



SECURING MICROSOFT TEAMS

OVERVIEW AND USER GUIDE

Nick Ross | Microsoft Certified Expert Administrator

OVERVIEW & USER

PURPOSE

This document is a guide to show how to harden Microsoft Teams environments. The controls provided here are recommendations and should be evaluated before being implemented in any customer environment.

AUDIENCE

This guide was written for Pax8 Partners with Microsoft Teams subscriptions.

PUBLISHED DATE

May 13, 2020

OVERVIEW & USER

TABLE OF CONTENTS

Utilize Private Channels	3
Block External Access	6
Limit Guest Access	11
Turn off File Sharing and File Storage Options	19
Block Third-Party Applications.....	22
Restrict Users Who Can Create Teams Channels	25
Set Teams Expiration	30
Set up Advanced Threat Protection Policies for Teams.....	32
Set up App Protection Policies	40
Set up Data Loss Prevention Polcies.....	46
Require MFA with Conditional Access.....	56
Conclusion.....	61



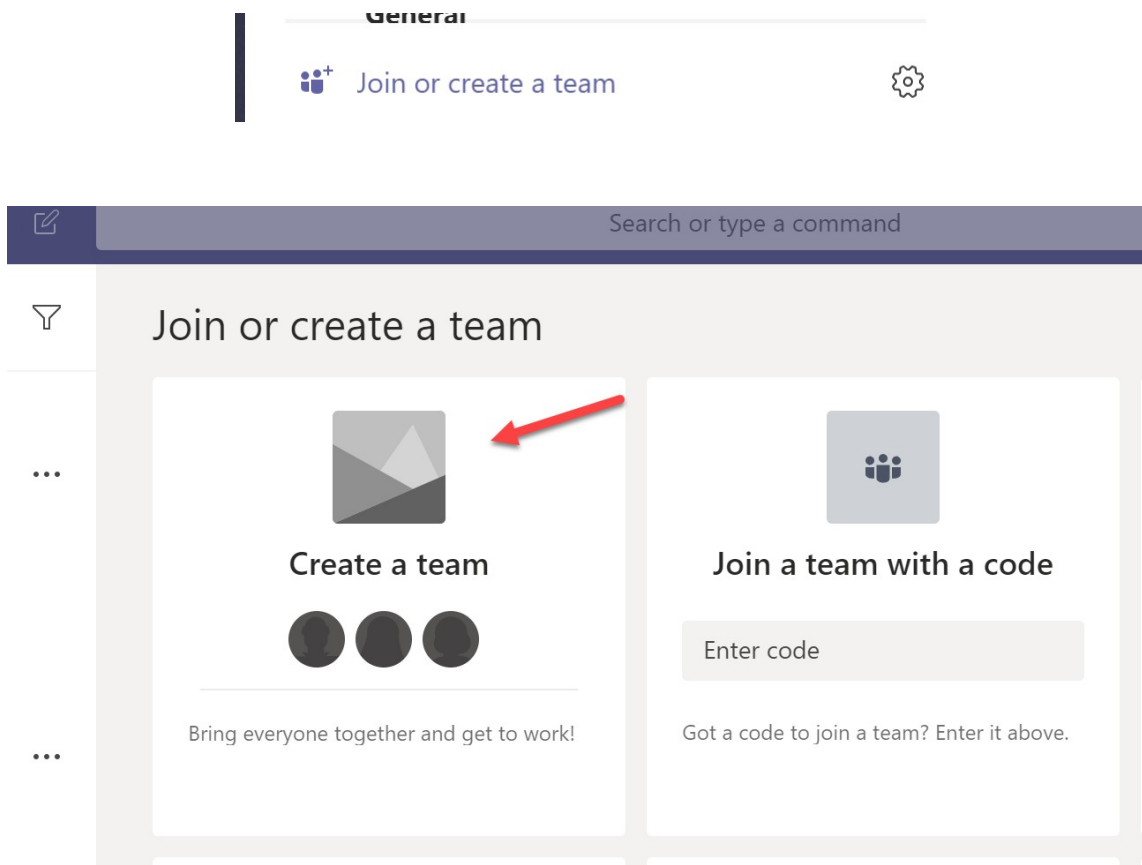
OVERVIEW & USER



UTILIZE PRIVATE CHANNELS

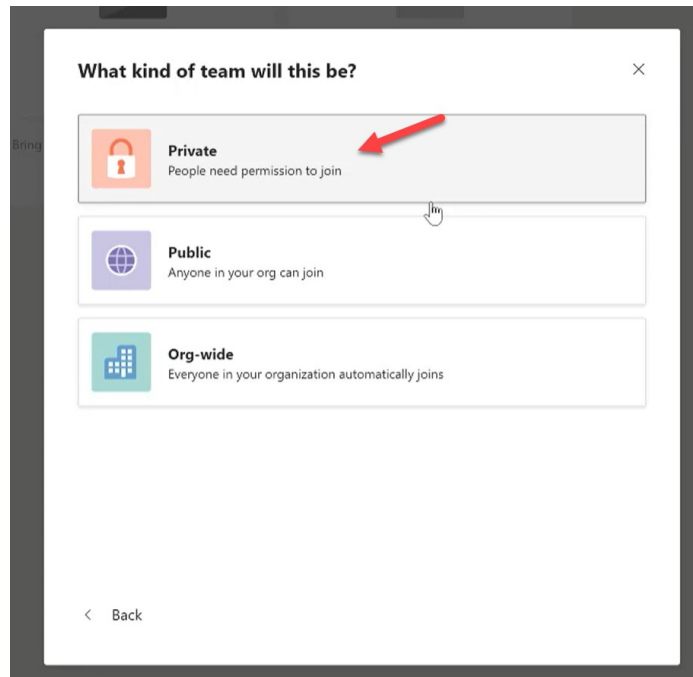
Description: Access controls are a fundamental part of any compliance regulation. Giving access to certain Teams channels where users are collaborating on sensitive topics or sharing critical documents should follow a model of least privilege. Microsoft Teams allows you to create private channels where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

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

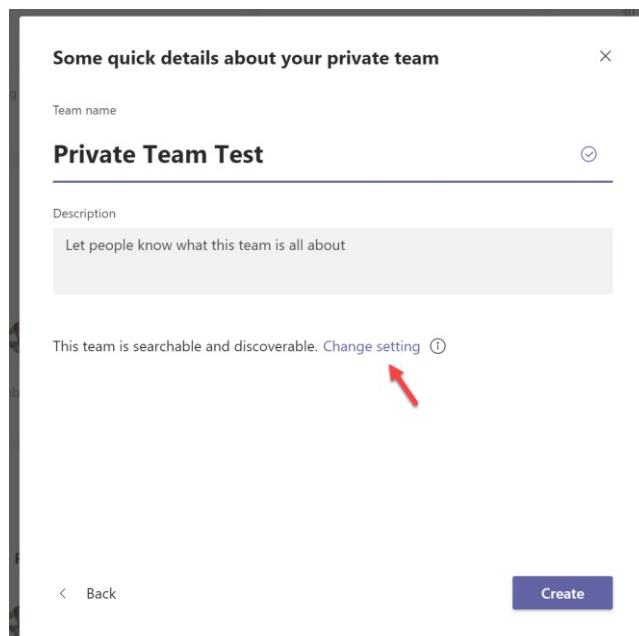


OVERVIEW & USER

2. Click Private

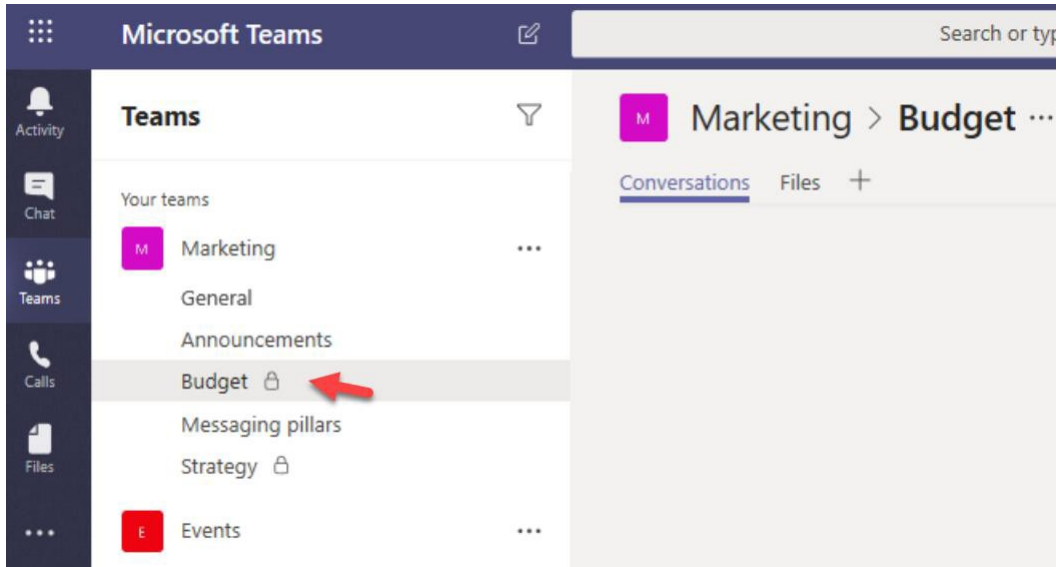


3. Here you can also choose if this team can be discoverable for additional security:



OVERVIEW & USER

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



RELEVANT 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)

