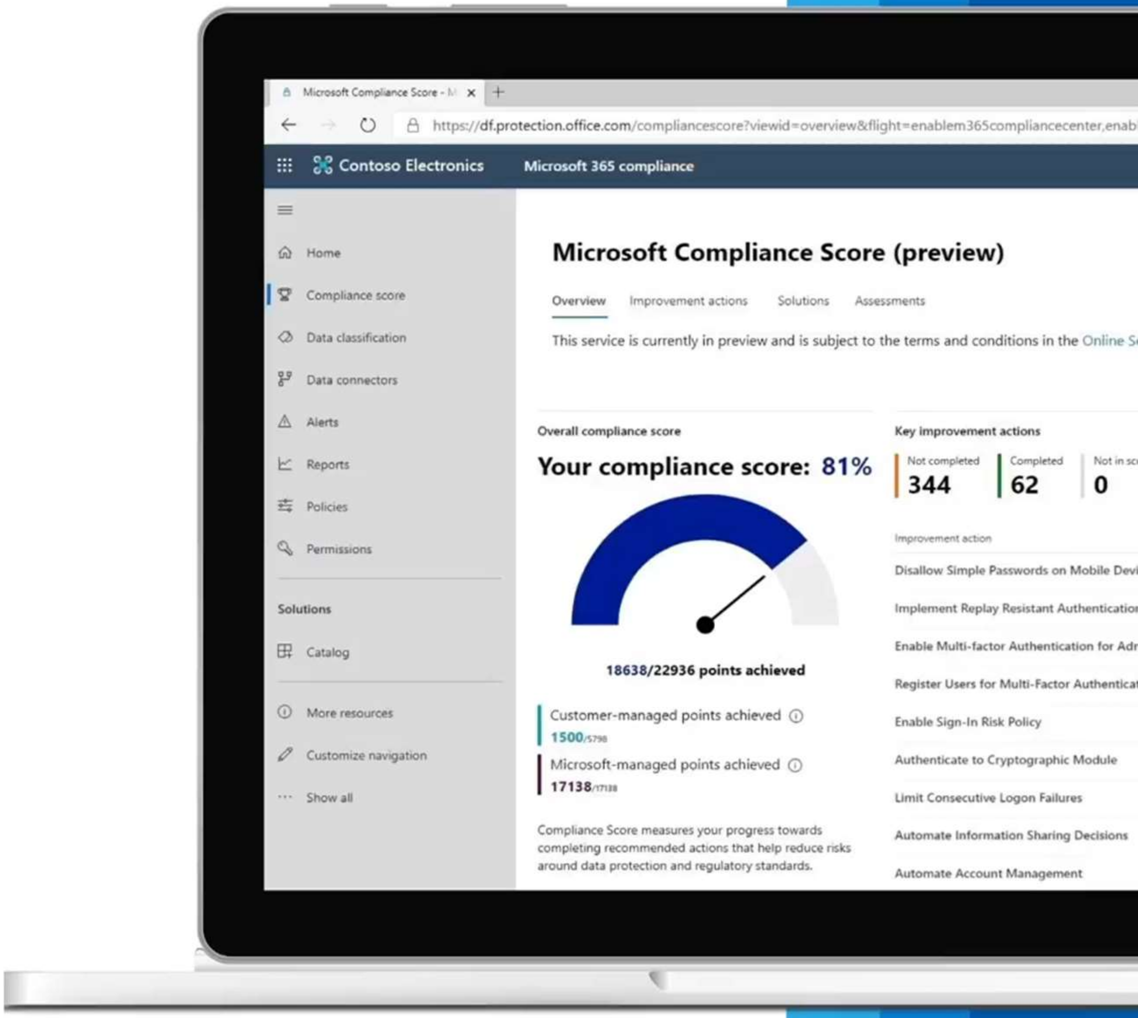
- Block credential stealing from the Windows local security authorit...
- Use advanced protection against ransomware
- Block Win32 API calls from Office macros
- Block execution of potentially obfuscated scripts
- Block Office applications from injecting code into other processes
- Block executable content from email client and webmail
- Encrypt all BitLocker-supported drives
- Turn on PUA protection

