2020

SECURING MICROSOFT TEAMS

OVERVIEW AND USER GUIDE

Nick Ross | Microsoft Certified Expert Administrator

SECURING MICROSOFT TEAMS

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

SECURING MICROSOFT TEAMS

OVERVIEW & USER

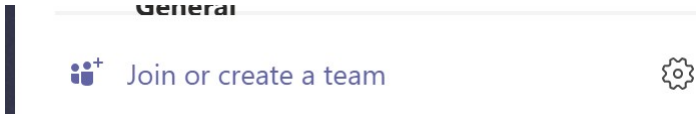
TABLE OF CONTENTS

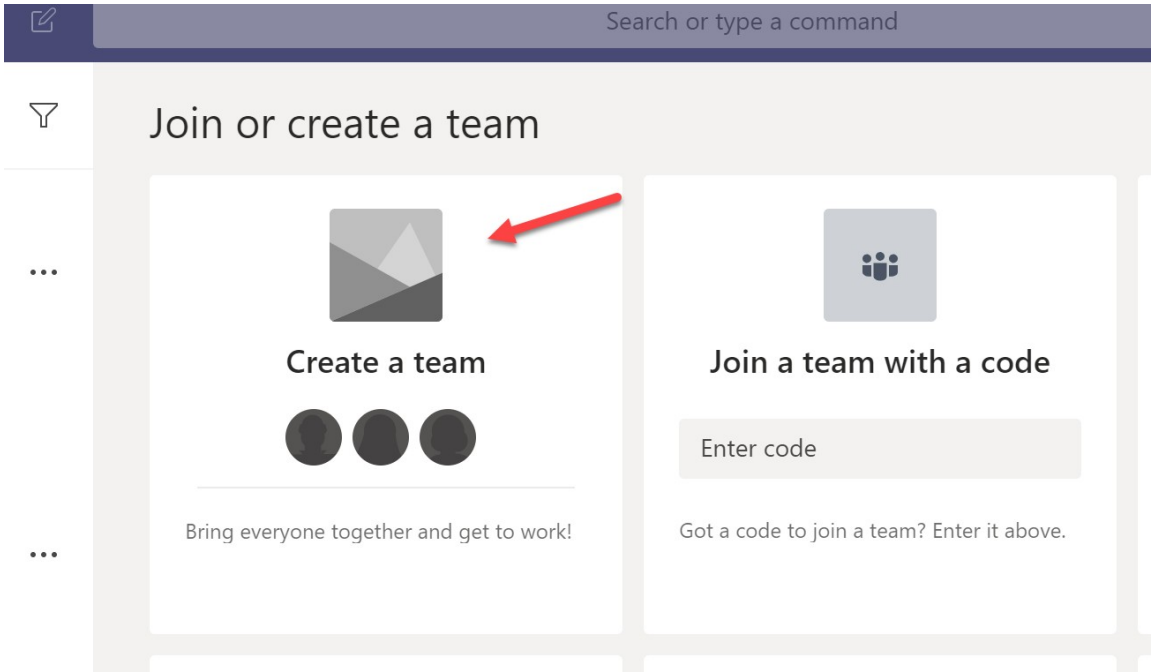
OVERVIEW & USER

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.

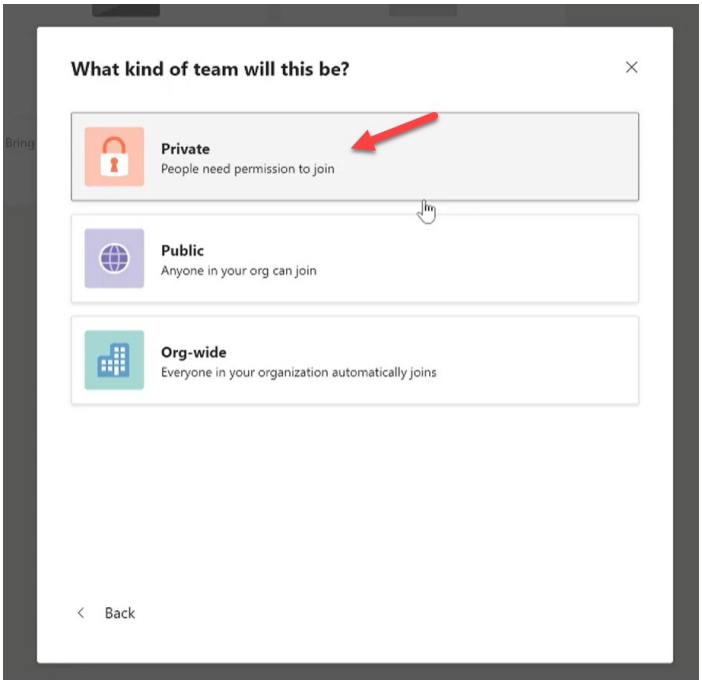
1. In the web or client application, click Teams>Join or create a team>Create a Team



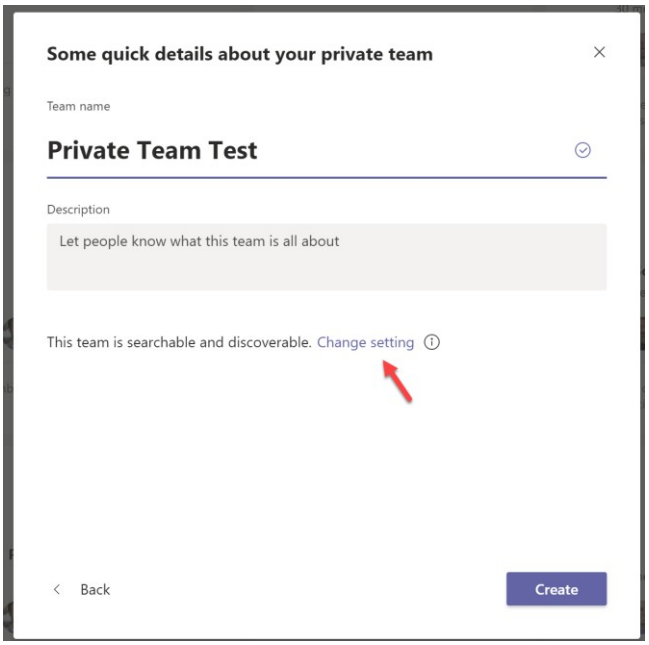


OVERVIEW & USER

2. Click Private

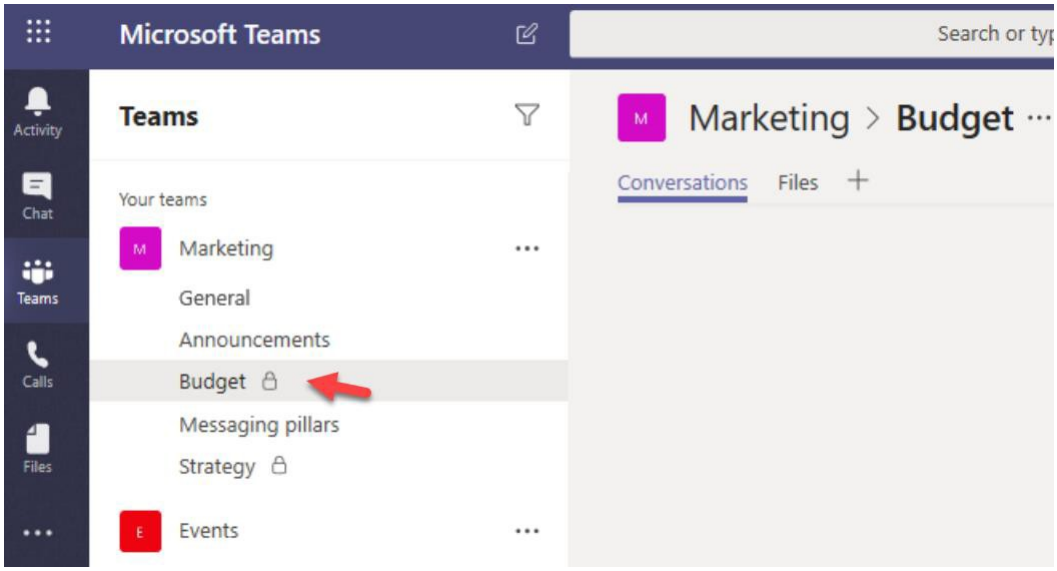


3. Here you can also choose if this team can be discoverable for additional security:



OVERVIEW & USER

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



RELEVANT COMPLIANCE CONTROLS:

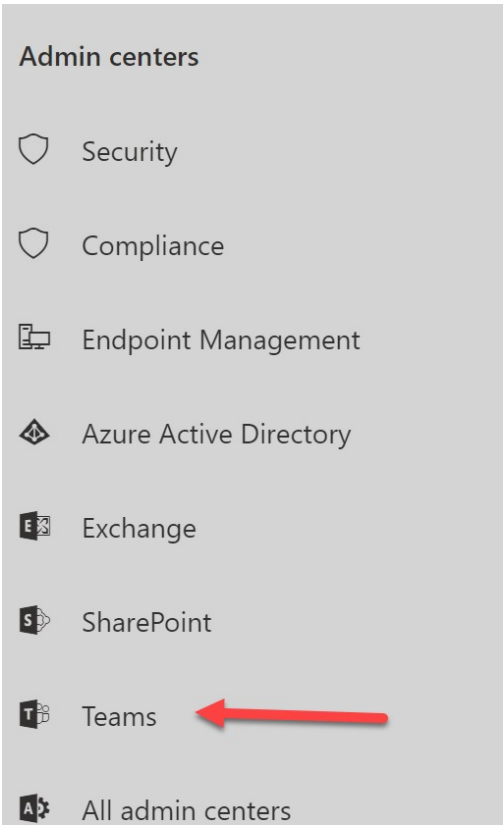
- NIST CSF PR.AC-4
- CCS CSC 12, 15
- ISA 62443-2-1:2009 4.3.3.7.3
- ISA 62443-3-3:2013 SR 2.1
- ISO/IEC 27001:2013 A.6.1.2, A.9.1.2,
- A.9.2.3, A.9.4.1, A.9.4.4
- NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC6, AC-16
- HIPAA Security Rule 45 C.F.R. §§
    - 164.308(a)(3), 164.308(a)(4),
    - 164.312(a)(1),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

OVERVIEW & USER

BLOCK EXTERNAL ACCESS

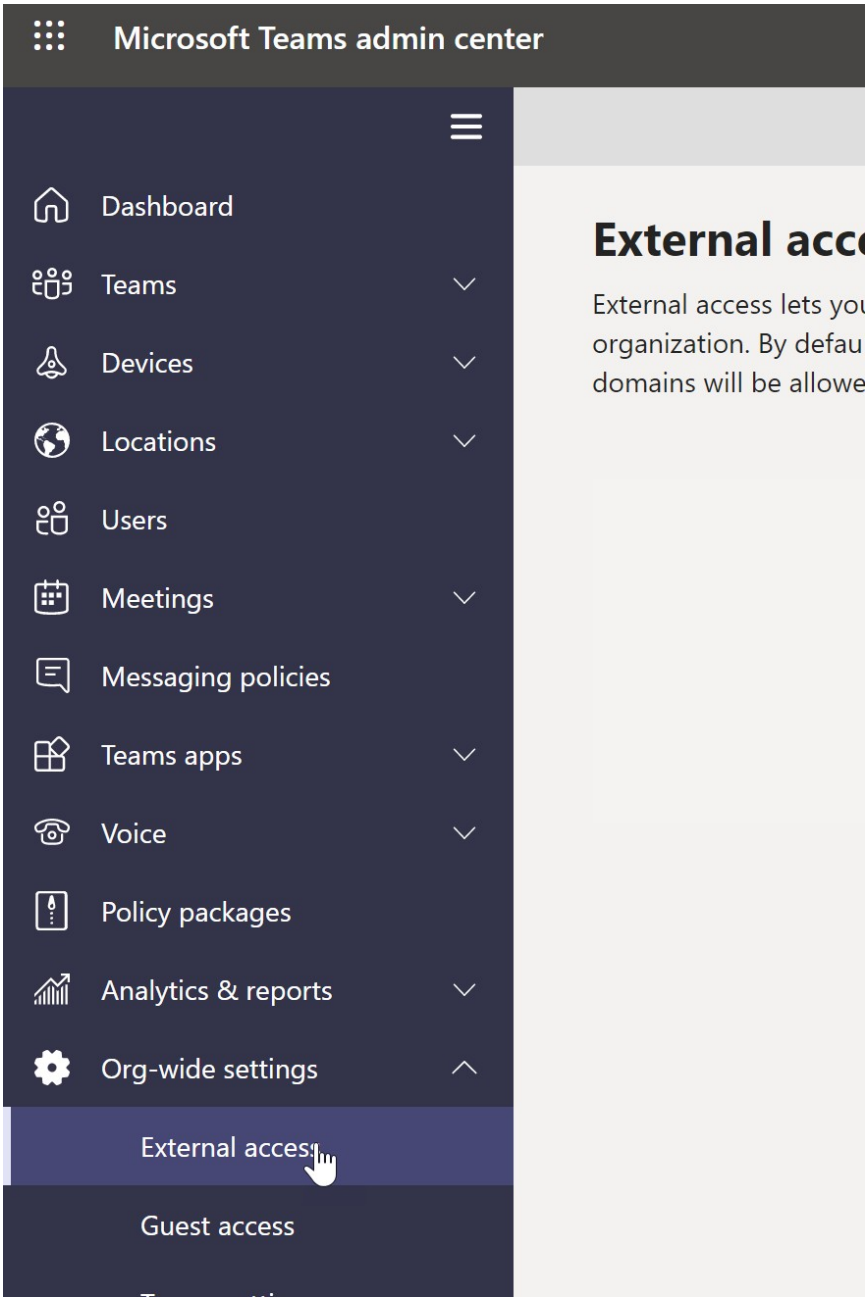
Description: You should not allow your users to communicate with Skype or Teams users outside your organization. While there are legitimate, productivity-improving scenarios for this, it also represents a potential security threat because those external users will be able to interact with your users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



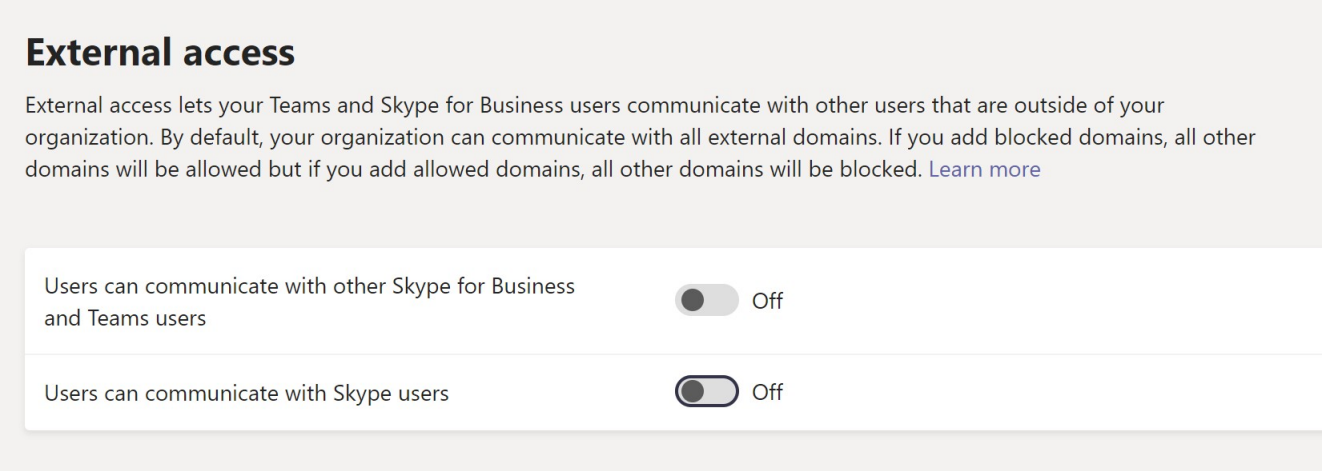
OVERVIEW & USER

2. Click Org-Wide Settings> External Access

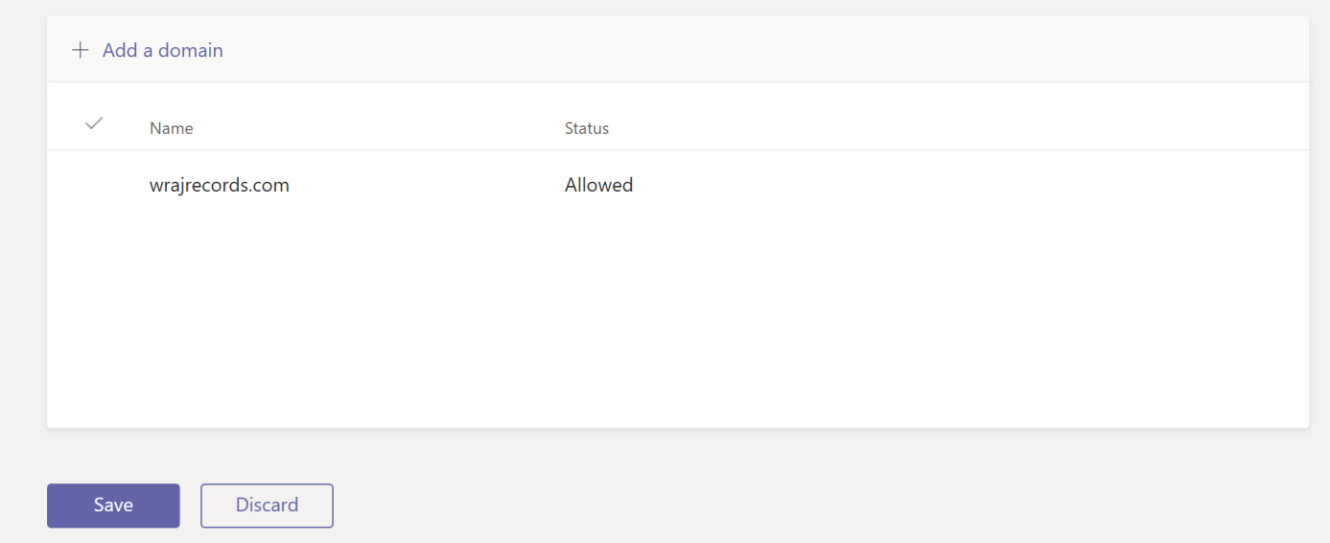


OVERVIEW & USER

3. Here, turn the toggles off:

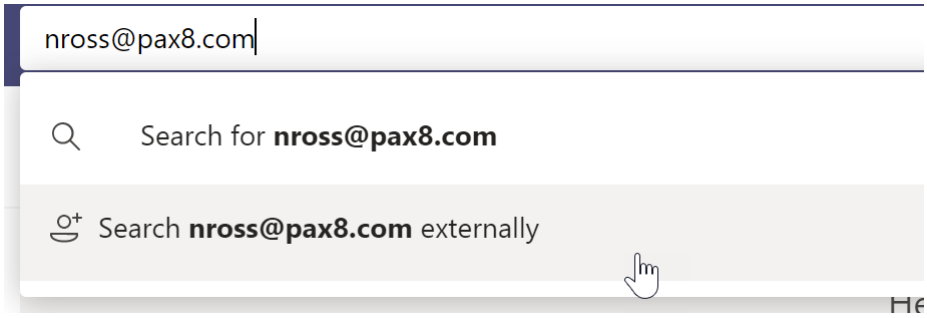


4. You can whitelist certain domains. This allows users to discover external users part of this domain and collaborate with them. This allows you to control the domains that users can collaborate with. Ensure that you have a proper, communicated method of how users can make request to collaborate with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

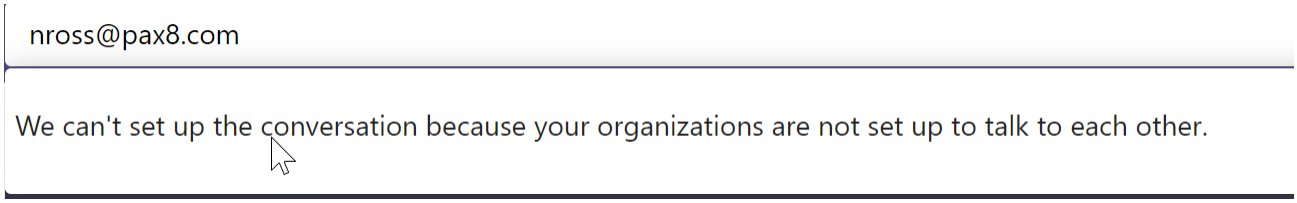


OVERVIEW & USER

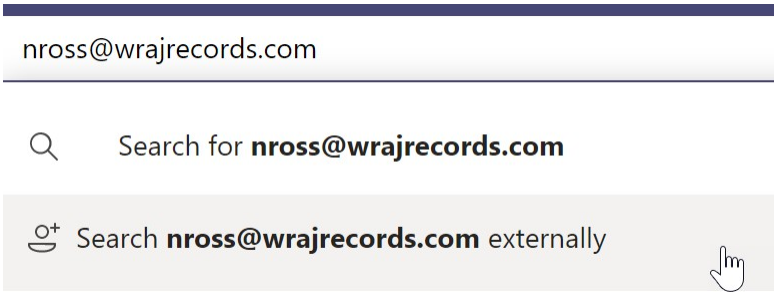
5. Users who search for external users in teams will see the following:

