Contents

Introduction to SharePoint in Microsoft 365

6/30/2020 • 4 minutes to read • Edit Online

Microsoft SharePoint is a cloud-based service that helps organizations share and manage content, knowledge, and applications to:

- Empower teamwork
- Quickly find information
- Seamlessly collaborate across the organization

The resources on this page are designed to get you started. Depending on the needs of your organization, you may want to read about migration and governance options before you start rolling SharePoint out to your users. If you're ready to get started with SharePoint, read about collaboration options and how to create a modern intelligent intranet. As you roll out SharePoint to your organization, remember to train your users to help them get the most out of these tools.

If you're just starting out with SharePoint, learn about the FastTrack onboarding and adoption services, find a SharePoint certified partner, or visit the SharePoint community.

Once you're using SharePoint, get the OneDrive sync app and the Mobile app. You can also suggest a feature.

Migration

If you have files on-premises that you need to move to SharePoint in Microsoft 365, or if you're still using SharePoint Server, the resources in this section can help you get started.

IF YOU'RE LOOKING FOR THIS INFORMATION:	GO TO THIS RESOURCE:
How to migrate content from file shares, SharePoint Server, or other cloud providers to OneDrive in Microsoft 365	Migrate content to OneDrive How to migrate from on-premises file shares to Microsoft 365 The SharePoint Migration Tool
How to use connect your existing on-premises SharePoint sites to SharePoint in Microsoft 365	Hybrid for SharePoint Server

Governance

If your organization has legal or other requirements that govern the handling of data, or if you have sensitive or confidential information that you want to protect, these references can help you configure SharePoint for your governance standards and policies.

IF YOU'RE LOOKING FOR THIS INFORMATION:	GO TO THIS RESOURCE:
How to ensure that you retain files for a specified period of time, or delete them on a specified schedule	Overview of retention policies OneDrive retention and deletion

IF YOU'RE LOOKING FOR THIS INFORMATION:	GO TO THIS RESOURCE:
How to classify documents based on the sensitivity of the information	Overview of sensitivity labels Enable sensitivity labels for Office files in SharePoint and OneDrive
How to prevent the loss or exfiltration of important data in documents emails	Overview of data loss prevention
Search for in-place items such as email, documents, and instant messaging conversations	Content Search in Microsoft 365

If you use OneDrive in your organization and you want to protect important files by saving them to the cloud, govern how much storage space users get, or govern how users sync file, these references will help you configure your policies.

IF YOU'RE LOOKING FOR THIS INFORMATION:	GO TO THIS RESOURCE:
Protect important files on users' desktops or in their Documents folder	Redirect and move Windows known folders to OneDrive
Control how users sync files to their devices	Use Group Policy to control OneDrive sync settings
Configure the amount of storage space users have in OneDrive	Set the default storage space for OneDrive users

Collaboration

SharePoint provides a rich collaboration environment where people inside and outside your organization can work together, coauthoring document. Microsoft 365 provides a variety of options to help you create a secure and productive file collaboration environment that meets the needs of your organization. Use these resources to get started.

IF YOU'RE LOOKING FOR THIS INFORMATION:	GO TO THIS RESOURCE:
Learn about file collaboration and how to plan your implementation	File collaboration in SharePoint with Microsoft 365
Learn about collaborating with people outside your organization	External sharing overview Collaborate with guests
Use the security and compliance features in Microsoft 365 to help secure your guest sharing environment	Create a secure guest sharing environment

Modern intranet

SharePoint provides a rich set of tools to help you create and maintain your organization's intranet. Use these resources to get started.

IF YOU'RE LOOKING FOR THIS INFORMATION:	GO TO THIS RESOURCE:
Learn about the different types of SharePoint sites	Plan your SharePoint site

IF YOU'RE LOOKING FOR THIS INFORMATION:	GO TO THIS RESOURCE:
Select whether to allow users to create their own sites	Manage site creation
Learn how to plan an intelligent intranet for your organization	Plan an intelligent SharePoint intranet Planning your SharePoint hub sites

Training

Administrators are often called upon to teach others in the organization how to use new technologies. Use these resources to help your users be successful with SharePoint in Microsoft 365.

IF YOU'RE LOOKING FOR THIS INFORMATION:	GO TO THIS RESOURCE:
Set up a customizable training portal with Microsoft training content for your organization	Microsoft 365 learning pathways
Show your users the basics of SharePoint	SharePoint training

Customization

SharePoint provides a wide range of options for customization. We recommend using the out-of-box features and functionality as much as possible to meet your organization's needs. If you do need to customize SharePoint, see these references.

IF YOU'RE LOOKING FOR THIS INFORMATION:	GO TO THIS RESOURCE:
Understand how to customize SharePoint using modern tools and techniques	Customizing SharePoint
Build SharePoint Framework solutions, apps, add-ins, and solutions	SharePoint development

Related topics

SharePoint Limits

Getting started with the SharePoint Online Management Shell

Microsoft Partner Center

Guide to the modern experience in SharePoint

6/5/2020 • 5 minutes to read • Edit Online

The modern experience in Microsoft SharePoint is designed to be compelling, flexible, and more performant. The modern experience makes it easier for anyone to create beautiful, dynamic sites and pages that are mobile-ready. But what are the differences between the classic and modern experiences, and how do you go about creating a modern experience for your organization? This guide is a starting point for people familiar with the classic experiences in SharePoint to help you learn about the modern experience and how you can begin to take advantage of it.

Information architecture and hub sites

Classic SharePoint architecture is typically built using a hierarchical system of site collections and sub-sites, with inherited navigation, permissions, and site designs. Once built, this structure can be inflexible and difficult to maintain. In the modern SharePoint experience, every site is a site collection and can be associated to a hub, which is a flat collection of sites that share navigation, branding, and other elements. This type of structure is far more flexible and adaptive to the changing needs of your organization. Learn about how to plan for Hub sites.

Navigation

The most effective SharePoint sites (and web sites in general) help visitors find what they need quickly so that they can use the information they find to make decisions, learn about what is going on, access the tools they need, or engage with colleagues to help solve a problem. The fundamental principles and good practices for site and page navigation are equally applicable to both classic and modern SharePoint architectures. However, your options for *implementing* navigation differs based on the framework for your sites and intranet. For example, the "inherited" navigation experiences available in classic SharePoint site hierarchies (sites with subsites) are not available in the modern experience, but *hubs* provide a great way to achieve the cross-site navigation features previously available in managed navigation and site hierarchies in classic SharePoint.

No matter which framework you are using, you can use the guidance in Plan navigation in the modern experience to help make good decisions for navigation.

Branding

In the classic SharePoint experience, there are a set of default themes and site designs that can require a considerable amount of customization to get them to match your organization's brand. Also, they aren't very responsive, making the experience on different devices inconsistent. Most site branding requires the use of custom master pages or alternate CSS configurations. SharePoint includes an updated set of default site themes and site designs (or templates) that are responsive and look great on any device. With site themes, you can customize your site's logo and colors to match your brand. You can also align the mobile SharePoint app for your users to match your company branding. Site designs provide specific layouts and other functionality for your site. Additional branding can be achieved using custom themes or site designs without worrying about something breaking when SharePoint is updated. To learn more about modern branding options, see Branding SharePoint sites in the modern experience.

Publishing

If you've implemented publishing sites or publishing-enabled sites in your organization, you know how important it is to create attractive and performant pages to distribute communication to a large number of people. In the modern experience, communication sites make it easy to create beautiful, dynamic, and performant sites and pages that are mobile-ready. There are differences from classic publishing, though, and things you'll want to think about planning your move to the modern experience. For more info, see Moving from Publishing sites to Communication sites.

Search

Search is an important part of any site – you want people to be able to find what they are looking for quickly and easily. SharePoint has both a classic and a modern search experience. Microsoft Search in SharePoint is the modern experience. The most visible difference is that the Microsoft Search box is placed at the top of SharePoint, in the header bar. Another difference is that Microsoft Search is personal and contextual. The results you see are different from what other people see, even when you search for the same words. You will also see different results based on where you are when you search. For example, searching at the root of your tenant looks across all of SharePoint. Searching from a hub finds content in all sites associated to the hub. Searching from an individual site finds content on that site. Searching from a list or library finds content in the list or library. You will also see results before you start typing in the search box, based on your previous activity and trending content in Microsoft 365, and the results update as you type. To learn more about the Microsoft Search experience for users, see Find what you need with Microsoft Search. There are other differences, especially around customization. To decide which experience your organization should use, see When to use which search experience.

Sharing and permissions

SharePoint continues to provide both SharePoint groups as well as security groups maintained by Azure Active Directory. Microsoft 365 also provides a third grouping option for SharePoint, Microsoft 365 groups. Microsoft 365 groups are similar to security groups, although Microsoft 365 groups include many additional benefits. Microsoft 365 groups are provided a group email address as well as additional tools such as a group calendar, notebook, Planner, and a SharePoint Team site. Users assigned to an Microsoft 365 group may also be classified as either a group owner or a group member, in comparison to security groups where all group members have equal access under the group. To learn about the differences, benefits, and best practices for permissions and sharing in the modern experience, see Sharing and permissions in the SharePoint modern experience.

Performance

The modern experience in SharePoint is designed to be compelling, flexible and – importantly - more performant. Both SharePoint performance as a whole and the performance of individual SharePoint components such as search, lists, and document libraries are affected by many factors, all of which contribute to the decisive performance metric: perceived end user latency, or the speed with which pages are rendered in the client browser. For more info, see Performance in the modern SharePoint experience.

Multilingual

Classic SharePoint publishing sites can use a feature called variations to create a site that supports multiple languages. Modern communication sites leverage a multilingual experience to make content in your intranet sites available in multiple languages. User interface elements like site navigation, site title, and site description can be shown in the user's preferred language. Additionally, you can provide pages and news posts on communication sites that you translate and that are shown in the user's preferred language. One of the most important differences in the modern experience is that, unlike the variations feature, which creates a separate *sub-site* for each language, the modern multilingual experience creates a corresponding page in the same site, but in a language-specific *folder* in the Site Pages library. To learn more, see Create modern multilingual communication sites, pages, and news.

Intro to file collaboration in Microsoft 365, powered by SharePoint

6/5/2020 • 14 minutes to read • Edit Online

Are you getting the most out of file collaboration in Microsoft 365, or are your users still storing files locally or on network file shares and sending them around in email? Maybe you're paying for another cloud storage service and not taking advantage of the space you get with your Microsoft 365 subscription. This article describes the benefits and key features of file collaboration in Microsoft 365. It also covers the steps to plan for and adopt Microsoft 365 file collaboration in your organization.

The file collaboration capabilities in Microsoft 365 are available to you whatever the size of your organization. If you have a small organization, each user can store their files in their individual library in OneDrive and you might want only a single team in Microsoft Teams for everyone in the organization.

Why use Microsoft 365 cloud file storage?

By taking full advantage of SharePoint-powered file storage in Microsoft 365, you can avoid purchasing cloud storage from other providers and enjoy:

Anywhere access to files

Enterprise-grade security

Secure sharing outside the organization

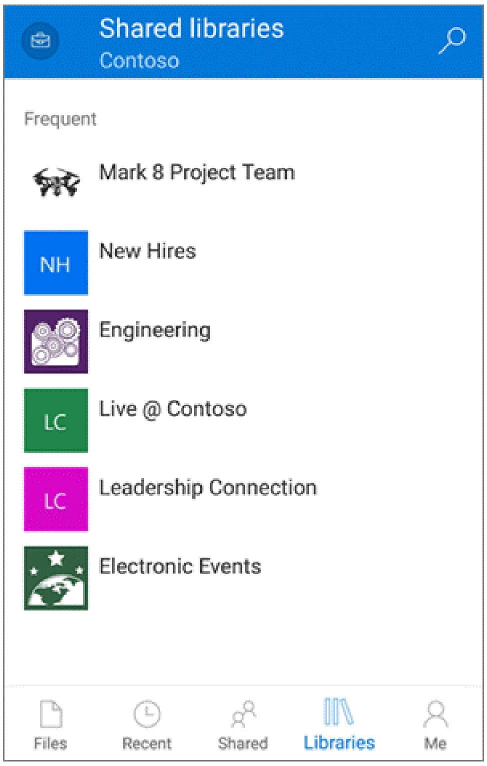
Real-time collaboration and file versioning

Intelligence that helps users discover files

Anywhere access

When users keep files on their local device or on a network share, they're out of luck when they don't have the device with them or don't have a connection to your network. If something happens to a user's device, the data might not be recoverable. If a user's device is upgraded, local data must be migrated. By storing files in the cloud, users can access them from all their devices, such as their phone and their home computer (depending on what you allow). They can even access files in a browser from other devices they trust. For example, if two colleagues travel to a customer site and one of their two laptops runs out of battery, they can both access all their files by signing in to portal.office.com on the other laptop. Get the SharePoint mobile app.

> **NOTE**
>
> If you're concerned about users signing in from kiosks or other shared, unmanaged devices, you might want to enable idle session sign-out.



Enterprise-grade security

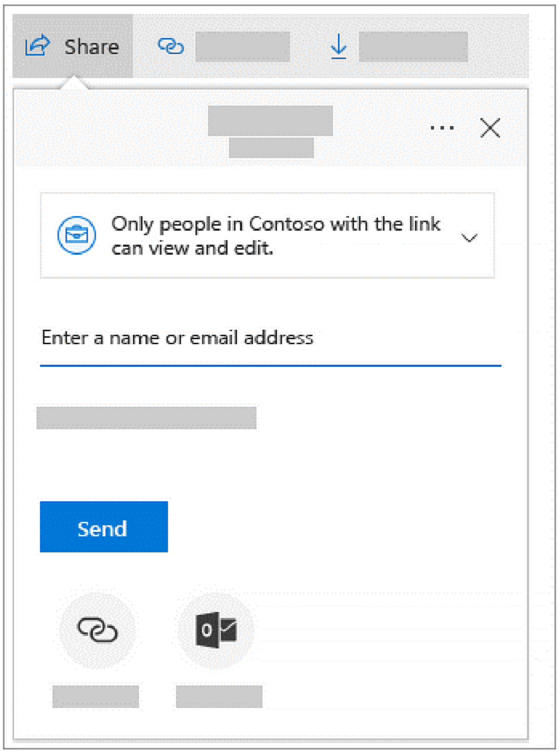
Files stored in SharePoint-powered storage locations in Microsoft 365 are encrypted in transit and in rest. (You can encrypt files by using your own key if you want.) Files are also scanned for viruses. As an admin, you can use tools in Microsoft 365 to further secure and monitor files in the Microsoft cloud:

- **Data loss prevention policies**. Warn or prevent users from sharing files that have specific labels outside the organization. See Overview of data loss prevention
- **Retention labels**. Classify files to be retained, permanently deleted, or marked as a record. See Overview of retention labels
- **Sensitivity labels**. Classify and protect highly confidential files with encryption and permissions. See Learn about sensitivity labels
- **Reports**. Monitor activity and usage in SharePoint and OneDrive. See Which activity reports are available in the admin center
- **Microsoft 365 Advanced Threat Protection (ATP)**. Protect against sharing malicious files. More info
- **Files Restore**. If a location is affected by malicious software, or someone deletes important files, you can restore a document library to an earlier point in time.

Plan for these features

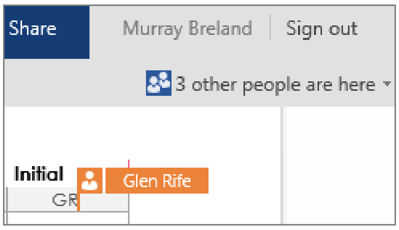
Secure sharing outside the organization

SharePoint powers secure file sharing in Microsoft 365. You can specify if you want people outside the organization to be able to access files without authenticating (by signing in or providing a verification code). You can even block external sharing altogether. We recommend using the most permissive sharing option that you can for each set of content. If you heavily restrict sharing and it blocks user productivity, users will typically find other ways to collaborate that provide you less oversight and control. For more info, see Control sharing.

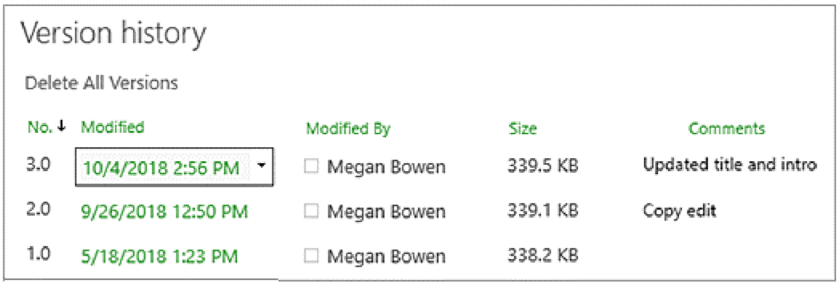


Real-time collaboration and version management

When users store Office files in the Microsoft 365 cloud, they can avoid the hassle of managing changes in different copies of files. Instead, they can collaborate on a single version by using either the desktop apps or the web versions of Office. People don't even need to have the Office desktop apps installed to edit Office files. Learn more about document collaboration and coauthoring. When multiple users edit an Office file at the same time, a notification will show them that other people are working in the file and they can see where in the file others are working.



Version history is also on by default, so users can view earlier changes and roll back as necessary. Learn more about working with version history.



Intelligence that helps users discover files

When users in the organization regularly store files in the Microsoft 365 cloud, they can quickly find recent files and other files that might be of interest. For example, they can discover files that coworkers or frequent collaborators are working on. More info

Key features

Most of the file collaboration features in Microsoft 365 are available to you regardless of your subscription type or the size of your organization.

- Migration tools
- Modern attachments
- A hub for teamwork: Microsoft Teams
- Access to all files in OneDrive
- Syncing for offline access
- Integration with Microsoft Office
- Auditing and reporting
- Hybrid
- Multi-geo

A hub for teamwork: Microsoft Teams

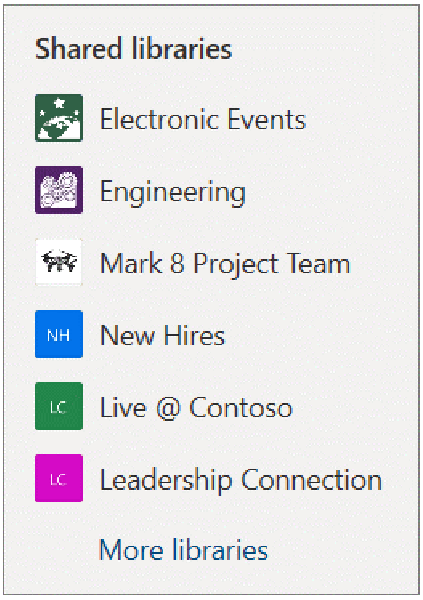
In the past, users would have to frequently switch between tools to collaborate. For example, users would write a document in Word. Then they would switch to Outlook to share the document as an attachment. Or they would open a browser to upload the document to a SharePoint site. In Microsoft 365, users can use Teams to chat, make calls, and have online meetings. They don't have to leave Teams to view and even edit the files they share. Learn more.

> **NOTE**
>
> When a user attaches a file to a chat, it's automatically uploaded to the user's individual library in OneDrive. When a user attaches a file to a Teams channel, it's automatically uploaded to the library for that team. Files shared with Yammer groups are now also saved in SharePoint.

Access to all files in OneDrive

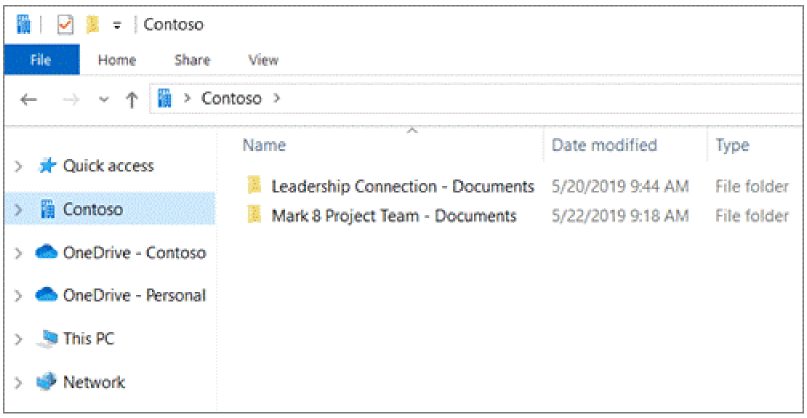
When your users use OneDrive, they can access their SharePoint or Microsoft Teams files on the web or in the mobile app without leaving OneDrive. Learn more

Because individual libraries in OneDrive are powered by SharePoint, users can easily move files between locations. For example, if a user drafts a file in their individual library in OneDrive, and later wants a team to own the file, the user can simply move the file to the team's library.



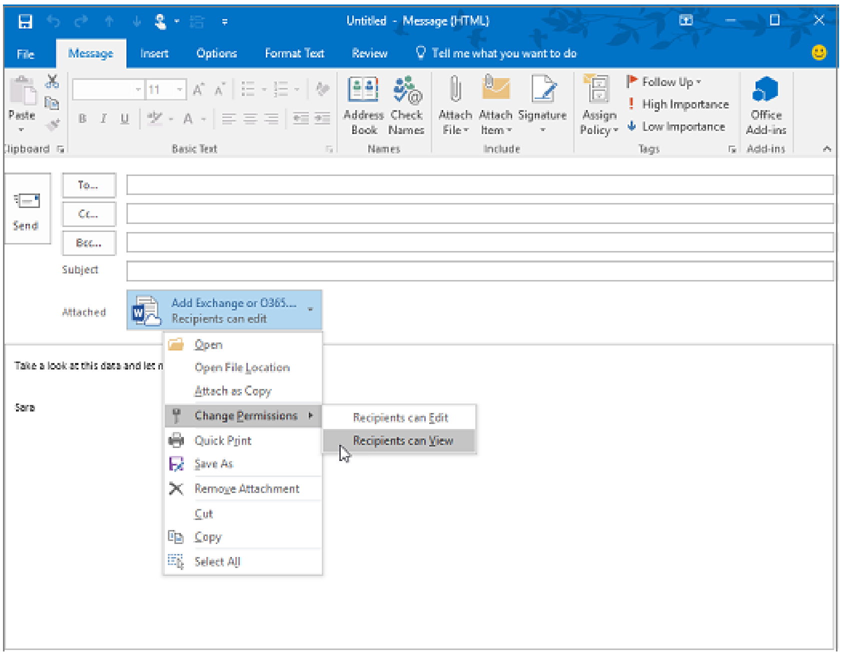
Sync for offline access

With the OneDrive sync app, users can sync files between their computer and the Microsoft 365 cloud. When users add, change, or delete a file or folder locally, the file or folder is added, changed, or deleted in the cloud and vice versa. Users can work with synced files directly in File Explorer and the apps they use. Whenever the user is online, any changes that they or other users make will sync automatically. With Files On-Demand (available with Windows 10 and Mac), users can easily browse and organize files in OneDrive and SharePoint by using File Explorer or Finder, but the files don't take up space on the local computer. Learn more about Files On-Demand.



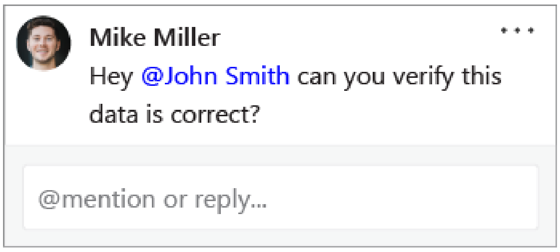
Modern attachments in Outlook

If your users are used to sharing files as attachments in Outlook, they can use the same steps they're familiar with to share a link to a file instead of emailing a copy. Within Outlook, users can even change the permission they give to the recipient. Learn more about attaching files.



Integrate with Microsoft Office

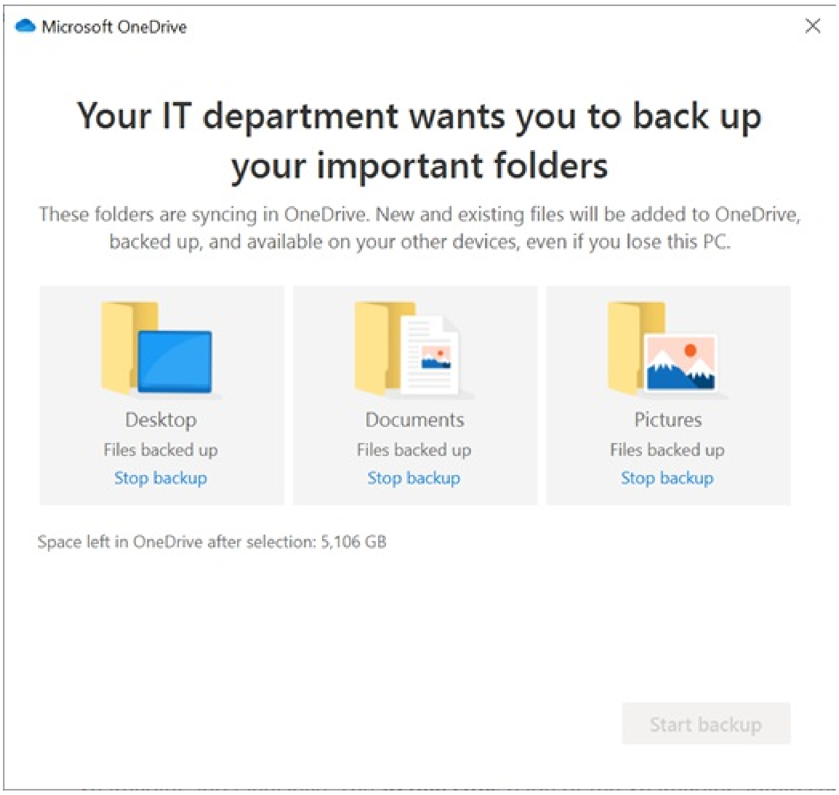
In the Office apps, users can easily open files saved in the Microsoft cloud and save documents to OneDrive. Learn more. When users comment on an Office document and use the @ sign with someone's name, the person mentioned receives mail with a link to the comment. Clicking the link brings them into the document and into the conversation.



Migration tools

You can choose one or more of the following options, depending on the number and location of files that you want to migrate.

- **SharePoint Migration Tool**. To migrate files from file shares or on-premises SharePoint, you can use the SharePoint Migration Tool. For info, see How the SharePoint Migration Tool works.
- **Known Folder Move**. If your users save most of their files to their Desktop, Documents, and Pictures folders, you can seamlessly move them to OneDrive using Known Folder Move so users can continue working in the locations they're used to.



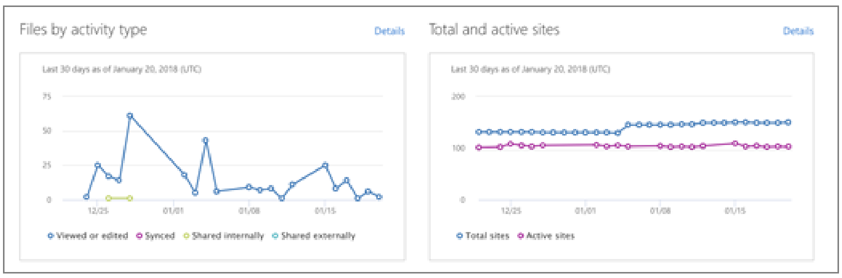
- **FastTrack migration benefit.** FastTrack provides you with a set of best practices, tools, resources, and experts. Guidance includes migrating content from file shares, Box, or Google Drive source environments, and introducing capabilities at the pace that works for you. The FastTrack data migration benefit will also perform specific data migration activities on your behalf if you have 500 or more licenses. See more details in the FastTrack Center Benefit Overview. To get started, go to FastTrack.Microsoft.Com, review resources, and submit a request for assistance.

Hybrid

If your organization uses SharePoint Server, setting up a hybrid environment can help you move to the cloud at your own pace. Hybrid features let you tie the two environments together in a variety of ways to make a more seamless user experience. You can consolidate search results between SharePoint Server and Microsoft 365, consolidate user profiles in Microsoft 365, and migrate your users' individual storage to OneDrive. Get started exploring hybrid.

Auditing and reporting

In the new SharePoint admin center, you can see SharePoint activity and usage reports, and go to the Microsoft 365 admin center for details.



Multi-geo

If you're a multinational organization with data residency requirements, you can use Multi-Geo in Microsoft 365 to specify where files are stored. For info, see Multi-Geo Capabilities in OneDrive and SharePoint in Microsoft 365.

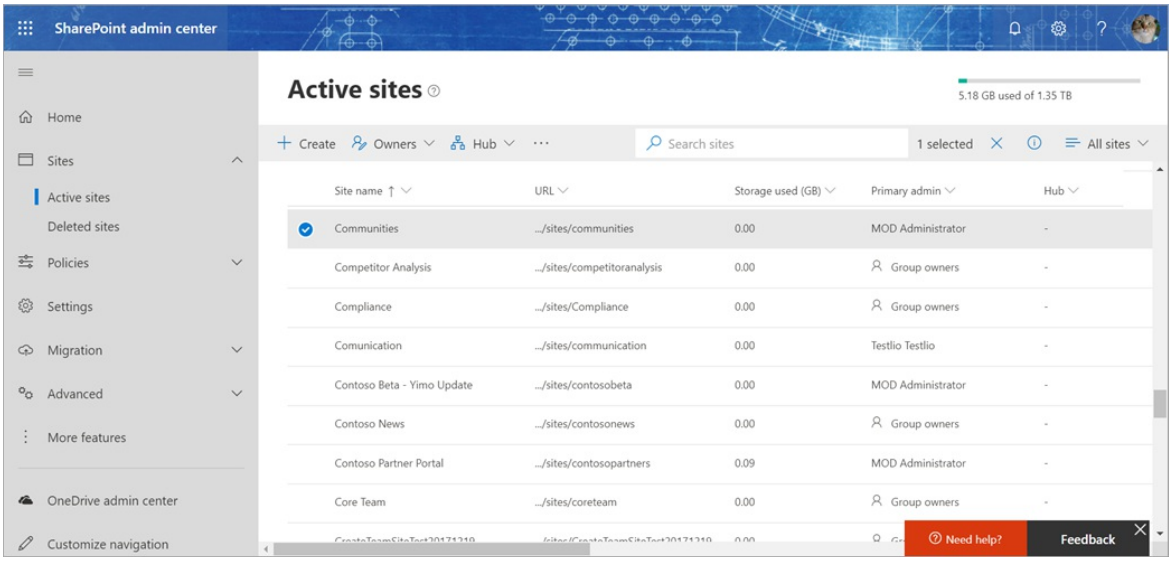
Unified search

Microsoft Search helps users find files within modern SharePoint sites and from the SharePoint start page, Office.com, Bing, and more. Learn more about the modern search experience in SharePoint.

Management options

As a global or SharePoint admin for your organization, you have a couple of options for managing SharePoint sites and settings:

- **New SharePoint admin center**. In the new SharePoint admin center, you can create and delete sites, manage site settings, and manage organization-level settings for SharePoint and OneDrive. The **Active sites** page of the SharePoint admin center lets you view the SharePoint sites in your organization, including communication sites and sites that belong to Microsoft 365 Groups. It also lets you sort and filter sites, search for a site, and create new sites. Get started with the new SharePoint admin center.



- **Microsoft PowerShell**. The SharePoint Online Management Shell is a PowerShell module that lets you run command-line operations. It makes performing batch operations more efficient, and is the only way to perform some management tasks in SharePoint and OneDrive. Get started with the SharePoint Online Management Shell.

Prerequisites

Purchase and assign licenses. SharePoint comes with Microsoft 365 plans and Office 365 plans. It also comes as a standalone plan. For more info about the features available in each plan, see the SharePoint service description. Some security features, such as Azure Information Protection, require an E3 or E5 plan. Cloud App Security, Advanced Threat Protection, Customer Lockbox, Customer Key, Advanced eDiscovery. For info, see Office 365 platform service description.

Assign the SharePoint admin role. Users assigned this role will have access to the SharePoint admin center and can change organization-level SharePoint and OneDrive settings, create and delete sites, and change site owners and other site settings. Learn more about the SharePoint admin role.

Estimate and test your network bandwidth. Before you roll out Microsoft 365 in your organization, make sure that your network is set up for optimum performance. Network planning and performance tuning. Before you deploy the sync app, make sure you also estimate the bandwidth users will need for syncing.

Limitations

- For info about SharePoint limits, see the SharePoint service description.
- For info about file name, size, and type limits when using the OneDrive sync app, see Invalid file names and file types.

Manage feature changes

- To learn about features coming soon, see the Microsoft 365 Roadmap.
- To keep on top of the latest SharePoint features rolling out, refer to the Message Center.
- To vote on feature requests or submit your own idea, visit the SharePoint UserVoice.

Plan user adoption

User adoption is important to the overall success of any rollout. To maximize your investment, you need to maximize your user engagement. To do that, start by focusing on three critical success factors:

- **Stakeholders.** Securing the participation and buy-in of key people within your organization is critical to successful user adoption. This support can come from business-focused leaders, IT leadership, or anyone else who has a vested interest in seeing Microsoft 365 file collaboration succeed in your organization. It's important to have both executive or business leader support and product champions to help carry the knowledge to their peers. Whether you're formally delegating the product champion role or allowing it to grow organically, champions are mission critical to user adoption. Studies have shown that people prefer to learn from a coworker than from an IT employee. For more information about how to identify key stakeholders, see the Identify key stakeholders guide. For more information about building a sustainable champion community, see Build a champion program.
- **Scenarios.** Identify and define your business scenarios and how those scenarios align with the benefits of file collaboration in Microsoft 365. Work with your key stakeholders to identify the goals of the business scenarios, and then match those goals against usage scenarios. For example, a business goal may be to maximize user productivity; a key usage scenario enabling that goal would be using OneDrive to access files from mobile devices, PCs, and Macs. For help with this process, see the Office 365 Productivity Library.
- **Awareness and training.** Creating awareness through awareness campaigns such as announcements, launch events, newsletters, town hall meetings, contests, and giveaways is a critical path to maximizing adoption. In addition, providing users with knowledge through classroom-style sessions and self-help guides helps them feel empowered to use OneDrive and Office 365. For more information about user communication and training on Office 365, see the Plan your Office 365 Launch: Communication and Training Guide.

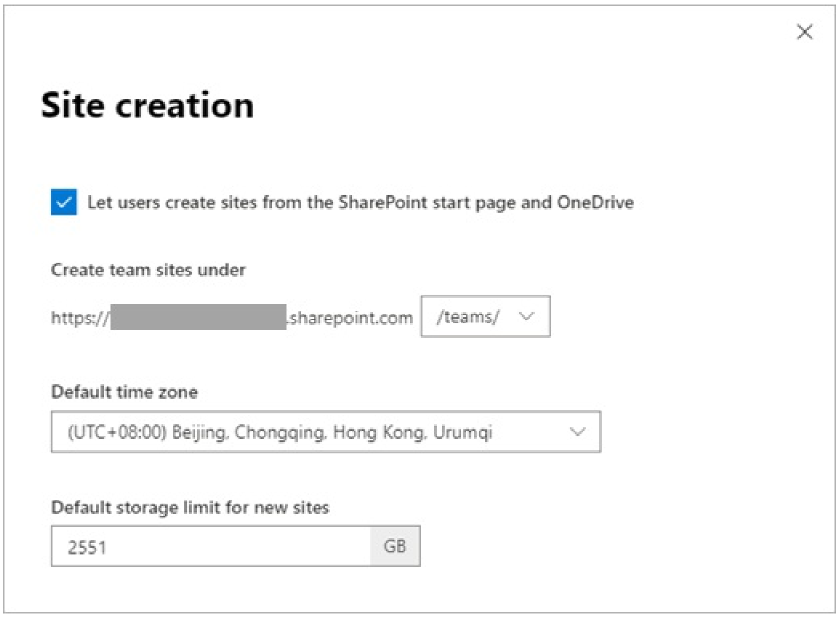
Many resources are available from Microsoft to help you drive user adoption within your environment. For more information about a recommended Microsoft 365 user adoption strategy, see the Microsoft 365 End User Adoption Guide. For more information about driving user engagement, see Success Factors for Office 365 End User Engagement. You can also contribute to or comment on adoption-related ideas in the Driving Adoption Tech Community.

Configure settings

To prepare for file collaboration in Microsoft 365, configure the following settings.

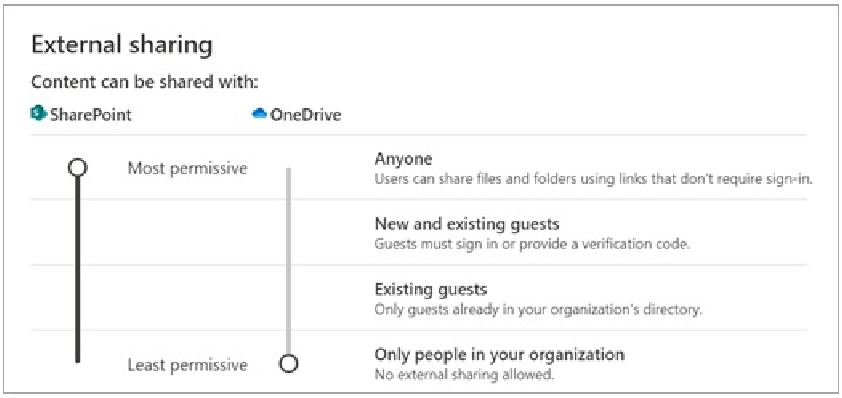
Create sites

When a Microsoft 365 group is created from anywhere within Microsoft 365, a SharePoint site is automatically created. You can let all users create groups, only some users, or you can block group creation and manage it centrally in your IT department. For info, see Manage who can create Office groups. You can also use a naming policy for groups and set an expiration period so that groups that are no longer being used will be deleted. For more info, see Plan for governance in Microsoft 365 Groups. If you allow users to create groups, you can also allow them to create team sites from the SharePoint start page and from OneDrive and manage default site settings. For info, see Manage site creation.



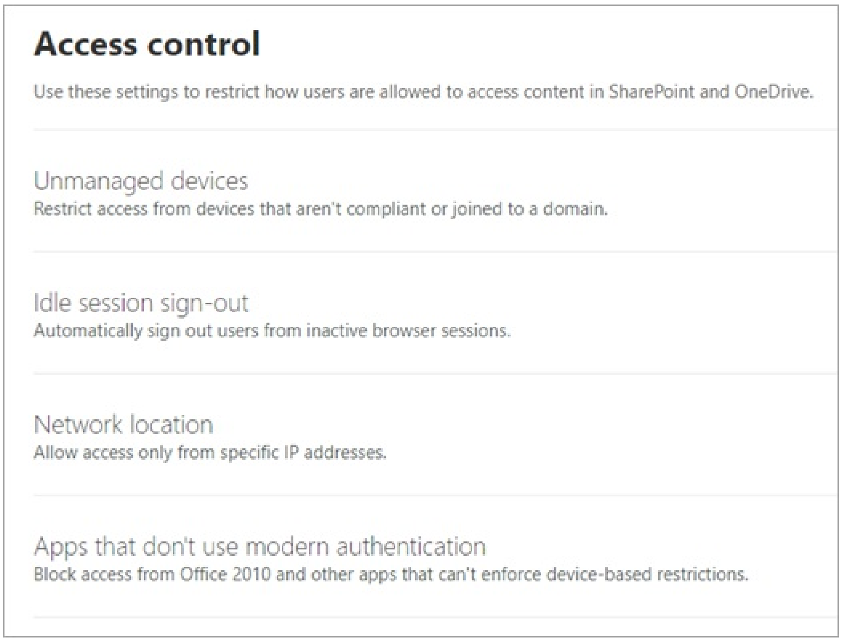
Sharing

To set up external sharing in your organization, you need to make sure that settings across multiple admin centers are set the way you want. Sharing with people outside your organization is enabled by default in SharePoint and OneDrive, but disabled for Microsoft Teams. Configure Microsoft 365 to enable guest collaboration for Teams. Set the external sharing level and the default sharing link type.



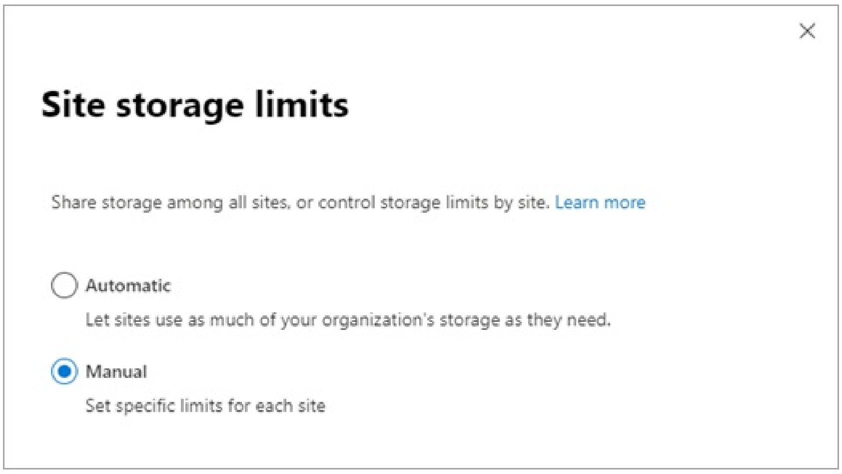
Security

- Design and deploy retention labels and DLP policies to protect sensitive and highly confidential files. Learn how.
- Block or limit access from unmanaged devices, sign out inactive users on unmanaged devices, or allow access from only specific IP address ranges. For info about setting up identity and device-access policies to protect content, see Policy recommendations for securing SharePoint sites and files.



Storage

By default, file storage for team sites is managed automatically. If you prefer to control storage manually, see Manage site storage limits. For info about setting the default storage space for individual libraries in OneDrive, see Set the default storage space for OneDrive users. For information about the amount of storage that comes with your plan, see SharePoint limits.



Specify team site libraries to sync automatically

To let users easily access team site files from File Explorer (as they might have previously accessed network file shares), you can specify particular team site libraries to sync on your users' computers automatically. To do this, use the OneDrive Group Policy object "Configure team site libraries to sync automatically." Your users need to be running Windows 10 and OneDrive Files On-Demand must be enabled.

File collaboration in SharePoint with Microsoft 365

6/25/2020 • 18 minutes to read • Edit Online

With Microsoft 365 services, you can create a secure and productive file collaboration environment for your users. SharePoint powers much of this, but the capabilities of file collaboration in Microsoft 365 reach far beyond the traditional SharePoint site. Teams, OneDrive, and a variety of governance and security options all play a role in creating a rich environment where users can collaborate easily and where your organization's sensitive content remains secure.

In the sections below, we call out the options and decisions that you as an administrator should consider when setting up a collaboration environment:

- How SharePoint relates to other collaboration services in Microsoft 365, including OneDrive, Microsoft 365 Groups, and Teams.
- How you can create an intuitive and productive collaboration environment for your users.
- How you can protect your organization's data by managing access through permissions, data classifications, governance rules, and monitoring.

We recommend that you download the Microsoft Teams and related productivity services in Microsoft 365 for IT architects poster and refer to it while you read this article. This poster provides detailed illustrations of how the collaboration services in Microsoft 365 relate to each other and interact.

Also see the File Protection Solutions in Microsoft 365 diagram for an overview of recommended solutions to protect your data.

Creating a successful collaboration experience

The technical implementation options that you choose for file collaboration in Microsoft 365 should balance what can seem to be contradictory requirements:

- Protecting your intellectual property
- Enabling self-service
- Creating a smooth user experience

Protecting your intellectual property

There are several options discussed later in this article for protecting your intellectual property. These include limiting who files can be shared with, applying governance policies based on sensitivity labels, and managing the devices that users use to access content.

In considering which options to choose, we recommend a balanced approach:

A configuration that allows users to share content freely can lead to accidental sharing of confidential data. However, a user experience that is difficult to use or too restrictive can lead to users finding alternative collaboration options that circumvent your governance policies, ultimately leading to even greater risk.

By using a combination of features – depending on the sensitivity of your data – you can create a collaboration environment that's easy to use and provides the security and auditing controls that you need.

Enabling self-service

In SharePoint Server on-premises, many organizations chose an IT-focused model where users must request sites and provide a business justification. This was done to prevent site sprawl and to apply governance policies around access to sensitive data.

In Microsoft 365, we recommend allowing users to create Teams, Microsoft 365 Groups, and SharePoint sites as needed. You can use sensitivity labels to enforce permissions governance, take advantage of security features that protect your content, and use expiration and renewal policies to make sure unused sites don't accumulate.

By choosing options that favor user self-service, you can minimize the impact on your IT staff while creating an easier experience for your users.

Creating a smooth user experience

The key to creating a smooth user experience is to avoid creating barriers for your users that they don't understand or that they must escalate to your help desk. For example, turning external sharing off for a site might cause user confusion or frustration; whereas labeling the site and its contents as confidential and using data loss prevention policy tips and emails to educate your users in your governance policies, can lead to a much smoother experience for them.

SharePoint, Microsoft 365 Groups, and Teams

In Microsoft 365, SharePoint is integrated with a variety of other services to provide a much richer experience than is possible with on-premises solutions such as SharePoint Server. These integrations affect how you manage user permissions and what your users can do in a collaboration scenario.

Traditionally, SharePoint permissions have been managed through a set of permissions groups within a site (Owners, Members, Visitors, etc.). In SharePoint in Microsoft 365, each SharePoint team site is part of a Microsoft 365 group. a Microsoft 365 group is a single permissions group that is associated with a variety of Microsoft 365 services, including 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 are given access to the SharePoint site along with the other connected services.

While you can continue to manage SharePoint site permissions separately by using SharePoint groups, we recommend managing permissions for SharePoint by adding people to or removing them from the associated Microsoft 365 group. This provides easier administration as well as giving users access to a host of related services that they can use for better collaboration.

Microsoft Teams provides a hub for collaboration by bringing together all the Microsoft 365 group-related services, plus a variety of Teams-specific services, in a single user experience with persistent chat. Teams uses the associated Microsoft 365 group to manage its permissions. Within the Teams experience, users can directly access SharePoint along with the other services without having to switch applications. This provides a centralized collaboration space with a single place to manage permissions. For collaboration scenarios in your organization, we highly recommend using Teams rather than using services such as SharePoint independently.

For details about how SharePoint and Teams interact, see How SharePoint and OneDrive interact with Microsoft Teams.

Collaboration in client applications

Office applications such as Word, Excel, and PowerPoint provide a wide variety of collaboration features, including co-authoring and @mentions, and are also integrated with sensitivity labels and data loss prevention (discussed below).

We highly recommend deploying Microsoft 365 Apps for enterprise. Microsoft 365 Apps for enterprise provides an always up-to-date experience for your users, with the latest features and updates delivered on a schedule that you can control.

For details about deploying Microsoft 365 Apps for enterprise, see Deployment guide for Microsoft 365 Apps for enterprise.

OneDrive libraries

While SharePoint provides shared libraries for shared files that teams can collaborate on, users also have an individual library in OneDrive where they can store files that they own.

When a user adds a file to their individual library, that file is not shared with anyone else. Users' individual libraries do, however, provide the same sharing capabilities as SharePoint, so users can share files in their individual libraries as needed.

A user's individual library can be accessed from Teams, as well as from the OneDrive web interface and mobile application.

On devices running Windows or macOS, users can install the OneDrive sync app to sync files from both OneDrive and SharePoint to their local disk. This allows them to work on files offline and also provides the convenience of opening files in their native application (such as Word or Excel) without the need of going to the web interface.

The two main decisions to consider for using OneDrive in collaboration scenarios are:

- Do you want to allow Microsoft 365 users to share files in their own library with people outside your organization?
- Do you want to restrict file sync in any way – such as only to managed devices?

These settings are available in the OneDrive admin center.

OneDrive is an important part of the Microsoft 365 collaboration story. For information about how to deploy OneDrive in your organization, see OneDrive guide for enterprises.

Securing your data

A big part of a successful collaboration solution is making sure your organization's data remains secure. Microsoft 365 provides a variety of features to help you keep your data secure while enabling a seamless collaboration experience for your users.

To help protect your organization's information, you can:

- **Control sharing** – by configuring sharing settings for each site that are appropriate to the type of information in the site, you can create a collaboration space for users while securing your intellectual property.
- **Classify and protect information** – by classifying the types of information in your organization, you can create governance policies that provide higher levels of security to information that is confidential compared to information that is meant to be shared freely.
- **Manage devices** – with device management, you can control access to information based on device, location, and other parameters.
- **Monitor activity** – by monitoring the collaboration activity happening in Teams and SharePoint, you can gain insights into how your organization's information is being used. You can also set alerts to flag suspicious activity.
- **Protect against threats** – by using policies to detect malicious files in SharePoint, OneDrive, and Teams, you can help ensure the safety of your organization's data and network.

These are each discussed in more detail below. There are many options to choose from. Depending on the needs of your organization, you can choose the options that give you the best balance of security and usability. If you are in an highly regulated industry or work with highly confidential data, you may want to put more of these controls in place; whereas if your organization's information is not sensitive you may want to rely on basic sharing settings and malicious file alerts.

Control sharing

The sharing settings that you configure for SharePoint and OneDrive determine who your users can collaborate with, both inside and outside your organization. Depending on your business needs and the sensitivity of your data, you can:

- Disallow sharing with people outside your organization.
- Require people outside your organization to authenticate.
- Restrict sharing to specified domains.

You can configure these settings for the entire organization, or for each site independently. For detailed information, see Turn sharing on or off and Turn sharing on or off for a site.

See Limit accidental exposure to files when sharing with guests for additional guidance around sharing with people outside your organization.

When users share files and folders, a shareable link is created which has permissions to the item. There are three primary link types:

- *Anyone* links give access to the item to anyone who has the link. People using an *Anyone* link do not have to authenticate, and their access cannot be audited.

  An *anyone* link is a transferrable, revocable secret key. It's transferrable because it can be forwarded to others. It's revocable because by deleting the link, you can revoke the access of everyone who got it through the link. It's secret because it can't be guessed or derived. The only way to get access is to get the link, and the only way to get the link is for somebody to give it to you.

- *People in your organization* links work for only people inside your Microsoft 365 organization. (They do not work for guests in the directory, only members).

Like an *anyone* link, a *people in my organization* link is a transferrable, revocable secret key. Unlike an *anyone* link, these links only work for people inside your Microsoft 365 organization. When somebody opens a *people in my organization* link, they need to be authenticated as a member in your directory. If they're not currently signed-in, they'll be prompted to sign-in.

- *Specific people* links only work for the people that users specify when they share the item.

A *specific people* link is a non-transferable, revocable secret key. Unlike *anyone* and *people in my organization* links, a *specific people* link will not work if it's opened by anybody except for the person specified by the sender.

Specific people links can be used to share with internal or external users. In both cases, the recipient will need to authenticate as the user specified in the link.

It's important to educate your users in how these sharing links work and which they should use to best maintain the security of your data. Send your users links to Share OneDrive files and folders and Share SharePoint files or folders, and include information about your organization's policies for sharing information.

Unauthenticated access with *Anyone* links

Anyone links are a great way to easily share files and folders with people outside your organization. However, if you're sharing sensitive information, this may not be the best option.

If you require people outside your organization to authenticate, *Anyone* links will not be available to users and you'll be able to audit guest activity on shared files and folders.

Though *Anyone* links do not require people outside your organization to authenticate, you can track the usage of *Anyone* links and revoke access if needed. If people in your organization frequently email documents to people outside your organization, *Anyone* links may be a better option than emailing an attachment.

If you want to allow *Anyone* links, there are several options for a more secure sharing experience.

You can restrict *Anyone* links to read-only. You can also set an expiration time limit, after which the link will stop working.

Another option is to configure a different link type to be displayed to the user by default. This can help minimize the chances of inappropriate sharing. For example, if you want to allow *Anyone* links but are concerned that they only be used for specific purposes, you can set the default link type to *Specific people* links or *People in your organization* links instead of *Anyone* links. Users would then have to explicitly select *Anyone* links when they share a file or folder.

You can also use data loss prevention to restrict *Anyone* link access to files that contain sensitive information.

People in your organization links

People in your organization links are a great way to share information within your organization. *People in your organization* links work for anyone in your organization, so users can share files and folders with people who aren't part of a team or members of a site. The link gives them access to the particular file or folder and can be passed around inside the organization. This allows for easy collaboration with stakeholders from groups that may have separate teams or sites – such as design, marketing, and support groups.

Creating a *People in your organization* link does not cause the file or folder to show up in search or give everyone direct access to the file or folder. Users must have the link in order to access the file or folder. The link does not work for guests or other people outside your organization.

Specific people links

Specific people links are best for circumstances where users want to limit access to a file or folder. The link only works for the person specified and they must authenticate in order to use it. These links can be internal or external (if you've enabled guest sharing).

Classify and protect information

Data loss prevention in Microsoft 365 provides a way to classify your teams, groups, sites, and documents, and to create a series of conditions, actions, and exceptions to govern how they're used and shared.

By classifying your information and creating governance rules around them, you can create a collaboration environment where users can easily work with each other without accidentally or intentionally sharing sensitive information inappropriately.

With data loss prevention policies in place, you can be relatively liberal with your sharing settings for a given site and rely on data loss prevention to enforce your governance requirements. This provides a friendlier user experience and avoids unnecessary restrictions that users might try to work around.

For detailed information about data loss prevention, see Overview of data loss prevention.

Sensitivity labels

Sensitivity labels provide a way to classify teams, groups, sites, and documents with descriptive labels that can then be used to enforce a governance workflow.

Using sensitivity labels helps your users to share information safely and to maintain your governance policies without the need for users to become experts in those policies.

For example, you could configure a policy that requires Microsoft 365 groups classified as confidential to be private rather than public. In such a case, a user creating a group, team, or SharePoint site would only see the "private" option when they choose a classification of confidential. For information about using sensitivity labels with teams, groups, and sites, see Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites

Conditions and actions

With data loss protection conditions and actions, you can enforce a governance workflow when a given condition is met.

Examples include:

- If customer information is detected in a document, then users cannot share that document with guests.
- If a document contains the name of a confidential project, then guests cannot open the document even if it has been shared with them.

Microsoft Cloud App Security offers additional granular conditions, actions, and alerts to help you secure your content. These include the ability to remove a user's permissions or quarantine the user when the specified condition is met.

User notifications

User notifications provide a way to communicate to your users – via email or policy tips – that data loss prevention has detected something that they should be aware of. The user can then decide the best course of action depending on the situation. For example, if a user unknowingly attempts to share a document that contains a credit card number, the user is prompted that a credit card number has been found and advised of your organization's policy regarding this.

Manage access

Microsoft 365 provides a variety of governance features to help you create an intuitive but secure collaboration environment for your users.

- Use device management to ensure your organization's information is accessed only by compliant devices.
- Use conditional access to ensure your confidential data is accessed only from locations and apps that you trust.
- Monitor information sharing in real time and through reports to ensure your governance requirements are met and sensitive information is being kept secure.

Additionally, you can use Azure Active Directory access reviews to automate a periodic review of group and team ownership and membership.

Device Management

Through device management, you can take additional steps to secure your organization's information. You can manage pretty much any device that your users might have – PCs, Macs, mobile devices, and Linux computers.

Examples include:

- Ensure devices have the latest updates before allowing access to Microsoft 365
- Prevent copy and paste of confidential data to personal or unmanaged apps
- Erase company data from managed devices

As you consider your options governing access to information through device management, keep in mind that guest users are likely to have unmanaged devices. For sites where you've enabled guest sharing, be sure to provide the needed access to unmanaged devices, even if that's just web access via a PC or Mac. Azure Active Directory conditional access (discussed below) offers some options to reduce the risk of guest users with unmanaged devices. Some settings can be configured directly from SharePoint.

Intune in Microsoft 365 provides detailed device profiling options and can also deploy and manage individual apps such as Office apps and OneDrive. For detailed information about Intune and device management, see What is Microsoft Intune?.

You can configure device management from the Microsoft 365 Device Management admin center.

Conditional access

Azure Active Directory conditional access provides additional controls to prevent users from accessing your organization's resources in risky situations, such as from untrusted location or from devices that aren't up to date.

Examples include:

- Block guest users from logging in from risky locations
- Require multi-factor authentication for mobile devices

You can create access policies that are specifically for guest users, allowing risk mitigation for users who most likely have unmanaged devices.

For detailed information, see What is Conditional Access?.

Real-time monitoring with alerts

Microsoft Cloud App Security provides an extensive policy infrastructure that you can use to monitor activity that you consider to be risky for your organization's data.

Examples include:

- Raise an alert when a confidential file is shared externally.
- Raise an alert when there's a mass download by a single user.
- Raise an alert when an externally shared file hasn't been updated for a specified period of time.

Cloud App Security can also watch for anomalous behavior such as unusually large uploads or downloads, access from unusual locations, or unusual admin activity.

By configuring alerts in Cloud App Security, you can be more confident in allowing an open sharing experience for your users.

You can see the alerts on the Cloud App Security alerts page.

For detailed information about Cloud App Security, see Microsoft Cloud App Security overview.

Monitoring with reports

A variety of reports are available in Microsoft 365 to help you monitor site usage, document sharing, governance compliance, and a host of other events.

For info about how to view reports on SharePoint site usage, see Microsoft 365 Reports in the Admin Center - SharePoint site usage.

For info about how to view data loss prevention reports, see View the reports for data loss prevention.

For info about how to view Cloud App Security reports, see Generate data management reports.

Manage threats

You can use ATP Safe Attachments (part of Microsoft 365 Advanced Threat Protection) to protect against users uploading malicious files to OneDrive, SharePoint, or Teams.

When ATP discovers a malicious file, that file is locked so that users cannot open, move, or copy the file.

The locked file is included in a list of quarantined items that you can monitor. You can then delete or release the file as appropriate.

For detailed info, see Microsoft 365 ATP for SharePoint, OneDrive, and Microsoft Teams.

Migrate files from on-premises

Microsoft 365 offers much greater versatility in collaboration scenarios than on-premises solutions such as SharePoint Server. If you have files in document libraries on SharePoint Server or in file shares, you can migrate them to SharePoint by using the SharePoint Migration Tool. The SharePoint Migration Tool can move files, OneDrive libraries, and even entire sites to SharePoint.

As part of your migration, you can use the Azure Information Protection scanner to scan and label sensitive information in your on-premises environment. With this information, you can reorganize your data if needed before migrating it to similarly labeled sites in SharePoint.

If the content that your users are collaborating on is located in SharePoint Server or in file shares, we recommend that you migrate it to Microsoft 365 to take advantage of the broader range of collaboration capabilities.

For information on how to migrate content with the SharePoint Migration Tool, see Download and install the SharePoint Migration Tool.

Related topics

Create a secure guest sharing environment

Best practices for sharing files and folders with unauthenticated users

Understanding how Microsoft Information Protection capabilities work together

How to deal with external sharing in Microsoft 365

Tutorial: Automatically apply Azure Information Protection classification labels

What's new in external sharing and collaboration with OneDrive and SharePoint

Protect and collaborate on files in the cloud with OneDrive, SharePoint, and Microsoft Teams

Add featured links to the SharePoint start page

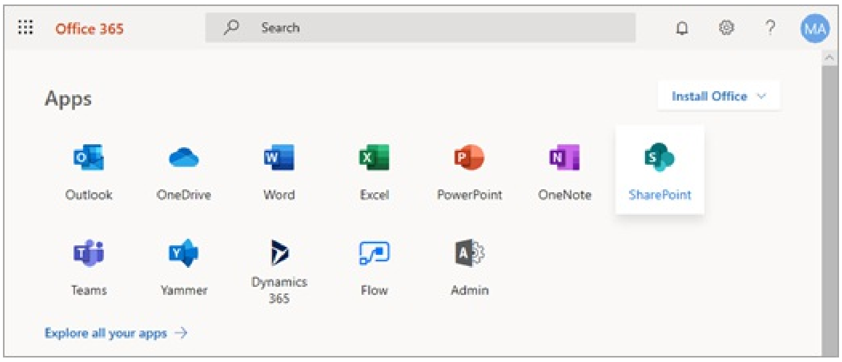
1/8/2021 • 2 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can feature the sites and content you want on the SharePoint start page by changing the **Featured links** list in the left pane. To add links to a SharePoint Server page, see Video: Add a link to a page.

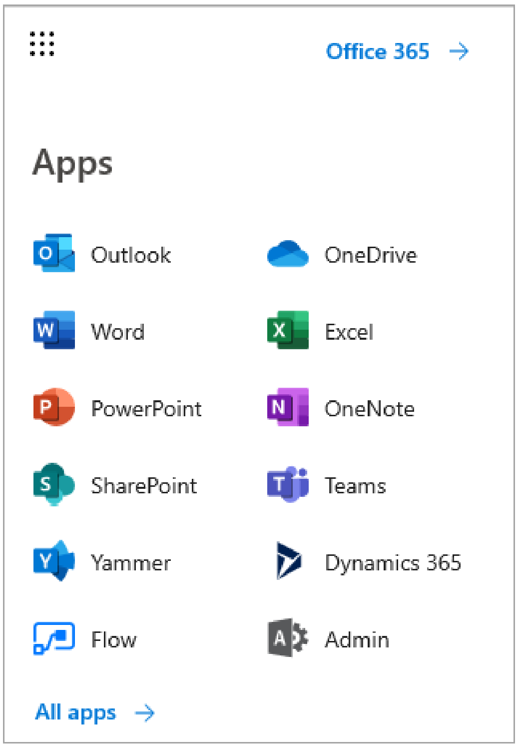
> **NOTE**
> To learn more about the SharePoint start page, see Find news, sites, and portals in Microsoft 365.

To view the SharePoint start page:

1. Sign in with your work or school account. For help, see Where do I sign in?.
2. Select SharePoint from the list of apps.



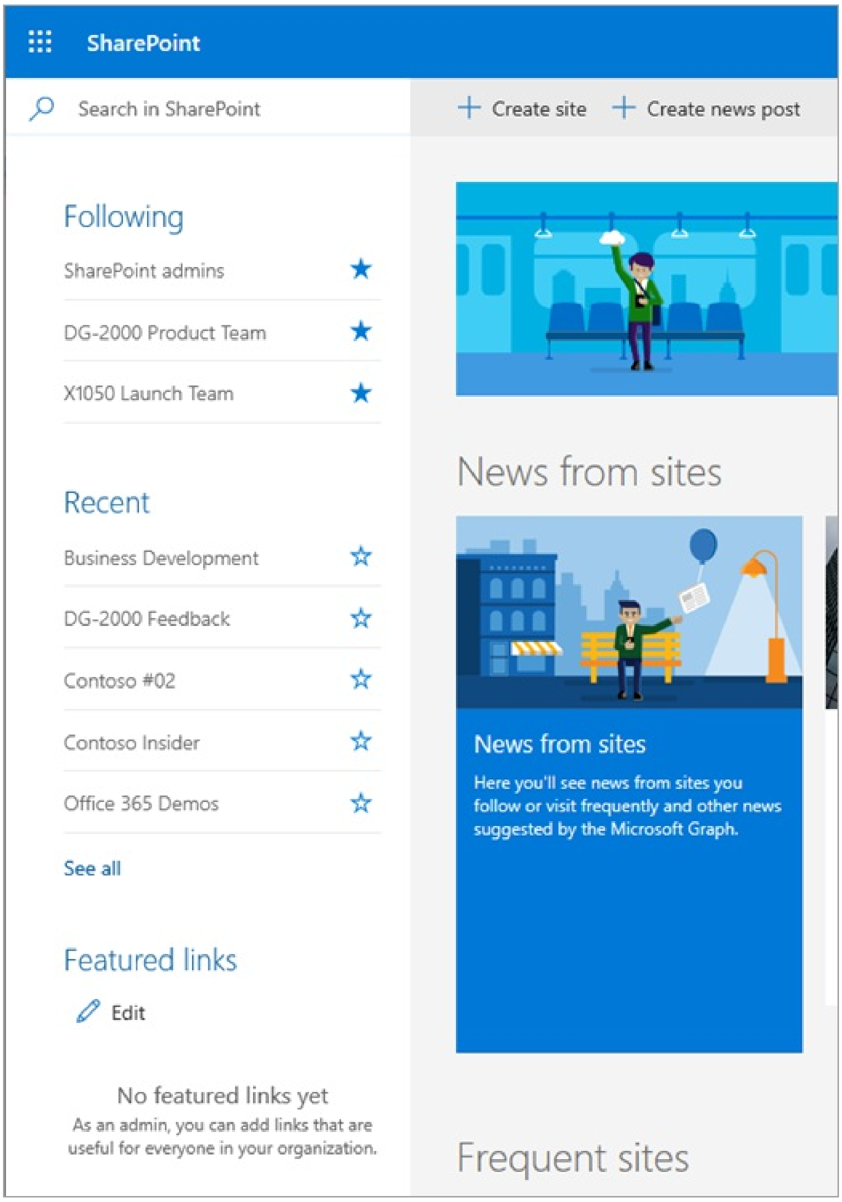
If you don't see the list of apps, select the app launcher icon in the top-left corner of the page, and then select **SharePoint**.



Can't find the app you're looking for? From the app launcher, to see an alphabetical list of all the available

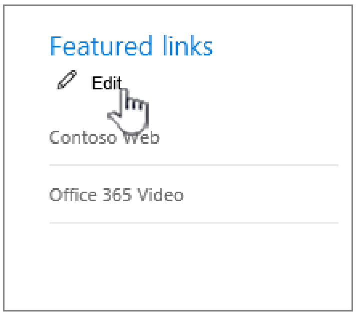
Microsoft 365 apps, select **All apps**. From there, search for a specific app.

On the left side of the page, a **Featured links** list appears.



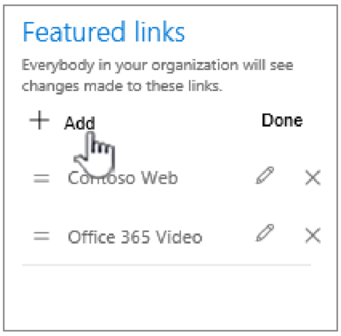
Add a link

1. Select **Edit**.

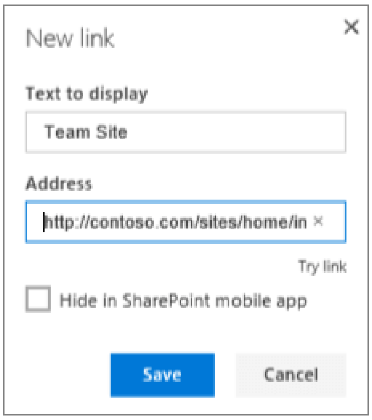


> **NOTE**
>
> If you don't see **Edit**, you don't have permission to change the Featured links list. Contact your administrator.

2. To add a link, choose **+ Add**.



3. Fill in the **Text to display** and **Address** in the **New link** dialog.



4. Select **Try link** to check the link.

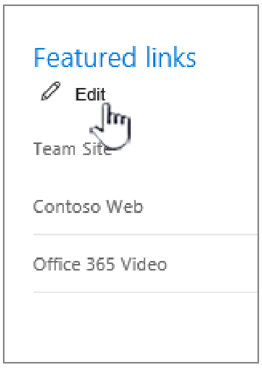
5. Select **Save**.

   The new link will appear at the top of the list. To change where the link appears, you can drag and drop it within the list.

6. To leave edit mode, select **Done** when you're finished.

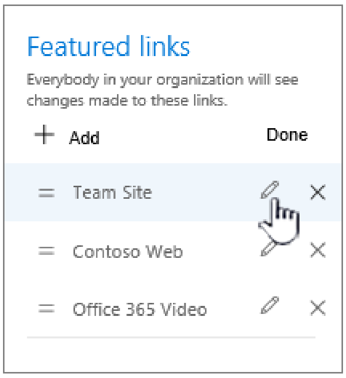
Edit a link

1. Select **Edit** at the top of the list.

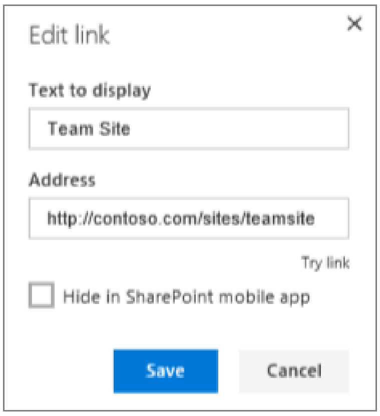


> **NOTE**
>
> If you don't see **Edit**, you don't have permission to change the Featured links list. Contact your administrator.

2. Select the link you want to change.



3. Fill in the **Text to display** and **Address** in the **Edit link** dialog.



4. Select **Try link** to check the link.

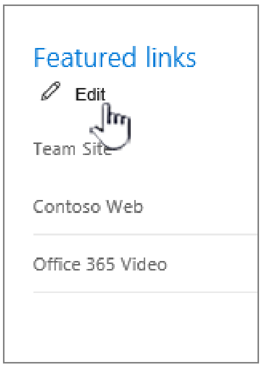
5. Select **Save**.

6. To leave edit mode, select **Done** when you're finished.

   To change where the link appears, you can drag and drop it within the list.

Change the order of links

1. Select **Edit** at the top of the list.



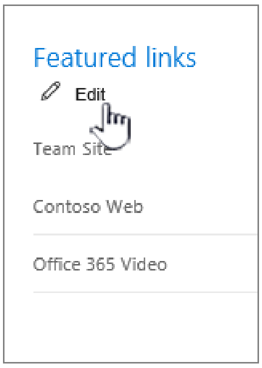
> **NOTE**
> If you do not see **Edit**, you don't have permissions to change the Featured links list. Contact your administrator.

2. Drag each link to the place you want within the list.

3. To leave edit mode, select **Done** when you're finished.

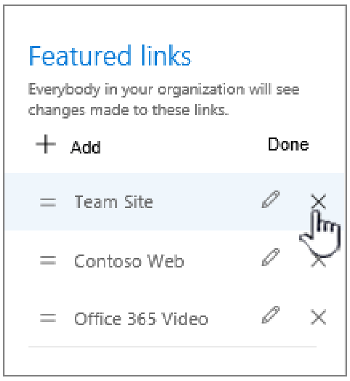
Delete a link

1. Select **Edit** at the top of the list.



> **NOTE**
> If you don't see **Edit**, you don't have permission to change the Featured links list. Contact your administrator.

2. Select **X**.



3. Select **Delete** in the confirmation dialog.

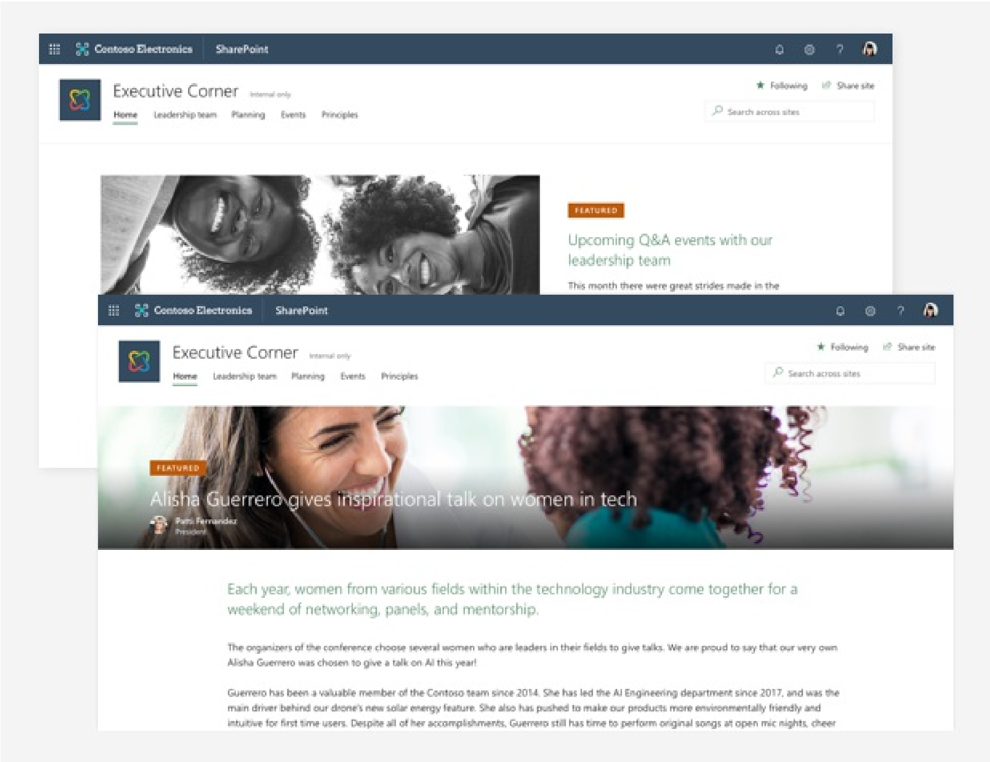
4. To leave edit mode, select **Done** when you're finished.

> **NOTE**
> If you had custom promoted sites in classic view of the SharePoint Sites page, the Featured links section of the SharePoint start page is pre-populated with those sites. The pre-population of promoted sites in the Featured links list happens only once when the first user visits the new SharePoint start page. If you go back to classic view and change the promoted sites, the changes will not be reflected in the Featured links list on the SharePoint start page.

Branding your SharePoint site

1/8/2021 • 3 minutes to read • Edit Online

In the modern SharePoint experience, you can easily change the look and feel of your site to match your company or organizational brand. You can customize the logo, colors, and navigation – often without writing a single line of code. Branding can be applied at the site level, to a group of sites, or to all sites within your organization.



> **NOTE**
>
> Branding your SharePoint site will not change the overall look of your Microsoft 365 service. For more info about branding Microsoft 365, see Customize the Microsoft 365 theme for your organization.

Site branding in the classic experience

In the classic SharePoint experience, there are a set of default themes that can require a considerable amount of customization to get them to match your organization's brand. Also, they aren't very responsive, making the experience on different devices inconsistent. Most site branding requires the use of custom master pages or alternate CSS configurations. Master pages provide a great deal of flexibility, but they can be problematic. For example, anytime updates are made to SharePoint, any customizations made to the master page may no longer work or may not work the way you expect them to. SharePoint ignores these customizations unless you're running in classic experience mode because they're incompatible with the modern user interface. To avoid this, use only the recommended modern approaches to brand your SharePoint sites.

Modern site branding

SharePoint includes an updated set of default site themes that are responsive and look great on any device. With site themes, you can customize your site's logo and colors to match your brand. Site designs provide specific layouts and other functionality for your site. Additional branding can be achieved using custom themes or site designs without worrying about something breaking when SharePoint is updated. Custom themes let you create additional color schemes beyond the defaults. Custom site designs let you control the site theme and other customizations like the site navigation, default applications, and other settings. Custom themes or designs can be applied to a new site when it's created or applied to an existing site or group of sites.

Branding hub sites

When you brand a SharePoint hub site, you can set it so the site branding is applied to any sites that associate with it. This includes any site theme or site design used by the hub site. This allows you to apply common navigation and branding across a set of sites and use accent colors to emphasize elements that need to stand out.

Classic experience vs. modern experience

Below is a summary of the differences between branding a site in the classic experience vs. branding in the modern SharePoint experience.

CLASSIC EXPERIENCE	MODERN EXPERIENCE
Unresponsive, OOB themes that you can customize	Responsive themes that look great on any device and can be customized to match your brand
Use custom master pages and CSS that are ignored in the modern experience	Use the SharePoint Framework to add header and footer, customize theme colors, etc.

Before you begin

Some things to consider before branding your classic experience sites in SharePoint are:

- Do you need a consistent brand across all sites or will different divisions, departments, or groups in your organization have their own?
- You should compile a list of all current sites, what site templates they use, any customizations that have been made to the master pages or CSS, and decide which of these customizations you need to keep. You can run the SharePoint "Modern" user interface experience scanner which will do a deep analysis of all the sites in your organization and create reports that give you details about sites that have incompatible master pages or alternate CSS settings. SharePoint handles branding differently for classic site templates such as the publishing site. You'll want to troubleshoot any custom theme issues you run into.
- What areas do you want to customize (logo, colors, fonts, header/footer, navigation)?
- Who in your organization can brand a site? You will need to make sure that they have site designer permissions or above to make these changes.

Ready to brand your classic SharePoint site using the modern experience?

Check out the below resources that provide more details about how to use the modern SharePoint experience to brand your site.

Branding SharePoint: The New Normal

Change the look of your SharePoint site

SharePoint site theming

Modernize site branding

Modernize your classic SharePoint sites

JSON schema

Theme generator

Sharing and permissions in the SharePoint modern experience

1/8/2021 • 6 minutes to read • Edit Online

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.

The three 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.
- **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 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. 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, but 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 a visitors permission for 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.

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. View-only permissions are managed through the site.

For details about how SharePoint and Teams interact, see How SharePoint and OneDrive interact with Microsoft Teams.

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.

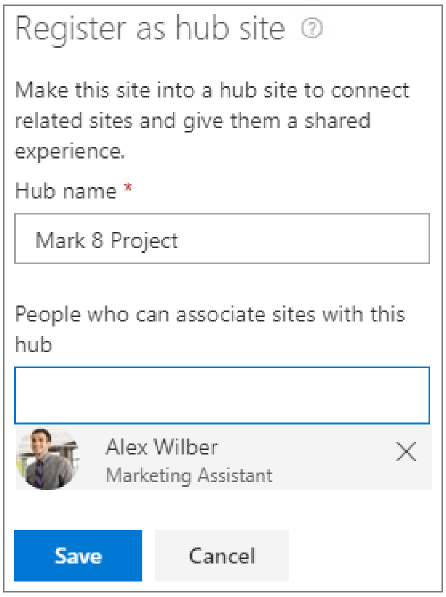
For information about how to share a site, see Share a site.

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 and cannot be changed by site owners.



Sharable 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 sharable 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.
- *People in your organization* links work for only people inside your Microsoft 365 organization. (They don't work for guests in the directory, only members).
- *Specific people* links only work for the people that users specify when they share the item.

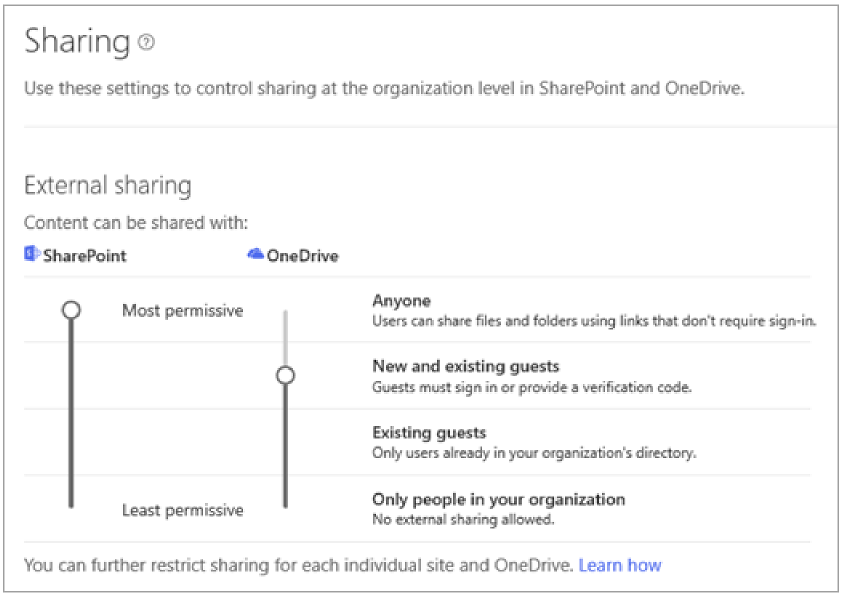
You can change the type of link that is presented to users by default for each site.

For more about the different types of sharing links, see 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). You can also use external sharing to share between licensed users on multiple Microsoft 365 subscriptions if your organization has more than one subscription. 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 for more information.

To set up guest sharing for a site, see Collaborate with guests in a 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 (Preview)

Azure AD B2B 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 one-time passcode feature is used for external sharing of files, folders, list items, document libraries and sites.

With Azure B2B 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 Preview.

See also

External sharing overview

Turn external sharing on or off for SharePoint

Collaborating with people outside your organization

Share SharePoint files or folders

Limit sharing in Microsoft 365

Moving from publishing sites to communication sites

11/2/2020 • 18 minutes to read • Edit Online

Being able to communicate broadly using attractive sites and pages is a key feature of organization intranets. For example, you might have an HR department home page that serves up important communication to hundreds or thousands of employees.

In the modern SharePoint experience, communication sites fulfill the same purpose as traditional publishing sites: to communicate broadly to a large audience while maintaining a level of control on the creation side. Communication sites support most of the same scenarios as publishing sites, and more capabilities are coming soon. Best of all, communication sites are easier to build and maintain and include new features such as a modern authoring canvas. They allow you to share news, reports, statuses, and other information in a visually compelling format. To sum up: you can quickly create beautiful pages that look great on mobile devices and that are accessible by default - all without heavy developer investment. You can get inspired with some great examples in the SharePoint look book.

Traditionally, sites and pages like this have been designed and built using the publishing features of Microsoft SharePoint – either team sites with publishing enabled or fully structured publishing sites. You could specify page layouts, design pages, and set up content approval workflows. Publishing features allowed for a tight level of control by a small number of people while allowing broad communication to many people. But with traditional design and deployment of publishing sites, developer involvement is usually required for customization of site functionality, navigation elements, and included investment in master pages, CSS, JavaScript, and web parts. Additionally, traditional site types designed for a PC browser may not work well or look attractive on mobile devices, and design and development efforts are needed to provide proper interaction with tools like screen readers or high-contrast color schemes. With all this, it commonly takes more time and resourcing to build, test, and deploy when using the classic publishing infrastructure.

Classic publishing site features that are not supported in modern communication sites

- **Classic Publishing Feature** – Turning on the classic publishing feature for a modern communication site is not supported. Instead, modern versions of the publishing features will be available outside of the publishing infrastructure. SharePoint Publishing Infrastructure is supported for a modern Team Site. For more info, see Enable publishing features.
- **Community Site Feature** – The Community Site feature is not supported for modern communication sites.
- **Video Content Type** – Video content type features are not supported for a modern communication site. Use the Stream web part as the modern replacement.
- **Classic Web Parts** – Classic web part features are not supported on a modern communication site. This includes script editor and content editor web parts. For more info, see Using web parts on SharePoint pages.
- **Save Site as a template** – The save site as a template feature is not supported on a modern communication site. For more info, see Save, download, and upload a SharePoint site as a template.
- **Save List/Library as a template** – The save list as a template feature will only work when custom scripts are allowed. For more info, see Allow or prevent custom script.
- **Reset to Site Definition** – The reset to site definition feature is not supported on a modern communication site.
- **Classic Record Center** – The Record Center feature is not supported on a modern communication site.

Instead, use the modern records management capabilities. For more info, see Records Management in Microsoft 365 and Learn about Records.

- **SharePoint 2010 and 2013 Workflows** – SharePoint 2010 and 2013 Workflows are not supported with modern communication sites. Instead, use Microsoft Power Automate. For more info, see Microsoft Power Automate and SharePoint 2010 workflow retirement.
- **Subsites** – Creation of subsites is available but not recommended. Additionally, a modern communication site as a subsite is not supported. Consider using the modern hub site feature instead. For more info, see What is a SharePoint hub site?

Get started: Move from a publishing site to a modern communication site

So, how you do move from publishing sites to communication sites? First, know that you don't have to change all your site collections and sites at once. If you have a very large collection of publishing sites, you can gradually begin using modern sites, pages, and web parts. For example, you can start with creating one or more new communication sites as home pages for existing sites. If you have several departments in your organization, you can create modern sites and implement modern features one department at a time. You can choose a strategy that works best for the size and scale for your organization. To help with determining your strategy, you can use the SharePoint Modernization scanner tool to find out which classic publishing features are used in your organization or in a subset of site collections. Find this tool and more information about it in Modernize classic publishing portals.

When you are ready to begin creating new communication sites and using modern features, here are some areas to consider:

- Structure and navigation
- Branding and site design
- Pages
- Web parts
- Sharing news
- Permissions and sharing
- Audience targeting
- Multilingual communication sites

Structure and navigation

Let's say your organization has a publishing site for Human Resources, with subsites for Benefits, Policies, Training, and Careers. It might be organized like this:

In this example, Human Resources is your site collection that includes four subsites for Benefits, Policies, Training, and Careers.

In the modern experience, you can use a hub to mimic the same structure while carrying design elements across related sites:

This structure is no longer hierarchical in the technical sense. Instead, it is a flat structure where each site is connected because they are part of the Human Resources hub. In this scenario, each site can be a communication site. But you can also include team sites for collaboration within the hub, while limiting their availability to the entire organization. With a hub, you can:

- Apply common navigation and branding across associated sites.
- Search across all associated sites.
- Easily aggregate news and other types of content across all sites.

The best part about hubs is that they are so flexible. As your organization changes, your intranet organization can change just as quickly, just by associating or disassociating a site.

To learn more about planning hubs, see Planning your SharePoint hubs. To create a hub, see Create a hub site. To learn more about navigation options and planning, see Planning navigation for modern SharePoint.

Branding and site design

In the modern SharePoint experience, it is easy to *change the look* and feel of your sites to match your company or organizational brand. You can customize the logo, colors, navigation, header, and footer – often without writing a single line of code. Branding can be applied at the site level, to a group of sites, or to all sites within your organization. SharePoint includes an updated set of default site themes and site designs (or templates) that are responsive and look great on any device. With site themes, you can customize your site's logo and colors to match your brand.

Coming soon are multiple options for headers and footers on communication sites, and options for navigation such as a mega menu. For these and other features that are in development, rolling out, or launched, check the Microsoft 365 Roadmap. To learn more about branding options, see Branding your SharePoint site. To learn more about planning navigation, see Planning navigation for modern SharePoint.

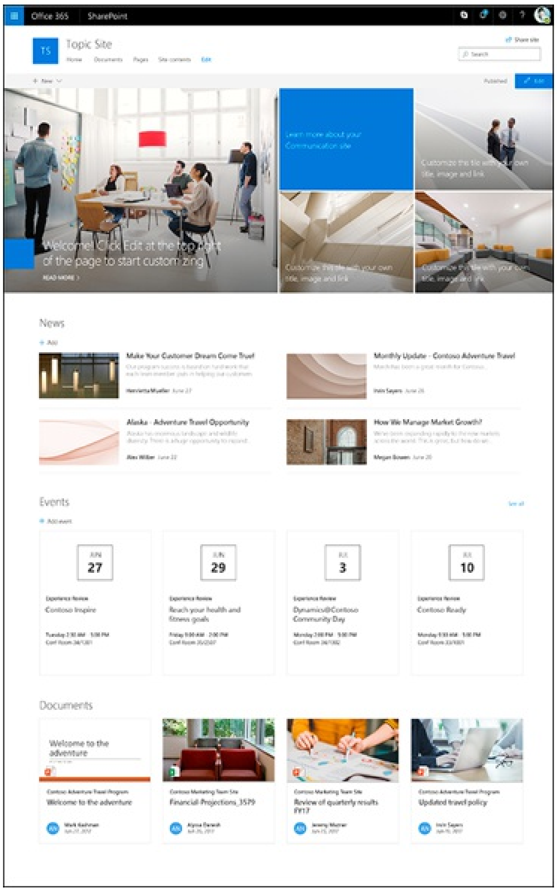
Classic site templates and modern site designs

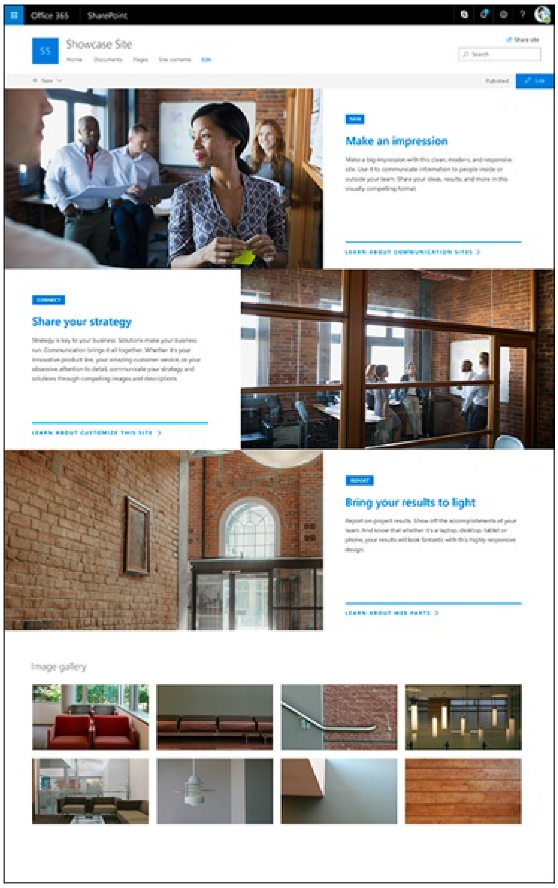
SharePoint handles branding differently for classic site templates, like the publishing site. Instead of a site template, communication sites have three out-of-the-box layout designs: *Topic*, *Showcase*, and one open layout: *Blank*.

When you create a communication site in SharePoint, you can start with a blank site or choose one of the other site designs, each of which comes with a default set of web parts. The options available are:

- **Topic** to share information such as news, events, and other content. The home page includes a Hero web part, to highlight and link to important content; a News web part, to distribute announcements, reports, status, and more; an Events web part based on a calendar list; and a Highlighted content web part to dynamically show documents based on your criteria.

- **Showcase** to use photos or images to showcase a product, team, or event. This is a highly visual design that includes a Hero web part with large imagery in a layered layout, and an Image gallery that can be displayed in several different layouts, such as a tiled layout or carousel layout.
- **Blank** to create your own design.





If you want more customized branding and theming applied to each new site, you can use site designs with site scripts to provide custom configurations to apply when new sites are created. They can be used each time a new site is created to apply a consistent set of actions. Common site design actions typically affect the site itself, such as setting the theme or logo, creating lists, or configuring navigation. You can find more information on how to use site designs and scripts at SharePoint site design and site script overview.

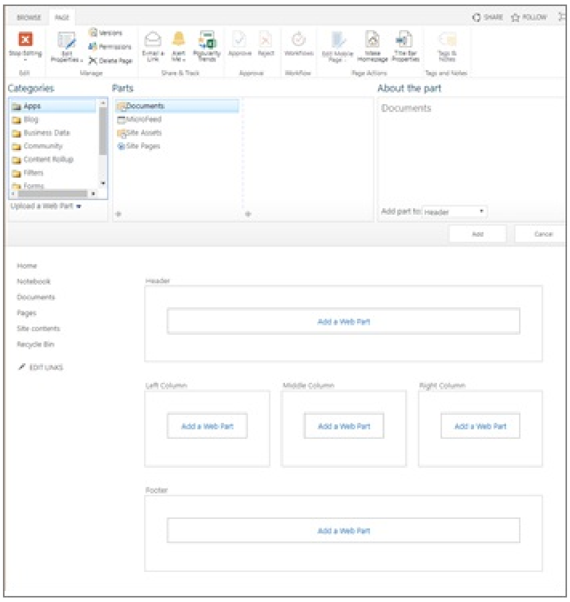
Pages

Master pages and page layouts are components of a publishing site. Page layouts and master pages work together to create the layout for a traditional SharePoint web page. Modern communication sites do not utilize master pages or page layouts, but do provide a greater level of flexibility for site owners and page authors.

In the classic experience, you may have created web part pages based on page layouts. Page layouts can be locked down to control what is authored on a page. However, they are inflexible in that pages based on page layouts are confined to the layout and options provided by the page layout.

Modern pages provide a fast, easy way to build responsive pages using the functionality of modern web parts. Pages are similar to classic web part pages and publishing pages, but are less structured and easier to create. And, each page's layout is flexible in that it can be changed anytime to align to the content for the page and the experience you are trying to create for your readers.

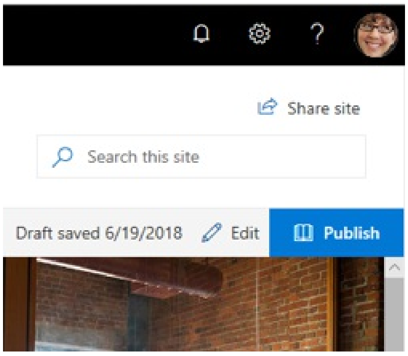
Classic web part page:



Modern web part page:

Pages are made up of a title area and sections. Sections can include a full-width column for full-bleed images or hero web parts or up to three regular columns. You can add a variety of web parts to the page, and easily move them around on the page to get the look you want. Check out this short video to see how to create, layout, and publish a page:

Publishing: On a classic publishing site, commands for Publish and Check in/Check out are available on the ribbon. In the modern experience, it is even easier for authors to discover how to edit and make their content visible with buttons to Edit, Save, and Publish right on the page. When a modern page is in edit mode, it is automatically checked out to the person who is editing. When a page is saved or published, it is automatically checked in. If someone has a page open for editing but hasn't made any changes to it for at least 5 minutes, it is automatically saved and taken out of Edit mode so that others can access and edit the page.



To learn more about how to create and edit pages, see Add a page to a site.

Content approval for pages

Content approval ensures that edits to pages meet company policies or standards. Classic publishing allows for content approval on pages using out-of-the-box workflows. Modern pages also provide for content approval and once it is enabled, users need only to press a Submit button on the page to start the approval flow. The recommended way to do this is to use the built-in Power Automate commands. Learn more at Page approval flow.

Scheduling

Scheduling content to "go live" at specific times is a feature of classic publishing sites and now a feature of modern pages. To learn more about modern page scheduling, see Schedule a SharePoint page or news post to go live at a specific time.

Moving from classic to modern pages: At this time, there is not a way to change a classic page into a modern page without using a multi-step code solution, which may work well for IT Admins and developers. If you are neither of those, we recommend you gradually start planning for and creating modern pages, as needed.

If you are using a classic publishing site, you should know that it is possible to create modern pages in a classic publishing site, but there is not an automated way to move from a publishing site to a communication site. To move to a communication site, we recommend you begin creating modern pages in a new communication site rather than in a classic publishing site.

There are several important advantages to moving to a new communication site. One of the most important advantages is that you can use the upgrade as an opportunity to re-think the "story" of your site and validate that the content is needed, up-to-date, and relevant to users. In addition, you can use the move as a time to look at the content that is no longer needed it and remove it. Cleaning up your unused content improves both user experiences and search outcomes – so consider the move as an opportunity to clean up legacy content and establish new governance practices to make sure that your content is kept up-to-date going forward.

Wiki pages

Wiki pages are a content type available in publishing sites, but they are not available in communication sites. However, you can create modern pages using either a Text web part or Markdown web part to cover many of the same scenarios as Wiki pages. Note that Wiki syntax is not available in a Text web part, with the exception of adding a hyperlink with the use of brackets "[[".

Web parts

Modern pages use modern web parts. Modern web parts are designed to be easier to use, faster, and look great on all devices. It is important to note that for security reasons, modern out-of-the-box web parts do not allow for the insertion of custom code including JavaScript.

> **IMPORTANT**
>
> Classic web parts cannot be used on modern pages and modern out-of-the-box web parts cannot be used on classic pages. Developers may create custom modern web parts that may work on both classic and modern pages. Additionally, there is not a 1:1 mapping of classic to modern web parts, but there are web parts that have similar purposes.

To learn about all of the modern web parts, see Using web parts on SharePoint pages. To learn about modern web parts that have similar purposes to classic web parts, see Classic and modern web part experiences.

For developers, the SharePoint Framework allows for the building of custom modern web parts that appear alongside out-of-the-box web parts in the web part toolbox. The SharePoint Framework also allows for custom extensions, the use of the Microsoft Graph API, as well as secure access to third-party solutions and APIs secured by Azure Active Directory. Developers are encouraged to consult the SharePoint starter kit, where you'll find a fully built sample solution that includes numerous web parts, extensions, and other components that you can use as an example and inspiration for your own customizations. Additionally, find design guidance and standards for web parts at Designing great SharePoint experiences.

Web parts unique to publishing sites

Publishing sites include a variety of web parts that enable authors to insert video, rich text, forms, and dynamic content onto a site page. Three web parts that have been unique to publishing sites are the *Content query* web part to show dynamic content, the *Summary links* web part, and the *Table of contents* web part to display links to important content. The following are a selection of modern web parts that help fulfill the same purposes as these web parts.

Content query: The Highlighted content web part serves a similar purpose as the Content Query web part. It dynamically displays content from a document library, a site, a site collection, or multiple sites. With the Highlighted content web part, many of the advanced and confusing search/query options of the Content Query web part have been replaced with streamlined query options. However, unlike its classic counterparts, custom display templates are not allowed.

Summary links, Table of contents: There is not a 1:1 mapping of these web parts to modern web parts. However, there are several modern web parts that can fulfill the same purpose, which is to help your users navigate from a page level to important content. These are:

> Quick links
>
> With Quick links, you can add links to a page and set display options like a carousel format called filmstrip, list, or a smaller compact format. Each of the links in the compact format can be arranged and displayed with or without images. It is currently not possible to populate Quick links based on a SharePoint list.
>
> Link
>
> The Link web part shows one complete URL link and adds the ability to show or hide a preview pane with the link target.
>
> Hero
>
> The Hero web part is, by default, included on both the Topic and Showcase communication site templates. It is an attractive way to bring focus and visual interest to your page. You can display up to five items in the Hero web part and use compelling images, text, and links to draw attention to each. You can use the Hero web part at the top of a page or anywhere in the page as well. In general, you don’t want to use more than one hero web part on the same page. And, if you have more than 5 critical items to emphasize, consider using a different method to feature this content, such as the Quick links web part in a grid view.
>
> Text

> In the Text web part, you can add links within your content using the toolbar. Additionally, with the Text web part you can create a link that opens in a new tab.

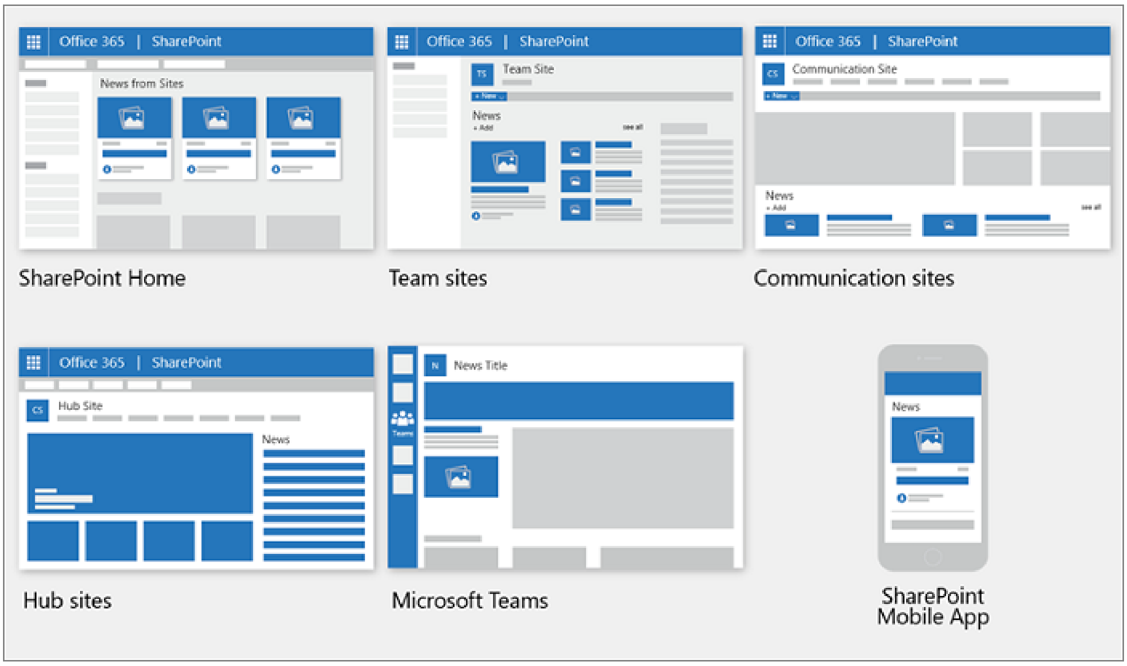
To learn more about modern web parts that have similar purposes to classic web parts, see Classic and modern web part experiences.

Sharing news

The News feature is an effective distribution system created to deliver relevant content across your organization.

Built on modern pages and web parts, you can tell stories with rich, attractive content that can be dynamically shown on the SharePoint start page, on team sites, communication sites, hubs, and even on the SharePoint mobile app. You can also choose to show News in a Teams channel.

Where news can be distributed



News posts can be created from the SharePoint start page, from a team site or communication site, and from pages that have the News web part on them already. You can customize sources and layouts of news, and you can also organize and order news posts as well as target specific audiences for news. To learn more about how to create and share News, see Create and share news on your SharePoint sites.

Users and permissions

You probably don't want a large group of people having the ability to make changes to your site that communicates information to a whole department or organization. Publishing portal sites included roles such as Approvers and Designers. Communication sites present a simplified experience, so not all these roles are present by default. While you could set up roles like these manually, we recommend that you use the new sharing interface, which also can provide you with needed controls.

To help you limit who has permissions to change the site, communication sites are not group-enabled like modern team sites. This means that a communication site is not automatically connected to a group of people with edit permissions. However, you can give specific people permission to make changes to your communication sites by selecting **Site permissions** under **Settings** and then **Share a site**. You can use Advanced permissions to give even more granular permissions if needed. For more in-depth information on the differences between classic and modern permissions, see Permissions and Sharing in the SharePoint modern experience.

You can also share a communication site externally if needed from the SharePoint admin center.

Audience targeting

In the classic experience, many types of content can be targeted to appear only to people who are members of a particular group or audience. This capability is available in the modern experience with modern Pages and documents, the News web part, the Highlighted content web parts, and navigation. For example, if you have two departments within your organization that have different policies, you can choose to show a News post about a policy to just the people in the department that the policy applies to. To learn how to enable audience targeting, see Target content to specific audiences.

Multilingual communication sites

If your organization spans a diverse population, you may want to make content in your intranet sites available in multiple languages. User interface elements like site navigation, site title, and site description can be shown in the user's preferred language. Additionally, you can provide pages and news posts on communication sites that you translate and that are shown in the user's preferred language.

To create pages on communications sites in different languages, you use the translation feature to make copies of pages created in your default language. The copies can then be manually translated. Published translation pages are automatically shown in the appropriate language site, including in the News and Highlighted content web parts for each language.

To learn how to set up and use the multilingual feature for communication sites, see Create multilingual communication sites, pages, and news.

> **NOTE**
>
> At this time, the multilingual feature is available for communication sites only.

Customizing SharePoint

6/5/2020 • 6 minutes to read • Edit Online

In earlier versions of SharePoint, it was possible to make changes to a SharePoint environment by deploying custom code that would run in the physical SharePoint server environment. Changes made to SharePoint that didn't require the deployment of custom code were referred to as "customizations", because the changes were not fundamentally changing the product's functioning but were rather configuring the existing product in a unique way. Examples of customizing SharePoint Server have included deploying custom branding elements such as master pages and style sheets to a site collection; deploying pre-configured web parts to a web part gallery; creating custom workflows in SharePoint Designer; changing the look and feel of list forms using InfoPath; and more. Because of the shared nature of the SharePoint infrastructure, Microsoft does not allow the deployment of custom code to its environment. As a result, the concept of customizing SharePoint as opposed to deploying custom code is no longer a relevant paradigm. However, it's still helpful to think of ways that SharePoint can be customized, or configured uniquely, in a broader sense of the word.

The purpose of this document is to help you understand how you can customize your SharePoint environment using modern tools and techniques.

Branding

Modern SharePoint sites allow you to change the look of the site by modifying elements such as the site logo and the colors used throughout the site. Branding your SharePoint site can help you match a site to a brand as well as help users differentiate between multiple SharePoint sites. While several themes options are available by default, it's also possible to specify unique theme colors by supplying SharePoint with a custom configuration file. Older, "classic" SharePoint sites allow administrators to apply custom branding and page layouts to a SharePoint site by applying a custom master page, applying a custom theme to a site, deploying custom page layouts, and more. Because classic sites are not as fast and mobile-friendly as modern sites, Microsoft recommends using modern sites going forward.

Navigation

Navigation helps users find the information they need quickly by providing links to pertinent information in a persistent manner. Planning your navigational strategy in modern sites is a critical element in the usability of your SharePoint environment. Modern SharePoint sites provide a streamlined model for adding navigational elements using the browser. The position of the navigation is determined by the kind of site being viewed, the size of a user's screen, and whether the megamenu option has been enabled for the site. Additionally, modern sites can take advantage of hub site navigation.

Note that legacy versions of SharePoint allowed navigational elements to be dynamically generated using the structured navigation and managed metadata navigation providers. These options are no longer available in modern sites. However, if you are using a classic site with modern pages, you can still use these providers and the modern pages will reflect the correct navigational links. In terms of layout, because modern sites do not allow you to customize the site's master page or style sheet, it's not possible to move the position of the navigation elements on the page as could be done in classic SharePoint sites.

Page content

Nearly every version of SharePoint has had a way of creating custom layouts for web pages, whether that was by selecting a web part page, a wiki page layout, or a publishing page layout. Modern sites also provide a similar functionality. However, rather than providing a static layout that provides a set number of editable regions on the page, modern pages provide the ability for page editors to "stack" column layouts on a row-by-row basis. Page editors can also choose various options related to how the title region of the page is displayed. Finally, the most fundamentally way to customize a modern page is to place custom content on the page. This can be done by adding modern web parts to the page. Note that web parts used in classic web sites will not work in modern sites. However, it is possible to create and deploy custom ("client-side") web parts that were created using the SharePoint Framework.

Workflows

Microsoft recommends using Power Automate for configuring and executing all workflows in your Microsoft 365 environment, including SharePoint. For example, it's possible to create unique approval workflows for content stored in SharePoint. Additionally, it's possible to use Power Automate as the default workflow engine for approving SharePoint page content, directly from the SharePoint user interface. Flows can be triggered by SharePoint actions (such as when an item is created in a list), or perform actions within SharePoint (such as update a list item). While SharePoint Designer workflows are still supported, new workflows should be created using Power Automate.

Forms

Power Apps can be used to create custom forms for use in modern SharePoint sites. There are several ways in which these Power Apps forms can be used in your SharePoint site:

- As a custom SharePoint list form
- As a custom SharePoint list view
- As a stand-alone app that uses a SharePoint as its data source

You can embed a Power App form in a modern page using the Power Apps web part.

Forms that were previously created using InfoPath and hosted in SharePoint using InfoPath Forms Services should be converted to Power Apps forms, as Microsoft has announced the deprecation of InfoPath.

Microsoft Forms can also be used for easily creating light-weight forms. Like Power Apps, it's possible to embed a Microsoft Form in a page using the Microsoft Forms web part.

Customize your SharePoint site programmatically

Legacy versions of SharePoint Server relied on solution packages to deploy content and make configuration changes to SharePoint sites. It's still possible to programmatically provision sites as well as customize team sites, lists and libraries, and site pages. There are various methods for making programmatic changes to your SharePoint environment, including using the Office Developer Patterns and Practices APIs, the Microsoft 365 CLI, the Microsoft Graph API, the SharePoint Framework, and more.

Use the SharePoint Framework (SPFx) to render custom web parts on a modern SharePoint page. Additionally, Extensions to the SPFx provide the ability to add scripts to pages, create modified views of data, and surface new commands in the SharePoint user interface. SPFx application packages can be deployed to SharePoint sites using the SharePoint App Catalog.

Use third-party add-ins and solutions

Not only can you deploy custom apps (also known as add-ins) to your environment, but you can also purchase add-ins from the SharePoint Store. You can make these add-ins available to all users across the sites in your organization by acquiring licenses for all users in your organization. Or, you can acquire licenses for only those who need to use it, and assign those licenses to the designated users. For more information, see Buy an app from the SharePoint Store and Manage app licenses for a SharePoint environment.

If you want to change the settings for whether or not site users can acquire apps from the SharePoint Store, see Configure settings for the SharePoint Store.

If you are interested in exploring services or applications from Microsoft partners that are available for SharePoint, browse Microsoft 365 apps on Microsoft AppSource. There are also many open-source solutions developed by the collective SharePoint community, including Microsoft, MVPs, Partners, and Customers on the Microsoft 365 Developer Patterns and Practices GitHub site.

Examples of modern customization approaches

The following table gives an example of older methods for customizing sites along with a current recommended approach:

LEGACY	MODERN
Implement branding using custom master pages, page layouts, and themes	Use the "apply a look" option to customize branding elements like logo, header, footer and colors
Use custom navigation providers such as structured navigation or managed metadata navigation to dynamically generate navigational elements	Manually specify navigational links
Create a wiki page and choose a text layout option to modify the layout of the page	Create a modern page and add section layouts to the page to arrange web parts on the page.
Create a workflow using SharePoint Designer	Create a workflow using Power Automate
Customize a SharePoint form using InfoPath	Customize a SharePoint form using a Power App
Deploy a web part to a site using a sandbox solution	Use the SharePoint App Catalog to deploy a client-side web part to a site

Change the default list and library experience

3/10/2020 • 2 minutes to read • Edit Online

The new SharePoint list and library experience is faster, simpler, and responsive on mobile devices. It also supports many new capabilities that are not available in the classic experience, including Power Apps and Power Automate integration, the Filters pane, and column formatting. Many sites that have features or customizations that don't work in the new experience will automatically switch back to the classic experience. For more information about this behavior, see Differences between the new and classic experiences for lists and libraries. To detect lists that won't work well with the new experience, run the SharePoint Modernization scanner.

It's no longer possible to select the classic experience as the default for all sites in your organization. Instead, we recommend setting it for only the specific sites that need it. To learn how to turn off the new list and library experience for a site collection, see Enable or disable site collection features. For info about changing this setting using PowerShell, see Opting out of the modern list and library experience.)

> **NOTE**
>
> Users can select the default experience for an individual list or library, overriding what you set. For info, see Switch the default experience for lists or document libraries from new or classic.

Classic home page modernization

6/18/2020 • 4 minutes to read • Edit Online

Modernizing the home page of a classic SharePoint team site makes the page look great on any device and makes it easier for users to customize the layout and see news and activity. This article covers all the details on how automatic modernization works and the controls you have as an administrator.

How it works

If a classic team site meets the following criteria for being updated, the home page will automatically modernize the next time a user visits. When users first experience the change, they'll see a walkthrough that highlights the new capabilities and includes a link to a help article with more details.

We encourage users to adopt the change in order to benefit from the power of modernized pages. However, if site admins or site owners want to revert to the classic home page, they can. Instructions are available in the support article.

Update criteria

- Classic team site (STS#0) only.
- Home page name in any language is 'Home.aspx'.
- Contains default web parts only: getting started (GettingStartedWebPart), Newsfeed (SiteFeedWebPart), and document library (XsltListViewWebPart).
- No text is present (wiki HTML is not customized).
- DisplayFormTemplateName = "WikiEditForm".
- ModernizeHomepageOptOut feature is not activated.
- No custom master pages are detected.
- The classic publishing feature is turned off.

> **NOTE**
> All update criteria must be met for a team site home page to qualify for the automatic upgrade.

The technical details

- Applies to both STS#0 site collections and all corresponding subsites.
- The update applies only to the home page. No other classic pages will be changed. We recommend using the SharePoint PnP modernization framework for all other site pages.
- The new modern home page is named 'Home.aspx' and the classic page gets renamed to 'Home(old).aspx'.
- This update does not create a Microsoft 365 Group for the team site.
- Classic site themes may not be identical once your page is updated to modern. Learn how to apply custom styles and color to your site.
- Only site admins can revert to the classic home page through the link appearing in the left navigation.

Site owners can revert to the classic page by visiting site pages and marking the classic page as their home page.

