Microsoft

Microsoft Teams Virtual Event

Teams 101!

Introductions

Karl Kocar
Technical Architect

@karlkocar
kakocar@microsoft.com
https://myteams.blog

Jack Lewis
Technical Architect

aka.ms/jacklewis
Jack.Lewis@microsoft.com

Upcoming 101 Events

Voice and Meetings When: Thursday, March 17, 2022

https://msevents.microsoft.com/event?id=3256377873

Platform Customisation Tuesday, March 22, 2022

https://msevents.microsoft.com/event?id=1272363986

Viva Thursday, March 24, 2022

https://msevents.microsoft.com/event?id=3719085570

Housekeeping

Please do not share the meeting invite URL with anybody

This is an action-packed agenda, so please stay on mute

Please ask questions in the Q&A or chat and be patient when waiting for a response

Please provide event feedback

Agenda (1000-1300)

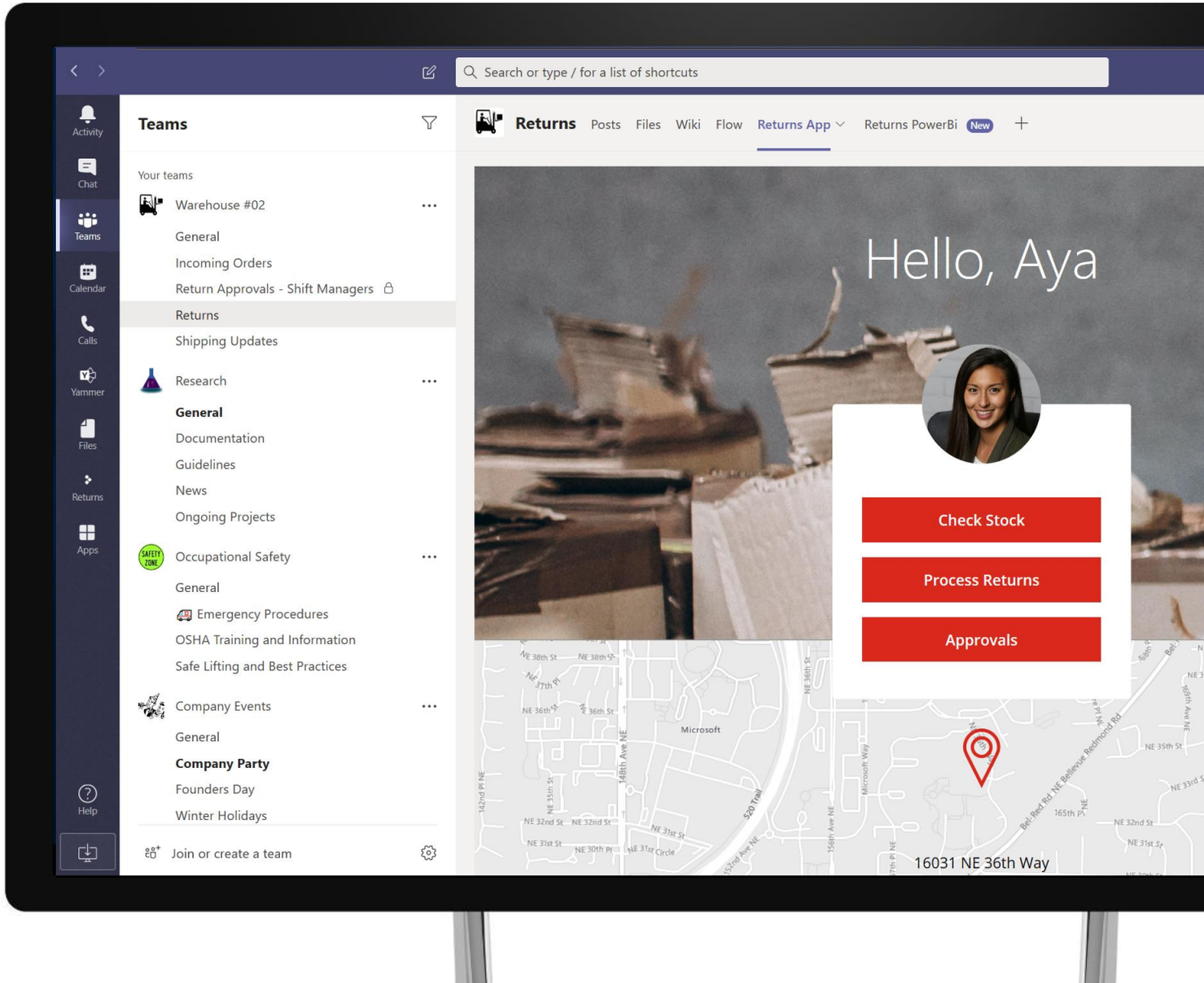
- **1000 - 1030 Teams Intro / Why / New Collab or Security Features / ACM (Jack)**
- **1030 – 1115 Teams Lifecycle (Karl)**
  - Naming
  - Classification - Classic
  - Team Creation
  - Guest Access
  - Archiving
  - Expiration
- **1115 – 1130 Break**
- **1130 – 1200 Information Protection and Governance (Karl)**
  - Classification – Modern
  - Sensitivity Labels
  - Retention Policies
  - Content Search / eDiscovery
- **1200 – 1215 Threat Management (Karl)**
  - ATP Safe Links for Teams
  - Sentinel
  - Secure Score
  - Audit Logs
- **1215 – 1245 Managing Teams 101 - Messaging, Meeting, Voice and Application Policies (Jack)**
  - Information Barriers
  - Private Channels
  - Messaging Polices
  - Meeting Polices
  - Application Policies
- **1245 Any Remaining Q&A**
- **1300 Close**

Teams 101
Introduction

Microsoft Teams

is the hub for teamwork in Microsoft 365

- Chats
- Meetings
- Calls
- Files
- Apps and workflows



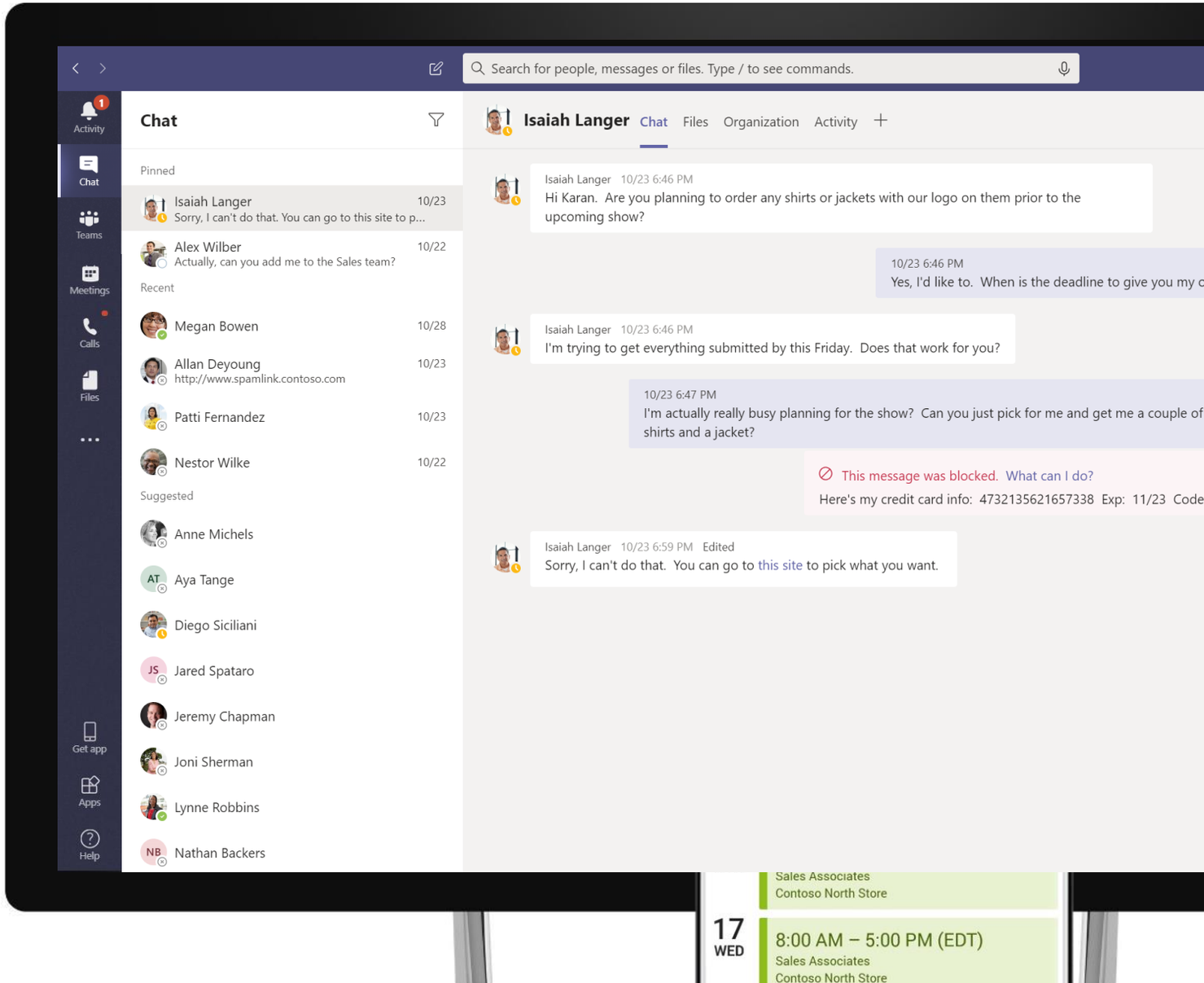
What can Teams do for your business

Transform workplace collaboration

Streamline business processes

Connect everyone on a single platform

Provide enterprise grade security & compliance



The Partner Opportunity with Microsoft Teams

270M+

More than 270M monthly active Teams users

500,000+

More than 500,000 organizations use Teams

x7

Daily active users of apps on Teams has grown seven times since the start of the pandemic

x2

The number of apps created on our Teams platform has doubled in one year

181

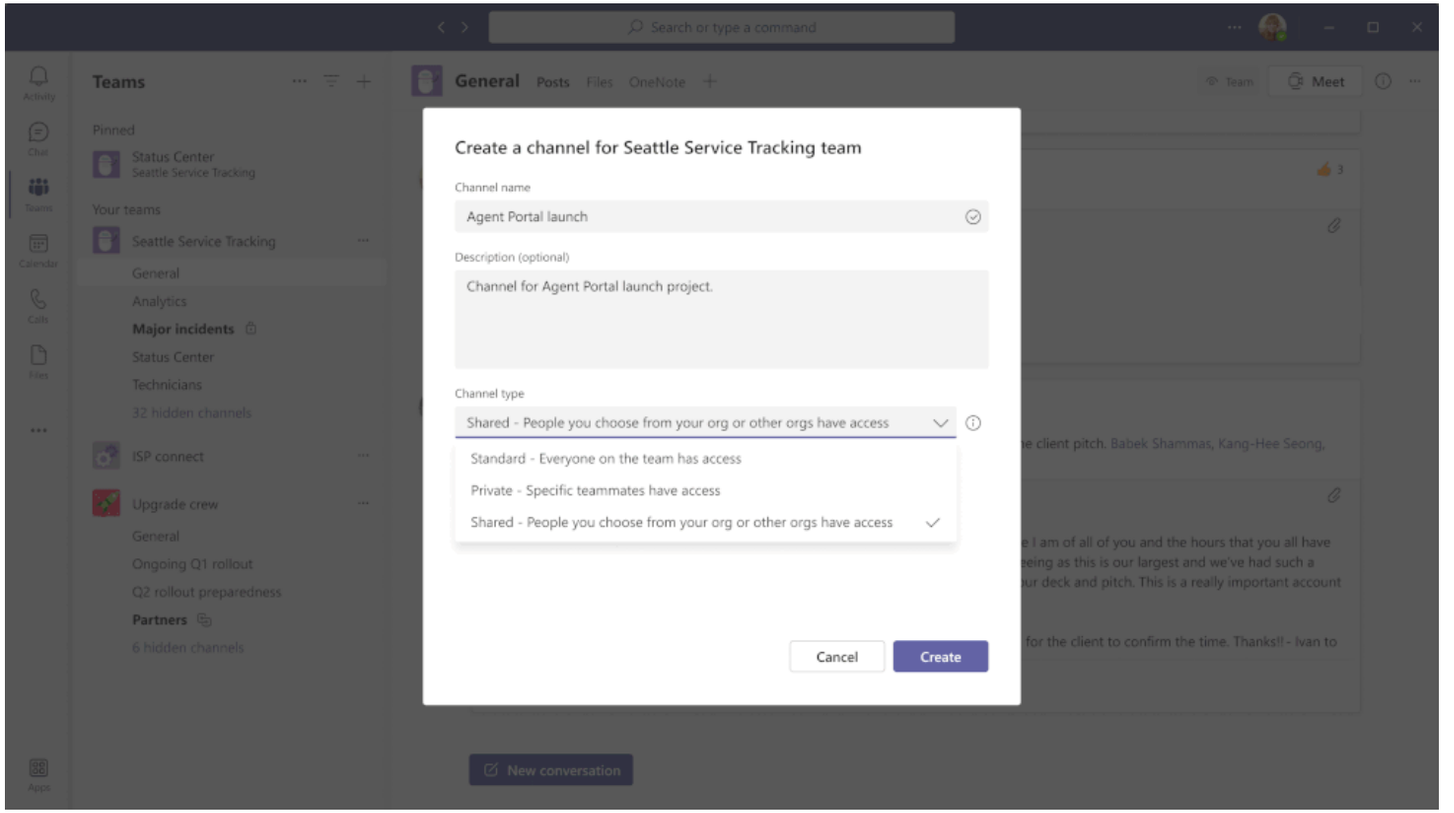
Teams in 181 markets with support for 53 languages and growing

[Build apps for Microsoft 365]

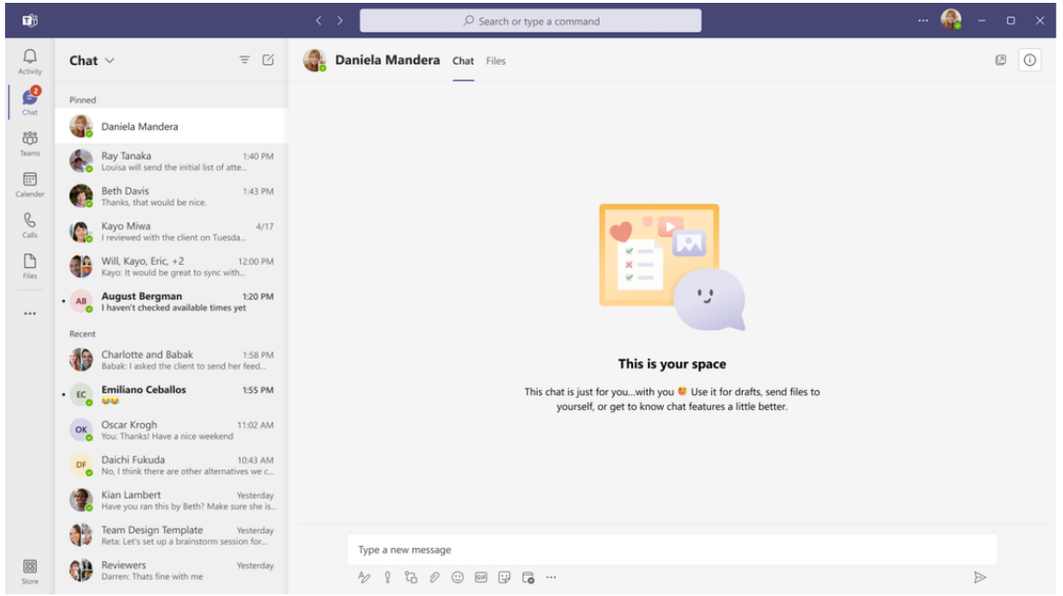
What’s new at Ignite 2021?

