Inova
SOLUTIONS

Welcome

Grab a coffee.

We'll begin shortly!

Improve your M365 Secure Score

Key recommendations for a secure baseline

Presented by: Nestor Diaz 1

Workshop 1/2

Date: 2025-May-28

Your host

Nestor Diaz

Country Manager PR | Inova Solutions

Inova SOLUTIONS

House Rules

- **This session is being recorded** – The recording will be shared after the event.
- **Stable connection recommended** – For the best experience, ensure a reliable internet connection.
- **Mics will be muted** – If you'd like to speak, please raise your hand to request unmute.
- **Hands-on experience!** – Make sure you have the right access and devices to follow along.

Inova Solutions is

Your passport to the cloud!

Inova Solutions is the strongest regional Microsoft Solutions Partner with offices in Curacao, Jamaica, Puerto Rico, Ecuador. In 16 years, we developed ourselves as the largest player for high-end Microsoft solutions across the Caribbean, delivering trusted high-end IT services.

Meet our MDs

Mission

Empowering organizations of all sizes to create business advantages by adopting digital transformation.

Johan Rog

Financial Managing Director

Hans Kruithof

Commercial Managing Director

10 tips to get started with Secure Score

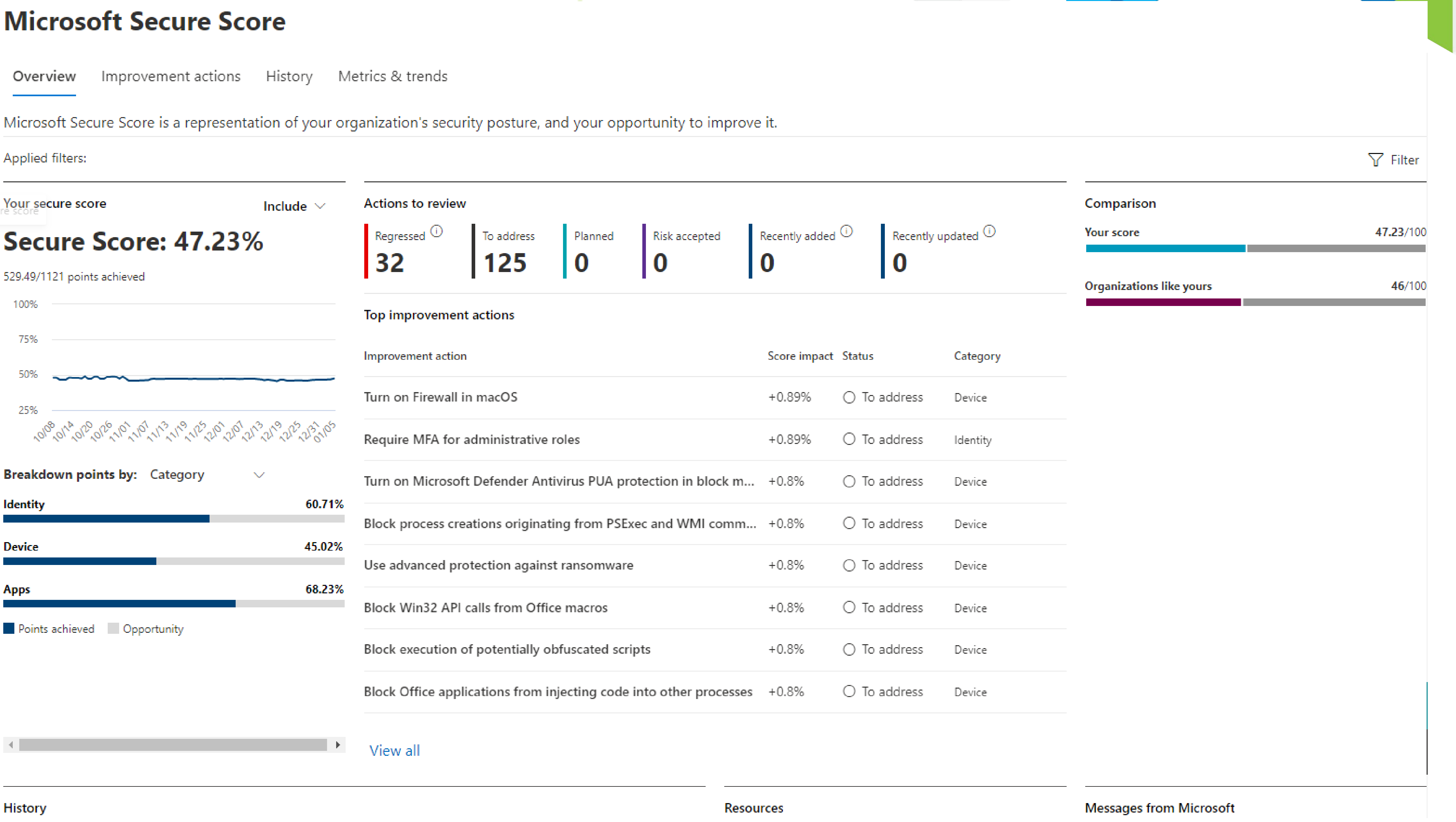
Last session

1. Follow best practice basics
2. Identity best practices
3. Enable Defender for Office 365
4. Safe Attachments
5. Safe Links

Today

6. Disable mail forwarding
7. Enable common attachment filters
8. MailTips
9. Impersonation Protection
10. Teams meeting permissions

When it comes to cybersecurity, the alarm bells are always ringing



Microsoft Secure Score

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

Applied filters:

Your secure score

Secure Score: 47.23%

529.49/1121 points achieved

Breakdown points by: Category

Identity	60.71%
Device	45.02%
Apps	68.23%

■ Points achieved □ Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
32	125	0	0	0	0

Top improvement actions

Improvement action	Score impact	Status	Category
Turn on Firewall in macOS	+0.89%	○ To address	Device
Require MFA for administrative roles	+0.89%	○ To address	Identity
Turn on Microsoft Defender Antivirus PUA protection in block m...	+0.8%	○ To address	Device
Block process creations originating from PSExec and WMI comm...	+0.8%	○ To address	Device
Use advanced protection against ransomware	+0.8%	○ To address	Device
Block Win32 API calls from Office macros	+0.8%	○ To address	Device
Block execution of potentially obfuscated scripts	+0.8%	○ To address	Device
Block Office applications from injecting code into other processes	+0.8%	○ To address	Device

Comparison

Your score	47.23/100
Organizations like yours	46/100

History

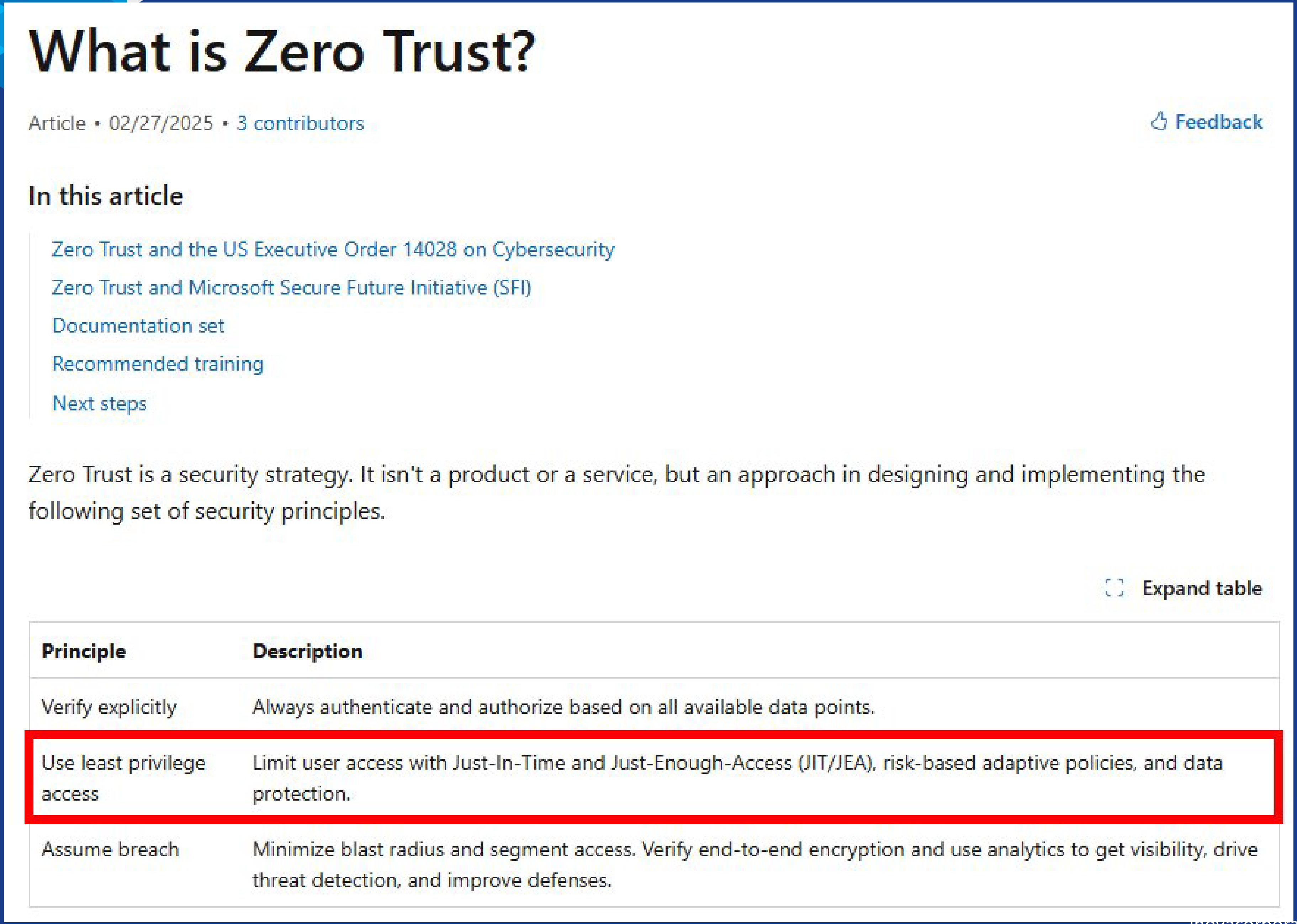
Resources

Messages from Microsoft

1. Best Practice Basics

What are some basic best practices?

1. Follow the principle of least privilege
   A. What is Principle of Least Privilege (POLP)? | CrowdStrike
2. Set up unified audit log (AND MONITOR IT)
   A. `Get-AdminAuditLogConfig | Format-List UnifiedAuditLogIngestionEnabled`
3. Have break glass accounts
   A. Break Glass account – and how to get notified when a Break Glass account is used – Blog - Sonne´s Cloud
   B. Manage emergency access admin accounts - Microsoft Entra ID | Microsoft Learn



What is Zero Trust?

Article • 02/27/2025 • 3 contributors

In this article

Zero Trust is a security strategy. It isn't a product or a service, but an approach in designing and implementing the following set of security principles.

Principle	Description
Verify explicitly	Always authenticate and authorize based on all available data points.
Use least privilege access	Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
Assume breach	Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

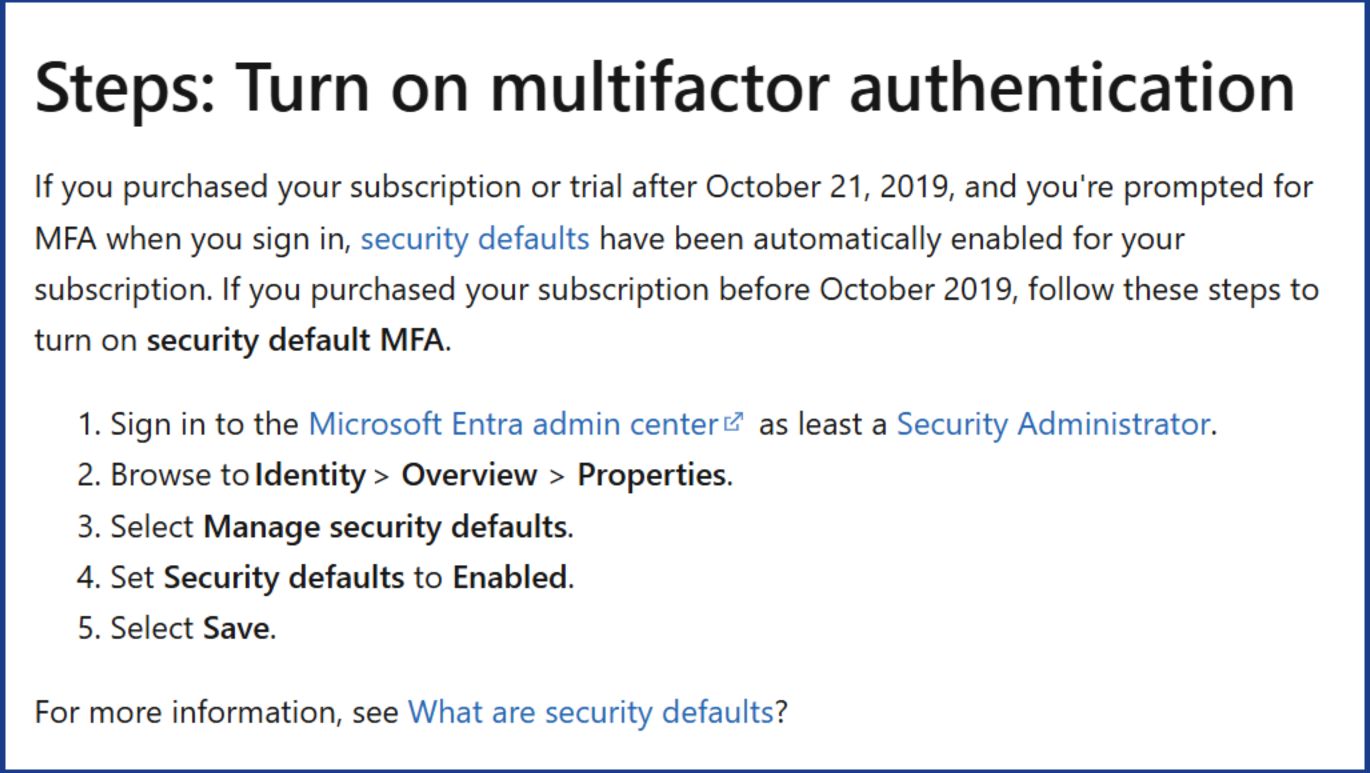
2. Identity Best Practices

Identity Best practices

1. Multi factor Authentication
   A. Set up for admins or all users?
   1. What are your additional auth factors?
      A. Email, phone, authenticator
      B. Phishing resistant: FIDO, Passkey, Windows Hello
   2. Security defaults (all licenses) vs Conditional Access (Entra ID P1)
   3. Remember your break glass accounts
2. Password Expiration

Your MFA Options: Security Defaults

[Providing a default level of security in Microsoft Entra ID - Microsoft Entra | Microsoft Learn]



Steps: Turn on multifactor authentication

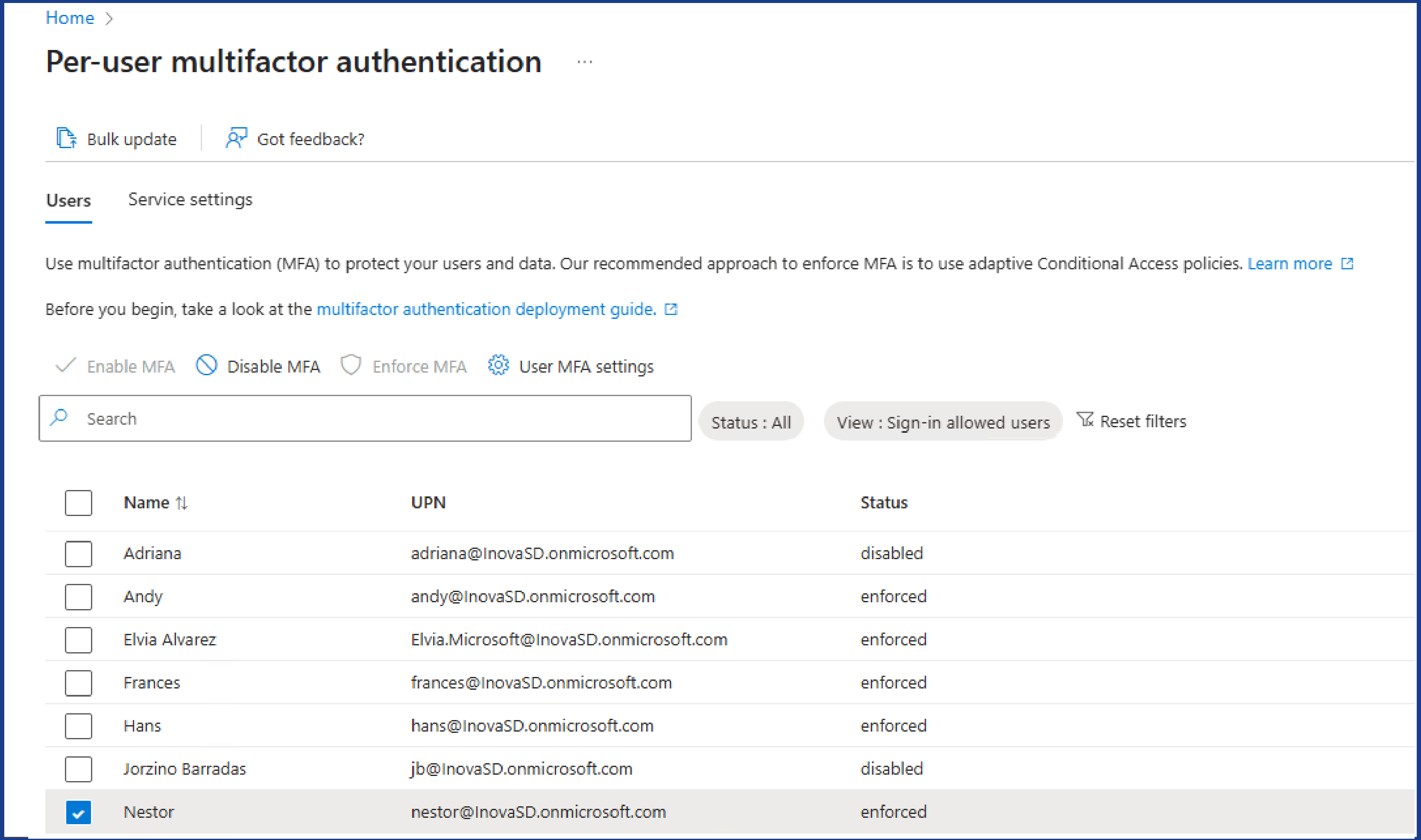
If you purchased your subscription or trial after October 21, 2019, and you're prompted for MFA when you sign in, security defaults have been automatically enabled for your subscription. If you purchased your subscription before October 2019, follow these steps to turn on **security default MFA**.

1. Sign in to the Microsoft Entra admin center as least a Security Administrator.
2. Browse to **Identity** > **Overview** > **Properties**.
3. Select **Manage security defaults**.
4. Set **Security defaults** to **Enabled**.
5. Select **Save**.

For more information, see What are security defaults?

Your MFA Options: Conditional Access

Start by ensuring Per-user MFA is off



Home >

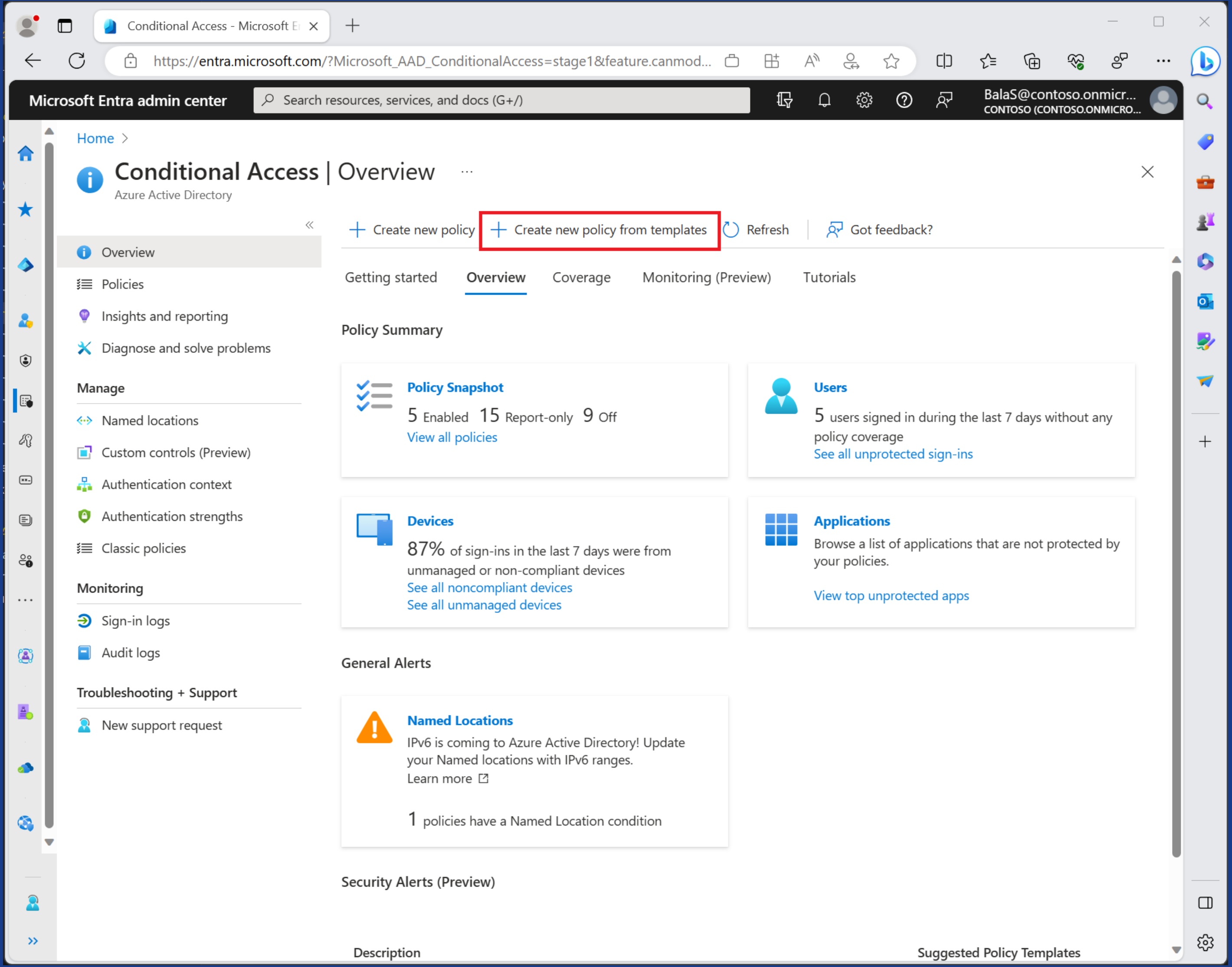
Per-user multifactor authentication ···

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

Before you begin, take a look at the multifactor authentication deployment guide.

☐	Name ⇅	UPN	Status
☐	Adriana	adriana@InovaSD.onmicrosoft.com	disabled
☐	Andy	andy@InovaSD.onmicrosoft.com	enforced
☐	Elvia Alvarez	Elvia.Microsoft@InovaSD.onmicrosoft.com	enforced
☐	Frances	frances@InovaSD.onmicrosoft.com	enforced
☐	Hans	hans@InovaSD.onmicrosoft.com	enforced
☐	Jorzino Barradas	jb@InovaSD.onmicrosoft.com	disabled
☑	Nestor	nestor@InovaSD.onmicrosoft.com	enforced

Your MFA Options: Conditional Access



Conditional Access - Microsoft E
https://entra.microsoft.com/?Microsoft_AAD_ConditionalAccess=stage1&feature.canmod...
Microsoft Entra admin center
Search resources, services, and docs (G+/)
BalaS@contoso.onmicr...
CONTOSO (CONTOSO.ONMICRO...
Home >
Conditional Access | Overview
Azure Active Directory
+ Create new policy
+ Create new policy from templates
Refresh
Got feedback?
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Authentication context
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
Troubleshooting + Support
New support request
Getting started
Overview
Coverage
Monitoring (Preview)
Tutorials

Policy Summary

Policy Snapshot
5 Enabled 15 Report-only 9 Off
View all policies

Users
5 users signed in during the last 7 days without any policy coverage
See all unprotected sign-ins

Devices
87% of sign-ins in the last 7 days were from unmanaged or non-compliant devices
See all noncompliant devices
See all unmanaged devices

Applications
Browse a list of applications that are not protected by your policies.
View top unprotected apps

General Alerts

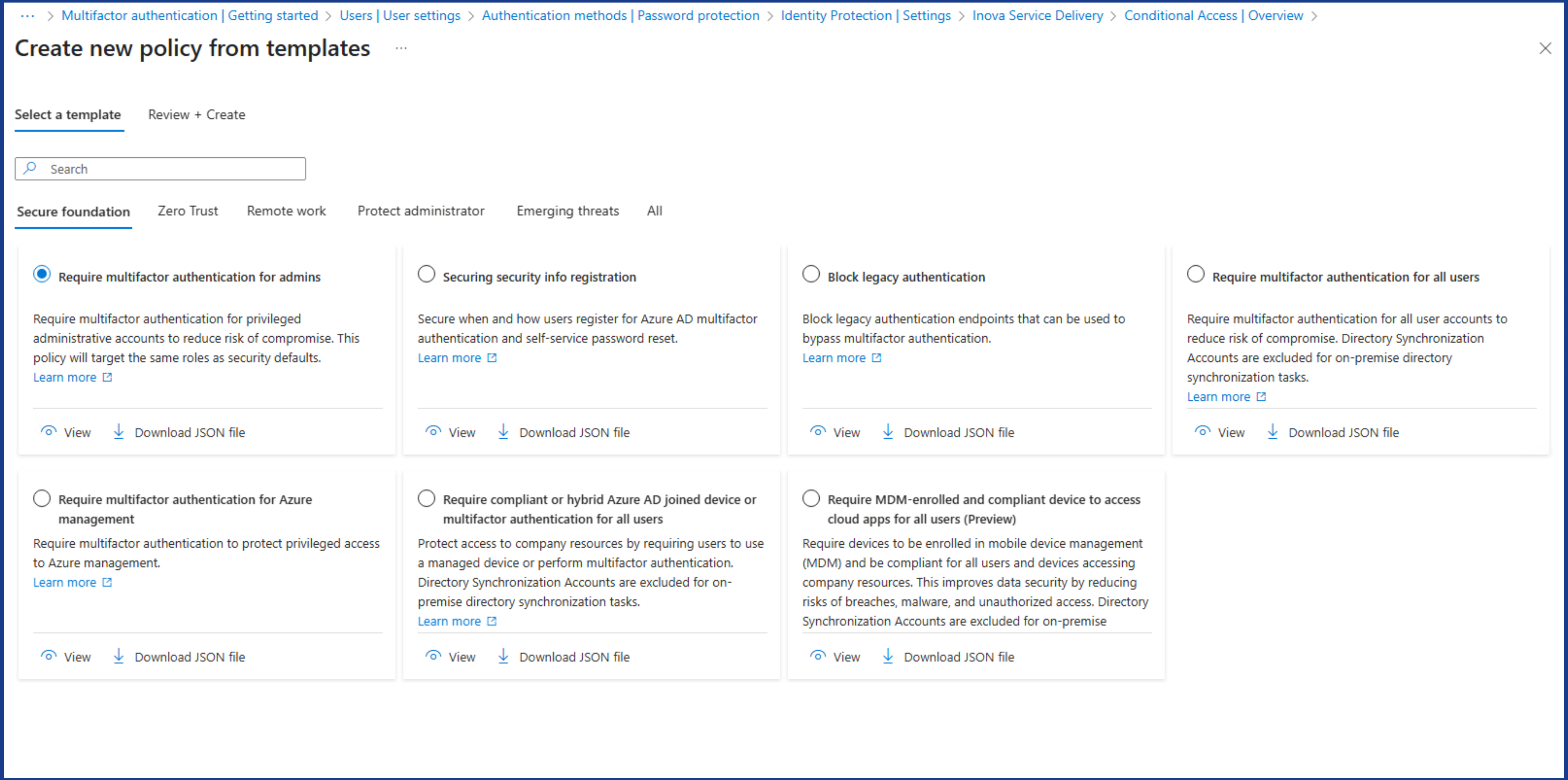
Named Locations
IPv6 is coming to Azure Active Directory! Update your Named locations with IPv6 ranges.
Learn more

1 policies have a Named Location condition

Security Alerts (Preview)

Description
Suggested Policy Templates

Your MFA Options: Conditional Access



··· > Multifactor authentication | Getting started > Users | User settings > Authentication methods | Password protection > Identity Protection | Settings > Inova Service Delivery > Conditional Access | Overview >

Create new policy from templates

Select a template | Review + Create

Search

Secure foundation | Zero Trust | Remote work | Protect administrator | Emerging threats | All

● **Require multifactor authentication for admins**

Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.
Learn more

View | Download JSON file

○ **Securing security info registration**

Secure when and how users register for Azure AD multifactor authentication and self-service password reset.
Learn more

View | Download JSON file

○ **Block legacy authentication**

Block legacy authentication endpoints that can be used to bypass multifactor authentication.
Learn more

View | Download JSON file

○ **Require multifactor authentication for all users**

Require multifactor authentication for all user accounts to reduce risk of compromise. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks.
Learn more

View | Download JSON file

○ **Require multifactor authentication for Azure management**

Require multifactor authentication to protect privileged access to Azure management.
Learn more

View | Download JSON file

○ **Require compliant or hybrid Azure AD joined device or multifactor authentication for all users**

Protect access to company resources by requiring users to use a managed device or perform multifactor authentication. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks.
Learn more