History

Mess

Microsoft 365 Security

Compliance Score



Microsoft Compliance Score (preview)

This service is currently in preview and is subject to the terms and conditions in the Online S

Overall compliance score

Your compliance score: 81%

18638/22936 points achieved

Customer-managed points achieved 1500/5798

Microsoft-managed points achieved 17138/17138

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Key improvement actions

Not completed	Completed	Not in sc
344	62	0

Improvement action

- Disallow Simple Passwords on Mobile Devi
- Implement Replay Resistant Authenticatio
- Enable Multi-factor Authentication for Adr
- Register Users for Multi-Factor Authentica
- Enable Sign-In Risk Policy
- Authenticate to Cryptographic Module
- Limit Consecutive Logon Failures
- Automate Information Sharing Decisions
- Automate Account Management

Microsoft

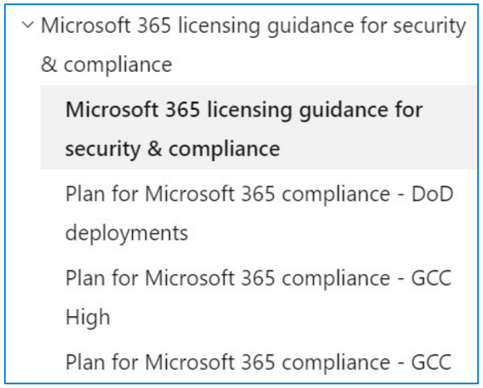
Licensing: Greatest Hits from Microsoft

Breakdown of basic & advanced use cases by SKU

Quick reference:

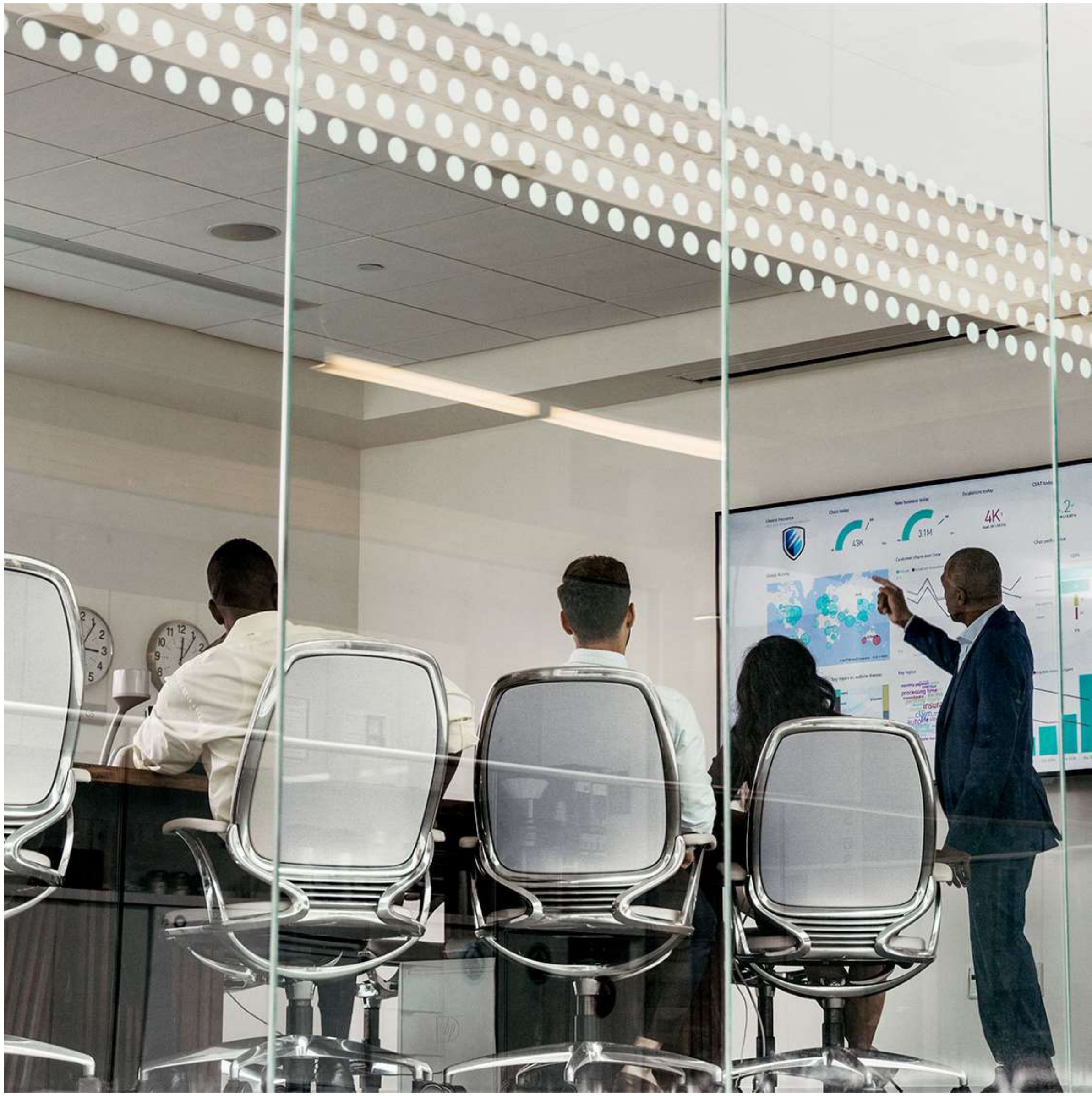
Manual = E3

Automated = E5



- Microsoft 365 licensing guidance for security & compliance
  - **Microsoft 365 licensing guidance for security & compliance**
  - Plan for Microsoft 365 compliance - DoD deployments
  - Plan for Microsoft 365 compliance - GCC High
  - Plan for Microsoft 365 compliance - GCC

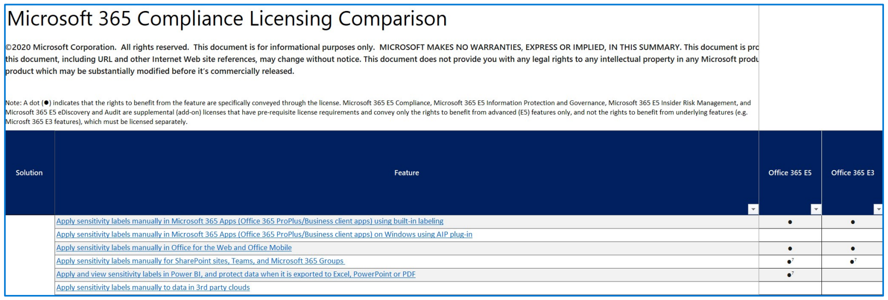
https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance



Microsoft

Licensing: The Master Class

"How much does it cost to do that specific thing? Is there an add-on instead?"