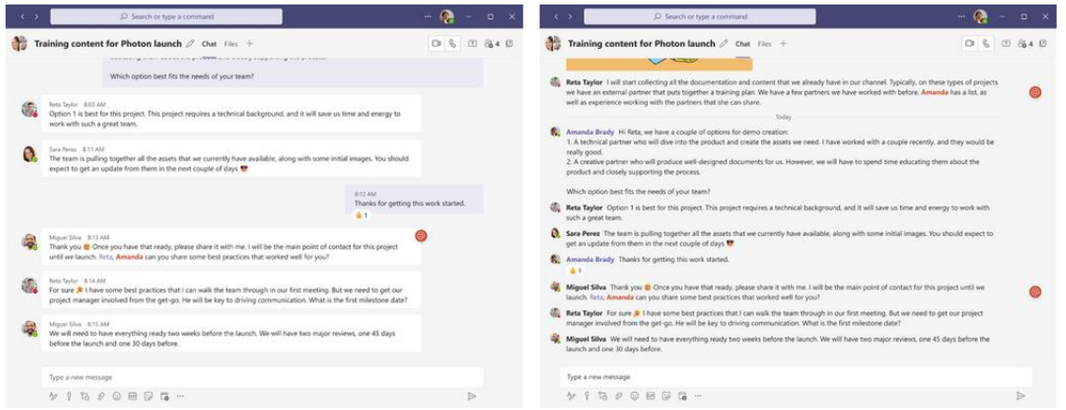
Available now or coming soon

Teams Connect

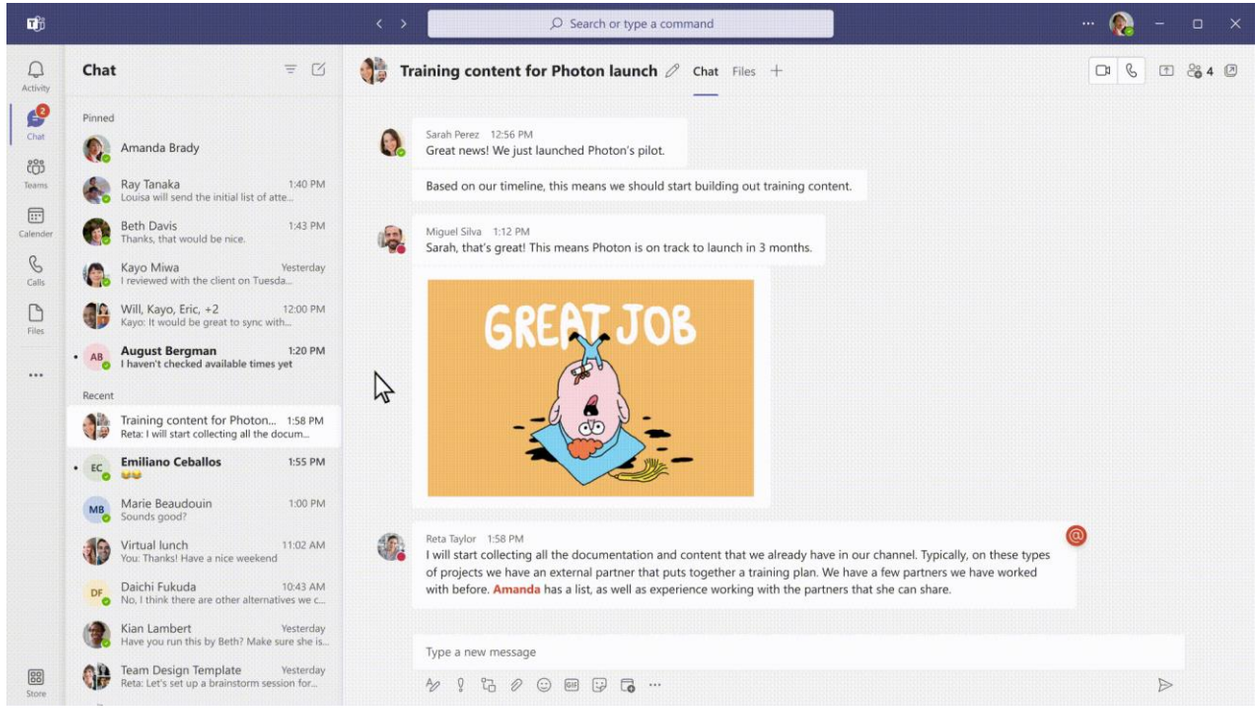


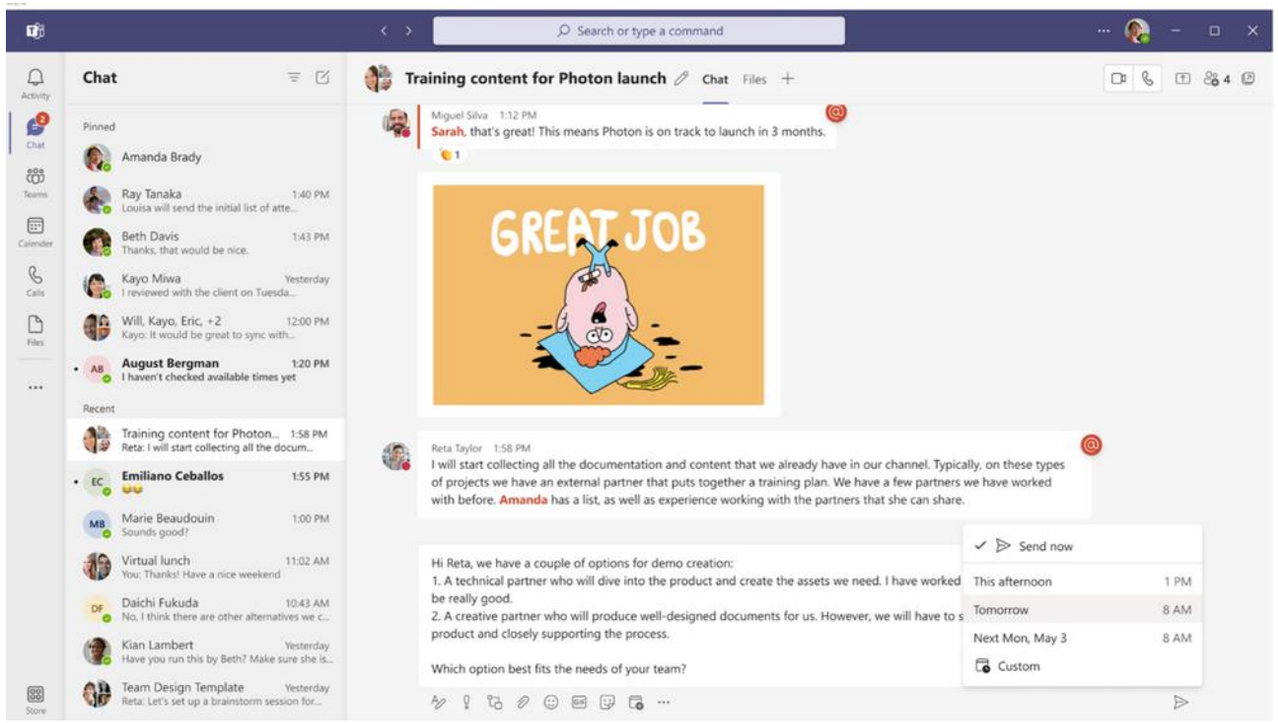
New Chat, People and Presence features



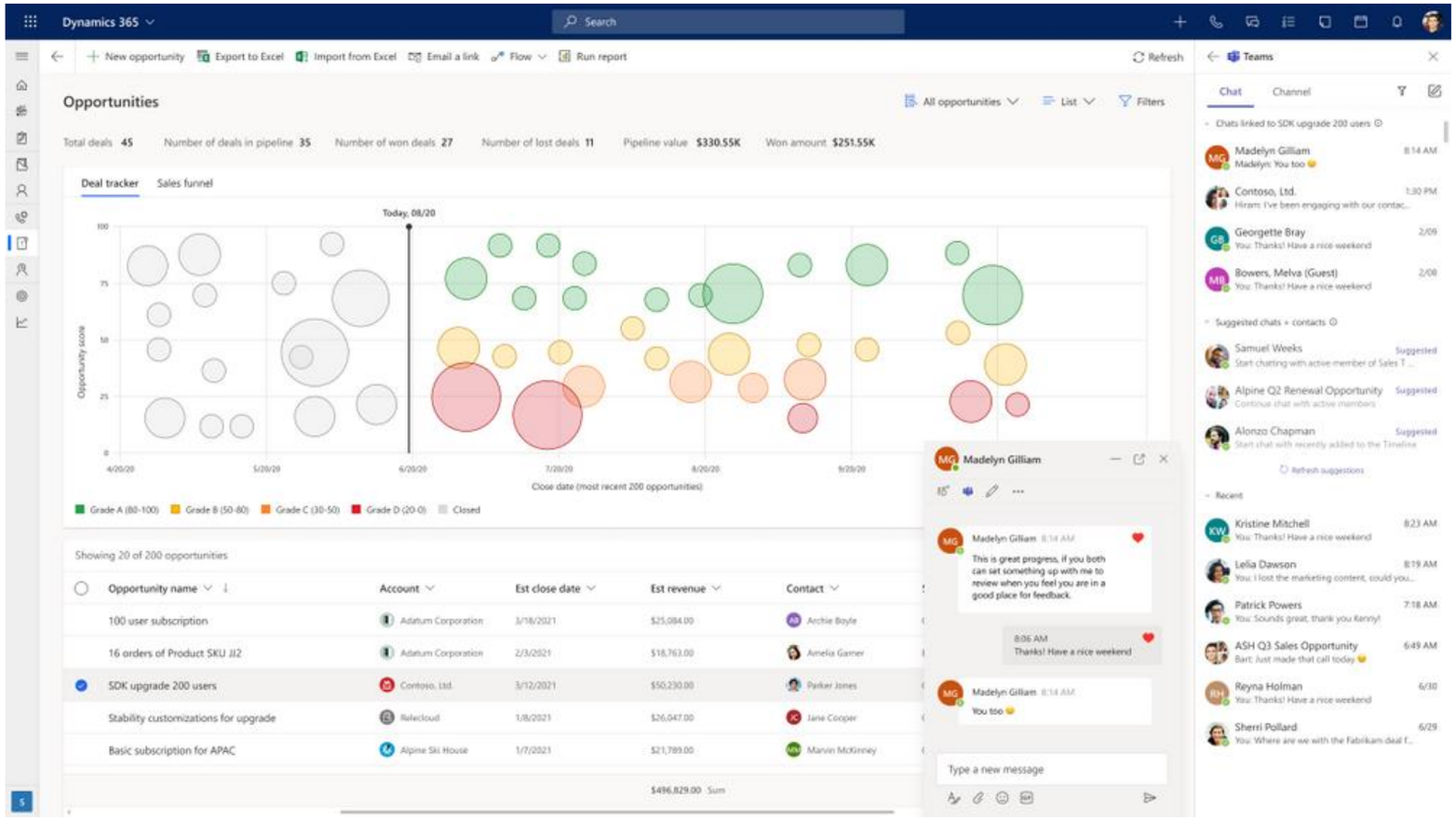


New Chat, People and Presence Features

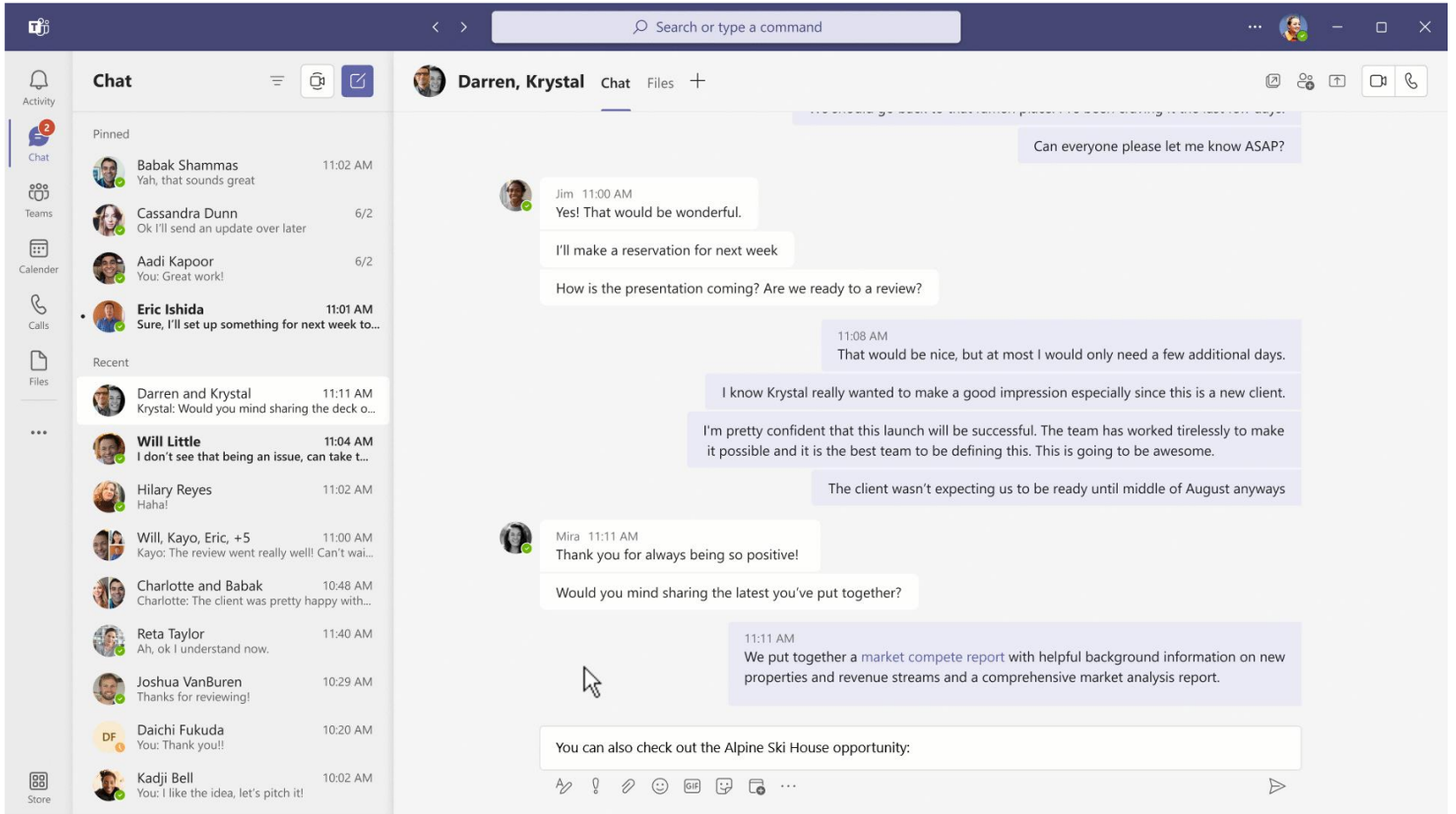




Dynamics/Teams Process Improvements



Dynamics/Teams Integrations



Security, compliance, and privacy

Retention and Deletion policies for Private Channels
Target retention and deletion policies to specific Teams or Teams end users
Teams Multi-Geo
Invite only meeting options & disable attendee video during meetings
Microsoft Graph Export API
Co-author in encrypted docs using Office Apps
Policy enhancements in Teams Admin Center

Behavioral insights enable transformations

50%

of transformations fail because behaviors don’t change

McKinsey, “The Five Frames – A Guide to Transformational Change,” 2013

Prosci® by the Numbers

20

Years of Research

10

Longitudinal Studies

6,000+

Research Participants

80%

Fortune 100 Companies

45,000+

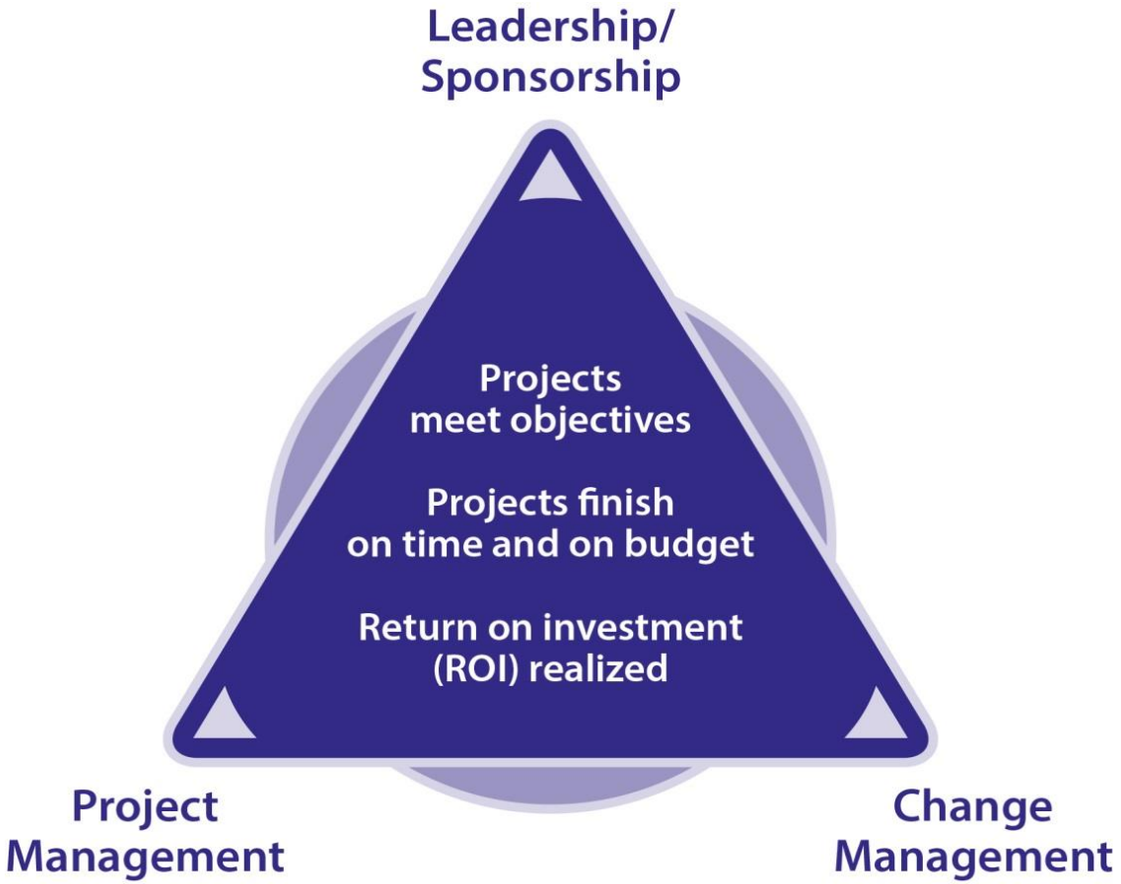
Certified Practitioners

100,000+

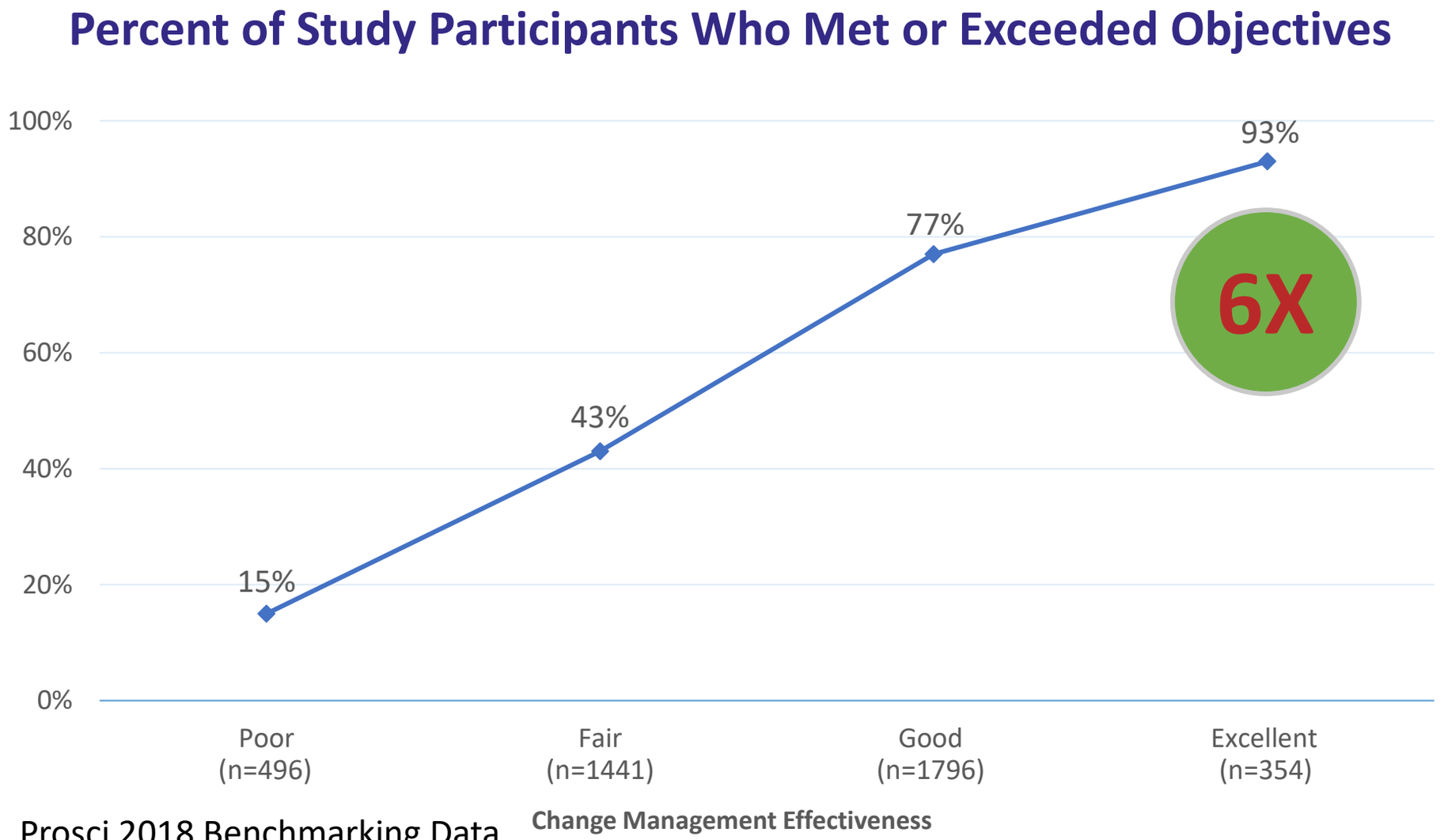
Community Members

Application

Applied to Your Project
Prosci® PCT™ Model



Data Supports the Connection



Prosci 2018 Benchmarking Data
Data from 2007, 2009, 2011, 2013, 2015, 2017

Research Finding

The number one obstacle
to success for major change projects
is ineffective sponsorship.

* Data from 1778 participants, 2018 Change Management Best Practices study.

Teams Security Lifecycle

Upcoming 101 Events

Voice and Meetings When: Thursday, March 17, 2022

https://msevents.microsoft.com/event?id=3256377873

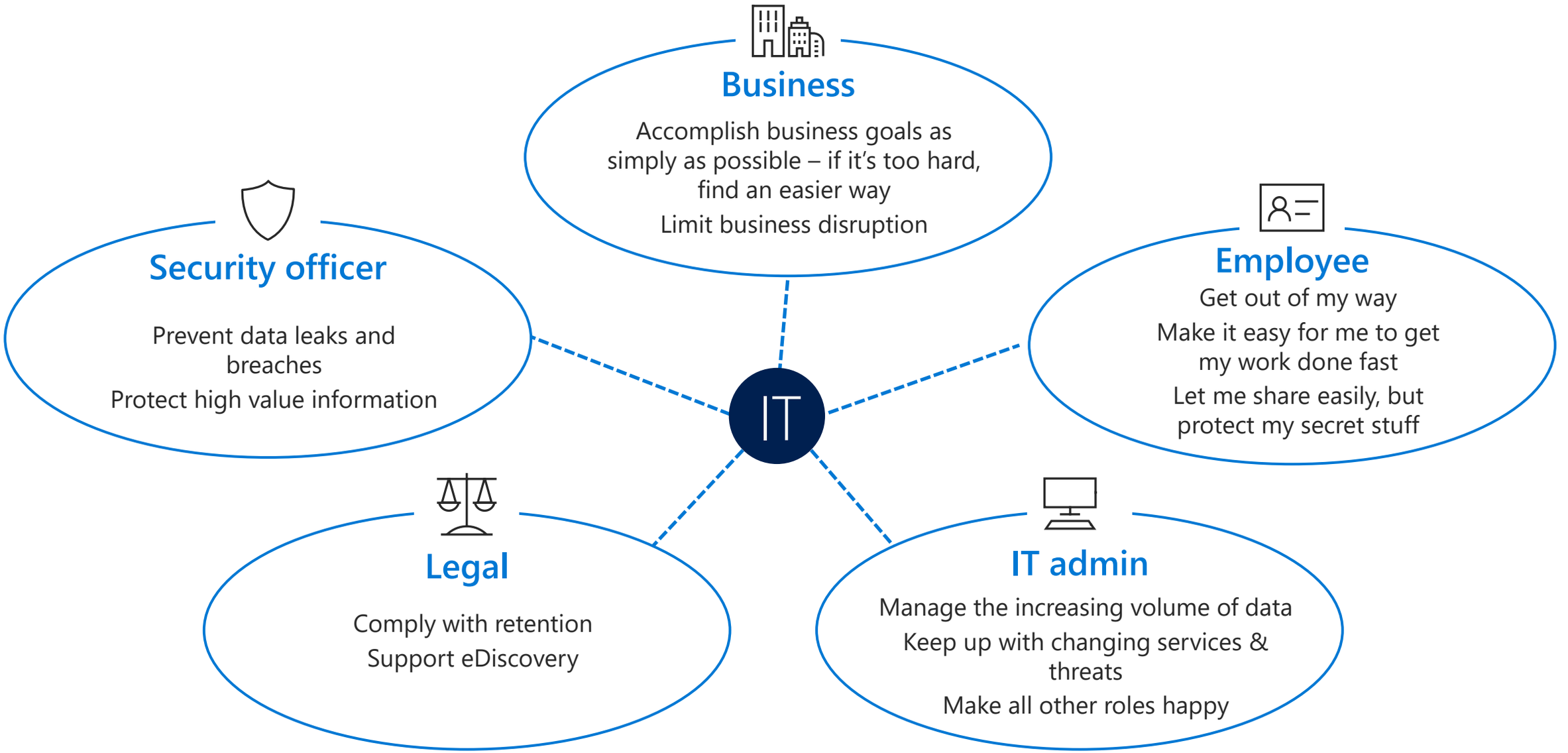
Platform Customisation Tuesday, March 22, 2022

https://msevents.microsoft.com/event?id=1272363986

Viva Thursday, March 24, 2022

https://msevents.microsoft.com/event?id=3719085570

Roles and their needs



Sample Controls for Teams

Teams Security benefits from controls provided across the Cloud

Azure Administration

Azure AD
Group/Teams Creation
Naming
Expiration
Azure B2B Guest Controls
Terms of Use
Access Reviews
Information Barriers
Conditional Access
Teams RBAC

Endpoint Manager
DLP for Teams

Microsoft Sentinel

Microsoft Defender for Cloud Apps (formerly MCAS)
Session Policies
File Policies

Microsoft 365 Administration

Teams Admin Portal
Org-wide Settings
Teams Private Channel Policy
Message Policies
Meetings Policies
App Policies
Voice Policies
Policy Packages

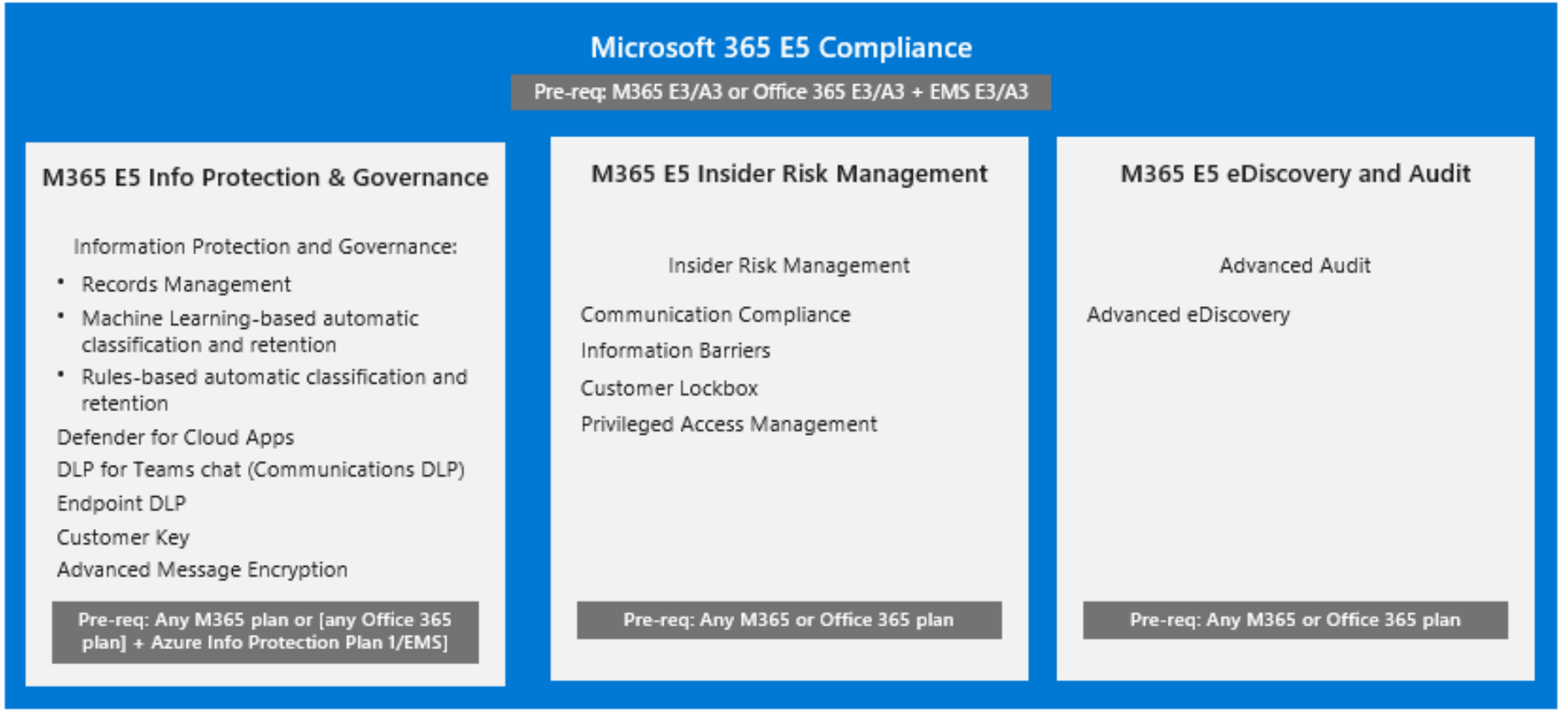
Client Admin
Team Owner Settings
Channel Moderation
User Settings (e.g. Privacy)

Microsoft 365 S&C Centres
Retention Policies
DLP Policies for Teams
Sensitivity Labels for Content
Sensitivity Labels for Groups
ATP Safe Attachments
ATP Safe Links (Preview)
Auditing
eDiscovery
Legal Hold
Compliance Content Search
Communications Compliance
Classification - Legacy

https://docs.microsoft.com/en-us/MicrosoftTeams/plan-teams-governance

Licensing Considerations

Be sure to validate the licensing requirements against the proposed security posture



AAD P1 and AAD P2 are important – Groups, Conditional Access, Access Reviews etc!