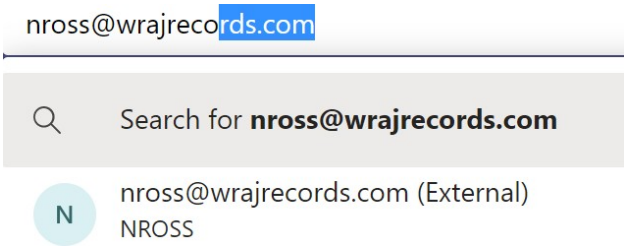


6. If they are not whitelisted, they will get the following when trying to search externally:

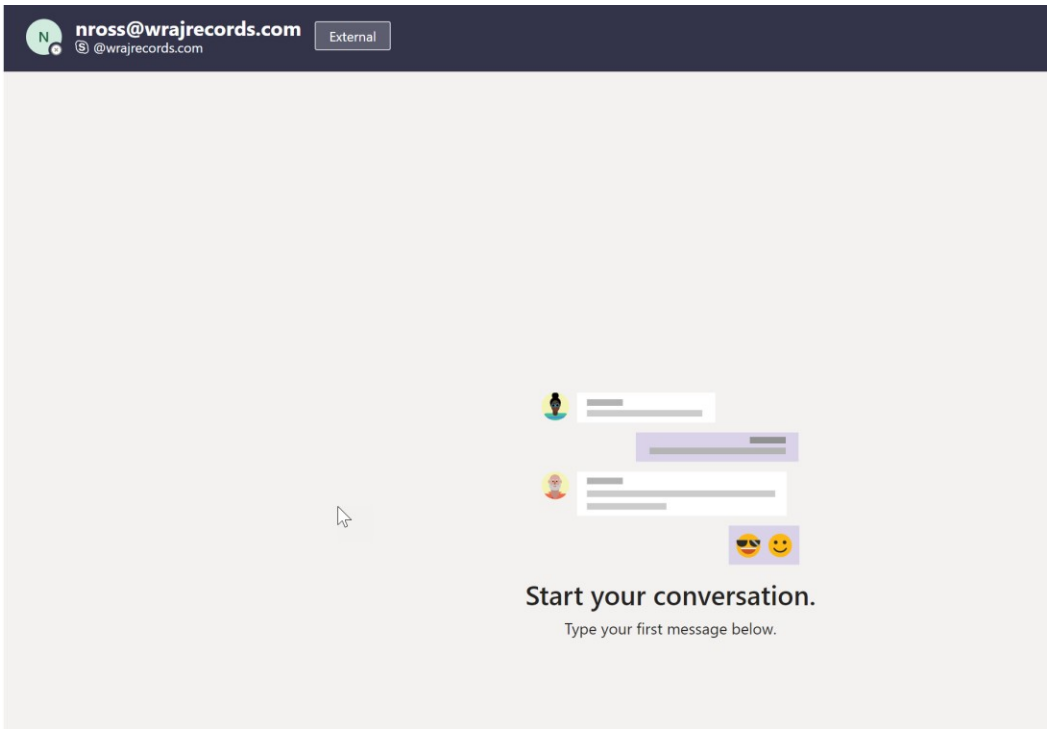


7. If the domain has been whitelisted, then users will have the following experience:





OVERVIEW & USER



RELEVANT COMPLIANCE CONTROLS:

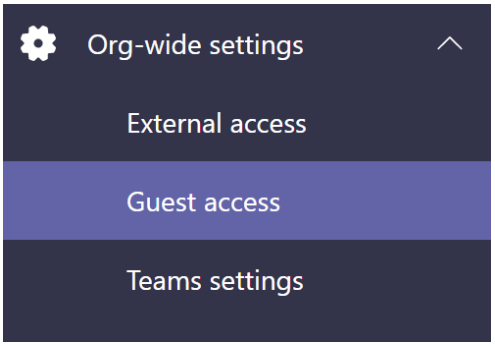
- NIST CSP DE.CM-7
- NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3,
- CM-8, PE-3, PE-6, PE-20, SI-4
- HIPAA Security Rule 45 C.F.R. §§
    - 164.308(a)(1)(ii)(D)
    - 164.312(b)
    - 164.314(b)(2)(i)

OVERVIEW & USER

LIMIT GUEST ACCESS

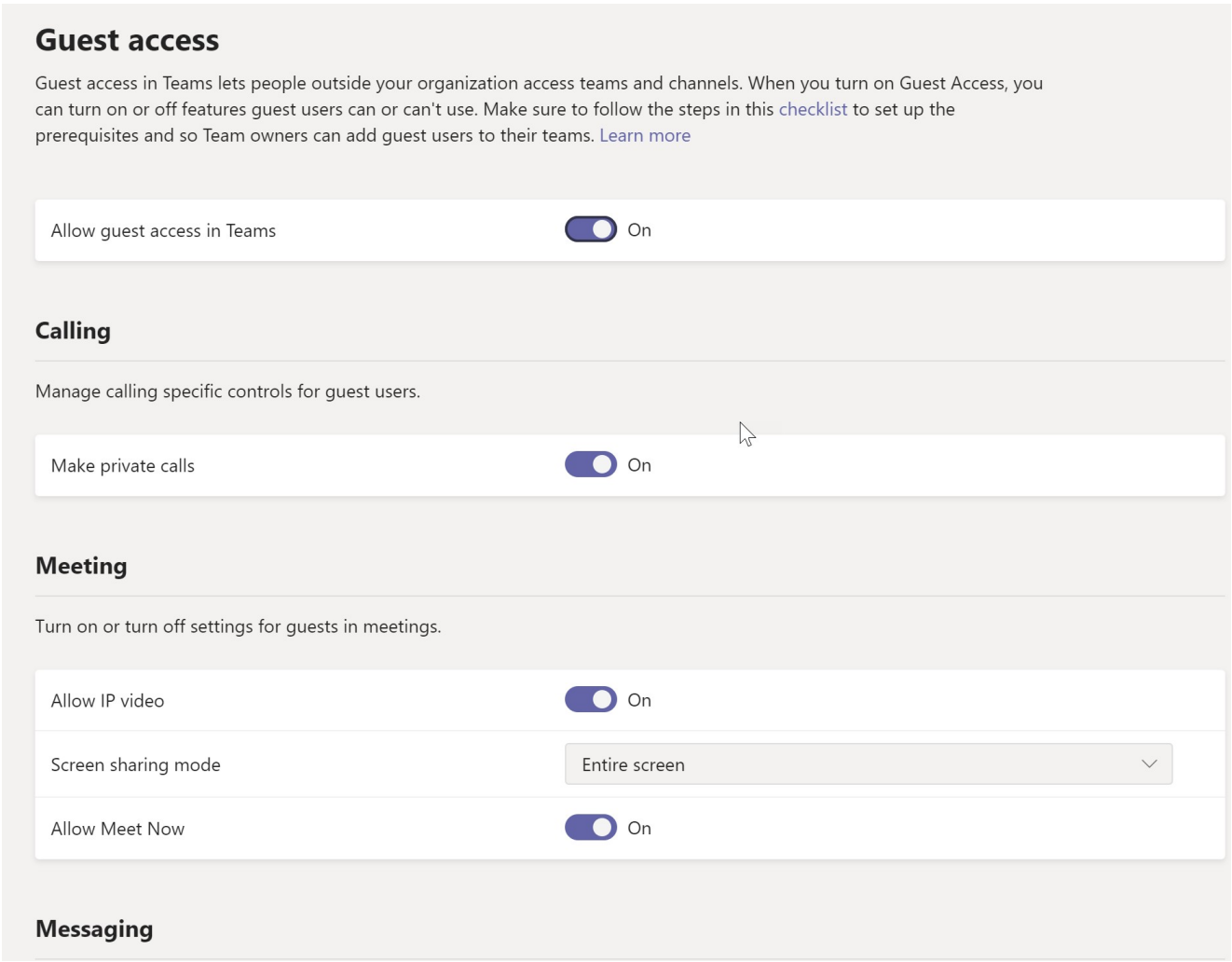
Description: By default, guess access in Teams is turned off. Team owners cannot add external users to any Teams channels. You can change this setting in the Teams admin center and external users can be invited to Teams Channels by owners of that channel. You should have a formal request process defined 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.



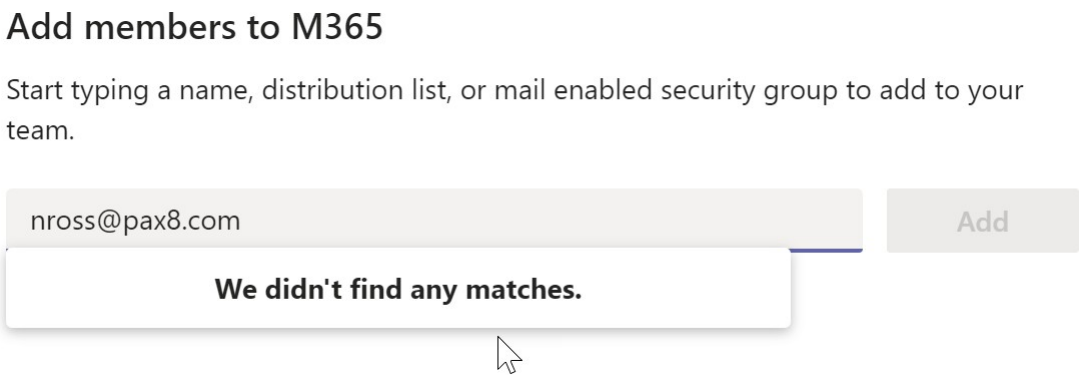
OVERVIEW & USER

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

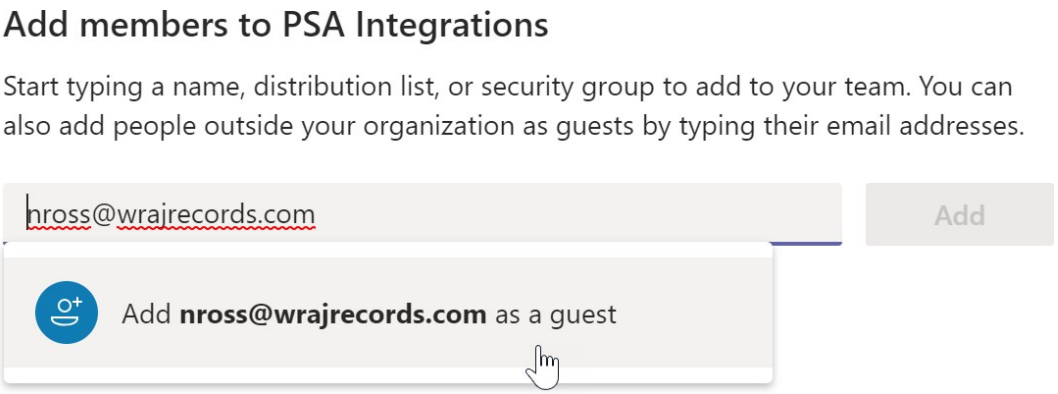


OVERVIEW & USER

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

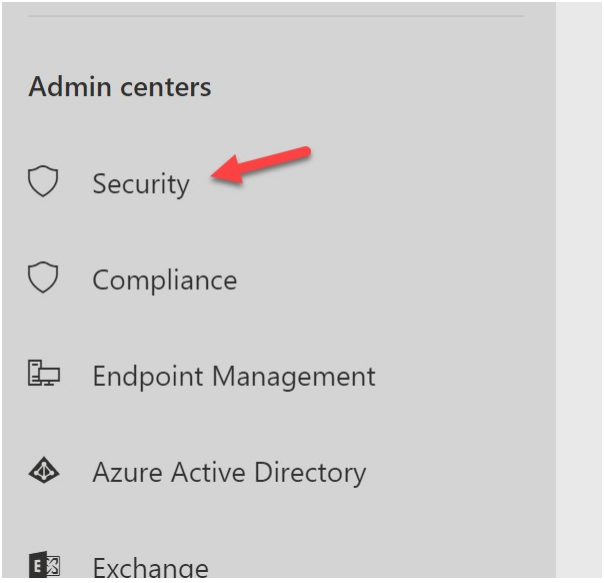


4. If Guess access is turned on, then owners can send invites to external participants:

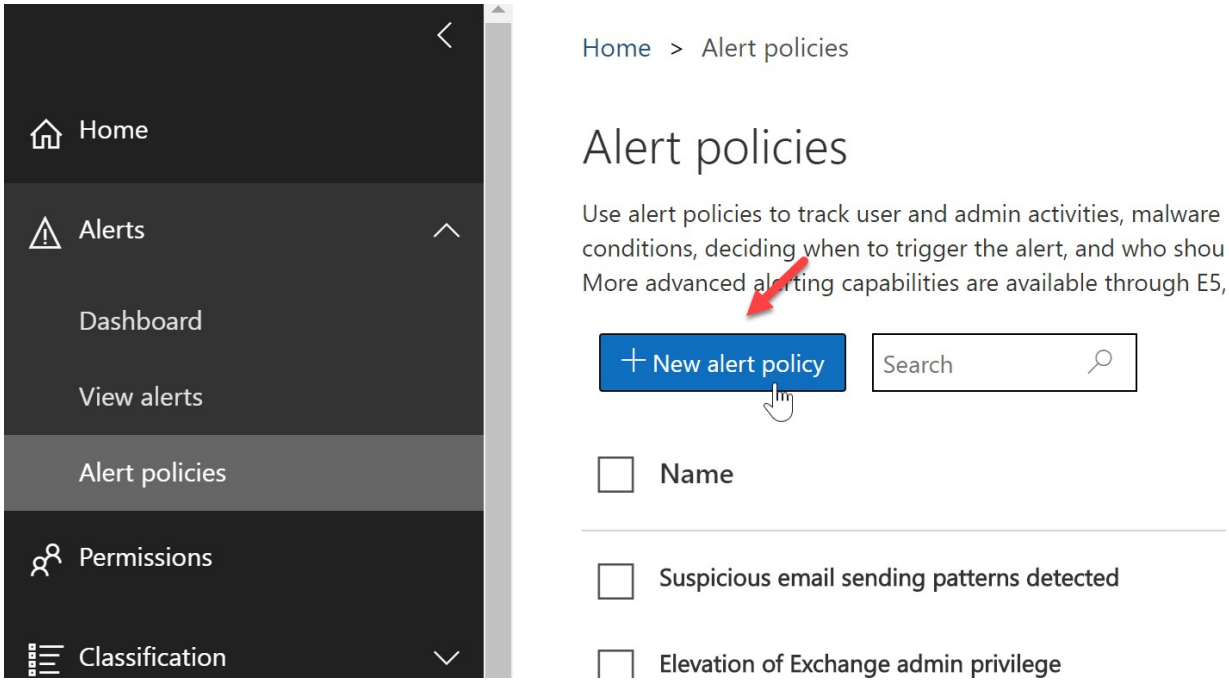


OVERVIEW & USER

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:

