Become a Microsoft 365 Security Black Belt in <1 Hour

Or: 49 Tips in 60 Minutes!

Ru Campbell

MC2MC

CONNECT


CONNECT · COLLABORATE · CREATE
MC2MC
CONNECT


2Pint


PATCH
MY PC


robopack


wortell


INGRAM
MICRO


The Collective


bechtle


lebon.IT


ConXioN
The new style of IT


VirtualMetric

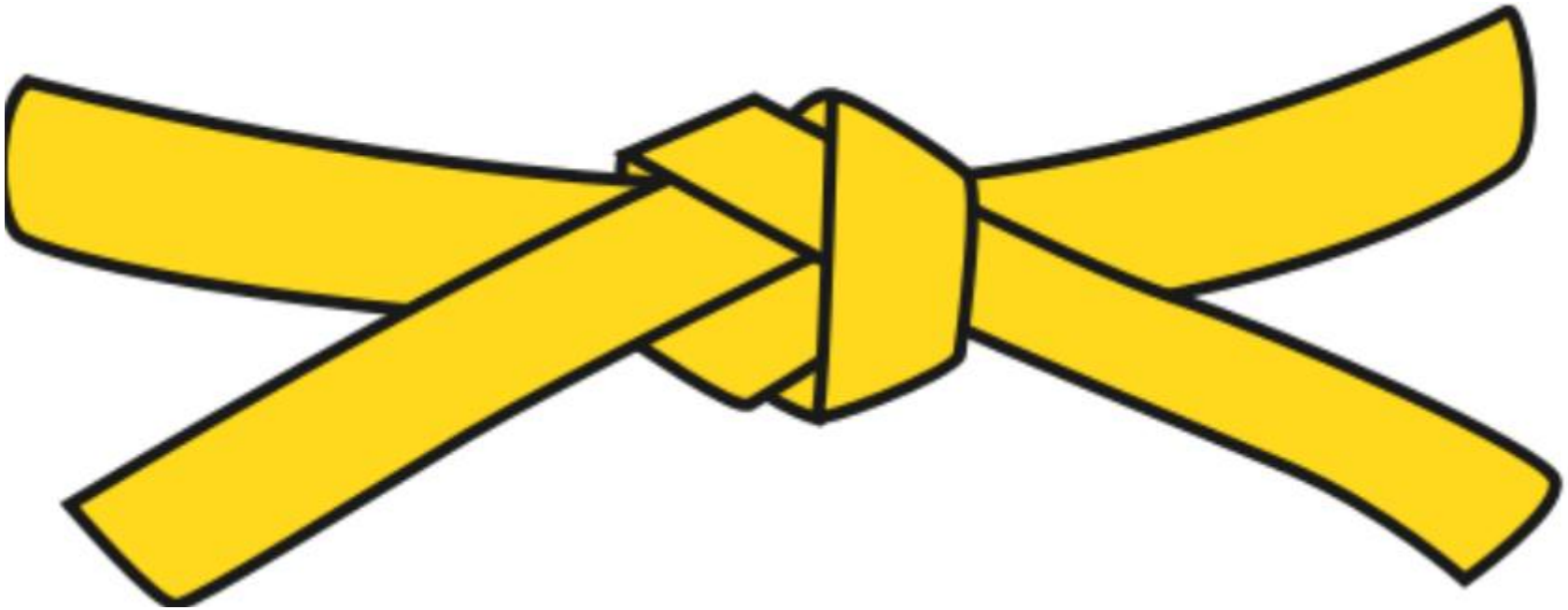

veeam


evri

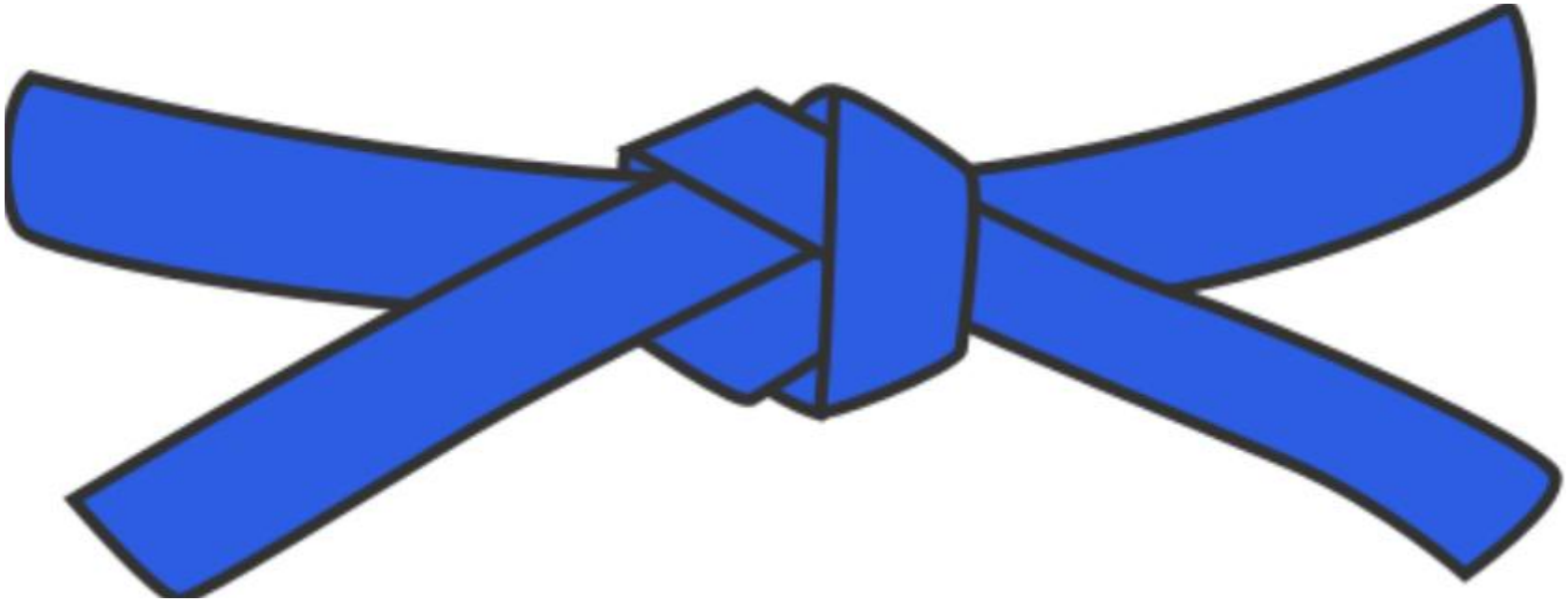
Defining *Microsoft 365 Security*

MC2MC
CONNECT

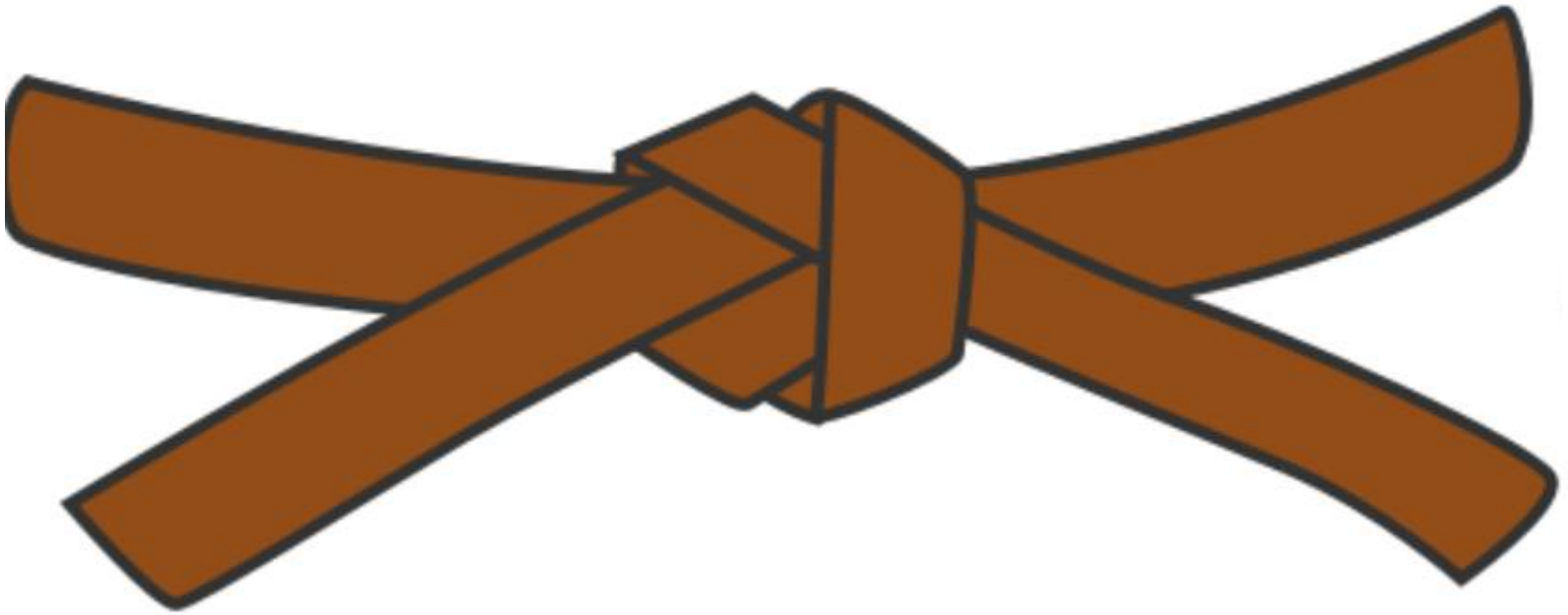
Raise your hands!



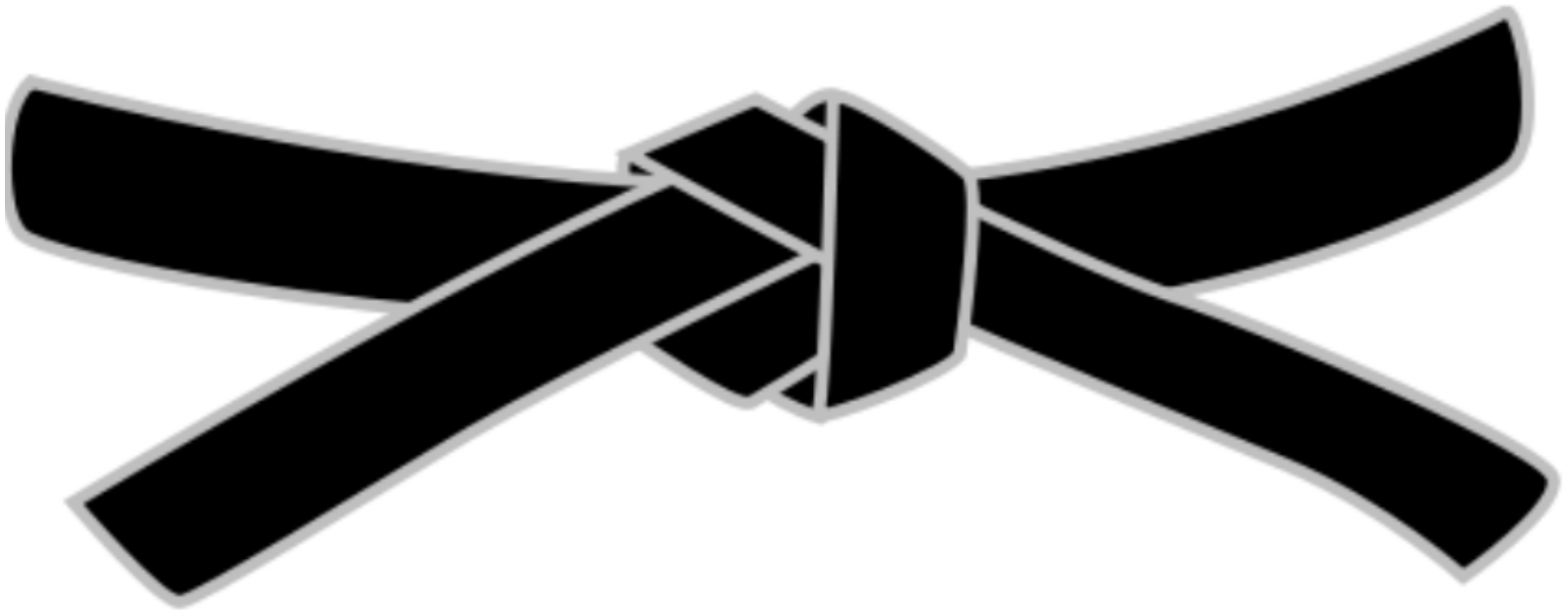
Raise your hands!



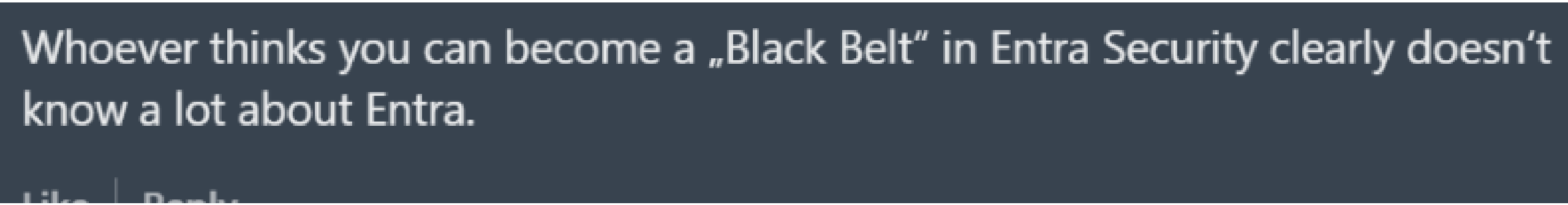
Raise your hands!



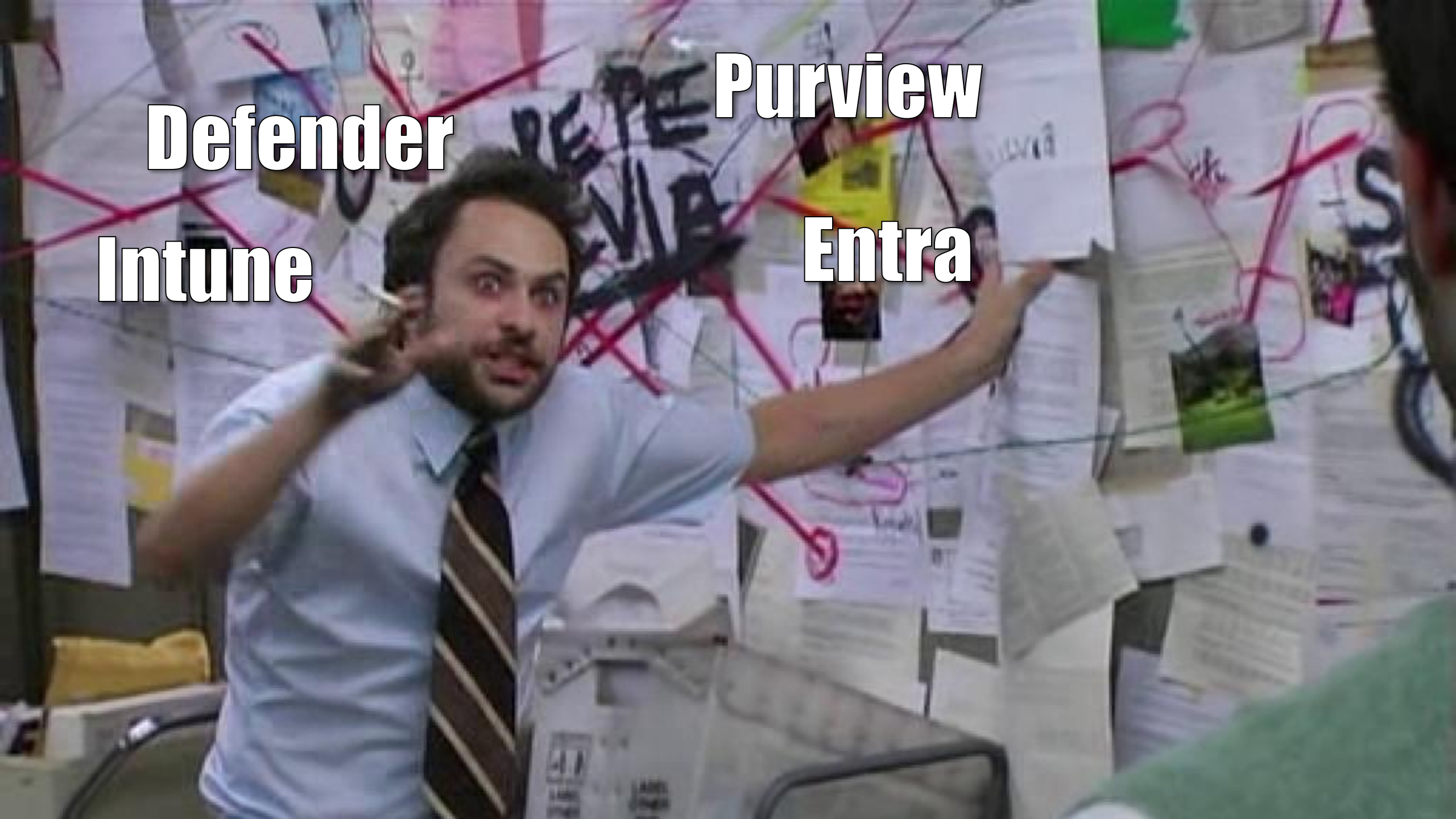
Raise your hands!



Yes, this is clickbait.




Defender
Intune
Entra
Purview


Defender
Purview
Intune
Entra

Entra

- **Admin self service password reset**

Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Learn & support

Password reset | Administrator Policy

Diagnose and solve problems

Manage

Properties
Authentication methods
Registration
Notifications
Customization
On-premises integration
Administrator Policy

Activity

Audit logs
Usage & insights

Troubleshooting + Support

New support request

Is self-service password reset enabled?

