

Microsoft Teams Virtual Event

Teams 101!

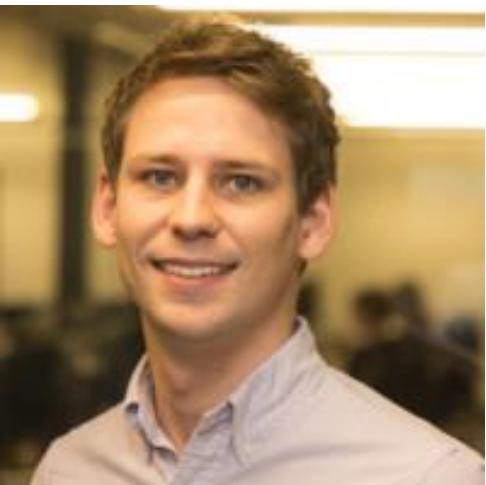


Introductions



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>

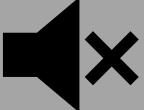
Viva Thursday, March 24, 2022

<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 Policies
 - Meeting Policies
 - Application Policies
- 1245 Any Remaining Q&A
- 1300 Close

Teams 101

Introduction

Microsoft Teams

is the hub for teamwork in Microsoft 365



Chats



Meetings



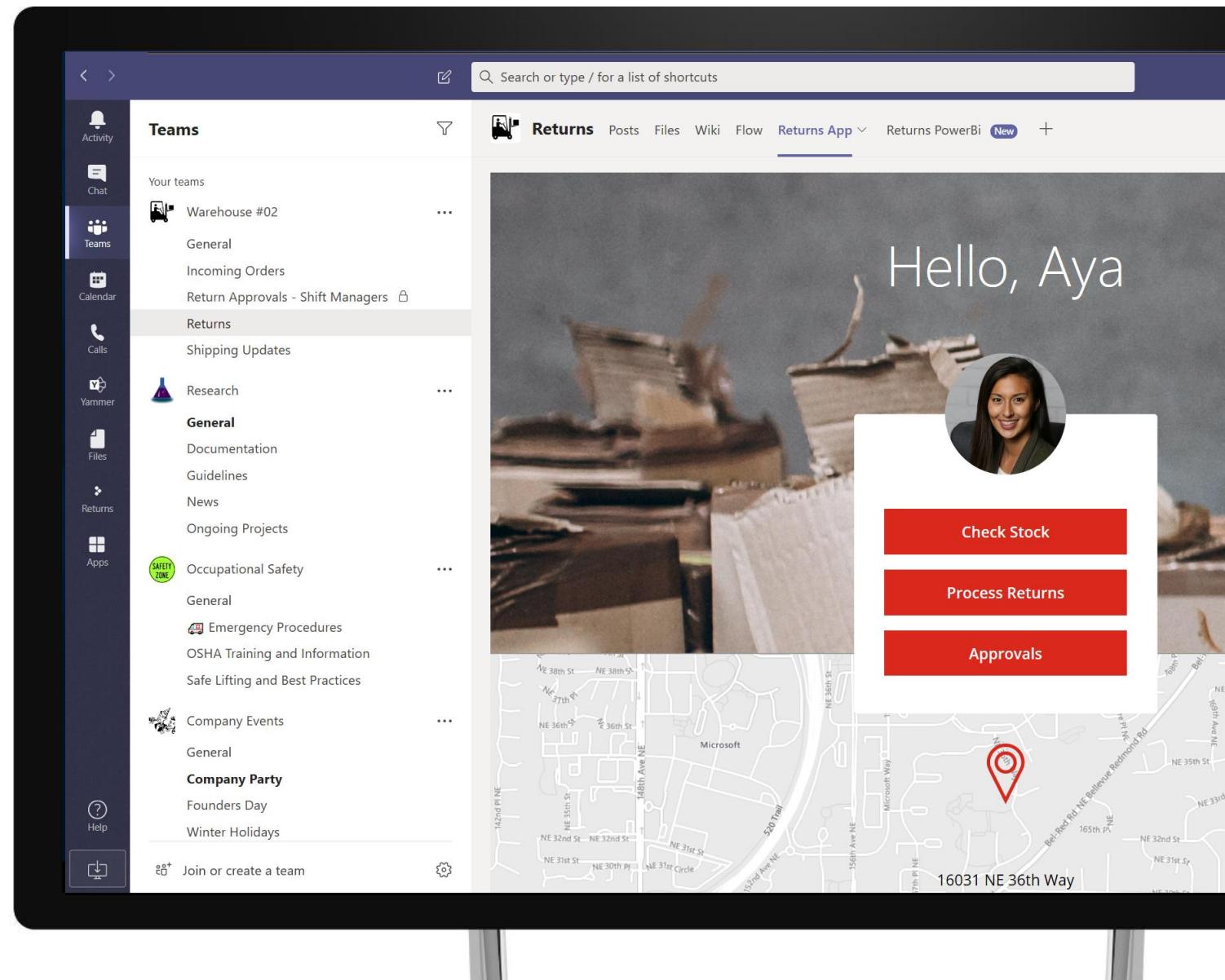
Calls



Files



Apps and workflows



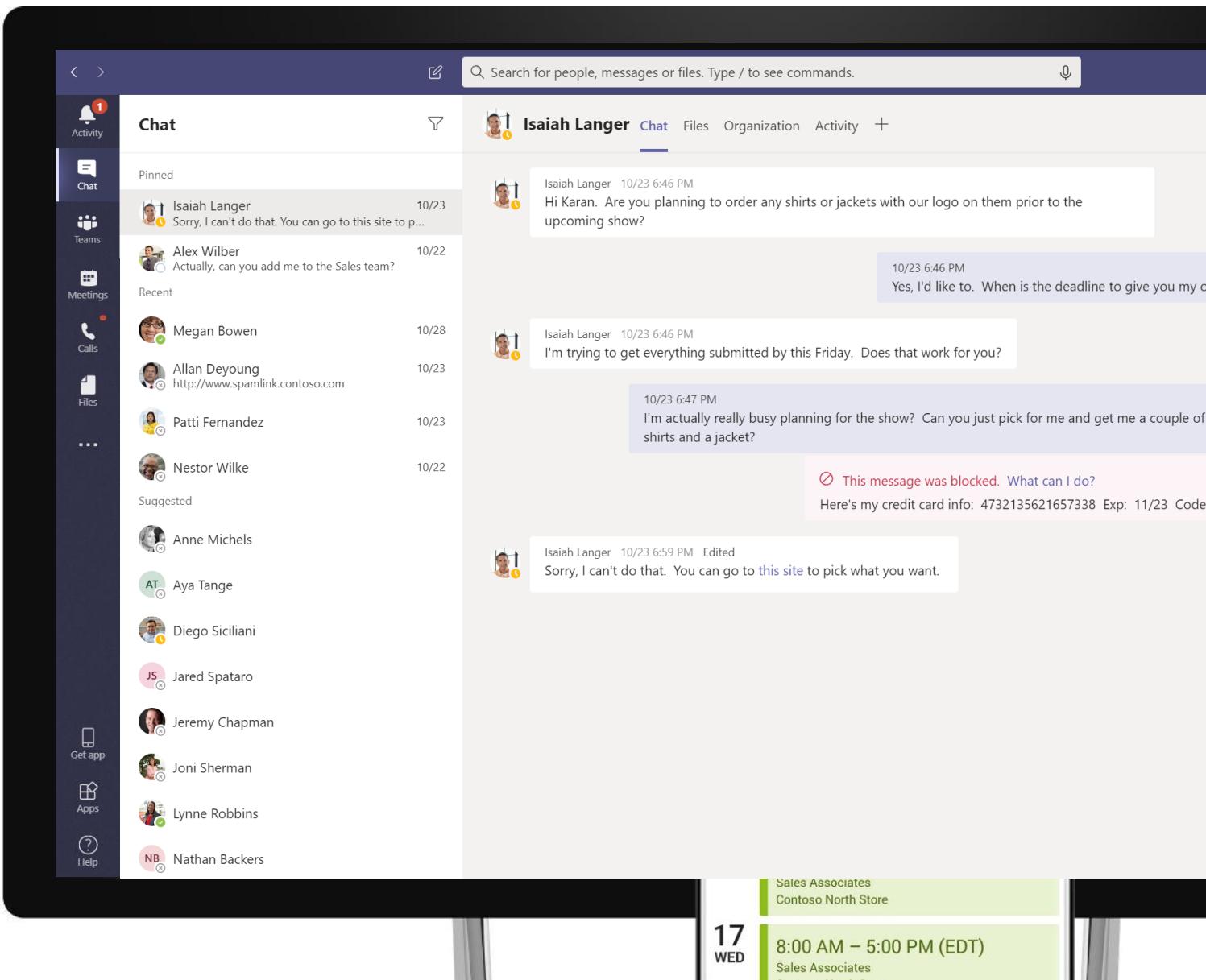
What can Teams do for your business

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



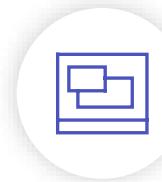
500,000+

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

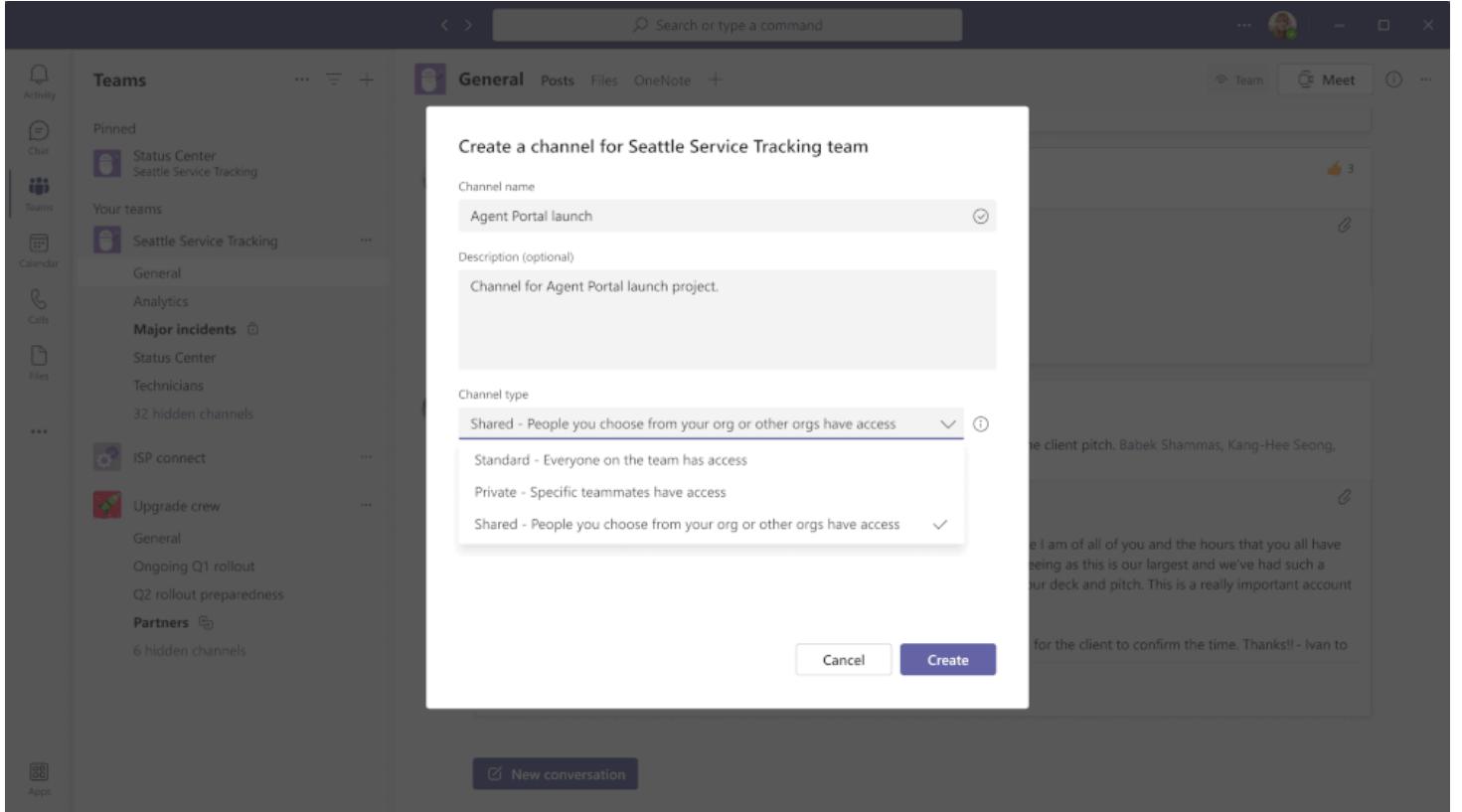
[Build apps for Microsoft 365](#)