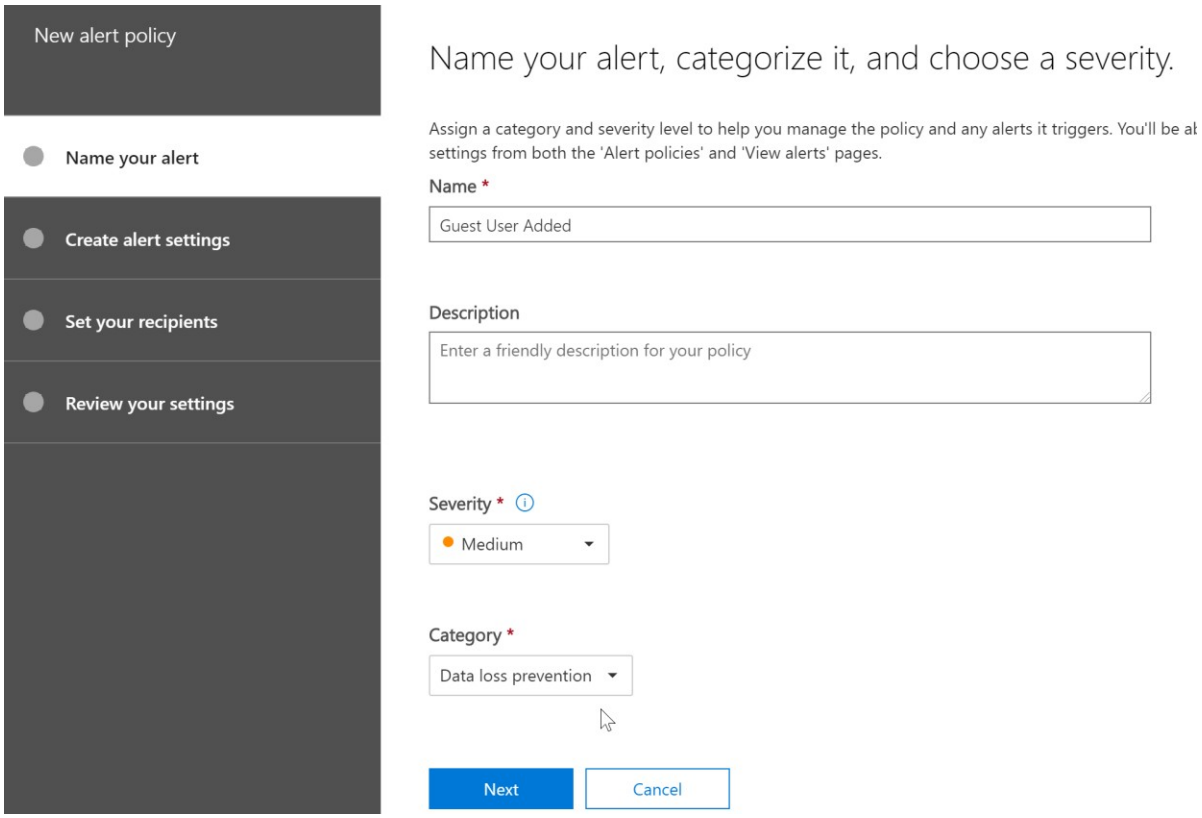


6. Click on Alerts>Alert policies>New Alert Policy:

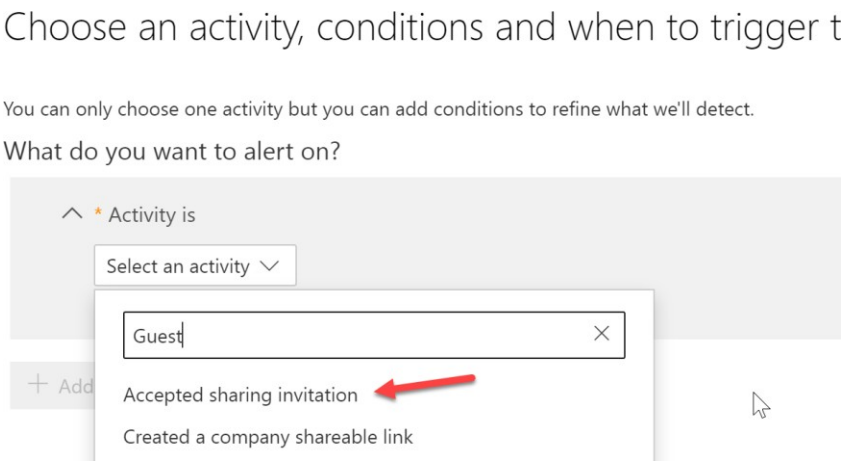


OVERVIEW & USER

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

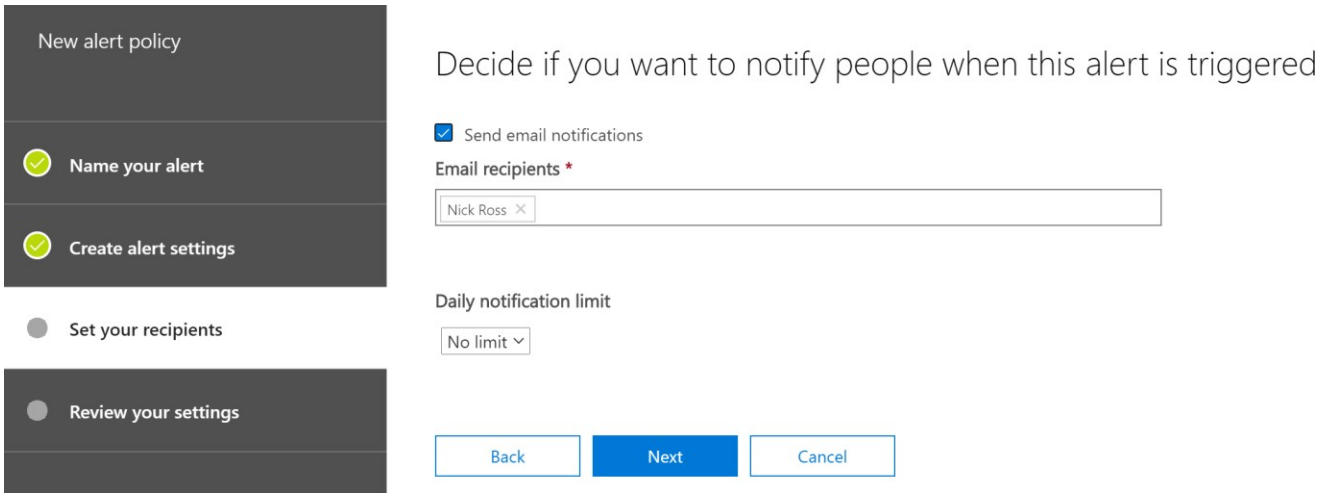


8. Type 'Guest' and select 'Accepted a sharing invitation'>Click Next:

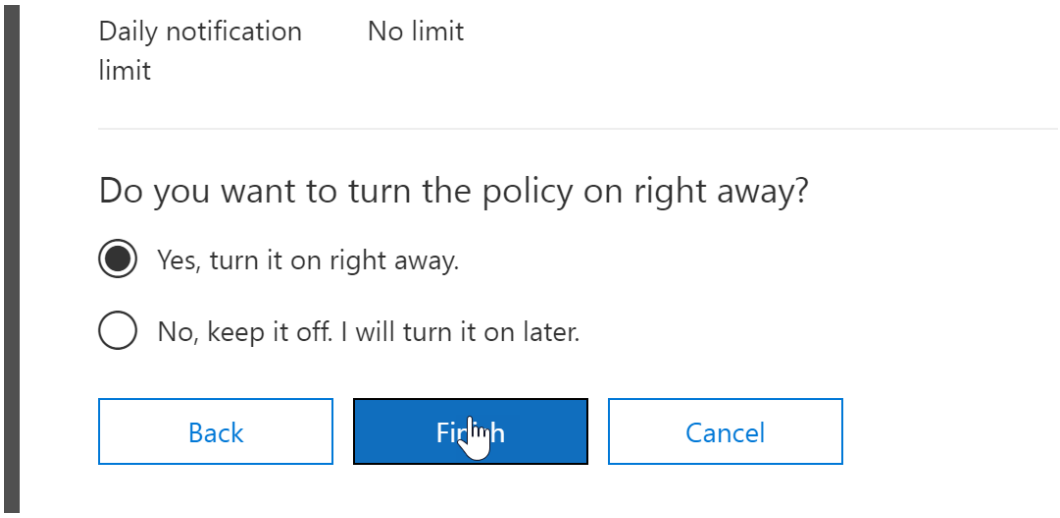


OVERVIEW & USER

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



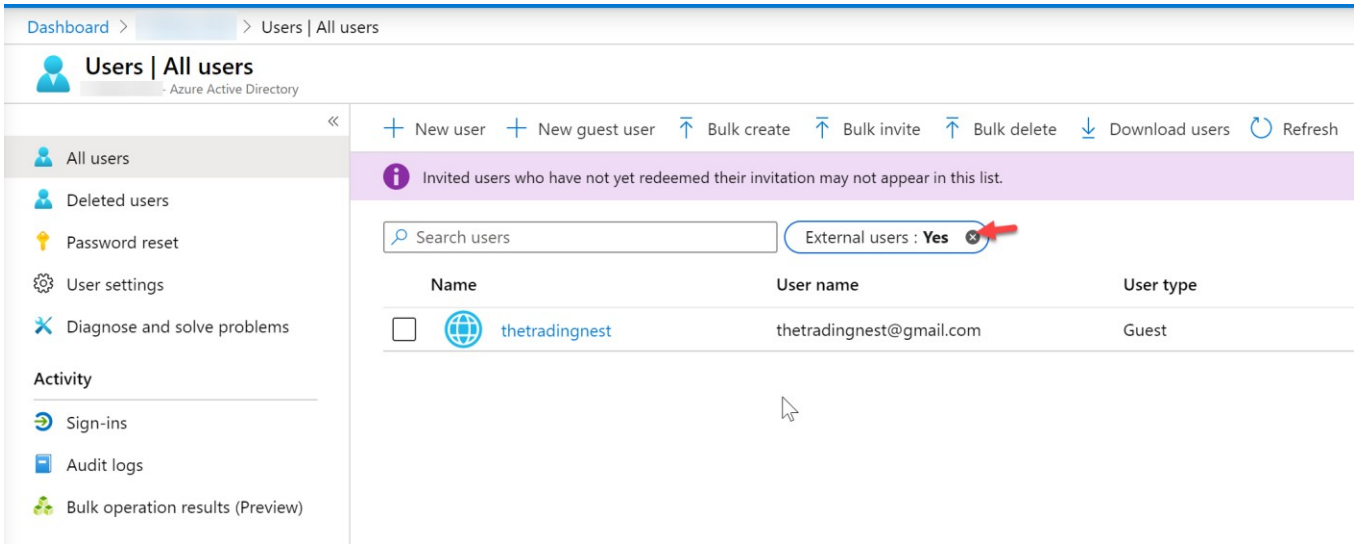
10. Review and Turn on the Alert:



OVERVIEW & USER

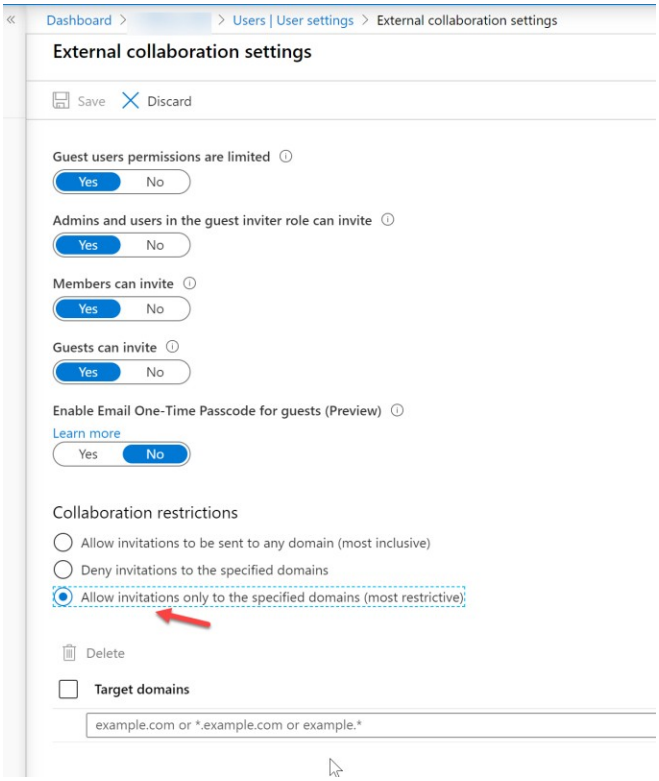
ADDITIONAL CONSIDERATIONS:

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



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:

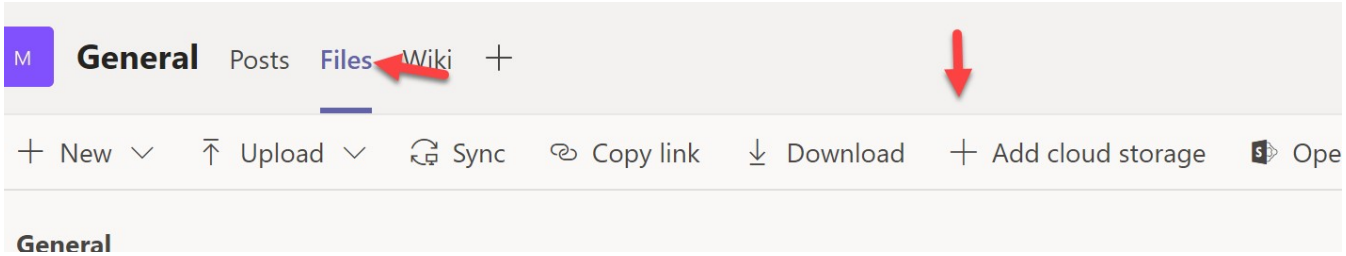
- NIST CSP DE.CM-7
- NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3,
- CM-8, PE-3, PE-6, PE-20, SI-4
- HIPAA Security Rule 45 C.F.R. §§
  - 164.308(a)(1)(ii)(D)
  - 164.312(b)
  - 164.314(b)(2)(i)

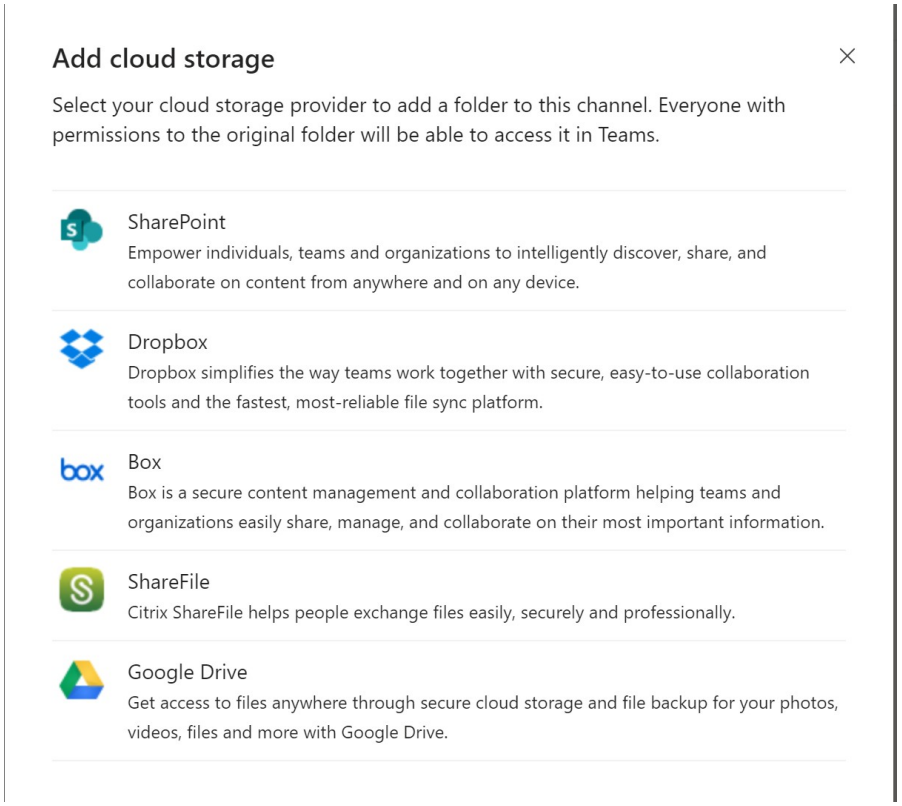
OVERVIEW & USER

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

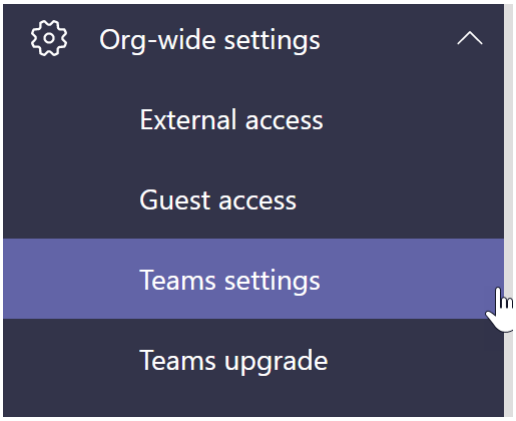
Ex.



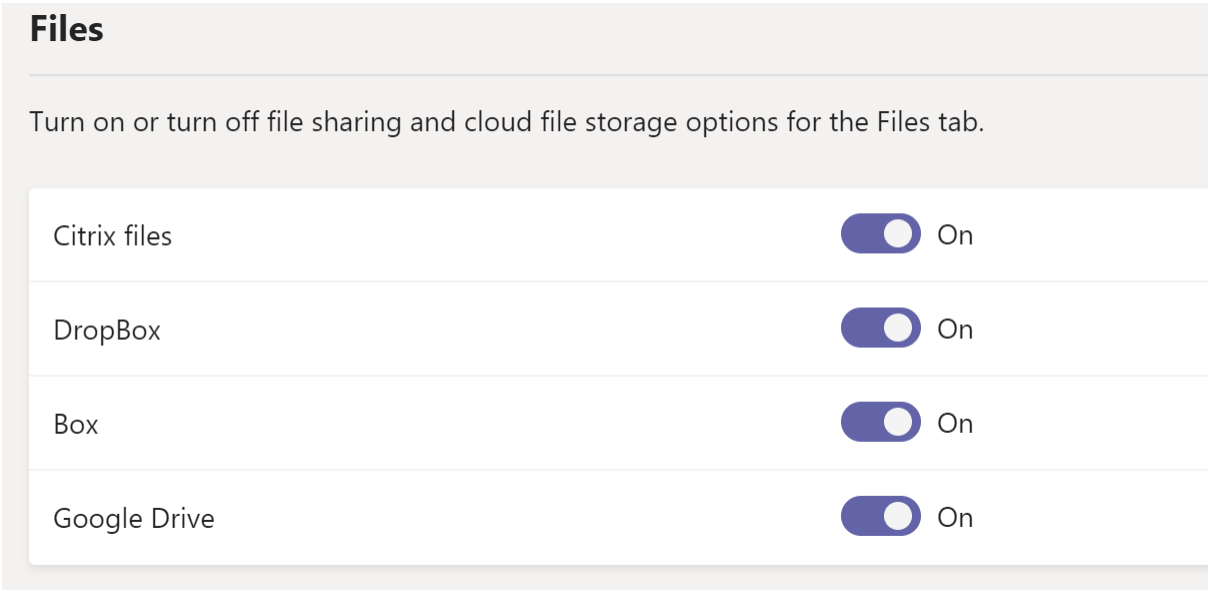


OVERVIEW & USER

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:



OVERVIEW & USER

RELEVANT COMPLIANCE CONTROLS:

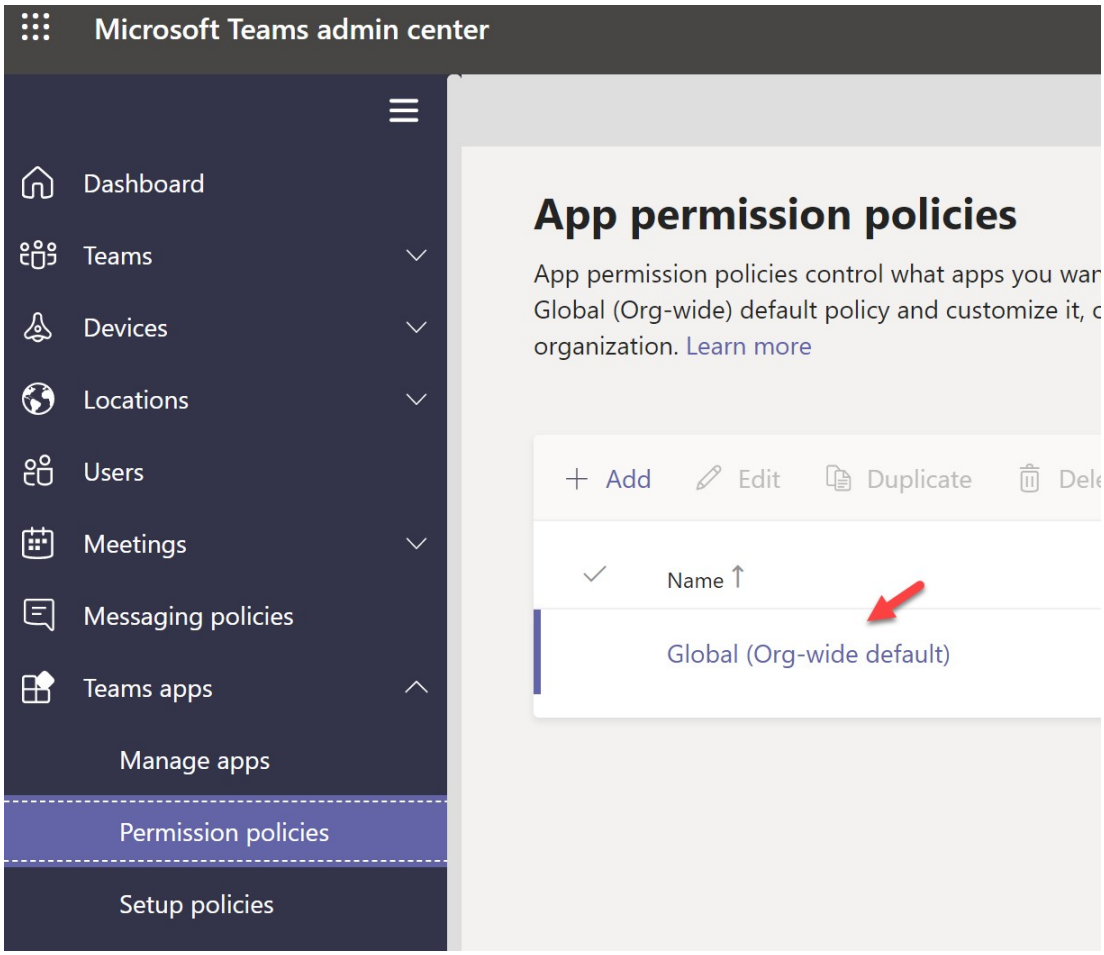
- NIST CSF PR-DS-5
- CCS CSC 17
- COBIT 5 APO01.06
- ISA 62443-3-3:2013 SR 5.2
- ISO/IEC 27001:2013 A.6.1.2, A.7.1.1,
- A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1,
- A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5,
- A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4,
- A.14.1.2, A.14.1.3
- NIST SP 800-53 Rev. 4 AC-4, 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

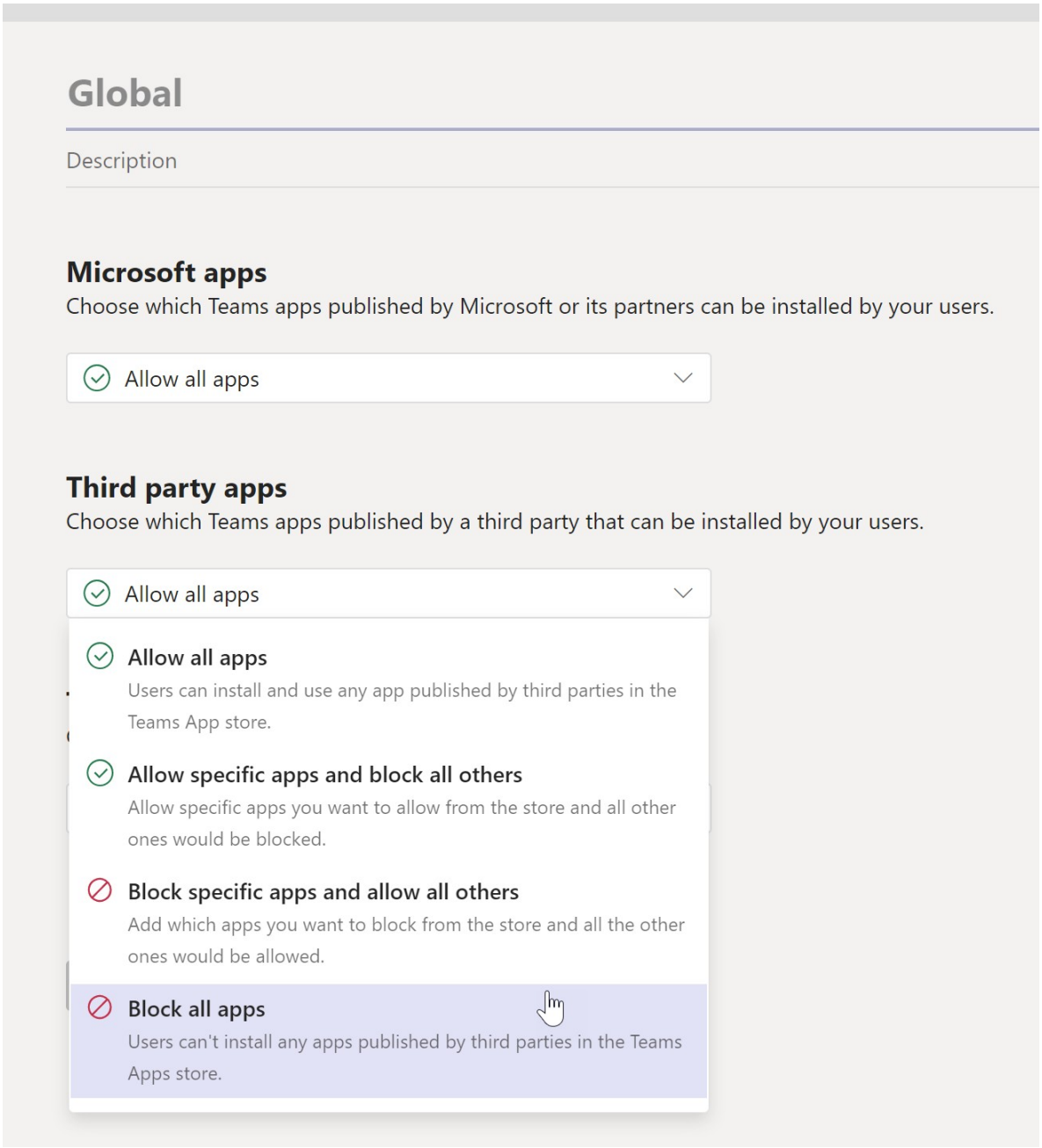
Description: By default, all users have access to the Teams app store which contains applications published by Microsoft and other third parties. While we do not want to inhibit productivity, we do want to ensure we are preventing data loss and shadow IT at the organization. Any of these apps can be 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:



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,
    - oA.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1,
    - oA.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5,
    - o A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4,
    - o 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. §§
    - o 164.308(a)(1)(ii)(D), 164.308(a)(3),
    - o 164.308(a)(4)
    - o 164.312(a), 164.312(e)

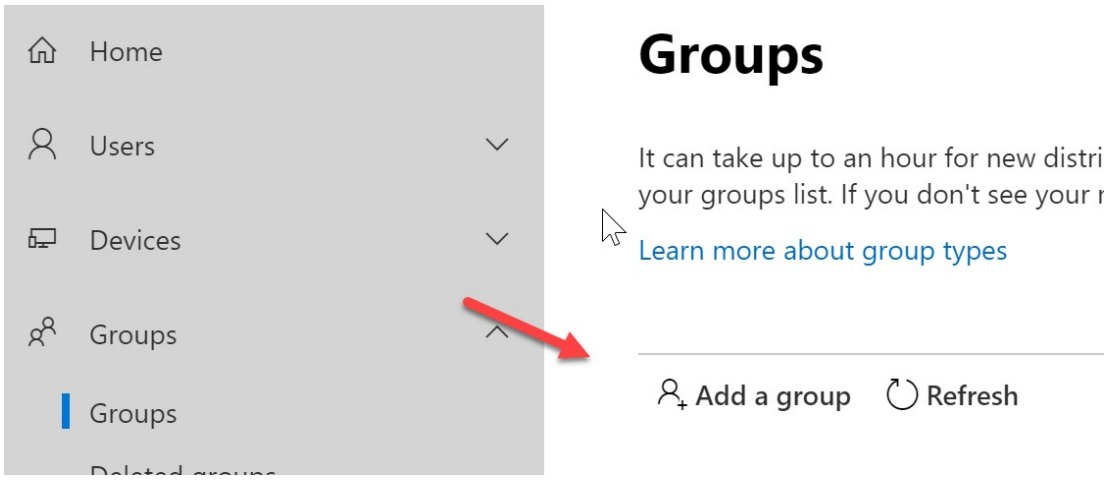
OVERVIEW & USER

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.