Yes

Number of methods required to reset:

2

Methods available to administrators:

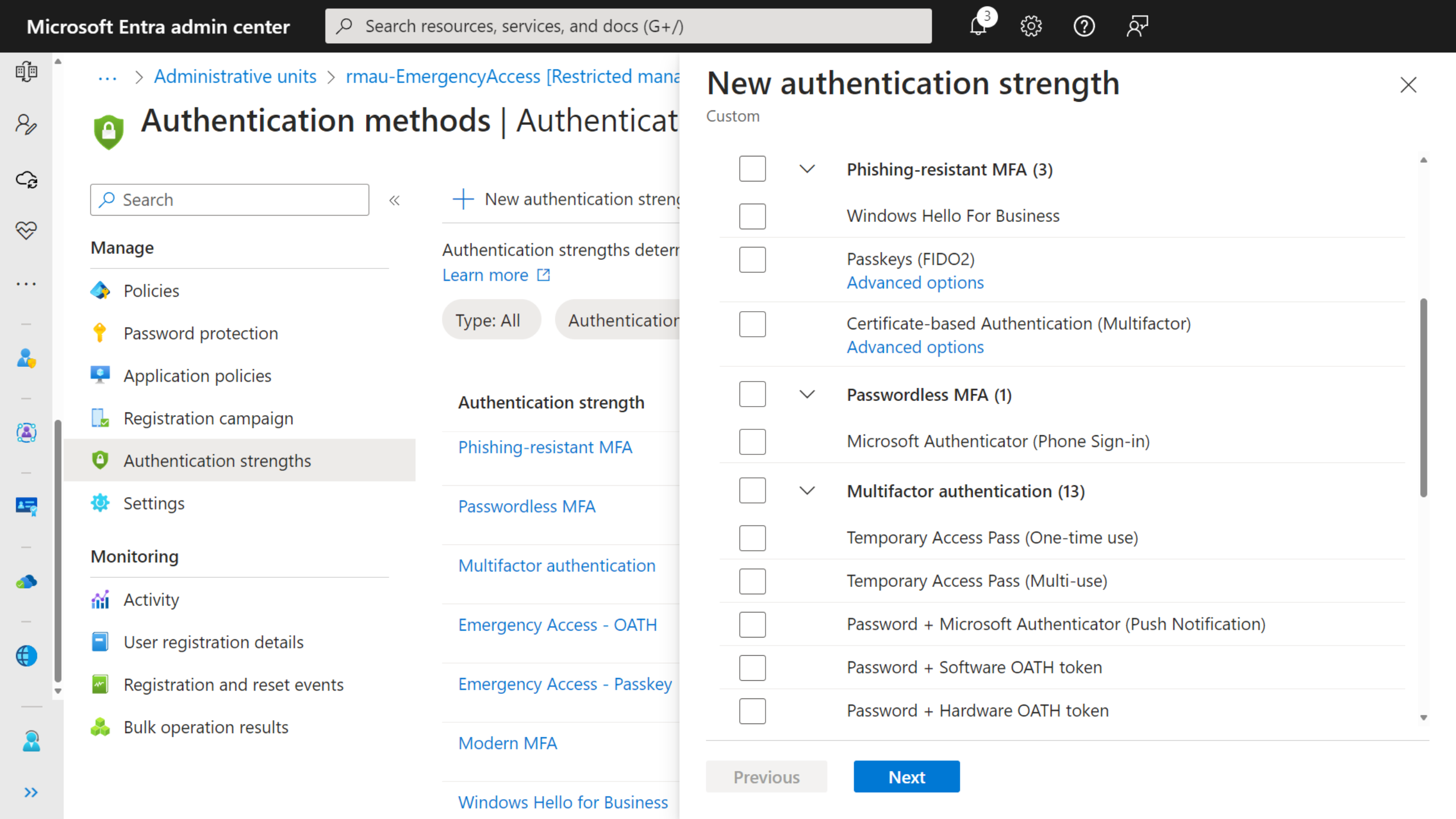
Email
Mobile phone (SMS only)
Mobile phone
Office phone
Mobile app code
Mobile app notification

Click here to learn more about administrator password policies.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\RuairidhCampbell> Import-Module Microsoft.Graph.Identity.SignIns
PS C:\Users\RuairidhCampbell> Connect-MgGraph -Scopes Policy.ReadWrite.Authorization
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Users\RuairidhCampbell> $params = @{
>> allowedToUseSSPR = $false
>> }
PS C:\Users\RuairidhCampbell> Update-MgPolicyAuthorizationPolicy -BodyParameter $params

ResponseHeaders
---------------
{b7fa8a7c-a2f6-4326-a3ea-50aeb775d772}


PS C:\Users\RuairidhCampbell> Get-MgPolicyAuthorizationPolicy | select AllowedToUseSspr

AllowedToUseSspr
----------------
           False
```

Entra

- Admin self service password reset
- **Authentication strengths but better**


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Administrative units > rmau-EmergencyAccess [Restricted mana
Authentication methods | Authenticat
Search
Manage
Policies
Password protection
Application policies
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
New authentication streng
Authentication strengths deter
Learn more
Type: All
Authentication
Authentication strength
Phishing-resistant MFA
Passwordless MFA
Multifactor authentication
Emergency Access - OATH
Emergency Access - Passkey
Modern MFA
Windows Hello for Business
New authentication strength
Custom
Phishing-resistant MFA (3)
Windows Hello For Business
Passkeys (FIDO2)
Advanced options
Certificate-based Authentication (Multifactor)
Advanced options
Passwordless MFA (1)
Microsoft Authenticator (Phone Sign-in)
Multifactor authentication (13)
Temporary Access Pass (One-time use)
Temporary Access Pass (Multi-use)
Password + Microsoft Authenticator (Push Notification)
Password + Software OATH token
Password + Hardware OATH token
Previous
Next

Add-PasskeyUsersToGroup.ps1

scripts > Add-PasskeyUsersToGroup.ps1 > ...

```powershell
<#
.SYNOPSIS
    Adds users with registered passkeys (FIDO2) to an Entra group.

.DESCRIPTION
    Queries all enabled member users in the tenant, checks if they have a FIDO2/passkey
    authentication method registered, and adds qualifying users to the specified group.
    Dry-run by default; use -Apply to make changes.

.PARAMETER GroupId
    The target Entra group ID (GUID) or display name.-

.PARAMETER Apply
    Apply changes. Without this switch, the script runs in dry-run mode.

.PARAMETER TenantId
    Optional tenant ID. Defaults to threatscape.onmicrosoft.com
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS AZURE

```
PS C:\Dev> .\scripts\Add-PasskeyUsersToGroup.ps1 -GroupId "63f463ad-53fa-4113-b20e-91f69ba16fea"
Fetching current group members...
  Current members: 10
Fetching current group members...
  Current members: 10
Fetching enabled member users...
  Users to scan: 73
Scanning for passkey authentication methods...
```

Entra

- Admin self service password reset
- Authentication strengths but better
- **Filters vs. platforms**

104-Admins-AllApps-UnsupportedPlatforms-Block

Conditional Access policy

Delete | View policy information

Network NEW
Not configured

Conditions
1 condition selected

Access controls

Grant
Block access

Session
0 controls selected

related activity in Microsoft Purview Insider Risk Management.
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps
Not configured

Filter for devices
Exclude filtered devices

Enable policy
Report-only | On | Off

Save

Device platforms

Configure
Yes | No

Include | Exclude

- Any device
- Select device platforms
  - Android
  - iOS
  - Windows Phone
  - Windows
  - macOS
  - Linux

Done

What is my User Agent?

Enter a user-agent string

```
Mozilla/5.0 (SMART-TV; Linux; Tizen 4.0) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/2.1
Chrome/56.0.2924.0 TV Safari/537.36
```

Method [normal] navigator.userAgent

Go!

navigator | ua-parser.js | platform.js

user-agent according to ua-parser-js v0.7.19

Mozilla/5.0 (SMART-TV; Linux; Tizen 4.0) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/2.1 Chrome/56.0.2924.0 TV Safari/537.36

BROWSER

- Name: Samsung Browser
- Version: 2.1
- Major: 2

ENGINE

- Name: WebKit
- Version: 537.36

OS

- Name: Tizen
- Version: 4.0

DEVICE

- Model: -
- Vendor: Samsung
- Type: smarttv

CPU

- Architecture: -

104-Admins-AllA

Conditional Access policy

Delete View policy

Network NEW

Not configured

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

Report-only On

Save

Filter for devices

Configure a filter to apply policy to specific devices. Learn more

Configure

Yes No

Devices matching the rule:

- ○ Include filtered devices in policy
- ◉ Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
	operatingSystem	Contains	Windows

+ Add expression

Rule syntax

Edit

```
device.operatingSystem -contains "Windows"
```

Done

PC-AP-467477 | Properties

Manage

- Properties
- Roles and administrators
- Administrative Units
- BitLocker keys (Preview)
- Local administrator password recovery

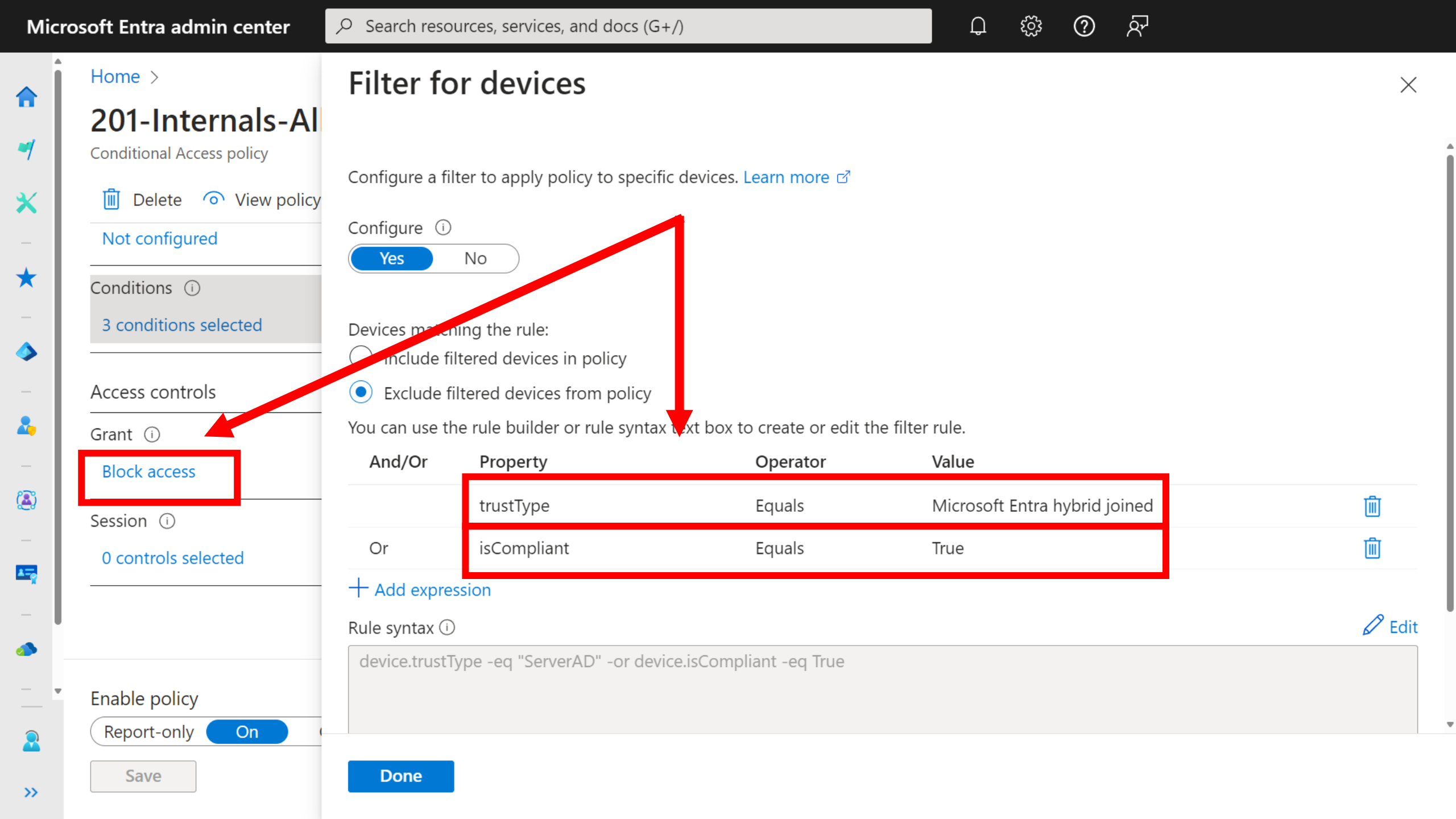
Enable | Disable | Delete | Manage | Got feedback?

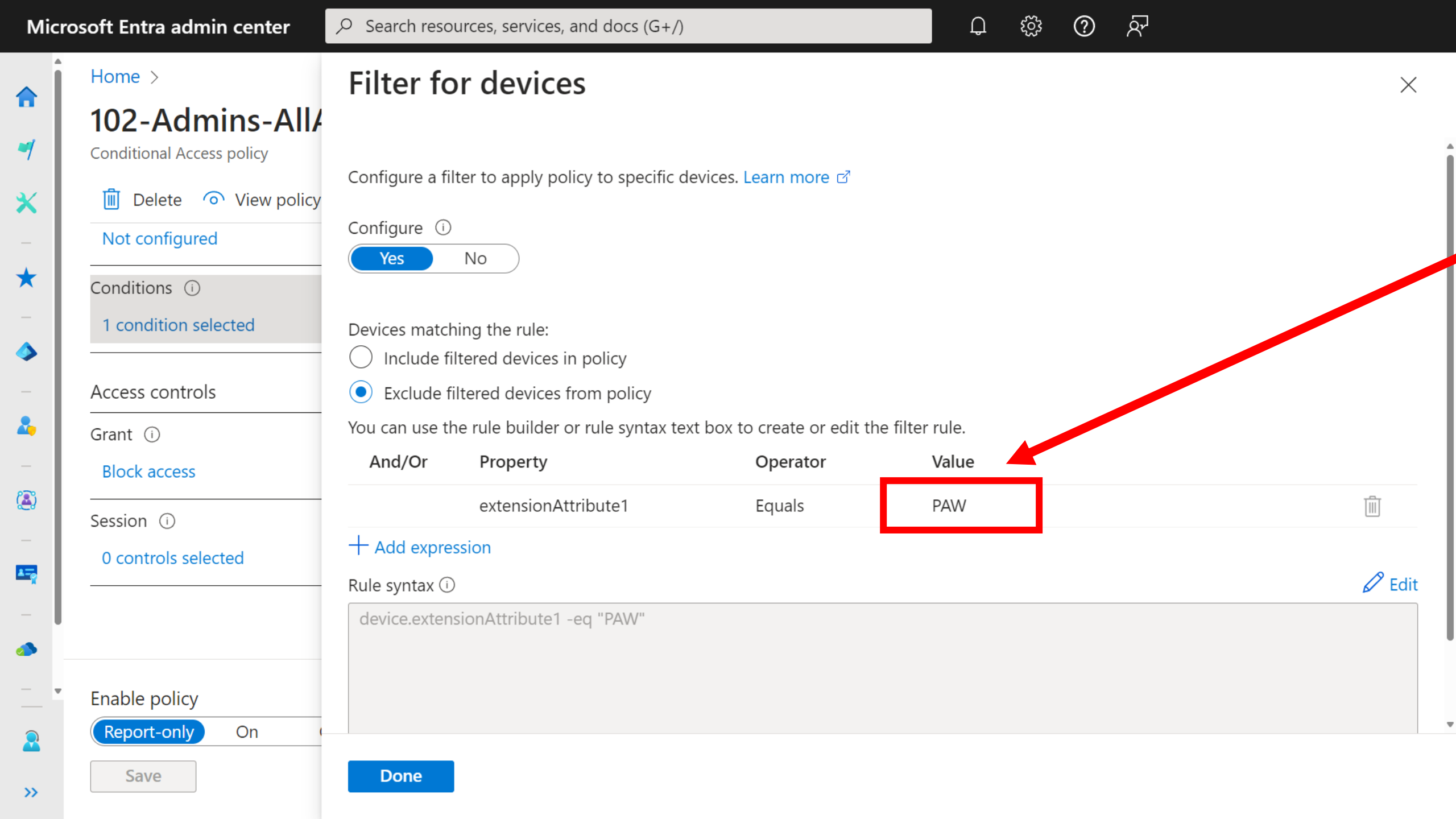
This device is a Windows Autopilot device. Devices deployed with Windows Autopilot cannot be deleted in the Microsoft Entra admin center. Learn more about managing Windows Autopilot devices.

Enabled	Yes
OS	Windows
Version	10.0.22631.3155
Join type	Microsoft Entra joined
Owner	(User) Ru Campbell
User principal name	
MDM	Microsoft Intune
Compliant	No
Registered	
Activity	

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- **Privileged access tiering**


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
201-Internals-Al
Conditional Access policy
Delete
View policy
Not configured
Conditions
3 conditions selected
Access controls
Grant
Block access
Session
0 controls selected
Enable policy
Report-only
On
Save
Filter for devices
Configure a filter to apply policy to specific devices. Learn more
Configure
Yes
No
Devices matching the rule:
Include filtered devices in policy
Exclude filtered devices from policy
You can use the rule builder or rule syntax text box to create or edit the filter rule.
And/Or
Property
Operator
Value
trustType
Equals
Microsoft Entra hybrid joined
Or
isCompliant
Equals
True
Add expression
Rule syntax
Edit
device.trustType -eq "ServerAD" -or device.isCompliant -eq True
Done


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
102-Admins-AllA
Conditional Access policy
Delete
View policy
Not configured
Conditions
1 condition selected
Access controls
Grant
Block access
Session
0 controls selected
Enable policy
Report-only
On
Save
Filter for devices
Configure a filter to apply policy to specific devices. Learn more
Configure
Yes
No
Devices matching the rule:
Include filtered devices in policy
Exclude filtered devices from policy
You can use the rule builder or rule syntax text box to create or edit the filter rule.
And/Or
Property
Operator
Value
extensionAttribute1
Equals
PAW
Add expression
Rule syntax
Edit
device.extensionAttribute1 -eq "PAW"
Done

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- **Hidden apps**

Home
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Learn & support

New

Conditional Access policy

Name *

Example: 'Device compliance app policy'

Assignments

Users

0 users and groups selected

Target resources

No target resources selected

"Select apps" must be configured

Network NEW

Not configured

Conditions

0 conditions selected

Enable policy

Report-only | On | Off

Create

Cloud ap

Include

Nor

All c

Sele

Edit filter

None

Select

None

Select

Cloud apps

Microsoft Exchange REST API Based Powershell

No results.

Selected items

Select

Applications
Enterprise applications
App registrations
Roles & admins
Billing
Settings
Protection
Identity Protection
Conditional Access
Security Center
Identity Secure Score
Multifactor authentication
Learn & support

Enterprise applications | All applications

Threatscape

Overview
Overview
Diagnose and solve problems
Manage
All applications
Private Network connectors
User settings
App launchers
Custom authentication extensions
Security
Conditional Access
Consent and permissions
Activity

New application | Refresh | Download (Export)

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

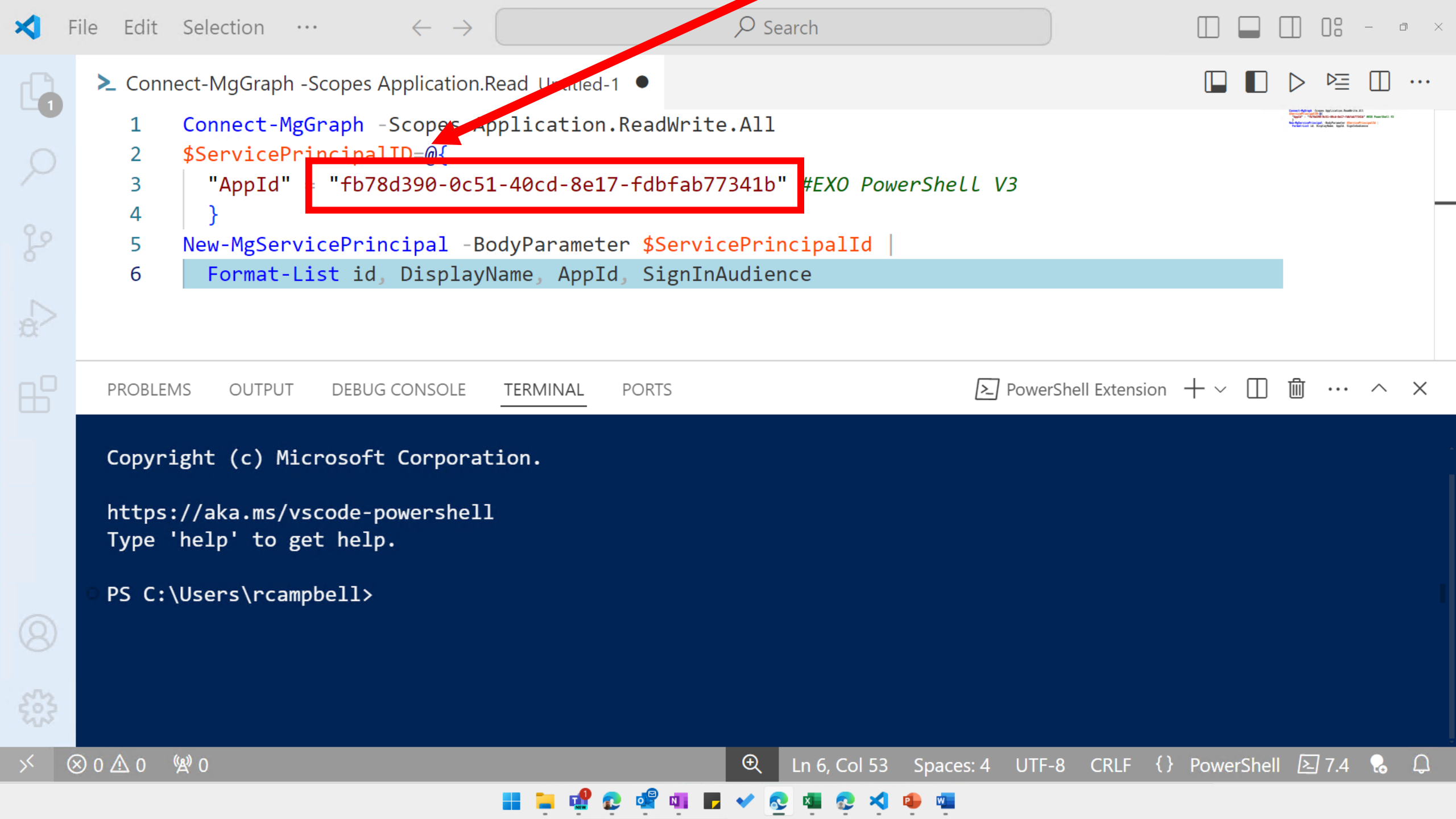
The list of applications that are maintained by your organization are in application registrations.

Microsoft Exchange REST API Based Powe...

