2020

HARDENING MICROSOFT 365 PLAYBOOK: BUSINESS EDITION

OVERVIEW AND USER GUIDE

Nick Ross | Microsoft Certified Expert Administrator

HARDENING MICROSOFT 365

OVERVIEW & USER GUIDE

PURPOSE

The primary purpose of this document is to minimize the potential for a data breach or a compromised account by following Microsoft security best practices and step through the actual configuration.

AUDIENCE

This document was designed for the SMB market who primarily work with the Business SKUs (Basic/Standard/Premium) available from Microsoft.

LAST UPDATED

May 2020

HARDENING MICROSOFT 365

OVERVIEW & USER GUIDE

CONTENTS

OVERVIEW & USER GUIDE

Checklist:

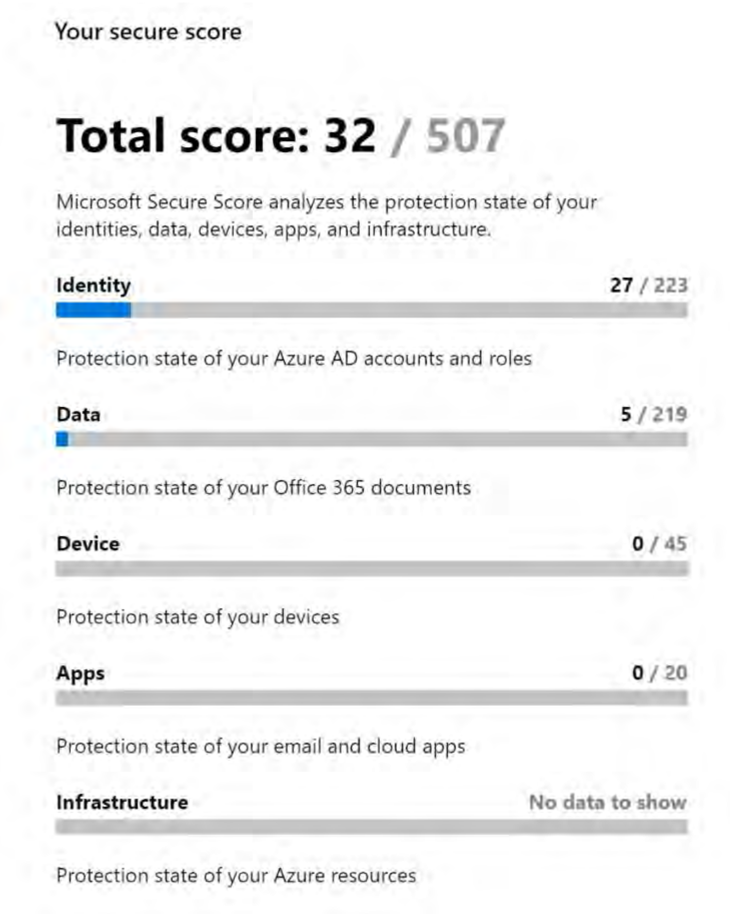
Azure Active Directory	
	Enable MFA
	Enable MFA For Admins
	Block Legacy Authentication
	Enable Self-Service Password Reset
	Do not expire passwords
	Delete/Block Accounts not used in last 30 days
	Designate more than 1 global admin but fewer than 5
	Do not allow users to grant consent to unmanaged applications

SharePoint and OneDrive	
	Configure Expiration Time for External Sharing Links
	Enable Versioning on all SharePoint Online document libraries
	Adopt the OneDrive Sync Client

OVERVIEW & USER GUIDE

Exchange Online		Auditing and Reporting	
	Enable Email Encryption		Review Mailbox Forwarding Rules Weekly
	Enable Client Rules Forwarding Block		Review the Mailbox Access Non-Owners Report Biweekly
	Set Outbound Spam Notifications		Review the Malware Detections Report Weekly
	Do not allow Mailbox Delegation		Review your account provisioning activity report weekly
	Set up Connection filtering		Enable Audit Log Search
	Spam Filtering Policy		Enable Mailbox Auditing for all Users
	Malware Policy		Review Role Changes Weekly
	Anti-phishing policy		
	Configure Enhanced Filtering		
	Configure ATP Safe Links and Attachments		
	Add SPF, DKIM, and DMAC		
	Do not allow calendar sharing details		

USING MICROSOFT SECURE SCORE



Your secure score

Total score: 32 / 507

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure.

Identity 27 / 223

Protection state of your Azure AD accounts and roles

Data 5 / 219

Protection state of your Office 365 documents

Device 0 / 45

Protection state of your devices

Apps 0 / 20

Protection state of your email and cloud apps

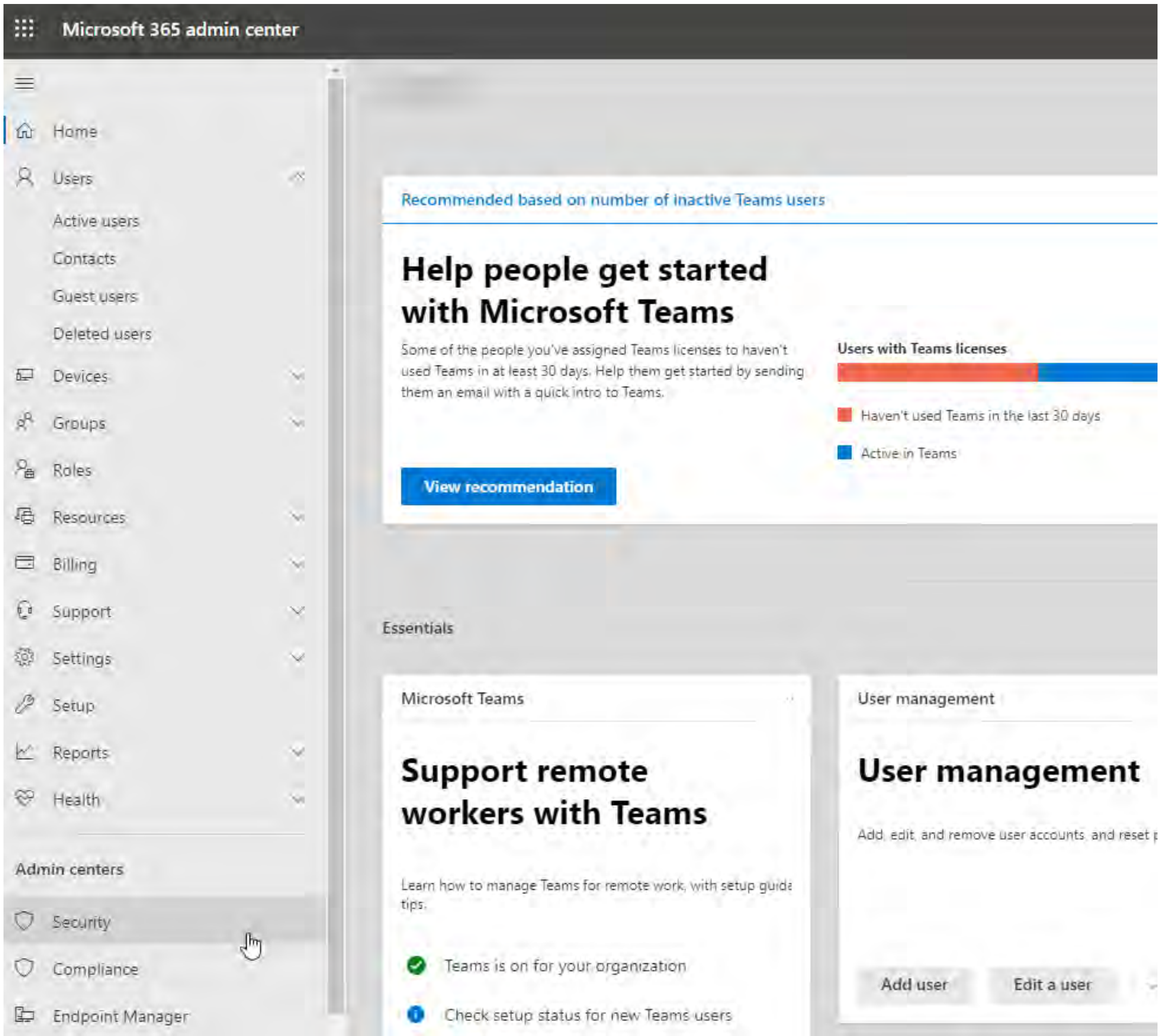
Infrastructure No data to show

Protection state of your Azure resources

You can think of Secure Score like a credit score for Microsoft. Secure Score figures out what Microsoft services you're using (like OneDrive, SharePoint, and Exchange) then looks at your settings and activities and compares them to a baseline established by Microsoft. You'll get a score based on how aligned you are with best security practices. The numerator is your current point value and the denominator is the amount of points available based on the security features you have available to configure. You can see the list of available security options for each Microsoft plan by clicking on this link.

Microsoft compares your score to 365 accounts with a similar seat size as your organization and allows you to configure your Industry Type to compare your score to others in your industry as well.

You can get to your tenant's Secure Score by logging into their 365 Admin Center with global admin creds and clicking on "Security" under Admin Centers.



Help people get started with Microsoft Teams

Some of the people you've assigned Teams licenses to haven't used Teams in at least 30 days. Help them get started by sending them an email with a quick intro to Teams.

Support remote workers with Teams

Learn how to manage Teams for remote work, with setup guide tips.

✓ Teams is on for your organization

ⓘ Check setup status for new Teams users

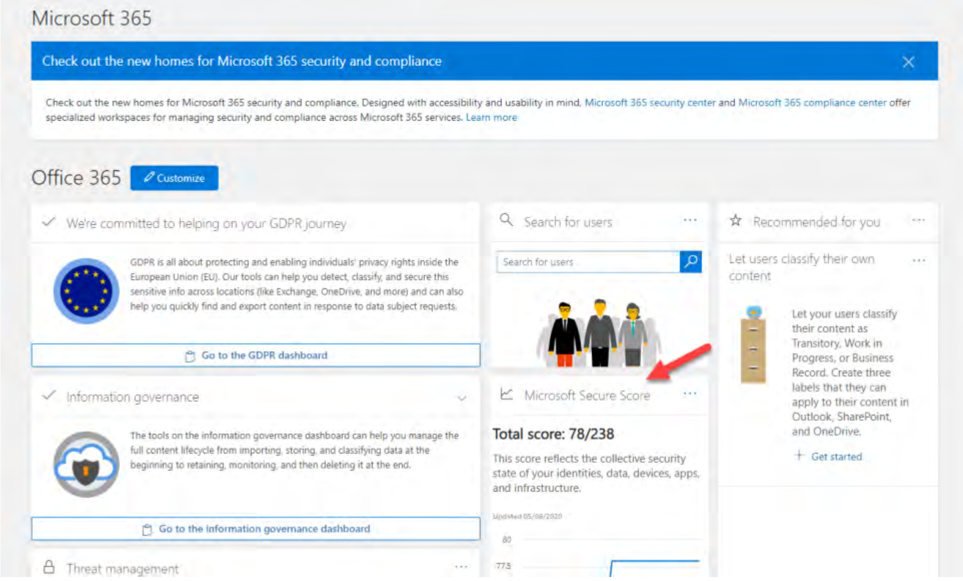
User management

Add, edit, and remove user accounts, and reset p

OVERVIEW & USER GUIDE

Here you will be able to click on the Secure Score data to see the recommendations. Some of the recommendations made in this guide come from Secure Score but we wanted to show you this location as it will update over time.

Classic View:



Microsoft 365

Check out the new homes for Microsoft 365 security and compliance

Check out the new homes for Microsoft 365 security and compliance. Designed with accessibility and usability in mind, Microsoft 365 security center and Microsoft 365 compliance center offer specialized workspaces for managing security and compliance across Microsoft 365 services. Learn more

Office 365

We're committed to helping on your GDPR journey

GDPR is all about protecting and enabling individuals' privacy rights inside the European Union (EU). Our tools can help you detect, classify, and secure this sensitive info across locations (like Exchange, OneDrive, and more) and can also help you quickly find and export content in response to data subject requests.

Go to the GDPR dashboard

Information governance

The tools on the information governance dashboard can help you manage the full content lifecycle from importing, storing, and classifying data at the beginning to retaining, monitoring, and then deleting it at the end.

Go to the information governance dashboard

Threat management

Search for users

Microsoft Secure Score

Total score: 78/238

This score reflects the collective security state of your identities, data, devices, apps, and infrastructure.

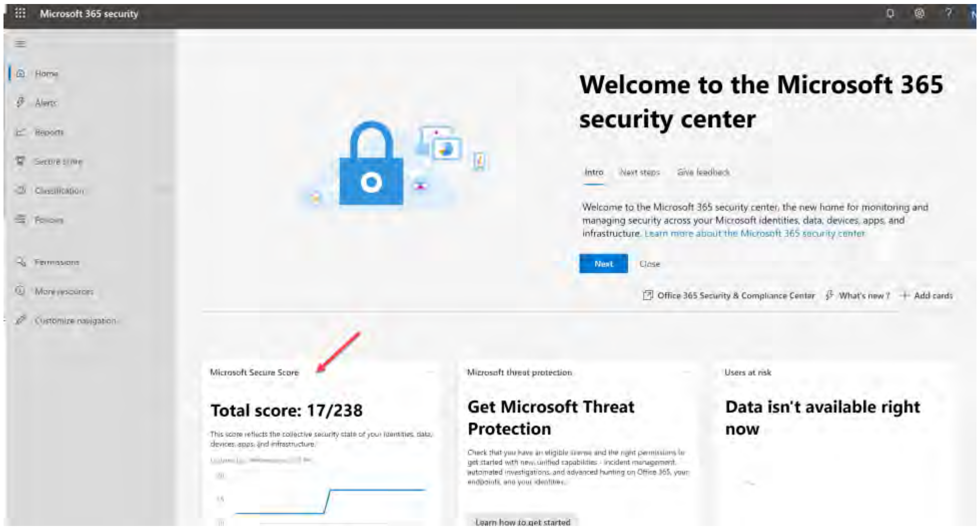
Updated 05/08/2020

Recommended for you

Let users classify their own content

Let your users classify their content as Transitory, Work in Progress, or Business Record. Create three labels that they can apply to their content in Outlook, SharePoint, and OneDrive.

Modern View:



Microsoft 365 security

Welcome to the Microsoft 365 security center

Welcome to the Microsoft 365 security center, the new home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure. Learn more about the Microsoft 365 security center

Microsoft Secure Score

Total score: 17/238

This score reflects the collective security state of your identities, data, devices, apps, and infrastructure.

Microsoft threat protection

Get Microsoft Threat Protection

Check that you have an eligible license and the right permissions to get started with new, unified capabilities - incident management, automated investigations, and advanced hunting on Office 365, your endpoints, and your identities.

Users at risk

Data isn't available right now

AZURE ACTIVE DIRECTORY

Enable MFA

You should enable MFA for all of your user accounts because a breach of any of those accounts can lead to a breach of any data that user has access to. MFA is encouraged to be mandatory across all users, especially in today's remote workforce. At a minimum, it should be enforced on all global admins.

Compliance Controls:

- CSA CCM301; Control DSI-02
- FedRAMP Moderate; Control IA-3
- GDPR; Control 6.6.5
- ISO 27018:2014; Control C.9.4.2, Control A.10.8
- NIST 800-171; Control 3.5.2
- NIST 800-53; Control IA-3

As of February 29, 2020, Microsoft enforced security defaults in tenants in efforts to enhance security. Security defaults is on in net new tenants that you spin up after this date and enforces the following:

- MFA on all accounts
- Blocks Legacy Authentication (IMAP/POP/SMTP)
- Enforcing MFA for users who access the Azure Portal, Azure PowerShell, Azure CLI
- Click here for the full article

OVERVIEW & USER GUIDE

Security defaults are NOT a hard requirement for non-partner tenants but are recommended. If you have a tenant licensed with conditional access, it is recommended that you enforce conditional access policies instead of security defaults. Both CANNOT be turned on at the same time. If you enable a conditional access policy, then you will have to turn off security defaults. MFA can also be enabled in the legacy portal but that will be deprecated in the future. For now, we will show you all three ways to enable MFA for users.

Licensing Considerations:

Enabling MFA and Security Defaults:

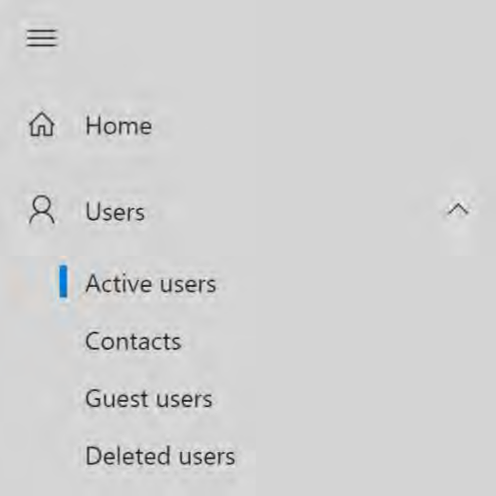
- All Microsoft licensing plans

Enabling Conditional Access Policies

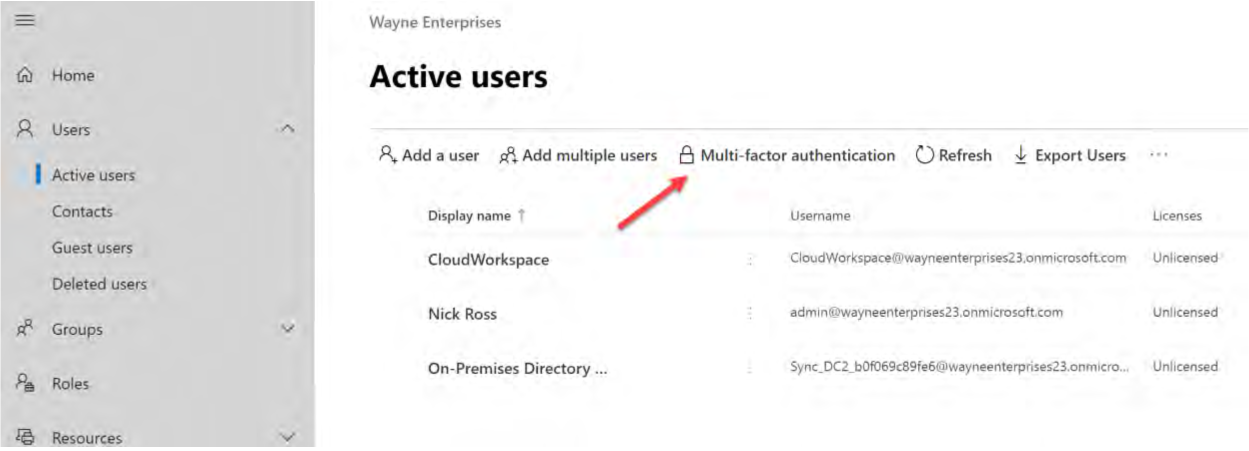
- Microsoft 365 Business Premium ($20/u/m)
- EMS + E3 ($87.5) or EMS + E5 ($14.80)
- Microsoft 365 E3 ($32) or Microsoft 365 E5 ($64)

Legacy Portal:

1. Go to the 365 Admin Center>Users>Active Users



2. Click Multi-factor Authentication

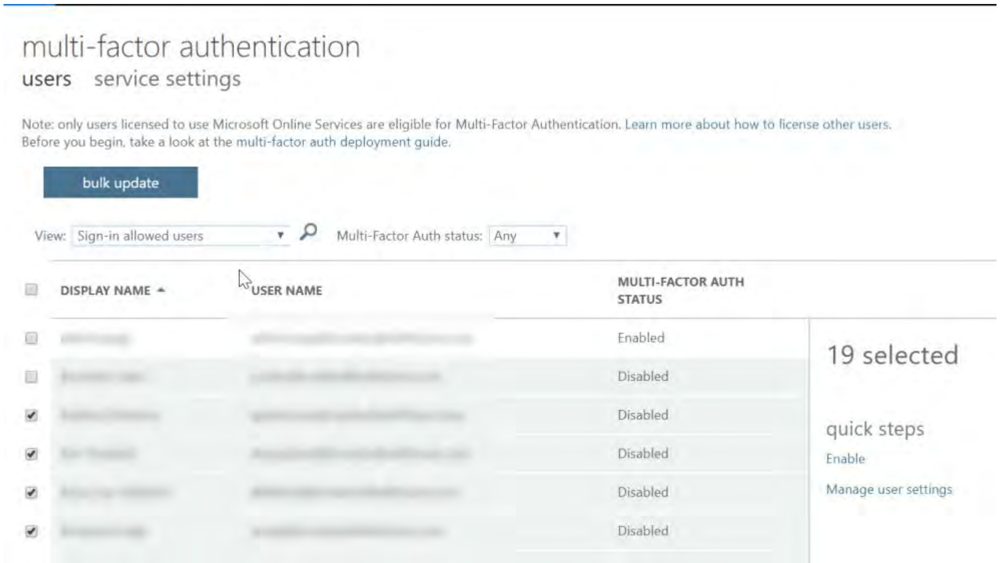


Wayne Enterprises

Active users

Display name ↑	Username	Licenses
CloudWorkspace	CloudWorkspace@wayneenterprises23.onmicrosoft.com	Unlicensed
Nick Ross	admin@wayneenterprises23.onmicrosoft.com	Unlicensed
On-Premises Directory ...	Sync_DC2_b0f069c89fe6@wayneenterprises23.onmicro...	Unlicensed

3. Select users to enable multi-factor authentication



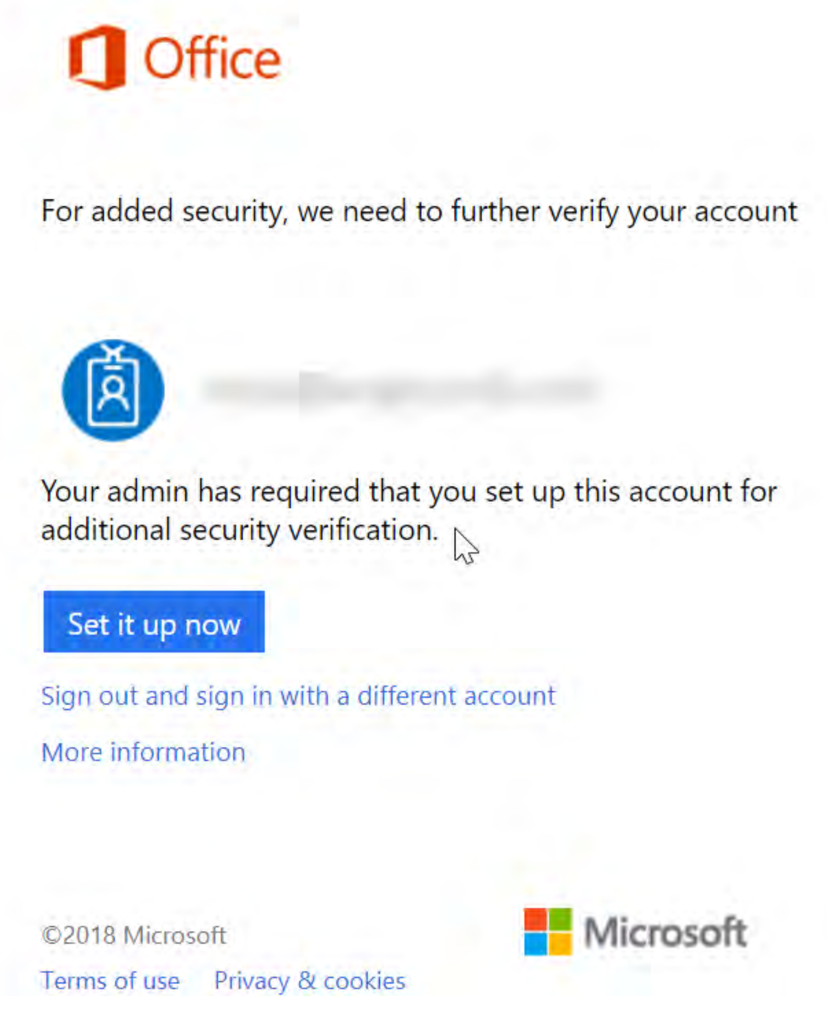
multi-factor authentication

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

□	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
□	[redacted]	[redacted]	Enabled
□	[redacted]	[redacted]	Disabled
☑	[redacted]	[redacted]	Disabled
☑	[redacted]	[redacted]	Disabled
☑	[redacted]	[redacted]	Disabled
☑	[redacted]	[redacted]	Disabled

19 selected

4. The next time the user signs in they will be prompted with the following:



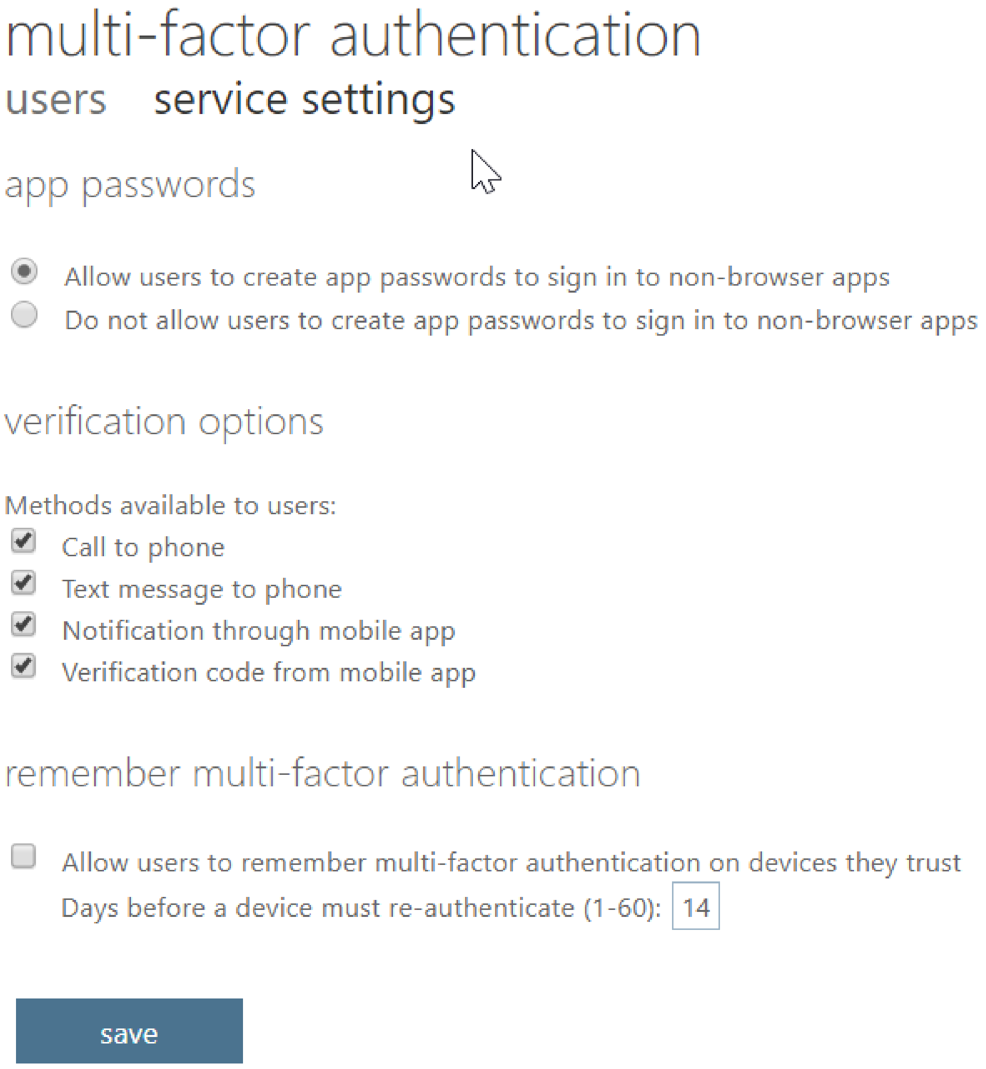
For added security, we need to further verify your account

[redacted]

Your admin has required that you set up this account for additional security verification.

OVERVIEW & USER GUIDE

5. Depending on your settings they will enter a phone used for the second form of authentication. You can adjust the settings by going to Service Settings on the top of the multi-factor page



multi-factor authentication

users service settings

app passwords

● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

☑ Call to phone
☑ Text message to phone
☑ Notification through mobile app
☑ Verification code from mobile app

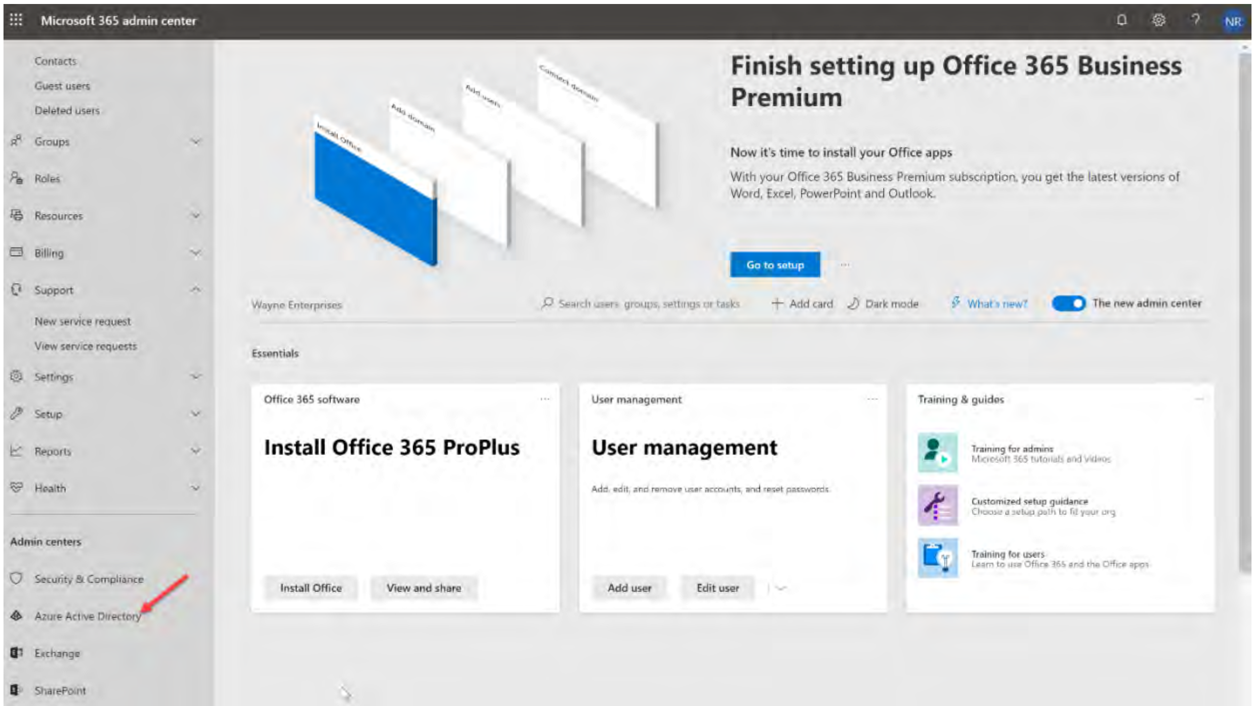
remember multi-factor authentication

□ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60): 14

Security Defaults:

1. In the 365 Admin Portal, click on the Azure Active Directory link under Admin Centers



Finish setting up Office 365 Business Premium

Now it's time to install your Office apps

With your Office 365 Business Premium subscription, you get the latest versions of Word, Excel, PowerPoint and Outlook.

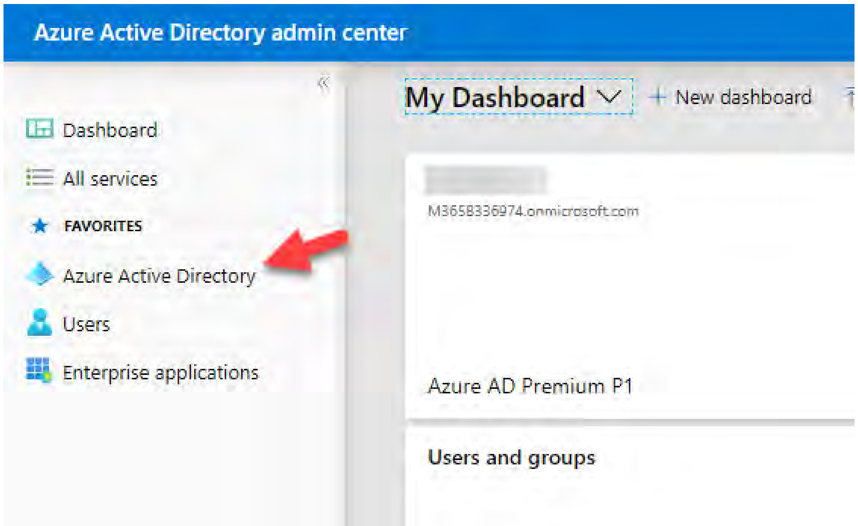
User management: Add, edit, and remove user accounts, and reset passwords

Training for admins: Microsoft 365 tutorials and videos

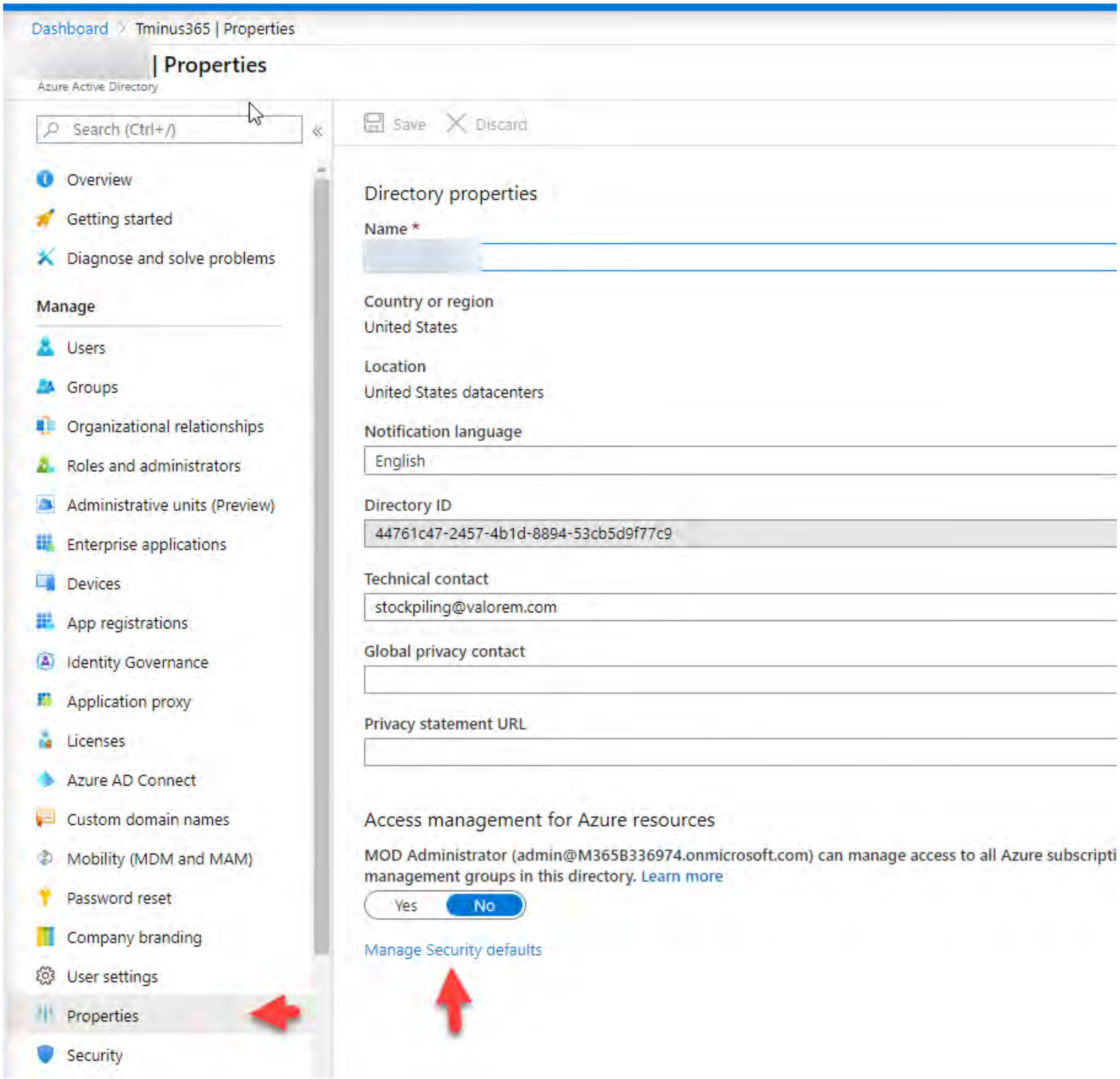
Customized setup guidance: Choose a setup path to fit your org

Training for users: Learn to use Office 365 and the Office apps

2. Click Azure Active Directory



3. Click Manage>Manage Security Defaults



Directory properties

Name *

[redacted]

Country or region

United States

Location

United States datacenters

Notification language

English

Directory ID

44761c47-2457-4b1d-8894-53cb5d9f77c9

Technical contact

stockpiling@valorem.com

Global privacy contact

Privacy statement URL

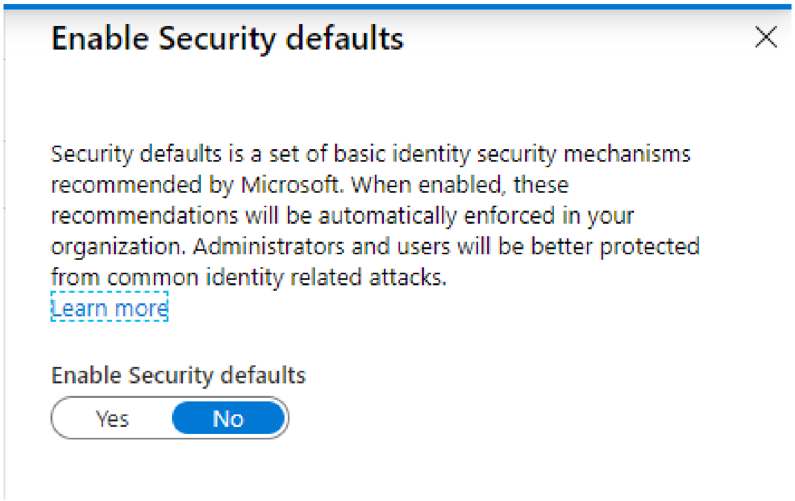
Access management for Azure resources

MOD Administrator (admin@M365B336974.onmicrosoft.com) can manage access to all Azure subscripti management groups in this directory. Learn more

Yes [✓ No]

Manage Security defaults

4. Toggle on Security Defaults



Enable Security defaults

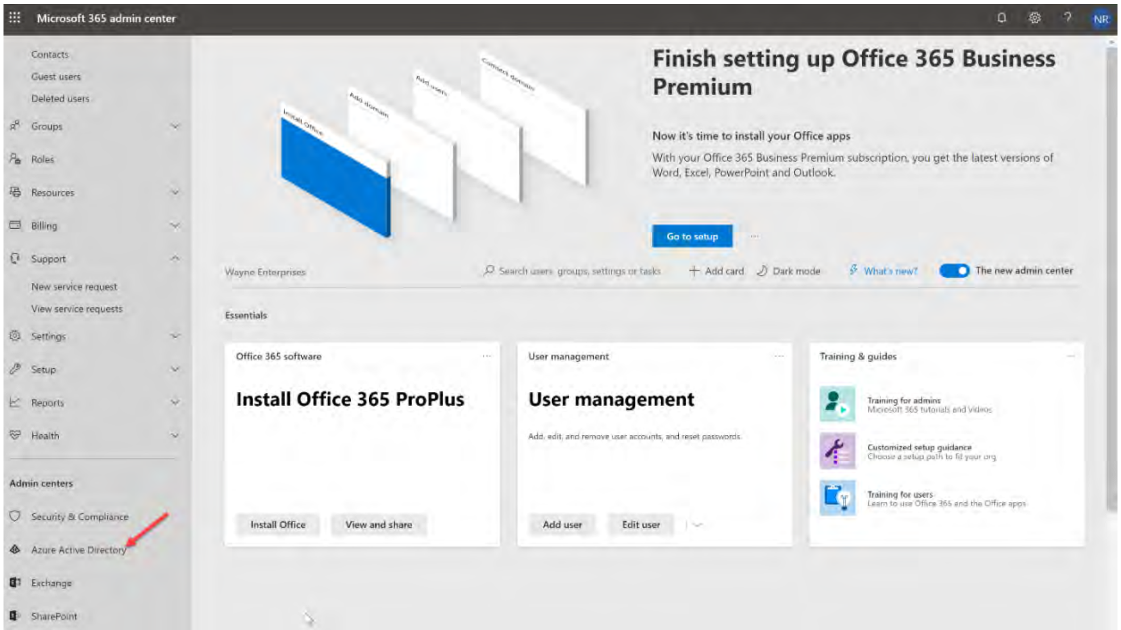
Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.
Learn more

Enable Security defaults: Yes [✓ No]

NOTE Turning on security defaults enforces MFA for all users. They will have 14 days to register after their first sign-in after you turn this on and they will only be able to use the Microsoft Authenticator app as their second form of authentication. Be sure to plan and communicate accordingly.

Conditional Access

1. In the 365 Admin Portal, click on the Azure Active Directory link under Admin Centers



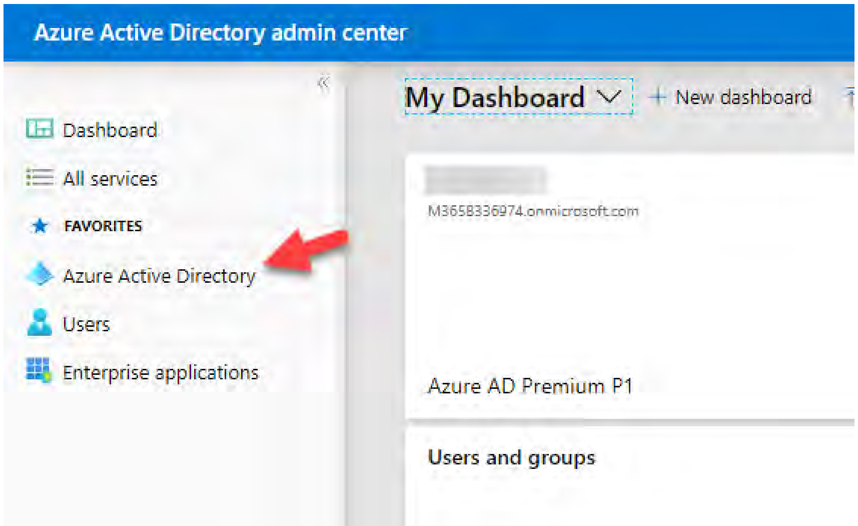
Finish setting up Office 365 Business Premium

Now it's time to install your Office apps

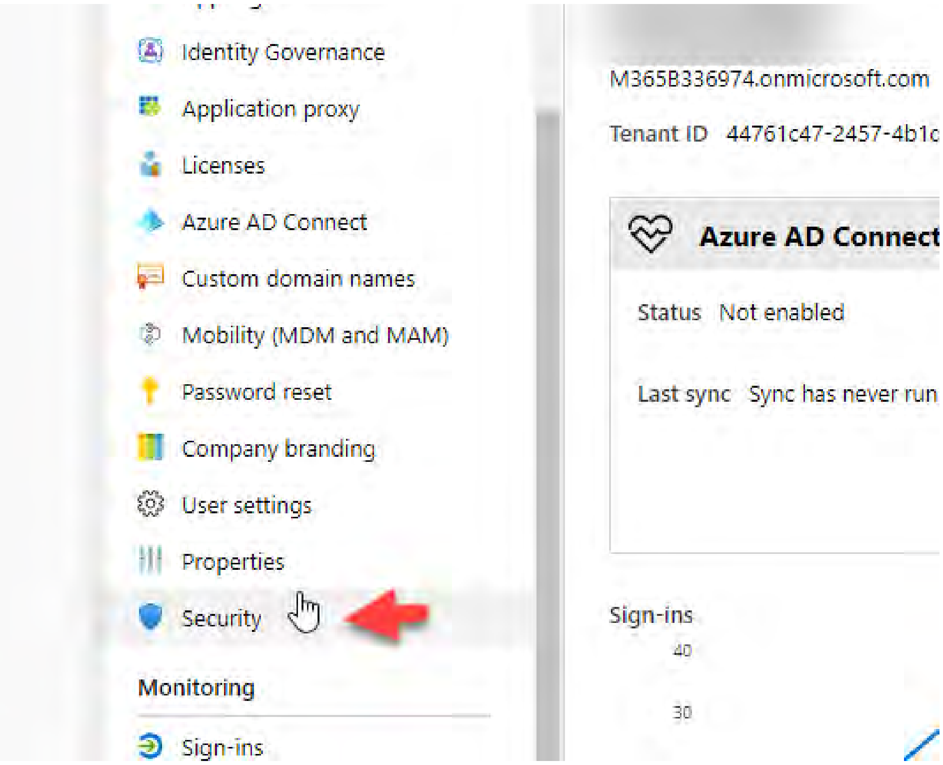
With your Office 365 Business Premium subscription, you get the latest versions of Word, Excel, PowerPoint and Outlook.

Add, edit, and remove user accounts, and reset passwords.

2. Click Azure Active Directory



3. Scroll down and click Security



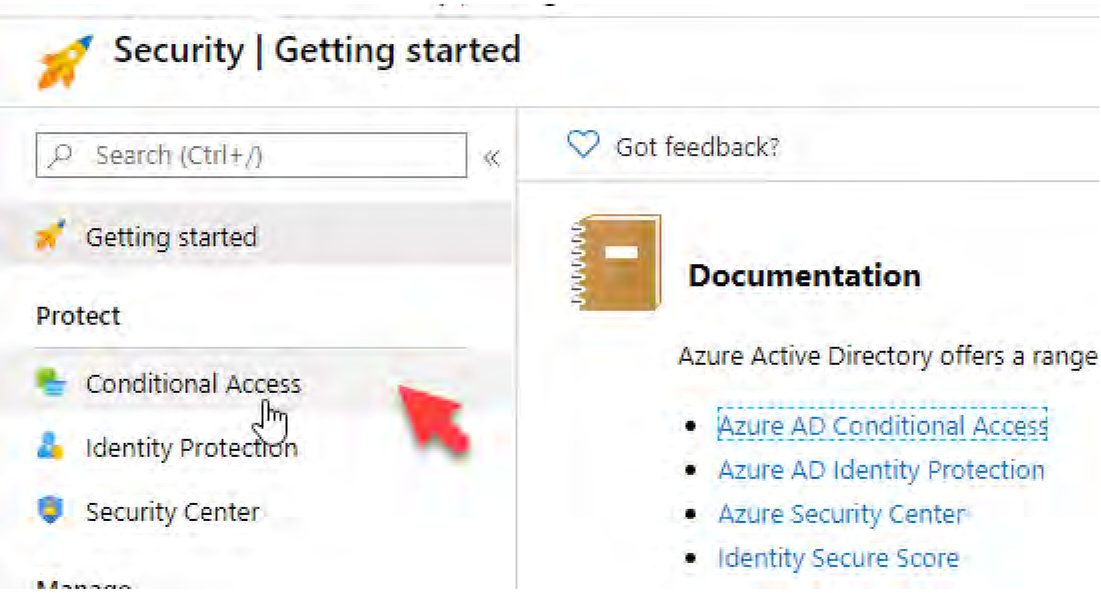
M365B336974.onmicrosoft.com

Tenant ID 44761c47-2457-4b1c

Status Not enabled

Last sync Sync has never run

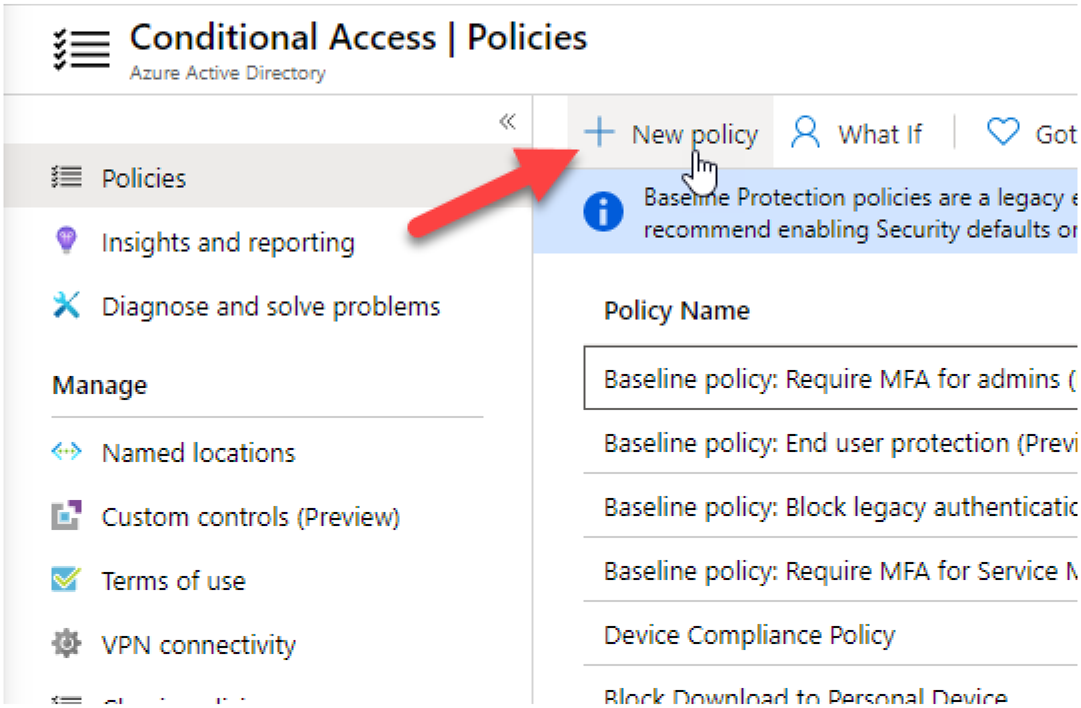
4. Click Conditional Access



Azure Active Directory offers a range

- Azure AD Conditional Access
- Azure AD Identity Protection
- Azure Security Center
- Identity Secure Score

5. Click New Policy



Conditional Access | Policies

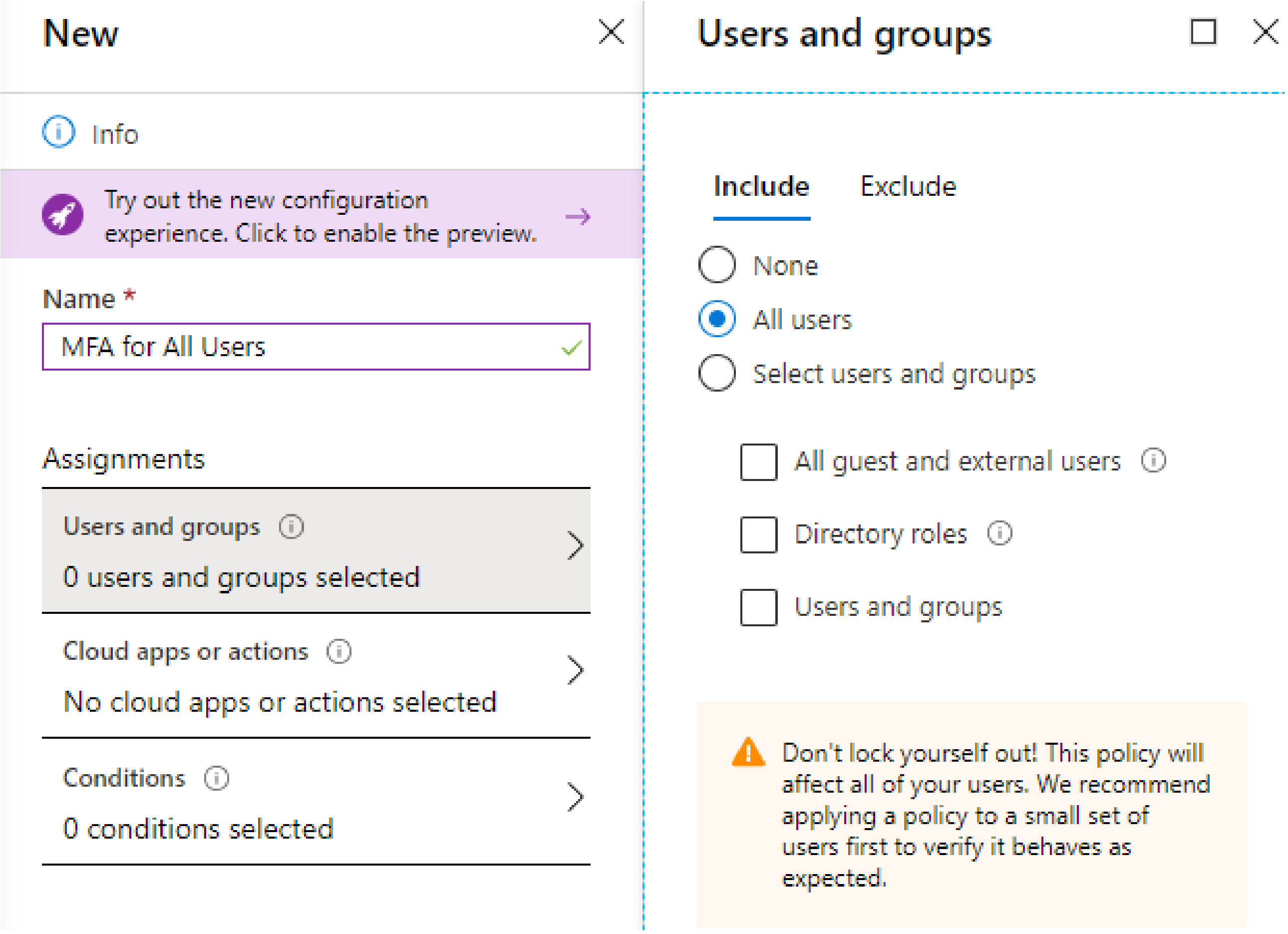
Azure Active Directory

Baseline Protection policies are a legacy e recommend enabling Security defaults or

Policy Name
Baseline policy: Require MFA for admins (
Baseline policy: End user protection (Previ
Baseline policy: Block legacy authenticatic
Baseline policy: Require MFA for Service N
Device Compliance Policy
Block Download to Personal Device

6. Give your policy a name and select all users under the users and groups blade

OVERVIEW & USER GUIDE



New

ⓘ Info

Try out the new configuration experience. Click to enable the preview. →

Name *

MFA for All Users ✓

Assignments

Users and groups ⓘ
0 users and groups selected

Cloud apps or actions ⓘ
No cloud apps or actions selected

Conditions ⓘ
0 conditions selected

Users and groups

Include | Exclude

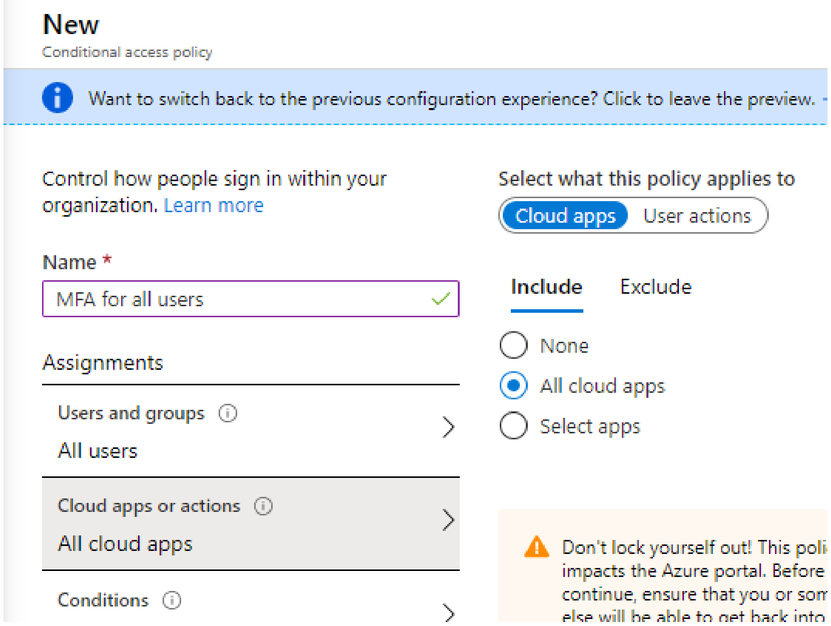
○ None
● All users
○ Select users and groups

□ All guest and external users ⓘ
□ Directory roles ⓘ
□ Users and groups

⚠ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

NOTE Microsoft gives you multiple warnings not to lock yourself out of the account. It is recommended that you create a break-glass global admin account so that you can get back in if you lose 2-factor on your primary account. You could use the exclude tab here to exclude that user from this list.

7. Select All Cloud Apps



New
Conditional access policy

Want to switch back to the previous configuration experience? Click to leave the preview.

Control how people sign in within your organization. Learn more

Name *
MFA for all users

Assignments

Users and groups
All users

Cloud apps or actions
All cloud apps

Conditions

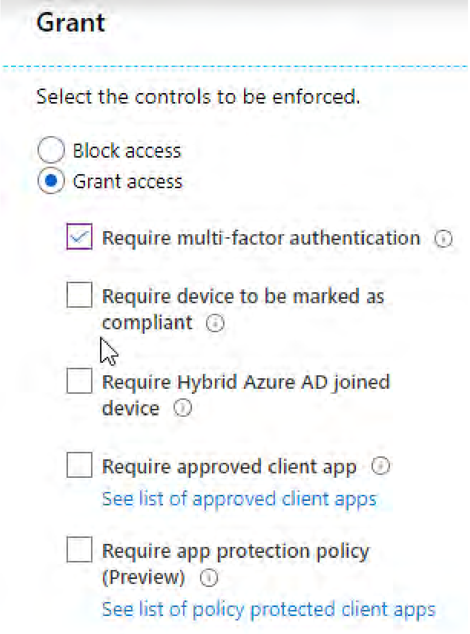
Select what this policy applies to
● Cloud apps ○ User actions

Include | Exclude

○ None
● All cloud apps
○ Select apps

Don't lock yourself out! This poli
impacts the Azure portal. Before
continue, ensure that you or som
else will be able to get back into

8. Skip the conditions section and in the Grant section, select Require Multi-factor Authentication



Grant

Select the controls to be enforced.

○ Block access
● Grant access

☑ Require multi-factor authentication

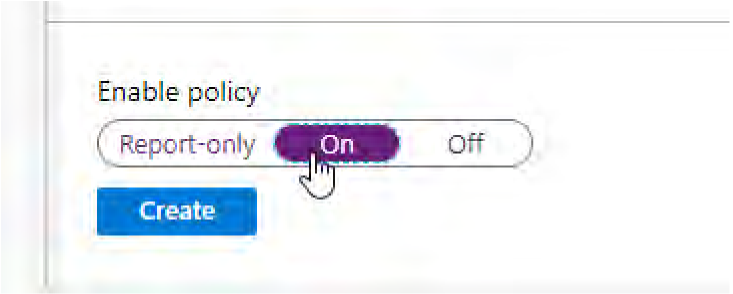
□ Require device to be marked as compliant

□ Require Hybrid Azure AD joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy (Preview)
See list of policy protected client apps

9. Enable the policy and click Create



PowerShell:

Enable MFA for all users

PowerShell Script

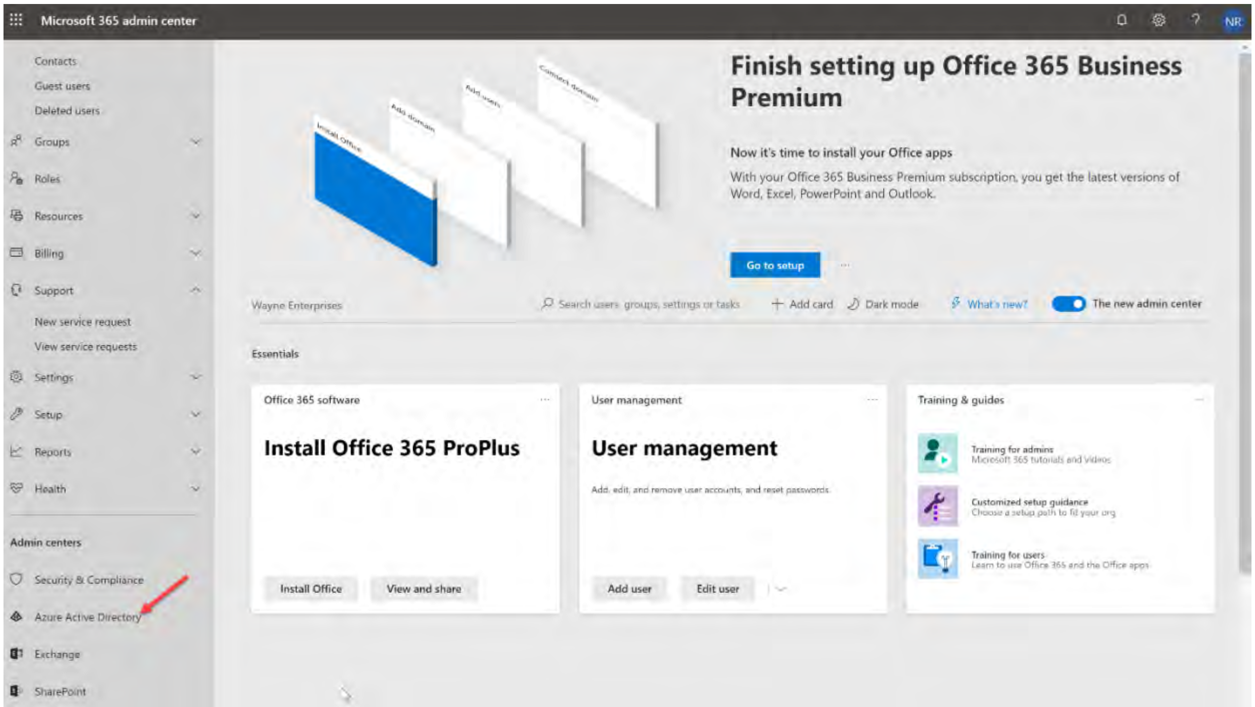
Enable MFA For Admins

If you are not going to want to turn MFA on for all users in the organization, you should at least be turning it on for privileged roles like global admins, exchange admins, etc. Dedicated accounts like global admin roles should ONLY be used when performing admin task and generally should not be used for day-to-day end-user functions. This will help reduce your attack surface from the standpoint of a privileged account. Note that you can enable MFA on admin users via the legacy MFA portal as shown in the previous section or with a conditional access policy which will be shown here.

Compliance Controls:

- CSA CCM301; Control DSI-02
- FedRAMP Moderate; Control IA-3
- GDPR; Control 6.6.5
- ISO 27018:2014; Control C.9.4.2, Control A.10.8
- NIST 800-171; Control 3.5.2
- NIST 800-53; Control IA-3

1. In the 365 Admin Portal, click on the Azure Active Directory link under Admin Centers



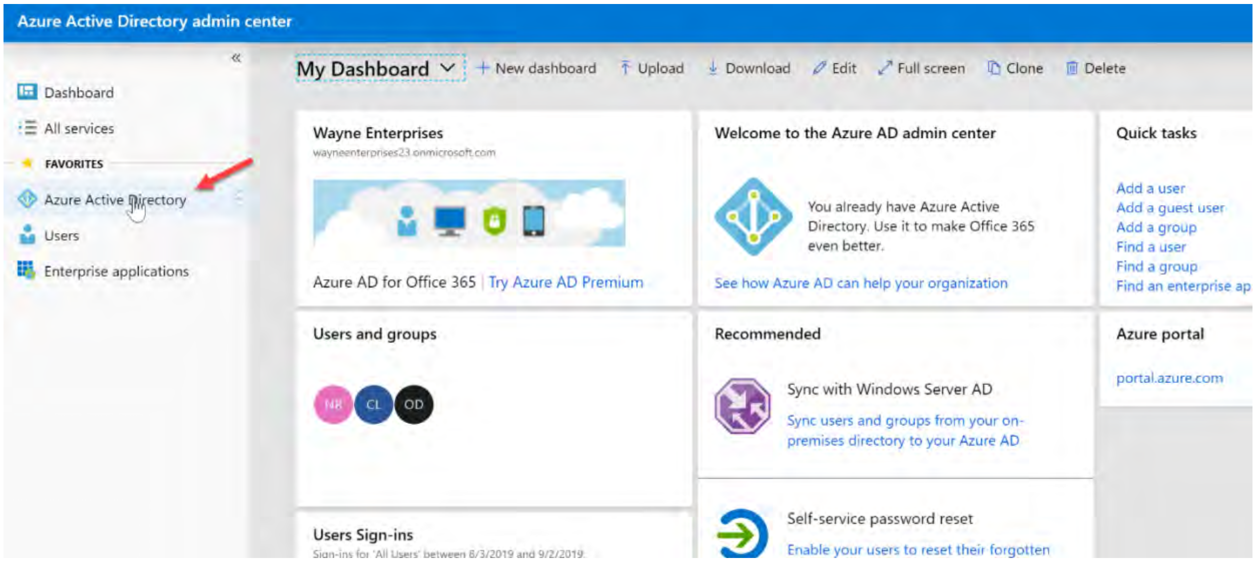
Finish setting up Office 365 Business Premium

Now it's time to install your Office apps

With your Office 365 Business Premium subscription, you get the latest versions of Word, Excel, PowerPoint and Outlook.

Add, edit, and remove user accounts, and reset passwords.

2. Click Azure Active Directory



You already have Azure Active Directory. Use it to make Office 365 even better.

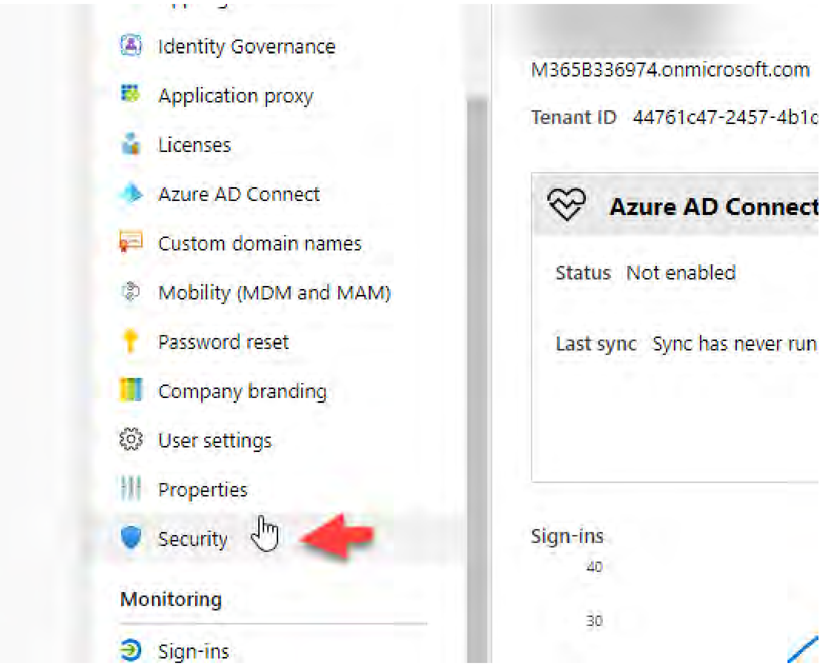
Sync users and groups from your on-premises directory to your Azure AD

Enable your users to reset their forgotten

Sign-ins for 'All Users' between 8/3/2019 and 9/2/2019

OVERVIEW & USER GUIDE

3. Scroll down and click Security



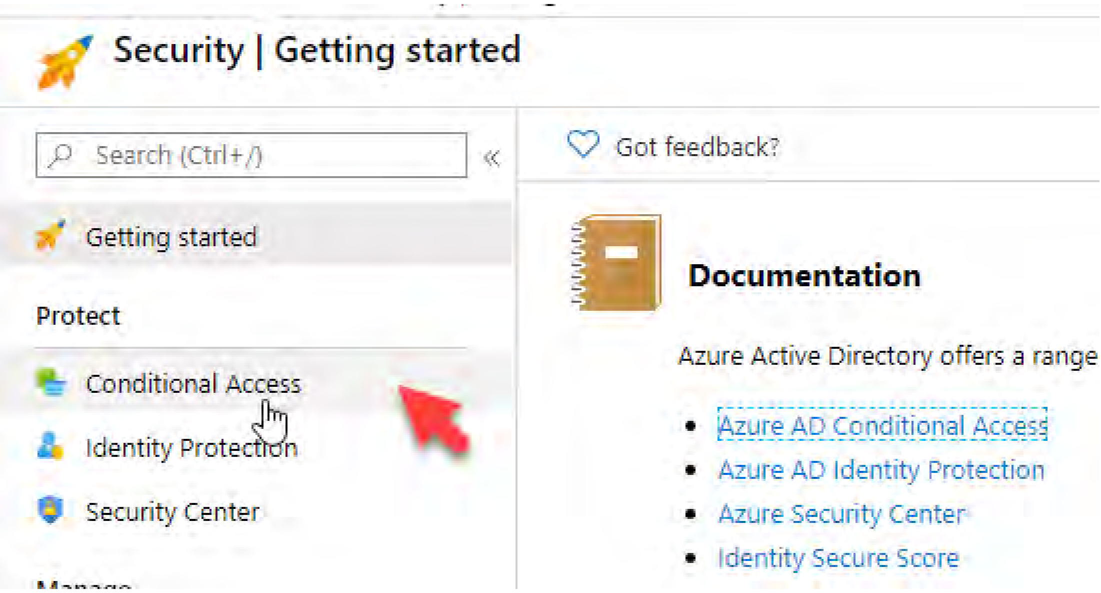
M365B336974.onmicrosoft.com

Tenant ID 44761c47-2457-4b1c

Status Not enabled

Last sync Sync has never run

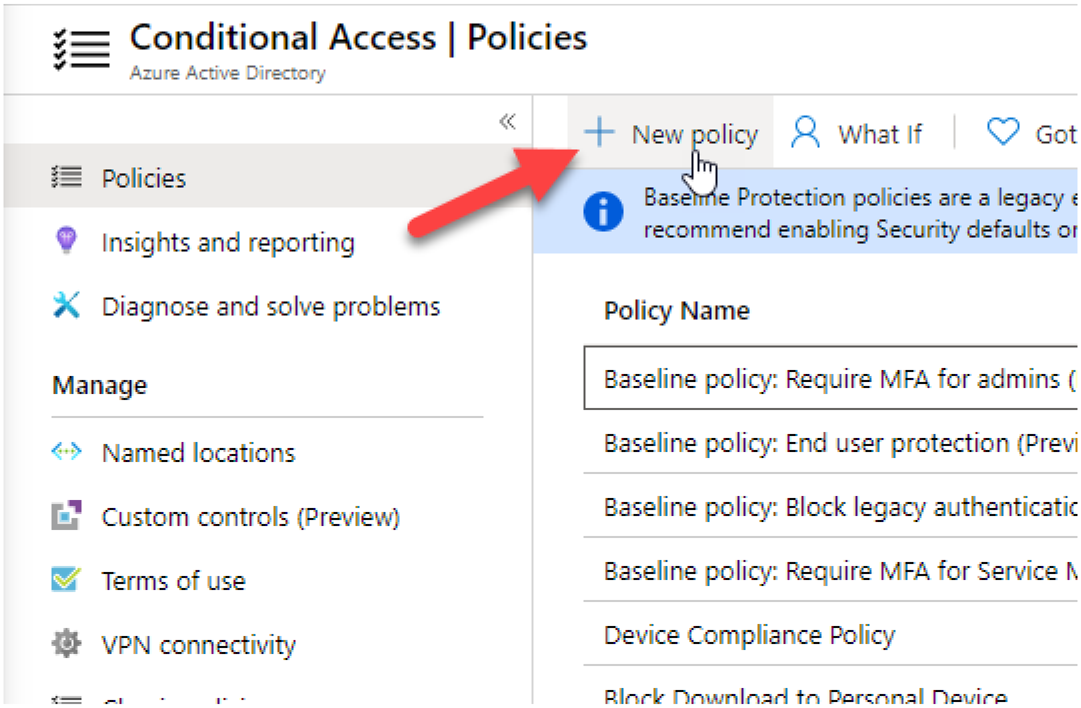
4. Click Conditional Access



Azure Active Directory offers a range

- Azure AD Conditional Access
- Azure AD Identity Protection
- Azure Security Center
- Identity Secure Score

5. Click New Policy



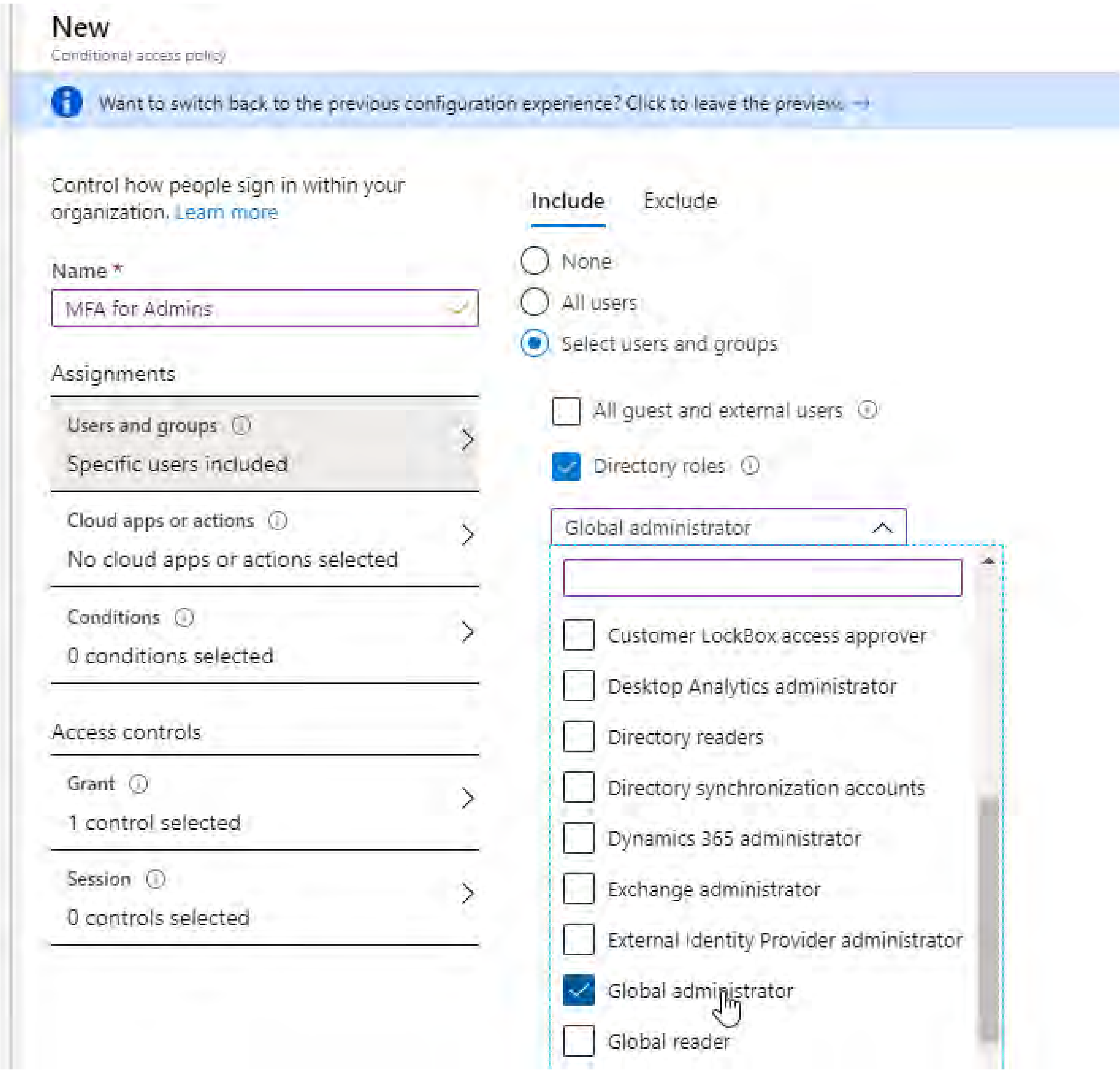
Conditional Access | Policies

Azure Active Directory

Baseline Protection policies are a legacy e
recommend enabling Security defaults or

Policy Name
Baseline policy: Require MFA for admins (
Baseline policy: End user protection (Previ
Baseline policy: Block legacy authenticatic
Baseline policy: Require MFA for Service N
Device Compliance Policy
Block Download to Personal Device

6. Give your policy a name and under the users and groups blade select Directory Roles. From the drop down, select Global Administrator at a minimum. If you have assigned other privileged roles like User Administrator or Security Administrator, we recommend adding them here too.