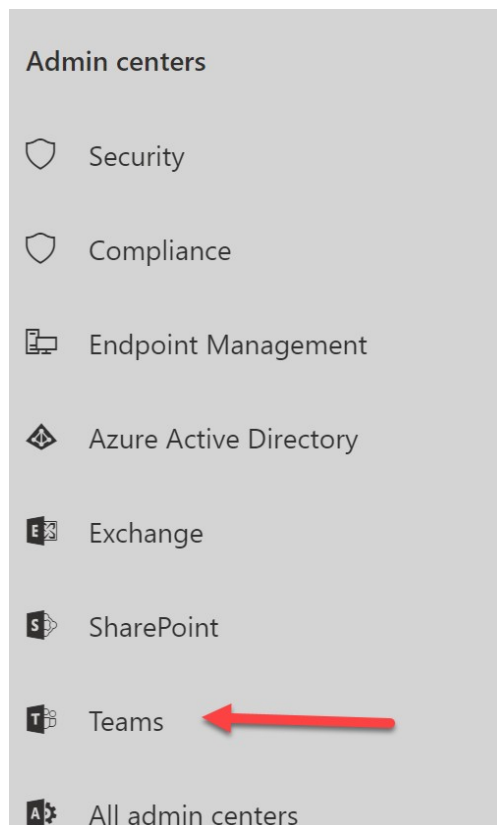
OVERVIEW & USER



BLOCK EXTERNAL ACCESS

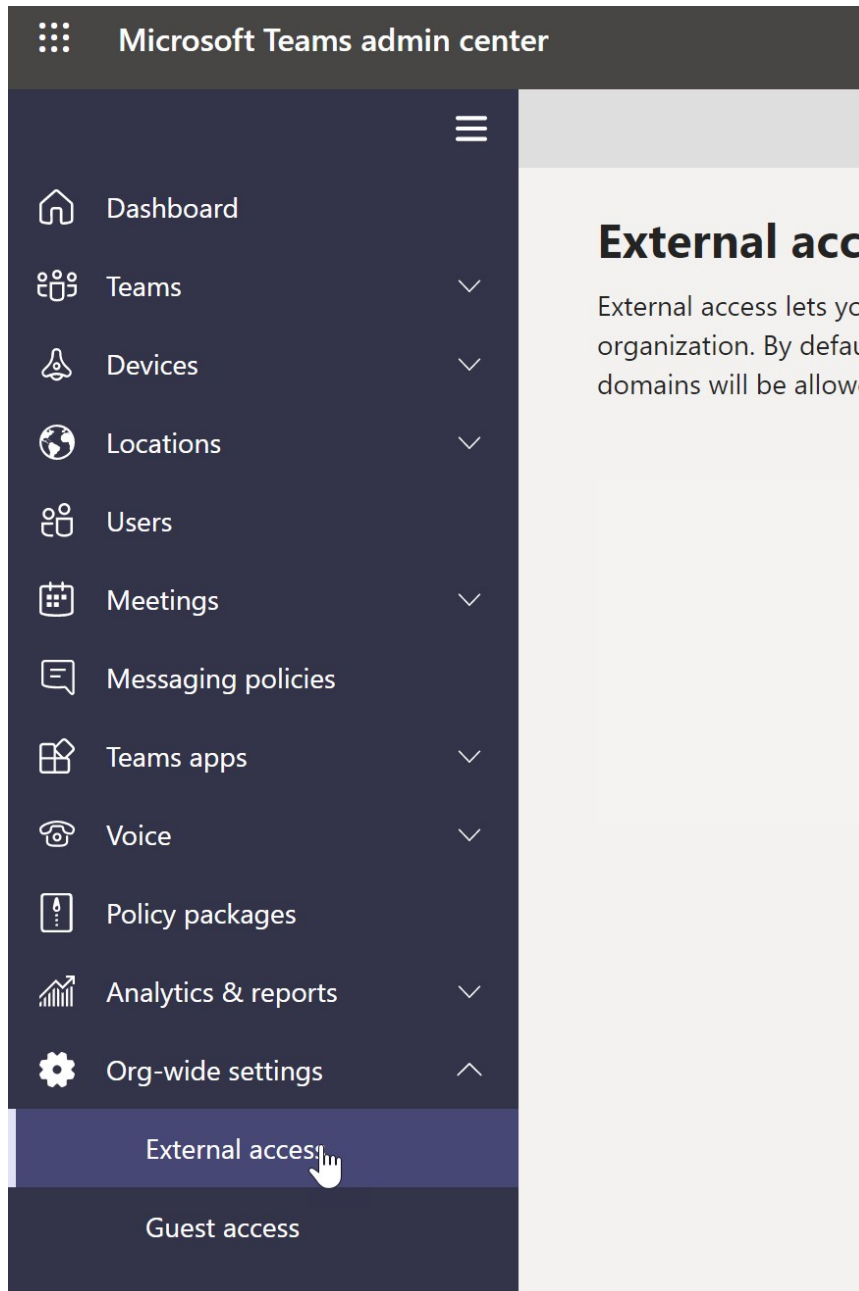
Description: You should not allow your users to communicate with Skype or Teams users outside your organization. While there are legitimate, productivity-improving scenarios for this, it also represents a potential security threat because those external users will be able to interact with your users 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

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



OVERVIEW & USER

2. Click Org-Wide Settings> External Access



OVERVIEW & USER

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	<input type="checkbox"/> Off
Users can communicate with Skype users	<input type="checkbox"/> 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:

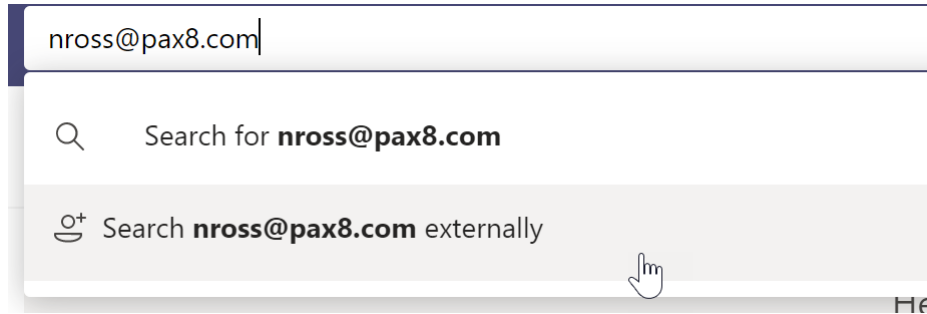
+ Add a domain

✓	Name	Status
	wrajrecords.com	Allowed

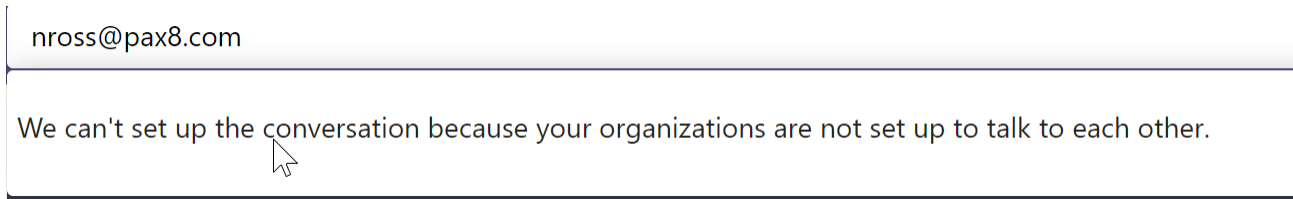
Save Discard

OVERVIEW & USER

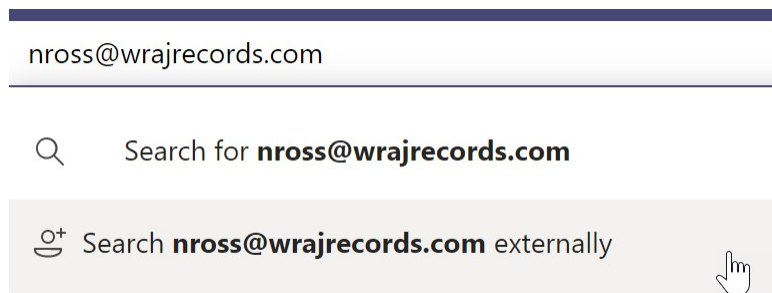
5. Users who search for external users in teams will see the following:



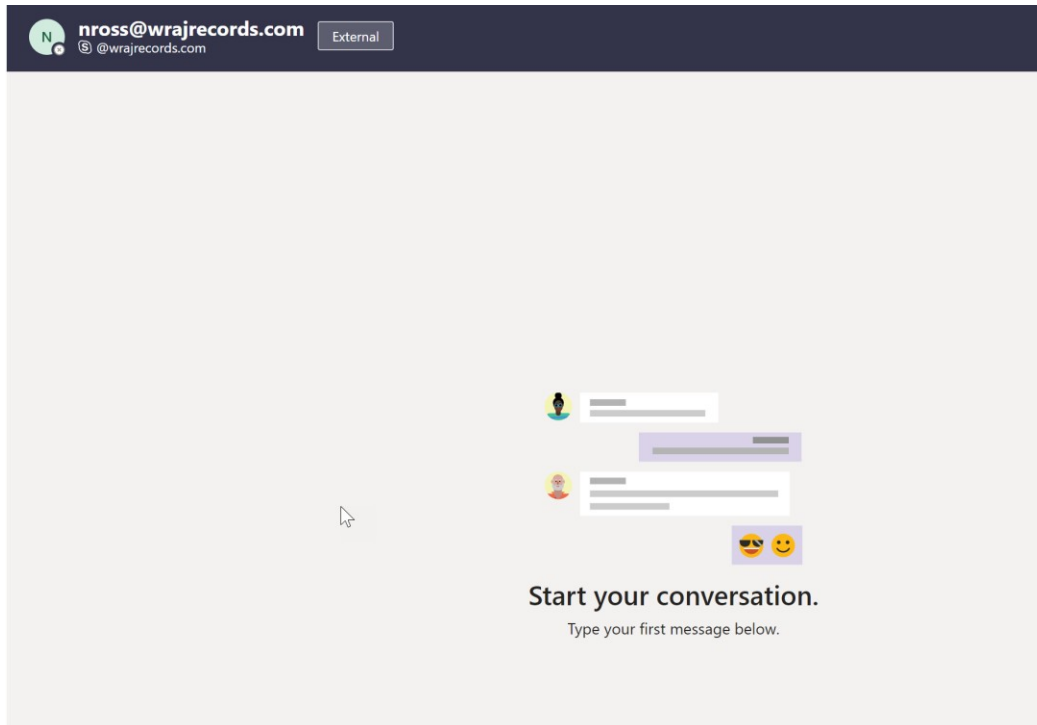
6. If they are not whitelisted, they will get the following when trying to search externally:



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



OVERVIEW & USER



RELEVANT 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)

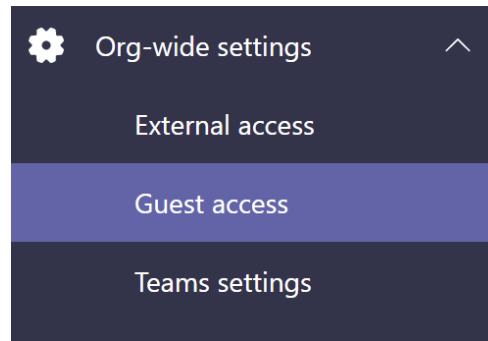
OVERVIEW & USER

LIMIT GUEST ACCESS

Description: By default, guess 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. Guess access should always be limited for a certain time period for security and compliance reasons.

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



OVERVIEW & USER

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

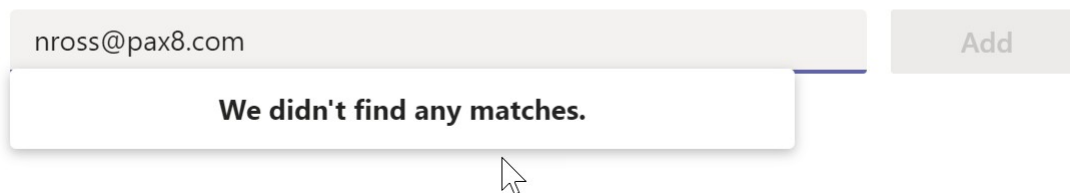
Messaging

OVERVIEW & USER

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

Add members to M365

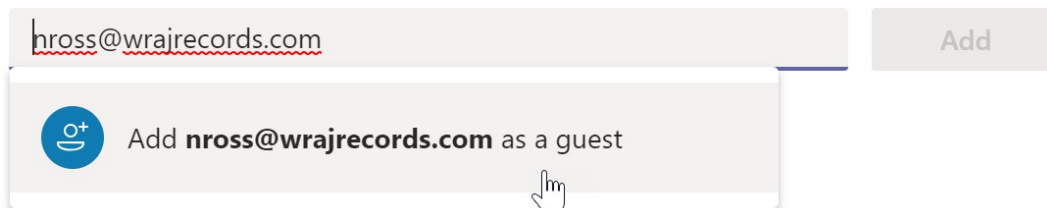
Start typing a name, distribution list, or mail enabled security group to add to your team.



