Teaching IT How To Manage And Govern Microsoft Teams And Other Office 365 Workloads

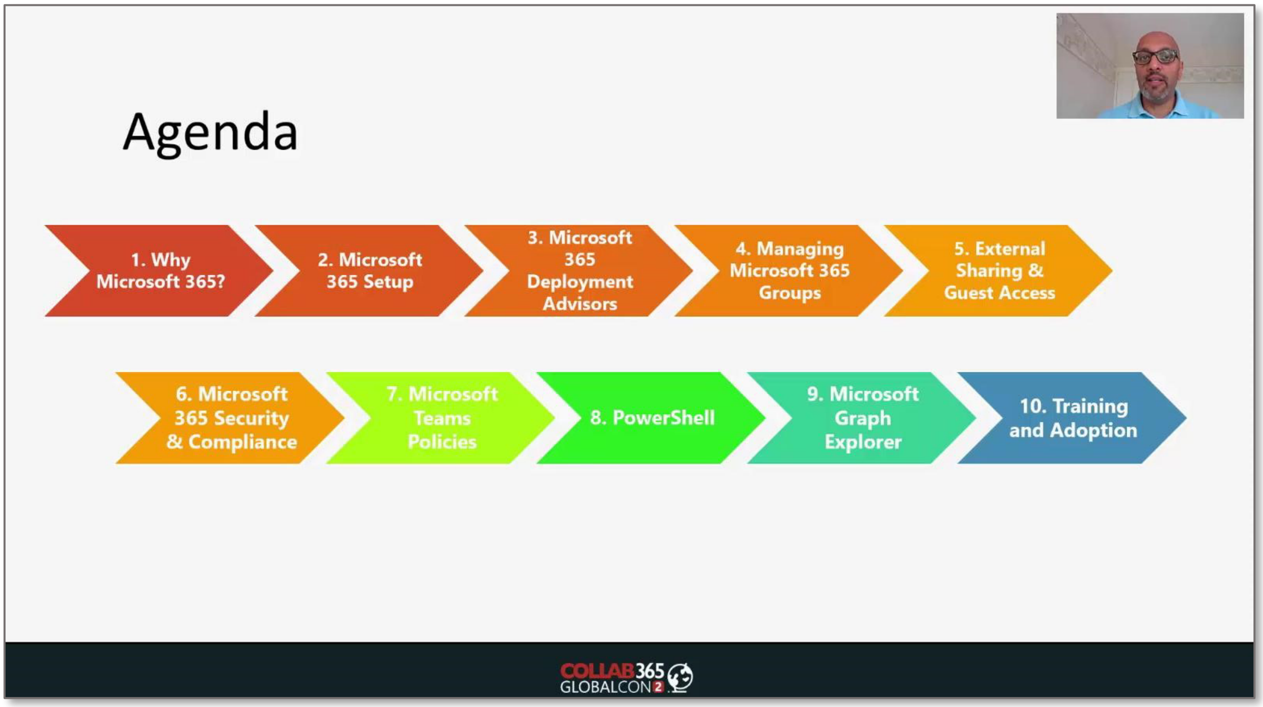
This eBook will consider 10 steps that will help you manage your Microsoft teams and Microsoft 365 workloads effectively to ensure your users remain happy and informed, throughout your organisation.

collab365.

Contents

Introduction

This eBook will consider ten steps that will help you manage your Microsoft teams and Microsoft 365 workloads effectively to ensure your users remain happy and informed throughout your organization.



Agenda

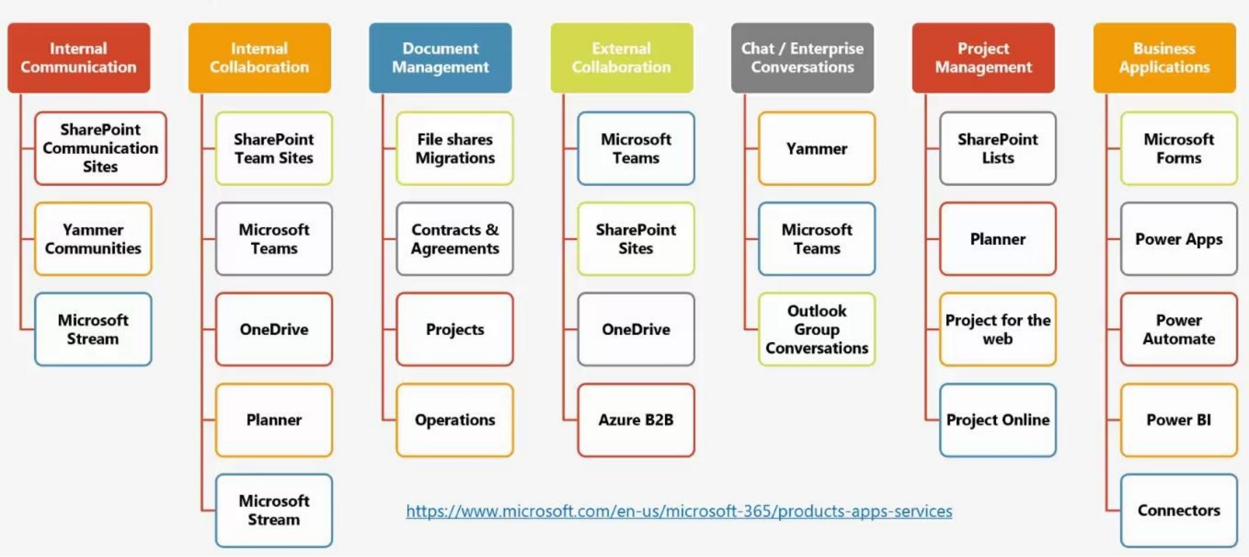
1. Why Microsoft 365?
2. Microsoft 365 Setup
3. Microsoft 365 Deployment Advisors
4. Managing Microsoft 365 Groups
5. External Sharing & Guest Access
6. Microsoft 365 Security & Compliance
7. Microsoft Teams Policies
8. PowerShell
9. Microsoft Graph Explorer
10. Training and Adoption

COLLAB365 GLOBALCON2

We'll look at various admin capabilities around Microsoft 365 setup to help you monitor your live environment, looking out for red alarms, as well as looking at deployment advisors, to help you roll out additional services. We'll also look at the Microsoft 365 groups in terms of how best to manage them as that's the underlying component for a lot of your online services. On the way, we will also consider external sharing, guest access, security, and compliance with policies, as well as looking at PowerShell tools for some advanced administration capabilities as well.

Why Microsoft 365?

Microsoft 365 provides many different services, SharePoint, Microsoft Teams, Yammer, etc.. Still, at the end of the day, it's all about what kind of services you're delivering that matters to the users. The diagram below groups different technical services into specific business needs, such as collaboration, external collaboration, document management and so on. You'll notice that some of the services appear in multiple categories, which just illustrates how central they are to many different business processes.



Internal Communication
- SharePoint Communication Sites
- Yammer Communities
- Microsoft Stream

Internal Collaboration
- SharePoint Team Sites
- Microsoft Teams
- OneDrive
- Planner
- Microsoft Stream

Document Management
- File shares Migrations
- Contracts & Agreements
- Projects
- Operations

External Collaboration
- Microsoft Teams
- SharePoint Sites
- OneDrive
- Azure B2B

Chat / Enterprise Conversations
- Yammer
- Microsoft Teams
- Outlook Group Conversations

Project Management
- SharePoint Lists
- Planner
- Project for the web
- Project Online

Business Applications
- Microsoft Forms
- Power Apps
- Power Automate
- Power BI
- Connectors

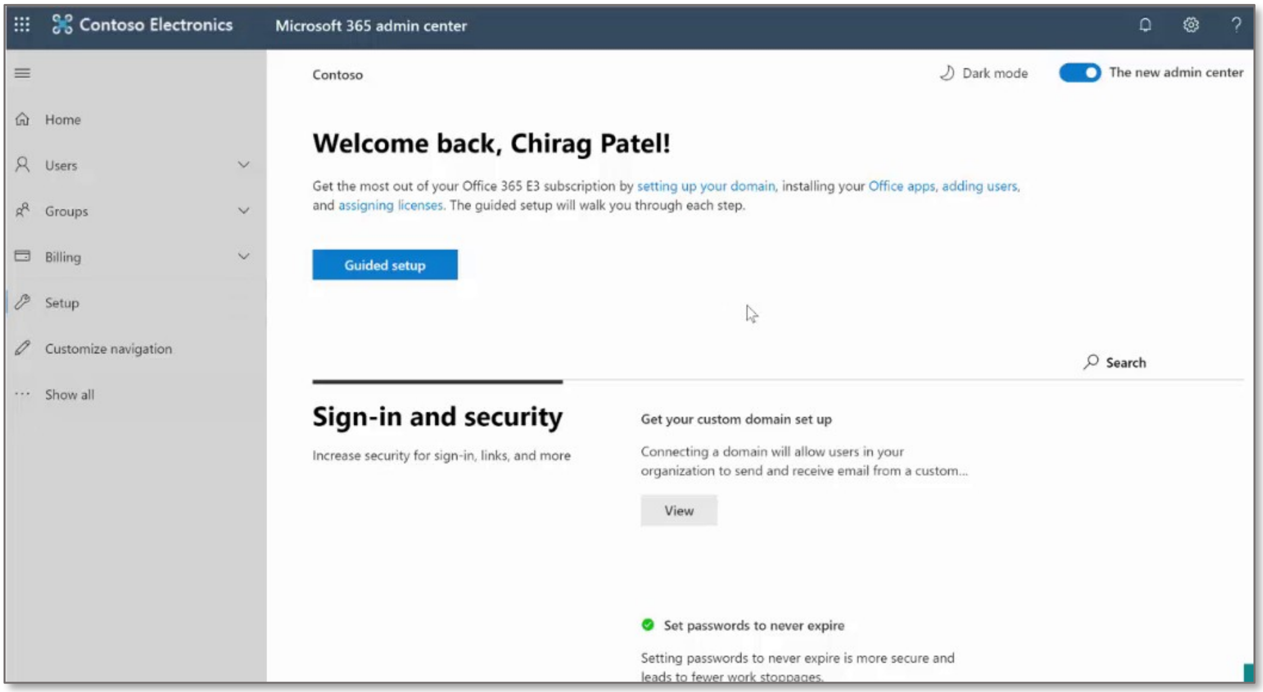
https://www.microsoft.com/en-us/microsoft-365/products-apps-services

If you look at document management, for example, you can have different contracts, agreements, and corporate projects. Once you group roughly the services you're providing, then you're able to fulfil and support your users in helping to meet the various scenarios that you may have.

Updates to apps and services you get as part of Microsoft 365 can be found here: https://www.microsoft.com/en-us/microsoft-365/products-apps-services.

Microsoft 365 Setup

The Setup options within the Microsoft 365 Admin Centre provide recommendations for tasks based on the Microsoft 365 Services you are using. It gives you traffic light indicators as to what's completed, or what needs to be completed and also provides information about what impact the changes will have on your users.



Contoso

Welcome back, Chirag Patel!

Get the most out of your Office 365 E3 subscription by setting up your domain, installing your Office apps, adding users, and assigning licenses. The guided setup will walk you through each step.

Sign-in and security

Increase security for sign-in, links, and more

Get your custom domain set up

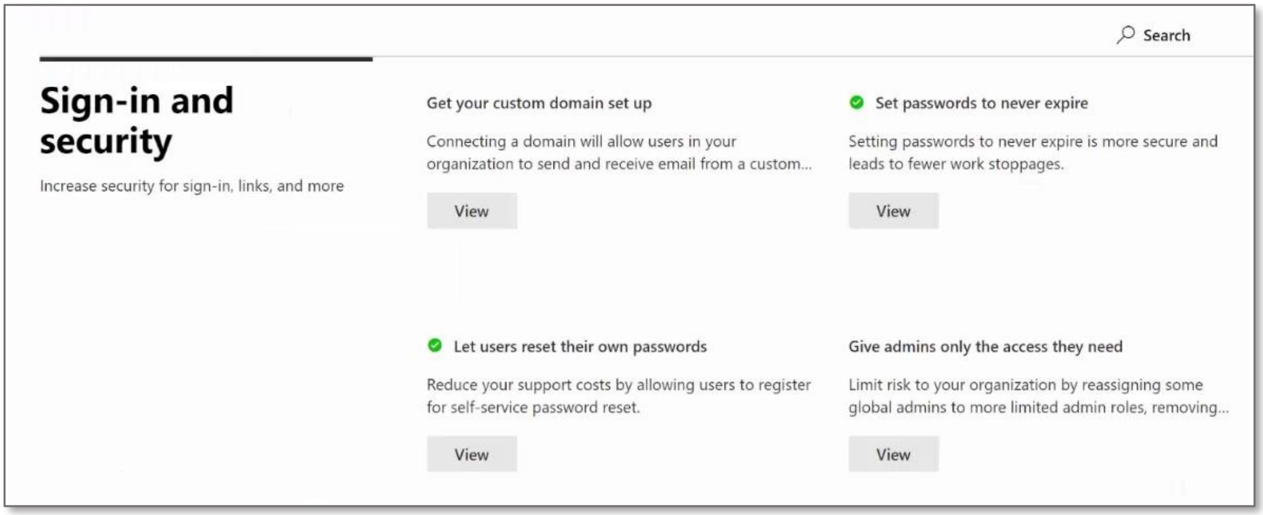
Connecting a domain will allow users in your organization to send and receive email from a custom...

✓ Set passwords to never expire

Setting passwords to never expire is more secure and leads to fewer work stoppages.

Using the Setup options

Let's take a look at that in slightly more detail. There are many different options in Setup. Green ticks against an item mean that you have configured that element. In my example below, I've set passwords never to expire and also to allow users to reset their passwords. Items without green ticks mean that those areas can be configured if you want them to be.



Sign-in and security

Increase security for sign-in, links, and more

Get your custom domain set up

Connecting a domain will allow users in your organization to send and receive email from a custom...

✓ Set passwords to never expire

Setting passwords to never expire is more secure and leads to fewer work stoppages.

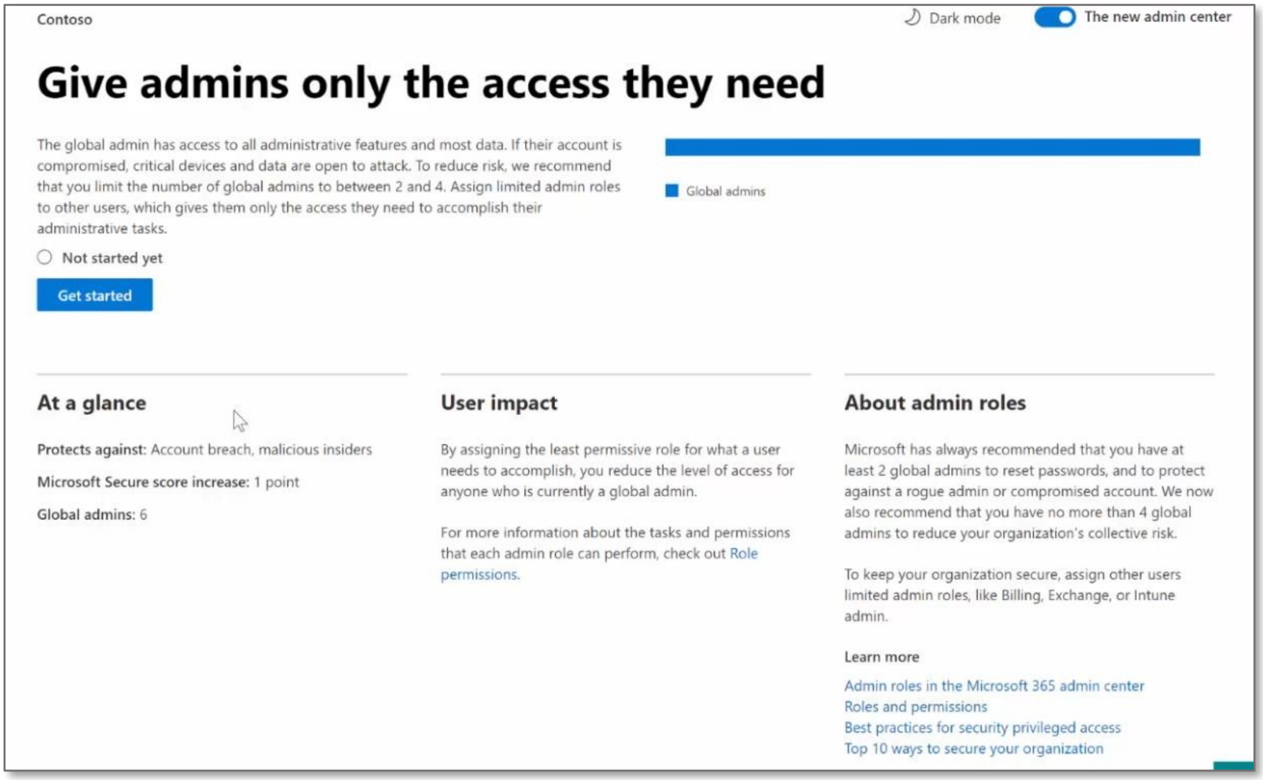
✓ Let users reset their own passwords

Reduce your support costs by allowing users to register for self-service password reset.

Give admins only the access they need

Limit risk to your organization by reassigning some global admins to more limited admin roles, removing...

By clicking ”View” for “Give admins only the access they need,” you will see additional information about the feature. The “At a glance” section summarises the effect of that control, and “User impact” section explains what will happen and also provides more links if available.



Give admins only the access they need

The global admin has access to all administrative features and most data. If their account is compromised, critical devices and data are open to attack. To reduce risk, we recommend that you limit the number of global admins to between 2 and 4. Assign limited admin roles to other users, which gives them only the access they need to accomplish their administrative tasks.

○ Not started yet

At a glance

Protects against: Account breach, malicious insiders

Microsoft Secure score increase: 1 point

Global admins: 6

User impact

By assigning the least permissive role for what a user needs to accomplish, you reduce the level of access for anyone who is currently a global admin.

For more information about the tasks and permissions that each admin role can perform, check out Role permissions.

About admin roles

Microsoft has always recommended that you have at least 2 global admins to reset passwords, and to protect against a rogue admin or compromised account. We now also recommend that you have no more than 4 global admins to reduce your organization's collective risk.

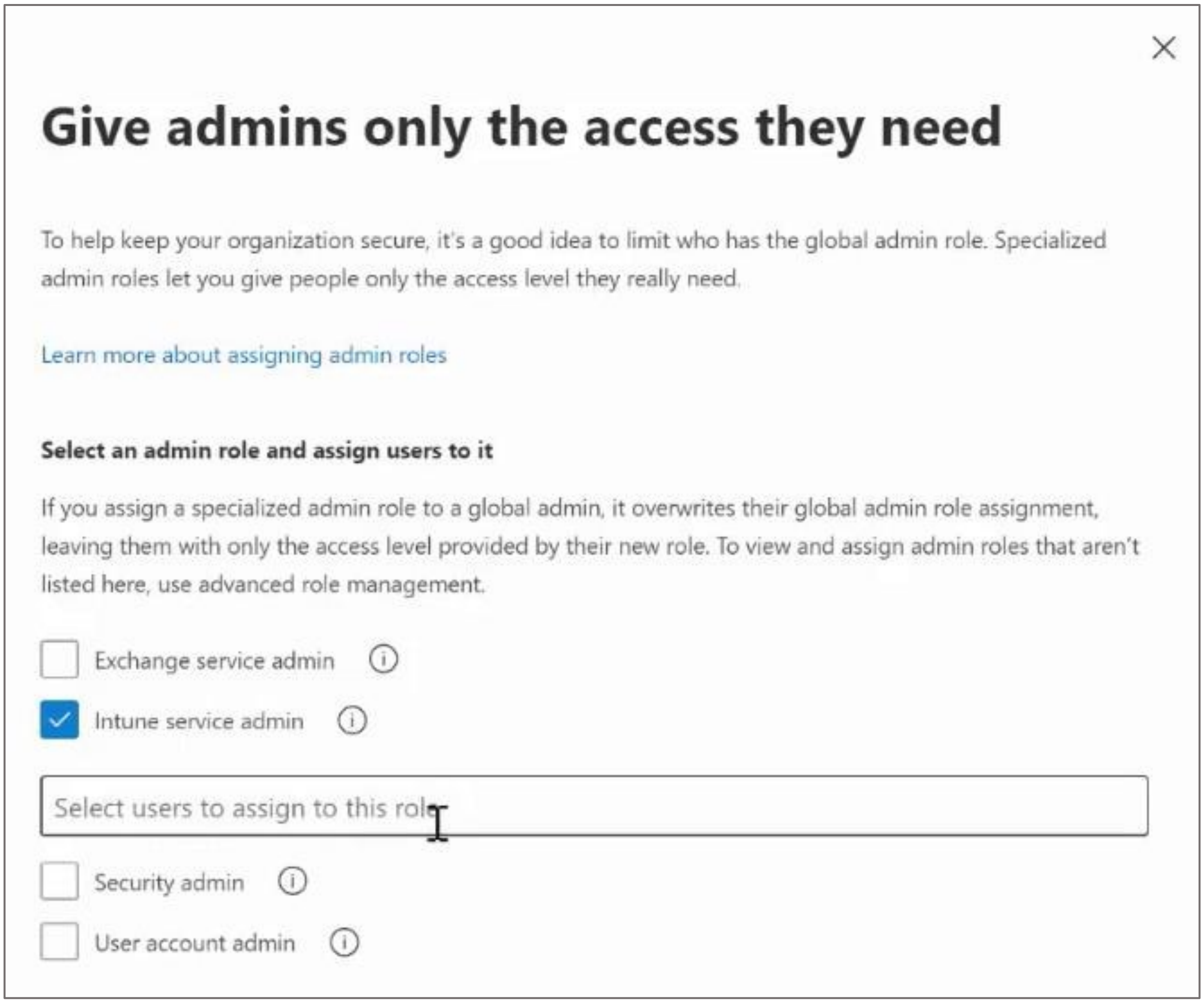
To keep your organization secure, assign other users limited admin roles, like Billing, Exchange, or Intune admin.

Learn more

Admin roles in the Microsoft 365 admin center
Roles and permissions
Best practices for security privileged access
Top 10 ways to secure your organization

We’ll consider the Microsoft Secure score increase later in this book. In the example above, you can see there are six global admins, which is quite a lot. The recommendation here is to reduce the number of Global admins, to no more than four, and only give that level of access to the people who need it to do their jobs. Following this recommendation and assigning less permissive roles to two of the current Global admins will reduce their level of access and reduce the organization's collective risk.

Click “Get started” to make changes, select the correct new admin role, identify the users who need to move to this new role, and finally click “Assign roles.”



Give admins only the access they need

To help keep your organization secure, it's a good idea to limit who has the global admin role. Specialized admin roles let you give people only the access level they really need.

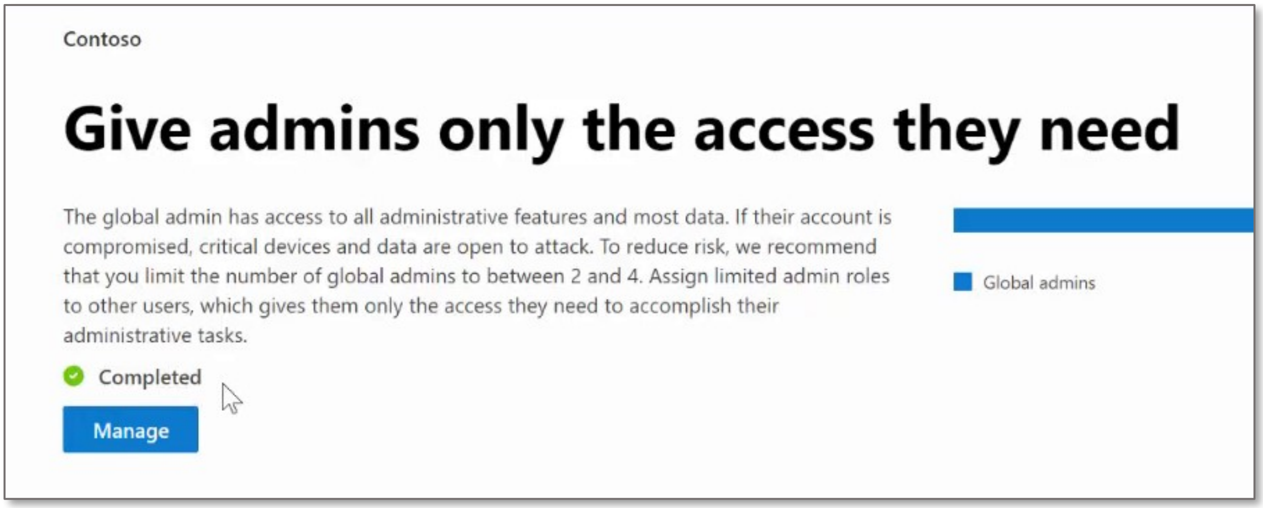
Learn more about assigning admin roles

Select an admin role and assign users to it

If you assign a specialized admin role to a global admin, it overwrites their global admin role assignment, leaving them with only the access level provided by their new role. To view and assign admin roles that aren't listed here, use advanced role management.

- ☐ Exchange service admin
- ☑ Intune service admin
- Select users to assign to this role
- ☐ Security admin
- ☐ User account admin

When you go back to the original screen, you'll notice that it has a completed status and green tick.



Contoso

Give admins only the access they need

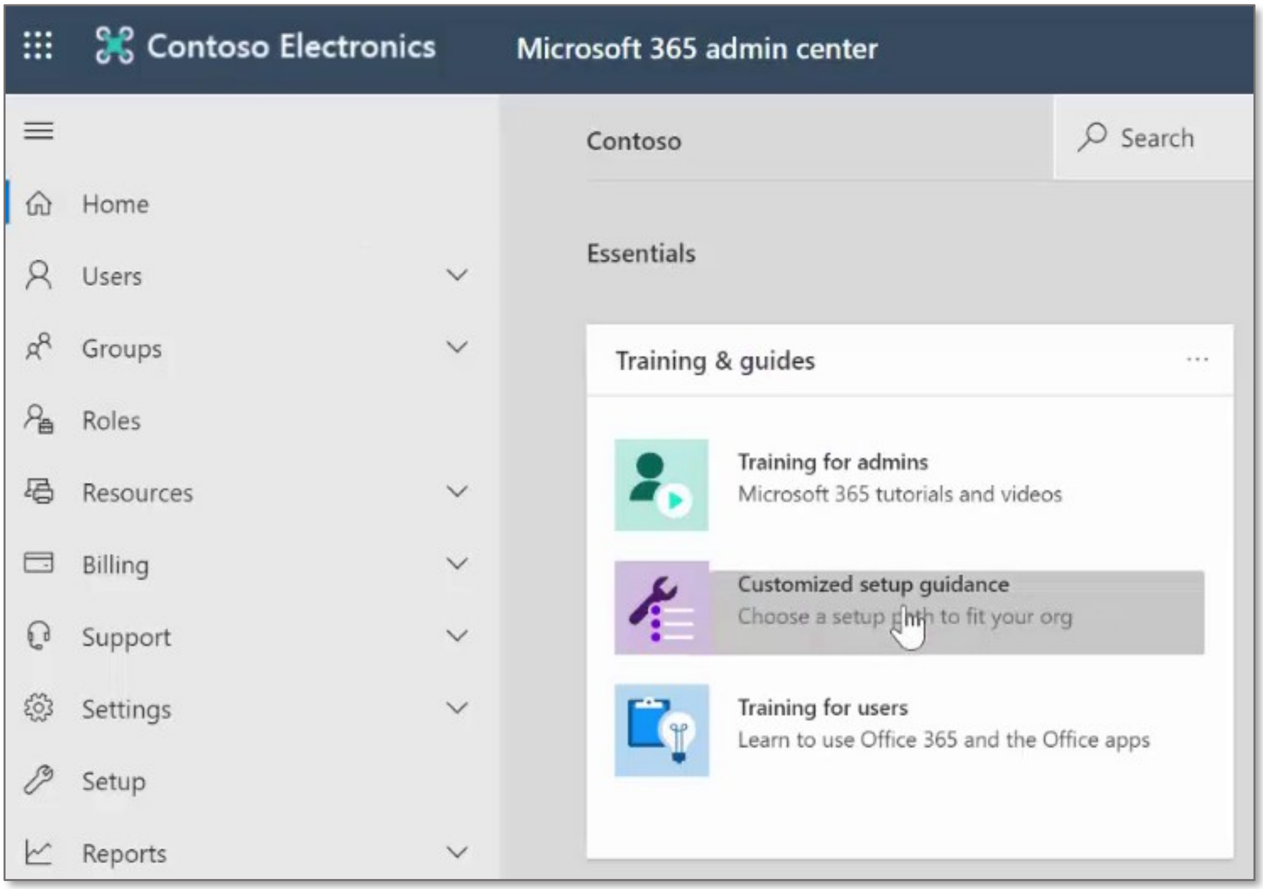
The global admin has access to all administrative features and most data. If their account is compromised, critical devices and data are open to attack. To reduce risk, we recommend that you limit the number of global admins to between 2 and 4. Assign limited admin roles to other users, which gives them only the access they need to accomplish their administrative tasks.

The Admin Centre allows you to amend many other configurations from this central point and is really helpful in managing and controlling your entire environment.

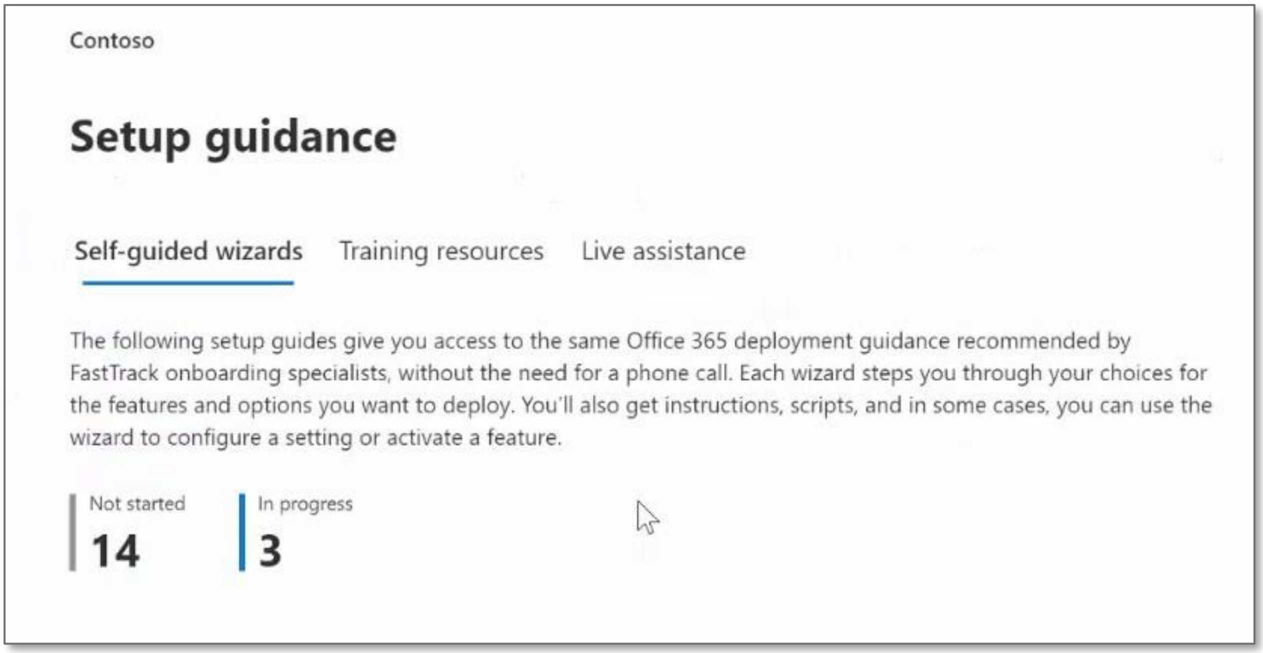
Microsoft 365 Deployment Advisors.

This area of the admin center helps you to configure and roll out additional services within Microsoft 365 admin.

From the main admin center, go to the “Training & guides” section and select “Customized setup guidance.”


Contoso Electronics
Microsoft 365 admin center
Home
Users
Groups
Roles
Resources
Billing
Support
Settings
Setup
Reports
Contoso
Search
Essentials
Training & guides
Training for admins
Microsoft 365 tutorials and videos
Customized setup guidance
Choose a setup path to fit your org
Training for users
Learn to use Office 365 and the Office apps

Once your users have been informed what updates are going to be rolled out, you can begin those activities from this area.



Contoso

Setup guidance

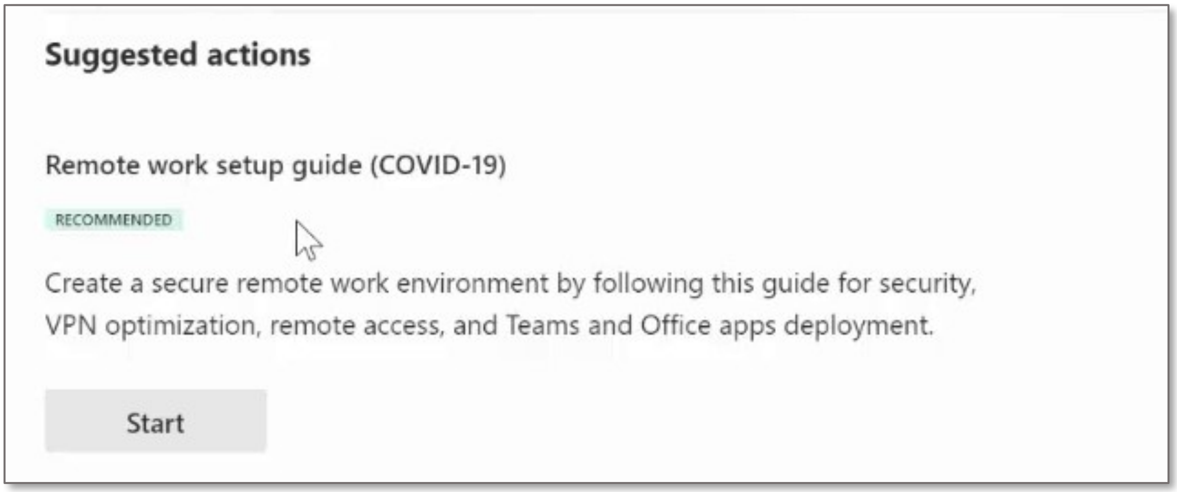
The following setup guides give you access to the same Office 365 deployment guidance recommended by FastTrack onboarding specialists, without the need for a phone call. Each wizard steps you through your choices for the features and options you want to deploy. You'll also get instructions, scripts, and in some cases, you can use the wizard to configure a setting or activate a feature.

Not started 14

In progress 3

The Self-guided wizards are like a shortcut to the Microsoft fast track program, and allow you to configure rollouts in house, using a set of guided steps.

The suggested action below will help secure the Microsoft 365 environment, in light of the COVID-19 situation, by making remote working environments more secure.



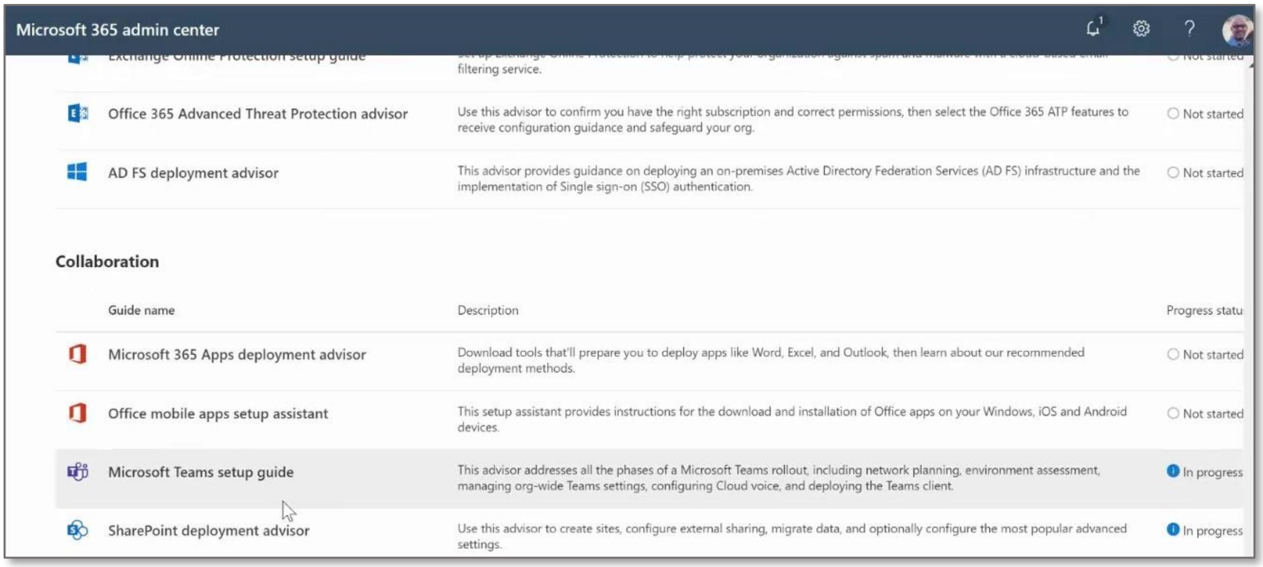
Suggested actions

Remote work setup guide (COVID-19)

RECOMMENDED

Create a secure remote work environment by following this guide for security, VPN optimization, remote access, and Teams and Office apps deployment.

There are several different sections grouping setups for various reasons, including Initial Setup, Security, and Collaboration.



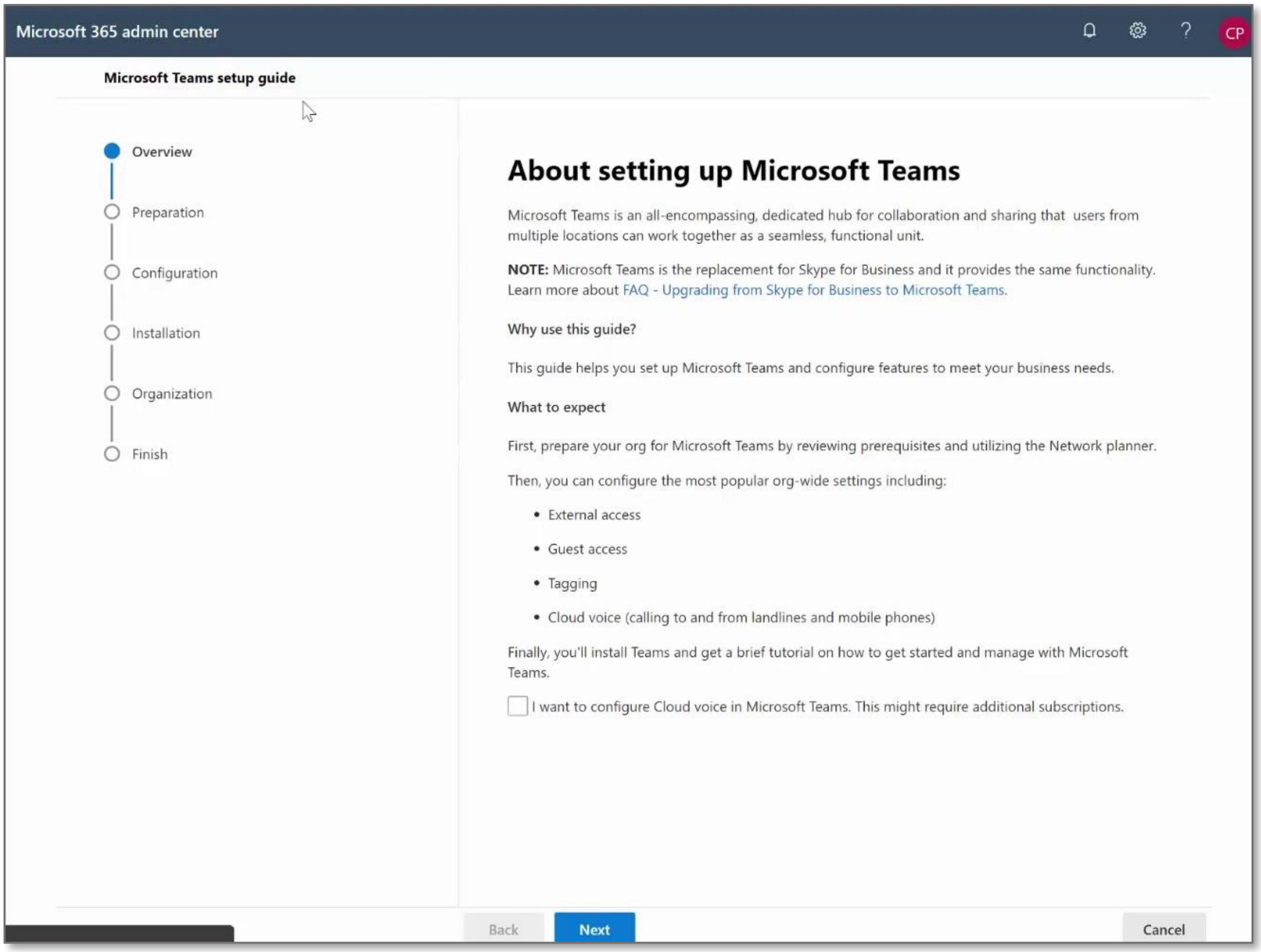
Exchange Online Protection setup guide	Set up Exchange Online Protection to help protect your organization against spam and malware with a cloud-based email filtering service.	○ Not started
Office 365 Advanced Threat Protection advisor	Use this advisor to confirm you have the right subscription and correct permissions, then select the Office 365 ATP features to receive configuration guidance and safeguard your org.	○ Not started
AD FS deployment advisor	This advisor provides guidance on deploying an on-premises Active Directory Federation Services (AD FS) infrastructure and the implementation of Single sign-on (SSO) authentication.	○ Not started

Collaboration

Guide name	Description	Progress statu
Microsoft 365 Apps deployment advisor	Download tools that'll prepare you to deploy apps like Word, Excel, and Outlook, then learn about our recommended deployment methods.	○ Not started
Office mobile apps setup assistant	This setup assistant provides instructions for the download and installation of Office apps on your Windows, iOS and Android devices.	○ Not started
Microsoft Teams setup guide	This advisor addresses all the phases of a Microsoft Teams rollout, including network planning, environment assessment, managing org-wide Teams settings, configuring Cloud voice, and deploying the Teams client.	● In progress
SharePoint deployment advisor	Use this advisor to create sites, configure external sharing, migrate data, and optionally configure the most popular advanced settings.	● In progress

On the right-hand side of the Collaboration section, you can see that there are two actions in progress.

By clicking on the Microsoft Teams setup guide, on the next screen, you can find out how much progress has been made and the remaining steps that need completing before reaching the finishing point. At each stage, additional information is provided on the right-hand side of the page to explain specific configurations.



About setting up Microsoft Teams

Microsoft Teams is an all-encompassing, dedicated hub for collaboration and sharing that users from multiple locations can work together as a seamless, functional unit.

NOTE: Microsoft Teams is the replacement for Skype for Business and it provides the same functionality. Learn more about FAQ - Upgrading from Skype for Business to Microsoft Teams.

Why use this guide?

This guide helps you set up Microsoft Teams and configure features to meet your business needs.

What to expect

First, prepare your org for Microsoft Teams by reviewing prerequisites and utilizing the Network planner.

Then, you can configure the most popular org-wide settings including:

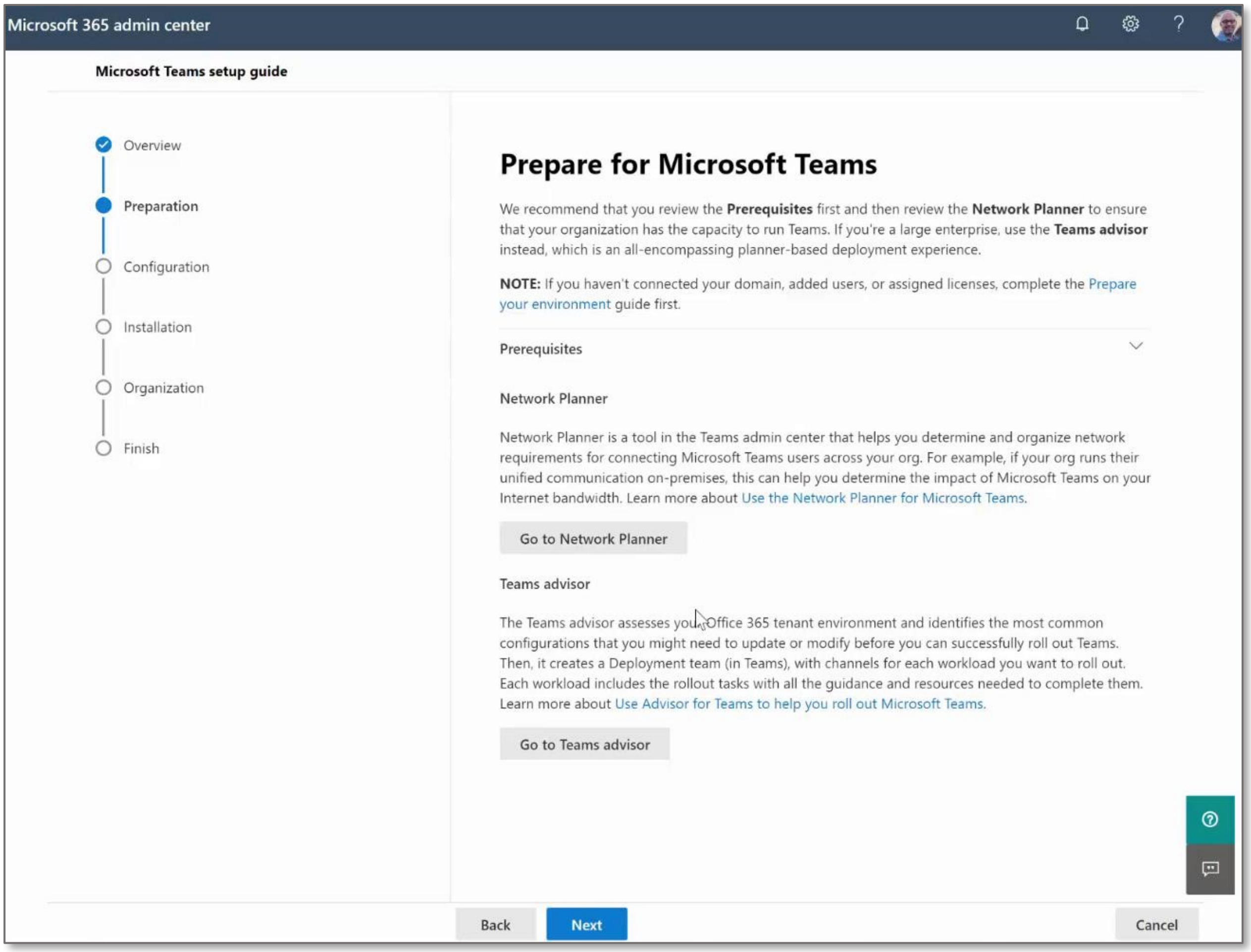
- External access
- Guest access
- Tagging
- Cloud voice (calling to and from landlines and mobile phones)

Finally, you'll install Teams and get a brief tutorial on how to get started and manage with Microsoft Teams.

☐ I want to configure Cloud voice in Microsoft Teams. This might require additional subscriptions.

In the example above, the checkbox is asking whether I want to configure a Cloud voice in Microsoft Teams. As it may require additional subscriptions, I'm going to skip that stage for now and click next to move on to the next step which is Prepare for Microsoft Teams.

At this stage, there are two outstanding actions, around network planner (to assess the network performance of the organization) and also to look at the Team's advisor (which carries out the assessment of the Microsoft 365). These two actions are also available within Microsoft Teams and can be actioned from the Microsoft Teams admin center, but from this Admin Centre, we have a quicker way to roll out Microsoft Teams.



Prepare for Microsoft Teams

We recommend that you review the **Prerequisites** first and then review the **Network Planner** to ensure that your organization has the capacity to run Teams. If you're a large enterprise, use the **Teams advisor** instead, which is an all-encompassing planner-based deployment experience.

NOTE: If you haven't connected your domain, added users, or assigned licenses, complete the Prepare your environment guide first.