Overall guidance

Every organization has different GRC (governance, risk and compliance) requirements

Do your own risk assessment and weigh identified risks vs. the available controls

Understand the possible downsides of aggressive postures relative to potential maintenance burdens and end-user impacts

Testing your final control scheme (the different combinations of settings) is imperative, for two main reasons:

1. Combined effects of different settings across control groups (and control points) may need to be assessed from a GRC efficiency perspective

2. End-user impacts (including possible avoidance behaviors) need to be considered.

Finally, as always, it is important to consider the potential business value of your decisions relative to cost and risk avoidance.

Teams Focus

For Microsoft Teams, you need to govern:

How Teams are requested, approved and created	How information access and containers are managed	How to retain/expire/dispose of information as appropriate
Provisioning	*Operations*	*Information Lifecycle*

What are Microsoft 365 Groups?

Single identity for teamwork and beyond

Membership service for M365 teamwork apps

Teams, Outlook, Yammer, SharePoint, Planner, Stream, Forms, StaffHub, Dynamics CRM, Power BI

Centrally managed and governed

Information protection, governance, and compliance

Extensible

Microsoft Graph, connectors, 3rd party app development

Group.Unified Template

```
PS C:\WINDOWS\system32> (Get-AzureADDirectorySetting -Id 19c61e9e-9455-475b-9ca0-4f75e00930d1).values

Name                           Value
----                           -----
EnableMIPLabels                False
CustomBlockedWordsList         Payroll,CEO,HR,Test
EnableMSStandardBlockedWords   False
ClassificationDescriptions
DefaultClassification          Internal
PrefixSuffixNamingRequirement  [Department] - [GroupName]
AllowGuestsToBeGroupOwner      False
AllowGuestsToAccessGroups      True
GuestUsageGuidelinesUrl
GroupCreationAllowedGroupId    42cb00a5-4967-45a7-b7cc-daac306e05fd
AllowToAddGuests               True
UsageGuidelinesUrl
ClassificationList             Internal,External,Confidential
EnableGroupCreation            False


PS C:\WINDOWS\system32>
```

Classification (Site) Label Doc: https://docs.microsoft.com/en-us/sharepoint/dev/solution-guidance/modern-experience-site-classification

[Create a team from scratch (microsoft.com)]

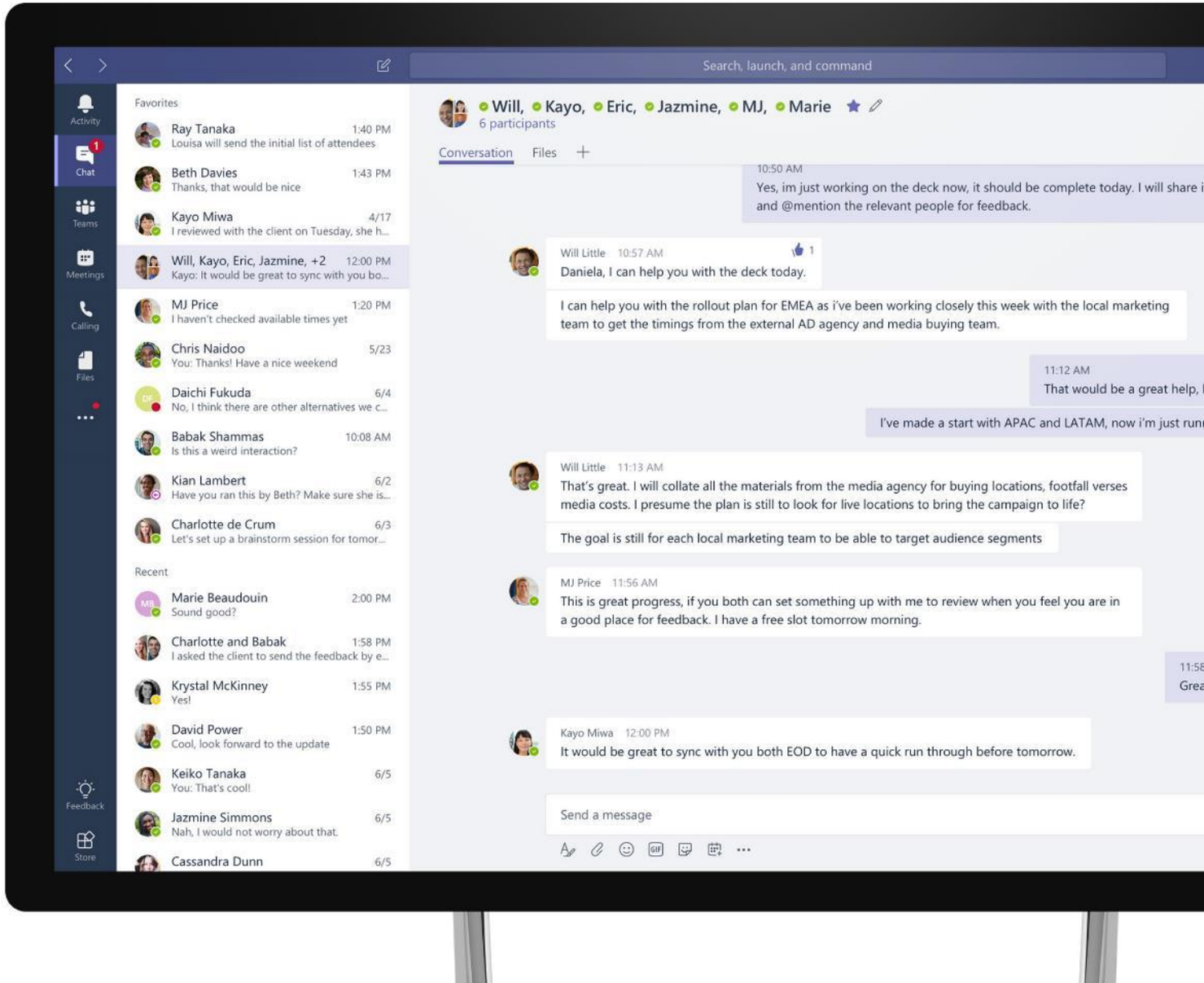
[Create a team from an existing team (microsoft.com)]

[Create a team from an existing group (microsoft.com)]

[Create a team from a template (microsoft.com)]

[Manage team settings and permissions in Teams (microsoft.com)]

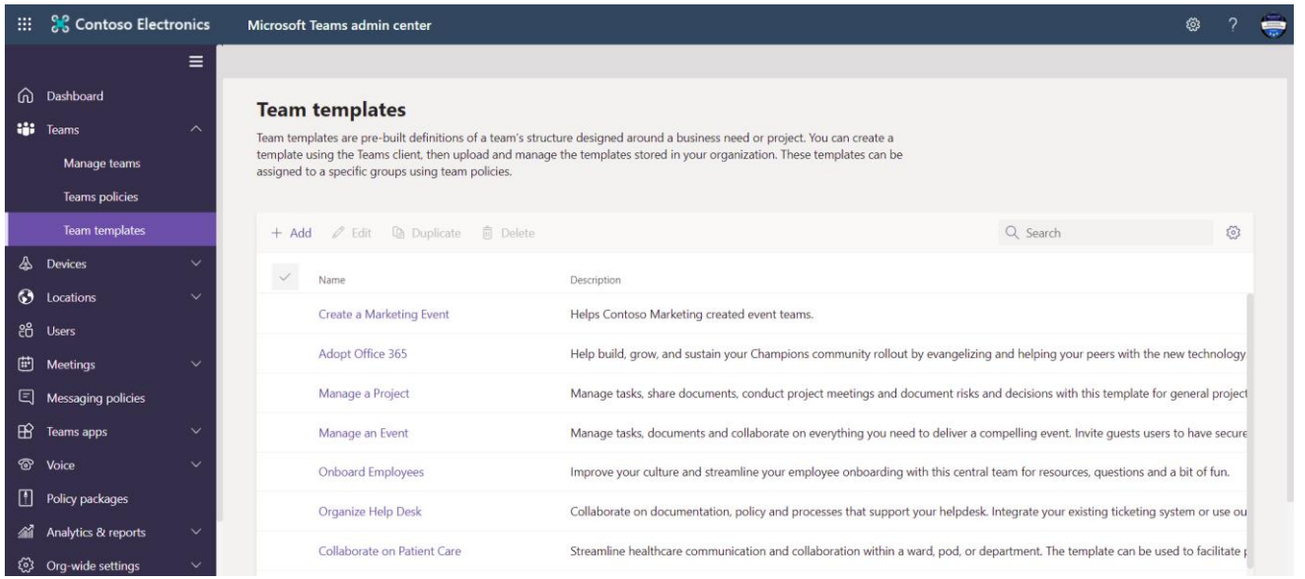
Can I build an automated Workflow to add custom controls for Teams creation?



Templates help control what gets created

- Team Templates
  - Provision teams using a template through the graph
  - Create a Team template from the Admin Portal

Base template type	baseTemplateId	Properties that come with this base template
Standard	`https://graph.microsoft.com/beta/teamsTemplates('standard')`	No additional apps and properties
Education - Class Team	`https://graph.microsoft.com/beta/teamsTemplates('educationClass')`	Apps: • OneNote Class Notebook (pinned to the **General** tab) • Assignments app (pinned to the **General** tab) Team properties: • Team visibility set to **HiddenMembership** (cannot be overridden)
Education - Staff Team	`https://graph.microsoft.com/beta/teamsTemplates('educationStaff')`	Apps: • OneNote Staff Notebook (pinned to the **General** tab)

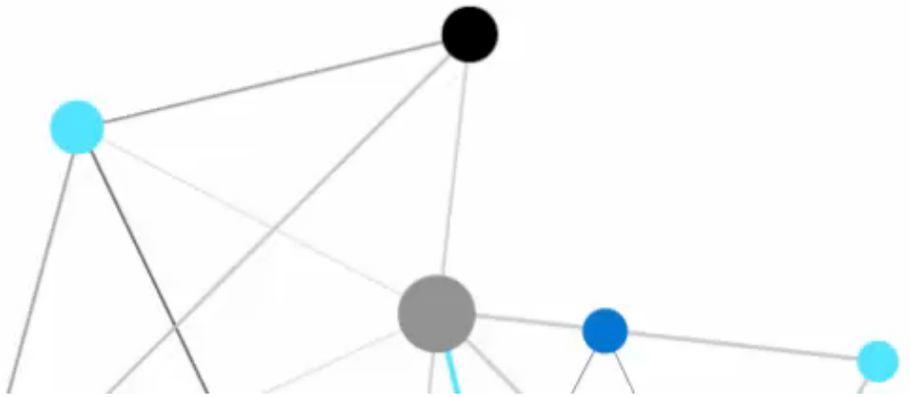


Microsoft

Microsoft Teams

Automating the Team Creation Process

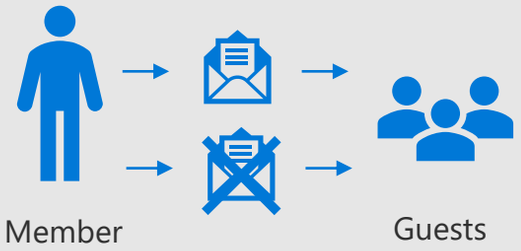
#MicrosoftEmployee



External Access Considerations

Group Level

Guest Access can be **enabled or disabled at the group level**.

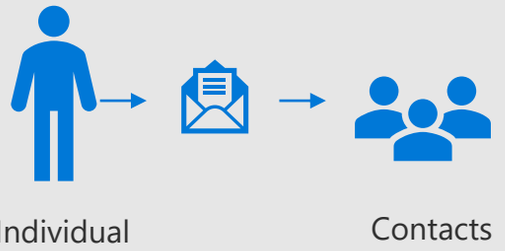


Guest Collaboration

Admins can set Azure, Teams, Group and SharePoint parameters to control Guest Access and Sharing. For example, can force the requirement for a verification code to access a Team.

External Federation

Admins can add allowed/blocked domains.

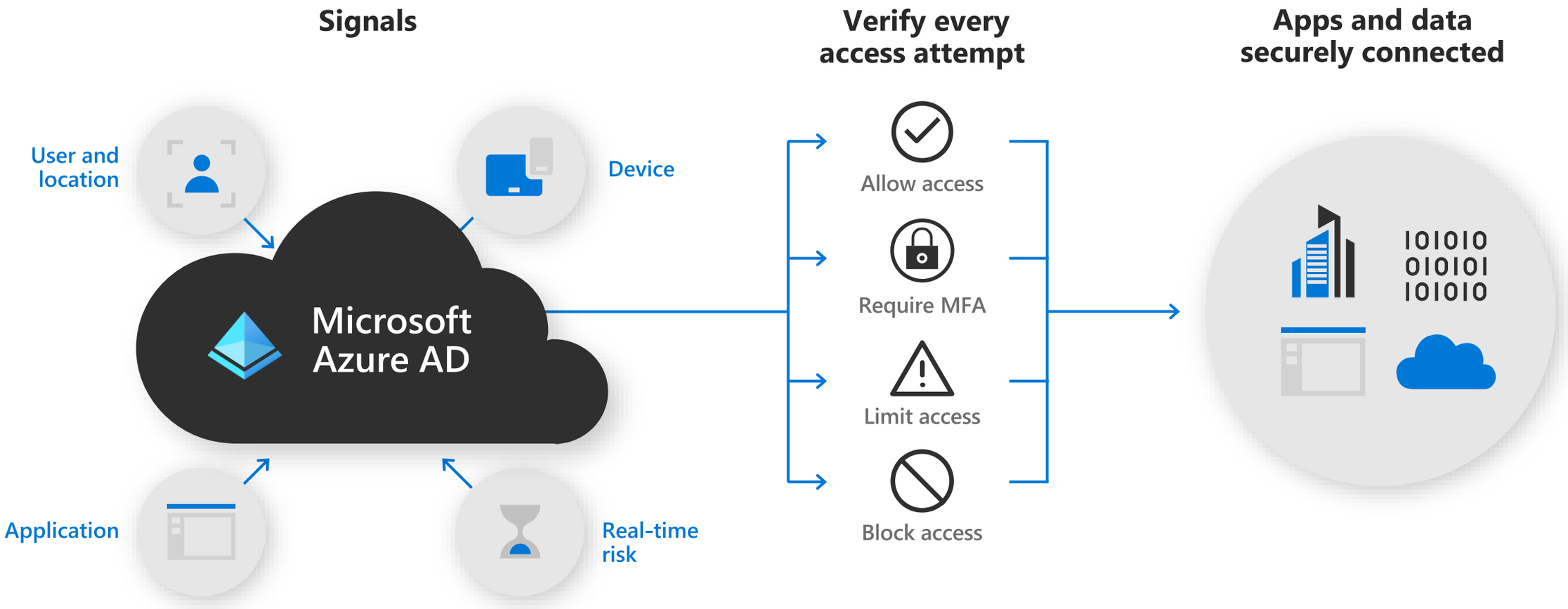


[Manage external access (federation) - Microsoft Teams | Microsoft Docs]

[Collaborate with guests in a team | Microsoft Docs]

Protect access for any user from anywhere

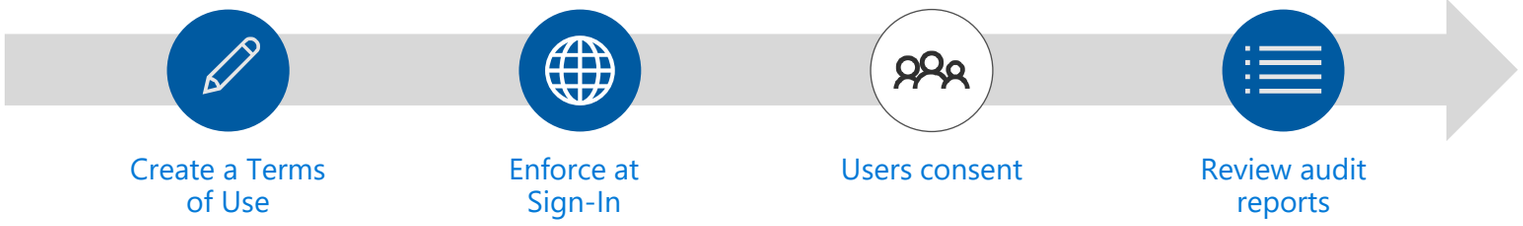
Apply consistent risk-based policies with Conditional Access.

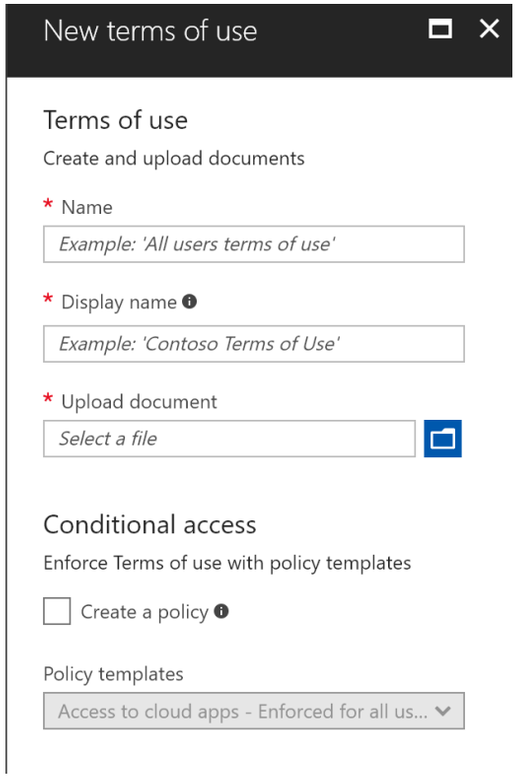


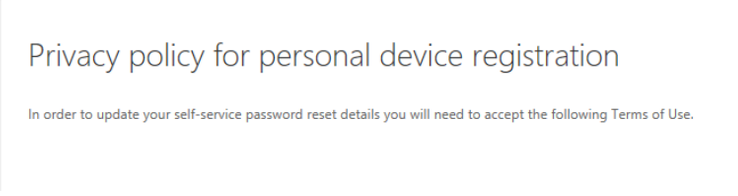
Azure AD feature - Terms of use

Configure, enforce, audit compliance

- Configure a terms of use by uploading a PDF document(s) for each necessary language
- Target to users, groups or applications using conditional access
  - Employees vs guests
  - Domestic vs international employees
  - High Business Impact apps (i.e. Teams)
  - Apps in scope of compliance (e.g., GDPR, SOX, …)
- Enforce acceptance of terms for users in scope
- Audit events show who accepted / which terms / when







Microsoft

Microsoft Teams

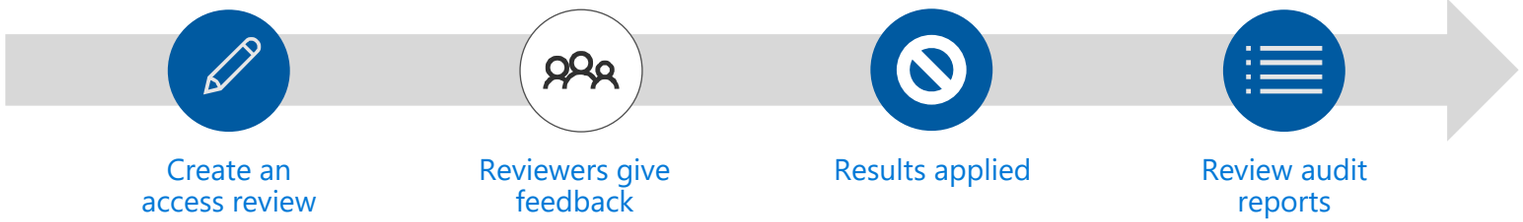
Guest Access MFA & TOU

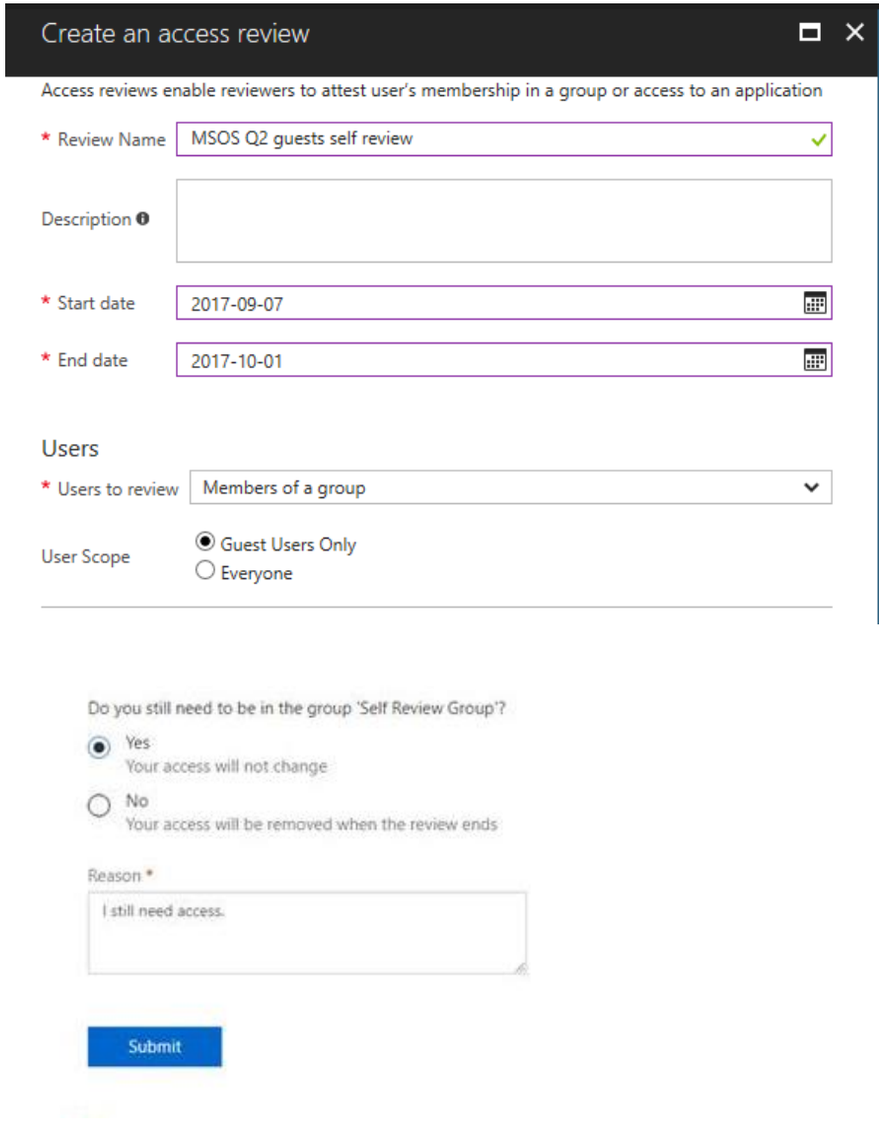
#MicrosoftEmployee

Azure AD feature - Access reviews

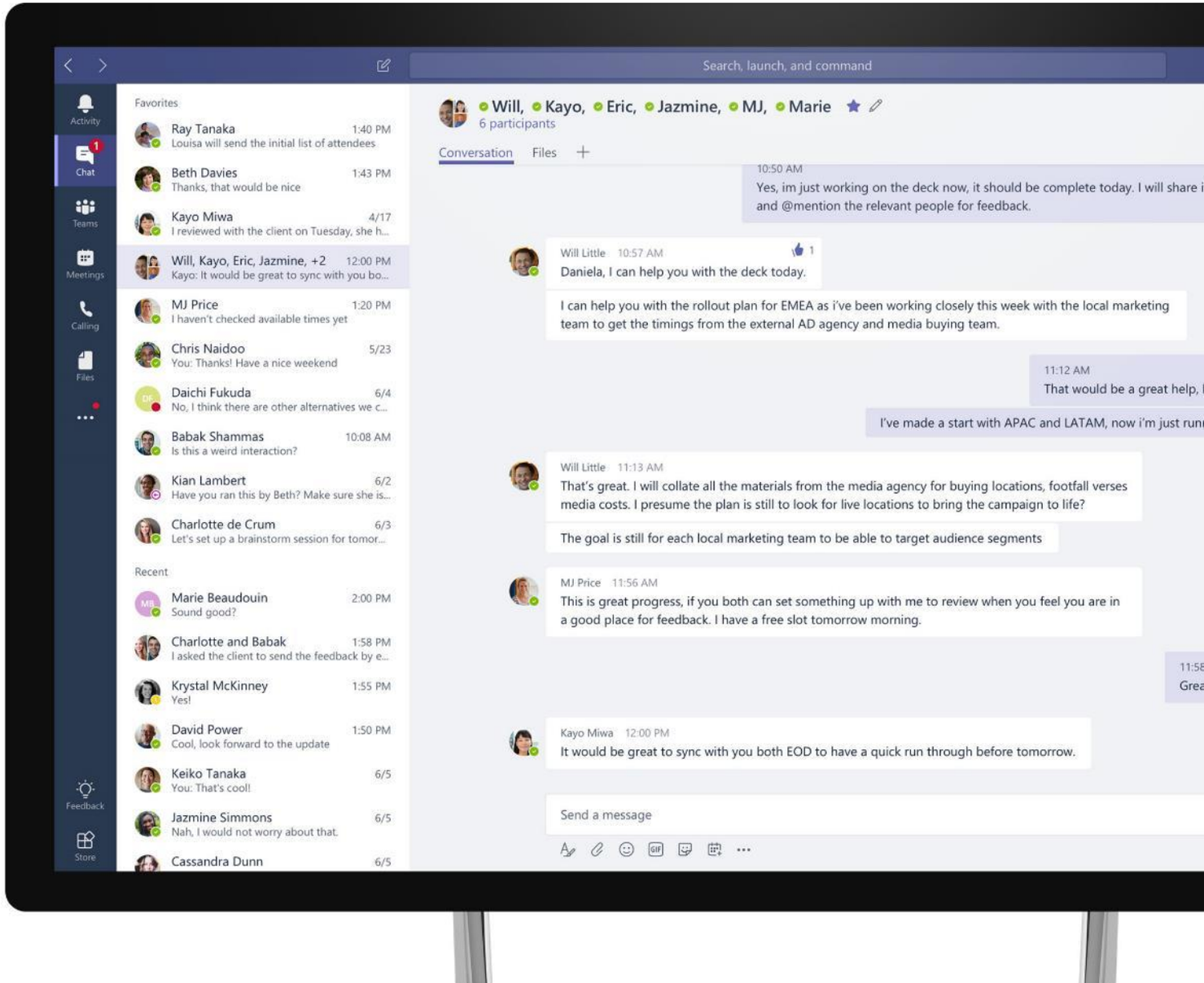
Recertify: attest and audit continued access

