

# Security and compliance in Microsoft Teams

02/29/2020 • 9 minutes to read •  +23 • Applies to: Microsoft Teams

## In this article

[Security](#)

[Compliance](#)

[Information Protection Architecture](#)

[Licensing](#)

[Location of data in Teams](#)

[Compliance standards](#)

[Related topics](#)

### Important

As a customer of Office 365, you own and control your data. Microsoft does not use your data for anything other than providing you with the service that you have subscribed to. As a service provider, we do not scan your email, documents, or teams for advertising or for purposes that are not service-related. Microsoft doesn't have access to uploaded content. Like OneDrive for Business and SharePoint Online, customer data stays within the tenant. You can check out more about our trust and security related information at the [Microsoft Trust Center](#). Teams follows the same guidance and principles as the Microsoft Trust Center.

Microsoft Teams is built on the Office 365 hyper-scale, enterprise-grade cloud, delivering the advanced security and compliance capabilities our customers expect. For more information on planning for security in O365, please review our O365 content. [The O365 security roadmap](#) is a good place to start. For more information on planning for compliance in O365, you can start with [the plan for security and compliance](#) article.

This article will provide further information about Teams-specific security and compliance. You should review these Microsoft Mechanics videos about security and compliance:

- [Microsoft Teams Essentials for IT: Security and Compliance](#) (12:42 min)
- [Microsoft Teams Controls for Security and Compliance](#) (10:54 min)

# Security

Teams enforces team-wide and organization-wide two-factor authentication, single sign-on through Active Directory, and encryption of data in transit and at rest. Files are stored in SharePoint and are backed by SharePoint encryption. Notes are stored in OneNote and are backed by OneNote encryption. The OneNote data is stored in the team SharePoint site. The Wiki tab can also be used for note taking and its content is also stored within the team SharePoint site.

Read [Identity models and authentication](#) for more insight into authentication and Teams, and [How modern authentication works](#) will help with modern authentication in particular.

Because Teams works in partnership with SharePoint, OneNote, Exchange, and more, you should be comfortable managing security in O365 all-up. To learn more about Office 365 security, read [Configure your Office 365 tenant for increased security](#).

## ⓘ Note

Currently, [private channels](#) supports limited security and compliance features. Support for the full set of security and compliance features in private channels is coming soon.

## Advance Threat Protection (ATP)

Advance Threat protection (ATP) is available for Microsoft Teams, along with SharePoint and OneDrive for Business, applications that integrate with Teams for content management. ATP allows you to determine if content in these applications is malicious in nature, and block this content from user access.

How the affected content is managed after detection is up to the settings you've selected in O365. We strongly recommend you consider all applications when it comes to configuring ATP, and for further reading, the [Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams](#) article will have detailed information on how to get started.

## Safe Links

While, at this time, ATP safe links are not available in Microsoft Teams, they are now in public preview through our Technology Adoption Program (TAP), and while a release date for general availability isn't set, we'll update this article when that time arrives. Meanwhile, for information on O365 Safe Links, please review [Office 365 ATP Safe Links](#).

## How Conditional Access policies work for Teams

Microsoft Teams relies heavily on Exchange Online, SharePoint Online, and Skype for Business Online for core productivity scenarios, like meetings, calendars, interop chats, and file sharing. Conditional access policies that are set for these cloud apps apply to Microsoft Teams when a user directly signs in to Microsoft Teams - on any client.

Microsoft Teams is supported separately as a cloud app in Azure Active Directory conditional access policies. Conditional access policies that are set for the Microsoft Teams cloud app apply to Microsoft Teams when a user signs in. However, without the correct policies on other apps like Exchange Online and SharePoint Online, users may still be able to access those resources directly. For more information about setting up a conditional access policy in the azure portal, go to: [Azure Active Directory Quickstart](#).

Microsoft Teams desktop clients for Windows and Mac support modern authentication. Modern authentication brings sign-in based on the Azure Active Directory Authentication Library (ADAL) to Microsoft Office client applications across platforms.

Microsoft Teams desktop application supports AppLocker. For more information about AppLocker prerequisites, please see: Requirements to use [AppLocker](#).

## Compliance

Teams has a wide range of information to help you with compliance areas, including retention policies, Data Loss Protection (DLP), eDiscovery and legal hold for channels, chats and files, audit log search, as well as mobile application management with Microsoft Intune. We've provided some information on all these topics below, and you can go to the Office 365 Security & Compliance Center to manage these settings.

### Retention Policies

Retention policies in Microsoft Teams allows you to both retain data that's important for your organization to keep, for regulatory, legal, business, or other reasons, and also to remove content and communications that are not relevant to be retained. You can also use retention policies to keep data for a period of time and then delete it. For further information, review the [Retention policies in Microsoft Teams](#) article.

### Data Loss Prevention (DLP)

Data Loss Prevention (DLP) in Microsoft Teams, as well as the larger DLP story for O365, revolves around business readiness when it comes to protecting sensitive documents and data in O365. Whether you have concerns around sensitive information in messages or documents, DLP policies will be able to help ensure your users don't share this sensitive data with the wrong people.

For information on Data Loss Prevention in Teams, please review [DLP for Microsoft Teams](#). A good article for O36 DLP concerns is <https://docs.microsoft.com/microsoft-365/compliance/data-loss-prevention-policies>.

## eDiscovery

Electronic discovery, or eDiscovery, 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. Capabilities include case management, preservation, search, analysis, and export of Teams data. This includes chat, messaging and files, meeting and call summaries. For Teams meetings and Calls, a summary of the events that happened in the meeting and call are created and made available in eDiscovery.

For more details about how to do O365 eDiscovery in Security & Compliance Center and run compliance content search for Teams content, please go to the links below:

[eDiscovery](#)

[Content Search](#)

We have a Teams-specific article for more information, [eDiscovery of guest-to-guest chats](#).

Customers can leverage in-place eDiscovery or [Advanced eDiscovery] per their [requirements](#). The following table outlines the differences between the two:

	<b>In-place eDiscovery</b>	<b>Advanced eDiscovery</b>
Case Management	X	X
Access Control	X	X
Content Searches	X	X
Hold(s)	X	X
Export	X	X

	<b>In-place eDiscovery</b>	<b>Advanced eDiscovery</b>
Duplication Detection	-	X
Relevance Searches with Machine Learning	-	X
Unstructured Data Analysis	-	X

## Legal Hold

During litigation, you may need all data associated with a user (custodian) or a Team to be preserved as immutable, so that it can be used as evidence for the case. You can do this by placing either a user (user mailbox) or a Team on legal hold. For a team legal hold, the team's mailbox can be put on the following holds:

- In-Place Hold (a subset of the mailbox or site collection through targeted queries or filtered content is put on hold), or
- Litigation Hold (the entire mailbox or site collection is placed on hold).

In either case, once the hold is set it ensures that, even if end users delete or edit channel messages that are in the group mailbox, immutable copies of that content are maintained and available through eDiscovery search. Legal holds are generally applied within the context of an eDiscovery case.

Please see the [Overview of retention policies](#) article to understand more about preservation and holds in the Office 365 Security & Compliance Center. For more Teams-specific information on legal hold, we also have our [Place a Microsoft Teams user or team on legal hold](#) article for you to learn more.

## Compliance Content Search

Content search can be used to search for all Teams data through rich filtering capabilities. The resulting data can be exported to a specific container for compliance and litigation support. This can be done with or without an eDiscovery case. This enables compliance admins to gather Teams data across all users, review and export it for further processing. Please refer to this [Content Search in O365](#) article to learn more about how to conduct a compliance content search for Microsoft Teams and other O365 content in the Office 365 Security & Compliance Center.

### Tip

Using content search, you can filter down to Microsoft Teams only content, such as Chat and Channel Messages, Meetings, and Calls, if necessary.

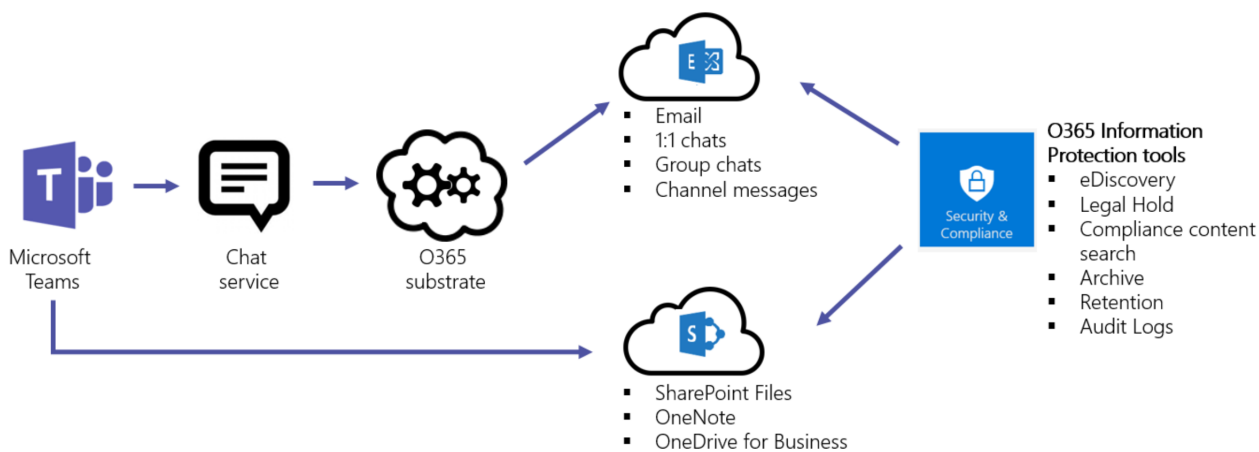
If you'd like further Teams-specific information on configuring content search, review the [Content search in Microsoft Teams](#) article.

## Auditing and Reporting

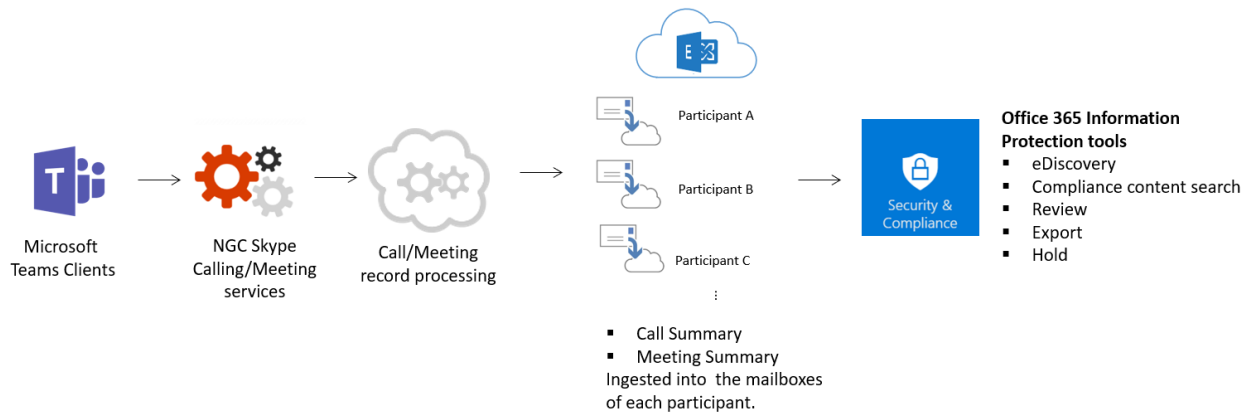
Audit log search plugs right into the Office 365 Security & Compliance Center and gives you the ability to set alerts, as well as report on audit events, by allowing the export of workload specific or generic event sets for admin use and investigation across an unlimited auditing timeline. You can set up alerts for all audit Log data within the Office 365 Security & Compliance Center, and filter and export this data for further analysis. Please refer to the [Search the audit log](#) article to learn more about how to conduct an Audit log for O365. To learn more about searching for Microsoft Teams events in the Office 365 Security & Compliance Center, we also have the [Turn on auditing in Teams](#) article for you to review.

## Information Protection Architecture

The following figure indicates the ingestion flow of Teams data to both Exchange and SharePoint for Teams Files and Messages.



The following figure indicates the ingestion flow of Teams Meetings and calling data to Exchange.



### Important

There can be up to a 24-hour delay to discover Teams content.

## Licensing

When it comes to information protection capabilities, Office 365 subscriptions and the associated standalone licenses will determine the available feature set.

For information on determining the licensing needs to implement features for security and compliance, please review: [Licensing for Office 365](#).

### Note

Content Search and eDiscovery do not need to be enabled in the Security & Compliance Center to work.





## Location of data in Teams

Data in Teams resides in the geographic region associated with your Office 365 tenant. To see what regions are supported currently, please review [Location of data in Microsoft Teams](#).

If you need to see which region houses data for your tenant, go to the [Microsoft 365 admin center](#) > **Settings** > **Organization profile**. Scroll down to **Data location**.

## Data location

Office 365 has been built from the ground-up to provide enterprise-grade security, privacy and compliance capabilities. As part of our transparency principles we publish the location of your core customer data at rest here.

Service Name	Region
 Exchange	North America
 SharePoint	North America
 Skype for Business	North America
 Microsoft Teams	North America

## Compliance standards

Teams is Tier D-compliant. This includes the following standards: ISO 27001, ISO 27018, SSAE16 SOC 1 and SOC 2, HIPAA, and EU Model Clauses (EUMC). Within the Microsoft compliance framework, Microsoft classifies Office 365 applications and services into four categories. Each category is defined by specific compliance commitments that must be met for an Office 365 service, or a related Microsoft service, to be listed in that category.

Services in compliance categories C and D that have industry-leading compliance commitments are enabled by default. Services in categories A and B come with controls to turn on or turn off these services for an entire organization. Details can be found in the [Compliance Framework for Industry Standards and Regulations](#). Teams also supports Cloud Security Alliance compliance.

## Related topics

[M365 Security](#) [M365 Compliance](#)

---

Is this page helpful?

 Yes  No

---