New
Conditional access policy

Want to switch back to the previous configuration experience? Click to leave the preview. →

Control how people sign in within your organization. Learn more

Name *
MFA for Admins

Assignments

Users and groups
Specific users included

Cloud apps or actions
No cloud apps or actions selected

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Include | Exclude

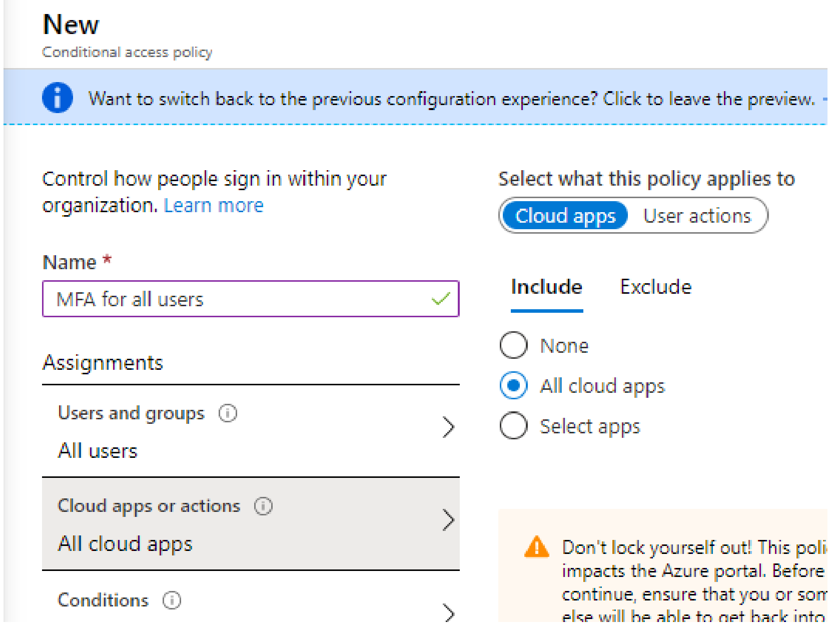
○ None
○ All users
● Select users and groups

□ All guest and external users
☑ Directory roles

Global administrator

□ Customer LockBox access approver
□ Desktop Analytics administrator
□ Directory readers
□ Directory synchronization accounts
□ Dynamics 365 administrator
□ Exchange administrator
□ External Identity Provider administrator
☑ Global administrator
□ Global reader

7. Select All Cloud Apps



New
Conditional access policy

Want to switch back to the previous configuration experience? Click to leave the preview.

Control how people sign in within your organization. Learn more

Name *
MFA for all users

Assignments

Users and groups
All users

Cloud apps or actions
All cloud apps

Conditions

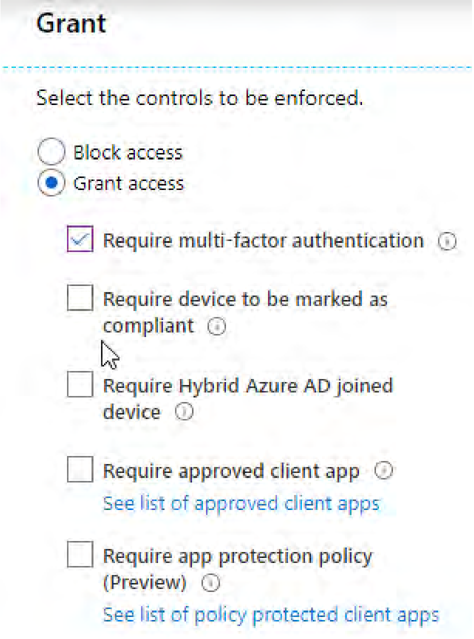
Select what this policy applies to
Cloud apps | User actions

Include | Exclude

○ None
● All cloud apps
○ Select apps

Don't lock yourself out! This poli
impacts the Azure portal. Before
continue, ensure that you or som
else will be able to get back into

8. Skip the conditions section and in the Grant section, select Require Multi-factor Authentication



Grant

Select the controls to be enforced.

○ Block access
● Grant access

☑ Require multi-factor authentication

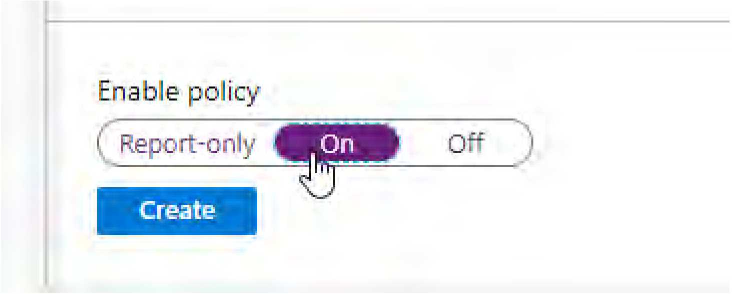
□ Require device to be marked as compliant

□ Require Hybrid Azure AD joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy (Preview)
See list of policy protected client apps

9. Enable the policy and click Create



Enable policy

Report-only | On | Off

PowerShell

We added some scripts here for multi-tenant commands via your partner center credentials. With these scripts you can identify Global admins across all customer tenants and chose to enable MFA

1. Retrieve a list of all Microsoft 365/Office 365 customers' global admins without multi-factor authentication

   PowerShell Script

2. Enable multi-factor authentication on admins in customer's M365/O365 tenant. Here we will take the export data we performed in step 7 and add the users for a particular tenant into a CSV file. Once complete, these admins will be prompted to establish MFA at their next sign in.

   PowerShell Script

3. Block Admin access till MFA requirements are met

   PowerShell Script

Block Legacy Authentication

End of support for legacy authentication like IMAP/POP is coming in October of 2020. Legacy authentication is more susceptible to password spray attacks or brute force attacks because you cannot layer on MFA. It is advised to block all legacy authentication methods within your customer's environments. Legacy authentication can be blocked by enabling Security Defaults or creating a conditional access policy. **Note that if you have any printers/copiers/scanners or IMAP accounts used for ticketing, you should update those protocols before blocking legacy auth.**

Licensing Considerations:

Enabling MFA and Security Defaults:

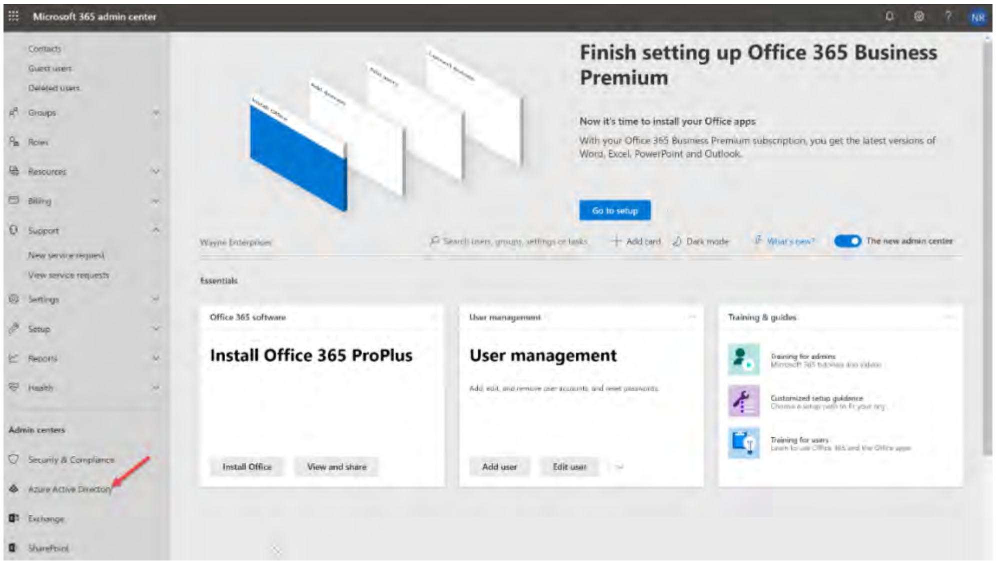
- All Microsoft licensing plans

Enabling Conditional Access Policies

- Microsoft 365 Business Premium ($20/u/m)
- EMS + E3 ($87.5) or EMS + E5 ($14.80)
- Microsoft 365 E3 ($32) or Microsoft 365 E5 ($64)

Security Defaults:

1. In the 365 Admin Portal, click on the Azure Active Directory link under Admin Centers



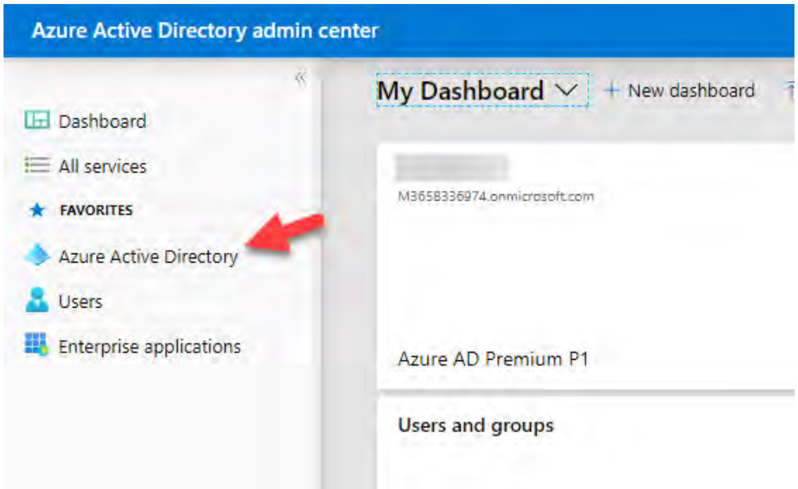
Finish setting up Office 365 Business Premium

Now it's time to install your Office apps

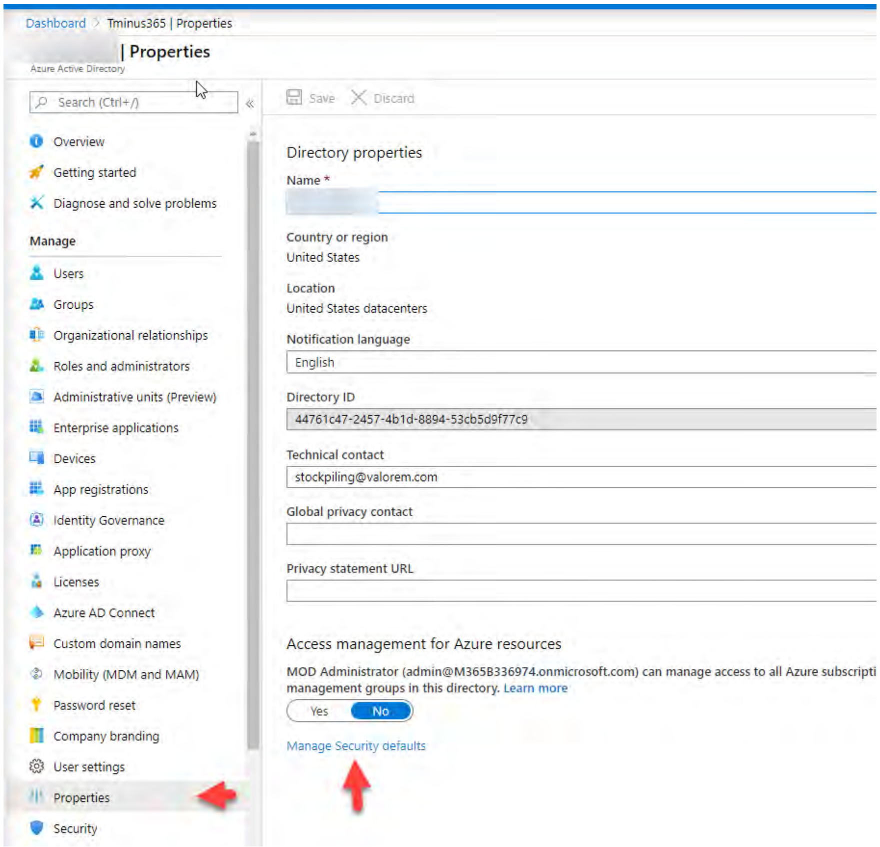
With your Office 365 Business Premium subscription, you get the latest versions of Word, Excel, PowerPoint and Outlook.

Add, edit, and remove user accounts, and reset passwords.

2. Click Azure Active Directory



3. Click Manage>Manage Security Defaults



[redacted] | Properties

Directory properties

Name * [redacted]

Country or region
United States

Location
United States datacenters

Notification language
English

Directory ID
44761c47-2457-4b1d-8894-53cb5d9f77c9

Technical contact
stockpiling@valorem.com

Global privacy contact

Privacy statement URL

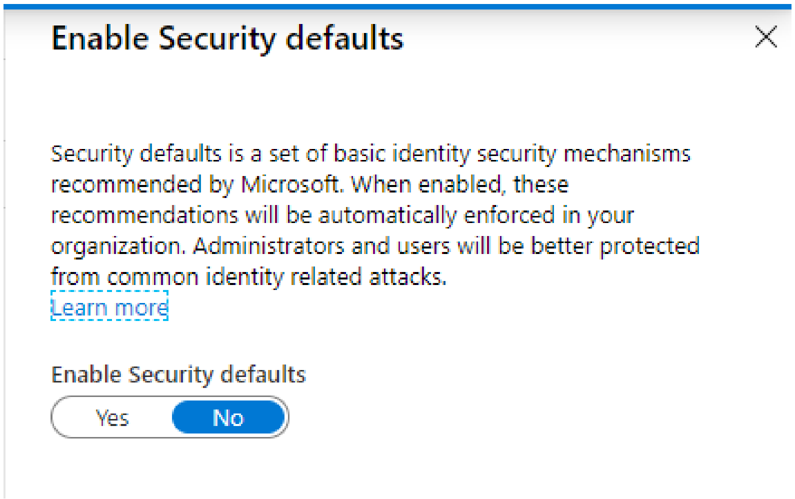
Access management for Azure resources

MOD Administrator (admin@M365B336974.onmicrosoft.com) can manage access to all Azure subscripti management groups in this directory. Learn more

Yes [✓ No]

Manage Security defaults

4. Toggle on Security Defaults



Enable Security defaults

Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.
Learn more

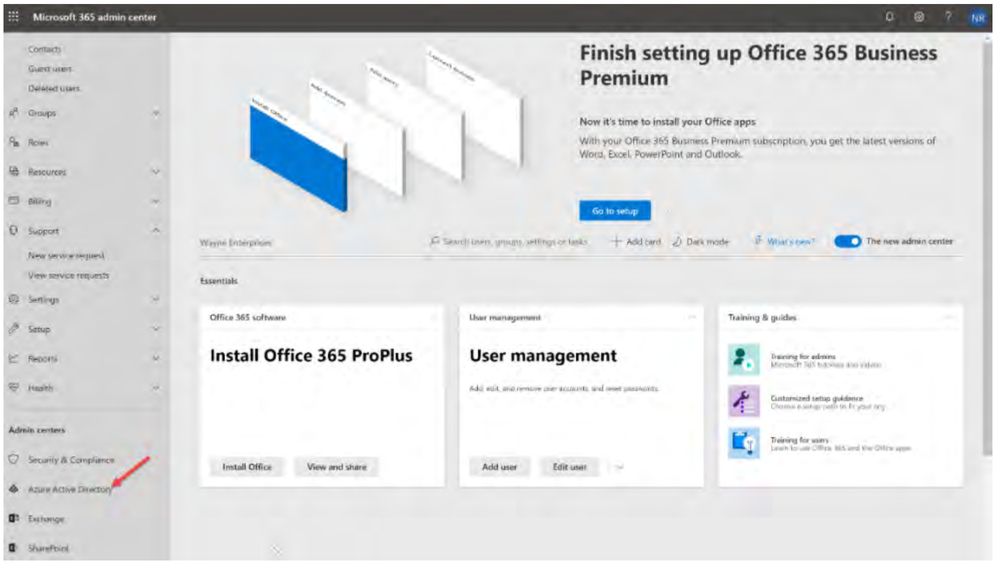
Enable Security defaults

Yes [✓ No]

NOTE Turning on security defaults enforces MFA for all users. They will have 14 days to register after their first sign-in after you turn this on and they will only be able to use the Microsoft Authenticator app as their second form of authentication. Be sure to plan and communicate accordingly.

Conditional Access

1. In the 365 Admin Portal, click on the Azure Active Directory link under Admin Centers



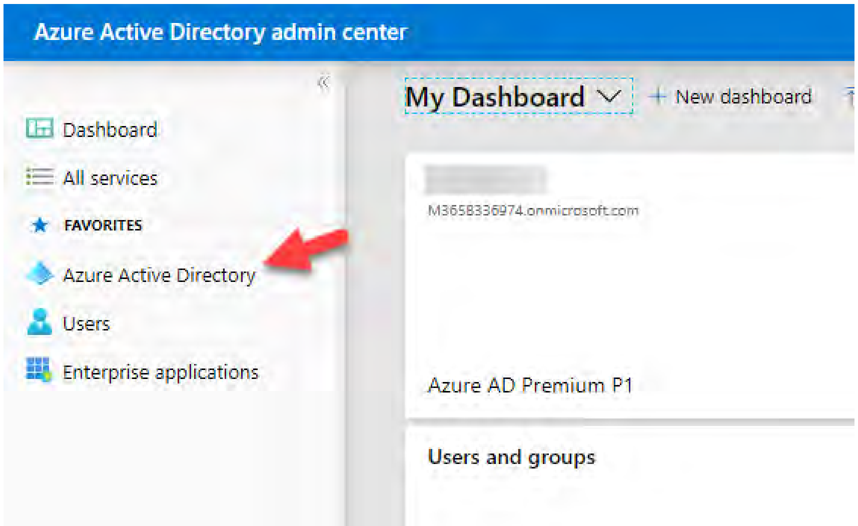
Finish setting up Office 365 Business Premium

Now it's time to install your Office apps

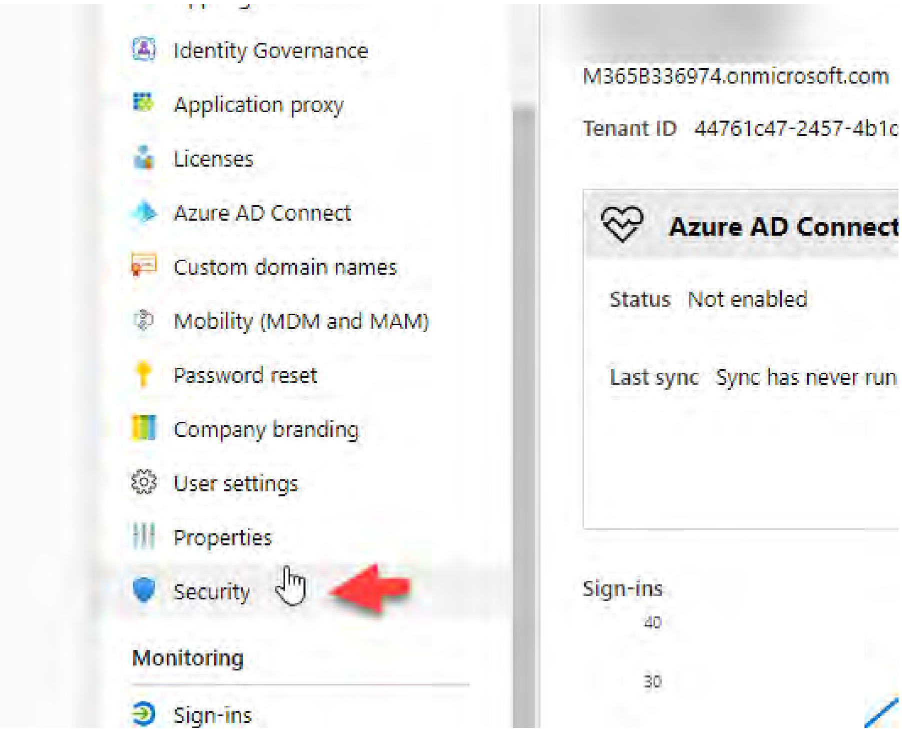
With your Office 365 Business Premium subscription, you get the latest versions of Word, Excel, PowerPoint and Outlook.

Add, edit, and remove user accounts, and reset passwords.

2. Click Azure Active Directory



3. Scroll down and click Security



M365B336974.onmicrosoft.com

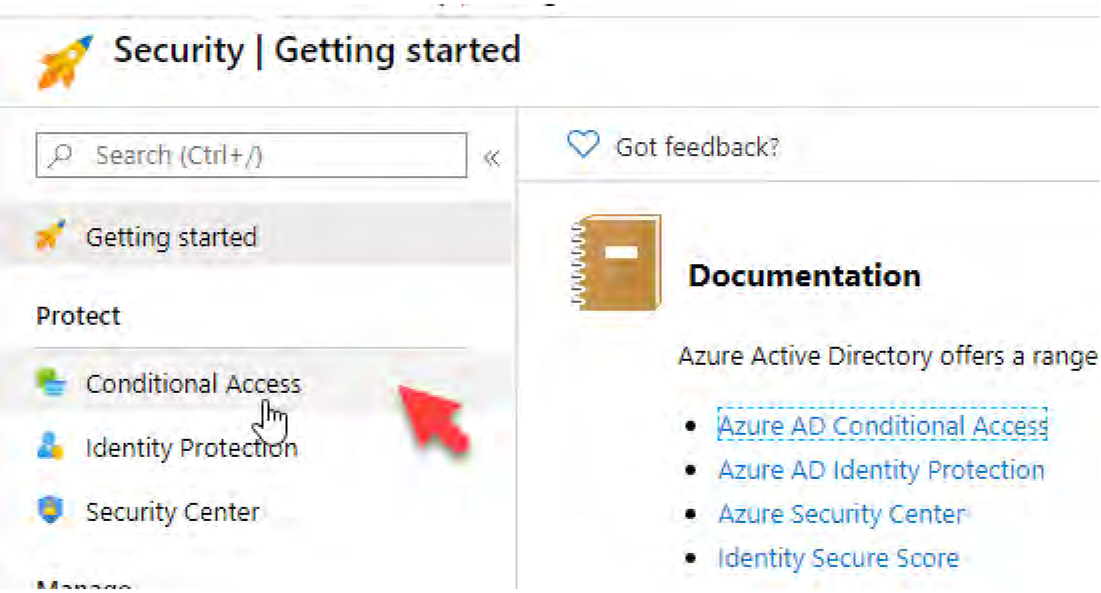
Tenant ID 44761c47-2457-4b1c

Azure AD Connect

Status Not enabled

Last sync Sync has never run

4. Click Conditional Access



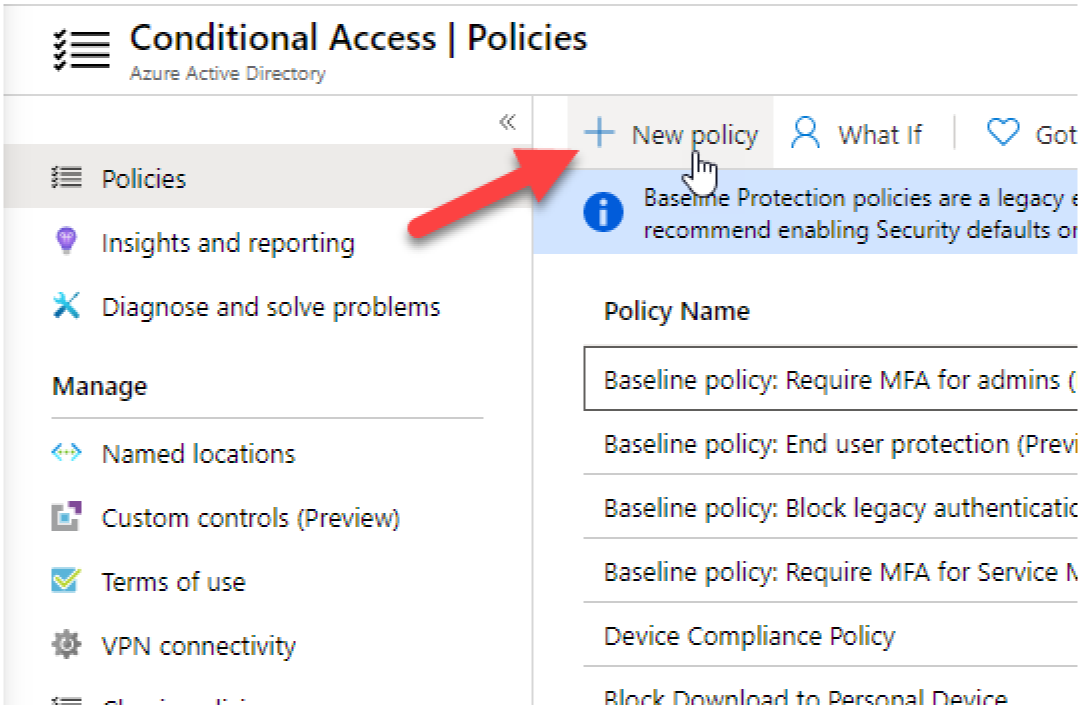
Security | Getting started

Documentation

Azure Active Directory offers a range

- Azure AD Conditional Access
- Azure AD Identity Protection
- Azure Security Center
- Identity Secure Score

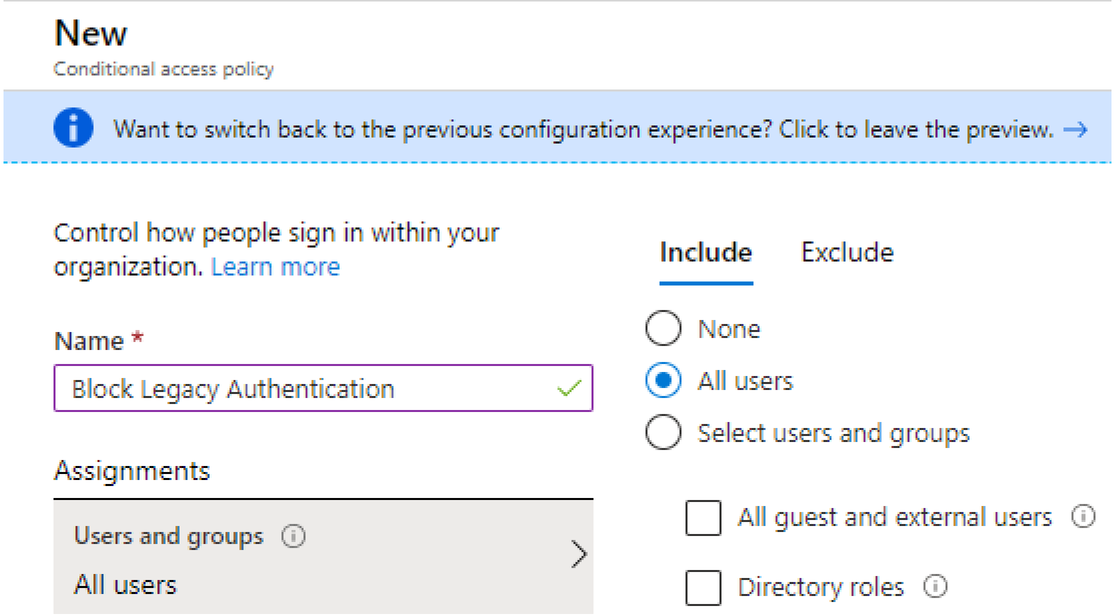
5. Click New Policy



Baseline Protection policies are a legacy e
recommend enabling Security defaults or

Policy Name
Baseline policy: Require MFA for admins (
Baseline policy: End user protection (Previ
Baseline policy: Block legacy authenticatic
Baseline policy: Require MFA for Service N
Device Compliance Policy
Block Download to Personal Device

6. Name your policy and scope to all users



Want to switch back to the previous configuration experience? Click to leave the preview. →

Control how people sign in within your organization. Learn more

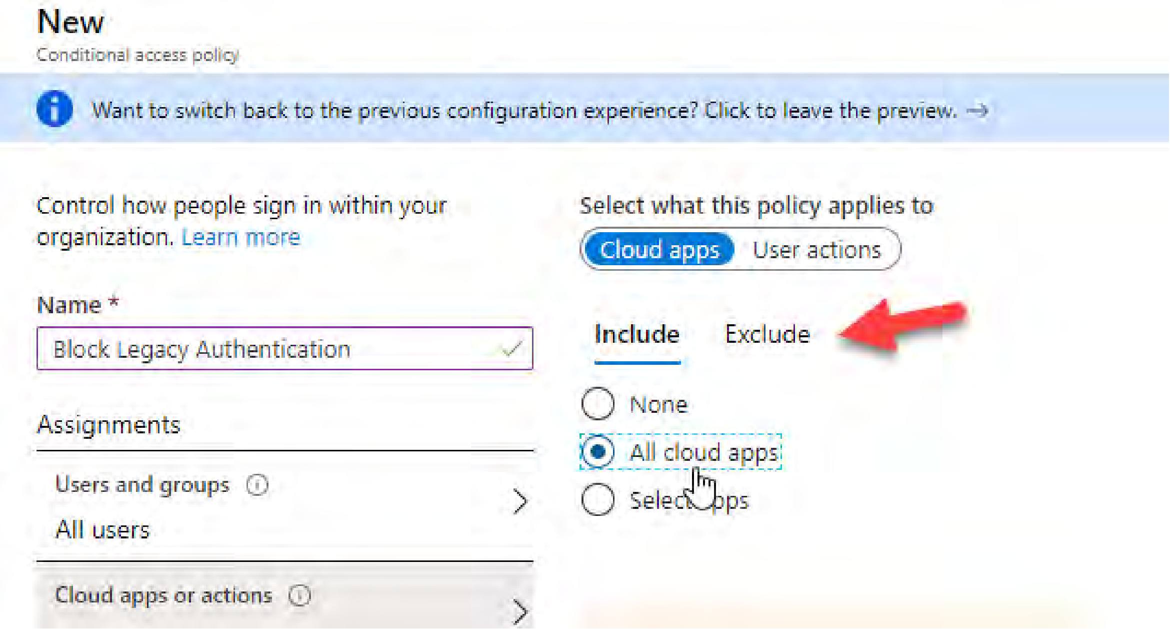
Name *
Block Legacy Authentication ✓

Users and groups ⓘ
All users

○ None
● All users
○ Select users and groups

□ All guest and external users ⓘ
□ Directory roles ⓘ

7. In the Cloud apps or actions blade, click All cloud apps. *NOTE* If you do have applications that use legacy auth, you could exclude them here to give yourself more time to update the protocol.



New

Conditional access policy

Want to switch back to the previous configuration experience? Click to leave the preview. →

Control how people sign in within your organization. Learn more

Name *

Block Legacy Authentication

Assignments

Users and groups

All users

Cloud apps or actions

Select what this policy applies to

Cloud apps | User actions

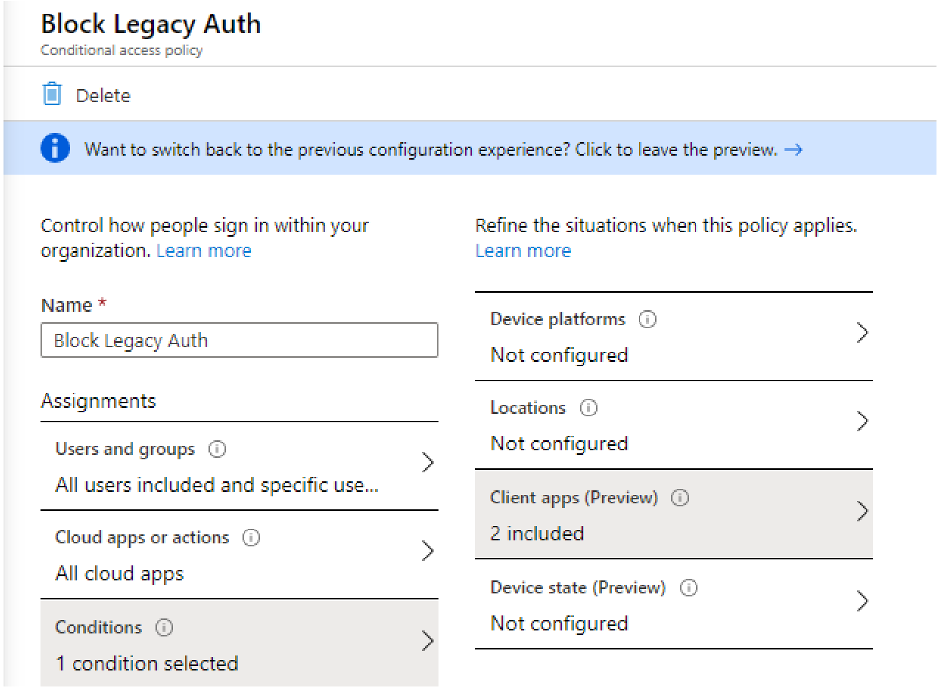
Include | Exclude

○ None

● All cloud apps

○ Select apps

8. In the conditions section, click Client Apps>Mobile Apps and Desktop Clients>Other Clients



Block Legacy Auth
Conditional access policy

Delete

Want to switch back to the previous configuration experience? Click to leave the preview. →

Control how people sign in within your organization. Learn more

Name *
Block Legacy Auth

Assignments

Users and groups ⓘ
All users included and specific use...

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
1 condition selected

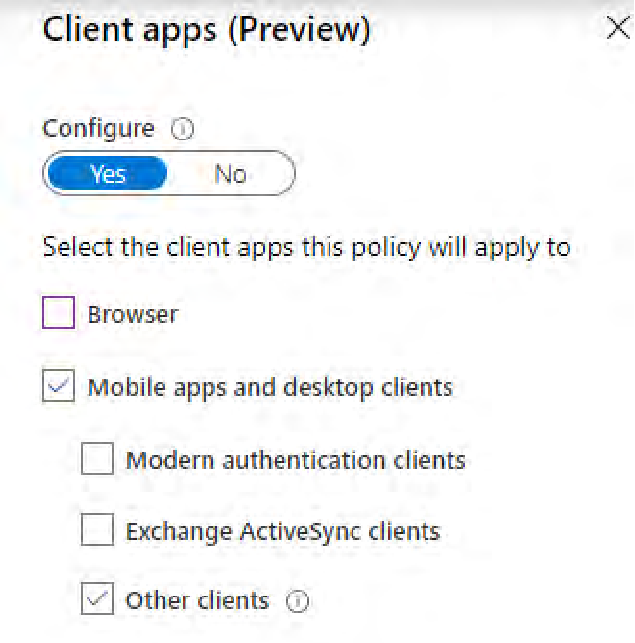
Refine the situations when this policy applies. Learn more

Device platforms ⓘ
Not configured

Locations ⓘ
Not configured

Client apps (Preview) ⓘ
2 included

Device state (Preview) ⓘ
Not configured



Client apps (Preview)

Configure ⓘ
● Yes ○ No

Select the client apps this policy will apply to

□ Browser

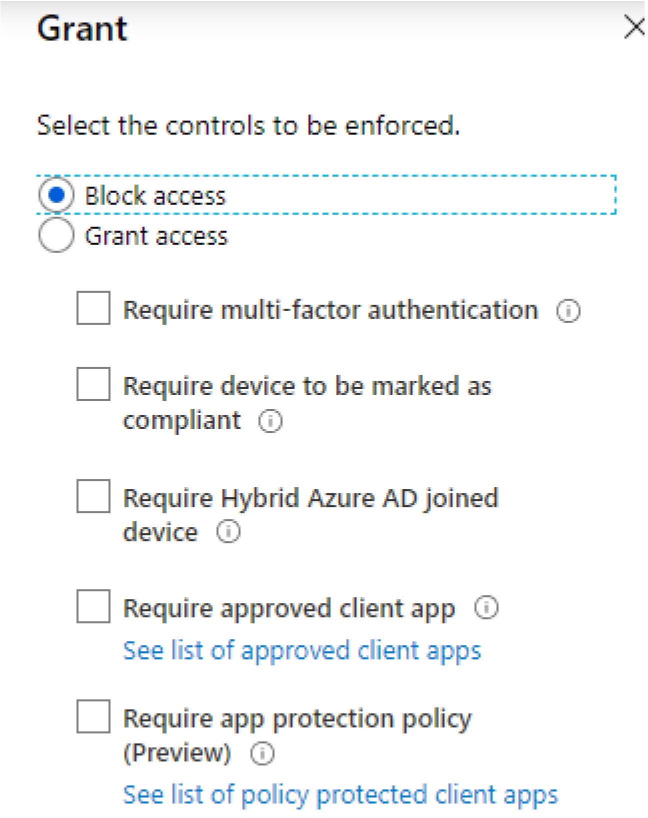
☑ Mobile apps and desktop clients

□ Modern authentication clients

□ Exchange ActiveSync clients

☑ Other clients ⓘ

9. In the Grant blade, leave the setting at Block Access



Grant

Select the controls to be enforced.

● Block access

○ Grant access

□ Require multi-factor authentication

□ Require device to be marked as compliant

□ Require Hybrid Azure AD joined device

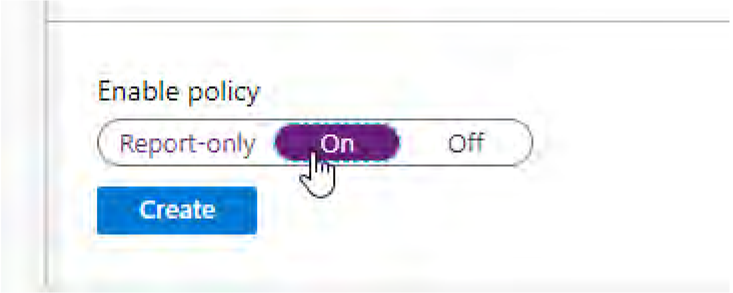
□ Require approved client app

See list of approved client apps

□ Require app protection policy (Preview)

See list of policy protected client apps

10. Enable the policy and click Create



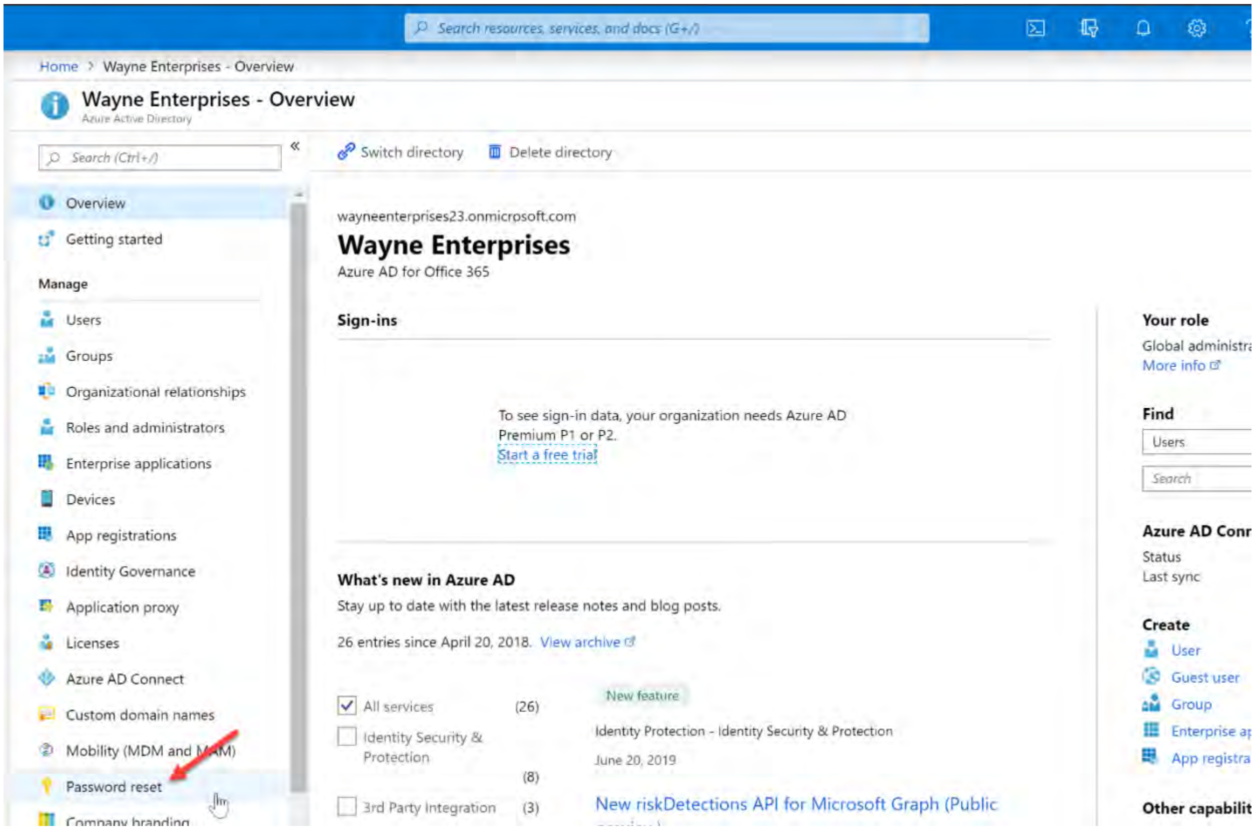
Enable policy

Report-only [✓ On] Off

Enable Self-Service Password Reset

With self-service password reset in Azure AD, users no longer need to engage helpdesk to reset passwords. This feature works well with Azure AD dynamically banned passwords, which prevents easily guessable passwords from being used.

1. Go to the Azure Active Directory Admin Portal and click on the Password Reset tab:



wayneenterprises23.onmicrosoft.com

Wayne Enterprises

Azure AD for Office 365

Sign-ins

To see sign-in data, your organization needs Azure AD Premium P1 or P2.
Start a free trial

What's new in Azure AD

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

26 entries since April 20, 2018. View archive

☑ All services (26)
□ Identity Security & Protection (8)
□ 3rd Party Integration (3)

New feature

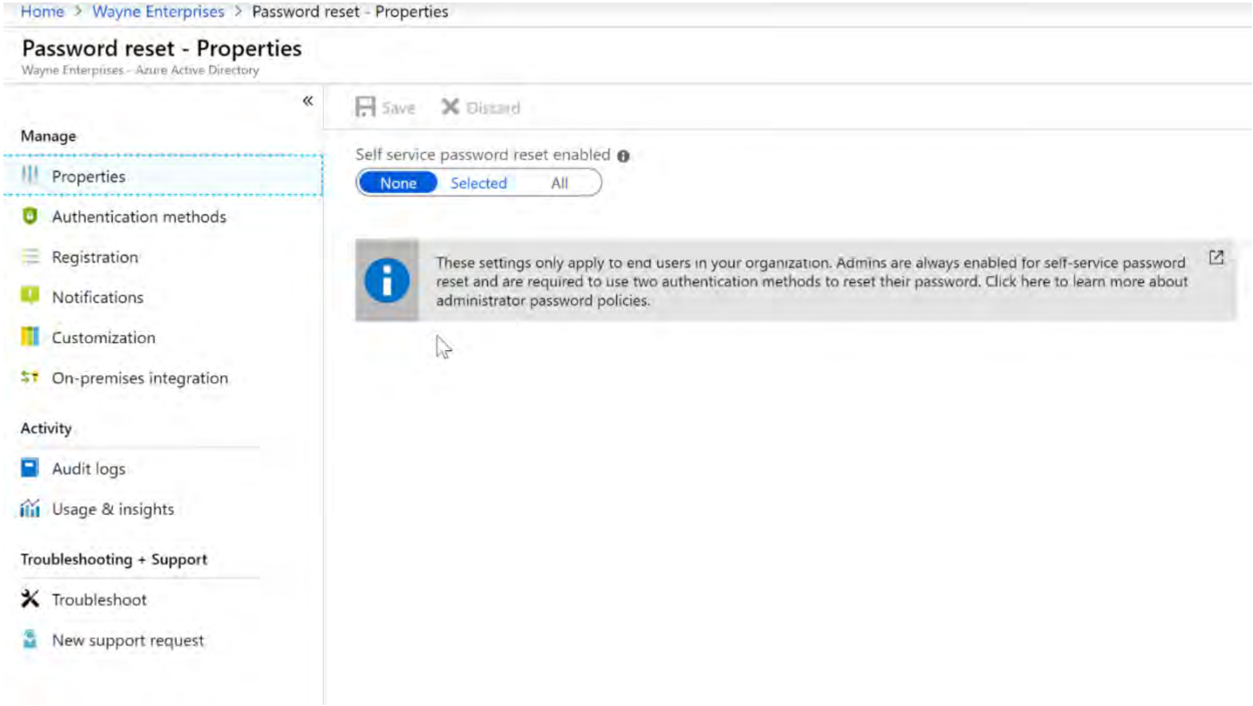
Identity Protection - Identity Security & Protection

June 20, 2019

New riskDetections API for Microsoft Graph (Public

Global administra

2. The default tab allows you to enable for all users or select groups of users if you do not want to turn it on for everyone


Home > Wayne Enterprises > Password reset - Properties

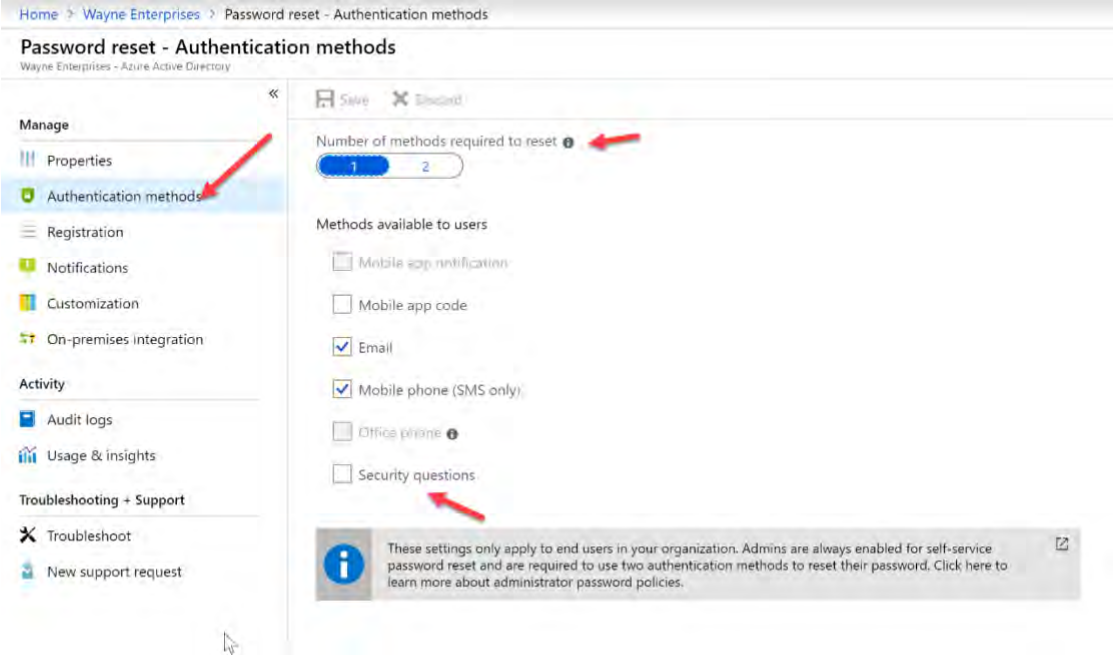
Password reset - Properties

Wayne Enterprises - Azure Active Directory

Self service password reset enabled: None | Selected | All (None chosen)

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

3. In the Authentication Methods tab, you can define what settings they can put in place. These may be the same you have selected for MFA. One that you could add that isn't available with MFA is security questions



Password reset - Authentication methods

Wayne Enterprises - Azure Active Directory

Number of methods required to reset: ● 1 ○ 2

Methods available to users

□ Mobile app notification

□ Mobile app code

☑ Email

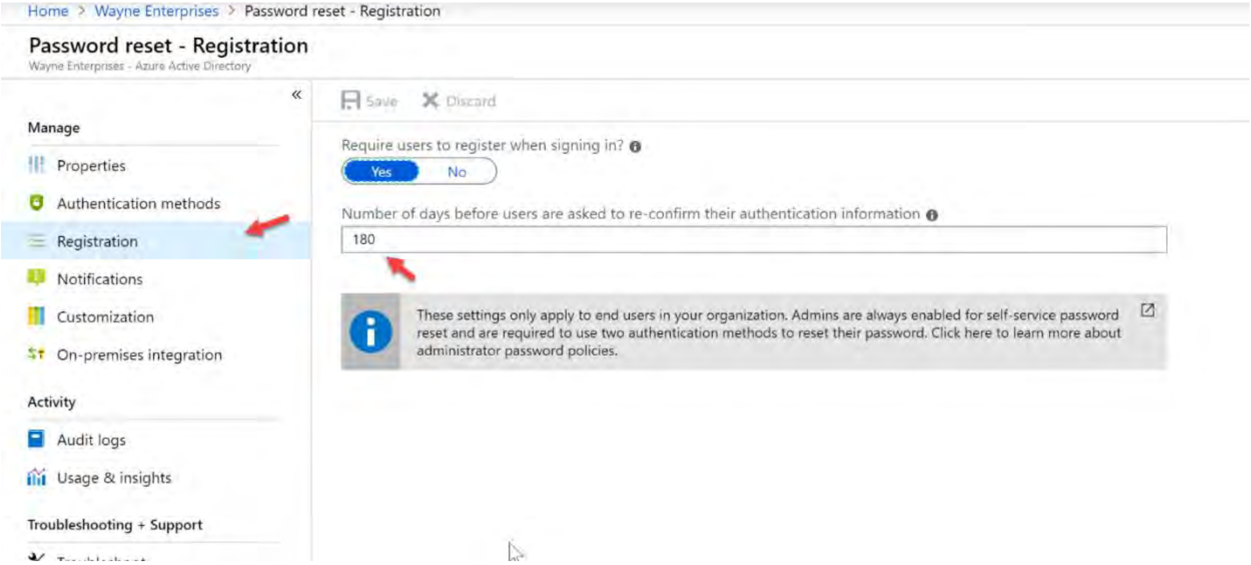
☑ Mobile phone (SMS only)

□ Office phone

□ Security questions

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

4. You can define the number of days before users are asked to confirm their recovery options and also get alerts if you want to know when someone has reset their password



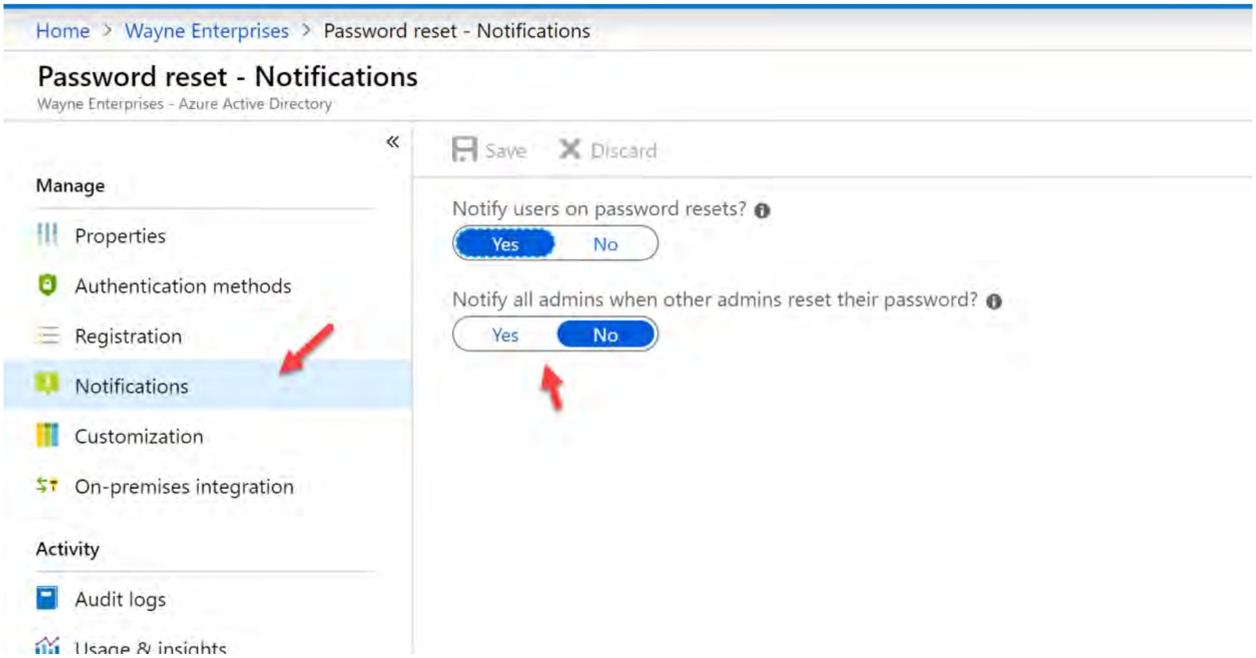
Password reset - Registration

Wayne Enterprises - Azure Active Directory

Require users to register when signing in? ● Yes ○ No

Number of days before users are asked to re-confirm their authentication information: 180

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.



Notify users on password resets? [✓ Yes] No

Notify all admins when other admins reset their password? Yes [✓ No]

PowerShell

1. Enable SSPR for a Single Tenant

   [PowerShell Script]

2. Enable SSPR All Tenants with Partner Center Credentials

   [PowerShell Script]

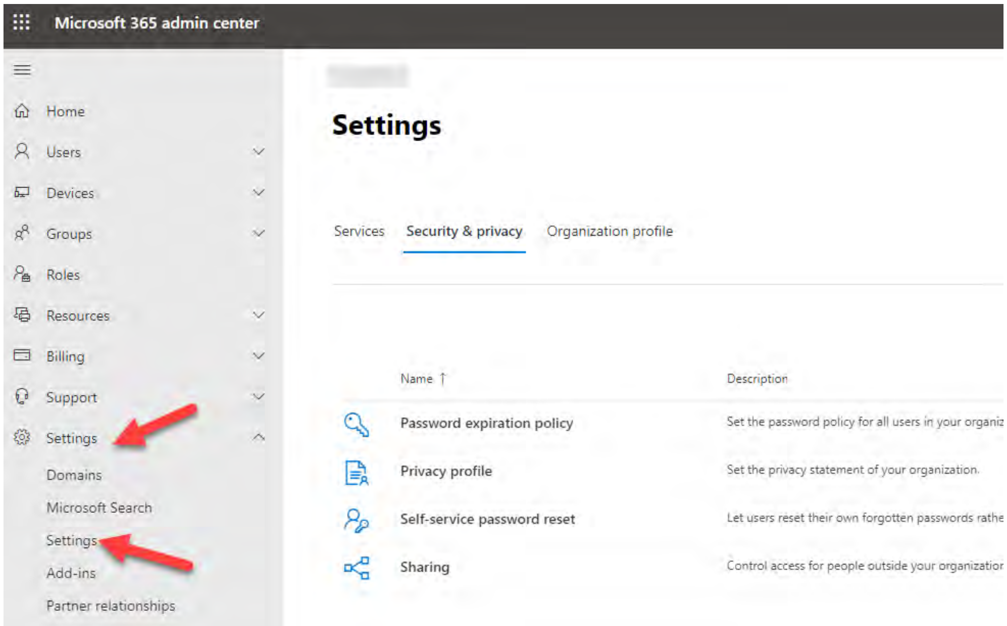
Do Not Expire Passwords

Research has found that when periodic password resets are enforced, passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset. If a user creates a strong password (long, complex and without any pragmatic words present) it should remain just as strong in 60 days as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason. Make sure you have MFA enabled before making this setting change.

Compliance Controls

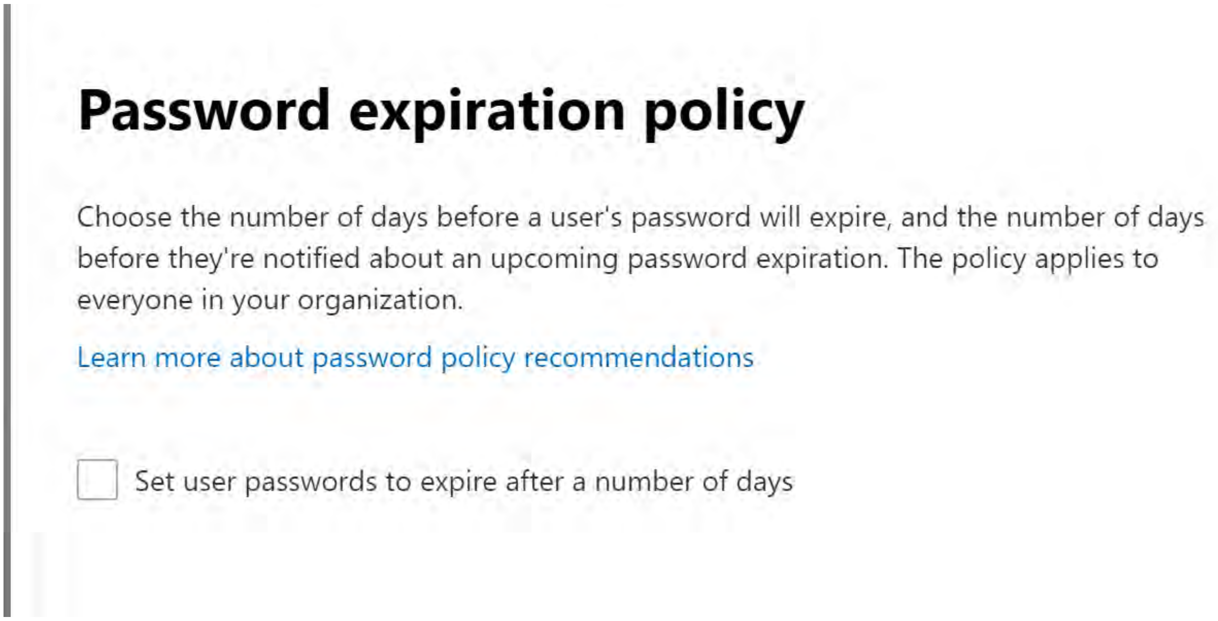
- FedRAMP Moderate; Control AC-7(a)
- NIST 800-171; Control 3.1.8
- NIST 800-53; Control AC-7(a)

1. In the 365 Admin Center, expand Settings and select Security & Privacy. From here you can click edit to make changes to the password policy



Name ↑	Description
Password expiration policy	Set the password policy for all users in your organiz
Privacy profile	Set the privacy statement of your organization.
Self-service password reset	Let users reset their own forgotten passwords rathe
Sharing	Control access for people outside your organizatior

2. Ensure the checkbox is unchecked



Password expiration policy

Choose the number of days before a user's password will expire, and the number of days before they're notified about an upcoming password expiration. The policy applies to everyone in your organization.

Learn more about password policy recommendations

□ Set user passwords to expire after a number of days

PowerShell

Change Password Policy for single tenant or all of your customer tenants

[Click here](#)

Delete/block accounts not used in last 30 days

Deleting or blocking accounts that haven't been used in the last 30 days, after checking with owners, helps prevent unauthorized use of inactive accounts. These accounts can be targets for attackers who are looking to find ways to access your data without being noticed. In GitHub, you can download a PowerShell script called "InactiveUsersLast90Days.ps1" to look up the users who have not logged in for the last 90 days.

Compliance Controls

- FedRAMP Moderate; Control AC-2(3)
- NIST 800-53; Control AC-2(3)

1. PowerShell Script

Designate More than 1 Global Admin but fewer than 5

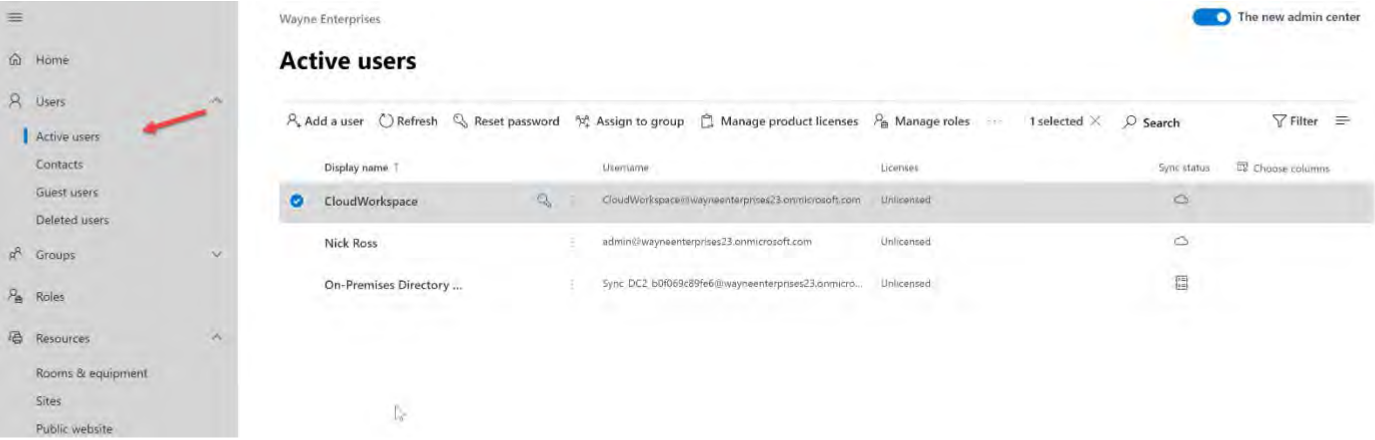
You should designate more than one global tenant administrator because that one admin can perform malicious activity without the possibility of being discovered by another admin. You could also set this second admin up with a mailbox in which all of the reports discussed in this playbook are filtered into.

Reducing the number of global admins limits the number of accounts with high privileges that need to be closely monitored. If any of those accounts are compromised, critical devices and data are open to attacks. Designating fewer than 5 global admins reduces the attack surface area.

Compliance Controls

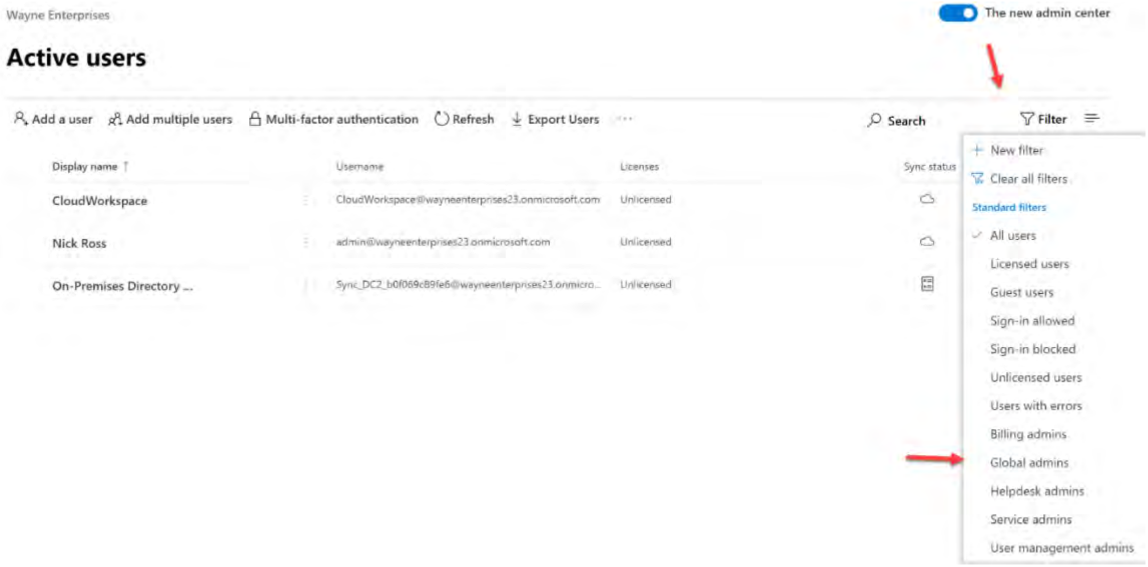
- CSA CCM301; Control DSI-02
- FedRAMP Moderate; Control IA-3
- GDPR; Control 6.6.5
- ISO 27018:2014; Control C.9.4.2, Control A.10.8
- NIST 800-171; Control 3.5.2
- NIST 800-53; Control IA-3

1. Log In to the 365 Admin Center>Go to Users>Active Users

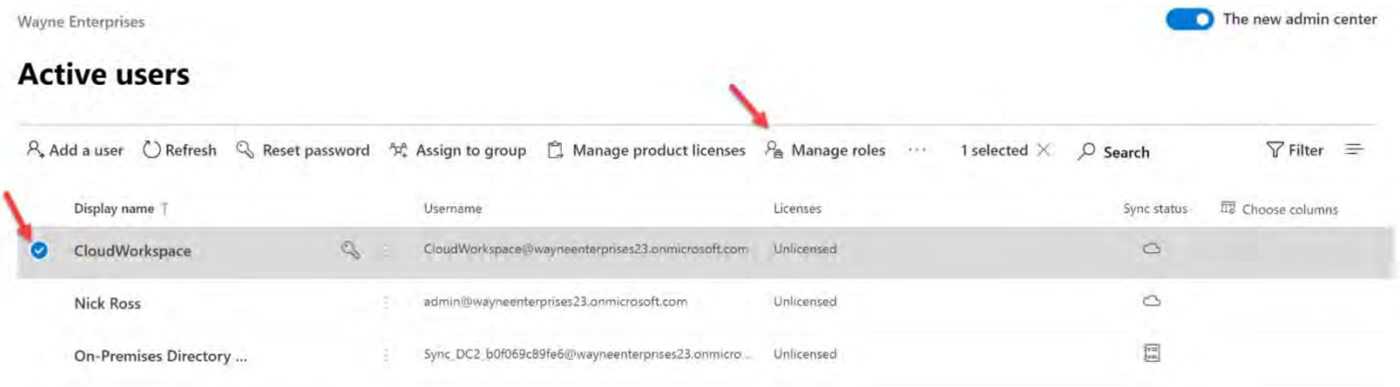


Display name ↑	Username	Licenses	Sync status
CloudWorkspace	CloudWorkspace@wayneenterprises23.onmicrosoft.com	Unlicensed	
Nick Ross	admin@wayneenterprises23.onmicrosoft.com	Unlicensed	
On-Premises Directory ...	Sync_DC2_b0f069c89fe6@wayneenterprises23.onmicro...	Unlicensed	

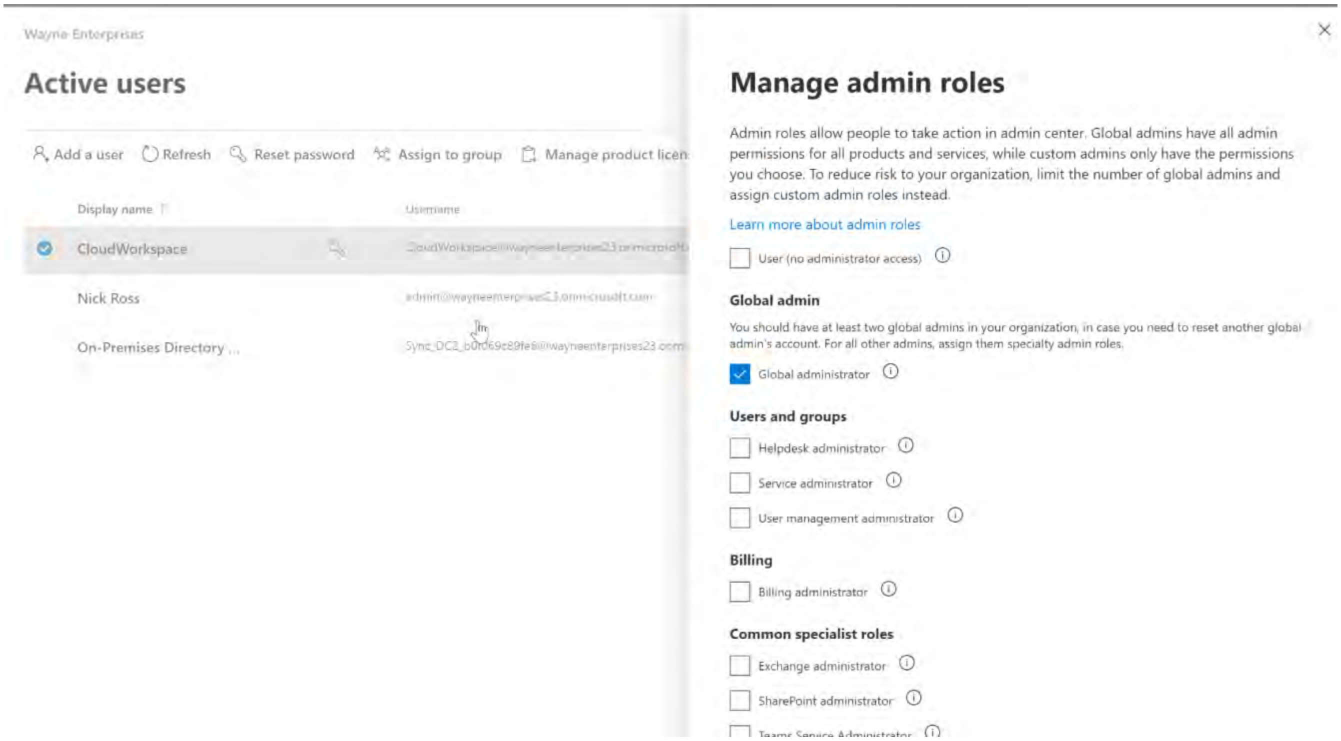
2. On this page, you can filter by Global Admin roles or you can manage user roles by selecting on a user and clicking on Manage Roles



Display name	Username	Licenses	Sync status
CloudWorkspace	CloudWorkspace@wayneenterprises23.onmicrosoft.com	Unlicensed	
Nick Ross	admin@wayneenterprises23.onmicrosoft.com	Unlicensed	
On-Premises Directory ...	Sync_DC2_b0f069c89fe6@wayneenterprises23.onmicro...	Unlicensed	



Display name	Username	Licenses	Sync status
CloudWorkspace	CloudWorkspace@wayneenterprises23.onmicrosoft.com	Unlicensed	
Nick Ross	admin@wayneenterprises23.onmicrosoft.com	Unlicensed	
On-Premises Directory ...	Sync_DC2_b0f069c89fe6@wayneenterprises23.onmicro...	Unlicensed	



Active users

Display name ↑	Username
✓ CloudWorkspace	CloudWorkspace@wayneenterprises23.onmicrosoft...
Nick Ross	admin@wayneenterprises23.onmicrosoft.com
On-Premises Directory ...	Sync_DC2_b0d69c89fe6@wayneenterprises23.com

Manage admin roles

Admin roles allow people to take action in admin center. Global admins have all admin permissions for all products and services, while custom admins only have the permissions you choose. To reduce risk to your organization, limit the number of global admins and assign custom admin roles instead.

