

Teams DLP Playbook

How to use this guide

Please use this guide as a starting point for protecting your sensitive information in Microsoft Teams communication channels via Microsoft Purview Data Loss Prevention. All links and references should be up to date, however, if you have a question about the correctness of any information in this document, please reach out to our [yammer group](#).

All screenshots in this guide contain the proper configuration settings according to the best practices at the time of publication. Please ensure that your configurations mirror those used in this guide. Please refer to the Microsoft documentation online at docs for the latest updates.

Though the name of this document is shown as a playbook, it can be equally considered a deployment guide. This document will be updated as and when new features are introduced to Microsoft Teams DLP. There are few abbreviations used in the document and please refer to the abbreviations at the end of this document.

This document covers in detail various use cases that can be achieved using Teams-DLP.

Introduction

This playbook provides an overview of how enterprise customers can deploy Microsoft Teams DLP for protecting sensitive information that is coming/going within or outside of the organization. Microsoft Purview Data Loss Prevention has integrations with multiple workloads that help to protect customer data with a single policy. Teams-DLP is one of the workloads within the DLP console. This playbook walks through the various aspects of deploying use cases across content/containers and shows the effectiveness of the unified DLP portal as a single place to define all aspects of your DLP strategy.

Using this play book will help to:

- Understand the unified console and interface.
- Develop a strategy for deploying Teams-DLP across the organization.
- Provide near real time Alerts with notifications.
- Review various scenarios to test Teams-DLP over chat and channel communication.

This playbook helps readers plan and protect sensitive information scenarios that normally exist in every organization. It also helps as a user guide to mitigate the risk of

exchanging crucial data while communicating over chat or giving access to sites for guest users.

Assumption: Sensitive Information Types (SITs) that are to be protected in Teams Chat or Channel messages have been identified.

Overview

Microsoft Purview Information Protection helps to identify, discover, classify, and protect sensitive information wherever it lives either at rest or in transit.

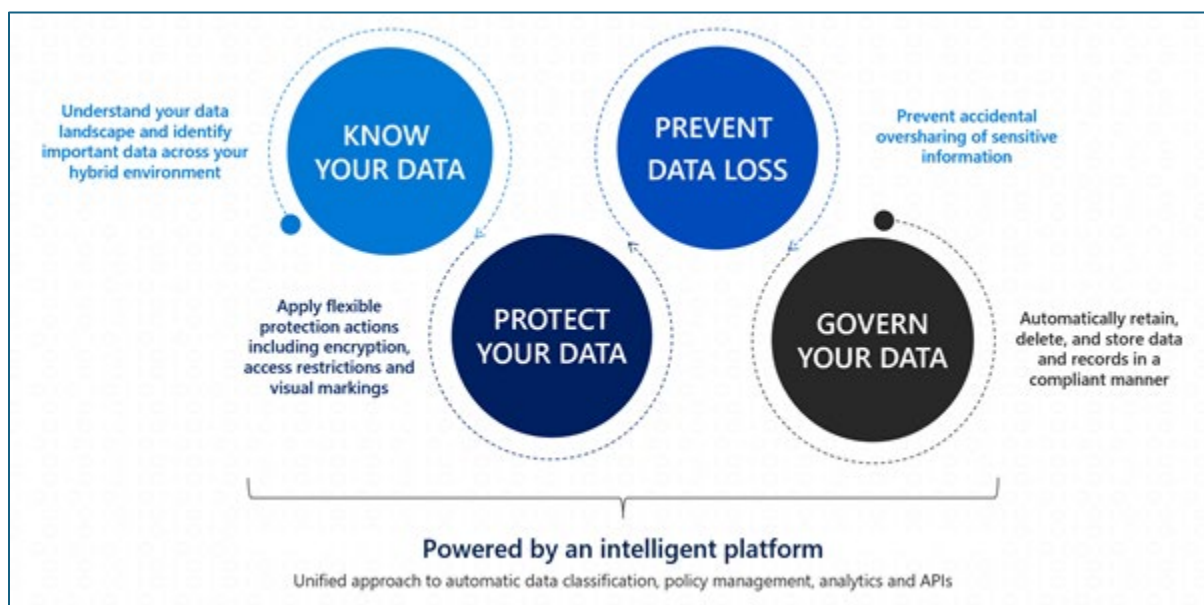


Figure 1: Microsoft Purview Information Protection Cycle

Know your data assists in understanding the current data landscape and provides organizations with the ability to identify sensitive content residing in Microsoft 365 across Exchange, SharePoint, OneDrive for Business, and physical devices depending on workloads used and licensing owned.

Protecting your data assists in applying flexible protection that includes visual marking, encryption and access restrictions across apps, services and devices that travel inside and outside the organization.

Prevent data loss (DLP) assists in preventing accidental data loss and oversharing of sensitive information within or outside the organization. In the Data Loss Prevention capability of Microsoft Purview Information Protection, **Global** and **Compliance** admins can create policies across workloads and apply rules to protect data oversharing. Pre-

defined built in regulatory templates across various industries are available. Administrators can also create their own custom policies to suit organizational needs.

The URL for creating DLP policies is: [DLP](#).

Log in with an appropriate role as described in [Role Requirements](#) and for creating policies inclusive of desired workloads. The most used role is Compliance Data Administrator.

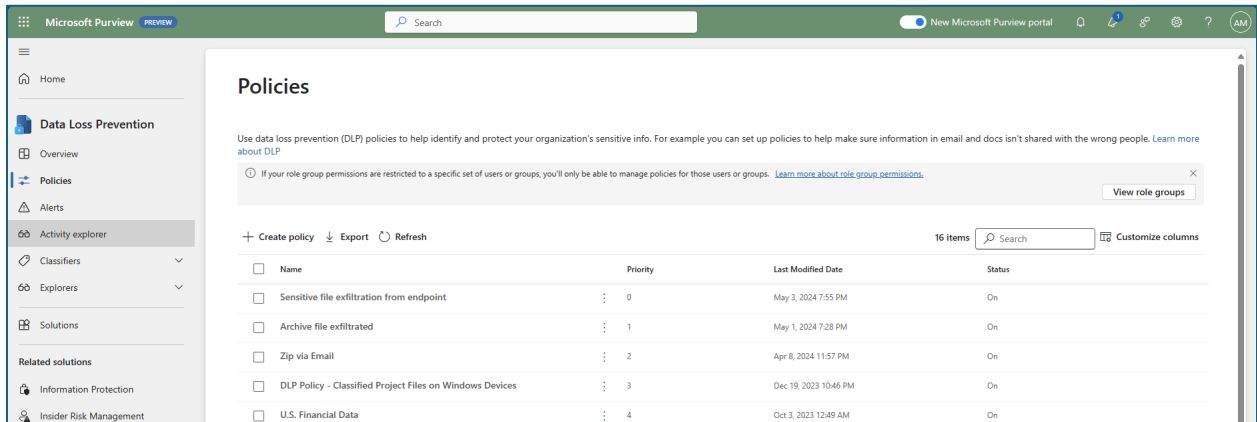


Figure 2: Microsoft Purview Portal DLP wizard

Data Loss Prevention capabilities are across workloads such as: Exchange, SPO, ODB, Instances, On-premises repositories, Power BI workspaces, Devices (Endpoint DLP), and Teams chat and channel messages.

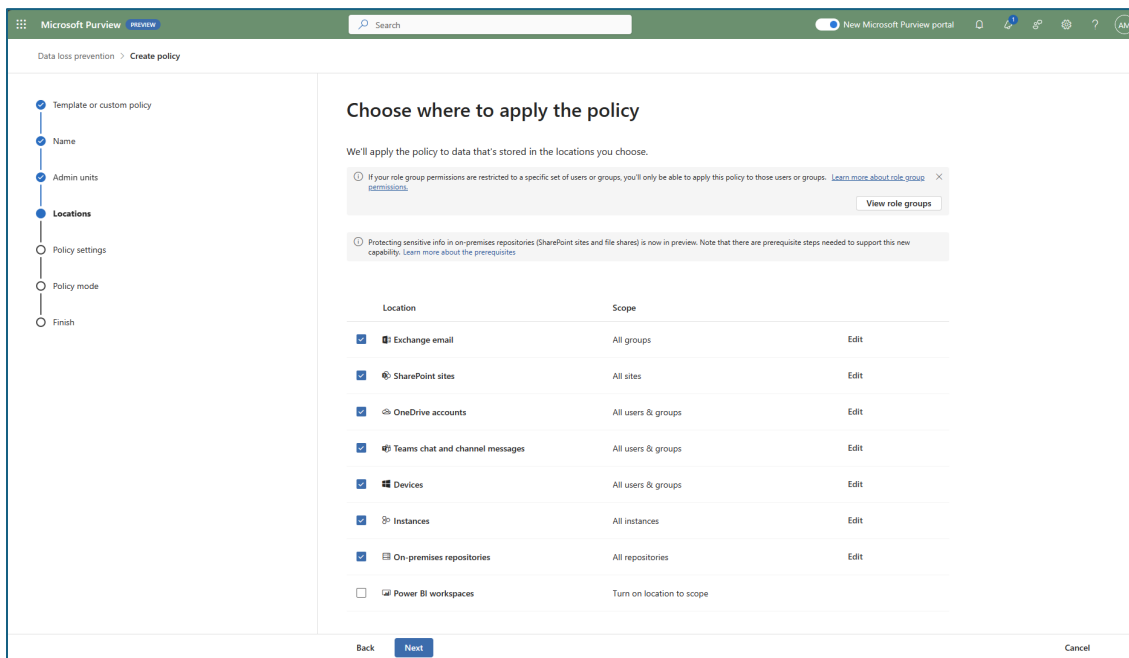


Figure 3: The ***NEW*** Microsoft Purview Portal – DLP across workloads

NOTE: The **new Microsoft Purview Portal will hit general availability late summer 2024 (DATE COULD CHANGE). This playbook uses screenshots and guidance from the new Microsoft Purview portal.**

This playbook explains the process of protecting data in the location “Teams chat and channel messages.” Individuals can explore the files that contain sensitive information or have labels applied using the Content Explorer. The user activities on these labels can be viewed using the Activity Explorer.

Activity Explorer provides a 360-degree view (also known as **know your data**) of user risky activities across the tenant and helps administrators take preventive measures. The below figure shows Activity Explorer with detailed metadata of user activity where and when it has happened.

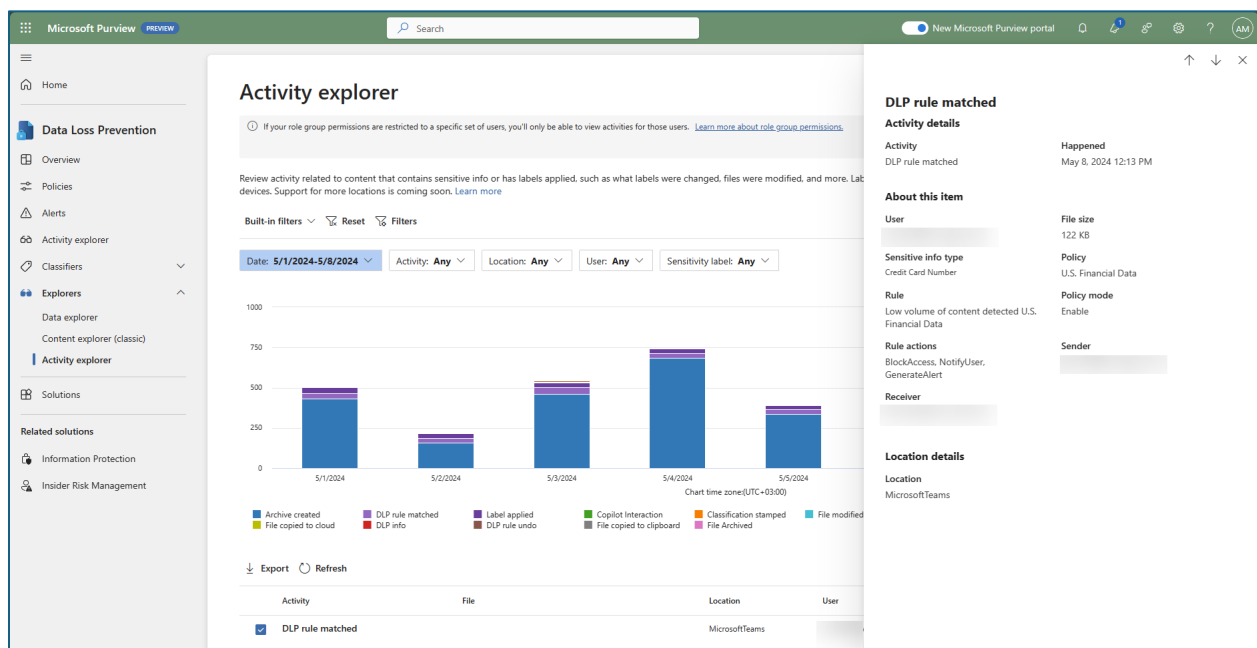


Figure 4: Activity Explorer with user activities

Similarly, Microsoft Purview Information Protection has a Content Explorer which is part of the Data Classification dashboard. Content Explorer shows a current snapshot of items with sensitivity labels, retention labels, and Sensitive Information Types (SITs) in your organization. A DLP policy can help protect sensitive information, which is detected through one or more sensitive information types. There are a few types of sensitive information types. Examples include the built-in SITs, named entity SITs, customer SITs, and exact data match SITs.

Some examples include region-based SITs such as Australia bank account number and worldwide like Credit card number. For a full list of built-in sensitive information types, please click [here](#).

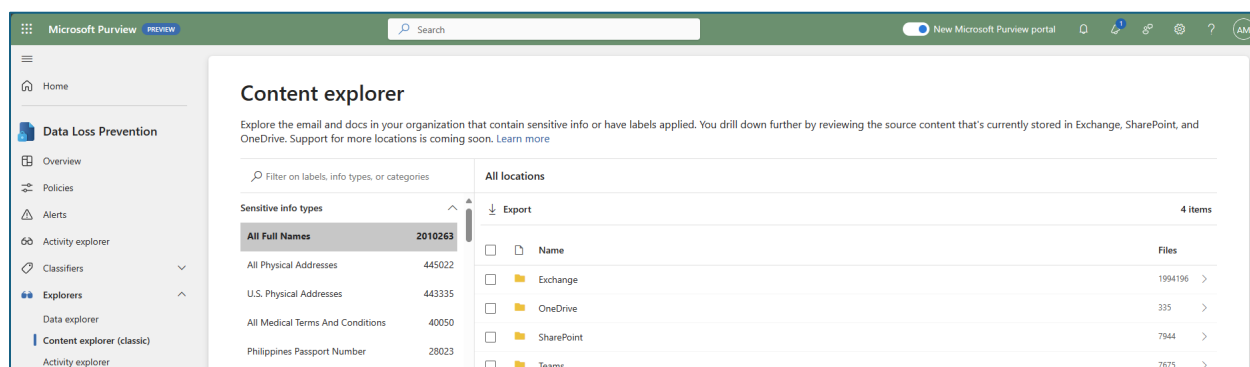


Figure 5: Content Explorer with summary view

Upon further drill down, the exact file and location containing sensitive information can be viewed for further action or protection, along with data pertaining to the last modification date and user.

Licensing Requirements

Office 365 Advanced Compliance, which is available as a standalone option and is included in Office 365 E5 and Microsoft 365 E5 Compliance. Office 365 and Microsoft 365 E3 include DLP protection for SharePoint, OneDrive, and Exchange Online. This also includes files that are shared through Teams because Teams uses SharePoint Online and OneDrive to share files. **Support for DLP protection in Teams chat and channel messages requires E5.**

NOTE: To learn more about licensing requirements and get the latest guidance, see [Licensing Guide](#).

Role Requirements

To create DLP policies or rules in the [Microsoft Purview portal](#), the user should have a role of **Global Admin**, **Compliance Admin**, or **Compliance Data Admin** (most used).

To get access to the content explorer tab, an account must be assigned membership in any one of these roles or role groups.

- Microsoft 365 role groups
 - Global administrator
 - Compliance administrator

- Security administrator
- Compliance data administrator

Membership in these role groups does not allow you to view the list of items in content explorer or to view the contents of the items in content explorer. Access to content explorer is highly restricted because it lets you read the contents of scanned files.

- Content Explorer List viewer: Membership in this role group allows you to see each item and its location in list view. The data classification list viewer role has been pre-assigned to this role group.
- Content Explorer Content viewer: Membership in this role group allows you to view the contents of each item in the list. The data classification content viewer role has been pre-assigned to this role group.