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

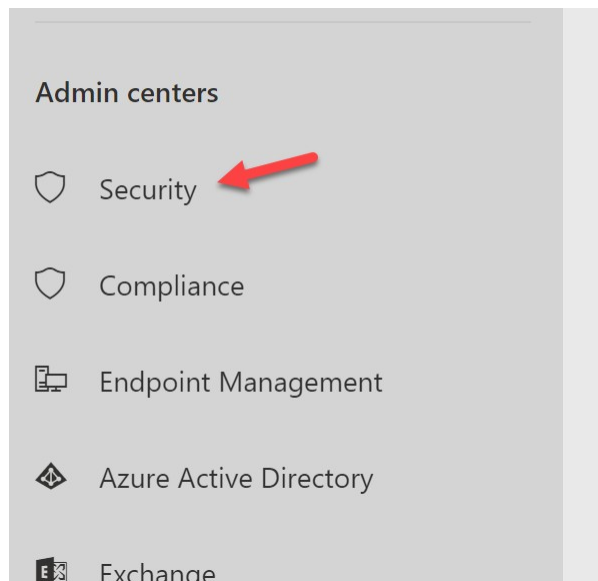
Add members to PSA Integrations

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.

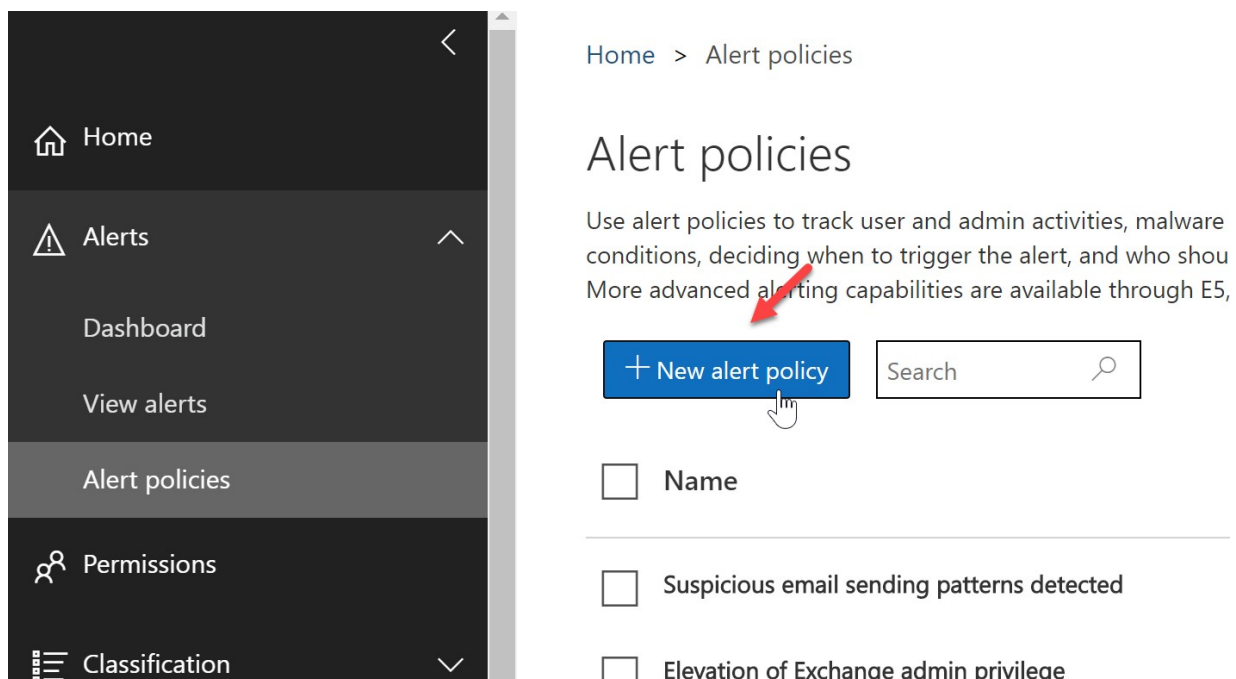


OVERVIEW & USER

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:



OVERVIEW & USER

7. Add Name, Description, Severity, and Category:

New alert policy

Name your alert

Create alert settings

Set your recipients

Review your settings

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

Assign a category and severity level to help you manage the policy and any alerts it triggers. You'll be at 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

Next Cancel

8. Type 'Guest' and select 'Accepted a 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

Accepted sharing invitation

Created a company shareable link

OVERVIEW & USER

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

New alert policy

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

Send email notifications

Email recipients *

Nick Ross X

Daily notification limit

No limit

Back Next Cancel

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.

Back Finish Cancel

OVERVIEW & USER

ADDITIONAL CONSIDERATIONS:

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

Dashboard > Users | All users

Users | All users
- Azure Active Directory

+ New user + New guest user ↑ Bulk create ↑ Bulk invite ↑ Bulk delete ↓ Download users ↻ Refresh

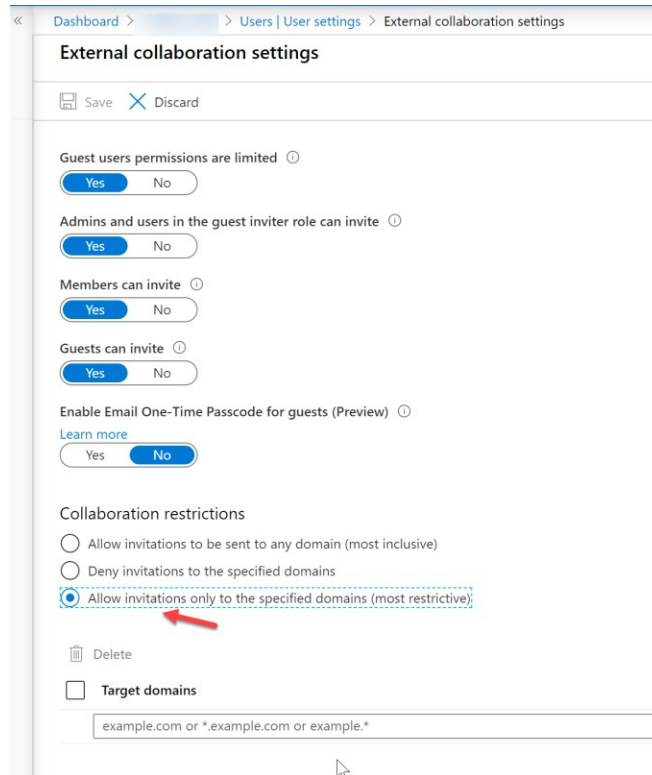
i Invited users who have not yet redeemed their invitation may not appear in this list.

Search users External users : **Yes**

	Name	User name	User type
<input type="checkbox"/>	thetradingnest	thetradingnest@gmail.com	Guest

OVERVIEW & USER

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



RELEVANT 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. §§
 - o 164.308(a)(1)(ii)(D)
 - o 164.312(b)
 - o 164.314(b)(2)(i)

OVERVIEW & USER



TURN OFF FILE SHARING AND FILE STORAGE OPTIONS

Description: By default, users can add external 3rd 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.

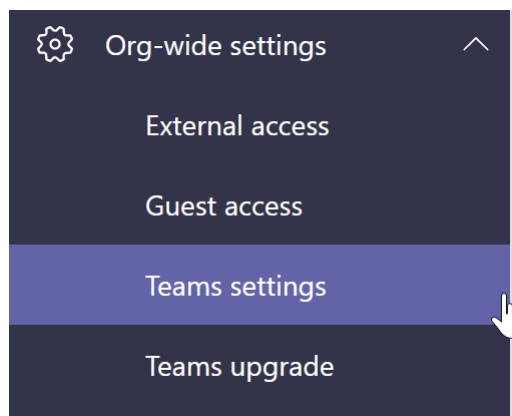


Google Drive

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

OVERVIEW & USER

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	<input checked="" type="checkbox"/> On
DropBox	<input checked="" type="checkbox"/> On
Box	<input checked="" type="checkbox"/> On
Google Drive	<input checked="" type="checkbox"/> On

OVERVIEW & USER

RELEVANT 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)

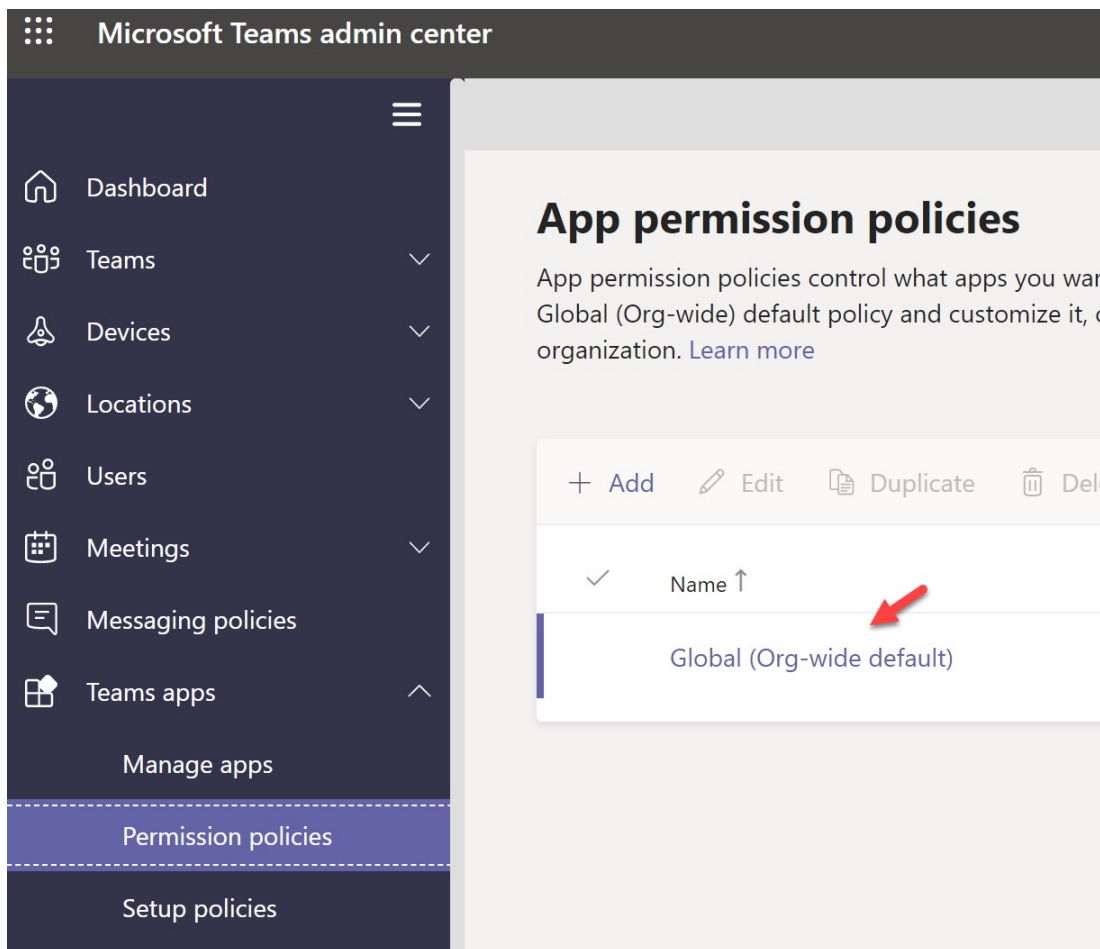
OVERVIEW & USER



BLOCK THIRD-PARTY APPLICATIONS

Description: 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.

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



OVERVIEW & USER

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

The screenshot shows the 'Global' settings page in the Microsoft Teams admin center. It features a 'Description' section and two main policy areas: 'Microsoft apps' and 'Third party apps'. Each area has a dropdown menu for selecting a policy. The 'Third party apps' dropdown is open, showing four options: 'Allow all apps', 'Allow specific apps and block all others', 'Block specific apps and allow all others', and 'Block all apps'. A mouse cursor is pointing at the 'Block all apps' option, which is highlighted in light blue.

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 specific apps and block all others**
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.

