



MICROSOFT TEAMS

CUSTOMER CONSIDERATIONS AND TOOLS FOR HIPAA COMPLIANCE

JULY 2021



Table of Contents

1.1 HOW TO USE THIS DOCUMENT	7
1.2 DOCUMENT SCOPE	7
1.4 LICENSING REQUIREMENTS	9
2. MICROSOFT TEAMS AND HIPAA REQUIREMENTS	9
2.1 HIPAA ADMINISTRATIVE SAFEGUARDS	10
2.1.1 <i>Business Associate Agreements</i>	10
2.1.2 <i>Workforce Training</i>	10
2.1.3 <i>Considerations for addressing Microsoft Teams in Policies and Procedures</i>	11
2.1.3.1 Categorization of Data and Associated Data Retention Policies	12
2.1.3.2 Identifying Situations Where PHI May Be Exchanged	13
2.1.3.3 Storage Location of PHI and Other Information	13
2.1.3.4 Information Access Policies and Controls	13
2.1.3.5 Guest Access to Information	14
2.1.3.6 Use of Applications from the Microsoft Teams Store	14
2.1.3.7 Use of Microsoft Teams on Mobile Devices	14
2.2.1 <i>Identity Management Controls</i>	16
2.2.1.1 Creation of Regular User Accounts	17
2.2.1.2 Maintenance of Regular User Accounts	17
2.2.1.3 Deprovisioning of Standard User Accounts	18
2.2.1.4 Federated Users	19
2.2.1.5 Guest Users	19
2.2.2 <i>Authentication Control</i>	19
2.2.2.1 Integrated Single Sign-On	19
2.2.2.2 Username and Password	20
2.2.2.3 Multifactor Authentication	20
2.2.2.4 Password-less Authentication	20
2.2.2.5 Federation	21
2.2.3 <i>Data Classification</i>	21
2.2.4 <i>Non-HIPAA Data Management Considerations</i>	22
2.2.4.1 Access Rights and Permissions	22
2.2.4.2 Data Retention Controls	22
2.2.4.3 Legal Hold Requirements	22
2.2.5 <i>Monitoring User Activity</i>	22
2.2.6 <i>Ongoing Assurance and Internal Validation</i>	23
2.2.6.1 User Account and Access Reviews	23
2.2.6.2 Data Classification Validation	23
2.2.6.3 Configuration Auditing	24
2.3 HANDLING SECURITY INCIDENTS	24
3. KEY MICROSOFT TEAMS CONFIGURATION CONSIDERATIONS	25
3.1 SMART LOCKOUT	25
3.2 PASSWORD STANDARDS	26
3.3 AUTHENTICATION METHODS	26
3.4 MULTIFACTOR AUTHENTICATION ("MFA")	27
3.5 LEAST PRIVILEGE	28
3.6 PASSWORD RESET	29
3.7 USER REGISTRATION AND DELETION	30

3.8 SECURITY MONITORING.....	31
3.9 CONFIGURING COMMUNICATIONS POLICIES TO HELP FOSTER CULTURE OF SAFETY AND INCLUSION	32
3.10 POLICY-BASED RECORDING FOR CALLINGS AND MEETINGS	33
3.11 eDISCOVERY AND LEGAL HOLD	34
3.13 DATA RETENTION AND DELETION	38
3.14 ENFORCE COMPANY-APPROVED PRODUCT LISTS	39
3.15 AUDITABLE EVENTS AND CONTENT.....	40
3.16 ROLE MANAGEMENT.....	41
4. USING COMPLIANCE MANAGER	43
4.1 PERFORM ONGOING RISK ASSESSMENTS.....	43
4.2 MONITOR USING COMPLIANCE MANAGER	43
4.3 INCREASE THE COVERED ENTITIES' OR BUSINESS ASSOCIATES' SCORE IN COMPLIANCE MANAGER.....	44
5. CONFIGURING MICROSOFT TEAMS COMPONENTS FOR INTERNAL COLLABORATION	45
5.1 GLOBAL TEAMS AND CHANNEL POLICIES.....	45
5.2 MESSAGING POLICIES FOR INTERNAL USERS.....	46
5.3 FILE SHARING AND CLOUD STORAGE OPTIONS	47
5.4 CONFIGURING MEETING POLICIES.....	47
6. CONFIGURING MICROSOFT TEAMS' COMPONENTS FOR EXTERNAL COLLABORATION	49
6.1 ENABLING ACCESS FOR EXTERNAL USER TYPES.....	50
6.1.1 <i>Enabling External Access in Microsoft Teams</i>	50
6.1.2 <i>Enabling Guest Access in Microsoft Teams</i>	51
6.2 CONFIGURING APP POLICIES IN MICROSOFT TEAMS.....	52
6.3 CONFIGURATION OF MESSAGING POLICIES.....	53
6.3.1 <i>Messaging Policies for External Users</i>	53
6.3.2 <i>Messaging Policies for Guest Users</i>	53
6.4 FILES SHARING AND STORAGE OPTIONS FOR FILES TAB	54
6.5 SHAREPOINT AND ONE DRIVE EXTERNAL COLLABORATION	55

Special thanks to [Edgile](#) for their contributions to this whitepaper

Disclaimer

The information and configurations provided in this document are for informational purposes only to help Covered Entities and Business Associates with implementing HIPAA requirements. **Although Microsoft can help with such implementation, the ultimate responsibility for using Microsoft Teams in a manner that is compliant with HIPAA remains with the Covered Entity or Business Associate, subject to the terms of any applicable Business Associate Agreement.**

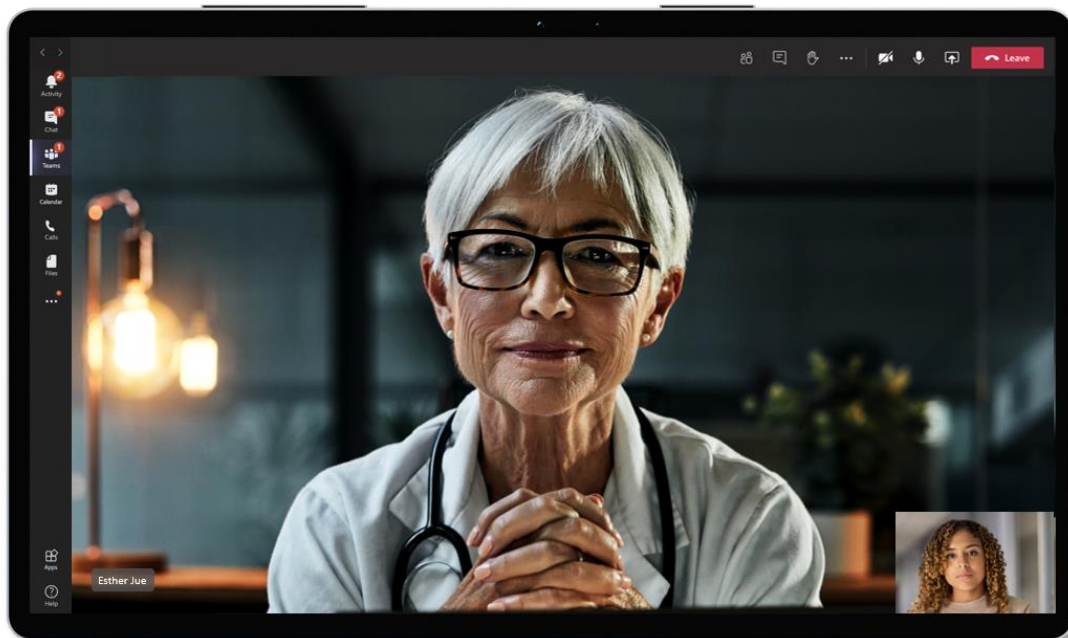
HIPAA Covered Entities and Business Associates may wish to conduct their own evaluations, including for purposes of their HIPAA Risk Analyses, to understand how Microsoft Teams can be implemented in their organization, including their policies and procedures, and any other HIPAA requirements.



1. Overview

[Microsoft Teams](#) is an enterprise collaboration tool offered by Microsoft and used by many different organizations subject to the Health Insurance Portability and Accountability Act of 1996, as amended (collectively, "HIPAA").

HIPAA establishes requirements for the use, disclosure, and safeguarding of individually identifiable health information, as well as for individual rights and breach notification. HIPAA applies to Covered Entities—specifically, health care providers, health plans, and health care clearinghouses—that use HIPAA covered transactions to bill or pay for health care, and create, receive, maintain, transmit, or access patients' protected health information ("PHI"). HIPAA further applies to Business Associates who perform certain functions or activities involving PHI as part of providing services to or on behalf of the Covered Entity. If a customer that is a Covered Entity or Business Associate provides PHI to Microsoft Teams or Microsoft Office 365 for storage or processing, then Microsoft would be considered a Business Associate of that organization.



Three major rules promulgated pursuant to HIPAA include the Privacy Rule, the Breach Notification Rule, and the Security Rule (collectively, the "HIPAA Rules"). As mentioned above, the HIPAA Privacy Rule provides individuals with rights to their PHI and regulates that use and disclosure of PHI by Covered Entities and Business Associates, and generally provides for safeguards of that information. The HIPAA Breach Notification Rule requires that Covered Entities notify individuals, the Department of Health and Human Services ("HHS"), and, in some cases, the media, of a breach of unsecured PHI and further requires

that Business Associates notify Covered Entities of a breach. The HIPAA Security Rule is essentially a sub-set of the HIPAA Privacy Rule that includes specific administrative, technical, and physical safeguards for electronic PHI. Because Microsoft Teams enables the use and disclosure of electronic PHI by Microsoft's customers, the HIPAA Security Rule's requirements are of particular importance for Covered Entities or Business Associates, and for Microsoft.

On its own, Microsoft Teams offers security features that allow Covered Entities and Business Associates to put in place appropriate technical safeguards to help meet their respective HIPAA obligations through granular configuration options and robust logging capabilities. Additional technical controls are possible when Microsoft Teams features are combined with the Microsoft Cloud security capabilities, including advanced authentication controls, compliance manager, and data encryption functionality.

Note, however, that any technical controls that are provided as part of Microsoft Teams will not completely satisfy a Covered Entities' or Business Associates' obligations under HIPAA. Administrative and physical controls, particularly around access, use, and disclosure of PHI, must also be defined in HIPAA Covered Entities' and Business Associates' policies and procedures.



This document has been developed to help both the technical staff responsible for implementing Microsoft Teams and the legal, privacy, and compliance teams responsible for HIPAA compliance. It is intended to provide an overview of HIPAA administrative considerations and helpful links between the applicable HIPAA Security Rule requirements and configurable Microsoft Teams controls, including some of the required technical configuration settings.

1.1 How to Use This Document

This document is intended to be used as follows:

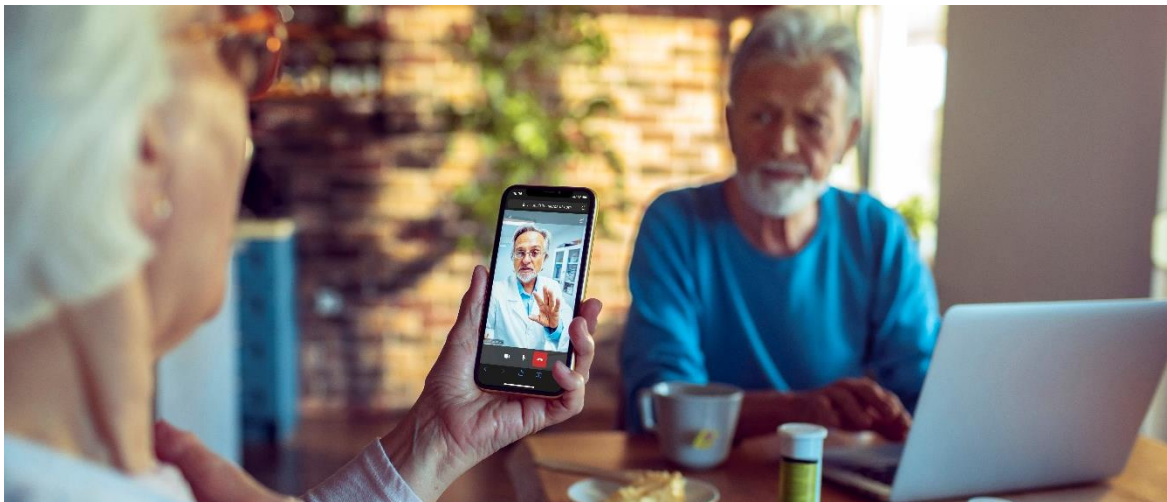
- Individuals with responsibility for implementing HIPAA requirements are encouraged to review Section 2 of the document, which provides information regarding non-technical considerations for the organization's HIPAA compliance.
- Information technology ("IT") and information security ("IS") teams should review Sections 3 through 6 to understand the controls and the recommended configuration settings for Microsoft Teams, together with the required underlying hardware.

Please note: This is not a comprehensive Microsoft Teams configuration guide. This document is designed to provide information and suggestions on implementing reasonable and appropriate safeguards using Microsoft Teams, as may be necessary under the HIPAA Rules.

1.2 Document Scope

The security settings for Microsoft Teams included in this document are for a standard O365 deployment. Deployments that may not be standard, including "hybrid deployments," will require specialized settings. Further, whether the SharePoint and/or Exchange servers are deployed on the entity's premises ("on-prem") or in the cloud will impact how some settings can be managed. Consumer and other non-business versions of Microsoft Teams are outside of the scope of this document.

The HIPAA Security Rule's requirements that include specific security controls to be applied to a computing environment are the primary scope of this document. Administrative and physical safeguards, including development of effective policies and procedures covering user notification, education, and appropriate use of PHI are highlighted, but it is up to each individual Covered Entity or Business Associate to ensure that any necessary non-technical controls are in the place.



1.3 Glossary of Terms



This document will be using the following terms throughout the compliance and configuration setting explanations. Any capitalized terms not included immediately below have the meaning attributed to them in the HIPAA Rules.

- **Business Associate (BA)**—A person or entity who creates, receives, maintains, or transmits Protected Health Information (PHI) for or on behalf of a Covered Entity or another Business Associate. See 45 C.F.R. § 160.103 for full definition.
- **Covered Entity**—Any health plan, healthcare clearing house or healthcare provider that transmits Protected Health Information (PHI) in electronic form in connection with a transaction covered under HIPAA. See 45 C.F.R. § 160.103 for full definition.
- **Individually Identifiable Health Information**—Information collected from an individual that is created or received by a Covered Entity or Business Associate that relates to the past, present, or future health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual that identifies or can reasonably identify the individual. See 45 C.F.R. § 160.103 for full definition.
- **Protected Health Information (PHI)**—Individually Identifiable Health Information that is transmitted or maintained by electronic media or transmitted or maintained in any other form or medium by a Covered Entity or Business Associate. See 45 C.F.R. § 160.103 for full definition. Note that PHI can include information that is merely demographic, such as zip codes.

For additional information and specific requirements and guidance, please refer to the HIPAA Rules, which can be found at 45 C.F.R. [Part 160](#), [Part 162](#), and [Part 164](#), and additional HIPAA guidance from HHS, which can be found at <https://www.hhs.gov/hipaa/index.html>.

1.4 Licensing Requirements

The specific security and compliance features available will vary depending upon the license(s) that have been purchased by the Covered Entity or Business Associate. The licensing options vary from base Office 365 ("O365") packages up through more robust packages including Microsoft 365 ("M365") tiers such as E3 and E5.¹

Any questions about licensing tiers, pricing, and suitability to Covered Entities and Business Associates can be discussed with an authorized Microsoft reseller or representative.

2. Microsoft Teams and HIPAA Requirements

Implementing the relevant requirements of HIPAA can be met through a combination of a policies, controls, and procedures that are developed to make sure that PHI and ePHI is not accessed, used, or disclosed in an unauthorized manner and that it is properly secured when not in use.



While this document is designed to assist customers on how to implement HIPAA requirements, customers should independently verify with their own legal counsel that their implementation meets all applicable HIPAA requirements.

¹ You may be wondering what the difference is between Microsoft 365 and Office 365, and where Microsoft Teams fits in. So long as you are using the business and enterprise versions of Microsoft Teams (not the home or consumer version), whether you license it through an Office 365 or Microsoft 365 suite, then the Microsoft HIPAA BAA would apply to the data you provide to Microsoft Teams for storage and processing. Microsoft 365 is a licensing SKU that itself includes the Office 365 suite of products like Microsoft Teams. See [Introducing Microsoft 365 | Microsoft 365 Blog](#) for more information.

2.1 HIPAA Administrative Safeguards

Microsoft Teams is a powerful collaboration tool for organizations that allows individuals to easily communicate and share information with one another. In addition to the technical guidance in this document, it is recommended customers take the following actions to implement Teams in a manner that supports the organization's compliance with HIPAA requirements:

- Evaluate whether Business Associate Agreements (BAAs) are in necessary with other organizations with whom PHI may be shared using Microsoft Teams.
- Perform workforce training to ensure personnel understand how to HIPAA requirements apply to their use Microsoft Teams when they are dealing with PHI.
- Conduct a HIPAA Security Rule Evaluation to understand the implications of implementing Microsoft Teams for the organization.
- Integrate the Evaluation into the enterprise HIPAA Risk Analysis and Risk Management Plan for the organization, for purposes of understanding and appropriately managing any risks related to Microsoft Teams.
- Update policies, procedures, and forms, as necessary, to address the access to, and use and disclosure of, PHI while using Microsoft Teams.
- Implement any additional administrative, technical, and physical controls that may be necessary for the organization, related to access to, and use and disclosure of, PHI while using Microsoft Teams.