Prerequisites

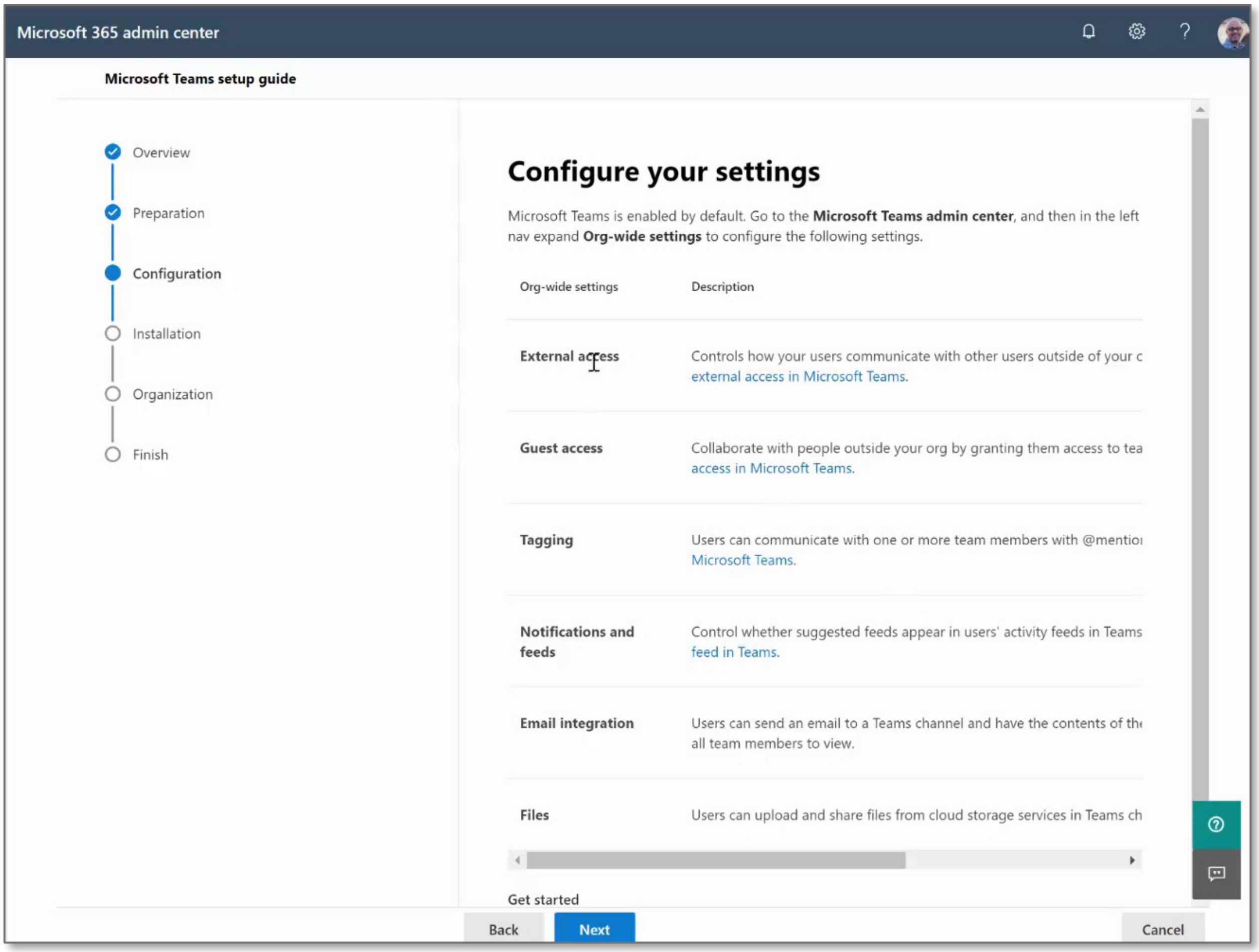
Network Planner

Network Planner is a tool in the Teams admin center that helps you determine and organize network requirements for connecting Microsoft Teams users across your org. For example, if your org runs their unified communication on-premises, this can help you determine the impact of Microsoft Teams on your Internet bandwidth. Learn more about Use the Network Planner for Microsoft Teams.

Teams advisor

The Teams advisor assesses your Office 365 tenant environment and identifies the most common configurations that you might need to update or modify before you can successfully roll out Teams. Then, it creates a Deployment team (in Teams), with channels for each workload you want to roll out. Each workload includes the rollout tasks with all the guidance and resources needed to complete them. Learn more about Use Advisor for Teams to help you roll out Microsoft Teams.

The next stage provides options around external access, guest access, tagging, notifications, and email integration.



Configure your settings

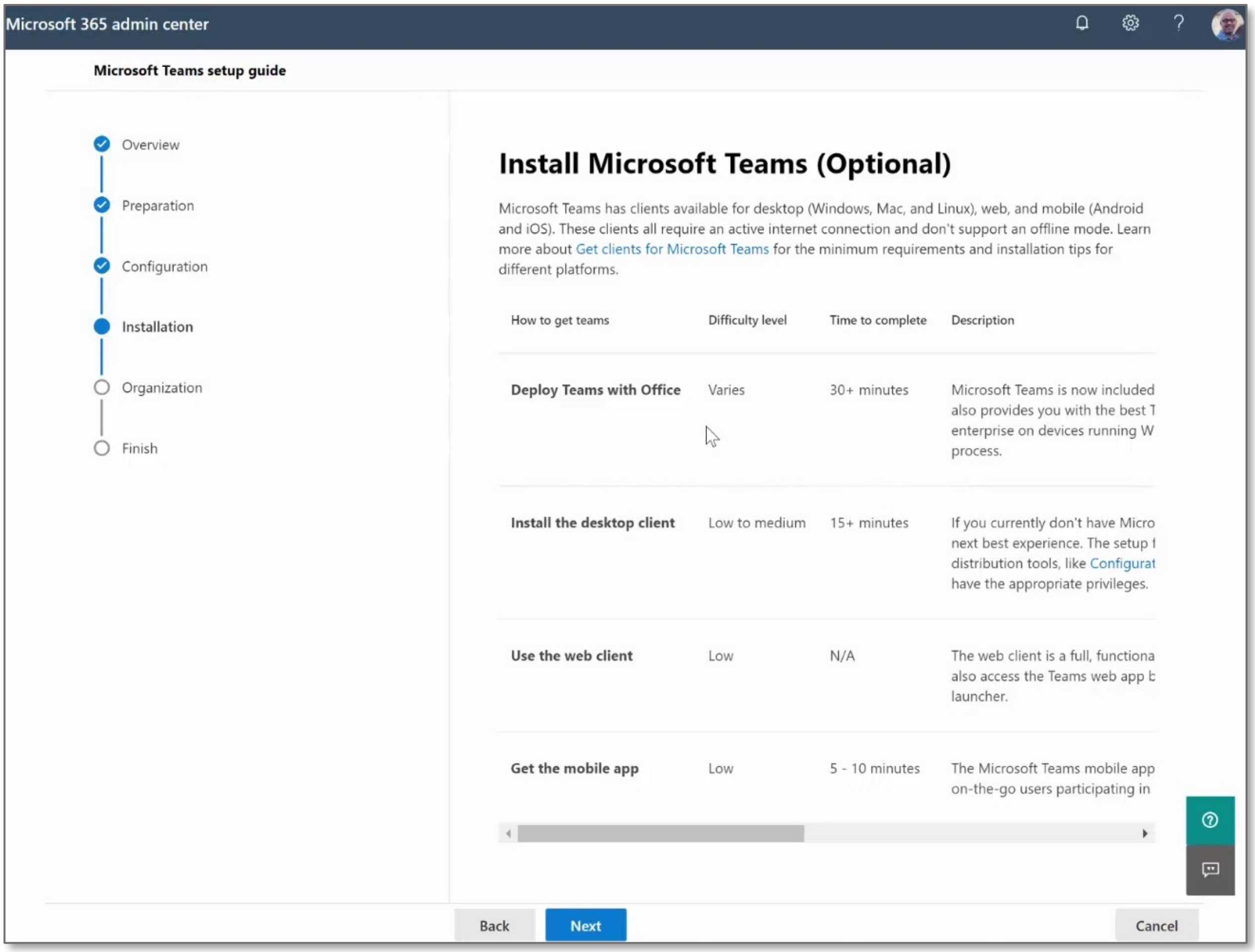
Microsoft Teams is enabled by default. Go to the **Microsoft Teams admin center**, and then in the left nav expand **Org-wide settings** to configure the following settings.

Org-wide settings	Description
External access	Controls how your users communicate with other users outside of your c external access in Microsoft Teams.
Guest access	Collaborate with people outside your org by granting them access to tea access in Microsoft Teams.
Tagging	Users can communicate with one or more team members with @mentioi Microsoft Teams.
Notifications and feeds	Control whether suggested feeds appear in users' activity feeds in Teams feed in Teams.
Email integration	Users can send an email to a Teams channel and have the contents of the all team members to view.
Files	Users can upload and share files from cloud storage services in Teams ch

Get started

These options can be set in the Microsoft Teams admin center.

Clicking “Next” takes us to the Installation screen where you have options to install into the desktop client, web client, etc.



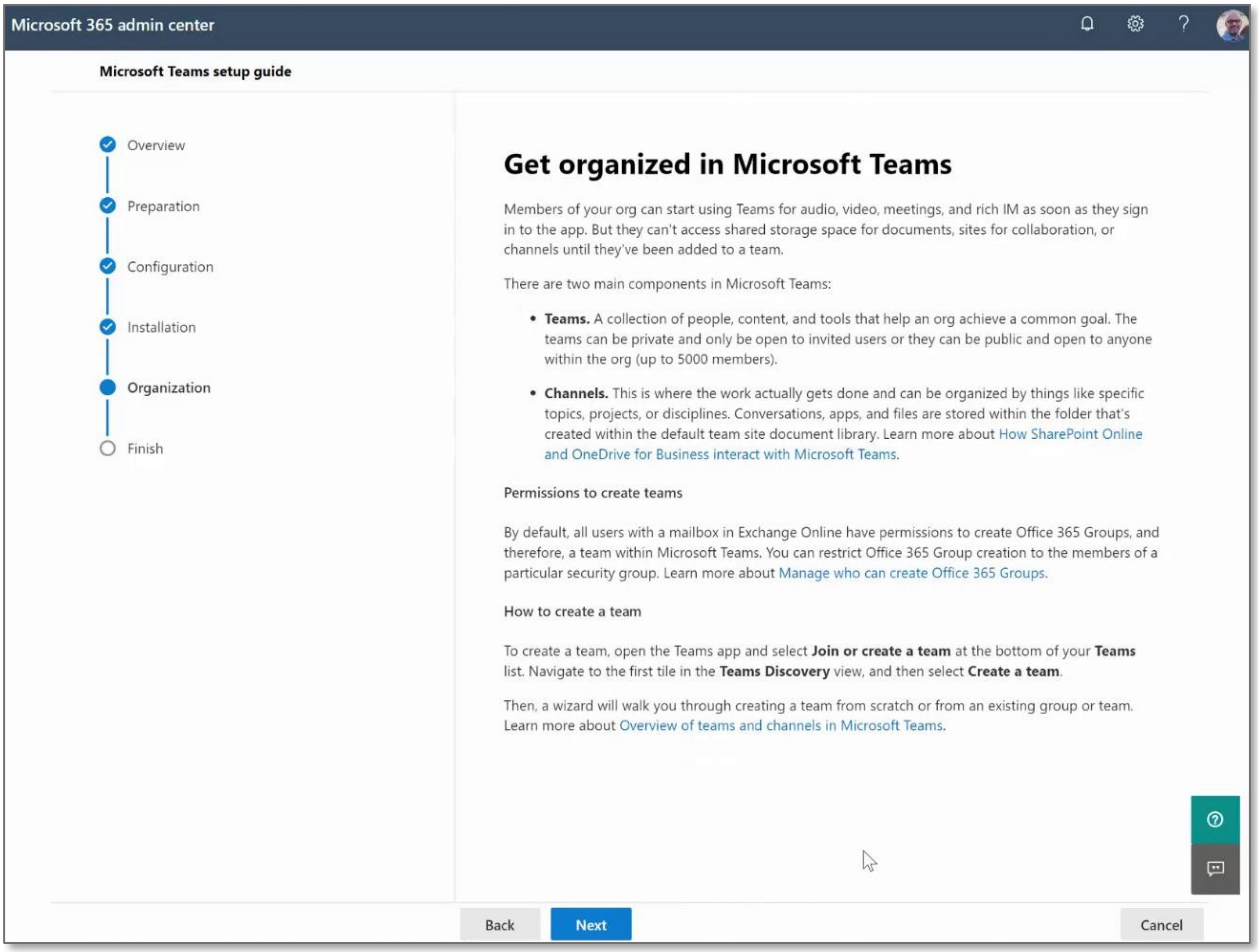
Install Microsoft Teams (Optional)

Microsoft Teams has clients available for desktop (Windows, Mac, and Linux), web, and mobile (Android and iOS). These clients all require an active internet connection and don't support an offline mode. Learn more about Get clients for Microsoft Teams for the minimum requirements and installation tips for different platforms.

How to get teams	Difficulty level	Time to complete	Description
Deploy Teams with Office	Varies	30+ minutes	Microsoft Teams is now included also provides you with the best T enterprise on devices running W process.
Install the desktop client	Low to medium	15+ minutes	If you currently don't have Micro next best experience. The setup f distribution tools, like Configurat have the appropriate privileges.
Use the web client	Low	N/A	The web client is a full, functiona also access the Teams web app b launcher.
Get the mobile app	Low	5 - 10 minutes	The Microsoft Teams mobile app on-the-go users participating in

The Next page tells me that once I finish this wizard, it's going to go and create the Microsoft Teams chat workspace using the settings specified earlier in this Setup.

The setup guide has, therefore, helped you create the plan to configure your instance of Teams.



Get organized in Microsoft Teams

Members of your org can start using Teams for audio, video, meetings, and rich IM as soon as they sign in to the app. But they can't access shared storage space for documents, sites for collaboration, or channels until they've been added to a team.

There are two main components in Microsoft Teams:

- **Teams.** A collection of people, content, and tools that help an org achieve a common goal. The teams can be private and only be open to invited users or they can be public and open to anyone within the org (up to 5000 members).
- **Channels.** This is where the work actually gets done and can be organized by things like specific topics, projects, or disciplines. Conversations, apps, and files are stored within the folder that's created within the default team site document library. Learn more about How SharePoint Online and OneDrive for Business interact with Microsoft Teams.

Permissions to create teams

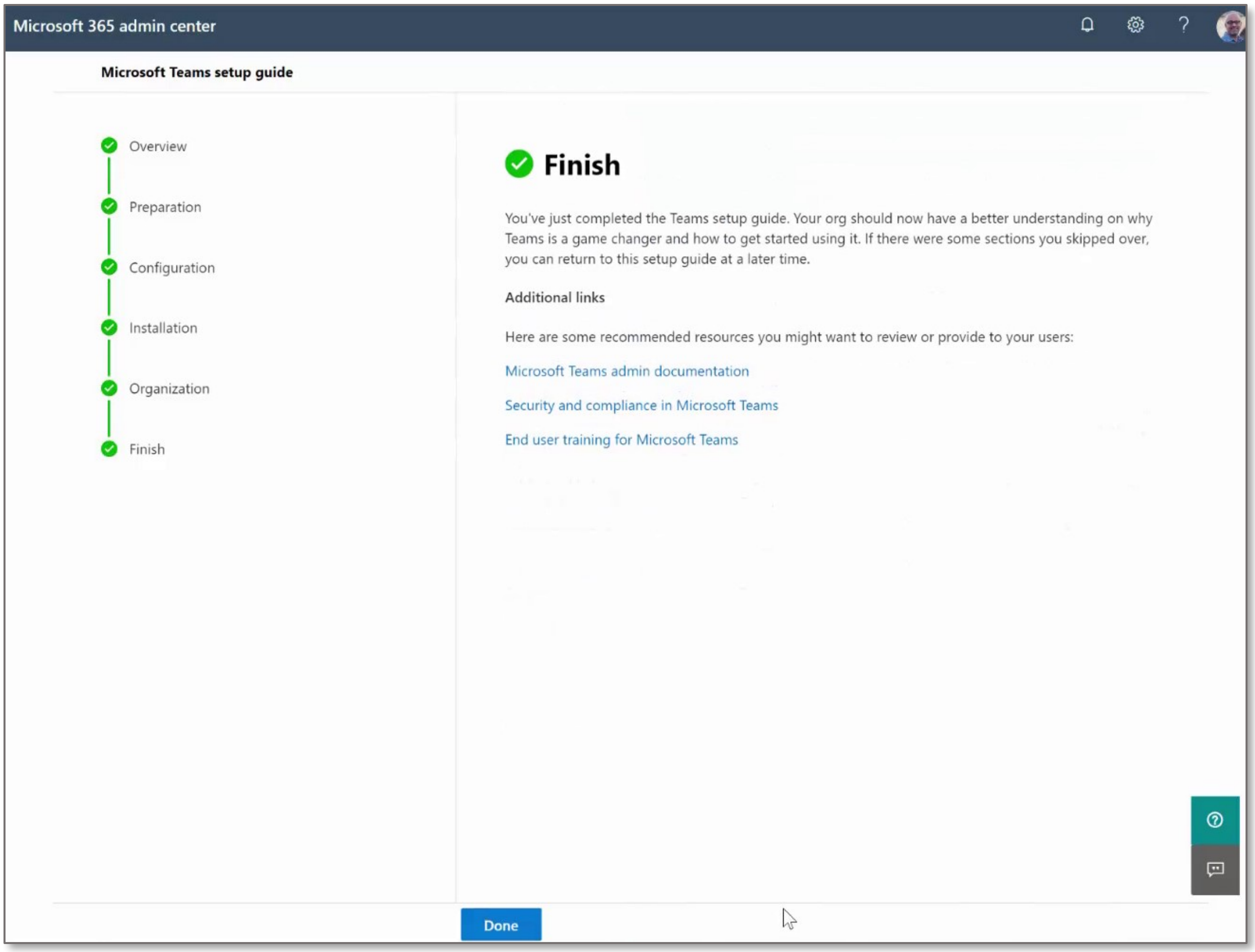
By default, all users with a mailbox in Exchange Online have permissions to create Office 365 Groups, and therefore, a team within Microsoft Teams. You can restrict Office 365 Group creation to the members of a particular security group. Learn more about Manage who can create Office 365 Groups.

How to create a team

To create a team, open the Teams app and select **Join or create a team** at the bottom of your **Teams** list. Navigate to the first tile in the **Teams Discovery** view, and then select **Create a team**.

Then, a wizard will walk you through creating a team from scratch or from an existing group or team. Learn more about Overview of teams and channels in Microsoft Teams.

Click next to arrive at the final screen, which includes additional documents to review for other configuration details.



Finish

You've just completed the Teams setup guide. Your org should now have a better understanding on why Teams is a game changer and how to get started using it. If there were some sections you skipped over, you can return to this setup guide at a later time.

Additional links

Here are some recommended resources you might want to review or provide to your users:

Microsoft Teams admin documentation

Security and compliance in Microsoft Teams

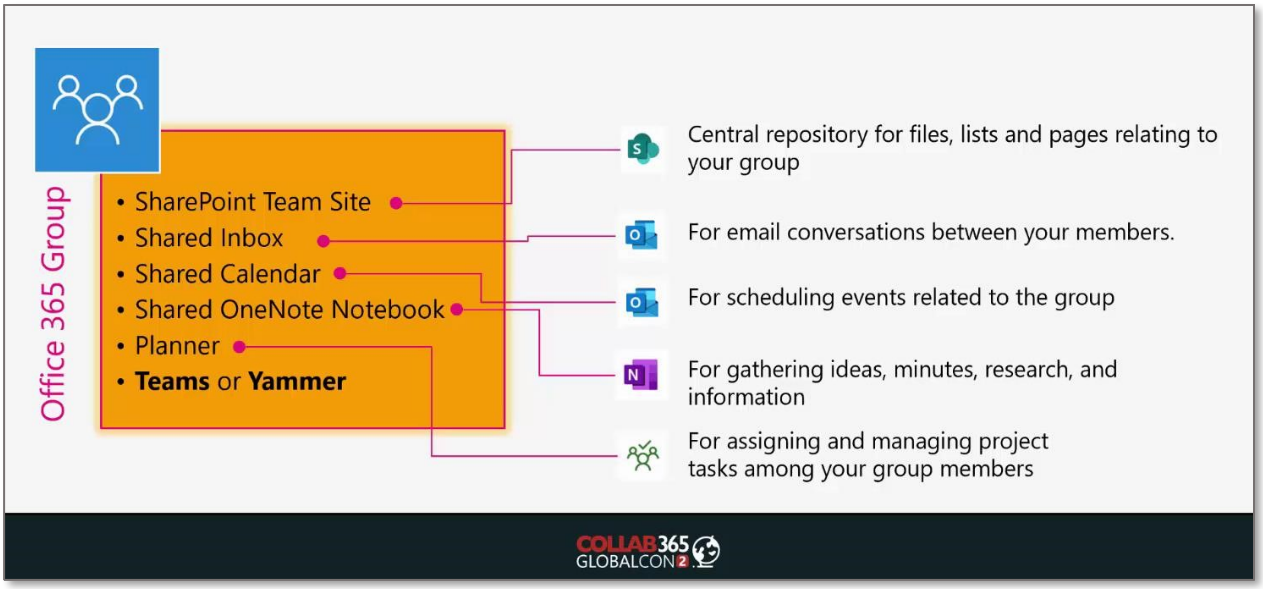
End user training for Microsoft Teams

Click done to roll out the service as per your settings and configuration choices.

A similar process can be followed for other rollouts and updates.

Managing Microsoft 365 Groups

The next step is around understanding Microsoft 365 groups. They were formally called Office 365 groups and were recently renamed, but they mean the same thing. Essentially with every Office 365 group, you get a SharePoint Team site, Exchange Inbox, Shared Calendar, OneNote, as well as being able to use Planner, create Microsoft Teams, or Yammer.



Office 365 Group

- SharePoint Team Site
- Shared Inbox
- Shared Calendar
- Shared OneNote Notebook
- Planner
- **Teams** or **Yammer**

Central repository for files, lists and pages relating to your group

For email conversations between your members.

For scheduling events related to the group

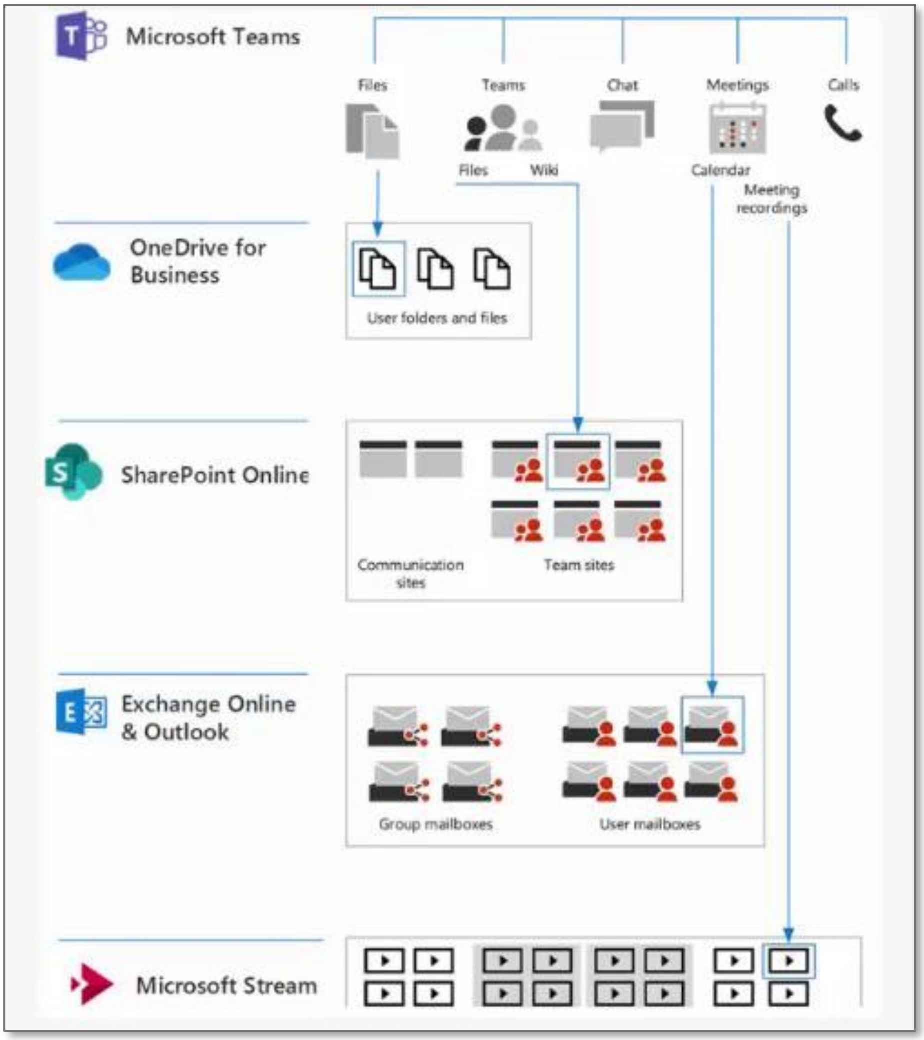
For gathering ideas, minutes, research, and information

For assigning and managing project tasks among your group members

A lot of the services in Microsoft 365, as well as some of the online third party connectors, make use of Microsoft 365 groups.