The account you use to access content explorer must be in one or both of the role groups. **These are independent role groups and aren't cumulative.** For example, if you want to grant an account the ability to view the items and their locations only, grant Content Explorer List viewer rights. If you want that same account to also be able to view the contents of the items in the list, grant Content Explorer Content viewer rights as well.

You can also assign either or both of the roles to a custom role group to tailor access to content explorer. A Global admin, can assign the necessary Content Explorer List Viewer, and Content Explorer Content Viewer role group membership.

For activity explorer, an account must be explicitly assigned membership in any one of these role groups or must be explicitly granted the role.

Microsoft Purview Roles	Microsoft Purview Role Groups	Microsoft 365 Roles	Microsoft 365 Role Groups
Information Protection Admin	Information Protection	Global Admins	Compliance Administrator
Information Protection Analyst	Information Protection Admins	Compliance Admins	Security Administrator
Information Protection Investigator	Information Protection Investigators	Security Admins	Security Reader
Information Protection Reader	Information Protection Analysts	Compliance Data Admins	
	Information Protection Readers		

There are roles and role groups that you can use to fine-tune your access controls. To learn more about them, see [Permissions in the Microsoft Purview compliance portal](#).

Data Loss Prevention for Teams-DLP

A DLP policy helps organizations prevent data loss. It also helps users to make better decisions when sending SITs knowingly or unknowingly. The process of creating a DLP policy with Teams as the workload is explained in the later sections of this document.

Scope of DLP Protection

Teams DLP policy scoping are different from other locations such as Exchange, SharePoint, etc. The policy is scoped on the types of chats based on the user or groups chosen. M365 Groups are used to scope public (standard channel and shared channel) chats. Users, Security Groups, or Distribution Groups are used to scope non-public (1:1/n and private channel) chats.

Policy scope	Teams Entities	DLP Protection
Individual user accounts	- 1:1/n chats - Standard and shared channel messages - Private channel messages	- Yes - No - Yes
Security groups/Distribution group/Non-mail-enabled Security group	- 1:1/n chats - Standard and shared channel messages - Private channel messages	- Yes - No - Yes
Microsoft 365 groups*	- 1:1/n chats - Standard and shared channel messages - Private channel messages	- No - Yes - No

Note: When a DLP policy is scoped to Microsoft 365 groups, DLP protection applies to group members using the standard and shared channels associated with the groups they belong to.

Protecting Sensitive Information in Messages

If someone is trying to share a chat message that contains sensitive information to an external user or guest, based on the creation of DLP-Rule for the Teams workload, the message will be blocked within seconds. Both the sender and receiver see the message blocked notification.

Protecting Sensitive Information in Documents Sharing

If a user attempts to share a document that contains sensitive information with external users or guests in a Microsoft Teams channel or chat, the DLP rule prevents opening the document by the external user. In this case, the DLP policy must include SharePoint and OneDrive locations for protection to be in place.

When new files are added to SharePoint or OneDrive in Microsoft 365, it may take a few moments for them to be crawled and indexed. It takes additional time for the Office Data Loss Prevention (DLP) policy to scan the content and apply rules to help protect sensitive information. If external sharing is turned on, sensitive content could be shared and accessed by guests before the Office DLP rule finishes processing.

You can ensure that documents are protected until DLP scan completes and marks them as safe to share by using a PowerShell cmdlet to enable a feature called **sensitive by default**. For more information, click [here](#).

To enable, run Set-SPOTenant -MarkNewFilesSensitiveByDefault BlockExternalSharing.

To disable, run Set-SPOTenant -MarkNewFilesSensitiveByDefault AllowExternalSharing.

Note: it might take up to 60 minutes for this new setting to take effect.

If you're following and creating **Endpoint DLP policies**, a similar functionality here would be the just-in-time protection. This can be configured in the Microsoft Purview portal by going to Settings > Data Loss Prevention > Just-in-time protection.

Note: Do NOT choose the Block users from completing actions option until you fully understand the impact of this feature.

Protection of Teams and SharePoint sites

Sensitivity labels can be used to protect data not only in documents and emails, but also in Teams and SharePoint sites. During creation, you're able to protect meetings that are scheduled in Outlook and Teams. You're also able to configure access control to groups & sites.

Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Fabric and Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

Items

Be aware that restricting the scope to only files or emails might impact access control settings and where the label can be applied. [Learn more](#)

Files


Protect files created in Word, Excel, PowerPoint, and more.

Emails

Protect messages sent from all versions of Outlook.

Meetings

Protect calendar events and meetings scheduled in Outlook and Teams.

 Parent label will automatically inherit meeting scope from sub labels

Groups & sites

Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

NOTE: To protect Teams meetings and chats, your org must have a Teams Premium license.

Define protection settings for groups and sites

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers. [Learn more about these settings](#)

Privacy and external user access

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

External sharing and Conditional Access

Control external sharing and configure Conditional Access settings to protect labeled SharePoint sites.

Private teams discoverability and shared channel settings

Decide whether private teams will be discoverable in searches and control the types of teams that can be invited to shared channels.

Teams settings can be defined such as: Private (or public), external user access and access from unmanaged devices. When you apply a sensitivity label to a supported container, the label automatically applies the classification and configured protection settings to the site or group. Referring to [using sensitivity labels in Teams, Groups or SharePoint sites](#).

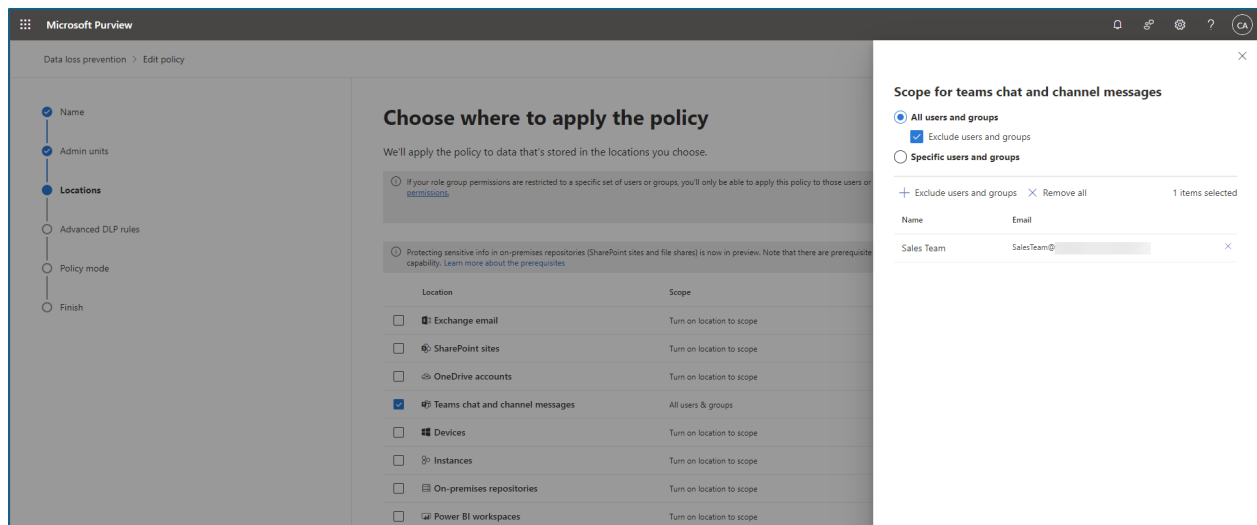
Sensitivity labels for containers support Teams shared channels. If a team has any shared channels, they automatically inherit sensitivity label settings from their parent team, and that label can't be removed or replaced with a different label.

Scoping of Teams-DLP policy:

Teams DLP policy scoping are different from other locations such as Exchange, SharePoint, etc. The policy is scoped on the types of chats based on the user or groups chosen. M365 Groups are used to scope public (standard channel and shared channel) chats. Users, Security Groups, or Distribution Groups are used to scope non-public (1:1/n and private channel) chats. Refer [here](#) on the latest scoping definition.

Example - Exclude chats from specific Teams channels

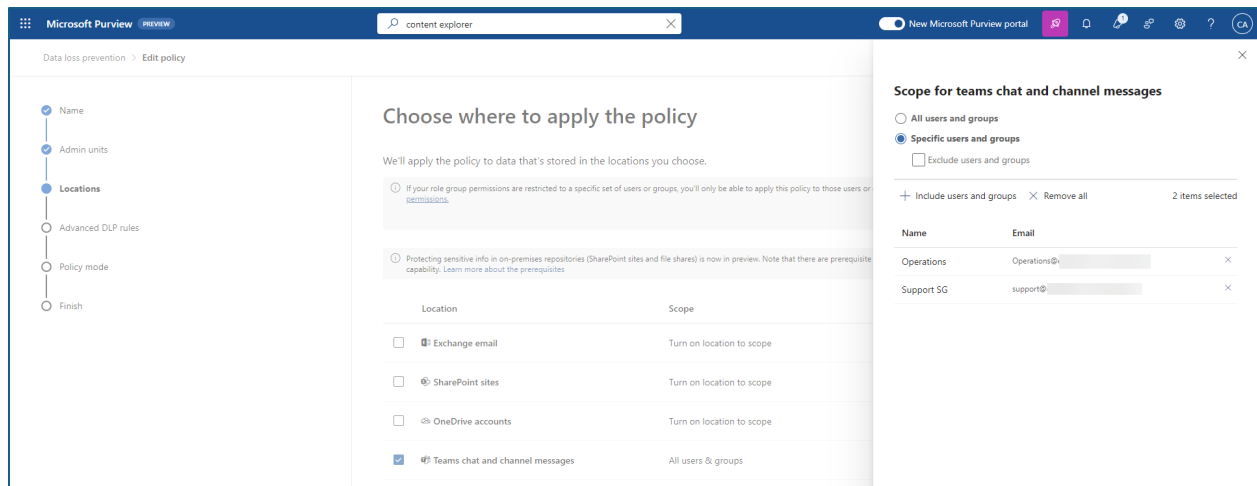
There are cases when there is a need to exclude certain channels from oversharing, such as the channels for Sales in Teams to handle credit card information. In the Microsoft Purview portal, select All users and groups and check the Exclude users and groups checkbox and then add the desired M365 Group.



Scoping a policy by selecting a M365 Group to exclude channels associated with the group in your organization. In this example, the policy will exclude the standard and shared channels under the Sales Teams team.

Example - Exclude all chats for a group of users

There are cases when there is a need to customize a policy such as allowing support and operations department to handle credential information.



Scoping a policy by selecting both a M365 group AND security group to exclude all chats for specific members in your organization. In this example, Support SG and Operations M365 Group have the same set of members.

Note: To ensure the policy is updated as group membership changes, it is important to consider synchronizing the M365 Group and security groups regularly.

Teams and Guest Access

Guest is a user type in Microsoft Teams which is included with Office 365 licenses. With guest access, you can provide access to teams, documents within channels, resources, chats, and applications for people external to your organization.

In a real-life scenario, guests may be a vendor, a supplier, or an external partner who is working on a project but is not a member of your organization and has a business account (Azure AAD/ Entra ID) or consumer email account (Outlook, Gmail, Hotmail, etc.). They can participate as guests in Teams and explore the channel experiences.

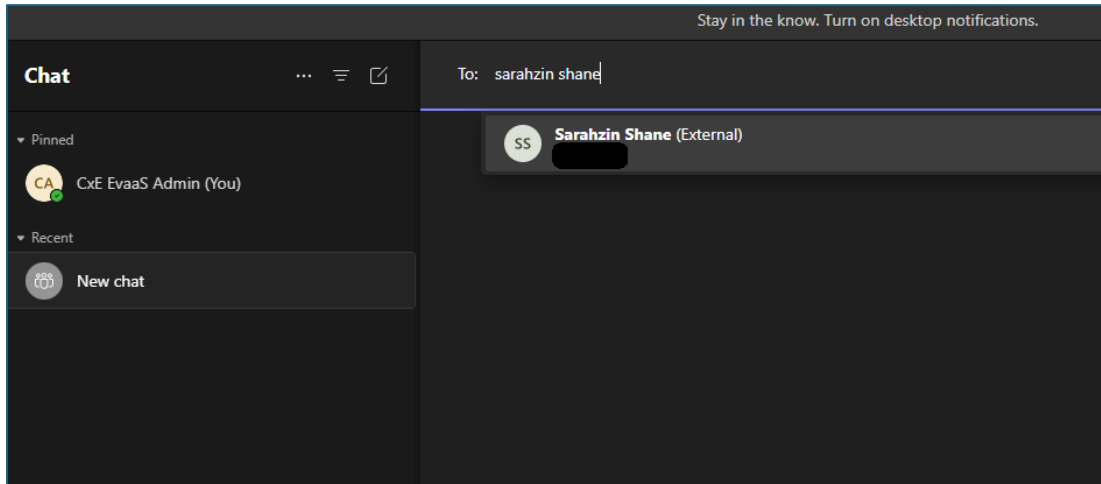
External Access (**Federation**) is turned on by default in Microsoft Teams, which means your organization can communicate with all external domains. The Teams admin can turn it off or specify which domains to include or exclude. Federation users do not have access to your organization's Teams or Teams' resources. **They can only communicate via 1-1 chat.** If a federation user needs access to Teams' channels and resources, they must be added as a **guest** in the organization.

Let's start with the explanation below.

1. Organizations (sender and receiver) which have O365 licenses and Teams enabled, can start 1-1 chats/meetings/voice calls.
 - The external user (receiver) will **not** be added by default to AAD and will not get access to internal resources like files or folders.

This external user will be considered a one-time user and which we call a **Federation user**.

- If the user needs additional privileges, administrators will provide access by converting them to a guest user.



2. If a member has been added to a Teams channel, the user profile will be automatically added (forced to add) to Azure Active directory and will be treated almost as an internal user (refer figure below). **This user is an external or guest user.**

Federation: Teams support 1:1 federation chat only. Teams do not currently support:

- Group Chats with one or more federation users
- Channel conversations with federation users

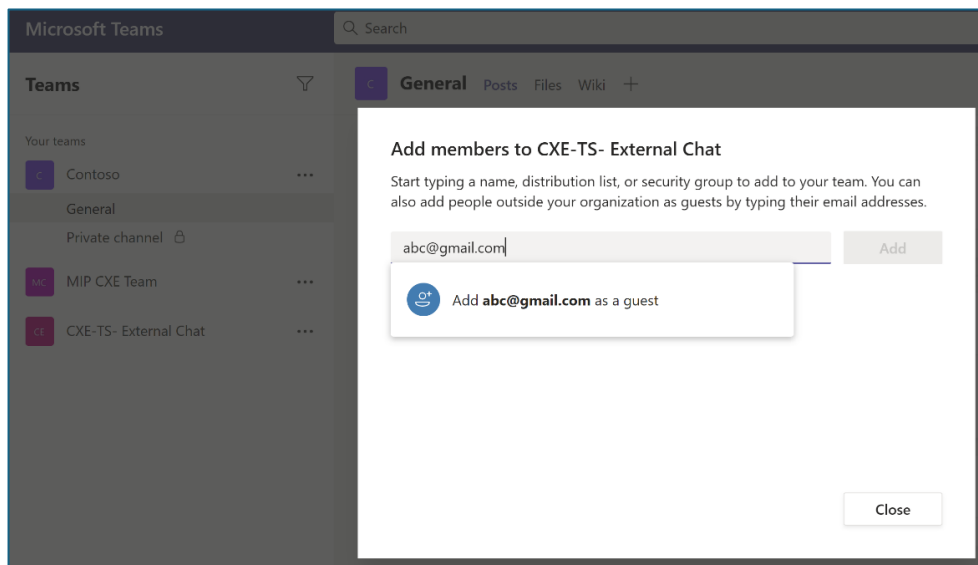


Figure 6: Adding members to external chat

To set-up guest access, please refer [here](#). The detailed comparison of Team member and guest has been explained in this [section](#). When a guest is invited to join a team, they receive a link to accept. The guest must accept the invitation before joining the team and the associated channels.

Below is the admin experience of adding additional privileges. Login to [Guest access - Microsoft Teams admin center](#).