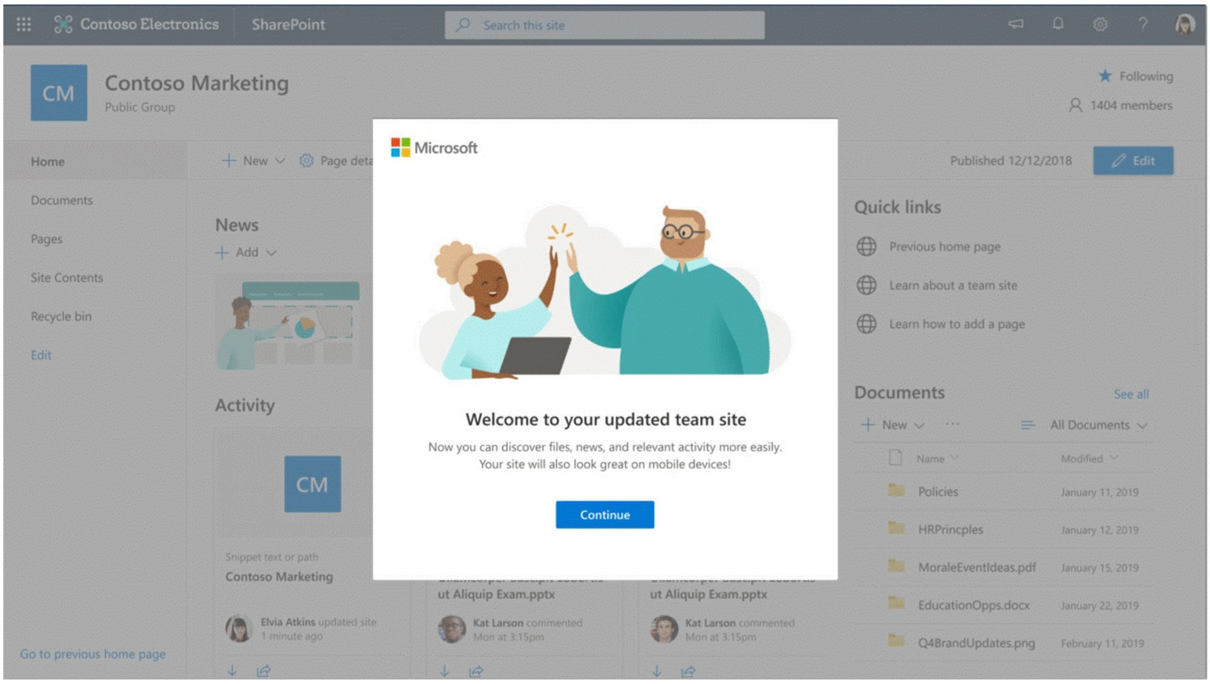
- Update happens on demand based on next site access. If a subsite is accessed, it will trigger the update for its root site collection and its other subsites. Remember, the update only applies to the root site collection and subsites if the criteria are met.
- We do not check the state of custom actions, therefore they will not transfer to your new modern page.
- We do not check the state of modern SharePoint lists and libraries for classic sites.

Why update classic team site home pages to modern?

Over the years, SharePoint modern pages have become powerful tools for collaboration and productivity at work and we want more users to take advantage of these capabilities. Automatically modernizing team site home pages that are not customized is the first step to helping classic site users get more out of SharePoint.

What to expect after a classic team site home page is updated to modern

When users first experience the change, they'll see a walkthrough that highlights the new capabilities and includes a link to a help article with more details like this:



For more training, download the classic to modern walkthrough.

How to prevent specific sites from being updated

To disable the update on specific sites, use one of the following options:

Option 1: Use PnP PowerShell to prevent a specific site from being upgraded by enabling a web scoped feature on each site and sub site that's being impacted.

Connect to the site using Connect-PnPOnline. For example,

```
Connect-PnPOnline -Url https://[tenant].sharepoint.com/sites/siteurl -Credentials $cred
```

To prevent modernization of an uncustomized home page, run:

```
Enable-PnPFeature -Identity F478D140-B148-4038-9CB0-84A8F1E4BE09 -Scope Web
```

If you later want to re-enable modernization of that page, run:

```
Disable-PnPFeature -Identity F478D140-B148-4038-9CB0-84A8F1E4BE09 -Scope Web
```

Option 2: Don't know what sites will be impacted by this change? You can use the SharePoint Modernization Scanner and run the scanner in "HomePageOnly" mode. The output of the modernization scanner run contains a file called SitesWithUncustomizedHomePages.csv. Use this file to get a list of sites and sub sites that will get a modern homepage. This tool will enable you to message users impacted if desired. If needed, use the PowerShell cmdlet above, or the following sample script to opt multiple sites out of the update: https://github.com/SharePoint/sp-dev-modernization/tree/dev/Scripts/HomePageModernizationOptOut

Option 3: Add an out-of-the-box SharePoint web part, a custom web part, or text to your team site home page.

> **NOTE**
>
> It's highly recommended that you modernize home pages to benefit from the latest SharePoint features and to improve the viewing experience for users on desktop and mobile. Another option for modernizing classic sites is to enable the communication site experience on a specific classic site. For info, see Enable the communication site experience on classic team sites.

What about new classic team sites STS#0 created after this change?

Classic team sites (STS#0) created after **May 1, 2020** will not get updated.

Can I also modernize the other pages in my sites?

For a more consistent user experience, we recommend that you modernize all pages on classic team sites. This can be self-service done via the open-source SharePoint PnP Page Transformation solution.

Getting excited about modern?

For more help in transitioning to modern, refer to the following resources:

- Guide to modern experience in SharePoint
- SharePoint modern inspiration
- Modernizing your classic sites
- Transform classic pages to modern pages
- Enable the communication site experience on classic team sites

Enable the communication site experience on classic team sites

11/2/2020 • 4 minutes to read • Edit Online

A SharePoint communication site is a great tool for sharing information with others in your organization. Your users can share news, reports, statuses, and other information in a visually compelling format. Now, any classic team site can have this capability too. By running a PowerShell cmdlet, you can bring modern communication site features to your classic team sites.

Requirements

- The site must be a **classic team site that's not connected to a Microsoft 365 group** (the STS #0 site template).
- The site must be the top-level site in the site collection. It can't be a subsite.
- The user who runs the PowerShell cmdlet must have full owner permission on the target site.
- The site must not have SharePoint Server Publishing Infrastructure enabled at the site collection level or SharePoint Server Publishing enabled at the site level. Learn how to enable and disable publishing features. If these features were previously enabled but have been deactivated, go to the site contents page and make sure it doesn't still contain a Pages library. Learn more about features enabled on a publishing site

Effects of this change

- A new modern page is created in the site and set as the home page. Open the site in a new tab to see the changes.
- Any user that has access to the site will see the new home page with the default web parts and content immediately. Until you're ready to launch the new communication site experience, you can change the home page back to the former page.
- Full width pages with horizontal navigation are available. (The top navigation from classic view is hidden, but can be seen on classic pages like the site settings page.) You can now customize the navigation on this site.
- Custom script isn't allowed on the site.
- Minor versioning on the Site Pages library is enabled. Learn more about versioning
- Site Pages are the default content type in the Site Pages library
- No site permissions are changed.
- The SharePoint lists and libraries experience isn't changed.
- Any content types enabled in the site aren't changed.
- If the classic site collection had subsites, they aren't changed.
- If you intend to launch this site as a high traffic portal experience or share the site with a large number of users, make sure to follow the portal launch guidelines.

Run the PowerShell cmdlet

You can use either the SharePoint Online Management Shell **OR** SharePoint PnP PowerShell to enable the communication site experience on a classic team site. We recommend that you test the experience with a minimally used classic site before running it on popular classic sites in your organization.

> **IMPORTANT**
>
> After you enable the communication site experience on a classic site, you can't undo the change.

SharePoint admin instructions

1. Download the latest SharePoint Online Management Shell. Version 20122.1200 or later is required.

   > **NOTE**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
   > On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

   ```
   Enable-SPOCommSite -SiteUrl <URL of target site>
   ```

For more info about this cmdlet, see Enable-SPOCommSite.

Site admin instructions

1. Learn how to use SharePoint PnP PowerShell commands.

2. In Windows 10, run the following commands in PowerShell:

   ```
   Install-Module SharePointPnPPowerShellOnline
   Connect-PnPOnline –Url <Url of Targetsite> –Credentials (Get-Credential)
   Enable-PnPCommSite
   ```

Frequently asked questions

Will this cmdlet change all my classic sites?

- No. The cmdlet can be run on one site at time.

Will this cmdlet change the site template?

- No. The cmdlet enables communication site features, but the site still has the STS#0 site template. The site will continue to appear as "Team site (classic experience)" in the SharePoint admin center.

Why can't I use this cmdlet on publishing sites?

- The modern communication site experience isn't compatible with SharePoint Server publishing features.

Can I run this command on the root site in my organization?

- Yes, if you meet the requirements listed at the beginning of this article.

How can I get a list of all classic sites that have the communication site experience enabled?

```
function Get-CommsiteEnabledSites{

    $adminUrl = Read-Host "Enter the Admin URL of 0365 (eg. https://<Tenant Name>-admin.sharepoint.com)"
    $userName = Read-Host "Enter the username of 0365 (eg. admin@<tenantName>.onmicrosoft.com)"
    $password = Read-Host "Please enter the password for $($userName)" -AsSecureString

    # set credentials
    $credentials = New-Object -TypeName System.Management.Automation.PSCredential -argumentlist $userName,
$password
    $SPOCredentials = New-Object Microsoft.SharePoint.Client.SharePointOnlineCredentials($userName,
$password)

    #connect to to Office 365

    try{

        Connect-SPOService -Url $adminUrl -Credential $credentials
        write-host "Info: Connected succesfully to Office 365" -foregroundcolor green

    }

    catch{

        write-host "Error: Could not connect to Office 365" -foregroundcolor red
        Break connectToO365

    }
    get-siteCollections
}



function get-siteCollections{

    write-host "----- List of classic sites with comm site feature enabled  -------" -foregroundcolor green

#Get all site collections
 $siteCollections = Get-SPOSite

 #loop through all site collections
 foreach ($siteCollection in $siteCollections){

  #set variable for a tab in the table
  $pixelsweb = 0
  $pixelslist = 0
  $enabledCommSite = Get-SPOIsCommSiteEnabled($siteCollection.url)
  $background = "white"
  if($enabledCommSite -ne ""){
   $background = "cyan"
  }
 }
}

function Get-SPOIsCommSiteEnabled($url){

    #fill metadata information to the client context variable
    $featureID = "f39dad74-ea79-46ef-9ef7-fe2370754f6f"
    $context = New-Object Microsoft.SharePoint.Client.ClientContext($url)
    $context.Credentials = $SPOcredentials
    $web = $context.Web
    $context.Load($web)
    $context.load($web.Features)

    try{

        $context.ExecuteQuery()
        $isCommSiteEnabled = $web.Features | Where {$_.DefinitionID -eq $featureID}
  $webTemplate = $web.WebTemplate
```

```
    if($webTemplate -ne "SITEPAGEPUBLISHING" -AND $isCommSiteEnabled){
        write-host "Found $($web.url)" -foregroundcolor green
     return "Enabled"

    }
      }
      catch{

          write-host "Could not find web" -foregroundcolor red

      }

      return ""
  }

  Get-CommsiteEnabledSites
```

See also

For info about automatically modernizing the home page on classic sites, see Classic home page modernization.

Differences between the classic and modern search experiences in SharePoint

1/8/2021 • 2 minutes to read • Edit Online

SharePoint in Microsoft 365 has both a classic and a modern search experience. Microsoft Search in SharePoint is the modern search experience. Both search experiences use the same search index to find results.

As a search admin, you can't enable or disable either search experience, both are enabled by default. Users get the classic search experience on publishing sites, classic team sites, and in the Search Center. Users get the Microsoft Search experience on the SharePoint start page, hub sites, communication sites, and modern team sites. Learn about classic and modern sites

The most visible difference is that the Microsoft Search box is placed at the top of the SharePoint, in the header bar. Another difference is that Microsoft Search is personal. The results you see are different from what other people see, even when you search for the same words. You'll see results before you start typing in the search box, based on your previous activity and trending content in Microsoft 365, and the results update as you type. Learn more about the Microsoft Search experience for users.

Search admin can customize the *classic* search experience, but not the Microsoft Search experience. As a search admin you can *tailor* Microsoft Search to your organization so it's easy for your users to find often needed content in your organization.

You use the SharePoint admin center to manage classic search and the Microsoft 365 admin center to manage Microsoft Search. Certain aspects of the classic search settings also impact the modern search experience:

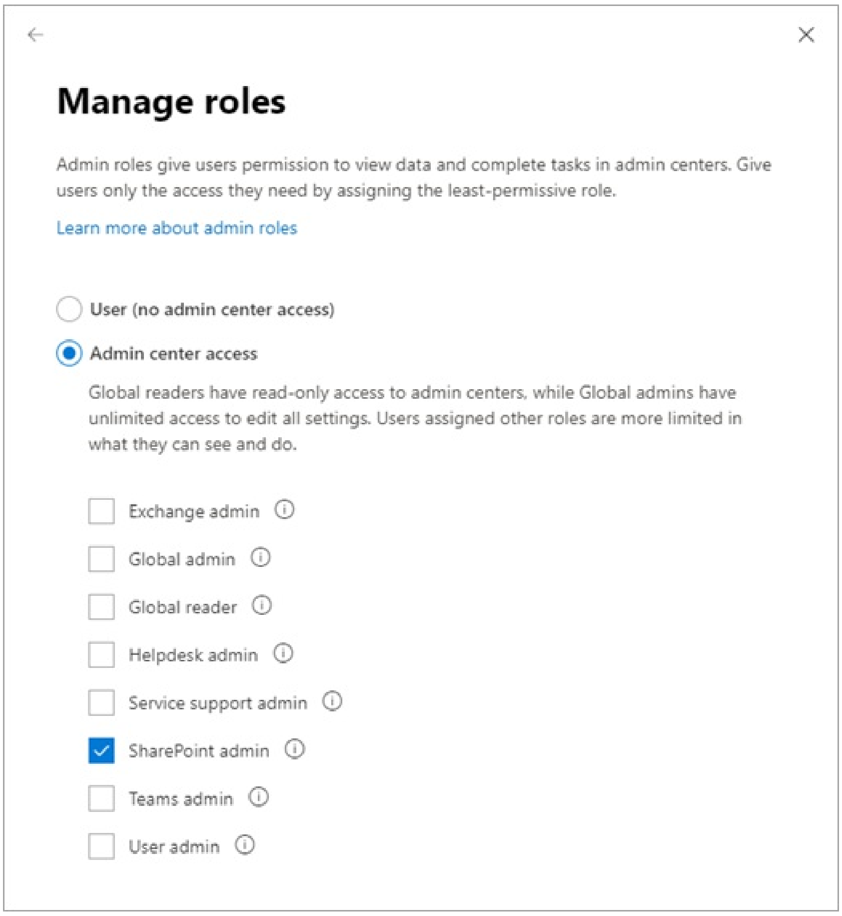
- The search schema determines how content is collected in and retrieved from the search index. Because both search experiences use the same search index to find search results, any changes you make to the search schema, apply to both experiences. The Microsoft Search experience doesn't support changing the sort order of results or building refiners based on metadata. Therefore, the following search schema settings don't affect the Microsoft Search experience:
  - Sortable
  - Refinable
  - Company name extraction (to be deprecated as of November 15th, 2019)
- The modern search experience only shows results from the default result source. If you change the default result source, both search experiences are impacted.
- Depending on the search scenario, some Microsoft Search features might not work if the classic global Search Center URL is not set to "yourcompanyname.sharepoint.com/search/pages". Ensure that the Search Center site collection exists, that its URL is set to "yourcompanyname.sharepoint.com/search/pages", and that all users have read access to it.
- If you temporarily remove a search result, the result is removed in both search experiences.
- The classic search experience lets admins define **promoted results** to help users find important content, while the Microsoft Search experience uses **bookmarks** to achieve the same. When you create a promoted result at the organization level, users might also see it on the **All** tab on the Microsoft Search results page if they searched across the whole organization. For example, when users search from the search box on a hub site, they're only searching in the sites associated with the hub and therefore they don't see any promoted results even if they are on the **All** tab. But when users search from the SharePoint start page, they might see promoted results on the **All** tab. If you have defined both a promoted result

and a bookmark for the same content (same URL), only the bookmark will appear on the **All** tab.

About the SharePoint admin role in Microsoft 365

6/5/2020 • 2 minutes to read • Edit Online

Global admins in Microsoft 365 can assign users the SharePoint admin role for help with administering Microsoft SharePoint. The global admin role already has all the permissions of the SharePoint admin role. For info about assigning a user the SharePoint admin role, see Assign admin roles in Microsoft 365 for business.



Users assigned the SharePoint admin role have access to the SharePoint admin center and can create and manage sites (previously called "site collections"), designate site admins, manage sharing settings, and more.

> **IMPORTANT**
>
> SharePoint admins can now manage Microsoft 365 groups, including creating, deleting, and restoring groups, and changing group owners.

Global admins and SharePoint admins don't have automatic access to all sites and each user's OneDrive, but they can give themselves access to any site or OneDrive. They can also use Microsoft PowerShell to manage SharePoint and OneDrive. See more about this role's Key tasks of the SharePoint admin below.

Site admins are users that have permission to manage sites, including any subsites. They don't need to have an admin role in Microsoft 365, and aren't given access to the SharePoint admin center.

NOTE

Global admins, SharePoint admins, and site admins all need to be assigned a SharePoint license.
There is a separate role within SharePoint called the **Term Store Administrator**. Users assigned this role can add or change terms in the term store (a directory of common terms you want to use across your organization). To learn more, see Assign roles and permissions to manage term sets.

Key tasks of the SharePoint admin

Here are some of the key tasks users can do when they are assigned to the SharePoint admin role:

- Create sites
- Delete sites
- Manage sharing settings at the organization level
- Add and remove site admins
- Manage site storage limits

Related topics

About Microsoft 365 admin roles

Getting started with SharePoint Online Management Shell

Get started with the new SharePoint admin center

6/24/2020 • 4 minutes to read • Edit Online

To go to the new SharePoint admin center, you need to sign in with an account that has admin permissions for your organization.

NOTE

If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center.
If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center.
Report data is not available for Office 365 Germany customers and US Government GCC High and DoD customers.

NOTE

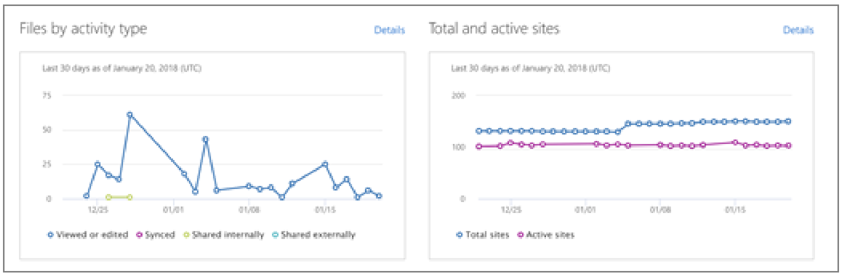
Microsoft Partners can't access the new SharePoint admin center.
Some functionality is introduced gradually to organizations that have opted in to the Targeted release option in Microsoft 365. This means that you might not yet see some features described in this article, or they might look different.

Help us improve the new SharePoint admin center! Tell us what you like or don't like, send a suggestion, or file a bug. To send us feedback, in the lower-right corner, select **Feedback**.

View reports

On the home page, at a glance, you can see:

- The number of files that have specific types of activity each day for the past 30 days. (If an activity occurs multiple times in one day on the same file, the file is counted only once for that day.)
- The number of total and active sites each day for the past 30 days. ("Active" sites are any where users view a page or view, modify, upload, download, share, or sync a file.)



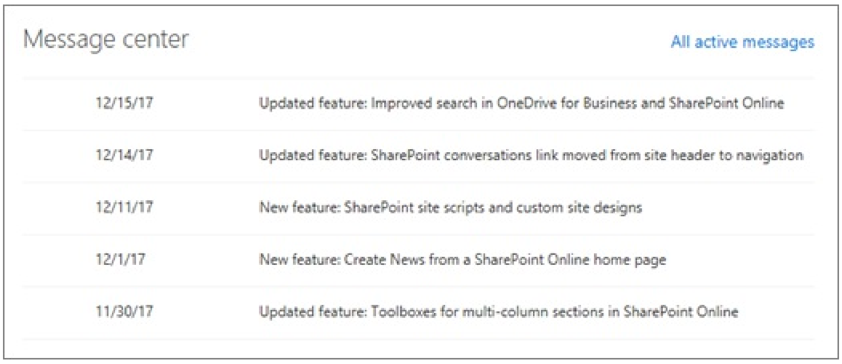
TIP

To filter a report, select an item in the legend. For example, on the **Files by activity type** chart, select **Viewed or edited**.
To see values for a specific day, point to that day on the report.
To see more details about a report, open the report in the Microsoft 365 admin center by selecting **Details**. Here, you can see tables of activity by site or users, change the reporting period, pivot the report, export the report data into a .csv file that you can open in Excel, and more. For more info about the SharePoint reports in the Microsoft 365 admin center, see Microsoft 365 Reports in the Admin Center - SharePoint activity and Microsoft 365 Reports in the Admin Center - SharePoint site usage.

> **NOTE**
>
> Reports typically don't include activity from the last 24 to 48 hours.

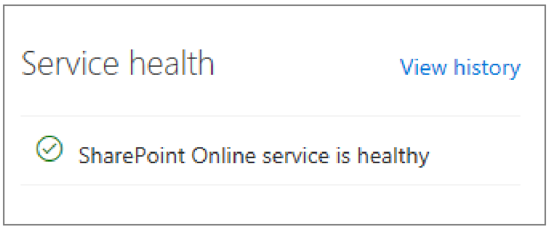
View Message center posts

In the **Message center** section of the home page, to help you manage upcoming changes, you can read official announcements about new and changed SharePoint features. Each post gives you an overview of a change, and how it might affect your users. To open a post, in the Microsoft 365 admin center, select it (where you can dismiss it if you want to hide it from the list). To sort and filter the list of messages across all Microsoft 365 services, select **All active messages**.



Service health

In the **Service health** section of the home page, you can see whether the SharePoint service is healthy, or if it's experiencing an active advisory or incident. For more info about an advisory or incident, select it to open the **Service health** page of the Microsoft 365 admin center.



Customize the navigation pane

1. At the bottom of the nav pane, select **Customize navigation**.
2. Select the items you want to appear in the nav pane, and then select **Save**.

> **TIP**
>
> To minimize the nav pane, at the top of the nav pane, select the **Collapse navigation menu** icon.

Where to find things in the new SharePoint admin center

If you're used to working in the classic SharePoint admin center, to learn where you can find features and tasks in the new admin center, use the following table.

CLASSIC	NEW	NOTES
site collections page	**Active sites** page	The new SharePoint admin center refers to site collections as "sites."
On the **site collections** page, select **New** > **Private Site Collection**.	**Active sites** page > **Create**	In the new SharePoint admin center, you can create Microsoft 365 group-connected team sites and communication sites, as well as classic sites.
On the **site collections** page, select **site collections** > **Delete**.	On the **Active sites** page, select **sites**, and then select **Delete**.	
On the **site collections** page, select a site collection > **Properties**.	On the **Active sites** page, to open the **details** pane, select the site's name.	In the new SharePoint admin center, you can edit site details.
On the **site collections** page, select a site collection > **Owners** > **Manage Administrators**.	On the **Active sites** page, select a site, and then select **Owners**.	The new experience also lets you view and edit Microsoft 365 Group owners.
On the **site collections** page, select a site collection > **Sharing**.	On the **Active sites** page, select a site, and then select **Sharing** (or select multiple sites, and then select **Bulk edit** > **Sharing**).	
On the **site collections** page, select **Buy Storage**.	Buy a file storage add-on from the Microsoft 365 admin center	
On the **site collections** page, select **Recycle Bin**.	**Deleted sites** page	
Sharing page	**Sharing** page	The new page includes the most common settings, and others are coming soon.
Settings page	**Settings** page	The new page includes the most common settings, and others are coming soon. At the bottom of the new **Settings** page, to access all the classic settings, select **classic settings page**.
Access control page	**Access control** page	The new SharePoint admin center contains all the classic settings and more.
Term store, User profiles, Search, Apps, BCS, Secure store, Records management, InfoPath, Configure hybrid (hybrid picker).	**More features** page	

See also

Manage sites in the new SharePoint admin center

What's new in the SharePoint admin center

1/8/2021 • 4 minutes to read • Edit Online

We're continuously adding new features to the new SharePoint admin center and fixing issues we learn about. Here's a summary of what's included. You can help us improve the admin center by sending us your suggestions and reporting bugs you encounter. In the lower-right corner of the admin center, click the **Feedback** button.

NOTE

The new SharePoint admin center is supported in Microsoft Edge, Internet Explorer, Chrome, Firefox, and Safari.

Some functionality is introduced gradually to organizations that have opted in to the Targeted release option in Microsoft 365. This means that you might not yet see some features described in this article.

For info about new features in the Microsoft 365 admin center, see What's new in the Microsoft 365 admin center. For info about new features in Migration Manager, see What's new in Migration Manager.

IMPORTANT

Microsoft 365 apps and services will not support Internet Explorer 11 starting August 17, 2021 (Microsoft Teams will not support Internet Explorer 11 earlier, starting November 30, 2020). Learn more. Please note that Internet Explorer 11 will remain a supported browser. Internet Explorer 11 is a component of the Windows operating system and follows the Lifecycle Policy for the product on which it is installed.

June 2020

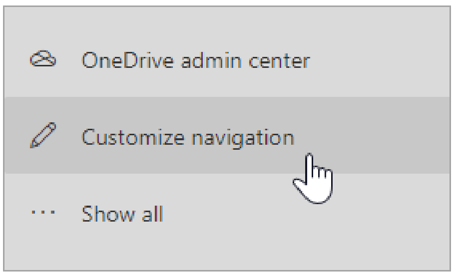
- **Improvements to the Export feature**. On the Active sites page, you can export your customized view as a .csv file.

April 2020

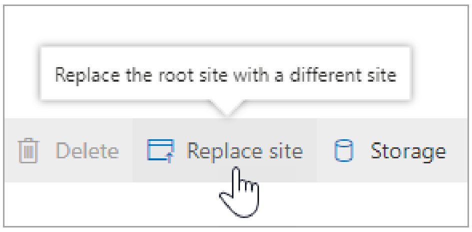
- **Support for the Global reader role**. Users assigned this role can view all info in the admin center, but can't save any changes. Learn more about this role.

December 2019

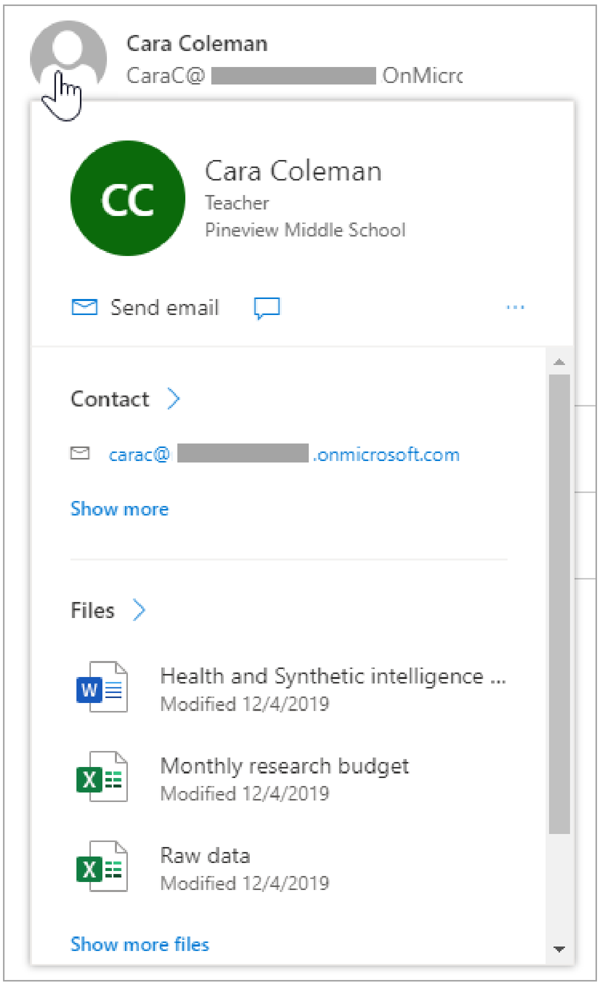
- **Customizable navigation pane**. You can customize the navigation pane to show or hide items.



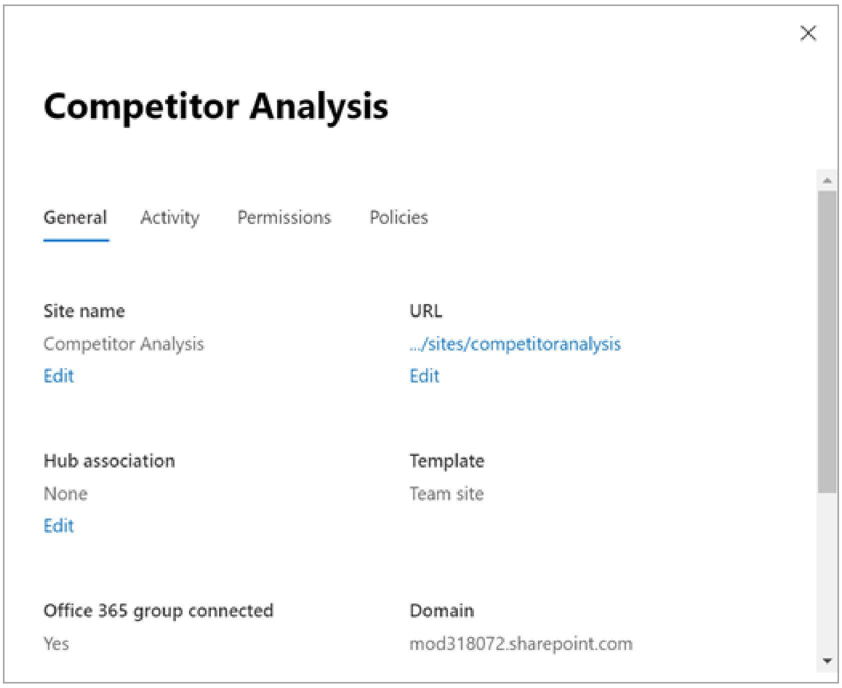
- **Root site replacement**. On the Active sites page, you can select and replace the root site.



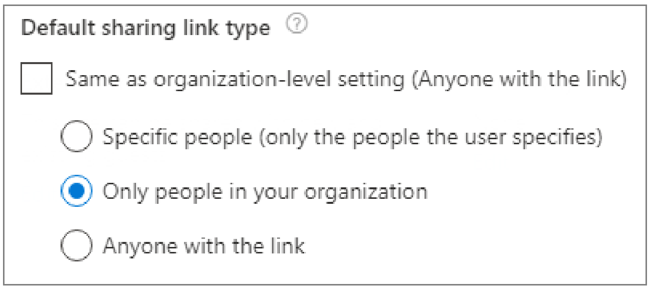
- **People cards**. On the Active sites page, you can point to a name in the Primary admin column or on the Permissions tab of the details panel and see info about the person.



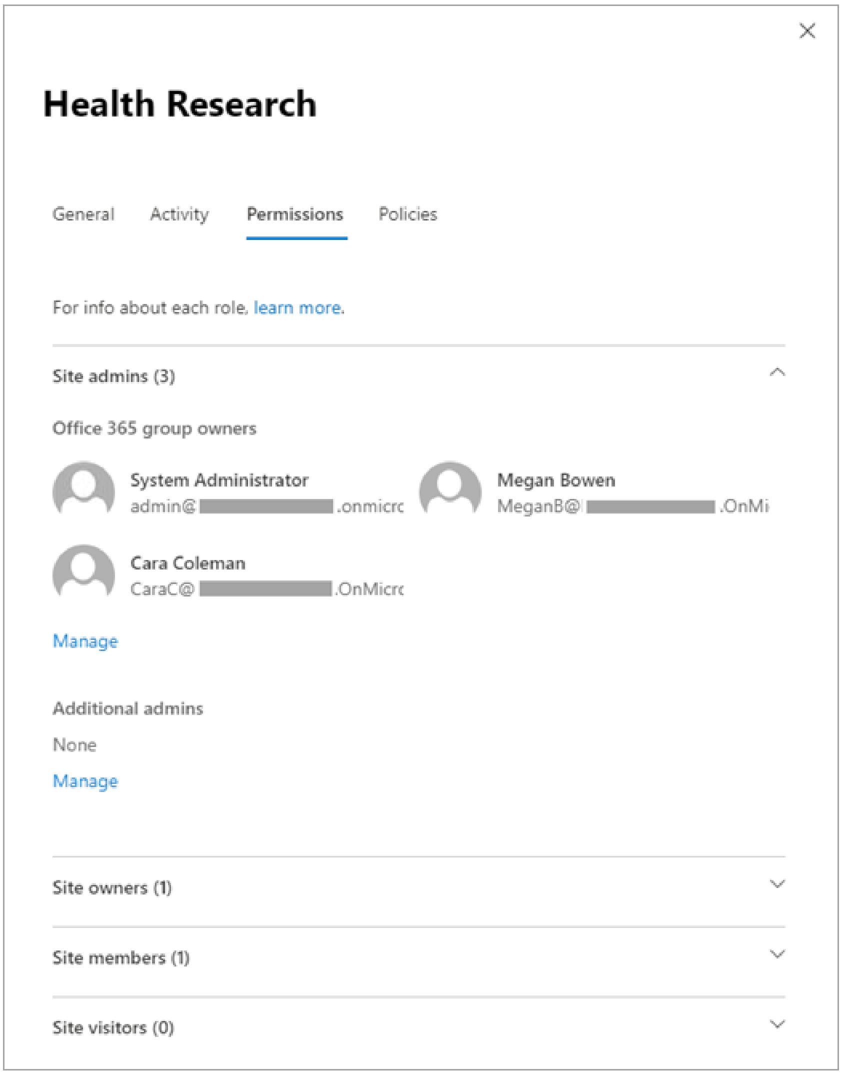
- **Redesigned details panel**. On the Active sites page, the details panel that appears when you select a site has been redesigned to divide the information among multiple tabs. Learn more about managing sites.



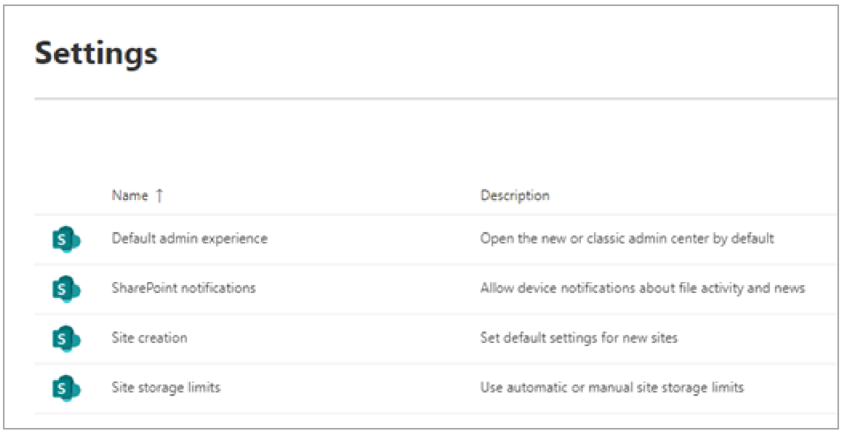
- **Additional site-level sharing settings**. On the Active sites page, when you select a site and then select **Sharing**, you can change the default sharing link type and default link permissions for the site.



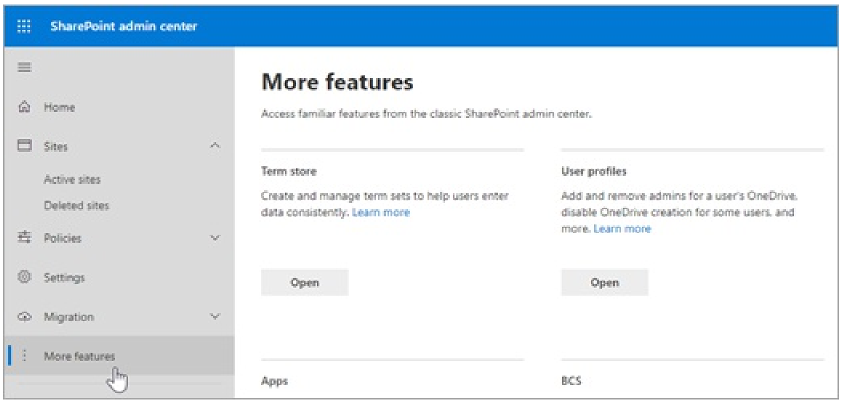
- **Site permission details**. On the Active sites page, a new experience lets you manage all site admins in one panel, view site members and visitors, and add site admins to sites that belong to Microsoft 365 groups. Learn more about managing site permissions



- **Redesigned Settings page**. The Settings page has been redesigned to let you see the value for each setting without selecting each one for more info.



- **Updated More features page**. Classic features can now be found on the More features page. Learn where to find features in the new SharePoint admin center.



November 2019

- If you're using the new sensitivity labels, you can view and edit them from the Active sites page.

October 2019

- From the Active sites page, you can change site addresses.

June 2019

- The new SharePoint admin center is set as the default experience unless you select to open the classic SharePoint admin center by default (on the Settings page). Learn how to select the default admin experience.
- On the Active sites page, you can select multiple sites and bulk edit sharing and hub association settings.
- Classic SharePoint admin features such as Term Store, User Profiles, Search, Apps, and more are available from the More features page so you can access them directly from the new SharePoint admin center.

In case you missed it

Home page and left pane

- Two charts, along with messages and service health filtered to SharePoint
- Links to the Microsoft 365 admin center for detailed reports, message center posts, and service health info
- Links to the OneDrive admin center and SharePoint Migration Tool
- A geo location selector for organizations that have set up Multi-Geo in OneDrive and SharePoint

Active sites page

- A list that includes the new types of sites that users create: team sites that belong to Microsoft 365 groups and communication sites
- The ability to create sites (including sites that belong to Microsoft 365 groups and communication sites) using the same experience available to users
- Extensive site info and insights such as site name, template, file and sharing info, and date created and modified
- The ability to sort, filter, and customize columns, as well as search by all text fields
- The ability to view and filter by hub association, and change a site's hub association
- Built-in views and the ability to create custom views

- The ability to edit site-level sharing status
- Export to CSV
- Support for locked sites and sites on hold

Deleted sites page

- A list of deleted sites with time deleted
- The ability to restore sites individually
- The ability to permanently delete sites, except sites connected to a Microsoft 365 group

Sharing page

- Organization-level external sharing settings, and file and folder link settings

Access control page

- The ability to create policies that restrict access from unmanaged devices, sign out users from inactive browser sessions, allow access from only specific IP addresses, and block access from apps that don't use modern authentication.

Settings page

- Settings for sync (if your organization used the previous sync app), notifications, site storage limits, default admin experience, and site creation

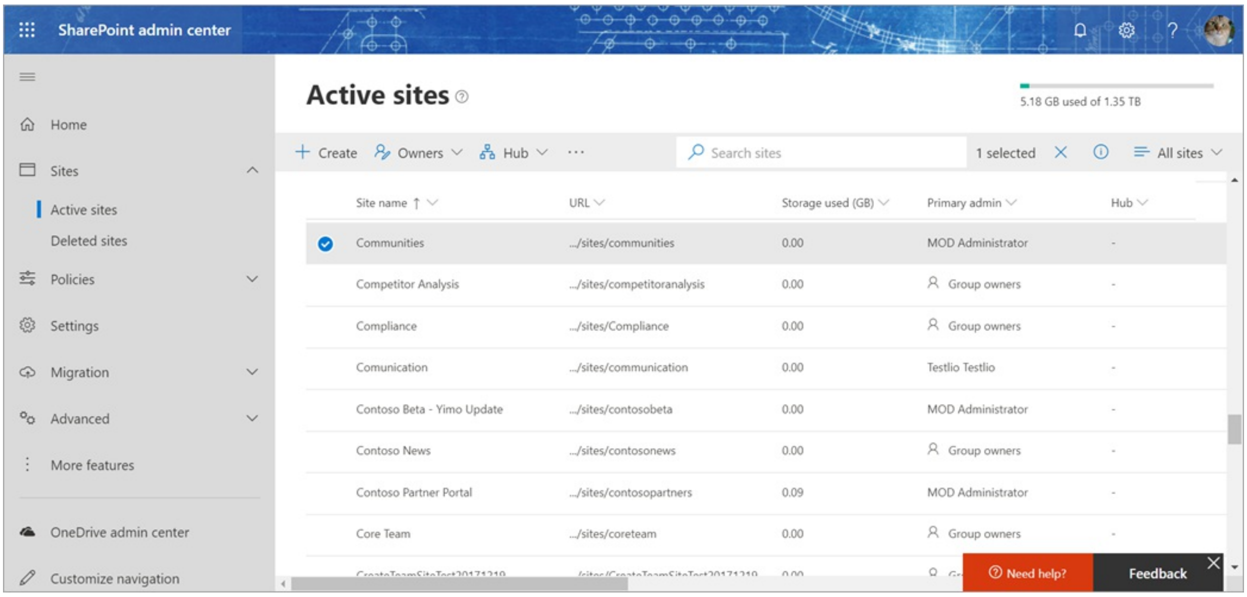
API management page

- The ability to view pending and approved web API permissions and approve or reject access requests

Manage sites in the new SharePoint admin center

7/14/2020 • 4 minutes to read • Edit Online

The Active sites page of the new SharePoint admin center lets you view the SharePoint sites in your organization (including the new communication sites and sites that belong to Microsoft 365 groups). It also lets you sort and filter sites, search for a site, and create new sites.



NOTE

The Active sites page lists the root website for each site collection. Subsites, redirect sites (REDIRECTSITE#0) created by changing a site address or replacing the root site, and Microsoft Teams private channel sites (TEAMCHANNEL#0) aren't included in the list.

Some functionality is introduced gradually to organizations that have opted in to the Targeted release option in Microsoft 365. This means that you might not yet see some features described in this article, or they might look different.

For more info about managing sites and storage, see:

- Create a site
- Delete a site
- Manage site storage limits

Add or remove site admins and group owners

1. In the left column, select a site.
2. Select **Permissions**. For a group-connected team site, you can add and remove group owners and additional site admins. For other sites, you can add and remove site admins and change the primary admin. Note that if you remove a person as a primary admin, they will still be listed as an additional admin. For info about each role, see About site permissions.

Change a site's hub association

1. In the left column, select a site.

2. Select **Hub**. The options that appear depend on whether the site you selected is registered as a hub site, or associated with a hub. The Hub menu lets you register a site as a hub site, associate it with a hub, change its hub association, and unregister it as a hub site. More info about hubs

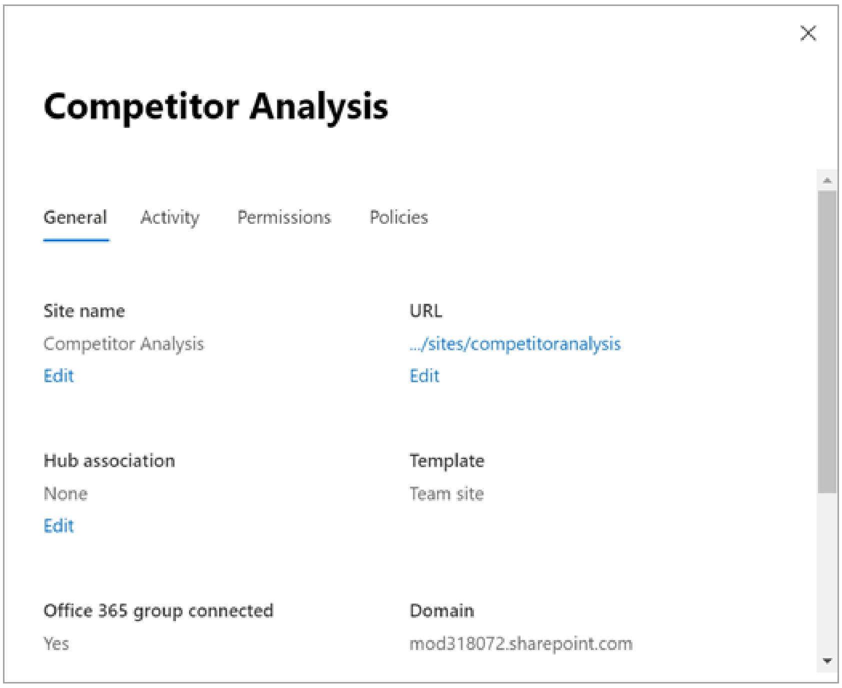
Change the external sharing setting for a site

1. In the left column, select a site.
2. Select **Sharing**.
3. Select an option, and then select **Save**. For info about the options, see Turn external sharing on or off for for a site.

> **NOTE**
>
> The options that are available depend on the organization-wide setting you've selected. The setting for a site can be more restrictive, but not more permissive.

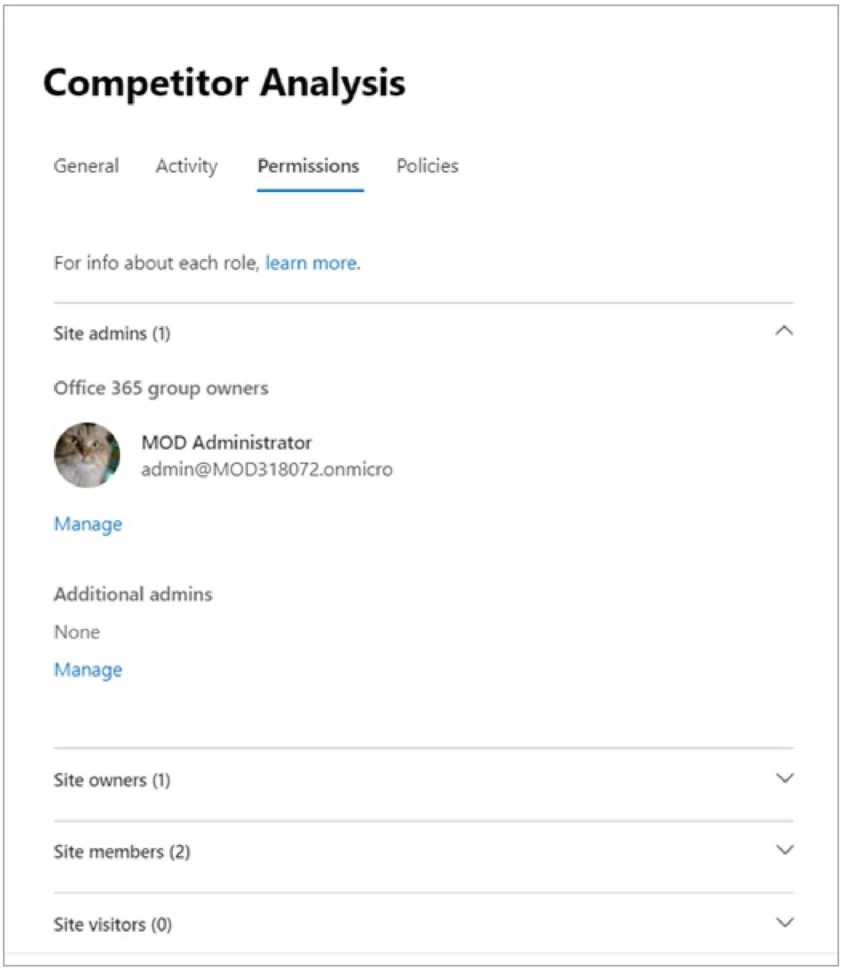
View site details

For more info about a site, select the site name to open the details panel.



To view site activity including the number of files stored and storage usage, select the **Activity** tab. Activity information is not available for Office 365 Germany customers and US Government GCC High and DoD customers.

To view site admins, owners, members, and visitors, select the **Permissions** tab.



For info about the roles in this panel, see About site permissions.

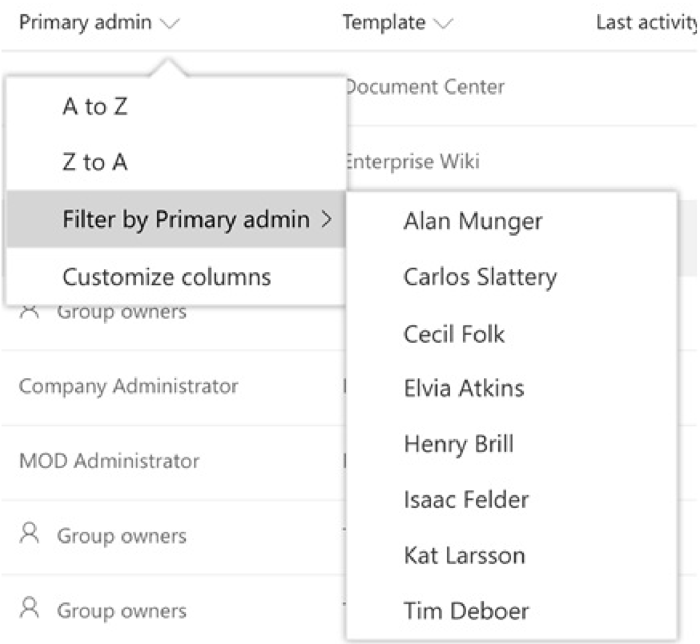
Sort and filter the site list

Sorting and filtering the site list is just like sorting and filtering other lists in SharePoint.

1. Select the arrow next to the column header.

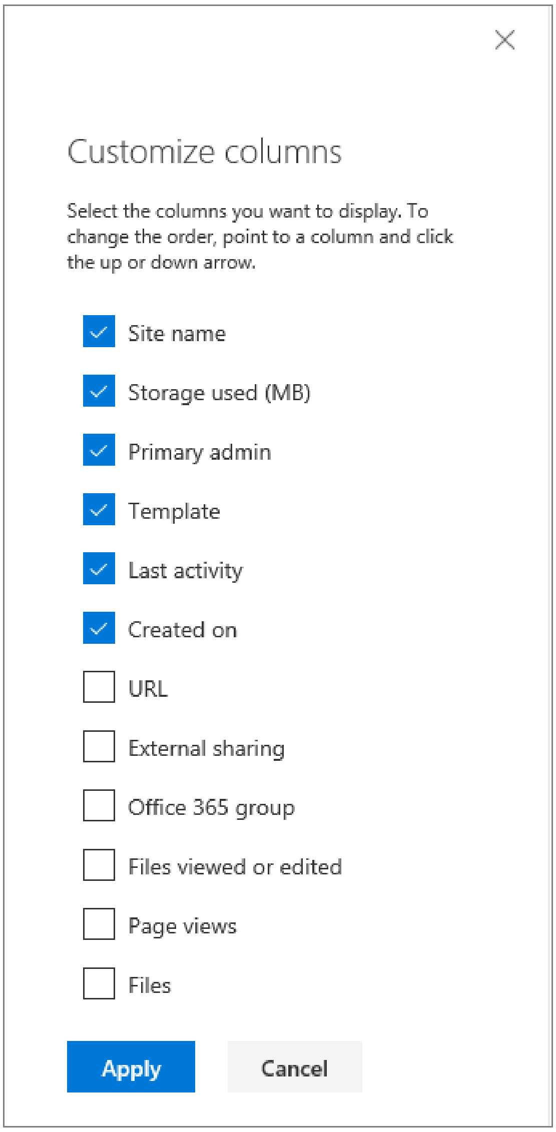
2. Select how you want to arrange the items. The options vary depending on the column. For example, you might have options to sort alphabetically, in numeric order, or chronologically.

   If the column allows filtering, a "Filter by" option appears. Select the value or values that you want to show. Your selections appear with a check mark beside them. To remove a selection, select that value again. To clear all filters on the column, select **Clear filters**.



Customize columns

1. Select the arrow next to any column header, and then select **Customize columns**.
2. To show and hide columns, select and clear check boxes.
3. To rearrange the columns, point to a column, and select the up or down arrow to move the column up or down.



NOTE

Data in the following columns is not available for Office 365 Germany customers and US Government GCC High and DoD customers:

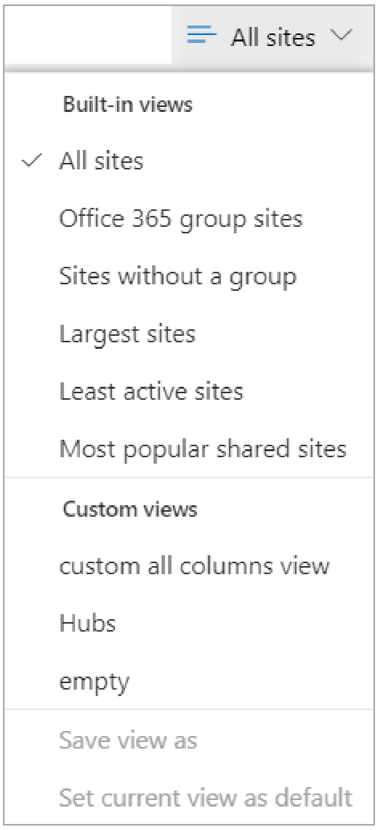
- Last activity
- File views or edited
- Page views
- Page visits
- Files
- Storage used

Switch views and create custom views

The new SharePoint admin center comes with a few built-in views: Microsoft 365 group sites, Sites without a group, Largest sites, Least active sites, and Most popular shared sites. You can also create and save custom views.

1. Customize columns, sort, and filter your view the way you want. (Views that are filtered through search can't be saved.)

2. On the far right of the command bar, next to the Search box, select the **View** menu (the name changes depending on your current view).



3. Select **Save view as**.

4. In the **Save as** dialog box, enter a name for the view.

> **NOTE**
> To set the view as default, in the **View** box, select **Set current view as default**.

Search for a site

You can search for a site by name, URL, primary admin, or template. To do this, enter keywords in the Search box, and press Enter.

> **NOTE**
> Search doesn't look in hub site display names for the keywords you enter.
> All characters you enter are treated as part of the query. Search doesn't recognize operators or wildcards (*).

Export to CSV

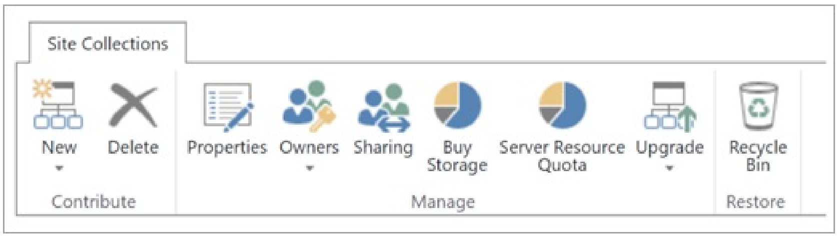
To export the site list you're viewing as a .csv file that you can work with in Excel, select **Export**.

> **NOTE**
> The .csv file lists the hub as a GUID and the template as an ID (for example, STS#0).