OVERVIEW & USER

RELEVANT 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
- NISTSP 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)

OVERVIEW & USER

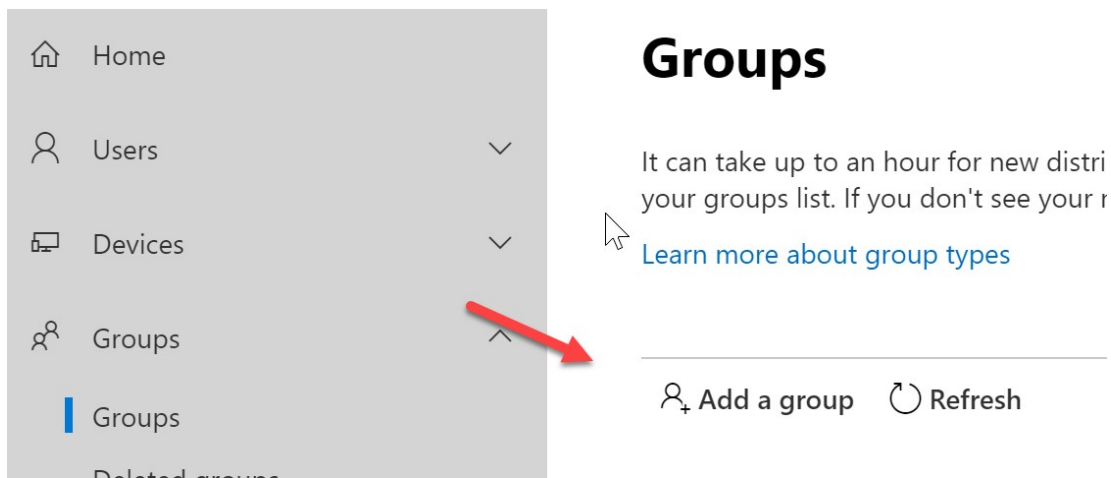


RESTRICT USERS WHO CAN CREATE TEAMS CHANNELS

Description: 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 an Microsoft 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 Microsoft 365 Groups. The setting is all or nothing in this regard.

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



OVERVIEW & USER

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

Group type

- Basics
- Finish

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.

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're

Name *

Teams Channel Creators

Description

Enter a description for your new group

OVERVIEW & USER

4. Click on the [following link](#) and Scroll down to the powershell section:

```
PowerShell Copy

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

Connect-AzureAD

$settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" | Where-object -Property Id -Value "00000000-0000-0000-0000-000000000000")
if(!$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" | Where-object -Property Id -Value "00000000-0000-0000-0000-000000000000")
}

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

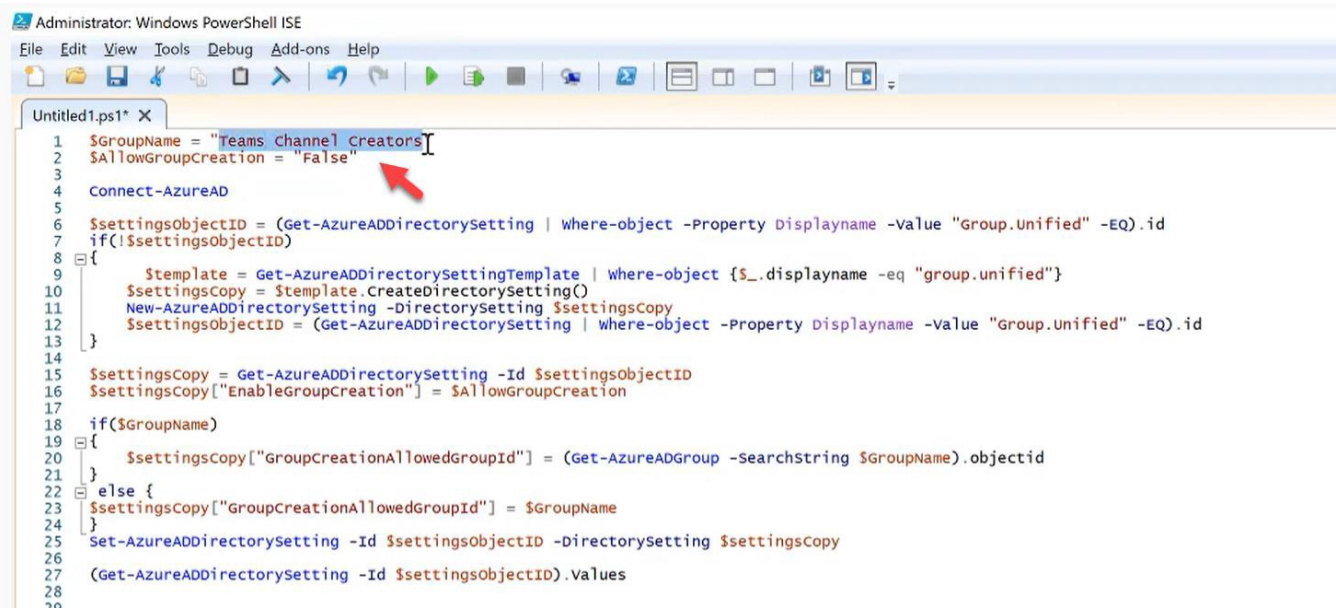
if($GroupName)
{
    $settingsCopy["GroupCreationAllowedGroupId"] = (Get-AzureADGroup -SearchString $GroupName).objectid
}
else {
    $settingsCopy["GroupCreationAllowedGroupId"] = $GroupName
}
Set-AzureADDirectorySetting -Id $settingsObjectID -DirectorySetting $settingsCopy

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

5. Run Powershell ISE as Admin (64x version) and run the following command: Import-Module AzureADPreview

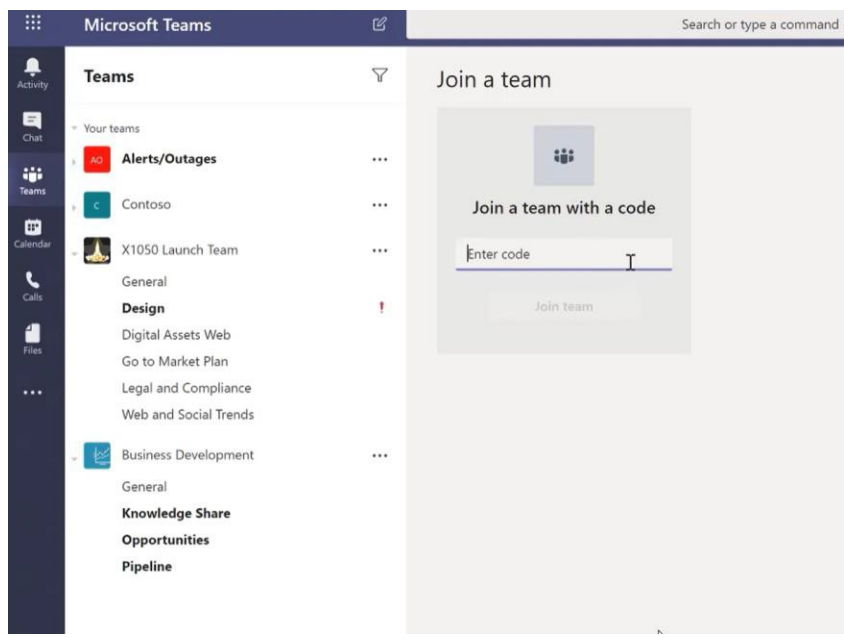
OVERVIEW & USER

- 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* X
1 $GroupName = "Teams Channel Creators"
2 $AllowGroupCreation = "False"
3
4 Connect-AzureAD
5
6 $SettingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -value "Group.Unified" -Eq).id
7 if(!$SettingsObjectID)
8 {
9     $Template = Get-AzureADDirectorySettingTemplate | Where-object {$_.displayname -eq "group.unified"}
10    $SettingsCopy = $Template.CreateDirectorySetting()
11    New-AzureADDirectorySetting -DirectorySetting $SettingsCopy
12    $SettingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -value "Group.Unified" -Eq).id
13 }
14
15 $SettingsCopy = Get-AzureADDirectorySetting -Id $SettingsObjectID
16 $SettingsCopy["EnableGroupCreation"] = $AllowGroupCreation
17
18 if($GroupName)
19 {
20     $SettingsCopy["GroupCreationAllowedGroupId"] = (Get-AzureADGroup -SearchString $GroupName).objectid
21 }
22 else {
23     $SettingsCopy["GroupCreationAllowedGroupId"] = $GroupName
24 }
25 Set-AzureADDirectorySetting -Id $SettingsObjectID -DirectorySetting $SettingsCopy
26
27 (Get-AzureADDirectorySetting -Id $SettingsObjectID).Values
28
29
```

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



OVERVIEW & USER

RELEVANT 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
- NISTSP 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)

OVERVIEW & USER



SET TEAMS EXPIRATION

Description: Organizations with a large number of teams often have teams 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 Microsoft 365 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.

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

OVERVIEW & USER

The screenshot shows the Azure Active Directory admin center interface. The top navigation bar is blue with the text 'Azure Active Directory admin center'. Below it, the breadcrumb trail shows 'Dashboard > Groups | Expiration'. The left sidebar contains a navigation menu with 'Dashboard', 'All services', 'FAVORITES', 'Azure Active Directory', 'Users', and 'Enterprise applications'. The main content area is titled 'Groups | Expiration' for 'Tminus365 - Azure Active Directory'. It features a 'Save' button and a 'Discard' button. The settings are organized into sections: 'All groups' (with links for 'All groups', 'Deleted groups', and 'Diagnose and solve problems'), 'Settings' (with 'General', 'Expiration', and 'Naming policy'), and 'Activity' (with 'Access reviews', 'Audit logs', and 'Bulk operation results (Preview)'). The 'Expiration' settings are expanded, showing: '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) *' set to 365; 'Email contact for groups with no owners *' set to admin@pax8.com; and 'Enable expiration for these Office 365 groups' with 'Selected' radio button chosen. Below the settings is a table with columns 'Name', 'Object Id', and 'M'. The table currently displays 'No groups found'.



OVERVIEW & USER

- 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 group expiration. If a group is not renewed, it is deleted along with its associated content from sources such as OneDrive and SharePoint.

Group lifetime (in days) * ⓘ 365 ^

Email contact for groups with no owners ⓘ 180 365

Enable expiration for these groups ⓘ Custom Selected None

RELEVANT COMPLIANCE CONTROLS:

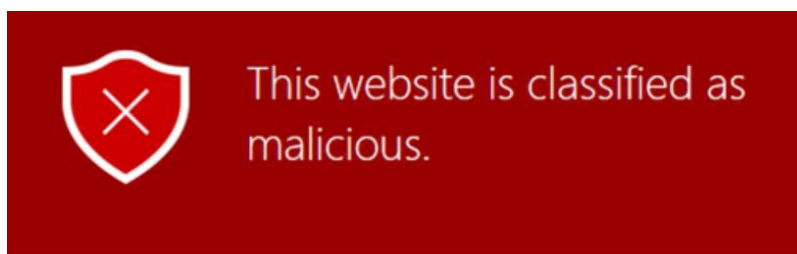
- NIST CSF PR.PT-1
- CCS CSC 14
- COBIT 5 APO11.04
- ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8,, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
- ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
- ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
- NISTSP 800-53 Rev. 4 AU Family
- HIPAA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

OVERVIEW & USER



SET UP ADVANCED THREAT PROTECTION POLICIES FOR TEAMS

Description: With Microsoft 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.



Opening this website might not be safe.