Learn more about admin roles

□ User (no administrator access) ⓘ

Global admin

You should have at least two global admins in your organization, in case you need to reset another global admin's account. For all other admins, assign them specialty admin roles.

☑ Global administrator ⓘ

Users and groups

□ Helpdesk administrator ⓘ

□ Service administrator ⓘ

□ User management administrator ⓘ

Billing

□ Billing administrator ⓘ

Common specialist roles

□ Exchange administrator ⓘ

□ SharePoint administrator ⓘ

□ Teams Service Administrator ⓘ

PowerShell:

1. View all Global Admins in one customer tenant

   PowerShell Script

2. View all Global Admins across all tenants with Partner Center credentials

   PowerShell Script

OVERVIEW & USER GUIDE

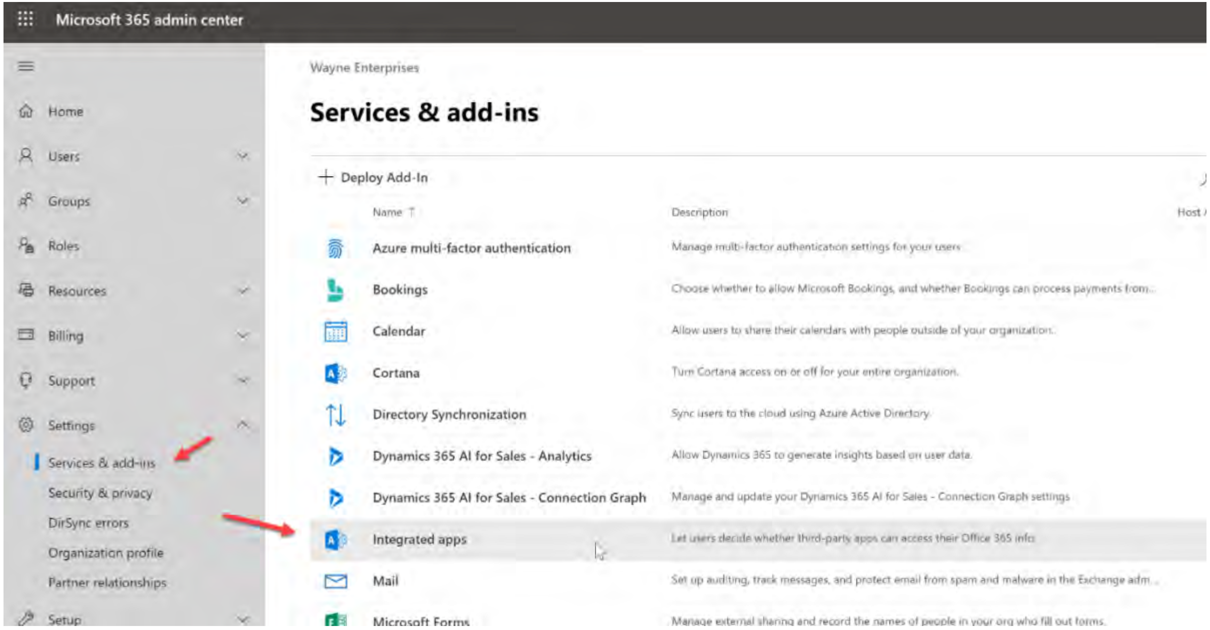
Do not allow users to grant consent to unmanaged applications

Tighten the security of your services by regulating the access of third-party integrated apps. Only allow access to necessary apps that support robust security controls. Third-party applications are not created by Microsoft, so there is a possibility they could be used for malicious purposes like exfiltrating data from your tenancy. Attackers can maintain persistent access to your services through these integrated apps, without relying on compromised accounts.

Compliance Controls

- FedRAMP Moderate; Control CM-8(3)(a)
- NIST 800-53; Control CM-8(3)(a)
- NIST CSF; Control ID.AM-1

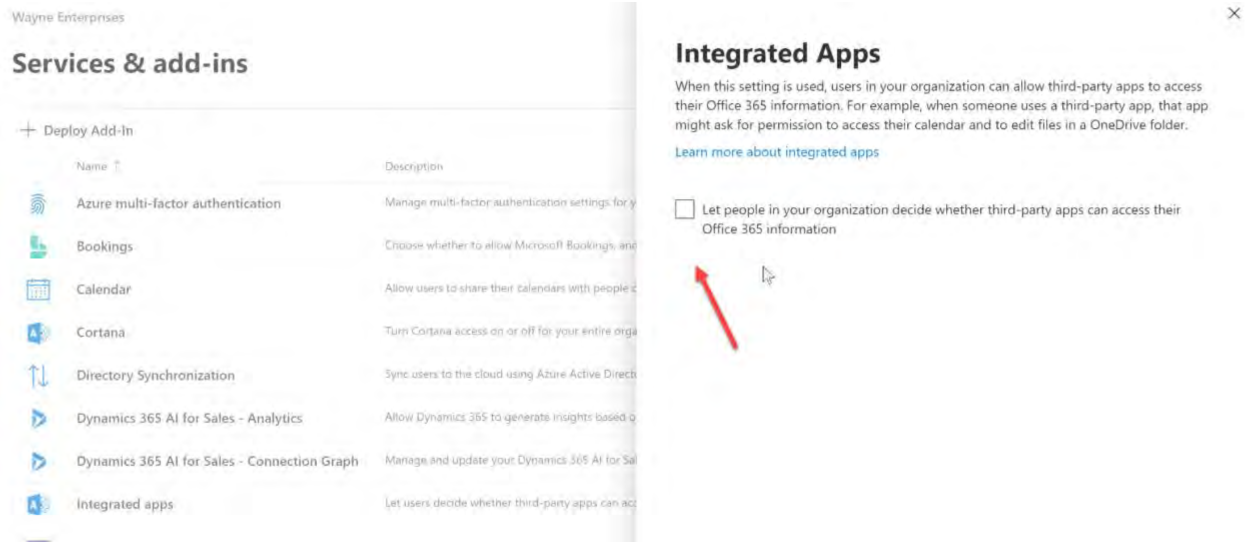
1. In the 365 Admin Portal, go to Settings>Services and Add-Ins>Integrated Apps



Services & add-ins

Name	Description	Host
Azure multi-factor authentication	Manage multi-factor authentication settings for your users	
Bookings	Choose whether to allow Microsoft Bookings, and whether Bookings can process payments from...	
Calendar	Allow users to share their calendars with people outside of your organization.	
Cortana	Turn Cortana access on or off for your entire organization.	
Directory Synchronization	Sync users to the cloud using Azure Active Directory	
Dynamics 365 AI for Sales - Analytics	Allow Dynamics 365 to generate insights based on user data.	
Dynamics 365 AI for Sales - Connection Graph	Manage and update your Dynamics 365 AI for Sales - Connection Graph settings	
Integrated apps	Let users decide whether third-party apps can access their Office 365 info	
Mail	Set up auditing, track messages, and protect email from spam and malware in the Exchange adm...	
Microsoft Forms	Manage external sharing and record the names of people in your org who fill out forms.	

2. Deselect the checkbox and save



Wayne Enterprises

Services & add-ins

Name ↑	Description
Azure multi-factor authentication	Manage multi-factor authentication settings for y
Bookings	Choose whether to allow Microsoft Bookings, and
Calendar	Allow users to share their calendars with people c
Cortana	Turn Cortana access on or off for your entire orga
Directory Synchronization	Sync users to the cloud using Azure Active Directo
Dynamics 365 AI for Sales - Analytics	Allow Dynamics 365 to generate insights based o
Dynamics 365 AI for Sales - Connection Graph	Manage and update your Dynamics 365 AI for Sal
Integrated apps	Let users decide whether third-party apps can acc

Integrated Apps

When this setting is used, users in your organization can allow third-party apps to access their Office 365 information. For example, when someone uses a third-party app, that app might ask for permission to access their calendar and to edit files in a OneDrive folder.

Learn more about integrated apps

☐ Let people in your organization decide whether third-party apps can access their Office 365 information

PowerShell:

1. Disable with PowerShell for one customer

   PowerShell Script

2. Disable with PowerShell across all customers with Partner Center credentials

   PowerShell Script

EXCHANGE ONLINE

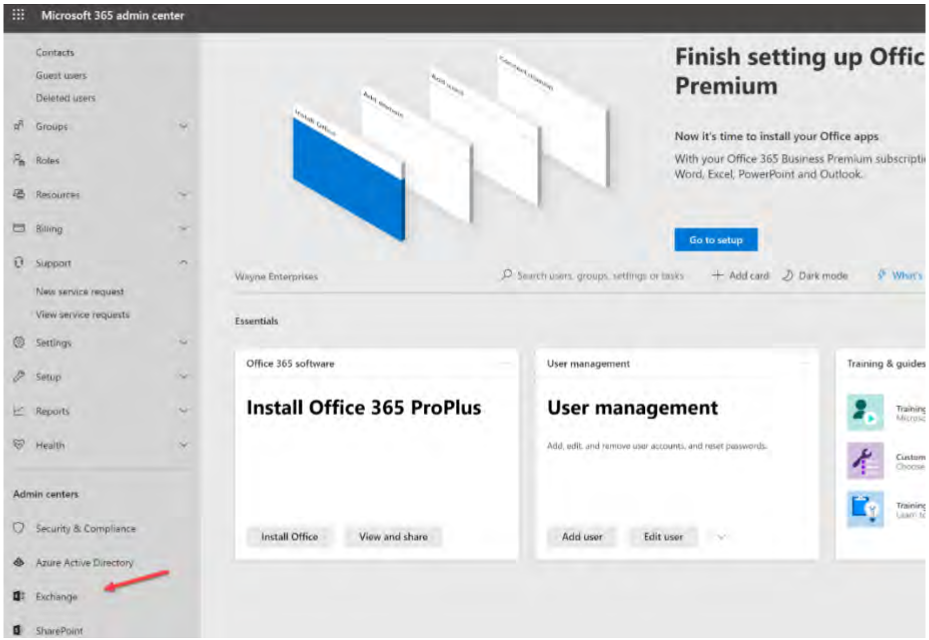
Enable Email Encryption

Email encryption rules can be added to encrypt a message with a particular keyword in the subject line or body. Most common is to add "Secure" as the key word in the subject to encrypt the message. M365/O365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services. Email message encryption helps ensure that only intended recipients can view message content.

Licensing Considerations:

- Microsoft 365 Business Premium ($20/u/m) -included
- Azure Information Protection Plan 1 add-on ($2/u/m)

1. In the 365 Admin Center, click on Exchange under Admin Centers

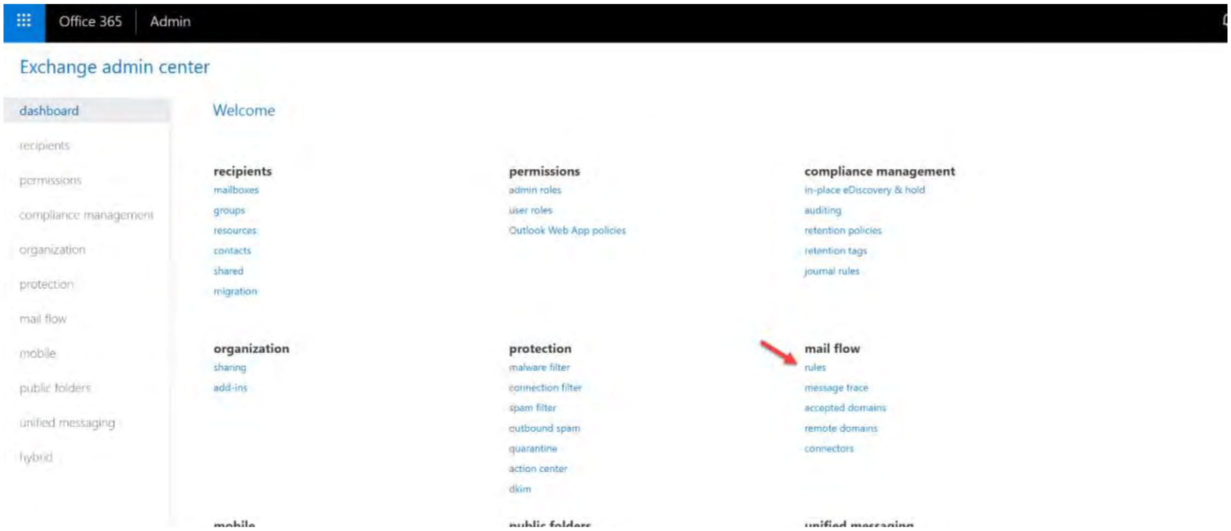


Now it's time to install your Office apps

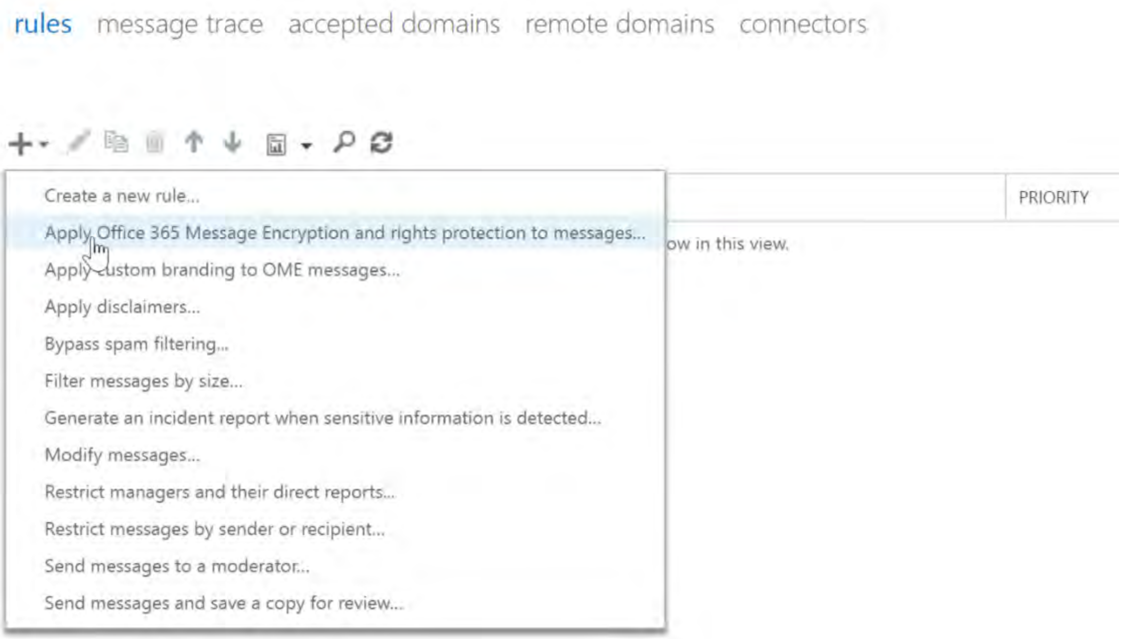
With your Office 365 Business Premium subscripti Word, Excel, PowerPoint and Outlook.

Add, edit, and remove user accounts, and reset passwords.

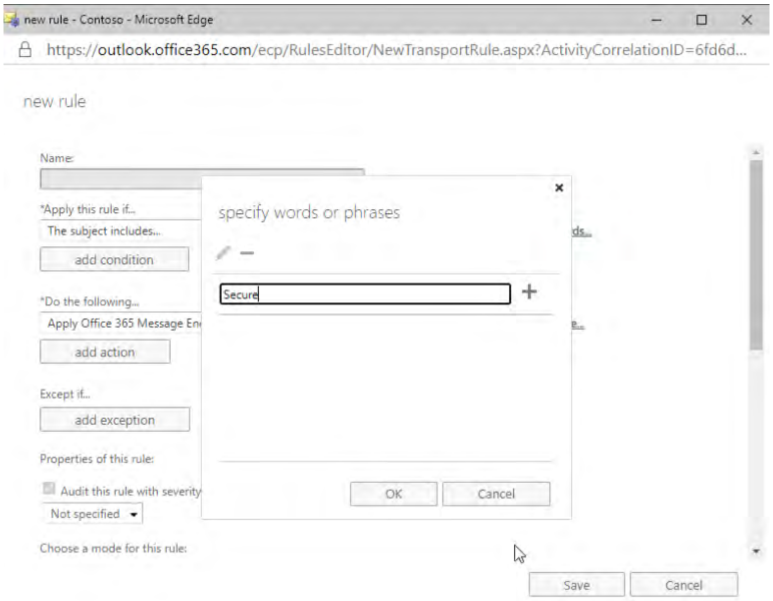
2. In the Mail Flow section, click on Rules



3. Click on the plus sign and click Apply Office 365 Message Encryption (allows you to define multiple conditions)


rules
message trace
accepted domains
remote domains
connectors
Create a new rule...
Apply Office 365 Message Encryption and rights protection to messages...
Apply custom branding to OME messages...
Apply disclaimers...
Bypass spam filtering...
Filter messages by size...
Generate an incident report when sensitive information is detected...
Modify messages...
Restrict managers and their direct reports...
Restrict messages by sender or recipient...
Send messages to a moderator...
Send messages and save a copy for review...
PRIORITY
ow in this view.

4. Name your policy and from the Apply This Rule If section, say "the subject or body includes…" and then add your keyword. Here, we are putting in "Secure"



new rule - Contoso - Microsoft Edge

https://outlook.office365.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=6fd6d...

new rule

Name:

*Apply this rule if...

The subject includes...

*Do the following...

Apply Office 365 Message En

Except if...

Properties of this rule:

Audit this rule with severity

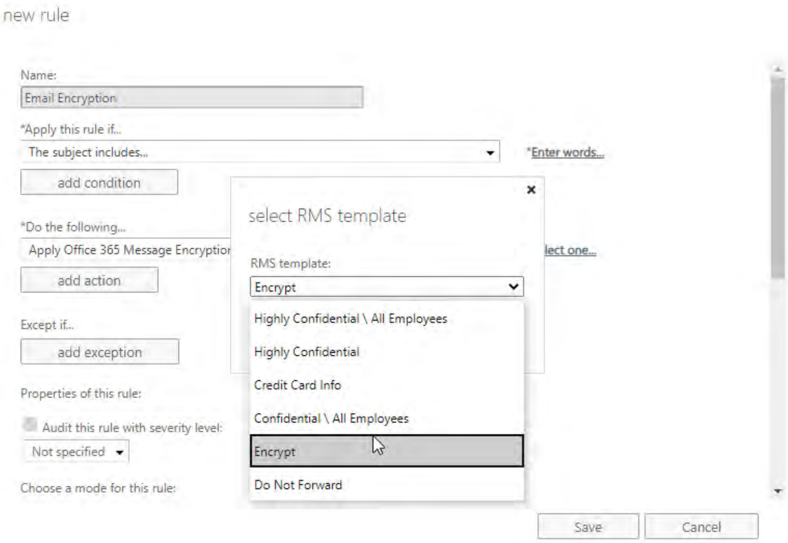
Not specified

Choose a mode for this rule:

specify words or phrases

Secure

5. In the Do the Following section, click the select one for the RMS template and chose encrypt



new rule

Name:

Email Encryption

*Apply this rule if...

The subject includes...

*Enter words...

*Do the following...

Apply Office 365 Message Encryption

lect one...

Except if...

Properties of this rule:

Audit this rule with severity level:

Not specified

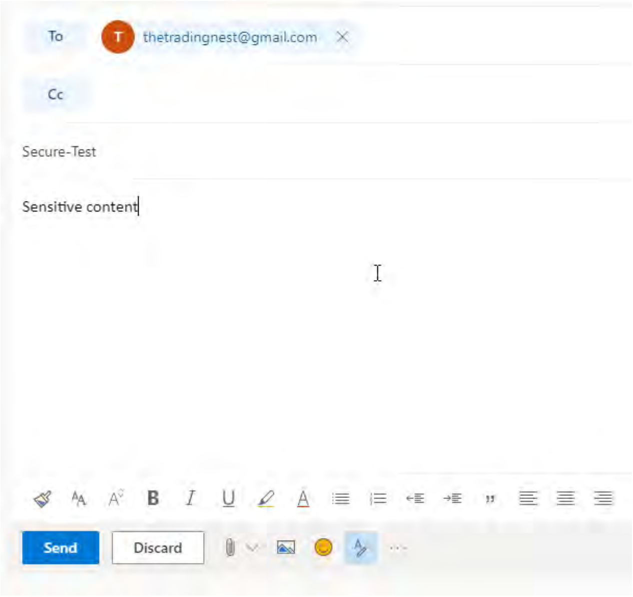
Choose a mode for this rule:

select RMS template

RMS template:

Encrypt

6. After you click Save you can test your policy. In this case, we are showing a message sent to a Gmail user

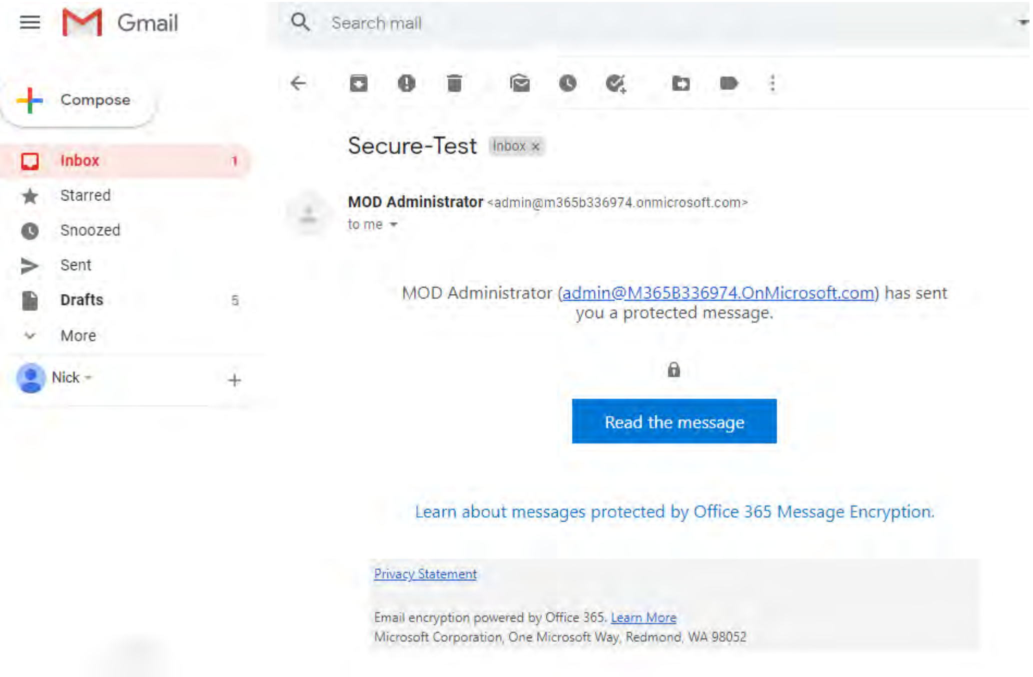

To: thetradingnest@gmail.com

Cc

Secure-Test

Sensitive content

7. Gmail user inbox:


Secure-Test

MOD Administrator <admin@m365b336974.onmicrosoft.com>
to me

MOD Administrator (admin@M365B336974.OnMicrosoft.com) has sent you a protected message.

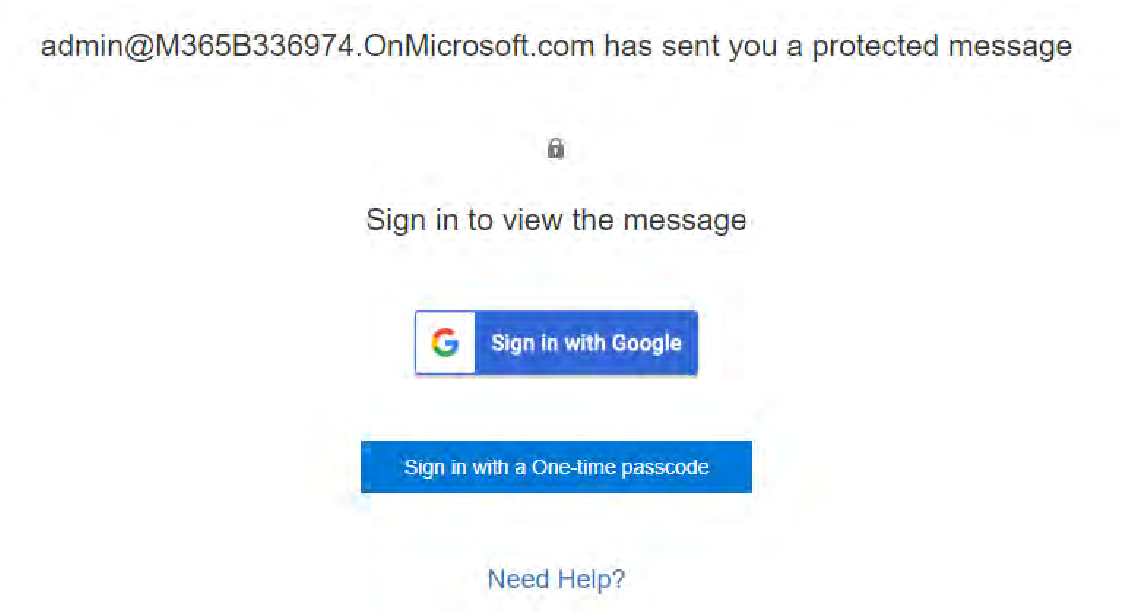
Read the message

Learn about messages protected by Office 365 Message Encryption.

Privacy Statement

Email encryption powered by Office 365. Learn More
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

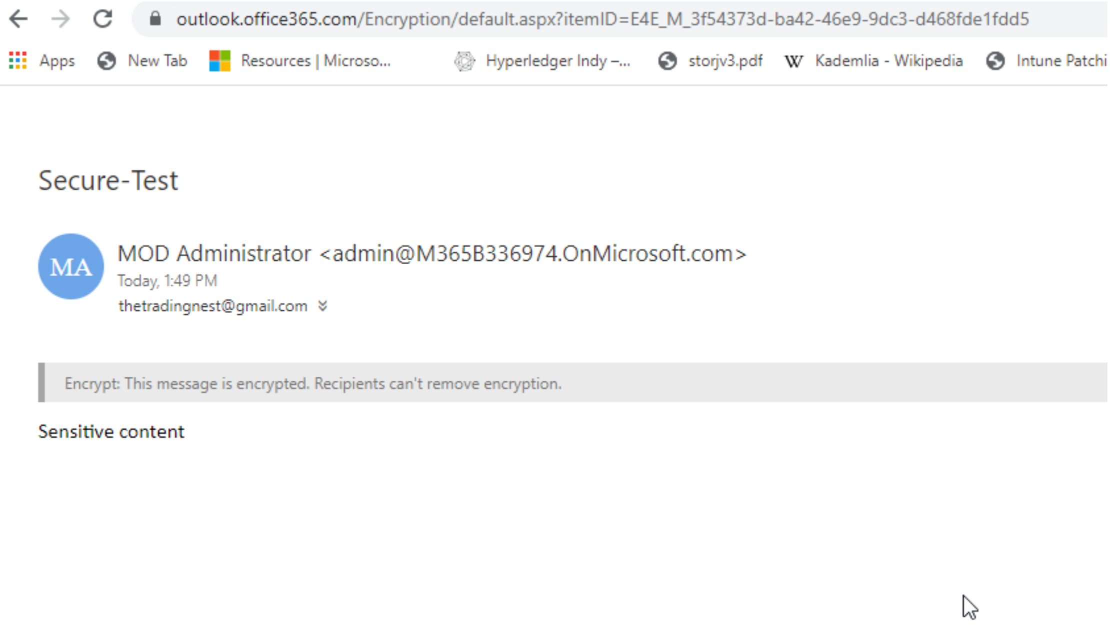
8. When the Gmail user clicks on Read the Message, they can choose to login with their Google credentials or get a one-time passcode sent to their email. In this case, we chose one-time passcode.



admin@M365B336974.OnMicrosoft.com has sent you a protected message

Sign in to view the message

9. After we type in the correct passcode, we can view the encrypted message in the OME portal and send an encrypted reply



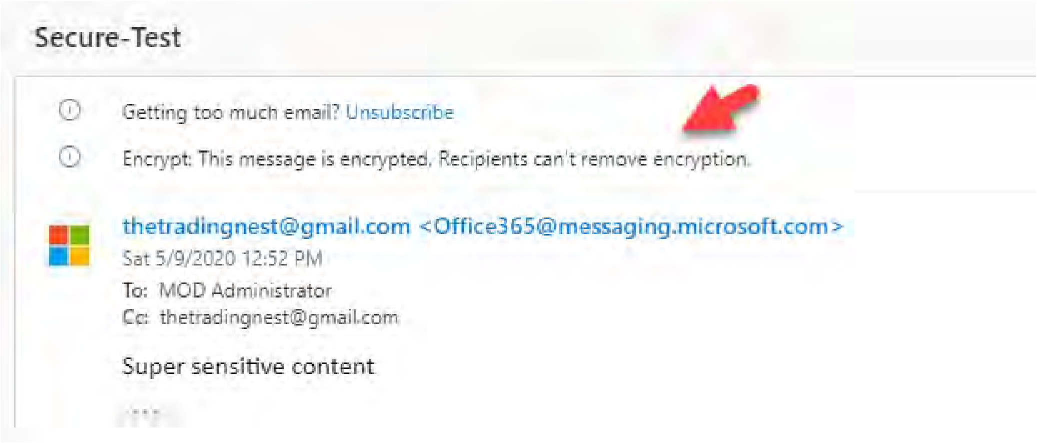
outlook.office365.com/Encryption/default.aspx?itemID=E4E_M_3f54373d-ba42-46e9-9dc3-d468fde1fdd5

Secure-Test

MOD Administrator <admin@M365B336974.OnMicrosoft.com>
Today, 1:49 PM
thetradingnest@gmail.com

Encrypt: This message is encrypted. Recipients can't remove encryption.

Sensitive content



Secure-Test

Getting too much email? Unsubscribe

Encrypt: This message is encrypted. Recipients can't remove encryption.

thetradingnest@gmail.com <Office365@messaging.microsoft.com>
Sat 5/9/2020 12:52 PM
To: MOD Administrator
Cc: thetradingnest@gmail.com

Super sensitive content

PowerShell

[Enable Mail Flow rule for Single Tenant]

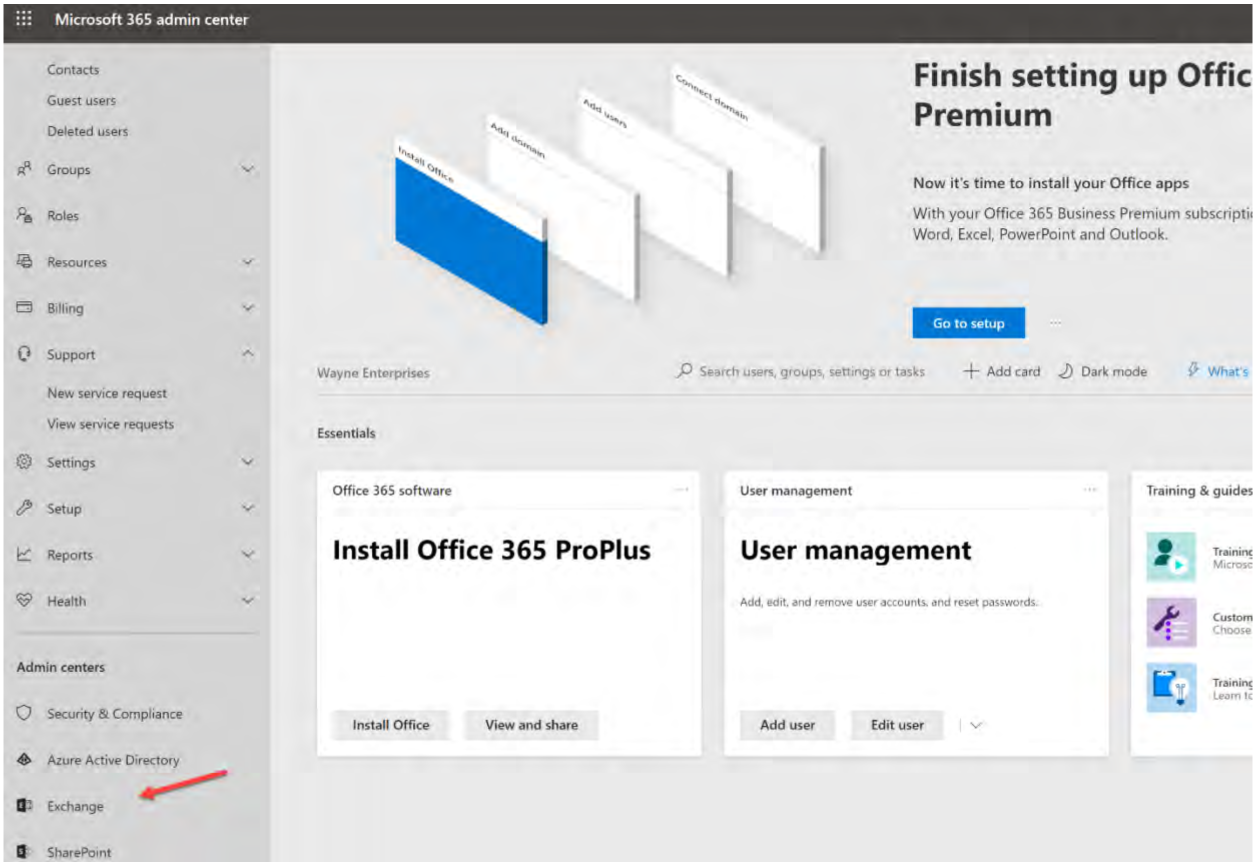
Enable Client Rules Forwarding Blocks

This is a transport rule to help stop data exfiltration with client created rules that auto-forwards email from users' mailboxes to external email addresses. This is an increasingly common data leakage method in organizations.

Compliance Controls

- GDPR; Control 6.8.2
- ISO 27018:2014; Control A.10.2

1. In the 365 Admin Center, click on Exchange under Admin Centers



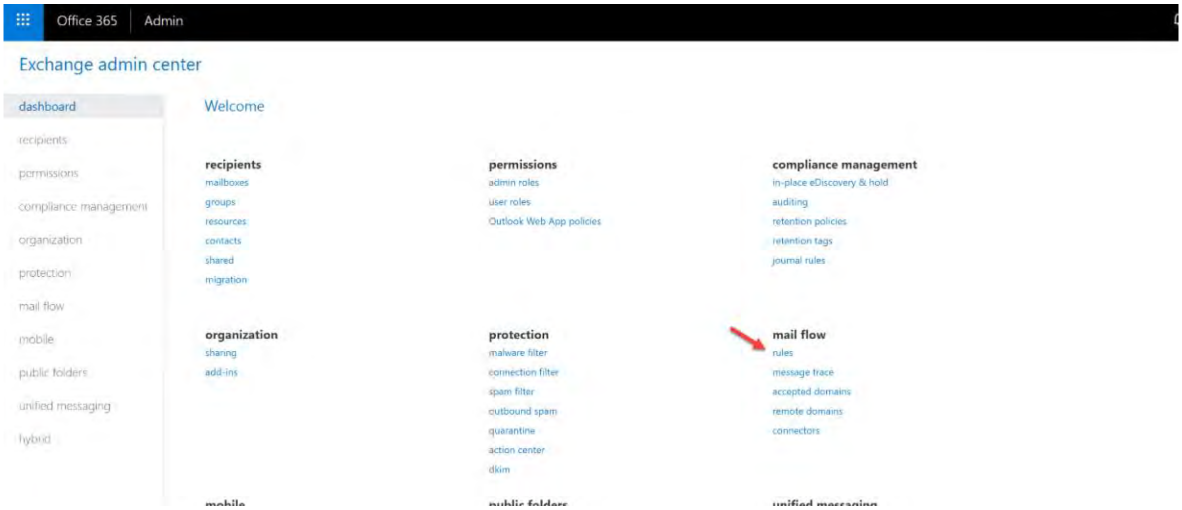
Now it's time to install your Office apps

With your Office 365 Business Premium subscripti Word, Excel, PowerPoint and Outlook.

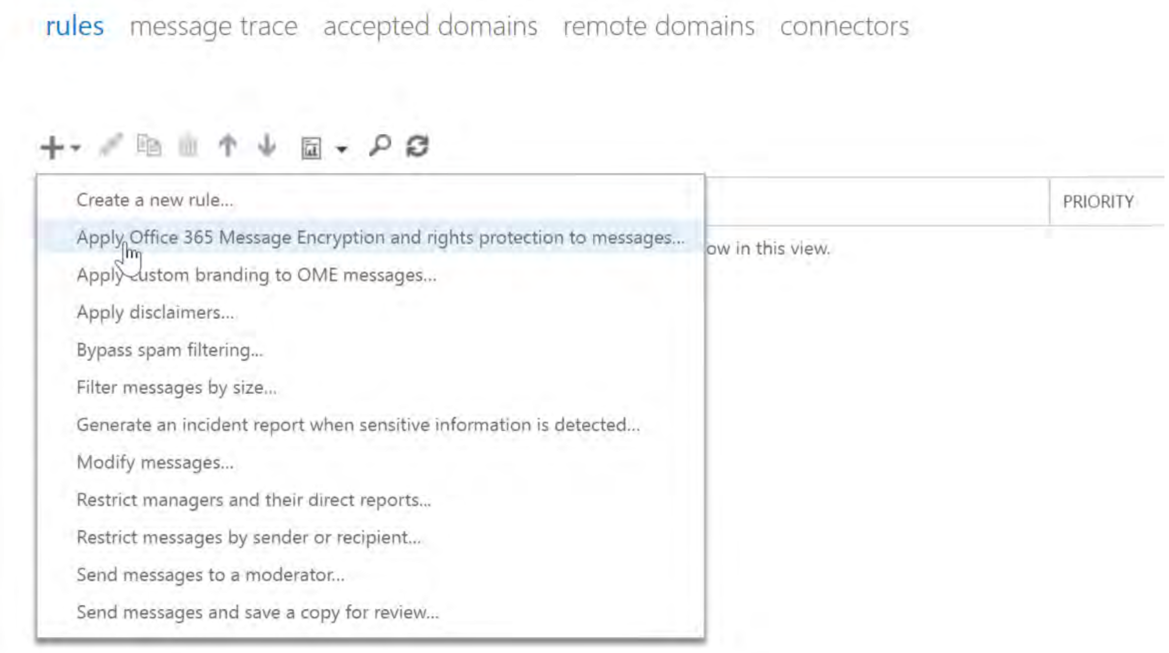
Add, edit, and remove user accounts, and reset passwords.

OVERVIEW & USER GUIDE

2. In the Mail flow section, click on Rules

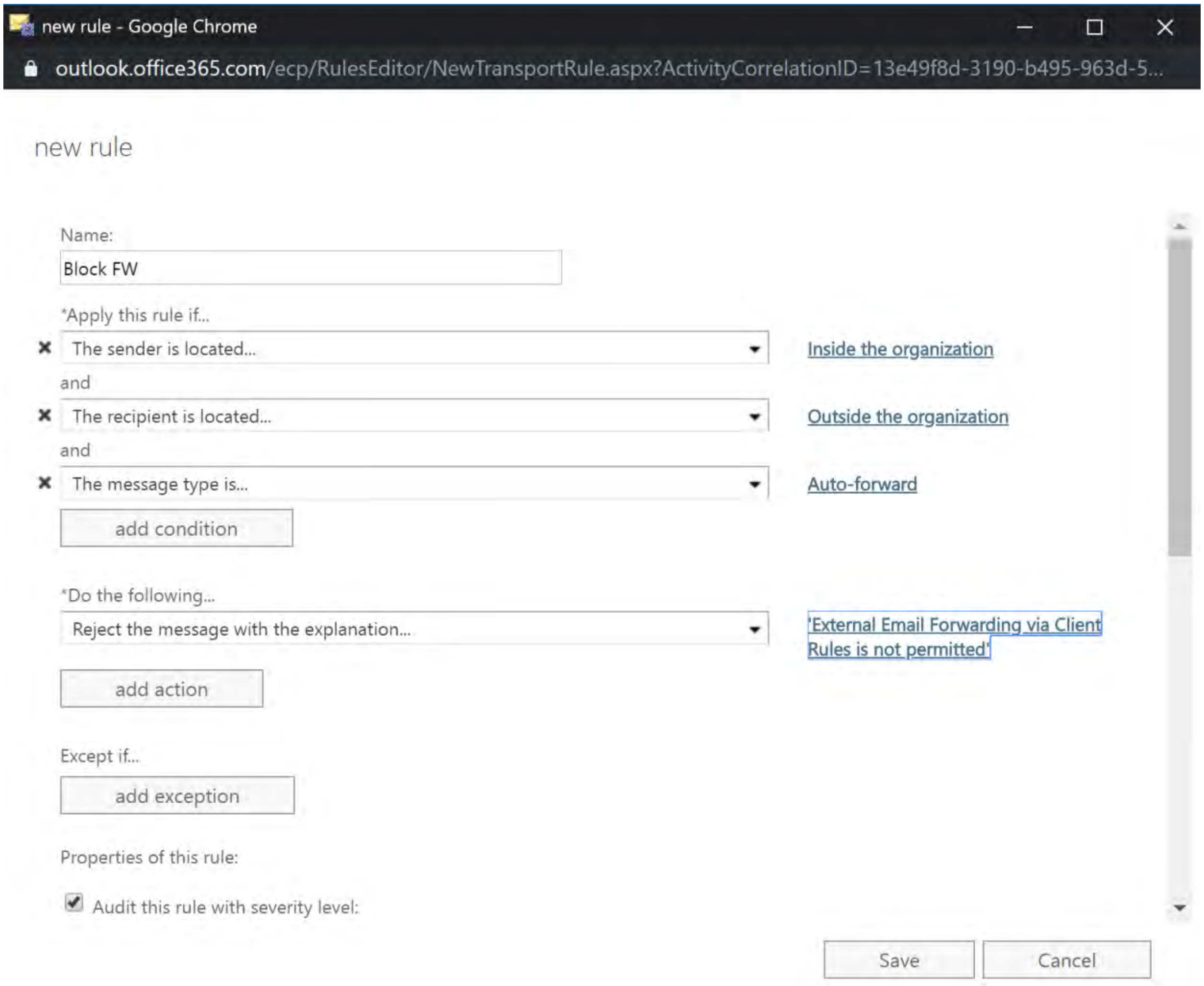


3. Click on the plus sign and click Apply Office 365 Message Encryption (allows you to define multiple conditions)


rules
message trace
accepted domains
remote domains
connectors
Create a new rule...
Apply Office 365 Message Encryption and rights protection to messages...
Apply custom branding to OME messages...
Apply disclaimers...
Bypass spam filtering...
Filter messages by size...
Generate an incident report when sensitive information is detected...
Modify messages...
Restrict managers and their direct reports...
Restrict messages by sender or recipient...
Send messages to a moderator...
Send messages and save a copy for review...
PRIORITY
ow in this view.

4. Add the following Properties to the rule:

```
IF The Sender is located 'Inside the organization'
AND IF The Recipient is located 'Outside the organization'
AND IF The message type is 'Auto-Forward'
THEN Reject the message with the explanation 'External Email Forwarding via Client Rules is not permitt
ed'.
```



new rule - Google Chrome

outlook.office365.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=13e49f8d-3190-b495-963d-5...

new rule

Name: Block FW

*Apply this rule if...

✖ The sender is located... — Inside the organization

and

✖ The recipient is located... — Outside the organization

and

✖ The message type is... — Auto-forward

*Do the following...

Reject the message with the explanation... — 'External Email Forwarding via Client Rules is not permitted'

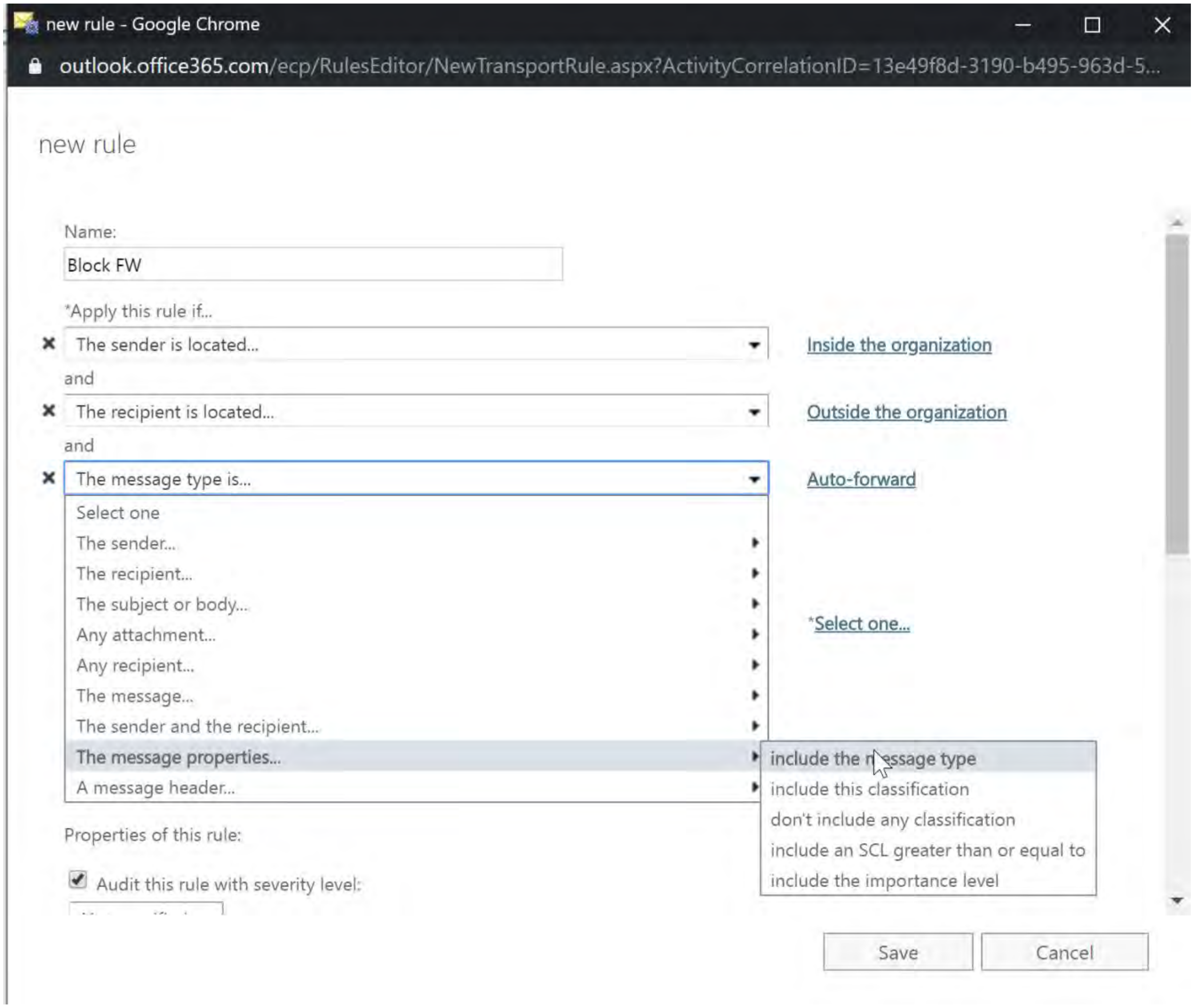
Except if...

Properties of this rule:

☑ Audit this rule with severity level:

OVERVIEW & USER GUIDE

TIP For the 3rd condition, you need to select Message Properties >Include this message type to get the Auto-forward option to populate



new rule - Google Chrome
outlook.office365.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=13e49f8d-3190-b495-963d-5...

new rule

Name:
Block FW

*Apply this rule if...

✖ The sender is located... — Inside the organization

and

✖ The recipient is located... — Outside the organization

and

✖ The message type is... — Auto-forward

Select one
The sender...
The recipient...
The subject or body...
Any attachment...
Any recipient...
The message...
The sender and the recipient...
The message properties...
A message header...
*Select one...
include the message type
include this classification
don't include any classification
include an SCL greater than or equal to
include the importance level

Properties of this rule:

☑ Audit this rule with severity level:

5. Click Save when complete. This rule will be enforced immediately. Clients will receive a custom Non-Delivery Receipt (NDR) message that is useful for highlighting external forwarding rules they may have not known existed, or that were created by a bad actor on a compromised mailbox. You can create exceptions for certain specified users or groups in the created transport rule.

PowerShell

1. Block Auto-Forward for one customer
   PowerShell Script

2. Block Auto-Forward for all of your customers via Partner Center credentials

   PowerShell Script

OVERVIEW & USER GUIDE

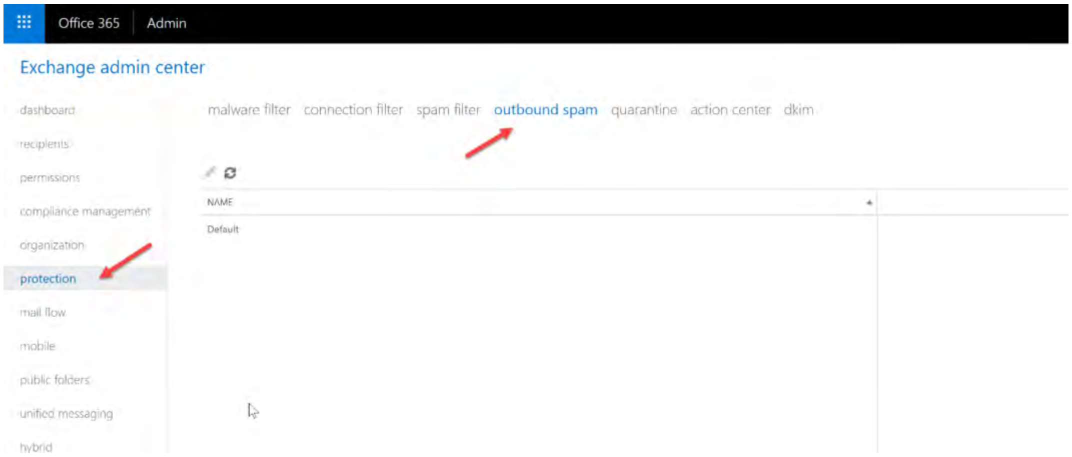
Set Outbound Spam Notifications

Setting your Exchange Online Outbound Spam notifications gives you visibility into when a user has been blocked for sending excessive or spam emails. The accounts will always be blocked, but when you configure notifications you will be notified and sent a copy of the email that caused the block to occur. A blocked account is a good indication that the account in question has been breached and that an attacker is using it to send spam emails.

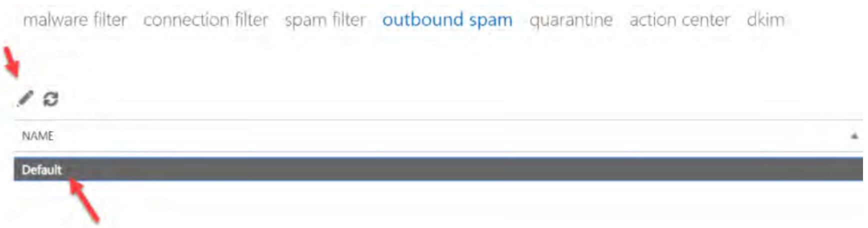
Compliance Controls

- HIPAA; Control 45 C.F.R. § 164.308(a)(5)(ii)(B)
- NIST 800-171; Control 3.14.2
- NIST 800-53; Control SI-3(a)

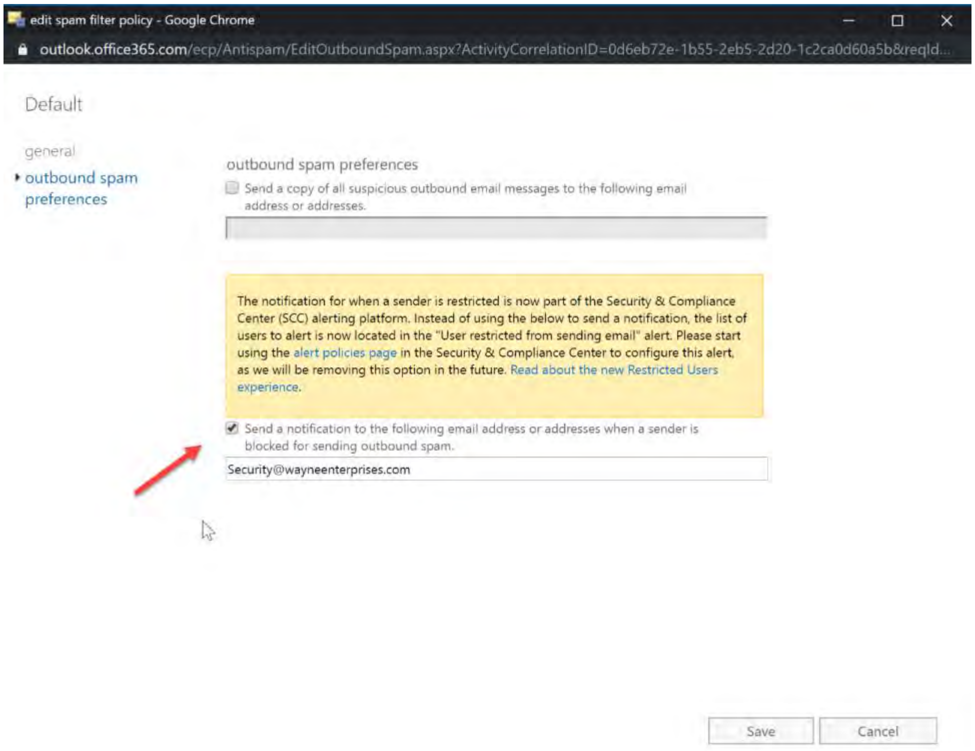
1. In the Exchange Admin Portal, go to Protection>Outbound Spam



2. Click on the Default policy and then click on the pencil icon to edit



3. Click on the outbound spam preferences icon and select the checkbox under the second section to add an email address for the alert. Make sure this email is something that people would actually check. This could be the support email for your organization which opens a ticket with your corresponding PSA tool.


edit spam filter policy - Google Chrome
outlook.office365.com/ecp/Antispam/EditOutboundSpam.aspx?ActivityCorrelationID=0d6eb72e-1b55-2eb5-2d20-1c2ca0d60a5b&reqId...
Default
general
outbound spam preferences
Save
Cancel

outbound spam preferences

□ Send a copy of all suspicious outbound email messages to the following email address or addresses.

The notification for when a sender is restricted is now part of the Security & Compliance Center (SCC) alerting platform. Instead of using the below to send a notification, the list of users to alert is now located in the "User restricted from sending email" alert. Please start using the alert policies page in the Security & Compliance Center to configure this alert, as we will be removing this option in the future. Read about the new Restricted Users experience.

☑ Send a notification to the following email address or addresses when a sender is blocked for sending outbound spam.

Security@wayneenterprises.com

4. PowerShell Script to Perform

Do not allow mailbox delegation

If your users do not delegate mailboxes, it is harder for an attacker to move from one account to another and steal data. Mailbox delegation is the practice of allowing someone else to manage your mail and calendar, which can precipitate the spread of an attack.

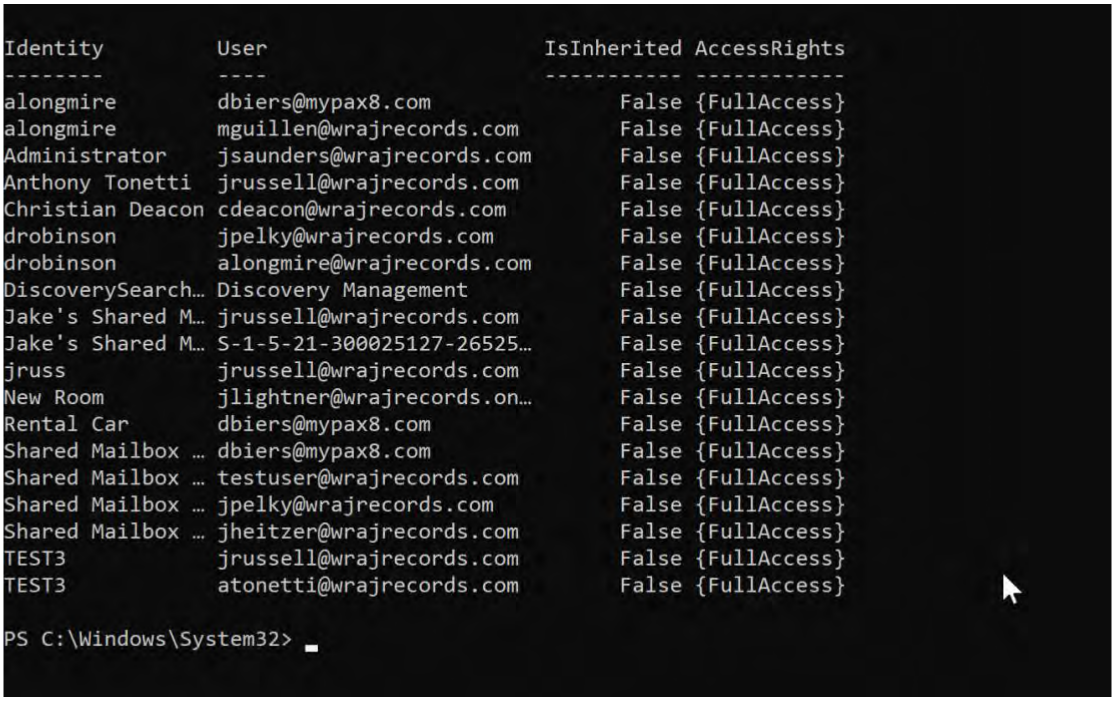
Compliance Controls

- FedRAMP Moderate; Control AC-2, Control AC-2(3)
- GDPR; Control 6.6.1
- ISO 27018:2014; Control C.9.2
- NIST 800-53; Control AC-2
- NIST CSF; Control DE.CM-1

1. To determine if there are any existing mailbox delegation permissions, run the following PowerShell script from Github. When prompted, enter in the global admin credentials for the tenant.

   PowerShell Script

2. If there are any delegation permissions existing, you will see them listed. If there are none, you will just get a new command line. Identity is the mailbox who has delegated admin permissions assigned and user is the person who has those permissions.



```
Identity         User                       IsInherited AccessRights
--------         ----                       ----------- ------------
alongmire        dbiers@mypax8.com                False {FullAccess}
alongmire        mguillen@wrajrecords.com         False {FullAccess}
Administrator    jsaunders@wrajrecords.com        False {FullAccess}
Anthony Tonetti  jrussell@wrajrecords.com         False {FullAccess}
Christian Deacon cdeacon@wrajrecords.com          False {FullAccess}
drobinson        jpelky@wrajrecords.com           False {FullAccess}
drobinson        alongmire@wrajrecords.com        False {FullAccess}
DiscoverySearch… Discovery Management             False {FullAccess}
Jake's Shared M… jrussell@wrajrecords.com         False {FullAccess}
Jake's Shared M… S-1-5-21-300025127-26525…        False {FullAccess}
jruss            jrussell@wrajrecords.com         False {FullAccess}
New Room         jlightner@wrajrecords.on…        False {FullAccess}
Rental Car       dbiers@mypax8.com                False {FullAccess}
Shared Mailbox … dbiers@mypax8.com                False {FullAccess}
Shared Mailbox … testuser@wrajrecords.com         False {FullAccess}
Shared Mailbox … jpelky@wrajrecords.com           False {FullAccess}
Shared Mailbox … jheitzer@wrajrecords.com         False {FullAccess}
TEST3            jrussell@wrajrecords.com         False {FullAccess}
TEST3            atonetti@wrajrecords.com         False {FullAccess}

PS C:\Windows\System32> _
```

3. You can run the following command to remove the access rights for users:

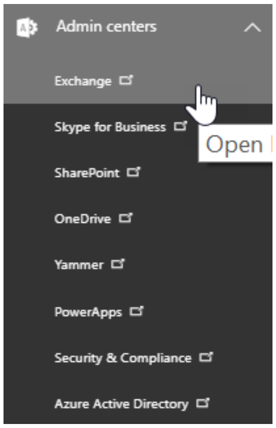
Remove-MailboxPermission -Identity Test1 -User Test2 -AccessRights FullAccess -InheritanceType All

Set up Connection Filtering:

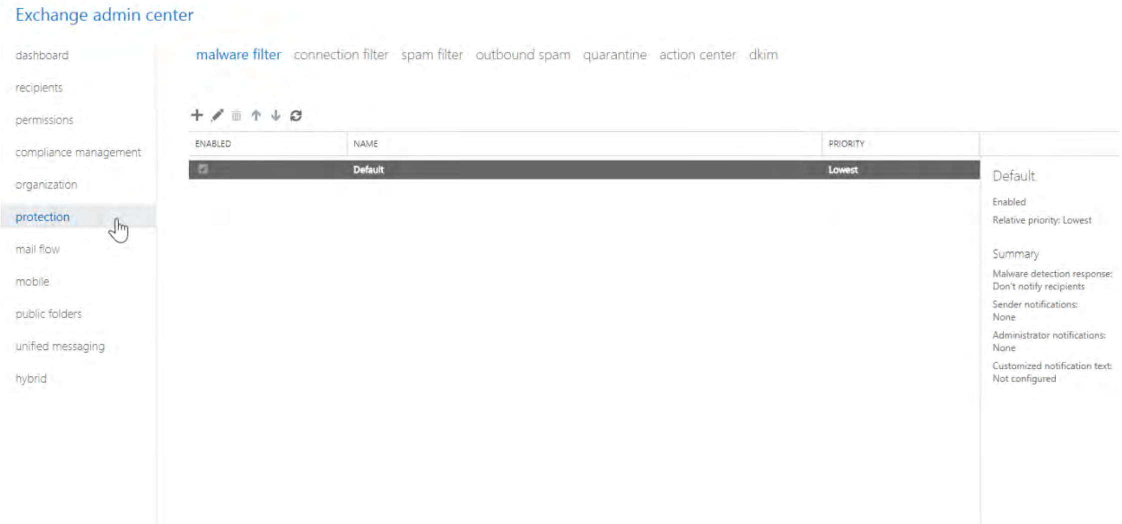
Questions to Ask:

- Do I need to create an allowed list from a specific IP range?
- Do I need to create a block list?

1. Go into Admin Centers>Exchange Admin Center



2. Select the Protection tab



ENABLED	NAME	PRIORITY
☑	Default	Lowest

Default

Enabled

Relative priority: Lowest

Summary

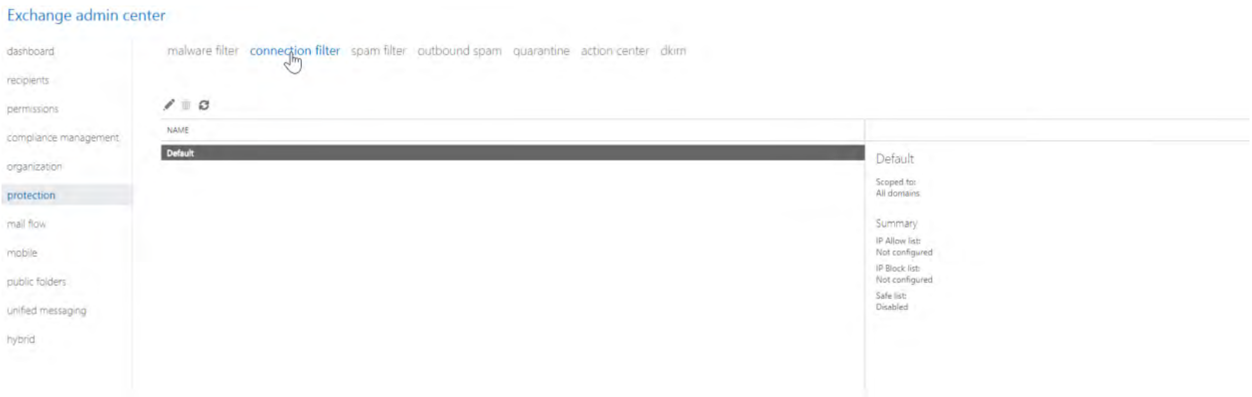
Malware detection response:
Don't notify recipients

Sender notifications:
None

Administrator notifications:
None

Customized notification text:
Not configured

3. Click on Connection Filter

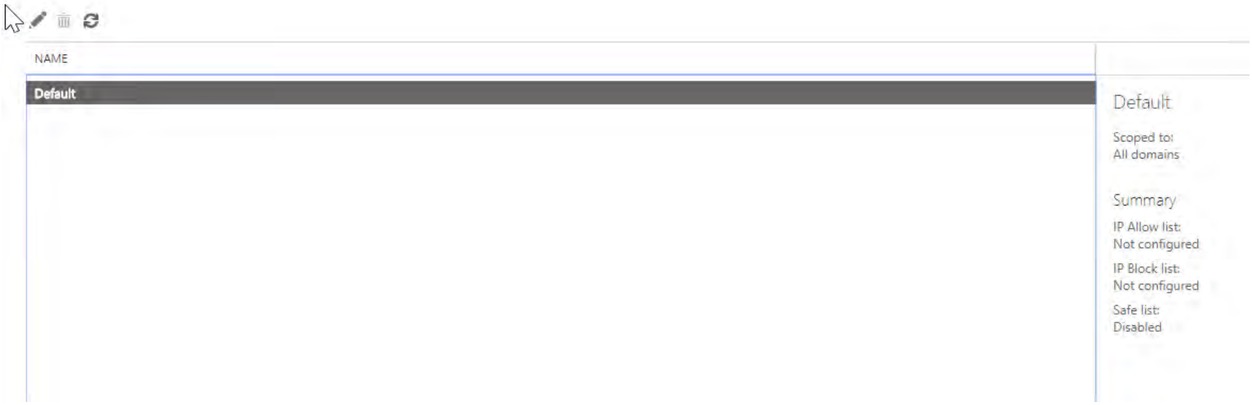


Default

Scoped to:
All domains

Summary
IP Allow list:
Not configured
IP Block list:
Not configured
Safe list:
Disabled

4. Click on the pencil icon to modify the default policy

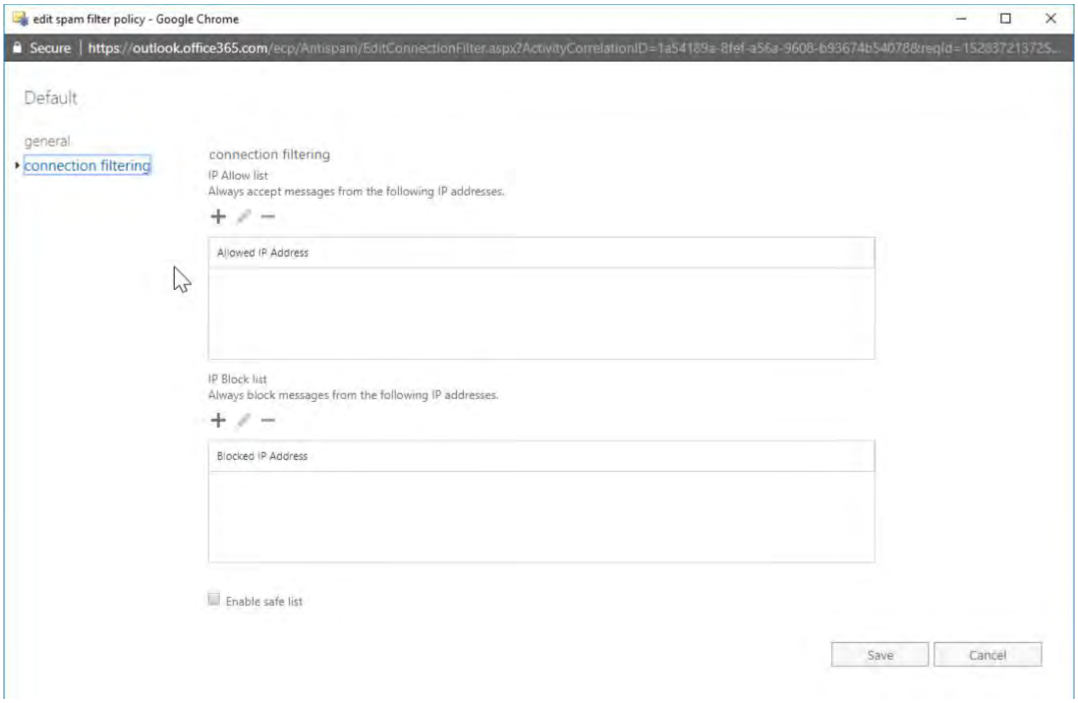


Default

Scoped to:
All domains

Summary
IP Allow list:
Not configured
IP Block list:
Not configured
Safe list:
Disabled

5. Click Connection Filtering, add Allowed/Block List



edit spam filter policy - Google Chrome

Secure | https://outlook.office365.com/ecp/Antispam/EditConnectionFilter.aspx?ActivityCorrelationID=1a54189a-8fef-a56a-9608-b93674b54078&reqId=15283721372S...

Default

general

connection filtering

connection filtering

IP Allow list

Always accept messages from the following IP addresses.

Allowed IP Address

IP Block list

Always block messages from the following IP addresses.

Blocked IP Address

□ Enable safe list

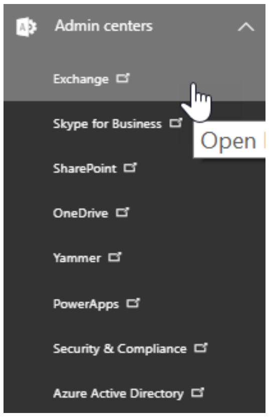
Spam Filtering:

Questions to Ask:

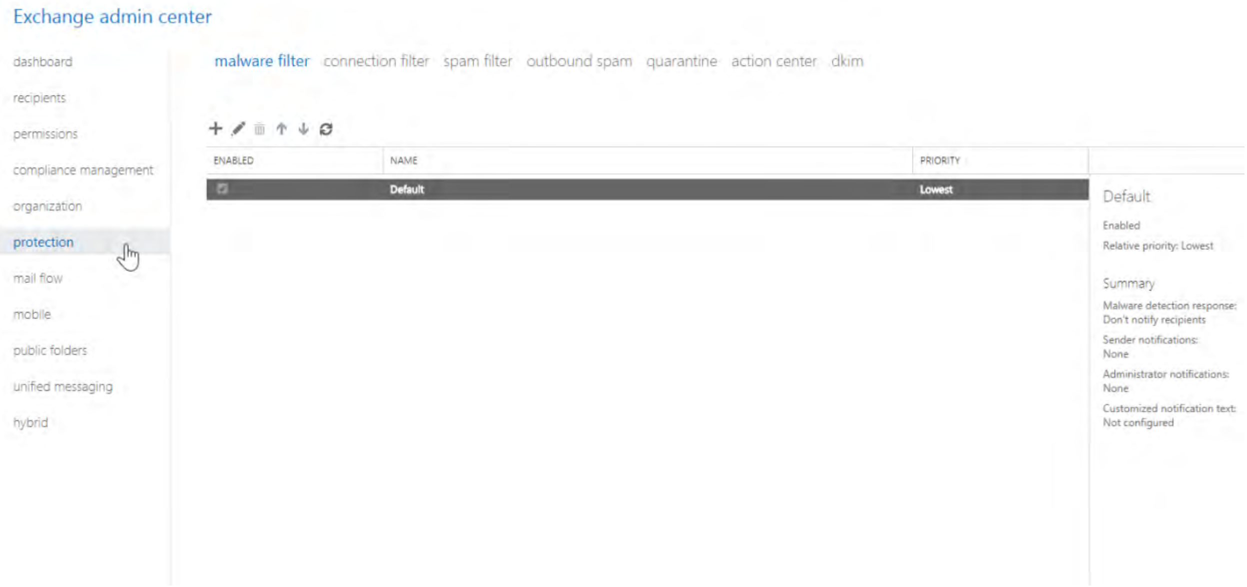
1. What actions do we want to take when a message is identified as spam?
   a. Move Message to Junk Folder (Default)
   b. Add X Header (Sends the message to the specified recipients, but adds X-header text to the message header to identify it as spam)
   c. Prepend Subject line with text (Sends the message to the intended recipients but prepends the subject line with the text that you specify in the Prefix subject line with this text input box. Using this text as an identifier, you can optionally create rules to filter or route the messages as necessary.)
   d. Redirect message to email address (Sends the message to a designated email address instead of to the intended recipients.)
2. Do we need to add allowed senders/domains or block senders/domains?
3. Do we need to filter messages written in specific language?
4. Do we need to filter message coming from specific countries/regions?
5. Do we want to configure any end-user spam notifications to inform users when messages intended for them were sent to quarantine instead? (From these notifications, end users can release false positives and report them to Microsoft for analysis.)

Steps:

1. Go to Admin Centers>Exchange Online Admin Center



2. Click on Protection



ENABLED	NAME	PRIORITY
☑	Default	Lowest

Default

Enabled

Relative priority: Lowest

Summary

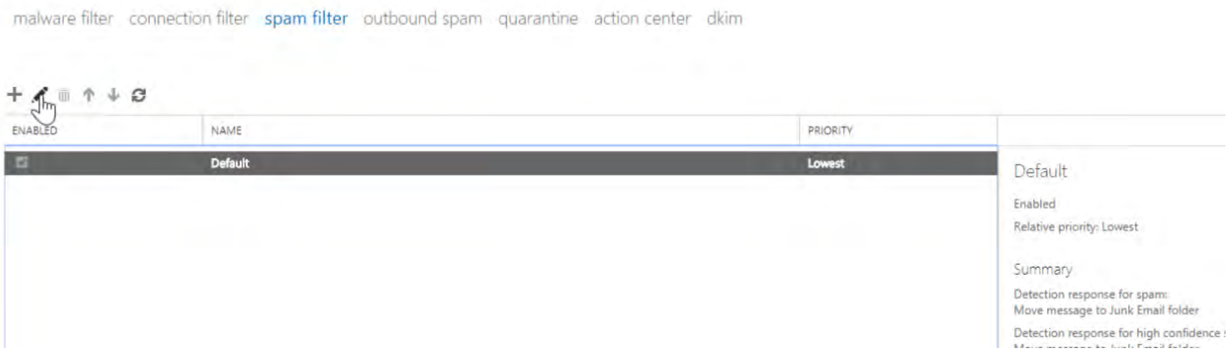
Malware detection response:
Don't notify recipients

Sender notifications:
None

Administrator notifications:
None

Customized notification text:
Not configured

3. Click on Spam Filter and click on the pencil icon to modify the default policy



ENABLED	NAME	PRIORITY
☑	Default	Lowest

Default

Enabled

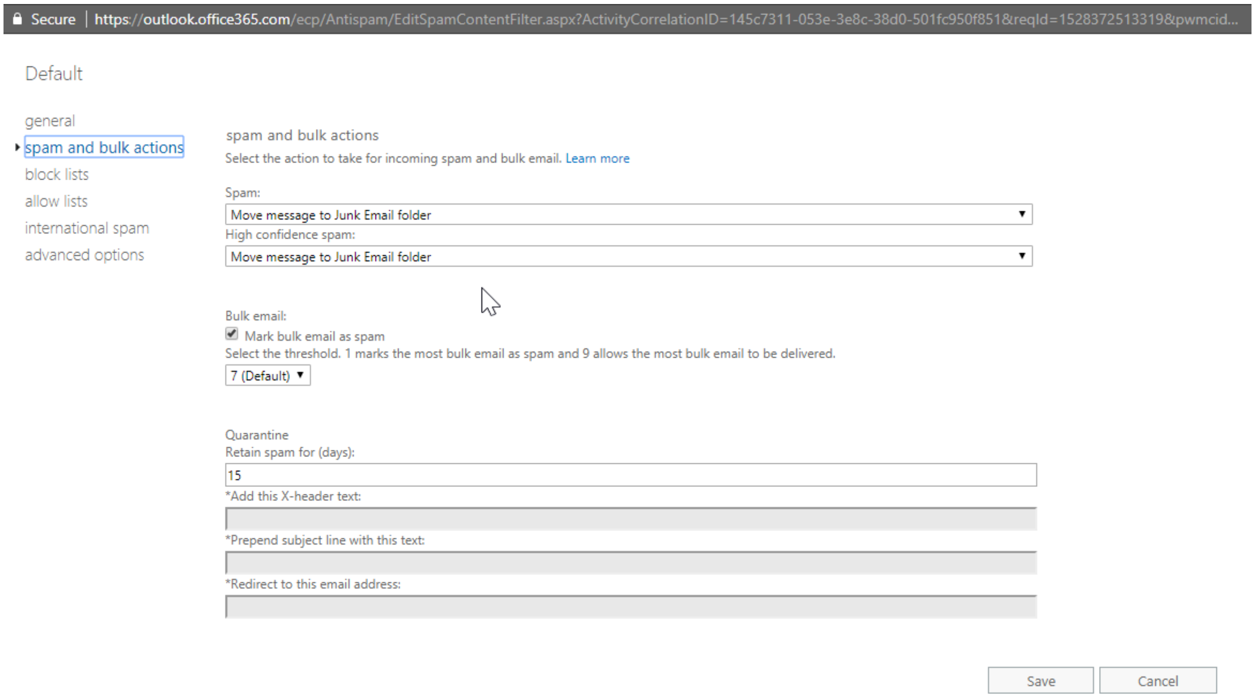
Relative priority: Lowest

Summary

Detection response for spam:
Move message to Junk Email folder

Detection response for high confidence :

4. Navigate through the tabs to configure any of the questions asked previously



https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=145c7311-053e-3e8c-38d0-501fc950f851&reqId=1528372513319&pwmcid...

spam and bulk actions

Select the action to take for incoming spam and bulk email. Learn more

Spam: Move message to Junk Email folder

High confidence spam: Move message to Junk Email folder

Bulk email:

☑ Mark bulk email as spam

Select the threshold. 1 marks the most bulk email as spam and 9 allows the most bulk email to be delivered.

7 (Default)

Quarantine

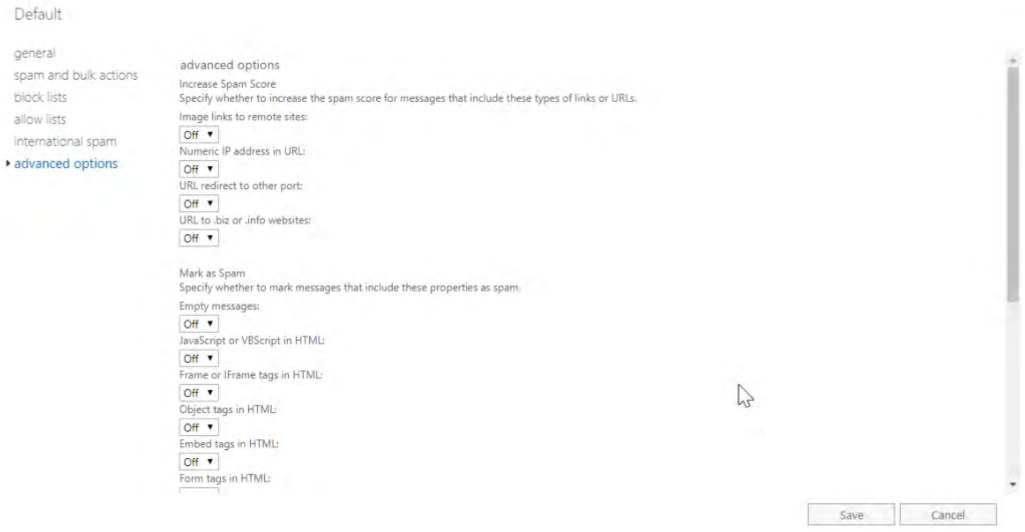
Retain spam for (days): 15

*Add this X-header text:

*Prepend subject line with this text:

*Redirect to this email address:

5. The Advanced Options tab allows you to get more granular with your policy and tighten the settings on the spam filter



advanced options

Increase Spam Score

Specify whether to increase the spam score for messages that include these types of links or URLs.

Image links to remote sites: Off

Numeric IP address in URL: Off

URL redirect to other port: Off

URL to .biz or .info websites: Off

Mark as Spam

Specify whether to mark messages that include these properties as spam.

Empty messages: Off

JavaScript or VBScript in HTML: Off

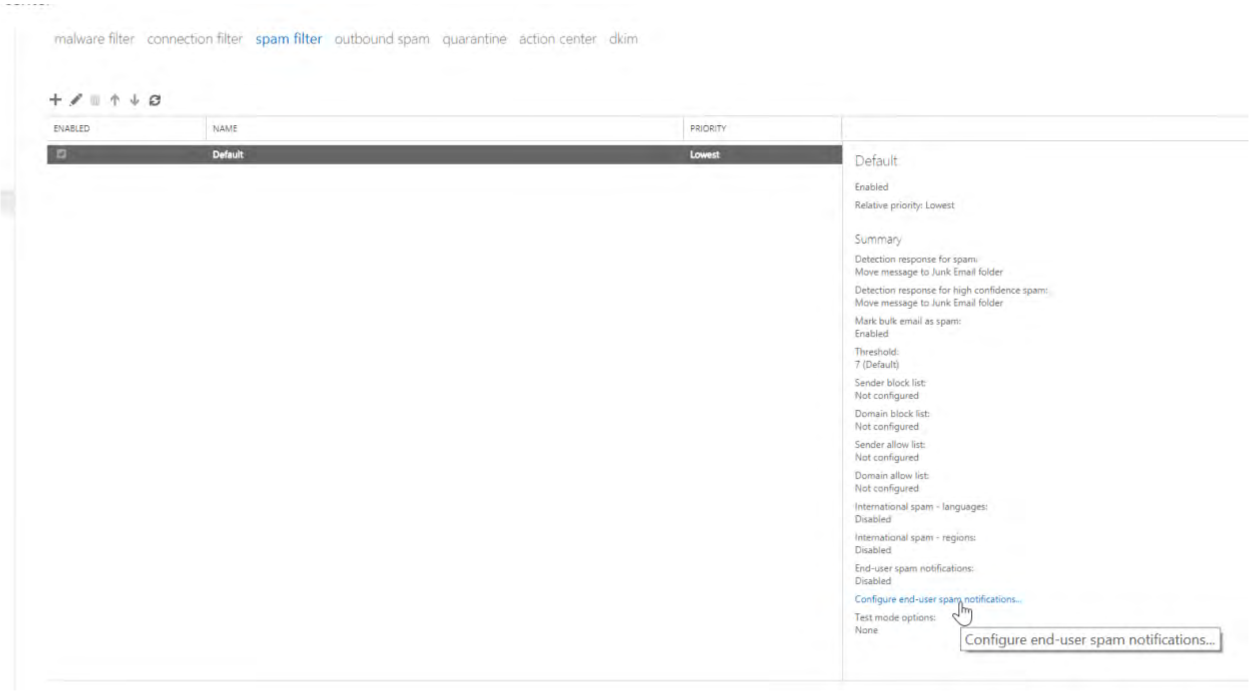
Frame or IFrame tags in HTML: Off

Object tags in HTML: Off

Embed tags in HTML: Off

Form tags in HTML:

6. You can configure end user spam notifications on the right-hand side of the page



ENABLED	NAME	PRIORITY
☑	Default	Lowest

Default

Enabled

Relative priority: Lowest

Summary

Detection response for spam:
Move message to Junk Email folder

Detection response for high confidence spam:
Move message to Junk Email folder

Mark bulk email as spam:
Enabled

Threshold:
7 (Default)

Sender block list:
Not configured

Domain block list:
Not configured

Sender allow list:
Not configured

Domain allow list:
Not configured

International spam - languages:
Disabled

International spam - regions:
Disabled

End-user spam notifications:
Disabled

Configure end-user spam notifications...

Test mode options:
None

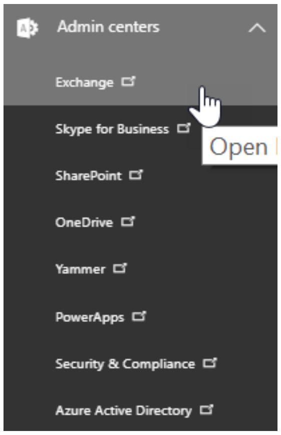
[PowerShell Commands to Configure]

OVERVIEW & USER GUIDE

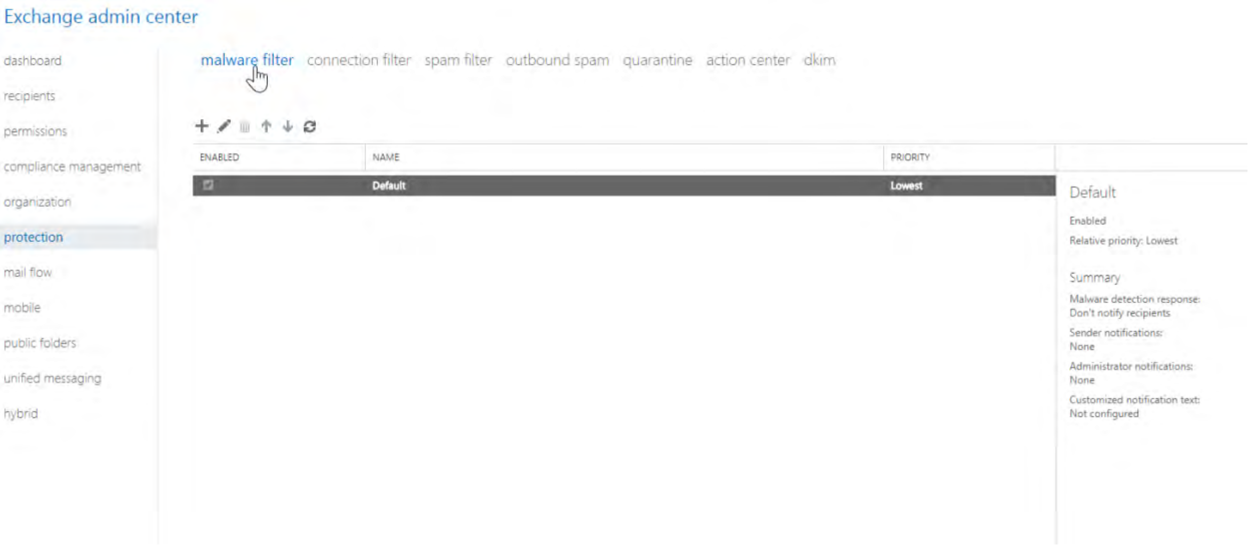
Malware:

- This is already set up company-wide via default anti-malware policy
- Do you need to create more granular policies for a certain group of users such as additional notifications via text or heightened filtering based on file extensions?

1. Go to Admin Centers>Exchange



2. Go to Protection>Malware Filter>Click on the pencil icon to modify default policy



ENABLED	NAME	PRIORITY
☑	Default	Lowest

Default

Enabled

Relative priority: Lowest

Summary

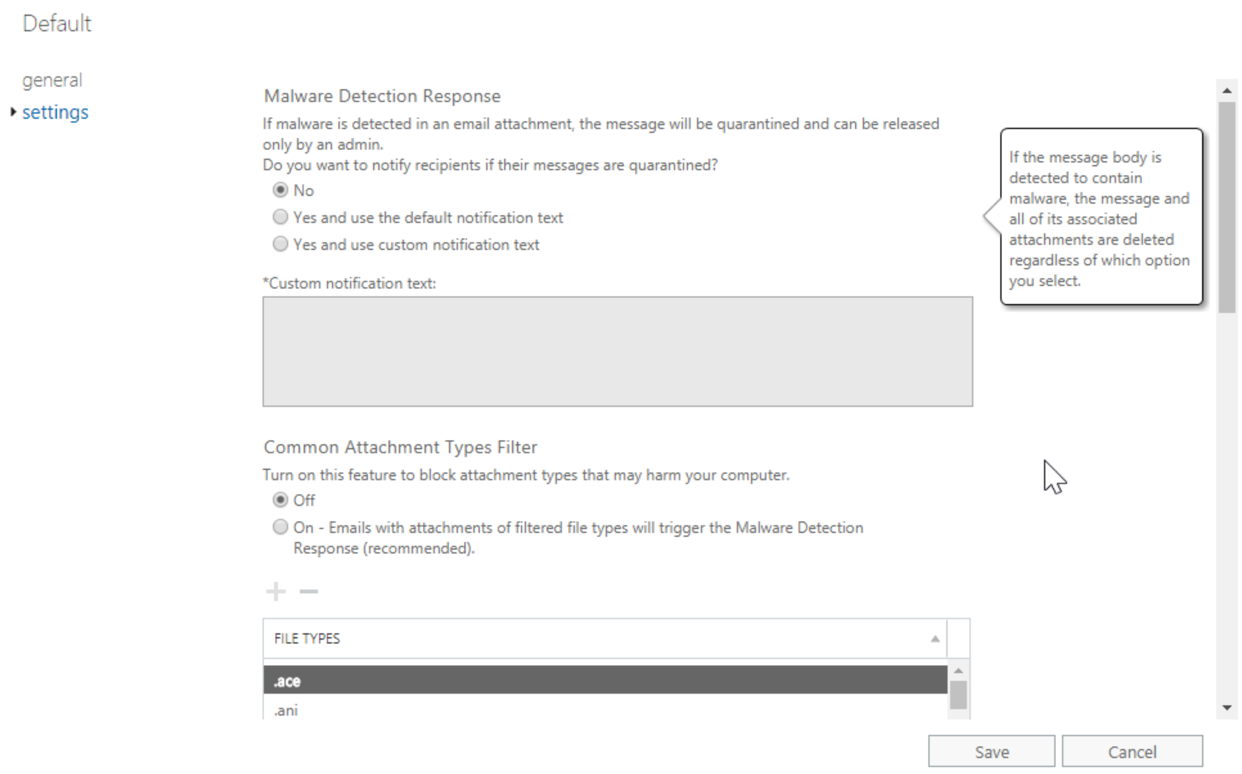
Malware detection response:
Don't notify recipients

Sender notifications:
None

Administrator notifications:
None

Customized notification text:
Not configured

3. Modify accordingly



Default

general

settings

Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin.

Do you want to notify recipients if their messages are quarantined?

● No

○ Yes and use the default notification text

○ Yes and use custom notification text

*Custom notification text:

If the message body is detected to contain malware, the message and all of its associated attachments are deleted regardless of which option you select.

Common Attachment Types Filter

Turn on this feature to block attachment types that may harm your computer.

● Off

○ On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended).

FILE TYPES
.ace
.ani

OVERVIEW & USER GUIDE

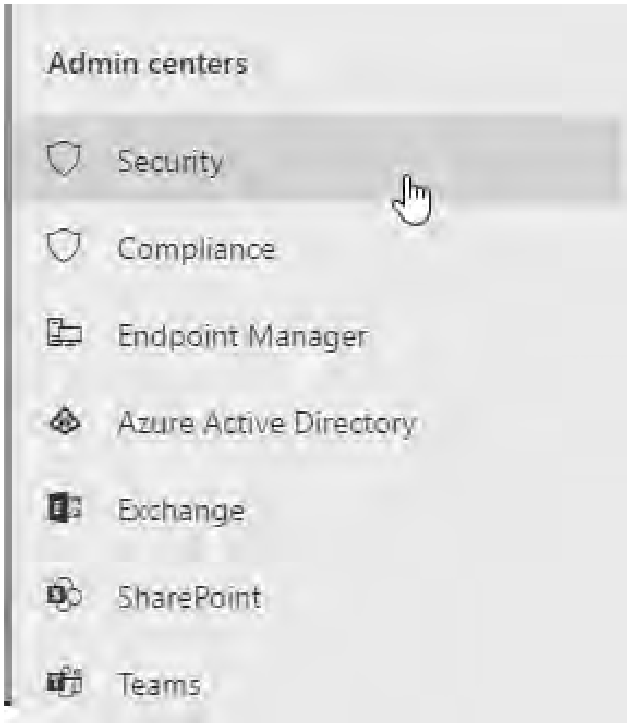
Anti-Phishing Policy

Microsoft 365 subscriptions come with a default policy for anti-phishing preconfigured but if you have the correct licensing for ATP, you can configure additional setting for impersonation attempts within the tenant. We will be configuring those additional settings here.

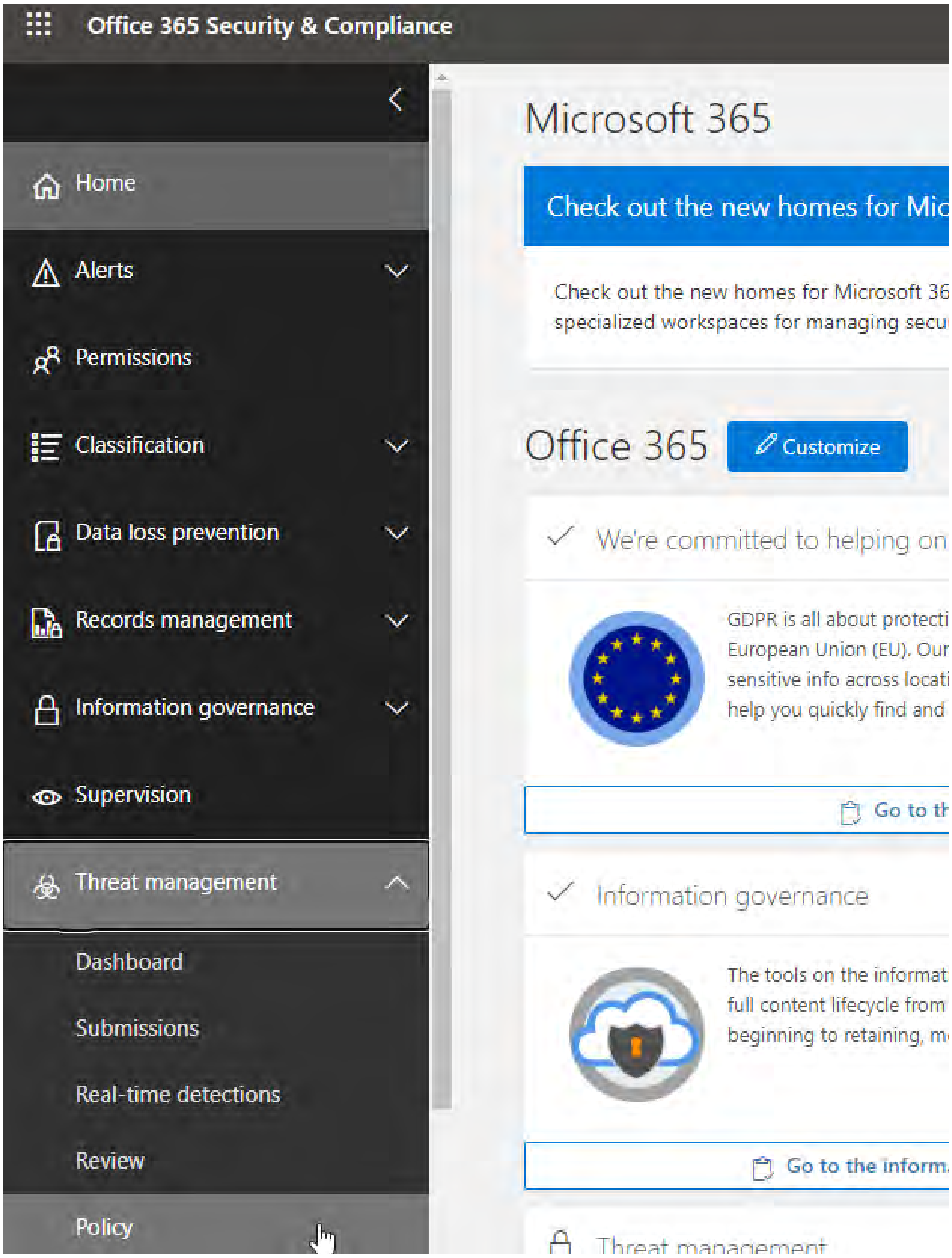
Licensing Considerations:

- Microsoft 365 Business Premium ($20/u/m) -included
- Advanced Threat Protection Plan 1 ($2/u/m)

1. In the 365 Admin Center, click Admin Centers>Security



2. Under Threat Management>click Policy

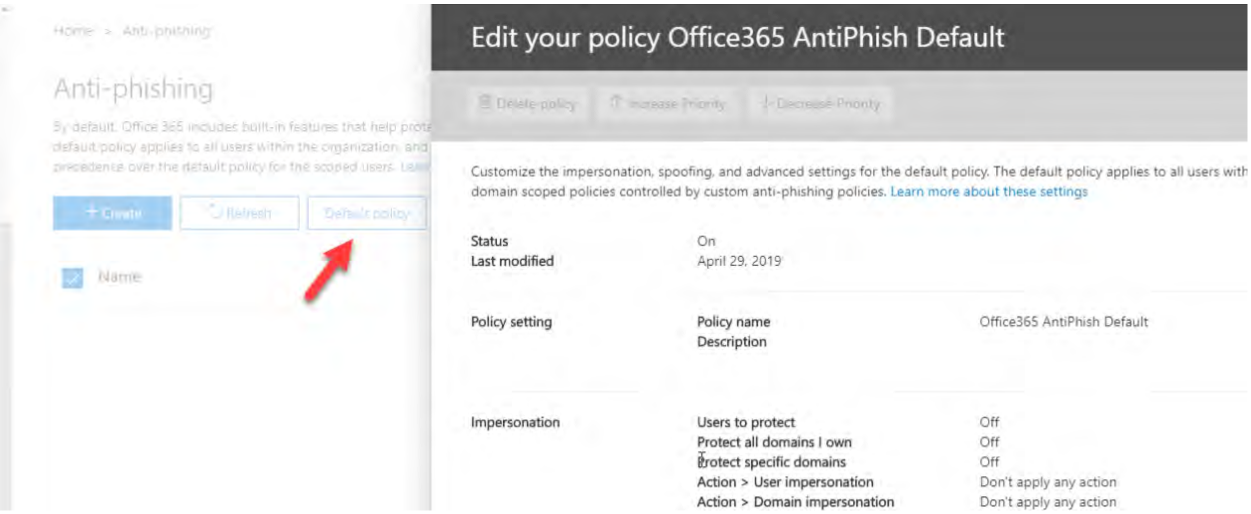


Check out the new homes for Microsoft 36
specialized workspaces for managing secu

GDPR is all about protecti
European Union (EU). Our
sensitive info across locati
help you quickly find and

The tools on the informat
full content lifecycle from
beginning to retaining, m

3. Click Anti-Phishing> Default Policy



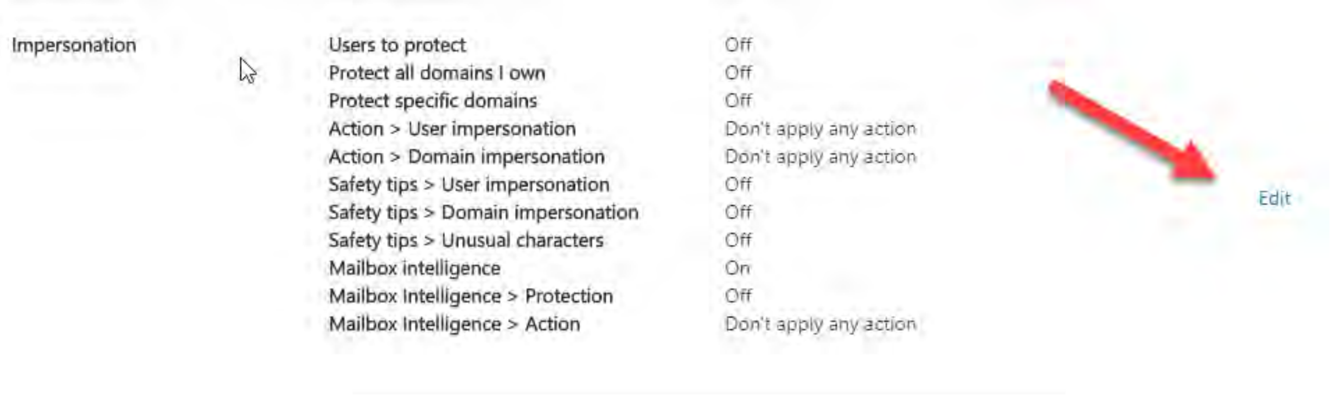
By default, Office 365 includes built-in features that help prote
default policy applies to all users within the organization, and
precedence over the default policy for the scoped users. Lea

Edit your policy Office365 AntiPhish Default

Customize the impersonation, spoofing, and advanced settings for the default policy. The default policy applies to all users with
domain scoped policies controlled by custom anti-phishing policies. Learn more about these settings

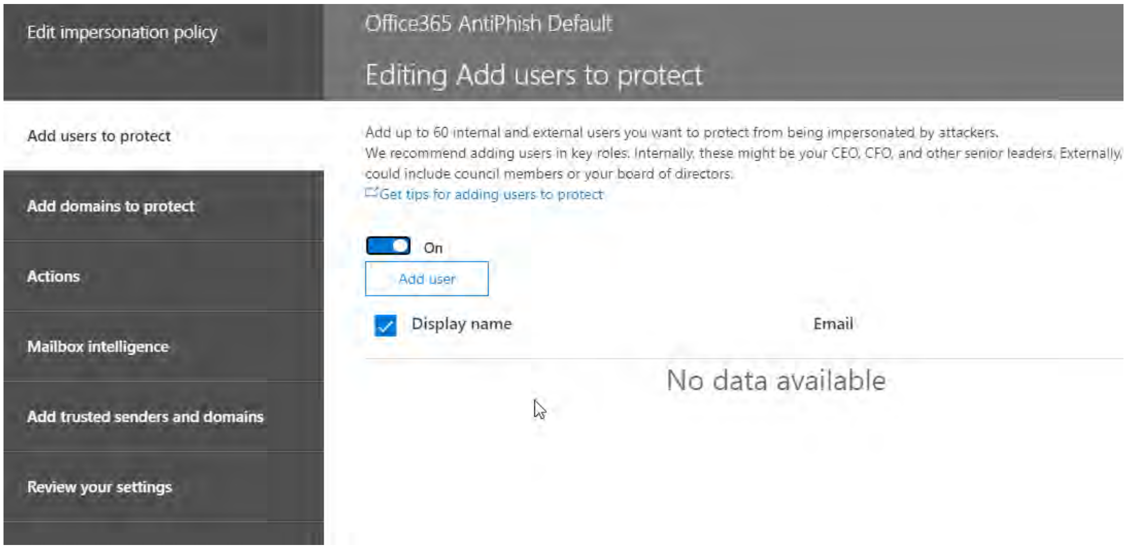
Status	On	
Last modified	April 29, 2019	
Policy setting	Policy name	Office365 AntiPhish Default
	Description	
Impersonation	Users to protect	Off
	Protect all domains I own	Off
	Protect specific domains	Off
	Action > User impersonation	Don't apply any action
	Action > Domain impersonation	Don't apply any action

4. Click on Edit in the Impersonation section



Impersonation	Users to protect	Off
	Protect all domains I own	Off
	Protect specific domains	Off
	Action > User impersonation	Don't apply any action
	Action > Domain impersonation	Don't apply any action
	Safety tips > User impersonation	Off
	Safety tips > Domain impersonation	Off
	Safety tips > Unusual characters	Off
	Mailbox intelligence	On
	Mailbox Intelligence > Protection	Off
	Mailbox Intelligence > Action	Don't apply any action

5. In the first section toggle the switch to on and add top executives or users within the organization that are most likely to get spoofed



Office365 AntiPhish Default

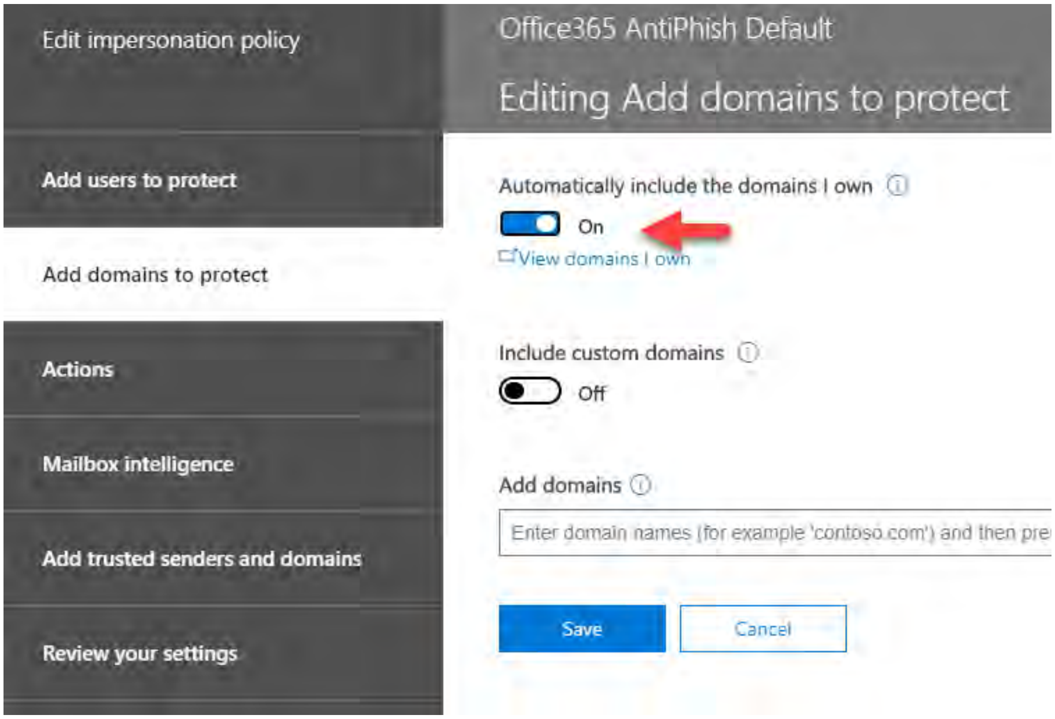
Editing Add users to protect

Add up to 60 internal and external users you want to protect from being impersonated by attackers. We recommend adding users in key roles. Internally, these might be your CEO, CFO, and other senior leaders. Externally, could include council members or your board of directors.

On

☑ Display name	Email
No data available	

6. In the Add Domains to Protect section, toggle the switch to automatically include domains I own



Office365 AntiPhish Default

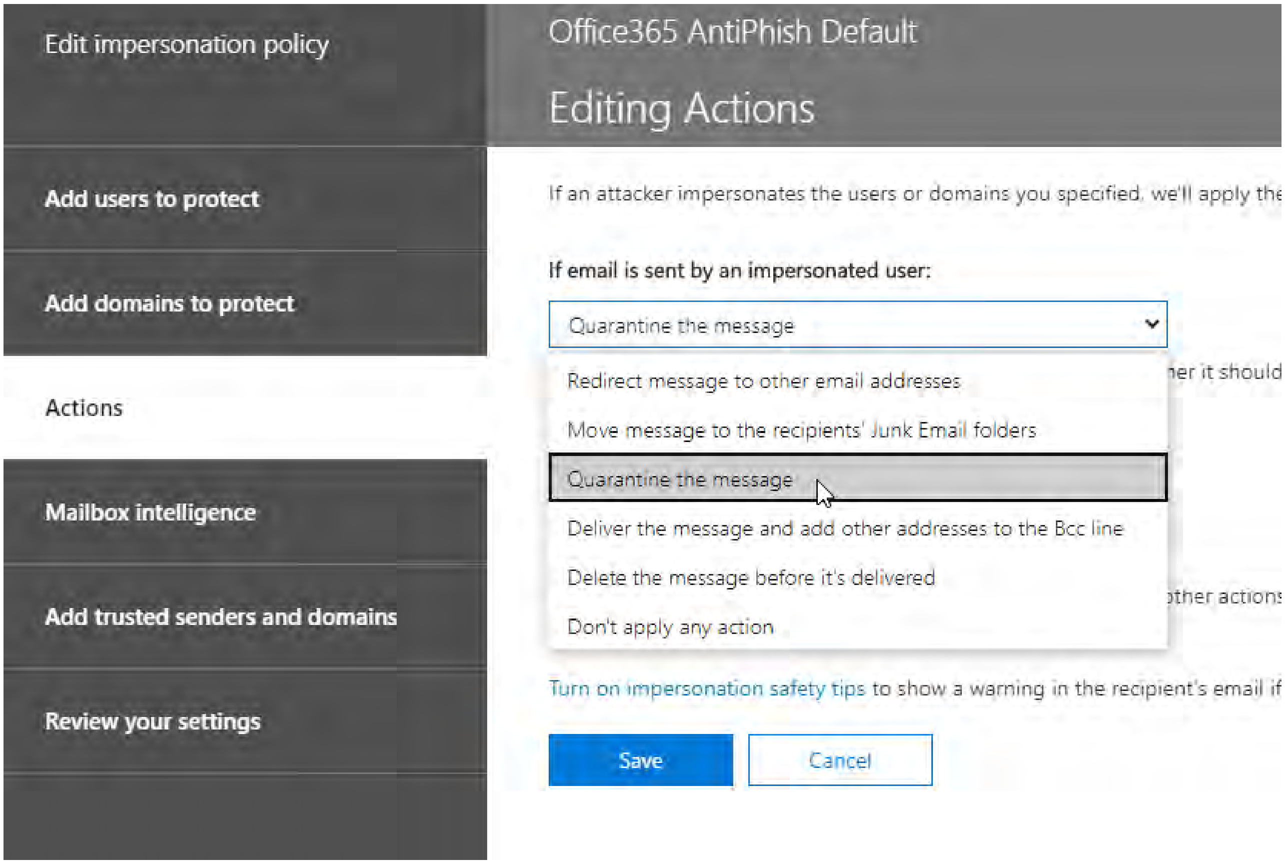
Editing Add domains to protect

Automatically include the domains I own: On

Include custom domains: Off

Add domains: Enter domain names (for example 'contoso.com') and then pre

7. In the Actions section, choose what action you want to take if a user or domain is impersonated. We recommend either quarantine or moving to Junk folder



Edit impersonation policy
Add users to protect
Add domains to protect
Actions
Mailbox intelligence
Add trusted senders and domains
Review your settings

Office365 AntiPhish Default

Editing Actions

If an attacker impersonates the users or domains you specified, we'll apply the

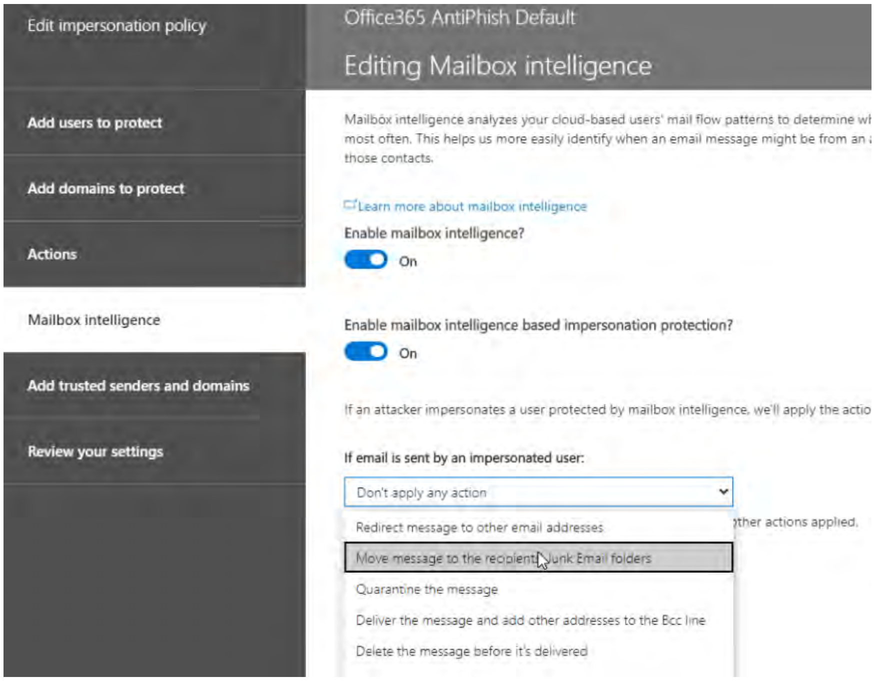
If email is sent by an impersonated user:

Quarantine the message

Redirect message to other email addresses
Move message to the recipients' Junk Email folders
Quarantine the message
Deliver the message and add other addresses to the Bcc line
Delete the message before it's delivered
Don't apply any action
ner it should
other actions

Turn on impersonation safety tips to show a warning in the recipient's email if

8. In the Mailbox Intelligence section, toggle on the protection and chose what action to take, like in the previous step



Office365 AntiPhish Default

Editing Mailbox intelligence

Mailbox intelligence analyzes your cloud-based users' mail flow patterns to determine wl
most often. This helps us more easily identify when an email message might be from an
those contacts.

Learn more about mailbox intelligence

Enable mailbox intelligence?
On

Enable mailbox intelligence based impersonation protection?
On

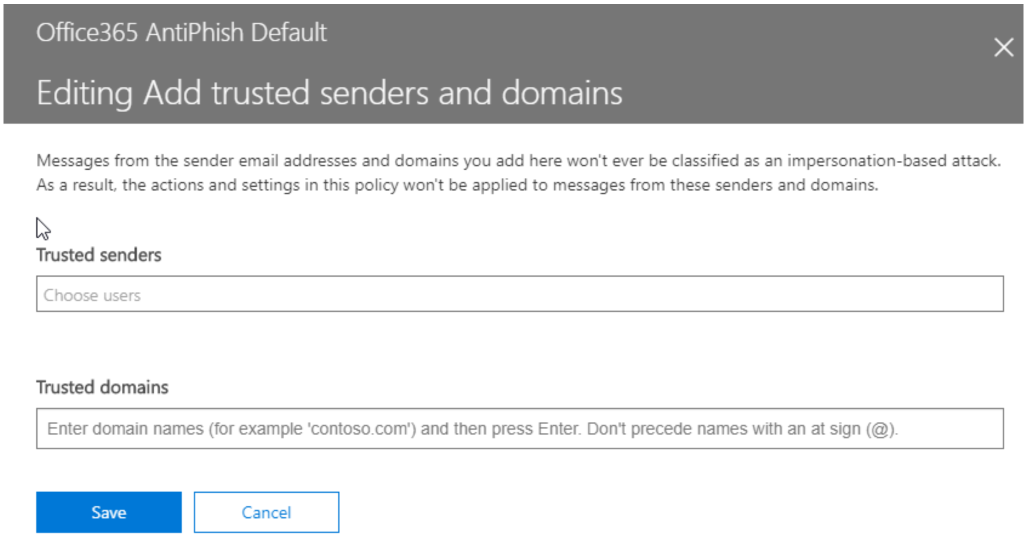
If an attacker impersonates a user protected by mailbox intelligence, we'll apply the actio

If email is sent by an impersonated user:
Don't apply any action

- Redirect message to other email addresses
- Move message to the recipients' Junk Email folders
- Quarantine the message
- Deliver the message and add other addresses to the Bcc line
- Delete the message before it's delivered

ther actions applied.

9. The final section allows you to whitelist senders and domains. Refrain from adding generic domains here like gmail.com.



Office365 AntiPhish Default

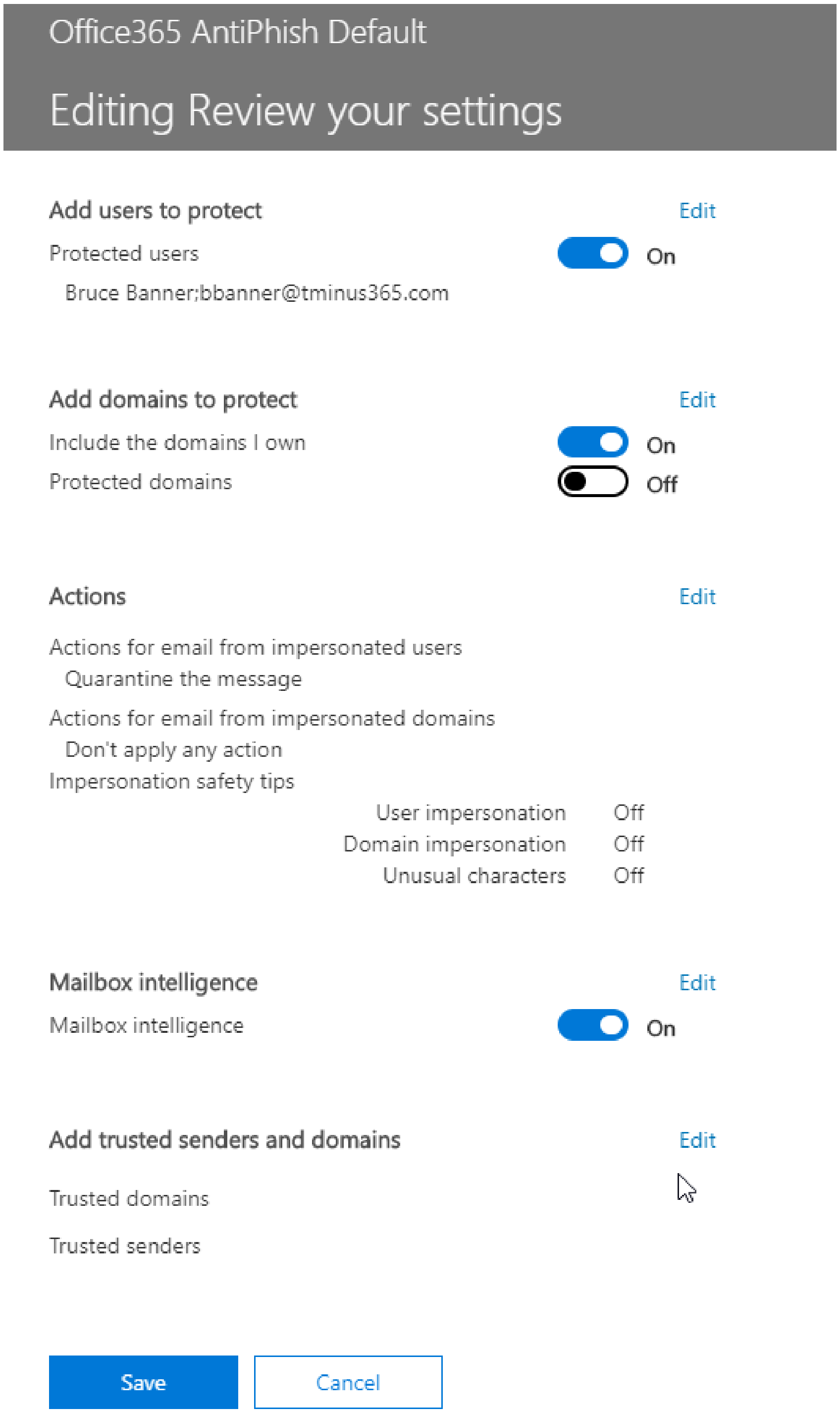
Editing Add trusted senders and domains

Messages from the sender email addresses and domains you add here won't ever be classified as an impersonation-based attack. As a result, the actions and settings in this policy won't be applied to messages from these senders and domains.

Trusted senders
Choose users

Trusted domains
Enter domain names (for example 'contoso.com') and then press Enter. Don't precede names with an at sign (@).

10. After you review your settings, you can choose to Save



Office365 AntiPhish Default

Editing Review your settings

Add users to protect — Edit

Protected users — On

Bruce Banner;bbanner@tminus365.com

Add domains to protect — Edit

Include the domains I own — On

Protected domains — Off

Actions — Edit

Actions for email from impersonated users

Quarantine the message

Actions for email from impersonated domains

Don't apply any action

Impersonation safety tips

User impersonation	Off
Domain impersonation	Off
Unusual characters	Off

Mailbox intelligence — Edit

Mailbox intelligence — On

Add trusted senders and domains — Edit

Trusted domains

Trusted senders

Configure Enhanced Filtering

Enhanced email filtering can be set up if you have a connector in 365 (3rd party email filtering service or hybrid configuration) and your MX record does not point to Microsoft 365 or Office 365. This new feature allows you to filter email based on the actual source of messages that arrive over the connector. This is also known as skip listing and this feature will allow you to overlook, or skip, any IP addresses that are considered internal to you in order to get the last known external IP address, which should be the actual source IP address. If you are using Office 365 ATP, this will enhance its machine learning capabilities and security around safe links/safe attachments/anti-spoofing from Microsoft's known malicious list based off IP. In a way, you are getting a secondary layer of protection by allowing Microsoft to view the IPs of the original email and check against their database.

For enhanced filtering configuration steps: click here

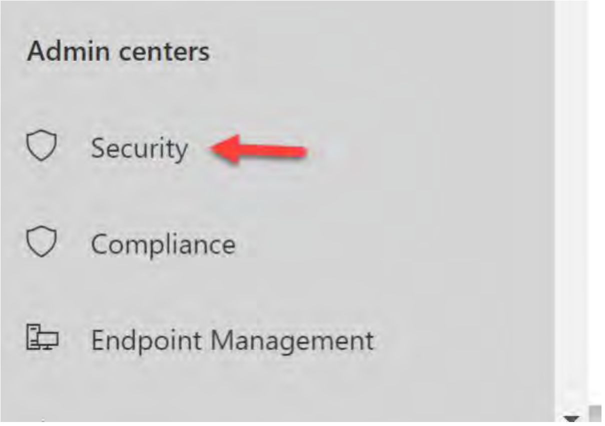
Configure ATP Safe Links and Safe Attachments Policy

Advanced Threat Protection (ATP) allows you to create policies for safe links and safe attachments across Exchange, Teams, OneDrive, and SharePoint. Real-time detonation occurs when a user clicks on any link and the content is contained in a sandbox environment. Attachments are opened inside a sandbox environment as well before they are fully delivered over email. This allows zero-day malicious attachments and links to be detected.

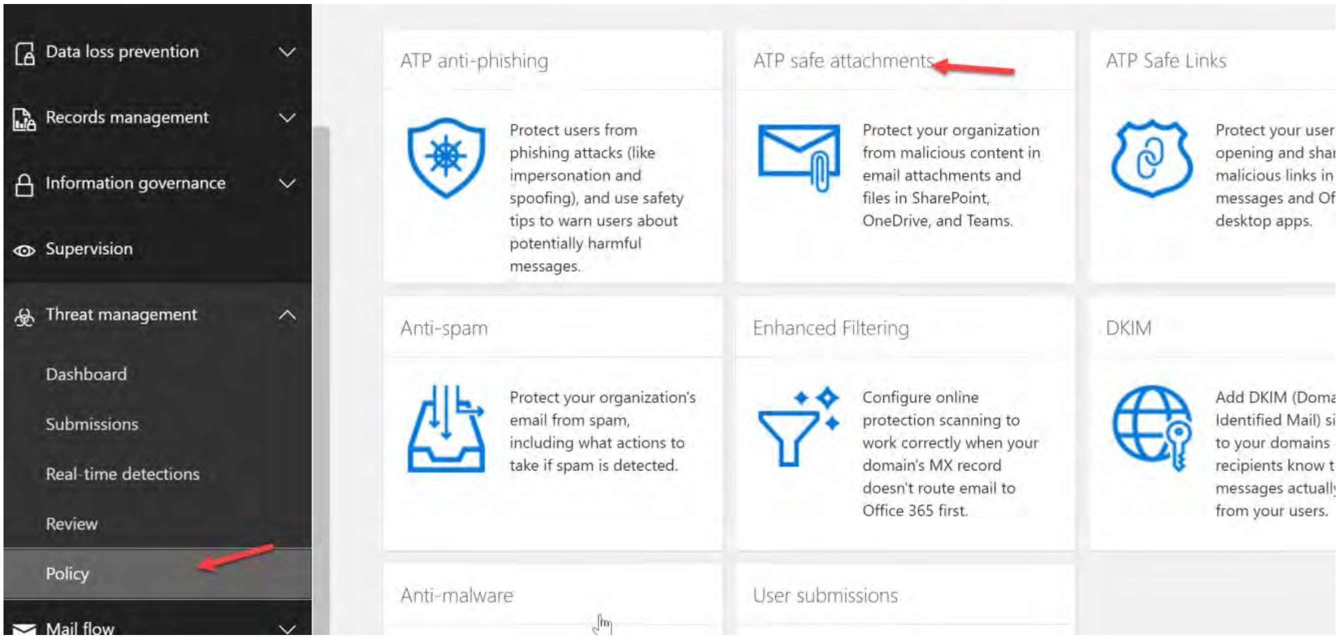
Licensing Considerations:

- Microsoft 365 Business Premium ($20/u/m) -included
- Advanced Threat Protection Plan 1 ($2/u/m)

1. In the 365 Admin Center, click Admin Centers>Security



2. Click on Threat Management>Policy>ATP Safe Attachments



ATP anti-phishing

Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.

ATP safe attachments

Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

ATP Safe Links

Protect your user opening and shar malicious links in messages and Of desktop apps.

Anti-spam

Protect your organization's email from spam, including what actions to take if spam is detected.

Enhanced Filtering

Configure online protection scanning to work correctly when your domain's MX record doesn't route email to Office 365 first.

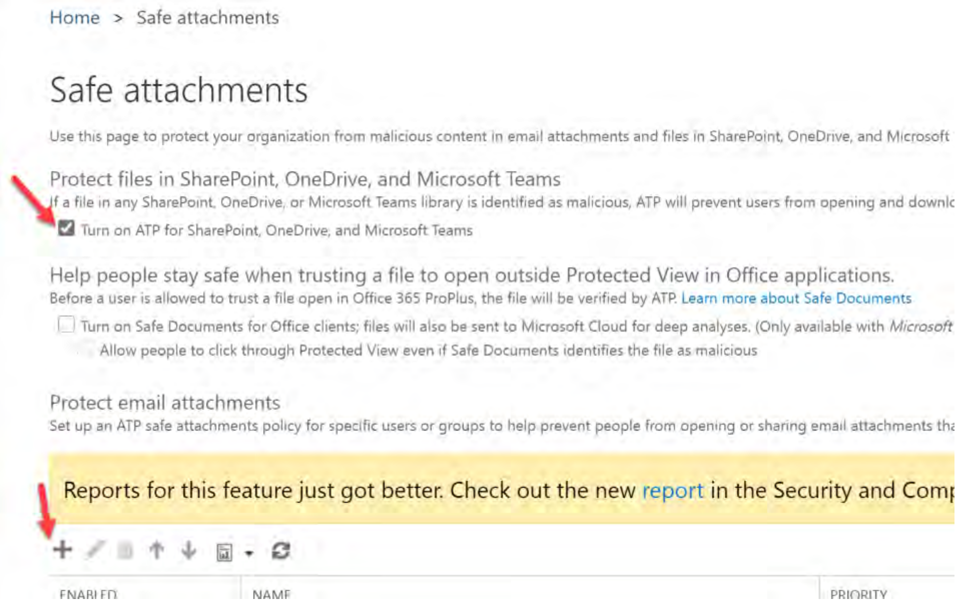
DKIM

Add DKIM (Doma Identified Mail) si to your domains recipients know t messages actually from your users.

Anti-malware

User submissions

3. Checkmark the box to turn on ATP for Teams. Select the + icon to create a new policy



Home > Safe attachments

Safe attachments

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

Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, ATP will prevent users from opening and downlc

☑ Turn on ATP for SharePoint, OneDrive, and Microsoft Teams

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 open in Office 365 ProPlus, the file will be verified by ATP. Learn more about Safe Documents

☐ Turn on Safe Documents for Office clients; files will also be sent to Microsoft Cloud for deep analyses. (Only available with *Microsoft*

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

Protect email attachments

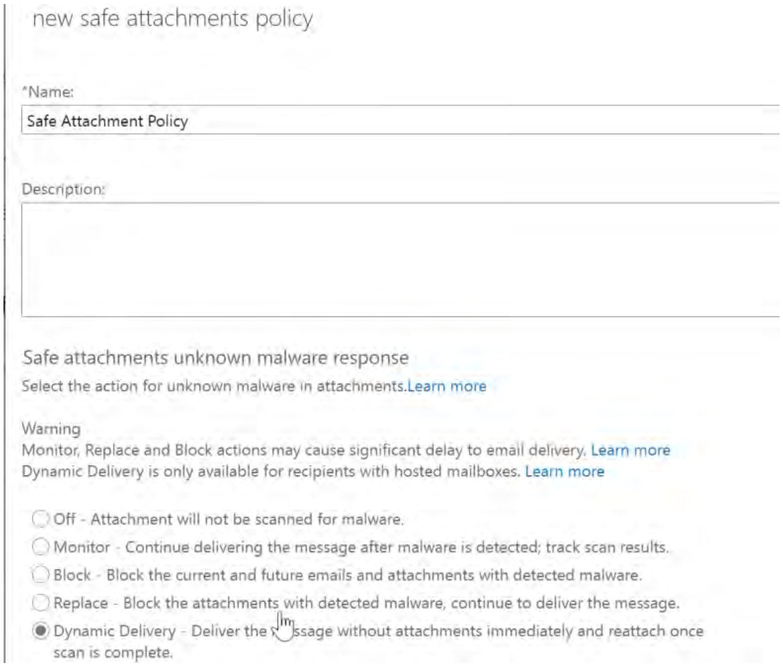
Set up an ATP safe attachments policy for specific users or groups to help prevent people from opening or sharing email attachments tha

Reports for this feature just got better. Check out the new report in the Security and Comp

+

ENABLED	NAME	PRIORITY

4. Add Name, Description, and choose Dynamic Delivery. For more on delivery methods, click here



new safe attachments policy

*Name:

Safe Attachment Policy

Description:

Safe attachments unknown malware response

Select the action for unknown malware in attachments.Learn more

Warning

Monitor, Replace and Block actions may cause significant delay to email delivery. Learn more

Dynamic Delivery is only available for recipients with hosted mailboxes. Learn more

○ Off - Attachment will not be scanned for malware.

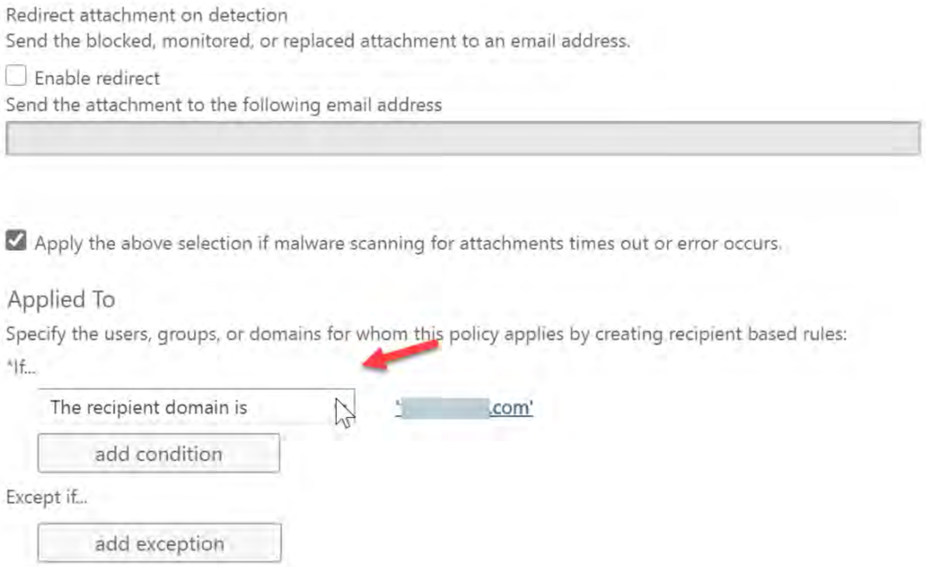
○ Monitor - Continue delivering the message after malware is detected; track scan results.

○ Block - Block the current and future emails and attachments with detected malware.

○ Replace - Block the attachments with detected malware, continue to deliver the message.

● Dynamic Delivery - Deliver the message without attachments immediately and reattach once scan is complete.

5. Add the Recipient Domain Is selection and choose the main domain in the tenant. Click Save when completed



Redirect attachment on detection

Send the blocked, monitored, or replaced attachment to an email address.

□ Enable redirect

Send the attachment to the following email address

☑ Apply the above selection if malware scanning for attachments times out or error occurs.

Applied To

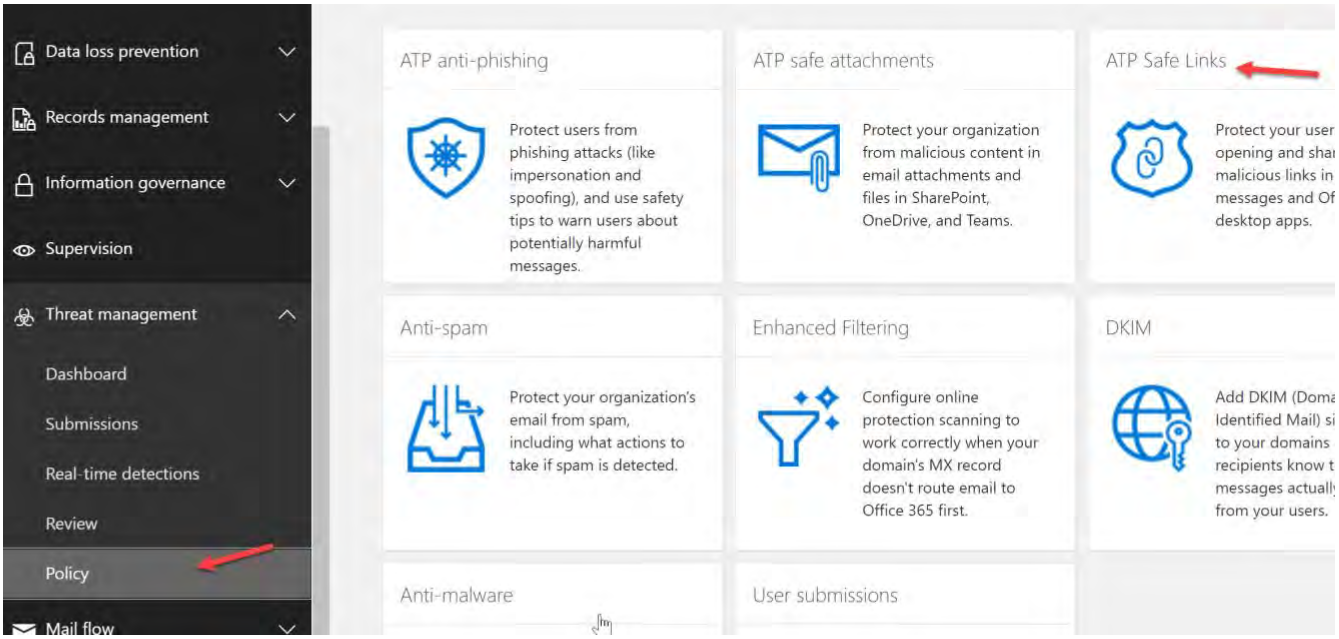
Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

The recipient domain is '[redacted].com'

Except if...

6. For Safe Links, go back to Threat Management>Policy>Safe Links



ATP anti-phishing

Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.

ATP safe attachments

Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

ATP Safe Links

Protect your user opening and shar malicious links in messages and Of desktop apps.

Anti-spam

Protect your organization's email from spam, including what actions to take if spam is detected.

Enhanced Filtering

Configure online protection scanning to work correctly when your domain's MX record doesn't route email to Office 365 first.

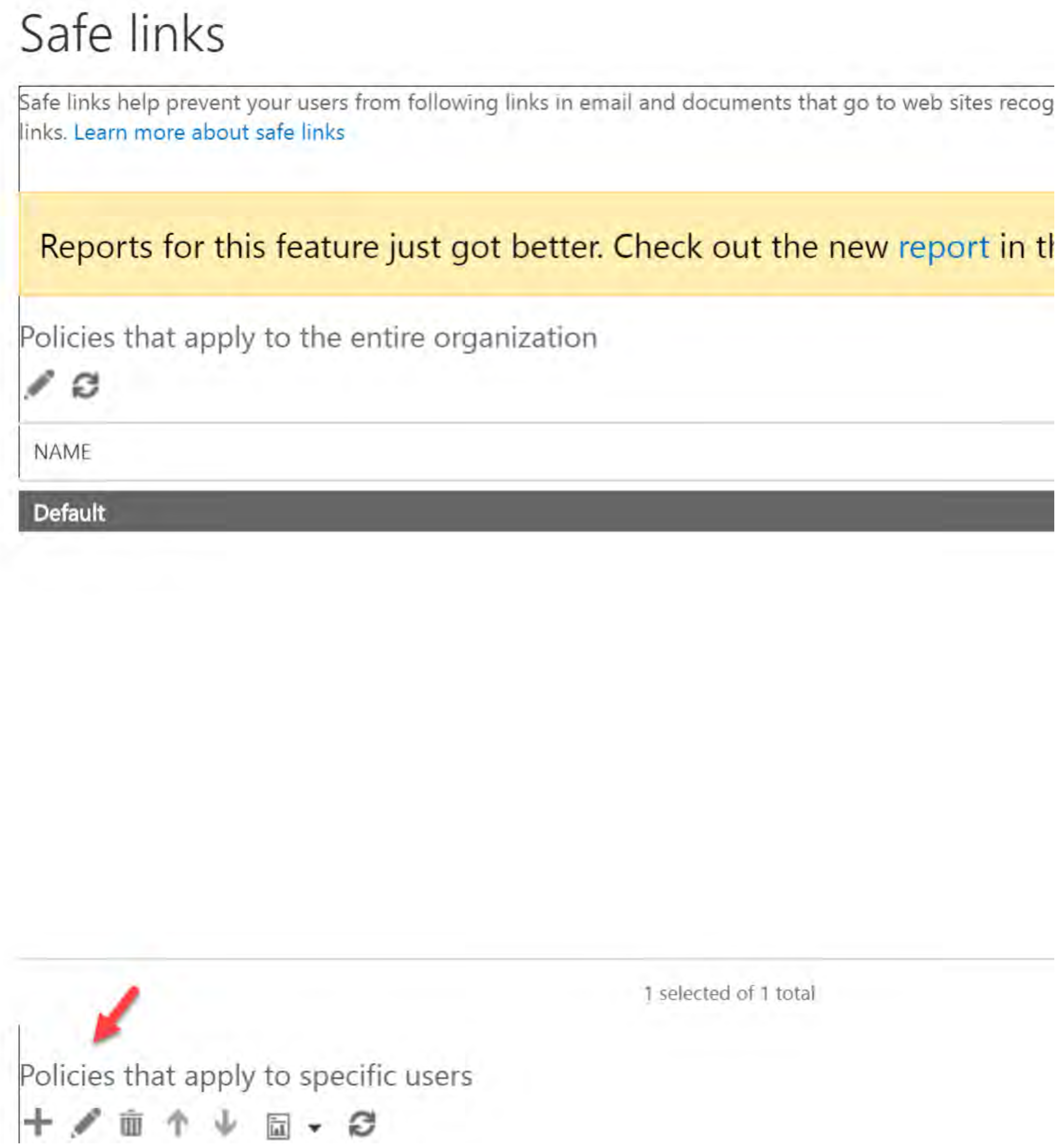
DKIM

Add DKIM (Doma Identified Mail) si to your domains recipients know t messages actuall from your users.