2.1.1 Business Associate Agreements

To help customers comply with HIPAA requirements, the Microsoft HIPAA Business Associate Agreement is available by default through the Microsoft Online Services Data Protection Addendum to all customers who are Covered Entities or Business Associates.

For other entities with which the organization may be sharing PHI using Microsoft Teams, consider whether a Business Associate Agreement may be necessary.

2.1.2 Workforce Training

HIPAA requires that Covered Entities and Business Associates appropriately train their workforce members. While reasonable and appropriate access controls may limit the people, who have access to PHI, such controls may not necessarily prevent impermissible use or disclosure of PHI, such as taking screen shots, or copying data from labeled documents for purposes not permitted by the HIPAA Rules. Effective training is recommended to supplement controls and to implement organizational policies and procedures.

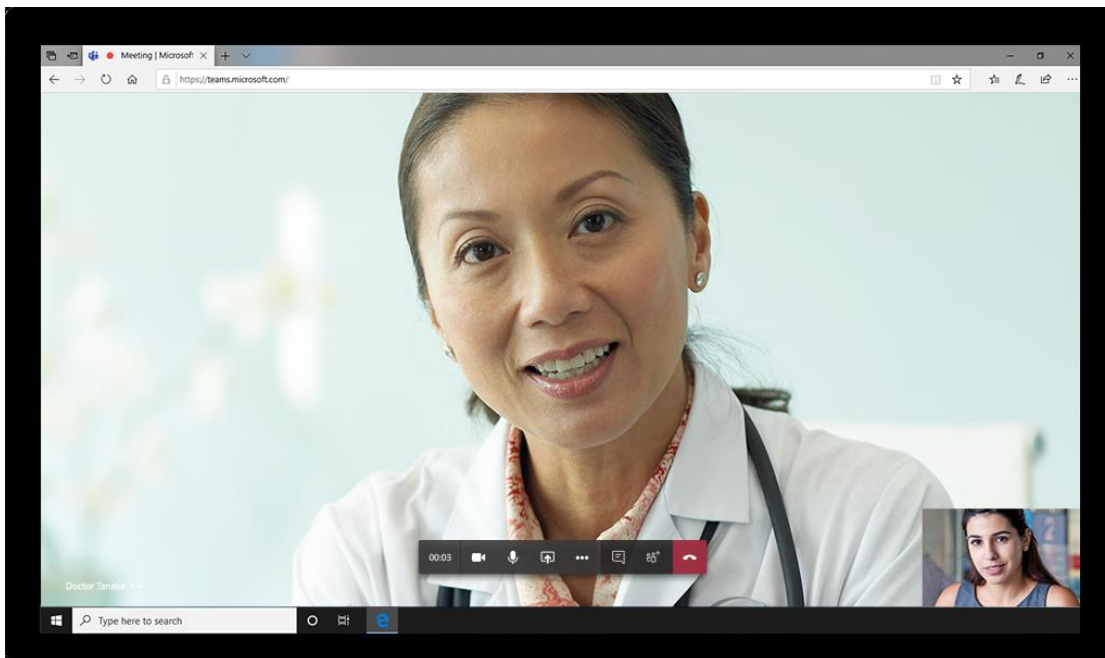
Training should be suited to the type of user (e.g., clinician or administrative staff) and include a variety of possible data sharing scenarios, such as:

- Communication within the organization between and among different groups (e.g., clinical and administrative communication, communication among clinicians, etc.),
- Communication with business associates or third-party organizations, and
- Communication between the clinician or care coordinator and the patient.

2.1.3 Considerations for addressing Microsoft Teams in Policies and Procedures

Updating the organization's policies, procedures, and forms can help with effective implementation of Microsoft Teams and can assist Covered Entities and Business Associates in assessing and implementing configuration options supported by Microsoft Teams. Policies and procedures can also be leveraged as the foundation for the workplace training. Key topics that may need to be included in updated policies and procedures include:

- ☐ Categorization of data and associated data retention policies
- ☐ Situations when PHI may be exchanged
- ☐ Storage location of PHI and other information
- ☐ Information access policies and controls
- ☐ External data sharing with business associates and other third-party entities
- ☐ Guest access to information
- ☐ Use of applications from the Microsoft Teams store
- ☐ Use of Microsoft Teams on mobile devices

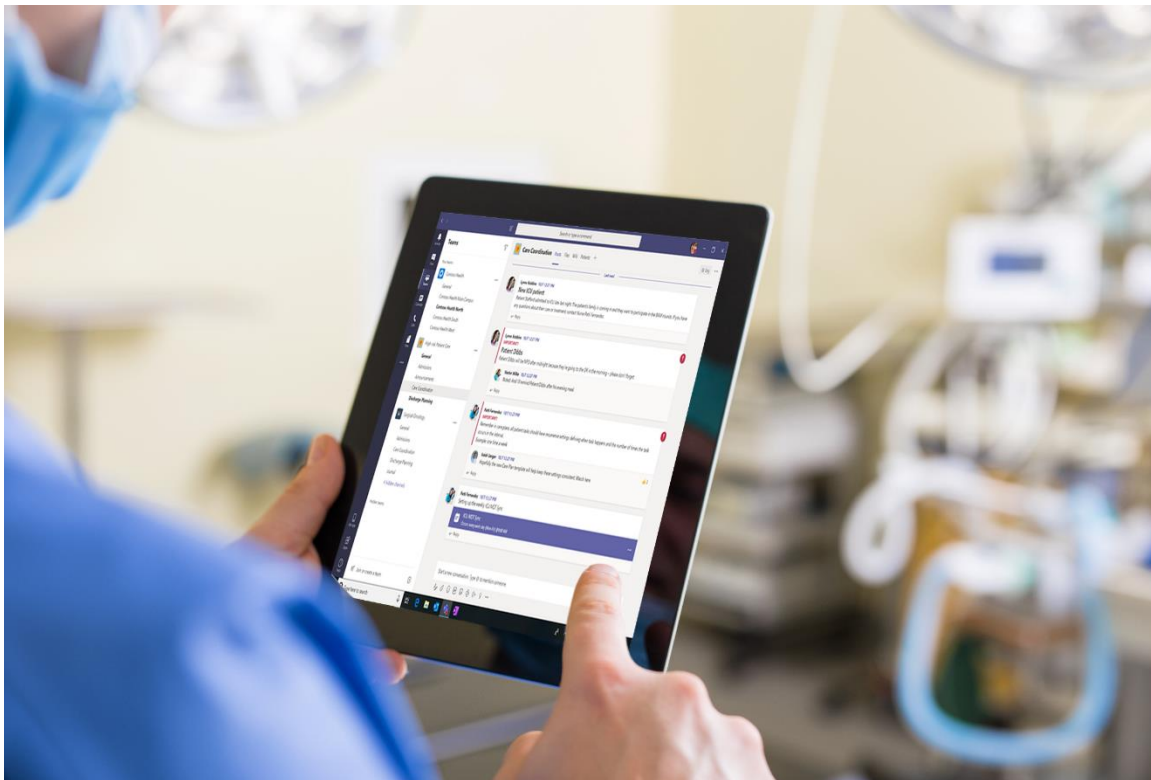


Below are considerations for policies and procedures on these topics.

2.1.3.1 Categorization of Data and Associated Data Retention Policies

As a collaboration platform, Microsoft Teams may retain PHI on behalf of Covered Entities and Business Associates. This PHI may be in the form of transcripts of messaging conversations, shared files, or other artifacts. Covered Entities and Business Associates should identify the categories of PHI and other sensitive or proprietary information it may obtain or share through Microsoft Teams. For each category, Covered Entities and Business Associates may wish to consider an appropriate data retention policy to ensure retrieval when required for legal retention obligations and deletion after a specified period of time. In addition, Covered Entities and Business Associates may wish to consider how and when such information may need to be imported or exported to an electronic health record (“EHR”) system or other component of a legal medical record.

As part of determining how long each type of data should be retained, Covered Entities and Business Associates may wish to consider maintaining a balance between compliance and auditability, while reducing concerns about storing and securing data indefinitely.



2.1.3.2 Identifying Situations Where PHI May Be Exchanged

Given regulatory requirements on use and disclosure of PHI,² Covered Entities and Business Associates should understand the situations in which PHI may be shared or exchanged using Microsoft Teams, including for purposes of implementing HIPAA requirements related to individual rights, such as access, amendment, and accounting of disclosures, and for workforce training on such requirements.

2.1.3.3 Storage Location of PHI and Other Information

Deciding where files may or may not be stored can determine how Microsoft Teams may be used to collaborate with other users—both internally and externally. Files that are shared within Microsoft Teams channels are stored on an underlying SharePoint Online instance in the M365/O365 environment.³ Covered Entities and Business Associates may wish to review their policies and procedures for PHI and determine what PHI can be shared via Microsoft Teams.

2.1.3.4 Information Access Policies and Controls

Consistent with the HIPAA Privacy Rule's standard limiting uses and disclosures of PHI to the "minimum necessary," the HIPAA Security Rule requires Covered Entities and Business Associates to document and implement policies and procedures for authorizing access to electronic PHI only when the access is appropriate based on the user or recipient's role (this type of access controls is called "role-based access"),⁴ and, more generally, to provide access to PHI to individuals and entities, only as permitted by the HIPAA Rules.

Data loss prevention procedures may also be useful to ensure that PHI is not lost, misused, or accessed by unauthorized users. Working in tandem with information access policies, these should include regular monitoring of PHI use and disclosure through Microsoft Teams to identify areas where PHI may have been inappropriately disclosed to prevent future occurrences through the same channels.

Additionally, defining what is allowed for search returns based upon PHI labels can help ensure that users can find only the data that they are authorized to view. The process of defining the search filters could involve the use of data labels which are mapped to the user groups who can view the data. These will assist with prevention of unauthorized use or disclosure as the user performing the search will not even know that certain files are present on the system. For more details on data labels, please refer to [Sensitivity labels for Microsoft Teams - Microsoft Teams | Microsoft Docs](#).

² 45 C.F.R. § 164.502(a)

³ For more information, see [Location of data in Microsoft Teams | Microsoft Docs](#).

⁴ 45 C.F.R. § 164.308(a)(4)(i)

2.1.3.5 Guest Access to Information

Microsoft Teams allows for guest access to be provided for users who do not have an account with the Covered Entity or Business Associate. Covered Entities and Business Associates may wish to consider to whom they would like to provide guest access, such as patients, whether such access is permitted by the HIPAA Rules, how best to provide instructions on use of Microsoft Teams, and how to revoke access as soon as possible when it is no longer necessary. As such, Covered Entities and Business Associate may wish to include guest user access as part of their information access policies.

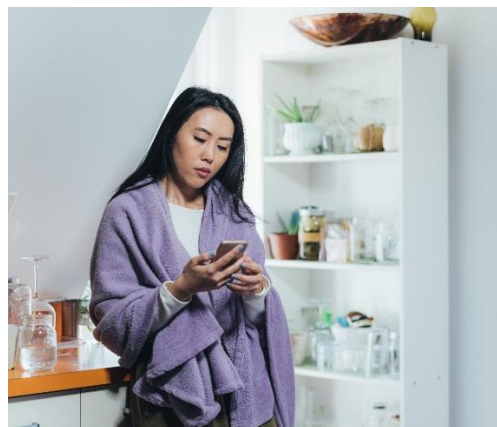
Considerations for this type of access include determining how the user may assert their identity in a validated way to allow for PHI sharing and how to prevent information sharing with guest accounts. Guests should be added within the Azure Active Directory administration portal and guest permissions can be limited using controls within Azure Active Directory or Microsoft Teams. For details on guest access, please refer to [Collaborate with guests in a Team–Microsoft Teams | Microsoft Docs](#). For details on preventing information sharing within Microsoft Teams, refer to [Information barriers in Microsoft Teams– Microsoft Teams | Microsoft Docs](#).

2.1.3.6 Use of Applications from the Microsoft Teams Store

Users may enhance their Microsoft Teams experience through applications available in the Microsoft Teams Store. Covered Entities and Business Associates may wish to revise their policies and procedures to address whether Microsoft Teams-related applications may be added into Microsoft Teams and, if so, what applications are approved for use and/or what additional organizational requirements apply to requests for additional applications.

2.1.3.7 Use of Microsoft Teams on Mobile Devices

Covered Entities and Business Associate may wish to determine whether Microsoft Teams may be used by authorized users on mobile devices. The Covered Entities' and Business Associates' policies and procedures for the use of mobile devices may need to include the types of mobile devices that are appropriate when using Microsoft Teams (phone, tablet, etc.), and the types of security controls that may be necessary on the mobile device for access to PHI using Microsoft Teams.



2.2 Technical Safeguards

Covered Entities' and Business Associates' policies and procedures and the controls implemented pursuant to those policies and procedures may need to be revised to include the technical controls that are supported within Microsoft Teams. The following technical safeguards can be considered as part of a Covered Entity's or Business Associate's implementation of Microsoft Teams:

- ☐ **Identity Management:** Identity management safeguards address adding users to the Microsoft Teams instances and underlying channels. Covered Entities and Business Associate may need to include registration (including identity validation) and removal of users from individual channels or teams based on changes in job role or relationship with Covered Entities or Business Associates. For further details, see section 2.2.1 below.
- ☐ **Authentication:** Authentication safeguards include determining who can have access to what data within the Microsoft Teams environment and allowing adherence to the principle of least privilege. This feature area includes adding users to access channels, file permissions, and creation of confidential channels. For further details, see section 2.2.2 below.
- ☐ **Data Classification:** Data classification controls allow Covered Entities and Business Associates to identify PHI and help facilitate the use of automation and data loss protection technologies to prevent unauthorized disclosure. For further details, see section 2.2.3 below.
- ☐ **Non-HIPAA Data Management Considerations:** Data management safeguards assist Covered Entities and Business Associates to address retention and disposal of data, which are an important part of any data security program. For further details, see section 2.2.4 below.
- ☐ **Monitoring User Activity:** Monitoring and auditing user activity helps Covered Entities and Business Associates identify inappropriate use or handling of PHI. For further details, see section 2.2.5 below.
- ☐ **Ongoing Assessment and Internal Validation:** Validating compliance with controls and standards for configurations as well as the periodic review of user accounts and access are utilized for audit readiness. For further details, see section 2.2.6 below.

2.2.1 Identity Management Controls



Identity management controls help make sure that identities provided with access to Microsoft Teams are appropriate and necessary. The standard lifecycle for identities passes through three phases, including the joiner (new identity), mover (updates to existing identities), and leaver (termination of an identity). Covered Entities and Business Associates may develop a more granular set of lifecycle states that include statuses such as active, leave of absence, inactive, terminated, and others.

For the purposes of the identity management controls, three types of users are listed below.

Regular users: These users are verified by the Covered Entities' or Business Associates' onboarding processes and maintained within the local Azure Active Directory ("Azure AD") instance supporting Microsoft Teams. Regular users may include internal personnel, external personnel including Business Associates, and even customers or patients depending on the policies and procedures of the Covered Entities and Business Associates.

Federated users: These users are maintained within another organization's directory service—for example, at a Business Associate—and the user authentication on those systems is trusted by the Covered Entities' or Business Associates' systems. This is common within business-to-business ("B2B") type relationships when Covered Entities or Business Associates do not want to maintain the user information internally, but only the access granted to it.

Guest users: These users are granted access to Microsoft Teams using an external public directory service, for example, a user who is identifying themselves using their Outlook, Gmail, or Yahoo email addresses. In this case, the user created the account themselves and are asserting that identity to the Covered Entities or Business Associates.

The following controls relate to identity management:

- Creation of regular user accounts
- Maintenance of regular user accounts
- Deprovisioning of regular user accounts
- Federated users
- Guest users

2.2.1.1 Creation of Regular User Accounts

User accounts for Microsoft Teams are maintained within an instance of Azure AD. The available features vary depending on the type of licensing purchased.

The base licensing for Microsoft Teams via O365 provides an interface to manually add users through the O365 administration tools. Users can be added to an Azure AD instance with a limited feature set, optimized for those Covered Entities and Business Associates looking for Office support.

