3.2 I can assess what permissions are needed for different users and content

Evidence: Descriptions in plans preparing their projects. Setting up real accounts on a collaborative site

**Sharing and permissions in the SharePoint modern experience**

* Article
* 03/21/2022
* 7 minutes to read
* 15 contributors

Traditionally, SharePoint permissions have been managed through a set of permissions groups within a site (Owners, Members, Visitors, etc.). In SharePoint in Microsoft 365, this remains true for some types of sites, but additional options are available and SharePoint is part of a much broader set of capabilities for [secure collaboration with Microsoft 365](https://docs.microsoft.com/en-us/microsoft-365/solutions/setup-secure-collaboration-with-teams).

The main types of sites in SharePoint are:

* **Team sites** - Team sites provide a collaboration environment for your teams and projects. Each team site, by default, is part of a Microsoft 365 group, which includes a mailbox, shared calendar, and other collaboration tools. Team sites may also be part of a team in Microsoft Teams. Permissions for team sites are best managed through the associated Microsoft 365 group or Teams team.
* **Channel sites** - Channel sites are team sites that are associated with a specific channel in a Teams team. Both private and shared channels create separate SharePoint sites just for the channel.
* **Communication sites** - Communication sites are for broadcasting news and status across the organization. Communication site permissions are managed by using the SharePoint Owners, Members, and Visitors groups for the site.
* **Hub sites** - [Hub sites](https://docs.microsoft.com/en-us/sharepoint/planning-hub-sites) are team sites or communication sites that the administrator has configured as the center of a hub. They're designed to provide connection between related sites through shared navigation. Permissions for hub sites can be managed through the Owners, Members, and Visitors groups, or through the associated Microsoft 365 group if there is one. Special permissions are needed to associate sites to a hub.

**Team site permissions and Microsoft 365 Groups**

By default, each SharePoint team site is part of an [Microsoft 365 group](https://support.office.com/article/b565caa1-5c40-40ef-9915-60fdb2d97fa2). a Microsoft 365 group is a single permissions group that is associated with various Microsoft 365 services. This includes a SharePoint site, an instance of Planner, a mailbox, a shared calendar, and others.

When you add owners or members to the Microsoft 365 group, they're given access to the SharePoint site along with the other group-connected services. Group owners become site owners, and group members become site members.

It's possible to manage SharePoint site permissions separately from the Microsoft 365 group by using SharePoint groups, unless it's a channel site. However, we recommend against it. In such a case, group members will continue to have access to the site, but users added directly to the site won't have access to any of the group services. The exception is view-only access - Microsoft 365 groups don't have view-only access, so any users you wish to have view permissions on the site must be added directly to the Visitors group on the site.

**Note**

When you create a new team or private or shared channel in Microsoft Teams, a team site in SharePoint gets automatically created. To edit the site description or classification for this team site, go to the corresponding channel’s [**settings in Microsoft Teams**](https://support.microsoft.com/office/change-a-team-s-data-security-classification-in-teams-bf39798f-90d2-44fb-a750-55fa05a56f1d).

**Using team sites with Teams**

Microsoft Teams provides a hub for collaboration by bringing together various services including a SharePoint team site. Within the Teams experience, users can directly access SharePoint along with the other services. Each team is associated with a Microsoft 365 group and Teams uses that group to manage its permissions.

For scenarios where a SharePoint site is used with Teams, we recommend doing all permission management through Teams. As with Microsoft 365 groups, team owners become site owners and team members become site members.

For private or shared channel sites, permission management must be done in Teams. Channel owners become sites owners in SharePoint and channel members become site members. Permissions in SharePoint can't be managed separately.

For details about how SharePoint and Teams interact, see [Overview of Teams and SharePoint integration](https://docs.microsoft.com/en-us/sharepoint/teams-connected-sites) and [Manage settings and permissions when SharePoint and Teams are integrated](https://docs.microsoft.com/en-us/sharepoint/manage-teams-sharepoint-experiences).

**Communication site permissions**

Communication sites aren't connected to Microsoft 365 groups and use the standard SharePoint permissions groups:

* Owners
* Members
* Visitors

Normally with communication sites, you'll have one or more owners, a relatively small number of members who create the content for the site, and a large number of visitors who are the people you're sharing information with.

You can give people permissions to the site by adding individual users, security groups, or Microsoft 365 groups to one of the three SharePoint groups. (Nested security groups can cause performance issues and are not recommended.)

If a communication site is used by members of a team in Teams, you may want to add the Microsoft 365 group associated with the team to the members group of the communication site. This will allow members of the team to create content in the communication site.

The visitors group is a good place to use security groups. In many organizations, this is the easiest way to add large numbers of users to a site.