Anti-malware

User submissions

7. Scroll down to Policies that apply to specific users and click the + icon



Safe links

Safe links help prevent your users from following links in email and documents that go to web sites recog
links. Learn more about safe links

Reports for this feature just got better. Check out the new report in tl

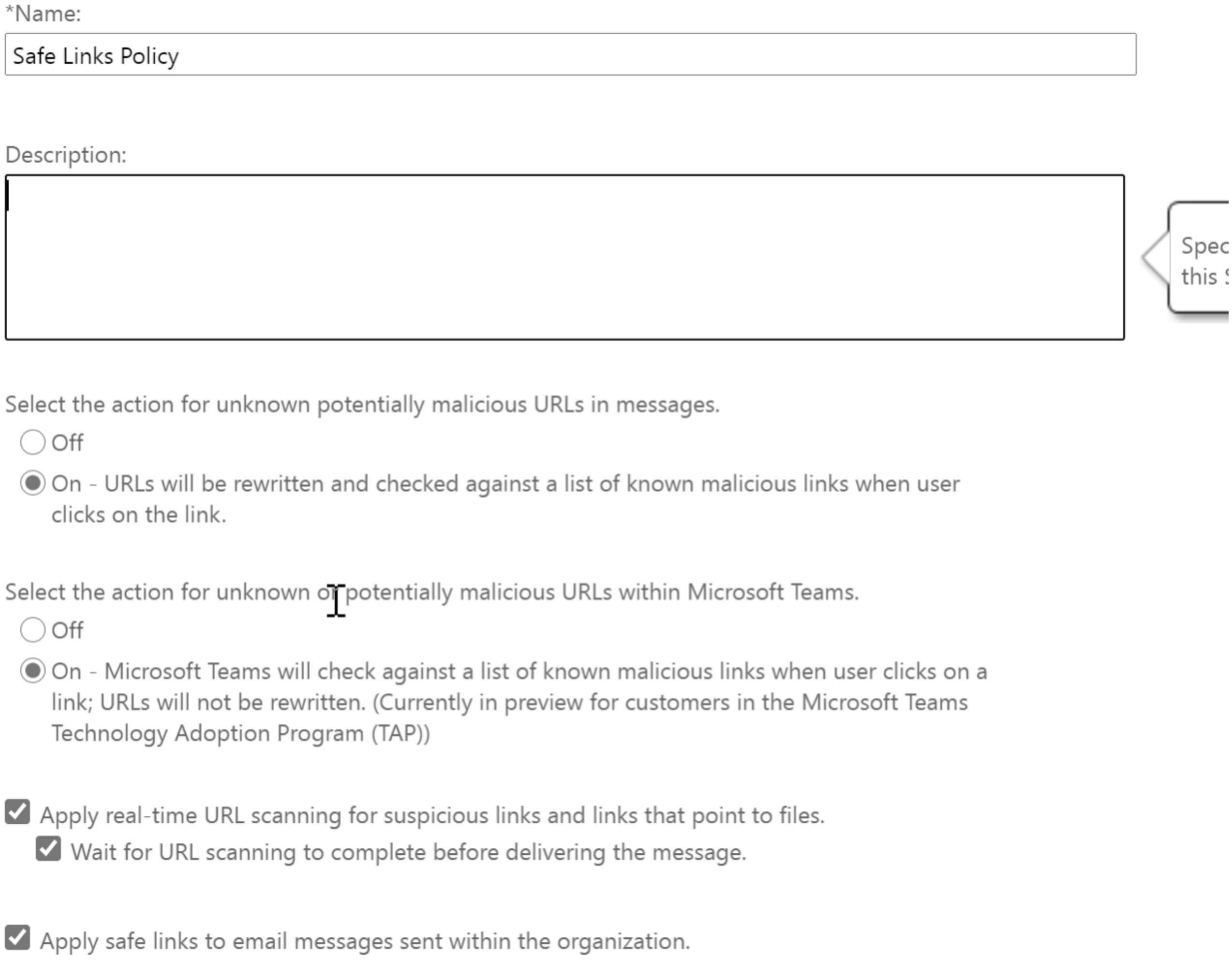
Policies that apply to the entire organization

NAME
Default

1 selected of 1 total

Policies that apply to specific users

8. Add a Name, Description, and turn on the necessary settings displayed below:



*Name:

Safe Links Policy

Description:

Select the action for unknown potentially malicious URLs in messages.

○ Off

● On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.

Select the action for unknown or potentially malicious URLs within Microsoft Teams.

○ Off

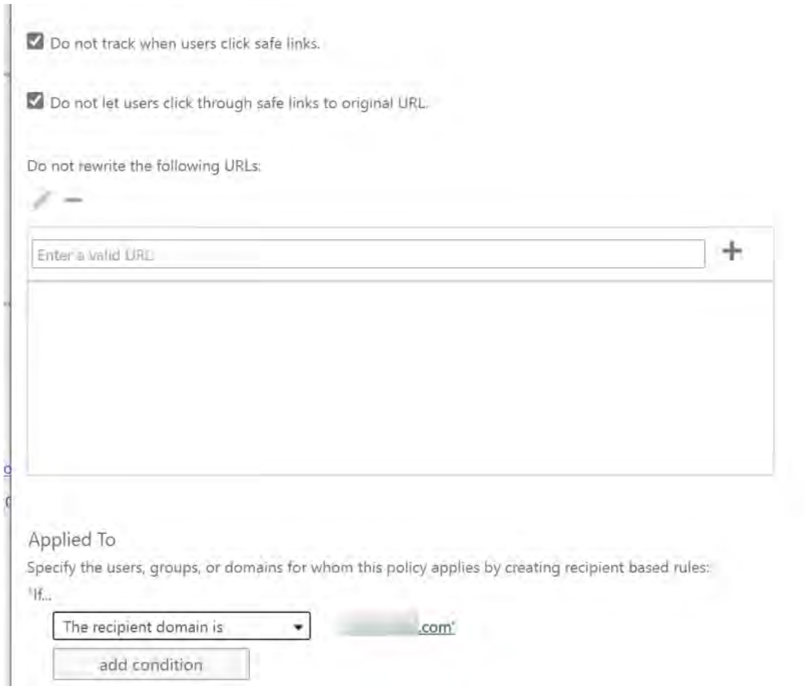
● On - Microsoft Teams will check against a list of known malicious links when user clicks on a link; URLs will not be rewritten. (Currently in preview for customers in the Microsoft Teams Technology Adoption Program (TAP))

☑ Apply real-time URL scanning for suspicious links and links that point to files.

☑ Wait for URL scanning to complete before delivering the message.

☑ Apply safe links to email messages sent within the organization.

9. You can choose to whitelist certain URLs. Like the safe attachments policy, apply to all users in the tenant by the domain name



☑ Do not track when users click safe links.

☑ Do not let users click through safe links to original URL.

Do not rewrite the following URLs:

Enter a valid URL

Applied To

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

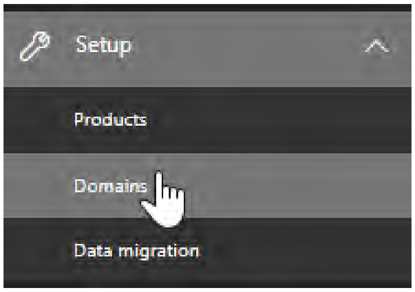
The recipient domain is '[redacted].com'

OVERVIEW & USER GUIDE

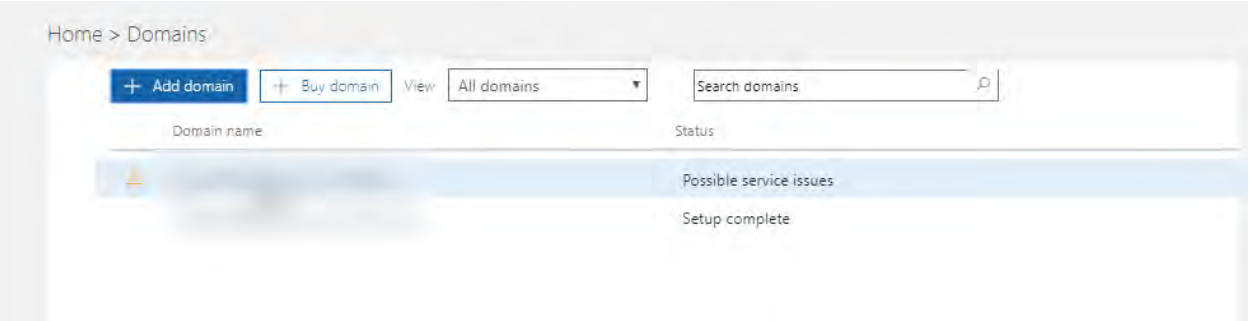
Add SPF, DKIM, and DMARC

- Do you have SPF records/DKIM records/DMARC in place?
- SPF validates the origin of email messages by verifying the IP address of the sender against the alleged owner of the sending domain which helps prevent spoofing
- DKIM lets you attach a digital signature to email messages in the message header of emails you send. Email systems that receive email from your domain use this digital signature to determine if incoming email that they receive is legitimate.
- DMARC helps receiving mail systems determine what to do with messages that fail SPF or DKIM checks and provides another level of trust for your email partners.

1. Go to Admin Center>Setup>Domains

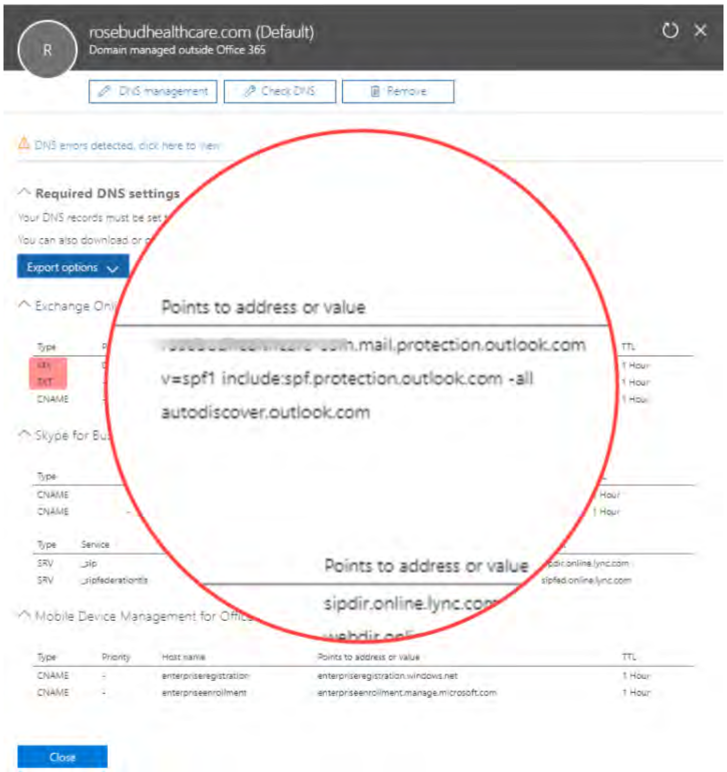


2. Click on the domain you want to add records to



Domain name	Status
	Possible service issues
	Setup complete

3. Take note of the MX and TXT record listed under the Exchange Online



rosebudhealthcare.com (Default)
Domain managed outside Office 365

DNS errors detected, click here to view

Required DNS settings

Your DNS records must be set

You can also download or

Exchange Onl

Points to address or value

[redacted].mail.protection.outlook.com

v=spf1 include:spf.protection.outlook.com -all

autodiscover.outlook.com

Type		TTL
MX		1 Hour
TXT		1 Hour
CNAME		1 Hour

Skype for Bu

Type		TTL
CNAME		Hour
CNAME	-	1 Hour

Type	Service	Points to address or value
SRV	_sip	sipdir.online.lync.com
SRV	_sipfederationtls	sipfed.online.lync.com

Points to address or value

sipdir.online.lync.com

Mobile Device Management for Office

Type	Priority	Host name	Points to address or value	TTL
CNAME	-	enterpriseregistration	enterpriseregistration.windows.net	1 Hour
CNAME	-	enterpriseenrollment	enterpriseenrollment.manage.microsoft.com	1 Hour

4. Add the TXT record of v=spf1 include:spf.protection.outlook.com -all to your DNS settings for our SPF record
5. For our DKIM records we need to publish two CNAME records in DNS

Use the following format for the CNAME Record:

```
Host name:                  selector1._domainkey.<domain>
Points to address or value: selector1-<domainGUID>._domainkey.<initialDomain>
TTL:                        3600

Host name:                  selector2._domainkey.<domain>
Points to address or value: selector2-<domainGUID>._domainkey.<initialDomain>
TTL:                        3600
```

Where:

<domain> = our primary domain

<domainGUID> = The prefix of our MX record (ex. domain-com.mail.protection.outlook.com)

<initialDomain> = domain.onmicrosoft.com

Example: DOMAIN = pax8.com

CNAME Record #1:

Host Name: selector1._domainkey.pax8.com

Points to address or value: selector1-pax8-com._domainkey.pax8.onmicrosoft.com

TTL: 3600

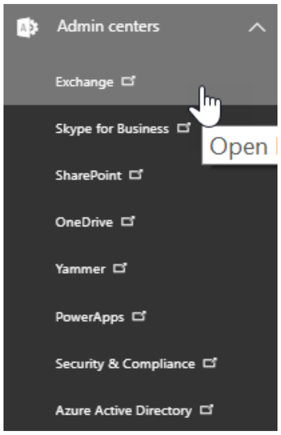
CNAME Record #2:

Host Name: selector2._domainkey.pax8.com

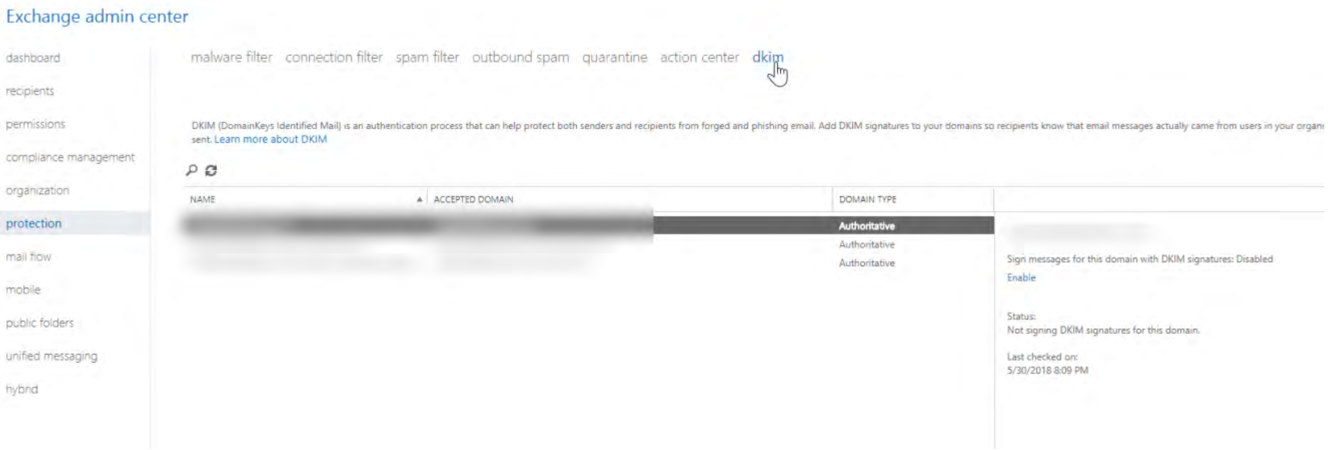
Points to address or value: selector2-pax8-com._domainkey.pax8.onmicrosoft.com

TTL: 3600

6. After publishing the records, go to Admin Centers>Exchange



7. Go to Protection>DKIM



DKIM (DomainKeys Identified Mail) is an authentication process that can help protect both senders and recipients from forged and phishing email. Add DKIM signatures to your domains so recipients know that email messages actually came from users in your organ
sent. Learn more about DKIM

NAME	ACCEPTED DOMAIN	DOMAIN TYPE
[redacted]	[redacted]	Authoritative
[redacted]	[redacted]	Authoritative
[redacted]	[redacted]	Authoritative

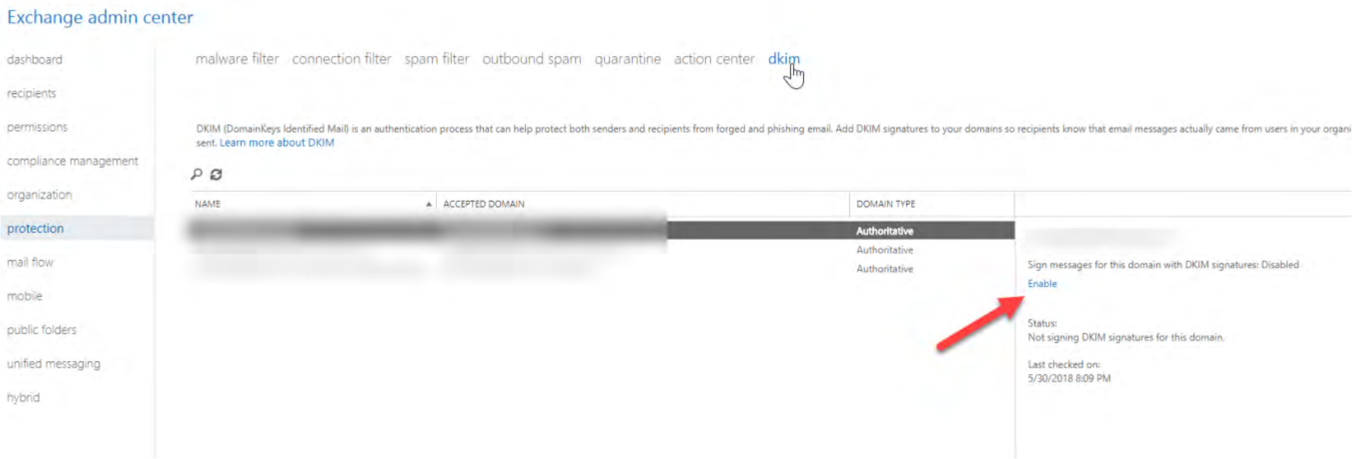
[redacted]

Sign messages for this domain with DKIM signatures: Disabled
Enable

Status:
Not signing DKIM signatures for this domain.

Last checked on:
5/30/2018 8:09 PM

8. Select the Domain for which you want to enable DKIM and click Enable on the right-hand side



DKIM (DomainKeys Identified Mail) is an authentication process that can help protect both senders and recipients from forged and phishing email. Add DKIM signatures to your domains so recipients know that email messages actually came from users in your organi sent. Learn more about DKIM

NAME	ACCEPTED DOMAIN	DOMAIN TYPE
[redacted]	[redacted]	Authoritative
[redacted]	[redacted]	Authoritative
		Authoritative

[redacted]

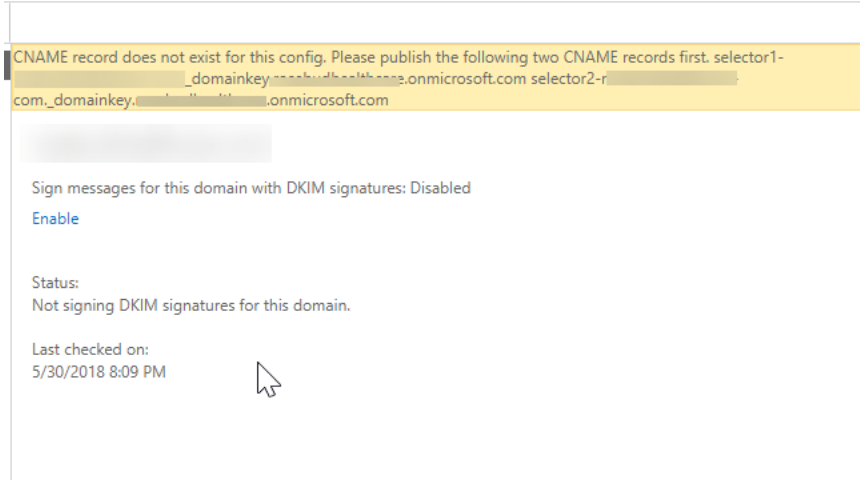
Sign messages for this domain with DKIM signatures: Disabled

Enable

Status:
Not signing DKIM signatures for this domain.

Last checked on:
5/30/2018 8:09 PM

9. If you have improperly added the CNAME records you will get an error message



CNAME record does not exist for this config. Please publish the following two CNAME records first. selector1-[redacted]_domainkey[redacted].onmicrosoft.com selector2-r[redacted] com._domainkey.[redacted].onmicrosoft.com

[redacted]

Sign messages for this domain with DKIM signatures: Disabled

Enable

Status:
Not signing DKIM signatures for this domain.

Last checked on:
5/30/2018 8:09 PM

10. With the SPF and DKIM records in place, we can now set up DMARC. The format for the TXT record we want to add is as follows:

```
_dmarc.domain TTL IN TXT "v=DMARC1; pct=100; p=policy
```

Where:

<domain> = domain we want to protect

<TTL> = 3600

<pct=100> = indicates that this rule should be used for 100% of email

<policy> = specifies what policy you want the receiving server to follow if DMARC Fails.

NOTE You can set <policy> to none, quarantine, or reject

Example:

1. _dmarc.pax8.com 3600 IN TXT "v=DMARC1; p=none"
2. _dmarc.pax8.com 3600 IN TXT "v=DMARC1; p=quarantine"
3. _dmarc.pax8.com 3600 IN TXT "v=DMARC1; p=reject"

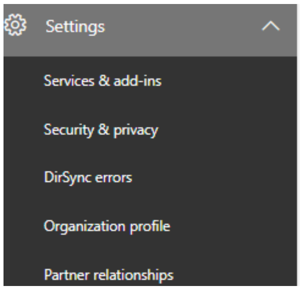
Do not Allow Calendar Details Sharing

You should not allow your users to share calendar details with external users. This feature allows your users to share the full details of their calendars with external users. Attackers will very commonly spend time learning about your organization (performing reconnaissance) before launching an attack. Publicly available calendars can help attackers understand organizational relationships, and determine when specific users may be more vulnerable to an attack, such as when they are traveling.

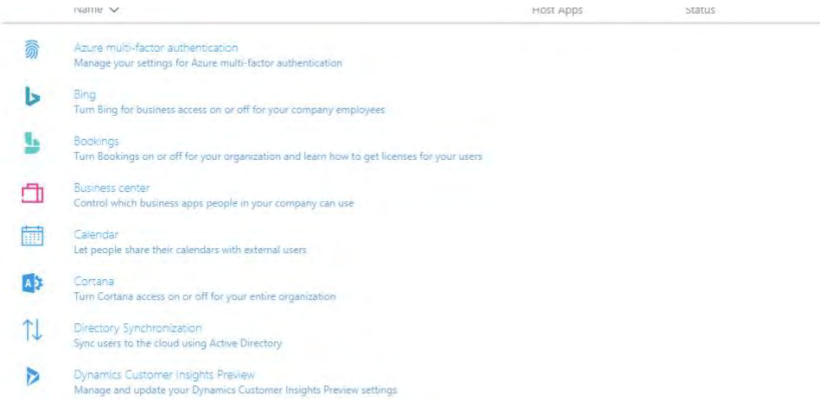
Compliance Controls

- FedRAMP Moderate; Control AC-2(9)
- NIST 800-53; Control AC-2(9)

1. Go to Settings>Services & Add-ins

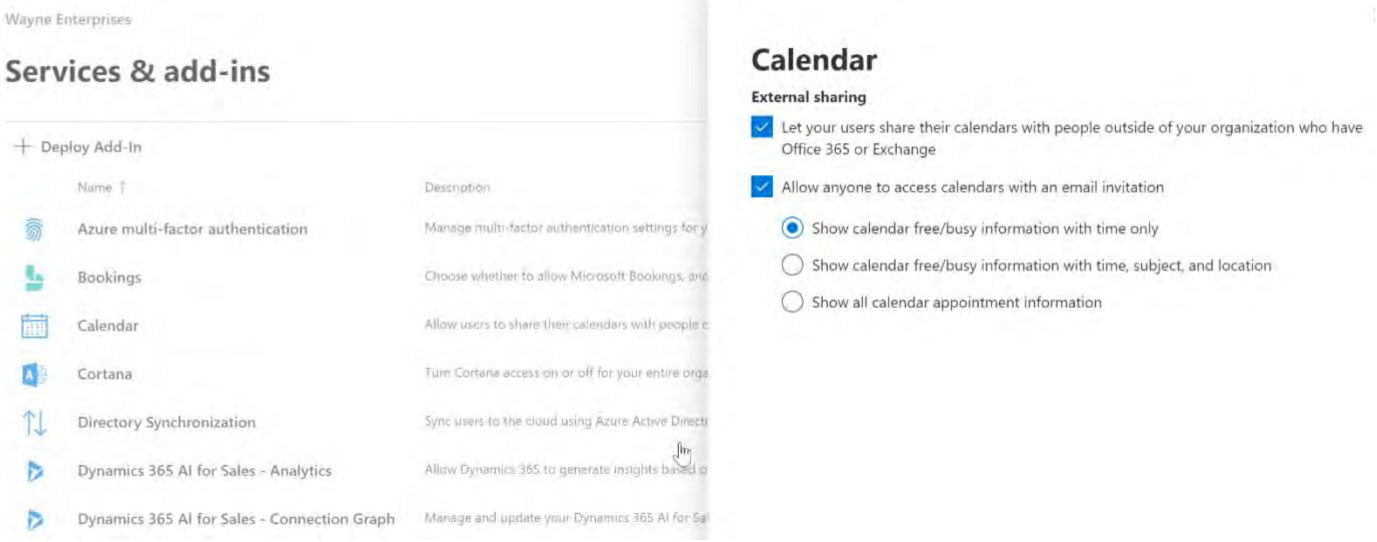


2. Click on Calendar



Name	Host Apps	Status
Azure multi-factor authentication Manage your settings for Azure multi-factor authentication		
Bing Turn Bing for business access on or off for your company employees		
Bookings Turn Bookings on or off for your organization and learn how to get licenses for your users		
Business center Control which business apps people in your company can use		
Calendar Let people share their calendars with external users		
Cortana Turn Cortana access on or off for your entire organization		
Directory Synchronization Sync users to the cloud using Active Directory		
Dynamics Customer Insights Preview Manage and update your Dynamics Customer Insights Preview settings		

3. Change the settings to "Calendar free/busy information with time only"



Wayne Enterprises

Services & add-ins

Name ↑	Description
Azure multi-factor authentication	Manage multi-factor authentication settings for y
Bookings	Choose whether to allow Microsoft Bookings, and
Calendar	Allow users to share their calendars with people c
Cortana	Turn Cortana access on or off for your entire orga
Directory Synchronization	Sync users to the cloud using Azure Active Directo
Dynamics 365 AI for Sales - Analytics	Allow Dynamics 365 to generate insights based o
Dynamics 365 AI for Sales - Connection Graph	Manage and update your Dynamics 365 AI for Sa

Calendar

External sharing

☑ Let your users share their calendars with people outside of your organization who have Office 365 or Exchange

☑ Allow anyone to access calendars with an email invitation

● Show calendar free/busy information with time only

○ Show calendar free/busy information with time, subject, and location

○ Show all calendar appointment information

PowerShell

1. Enable this setting on one tenant via PowerShell

[PowerShell Script]

2. Enable this setting in all tenants via Partner Center credentials

[PowerShell Script]

OVERVIEW & USER GUIDE

AUDITING AND REPORTING

Enable Audit Log Search

You should enable audit data recording for your Microsoft 365 or Office 365 service to ensure that you have a record of every user and administrator's interaction with the service, including Azure AD, Exchange Online, and SharePoint Online/OneDrive for Business. This data will make it possible to investigate and scope a security breach, should it ever occur. You (or another admin) must turn on audit logging before you can start searching the audit log.

Compliance Controls:

- CSA CCM301; Control IAM-01
- FedRAMP Moderate; Control AU-9
- GDPR; Control 6.9.4
- ISO 27001:2013; Control A.12.4.2
- ISO 27018:2014_ID; Control C.12.4.2, Part 1
- NIST 800-171; Control 3.3.8
- NIST 800-53; Control AU-9
- NIST CSF; Control RS.AN-1

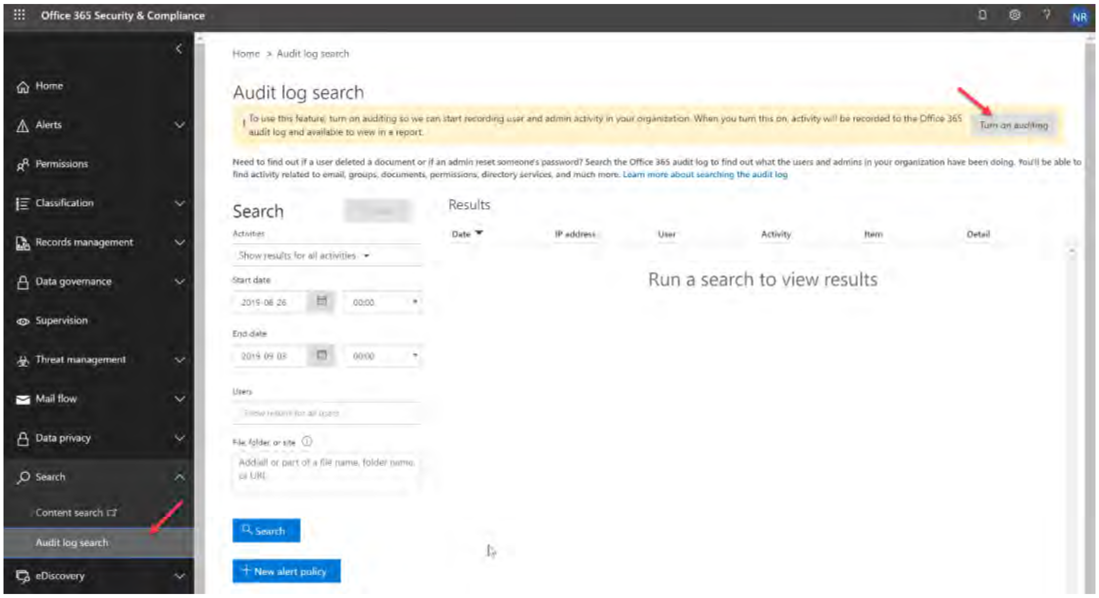
Questions to Ask:

1. How often do I want to get reports on audit log data? (Recommended bi-weekly)
2. Is there a certain environment I need to more closely monitor? (Exchange, SharePoint, OneDrive, etc.)

How to Turn the Audit Log On

How to Search the Audit Log

1. Go to Admin Centers>Security and Compliance Center>Search>Audit Log search



Audit log search

! To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report.

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Activities: Show results for all activities

Start date: 2019-08-26 00:00

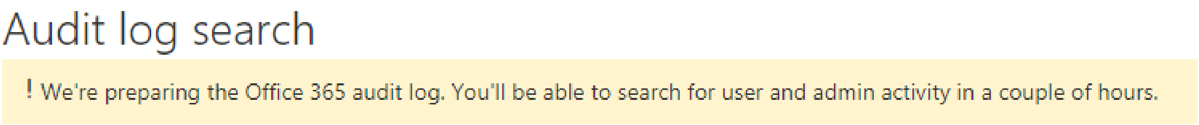
End date: 2019-09-03 00:00

Users: Show results for all users

File, folder, or site: Add all or part of a file name, folder name, or URL

Run a search to view results

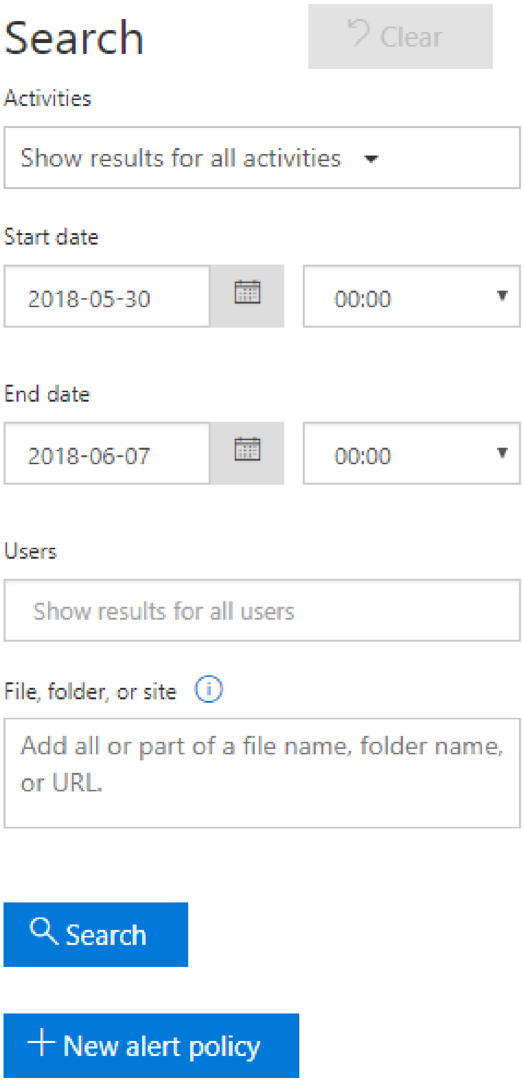
After you turn on Auditing, you will see the following:



Audit log search

! We're preparing the Office 365 audit log. You'll be able to search for user and admin activity in a couple of hours.

2. You can create a custom search based off:
   a. Activity
   b. Date Range
   c. Users
   d. File/Folder/Site



Search

Activities

Show results for all activities

Start date

2018-05-30 00:00

End date

2018-06-07 00:00

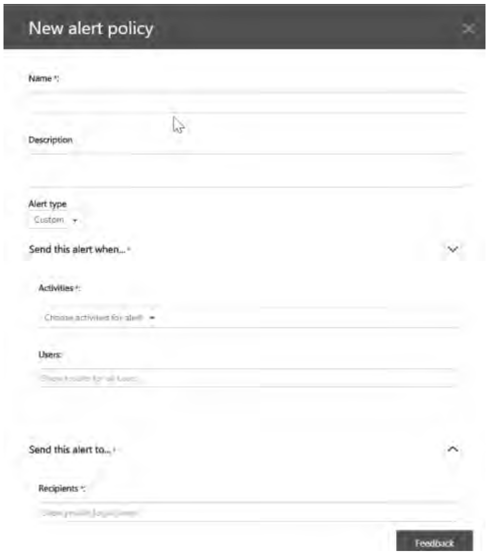
Users

Show results for all users

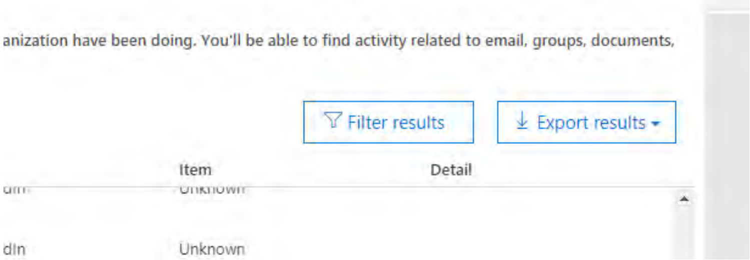
File, folder, or site

Add all or part of a file name, folder name, or URL.

Create a New Alert Policy based off a certain event



Export Entries CSV


anization have been doing. You'll be able to find activity related to email, groups, documents,

	Item	Detail
dm	Unknown	
dm	Unknown	

PowerShell

1. Turn on Audit log for one tenant

   PowerShell Script

2. Turn on Audit Log for all tenants via Partner Center credentials

   PowerShell Script

3. If want to search the audit log via PowerShell you would use the commands below:

```
$auditlog = Search-UnifiedAuditLog -StartDate 06/01/2019 -EndDate 06/30/2019 -RecordType SharePointFileOperation
```

Where you can customize the start date, end date, and record type. A list of all record types you can search for can be found here:

Click here

From there you could use the following command to export certain properties to a CSV file:

```
$auditlog | Select-Object -Property CreationDate,UserIds,RecordType,AuditData | Export-Csv -Append -Path c:\AuditLogs\PowerShellAuditlog.csv -NoTypeInformation
```

Enable Mailbox Auditing for All Users

By default, all non-owner access is audited, but you must enable auditing on the mailbox for owner access to also be audited. This will allow you to discover illicit access of Exchange Online activity if a user's account has been breached. We will need to run a PowerShell script to enable auditing for all users.

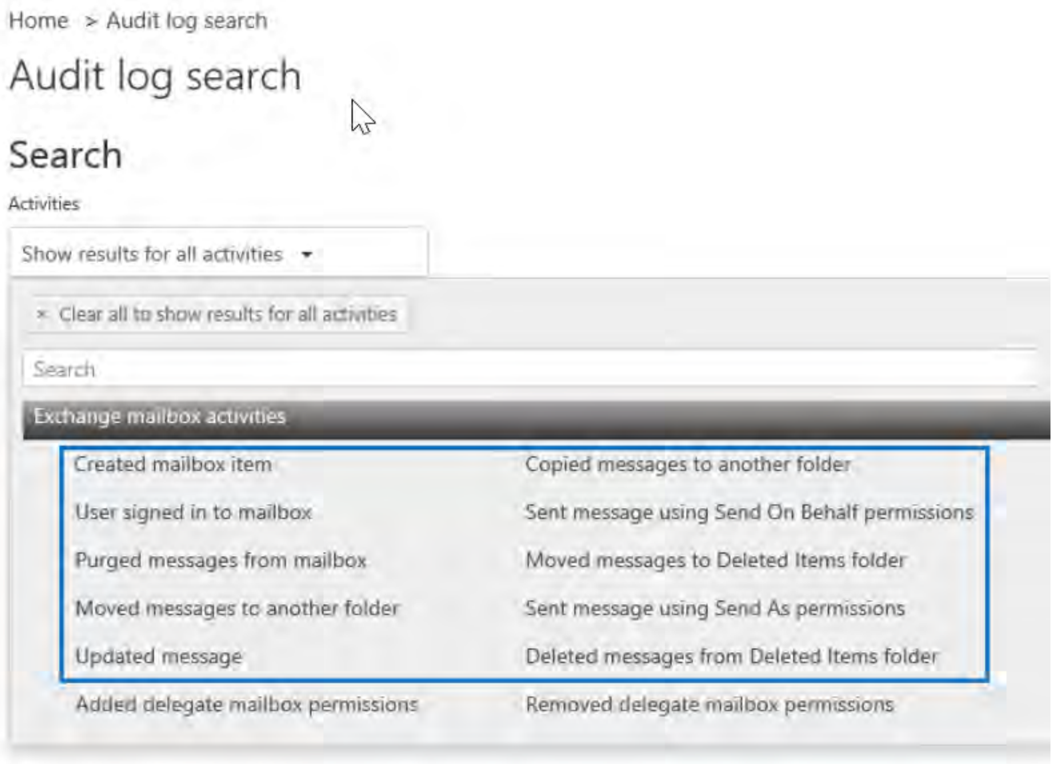
Compliance Controls

- CSA CCM301; Control IAM-01
- FedRAMP Moderate; Control AU-9
- GDPR; Control 6.9.4
- ISO 27001:2013; Control A.12.4.2
- ISO 27018:2014_ID; Control C.12.4.2, Part 1
- NIST 800-171; Control 3.3.8
- NIST 800-53; Control AU-9
- NIST CSF; Control RS.AN-1

1. PowerShell Script to Enable

NOTE Use the audit log to search for mailbox activity that have been logged. You can search for activity for a specific user mailbox.

2. Go to Admin>Security and Compliance Center>Search & Investigation>Audit Log search



Home > Audit log search

Audit log search

Search

Activities

Show results for all activities ▾

× Clear all to show results for all activities

Search

Exchange mailbox activities

Created mailbox item

User signed in to mailbox

Purged messages from mailbox

Moved messages to another folder

Updated message

Added delegate mailbox permissions

Copied messages to another folder

Sent message using Send On Behalf permissions

Moved messages to Deleted Items folder

Sent message using Send As permissions

Deleted messages from Deleted Items folder

Removed delegate mailbox permissions

List of Mailbox Auditing Actions

PowerShell

1. Enable Mailbox Auditing on all customer tenants

   PowerShell Script

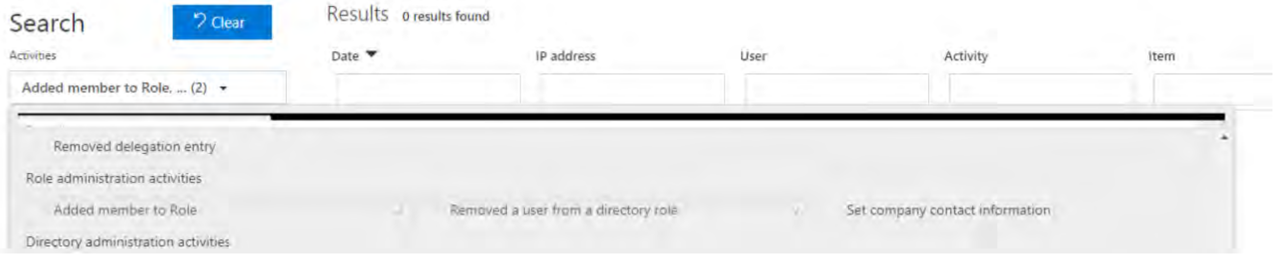
OVERVIEW & USER GUIDE

Review Role Changes Weekly

You should do this because you should watch for illicit role group changes, which could give an attacker elevated privileges to perform more dangerous and impactful things in your tenancy.

1. Go to Admin>Security and Compliance Center>Search & Investigation>Audit Log search

2. Filter the search by going to Role Administration Activities and select "Added Member to Role" and "Removed a user from a Directory Role"



Search

Activities: Added member to Role, ... (2)

Results 0 results found

Date | IP address | User | Activity | Item

Removed delegation entry

Role administration activities

Added member to Role | Removed a user from a directory role | Set company contact information

Directory administration activities

3. Monitor Role Changes in all customer accounts

https://gcits.com/knowledge-base/monitor-office-365-admin-role-changes-in-all-customer-tenants/

Review Mailbox Forwarding Rules Weekly

You should review mailbox forwarding rules to external domains at least every week. There are several ways you can do this, including simply reviewing the list of mail forwarding rules to external domains on all of your mailboxes using a PowerShell script, or by reviewing mail forwarding rule creation activity in the last week from the Audit Log Search. While there are lots of legitimate uses of mail forwarding rules to other locations, it is also a very popular data exfiltration tactic for attackers. You should review them regularly to ensure your users' email is not being exfiltrated. Running the PowerShell script linked below will generate two csv files, "MailboxDelegatePermissions" and "MailForwardingRulesToExternalDomains", in your System32 folder.

Compliance Controls

- GDPR; Control 6.8.2
- ISO 27018:2014; Control A.10.2

PowerShell

1. Monitor on a single tenant

   PowerShell Script

2. Monitor External Mailbox Forwards in all Microsoft 365/Office 365 Customer tenants

   PowerShell Script

OVERVIEW & USER GUIDE

Review the Mailbox Access by Non-Owners Report Bi-Weekly

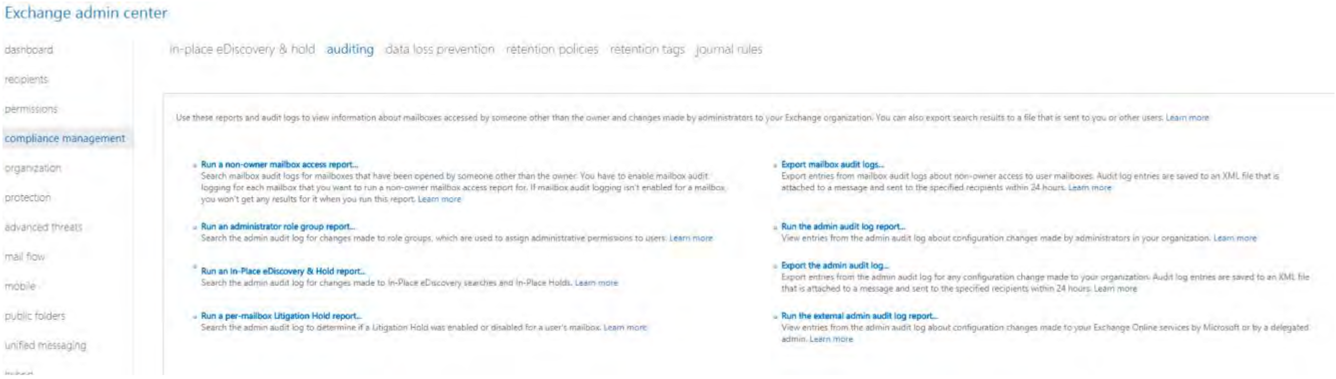
This report shows which mailboxes have been accessed by someone other than the mailbox owner. While there are many legitimate uses of delegate permissions, regularly reviewing that access can help prevent an external attacker from maintaining access for a long time and can help discover malicious insider activity sooner.

Compliance Controls

- FedRAMP Moderate; Control AC-6(9)
- NIST 800-171; Control 3.1.7
- NIST 800-53; Control AC-6(9)

1. In EAC, go to Compliance Management>Auditing

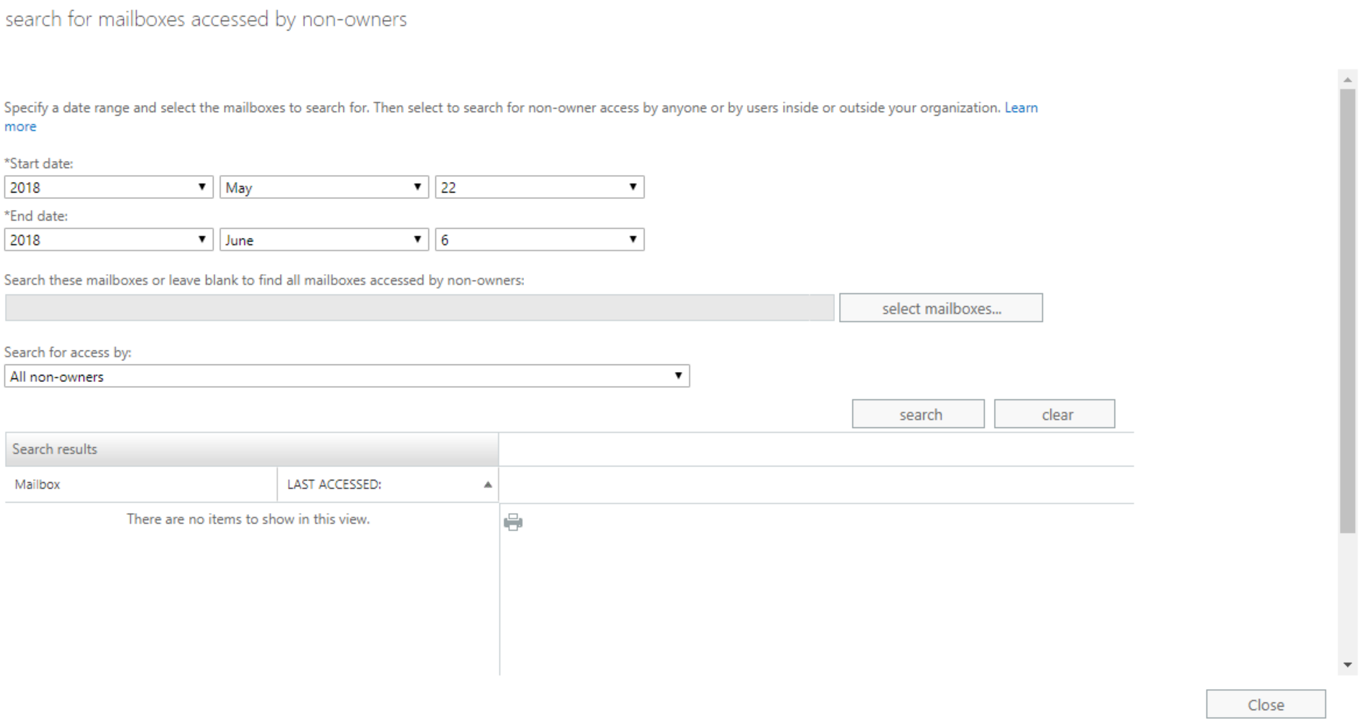
2. Click on "Run a non-owner mailbox access report…"



Use these reports and audit logs to view information about mailboxes accessed by someone other than the owner and changes made by administrators to your Exchange organization. You can also export search results to a file that is sent to you or other users. Learn more

- **Run a non-owner mailbox access report...**
  Search mailbox audit logs for mailboxes that have been opened by someone other than the owner. You have to enable mailbox audit logging for each mailbox that you want to run a non-owner mailbox access report for. If mailbox audit logging isn't enabled for a mailbox, you won't get any results for it when you run this report. Learn more
- **Run an administrator role group report...**
  Search the admin audit log for changes made to role groups, which are used to assign administrative permissions to users. Learn more
- **Run an In-Place eDiscovery & Hold report...**
  Search the admin audit log for changes made to In-Place eDiscovery searches and In-Place Holds. Learn more
- **Run a per-mailbox Litigation Hold report...**
  Search the admin audit log to determine if a Litigation Hold was enabled or disabled for a user's mailbox. Learn more
- **Export mailbox audit logs...**
  Export entries from mailbox audit logs about non-owner access to user mailboxes. Audit log entries are saved to an XML file that is attached to a message and sent to the specified recipients within 24 hours. Learn more
- **Run the admin audit log report...**
  View entries from the admin audit log about configuration changes made by administrators in your organization. Learn more
- **Export the admin audit log...**
  Export entries from the admin audit log for any configuration change made to your organization. Audit log entries are saved to an XML file that is attached to a message and sent to the specified recipients within 24 hours. Learn more
- **Run the external admin audit log report...**
  View entries from the admin audit log about configuration changes made to your Exchange Online services by Microsoft or by a delegated admin. Learn more

3. Specify a data range and run a search



search for mailboxes accessed by non-owners

Specify a date range and select the mailboxes to search for. Then select to search for non-owner access by anyone or by users inside or outside your organization. Learn more

*Start date: 2018 ▾ May ▾ 22 ▾

*End date: 2018 ▾ June ▾ 6 ▾

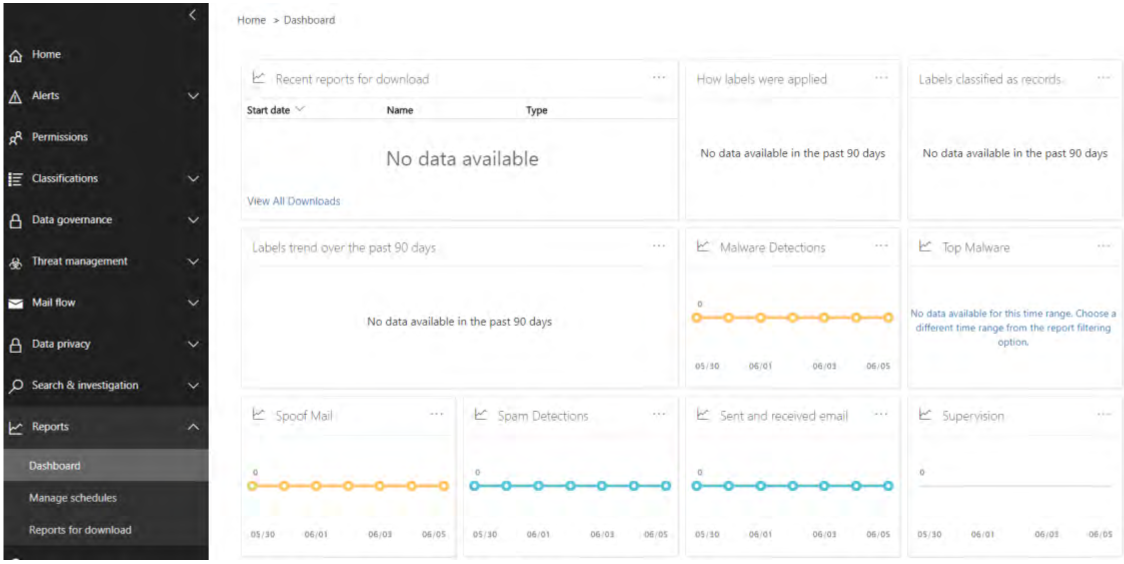
Search these mailboxes or leave blank to find all mailboxes accessed by non-owners:

Search for access by: All non-owners ▾

Review the Malware Detections Report Weekly

This report shows specific instances of Microsoft blocking a malware attachment from reaching your users. While this report isn't strictly actionable, reviewing it will give you a sense of the overall volume of malware being targeted at your users, which may prompt you to adopt more aggressive malware mitigations.

1. Go to Admin>Security and Compliance Center>Reports>Dashboard



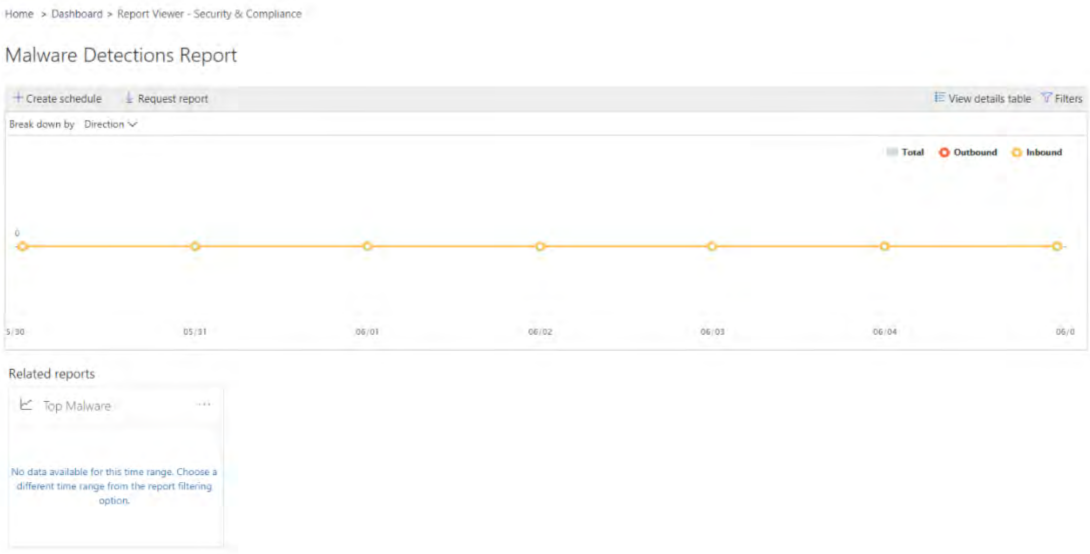
No data available

No data available in the past 90 days

No data available for this time range. Choose a different time range from the report filtering option.

2. Click on Malware Detections

3. View the Detection Report

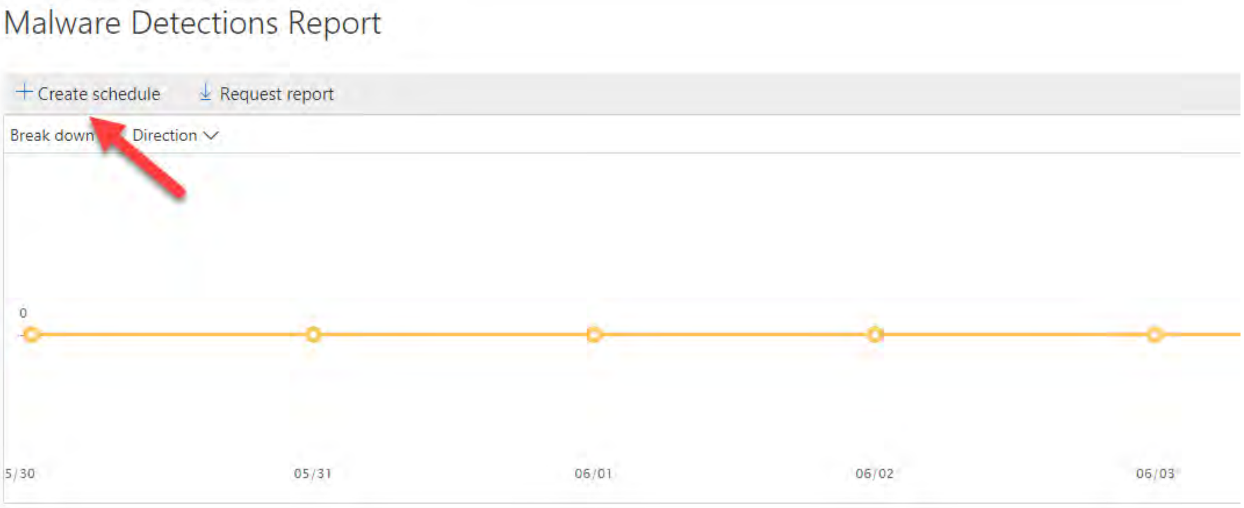


Home > Dashboard > Report Viewer - Security & Compliance

Malware Detections Report

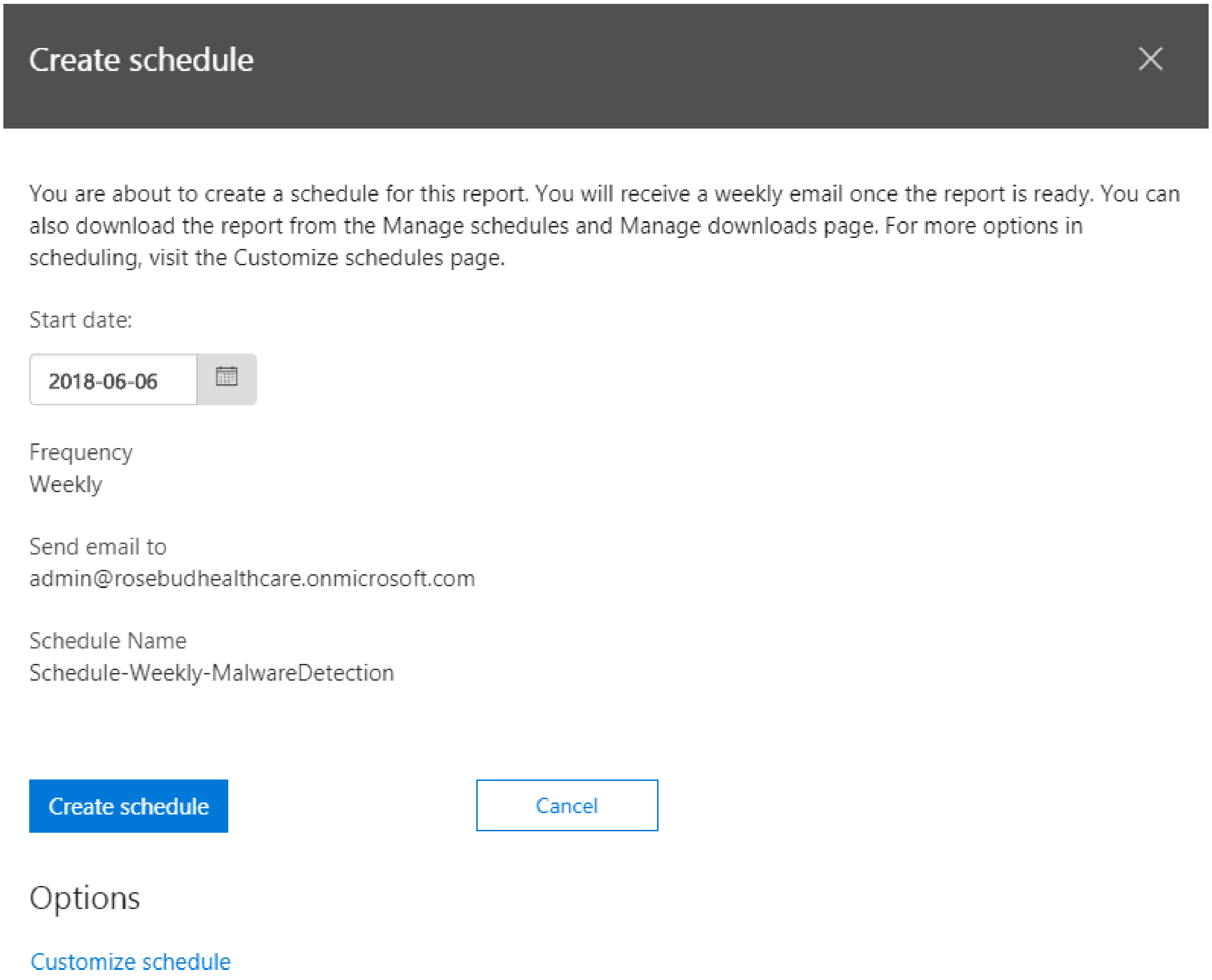
No data available for this time range. Choose a different time range from the report filtering option.

4. Click "+ Create Schedule"



Malware Detections Report

5. Create a weekly report schedule and send it to the appropriate email address



Create schedule

You are about to create a schedule for this report. You will receive a weekly email once the report is ready. You can also download the report from the Manage schedules and Manage downloads page. For more options in scheduling, visit the Customize schedules page.

Start date:

2018-06-06

Frequency
Weekly

Send email to
admin@rosebudhealthcare.onmicrosoft.com

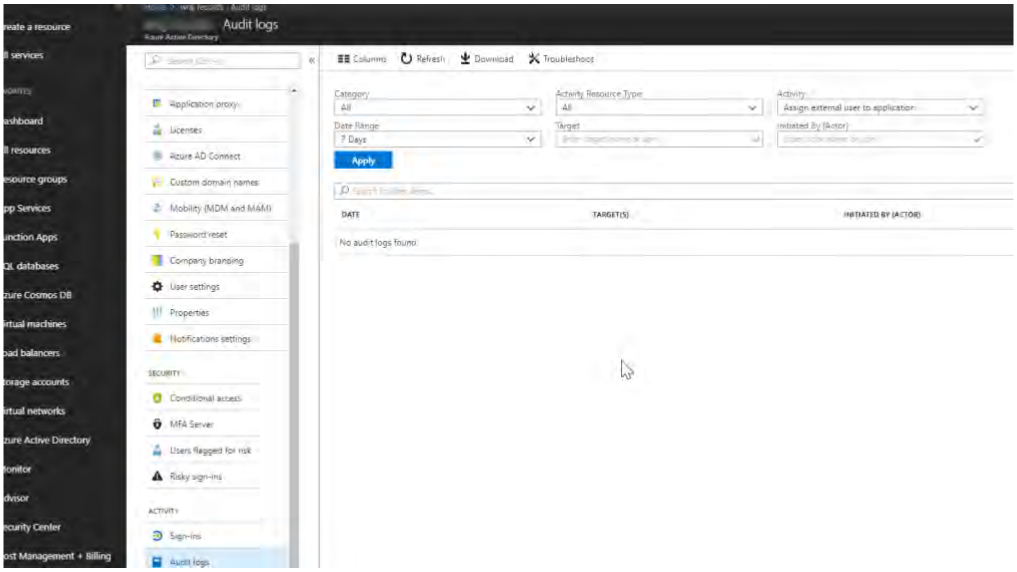
Schedule Name
Schedule-Weekly-MalwareDetection

OVERVIEW & USER GUIDE

Review your Account Provisioning Activity Report Weekly

This report includes a history of attempts to provision accounts to external applications. If you don't usually use a third-party provider to manage accounts, any entry on the list is likely illicit. But, if you do, this is a great way to monitor transaction volumes, and look for new or unusual third-party applications that are managing users.

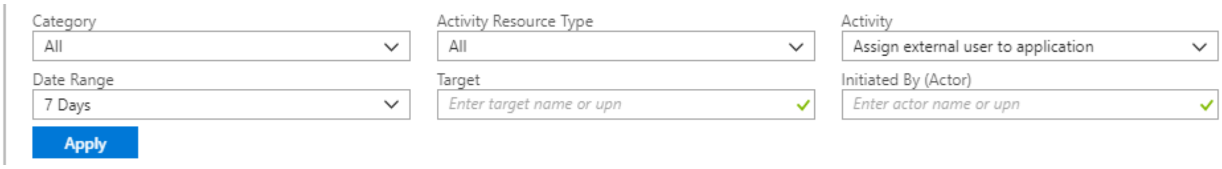
1. Go to Admin Centers>Azure Active Directory>Audit Logs



Category: All
Activity Resource Type: All
Activity: Assign external user to application
Date Range: 7 Days

No audit logs found

2. In the Activity section, search for "external" and select Assign External User to Application



Category	Activity Resource Type	Activity
All	All	Assign external user to application
Date Range	Target	Initiated By (Actor)
7 Days	*Enter target name or upn*	*Enter actor name or upn*

TEAMS

Utilize Private Channels

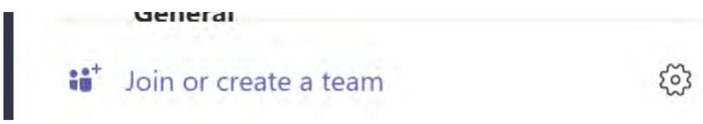
Access controls are a fundamental part of any compliance regulation. Giving access to certain Teams channels where users are collaborating on sensitive topics or sharing critical documents should follow a model of least privilege. Microsoft Teams allows you to create private channels where users can request access to the owners and all other users are prohibited from seeing the content.

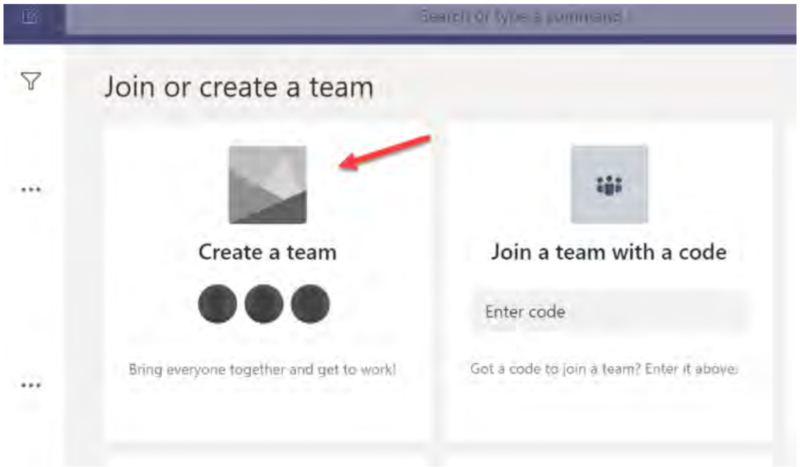
Compliance Controls

- NIST CSF PR.AC-4
- CCS CSC 12, 15
- ISA 62443-2-1:2009 4.3.3.7.3
- ISA 62443-3-3:2013 SR 2.1
- ISO/IEC 27001:2013 A.6.1.2, A.9.1.2,
- A.9.2.3, A.9.4.1, A.9.4.4
- NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC6, AC-16
- HIPAA Security Rule 45 C.F.R. §§
    - 164.308(a)(3), 164.308(a)(4),
    - 164.312(a)(1
    - 164.312(a)(2)(i), 164.312(a)(2)(ii)

OVERVIEW & USER GUIDE

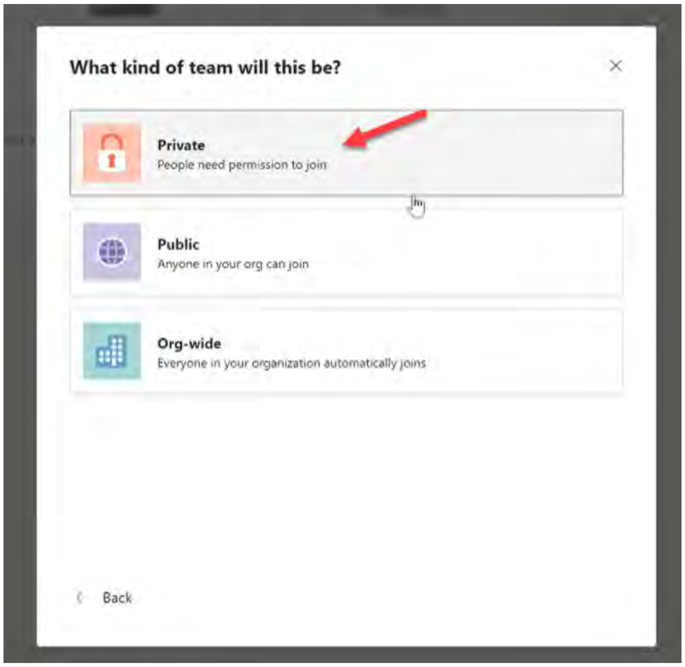
1. In the web or client application, click Teams>Join or create a team>Create a Team




Join or create a team

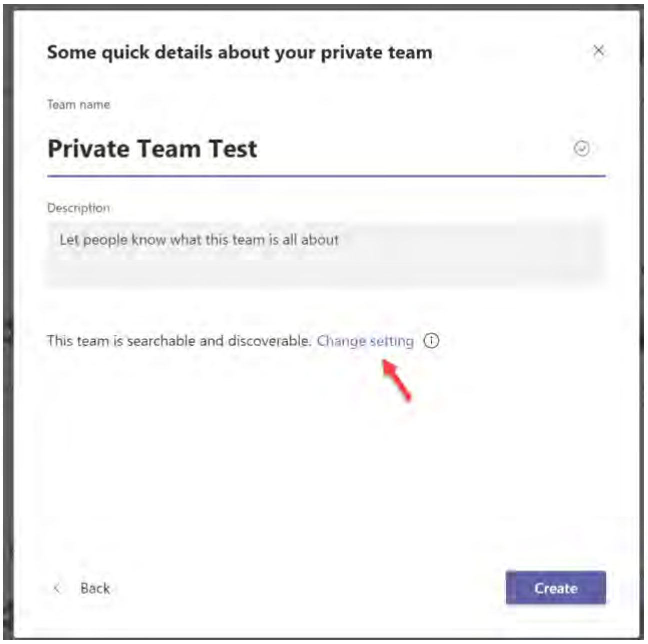
Search or type a command
Create a team
Bring everyone together and get to work!
Join a team with a code
Enter code
Got a code to join a team? Enter it above.

2. Click Private


What kind of team will this be?

Private
People need permission to join
Public
Anyone in your org can join
Org-wide
Everyone in your organization automatically joins
Back

3. Here you can also choose if this team can be discoverable for additional security:



Some quick details about your private team

Team name

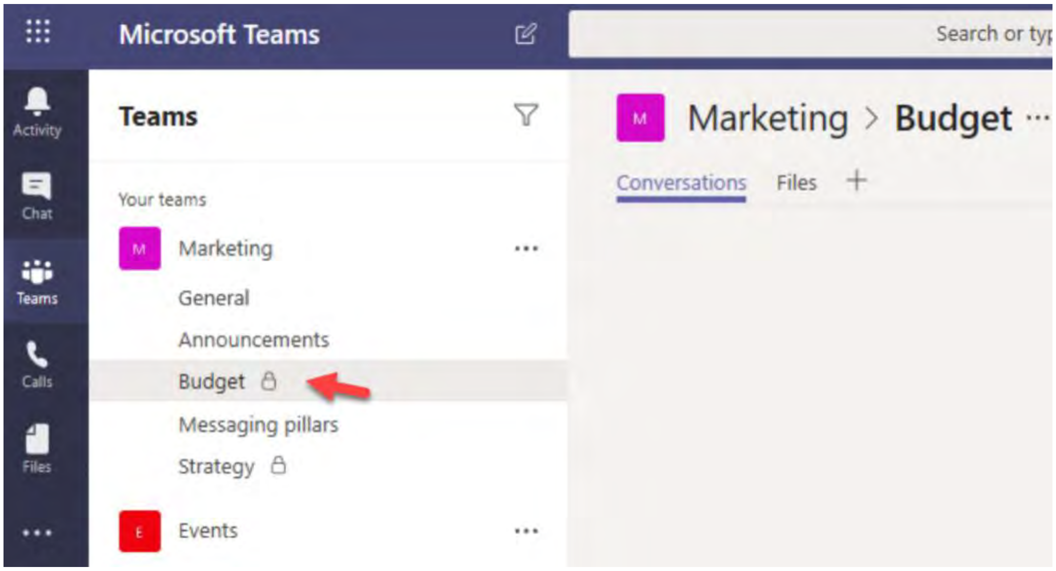
Private Team Test

Description

Let people know what this team is all about

This team is searchable and discoverable. Change setting

4. After the Team is created, you will see a lock icon next to the channel



OVERVIEW & USER GUIDE

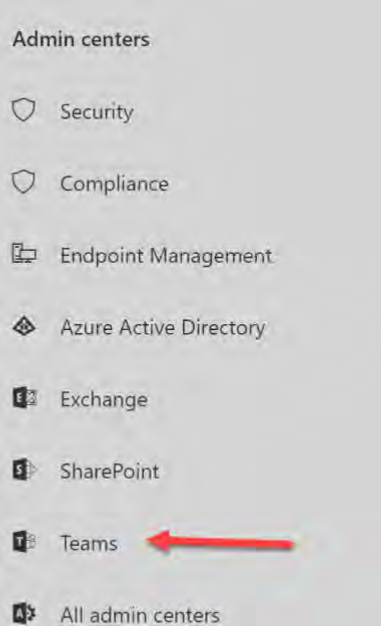
Block External Access

You should not allow your users to communicate with Skype or Teams users outside your organization. While there are legitimate, productivity-improving scenarios for this, it also represents a potential security threat because those external users will be able to interact with your users over Skype for Business or Teams. Attackers may be able to pretend to be someone your user knows and then send malicious links or attachments, resulting in an account breach or leaked information.

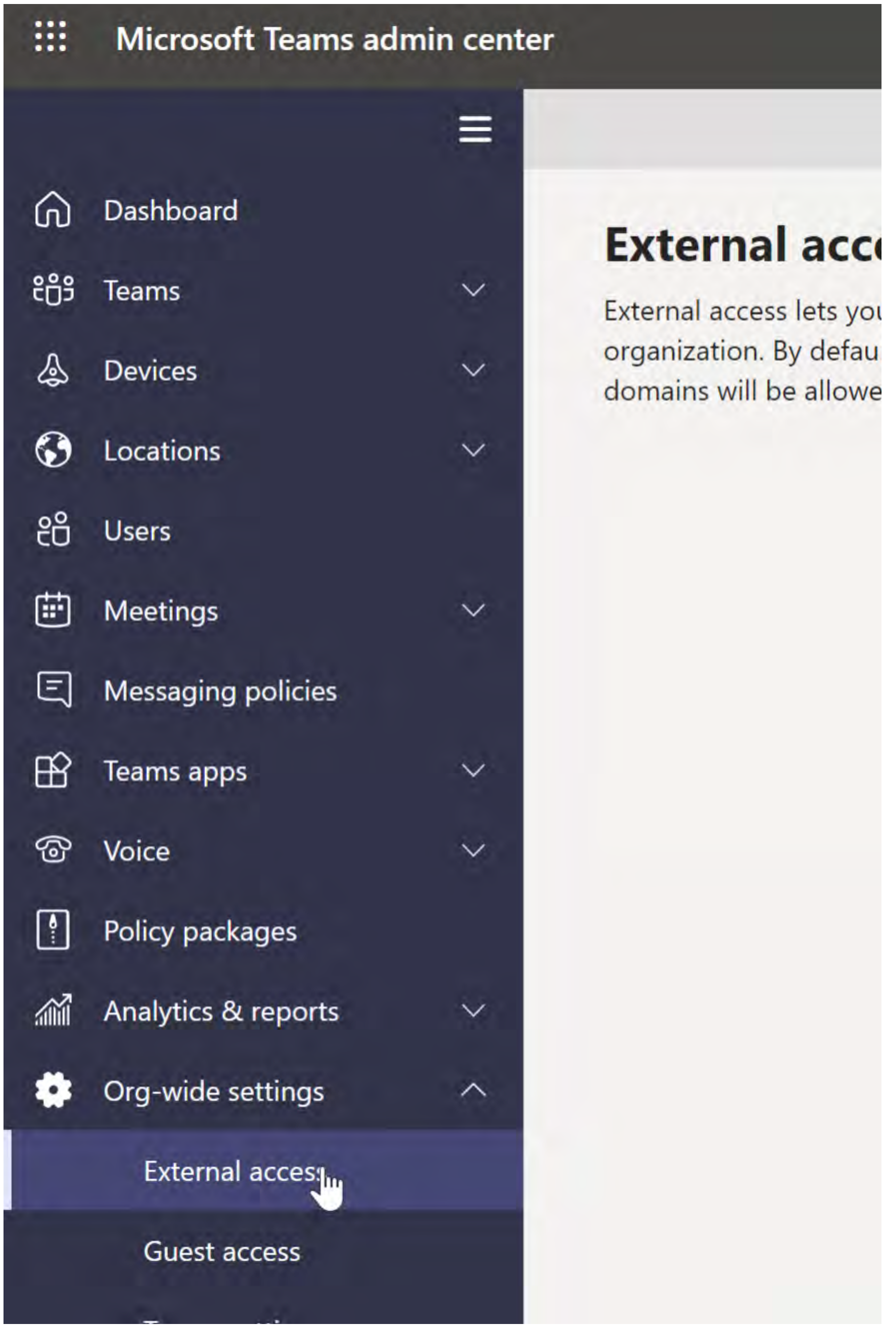
Compliance Controls:

- NIST CSP DE.CM-7
- NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3,
- CM-8, PE-3, PE-6, PE-20, SI-4
- HIPAA Security Rule 45 C.F.R. §§
    - 164.308(a)(1)(ii)(D)
    - 164.312(b)
    - 164.314(b)(2)(i)

1. In the 365 Admin Center>Click All Admin Centers Teams.



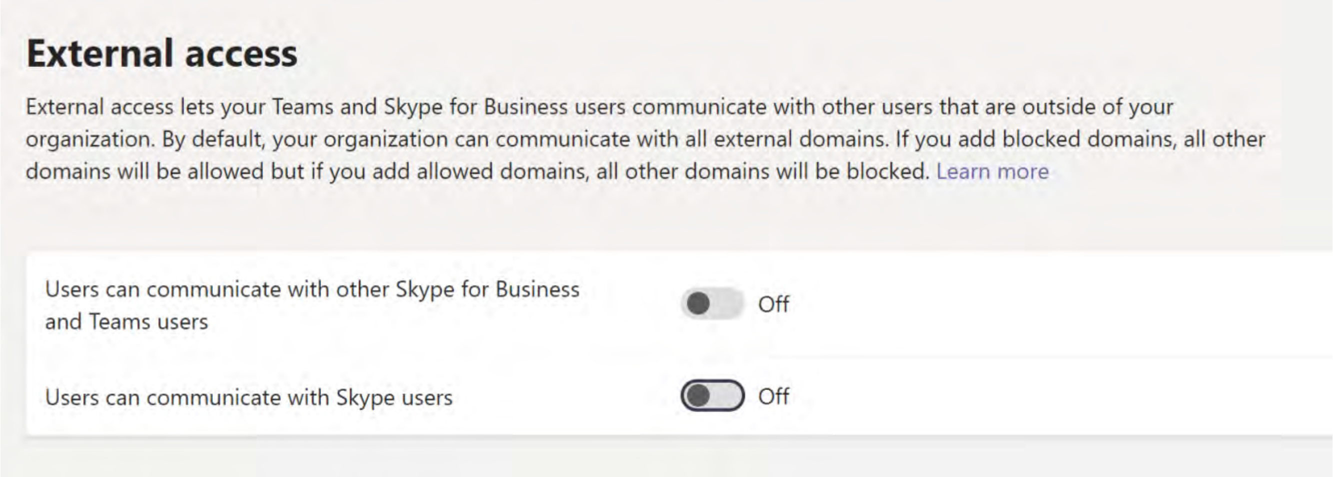
2. Click Org-Wide Settings> External Access



External acc

External access lets you
organization. By defau
domains will be allowe

3. Here, turn the toggles off:



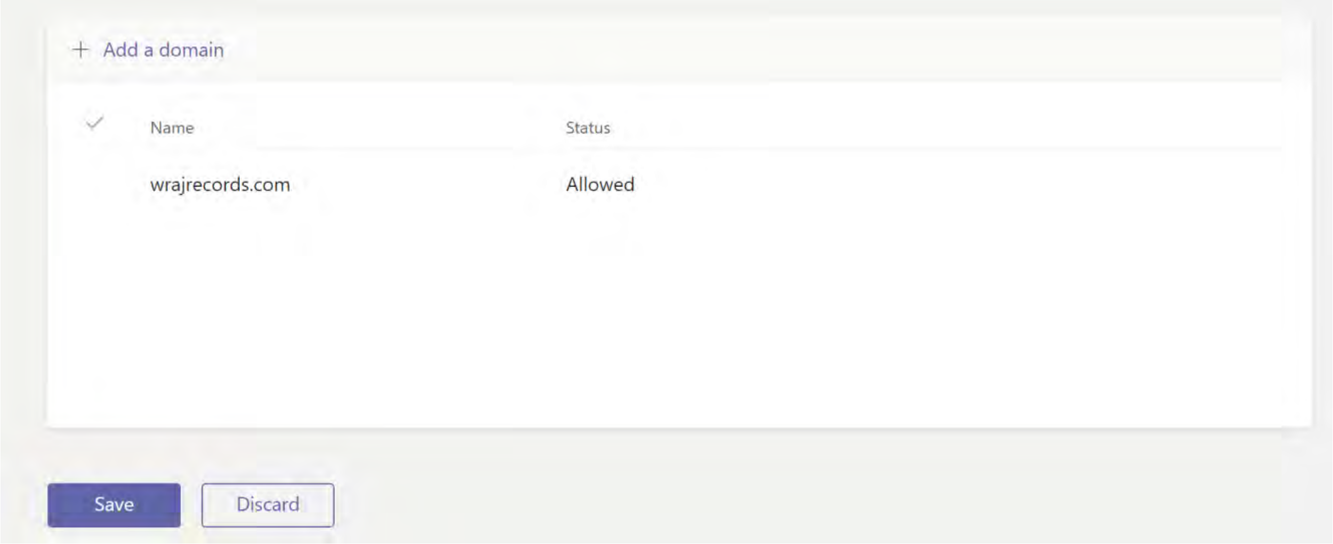
External access

External access lets your Teams and Skype for Business users communicate with other users that are outside of your organization. By default, your organization can communicate with all external domains. If you add blocked domains, all other domains will be allowed but if you add allowed domains, all other domains will be blocked. Learn more

Users can communicate with other Skype for Business and Teams users: Off

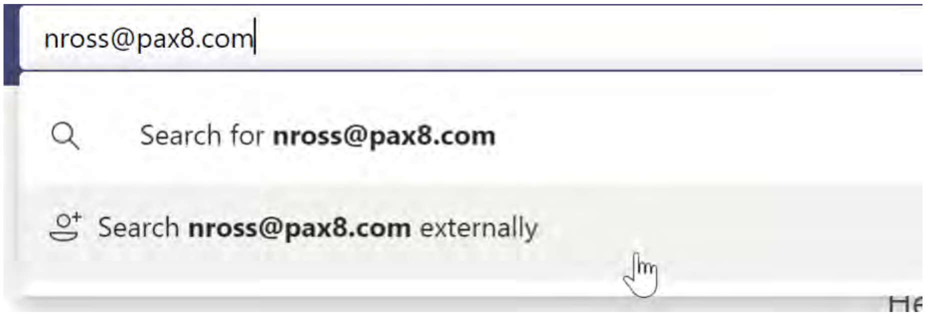
Users can communicate with Skype users: Off

4. You can whitelist certain domains. This allows users to discover external users part of this domain and collaborate with them. This allows you to control the domains that users can collaborate with. Ensure that you have a proper, communicated method of how users can make request to collaborate with external organizations



Name	Status
wrajrecords.com	Allowed

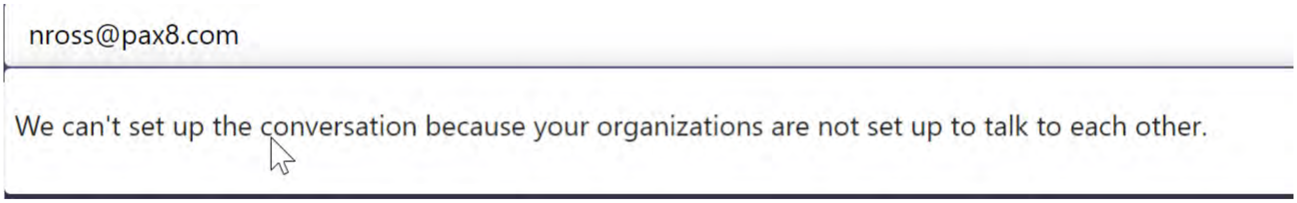
5. Users who search for external users in teams will see the following:



nross@pax8.com

Search for **nross@pax8.com**
Search **nross@pax8.com** externally

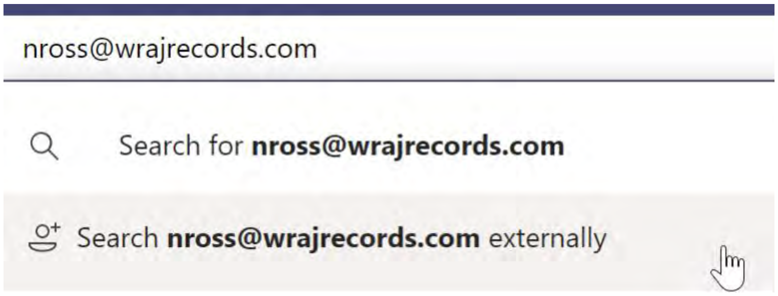
6. If they are not whitelisted, they will get the following when trying to search externally:



nross@pax8.com

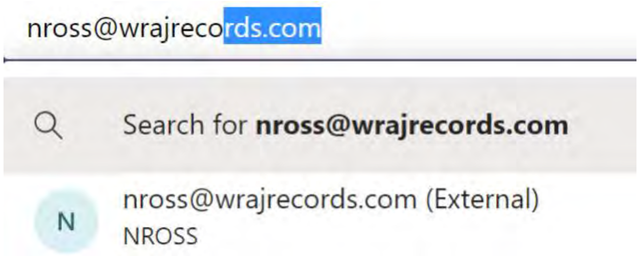
We can't set up the conversation because your organizations are not set up to talk to each other.

7. If the domain has been whitelisted, then users will have the following experience:



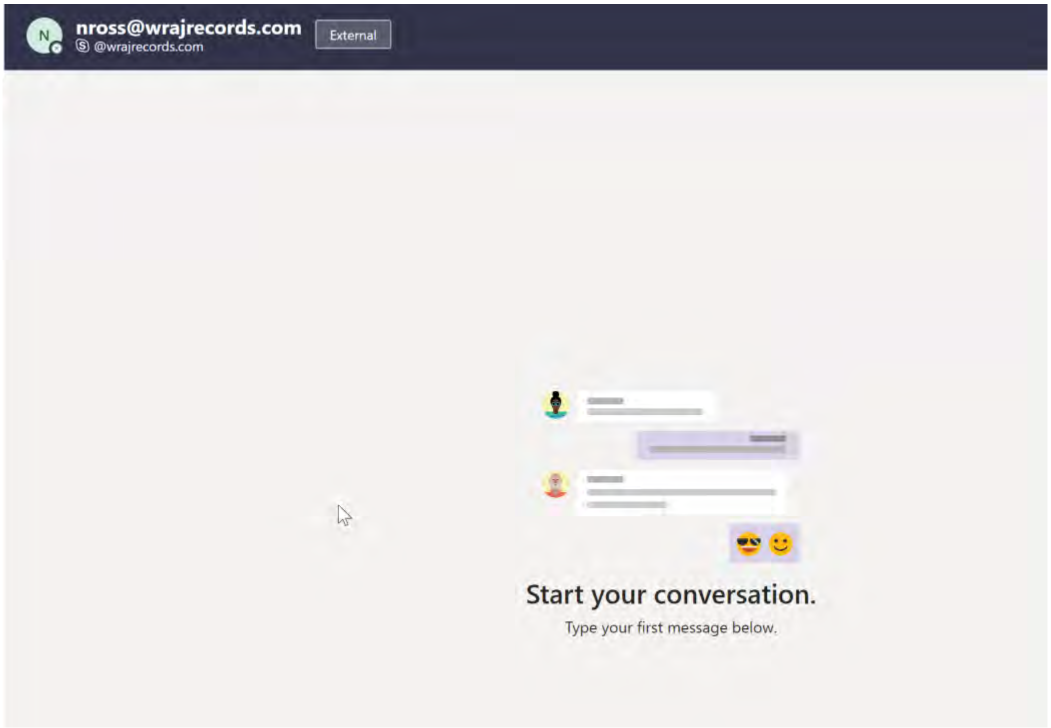
nross@wrajrecords.com

Search for **nross@wrajrecords.com**
Search **nross@wrajrecords.com** externally



nross@wrajrecords.com

Search for **nross@wrajrecords.com**
N
nross@wrajrecords.com (External)
NROSS



nross@wrajrecords.com
@wrajrecords.com

Start your conversation.

Type your first message below.

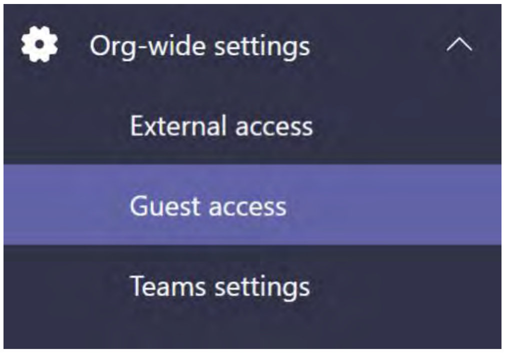
Limit Guest Access

By default, guest access in Teams is turned off. Team owners cannot add external users to any Teams channels. You can change this setting in the Teams admin center and external users can be invited to Teams Channels **by owners of that channel.** You should have a formal request process defined for adding external guest users to Teams channel where users submit business justification. Once you enable guest access, you can control the settings for the access rights that user has within the channel. Guest access should always be limited for a certain time period for security and compliance reasons.

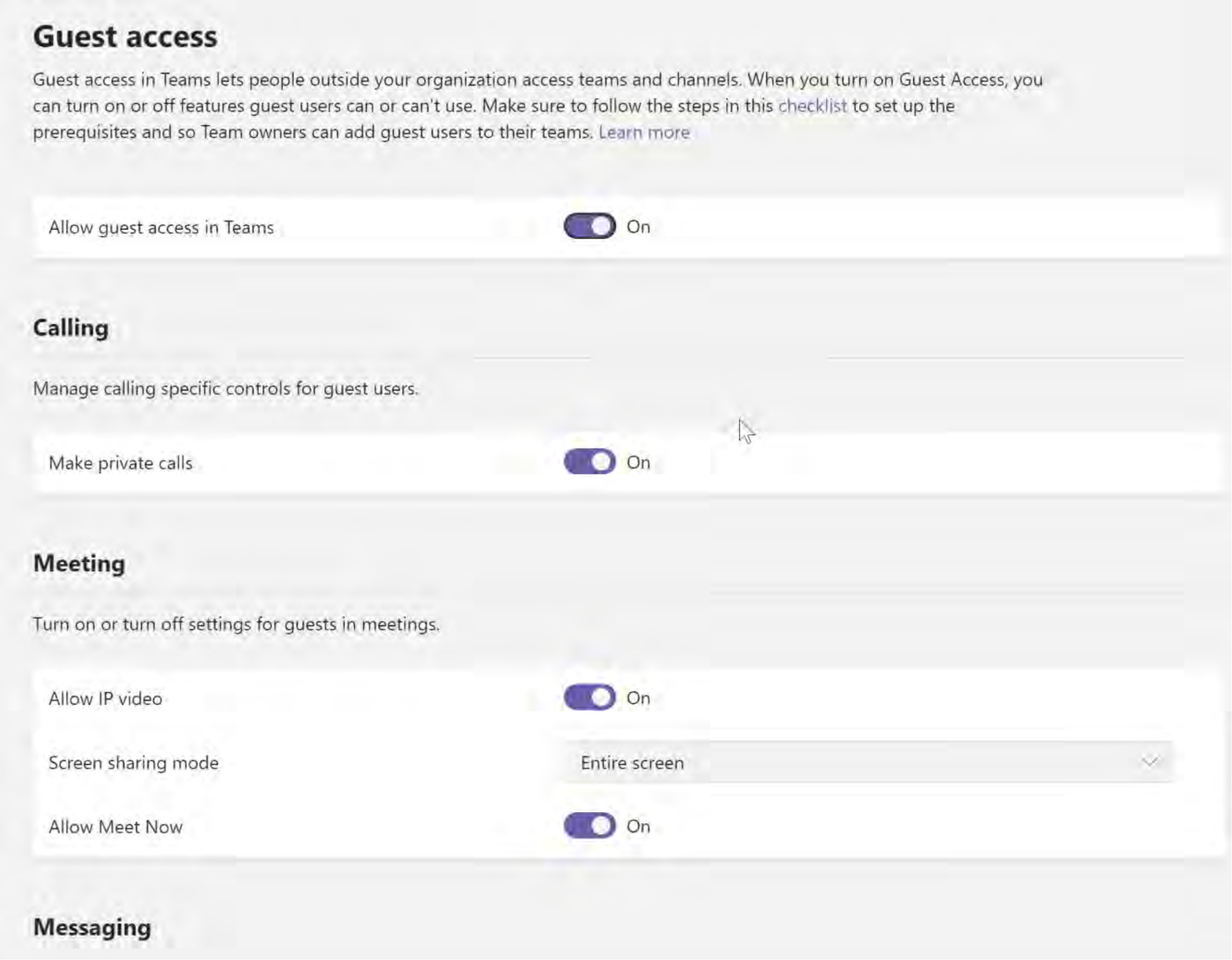
Compliance Controls

- NIST CSP DE.CM-7
- NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3,
- CM-8, PE-3, PE-6, PE-20, SI-4
- HIPAA Security Rule 45 C.F.R. §§
  - 164.308(a)(1)(ii)(D)
  - 164.312(b)
  - 164.314(b)(2)(i)

1. In the Teams Admin Center, click on Org-wide settings>Guest Access



2. Temporarily turn on guest access and review the settings available



Guest access

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

Allow guest access in Teams — On

Calling

Manage calling specific controls for guest users.

Make private calls — On

Meeting

Turn on or turn off settings for guests in meetings.

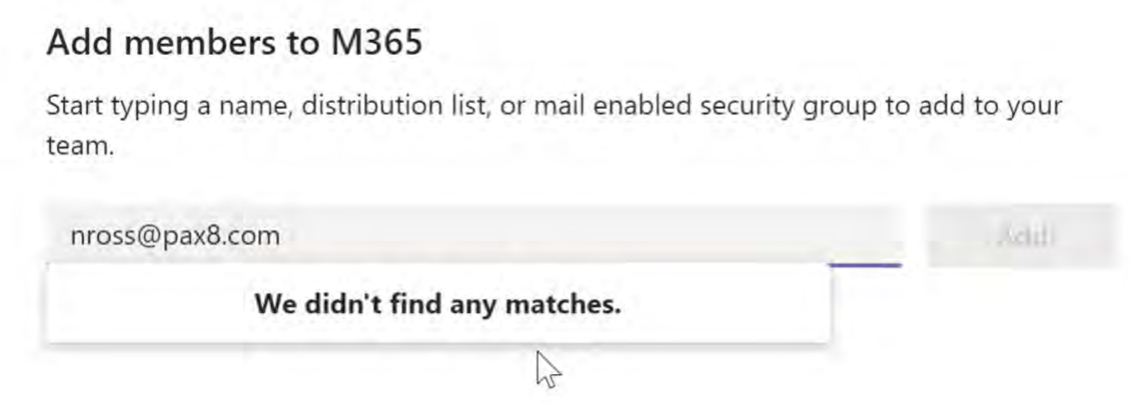
Allow IP video — On

Screen sharing mode — Entire screen

Allow Meet Now — On

Messaging

3. If guest access is turned off, then owners of channels will not be able to invite external participants. Example:



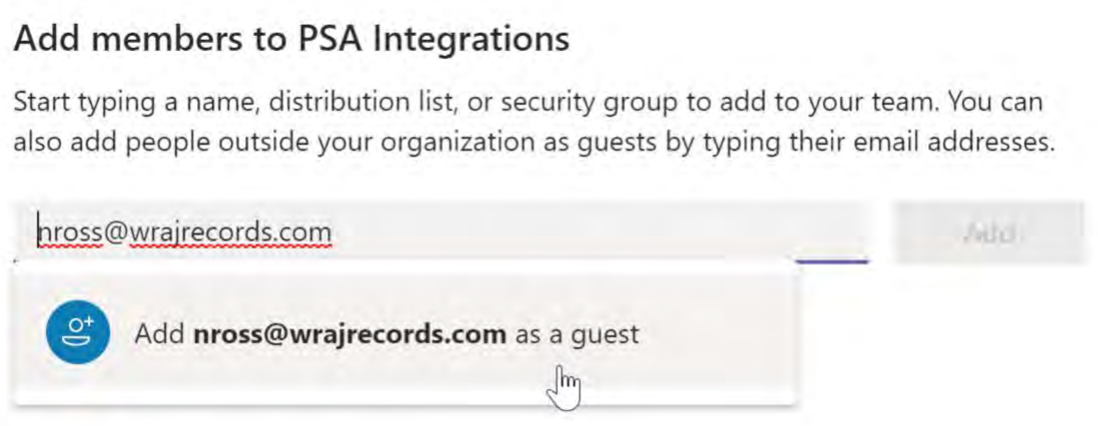
Add members to M365

Start typing a name, distribution list, or mail enabled security group to add to your team.

nross@pax8.com

We didn't find any matches.

4. If guest access is turned on, then owners can send invites to external participants



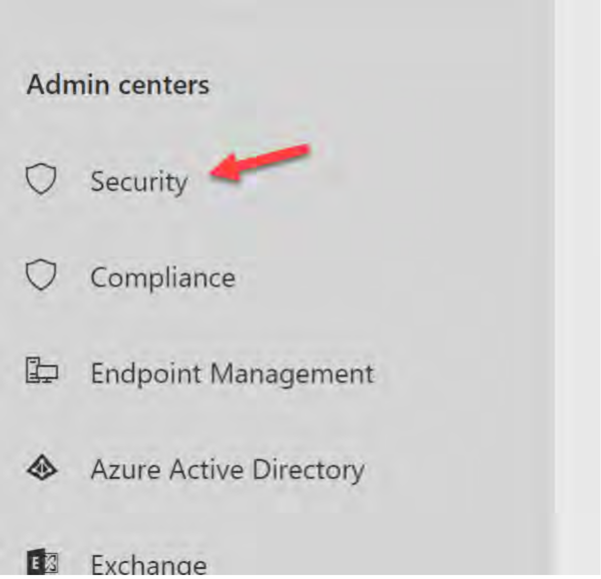
Add members to PSA Integrations

Start typing a name, distribution list, or security group to add to your team. You can also add people outside your organization as guests by typing their email addresses.

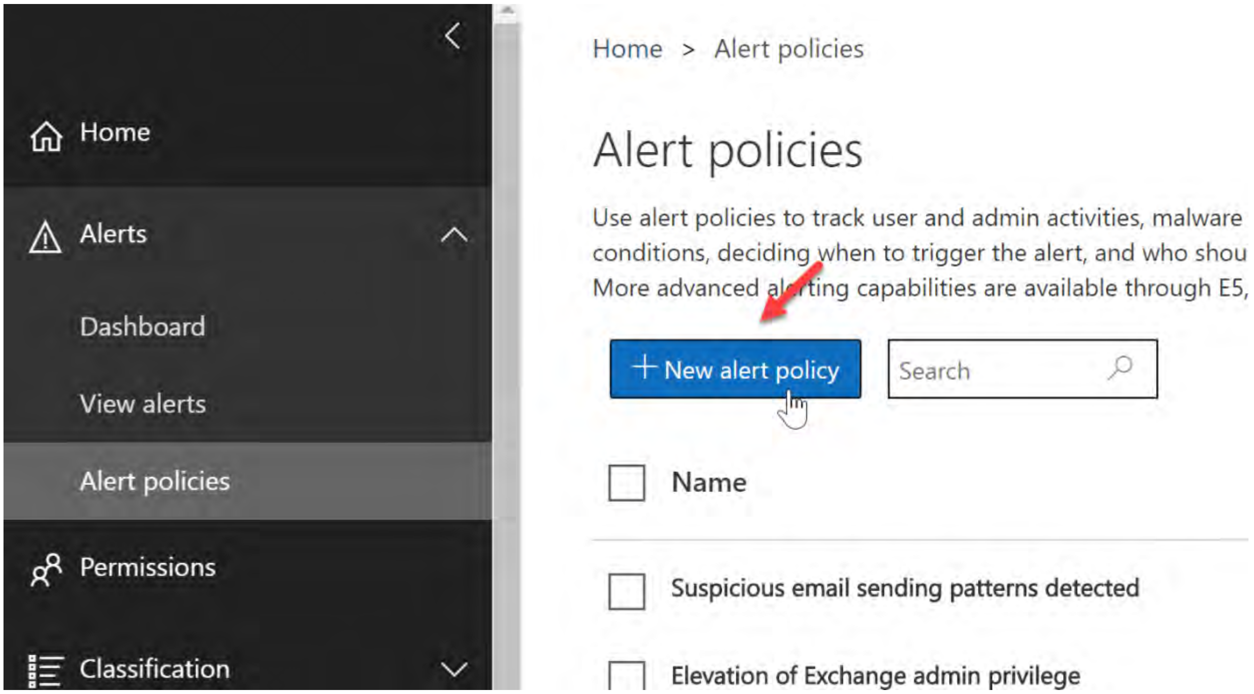
nross@wrajrecords.com

Add **nross@wrajrecords.com** as a guest

5. In the Security and Compliance Center, you can set up alerts to get a notification when guest users are added. In the 365 Admin Center>Click Admin Centers>Security



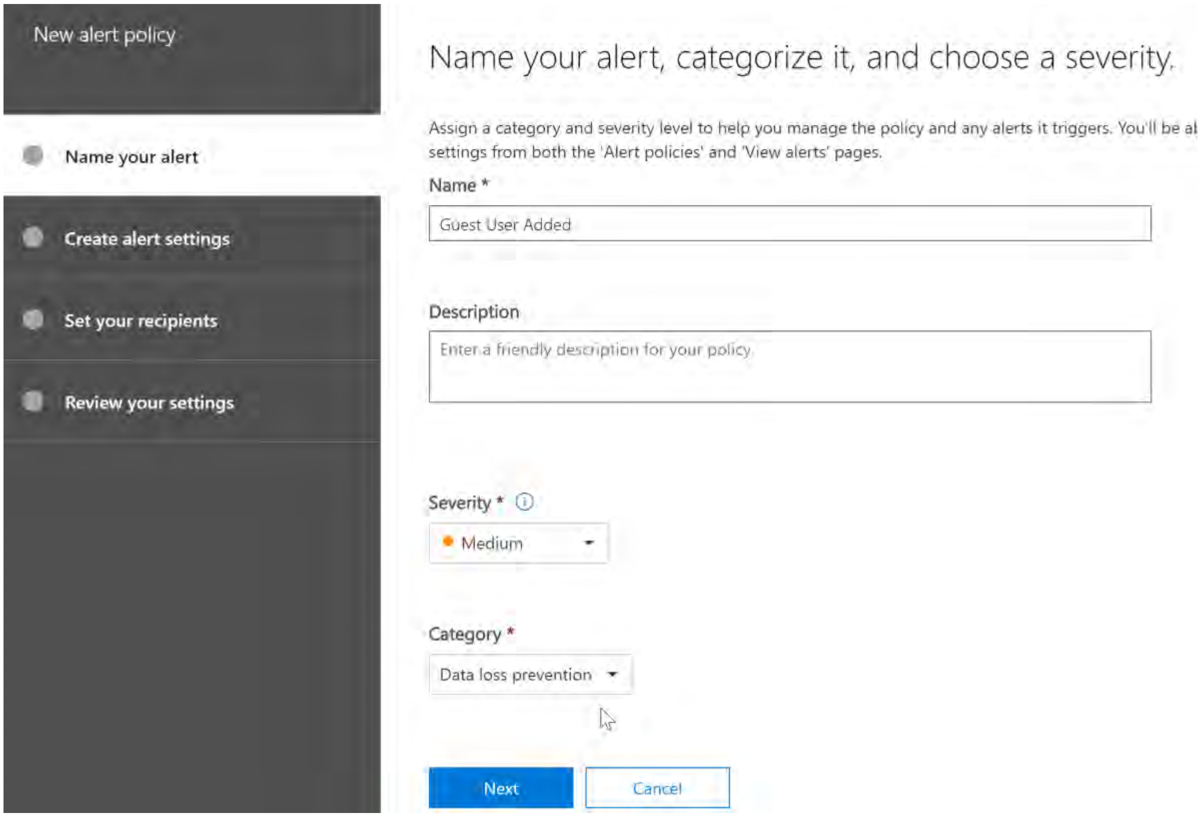
6. Click on Alerts>Alert policies>New Alert Policy



Use alert policies to track user and admin activities, malware conditions, deciding when to trigger the alert, and who shou More advanced alerting capabilities are available through E5,

□	Name
□	Suspicious email sending patterns detected
□	Elevation of Exchange admin privilege

7. Add Name, Description, Severity, and Category



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 al settings from both the 'Alert policies' and 'View alerts' pages.

Name *

Guest User Added

Description

Enter a friendly description for your policy

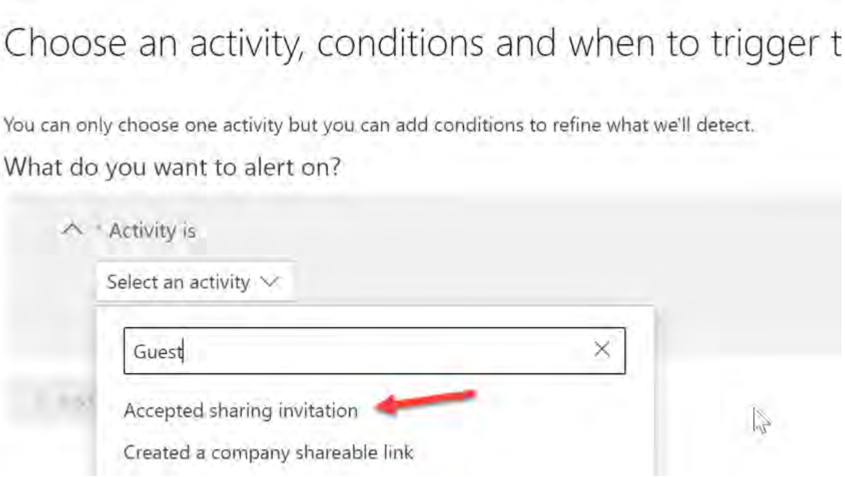
Severity *

● Medium

Category *

Data loss prevention

8. Type ‘Guest’ and select Accepted Sharing Invitation>click Next



Choose an activity, conditions and when to trigger t

You can only choose one activity but you can add conditions to refine what we'll detect.

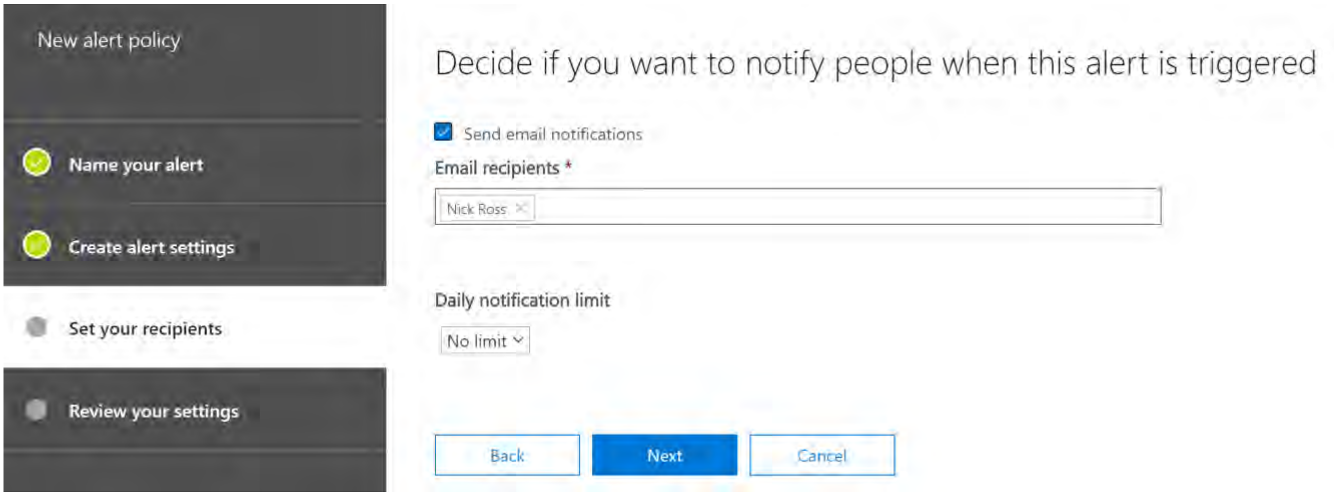
What do you want to alert on?

* Activity is

Select an activity

Guest

9. Specify the email address you would like this to go to



New alert policy

- Name your alert
- Create alert settings
- Set your recipients
- Review your settings

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

☑ Send email notifications

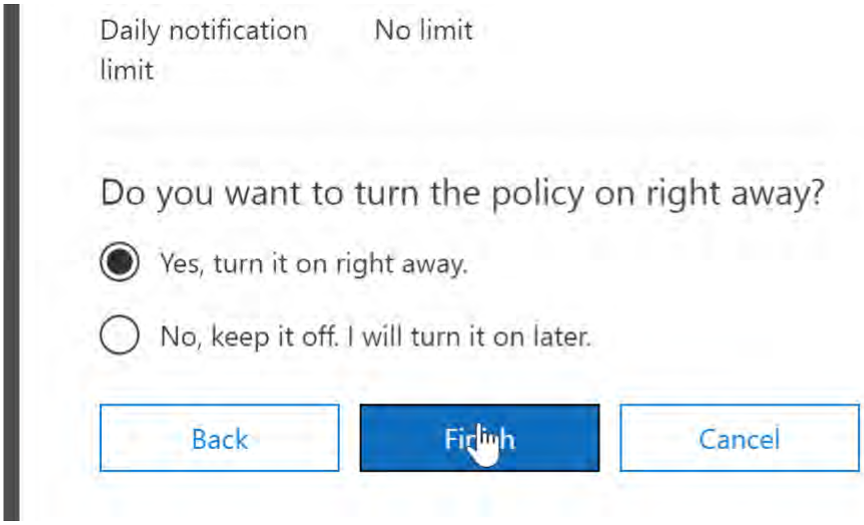
Email recipients *

Nick Ross ×

Daily notification limit

No limit

10. Review and turn on the alert



Daily notification limit: No limit

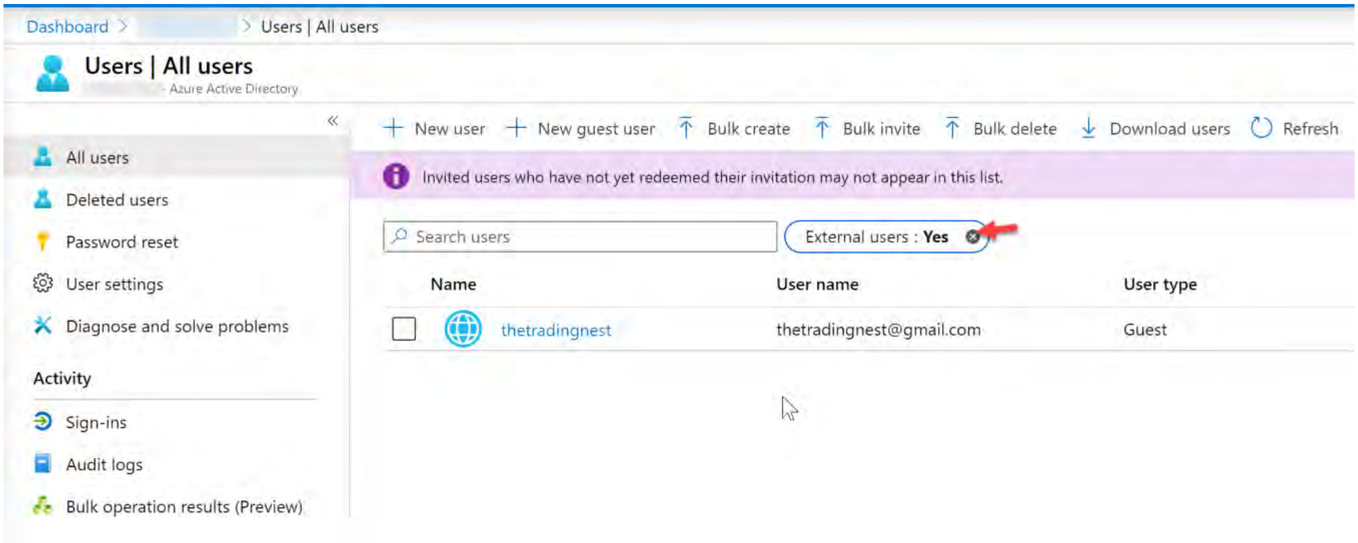
Do you want to turn the policy on right away?

● Yes, turn it on right away.

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

Additional Considerations:

- Periodically review guest access users in the Azure Active Directory Portal (monthly/quarterly)

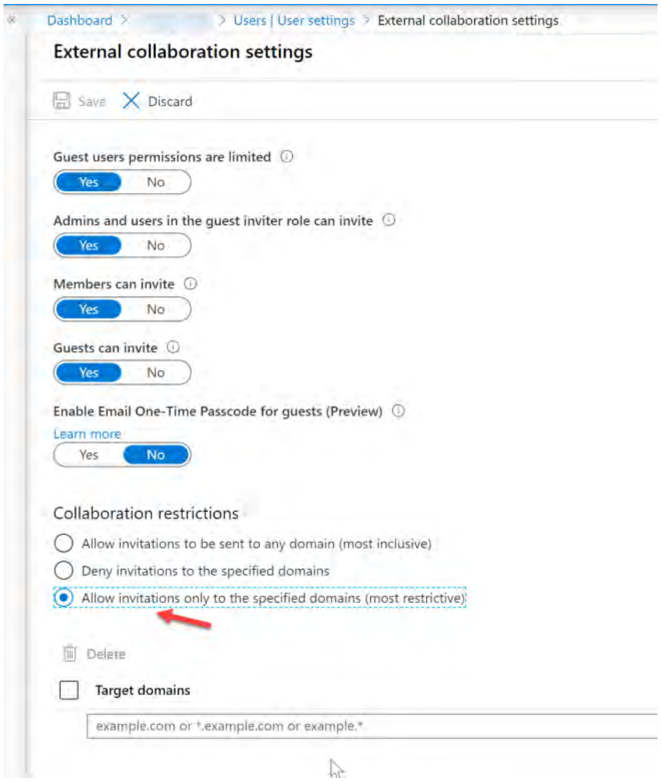


Invited users who have not yet redeemed their invitation may not appear in this list.

External users : **Yes**

	Name	User name	User type
□	thetradingnest	thetradingnest@gmail.com	Guest

- In Azure Active Direcotory, limit the domains for external collaboration and configure other settings. Admin Center>Azure Active Directory>Users>User Settings>Manage external collaboration settings



Dashboard > > Users | User settings > External collaboration settings

External collaboration settings

Guest users permissions are limited ⓘ
[✓ Yes] No

Admins and users in the guest inviter role can invite ⓘ
[✓ Yes] No

Members can invite ⓘ
[✓ Yes] No

Guests can invite ⓘ
[✓ Yes] No

Enable Email One-Time Passcode for guests (Preview) ⓘ
Learn more
Yes [✓ No]

Collaboration restrictions

○ Allow invitations to be sent to any domain (most inclusive)
○ Deny invitations to the specified domains
● Allow invitations only to the specified domains (most restrictive)

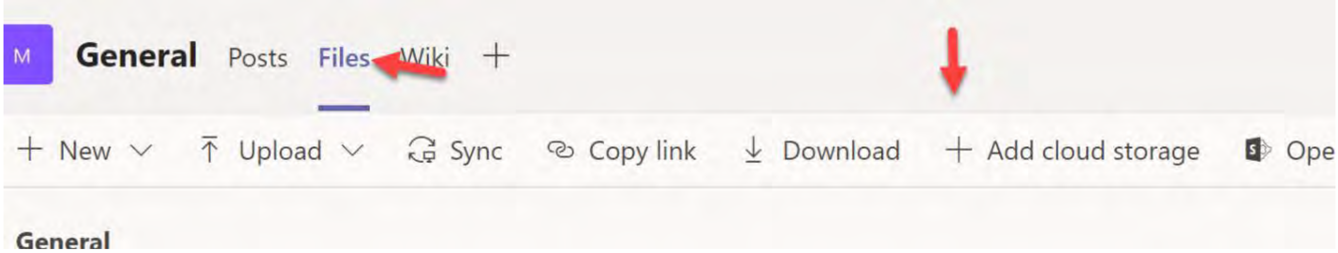
□ Target domains

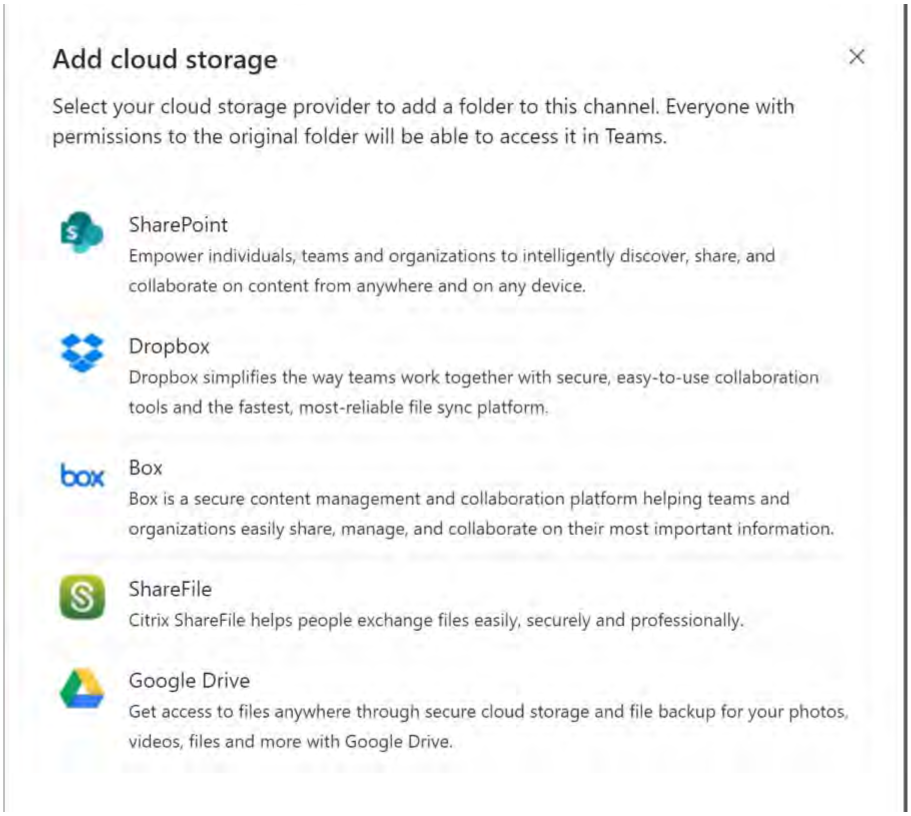
example.com or *.example.com or example.*

Turn off File Sharing and File Storage Options

By default, users can add external third-party storage providers like Google and DropBox to their Teams channels for file storage. Only managed, trusted providers should be allowed for data loss prevention purposes.

Ex.





Add cloud storage

Select your cloud storage provider to add a folder to this channel. Everyone with permissions to the original folder will be able to access it in Teams.

SharePoint
Empower individuals, teams and organizations to intelligently discover, share, and collaborate on content from anywhere and on any device.

Dropbox
Dropbox simplifies the way teams work together with secure, easy-to-use collaboration tools and the fastest, most-reliable file sync platform.

Box
Box is a secure content management and collaboration platform helping teams and organizations easily share, manage, and collaborate on their most important information.

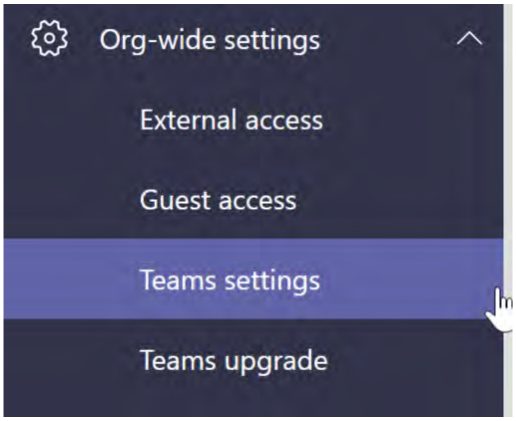
ShareFile
Citrix ShareFile helps people exchange files easily, securely and professionally.

Google Drive
Get access to files anywhere through secure cloud storage and file backup for your photos, videos, files and more with Google Drive.

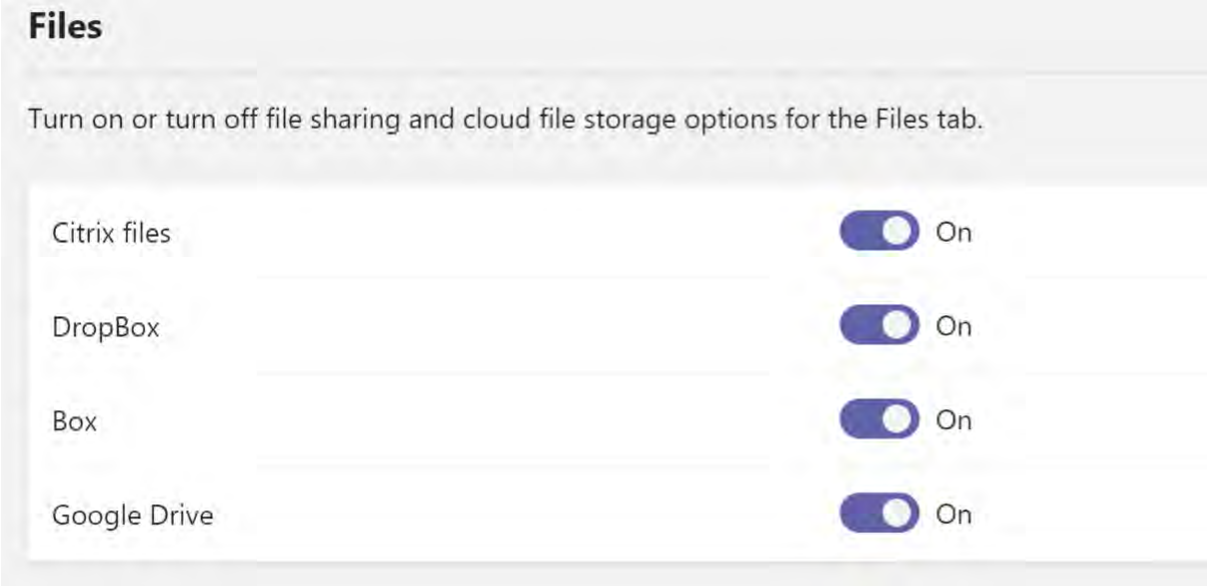
Compliance Controls:

- NIST CSF PR-DS-5
- CCS CSC 17
- COBIT 5 APO01.06
- ISA 62443-3-3:2013 SR 5.2
- ISO/IEC 27001:2013 A.6.1.2, A.7.1.1,
- A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1,
- A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5,
- A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4,
- A.14.1.2, A.14.1.3
- NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
- HIPAA Security Rule 45 C.F.R. §§
    - 164.308(a)(1)(ii)(D), 164.308(a)(3),
    - 164.308(a)(4), 164.310(b), 164.310(c),
    - 164.312(a), 164.312(e)

1. In the Teams Admin Center, click Org-wide Settings>Teams Settings



2. Scroll down to the Files section and un-toggle each provider that is not managed by the company



Files

Turn on or turn off file sharing and cloud file storage options for the Files tab.

Citrix files On

DropBox On

Box On

Google Drive On

OVERVIEW & USER GUIDE

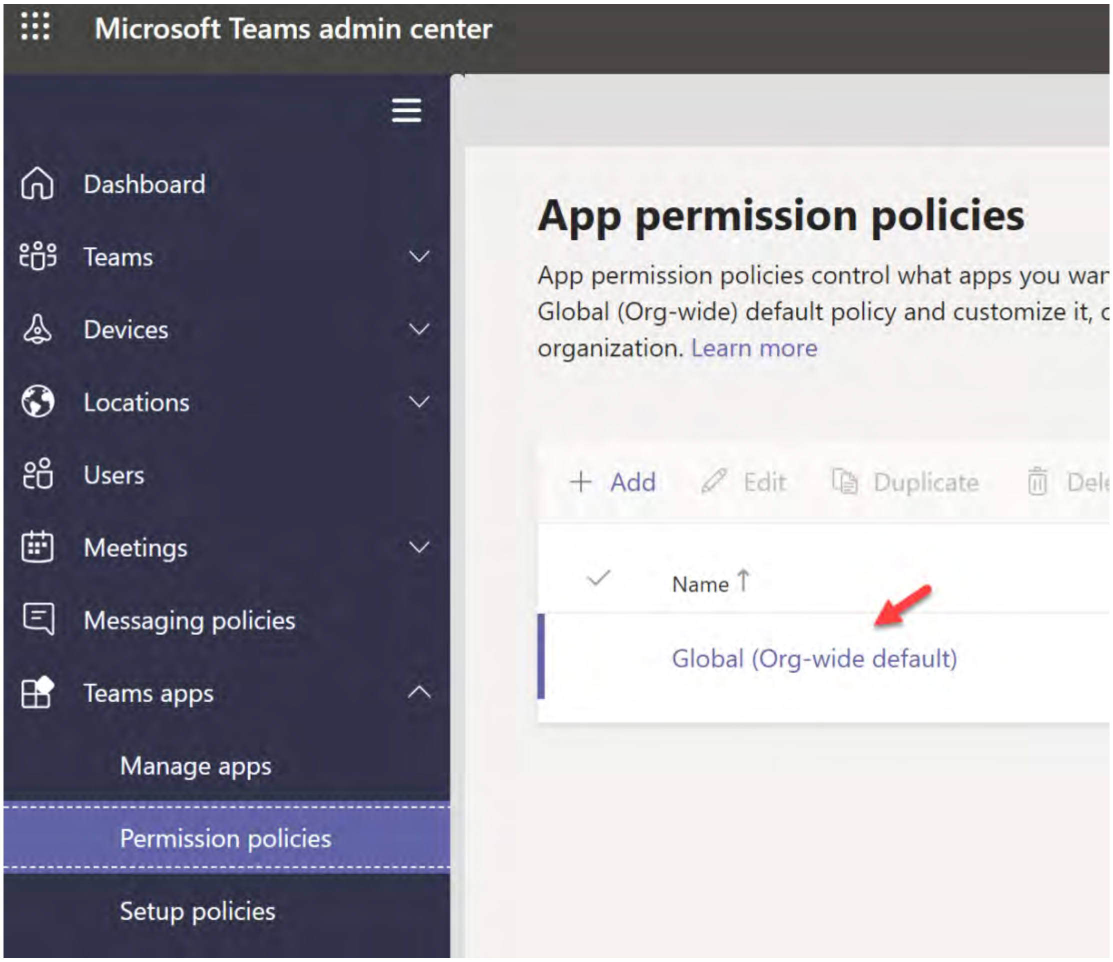
Block Third-Party Applications

By default, all users have access to the Teams app store which contains applications published by Microsoft and other third parties. While we do not want to inhibit productivity, we do want to ensure we are preventing data loss and shadow IT at the organization. Any of these apps can be added to a Teams channel and users could begin to share corporate data back and forth with applications that are unmanaged. It is recommended that you whitelist applications that users can add and create a formal request process for additional applications.

Compliance Controls:

- NIST CSF PR-DS-5
- CCS CSC 17
- COBIT 5 APO01.06
- ISA 62443-3-3:2013 SR 5.2
- ISO/IEC 27001:2013 A.6.1.2, A.7.1.1,
  - A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1,
  - A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5,
  - A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4,
  - A.14.1.2, A.14.1.3
- NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
- HIPAA Security Rule 45 C.F.R. §§
  - 164.308(a)(1)(ii)(D), 164.308(a)(3),
  - 164.308(a)(4)
  - 164.312(a), 164.312(e)

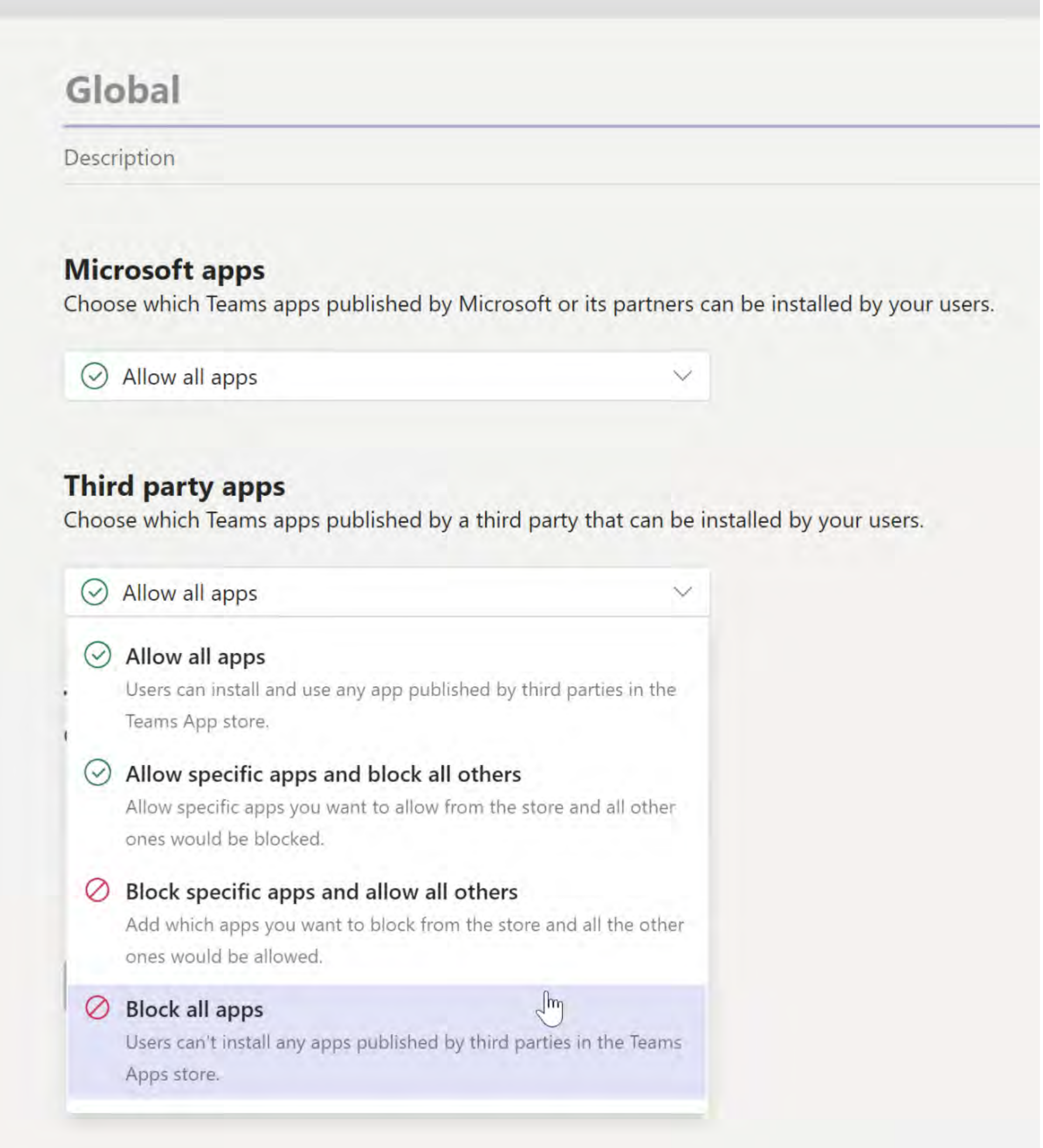
1. In the Teams Admin Center, go to Teams Apps>Permission Policies>Global



App permission policies

App permission policies control what apps you war Global (Org-wide) default policy and customize it, c organization. Learn more

2. Choose to block all third-party applications or evaluate which apps you want to whitelist. Doing the same for Microsoft Applications is recommended



Global

Description

Microsoft apps

Choose which Teams apps published by Microsoft or its partners can be installed by your users.

✓ Allow all apps

Third party apps

Choose which Teams apps published by a third party that can be installed by your users.

✓ Allow all apps

✓ Allow all apps
Users can install and use any app published by third parties in the Teams App store.

✓ Allow specific apps and block all others
Allow specific apps you want to allow from the store and all other ones would be blocked.

⊘ Block specific apps and allow all others
Add which apps you want to block from the store and all the other ones would be allowed.

⊘ Block all apps
Users can't install any apps published by third parties in the Teams Apps store.

Restrict Users who can Create Teams Channels

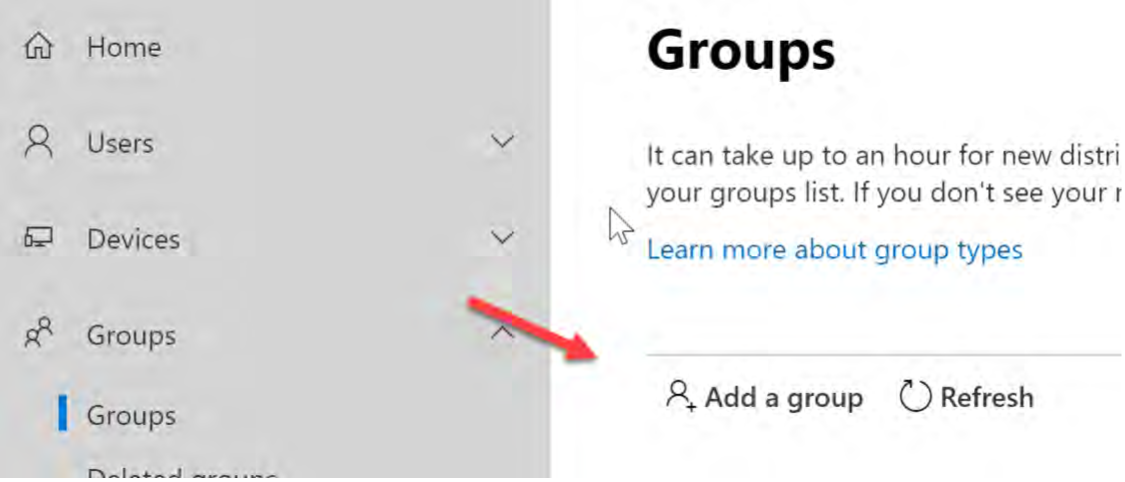
Users within a tenant have the ability to create a public or private Teams channel by default. Behind the scenes, creating a Teams channel also creates a Microsoft 365 or Office 365 Group and a SharePoint site with a document library that stores all documents shared within the Teams channel. Over time, if this is not managed, the environment could quickly get out of hand with the number of Teams channels being created. This could lead to data loss, insecure sharing of documentation, and overall confusion across the organization. We recommend limiting the creation of Teams channels to certain members within the organization and creating a formal request process for new channels. If you do not want to restrict this to a certain group, we recommend you at least set up expiration policies around Teams channels that are processed for review based on activity in the channel. We discuss that in the next section.

***NOTE* It is very important that you properly plan and communicate any changes here before rolling them out. The goal is not to inhibit productivity and force users to go to outside channels to collaborate, causing shadow IT. It is imperative that you make the request for creating a new Teams channel as seamless as possible. Restricting the creation of Teams channels also restricts who can create Groups. The setting is all or nothing in this regard.**

Compliance Controls:

- NIST CSF PR.PT-1
- CCS CSC 14
- COBIT 5 APO11.04
- ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8,, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
- ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
- ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
- NIST SP 800-53 Rev. 4 AU Family
- HIPAA Security Rule 45 C.F.R. §§
  - 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C),164.312(b)

1. In the 365 Admin Center, go to Groups>Add Group

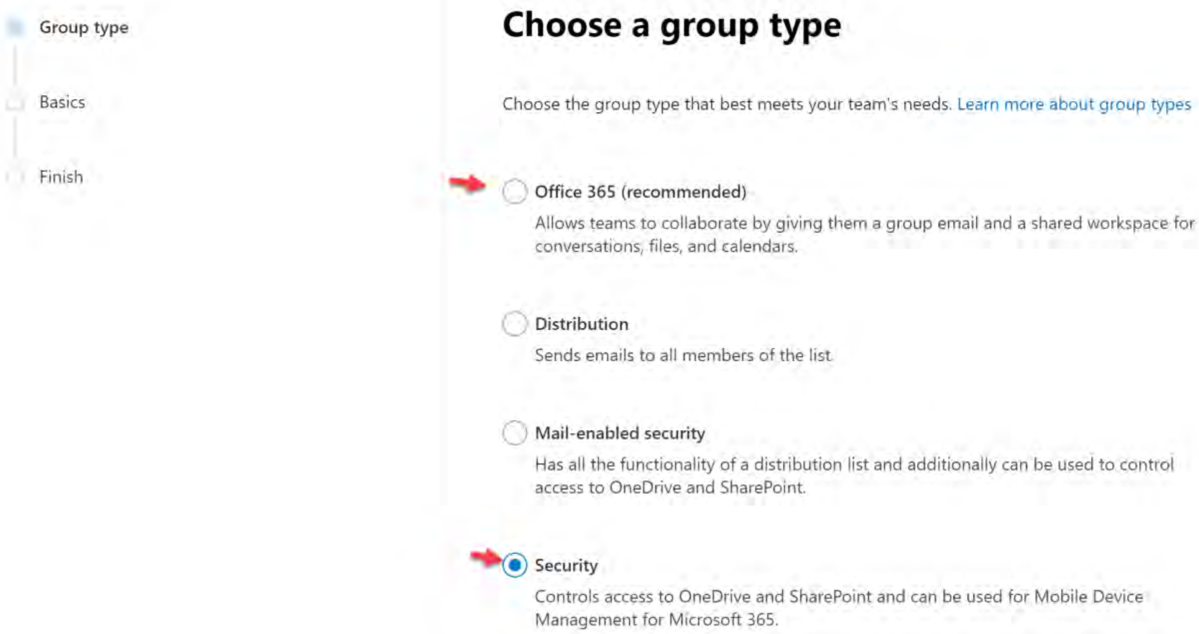


Groups

It can take up to an hour for new distri
your groups list. If you don't see your r

Learn more about group types

2. Add a 365 Group or Security Group. This will house the members who will have access to create 365 Groups and Teams Channels



Choose a group type

Choose the group type that best meets your team's needs. Learn more about group types

○ Office 365 (recommended)
Allows teams to collaborate by giving them a group email and a shared workspace for conversations, files, and calendars.

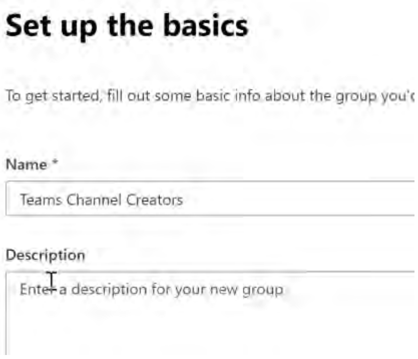
○ Distribution
Sends emails to all members of the list.

○ Mail-enabled security
Has all the functionality of a distribution list and additionally can be used to control access to OneDrive and SharePoint.

● Security
Controls access to OneDrive and SharePoint and can be used for Mobile Device Management for Microsoft 365.