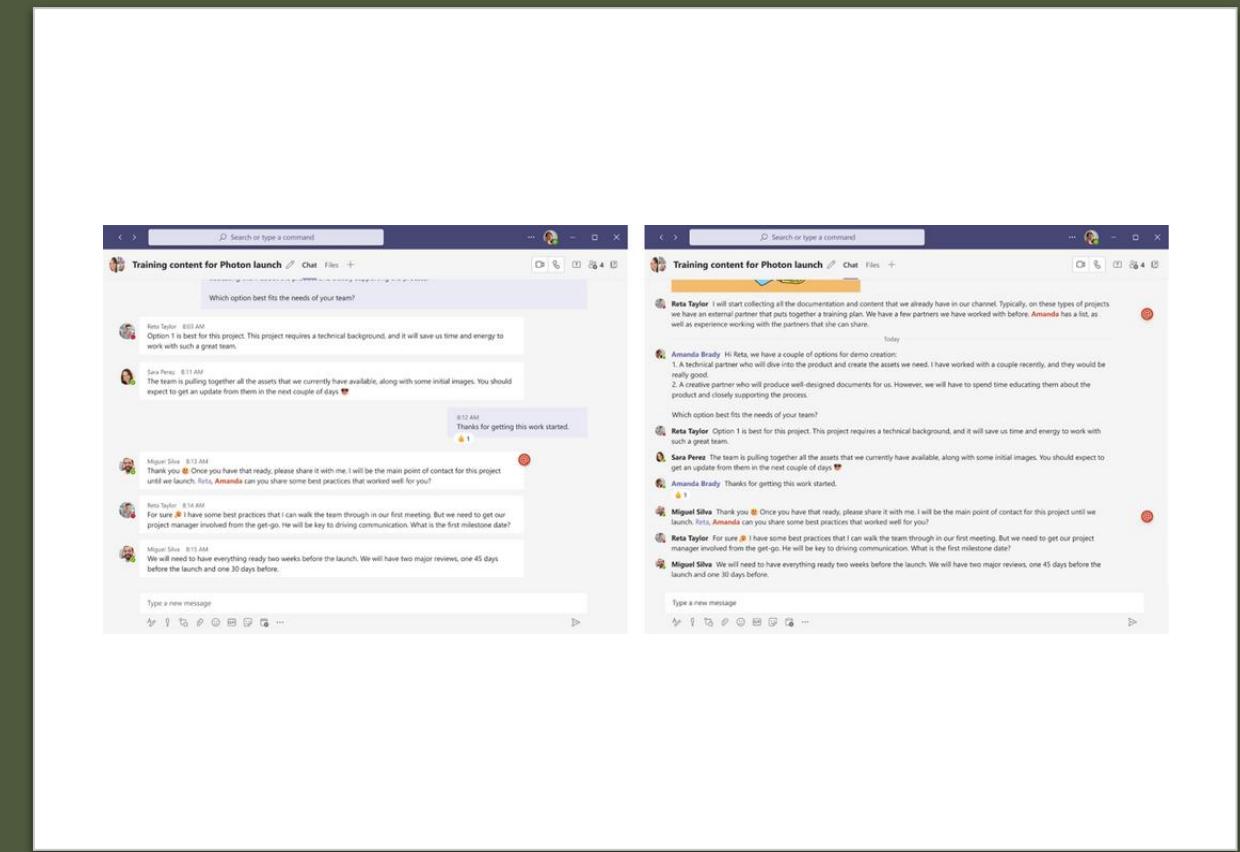
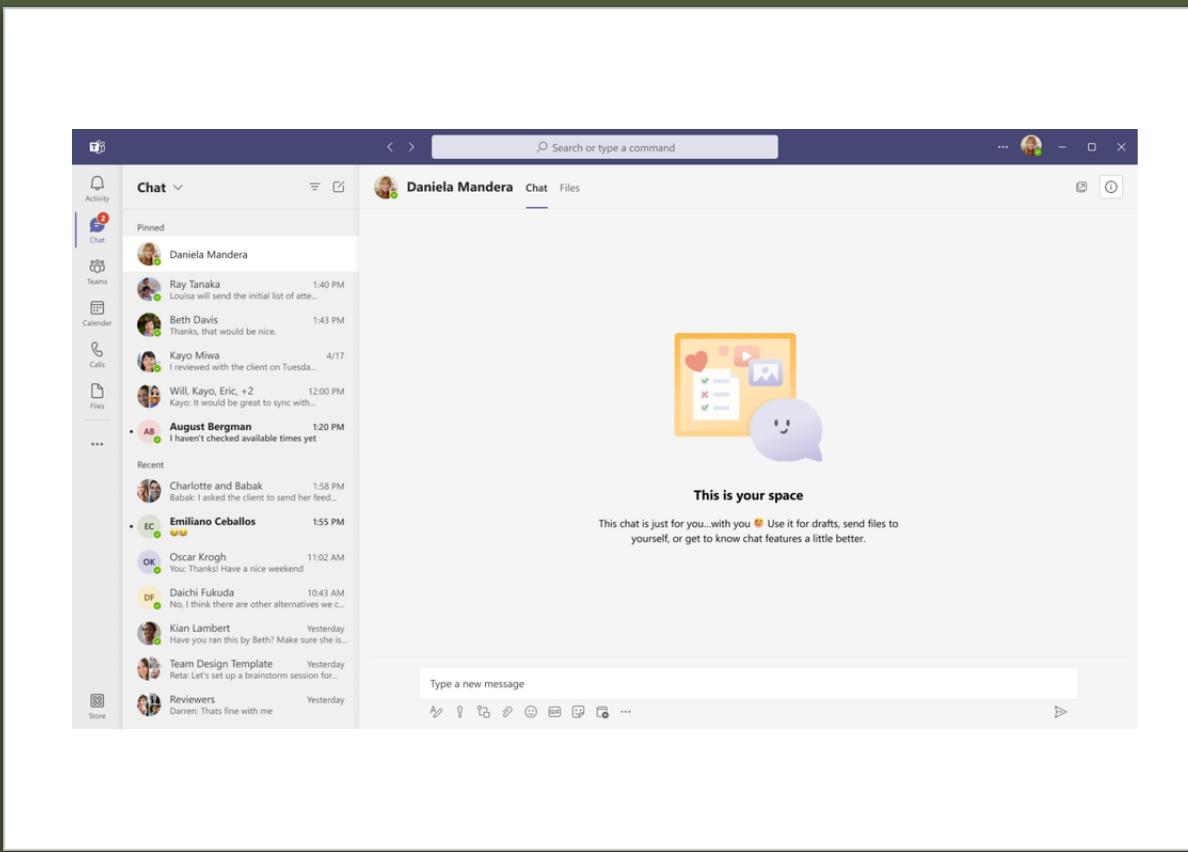
What's new at Ignite 2021?

Available now or coming soon

Teams Connect



New Chat, People and Presence features



New Chat, People and Presence Features

The image displays two side-by-side screenshots of the Microsoft Teams Chat interface, illustrating the "New Chat, People and Presence Features".

Left Screenshot: Shows a channel named "Training content for Photon launch". The conversation includes messages from Sarah Perez, Ray Tanaka, Beth Davis, Kayo Miwa, Will, Kayo, Eric, +2, August Bergman, and Reta Taylor. A pinned message from Amanda Brady is visible. A cartoon illustration of a character shouting "GREAT JOB" is included in the thread.

Right Screenshot: Shows the same channel. It highlights a message from Miguel Silva (@Sarah) stating, "Sarah, that's great! This means Photon is on track to launch in 3 months." Below this message is another cartoon illustration of a character shouting "GREAT JOB". A message from Reta Taylor follows, detailing her plan to start collecting documentation. A dropdown menu for sending the message is open, showing options: "Send now" (selected), "1 PM", "Tomorrow", "8 AM", "Next Mon, May 3", "8 AM", and "Custom".

Dynamics/Teams Process Improvements

Dynamics 365 Opportunities dashboard showing a deal tracker and sales funnel.

Key metrics displayed:

- Total deals: 45
- Number of deals in pipeline: 35
- Number of won deals: 27
- Number of lost deals: 11
- Pipeline value: \$330.55K
- Won amount: \$251.55K

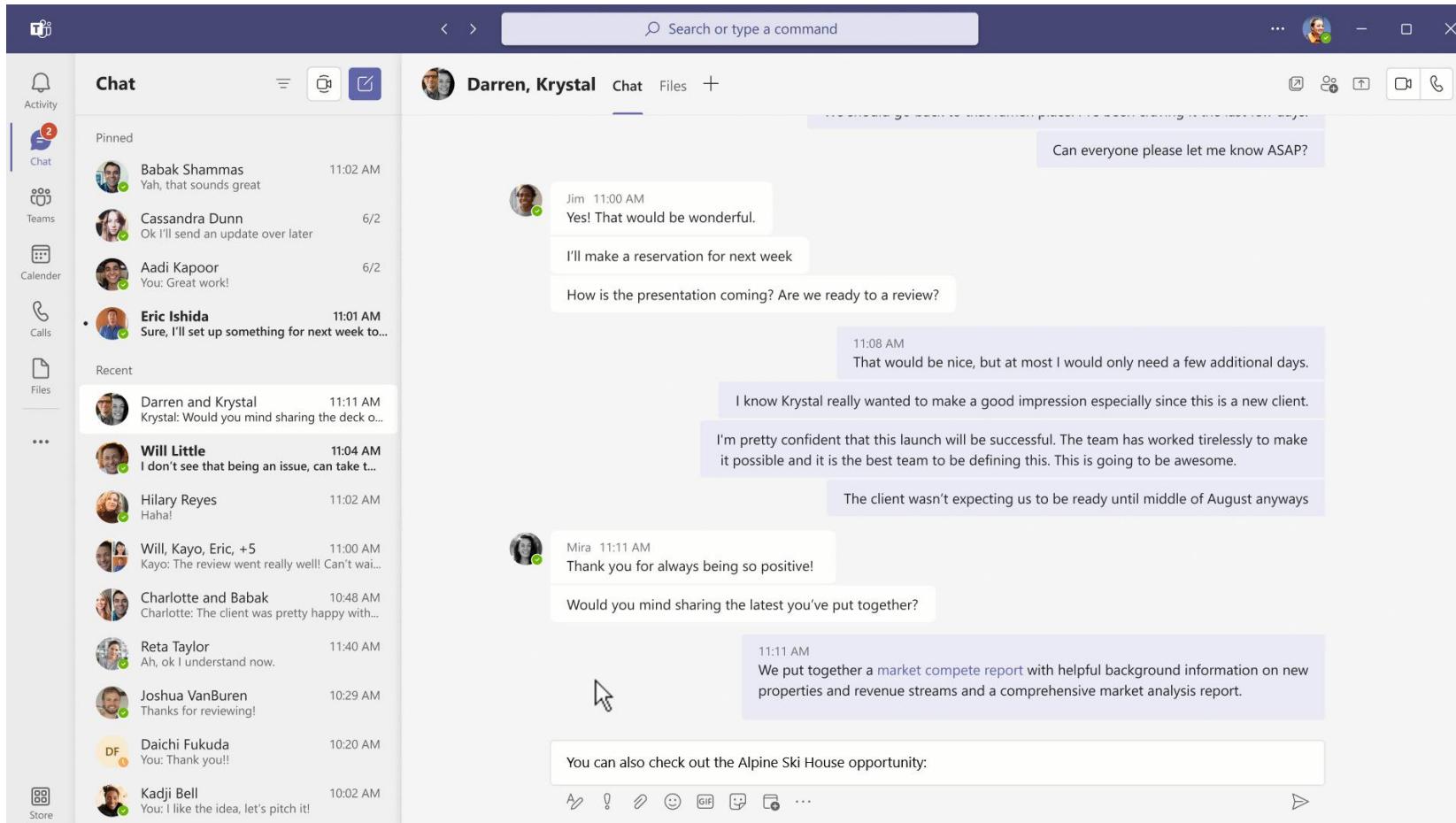
The deal tracker shows opportunity score (Y-axis, 0-100) versus close date (X-axis, 4/20/20 to 9/20/20). Opportunities are categorized by grade: Grade A (80-100), Grade B (50-80), Grade C (30-50), Grade D (20-0), and Closed.

Recent activity in the Microsoft Teams channel:

- Madelyn Gilliam: You too! 8:14 AM
- Contoso, Ltd.: Hiram: I've been engaging with our contact... 8:30 PM
- Georgette Bray: You: Thanks! Have a nice weekend 2:06
- Bowers, Melva (Guest): You: Thanks! Have a nice weekend 2:00
- Suggested chats + contacts: Suggested
- Samuel Weeks: Start chatting with active member of Sales T... 8:30 AM
- Alpine Q2 Renewal Opportunity: Continue chat with active members 8:30 AM
- Alonzo Chapman: Start chat with recently added to the Timeline 8:30 AM
- Recent: Kristine Mitchell: You: Thanks! Have a nice weekend 8:23 AM
- Lelia Dawson: You: I lost the marketing content, could you... 8:19 AM
- Patrick Powers: You: Sounds great, thank you Karry! 7:18 AM
- ASH Q3 Sales Opportunity: Bart: Just made that call today! 6:49 AM
- Reyna Holman: You: Thanks! Have a nice weekend 6:30
- Sherri Pollard: You: Where are we with the Fabrikam deal t... 6:29