Users may ask, “Why would I use SharePoint when I can use Teams to access files and OneDrive.” There may be instances within your environment where you want to create a SharePoint team site, but not associate Microsoft Teams with it. An example is for document management, where you want to deploy SharePoint sites purely from a document management perspective and leave the collaboration aspect of chat and communication separately, or maybe in another chat workspace altogether.

The platform components of Microsoft 365, that Microsoft Teams depends on are shown in the diagram below.



- Files and chat files reside in a user's (the person who shared their files) OneDrive. OneDrive should be used for private or personal purposes when you want to collaborate with just a few specific people.
- Files from a Team chat workspace reside within SharePoint Online. A SharePoint, based, Microsoft teams chat space is a better place to keep the workload of a larger team in SharePoint.
- Meeting recordings reside in Microsoft Stream.
- Group-wide conversations can only currently be held within a specific channel inside Microsoft Teams. You can use the General channel as well as an outlook

group to allow your emails to go to the entire group without having to use the channels inside Microsoft Teams.

Channels in Microsoft Teams are separate and different to the channels inside Microsoft Stream. Channels in Microsoft Stream allow you to group videos around a particular topic for that specific team.

Teams created in Microsoft teams will also appear in Microsoft Stream.

Tools to manage Microsoft 365 Groups

The first step is to create a dedicated group of security members who can actually create Microsoft 365 Groups.

The next decision is to consider creating a naming convention, to set rules on display name or aliases depending on what team chat workspaces you create. You may also want to extend this to include names for documents, contracts, as well as projects, so you have a consistent approach across the whole group configuration.

If you go into Azure AD, you can manage group settings as well as being able to set expiry dates. Without expiry dates, your Microsoft 365 groups will exist indefinitely, and the list will keep on growing. When users search for specific groups, they'll just be overwhelmed by the sheer number of groups that you have. Groups can be restored if they get deleted by accident.

A big part of Microsoft 365 groups is to be able to manage and understand the dependencies between various online services that you have and being able to report the total number of groups you have.

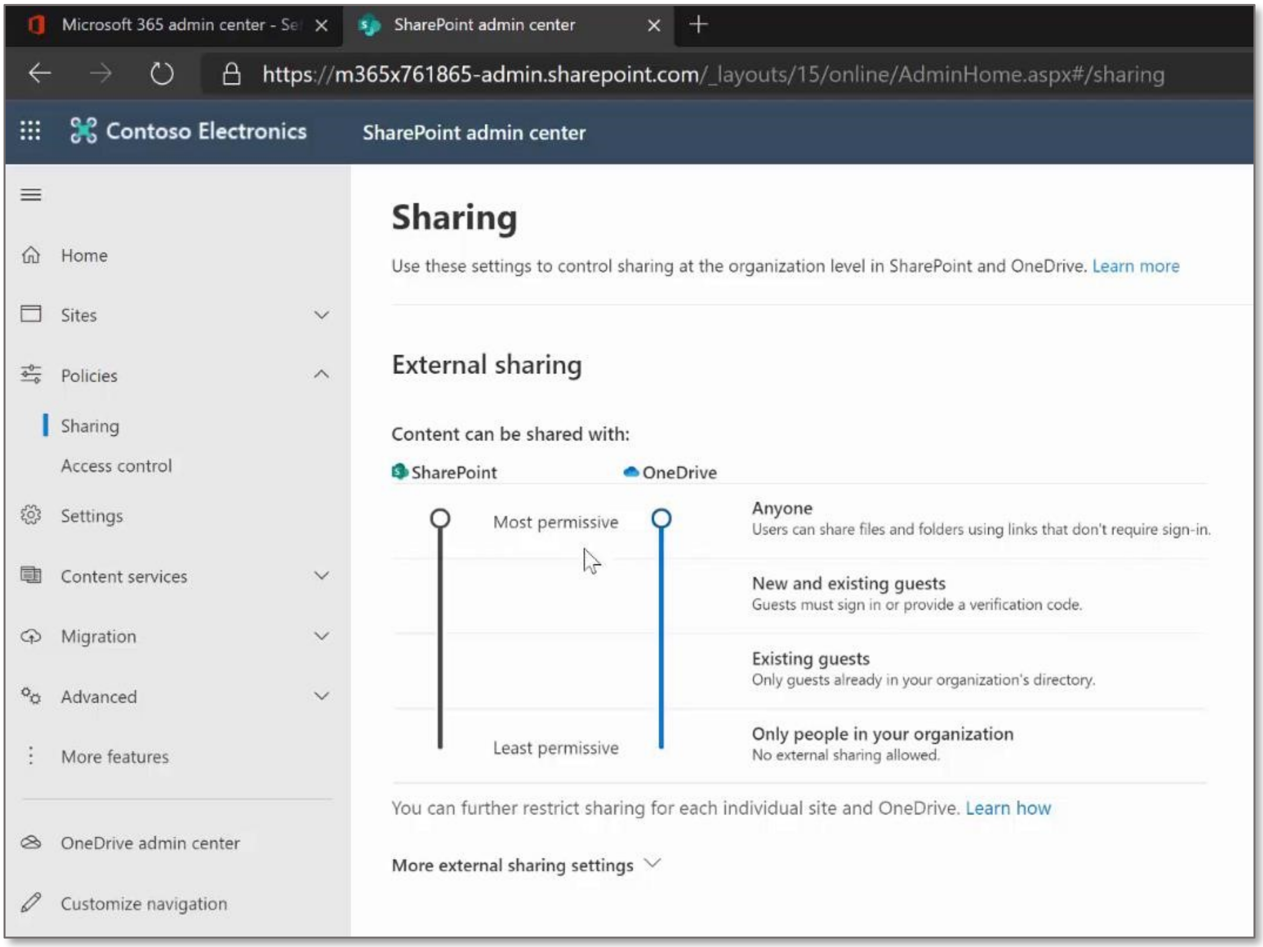
External Sharing and Guest Access

The next step is effectively managing your external sharing and guest access.

Microsoft Teams also has an area to control the guest access, which, by default, is disabled.

SharePoint has an external sharing model where you can control SharePoint all the way down to individual SharePoint sites, as well as OneDrive. So let's take a look at that in slightly more detail.

In the SharePoint admin center, from the left-hand options, go to policies and then sharing. The default position is to allow anyone to access your environment.



Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive. Learn more

External sharing

Content can be shared with:

SharePoint OneDrive

Most permissive

Least permissive

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. Learn how

More external sharing settings

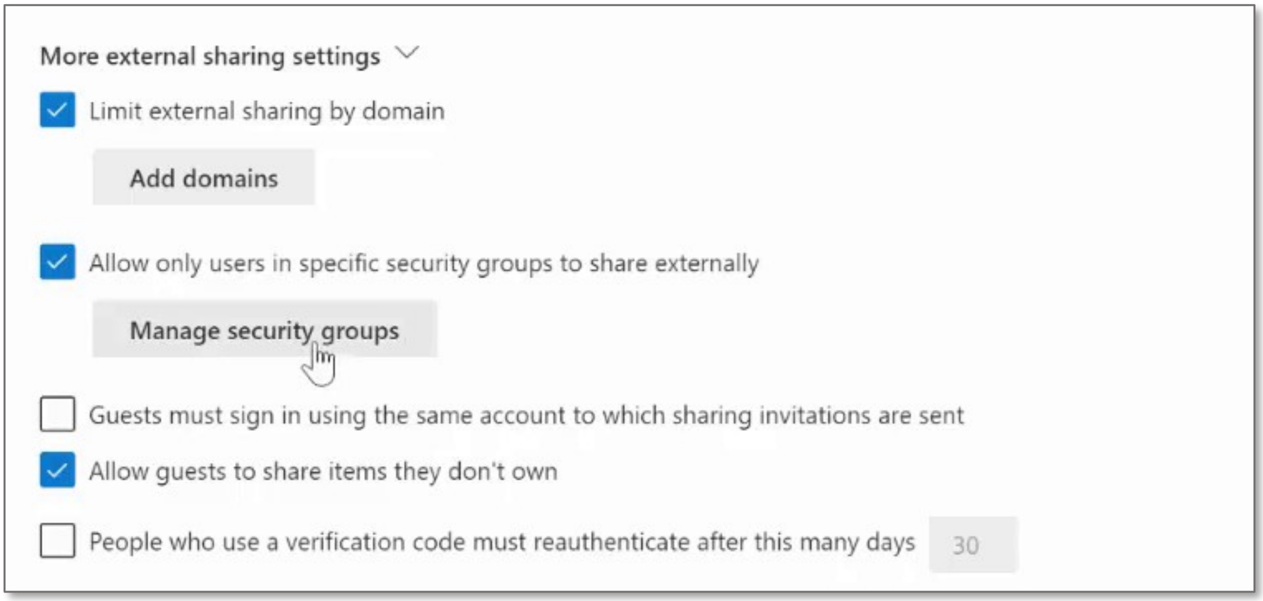
The sliders for both OneDrive and SharePoint can be moved up or down the scales to decide whether content can be shared with:

- Anyone,

- New & Existing Guests,
- Existing Guests or
- Only people within your organization

Move the slider button to select the required level. You will notice that changes made to the sharing configuration for SharePoint are also reflected in OneDrive. You can make further restrictions in OneDrive, and make OneDrive only available for existing guests, but you can't set OneDrive to be more permissive than SharePoint.

More external sharing settings are available further down the screen. It's possible to limit sharing by domain and also for specific security groups, so not everybody has got that right to share.



More external sharing settings

☑ Limit external sharing by domain

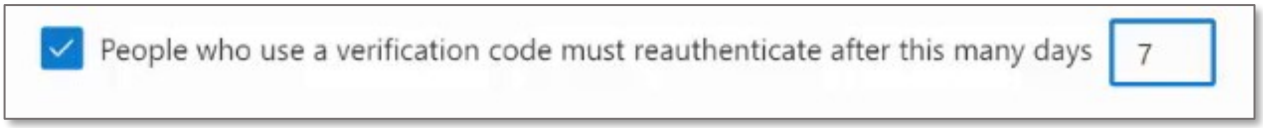
☑ Allow only users in specific security groups to share externally

□ Guests must sign in using the same account to which sharing invitations are sent

☑ Allow guests to share items they don't own

□ People who use a verification code must reauthenticate after this many days 30

A handy option is the requirement to get users reauthenticate after a set number of days. So if they haven't used the system or accessed the tenant at all, then it will require them to reauthenticate to access information.



☑ People who use a verification code must reauthenticate after this many days 7

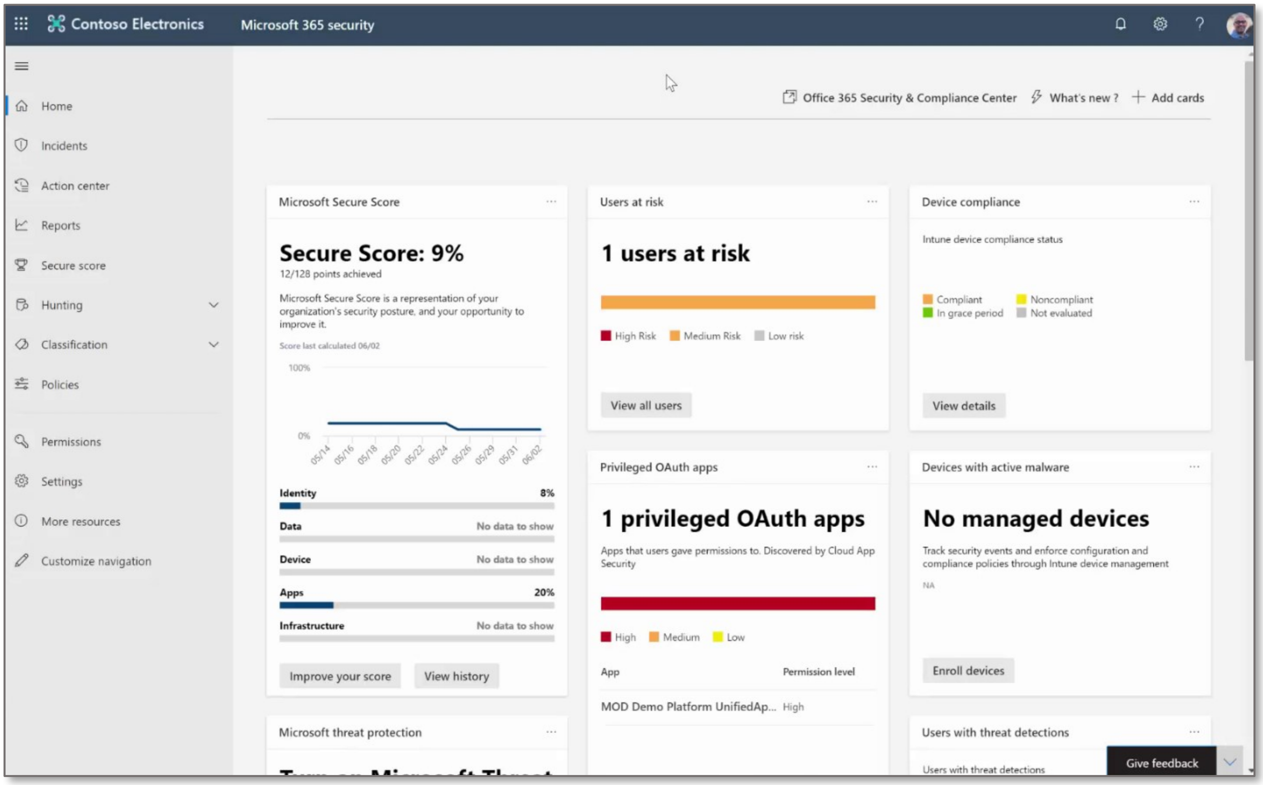
Remember to save your chosen settings before moving on.

Microsoft 365 Security & Compliance

The sixth step you have is managing the security and compliance position of your Microsoft 365 environment. This covers all of your workloads in there, not just Microsoft Teams. When you look at the Secure score, essentially you are assessed based on what configurations you've enabled, to meet those particular set of requirements, as well the security and compliance elements that are incorporated from Microsoft.

The idea here is not to get the maximum score, but get a high enough score to make sure that your information and devices are well protected. So let's take a look at that.

Security centre admin



Microsoft Secure Score

Secure Score: 9%

12/128 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last calculated 06/02

Identity	8%
Data	No data to show
Device	No data to show
Apps	20%
Infrastructure	No data to show

Microsoft threat protection

Turn on Microsoft Threat

Users at risk

1 users at risk

Device compliance

Intune device compliance status

Privileged OAuth apps

1 privileged OAuth apps

Apps that users gave permissions to. Discovered by Cloud App Security

App	Permission level
MOD Demo Platform UnifiedAp...	High

Devices with active malware

No managed devices

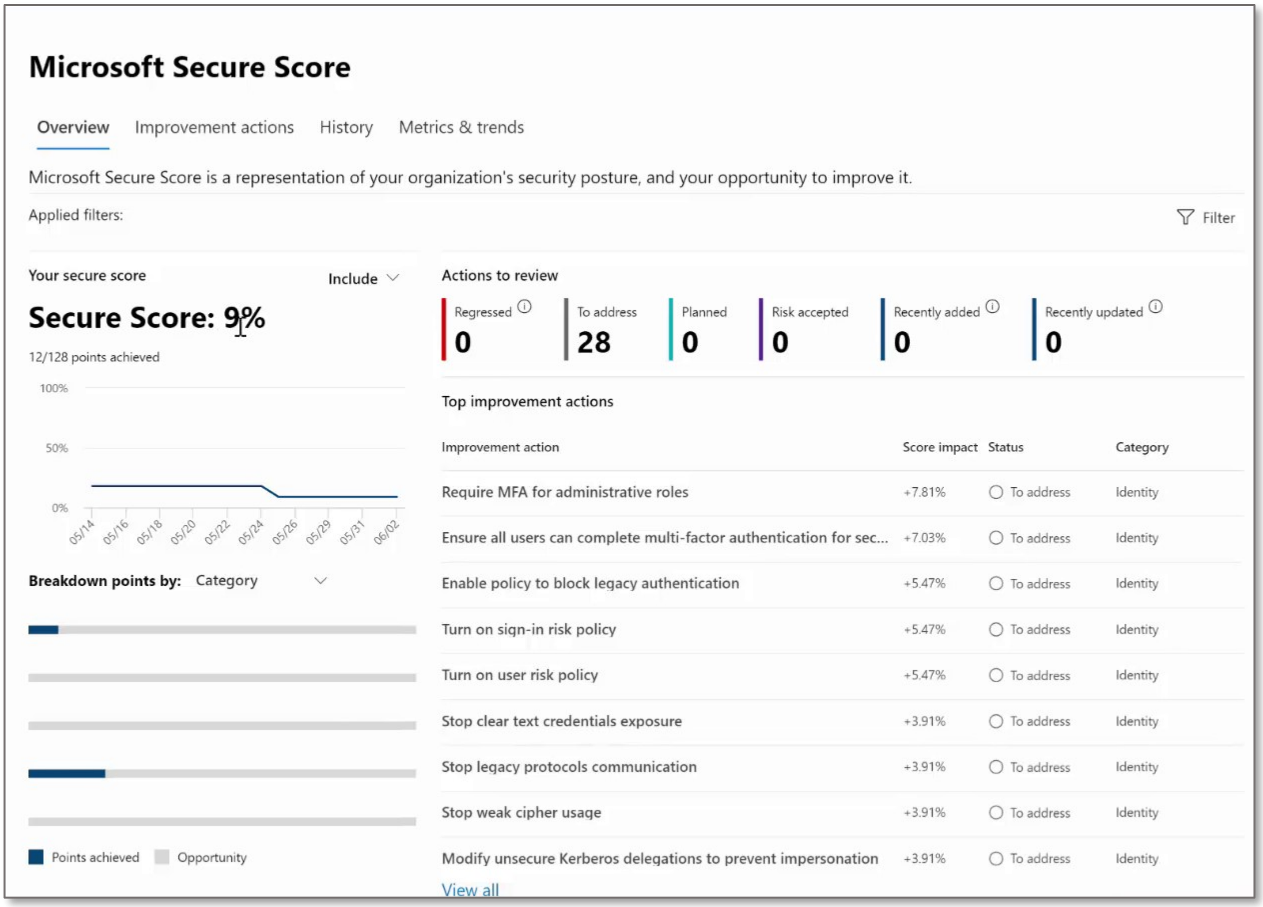
Track security events and enforce configuration and compliance policies through Intune device management

NA

Users with threat detections

Users with threat detections

You can see that in this example, there is a 9% secure score, which is very low. Only 12 out of 128 points have been achieved. You can click to reveal more detail.



Microsoft Secure Score

Overview | Improvement actions | History | Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Filter

Your secure score

Include

Secure Score: 9%

12/128 points achieved

Breakdown points by: Category

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
0	28	0	0	0	0

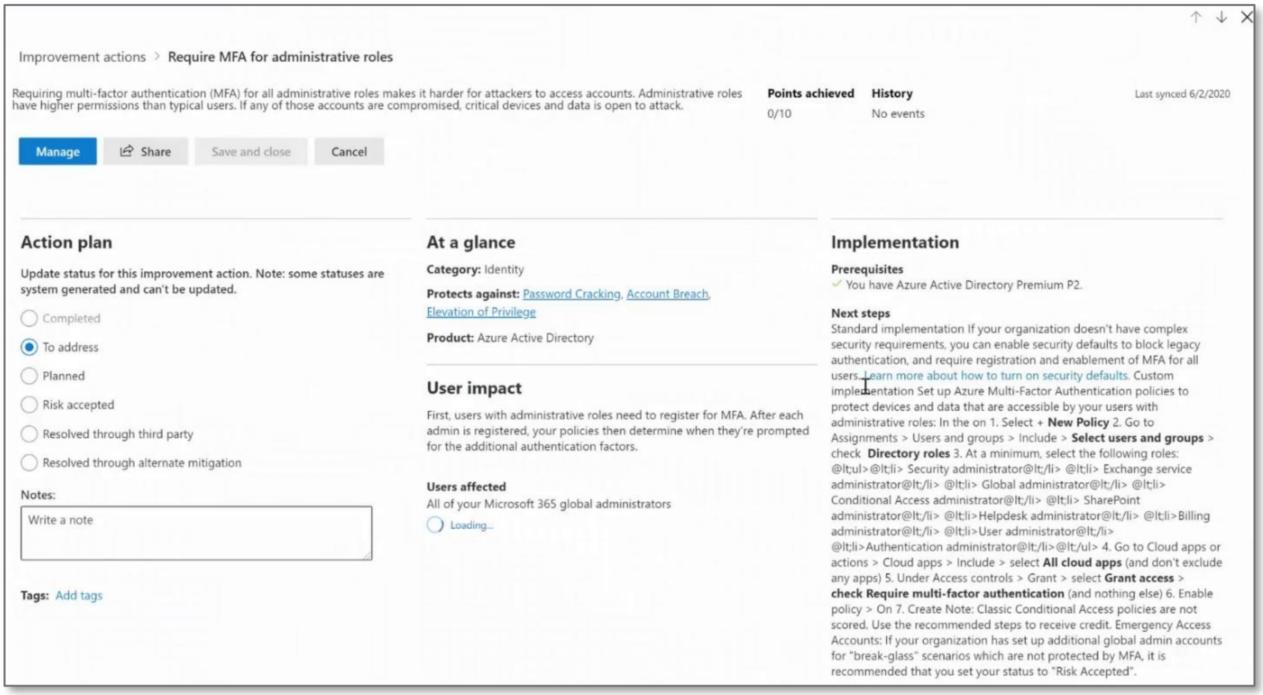
Top improvement actions

Improvement action	Score impact	Status	Category
Require MFA for administrative roles	+7.81%	○ To address	Identity
Ensure all users can complete multi-factor authentication for sec...	+7.03%	○ To address	Identity
Enable policy to block legacy authentication	+5.47%	○ To address	Identity
Turn on sign-in risk policy	+5.47%	○ To address	Identity
Turn on user risk policy	+5.47%	○ To address	Identity
Stop clear text credentials exposure	+3.91%	○ To address	Identity
Stop legacy protocols communication	+3.91%	○ To address	Identity
Stop weak cipher usage	+3.91%	○ To address	Identity
Modify unsecure Kerberos delegations to prevent impersonation	+3.91%	○ To address	Identity

View all

Improvement actions are suggested and also provide a score impact, so you can know how much your secure score will improve by following the recommendations.

Clicking on each improvement action will drill down into further detail.



Improvement actions > **Require MFA for administrative roles**

Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data is open to attack.

Points achieved 0/10

History No events

Last synced 6/2/2020

Action plan

Update status for this improvement action. Note: some statuses are system generated and can't be updated.

○ Completed
● To address
○ Planned
○ Risk accepted
○ Resolved through third party
○ Resolved through alternate mitigation

Notes:

Write a note

Tags: Add tags

At a glance

Category: Identity

Protects against: Password Cracking, Account Breach, Elevation of Privilege

Product: Azure Active Directory

User impact

First, users with administrative roles need to register for MFA. After each admin is registered, your policies then determine when they're prompted for the additional authentication factors.

Users affected

All of your Microsoft 365 global administrators

Loading...

Implementation

Prerequisites

✓ You have Azure Active Directory Premium P2.

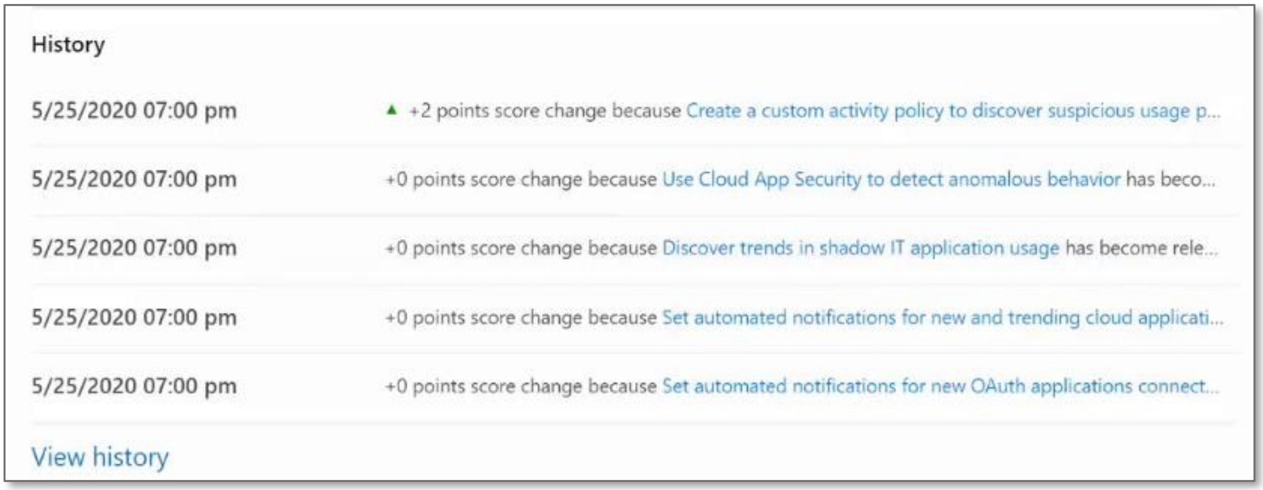
Next steps

Standard implementation If your organization doesn't have complex security requirements, you can enable security defaults to block legacy authentication, and require registration and enablement of MFA for all users. Learn more about how to turn on security defaults. Custom implementation Set up Azure Multi-Factor Authentication policies to protect devices and data that are accessible by your users with administrative roles: In the on 1. Select + **New Policy** 2. Go to Assignments > Users and groups > Include > **Select users and groups** > check **Directory roles** 3. At a minimum, select the following roles: @lt;ul>@lt;li> Security administrator@lt;/li> @lt;li> Exchange service administrator@lt;/li> @lt;li> Global administrator@lt;/li> @lt;li> Conditional Access administrator@lt;/li> @lt;li> SharePoint administrator@lt;/li> @lt;li>Helpdesk administrator@lt;/li> @lt;li>Billing administrator@lt;/li> @lt;li>User administrator@lt;/li> @lt;li>Authentication administrator@lt;/li>@lt;/ul> 4. Go to Cloud apps or actions > Cloud apps > Include > select **All cloud apps** (and don't exclude any apps) 5. Under Access controls > Grant > select **Grant access** > **check Require multi-factor authentication** (and nothing else) 6. Enable policy > On 7. Create Note: Classic Conditional Access policies are not scored. Use the recommended steps to receive credit. Emergency Access Accounts: If your organization has set up additional global admin accounts for "break-glass" scenarios which are not protected by MFA, it is recommended that you set your status to "Risk Accepted".

In the Action Plan section, you can set the radio button to accept the risk, leave it to address in the future, plan to take the recommended action or resolve through either a third party or alternative mitigation, leaving a note to explain your decision.

The "At a glance" section explains what kind of impact it has, and the Implementation section explains the next steps and provides detailed guidance around how to proceed.

Further down the screen, you can see the history of changes made to this setting and their impact on the overall score.

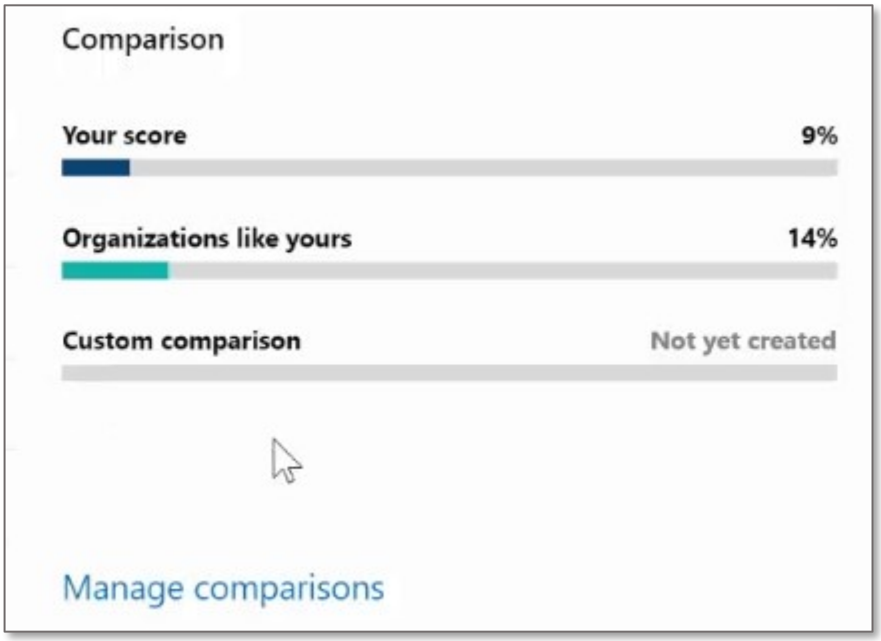


History

5/25/2020 07:00 pm	▲ +2 points score change because Create a custom activity policy to discover suspicious usage p...
5/25/2020 07:00 pm	+0 points score change because Use Cloud App Security to detect anomalous behavior has beco...
5/25/2020 07:00 pm	+0 points score change because Discover trends in shadow IT application usage has become rele...
5/25/2020 07:00 pm	+0 points score change because Set automated notifications for new and trending cloud applicati...
5/25/2020 07:00 pm	+0 points score change because Set automated notifications for new OAuth applications connect...

View history

Also, comparisons to other organizations are provided, so you can review how your security settings compare to similar organizations.



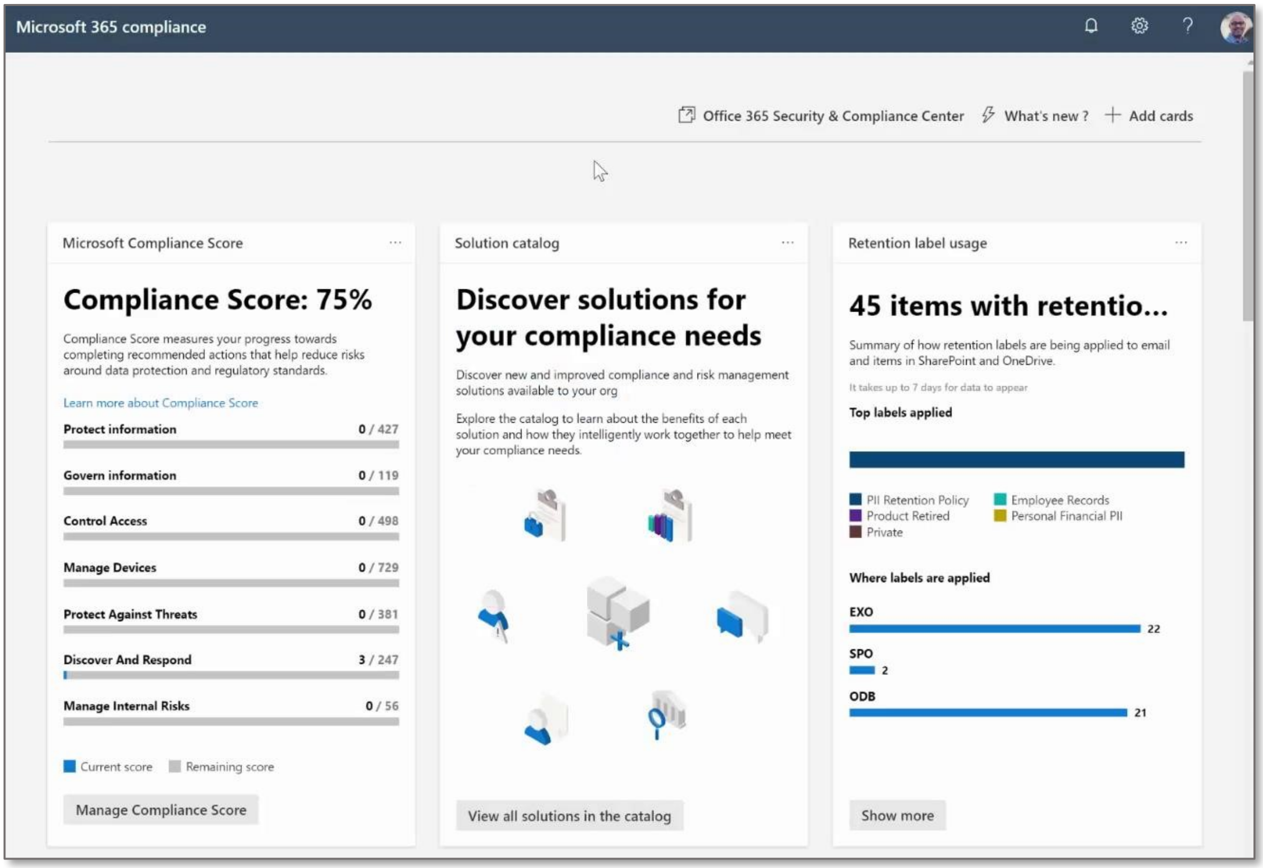
Comparison

Your score	9%
Organizations like yours	14%
Custom comparison	Not yet created

Manage comparisons

Compliance Admin

So the next aspect we want to look at is the compliance admin, which has a similar layout and provides an overall compliance score.



Microsoft 365 compliance

Office 365 Security & Compliance Center | What's new ? | + Add cards

Microsoft Compliance Score

Compliance Score: 75%

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Learn more about Compliance Score

Protect information	0 / 427
Govern information	0 / 119
Control Access	0 / 498
Manage Devices	0 / 729
Protect Against Threats	0 / 381
Discover And Respond	3 / 247
Manage Internal Risks	0 / 56

■ Current score ■ Remaining score

Manage Compliance Score

Solution catalog

Discover solutions for your compliance needs

Discover new and improved compliance and risk management solutions available to your org

Explore the catalog to learn about the benefits of each solution and how they intelligently work together to help meet your compliance needs.

View all solutions in the catalog

Retention label usage

45 items with retentio...

Summary of how retention labels are being applied to email and items in SharePoint and OneDrive.

It takes up to 7 days for data to appear

Top labels applied

■ PII Retention Policy ■ Employee Records
■ Product Retired ■ Personal Financial PII
■ Private

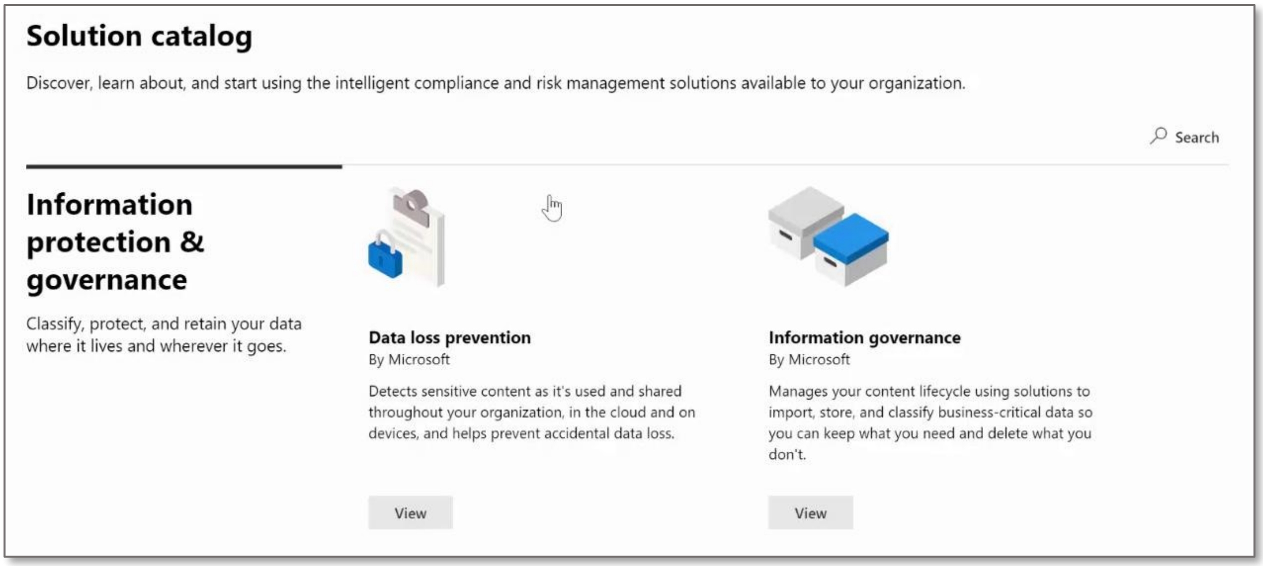
Where labels are applied

EXO	22
SPO	2
ODB	21

Show more

This provides the same sort of information around what actions can be taken to improve and increase the compliance score.

The section in the middle, “Solution catalog”, provides various sections to help with Information protection and guidance, Insider risk management, and Discovery and response.



Solution catalog

Discover, learn about, and start using the intelligent compliance and risk management solutions available to your organization.

Information protection & governance

Classify, protect, and retain your data where it lives and wherever it goes.

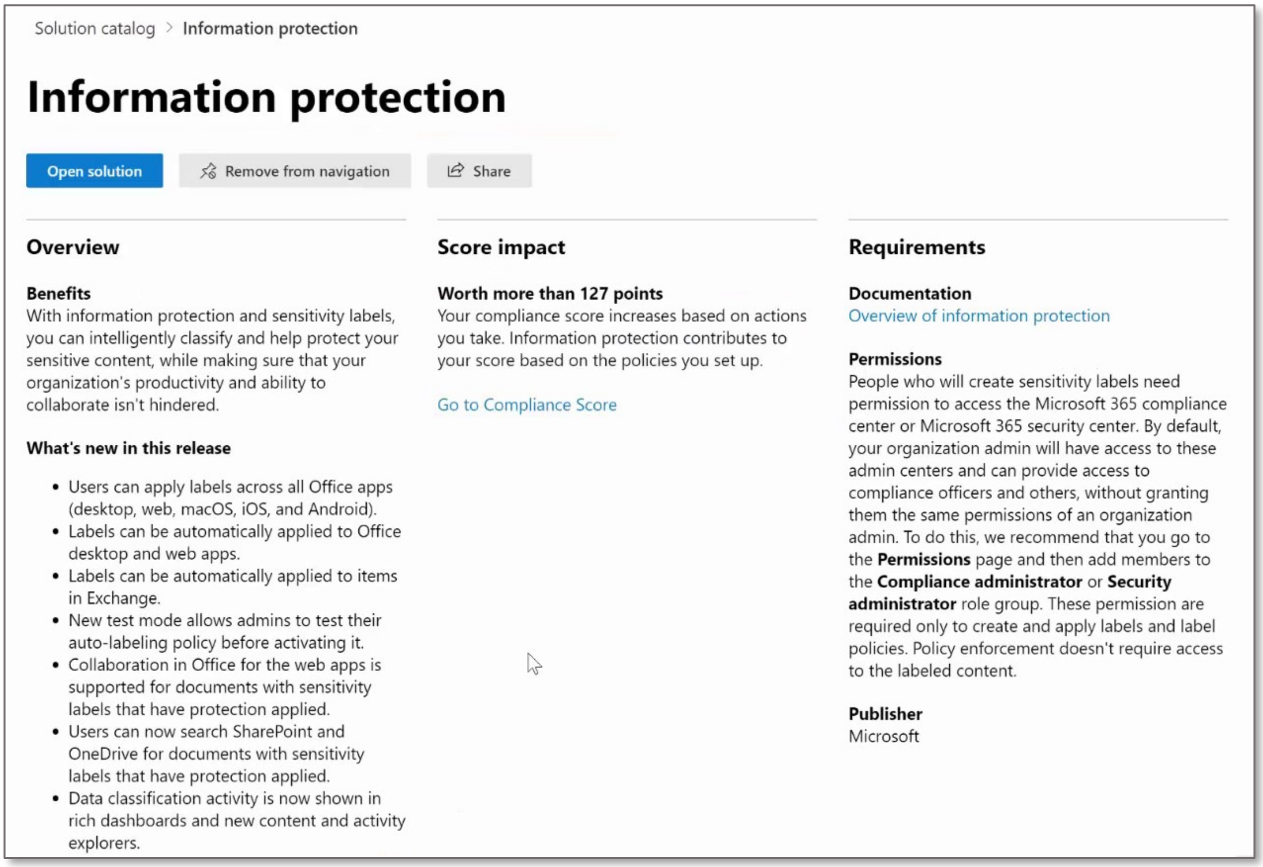
Data loss prevention
By Microsoft

Detects sensitive content as it's used and shared throughout your organization, in the cloud and on devices, and helps prevent accidental data loss.

Information governance
By Microsoft

Manages your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't.

Selecting "View" for the Information protection section takes you to more information as below.



Information protection

Overview

Benefits
With information protection and sensitivity labels, you can intelligently classify and help protect your sensitive content, while making sure that your organization's productivity and ability to collaborate isn't hindered.

What's new in this release

- Users can apply labels across all Office apps (desktop, web, macOS, iOS, and Android).
- Labels can be automatically applied to Office desktop and web apps.
- Labels can be automatically applied to items in Exchange.
- New test mode allows admins to test their auto-labeling policy before activating it.
- Collaboration in Office for the web apps is supported for documents with sensitivity labels that have protection applied.
- Users can now search SharePoint and OneDrive for documents with sensitivity labels that have protection applied.
- Data classification activity is now shown in rich dashboards and new content and activity explorers.

Score impact

Worth more than 127 points
Your compliance score increases based on actions you take. Information protection contributes to your score based on the policies you set up.

Go to Compliance Score

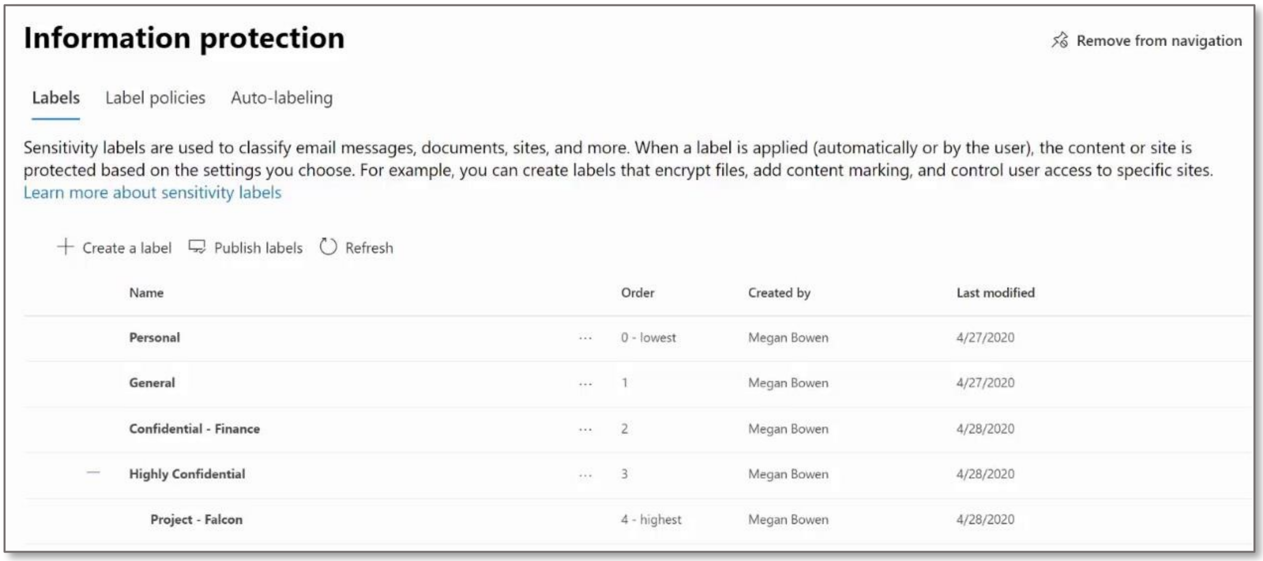
Requirements

Documentation
Overview of information protection

Permissions
People who will create sensitivity labels need permission to access the Microsoft 365 compliance center or Microsoft 365 security center. By default, your organization admin will have access to these admin centers and can provide access to compliance officers and others, without granting them the same permissions of an organization admin. To do this, we recommend that you go to the **Permissions** page and then add members to the **Compliance administrator** or **Security administrator** role group. These permission are required only to create and apply labels and label policies. Policy enforcement doesn't require access to the labeled content.

Publisher
Microsoft

This provides additional detail about what's in this particular release, additional steps you can take, and constantly gets updated as, and when new configuration elements get rolled out in Microsoft 365. This particular area of information protection could have an impact of 127 points, clicking "Open Solution" takes you straight into the information protection area (so saves you from trying to locate it from the menu structure.)

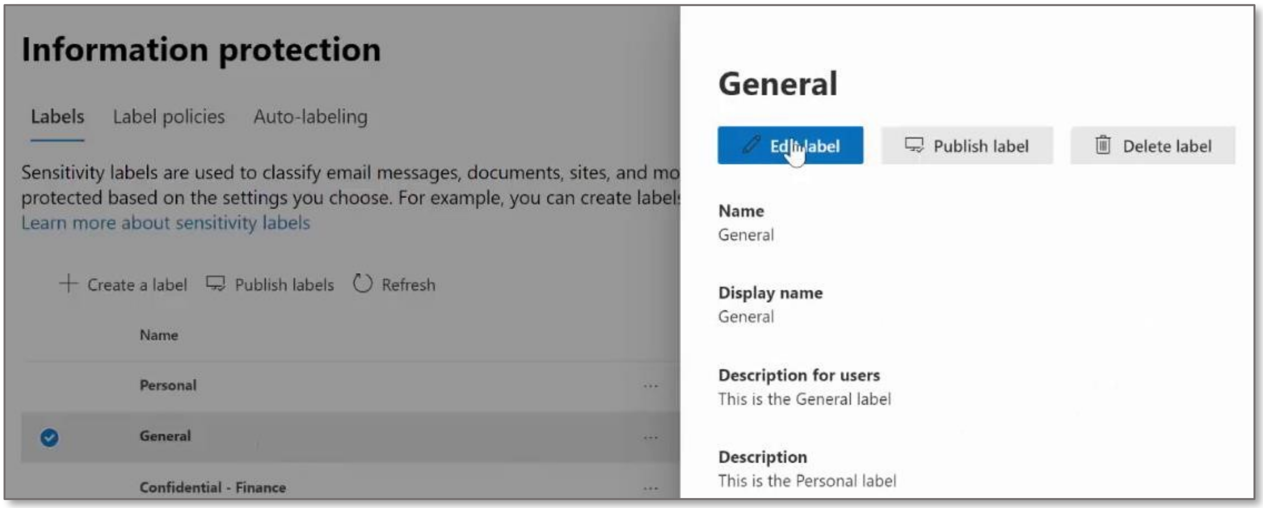


Information protection

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites.
Learn more about sensitivity labels

Name	Order	Created by	Last modified
Personal	0 - lowest	Megan Bowen	4/27/2020
General	1	Megan Bowen	4/27/2020
Confidential - Finance	2	Megan Bowen	4/28/2020
Highly Confidential	3	Megan Bowen	4/28/2020
Project - Falcon	4 - highest	Megan Bowen	4/28/2020

This shows that I currently have four labels, which can be used to classify messages, documents, sites, etc. Each one can be edited.



Information protection

Sensitivity labels are used to classify email messages, documents, sites, and mo
protected based on the settings you choose. For example, you can create label
Learn more about sensitivity labels

General

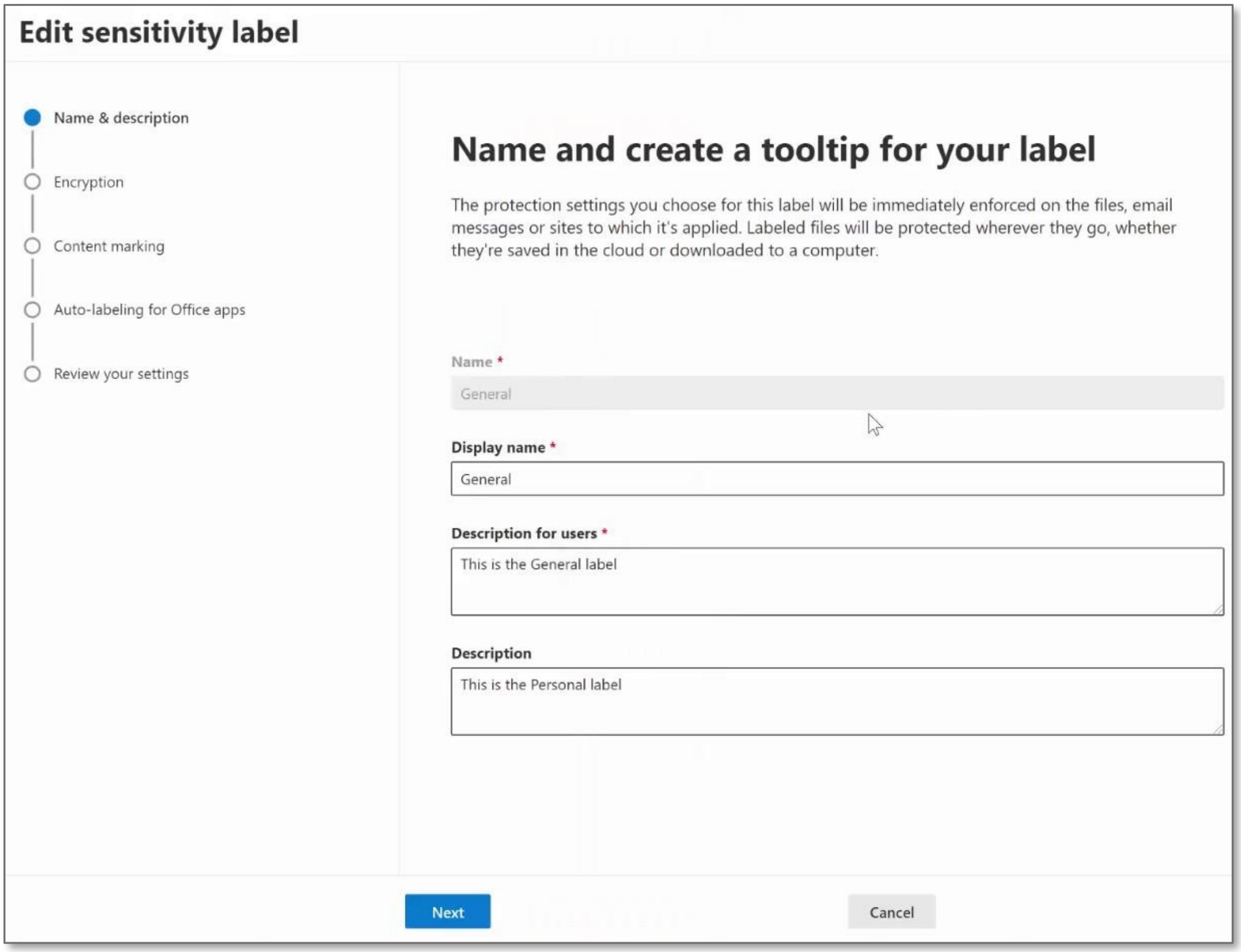
Name
General

Display name
General

Description for users
This is the General label

Description
This is the Personal label

You can amend the display name and descriptions.



Edit sensitivity label

Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced on the files, email messages or sites to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

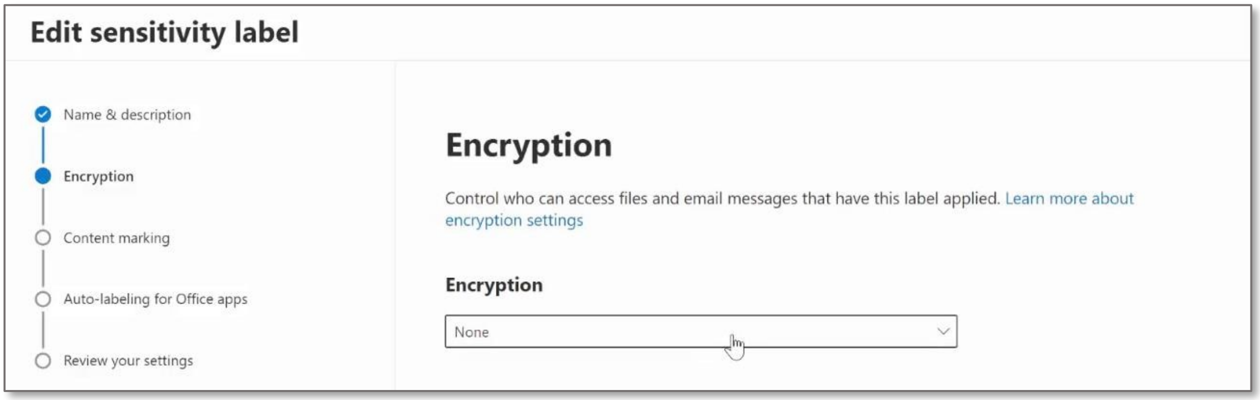
Name *
General

Display name *
General

Description for users *
This is the General label

Description
This is the Personal label

You can also set encryption options.



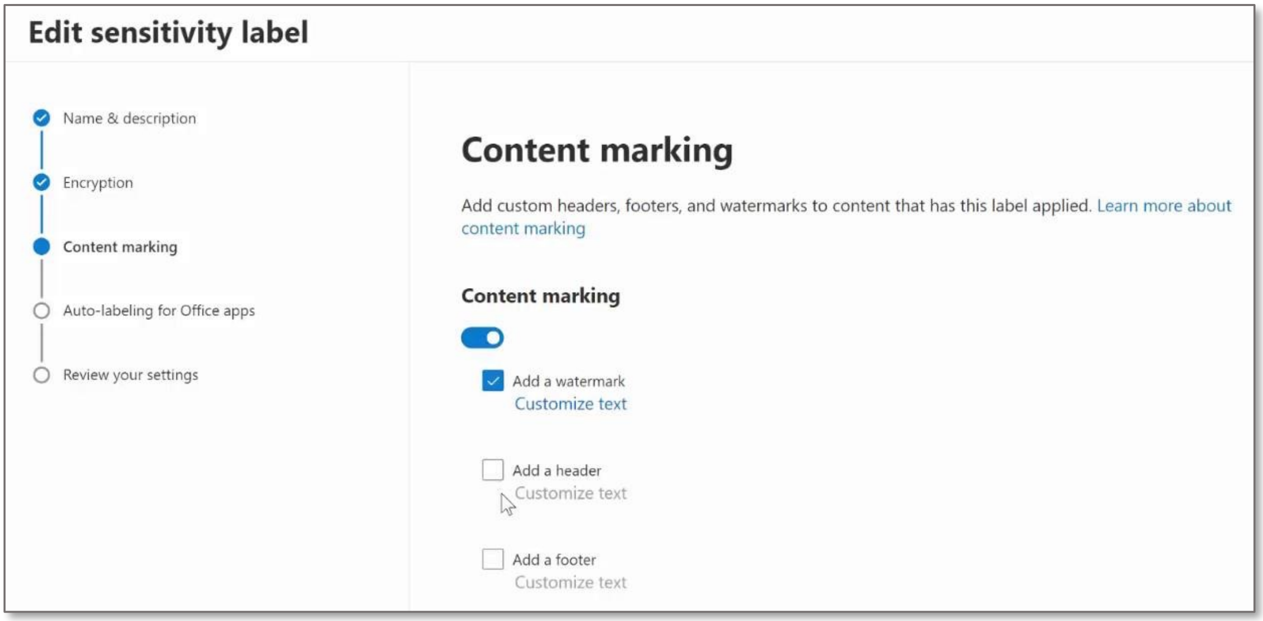
Edit sensitivity label

Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

Encryption
None

Content marking items can also be added.



Edit sensitivity label

- ✓ Name & description
- ✓ Encryption
- ● Content marking
- ○ Auto-labeling for Office apps
- ○ Review your settings

Content marking

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

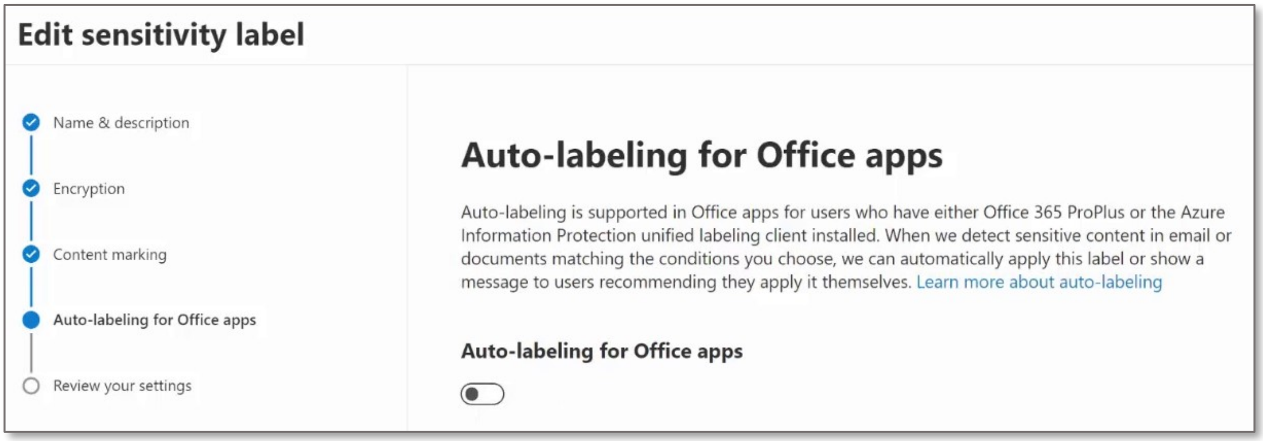
Content marking

☑ Add a watermark
Customize text

□ Add a header
Customize text

□ Add a footer
Customize text

Auto labeling options are also available.



Edit sensitivity label

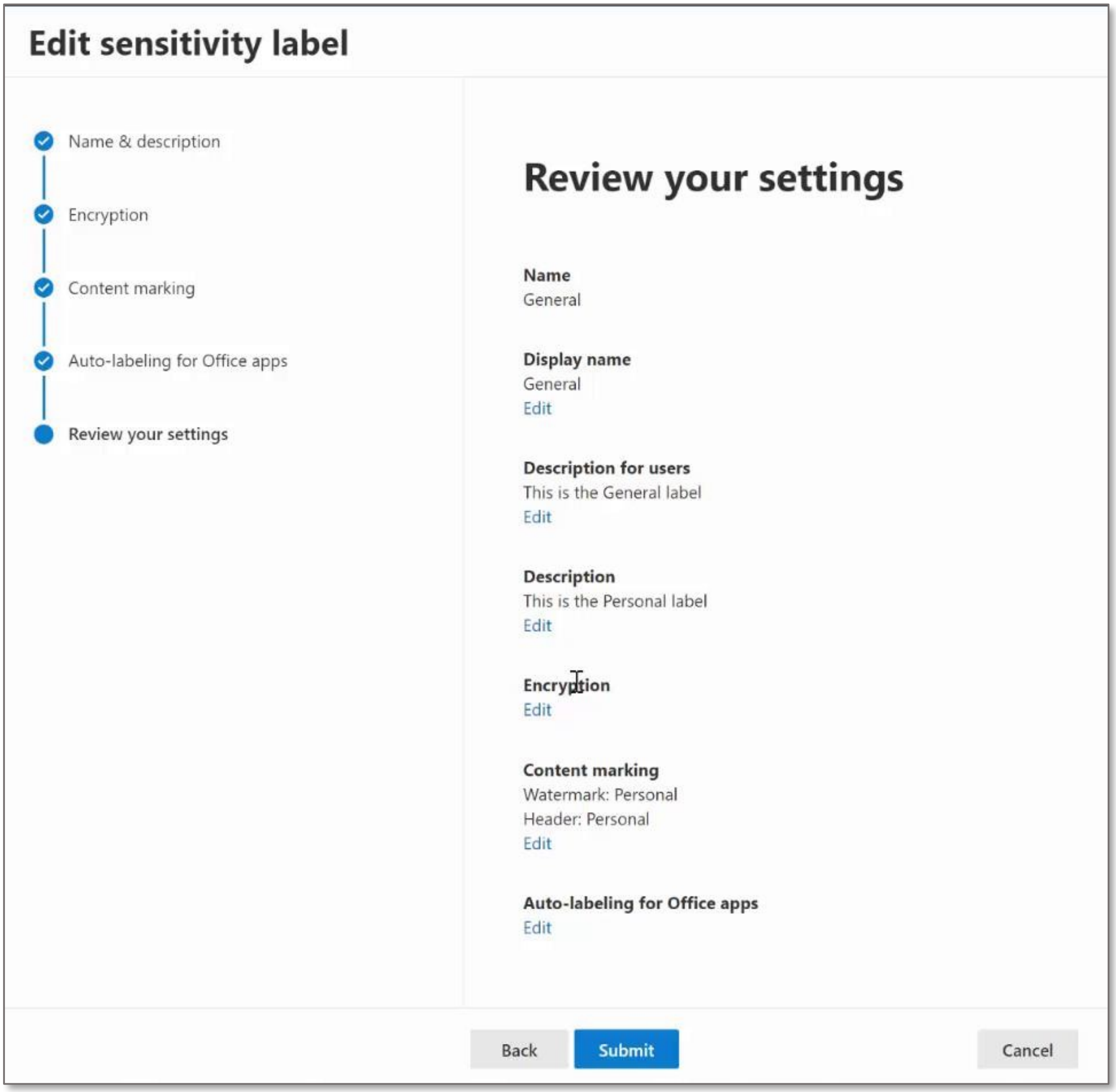
- ✓ Name & description
- ✓ Encryption
- ✓ Content marking
- ● Auto-labeling for Office apps
- ○ Review your settings

Auto-labeling for Office apps

Auto-labeling is supported in Office apps for users who have either Office 365 ProPlus or the Azure Information Protection unified labeling client installed. When we detect sensitive content in email or documents matching the conditions you choose, we can automatically apply this label or show a message to users recommending they apply it themselves. Learn more about auto-labeling

Auto-labeling for Office apps

Then review all of the settings before finally submitting them.



Edit sensitivity label

Review your settings

Name
General

Display name
General
Edit

Description for users
This is the General label
Edit

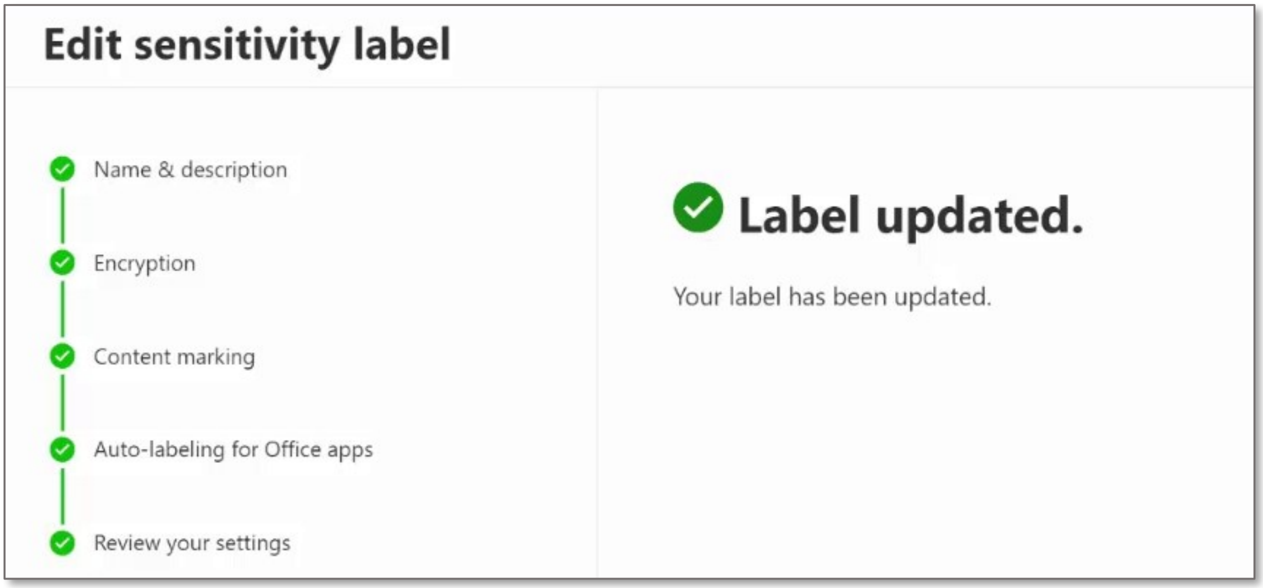
Description
This is the Personal label
Edit

Encryption
Edit

Content marking
Watermark: Personal
Header: Personal
Edit

Auto-labeling for Office apps
Edit

The changes will then be reflected wherever that label is used.



Edit sensitivity label

- ✓ Name & description
- ✓ Encryption
- ✓ Content marking
- ✓ Auto-labeling for Office apps
- ✓ Review your settings

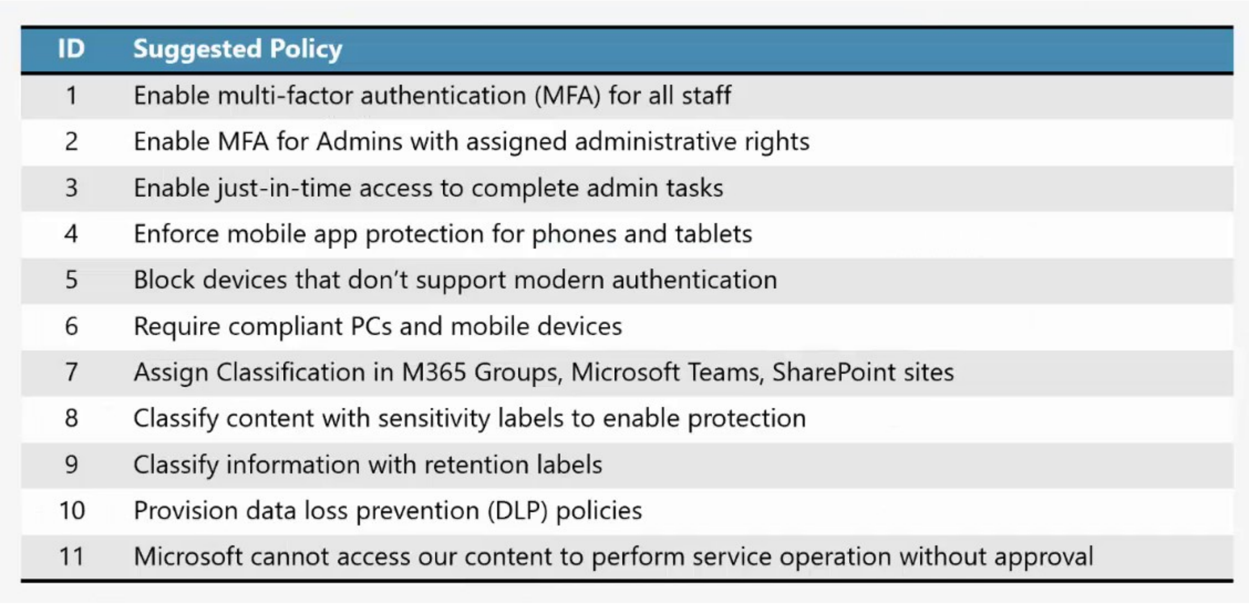
✓ Label updated.

Your label has been updated.

That gives an overview of how to use the compliance center, the score, and also enabling your solution catalogue to get to various configuration elements within it.

In some organizations, security and compliance are left as a separate phase of the project or program or only considered after services have been rolled out. Ideally, legal and security teams, as well as other leadership teams, need to be included from an early stage in a joint effort to implement this properly.

As a starting point, here is a starter list of policies that could be implemented to help with your overall security and compliance position:



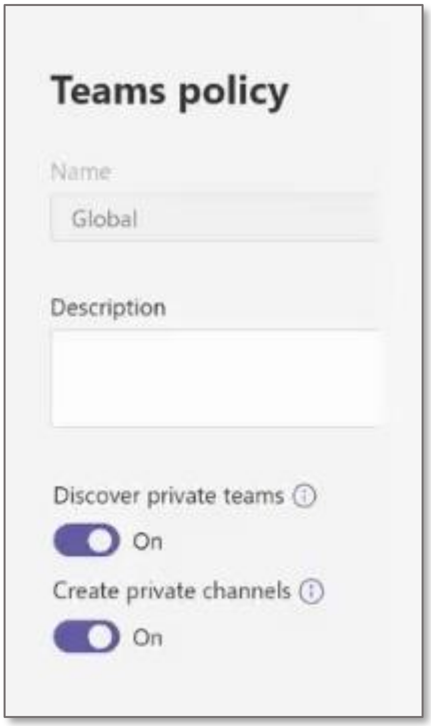
ID	Suggested Policy
1	Enable multi-factor authentication (MFA) for all staff
2	Enable MFA for Admins with assigned administrative rights
3	Enable just-in-time access to complete admin tasks
4	Enforce mobile app protection for phones and tablets
5	Block devices that don't support modern authentication
6	Require compliant PCs and mobile devices
7	Assign Classification in M365 Groups, Microsoft Teams, SharePoint sites
8	Classify content with sensitivity labels to enable protection
9	Classify information with retention labels
10	Provision data loss prevention (DLP) policies
11	Microsoft cannot access our content to perform service operation without approval

Additionally, this link provides more information for Business Decision Makers (BDM): https://docs.microsoft.com/en-us/microsoft-365/security/microsoft-365-security-forbdm

Microsoft Teams Policies

The seventh step is Microsoft teams, and depending on how you roll out additional services, there might be some specific policy configurations that you want to enable or disable.

For example, the Teams policy allows you to control whether users can discover private teams and create private channels.



Teams policy

Name

Global

Description

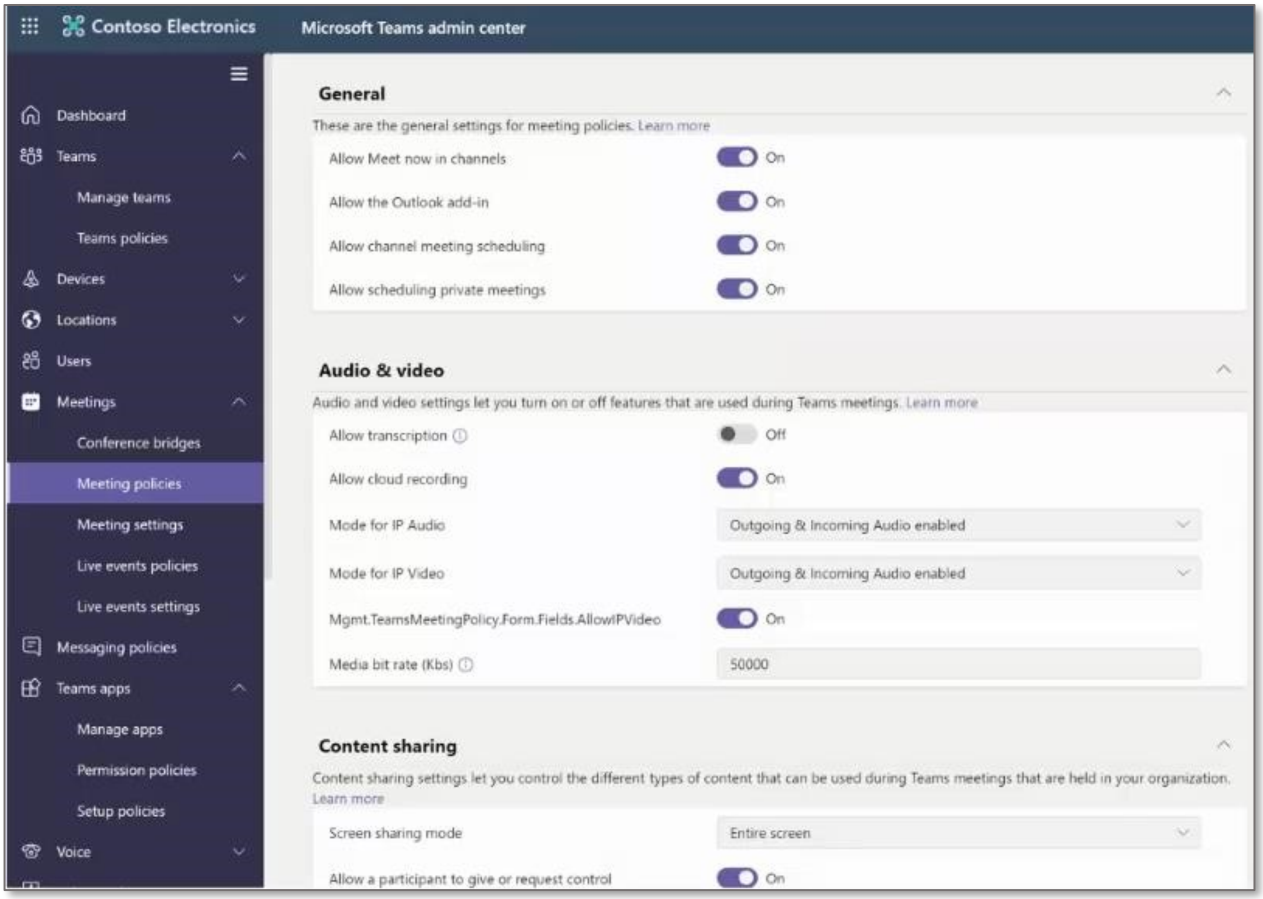
Discover private teams ⓘ

On

Create private channels ⓘ

On

In the Microsoft Teams admin centre, you can set other policy settings as well as meeting policies. The Outlook add-in will allow your users to forward any emails they receive into Microsoft teams channels – if you don't want that happen, then you can simply just switch that off. You can also allow transcription for audios and videos that take place in your team's environment.



General

These are the general settings for meeting policies. Learn more

Allow Meet now in channels: On

Allow the Outlook add-in: On

Allow channel meeting scheduling: On

Allow scheduling private meetings: On

Audio & video

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

Allow transcription: Off

Allow cloud recording: On

Mode for IP Audio: Outgoing & Incoming Audio enabled

Mode for IP Video: Outgoing & Incoming Audio enabled

Mgmt.TeamsMeetingPolicy.Form.Fields.AllowIPVideo: On

Media bit rate (Kbs): 50000

Content sharing

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

Screen sharing mode: Entire screen

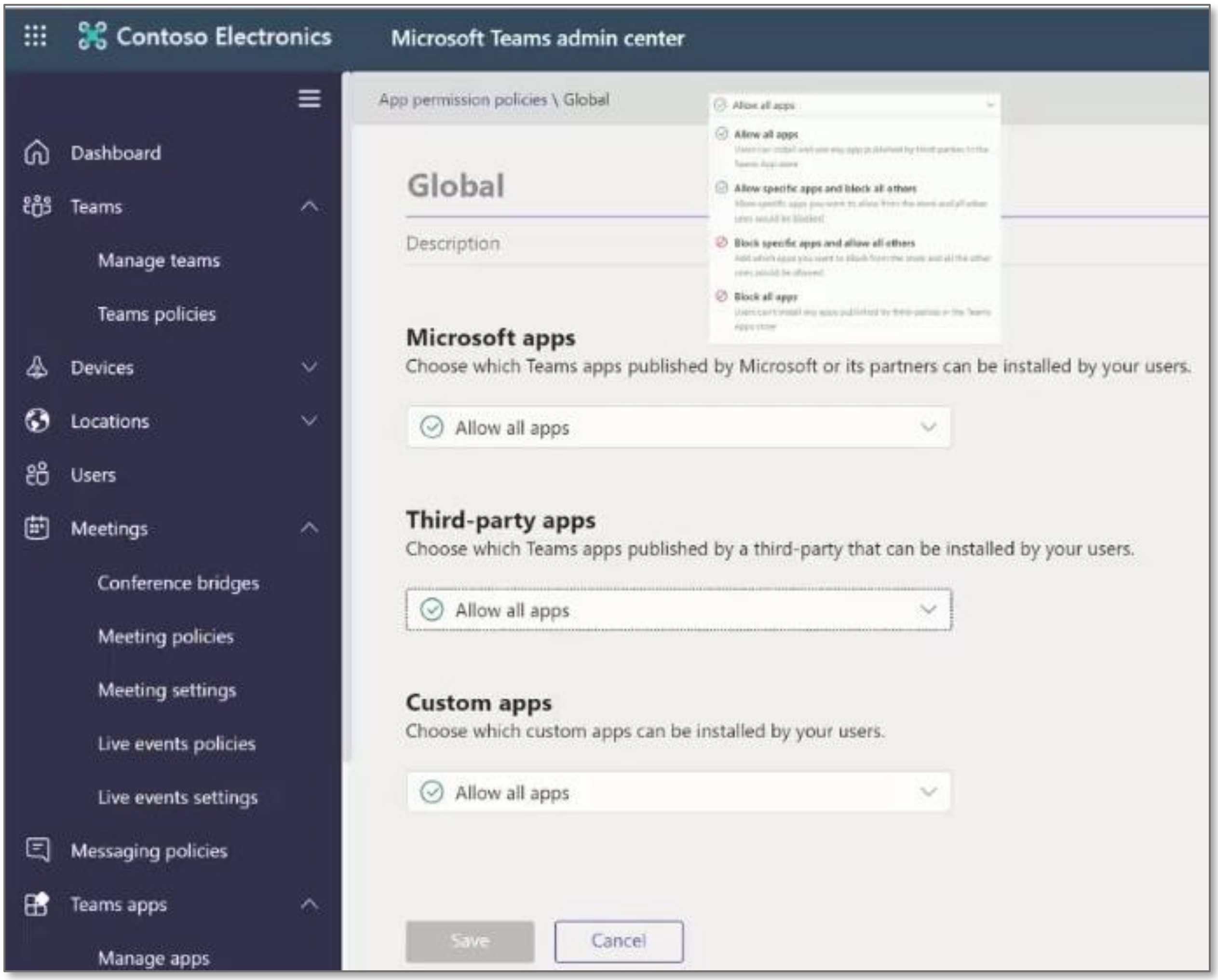
Allow a participant to give or request control: On

These are some of the ways you can govern Microsoft teams, remember you also need to have policies in place and be able to support your users effectively.

Teams Apps

Microsoft Teams is a large platform that allows many third-party apps to integrate with it. You may not want to allow all the apps to be available to your users who could then connect and bring them into their teams.

You can initially set your global policy, and then create additional policies for specific departments or business units who may need to use some additional apps. You can, therefore, ensure that everyone has access to the tools they need.



Global

Description

○ Allow all apps

- **Allow all apps**
  [illegible]
- **Allow specific apps and block all others**
  [illegible]
- **Block specific apps and allow all others**
  [illegible]
- **Block all apps**
  [illegible]

Microsoft apps

Choose which Teams apps published by Microsoft or its partners can be installed by your users.

Allow all apps

Third-party apps

Choose which Teams apps published by a third-party that can be installed by your users.

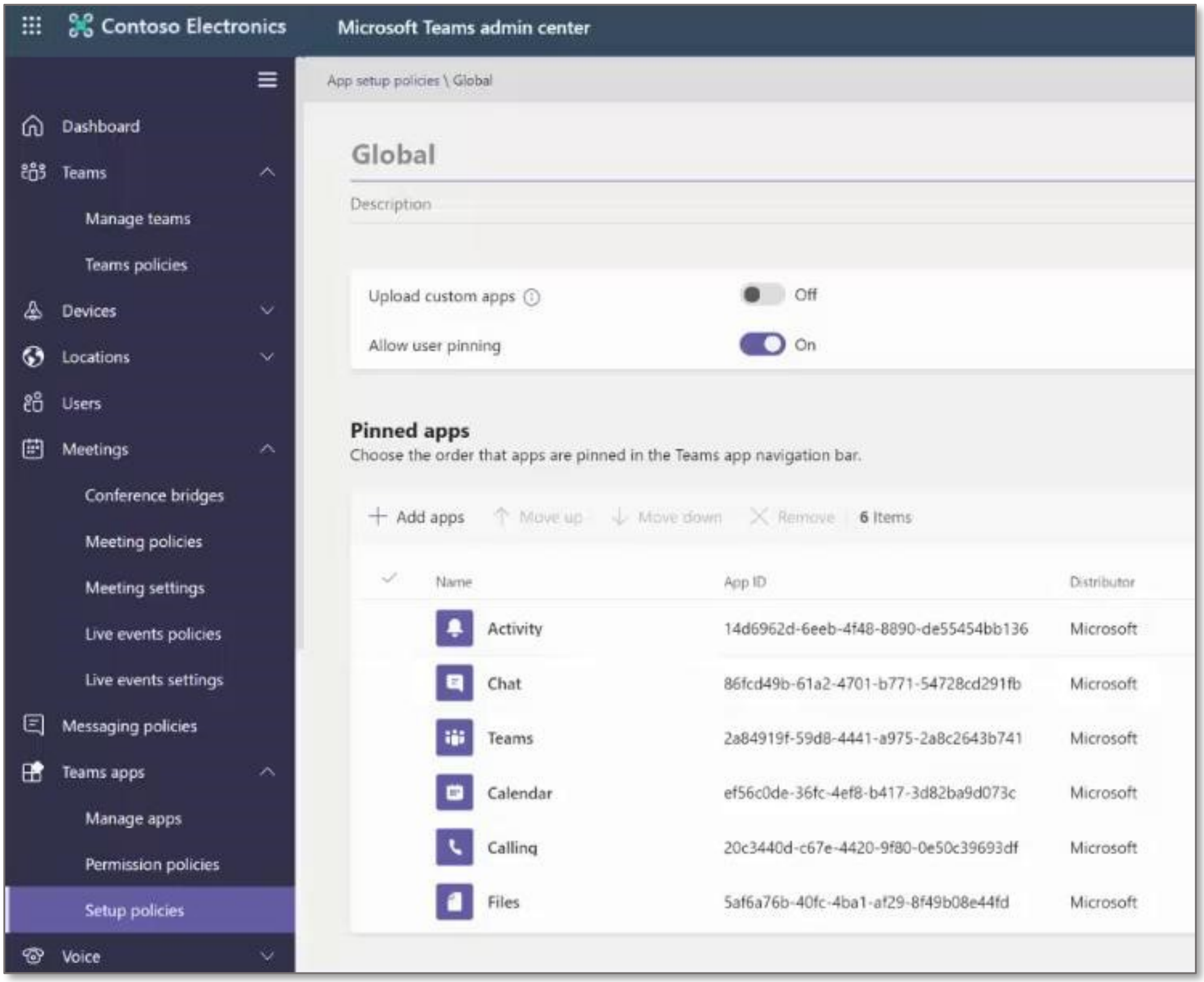
Allow all apps

Custom apps

Choose which custom apps can be installed by your users.

Allow all apps

You can pre-determine which apps are pinned to the left rail menu for your Teams, so it's easy for users to access key apps. You can also control what other apps can be pinned as well.



Global

Description

Upload custom apps: Off

Allow user pinning: On

Pinned apps

Choose the order that apps are pinned in the Teams app navigation bar.

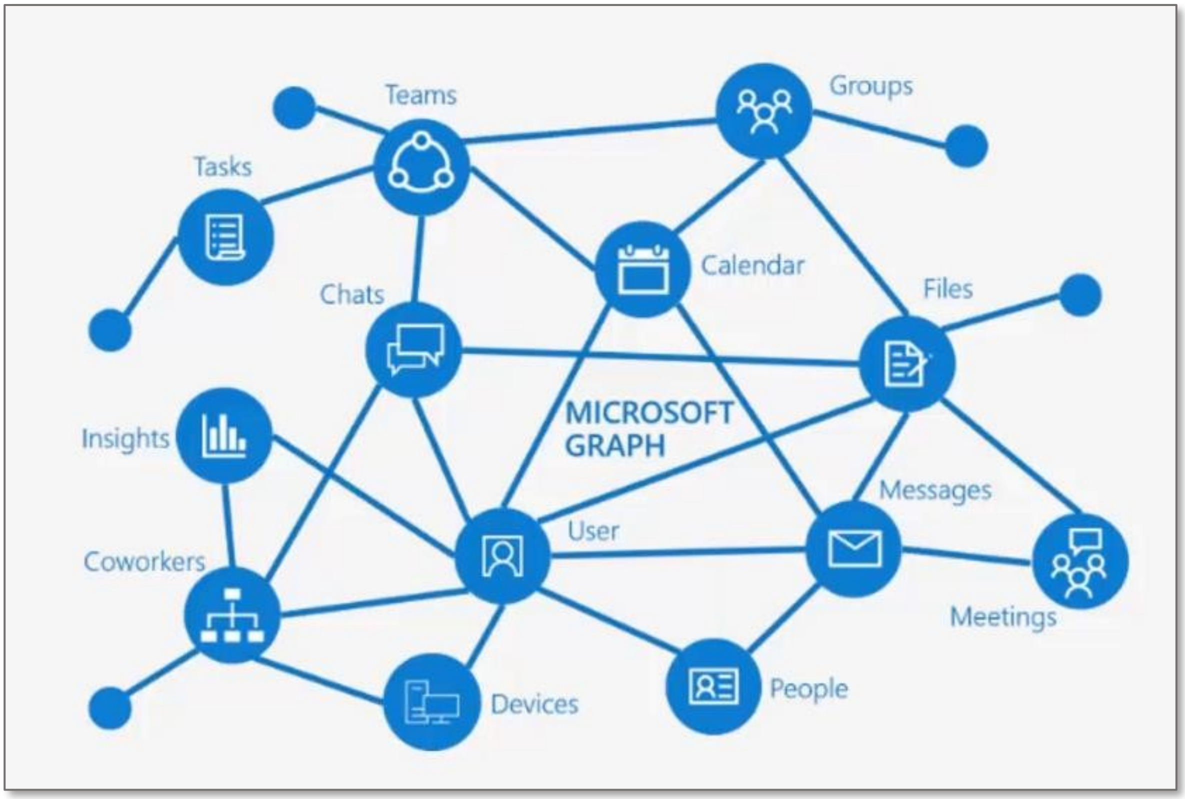
6 Items

Name	App ID	Distributor
Activity	14d6962d-6eeb-4f48-8890-de55454bb136	Microsoft
Chat	86fcd49b-61a2-4701-b771-54728cd291fb	Microsoft
Teams	2a84919f-59d8-4441-a975-2a8c2643b741	Microsoft
Calendar	ef56c0de-36fc-4ef8-b417-3d82ba9d073c	Microsoft
Calling	20c3440d-c67e-4420-9f80-0e50c39693df	Microsoft
Files	5af6a76b-40fc-4ba1-af29-8f49b08e44fd	Microsoft

There are many other settings in the Microsoft Teams admin center for you to discover.

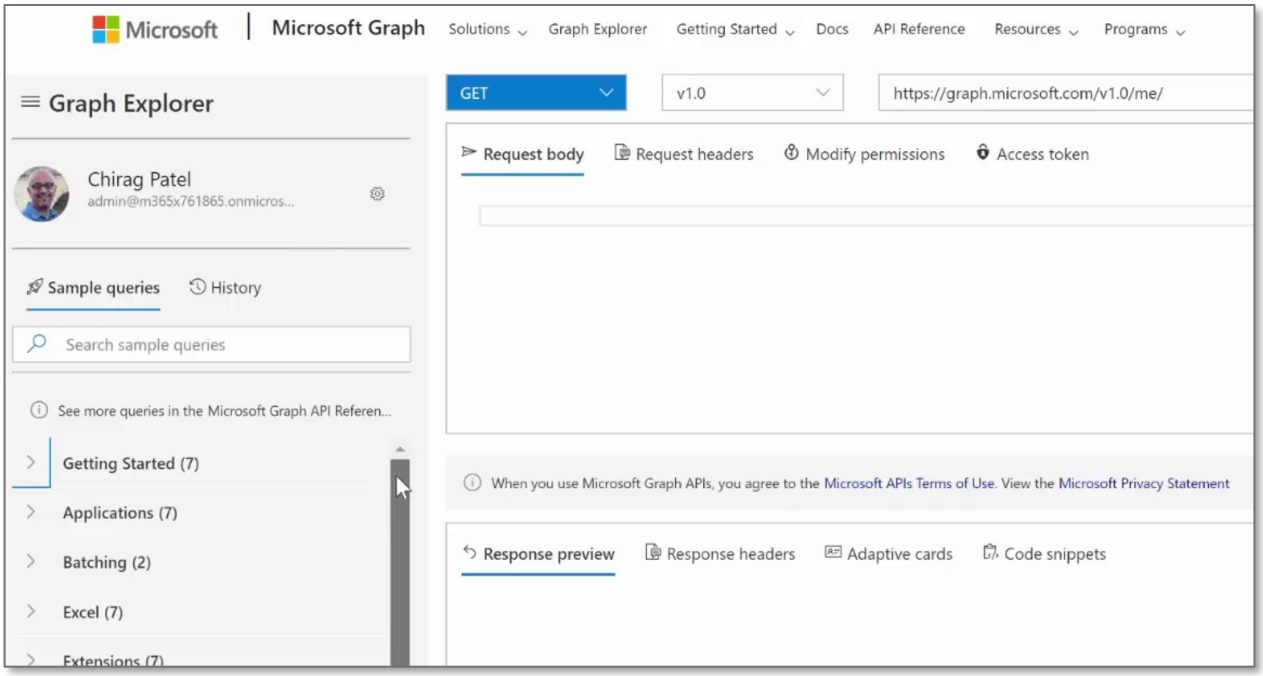
Microsoft Graph Explorer

Microsoft graph is the tool which allows you to access all parts of Microsoft 365 through the graph API interface. It provides a single endpoint whether you're developing applications, or simply trying to look after your environment.



Microsoft Graph Explorer is a web-based tool that you can use to build and test requests using Microsoft Graph API. Sample queries are provided in Graph Explorer to enable you to run common requests quickly.

In the screenshots below I'm signed into Graph as a global admin for this particular tenant. On the left-hand side I have a set of sample queries which look at all workloads for Microsoft 365 services.



Microsoft | Microsoft Graph Solutions Graph Explorer Getting Started Docs API Reference Resources Programs

Graph Explorer

GET v1.0 https://graph.microsoft.com/v1.0/me/

Request body Request headers Modify permissions Access token

Chirag Patel
admin@m365x761865.onmicros...

Sample queries History

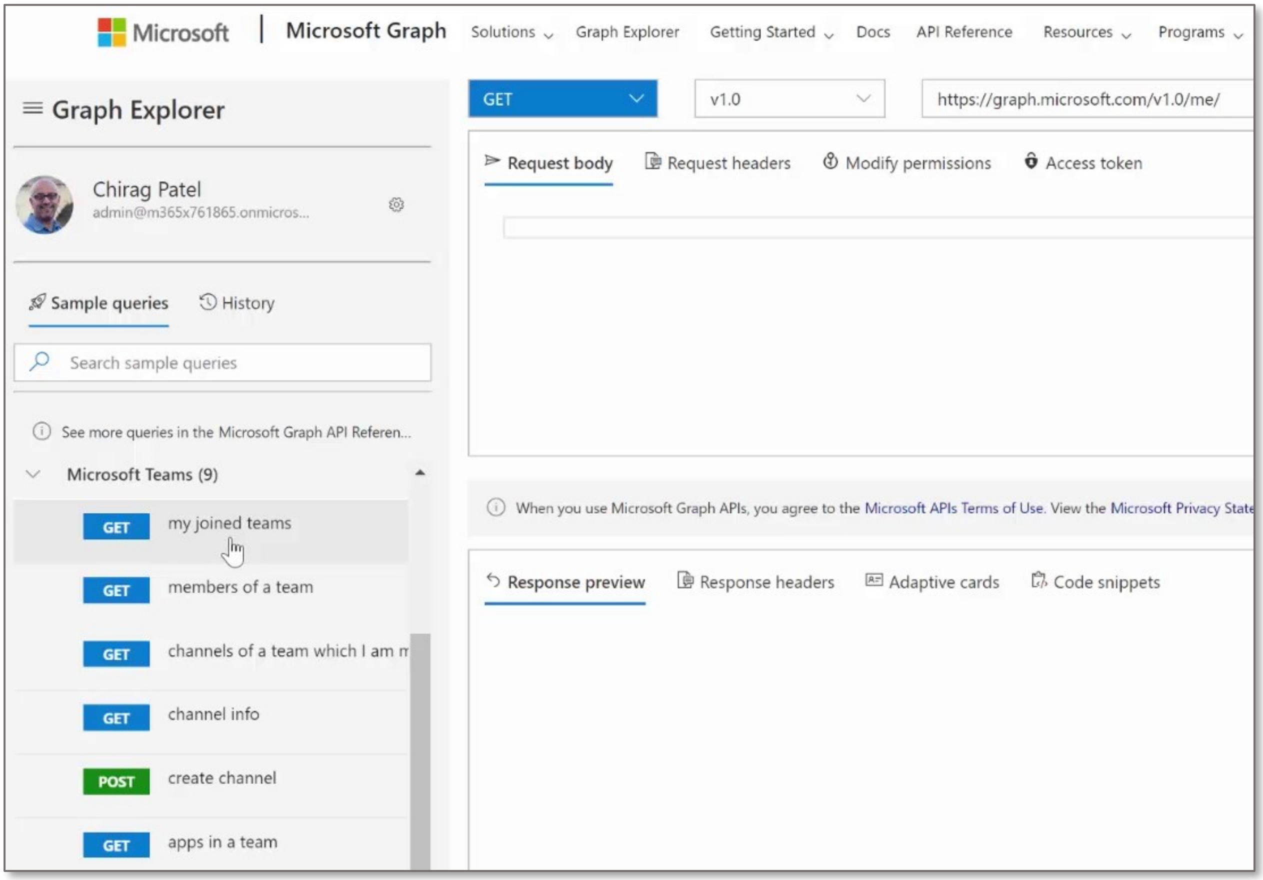
Search sample queries

See more queries in the Microsoft Graph API Referen...

- Getting Started (7)
- Applications (7)
- Batching (2)
- Excel (7)
- Extensions (7)

When you use Microsoft Graph APIs, you agree to the Microsoft APIs Terms of Use. View the Microsoft Privacy Statement

Response preview Response headers Adaptive cards Code snippets



Microsoft | Microsoft Graph Solutions Graph Explorer Getting Started Docs API Reference Resources Programs

Graph Explorer

GET v1.0 https://graph.microsoft.com/v1.0/me/

Request body Request headers Modify permissions Access token

Chirag Patel
admin@m365x761865.onmicros...

Sample queries History

Search sample queries

See more queries in the Microsoft Graph API Referen...

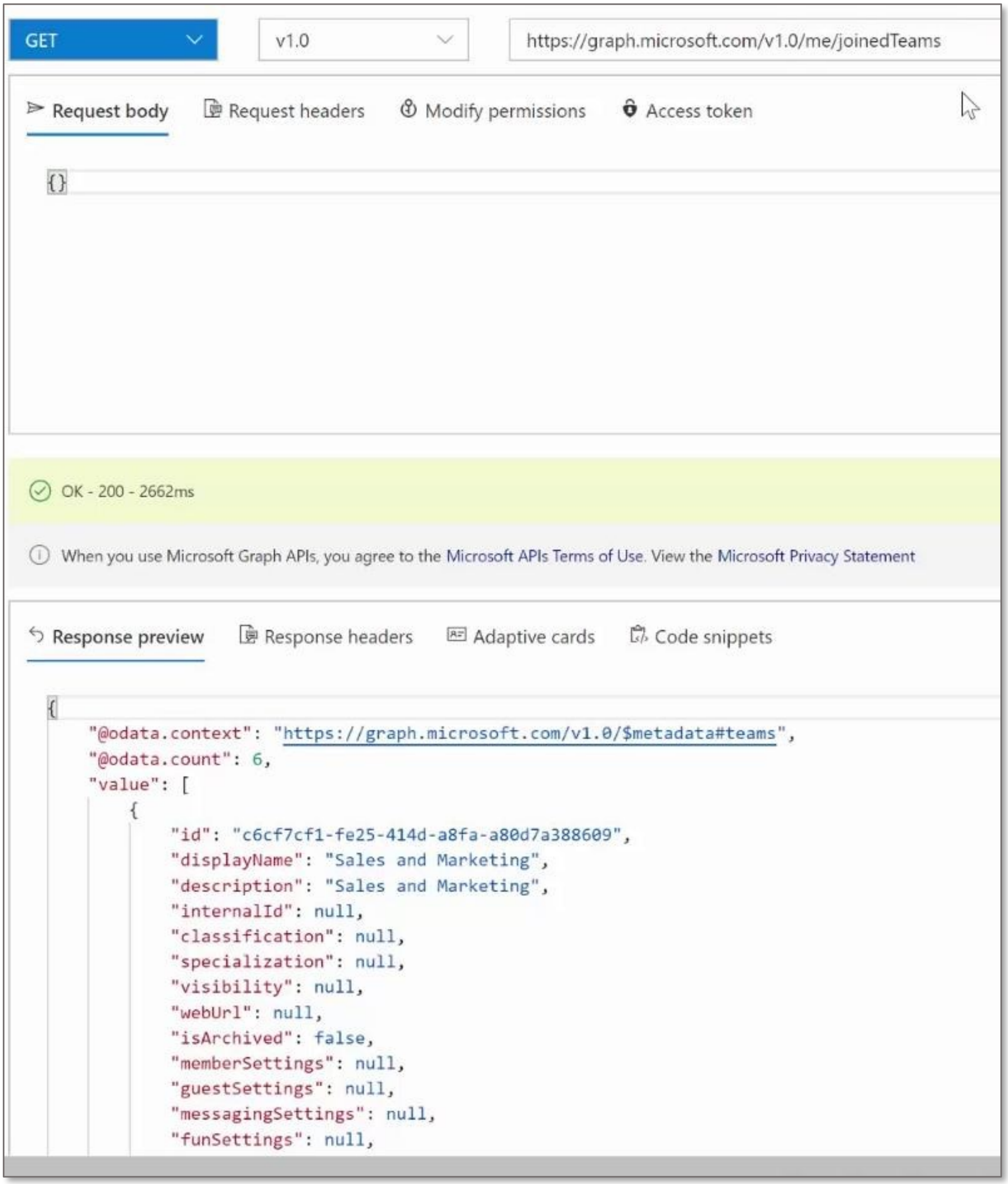
Microsoft Teams (9)

- GET my joined teams
- GET members of a team
- GET channels of a team which I am m
- GET channel info
- POST create channel
- GET apps in a team

When you use Microsoft Graph APIs, you agree to the Microsoft APIs Terms of Use. View the Microsoft Privacy State

Response preview Response headers Adaptive cards Code snippets

By expanding the teams option and running the query to get a list of the teams that I am a member of, I get the following response:



https://graph.microsoft.com/v1.0/me/joinedTeams

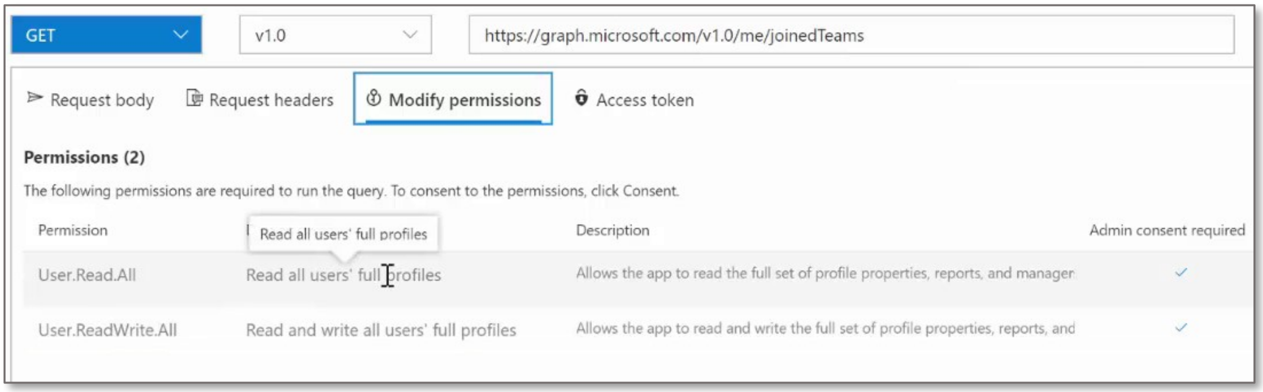
{}

OK - 200 - 2662ms

When you use Microsoft Graph APIs, you agree to the Microsoft APIs Terms of Use. View the Microsoft Privacy Statement

```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#teams",
    "@odata.count": 6,
    "value": [
        {
            "id": "c6cf7cf1-fe25-414d-a8fa-a80d7a388609",
            "displayName": "Sales and Marketing",
            "description": "Sales and Marketing",
            "internalId": null,
            "classification": null,
            "specialization": null,
            "visibility": null,
            "webUrl": null,
            "isArchived": false,
            "memberSettings": null,
            "guestSettings": null,
            "messagingSettings": null,
            "funSettings": null,
```

The information is presented in a code format, but can then be used in other applications or by developers for inclusion as they build applications.



https://graph.microsoft.com/v1.0/me/joinedTeams

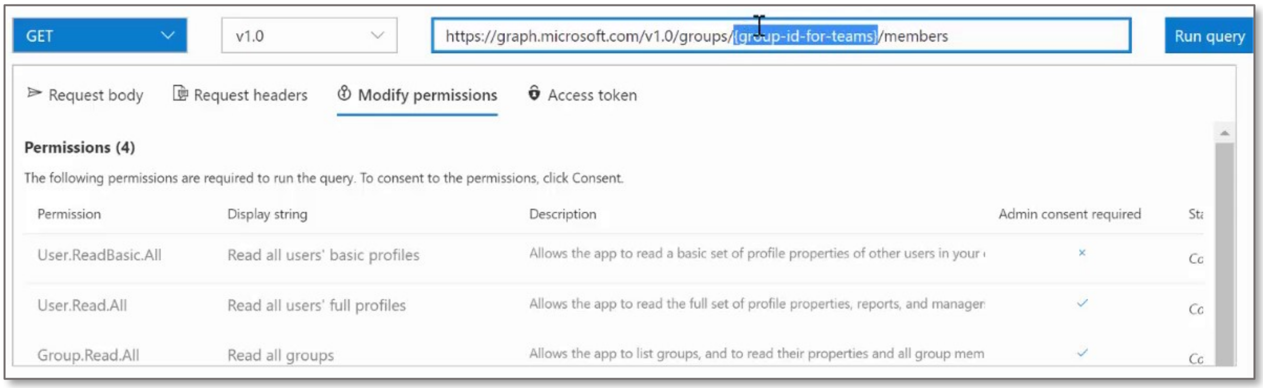
Permissions (2)

The following permissions are required to run the query. To consent to the permissions, click Consent.

Permission		Description	Admin consent required
User.Read.All	Read all users' full profiles	Allows the app to read the full set of profile properties, reports, and manager	✓
User.ReadWrite.All	Read and write all users' full profiles	Allows the app to read and write the full set of profile properties, reports, and	✓

The Modify permissions option tells me what permissions you need in order to run this query, otherwise it's going to be access denied.

To find the members of a team, you need to know the Team ID (shown in the code sample above) and paste it into the query address, then run the query.



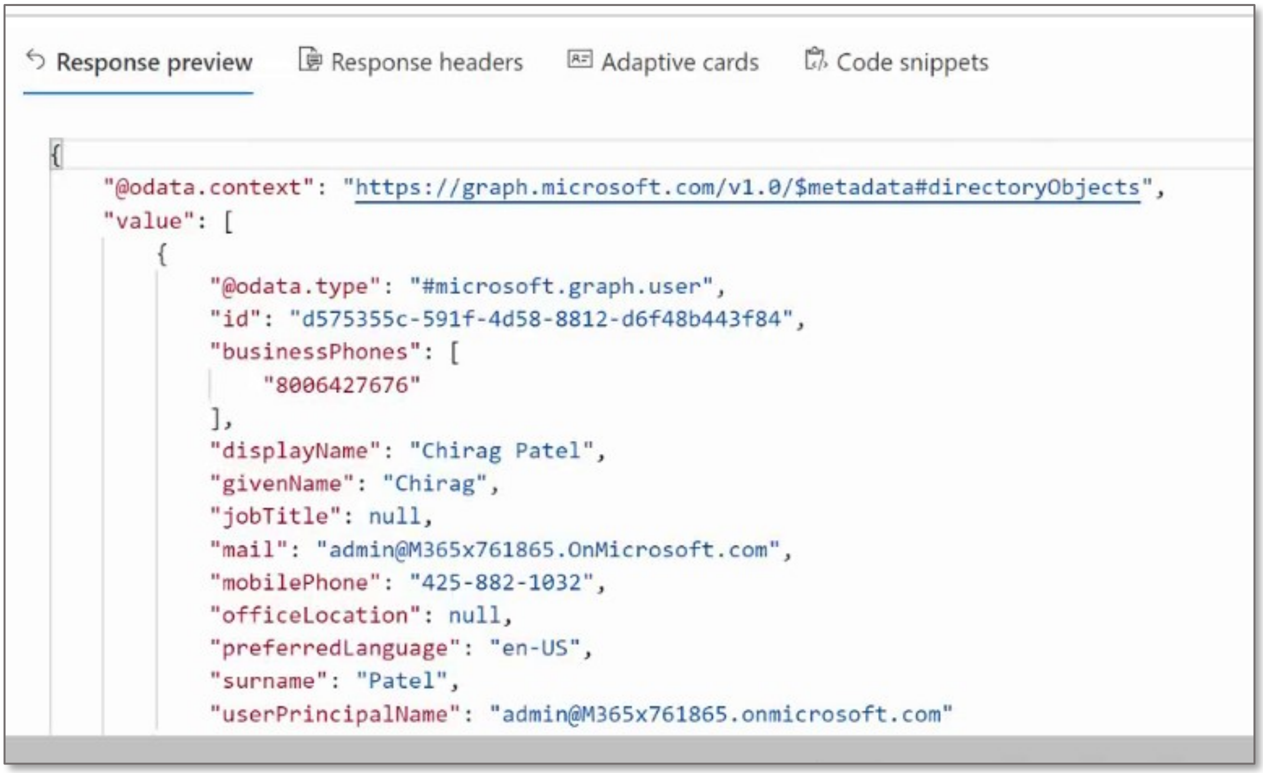
https://graph.microsoft.com/v1.0/groups/{group-id-for-teams}/members

Permissions (4)

The following permissions are required to run the query. To consent to the permissions, click Consent.

Permission	Display string	Description	Admin consent required	Sta
User.ReadBasic.All	Read all users' basic profiles	Allows the app to read a basic set of profile properties of other users in your	×	Co
User.Read.All	Read all users' full profiles	Allows the app to read the full set of profile properties, reports, and manager	✓	Co
Group.Read.All	Read all groups	Allows the app to list groups, and to read their properties and all group mem	✓	Co

The response is again in code, but you can scroll down to find the names of the people in the team.



```
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#directoryObjects",
    "value": [
        {
            "@odata.type": "#microsoft.graph.user",
            "id": "d575355c-591f-4d58-8812-d6f48b443f84",
            "businessPhones": [
                "8006427676"
            ],
            "displayName": "Chirag Patel",
            "givenName": "Chirag",
            "jobTitle": null,
            "mail": "admin@M365x761865.OnMicrosoft.com",
            "mobilePhone": "425-882-1032",
            "officeLocation": null,
            "preferredLanguage": "en-US",
            "surname": "Patel",
            "userPrincipalName": "admin@M365x761865.onmicrosoft.com"
```

Using Microsoft Graph is a very quick way to explore the Microsoft 365 environment without having to go into any of the actual programs themselves.

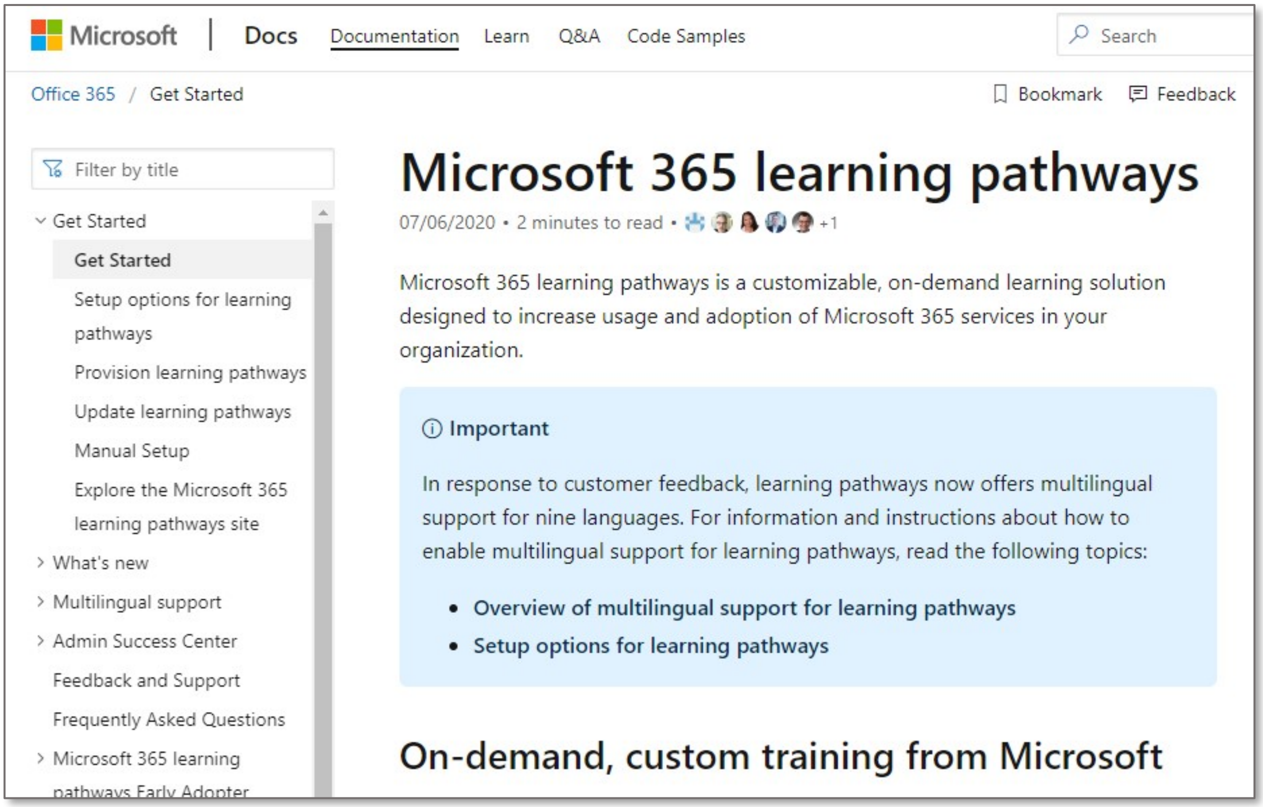
Training and Adoption

Last but not least is always about the users in terms of how do you train them. If you don't have a training department or not enough training resources to keep up with new features getting rolled out you can use the Microsoft 365 Learning Pathways.

Microsoft 365 Learning Pathways

The SharePoint team have provided a dedicated site, called Microsoft 365 learning pathways. This is essentially a site that looks just like a SharePoint site but has been preloaded with training material (the link is shown below) for each of the Microsoft 365 services. It's a kind of on-demand, learning solution which can be customized further by adding other third-party systems that you may already have.

https://docs.microsoft.com/en-us/office365/customlearning



Microsoft 365 learning pathways

07/06/2020 • 2 minutes to read • +1

Microsoft 365 learning pathways is a customizable, on-demand learning solution designed to increase usage and adoption of Microsoft 365 services in your organization.

ⓘ Important

In response to customer feedback, learning pathways now offers multilingual support for nine languages. For information and instructions about how to enable multilingual support for learning pathways, read the following topics:

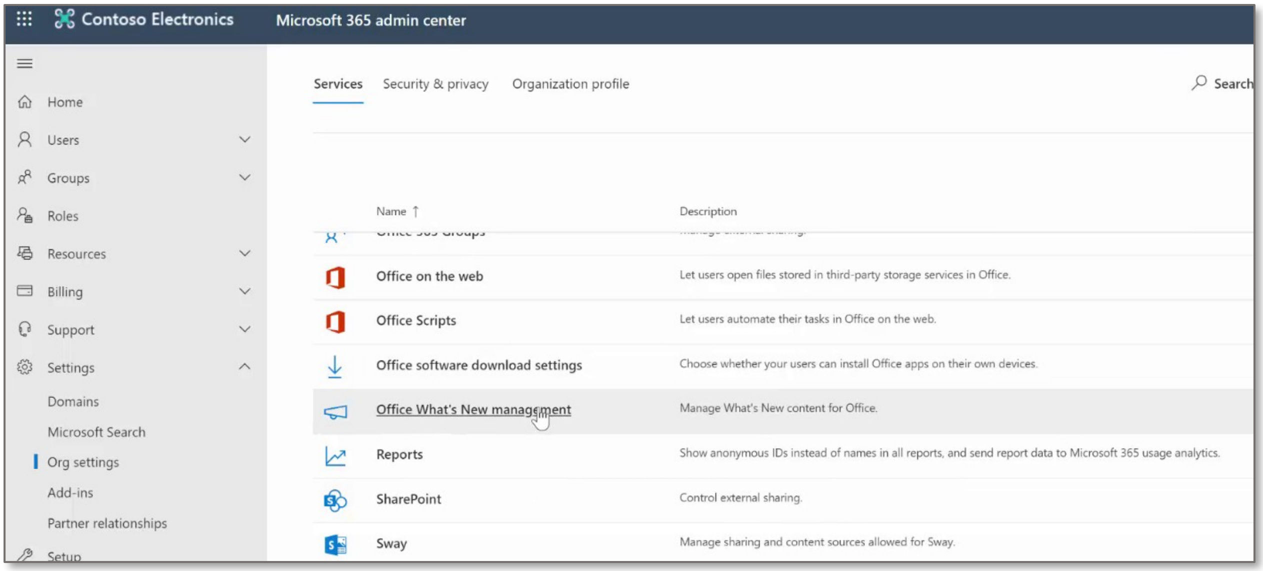
- Overview of multilingual support for learning pathways
- Setup options for learning pathways

On-demand, custom training from Microsoft

This is a very quick way to help support your users and manage help content that Microsoft has already produced for us.

Office What’s New Management

This allows you to control the “What’s new” notifications that are sent to your users. From the Microsoft 365 admin center, settings option, choose “Org settings” and then scroll down the screen to find the “Office What’s New management.”



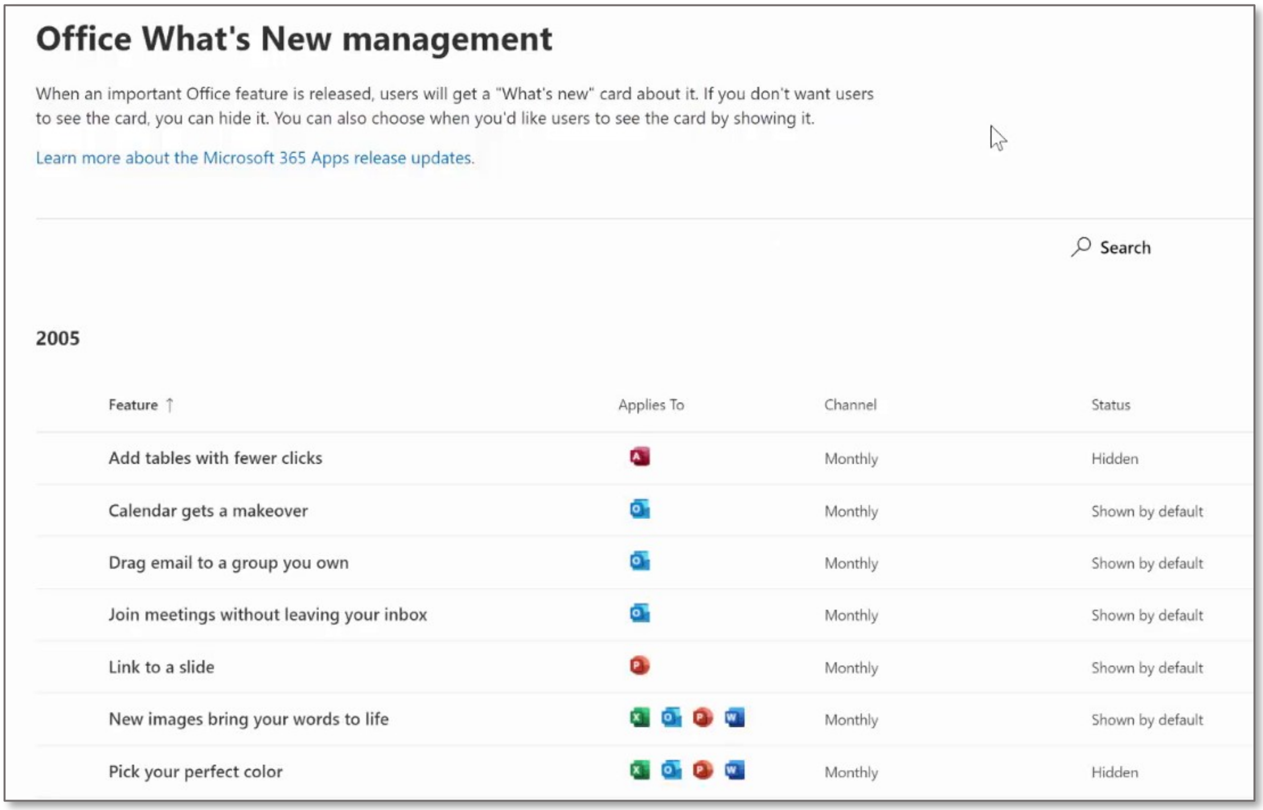
Contoso Electronics | Microsoft 365 admin center

- Home
- Users
- Groups
- Roles
- Resources
- Billing
- Support
- Settings
  - Domains
  - Microsoft Search
  - Org settings
  - Add-ins
  - Partner relationships
- Setup

Services | Security & privacy | Organization profile | Search

Name ↑	Description
Office 365 Groups	Manage external sharing.
Office on the web	Let users open files stored in third-party storage services in Office.
Office Scripts	Let users automate their tasks in Office on the web.
Office software download settings	Choose whether your users can install Office apps on their own devices.
Office What's New management	Manage What's New content for Office.
Reports	Show anonymous IDs instead of names in all reports, and send report data to Microsoft 365 usage analytics.
SharePoint	Control external sharing.
Sway	Manage sharing and content sources allowed for Sway.

This is the May 2020 release, and shows the set of features that it contained and which services they apply to. Earlier releases are shown further down the page.



Office What's New management

When an important Office feature is released, users will get a "What's new" card about it. If you don't want users to see the card, you can hide it. You can also choose when you'd like users to see the card by showing it.

Learn more about the Microsoft 365 Apps release updates.

Search

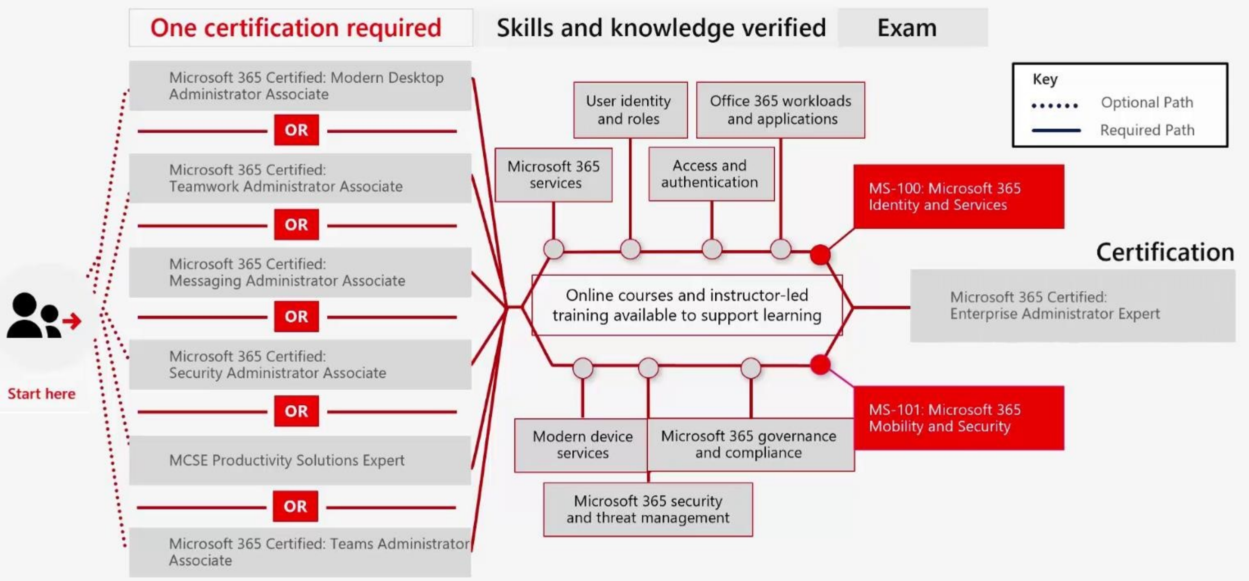
2005

Feature ↑	Applies To	Channel	Status
Add tables with fewer clicks	A	Monthly	Hidden
Calendar gets a makeover	O	Monthly	Shown by default
Drag email to a group you own	O	Monthly	Shown by default
Join meetings without leaving your inbox	O	Monthly	Shown by default
Link to a slide	P	Monthly	Shown by default
New images bring your words to life	X O P W	Monthly	Shown by default
Pick your perfect color	X O P W	Monthly	Hidden

You can click on each feature and decide whether you want to hide the notifications about the feature to users.

Microsoft 365 Enterprise Administrator certification

From the IT team perspective, the platform is constantly changing and developing and to prove you understand the full capability of Microsoft 365 you can gain an MS-100 or MS-101 certification.


One certification required
Skills and knowledge verified
Exam
Key
Optional Path
Required Path
Start here
Microsoft 365 Certified: Modern Desktop Administrator Associate
OR
Microsoft 365 Certified: Teamwork Administrator Associate
OR
Microsoft 365 Certified: Messaging Administrator Associate
OR
Microsoft 365 Certified: Security Administrator Associate
OR
MCSE Productivity Solutions Expert
OR
Microsoft 365 Certified: Teams Administrator Associate
User identity and roles
Office 365 workloads and applications
Microsoft 365 services
Access and authentication
Online courses and instructor-led training available to support learning
Modern device services
Microsoft 365 governance and compliance
Microsoft 365 security and threat management
MS-100: Microsoft 365 Identity and Services
MS-101: Microsoft 365 Mobility and Security
Certification
Microsoft 365 Certified: Enterprise Administrator Expert

Meet the Presenter

Chirag Patel

Chirag is an Independent Consultant at Patel Consulting,

BCS Chartered IT Professional, TOGAF Certified Architect, Microsoft 365 Certified Enterprise Administrator Expert and Microsoft Service Adoption specialist based in London, UK with more than 20 years of industry experience.