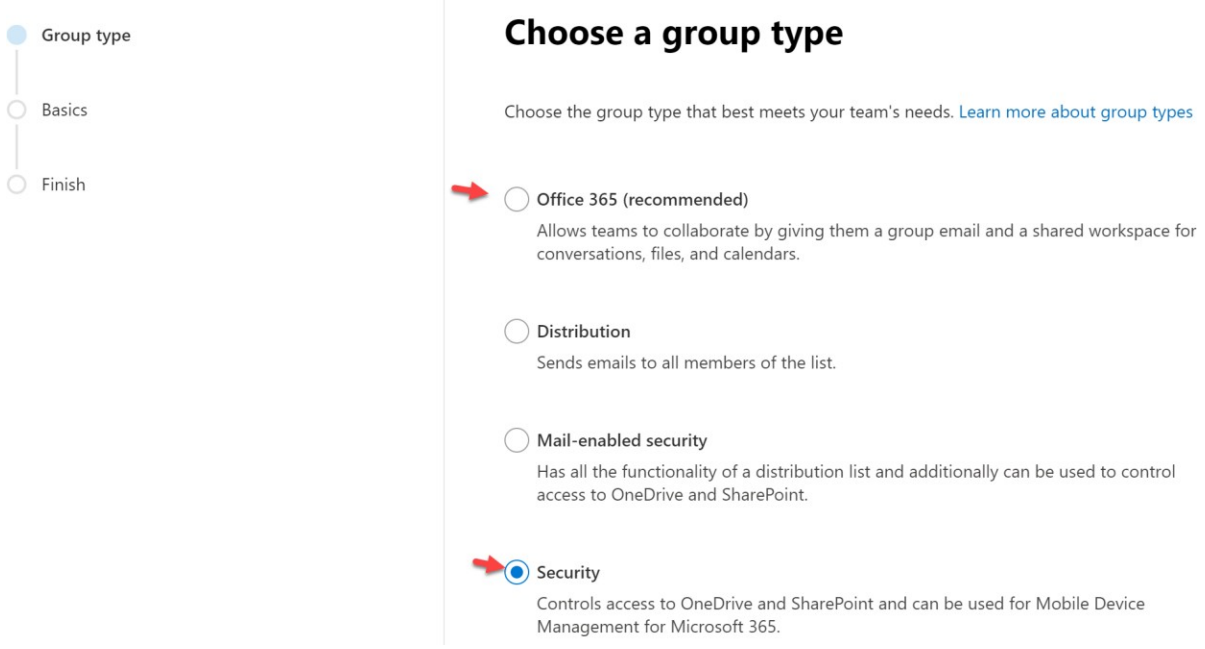
NOTE It is very important that you properly plan and communicate any changes here before rolling them out. The goal is not to inhibit productivity and force users to go to outside channels to collaborate, causing shadow IT. It is imperative that you make the request for creating a new Teams channel as 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

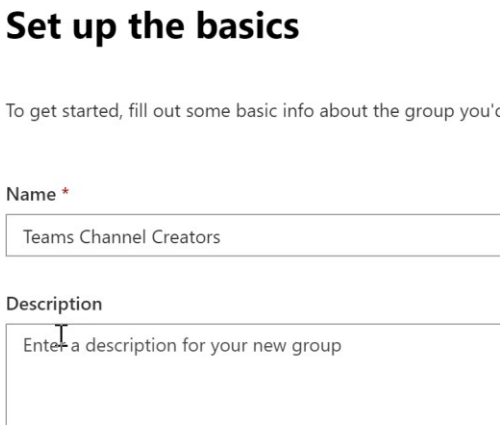


OVERVIEW & USER

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



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



OVERVIEW & USER

4. Click on the following link and Scroll down to the powershell section:

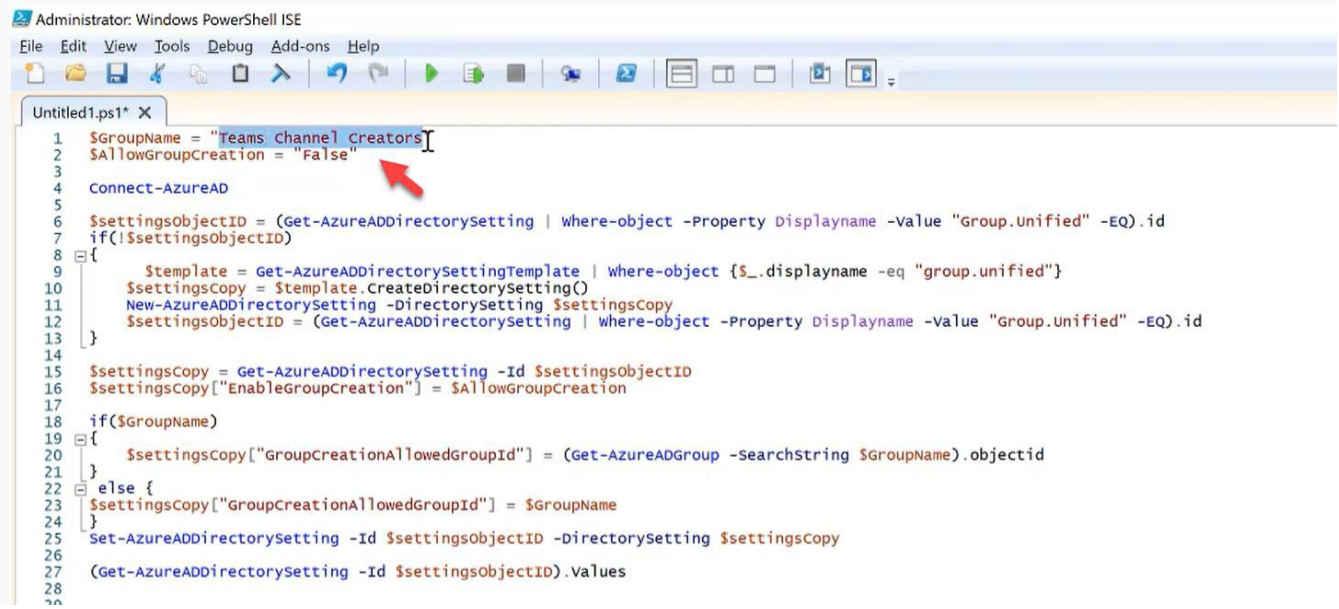
PowerShell Copy

```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
```

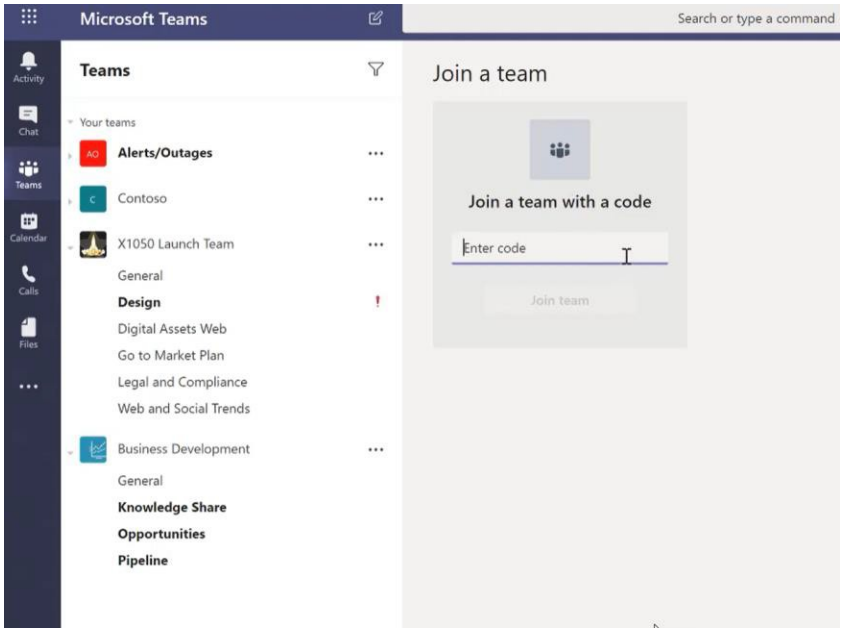
5. Run Powershell ISE as Admin (64x version) and run the following command: Import-Module AzureADPreview

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:



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
- 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)

OVERVIEW & USER

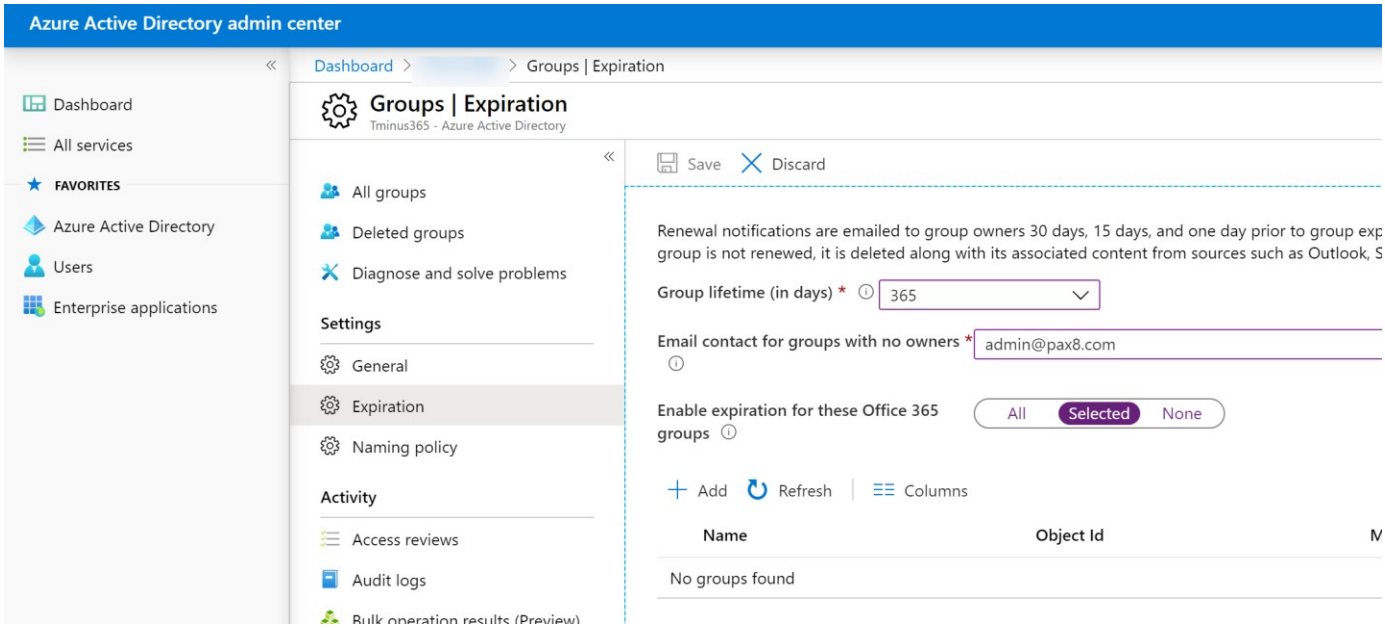
SET TEAMS EXPIRATION

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.

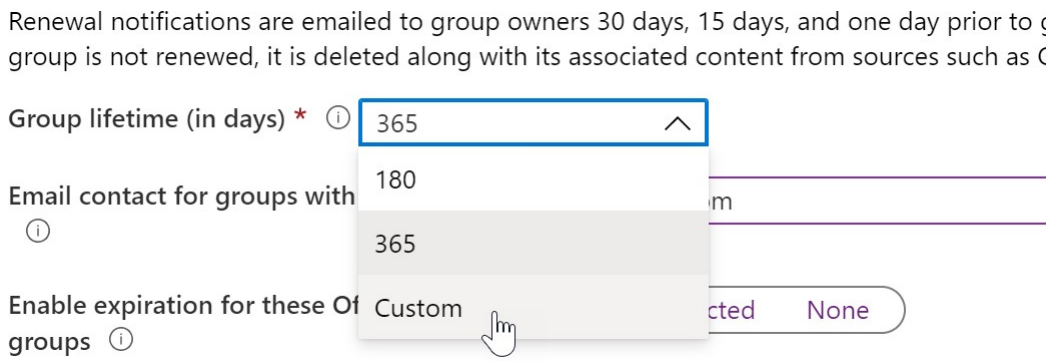
1. In the 365 Admin Center, go to Admin Centers>Azure Active Directory>Groups>Expiration

OVERVIEW & USER



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



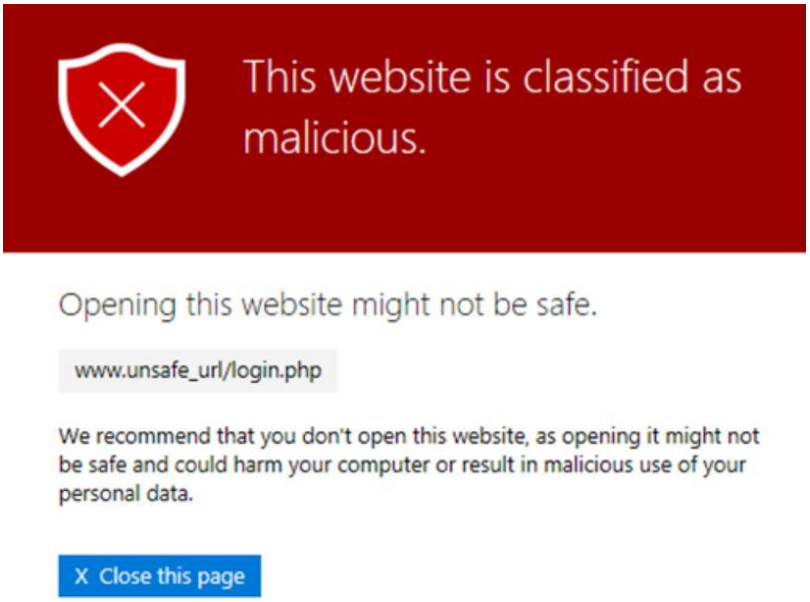
RELEVANT COMPLIANCE CONTROLS:

- 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
- 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)

OVERVIEW & USER

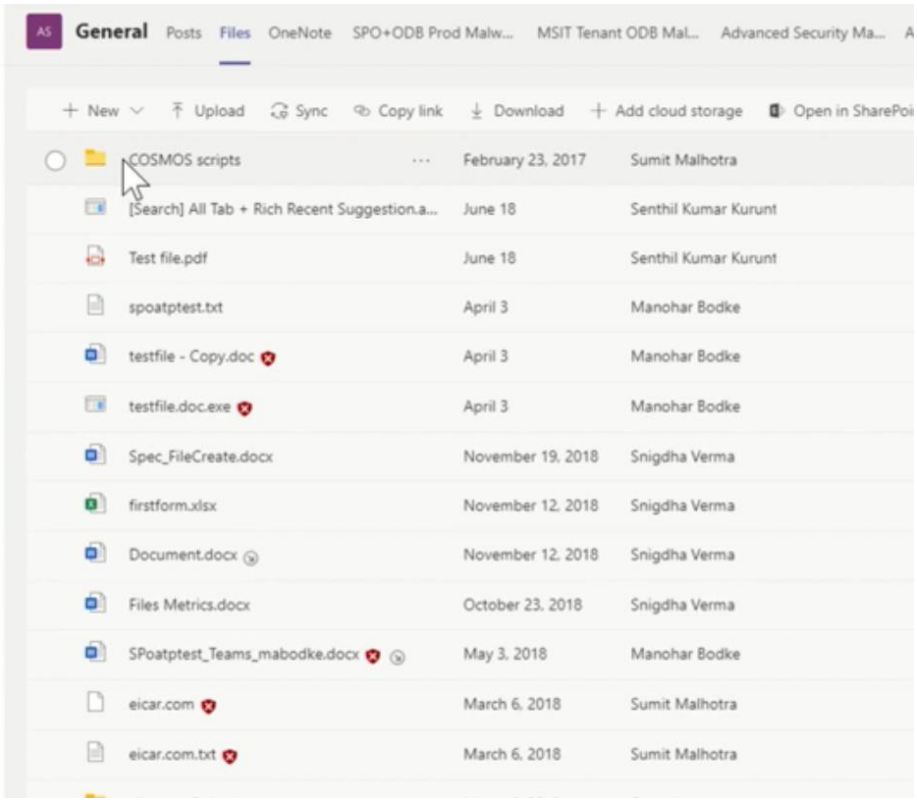
SET UP ADVANCED THREAT PROTECTION POLICIES FOR TEAMS

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.