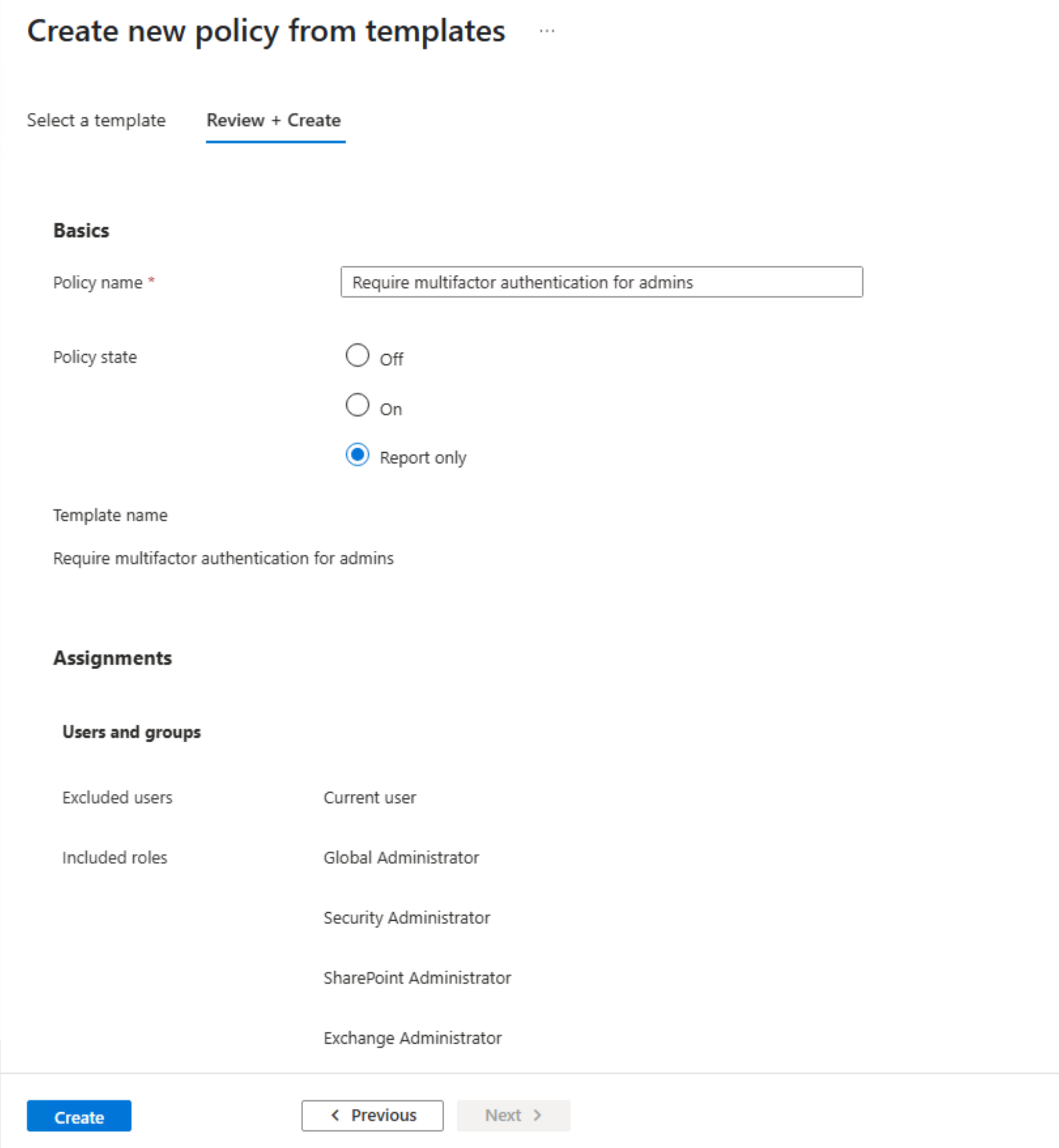
View | Download JSON file

○ **Require MDM-enrolled and compliant device to access cloud apps for all users (Preview)**

Require devices to be enrolled in mobile device management (MDM) and be compliant for all users and devices accessing company resources. This improves data security by reducing risks of breaches, malware, and unauthorized access. Directory Synchronization Accounts are excluded for on-premise

View | Download JSON file

Your MFA Options: Conditional Access



Create new policy from templates ···

Basics

Policy name * Require multifactor authentication for admins

Policy state
○ Off
○ On
● Report only

Template name

Require multifactor authentication for admins

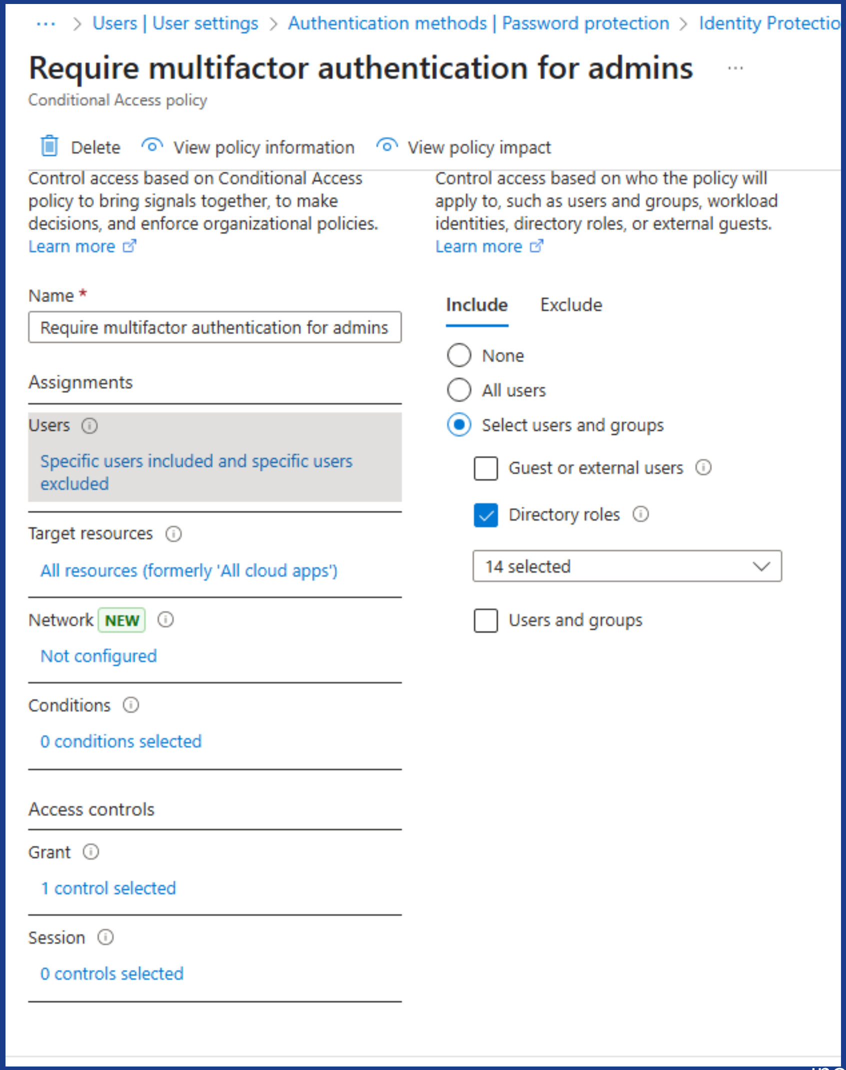
Assignments

Users and groups

Excluded users	Current user
Included roles	Global Administrator Security Administrator SharePoint Administrator Exchange Administrator

Your MFA Options: Conditional Access

[Set up multifactor authentication for users - Microsoft 365 admin | Microsoft Learn]


··· > Users | User settings > Authentication methods | Password protection > Identity Protectio
Delete
View policy information
View policy impact
···

Require multifactor authentication for admins

Conditional Access policy

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

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. Learn more

Name *

Require multifactor authentication for admins

Assignments

Users ⓘ
Specific users included and specific users excluded

Target resources ⓘ
All resources (formerly 'All cloud apps')

Network NEW ⓘ
Not configured

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
1 control selected

Session ⓘ
0 controls selected

Include | Exclude

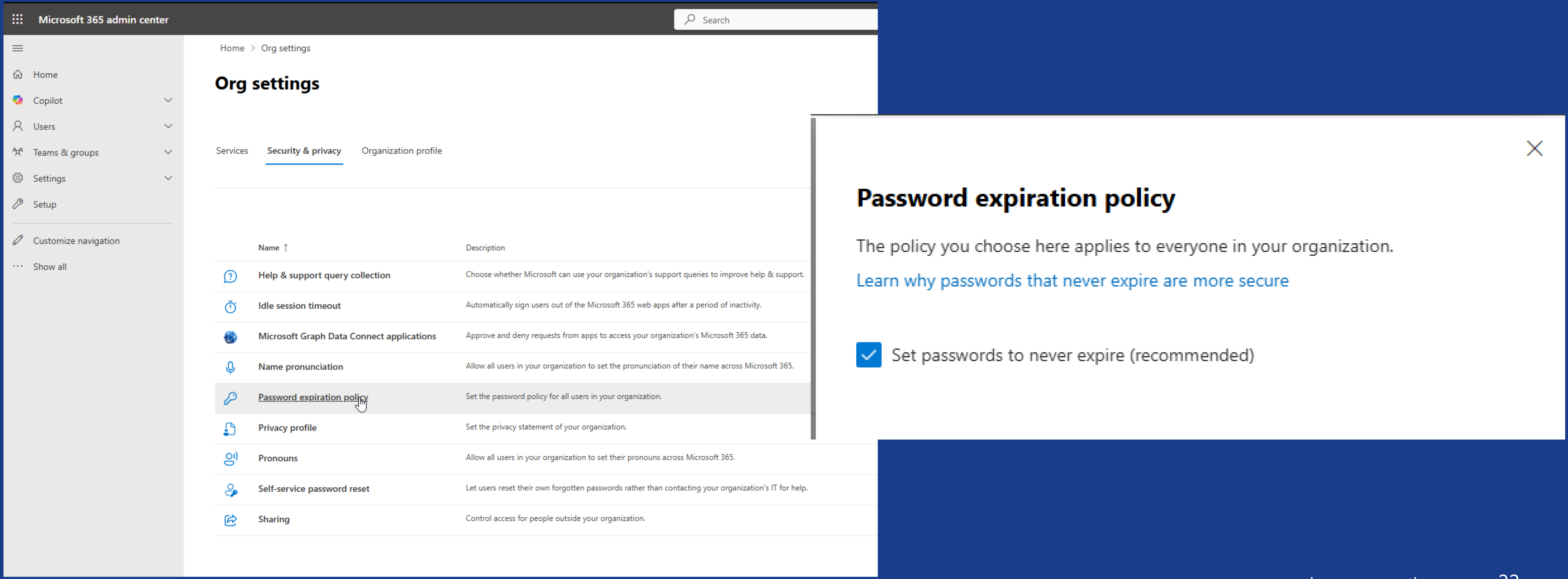
○ None
○ All users
● Select users and groups
- □ Guest or external users ⓘ
- ☑ Directory roles ⓘ
- 14 selected
- □ Users and groups

Identity Best practices

1. Multi factor Authentication
   - A. Set up for admins or all users?
   - B. What are your additional auth factors?
     - A. Email, phone, authenticator
     - B. Phishing resistant: FIDO, Passkey, Windows Hello
   - C. Security defaults (all licenses) vs Conditional Access (Entra ID P1)
   - D. Remember your break glass accounts
2. Password Expiration

Password Expiration Policy

https://go.microsoft.com/fwlink/p/?linkid=2072756



Home > Org settings

Org settings

Services | Security & privacy | Organization profile

Name ↑	Description
Help & support query collection	Choose whether Microsoft can use your organization's support queries to improve help & support.
Idle session timeout	Automatically sign users out of the Microsoft 365 web apps after a period of inactivity.
Microsoft Graph Data Connect applications	Approve and deny requests from apps to access your organization's Microsoft 365 data.
Name pronunciation	Allow all users in your organization to set the pronunciation of their name across Microsoft 365.
Password expiration policy	Set the password policy for all users in your organization.
Privacy profile	Set the privacy statement of your organization.
Pronouns	Allow all users in your organization to set their pronouns across Microsoft 365.
Self-service password reset	Let users reset their own forgotten passwords rather than contacting your organization's IT for help.
Sharing	Control access for people outside your organization.

Password expiration policy

The policy you choose here applies to everyone in your organization.

Learn why passwords that never expire are more secure

☑ Set passwords to never expire (recommended)

3. Enable Defender for Office 365

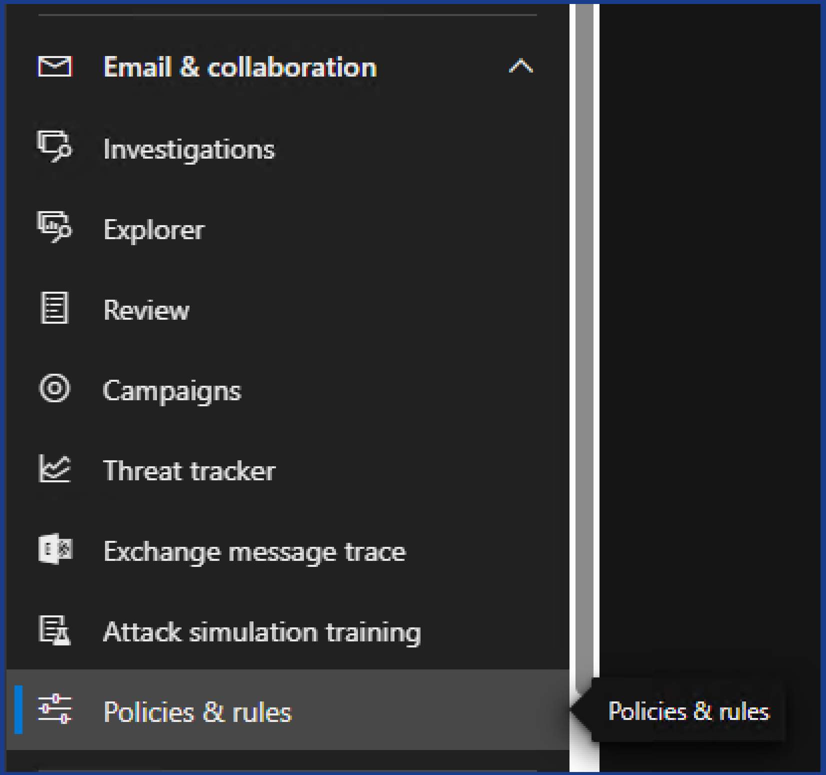
What is Defender for Office 365?

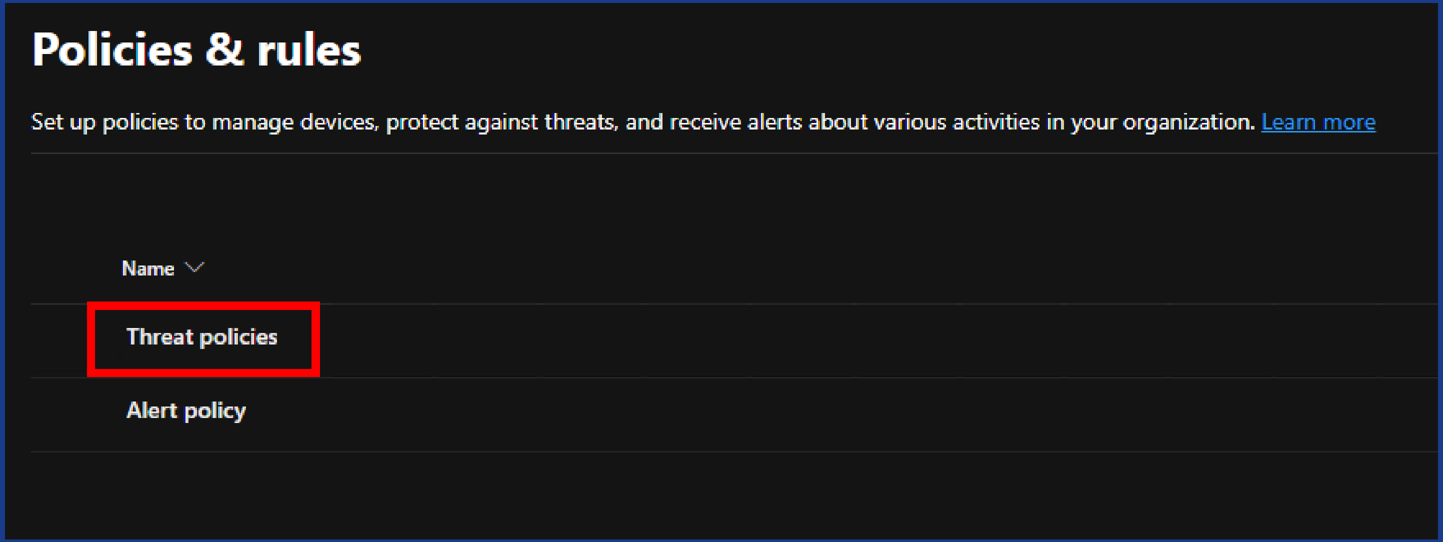
1. Add-on that protects against threats in email, links (URLS), file attachments, and collaboration tools.
   A. Why do I need Microsoft Defender for Office 365? - Microsoft Defender for Office 365 | Microsoft Learn
2. Must be configured; not on by default

4. Create a Safe Attachments policy

Turn on DfO365: Safe Attachments

https://security.microsoft.com/safeattachmentv2



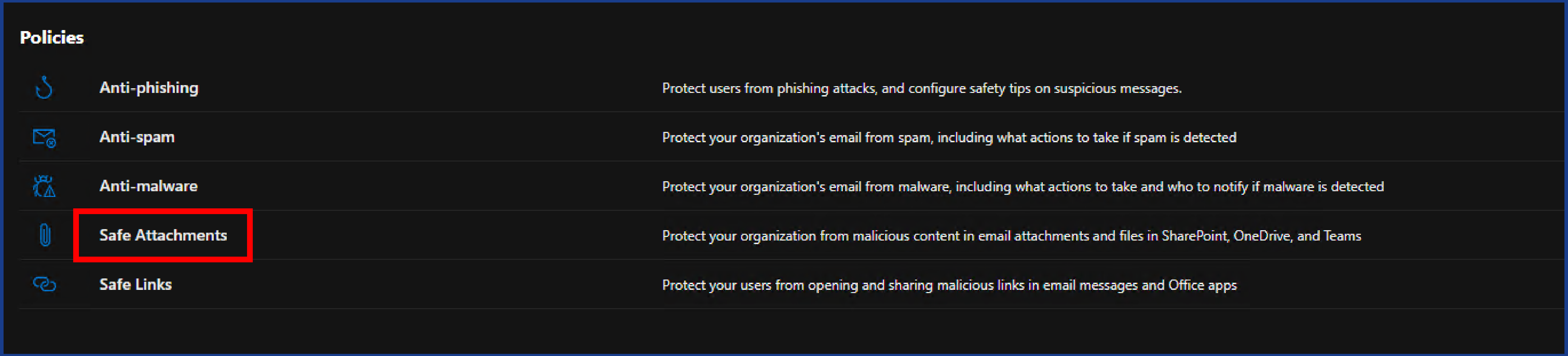


Policies & rules

Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization. Learn more

Name
Threat policies
Alert policy

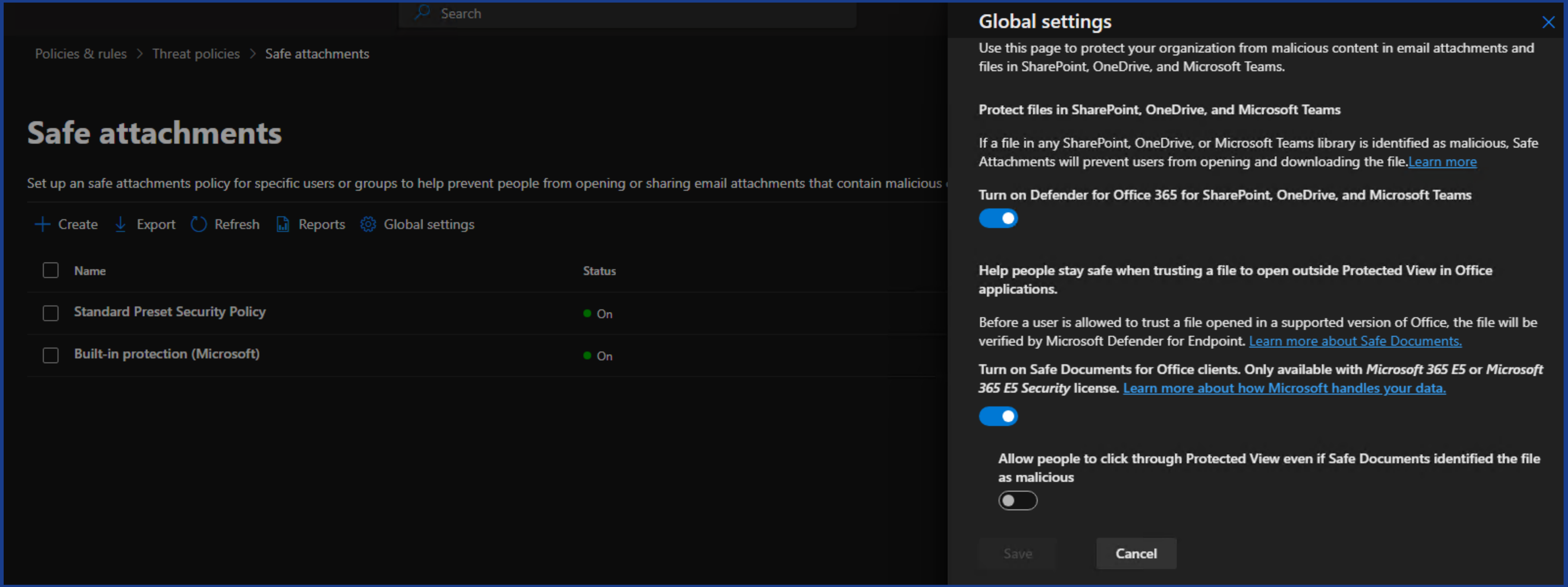
Turn on DfO365: Safe Attachments



Policies

Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Turn on DfO365: Safe Attachments



Policies & rules > Threat policies > Safe attachments

Safe attachments

Set up an safe attachments policy for specific users or groups to help prevent people from opening or sharing email attachments that contain malicious

	Name	Status
□	Standard Preset Security Policy	● On
□	Built-in protection (Microsoft)	● On

Global settings

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams.

Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, Safe Attachments will prevent users from opening and downloading the file.Learn more

Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams

On

Help people stay safe when trusting a file to open outside Protected View in Office applications.

Before a user is allowed to trust a file opened in a supported version of Office, the file will be verified by Microsoft Defender for Endpoint. Learn more about Safe Documents.

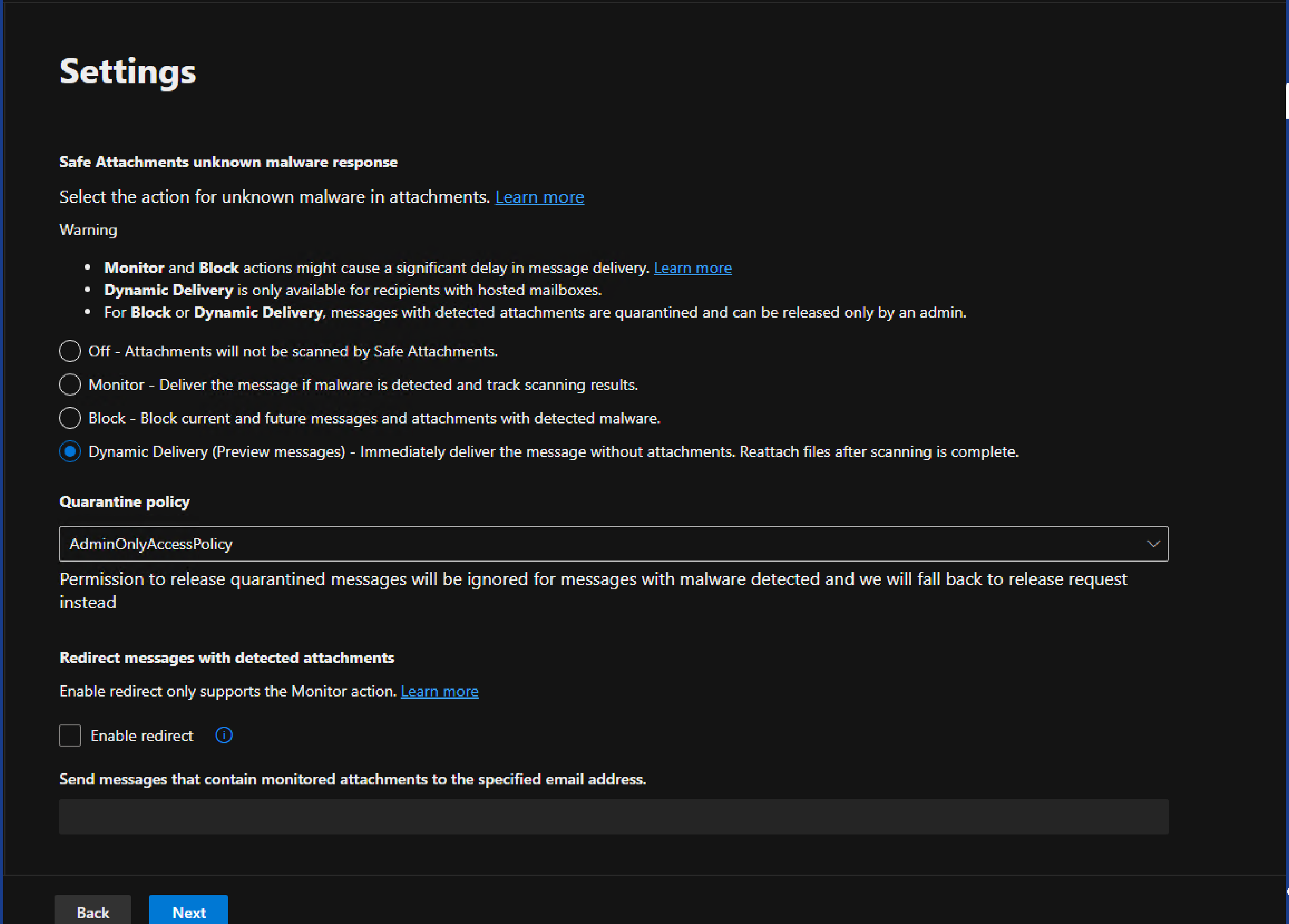
Turn on Safe Documents for Office clients. Only available with *Microsoft 365 E5* or *Microsoft 365 E5 Security* license. Learn more about how Microsoft handles your data.

On

Allow people to click through Protected View even if Safe Documents identified the file as malicious

Off

Turn



Settings

Safe Attachments unknown malware response

Select the action for unknown malware in attachments. Learn more

Warning

- **Monitor** and **Block** actions might cause a significant delay in message delivery. Learn more
- **Dynamic Delivery** is only available for recipients with hosted mailboxes.
- For **Block** or **Dynamic Delivery**, messages with detected attachments are quarantined and can be released only by an admin.

○ Off - Attachments will not be scanned by Safe Attachments.

○ Monitor - Deliver the message if malware is detected and track scanning results.

○ Block - Block current and future messages and attachments with detected malware.

● Dynamic Delivery (Preview messages) - Immediately deliver the message without attachments. Reattach files after scanning is complete.

Quarantine policy

AdminOnlyAccessPolicy

Permission to release quarantined messages will be ignored for messages with malware detected and we will fall back to release request instead

Redirect messages with detected attachments

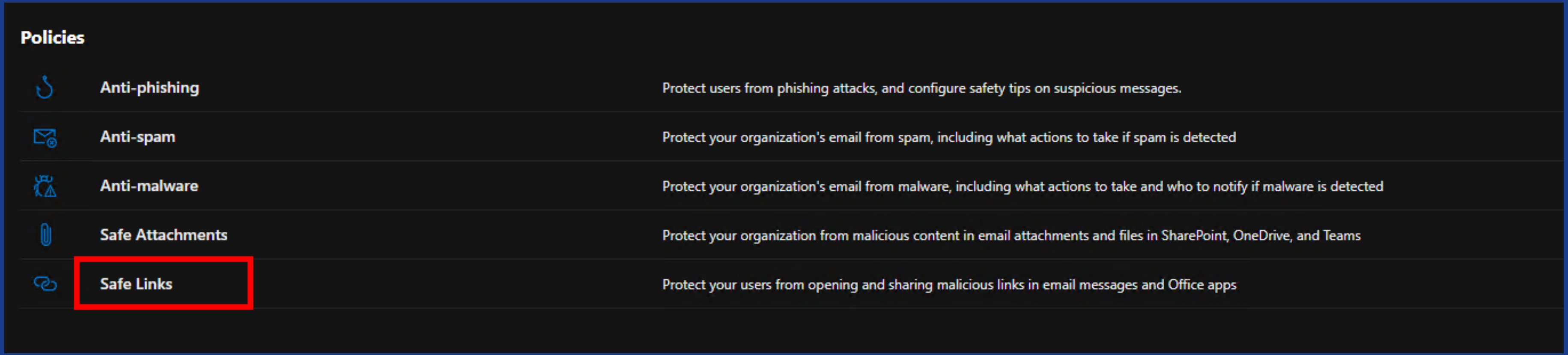
Enable redirect only supports the Monitor action. Learn more

□ Enable redirect

Send messages that contain monitored attachments to the specified email address.

5. Create a Safe Links policy

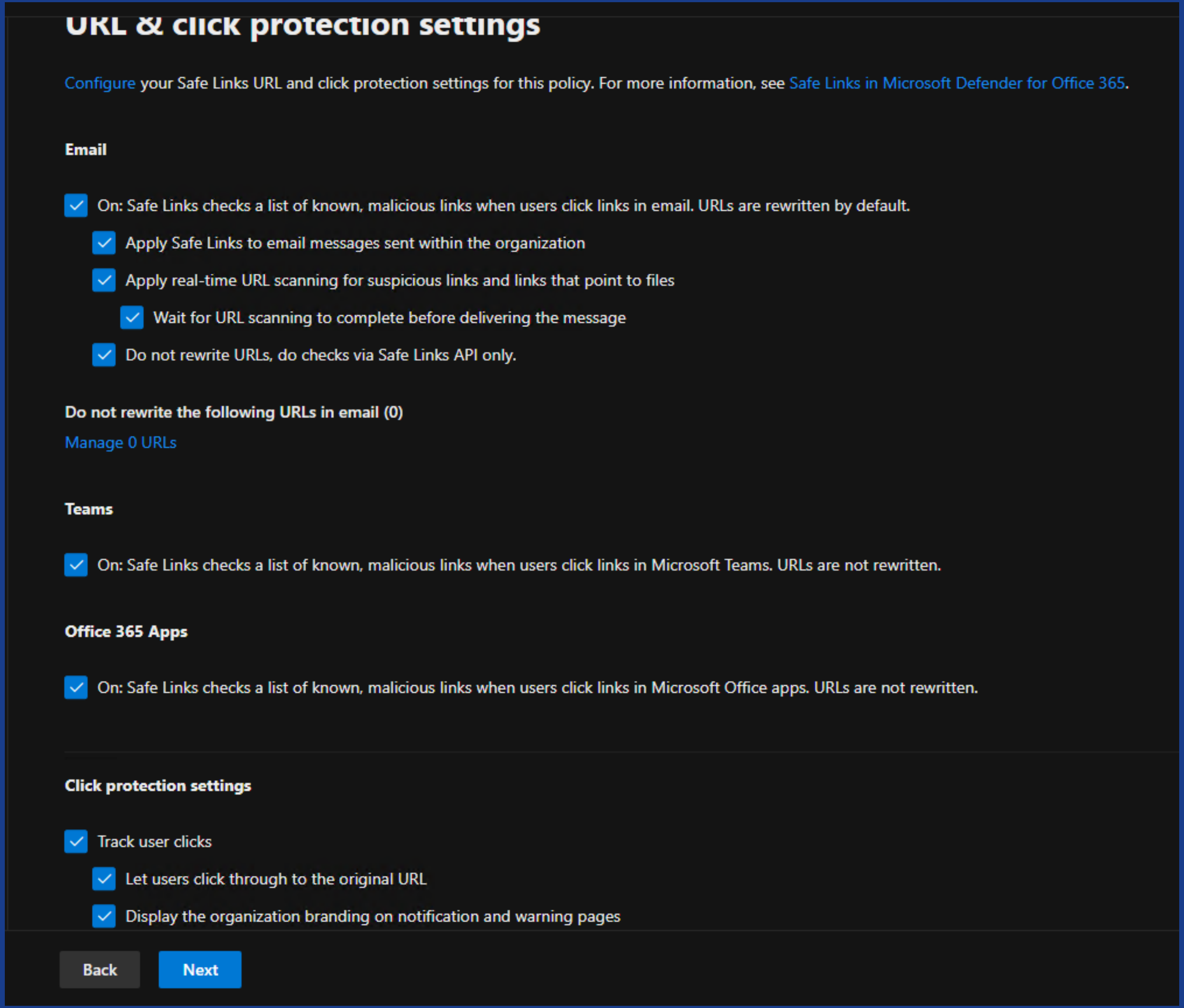
Turn on DfO365: Safe Links



Policies

	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Turn on DfO365: Safe Links



URL & click protection settings

Configure your Safe Links URL and click protection settings for this policy. For more information, see Safe Links in Microsoft Defender for Office 365.

Email

- ☑ On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default.
  - ☑ Apply Safe Links to email messages sent within the organization
  - ☑ Apply real-time URL scanning for suspicious links and links that point to files
    - ☑ Wait for URL scanning to complete before delivering the message
  - ☑ Do not rewrite URLs, do checks via Safe Links API only.

Do not rewrite the following URLs in email (0)

Manage 0 URLs

Teams

☑ On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten.

Office 365 Apps

☑ On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office apps. URLs are not rewritten.

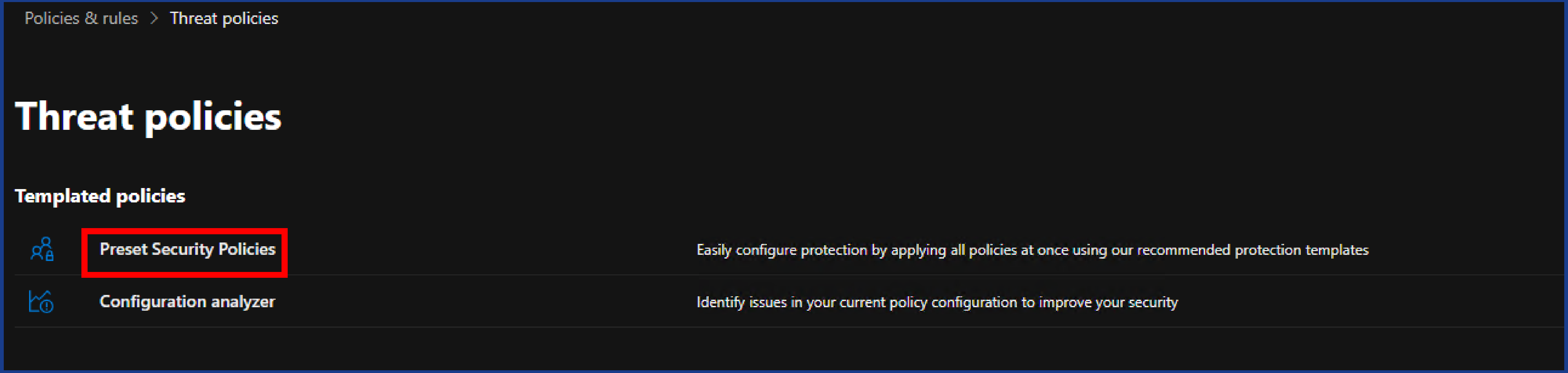
Click protection settings

- ☑ Track user clicks
  - ☑ Let users click through to the original URL
  - ☑ Display the organization branding on notification and warning pages

Turn on DfO365: Preset Security Policies

Inova SOLUTIONS

[Microsoft recommendations for EOP and Defender for Office 365 security settings - Microsoft Defender for Office 365 | Microsoft Learn]



Policies & rules > Threat policies

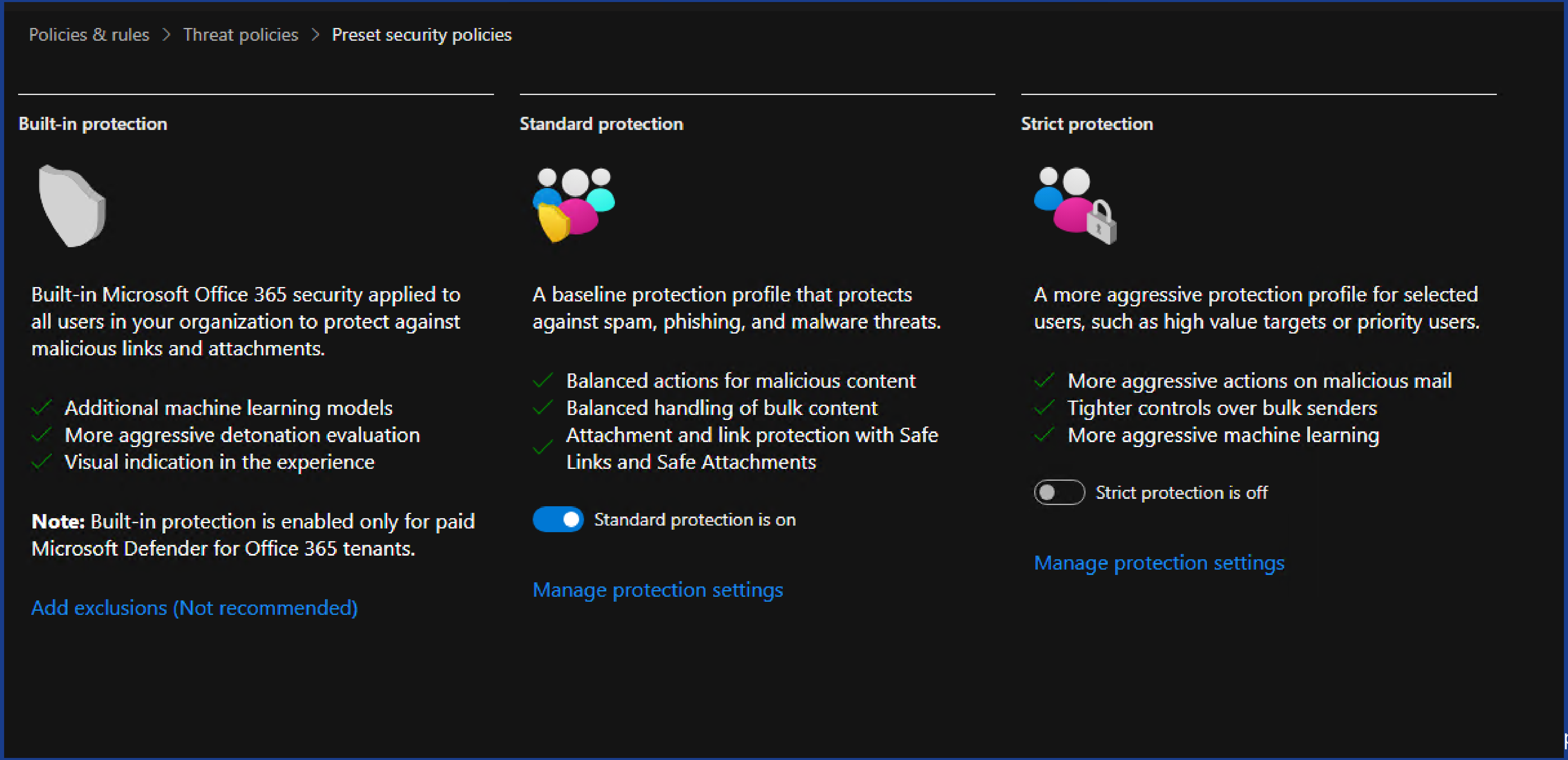
Threat policies

Templated policies

Preset Security Policies	Easily configure protection by applying all policies at once using our recommended protection templates
Configuration analyzer	Identify issues in your current policy configuration to improve your security

Turn on DfO365: Preset Security Policies

[Microsoft recommendations for EOP and Defender for Office 365 security settings - Microsoft Defender for Office 365 | Microsoft Learn]



Policies & rules > Threat policies > Preset security policies

Built-in protection

Built-in Microsoft Office 365 security applied to all users in your organization to protect against malicious links and attachments.

- ✓ Additional machine learning models
- ✓ More aggressive detonation evaluation
- ✓ Visual indication in the experience

Note: Built-in protection is enabled only for paid Microsoft Defender for Office 365 tenants.

Add exclusions (Not recommended)

Standard protection

A baseline protection profile that protects against spam, phishing, and malware threats.

- ✓ Balanced actions for malicious content
- ✓ Balanced handling of bulk content
- ✓ Attachment and link protection with Safe Links and Safe Attachments

● Standard protection is on

Manage protection settings

Strict protection

A more aggressive protection profile for selected users, such as high value targets or priority users.

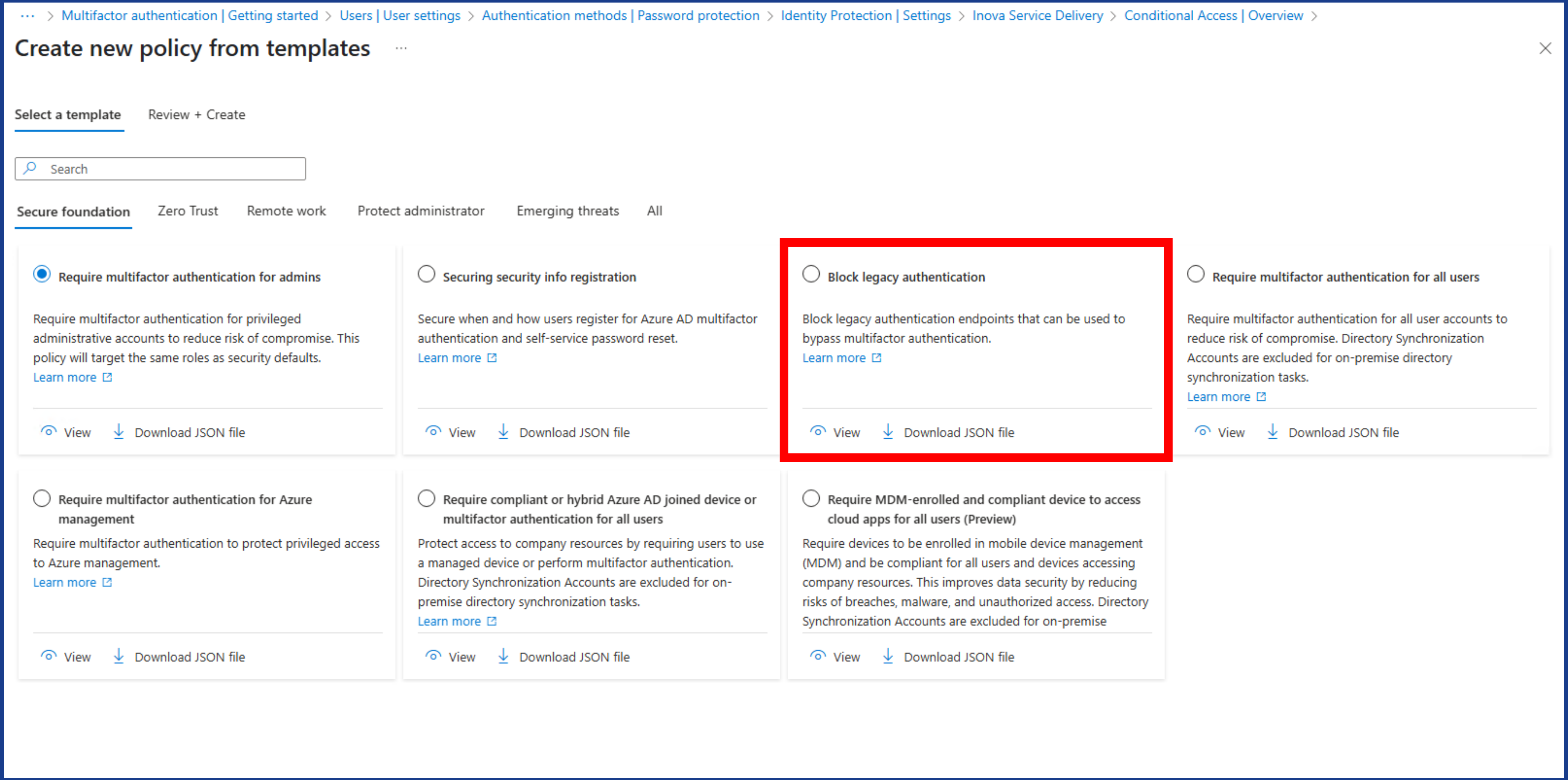
- ✓ More aggressive actions on malicious mail
- ✓ Tighter controls over bulk senders
- ✓ More aggressive machine learning

○ Strict protection is off

Manage protection settings

BONUS: Disable legacy authentication

Disable legacy authentication



··· > Multifactor authentication | Getting started > Users | User settings > Authentication methods | Password protection > Identity Protection | Settings > Inova Service Delivery > Conditional Access | Overview >

Create new policy from templates ···

Select a template   Review + Create

Search

Secure foundation   Zero Trust   Remote work   Protect administrator   Emerging threats   All

● **Require multifactor authentication for admins**

Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.
Learn more

View   Download JSON file

○ **Securing security info registration**

Secure when and how users register for Azure AD multifactor authentication and self-service password reset.
Learn more

View   Download JSON file

○ **Block legacy authentication**

Block legacy authentication endpoints that can be used to bypass multifactor authentication.
Learn more

View   Download JSON file

○ **Require multifactor authentication for all users**

Require multifactor authentication for all user accounts to reduce risk of compromise. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks.
Learn more

View   Download JSON file

○ **Require multifactor authentication for Azure management**

Require multifactor authentication to protect privileged access to Azure management.
Learn more

View   Download JSON file

○ **Require compliant or hybrid Azure AD joined device or multifactor authentication for all users**

Protect access to company resources by requiring users to use a managed device or perform multifactor authentication. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks.
Learn more

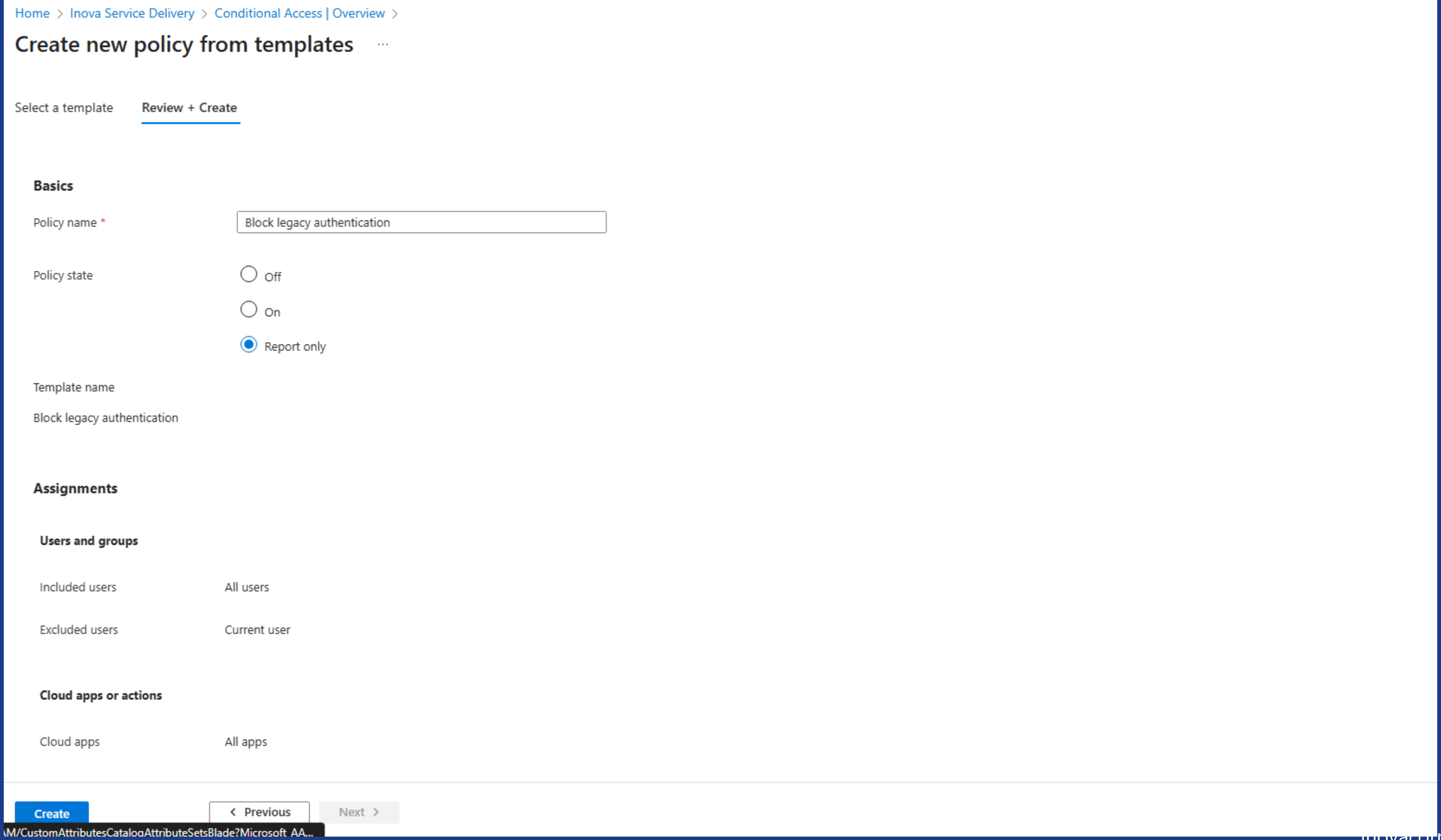
View   Download JSON file

○ **Require MDM-enrolled and compliant device to access cloud apps for all users (Preview)**

Require devices to be enrolled in mobile device management (MDM) and be compliant for all users and devices accessing company resources. This improves data security by reducing risks of breaches, malware, and unauthorized access. Directory Synchronization Accounts are excluded for on-premise

View   Download JSON file

Disable legacy authentication



Home > Inova Service Delivery > Conditional Access | Overview >

Create new policy from templates

Select a template
Review + Create

Basics

Policy name * Block legacy authentication

Policy state
○ Off
○ On
● Report only

Template name

Block legacy authentication

Assignments

Users and groups

Included users All users

Excluded users Current user

Cloud apps or actions

Cloud apps All apps

Create
< Previous
Next >
\M/CustomAttributesCatalogAttributeSetsBlade?Microsoft_AA...

BONUS: Create break glass accounts

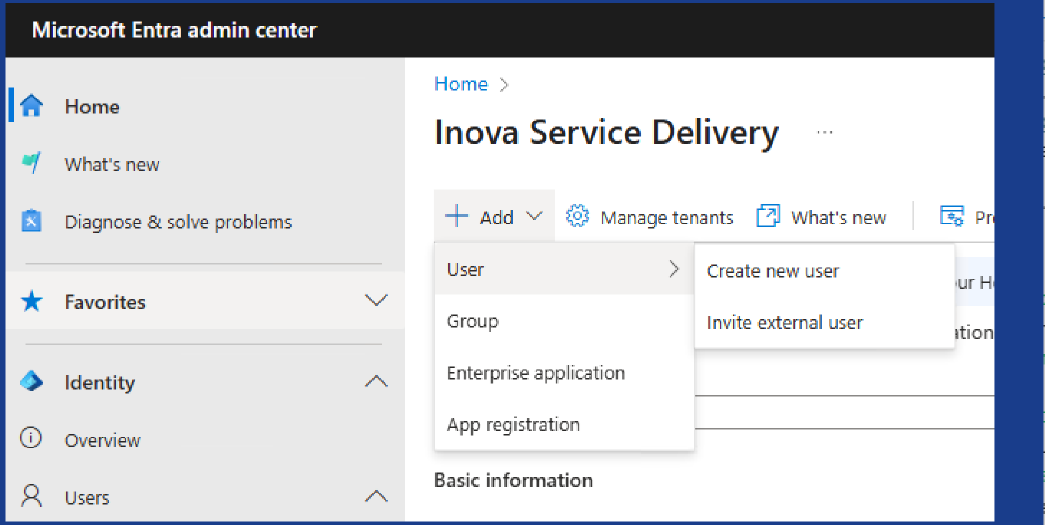
Why would you want break glass accounts?

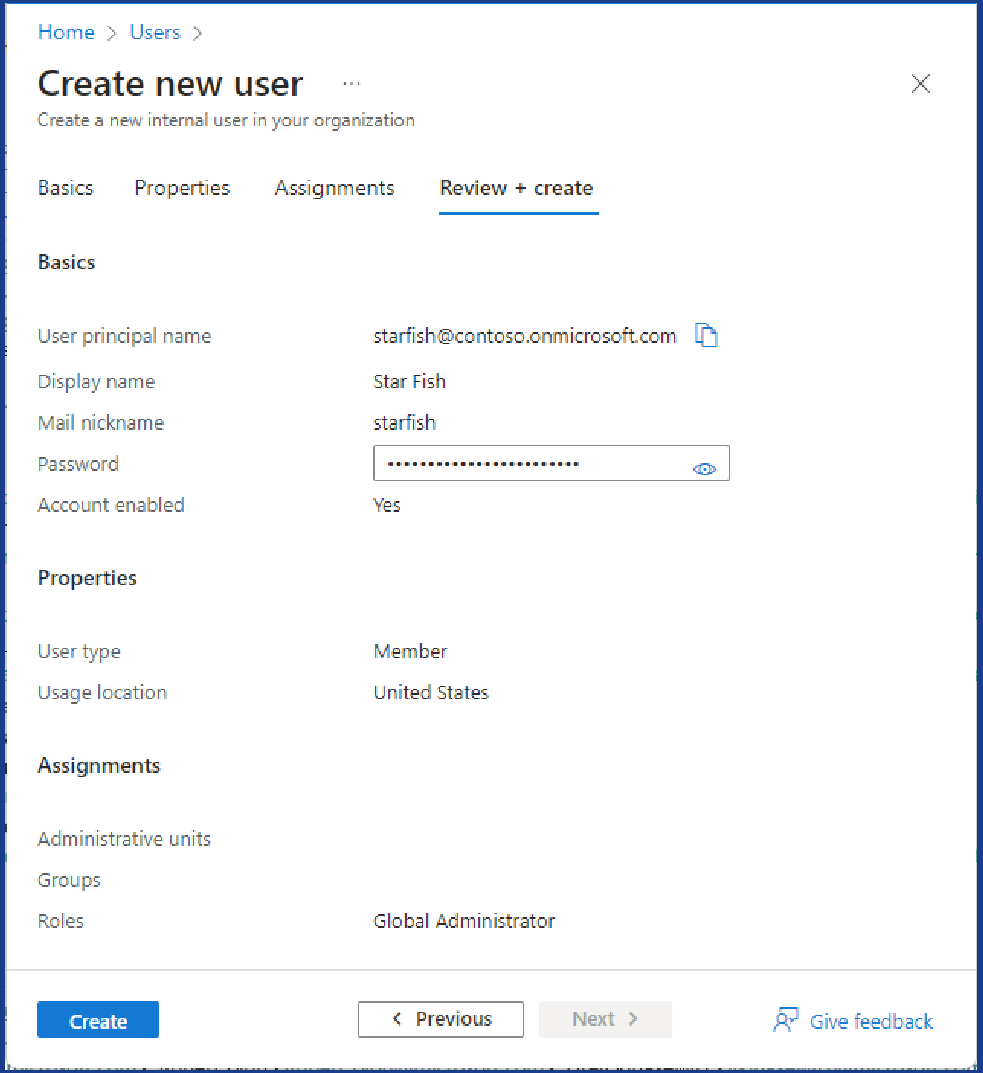
1. Multi factor Authentication methods may be unavailable
   A. Cell phone service unavailable
   B. Phone destroyed/lost/stolen
   C. Configuration mistakes
2. Activated only in an **emergency**, using a predefined process
3. Ideally have at least two break glass accounts
4. Cloud and on-prem break glass should be kept separate

Break Glass key concepts

1. Break glass accounts do not belong to a single person
2. Break glass accounts are **strictly** monitored
3. Can have MFA, but not based on a personal device
   A. MFA devices should be stored in a known, accessible location
   B. FIDO passkey or Certificate-based auth recommended
4. Activation of break glass account should involve both technical and business process steps
5. Credential must not expire or be in scope of automated cleanup due to lack of use.

Break glass account: User creation





Create new user

Create a new internal user in your organization

Basics

User principal name	starfish@contoso.onmicrosoft.com
Display name	Star Fish
Mail nickname	starfish
Password	••••••••••••••••••••••••
Account enabled	Yes

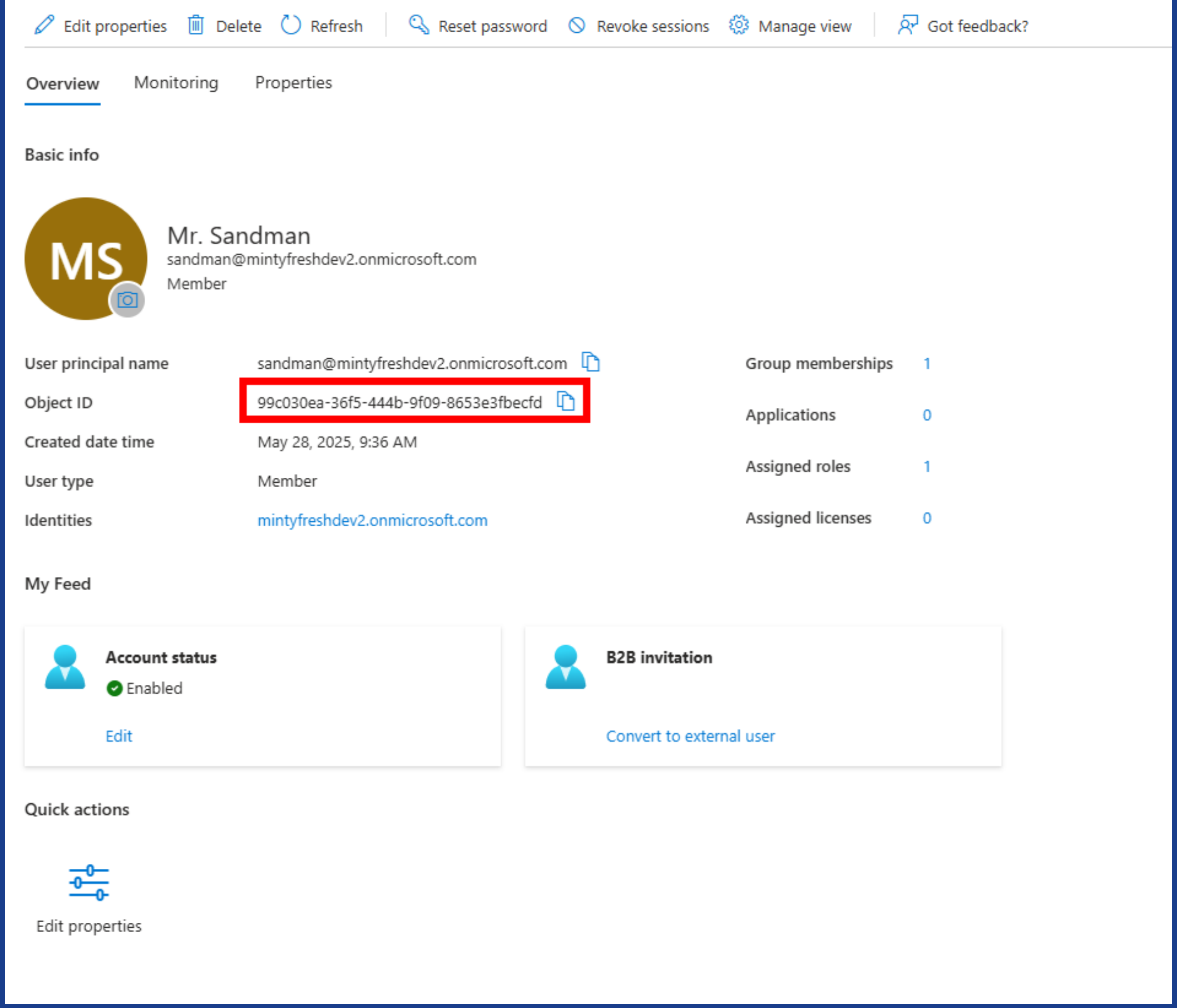
Properties

User type	Member
Usage location	United States

Assignments

Administrative units	
Groups	
Roles	Global Administrator

Break glass account: User creation



Basic info

MS

Mr. Sandman
sandman@mintyfreshdev2.onmicrosoft.com
Member

User principal name	sandman@mintyfreshdev2.onmicrosoft.com	Group memberships	1
Object ID	99c030ea-36f5-444b-9f09-8653e3fbecfd	Applications	0
Created date time	May 28, 2025, 9:36 AM	Assigned roles	1
User type	Member	Assigned licenses	0
Identities	mintyfreshdev2.onmicrosoft.com		

My Feed

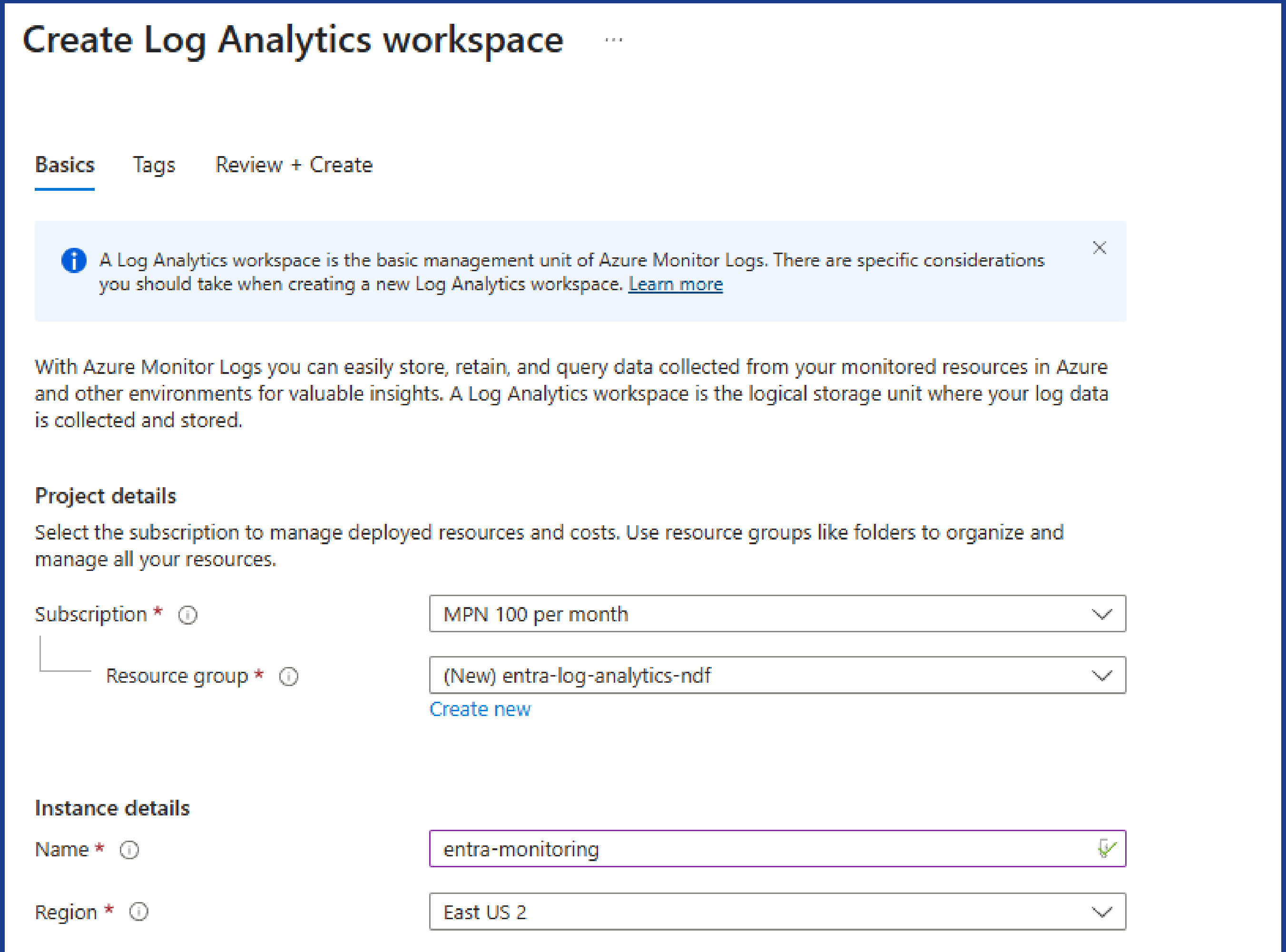
Account status
✓ Enabled
Edit

B2B invitation
Convert to external user

Quick actions

Break glass account: Monitoring

We'll use Azure for this one.



Create Log Analytics workspace ···

Basics | Tags | Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

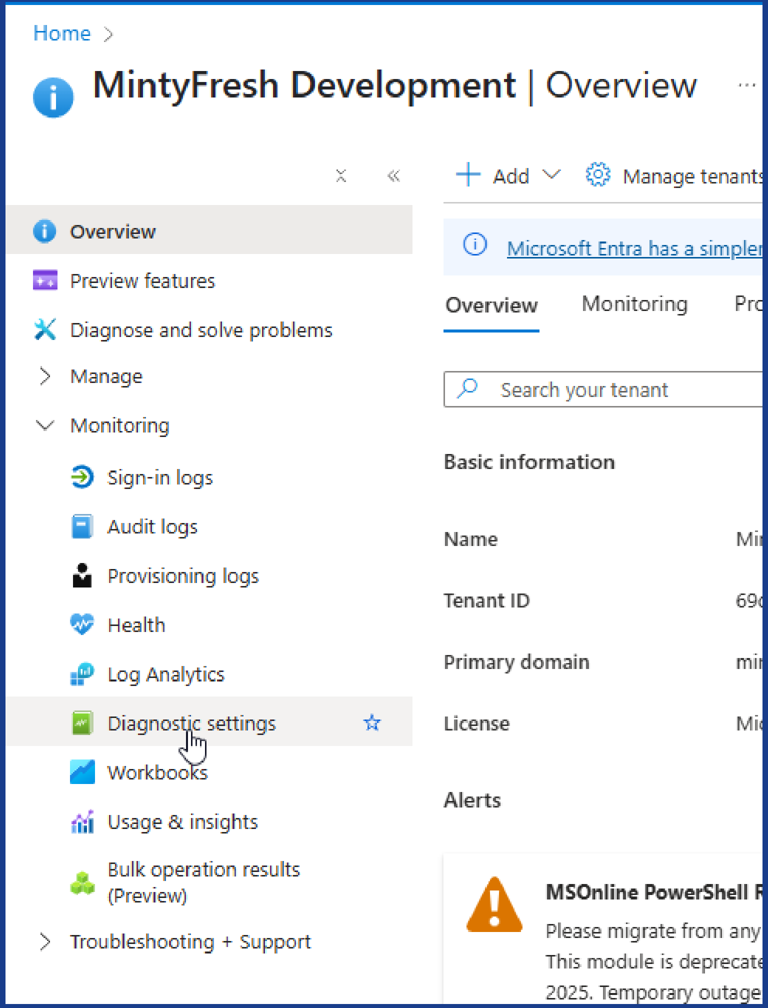
Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	MPN 100 per month
Resource group *	(New) entra-log-analytics-ndf Create new

Instance details

Name *	entra-monitoring
Region *	East US 2



Home >

MintyFresh Development | Overview ···

- Overview
- Preview features
- Diagnose and solve problems
- Manage
- Monitoring
  - Sign-in logs
  - Audit logs
  - Provisioning logs
  - Health
  - Log Analytics
  - Diagnostic settings
  - Workbooks
  - Usage & insights
  - Bulk operation results (Preview)
- Troubleshooting + Support

+ Add | Manage tenants

Microsoft Entra has a simpler

Overview | Monitoring | Pro

Search your tenant

Basic information

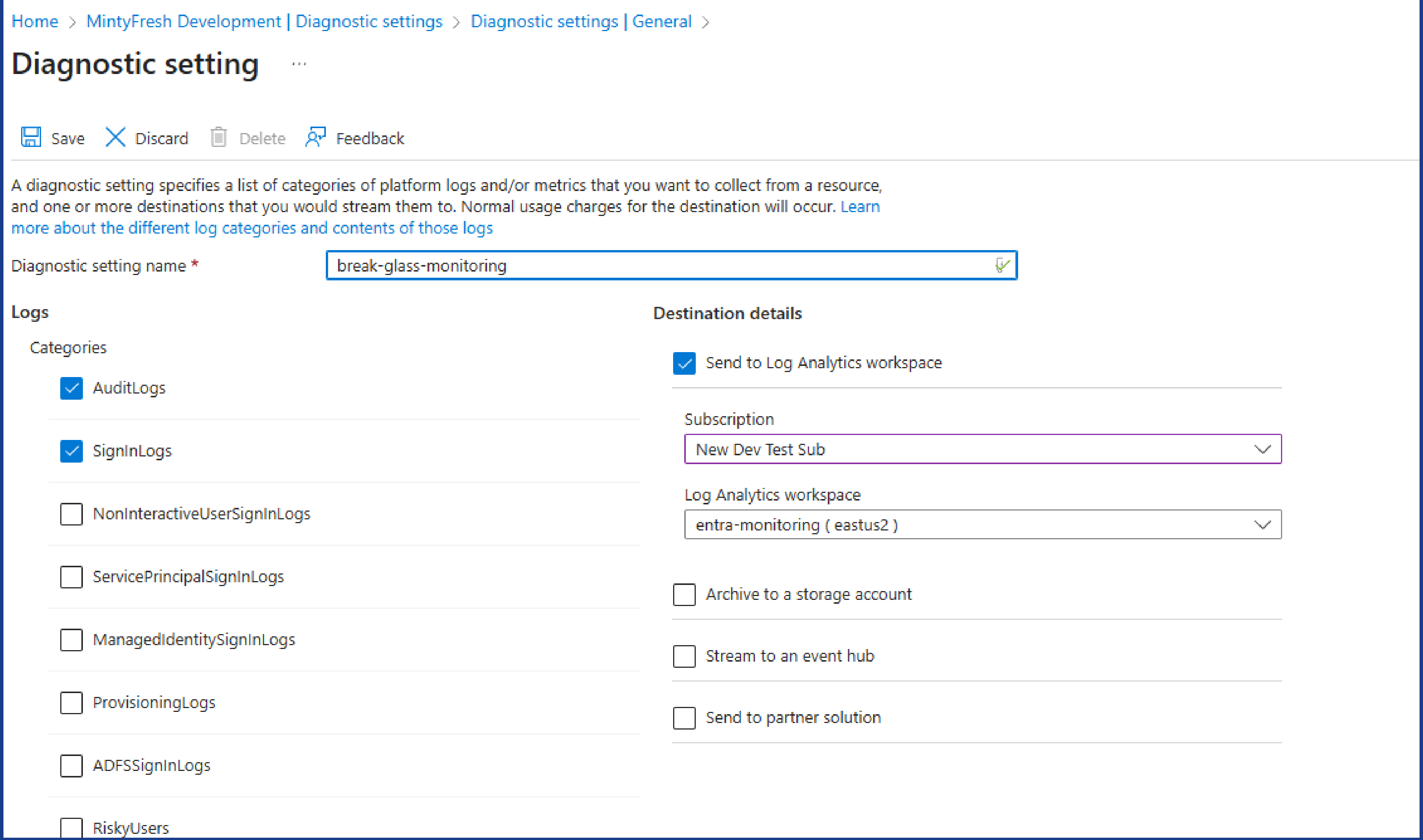
Name	Mi
Tenant ID	69
Primary domain	mi
License	Mi

Alerts

MSOnline PowerShell R

Please migrate from any
This module is deprecate
2025. Temporary outage

Break glass account: Monitoring



Home > MintyFresh Development | Diagnostic settings > Diagnostic settings | General >

Diagnostic setting ...

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name * break-glass-monitoring

Logs

Categories

- ☑ AuditLogs
- ☑ SignInLogs
- □ NonInteractiveUserSignInLogs
- □ ServicePrincipalSignInLogs
- □ ManagedIdentitySignInLogs
- □ ProvisioningLogs
- □ ADFSSignInLogs
- □ RiskyUsers

Destination details

☑ Send to Log Analytics workspace

Subscription: New Dev Test Sub

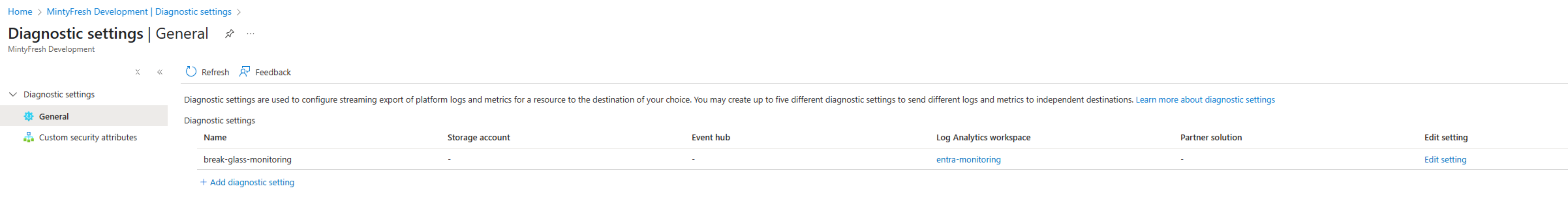
Log Analytics workspace: entra-monitoring (eastus2)

□ Archive to a storage account

□ Stream to an event hub

□ Send to partner solution

Break glass account: Monitoring


Home > MintyFresh Development | Diagnostic settings >
Refresh
Feedback
Diagnostic settings
General
Custom security attributes

Diagnostic settings | General

MintyFresh Development

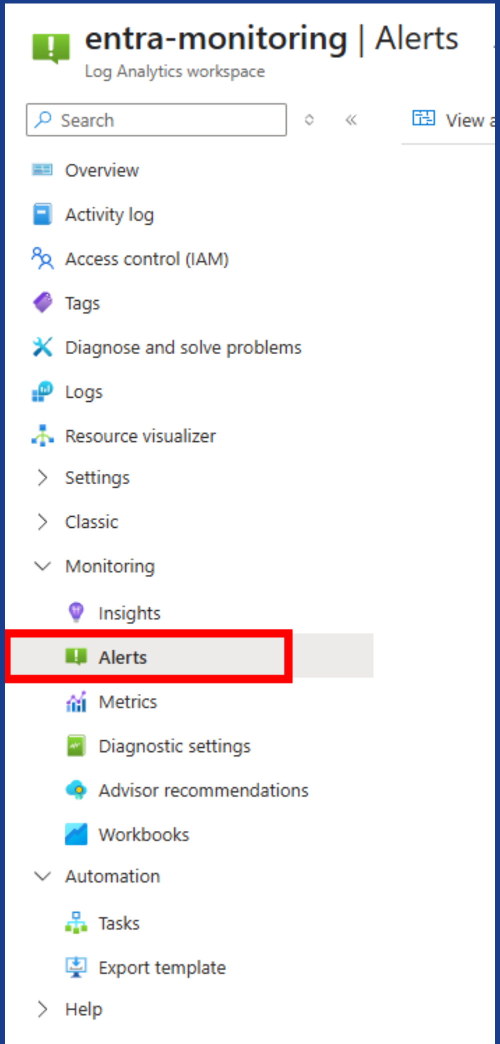
Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings

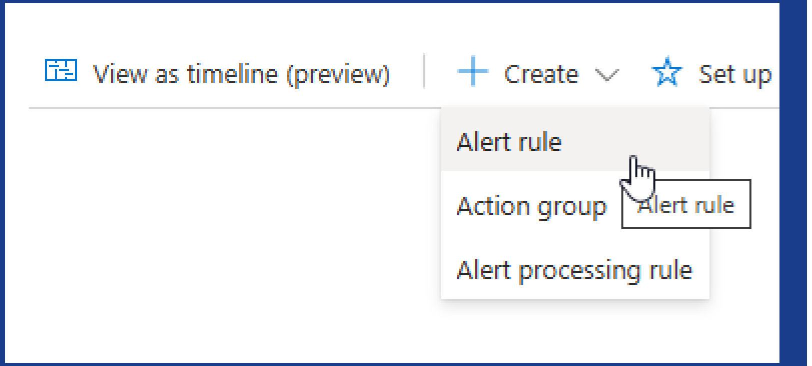
Diagnostic settings

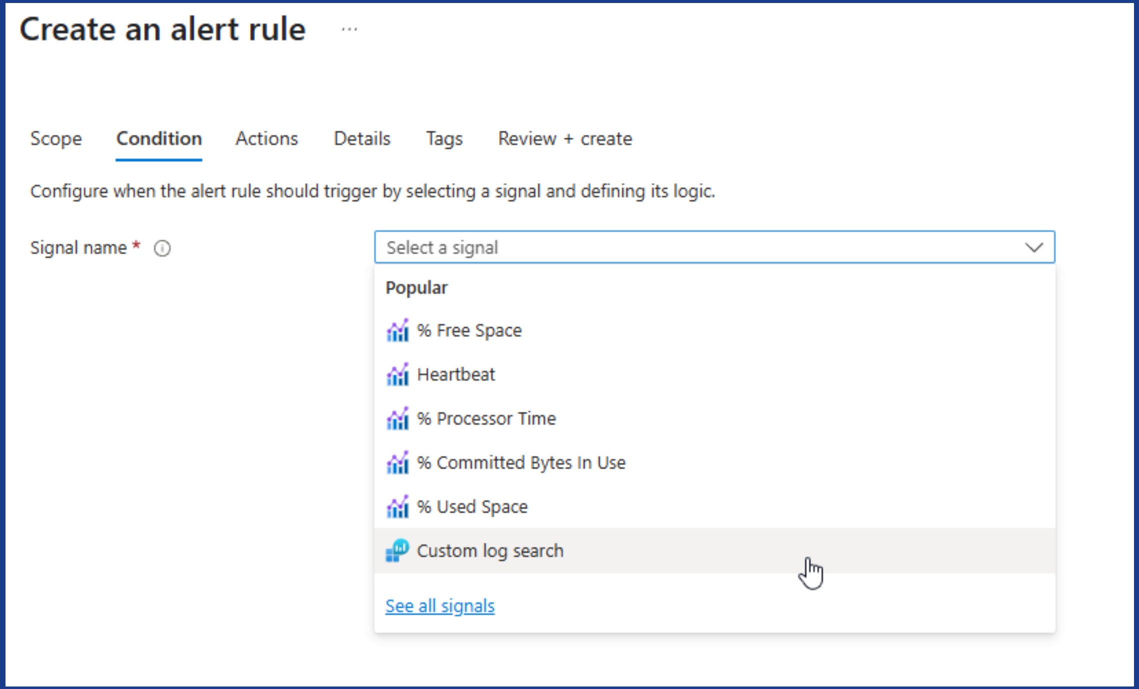
Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
break-glass-monitoring	-	-	entra-monitoring	-	Edit setting

+ Add diagnostic setting

Break glass account: Monitoring



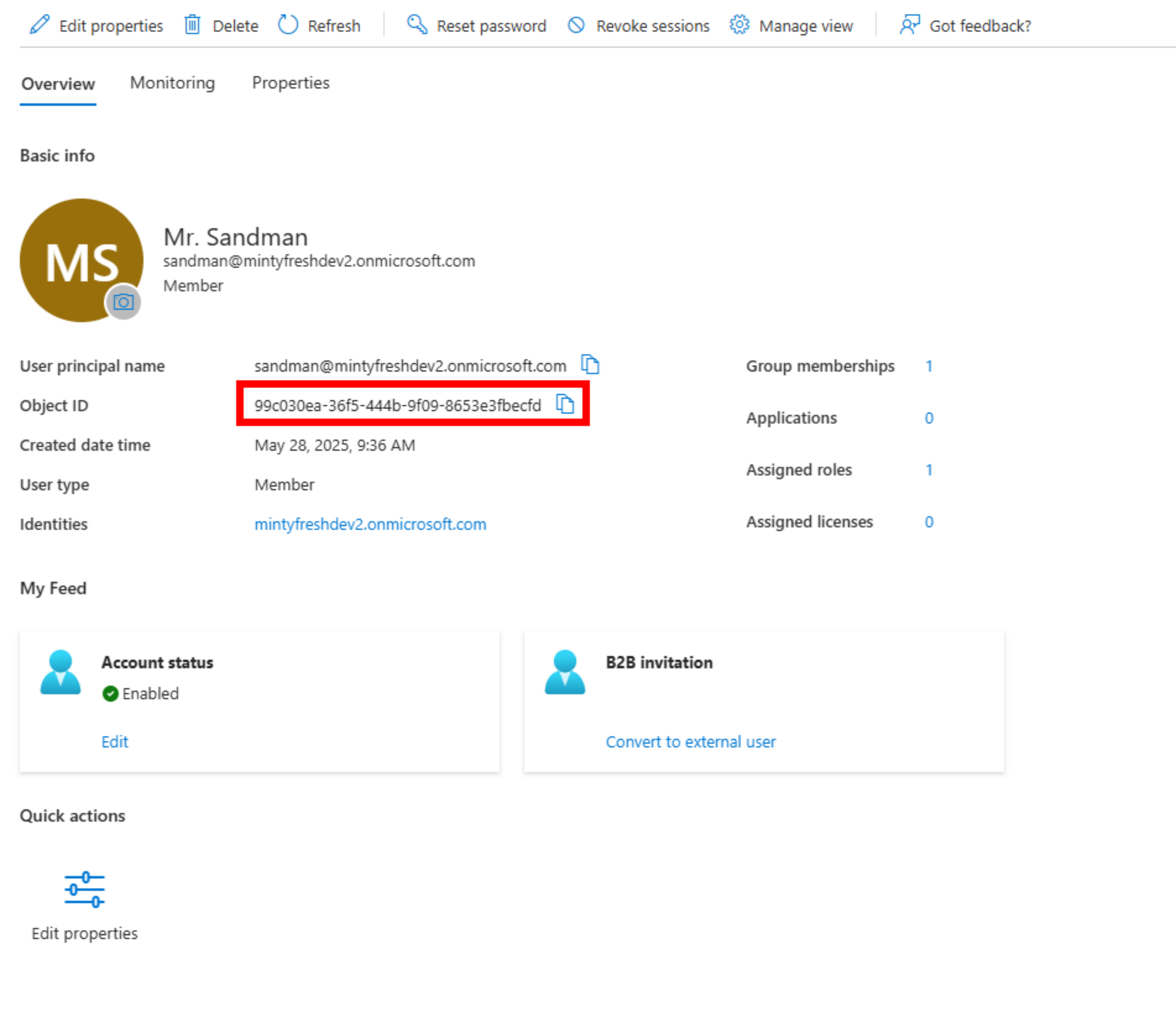




Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name * Select a signal

Break glass account: Monitoring



Basic info

Mr. Sandman
sandman@mintyfreshdev2.onmicrosoft.com
Member

User principal name	sandman@mintyfreshdev2.onmicrosoft.com	Group memberships	1
Object ID	99c030ea-36f5-444b-9f09-8653e3fbecfd	Applications	0
Created date time	May 28, 2025, 9:36 AM	Assigned roles	1
User type	Member	Assigned licenses	0
Identities	mintyfreshdev2.onmicrosoft.com		

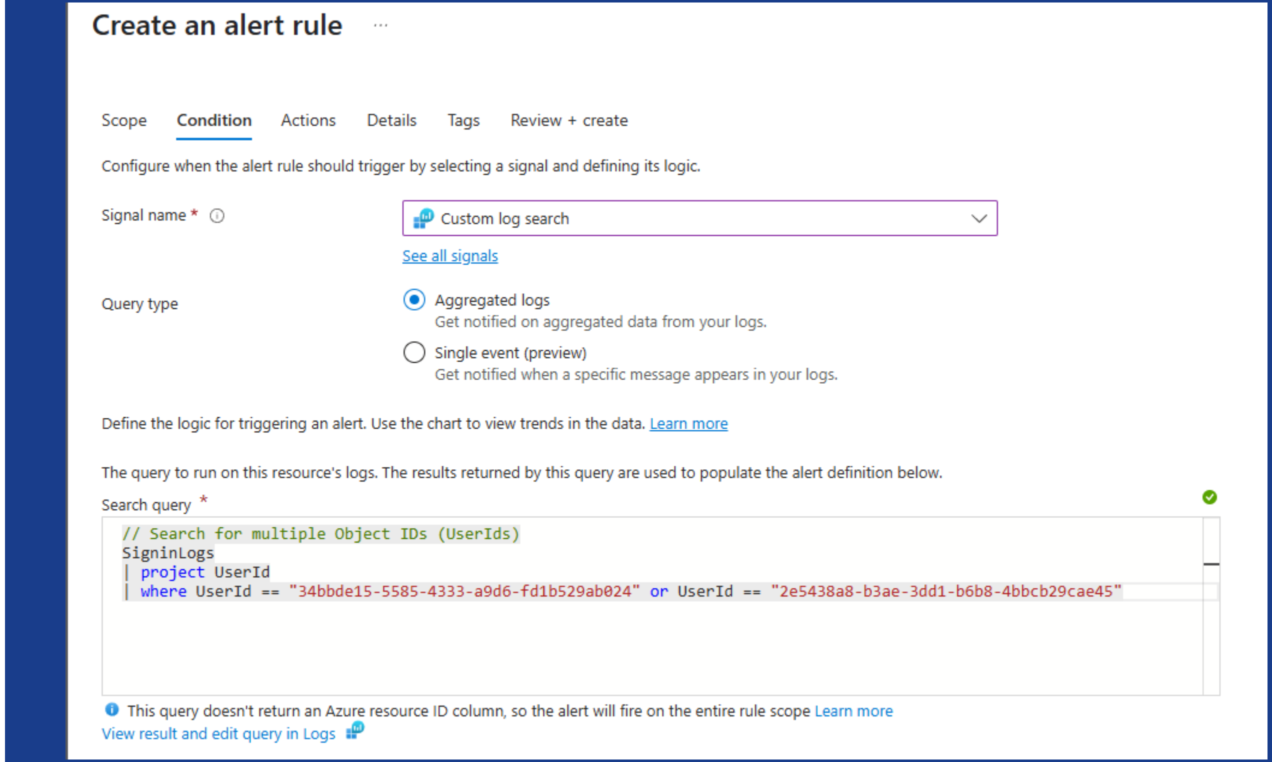
My Feed

Account status
✓ Enabled
Edit

B2B invitation
Convert to external user

Quick actions

Edit properties



Create an alert rule

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name * : Custom log search

See all signals

Query type:
● Aggregated logs
Get notified on aggregated data from your logs.
○ Single event (preview)
Get notified when a specific message appears in your logs.

Define the logic for triggering an alert. Use the chart to view trends in the data. Learn more

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query *

```
// Search for multiple Object IDs (UserIds)
SigninLogs
| project UserId
| where UserId == "34bbde15-5585-4333-a9d6-fd1b529ab024" or UserId == "2e5438a8-b3ae-3dd1-b6b8-4bbcb29cae45"
```

This query doesn't return an Azure resource ID column, so the alert will fire on the entire rule scope Learn more

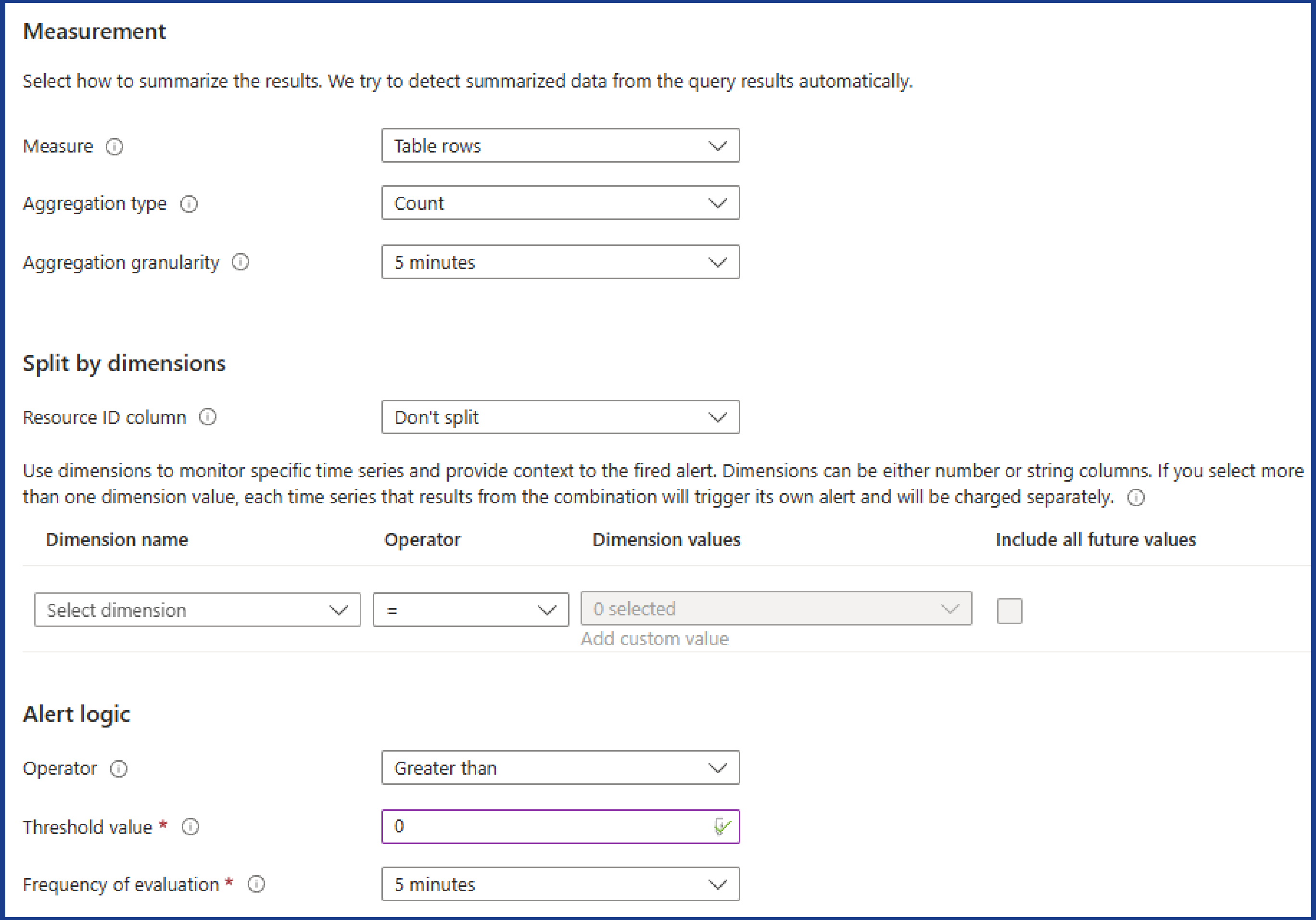
View result and edit query in Logs

Break glass account: Monitoring

```
// Search for multiple Object IDs (UserIds)

SigninLogs
| project UserId
| where UserId == "[Object IID 1]" or UserId ==
"[Object ID 2]"
```

Break glass account: Monitoring



Measurement

Select how to summarize the results. We try to detect summarized data from the query results automatically.