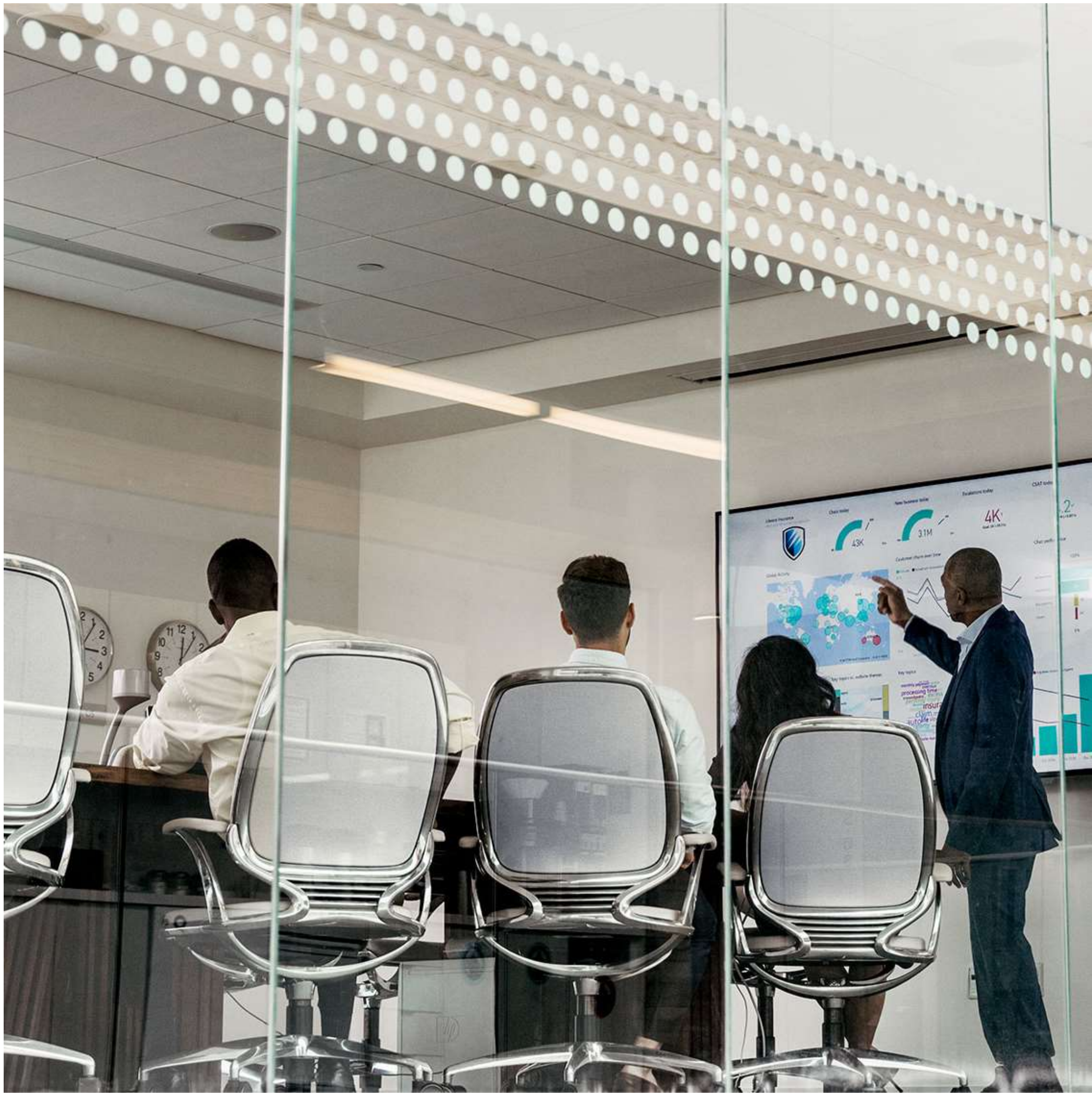


Microsoft 365 Compliance Licensing Comparison

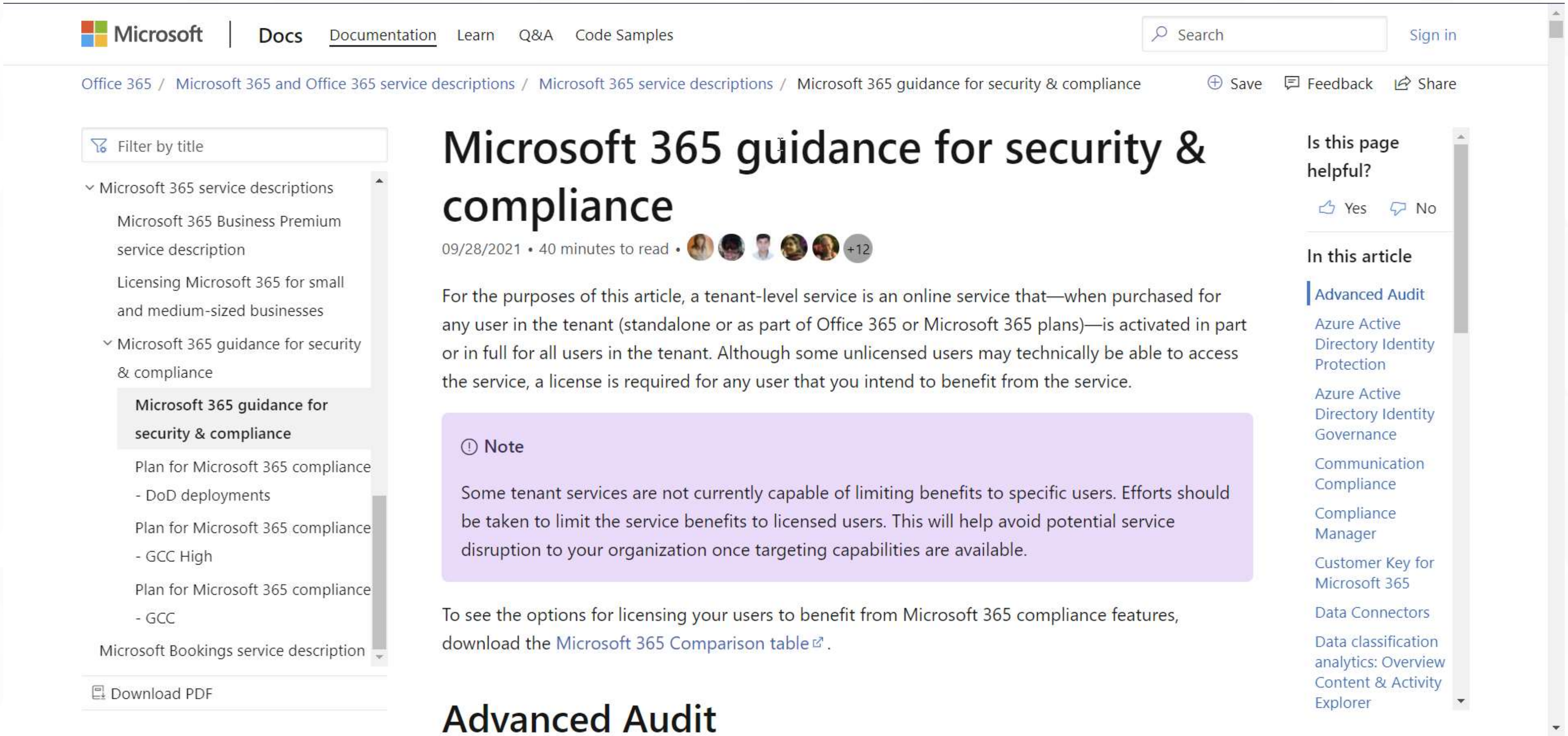
Note: A dot (●) indicates that the rights to benefit from the feature are specifically conveyed through the license. Microsoft 365 E5 Compliance, Microsoft 365 E5 Information Protection and Governance, Microsoft 365 E5 Insider Risk Management, and Microsoft 365 E5 eDiscovery and Audit are supplemental (add-on) licenses that have pre-requisite license requirements and convey only the rights to benefit from advanced (E5) features only, and not the rights to benefit from underlying features (e.g. Microsft 365 E3 features), which must be licensed separately.

Solution	Feature	Office 365 E5	Office 365 E3
	Apply sensitivity labels manually in Microsoft 365 Apps (Office 365 ProPlus/Business client apps) using built-in labeling	●	●
	Apply sensitivity labels manually in Microsoft 365 Apps (Office 365 ProPlus/Business client apps) on Windows using AIP plug-in		
	Apply sensitivity labels manually in Office for the Web and Office Mobile	●	●
	Apply sensitivity labels manually for SharePoint sites, Teams, and Microsoft 365 Groups	●[7]	●[7]
	Apply and view sensitivity labels in Power BI, and protect data when it is exported to Excel, PowerPoint or PDF	●[7]	
	Apply sensitivity labels manually to data in 3rd party clouds		

https://docs.microsoft.com/en-us/office365/servicedescriptions/downloads/microsoft-365-compliance-licensing-comparison.xlsx



What are the Microsoft Licensing Requirements for all of this?