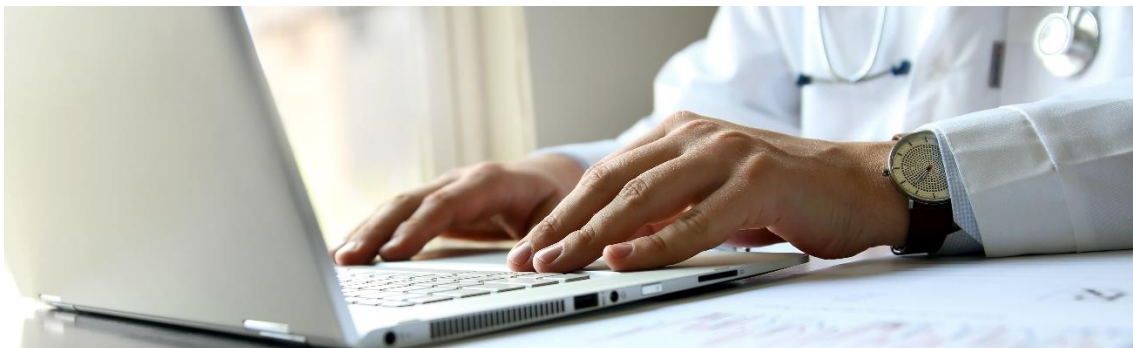
Automation of user account management ranges from the synchronization of accounts from the on-premises Active Directory, through use of a complete identity and access management (IAM) synchronization tool that can collect user data from multiple sources to provision users as well as manage group memberships based on user identity information (assisted in Authorization, discussed later). This will help users get set up within the environment and configured with permissions to access different channels.

Note that HIPAA requires unique identifiers be maintained for users, so that appropriate activity tracking can be regularly reviewed and audited. The use of automation simplifies the generation and tracking of the unique IDs—the email address for O365. It may also be used to create a master list of addresses assigned to a user throughout their lifecycle in cases where policies may allow primary email address changes (*e.g.*, an employee gets married and opts to take on their spouse's last name).

2.2.1.2 Maintenance of Regular User Accounts

The ongoing maintenance of the user accounts is important to help ensure that individuals can readily identify to whom they are talking.

If Covered Entities' and Business Associates' policies and procedures allow, some changes may result in a new primary email address for particular users. The process of assigning new addresses can be managed as part of the ongoing maintenance of the accounts. Past email addresses may either be added as aliases to the original assignee or not reassigned for a period defined in Covered Entities and Business Associates' policies and procedures. This process of retaining aliases or preventing reassignment will assist in preventing an unauthorized user from receiving PHI.



2.2.1.3 Deprovisioning of Standard User Accounts

Disabling or removing user accounts when a user no longer requires the access or has been terminated is important to prevent access abuse. The processes here will be determined by the Covered Entities' or Business Associates' policies and procedures.

If the accounts are manually managed in the Azure AD, the processes for notifying the appropriate IT Team to disable or remove the account may need to be established in association with the Covered Entities' or Business Associates' policies and procedures.

As with the provisioning and maintenance of the user accounts, automation may be used whenever possible. If a particular Covered Entity or Business Associate is using on-premises Active Directory, the Azure AD Connect should be deployed to automate the disabling of the user accounts used by Microsoft Teams.

Robust synchronization tools (including the deployment of the Azure Synchronization Engine) will aid in tying the accounts back to authoritative sources (e.g., the Human Resources database) to align the user account status with current employment status.



2.2.1.4 Federated Users

If Covered Entities and Business Associates allow the use of federated users, they have agreed to trust/utilize the Business Associates' or other external organizations' identity management processes. In these scenarios, the identities are asserted via the federation agreement to the Microsoft Teams instance during authentication. Access controls would be based on the assertions within the identity data presented during authentication.

If Business Associates are authorized to use federated identities for authentication, it is critical that the identity management processes used to maintain those identities are verified and Covered Entities' or original Business Associates' requirements for identity verification are included in any applicable Business Associate Agreements.

2.2.1.5 Guest Users

Covered Entities and Business Associates may allow users to assert their identity through a public identity provider. In these cases, the Covered Entities and Business Associates may wish to consider methods to verify the identity of the user behind the identity before granting any access to Microsoft Teams. Depending on Covered Entities' or Business Associates' risk appetite, they may opt to have users register directly so that the Covered Entity's or Business Associate's internal identity management processes are utilized to verify the identities.

If the decision is made to use guest users, care should be taken to establish boundaries as to what types of information, including PHI, may be shared in policies and procedures addressing guest user access.

Microsoft Teams provides policy-based configuration options to control the functions and features that guest users are authorized to use.

2.2.2 Authentication Control



Microsoft Teams allows for a variety of different authentication techniques. These range from the basic username and password to more advanced features, including multifactor authentication and federation.

2.2.2.1 Integrated Single Sign-On

The use of integrated single sign-on ("SSO") is common for users who are already logged into internal systems using their Azure AD credentials. In this scenario, the authentication occurred when the user logged into their domain-joined workstation. Access to Microsoft Teams is simply facilitated by the native SSO capabilities built into the Azure Active Directory. SSO is an ideal mechanism for internal users, as it eliminates the need to reauthenticate each time Microsoft Teams is used.

2.2.2.2 Username and Password

The HIPAA Security Rule generally requires the use of passwords for authentication of users into an environment. For Microsoft Teams, the minimum password complexity required is 8 characters with a mix of upper- and lower-case characters, numbers, and special characters. This is supported by the underlying Azure AD instance and can be configured to require more stringent requirements, depending on the Covered Entities' or Business Associates' password policies.

2.2.2.3 Multifactor Authentication

Multifactor authentication is based on the "security-in-depth" principle. It requires that a user authenticate using two or more of the following factors

- **Something the user knows**—This is generally their password, PIN, or other memorized data they enter when logging into a system.
- **Something the user has**—Tokens, smartcards, and security keys are all something the user may physically possess and present to the system via ports on the computer or specialized hardware.
- **Something they are**—This factor refers to biometric data, such as fingerprints, retinal scanners, facial recognition (*e.g.*, Windows Hello for Business).
- **Something they do**—This refers to behavior patterns, such as how a user types a given string. For example, a user may type "The quick brown fox jumps over the lazy dog" within a certain timespan, pause at different key combinations, use the right or left shift keys, etc.

The use of multifactor authentication can provide a higher confidence that the user who has logged into Microsoft Teams is really the account owner. If the Microsoft Teams instance is being used to discuss and exchange large amounts of PHI, multifactor authentication should be considered. Microsoft Azure AD supports the traditional voice call and SMS messages for receiving a passcode, but also provides other options including Windows Hello for Business, Microsoft Authenticator applications, FIDO2 security key, OATH hardware tokens, and OATH software tokens.

The policies and procedures defining the authorization requirements for internal users, privileged users, business associate users, and other external users should clearly define whether multifactor authentication is required by Covered Entities or Business Associates.

2.2.2.4 Password-less Authentication

The use of password-less authentication has become more popular because it simplifies the sign in process for users and does not require the memorization of complex passwords. Many of the mechanisms that are allowed as the second step in multifactor authentication may also be used as primary authentication methods. These include Windows Hello for Business, the Microsoft Authenticator App, FIDO2 security keys, and SMS messages.

Workforce members responsible for implementation of HIPAA Rules' requirements should review any decisions regarding password-less authentication to ensure a proper risk assessment is completed prior to adoption. It would be up to the Covered Entities or Business Associates using these methods to prove the password-less security methods were properly vetted before being put in service over regular username and password authentication.

2.2.2.5 Federation

Federation allows a user's identity from a trusted organization to be asserted to multiple other systems across security domains. At a high level, the identity information is asserted to the Covered Entities or Business Associates via an agreed upon method. The assertion contains information about who the user is and any other authorization data that needs to be shared with the Covered Entities or Business Associates.

One of the key benefits of federation is that Business Associates of Covered Entities and Business Associates are responsible for their own identity management, instead of the Covered Entities or original Business Associates. However, the Covered Entities and Business Associate may wish to complete appropriate due diligence and ensure the identity management practices of the business associate are acceptable and include these requirements in any Business Associate Agreements.

2.2.3 Data Classification



The creation and use of a proper data classification model can help users know the type of data they are accessing and enable technology to prevent unauthorized disclosures, whether accidental or intentional. Covered Entities and Business Associates may decide to classify or identify data in such a way that the minimum necessary standard could be reasonably enforced.

The boundaries of how data is classified will allow use of "information barriers", which can be used to prevent PHI from being inappropriately shared between different groups, for example, someone trying to send clinical data to personnel who should not view or access such information.

2.2.4 Non-HIPAA Data Management Considerations



Data management focuses on the security “CIA” triad—Confidentiality, Integrity and Availability. Confidentiality means the appropriate security is being provided to data so only those who should have access do and the privacy of the data is protected.

Integrity means that the data should only be created and modified by those with appropriate permissions, and thus, can be relied upon by users. Availability means that data is in a place and accessible pursuant to access rights established for those who need it.

Covered Entities and Business Associates may wish to consider the following areas of data management:

- Access rights and permissions
- Data retention controls
- Legal hold requirements

2.2.4.1 Access Rights and Permissions

Data classifications helps ensure that the access rights to the data are appropriate to allow users who should have access and block users who should not. Using data classifications, rather than file structures or individual file-based permissions, simplifies access to a classification category.

2.2.4.2 Data Retention Controls

Data retention controls define how long data may be retained within a system. If data is retained for too long of a period, Covered Entities and Business Associates may increase their exposure if a breach occurs and may incur increased costs for data archival and storage.

2.2.4.3 Legal Hold Requirements

2.2.5 Monitoring User Activity



Monitoring user activity is an important component of any data security program. The logs of user activity can be used to show implementation of applicable HIPAA requirements by Covered Entities and Business Associates. Additionally, it also allows for investigations into breaches or misuse of PHI by individuals or groups.

Microsoft Teams provides features for monitoring through user active logs and Azure AD’s security events (see, e.g., Section 3.8. “Security Monitoring” below, [Azure Active Directory reports and monitoring documentation | Microsoft Docs](#), and [Microsoft 365 auditing solutions - Microsoft 365 Compliance | Microsoft Docs](#)).

2.2.6 Ongoing Assurance and Internal Validation



Part of a Covered Entity's or Business Associate's compliance activities may include regular and ongoing assurance and validation that defined policies are followed and that subordinate controls have been implemented with fidelity.

The assurance testing and review process should include:

- User account and access reviews
- Data classification validation
- Configuration auditing

2.2.6.1 User Account and Access Reviews

Reviews of user accounts and their assigned access demonstrate that identity management and user access processes are working correctly. Regardless of whether automation or manual processes are used, the process of collecting and reviewing documentation that the processes used follow documented internal processes and controls can be critical to present effectiveness evidence to auditors for internal purposes and/or external attestations and certifications.

User account reviews can be conducted by comparing the list of active personnel to the list of active accounts with access to the Microsoft Teams site. Use of identity management automation tools simplifies this process. The managed accounts can be validated by showing proof the automation is operating correctly in creating, updating, and terminating accounts based on defined events from authoritative identity data sources (for example, human resources data for employees).

Covered Entities and Business Associates may wish to consider using the access review certifications provided with Azure AD. This simplifies the creation and management of the certification process, making the review consistent during each execution.

2.2.6.2 Data Classification Validation

Covered Entities and Business Associates may wish to undertake testing to help ensure that data classifications are appropriately assigned, and access permissions are correctly applied. In these cases, selection of random documents with different contents may be reviewed to test that they have been flagged to the appropriate classifications.

To confirm that classification assignments are working correctly, access controls operating on the labels should be tested by going through scenarios where data are both accessible and not accessible. This helps ensure that both positive and negative cases are operating correctly. These tests should cover the data classification levels that are in use.

2.2.6.3 Configuration Auditing

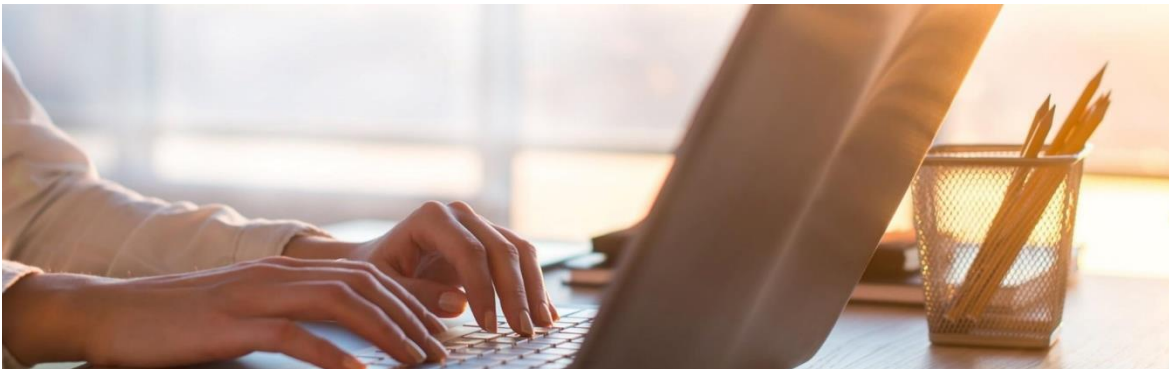
Use of a configuration management tool is ideal, but if the Microsoft Teams settings are manually configured, it is important to review them on a periodic basis to ensure they have not been changed from the expected baseline. Any changes in the configuration should be explored to help ensure they are properly documented and did not compromise the overall security and compliance needs of Covered Entities and Business Associates.

2.3 Handling Security Incidents

The HIPAA Security Rule requires the implementation of policies and procedures to address “security incidents,” which include any attempted or unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Unauthorized access to Microsoft 365 infrastructure systems and exfiltration of customer data may constitute a successful security incident under HIPAA.

Whenever there is a successful security incident, Microsoft 365 strives to respond quickly and effectively to protect Microsoft 365 services and customer data in accordance with the Business Associate Agreement between Microsoft and the Covered Entity or Business Associate.

The Covered Entity or Business Associate will want to review how its broader organizational policies and procedures appropriately take into consideration the shared responsibility model for Microsoft Teams.



3. Key Microsoft Teams Configuration Considerations

The key Microsoft Teams configuration areas that will help achieve implementation of HIPAA requirements include:

- Smart logout
- Password standards
- Authentication methods
- Multifactor authentication ("MFA")
- Least privilege
- Password reset
- User registration and deletion
- Security monitoring
- Policy-based recording for calls and meetings
- eDiscovery and legal hold
- Classify and protect sensitive information
- Data retention and deletion
- Enforce company approved products lists
- Auditable events and content
- Role management
- Information barriers

3.1 Smart Lockout

Smart lockout is a built-in Azure AD feature that makes guessing a password through password spray attacks more difficult.

Smart lockout can be configured by navigating to the **Azure Active Directory > Security > Authentication methods > Password protection** as shown in Figure 1. For more in-depth information regarding smart lockout, refer to [Prevent attacks using smart lockout–Azure Active Directory | Microsoft Docs](#).

For auditing and reporting such events, it is recommended to enable Security Audit Events in Azure AD as detailed in [Enable security audits for Azure AD Domain Services | Microsoft Docs](#).



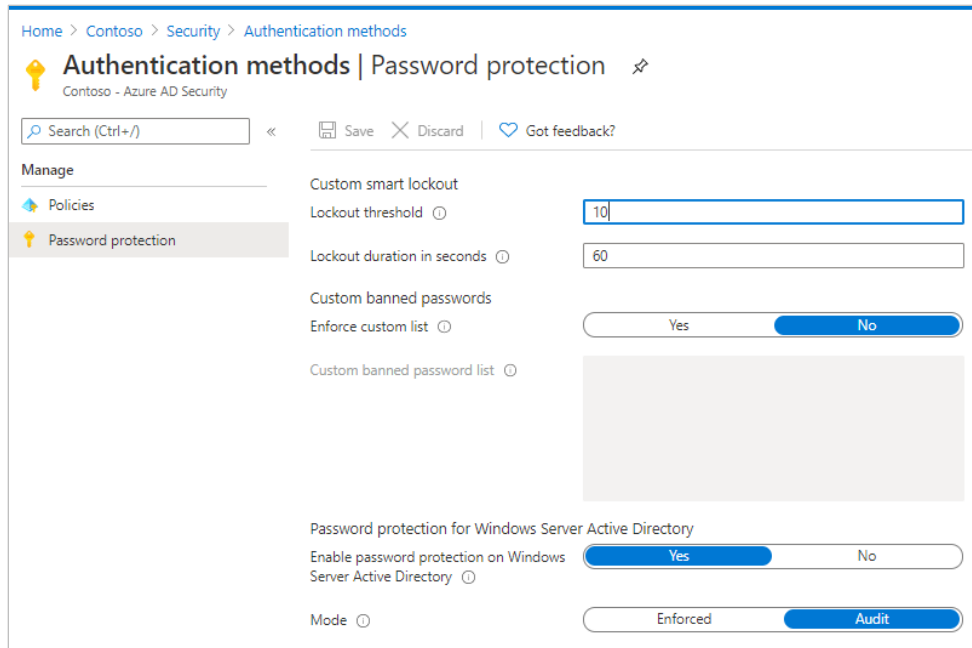


Figure 1: Smart lockout settings in Azure Active Directory

3.2 Password Standards

Password standards have very subtle pros and cons, and it is best to regularly educate users about password hygiene. Microsoft has published Password guidance in [Microsoft Password Guidance-1.pdf](#). Some of the Azure AD password settings cannot be modified. Details on which settings can or cannot be configured are provided in [Self-service password reset policies–Azure Active Directory | Microsoft Docs](#). Refer to the **Mapping Controls to Licensing** section for additional details.

3.3 Authentication Methods

Azure AD provides various authentication methods to reduce the likelihood of unauthorized access due to lost or stolen devices. Authentication methods can be configured by navigating to the Azure Active Directory > **Security** > **Authentication methods** as shown in Figure 2. For more in-depth information regarding authentication methods, please refer to [Authentication methods and features–Azure Active Directory | Microsoft Docs](#).

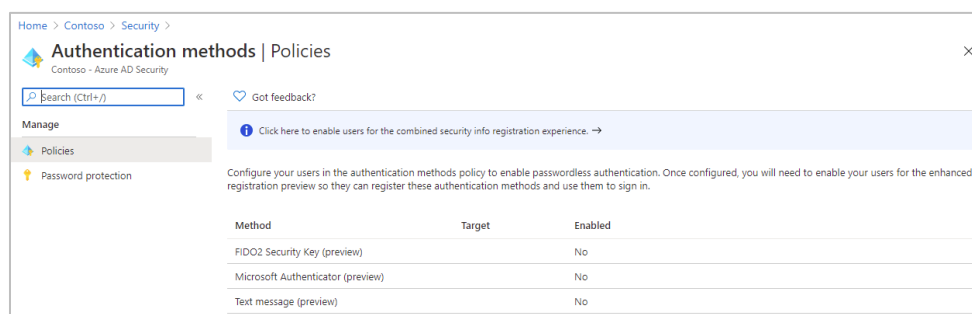


Figure 2: Authentication methods in Azure Active Directory

3.4 Multifactor Authentication (“MFA”)

Azure AD MFA helps safeguard data and applications by requiring a second form of authentication during sign in. MFA can be configured by navigating to the **Azure Active Directory > Security > MFA** as shown in Figure 3. More in-depth information regarding MFA is provided in [Azure AD Multi-Factor Authentication overview | Microsoft Docs](#).

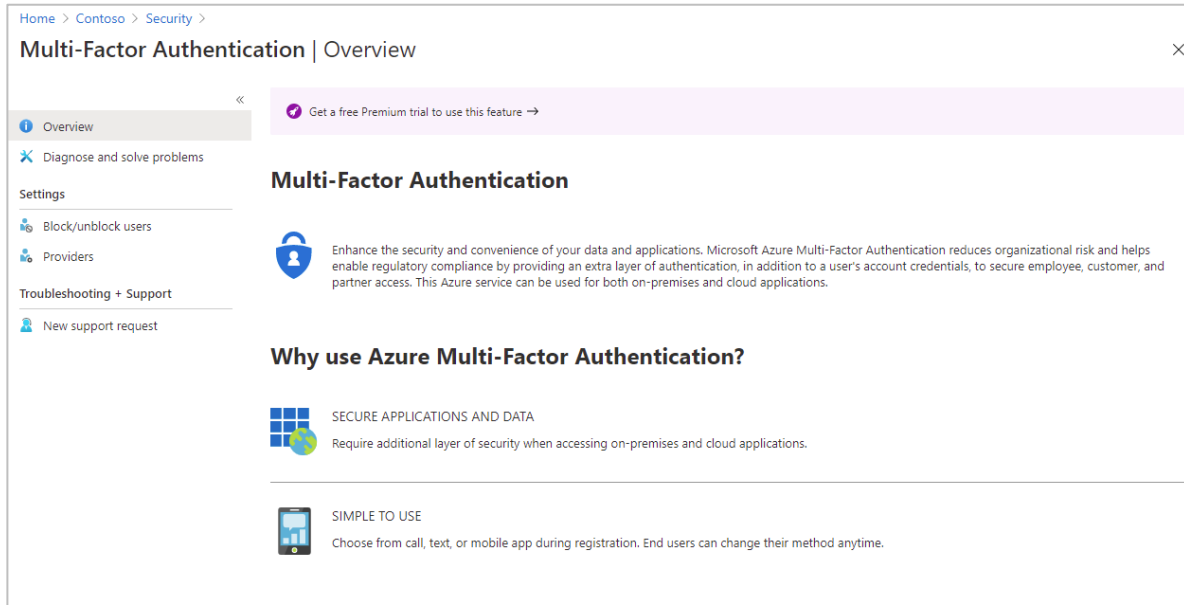


Figure 3: Multifactor authentication settings in Azure Active Directory

For more granular controls, Conditional Access policies can be used to define events or applications that require MFA. Based on a Covered Entities' and Business Associates' policies and procedures, the following factors can be evaluated before access is granted or denied:

- Group membership
- User's sign in location
- Sign in risk
- Device compliance status
- Application type
- Legacy authentication
- MFA status

Conditional Access can be configured by navigating to the **Azure Active Directory > Security > Conditional Access** as shown in Figure 4. Details are provided in [Building a Conditional Access policy–Azure Active Directory | Microsoft Docs](#).

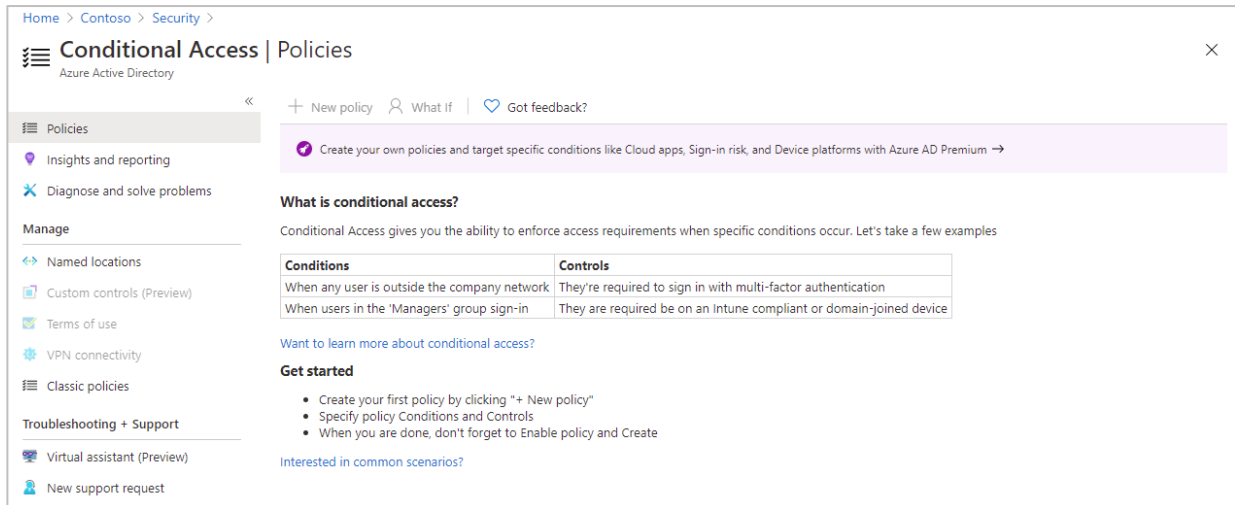


Figure 4: Conditional access policy settings in Azure Active Directory

3.5 Least Privilege

Least privilege is one of the security principals in Microsoft's [Best practices for Azure RBAC | Microsoft Docs](#). It states that assignment of least privileges required to a user to accomplish a task. Covered Entities and Business Associates can see available roles by navigating to the **Azure Active Directory > Roles and administrators**. For assigning specific roles to a user or group, click on a role, choose assignments, and add assignments as shown in Figure 5.

Microsoft has published a task-by-privilege chart in [Delegate roles by admin task–Azure Active Directory | Microsoft Docs](#).

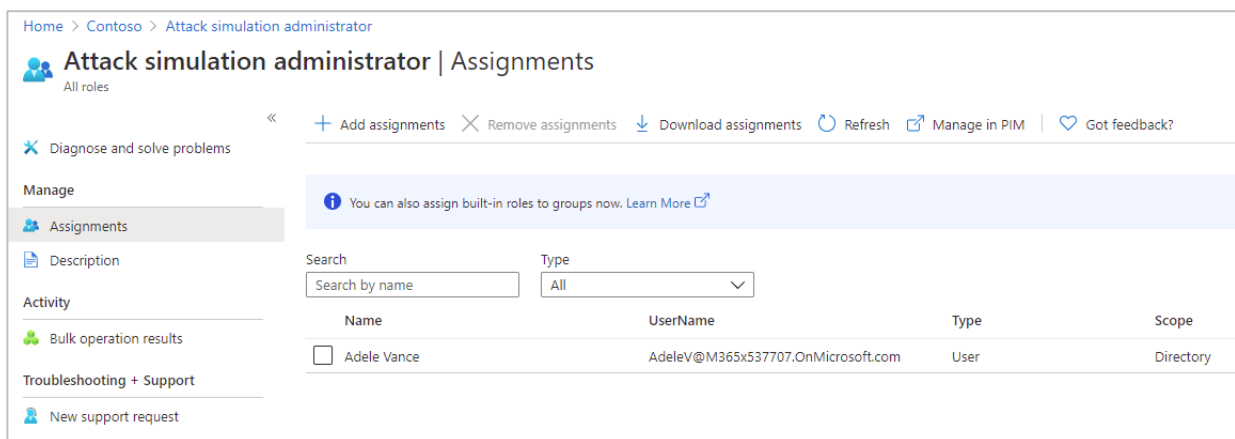


Figure 5: Assigning least privilege roles to users/groups in Azure Active Directory

3.6 Password Reset

Self-service password reset ("SSPR") is an Azure AD feature that allows users to reset their passwords without involving the IT help desk. SSPR can be configured by navigating to the **Azure Active Directory > Password reset** as shown in Figure 6.

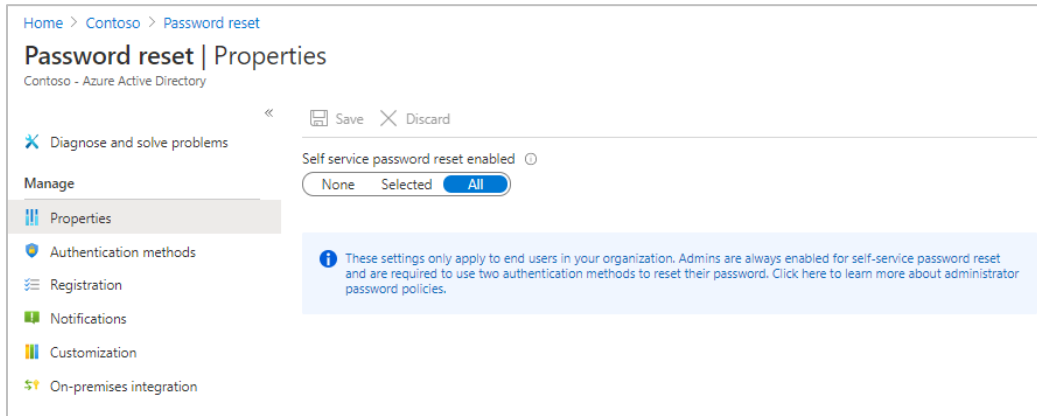


Figure 6: Password reset settings in Azure Active Directory

Users must be registered for SSPR before they can change their password. This registration activity is usually done via an organization-wide campaign. Once registered, a user can navigate to <https://aka.ms/sspr> and reset their password. SSPR prompts the user to enter a user ID and pass a captcha. Azure AD now verifies that the user can use SSPR by doing the following checks:

- The user has SSPR enabled and is assigned an Azure AD license.
- The user has the right authentication methods defined on their account in accordance with administrator policy.
 - If the policy requires only one method, confirm the user has the appropriate data defined for at least one of the authentication methods enabled by the administrator policy.
 - If the policy requires two methods, confirm the user has the appropriate data defined for at least two of the authentication methods enabled by the administrator policy.
 - If an Azure administrator role is assigned to the user, then the strong two-gate password policy is enforced. For more information, see [Administrator reset policy differences](#).
- The user's password is managed on-premises in cases where the Azure AD tenant is using federated, pass-through authentication, or password hash synchronization:
 - If SSPR writeback is configured and the user's password is managed on-premises, the user can proceed to authenticate and reset their password.
 - If SSPR writeback isn't deployed and the user's password is managed on-premises, the user is asked to contact their administrator to reset their password.

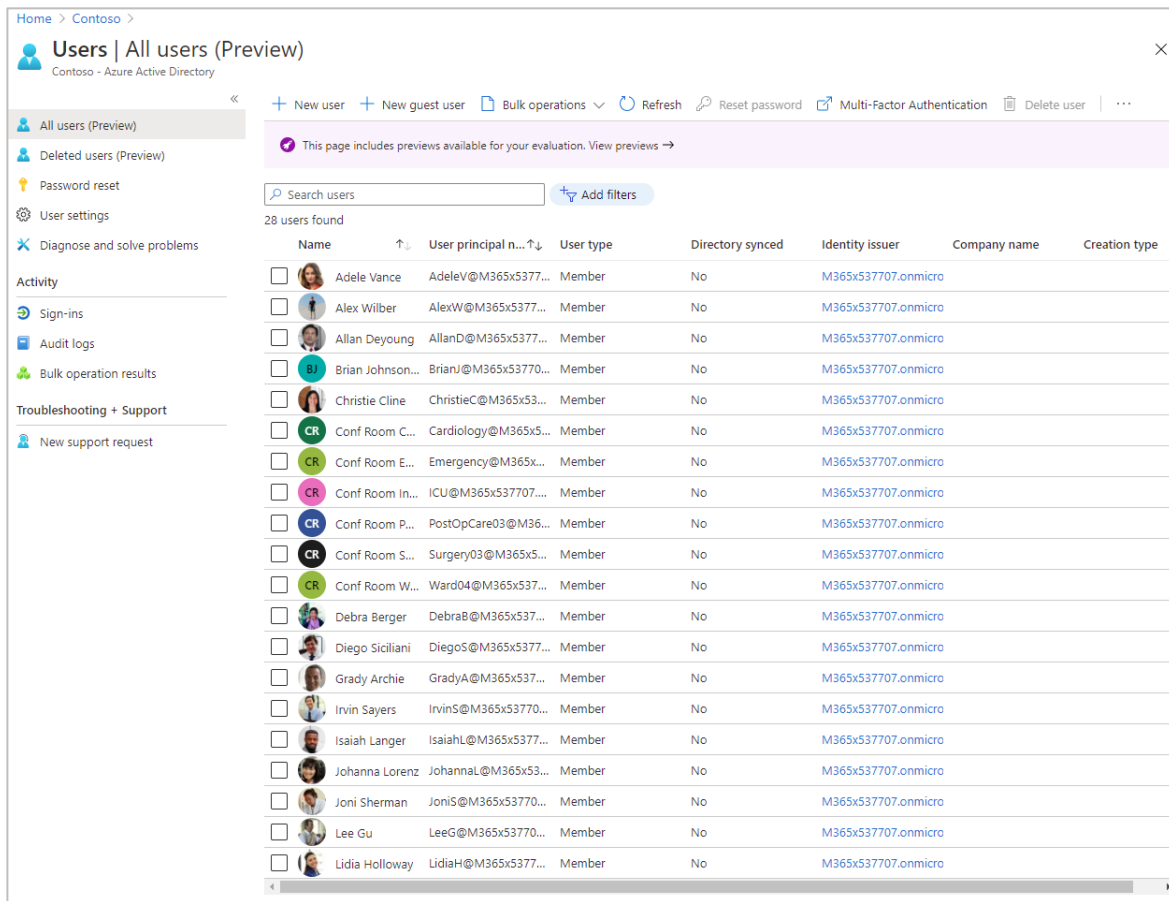
If all the previous checks are successfully completed, the user is guided through the process to reset or change their password.

More details on SSPR are provided in [Self-service password reset deep dive–Azure Active Directory | Microsoft Docs](#).

3.7 User Registration and Deletion

Users can be created and deleted manually in Azure AD by navigating to the **Azure Active Directory > Users** and selecting New user or Delete user for single users or by choosing bulk operations for multiple users, as shown in Figure 7. Covered Entities and Business Associates can use synchronization tools like Azure AD Connect to provision and deprovision accounts using on-premises AD in the case of hybrid deployment.

For more details on how to create and delete users in Azure AD, refer to [Add or delete users– Azure Active Directory | Microsoft Docs](#).



The screenshot shows the 'Users | All users (Preview)' page in the Azure Active Directory portal. The left sidebar contains navigation links: All users (Preview), Deleted users (Preview), Password reset, User settings, Diagnose and solve problems, Activity, Sign-ins, Audit logs, Bulk operation results, Troubleshooting + Support, and New support request. The main area displays a table of 28 users. At the top of the main area, there are buttons for 'New user', 'New guest user', 'Bulk operations', 'Refresh', 'Reset password', 'Multi-Factor Authentication', and 'Delete user'. A search bar and 'Add filters' button are also present. A purple banner states: 'This page includes previews available for your evaluation. View previews →'. The table has columns for Name, User principal name, User type, Directory synced, Identity issuer, Company name, and Creation type. The first few rows show users like Adele Vance, Alex Wilber, Allan Deyoung, Brian Johnson, and Christie Cline. The last row shows Lidia Holloway.

	Name	User principal n...	User type	Directory synced	Identity issuer	Company name	Creation type
<input type="checkbox"/>	Adele Vance	AdeleV@M365x5377...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Alex Wilber	AlexW@M365x5377...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Allan Deyoung	AllanD@M365x5377...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Brian Johnson...	BrianJ@M365x53770...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Christie Cline	ChristieC@M365x53...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Conf Room C...	Cardiology@M365x...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Conf Room E...	Emergency@M365x...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Conf Room In...	ICU@M365x537707...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Conf Room P...	PostOpCare03@M36...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Conf Room S...	Surgery03@M365x5...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Conf Room W...	Ward04@M365x537...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Debra Berger	DebraB@M365x537...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Diego Siciliani	DiegoS@M365x5377...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Grady Archie	GradyA@M365x537...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Irvin Sayers	IrvinS@M365x53770...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Isaiah Langer	IsaiahL@M365x5377...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Johanna Lorenz	JohannaL@M365x53...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Joni Sherman	JoniS@M365x53770...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Lee Gu	LeeG@M365x53770...	Member	No	M365x537707.onmicro		
<input type="checkbox"/>	Lidia Holloway	LidiaH@M365x5377...	Member	No	M365x537707.onmicro		

Figure 7: Users list in Azure Active Directory

3.8 Security Monitoring

The reporting architecture in Azure AD consists of the following security monitoring components:

- **Activity Reporting**
 - **Sign-ins**—[Sign-ins](#) provides information about when users, applications, and managed resources sign in to Azure AD and access resources.
 - **Audit logs**—[Audit logs](#) provide system activity information about users and group management, managed applications, and directory activities.
- **Security Reporting**
 - **Risky sign-ins**—A [risky sign-in](#) is an indicator for a sign-in attempt by someone who isn't the legitimate owner of a user account.
 - **Users flagged for risk**—A [risky user](#) is an indicator for a user account that might have been compromised.

Azure AD audit events can be enabled by navigating to the **Azure AD Domain Services > Diagnostic settings** as shown in Figure 8. For more details, please refer to [Enable security audits for Azure AD Domain Services | Microsoft Docs](#).

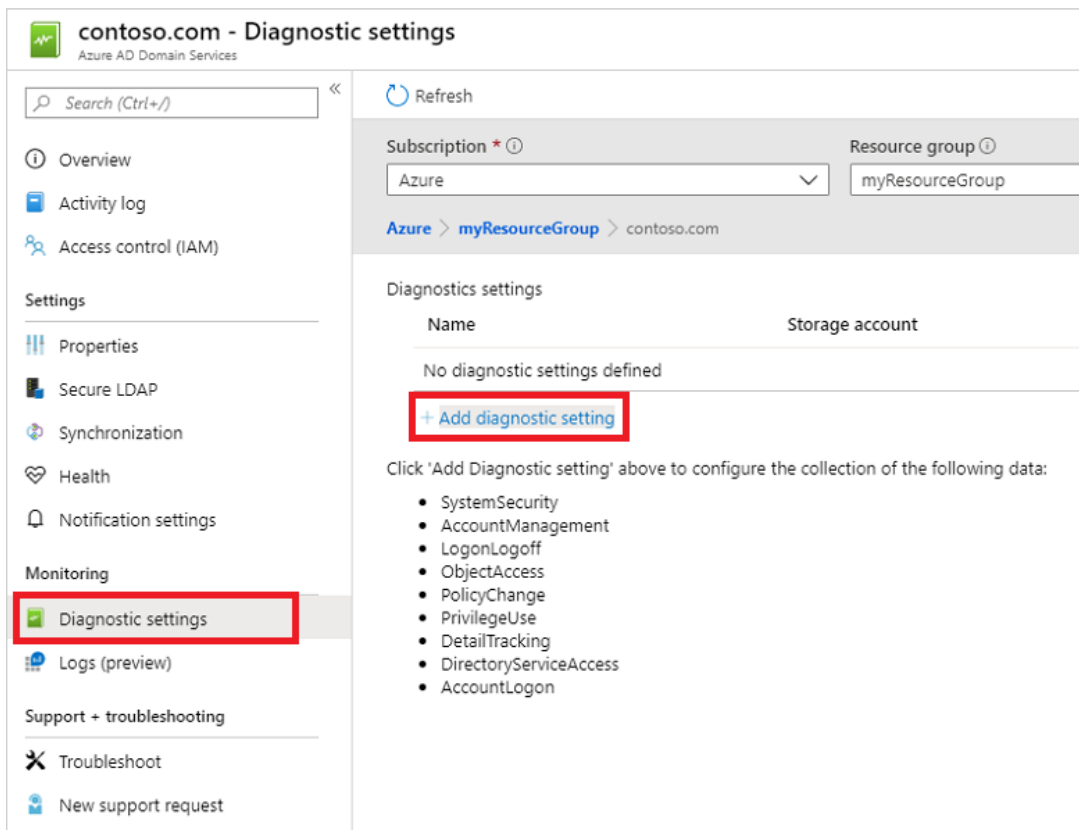


Figure 8: Monitoring and diagnostic settings in Azure Active Directory

3.9 Configuring Communications Policies to Help Foster Culture of Safety and Inclusion

Communication compliance is a solution in Microsoft 365 that can help minimize communication risks by helping to detect, capture, and act on inappropriate messages within communications tools such as Microsoft Teams used by Covered Entities and Business Associates. By configuring pre-defined and/or custom communications policies through the in-built functionality in communications compliance, the following types of inappropriate content in Microsoft Teams Chat and Channel messages can be identified: offensive, profane, and harassing language; adult, racy, and gory images; and sharing of sensitive information. Communication compliance policies define which communications and users are subject to review in an organization, define which custom conditions the communications must meet, and specify who should do reviews.

Microsoft Teams' administrators can configure communication compliance policies at User level or at Microsoft Teams level. Communication compliance can be configured by navigating to **compliance.microsoft.com > Communication compliance** as shown in Figure 9.

For more details, please refer to [Learn about communication compliance—Microsoft 365 Compliance | Microsoft Docs](#).

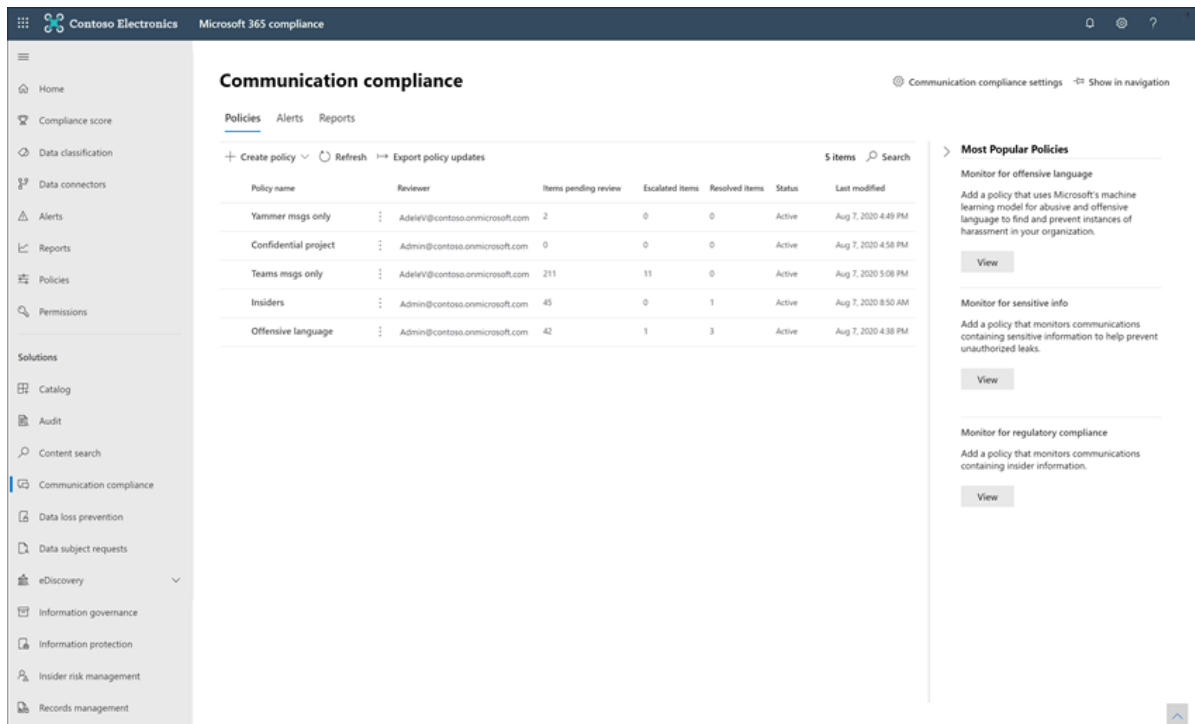


Figure 9: Communication compliance policy settings in Microsoft 365 compliance

3.10 Policy-Based Recording for Callings and Meetings

Policy-based recording enables Covered Entities or Business Associates that adopt Microsoft Teams for callings and meetings to stipulate, using an administrative policy, when calls and online meetings should be automatically recorded and captured for subsequent processing and retention as required by relevant corporate or regulatory policy.

Microsoft Teams' administrators can determine which users are to be recorded and which recorder will be used for each user by creating and assigning compliance recording policies. Users under this policy will be aware that their digital interactions with Microsoft Teams are being recorded but will not be able to disable the recording and will not have access to the recording once the interaction is complete. The recording may become part of the Covered Entities' or Business Associates' archive available as part of the legal medical record, or to compliance and legal personnel for eDiscovery, legal hold, and other corporate retention uses.

For more details, please refer to [Introduction to Microsoft Teams Policy-based Recording for Calling & Meetings–Microsoft Teams | Microsoft Docs](#).



3.11 eDiscovery and Legal Hold

Covered Entities and Business Associates may be required to preserve electronically-stored information when involved in litigation. Within Microsoft Teams, an entire team or select users can be put on hold or legal hold. This will help ensure that messages that were exchanged in those teams (including private channels) or messages exchanged by those individuals are discoverable by the Covered Entities' or Business Associates' compliance managers or Microsoft Teams' administrators ("Admins").

The eDiscovery Manager or eDiscovery administrator can then search and consume this information for compliance. To create an eDiscovery case, navigate to **compliance.microsoft.com > eDiscovery > Core > Create a case** as shown in Figure 10. Once a case is created Covered Entities and Business Associates can place a hold on content locations of people of interest. These locations can include SharePoint sites and mailboxes associated with Microsoft Teams, One Drive, and O365 Groups.

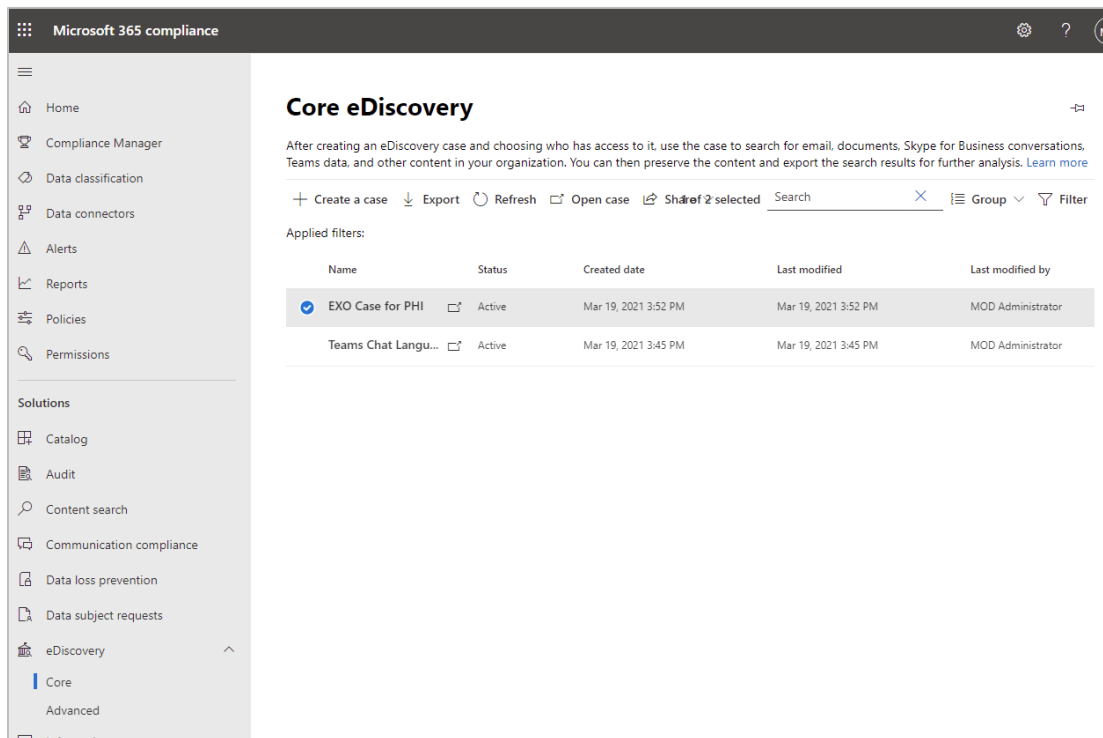


Figure 10: Creating an eDiscovery case using Microsoft 365 compliance

Note: Not all Microsoft Teams content is eDiscoverable.

After creating a hold, you can start creating and running different searches that are relevant to the case. The searches could be keyword, properties or condition based. You can create searches:

- Using Boolean search operators, search conditions, and other search query techniques to refine your search results, for example, `sharedwithusersuser:"garthf@contoso.com" AND fileextension:xlsx;`
- For sensitive data types and custom sensitive data types in SharePoint and OneDrive for Business, for example, `SensitiveType:"Credit Card Number"(c:c)(lastmodifiedtime<2016-01-01)`
- For site content that is shared with users outside of your organization, for example, `ViewableByExternalUsers:true AND ContentType:document NOT FileExtension:aspx`

To search for email messages or calendar meetings that were sent between 12/1/2014 and 11/30/2014 and that contain words that start with "phone" or "smartphone," create a search as shown in Figure 11.

The screenshot shows a search interface with the following elements:

- What do you want us to look for?**
You can enter a few keywords or leave this blank to search for all content. [Learn more](#)
- Search Query:** `phone* OR smartphone*`
- Conditions**
You can also add conditions to narrow your results.
- Condition 1:**
 - Field: `Sent date`
 - Operator: `between`
 - Value 1: `2014-12-01`
 - Value 2: `2015-11-30`
- Condition 2:**
 - Field: `Message type`
 - Operator: `equals any of`
 - Value: `email;meetings`

Figure 11: Creating a date and keyword search

For advanced searches, refer to [Content Search–Microsoft 365 Compliance | Microsoft Docs](#).

For more details, please refer to [Get started with core eDiscovery cases in Microsoft 365–Microsoft 365 Compliance | Microsoft Docs](#).

3.12 Classify and Protect Sensitive Information

Microsoft Teams chats and channel messages can be protected with sensitivity labels after creating Microsoft's sensitive information types, which are pattern-based classifiers.

Microsoft has released more than 200 sensitive information types out of the box, including:

- Social Security numbers
- Credit card numbers
- U.S. tax identification numbers
- Bank account numbers
- Routing numbers
- Password numbers
- Driver's license identification
- Disease classifications and other PHI

Microsoft also allows IT and security administrators to develop their own designations regarding custom sensitive information types. Designations for sensitive information types can be created and customized based on the following pattern-recognition methods:

- **Keywords**—A sensitive information type could be created to detect documents or chat sessions which contain the keywords "Social Security number" or "SSN"
- **Regular Expressions**—A sensitive information type could be created to detect documents or chat sessions which contain a pattern of digits that matches the format: xxx-xx-xxxx.
- **Exact Data Matching**—A sensitive information type could be created to detect documents or chat sessions which detect ONLY specific 5- or 6-digit numbers. For example, the system could alert on or block when a user mentions a legitimate employee ID in a chat or document while not taking any action on documents or chat sessions without a valid employee ID. In this case, the system would detect on a real instance of an employee ID—"Kevin's employee ID is 272727"—without detecting on a fake instance of an employee ID—"My employee ID is 123456."
- **Trainable Classifiers**—This classification method is well-suited for content that is not easily identifiable via the other methods. It leverages machine learning by comparing known true instances of a document type to new documents. The classifier will make a prediction as to whether the document is of a certain document category. Microsoft has built several out of the box trainable classifiers, including:
 - Resumes
 - Documents that detail an applicant's experience and education
 - Source code
 - Files that contain commands or code written in the top 25 computer programming languages on GitHub
 - Harassment
 - Offensive language based on the following traits: race, ethnicity, religion, national origin, gender, sexual orientation, age, and disability
 - Profanity

- Offensive language text or expressions
- Threats
- Offensive language with threats of violence

Once created, these sensitive information types can be used to protect Microsoft Teams and other applications via DLP policies, as shown in Figure 12.

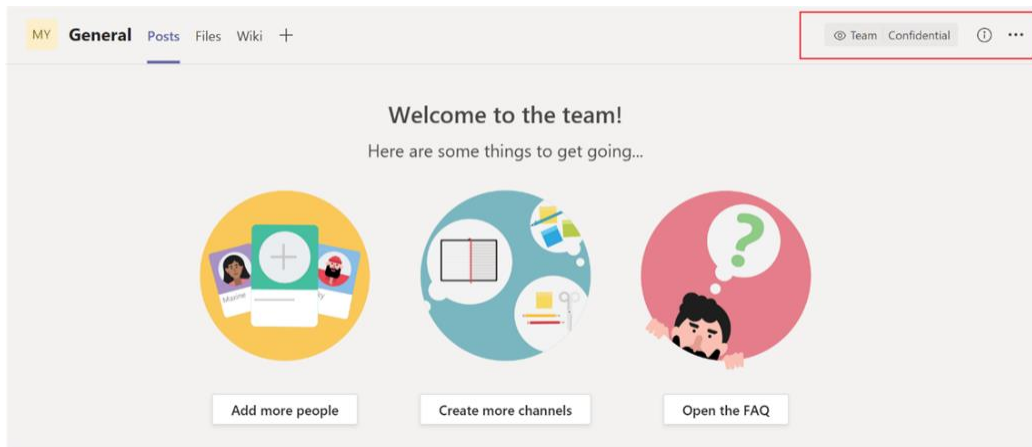


Figure 12: Classifying sensitive information using labels in Microsoft Teams

There are three ways that labels can be applied to documents:

- End users can classify documents with appropriate sensitivity labels
- Microsoft can scan documents on creation and on each save for sensitive information and recommend the end user to apply a particular sensitivity label
- Microsoft can scan documents on creation and on each save for sensitive information and can automatically apply a sensitivity label

Microsoft Data Loss Prevention can help detect, alert, and block sensitive data as it moves within the Office 365 environment and when users attempt to send data to external parties.

To configure DLP, navigate to **protection.microsoft.com > Data loss prevention > Create a policy.**

For more details, please refer to [Data loss prevention and Microsoft Teams–Microsoft 365 Compliance | Microsoft Docs.](#)

3.13 Data Retention and Deletion

Microsoft has created several methods of classifying and retaining sensitive information in Covered Entities and Business Associates through labels that can apply various retention policies to documents and Microsoft Teams chats. Retention labels may assist Covered Entities and Business Associates by:

- Retaining any necessary files in the event of a legal inquiry or audit, and
- Deleting old content can reduce the amount of sensitive data Covered Entities and Business Associates may have, empowers team members to only focus on more recent documents, and reduce the amount of money Covered Entities and Business Associates pay for storage.

Retention labels allow Covered Entities and Business Associates to hold documents for a specified amount of time and can be targeted to specific mailboxes or SharePoint sites. The labels provide IT and compliance administrators various methods to customize retention of documents to meet business policies or regulations.

Data retention and deletion can be configured by navigating to **compliance.microsoft.com > Policies > Retention > New retention policy** and creating a retention policy, as shown in Figure 13.

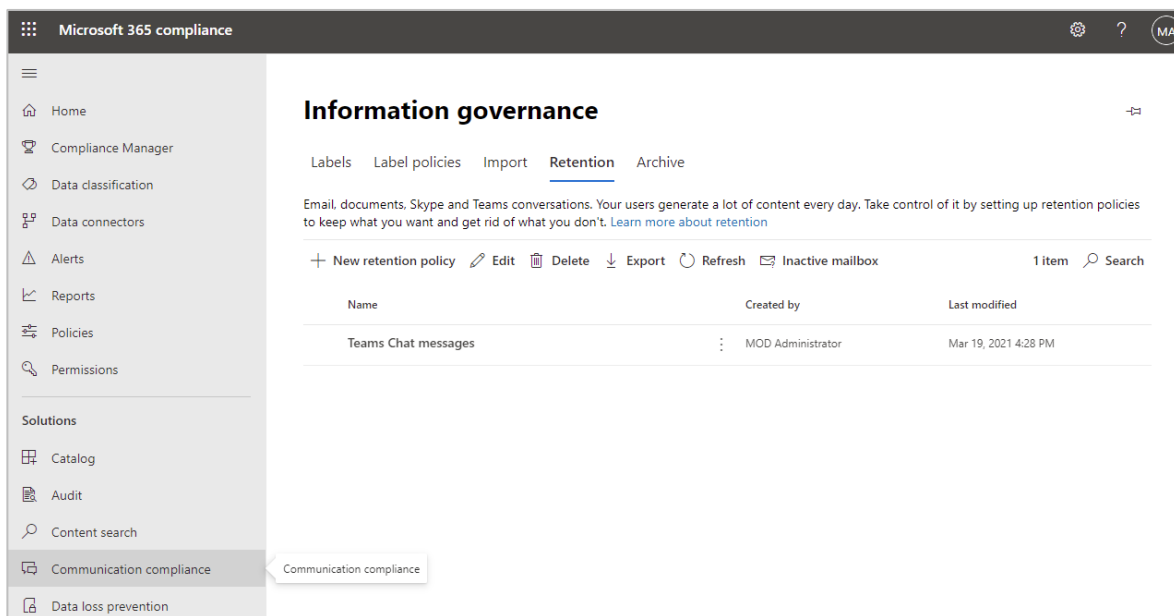
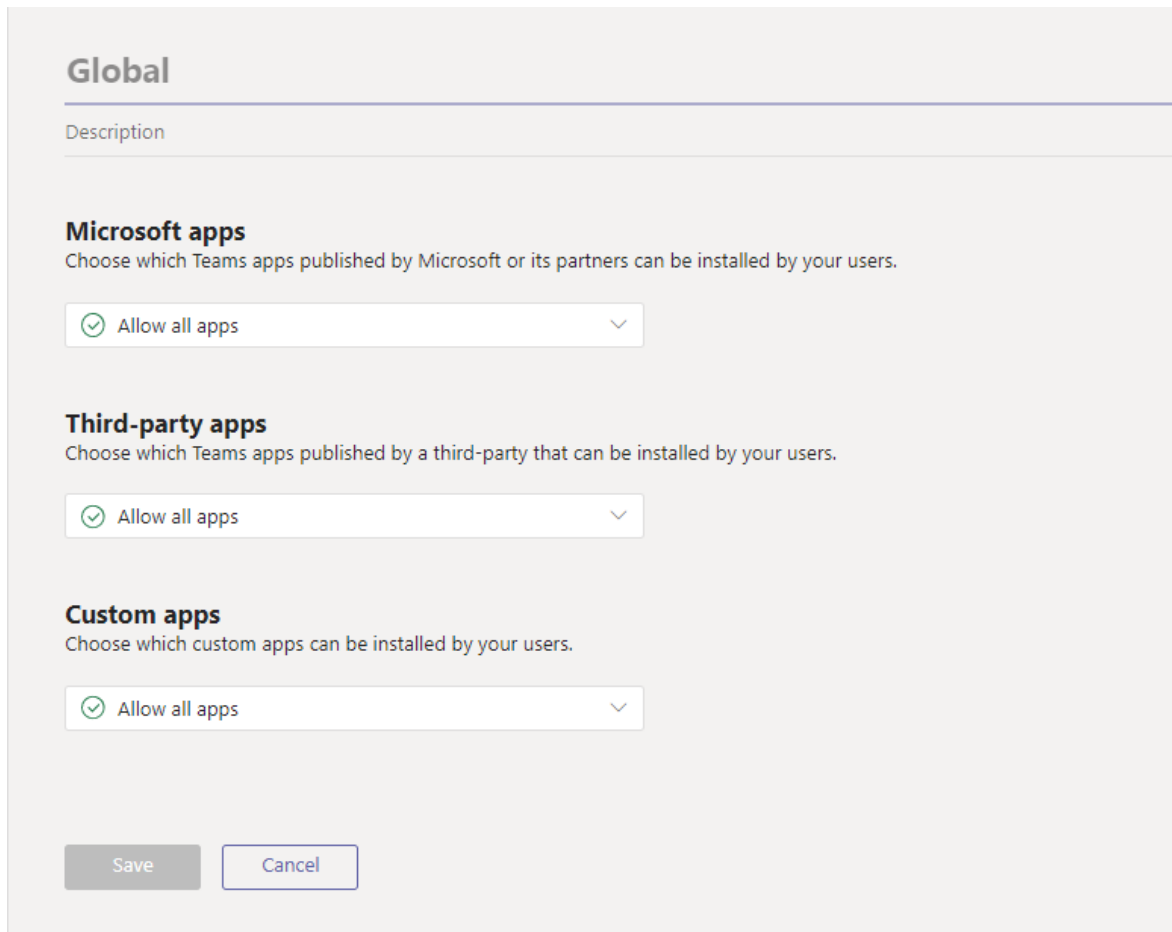


Figure 13: Using data retention policies to determine what kind of information is retained.

For more information on Microsoft Teams' retention policies, please refer to [Create and configure retention policies to automatically retain or delete content–Microsoft 365 Compliance | Microsoft Docs](#).

3.14 Enforce Company-Approved Product Lists

Application permission policies can be configured to control which applications are available to Microsoft Teams users in Covered Entities and Business Associates. Microsoft Teams can allow or block all or specific applications from Microsoft, third parties, and a particular Covered Entity or Business Associate itself. To configure company-approved product lists, navigate to **Microsoft Teams admin center > Teams apps > Permission policies** and click **Add**, as shown in Figure 14.



The screenshot shows the 'Global' settings page in the Microsoft Teams admin center. At the top, there is a 'Global' header and a 'Description' field. Below this, there are three sections for configuring app permissions:

- Microsoft apps**: Choose which Teams apps published by Microsoft or its partners can be installed by your users. The dropdown menu is set to 'Allow all apps'.
- Third-party apps**: Choose which Teams apps published by a third-party that can be installed by your users. The dropdown menu is set to 'Allow all apps'.
- Custom apps**: Choose which custom apps can be installed by your users. The dropdown menu is set to 'Allow all apps'.

At the bottom of the page, there are two buttons: 'Save' and 'Cancel'.

Figure 14: Setting app permission policies in Microsoft Teams

3.15 Auditable Events and Content

Auditable events are events that can be captured, stored, and investigated for security monitoring and threat hunting. In Azure AD, navigate to **Azure Active Directory > Audit logs**. In addition, certain Microsoft Teams related events can be captured after enabling Audits. To enable auditing for Microsoft Teams, navigate to **Microsoft 365 compliance manager > Audit** and click **Start recording user and admin activity**, as shown in Figure 15.

Microsoft Compliance Manager allows eDiscovery Managers to search O365 data for specific keywords. To do a content search, navigate to **Microsoft 365 Compliance Manager > Content search**, click **New search** and enter keywords you want to search for, as shown in Figure 16. Note that to use content search you need to be a member of the eDiscovery Manager role group.

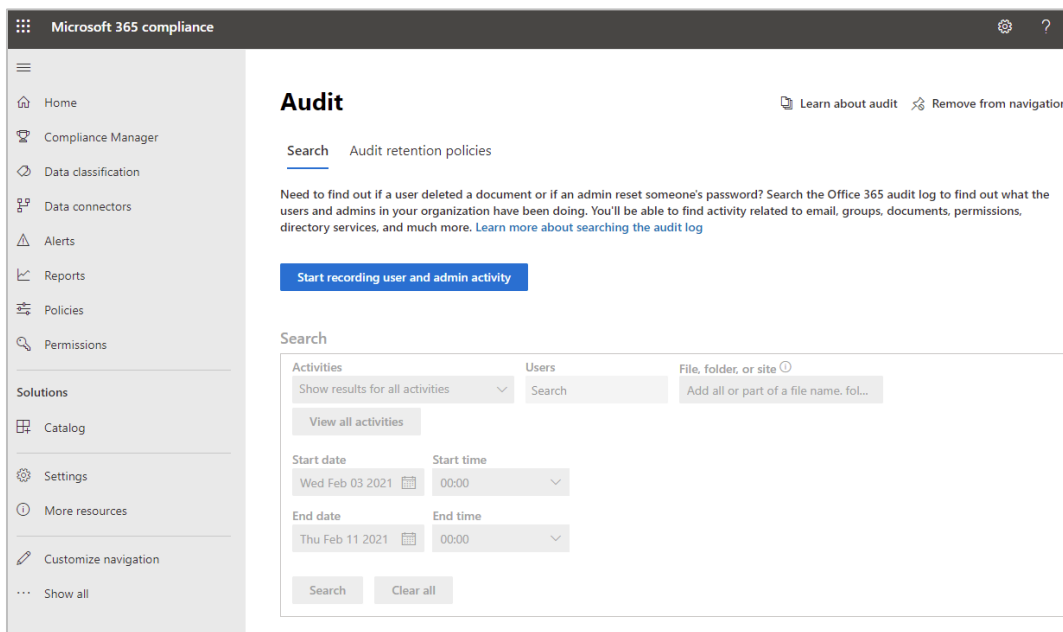


Figure 15: Setting up audit logs using the compliance manager

For more information on how to integrate Microsoft Teams audit logs with Azure Sentinel, refer to [Azure Sentinel and Microsoft Teams–Microsoft Teams | Microsoft Docs](#).

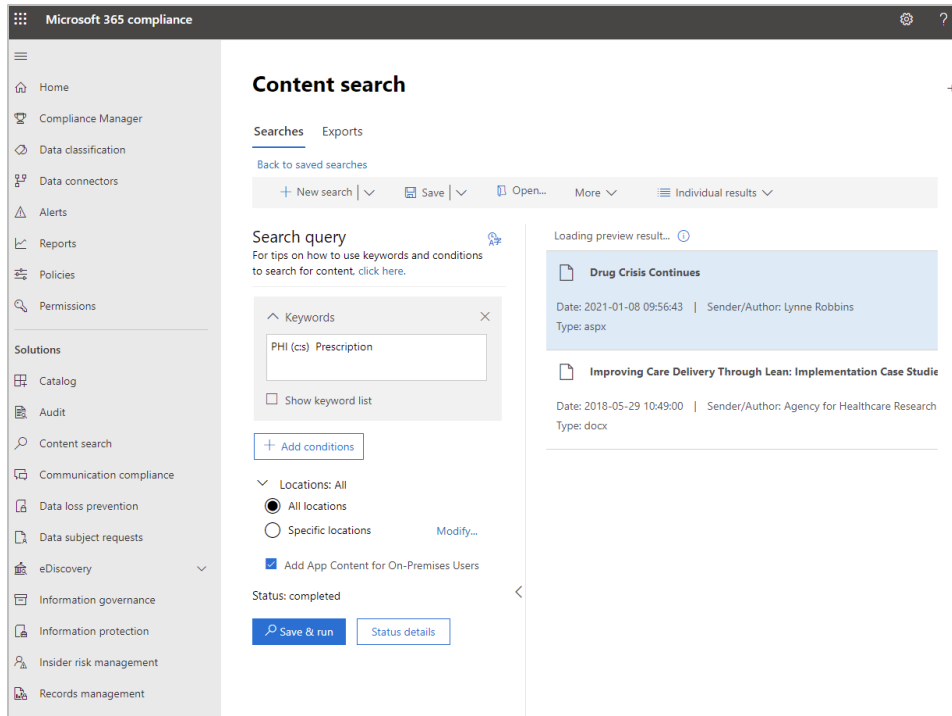


Figure 16: Specifying search queries for audit logs

3.16 Role Management

Azure AD Roles help enforce Role-Based Access Control (“RBAC”) principals. RBAC is an authorization system that provides fine-grained access management of Azure resources to allow, restrict or revoke access to sensitive information like PHI. To assign a user a role, navigate to the **Azure Active Directory > Users**, select a user and choose **Assigned roles** and click **Add assignment** as shown in Figure 17. For further details refer to [View and assign administrator role permissions–Azure AD | Microsoft Docs](#).

A list of Azure AD roles can be found at [Azure AD role descriptions and permissions–Azure Active Directory | Microsoft Docs](#).

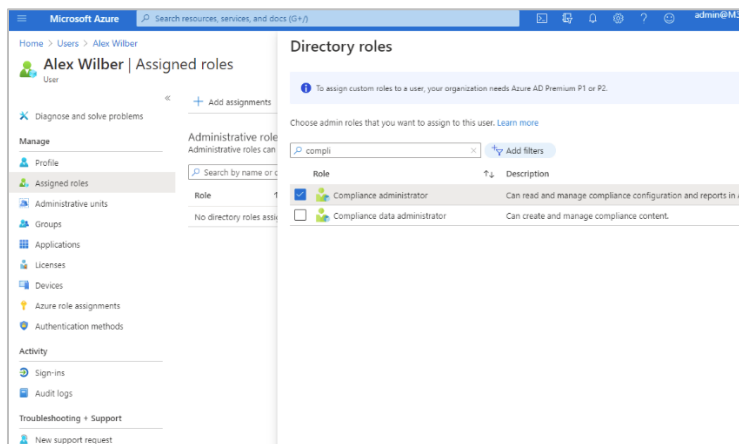


Figure 17: Assigning roles to users within Azure Active Directory

3.17 Information Barriers

Information barrier policies provide control over which users or groups can communicate and collaborate with one another. Information barriers are helpful in preventing information sharing between departments that should not be sharing particular types of data. These policies also prevent user search and discovery in Microsoft Teams as shown in Figure 18.

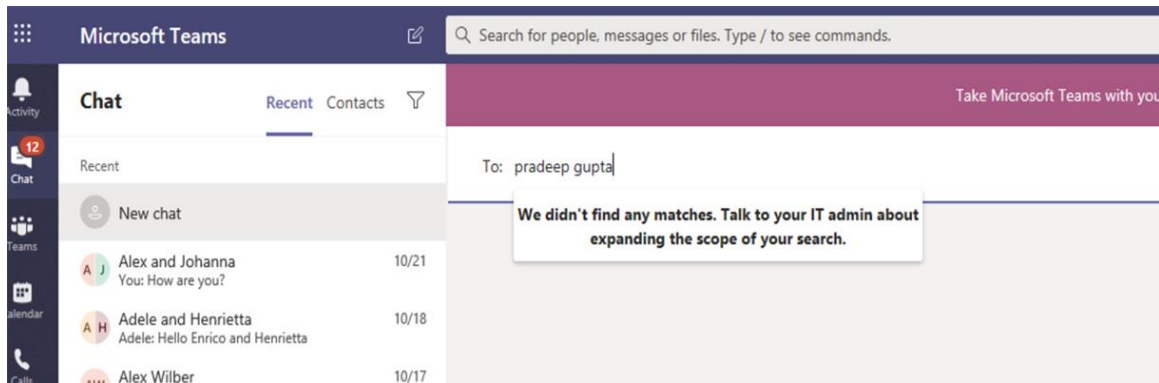


Figure 18: User search in Microsoft Teams failing due to an Information barrier policy

Note: Information barrier policies do not apply to email communication, support only two-way restrictions, and are triggered in following scenarios:

- Members are added to a team
- A new chat is requested
- A user is invited to join a meeting
- A screen is shared between two or more users
- A user places a phone call in Microsoft Teams
- Guests are in Microsoft Teams

For further details, refer to [Information barriers in Microsoft Teams–Microsoft Teams | Microsoft Docs](#).

4. Using Compliance Manager

[Microsoft Compliance Manager](#) is a feature in the [Microsoft 365 compliance center](#) that helps manage Covered Entities' and Business Associates' implementation requirements with greater ease and convenience. Compliance Manager provides assistance throughout the compliance journey—from taking inventory of data protection risks, to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors. Compliance Manager translates complex regulatory requirements to specific controls and through a compliance score, provides a quantifiable measure of compliance. The tool offers intuitive compliance management, a vast library of scalable assessments, and built-in automation.

4.1 Perform Ongoing Risk Assessments

Compliance Manager scans through the enterprise environment and detects system settings, automatically updating technical control status. For example, if multifactor authentication is configured in the Azure Active Directory (AAD) portal, Compliance Manager can detect the setting and reflect that in the control details. Conversely, if multifactor authentication is not configured, then Compliance Manager can flag that as a recommended action to take. With the ongoing control assessment, Covered Entities and Business Associate can proactively maintain compliance instead of reactively fixing settings following an audit. For details, please go to [this document](#).

4.2 Monitor Using Compliance Manager

The Compliance Manager dashboard shows the current compliance score, provides visibility into what may need attention, and guides key improvement actions, as shown in Figure 19.

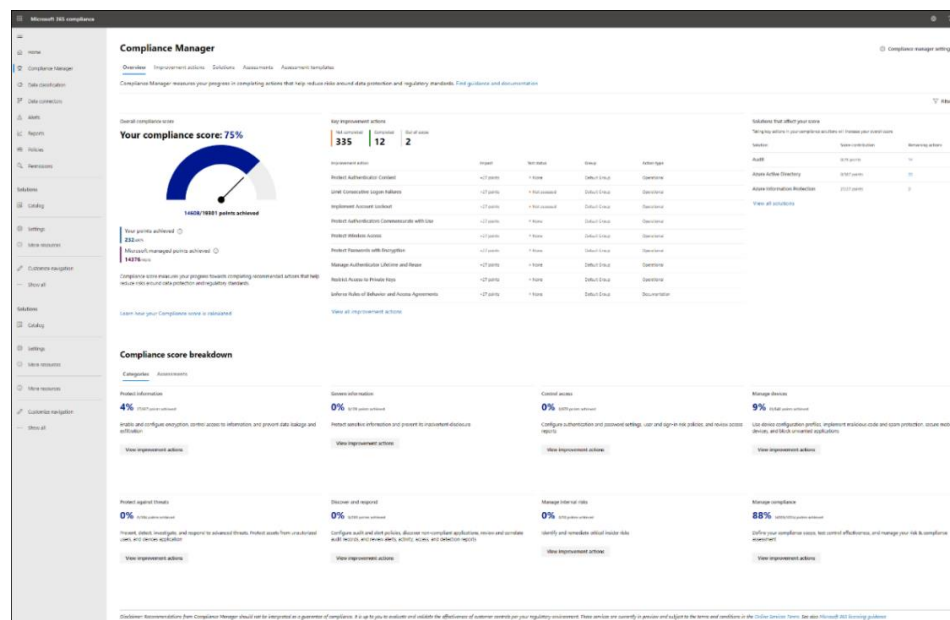


Figure 19: Compliance Manager dashboard in Microsoft 365

4.3 Increase the Covered Entities' or Business Associates' Score in Compliance Manager

The compliance score is a risk-based assessment to help in understanding the organization's compliance posture by measuring progress in completing improvement actions. For details, please go to [this document](#).



5. Configuring Microsoft Teams Components for Internal Collaboration

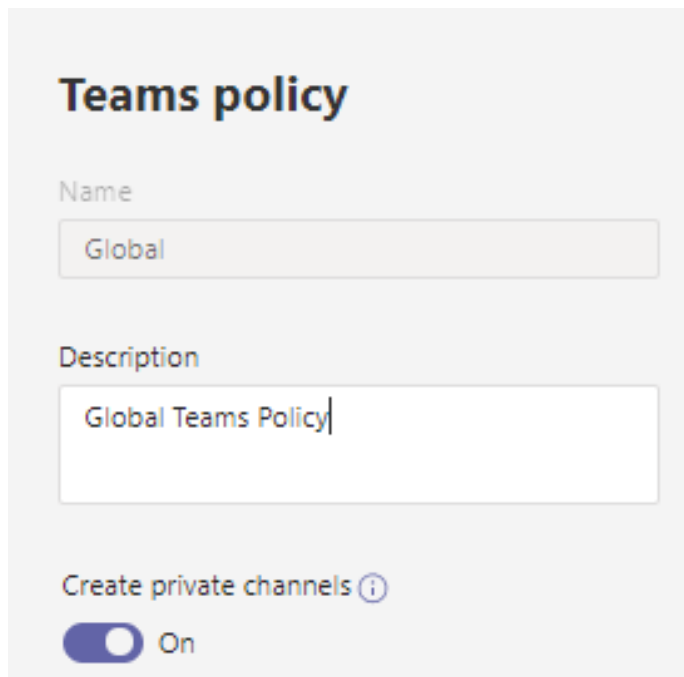
Microsoft Teams helps augment communication and productivity by improving Covered Entities' and Business Associates' ability to quickly connect with others inside the organization. Covered Entities and Business Associate can work more efficiently and more effectively when they are highly collaborative. However, increased productivity cannot be the only consideration when moving to Microsoft Teams. It is imperative to implement all the necessary security controls within Microsoft Teams to ensure the Covered Entities' or Business Associates' sensitive information is protected.

5.1 Global Teams and Channel Policies

To facilitate business operations in a secure fashion, Microsoft Teams' Global Team and Channel Policies may be configured for a seamless user experience while enhancing a Covered Entities' and Business Associates' security posture.

An administrator can choose whether users should be able to create Private Team channels. This can be configured by navigating to the following blade within the Microsoft Teams admin portal: **Microsoft Teams Admin Center > Teams > Teams Policies**, as shown in Figure 20.

The administrator can select or create a Teams policy and choose whether a group of users will be able to create Private Team channels.



The screenshot displays the 'Teams policy' configuration interface. It includes a 'Name' text box containing 'Global', a 'Description' text box containing 'Global Teams Policy', and a 'Create private channels' section with a toggle switch currently turned 'On'.

Figure 20: Teams policy configuration in Microsoft Teams

5.2 Messaging Policies for Internal Users

Covered Entities or Business Associates may wish to regulate how users can message other users. Users can be empowered to share information quickly while complying with enterprise security policies. The Microsoft Teams Admin portal provides many configuration settings for managing messaging policies.

A Microsoft Teams security administrator can configure these policies by navigating to the following blade within the Microsoft Teams Admin portal: **Microsoft Teams Admin Center > Teams > Messaging Policies**, as shown in Figure 21.

Security engineers can create Microsoft Teams messaging policies specific to certain groups and users so they can:

- Control whether Microsoft Teams channel owners can delete messages sent within their Teams channel,
- Control whether users can delete messages they have sent, and
- Control whether users can edit messages they have sent.

The complete set of options which can be configured is shown in Figure 21.

New messaging policy

Add a friendly description so you know why it was created

Owners can delete sent messages	<input type="checkbox"/> Off
Delete sent messages	<input checked="" type="checkbox"/> On
Edit sent messages	<input checked="" type="checkbox"/> On
Read receipts	User controlled
Chat	<input checked="" type="checkbox"/> On
Use Giphy in conversations	<input checked="" type="checkbox"/> On
Giphy content rating	Moderate
Use Memes in conversations	<input checked="" type="checkbox"/> On
Use Stickers in conversations	<input checked="" type="checkbox"/> On
Allow URL previews	<input checked="" type="checkbox"/> On
Translate messages	<input checked="" type="checkbox"/> On
Allow immersive reader for viewing messages	<input checked="" type="checkbox"/> On
Send urgent messages using priority notifications	<input checked="" type="checkbox"/> On
Create voice messages	Allowed in chats and channels
On mobile devices, display favorite channels above recent chats	Disabled
Remove users from group chats	<input checked="" type="checkbox"/> On
Suggested replies	<input checked="" type="checkbox"/> On

Save Cancel

Figure 21: Options for configuring messaging policies within Microsoft Teams

5.3 File Sharing and Cloud Storage Options

Administrators can select options for how users will be able to store and share files in the cloud, as shown in Figure 22. Microsoft Teams supports the following cloud file storage and file sharing software solutions:

- Citrix Files
- Dropbox
- Box
- Google Drive
- Egnyte

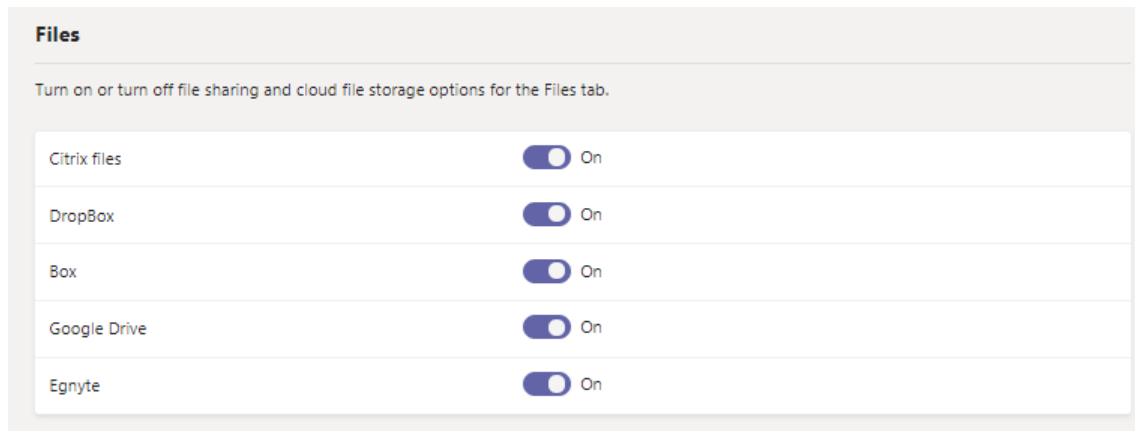


Figure 22: Configurable file storing/sharing options in Microsoft Teams

5.4 Configuring Meeting Policies

Administrators can specify how multiple granular settings relate to a Covered Entities' and Business Associates' Microsoft Teams meetings. The configuration settings are broken up into the following sections:

- General (see Figure 23)
- Audio and video (see Figure 24)
- Content sharing (see Figure 25)
- Participants and guests (see Figure 26)

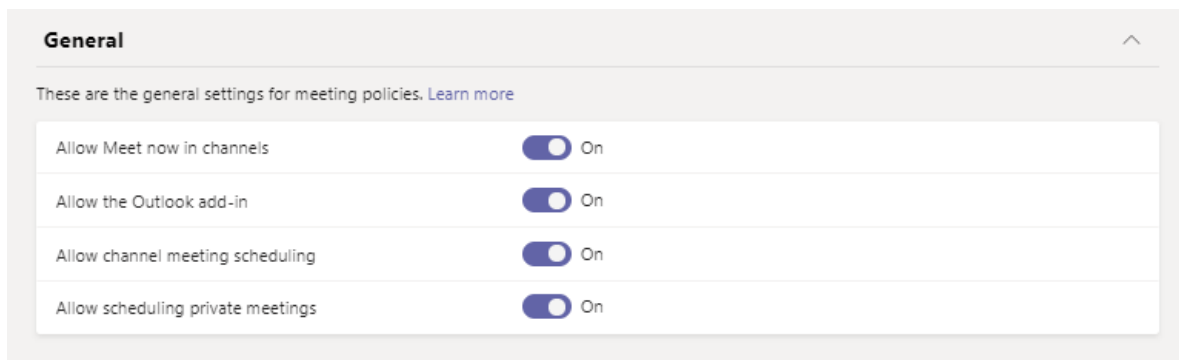


Figure 23: General meeting policy settings in Microsoft Teams

Audio & video

Audio and video settings let you turn on or off features that are used during Teams meetings. [Learn more](#)

Allow transcription ⓘ	<input type="checkbox"/> Off
Allow cloud recording	<input checked="" type="checkbox"/> On
Mode for IP audio	Outgoing and incoming audio enabled ▾
Mode for IP video	Outgoing and incoming video enabled ▾
Allow IP video	<input checked="" type="checkbox"/> On
Allow NDI streaming ⓘ	<input type="checkbox"/> Off
Media bit rate (Kbs) ⓘ	50000

Figure 24: Audio and video meeting policy settings in Microsoft Teams

Content sharing

Content sharing settings let you control the different types of content that can be used during Teams meetings that are held in your organization. [Learn more](#)

Screen sharing mode	Entire screen ▾
Allow a participant to give or request control	<input checked="" type="checkbox"/> On
Allow an external participant to give or request control	<input type="checkbox"/> Off
Allow PowerPoint sharing	<input checked="" type="checkbox"/> On
Allow whiteboard	<input checked="" type="checkbox"/> On
Allow shared notes ⓘ	<input checked="" type="checkbox"/> On

Figure 25: Content sharing meeting policy settings in Microsoft Teams

Participants & guests

Participant and guest settings let you control access to Teams meetings. [Learn more](#)

Let anonymous people start a meeting ⓘ	<input type="checkbox"/> Off
Roles that have presenter rights in meetings	Everyone, but user can override ▾
Automatically admit people ⓘ	People in my organization and guests ▾
Allow dial-in users to bypass the lobby ⓘ	<input type="checkbox"/> Off
Allow Meet now in private meetings	<input checked="" type="checkbox"/> On
Enable live captions	Disabled but the user can override ▾
Allow chat in meetings	Enabled ▾

Figure 26: Participants and guests meeting policy settings in Microsoft Teams

6. Configuring Microsoft Teams' Components for External Collaboration

As with internal users, Microsoft Teams also provides a powerful platform for collaboration with external users. There are two types of external users supported in Microsoft Teams:

- **External User**—These are users who are not within the Covered Entities or Business Associates, such as one of their Business Associates, patients, or other users with a verified identity.
- **Guest User**—These users are a subclass of external users but are accessing the system without a verified identity. This type of user may be asking general questions about the Covered Entities' or Business Associates' available services or a user contacting a helpdesk for general support requests.

Implementation of defined security controls and HIPAA regulatory requirements can be assisted by establishing the proper configuration of the following settings:

- Enabling access for external user types
- Configuring application policies
- Defining messaging policies



6.1 Enabling Access for External User Types

Because Microsoft Teams supports two types of external users, both types must be explicitly enabled to grant access.

6.1.1 Enabling External Access in Microsoft Teams

External access is a way for Microsoft Teams users from an entire external domain to find, call, chat, and set up meetings. It is recommended to set external access settings to "Off" if Covered Entities or Business Associates do not collaborate with external users. The next option is to set this to "On" and include a whitelist of approved domains.

With the below settings switched to "On" by default, Covered Entities and Business Associates can both receive and send messages outside of the organization's domain, which may pose risks to PHI.

External access can be configured by navigating to the **Microsoft Teams Admin portal** > **Org-wide Settings** > **External Access** as shown in Figure 27. For more information on External access, please refer to [this document](#).