Measure ⓘ	Table rows
Aggregation type ⓘ	Count
Aggregation granularity ⓘ	5 minutes

Split by dimensions

Resource ID column ⓘ	Don't split

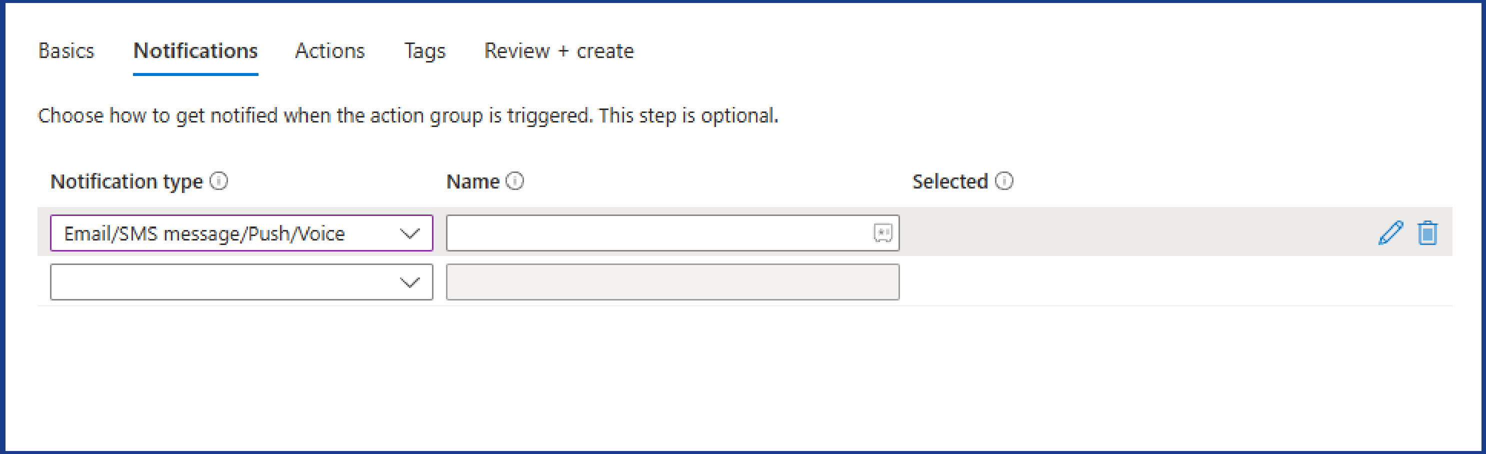
Use dimensions to monitor specific time series and provide context to the fired alert. Dimensions can be either number or string columns. If you select more than one dimension value, each time series that results from the combination will trigger its own alert and will be charged separately. ⓘ

Dimension name	Operator	Dimension values	Include all future values
Select dimension	=	0 selected Add custom value	□

Alert logic

Operator ⓘ	Greater than
Threshold value * ⓘ	0
Frequency of evaluation * ⓘ	5 minutes

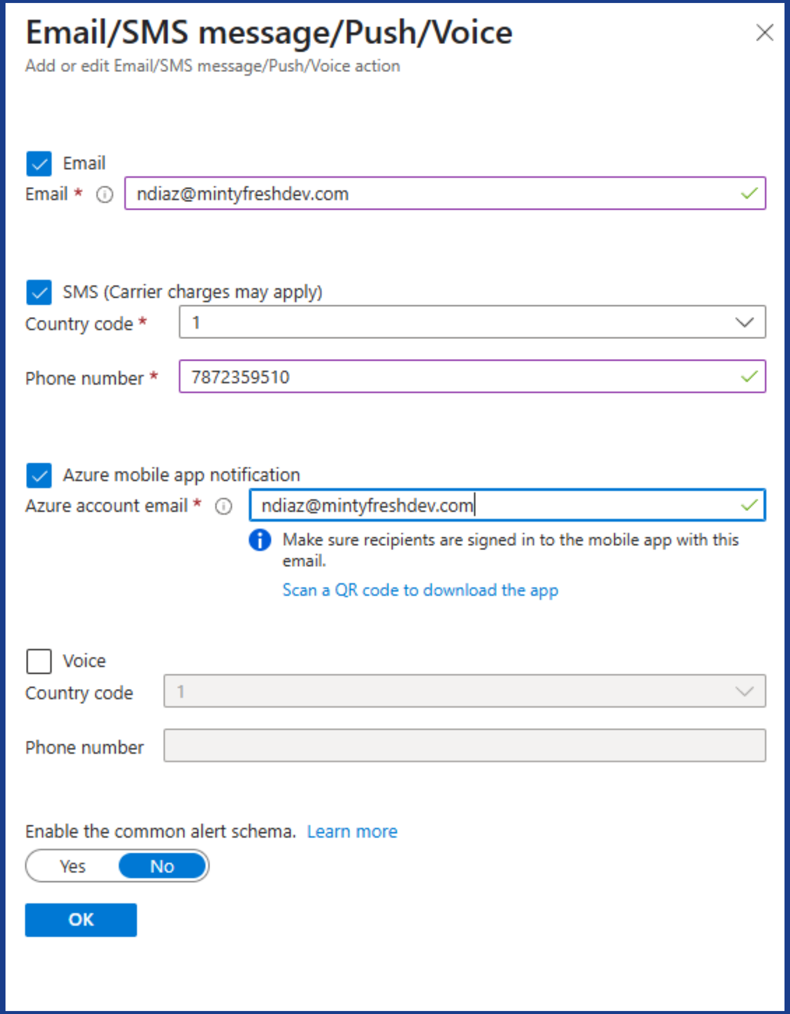
Break glass account: Monitoring



Basics | **Notifications** | Actions | Tags | Review + create

Choose how to get notified when the action group is triggered. This step is optional.

Notification type ⓘ	Name ⓘ	Selected ⓘ
Email/SMS message/Push/Voice		



Email/SMS message/Push/Voice

Add or edit Email/SMS message/Push/Voice action

☑ Email

Email * ⓘ ndiaz@mintyfreshdev.com

☑ SMS (Carrier charges may apply)

Country code * 1

Phone number * 7872359510

☑ Azure mobile app notification

Azure account email * ⓘ ndiaz@mintyfreshdev.com

ⓘ Make sure recipients are signed in to the mobile app with this email.

Scan a QR code to download the app

☐ Voice

Country code 1

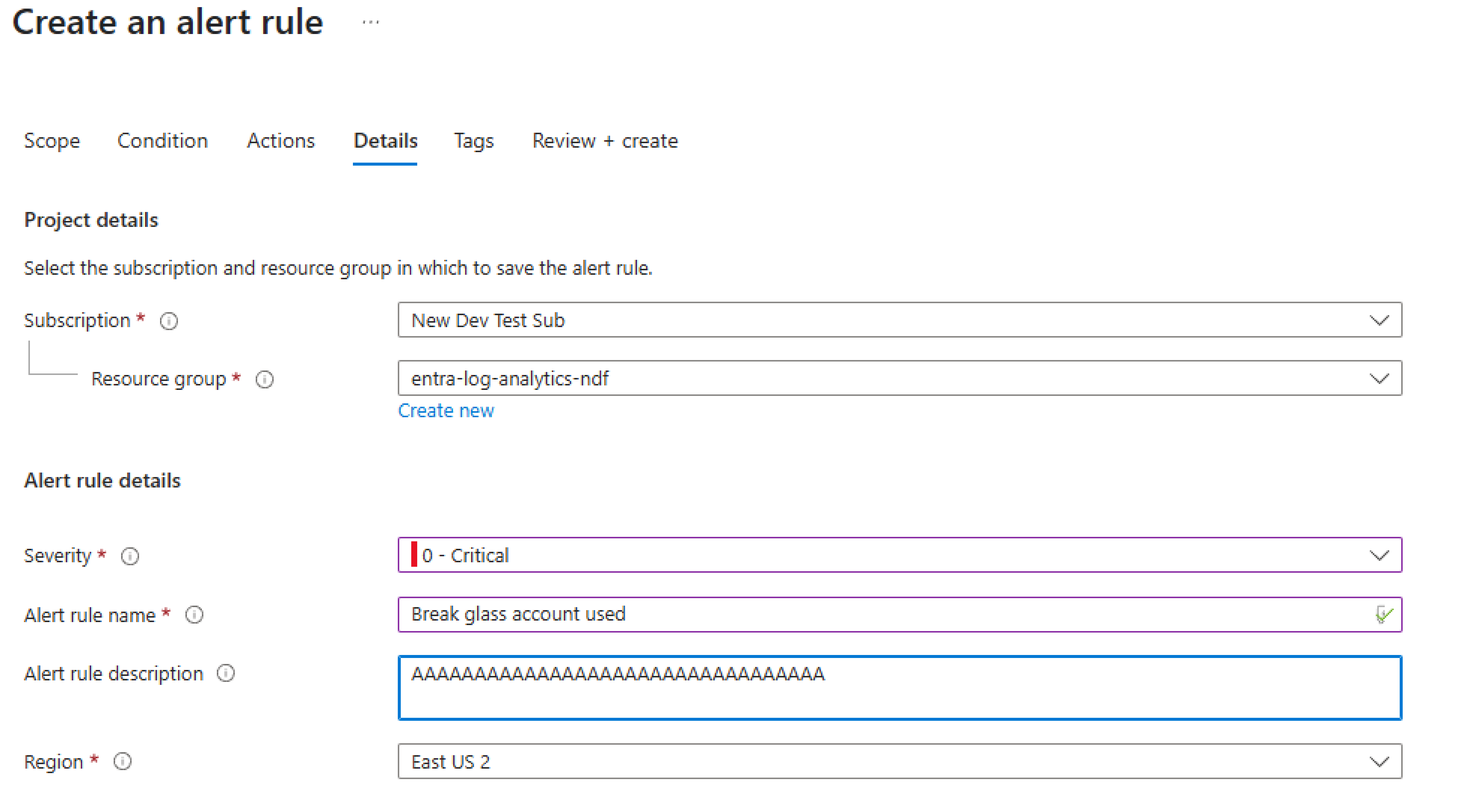
Phone number

Enable the common alert schema. Learn more

Yes [✓ No]

OK

Break glass account: Monitoring



Create an alert rule

Project details

Select the subscription and resource group in which to save the alert rule.

Subscription *	New Dev Test Sub
Resource group *	entra-log-analytics-ndf

Alert rule details

Severity *	0 - Critical
Alert rule name *	Break glass account used
Alert rule description	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Region *	East US 2

Break Glass: additional considerations

1. If account use is detected:
   - Preserve the logs from Microsoft Entra
   - Conduct a review of the usage to determine why the account was used and actions performed
2. Test break glass accounts
   - Confirm access, function, and monitoring
   - Review who has access to accounts
   - Review access request process
   - At least once every 90 days, or when key changes occur (staff or config)

Improve your M365 Secure Score

Key recommendations for a secure baseline

Presented by: Jorziño Barradas
Workshop 2/2

Date: 2025-June-4

Your host

Jorziño Barradas

Cloud Solutions Specialist

Inova Solutions

Previous Session Recap

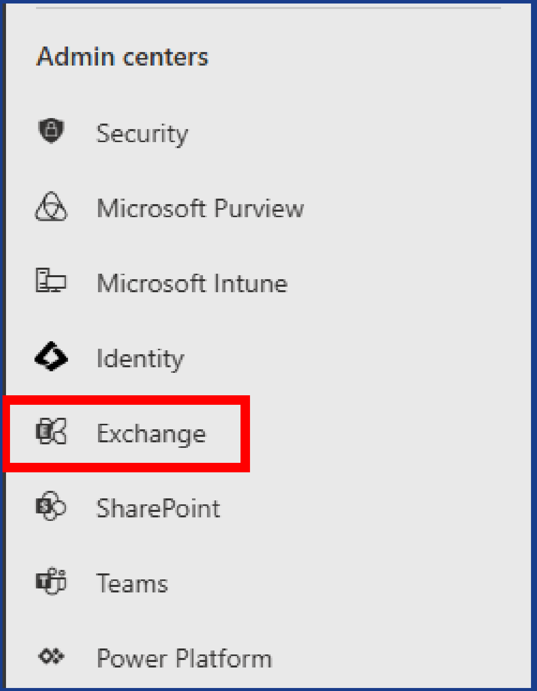
1. Follow best practice basics (least permissions required, break glass accounts)
2. Identity best practices (MFA, Conditional Access, Password Expiration)
3. Enable Defender for Office 365 (Add-on that protects against threats in email, links (URLS), file attachments)
4. Safe Attachments (scan attachments to identify malware)
5. Safe Links (scan and open links to identify malware)

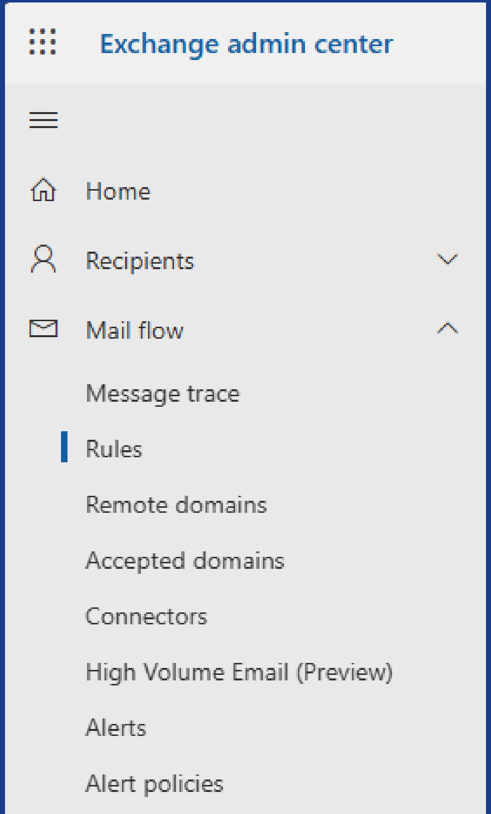
6. Disable all Mail Forwarding

Disable ALL Mail Forwarding?

1. Well, kinda…
   A. There might be a reason to keep some mail forwarding, but ensure it’s well documented
   B. Ideally, no **external** mail forwarding
2. Two steps:
   1. Manual removal of transport rules
   2. Set up anti-spam outbound policy

Disable Mail FW: Transport Rules



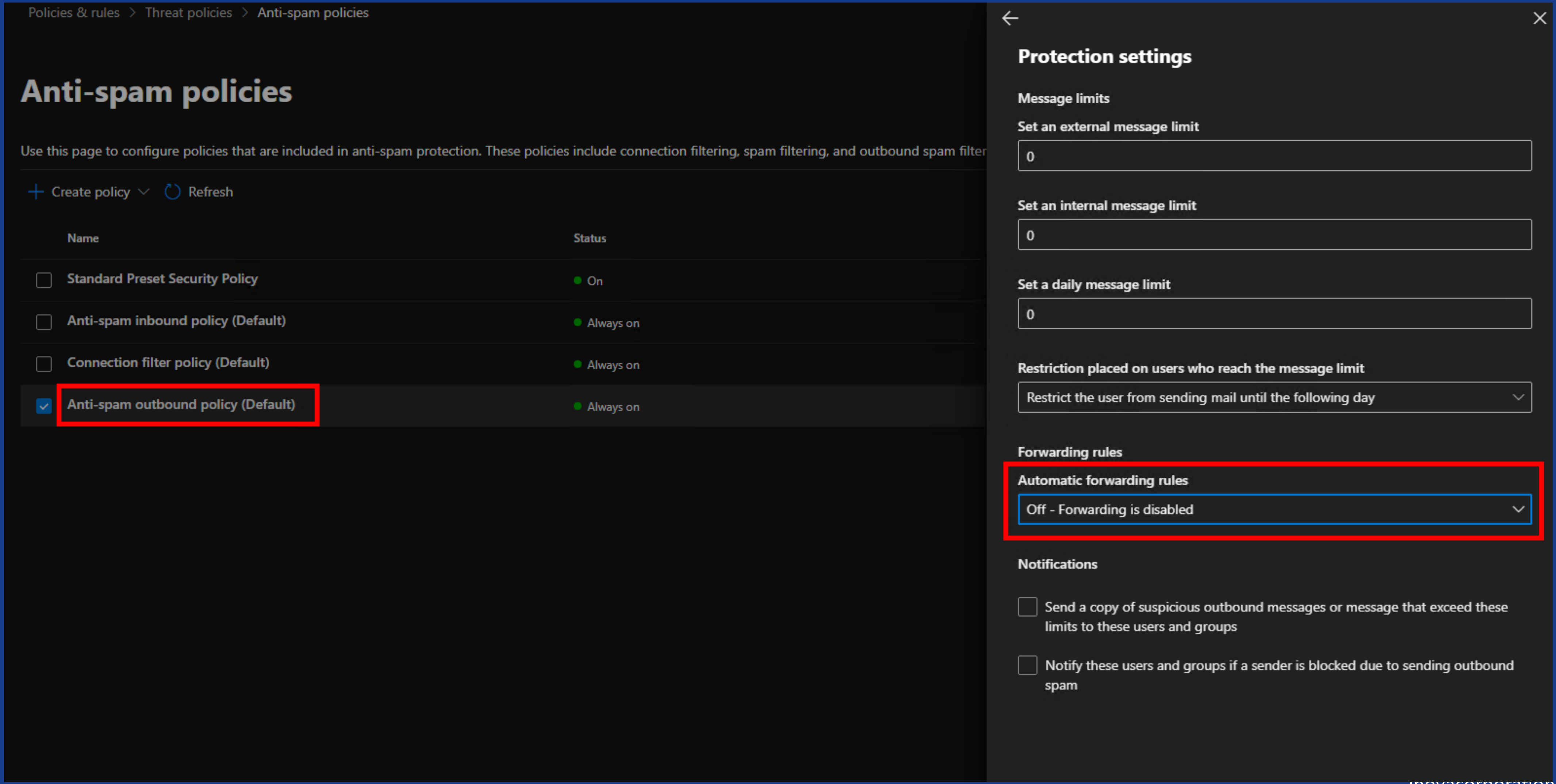


Check rules to remove all external email FW

Check via PS

Get-TransportRule | Where-Object {$_.RedirectMessageTo -ne $null} | ft Name,RedirectMessageTo

Disable Mail FW: Outbound Spam



Policies & rules > Threat policies > Anti-spam policies

Anti-spam policies

Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, and outbound spam filter

	Name	Status
□	Standard Preset Security Policy	● On
□	Anti-spam inbound policy (Default)	● Always on
□	Connection filter policy (Default)	● Always on
☑	Anti-spam outbound policy (Default)	● Always on

Protection settings

Message limits

Set an external message limit: 0

Set an internal message limit: 0

Set a daily message limit: 0

Restriction placed on users who reach the message limit: Restrict the user from sending mail until the following day

Forwarding rules

Automatic forwarding rules: Off - Forwarding is disabled

Notifications

□ Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups

□ Notify these users and groups if a sender is blocked due to sending outbound spam

7. Enable Attachment Types Filter

Enable Attachment Types Filter

- Files commonly used to deliver malware
  - Executables (.exe, .scr, .js)
  - Script files (.vbs, .bat, .cmd)
  - Compressed files (.zip, .jar) depending on policy

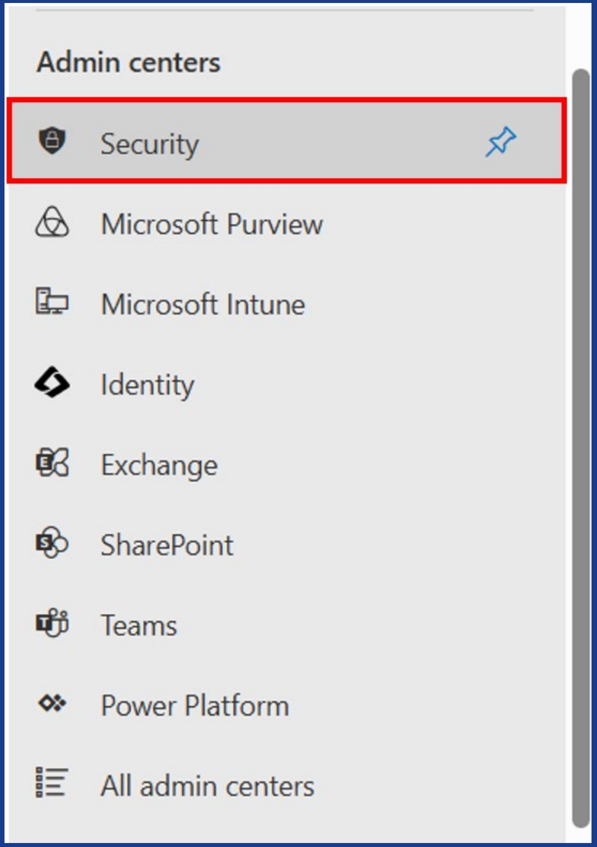
- Application in form a file which will run as soon as it is downloaded.

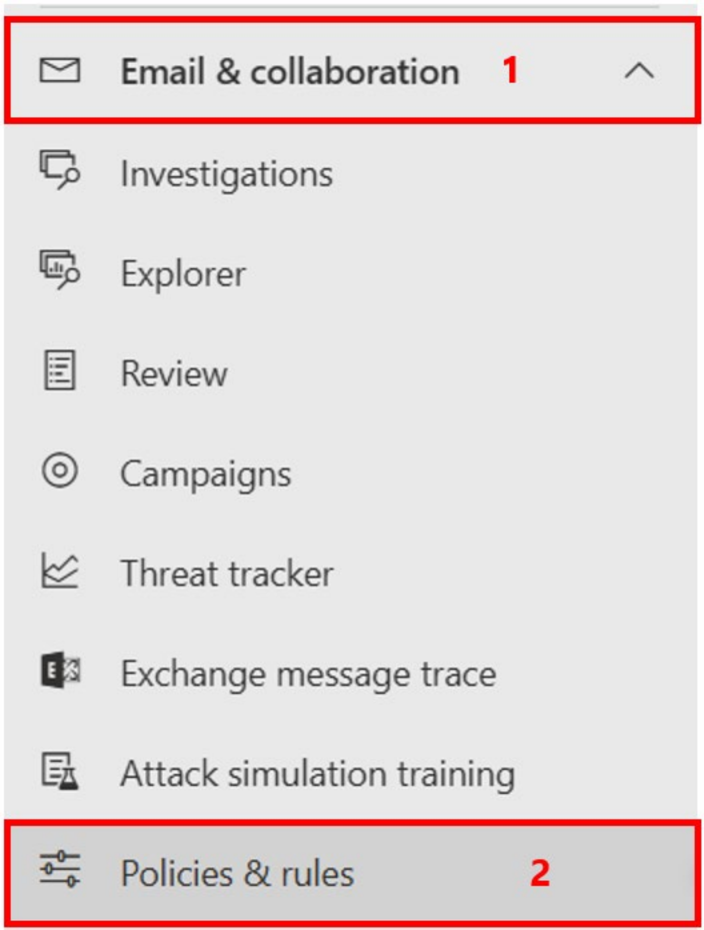
  - Scan your hardware

  - Scan your networks

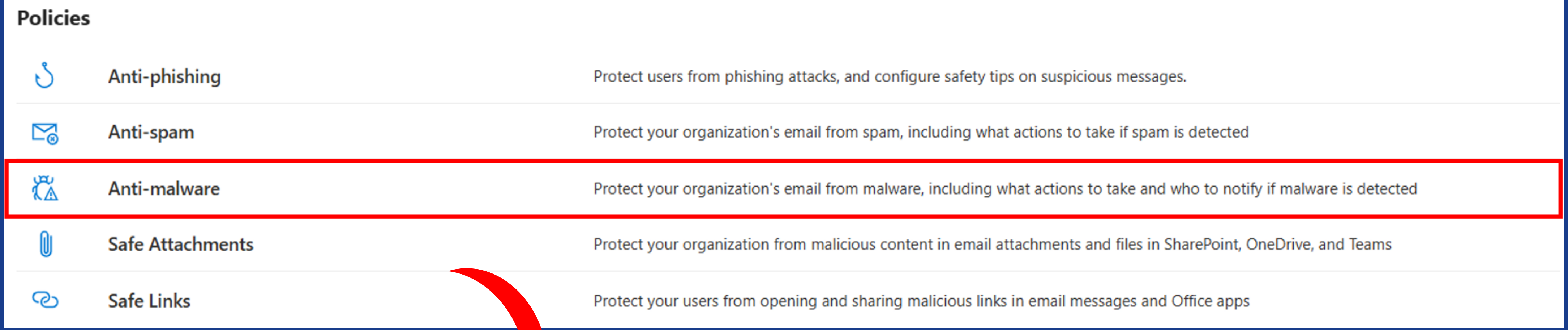
  - Install Malware

Enable Attachment Types Filter



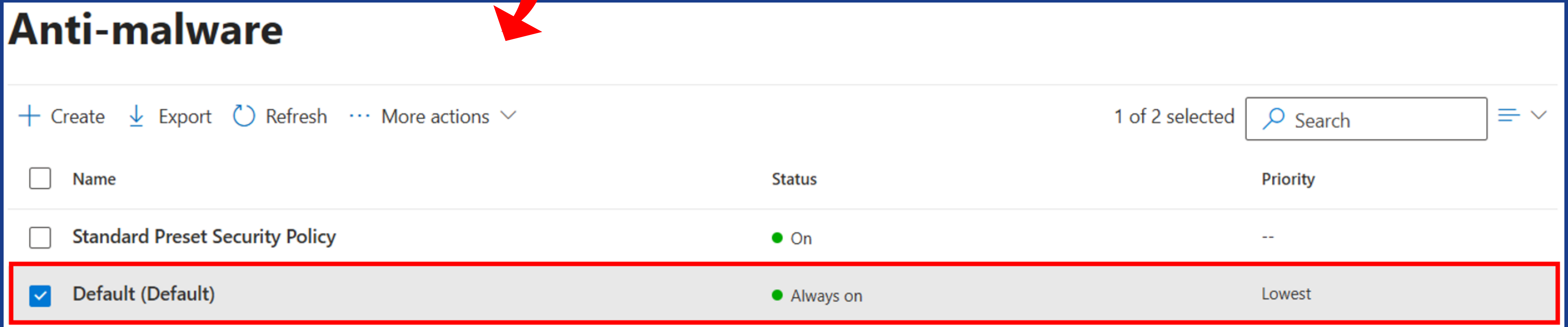


Enable Attachment Types Filter



Policies

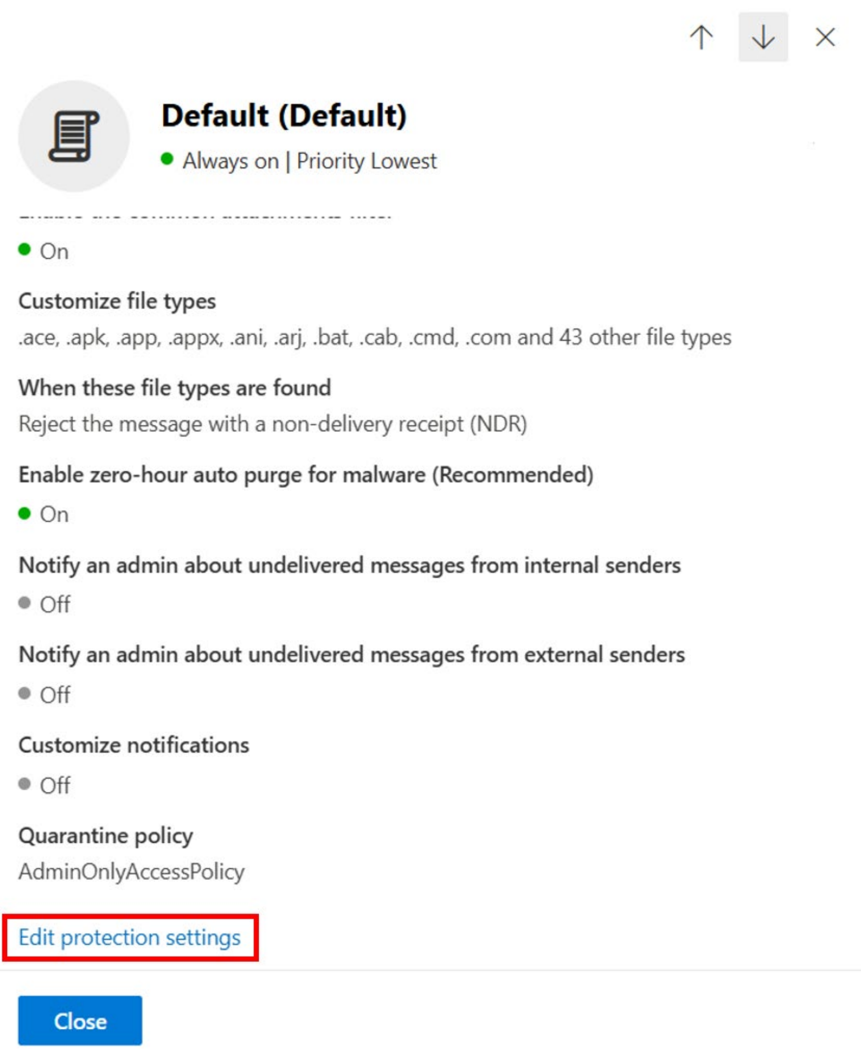
Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps



Anti-malware

	Name	Status	Priority
□	Standard Preset Security Policy	● On	--
☑	Default (Default)	● Always on	Lowest

Enable Attachment Types Filter



Default (Default)

● Always on | Priority Lowest

● On

Customize file types

.ace, .apk, .app, .appx, .ani, .arj, .bat, .cab, .cmd, .com and 43 other file types

When these file types are found

Reject the message with a non-delivery receipt (NDR)

Enable zero-hour auto purge for malware (Recommended)

● On

Notify an admin about undelivered messages from internal senders

● Off

Notify an admin about undelivered messages from external senders

● Off

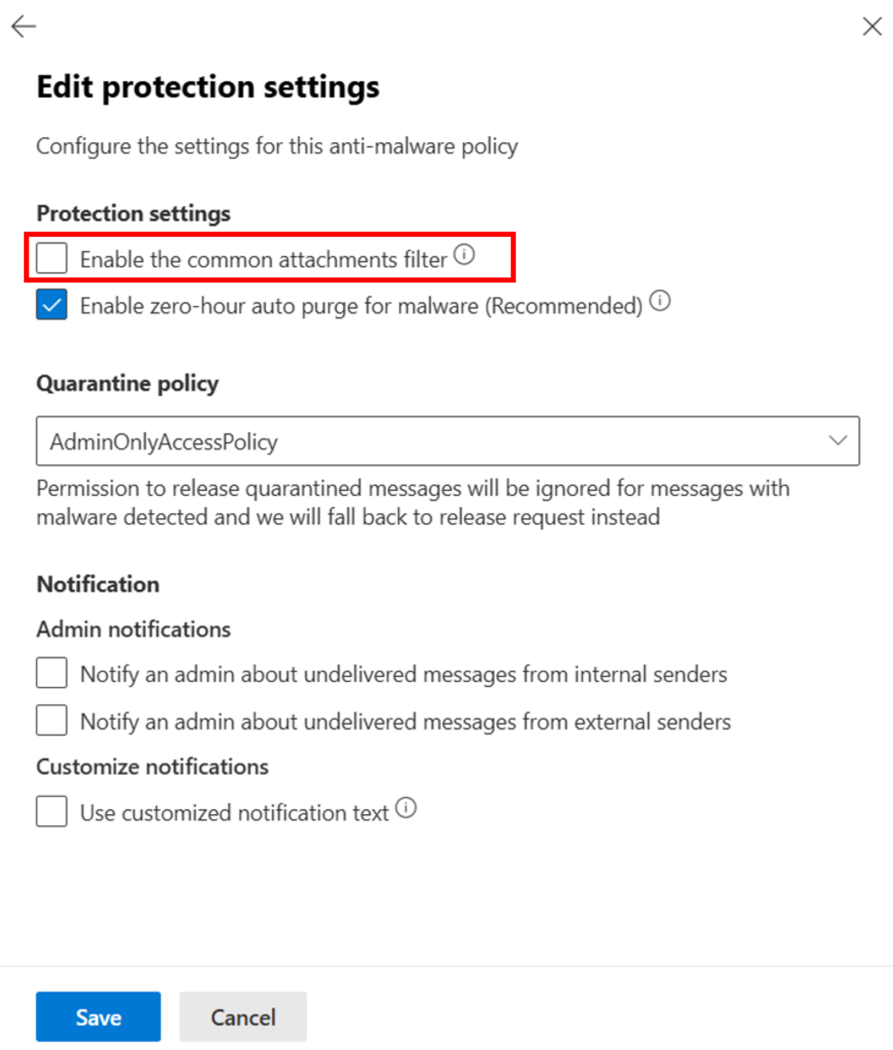
Customize notifications

● Off

Quarantine policy

AdminOnlyAccessPolicy

Edit protection settings



Edit protection settings

Configure the settings for this anti-malware policy

Protection settings

□ Enable the common attachments filter ⓘ

☑ Enable zero-hour auto purge for malware (Recommended) ⓘ

Quarantine policy

AdminOnlyAccessPolicy

Permission to release quarantined messages will be ignored for messages with malware detected and we will fall back to release request instead

Notification

Admin notifications

□ Notify an admin about undelivered messages from internal senders

□ Notify an admin about undelivered messages from external senders

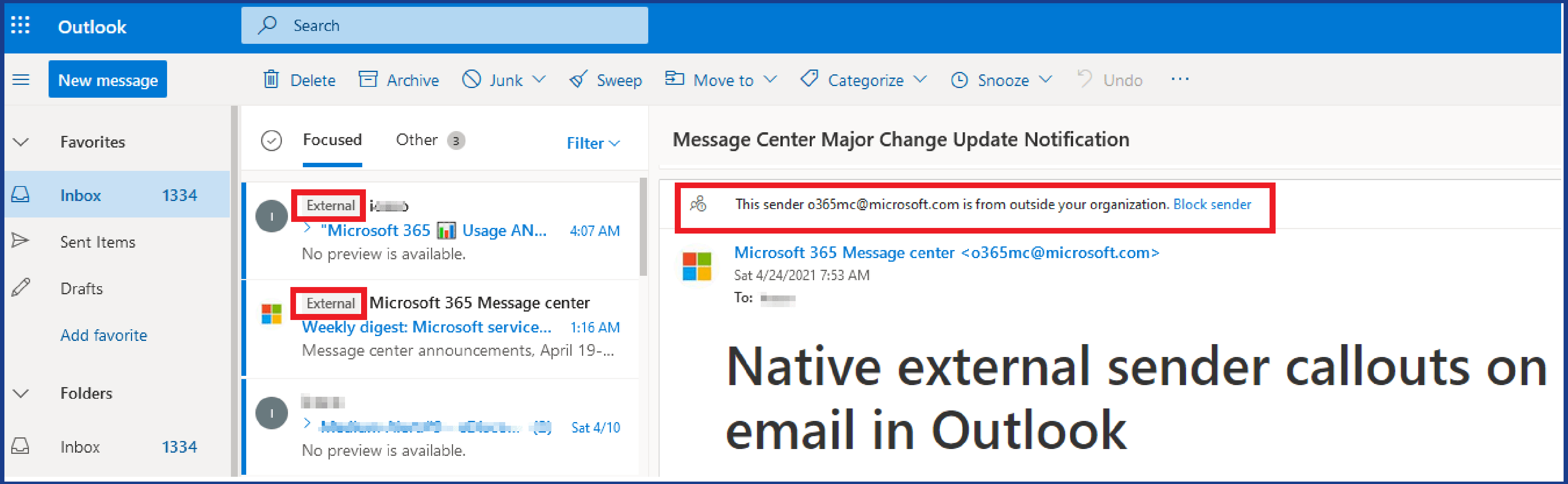
Customize notifications

□ Use customized notification text ⓘ

8. Enable MailTips

What Are MailTips?

- Informative messages when composing an email
- Analyze email content, including recipients to detect potential problems
- Implemented as a web service in Exchange



External i[redacted]
"Microsoft 365 📊 Usage AN... 4:07 AM
No preview is available.

External Microsoft 365 Message center
Weekly digest: Microsoft service... 1:16 AM
Message center announcements, April 19-...

[redacted]
[redacted] Sat 4/10
No preview is available.

Message Center Major Change Update Notification

This sender o365mc@microsoft.com is from outside your organization. Block sender

Microsoft 365 Message center <o365mc@microsoft.com>
Sat 4/24/2021 7:53 AM
To: [redacted]

Native external sender callouts on email in Outlook

Benefits of MailTips

- Increase Productivity

  Avoid sending email to out of office team members, users with mailbox full

- Avoid Non-Delivery Reports (NDR)

  Sending messages to invalid internal or restricted recipient

- Preventing Data Leakage

  Prevent sending email to external users, large distribution groups, or reply-all on BCC email

Enable MailTips

1. Run Microsoft Exchange Online PowerShell Module
2. Connect using "Connect-ExchangeOnline"
3. Run the following PowerShell command:

```
Set-OrganizationConfig -MailTipsAllTipsEnabled $true -MailTipsExternalRecipientsTipsEnabled $true -
MailTipsGroupMetricsEnabled $true -MailTipsLargeAudienceThreshold '25'
```

Connect to Exchange Online Guideline:

Connect to Exchange Online PowerShell | Microsoft Learn

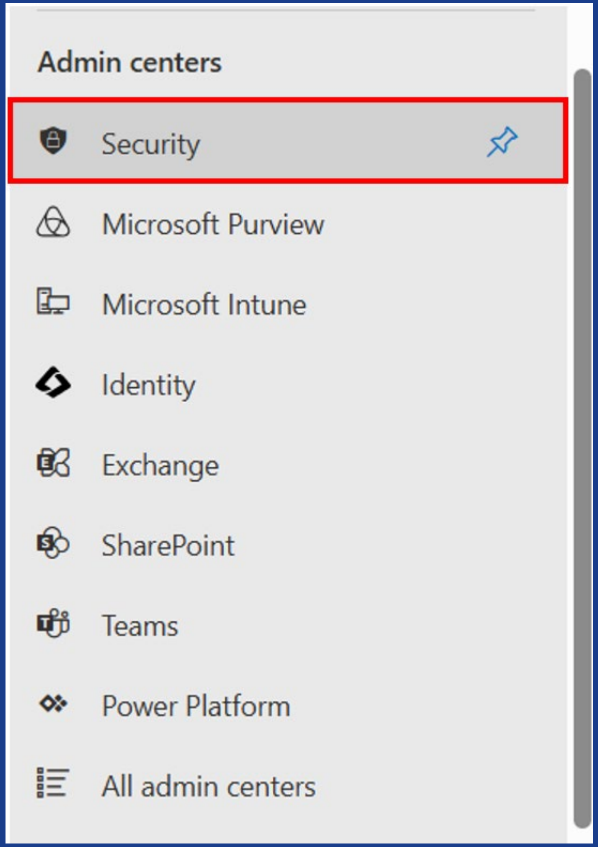
9. Enable Impersonation Protection

Types of Impersonation?

- A fraudster pretending to be someone in your organization.
- Will create a fake account that is similar to someone in your organization.

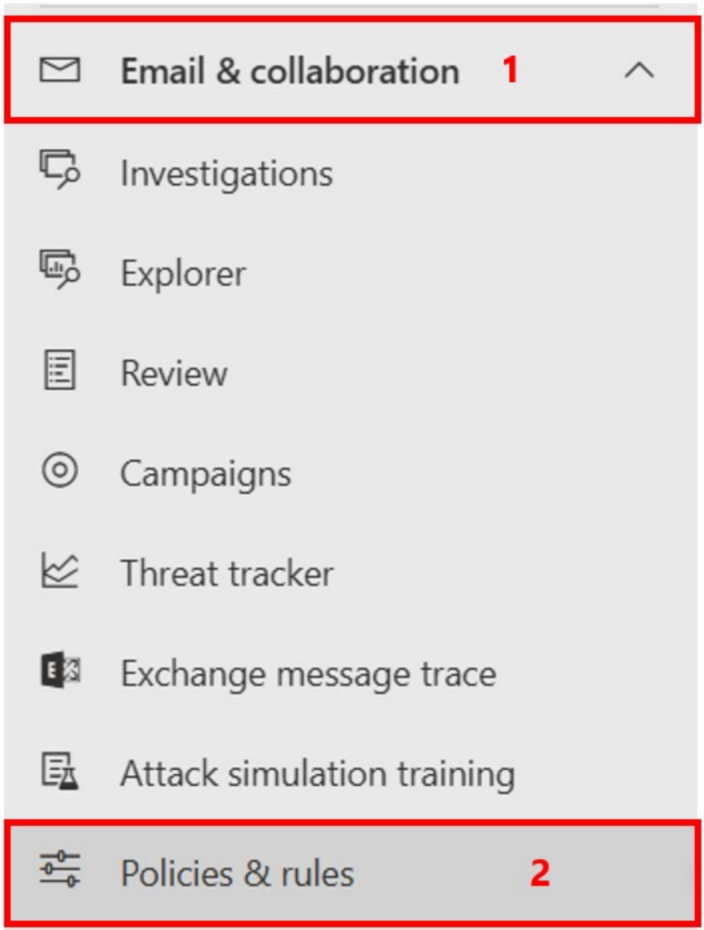
  - Most likely the CEO or management position.
- Skippie@contoso.com -> Skippie@contososo.com
- Send emails to someone in your department for payments.
- Impersonation Protection -> User & Domain
- Requirements: Microsoft Defender Plan 2

Enable Impersonation



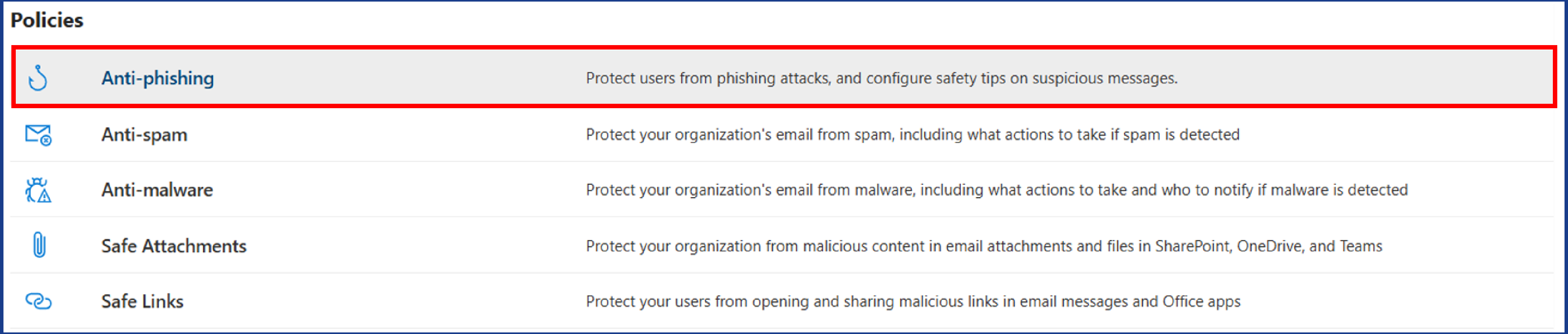
Admin centers

- Security
- Microsoft Purview
- Microsoft Intune
- Identity
- Exchange
- SharePoint
- Teams
- Power Platform
- All admin centers



- Email & collaboration 1
- Investigations
- Explorer
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules 2

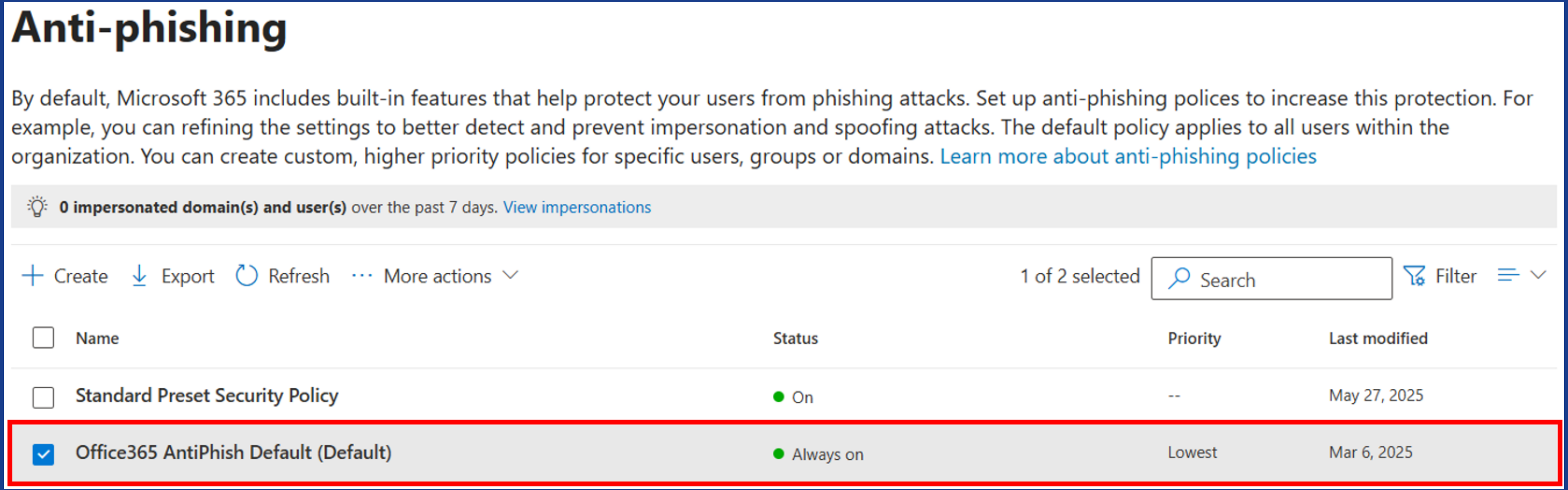
Enable Impersonation



Policies

	Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
	Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
	Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
	Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
	Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Enable Impersonation



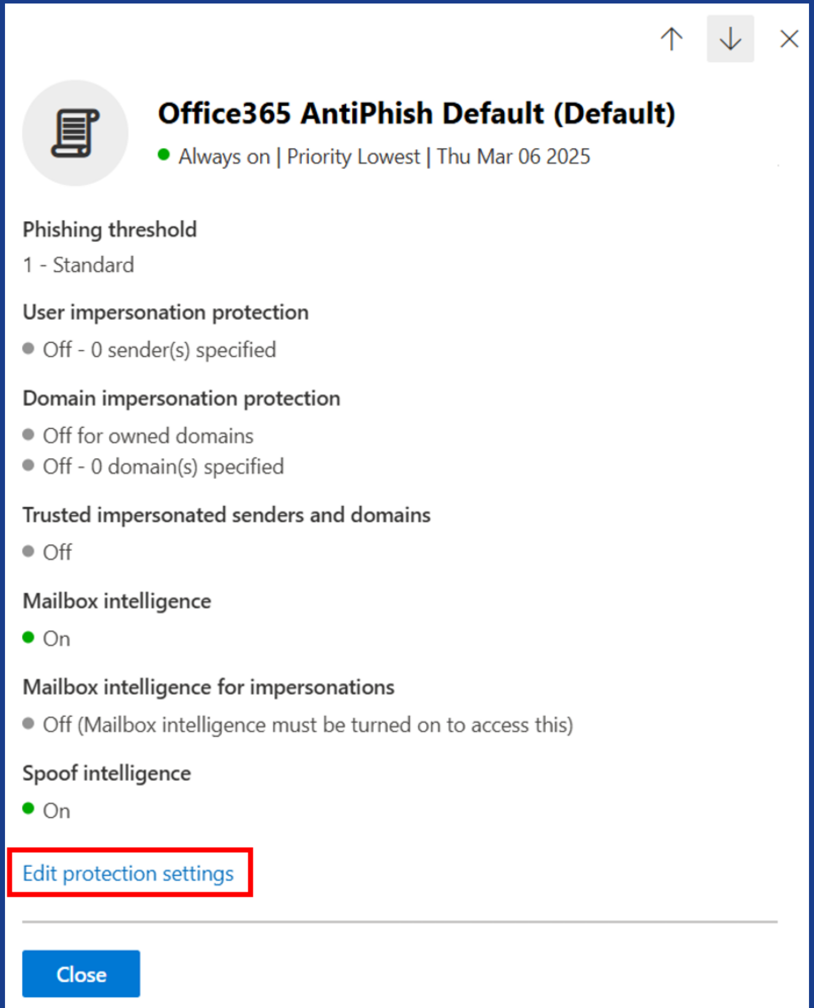
Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing polices to increase this protection. For example, you can refining the settings to better detect and prevent impersonation and spoofing attacks. The default policy applies to all users within the organization. You can create custom, higher priority policies for specific users, groups or domains. Learn more about anti-phishing policies

0 impersonated domain(s) and user(s) over the past 7 days. View impersonations

□	Name	Status	Priority	Last modified
□	Standard Preset Security Policy	● On	--	May 27, 2025
☑	Office365 AntiPhish Default (Default)	● Always on	Lowest	Mar 6, 2025

Enable Impersonation



Office365 AntiPhish Default (Default)

● Always on | Priority Lowest | Thu Mar 06 2025

Phishing threshold

1 - Standard

User impersonation protection

● Off - 0 sender(s) specified

Domain impersonation protection

● Off for owned domains

● Off - 0 domain(s) specified

Trusted impersonated senders and domains

● Off

Mailbox intelligence

● On

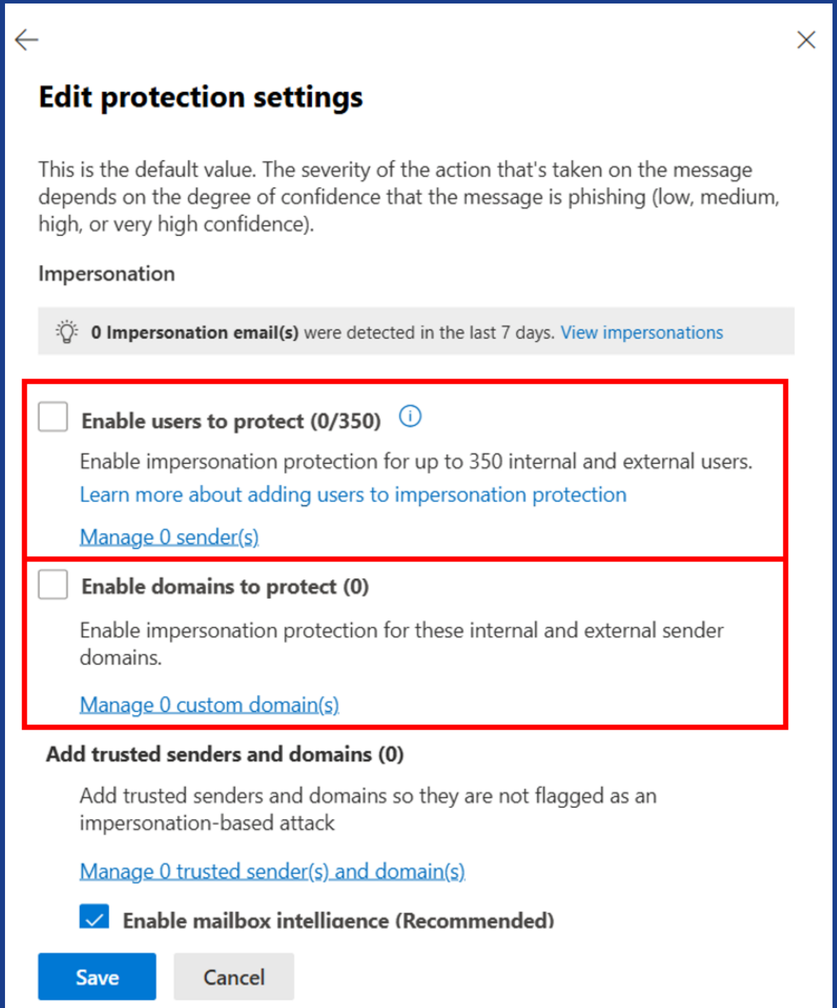
Mailbox intelligence for impersonations

● Off (Mailbox intelligence must be turned on to access this)

Spoof intelligence

● On

Edit protection settings



Edit protection settings

This is the default value. The severity of the action that's taken on the message depends on the degree of confidence that the message is phishing (low, medium, high, or very high confidence).

Impersonation

0 Impersonation email(s) were detected in the last 7 days. View impersonations

□ **Enable users to protect (0/350)**

Enable impersonation protection for up to 350 internal and external users. Learn more about adding users to impersonation protection

Manage 0 sender(s)

□ **Enable domains to protect (0)**

Enable impersonation protection for these internal and external sender domains.

Manage 0 custom domain(s)

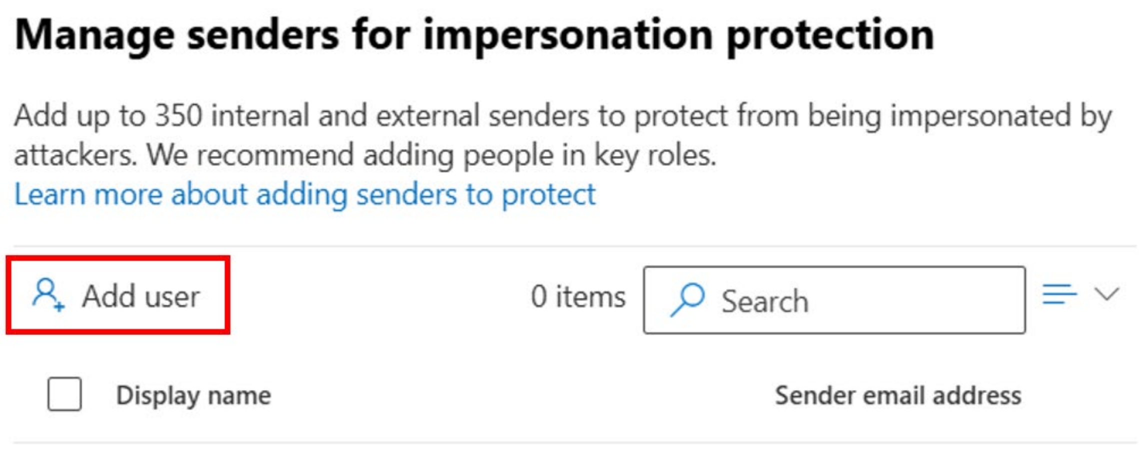
Add trusted senders and domains (0)

Add trusted senders and domains so they are not flagged as an impersonation-based attack

Manage 0 trusted sender(s) and domain(s)

☑ **Enable mailbox intelligence (Recommended)**

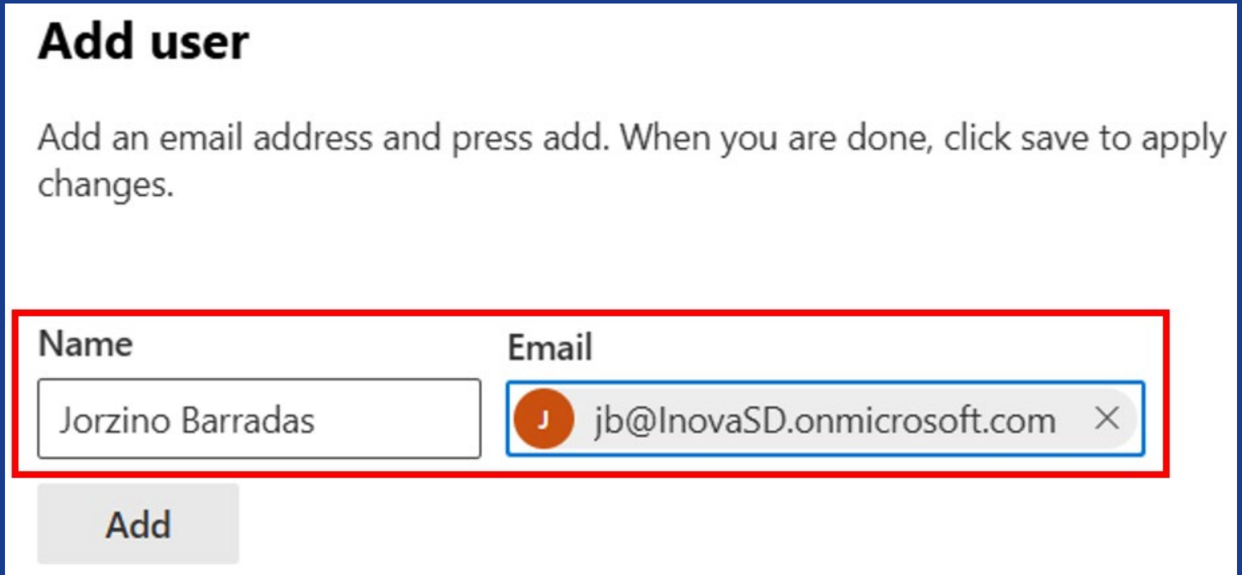
Enable Impersonation



Manage senders for impersonation protection

Add up to 350 internal and external senders to protect from being impersonated by attackers. We recommend adding people in key roles.

Learn more about adding senders to protect



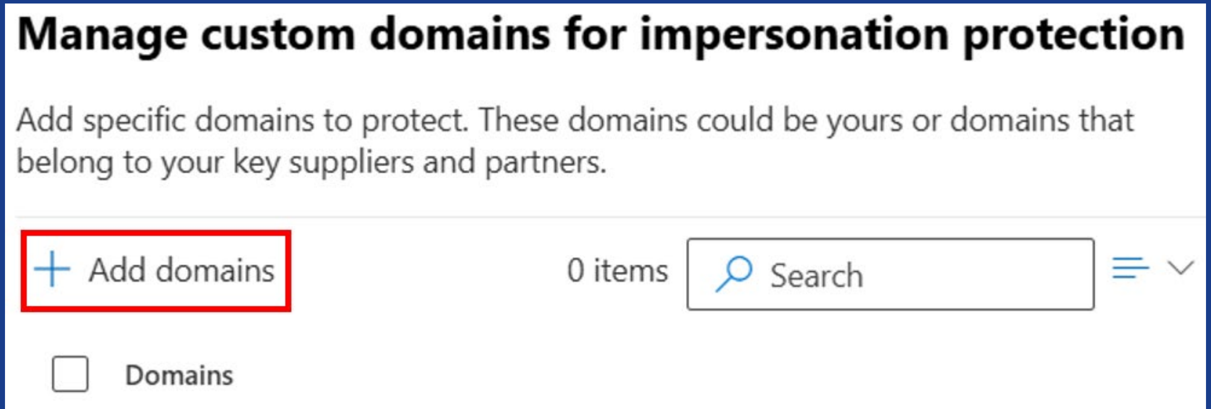
Add user

Add an email address and press add. When you are done, click save to apply changes.

Name: Jorzino Barradas

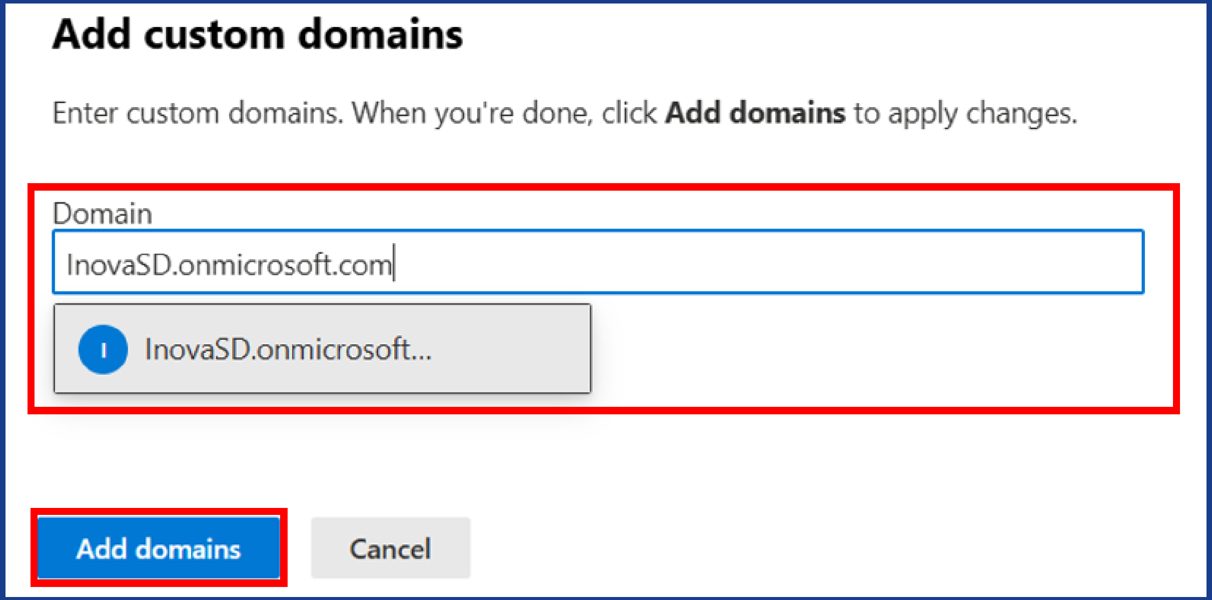
Email: jb@InovaSD.onmicrosoft.com

Enable Impersonation



Manage custom domains for impersonation protection

Add specific domains to protect. These domains could be yours or domains that belong to your key suppliers and partners.



Add custom domains

Enter custom domains. When you're done, click **Add domains** to apply changes.

Domain: InovaSD.onmicrosoft.com

10. Configure Teams Meeting Permissions

Why is Meeting Permissions Important?

- Prevents Accidental Data Exposure

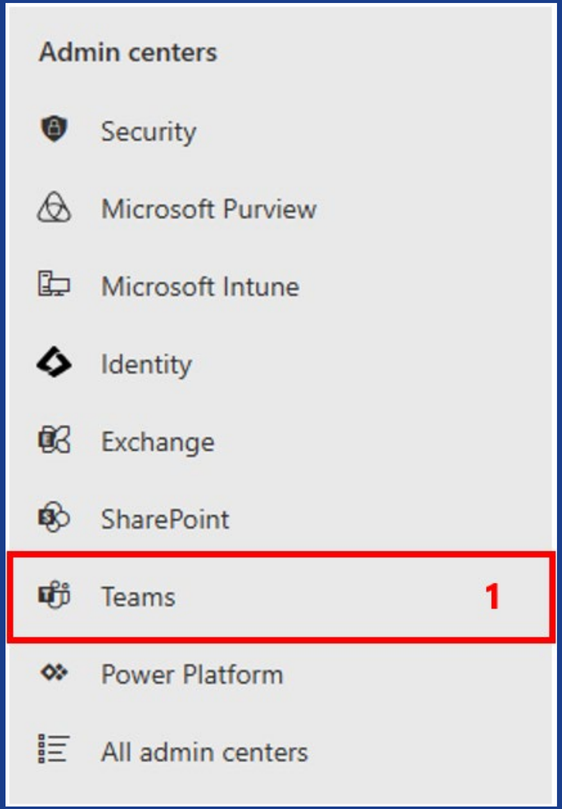
  - Unauthorized attendees

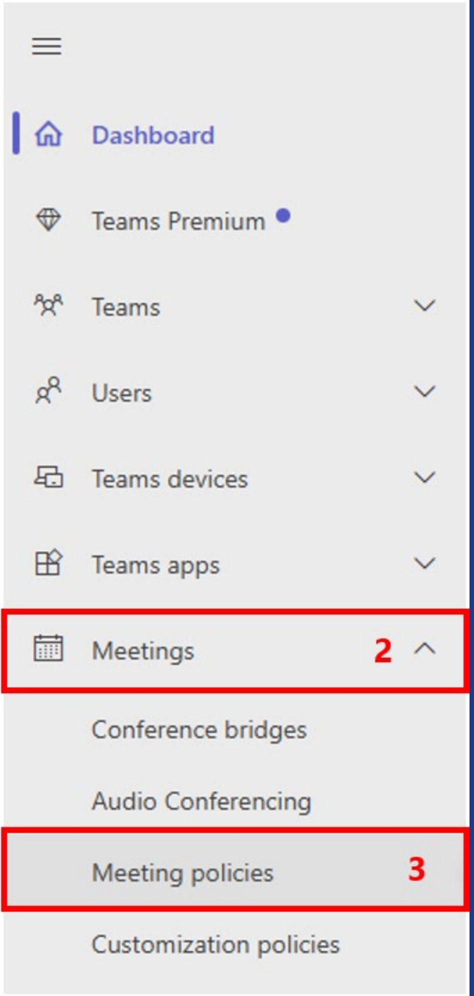
  - Accidentally share sensitive information

- Actions:

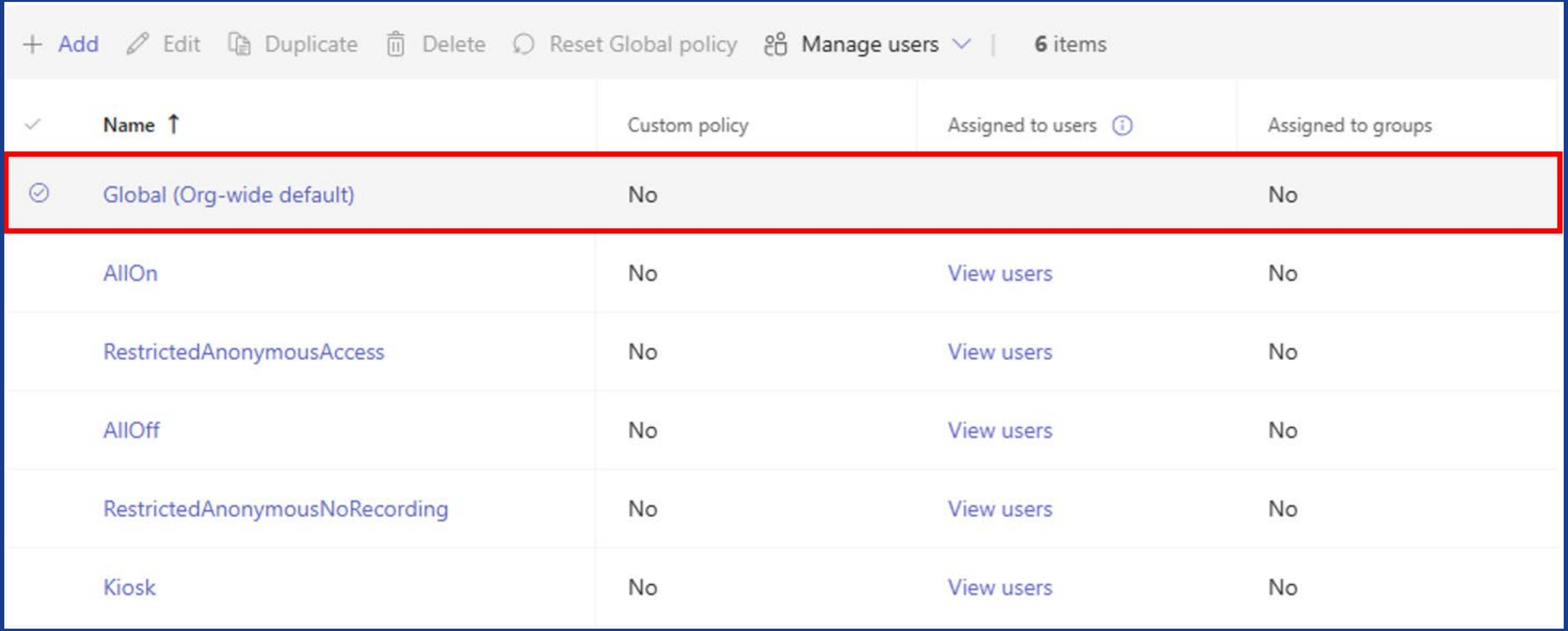
1. Configure which users can present in Teams
2. Configure which users should be automatically admitted to Teams

Teams Permissions: Configure Presenter



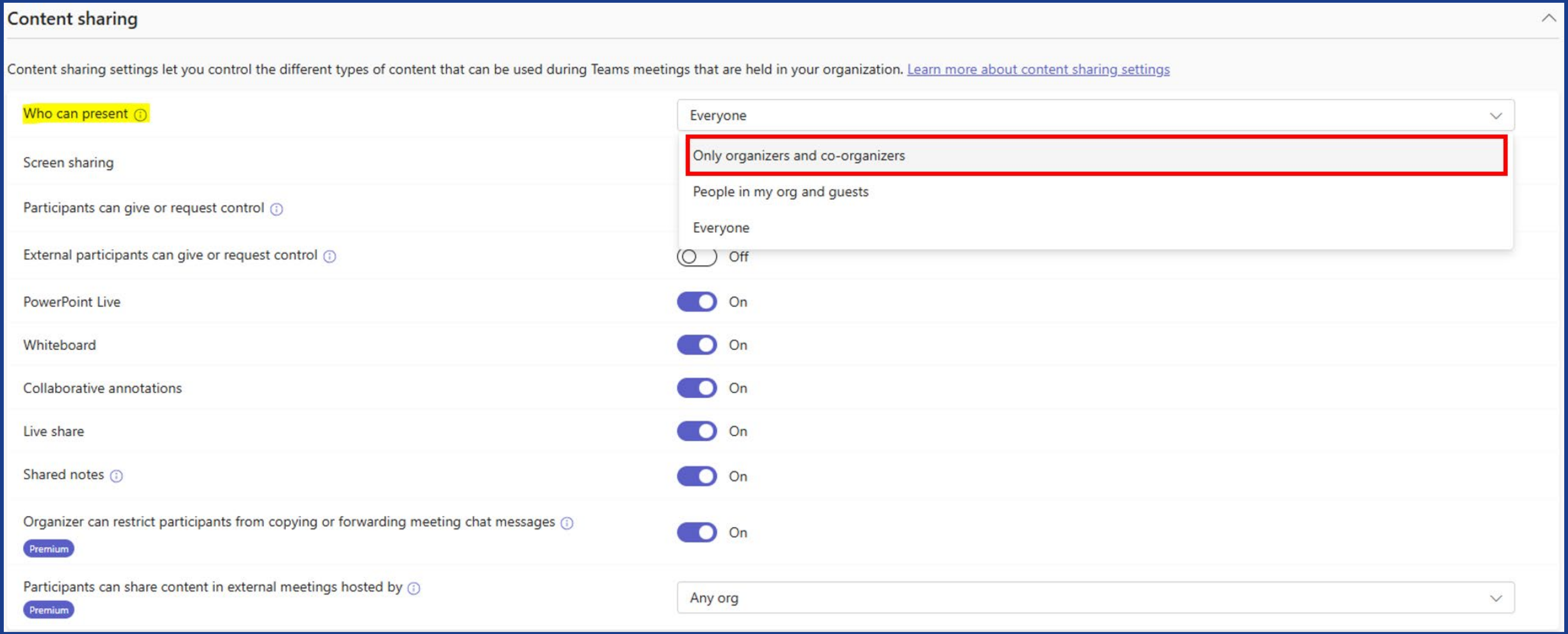


Teams Permissions: Configure Presenter



✓	Name ↑	Custom policy	Assigned to users ⓘ	Assigned to groups
✓	Global (Org-wide default)	No		No
	AllOn	No	View users	No
	RestrictedAnonymousAccess	No	View users	No
	AllOff	No	View users	No
	RestrictedAnonymousNoRecording	No	View users	No
	Kiosk	No	View users	No

Teams Permissions: Configure Presenter



Content sharing

Content sharing settings let you control the different types of content that can be used during Teams meetings that are held in your organization. Learn more about content sharing settings

Who can present: Everyone

Only organizers and co-organizers
People in my org and guests
Everyone

Screen sharing

Participants can give or request control

External participants can give or request control: Off

PowerPoint Live: On

Whiteboard: On

Collaborative annotations: On

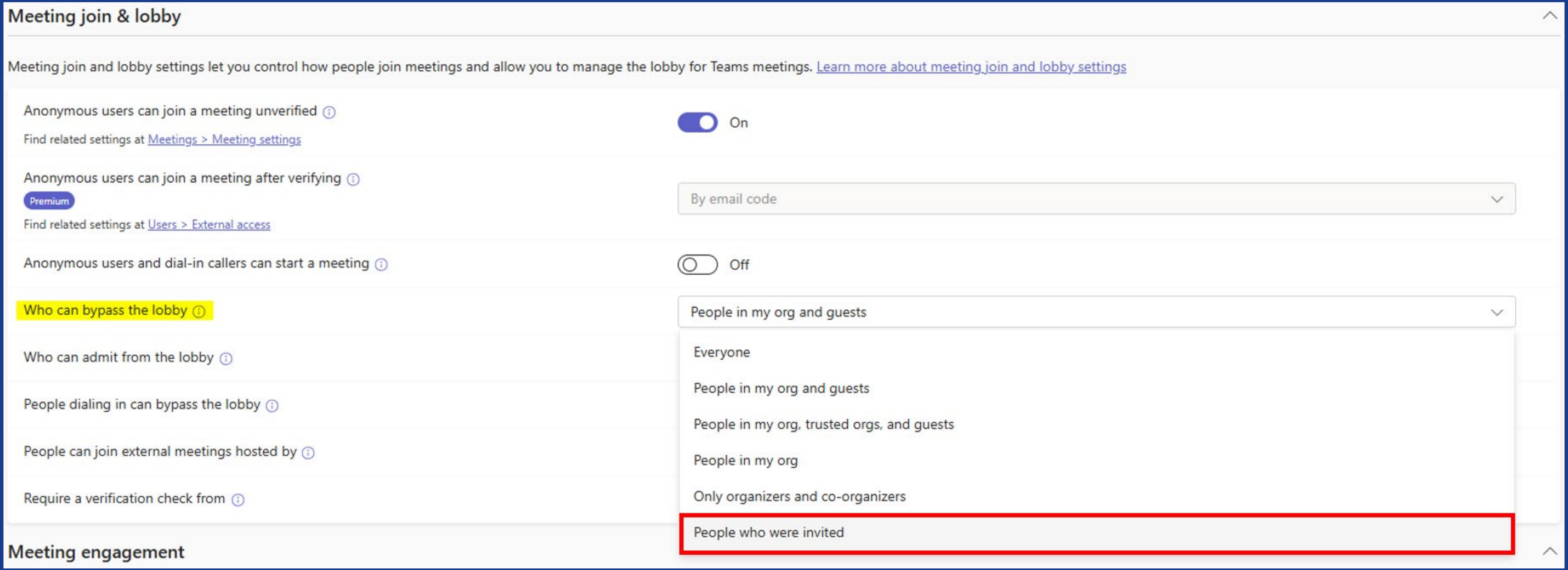
Live share: On

Shared notes: On

Organizer can restrict participants from copying or forwarding meeting chat messages (Premium): On

Participants can share content in external meetings hosted by (Premium): Any org

Teams Permissions: Auto-Admit to Meetings



Meeting join & lobby

Meeting join and lobby settings let you control how people join meetings and allow you to manage the lobby for Teams meetings. Learn more about meeting join and lobby settings

Anonymous users can join a meeting unverified ⓘ
Find related settings at Meetings > Meeting settings
On

Anonymous users can join a meeting after verifying ⓘ
Premium
Find related settings at Users > External access
By email code

Anonymous users and dial-in callers can start a meeting ⓘ
Off

Who can bypass the lobby ⓘ
People in my org and guests

- Everyone
- People in my org and guests
- People in my org, trusted orgs, and guests
- People in my org
- Only organizers and co-organizers
- People who were invited

Who can admit from the lobby ⓘ

People dialing in can bypass the lobby ⓘ

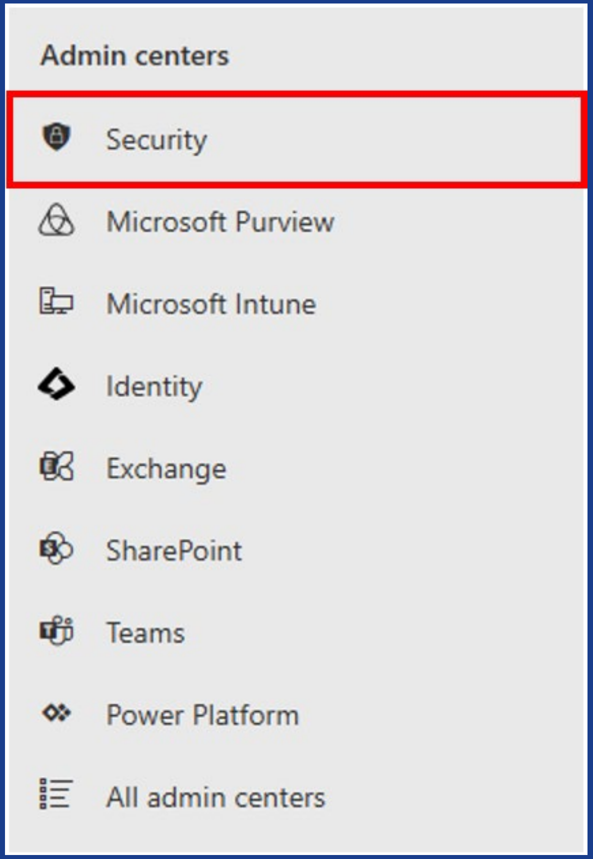
People can join external meetings hosted by ⓘ

Require a verification check from ⓘ

Meeting engagement

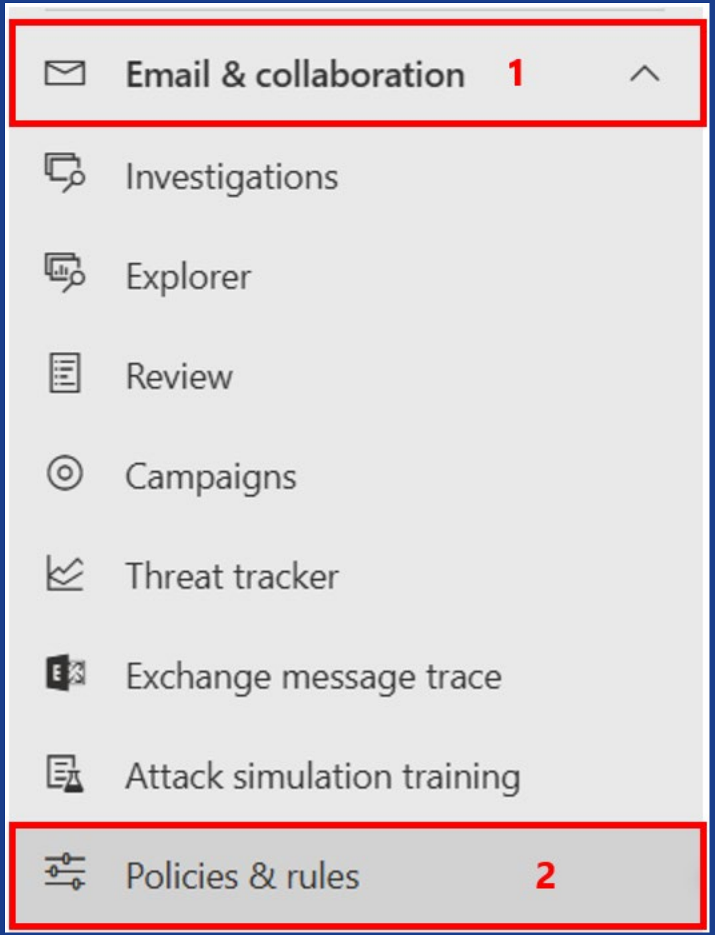
BONUS: Alert on New Mail Forwarding Rules

How to Implement?



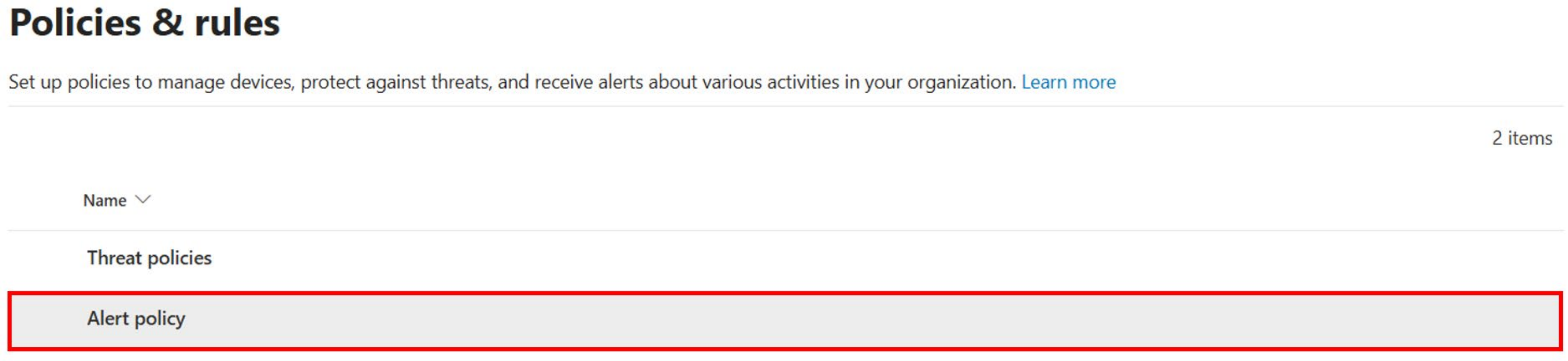
Admin centers

- Security
- Microsoft Purview
- Microsoft Intune
- Identity
- Exchange
- SharePoint
- Teams
- Power Platform
- All admin centers



- Email & collaboration 1
- Investigations
- Explorer
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules 2

How to Implement?

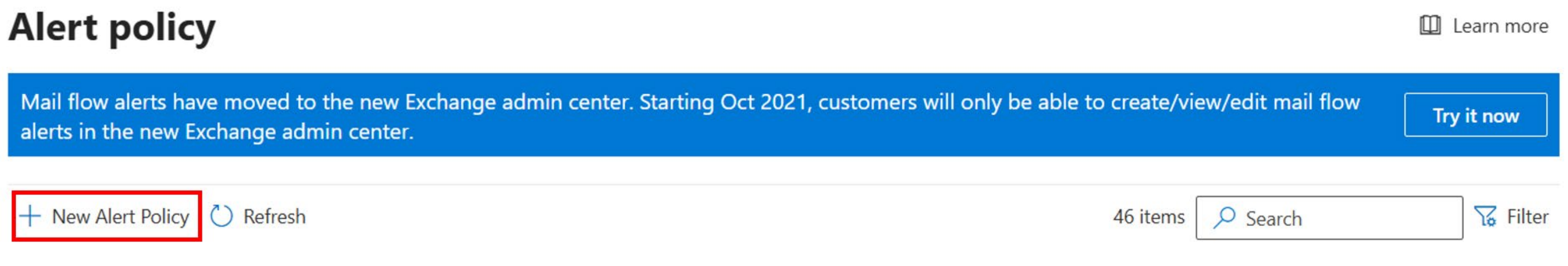


Policies & rules

Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization. Learn more

2 items

Name
Threat policies
Alert policy

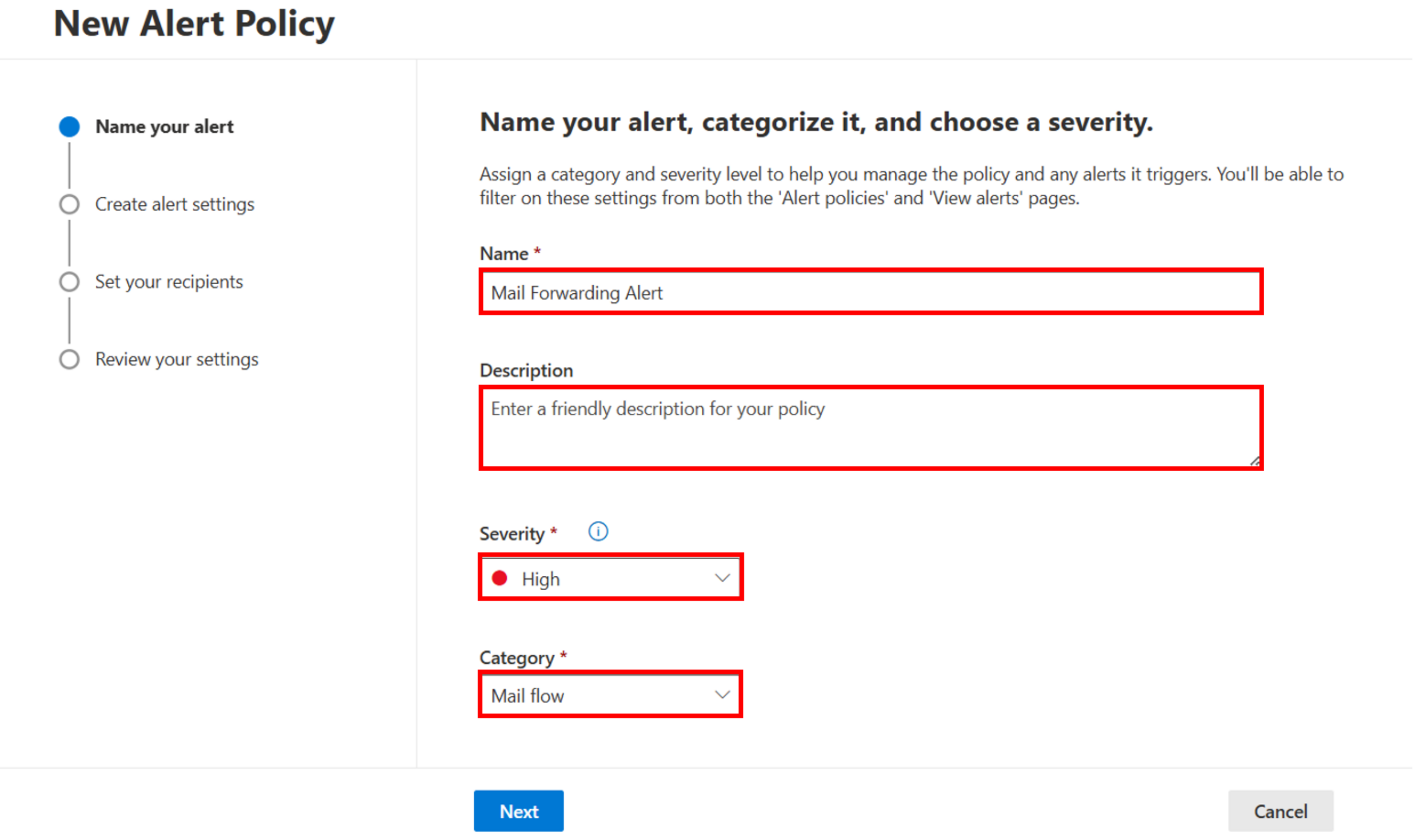


Alert policy

Learn more

Mail flow alerts have moved to the new Exchange admin center. Starting Oct 2021, customers will only be able to create/view/edit mail flow alerts in the new Exchange admin center.

How to Implement?



New Alert Policy

● Name your alert
○ Create alert settings
○ Set your recipients
○ Review your settings

Name your alert, categorize it, and choose a severity.

Assign a category and severity level to help you manage the policy and any alerts it triggers. You'll be able to filter on these settings from both the 'Alert policies' and 'View alerts' pages.

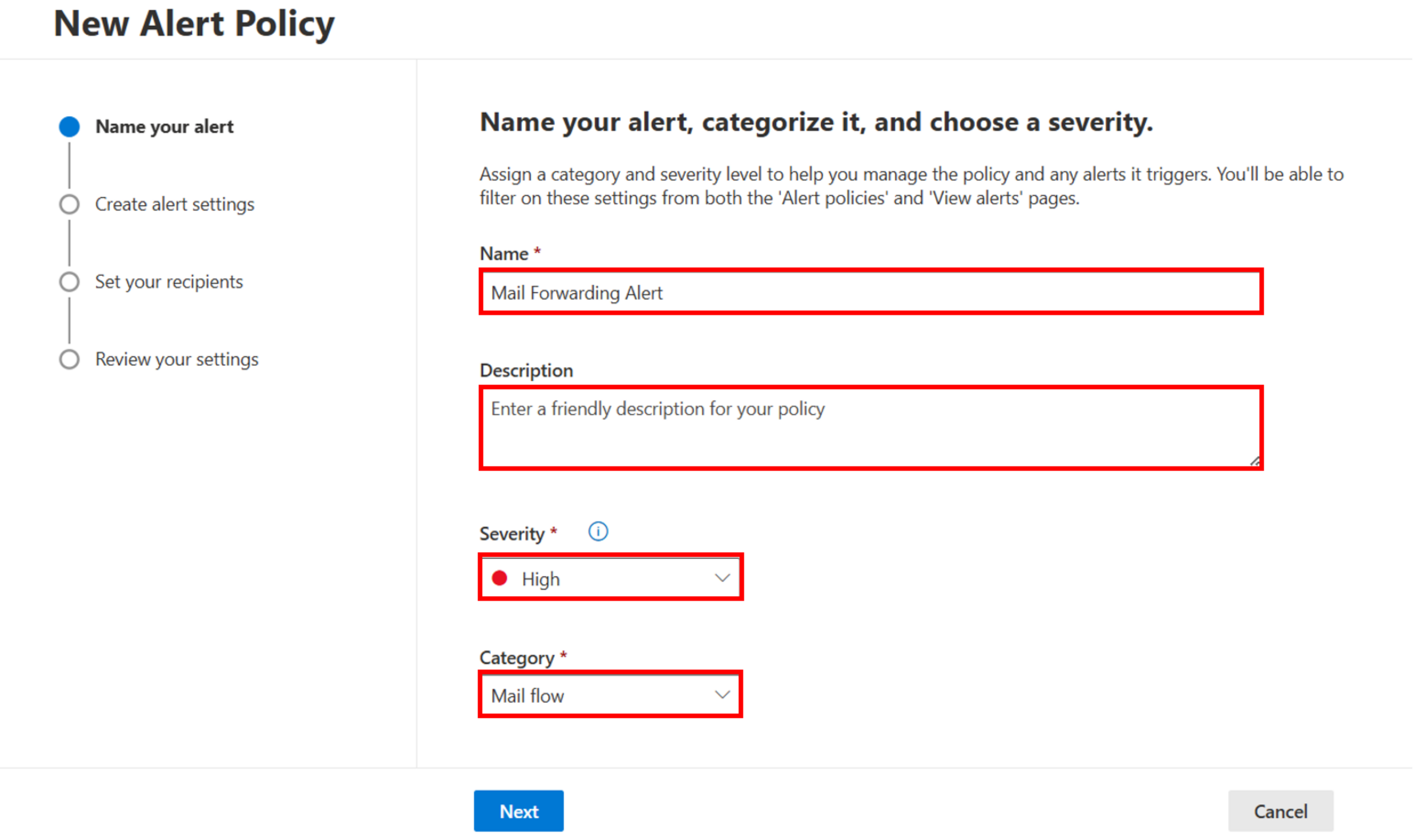
Name *
Mail Forwarding Alert

Description
Enter a friendly description for your policy

Severity *
● High

Category *
Mail flow

How to Implement?



New Alert Policy

● Name your alert
○ Create alert settings
○ Set your recipients
○ Review your settings

Name your alert, categorize it, and choose a severity.

Assign a category and severity level to help you manage the policy and any alerts it triggers. You'll be able to filter on these settings from both the 'Alert policies' and 'View alerts' pages.

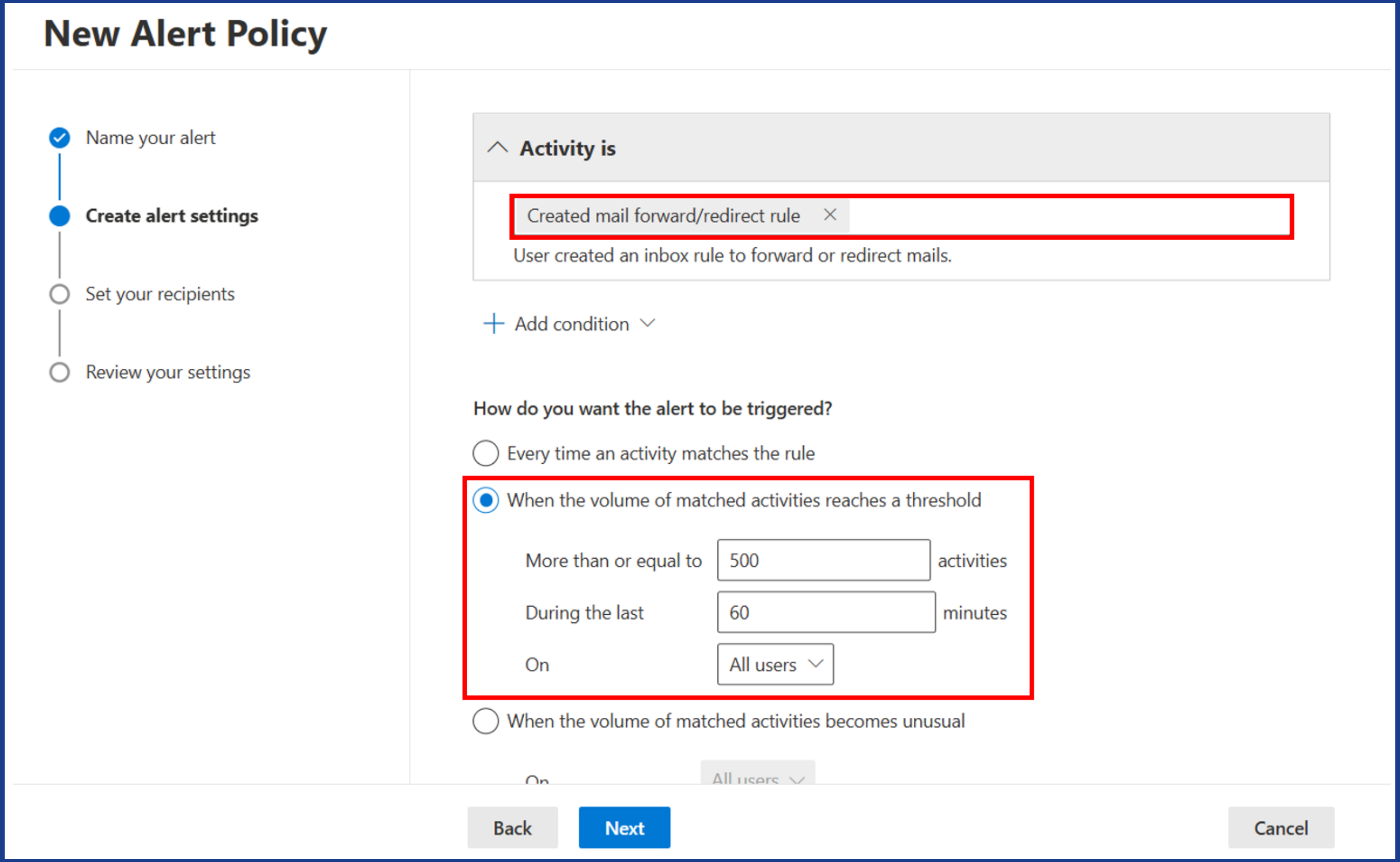
Name *
Mail Forwarding Alert

Description
Enter a friendly description for your policy

Severity *
● High

Category *
Mail flow

How to Implement?



New Alert Policy

- ✓ Name your alert
- ● **Create alert settings**
- ○ Set your recipients
- ○ Review your settings

Activity is

Created mail forward/redirect rule ✕

User created an inbox rule to forward or redirect mails.

+ Add condition

How do you want the alert to be triggered?

○ Every time an activity matches the rule

● When the volume of matched activities reaches a threshold

More than or equal to 500 activities

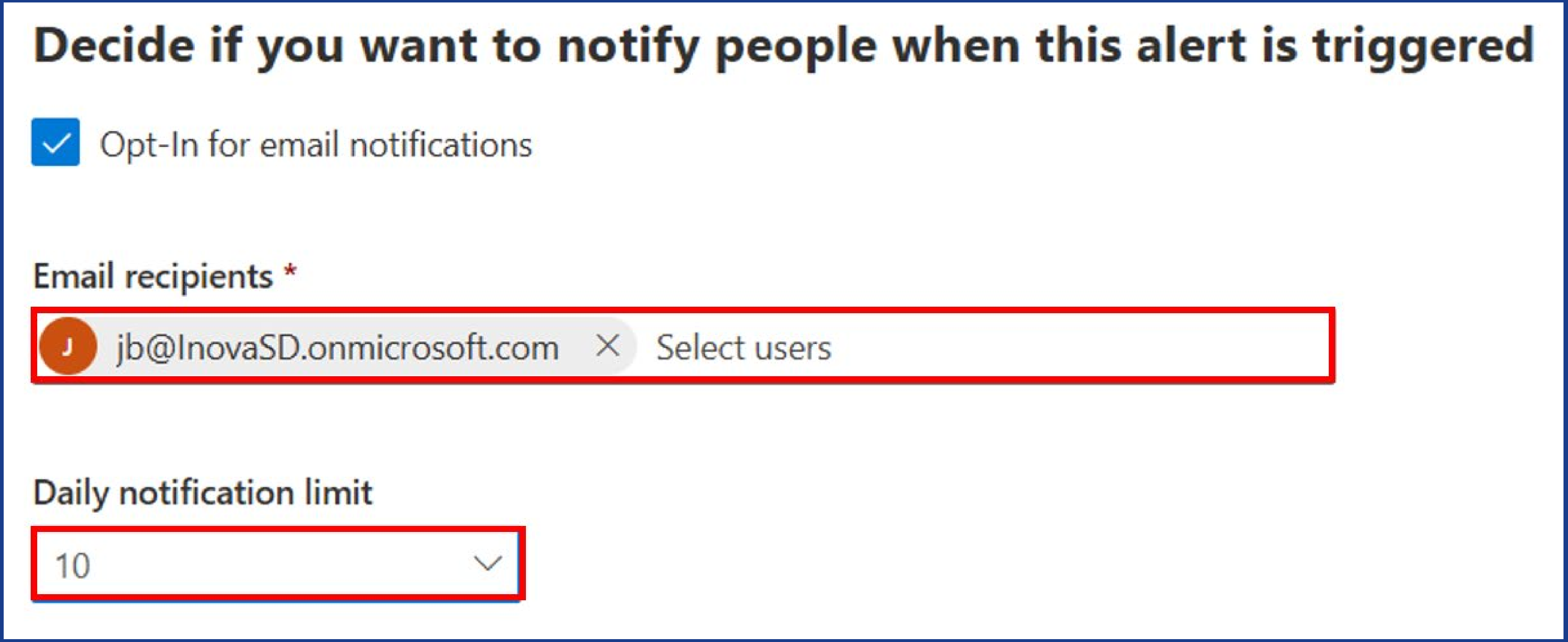
During the last 60 minutes

On All users

○ When the volume of matched activities becomes unusual

On All users

How to Implement?



Decide if you want to notify people when this alert is triggered

☑ Opt-In for email notifications

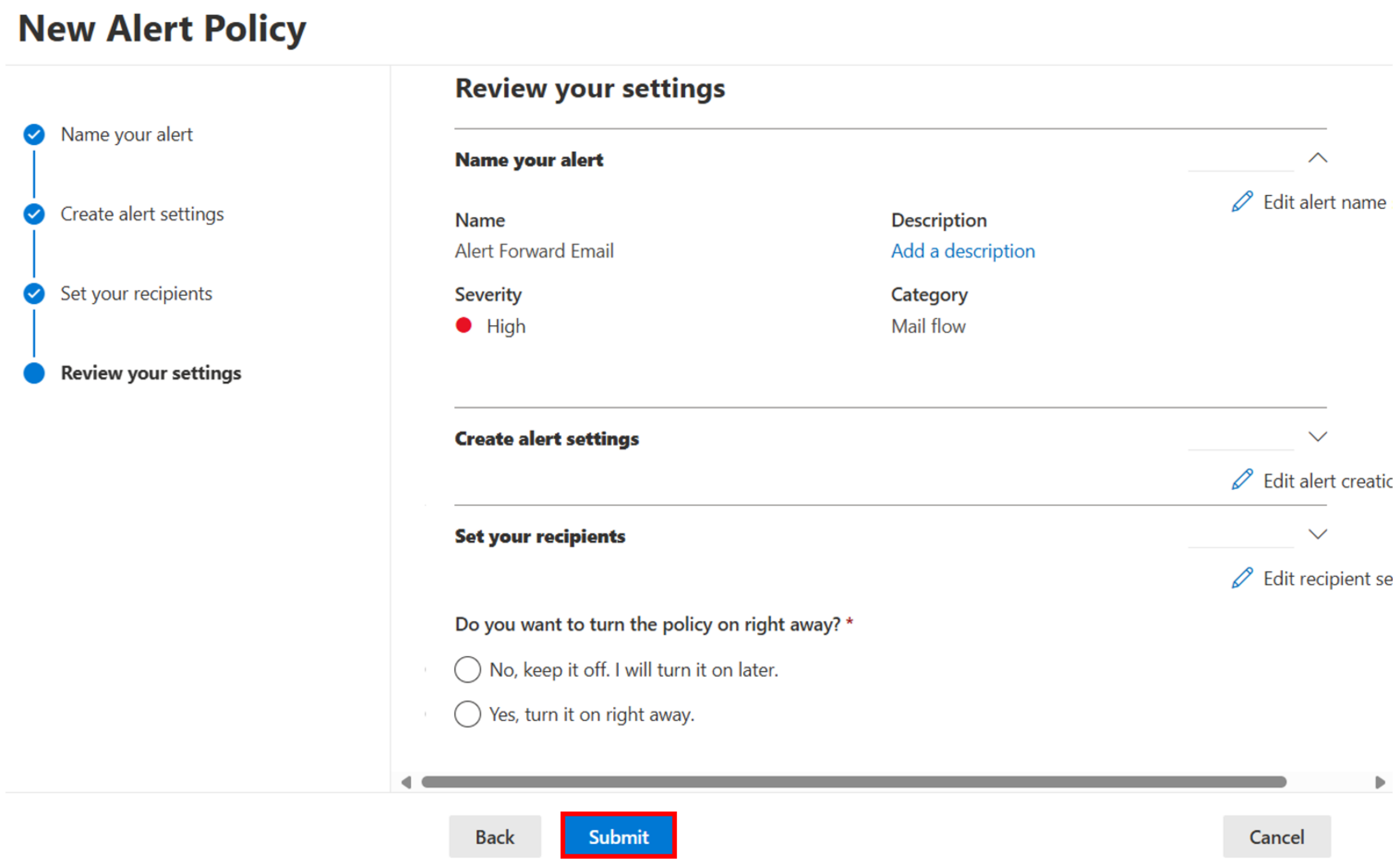
Email recipients *

jb@InovaSD.onmicrosoft.com × Select users

Daily notification limit

10

How to Implement?



New Alert Policy

- ✓ Name your alert
- ✓ Create alert settings
- ✓ Set your recipients
- ● **Review your settings**

Review your settings

Name your alert

Edit alert name

Name: Alert Forward Email

Description: Add a description

Severity: 🟥 High

Category: Mail flow

Create alert settings

Edit alert creatic

Set your recipients

Edit recipient se

Do you want to turn the policy on right away? *

○ No, keep it off. I will turn it on later.

○ Yes, turn it on right away.

BONUS: Rate Limiting

I taught More Emails were Always Good

Problem:

If a user account is compromised (via phishing or malware), attackers often:

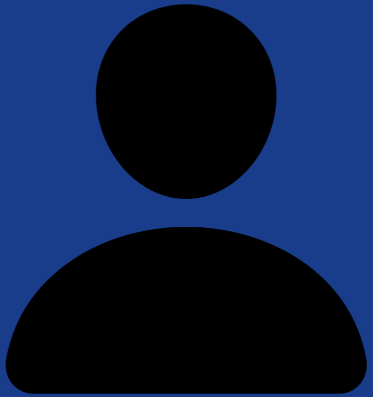
- Send thousands of external emails quickly
- Try to spread malware, phishing links, or spam
- Target clients, partners, or other users with your company’s reputation

This leads to:

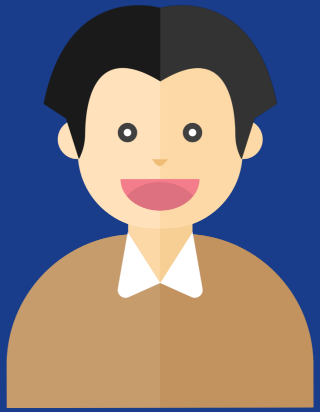
- Email blacklisting of your domain
- Loss of reputation with external parties
- Data leakage

Solution: Limiting the Recipients

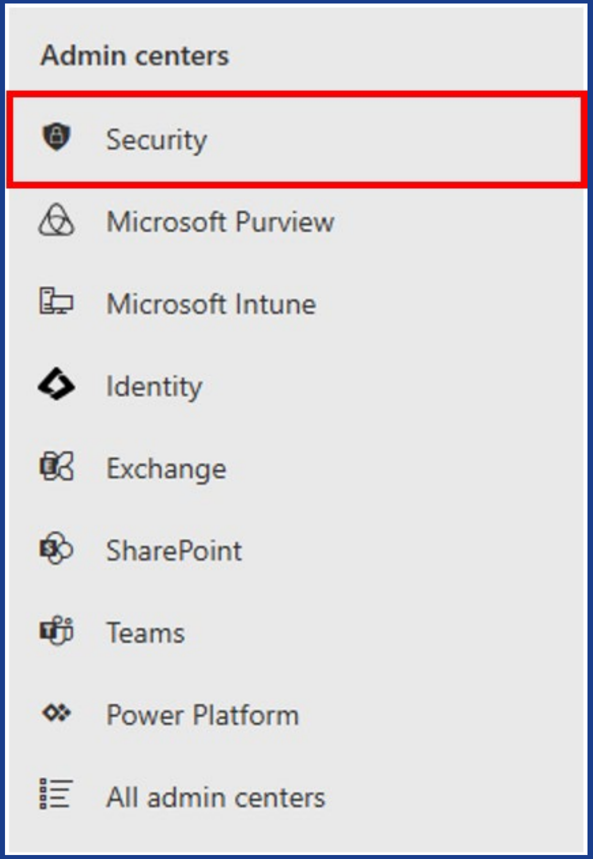
Limiting the number of **External** recipients a user can email per **hour**



Limiting the number of **internal** recipients a user can email per **hour**

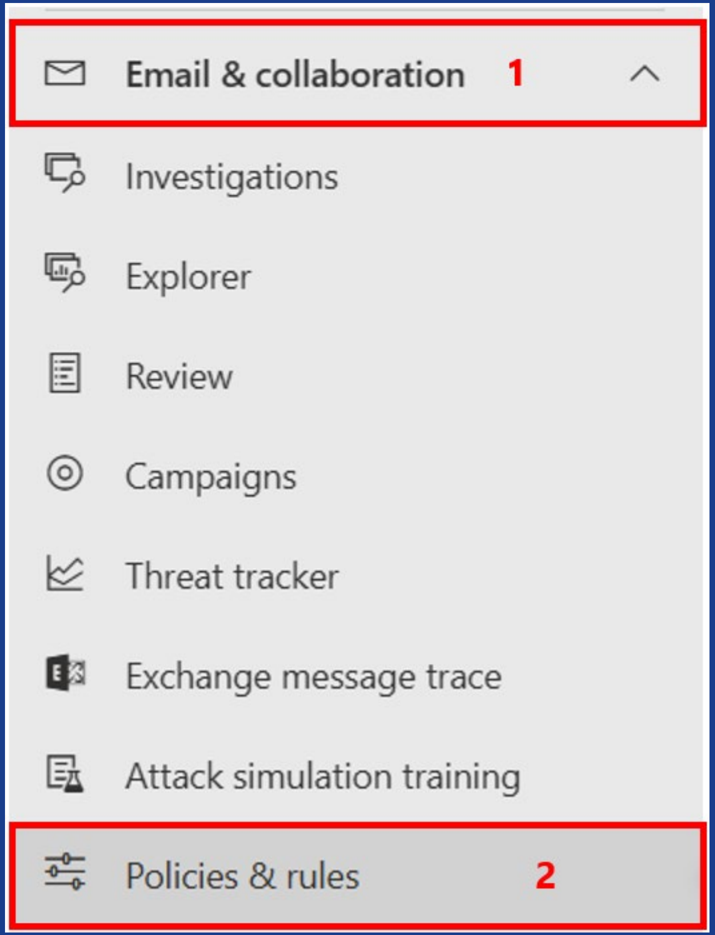


Limiting the Number of External Recipients



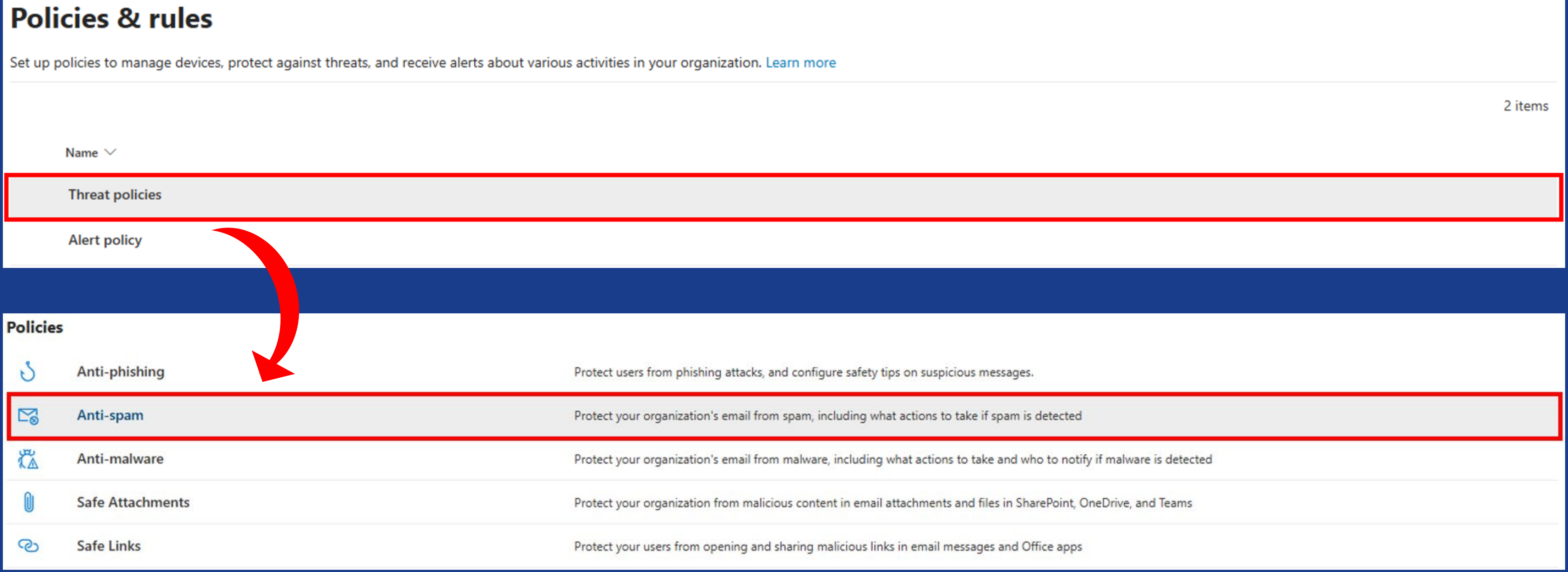
Admin centers

- Security
- Microsoft Purview
- Microsoft Intune
- Identity
- Exchange
- SharePoint
- Teams
- Power Platform
- All admin centers



- Email & collaboration 1
- Investigations
- Explorer
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules 2

Limiting the Number of External Recipients



Policies & rules

Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization. Learn more

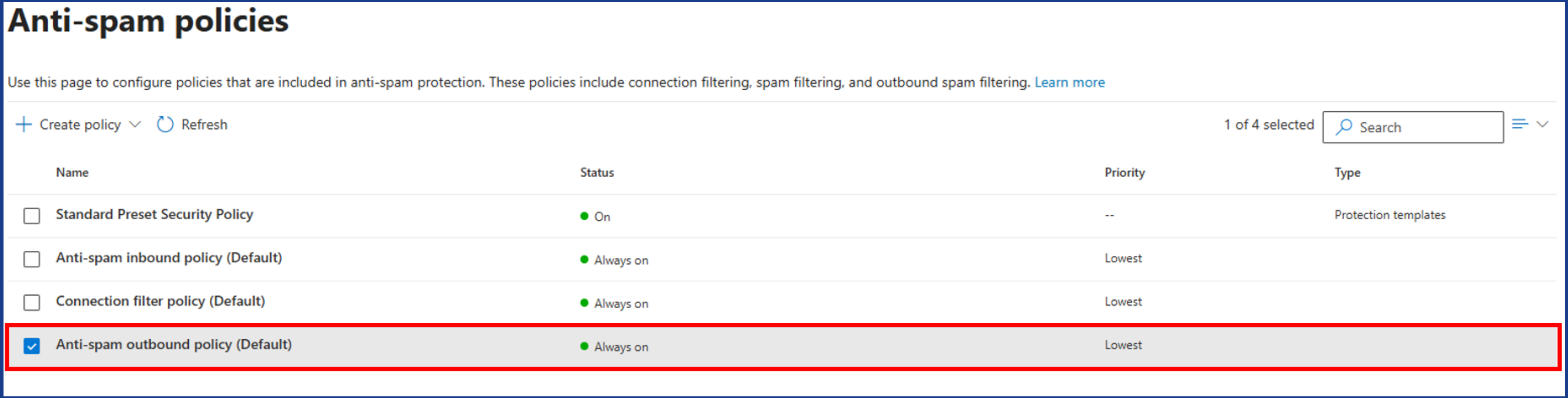
2 items

Name
Threat policies
Alert policy

Policies

Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

Limiting the Number of External Recipients

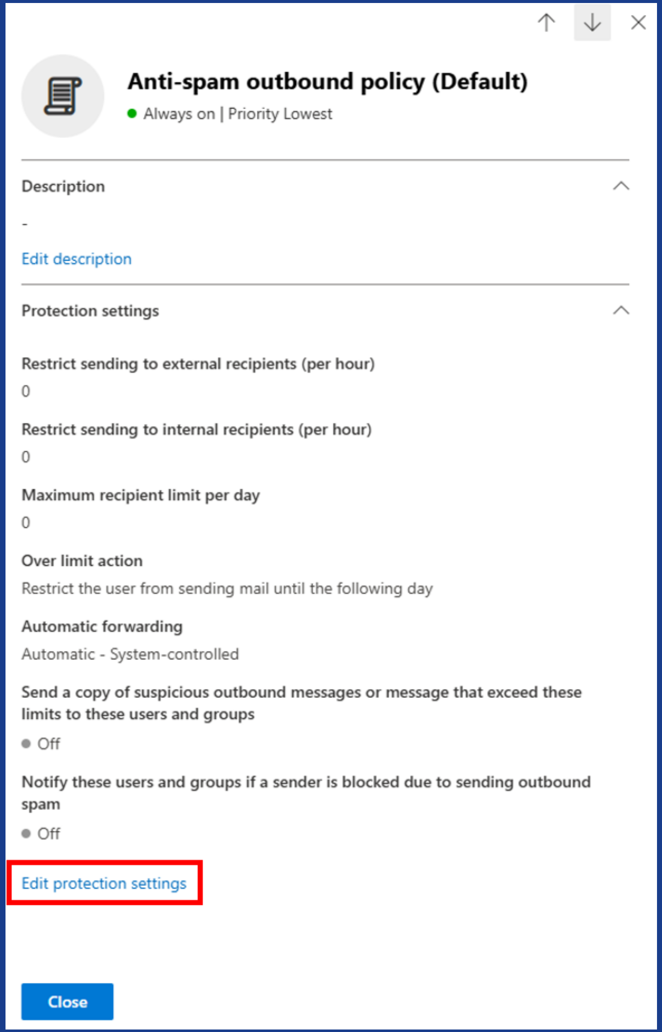


Anti-spam policies

Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, and outbound spam filtering. Learn more

	Name	Status	Priority	Type
☐	Standard Preset Security Policy	● On	--	Protection templates
☐	Anti-spam inbound policy (Default)	● Always on	Lowest	
☐	Connection filter policy (Default)	● Always on	Lowest	
☑	Anti-spam outbound policy (Default)	● Always on	Lowest	

Limiting the Number of External Recipients



Anti-spam outbound policy (Default)

● Always on | Priority Lowest

Description

-

Edit description

Protection settings

Restrict sending to external recipients (per hour)

0

Restrict sending to internal recipients (per hour)

0

Maximum recipient limit per day

0

Over limit action

Restrict the user from sending mail until the following day

Automatic forwarding

Automatic - System-controlled

Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups

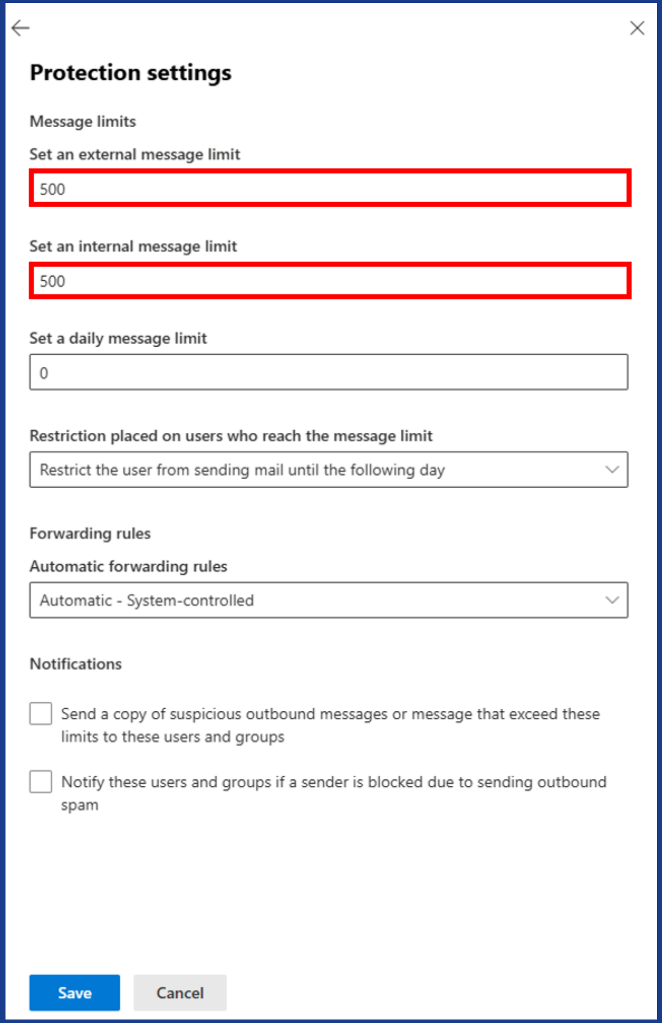
● Off

Notify these users and groups if a sender is blocked due to sending outbound spam

● Off

Edit protection settings

Close



Protection settings

Message limits

Set an external message limit

500

Set an internal message limit

500

Set a daily message limit

0

Restriction placed on users who reach the message limit

Restrict the user from sending mail until the following day

Forwarding rules

Automatic forwarding rules

Automatic - System-controlled

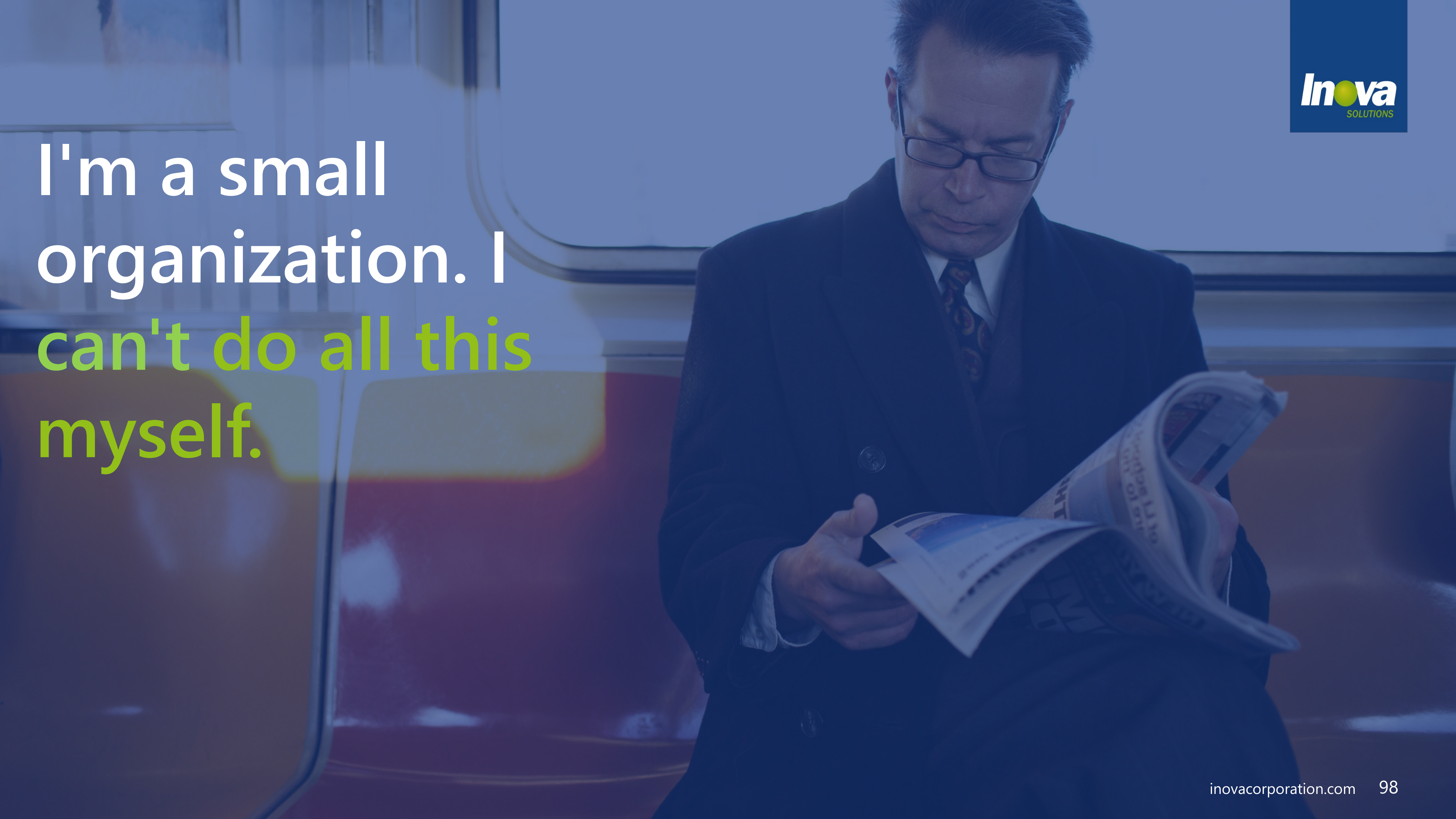
Notifications

□ Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups

□ Notify these users and groups if a sender is blocked due to sending outbound spam

Save

Cancel



I'm a small organization. I can't do all this myself.

The offer: only for the next 30 days

Microsoft
Solutions partner

1 Cloud + Copilot Security Assessment

- A thorough assessment of your tenant security + data protection policies
- Adjusted to your licensing
- Includes implementation of best practices

Starting at

USD $3150

2 G360 – Data backup & protect

- Backup solution for Microsoft 365, G Suite, and Salesforce
- Built-in security and compliance
- Can be managed by your team or ours

Starting at

USD $2.25 P/M

3 G360 – Security management

- Monitoring solution for the security of your M365 tenant
- Evaluate your tenant against a custom baseline
- Plans include monitoring, incident remediation, and continuous reporting

Starting at

USD $5.75 P/M

4 Inova Shield – Managed Services

- A single subscription for your SMB's IT needs.
- Currently limited to businesses with 50 seats or fewer.

Starting at

USD $115 P/M

Thank you!

Let’s connect

☎ (787) 793 2414

✉ sales@inovacorporation.com

inovacorporation.com