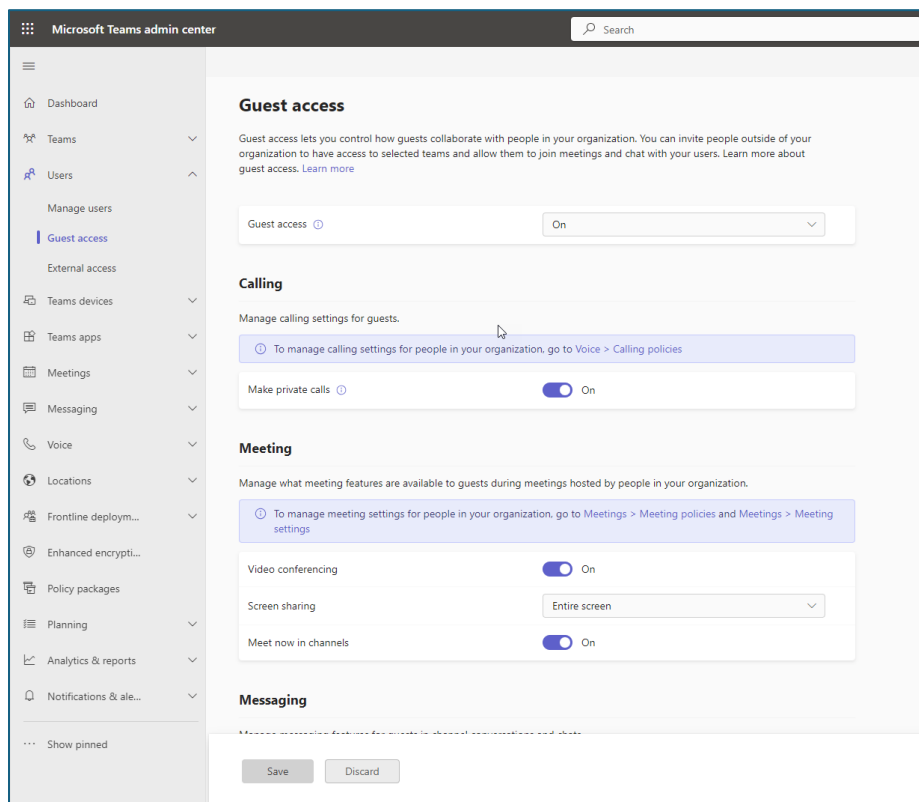


Figure 7: Admin experience at Microsoft admin center for controlling guest access.

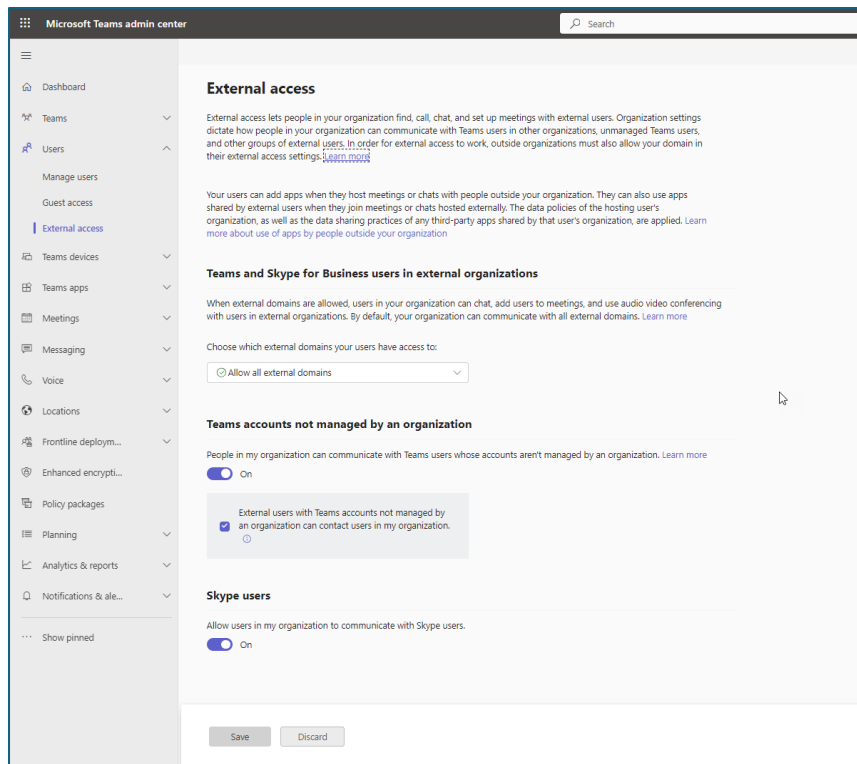


Figure 8: External access setting allows – Chat/voice calls/meetings for federation domains.

Requirements for Federation or Guest user scenarios

To test the scenarios, a Teams-DLP policy is required along with a guest and federation user. Below steps help in setting up the DLP-Policy and adding new guest users.

Step 1: Create Teams-DLP policy

DLP policies help organizations prevent data loss. The process of creating a unified DLP policy with Teams as the workload is explained in the process below.

- Sign in to the [Microsoft Purview portal](#)
- Open the **Data Loss Prevention** solution and navigate to **Policies** > + **Create policy**.

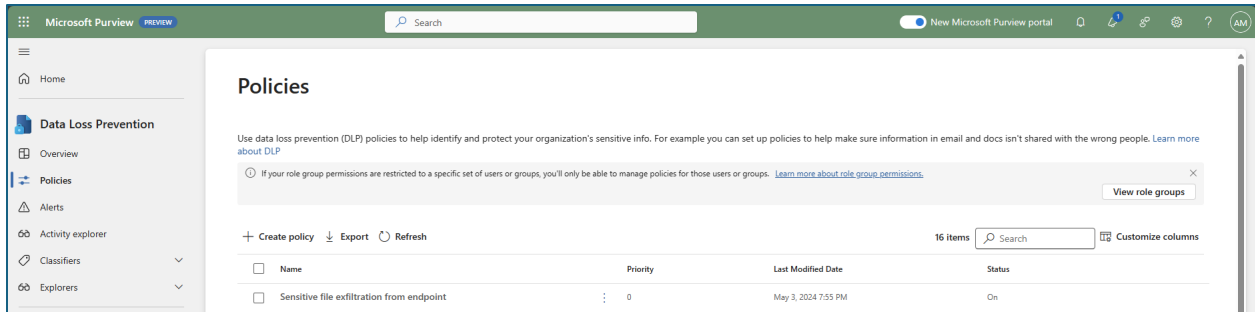


Figure 9: DLP policy creation

By default, Microsoft provides Industry standard regulatory templates to protect sensitive information. The templates have been divided into 5 categories – Enhanced, **Financial, Medical and Health, Privacy** and **Custom**. Each of the first 4 categories have pre-defined data protection templates based on industry needs. There is also an option to filter based on country and region. If your organization needs a combination of these templates or a new need that is not available in the list, select **Custom** Category – **Custom policy**. This allows you to choose sensitive types that work for your organization’s needs.

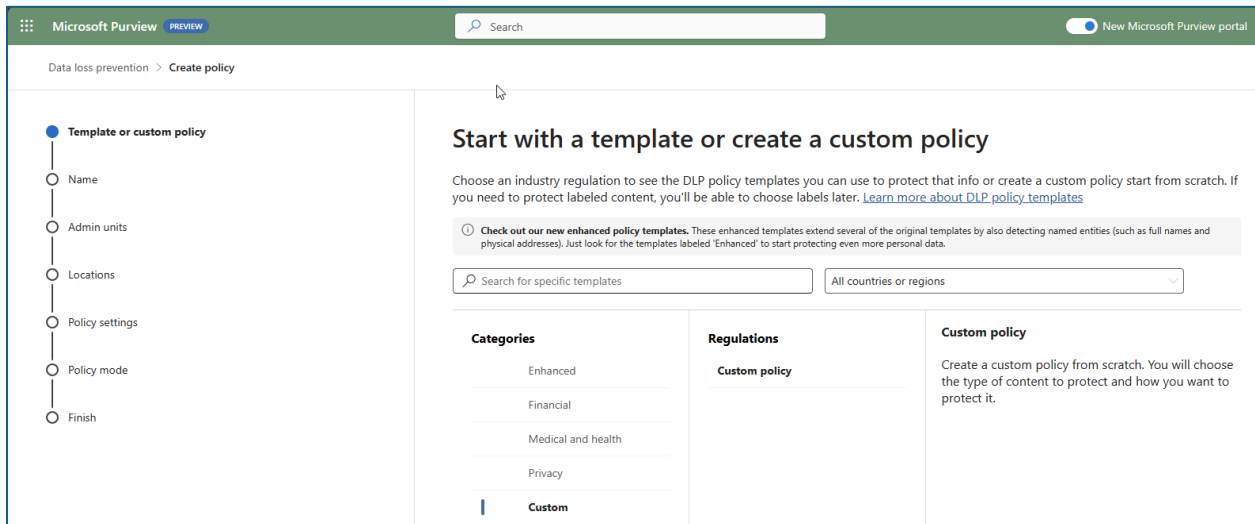


Figure 10: Selecting a template

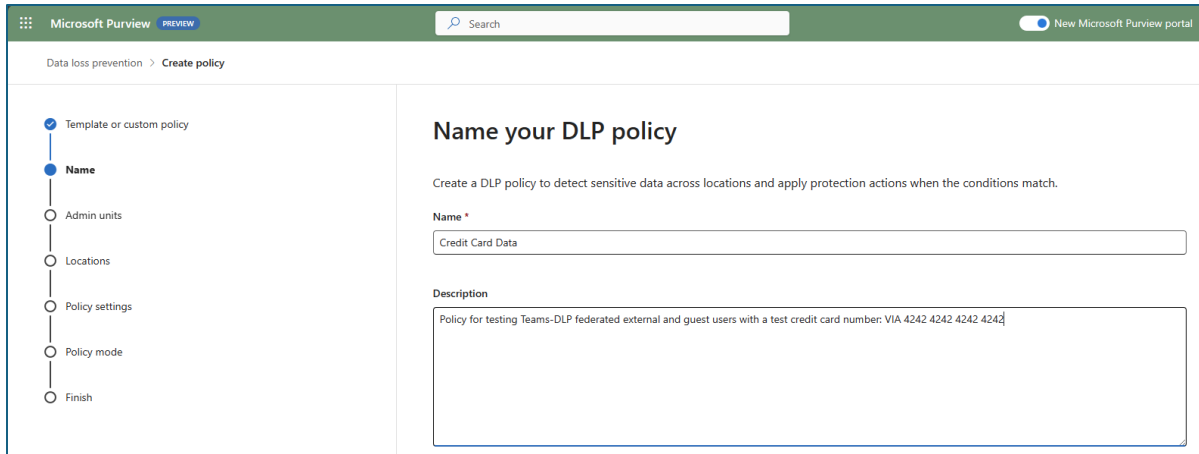


Figure 11: DLP Policy name

Next, the screen below allows administrators to select the accounts where the chosen sensitive information needs to be protected. It can be implemented across the entire organization, a particular project, or a particular entity of the organization. Also, there is an option to explicitly exclude some accounts from this protection based on the need. If you do not define any explicit inclusions or exclusions, the policy will apply to **All Employees** with No exclusions by default.

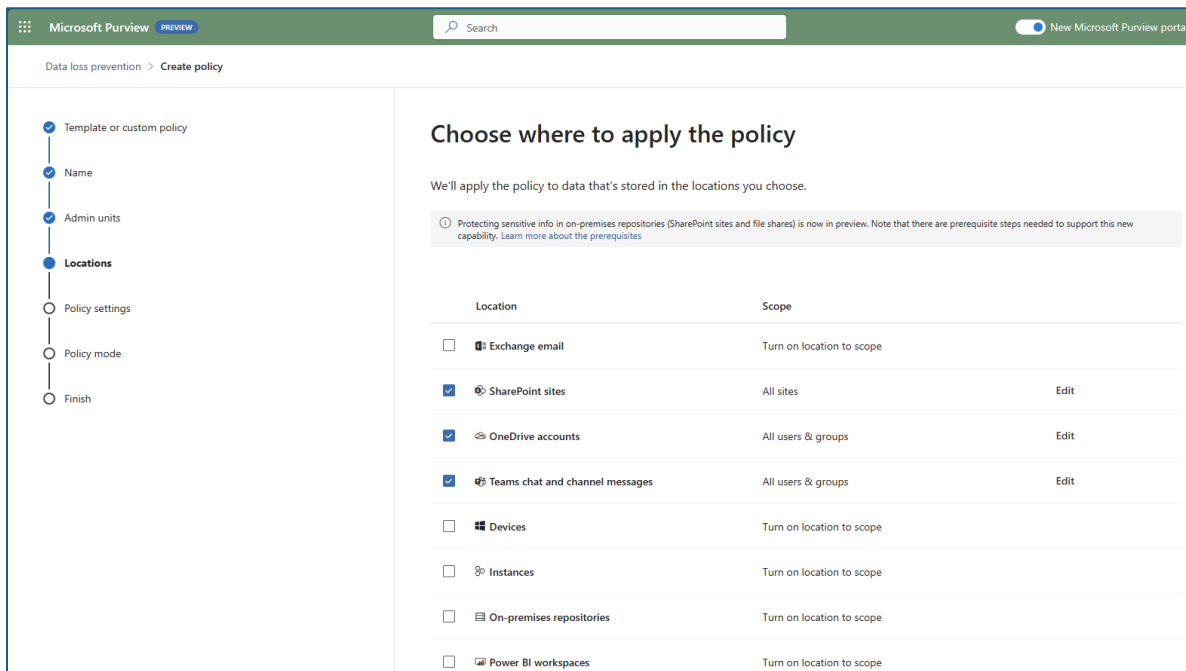


Figure 12: Policy applies to desired locations.

Once the applicable project team and business entities to be protected are selected, we need to create a rule and action on the policy as shown on the screen below.

Create a rule by adding conditions (*is this rule applicable to Within the Organization or Outside the Organization*) and under content contains, add the sensitive information types which were identified as part of the data classification needs of your organization. In the list of sensitive information types, one has the ability to select SIT's that were created using regular expressions, out of the box (OOB) provided, matching keywords and trainable classifiers.

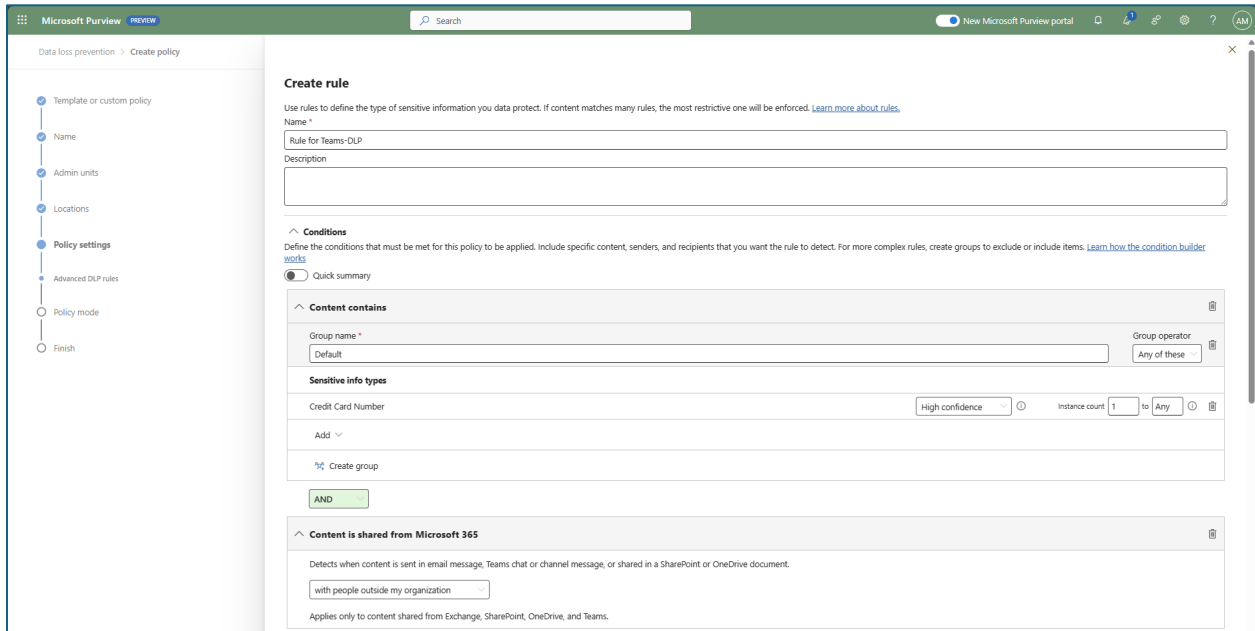


Figure 13: Creation of DLP rules

Add exceptions if any and then create actions. By default users are blocked from sending the Teams chats and channel messages that contain the SIT you are protecting. But you can choose who has access to files shared from SharePoint, OneDrive, and Teams

Click Next, you can enable the policy right away or you can choose to run the policy in simulation mode before enabling, as shown below.

