habanero

WHAT YOU NEED TO KNOW

Microsoft Teams governance

The legal stuff.

Habanero shall have no liability for errors, omissions or inadequacies in the information contained here-in or for interpretations thereof. The opinions expressed herein are subject to change without notice.

DATE	VERSION NUMBER
January 28, 2021	1.0

1.0

Introduction

It's no surprise that in 2020, Microsoft Teams became the fastest growing business app in Microsoft's history, with over 115 million active daily users.

Microsoft had already been experiencing incredible growth when the pandemic accelerated this momentum, causing many organizations to fast-track their rollout as an emergency measure to sustain basic operations.

As the dust started to settle, organizations started to take a step back, evaluating their underlying configuration and governance model to make sure they were set up for long-term success.

Whether you are heading into your first implementation or on the back-side of an emergency deployment of Microsoft Teams, we created this guide to help introduce you to the many governance and configuration decisions you will need to wrestle with, along with some tips we've learned along the way.

Here is a summary of key areas we think you'll want to be aware of:

- Clarifying ownership and accountability
- Understanding Microsoft 365 Groups
- Controlling Microsoft Teams provisioning and avoiding sprawl
- What to do about naming conventions
- External and guest access
- Setting a Microsoft Teams expiration policy
- Archiving teams
- Additional configuration options to consider

While we feel this guide will be valuable to anyone involved in managing Microsoft Teams, we also recommend you familiarize yourself with Microsoft's official documentation. The core governance features and functionality will undoubtably evolve, so be sure to bookmark the Microsoft Docs for Teams overview.

2.0

Clarifying ownership and accountability

When it comes to ownership and decision-making, we are seeing organizations struggle as they shift from an older, decentralized approach of application ownership to the cloud services model.

Leveraging the old model of assigning individuals to different applications can be problematic, as the delineation or boundary between different Microsoft cloud services is not as clear as one might think. Instead, applications and services within Microsoft 365 are quite interconnected, both in terms of capabilities and governing policies.

Since Microsoft Teams launched a few years ago, we have seen many rollouts stall due to internal debates about who owns the rollout. This is because Microsoft Teams includes so many things!

FOR EXAMPLE

We know when creating a Microsoft Team, you get a shared mailbox and calendar. Does that mean that the group that supports email/Exchange owns Microsoft Teams? We also know that when a Microsoft Team is created, we get a SharePoint site. Does that mean that the group that supports SharePoint owns Microsoft Teams? How about other Microsoft Teams capabilities, like telephony, conferencing and chat services? Who manages those?

Microsoft Teams has a complex architecture that connects to several other Microsoft 365 applications and services, so there is more to consider besides just Exchange Online and SharePoint Online. The important point to stress here is that your ownership and support model for Microsoft 365 and Microsoft Teams may need to evolve from how you've managed applications in the past.

We can extrapolate Microsoft 365 service ownership challenges to medium and larger organizations with clearly defined roles and responsibilities (like SharePoint and Exchange administrators), whereas in smaller organizations people tend to wear many hats (IT systems administrator).

Regardless of the size of your organization, you will be equally impacted by the interconnectedness of services when it comes to governance and control. As such, rolling out Microsoft Teams before other services may force you to make some choices out of context for other services, like Yammer or SharePoint Online.

Now that you are clear on who owns Microsoft Teams, let's look at what really drives the Microsoft Teams platform with all the connected services and capabilities.

What we recommend

Rethink your approach towards application or service ownership and operational accountabilities when it comes to Microsoft 365.

Microsoft 365 tenant and service ownership

We recommend organizations rethink their approach towards application or service ownership and operational accountabilities when it comes to Microsoft 365. One approach that scales well is to establish accountability and structure that embodies the following concepts:

Primary business owner or executive sponsors: This group sets budget, defines program ownership and key operating guidelines.

Digital workplace steering committee: This group represents individual interests from different business stakeholder groups. They may recommend projects or capabilities based on their own perceived business need or to support companywide initiatives and the value they would provide.

Project team: This group is hands-on during the implementation phase of the project and responsible for transition to operations.

Operational support team: This group is focused on the maintenance and administration of Microsoft 365 services; they are also responsible for implementing changes to the Microsoft 365 roadmap set within the digital workplace steering committee.

Collaboration services support team: This group is focused on change management and adoption. They are often responsible for ongoing end-user support to increase adoption and raise awareness of Microsoft 365 collaboration services.

NEXT UP: UNDERSTANDING MICROSOFT 365 GROUPS

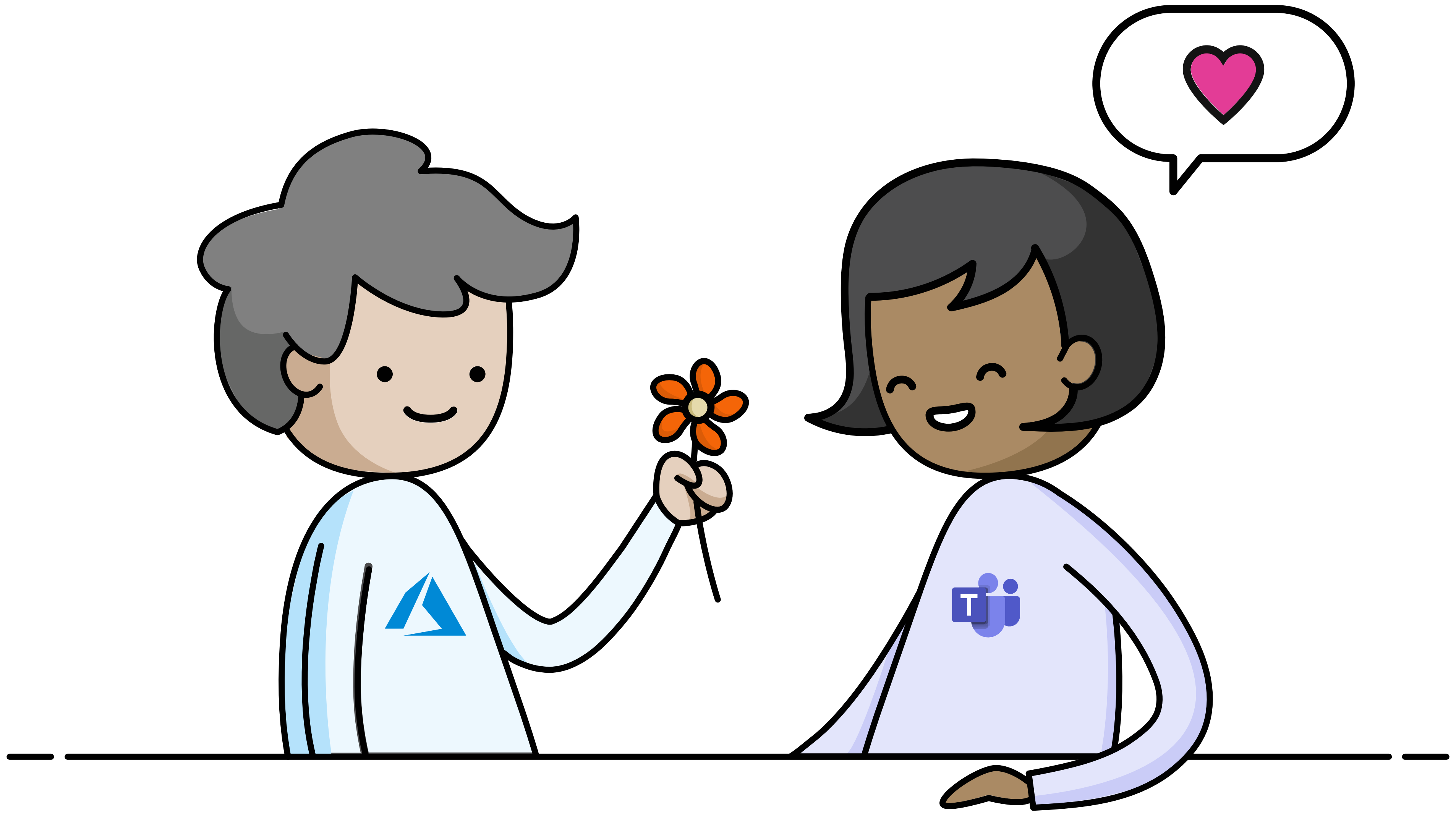
3.0

Understanding Microsoft 365 Groups

Microsoft 365 Groups is a service used to facilitate a shared experience across Microsoft 365 services, and the configuration and policies related to that functionality reside within Azure Active Directory. However, it's not at the forefront in terms of the end-user's experience.

Before implementing Microsoft Teams, it is important to understand the relationship that exists among Microsoft 365 Groups, Microsoft Teams and Azure Active Directory, because it enables you to self-manage who you can collaborate with in the services that have been enabled within your organization.

In the following sub-sections, we'll explore the other Ws of Microsoft Groups: who, what, where and when.



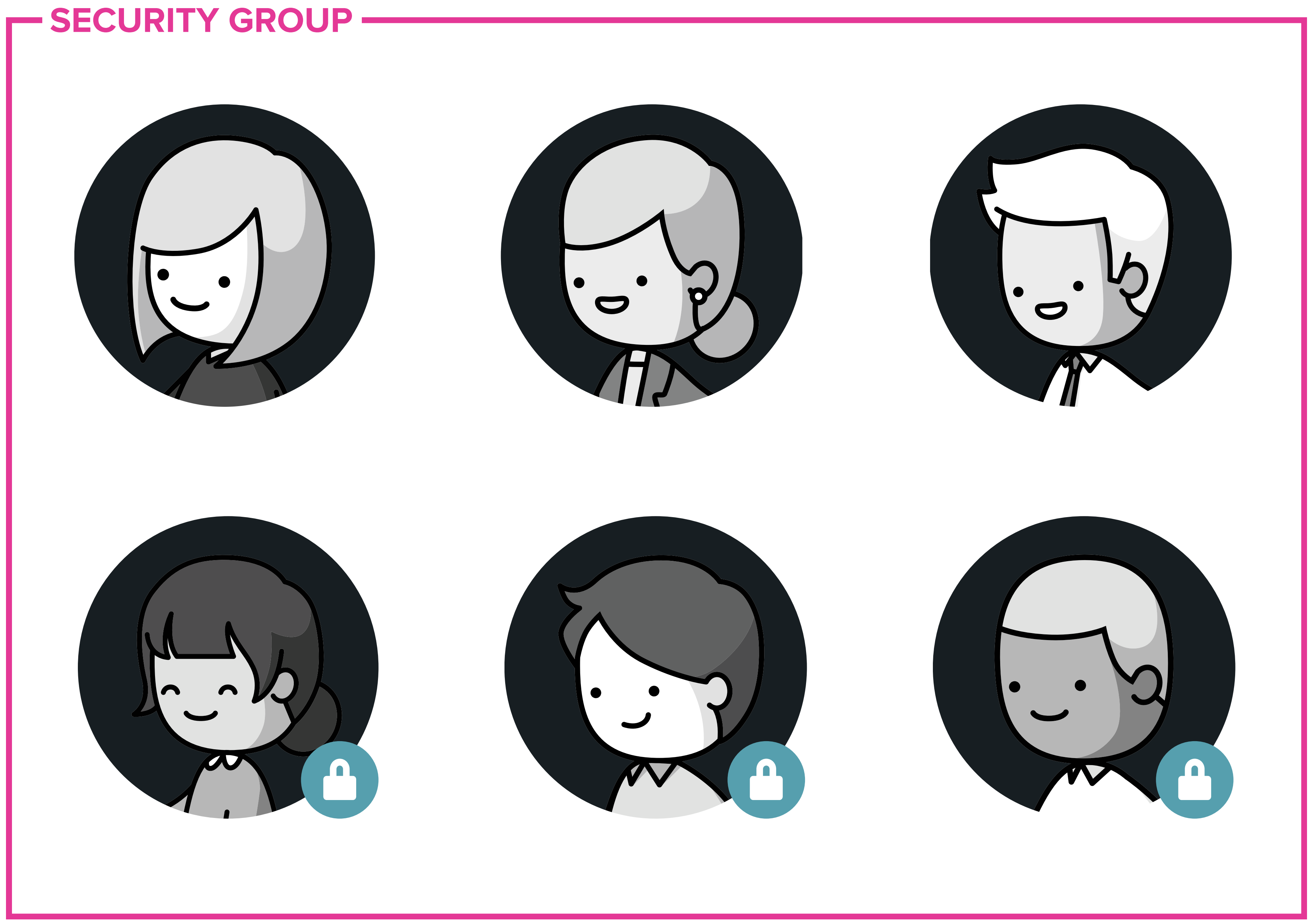
3.1

Who can provision Microsoft 365 Groups?

By default, every licensed user within your organization can create a Microsoft 365 Group; however, there are options to restrict provisioning within your tenant.

To do that, you would have to create a security group in Azure Active Directory and use that security group membership to enable those users to provision Microsoft 365 Groups.

The next logical W should be the what; however, when it comes to Microsoft 365 Groups, the next stop is the where.



3.2

Where can you provision Microsoft 365 Groups?

We now know who can provision a Microsoft 365 Group when restriction controls are not implemented. Now, let's look at where you can create a Microsoft 365 Group.

First, let us state that once provisioned, a Microsoft 365 Group object can be found in Azure Active Directory.

The option to provision a Microsoft 365 Group is available to users from multiple locations and these options increase if the user has been assigned one of the necessary administrator roles.

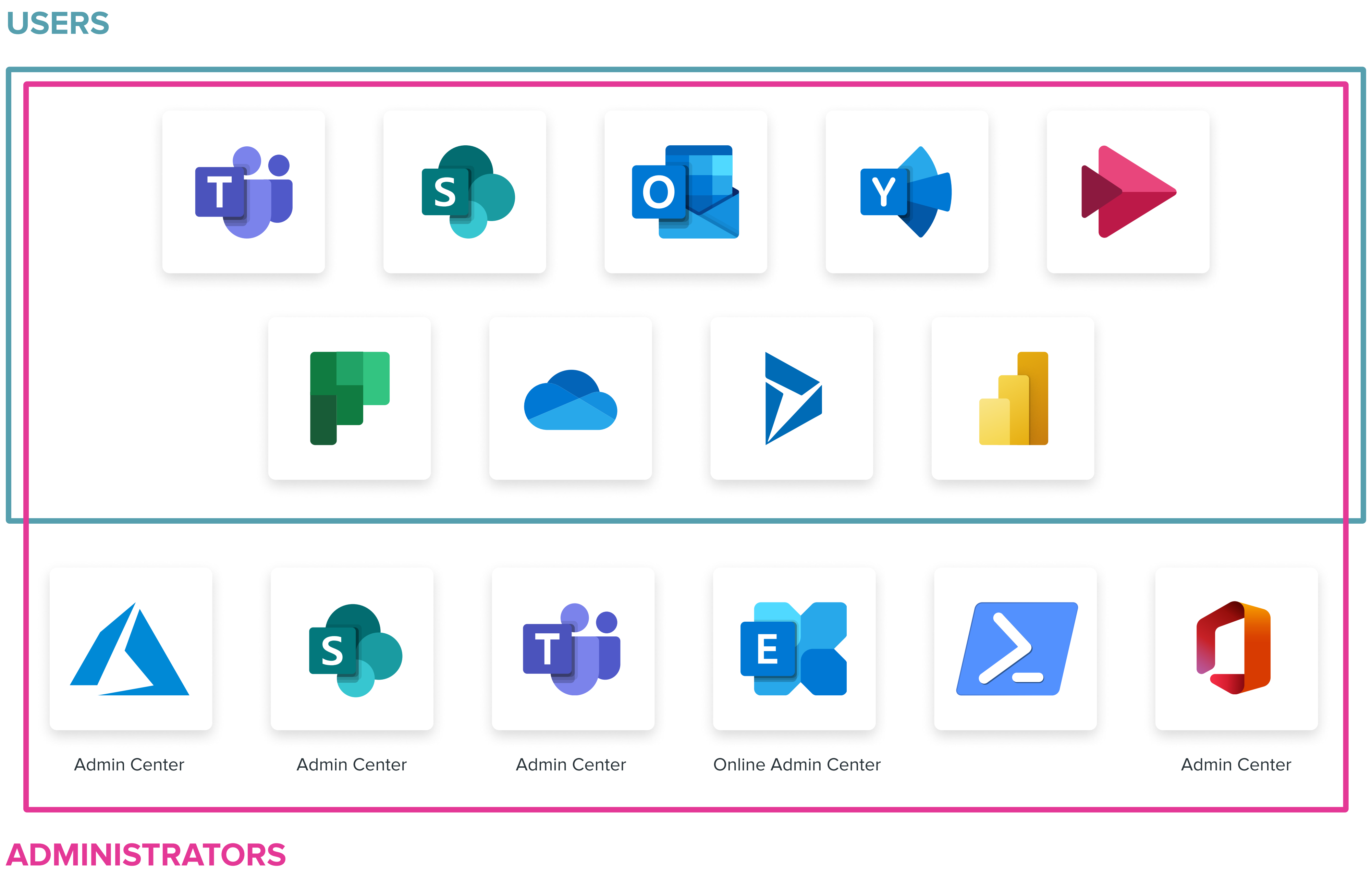
Using the default Microsoft 365 out-of-the-box configuration, the following options are available when creating a Microsoft 365 Group:

Users can provision Microsoft 365 Groups from:

- Microsoft Teams
- SharePoint
- Outlook
- Yammer
- Stream
- Planner
- OneDrive
- Dynamics 365
- Power BI (Workspace Creation Classic Mode)

Administrators can provision Microsoft 365 Groups from all the previously listed locations, as well as:

- Azure Active Directory Admin Center
- SharePoint Admin Center
- Teams Admin Center
- Exchange Online Admin Center
- PowerShell
- Microsoft 365 Admin Center



3.3

What do you get with a Microsoft 365 Group?

So, now that we know who can provision a Microsoft 365 Group, as well as why and where they can create it, we can move onto what gets provisioned with a Microsoft 365 Group.

As almost everything else we experienced so far in relation to Microsoft 365 Groups, there is no one-size-fits-all. So, what gets created when you provision a Microsoft 365 Group depends on where the provisioning process was initiated.

As a result, when the Microsoft 365 Groups provisioning process is done from one of the following locations:

- Azure Active Directory
- SharePoint Online (or admin center)
- OneDrive for Business (web only)
- Outlook (or Exchange Online admin center)
- PowerShell

The following default capabilities get provisioned automatically:

- Microsoft 365 Group
- SharePoint team site with wiki
- Shared Exchange mailbox and calendar

NOTE: Many people think OneNote is included in this list because of a navigation item in the SharePoint site labelled "Notebook," but the OneNote notebook is not provisioned until you click that link.

But when you create a Microsoft 365 Group from one of the locations detailed in Section 3.2, you get the default capabilities plus the service it was created from.

For example:

When creating from Microsoft Teams, you will get the Microsoft 365 Group, plus the following:

- SharePoint team site with wiki
- Shared Exchange mailbox and calendar
- A team within Microsoft Teams

When creating from Yammer, you will get the Microsoft 365 Group, plus the following:

- SharePoint team site with wiki
- Shared Exchange mailbox and calendar
- A Yammer community

When creating from Planner, you will get the Microsoft 365 Group, plus the following:

- SharePoint team site with wiki
- Shared Exchange mailbox and calendar
- A Planner board

NOTE: You cannot have a team within Microsoft Teams and a Yammer community connected to the same Microsoft 365 Group. It must be one or the other.

I think you get the picture; however, you may be thinking, what if I need more than one service? We did mention that:

> Microsoft uses Groups as a service to facilitate a shared experience across other Microsoft 365 services.

Well that is where we are going next!

As we have already stated, all Microsoft 365 Groups come with a mandatory SharePoint site, shared mailbox and calendar.

After that, the options of what collaboration services your group will use is entirely up to the owners and/or members using these workspaces, with the caveat that the various services and applications have been enabled and are allowed by your organization.

So, if you want to use Planner, you can. If you want to use Microsoft Lists, you can. If you want to use Microsoft Forms, you can. I think you see where we are going with this!

The underlying Microsoft 365 Group membership service determines who has access to the group's content and who does not. As long as you, and the people you are collaborating with belong to a Microsoft 365 Group, you can use anything within the tenant that is enabled and you are licensed for.

Microsoft 365 Group membership provides access to the following capabilities:

- Microsoft Teams
- SharePoint
- OneNote
- Dynamics 365
- Microsoft Sway
- Microsoft Lists
- Yammer
- Shared mailbox/ calendar
- Microsoft Forms
- Power Automate
- Power Apps
- Power BI
- Planner
- Whiteboard

It's worth mentioning again that a Microsoft 365 Group created from Yammer cannot have Microsoft Teams added to it or vice versa.

To get a clear understanding of what tools you get when you create a group, see Figure 1 on the next page (inspired by Matt Wade's infographic, "An Everyday Guide to Microsoft 365 Groups").

Figure 1: What tools you get when you create a Group

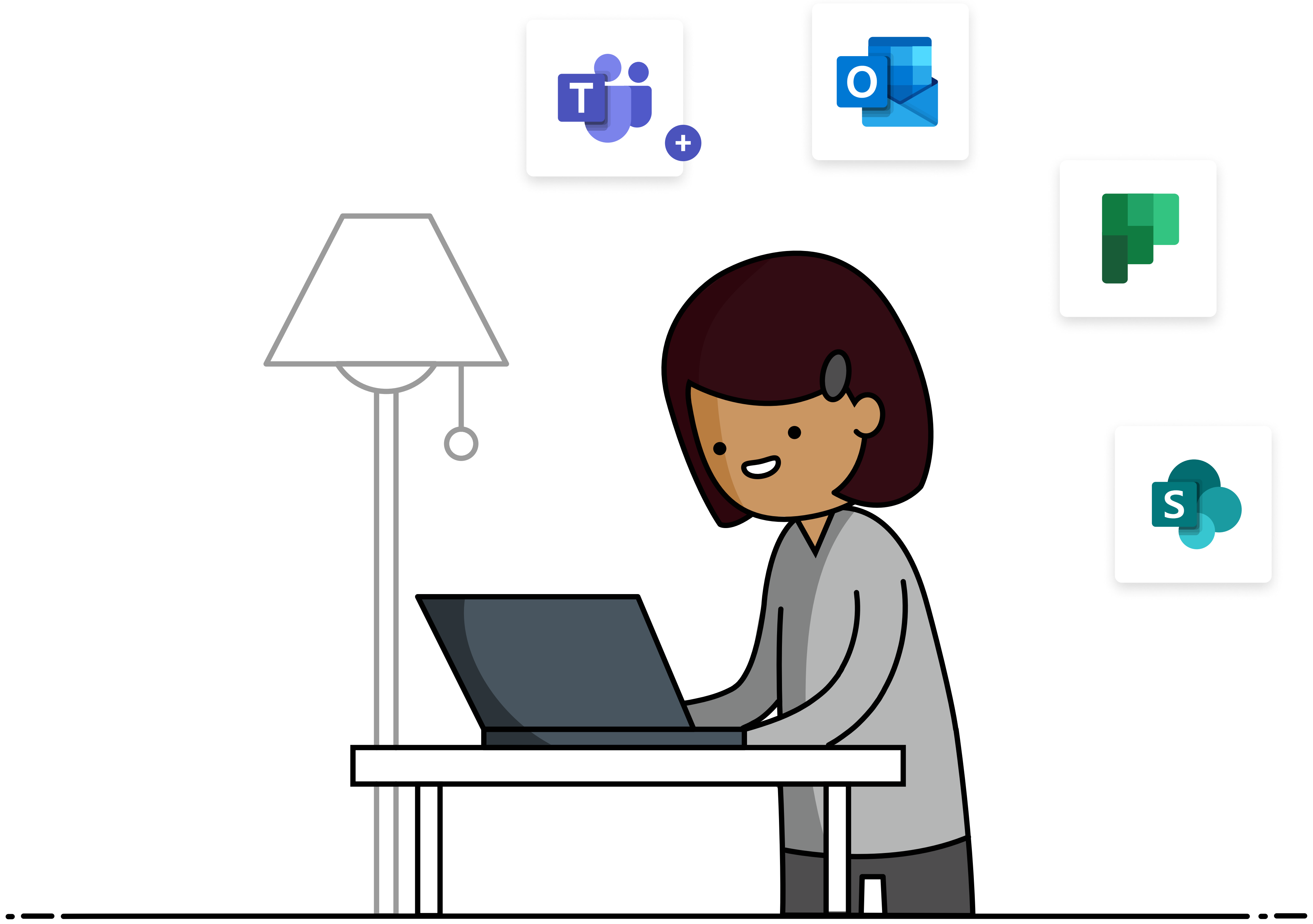
	WHERE ARE YOU CREATING A GROUP FROM?					
INCLUDED WITH YOUR CHOICE	Yammer	Teams	Stream	Planner	Outlook	SharePoint
Yammer feed Threaded discussions, questions, polling and shout-outs	✓	✗	✗			
Forms workspace Forms, surveys and questionnaires	✓	✓	✓			
OneNote notebook Online note-taking tool	✓	✓	✓			
Planner plan Simple project management tool	✓	✓	✓			
Power BI workspace Dashboards and business analytics	✓	✓	✓			
SharePoint site (the files tab) SharePoint document library and team site	✓	✓	✓			
Stream video portal Online video portal with transcription and facial recognition	✓	✓	✓			
Teams wiki Simple knowledge management tool	✗	✓	✗			
Teams chat Chat, bots, audio/video conferencing, channels and third-party app integration	✗	✓	✗			
Outlook inbox and shared calendar Email conversations, shared events and meetings in one central place	✗	✓	✓			

3.4

When do you create a Microsoft 365 Group?

As we stated previously, you'll end up with a Microsoft 365 Group every time a new collaboration workspace gets created. These spaces could be anything from a new Planner plan to a full-fledged team in Microsoft Teams.

In some situations, you may already have a Microsoft 365 Group that has only the shared mailbox, calendar and the SharePoint site, but you are considering adding a team within Microsoft Teams to it. At this point, you'll need to consider if the people within the existing Microsoft 365 Group membership are indeed the people you need to collaborate with.



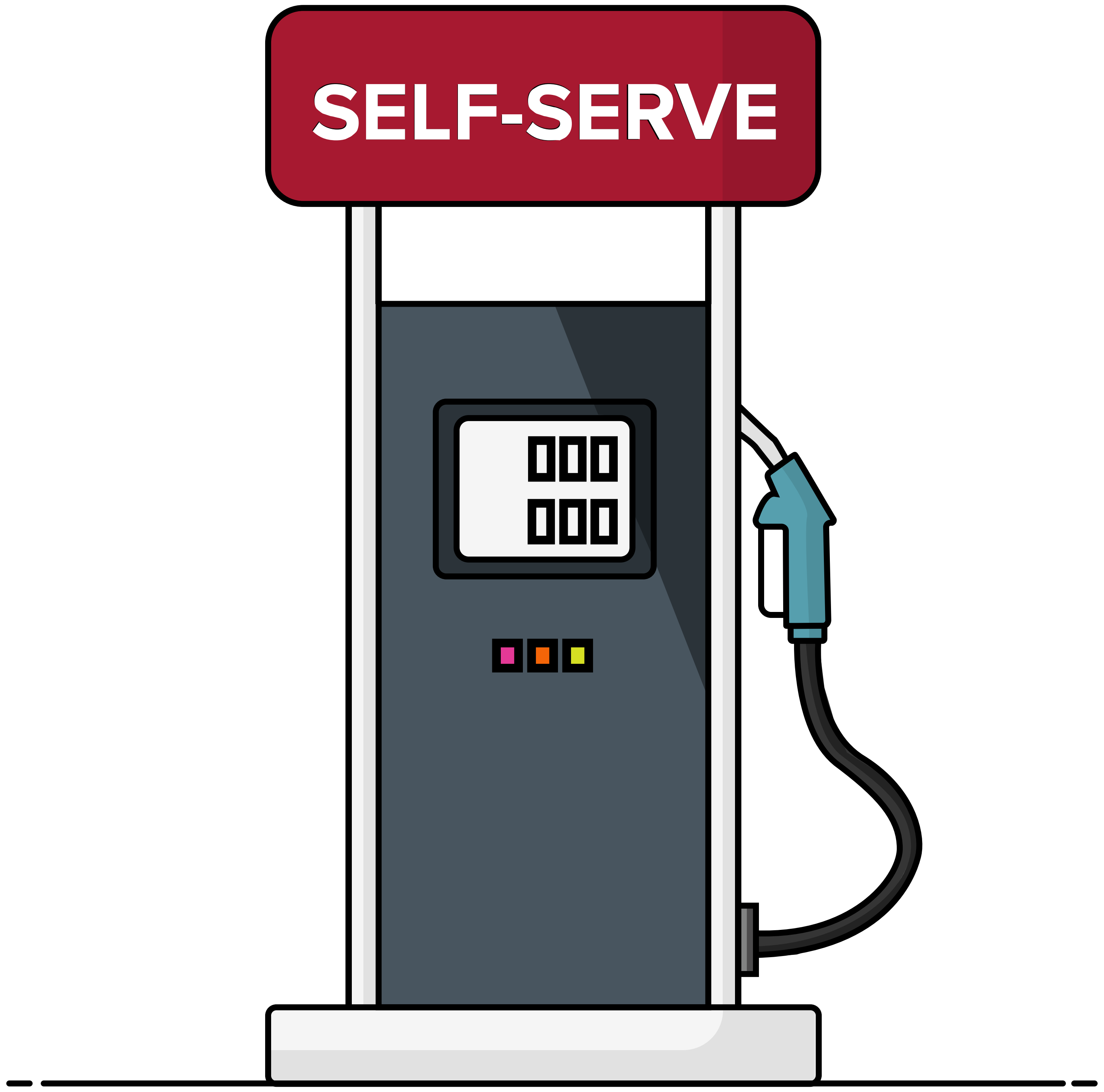
4.0

Controlling the Microsoft Teams provisioning process

One of the most common concerns with SharePoint and/or Microsoft Teams is how to avoid sprawl. In the early days of Microsoft Teams, Microsoft advised leaving the provisioning process wide open, or as many refer to it, “enabling self-service.” In theory this is great because you don’t want to limit a user’s ability to create collaboration spaces to get their work done, but eventually someone needs to be responsible for what is left behind.

To deal with this, IT would commonly turn off or restrict self-provisioning to avoid Microsoft Teams sprawl. Unfortunately, that decision ended up frustrating users and thus stifled adoption, as IT was often not able to provide a reasonable turnaround time on new requests.

During the pandemic in 2020, we noticed that many organizations chose to prioritize usage and adoption in support of working remotely over their concerns regarding sprawl.



We expect many organizations will regroup on this decision throughout 2021 as they reflect on the amount of growth or sprawl that has taken place. There are some legitimate reasons why you might consider adding more control over what is offered out-of-the-box.

For instance, you may want to:

- Introduce more flexibility to allow self-service creation in one workload and not the other. It might be okay in Microsoft Teams, but you want to lock it down in Yammer.
- Improve upon the out-of-the-box guidance or templated options available to users during the creation of a team within Microsoft Teams.
- Use your existing standardized service request platform (like ServiceNow for example) because it works well for your organization and is familiar to your users.
- Create a process that helps to identify business-critical teams or ones where special access for external users is required or not, or where you may be storing important records for the business.
- Offload the creation process to an admin account or service, so that way individual users do not have to worry about their Microsoft 365 Group creation limit (Microsoft currently limits 250 active Azure Active Directory objects – Microsoft 365 Groups, teams, Yammer communities, etc. – per individual account)

Our overarching advice for organizations worried about Microsoft Teams sprawl is to try, as best as they can, to embrace it. If you feel like there is a potential mess emerging that will erode the employee experience, then you should augment the basic capabilities through customization (PowerApps, PowerAutomate and PowerShell scripts, for example) or third-party software vendors.

When it comes to building something custom versus third-party alternatives, we prefer AvePoint's Cloud Governance product for Microsoft 365. If you're curious how AvePoint can help, contact us to learn more.

If you have the option of adopting a third-party tool, then you can tailor the front-end site provisioning process and implement richer controls that will better align with your organizational governance needs.

Let's take a closer look at the out-of-the-box approach compared to a custom forms-based process.

4.1

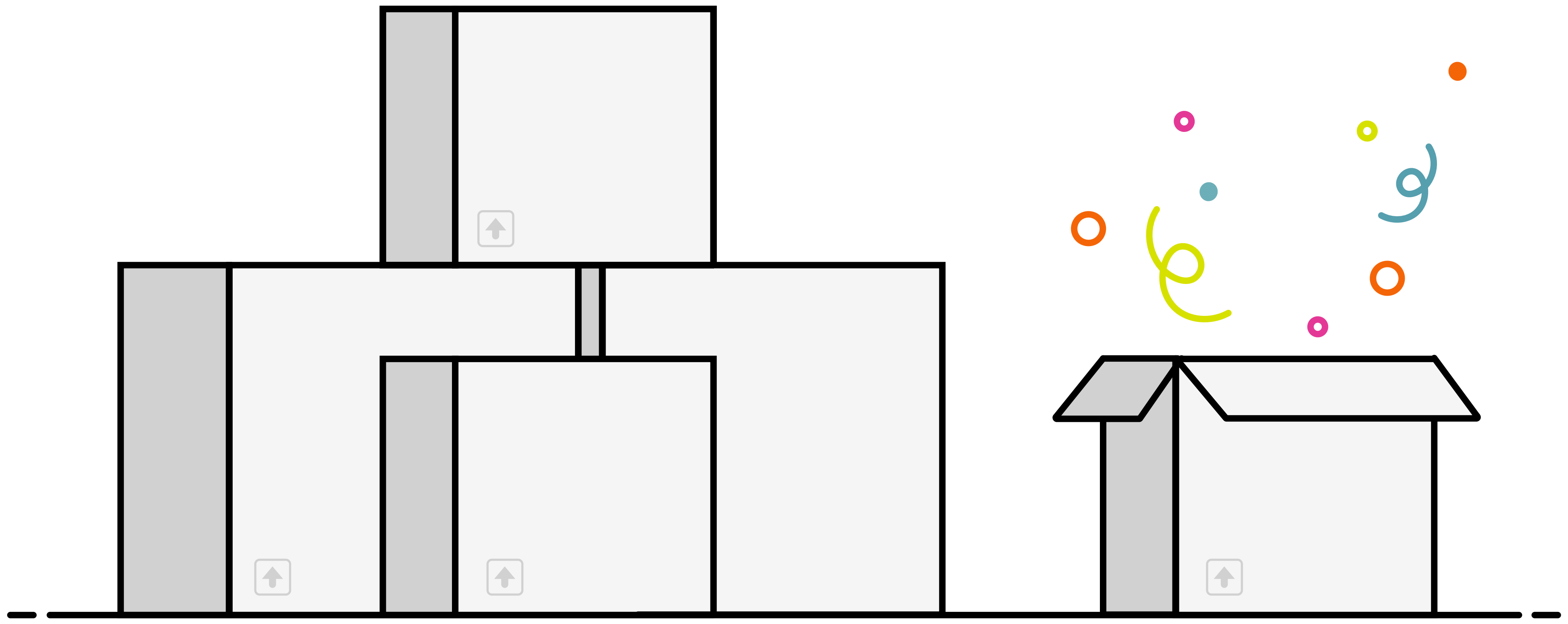
Managing the provisioning of Microsoft Teams using the out-of-the-box process

An out-of-the-box open provisioning process is the default in Microsoft Teams – for good reason. It is the simplest and fastest way to set up a provisioning process. You simply assign licences to your users and you are good to go. As a bonus, you can be sure that the solution will continue to work regardless of any changes or updates from Microsoft.

While this may be the fastest approach, it may not be the best for your organization if you have more complex governance requirements. Before you can determine if out-of-box provisioning will meet your organization's needs, you will need to evaluate the following:

- Guidance
- Available options
- Naming conventions
- Public vs private
- Automation vs approval

If any of these scenarios need to be tweaked, or you need to support more complex governance requirements, we recommend a customized forms-based process suggested in the next section.



4.2

Managing teams provisioning through a customized process

If the out-of-the-box provisioning process won't work for your organization, you can implement a request form using a tool like AvePoint Cloud Governance, PowerApps or ServiceNow. Keep in mind some of the following best practices we'd recommend when designing the request form.

Guidance
Provide helpful tips and guidance on different aspects of the team provisioning process.

FOR EXAMPLE

You can include a link to a helpful article on best practices for a team at the start of the form and encourage users to read (or watch a video on the topic) before proceeding further.

Available options
Ask for the business intent of the team (project, event, financial, etc.) and what type of work they will be doing. This information can be used to help users select the right type of site template for collaboration.

Naming conventions
The information provided during a guided provisioning process will support organizations implementing complex custom naming conventions.

Public vs private
The provisioning process can determine the default, recommended or even mandatory visibility value for every team based on what information the user provides.

Ownership
Governance may direct that every team has at least two owners, which could be easily enforceable using a custom provisioning process.

Self-service vs approvals
For most collaboration scenarios, employee self-service with automatic provisioning will meet the needs of the organization. However, there will always be instances where more complex collaboration scenarios (such as sensitive information, Guest Access, critical business processes, etc.) will require approval prior to provisioning, which can be easily integrated into a custom process.

So, while there are numerous benefits to implementing a custom provisioning process, a common drawback is that you will need to invest time and resources to ensure your solution is always compatible and up to date with Microsoft's updates.

What we recommend

Automate the provisioning process with AvePoint or ServiceNow.

Microsoft Teams provisioning

Essentially, all organizations have three basic provisioning options:

1. Out-of-the-box, employee self-service provisioning
2. Manual, centrally managed provisioning (like the IT department)
3. A customized, automated solution

We recommend automating the provisioning process with something like AvePoint or ServiceNow.

Leaving everything wide open can get very messy, very quickly and result in Microsoft Teams sprawl. If you funnel everything through a central group, the group can be seen as a bottleneck that hinders users from getting work done. It might seem like the best approach when you get started, but organizations should look to automate this process as soon as possible.

We feel automation is the best approach for most organizations because it offers the best of both worlds. Automation can manage complex organizational requirements, like naming conventions, and expiration policies, while also supporting workflows when oversight is required (for example, Guest Access).

NEXT UP: WHAT TO DO ABOUT NAMING CONVENTIONS

5.0

What to do about naming conventions

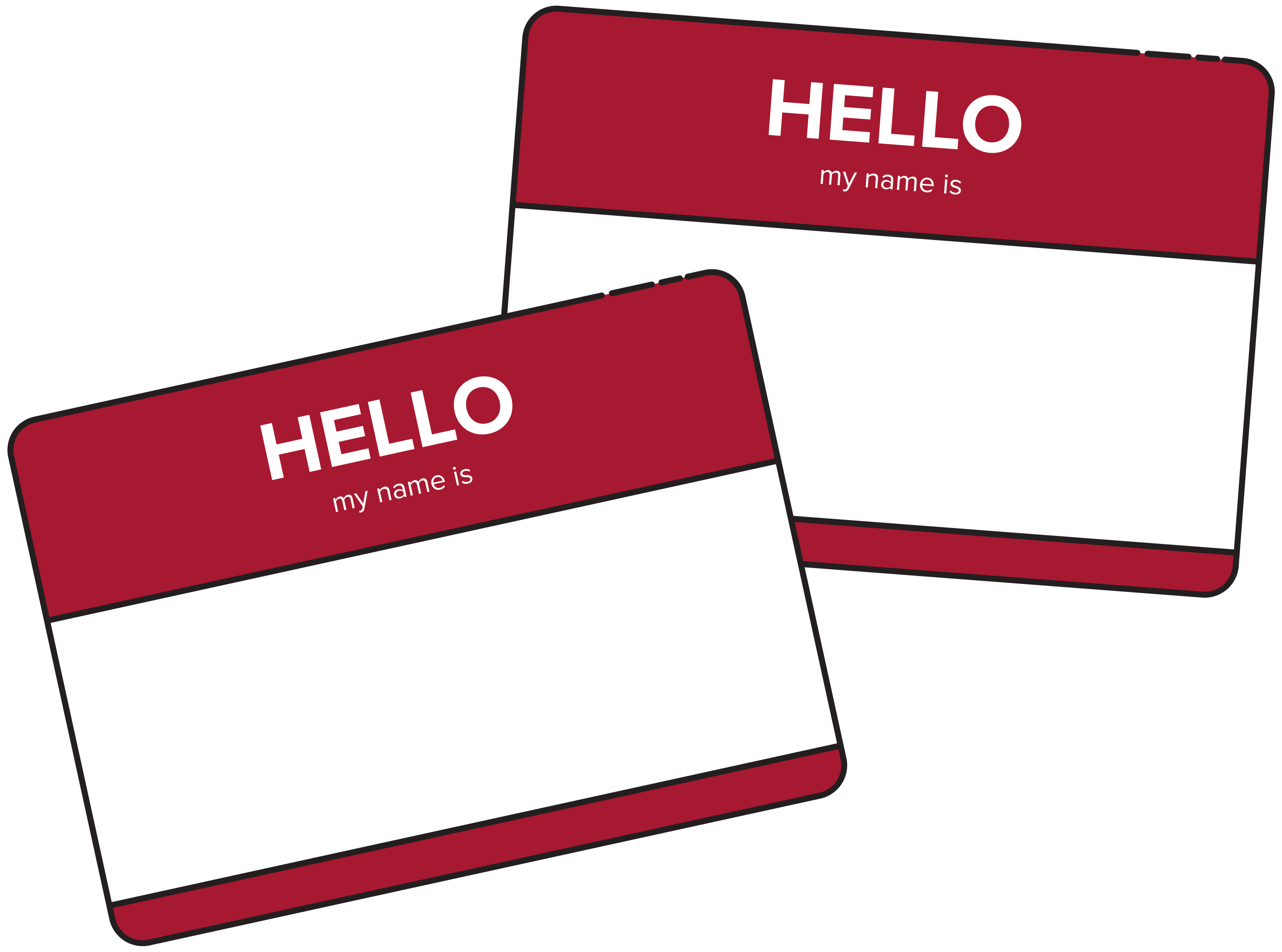
A naming convention is a governance element that often gets overlooked when it comes to Microsoft Teams. While there is no single approach that will work in every organization, with a little research you can often identify a usage pattern that can be supported with some naming logic.

Some common themes we see with naming conventions:

- You may want to consider using a prefix or suffix to identify if the site is internal or if it allows external sharing.
- You may want to indicate the type of site – for example, project, department or community.
- You may want to restrict the use of some reserved words – for example, HR, accusation, discipline, etc.
- You may want to indicate the type of information contained in the site – for example, confidential or restricted.

Implementing that naming convention is another story altogether. This is partly due to the out-of-the-box process that Microsoft offers and partly due to Microsoft 365's limitations on what an organization can and cannot control.

Let's explore some of the implementation options that are available.



5.1

Manual

Some organizations choose to adopt a manual naming convention that is flexible, while still aiming to maintain certain standards. In that case, you need to communicate and train your users to implement the desired naming convention.

The problem with this approach is there is no oversight to ensure that the naming convention is being followed by your users. Manual reviews will be required to support alignment with your governance policies. Remediation (renaming collaboration spaces) requires significant work and complete alignment may not even be possible.

To demonstrate this, here's an example of an organization that has implemented a naming convention where the type of collaboration is a prefix (in this case, Projects = PRJ), and External Access, if enabled, is a suffix (External = EXT).

If a site was provisioned using the name:

"ServiceNow Upgrade"

To remediate this and have the Microsoft Team named properly, it would need to be renamed:

"PRJ – ServiceNow Upgrade – EXT"

Renaming a team is simple, as any owner can rename the team using the Microsoft Teams application. But there are other issues that require manual remediation to keep your environment consistent.

FOR EXAMPLE

Manually renaming a team:

- ✕ Will not update the Microsoft 365 Group email address (SMTP alias), but it can be manually remediated via PowerShell.
- ✕ Will not automatically change the connected SharePoint Online site URL, but it can be manually remediated from within the SharePoint Online admin centre.
- ✕ Will not update shared links. If the SharePoint Online site URL is updated to match the new naming, all links that have been shared will now be broken.

If these manual remediations are not completed, this will impact the administrators tasked with support (like looking up a site name after a user has changed it).

There is a way to implement some automation and structure using administrative controls through the Azure Active Directory group naming policy.

5.2

Semi-automatic

Naming conventions don't have to be manual or customized. There is a solution in the middle, which may be just enough for your organization: the Azure Active Directory group naming policy. But it also has its limitations:

- A group naming policy applies to all of Microsoft 365 and cannot be selectively applied to Microsoft Teams–based Groups. So, if you want to add a "Teams" prefix to all Microsoft Teams–based groups automatically, you can't do this.
- It can add a user-defined, static (non-selectable) prefix or suffix term to a team name.
- There are certain Active Directory attributes that can be added dynamically to group names. Administrators can bypass these, but users don't have a choice. For example, you can add the department attribute as a suffix. Then, whenever an end-user creates a Microsoft 365 Group (not just a team), their group will have their department in Active Directory added to the group name.

FOR EXAMPLE

A team created with name "Contoso Teams Rollout" (which may include stakeholders from IT, finance and human resources) would become "Contoso Teams Rollout – Finance," if my department (as the creator) were set as "finance" in Azure Active Directory. You can see how this may have limited benefit, especially if you want cross-departmental teams, or you want to have people create teams on others' behalf.

- It does have one advantage in that your team (or group) owners cannot rename their teams/groups to remove the prefix/suffix after creation.
- You can choose to upload a list of blocked words to your tenant. These words are not allowed to be used in team/group creation. Profanity is an obvious example of what you may want to limit, but you can add other words, such as department names like "HR" or "Human Resources."

It is important to note that for each unique user who is a member of one or more Microsoft 365 Groups (within your organization), you will need to have Azure Active Directory Premium P1 or an Azure Active Directory Basic EDU licence to leverage this functionality.

You can read more about group naming policies and custom blocked words in Microsoft Docs.

5.3

Automatic

Naming conventions should always rely on conditional logic. Unfortunately, the current out-of-the box capability, which leverages the Azure Active Directory group naming policy, does not have the ability to support conditional logic in naming conventions.

This means if your organization wants to implement a naming convention that has conditional logic (such as, is this team for a department or a project?) then you need to implement a custom process.

A naming convention that leverages conditional logic can easily be added to an organization's custom provisioning process. This way, when you guide your users through the process and collect the information required to support your provisioning governance, you can leverage this information to implement the naming convention as well.

To illustrate this, let's look at our previous example of creating a team called "Contoso Teams Rollout":

- If the collaboration space were to support a training opportunity, we would automatically use a prefix of "TRA."
- But, if the collaboration space were to support a project, we would automatically use the prefix of "PRJ."
- In both of those cases the department of the user provisioning the site is irrelevant and should not be part of the naming convention.
- If the project team includes external resources, we will automatically add the EXT suffix.

The above example can also be used to illustrate the ease of alignment with organizational governance policies by indicating the sensitivity of the information the collaboration space will contain, which could be represented by symbols like locks or keys, as required.

If, as an organization, you require a naming convention policy that has strict controls around it and your naming convention has logic built into it, you will need to use a third-party solution to manage it. Some of these solutions can even inspect sites that were already provisioned and report on exceptions.

As in the custom provisioning process, while there are numerous benefits to leveraging an automated process for naming conventions, a common drawback is that you will need to invest time and resources to ensure your solution is always compatible and up to date with updates that Microsoft will make. Furthermore, as organization governance plans are forever evolving, the custom processes used will need to be updated accordingly to keep them relevant.

What we recommend

Start with a strategy that includes a prefix and a suffix when required.

Naming conventions

We recommend starting with a strategy that includes a prefix and a suffix when required. This helps users who are part of multiple teams understand the owner and intent of the site, and administrators who have to manage hundreds if not thousands of Microsoft 365 Groups and/or teams.

For prefixes, we recommend organizations use something short (two or three characters) that represent the type/purpose of the team.

For departments, something like:

[Department Name] – [Title/Name]

HR – Compensation

HR – Recruiting

IT – Network

IT – Infrastructure

COR – Legal

COR – Communications

For projects, something like:

[Project Abbreviation] – [Project Name]

PRJ – Exchange Migration

PRJ – Corporate Website Upgrade

PRJ – Company Rebranding

For suffixes, we recommend an even simpler convention that just adds an EXT to the end of the Microsoft 365 Group and/or team if Guest Access is enabled. This way, all stakeholders (admins, owners and members) can see that the information stored here is accessible by external parties. This helps them know what kind of content can be stored in this location.

NEXT UP: EXTERNAL AND GUEST ACCESS

6.0

External and guest access

This is a topic that creates a lot of confusion because of the terminology used, so it is helpful to review the terms and explain the expected behaviour of these configuration options.

6.1

External access in Microsoft Teams

✓ **What it is**

External Access allows your users to communicate with other organization's users. You can, of course, control the domains that your end-users can communicate with. In Skype for Business or Lync terminology, this is called federation. Also, both organizations need to be configured to allow federation if they wish to communicate with each other.

☒ **What it is not**

External users will not have access to teams and channel information.

You can, within the Microsoft Teams admin center, specify the level of External Access your organization wants to allow.

Open federation

This is the default option, which allows communication with all domains. We recommend revisiting this configuration and confirming this is the desired outcome for your organization.

FOR EXAMPLE

Anyone can communicate with anyone.

Allow specific domains

The Microsoft Teams administrator will configure the Allow list with the domains that should be allowed for External Access. All other domains will be blocked.

FOR EXAMPLE

ACME.com is added to your organization's Allow list. This means all users from ACME.com can communicate with all users within your organization, but your users can only communicate with ACME.com.

Block specific domains

The Microsoft Teams administrator will configure the Block list with the domains that should not be allowed for External Access. All other domains will be allowed.

FOR EXAMPLE

ACME.com is added to your organization's Block list. This means all users from within your organization can communicate with everyone except for ACME.com.

6.2

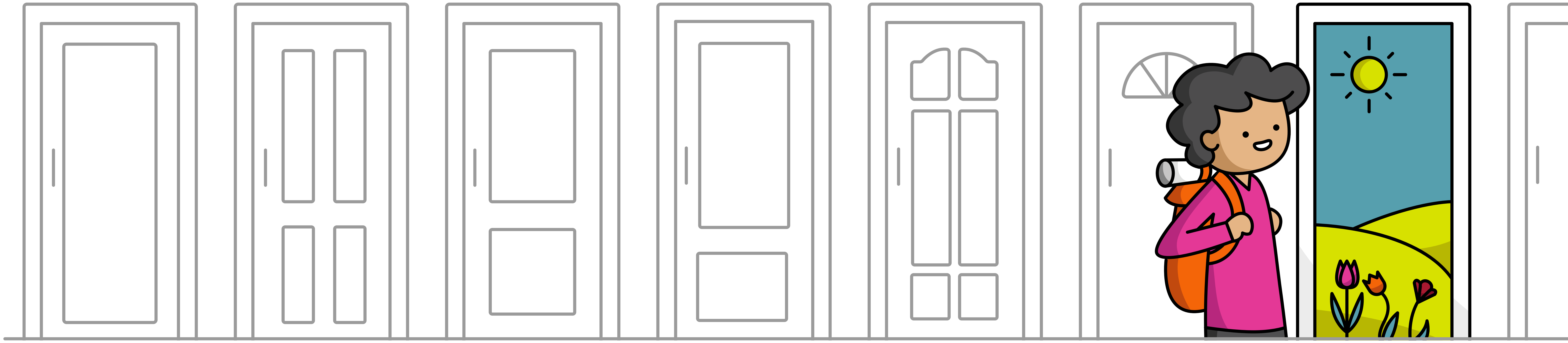
Guest access

✓ **What it is**

Guest Access allows you to add members of other organizations (or even non-organizational users with personal email accounts) to your teams within Microsoft Teams, where they have access to certain team resources like files and conversations. It is for collaborating and sharing resources stored within a team.

⊗ **What it is not**

This is not meant to be used for chatting with users from other organizations. That is External Access.



If Guest Access is enabled for your tenant and Microsoft Teams, then by default, users can invite guests from any organization and even from non-business domains like Gmail or Proton Mail. However, there is an option available for your organization to allow or deny specific domains in Azure Active Directory's business-to-business sharing.

Generally, you get five Guest Access licences for each licensed user of Microsoft 365. So, your organization is limited (though quite generously) in how many guests it can have on its tenant.

FOR EXAMPLE

If you have Guest Access enabled and have allowed ACME.com through Azure Active Directory's busines-to-business sharing settings (but not External Access), only the members of ACME.com who are added to at least one team in your organization can only see the files and conversations for the team that they are added to (or multiple teams, if they are added to multiple teams). They can chat only with other members of the teams to which they belong. Also, each unique guest user will only use a single Guest Access licence, regardless of how many teams they are members of.

We recommend you keep your implementation as open as feasible unless you are in a highly regulated industry where data loss can create huge liabilities for the organization. However, even in that case, you can mitigate the data-loss scenarios using Microsoft 365's DLP (data loss prevention) policies that are available in the Security and Compliance Center.

You can read more on External Access and Guest Access in Microsoft Docs.

What we recommend

For External Access, leave the default setting of Open Federation as-is.

For Guest Access, only enable the functionality with organizations you trust.

External access

We recommend that you leave the default setting of Open Federation as-is. This helps your users communicate with everyone else using Microsoft Teams. This does not give other organizations access to your content; that is configured with Guest Access.

Guest access

We recommend that you enable this functionality but only with organizations that you trust. You can do this by maintaining a list of trusted domains in Azure Active Directory, so your users can invite users from these domains to collaborate.

We also recommend only enabling this for teams where required. You can support this through the SharePoint admin center, PowerShell scripts or third-party tools.

NEXT UP: SETTING A MICROSOFT TEAMS EXPIRATION POLICY

7.0

Setting a Microsoft Teams expiration policy

You can keep inactive teams in-check and control sprawl with the Microsoft 365 Groups expiration policy. This out-of-the-box feature enables administrators to set an expiration policy (in days) for all Microsoft 365 Groups (which of course includes Microsoft Teams).

Active Microsoft 365 Groups are renewed automatically. Activity is defined as someone visiting a Microsoft Teams channel or performing an action on the underlying SharePoint site (like reading, editing or searching for a document).

Inactive Microsoft 365 Groups must be renewed by one of the group owners.

FOR EXAMPLE

If you set the group lifecycle to be 180 days, then each Microsoft 365 Group will come up for renewal roughly every six months. Inactive group owners will get up to three notifications to renew their group:

- 🔔 Renewal notification 1: 30 days prior to expiration
- 🔔 Renewal notification 2: 15 days prior to expiration
- 🔔 Renewal notification 3: 1 day prior to expiration

All they must do to renew the group for the next period is act on one of those notifications. If they fail to act or if the group is no longer needed, it is soft deleted (can be recovered) for approximately the next 30 days. If no action is taken beyond that timeframe, the group and all associated services (like the team and SharePoint site) will be permanently deleted.

While this is a great feature for keeping outdated Microsoft 365 Groups and teams in check, it does have some limitations that can pose a significant challenge for many organizations to overcome:

- At the time of writing, there can only be one group expiration policy per Microsoft 365 tenant. This policy can be applied to:
  - All groups in your organization
  - None of the groups in your organization
  - Selected groups in your organization (manually assigned)
- You cannot have different expiration policies for groups within different apps.

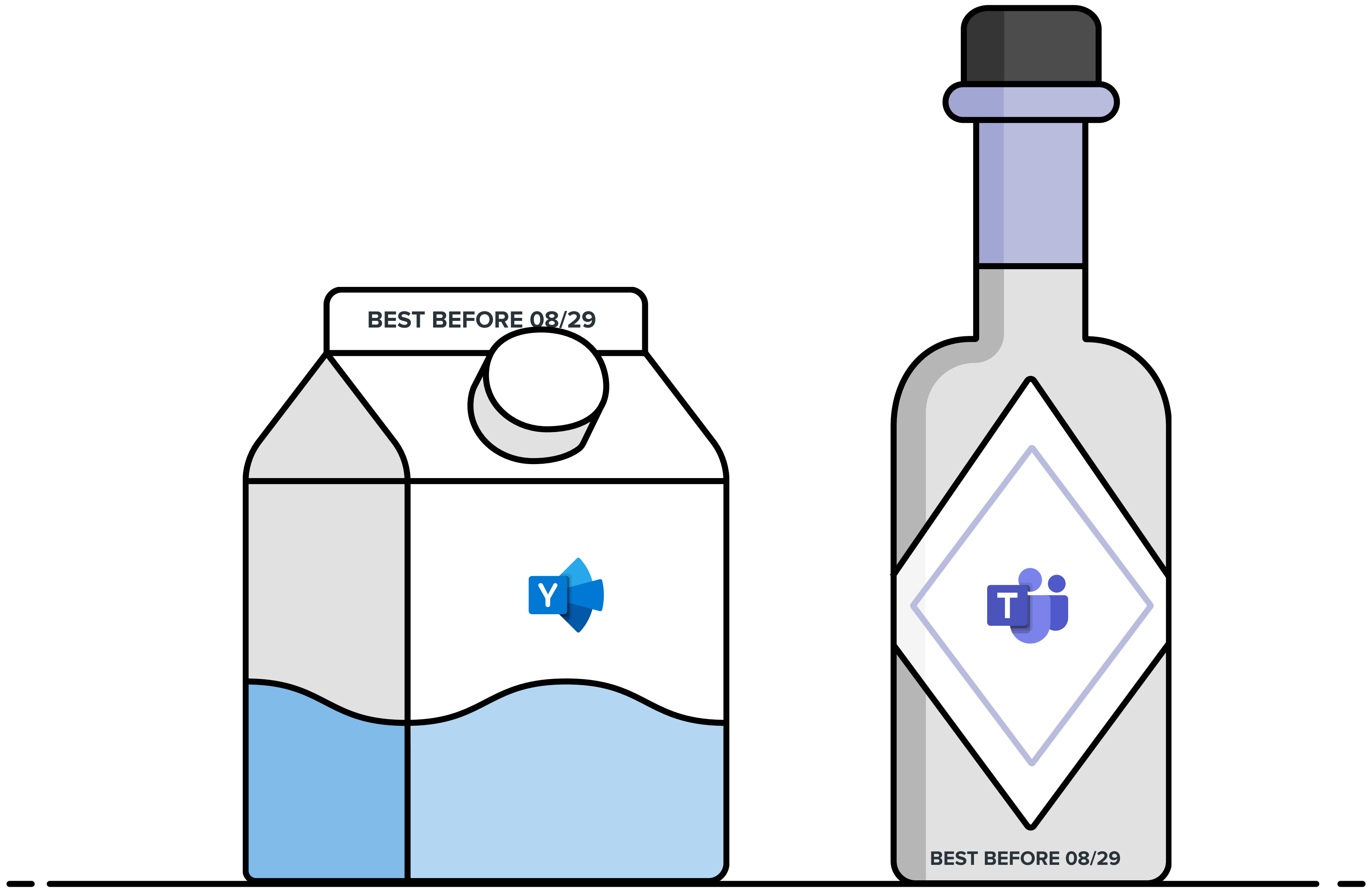
FOR EXAMPLE

You can't set the renewal for Microsoft 365 Groups created from Yammer to three years and Microsoft 365 Groups created from Microsoft Teams to 180 days.

If your organization has more complex lifecycle requirements for your Microsoft 365 Groups, you will have to leverage custom capabilities that are only found within a third-party solution.

You can learn more about the Microsoft 365 Groups expiration policy in Microsoft Docs.

NOTE: Microsoft 365 security and compliance retention policies still apply to groups. They are separate from and trump expiration policies.



What we recommend

Consider implementing a Microsoft 365 Group expiration policy (that includes Microsoft Teams) of at least 180 days to start.

Microsoft Teams expiration

We recommend that all organizations consider implementing a Microsoft 365 Group expiration policy (that includes Microsoft Teams) of at least 180 days to start.

If your organization requires more flexibility to support lifecycle management, you will need to invest in a third-party solution.

NEXT UP: MICROSOFT TEAMS ARCHIVAL

8.0

Archiving teams

The process of archiving a team (along with the apps and services associated with it through the Microsoft 365 Group) changes the state of the team to read-only. This means that everyone can still access the information but can no longer make any further changes. This includes everything from posts and comments to files and workflows.

The only adjustments that can be made are in relation to access permissions and archival status. This means that owners of the team can only:

1. Add/remove individuals to access the read-only content
2. Switch the team back to an active state, which would make all information writable again

A real-world example we see from organizations for archiving teams is projects. When teams are used to support projects, we know that they will at some point be closed out. This does not mean that the information contained within this space is no longer needed. Quite often project managers and stakeholders may want to refer to a closed project to view documentation, budgets, planning and decisions. You do not want this information to be editable but want it available for historic purposes.

To keep it active, team owners still need to follow the rules of the Microsoft 365 Group expiration policy.

9.0

Additional configuration options to consider

There are other controls and policies available within the Microsoft Teams administration interface that can help you govern specific aspects of your Microsoft Teams implementation.

9.1

Cloud file storage options

By default, Microsoft Teams allows the use of various cloud storage services from the file tab. Your users will automatically have access to their OneDrive for Business files, but they will have the option to add additional cloud storage accounts to this area by default. The services include Dropbox, Box and Google Drive, just to name a few.

If you want to disable these services and not give users the ability to add them, you can turn them all off, except OneDrive for Business.

If you are trying to keep your information contained within the Microsoft 365 environment so it is covered by organizational data loss prevention (DLP) policies, turn off these third-party services.

9.2

Allowed apps policy

There are three categories of apps that can be added to Microsoft Teams:

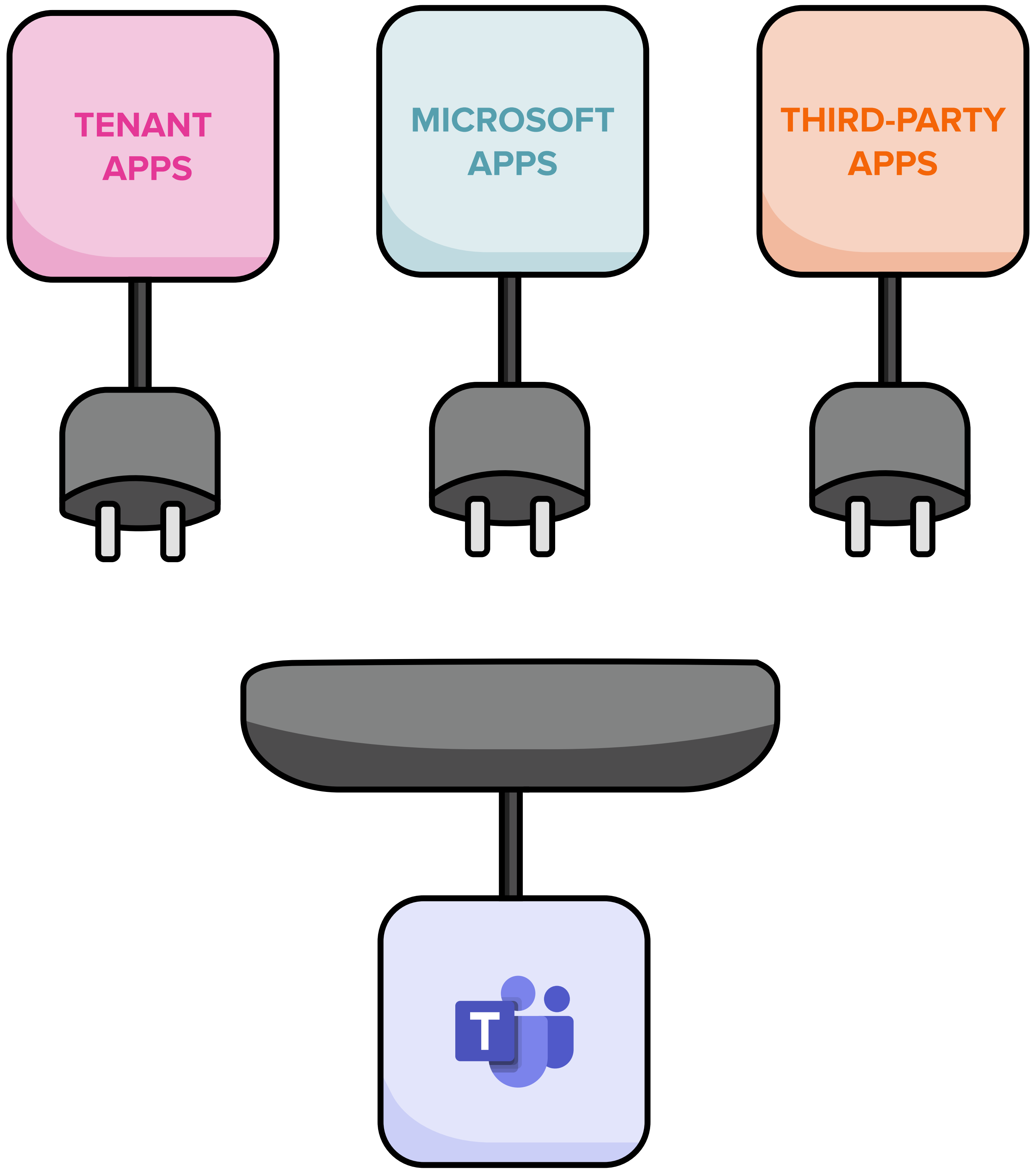
1. **Microsoft apps:** Apps created and published by Microsoft to be used in Microsoft Teams for Microsoft 365 services
2. **Third-party apps:** Apps published by third parties in the Microsoft Teams store (for example, Trello or Zoho)
3. **Tenant apps:** Custom apps uploaded to your tenant

In each category, you can choose to allow:

- All available apps
- No apps
- Specifically selected apps

You can also create and apply multiple policies to different end-users in your organization if they have different licences/entitlements for usage.

As a rule, for the **Microsoft** app category, we recommend you allow the use of Microsoft apps and keep this access aligned with the licences/entitlements available to end-users. For **third-party** and **tenant apps**, those decisions need to be made based on organizational requirements.



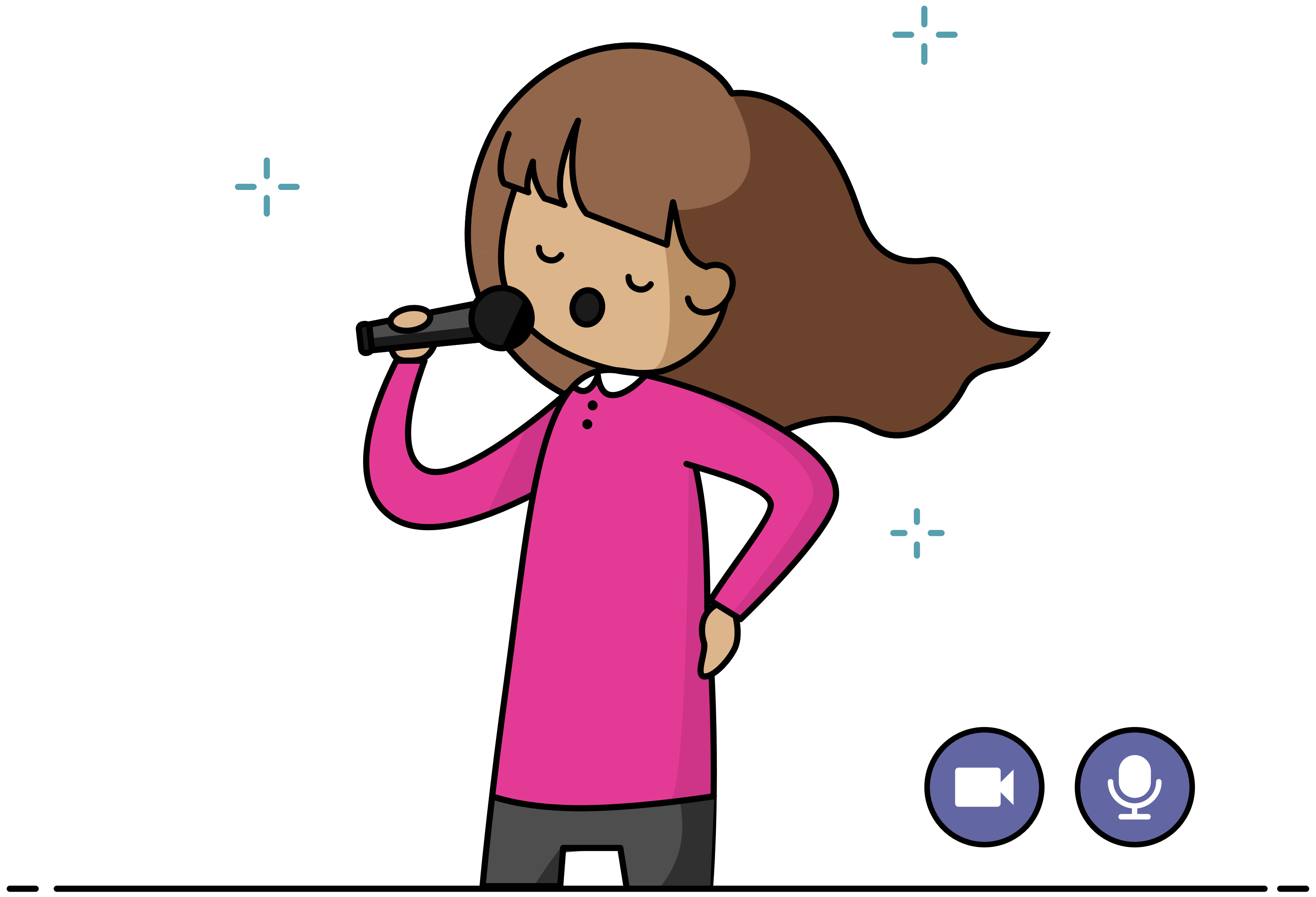
9.3

Live events

Out of the box, all your users can schedule, record and join live events from Microsoft Teams. But you can create and assign live event policies to trim which options for live events are available to certain groups of users within your organization.

FOR EXAMPLE

- You could lock down the ability to schedule and record live events for most of your organization's users but still allow them to join.
- Then through another policy, anyone in communications could have the ability to schedule, record and join a live event; for example, to help facilitate a town hall.



9.4

Data loss prevention and mobile device management

Data loss prevention (DLP) is sometimes confused with disaster recovery (backup and restore). It can be helpful to think of DLP as data “leak” prevention, where you prevent accidental or intentional disclosure of proprietary or sensitive information.

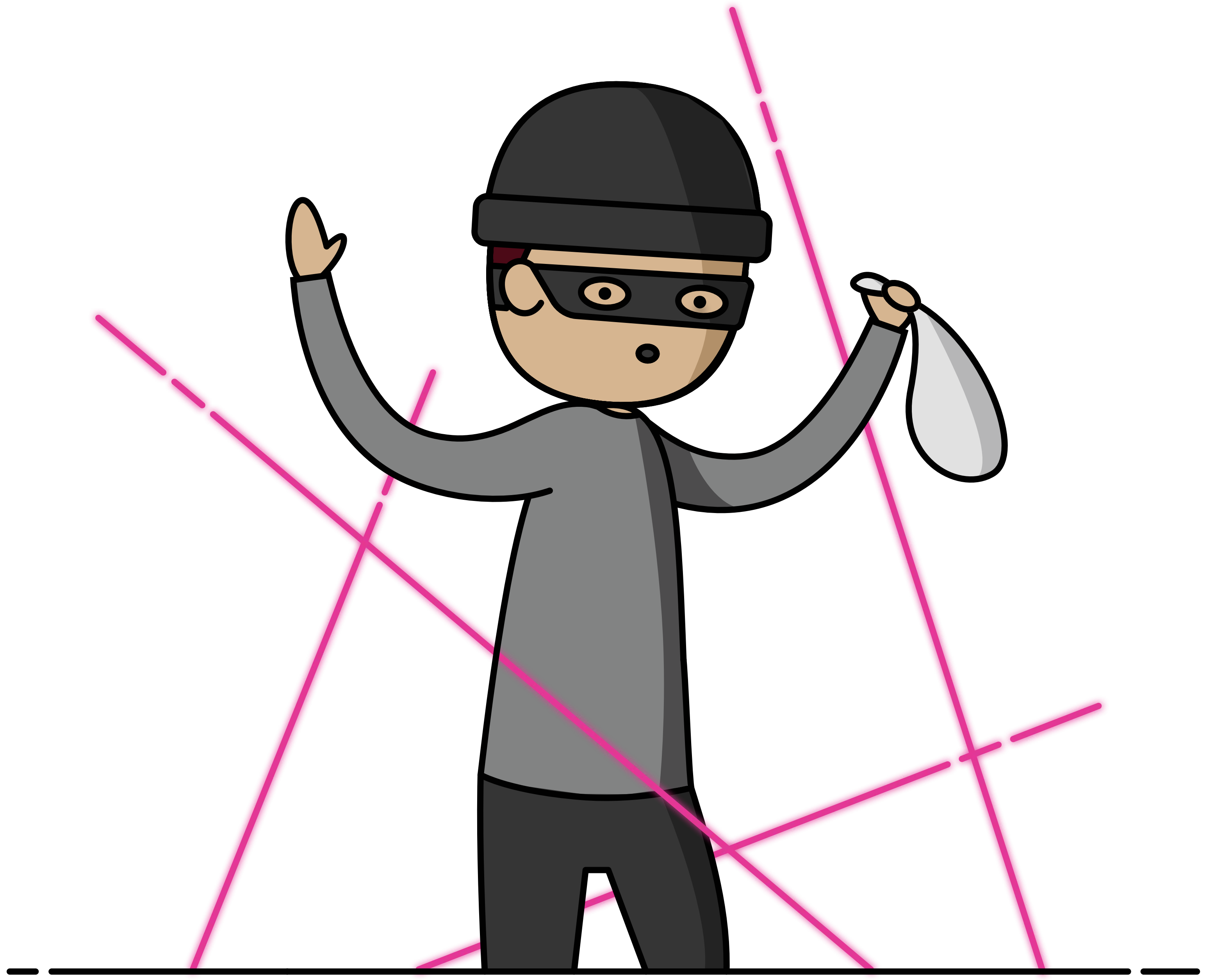
Mobile device management policies control access for corporate mobile devices and can deal with BYOD (bring your own device) scenarios to mitigate data leaks or losses.

Both controls operate at a higher level in the tenant than Microsoft Teams. There are very easy-to-implement DLP templates that cover patterns for common private and financial information types and that enable you to either prevent or warn users, administrations and/or the information management team when they are dealing with sensitive information covered by a policy.

FOR EXAMPLE

Templates exist for identifying credit card and social insurance numbers across Microsoft 365 services (Exchange, SharePoint, Microsoft Teams, etc.) and can trigger alerts and warnings or outright block users from sharing this information with external parties.

You can read more about Data Loss Prevention (DLP) and Mobile Device Management (MDM) in Microsoft Docs.



What we recommend

Enable all Microsoft apps your organization is licensed for.

Microsoft Teams apps

By default, Microsoft, third-party and custom apps are allowed.

We recommend enabling all Microsoft apps that your organization is licensed for. We know that the information stored within these apps are safe and secure.

If your organization has vetted or invested in other services or platforms (like Salesforce or ServiceNow), we recommend enabling these individual third-party apps as well.

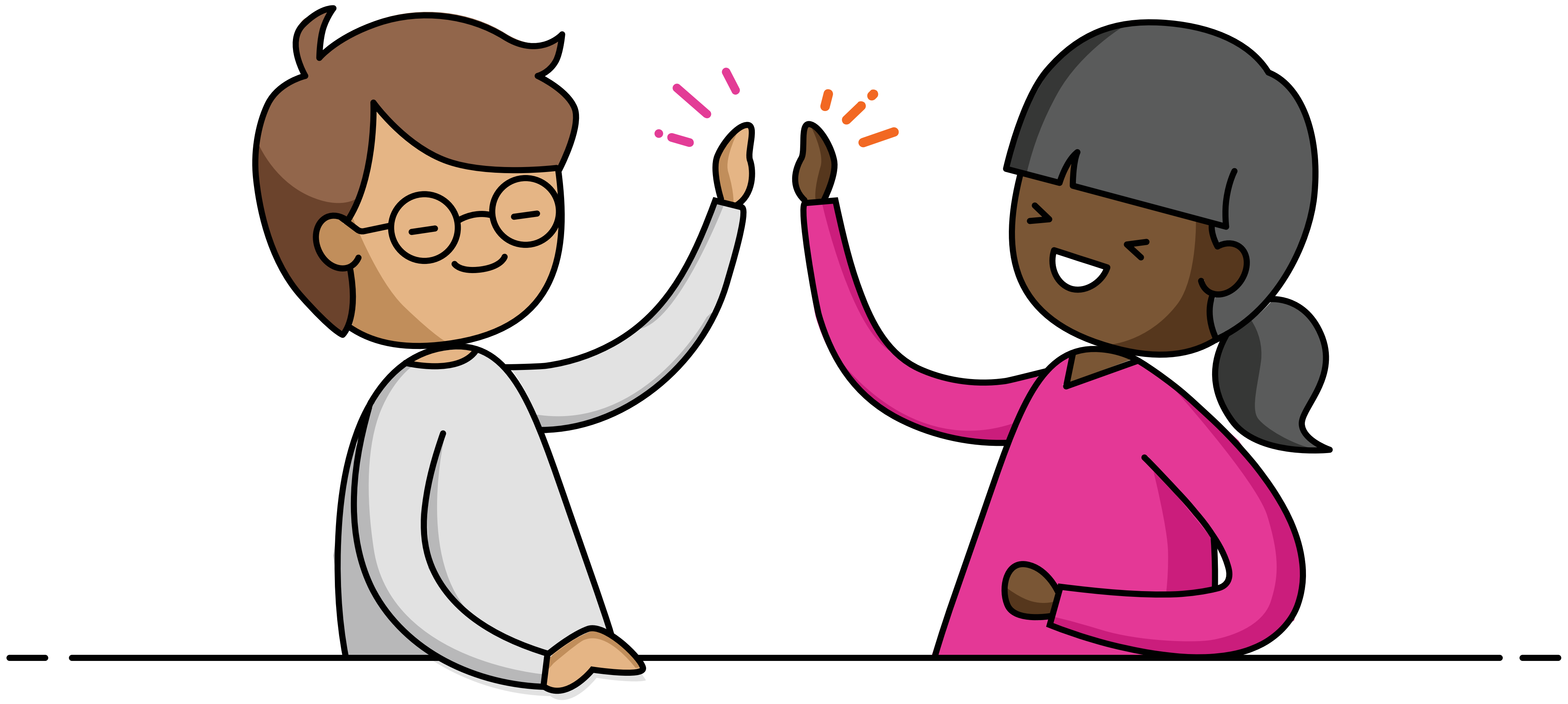
When it comes to custom apps, we don't see any harm in allowing them, because Microsoft Teams administrators are the only people who can add them to your tenant.

10.0

Conclusion

Microsoft Teams is a powerful tool for communication and collaboration. By taking some time to understand its relationship with Microsoft 365 and your configuration options, you can greatly simplify and streamline the rollout process.

While we recommend you take the time to consider your own requirements, we hope the information in this guide helps serve as a starting point for your Microsoft Teams journey. If you'd like more support, our digital workplace consultants can help you develop a configuration and governance model that sets you up for long-term success.



Get in touch

If you have questions or want to learn more about how to get Microsoft Teams working better for you, let us know. We'd love to talk.

1-866-841-6201

habaneroconsulting.com

Let's get social!

HabaneroConsulting

HabaneroConsult

in Habanero Consulting Group

habanero

habanero