OVERVIEW & USER GUIDE

3. Name the Group, Save, and add the appropriate members once the group has finished being created



Set up the basics

To get started, fill out some basic info about the group you'(

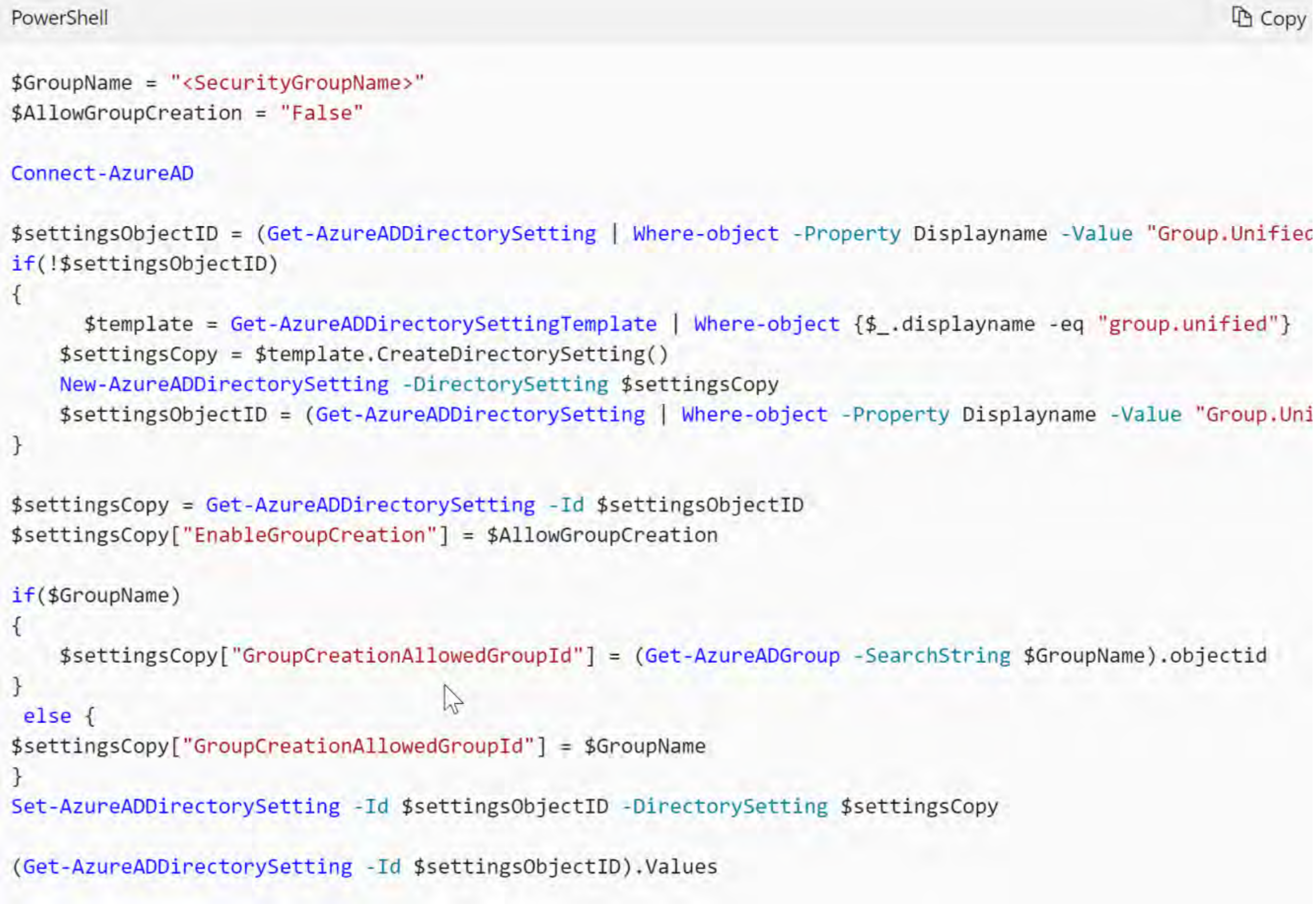
Name *

Teams Channel Creators

Description

Enter a description for your new group

4. Click on the following link and scroll down to the PowerShell section

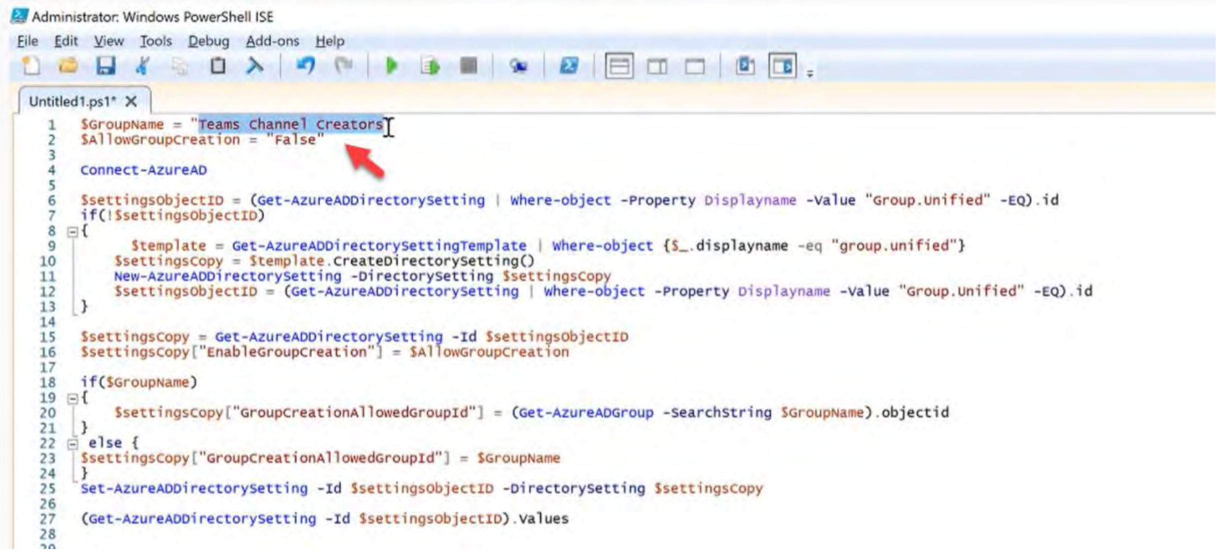


```powershell
$GroupName = "<SecurityGroupName>"
$AllowGroupCreation = "False"

Connect-AzureAD

$settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unifiec
if(!$settingsObjectID)
{
      $template = Get-AzureADDirectorySettingTemplate | Where-object {$_.displayname -eq "group.unified"}
    $settingsCopy = $template.CreateDirectorySetting()
    New-AzureADDirectorySetting -DirectorySetting $settingsCopy
    $settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Uni
}

$settingsCopy = Get-AzureADDirectorySetting -Id $settingsObjectID
$settingsCopy["EnableGroupCreation"] = $AllowGroupCreation

if($GroupName)
{
    $settingsCopy["GroupCreationAllowedGroupId"] = (Get-AzureADGroup -SearchString $GroupName).objectid
}
 else {
$settingsCopy["GroupCreationAllowedGroupId"] = $GroupName
}
Set-AzureADDirectorySetting -Id $settingsObjectID -DirectorySetting $settingsCopy

(Get-AzureADDirectorySetting -Id $settingsObjectID).Values
```

5. Run PowerShell ISE as Admin (64x version) and run the following command:

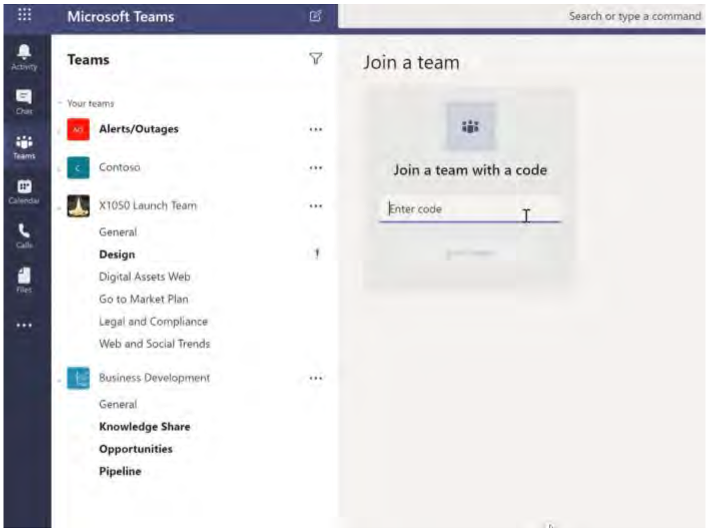
Import-Module AzureADPreview

6. Copy and paste the script for the website linked on step 4. Change the group name to the display name of the group you created in step 3


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*

```
$GroupName = "Teams Channel Creators"
$AllowGroupCreation = "False"

Connect-AzureAD

$settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id
if(!$settingsObjectID)
{
      $template = Get-AzureADDirectorySettingTemplate | Where-object {$_.displayname -eq "group.unified"}
    $settingsCopy = $template.CreateDirectorySetting()
    New-AzureADDirectorySetting -DirectorySetting $settingsCopy
    $settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id
}

$settingsCopy = Get-AzureADDirectorySetting -Id $settingsObjectID
$settingsCopy["EnableGroupCreation"] = $AllowGroupCreation

if($GroupName)
{
    $settingsCopy["GroupCreationAllowedGroupId"] = (Get-AzureADGroup -SearchString $GroupName).objectid
}
 else {
$settingsCopy["GroupCreationAllowedGroupId"] = $GroupName
}
Set-AzureADDirectorySetting -Id $settingsObjectID -DirectorySetting $settingsCopy

(Get-AzureADDirectorySetting -Id $settingsObjectID).Values
```

7. After you run the script, all users who are not part of the group will not be able to create new channels



Set Teams Expiration

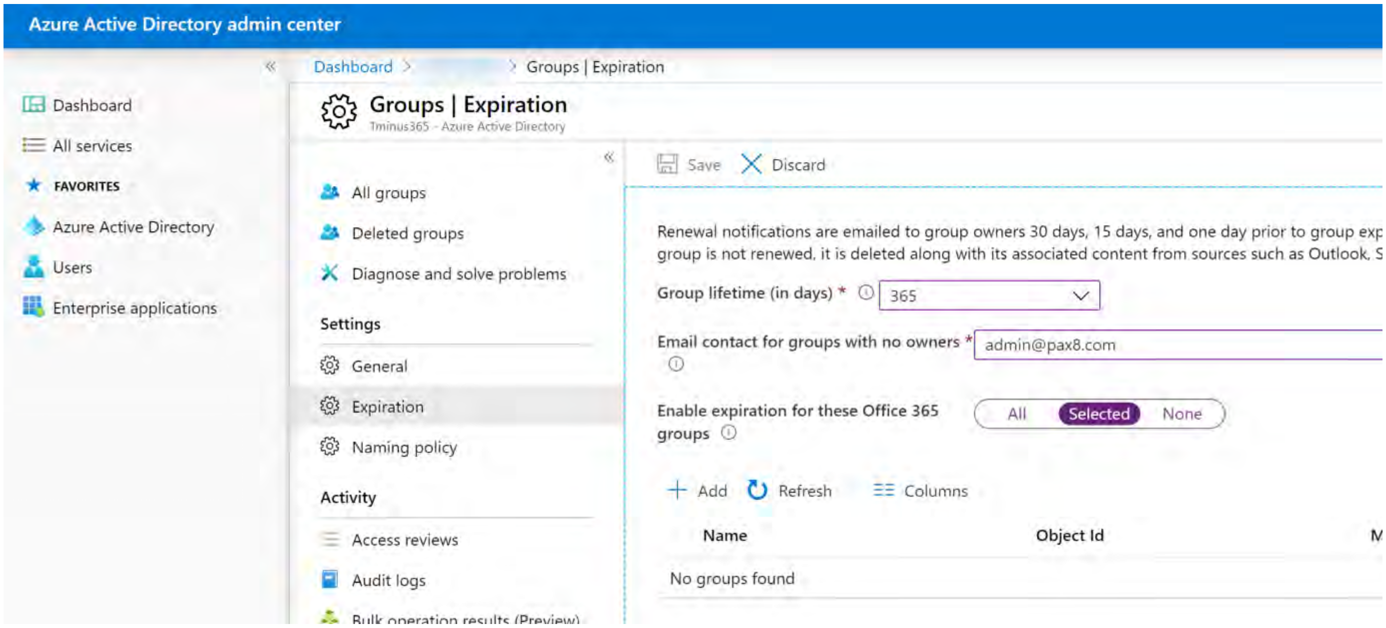
Organizations with a large number of teams often have Teams channels that are never actually used. This can happen because of several reasons including product experimentation, short-term team collaboration, or team owners leaving the organization. Over time, such teams can accumulate and create a burden on tenant resources. To curb the number of unused teams, as an admin, you can use group expiration policy to automatically clean up unused teams. Because teams are backed by groups, group expiration policies automatically apply to teams as well.

When you apply an expiration policy to a team, a team owner receives a notification for team renewal 30 days, 15 days and 1 day before the team's expiration date. When the team owner receives the notification, they can click Renew now in team settings to renew the team. To prevent accidental deletion, auto-renewal is automatically enabled for a team in the group expiration policy. When the group expiration policy is set up, any team that has at least one channel visit from any team member before its expiration date is automatically renewed without any manual intervention from the team owner.

Compliance Controls:

- NIST CSF PR.PT-1
- CCS CSC 14
- COBIT 5 APO11.04
- ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8,, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
- ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
- ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
- NIST SP 800-53 Rev. 4 AU Family
- HIPAA Security Rule 45 C.F.R. §§
    - 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b)

1. In the 365 Admin Center, go to Admin Centers>Azure Active Directory>Groups>Expiration



Azure Active Directory admin center

Groups | Expiration

Tminus365 - Azure Active Directory

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group exp
group is not renewed, it is deleted along with its associated content from sources such as Outlook, S

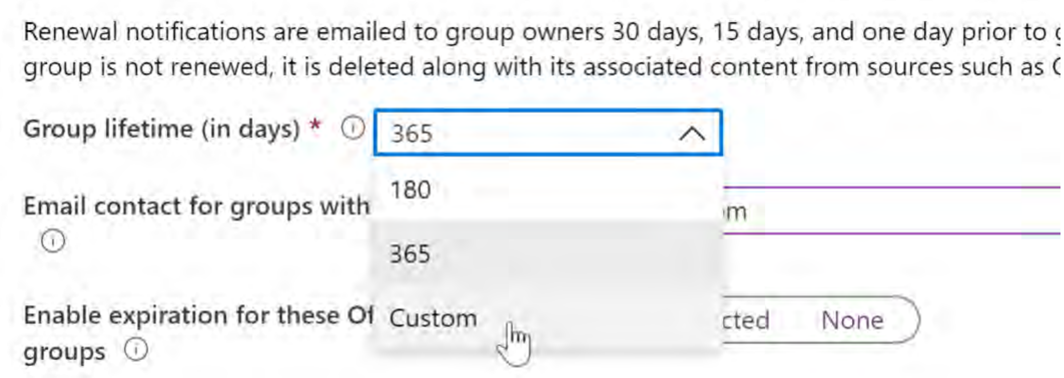
Group lifetime (in days) * 365

Email contact for groups with no owners * admin@pax8.com

Enable expiration for these Office 365 groups: All [✓ Selected] None

Name	Object Id	M
No groups found		

2. Here you can create custom policies to define group lifetime, an email contact for groups with no owners, and the ability to scope the policy to certain Teams channels. If you choose All, then you will not have to review this in the future. Group lifetime can be custom



Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to g
group is not renewed, it is deleted along with its associated content from sources such as (

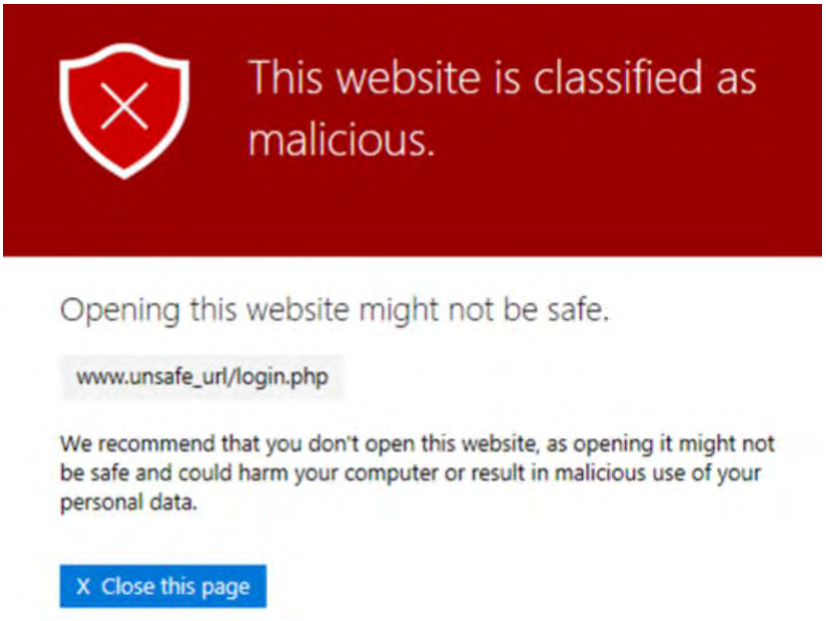
Group lifetime (in days) * 365

Email contact for groups with ... m

Enable expiration for these Of... groups: ...cted None

Set up Advanced Threat Protection Policies for Teams

With Office 365 Advanced Threat Protection, you can configure safe link policies and safe attachment policies within many Office environments, including Teams. A safe links policy will allow you to have real-time click protection with any links shared over Teams chats. This will detonate the URL in a sandbox environment and scan for malicious content. If malicious content is detected, the user will be prevented from continuing.



This website is classified as malicious.

Opening this website might not be safe.

www.unsafe_url/login.php

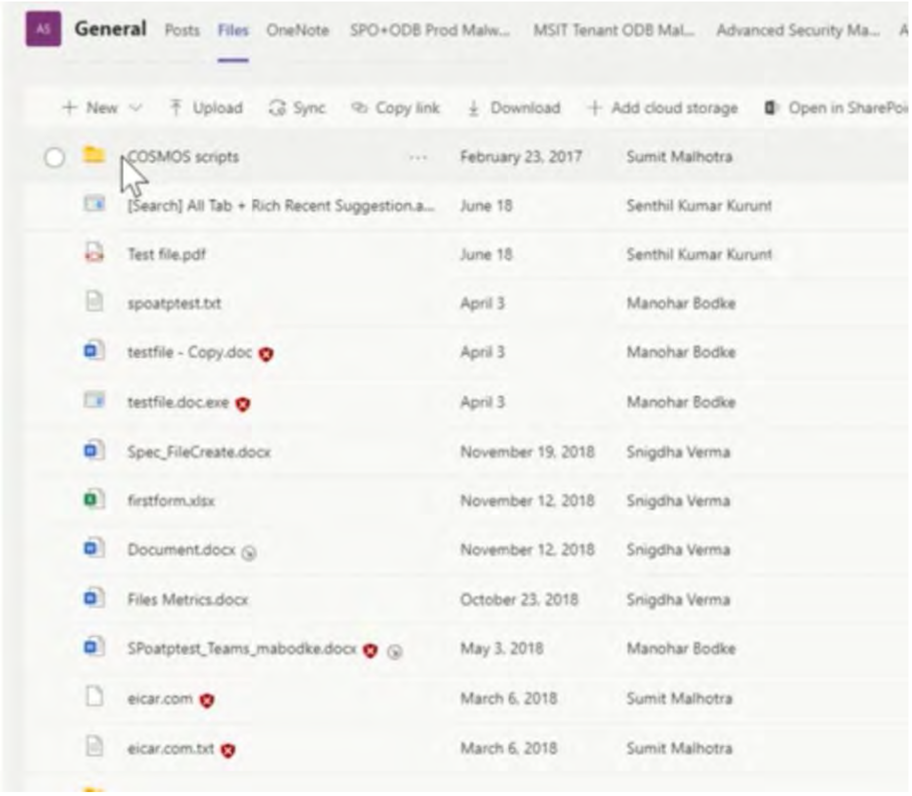
We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

Compliance Controls:

- NIST CSF DE.CM-4
- CCS CSC 5
- COBIT 5 DSS05.01
- ISA 62443-2-1:2009 4.3.4.3.8
- ISA 62443-3-3:2013 SR 3.2
- ISO/IEC 27001:2013 A.12.2.1
- NIST SP 800-53 Rev. 4 SI-3
- HIPAA Security Rule 45 C.F.R. §§
    - 164.308(a)(5)(ii)(B)

OVERVIEW & USER GUIDE

Safe attachments scan files shared in Teams and also the files part of the document library associated with the Teams channel.

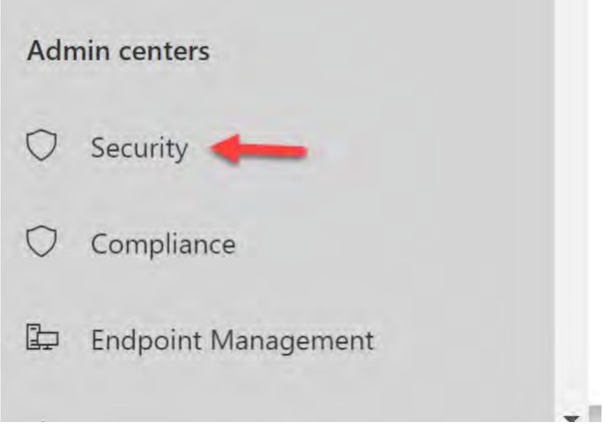


COSMOS scripts ···	February 23, 2017	Sumit Malhotra
[Search] All Tab + Rich Recent Suggestion.a...	June 18	Senthil Kumar Kurunt
Test file.pdf	June 18	Senthil Kumar Kurunt
spoatptest.txt	April 3	Manohar Bodke
testfile - Copy.doc	April 3	Manohar Bodke
testfile.doc.exe	April 3	Manohar Bodke
Spec_FileCreate.docx	November 19, 2018	Snigdha Verma
firstform.xlsx	November 12, 2018	Snigdha Verma
Document.docx	November 12, 2018	Snigdha Verma
Files Metrics.docx	October 23, 2018	Snigdha Verma
SPoatptest_Teams_mabodke.docx	May 3, 2018	Manohar Bodke
eicar.com	March 6, 2018	Sumit Malhotra
eicar.com.txt	March 6, 2018	Sumit Malhotra

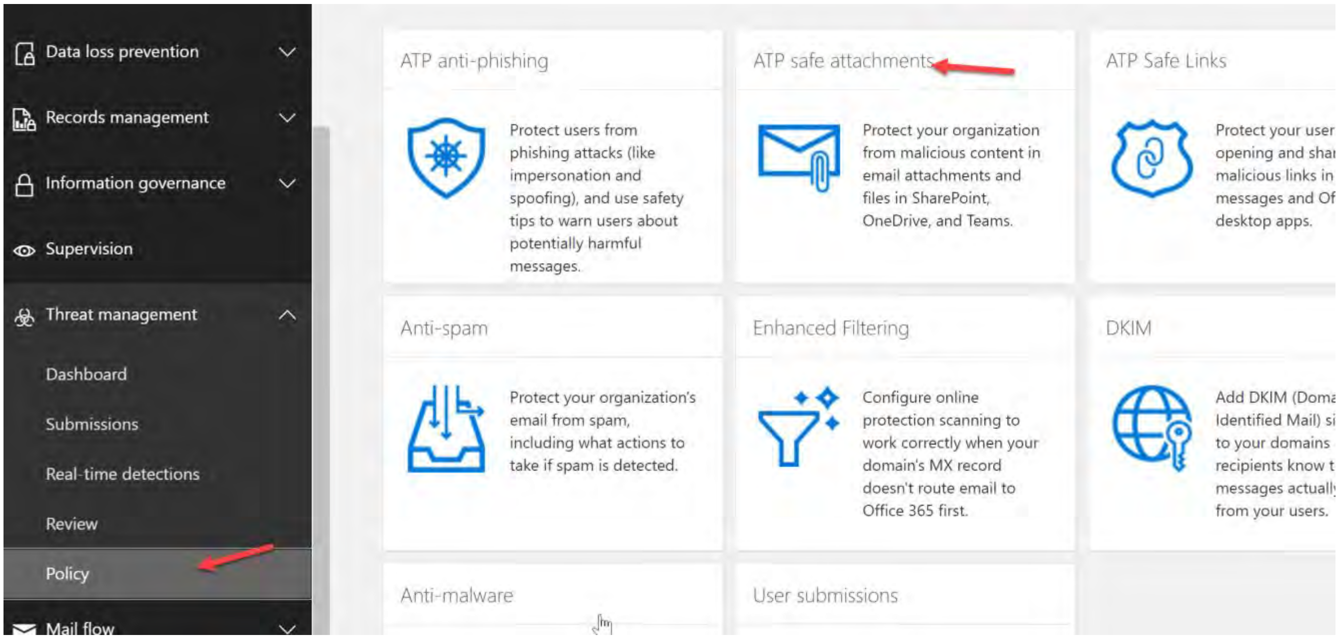
License Requirements:

- Microsoft Advanced Threat Protection Plan (1) $2/u/m
- Microsoft 365 Business Premium $20/u/m

1. In the 365 Admin Center, click Admin Centers>Security



2. Click on Threat Management>Policy>ATP Safe Attachments



ATP anti-phishing: Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.

ATP safe attachments: Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

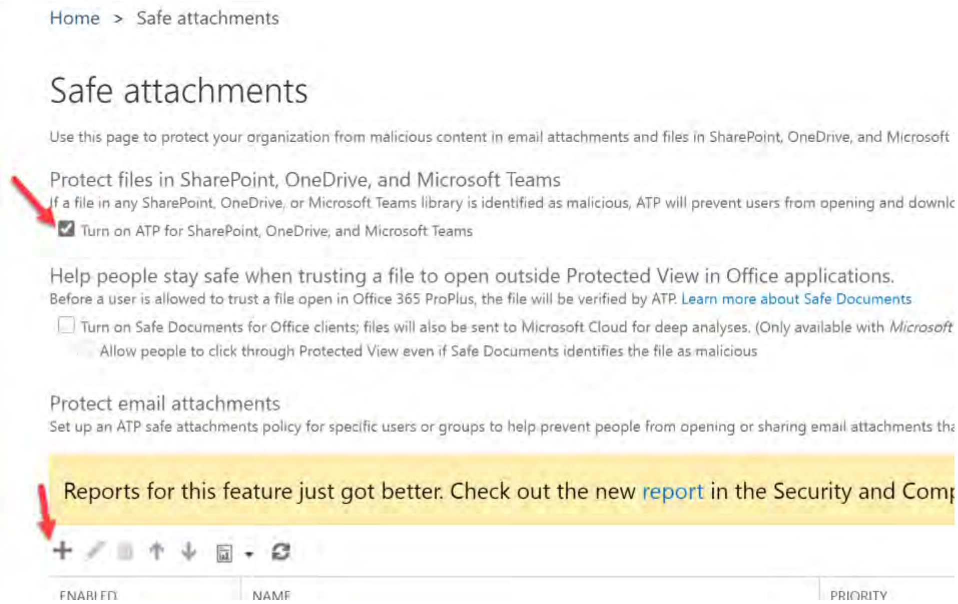
ATP Safe Links: Protect your user opening and shar malicious links in messages and Of desktop apps.

Anti-spam: Protect your organization's email from spam, including what actions to take if spam is detected.

Enhanced Filtering: Configure online protection scanning to work correctly when your domain's MX record doesn't route email to Office 365 first.

DKIM: Add DKIM (Doma Identified Mail) si to your domains recipients know t messages actually from your users.

3. Checkmark the box to turn on ATP for Teams. Select the + icon to create a new policy



Home > Safe attachments

Safe attachments

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

Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, ATP will prevent users from opening and downlc

☑ Turn on ATP for SharePoint, OneDrive, and Microsoft Teams

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 open in Office 365 ProPlus, the file will be verified by ATP. Learn more about Safe Documents

☐ Turn on Safe Documents for Office clients; files will also be sent to Microsoft Cloud for deep analyses. (Only available with *Microsoft*

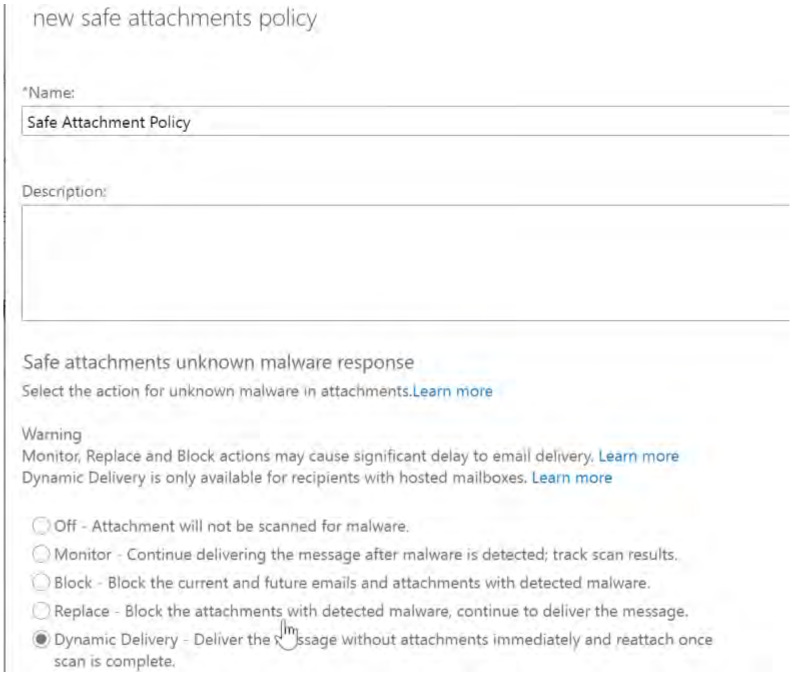
Allow people to click through Protected View even if Safe Documents identifies the file as malicious

Protect email attachments

Set up an ATP safe attachments policy for specific users or groups to help prevent people from opening or sharing email attachments tha

Reports for this feature just got better. Check out the new report in the Security and Comp

4. Add Name, Description, and choose Dynamic Delivery. For more on delivery methods, [click here]



new safe attachments policy

*Name:
Safe Attachment Policy

Description:

Safe attachments unknown malware response

Select the action for unknown malware in attachments.Learn more

Warning

Monitor, Replace and Block actions may cause significant delay to email delivery. Learn more

Dynamic Delivery is only available for recipients with hosted mailboxes. Learn more

○ Off - Attachment will not be scanned for malware.

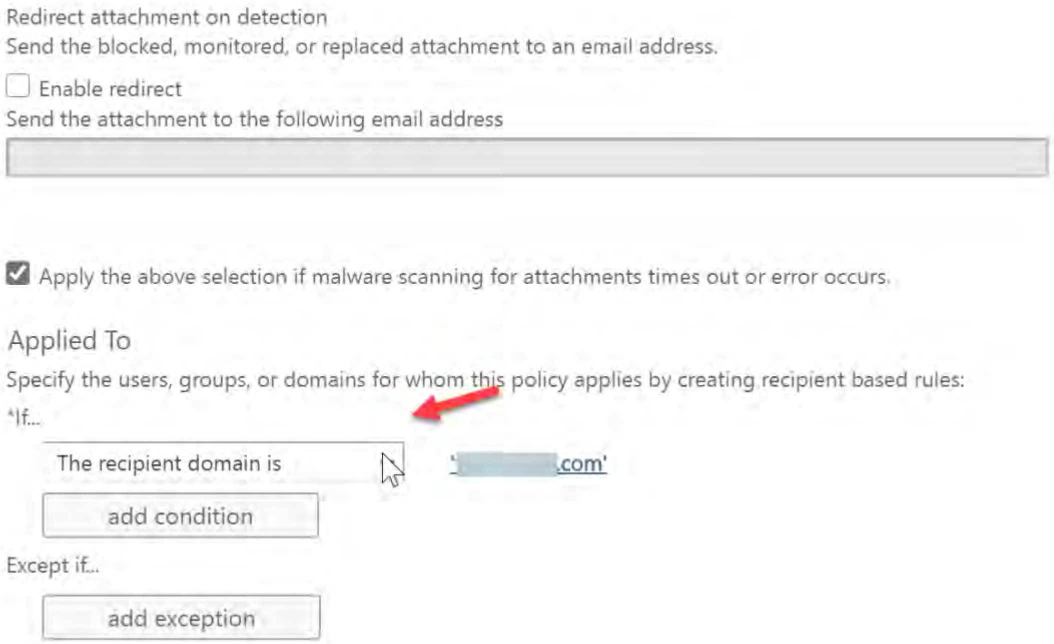
○ Monitor - Continue delivering the message after malware is detected; track scan results.

○ Block - Block the current and future emails and attachments with detected malware.

○ Replace - Block the attachments with detected malware, continue to deliver the message.

● Dynamic Delivery - Deliver the message without attachments immediately and reattach once scan is complete.

5. Add the recipient domain is selection and chose the main domain in the tenant. Click Save when completed



Redirect attachment on detection
Send the blocked, monitored, or replaced attachment to an email address.

□ Enable redirect

Send the attachment to the following email address

☑ Apply the above selection if malware scanning for attachments times out or error occurs.

Applied To

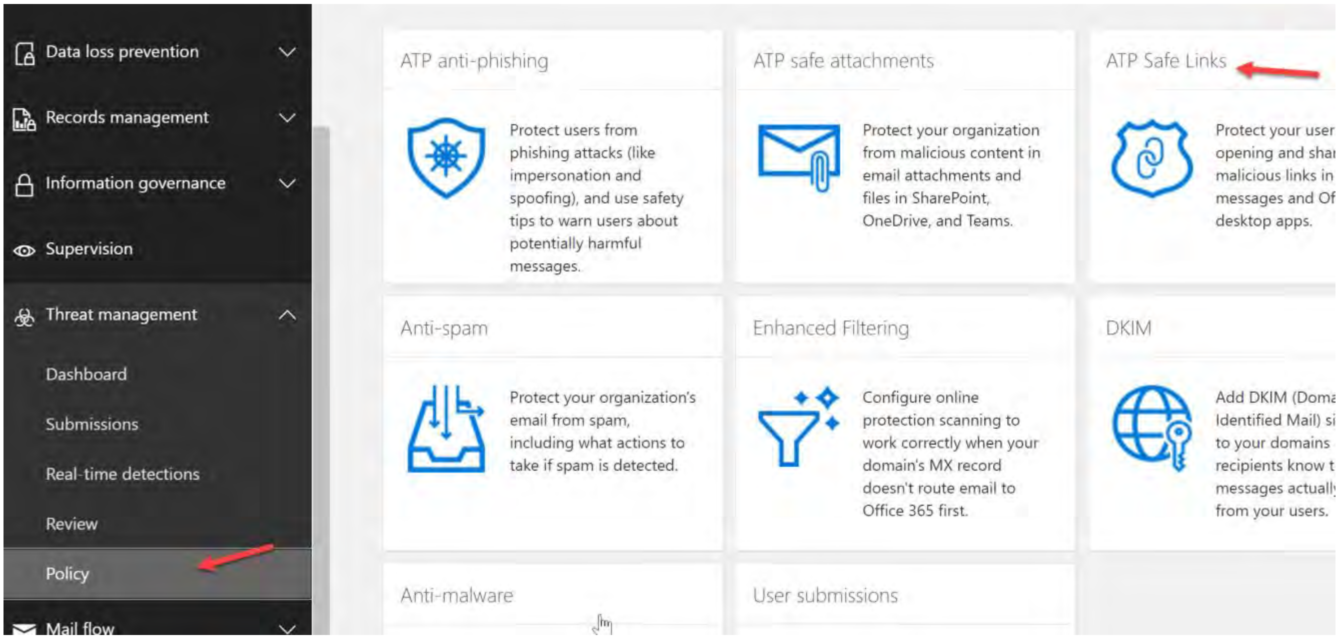
Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

The recipient domain is '[redacted].com'

Except if...

6. For Safe Links, go back to Threat management>Policy>Safe Links



ATP anti-phishing

Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.

ATP safe attachments

Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

ATP Safe Links

Protect your user opening and shar malicious links in messages and Of desktop apps.

Anti-spam

Protect your organization's email from spam, including what actions to take if spam is detected.

Enhanced Filtering

Configure online protection scanning to work correctly when your domain's MX record doesn't route email to Office 365 first.

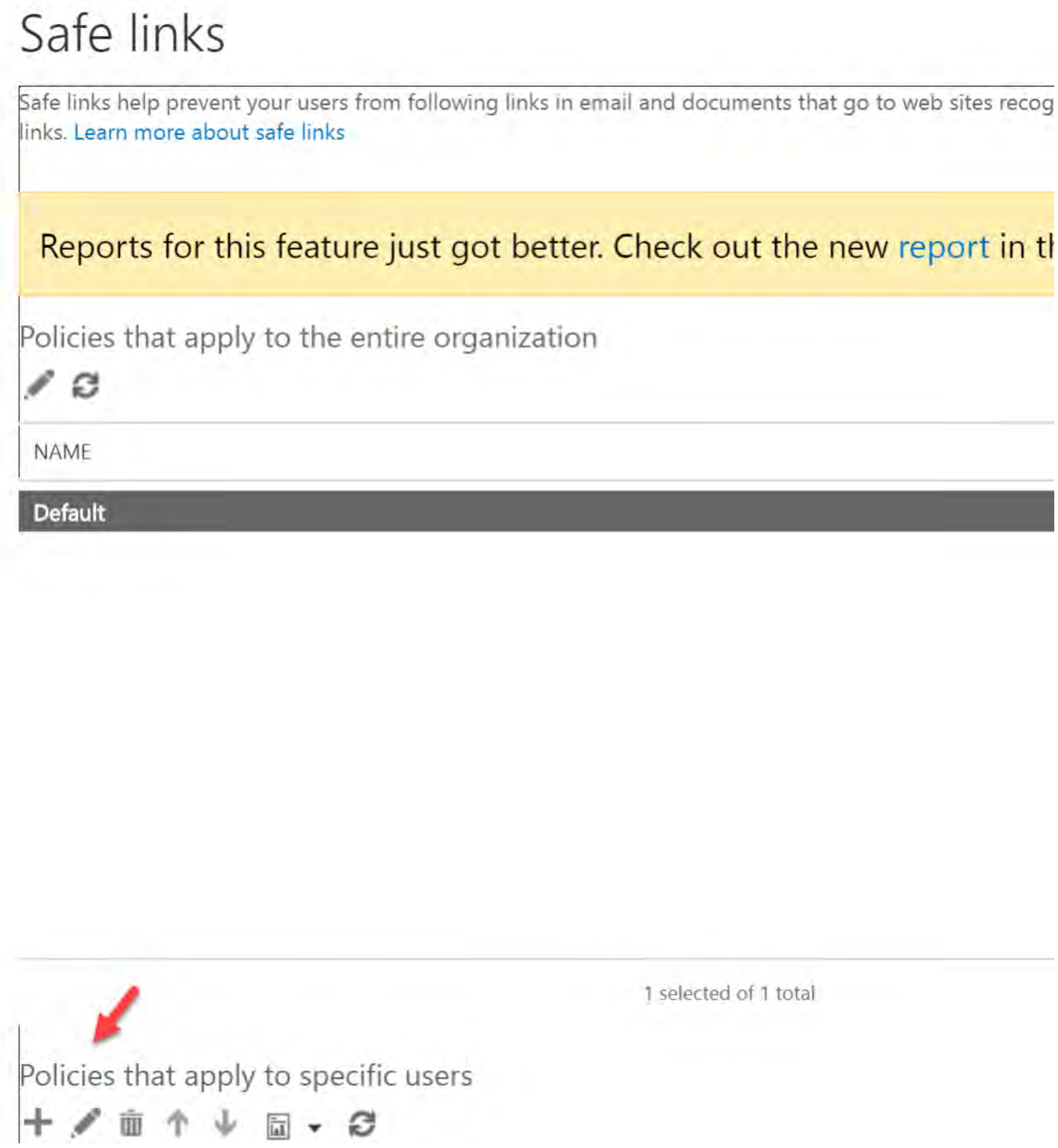
DKIM

Add DKIM (Doma Identified Mail) si to your domains recipients know t messages actuall from your users.

Anti-malware

User submissions

7. Scroll down to Policies that apply to specific users and click the + icon



Safe links

Safe links help prevent your users from following links in email and documents that go to web sites recog
links. Learn more about safe links

Reports for this feature just got better. Check out the new report in th

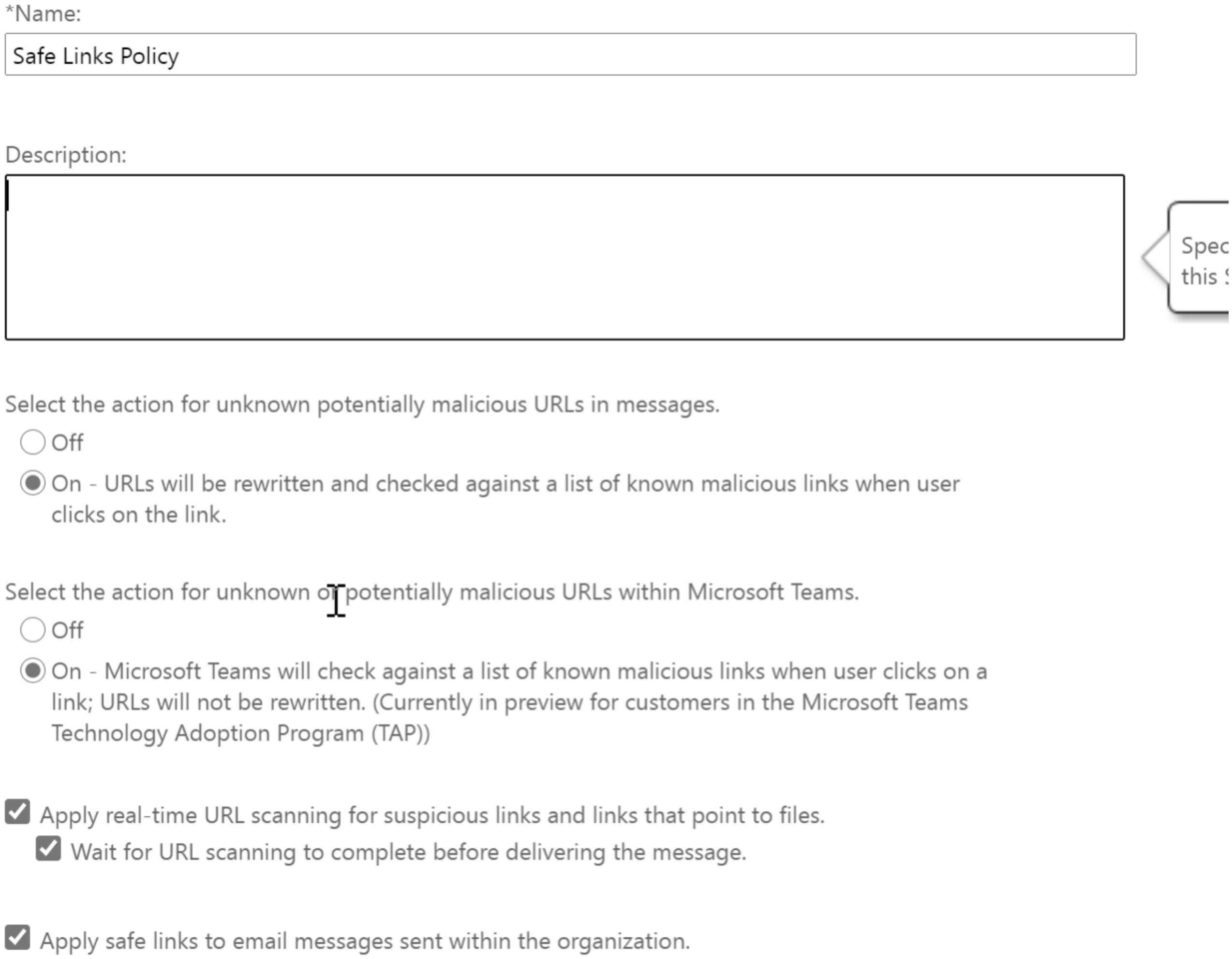
Policies that apply to the entire organization

NAME
Default

1 selected of 1 total

Policies that apply to specific users

8. Add a Name, Description, and turn on the necessary settings displayed below:



*Name:

Safe Links Policy

Description:

Select the action for unknown potentially malicious URLs in messages.

○ Off

● On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.

Select the action for unknown or potentially malicious URLs within Microsoft Teams.

○ Off

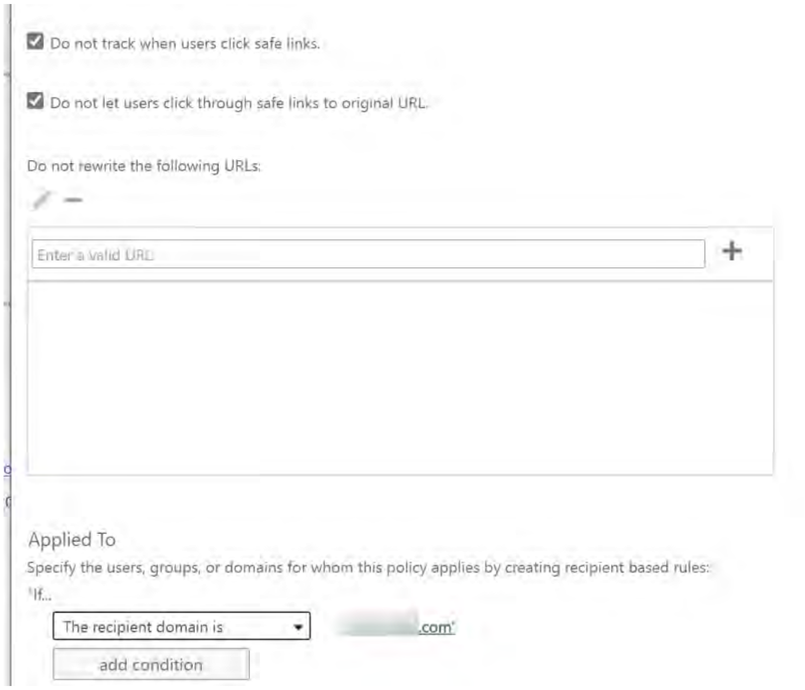
● On - Microsoft Teams will check against a list of known malicious links when user clicks on a link; URLs will not be rewritten. (Currently in preview for customers in the Microsoft Teams Technology Adoption Program (TAP))

☑ Apply real-time URL scanning for suspicious links and links that point to files.

☑ Wait for URL scanning to complete before delivering the message.

☑ Apply safe links to email messages sent within the organization.

9. You can choose to whitelist certain URLs. Like the safe attachments policy, apply to all users in the tenant by the domain name



☑ Do not track when users click safe links.

☑ Do not let users click through safe links to original URL.

Do not rewrite the following URLs:

Applied To

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

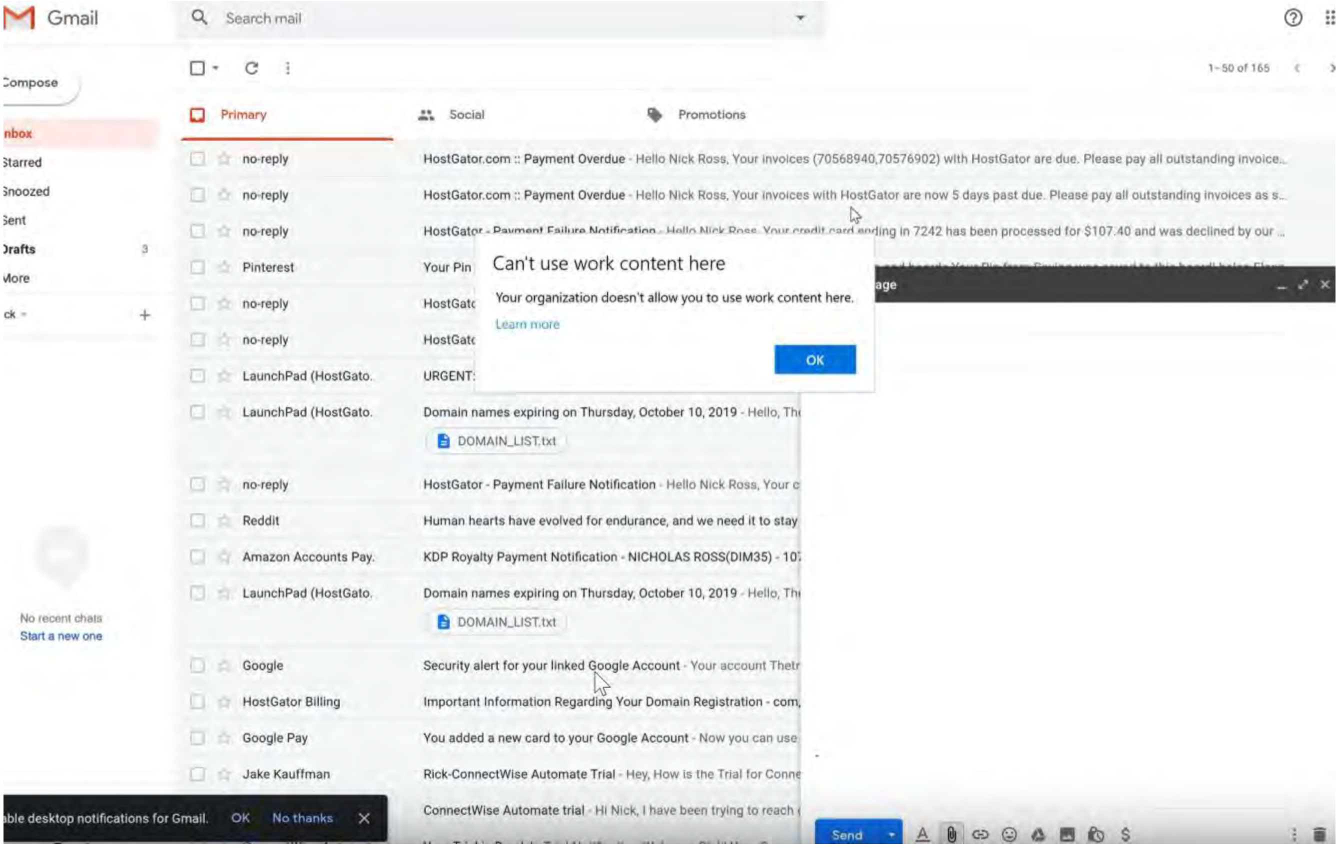
The recipient domain is [redacted].com'

OVERVIEW & USER GUIDE

Set up app Protection Policies

App Protection Policies are part of the mobile application management (MAM) solution with Microsoft Intune. App protection policies allow you to protect applications on Windows, iOS, and Android devices, no matter if they are enrolled in the Intune MDM solution or not. These policies allow you to prevent data loss to untrusted or unmanaged applications. They prevent save as and cut/copy/paste abilities to unmanaged locations.

Ex. A user trying to upload a Teams document to their personal Gmail



Can't use work content here

Your organization doesn't allow you to use work content here.

Learn more

OK

```
no-reply               HostGator.com :: Payment Overdue - Hello Nick Ross, Your invoices (70568940,70576902) with HostGator are due. Please pay all outstanding invoice...
no-reply               HostGator.com :: Payment Overdue - Hello Nick Ross, Your invoices with HostGator are now 5 days past due. Please pay all outstanding invoices as s...
no-reply               HostGator - Payment Failure Notification - Hello Nick Ross, Your credit card ending in 7242 has been processed for $107.40 and was declined by our ...
Pinterest              Your Pin
no-reply               HostGatc
no-reply               HostGatc
LaunchPad (HostGato.   URGENT:
LaunchPad (HostGato.   Domain names expiring on Thursday, October 10, 2019 - Hello, Th
                       DOMAIN_LIST.txt
no-reply               HostGator - Payment Failure Notification - Hello Nick Ross, Your c
Reddit                 Human hearts have evolved for endurance, and we need it to stay
Amazon Accounts Pay.   KDP Royalty Payment Notification - NICHOLAS ROSS(DIM35) - 10
LaunchPad (HostGato.   Domain names expiring on Thursday, October 10, 2019 - Hello, Th
                       DOMAIN_LIST.txt
Google                 Security alert for your linked Google Account - Your account Thetr
HostGator Billing      Important Information Regarding Your Domain Registration - com,
Google Pay             You added a new card to your Google Account - Now you can use
Jake Kauffman          Rick-ConnectWise Automate Trial - Hey, How is the Trial for Conne
                       ConnectWise Automate trial - Hi Nick, I have been trying to reach
```

License Requirements:

- Microsoft 365 Business Premium $20/u/m

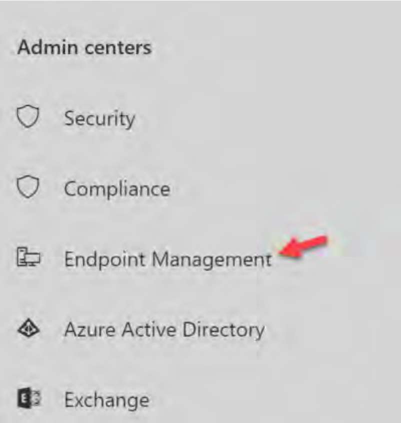
OVERVIEW & USER GUIDE

- Microsoft Enterprise Mobility + Security E3 $8.75/u/m
- Microsoft Intune $6/u/m

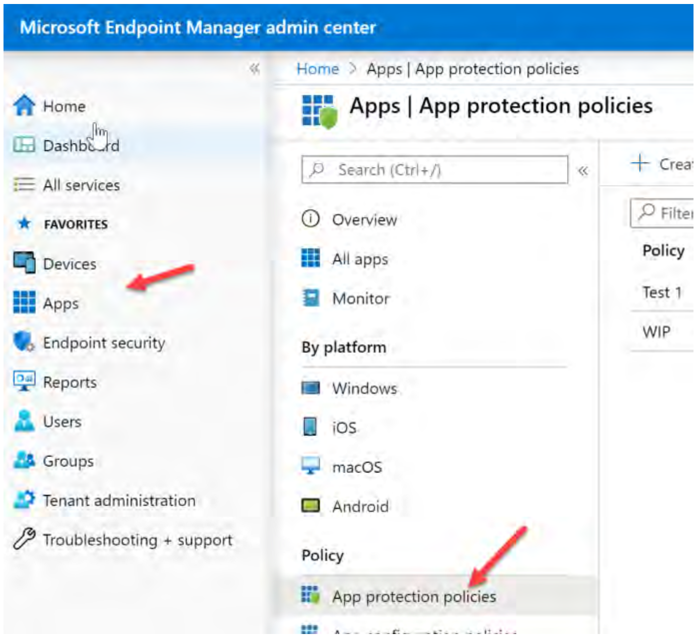
Compliance Controls:

- NIST CSF PR-DS-5
- CCS CSC 17
- COBIT 5 APO01.06
- ISA 62443-3-3:2013 SR 5.2
- ISO/IEC 27001:2013 A.6.1.2, A.7.1.1,
  - A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1,
  - A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5,
  - A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4,
  - A.14.1.2, A.14.1.3
- NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
- HIPAA Security Rule 45 C.F.R. §§
  - 164.308(a)(1)(ii)(D), 164.308(a)(3),
  - 164.308(a)(4)
  - 164.312(a), 164.312(e)

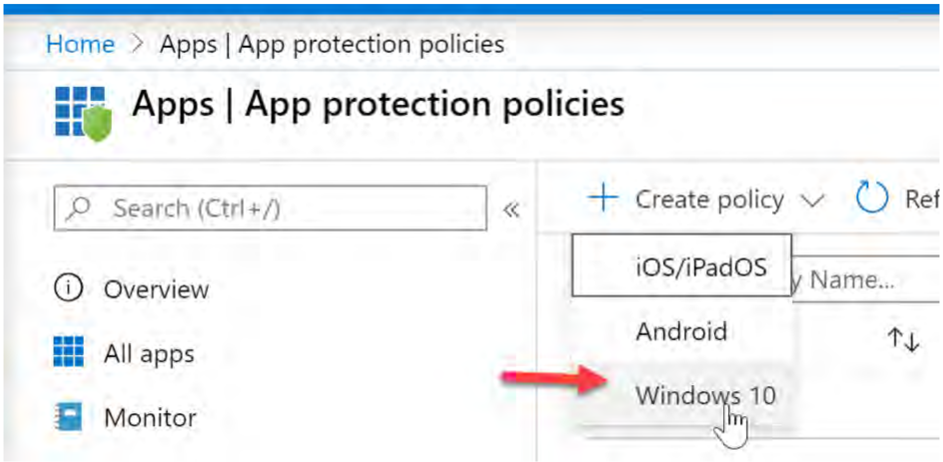
1. In the 365 Admin Center, click on Endpoint Manager



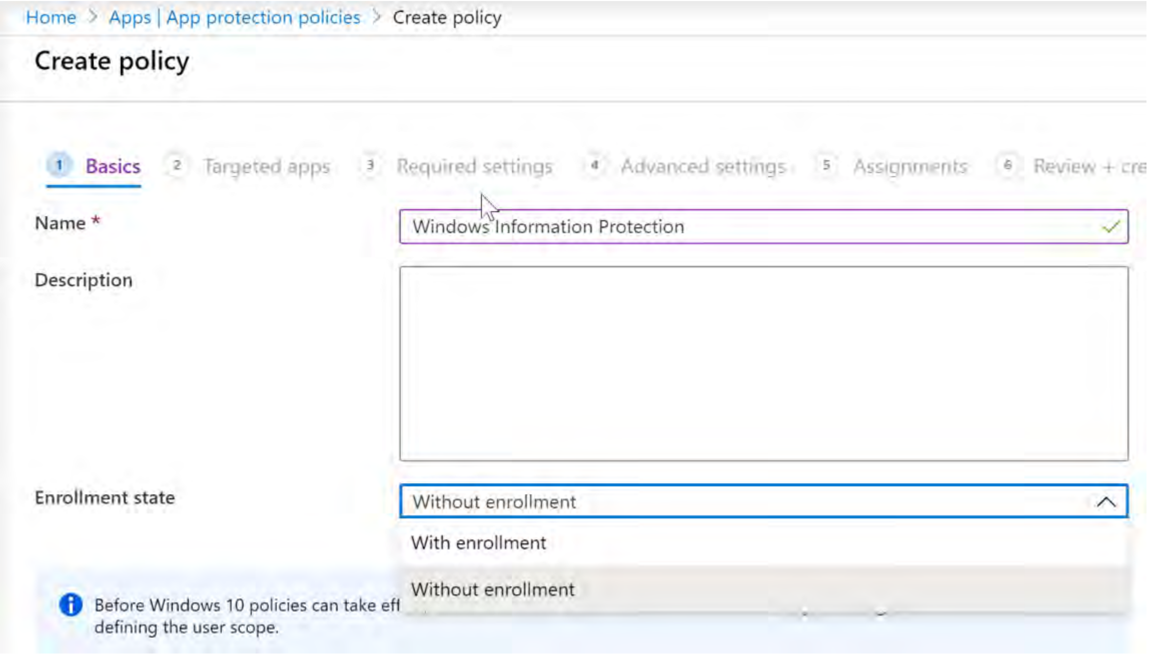
2. Click Apps>App Protection Policies



3. Click Create Policy>Windows 10 (We will only be covering Windows 10 in this guide)



4. Here you can name the policy and chose devices enrolled in Intune or not enrolled. For this example, we will choose not enrolled:



Home > Apps | App protection policies > Create policy

Create policy

1 Basics · 2 Targeted apps · 3 Required settings · 4 Advanced settings · 5 Assignments · 6 Review + cre

Name * Windows Information Protection

Description

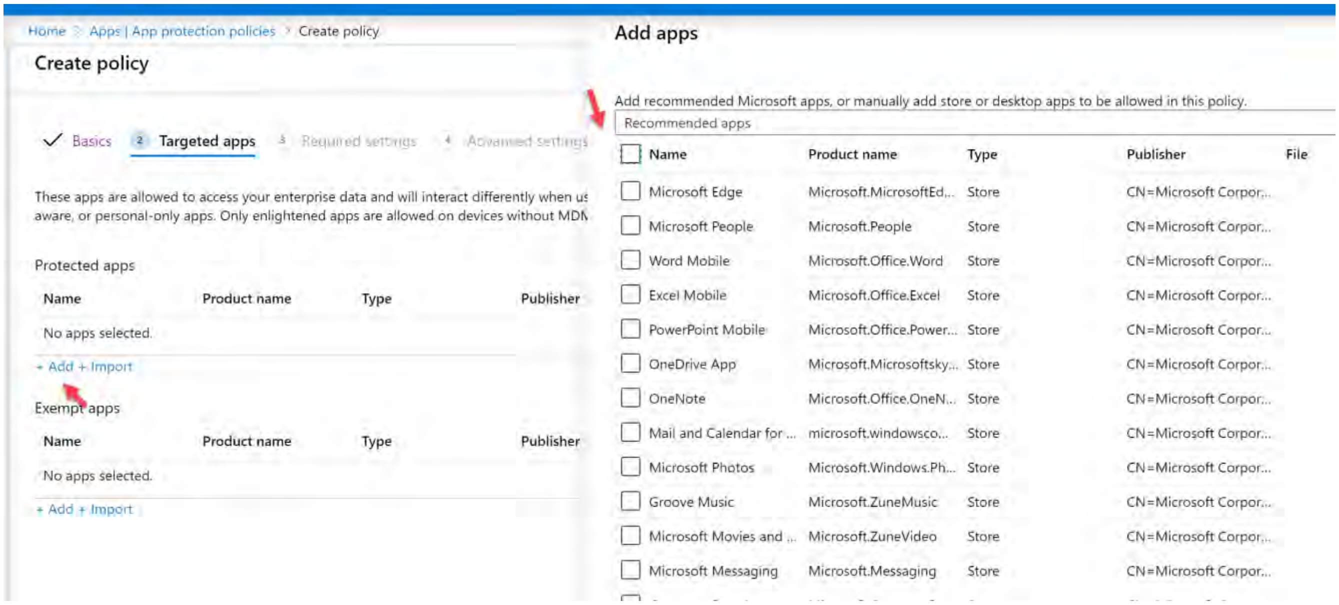
Enrollment state: Without enrollment

With enrollment

Without enrollment

Before Windows 10 policies can take eff defining the user scope.

5. Click +Add and add appropriate applications. At the minimum, add the entire Office suite. You can import third-party applications



Home > Apps | App protection policies > Create policy

Create policy

✓ Basics · 2 Targeted apps · 3 Required settings · 4 Advanced settings

These apps are allowed to access your enterprise data and will interact differently when us aware, or personal-only apps. Only enlightened apps are allowed on devices without MDN

Protected apps

Name	Product name	Type	Publisher
No apps selected.			

+ Add + Import

Exempt apps

Name	Product name	Type	Publisher
No apps selected.			

+ Add + Import

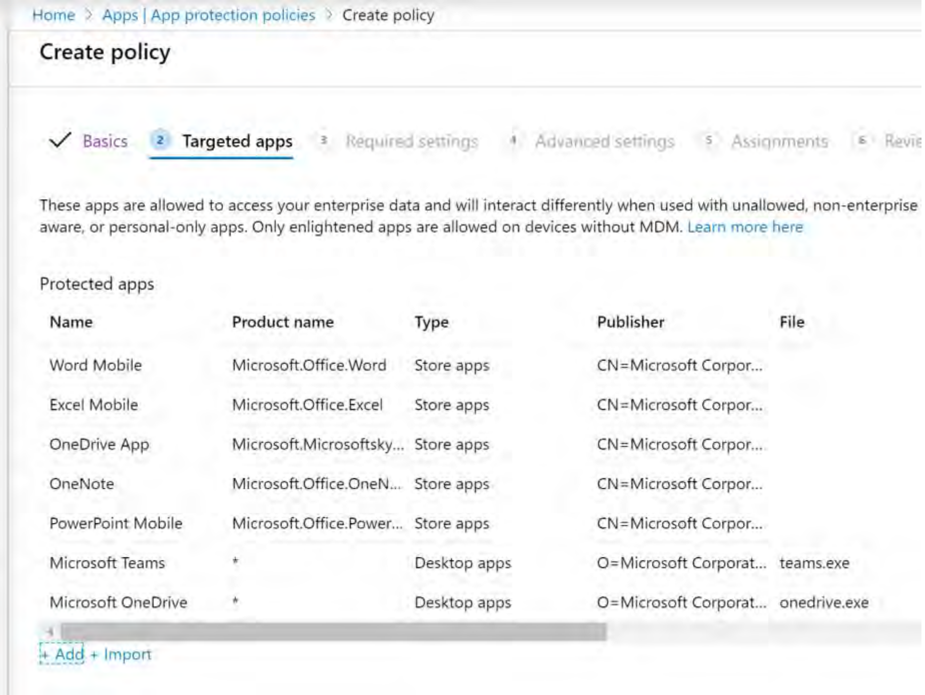
Add apps

Add recommended Microsoft apps, or manually add store or desktop apps to be allowed in this policy.

Recommended apps

□ Name	Product name	Type	Publisher	File
□ Microsoft Edge	Microsoft.MicrosoftEd...	Store	CN=Microsoft Corpor...	
□ Microsoft People	Microsoft.People	Store	CN=Microsoft Corpor...	
□ Word Mobile	Microsoft.Office.Word	Store	CN=Microsoft Corpor...	
□ Excel Mobile	Microsoft.Office.Excel	Store	CN=Microsoft Corpor...	
□ PowerPoint Mobile	Microsoft.Office.Power...	Store	CN=Microsoft Corpor...	
□ OneDrive App	Microsoft.Microsoftsky...	Store	CN=Microsoft Corpor...	
□ OneNote	Microsoft.Office.OneN...	Store	CN=Microsoft Corpor...	
□ Mail and Calendar for ...	microsoft.windowsco...	Store	CN=Microsoft Corpor...	
□ Microsoft Photos	Microsoft.Windows.Ph...	Store	CN=Microsoft Corpor...	
□ Groove Music	Microsoft.ZuneMusic	Store	CN=Microsoft Corpor...	
□ Microsoft Movies and ...	Microsoft.ZuneVideo	Store	CN=Microsoft Corpor...	
□ Microsoft Messaging	Microsoft.Messaging	Store	CN=Microsoft Corpor...	

6. When you are ready, click Next



Home > Apps | App protection policies > Create policy

Create policy

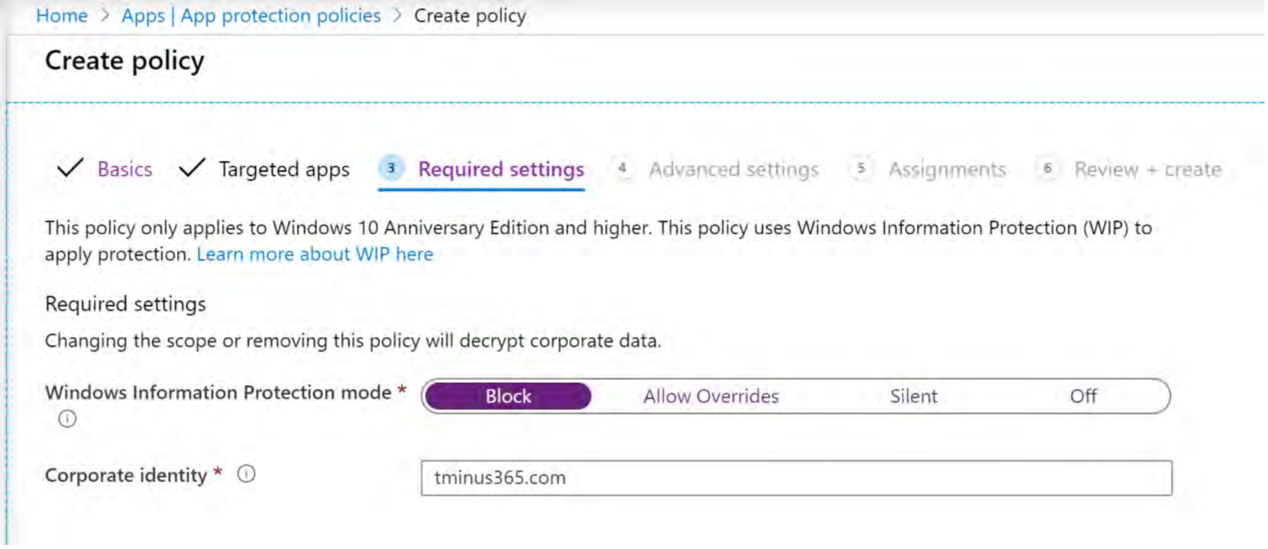
✓ Basics 2 Targeted apps 3 Required settings 4 Advanced settings 5 Assignments 6 Revie

These apps are allowed to access your enterprise data and will interact differently when used with unallowed, non-enterprise aware, or personal-only apps. Only enlightened apps are allowed on devices without MDM. Learn more here

Protected apps

Name	Product name	Type	Publisher	File
Word Mobile	Microsoft.Office.Word	Store apps	CN=Microsoft Corpor...	
Excel Mobile	Microsoft.Office.Excel	Store apps	CN=Microsoft Corpor...	
OneDrive App	Microsoft.Microsoftsky...	Store apps	CN=Microsoft Corpor...	
OneNote	Microsoft.Office.OneN...	Store apps	CN=Microsoft Corpor...	
PowerPoint Mobile	Microsoft.Office.Power...	Store apps	CN=Microsoft Corpor...	
Microsoft Teams	*	Desktop apps	O=Microsoft Corporat...	teams.exe
Microsoft OneDrive	*	Desktop apps	O=Microsoft Corporat...	onedrive.exe

7. Here we can choose what actions will be taken. Block prevents users from sharing data outside the trusted applications. Silent will collect log data without actually enforcing anything



Home > Apps | App protection policies > Create policy

Create policy

✓ Basics ✓ Targeted apps 3 Required settings 4 Advanced settings 5 Assignments 6 Review + create

This policy only applies to Windows 10 Anniversary Edition and higher. This policy uses Windows Information Protection (WIP) to apply protection. Learn more about WIP here

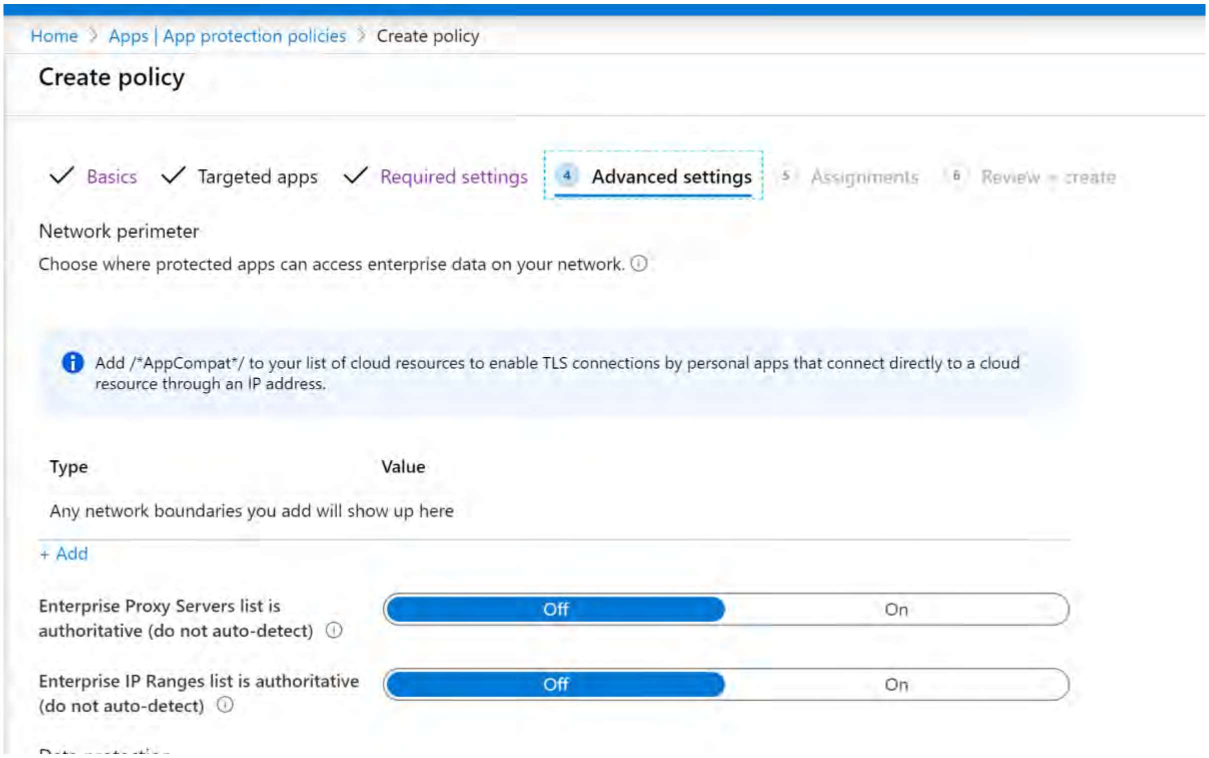
Required settings

Changing the scope or removing this policy will decrypt corporate data.

Windows Information Protection mode * ⓘ [✓ Block] Allow Overrides Silent Off

Corporate identity * ⓘ tminus365.com

8. We will not configure anything on the Advanced Settings page



Home > Apps | App protection policies > Create policy

Create policy

✓ Basics ✓ Targeted apps ✓ Required settings 4 Advanced settings 5 Assignments 6 Review + create

Network perimeter

Choose where protected apps can access enterprise data on your network. ⓘ

Add /*AppCompat*/ to your list of cloud resources to enable TLS connections by personal apps that connect directly to a cloud resource through an IP address.

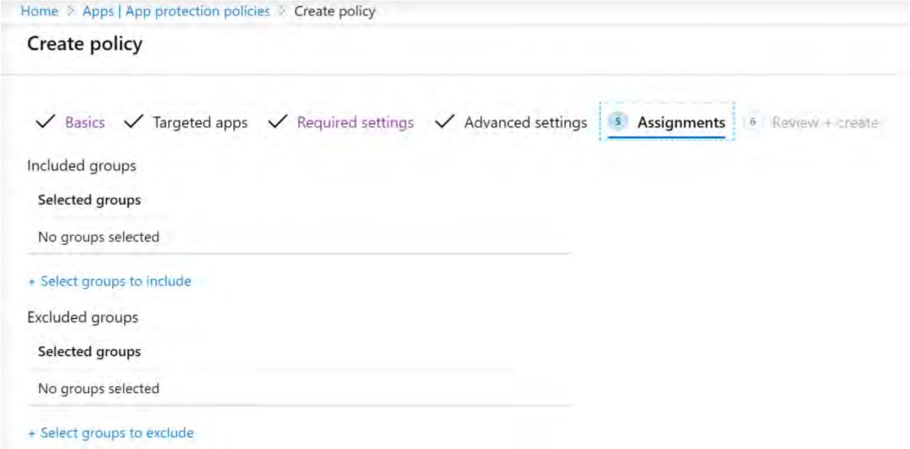
Type	Value
Any network boundaries you add will show up here	

+ Add

Enterprise Proxy Servers list is authoritative (do not auto-detect) ⓘ: [✓ Off] On

Enterprise IP Ranges list is authoritative (do not auto-detect) ⓘ: [✓ Off] On

9. Last, we can scope the policy to certain users and Create



Home > Apps | App protection policies > Create policy

Create policy

✓ Basics ✓ Targeted apps ✓ Required settings ✓ Advanced settings 5 Assignments 6 Review + create

Included groups

Selected groups
No groups selected

+ Select groups to include

Excluded groups

Selected groups
No groups selected

+ Select groups to exclude

OVERVIEW & USER GUIDE

Set up Data Loss Prevention Policies

Data loss prevention policies allow us to prevent the sharing of sensitive information across Teams chats. Policies come with pre-defined templates that can detect for certain information being shared like PII, credit card numbers, social security numbers, etc. The policies are granular in the fact that we can prevent users from sharing the information or we can allow overrides with business justification.