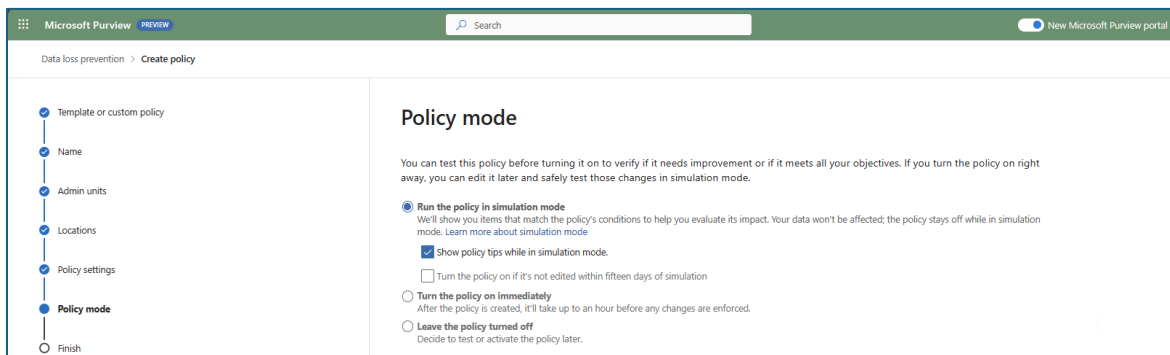


Figure 14: Test first and then deploy.

Step 2: Add a Guest User

Guest users can be added in two ways: From Microsoft Entra or from the Channel->Add member screen in Teams.

New user - Microsoft Entra admin center example

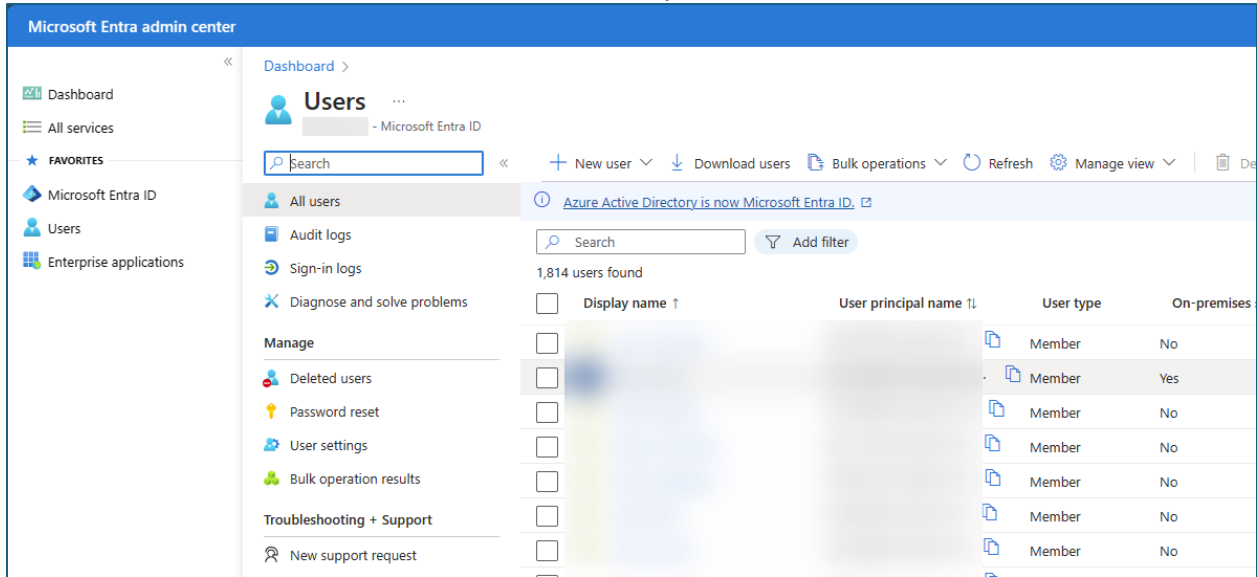


Figure 15: Adding a guest user through Entra ID (formerly Azure Active Directory).

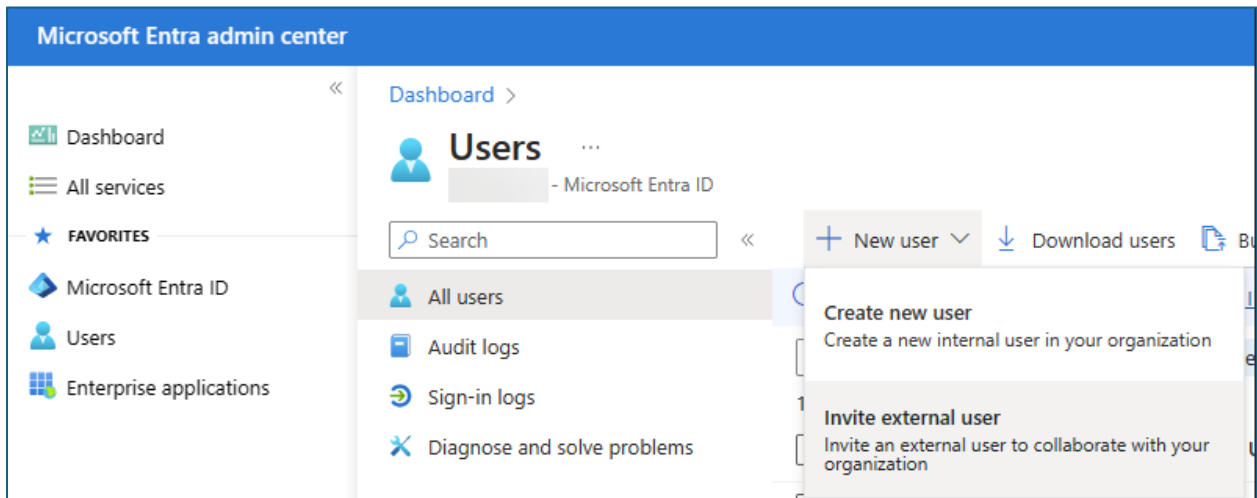


Figure 16: Sending the Invite to a guest user

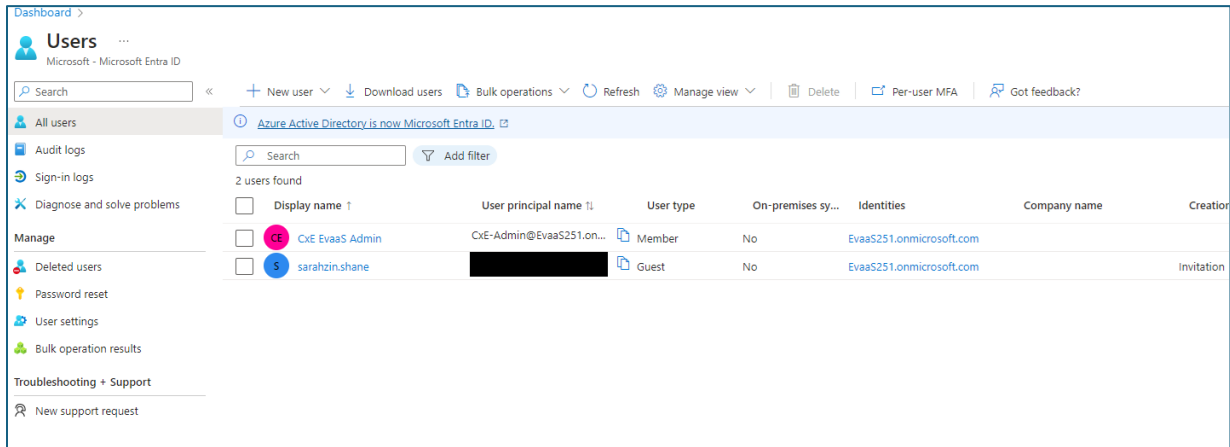


Figure 17: The user added to AAD

Once added the new guest user receives a message as shown below:

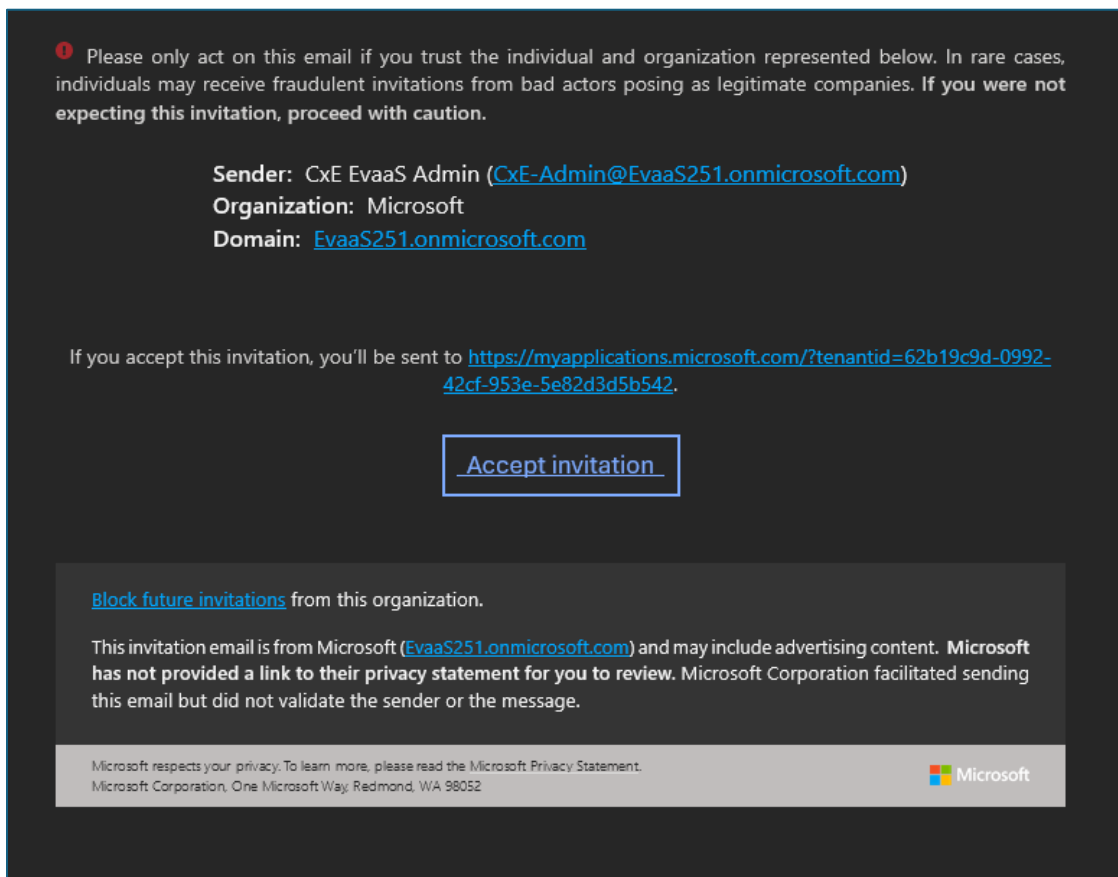


Figure 18: E-mail message to guests with a link to accept

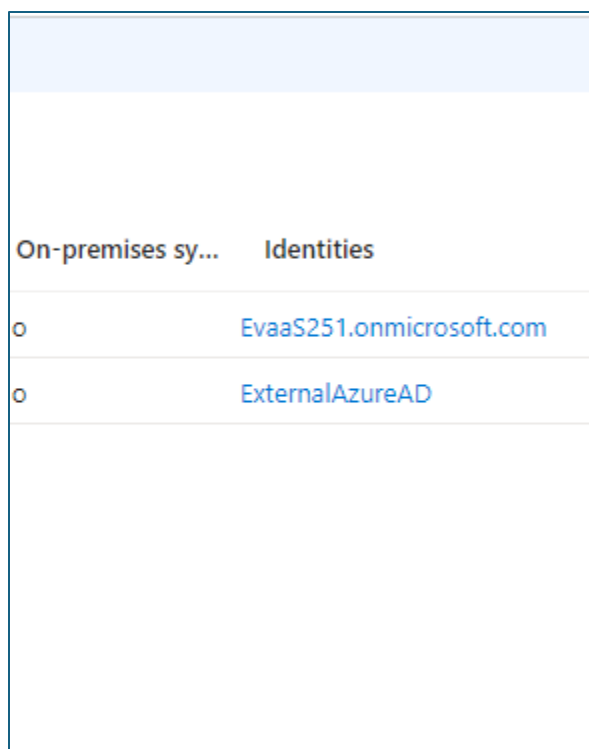


Figure 19: Identities changes for the external user after accepting.

From this point the user is a member of AAD and has access to all tenant resources, just like an internal user. The admin can restrict access based on organizational needs.

Step 3: Create a Teams Channel

In the above steps, we have created a DLP policy and added an external user. It is important to consider protecting your Teams channel messages holistically and not just individual files within those sites. There are various control options available in the M365 compliance center to enable various group settings and to restrict sharing of sensitive information via chat or by sharing the files. The sensitivity labels are then available to a user who is creating a new team.

At a Team channel or site level, three types of controls are possible:

1. Who can join a Team? a. Privacy – **Public** vs **Private** b. Choose **public** for anyone in your organization to join the team, or **private** for only selective members can join the team. c. Control whether the Team owner can add guests to the team.
2. Control access to Teams sites from unmanaged devices a. For unmanaged devices (those not hybrid AD joined or complaint on Intune), allow full access, web only access, or block access completely.

3. Granular control for external sharing of files in Teams sites. a. Choose the level of external sharing: anonymous, secure external sharing, or block external access completely.

Let us create a Teams channel and add a user to the channel:

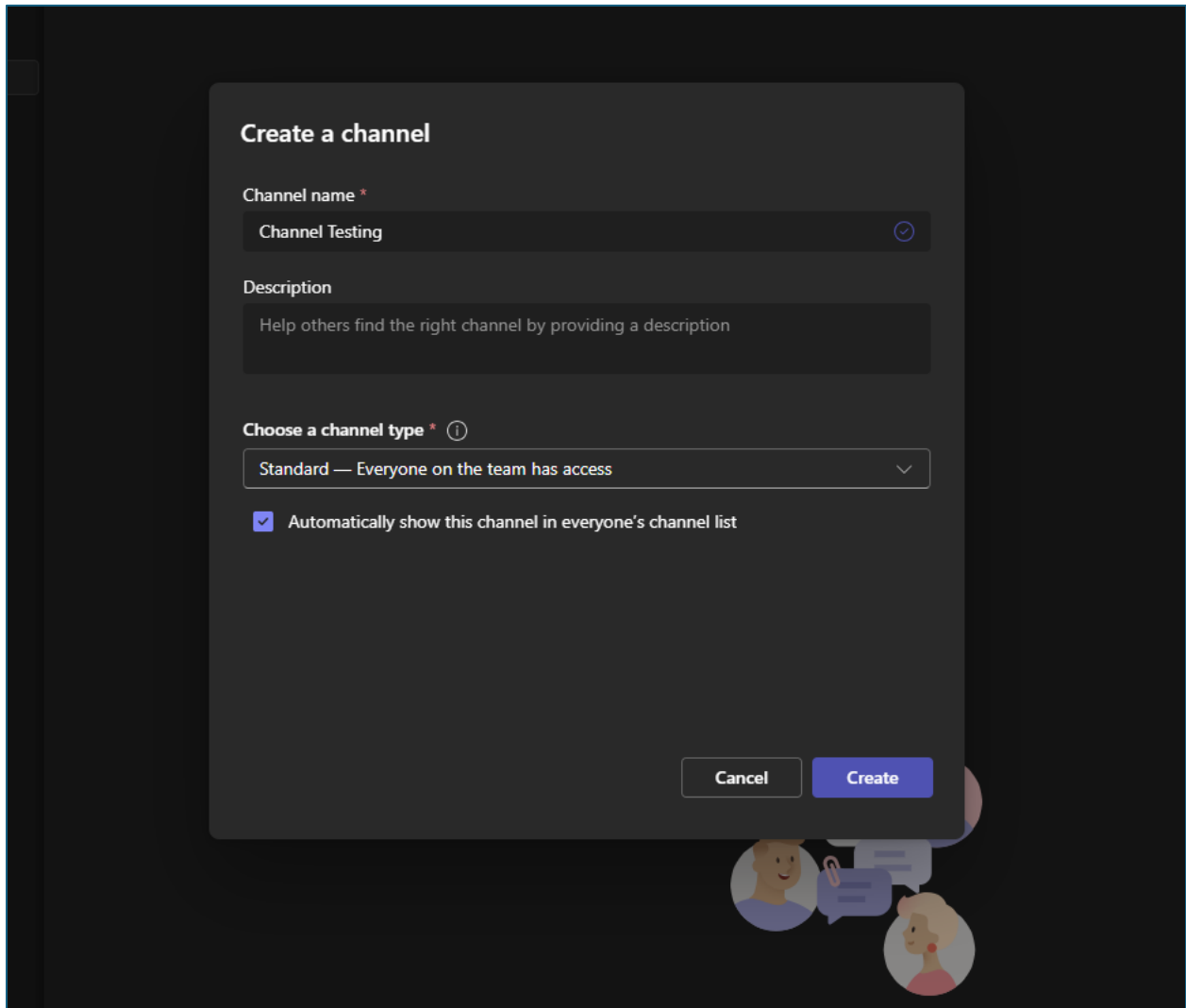


Figure 20: New Teams Channel creation

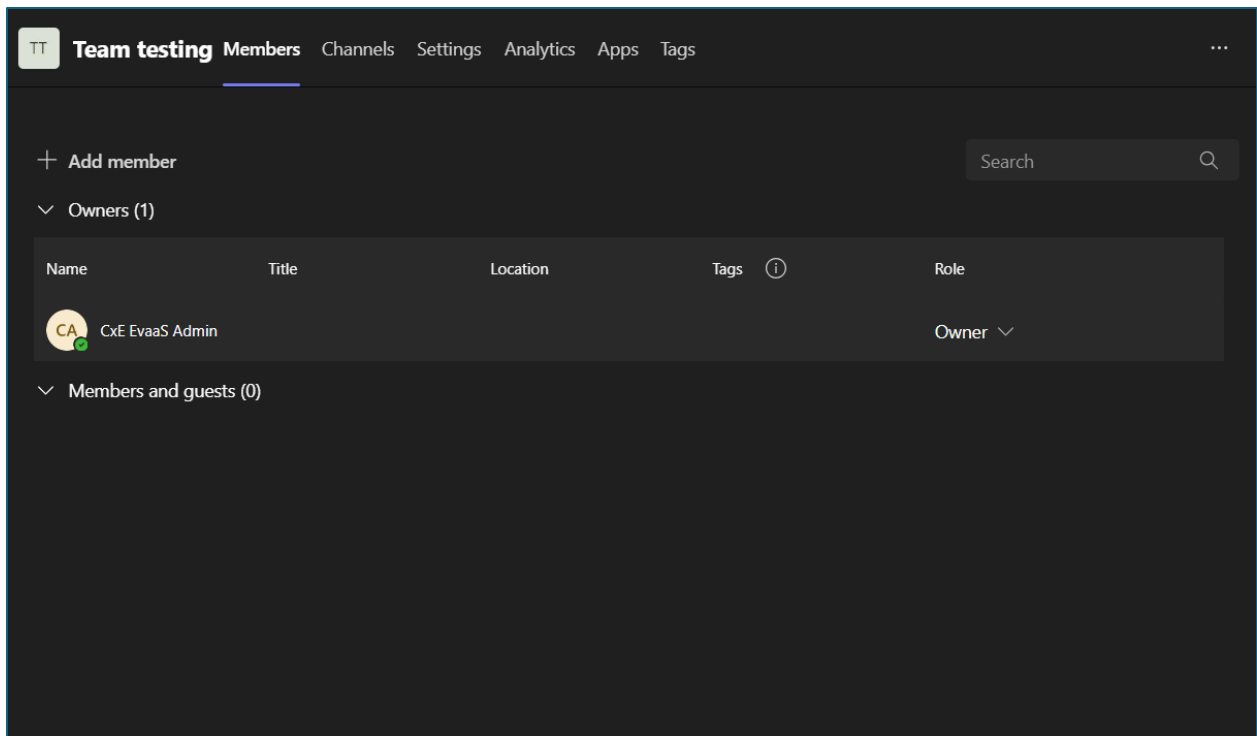


Figure 21: List of members

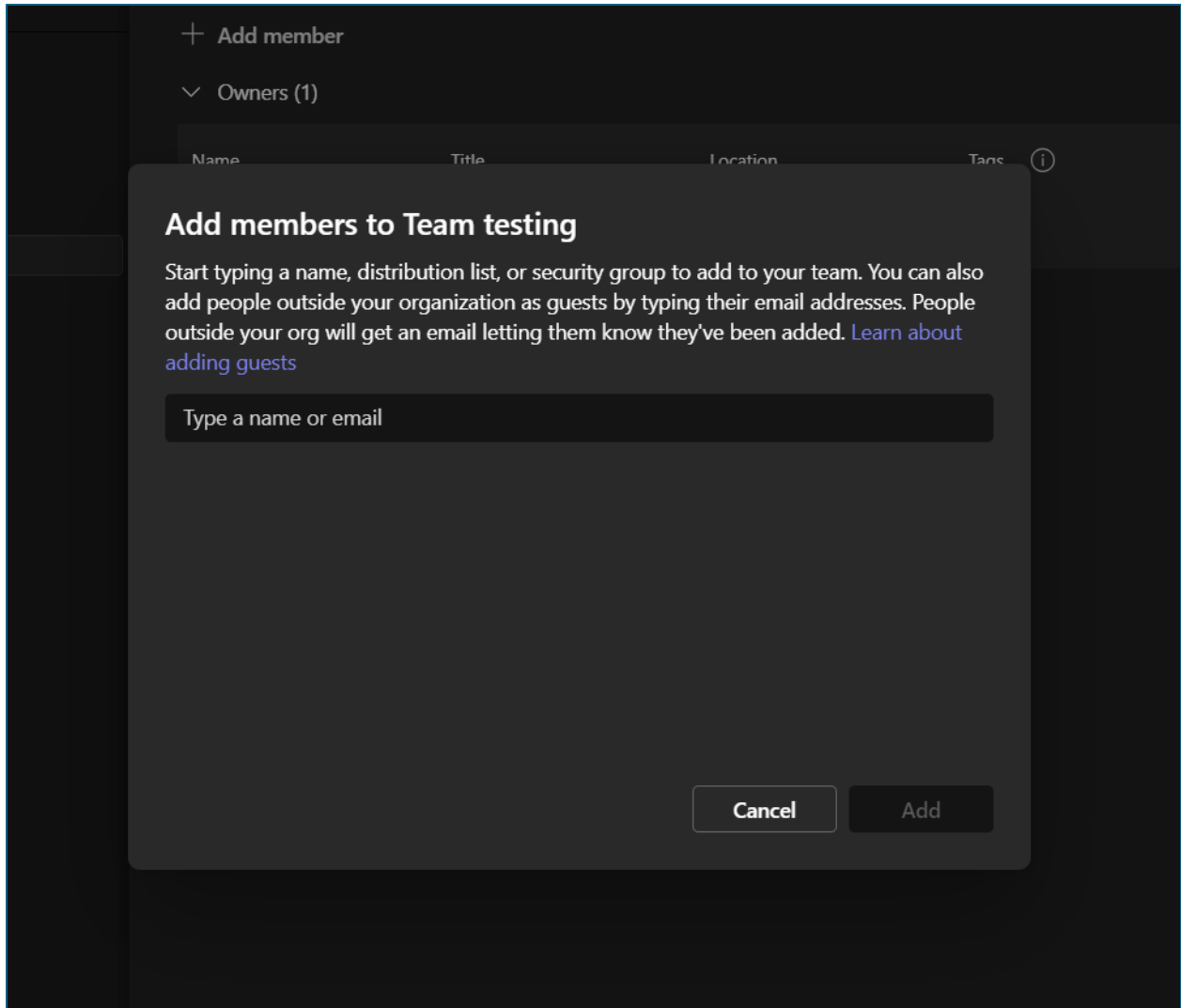


Figure 22: Adding members

Next add a new external user to the newly created channel. Please note that the first user was added through the AAD admin center and this external user is being added through Teams channel -> Add member.

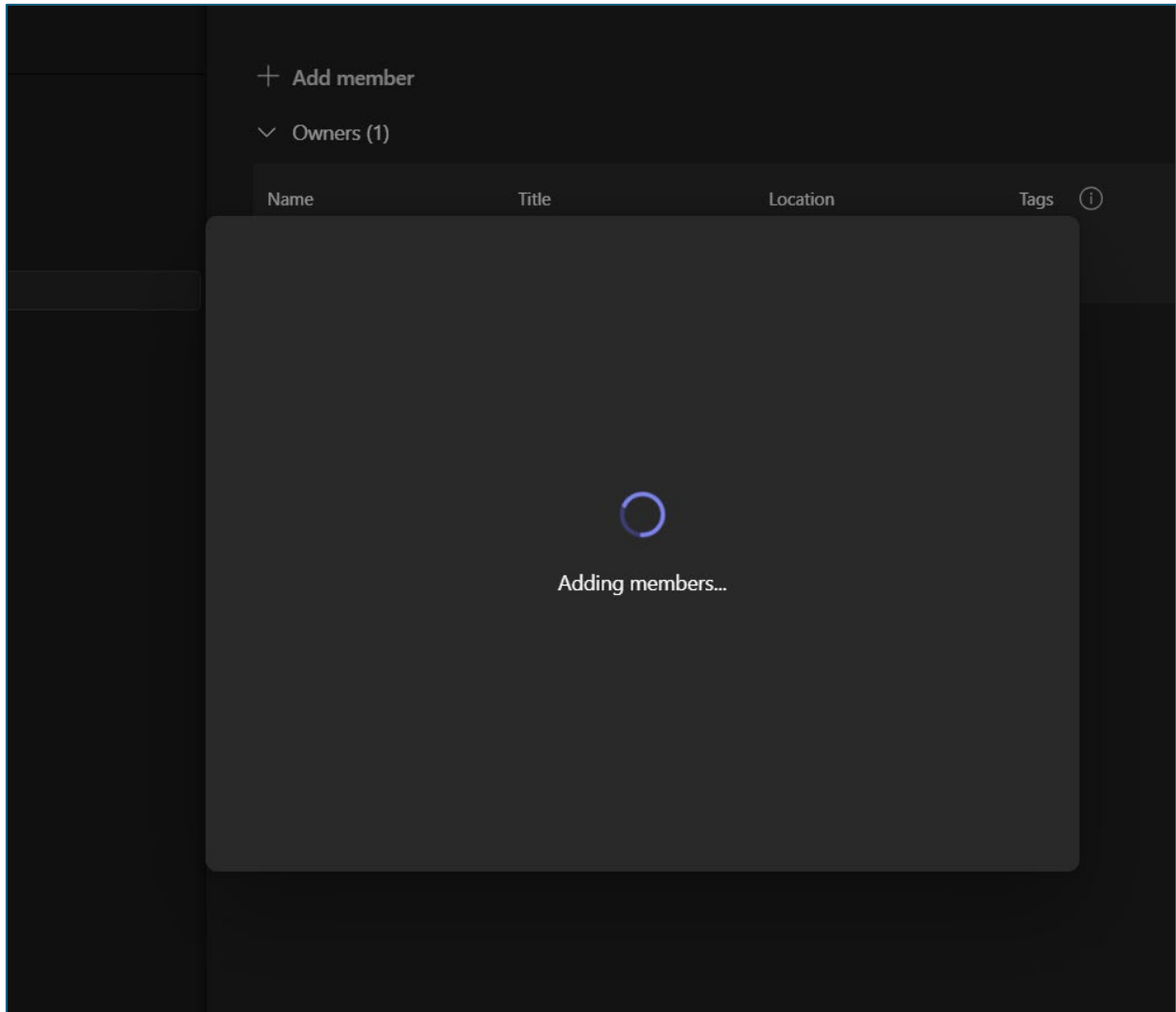


Figure 23: Adding guest users as a member to the newly created channel

Please note that this newly added user will automatically be added to AAD, as displayed below:

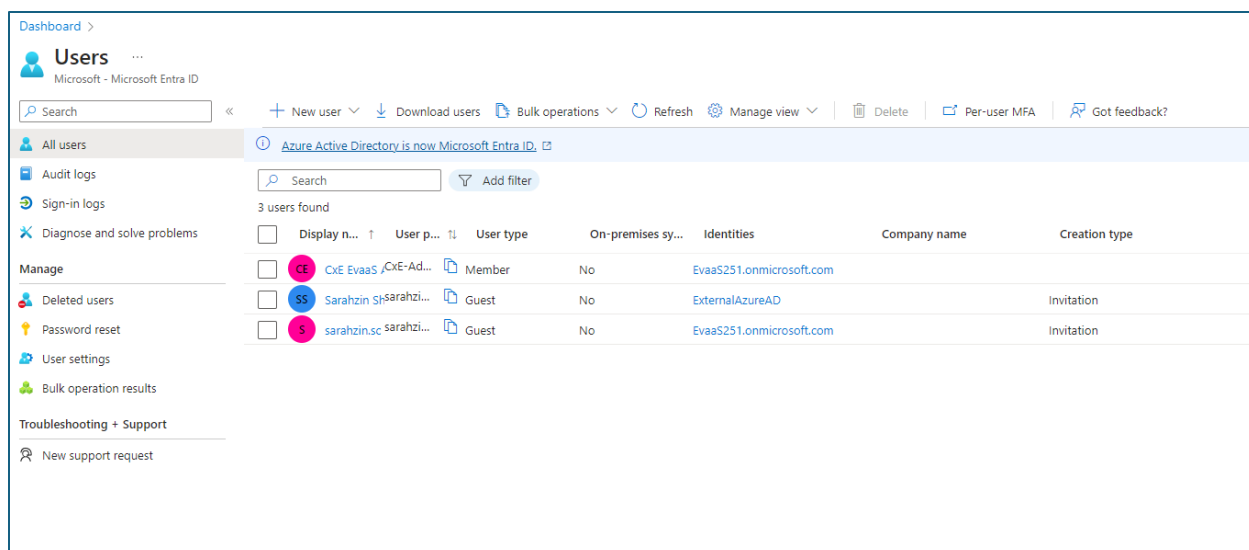


Figure 24: Checking the added user from the AAD admin center

In the above steps, we have added 2 users. These 2 users are now added to AAD.

Step 4: Add External (Guest) or Federation User

Next, let us attempt to add a new user, who is a federation and should not be part of AAD. Refer to [here](#) for more details.

When trying to add the 3rd new user to the existing Teams channel, assume that the user has an O365 license in the tenant. When attempting to add the user directly from Teams, the application only allows the user to be added as a guest user. Since we do not want this user to be added to AAD we will keep them as federation users (or One-time chat user).