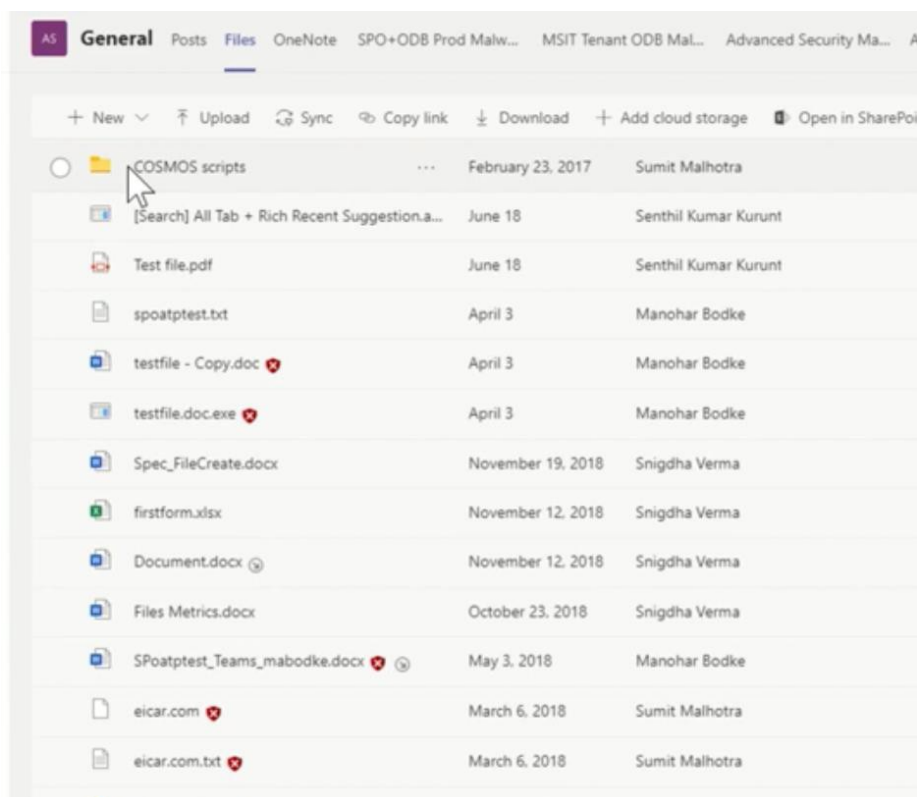
`www.unsafe_url/login.php`

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.

X Close this page

OVERVIEW & USER

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



License Requirements:

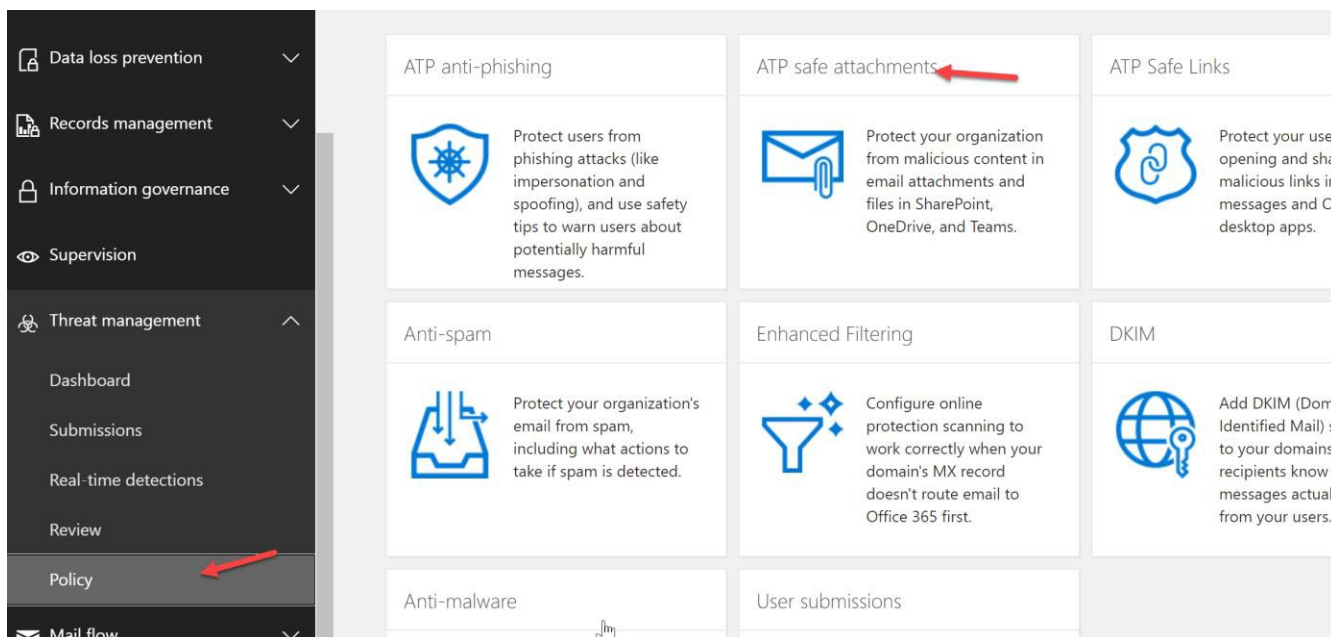
- [Microsoft Advanced Threat Protection Plan \(1\) \\$2/u/m](#)
- [Microsoft 365 Business Standard \\$20/u/m](#)

OVERVIEW & USER

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



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



OVERVIEW & USER

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 downl

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 the

Reports for this feature just got better. Check out the new [report](#) in the Security and Comp

+ [edit] [delete] [up] [down] [print] [refresh]

FNARI FD	NAMF	PRIORITY
----------	------	----------

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

new safe attachments policy

*Name:

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.



OVERVIEW & USER

- 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

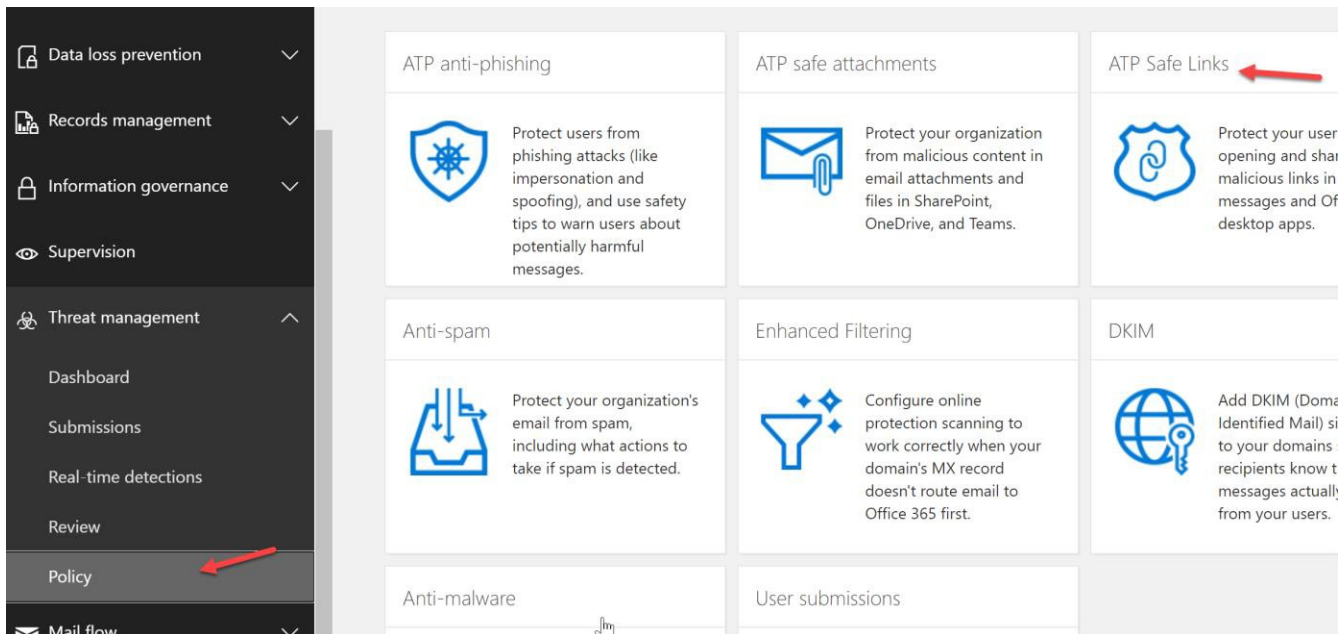
Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

The recipient domain is

Except if...

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



OVERVIEW & USER

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

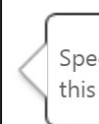


OVERVIEW & USER

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

*Name:

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.

OVERVIEW & USER

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

The screenshot shows the configuration interface for safe links in Microsoft Teams. At the top, there are two checked checkboxes: "Do not track when users click safe links." and "Do not let users click through safe links to original URL." Below these is the section "Do not rewrite the following URLs:" which includes a list box with a minus sign icon and a text input field containing "Enter a valid URL" and a plus sign icon. At the bottom, the "Applied To" section is visible, with the instruction "Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:". Below this, there is a dropdown menu labeled "If..." with the selected option "The recipient domain is", followed by a text input field containing ".com" and an "add condition" button.

RELEVANT 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. §§
 - o 164.308(a)(5)(ii)(B)

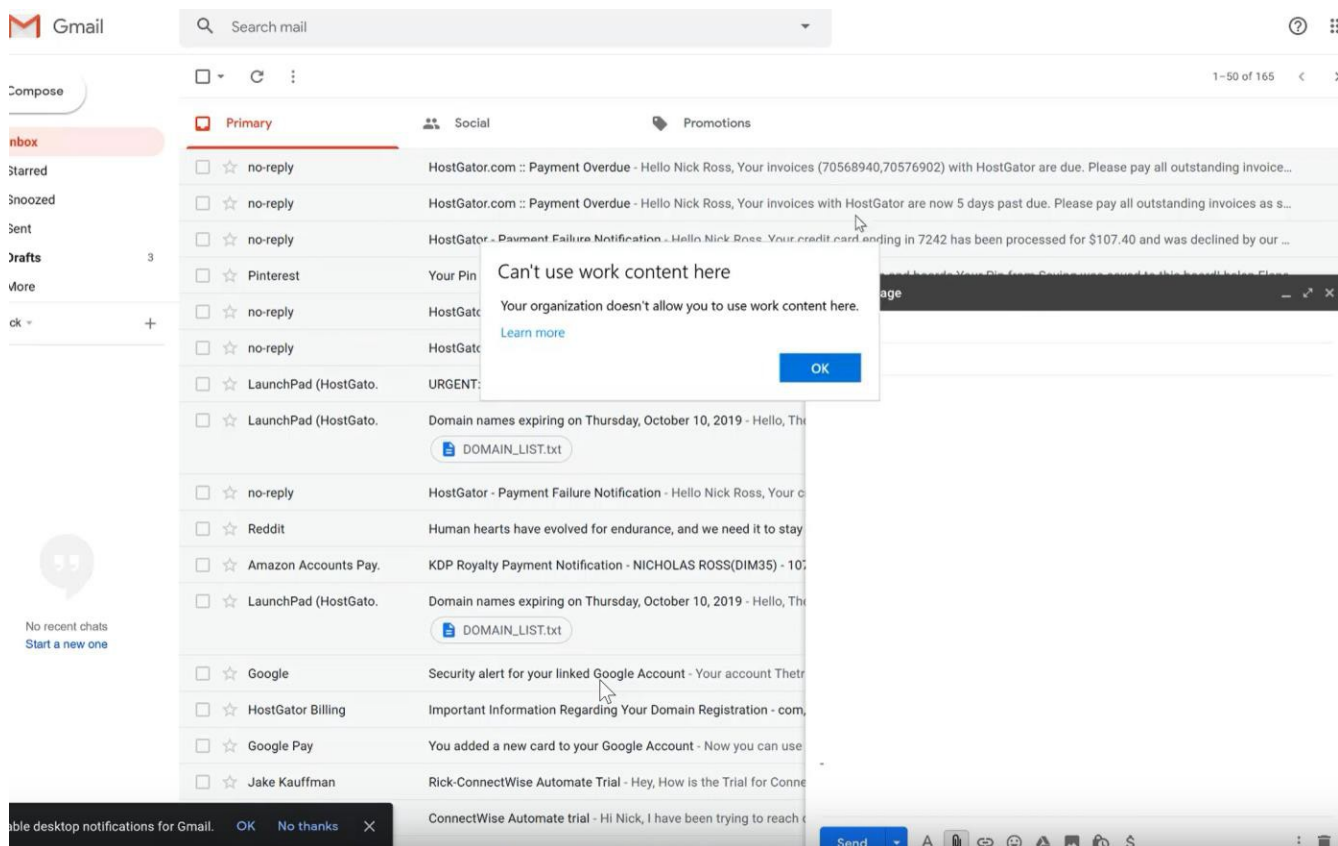
OVERVIEW & USER



SET UP APP PROTECTION POLICIES

Description: 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:

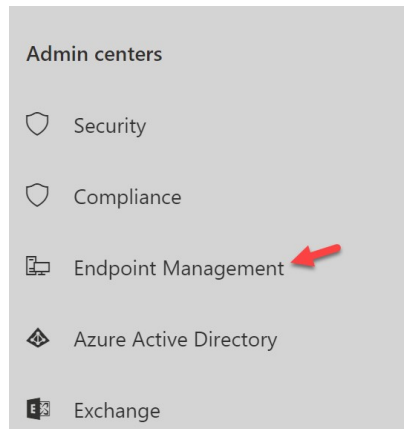


OVERVIEW & USER

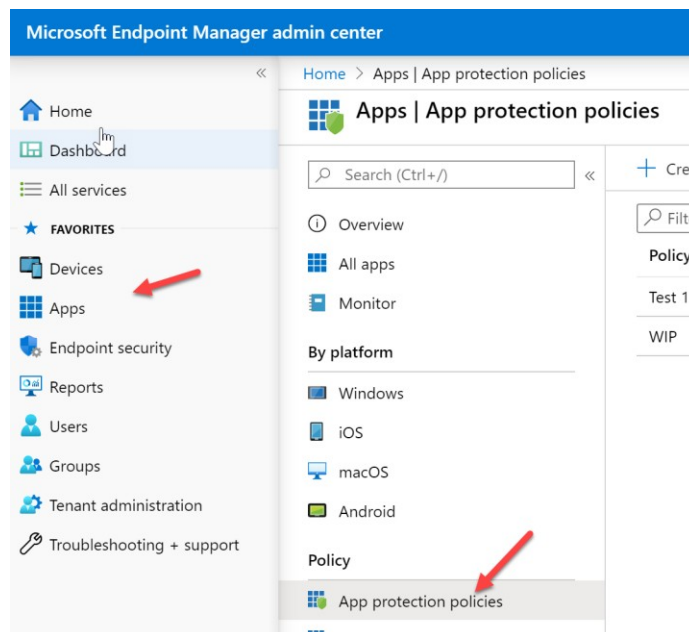
License Requirements:

- [Microsoft 365 Business Standard](#) \$20/u/m
- [Microsoft Enterprise Mobility + Security E3](#) \$8.75/u/m
- [Microsoft Intune](#) \$6/u/m

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

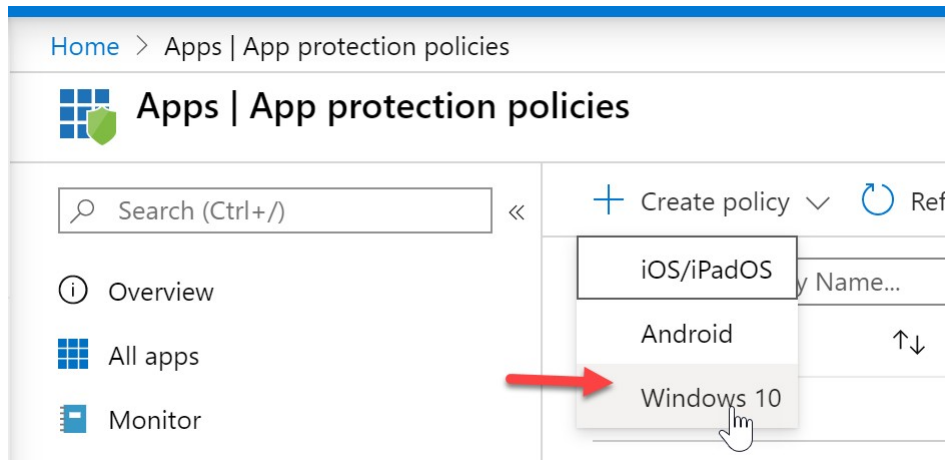


2. Click Apps>App Protection Policies

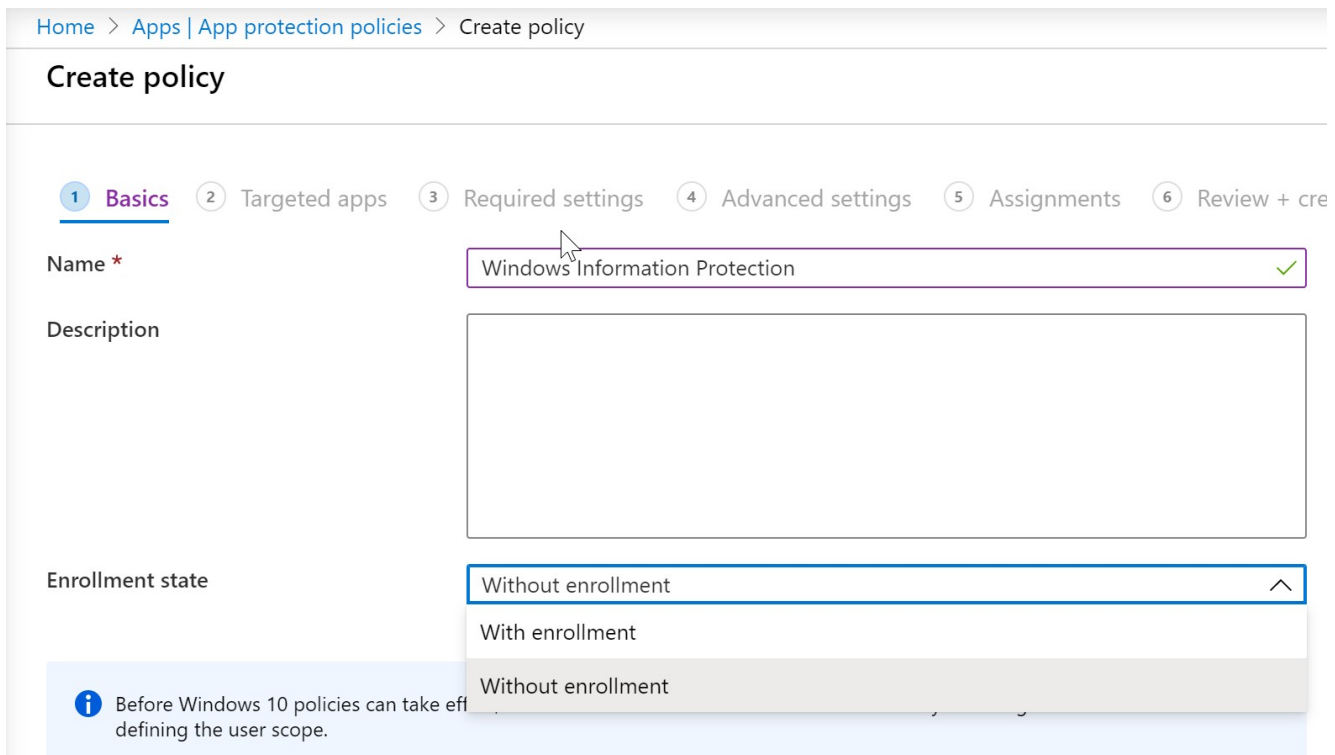


OVERVIEW & USER

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:



OVERVIEW & USER

5. Click+ Add and add allow appropriate applications. At the minimum, add the entire office suite. You can import 3rd 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 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
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

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

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

[+ Add + Import](#)

OVERVIEW & USER

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.

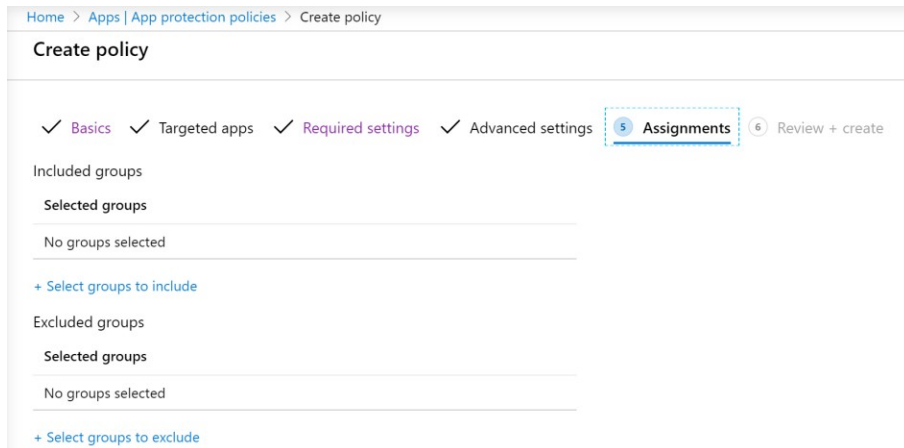
i Add /*AppCompat*/ to your list of cloud resources to enable TLS connections by personal apps that connect directly to a cloud resource through an IP address.

Type	Value
Any network boundaries you add will show up here	
+ Add	
Enterprise Proxy Servers list is authoritative (do not auto-detect)	Off
Enterprise IP Ranges list is authoritative (do not auto-detect)	Off



OVERVIEW & USER

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



RELEVANT 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)

OVERVIEW & USER



SET UP DATA LOSS PREVENTION POLICIES

Description: 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.

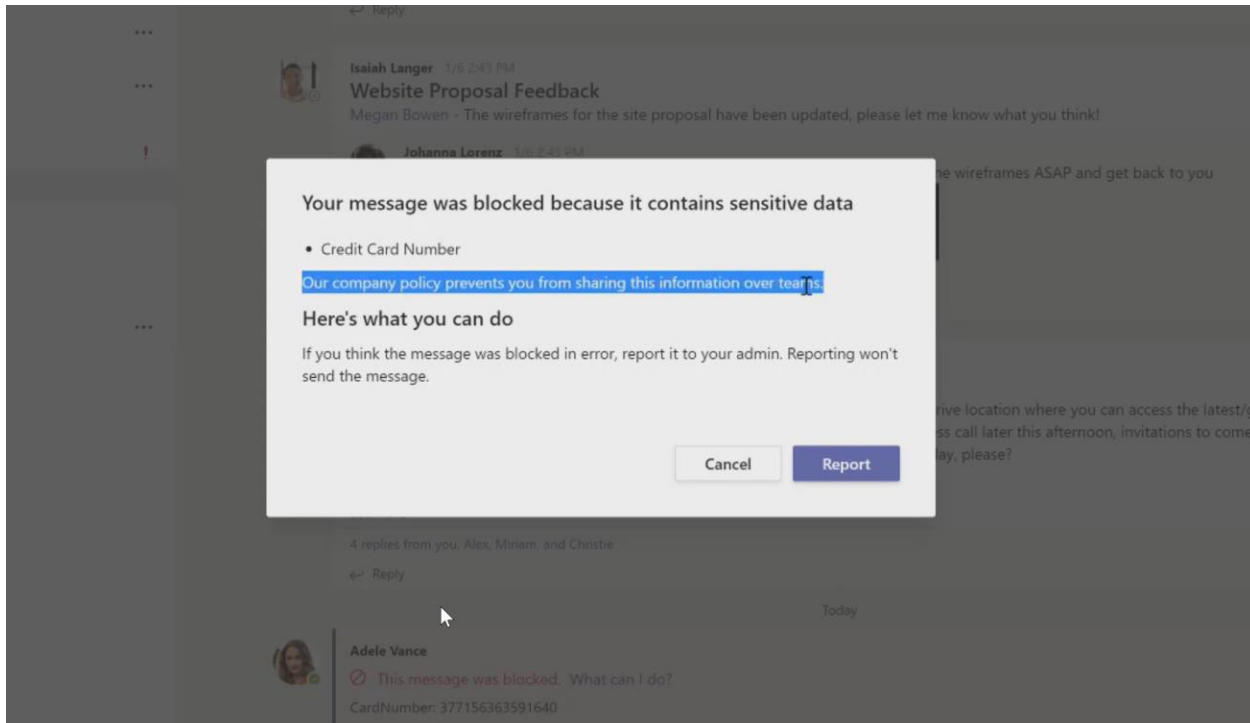
License Requirements:

- [Microsoft 365 Business Standard \\$20/u/m](#)
- [Microsoft Office 365 E3 \\$20/u/m](#)

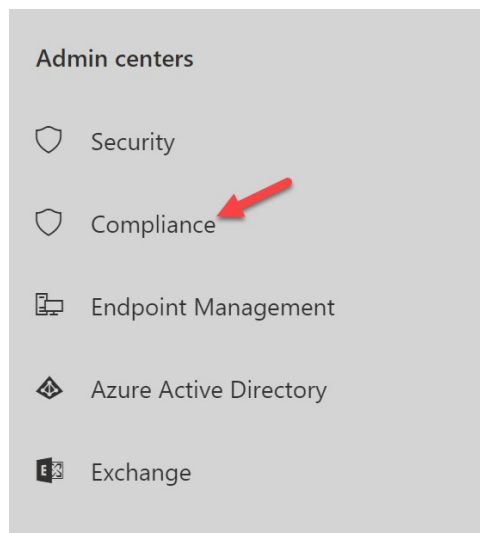
Ex. User sending Credit Card Information



OVERVIEW & USER

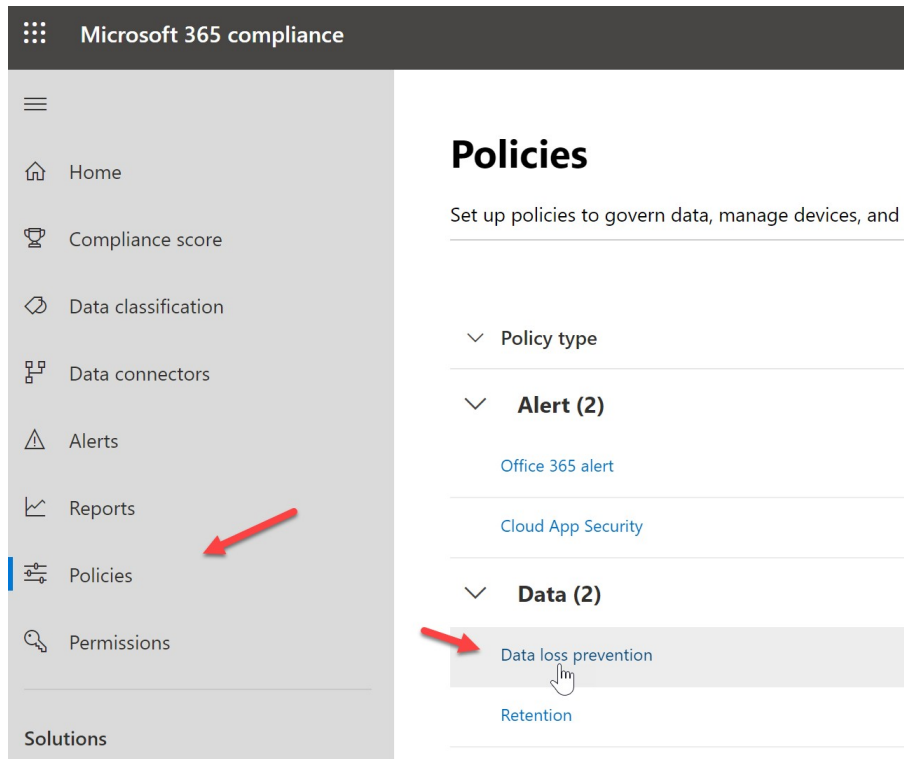


1. In the 365 Admin Center, click on Admin Centers>Compliance



OVERVIEW & USER

2. Click Policies>Data Loss Prevention



3. Click Create Policy

Data loss prevention

Use data loss prevention (DLP) policies to help identify and protect the wrong people. [Learn more about DLP](#)

+ Create policy ↓ Export ↻ Refresh

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

OVERVIEW & USER

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](#)

Search Show options for

42 results

- Financial
- Medical and health
- Privacy
- Custom

PCI Data Security Standard (PCI DSS)	U.S. Financial Data
Saudi Arabia - Anti-Cyber Crime Law	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.
Saudi Arabia Financial Data	Protects this information: Credit Card Number U.S. Bank Account Number ABA Routing Number
U.K. Financial Data	

5. Add a name and description

New DLP policy

- Choose the information to protect
- Name your policy**
- Choose locations
- Policy settings
- Review your settings

Name your policy

Name *

Description



OVERVIEW & USER

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

New DLP policy

- ✓ Choose the information to protect
- ✓ Name your policy
- Choose locations**
- Policy settings
- Review your settings

Choose locations

Status	Location	Include	Exclude
<input type="checkbox"/>	Exchange email		
<input type="checkbox"/>	SharePoint sites		
<input type="checkbox"/>	OneDrive accounts		
<input checked="" type="checkbox"/>	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

OVERVIEW & USER

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](#)

+ New rule

Name	Status	Priority
<input type="checkbox"/> Low volume of content detected U.S. Financial	<input checked="" type="checkbox"/>	0

[Edit rule](#) [Delete rule](#)

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



OVERVIEW & USER

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

Low volume of content detected U.S. Financial

Name	Conditions	Exceptions	Actions	User notifications	User
------	------------	------------	---------	--------------------	------

^ Exceptions

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

+ Add an exception ▾

^ 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)



OVERVIEW & USER

^ 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

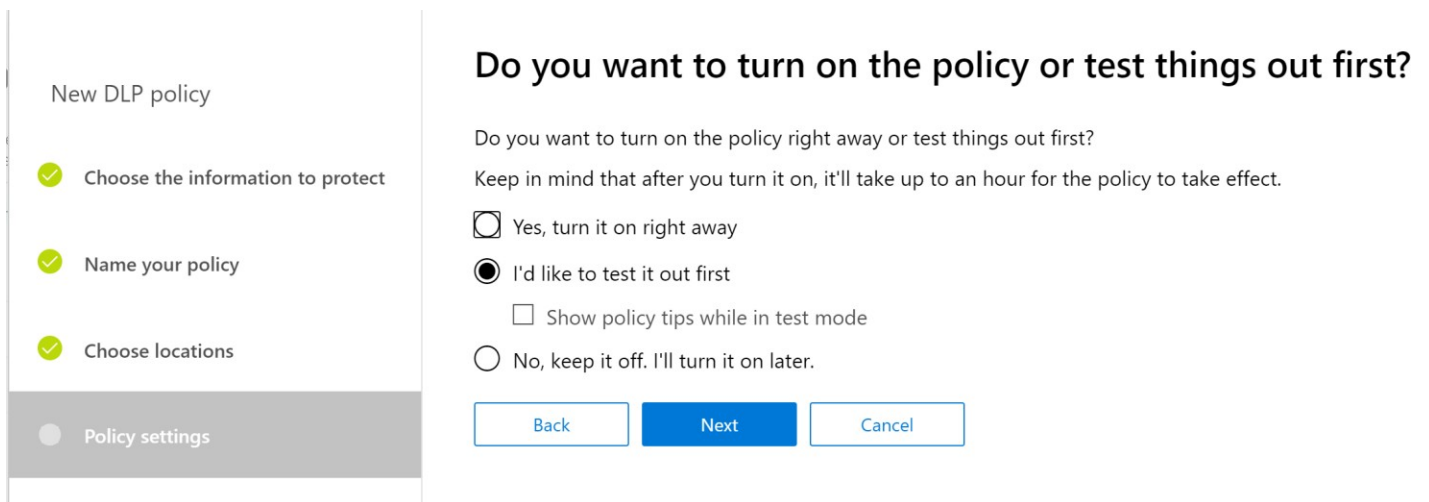
OVERVIEW & USER

^ User overrides

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



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.



New DLP policy

- ✓ Choose the information to protect
- ✓ Name your policy
- ✓ Choose locations
- Policy settings

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.

Back Next Cancel

OVERVIEW & USER

RELEVANT 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
- NISTSP 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)

OVERVIEW & USER



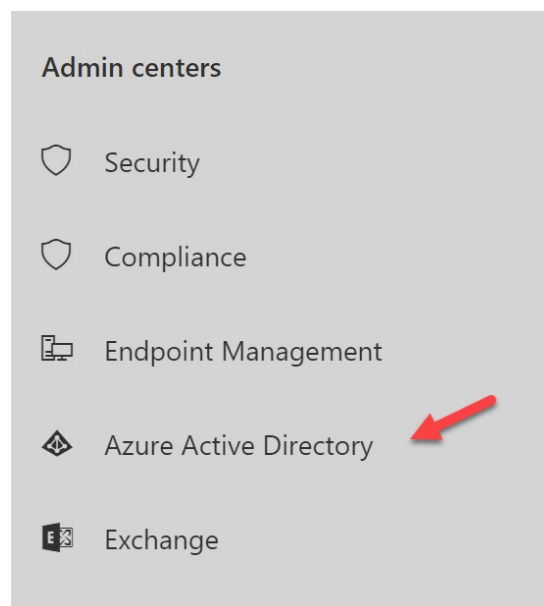
REQUIRE MFA WITH CONDITIONAL ACCESS

Description: Conditional Access policies within Microsoft 365 allow us to enforce specific controls when certain conditions are met. For example, we can define a policy that says if a user is trying to access corporate resources from a remote location, they will be prompted with MFA. We can target this policy specifically to Teams access.

Licensing Requirements:

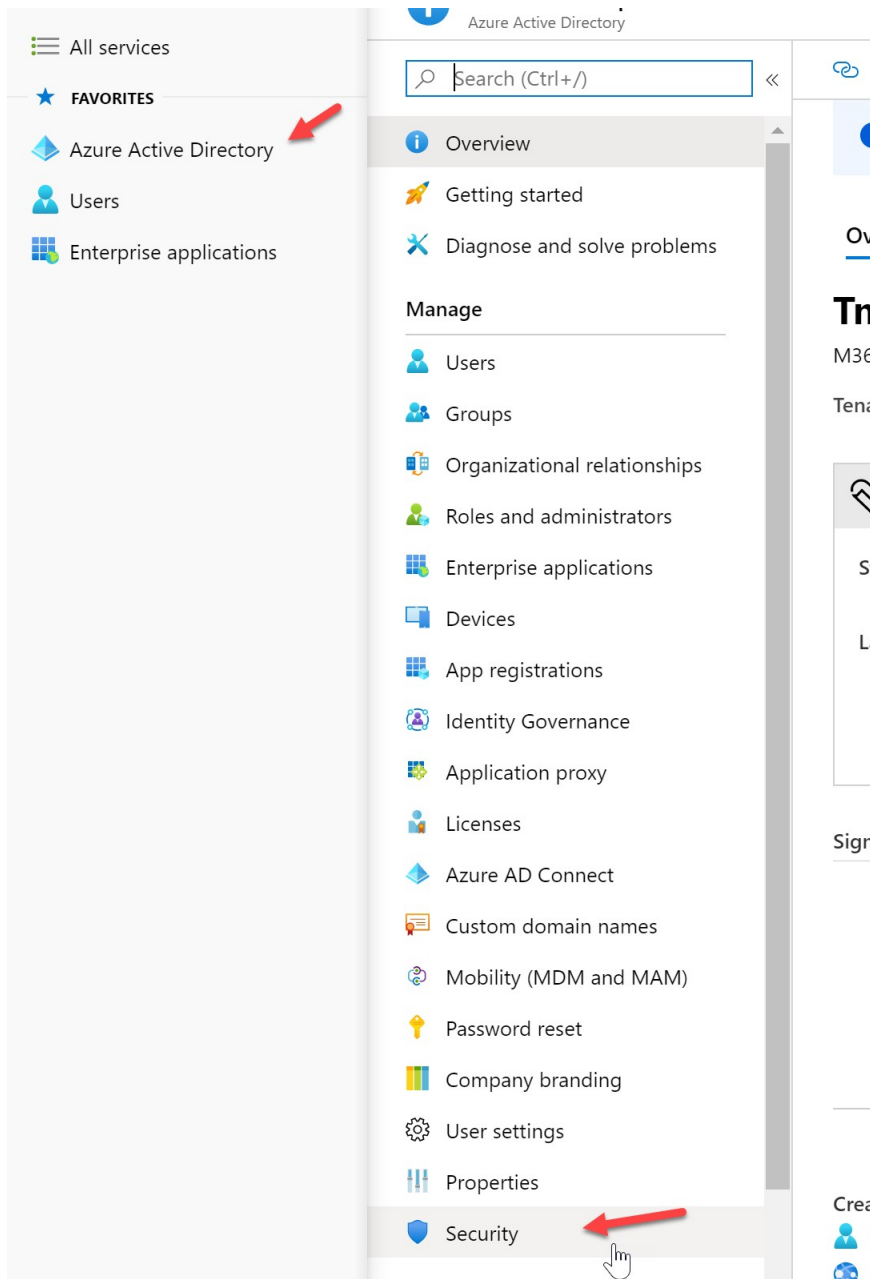
- [Microsoft 365 Business Standard](#) \$20/u/m
- [Microsoft Enterprise Mobility + Security E3](#) \$8.75/u/m
- [Azure Active Directory Premium Plan 1](#) \$6/u/m

1. In the 365 Admin Center, click Admin Centers>Azure Active Directory



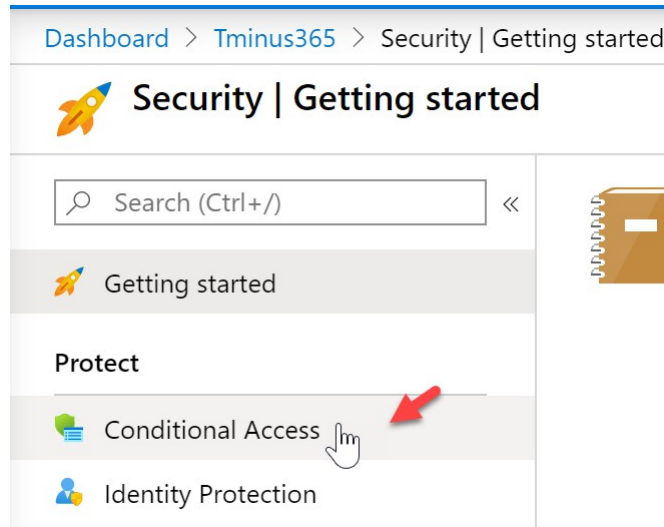
OVERVIEW & USER

2. Click Azure Active Directory>Security

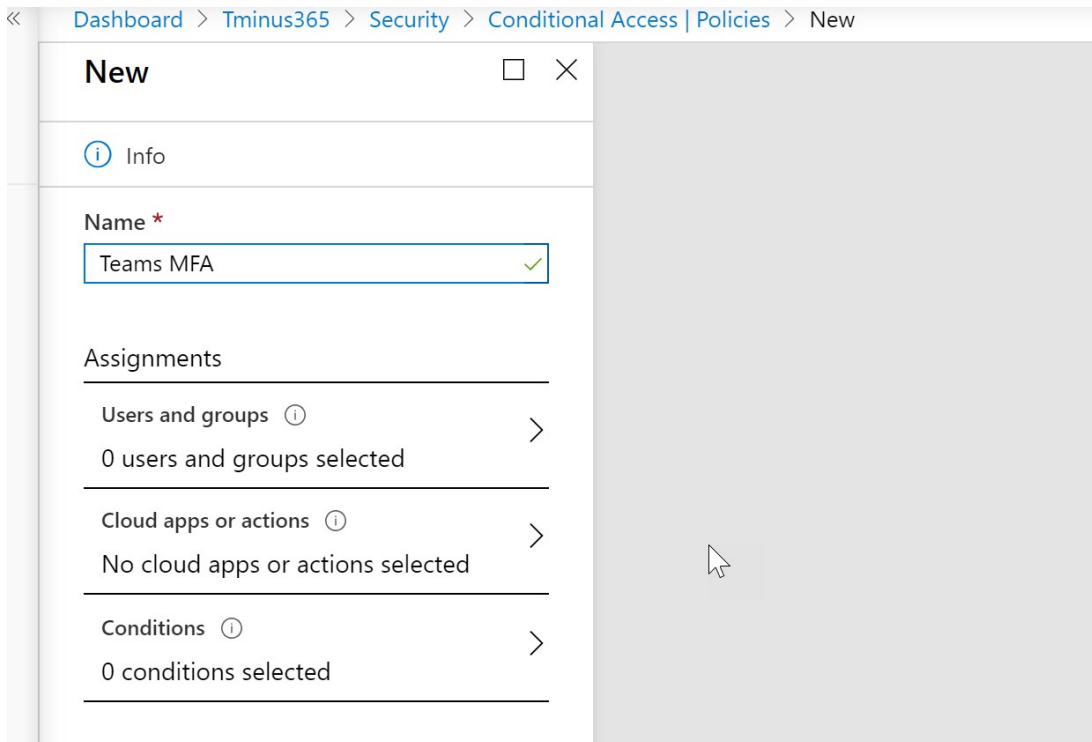


OVERVIEW & USER

3. Click Conditional Access

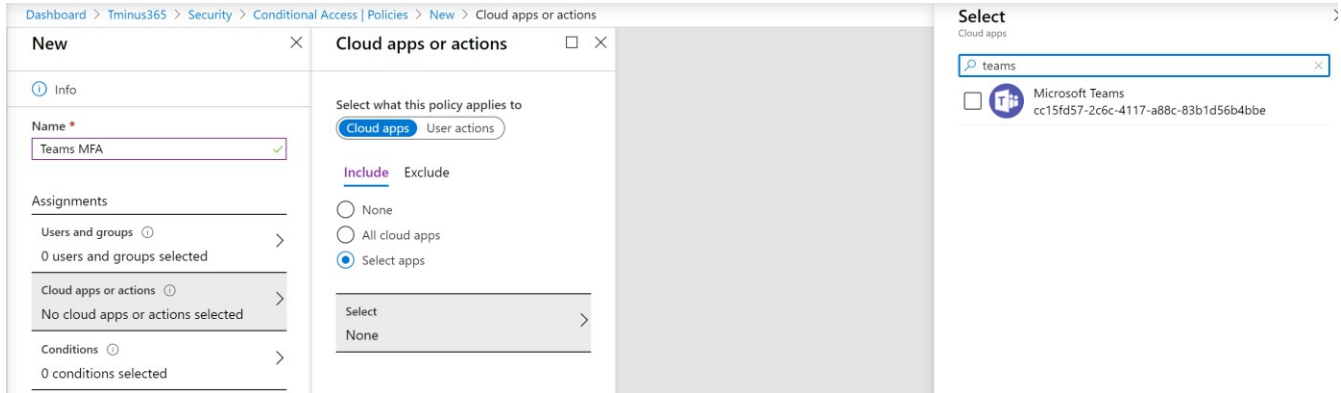


4. Click +New Policy. Name the Policy and click on users and groups to scope the policy:

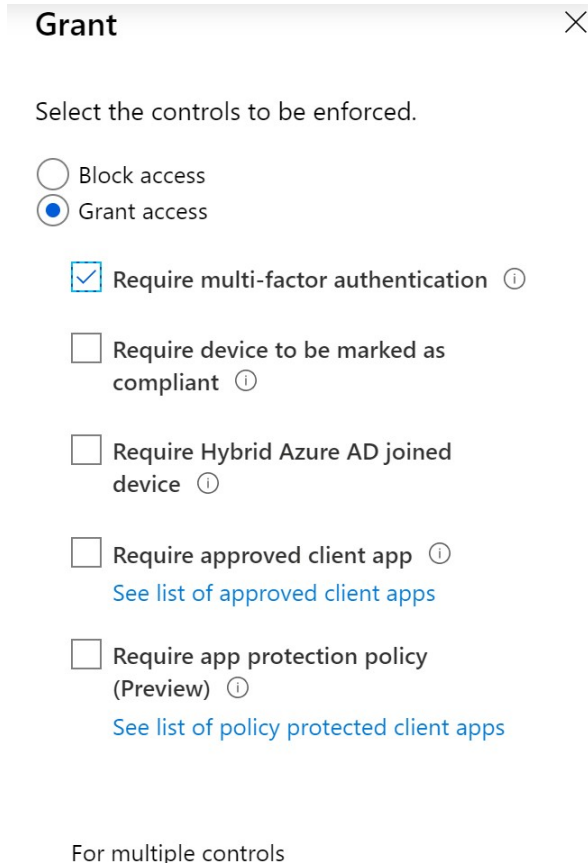


OVERVIEW & USER

5. In the Cloud Apps section, search for Teams



6. On the Grant tab, select Grant Access and Require Multi-factor Authentication. Then click Create



OVERVIEW & USER

RELEVANT COMPLIANCE CONTROLS:

- NIST CSF PR.AC-1
- CCS CSC 16
- COBIT 5 DSS05.04, DSS06.03
- ISA 62443-2-1:2009 4.3.3.5.1
- ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
- ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
- NIST SP 800-53 Rev. 4 AC-2, IA Family
- HIPAA Security Rule 45 C.F.R. §§
 - 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C),
 - 164.308(a)(4)(i), 164.308(a)(4)(ii)(B),
 - 164.308(a)(4)(ii)(C), 164.312(a)(2)(i),
 - 164.312(a)(2)(ii), 164.312(a)(2)(iii),
 - 164.312(d)

OVERVIEW & USER

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