- Review Office group members, security group members, and users assigned to applications
- Optionally, scope the reviews to just guests
- Select reviewers from the resource
  - Group owners
  - Members review their own access
  - Select specific individuals in the directory

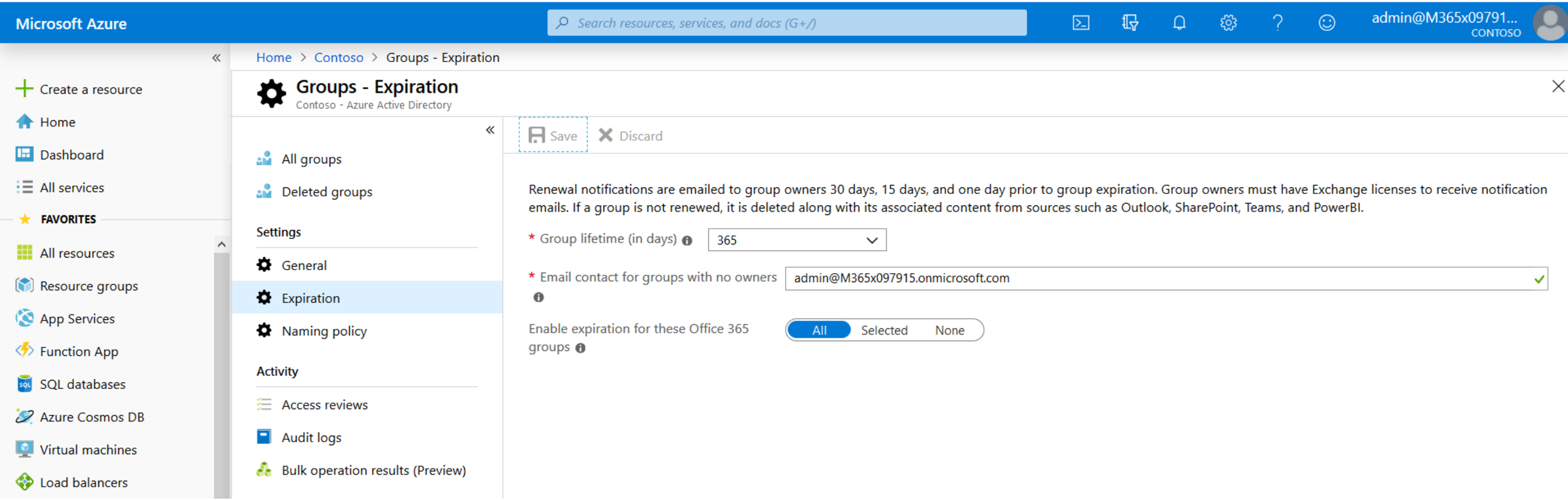




What’s the most straightforward way to get rid of unused Teams?



Tenant Group Expiration Policy



Managing and governing Office 365 groups at scale

Creation permissions

Naming policy

Expiration policy

Soft delete and restore

Guest access

Reporting

Policies and information protection

Azure AD access reviews

Governance (Licensing) Planning:
https://docs.microsoft.com/en-us/MicrosoftTeams/plan-teams-governance

Break

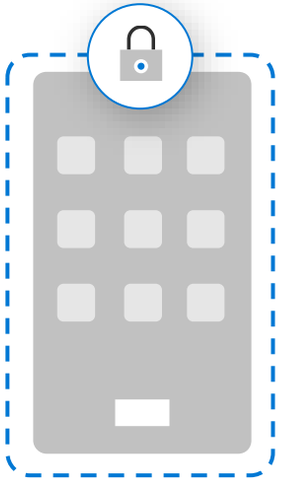
Back at 1130

Information Protection

Protect your data on virtually any device with Endpoint Manager

Mobile **Device** Management (MDM)

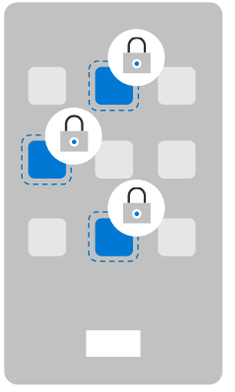
Conditional Access
Restrict access to managed and compliant devices.



- Enroll devices for management.
- Report and measure device compliance.
- Provision settings, certs, profiles.
- Remove corporate data from devices.

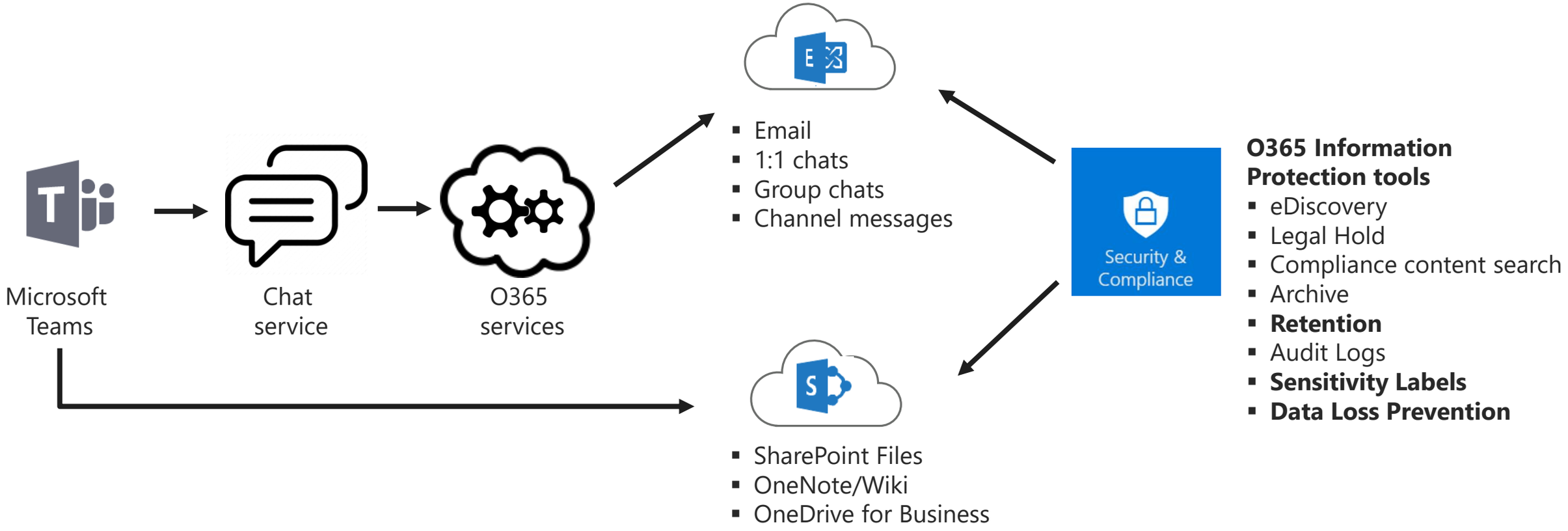
Mobile **Application** Management (MAM)

Conditional Access
Restrict which apps can be used to access email or files.



- Publish mobile apps to users.
- Report app inventory and usage.
- Configure and update apps.
- Secure and remove corporate data within mobile apps.

Information Protection Architecture



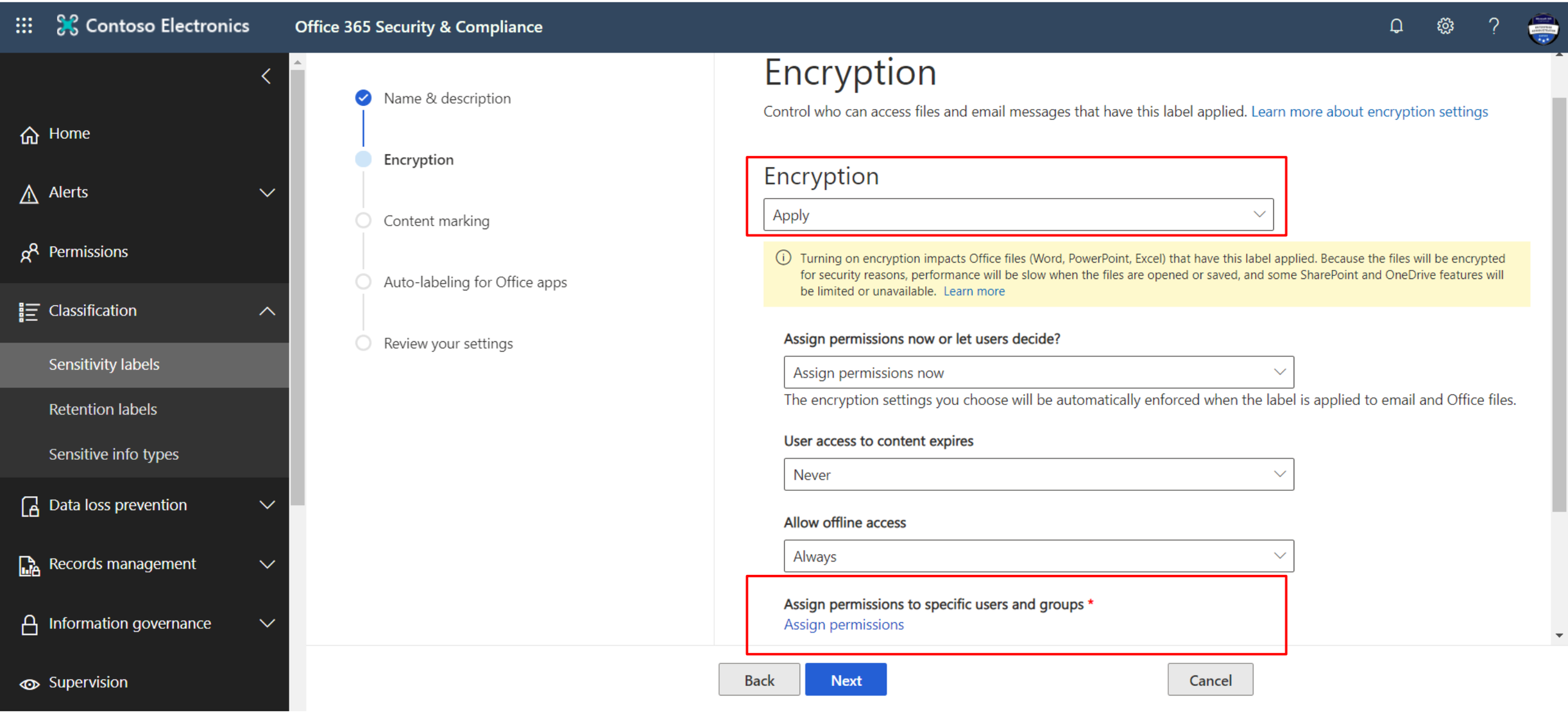
Teams chats are stored in a hidden folder in the mailbox of each user included in the chat, and Teams channel messages are stored in a similar hidden folder in the group mailbox for the team.

Sensitivity labels enable policy-driven outcomes

- Customizable
- Persists as container metadata or file metadata
- Readable by other systems
- Enforce DLP policies across devices, apps, services
- Extensible to partner solutions

- Manual or automated application
- Apply to content or containers
- Label data at rest, data in use, or data in transit
- Enable protection actions based on labels
- Seamless end user experience across productivity applications

Sensitivity labels – Modern Classification

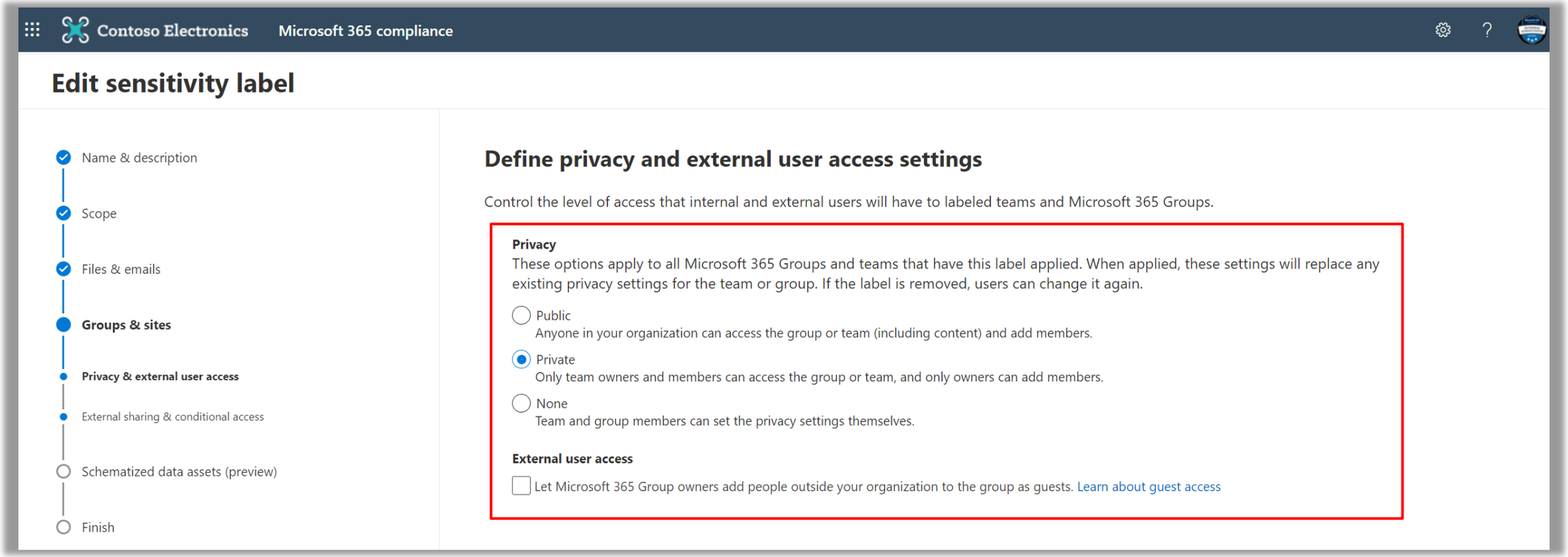


Microsoft

Teams Meetings Security

Document Permissions

Sensitivity labels with Teams, Office 365 Groups, and SharePoint sites

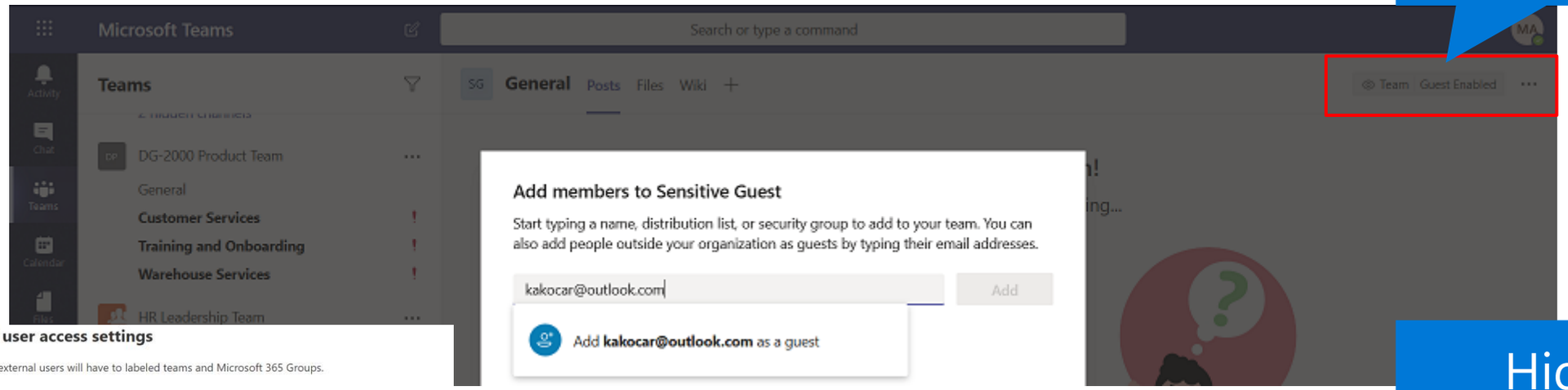


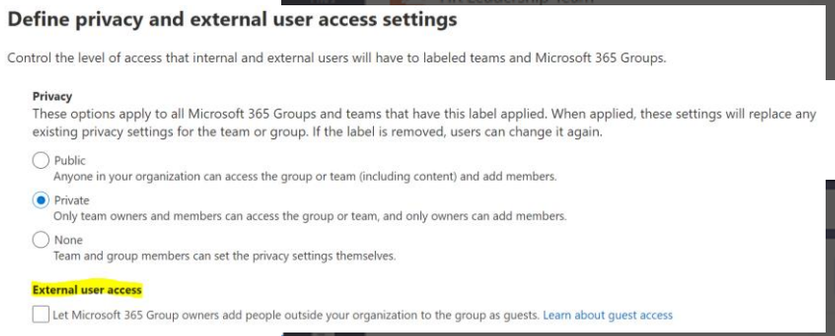
Microsoft Ignite BRK3007: https://myignite.techcommunity.microsoft.com/sessions/81519?source=sessions

Doc: https://docs.microsoft.com/en-gb/microsoft-365/compliance/sensitivity-labels-teams-groups-sites

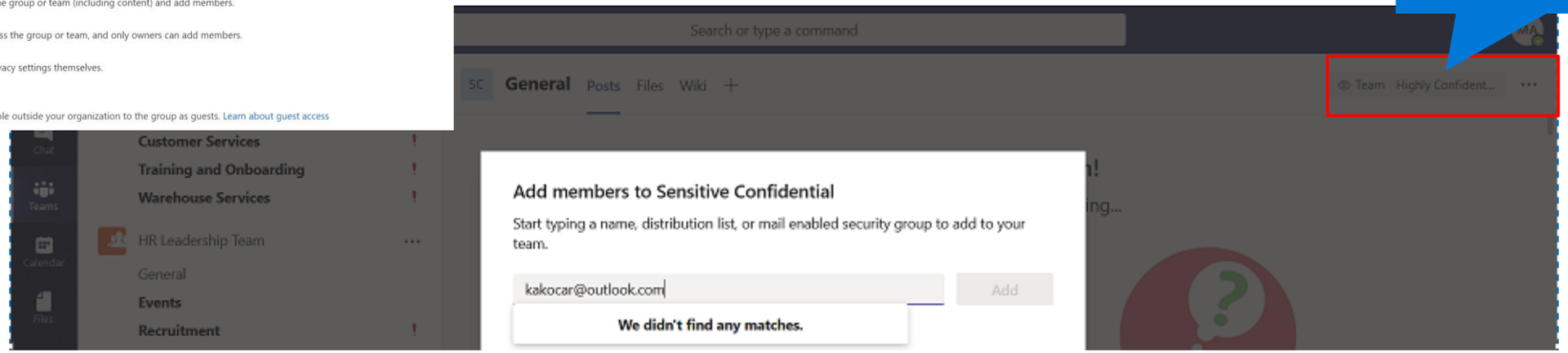
Sensitivity Labels and Guest Access

Guest Enabled

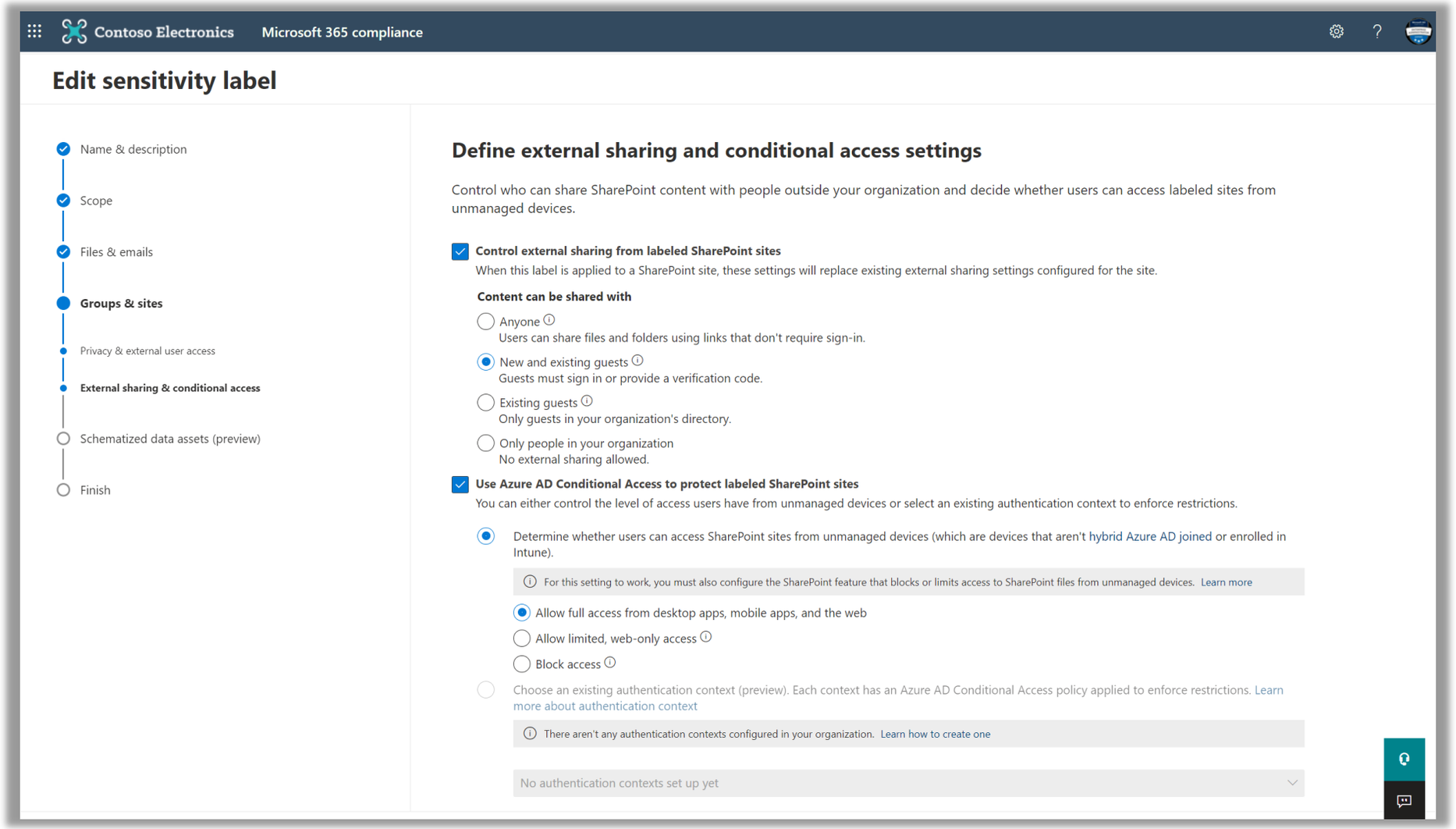




Highly Confidential



Sensitivity labels with Teams, Office 365 Groups, and SharePoint sites



DLP in Microsoft 365

Intelligent detection and control of sensitive information

Intelligent data detection & discovery

Identify sensitive information across locations, leveraging 100+ sensitive information types, custom patterns

Flexible policy management & enforcement

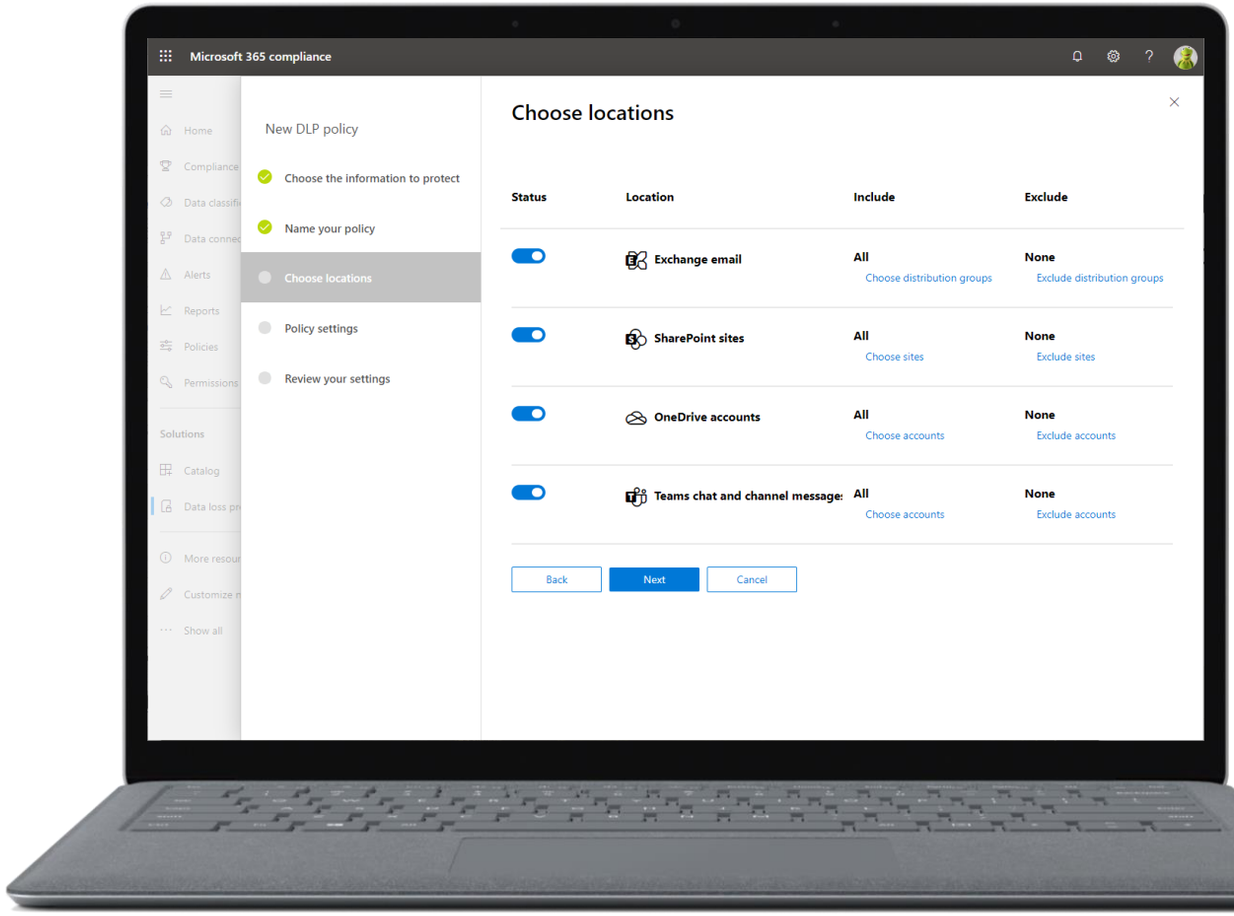
Control and restrict movement of sensitive information

Comprehensive monitoring & alerting

Take action on reports, policy violation alerts, improper data use

Integrated user experiences

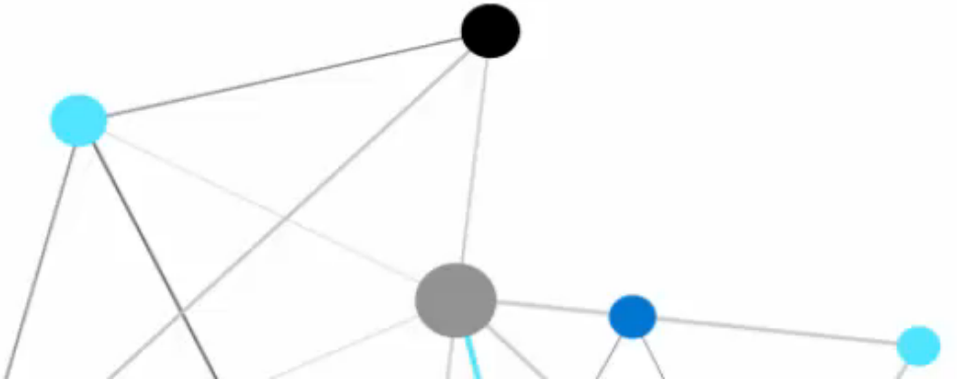
Built-in experiences in apps and services



Microsoft

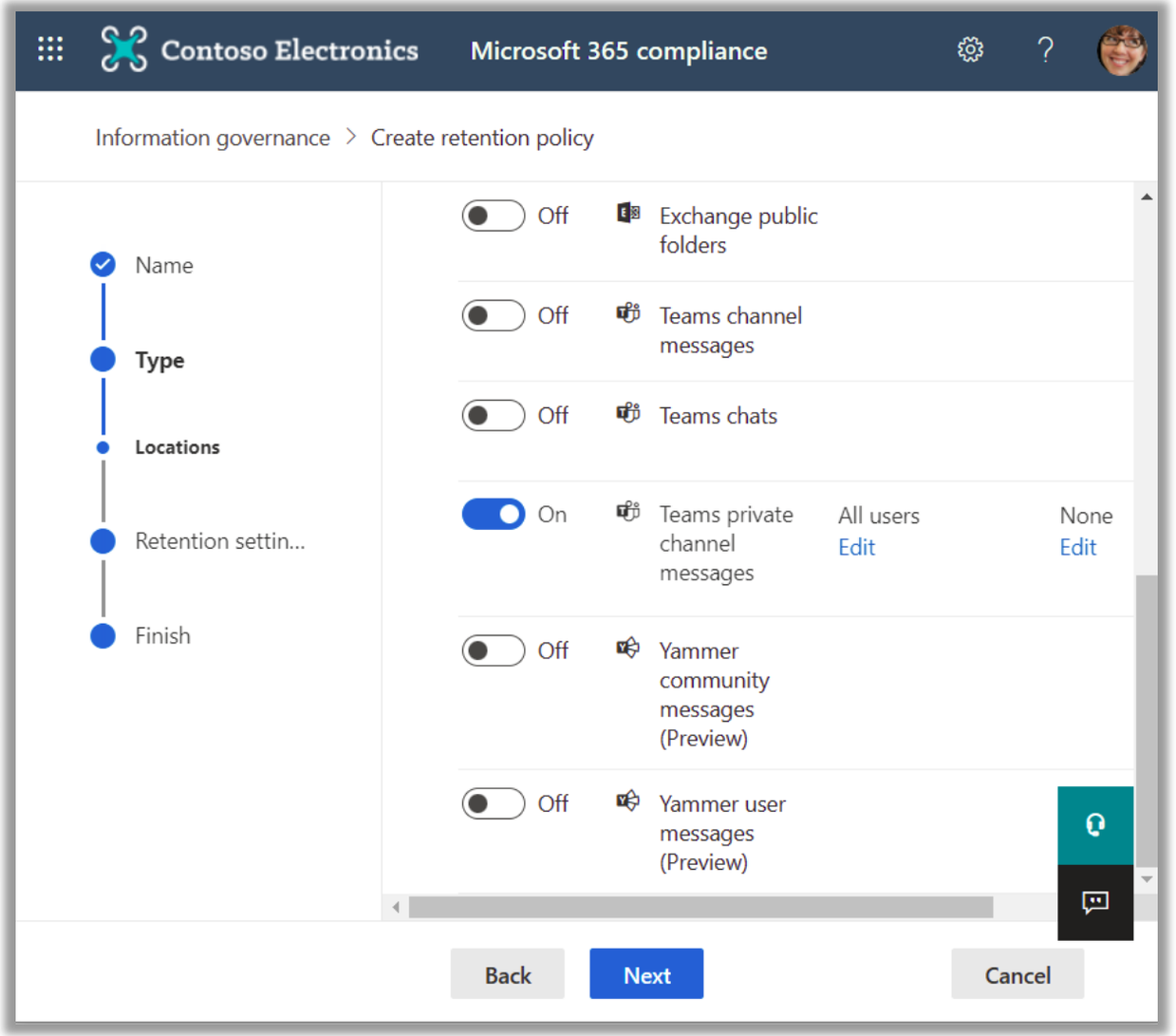
Microsoft Teams Meetings

DLP in Meeting Chat



Retention Policies for Microsoft Teams

Features	Comments
Retention Policies for Teams Chat and Channel Messages	Teams requires a retention policy that's separate from other workloads.
Support for retention policies for Teams Files	To retain or delete files in Teams, create retention policies that apply to OneDrive for Business and SharePoint Online.
Support for Preservation and Deletion policies > 1 day	Teams may take up to three to seven days to clean up expired messages.
Private Channels	Supported



https://docs.microsoft.com/en-us/microsoftteams/retention-policies

Search and eDiscovery Overview

Feature	What it does	Who typically uses it
Content Search	Search for items such as email and documents in your 365 organization	Security team, Human Resources, 3rd Party Investigators
Core eDiscovery	Same as above, but you can place content on "**Hold**" in context of cases	Legal Team, Investigators
Advanced eDiscovery	Same, but with many more advanced features than core eDiscovery	Same as above

Use Cases

- **LITIGATION**
- **INVESTIGATIONS**
- **FREEDOM OF INFORMATION ACT REQUESTS**
- **DATA SPILLAGE / SEARCH & PURGE**

Getting relevant results: Teams

- **Channels**
  - Conversations stored in the mailbox that's associated with the team
  - Files shared stored on the Team's mailbox site

- **Chats**
  - Conversations stored in the mailbox of the users involves in the chat
  - Files stored in the OneDrive account *of the user who shares the file*

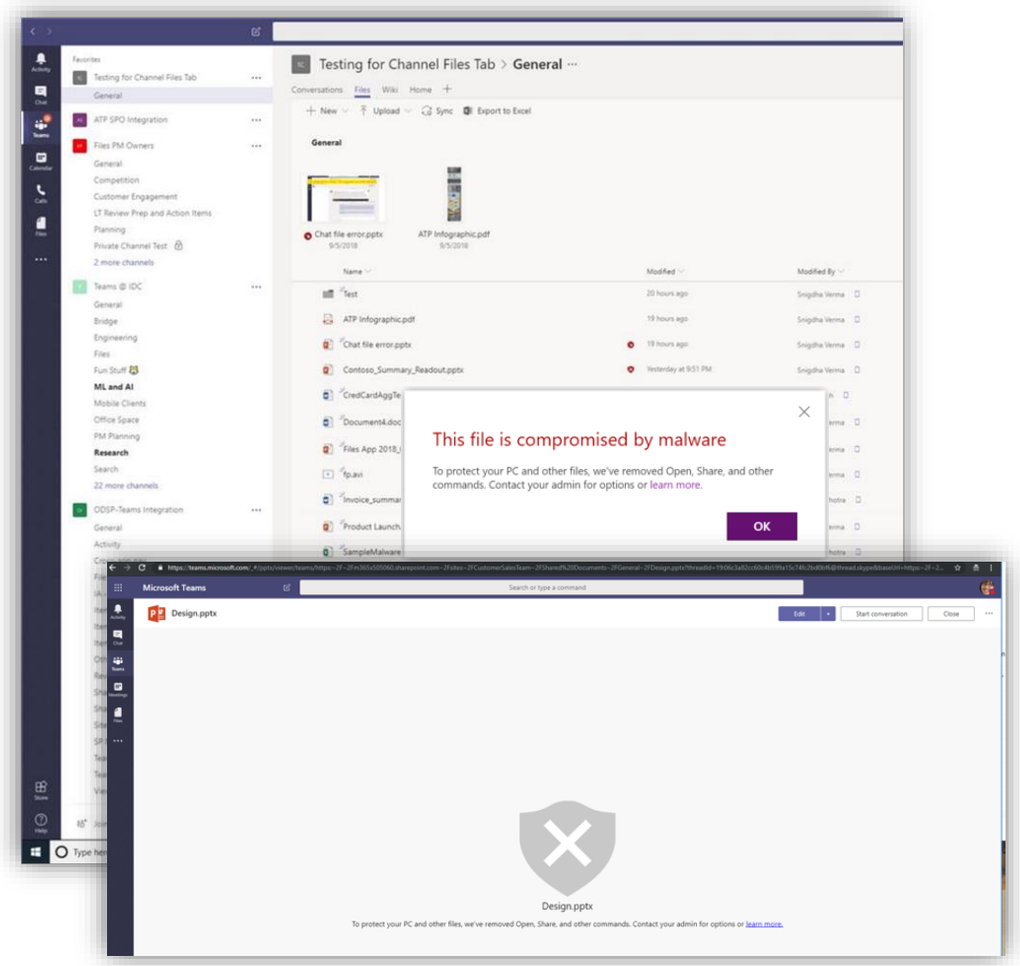
- **Meetings & Calls**
  - Summary information for Teams Channel meetings/calls are stored in mailboxes of users who dialed-in to the meeting/call

Conduct an eDiscovery investigation of content - Microsoft Teams | Microsoft Docs

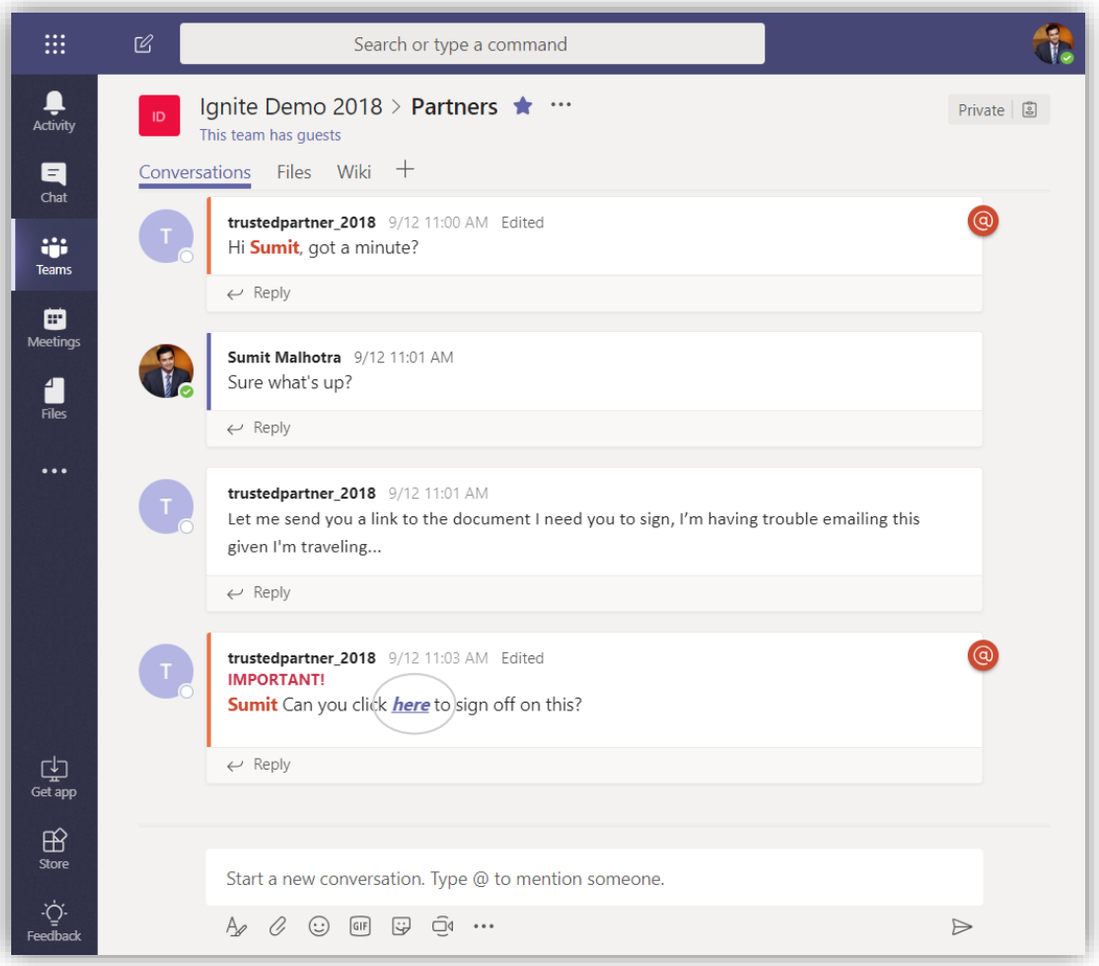
It can take up to **8 hours for meetings and calls to be made available** for searching

Threat Management

ATP Protection within Microsoft Teams



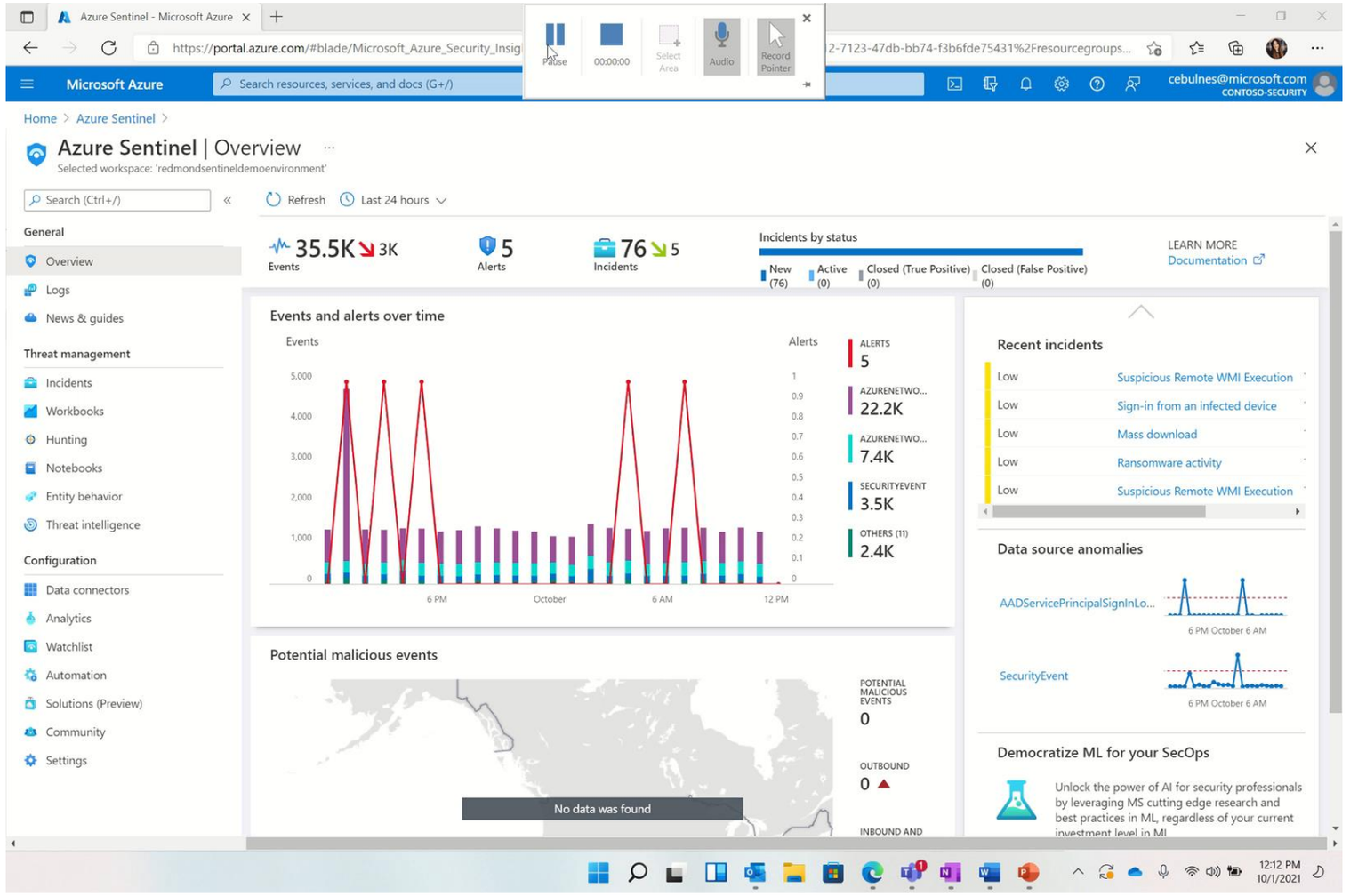
Microsoft Teams on Windows showing files detected and blocked by [Office 365 ATP]



Malicious URL in conversations from Guest/External user in **Microsoft Teams** on Windows is protected by SafeLinks

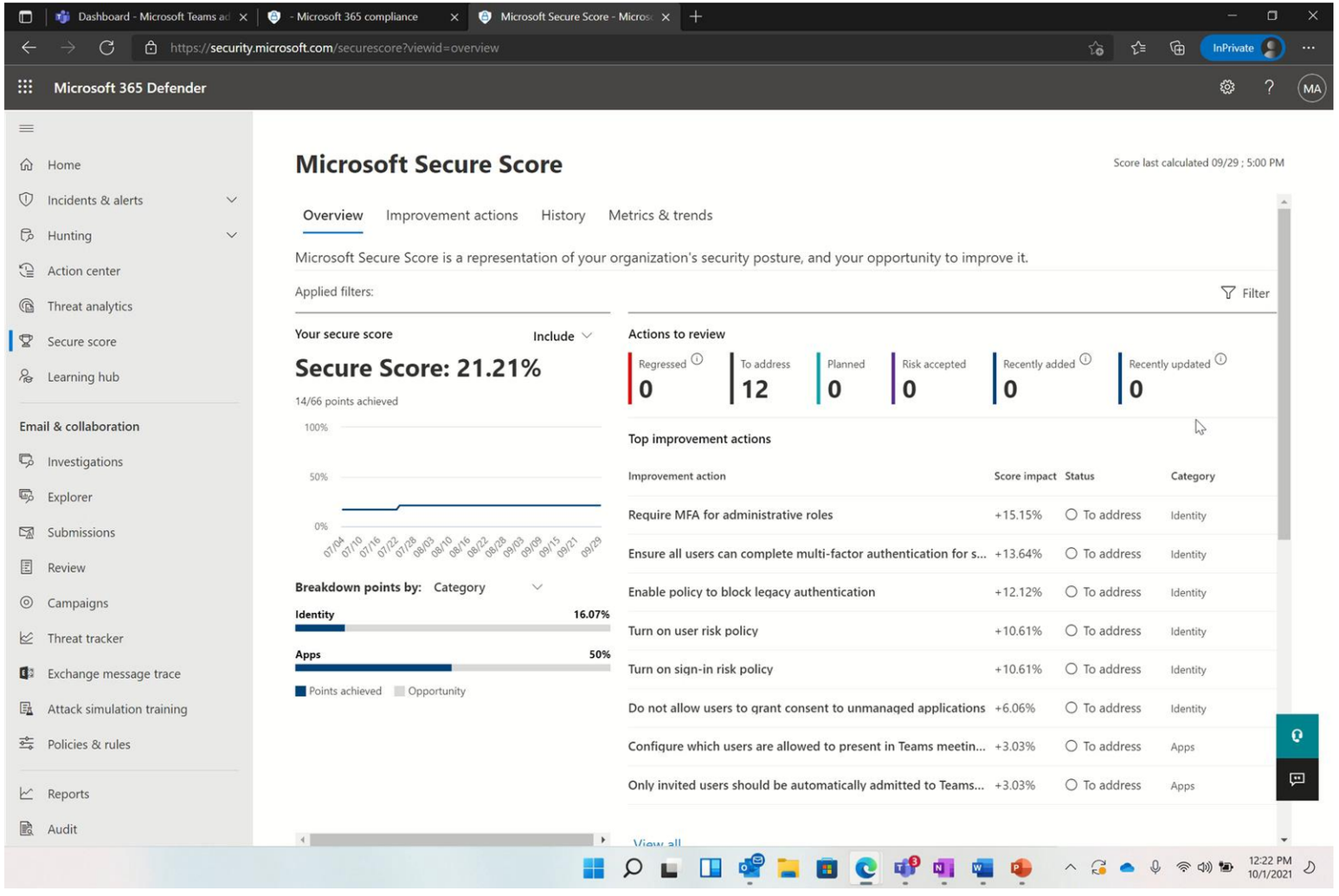
Sentinel Integration for Microsoft Teams

Admin uses audit logs to check on activities, but she wants to get **alerted** for suspicious activity that happens in her tenant. Name recently changed to Microsoft Sentinel.



Secure Score for Microsoft Teams

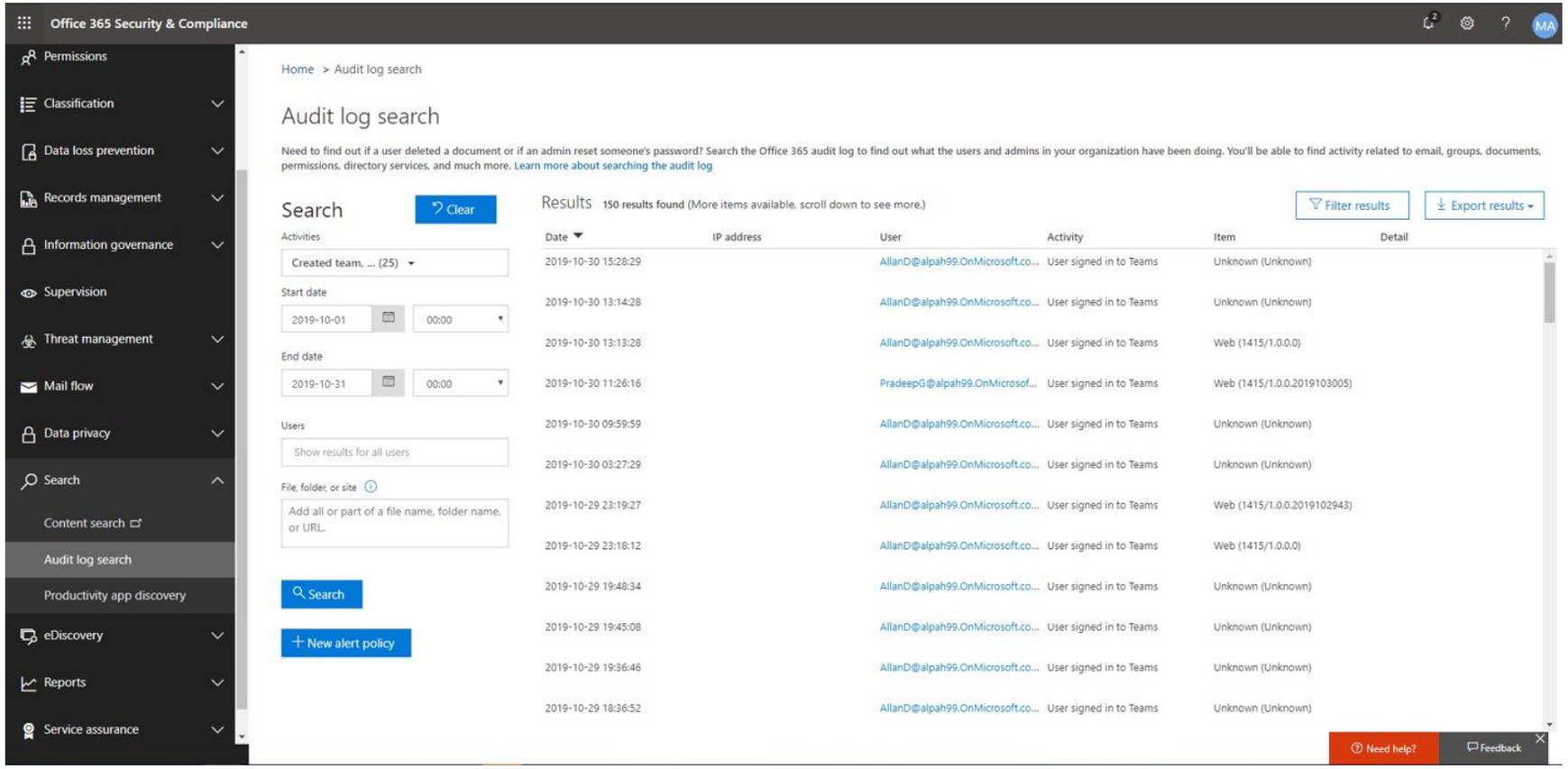
Admin looks over her policies; given she has been receiving incidents from Sentinel, she goes to Secure Score to view recommendations for policies that she may have missed



Teams Audit Logs

The audit log can help you investigate specific activities across Microsoft 365 services. For Microsoft Teams, here are some of the activities that are audited

- Team creation
- Team deletion
- Added channel
- Deleted channel
- Changed channel setting



Getting relevant results: Teams

- **Channels**
  - Conversations stored in the mailbox that's associated with the team
  - Files shared stored on the Team's mailbox site

- **Chats**
  - Conversations stored in the mailbox of the users involves in the chat
  - Files stored in the OneDrive account *of the user who shares the file*

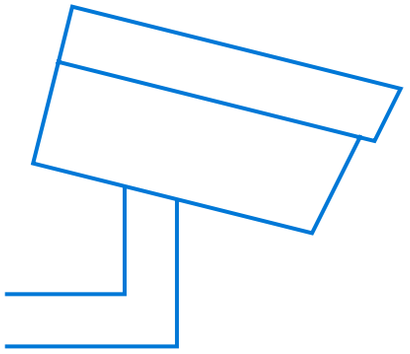
- **Meetings & Calls**
  - Summary information for Teams Channel meetings/calls are stored in mailboxes of users who dialed-in to the meeting/call

Conduct an eDiscovery investigation of content - Microsoft Teams | Microsoft Docs

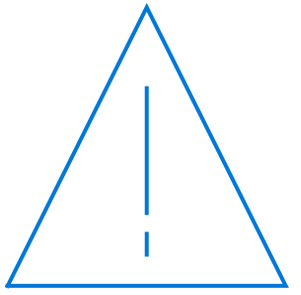
It can take up to **8 hours for meetings and calls to be made available** for searching

Managing Teams Policies

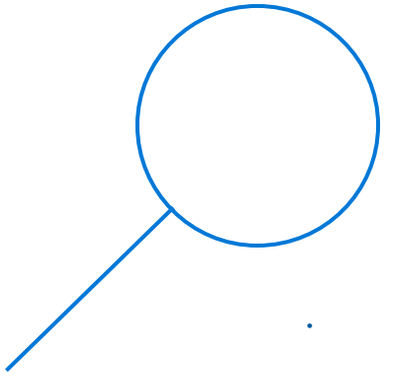
Information Barrier (IB)/Ethical wall in Teams



Control flow of information



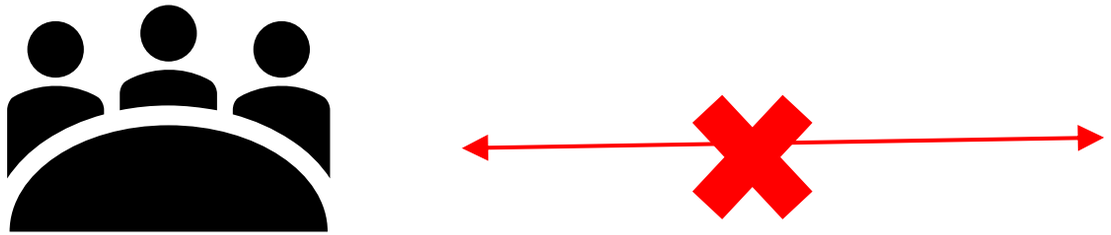
Quarantine information



Restrict information sharing

Information Barrier in Teams

Policy example – Investment Bankers cannot find/communicate with Financial advisors

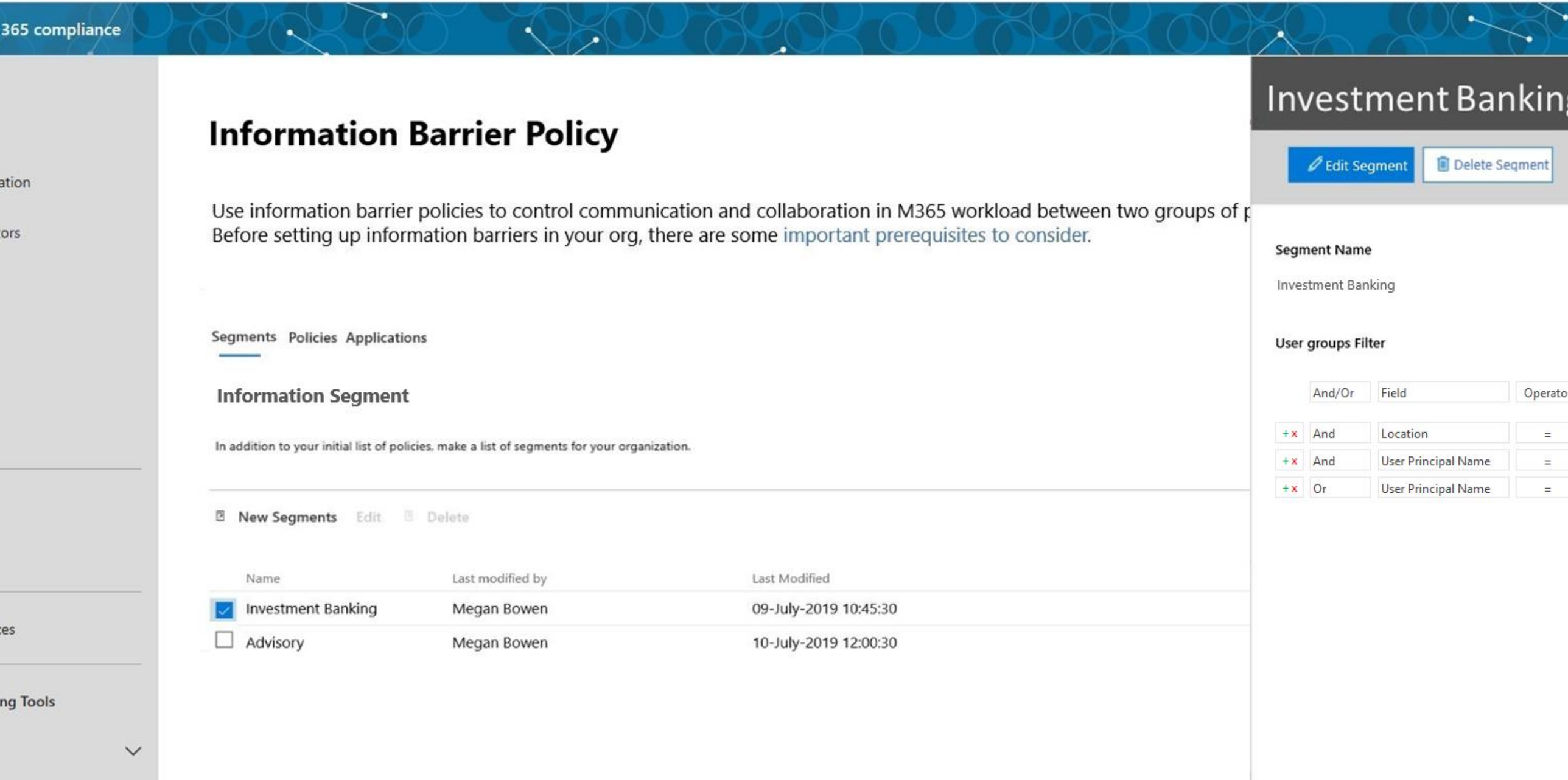


Investment Banker segment

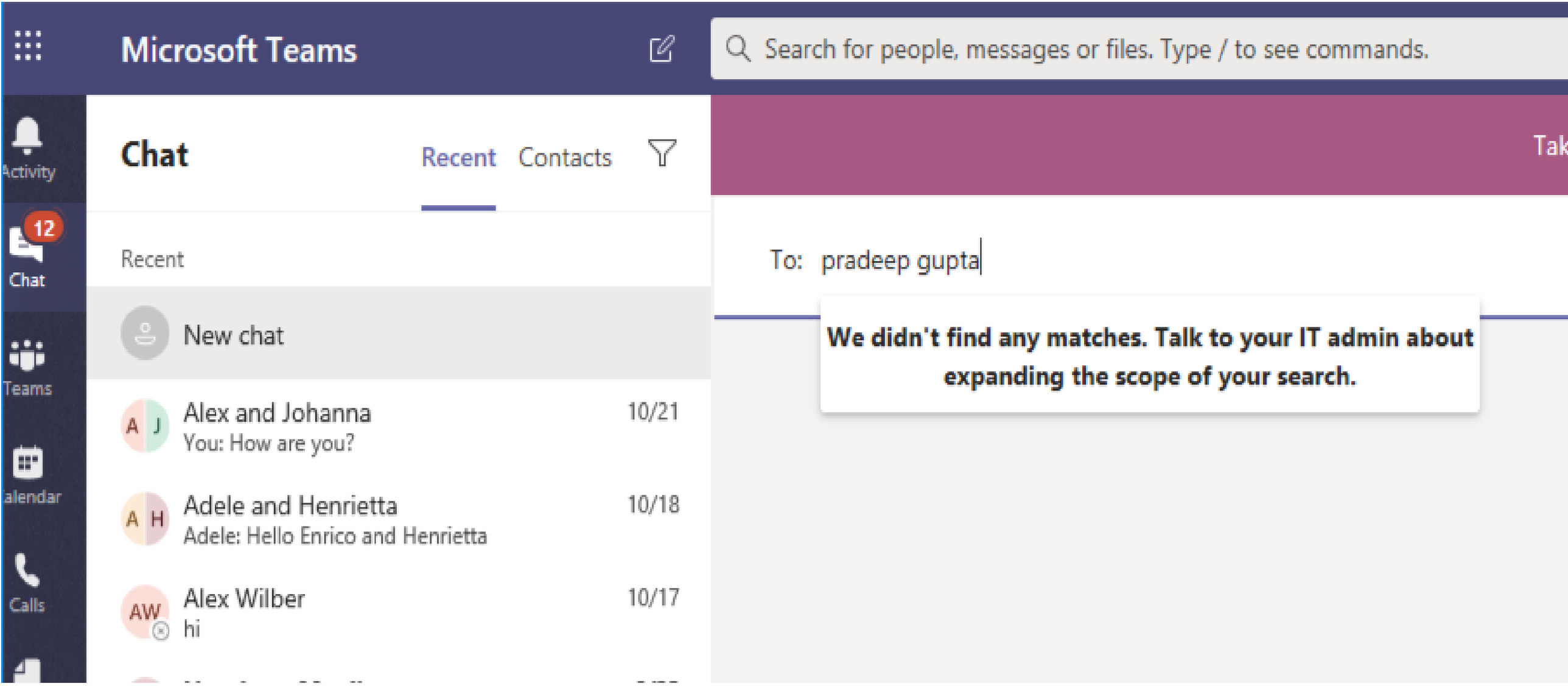
Financial advisor Segment

HR Segment

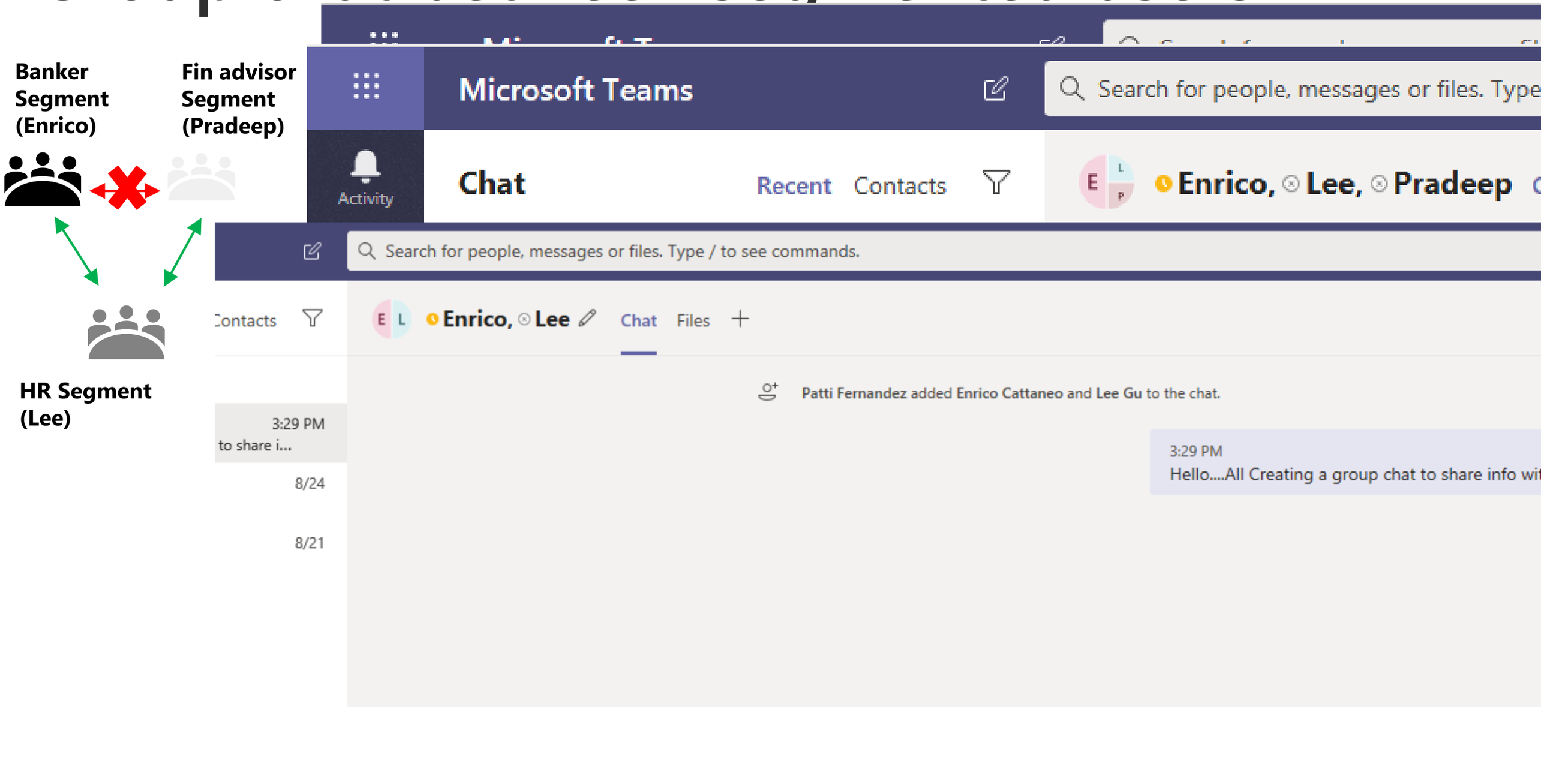
Info Barrier policies in SCC



1x1 chats with users in conflicting segment



Group chat between segmented users

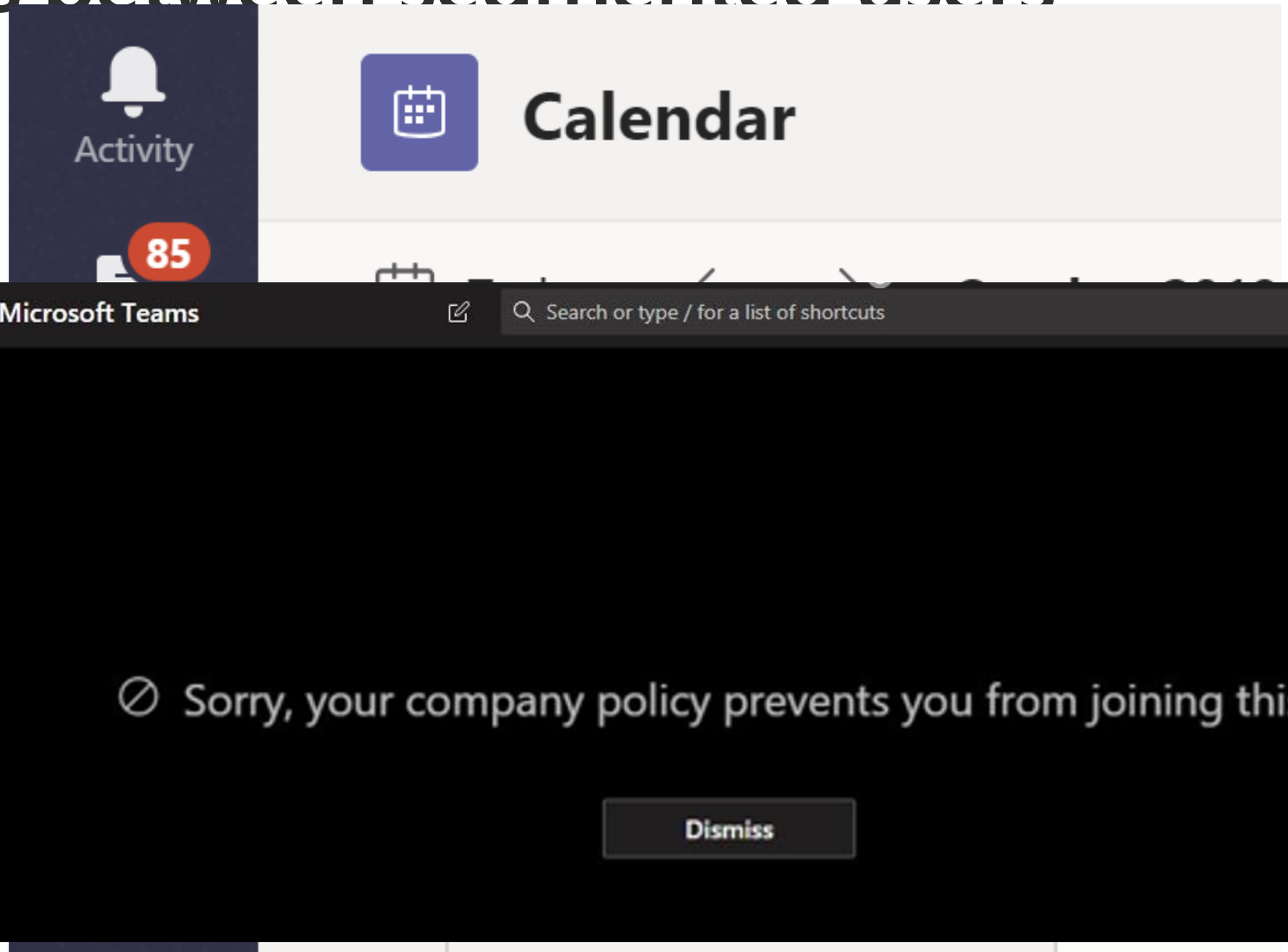


Meetings between segmented users

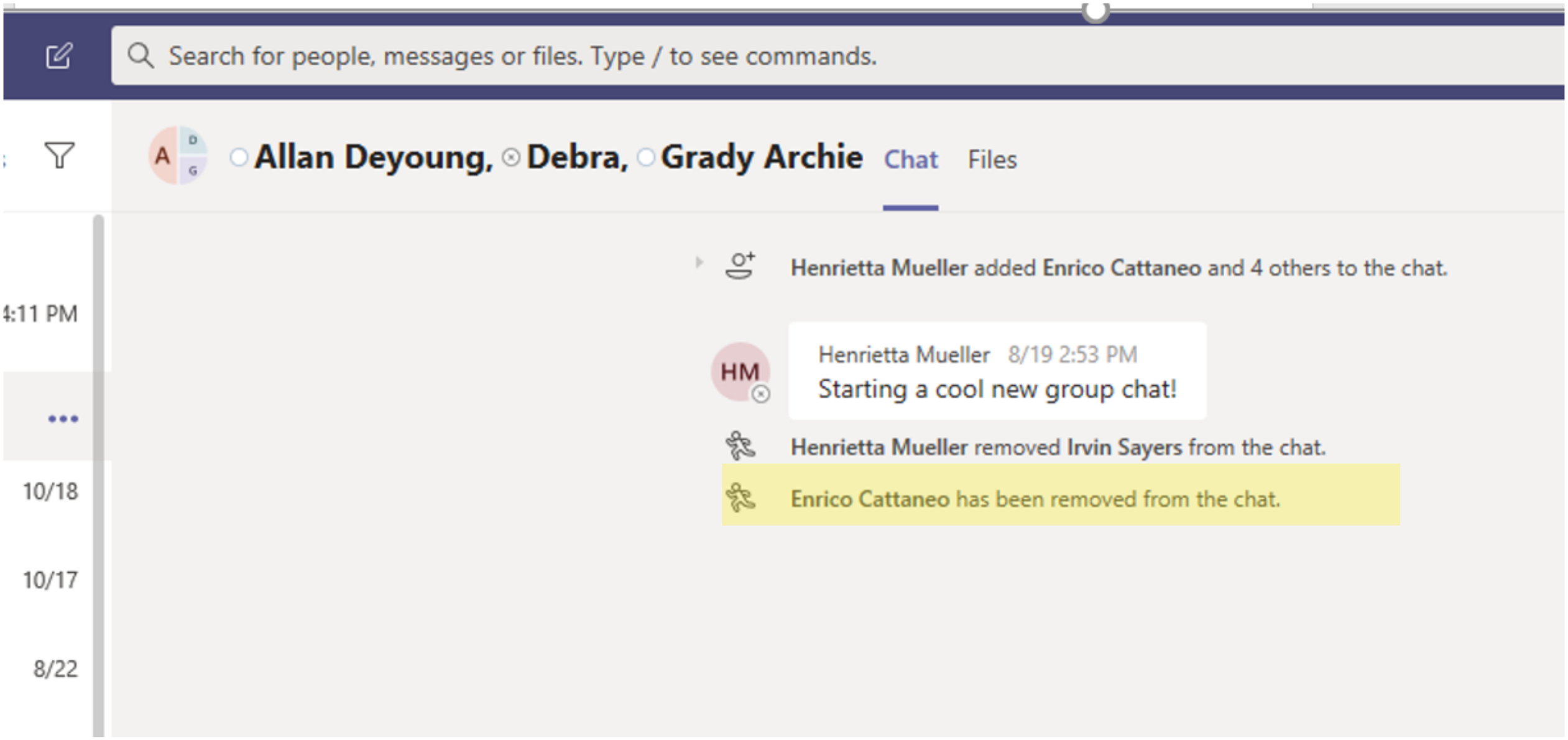
Banker Segment (Enrico)

Fin advisor Segment (Pradeep)

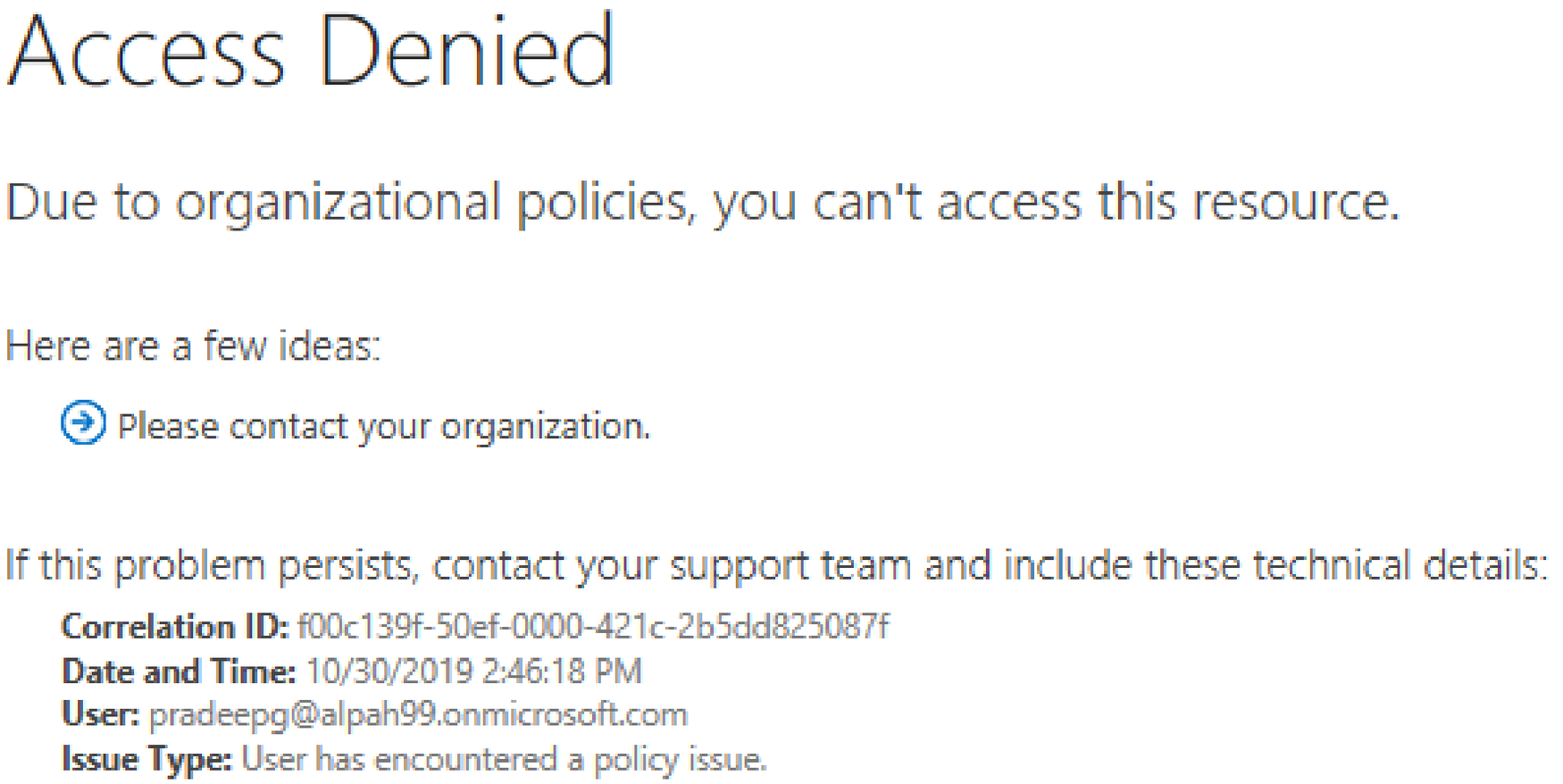
HR Segment (Lee)



Users move between departments



IB & files stored in SPO sites

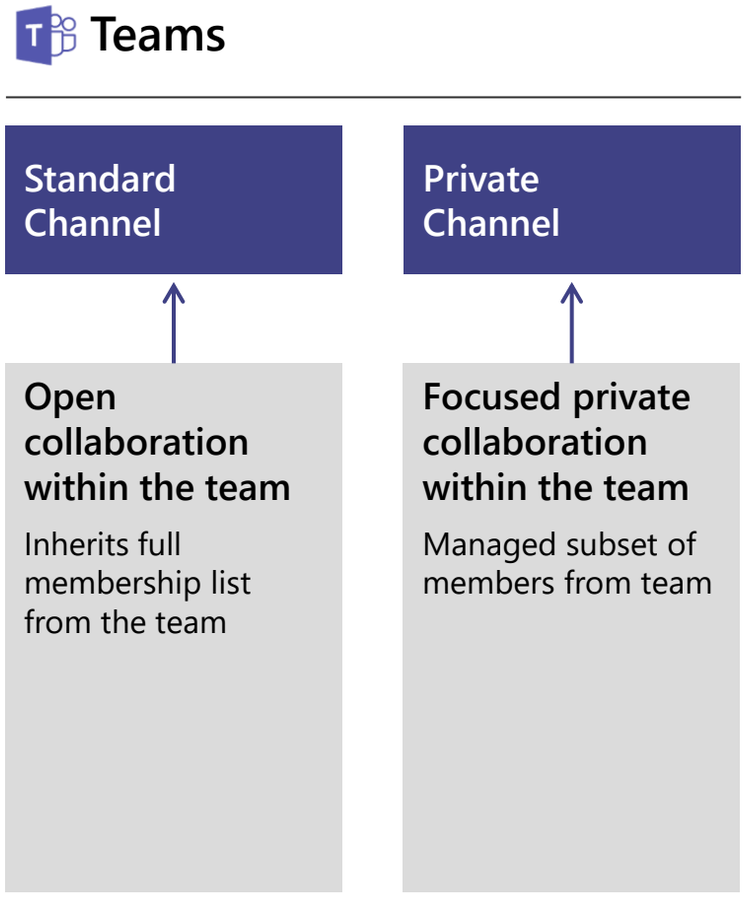


When is IB checked?

- Members are added to a team
- New chat (1x1, group) is created
- **Member is invited to a meeting**
- **Screen sharing**
- **Phone call (VOIP) in Teams**
- **Access to SPO site & sharing files**

Private channels

Focused private collaboration within a team



Creation

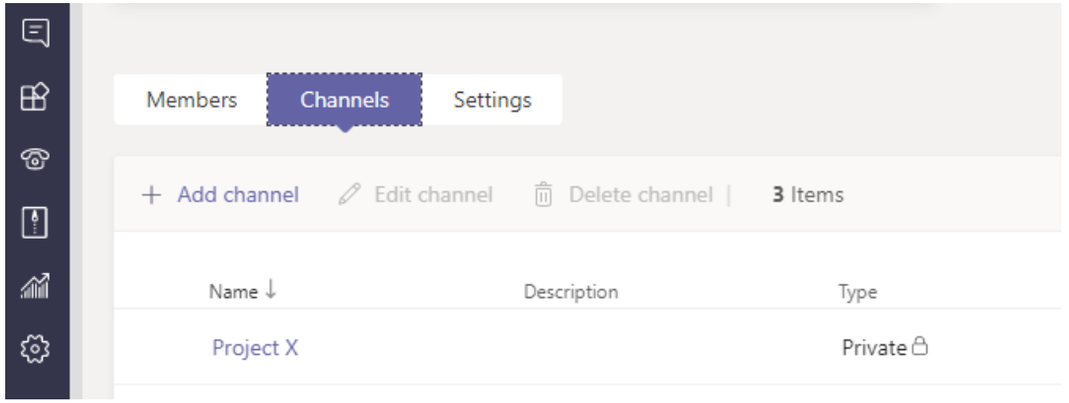
- Admins can control via policies who can create private channels in tenant
- Team owners can control via setting if members can create private channels
- Limited to 30 private channels per team at launch (in addition to 200 standard channels)

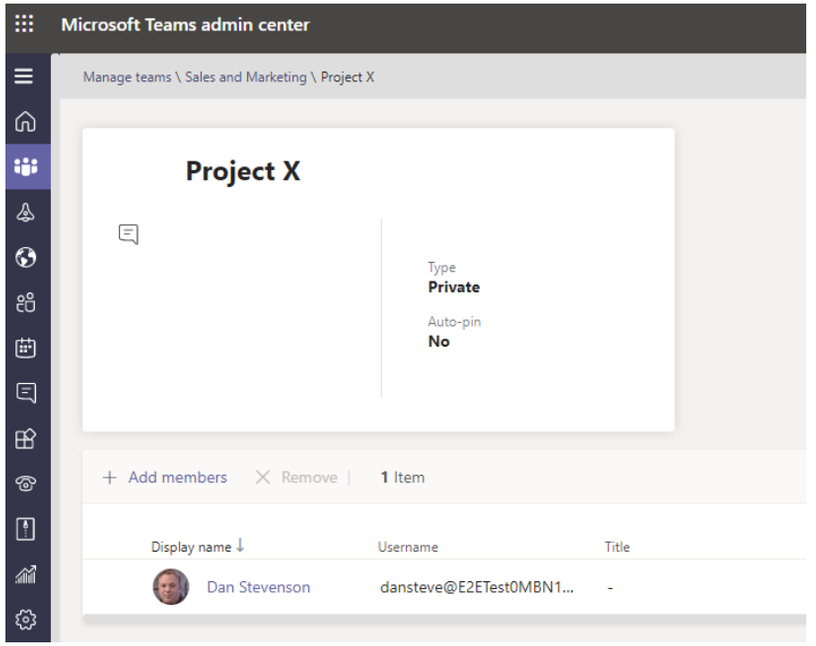
Membership

- Private channel owners can add members and guests to a private channel
- Only existing members and guests in the team can be added to a private channel
- Only members of the private channel can view private channel content
- Limited to 250 members per private channel at launch

Administration

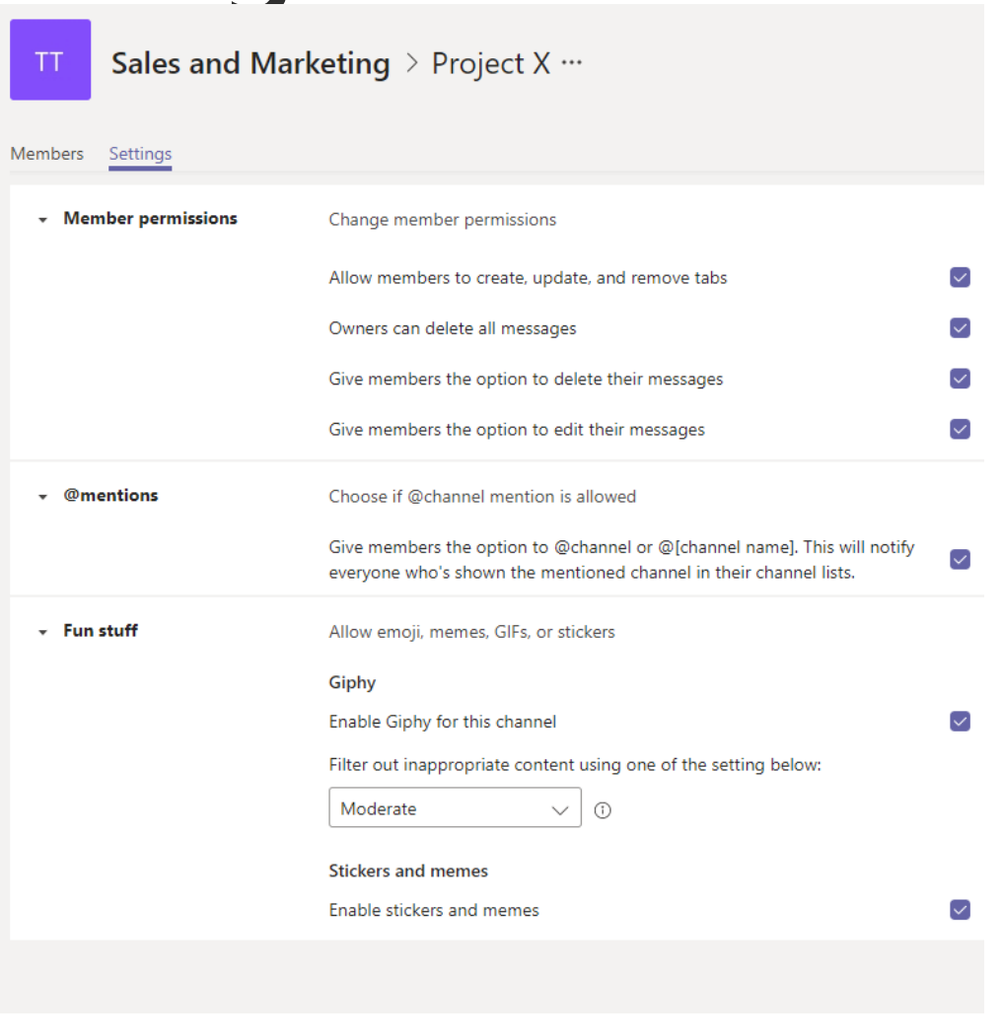
- **All teams and channels, including private channels, can be managed from the Teams admin portal**
  - Create or delete private channels
  - Edit channel name & description
  - Add or remove members
  - Promote or demote members and owners
- **PowerShell & Graph API support**





Channel owners and settings

- **Private channels owners manage the membership and life cycle of private channels**
  - Last owner of a private channel cannot be removed from the team
  - If a private channel becomes ownerless (user leaves company), an existing non-guest member is auto-promoted to owner
- **Private channels inherit settings from the team on create**
  - Settings can be changed at channel level



Team owners and private channels

- Team owners can control if members can create private channels
- Team owners can see names, last activity time and owners of all private channels in a team
- Team owners can delete team or individual private channels without being a member
- Removing a member from the team removes them from all private channels*

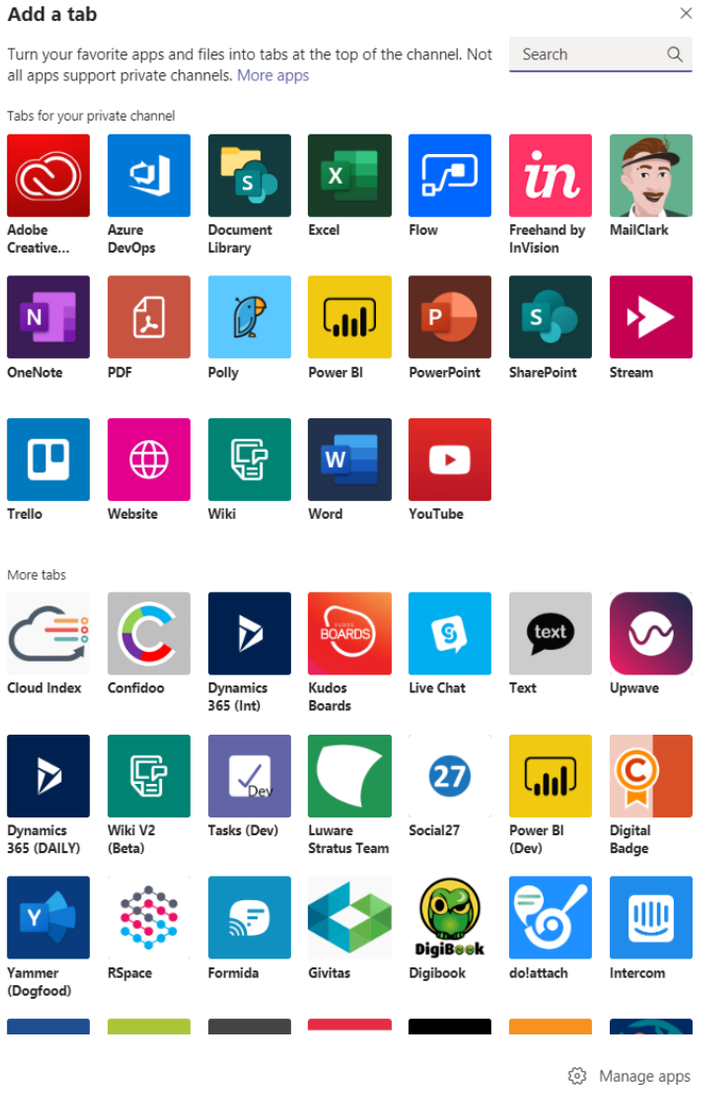
Private channel information	Team owner can see	Team members can see
Name and description	All private channels in the team	Only when added to the private channel
Conversations and tabs	Only when added to the private channel	Only when added to the private channel
Files and content	Only when added to the private channel	Only when added to the private channel

*Blocked from removing anyone who is the last owner of a private channel

Apps in private channels

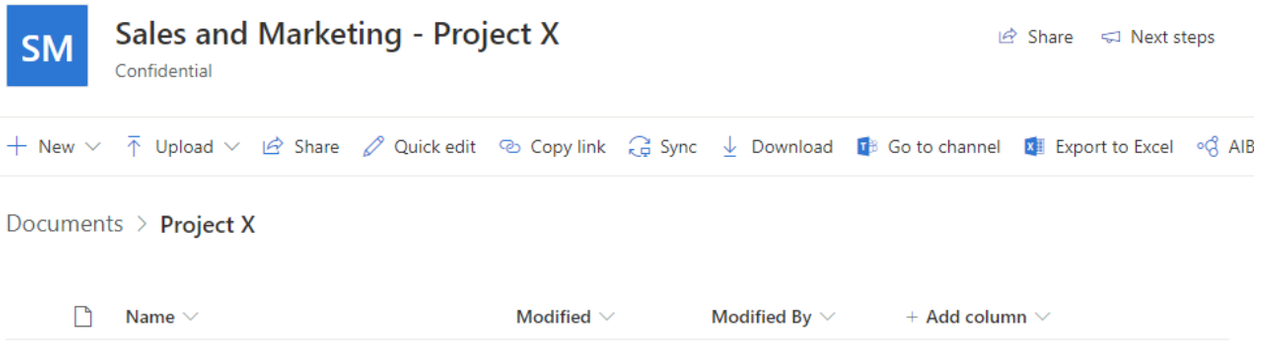
- Tabs and connectors supported
- Apps must be installed in the team before they can be used in a private channel

- Bots and message extension support coming later
- Support for certain Office 365 group connected apps like Planner coming later



Files in private channels

- **Private channel files are stored in its own site collection**
  - Ensures access to private channel documents is restricted to members
  - Site is named as <team name>-<channel name>
  - Comes with doclib, lists can be added, pages not supported
- **Lifecycle of the site collection is tied to private channel**
  - Site collection created in the same geo as team, inherits guest permission on create
  - Membership and data classification of the site collection is kept in sync with team
- **Site collections per tenant limit has been enhanced from 500K to 2M**



Site management

- **Management via PowerShell**
  - Filter by template “TeamChannel#0”
  - Sites hidden in the SharePoint admin center
- **Owner and member groups managed by Teams**
  - Any direct changes to these groups in SP will be synchronized with the private channel owner and members list
  - Use visitor or a new group if you need to grant users access to documents and not channel conversations

Get all sites backing private channels in tenant

```
Get-SPOSite -Limit ALL -Template "TEAMCHANNEL#0"
```

Default site membership groups and permissions

Name	Type	Permission Levels
Sales and Marketing - Project X Members	SharePoint Group	Contribute
Sales and Marketing - Project X Owners	SharePoint Group	Full Control
Sales and Marketing - Project X Visitors	SharePoint Group	Read

PowerShell & Graph API

- Create, list, update and delete private channels in a team
- Add, list, update, or delete members in a private channel

Channel creation

Graph API	PowerShell Commands
`POST /teams/{id}`	`New-TeamChannel`
`GET /teams/{id}/channels`	`Get-TeamChannel`
`PATCH /teams/{id}/channels/{id}`	`Set-TeamChannel`
`DELETE /teams/{id}/channels/{id}`	`Remove-TeamChannel`

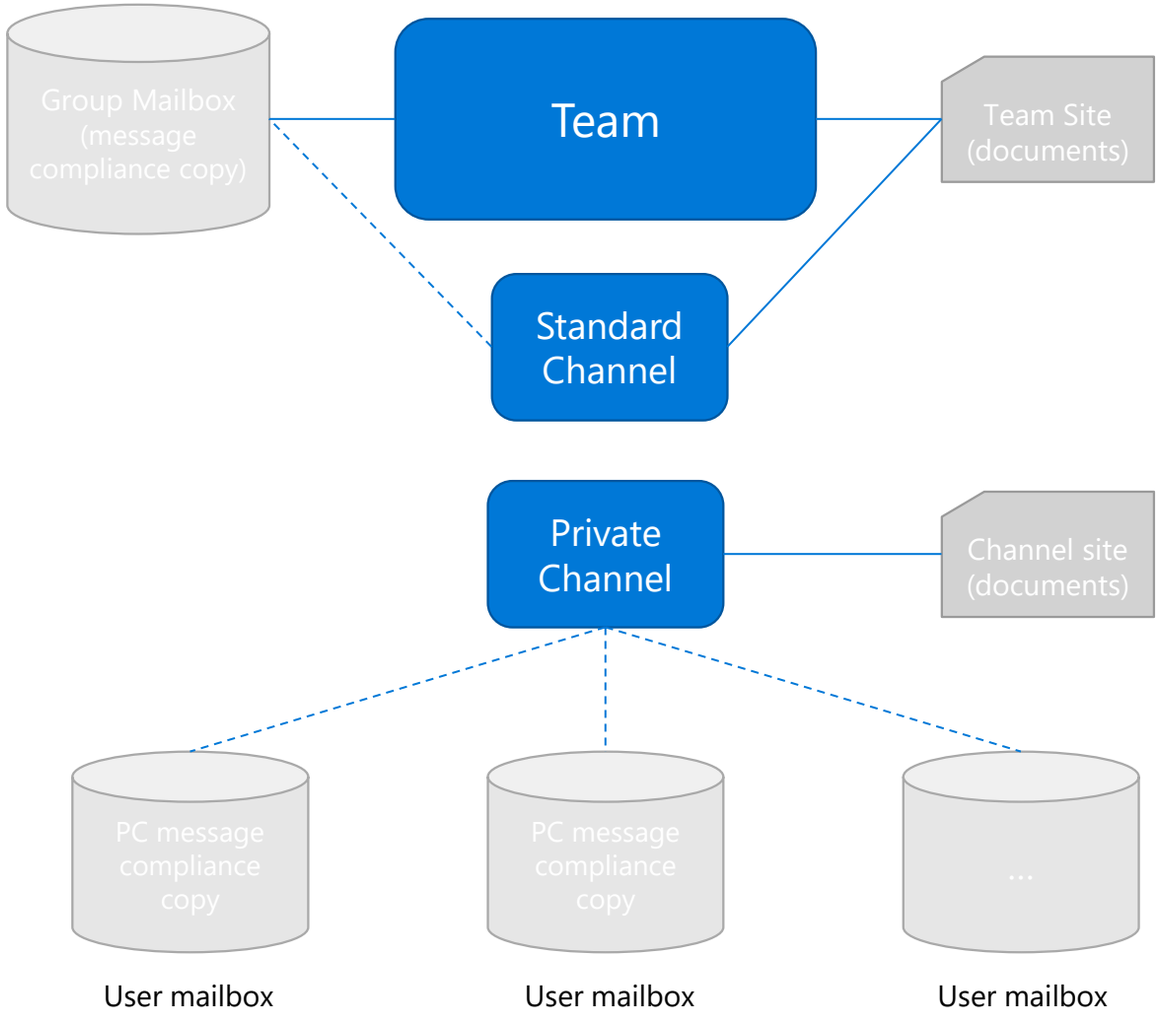
Channel membership

Graph API	PowerShell Commands
`POST /teams/{id}/channels/{id}/members`	`Add-TeamChannelUser`
`GET /teams/{id}/channels/{id}/members`	`Get-TeamChannelUser`
`PATCH /teams/{id}/channels/{id}/members`	`Remove-TeamChannelUser`
`DELETE /teams/{id}/channels/{id}/members`	

Information Protection

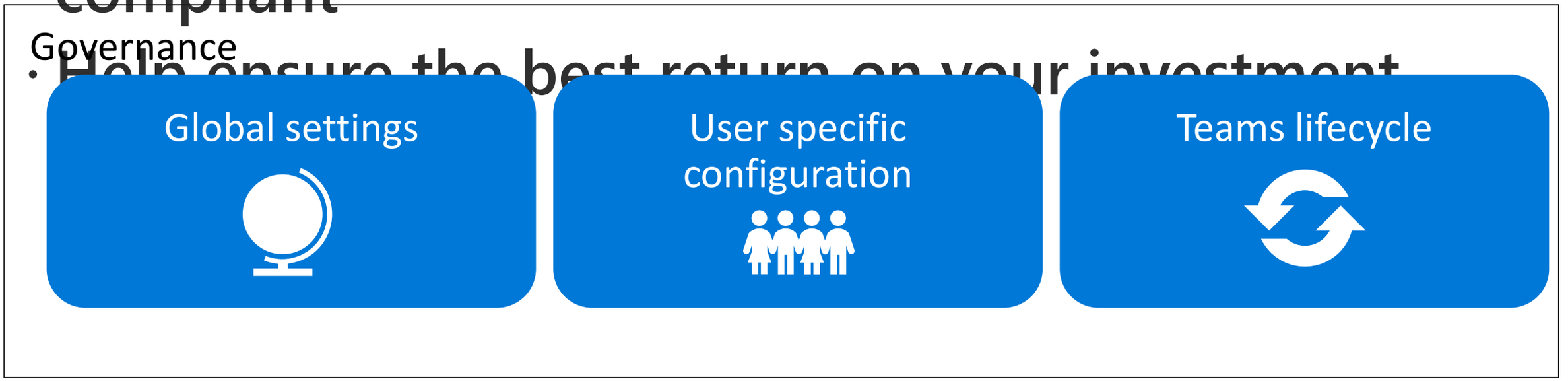
- **eDiscovery support for channel messages and documents**
  - Include private channel member mailboxes and SP site collection in discovery query
- **Retention support for private channel documents**
  - Default retention policy for sites apply, manage via PowerShell
  - Retention support for private channel messages coming later

eDiscovery, Retention & Hold on group (team) does not automatically apply to private channels in the team



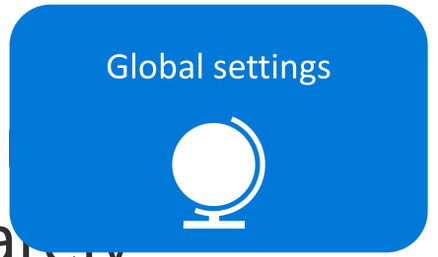
Team Governance

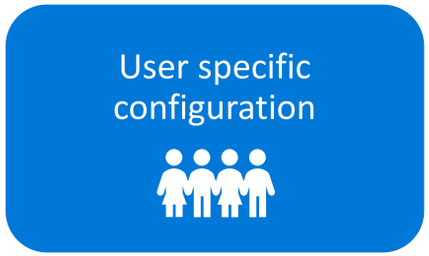
- Streamline the deployment of products and technologies, such as Teams
- Help keep your organization's system secure and compliant
- Help ensure the best return on your investment



Configuration vs. Lifecycle

- **Configuration of Teams**
  - Global settings and user specific configuratio
  - Considered “static”: once defined, changed rarely
  - Defined and configured by admin
- **Lifecycle of teams**
  - Each individual team has own lifecycle: Initiate, active, sunse
  - Configured by team owner or admin

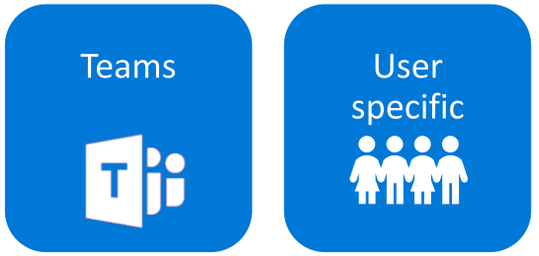




Where do I configure it?
Who does it apply to?

Where a setting is configured?	Can it be user specific or is it global?
Teams, Groups setting, Security & compliance	Global settings, User specific, Groups

Role Based Access Control



- Allows setting administrators who need different levels of access for managing Teams

Rolle	Can do these tasks
Teams Service Administrator	Manage the Microsoft Teams service, and manage and create Office 365 Groups
Teams Communications Administrator	Manage calling and meetings features within the Microsoft Teams service
Teams Communications Support Engineer	Troubleshoot communications issues within Teams by using **advanced** tools.
Teams Communications Support Specialist	Troubleshoot communications issues within Teams by using **basic** tools.

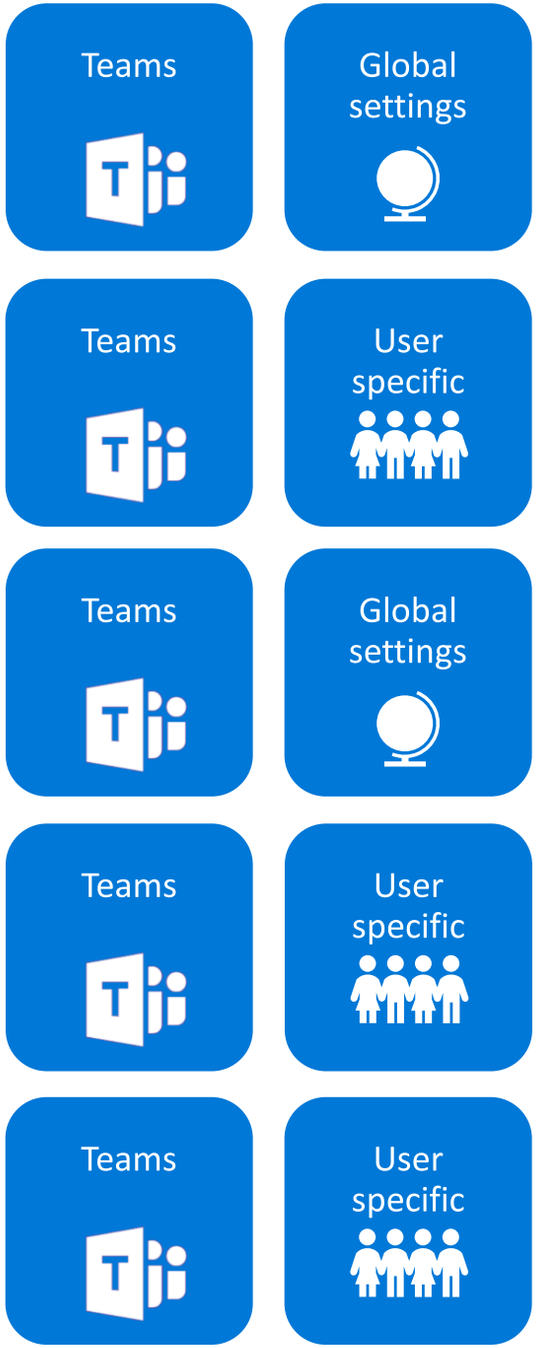
Teams settings

Messaging policies

Meeting settings

Meeting policies

Live events policies



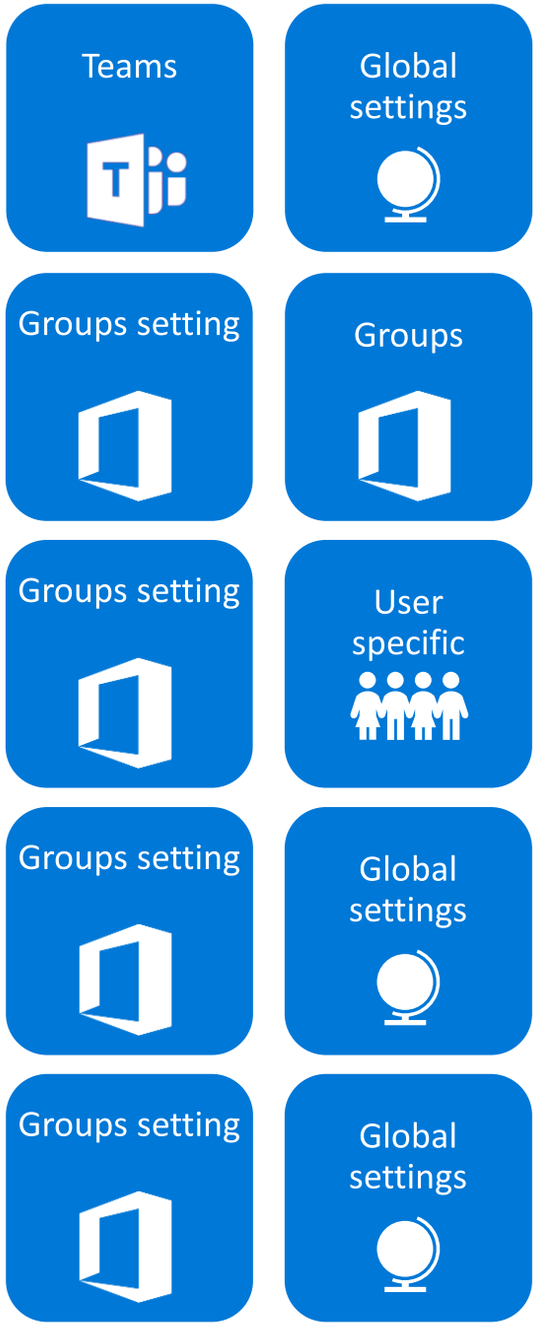
External access

Guest access

Allow Team Creation

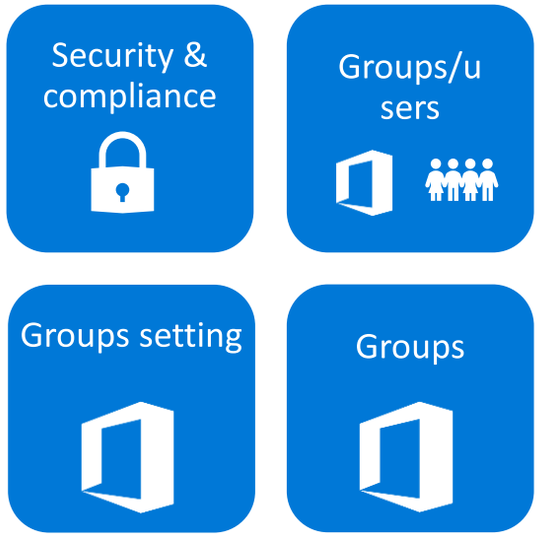
Naming of teams

Classification



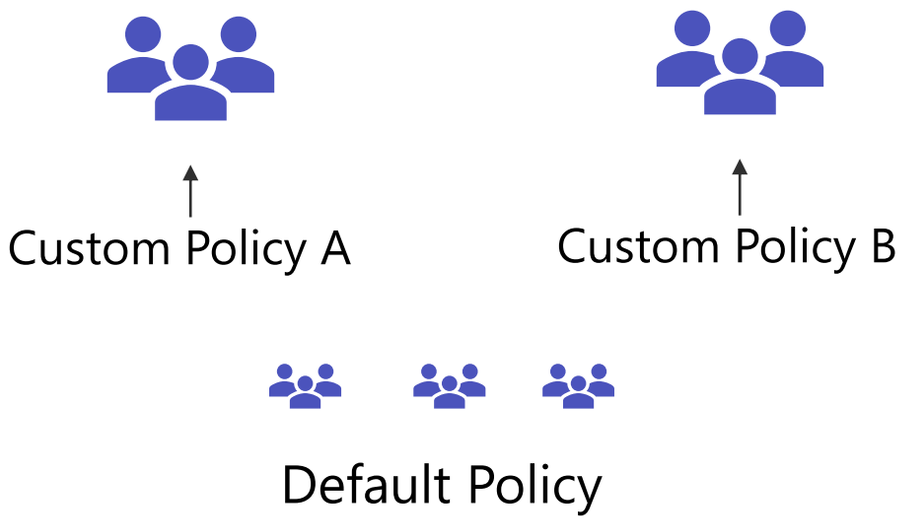
Retention policies

Expiration policies



Microsoft Teams Policy model

Policies can apply across whole organization (Global/Default) or assigned to individual users. Unless there's a separate configuration, guest users in your organization always get the Default policy.



Microsoft

Manage Teams Apps

Apps In Teams

1st Party Apps

- Developed by Microsoft
- Office 365 or Office workloads
- Enable better together scenarios

3rd Party Apps

- Not built by Microsoft
- Popular work applications
- Enabled in central location

Custom Apps

- Built by your organization
- Custom for business needs
- Accessible by users in Teams

New ways to manage apps

Enable

App permission policies and org-wide settings

Available

Block or allow apps, either org-wide or for specific user

Disable interactions with specific apps

Side loading policies

Available

Control which users can upload custom apps to teams

Org-wide setting for interactions with custom apps

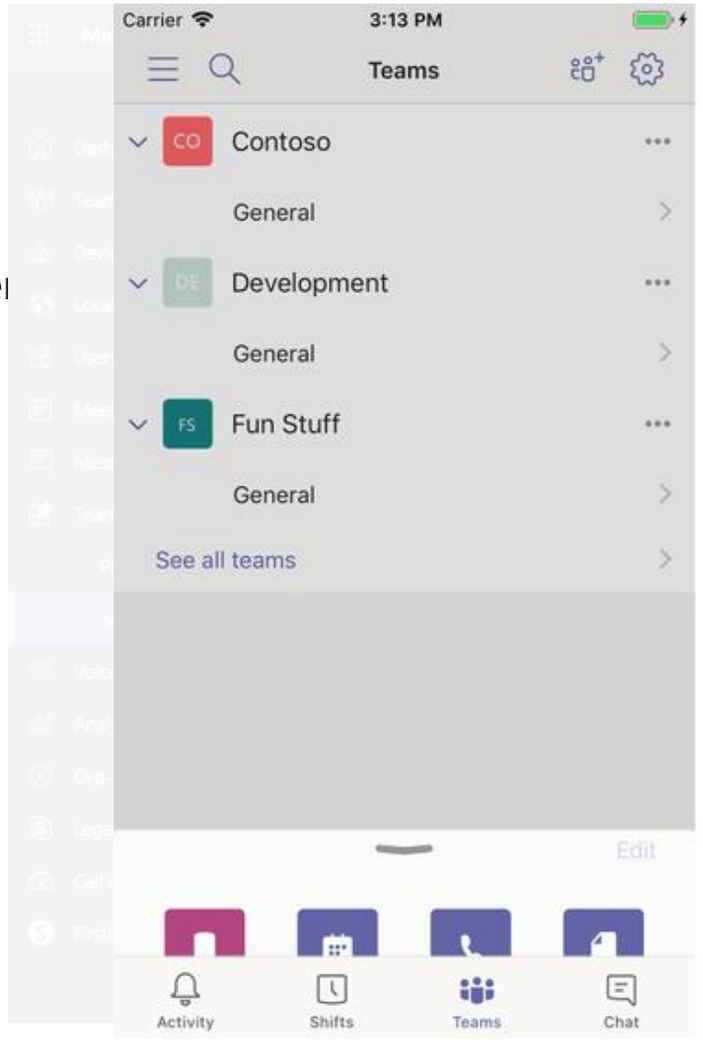
App setup policies

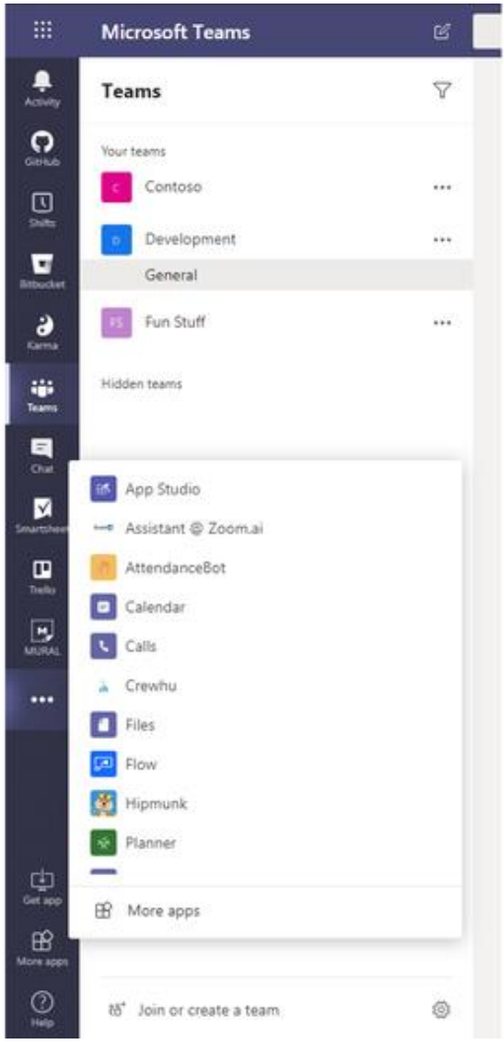
Available

Customize your users' app experience

Choose the apps that you want to pin to the app bar

Promote





Assign a custom app setup policy to users in a group

Get the GroupObjectId of the particular group.

```
$group = Get-AzureADGroup -SearchString "Contoso Pharmaceuticals HR Project"
```

Get the members of the specified group.

```
$members = Get-AzureADGroupMember -ObjectId $group.ObjectId -All $true | Where-Object {$_.ObjectType -eq "User"}
```

Assign all users in the group to a particular app setup policy. In this example, it's HR App Setup Policy.

```
$members | ForEach-Object { Grant-CsTeamsAppSetupPolicy -PolicyName "HR App Setup Policy" -Identity $_.EmailAddress}
```

Depending on the number of members in the group, this command may take several minutes to execute.

Close

Next Steps…..

Link to Today’s Slides:
https://aka.ms/mclass-presentation

Survey:
https://aka.ms/mclass-survey

Teams 101 Click Through Labs

- Managing Teams and Guest Access (immersivelearning.online)

In this exercise, we will be managing teams in the Contoso corporation. Including creating a team and its owners, setting policies for team members, and configuring and setting guest access policies.

- Configure Governance in Microsoft Teams (immersivelearning.online)

In this exercise, we will be creating a Teams messaging retention policy for the Contoso company that excludes a subset of users. We will also learn how to archive, delete and restore a team.

- Teams Security (immersivelearning.online)

In this Interactive Guide – we will focus on (1) identity and access management and (2) threat protection for Microsoft Teams. In the lab you will Configure conditional access policy to require Multi-Factor Authentication (MFA) for Microsoft Teams, Enable Office 365 Advanced Threat Protection (ATP) for Teams by configuring ATP Safe Attachments, Configure Microsoft Teams settings and policies to control access to messages, apps, meetings and files.

- Teams compliance (immersivelearning.online)

After completing this lab, you will be able to: Create and apply sensitivity labels to Teams,

Create and monitor a new sensitive info type with Communication Compliance, Create a new data loss prevention (DLP) policy, Create an information barrier policy

Upcoming 101 Events

Voice and Meetings When: Thursday, March 17, 2022

https://msevents.microsoft.com/event?id=3256377873

Platform Customisation Tuesday, March 22, 2022

https://msevents.microsoft.com/event?id=1272363986

Viva Thursday, March 24, 2022

https://msevents.microsoft.com/event?id=3719085570

Lab and Break