Find site collection features in the new SharePoint admin center

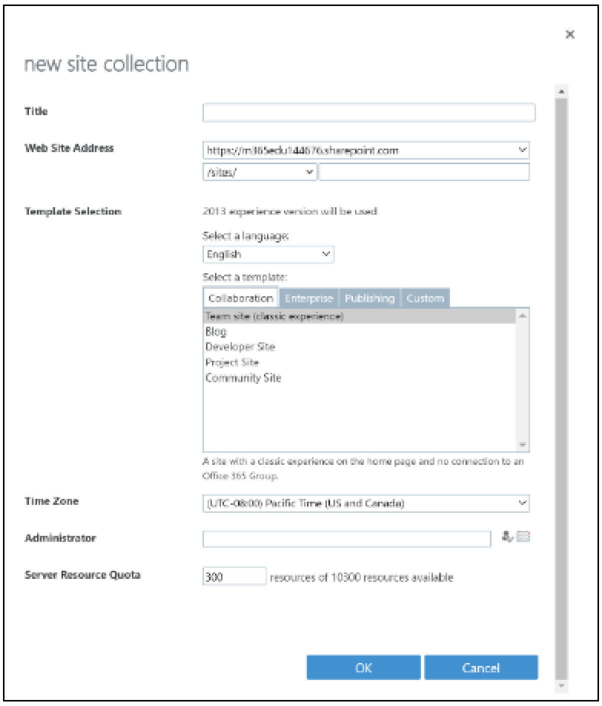
1/8/2021 • 6 minutes to read • Edit Online

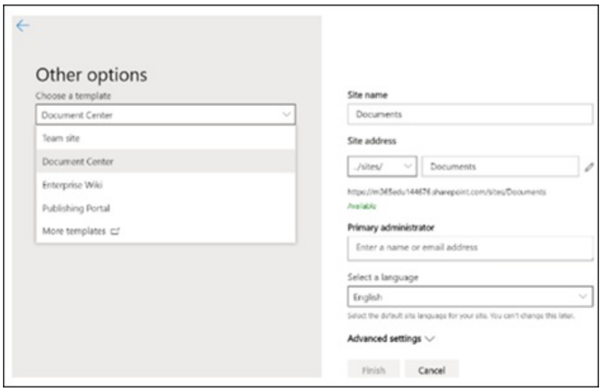
This article covers all the features on the classic site collections page and where you can find them in the new SharePoint admin center.



Create a new private site collection

To create a site collection in the new SharePoint admin center, go to the Active sites page, and then select **Create**. To create a classic site, select **Other options**.

<table>
<tr><th>CLASSIC</th><th>NEW</th></tr>
<tr><td>


</td><td>


</td></tr>
</table>

CLASSIC	NEW
Title	Site name
Change the URL path to /sites/ or /teams/	Site address boxes appear after you begin entering a site name.

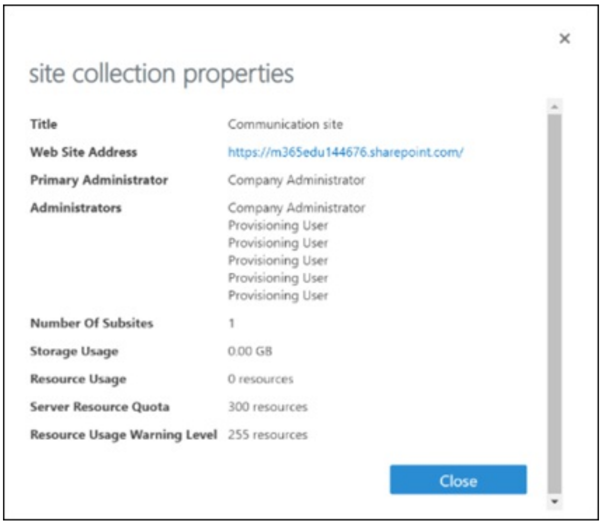
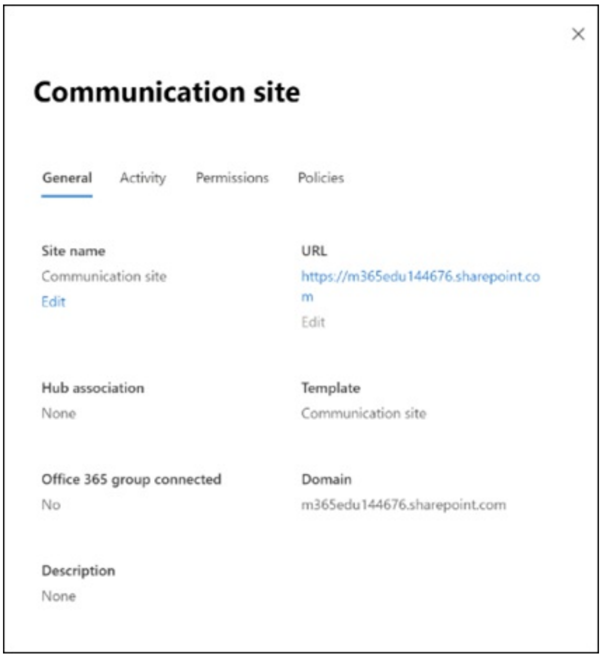
CLASSIC	NEW
Web Site Address	Site address boxes appear after you begin entering a site name. The name is entered by default as the address. To change it, select the Edit icon.
Select a language	Select a language
Select a template: **Community**: Team site (classic experience), Blog, Developer site, Project Site, Community Site **Enterprise**: Document Center, eDiscovery Center, Records Center, Team Site – SharePoint Online configuration, Business Intelligence Center, Compliance Policy Center, My Site Host, Community Portal, Basic Search Center, Visio Process Repository **Publishing**: Publishing Portal, Enterprise Wiki, Product Catalog **Custom**: <Select template later...>	In the **Choose a template** box, you can select **Document Center**, **Enterprise Wiki**, or **Publishing Portal**. To select the others, select **More templates**. This opens the classic Create Site Collection window.
Time Zone	Expand **Advanced settings** and select **Time zone**.
Administrator	Primary Administrator
Server Resource Quota	This setting has had no effect for more than a year.
Private Site Collection with Project Web App	Create a site and then use the PowerShell cmdlet Set-SPOSite -EnablePWA to add or remove Project Web App.

Delete

On the Active sites page, select the site, and on the command bar, select **Delete**. As with the classic SharePoint admin center, you can't delete the root (top-level) site. To swap this site with a different site, see Replace your root site.

Properties

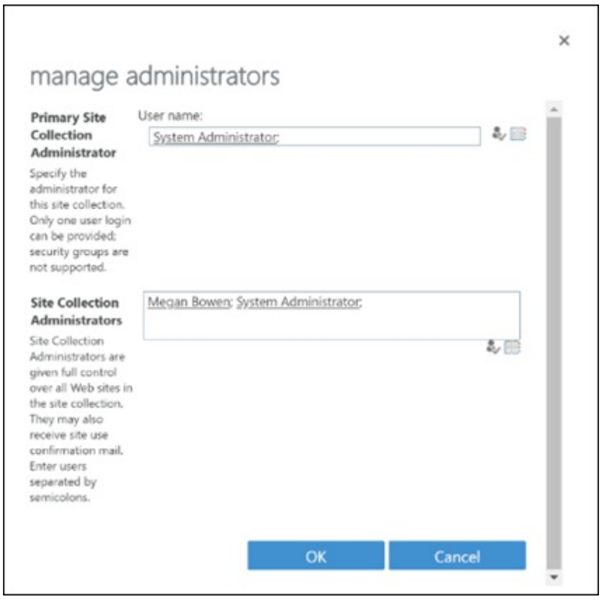
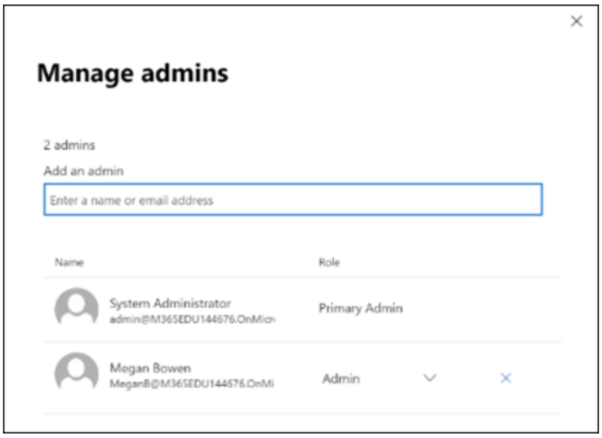
The columns on the Active sites page show most of this information, so you don't even need to select a site to see details. To see the properties for an individual site, select anywhere in the site row, except in the URL column.

CLASSIC	NEW
	

CLASSIC	NEW
Title	Site name column
Complete Web Site Address link	URL column shows the path after the domain. You can copy the link to save the full URL to the Clipboard.
Primary Administrator	Primary admin column.
Other Administrators	For any sites that aren't connected to a Microsoft 365 group, select the site, and on the command bar, select **Permissions**, and then select **Manage admins**. (For group-connected sites, you have options for managing group owners and additional admins.)
Number of subsites	Not available
Storage Usage	Storage used (GB) column.
Resource Usage, Server Resource Quota, Resource Usage Warning Level	These settings have had no effect for more than a year.

Owners

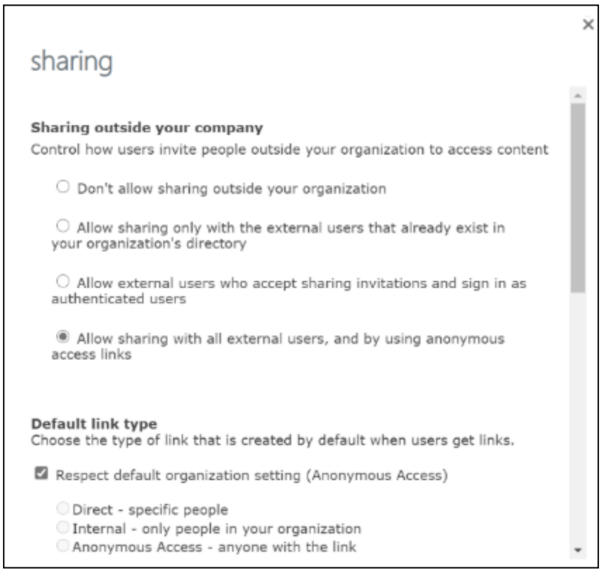
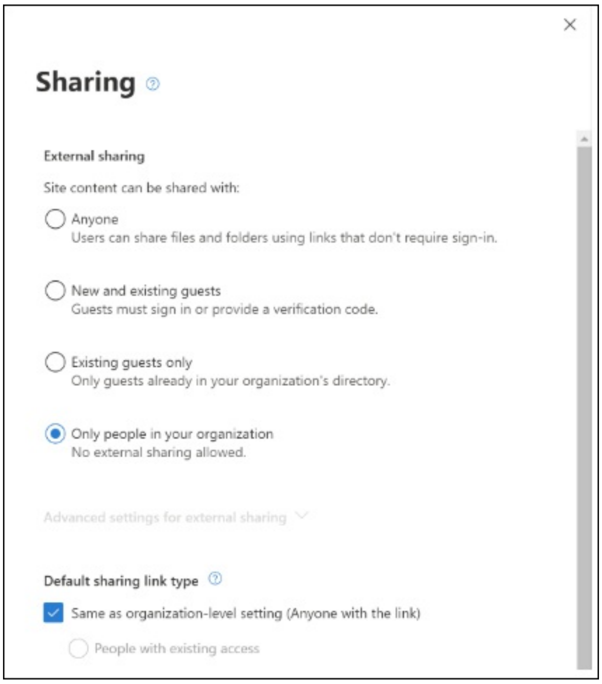
To change the owners for any site that isn't connected to a Microsoft 365 group, go to the Active sites page, select the site, select **Permissions** on the command bar, and then select **Manage admins**.

CLASSIC	NEW
	

CLASSIC	NEW
Primary Site Collection Administrator	Switch the role of an existing admin to Primary Admin, or add an admin and then switch them to Primary admin.
Site Collection Administrators	Use the Add an admin box to add an admin and the Remove button to remove an admin.
Add Support Partner	This option is available in PowerShell only. Go to the Site Permissions page for a site where you've added the support partner.Copy the encoded string for the partner, and to add it to other sites, use the PowerShell cmdlet Set-SPOUser.

Site collection-level sharing

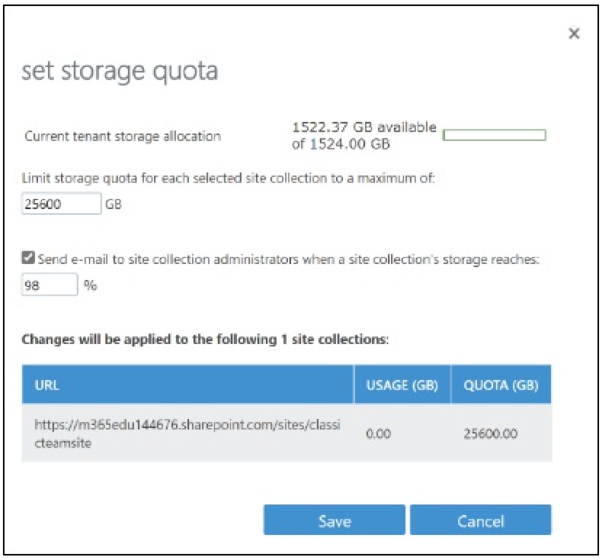
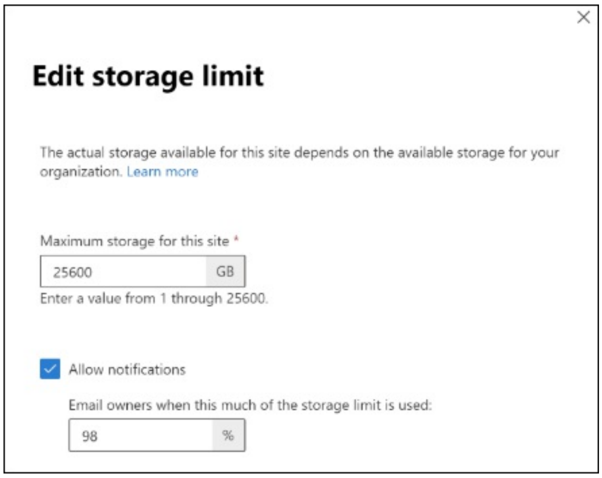
To change sharing settings for a site, go to the Active sites page, select the site, and select **Sharing** on the command bar.

CLASSIC	NEW
	

CLASSIC	NEW
Sharing outside your company	External sharing - "Don't allow sharing outside your organization" is the same as "Only people in your organization." - "Allow sharing only with the external users that already exist in your organization's directory" is the same as "Existing guests only." - "Allow external users who accept sharing invitations and sign in as authenticated users" is the same as "New and existing guests." - "Allow sharing with all external users, and by using anonymous access links" is the same as "Anyone."
Default link type	Default sharing link type - "Respect default organization setting" is the same as "Same as organization-level setting." - "Direct" is the same as "Specific people." - "Internal" is the same as "Only people in your organization." - "Anonymous Access" is the same as "Anyone with the link."
Default link permission	"Respect default organization setting" is the same as "Same as organization-level setting." Both the classic and new admin centers have View and Edit options.
Limit external sharing by domain	Under **Advanced settings for external sharing**, select **Limit sharing by domain**.
Turn off sharing for all non-owners on all sites in the site collection	This option is available in PowerShell only. Use the cmdlet Set-SPOSite -DisableSharingForNonOwners

Storage quota

These options appear if you use manual site storage limits in your organization. To change the storage limit for a site, go to the Active sites page, select the site, and select **Storage** on the command bar.

CLASSIC	NEW
	

CLASSIC	NEW
Limit storage quota for each selected site collection to a maximum of	Maximum storage for this site
Send e-mail to site collection administrators when a site collection's storage reaches	Allow notifications

Buy storage

In the Microsoft 365 admin center, go to the Purchase services page.

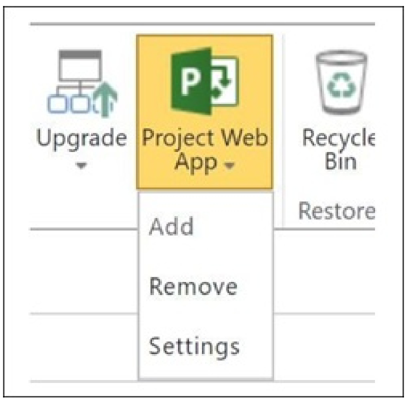
Server resource quota

These settings have had no effect for more than a year.

Upgrade settings and notifications

These features haven't been in use for more than a year.

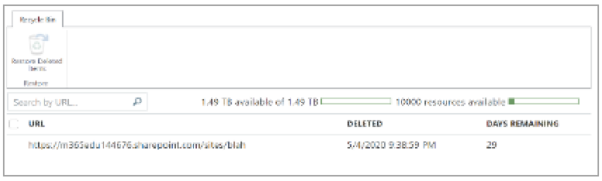
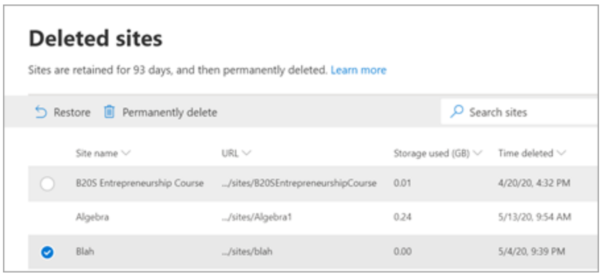
Project Web App



CLASSIC	NEW
Add or remove	These commands are available in PowerShell only. Use the cmdlet Set-SPOSite -EnablePWA
Settings (SharePoint Permission Mode or Project Permission Mode) and Project Web App Size	To change the permission mode, go to the site as the Project Web App Administrator and follow the steps in Change permission management in Project Online. You can review the size of the Project Web App site using the above instructions where it is located on the same page under the section "Project Web App Usage".

Recycle bin

To view your deleted sites, go to the new SharePoint admin center, go to the Deleted sites page.

CLASSIC	NEW
	

CLASSIC	NEW
Restore Deleted Items	Select the site, and on the command bar, select **Restore**.
Deleted (date)	Time deleted column.
Days remaining	This info is incorrect in the classic admin center. To calculate this value in the new SharePoint admin center, use the Time deleted column.

Search by URL

On the Active sites page, use the Search box. As with the classic SharePoint admin center, you can also sort by URL.

Available storage and storage limit bar

The upper-right corner of the Active sites page shows the storage used (in GB) and storage limit for your organization.

Available resources bar

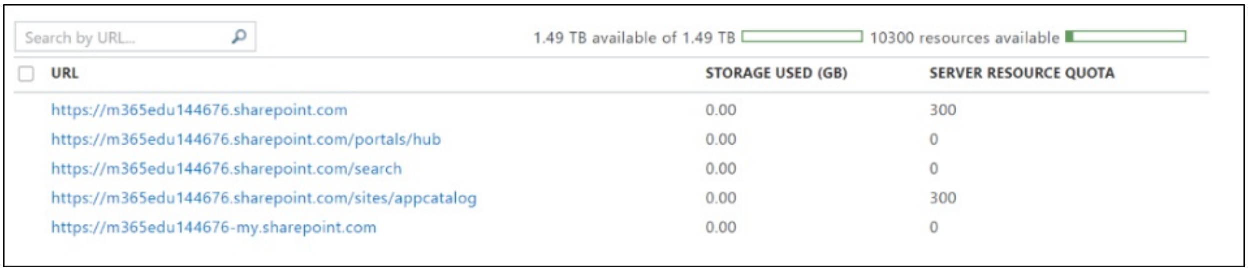
Server resource quota and availability have had no effect for more than a year.

Project Web App instances available

This information is no longer displayed because you shouldn't need to worry about running out of Project Web

App instances.

Site list



Most of the sites listed in the classic SharePoint admin center are included on the Active sites page. A few are hidden because they're system sites that you shouldn't need to change. The Active sites page contains all the new team sites and communication sites that don't appear in the classic SharePoint admin center. To see the site list as it in the way it appeared in the classic SharePoint admin center, from the **View** menu, select **Classic sites**.

In both the classic and new admin centers, you can select multiple sites and bulk edit the sharing or storage settings, or delete the sites.

In the classic site list, locked sites appear with an icon. In the new SharePoint admin center, to see if a site is locked, select the site to open the details panel. **This site is locked** appears at the top of the panel.

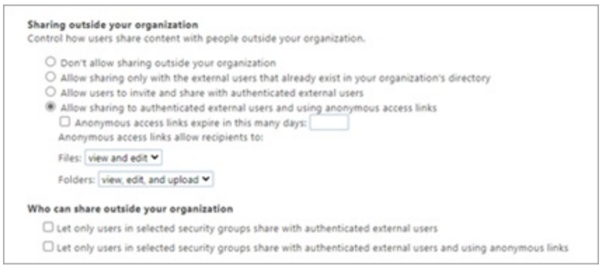
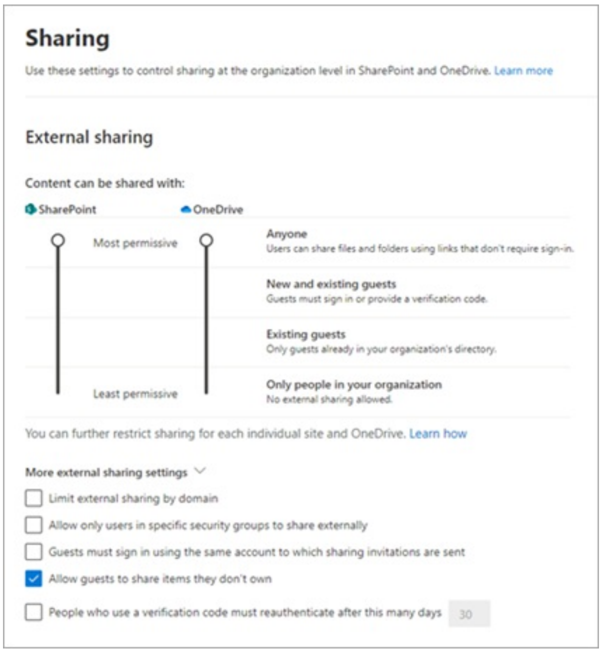
If you use manual storage limits, the Storage limit and Percent used columns appear. In the new SharePoint admin center, on the Active sites page, the Storage limit and Storage used columns appear. The Storage used column isn't color coded. The Storage limit column can be sorted by size.

Find sharing settings in the new SharePoint admin center

11/2/2020 • 2 minutes to read • Edit Online

This article covers all the features on the sharing page in the classic SharePoint admin center and where you can find them on the Sharing page in the new SharePoint admin center.

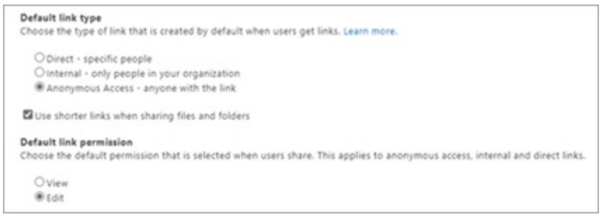
Sharing outside your organization

CLASSIC	NEW
	

CLASSIC	NEW
A. Don't allow sharing outside your organization B. Allow sharing only with the external users that already exist in your organization's directory C. Allow users to invite and share with authenticated external users D. Allow sharing to authenticated external users and using anonymous access links	Under **External sharing**, drag the SharePoint slider to the corresponding option: A. Only people in your organization B. Existing guests C. New and existing guests D. Anyone
Anonymous access links expire in this many days	In **File and folder links**, under **Choose expiration and permissions options for Anyone links**, select **These links must expire within this many days**.
Anonymous access links allow recipients to	In **File and folder links**, under **Choose expiration and permissions options for Anyone links**, select **These links can give these permissions**.

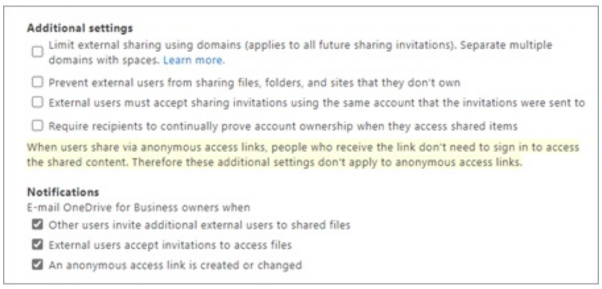
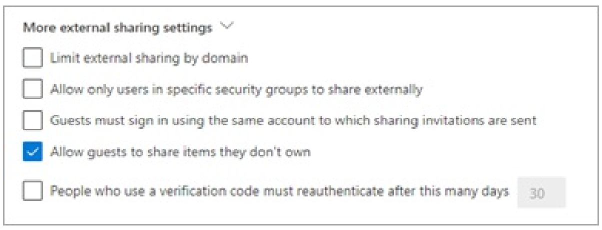
CLASSIC	NEW
Let only users in selected security groups share with authenticated external users Let only users in selected security groups share with authenticated external users and using anonymous links	Expand **More external sharing settings** and select **Allow only users in specific security groups to share externally**. In the Manage security groups panel, under **Can share with**, select **Anyone** or **Authenticated guests only**.

Default links

CLASSIC	NEW
 	

CLASSIC	NEW
Default link type A. Direct - specific people C. Internal - only people in your organization C. Anonymous Access - anyone with the link	In **File and folder links**, under **Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive**, select the corresponding option: A. Specific people (only the people the user specifies) B. Only people in your organization C. Anyone with the link
Use shorter links when sharing files and folders	Under **Other settings**, select **Use short links for sharing files and folders**.
Default link permission View Edit	In **File and folder links**, under **Choose the permission that's selected by default for sharing links**, select an option. View Edit

Additional settings

CLASSIC	NEW
 	

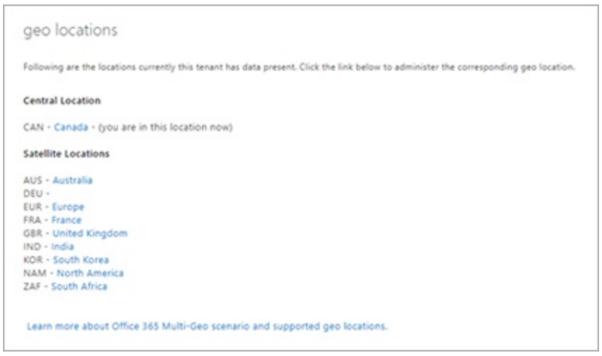
CLASSIC	NEW
Limit external sharing using domains	Under **External sharing**, expand **More external sharing settings**, and then select **Limit external sharing by domain**.
Prevent external users from sharing files, folders, and sites that they don't own	Under **External sharing**, expand **More external sharing settings**, and then select **Allow guests to share items they don't own**.
External users must accept sharing invitations using the same account that the invitations were sent to	Under **External sharing**, expand **More external sharing settings**, and then select **Guests must sign in using the same account to which sharing invitations are sent**.
Require recipients to continually prove account ownership when they access shared items	Under **External sharing**, expand **More external sharing settings**, and then select **People who use a verification code must reauthenticate after this many days**.
Notifications E-mail OneDrive for Business owners when A. Other users invite additional external users to shared files B. External users accept invitations to access files C. An anonymous access link is created or changed	A. Use the PowerShell cmdlet `Set-SPOTenant -NotifyOwnersWhenItemsReshared`. B. This setting doesn't work in the new sharing experience that appears in most places. C. Use the PowerShell cmdlet `Set-SPOTenant -OwnerAnonymousNotification`. More info about using Set-SPOTenant Get started with the SharePoint Online Management Shell

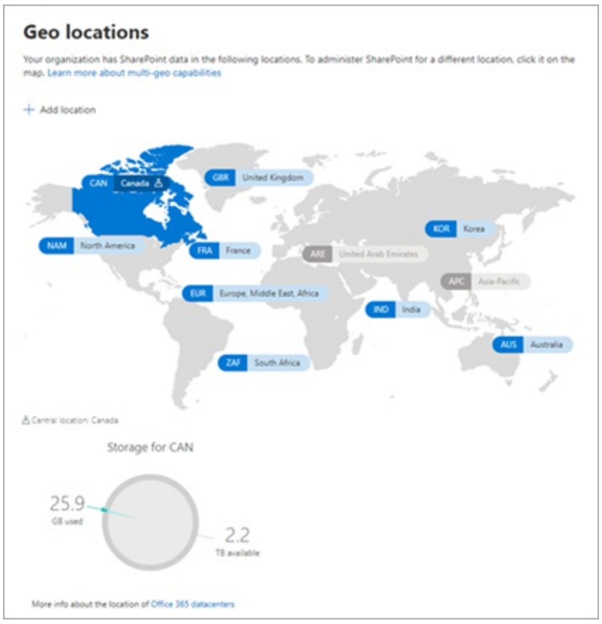
Find geo location features in the new SharePoint admin center

11/2/2020 • 2 minutes to read • Edit Online

This article covers all the features on the geo locations page in the classic SharePoint admin center and where you can find them on the Geo locations page in the new SharePoint admin center. In the new SharePoint admin center, you can also add and delete satellite locations.

Manage geo locations

<table>
<tr><th>CLASSIC</th><th>NEW</th></tr>
<tr><td>


</td><td>


</td></tr>
</table>

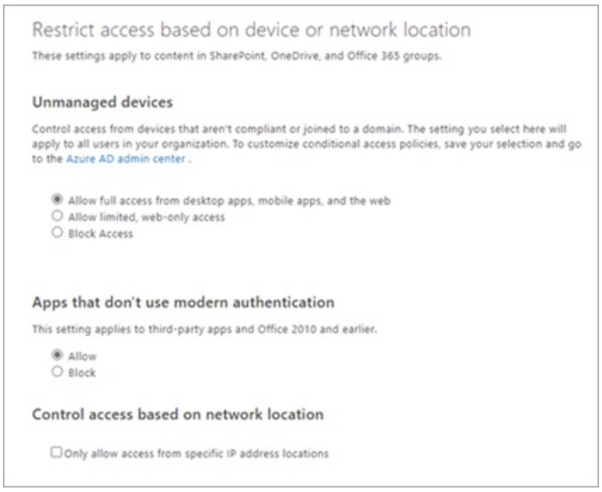
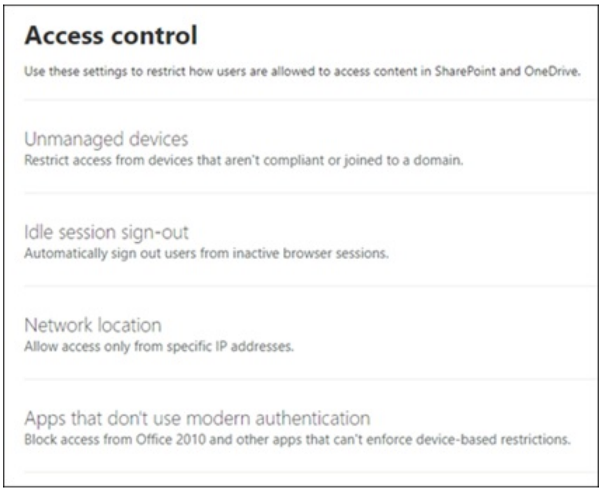
CLASSIC	NEW
Switch between locations	Select a different location on the map or from the list at the top of the navigation pane.
Identify the central location	Look for the pin on the map.
See list of satellite locations	Expand the list at the top of the navigation pane.

Find access control features in the new SharePoint admin center

11/2/2020 • 2 minutes to read • Edit Online

This article covers all the features on the control access page in the classic SharePoint admin center and where to find them on the Access control page in the new SharePoint admin center. In the new SharePoint admin center, you can also sign out inactive users. Learn more

Control access

CLASSIC	NEW
	

CLASSIC	NEW
Unmanaged devices	Unmanaged devices (The same options are available.)
Apps that don't use modern authentication	Apps that don't use modern authentication
Control access based on network location	Network location (This setting works the same way.)

Performance in the modern SharePoint experience

11/2/2020 • 3 minutes to read • Edit Online

The modern experience in Microsoft SharePoint is designed to be compelling, flexible and – importantly - more performant. Both SharePoint performance as a whole and the performance of individual SharePoint components such as search, lists and document libraries are affected by many factors, all of which contribute to the decisive performance metric: perceived end user latency, or the speed with which pages are rendered in the client browser. The SharePoint modern experience incorporates key performance improvements that help to minimize latency and improve SharePoint page responsiveness:

- Client-side processing and data requests
- Microsoft 365 Content Delivery Network (CDN)

More powerful computers and modern advancements in network architectures and web browsers have made it possible to improve the overall SharePoint user experience by shifting much of the data caching and processing from the server to the client machine. In this article, you will learn about how the SharePoint modern experience leverages client-side processing and the Microsoft 365 CDN to improve performance.

Client-side processing and data requests

In the classic SharePoint architecture, the SharePoint server farm executes data requests and other processing operations, returning results and rendered pages to the client. This model was intended to reduce the load on the client machine and browser, and also to reduce network traffic between the client and server farm, factors which were critical performance bottlenecks in legacy environments.

The SharePoint modern experience is designed to take advantage of the computing power of user computers and modern web browser capabilities to allow the client computer to directly perform certain data requests and processor-intensive operations such as page rendering.

The SharePoint modern experience client-side processing model can provide dramatic improvement in perceived end user latency over the classic SharePoint architecture. Keep in mind that there may be a greater dependency on the client-side execution environment as compared to the classic SharePoint architecture. As with any change to your network architecture, you should conduct a limited pilot to identify and resolve potential bottlenecks before rolling the SharePoint modern experience into your production environment.

Microsoft 365 Content Delivery Network (CDN)

SharePoint latency is affected in part by the physical distance between your users and the location of your SharePoint environment (tenant). This consideration is particularly important for organizations that have a global presence where a site may be hosted on one continent while users on the other side of the world are accessing its content.

You can use the built-in Microsoft 365 Content Delivery Network (CDN) to host static assets to provide better performance for your SharePoint sites. The Microsoft 365 CDN improves performance by caching static assets closer to the browsers requesting them, which helps to speed up downloads and reduce latency. Also, the Microsoft 365 CDN uses the HTTP/2 protocol for improved compression and download speeds.

The Microsoft 365 CDN is composed of multiple CDNs that allow you to host static assets in multiple locations, or *origins*, and serve them from global high-speed networks. Depending on the kind of content you want to host in the Microsoft 365 CDN, you can add **public** origins, **private** origins or both.

Content in **public** origins within the Microsoft 365 CDN is accessible anonymously, and can be accessed by anyone who has URLs to hosted assets. Because access to content in public origins is anonymous, you should only use them to cache non-sensitive generic content such as JavaScript files, scripts, icons and images. The Microsoft 365 CDN is used by default for downloading generic resource assets like the Microsoft 365 client applications from a public origin.

Private origins within the Microsoft 365 CDN provide private access to user content such as SharePoint document libraries, sites and media such as videos. Access to content in private origins is secured with dynamically generated tokens so it can only be accessed by users with permissions to the original document library or storage location. Private origins in the Microsoft 365 CDN can only be used for SharePoint content, and you can only access assets through redirection from your SharePoint environment.

The Microsoft 365 CDN service is included as part of your SharePoint subscription.

For info about how to use the Microsoft 365 CDN, see Use the Microsoft 365 Content Delivery Network (CDN) with SharePoint.

For more info about the Microsoft 365 CDN, see Microsoft 365 CDN.

Related topics

Performance guidance for SharePoint portals

Tune SharePoint performance

Content Delivery Networks

Use the Microsoft 365 Content Delivery Network (CDN) with SharePoint

Creating and launching a healthy SharePoint portal

1/8/2021 • 2 minutes to read • Edit Online

A portal is a Microsoft SharePoint site on your intranet that has a large number of site viewers who consume content on the site. In large organizations there could be several of these; for example, a company portal and an HR portal. Typically portals have relatively few people who create and author the site and its content. Most visitors to the portal only read and consume the content.

Guidance

This set of guidance will walk you through best practices and recommendations before you launch your portal and how to keep your portal healthy.

	WHAT TO DO	FOLLOW THIS	
	Plan the rollout of your portal	Launch in waves	
	Portal design guidance	Review the guidance while designing your sites	
	Run the Page Diagnostics for SharePoint tool	Validate your pages and follow the guidance	
	Optimize your Performance	Follow the guidance below and run the Page Diagnostics for SharePoint tool	
	Use CDN for better performance	Implement Public and Private Content Delivery Networks (CDN)	
	Batch REST API calls to SharePoint	Combine operations into fewer requests	
	Improve performance for slow web parts	Follow guidance to remediate common issues	
	Review page weight	Follow guidance to reduce page weight in your site pages	
	Limit the number of requests to a page	Limit the number of web parts and calls into SharePoint	
	Optimize your images	Follow basic image optimization for the web	

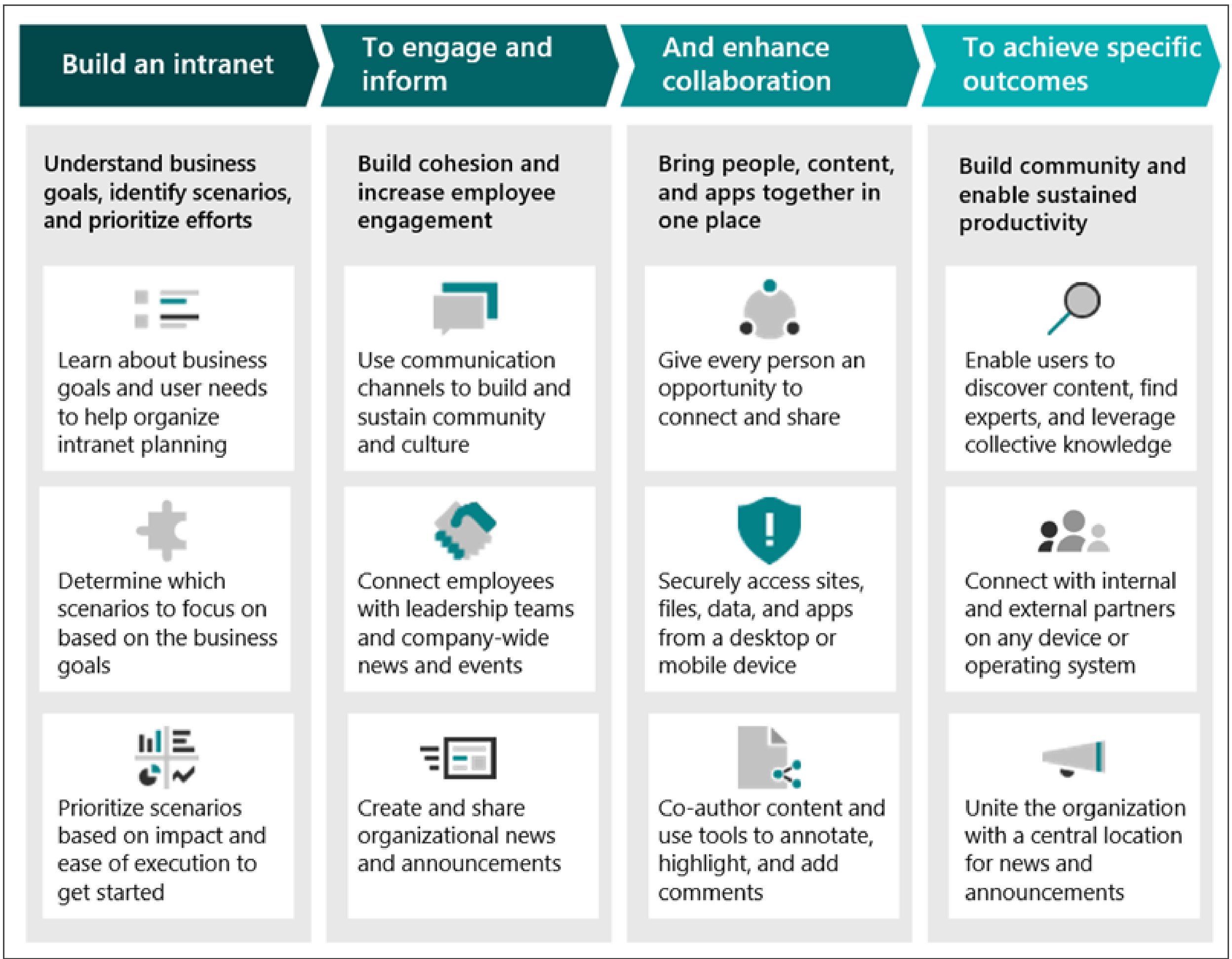
	WHAT TO DO	FOLLOW THIS	
	Limit and use Iframes carefully	Don't use more than 2 Iframes on a page	
	Optimize extensions	Follow the guidance to optimize and limit your custom extensions	
	Modern portal limits	Follow the limits for modern portals to further optimize performance	
	Network optimization	Configure your URLs and IP endpoints	

Intelligent intranet overview

1/8/2021 • 5 minutes to read • Edit Online

Keep employees informed and engaged by providing a shared place to securely view and collaborate on content, and to connect and communicate with colleagues. Build community and culture within your organization by bringing people together through events, networking opportunities, and strategic communication channels. Personalize, share, and manage organizational news and shared content to drive organizational efficiencies securely on any device.

In this solution



Build an intelligent intranet

Learn how to move through the process of creating an intranet for your organization. Get familiar with common intranet planning and creation roles, design stages, and the intranet lifecycle. Learn how to align goals into priority scenarios that you can get started implementing quickly. Then, learn how to engage with viewers and maintain your intranet over time as the organization changes and scales.

Help your organization engage and inform

Use SharePoint and other Microsoft 365 products to create communication channels that serve specific audiences. Learn how to create and share organizational news and use the News web part into key landing pages and portals.

Integrate Yammer and the Yammer web parts to embed conversations and highlights in sites. Leverage the power of video to share pre-recorded messages and record organizational events for later viewing. Use content services like audience targeting to make sure key audience are targeted specific content.

Enhance collaboration and sharing

Create and increase opportunities to collaborate across your organization. Use Microsoft Lists and document libraries to securely store and dynamically display content that can be accessed on any device. Then, users can view, share, and co-author content in real time.

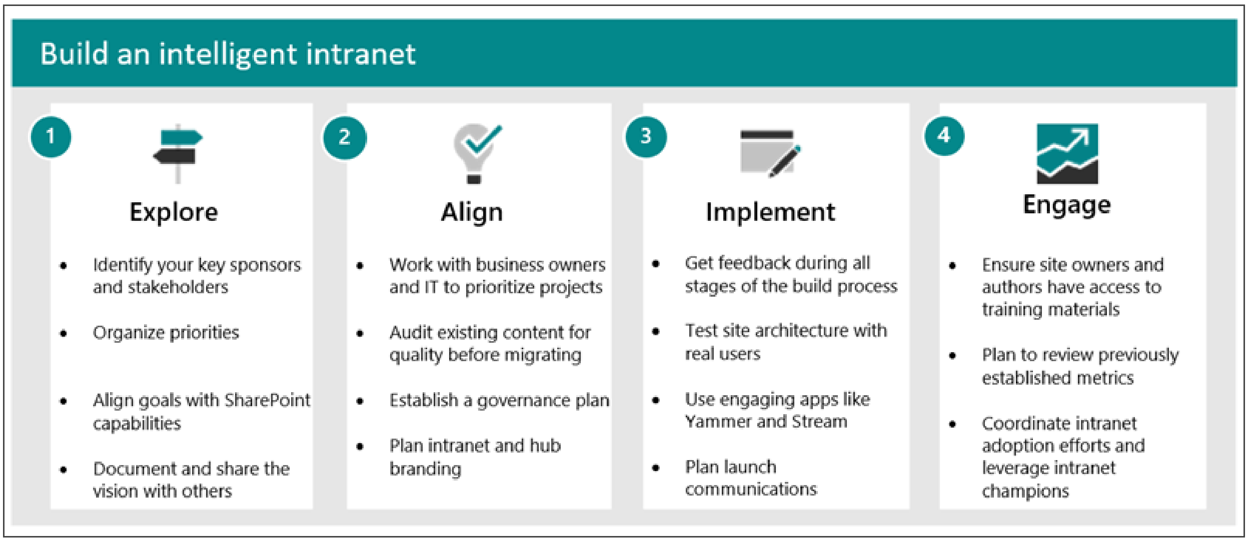
Use SharePoint team sites to create secure collaboration spaces for teams to share content, get updates, and news. Consider adding Microsoft Teams to your team site to add real-time chat and virtual meetings.

Achieve specific outcomes

Use SharePoint to achieve specific business outcomes like narrowing the distance between leadership teams and individual contributors by creating a leadership site that encourages sharing news and starting conversations. Use SharePoint to unite and inform groups of people with related interests by setting up news for a hub site. View custom solutions in the look book to help inspire your next site design or get help with new employee onboarding, crisis communication, and more.

Overview of how to set up an intelligent intranet

Harness the power of the intelligent intranet to communicate effectively across the organization, engage employees, and connect with relevant information and knowledge. Learn more about intranet planning and implementation phases and how to get started, and considerations like how to design your home site and use multi-lingual features. Then, use the intranet roadmap to prepare business owners, stakeholders, site owners, and content authors.



Explore what's possible

Get inspired by what you can accomplish with SharePoint by viewing compelling business scenarios, the SharePoint look book, and guided walkthroughs. Learn more about how to think about your intelligent intranet.

Understand and align

Align stakeholder goals with organizations objectives in order to identify priority business outcomes and to get started planning your intelligent intranet. Learn more about intranet governance before you start building and ensure you have a plan in place to manage intranet governance. Explore various opportunities to engage viewers in workplace communications using Yammer, Teams, live events, and site templates. Get familiar with the intranet lifecycle and basic SharePoint intranet and site building blocks.

Implement plans and start building

Start building the home site, hubs, sites, and pages that will make up the framework of your intranet. Learn more about intranet wayfinding and how to implement multi-geo features if needed. Consider using information barriers to ensure confidential content is seen by the right users or use audience targeting to target specific content to certain groups of users.

Engage and manage

Measure intranet effectiveness by reviewing Microsoft 365 usage analytics and SharePoint hub and page usage analytics. Learn how to improve SharePoint adoption and how to maintain your intranet over time.

Make sure site owners and authors have appropriate training to create, build, and maintain sites. Use support resources available such as the Microsoft Learning Pathways solution as well as your own guidance to ensure that authors are aware of and follow good content and design practices. Consider forming a site owner or intranet champions community to ensure that site owners stay up to date of new capabilities and guidance.

DESIGN PROCESS	LEARN MORE
Plan sites - Help site owners understand how to plan to create high impact sites that meet objectives.	Plan your SharePoint communication site Get inspired with the SharePoint look book Guided Walkthroughs: Creating sites for your organization
Build sites - Learn how to create and customize sites that align with your organization.	Create and use modern pages on a SharePoint site Customize your SharePoint site Customize the navigation on your SharePoint site Using web parts on SharePoint pages
Manage sites - Show site owners how to maintain site content and use site analytics to engage viewers.	Management and life cycle of a SharePoint modern page Manage your SharePoint site settings View usage data for your SharePoint site

SharePoint intranet key capabilities by enterprise product license

CAPABILITY OR FEATURE	DESCRIPTION	LICENSING
Office apps	Office client apps – Word, Excel, PowerPoint, OneNote, Publisher, and Access on up to 5 PC/Macs, tablets, or mobile devices per person.	M365 E5 M365 E3
Social and intranet	Use SharePoint and Yammer to connect and engage across your organization with an intelligent, mobile intranet and enterprise social networking.	M365 E5 M365 E3
Files and content	OneDrive helps you work on a file and save it directly to OneDrive or SharePoint and changes are updated across synced devices. Stream lets you easily create engaging video content. Access and sync files on PC or Mac and mobile devices. Share files with external contacts by providing access or guest links.	M365 E5 M365 E3
Work management	Efficiently manage work across individuals, teams, and organizations. Create and automate business processes.	M365 E5 M365 E3

Learn more

Get more information about Microsoft 365 for enterprise
Microsoft 365 small business license options

More intelligent intranet resources

How to think about your intelligent intranet

Plan an intelligent SharePoint intranet

Introduction to SharePoint information architecture

Planning intranet governance

Branding your SharePoint site

SharePoint adoption resources

How to think about your intelligent intranet

11/2/2020 • 5 minutes to read • Edit Online

These days, there's an abundance of discussions about best practices to modernize your intranet - designing an intranet the new way, in the “modern” way, in the intelligent way - and so on. There aren't many discussions about what modern means as a concept, how modern thinking relates to technology, and how to apply modern principals to your organization's intranet.

Use this guide to understand how to leverage SharePoint to meet your organization's needs through integrating modern concepts into the design of your intranet, portals, and sites.

What does intelligent mean?

In the modern world, the intranet should be the center of your workplace. An intelligent SharePoint intranet is engaging, informative, personalized, and integrated with the other portals and sites in your intranet as well as other Microsoft 365 apps like Microsoft Teams and Yammer. Modern intranets take many shapes and sizes depending on the ever-evolving needs of the business.

Hallmarks of what constitutes an intelligent intranet:

- **Rapid deployment**: Adaptable designs can be built using out of the box pages and web parts and no longer solely depends on IT to deploy.
- **Built with the UX in mind**: Accessible design principals are built into the modern experience enabling viewers to securely access the intranet on any device.
- **Personalized experience**: Features like audience targeting, news, the Highlighted Content web part, and the My Feed web part make it easy to dynamically display personalized content.
- **Software as a service**: Updates are automatic, ensuring you are using the latest technology.

Why invest in the modern approach?

Investing in the modern approach looks different depending on the condition of your current intranet but no matter the path it will require strategic planning and a team to implement changes. By spending resources modernizing your intranet now, you will enable your organization to move faster and more efficiently than before.

What makes modernizing your intranet worth the effort:

- **Move at the speed of your business**: Display content dynamically using flexible designs that scale as your business grows.
- **Meet employees where they are**: Target relevant content to specific viewers on any device.
- **Reduce the cost of technical resources**: Security, permissions, sharing, and other governance components can be centrally managed across Microsoft 365 apps.
- **Improves the likelihood of intranet success**: Viewers are more likely to use the intranet when content is relevant, easy to navigate, and mobile.

How to think about intelligent intranets

Secure and accessible

TRADITIONAL	NEW	HOW TO GET STARTED
Deployed solely by IT	Relies on a collaborative approach with several stakeholders across departments of the organization	Instead of assigning intranet tasks to a few IT members, assemble a team that represents the needs of your viewers and business to create intranet solutions. Learn more about modern intranet teams
Manually governed by IT	Uses governance models that provide flexibility for users in a compliant way based of the organization's goals - sharing, provisioning, risk mitigation	Instead of asking for permission to create a site from IT, site owners can create their own sites using SharePoint's out-of-the-box responsive designs and custom theming. Learn more about managing site creation
Resources can only be accessed in the office or on a computer	Work anytime, anywhere, any place, on any device	Instead of limiting access to content, use SharePoint security and compliance features to make sure viewers have access to the right information on any device. SharePoint works by default on mobile devices.

Informs and engages

TRADITIONAL	NEW	HOW TO GET STARTED
Communication primarily through email	Communicate primarily through SharePoint news, community portals, and Yammer	Instead of sharing a project update in a newsletter, announce your update on your project's site and in the Yammer feed to start an engaging conversation. Learn more about using the Yammer web part
Outdated news is shared in a corporate news feed or newsletter	SharePoint news posts transform news into a visually engaging experience that can be created quickly and distributed to specific audiences in real-time	Instead of communicating big announcements through an org-wide email, create a news post that will dynamically display to your relevant audience. Learn more about creating a news site
Disjointed experience for international organizations	Multi-lingual and audience targeting features ensure users relate to relevant information	Instead of creating separate experiences for unique viewers, target navigational links to specific audiences. Learn more about targeting content to specific audiences

Builds community and culture

TRADITIONAL	NEW	HOW TO GET STARTED

TRADITIONAL	NEW	HOW TO GET STARTED
Intranet structure is based on organization structure	Role and task-based portals house community initiative-driven projects	Instead of separating content by organizational structure, use hubs to organize content based on business initiatives. Learn more about planning hubs
In-person gatherings to build team and organizational culture	Frequent engagement through online events that showcase people, celebrate milestones, and maintain consistent conversation using Yammer and Microsoft Stream	Instead of semi-annual gatherings, record online events and embed the event recording using Microsoft stream in a news post. Learn more about using the Stream web part
Infrequent interaction between the organization and leadership	Aligns organizations with leadership through live events, dynamic content like news, and social connection	Instead of formal engagements with leadership, create accessible outlets in the form of live events in Yammer. Learn more about organizing a live event in Yammer

Creates and extends knowledge

TRADITIONAL	NEW	HOW TO GET STARTED
Static information like FAQ	Dynamic information that's community generated in Yammer	Instead of creating a FAQ page, embed a Yammer web part that connects viewers to subject matter experts and provides insights into previous conversations. Learn more about using the Yammer web part
Browse to find	Search *and* browse to find	Instead of limiting viewers access to content, use SharePoint modern search features that protect sensitive content while increasing search success. Learn more about search in SharePoint
Collection of websites	Collection of experiences	Instead of organizing your internet by area of business, organize by business outcomes and initiatives. Learn more about planning hubs
Limited number and access to subject matter experts	Find subject matter experts and communities of expertise	Instead of relying on finding subject matter experts in siloed organizations, surface expertise in social communities like Yammer and Teams. Learn more about organizing a live event in Yammer

Moving in the modern direction

Understand that your intranet is an ever-evolving component of your business that will need to grow and scale alongside your organization. Focus on incorporating modern changes that will have the greatest impact to your business first. Plan and schedule when changes will be incorporated and how you will track progress. Use site analytics to understand user behavior and collect feedback from users along the way.

Signals your intranet is moving in the modern direction:

- It's where you start your workday
- It's always with you
- Promotes collaboration
- It makes your job easier
- Everything is in one place

Signals your organization can benefit from modern:

- Currently sharing documents in shared folders on a server
- It's difficult to be productive on-the-go
- Your business is growing faster than you can keep up with
- Unmanageable volume of emails
- Your organization has offices in multiple locations

More modern resources

Modern inspiration in the SharePoint look book

Information architecture in modern SharePoint

Modernize your classic SharePoint sites

Modernize your classic SharePoint pages

SharePoint modernization scanner

Intelligent intranet roadmap

11/2/2020 • 21 minutes to read • Edit Online

Your intranet might include your organization's main landing page, portals for corporate communications, and individual sites for departments or divisions (like IT or HR). In this article we look at the high-level tasks needed to create and maintain a successful intranet with SharePoint in Microsoft 365.

Whether you're the organization intranet owners, an IT Professional or administrator, a site owner, or a content creator you're in the right place. Use this article as a guide to help you find the resources that you need for your role and the goals that you have for your intranet. As you read the sections below, follow the links for more detailed information on the areas that you're working on.

Roadmap contents:

Who should use this roadmap?

- Organization intranet owners — This is the person managing the overall direction and coordination of your organization's intranet.
- IT pros and admins — One or more IT and SharePoint administrators who will be responsible for managing the backend configuration and implementation for your organization's intranet.
- Business owners and site owners — The various stakeholders who will be responsible for creating and maintaining portions of the intranet.
- Content authors — The people creating and managing content on sites and pages.

What you'll learn:

- Understand, at a high level, the various roles and responsibilities of creating an intelligent intranet.
- See what you can do with SharePoint out-of-the-box sites and web parts.
- Framework for planning and aligning your intranet around strategic business outcomes.
- Known success factors for creating engaging intranet experiences.

Keep in mind:

Intranets are a constant work in progress and are never really considered done. Make sure you have a plan to keep your content relevant, otherwise your intranet will start losing value on the day that you launch. Celebrate your initial launch, plan to monitor and maintain your intranet and its content over time as the organization changes and business goals evolve.

How to think about an intelligent vs traditional intranet design

The new, modern experience in SharePoint is designed to be compelling, flexible, and more performant. The modern experience makes it easier for anyone to create beautiful, dynamic sites and pages that are accessible and mobile-ready. Modern SharePoint supports intelligent workplaces — those that leverage the collective knowledge of current users, share and collaborate easily, and engage audiences with targeted content and news.

TRADITIONAL INTRANET	INTELLIGENT INTRANET
Communication primarily through email	Communication primarily through SharePoint sites and community portals
Static information like FAQ	Dynamic information that's community generated in Yammer
Corporate news dominates the newsfeed	Personalized news and content is targeted to specific audiences
Hierarchical collection of websites	Dynamic collection of experiences and services provided by independent site collections

Key success factors

Over the years, we have learned about what makes an intranet successful. These factors can help accelerate the creation, adoption, and overall success of your intranet:

- Ensure that your intranet goals are directly tied to key business outcomes.
- Have an executive sponsor and identify intranet champions.
- Establish KPIs that are regularly communicated from the project's start to finish.
- Design for simplicity and longevity.
- Involve your business owners and users to get feedback during all stages of the design process.
- Establish a governance plan that defines roles and responsibilities, guidelines, and best practices, compliance and retention, provisioning sites, and expectations for content management.
- Audit existing content to ensure quality and relevancy before migrating to a new intranet.
- Align your intranet with your organization brand and culture.
- Enable social connection that encourages communication, engagement, and collaboration.
- Train your content creators and your users.

Introduction to roles, tasks, and timelines

At-a-glance:

YOUR ROLE	ALIGNING TASKS	IMPLEMENTATION TASKS	MANAGEMENT TASKS
Organization intranet owners	Strategy, branding, adoption, governance, information architecture, and change management		
IT pros / Admins	Platform integration, content migration, performance, scalability, user training	Site creation, navigation, search, branding, publishing	
Business owners / site owners	Business objectives, permissions, content audit, and migration	Site creation, navigation, branding, audience targeting	Site management, scheduled content audits
Content authors	Content best practices, content, and site design	Create and maintain content, content collaboration	Update existing content, publish new content

See what the intranet lifecycle looks like.

Learn more about basic site building blocks.

Organization intranet owners

The intranet owners work with business owners and IT to prioritize the intranet projects in your portfolio for the greatest business benefit.

Start by getting inspired with the SharePoint look book. The look book provides examples of intranet pages that you can build in SharePoint and will give you an idea of the possibilities. Keep these in mind as you proceed through the planning and implementation process.

Next, start to plan your intelligent SharePoint intranet by working with your key stakeholders to understand your key business and intranet goals. Do research with intranet users to discover key personas and scenarios. Review your existing intranet and determine which initiative to start with for your best return on investment. As you prioritize your intranet initiatives, consider how to get the best performance and scalability from the portals that you build. If your existing intranet is using SharePoint server, consider how migrating your content to SharePoint fits into your overall plan. To troubleshoot page performance issues, use the page diagnostics tool.

Choose one or more opportunities to start with and meet with the business owners in that area of your organization to plan the solution Some solutions may require coordination among different parts of the organization.

As you plan and implement your intranet, keep in mind these key success factors:

- For your intranet, as a whole:
  - Have a sponsor for each initiative and an executive sponsor from the business for the intranet as a whole.
  - Ensure that your intranet goals are directly tied to key business goals.
  - Get a core team together to think about governance — make sure you align your governance decisions to business goals.
  - Align your intranet with your organization brand and culture.
  - Don't assume you have to launch with a "big bang" — align communications and training with your launch plan.
- For each initiative:
  - Gather outcomes, not requirements — be sure to talk to site users, not just owners.
  - Design to align to your organization standards — but allow the site "story" to dictate the navigation and page layouts.
  - Establish success goals for each site and review them regularly.
  - Test your proposed navigation with site visitors — make sure that visitors can easily get to their top tasks.

Key tasks:

Organize your intranet

A critical part of your SharePoint intranet is your site architecture. By using a series of communication sites and hubs, you can create an intuitive intranet with common navigation across related sites and an easy-to-manage permissions structure. For a detailed look at site navigation in SharePoint, see Planning navigation for the modern SharePoint experience.

Start by — Developing an understanding about what you need your intranet to accomplish and start organizing content assets to align with key outcome goals. Organize depending on the needs of the business — by region, department, or function — and by the topics that your users care about.

You'll know you're done when — Business owners and users confirm they can find and have access to the content that makes their jobs more productive.

Brand your intranet

Branding provides a way to align your intranet with your organizational culture. With SharePoint, you can add branding to your SharePoint site, and also customize the Microsoft 365 theme for your organization.

Start by — Answer, do you need a consistent brand across all sites or will different divisions, departments, or groups in your organization have their own look and feel? Then, collect approved brand assets like brand colors, logos, and images depending on your organization's branding requirements.

You'll know you're done when — You've determined the end-to-end look of the intranet from the home page to hubs to individual sites.

IT pros and admins

IT Pros and admins implement the needed platform integration steps needed by your business owners for their intranet portals — such as with databases or line of business applications. This may include content migration from existing systems. They also work with other stakeholders and the business to determine a governance strategy for the intranet and train people in the organization to use SharePoint and other tools to manage the intranet.

As you plan and implement your intranet, keep in mind these key success factors:

- Establish a governance plan that supports business needs as well as your retention, security, and compliance goals.
- Make sure all site owners, content authors, and visitors understand how governance applies to their roles.
- Clean up existing content prior to migration. Only migrate content that is relevant, current, and supports the outcome goals of each site.
- Enable social connection that encourages communication, engagement, and collaboration.
- Train your content authors and your users.

Key tasks:

Plan and align the governance strategy

Governance is the set of policies, roles, and processes that control how your organization's business divisions and IT teams work together to achieve its goal — ensuring organization content and communications are secure and viewers benefit from a consistent experience. Every organization has unique needs and goals that influence its approach to governance. Some details to consider when planning your governance strategy: naming conventions, guest access, classification of sites, groups, and files.

Start by — Understanding the rules and requirements of your organization, in combination with the needs of business owners and site owners. Then, develop a plan alongside IT, HR and senior leadership that allows employees to maximize the value of SharePoint with minimal oversight in a way that's compliant.

You'll know you're done when — When governance stakeholders, business owners, and content creators can work effortlessly in SharePoint without slowing the rhythm of business.

Migrate content from your existing intranet

Your existing intranet may contain content from a variety of sources located on different platforms. A key task in creating your intelligent SharePoint intranet is determining the state of your existing content and deciding which content to migrate to the new intranet.

Your current business owners and site owners may be best suited to evaluate if content should be migrated and you may want to have them perform the actual migration, depending on what's involved. They may need your assistance depending on the quantity and location of the content to be moved. The SharePoint Migration Tool can help you migrate content from SharePoint server and from file shares. Mover can help you migrate from other cloud providers.

Start by — Working with business leaders and other content stakeholders to review your existing content for relevance and accuracy.

You'll know you're done when — A curated set of content has been migrated to SharePoint.

Customize SharePoint to meet your business needs

With the SharePoint intelligent experience, you can create an engaging, easy to maintain intranet without the need for customization. We highly recommend using SharePoint default experiences where possible. This will provide easier change management over time.

If you do need to customize SharePoint, SharePoint provides Framework solutions, apps, add-ins, and solutions to help you meet your business needs. For more info, see SharePoint development.

Train your content authors

Depending on their background, the people in your organization may need some help getting started with SharePoint. Microsoft 365 learning pathways provides a way to bring a curated set of Microsoft content to your users. Other references that can help your content creators manage updates to the site include:

- Create a document library in SharePoint
- Create a list in SharePoint
- Add text and tables to your page
- Add content to your page using the Embed web part
- Use the image web part
- Use the News web part on a SharePoint page

Start by — Determining your users' needs for training on SharePoint and making these references known.

You'll know you're done when — Questions about SharePoint intranet usage on organization social media channels and through the help desk have decreased to a modest level.

Business owners and site owners

As a business owner, you may be responsible for intranet content for a specific area of your organization such as HR or operations. You may also be the site owner, the person who has the permissions in SharePoint to create and maintain the content and experiences on the site. Before you start configuring individual sites, for some ideas, look over the SharePoint look book. As part of your overall governance plan, you may decide that sites need to follow consistent patterns to ensure that readers to not have to spend too much time orienting themselves as they go from site to site or topic to topic in the intranet.

Keep in mind these key success factors as you plan and implement your intranet:

- Have a relentless focus on user experiences as you implement your site — check labels for relevance, ensure images relate to the content, don't assume — test!
- Clean up existing content prior to migration. Only migrate content that is relevant, current, and supports the outcome goals of the site.
- Involve your users to get feedback during all stages of the build process.
- Make sure the site owner or contact is visible in a consistent place on the home page of the site so that visitors know to whom they should reach out for feedback.
- Plan launch communications, which might include a launch event or activity. Celebrate your success!

Key tasks:

Migrate your data

One of the largest tasks in creating a new intranet site is migrating your existing data to SharePoint. We highly recommend doing a content audit to see what's being used, what's up-to-date, and what's no longer needed and can be deleted or archived.

Look for opportunities to eliminate prior versions of documents that you no longer need. If you migrate files ending .v1, .v2, and so on, you will create confusion for your users who won't be able to rely on search to consistently find the latest version of documents.

Train your users to take advantage of SharePoint's automated versioning — and remove version IDs and dates from file names wherever possible, migrating only the latest and most accurate version. Better still, see if you can convert legacy documents to modern pages to create more engaging and easier to consume content. You will get better search experiences and achieve higher user satisfaction and easier maintenance by removing content that's no longer needed prior to migration.

If you're migrating files from SharePoint Server on-premises or file shares, you can use the SharePoint Migration Tool.

Video is a great way to communicate to the people in your organization for executive briefings or when sharing ideas through video can lead to greater engagement. Use Microsoft Stream to deliver live and on-demand meetings, events, and training. If you have existing video content that you want to make available on your new intranet site, upload it to Stream as part of your content migration process.

Start by — Understanding the full scope of content that might need to be migrated and then define the criteria used to target content that should be migrated, should be edited and then migrated, and should be retired.

You'll know you're done when — You've got the minimum amount of content necessary to create and launch an effective SharePoint site.

Determine your permissions and sharing strategy

SharePoint permissions are managed through a set of roles within a site — owners, members, and visitors. Depending on the type of site, there may be additional permission and sharing options available like using Microsoft 365 groups.

Start by — Determining who needs access, who should not have access, and how you will grant access requests.

You'll know you're done when - All site owners and users have access to the content they need, while securing confidential content when appropriate.

Design the intranet portal page

The main intranet portal for your organization is a big part of your new SharePoint intranet. You can create this page at any time during your intranet development project. You can still point to your legacy intranet sites with an intelligent portal home page. If you have an existing communication site that you want to use as your main portal page, you can move it to the root site.

The mega menu, news web part, and Yammer feeds can all be used to make your main portal page an engaging and productive destination for your users. For an end-to-end look at creating this page, read Guided walkthrough: Creating an Enterprise Landing site for your organization.

Start by — Considering the goals from the perspective of your organization's communications team, your executive sponsor, your IT department, and end users. Design the portal home page with simplicity and scalability in mind.

You'll know you're done when — You've created a launch plan for redirecting from your current portal page to the new page and have shared this plan with all stakeholders and users.

Design your business, or topic-specific intranet site

As you start designing the intranet sites for your services and functions, make sure you have done research with your users to better understand their needs and how they currently interact with your content. To create custom surveys and questionnaires and spend time observing users and meeting with them, you can use Forms.

We recommend developing your intranet pages using communication sites. With communication sites, you can share news, reports, statuses, and other information through a variety of templates and web parts. For an end-to-end look at setting up a communication site, see Guided walkthrough: Creating a communication site for your organization. Learn more about how to plan your sites.

To post important or interesting stories, announcements, people news, status updates, and more that can include graphics and rich formatting, you can use the news web part. Within the news web part, to prioritize specific content for specific audiences, you can set up audience targeting. For an end-to-end look at using news in SharePoint, see Guided walkthrough: setting up news for your organization.

To align your organization's branding requirements, you can change the look of your site.

Start by — Prioritizing business objectives, and then decide the type of sites and web parts that will be needed initially.

You'll know you're done when — Business and site owners have dedicated areas in SharePoint that can been owned and maintained with little oversight.

Content authors

Content authors are the people who create content on sites. Content authors can take on many responsibilities such as creating and publishing news, creating topic-specific pages, or serving as subject matter experts and thought leaders for special projects and initiatives. Content authors should get familiar with SharePoint design fundamentals.

As you create and manage content for your intranet, keep in mind these key success factors:

- Consider whether content is best presented as a page or a document. Use pages when your content is dynamic and most easily communicated with engaging web parts such as images, video, or links. Use documents when your content is designed to be downloaded or printed.
- Summarize up front — place the information readers must have for your communication to be successful at the top of the page before you focus on the design.
- Use sections and heading styles to visually separate topics and concepts to make your pages more readable and accessible.
- Create custom page templates to drive consistency and simplify page creation.
- Ensure you follow image and video guidelines to keep page performance high.

Key tasks:

Inform and engage

Collect and manage content using SharePoint pages. Use lists for information you might collect in Excel. Lists enable you and your audience to gather, track, and share information. Improve the display of lists with column and list view formatting using the List web part. Use libraries to store documents. Easily add, reorder, sort, filter, and create custom views of libraries using the Document library web part.

Dynamically display content from a document library, a site, a site collection, or all sites using the Highlighted content web part.

Create and curate news relevant to your audience using the News web part. Quickly create eye-catching posts like announcements, people news, status updates, and more that can include graphics and rich formatting.

Customize the way your users view content and news by using audience targeting. Audience targeting enables specific content to be prioritized to specific audiences on the SharePoint start page, news on the mobile app, and in News web part when audience targeting is enabled.

Enable users to work on any device. When users keep files on their local device or on a network share, they're out of luck when they don't have the device with them or don't have a connection to your network. If something happens to a user's device, the data might not be recoverable. Get the SharePoint mobile app.

Start by — Organizing content into topics, creating pages for each topic. Determine whether the page content should include text, links, list, or libraries. Align the content to the story to ensure that the reader can get the information that they need efficiently by quickly scanning or skimming the page.

You'll know you're done when — You can confirm users have access to the right information at the right time by using site usage and analytics, and asking users for feedback.

Build culture and community

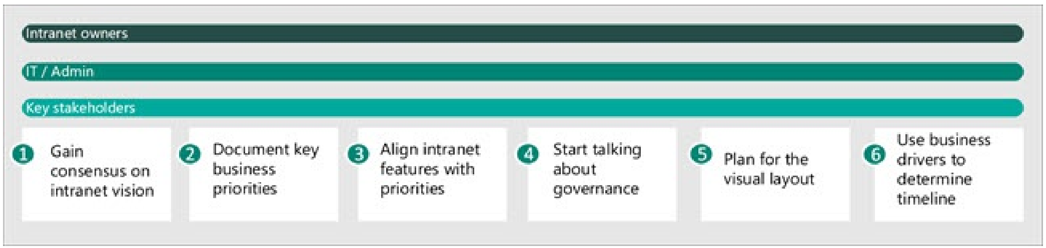
Help work groups connect and engage across your organization using Yammer. Learn more about the Yammer Highlights and Yammer Conversations web parts. Sometimes content needs to be delivered through video - like when organization-wide announcements are made or when senior leaders host a live event or when you want to provide examples on pages that provide instructions. Microsoft Stream is your organization's own video site. To display video content, use the Stream web part on your site.

Start by — Finding news, announcements, and events to amplify on your site.

You'll know you're done when — You are regularly promoting news and events that start conversations and engage and connect wide audiences.

Get started

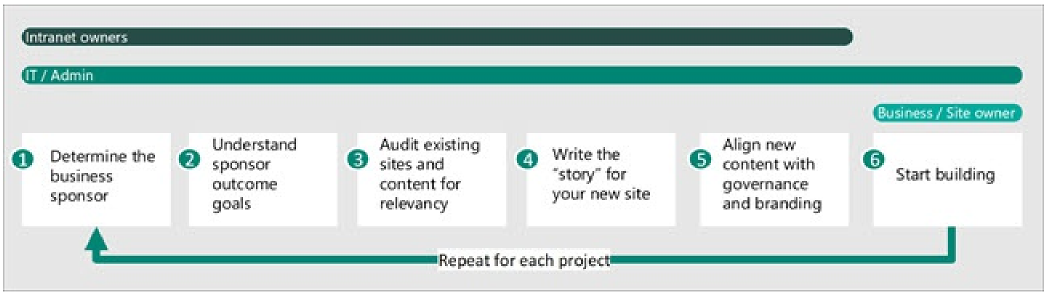
Explore



- Identify your key sponsors and stakeholders and review key organizational priorities. Document a vision that will help provide direction and help you prioritize opportunities.
- Align key outcome goals with SharePoint capabilities to identify where you may need to invest in customization. Consider whether an "intranet in a box" solution might be appropriate for your organization.
- Think about governance. What processes will you need to create to provision, manage, and maintain sites and content? Do you have security, retention, or compliance goals that need to be considered?
- Think about branding and architecture — do you want all sites to share a common look and feel?
- Analyze possible opportunities to identify priorities.

ROLE	EXPLORATION TASKS
Organization intranet owners	Identify your key sponsors and stakeholders and review key organizational priorities. Document a vision that will help provide direction and help you prioritize opportunities.
IT pros / Admins	Organize a core team to plan governance — make sure you align your governance decisions to business goals.
Business owners / site owners	Help identify key organizational opportunities and priorities.

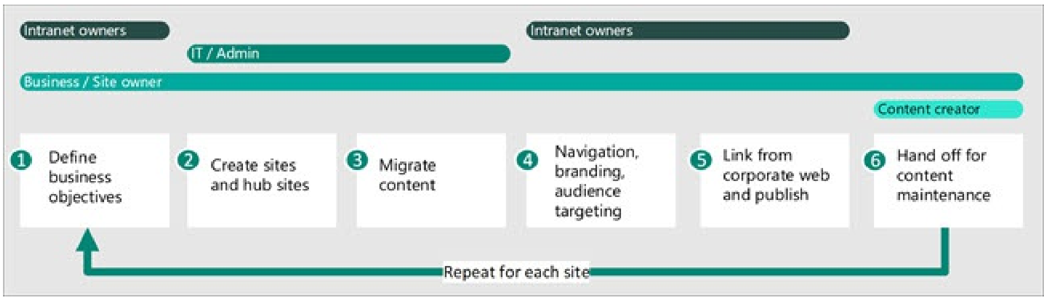
Align



- Work with business owners and IT to prioritize the intranet projects in your portfolio for the greatest business benefit in the shortest time.
- Start by developing an understanding about what you need your intranet to accomplish and start organizing content assets and business outcomes. Organize depending on the needs of the business — by region, department, or function — and by the topics that your users care about.
- As you prioritize your intranet projects, consider how to get the best performance and scalability from the portals that you build.

ROLE	ALIGNING TASKS
Organization intranet owners	Communicate goals and progress from project start to finish. Director of the branding direction, governance strategy, information architecture, change management, and product adoption.
IT pros / Admins	Responsible for platform integration, content migration, performance, scalability, and end-user training.
Business owners / site owners	Develop and plan solutions to business objectives. Responsible for site permissions, content audit, and content migration.
Content authors	Authority on content best practices, content creation, content management and page design.

Implement

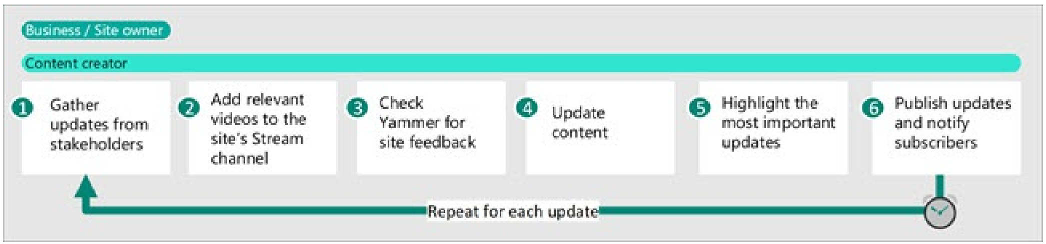


- Communicate goals progress regularly.
- Measure, learn, and pivot as you go.
- Get feedback regularly.

ROLE	IMPLEMENTATION TASKS
Organization intranet owners	Get user feedback along the way. Use findings from user feedback to learn and pivot your intranet plan.

ROLE	IMPLEMENTATION TASKS
IT pros / Admins	Implement decisions made by the intranet stakeholders regarding site creation, navigation, search, branding, and publishing.
Business owners / site owners	Use business objectives to drive decisions around site creation, navigation, branding, and audience targeting.
Content authors	Create solutions to business objectives by creating and sharing relevant content with the right audiences.

Engage, manage, and maintain



- Celebrate the launch of your new intranet.
- Use metrics to measure progress.
- Communicate what's new.
- Maintain high quality content.
- Educate users.

ROLE	MANAGEMENT TASKS
Organization intranet owners	Celebrate the launch of your new intranet. Communicate goals and progress regularly after the launch.
IT pros / Admins	Communicate what's new with intranet stakeholders and business owners. Educate end-users about publishing rules like site creation and content retention policies.
Business owners / site owners	Schedule content audits and use site usage metrics to measure progress.
Content authors	Refresh existing content, publish new content and participate in scheduled content audits to keep content up-to-date and compliant.

Related topics

SharePoint adoption resources

Ways to work with SharePoint

Guide to the Modern experience in SharePoint

Intelligent Intranet Envisioning Workshop PowerPoint deck

Plan your intranet

Plan your communication site — get started

Plan an intelligent SharePoint intranet

1/8/2021 • 12 minutes to read • Edit Online

Microsoft SharePoint offers a wide variety of options and tools to create intranet sites for your organization. Moving your intranet to SharePoint in Microsoft 365 might take a while, particularly if you already have extensive intranet content. In this article, we'll look at how to plan a new SharePoint intranet with a focus on quickly bringing sites online and getting a return on your investment.

We'll cover how to:

- Understand your key organizational priorities
- Understand your audience
- Plan for governance
- Review your current intranet
- Identify and prioritize your business initiatives
- Identify one key scenario to prototype and pilot
- Launch the pilot and engage with your users

What's possible with SharePoint?

With SharePoint, any user can create highly functional intranet pages quickly without the need for writing code or other difficult customizations. These sites look great on any device or screen and provide deeply engaging experiences for your users.

If you're currently using SharePoint Server for your intranet, you'll find SharePoint in Microsoft 365 to be much easier to work with. Responsive, dynamic pages are easy for anyone to create, and the requirements for IT to build and maintain custom solutions are much less.

As a first step, to see examples of what's possible with SharePoint, we recommend that you review the SharePoint look book. The look book provides a variety of examples about how to include news, events, resources, and personalized content in SharePoint sites that anyone can create and maintain.

For an understanding about how the different component parts work together, review the Guide to the Modern experience in SharePoint.

For an interactive workshop to learn how to succeed with a SharePoint intranet, look for an Accelerator workshop in a city near you.

In the following sections, we look at how to find the best starting point for your SharePoint intranet and how to prioritize the different intranet solutions that you may need for your organization. Keep these references handy as you work with your stakeholders - they can help you get the most value and best time to value for your intranet solutions.

Understand current business goals and key stakeholders

The most successful intranets don't just look good, they are primarily focused on helping people get work done and often on promoting engagement. The look book can help inspire you to think about how your content might appear, but your business outcome goals are important to understand what content and functionality are most important for your users and your organization.

All organizations have important strategic goals that drive behavior and investments. If you want to be sure that your intranet is successful – and gets the right level of funding – you need to ensure that it is aligned with these goals. You can also use these goals to help prioritize your intranet initiatives. Unlike many technology projects, an intranet project is never "done" because your organization priorities and interests will change over time. But, at any given time, you want to focus on the intranet initiatives that are most closely aligned with your organizational priorities and key business stakeholders.

In addition, take a look at recent employee satisfaction survey data. A good way to become more informed about the information and tools that your employees need is to look at the pain points identified in these surveys.

Understand your audience

A good place to start thinking about your new intranet is what it will be like when the intranet is in place. What will people be able to accomplish? How will they start their day? What will people say about the intranet? One potentially helpful exercise to frame the overall objectives for the intranet is to engage your key intranet stakeholders in a cover story exercise. This is an exercise in imagination. The purpose is to think broadly about an ideal future state by imagining a magazine cover story about the new intranet, including the key headlines, sidebars, and quotes from users.

With the end in mind, it can also be helpful to create personas for your key users. A persona is a fictional but realistic description of a typical intranet user (for example, new starter/new employee, knowledge worker, field worker, sales rep, people manager, or content author). You'll want to do some research to engage with people who represent these different personas to understand their information requirements. You can't build an intranet without an understanding of the people for whom you are building it. Site owners alone are not enough – their perspective is what they want to publish. That is often not the same thing as what their users want to consume.

Think about governance

If your users complain that search is not successful because too much irrelevant content is discovered, this can indicate a governance problem. Before you think about your new intranet project, think about how you will govern the architecture and the content. These are decisions that are a lot easier to make and enforce if they are decided early in your intranet project. For example, you will want to think about:

- Who can provision new sites and when they are provisioned, what is the process to ensure that sites are discovered in navigation or as key bookmarks in search?
- Do you want all sites to follow a similar pattern so that users can easily find key content as they move from site to site?
- Who is accountable and responsible for the content on sites? How often does content need to be reviewed?
- Is content management for intranet sites in the performance goals or job descriptions for people with edit or owner permissions?
- Does intranet content need to be retained based on your retention policies or classified based on its sensitivity?

You do not need to make every governance decision up front, but if you don't have a plan for how you will govern your new, intelligent intranet, it can quickly become a wasteland of information that fails to achieve your critical business goals.

Review your existing intranet

Your current intranet may be composed of sites from different business groups, such as HR, IT, Facilities, Engineering, and others. As a first step to planning your new SharePoint intranet, we recommend taking an inventory of your existing sites and meeting with the owners of each to determine their business outcome goals for new sites. Take stock of where your content is located and how much content you would need to move when creating a new intranet site. Look at your current content to understand if it is current or needs to be updated prior to moving to a new site. It's not unusual to find a migration strategy where existing content is left behind. You don't have to migrate anything – you may find that it is more effective to create new content that is optimized for the modern SharePoint experience rather than migrate existing, out-of-date content to the new location.

As part of these meetings, you can identify the business needs that are addressed by each existing site as well as any requirements you might have for new sites.

In addition to meeting with current site owners, you may also want to convene a focus group of new employees. New employees are a key audience for the intranet and people who have joined the organization in the past two to three months can provide some valuable insights about what is missing or hard to learn in your current intranet, or resources they wish they had when they first started. They may also provide you with some valuable ideas from the organizations where they previously worked to help you think about new and important capabilities to incorporate.

Think of this step as an opportunity to learn. You are learning about what is important to your users and to the business. You will use this information to identify initiatives for your intranet.

Identify initiatives

Using the information you gathered during your research, work with your key intranet stakeholders to identify initiatives that reflect your organizational priorities – as well as any barriers that might exist when you are implementing them.

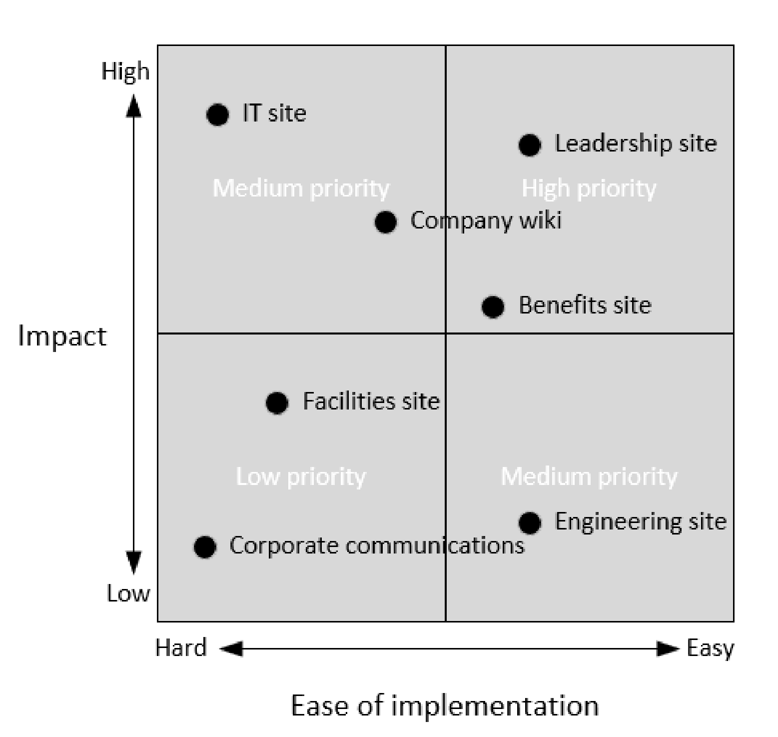
While you may ultimately implement solutions to address all of the identified initiatives, prioritizing which project to do first will help you achieve early success and user engagement as efficiently as possible.

Review each initiative you have identified for the following criteria:

- Does it solve a real problem?
- How many people will use it?
- Can it be built in a reasonable time frame?
- What's the return on investment?

Analyze each initiative for its positive impact on your users with respect to the ease of implementation. A high impact initiative that can be built with a minimum of customization can be an ideal first project.

Consider plotting your business initiatives on a grid, like the following, and review with your intranet stakeholders and IT department to choose the best option to start with.



To help decide which initiative to address first, work with the business leaders for that area to work out the objectives for the solution, who will be responsible for driving success in this area, and the metrics that you'll use to measure success. Don't just focus on system metrics. Think about actual business impact. For example:

INITIATIVE	KEY CONTENT	BUSINESS OWNER	SYSTEM SUCCESS METRIC	BUSINESS SUCCESS METRIC
Educate employees about benefits (Benefits site)	- Announcements - Training videos	HR	- News post views - Training video views	Help requests are reduced by x%
Weekly news post by a senior leader	- Streaming events - Formal training	Engineering	- Training content produced for all aspects of coding excellence - Monthly streaming events	Training completed successfully by x% of engineering staff
Foster positive employee agreement about company strategy (Executive Leadership Yammer Community)	News posts - Streaming events - Yammer conversations	HR	Ongoing monthly activity posts by leadership and comments by employees	- Yammer conversations show positive sentiment - Comments addressed within 24 hours – "no question/comment left behind" - x% increase in employee satisfaction scores for executive communications
Improve timeliness consistency in proposal development (Marketing site)	- Company business value slides - Proposal templates	Marketing	- Slide downloads - Sales team alignment	x% reduction in the time to create proposals

Choose pilot scenarios

Work with the owner of each scenario to determine what an ideal solution would look like to them:

- Who are your visitors?
- What do the visitors to the site want to accomplish or learn?
- What tools or technology do they use today?
- What information do you want to promote?
- What tools or technology do you want visitors to use to accomplish their key tasks?
- Who are the champions who will help them transition to the new site or solution?
- How will you know if your solution is successful?

For example, create a table like the following to list business scenarios that you want to address with intranet sites across your organization:

AS AN...	I NEED TO...	SO THAT...	I KNOW THIS IS SUCCESSFUL WHEN...
Employee	Understand and be able to update my benefits	I can take advantage of a key lifecycle benefit	Help requests are reduced
Employee	Learn about how to use the self-service benefits portal	Make updates on my own	THelp requests are reduced
HR employee	Promote the use of the self-service benefits portal	I can spend more time working with employees on unique benefits questions and scenarios	All of my employee interactions are about individual critical scenarios

From the high priority scenarios, identify which ones meet these three key criteria:

- Can you build a prototype quickly (a few days)?
- Is there a committed sponsor?
- Is there enough up-to-date content to demonstrate key capabilities?
- Is there a specific audience for a pilot?

After you have compiled this information, create a design brief to help map out the user journey about how you want the site to operate. For example:

USER JOURNEY COMPONENT	DESCRIPTION
Scenario	Leadership site: One-stop site for employees to hear from company leadership, learn the company's goals, and hear the latest news from customer meetings and industry events.
Users	All company employees.
Value	Increase employee awareness and alignment with company strategy and business initiatives.
User journey	- News post is sent to the company announcing a leadership Q&A meeting - Allan goes to the leadership portal to watch the event live - Allan uses Yammer to ask a question at the meeting - Allan shares the recording link with coworkers.

USER JOURNEY COMPONENT	DESCRIPTION
Metrics	- Live event views - Event recording views - Yammer engagement
Stretch goals	- Continued Yammer engagement - Improving employee sentiment (survey)

Choose solution components

SharePoint offers a variety of building blocks that you can use to create an intranet:

- Communication sites - Use communication sites to share news, reports, statuses, and other information through a variety of templates and web parts.
- Home site - A home site is a communication site that you set as the intranet landing page for your organization.
- Hub sites - Use hub sites to organize related sites and teams and centralize news, search, and content management.
- SharePoint news - Use the news web part to post important or interesting stories, announcements, people news, status updates, and more that can include graphics and rich formatting.
- Yammer - Use Yammer to connect with people across your organization beyond the boundaries of projects, functions, and departments.
- Forms - Use forms to create custom quizzes, surveys, questionnaires, registrations, and more.
- Stream - Use Stream to deliver live and on-demand meetings, events, and training.

For the scenario that you've decided to build, choose the components that you'll need to use to meet the site's business objectives. We recommend creating a rapid prototype, and granting access to your key stakeholders. This provides a substantive framework for further discussions and revisions of the design.

At this stage, we recommend that you involve your help desk so that they are prepared to answer questions after the site rolls out to a larger audience.

For best practices for launching an intranet site, review Creating and launching a healthy SharePoint portal.

Roll out the pilot

When the prototype has evolved to a point where you want to share it more broadly, you can roll it out to a pilot group, or even to the whole organization. User adoption is a critical part of success for a new intranet site. To drive site usage, we recommend that you use both a top down and bottom up approach:

- Recruit executive sponsors who can ensure that the intranet project is funded, and can help message the importance of the new site to others in the organization.
- Empower champions throughout the organization to promote the new site on a grass roots level.

Other things you can do to drive success include:

- Have launch events and communications campaigns.
- Provide formal training.
- Hold regular office hours where users can ask questions.

As the site rolls out and more users engage, watch your success metrics and make adjustments as needed to drive additional engagement and user satisfaction.

When the site is on its way to success, take stock of any lessons learned in the process and proceed on to the next intranet project that you want to undertake.

Related topics

SharePoint look book

Intelligent Intranet Envisioning Workshop PowerPoint deck

Considerations when planning for a global intranet

1/8/2021 • 4 minutes to read • Edit Online

If your organization has team members in multiple locations around the world, you have additional considerations and options as you plan for your SharePoint intelligent intranet. For example, you may want different branding for individual regions. You may want to target content to team members in certain regions or countries. You may want to provide sites in multiple languages. Or you may need to comply with data residency requirements in certain countries. Here are options to consider which can be used independently or in combination to meet the needs of your global intranet and create the best experience for your users.

Hub sites

Multilingual sites and pages

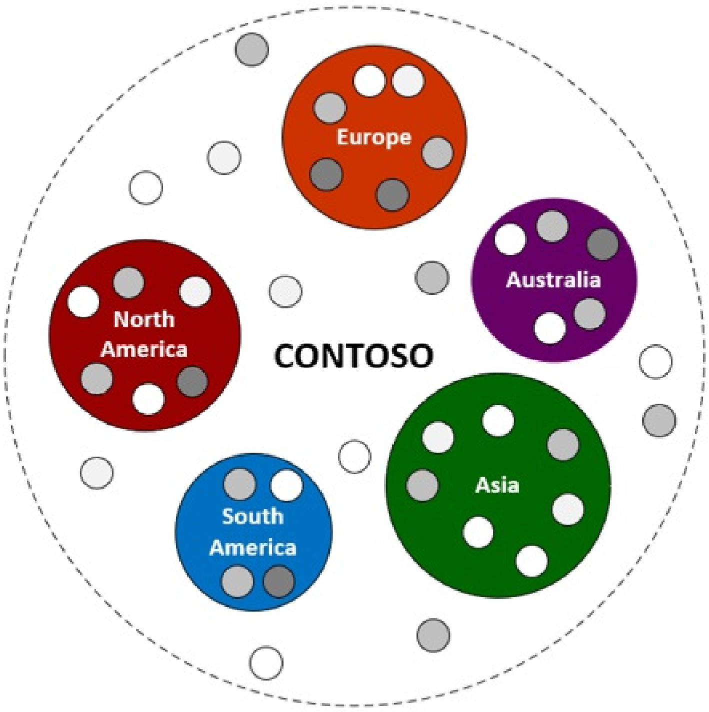
Regional settings

Audience targeting

Multi-Geo for data residency requirements

Hub sites

The advantage to using hub sites is that they provide a flat architecture that is flexible and carries branding and navigation across multiple sites connected to the hub.



If you have subsidiaries in different regions that have their own branding and navigation, an option for you is to create a hub site for each region.

Learn how to plan for hub sites

Multilingual sites and pages

A separate consideration for a global or regional intranet is whether you want to set up sites on your intranet to be multilingual so that users can read and work with content in their preferred languages.

User interface elements like site navigation, site title, and site description can be shown in the user's preferred language. Additionally, you can provide pages and news posts on communication sites that you translate to users' preferred languages. For example, you may have provisioned your site with a default language of English, but you have users who have set their language preference to Spanish, and users who have set their language preference to French. You can set up your site(s) to view in the site default language as well as in French and Spanish.

> **Note** User interface elements and pages are not translated automatically. Each page created in your default language can have a corresponding page in a chosen target language that you, or someone you assign, manually translates. After you translate such a page and publish it, it will automatically be displayed to users who have set a preferred language in their Office personal profile.

Next steps for multilingual sites and pages

- Site owners determine which languages to support on their sites
- Site owners enable multilingual features and choose languages
- Create multilingual communication sites, pages, and news
- Set up a multilingual site name, navigation and footer

Regional settings for sites

Site owners can change regional settings for a site to specify calendar settings and how numbers, dates, and times are shown for all users of a site. Individual users can choose to specify their own personal settings.

Audience targeting

Audience targeting helps the most relevant content get to the right audiences. By enabling audience targeting, specific content will be prioritized to specific audiences through SharePoint web parts, page libraries, and navigational links.

For example, you might want to prominently display news about a sales meeting in Asia to users in that region rather than display it prominently to all regions.

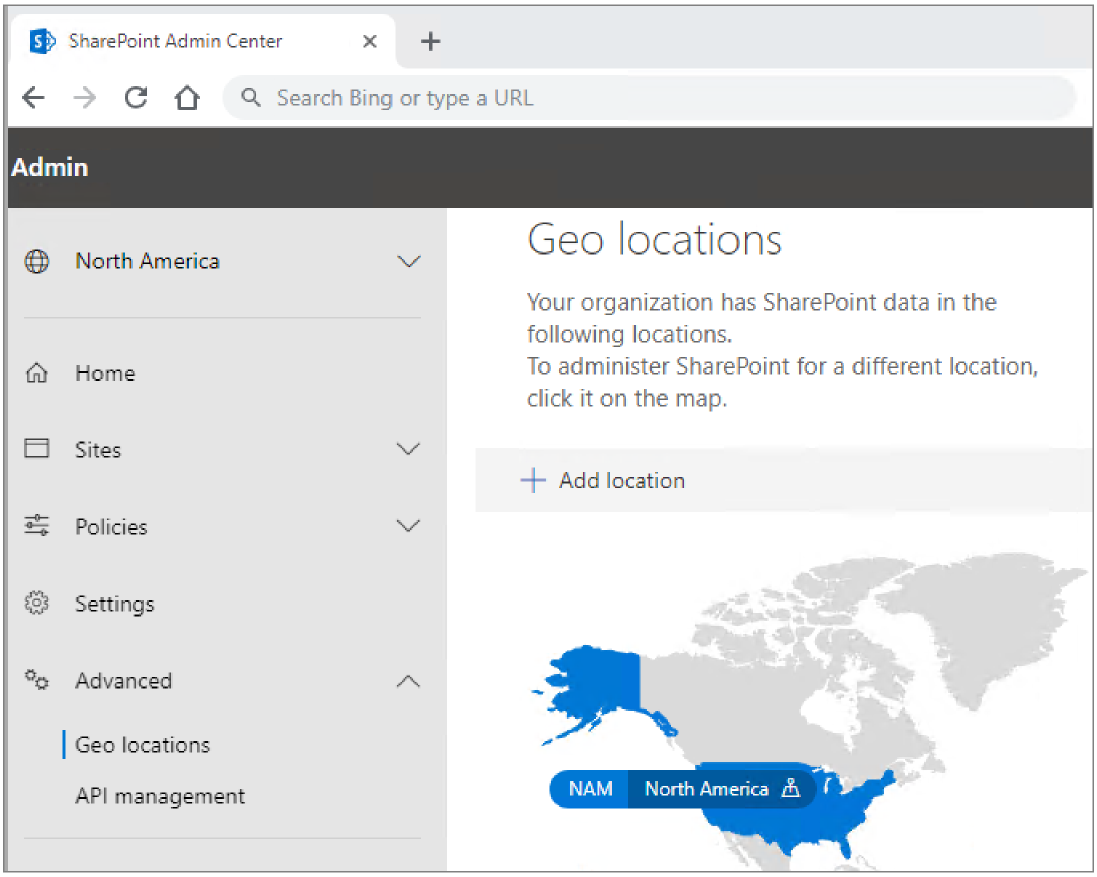
Next steps for audience targeting

- Learn how to set up audience targeting
- Learn more about creating groups for audience targeting

Microsoft 365 Multi-Geo

Some countries have laws requiring that user data be stored within that country. To accommodate these requirements, you can set up a Microsoft 365 Multi-Geo tenant. With a Multi-Geo tenant, your tenant may be provisioned in one country, but user data for SharePoint, OneDrive, and Exchange can be stored in other countries. For example, you may have 5,000 employees in Europe and 8,000 employees in North America. All the users are working within the same tenant, but data for the 5,000 employees are stored in Europe while data for the 8,000 employees is stored in North America. This allows for seamless collaboration across your organization while still meeting data residency requirements.

The M365 administrator needs to enable Multi-Geo, and then SharePoint admins manage the Multi-Geo feature in the SharePoint admin center.



Notes Due to the unique nature of data requirements in China, a differentiated version of Office 365 is available and operated by a partner from datacenters inside China. This service is not considered a Multi-Geo service. It is powered by technology that Microsoft has licensed to 21Vianet. For more information, see Office 365 operated by 21Vianet - Service Descriptions.

A differentiated service called Microsoft Cloud Germany is being migrated to Office 365 services in the new German datacenter. For more information see Migration from Microsoft Cloud Deutschland to Office 365 services in the new German datacenter regions.

Next steps for Microsoft 365 Multi-Geo

- Microsoft 365 administrators plan and set up Multi-Geo for their organization
- SharePoint administrators set up Multi-Geo in the SharePoint admin center to enable Multi-Geo features across the user experience

Planning intranet governance

1/8/2021 • 19 minutes to read • Edit Online

As you plan your new intranet project, think about how you'll govern the site architecture and the content. Your intranet governance plan should be created in the context of the overall governance plan for Microsoft 365. As a key business solution in your digital workplace, your intranet will have its own unique governance requirements and expectations, especially because of its organization-wide focus and impact.

Planning intranet governance should happen during the envisioning process - to ensure that all stakeholders have shared vision and goals. Envisioning is only the beginning. Your intranet governance plan will evolve as your organization evolves and as new capabilities are added to SharePoint and Microsoft 365.

A good governance plan helps define the priorities for the intranet and helps to prevent content sprawl. It also ensures that roles and responsibilities are clearly defined and communicated – and ideally, incorporated into job descriptions or performance goals. One aspect that often separates your intranet from other solutions is the number of people who are involved in creating and maintaining content. To ensure ongoing success, it is important to make sure that each of your intranet stakeholders and users understand their roles and responsibilities.

Intranet governance also includes policies and procedures but it is so much more than that. Intranet governances needs to include a plan for user training, monitoring usage,user behavior, and communicating expectations to all of the diverse stakeholders involved. This is why creating a governance plan document is challenging. It is difficult to create a single document that addresses these multiple audiences and can be communicated in a way that encourages adherence and adoption.

Instead of creating a document or series of documents, consider creating a resource site that incorporates training as well as governance in a single place. Think about how you can combine "how to" (training) with "how should" (governance) so that when your intranet users visit your user resource destination, they understand both "why" and "how" your intranet is designed and governed the way you have implemented.

You can consider leveraging the Microsoft 365 Learning Pathways site as a possible starting point or create your own user resource center that integrates with or complements the Learning Pathways content.

Having an effective governance plan in place enables the decision-making process for the intranet. By reviewing and revising the governance plan on a regular basis, you can help ensure that your intranet remains a critical asset for your organization.

Governance Team

As a key business asset, intranet governance needs to reflect the goals of business stakeholders and the legal and regulatory environment for your organization – not just the expectations of your IT department. Create a governance team that includes core members from key business stakeholder groups in your organization in addition to IT.

There is no magic size for the governance team, but it should be small enough to make it easy to make decisions and representative enough to incorporate the "voice of the business" as well as IT. When you have specific topics to review that extend beyond the expertise of the team, you can bring in outside members (such as Legal or Records Management) to ensure that your decisions are aligned with organizational constraints.

Your governance team may meet on a frequent basis during intranet planning and then less frequently over time. The goal is to establish a rhythm that works for your intranet and team members. Since governance has an ongoing role for your intranet success, the governance team should not be disbanded when you launch.

Governance Plan Elements

There is no “one size fits all” model when it comes to intranet governance. In fact, your intranet governance plan may be different for different types of content. For example, you may want to have more formal policies and stricter governance guidelines for sites that face the entire organization and less strict policies for content that is more targeted, such as content for an individual department or a one-time event (see Figure 1). The best approach is to look at the different elements and think about what is critical or necessary for your organization. Consider your audience and the culture of your organization to guide your decisions and approach, as well as your overall Microsoft 365 governance expectations.

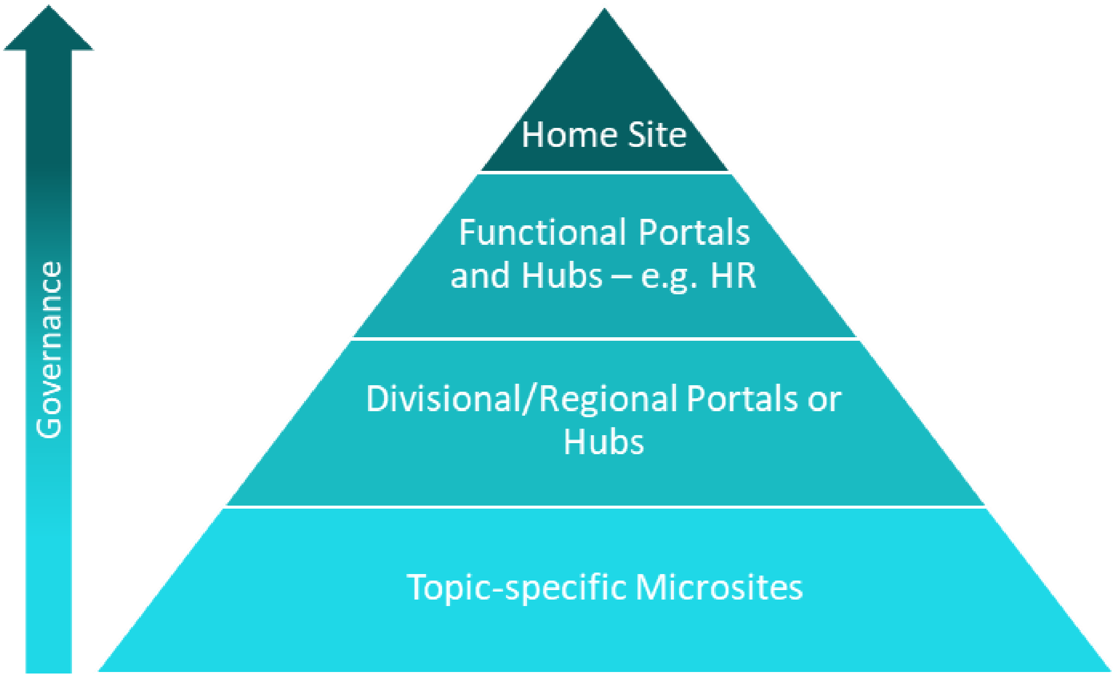


Figure 1. Your governance decisions may be different (and stricter) based on the "reach" of your content.

At a minimum, consider each of these elements as part of your intranet governance planning effort.

- Vision
- Policies and guidelines
- Site provisioning and decommissioning
- Information architecture and search
- Branding
- Content management
- Security and information management
- Roles and responsibilities
- Feedback
- Training and support
- Measurement

Vision

The vision statement describes, at a high level, what you want to want to achieve with your intranet - essentially how the solution delivers value to the organization and to each individual employee. Use the intranet vision statement to guide your governance plan. Be sure that the vision is clear because the degree of formality and the depth to which you need to document the governance plan should align with the outcomes you want to achieve.

A clear vision statement provides critical guidance to the inevitable decision tradeoffs you will need to make for your governance plan. For example, you probably do not want a completely uncontrolled environment with unstructured and “unfindable” content if your intranet vision is to provide a key source of organizational knowledge and information. In this case, the unstructured environment with no controls is unpredictable and will likely misalign with desired business outcomes. In a different scenario, some users may have a goal to create an experimental place where new site owners can create "practice" sites to try out new skills or test alternative approaches to solve specific business problems. For this use case, an overly restrictive governance plan may not make a lot of sense. You may determine that you don't want to support an unlimited number of "practice" sites, so you may want a governance policy that says that all "test" sites are deleted after a specific period of time. But, for these practice or test sites, the unstructured environment is fine. You can only know what is level of governance is ideal because you have a clear vision. The vision provides a framework for both the context and your investment in governance. Once you are clear about your intranet vision, your governance team can use that vision to guide the governance decisions.

Your intranet vision includes defining ownership. There is no right answer about which organizational entity should "own" the intranet – and often, intranet ownership is shared by more than one organizational unit. However, most intranet professionals agree that there is one organization that should not be the exclusive intranet owner – IT. IT cannot build an intranet for the business. IT can only build an intranet with the business and with a commitment from the business. Successful intranets have a champion and owner from the business, ideally at an executive level.

Policies and guidelines

Policies define the rules and guidelines for your intranet. From a governance perspective, policies are usually driven by statutory, regulatory, or organizational requirements. Users are expected to meet policies without deviation. If your organization is subject to regulatory oversight, be sure you can enforce your policies as a failure to do so may target your organization as being "non-compliant." Guidelines are usually established to encourage consistent practices. In many cases, guidelines are more recommendations, but policies are requirements.

For example, consider the topic of site ownership. A policy might state, "All SharePoint sites will have a primary and secondary contact responsible for the site and its content." A related guideline might state, "The site contact is listed in a web part in the lower left-hand corner of the site home page." The guideline might become a policy for major functional sites but remain a guideline or recommendation for topic-specific microsites. Another example of a policy is whether external users can have access to the intranet as a whole or only to individual sites. The policy might have a default value of no external access but there could be a process that allows for exceptions to allow specific partner users to have access to some intranet sites.

Each organization will have its own set of policies and guidelines. General topics should include content oversight, site design, branding and user experience, site management, and security.

Steps to ensure success:

- Verify that your intranet policies and guidelines do not conflict with broader organizational polices and your overall governance decisions for Microsoft 365.
- Publish policies and guidelines where users can easily find and follow them. Some policies may need to be published for "all users," while others may need to be secured to protect the integrity of the application. Consider creating a governance site rather than a document to facilitate publishing and "consuming" governance policies and guidelines.
- Leverage capabilities to automatically apply policies and guidelines wherever you can. For example, you can enforce content management and retention policies with information protection capabilities in Microsoft 365. You can encourage following design guidelines by using site designs to embed best practices in sites as they are created. The best way to ensure that your policies are followed is to ensure that site owners and authors don't have to think about them. Try to automate as much as you can and where you can't automate, plan to provide training to ensure that site owners and content authors clearly understand governance expectations.
- Regularly review and revise policies and guidelines to keep them aligned to organizational needs.

Consider these topics for your intranet policies and guidelines:

- External sharing – can external users access intranet sites?
- Default sharing links for intranet documents - consider setting the default for all intranet sites to be "People with existing access" to ensure that site owners don't accidentally create links that allow visitors to edit key intranet documents.
- Site navigation – for individual sites and the intranet as a whole.
- Site designs - including guidance for items like the positions of key web parts on departmental home pages. Do you want all sites to follow a similar pattern so that users can easily find key content as they move from site to site? If so, then you may want to leverage site designs to ensure that it is easy for site owners to follow your design patterns.
- Metadata architecture and content types - for example, policies for enterprise content types and organization-wide metadata).
- Guidelines for Teams chat and Yammer conversations - including more than just messaging policies for Teams and how to participate in a Yammer conversation, but also conversation guidelines (such as using @mentions sparingly and organization-specific "do's and don'ts").
- User profiles – including expectations for the About me statement as well as expectations for skills and expertise (for example, how well do you have to know a topic to list it in the skills and expertise area of your profile?).
- Organizational policies and guidelines for intranet site names, file names, Microsoft 365 Group names, etc.
- Learn more about Microsoft 365 intranet governance decisions.

Site provisioning and decommissioning

A key intranet governance decision involves determining who can create a new intranet site. Your modern intranet architecture will be "flat" which means that your intranet will contain a lot of sites. Do you want to provide a self-service model for new intranet sites or do you want to manage site creation through a form submission and workflow? There is no right answer to this question – but no matter which approach you choose, you need to think about governance. There are two popular solutions to governing new site creation:

Implement a site request process for intranet sites

You can easily hide the option to create a new site in the SharePoint admin center. If you do so, you will want to create a process for users to request a new intranet site. Having a request process makes it easy to review and track site requests and ensures that your environment remains "tidy," but if your review and approval process takes too long, it could be frustrating for your users. Your provisioning process can leverage a site design to ensure consistency or you can manually create sites to follow your design patterns. A key part of your provisioning process will be to ensure that new site owners have the appropriate guidance and training that they need to be successful when you fulfill their site requests.

Allow self-service site creation

If you enable self-service site provisioning, you will want to consider providing site designs that embed your best practices so that new site owners start with a "template" that aligns to your governance guidelines. You will also want to track new sites in the Admin Center so that you can follow up with new site owners to provide the information that they need to be successful after the site has been created.

In addition to providing a process to provision new sites, you will also want to think about a process to provision new hubs and associated hubs. Hubs must be provisioned by the Global or SharePoint Admin so you will need to think about how you will plan and govern the creation of new hubs.

When an intranet site is no longer needed, there may be cases where your records management process prohibits deletion of the site and/or content. Another key governance decision is planning how you will delete or decommission intranet sites in the context of both legal holds and records management requirements. Learn more about Microsoft 365 compliance, including records management and advanced eDiscovery.

Information architecture and search

Well-planned information architecture is a prerequisite for a successful and well-performing intranet. It is difficult to separate planning your intranet information architecture from planning your intranet governance. These two planning tasks go together and you will likely find that you are thinking about the two aspects of your intranet iteratively and simultaneously. Intranet governance should cover several key aspects of your information architecture:

- **Navigation architecture** – how your sites and hubs will be associated to support users who navigate or browse for content.
- **Page architecture** – guidelines for pages, especially site home pages, to help create consistent experiences across all intranet sites.
- **Metadata architecture** – columns and content type planning to support consistent approaches for organizing content and pages.
- **Search experiences** – understanding how users will find content when they don't know where it might be in the architecture and how they will discover content. You can help users discover content and improve search outcomes by leveraging several features in search, including acronyms, bookmarks, Q&A, floor plans, and locations. For more information, learn how to make content easy to find and how search experiences work in SharePoint. Your governance plan should include how you will support and manage the creation of the search discovery attributes.

Branding

Brand standards help to define the look and feel of your intranet. These standards are reflected in site and page designs. Your brand standards can include standards for the use of imagery, including requirements to use only brand-compliant images or icons from an organization assets library on intranet pages, as well as requirements to leverage only brand-compliant custom themes for sites. Your standards might prescribe a specific theme for different types of sites or sites with different access levels. Your standards might also include content authoring standards such as tone of voice, spelling conventions, accessibility standards, and other guidelines that support your organizational brand. Learn more about branding in SharePoint.

Content management

Content management is one of the most important parts of your intranet governance plan. Many intranet users complain about intranet search – that they can't find what they are looking for. Most often, the problem is not with search; the problem is that there is no content management in the governance plan!

Some common content issues include: Files are often duplicated rather than linked – so search finds multiple copies of the same document and the searcher doesn't know which one is the correct version. File names often include version numbers instead of allowing SharePoint to manage versions – so search finds all the various versions of a document and not just the most recent, making it harder for the searcher to find the current version of a file.

Your governance plan should include these key content management concepts:

Content creation

- Where should content be published? For example, if I am not the "owner" of a document, should I publish it to my intranet site? Or instead, should I find the owner and ask them to publish it so that I can add a link?
- Are there guidelines for creating intranet content? For example, what is the appropriate tone of voice and are there specific guidelines organizing content on pages? When should content authors create documents for the intranet and when should they create pages?
- Are there accessibility standards that content authors need to follow? Consider these 8 tips to create accessible SharePoint pages (from the Humans of IT Blog on the Microsoft Tech Community).
- How should files be named? Should your governance content include file naming recommendations such as not including version numbers in file names?