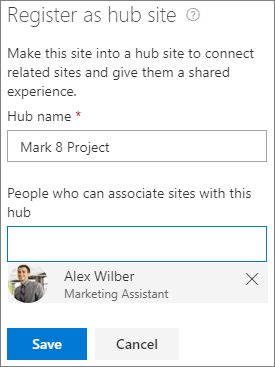
For information about how to share a site, see [Share a site](https://support.microsoft.com/office/958771a8-d041-4eb8-b51c-afea2eae3658).

**Hub site permissions**

Managing the permissions of a hub site is dependent on the underlying type of site. If the site is a group-connected team site, then you should manage permissions through the Microsoft 365 group. If it's a communication site, then you should manage permissions through the SharePoint groups.

Hub site owners define the shared experiences for hub navigation and theme. Hub site members create content on the hub as with any other SharePoint site. Owners and members of the sites associated with the hub create content on their individual sites.

The SharePoint admin must specify which users can connect other sites to the hub. This is done in the [SharePoint admin center](https://go.microsoft.com/fwlink/?linkid=2185219) and cannot be changed by site owners.



**Shareable links**

Giving people permissions to a site, group, or team gives them access to all site content. If you want to share an individual file or folder, you can do so with shareable links. There are three primary link types:

* *Anyone* links give access to the item to anyone who has the link, including people outside your organization. People using an *Anyone* link don't have to authenticate, and their access can't be audited. *Anyone* links can't be used with files in a Teams shared channel site.
* *People in your organization* links work for only people inside your Microsoft 365 organization. (They don't work for guests or external participants in Teams shared channels).
* *Specific people* links only work for the people that users specify when they share the item. For files in a Teams shared channel site, *specific people* links can only be sent to others in the channel.

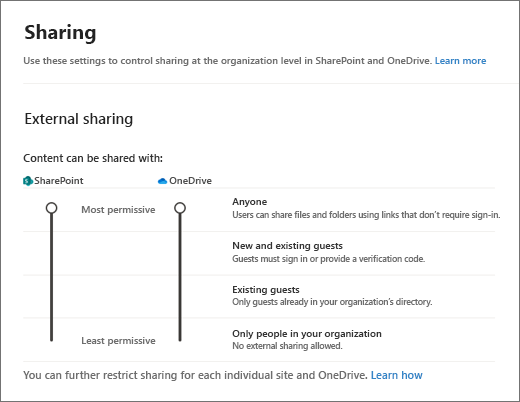
You can [change the type of link that is presented to users by default](https://docs.microsoft.com/en-us/sharepoint/change-default-sharing-link) for each site.

For more about the different types of sharing links, see [Securing your data](https://docs.microsoft.com/en-us/sharepoint/deploy-file-collaboration#securing-your-data).

**Guest sharing**

The external sharing features of SharePoint let users in your organization share content with people outside the organization (such as partners, vendors, clients, or customers). Planning for external sharing should be included as part of your overall permissions planning for SharePoint.

SharePoint has external sharing settings at both the organization level and the site level (previously called the "site collection" level). To allow external sharing on any site, you must allow it at the organization level. You can then restrict external sharing for other sites.



Whichever option you choose at the organization or site level, the more restrictive functionality is still available. For example, if you choose to allow sharing using *Anyone* links, users can still share with guests, who sign in, and with internal users.

External sharing is turned on by default for your organization. Default settings for individual sites vary depending on the type of site. See [Site level settings](https://docs.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-guest-settings) for more information.

[Shared channels in teams](https://docs.microsoft.com/en-us/MicrosoftTeams/shared-channels) do not use guest accounts for sharing with people outside the organization. However, external sharing must be enabled for people outside the organization to be invited to shared channels.

Guest sharing for private and shared channel sites can only be changed by using PowerShell.

To set up guest sharing for a site, see [Collaborate with guests in a site](https://docs.microsoft.com/en-us/microsoft-365/solutions/collaborate-in-site).

**Security and privacy**

If you have confidential information that should never be shared externally, we recommend storing the information in a site that has external sharing turned off. Create additional sites as needed to use for external sharing. This helps you to manage security risk by preventing external access to sensitive information.

**SharePoint and OneDrive integration with Azure AD B2B**

Azure AD B2B collaboration provides authentication and management of guests. Authentication happens via one-time passcode when they don't already have a work or school account or a Microsoft account (MSA).

With SharePoint and OneDrive integration, the Azure B2B collaboration one-time passcode feature is used for external sharing of files, folders, list items, document libraries and sites. (Shared channels in Teams don't use Azure B2B collaboration, but rather [Azure B2B direct connect](https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-direct-connect-overview).)

With Azure B2B collaboration integration, all guests are added to the directory and can be managed using Microsoft 365 security and compliance tools. We encourage you to try the [SharePoint and OneDrive integration with Azure AD B2B](https://docs.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration).