Enabling Working from Home in a Secure Way with Teams
Managing Teams: onboarding

Prepare your environment:
- Check your environment's readiness for Teams
- Prepare your organization's network for Teams
- Learn about the benefits of installing the desktop, web, and mobile clients

Learn how to use Microsoft Teams
The people who will be supporting the product should be ready to use Microsoft Teams themselves

Assign the right admin roles
You can designate administrators who need different levels of access for managing Microsoft Teams:
- Teams Service Administrator
- Teams Communications Administrator
- Teams Communications Support Engineer
- Teams Communications Support Specialist
Managing Teams

Microsoft Teams Admin Center
Communications and Teams specific features (e.g., meetings, messaging and calling)
https://admin.teams.microsoft.com/

Microsoft 365 Compliance Center
Microsoft 365 Security Center
Security & Compliance across Microsoft 365 (e.g., retention and eDiscovery)

Azure Active Directory Admin Center
Groups, identity, licenses, and access across Microsoft 365 (e.g., Group policies for naming, expiration, etc.)
Managing Teams: settings vs. policies

**Settings – (e.g. guest, federation, audio conferencing)**
- A collection of configuration elements.
- Generally grouped by modality.
- Per tenant only with multiple instances (Bridges, Teams, Voice Apps).

**Policies – (e.g. messaging policy, meeting policy, voice policy)**
- A collection of configuration elements.
- Generally grouped by modality.
- Per user (including multiple) or per tenant; per group coming soon!
Common Teams settings and policies

Org-wide settings
• e.g. external access, guest access, etc.

Teams and Channels:
• Teams policies: Define what users in your organization can do in teams and channels.

Messaging
• Messaging Policies: Select which chat and channel messaging features are available to users in Microsoft Teams.

Meetings
• Meeting Settings: Manage settings that apply to all Teams meetings that users schedule in your organization.
• Meeting Policies: Control the features that are available to meeting participants for meetings that are scheduled by users in your organization.

Apps:
• App permission Policies: Control what apps are available to Microsoft Teams users in your organization.
• App Setup Policies: Customize Microsoft Teams to highlight the apps that are most important for your users.
• Custom app policies and settings: Control who in your organization can upload custom apps to Microsoft Teams.
Configure Guest access

Org wide setting

Allows for collaboration with external partners in Teams

All data generated by guest users is stored in your tenant and all actions visible in your Unified Audit Log.

Files uploaded to Teams by guests can be detonated by Office ATP.

Mange who can invite guests from the Azure AD portal.

MFA can be used to authenticate guest users.
Choose the domain to use when creating Office 365 Groups

Create subdomains for your Office 365 groups

Exchange online Email Address Policy decides the sub domain used

New-EmailAddressPolicy -Name Groups - IncludeUnifiedGroupRecipients - EnabledEmailAddressTemplates "SMTP:@groups.contoso.com" -Priority 1

https://docs.microsoft.com/en-us/office365/admin/create-groups/choose-domain-to-create-groups?view=o365-worldwide
Group Naming convention

Control naming of Teams

Pre- and post fix either AAD attributes or fixed values.

Banned words.

https://docs.microsoft.com/en-us/office365/admin/create-groups/groups-naming-policy?view=o365-worldwide
Sensitivity labels on Teams (Preview)

Access Review

Review of membership to Teams

Either by owners or members

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

*Requires Azure AD Premium P2
Microsoft Teams data residency

Our promise
Microsoft Teams will store the following customer data at rest only when a tenant is provisioned within a geo/region as outlined above:

- Microsoft Teams chats, channel messages, images, voicemail, and contacts
- SharePoint Online site content and the files stored within that site
- Files uploaded to OneDrive for Business

Microsoft Teams will continue to be rolled out to more local datacenters aligned with the Office 365 data residency strategy.
# Data entity storage

Key data entities and location where data is stored at rest

<table>
<thead>
<tr>
<th>Entity</th>
<th>Storage</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Chat service table storage (moving to Cosmos DB)</td>
<td>Ingested to Exchange to enable compliance</td>
</tr>
<tr>
<td>Image</td>
<td>Media service on Azure (using Blob storage)</td>
<td>Ingested to Exchange to enable compliance</td>
</tr>
<tr>
<td>Files</td>
<td>Team files ➔ SharePoint Chat files ➔ OneDrive for Business</td>
<td></td>
</tr>
<tr>
<td>Voicemail</td>
<td>Individual mailbox in Exchange</td>
<td></td>
</tr>
<tr>
<td>Recording</td>
<td>Media service on Azure (using Blob storage) (&lt;24 hours)</td>
<td>Encoded to Stream</td>
</tr>
<tr>
<td>Calendar meeting</td>
<td>Individual mailbox in Exchange</td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td>Exchange</td>
<td></td>
</tr>
<tr>
<td>Telemetry</td>
<td>Microsoft Data warehouse (No customer content)</td>
<td></td>
</tr>
</tbody>
</table>
Groups in Office 365