Microsoft
Docs
Documentation
Learn
Q&A
Code Samples
Search
Sign in
Office 365 / Microsoft 365 and Office 365 service descriptions / Microsoft 365 service descriptions / Microsoft 365 guidance for security & compliance
Save
Feedback
Share
Filter by title
Microsoft 365 service descriptions
Microsoft 365 Business Premium service description
Licensing Microsoft 365 for small and medium-sized businesses
Microsoft 365 guidance for security & compliance
Microsoft 365 guidance for security & compliance
Plan for Microsoft 365 compliance - DoD deployments
Plan for Microsoft 365 compliance - GCC High
Plan for Microsoft 365 compliance - GCC
Microsoft Bookings service description
Download PDF
Is this page helpful?
Yes
No
In this article
Advanced Audit
Azure Active Directory Identity Protection
Azure Active Directory Identity Governance
Communication Compliance
Compliance Manager
Customer Key for Microsoft 365
Data Connectors
Data classification analytics: Overview Content & Activity Explorer
+12

Microsoft 365 guidance for security & compliance

09/28/2021 • 40 minutes to read •

For the purposes of this article, a tenant-level service is an online service that—when purchased for any user in the tenant (standalone or as part of Office 365 or Microsoft 365 plans)—is activated in part or in full for all users in the tenant. Although some unlicensed users may technically be able to access the service, a license is required for any user that you intend to benefit from the service.

> ⓘ **Note**
>
> Some tenant services are not currently capable of limiting benefits to specific users. Efforts should be taken to limit the service benefits to licensed users. This will help avoid potential service disruption to your organization once targeting capabilities are available.

To see the options for licensing your users to benefit from Microsoft 365 compliance features, download the Microsoft 365 Comparison table.

Advanced Audit

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWIf1n

Next Steps!

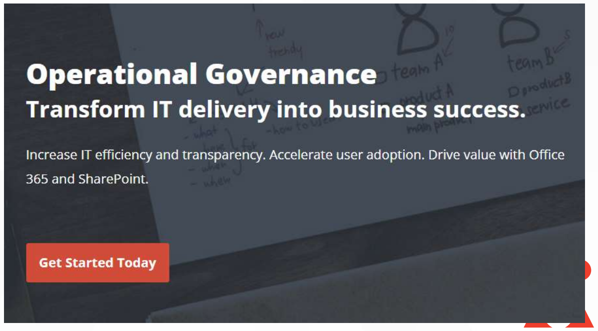
Resources to dig in deeper on today's topics…

See Policies and Insights in action! How to videos available here…
https://youtu.be/kgbnQvl-sFc

AvePoint Policies & Insights
For Microsoft 365

Whitepaper:
Implementing a Best Practice Approach to Risk-Based Data Protection and Cybersecurity
https://www.avepoint.com/resources/whitepaper-form/4429

Request a demonstration of the AvePoint solutions discussed today!
https://www.avepoint.com/get-started



Operational Governance
Transform IT delivery into business success.

Increase IT efficiency and transparency. Accelerate user adoption. Drive value with Office 365 and SharePoint.

thank you

AvePoint®

☎ Sales@AvePoint.com | +1 800.661.6588

www.AvePoint.com

in

thank you

Sales@AvePoint.com

www.AvePoint.com

AvePoint

Gracias

Hvala

Ahsante

Cám ơn

நன்றி

谢谢

תודה

ευχαριστώ

Obrigado

Teşekkürler

شكريه

Köszönöm

Tack

多謝晒

Danke

Kiitos

متشكرم

Terima Kasih

ありがとうございます

Mulţumesc

дякую

Grazie

شكراً

Salamat Po

Dank u Wel

ขอบคุณครับ

спасибо

Ďakujem

благодаря

Tak

감사합니다

Děkuji

Dziękuję

Merci

धन्यवाद