CHAPTER 5

Microsoft Teams Governance and Life Cycle Management

You have already learned that Microsoft Teams is built on Office 365 Groups, which is part of Office 365 that includes multiple tools to design governance capabilities that organizations require. This chapter provides you with a comprehensive overview of Microsoft Teams governance and life cycle management. Managing governance and life cycle management for Teams is essential for consistent and coordinated interaction between users and allows them to collaborate with confidence. Prior to deploying Teams, you as a Teams admin must consider things, like who can create teams, how to handle unused Teams, who can create private channels, what the Teams naming convention is, and so on. Also, you will learn the features that you can use for Teams governance, such as group creation, classification, expiration policy, sensitivity labels, data loss prevention policies, and naming policy.

After completing this chapter, you will be able to do the following.

- User provisioning Configure and manage conditional access policy.
- Manage information protection using data loss prevention (DLP).
- Create and manage eDiscovery for Teams.
- Manage data governance and retention in Teams.
- Manage internal risk through information barrier (IB) in Teams.
- Create and manage Office 365 Group classification for Teams and Outlook.
- Create and manage Office 365 Group expiration policy for Teams.
- Create and manage Office 365 Group naming policy for Teams.

B. N. Ilag, *Understanding Microsoft Teams Administration*, https://doi.org/10.1007/978-1-4842-5875-0_5

User Provisioning for Microsoft Teams

Before using Microsoft Teams and its features, each user must provision for Teams; without provisioning, users cannot avail themselves of Teams features. Teams user provisioning involves enabling Teams licenses as well as add-on licenses, including Phone System and Office 365 Audio Conferencing, and granting the required policies.

Enabling a User Teams License

To enable a Teams license for a user, as well as add-on licenses, follow this procedure.

1. Log in to Office 365 admin center and navigate to Users. Select Active Users and find the user to whom you need to assign a license. You can then enable all necessary licenses. Figure 5-1 shows user Balu Ilag with all required licenses needed to use Teams as a unified communication and collaboration tool.

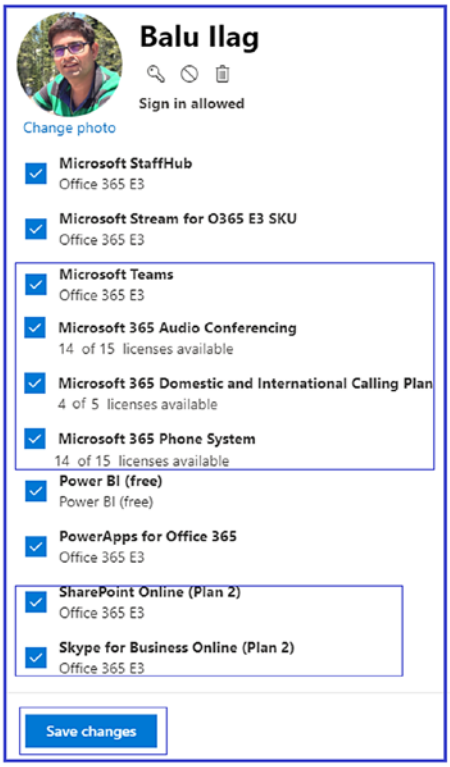

Figure 5-1. *Enabling licenses for a user*

As a Teams admin, you can manage user accounts in Office 365 admin center for modifying users' display attributes and passwords (depending on the organization topology). You can use the Teams admin center to assign and manage any Teams-specific policies such as meeting policy, live event policy, Teams policy, and so on. You can refer to Chapter 1 for an overview of licensing.

Assigning Meeting Policy to a User Account Using Teams Admin Center

You can assign or remove any policy from a user account using Teams admin center. This includes meeting policies, message policies, live event policies, emergency calling policies, and so on. Follow the steps to assign a Teams meeting policy. After you create a meeting policy, the next step is to assign the policy to a user. You can assign a meeting policy within the Teams Admin center in both the Users and Meeting Policy sections. Follow this procedure to assign a meeting policy in the Users section.

1. Log in to Teams admin center, and navigate to Users. Select the users to whom you want to apply the policy and then click Edit Settings.
2. In the Edit User Policies window, shown in Figure 5-2, select the required meeting policy, and then click Apply.

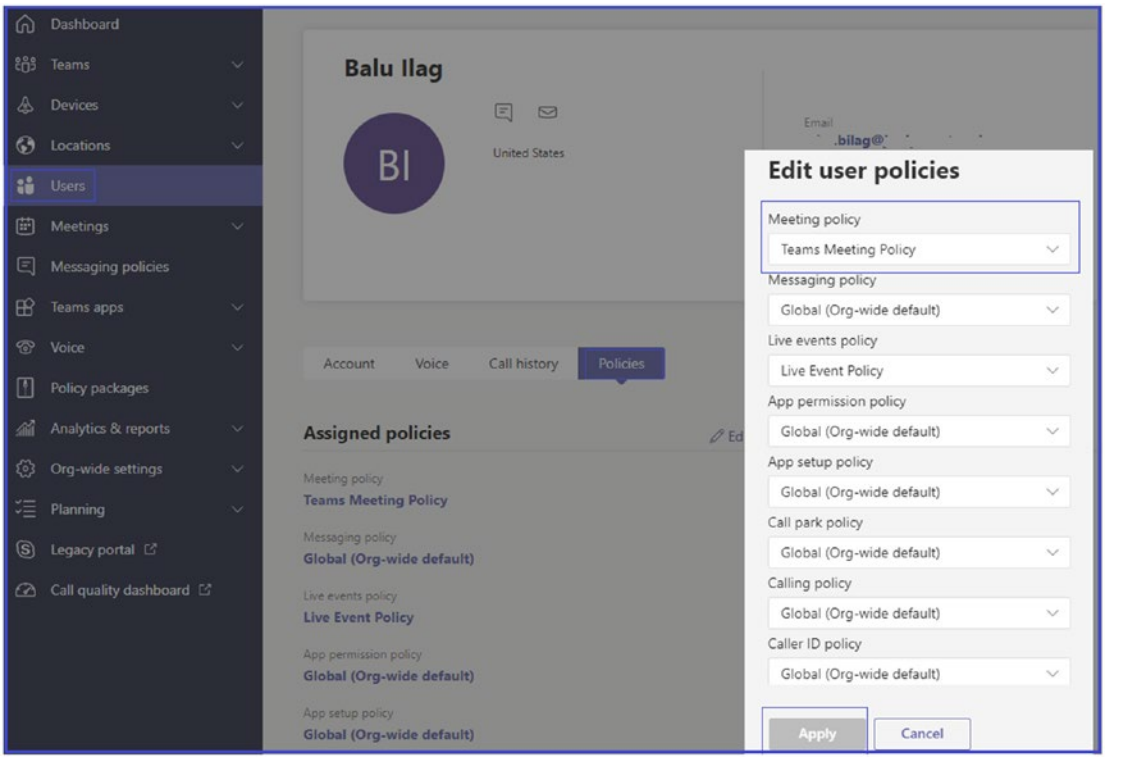

Figure 5-2. *Assigning a meeting policy*

You can also assign a meeting policy in the Meeting Policies section. To do so, log in to Teams admin center and then navigate to Meetings. Select the required meeting policy and then click Manage Users. In the Manage Users windows, select the user to whom to assign the policy, as shown in Figure 5-3. Click Apply.

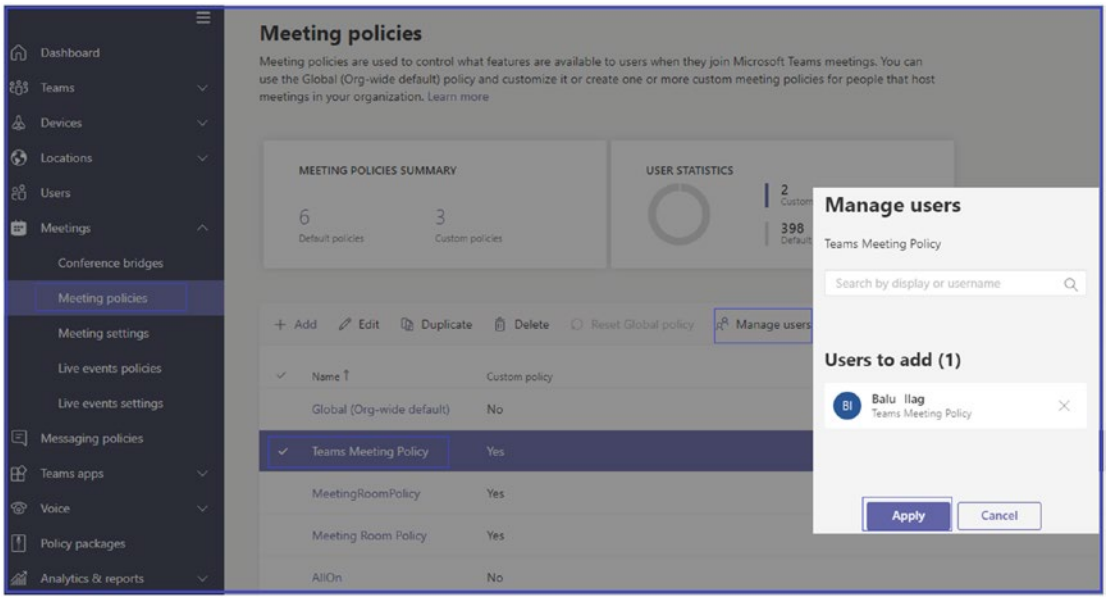

Figure 5-3. *Assigning a policy using the Meeting Policies section*

Third-Party Application and Policy Management

As a Teams admin, you must be aware of the apps that Teams has. Microsoft Teams apps offer multiple features that allow your organization to maximize its Teams experience. These apps include the functionality of tabs, messaging extensions, connectors, and bots provided by Microsoft, built by a third party, or created by developers in your organization. You can manage the apps using the Teams apps section in the Teams admin center, where you can set policies to manage apps for your organization. For example, you can set policies to control what apps are available to Teams users, and you can customize Teams by including the apps that are most important for your users. Figure 5-4 shows the available options to manage apps, manage permission policies, and set up new custom policies.

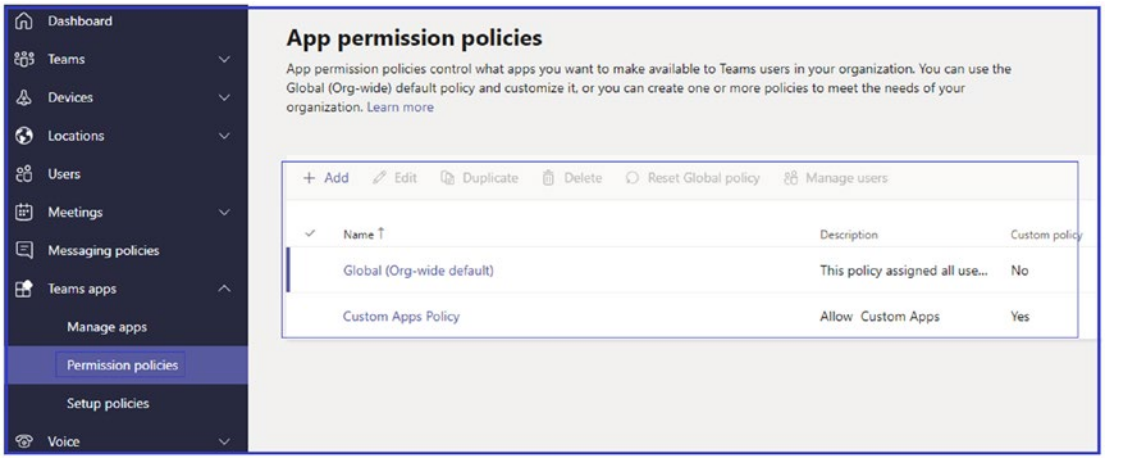

Figure 5-4. *Teams apps and policies*

Teams Apps Permission Policies

Using app permission policies, you can block or allow apps either organization-wide or for specific users. When you block an app, all collaborations with that app are disabled, and the app will no longer appear in Teams. For example, you can use app permission policies to disable an app that creates a permission or data loss risk to your organization.

Managing the Custom App Setup Policies

Admins can use the Teams admin center to manage or edit a policy, including the Global (Org-wide default) policy and custom policies that admins have created. Follow this procedure to manage policies.

1. Log in to Teams admin center, and navigate to Teams Apps. Select Setup Policies and then select the policy you want to work with. Click Edit to manage the policy settings.
2. On the edit page, make the changes that you want. You can add, remove, and change the order of apps, and then click Save.

Assigning a Custom App Setup Policy to Users

You can use the Teams admin center to assign a custom app setup policy to individual users, or you can use the Skype for Business Online PowerShell module to assign a custom policy to groups of users, such as a distribution group or security group. There are multiple ways to assign an app setup policy to your users in the Teams admin center. You can assign users either in Setup Policies or in Users in Teams admin center.

To assign policies to users using the Teams admin center, follow these steps.