- Microsoft Teams uses **group membership** as the access control list for Files and Notes tabs
- Owners of existing Groups can move them **over** to Microsoft Teams
- When a Group becomes a Team, its **existing SharePoint and OneNote** are automatically ported over to Teams
- To work with Teams, Groups must be **private** and must have **fewer than 5,000 members**
- Team creation settings are **controlled through the admin portal** where you control group creation settings
SharePoint Online

• The Teams site is created in SharePoint Online
• Each Channel in a Team gets a folder on this SharePoint Online site
• The Files tab uploads your collaboration files to this SharePoint Online site
• Files shared within a conversation are automatically added to the Files tab
• Permissions and file security options set in SharePoint are automatically reflected within Teams
• Files can be managed in the SharePoint web client by clicking the “…” next to the file name
Private channels
Focused private collaboration within a team

Teams

<table>
<thead>
<tr>
<th>Channel A (Standard)</th>
<th>Channel B (Private)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open collaboration within the team</td>
<td>Focused private collaboration within the team</td>
</tr>
<tr>
<td>Inherits full membership list from the team</td>
<td>Managed subset of members from team</td>
</tr>
</tbody>
</table>

Access control of channel content
- Separate SPO site collection for files with access restricted to channel members
- Copy of channel messages in private channel user mailboxes for compliance

Creation
- Admins can control via policies who can create private channels in tenant
- Team owners can control via setting if members can create private channel in team

Membership
- 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

Lifecycle and classification tied to parent team
- Private channel lifecycle is tied to parent team
- SP site data classification and lifecycle same as private channel
OneDrive for Business

- Private chat files are hosted in your OneDrive for Business
- Files shared in private chat are automatically shared in the sender's OneDrive
- Permissions are automatically granted to all participants in a private chat where a file is shared
- Clicking Files in the left rail gives you instant access to your OneDrive for Business files
Exchange

• Exchange Online creates a group mailbox and calendar for each newly-created Team

• Meetings created within Microsoft Teams are pushed to your Exchange calendar

• Meetings created in Exchange sync to the Meetings tab in Microsoft Teams
Security and compliance in Teams

Manage information protection
- Data loss prevention
- Sensitivity labels

Manage information governance
- Retention policies

Discover and respond
- eDiscovery
- Audit log

Regulatory compliance
Support for over 42 national, regional, and industry-specific regulations including
- ISO 27018
- SOC 1 and 2
- HIPAA/HITECH
- GDPR
- GLBA
- FedRAMP

Managing internal risk
- Information barriers
- Supervision

What’s new?

<table>
<thead>
<tr>
<th>1 day retention policies</th>
<th>Information barriers for SPO files in Teams</th>
<th>Sensitivity labels for Teams (Preview)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe links</td>
<td>e-Discovery support for threaded conversation</td>
<td>Audit log support for messaging events</td>
</tr>
<tr>
<td>Capability</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Archive</td>
<td>Any content stored in any Teams related workload needs to be preserved immutably.</td>
<td></td>
</tr>
<tr>
<td>Compliance Content search</td>
<td>Any content stored in any workload can be search through rich filtering capabilities and be exported to a specific container for compliance and litigation support.</td>
<td></td>
</tr>
<tr>
<td>eDiscovery – Messaging/Files</td>
<td>Rich in-place eDiscovery capabilities including case management, preservation, search, analysis and export to help our customers simplify the eDiscovery process to quickly identify relevant data while decreasing cost and risk.</td>
<td></td>
</tr>
<tr>
<td>Legal hold</td>
<td>When any team or individual is put on In-Place Hold or litigation hold, the hold is placed on both the primary and the archive messages (No edits or deletes).</td>
<td></td>
</tr>
<tr>
<td>Auditing and reporting</td>
<td>All Team activities and business events must be captured and available for customer search and export.</td>
<td></td>
</tr>
<tr>
<td>Conditional Access and Intune MAM</td>
<td>Ensure that access to Microsoft Teams is restricted to devices that are compliant with IT Admin or Corporate Organization set policies and security rules both for the Teams Apps and the services it uses under the hood. Includes MAC Support for Conditional Access as well.</td>
<td></td>
</tr>
<tr>
<td>Moderator support</td>
<td>The ability to have a moderator (owner of team) of a Team delete data from any user in the team that is inappropriate and mute users in a team/channel.</td>
<td></td>
</tr>
<tr>
<td>Windows Information Protection</td>
<td>Windows Information Protection (WIP), previously known as enterprise data protection (EDP), helps to protect against this potential data leakage without otherwise interfering with the employee experience. WIP also helps to protect enterprise apps like MS Teams.</td>
<td></td>
</tr>
<tr>
<td>Allowed List of Apps</td>
<td>An Admin can control the list of 3P apps (bots, connectors, tabs) that can be used by end users within a tenant.</td>
<td></td>
</tr>
<tr>
<td>Retention / Preservation</td>
<td>Help organizations reduce the liabilities associated with messaging. The Customer can configure their tenant to retain data for a fixed period of time or retain it with unlimited storage for different Teams workloads.</td>
<td></td>
</tr>
<tr>
<td>eDiscovery – Calling/Meetings</td>
<td>Rich in-place eDiscovery capabilities including case management, preservation, search, analysis and export to help our customers simplify the eDiscovery process to quickly identify relevant data while decreasing cost and risk.</td>
<td></td>
</tr>
<tr>
<td>Data loss prevention (DLP)</td>
<td>Identify any sensitive data stored being transferred within or outside of Customer Organization in Teams to intercept and prevent leakage for Files and Chat/Channel Messages.</td>
<td></td>
</tr>
<tr>
<td>Advanced Threat Protection</td>
<td>Support for safe files and safe links in Microsoft Teams to protect your organization from malicious attacks with the power of Office 365 Advanced threat protection.</td>
<td></td>
</tr>
<tr>
<td>Business Information Barriers</td>
<td>Prevent exchanges or communication that could lead to conflicts of interest. (a.k.a. Ethical walls)</td>
<td></td>
</tr>
<tr>
<td>Conversation/Chat Supervision</td>
<td>Supervision policies in Office 365 allow you to capture employee communications for examination by designated reviewers. You can define specific policies that capture internal and external email, Microsoft Teams, or 3rd-party communications in your organization.</td>
<td></td>
</tr>
<tr>
<td>Voice Compliance Recording</td>
<td>Provide APIs to allow software vendors the ability to listen and to record calls to meet the requirements set by MiFiD II. APIs aiming for Q4 CY2019.</td>
<td></td>
</tr>
<tr>
<td>Outbound Guest Access Policies</td>
<td>(Admins) restrict employees’ ability to be added as Guests to other tenants (block completely or restrict to trusted tenants). Preview in Q1 CY2020.</td>
<td></td>
</tr>
<tr>
<td>Customer Key</td>
<td>Encrypt customer content in Teams messages, similar to the EXO model, with cloud provider having access to the key. Preview in H1 CY2020.</td>
<td></td>
</tr>
</tbody>
</table>
Compliance builds on Office 365: Messages and Files

Microsoft Teams → Chat service → O365 substrate

- Email
- 1:1 and group chats (user mailbox)
- Channel messages (group mailbox)

SharePoint Files
OneDrive for Business

O365 Information Protection tools
- eDiscovery
- Content search
- Hold
- Retention
- Audit Logs
Compliance Architecture for Calls and Meetings

Microsoft Teams Clients → Calling/Meeting services → Call/Meeting record processing → O365 Information Protection tools

- eDiscovery
- Content search
- Hold
- Retention
- Audit Logs

- Call Summary
- Meeting Summary
Ingested into the mailboxes of each participant.
Compliance boundary

- **User Browser, Desktop, Mobile**
- **Guest user**
- **Anonymous join to a meeting**
- **Federation communication**

### Microsoft Teams

#### Connectors
- Data posted to a channel
- Query to Giphy
- Push notifications to Apple or Google to notify mobile client
- Optional Box, Dropbox, Google drive, Citrix File share
- Get a preview of a URL that is posted to a message

#### Email a channel
- Data posted to a channel
- URL Preview

#### Apps/Bots
- Push Notifications (Mobile)
- Files Cloud storage (3rd party)
- Optional Box, Dropbox, Google drive, Citrix File share

#### Tabs
- Any third-party tab is hosted outside the compliance boundary

#### Apps/Bots
- Any third-party app/bot or line of business app is hosted outside the compliance boundary

#### Graph API
- Graph APIs can be exposed to line of business apps or 3rd party apps

#### Calling Plan (PSTN)
- Enables inbound/outbound calling outside the organization

### Compliance boundary

- **Standard Teams user**
- **Guest added via AAD B2B**
- **Anonymous user joining a meeting**
- **Communication between multiple tenants**

### 2-way communication

- Standard Teams user
- User Browser, Desktop, Mobile
- Guest added via AAD B2B
- Anonymous user joining a meeting
- Communication between multiple tenants

### Inbound data

- Federation communication
- Guest added via AAD B2B
- Anonymous user joining a meeting