Information protection

- Does your organization have a requirement to protect certain types of sensitive information? If so, can your governance plan (and deployment) leverage Microsoft 365 information protection capabilities such as sensitivity labels and retention policies?

Content review

- Do you want to set up flows using Power Automate to trigger intranet content review at a specific time interval?
- Who is accountable to review content and at what frequency? Is it the site owner or the content author or another role? Is the expectation different for different types of sites or different types of content?

Content disposition

- Do you have requirements to implement records retention policies on some or all content to prevent accidental deletion?

Security and information management

Your governance plan should not only include what *should* be posted on the intranet – but it should also include guidelines for content that *should not* be posted on the intranet. You may be able to enforce some policies using automated information protection capabilities, but you will want to provide training and guidance for site owners and content authors to ensure that they understand their responsibilities when it comes to security and information management for both sites and content.

Roles and responsibilities

Roles and responsibilities describe how each employee as an individual or in a role (such as Site Owner) is responsible for ensuring success of the intranet. Documenting roles and responsibilities is a critical aspect of your intranet governance plan. To ensure that intranet responsibilities are treated seriously, it is helpful to partner with your human resources organization to ensure that intranet responsibilities are part of job descriptions or performance goals.

It "takes a village" to successfully support an intranet in any organization. You will need a team - and the team may include specialized roles that you leverage on an occasional basis, such as developers to create a custom web part, permanent roles such as site owners for whom intranet site management is a small part of their job, and other permanent roles for people whose entire job responsibilities involve intranet management. Some organizations find it helpful to organize their intranet resources in a center of excellence, which may include full time members of the IT staff supplemented with virtual members who work in different business groups around the organization. Others extend their centralized staff to include "intranet champions," who extend the support team into various departments and geographic locations by volunteering to help ensure intranet success.

No matter who is in your "village," it is critically important that everyone understands their role and for which aspects of the intranet they are responsible. Figure 2 shows an example of a role and responsibilities description for an intranet Site Owner.

Some of the key roles to consider for your intranet governance plan include:

- Intranet Steering Committee
- Intranet Business Owner
- Intranet Technology Owner
- Corporate Communications
- Training
- Intranet Governance Team
- Site Owners
- Hub Owners
- Site Members/Editors
- Site Visitors
- Yammer Community Owners

- Yammer Community Members
- Team Owners
- Team Members
- Intranet/SharePoint/Microsoft 365 Champions

Feedback

Your intranet governance plan should incorporate a mechanism to collect feedback from intranet users. This includes a vehicle to collect feedback – for example, a Microsoft Form linked from the footer of your home site – but also mechanisms to gather and process the feedback and take actions based on the feedback. It is a good idea to acknowledge all feedback, even if you don't plan to take an immediate action.

Training and support

Your intranet will not be successful if you don't incorporate a way to provide training and support for all users, but most especially, Site Owners. The best way to reinforce your governance policies and guidelines is to build them in to your training. In other words, don't provide training that only shows "how to" – make sure that your training also includes your policies and guidelines – the "how should" aspect of your governance plan.

It is helpful to provide a dedicated site where Site Owners and other intranet users can find training and governance information. You can create your own "user resource center" as described earlier or leverage a third-party or Microsoft-provided training environment. To ensure that your training content is always current, you can link to content in Microsoft's training platforms such as support.office.com and docs.microsoft.com. You can also embed the support.office.com training into your own environment by deploying Microsoft 365 Learning Pathways in your tenant and adapting the content to include your governance policies and guidelines.

You can help your intranet users find your training content by adding a custom tile to your Organization Profile or adding a custom help link directly in Microsoft 365.

Measurement

Your intranet measurement plan should be aligned to the criteria for success defined for the intranet vision. It should define the metrics and analytics used to track success, any associated KPIs, and processes for evaluating metrics and taking action to make improvements.

Look for metrics that are more than just page views. Just because a page is viewed does not mean it is adding value to users. Instead, look at metrics that measure business value. For example, are you seeing fewer support tickets related to expense processing because your intranet was updated to include better and more up-to-date content about expense reports? Are you seeing fewer help desk calls regarding how to upload documents because you have updated your training content and made it more accessible? Are HR representatives spending more time on unique issues because the HR content is organized more effectively?

If your initial design plan identified key business outcomes or surveyed users to ensure they had easy access to the information they need for their job, repeat the process after you have deployed or updated your intranet to identify the business impact of your intranet update or investment. Supplement this data with qualitative feedback from site owners and users to create a comprehensive assessment of the effectiveness of your intranet and your governance plan. Don't be afraid to decommission content or sites that are no longer relevant. You can optimize your intranet value by using metrics to identify duplicate, out-dated, and irrelevant content and sites.

Additional intranet governance resources:

SharePoint governance overview

How to think about your modern intranet

Engage audiences with workplace communication

1/8/2021 • 9 minutes to read • Edit Online

Learn how to keep everyone informed and engaged using SharePoint, Microsoft Teams, Yammer, and Stream for live events and other workplace communication methods across your M365 environment. Learn more about the powerful strategies and communication tools available to you that help drive engagement in your organization. In this article:

- Introduction to live events across Microsoft 365 applications
- Learn how to connect leaders and team members using live events
- Learn how to create a culture of inclusion using personalization and multilingual features
- Discover the best communication channels and methods for your workplace

Introduction to live events across Microsoft 365

You can create a live event wherever your audience, team, or community is currently communicating using Microsoft Stream, Microsoft Teams, Yammer, and SharePoint. Your organization's goals and M365 configuration will determine how you leverage and combine M365 apps to host live events.

Live events allow attendees to receive notifications and to participate in real time, with high-definition videos and interactive discussion on Teams or Yammer web, mobile, and desktop apps. After an event, it's easy to make the recording available on an event page in SharePoint. The recording is automatically transcribed by Stream and detects changes in speakers and topics, making it easy to search for content later.

These features become especially valuable when considering employees who are in different time zones or unable to attend live. Keep the conversation going so everyone still feels connected with leaders and peers after the event, which is a great method to overcome geographical and organizational boundaries.

Learn more about live events across M365 apps.

Benefits of using live event features across SharePoint, Teams, Yammer, and Stream:

Employee engagement is a major contributor to workplace satisfaction, loyalty, and productivity at any organization. Interactive live events allow program coordinators to effectively communicate business updates, training opportunities, and announcements in a way that makes an impact on the daily lives of employees and fosters ongoing collaboration and knowledge-sharing.

- **Reach large audiences with video and interactive discussion.** Viewers can join the event regardless of their office location or work-from-home status.
- **Share your screen or share the stage.** Easily deliver live events sharing content from your desktop or webcam. For high-profile events, connect to professional cameras, multiple content sources, and more.
- **Empower everyone to participate.** Moderated attendee Q&A or open dialog including all participants provide multiple options for interactions during broadcasts.
- **Watch recorded events anytime with on-demand events.** Ensure viewers never miss an event with on-demand video. Now anyone can catch up quickly and see transcripts, captions, and speaker timelines to help find the moments that matter to them.

Summary of live event apps:

Your organization's goals and M365 configuration will determine how you leverage and combine M365 apps to host live events.

Teams - If you want your audience to view the event in Microsoft Teams, create the event so your viewers can join and watch from Microsoft Teams. **Yammer** - If your audience is already using Yammer, you can create live events and have them show up directly in Yammer where the viewers can participate in live discussions before the event, while watching the event, and after the event. **Stream** – If you don't want viewers to watch the event in either application, you can use Stream.

How to decide which app is best for your live event

There are other considerations besides tenant configuration that will determine which apps you select depending on the level of engagement desired and governance policy of your organization. Depending on which service you create the live event from, and the type of event, there will be a different set of features available as the producer, presenter, and viewer of the live event.

While planning your event, ask and find answers to these questions:

- What application are users currently using to attend live events and watch videos?
- What device are users likely to use when attending a live event or watching a video?
- How do you want viewers to engage with event presenters?
- What production set up is preferred?
- What are the ideal post-event next steps?

Learn more about the differences between live events in Teams, Yammer, and Stream to get answers to these questions. Use site and hub analytics to get more insights about how users are currently engaging with SharePoint content to help you make decisions.

Leadership connection

Bring the organization together by combining communication channels with M365 live event features across Stream, Yammer and Teams. Then, see how you can leverage SharePoint using the leadership connection guided walkthrough example to create sites that help connect viewers with leadership by creating new communication channels and a video archive library of recorded events for later viewing.

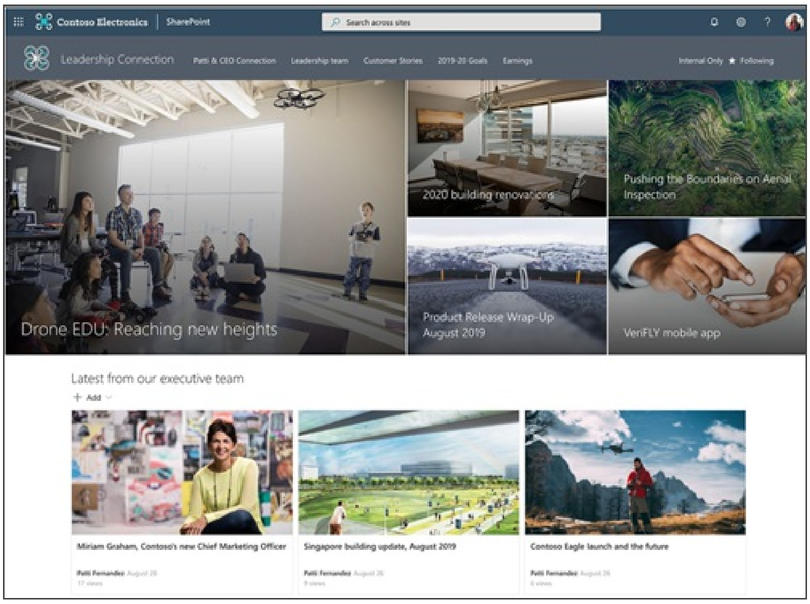
Company-wide events

Large events that include all employees like "town halls" or "all hands meetings" are one of the ideal scenarios for leveraging a live event. When planning for a live event, start by ensuring your M365 environment is set up and configured following guidance for each app in the *admin* section. The admin role is responsible for all the work behind the scenes work that makes the event possible and ensures the live event follows your organization's security and compliance policies. Then, learn about live event planning and production in the section for the *producers* and *presenters*.

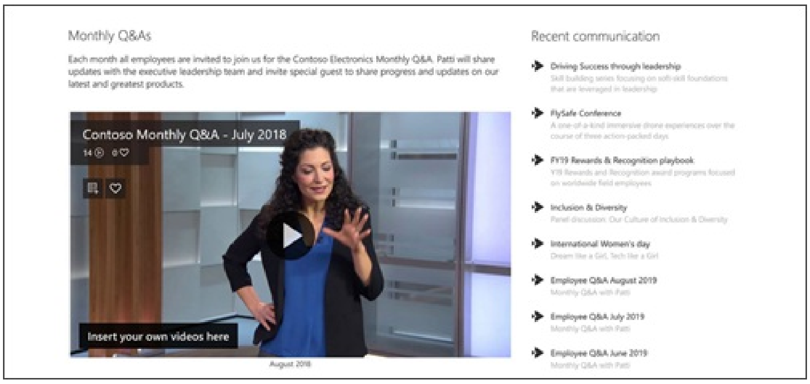
TEAMS	YAMMER	STREAM
Admin	Admin	Admin
1. Admin quick start - get ready for Microsoft Teams live events 2. Set up and configure settings in Teams live events for your tenant 3. Start planning a live event in Teams	1. Review the Yammer live events overview 2. Understand there are some changes between the new Yammer and classic Yammer	1. Get started with live events in Microsoft Stream 2. Create a live event 3. Use Microsoft Stream in Teams
Presenters and producers	Presenters and producers	Presenters and producers

TEAMS	YAMMER	STREAM
1. Get started with Teams live events 2. Learn how to produce an event 3. Plan and schedule a live event 4. Use the Teams live event organizer checklist 5. Manage recordings and reports	1. Organize and event in Yammer 2. Review Step-by-step playbook of hosting an event in Yammer 3. Learn how to drive engagement for your Yammer event	Use the Stream web part to add a video to a SharePoint page

Create a leadership site in SharePoint



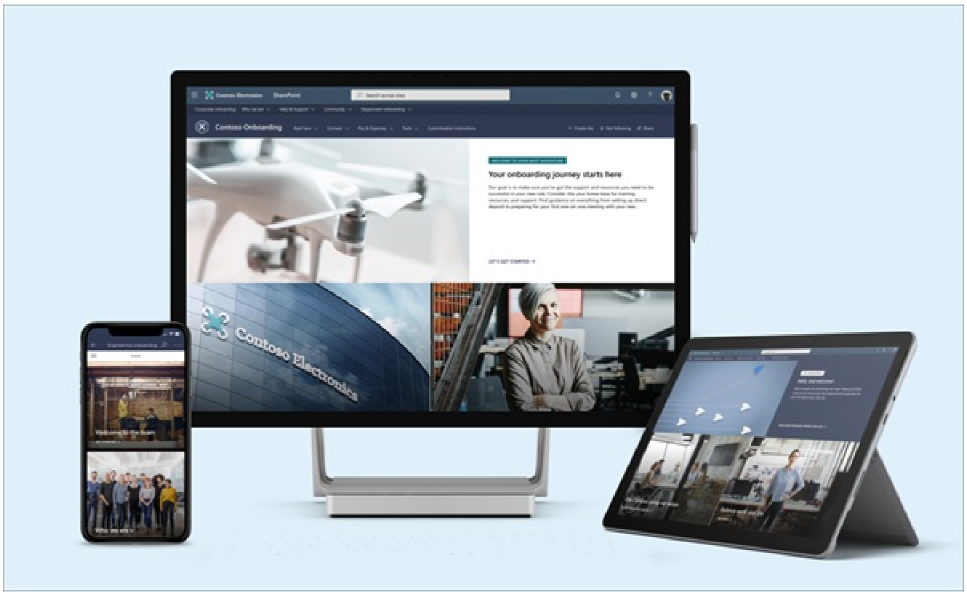
Use SharePoint to create a place for your organization to share news from leadership and recordings from company-wide events. Get inspiration from a step-by-step example of how to create a leadership site for your organization.



In this example you'll see a great way to leverage recordings of live events on a SharePoint page. Showcase recordings on a page using the Stream web part. Then, create a list of links to previous recordings using the Quick links web part. Consider adding the Events web part to your leadership site to share upcoming company-wide events with all employees.

Create a culture of inclusion

Technology allows for a much broader reach across the globe and can be used to keep organizations connected. Leverage live event to foster a culture of inclusion that ensures all employees can participate in opportunities to network with each other, engage in collaborative discussions, and connect to leadership. See how you can leverage M365 live event features and other communication channels into SharePoint pages to boost reach and viewership for important content.



- **Welcome new team members** – Provision the New employee onboarding template to create a welcoming and inclusive environment for new team members.
- **Keep the conversation going with Yammer** – The Yammer conversations or highlights web parts enable dynamic communication channels where you need them most. When users post questions and get answers, other users can view responses and benefit from past conversations stored in Yammer.
- **Personalize the viewing experience** – Make sure viewers get what they need when they need it by using audience targeting to personalize the experience for viewers across navigational links, pages, and news posts.
- **Provide multiple language options** - Use multilingual communication sites and news if your organization spans a diverse population to make content in your intranet sites available in multiple languages. User interface elements like site navigation, site title, and site description can be shown in the user's preferred language. Additionally, you can provide pages and news posts on communication sites that you translate and that are shown in the user's preferred language.

Streamline workplace communication

Across M365 there are multiple ways to communicate – between email, Teams persistent chat, Yammer conversations – there are plenty of options. Knowing which method to use depends on the communication culture of your organization. It's important to meet viewers where they are. Use established communication channels to connect users across apps to promote collaboration and engagement.

Organizational news

Create and share news fast using SharePoint out-of-the-box news post features quick layout options and web parts that dynamically roll-up news across sites. Learn more about how to create and share news in SharePoint. Use the News web part on SharePoint sites and hub pages to share news sources across your organization's intranet. Finally, create and send a news digest for newsletter style messaging that can be shared in an email or Teams channel message.

Maintain high-quality content in SharePoint

Understand how users are consuming content, what devices are typically used, and what content is popular using by viewing usage data for your SharePoint site. Use content insights to make adjustments to your organization's communication strategy. For example, if you learn that most users are reading news on a mobile device in the evening, you can make a point to post news in the evenings.

Make it easy for users to follow your organization's site usage and creation guidelines by streamlining site and page designs in SharePoint. Templates ensure a consistent design and navigational experience across your intranet and help users create sites faster. Learn more about creating page templates in SharePoint.

Add resources to Teams

Meet users where they are. If you are already using Teams, there are many options to share content across apps in Teams by adding resources as tabs in Teams or sharing a message in a channel. Add a SharePoint page or list as a tab in Teams or add a Yammer page as a tab in Teams to keep content and communication for specific departments, teams, or projects in one place. Make sure important messages get to the right audiences by sending an email to a Teams channel or by sending an announcement to a Teams channel. Finally, bring your organization's intranet closer to resources in Teams by creating an intranet portal app from a SharePoint site or page.

More workplace communication resources

IT roundtable: Migrating from Skype meeting broadcasts to live events across M365 apps

How leaders can bring employees together during COVID-19

Transform your communications, company meetings, and trainings

Learn more about live events across M365 apps

SharePoint modernization scanner

SharePoint governance overview

1/8/2021 • 2 minutes to read • Edit Online

Governance is the set of policies, roles, responsibilities, and processes that control how your organization's business divisions and IT teams work together to achieve its goals. We recommend that you consider governance first as you start working with SharePoint. Having a governance plan in place early can help your organization stay compliant with your business processes and regulations.

Two of the primary ways SharePoint is used in an organization are *intranet sites* and *collaboration*. See Planning intranet governance and Overview of collaboration governance in Microsoft 365 for a look at governance in these two areas.

Resources

Use these resources to further explore governance in Microsoft SharePoint and related services.

SharePoint

- Manage site creation for SharePoint in Microsoft 365
- SharePoint site designs & site script overview
- Learn about retention policies
- Managing sites in the new SharePoint admin center

Related services

SharePoint is tightly integrated with other Microsoft 365 services, including Microsoft 365 Groups, Teams, and Yammer. It's important to think about SharePoint governance in a way that's inclusive of these other services. Microsoft 365 includes a variety of options to enable your governance policies across SharePoint and related services, including Teams, Planner, Stream, Outlook, Yammer and Microsoft 365 Groups.

To see how SharePoint governance capabilities overlap with other Microsoft 365 services, see:

- Settings interactions between Microsoft 365 Groups and SharePoint
- Settings interactions between Microsoft 365 Groups, Teams and SharePoint

For lifecycle guidance for SharePoint sites together with related Microsoft 365 services, see:

- Plan organization and lifecycle governance for Microsoft 365 groups and Microsoft Teams
- End of lifecycle options for groups, teams, and Yammer

Related topics

Manage who can create Microsoft 365 Groups

Microsoft 365 reports in the admin center – Microsoft 365 Groups

Create a secure guest sharing environment

Limit accidental exposure to files when sharing with people outside your organization

Create guidelines for site usage

11/2/2020 • 4 minutes to read • Edit Online

Using the steps below as a template, create your own custom guidance for SharePoint site owners on how sites are set up and managed in your organization. Each section provides guidance about what to include, sample text to help you get started, and links to resources to learn more about each area.

Download the PDF

Introduction

Guidance:

- Provide a short introduction to frame your guidelines. If you have broader business or digital resource use policy, link to it if it applies to SharePoint sites as well.

Sample text:
A SharePoint site is designed to be a powerful tool for team collaboration and communication. [enter your IT/productivity service org] administers the Microsoft 365 service your site is built on. The goal is to make it easy to accomplish your business goals.

General guidelines

Guidance:

- Provide general policy statements that you want your users to follow. These may include key business uses you have defined for sites, internal communication policies, or security and privacy guidelines.

Resources:

- Plan your SharePoint site
- Guide to the modern experience in SharePoint

Sample text:
*Here are some things to keep in mind as you work with your SharePoint sites. Refer to [**insert your organization's name**] business resource use policy. These policies apply to all SharePoint site usage.*

Guidelines for creating your site

Guidance:

- Provide basic procedural guidance. How does someone get a SharePoint site? It may be via the "Create site" link on the SharePoint start page or you may have a unique provisioning process for your organization.
- If you have specific site templates that you want your site owners to select when they create their own sites, include that info in this section.
- Include information on custom provisioning solutions.
- Are there any ownership or site classification requirements your organization has implemented?
- When you set up your site, it's important to select the appropriate site classification level. Include references or links to your your organization's data classification guidelines.

Resources:

- Manage site creation in SharePoint
- Secure SharePoint sites and files
- Branding and site provisioning solutions for SharePoint

Sample text:
*Sites can be created via the "Create site" link at [***insert your SharePoint link***].*

You should have two site owners who are both full time employees at your org.

*When you set up your site, it's important to select the appropriate site classification level. [***Insert link to your organization's data classification guidelines***].*

Your site designs and customizations

Guidance:

- Provide information on design guidelines. Does your organization have or allow custom themes? Or do you stick with out-of-the-box options?
- Do you have specific templates or web parts you want site owners to use? Explain those so they understand why and how.
- Does your organization allow custom scripts and add-ins?
- We recommend creating a way for site owners to engage with your team when they want to customize a site. Set up a service ticket category or form to make it easy to contact you.

Resources:

- Manage site creation
- SharePoint site theming overview
- Plan customizations, solutions and apps for SharePoint

Sample text:
*It's important that your site meet your business needs. If you need to create a custom add-in or deploy a resource-intensive app, work with our internal team. For more information, contact [***insert information on how to contact your IT team***].*

Sharing guidelines

Guidance:

- Provide information on the way your organization has set up sharing. If you have modified the settings from the defaults, you can tell your site owners what the sharing settings are for your organization, including for external sharing.

Resources:

- Plan your permissions strategy

Sample text:
Your site and its contents can be shared internally within our organization or externally with your customers or partners.

As site owner, you will receive access requests when someone shares your site. You can approve or decline any requests sent to you.

Capacity guidelines

Guidance:

- Provide information on the site storage guidelines or limits (if you manage them manually). Tell site owners if you have a process and policy for requesting more.

Resources:

- Manage site storage limits

Sample text:
Your site allows for _____ MB/GB of storage. You're encouraged to remove files and content you don't need anymore.

Managing access

Guidance:

- Provide detailed information on site access. What are your processes and policies for managing site access? What level of control do your site owners have? If you manage access on behalf of your site owners, let them know that you will be reviewing site permissions regularly to keep them in line with your organization's policies. Explain how you will communicate changes to permissions to them.

Resources:

- Secure SharePoint Sites and Files

Sample text:
Plan to review your site's permissions on a regular basis and set the level of access appropriately.

Site lifecycle policy

Guidance:

- Provide your organization's lifecycle policy for sites. Does your organization set site expirations automatically or with a managed process? Do you set Microsoft 365 Group expiration policies that impact SharePoint team sites? Let your site owners know when their site will expire, how they will be notified, what will happen and what they need to do to extend their site.
- Setting this policy requires Microsoft 365 global admin permissions.
- Does your organization take extra measures related to site backup and restore? Let your site owners know how long the backup is available and if needed, how to get a site restored.

Resources:

- Microsoft 365 Group Expiration Policy

Introduction to SharePoint information architecture

1/8/2021 • 15 minutes to read • Edit Online

Well-planned and executed information architecture is a prerequisite for an intelligent and high-performing intranet, hub, or site. The most important first step in planning an effective information architecture is understanding your users and helping them find what they need to complete tasks in a way that makes the most sense to them.

Information architecture also helps improve user adoption, satisfaction, and productivity while reducing IT costs, information overload, and minimize compliance and security risks.

In this article:

- Learn the main elements of information architecture
- Review the different roles involved in implementing information architecture
- Understand the different levels of information architecture – global, hub, and local
- Explore SharePoint information architecture building blocks

Information architecture elements in SharePoint

Information architecture is about how you organize and label your content and how your visitors interact with the content to get work done. This includes elements like navigation, search, site hierarchy, taxonomy, and security. Modern SharePoint information architecture is also about how to ensure the right content gets to the right people and follows your organization's content compliance regulations.

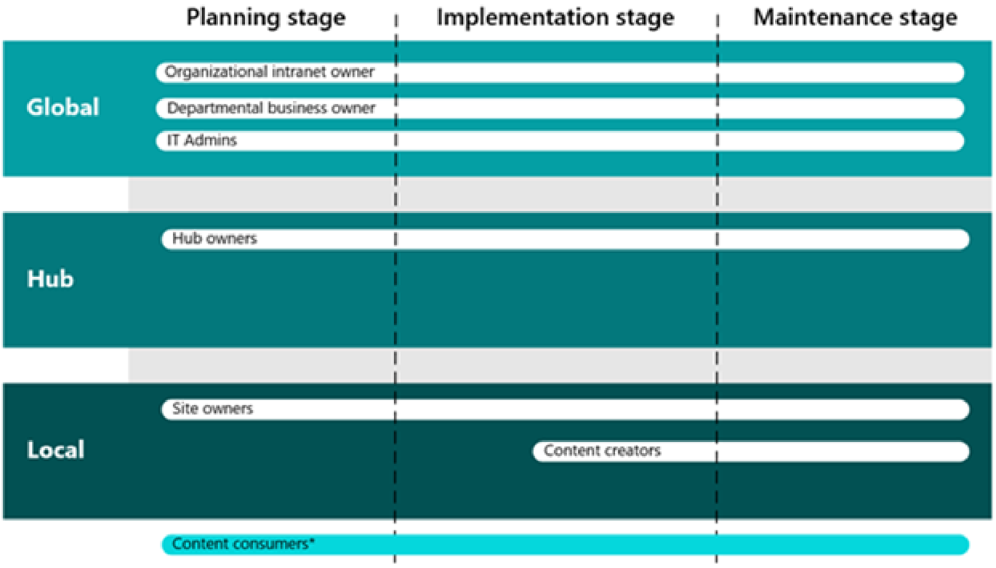
Information architecture covers 6 main elements that relate to way finding in SharePoint:

- **Global navigational structure** – Considered the top level of navigation across your SharePoint tenant and how you structure your sites so that users can find content including the home site of your intranet.
- **Hub structure and organization** – Hubs enable you to group together similar topics, tasks, and content.
- **Local site and page navigational structure** – How content is organized on each site and page so that users can further navigate or consume content effectively.
- **Metadata architecture** – Metadata impacts search and browsing structure as well as compliance and retention policies.
- **Search experiences** – How your users "consume" information architecture in addition to browsing.
- **Personalized content experiences** – How specific content is targeted to certain users and groups of users.

Designing the optimal structure for hubs, sites, and pages requires sufficient planning. It also requires knowledge of the domain, content, understanding the user experience, awareness of design approaches, and best practices in Microsoft SharePoint. Even with a good plan, information architecture is a continuous process. Over time, organizations change, people change, and projects change. Over time you will learn about your users, which will allow for adjustment that make content more discoverable.

Understand your role and how to collaborate

Information architecture for your organization will be the most effective by collaborating with many types of roles involved in your intranet such as: intranet owners, departmental business owners, IT administrators, and hub owners just to name a few. Learn more about how each role plays a part in planning, implementing, and managing ongoing maintenance for organizational information architecture.



Organization intranet owner(s) – The organizational intranet owner(s) consist of a mix of decision-makers and job functions to manage the overall direction and coordination of your organization's intranet. Organizational intranet owners work with business owners (departments) and IT admins to establish global and hub level navigation. Organizational intranet owners will spend most of their time working on planning and implementing global and hub level navigation.

Departmental business owners – Departmental business owners represent large areas of the organization, like human resources, marketing, and engineering. Departmental business owners work with organizational intranet owners to ensure their area of the business is well-represented in global and hub navigation. Organizational intranet owners should be included early in the planning stage to ensure business and user needs are met.

IT Admins – IT admins partner with organizational intranet owners and departmental business owners to implement high level navigational structure like implementing the start page and hubs. IT admins also help implement certain governance policies around site creation and usage. IT admins are involved in planning, implementing, and maintaining information architecture as the business changes and scales. Hub owners – Hub owners manage hub-level content, branding, permissions, and navigational elements for hub in your organization's intranet. Hub owners partner with departmental business owners and IT admins to plan, create, and manage hubs throughout the lifecycle of your organization's intranet architecture.

Site owners – Site owners manage site-level content, branding, permissions, and navigation. Depending on the needs of the business and users, site owners can associate their sites to hubs if the hub owner allows.

Content creators – Content creators are responsible for keeping site content updated and publishing news. Content creators should be given a site member permission level to make changes to sites and pages. Content creators partner with site owners during the implementation and management stages.

Content consumers – Content consumers are not represented in the counts as anyone who is using and viewing content throughout the three levels of navigation. Intranet owners, departmental business owners, hub owners, and site owners should regularly engage with content consumer – especially during the planning process – to ensure the right content is findable and usable.

Guiding principle: the world is flat

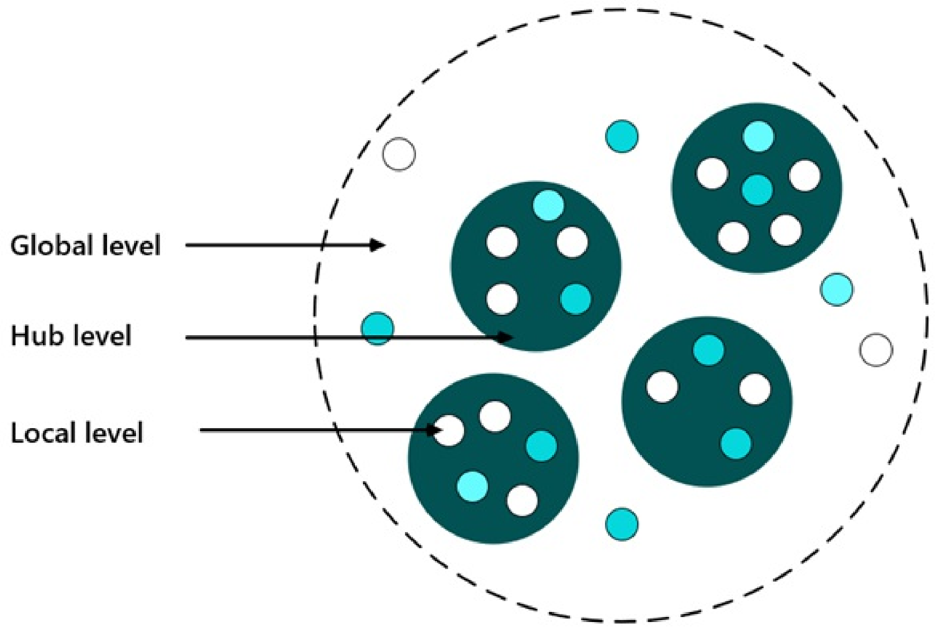
Classic SharePoint architecture is typically built using a hierarchical system of site collections and sub-sites, with inherited navigation, permissions, and site designs. Once built, this structure can be inflexible and difficult to maintain. In the modern SharePoint experience, sub-sites are not recommended. In the new "flat" world of modern SharePoint, plan to create one site for each discrete topic, task, or unit of work. This will allow you to easily distribute management and accountability for each content collection and support your ability to move sites around in your navigational architecture without breaking links. Moreover, when a topic is no longer needed, you can easily archive or delete a site with minimal impact.

In the new flat world, you have several ways to connect sites and content to each other as part of your information architecture toolkit:

- Use "roll up" web parts such as News, Highlighted content, or Sites to dynamically surface content from other sites in an existing site.
- Use inline hyperlinks to provide additional detail about a topic to provide more information to your reader (as demonstrated in the previous bullet).
- Add explicit links to related sites in your site navigation.
- Connect families of related sites using hubs.

Levels of navigation

There are three levels of navigation to think about for modern SharePoint experiences:



- Global navigation for the entire collection of sites that comprise your intranet
- Hub navigation for groups of related sites
- Local navigation of an individual site

Global navigation

Many intranets include top navigation that persists on every site. Global navigation allows you to create an overall navigation story for your intranet that visually connects all the sites, content, and tools your viewers need to get work done. Every organization has a different requirement for what goes in global navigation, but some of the category labels often used include concepts such as:

- Home
- About Us
- News
- Working Here/Work Resources/Administrative Services/Administration
- Operations/Operations Services
- Pay & Benefits
- Life & Career

- Locations
- Policies & Procedures/Tools & Resources/Safety & Security

The goal of global navigation is to support browsing to content, but since there is limited real estate available for global navigation links, global links generally point to major category navigation pages, sub-links, or a mega menu experience to provide enough "information scent" to help viewers navigate their way to the content they need. Because the context for global navigation must be broad, it is challenging to make the labels both comprehensive and useful. If you plan to implement global navigation, consider using one of the testing methods discussed earlier to make sure that your proposed navigation resonates with users.

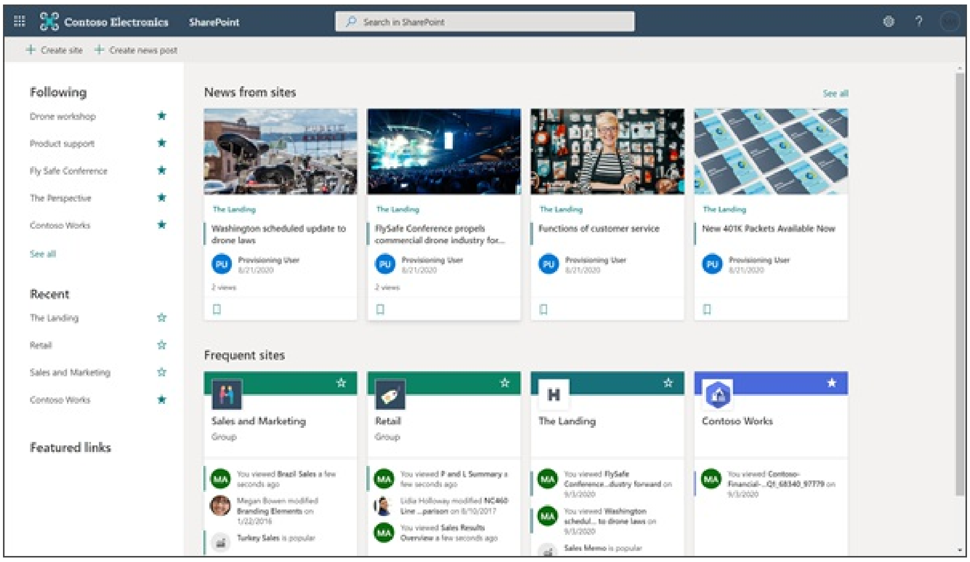
Global navigation is not yet available for modern SharePoint intranets. Until it is available, there are several ways to create a global navigation experience for your modern SharePoint intranet:

- Create a custom SharePoint Framework Extension to deliver and apply global navigation to each new site as it is created.
- Create a "navigation" site (for example, your intranet "home" site) and use the logo in the suite bar and a Featured Site link on the SharePoint start page to make it easy for people to navigate to the "home" site from every destination site in your tenant.
- Use a single hub for the entire organization. This might be a reasonable strategy for a small organization, but the benefits of hubs decrease in value if you only have one so this may not work for the long term.
- Wait to add global navigation until it is available natively in the product.

Where you'll see global navigation elements:

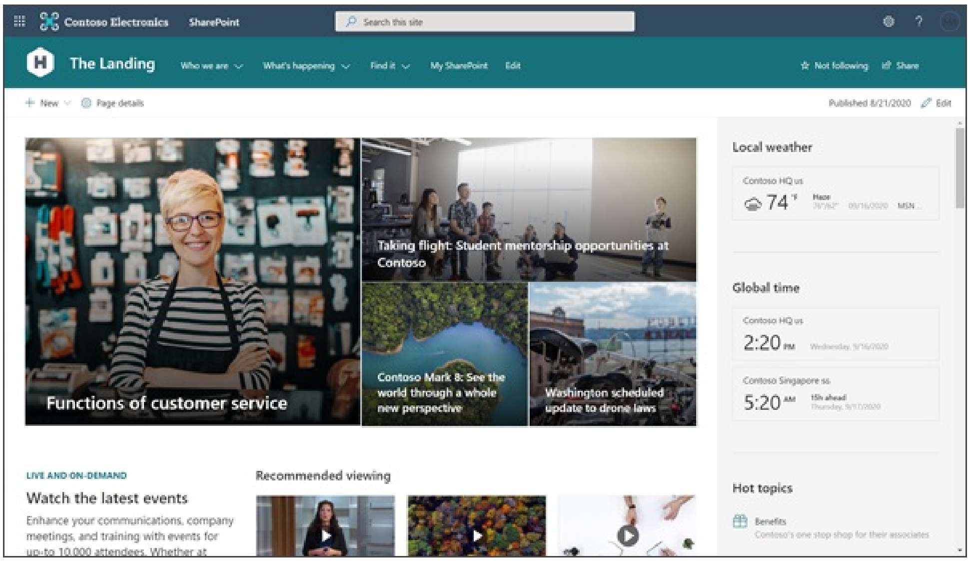
The start page

The SharePoint start page is where you can easily find and access SharePoint sites and portals within your organization. This is the first opportunity users will have to start discovering news, sites, and easily navigate to the top of your intranet by selecting the logo.



The home site

A home site is a SharePoint communication site that you create and set as the top landing page for all users in your intranet. It brings together news, events, embedded video and conversations, and other resources to deliver an engaging experience that reflects your organization's voice, priorities, and brand. This is a good place to display entry points to frequently accessed resources for human relations, information technology, departmental portals, and organizational news.

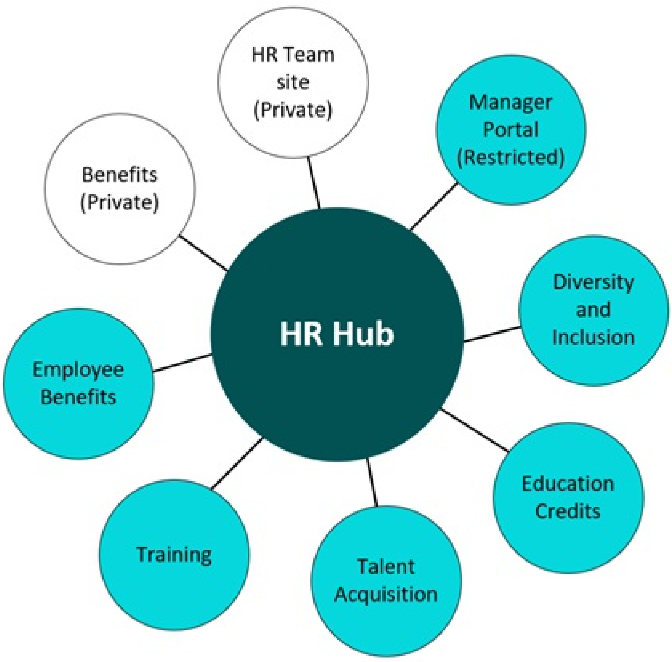


Hub navigation

The default navigation experiences available in classic SharePoint site hierarchies (sites with subsites) are not available in the "flat" world of modern SharePoint, where each unit of work or project or team gets its own site collection. Flat architectures are great for governance but can make it harder to implement navigation that connects multiple sites.

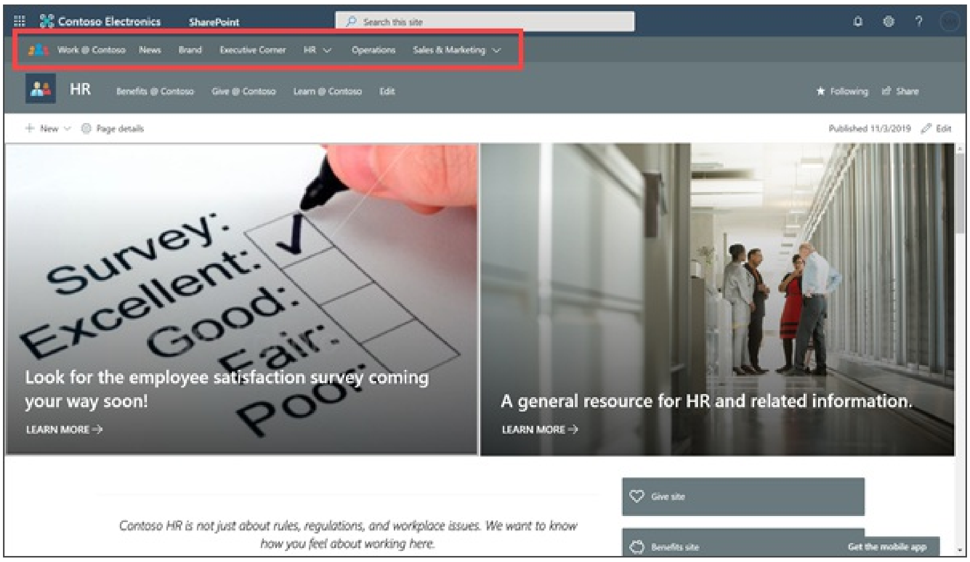
Hubs provide a great way to achieve the cross-site navigation features previously available in managed navigation and site hierarchies in classic SharePoint. One of the important planning decisions for hubs is planning the hub navigation.

Hub navigation appears above the local navigation on each site, just below the suite bar, as shown in the image earlier in this article. Hub navigation is established in the site that is declared to be the hub. It is defined by the hub owner and is shared by all the associated sites.



Where you'll see hub navigation elements:

SharePoint hubs help you meet the needs of your organization by connecting and organizing sites based on project, department, division, region, etc. making it easier to discover related content such as news and other site activities, apply common navigation, branding, site structure across associated sites and search across all associated sites.



A hub is a special capability that a SharePoint Administrator can add to a site that designates a site as the “head” of a family of related sites. Sites that are associated to the hub share navigation, branding, and other elements.

Each site can belong to only one hub at a time, but you can associate hubs together in a combination of navigation links and associated hubs as part of your navigation experience. Using hubs is far more flexible and adaptive to the changing needs of your organization. For more info, see Planning your SharePoint hubs.

Local navigation

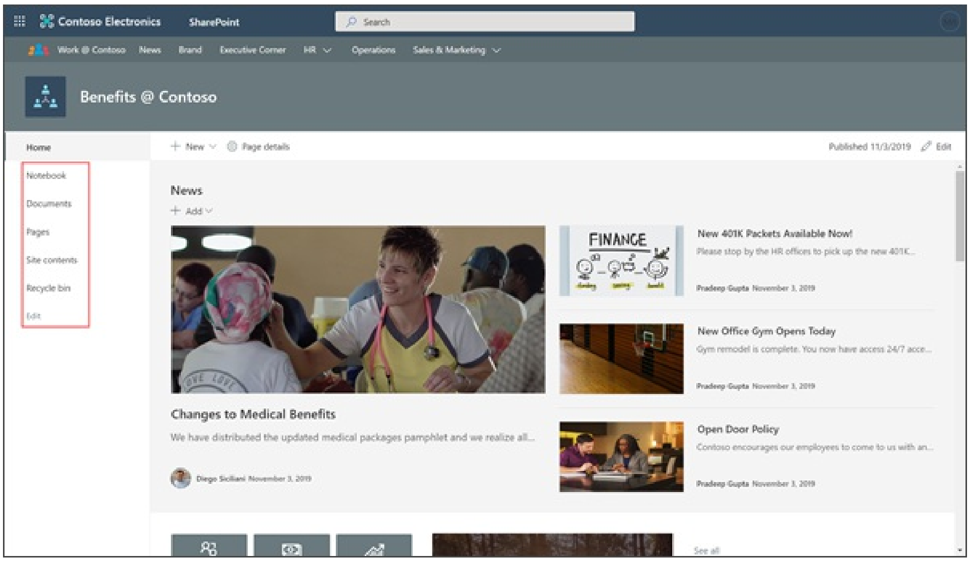
Local navigation is the static navigation that viewers see on every page of your site. For team sites, local navigation shows up on the left side of the page in the area referred to as the "quick launch". For communication sites, local navigation shows up at the top of the page. Local navigation is on every page in your site – so make sure it is relevant. Think about how viewers might explore your content and use local navigation to support that exploration.

Example: A travel site might have the following local navigation links that support viewers who are exploring the travel site from the perspective of "what am I allowed to do?" as well as viewers who are exploring the travel site from the perspective of the travel process – before, during, and after their trip.

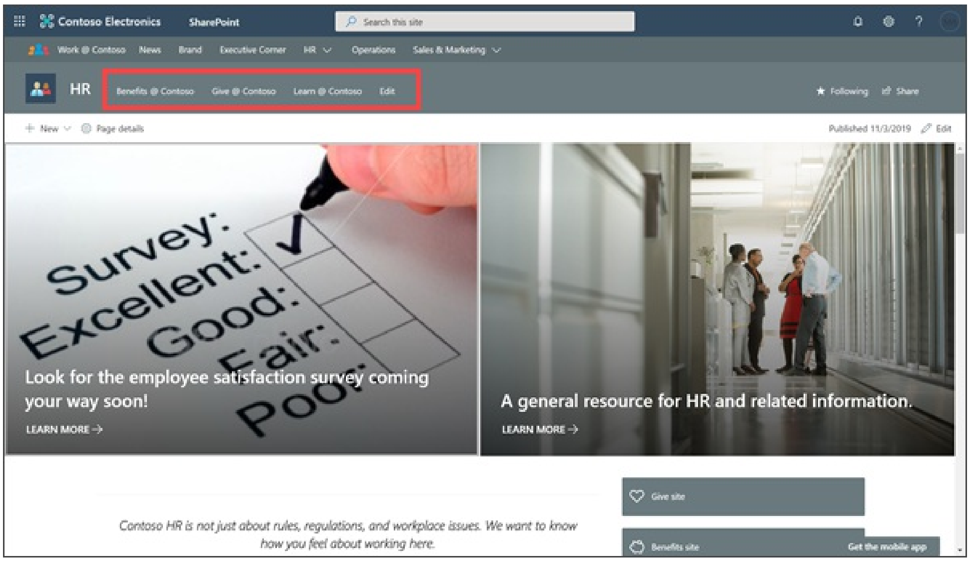
- Travel guidelines
  - Air
  - Car
  - Ground transportation
  - Hotel
  - Train
- Before you go
  - Travel approval
  - Booking service
- During your trip
  - Travel safety
  - Itinerary changes
- After you return
  - Expense reporting
  - Trip reports

Where you’ll see local navigation elements:

Team site navigation



Communication site navigation



Sites

Your intranet and portals will be comprised of team sites and communication sites that will provide further access into the site's pages, lists, and libraries. Every page in each site tells a story for the reader.

One component to modern SharePoint team sites that makes information architecture easier to implement and maintain are Microsoft 365 groups. M365 groups is a membership service that allows for easy hub and site permissions as well as additional functionality for SharePoint team sites and Microsoft Teams. With Microsoft 365 groups, you can give a group of people access to a collection of collaboration resources like Planner, OneNote, SharePoint team sites, and more. M365 groups can only be used on SharePoint team sites.

Pages

Pages within team or communication sites provide an opportunity to use dynamic web parts that automatically update content from other sites and pages like News, Highlighted content, or Sites web parts.

Your sites will generally include three types of pages:

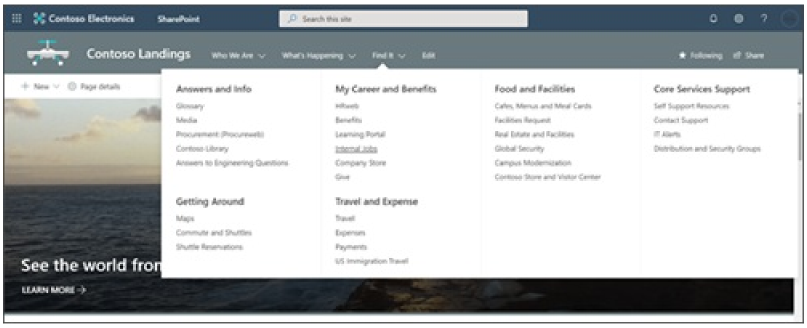
- The **home page** where you will provide an overview of your content and introduce the reader to what they will find on the site.
- Navigation pages that provide options or summary information for the reader and help them get to a decision point about where they want to go next.
- **Destination pages** that are the end point of the reader's journey. This is where you will present information

to read, print, or download. If you have a lot of information on your destination page or you want to provide supplemental explanations for detailed topics, you can create an ancillary page.

Since we know that most readers do not read every word on a web page or even scroll to the bottom, you need to pay attention to how you present information on each page. Make sure that you put the most important information – the information that your readers must have for your communication to be successful – at the top of the page. As the page continues, you can add additional information that is helpful, but not crucial. Think of this as writing with your summary or conclusion up front, instead of at the end. Use sections, headings, and bullets to make your pages easier to read. For more info, see Add sections and columns on SharePoint modern page.

Navigational elements

Navigational elements are menu styles like the mega menu, cascade menu, and footer menus. Secondary navigational elements include inline links and buttons.



Personalization elements

Audience targeting - Audience targeting helps the most relevant content get to the right audiences. By enabling audience targeting, specific content will be prioritized to specific audiences through SharePoint web parts, page libraries, and navigational links.

Information barriers - Information barriers are policies in Microsoft 365 that a compliance admin can configure to prevent users from communicating and collaborating with each other. This is useful if, for example, one division is handling information that shouldn't be shared with specific other divisions, or a division needs to be prevented, or isolated, from collaborating with all users outside of the division. Information barriers are often used in highly regulated industries and those with compliance requirements, such as finance, legal, and government.

Multilingual considerations - If your organization spans a diverse population, you may want to make content in your intranet sites available in multiple languages. User interface elements like site navigation, site title, and site description can be shown in the user's preferred language. Additionally, you can provide pages and news posts on communication sites that you translate and that are shown in the user's preferred language.

To show the site name, navigation, and footer of your site in the different languages you've made available, each must be translated manually. For example, let's say you've created a communication site with an English default language, and you've enabled the site for Spanish and German languages. When you create a site, you set up the site name and description in the default language (in this case, English). You can also update the site name and description after site creation. Then you create the navigation nodes and footer content in English.

After the site is set up in English, a user with Spanish as their preferred personal language manually edits and translates the title, description, navigation and footer content into Spanish. A user with German as their preferred personal language does the same for German. Once the content is translated, it will display for all users of those preferred languages.

Metadata architecture

Columns and content types are the two most important metadata elements that you can use to organize documents and pages in your SharePoint site. Metadata helps your users filter and sort content within a list or library – but also helps with search. Use columns in your Site Pages library as well so that you can use highlighted content web parts to dynamically connect related pages based on shared metadata.

Folders are another way to organize document content, but folders are a physical construct with limited flexibility. Folders are not necessarily bad – they can help you manage performance and security in your document libraries – but folder structures with more than one or two levels of nesting create a significant discoverability burden for users and should be avoided. Every site comes with one document library – but you are not limited to just one library. Instead of using the one default Documents library on your intranet sites, consider adding topic-specific libraries and add site columns to organize your content within the libraries to avoid creating multiple levels of nested folders.

Search experiences

Search leverages your information architecture investments to help users find content when they don't know where it might be in your architecture. It also helps users discover content that they may not have known about.

You can help users discover content and improve search outcomes by leveraging several features in search, including acronyms, bookmarks, Q&A, floor plans, and locations. For more info, see Make content easy to find and Search experiences in SharePoint.

Next: learn about SharePoint information architecture principals

Information architecture in modern SharePoint

1/8/2021 • 8 minutes to read • Edit Online

The most effective SharePoint sites help viewers find what they need quickly so that they can use the information they need to make decisions, learn about what is going on, access frequently used tools, and engage with colleagues to help solve specific problems.

Even when search is available, most viewers start their web experiences by browsing. That pattern persists on internal web sites as well. Good navigation experiences present viewers with a complete picture of what is available, and combined with the home page, provide a comprehensive "story."

In this article:

- Understand basic information architecture principals
- Learn more about how to write effective labels and links
- See how to ensure frequently used tools and content are findable

Information architecture goals

Navigation should always be planned from the perspective of the user. Planning effective navigation involves considering not just the information you want to present, but also thinking about the information your viewers want or need to consume. Therefore, organizing and labeling your navigation links is critical for the purposes of usability and findability.

Successful intranet and site navigation experiences enable users to:

- **Find information** – Users need to find documents, files, and links most relevant to the work they do without spending time sifting through content. Make sure to present only the most relevant and high-priority information first.
- **Take action** – Users typically have a specific task in mind when they visit a site. Make sure common tasks are built-in to navigational structure as labels and links so that they can be easily identified and accessed.
- **Understand company structure** – When viewed at-a-glance, users should be able to get a sense for how to organization is structured. Make sure you incorporate hierarchy and structure into site and intranet navigation.

Get organized

There is no one right way to organize your navigation links. You will make different choices based on the type of site you are creating and your viewers. Organizing concepts might include:

- Services
- Products
- Activities
- Audiences (if your viewers can clearly identify the audience to which they belong – such as student or teacher)
- Expertise areas or functions

As you organize user needs and business needs, consider the following:

- **How can information architecture reduce the cognitive load for your viewers?** - Cognitive load is the amount of information that a person can process at any given time. Managing the user's cognitive load helps prevent information overload and time wasted finding resources. Ensure you understand your viewers needs prior to implementing information architecture.

- **What is the current mental model of your users?** - Mental models are the existing models people use while interacting with a website or application. Information is easier to discover when it is in a place that matches the user's mental model of where it should be.
- **How can information architecture help users make better and more efficient decisions?** - Decision making can be incredibly taxing. Information architects can help us make decisions by providing certain information at key moments.

The default navigation for all SharePoint sites primarily includes type of content. For communication sites, the default navigation includes Documents, Pages, and Site Contents. These categories are helpful as you are building your site, but they are not typically going to add value to your viewers once your site is ready to launch. This is because the consumer of a communication site typically doesn't care about the type of content – they care about the purpose or subject of the content. For communication sites, plan to delete the "out of the box" navigation when you are ready to launch and replace it with something that aligns with the guidance provided in the local navigation section of this guide.

The default navigation for team sites includes links to the related services provided by Microsoft 365 for modern teams – including a link to the shared team notebook and the conversations for the team in Outlook. These represent the typical features that teams need to effectively collaborate and might be hard for people to find without the experience provided by the navigation. You may choose to supplement or refine these links for your team sites, but you will also likely find that the default navigation experience is a good starting point. You may be more likely to keep most of these links than you would with a communication site.

Prioritize usability and findability

The key goal when we plan navigation is to make our sites useable and our content findable. The best way to ensure that your navigation meets these goals is to test it. There are several cost-effective approaches that you can use to ensure that your navigation design is effective, including:

- **Card Sorting** - Primarily helpful for planning navigation.
- **Tree Testing** - Helpful for testing suggested navigation paths.
- **Usability Testing** - Task-based scenarios that are helpful for comprehensive testing of site and page navigation.

These two resources provide an overview of techniques and tools for testing the usability and findability of your navigational strategy:

- Usability Analysis
- Overview of Testing Approaches

Write clear and intuitive labels

The words you use for navigation matter – not just because the real estate for navigation is limited – but also because your labels are what guide your viewers to the content. Each label makes a promise: if you select this link, you should get the information you expect to find.

To ensure that your labels keep their promises, make sure they are:

- **Specific** - Tell the viewer exactly what they will find when they select the link. If the target for your link includes Policies and Procedures, make sure the label includes both terms.
- **Comprehensive** - Describe content with your collection of labels. You should not plan to link to every single page or document in your navigation, but your navigation should provide a complete picture of the content on your site.