1. Log in to Teams admin center and navigate to Teams apps. Select Setup Policies.
2. Select the custom policy and then click Manage Users.
3. On the Manage Users page, search for the user by display name or by username, select the name, and then click Add. Repeat this step for each user who you want to add.
4. Once you are finished adding users, click *Apply*.

Creation and management of custom policies for apps was covered in Chapter 2.

Teams Governance and Life Cycle Management

So far you have learned how Microsoft Teams can change workplace collaboration, providing a centralized workplace for users to come together to chat, meet, call, create, and make decisions. Teams provides a single place where users can connect and organize teams or projects without disturbing other workflows. Teams also provides a single platform where users can access all business-critical information and applications, and automate their repeatable processes efficiently.

Organizations can bring their applications (custom apps), tools, and services into Teams, and Teams supports all of this work. As an admin, you can also connect everyone in your organization through the single platform of Teams, bringing together such diverse functions as technology organization, manufacturing flow, a classroom, and hospitals. Everyone can come together and leverage the power of Teams.

Teams and information security admins in your organization must be aware of what Teams provides to securely maintain the data that Microsoft Teams generates. When the data are generated, your concern as an administrator is who is accessing the data

and how it can be secured and accessed by only the users who need the data. Microsoft itself is investing a great deal in securing Teams data, and Teams benefits from the all security, compliance, and identity investments that Microsoft has already made in the information protection and compliance area.

To understand the Teams security and compliance capabilities it is important to separate queues such as identity and access management, information protection, the ability to discover content and able to respond to it, application of data governance policies, what type of content exists and how long it is retained, and finally the ability to manage the risks. This topic will provide you the information that you need to manage Teams governance and overall life cycle.

Microsoft Teams Identity and Access Management

Teams identity was already covered in Chapter 2, but a recap is in order. Identity management is crucial for any application or system. If bad actors compromise an identity, your data and content could be misused. Because Teams leverages Azure AD for identity, the investments and improvements in Azure are directly applied to Microsoft Teams.

Microsoft Teams has strong authentications because it uses smart protection policies and risk assessment to block threats. As a Teams admin or security admin, you need to ensure that your organization's users have strong passwords and have MFA enabled. Once you have enabled MFA for SharePoint Online and Exchange Online, you are automatically supported for Teams because Teams uses SharePoint and Exchange extensively. When a user tries to log in to Teams, he or she will be challenged for the two-factor workflow or whether you have a PIN enabled and both have the same workflow [95].

Another aspect of identity is what authorized users have access to. This is specifically based on a policy that is defined in conditional access in Azure AD, and Microsoft Teams is part of this feature as well. Figure 5-5 shows conditional access based on the signal that comes from the devices, applications, and users. Microsoft determines the risk score, and as a Teams admin you configure the policies that determine who can access the Teams application based on the conditions applied.

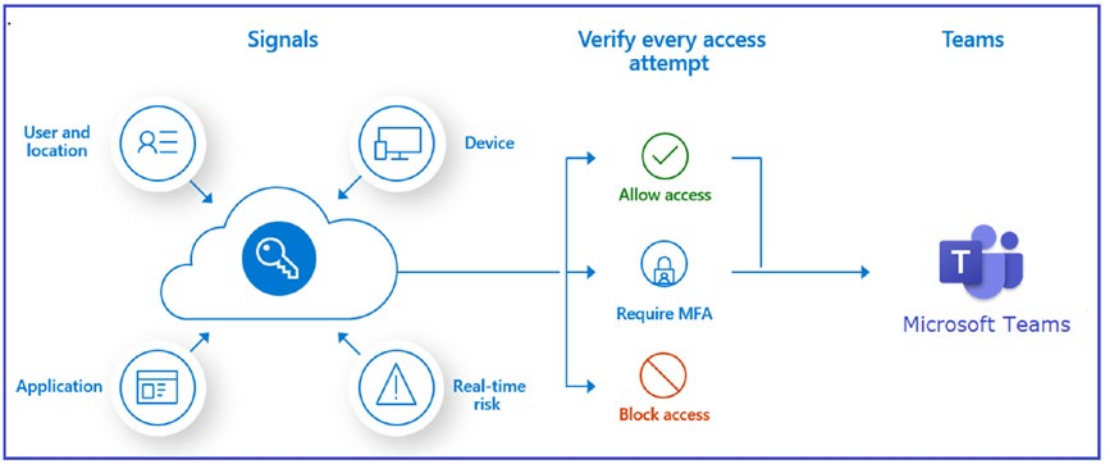

Figure 5-5. *Conditional access workflow [22a]*

Remember, the conditional access policies prevent access for authenticated users from unmanaged devices.

Configuring Conditional Access Policy for Microsoft Teams

Azure AD conditional access is a vast topic and includes many facets. For purposes of this book, I have designed an example conditional access policy. If you are interested in learning more about Azure AD and conditional access, refer to the Microsoft documentation at `https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview`.

Follow this procedure to implement a conditional access policy for Teams.

1. Log in to the Azure AD portal at `https://portal.azure.com`. You must have appropriate permission (e.g., Global admin role permission) to design conditional access.
2. On the Microsoft Azure home page, navigate to Conditional Access - Policies and open the link.
3. Click + New to create new conditional access policy. Enter a meaningful name so that the policy can be easily identified. For our test policy, the given name is CA for MS Teams.
4. Under Assignments, select the users and groups to which this policy will apply and then click Done. In the example in Figure 5-6, the user account selected is for Balu Ilag, `bilag@bloguc.com`.

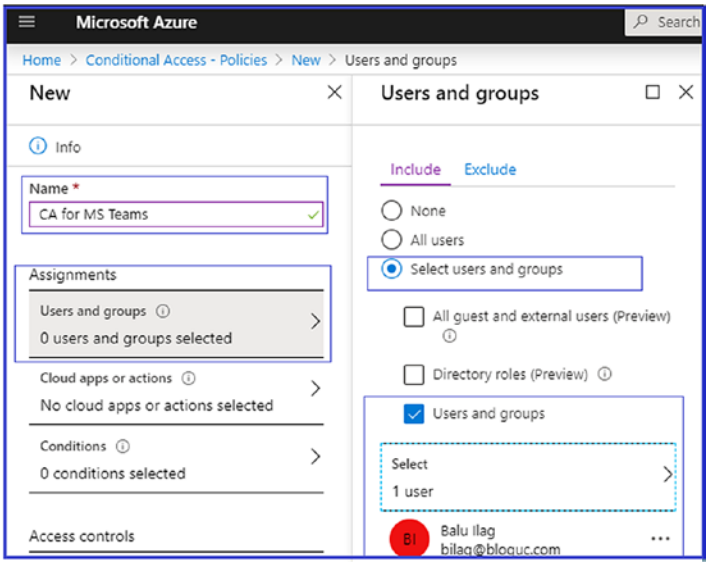

Figure 5-6. *Conditional access policy assignment*

5. In the Cloud Apps Or Actions pane, select Microsoft Teams as a first-party application. Select Microsoft Teams, as shown in Figure 5-7, and then click Done.

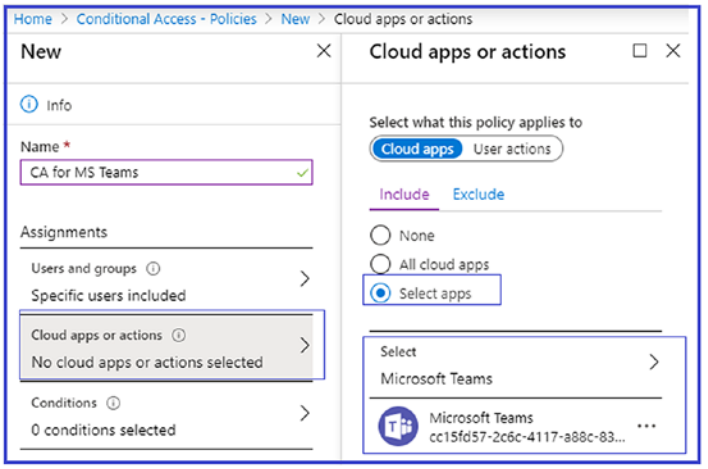

Figure 5-7. *Cloud app as Teams*

6. Select Conditions. In the Conditions pane, you will see different available options.

   a. *Sign-in Risk:* This will allow you to select the sign-in risk level: High, Medium, Low, or No Risk. To enable this, set the toggle on Yes and then select the applicable sign-in risk. For the example shown in Figure 5-8, medium risk is selected. You can set risk as per your organization requirements.

   b. *Device Platforms:* Select the platform, such as Any Device, or choose a specific platform—Android, iOS, Windows Phone, Windows, and macOS—to which to apply this policy. To enable this, first set the toggle to Yes and then select the platform. For the example test policy shown in Figure 5-8, Android, iOS, Windows Phone, Windows, and macOS device platforms are selected.

   c. *Locations:* Select the location to control users' access based on their physical locations. To enable this, set the toggle to Yes and then select the location. For the example test policy in Figure 5-8, All Trusted Locations is selected. Click Done. You can select the location as per your organization requirement.

   d. *Client Apps (Preview):* Select the client app to which this policy is applied and then click Done. For this example, no client app is selected.

   e. *Device State (Preview):* Select the device state and then choose to enable this for all devices or exclude any devices and then click Done. For this example, test policy All Device State is selected.

   f. Click Done to add the selected conditions, shown in Figure 5-8.

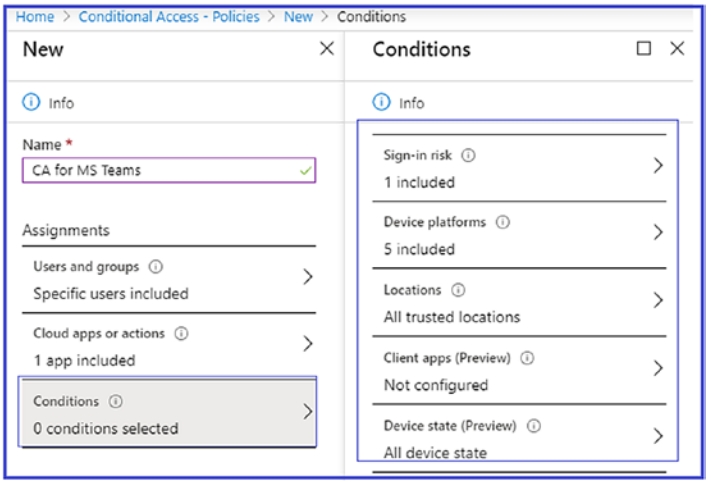

Figure 5-8. *Conditions settings*

7. *Access Controls:* Select the controls to be enforced, like Block or Grant. If Grant is chosen, then select Require Multi-Factor Authentication, Require Device To Be Marked As Compliant, Require Hybrid Azure AD Joined Device, and so on.

8. *Session:* The session controls enable limited experiences within a cloud app. Select the session usage requirements. For the example shown in Figure 5-9, Sign-In Frequency - 5 days is selected.

9. Click Create, as shown in Figure 5-9, to build this conditional access policy.

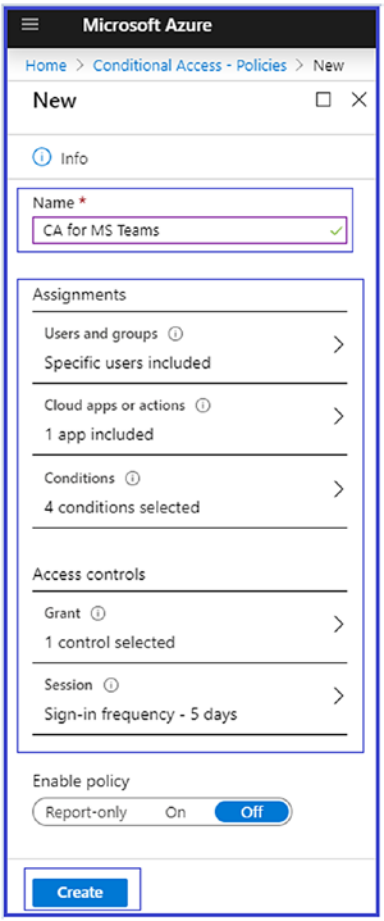

Figure 5-9. *Creating a conditional access policy*

User Experience When User Accesses the Teams Application

Figure 5-10 shows a warning message preventing users from accessing the Teams application from an unmanaged device. This is an example of the granular control that conditional access policy provides, preventing authorized users from accessing the Teams application from an unmanaged device. In this workflow, the first part is authorizing the user and the second part is applying conditions based on the policy to prevent a user from accessing the Teams app from an unmanaged device. Another valuable condition available through a conditional access policy is the prevention of Teams app access from nonwork locations.