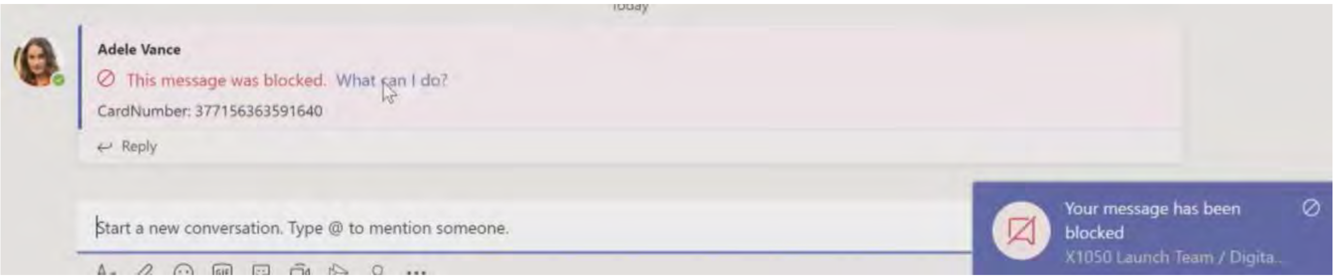
License Requirements:

- Microsoft 365 Business Premium $20/u/m
- Microsoft Office 365 E3 $20/u/m

Compliance Controls:

- NIST CSF PR-DS-5
- CCS CSC 17
- COBIT 5 APO01.06
- ISA 62443-3-3:2013 SR 5.2
- ISO/IEC 27001:2013 A.6.1.2, A.7.1.1,
  - A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1,
  - A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5,
  - A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4,
  - A.14.1.2, A.14.1.3
- NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
- HIPAA Security Rule 45 C.F.R. §§
  - 164.308(a)(1)(ii)(D), 164.308(a)(3),
  - 164.308(a)(4)
  - 164.312(a), 164.312(e)

Ex. User sending credit card information



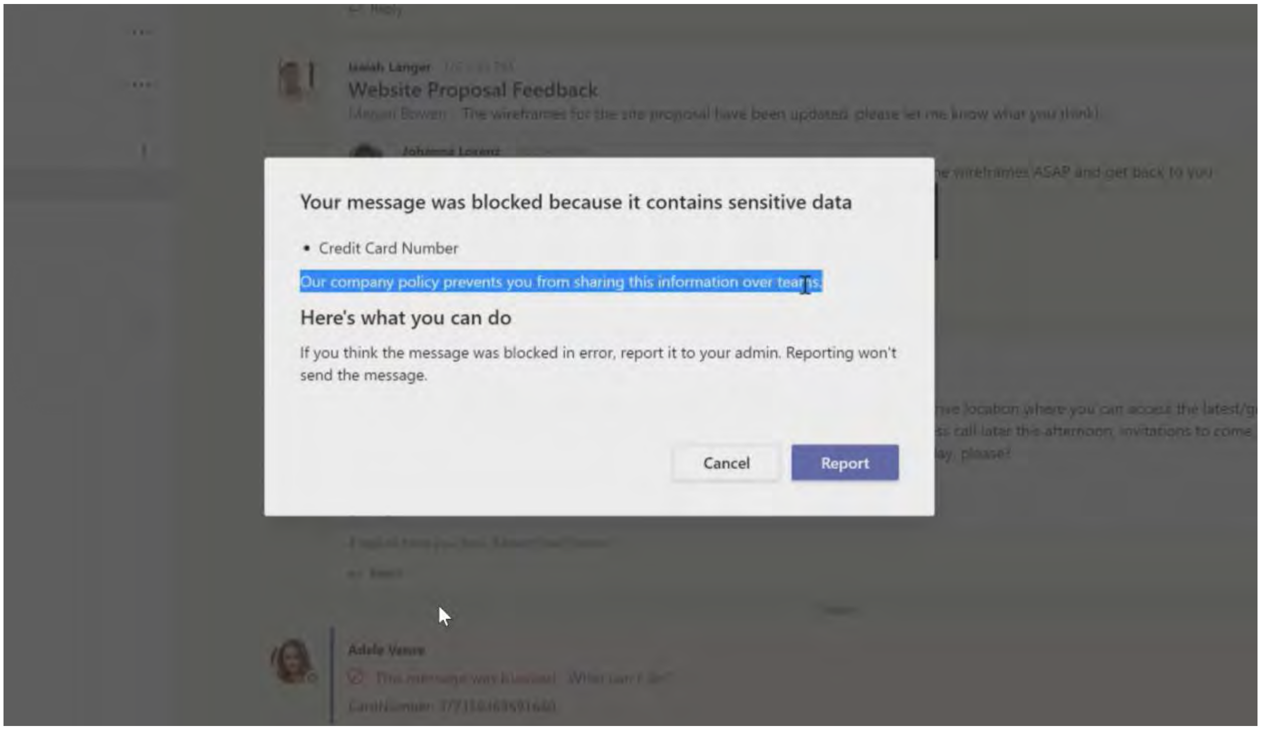
Adele Vance

This message was blocked. What can I do?

CardNumber: 377156363591640

Your message has been blocked

X1050 Launch Team / Digita...



Your message was blocked because it contains sensitive data

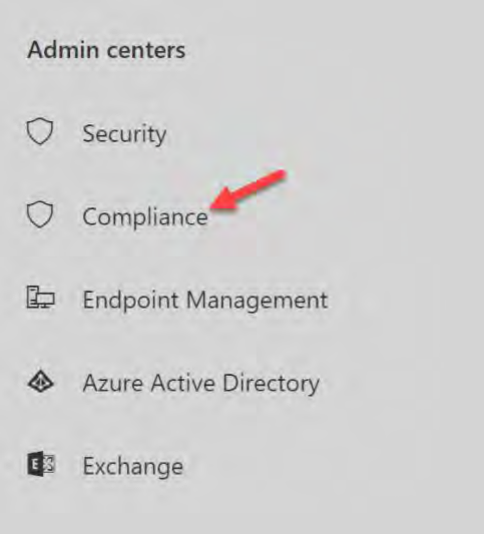
- Credit Card Number

Our company policy prevents you from sharing this information over teams.

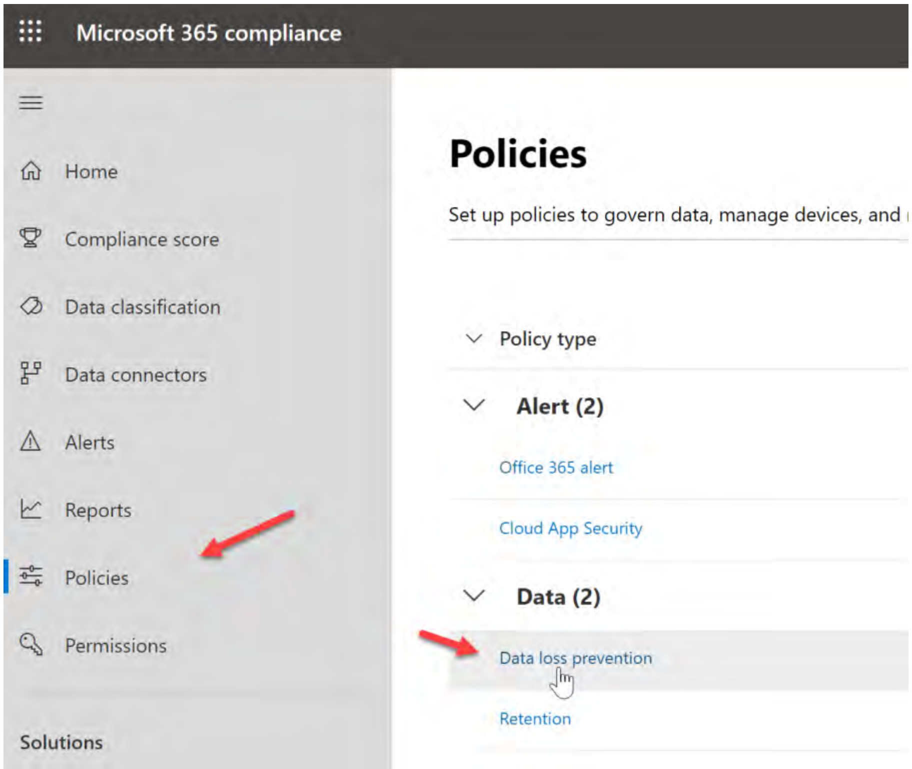
Here's what you can do

If you think the message was blocked in error, report it to your admin. Reporting won't send the message.

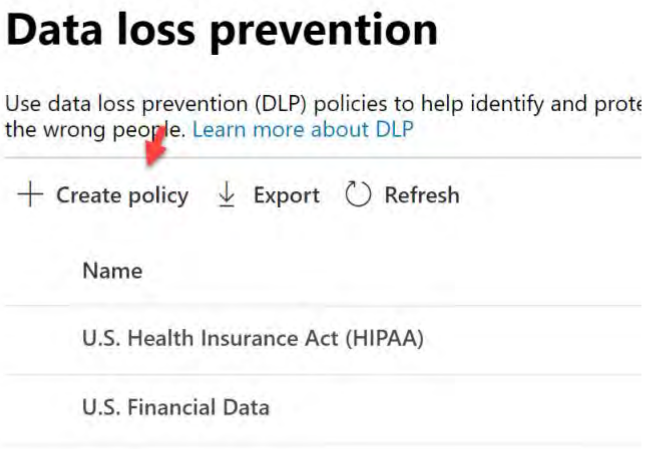
1. In the 365 Admin Center, click on Admin Centers>Compliance



2. Click Policies>Data Loss Prevention



3. Click Create Policy

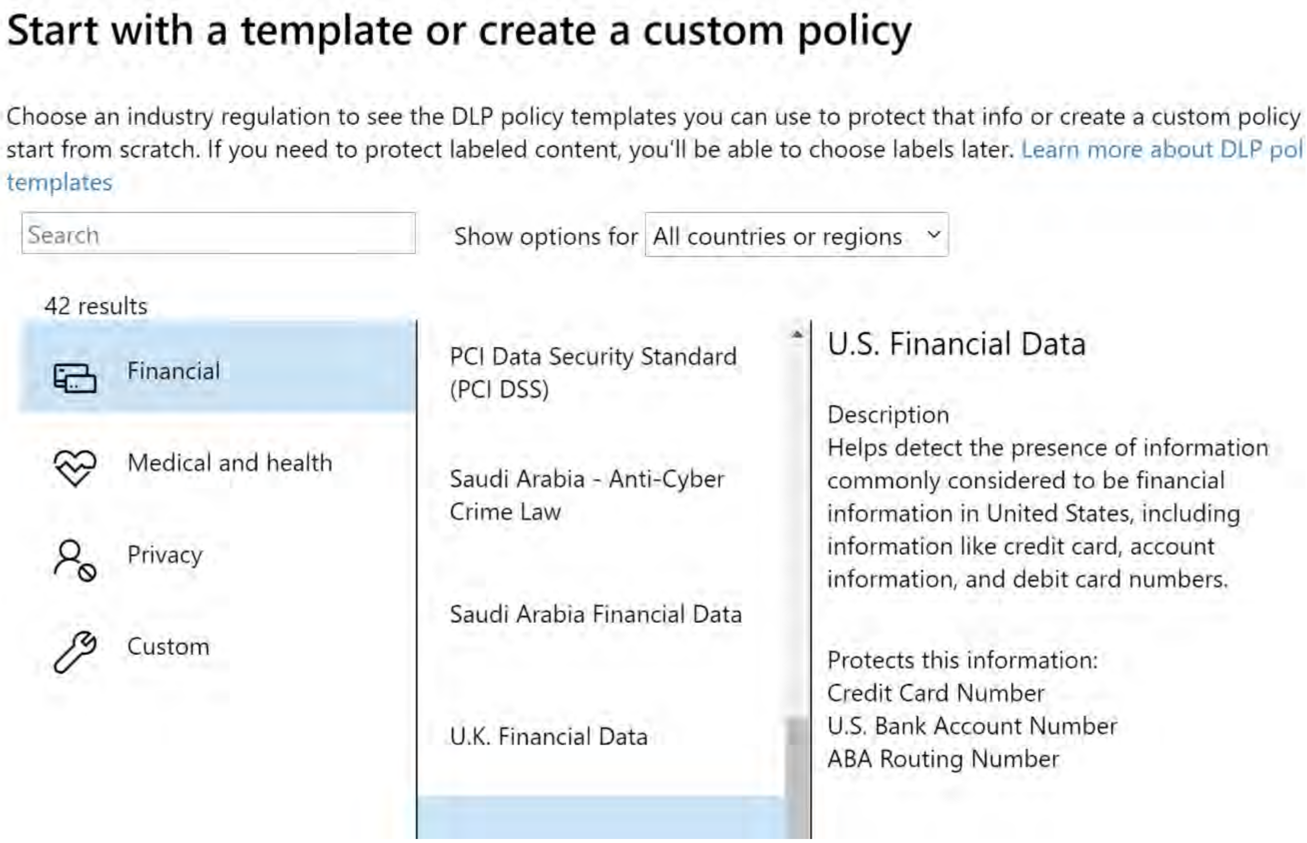


Data loss prevention

Use data loss prevention (DLP) policies to help identify and prote
the wrong people. Learn more about DLP

Name
U.S. Health Insurance Act (HIPAA)
U.S. Financial Data

4. Choose a template, if applicable



Start with a template or create a custom policy

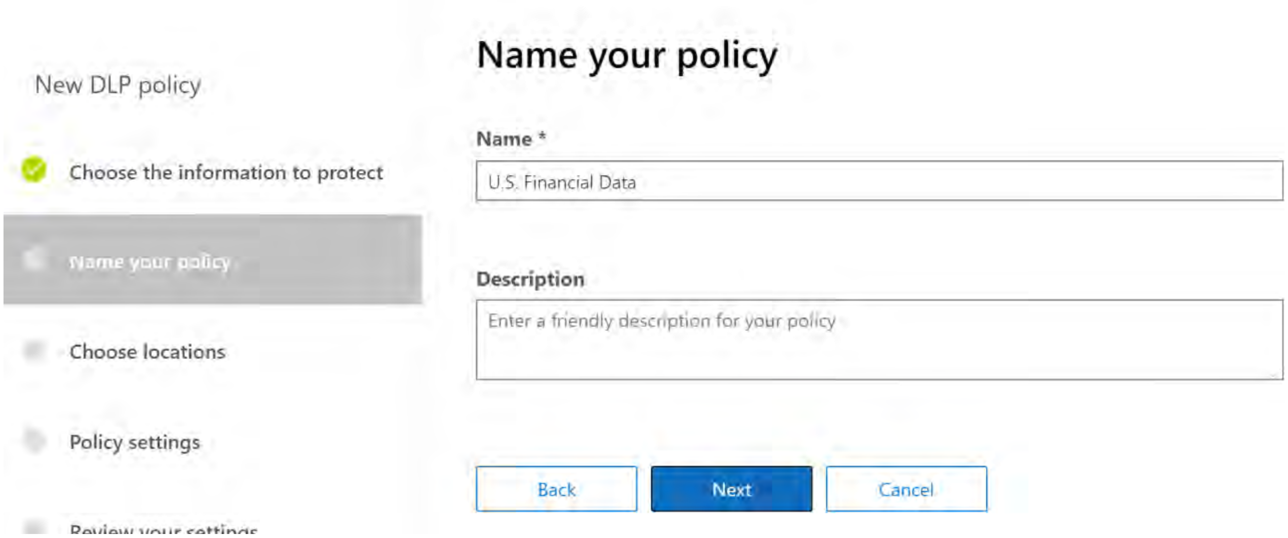
Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. Learn more about DLP pol templates

U.S. Financial Data

Description
Helps detect the presence of information commonly considered to be financial information in United States, including information like credit card, account information, and debit card numbers.

Protects this information:
Credit Card Number
U.S. Bank Account Number
ABA Routing Number

5. Add a name and description



Name your policy

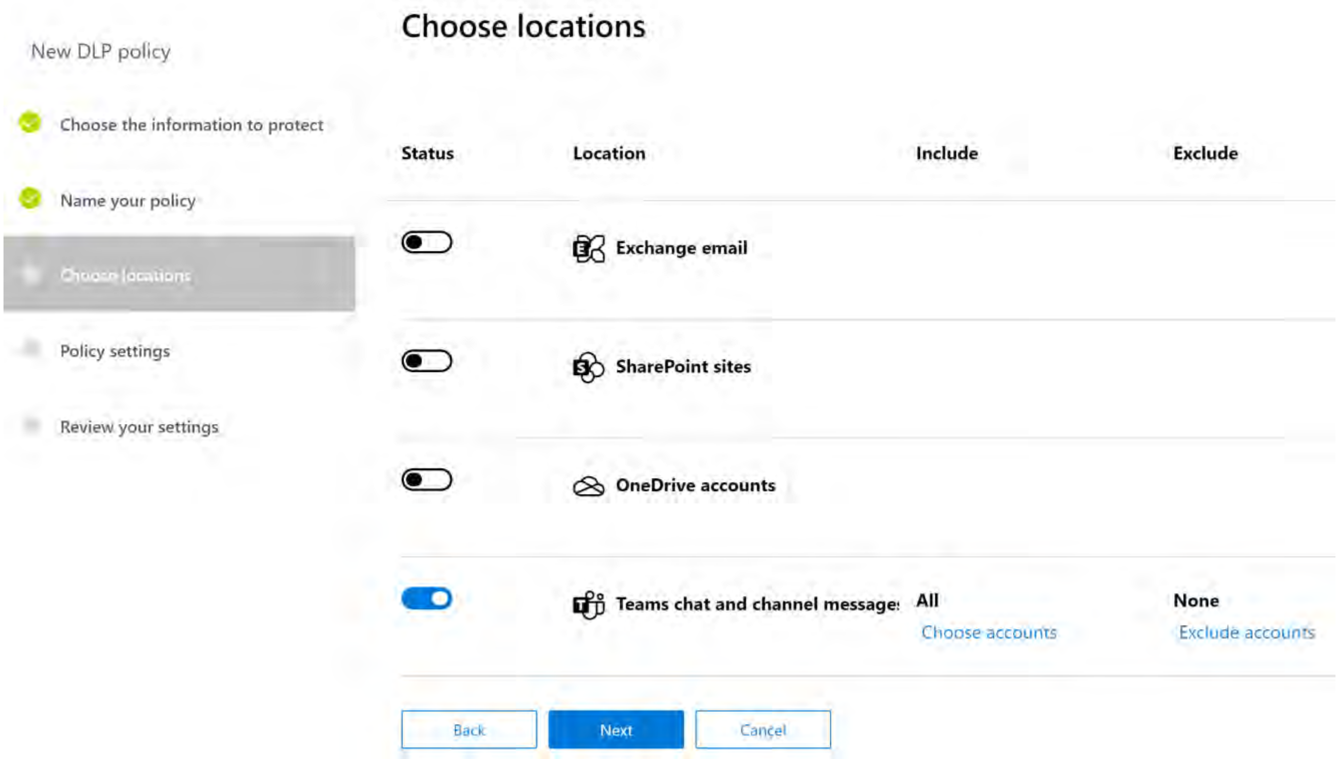
Name *

U.S. Financial Data

Description

Enter a friendly description for your policy

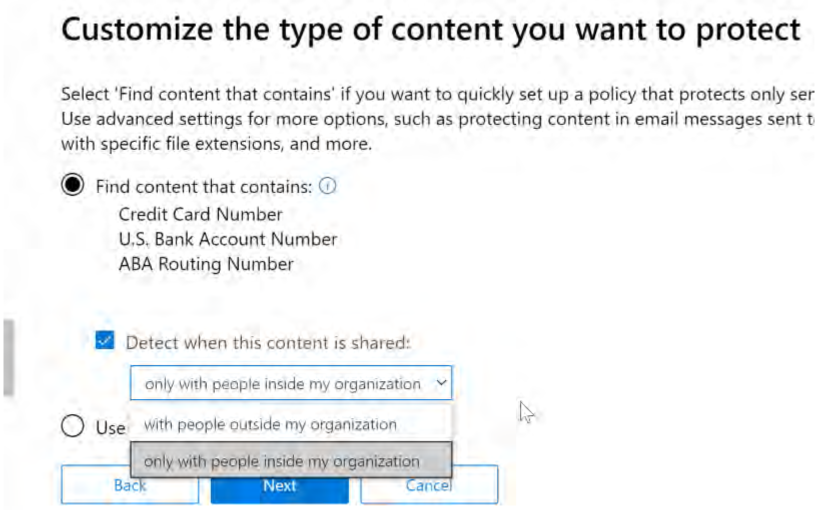
6. Choose Locations. *NOTE* You can scope this to certain users



Choose locations

Status	Location	Include	Exclude
Off	Exchange email		
Off	SharePoint sites		
Off	OneDrive accounts		
On	Teams chat and channel message:	All Choose accounts	None Exclude accounts

7. You can choose an external or internal policy here



Customize the type of content you want to protect

Select 'Find content that contains' if you want to quickly set up a policy that protects only ser
Use advanced settings for more options, such as protecting content in email messages sent t
with specific file extensions, and more.

● Find content that contains:
Credit Card Number
U.S. Bank Account Number
ABA Routing Number

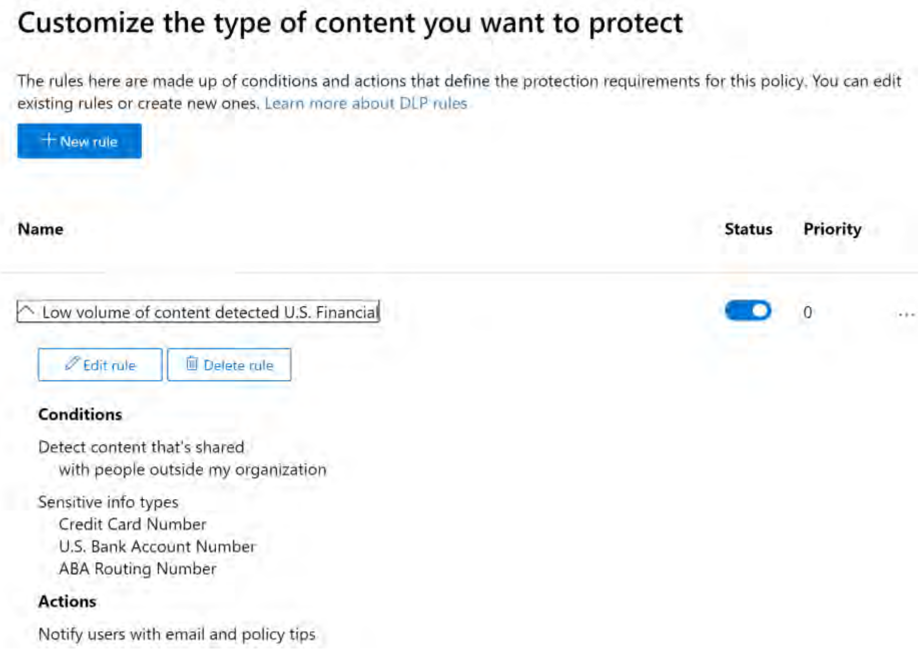
☑ Detect when this content is shared:

only with people inside my organization

○ Use

with people outside my organization
only with people inside my organization
Back
Next
Cancel

8. If you choose the advanced settings, you can modify the rules or create new rules



Customize the type of content you want to protect

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones. Learn more about DLP rules

Name	Status	Priority
Low volume of content detected U.S. Financial	On	0

Conditions

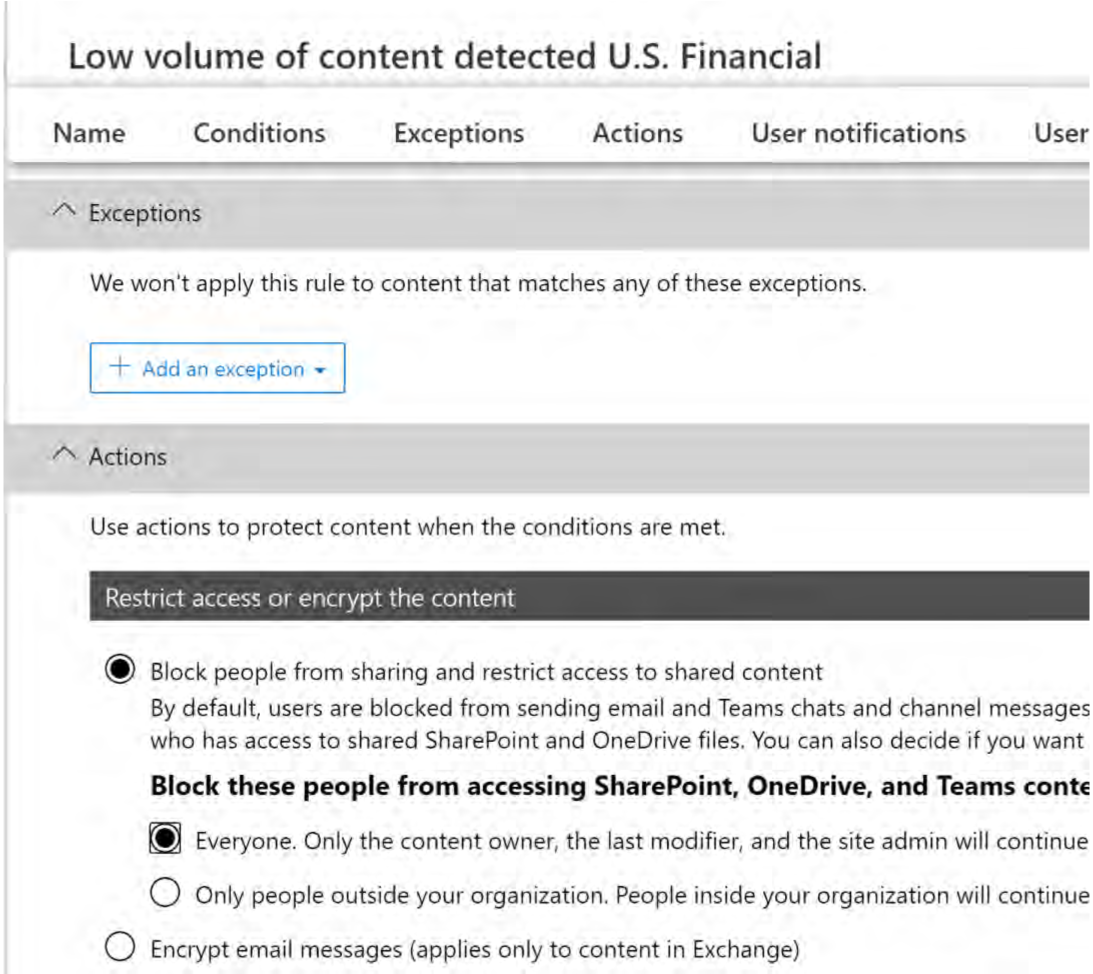
Detect content that's shared
with people outside my organization

Sensitive info types
Credit Card Number
U.S. Bank Account Number
ABA Routing Number

Actions

Notify users with email and policy tips

9. If you edit one of the rules you can set the actions that apply to the user such as blocking the message, allowing override, setting the policy tip, etc.



Low volume of content detected U.S. Financial

^ Exceptions

We won't apply this rule to content that matches any of these exceptions.

^ Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content

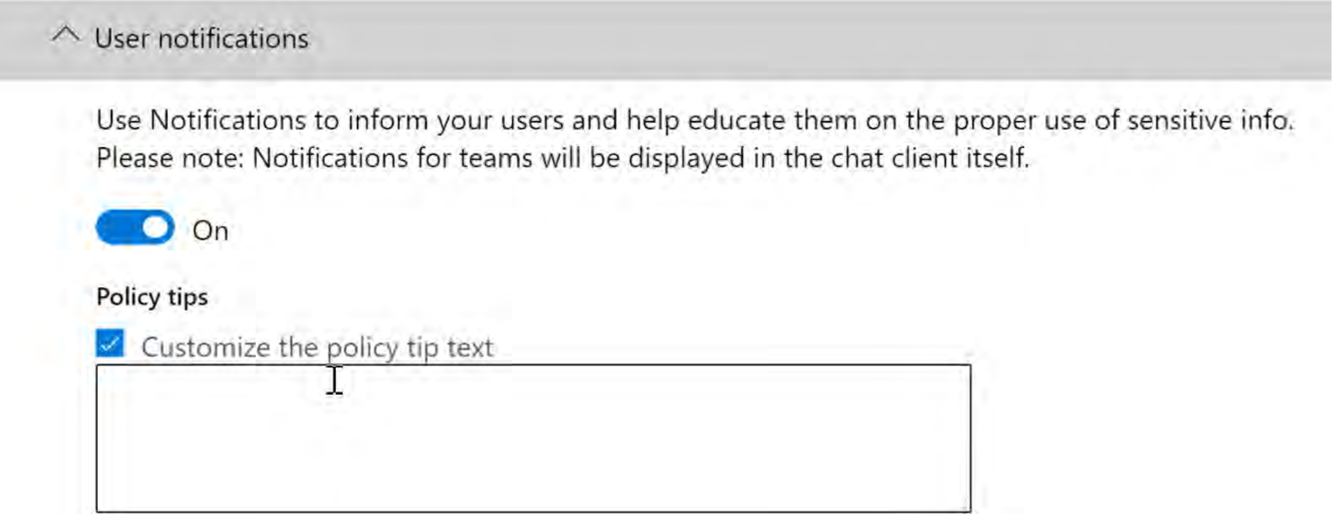
● Block people from sharing and restrict access to shared content
By default, users are blocked from sending email and Teams chats and channel messages
who has access to shared SharePoint and OneDrive files. You can also decide if you want

Block these people from accessing SharePoint, OneDrive, and Teams conte

● Everyone. Only the content owner, the last modifier, and the site admin will continue

○ Only people outside your organization. People inside your organization will continue

○ Encrypt email messages (applies only to content in Exchange)



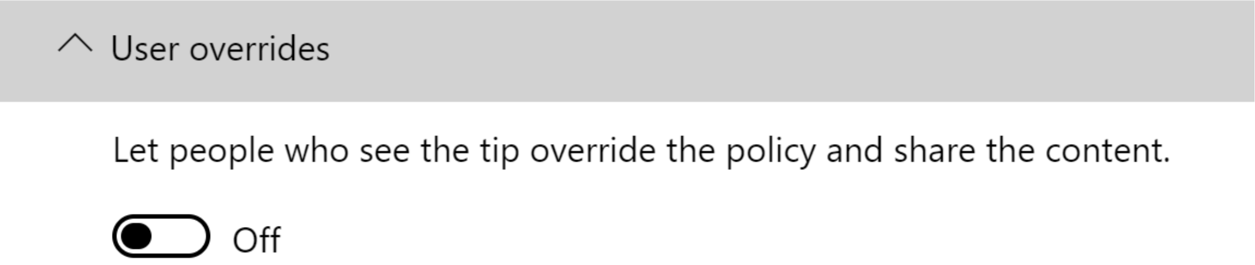
User notifications

Use Notifications to inform your users and help educate them on the proper use of sensitive info. Please note: Notifications for teams will be displayed in the chat client itself.

On

Policy tips

☑ Customize the policy tip text

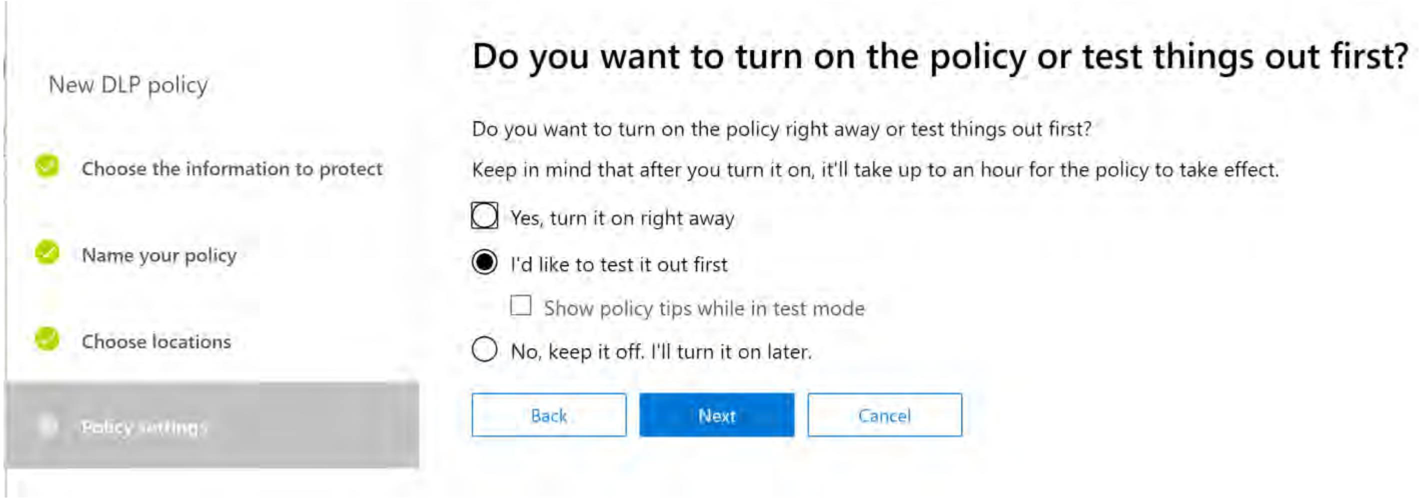


User overrides

Let people who see the tip override the policy and share the content.

Off

10. You can choose to turn it on right away or test it out to better understand impact. After you decide, you can create the policy



Do you want to turn on the policy or test things out first?

Do you want to turn on the policy right away or test things out first?

Keep in mind that after you turn it on, it'll take up to an hour for the policy to take effect.

○ Yes, turn it on right away

● I'd like to test it out first

□ Show policy tips while in test mode

○ No, keep it off. I'll turn it on later.

SHAREPOINT AND ONEDRIVE

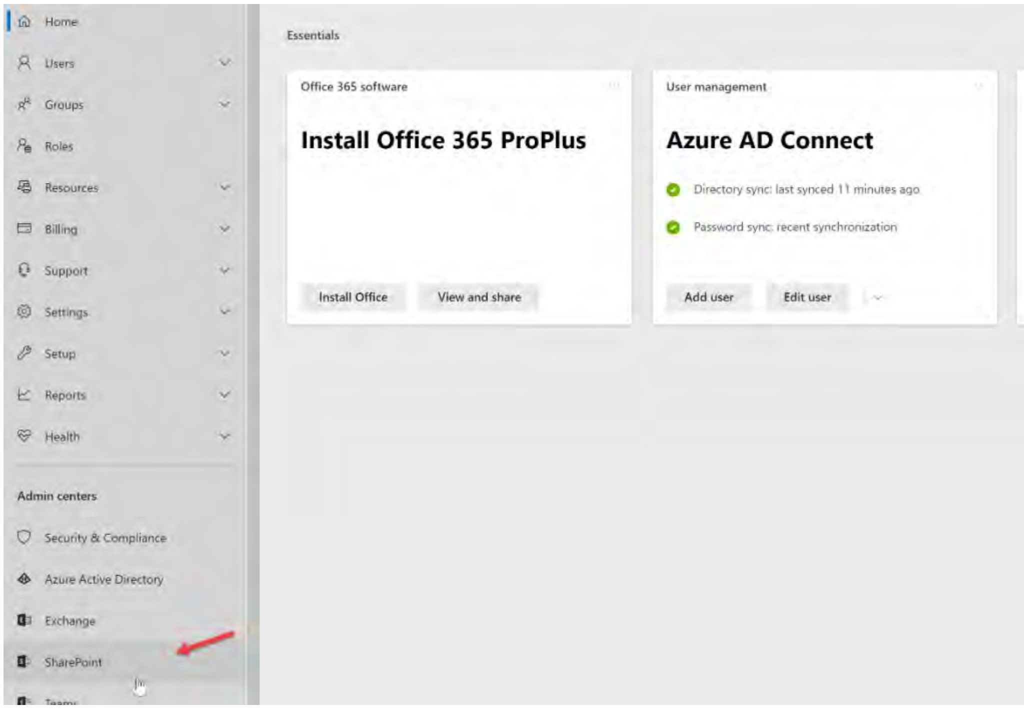
Configure Expiration Time for External Sharing Links

You should restrict the length of time that anonymous access links are valid. An attacker can compromise a user account for a short period of time, send anonymous sharing links to an external account, then take their time accessing the data. They can also compromise external accounts and steal the anonymous sharing links sent to those external entities well after the data has been shared.

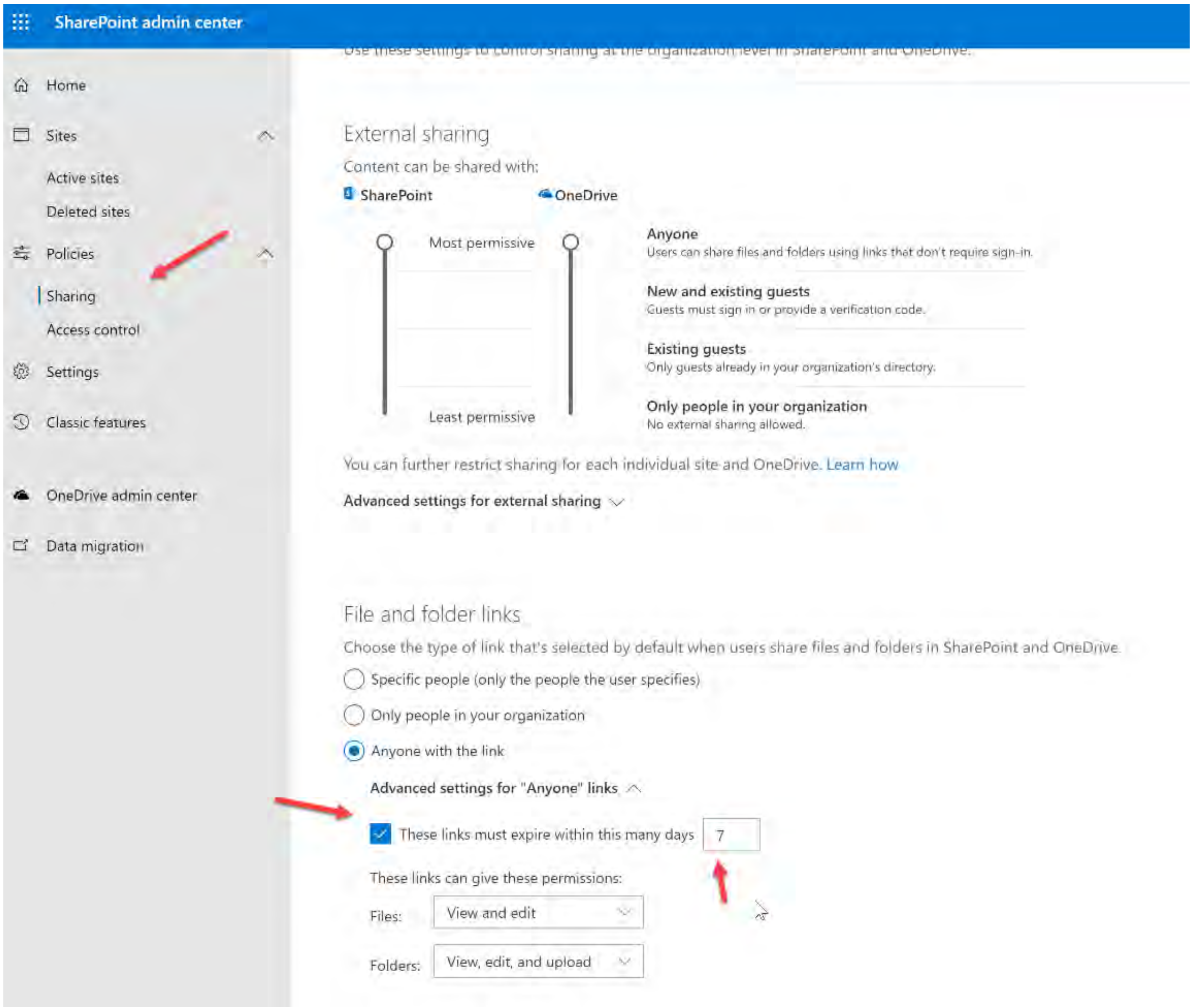
Compliance Controls

- FedRAMP Moderate; Control AC-21(a)
- NIST 800-53; Control AC-21(a)

1. Go to Admin Centers>SharePoint



2. Expand the Policies tab and click on Sharing. From here you can set the number of days in which links expire



SharePoint admin center

Use these settings to control sharing at the organization level in SharePoint and OneDrive.

External sharing

Content can be shared with:

SharePoint OneDrive

Most permissive

Least permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. Learn how

Advanced settings for external sharing

File and folder links

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

○ Specific people (only the people the user specifies)

○ Only people in your organization

● Anyone with the link

Advanced settings for "Anyone" links

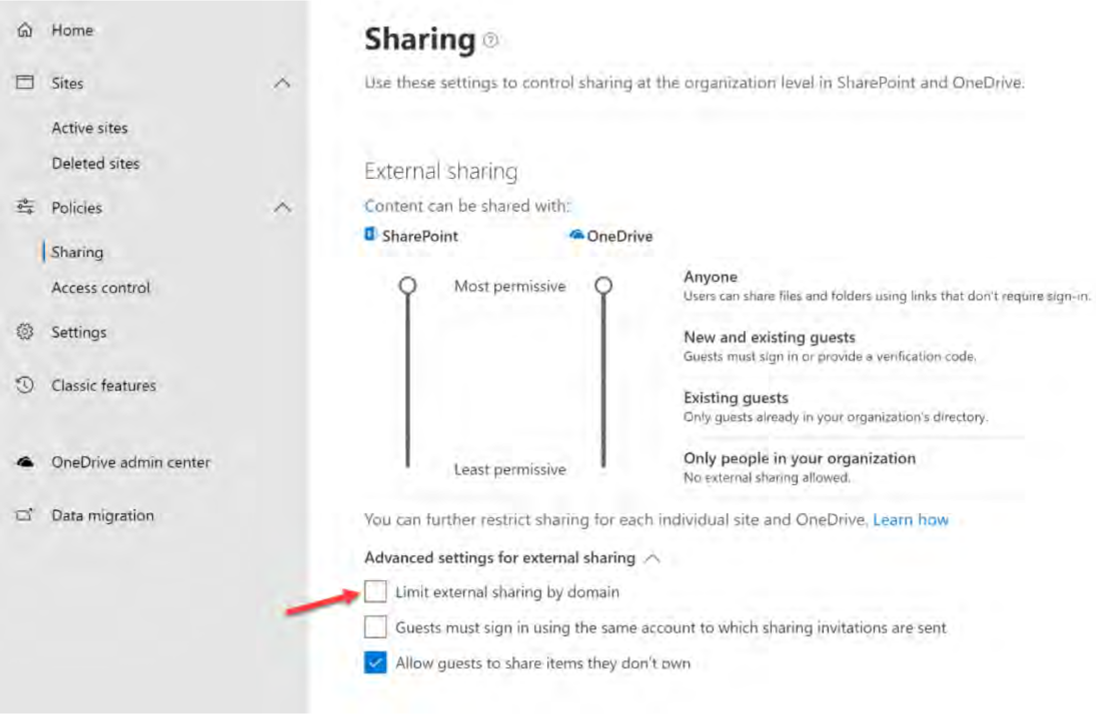
☑ These links must expire within this many days 7

These links can give these permissions:

Files: View and edit

Folders: View, edit, and upload

3. If you expand the Advanced Settings for External Sharing you could get more restrictive to your sharing permissions and only limit them to certain domains



Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive.

External sharing

Content can be shared with:

SharePoint OneDrive

Most permissive

Least permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. Learn how

Advanced settings for external sharing

☐ Limit external sharing by domain

☐ Guests must sign in using the same account to which sharing invitations are sent

☑ Allow guests to share items they don't own

4. Set Links to Expire with PowerShell. **NOTE** Modify the script if you want something other than 7 days. In some cases, 30 days may be more appropriate

PowerShell Script

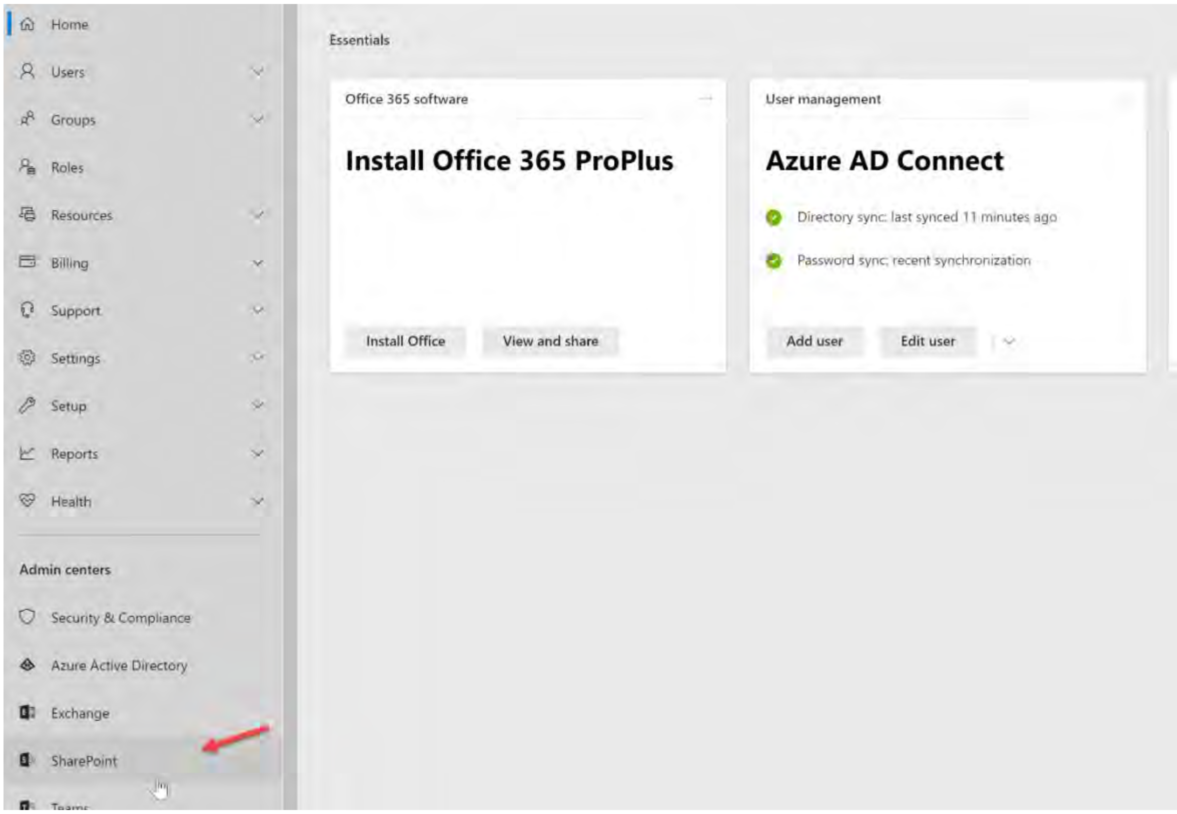
Enable Versioning on all SharePoint Online Document Libraries

You should enable versioning on all of your SharePoint online site collection document libraries. This will ensure that accidental or malicious changes to document content can be recovered. **Note** By default creating major versions (1.0, 2.0, etc.) is on. If you want to enable major and minor versions (1.1, 1.2, etc.) then you will need to follow the steps below.

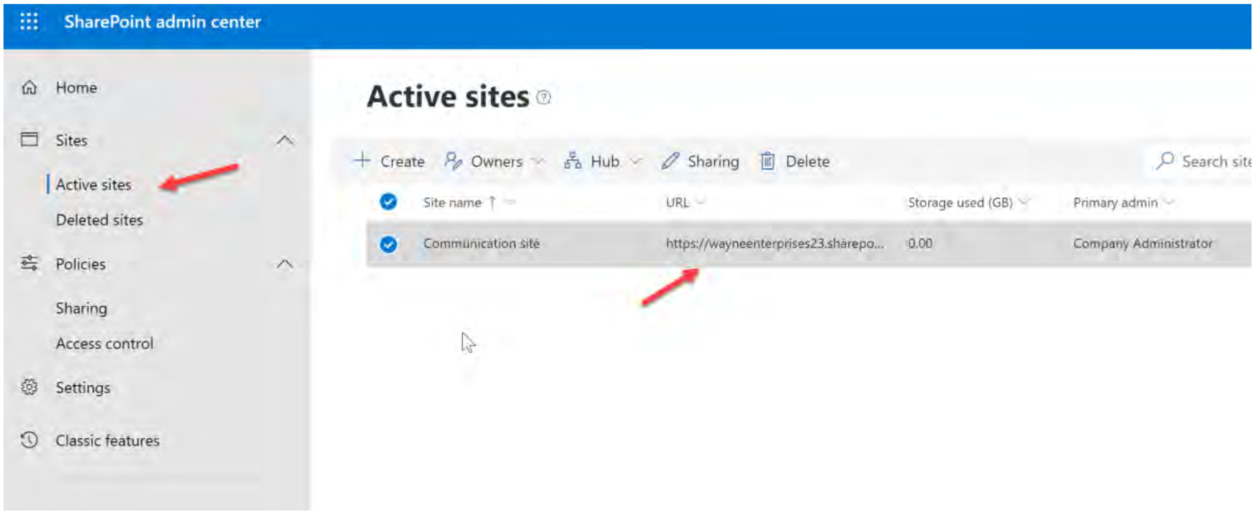
Compliance Controls

- GDPR; Control 6.9.2
- NIST CSF; Control PR.IP-4

1. Go to Admin Centers>SharePoint

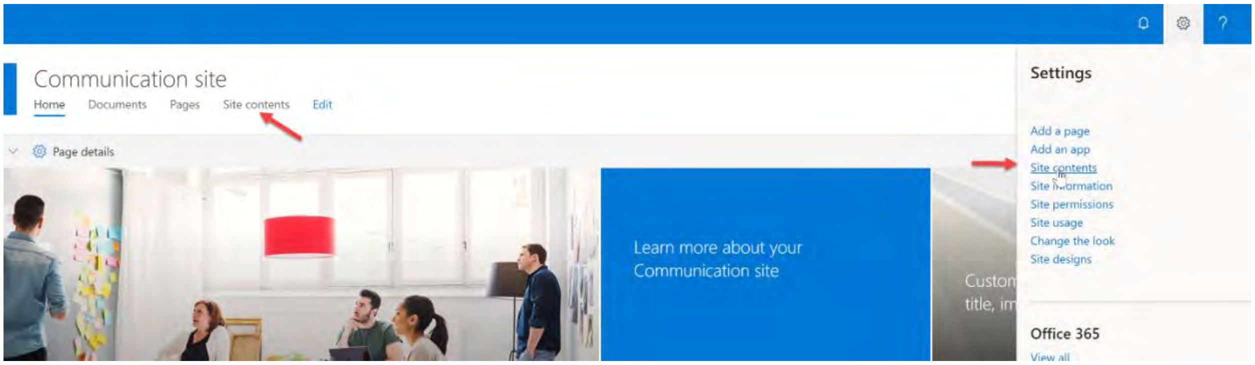


2. Go to one of the sites you want to configure versioning on

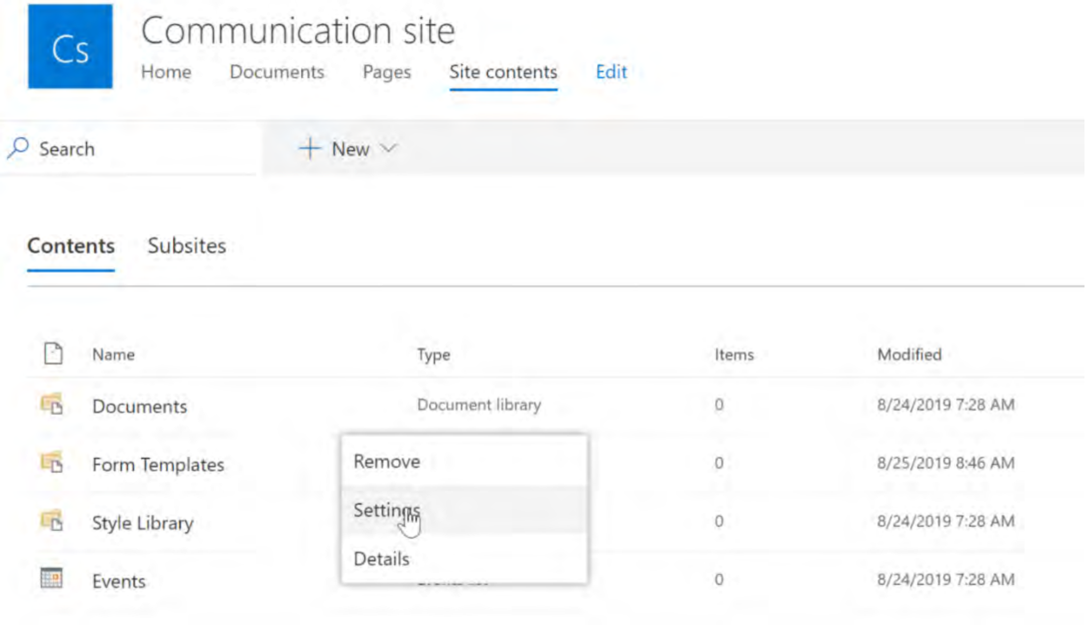


Site name ↑	URL	Storage used (GB)	Primary admin
Communication site	https://wayneenterprises23.sharepo...	0.00	Company Administrator

3. Go to Settings>Site Contents

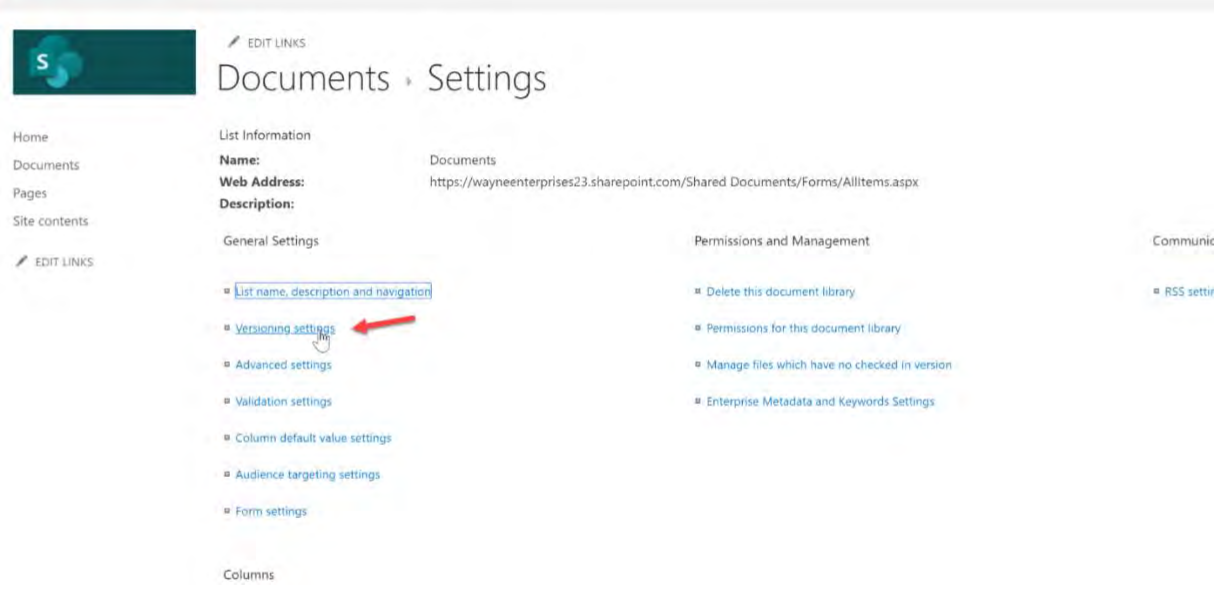


4. Next, click on the 3 dots next to a document library you want to modify and click Settings



Name	Type	Items	Modified
Documents	Document library	0	8/24/2019 7:28 AM
Form Templates		0	8/25/2019 8:46 AM
Style Library		0	8/24/2019 7:28 AM
Events		0	8/24/2019 7:28 AM

5. Select Versioning Settings



List Information

Name: Documents

Web Address: https://wayneenterprises23.sharepoint.com/Shared Documents/Forms/AllItems.aspx

Description:

General Settings

- List name, description and navigation
- Versioning settings
- Advanced settings
- Validation settings
- Column default value settings
- Audience targeting settings
- Form settings

Permissions and Management

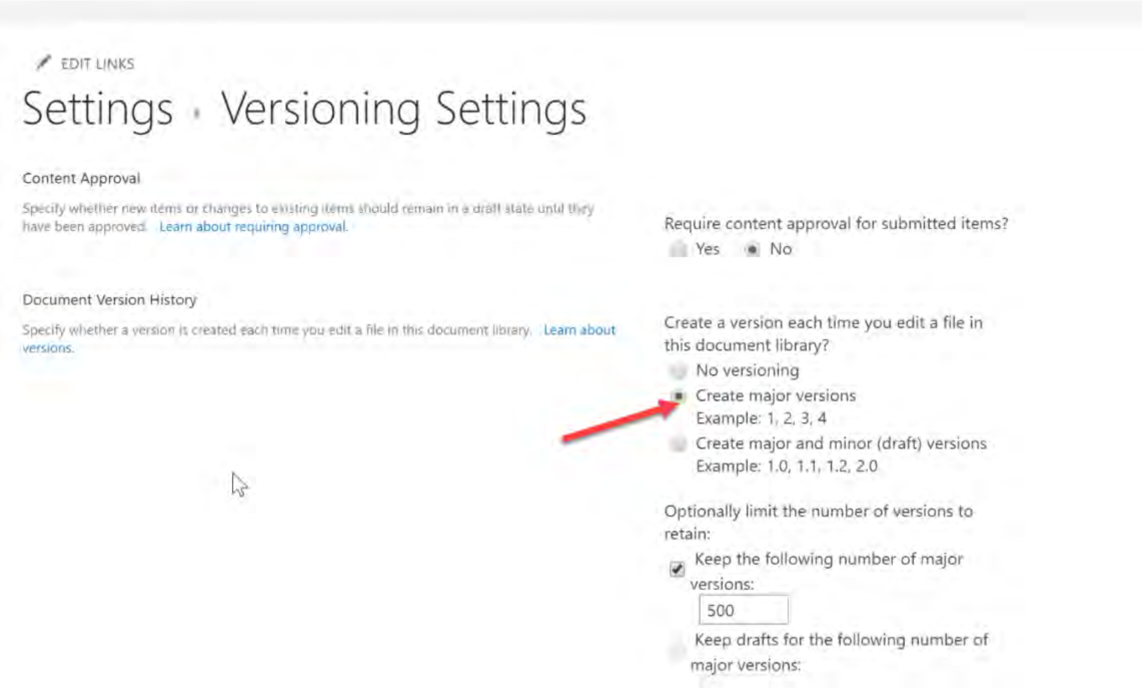
- Delete this document library
- Permissions for this document library
- Manage files which have no checked in version
- Enterprise Metadata and Keywords Settings

Communic

- RSS settir

Columns

6. Ensure Versioning is enabled



EDIT LINKS

Settings › Versioning Settings

Content Approval

Specify whether new items or changes to existing items should remain in a draft state until they have been approved. Learn about requiring approval.

Require content approval for submitted items?

○ Yes ● No

Document Version History

Specify whether a version is created each time you edit a file in this document library. Learn about versions.

Create a version each time you edit a file in this document library?

○ No versioning

● Create major versions
Example: 1, 2, 3, 4

○ Create major and minor (draft) versions
Example: 1.0, 1.1, 1.2, 2.0

Optionally limit the number of versions to retain:

☑ Keep the following number of major versions:
500

□ Keep drafts for the following number of major versions:

PowerShell

1. Enable versioning for all lists and libraries for a site PowerShell

   [PowerShell Script]

Adopt the OneDrive Sync Client

Storing user documents in OneDrive for Business safeguards content against data loss. Keeping documents on local client machines leaves them vulnerable to malware attacks like Ransomware that destroy or leak that data. OneDrive for Business gives you an effective backup and restore mechanism to recover from an attack on your locally stored documents. Getting your users to adopt the sync client helps you prevent data loss, takes up less storage on their devices from files on demand, and allows them to easy migrate to a new workstation and have all of their files readily available.

Compliance Controls

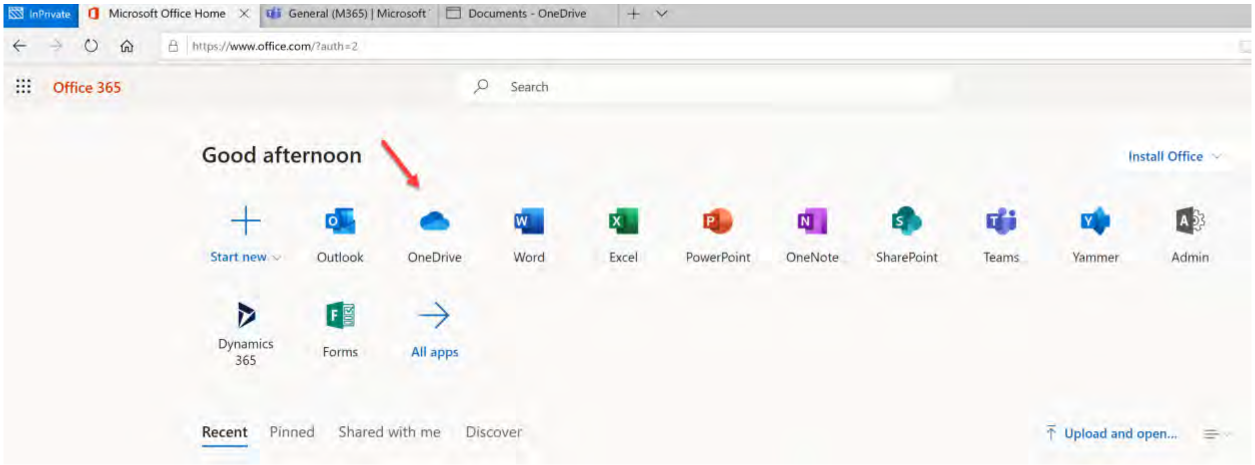
- FedRAMP Moderate; Control SC-8
- HIPAA; Control 45 C.F.R. § 164.312(a)(2)(iv), Control 45 C.F.R. § 164.312(e)(1), Control 45 C.F.R. § 164.312(e)(2)(i)
- ISO 27001:2013; Control A.13.2.3
- NIST 800-171; Control 3.13.8
- NIST 800-53; Control SC-8

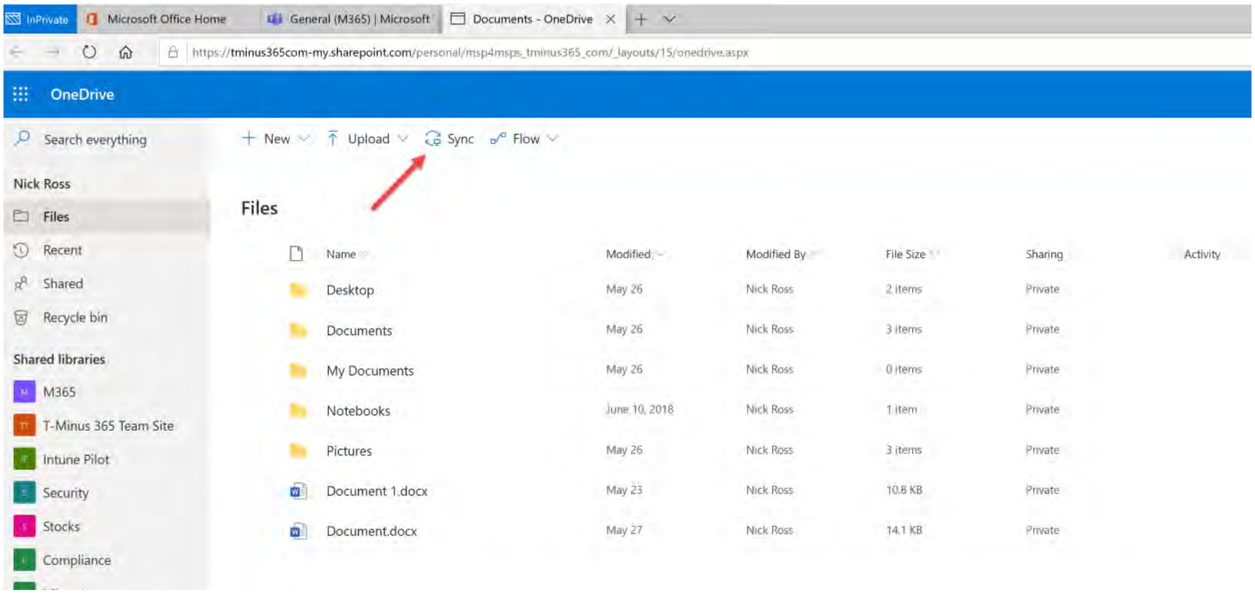
  https://support.office.com/en-us/article/sync-files-with-the-onedrive-sync-client-in-windows-615391c4-2bd3-4aae-a42a-858262e42a49

1. If you are still in a hybrid environment with Active Directory, you can use Group Policy to silently sync users OneDrive with their Windows Credentials. The steps are defined in the following support article:

   https://docs.microsoft.com/en-us/onedrive/use-group-policy

2. Users can also sync their OneDrive Libraries from within the webapp itself. If they login to office.com and go to the OneDrive application, they will have the Sync button at the top of the page



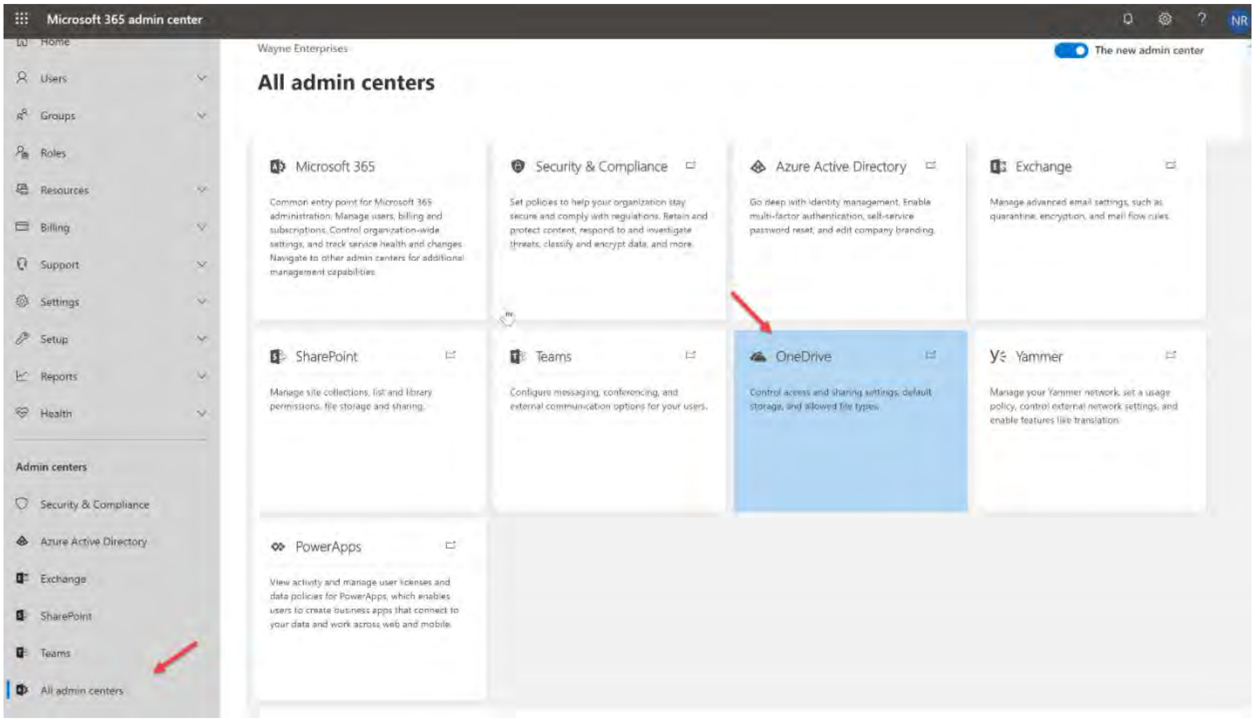


Files

Name	Modified	Modified By	File Size	Sharing	Activity
Desktop	May 26	Nick Ross	2 items	Private	
Documents	May 26	Nick Ross	3 items	Private	
My Documents	May 26	Nick Ross	0 items	Private	
Notebooks	June 10, 2018	Nick Ross	1 item	Private	
Pictures	May 26	Nick Ross	3 items	Private	
Document 1.docx	May 23	Nick Ross	10.8 KB	Private	
Document.docx	May 27	Nick Ross	14.1 KB	Private	

OVERVIEW & USER GUIDE

3. If you would like to get more restrictive with the ability to access OneDrive files, you could restrict access based on certain IP ranges. If you go into the 365 Admin Center>Admin Center>All Admin Centers>OneDrive, you will have the Device Access tab in which you can define IP ranges for their local network



All admin centers

Microsoft 365

Common entry point for Microsoft 365 administration. Manage users, billing and subscriptions. Control organization-wide settings, and track service health and changes. Navigate to other admin centers for additional management capabilities.

Security & Compliance

Set policies to help your organization stay secure and comply with regulations. Retain and protect content, respond to and investigate threats, classify and encrypt data, and more.

Azure Active Directory

Go deep with identity management. Enable multi-factor authentication, self-service password reset, and edit company branding.

Exchange

Manage advanced email settings, such as quarantine, encryption, and mail flow rules.

SharePoint

Manage site collections, list and library permissions, file storage and sharing.

Teams

Configure messaging, conferencing, and external communication options for your users.

OneDrive

Control access and sharing settings, default storage, and allowed file types.

Yammer

Manage your Yammer network, set a usage policy, control external network settings, and enable features like translation.

PowerApps

View activity and manage user licenses and data policies for PowerApps, which enables users to create business apps that connect to your data and work across web and mobile.

CONCLUSION

I hope this article provided you some targeted guidance on Securing Microsoft Teams. Any feedback to improve this guide further would be greatly appreciated and can be sent to the following email:

feedback@pax8.com

For all other questions or additional assistance, please reach out to your CSA or our support team:

Support (Existing Partners Only)

- Support: 1-855-884-7298 Ext. 3
- Email: support@pax8.com
- Hours: 24/7