OVERVIEW & USER

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



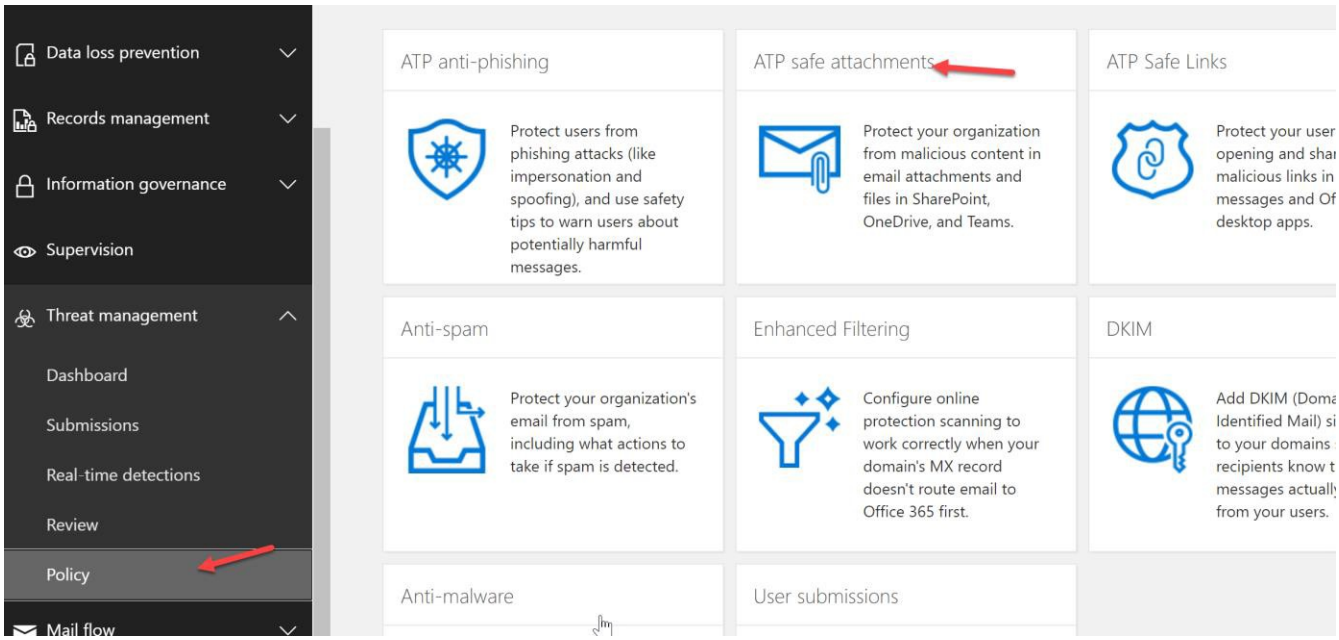
License Requirements:

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

OVERVIEW & USER

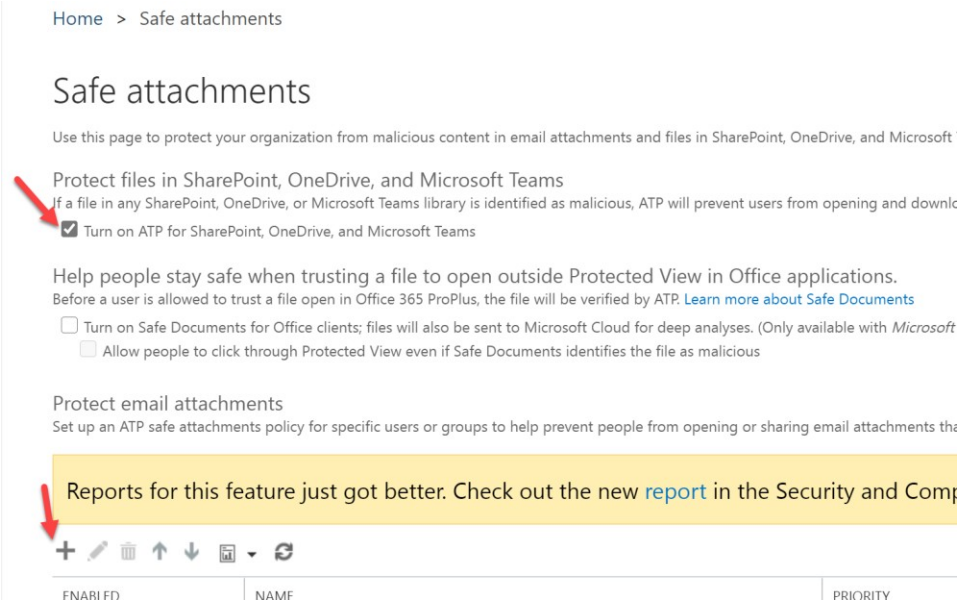
1. In the 365 Admin Center, click Admin Centers>Security

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

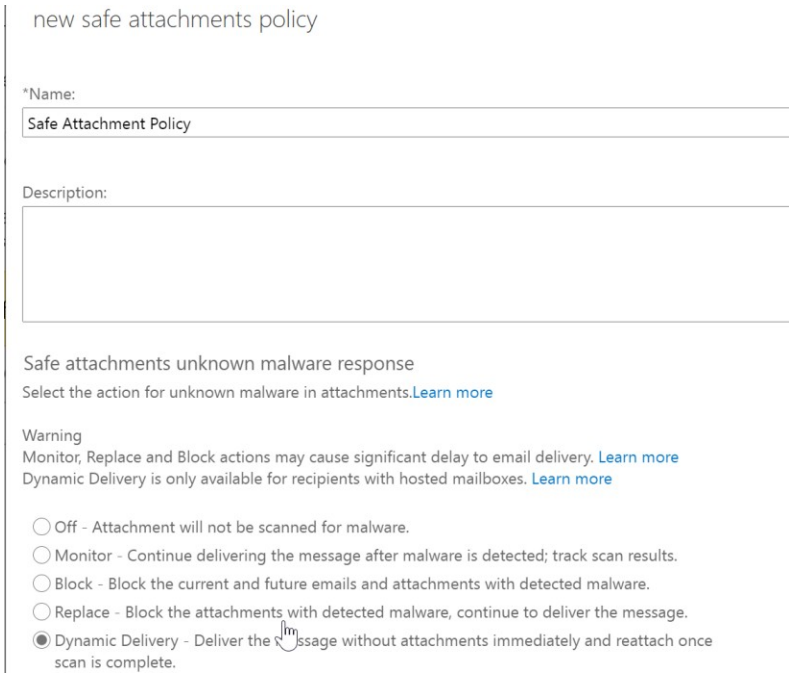


OVERVIEW & USER

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

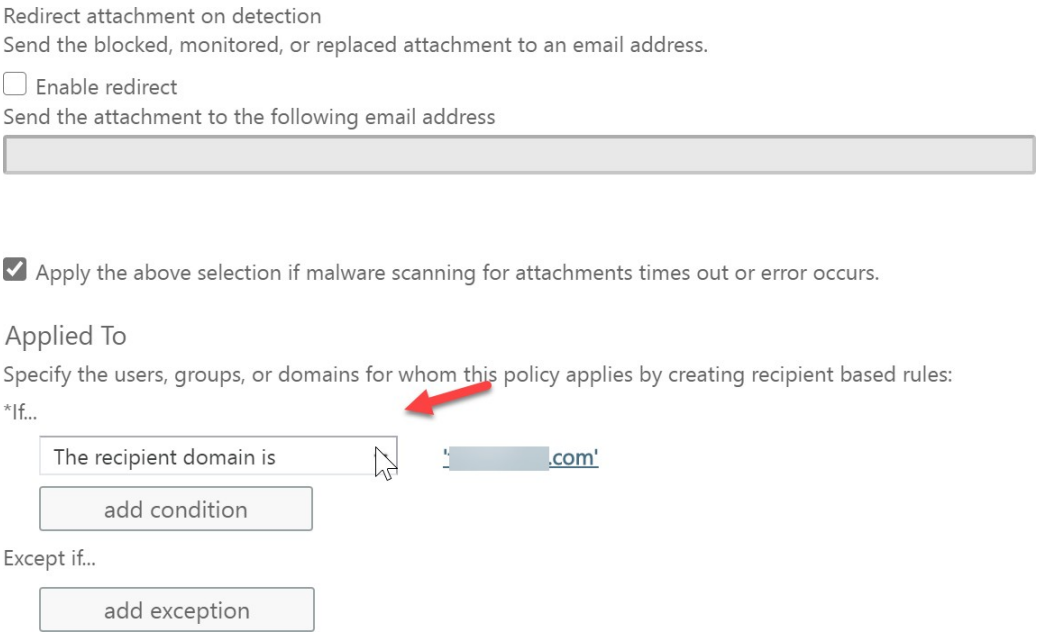


4. Add Name, Description, and choose Dynamic Delivery. For more on delivery methods, click here:

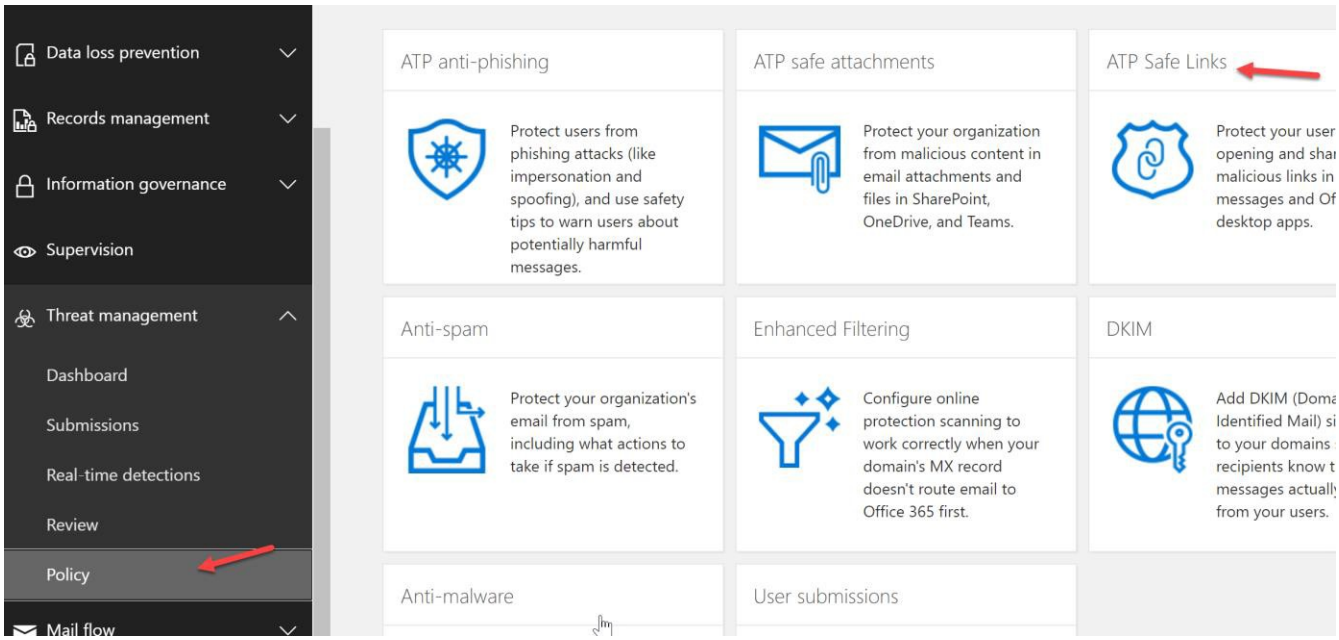


OVERVIEW & USER

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

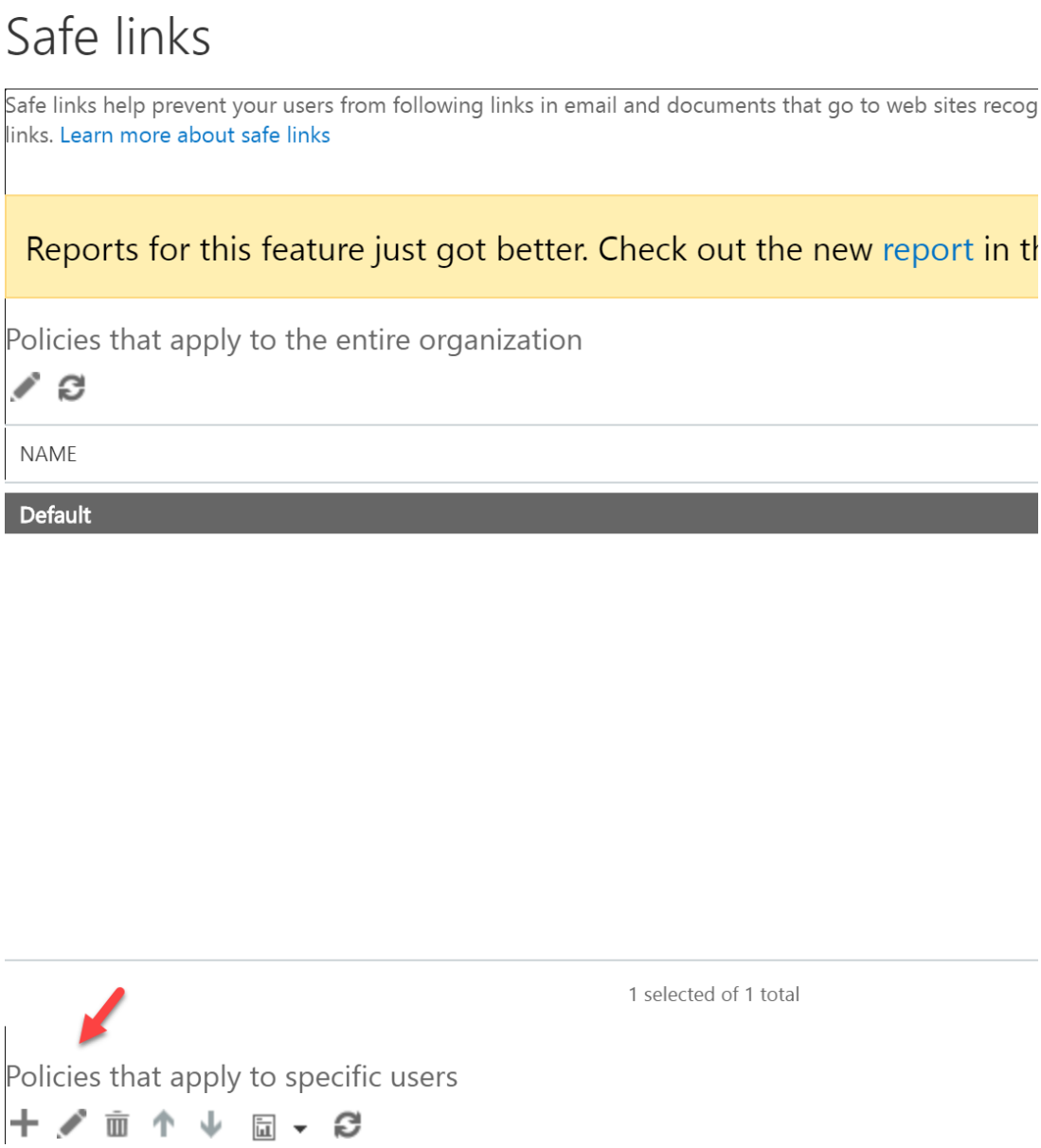


6. For Safe Links, go back to Threat management>Policy>Safe Links



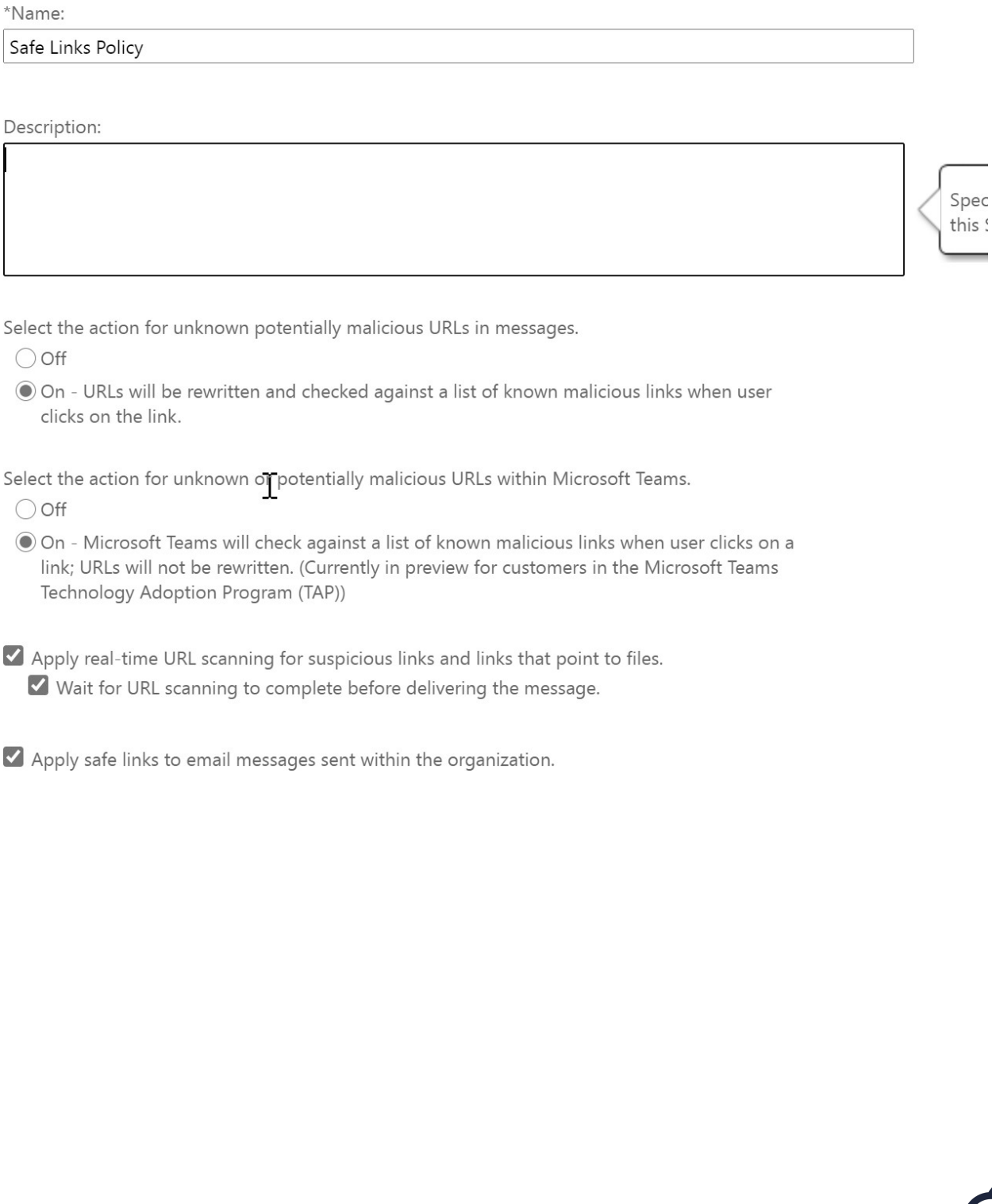
OVERVIEW & USER

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



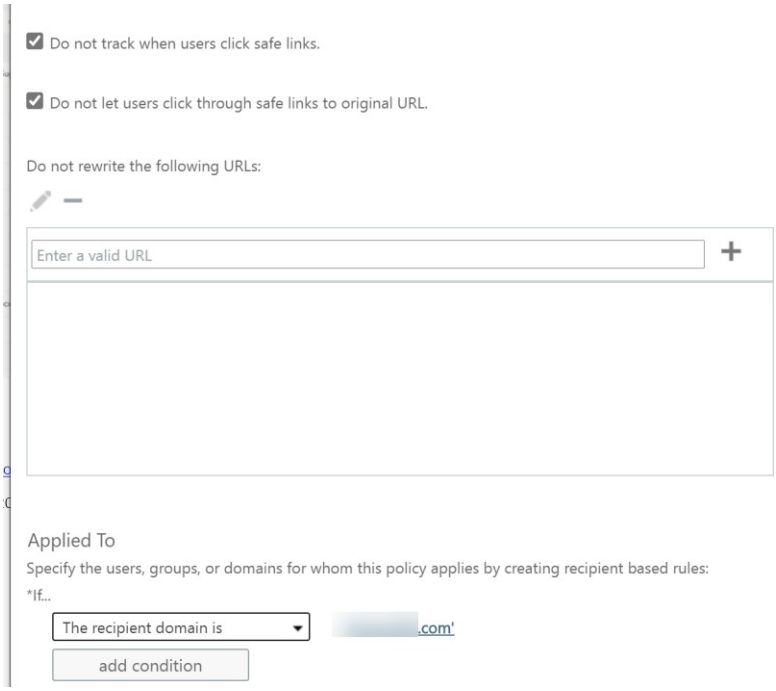
OVERVIEW & USER

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



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.



RELEVANT COMPLIANCE CONTROLS:

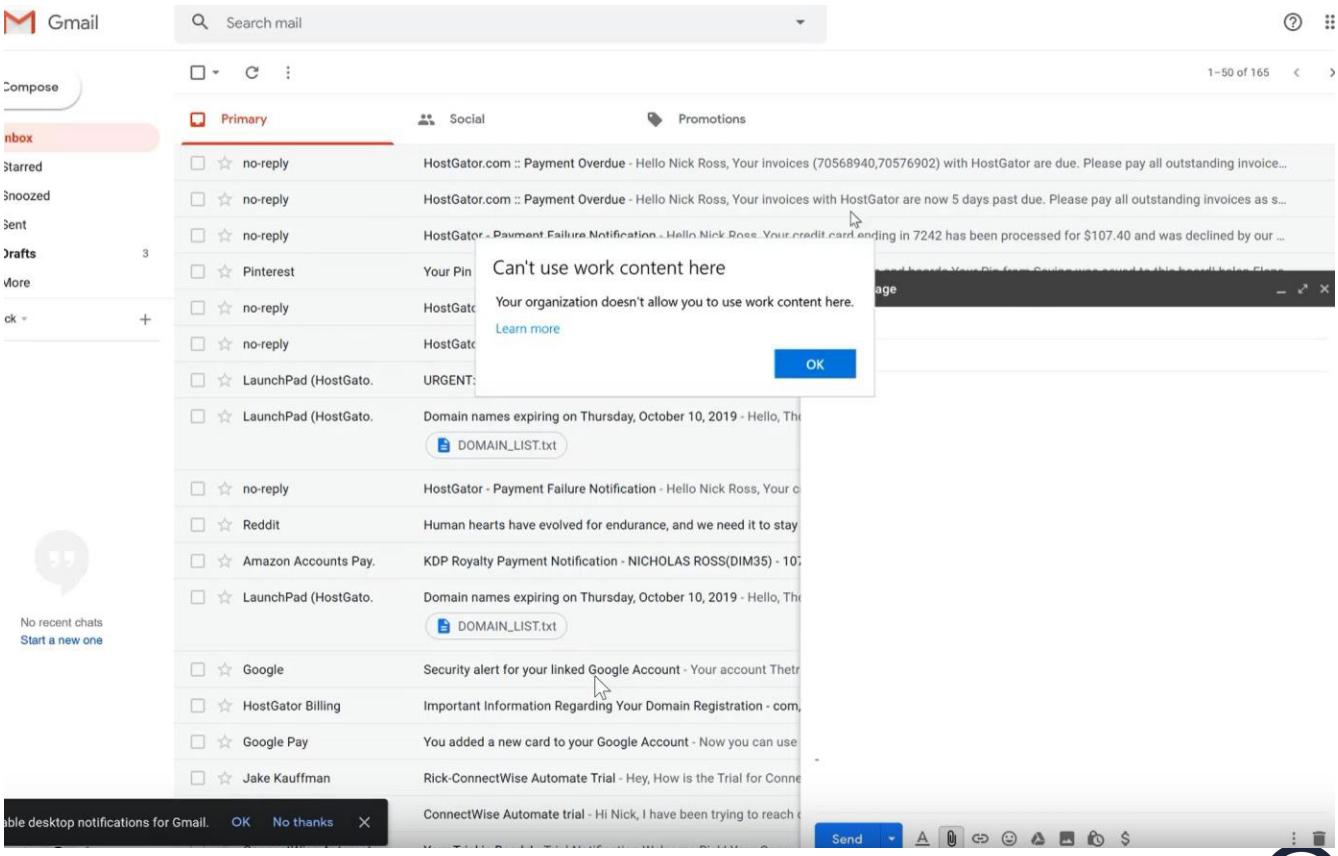
- NIST CSF DE.CM-4
- CCS CSC 5
- COBIT 5 DSS05.01
- ISA 62443-2-1:2009 4.3.4.3.8
- ISA 62443-3-3:2013 SR 3.2
- ISO/IEC 27001:2013 A.12.2.1
- NIST SP 800-53 Rev. 4 SI-3
- HIPAA Security Rule 45 C.F.R. §§
    - 164.308(a)(5)(ii)(B)

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:

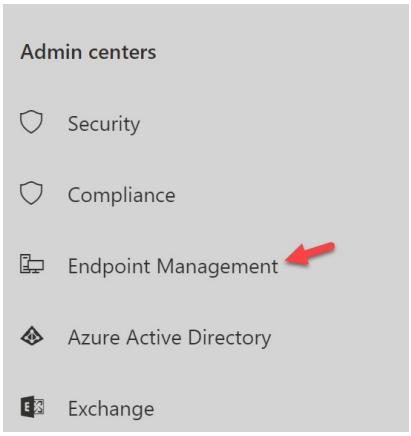


OVERVIEW & USER

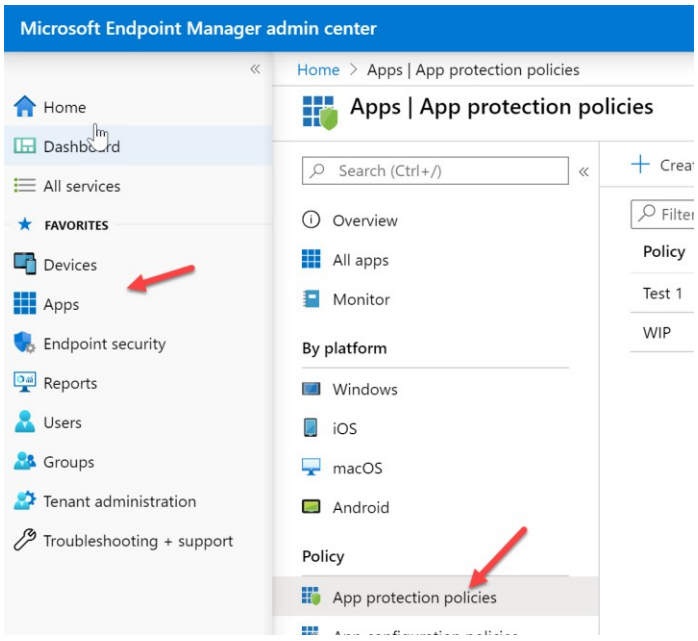
License Requirements:

- 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

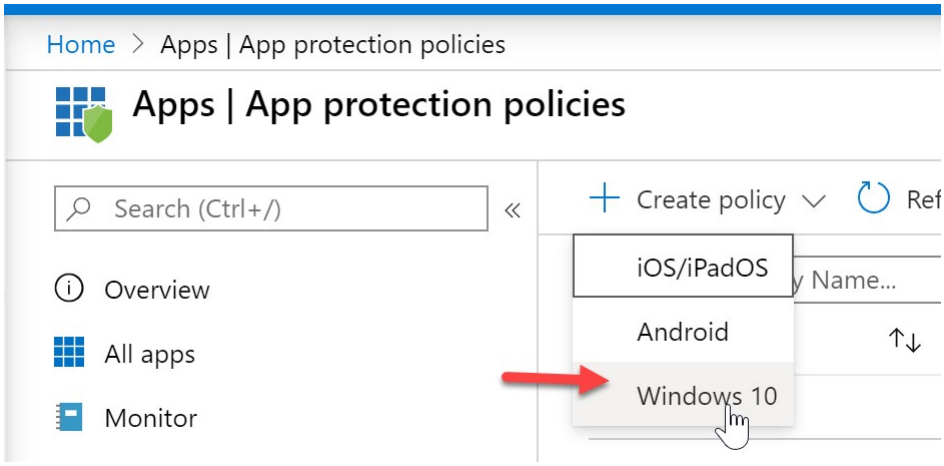


2. Click Apps>App ProtectionPolicies

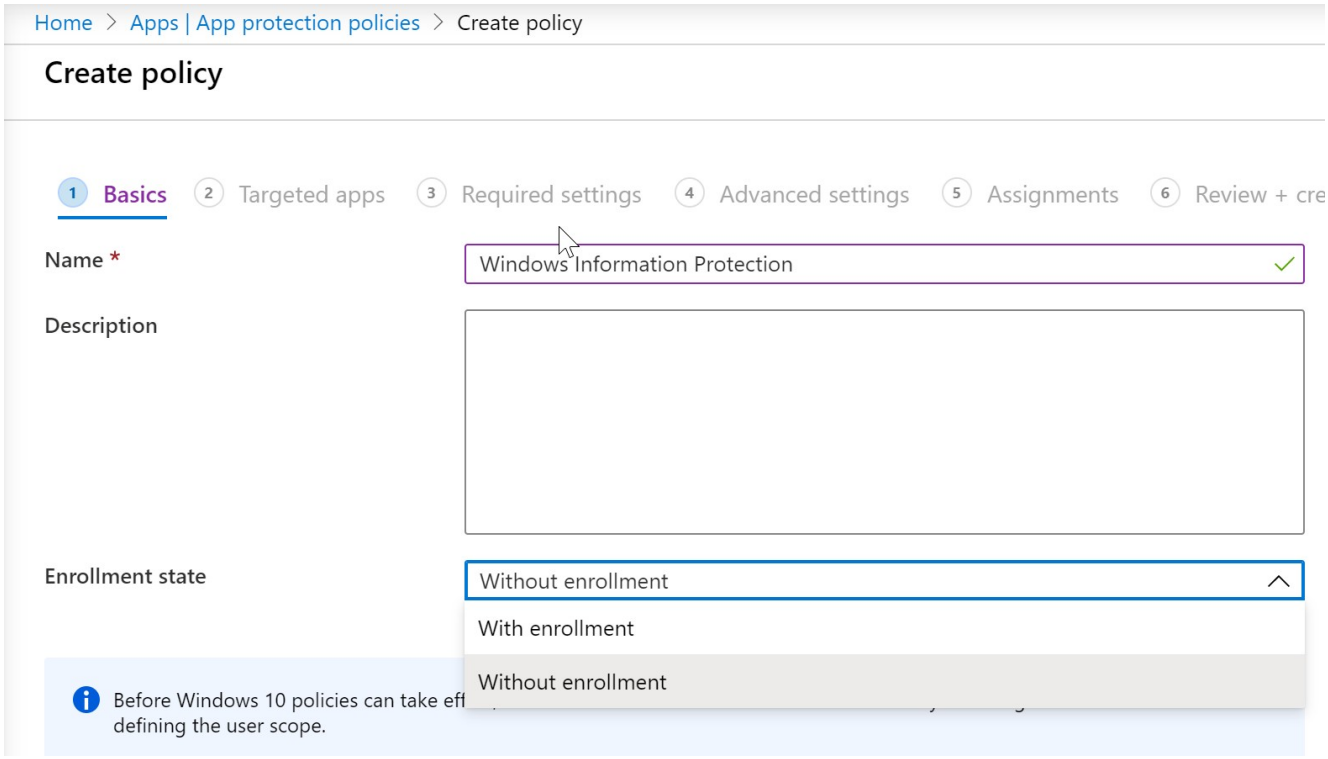


OVERVIEW & USER

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

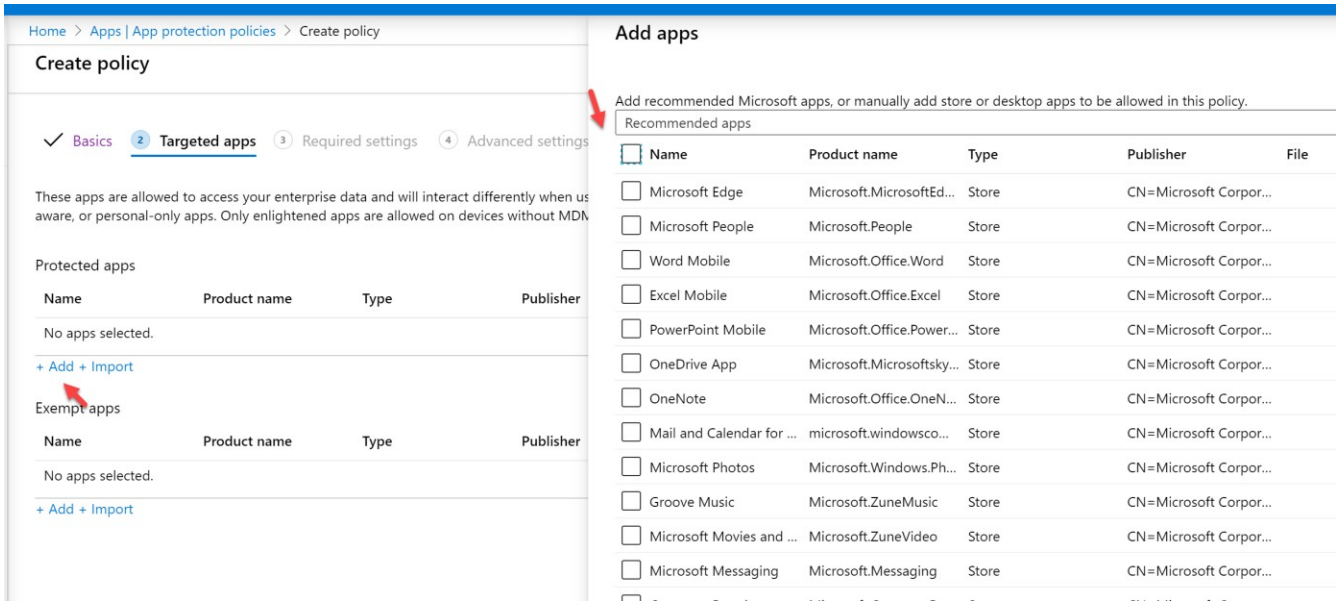


4. Here you can name the policy and chose devices enrolled in Intune or not enrolled. For this example, we will choose not enrolled:

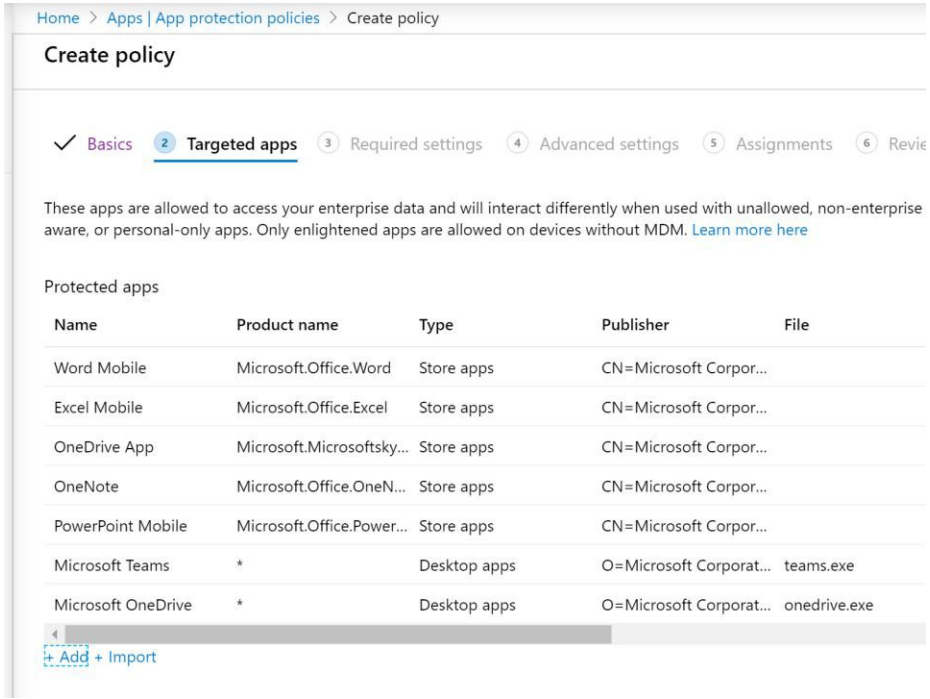


OVERVIEW & USER

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

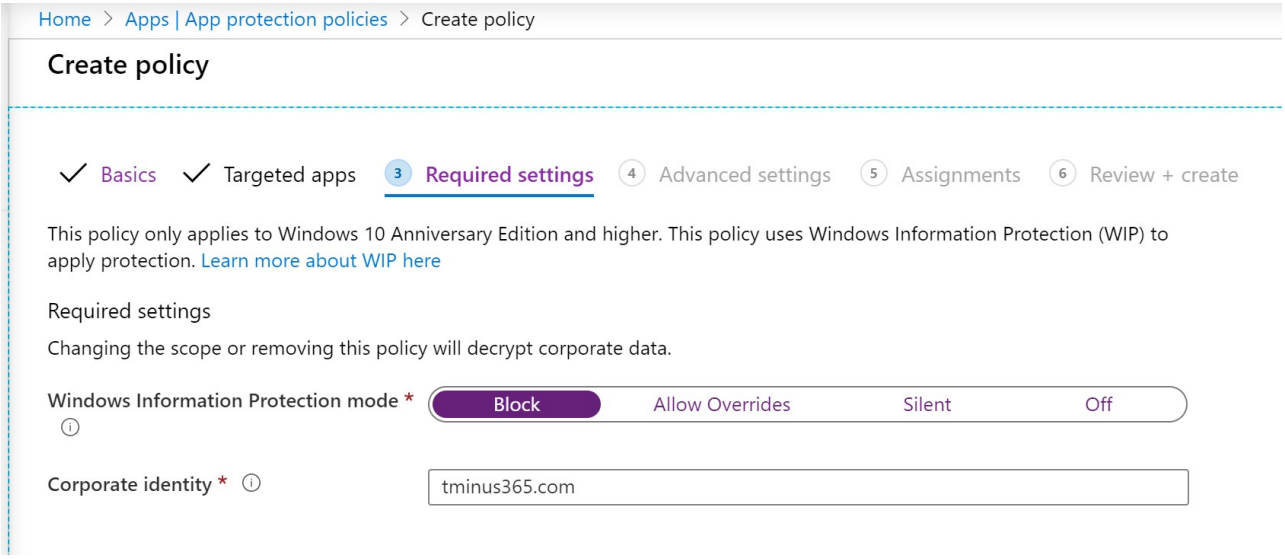


6. When you are ready, click Next

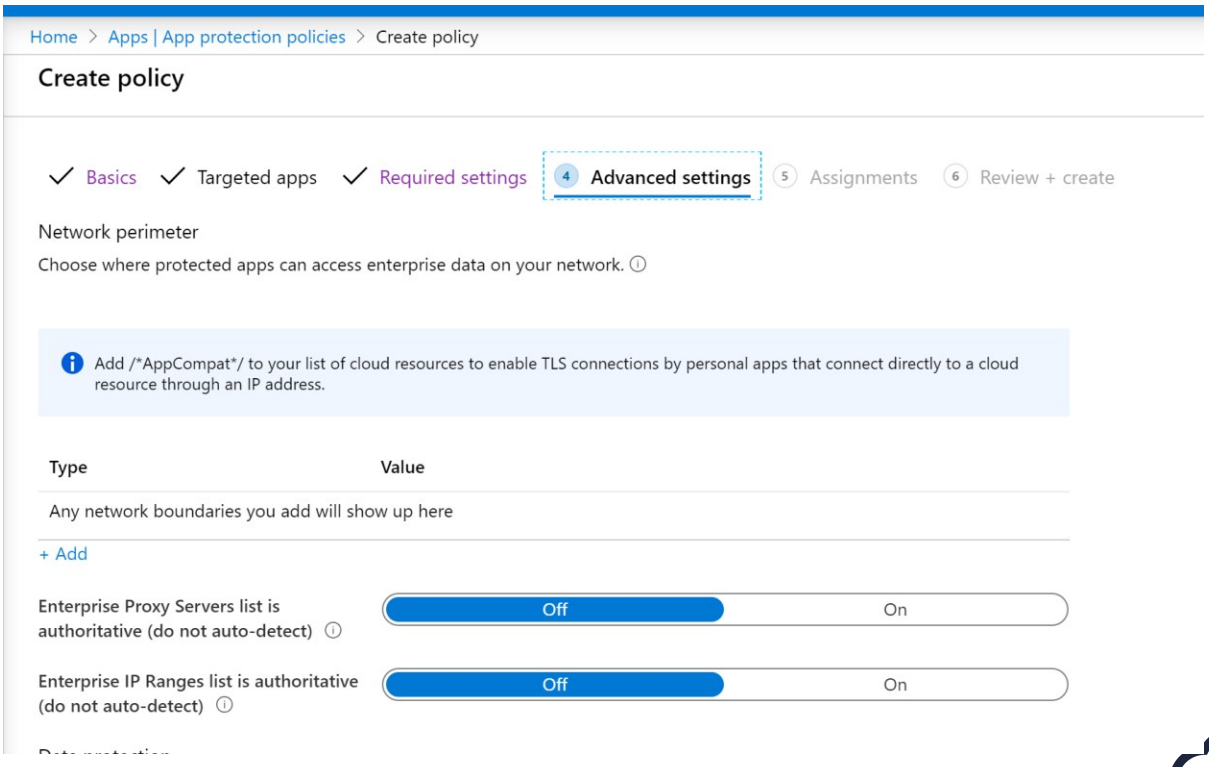


OVERVIEW & USER

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:

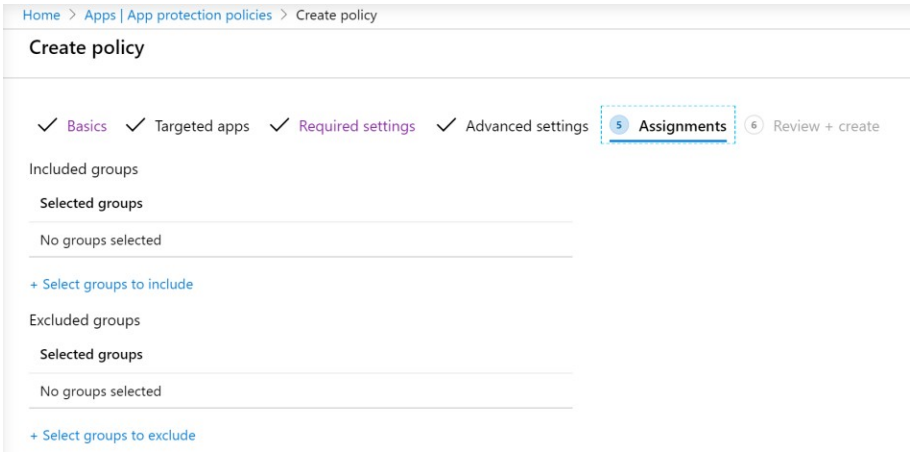


8. We will not configure anything on the advanced settings page:



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,
    - oA.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1,
    - oA.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5,
    - o A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4,
    - o 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. §§
    - o 164.308(a)(1)(ii)(D), 164.308(a)(3),
    - o 164.308(a)(4)
    - o 164.312(a), 164.312(e)