- **Concise** - Keep your labels short and to the point.
- **Familiar** - Don't make up terms in your labels. Keep your viewers in mind – if you use an unfamiliar term, your viewers will be confused and unable to find what they need.
- **Front-loaded** - Make sure that your labels are "scannable." For example, Company Information is better than Information About our Company.
- **Clear** - As much as possible, you want your navigation labels to be mutually exclusive – at least for the major categories. It is perfectly fine to have a sub-link display in multiple categories – especially if viewers might expect to find it in more than one place – but the major categories need to be easily distinguished from one another.
- **Targeted** - It's not a good idea to show people links to private sites that they don't have access to. Where appropriate, use the audience targeting features for SharePoint to target navigation links to viewers for whom the link will work. Note that there are exceptions to this guideline. For example, you may want to use your navigation to help people discover sites that they may not have access to today but could be approved to join. If you do provide links in navigation to private sites, be sure that the owner of the site knows that they may be getting a lot of access requests!

Think about link target interactions

Many usability guidelines recommend limiting the number of new windows that are automatically opened for site viewers. Most of the time, opening a link in the same window allows site viewers to use the back button when they want to return to your site. When a viewer wants to open a link in a new window, the guidelines recommend that the viewer be allowed to choose this outcome by "right clicking" the link. An exception to this guideline is the recommendation to always open documents in a new window to prevent users from accidentally closing the browser window when they close the document.

By default, navigation links on modern SharePoint sites open to a link that points to:

- **A page or site in the same tenant** (same site or another site) - Links open in the same tab.
- **A document** (same site or different site) - Links open in a new tab.
- **An external site or document** (internet site) - Links open in a new tab.

In classic SharePoint sites with publishing features, you can choose to open navigation links in a new window. This allows you to consider the context for your site viewers and determine whether it might be helpful to open a link in a new window. There is no way to select how navigation links open in modern SharePoint sites. This means that your navigation links will follow the default guidelines, but you still need to be especially careful about the labels for navigation links to make sure that your viewers know that they are leaving the site when they select the link.

Make sure that the navigation label accurately describes the destination – a place on a completely different site or an application – and if you know that the back button may not work, consider using an alternative way to present the link, such as the text web part where you can elect to open a link in a new window.

At the current time, only the Text web part lets you create a hyperlink and choose how the link opens. When you add a hyperlink to text, you have the option to choose to open the link in a new tab.

Test usability and findability with real users

Once you have established a basic working structure for global, hub, or local level navigation experiences, you should test your design with real-life users. Create tasks and ask users to complete the tasks. Ask users to "think out loud" as they are looking for information and resources. Note where improvements to can be made and then implement and test the changes again. Plan to review basic global, hub, and local navigation experiences as your business changes and grows.

Learn more about navigation basics like how to write effective labels, how to test findability, and how to use menu styles.

Next: learn about SharePoint information architecture models and examples

Information architecture models and examples

1/8/2021 • 8 minutes to read • Edit Online

Navigation design accounts for the visual way of finding components (menus, links, sites, and pages) that help users understand how to interact with SharePoint sites and portals and what types of information is available. Options for implementing navigation differ based on the framework for your sites and intranet.

In this article:

- Learn about information architecture elements
- Explore common information architecture models and scenarios
- Use the models and scenarios as a starting point for navigational design

Information architecture modeling elements

Information architecture elements are secondary components to navigation design that compliment building blocks. The following components should be considered when selecting, planning, and implementing navigational design for global, hub, or local navigation.

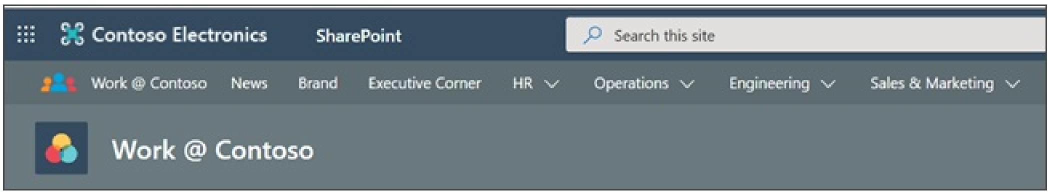
- **Site hierarchy** – Use hubs and visual layouts to establish visual hierarchy
- **Security** – Data governance, administration and editing privileges
- **Taxonomy** – Record management, compliance requirements

Common models for navigation design

The way you organize sites and content will depend on the composition of your organization and the needs and goals of your users. For example, if your goal is to enable front-line workers with specific sites and documents, you may decide to optimize navigation for a mobile device. Another example, if your goal is to create a collaboration space for your team, you may decide to design your SharePoint team site to align with Microsoft Teams.

Common methods of organizing navigational design:

By department

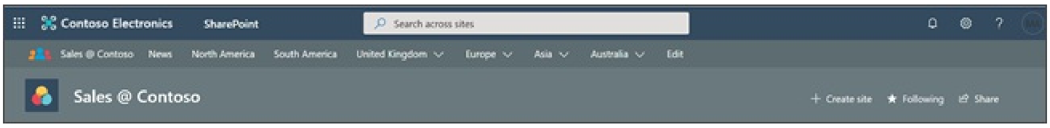


Benefits - Most users already have a well-established mental model for navigation broken down by department. This model scales many sizes and types of organizations and is a common method for organizing and planning hubs.

Governance considerations - For large organizations, especially with international offices, it can be challenging to make sure the right people have access to the right content for security and compliance purposes. Consider using personalization elements like information barriers and audience targeting to help surface content the specific audiences.

Maintenance considerations - As the business grows and departments and team move, you will need to update global, hub, and local navigation to reflect organizational changes.

By geographic location



Benefits - Organizing by geographic location is an effective way to bring people of similar disciplines together to collaborate and build community. For large or organizations, and international organizations, location can be an important decision-making factor for users. Organizing by region may be important when certain topics have different laws and mandates depending on the region. For example, crisis management sites or human resource guidelines.

Governance considerations - Many governance details may very among region, for example site creation policy, data retention, and data storage policies too. Learn more about the multi-geo user experience and multi-geo configuration.

Maintenance considerations - When the organization moves locations, navigation will need to be updated to reflect those changes. There are other multi-geo considerations to plan when enabling SharePoint, Microsoft 365 groups, and other Microsoft 365 apps globally. Multi-geo enables global businesses to control the country or region where shared resources like SharePoint Team Sites, Office 365 Groups content (associated SharePoint Sites and shared mailboxes) are stored and managed.

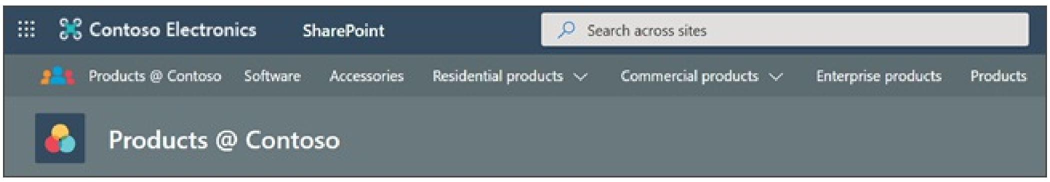
By task or scenario

Benefits - Organizing by scenario within navigation helps users learn about a general concept, for example "about us" pages. Organizing by common and frequently used tasks is helpful in the same way, for example tasks like "get reimbursed" or "pick a healthcare plan."

Governance considerations - This style of navigation could attract a broad and high-volume audience depending on the rest of your navigation design. High volume sites should take extra care in ensuring page performance is managed by optimizing image sizes and other details. Consider using tactics like creating hubs to organize tasks by departmental needs, which will make it easier to manage page access and organization.

Maintenance considerations - When organizational information (leadership, locations, etc.) becomes outdated, navigation will need to be updated.

By portfolio



Benefits - Sometimes content is best organized by type, or portfolio, to display content in natural groupings or for specific audiences. Organizing your navigation by portfolio offers flexibility as your business scales and grows.

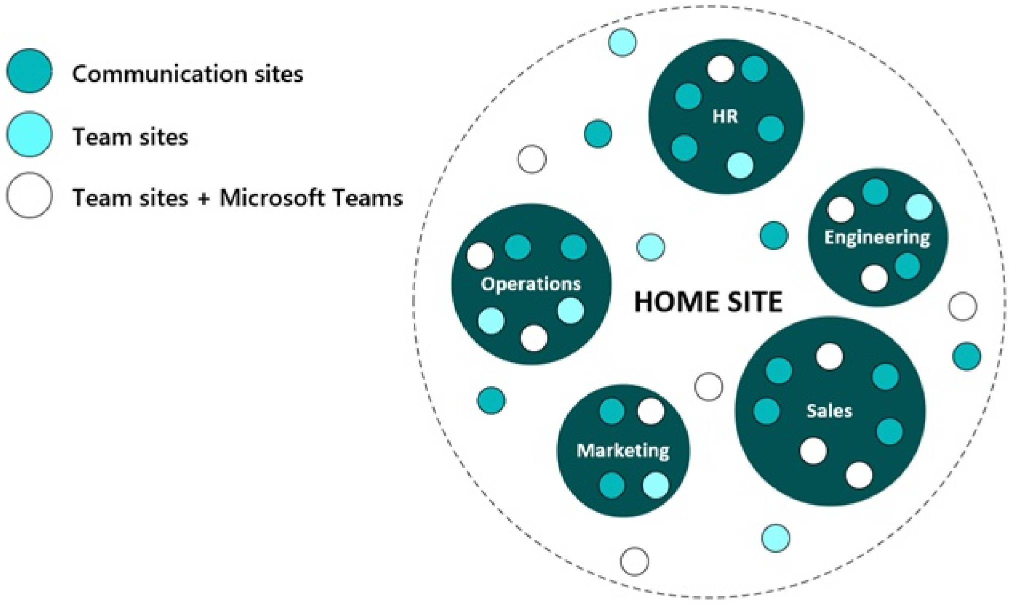
Governance considerations - For large organizations, especially with international offices, it can be challenging to make sure the right people have access to the right content for security and compliance purposes. Consider using personalization elements like information barriers and audience targeting to help surface content the specific audiences.

Maintenance considerations - As the business and portfolios grow, the navigation needs to reflect organizational changes.

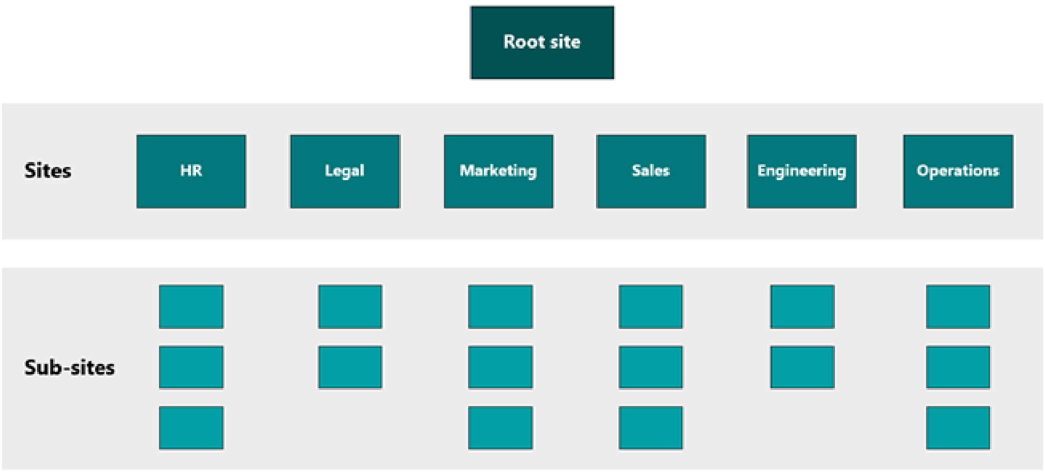
Scenarios

Scenario 1: Move to modern navigation from classic navigation

Modern navigation



Classic navigation



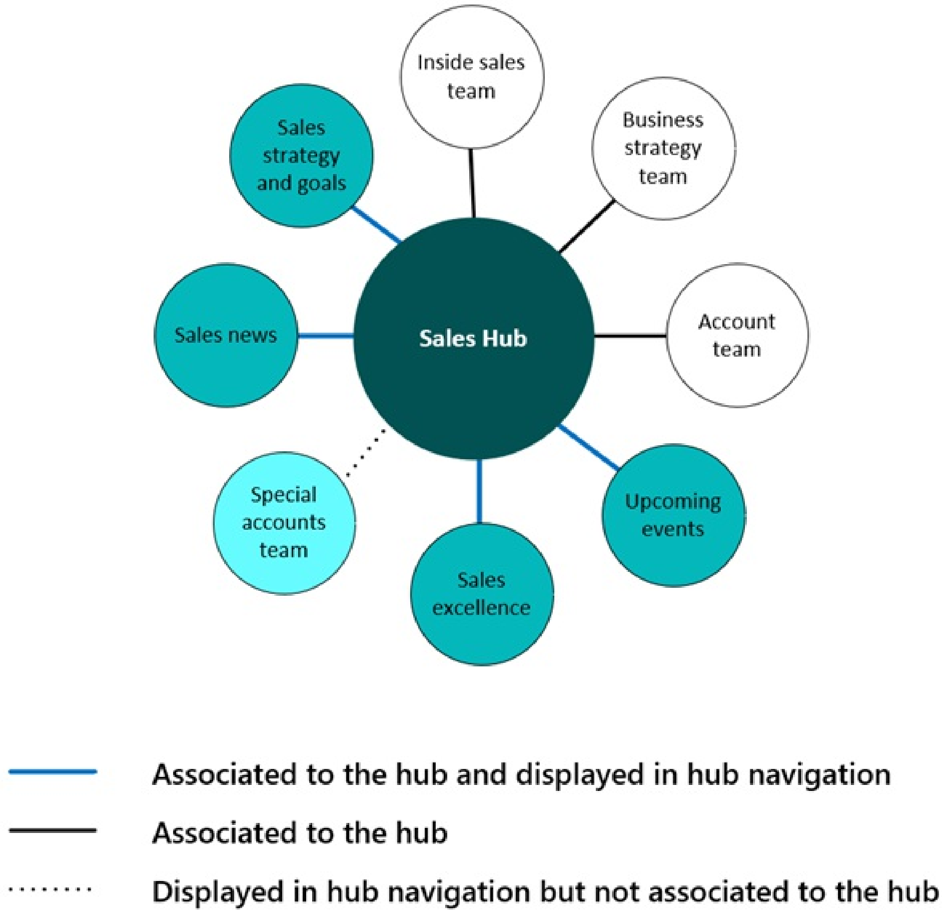
Your intranet is an ever-evolving component of your business that will need to grow and scale alongside your organization. Modern intranet navigation differs from classic navigation in the sense that it is “flat” -- in the modern SharePoint experience, sub-sites are not recommended. In the new “flat” world of modern SharePoint, plan to create one site for each discrete topic or unit of work. Classic SharePoint architecture is typically built using a hierarchical system of site collections and sub-sites, with inherited navigation, permissions, and site designs. Once built, this structure can be inflexible and difficult to maintain.

Focus on incorporating modern changes that will have the greatest impact to your business first. Plan and schedule when changes will be incorporated and how you will track progress. Use site analytics to understand user behavior and collect feedback from users along the way. How to get started

Moving to modern navigation from classic SharePoint navigation is a process that depends on the size of your organization and the complexity of your tenant’s configuration. Below are general guidelines and tools you can use to get started:

- Define new intranet business objectives and choose pilot scenarios
- Learn about user needs and find methods to test potential designs
- Take an inventory of your current sites and subsites
- Start planning hubs and your home site by grouping high priority tasks and content
- Release hubs and associated sites in phases
- Regularly review hub and site analytics to track page traffic and popular content
- Make navigation changes based on your learning from user testing and analytics

Scenario 2: Consider modern hub navigation configuration



These are special considerations for planning hub navigation. A site can be:

- In the hub navigation and be associated to the hub
- Associated to a hub and not be in the hub navigation
- In the hub navigation and not associated to the hub

Example 1 - Site is in the hub navigation and associated to the hub

Showcasing sites associated to the hub allows viewers to discover the sites within the hub family and easily navigate among and across the “family members.” Adding an associated site to the hub navigation displays the organizational framework for the collection of sites in the hub navigation. All sites in the hub share a common theme and navigation helps to establish the identity of the hub family both visually and via viewer interaction. Your hub links can go to sites or content pages or a combination of both – but use the practices described for link labeling to ensure that you are providing clear and consistent experiences.

When you choose to show all associated sites (and associate hubs) in the hub navigation, think about whether all the people who have access to the hub will also have access to each of the sites associated to the hub. For example, if you add links to private sites in the navigation, you are increasing their "discoverability," which can be a good thing – if the site owners for those private sites are prepared to get access requests. However, you may not want to show restricted sites in the navigation if the site owner does not want the site or the content to be discovered.

To ensure that your hub navigation links keep their promises, consider the following options:

- For links that should not be discoverable to all viewers, target the link so that it only shows up for audiences who have access to the content.
- For "discoverable" but restricted links, consider adding the word restricted, or request access, or private to the label. Have a conversation with those site owners to make sure that they are prepared for potentially more frequent access requests. In addition, you could consider adding the “lock” emoji to your private or restricted sites.

Example 2 - Site is associated to the hub and not shown in the hub navigation

If the use case for your hub is primarily about sharing a common theme or for rolling up content for people who are members of private sites, you may want to associate a site to a hub but not showcase the site in the shared hub navigation. One reason that this might be OK is that the members of the private sites already know about the sites and don't need the hub to provide links to the site. However, these same site members would find it useful to see the news and activity rolled up from their private sites on the hub (via the Highlighted Content and News web parts.

Another reason not to show associated sites is that the owners of one or more private sites do not want the sites to be discovered in the hub navigation or they are not prepared to manage unexpected access requests.

Example 3 - Site is added to hub navigation but not associated to the hub

One of the nice features of hub navigation is that it allows you to plan a shared navigation experience for all the sites associated to the hub – including links to frequently needed sites that are not part of the hub.

If a site is associated to a hub, it is reflected in the hub navigation. You may not want all sites that are related to the hub "family" to be associated to the hub. For example, consider a scenario when you are collaborating with external partners on a team site. You may not want to associate external sites to your hub because you may not want to display the shared navigation for the hub to external partners. But, you may want to add links to the external sites to the hub navigation to make it easier for internal viewers to discover these related external sites.

This presents a convenient way to showcase links to all the external sites managed by the business group without having to worry about exposing navigation links to external viewers. When internal viewers navigate to the external sites, they will no longer see the hub context and theme – but this is the desired outcome.

A site can only be associated to one hub. However, you can increase discovery by adding navigational links to other hubs or other sites in your hub navigation.

Next: learn how to get started planning and implementing SharePoint navigational design

Get started planning and implementing SharePoint navigation design

1/8/2021 • 3 minutes to read • Edit Online

To begin, understand that no two organizations will build identical architecture structures in SharePoint. This is because your architecture design stems from the unique needs of your organization and users. Also, remember that architectural structure will change over time as you learn more about user needs and as the business scales and grows.

Similar to SharePoint intranet content, SharePoint architecture should be reviewed and revised as often as needed to ensure users have easy access to relevant content and resources.

In this article:

- Explore how to understand users' needs, content requirements, and scope
- Learn how to think about planning, implementing, and managing global, hub, and local navigation

First: Understand your users

The most important step in planning an effective information architecture is understanding your users:

- Who are your users? What key roles do they have?
- What vocabulary to they have? What terms do they use to look for content?
- What do they want to learn?
- What do they want to do? What are their top tasks?

Next: Understand your content

In addition to understanding your users and their experiences, you also need to understand your content. Think about how content is distributed across current intranet sites, libraries, and folders. Look at usage data to understand what content is accessed most and least frequently.

Think about the categories of information in your organization, such as services, products, areas of expertise, and functions. Don't just think about the organization chart. Think about the information people need in their daily work and the key business outcomes you want to achieve. Use this information, and your knowledge of your users, to organize groups of related information, such as key business processes, major projects or initiatives, key business roles, frequent tasks, services, as well as organizational units.

Then: Understand your scope

Information architecture includes five primary elements:

- **Portal navigational structure** – How you structure your sites so that users can find content including the home site of your intranet.
- **Hub structure and organization** – How you group together similar topics, tasks, and content.
- **Site and page architecture** – How content is organized on each site and page so that users can further navigate or consume content effectively.
- **Metadata architecture** – How to structure and label your individual content items for browsing and searching as well as compliance and retention.
- **Search experiences** – How your users "consume" information architecture in addition to browsing.

Finally: Decide which navigational model works and start to plan and implement

New navigational design for a site:

> **NOTE**
>
> To edit site navigation, you must be a site owner.

PLAN	BUILD	MANAGE
1. Ensure you understand your users needs and the site goals 2. Learn about designing for local navigation	1. Customize the navigation of your site 2. Consider joining a hub site to increase viewership 3. Target navigational links to specific audiences	1. Use site analytics to understand how users are engaging with your site 2. Review site navigation as needed to ensure all links are active, relevant, and up to date

New navigational design for a hub:

> **NOTE**
>
> To edit hub navigation, you must be the hub owner or tenant administrator.

PLAN	BUILD	MANAGE
1. Ensure you understand your users needs and the site goals 2. Learn about designing for global navigation 3. Consider using a hub site to group similar sites together 4. Learn about multi-lingual considerations	1. Decide on a menu style 2. Customize the navigation for individual sites 3. Set up associations and permissions for hub sites	1. Use hub analytics to understand how users are engaging with your site 2. Review site navigation as needed to ensure all links are active, relevant, and up to date

New navigational design for an intranet site:

> **NOTE**
>
> To edit intranet site navigation, you must be the hub owner or tenant administrator.

PLAN	BUILD	MANAGE
1. Define new intranet business objectives and choose pilot scenarios 2. Learn about user needs and find methods to test potential designs 3. Take an inventory of your current sites and subsites 4. Plan the home site	1. Start planning hubs and your home site by grouping high priority tasks and content 2. Set up associations and permissions for hub sites 3. Release hubs and associated sites in phases	1. Establish an intranet review team that ensures navigation and content are up to date and aligned with your organization 2. Regularly review hub and site analytics to track page traffic and popular content 3. Make navigation changes based on your learning from user testing and analytics

Next: learn how to get started planning and implementing SharePoint site navigation

Plan and implement SharePoint site navigation

1/8/2021 • 9 minutes to read • Edit Online

The fundamental principles and practices for site and page navigation apply to classic and modern SharePoint architectures. However, your options for implementing navigation differs based on the framework for your sites and intranet. For example, the default navigation experiences available in classic SharePoint site hierarchies - sites with subsites - are not available in the modern experience.

Instead, hubs provide a great way to achieve the cross-site navigation features previously available in managed navigation and site hierarchies in classic SharePoint. No matter which framework you are using, you can use the guidance in this document to help you create the right navigation for your organization.

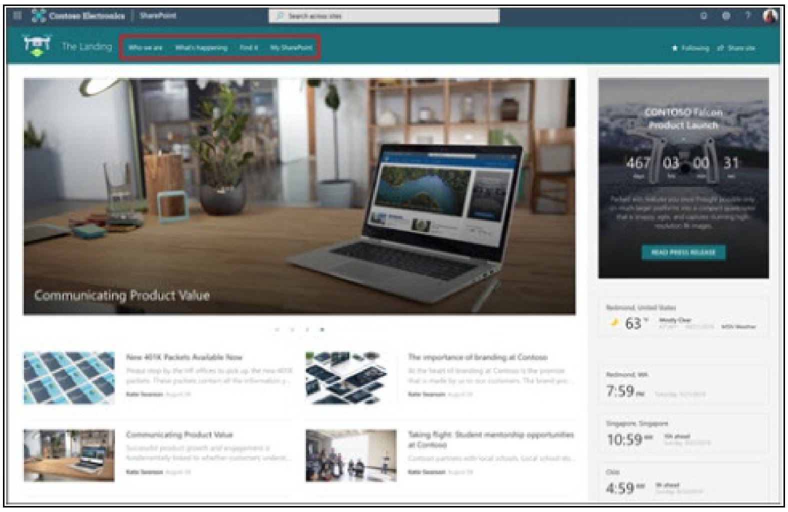
In this article:

- Explore considerations and best practices for site and page navigation design
- Learn about site navigation best practices
- Learn about menu styles and experiences

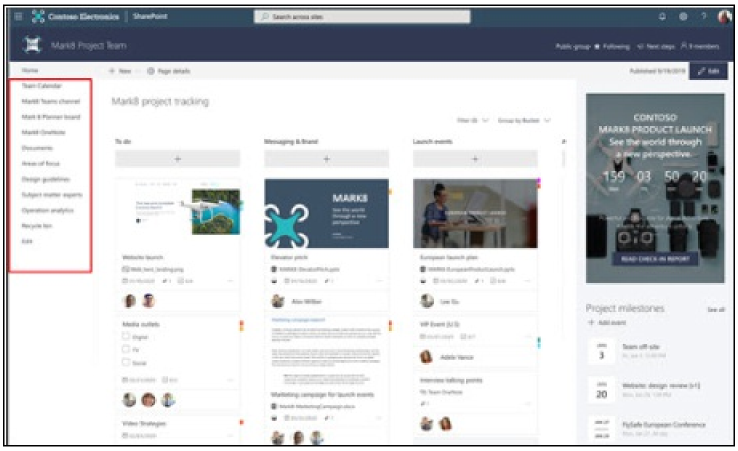
SharePoint site navigation

This planning guide primarily addresses *site* navigation: the top (communication site and hubs) and left (team site) navigation experiences.

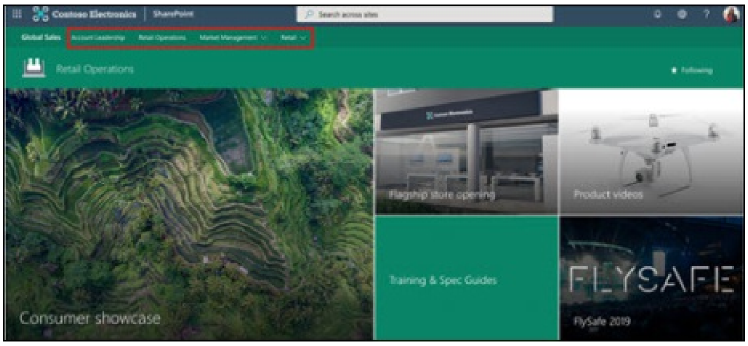
Communication site navigation



Team site navigation



Hub navigation



"When we're observing customers carrying out tasks on websites we notice certain common patterns. For example, we find that when people arrive at a particular site they start by ***navigating about 70% of the time****. When people get stuck navigating they may resort to using site search."* -- Gerry McGovern

Why navigation is important

The most effective SharePoint sites help viewers find what they need quickly so that they can use the information they to make decisions, learn about what is going on, access the tools they need, or engage with colleagues to help solve a problem.

Even when search is available, most viewers start their web experiences by browsing. That pattern persists on internal web sites as well. Good navigation experiences present viewers with a complete picture of what is available on the site and, combined with the home page, provide a comprehensive "story" for the site.

Page navigation and site navigation display differently. The links that you see in site navigation are static on every page in the site. The navigation links on individual pages are accessed only when the viewer lands on the page. A benefit to on-page links is that they can be different from page to page. Both types of navigational links guide your viewers by providing *wayfinding* experiences.

The key advantage of site navigation links is that they are always visible in the context of the site. Because site navigation links are persistent, they provide an opportunity to provide significant value for site viewers as they traverse the site and address their goals: to find and do what they came for. Hub navigation links extend this wayfinding experience to other sites in the hub “family.” This supports navigating to related content not just on the site, but on related sites as well.

Site and page navigation fundamentals

Planning site and page navigation involves thinking about:

- **Organizing** – Grouping logical and similar intents
- **Labeling** – Writing clear labels your users will immediately understand

- **Usability** – Users' ability to easily navigate the end to end experience
- **Findability** – Users' ability to quickly find what they need

Navigation should always be planned from the perspective of the user of information – the viewers to your site. Planning effective navigation involves considering not just the information you want to *present*, but also thinking about the information your viewers want or need to *consume*.

Therefore, organizing and labeling your navigation links is critical for the purposes of usability and findability. If 70% of viewers come to your sites expecting to browse for information, the usability of your site depends on creating a great browsing experience. To learn more, see Information architecture principals in SharePoint

Organizing

There is no one right way to organize your navigation links. You will make different choices based on the type of site you are creating and your viewers. Organizing concepts might include:

- Services
- Products
- Activities
- Audiences (if your viewers can clearly identify the audience to which they belong – such as student or teacher)
- Expertise areas or functions

The default navigation for all SharePoint sites primarily includes *type* of content. For **communication sites**, the default navigation includes Documents, Pages, and Site Contents. These categories are helpful as you are building your site, but they are not typically going to add value to your viewers once your site is ready to launch.

This is because the consumer of a communication site typically doesn't care about the *type* of content – they care about the *purpose* or *subject* of the content. For communication sites, plan to delete the "out of the box" navigation when you are ready to launch and replace it with something that aligns with the guidance provided in the local navigation section of this guide.

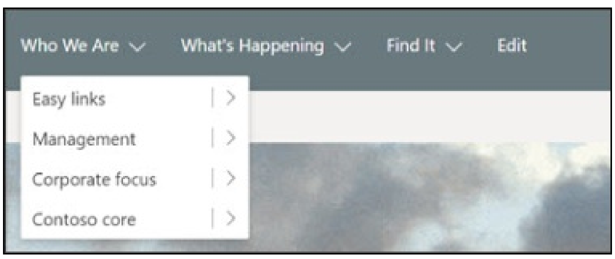
The default navigation for **team sites** includes links to the related services provided by Microsoft 365 for modern teams – including a link to the shared team notebook and the conversations for the team in Outlook. These represent the typical features that teams need to effectively collaborate and might be hard for people to find without the experience provided by the navigation.

You may choose to supplement or refine these links for your team sites, but you will also likely find that the default navigation experience is a good starting point. You may be more likely to keep most of these links than you would with a communication site.

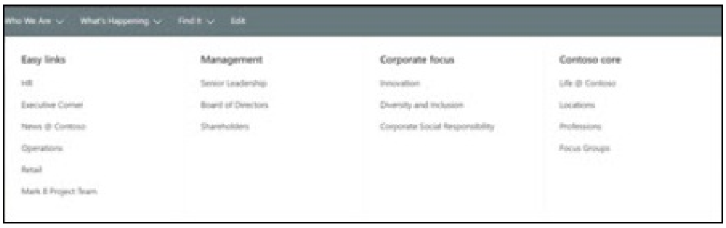
Navigation menus in SharePoint

There are two types of navigation menu styles for SharePoint sites - cascading and mega menu. Team sites only support the cascading menu style but communication sites support both mega menus and cascading menus. Hubs, whether they are team sites or communication sites, add an additional mega menu to the site. Mega menus are not available in on premises sites. Learn about how to customize the navigation on your SharePoint site.

Cascading menu



Mega menu



Menu links

There are two types of navigation links: a label and a link. A label is simply a category link – it lets you group related links but is not a link itself. A link requires a hyperlink and presents a “clickable” experience for the user. A label should always have at least one link below.

Both cascading and mega menus support up to three levels of navigation in your menu. The first level represents the tabs you see across the top. The second level is the next level below the tab and the third level is indented or below the second level. Mega menus work best when you are using all three levels of navigation experiences. If you use a mega menu, the second level of links will appear in **bold**. If you only need two levels in your menu, consider using the cascading style.

Menu experiences

There are two types navigation experiences – targeted and not targeted. With targeted navigation, you can choose who sees navigation links to create more personal navigation experiences. With non-targeted links, all users see the link, even if they don’t have access to the target location. Learn about how to target navigation links in menus.

Menu symbols

All types of menu links support some decoration with emojis. Emojis can be used at the beginning or end of a link label to add some visual interest to your links.

Choose an emoji that relates to the label topic. You can search for emojis at emojipedia.org, or use the Windows key plus a period (.). Copy the emoji and add it to the label when you are editing your navigation.

Link to pages, not individual documents

Document links open in a new window, which is helpful if someone wants to close the document after reading, but document links take viewers to a new context. In some cases, this may be the experience you want. But when navigation points to a page with an embedded document instead of directly to a document, you have an opportunity to provide *context* for the document and retain the navigational context for the site. Think about the following alternatives if you want to use a navigation link to open to a single document:

- Can you re-create the document content as a page instead of a document? Pages are easier to read online and provide opportunities to create rich, dynamic experiences for your viewers. Modern pages are easier to read on mobile devices. Documents are great when viewers need to download or print – but when all they need to do is read, a short, well-crafted page is a better way to present and maintain information.
- Embed the document or a link to the document on a page. When a visitor clicks the link to a page, the site navigation remains visible. The page allows you to provide context for the document and it also keeps the viewer in the context of your site.

Practice progressive disclosure

Navigation should answer the question, "What can I do on this site or from this location?" But, limited real estate on the navigation bar or quick launch means you need to apply the principle of progressive disclosure. This approach suggests that you group your content into logical categories and provide a limited set of choices for your viewers to allow them to explore each content category to learn more.

Progressive disclosure applies to all types of navigation and not just top or site navigation. It also applies to page content. You don't need to have a link to every bit of content on your site or in your portal in the navigation – but your viewers should be able to get a sense of the entire site by exploring your navigation options. Great navigation experiences help viewers understand:

- Where am I?
- What can I do here?
- Where can I go next?

Plan to optimize the navigation experiences for your viewers by combining navigation and page links to answer these three questions.

Managing navigation expectations

Navigation enhances the story of your digital workplace by making it easy for users to browse the content they need. On the internet, we expect to have to search for the content we need. Yet on the intranet, viewers expect a navigation experience that is carefully curated to help them understand and find the content they need.

Curating a navigation experience for intranets and digital workplaces comprised of even just a few hundred sites can be a daunting task – especially your goal (or the goal assigned to you) is to make sure that all content is findable in "three clicks." Contrary to popular belief, your viewers will not leave your site or give up if they are unable to find what they are looking for in three clicks! More or fewer clicks do not make viewers happier or perceive that the site is faster.

What really matters in navigation experiences is "information scent" – whether the label for the link provides an adequate clue about where the "click" will go. It is the quality of the label and whether the label fulfills its promise that has the highest impact on usability. Viewers are willing to click to find information if they are confident that with each click, they are headed in the right direction – closer to their goal.

"Information scent" on SharePoint sites can be achieved with **clear, mutually exclusive labels** for links and labels lists and libraries that clearly tell viewers what they will find. You can improve your navigation by spending time testing to make sure that the navigation labels resonate with your viewers and following the guidance for labels recommended in this document. Your navigation outcomes will be most successful if you take the time to understand your viewers, their key "tasks and asks," and design navigation experiences that keep their promises.

Planning your SharePoint hub sites

1/8/2021 • 22 minutes to read • Edit Online

Hub sites help you organize your intranet. Getting the most value from hub sites requires some up-front planning. Read on to find out more about hub sites and how you can plan for them.

Setting the stage

SharePoint hub sites provide an important building block for your intranet. They're the "connective tissue" you use when organizing families of team sites and communication sites together.

One of the key principles of modern intranets based on Microsoft SharePoint is that each unit of work should get a separate site collection. This helps you to manage governance and growth over time. Each communication site and Microsoft 365 group-connected team site is created as a site collection that can have its own permissions. A hub site (most commonly created from a communication site) should also be considered its own unit of work that brings together many other sites.

In the past, many organizations used subsites to create connective tissue for their intranets. They used the site collection's shared navigation to connect sites and the hierarchical structure of subsite relationships to nest sites within sites. However, subsites don't give any room for flexibility and change. Since subsites are a physical construct reflected in the URL for content, if you reorganize your business relationships, you break all the intranet relationships in your content. Subsites can also create challenges when it comes to governance because many features (including policy features like retention and classification) in SharePoint apply to all sites within the site collection, whether you want them to or not. This means that you must frequently enable a feature for the entire site collection, even if it's only applicable to one subsite.

What is the one thing that we can guarantee is going to happen in every business? Change! As your organization evolves, you need intranets that make it easy to align experiences with the way you work and that can adapt to the inevitable changes in the way you work. This is a key benefit provided by SharePoint hub sites; they model relationships as links, rather than hierarchy or ownership, so that you can adapt to the changes in the way you work in a dynamic, changing world.

Getting started

Before you start making hubs sites, let's recap the three things hub sites give you:

- Shared navigation and brand
- Roll-up of content and search
- A home destination for the hub

Now let's think about the information you're trying to share throughout your intranet, and consider the business outcomes you're trying to enable.

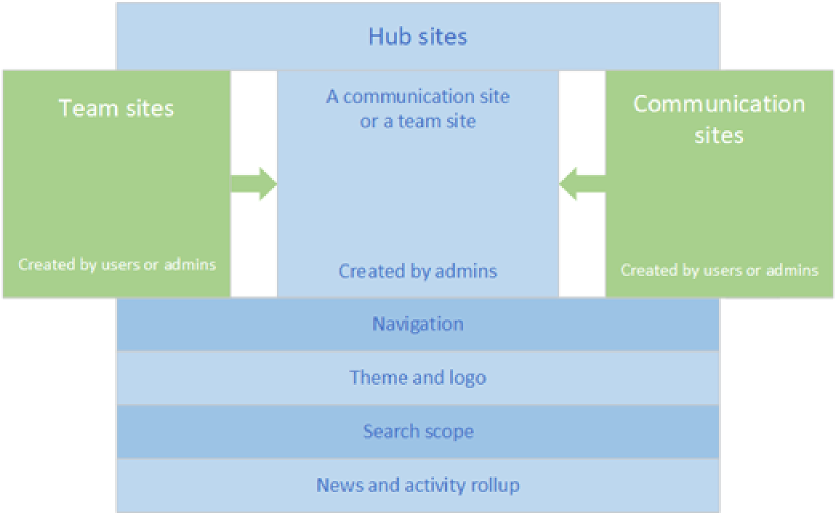
An intranet can play many roles in an organization. It's an internally facing site, a place to communicate important news, and a collaboration platform. It's also a way to showcase your corporate culture. It can be the foundation of your digital workplace. An intranet lets you tell stories and share information. Empowering employees with a voice on your intranet can provide a way to move to a culture of collaboration that enables your organization to transform and adapt to change.

Many successful intranets include the following elements:

- **Communication**: For example, a home page that includes news from around the organization to keep employees informed, overall navigation, links to key tools and information, internal marketing promotions, and a place to engage employees around important topics.
- **Content**: A place for the functional parts of the organization, such as Human Resources (HR), Legal, and Information Technology (IT), to offer their services to the rest of the organization. For example, the HR part of the intranet could be where employees can find out how many vacation days they have left, whether their benefits program offers vision or dental coverage, or what training is available for individual roles. The Legal area might be where employees can find a sample Non-Disclosure Agreement they can execute prior to having a conversation with a prospective vendor.
- **Actions and activities**: Links to the time-tracking system or the expense report form and a place where managers can approve expenses or timesheets.
- **Collaboration**: Places where teams can get work done and where role or topic-based communities can share knowledge and leverage expertise across the organization and with external partners in the extended enterprise.
- **Culture**: Stories and places that allow employees to engage or learn, including profiles, communities and clubs, and even images and branding that reflect the organizational structure. Sometimes even the intranet name embodies the culture. For example, an electric utility has an intranet called "The Grid" with messaging and promotions to make sure that "no one works off The Grid."
- **Mobility**: The ability for employees to get work done from any device while they're on the go.
- **Search**: The ability for employees to find content even if they don't know where it lives.

The emphasis for each of these elements can vary based on organizational priorities and to some extent, the digital maturity of the organization. Microsoft 365 provides three main building blocks to help you create your intranet in a way that allows you to configure experiences that align with your organization, your employees, and your readiness. Different organizations will use the building blocks in different ways, but the building blocks themselves reflect common patterns that organizations use to get work done:

- Team sites (collaboration)
- Communication sites (communication)
- Hub sites (connection)



At their core, the three types of building blocks share a common structure. For example, they share the same set of internal web parts. However, there are some fundamental differences in intent, usage expectations, governance (including how they are created), and how and which web parts you might use on each type of site.

	TEAM SITE	COMMUNICATION SITE	HUB SITE
Primary business objective	**Collaborate** When you want to create a place where the members of a work group or project team can work together on project deliverables, plan an event, track status, or exchange ideas, you want a team site. Team sites are connected by default to a Microsoft 365 group to deliver a full range of communication and collaboration tools, including Microsoft Teams and Planner.	**Communicate** When you want to broadcast a message, tell a story, share content for viewing (but not editing), or showcase services or people, you want a communication site. Communication site owners often want to include an engagement component - for example an "Ask Business Development" area on a site communicating information about business development. This is a great place to connect a Yammer group.	**Connect** When you want to create a shared experience for a family of related sites—to discover related content by rolling up site activity and news, organize related sites so that they share a common navigation, and apply a common look and feel.
Content authors	**All members are content authors** who jointly create and edit content.	**Small number of content authors** and a much larger number of content readers or consumers.	**Hub site owner** defines the shared experiences for hub navigation and theme. **Hub site members** create content on the hub site as with any other SharePoint site. Owners and members of the sites associated with the parent hub create content on individual sites.

	TEAM SITE	COMMUNICATION SITE	HUB SITE
Governance (as allowed for your organization based on the settings in the Security & Compliance center)	Norms typically **determined by the team**. Practices are aligned in the best way to get work done.	Policies often **determined by the organization** to ensure consistency of experience and effective management of organizational information.	Governance **determined by each owner of the associated site based on the type of site and organizational policies**. The best experience for visitors is achieved when everyone has at least read permissions for associated sites (but this is not required).
Permissions	Microsoft 365 group, plus SharePoint groups and permission levels	SharePoint group	Same as original site type. Hub sites do not alter an associated site's permissions.
Created by	**Site owner** (unless this has been disabled in your organization) or **admin**.	**Site owner** (unless this has been disabled in your organization)	**Global admin** or **SharePoint admin** in Microsoft 365
Examples	Project team working together to complete deliverables and manage tasks Holiday party planning committee planning the annual get-together HR performance management team Executive committee—different leadership groups within the organization Extranet site to work with Partner A	Travel team publishing guidelines about corporate travel Policies and procedures Micro-site for a new corporate initiative Resources for the sales team for a product or service	HR hub that provides a connection and roll-up for all HR functions, such as benefits, compensation, performance management, talent acquisition, and a manager portal Sales hub providing enterprise resources for the Sales organization and connecting regional sales team and communication sites Location-specific hub that groups the communication and team sites for a specific location (the New York office)

What should be a hub site?

Hub sites complement the search experience by helping you discover information in context.

One of the biggest challenges with intranet design is figuring out how the intranet navigation should be organized. In the new world where all team and communication sites are peer site collections, information architects must think about creating experiences that will allow intranet users to find what they need in multiple "find" scenarios:

- I know it exists, and I know where it is
- I know it exists, but I don't know where it is
- I don't know if it exists

These scenarios are enabled with a combination of navigation, search, and discovery (or serendipity) and should be a factor in how you design and organize your hub sites. One of the important capabilities that hub sites enable is the serendipitous discovery of information because they can surface contextually relevant content from sites you may not follow but are associated with the hub. The SharePoint start page was built to support discovery and search across the entire organization's content, but if you already have a particular context in mind, hub sites can be very helpful in narrowing those experiences down to a handful of related sites.

As a starting point in your hub planning, think about hub sites for key functions that your users need to get work done—for example: HR, Finance, Communications or Public Relations, Legal, and IT. These functions may be represented in different organizational departments or business units in large organizations or combined into the role of a few people in smaller organizations.

Let's take HR as an example. HR often encompasses the following sub-functions:

- Benefits
- Pay and compensation
- Talent acquisition or recruiting
- Performance management
- Professional development or training
- Manager portal

Using the guiding principle of creating a site for each unit of work, you can think about an HR family of sites that could include six functional sites for each of these functions plus an HR home that connects the related sites to provide an overall HR experience. This is another way to think about the value of hub sites: they allow you to create an experience that improves information discovery for a specific context (in our example, for employees looking for HR information).

In the classic intranet model, you might have created an HR site and used subsites to support each HR function. In the new flat world of modern SharePoint sites, the HR family is connected using the HR hub to provide that connective tissue for navigation within the family and to provide an opportunity to serendipitously discover content on a related member of the family when users navigate to the HR home. For example, if you're on the HR hub reading a news announcement about open enrollment because you're in the process of onboarding a new employee, you might be happy to know that a new version of the "Welcome to the Company" onboarding toolkit was just released on the Talent Acquisition site. Likewise, if you're trying to find the HR team's office sharing policy, you'll appreciate being able to limit your search to only the HR-affiliated sites, rather than the entire organization.

You don't have to have a hub site for every function. However, when a function provides multiple logically different services (as in the HR example), it's a good practice to create a hub site to provide a single starting place for your users. Often, intranet users start their exploration with browsing. Hub sites help combine the benefits of browsing ("I know this is an HR topic") with the benefits of a more narrowly scoped search ("I want to find information about vision benefits, not the company's strategic vision."). Even if the users don't know which sub-function provides a service, they can navigate to the HR hub and then, using the search scope provided by the hub, search (or navigate) within the HR hub to quickly find what they need.

Some organizational functions have an enterprise-wide scope but a regional or product execution. For example, think about a Sales department that may have sites for sales regions and sites for location-based offices. This type of function has always presented a challenge to hierarchical intranet content organization using subsites. Do we make the Southeast Sales site a subsite of the Southeast Region site or the Sales site? And, what happens when a state within the southeast region moves; for example, from the southeast region to the northeast region? This type of dynamic organizational movement creates a nightmare for intranet organization if you use subsites, but not with hub sites. Picking a hub may create some angst because an individual site can be associated with only one hub, but keep in mind that content from a site can appear on multiple hubs. You can customize sources for the following web parts on a hub:

- News
- Highlighted content
- Sites
- Events

> **NOTE**
>
> An organization can have up to 2,000 hub sites. You might not need a hub site for every function and it's important to do some planning before you create hubs.

There is no "one size fits all" way to determine how to align sites to a hub in this scenario. Always start by answering these questions:

- Who is your audience and what do they need to accomplish?
- How do the people who need the information get their work done?

Align your hub to create experiences that enable the user first. You may want to think about how people in each work group think about the work they do by aligning regional sites with the *function*, since sales content for the northeast is more likely to be organized similarly to sales content for the southeast than it will be for the southeast regional office. But this is very much an "it depends" situation. In some organizations, it will make much more sense to organize all functions around a regional hub than a functional hub. With hub sites multi-geo capabilities, you can create a better user experience associating Austria Sales with the Austria hub and not the global Sales hub. In this type of scenario, you can use a link on the Austria sales site to connect it to the global Sales hub and add each regional sales site to the Hub navigation for global sales.

> **NOTE**
>
> A site can only associate with a hub family. However, hub families can be connected to one another using links either on the page or in hub navigation.

A good practice is to start with a consistent approach for all functions that have a pattern, such as Sales. If you align region-specific functions to the regional hub, do that for all functions. Either approach is valid, but from a usability perspective, it helps to be consistent.

How should I organize my hub site?

Hub sites provide two primary organizational experiences that you should think about as part of the hub planning process. Though creating a hub site must be done by the global or SharePoint admin in Microsoft 365, planning, managing, and organizing the hub site is the responsibility of the hub site owner. The organizing concepts for hubs are:

- Association
- Navigation

Association

A site becomes part of a hub family by Associating a SharePoint site with a hub site. When creating a hub site, SharePoint admins should allow only certain site owners to associate sites with the hub.

After a SharePoint admin gives a site owner permission to associate their sites with a hub site, the site owner can then choose to associate the sites with the hub. When they do, the site inherits the hub site theme and shared navigation. Content from their site will roll up to the hub site, and the site will be included in the hub site search scope.

Associating with the hub does not automatically add the site to the hub navigation. Hub site owners determine which sites are included in the navigation. They can also configure the News, Sites, and Highlighted content to roll up activity from all associated sites or only selected sites.

> **NOTE**
>
> Association with a hub does not change the permissions on a site. If you associate a site that has restricted access with a hub, only users who have access to the restricted site will see content rolled up on the hub. Information surfaced on the hub site is security trimmed: if you don't have access to the content, you won't see it. Something you may want to consider is adjusting permissions on the associated sites after you have assembled your hub family.

Navigation

The hub site owner determines which sites are reflected in the shared navigation, and can also include links to other resources. This navigation appears at the top, below the suite bar. Most of the time, you will want to add associated sites to your hub navigation. That's one of the benefits of the experiences that you can enable with a hub. Your hub navigation can have up to three levels, which lets you organize your hub family in a way that helps users discover and find relevant content.

However, you may not want to add every associated site to your navigation and you may want to consider adding sites that aren't associated to the navigation. Consider the following as you plan your hub navigation.

- **Do you want to add private or restricted access sites to the navigation?** Maybe. For example, HR may want to associate their private team site with the HR hub to make it more convenient for HR team members. But, the HR hub owner may not want to add the private HR team site to the shared navigation for the HR hub because this would make the private HR site more discoverable by everyone in the organization, who will get an access challenge when they click the link to the HR team site. Unless the owner of the HR team site wants to spend a lot of time denying access requests, it might be a good idea to leave the private team site off the navigation for the HR hub. On the other hand, there may be a site that is "semi-private" that you want interested people to discover. For example, you might have a community that wants to restrict membership to people with a specific expertise, but also wants to discover experts across the organization. In this scenario, users might get an access denied/request access message, but the site owner is prepared and wants to grant access to interested people.

  > **TIP**
  >
  > If you add links to private sites in your hub navigation, add (restricted) or (private) or (external) to the link name to help users understand that they may not have access to the navigation link.

- **Do you want to add sites that are not associated with the hub to the navigation?** Maybe. Since an individual site can only be associated with one hub, adding sites that aren't associated with your hub helps provide a way to connect your hub to related sites. For example, if you choose to associate functions within a region with a regional hub instead of the global function hub, you could add navigation links from the function hub to each of the region sites. For example, if you have a function hub for HR, you could add the regional HR sites (Northeast HR, Southeast HR, and so on) to the navigation of the HR hub to create a comprehensive HR experience. Note that when you do this, the news and activity in the regional HR sites will not show up on the HR hub (but they will show up on the regional hub). And, when you navigate from the HR hub to the regional HR site, you will be on a site that has the regional hub navigation and theme, not the HR navigation and theme. There is nothing inherently wrong or bad about this scenario, but you should be aware of the implications when you plan your hub navigation experiences

> **TIP**
> Don't associate extranet sites with the hub if you don't want extranet users to see the shared navigation. Consider just adding the external sites to the hub navigation so that internal users have quick access to relevant extranet sites.

Can I make just one hub site for my whole organization?

There is no requirement to have more than one hub for your organization, but you should think about what this means for both organization and information discovery. It might be a way to get started, but it will probably not be where you end up.

If you have only one hub, you'll miss the ability to easily surface related information in context. For example, if you have a single enterprise hub, it will be harder to surface just HR-related news on the HR site. Even small organizations may find that restricting the context in which users find information is helpful in managing information overload.

If you want to get started with a single organizational hub and you also want to be able to provide context for the information users see, you can do it, but it will require a publishing "contract" with content authors. Here are a few ways to achieve that outcome with a single hub:

- **Naming conventions**: Add a prefix to news article titles and use a Highlighted content web part to roll up news that, for example, starts with HR on the HR site and Sales on the Sales site or to group news on the hub site.
- **Page metadata**: Map a custom property to a managed property and apply it to pages. Use your custom page metadata in a Highlighted Content web part on a page on any site. This approach gives you increased flexibility in information presentation.

You can probably see that these approaches might be easier to implement with a small publishing group and much harder if content publishing is distributed across the organization. If your organization, like many, has or is driving towards a distributed publishing model, you will want to think about the implications, training, and publishing "contracts" you will need to implement if you start with a single organizational hub.

Know how your audience will consume SharePoint hub sites

Your audience might consume SharePoint hub sites via the SharePoint start page in Microsoft 365—both the sites themselves and how news flows from the hub to the start page. Also, consider SharePoint mobile apps, which could be used to access the hub home page, news, and navigation to associated sites. Consider the value of mobile app notifications. Encourage your users to stay connected on the go with the SharePoint mobile app. Make sure that you consider operating systems, screen sizes, resolution, and form factors. All modern sites, pages, news, and lists should work well across all of these, and some will reflow as people consume content on small devices.

Additional important considerations

- **Finding hubs if you have more than one**. Hub sites are an important building block for your intranet. But for most organizations, hub sites are not going to provide the type of global navigation that intranet designers want. Here are some ways you can make your hub sites discoverable:
  - **On the SharePoint start page**. Pin your hub sites to the Featured links area of the SharePoint start page. Encourage all users to "follow" hub sites.
  - **On the SharePoint mobile app**. Hub sites can also be found on the SharePoint mobile app and are even more discoverable if users follow hub sites.
  - **From the organization portal**. If you have an existing organizational intranet or portal, you can link to your hub sites in your existing navigation.
  - **On each hub site**. Consider adding a link to your organizational portal home page on each hub site. Add the link to the organization portal ("home home") to the far right in your hub navigation to keep the primary focus of your hub site on the hub site context.
- **Reaching the right audience for news**. Hub sites help you bring news to the right people at the right time and in the right context. News doesn't flow down to associated sites, only up from the associated site to the hub. If you want the broadest reach for your news, publish it to the hub site. To make hub news more visible, you may want to have two news web parts on your home page: one for new published on the hub home and another that includes news rolled up from associated sites (all or only selected sites).
- **Hub naming conventions**. Think about naming conventions for hub sites to make them more discoverable. Some options include names such as HR Central, HR Hub, HR Portal. Try to choose a consistent naming convention for all hub sites.
- **Getting ready to hub**. Once you have planned your hubs, you can transform an existing site (preferably a communication site) to become a hub site or create a new communication site and make it a hub site. Then, you can add and configure the web parts and navigation on the hub site to emphasize the hub capabilities.
- **Subsites**. Hub sites solve many or most of the use cases for which you previously used subsites. We recommend using hub sites going forward to organize the sites in your intranet. However, subsites will continue to be supported as a classic feature, and we'll add the new team site template as a subsite option.

Use hub sites when they align with your business outcomes and solve a need for your users. The capabilities of hub sites are evolving, and we're working to implement some of the most requested features as soon as we can, such as the ability to target the navigation links in hub sites to specific groups of people.

Need more help?

If you have technical questions about this topic, you may find it helpful to post them on the SharePoint discussion forum. It's a great resource for finding others who have worked with similar issues or who have encountered the same situation.

Principal author: Susan Hanley, MVP
LinkedIn: http://www.linkedin.com/in/susanhanley
Website: www.susanhanley.com
Blog: http://www.computerworld.com/blog/essential-sharepoint

Create a hub site in SharePoint

5/1/2020 • 2 minutes to read • Edit Online

If you're a global or SharePoint admin in Microsoft 365, you can convert any existing site to a hub site.

NOTE

We recommend selecting a communication site, or a team site that uses the new template. If you use a classic team site, the hub navigation will appear only on modern pages, and hub site settings will only appear on modern pages.
Sites that are already associated with another hub can't be converted to a hub site.
You can create up to 2,000 hub sites for an organization. There is no limit on the number of sites that can be associated with a hub site.
When users associate their sites with a hub, it doesn't impact the permissions of either the hub site or the associated sites. It's important to make sure all users you allow to associate sites to the hub have permission to the hub.