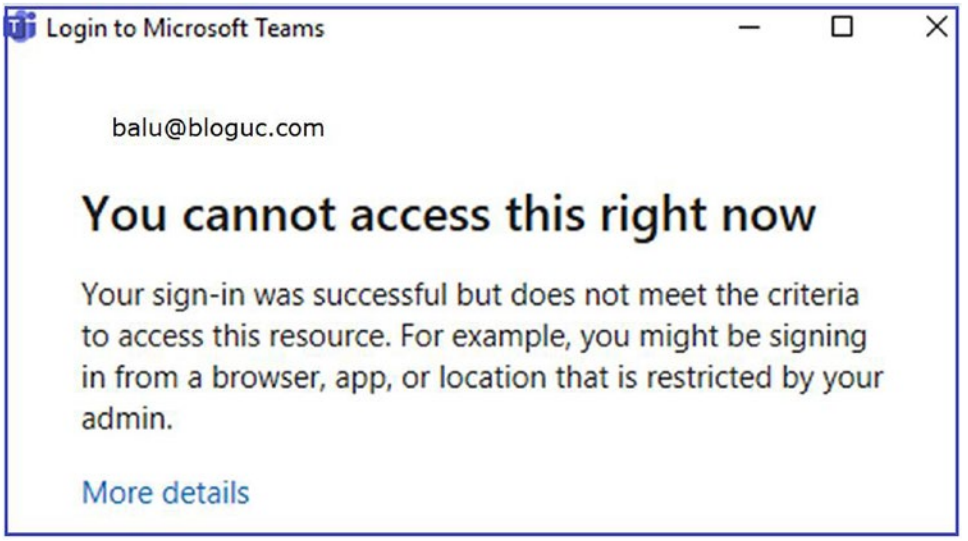

Figure 5-10. *Teams app access blocked from an unmanaged device*

Managing Information Protection Using Data Loss Prevention

In any application, an identity considered a front door. Once you secure the front door then you will be dealing with how to control the flow of information, and Teams is no exception. Microsoft Teams achieves information protection through the Office 365 data loss prevention (DLP) stack. DLP enables Teams and security admins to create policies to determine what is considered sensitive or nonsensitive information. Microsoft made this easier for admins by providing more than 80 predefined rules. An admin can leverage these existing predefined rules or create new custom rules or policy that an organization wants. You can monitor content, detect policy violations, and remediate violations as per the requirement.

Once you create policies, Teams monitors the content, and whenever a policy violation is detected, the end user gets notified, or you can set the policy to prevent access as well.

DLP Policies in Action

You can create DLP policies for different kind of workloads and enable them for Exchange, SharePoint, or Teams. There is only one portal to create DLP policies for all Office 365 applications, which means you don't have to switch among different portals for different applications.

As an example, two users from Bloguc Organizations are trying to share content. The sender is trying to send some content, but Bloguc Organization has already implemented a DLP policy that blocks the content because it includes sensitive information. The notification message to the sender, shown in Figure 5-11, says, "This message was blocked," and also indicates why the content was blocked [99].

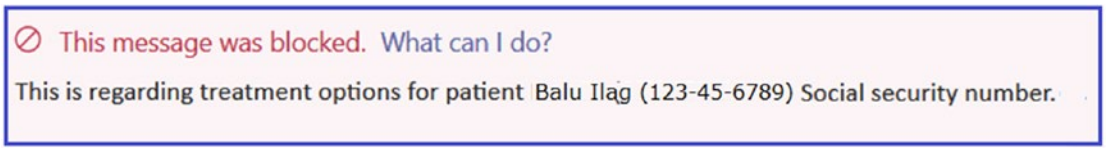

Figure 5-11. *DLP policy blocked notification*

The sender is also given the option to override the policy conditions and send the message or report it to a security admin. Figure 5-12 shows the override options.

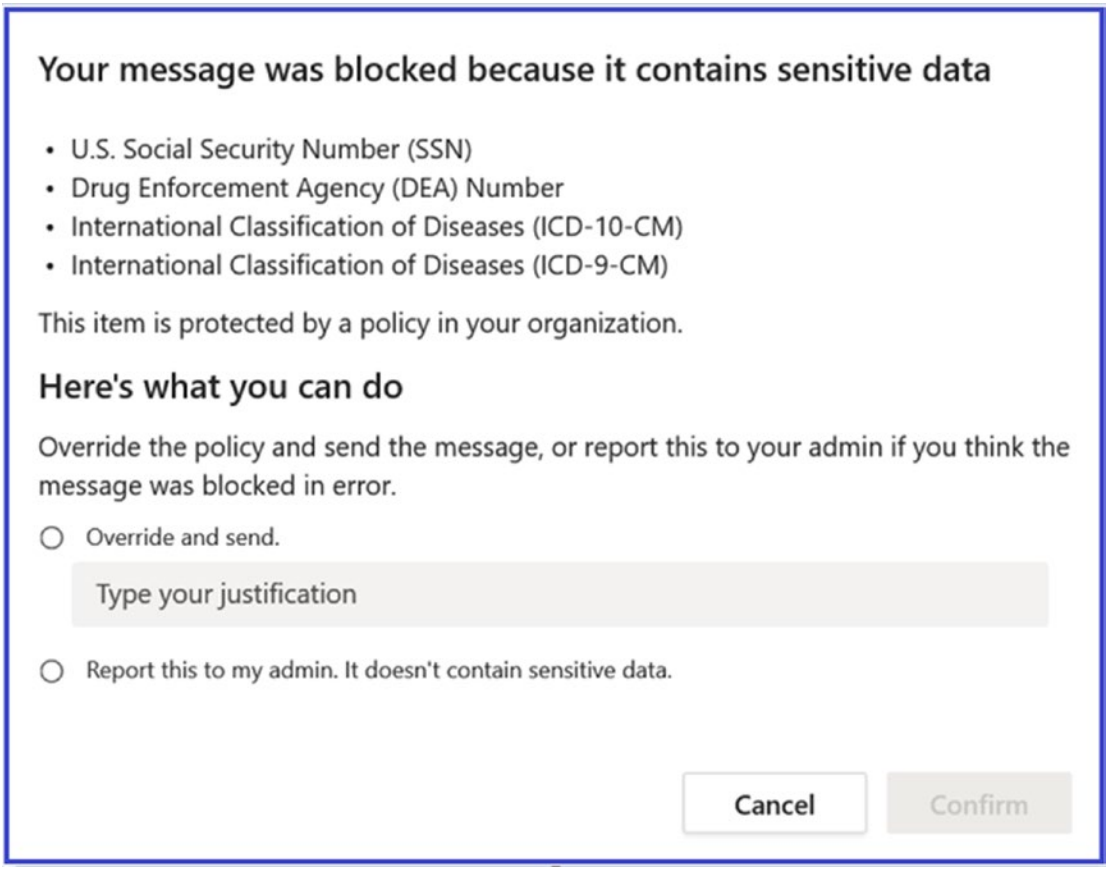

Figure 5-12. *DLP policy override options [22a]*

The receiver will just get the message saying "This message was blocked due to sensitive content," as displayed in Figure 5-13.

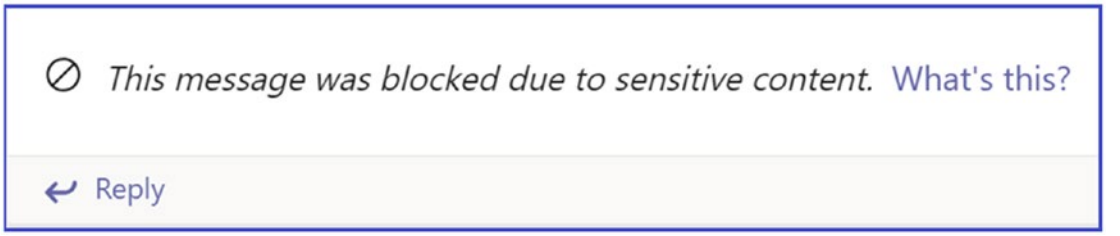

Figure 5-13. *Message blocked due to sensitive content*

This is considered a passive DLP solution, not active. You might wonder why it is considered passive. The reason is that when someone sends sensitive content, the receiver will see the content for a few seconds before it is removed from view. If you want to learn more, refer to the Microsoft documentation about DLP policies at `https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies`, which helps explain why the message was blocked.

DLP policies are very useful and provide a solution for preventing the accidental sharing of critical information about confidential projects, both internally and externally.

As of this writing, to leverage DLP policies, both the sender and receiver should be moved to TeamsOnly mode. If the sender is in Island mode and the receiver is in TeamsOnly mode, then the DLP policy will not work the way it should. In addition, the time taken to block the content and generate the warning message is quite lengthy. Microsoft is working to reduce this delay.

Creating a DLP Policy for Microsoft Teams

Teams or security admins can create new or DLP policies or modify existing ones; however, you must have permission to execute the modification steps outlined here. Remember, by default, an organization's tenant admin will have access to Security & Compliance Center, and they can give Teams or security admins and other people access to the Security & Compliance Center, without giving them all of the permissions of the tenant admin. To create a DLP policy follow this procedure.

1. Log in to Office 365 Security & Compliance Center by browsing to the site at `https://protection.office.com`. Select Data Loss Prevention and then select Policy. Click + Create A Policy. Figure 5-14 shows the Create A Policy option [23a].

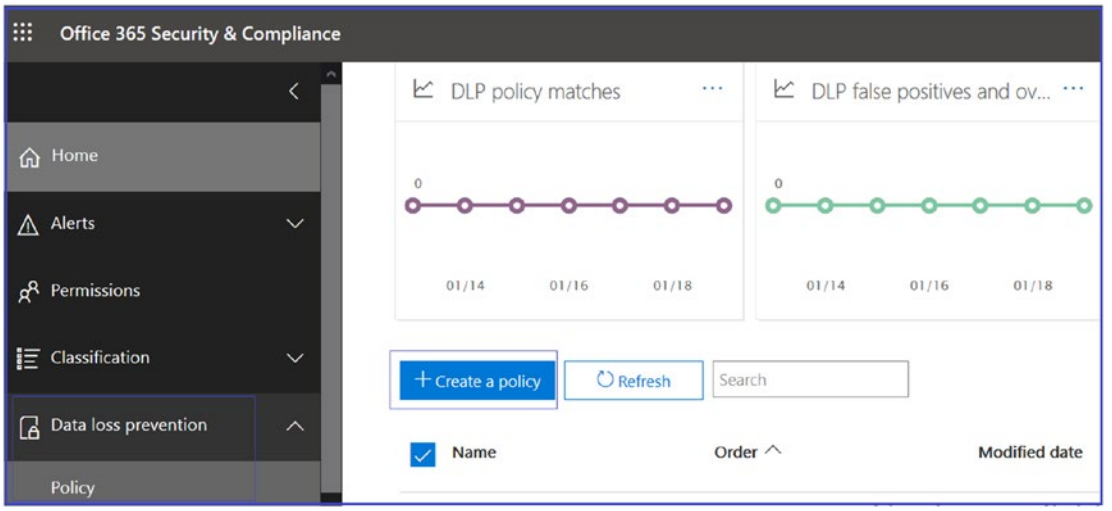

Figure 5-14. *DLP policy creation options*

2. Select a template, and then click Next. In the example shown in Figure 5-15, the U.S. Personally Identifiable Information (PII) Data template is selected.

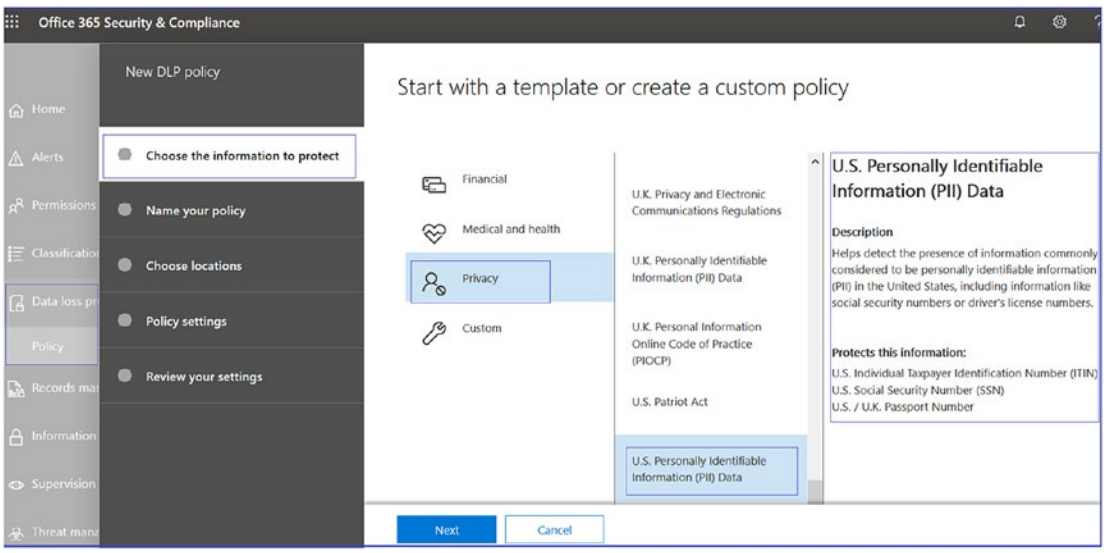

Figure 5-15. *Choosing an available DLP template*

3. On the next page, enter a name and description for the policy, and then click Next. Figure 5-16 shows the name given is U.S. Personally Identifiable Information (PII) Data- Bloguc Org, and the description identifies this policy correctly.