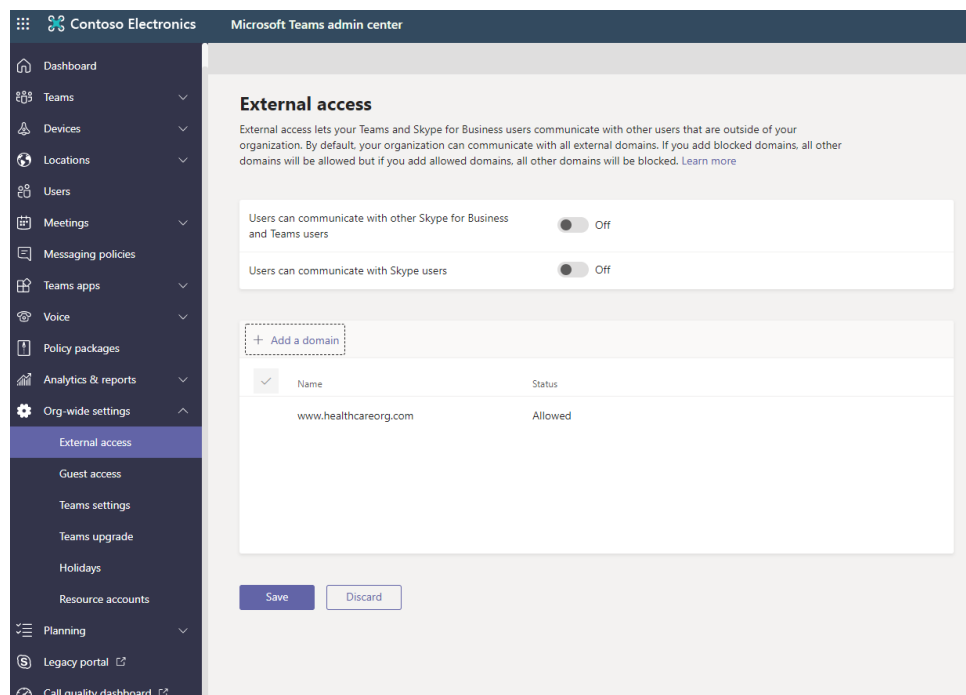


Figure 27: Configuring external access settings using the Microsoft Teams admin portal

Please note:

- Covered Entities or Business Associates may wish to add their Business Associates' applications to the whitelist or use [DLP policies](#) to detect and prevent or flag ePHI shared externally.
- The allowed or blocked domains only apply to meetings if anonymous access to meetings is "Off."

6.1.2 Enabling Guest Access in Microsoft Teams

Guest access in Microsoft Teams lets an individual user outside an organization access Microsoft Teams and channels. A guest user can be given nearly all the same capabilities as a native team member. It is recommended to set Guest access settings to “Off” if you do not collaborate externally, as shown in Figure 28.

If Covered Entities or Business Associates want to allow users to invite guest users, restrictions can be placed to limit which domains guest users can be invited from by following steps outlined [here](#) and keeping Guest access settings to “On.”

With the below settings switched to “On” by default, Covered Entities or Business Associates can both receive and send messages outside of their domains, which may pose a risk to PHI.

Guest access can be configured by navigating to the **Microsoft Teams Admin portal > Org-wide Settings > Guest Access**, as shown in Figure 28. For more information regarding Guest access, please refer to [this document](#).

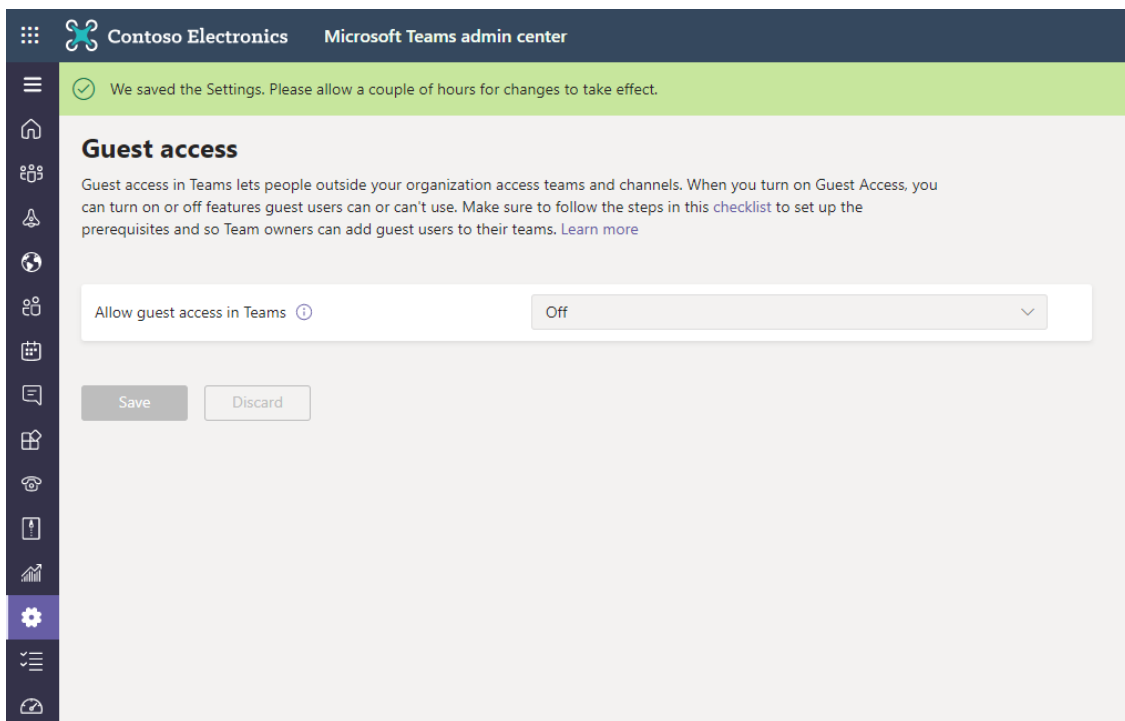


Figure 28: Allowing guest access in Microsoft Teams using the admin portal

6.2 Configuring App Policies in Microsoft Teams

If Covered Entities or Business Associates are beginning to roll out Microsoft Teams, it is reasonable to immediately turn off all custom and third-party applications within the application. While turning on custom and third-party apps can provide increased productivity, it is necessary for Covered Entities or Business Associates to first analyze each application to make sure they comply with the HIPAA Rules' requirements.

Once Microsoft Teams has been rolled out to a Covered Entity or Business Associate, the organization's IT teams can begin allowing certain applications to be added. Whenever a user adds an application, Microsoft Teams will explicitly show the user the privacy policies and the permissions the app is requesting. The end user must accept those terms to install the application.

App Settings can be configured by navigating to the **Microsoft Teams Admin portal > Teams Apps > Manage Apps** and selecting the option **Org-wide app settings**, as shown in Figure 29. For more information on configuring custom and third-party application policies, please refer to [this document](#).

Org-wide app settings

Third-party apps

You can control which third-party apps can be installed for your organization. [Learn more](#)

Allow third-party apps ⓘ

☐ Off

Allow any new third-party apps published to the store by default ⓘ

☐ Off

Custom apps

If your organization requires apps other than those available in the Teams Apps store, custom apps can be developed as app packages and uploaded. [Learn more](#)

Allow interaction with custom apps ⓘ

☐ Off

The apps you have blocked may still have access to the data in the team it has been installed in. To disable this apps' data access, have your Global Admin, Application Admin, or Cloud Application Admin, go to [Azure Active Directory admin center](#) and set 'Enabled for users to sign in?' to false. For more information, see [Learn more](#).

Save **Cancel**

Figure 29:
Configuring org-wide app setting in the Microsoft Teams admin portal.

6.3 Configuration of Messaging Policies

The messaging policy configuration is also divided between the external and guest user types within Microsoft Teams. This helps to ensure implementation of HIPAA regulations due to the ability of Microsoft Teams users to readily identify verified external users from non-verified guest accounts.

6.3.1 Messaging Policies for External Users

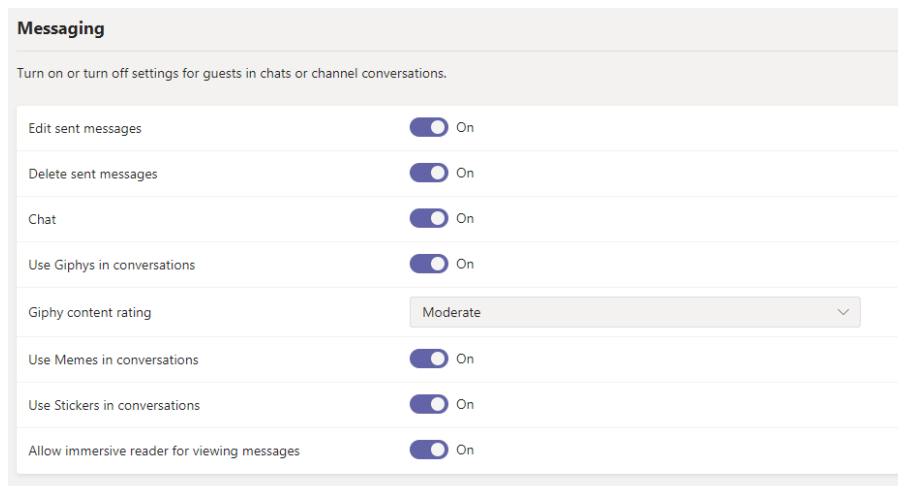
Microsoft defines external users as users which live in an external Azure Active Directory domain not managed by the Covered Entity or Business Associate. External users are only able to communicate with an organization via Microsoft Teams if that organization allows the external domain to communicate with them. (Note: By default, this is configured as "On" for all external Azure Active Directory domains.) By configuring trusted external domains in Microsoft Teams, Covered Entities' and Business Associates' IT team can allow external users from specific domains to find, chat, call, and set up meetings with members of the particular Covered Entity or Business Associate.

In most cases, chatting with external users via federation is limited to text only. However, external users can have a native Microsoft Teams chat experience if both Microsoft Teams users are in Teams Only mode. For more information about this experience, its prerequisites and the complete set of granular access options for external users, refer to [this document](#).

6.3.2 Messaging Policies for Guest Users

Admins can control settings for guests in chats or channel conversations. By default, these settings are switched to "On." With the previous external access settings in place, it may be safe to leave these settings in their default configurations. However, admins can choose to further restrict capabilities based on Covered Entities' or Business Associates' preferences. These settings can be configured by navigating to the **Microsoft Teams Admin portal > Org-wide Settings > Guest Access > Messaging**, as shown in Figure 30.

For the complete set of granular access options for guest users, refer to [this document](#).



The screenshot shows the 'Messaging' settings page in the Microsoft Teams Admin portal. The page title is 'Messaging' and it includes a subtitle: 'Turn on or turn off settings for guests in chats or channel conversations.' Below this, there is a list of settings, each with a toggle switch and a label. All toggle switches are currently turned 'On'. The settings are:

Setting	Status
Edit sent messages	On
Delete sent messages	On
Chat	On
Use Giphy in conversations	On
Giphy content rating	Moderate
Use Memes in conversations	On
Use Stickers in conversations	On
Allow immersive reader for viewing messages	On

*Figure 30:
Messaging
policies for
guest users in
the Microsoft
Teams admin
portal*

6.4 Files sharing and storage options for files tab

Admins can control files storage and sharing settings that are applicable across Covered Entities or Business Associates. By default, these settings are switched to "On." It is recommended to switch these settings to "Off." These settings can be configured by navigating to the **Microsoft Teams Admin portal > Org-wide Settings > Team Settings > Files**, as shown in Figure 31.

For the complete set of organization-wide permissions, please refer to [this document](#).

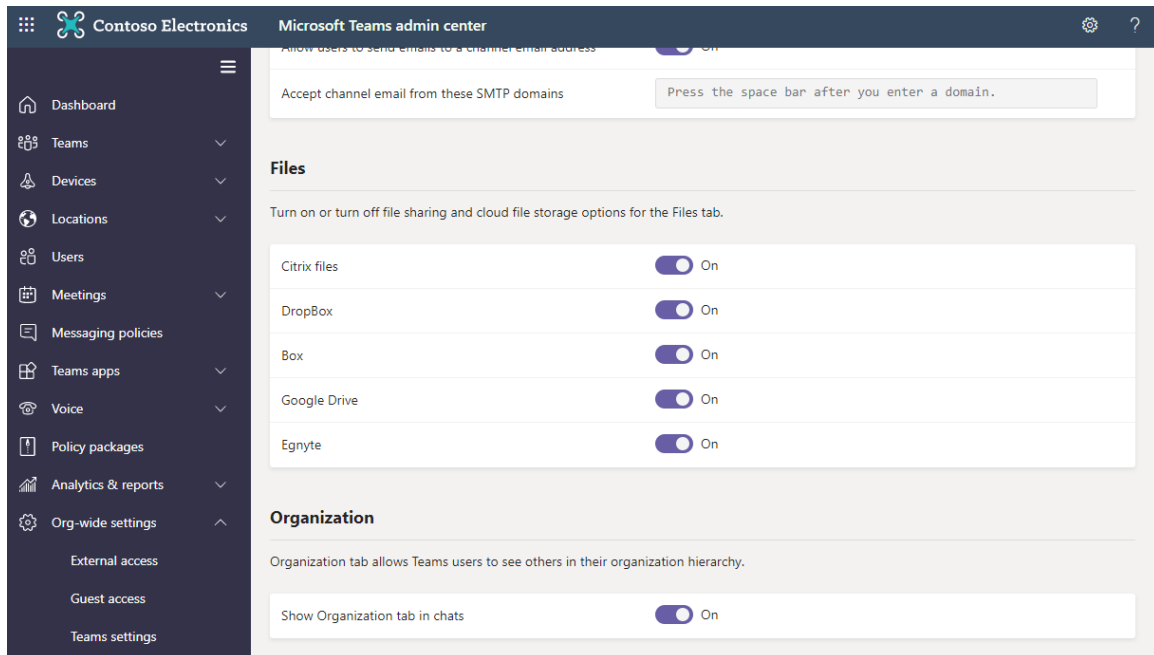


Figure 31: Organization-wide file sharing settings in the Microsoft Teams admin portal

6.5 SharePoint and One Drive External Collaboration

Admins can control external collaboration settings for SharePoint Online and One Drive. By default, these settings are set to “most permissive,” which allows for file and folder sharing without sign-in. With the previous external access settings in place, it may be safe to leave these settings in their default configurations. However, admins can choose to further restrict capabilities based on the Covered Entities’ or Business Associates’ preferences. These settings can be configured by navigating to the **SharePoint Admin center > Policies > Sharing**, as shown in Figure 32.

To learn more about SharePoint Online and OneDrive external sharing, please refer to [this document](#).

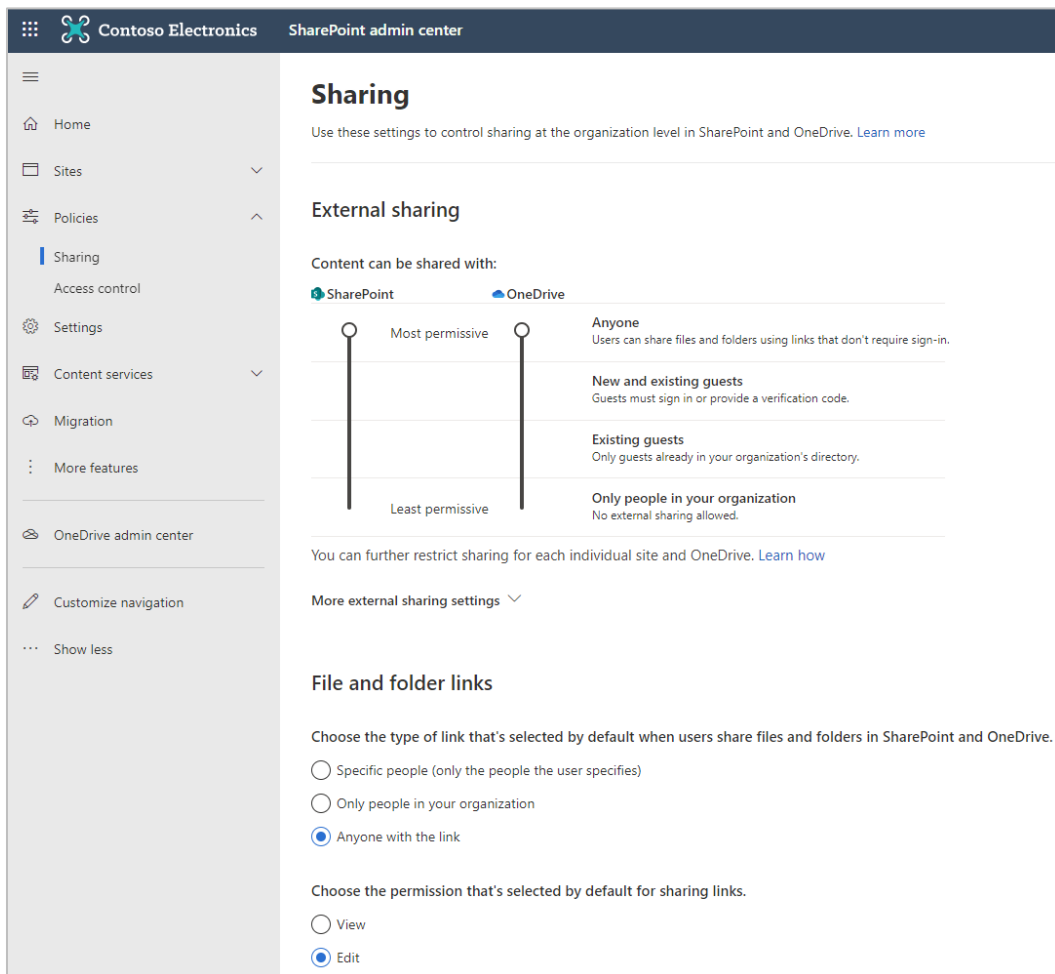


Figure 32: Configuring external collaboration with SharePoint Online / OneDrive in the SharePoint admin center.