Message input field: Type a new message

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

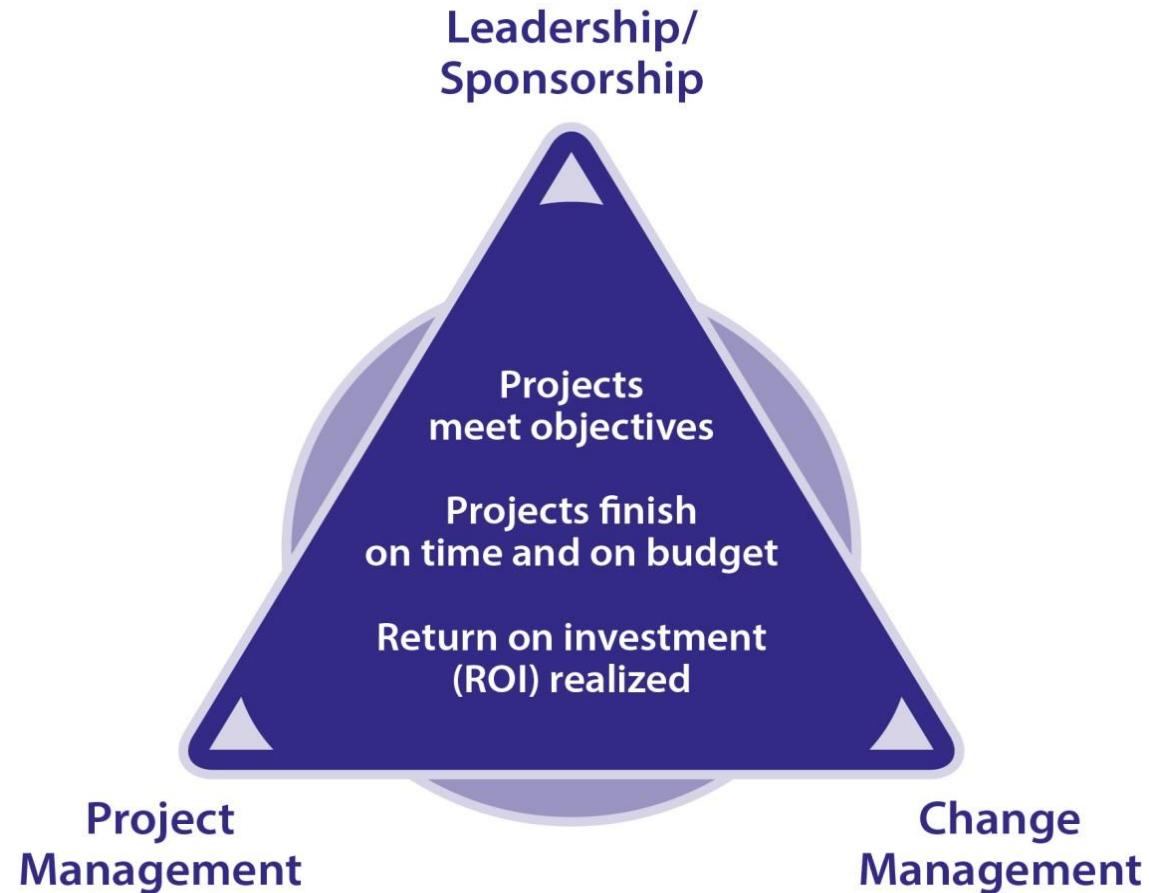
45,000+

Certified Practitioners

100,000+

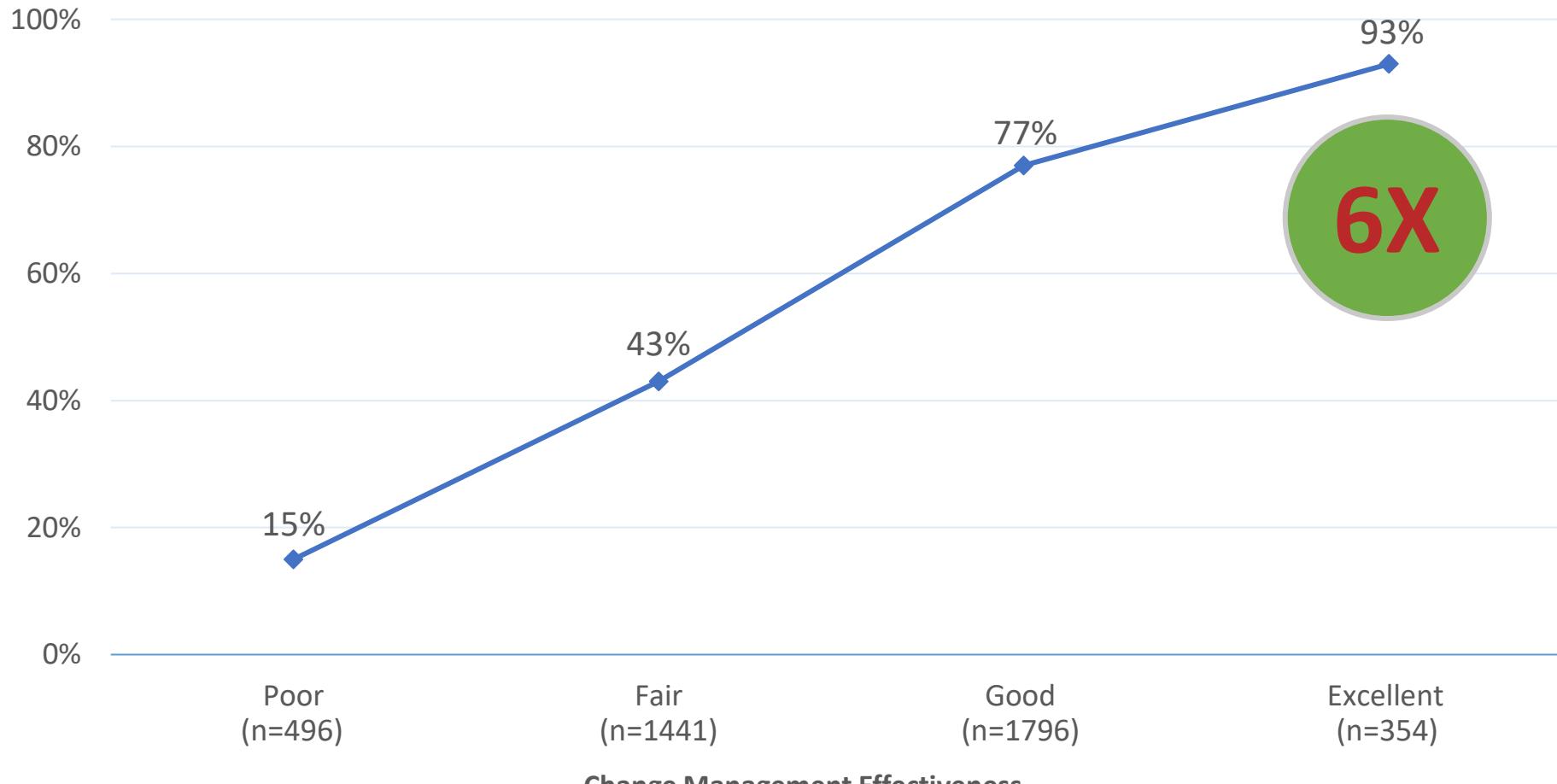
Community Members

Applied to Your Project Prosci® PCT™ Model



Data Supports the Connection

Percent of Study Participants Who Met or Exceeded Objectives



Prosci 2018 Benchmarking Data

Data from 2007, 2009, 2011, 2013, 2015, 2017

Change Management Effectiveness

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>

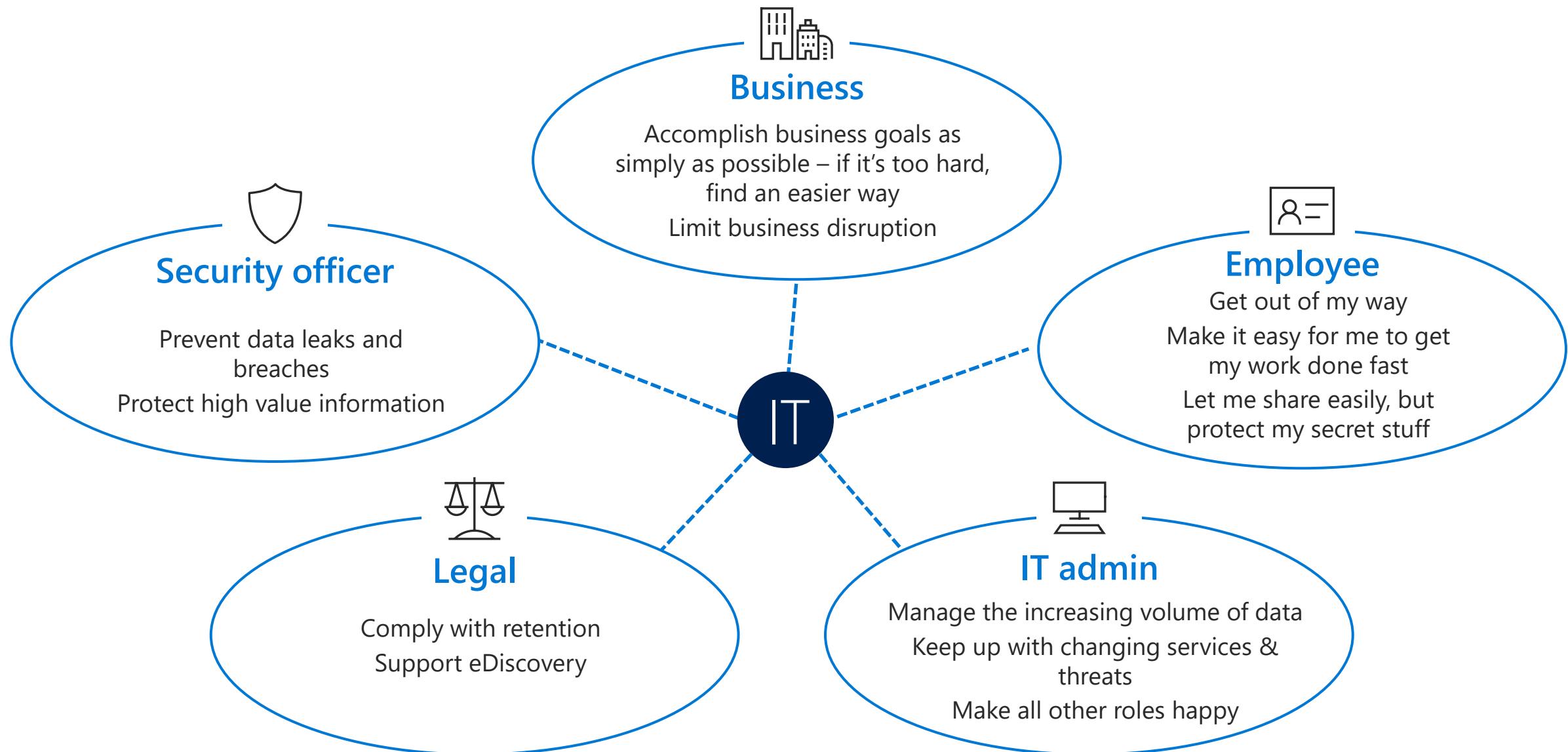
Platform Customisation Tuesday, March 22, 2022

<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	Microsoft 365 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

Licensing Considerations

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

Microsoft 365 E5 Compliance
Pre-req: M365 E3/A3 or Office 365 E3/A3 + EMS E3/A3

M365 E5 Info Protection & Governance Information Protection and Governance: <ul style="list-style-type: none">• Records Management• Machine Learning-based automatic classification and retention• Rules-based automatic classification and retention Defender for Cloud Apps DLP for Teams chat (Communications DLP) Endpoint DLP Customer Key Advanced Message Encryption Pre-req: Any M365 plan or [any Office 365 plan] + Azure Info Protection Plan 1/EMS	M365 E5 Insider Risk Management Insider Risk Management Communication Compliance Information Barriers Customer Lockbox Privileged Access Management Pre-req: Any M365 or Office 365 plan	M365 E5 eDiscovery and Audit Advanced Audit Advanced eDiscovery Pre-req: Any M365 or Office 365 plan
---	---	--

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

Provisioning

How information access and containers are managed

Operations

How to retain/expire/dispose of information as appropriate

Information Lifecycle

What are Microsoft 365 Groups?

Single identity for teamwork and beyond



**Microsoft 365
Groups**



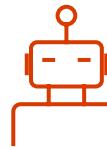
Membership service for M365 teamwork apps

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>
```

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

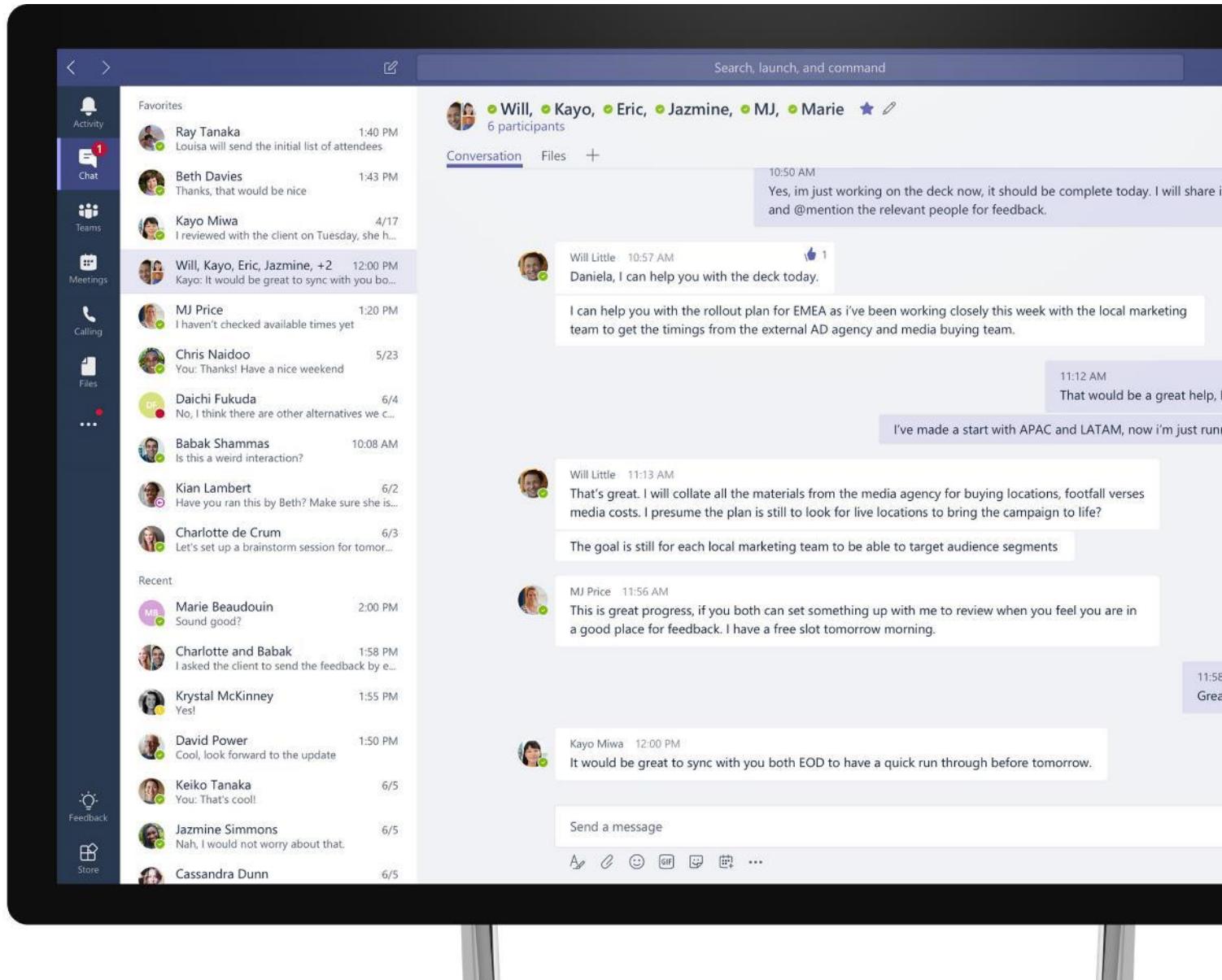
[Create a team from an existing team](#)
(microsoft.com)

[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	<code>https://graph.microsoft.com/beta/teamsTemplates('standard')</code>	No additional apps and properties
Education - Class Team	<code>https://graph.microsoft.com/beta/teamsTemplates('educationClass')</code>	<p>Apps:</p> <ul style="list-style-type: none">• OneNote Class Notebook (pinned to the General tab)• Assignments app (pinned to the General tab) <p>Team properties:</p> <ul style="list-style-type: none">• Team visibility set to HiddenMembership (cannot be overridden)
Education - Staff Team	<code>https://graph.microsoft.com/beta/teamsTemplates('educationStaff')</code>	<p>Apps:</p> <ul style="list-style-type: none">• OneNote Staff Notebook (pinned to the General tab)

The screenshot shows the Microsoft Teams Admin Center interface. On the left is a navigation sidebar with options like Dashboard, Teams, Manage teams, Teams policies, and Team templates (which is currently selected). The main content area is titled "Team templates". It contains a brief description: "Team templates are pre-built definitions of a team's structure designed around a business need or project. You can create a template using the Teams client, then upload and manage the templates stored in your organization. These templates can be assigned to a specific group using team policies." Below this is a table listing several pre-built team templates:

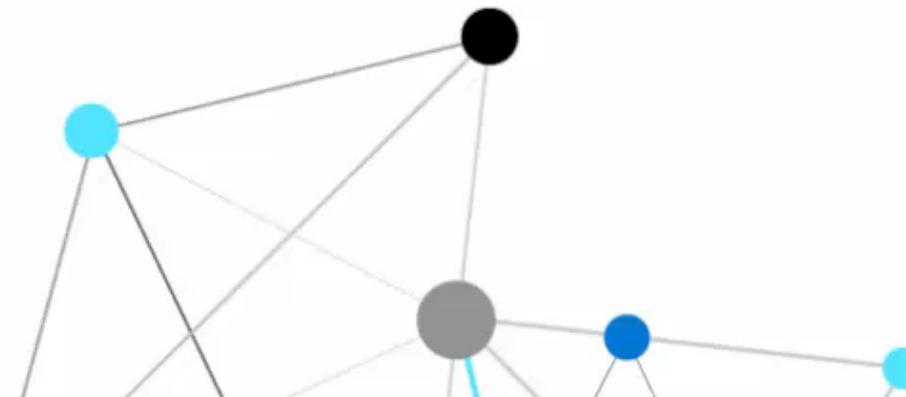
Name	Description
Create a Marketing Event	Helps Contoso Marketing create event teams.
Adopt Office 365	Help build, grow, and sustain your Champions community rollout by evangelizing and helping your peers with the new technology.
Manage a Project	Manage tasks, share documents, conduct project meetings and document risks and decisions with this template for general project.
Manage an Event	Manage tasks, documents and collaborate on everything you need to deliver a compelling event. Invite guests users to have secure.
Onboard Employees	Improve your culture and streamline your employee onboarding with this central team for resources, questions and a bit of fun.
Organize Help Desk	Collaborate on documentation, policy and processes that support your helpdesk. Integrate your existing ticketing system or use ou.
Collaborate on Patient Care	Streamline healthcare communication and collaboration within a ward, pod, or department. The template can be used to facilitate p.



Microsoft Teams

Automating the Team Creation Process

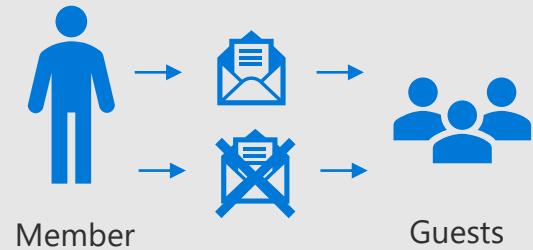
#MicrosoftEmployee



External Access Considerations

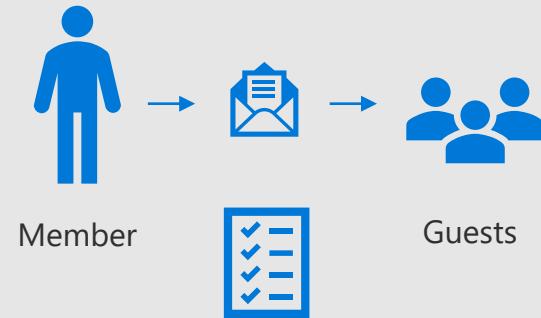
Group Level

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



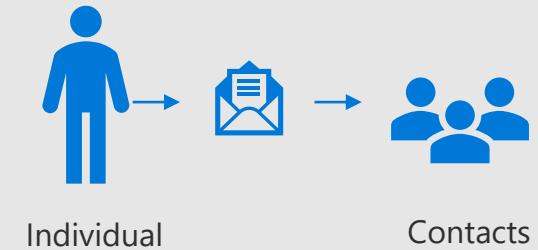
Guest Collaboration

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.

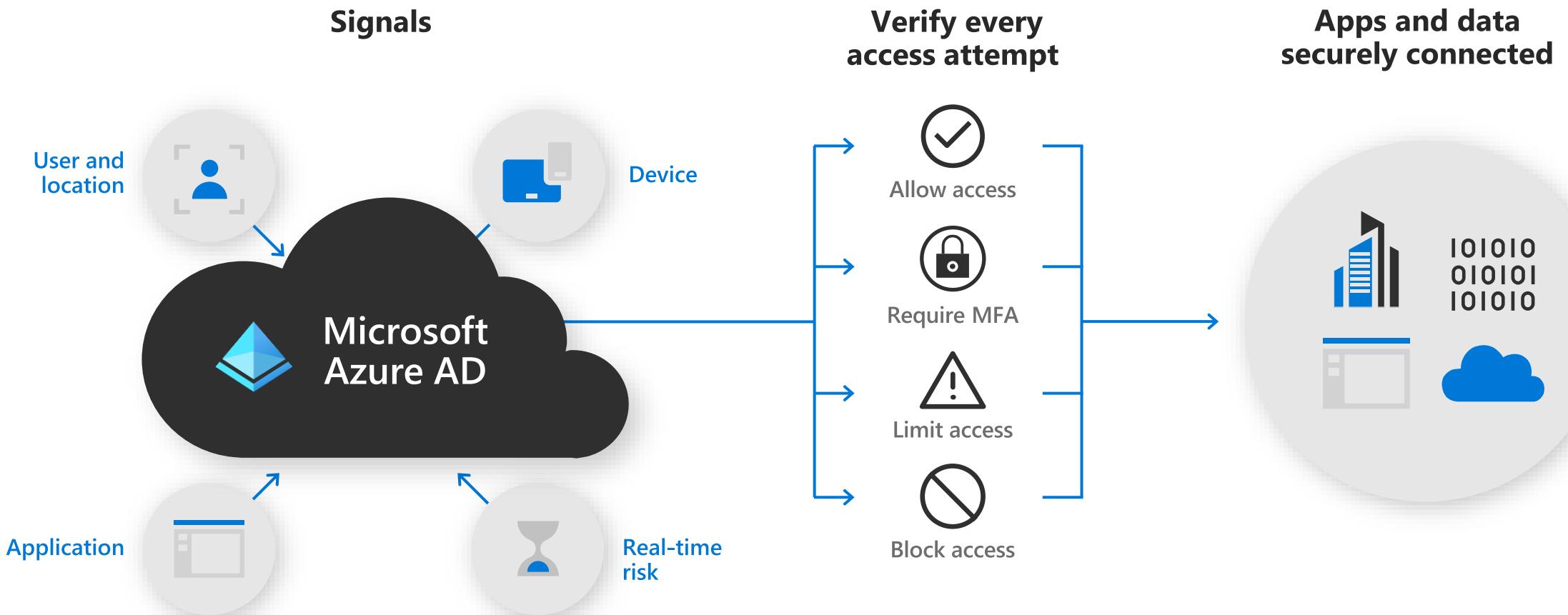


[Manage external access \(federation\) - Microsoft Teams | Microsoft Docs](#)

[Collaborate with guests in a team | Microsoft Docs](#)

Protect access for any user from anywhere

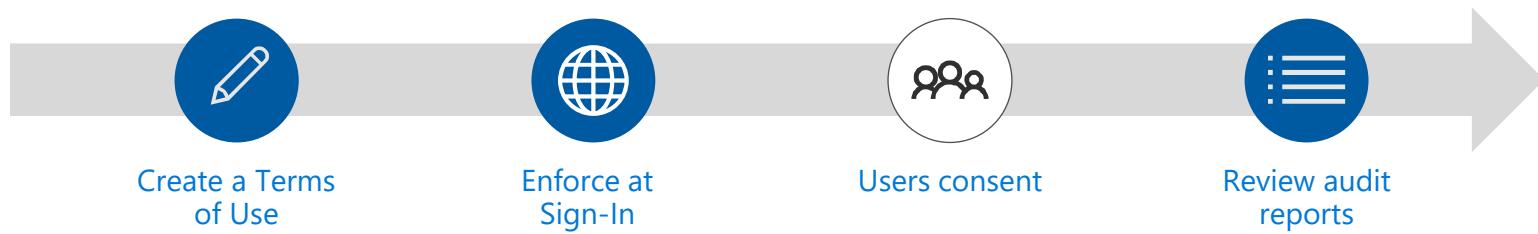
Apply consistent risk-based policies with Conditional Access.



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



New terms of use X

Terms of use
Create and upload documents

* Name
Example: 'All users terms of use'

* Display name ?
Example: 'Contoso Terms of Use'

* Upload document
Select a file Browse

Conditional access
Enforce Terms of use with policy templates

Create a policy ?

Policy templates
Access to cloud apps - Enforced for all us... ▼

Privacy policy for personal device registration

In order to update your self-service password reset details you will need to accept the following Terms of Use.

Microsoft Teams

Guest Access MFA & TOU

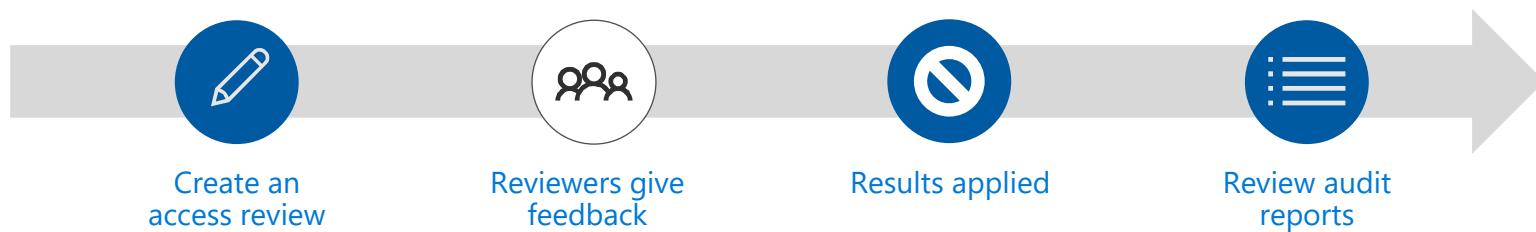
#MicrosoftEmployee



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



Create an access review

Access reviews enable reviewers to attest user's membership in a group or access to an application

* Review Name: MSOS Q2 guests self review

Description: (empty)

* Start date: 2017-09-07

* End date: 2017-10-01

Users

* Users to review: Members of a group

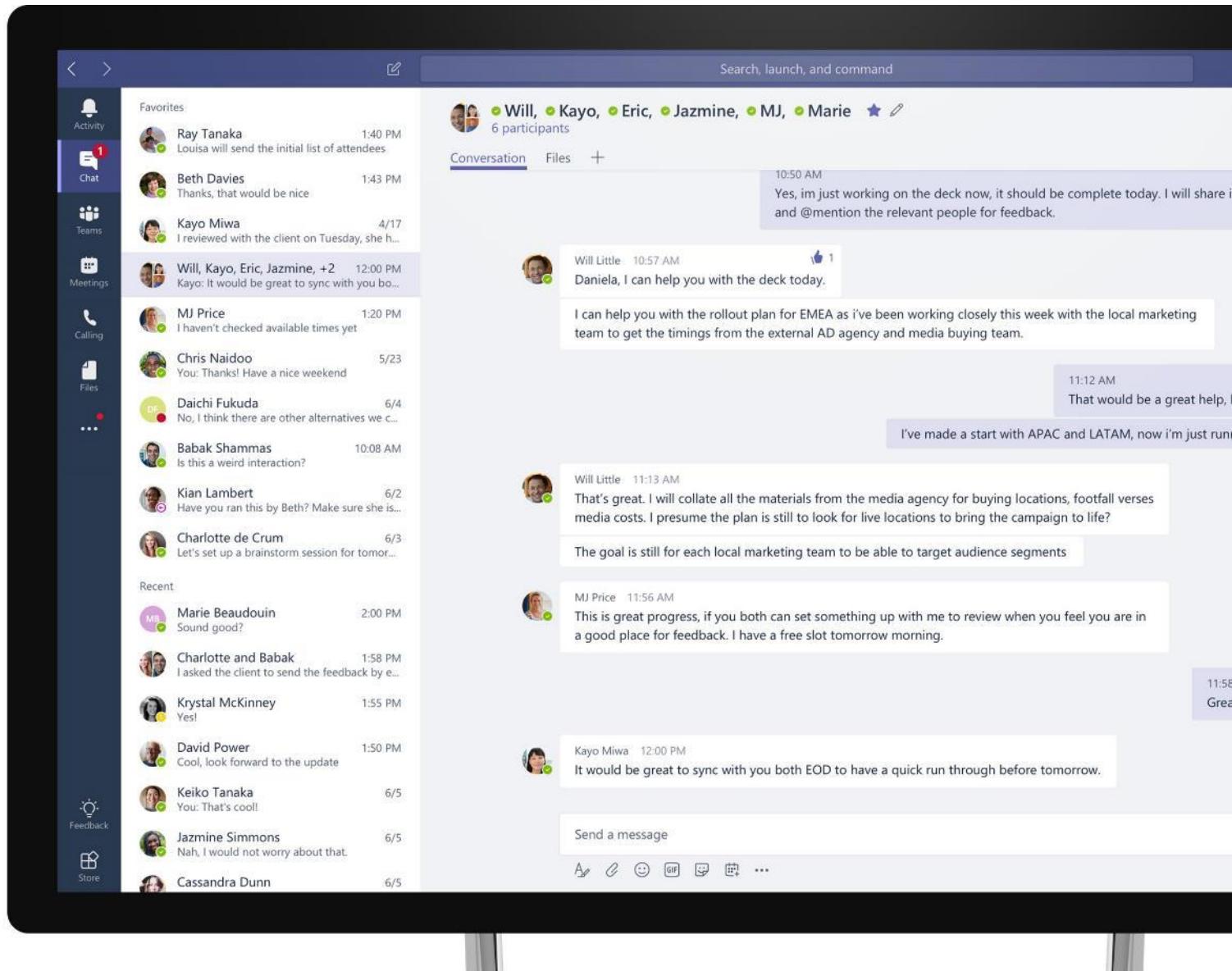
User Scope:
 Guest Users Only
 Everyone

Do you still need to be in the group 'Self Review Group'?
 Yes: Your access will not change.
 No: Your access will be removed when the review ends.

Reason *:
I still need access.

Submit

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



Tenant Group Expiration Policy

Microsoft Azure Search resources, services, and docs (G+) Home Contoso Groups - Expiration Save Discard

Groups - Expiration
Contoso - Azure Active Directory

All groups
Deleted groups
Settings
General
Expiration
Naming policy
Activity
Access reviews
Audit logs
Bulk operation results (Preview)

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and PowerBI.

* Group lifetime (in days) 365

* Email contact for groups with no owners ✓

Enable expiration for these Office 365 groups All Selected None

Managing and governing Office 365 groups at scale

[Creation permissions](#)

[Reporting](#)

[Naming policy](#)

[Policies and information protection](#)

[Expiration policy](#)

[Azure AD access reviews](#)

[Soft delete and restore](#)

[Guest access](#)

Governance (Licensing) Planning:

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

Break
Back at 1130

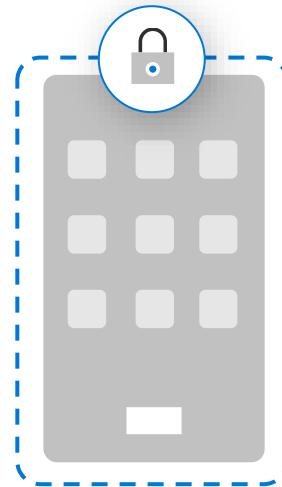
Information Protection

Protect your data on virtually any device with Endpoint Manager

Mobile Device Management (MDM)

Conditional Access

Restrict access to managed and compliant devices.

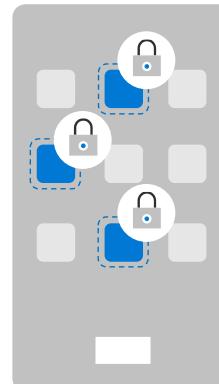


- Enroll devices for management.
- Report and measure device compliance.
- Provision settings, certs, profiles.
- Remove corporate data from devices.

Mobile Application Management (MAM)

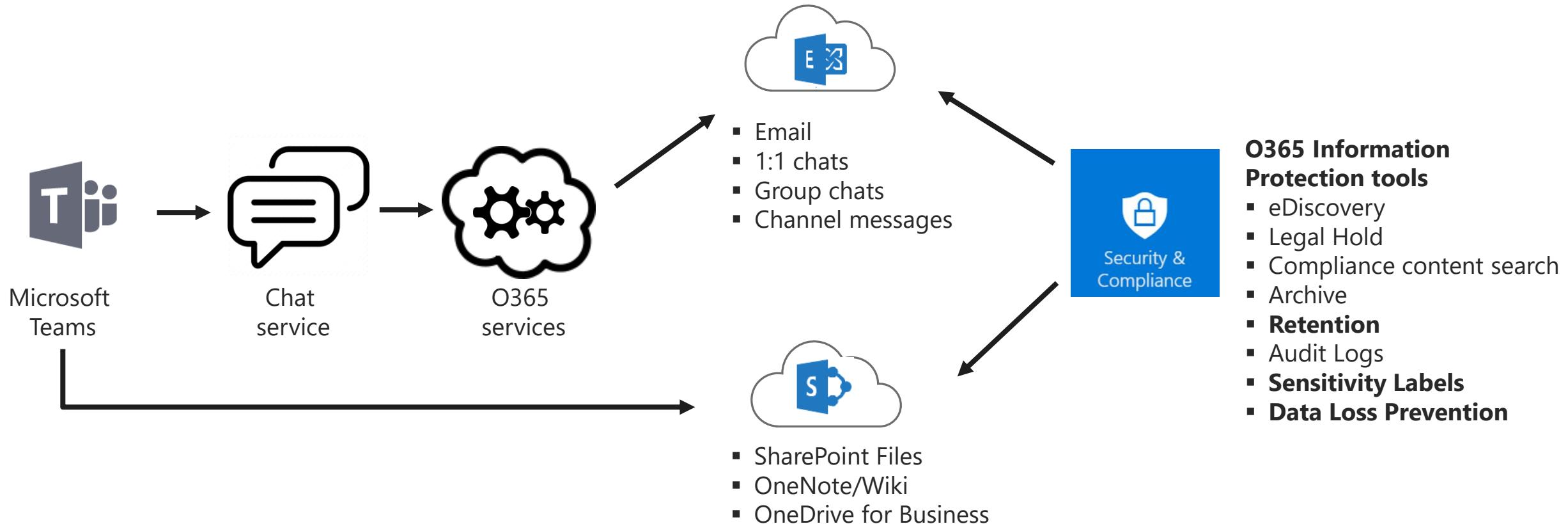
Conditional Access

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

The screenshot shows the Microsoft 365 Security & Compliance center interface. On the left, the navigation menu includes Home, Alerts, Permissions, Classification (selected), Sensitivity labels (selected), Retention labels, Sensitive info types, Data loss prevention, Records management, Information governance, and Supervision.

In the main content area, under the 'Classification' section, a sensitivity label is being configured. The 'Encryption' step is currently selected. The configuration screen is titled 'Encryption' and describes controlling access to files and messages. A red box highlights the 'Encryption' dropdown menu, which contains an 'Apply' option. Below this, a note states that turning on encryption impacts Office files and may affect performance and SharePoint features. Another red box highlights the 'Assign permissions now or let users decide?' section, which is set to 'Assign permissions now'. The note below explains that chosen encryption settings will be enforced automatically. Further down, options include 'User access to content expires' (set to 'Never'), 'Allow offline access' (set to 'Always'), and a red box highlighting the 'Assign permissions to specific users and groups *' section, which has a 'Assign permissions' link. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Contoso Electronics

Office 365 Security & Compliance

Home

Alerts

Permissions

Classification

Sensitivity labels

Retention labels

Sensitive info types

Data loss prevention

Records management

Information governance

Supervision

Name & description

Encryption

Content marking

Auto-labeling for Office apps

Review your settings

Encryption

Control who can access files and email messages that have this label applied. [Learn more about encryption settings](#)

Encryption

Apply

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires

Never

Allow offline access

Always

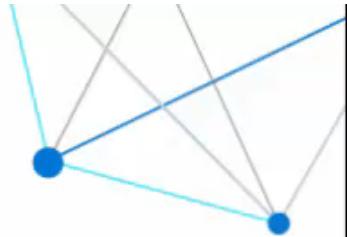
Assign permissions to specific users and groups *

Assign permissions

Back

Next

Cancel



Teams Meetings Security

Document Permissions



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

Contoso Electronics Microsoft 365 compliance

Edit sensitivity label

Name & description

Scope

Files & emails

Groups & sites

Privacy & external user access

External sharing & conditional access

Schematized data assets (preview)

Finish

Define privacy and external user access settings

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

Privacy

These options apply to all Microsoft 365 Groups and teams that have this label applied. When applied, these settings will replace any existing privacy settings for the team or group. If the label is removed, users can change it again.

Public
Anyone in your organization can access the group or team (including content) and add members.

Private
Only team owners and members can access the group or team, and only owners can add members.

None
Team and group members can set the privacy settings themselves.

External user access

Let Microsoft 365 Group owners add people outside your organization to the group as guests. [Learn about guest access](#)

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

The screenshot shows the Microsoft Teams interface. On the left, there's a sidebar with icons for Activity, Chat, Teams, Calendar, and Files. The main area shows a list of teams: DG-2000 Product Team, General, Customer Services, Training and Onboarding, Warehouse Services, and HR Leadership Team. A modal window titled "Add members to Sensitive Guest" is open, showing a search bar with "kakocar@outlook.com" and a button to "Add". Above the modal, the team name "General" is followed by "SG" and "Guest Enabled". A red box highlights the "Guest Enabled" status.

Define privacy and external user access settings

Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.

Privacy
These options apply to all Microsoft 365 Groups and teams that have this label applied. When applied, these settings will replace any existing privacy settings for the team or group. If the label is removed, users can change it again.

Public
Anyone in your organization can access the group or team (including content) and add members.

Private
Only team owners and members can access the group or team, and only owners can add members.

None
Team and group members can set the privacy settings themselves.

External user access
 Let Microsoft 365 Group owners add people outside your organization to the group as guests. Learn about guest access

Highly
Confidential

The screenshot shows the Microsoft Teams interface. On the left, there's a sidebar with icons for Chat, Teams, Calendar, and Files. The main area shows a list of teams: Customer Services, Training and Onboarding, Warehouse Services, HR Leadership Team, General, Events, and Recruitment. A modal window titled "Add members to Sensitive Confidential" is open, showing a search bar with "kakocar@outlook.com" and a button to "Add". Above the modal, the team name "General" is followed by "SC" and "Highly Confidential...". A red box highlights the "Highly Confidential" status.

Add members to Sensitive Confidential

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

kakocar@outlook.com

We didn't find any matches.

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

The screenshot shows the 'Edit sensitivity label' interface in the Microsoft 365 compliance center. The left sidebar lists steps: Name & description (checked), Scope (checked), Files & emails (checked), **Groups & sites** (checked), Privacy & external user access (unchecked), External sharing & conditional access (unchecked), Schematized data assets (preview) (unchecked), and Finish (unchecked). The main content area is titled 'Define external sharing and conditional access settings'. It includes a note about controlling external sharing for SharePoint sites and two sections: 'Content can be shared with' (with 'New and existing guests' selected) and 'Use Azure AD Conditional Access to protect labeled SharePoint sites' (with 'Determine whether users can access SharePoint sites from unmanaged devices' selected). A note states that this requires configuring the SharePoint feature to block or limit access from unmanaged devices. The bottom status bar says 'No authentication contexts set up yet'.

Contoso Electronics Microsoft 365 compliance

Edit sensitivity label

Name & description

Scope

Files & emails

Groups & sites

Privacy & external user access

External sharing & conditional access

Schematized data assets (preview)

Finish

Define external sharing and conditional access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

Control external sharing from labeled SharePoint sites

When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

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

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

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

Only people in your organization
No external sharing allowed.

Use Azure AD Conditional Access to protect labeled SharePoint sites

You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

Determine whether users can access SharePoint sites from unmanaged devices (which are devices that aren't hybrid Azure AD joined or enrolled in Intune).

ⓘ For this setting to work, you must also configure the SharePoint feature that blocks or limits access to SharePoint files from unmanaged devices. [Learn more](#)

Allow full access from desktop apps, mobile apps, and the web

Allow limited, web-only access ⓘ

Block access ⓘ

Choose an existing authentication context (preview). Each context has an Azure AD Conditional Access policy applied to enforce restrictions. [Learn more about authentication context](#)

ⓘ There aren't any authentication contexts configured in your organization. [Learn how to create one](#)

No authentication contexts set up yet

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



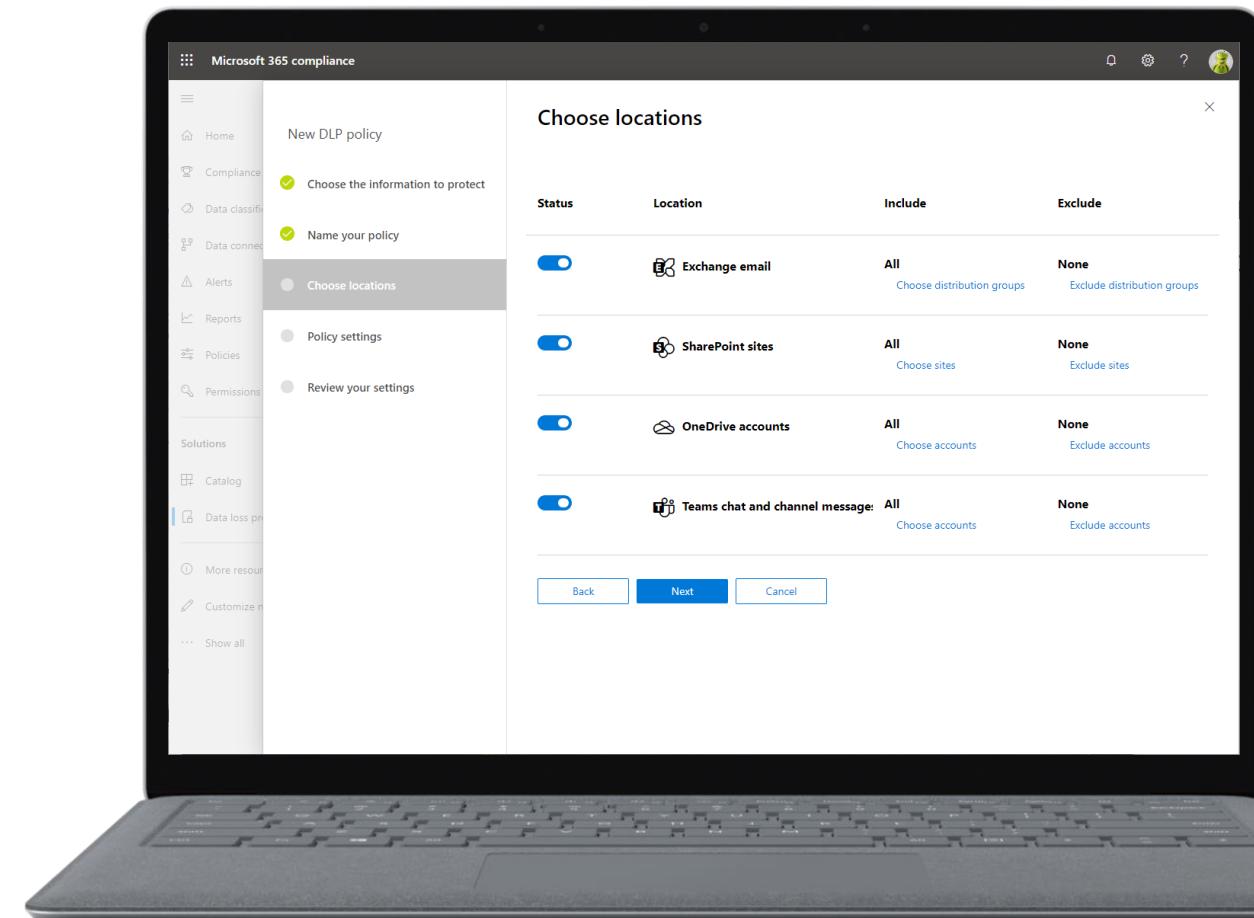
Comprehensive monitoring & alerting

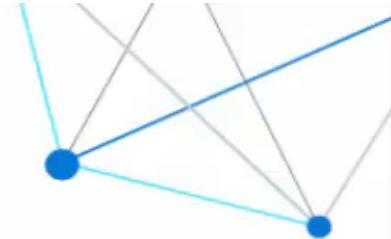
Take action on reports, policy violation alerts, improper data use



Integrated user experiences

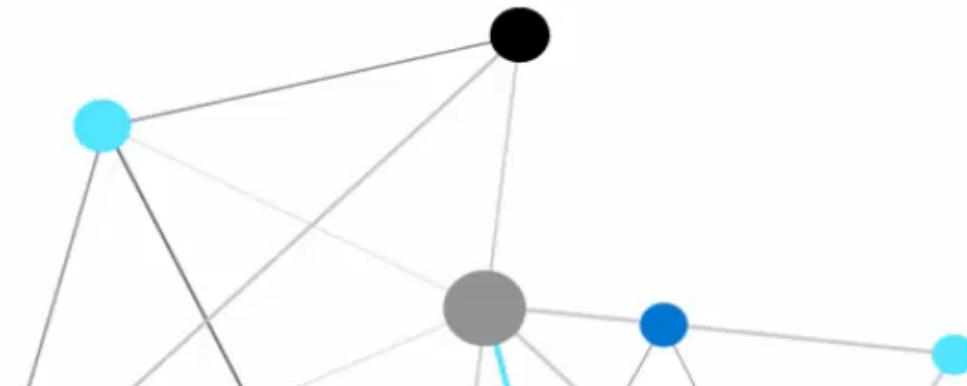
Built-in experiences in apps and services





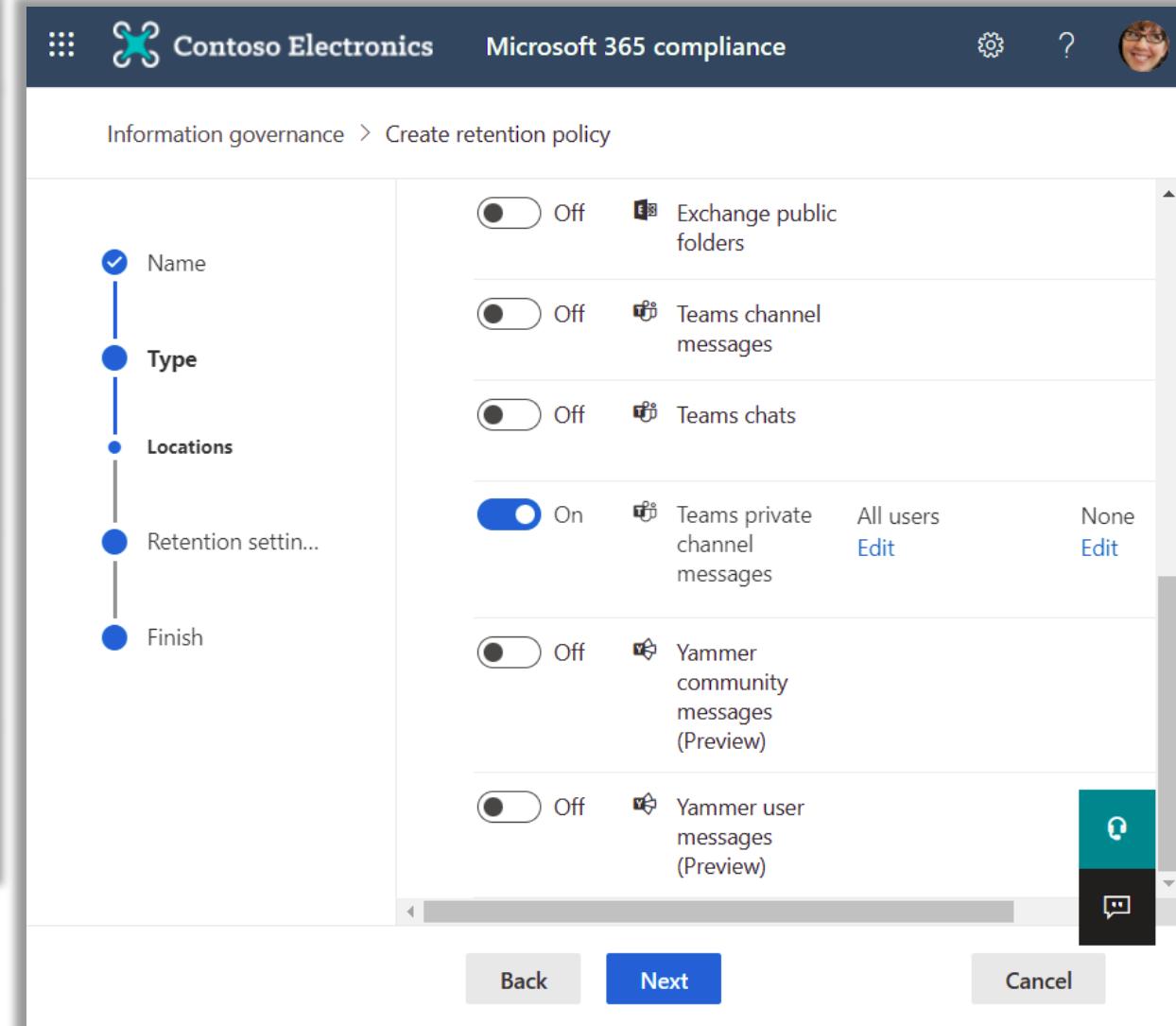
Microsoft Teams Meetings

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



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, 3 rd Party Investigators
<u>Core</u> eDiscovery	Same as above, but you can place content on “ Hold ” in context of cases	Legal Team, Investigators
<u>Advanced</u> 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

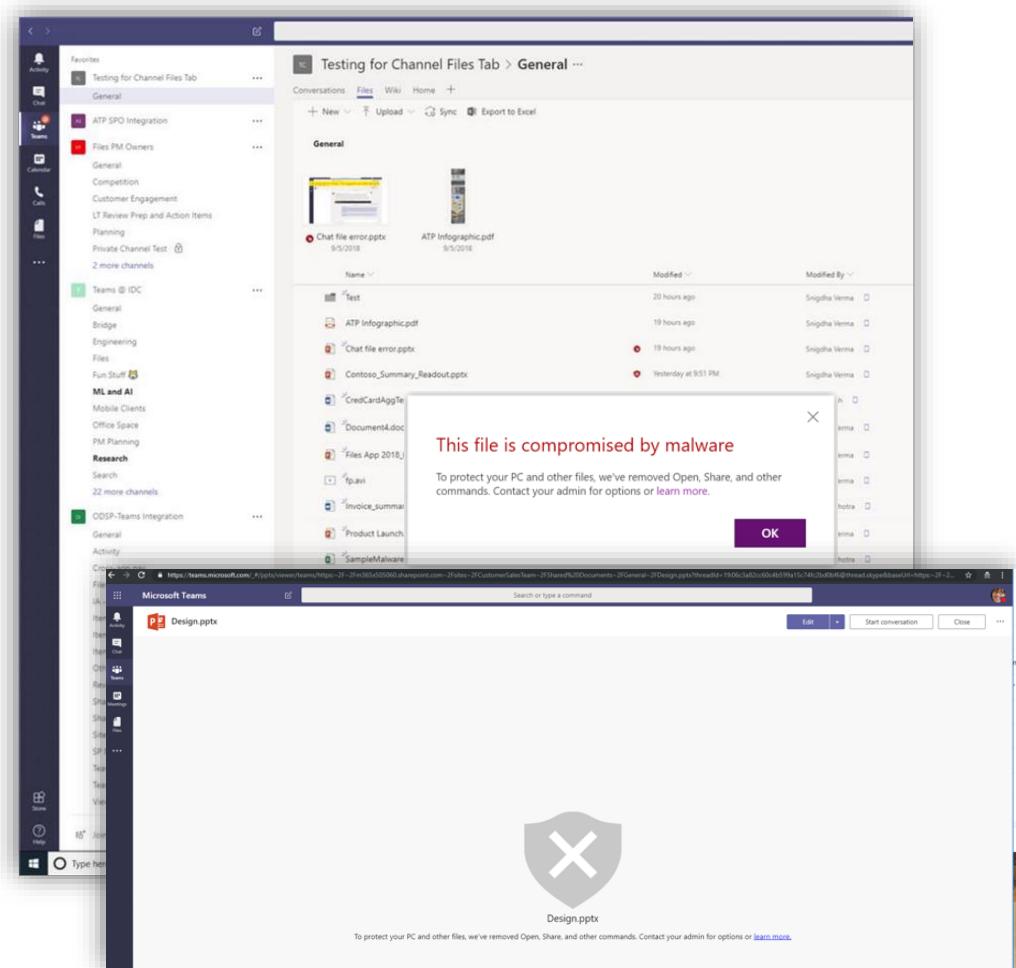
- **Channels**
 - Conversations stored in the mailbox that's associated with the team
 - Files shared stored on the Team's mailbox site
- **Chats**
 - Conversations stored in the mailbox of the users involves in the chat
 - Files stored in the OneDrive account *of the user who shares the file*
- **Meetings & 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](#)

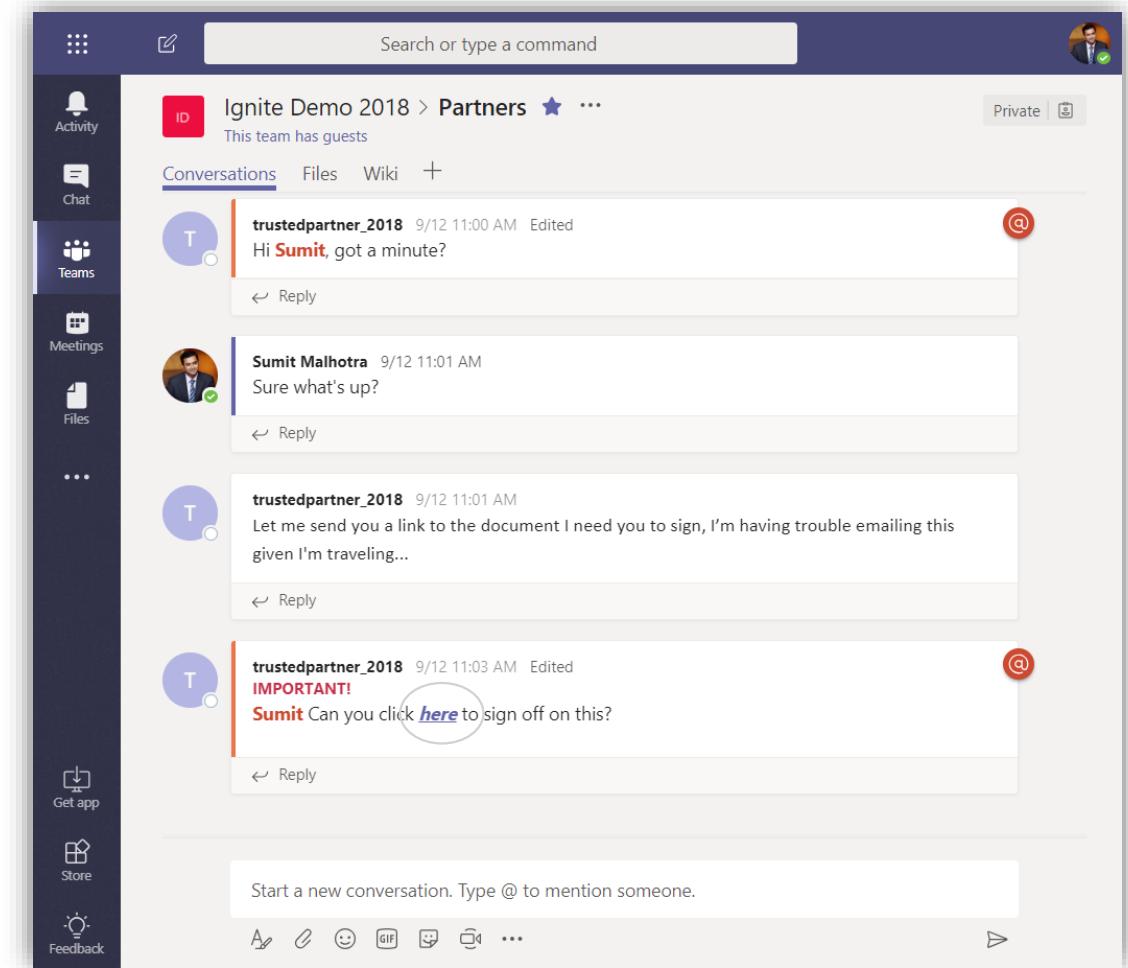
It can take up to **8 hours for meetings and calls to be made available** for searching

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

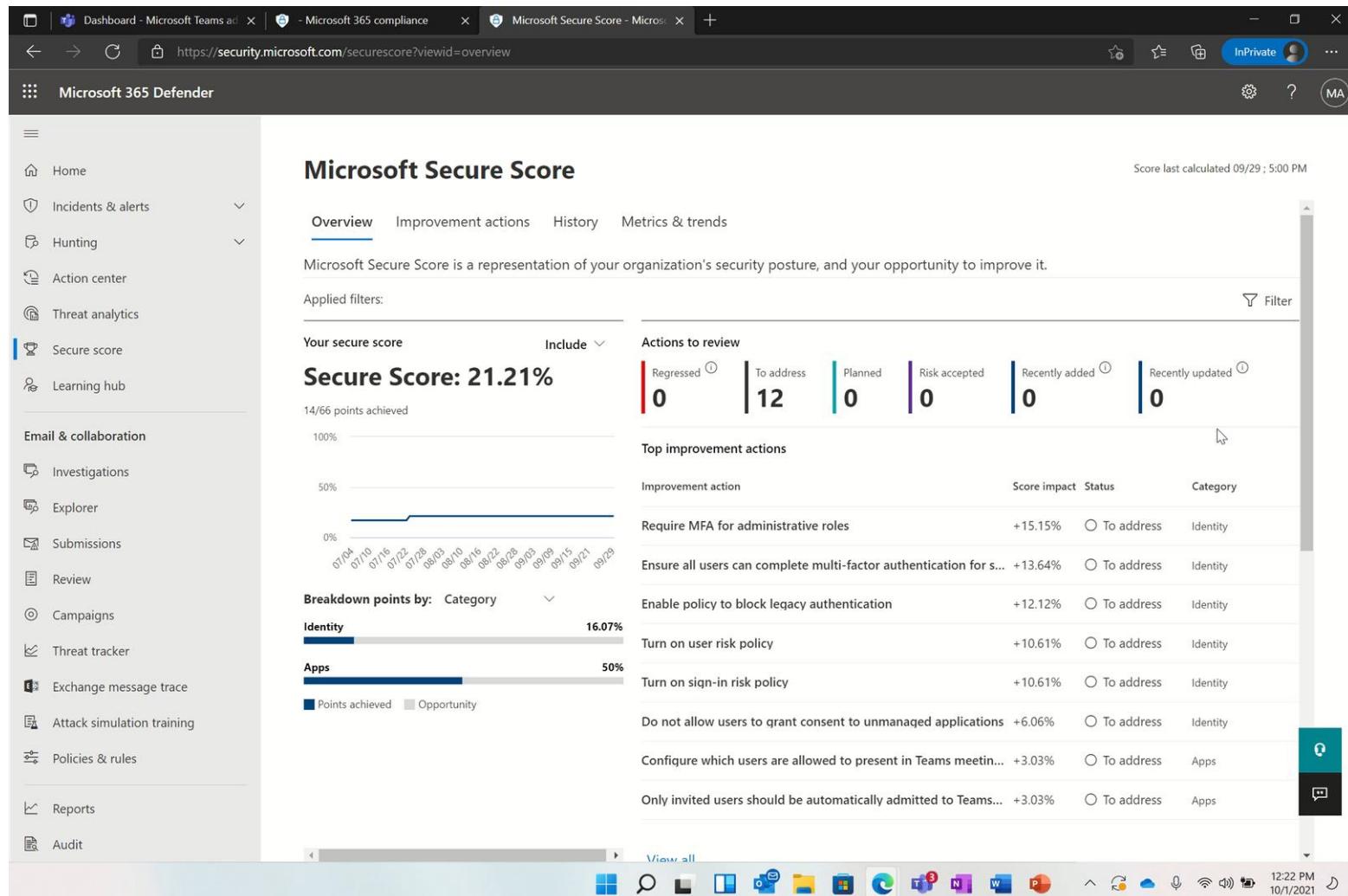
Sentinel Integration for Microsoft Teams

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.

The screenshot shows the Azure Sentinel Overview page. Key statistics include 35.5K Events, 5 Alerts, and 76 Incidents. A chart titled "Events and alerts over time" shows spikes in events and alerts between 6 PM and 12 AM. Another section, "Potential malicious events", shows a world map with no data found. On the right, there's a "Recent incidents" list and sections for "Data source anomalies" and "Democratize ML for your SecOps". The top of the screen features a Microsoft Teams interface with video and audio controls.

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

The screenshot shows the Microsoft 365 Security & Compliance center with the 'Audit log search' page selected. The left sidebar lists various compliance categories like Permissions, Classification, Data loss prevention, etc. The main area displays a search interface with fields for 'Activities' (set to 'Created team, ... (25)'), 'Start date' (10/01/2019), 'End date' (10/31/2019), 'Users' (Show results for all users), and 'File, folder, or site' (with a placeholder for file name). A large table on the right lists 150 audit log entries. The columns include Date, IP address, User, Activity, Item, and Detail. Most entries show 'User signed in to Teams' with 'Unknown (Unknown)' details. One entry from 10/29 at 19:48:34 is listed under 'Audit log search'.

Date	IP address	User	Activity	Item	Detail
2019-10-30 15:28:29		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Unknown (Unknown)	
2019-10-30 13:14:28		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Unknown (Unknown)	
2019-10-30 13:13:28		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Web (1415/1.0.0.0)	
2019-10-30 11:26:16		PradeepG@alpah99.OnMicrosco...	User signed in to Teams	Web (1415/1.0.0.2019103005)	
2019-10-30 09:59:59		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Unknown (Unknown)	
2019-10-30 03:27:29		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Unknown (Unknown)	
2019-10-29 23:19:27		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Web (1415/1.0.0.2019102943)	
2019-10-29 23:18:12		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Web (1415/1.0.0.0)	
2019-10-29 19:48:34		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Unknown (Unknown)	
2019-10-29 19:45:08		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Unknown (Unknown)	
2019-10-29 19:36:46		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Unknown (Unknown)	
2019-10-29 18:36:52		AllanD@alpah99.OnMicrosoft.co...	User signed in to Teams	Unknown (Unknown)	

Getting relevant results: Teams

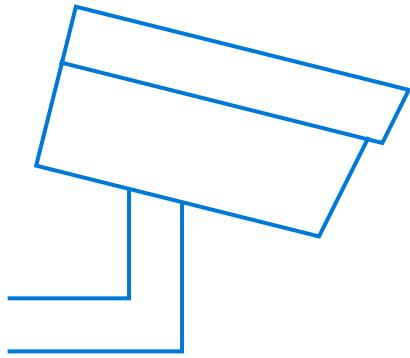
- **Channels**
 - Conversations stored in the mailbox that's associated with the team
 - Files shared stored on the Team's mailbox site
- **Chats**
 - Conversations stored in the mailbox of the users involves in the chat
 - Files stored in the OneDrive account *of the user who shares the file*
- **Meetings & 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](#)

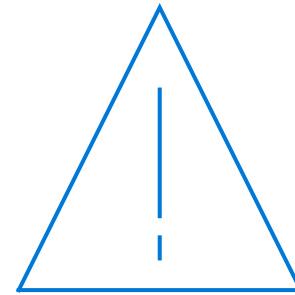
It can take up to **8 hours for meetings and calls to be made available** for searching

Managing Teams Policies

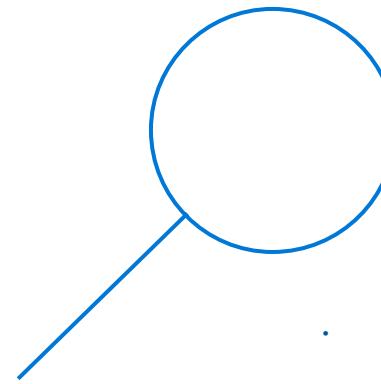
Information Barrier (IB)/Ethical wall in Teams



Control flow of
information



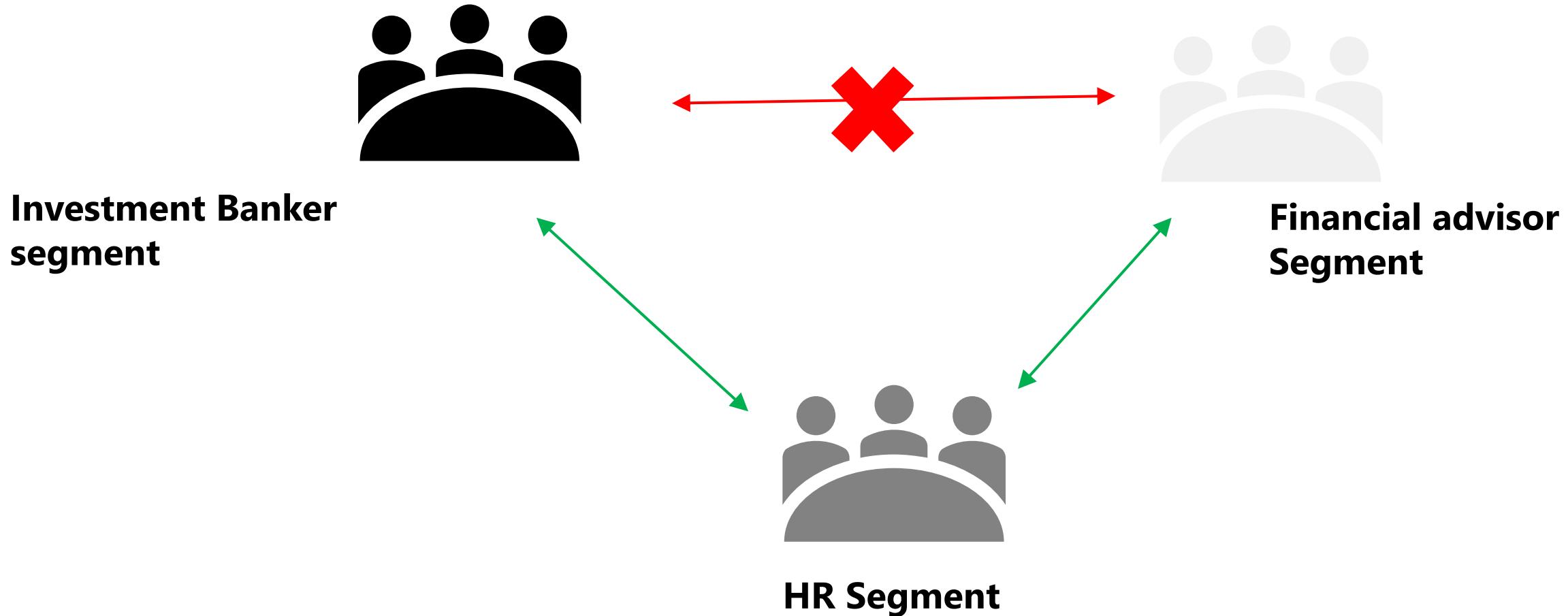
Quarantine
information



Restrict information
sharing

Information Barrier in Teams

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



Info Barrier policies in SCC

365 compliance

Information Barrier Policy

Use information barrier policies to control communication and collaboration in M365 workload between two groups of people. Before setting up information barriers in your org, there are some [important prerequisites](#) to consider.

Segments Policies Applications

Information Segment

In addition to your initial list of policies, make a list of segments for your organization.

New Segments

Name	Last modified by	Last Modified
<input checked="" type="checkbox"/> Investment Banking	Megan Bowen	09-July-2019 10:45:30
<input type="checkbox"/> Advisory	Megan Bowen	10-July-2019 12:00:30

Investment Banking

Segment Name

Investment Banking

User groups Filter

<input type="checkbox"/> And/Or	<input type="text" value="Field"/>	<input type="text" value="Operator"/>
<input type="checkbox"/> +	<input type="checkbox"/> And	<input type="text" value="Location"/>
<input type="checkbox"/> +	<input type="checkbox"/> And	<input type="text" value="User Principal Name"/>
<input type="checkbox"/> +	<input type="checkbox"/> Or	<input type="text" value="User Principal Name"/>

1x1 chats with users in conflicting segment

The image shows the Microsoft Teams Chat interface. On the left is a dark sidebar with icons for Activity, Chat (highlighted with a red circle containing '12'), Teams, Calendar, and Calls. The main area has a blue header with the Microsoft Teams logo and a search bar. Below the header, the Chat tab is selected, showing tabs for Recent and Contacts. A large search input field contains the text "To: pradeep gupta". A message bubble on the right says "We didn't find any matches. Talk to your IT admin about expanding the scope of your search." Below the search field, there are three recent chat entries:

- Alex and Johanna (10/21): You: How are you?
- Adele and Henrietta (10/18): Adele: Hello Enrico and Henrietta
- Alex Wilber (10/17): hi

Group chat between segmented users

The screenshot shows a Microsoft Teams interface with three users added to a group chat:

- Banker Segment (Enrico)**: Represented by a black icon with two people and a red 'X' over it.
- Fin advisor Segment (Pradeep)**: Represented by a grey icon with two people.
- HR Segment (Lee)**: Represented by a grey icon with three people.

Green arrows point from the icons of the first two users to the search bar at the top of the Teams window, indicating they were found through segmentation. The third user was found via a general search.

Microsoft Teams Chat View:

- Recent Contacts**: Shows the three users added to the group.
- Chat Tab**: Active tab.
- Search Bar**: Displays "Search for people, messages or files. Type / to see commands."
- Message Preview**: Shows a message from Patti Fernandez at 3:29 PM: "Patti Fernandez added Enrico Cattaneo and Lee Gu to the chat."
- Message Input**: Shows a message from Lee Gu at 3:29 PM: "Hello....All Creating a group chat to share info wi...

Meetings between segmented users

The image shows a Microsoft Teams interface. At the top left, there are three user segments: "Banker Segment (Enrico)" (black), "Fin advisor Segment (Pradeep)" (dark blue), and "HR Segment (Lee)" (light gray). A red 'X' icon is placed between the first two segments, indicating they cannot communicate. Green arrows point from the "Banker Segment" and "HR Segment" icons towards the "Fin advisor Segment". The main area shows a Microsoft Teams window with a "Calendar" tab selected. The "Activity" tab has a red notification bubble with the number "85". The Teams sidebar on the left lists "Activity", "Chat" (with 1 notification), "Teams", "Calendar" (selected), "Calls", "Files", and "Apps". A central message box displays the error: "🚫 Sorry, your company policy prevents you from joining this call". A "Dismiss" button is at the bottom right of the message box.

Banker Segment (Enrico)

Fin advisor Segment (Pradeep)

HR Segment (Lee)

Activity

85

Microsoft Teams

Activity

Chat

Teams

Calendar

Calls

Files

Apps

Dismiss

🚫 Sorry, your company policy prevents you from joining this call

Users move between departments

Search for people, messages or files. Type / to see commands.

Allan Deyoung, Debra, Grady Archie Chat Files

4:11 PM

...

10/18

10/17

8/22

▶ Henrietta Mueller added Enrico Cattaneo and 4 others to the chat.

HM Henrietta Mueller 8/19 2:53 PM Starting a cool new group chat!

Henrietta Mueller removed Irvin Sayers from the chat.

Enrico Cattaneo has been removed from the chat.

IB & files stored in SPO sites

Access Denied

Due to organizational policies, you can't access this resource.

Here are a few ideas:

- Please contact your organization.

If this problem persists, contact your support team and include these technical details:

Correlation ID: f00c139f-50ef-0000-421c-2b5dd825087f

Date and Time: 10/30/2019 2:46:18 PM

User: pradeepg@alpah99.onmicrosoft.com

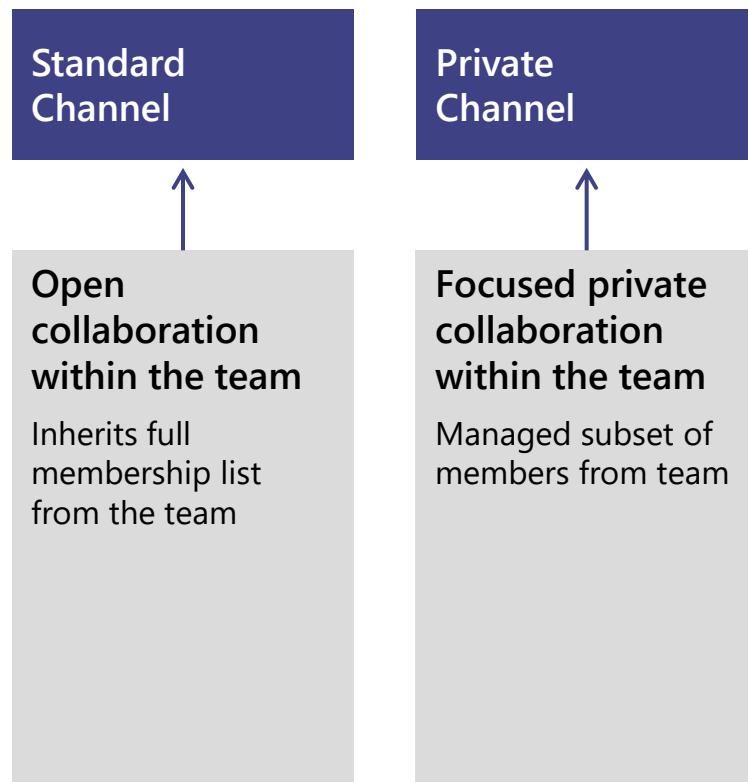
Issue Type: User has encountered a policy issue.

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

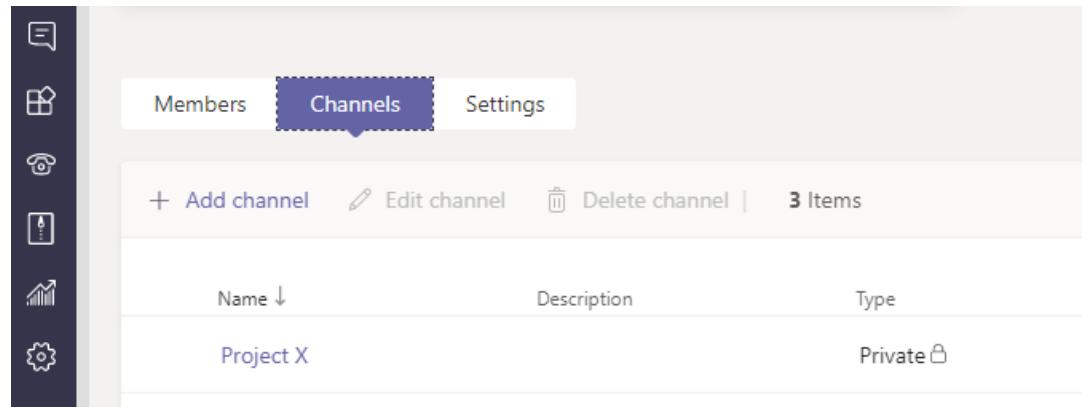
- Admins can control via policies who can create private channels in tenant
- Team owners can control via setting if members can create private channels
- Limited to 30 private channels per team at launch (in addition to 200 standard channels)

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



A screenshot of the Microsoft Teams admin center. The left sidebar shows navigation options like Home, Teams, Channels, and Admin. The main area shows a channel named "Project X" under "Manage teams \ Sales and Marketing \ Project X". The channel details show it is a Private channel and not auto-pinned. Below the channel details is a "Members" section with a count of 1 Item. A table lists one member: Dan Stevenson, with columns for Display name, Username, and Title.

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

The screenshot shows the 'Settings' tab for a channel named 'Project X' within the 'Sales and Marketing' team. The interface is organized into sections: 'Member permissions', '@mentions', 'Fun stuff', and 'Stickers and memes'. Under 'Member permissions', four options are listed, each with a checked checkbox: 'Allow members to create, update, and remove tabs', 'Owners can delete all messages', 'Give members the option to delete their messages', and 'Give members the option to edit their messages'. Under '@mentions', there is one option: 'Choose if @channel mention is allowed', which is also checked. Under 'Fun stuff', there are two options: 'Allow emoji, memes, GIFs, or stickers' (checked) and 'Giphy' (with a sub-option 'Enable Giphy for this channel' and a dropdown menu set to 'Moderate'). Under 'Stickers and memes', there is one option: 'Enable stickers and memes', which is checked.

Team owners and private channels

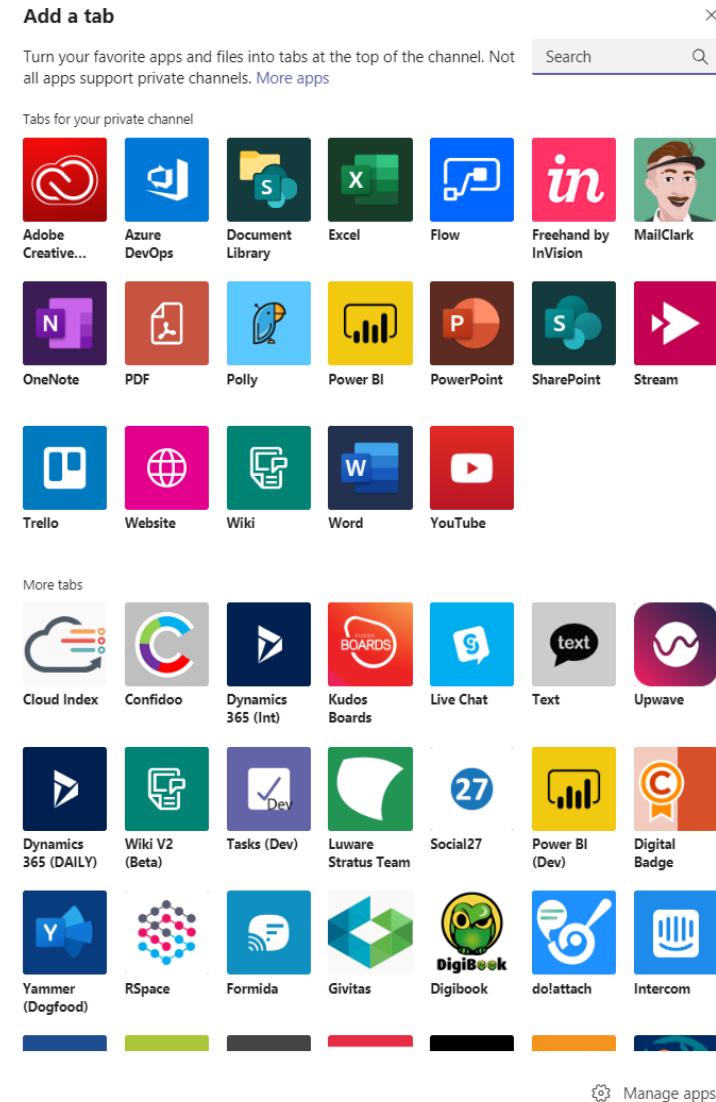
- Team owners can control if members can create private channels
- Team owners can see names, last activity time and owners of all private channels in a team
- Team owners can delete team or individual private channels without being a member
- Removing a member from the team removes them from all private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

The screenshot shows a SharePoint site collection titled "Sales and Marketing - Project X". The page header includes a blue "SM" logo, the site title, and links for "Share" and "Next steps". Below the header is a toolbar with actions: New, Upload, Share, Quick edit, Copy link, Sync, Download, Go to channel, Export to Excel, and AIB. The main content area shows a breadcrumb navigation path: Documents > Project X. A table header is visible with columns: Name, Modified, Modified By, and Add column.

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

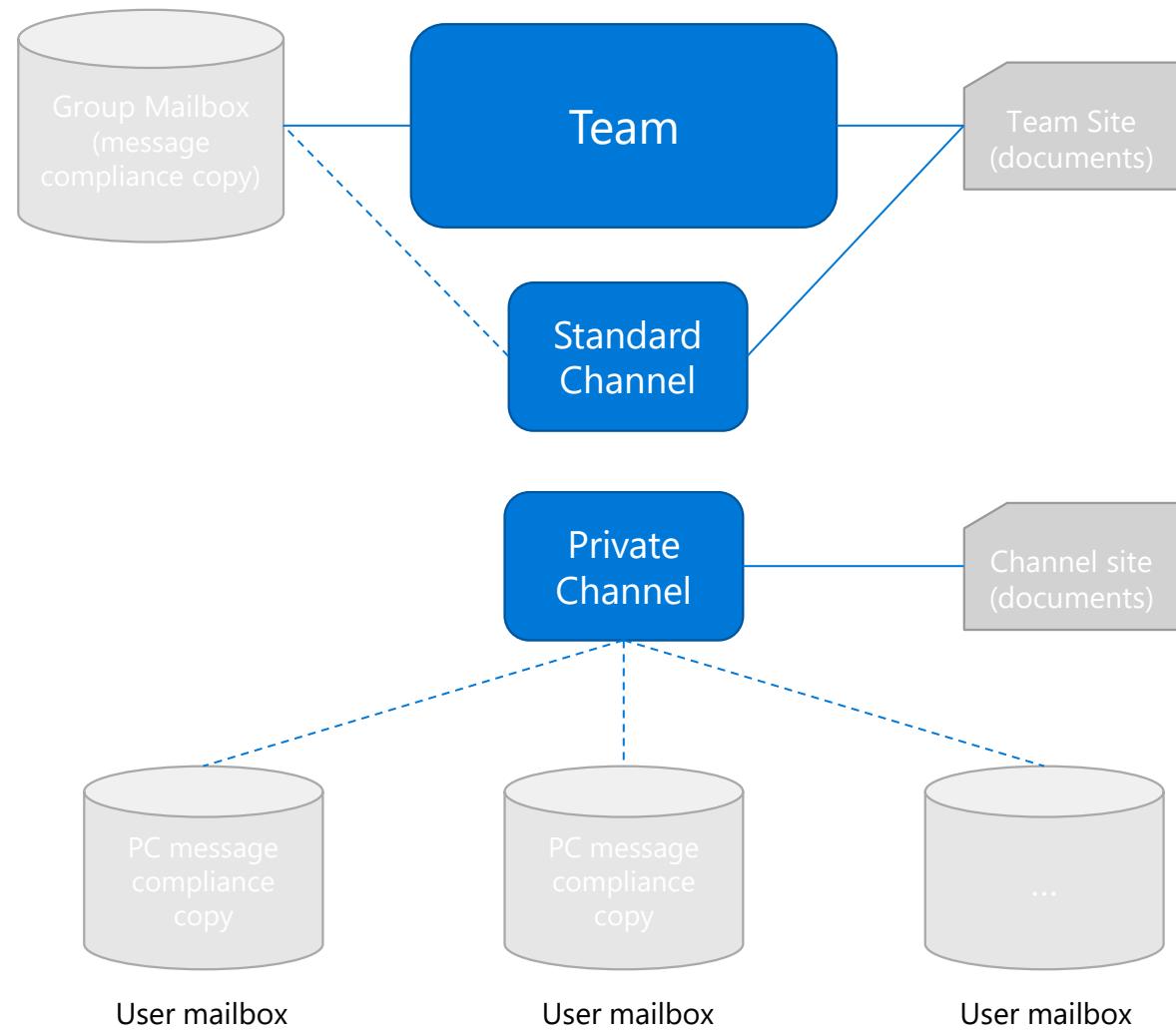
Channel membership

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	Set-TeamChannelUser
DELETE /teams/{id}/channels/{id}/members	Remove-TeamChannelUser

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

Governance

• Help ensure the best return on your investment

Global settings



User specific configuration



Teams lifecycle



Configuration vs. Lifecycle

- **Configuration of Teams**

- Global settings and user specific configuration
- Considered “static”: once defined, changed rarely
- Defined and configured by admin

Global settings



User specific configuration



- **Lifecycle of teams**

- Each individual team has own lifecycle: Initiate, active, sunset
- Configured by team owner or admin

Teams lifecycle



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

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

Role Based Access Control

Teams



User specific



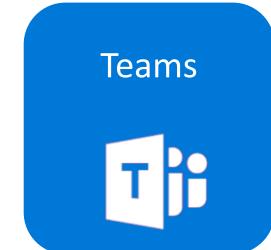
- Allows setting administrators who need different levels of access for managing Teams

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.

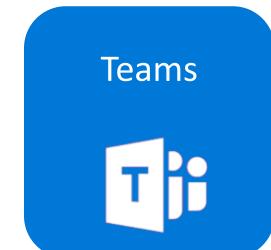
Teams settings



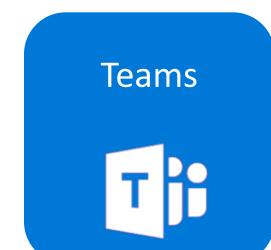
Messaging policies



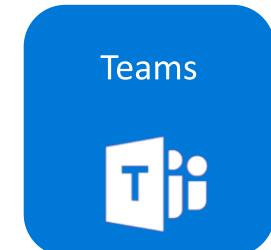
Meeting settings



Meeting policies



Live events policies



External access



Guest access



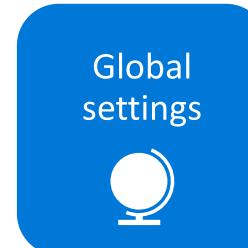
Allow Team Creation



Naming of teams



Classification



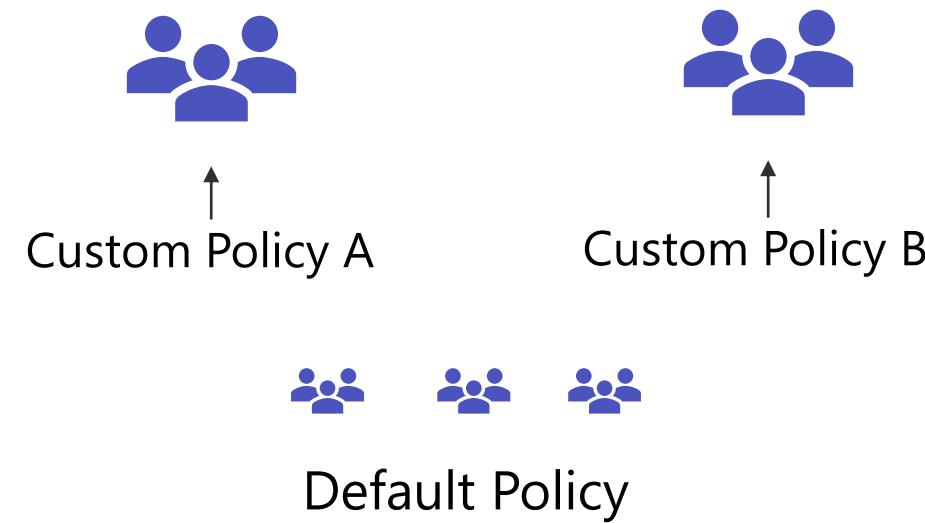
Retention policies

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.





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

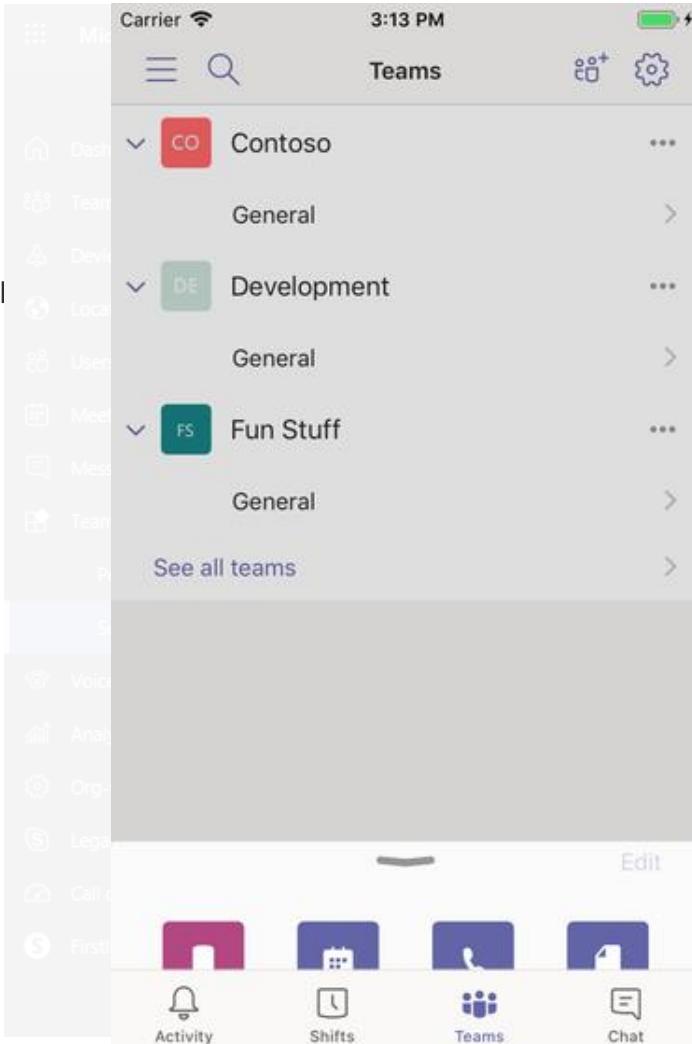
Enable



App permission policies and org-wide settings

Available

Block or allow apps, either org-wide or for specific users
Disable interactions with specific apps



Side loading policies

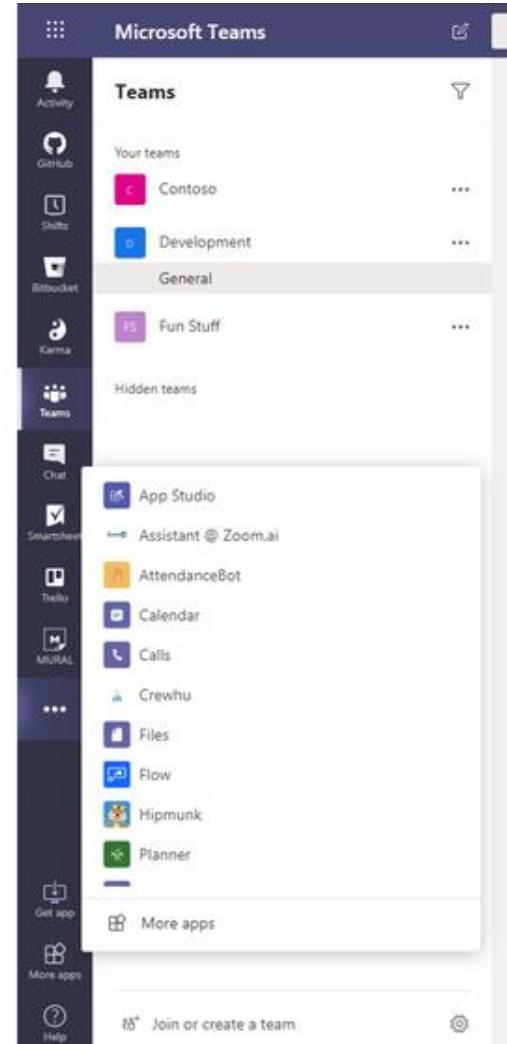
Available

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"
```

 Copy

Get the members of the specified group.

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

 Copy

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}
```

 Copy

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