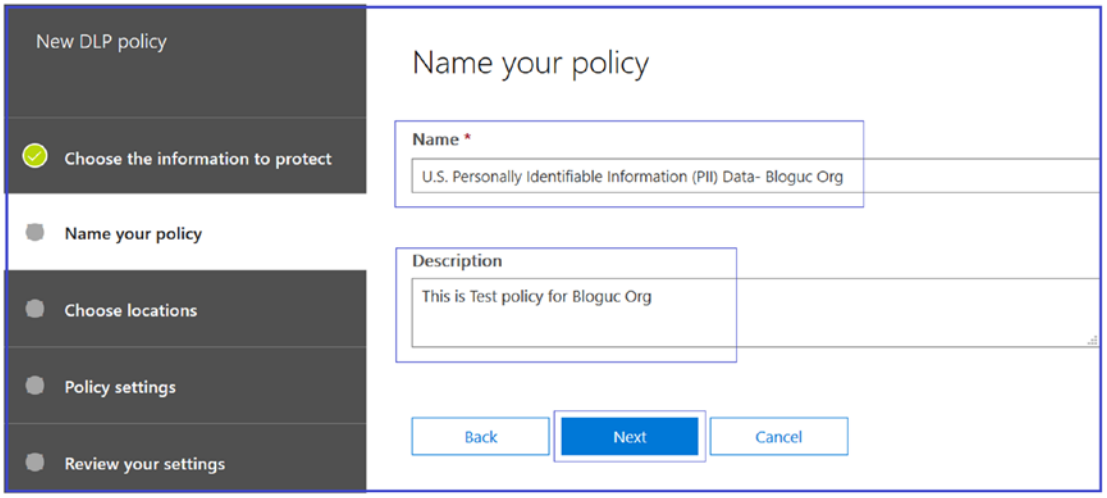

Figure 5-16. *DLP policy name and description*

4. On the next page, the Choose Locations tab, keep the default setting that includes all locations, or select Let Me Choose Specific Locations, and then click Next. For the example shown in Figure 5-17, the default selection that includes Exchange email, Teams chats, channel messages, and OneDrive and SharePoint documents is selected. If you have selected specific locations, select them for your DLP policy, and then click Next.

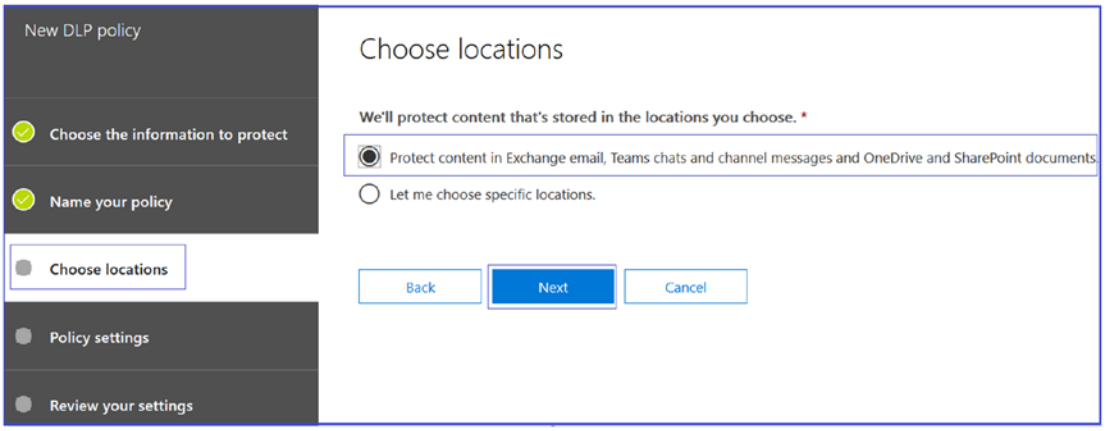

Figure 5-17. *DLP policy locations*

Note If you want to make sure documents that contain sensitive information are not shared inappropriately, make sure SharePoint sites and OneDrive accounts are turned on, along with Teams chat and channel messages. Channels in Microsoft Teams are strongly dependent on Exchange Online functionality. Make sure that the Exchange email location is also enabled for the policies that should be applied for the content of the channels [23a].

---

5. On the next page, the Policy Settings tab, under Customize The Type Of Content You Want Io Protect, keep the simple default settings, or choose Use Advanced Settings, and then click Next. If you choose to use advanced settings, you can create or edit rules for your policy. For this example, shown in Figure 5-18, the default setting is retained to keep the policy simple.

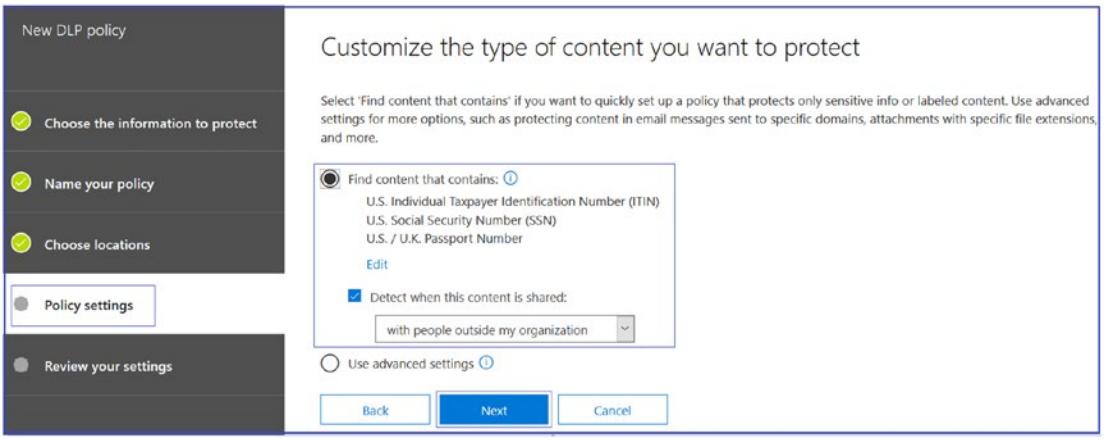

Figure 5-18. *DLP policy settings*

6. On the next page of the Policy Settings tab, under What Do You Want To Do If We Detect Sensitive Info?, review the settings. (Here's where you can select to keep default policy tips and email notifications or customize them.) When you are done reviewing and editing the settings, click Next. For this example, all the default settings are retained, as shown in Figure 5-19.

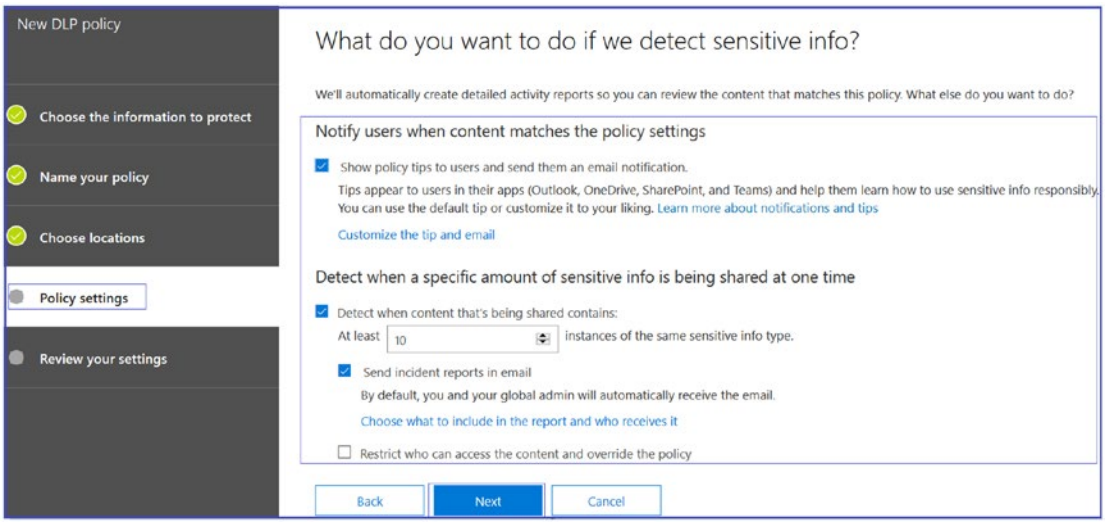

Figure 5-19. *Policy settings for sensitive information*

7. On the next page of the Policy Settings tab, under Do You Want To Turn On The Policy Or Test Things Out First?, select whether to turn the policy on, test it first, or keep it turned off for now, and then click Next. Testing the policy first before turning it on, as selected in Figure 5-20, is recommended.

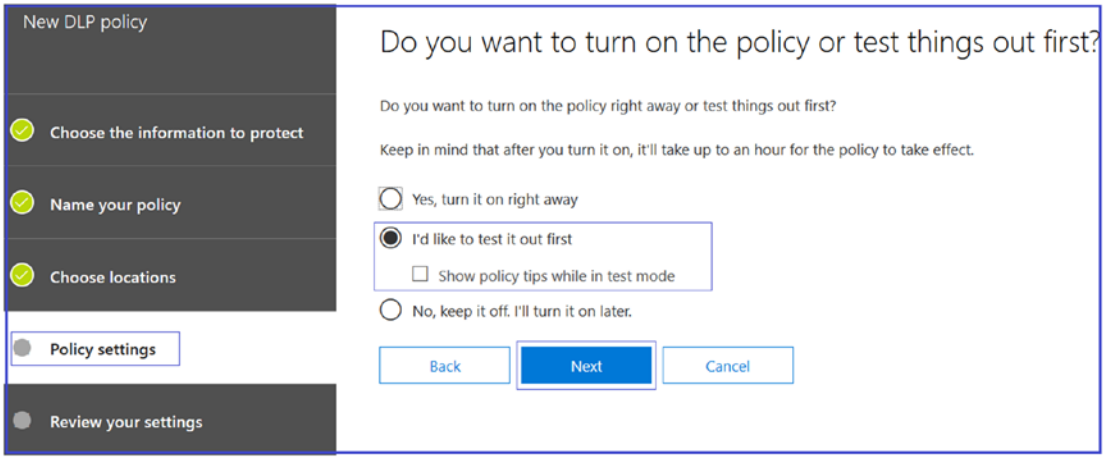

Figure 5-20. *Policy setting for testing*

8. On the Review Your Settings tab, shown in Figure 5-21, review the settings for the new policy that you created. Select Edit to make changes if required. When you are finished making changes, click Create.

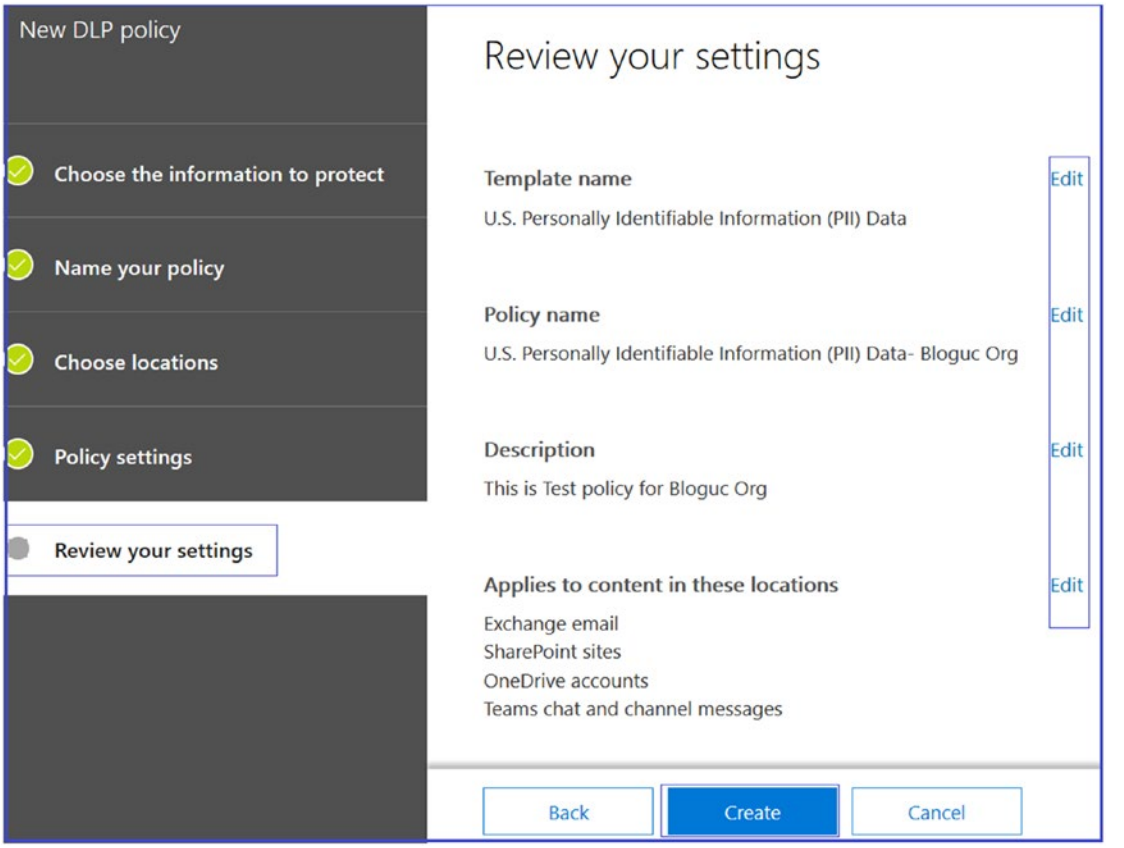

Figure 5-21. *Reviewing settings*

DLP policy could take some time to populate, so sometimes it takes up to an hour for your new policy to work. You can make changes in the policy that you created to customize the policy per your organization's requirements.

Creating and Managing eDiscovery for Teams

From a manageability and content discovery perspective, Microsoft has provided some tools that Teams admins can use to retrieve information like who is creating content, monitoring, or reporting. Using Teams, you can discover the content through eDiscovery and put some users on a legal hold so that they cannot tamper with content that was created in Teams. For example, if User A is under litigation and he shared the information with an external user, then you as an admin have the workflow that will help to export the content and hand it out.

Create eDiscovery Workflows for Teams

You can access eDiscovery through the Office 365 Security & Compliance Center. The advanced eDiscovery workflow is available in Office 365 and Teams is one of the primary applications that can be used. In eDiscovery, you can search content that was created in Teams and content that was exchanged in conversation, including one-to-one chat, group chat, and channel chat. All these contents are discoverable to you as a Teams admin and security admins.

To use the eDiscovery search, first log in to `https://protection.office.com/` and then navigate to eDiscovery. Select eDiscovery or Advanced eDiscovery, as shown in Figure 5-22. Click + Create A Case to create a case for eDiscovery.

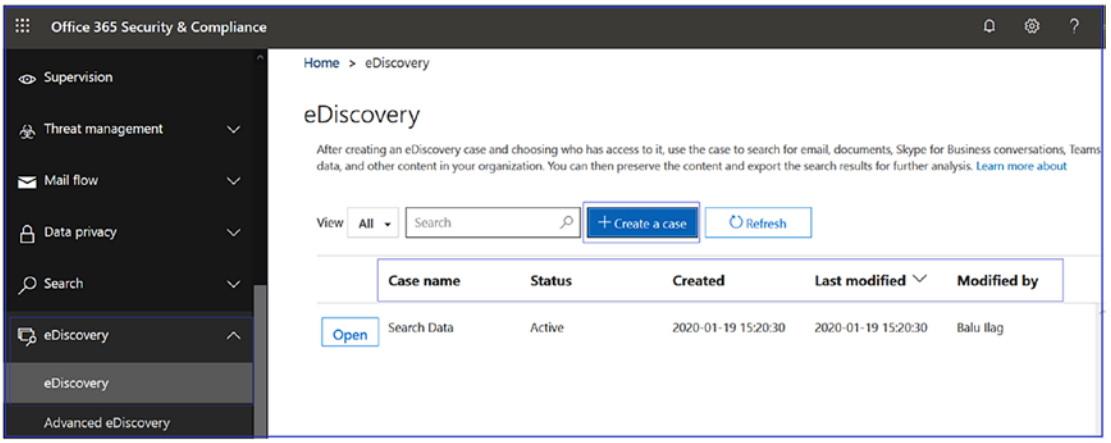

Figure 5-22. *eDiscovery search*

Microsoft has updated the eDiscovery search capability to show the threaded conversation view when a security admin searches in eDiscovery.

There is another feature, redaction, that Microsoft added in eDiscovery search, displayed in Figure 5-23. How does it work? Here is an example: You search some content that is required, and the requested content is one conversation. However, the search results show three threads of conversation. A security admin can activate redaction for the two conversation threads that are not required, so that only the required details are shared. You can manage the existing search cases that you have previously created under eDiscovery.

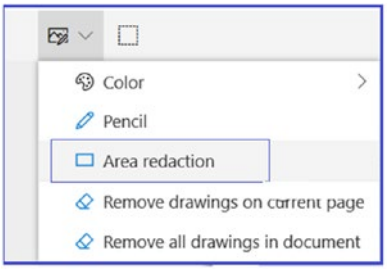

Figure 5-23. *Redaction feature [22a]*

Data Governance and Retention in Teams

Microsoft Teams is part of the Office 365 service that keeps everything secure. Additionally, it allows creation of retention policies.

Retention Policies for Teams

In Microsoft Teams, retention policies are very useful for retaining Teams or chat data, as well as defining deletion policies. For most organizations, the volume and complexity of data increases daily, including email to documents to instant messages, and many more. Efficiently managing or governing these data is very important because as a Teams admin, you should comply proactively with industry regulations and internal policies that require you to retain content for a minimum period of time. For example, the Sarbanes-Oxley (SOX) Act might require you to retain certain types of content for seven years. Teams is already certified by more than 42 regional or national and industry-specific regulations [22a].

This can also help reduce your risk in the event of litigation or a security breach by permanently deleting old content that you are no longer required to keep. Teams also helps your organization share knowledge effectively and be more responsive by ensuring that your users work only with content that is current and relevant to them.

Specific to the retention policy, it helps organizations either retain data for compliance (namely, preservation policy) for a specific period or remove data (namely, deletion policy) if it is considered a liability after a specific period. Retention policies are available in the Security & Compliance Center, and they work across the different workloads and data types, such as Exchange email, SharePoint document libraries, and OneDrive for Business files.

As you know, Teams chat conversations are persistent and retained by default in Exchange Online. With the addition of retention policies, administrators can configure retention policies (both preservation and deletion) in the Security & Compliance Center for Teams chat and channel messages.

Creating and Managing Retention Policies

Managing Retention Policies

You can manage retention policies using Office 365 Security & Compliance center, or you can use PowerShell. To manage Teams retention policies, log in to the Office 365 Security & Compliance Center and navigate to Information Governance. Select Retention, as shown in Figure 5-24.

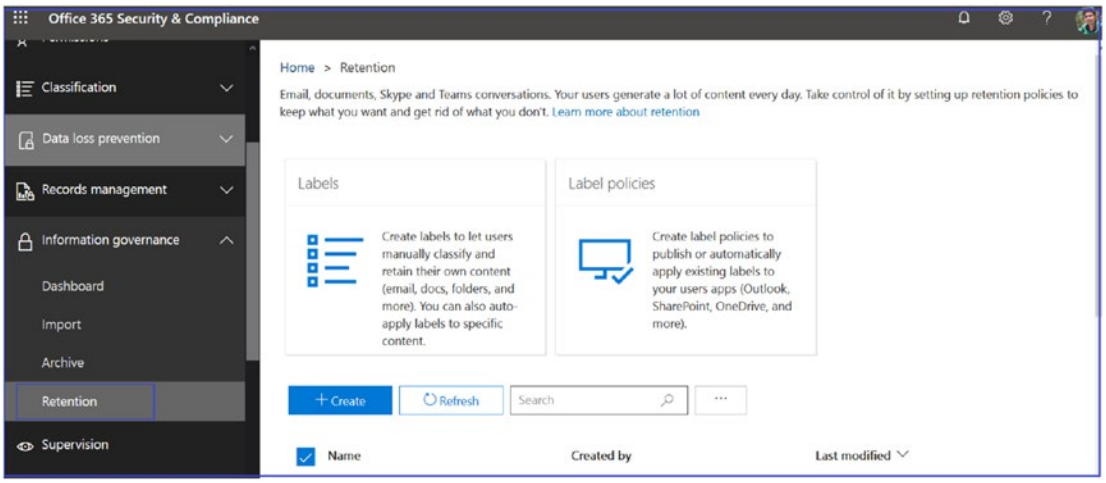

Figure 5-24. *Retention policy*

Microsoft Teams retention policies support different tasks, such as preservation, that allow and organization to keep Teams data for a specified duration and then do nothing. Another policy preserves and then deletes the Teams data. This kind of policy allows an organization to keep Teams data for a specified duration and then it will be deleted. In addition, there is another policy that allows deletion of Teams data after a specified duration.

So far, advanced retention policy doesn't support Teams chat and Teams channel message locations, but Microsoft might support advanced retention policy for Teams chat and channel messages in the future.

Creating Teams Retention Policy

As a Teams admin, you must know how to create retention policies for Teams private chats (one-to-one chat and group chat) and Teams channel messages. In many instances, organizations consider private chat data as more of a liability than channel messages, which are usually more project-related conversations. To create a retention policy, follow this procedure.

1. log in to Office 365 Security & Compliance Center (`https://protection.office.com/homepage`) and navigate to Information Governance. Select Retention and then click Create Policy. Figure 5-25 shows settings for retention policy creation.

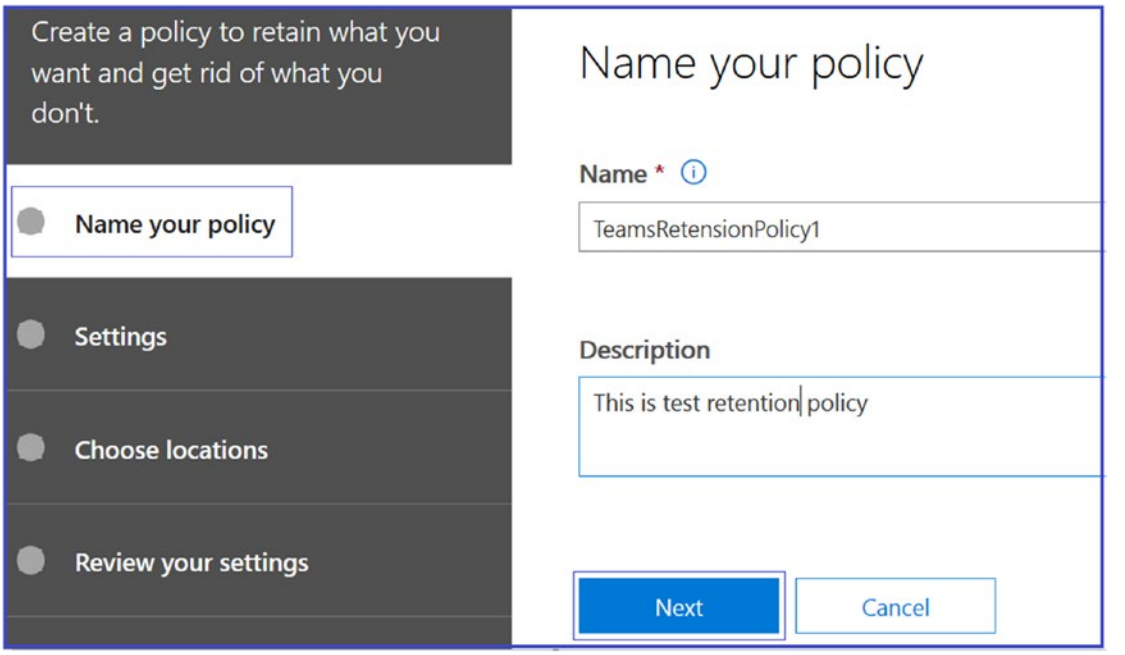

Figure 5-25. *Creating a retention policy*

2. Enter a meaningful name and description for the retention policy. Click Next.
3. On the Settings tab, define retention policies for these locations. Set how long you want to retain the content. For example, Figure 5-26 shows that the content will be retained for 7 years.

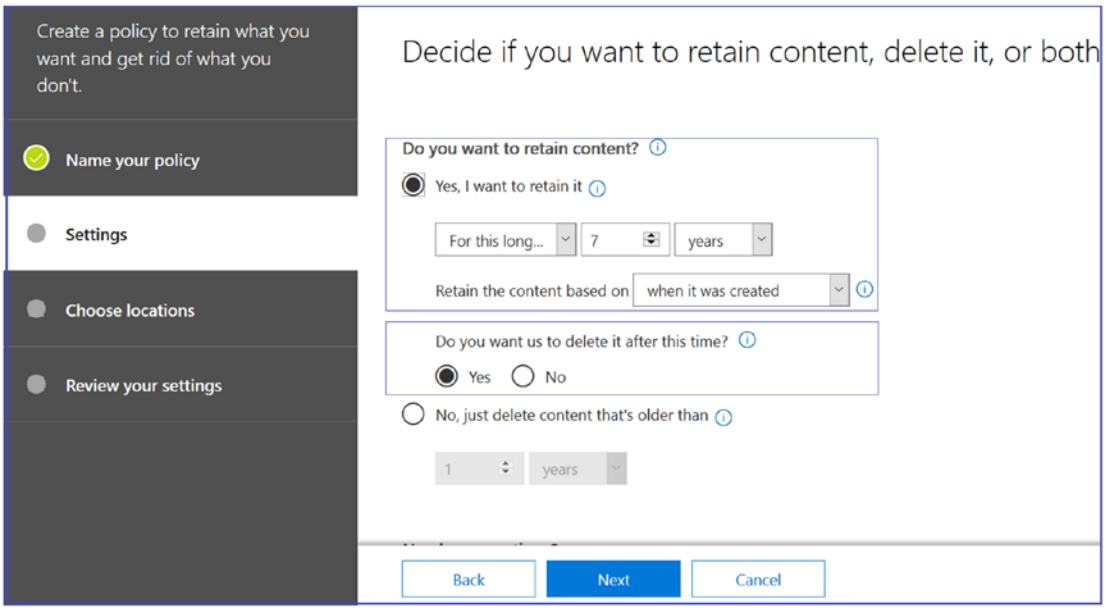

Figure 5-26. *Retention policy settings and duration*

4. Decide whether you want to delete the content after 7 years. Click Next.

5. On the Choose Locations tab, select the appropriate applications for retention, as shown in Figure 5-27.

6. Next, choose the locations for Teams and to which teams these settings will apply.

   - Turn on the Teams Channel Messages setting and choose for all teams or choose specific the teams.

   - Turn on Teams Chats and choose for all the users and or exclude users.

7. When you turn on Teams channel messages, you can specify teams to which this policy will apply. For example, for teams X, Y, and Z, the admin can set the deletion policies for 1 year (by selecting those teams individually) and apply a 3-year deletion policy to the rest of the teams. Click Next to review the settings.

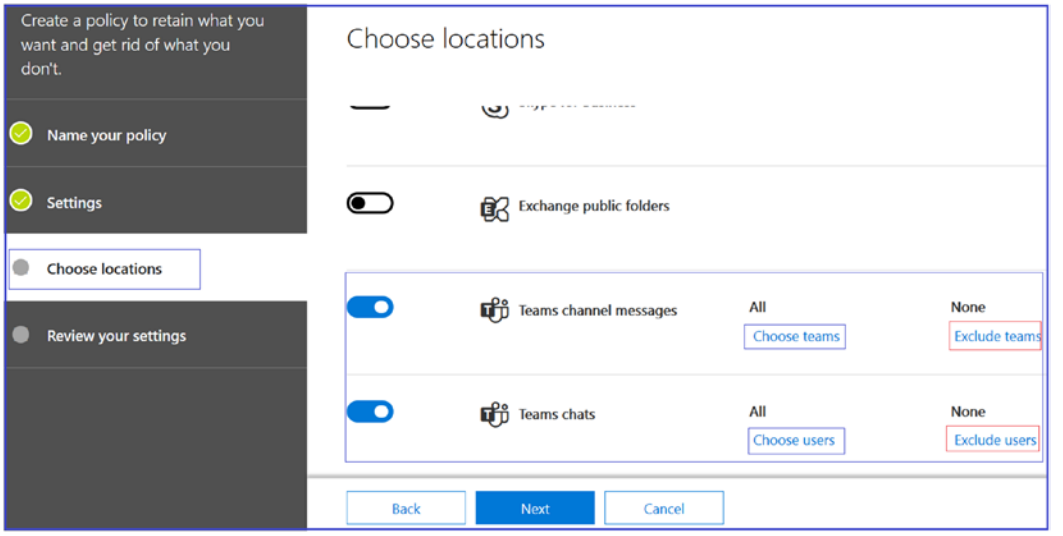

Figure 5-27. *Choose location for retention*

8. On the next tab, review all the settings and click Create This Policy, as shown in Figure 5-28.

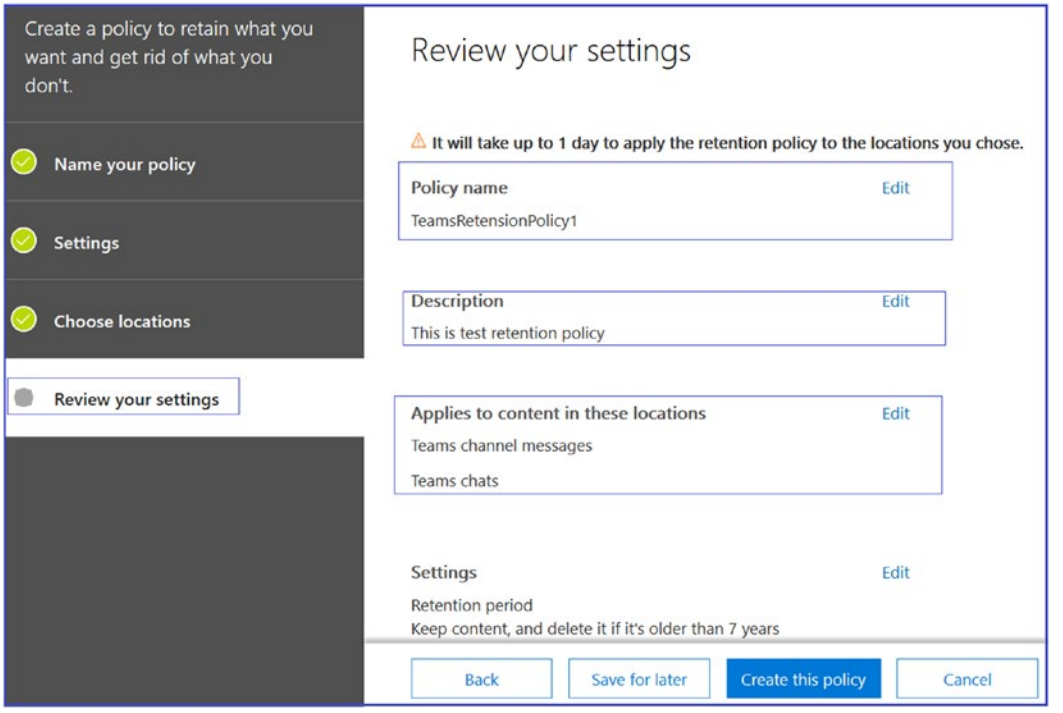

Figure 5-28. *Reviewing the Retention policy*

After policy creation you can see the policy created and its last modified date, as illustrated in Figure 5-29. In this example, Teams chats and Teams channel messages will be maintained for 7 years.

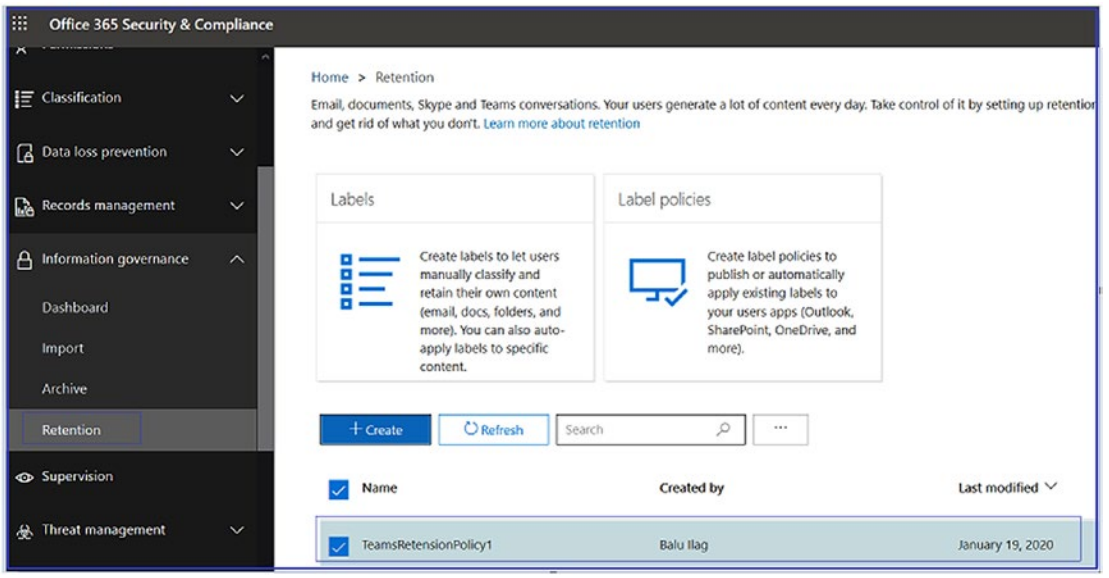

Figure 5-29. *Retention policy created*

Retention policies allow you to preserve your data for a specific amount of time and then delete the data after that period. Microsoft Teams supports retention policies as short as one day. Retention policies can be configured to retain data for a specific amount of time so that even if the user deletes the data, admins still have access to it. Another policy is to delete data, so if a user wants to delete data after specific period of time, then you will be able to do this.

You as a Teams admin can create a retention policy based on when the information is created, or you can create policies based on when information was last modified. Microsoft provides the flexibility to create retention policies based on the organization's requirements [99].

Managing Internal Risk Through Information Barrier in Teams

Managing internal risk is another important consideration. DLP prevents the compromise of sensitive information, but organizations are subject to different kinds of risk, such as IP theft, or content leaks, insider trading, and conflicts of interest. Figure 5-30 shows several types of risk that organizations are subject to.

Figure 5-30. *Risks that organizations face [22a]*

One of the major tools that Teams uses to mitigate risk is the information barrier (IB). An IB is often called an ethical wall, a barrier in your organization created between different departments or internal units. For example, if you have groups of users that are not supposed to interact with other groups of users, you as a Teams or security admin can create segments and prevent these segments from talking to each other.

This setup is typically used in regulated industry, education, and financial sectors. Basically, IBs build logical boundaries to prevent communication between Group A and Group B. For example, investment bankers cannot find or communicate with financial advisors, but both groups can communicate with human resources (HR). The investment bankers cannot communicate with financial advisors because of potential influence issues. The Microsoft Teams solution is creation of IB segments, which ensure that you as an admin can put investment bankers in one segment and financial advisors in another segment. IB policies will prevent communication between the segments. Both segments, however, can communicate with the HR team without any barriers. This process is illustrated in Figure 5-31.

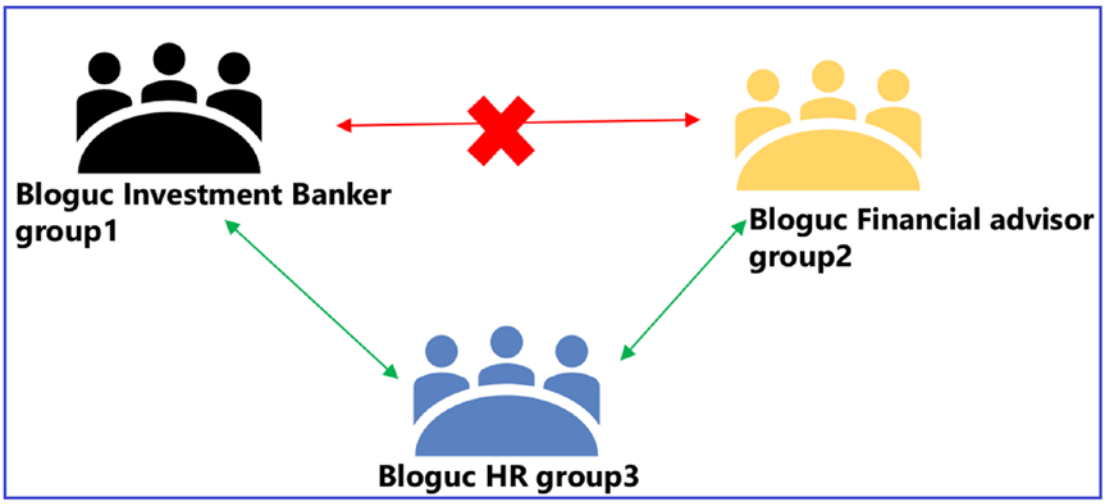

Figure 5-31. *Information barriers between groups [22a]*

Information Barrier Policies

IB policies allow you to control communication and collaboration in Microsoft 365 workloads between two groups of people. You can set IB policies to prevent a day trader from calling someone on the marketing team or to keep finance personnel working on confidential company information from receiving calls from certain groups within the organization. Perhaps the organization wants to allow a research team to call or chat online only with the product development team.

Who Can Set Up Information Barriers Policies?

The tenant admins, compliance administrator, or IB administrator can define policies to allow or prevent communications between groups of users in Microsoft Teams. IB policies can be defined to prevent or allow communications in Microsoft Teams. Such policies can prevent people from calling or chatting with those they shouldn't or enable people to communicate only with specific groups in Microsoft Teams. With IB policies in effect, whenever users who are covered by those policies attempt to communicate with others in Microsoft Teams, checks are performed to prevent (or allow) communication, as defined by IB policies [24a].

Note At present, IBs do not apply to email communications or to file sharing through SharePoint Online or OneDrive. In addition, IBs are independent from compliance boundaries.

Defining Information Barrier Policies

Before defining an IB policy, you as a Teams or security admin need to the prerequisites listed here.

1. Verify that you have the required licenses and permissions. IB is included in subscriptions such as Microsoft 365 E5, Office 365 E5, Office 365 Advanced Compliance, and Microsoft 365 E5 Information Protection and Compliance. Also, as a Teams admin you must have one of the following role permissions to define or edit IB policies:
   - Microsoft 365 global administrator
   - Office 365 global administrator
   - Compliance administrator
   - IB Compliance Management (this is a new role)
2. Validate that the directory includes data for the segmenting users. Make sure that your organization's structure is reflected in directory data. To do this, make sure that user account attributes, such as group membership, department name, and so on, are populated correctly in Azure AD (or Exchange Online).
3. Before you define your organization's first IB policy, you must enable scoped directory search in Microsoft Teams. Wait at least 24 hours after enabling scoped directory search before you set up or define IB policies.
4. To look up the status of a policy application, audit logging must be turned on. We recommend doing this before you begin to define segments or policies.

5. Before you define and apply IB policies, make sure no Exchange address book policies are in place. (IBs are based on address book policies, but the two kinds of policies are not interchangeable.)
6. As of this writing, IB policies are defined and managed in the Office 365 Security & Compliance Center using PowerShell commands. No GUI is available.
7. When your policies are in place, IBs can remove people from chat sessions they are not supposed to be in. This helps ensure your organization remains compliant with policies and regulations. Use the following procedure to enable IB policies to work as expected in Microsoft Teams [24b].

Defining an IB policy is a three-part process.

1. Segment the users in your organization by determining what policies are needed, then make a list of segments. Identify which attributes to use and then define segments in terms of policy filters.
2. Define the IB policies, but do not apply them yet. Select from two kinds: block or allow.
3. Apply the IB policies involving tasks like setting policies to active status, running the policy application, and viewing policy status.

There are many steps involved in defining IB policies, and they change frequently. Refer to the Microsoft official documentation at https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies? for up-to-date information.

Creating and Managing Office 365 Group Classification

Microsoft Teams is built on Office 365 Groups. Office 365 Groups has multiple capabilities, and one of them is classification, which is often used in organizations to classify content. As an admin, you can determine and add information about the group purpose. For example, your organization decides to inform users what type of documents are stored within the Office 365 Group. This type of group functionality is called group classification. You as an admin can configure group classification so that when users in your organization create a group, they can choose a classification like, Standard, Internal, or Confidential.

Note Office 365 Group classifications do not exist by default. Admins will need to create the group classifications so that users can apply them when they create a group.

Enabling and Configuring Office 365 Group Classifications

Remember, group classification is not enabled by default. Before users can apply classifications to Office 365 Groups, you as an admin need to configure the classifications using Azure AD Windows PowerShell commands. First, install the latest AzureADPreview module using the following PowerShell commands [99].

- Remove any earlier version of AzureADPreview using this command

  ```
  Uninstall-Module AzureADPreview
  Uninstall-Module azuread
  ```

- Install the latest version of AzureADPreview using this command.

  ```
  Install-Module AzureADPreview
  ```

To configure the classifications Standard, Internal, and Confidential, use the following command.

```
$Template = Get-AzureADDirectorySettingTemplate | Where {$_.DisplayName -eq
"Group.Unified"}
if (!($Setting=Get-AzureADDirectorySetting|Where {$_.TemplateId
-eq $Template.
Id})) {$Setting = $Template.CreateDirectorySetting}
$setting["ClassificationList"] = "Standard, Internal, Confidential"
```

As the next step, you must associate a description with each classification using the settings attribute `ClassificationDescriptions`, where classification should match the strings in the `ClassificationList`. For example, to add a description to the classifications Standard, Internal, and Confidential, run the following command.

```
$setting["ClassificationDescriptions"] = "Standard: General communication,
Internal: Company internal data, Confidential: Data that has regulatory
requirements"
```

To validate that the classification configuration is added correctly to the group, you need to run the `$Setting. Values` command.

To commit the setting to Azure AD and make sure the classifications can be applied by your users, you need to run this command.

```
Set-AzureADDirectorySetting -Id $Setting.Id -DirectorySetting $Setting
```

Note The classification settings update could take an hour before they are available for all users, so be patient after configuring the classification.

Configuring Classifications from Outlook and Teams Client

After enabling Office 365 Group classifications, you as an admin can assign the classification to a group from Outlook or Teams client. To do so, log in to Microsoft Teams client and select Teams. Select Join Or Create and then select appropriate the classification, as shown in Figure 5-32.

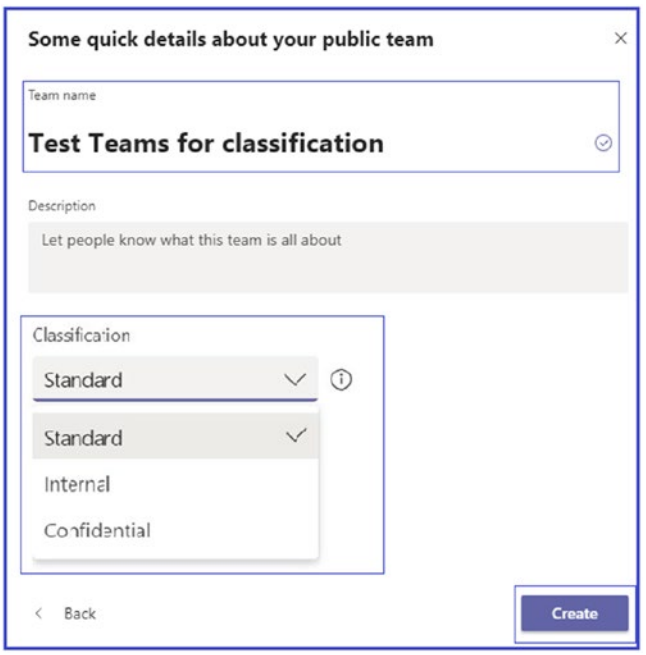

Figure 5-32. *Classification options*

You can also configure classifications on Office 365 Groups using Windows PowerShell. To set a classification to an Office 365 Group, you use the `Set-UnifiedGroup` command with the `-Classification` parameter. For example, to set a Confidential classification on the group SecretData@bloguc.com, run this command in Exchange Online PowerShell.

```
Set-UnifiedGroup "SecretData@bloguc.com" -Classification "Confidential"
```

You can also create a group and assign a classification during the group creation process. For example, to create a new private group named HRDepartment@bloguc.com with a classification of Internal, run the following cmdlet:

```
New-UnifiedGroup "HRDepartment@bloguc.com" -Classification "Internal"
-AccessType "Private"
```

Creating and Managing Office 365 Group Expiration Policy That Applies to Associated Content

Microsoft Teams is built on Office 365 Groups and every team has Office 365 Groups associated with it. This means whenever a user creates a new team, an Office 365 Group is automatically provisioned. Therefore, as the number of teams grows, the Office 365 Group count automatically grows as well. As a Teams admin, you must manage these groups to control their expansion. In many cases, users create a team for a specific task, but after that task is completed, the team and Office 365 Group remain active but unused. For example, User A created a team for implementing Microsoft Identity Manager in Bloguc Organization. When the project ended, User A forgot to delete that project team. That means the Office 365 Groups and team content still exist. Such use cases will increase the Office 365 Group (and team) count, which adds to management overhead and eventually makes IT administration difficult.

To manage Office 365 Groups regardless of a team's association, you need a method to clean up the unused groups and simplify management. The best solution is to set a group expiration policy, which helps to remove unused groups from the directory system. The group expiration is turned off by default in Office 365. When you decide to implement group expiration, you need to enable the feature for your organization

tenants and specify an expiration period for the Office 365 Group. Once you set up group expiration, when the expiration date for a group approaches, an email notification is sent to the group owners (whoever created or was set as an owner of the group) to determine if group renewal is required for an additional period. If the group is not renewed, it will be deleted automatically [95].

Note If group expiration policy changes are made by an admin, the Office 365 expiration period will be recalculated for the groups.

Important When an Office 365 Group expires, all the group's associated content will be deleted, including Outlook, Planner, and SharePoint. However, there is an option to recover content for up to 30 days from the expiration date.

Note Renewal notifications are emailed to group owners 30 days, 15 days, and 1 day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Microsoft Teams, and PowerBI.

To configure the Office 365 Group expiration policy, perform these steps.

1. Log in to Azure Active Directory admin center (`https://aad.portal.azure.com/`) as a global administrator. In the left pane, select Azure Active Directory. Under Manage, select Groups, and then select Expiration to open the expiration settings page, shown in Figure 5-33.

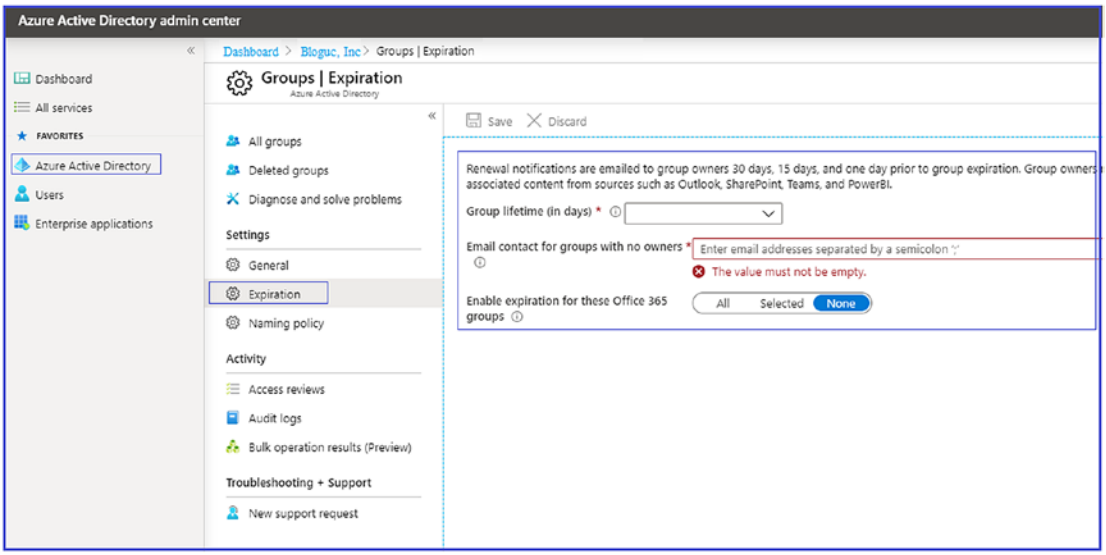

Figure 5-33. *Group expiration settings page*

2. On the Expiration page, you can specify several options.

   - *Group Lifetime (In Days):* This option sets the group lifetime in days with choices of 180, 365, or Custom. The Custom setting requires a lifetime of at least 30 days. The example in Figure 5-34 shows a setting of Custom and 90 days.

   - *Email Contact For Groups With No Owners:* Specify an email address where the renewal and expiration notifications should be sent when a group has no owner. If the group does not have an owner, the expiration emails will go to a specified admin. Figure 5-34 shows the contact email account for groups with no owner.

   - *Enable Expiration For These Office 365 Groups:* Select the Office 365 Groups for which you would like to configure this expiration policy. The options are All, for all the groups within your organization; Selected, for only specific groups; and None, which turns this off entirely. For this example, in Figure 5-34, the Selected option is chosen and the group Test is specified.

Note You should set the expiration policy for a test group first. Once this setting is properly tested, then you can enable expiration policy for the all the groups in your organization.

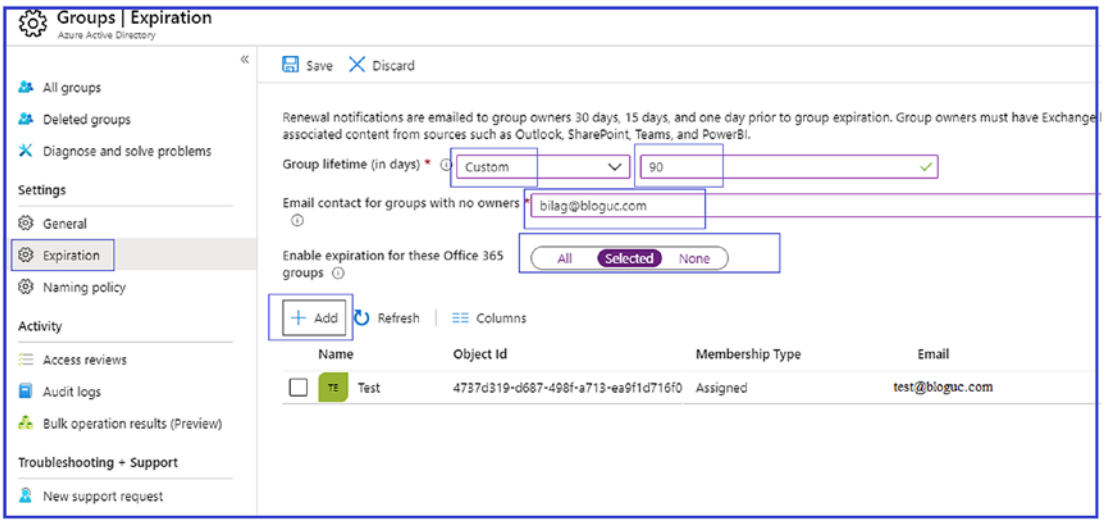

Figure 5-34. *Group expiration settings*

3. After finishing the configuration, click Save.

Remember that group expiration is a feature that is incorporated in an Azure AD Premium subscription. An Azure subscription license is necessary for the admins who are going to configure the settings and the members of the affected groups. Specific to the management aspect, you as a Teams admin (with Office 365 global admin group permission) can create, view, modify, or delete the Office 365 Groups expiration policy settings and users can renew or restore an Office 365 Group that they own.

How Group Expiration Works with the Retention Policy

When you as a security admin set up a retention policy in the Microsoft 365 Security & Compliance Center for groups, then the expiration policy works in association with retention policy. Once a group expires, the group's conversations in Outlook and files in SharePoint Online are kept in the retention container for the duration (number of days)

specified in the retention policy. The users will not see the group or its content after expiration, however. That's why a user must monitor the group expiration notification and act in a timely manner instead of losing control of their content [96].

How Group Owners Receive Expiration Notifications

Specific to the group expiration notification, when a group is about to expire, group owners will be notified via email, irrespective of how the group was created, whether through SharePoint, Planner, Teams, or any other Office 365 application. If the group was created via Teams, the group owner will receive a notification to renew through the activity section in the Microsoft Teams client. The group owner will receive the group expiration notification before 30 days, and if it is not renewed, an additional renewal email will be sent 15 days before the expiration. In the event the group is still not renewed, one more email notification will be sent the day before the expiration.

If no one renews the group before it expires, it will be automatically deleted, but the admins will still be able to restore the group within 30 days after the expiration date. It is important to understand that not every admin can restore the expired group, as specific permissions are required to restore a group: Global administrators, Group administrators, Partner Tier2 support, and Intune administrators can restore any deleted Office 365 Group.

Creating and Managing Office 365 Groups Naming Policy Applicable to Teams

When a user creates an Office 365 Group or Microsoft Teams team (which creates an Office 365 Group in the back end) for their professional use then the expectation is that they should use a meaningful name. Out of the box, users can use any name while creating a group, but if your organization requires a specific naming format, you as an admin can achieve this using a group naming policy that implements a consistent naming strategy for groups created by users. The naming policy will be able to help users identify the function of the group, membership, or the person who created the group. The policy is applied to groups that are created across all Office 365 apps, including Outlook, Teams, SharePoint, Planner, and Yammer. It applies for group names and group aliases, as well.

When creating a naming policy, you must be aware that the maximum group name length is 53 characters, including the prefixes and suffixes. Prefixes and suffixes can

contain special characters in the group name (and group alias), and if they contain special characters that are not allowed in the group name they will be removed and applied to the group alias. This will result in group prefixes and suffixes that will be different from the ones applied to the group alias. Finally, be aware that if you are using Yammer Office 365 connected groups, avoid using the following characters in your naming policy: @, #, [,], <, and >. If these characters are in the naming policy, regular Yammer users will not be able to create groups.

The Office 365 Group naming policy includes a prefix-suffix naming policy. You can use prefixes or suffixes to describe the naming convention of groups. For example, if you configure GRP as a prefix, then the Marketing group will be names GRP Marketing. Custom blocked words is another important features, as it allows an admin to specify a variety of words that will be blocked in groups created by users, such as CEO, CFO, Invoice, Billings, Payments, HR, and so on.

Working with Prefixes and Suffixes in a Group Naming Policy

Specific to the naming policy, prefixes and suffixes can either be fixed strings or user attributes. When using fixed strings, it is advised that an admin assign short strings that will help differentiate groups in the Global Address List (GAL). Some of the frequently used prefixes and suffixes are keywords such as, Ext_name, Int_name, Grp_Name, #Name, or _Name.

Using attributes, you can use attributes that can assist in identification of which user has created the group, like [Department], and where it was created from, like [Country]. For example, a naming policy of GRP [GroupName] [Department] will result in the following if the group is named My Group and the user's department is Marketing: GRP My Group Marketing. Attributes supported in Azure AD are [Department], [Company], [Office], [StateOrProvince], [CountryOrRegion], and [Title]. Unsupported user attributes are considered fixed strings (e.g., [postalCode]). Also, extension attributes and custom attributes are not supported. It's advisable to use attributes that have values filled in for all the users in your organization and not to use attributes that have longer values.

Creating and Managing Group Naming Policy in Office 365 Tenant

Naming policy provides a way to standardize Office 365 Groups naming, and it allows you to block certain names as well. You can configure naming policy using Azure AD admin center and Windows PowerShell. To create a naming policy, follow this procedure.

1. Log in to Azure Active Directory admin center (https://aad.portal.azure.com/) as a global administrator. In the left pane, select Azure Active Directory. Under Manage, select Groups. In the Settings section, select Naming Policy. Open the Group Naming Policy tab, shown in Figure 5-35.

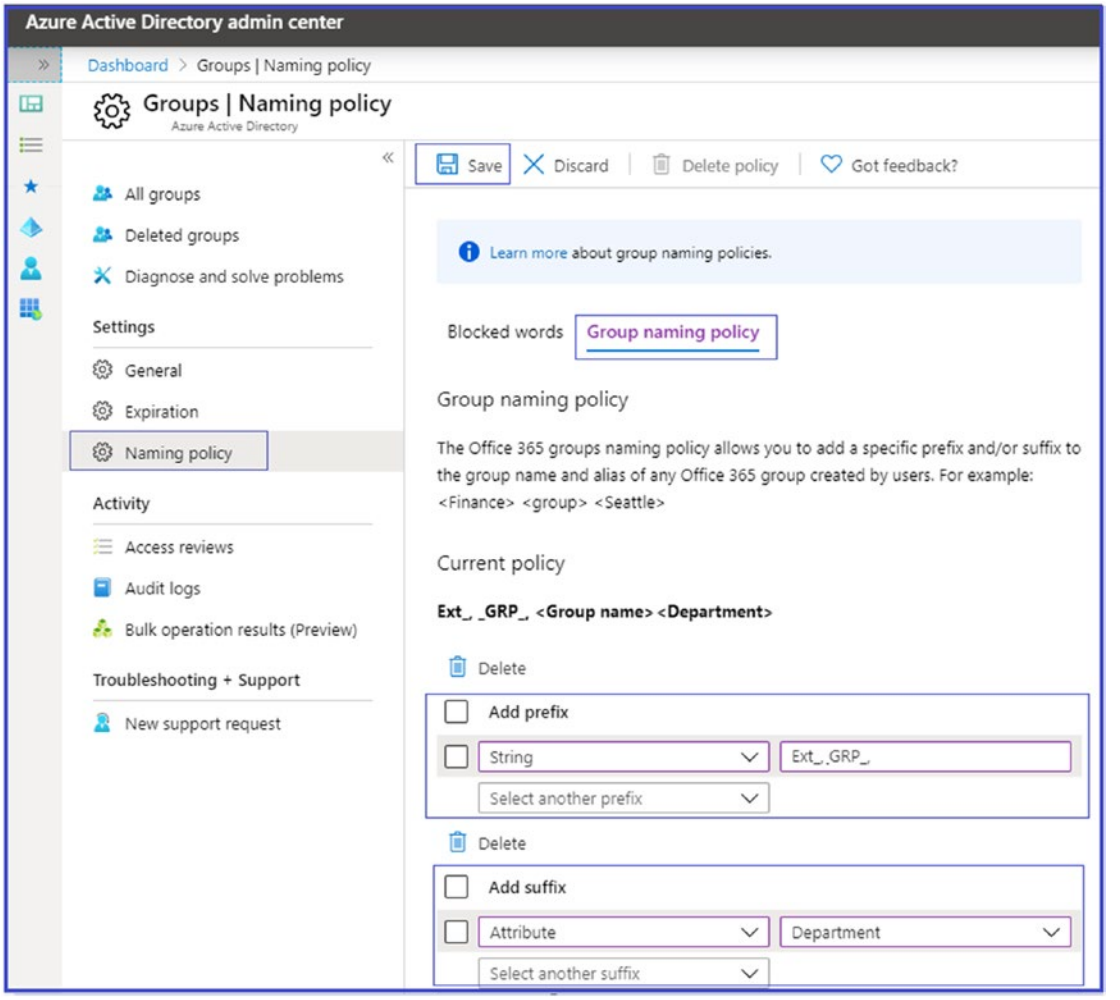

Figure 5-35. *Creating a naming policy*

2. In the Current Policy section, select whether you would like to require a prefix or suffix (or both) and select the appropriate check boxes. For either of these settings, choose between Attribute and String. Figure 5-35 shows the Ext_ and GRP_ prefixes and a Department suffix selected.

Creating Office 365 Groups Naming Policy Using Windows PowerShell with Azure AD Module

Before creating a new policy, you must check if any existing Office 365 Groups naming policy is available. Install latest Azure AD PowerShell module (if it is not already installed). Open Windows PowerShell as an administrator and connect to Azure AD, and then run this command.

```
$Setting = Get-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting |
where -Property DisplayName -Value "Group.Unified" -EQ).id
$Setting.Values
```

In the output, check the values for `CustomBlockedWordsList`, `EnableMSStandardBlockedWords`, and `PrefixSuffixNamingRequirement`.

Execute the next PowerShell command to create the naming policy in the existing PowerShell module that is connected to the Azure AD.

```
$Setting = Get-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting |
where -Property DisplayName -Value "Group.Unified" -EQ).id
```

Set the group name prefixes and suffixes; for example, the prefixes `Ext_` and `GRP_`.

```
$Setting["PrefixSuffixNamingRequirement"] ="Ext_[GroupName]","GRP_
[GroupName]"
```

To configure custom blocked words that you want to restrict— for example, Invoices, Payroll, and CEO—run this command.

```
$Setting["CustomBlockedWordsList"]="Invoices,Payroll,CEO"
```

You can modify the setting in the Azure AD directory by running this command.

```
Set-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting | where
-Property DisplayName -Value "Group.Unified" -EQ).id -DirectorySetting
$Setting
```

Managing Naming Policy

You can add or remove a naming policy using Azure AD. To add or remove a naming policy, log in to Azure AD and then open the Naming Policy page to add or modify the policy. If you are removing an existing policy, then it will ask for confirmation. Once you confirm the deletion, the naming policy is removed, along with all prefix-suffix naming policies and any custom blocked words.

Adding Custom Blocked Words Under Naming Policy

In a naming policy, custom blocked words are those users are not permitted to use when creating a group. You can also list several blocked words, which need to be separated by a comma. The blocked words check is done on the group name when it is entered by a user. For example, if a user enters CEO and Prefix_ as the naming policy, Prefix_CEO will fail. A substring search is not conducted, so that users can use common words like Pilot even if lot is a blocked word.

To add the a custom blocked word, log in to Azure AD. Under Manage, select Groups. In the Settings section, select Naming Policy, and then click the Blocked Words tab, shown in Figure 5-36.

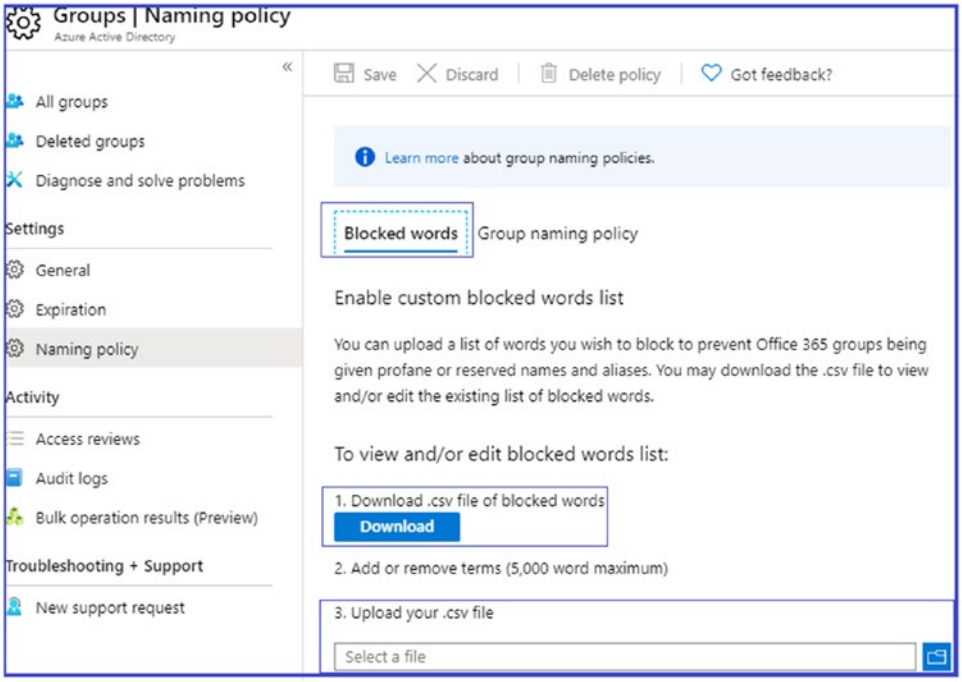

Figure 5-36. *Custom blocked words*

Summary

In summary Microsoft Teams is built on Office 365 Groups, which contains a set of tools to implement governance capabilities that any organization requires. In this chapter, you learned about the features you can use for Teams governance, including Teams identity management (including conditional access policies), DLP, eDiscovery, retention, and classification. You also learned how to set expiration policies and naming policies.