Application ID starts with | Add filters

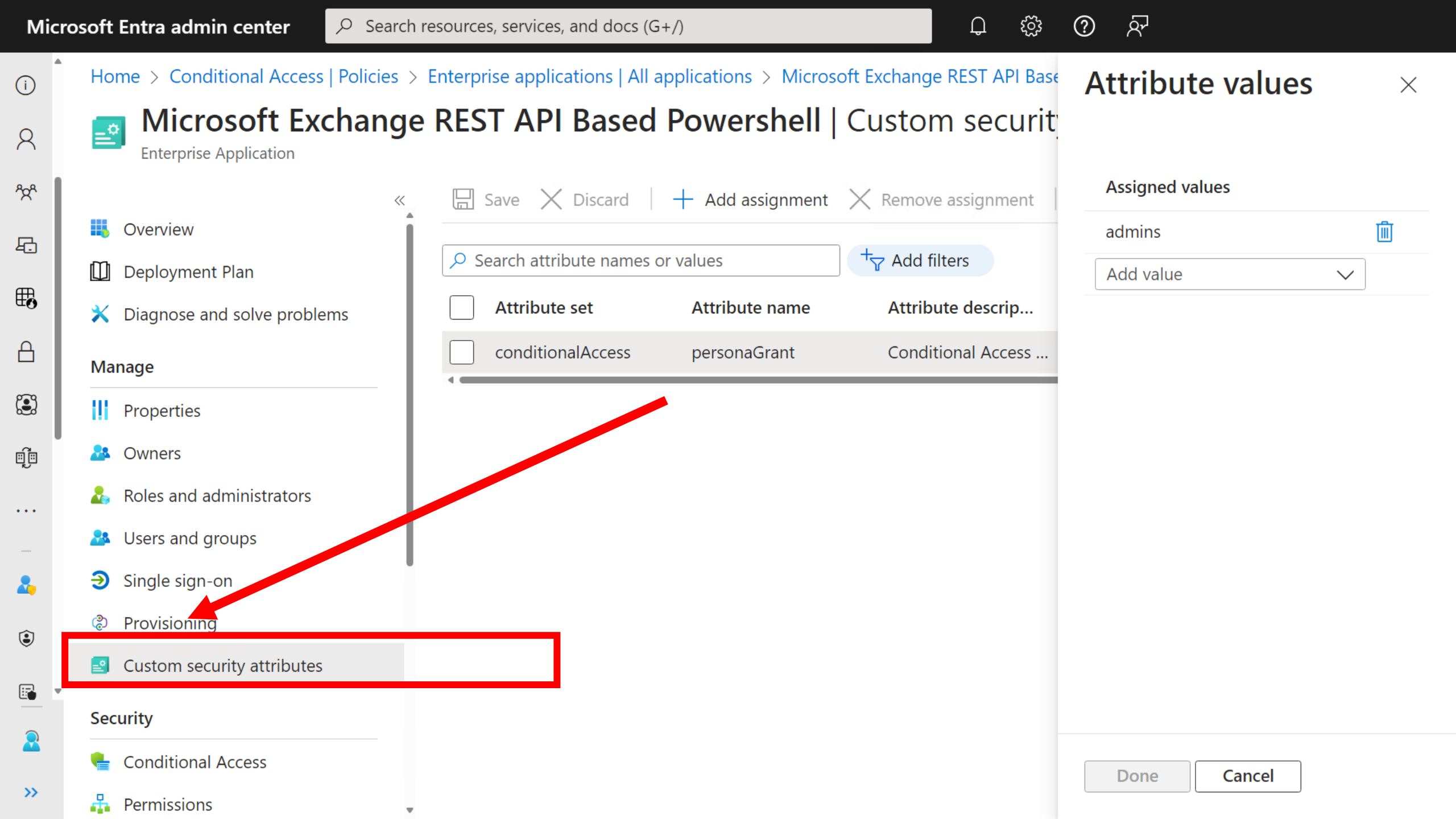
0 applications found

Name	Object ID	Applic
No results		


File
Edit
Selection
Search
Connect-MgGraph -Scopes Application.Read
1 Connect-MgGraph -Scopes Application.ReadWrite.All
2 $ServicePrincipalID=@{
3 "AppId" = "fb78d390-0c51-40cd-8e17-fdbfab77341b" #EXO PowerShell V3
4 }
5 New-MgServicePrincipal -BodyParameter $ServicePrincipalId |
6 Format-List id, DisplayName, AppId, SignInAudience
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
PowerShell Extension
Copyright (c) Microsoft Corporation.
https://aka.ms/vscode-powershell
Type 'help' to get help.
PS C:\Users\rcampbell>
Ln 6, Col 53
Spaces: 4
UTF-8
CRLF
PowerShell
7.4

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- **Custom security attributes**


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home > Conditional Access | Policies > Enterprise applications | All applications > Microsoft Exchange REST API Base
Microsoft Exchange REST API Based Powershell | Custom securit
Enterprise Application
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Custom security attributes
Security
Conditional Access
Permissions
Save
Discard
Add assignment
Remove assignment
Search attribute names or values
Add filters
Attribute set
Attribute name
Attribute descrip...
conditionalAccess
personaGrant
Conditional Access ...
Attribute values
Assigned values
admins
Add value
Done
Cancel

Edit filter

Configure
Yes No

Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview, only attributes of type String are supported. Attributes of type Integer or Boolean will not be shown. Learn more

And/Or	Attribute	Operator	Value
	conditionalAccess_personaGrant	Contains	admins

Add expression

Rule syntax

Edit

```
CustomSecurityAttribute.conditionalAccess_personaGrant -contains "admins"
```

Done

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- **Conditional Access allow listing**

204-Internals-AllAppsExBYODSanctioned-Unmanaged-Block

Conditional Access policy

Delete | View policy information

204-Internals-AllAppsExBYODSanctioned-U...

Assignments

Users

Specific users included and specific users excluded

Target resources

All cloud apps included and 6 apps excluded

Network NEW

Not configured

Conditions

1 condition selected

Include | Exclude

Select the cloud apps to exempt from the policy

Edit filter

Configured

Select excluded cloud apps

Windows Store for Business and 5 more

Office 365

Enable policy

Report-only | On | Off

Save

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- **Sign-in frequency**

019-Global-RegisterSecurityInfo-SignInFrequencyEveryTime

Conditional Access policy

Delete View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more

Name *
019-Global-RegisterSecurityInfo-SignInFreq...

Assignments

Users
Specific users included and specific users excluded

Target resources
1 user action included

Enable policy
Report-only On Off

Save

Session

Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more

- [ ] Use Conditional Access App Control
- [x] Sign-in frequency
  - ( ) Periodic reauthentication
  - (•) Every time
- [ ] Persistent browser session
- [ ] Customize continuous access evaluation
- [ ] Disable resilience defaults
- [ ] Require token protection for sign-in sessions (Preview)
- [ ] Use Global Secure Access security profile

Select

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- Sign-in frequency
- **Authentication contexts**

Conditional Access | Authentication contexts

Microsoft Entra ID

Overview
Policies
Insights and reporting
Diagnose and solve problems

Manage

Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies

Monitoring

Sign-in logs

New authentication context | Refresh | Got feedback?

Get started | Authentication contexts

Manage authentication context to protect data and actions in your apps. Authentication contexts cannot be deleted when they are referenced by Conditional Access policies. Learn more

Name	Description
Phishing-resistant MFA	Require any supported type of phishing-resistant MFA
Passkey (FIDO2)	Require a passkey (FIDO2) of any kind
Windows Hello for Business	Require Windows Hello for Business
Reauthentication	Require full reauthentication
Compliant device	Require a compliant device
Hybrid joined device	Require a hybrid Entra joined device
Compliant or hybrid device	Require a compliant or hybrid Entra joined device
Compliant and hybrid device	Require a compliant and hybrid Entra joined device
Privileged access workstation	Require a privileged access workstation (PAW) based on E...

055-Global-AuthContext-Compliant

Conditional Access policy

Delete | View policy information

excluded

Target resources
1 authentication context included

Network NEW
Not configured

Conditions
1 condition selected

Access controls

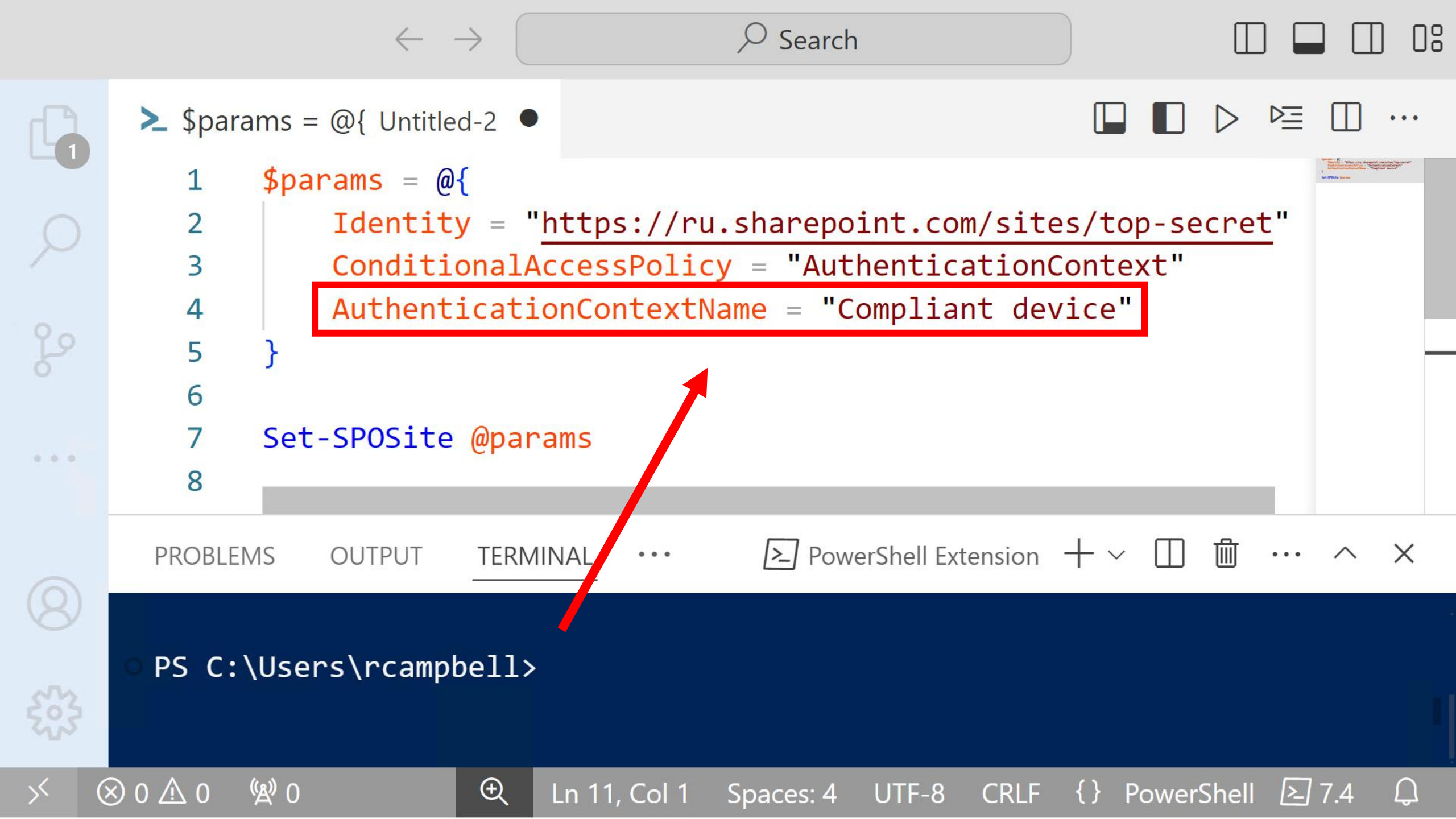
Grant
Block access

Select the authentication contexts this policy will apply to

- [ ] Phishing-resistant MFA
- [ ] Passkey (FIDO2)
- [ ] Windows Hello for Business
- [ ] Reauthentication
- [x] Compliant device
- [ ] Hybrid joined device
- [ ] Compliant or hybrid device
- [ ] Compliant and hybrid device
- [ ] Privileged access workstation

Enable policy
Report-only | On | Off

Save


Search
$params = @{ Untitled-2
1 $params = @{
2 Identity = "https://ru.sharepoint.com/sites/top-secret"
3 ConditionalAccessPolicy = "AuthenticationContext"
4 AuthenticationContextName = "Compliant device"
5 }
6
7 Set-SPOSite @params
8
PROBLEMS
OUTPUT
TERMINAL
PowerShell Extension
PS C:\Users\rcampbell>
0 0 0
Ln 11, Col 1
Spaces: 4
UTF-8
CRLF
{} PowerShell
7.4

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- Sign-in frequency
- Authentication contexts

- **PIM is not a security boundary (sometimes)**

Password reset
Custom security attributes
Risky activities
Show more
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verified ID
Learn & support

Edit role setting - Global Administrator

Privileged Identity Management | Microsoft Entra roles

Activation | Assignment | Notification

Activation maximum duration (hours)

10

On activation, require

- None
- Azure MFA
- Microsoft Entra Conditional Access authentication context

Learn more

- [x] Require justification on activation
- [ ] Require ticket information on activation
- [ ] Require approval to activate

Update | Next: Assignment

Password reset
Custom security attributes
Risky activities
Show more
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verified ID
Learn & support

Edit role setting - Global Administrator

Privileged Identity Management | Microsoft Entra roles

Activation | Assignment | Notification

Activation maximum duration (hours)

10

On activation, require

- None
- Azure MFA
- Microsoft Entra Conditional Access authentication context

Learn more

- [x] Require justification on activation
- [ ] Require ticket information on activation
- [x] Require approval to activate

Update | Next: Assignment

Password reset
Custom security attributes
Risky activities
Show more
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verified ID
Learn & support

Edit role setting - Global Administrator

Privileged Identity Management | Microsoft Entra roles

Activation | Assignment | Notification

Activation maximum duration (hours)

10

On activation, require

- None
- Azure MFA
- Microsoft Entra Conditional Access authentication context

Learn more

Reauthentication

Require full reauthentication

Require justification on activation

Update | Next: Assignment

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- Sign-in frequency
- Authentication contexts
- PIM is not a security boundary (sometimes)
- **Cross-tenant access settings**

Applications
Protection
Identity governance
External Identities
Overview
All identity providers
User flows
Custom authentication extensions
Cross-tenant access settings
External collaboration settings
Cross-tenant synchronization
Show more
Learn & support

Inbound access settings - Default settings

...

B2B collaboration | B2B direct connect | Trust settings

Configure whether your Conditional Access policies will accept claims from other Microsoft Entra tenants when external users access your resources. The default settings apply to all external Microsoft Entra tenants except those with organization-specific settings.

You'll first need to configure Conditional Access for guest users on all cloud apps if you want to require multifactor authentication or require a device to be compliant or Microsoft Entra hybrid joined.
Learn more

- [ ] Trust multifactor authentication from Microsoft Entra tenants
- [ ] Trust compliant devices
- [ ] Trust Microsoft Entra hybrid joined devices

Save | Discard

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- Sign-in frequency
- Authentication contexts
- PIM is not a security boundary (sometimes)
- Cross-tenant access settings
- **App assignment requirements**

Overview
Users
All users
Deleted users
User settings
Groups
Devices
Applications
Enterprise applications
App registrations
Protection
Identity governance
Learn & support

Microsoft Graph Command Line Tools | Properties

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes

Security

Conditional Access

Save | Discard | Delete | Got feedback?

Enabled for users to sign-in? Yes / No

Name: Microsoft Graph Command Line Tools

Homepage URL: https://docs.microsoft.com/en-us/gr...

Logo

Application ID: 14d82eec-204b-4c2f-b7e8-296a70d...

Object ID: fded749e-7978-4ab8-b08c-42ebce1...

Assignment required? Yes / No

Visible to users? Yes / No

Notes

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- Sign-in frequency
- Authentication contexts
- PIM is not a security boundary (sometimes)
- Cross-tenant access settings
- App assignment requirements
- **RBAC for Applications**

Random enterprise app | Permissions

Enterprise Application

Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes

Security

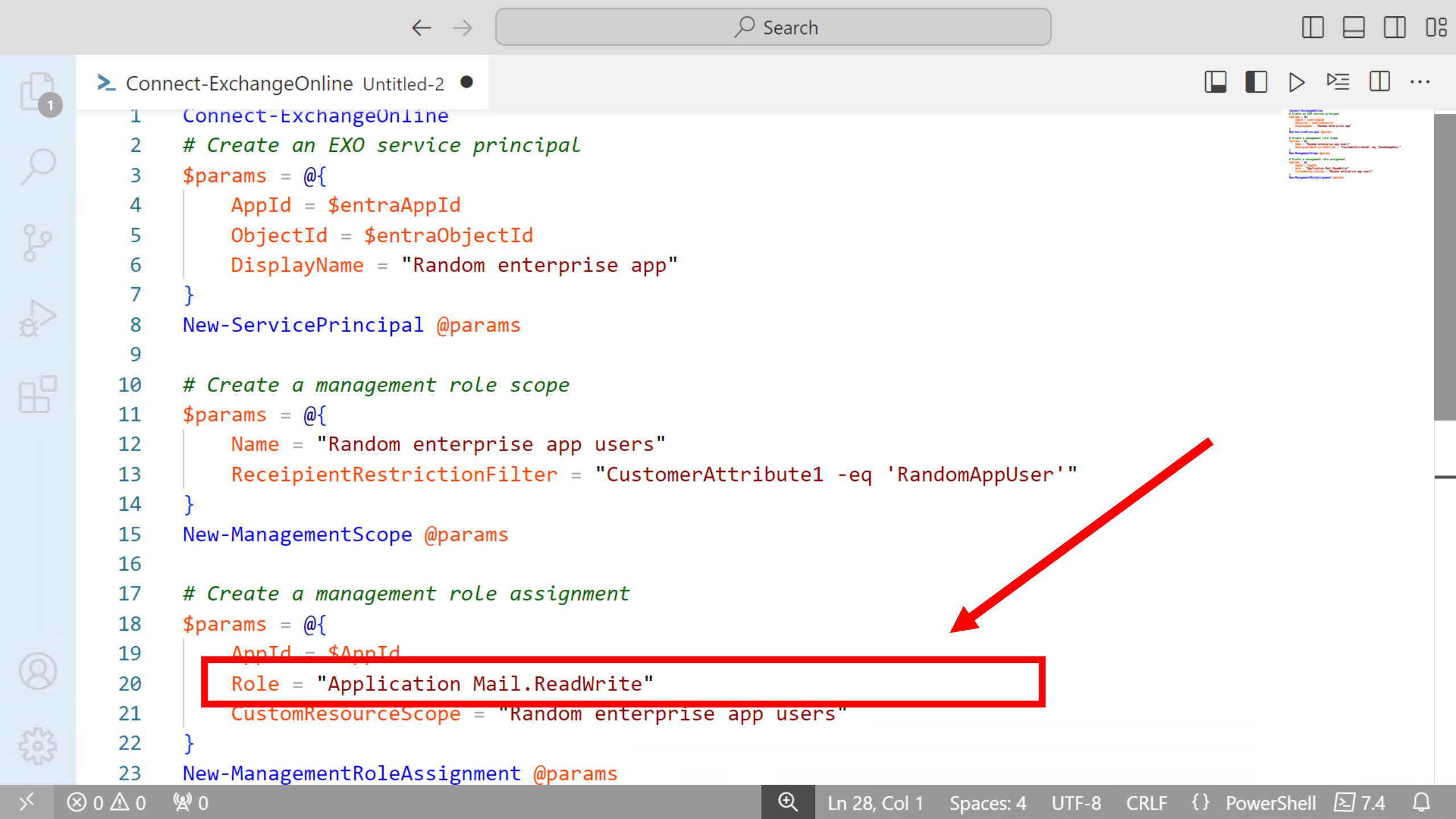
Conditional Access
Permissions
Token encryption

Activity

Sign-in logs
Usage & insights
Audit logs
Provisioning logs

Refresh | Review permissions | Got feedback?

Microsoft Graph	Mail.ReadWrite	Read and write mail in all ...	Application	Admin consent
Microsoft Graph	User.ReadWrite.All	Read and write all users' fu...	Application	Admin consent
Microsoft Graph	Group.Read.All	Read all groups	Application	Admin consent
Microsoft Graph	Directory.ReadWrite.All	Read and write directory d...	Application	Admin consent
Microsoft Graph	Contacts.ReadWrite	Read and write contacts in ...	Application	Admin consent
Microsoft Graph	Group.ReadWrite.All	Read and write all groups	Application	Admin consent
Microsoft Graph	Files.ReadWrite.All	Read and write files in all si...	Application	Admin consent
Microsoft Graph	User.Read.All	Read all users' full profiles	Application	Admin consent
Microsoft Graph	Calendars.ReadWrite	Read and write calendars i...	Application	Admin consent
Microsoft Graph	MailboxSettings.Read...	Read and write all user mai...	Application	Admin consent
Microsoft Graph	Sites.FullControl.All	Have full control of all site ...	Application	Admin consent
Microsoft Graph	Notes.ReadWrite.All	Read and write all OneNot...	Application	Admin consent
Office 365 Exchange Online				
Office 365 Exchange O...	full_access_as_app	Use Exchange Web Service...	Application	Admin consent


Search
Connect-ExchangeOnline Untitled-2
Connect-ExchangeOnline
# Create an EXO service principal
$params = @{
AppId = $entraAppId
ObjectId = $entraObjectId
DisplayName = "Random enterprise app"
}
New-ServicePrincipal @params
# Create a management role scope
$params = @{
Name = "Random enterprise app users"
ReceipientRestrictionFilter = "CustomerAttribute1 -eq 'RandomAppUser'"
}
New-ManagementScope @params
# Create a management role assignment
$params = @{
AppId = $AppId
Role = "Application Mail.ReadWrite"
CustomResourceScope = "Random enterprise app users"
}
New-ManagementRoleAssignment @params
Ln 28, Col 1
Spaces: 4
UTF-8
CRLF
PowerShell
7.4

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- Sign-in frequency
- Authentication contexts
- PIM is not a security boundary (sometimes)
- Cross-tenant access settings
- App assignment requirements
- RBAC for Applications
- **AppTotal**

OVERVIEW

Microsoft Graph Co...

https://learn.microso...

APPTOTAL VERIFIED

VERIFIED

DESCRIPTION

Microsoft Graph is the gateway to data and intelligence in Microsoft 365. It provides a unified programmability model that you can use to access the tremendous amount of data in Microsoft 365, Windows 10, and Enterprise Mobility + Security.

PUBLISHER	TAGS	CATEGORY	PLATFORM VERIFIED	TYPE	APP ID
Microsoft	Application, OAuth, Enterprise App, 1st Party	IT/Admin	No Data	Data	14d82eec-204b-4c2f-b7e8...

SUMMARY

APP RISK

PERMISSION

RISKS

Want to

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- Sign-in frequency
- Authentication contexts
- PIM is not a security boundary (sometimes)
- Cross-tenant access settings
- App assignment requirements
- RBAC for Applications
- AppTotal
- **Application authentication policies**

Enterprise applications | Application policies

Campbell

Overview
Overview
Diagnose and solve problems
Manage
All applications
Private Network connectors
User settings
App launchers
Custom authentication extensions
Security
Conditional Access
Consent and permissions
Application policies
Activity
Sign-in logs
Usage & insights

Refresh | Got feedback?

Define app management policies for your organization. Use these policies to reduce security risk caused by insecure app configurations. Learn more

Policy name	Description
Password restrictions	
Block password addition	Block the addition of new passwords
Restrict max password lifetime	Restrict the max lifetime of newly added passwords
Block custom passwords	Block passwords that are not system-generated
Certificate restrictions	
Restrict max certificate lifetime	Restrict the max lifetime of newly added certificates
Identifier URI restrictions	
Block custom identifier URIs	Block the addition of new custom identifier URIs
Block identifier URIs without unique tenant identifiers	Block the addition of identifier URIs not containing a unique tenant identifier

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- Sign-in frequency
- Authentication contexts
- PIM is not a security boundary (sometimes)
- Cross-tenant access settings
- App assignment requirements
- RBAC for Applications
- AppTotal
- Application authentication policies
- **Application ownership**

microsoft.directory/servicePrincipals/basic/update	Update basic properties on servic principals in Microsoft Entra ID.
microsoft.directory/servicePrincipals/credentials/update	Update the `servicePrincipals.credentials` property in Microsoft Entra ID.
microsoft.directory/servicePrincipals/delete	Delete service principals in Micros Entra ID.
microsoft.directory/servicePrincipals/owners/update	Update the `servicePrincipals.owners` proper in Microsoft Entra ID.
microsoft.directory/servicePrincipals/permissions/update	Update the `servicePrincipals.permissions` property in Microsoft Entra ID.
microsoft.directory/servicePrincipals/policies/update	Update the `servicePrincipals.policies` prop in Microsoft Entra ID.
microsoft.directory/signInReports/allProperties/read	Read all properties (including privileged properties) on sign-in reports in Microsoft Entra ID.
microsoft.directory/servicePrincipals/synchronizationCredentials/manage	Manage application provisioning secrets and credentials
microsoft.directory/servicePrincipals/synchronizationJobs/manage	Start, restart, and pause applicatic

In this article

Entra

- Admin self service password reset
- Authentication strengths but better
- Filters vs. platforms
- Privileged access tiering
- Hidden apps
- Custom security attributes
- Conditional Access allow listing
- Sign-in frequency
- Authentication contexts
- PIM is not a security boundary (sometimes)
- Cross-tenant access settings
- App assignment requirements
- RBAC for Applications
- AppTotal
- Application authentication policies
- Application ownership
- **Don’t accept the default app consent (usually)**

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Consent and permissions | User consent settings

Overview
Users
All users
Deleted use
User setting
Groups
Devices
Application
Enterprise a
App registr
Protection
Identity go
Learn & support

Save | Discard | Got feedback?

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

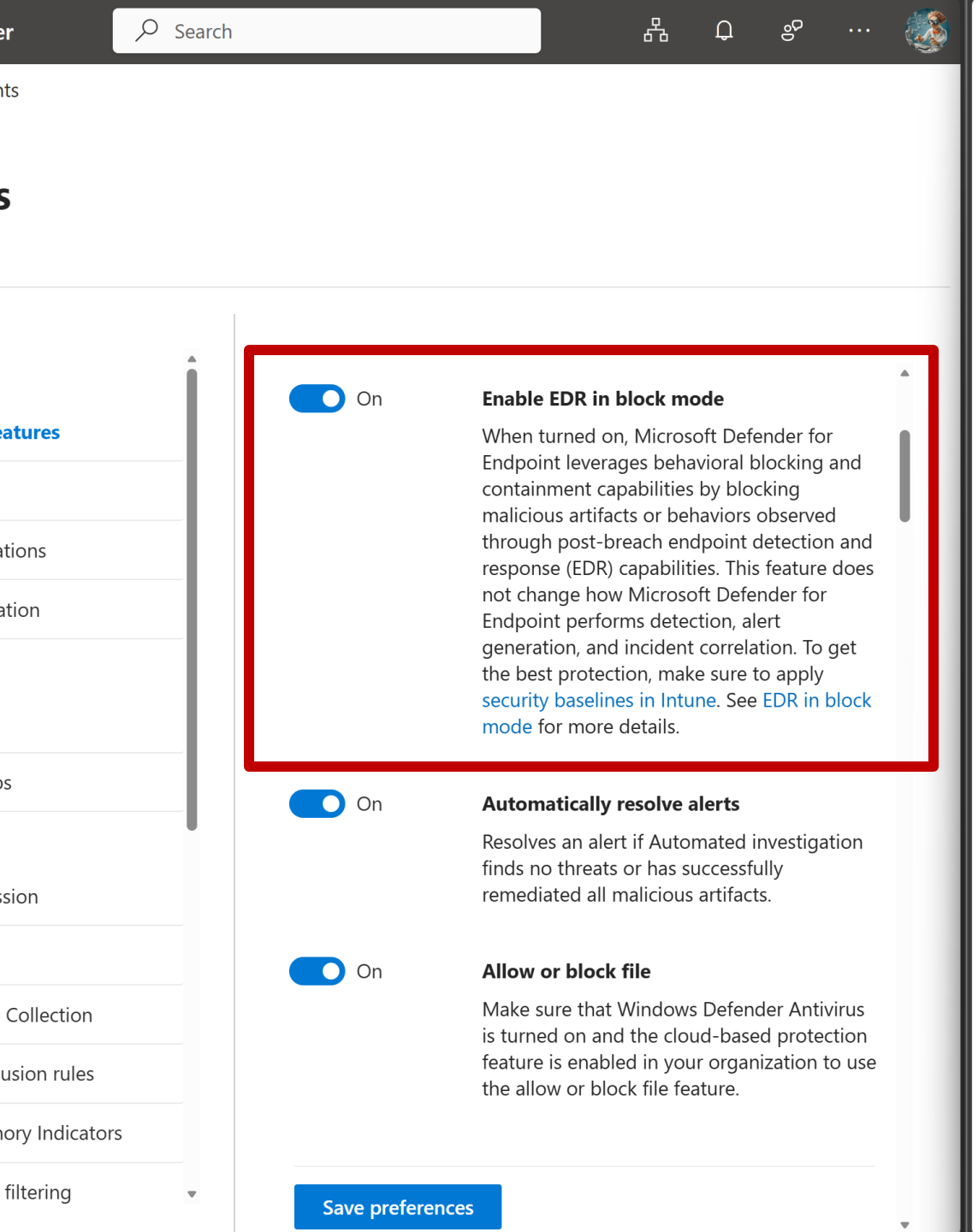
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- ○ Do not allow user consent
  An administrator will be required for all apps.
- ○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- ◉ Allow user consent for apps
  All users can consent for any app to access the organization's data.

⚠ With your current user settings, all users can allow applications to access your organization's data on their behalf. Learn more about the risks
Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". Learn

Defender

- **EDR in block mode**



Configuration/PassiveRemediation

Expand table

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 10, version 1607 [10.0.14393] and later

Device Copy

```
./Device/Vendor/MSFT/Defender/Configuration/PassiveRemediation
```

Setting to control automatic remediation for Sense scans.

Description framework properties:

Expand table

Property name	Property value
Format	`int`
Access Type	Add, Delete, Get, Replace
Default Value	0x0

Allowed values:

Expand table

Flag	Description
0x0 (Default)	Passive Remediation is turned off (default).
0x1	PASSIVE_REMEDIATION_FLAG_SENSE_AUTO_REMEDIATION: Passive Remediation Sense AutoRemediation.
0x2	PASSIVE_REMEDIATION_FLAG_RTP_AUDIT: Passive Remediation Realtime Protection Audit.
0x4	PASSIVE_REMEDIATION_FLAG_RTP_REMEDIATION: Passive Remediation Realtime

Defender

- EDR in block mode
- **Block at first sight**

MDAV - Level 3

Before Running Scan — Enabled

Cloud Block Level — Zero Tolerance

- Not configured
- Default State (Default)
- High
- High Plus
- Zero Tolerance

Cloud Extended Timeout

Days To Retain Cleaned Malware

Disable Catchup Full Scan

Disable Catchup Quick Scan — Disabled

Enable Low CPU Priority — Disabled (Default)

Enable Network Protection — Enabled (block mode)

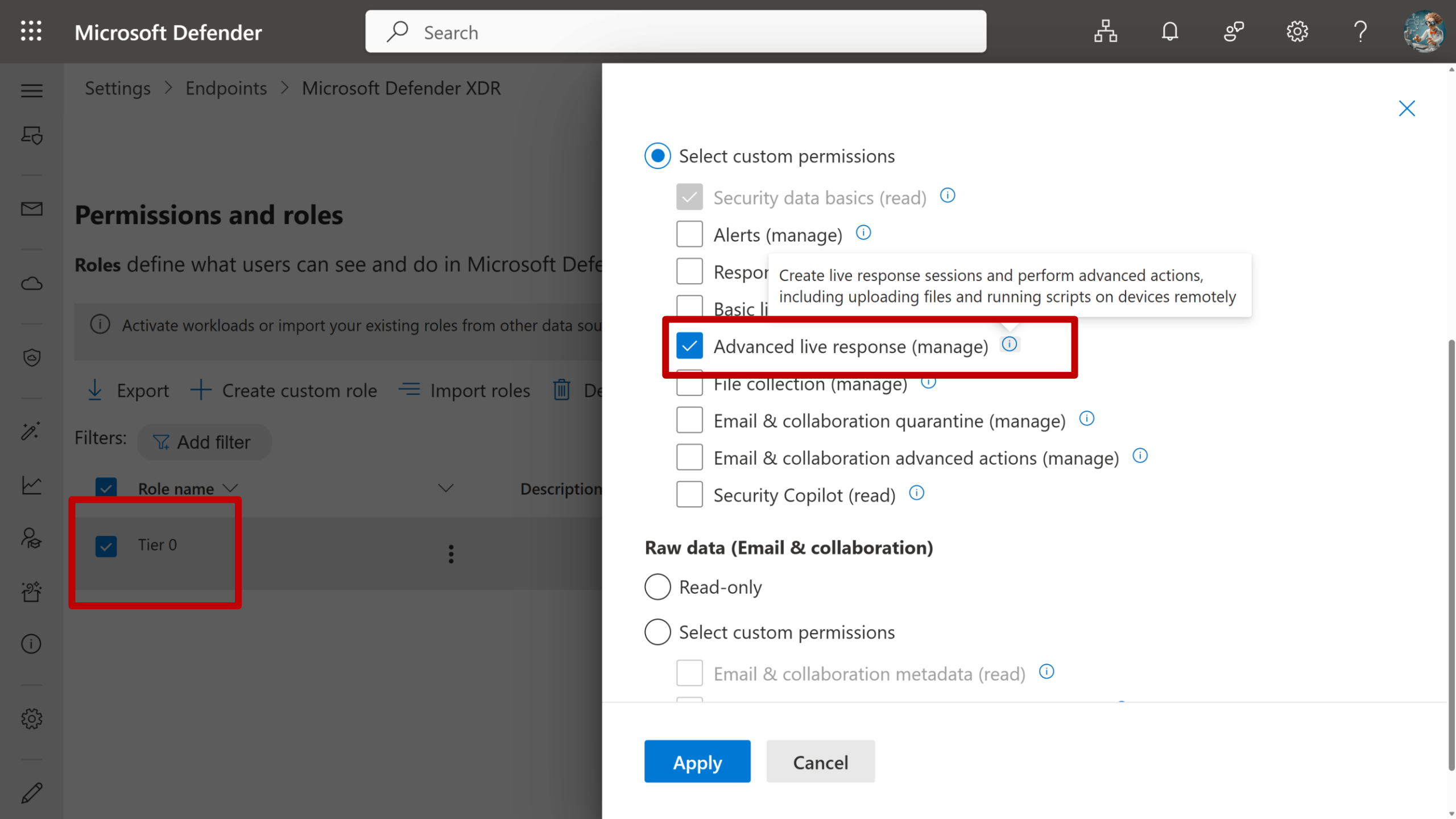
Excluded Extensions

Add | Remove | Import | Export

Excluded Extensions ↑

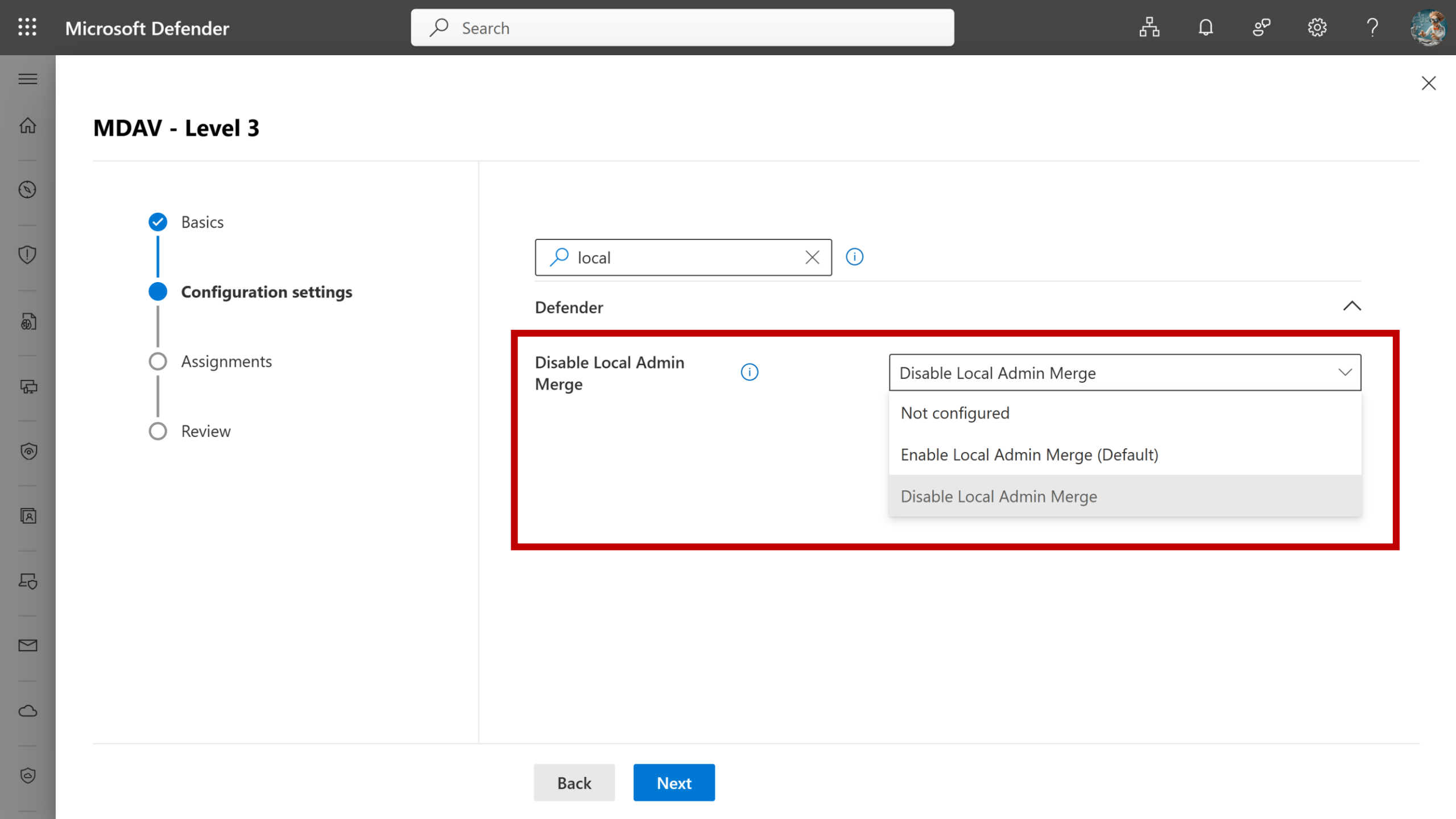
Defender

- EDR in block mode
- Block at first sight
- **Device groups = tiering**


Microsoft Defender
Search
Settings > Endpoints > Microsoft Defender XDR
Permissions and roles
Roles define what users can see and do in Microsoft Defe
Activate workloads or import your existing roles from other data sou
Export
Create custom role
Import roles
Filters:
Add filter
Role name
Description
Tier 0
Select custom permissions
Security data basics (read)
Alerts (manage)
Respor
Basic li
Create live response sessions and perform advanced actions, including uploading files and running scripts on devices remotely
Advanced live response (manage)
File collection (manage)
Email & collaboration quarantine (manage)
Email & collaboration advanced actions (manage)
Security Copilot (read)
Raw data (Email & collaboration)
Read-only
Select custom permissions
Email & collaboration metadata (read)
Apply
Cancel

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- **Tamper protection**


Microsoft Defender
Search
MDAV - Level 3
Basics
Configuration settings
Assignments
Review
local
Defender
Disable Local Admin Merge
Disable Local Admin Merge
Not configured
Enable Local Admin Merge (Default)
Disable Local Admin Merge
Back
Next

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- **Contextual exclusions**

Create a new policy

- Assignments
- Review + create

Excluded Extensions

Add | Remove | Import | Export

Excluded Extensions

Excluded Paths

Add | Remove | Import | Export

Excluded Paths

Excluded Processes

Add | Remove | Import | Export

Excluded Processes

C:\Users*\Documents\LargeDataSet.csv {Process:"C:\Program Files\PROLAB\bin\prolab.exe"}

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- **Additional auditing**

Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support

ALL - Improve MDE Telemetry

Device configuration profile

Summarize with Copilot Delete

Auditing

Account Logon Logoff Audit Logoff	Success+ Failure
Account Logon Logoff Audit Logon	Success+ Failure
Audit Authentication Policy Change	Success+Failure
Audit Authorization Policy Change	Success+Failure
Audit Other Logon Logoff Events	Success+Failure
Audit Security Group Management	Success+Failure
Audit Security System Extension	Success+Failure

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- Additional auditing
- **Performance mode**

0x4	PASSIVE_REMEDIATION_FLAG_RTP_REMEDIATION: Passive Remediation Realtime Protection Remediation.

Configuration/PerformanceModeStatus

Expand table

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 11, version 21H2 [10.0.22000] and later

Device Copy

```
./Device/Vendor/MSFT/Defender/Configuration/PerformanceModeStatus
```

This setting allows IT admins to configure performance mode in either enabled or disabled mode for managed devices.

Description framework properties:

Expand table

Property name	Property value
Format	`int`
Access Type	Add, Delete, Get, Replace
Default Value	0

Allowed values:

Expand table

Value	Description
0 (Default)	Performance mode is enabled (default).
1	Performance mode is disabled.

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- Additional auditing
- Performance mode
- **Update rings + sources**

MDAV Update Channels

Beta Channel	Engine + Platform		Testing
Current Channel (Preview)			Pre-production
Current Channel (Staged)		SIU	Later in gradual release
Current Channel (Broad)			After gradual release
Default			Managed by Microsoft
Critical: Time Delay			48 hour delay

Windows policies | macOS policies | Linux policies

Create new policy | Export | Search | Customize columns | Filter

Policy Name	Policy Type	Policy category	Assigned	Platform	Target	Last modified
BAFS	Microsoft Defender...	Antivirus	true	windows10	mdm,microsoftSense	10 Jun 2024 10:17
LKL - Device control	Device Control	Attack surfac...	true	windows10	mdm,microsoftSense	22 May 2024 06:39
MDAV - Level 1	Microsoft Defender...	Antivirus	false	windows10	mdm,microsoftSense	20 Aug 2025 13:24
MDAV - Level 2	Microsoft Defender...	Antivirus	false	windows10	mdm,microsoftSense	20 Aug 2025 13:24
MDAV - Level 3	Microsoft Defender...	Antivirus	false	windows10	mdm,microsoftSense	20 Aug 2025 13:25
MDAV Updates - Ring 1	Defender Update c...	Antivirus	false	windows10	mdm,microsoftSense	14 Jul 2025 11:12
MDAV Updates - Ring 2	Defender Update c...	Antivirus	false	windows10	mdm,microsoftSense	14 Jul 2025 11:13
MDAV Updates - Ring 3	Defender Update c...	Antivirus	false	windows10	mdm,microsoftSense	14 Jul 2025 11:14
MDE Onboarding	Endpoint detection...	Endpoint det...	true	windows10	mdm,microsoftSense	9 May 2024 06:37

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- Additional auditing
- Performance mode
- Update rings + sources
- **File hash computation**

Configuration/EnableFileHashComputation

Expand table

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 10, version 1903 [10.0.18362] and later

Device Copy

```
./Device/Vendor/MSFT/Defender/Configuration/EnableFileHashComputation
```

Enables or disables file hash computation feature. When this feature is enabled Windows defender will compute hashes for files it scans.

Description framework properties:

Expand table

Property name	Property value
Format	`int`
Access Type	Add, Delete, Get, Replace
Default Value	0

Allowed values:

Expand table

Value	Description

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- Additional auditing
- Performance mode
- Update rings + sources
- File hash computation

- **Priority accounts**

Email & collaboration
Overview
Investigations
Explorer
Review
Campaigns
Threat tracker
Exchange message trace
Attack simulation training
Policies & rules
Cloud apps
Cloud security

User reported settings
User tags
Priority account protection
Microsoft Teams protection
MDO automation settings

Priority account protection

Priority account protection

On

Protect your Priority account users with:

- Additional machine learning models and heuristics focused on Priority account usage patterns
- More detailed evaluation of detonation results
- Visual indicators for emails sent to Priority accounts

Manage priority account users
Learn more about priority account users

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- Additional auditing
- Performance mode
- Update rings + sources
- File hash computation
- Priority accounts
- **Linked identities**

Link accounts

- Select accounts
- Enter justification
- Review and finish

Link accounts to (Admin) Ru Campbell

break

Display name	Account U...	Sou...	Sou...	Iden...
Identity: (Emergency Access) Break Glass 1 (1)				
(Emergency Access) Break Glass 1	breakglass1-8...	c55523...	Ent...	breakgl...
Identity: (Emergency Access) Break Glass 2 (1)				
(Emergency Access) Break Glass 2	breakglass2-9...	4d3776...	Ent...	breakgl...

Next

Cancel

Defender

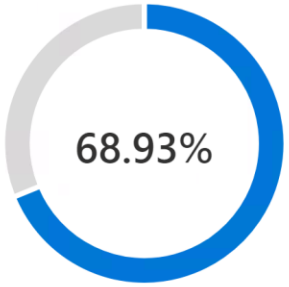
- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- Additional auditing
- Performance mode
- Update rings + sources
- File hash computation
- Priority accounts
- Linked identities
- **ISPM**

Microsoft Defender

Search

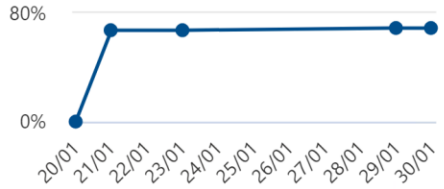
Recommendations summary

Identities secure score



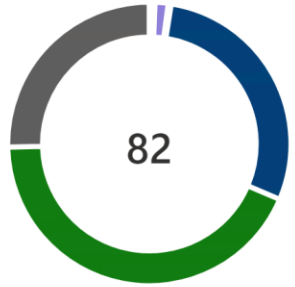
Score history

-31% (last 14 days)



View history

Recommendations by status



Alte...
Plan...
Risk ...
Thir...
To a...
Co...
No ...

Score comparison

Your score 68.93 / 100

Organizations of a similar size 53 / 100

Export

82 items

Search

Customize columns

Filter set: None

Save

Add filter

Name	Identity Score impact	Points achieved	Status	Product	Last synced	Related initiati...	Related metrics
Reversible passwords found in GPOs	+2.52%	0/8	To address	Defender for Identity	Feb 1, 2026 22:...	1	2
Locate accounts in built-in Operator Groups	+2.52%	0/8	To address	Defender for Identity	Feb 1, 2026 22:...	-	1
Stop clear text credentials exposure	+1.58%	0/5	To address	Defender for Identity	Feb 1, 2026 22:...	6	6
Remove dormant accounts from sensitive groups	+1.58%	0/5	To address	Defender for Identity	Feb 1, 2026 22:...	4	3
Modify unsecure Kerberos delegations to prevent impersonation	+1.58%	0/5	To address	Defender for Identity	Feb 1, 2026 22:...	4	4
Disable Print spooler service on domain controllers	+1.58%	0/5	To address	Defender for Identity	Feb 1, 2026 22:...	4	5
Protect and manage local admin passwords with Microsoft LAPS	+1.58%	0/5	To address	Defender for Identity	Feb 1, 2026 22:...	5	6

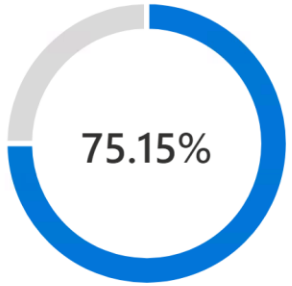
Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- Additional auditing
- Performance mode
- Update rings + sources
- File hash computation
- Priority accounts
- Linked identities
- ISPM
- **SSPM**

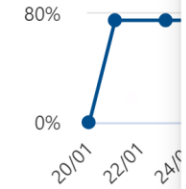
Home
Exposure management
Overview
Initiatives
Recommendations
Vulnerability management
Attack surface
Secure score
Data connectors
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints

Recommendations summary

SaaS apps secure score



Score history



View history

Score comparison

Your score 75.15 / 100

Organizations of a simil... 43.66 / 100

Export

Search

Customize columns

Filter set: None Save

Product: Atlassian (preview), Citrix ShareFile, DocuSign, +10

Name	Status	Product	Last synced	Rel
Disable 'Allow members to change repository visibilities for this	0/6 To address	GitHub	Feb 2, 2026 09:...	-
Enable single sign on (SSO) (GitHub (ts-dev))	3/3 Completed	GitHub	Feb 2, 2026 09:...	-
Disable private repository forking (GitHub (ts-dev))	7/7 Completed	GitHub	Feb 2, 2026 09:...	-
Disable 'Members will be able to create public repositories, visibl	4/4 Completed	GitHub	Feb 2, 2026 09:...	-
Disable 'Allow members to view dependency insights' (GitHub (t	4/4 Completed	GitHub	Feb 2, 2026 09:...	-
Disable 'members with admin permissions for repositories can de	6/6 Completed	GitHub	Feb 2, 2026 09:...	-
Disable 'Allow repository administrators to invite outside collabo	4/4 Completed	GitHub	Feb 2, 2026 09:...	-

Reset filter

Product

- [ ] App governance
- [x] Atlassian (preview)
- [x] Citrix ShareFile
- [ ] Defender External Attack Surface Management
- [ ] Defender for Cloud
- [ ] Defender for Cloud Apps
- [ ] Defender for Endpoint
- [ ] Defender for Identity
- [ ] Defender for IoT
- [ ] Defender for Office
- [x] DocuSign
- [x] Dropbox (preview)
- [ ] Entra ID
- [ ] Exchange Online
- [x] GitHub
- [x] Google Workspace
- [ ] Intune
- [ ] Microsoft 365 Defender
- [ ] Microsoft Information Protection
- [x] NetDocuments (preview)
- [ ] Okta
- [x] Salesforce
- [x] ServiceNow

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- Additional auditing
- Performance mode
- Update rings + sources
- File hash computation

- Priority accounts
- Linked identities
- ISPM
- SSPM
- **Access policies**

CA006: Guest users - session policies for web apps

Conditional Access policy

Delete | View policy information

Network NEW

Not configured

Conditions

1 condition selected

Access controls

Grant

0 controls selected

Session

3 controls selected

Enable policy

Report-only | On | Off

Save

Session

to enable limited experiences within specific cloud applications. Learn more

Use app enforced restrictions

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more

Use Conditional Access App Control

Use custom policy...

Monitor only (Preview)

Block downloads (Preview)

Use custom policy...

onboarded for any app.
Learn more

Select

Activities matching all of the following

Edit and preview results

IP address | Category | equals | Select value

Add a filter

Administrative
Cloud provider
Corporate
Risky
VPN
Other
No value
Manage IP address ranges

Actions

Select an action to be applied when user activity matches t

Test
Monitor all activities

Block
A default block message is displayed when possible

Customize block message

gonnae no

Alerts

Session control type *

Select the type of control you want to enable:

Control file download (with inspection)

Actions

Select an action to be applied when user activity matches the policy.

- Audit
  Monitor activities
- Block
  A default block message is displayed when possible
  - Also notify user by email
  - Customize block message
- Protect
  Apply sensitivity label to downloads & monitor all activities
- Require step-up authentication PREVIEW FEATURE
  Re-evaluate Azure AD Conditional Access polices based on the authentication context.
  Unpublished authentication context will not be enforced
  Configure authentication context

Defender

- EDR in block mode
- Block at first sight
- Device groups = tiering
- Tamper protection
- Contextual exclusions
- Additional auditing
- Performance mode
- Update rings + sources
- File hash computation
- Priority accounts
- Linked identities
- ISPM
- SSPM
- Access policies
- **Session policies**

CA006: Guest users - session policies for web apps

Conditional Access policy

Delete | View policy information

Network NEW

Not configured

Conditions

1 condition selected

Access controls

Grant

0 controls selected

Session

3 controls selected

Enable policy

Report-only | On | Off

Save

Session

to enable limited experiences within specific cloud applications. Learn more

Use app enforced restrictions

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more

Use Conditional Access App Control

Use custom policy...

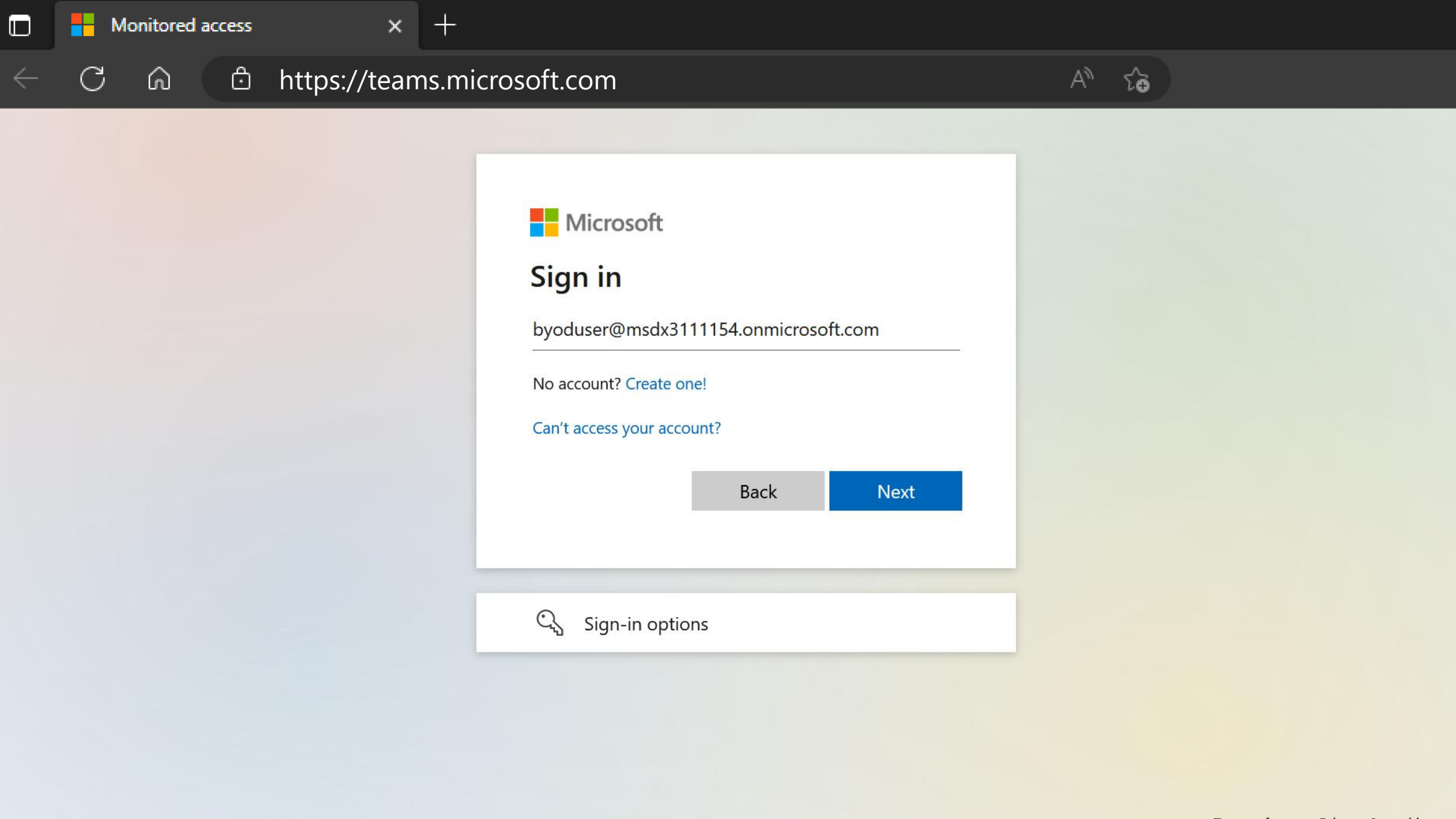
Monitor only (Preview)

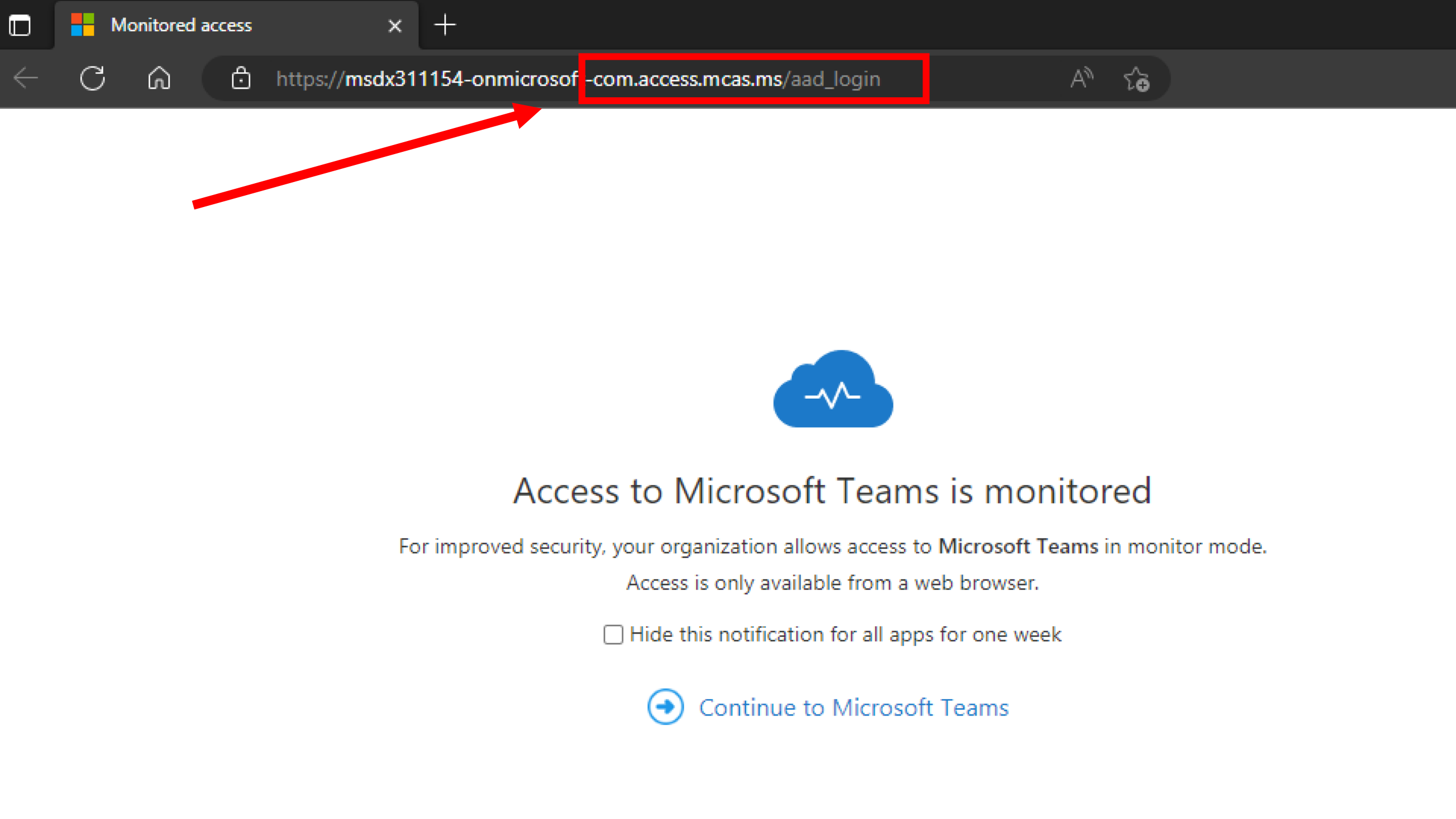
Block downloads (Preview)

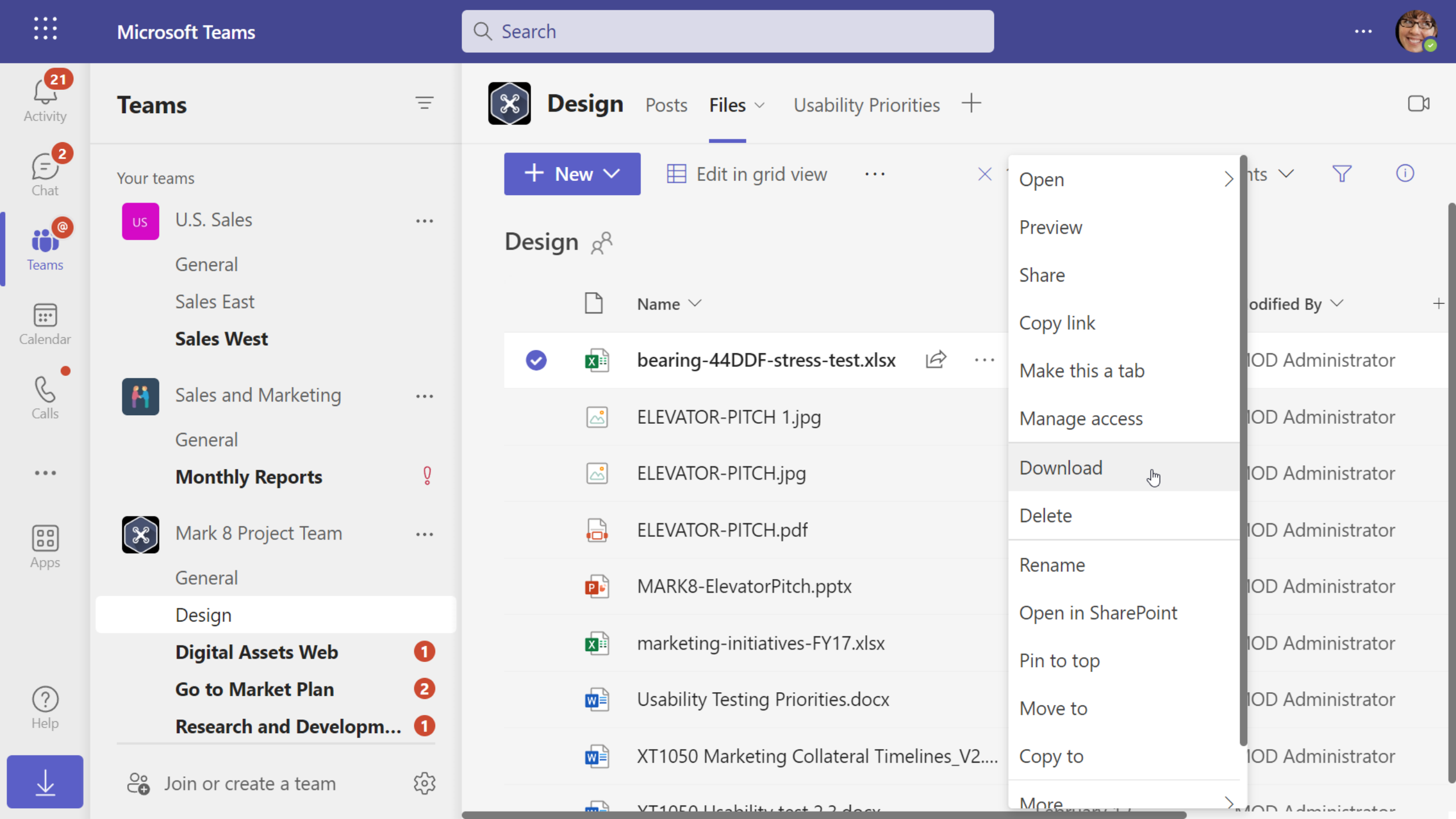
Use custom policy...

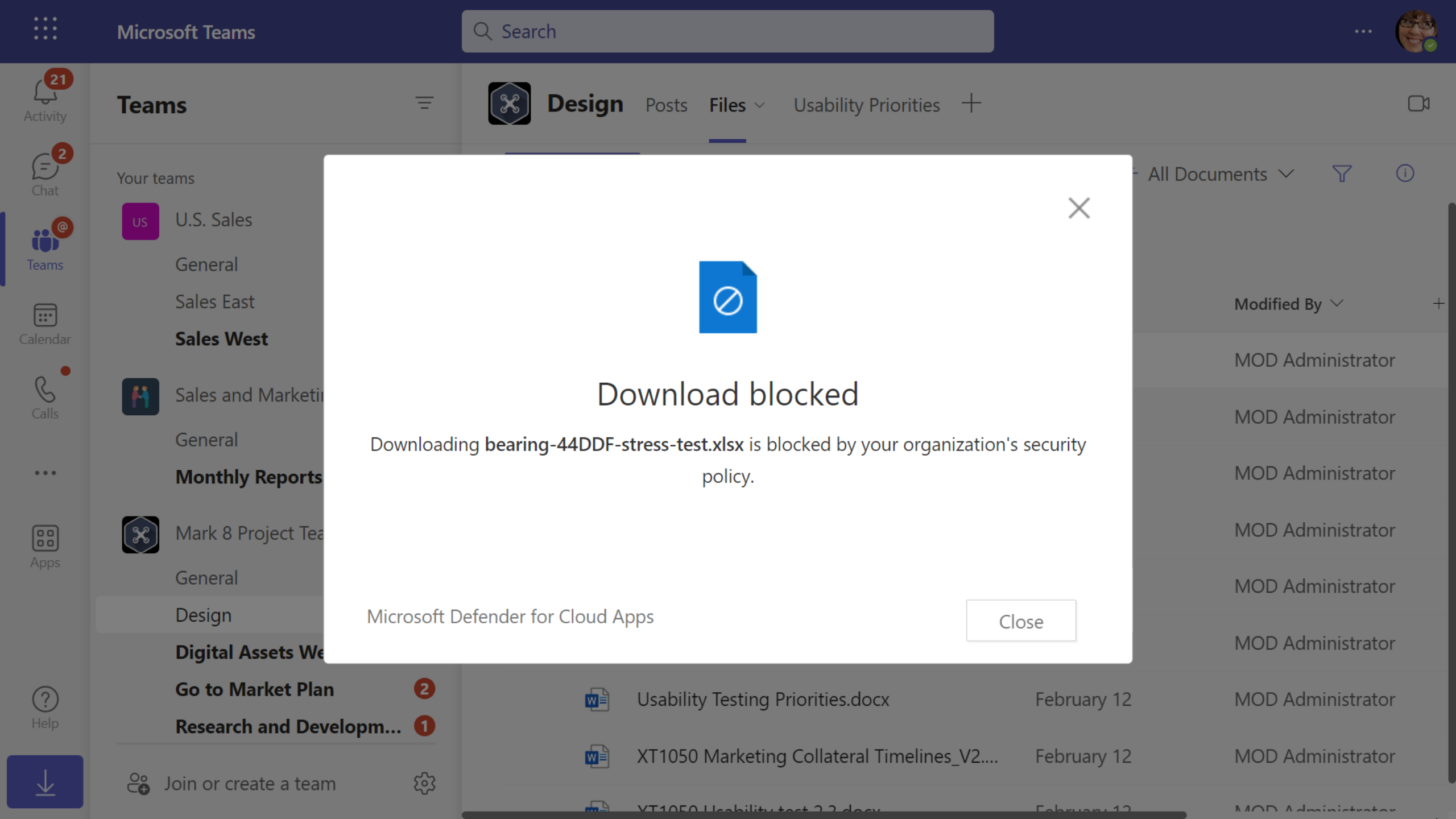
onboarded for any app.
Learn more

Select


Monitored access
https://teams.microsoft.com
Microsoft
Sign in
byoduser@msdx3111154.onmicrosoft.com
No account? Create one!
Can't access your account?
Back
Next
Sign-in options


Monitored access
https://msdx311154-onmicrosof-com.access.mcas.ms/aad_login
Access to Microsoft Teams is monitored
For improved security, your organization allows access to Microsoft Teams in monitor mode.
Access is only available from a web browser.
Hide this notification for all apps for one week
Continue to Microsoft Teams


Microsoft Teams
Search
Activity
Chat
Teams
Calendar
Calls
Apps
Help
Teams
Your teams
U.S. Sales
General
Sales East
Sales West
Sales and Marketing
General
Monthly Reports
Mark 8 Project Team
General
Design
Digital Assets Web
Go to Market Plan
Research and Developm...
Join or create a team
Design
Posts
Files
Usability Priorities
New
Edit in grid view
Design
Name
bearing-44DDF-stress-test.xlsx
ELEVATOR-PITCH 1.jpg
ELEVATOR-PITCH.jpg
ELEVATOR-PITCH.pdf
MARK8-ElevatorPitch.pptx
marketing-initiatives-FY17.xlsx
Usability Testing Priorities.docx
XT1050 Marketing Collateral Timelines_V2....
Open
Preview
Share
Copy link
Make this a tab
Manage access
Download
Delete
Rename
Open in SharePoint
Pin to top
Move to
Copy to
More

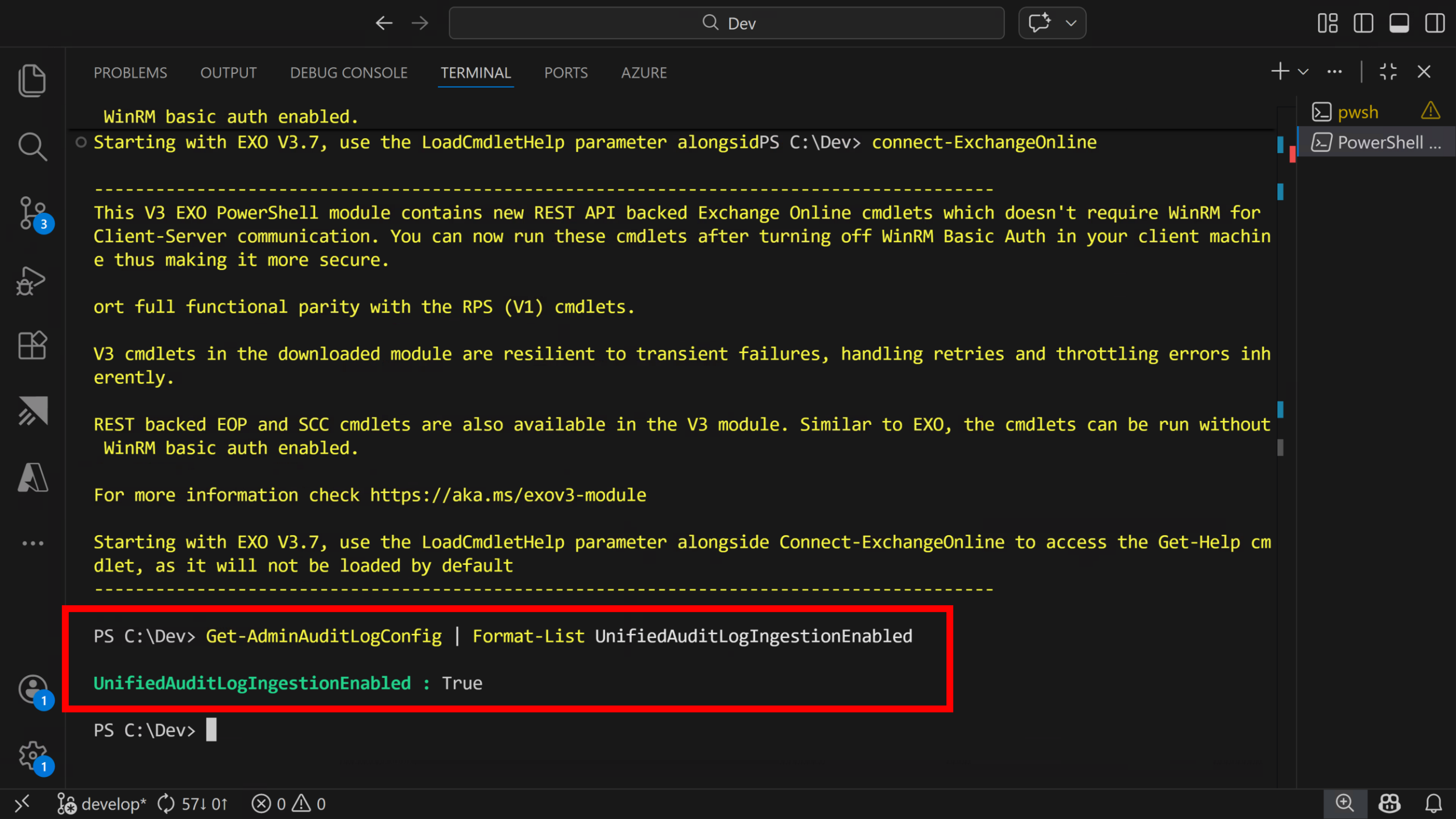

Microsoft Teams
Search
Activity
Chat
Teams
Calendar
Calls
Apps
Help
Teams
Your teams
U.S. Sales
General
Sales East
Sales West
Sales and Marketi
General
Monthly Reports
Mark 8 Project Tea
General
Design
Digital Assets We
Go to Market Plan
Research and Developm...
Join or create a team
Design
Posts
Files
Usability Priorities
All Documents
Modified By
MOD Administrator
Download blocked
Downloading bearing-44DDF-stress-test.xlsx is blocked by your organization's security policy.
Microsoft Defender for Cloud Apps
Close
Usability Testing Priorities.docx
February 12
XT1050 Marketing Collateral Timelines_V2....
February 12

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- **Purview Audit enablement**

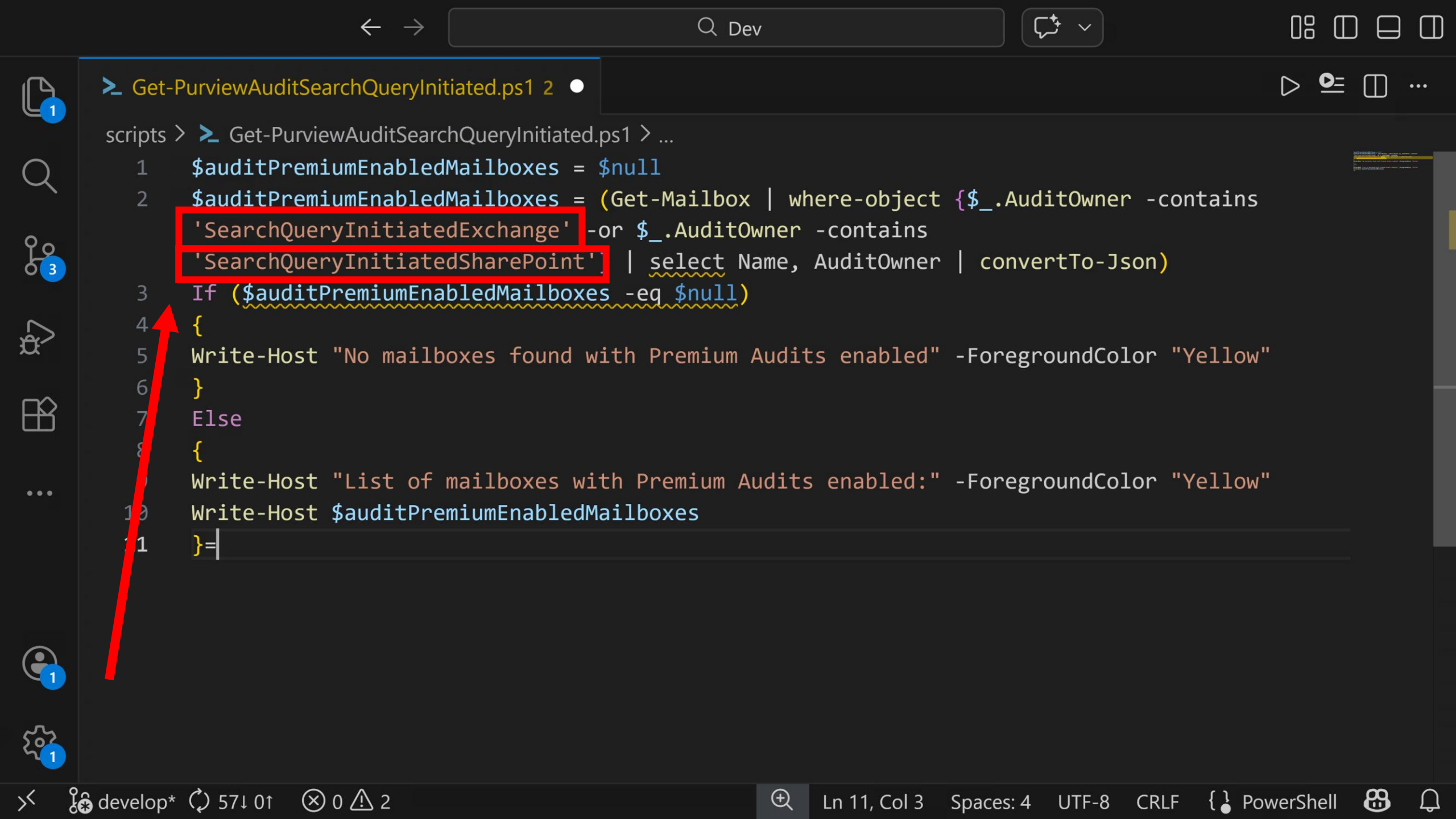

Dev
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
AZURE
pwsh
PowerShell ...
WinRM basic auth enabled.
Starting with EXO V3.7, use the LoadCmdletHelp parameter alongsidPS C:\Dev> connect-ExchangeOnline
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't require WinRM for Client-Server communication. You can now run these cmdlets after turning off WinRM Basic Auth in your client machine thus making it more secure.
ort full functional parity with the RPS (V1) cmdlets.
V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inherently.
REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets can be run without WinRM basic auth enabled.
For more information check https://aka.ms/exov3-module
Starting with EXO V3.7, use the LoadCmdletHelp parameter alongside Connect-ExchangeOnline to access the Get-Help cmdlet, as it will not be loaded by default
PS C:\Dev> Get-AdminAuditLogConfig | Format-List UnifiedAuditLogIngestionEnabled
UnifiedAuditLogIngestionEnabled : True
PS C:\Dev>
develop*
57↓ 0↑
0
0

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- Purview Audit enablement
- **… and some more bits**

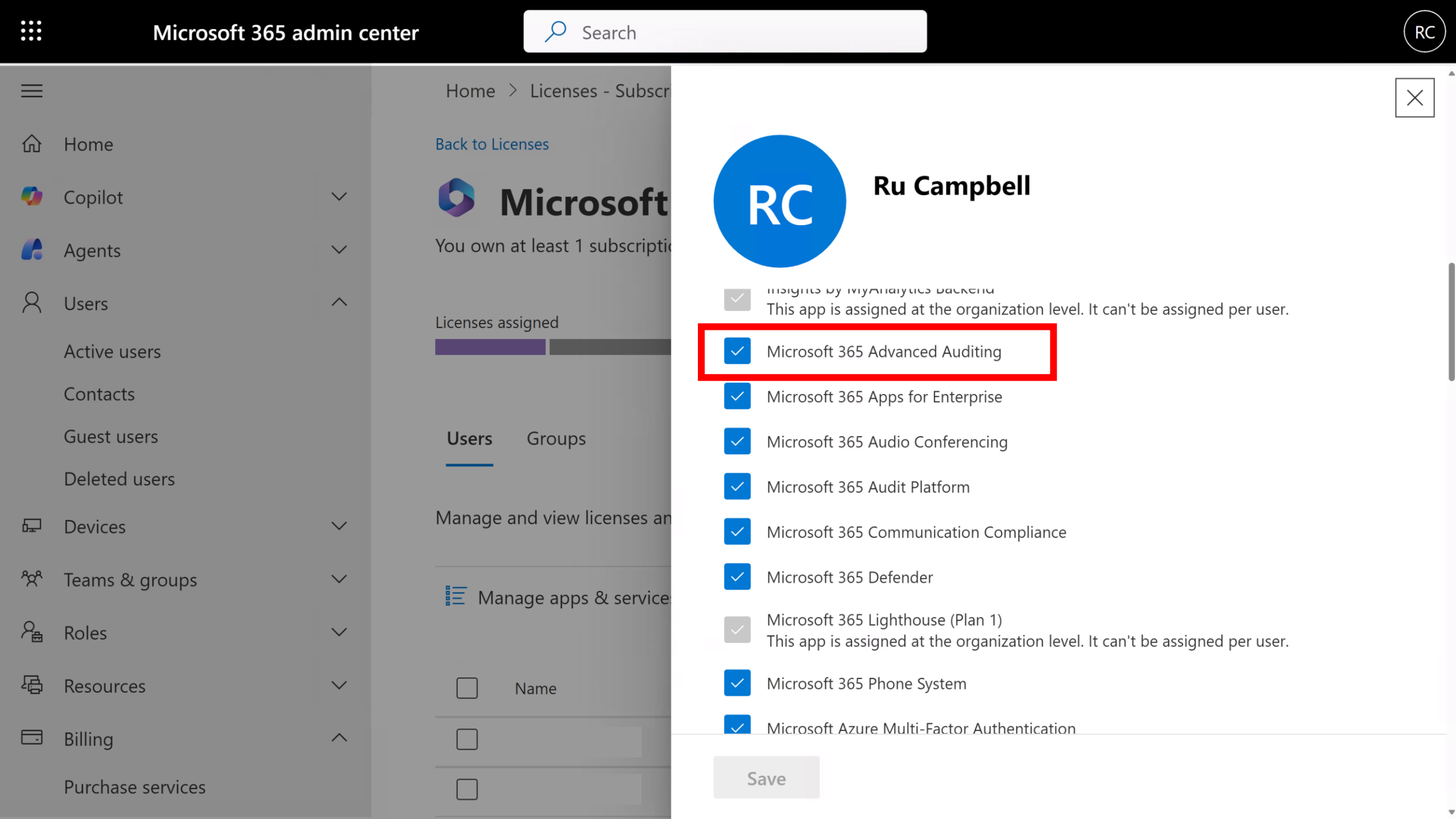

Dev
Get-PurviewAuditSearchQueryInitiated.ps1 2
scripts > Get-PurviewAuditSearchQueryInitiated.ps1 > ...
1 $auditPremiumEnabledMailboxes = $null
2 $auditPremiumEnabledMailboxes = (Get-Mailbox | where-object {$_.AuditOwner -contains
'SearchQueryInitiatedExchange' -or $_.AuditOwner -contains
'SearchQueryInitiatedSharePoint'} | select Name, AuditOwner | convertTo-Json)
3 If ($auditPremiumEnabledMailboxes -eq $null)
4 {
5 Write-Host "No mailboxes found with Premium Audits enabled" -ForegroundColor "Yellow"
6 }
7 Else
8 {
9 Write-Host "List of mailboxes with Premium Audits enabled:" -ForegroundColor "Yellow"
10 Write-Host $auditPremiumEnabledMailboxes
11 }
develop* 57↓ 0↑ 0 2
Ln 11, Col 3 Spaces: 4 UTF-8 CRLF PowerShell

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- Purview Audit enablement
- … and some more bits
- **Audit (Premium) gotcha**

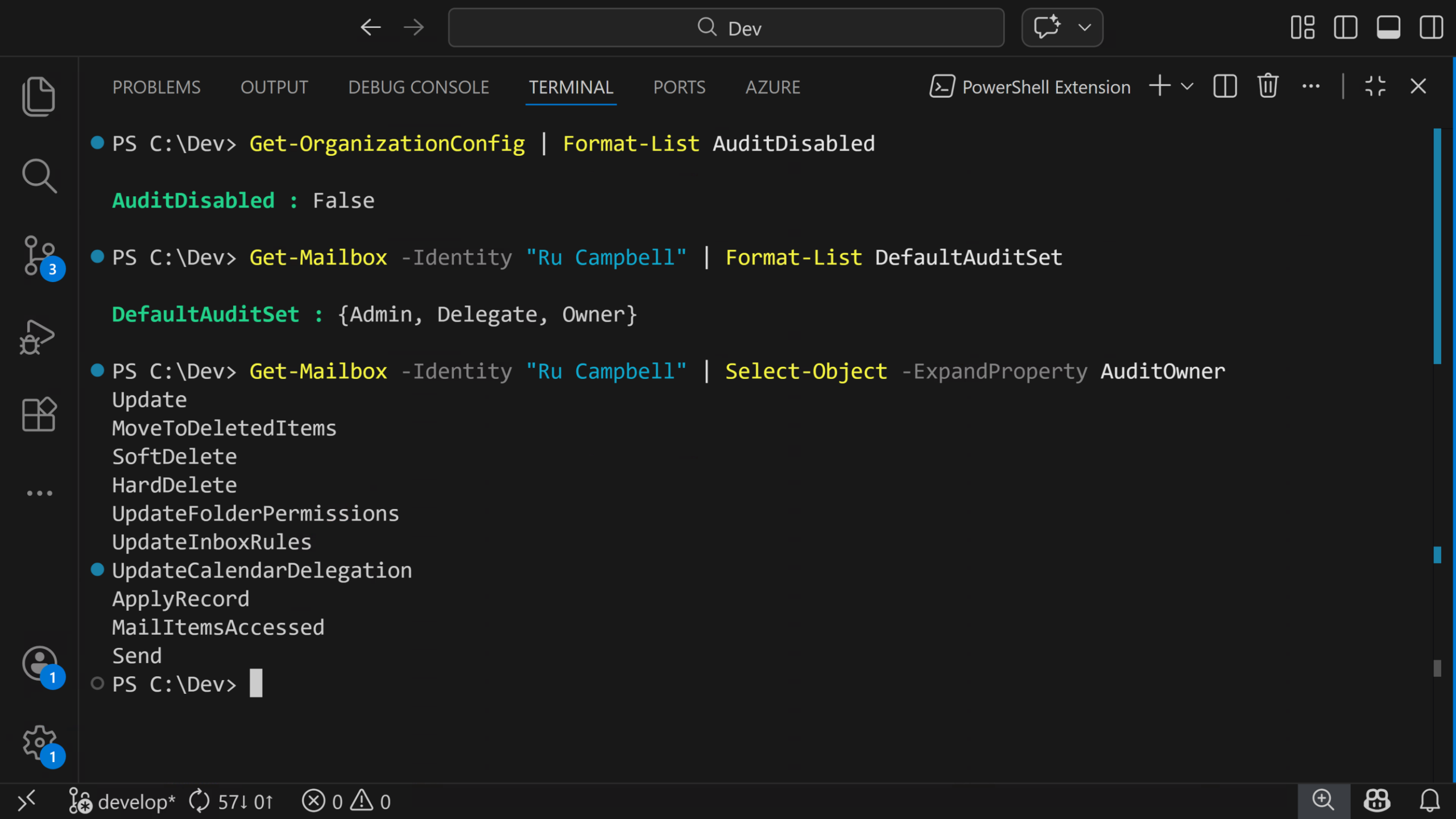

Microsoft 365 admin center
Search
RC
Home
Copilot
Agents
Users
Active users
Contacts
Guest users
Deleted users
Devices
Teams & groups
Roles
Resources
Billing
Purchase services
Home > Licenses - Subscri
Back to Licenses
Microsoft
You own at least 1 subscripti
Licenses assigned
Users
Groups
Manage and view licenses an
Manage apps & service
Name
RC
Ru Campbell
This app is assigned at the organization level. It can't be assigned per user.
Microsoft 365 Advanced Auditing
Microsoft 365 Apps for Enterprise
Microsoft 365 Audio Conferencing
Microsoft 365 Audit Platform
Microsoft 365 Communication Compliance
Microsoft 365 Defender
Microsoft 365 Lighthouse (Plan 1)
This app is assigned at the organization level. It can't be assigned per user.
Microsoft 365 Phone System
Microsoft Azure Multi-Factor Authentication
Save

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- **Mailbox auditing**

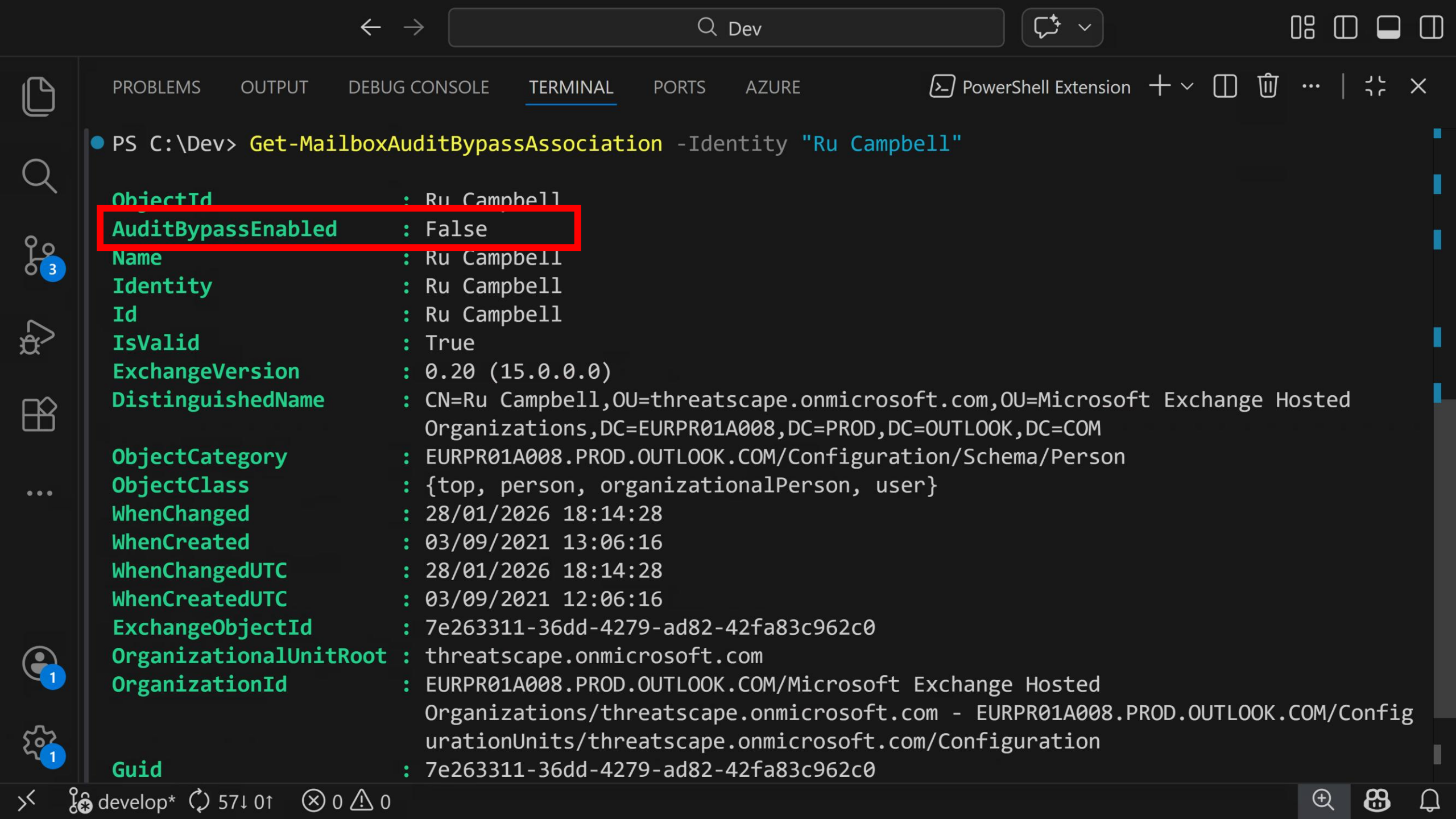

Dev
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
AZURE
PowerShell Extension
PS C:\Dev> Get-OrganizationConfig | Format-List AuditDisabled
AuditDisabled : False
PS C:\Dev> Get-Mailbox -Identity "Ru Campbell" | Format-List DefaultAuditSet
DefaultAuditSet : {Admin, Delegate, Owner}
PS C:\Dev> Get-Mailbox -Identity "Ru Campbell" | Select-Object -ExpandProperty AuditOwner
Update
MoveToDeletedItems
SoftDelete
HardDelete
UpdateFolderPermissions
UpdateInboxRules
UpdateCalendarDelegation
ApplyRecord
MailItemsAccessed
Send
PS C:\Dev>
develop*
57↓ 0↑
0
0

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- **Mailbox audit bypass**

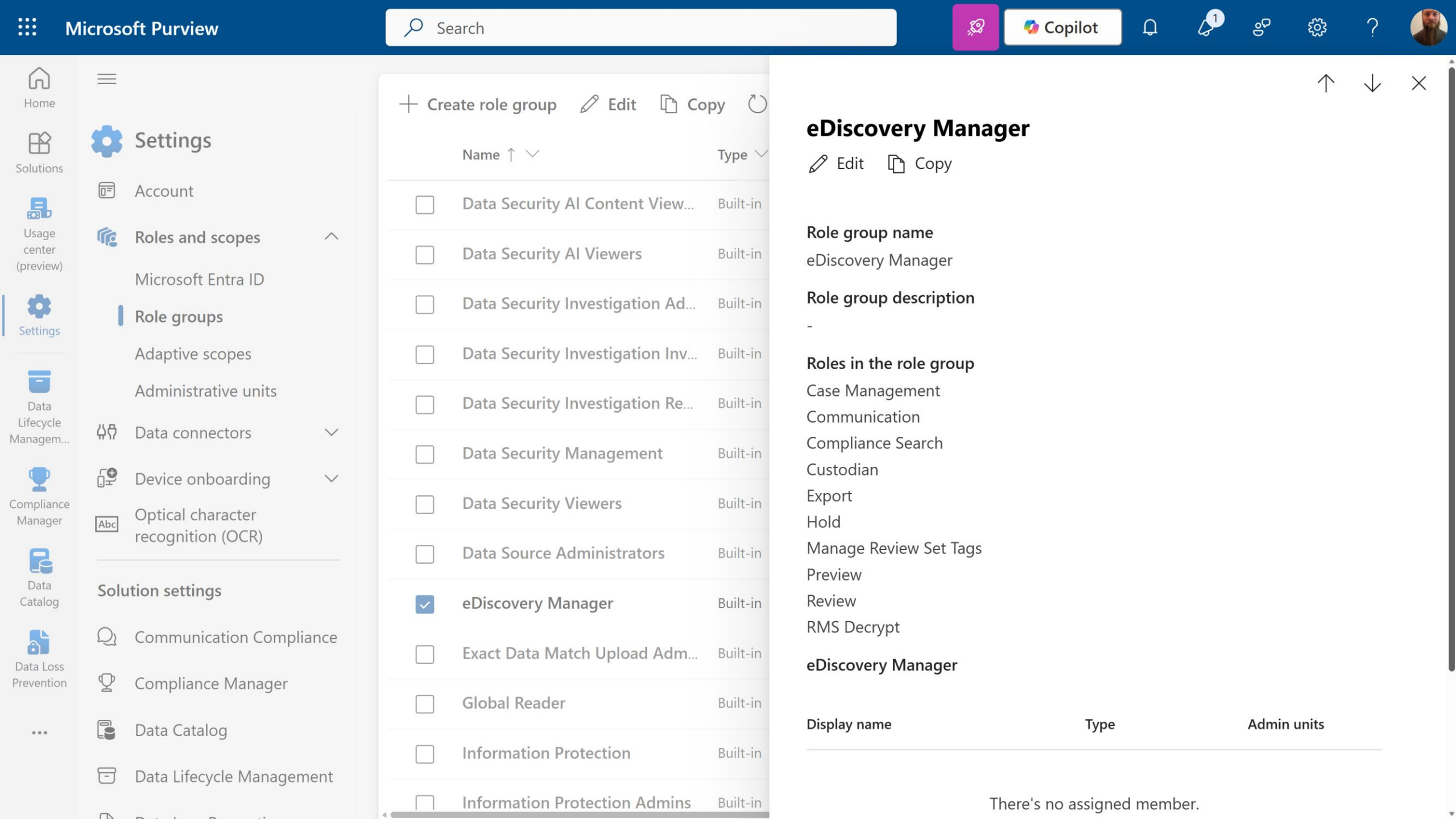

Dev
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
AZURE
PowerShell Extension
PS C:\Dev> Get-MailboxAuditBypassAssociation -Identity "Ru Campbell"
ObjectId : Ru Campbell
AuditBypassEnabled : False
Name : Ru Campbell
Identity : Ru Campbell
Id : Ru Campbell
IsValid : True
ExchangeVersion : 0.20 (15.0.0.0)
DistinguishedName : CN=Ru Campbell,OU=threatscape.onmicrosoft.com,OU=Microsoft Exchange Hosted Organizations,DC=EURPR01A008,DC=PROD,DC=OUTLOOK,DC=COM
ObjectCategory : EURPR01A008.PROD.OUTLOOK.COM/Configuration/Schema/Person
ObjectClass : {top, person, organizationalPerson, user}
WhenChanged : 28/01/2026 18:14:28
WhenCreated : 03/09/2021 13:06:16
WhenChangedUTC : 28/01/2026 18:14:28
WhenCreatedUTC : 03/09/2021 12:06:16
ExchangeObjectId : 7e263311-36dd-4279-ad82-42fa83c962c0
OrganizationalUnitRoot : threatscape.onmicrosoft.com
OrganizationId : EURPR01A008.PROD.OUTLOOK.COM/Microsoft Exchange Hosted Organizations/threatscape.onmicrosoft.com - EURPR01A008.PROD.OUTLOOK.COM/ConfigurationUnits/threatscape.onmicrosoft.com/Configuration
Guid : 7e263311-36dd-4279-ad82-42fa83c962c0
develop* 57↓ 0↑
0 0

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- **Purview RBAC**


Microsoft Purview
Search
Copilot
Home
Solutions
Usage center (preview)
Settings
Data Lifecycle Managem...
Compliance Manager
Data Catalog
Data Loss Prevention
Settings
Account
Roles and scopes
Microsoft Entra ID
Role groups
Adaptive scopes
Administrative units
Data connectors
Device onboarding
Optical character recognition (OCR)
Solution settings
Communication Compliance
Compliance Manager
Data Catalog
Data Lifecycle Management
Create role group
Edit
Copy
Name
Type
Data Security AI Content View...
Data Security AI Viewers
Data Security Investigation Ad...
Data Security Investigation Inv...
Data Security Investigation Re...
Data Security Management
Data Security Viewers
Data Source Administrators
eDiscovery Manager
Exact Data Match Upload Adm...
Global Reader
Information Protection
Information Protection Admins
Built-in
eDiscovery Manager
Edit
Copy
Role group name
eDiscovery Manager
Role group description
-
Roles in the role group
Case Management
Communication
Compliance Search
Custodian
Export
Hold
Manage Review Set Tags
Preview
Review
RMS Decrypt
eDiscovery Manager
Display name
Type
Admin units
There's no assigned member.

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- **Extension requirement**

Find by title

Help protect files that Endpoint Data Loss Prevention doesn't scan

Help protect against sharing of a defined set of unsupported files from Endpoints

Disable Microsoft Purview data loss prevention scanning for some supported files and apply controls

Always-on diagnostics for endpoint DLP

Download PDF

10. Select **Google** > **Google Chrome** > **Extensions**.
11. Select **Configure the list of force-installed apps and extensions**.
12. Change the toggle to **Enabled**.
13. Enter the following value for the extensions and app IDs and update URL: `echcggldkblhodogklpincgchnpgcdco;https://clients2.google.com/service/update2/crx`.
14. Select **Next**.
15. Add or edit scope tags on the **Scope tags** tab as needed and select **Next**.
16. Add the required deployment users, devices, and groups on the **Assignments** tab and select **Next**.
17. Add applicability rules on the **Applicability Rules** tab as required and select **Next**.

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- **MFA exclusions**

Conditional Access policies and encrypted documents

If your organization has implemented Microsoft Entra Conditional Access policies that include **Microsoft Rights Management Services** and the policy extends to external users who need to open documents encrypted by your organization:

- For external users who have a Microsoft Entra account in their own tenant, we recommend you use External Identities cross-tenant access settings to configure trust settings for MFA claims from one, many, or all external Microsoft Entra organizations.
- For external users not covered by the previous entry, for example, users who don't have a Microsoft Entra account or you haven't configured cross-tenant access settings for trust settings, these external users must have a guest account in your tenant.

Without one of these configurations, external users can't open the encrypted content and see an error message. The message text might inform them that their account needs to be added as an external user in the tenant, with the incorrect instruction for this scenario to **Sign out and sign in again with a different Microsoft Entra user account**.

If you can't meet these configuration requirements for external users who need to open content encrypted by your organization, you must either remove Microsoft Rights Management Services from the Conditional Access policies, or exclude external users from the policies.

For more information, see the frequently asked question, I see Microsoft Rights Management

In this article

Purview + Intune + Exchange Online

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- MFA exclusions

Intune

- **OIB**

OIB Deployer

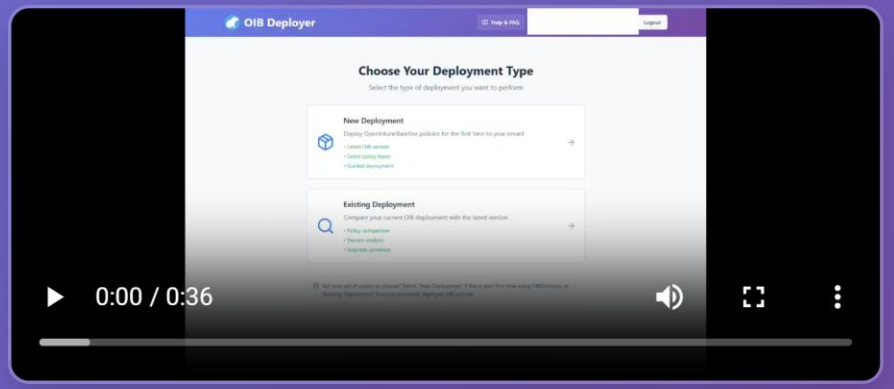
Help & FAQ

Deploy and Manage OpenIntuneBaseline in Microsoft Intune

The OpenIntuneBaseline project provides a comprehensive set of Microsoft Intune security baselines designed to enhance your organization's security posture. Deploy proven security configurations with enterprise-grade automation and governance.

Deploy Now

View Documentation



Demo: OpenIntuneBaseline security policy deployment walkthrough

Purview + Intune + Exchange Online

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- MFA exclusions

Intune

- OIB
- **Enrolment restrictions**

Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Edit restriction

Device type restriction

1 Platform settings 2 Review + save

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. Learn more

Type	Platform	versions	Personally owned	Device manufacturer
Android Enterprise (work profile)	Allow / Block	Allow min/max range: Min Max	Allow / Block	Manufacturer name
Android device administrator	Allow / Block	Allow min/max range: Min Max	Allow / Block	Manufacturer name
iOS/iPadOS	Allow / Block	Allow min/max range: Min Max	Allow / Block	Restriction not supported
macOS	Allow / Block	Restriction not supported	Allow / Block	Restriction not supported
Windows (MDM)	Allow / Block	Allow min/max range: Min Max	Allow / Block	Restriction not supported

Review + save Cancel

Purview + Intune + Exchange Online

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- MFA exclusions

Intune

- OIB
- Enrolment restrictions
- **Enrolment notifications**

Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Create an enrollment notification

Enrollment Notifications

Basics | 2 Notification settings | 3 Scope tags | 4 Assignments | 5 Review + create

Configure the enrollment notifications you want to send to Windows devices. Learn more about enrollment notifications

Push Notification

Send Push Notification: Off

Email Notification

Send Email Notification: On

Subject *: You've enrolled an Intune device

Raw HTML editor: On

Message *

```
1  Hi
```

Previous | Next

Purview + Intune + Exchange Online

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- MFA exclusions

Intune

- OIB
- Enrolment restrictions
- Enrolment notifications
- **Conditional launch**

Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Agents
Reports
Users
Groups
Tenant administration
Troubleshooting + support

Create policy

App conditions

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	1440	Block access (minutes)
Offline grace period	90	Wipe data (days)
Disabled account		Block access
Select one		

Device conditions

Configure the following conditional launch settings for device based conditions through your app protection policy.

Similar device based settings can be configured for enrolled devices. Learn more about configuring device compliance settings for enrolled devices.

Setting	Value	Action
Jailbroken/rooted devices		Block access
Min OS version	26.2	Warn
Min OS version	26.1	Block access

Previous Next

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- MFA exclusions

Intune

- OIB
- Enrolment restrictions
- Enrolment notifications
- Conditional launch

Exchange Online

- **Automatic email forwarding**

Overview

If you want to quickly compare various methods, you can refer to the following table:

Automatic forwarding option	**Remote domain**	**Transport rule**	**Outbound spam filter policy**
Block Outlook forwarding using inbox rules	Yes	Yes	Yes
Block Outlook forwarding configured using OOF rule	Yes	Yes	Yes
Block OWA forwarding setting (ForwardingSmtpAddress)	Yes	No	Yes
Block external forwarding set by the admin using EAC (ForwardingSMTPAddress)	Yes	No	Yes
Block forwarding using Power Automate / Flow	No	Yes	No
Does the sender get NDR when auto forward is blocked?	No	Yes	Yes
Customization and granular control	No	Yes	Yes

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

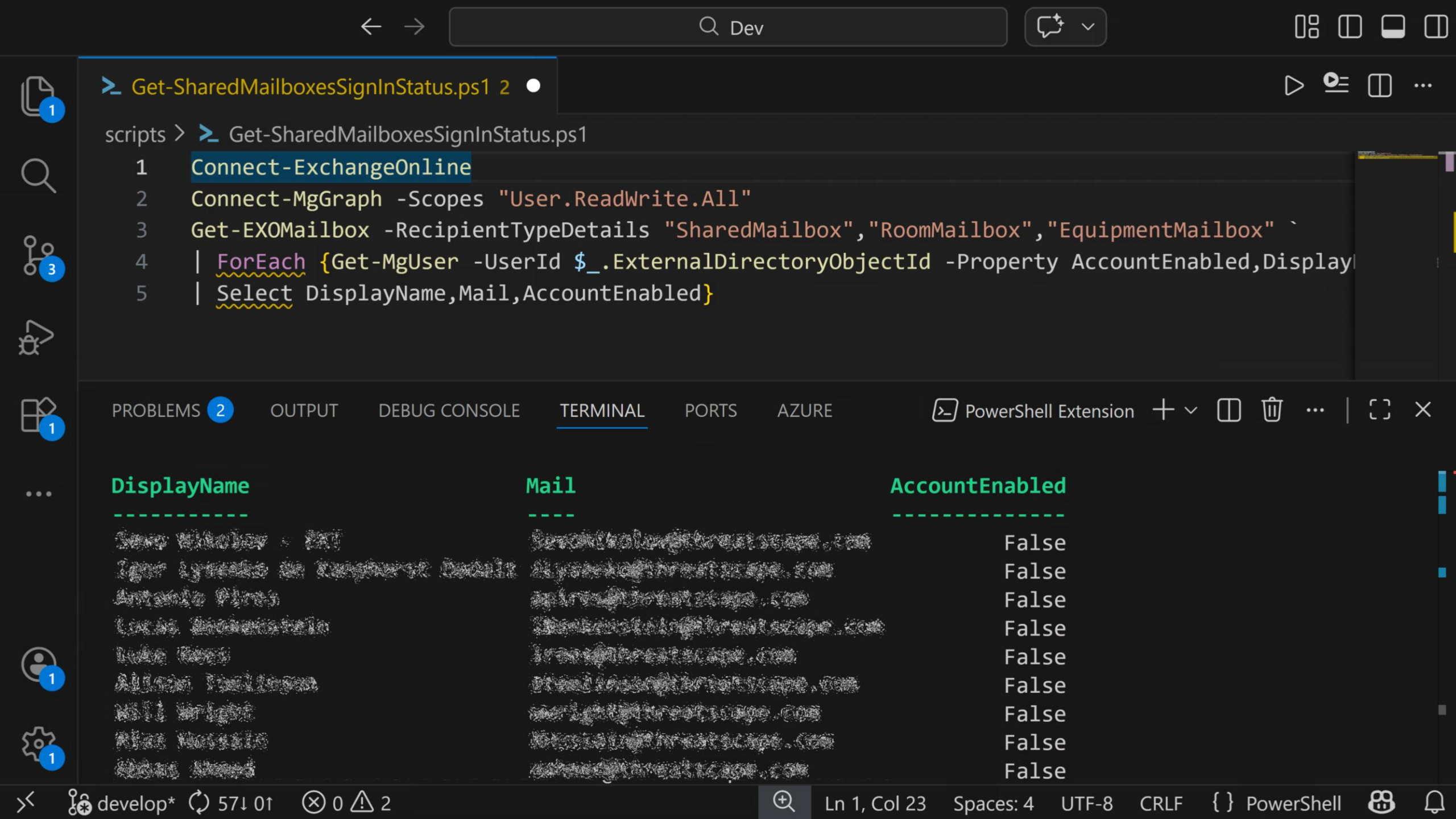
- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- MFA exclusions

Intune

- OIB
- Enrolment restrictions
- Enrolment notifications
- Conditional launch

Exchange Online

- Automatic email forwarding
- **Shared account sign-in**


Dev
Get-SharedMailboxesSignInStatus.ps1 2
scripts > Get-SharedMailboxesSignInStatus.ps1
1 Connect-ExchangeOnline
2 Connect-MgGraph -Scopes "User.ReadWrite.All"
3 Get-EXOMailbox -RecipientTypeDetails "SharedMailbox","RoomMailbox","EquipmentMailbox" `
4 | ForEach {Get-MgUser -UserId $_.ExternalDirectoryObjectId -Property AccountEnabled,Displayl
5 | Select DisplayName,Mail,AccountEnabled}
PROBLEMS 2
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
AZURE
PowerShell Extension
DisplayName
Mail
AccountEnabled
False
False
False
False
False
False
False
False
False
False
develop* 57↓ 0↑
0 2
Ln 1, Col 23
Spaces: 4
UTF-8
CRLF
PowerShell

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

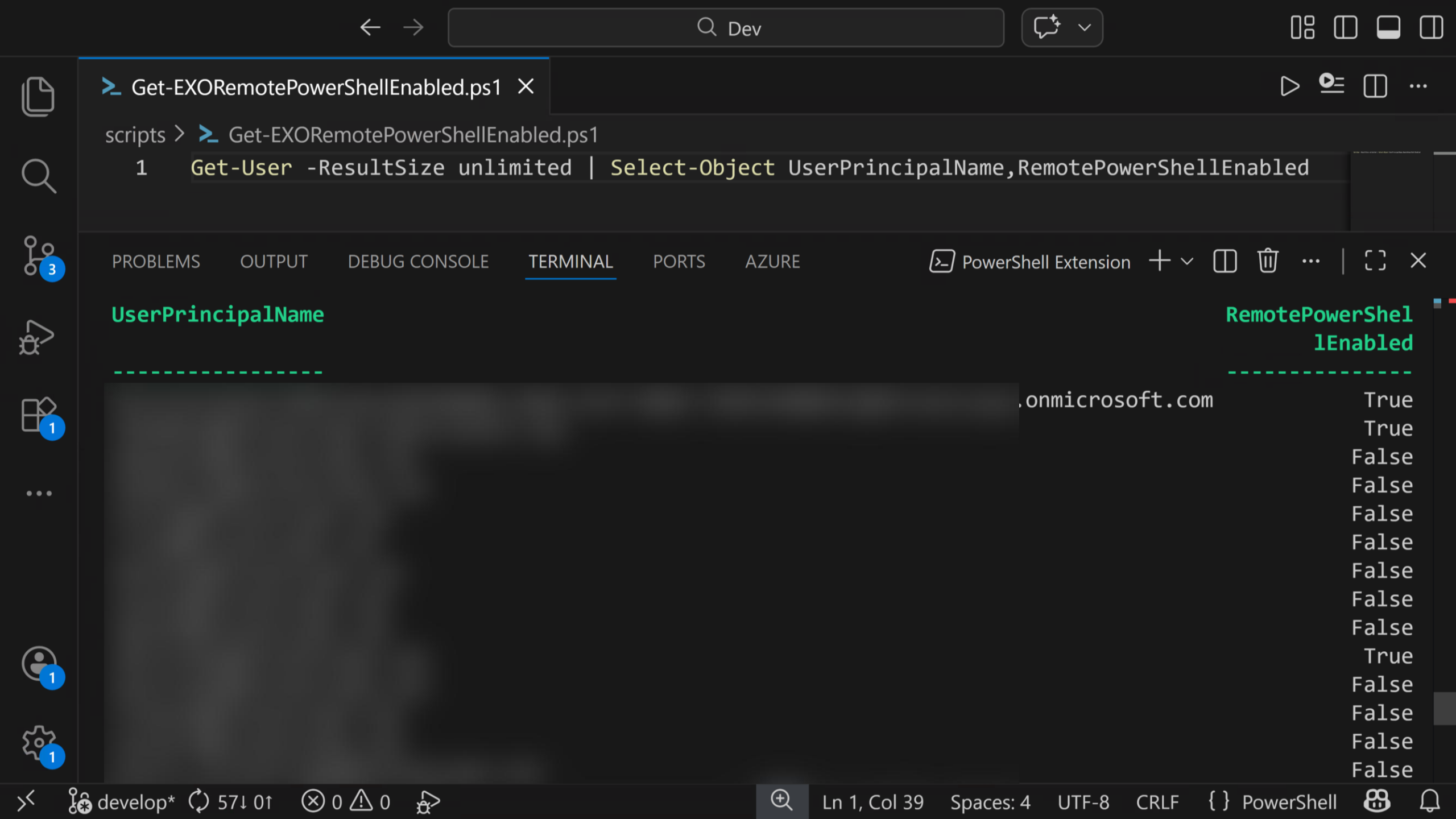
- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- MFA exclusions

Intune

- OIB
- Enrolment restrictions
- Enrolment notifications
- Conditional launch

Exchange Online

- Automatic email forwarding
- Shared account sign-in
- **PowerShell for EXO users**


Dev
Get-EXORemotePowerShellEnabled.ps1
scripts > Get-EXORemotePowerShellEnabled.ps1
1 Get-User -ResultSize unlimited | Select-Object UserPrincipalName,RemotePowerShellEnabled
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
AZURE
PowerShell Extension
UserPrincipalName
RemotePowerShellEnabled
.onmicrosoft.com
True
True
False
False
False
False
False
False
False
True
False
False
False
False
develop*
57↓ 0↑
0 0
Ln 1, Col 39
Spaces: 4
UTF-8
CRLF
PowerShell

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- MFA exclusions

Intune

- OIB
- Enrolment restrictions
- Enrolment notifications
- Conditional launch

Exchange Online

- Automatic email forwarding
- Shared account sign-in
- PowerShell for EXO users
- **Direct Send**

Microsoft Defender

Search

Advanced hunting

Help resources

DirectSendUsage

View details

Run query | Set in query | Save | Share link | Create detection rule

Query

```
1  EmailEvents
2  |where Timestamp > ago(30d)
3  | where EmailDirection == 'Inbound'
4  | extend LeftPartSender = substring(SenderFromAddress, 0, indexof(SenderFromAddress, '@'))
5  | extend LeftPartRecipient = substring(RecipientEmailAddress, 0, indexof(RecipientEmailAddr
6  | where LeftPartSender == LeftPartRecipient
7  | where isempty(Connectors) // not coming in on a connector
8  | where DeliveryLocation == 'Inbox/folder'
9  | where parse_json(AuthenticationDetails) contains 'fail'
10 | project Timestamp, RecipientEmailAddress, SenderFromAddress, Subject, NetworkMessageId, R
```

Purview + Intune + Exchange Online

MC2MC CONNECT

Purview

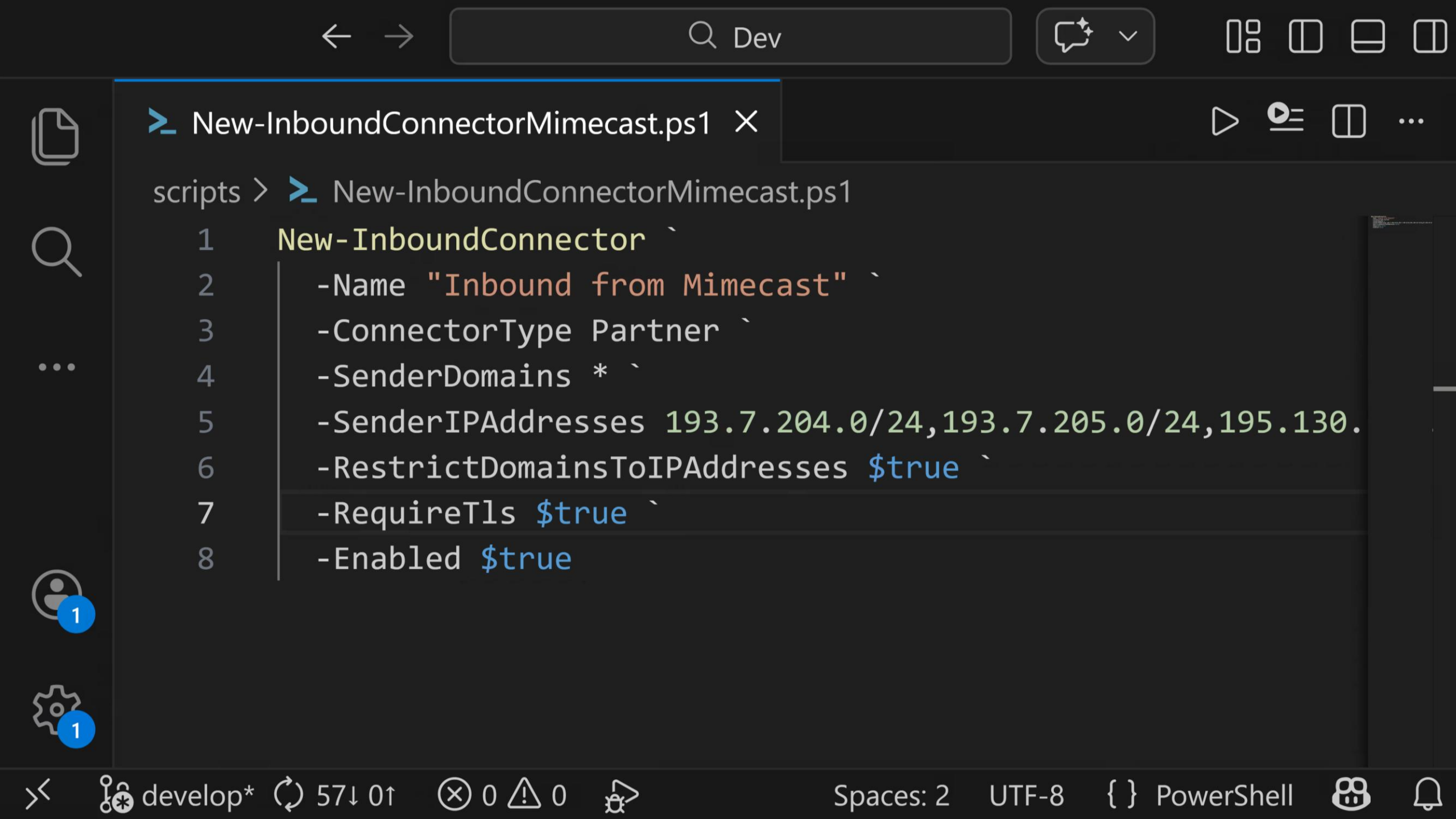
- Purview Audit enablement
- … and some more bits
- Audit (Premium) gotcha
- Mailbox auditing
- Mailbox audit bypass
- Purview RBAC
- Extension requirement
- MFA exclusions

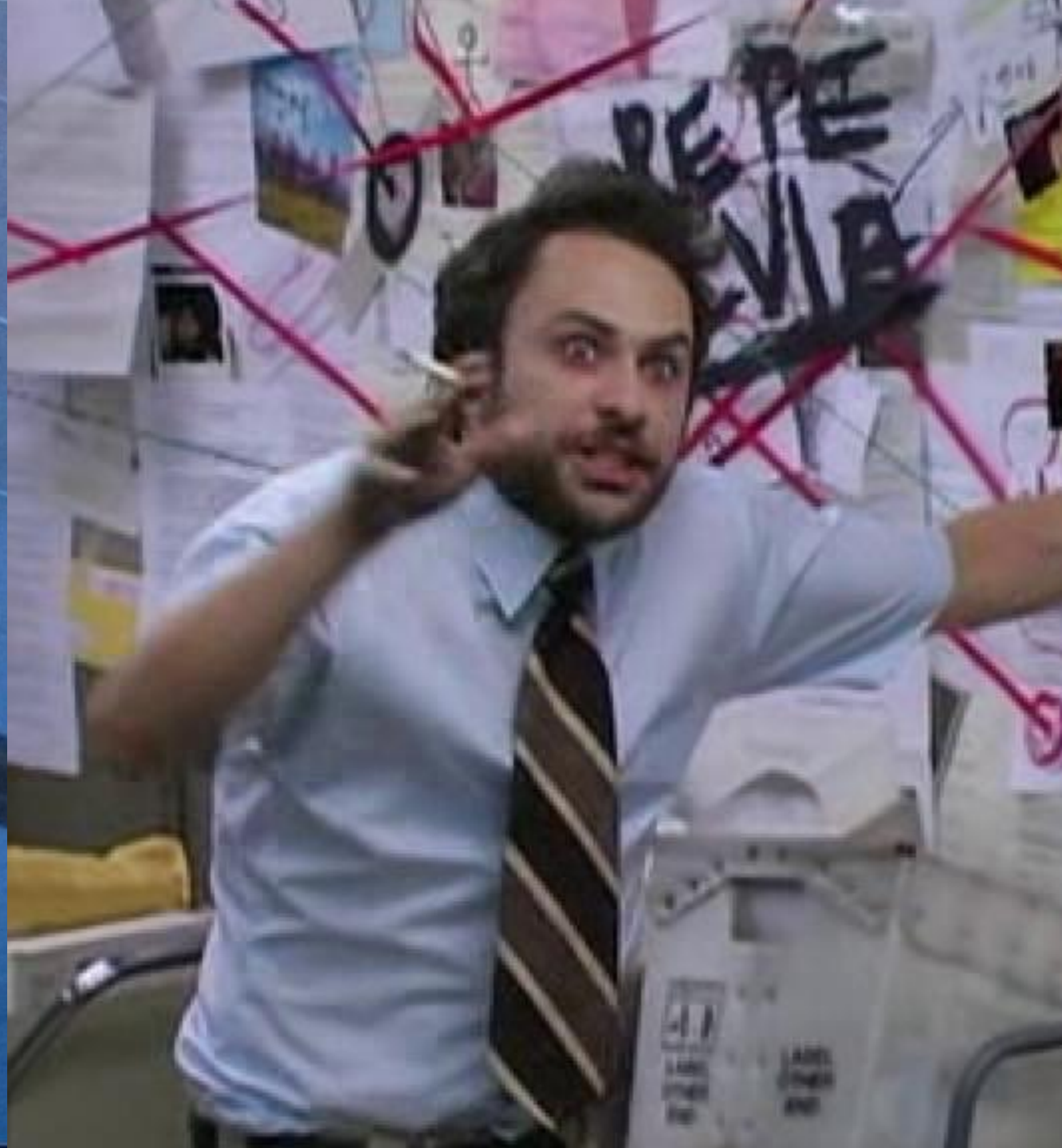
Intune

- OIB
- Enrolment restrictions
- Enrolment notifications
- Conditional launch

Exchange Online

- Automatic email forwarding
- Shared account sign-in
- PowerShell for EXO users
- Direct Send
- **If 3rd party gateway used, accept only from it**


Dev
New-InboundConnectorMimecast.ps1
scripts > New-InboundConnectorMimecast.ps1
1 New-InboundConnector `
2 -Name "Inbound from Mimecast" `
3 -ConnectorType Partner `
4 -SenderDomains * `
5 -SenderIPAddresses 193.7.204.0/24,193.7.205.0/24,195.130.
6 -RestrictDomainsToIPAddresses $true `
7 -RequireTls $true `
8 -Enabled $true
develop* 57↓ 01↑ 0 0 Spaces: 2 UTF-8 { } PowerShell



About me

- Practice Lead – Microsoft Security, Threatscape
- Author – Defender stuff, Packt
- Instructor – Defender stuff, LinkedIn
- Organiser – M365 Security & Compliance User Group