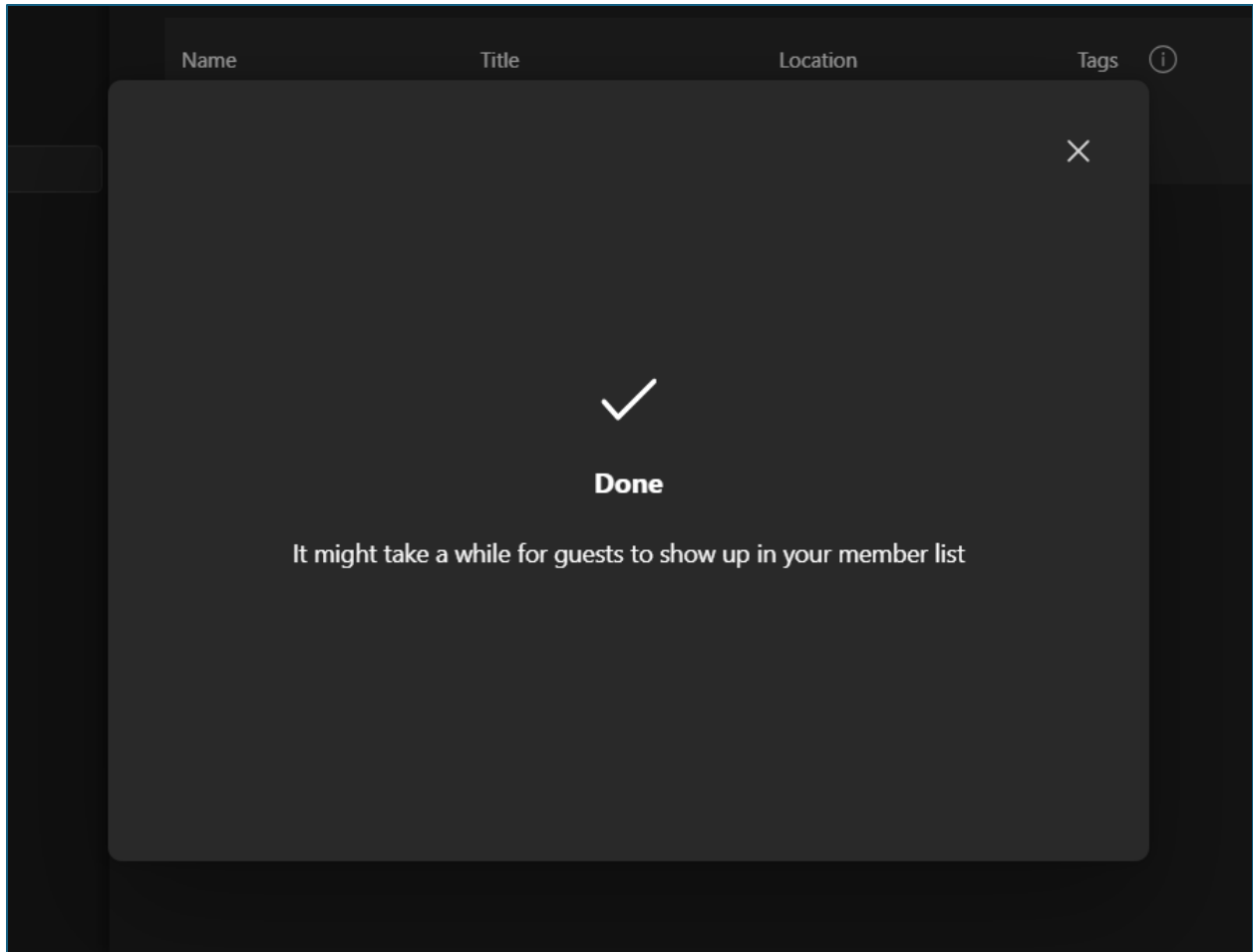


Figure 25: Trying to add a Federation user to the channel.

We now have 2 guest users, a federation user, a Teams-DLP rule, and a Teams channel. We are ready to test the scenarios.

User Experience

Scenario 1: Sharing Credit card details to a Federation user via 1-1 chat.

Sender's Screen:

The Sender is attempting to send credit card information to the newly created federation user via 1-1 chat:

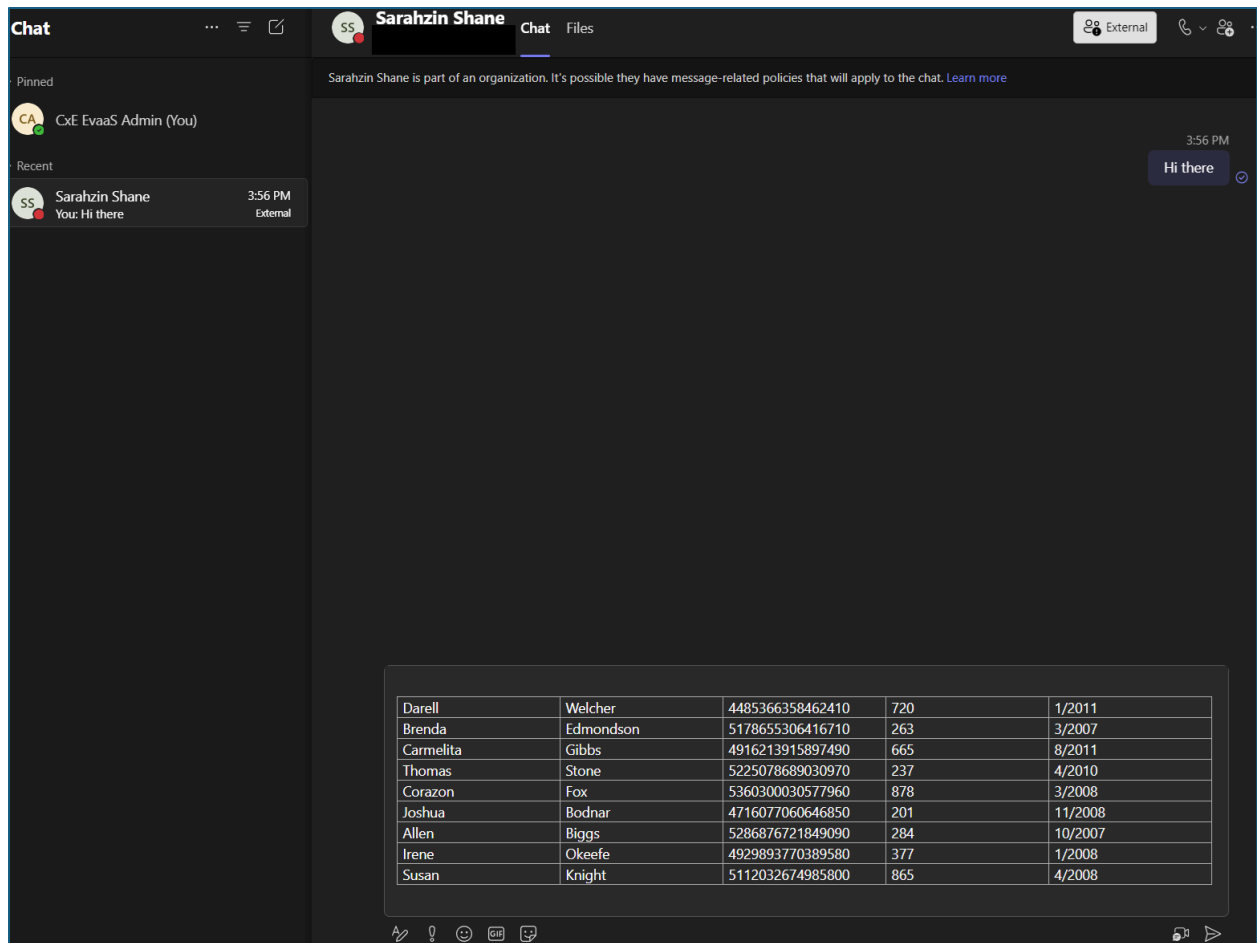
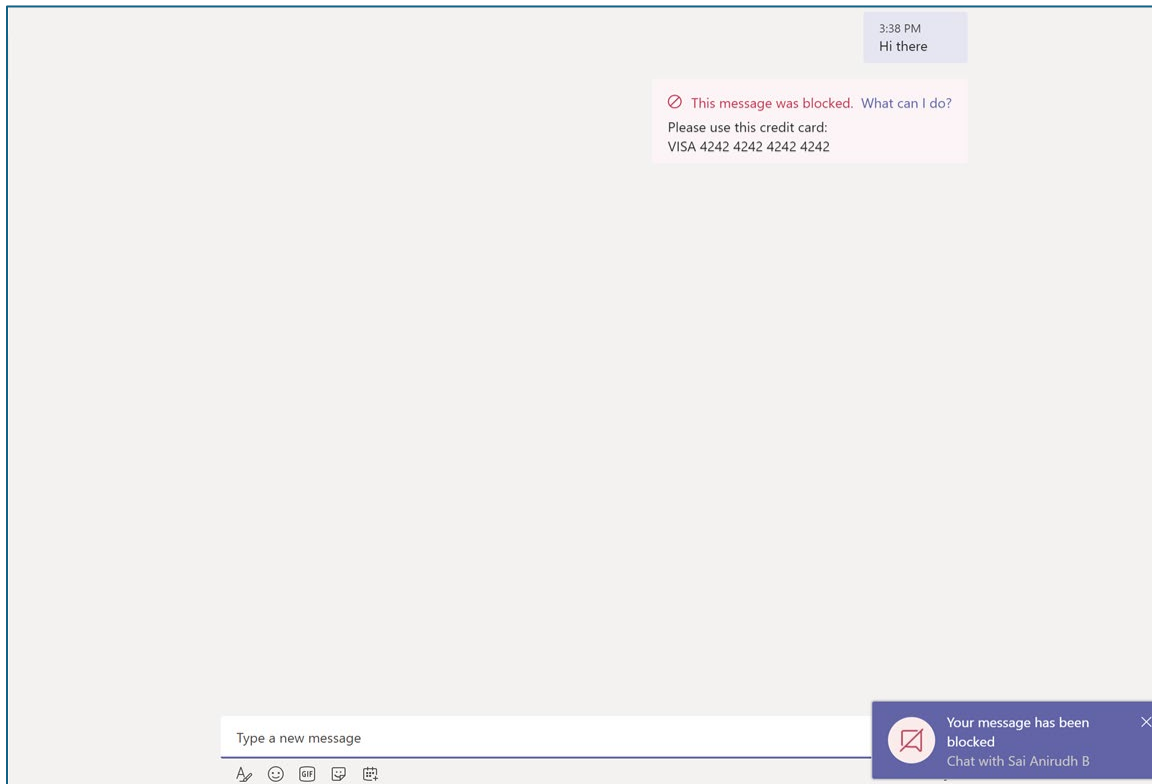


Figure 26: Credit card information in Team chat

The message is blocked as the DLP rule is activated and the sender is notified:

Figure 27: Blocked credit card message



Receiver Screen:

The receiver gets a blank blocked message, as shown below. Please note that there will be a delay of a few seconds in blocking the message and which is normal behavior (passive DLP).

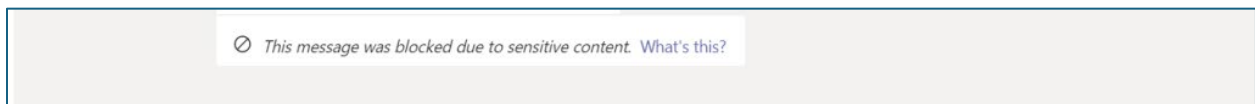


Figure 28: Blank blocked message

Scenario 2: Sharing a file from SharePoint /OneDrive to Federation user.

Senders Screen:

The Sender is trying to attach a file which has credit card information via 1-1 chat:

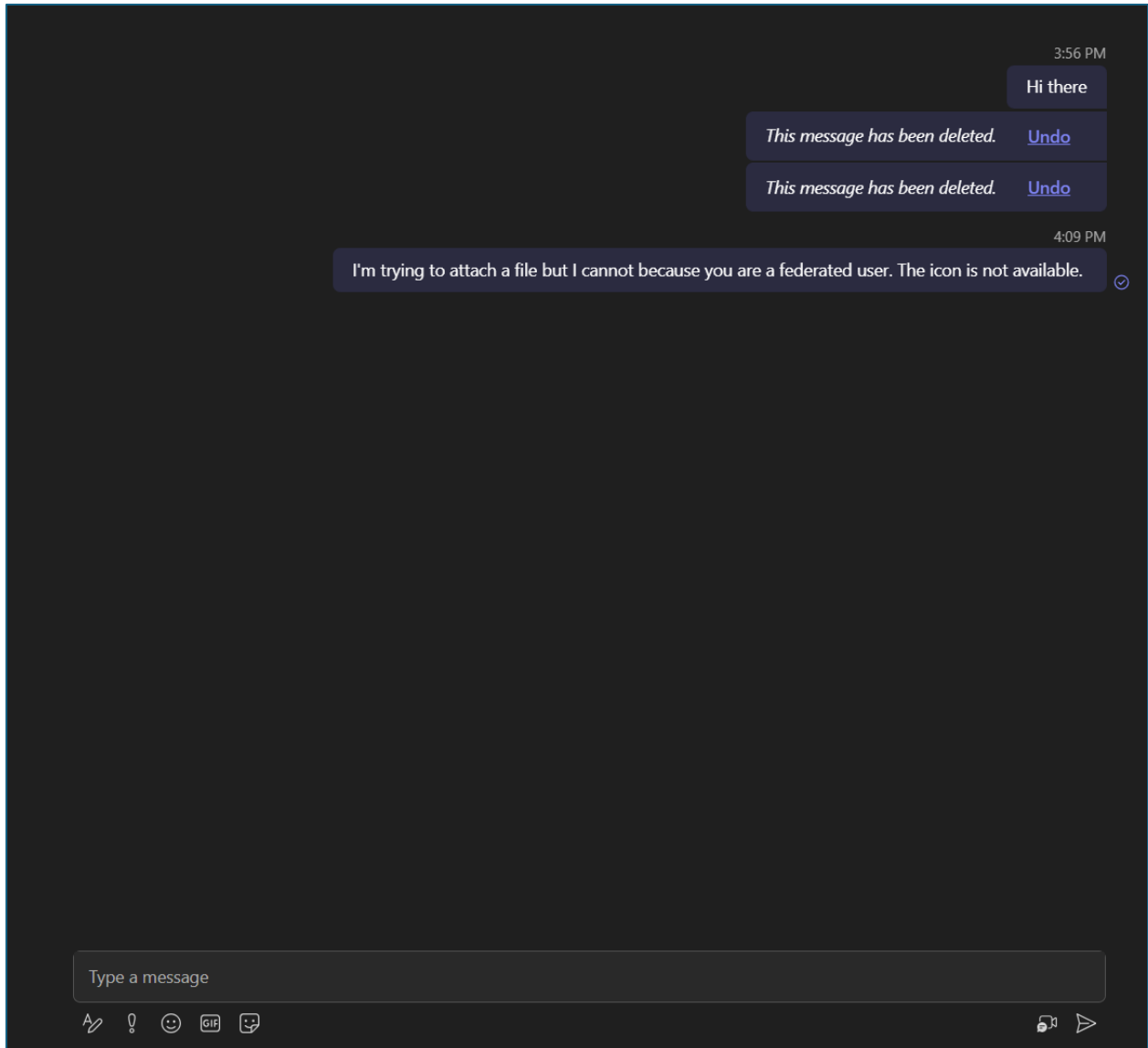


Figure 29: Option to upload files missing

Notice there is no option to upload a file to the federation user since they are not in AAD.

Receivers Screen:

In this scenario the receiver will not get a message.

Scenario 3: Sharing Credit card details with a Federation user via 1-1 chat.

If the federation user (Sender) has shared a SIT via 1-1 chat, the DLP rule acted will be based on the federation user organization policies. In the above scenario, if a credit

card is not a SIT in the federation user's organization, the message will come as-is to the receiver. The receiver will not have any control over the federation users' DLP policies.

Scenario 4: Sharing Credit card details to Guest user via 1-1 chat.