### Outbound data

- User Browser, Desktop, Mobile
- Guest added via AAD B2B
- Anonymous user joining a meeting
- Communication between multiple tenants

---

**Important Notes:**

- Data posted to a channel
- Query to Giphy
- Push notifications to Apple or Google to notify mobile client
- Optional Box, Dropbox, Google drive, Citrix File share
- Get a preview of a URL that is posted to a message

---

**Technical Details:**

- Enables inbound/outbound calling outside the organization
- Standard Teams user
- Guest added via AAD B2B
- Anonymous user joining a meeting
- Communication between multiple tenants

---

**Key Features:**

- User Browser, Desktop, Mobile
- Guest added via AAD B2B
- Anonymous user joining a meeting
- Communication between multiple tenants

---

**Technical Integration:**

- Federation communication
- Email a channel
- Apps/Bots
- Tabs
- Graph API
- Calling Plan (PSTN)
Retention

• Supports **preservation and deletion**
  • Preserve data certain timespan
  • Delete data after certain timespan
  • Perform disposition review on data after certain timespan
  • Can be combined

• Configuration
  • Can be based on file creation or last modified
  • Can be scoped to specific users or groups
  • Can be configured independently for chats and channels

• Retention is effective on the back-end
  • If user deletes messages, they will stay discoverable for admins

• Use content search to review retained data
Retention

Minimum for retention is 1 day

Retention is retroactive

E.g. a policy set to delete content after 60 days, will delete all older content when enabled

Possible delay in deletion

Exchange Life Cycle assistant (ELC) runs daily, but it has an SLA of 7 days
E.g. with retention policy to delete after 60 days, these items could persist for up to 67 days
In most cases, there is no delay
Hold

- Define locations and conditions
  - Same as for content search
- Once hold is enabled
  - All versions of modified items will be kept
  - Deleted items will be kept
- Can be configured via Exchange portal or eDiscovery case
- Data Locations

<table>
<thead>
<tr>
<th>Scenario</th>
<th>What to place on hold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Teams Private Chats</td>
<td>User mailbox</td>
</tr>
<tr>
<td>Microsoft Teams Channel Chats</td>
<td>Group mailbox used for the team</td>
</tr>
<tr>
<td>Microsoft Teams Content (e.g. Wiki, Files)</td>
<td>SharePoint site used by the team</td>
</tr>
<tr>
<td>Private Content</td>
<td>OneDrive for Business site of the user</td>
</tr>
</tbody>
</table>
eDiscovery

Electronic discovery is the electronic aspect of identifying, collecting and producing electronically stored information (ESI) in response to a request for production in a law suit or investigation.

Create “case” for eDiscovery process

Combines a set of searches and hold configuration

Hold can be configured directly from eDiscovery
Search can be scoped to items on hold

Results can be exported
Smart Camera

Teams mobile client has its own camera app

Take picture from within the app

Secure

Pictures are not auto-stored user’s mobile device

Smart – integrating Office Lens functionality

Auto crop and optimization based on image type such as document, whiteboard, or index card
Is Teams secure?

- All communication to and from clients and within the platform is encrypted end-to-end
- All actions are logged in the Office 365 Unified audit log
- All chat and files are stored and governed by retention policies
- Data Loss Prevention capabilities prevent accidental or deliberate loss of files or information
- Guest access is a secure way of including external partners
- Conditional access policies and Microsoft Cloud App Security can e.g. prevent login without MFA from or file downloads to unmanaged devices
Best practices for security and compliance in Microsoft Teams

- Enable conditional access for all users
- Configure guest access in Teams and Sharepoint
- Enable MFA for guest users through Conditional Access
- Configure retention policies
- Enable Sensitivity labels
- Enable Office 365 Advanced Threat Protection to ensure detonation of all web-links in chat and file-uploads by guests
License requirements – Compliance Features

**eDiscovery**

Search and investigation included in all licenses

Export requires Office E3 or E5

Advanced eDiscovery
- Provides text analytics, machine learning, and the Relevance/predictive coding capabilities
- Office E1/E3 with Advanced eDiscovery standalone license or Office E5

**Hold**

Exchange Online Plan 2 (included in Office E3 and E5)

**Supervision**

Office E3 with Advanced Compliance add-on or Office E5
License requirements – Security Features

• Unified Audit Log
  • Up to 90 days retention: Office F1 F3 E1 E3
  • Up to 365 days retention: Office E5 or Advanced Compliance add-on

• Conditional Access
  • EMS E3 or Azure AD Premium Plan 1

• Access Review
  • EMS E3 or Azure AD Premium Plan 2

• Safe document and safe links
  • Office E5 or Office ATP Plan 1