OVERVIEW & USER

SET UP DATA LOSS PREVENTION POLCIES

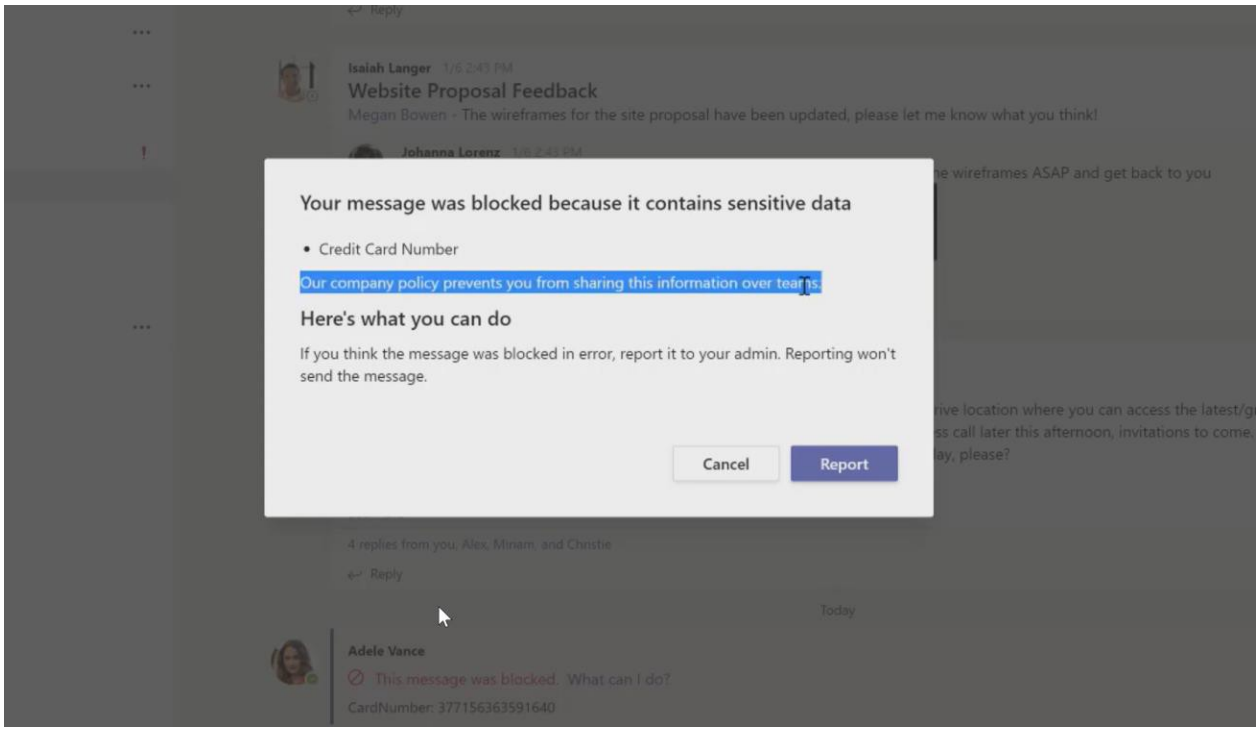
Description: Data loss prevention policies allow us to prevent the sharing of sensitive information across Teams chats. Policies come with pre-defined templates that can detect for certain information being shared like PII, credit card numbers, social security numbers, etc. The policies are granular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

License Requirements:

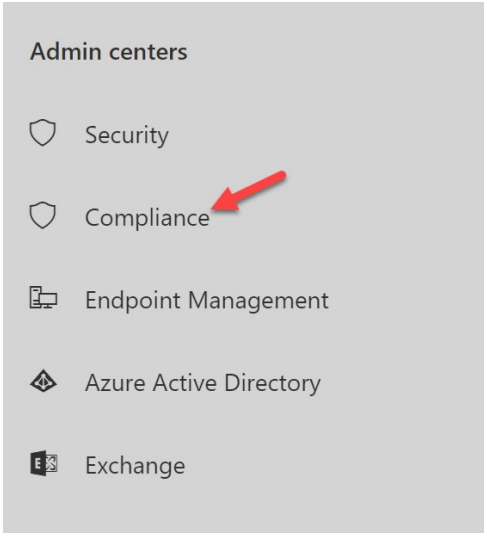
- Microsoft 365 Business Standard $20/u/m
- Microsoft Office 365 E3 $20/u/m

Ex. User sending Credit Card Information

OVERVIEW & USER

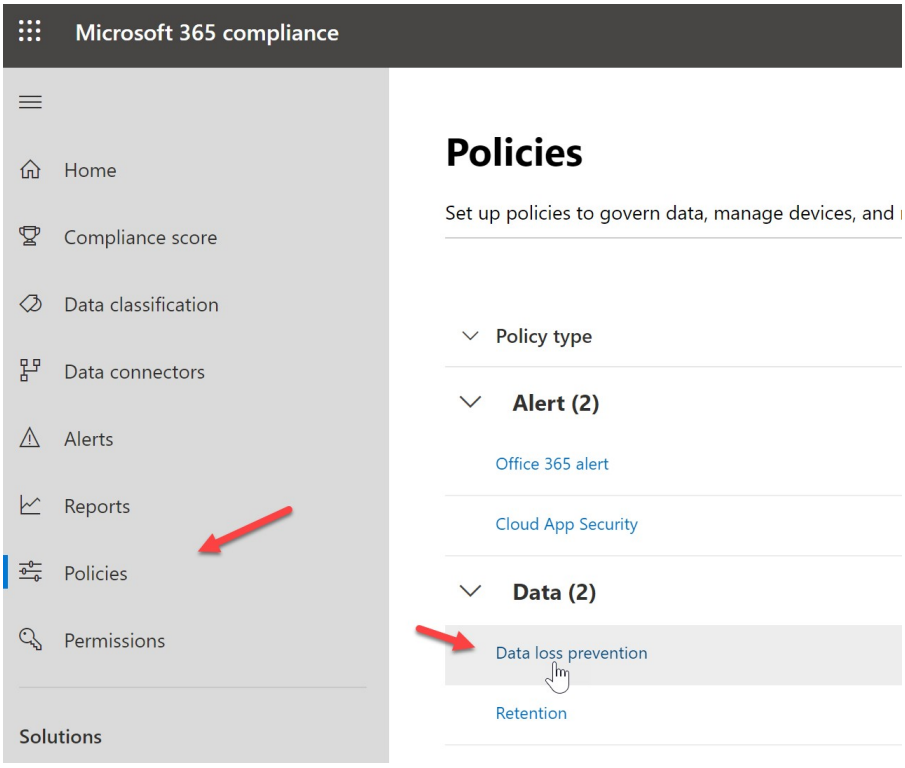


1. In the 365 Admin Center, click on Admin Centers>Compliance

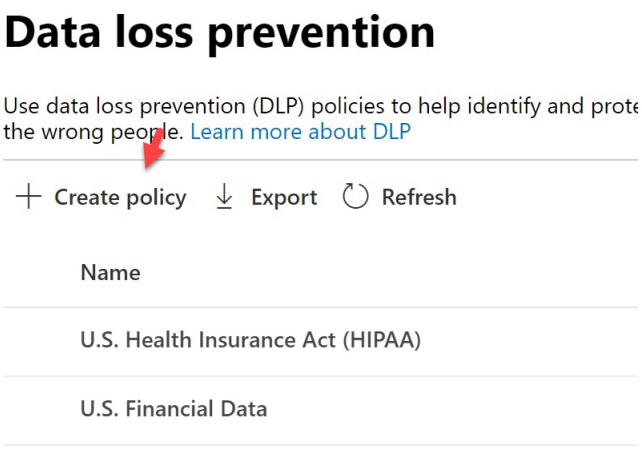


OVERVIEW & USER

2. Click Policies>Data LossPrevention

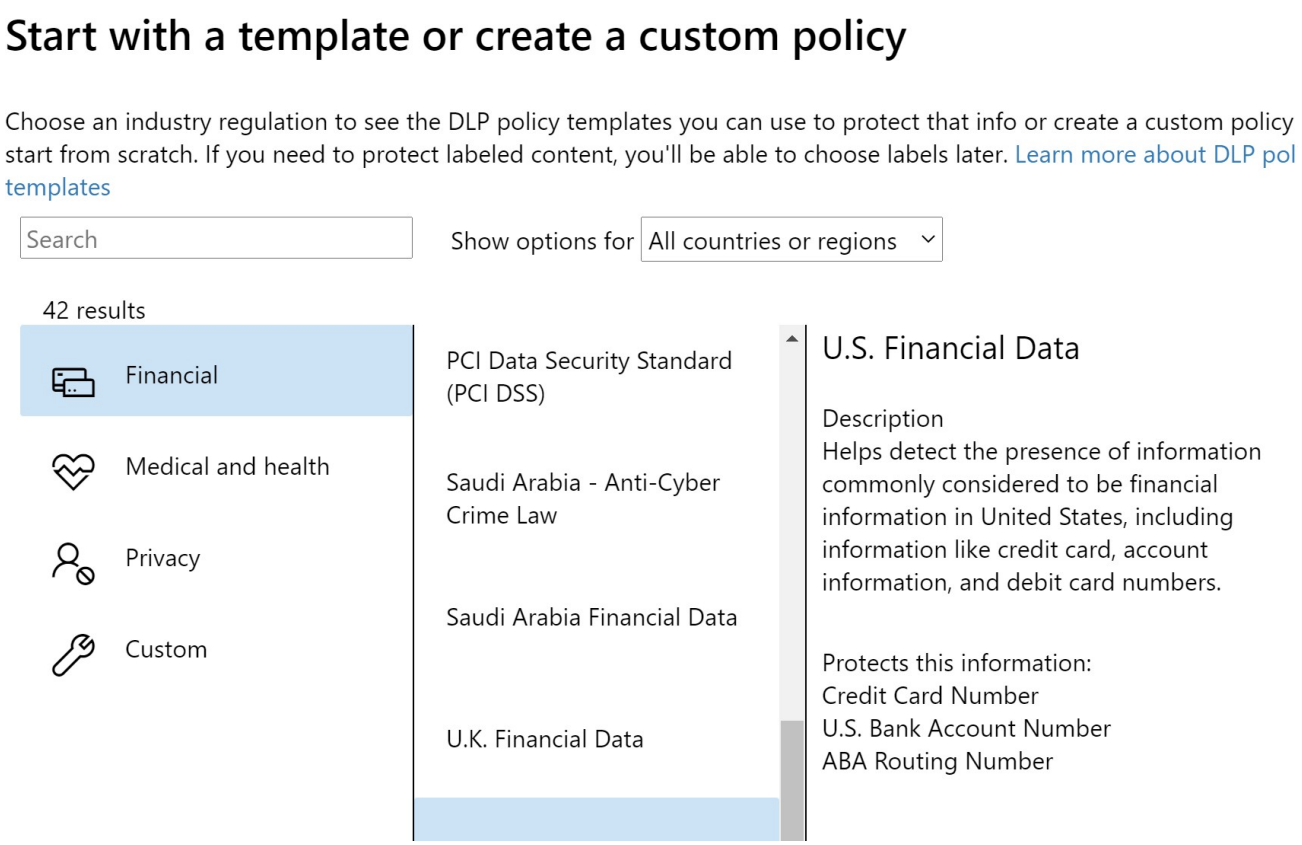


3. Click Create Policy

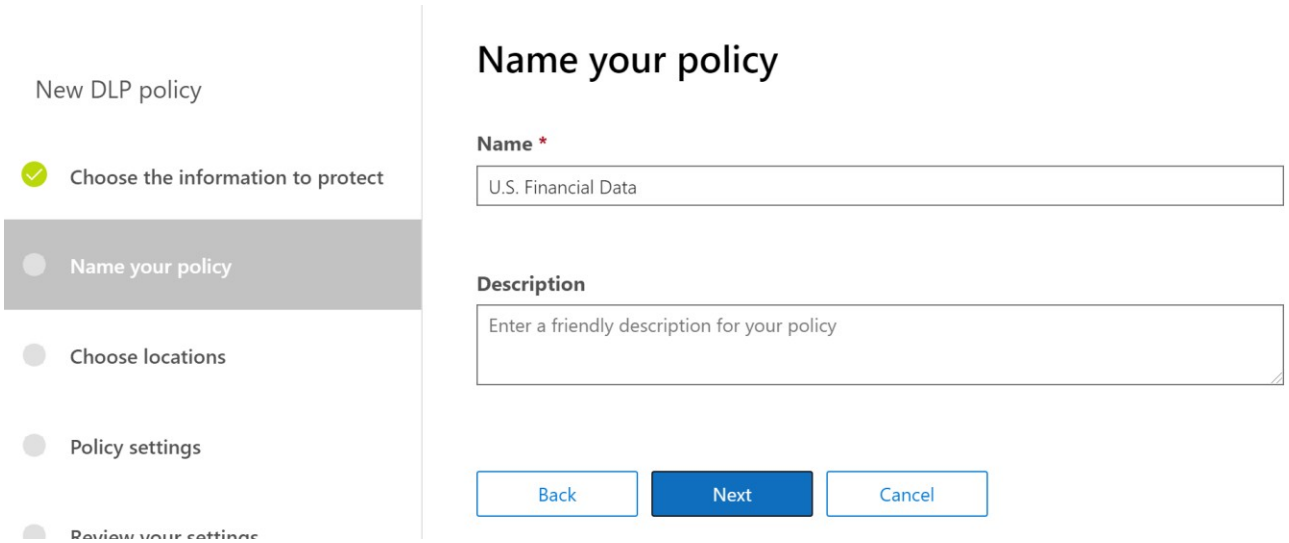


OVERVIEW & USER

4. Choose a template if applicable:

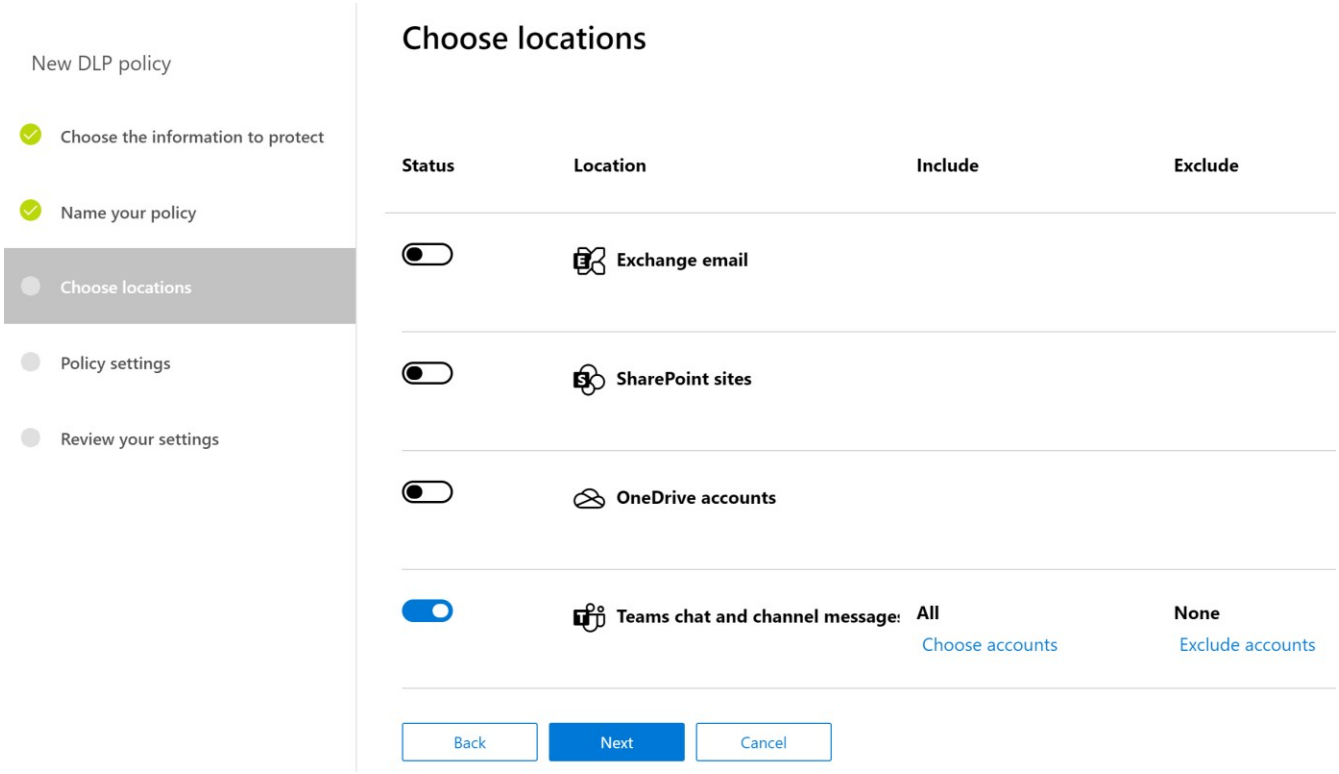


5. Add a name and description

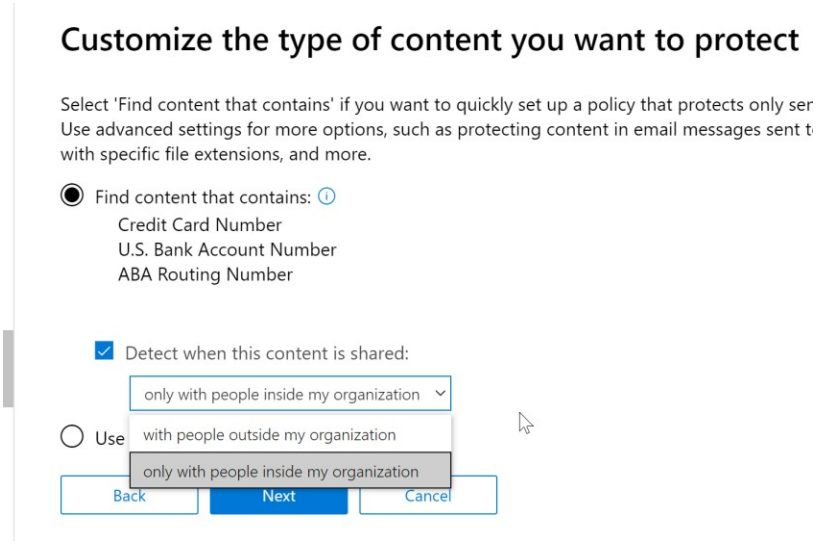


OVERVIEW & USER

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

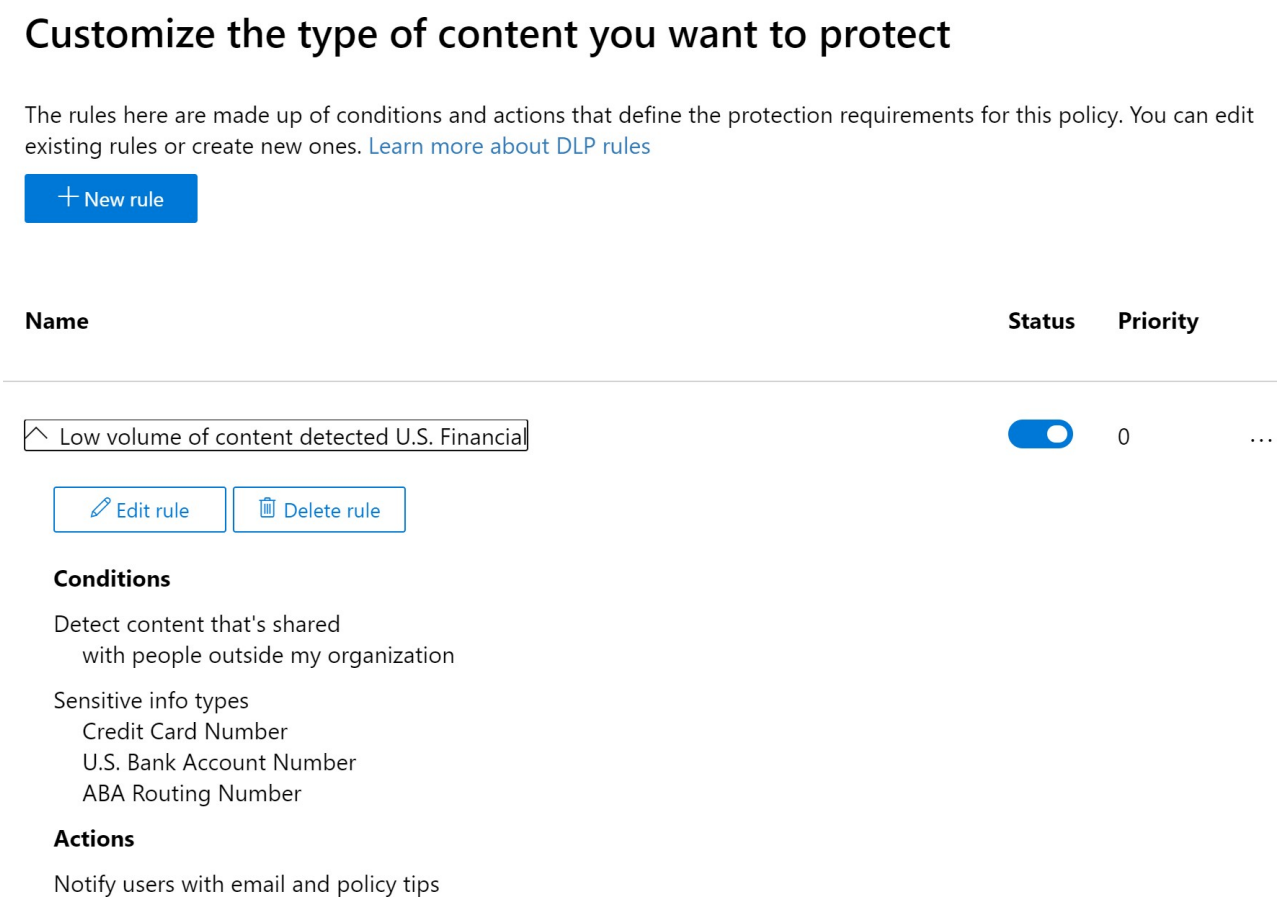


7. You can choose an external or internal policy here



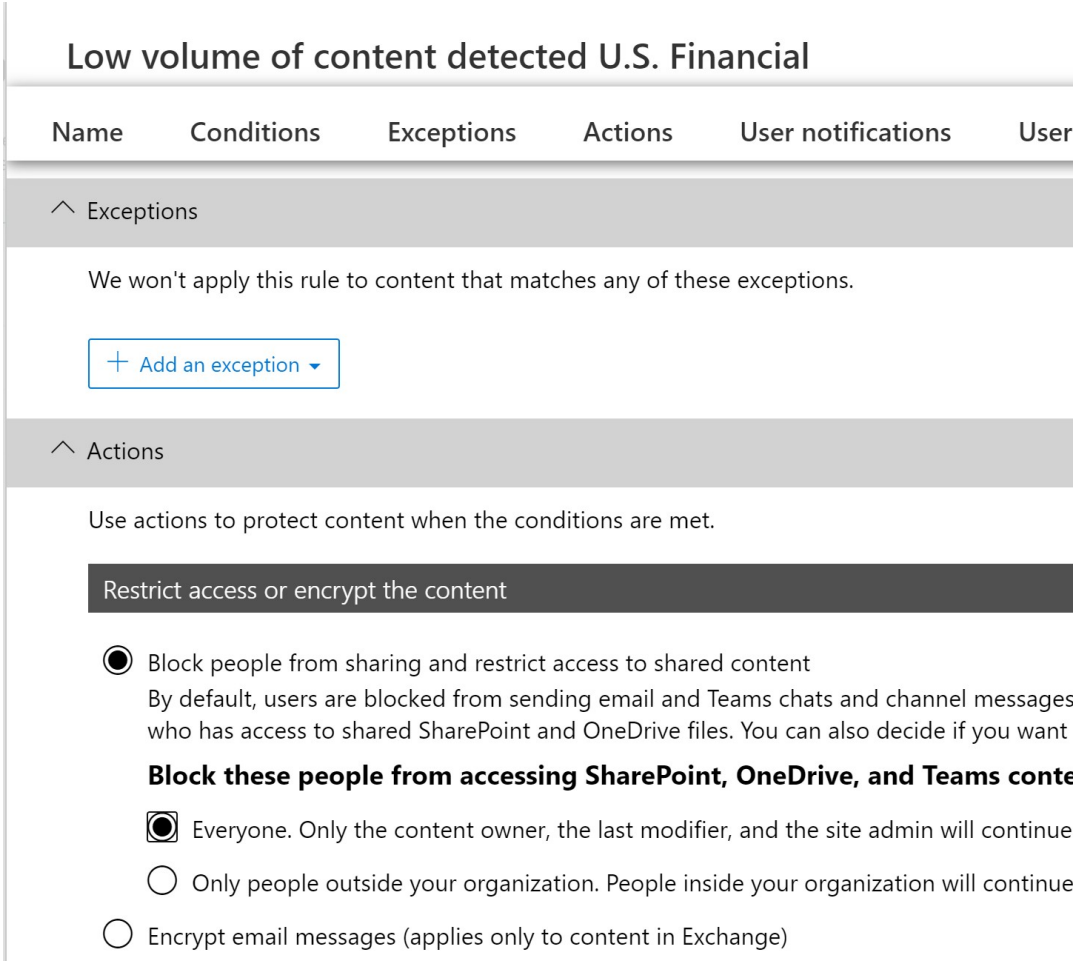
OVERVIEW & USER

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

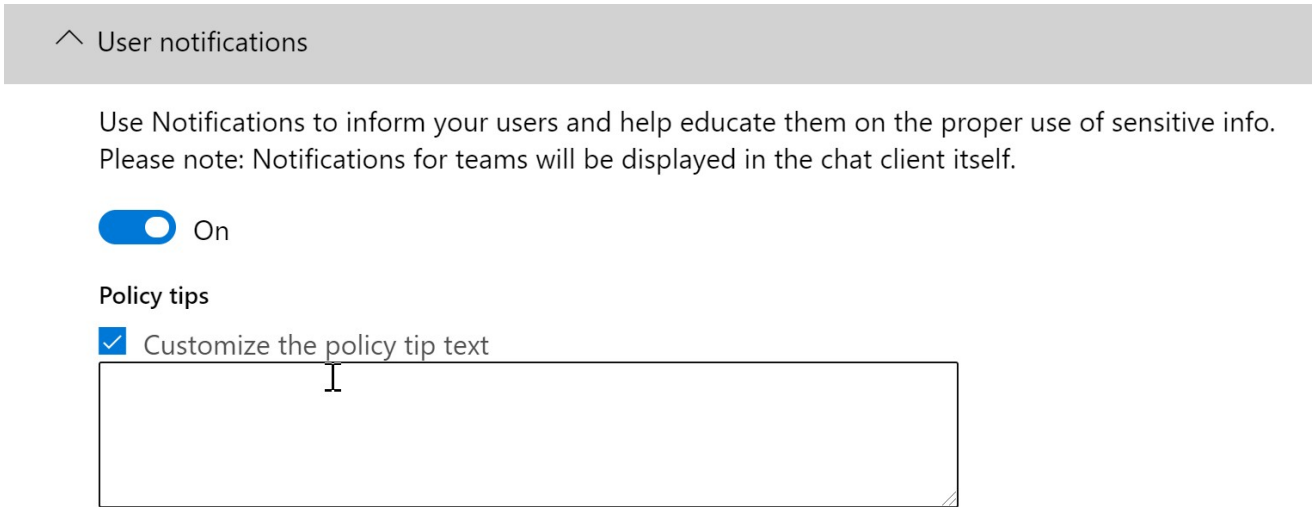


OVERVIEW & USER

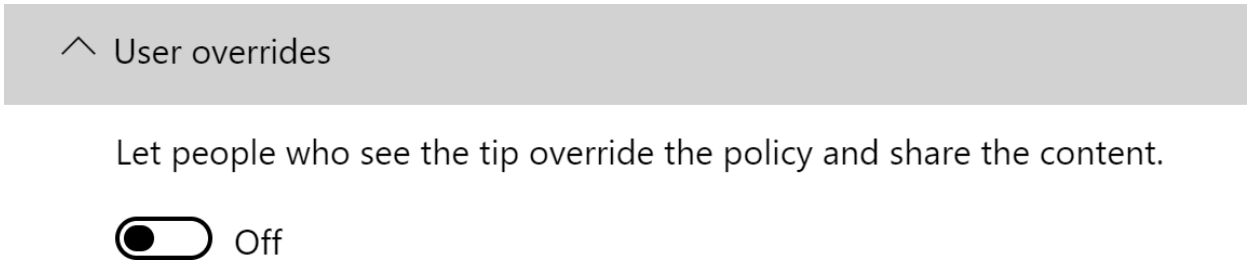
9. If you edit one of the rules you can set the actions that apply to the user such as blocking the message, allowing override, setting the policy tip, etc.:



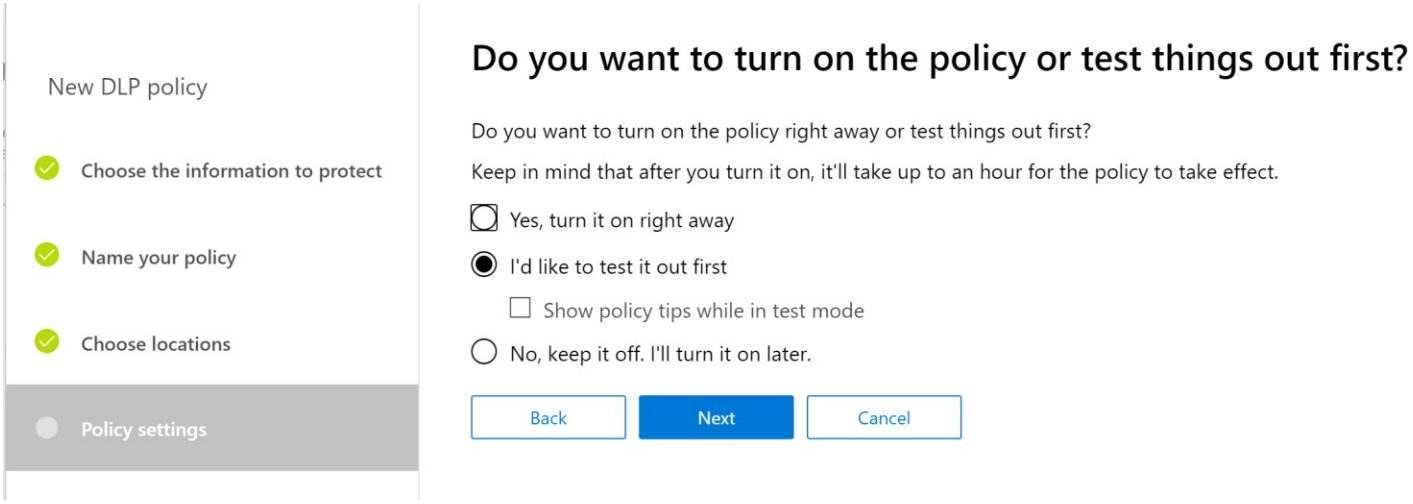
OVERVIEW & USER



OVERVIEW & USER



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.



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,
    - oA.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1,
    - oA.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5,
    - o A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4,
    - o 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. §§
    - o 164.308(a)(1)(ii)(D), 164.308(a)(3),
    - o 164.308(a)(4)
    - o 164.312(a), 164.312(e)

OVERVIEW & USER

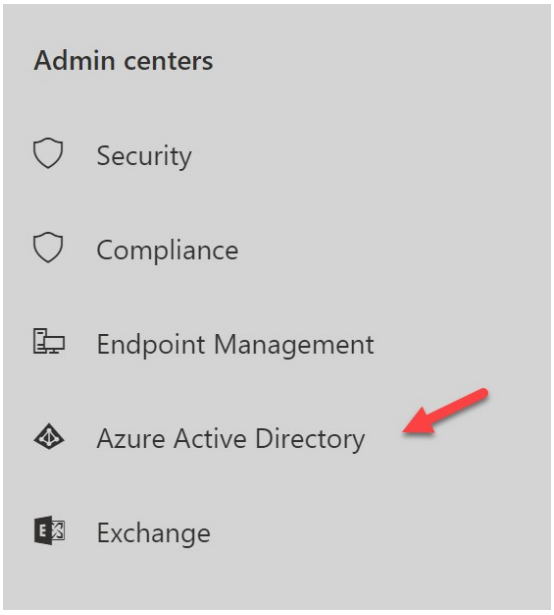
REQUIRE MFA WITH CONDITIONAL ACCESS

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:

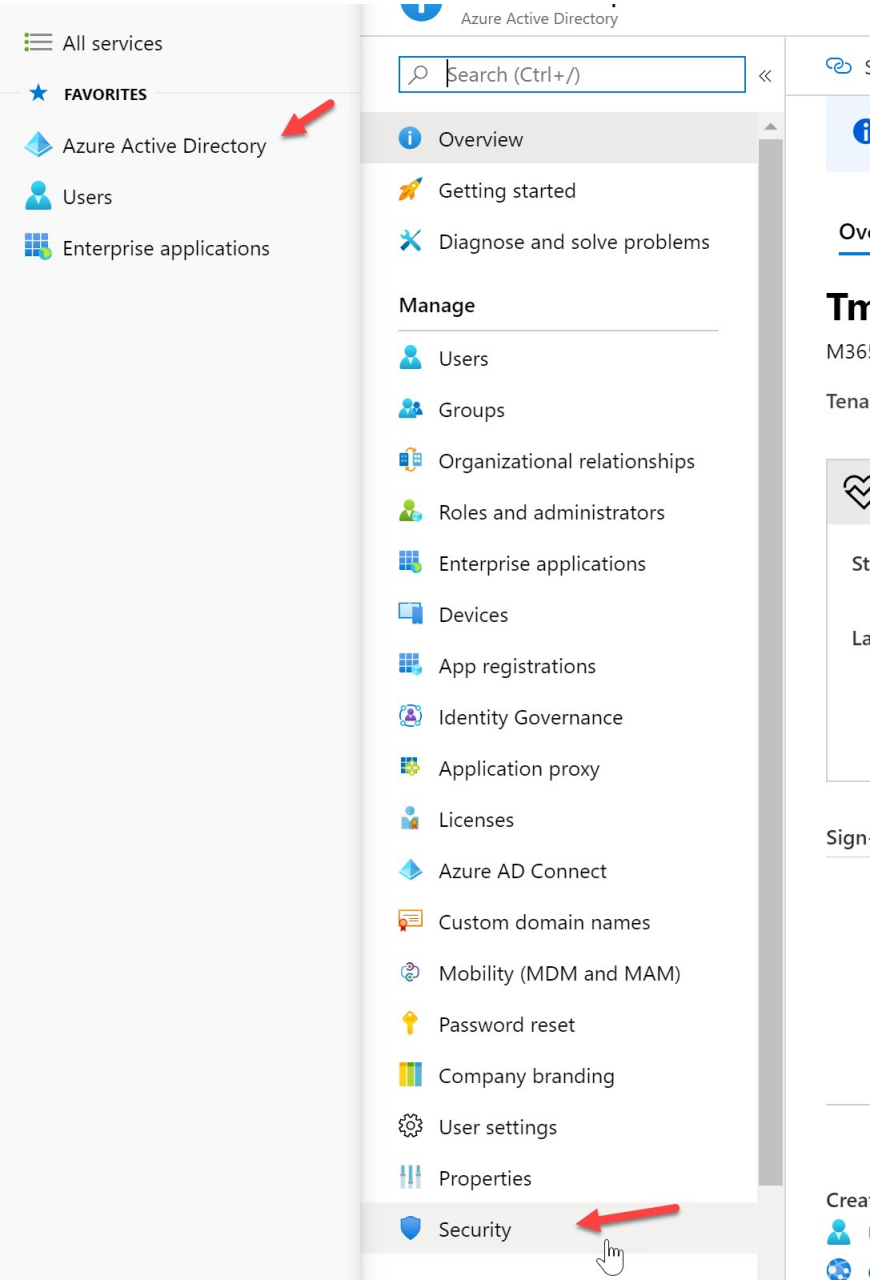
- Microsoft 365 Business Standard $20/u/m
- Microsoft Enterprise Mobility + Security E3 $8.75/u/m
- Azure Active Directory Premium Plan 1 $6/u/m

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



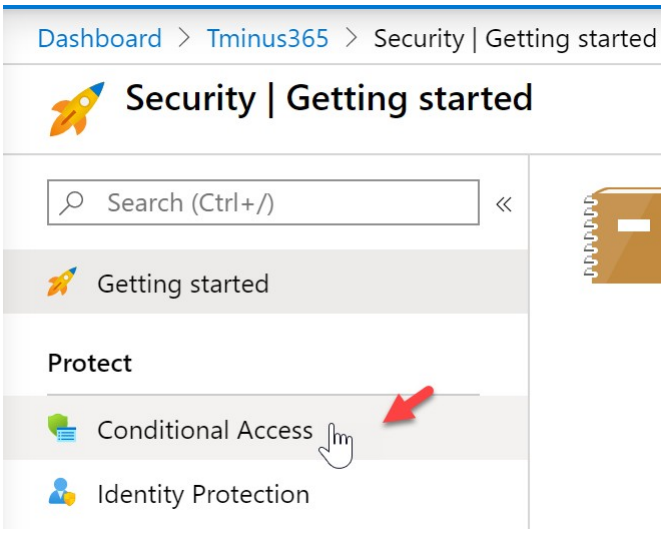
OVERVIEW & USER

2. Click Azure ActiveDirectory>Security

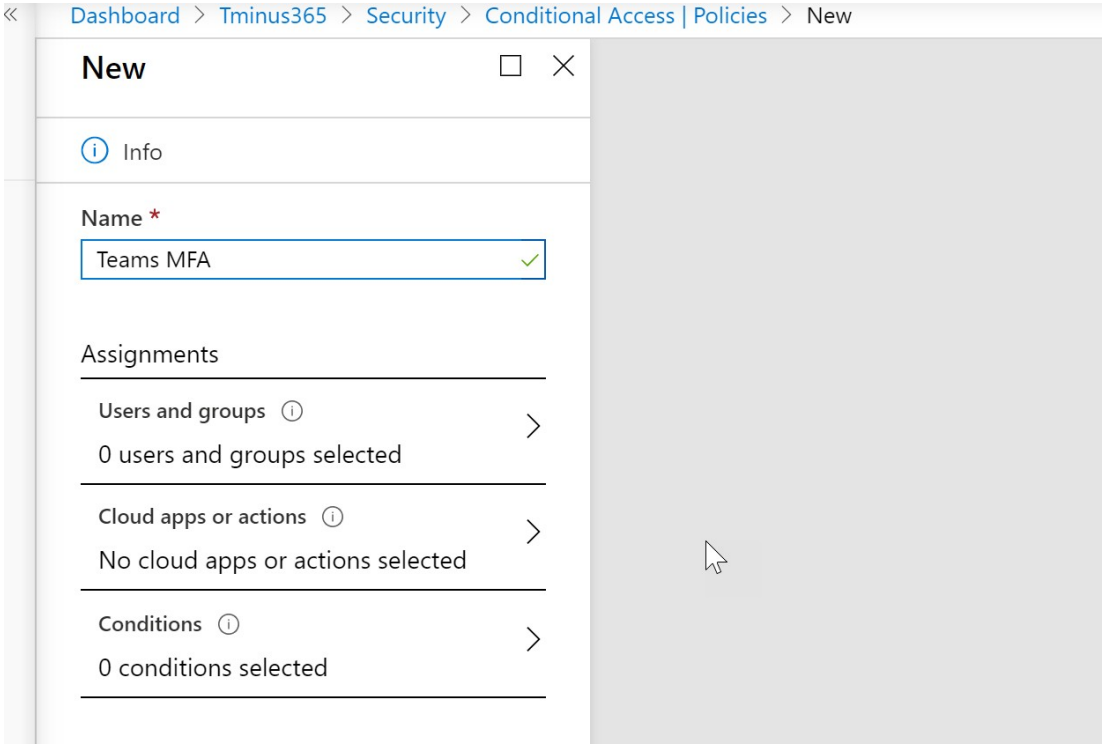


OVERVIEW & USER

3. Click Conditional Access

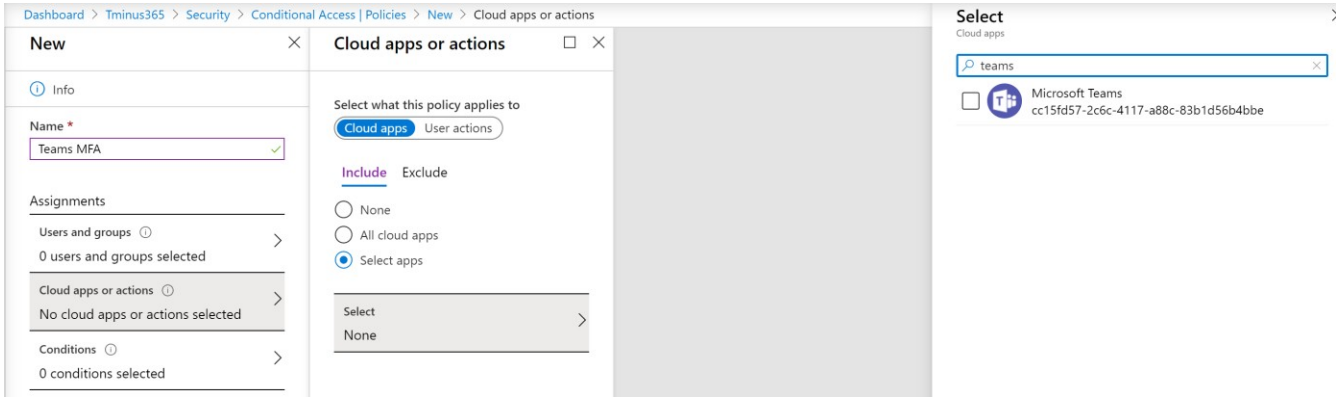


4. Click +New Policy. Name the Policy and click on users and groups to scope the policy:

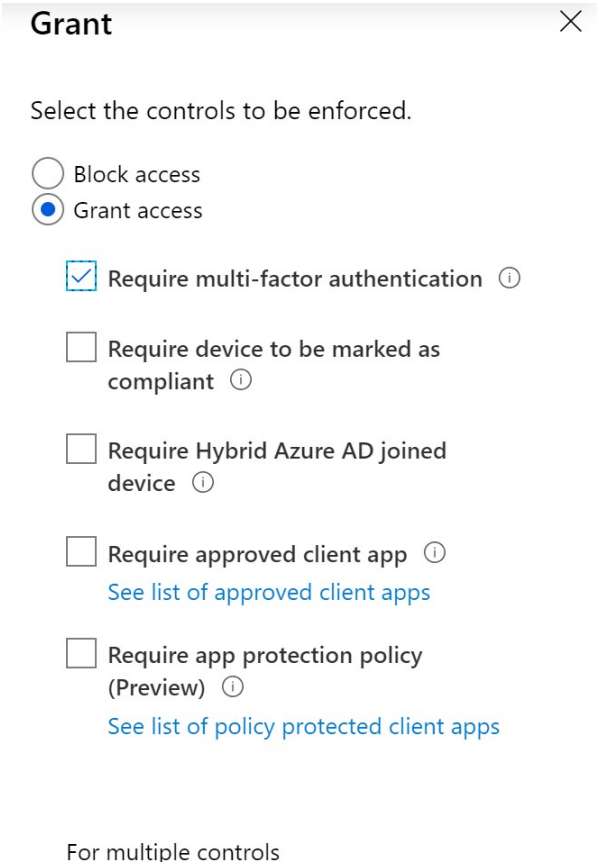


OVERVIEW & USER

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