The Sender and Receiver can chat, just like an internal user since the guest is a member of AAD. The Sender then attempts to share sensitive information via chat:

Senders Screen:

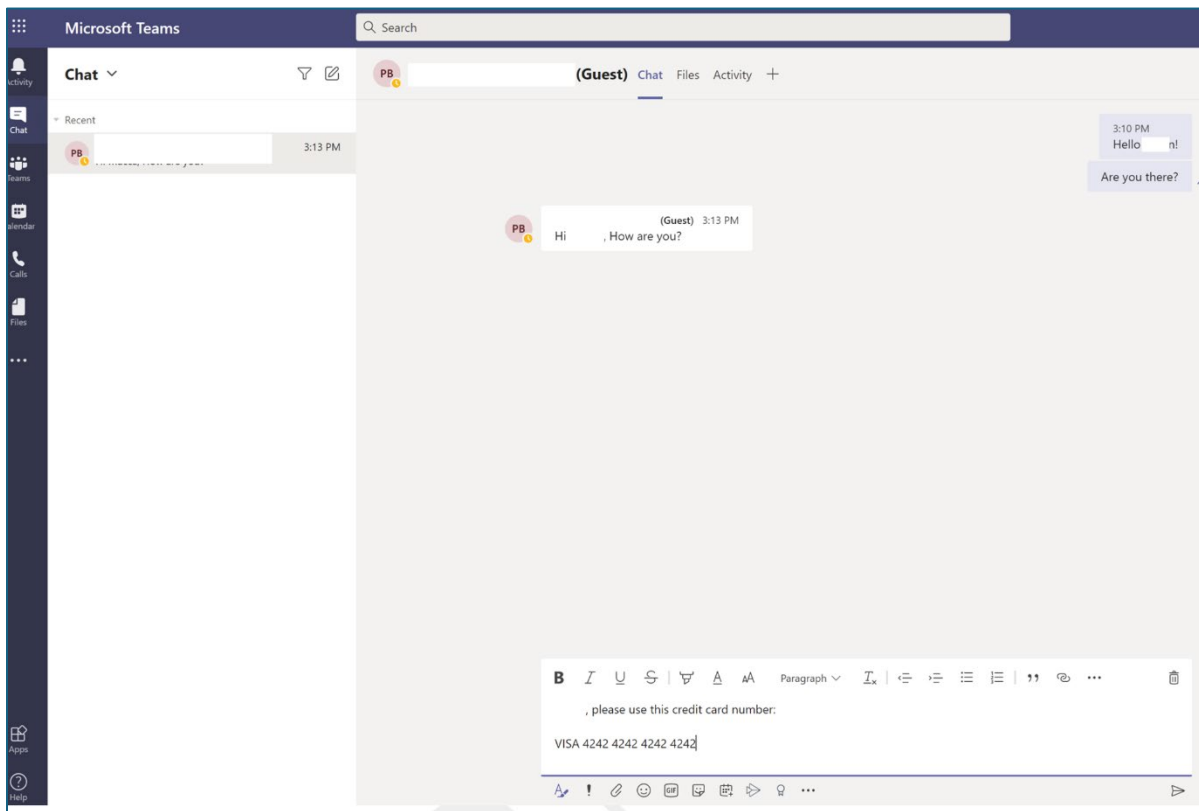


Figure 30: Guest user Teams chat

The DLP rule is activated and the message is blocked:

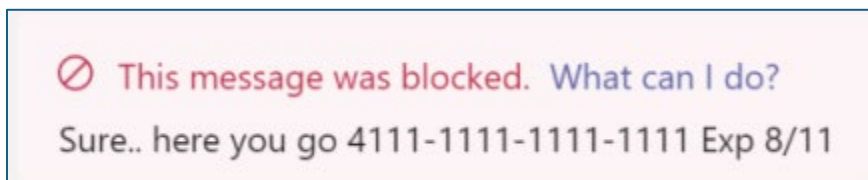


Figure 31: DLP blocked message

Receivers Screen:

The Receiver receives the blocked message, as shown below:

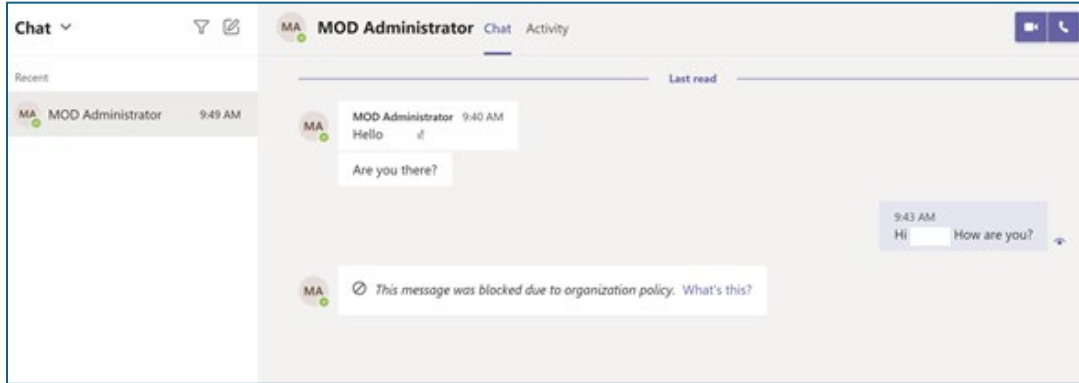


Figure 32: Blocked message to receiver

Scenario 5: Sharing a file via 1-1 chat with Guest User.📌

Senders Screen:

The Sender is trying to attach a file, which has credit card information, via 1-1 chat to the guest user:

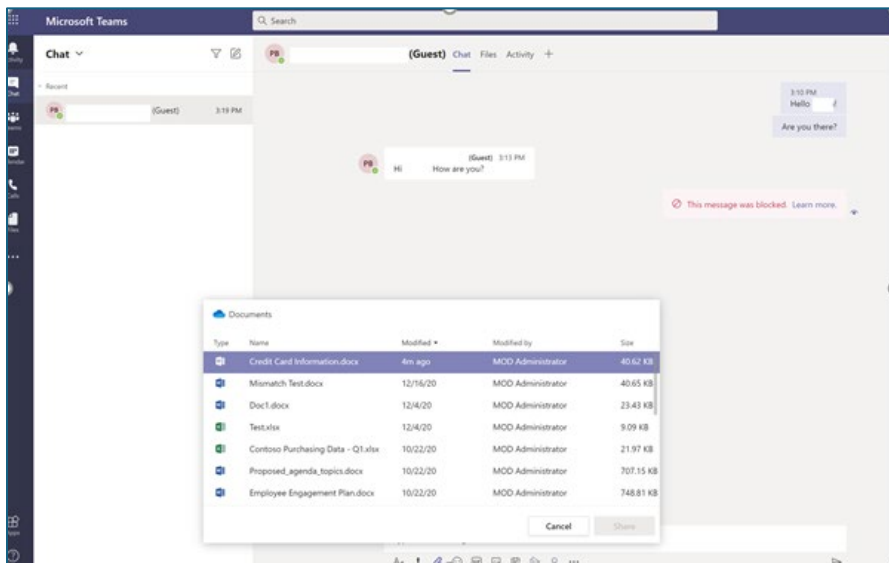


Figure 33: Attaching a file in chat with credit card information

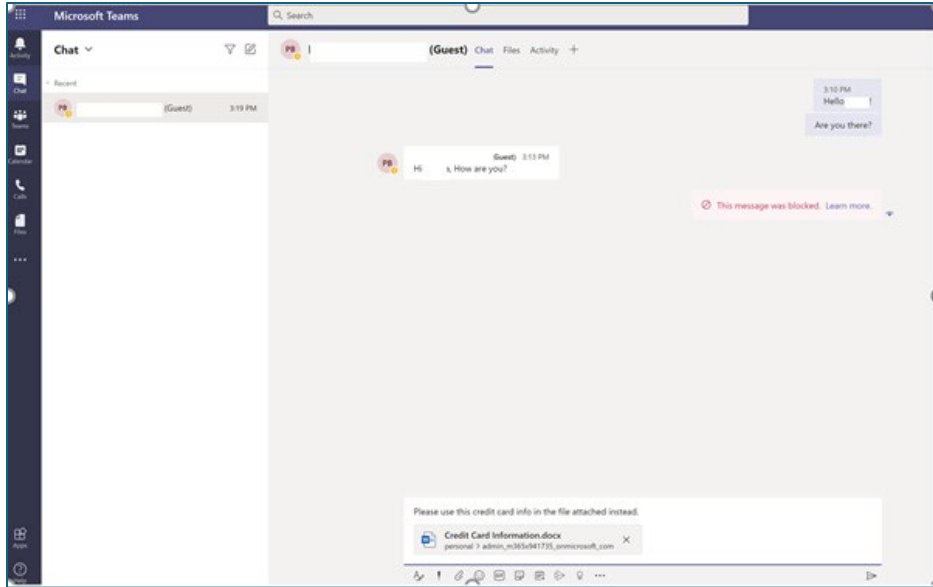


Figure 34: Attaching a file in chat with credit card information

Receivers Screen:

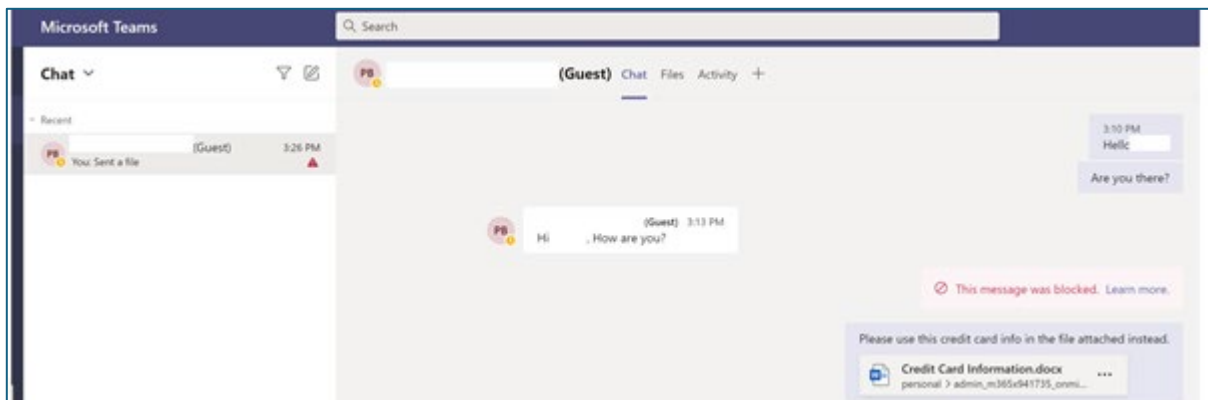


Figure 36: Message

This message was received by the receiver:

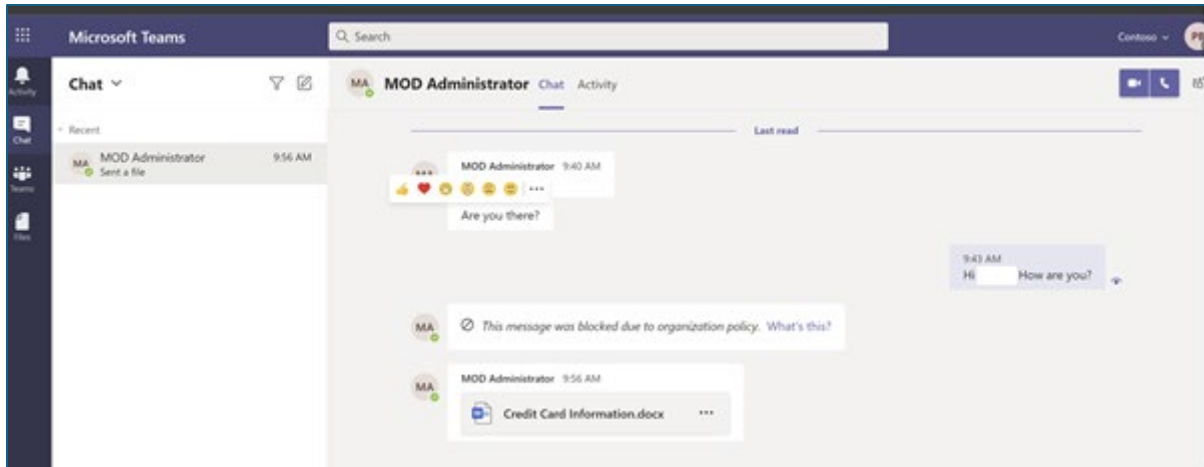


Figure 36: UI message to receiver

The receiver while attempting to open the attachment:

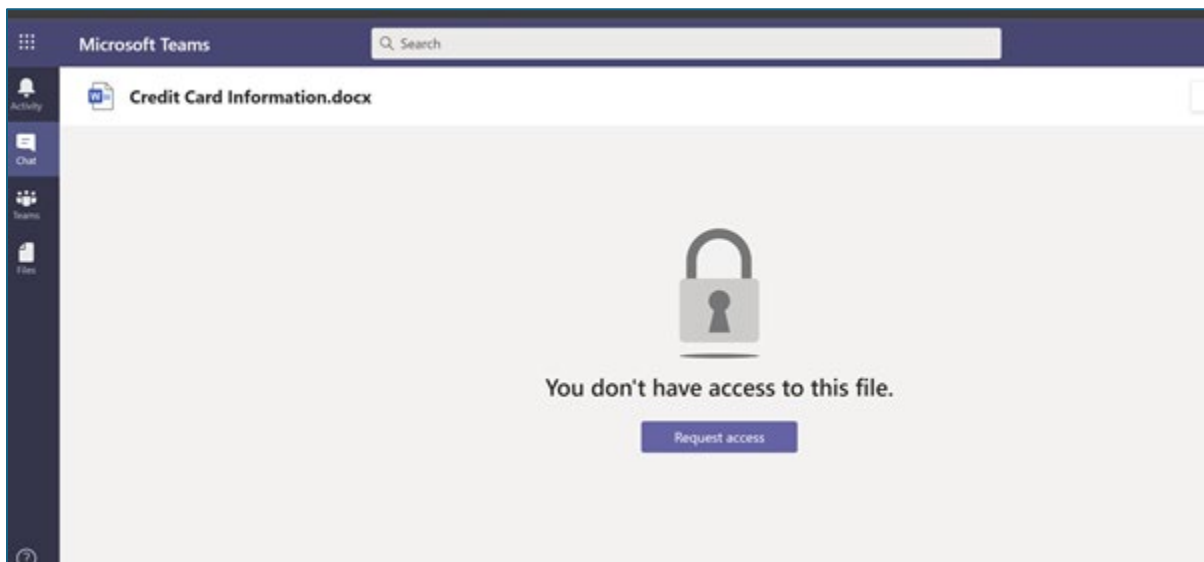



Figure 37: Error message when opening file

And upon clicking **Request Access**:

Access Denied

Due to organizational policies, you can't access these resources as a guest user.

Here are a few ideas:

 Please contact your organization.

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

Correlation ID: be5b999f-a0e7-0000-5e43-437da5dd917a

Date and Time: 12/20/2020 8:29:21 PM

User: _m365x708261.onmicrosoft.com#ext#@m365x941735.onmicrosoft.com

Issue Type: User has encountered a policy issue.

Figure 38: Access Denied message

Scenario 6: Sharing Credit card details to Guest users via Teams channel chat.

Senders Screen:

The Sender attempts to share a credit card number via the channel chat:

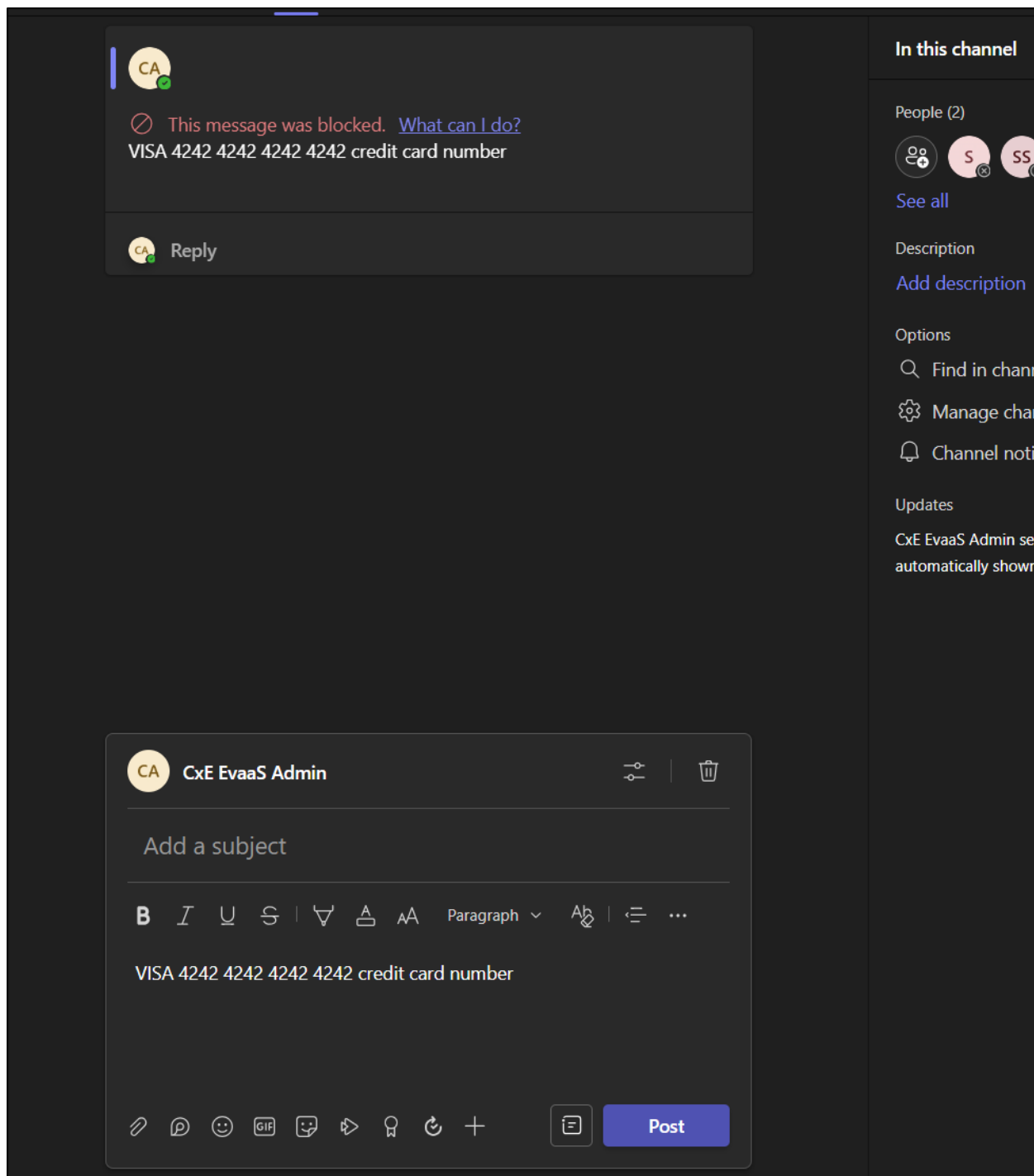


Figure 39: Attaching a file in channel with credit card information

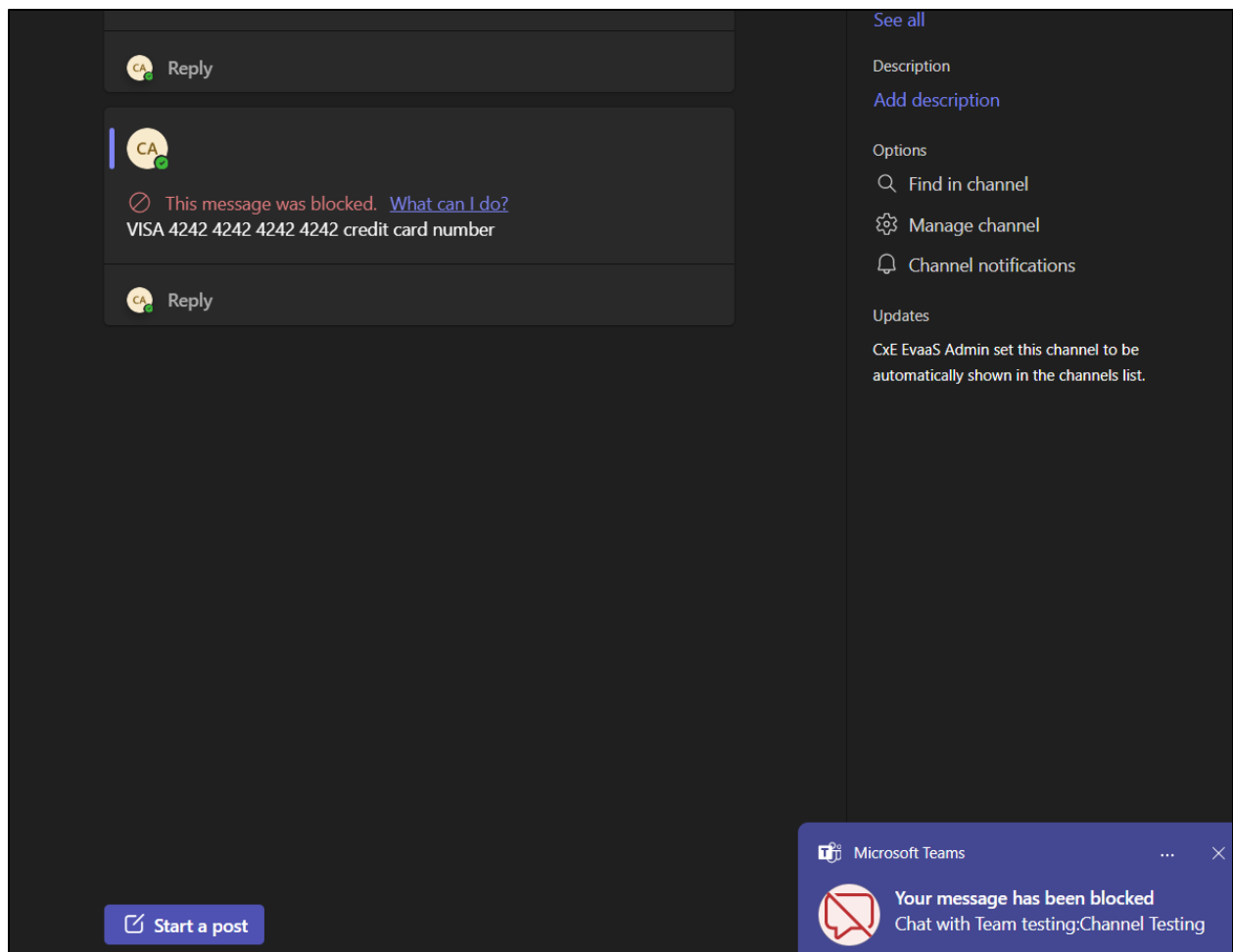


Figure 40: Attaching a file in channel with credit card information

Receivers Screen:

The message was blocked.

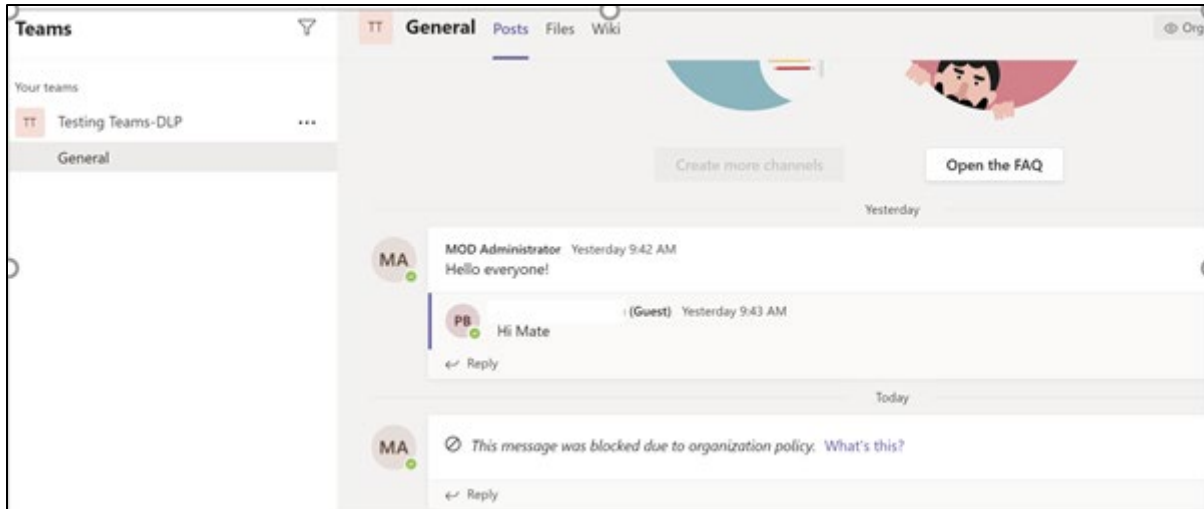


Figure 41: Message blocked in Teams channel

Scenario 7: Sharing a file to a Guest User on Teams channel

Senders Screen:

The Sender attempts to share a file that has credit card number details over the chat in the channel:

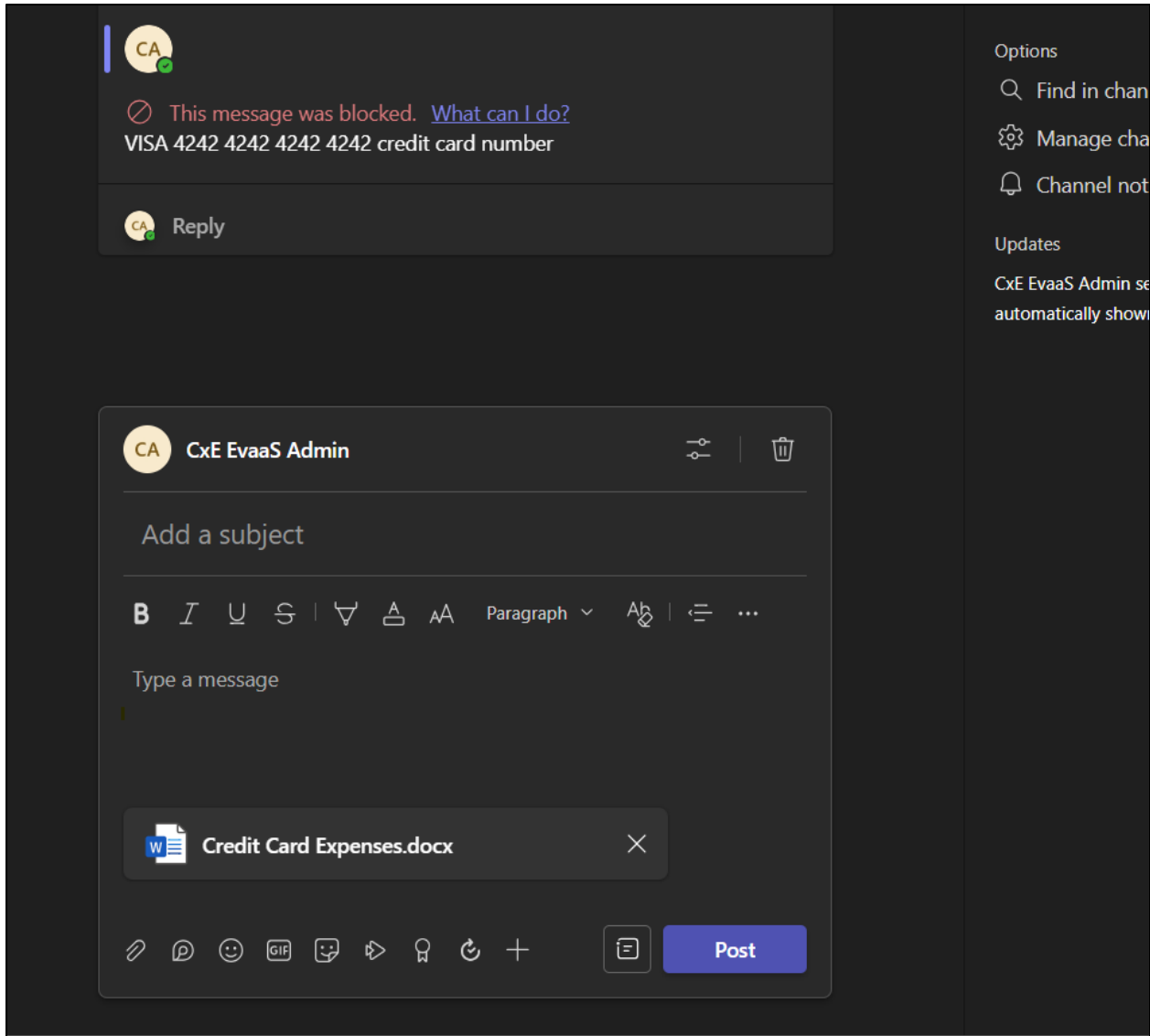


Figure 42: Attaching a file in channel with credit card information

Receivers Screen:

The Receiver gets the message and, upon opening the file, receives an access denied message.

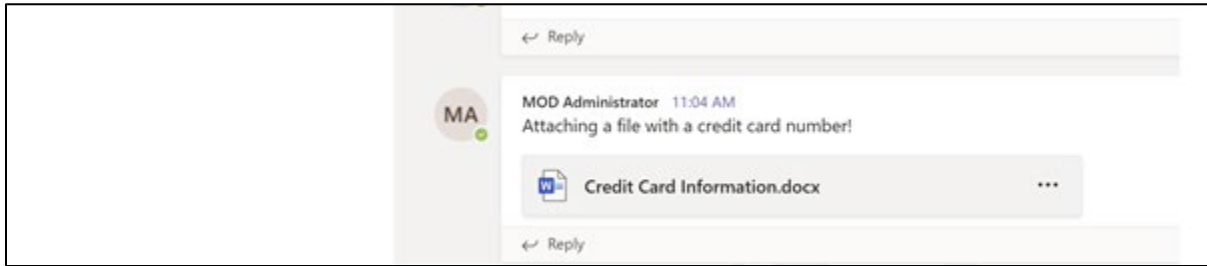


Figure 43: Error messages when opening

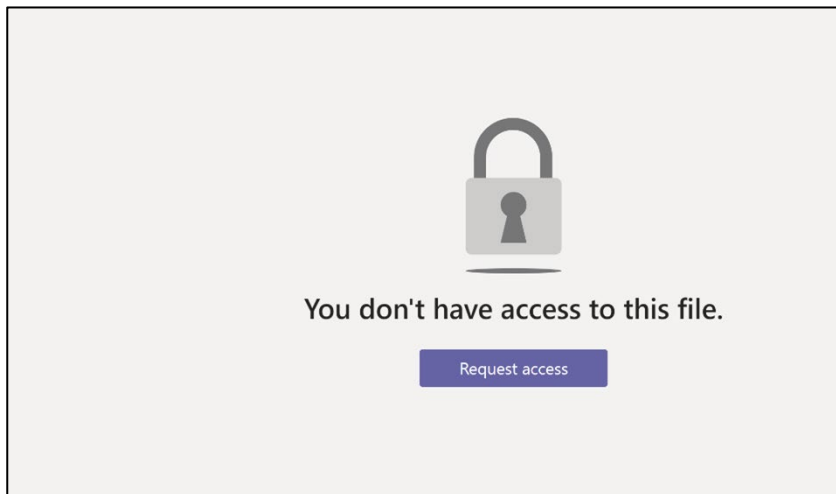


Figure 44: Error message.

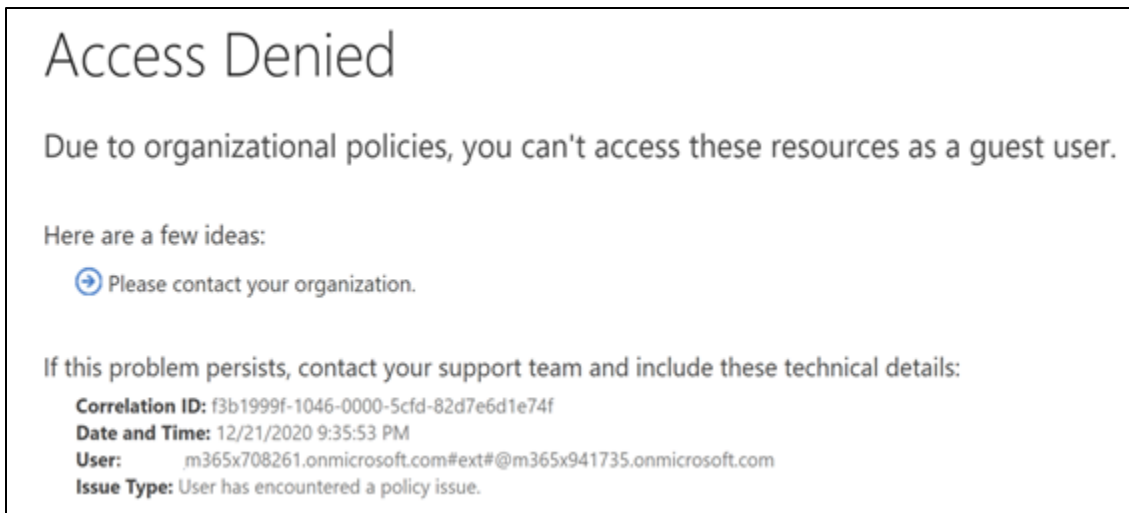


Figure 45: Error messages when opening

Implementation Strategy

See [Microsoft 365 productivity illustrations](#) for guidance on implementation of all M365 capabilities with a focus on cross technologies.

Based on experience, a solid Implementation strategy follows these three phases:

Crawl -The first stage is about starting to evaluate where your organization is today regarding security and compliance with your goal of defining a strategic direction for your company. Use this strategy to foster adoption of a solution by gathering the requirements of supporting systems, impact on end users, and skillset needed for each role owner. The crawl phase describes steps you should do at the beginning of any deployment, whether your requirements are basic or advanced. It includes steps for education, defining requirements, and evaluation or testing.

This phase is primarily to identify data classification needs like identifying the key critical Sensitive Information Types (SIT).

Walk -The second stage builds the foundation for a successful, scale, and sustainable deployment. In this phase, you plan the details of your implementation and to build the solution. You may also run a pilot or proof of concept with a select group of users or locations.

This phase deals with protecting the identified SITs. This can be done either by labelling the documents or by applying rules across workloads. Test these policies on certain users/groups before deploying directly into production.

Run -The last stage is about optimizing the solution for Microsoft 365. In this phase you will set up an automated scalable approach for each solution.

Keep monitoring the results and fine tune the rules. Validate the results through alerts and take measures.

Abbreviations

Name	Description
MIP	Microsoft Purview Information Protection
DLP	Data Loss Prevention
SCC	Security and Compliance Center

Name	Description
RBAC	Role Based Access Control
SIT	Sensitive Information Type
SPO	SharePoint Online
EXO	Exchange Online
ODB	OneDrive for Business
OOB	Out of the box
AAD	Azure Active Directory