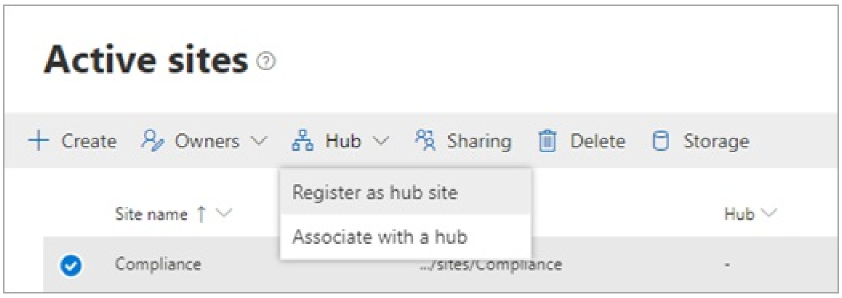
Create a hub site in the new SharePoint admin center

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

NOTE

If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

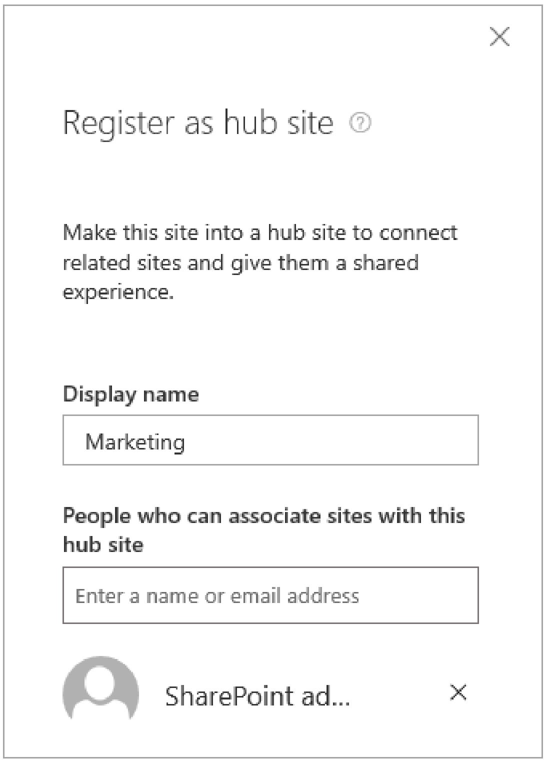
2. Select the site, select **Hub**, and then select **Register as hub site**.



TIP

Using the Hub site menu, you can also associate a site with the hub site, change a site's association to a different hub site, or disassociate a site from a hub site.

3. Enter a display name for the hub site, and specify the individual users or security groups you want to allow to associate sites with the hub.



> **IMPORTANT**
>
> If you leave the **People who can associate sites with this hub** box empty, any user can associate their site with the hub.
>
> If you later want to change the hub site display name or the list of people who can associate sites with the hub, you need to use PowerShell or go to hub site settings on the hub site.

4. Select **Save**.

Related topics

- For info about using a site design that gets applied when sites join the hub, see Set up a site design for your hub site. For more info about site designs and site scripts, see SharePoint site design and site script overview.
- To learn how to use Microsoft PowerShell to create and manage hub sites, see Manage SharePoint hub sites.
- For info about how site owners can customize hub sites, see Set up your SharePoint hub site.
- For info about removing a hub site, see Remove a hub site.

Unregister a site as a hub site

5/1/2020 • 2 minutes to read • Edit Online

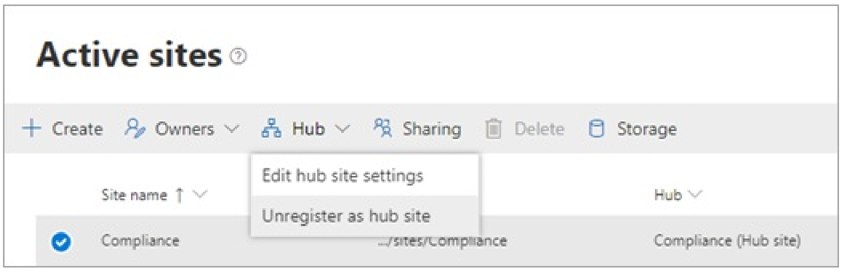
If you're a global or SharePoint admin in Microsoft 365, you can make a hub site no longer a hub site (unregister it as a hub site). Make sure you do this before you delete the hub site. When you unregister a hub site, any sites still associated with the hub will be disassociated the next time a user accesses them. Disassociating a site will remove the hub site navigation bar from the top of the site. The look that the site inherited from the hub site will stay the same and features such as additional navigation links, applications, or custom lists with specific columns that were added as part of the inherited hub site design will remain. Any hub-site-related web parts added to the home page will only show information from the site instead of from sites associated with the hub.

Unregister a hub site in the new SharePoint admin center

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select the site, select **Hub**, and then select **Unregister as hub site**.



3. Select **OK**.

> **NOTE**
>
> If a hub site has associated sites when you unregister it, it might take a while for the sites to be disassociated. If you re-register the hub site, the sites may remain associated.

Related topics

To learn how to use Microsoft PowerShell to manage and delete hub sites, see Manage SharePoint hub sites.

Set up a site design for your hub site

6/5/2020 • 2 minutes to read • Edit Online

A site design is one or more site scripts that Microsoft SharePoint runs when a site is associated with a hub site. Actions describe changes to apply to the new site, such as creating a new list or adding nodes to the site navigation. Site designs provide reusable lists and custom actions so your users can quickly get started with the features they need.

> **NOTE**
>
> For organizations using Multi-Geo Capabilities in Microsoft 365, hub site designs work only when sites are in the same geo location as the hub site.

> **NOTE**
>
> These instructions require the SharePoint admin or Global Admin role in Microsoft 365.

1. Create a JSON script, add it, and create the site design

Follow the steps in Get started creating site designs and site scripts. For the full list of supported actions, see Site design JSON schema. Note that when you create the site design, the site template you provide ("64" for team site or "68" for communication site) doesn't matter.

2. Scope access to the hub site design

When a site design is first created, it is available to everyone. You can grant View rights to the site design. After rights are granted, only the users or groups (principals) specified have access. We recommend granting access to the same principal used to scope the hub site.

```
Grant-SPOSiteDesignRights
  -Identity <ID>
  -Principals ("HR@contoso.sharepoint.com")
  -Rights View
```

Replace with the site design ID from when you added the site script.

3. Set your site design for the hub site

You can set the hub site design in two ways. You can do it using the following PowerShell command:

```
Set-SPOHubSite https://contoso.sharepoint.com/sites/Marketing
-Title "Marketing Hub"
-LogoUrl https://contoso.sharepoint.com/sites/Marketing/SiteAssets/hublogo.png
-Description "Hub for the Marketing division"
-SiteDesignId "<ID>"
```

Replace with the site script ID from when you added the site script.

You can also let hub site owners set the hub site design by using a new option available in the UI. For info about the hub site settings available to site owners, see Set up your SharePoint hub site.

Control settings for Microsoft Lists

11/2/2020 • 2 minutes to read • Edit Online

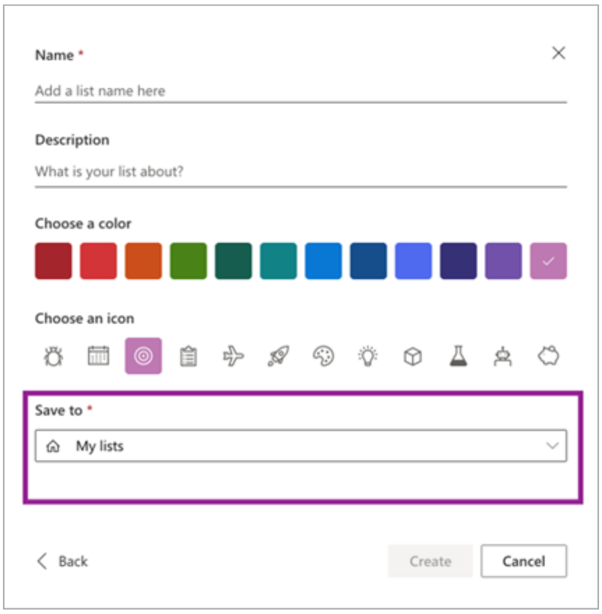
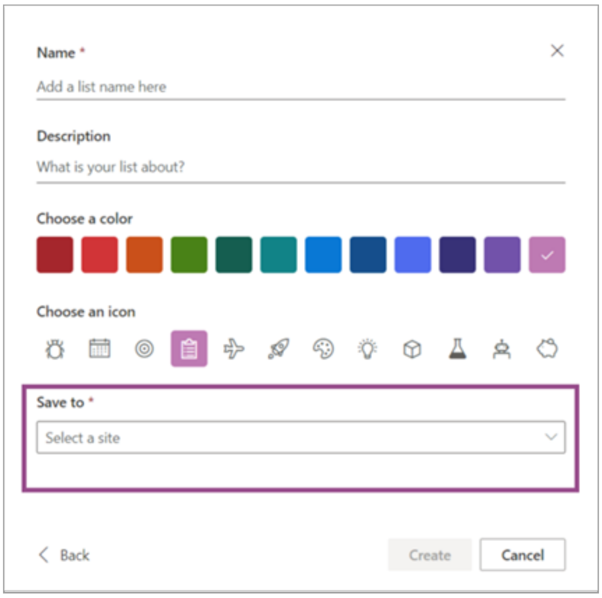
As a global or SharePoint admin in Microsoft 365, you can control settings for Microsoft Lists. You can:

- Disable the creation of personal lists (prevent users from saving new lists to "My lists").
- Disable built-in list templates that aren't relevant for your organization.

You control both of these settings by using Microsoft PowerShell.

Disable creation of personal lists

If you change this setting, when users create a list, they must select a SharePoint site for saving the list. The "Save to" setting doesn't include the "My lists" option.

<table>
<tr><th>DEFAULT</th><th>PERSONAL LIST CREATION DISABLED</th></tr>
<tr><td>
</td><td>
</td></tr>
</table>

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

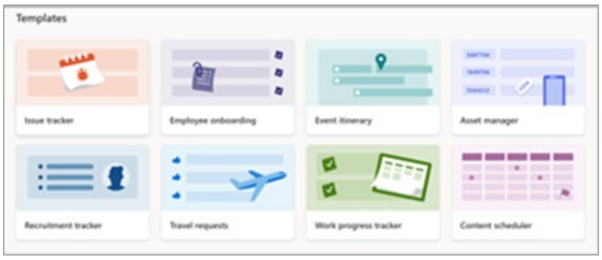
3. Run the following command:

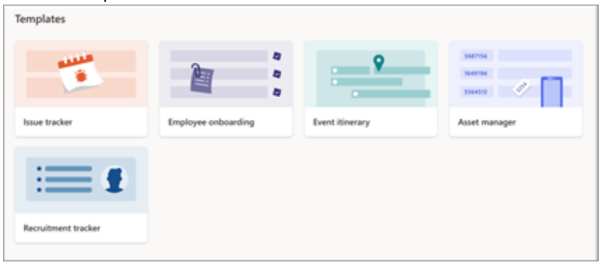
```
Set-SPOTenant -DisablePersonalListCreation $true
```

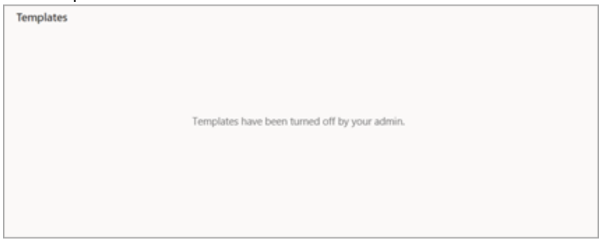
To re-enable the creation of personal lists, set the parameter to `$false`.

Disable built-in list templates

Disabling these templates removes them from all places users create lists (the Lists app, Microsoft Teams, and SharePoint sites).

<table>
<tr><th>DEFAULT</th><th>BUILT-IN LIST TEMPLATES DISABLED</th></tr>
<tr><td>


</td><td>
Some templates disabled


All templates disabled


</td></tr>
</table>

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

```
Set-SPOTenant -DisableModernListTemplateIds '<template ID>'
```

Where the template ID is:

- Issue tracker: 'C147E310-FFB3-0CDF-B9A3-F427EE0FF1CE'
- Employee onboarding: 'D4C4DAA7-1A90-00C6-8D20-242ACB0FF1CE'
- Event itinerary: '3465A758-99E6-048B-AB94-7E24CA0FF1CE'
- Asset manager: 'D2EDA86E-6F3C-0700-BE3B-A408F10FF1CE'
- Recruitment tracker: '3A7C53BE-A128-0FF9-9F97-7B6F700FF1CE'

- Travel requests: 'C51CF376-87CF-0E8F-97FF-546BC60FF1CE'
- Work progress tracker: 'B117A022-9F8B-002D-BDA8-FA266F0FF1CE'
- Content scheduler: '9A429811-2AB5-07BC-B5A0-2DE9590FF1CE'
- Incidents: 'E3BEEF0B-B3B5-0698-ABB2-6A8E910FF1CE'
- Patient care coordination: '0134C13D-E537-065B-97D1-6BC46D0FF1CE'
- Loans: '7C920B56-2D7A-02DA-94B2-57B46E0FF1CE'

To re-enable a built-in template, use the parameter `EnableModernListTemplateIds`.

Add a sample site to your tenant

6/5/2020 • 2 minutes to read • Edit Online

Discover the modern experiences you can build with Microsoft SharePoint. Use the SharePoint look book and integrated provisioning service to find inspiring samples of communication sites and team sites that look great on the web and on mobile devices. Then, add one or more sample sites to your tenant. You can customize the sample to use for your own site or use the site for learning or showing to your colleagues. You can do this all with the SharePoint look book and the integrated SharePoint provisioning service.

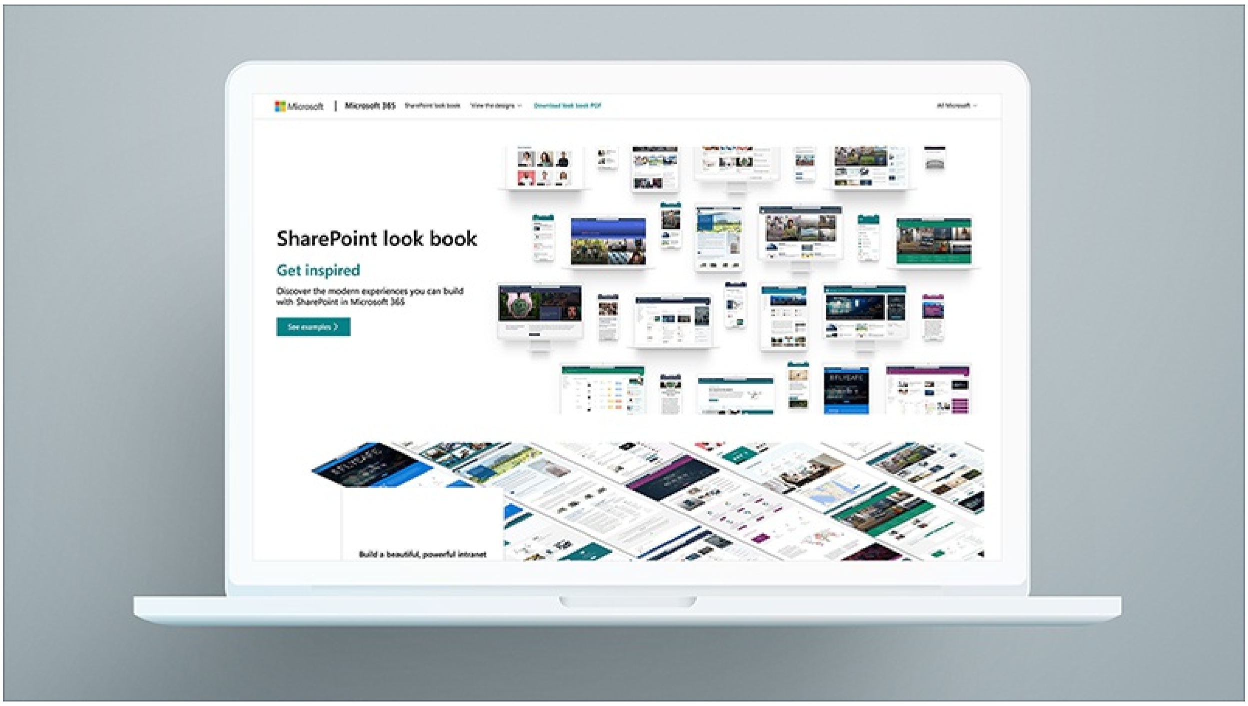
What's included in a sample? You'll get:

- A modern communication or team site, depending on the sample you choose
- A site home page with sample branding, web parts, content, and images
- Sample news posts and pages
- Sample navigation

Get started

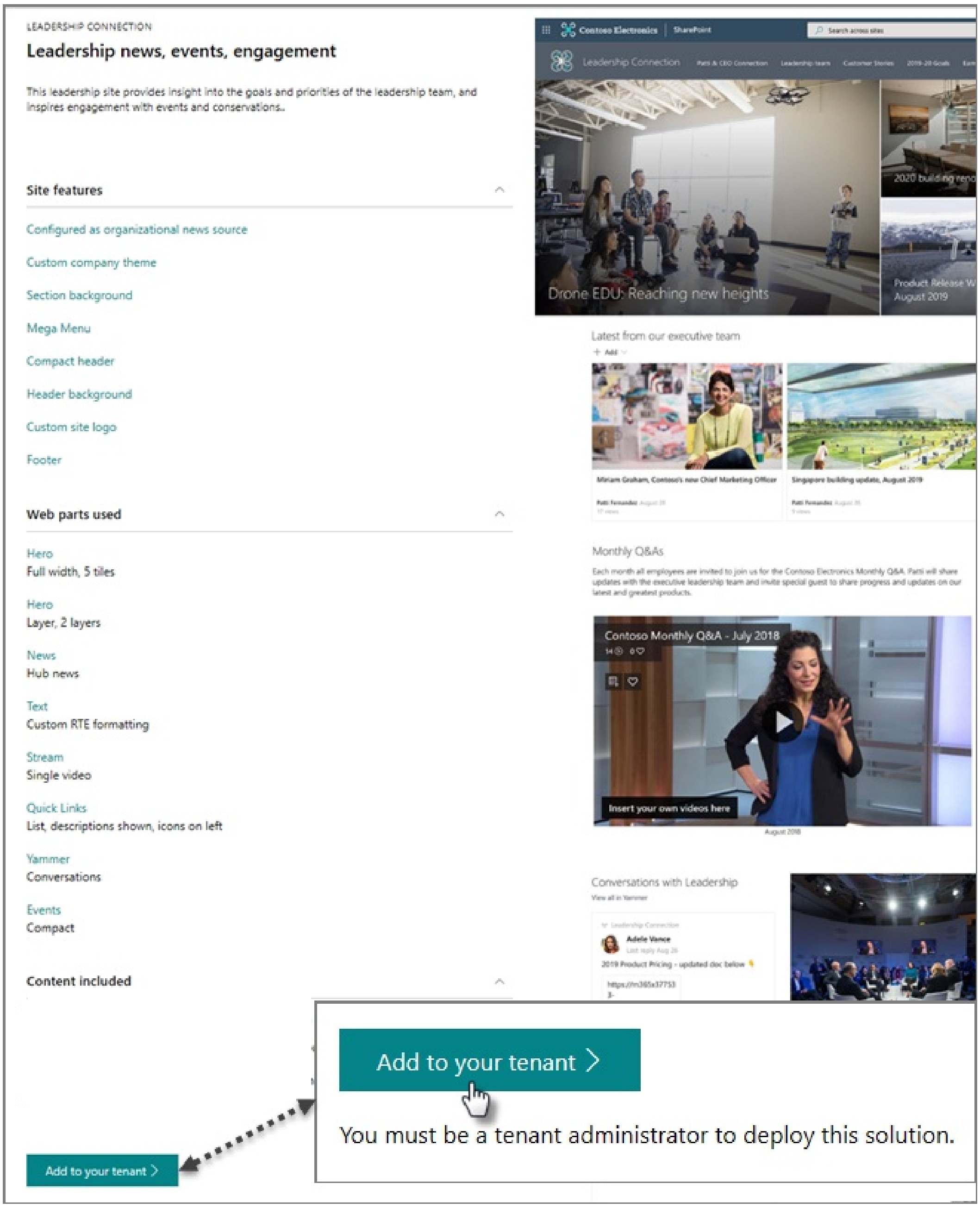
Select a sample you like

Browse the samples in the online SharePoint look book.



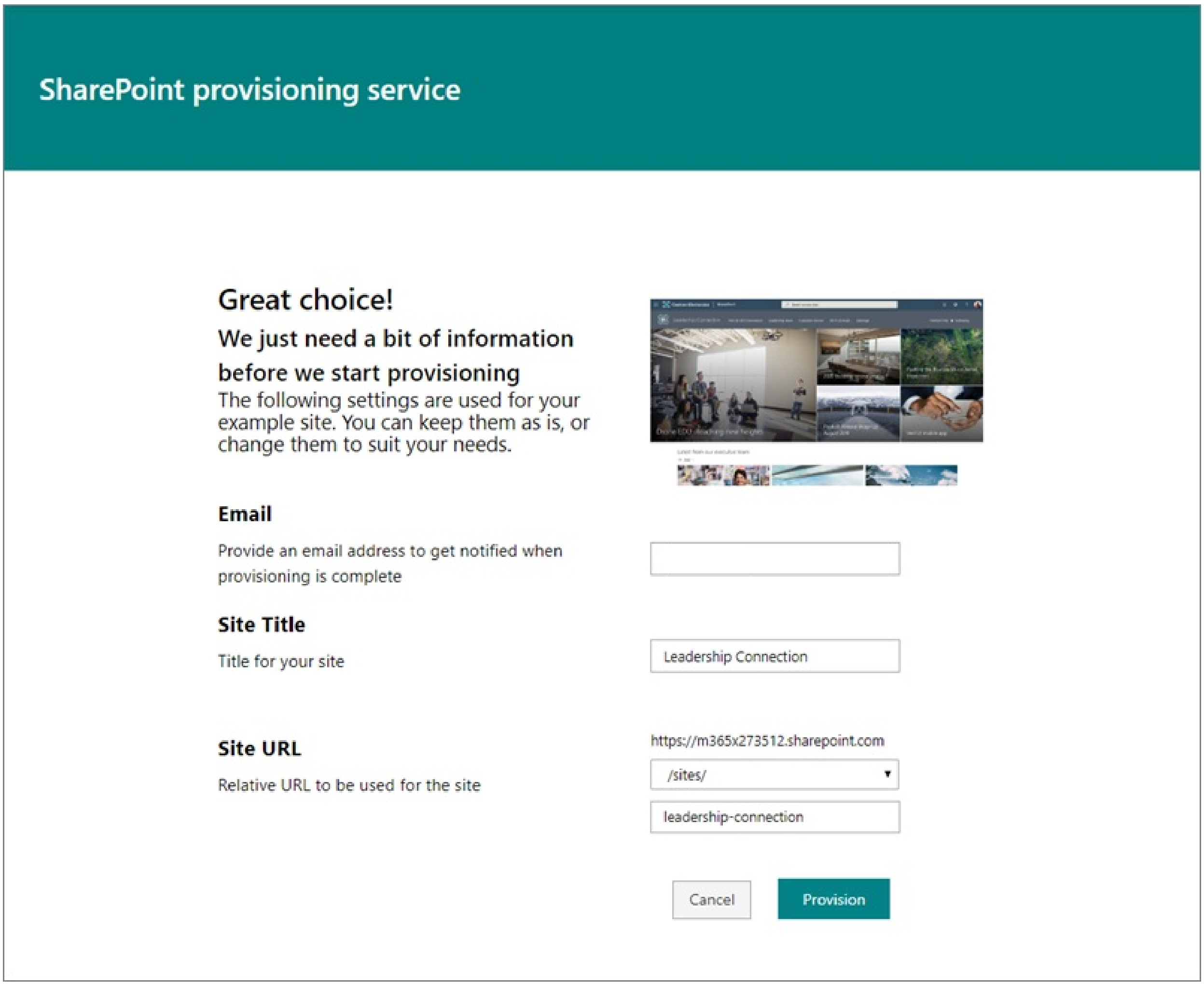
Select a sample to learn more about it. You'll see the site features, web parts used, and content included. To show you how to use these features, links are provided to a help topic for each feature and its web part(s) in the list.

After you've decided on the sample you want to use in your tenant, near the bottom of the page, select **Add to your tenant**. To use this service, you'll need to be signed in as a global or SharePoint admin in Microsoft 365.



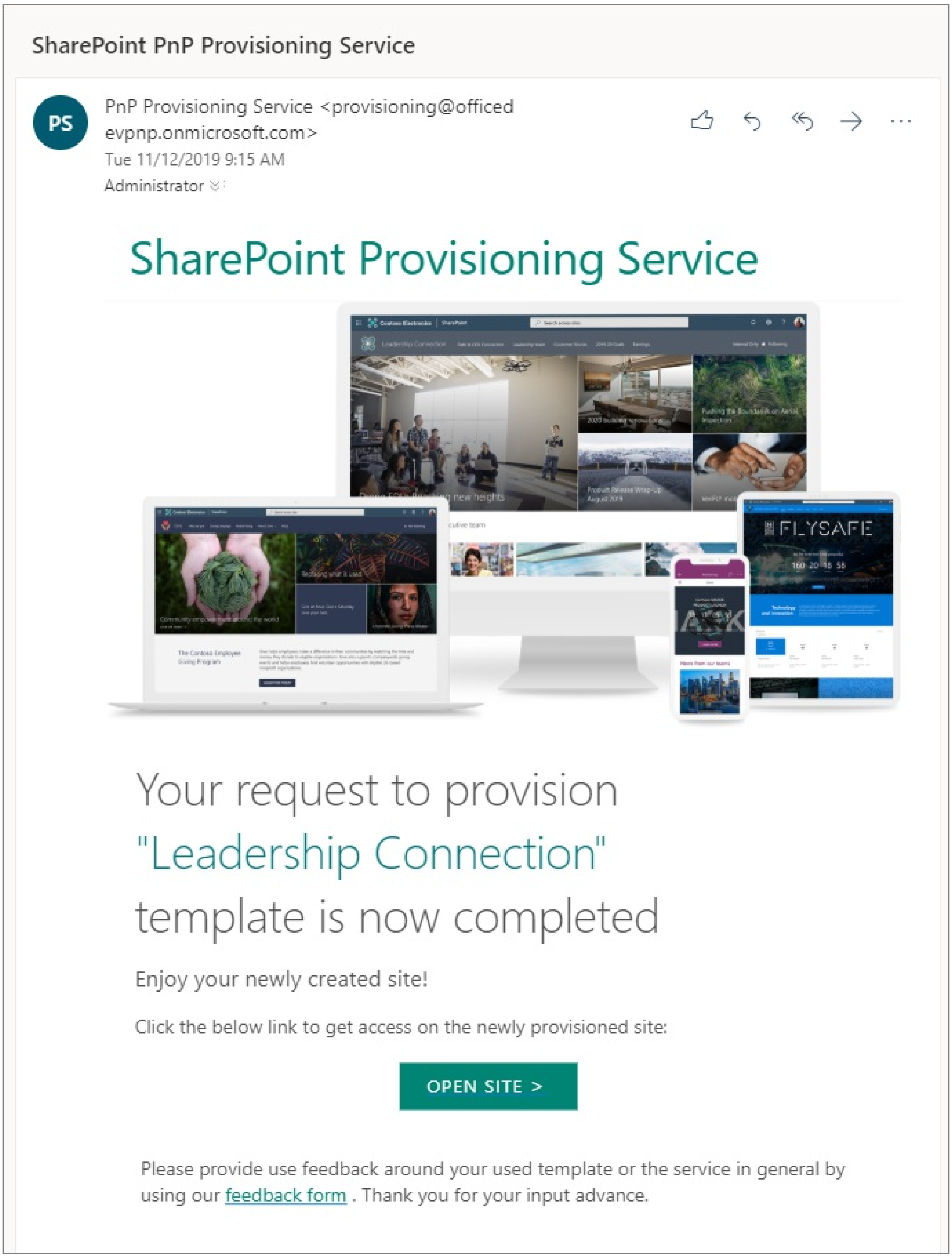
Enter your information

Next, enter your email address (for a notification of when your site is ready to use), the title you want to use for your site, and the site URL you want to use.



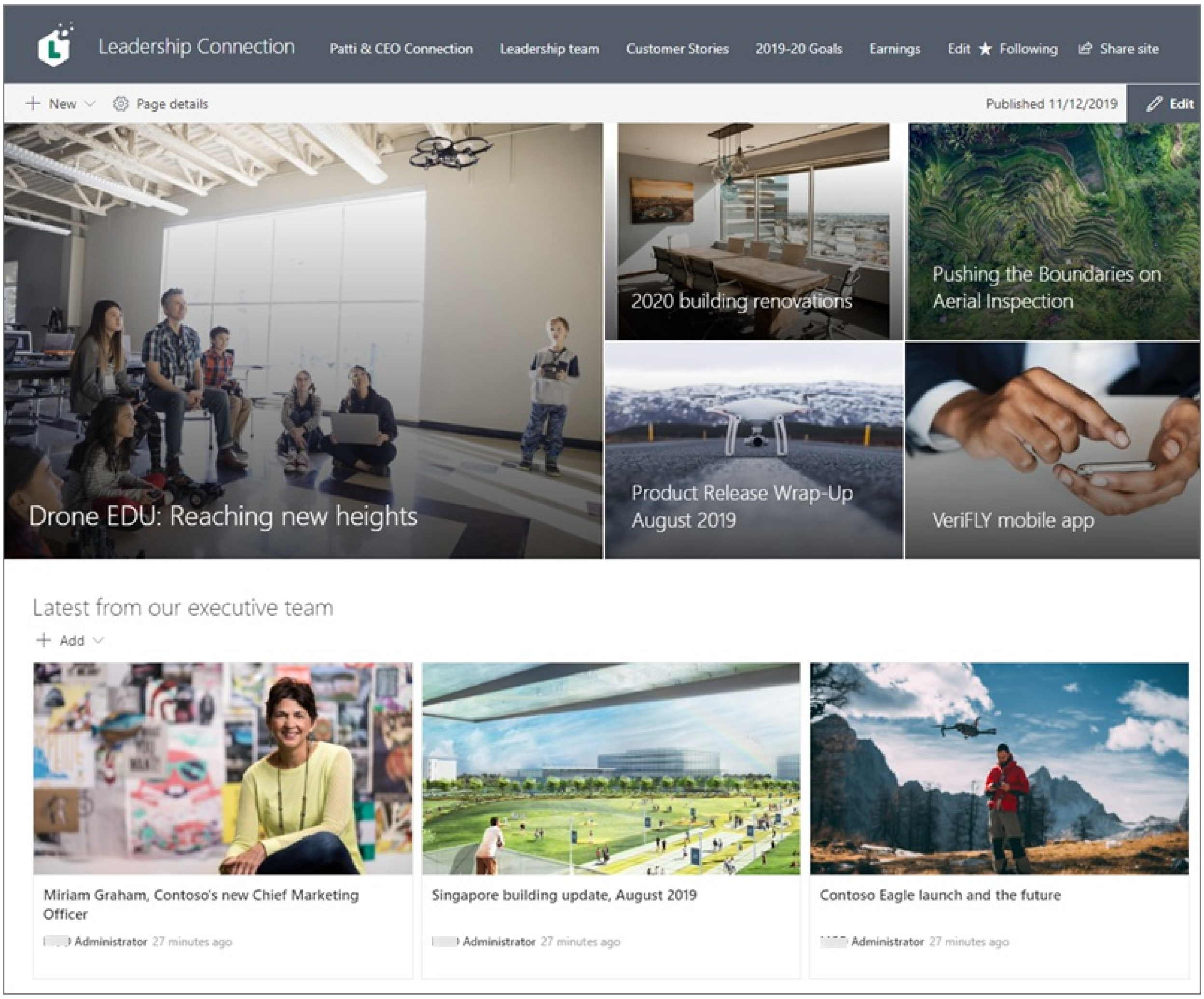
Start provisioning

Select **Provision**, and in a short time your site will be ready for you to use. How will you know? You'll get an email (sent to the email address you provided on the form above) like this:



Open and explore your site

Select **Open site**, and you'll see your sample site and content in your tenant!



From here, you can explore the site and edit the pages and content.

Additional resources

Create a communication site

Create a team site

Using web parts

Create and use modern pages

SharePoint Design Guidance

Overview of the Microsoft New Employee Onboarding hub

11/2/2020 • 20 minutes to read • Edit Online

Microsoft has created an open source New Employee Onboarding (NEO) hub to help organizations improve their onboarding process and experience the benefits of a well-planned new employee onboarding process. The NEO hub helps organizations:

- Provide new employee experiences and information
- Connect new employees to people & culture
- Help stakeholders easily contribute to new employee onboarding
- Measure effectiveness of new employee onboarding

Why invest in a new employee onboarding site?

New employee onboarding (NEO) should be a strategic process that integrates new employees into an organization and its culture while providing the knowledge and tools needed to become fully contributing team members. NEO processes often fall short for both the new hires and the organization. Only 12% of employees strongly agree their organization does a great job of onboarding new employees. An engaging and well organized NEO process can make all the difference in helping a new hire navigate through an exciting – but stressful - career journey, and it can have major organizational benefits.

Strategically planned NEO experience can:

Improve new hire performance and time to productivity - Organizations with a standard onboarding process report 50% greater new-hire productivity.*

Improve new employee retention - Based on our research, 69% of employees are more likely to stay with a company for three years if they had a great onboarding experience. Employees who have a negative onboarding experience are twice as likely to look for new opportunities in the near future.**

The NEO experience process:

PROVIDE NEW EMPLOYEE EXPERIENCES AND INFORMATION	CONNECT NEW EMPLOYEES TO PEOPLE AND CULTURE	HELP STAKEHOLDERS EASILY CONTRIBUTE TO NEW EMPLOYEE ONBOARDING	MEASURE EFFECTIVENESS OF NEW EMPLOYEE ONBOARDING
Sense of place	Pre-onboarding	Departmental and team onboarding	Value realization
Onboarding journey	Social connections and live events	Easy to create and maintain compelling content experiences	Example model for KPIs

NEO hub features:

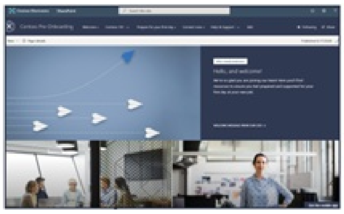
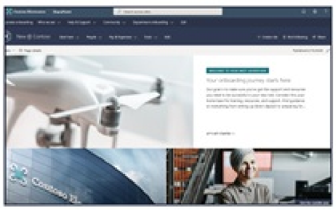
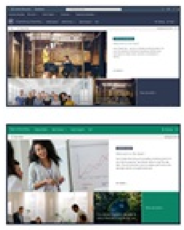
- **A fully configured and customizable set of new hire sites built on SharePoint communication sites:** The NEO hub includes the sites, information architecture, design, user interface and features to help provide new hires with a great onboarding experience. The NEO hub can be customized to add your organization's new hire content and to align with its look and feel. The NEO hub sites are responsive and work as they should on mobile.
- **Onboarding journey:** Onboarding can be an overwhelming experience for new hires with everything the

new hire is typically expected to do and learn in a short period of time. Avoid overwhelming your new employees by providing them a curated onboarding journey that paces the new hire through a configurable activity list of administrative, technology, culture, training, and connection related to-do's. The onboarding journey comes with a pre-configured list of new employee onboarding activities for you to customize for your processes.

- **Sample new hire site pages:** To inspire and provide design templates for arranging your content, the NEO hub includes sample inner site pages. Use these site pages as templates for your content.
- **Easy provisioning:** Provision the NEO hub from the SharePoint look book with just a few steps.
- **Mobile ready:** The NEO hub can be easily accessed on a mobile device when you get the SharePoint mobile app.

NEO hub sites:

New employee onboarding involves multiple levels within an organization, including corporate onboarding, and departmental onboarding. Sometimes teams within a department also need a unique onboarding experience. Each onboarding level provides its own unique value, contributing to a comprehensive onboarding experience each new employee should experience. Research has shown Pre-onboarding new hires, after they sign their acceptance letter but before they officially join the company, can lead to higher performance and better retention rates. To deliver a consistent and integrated new hire onboarding experience the Microsoft open source New Employee Onboarding hub consists of three types of SharePoint site templates, designed to work as one cohesive and familiar experience for new hires.

PRE-ONBOARDING SITE	CORPORATE ONBOARDING SITE	DEPARTMENTAL ONBOARDING SITES
		
Share the Pre-onboarding site with new hires as soon as the job offer has been accepted	Share the Corporate onboarding site with new hires on their first day	Managers and onboarding buddies should share their respective Departmental onboarding site

1. **Pre-Onboarding site:** A site for new hires, who have yet to officially join the company, to learn more about the company they have joined and to get ready for their official start date. External guest access can be used for providing pre-start hires, with no corporate credentials, access to the Pre-onboarding site only.
2. **Corporate onboarding site:** A place for new hires to visit to get the information they need and make the connections they want to successfully onboard to the organization.
3. **Departmental onboarding sites:** A place for new hires to visit to learn more about the department they are joining, its people, culture, and priorities. The new employee onboarding hub includes two departmental template sites, one for an engineering department and one for a sale department

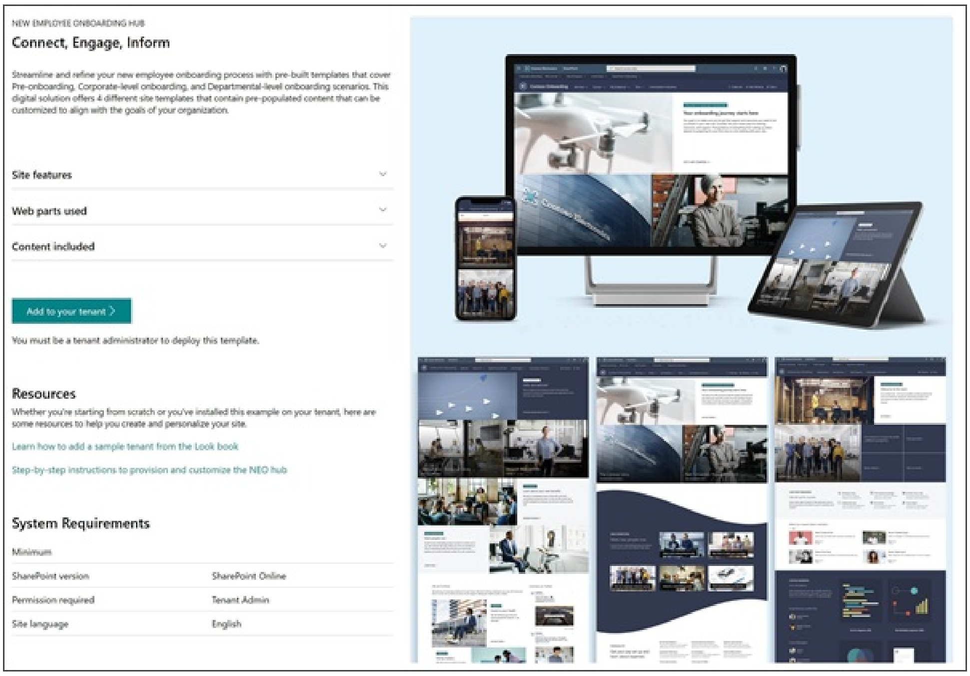
Step 1: Provision NEO hub

The New Employee Onboarding (NEO) hub can be provisioned from the SharePoint look book. With the SharePoint look book, a **Microsoft 365 global admin** can start the provisioning process with a few steps. The whole process takes about 20 minutes to provision. Before starting the provisioning process, make sure you have met the prerequisites for provisioning.

Prerequisites

To successfully set up the NEO hub via the SharePoint look book, the person doing the provisioning must be a Global admin of the tenant where the NEO hub will be provisioned. If you have never provisioned a template form the Look book, review overview guidance.

Provision the NEO hub



1. Go to the NEO hub solution page.

2. Select **Add to your tenant**. If you are not signed into to your tenant, the SharePoint look book will ask for your Global admin credentials.

3. From the permissions requested dialog box, select **Consent on behalf of your organization** and then select **Accept**.

   The provisioning service requires these permissions to provision the site template. There is no overall impact on your tenant and these permissions are explicitly used for the purpose of the solution installation. You must accept these permissions to proceed with the installation.

4. Complete the fields on the provisioning information page as appropriate for your installation. At a minimum enter the email address where you wish to get notifications about the provisioning process and the URL prefix for your site to be provisioned to.

   > **NOTE**
   > Provisioning the NEO Hub will result in 4 separate site collections getting installed in your tenant. You will be prompted to enter the 4 new site URLs where you can edit the site name, site title, description, and default value.

5. Select **Provision** when ready to install the NEO hub into your tenant environment. The provisioning process will take up to 15 minutes. You will be notified via email (to the notification email address you entered on the Provisioning page) when the site is ready for access.

> **NOTE**
> Have provisioning questions? Need to report an issue? Post your questions and comments about the provisioning of the NEO hub to the SharePoint provisioning service forum.

Enable external sharing for the Pre-onboarding site

The Pre-onboarding site is intended to be shared with new hires as soon as they sign their offer letter, but before they start their first day at work. Therefore, this site needs to be shared with external users. External sharing is off by default for SharePoint communication sites. In order for site owners to share externally, turn on external sharing for the Pre-onboarding site.

Add owners to all sites

As the Global admin, you may not be the person customizing the sites, so you'll need to assign a few site owners to the sites. Owners have administrative privileges on the site so they can modify site pages, content, and branding.

1. Select **Share** in the right-hand corner of the site.
2. Add users, Office 365 Groups, or security groups to give them access to the site.
3. Assign users as a **Site owner** to allow permission to customize the site.
4. Include the site URL in the Share message, and then select **Share**.

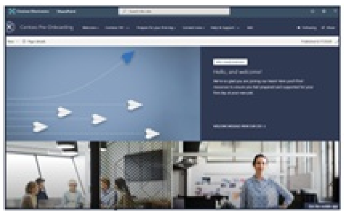
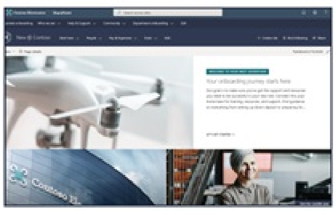
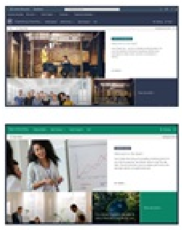
Step 2: Customize the onboarding experience

The New Employee Onboarding (NEO) hub consists of four SharePoint site templates that can be customized to fit the needs of your users and organization. Many of the core pages are already built and pre-populated with content. Review content on sites and pages, then plan on customizing content, images, branding, web parts, and pages.

It's important to make sure the right content is available to users at the right time. It's also important to make new employees feel welcome before their first day. Organizations with a standardized onboarding process report 50% greater new-hire productivity. Alternatively, employees who have a negative onboarding experience are twice as likely to look for new opportunities shortly after starting a new job.

Before you customize content in the NEO experience, ensure you understand the needs of your users and the business objectives of your organization. New hires will need different kinds of support and resources depending on the onboarding phase and culture of your organization. Begin by signing into your account and reviewing pre-populated content. Then, customize content and prepare to share the site with new hires.

NEO hub contents:

PRE-ONBOARDING SITE	CORPORATE ONBOARDING SITE	DEPARTMENTAL ONBOARDING SITES
		
Share the Pre-onboarding site with new hires as soon as the job offer has been accepted	Share the Corporate onboarding site with new hires on their first day	Managers and onboarding buddies should share their respective Departmental onboarding site

1. **Pre-Onboarding site:** A site for new hires, who have yet to officially join the company, to learn more about the company they have joined and to get ready for their official start date. External guest access can be used for pre-start hires who don't already have corporate credentials to give them access to the Pre-onboarding site only.

2. **Corporate onboarding site:** A place for new hires to visit to get the information they need and make

the connections they want to successfully onboard to the organization.

> **NOTE**
>
> The corporate new hire site is a hub and the departmental site templates are associated sites. This creates a coherent and consistent experience for the new hire across the corporate and departmental new hire sites. Learn more about SharePoint hub sites.

3. **Departmental onboarding sites:** A place for new hires to visit to learn more about the department they are joining, its people, culture, and priorities. The new employee onboarding hub includes two departmental template sites, one for an engineering department and one for a sales department. Consider associating departmental onboarding sites with existing department portals if you have them.

Get started - Sign into your Microsoft 365 account

> **NOTE**
>
> You need to be a site owner to customize and share the NEO sites. Work with your SharePoint administrator if you don't already have access.

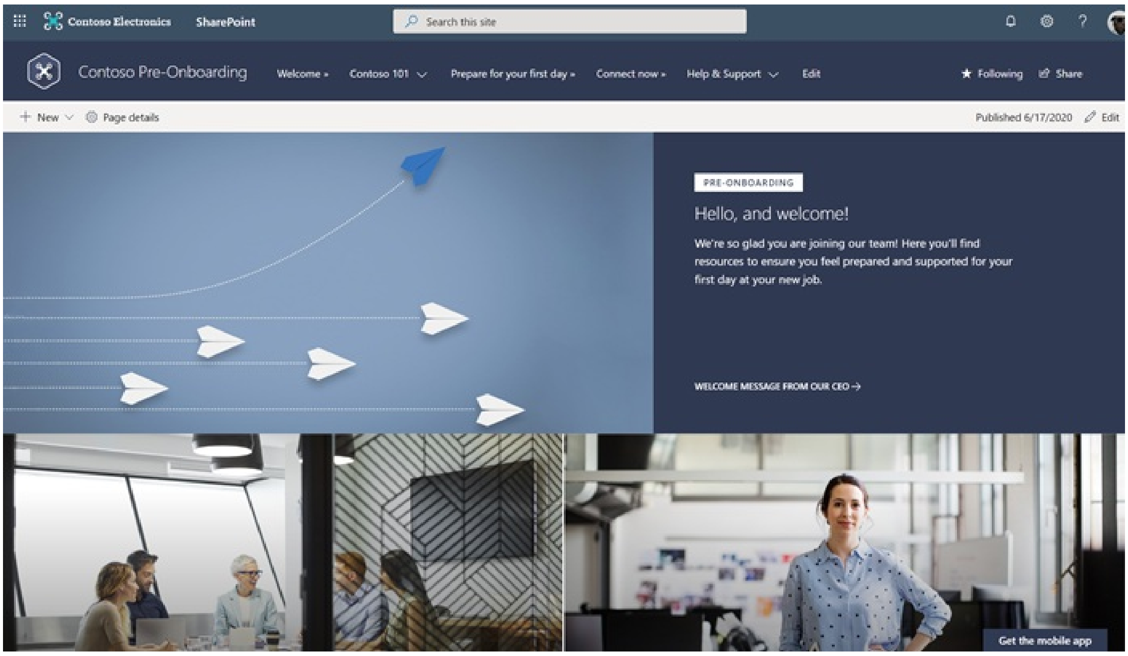
1. Open your web browser and navigate to office.com or your organization's sign-in location.
2. Sign in with your username and password.
3. Navigate to the location of the site using the URL supplied by your Global admin, or select SharePoint from the Microsoft 365 home page, and then select the site.

Explore and review pre-populated content

Pre-Onboarding site:

This is where a new hire starts their onboarding journey. This site is for new hires who have accepted their job offer but have not officially joined the company yet. In this stage, new hires will be interested in learning more about the company, how to get ready for their official start date, and who to go to for questions.

> **NOTE**
>
> The NEO hub comes with many pre-built pages that can be identified in the site navigation with this symbol ">>." Determine which pages and content to keep, edit, or delete based on the needs of your organization.



Pre-populated site content:

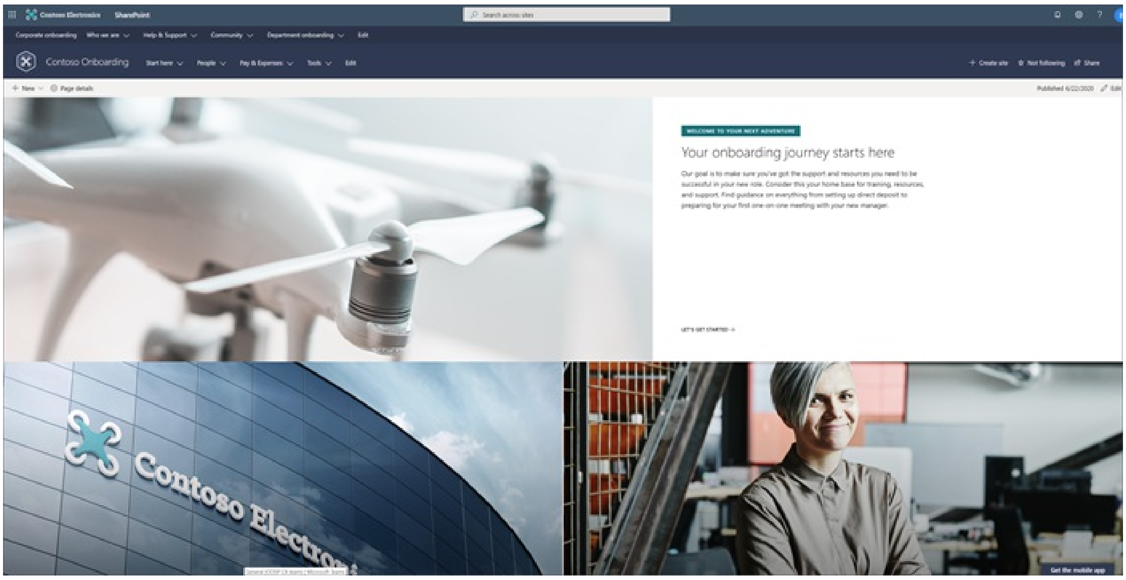
- **Home page** – This is the first site your user will see after they agree to accept the job. Use this landing page as an opportunity to highlight big concepts and get new employees excited about starting their new job. Provide content for topics like organization leaders, values, communities of interest, benefits, and career planning resources.

> **IMPORTANT**
>
> Plan to connect social media accounts to the Hero web part and the Twitter web part.

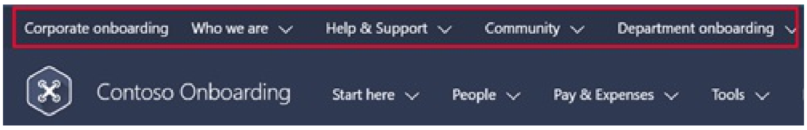
- **Welcome** – Give new hires a warm welcome and place to start understanding onboarding tasks and how to prepare for their first day. This is a good opportunity to include a video message from leadership. Use the YouTube web part, or Embed web part to display the video.
- **Contoso 101** – Provide high level information about the organization that engages and excites. Share more about leadership and values in Our leadership team and Our values pages.
- **Prepare for your first day** – Ensure new hires feel prepared and supported on their first day by providing details on what to bring and where to go.
- **Help & Support** – Highlight where to go for support and customize questions and answers for the FAQ page.

Corporate new hire site:

This is the hub for the new employee onboarding experience and is designed to provide a high-level view of organizational goals, leadership, team structure, and resources. In this phase, users are looking for guidance, support, and clarity. Use this site to outline onboarding details and expectations during the first months of onboarding. Ensure users have access to support channels like Yammer, write FAQs relevant to your organization, and customize the onboarding checklist to include the activities you want all new hires to do in their first 30, 60, 90 days.



Corporate new hire site navigation:



Pre-populated hub contents:

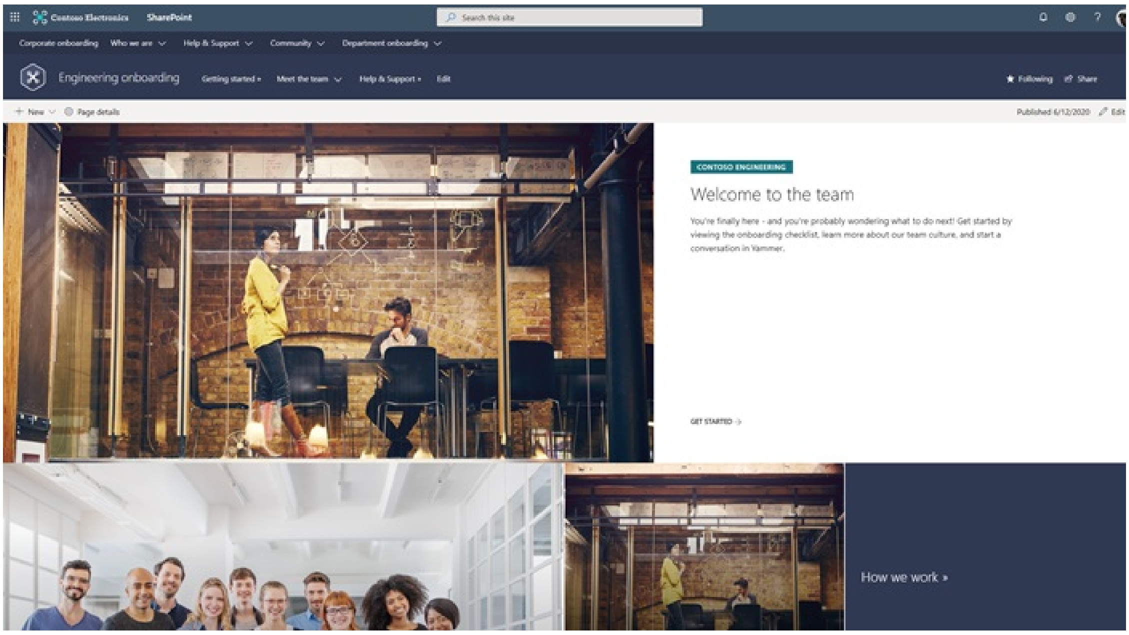
- **Corporate onboarding (home page)** – Highlight key resources in hub navigation. Customize the hub and site navigation to display major content categories to new hires.
- **Who we are** – Introduce users to more detail about the organization in the Our story, Our leadership, Our teams pages. Customize these pages and the Office locations page for your organization.
- **Help & Support** - Highlight where to go for support and customize questions and answers for the FAQ page.
- **Community** – Help new hires start building community right away and make sure new hires are aware of Employee resource groups and other connection channels.
- **Departmental onboarding** – Provide an entry point to departmental-level information from the hub navigation where users can access departmental onboarding sites. Templates for an Engineering and Sales onboarding site have been included. Use these site templates as both a source of inspiration of what your organization's departmental onboarding sites could look like and to accelerate the creation of these sites for your organization.

Pre-populated site (Corporate new hire site) contents:

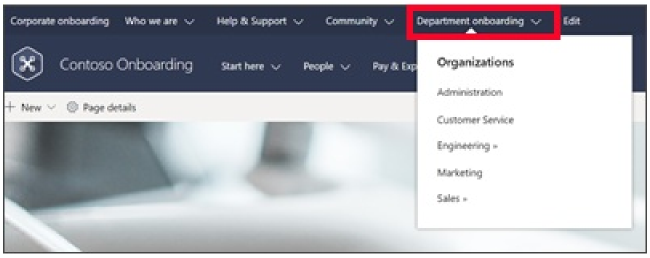
- **Home page** – Provide a high-level view of big concepts that will be relevant to new users. This is a great location to help new employees build their network and learn from more experienced and knowledgeable employees with Microsoft Teams live events
- **Start here** – Specify what new hires should do in their first 30, 60, and 90 days of onboarding by creating an onboarding process in on the Start your journey here page. The new hire checklist found in this section comes pre-populated with a set of generic onboarding activities. Customize list content to meet your needs. Learn more about working with SharePoint lists.

Departmental onboarding:

From the corporate onboarding hub, users can access specific resources for departmental onboarding. Here, users need to learn about departmental leadership, culture, goals, and resources. Use departmental sites to provide access to communication channels, training guides, and events relevant to new hires.The new employee onboarding hub includes two departmental template sites, one for an engineering department and one for a sale department. Consider associating departmental onboarding sites with existing department portals if you have them.



Departmental site location in NEO hub navigation:



Pre-populated site contents:

- **Home page** - Provide a high-level view of big concepts that will be relevant to new hires.
- **Getting started** – Help users quickly understand onboarding tasks, departmental procedures, and anything else that will help new hires be successful.
- **Meet the team** – Introduce new hires to people, the organization structure and goals on the Leadership, The organization, and Our priorities pages. Edits the Call to Action web part to include links and images.
- **Help and support** - Highlight where to go for support and consider creating a FAQ section.

Next steps: Customize place-holder content, edit the site navigation, add pages as needed, and hook up social media accounts in web parts.

Customize the content and look of your NEO sites

Now that you've reviewed the pre-built pages and pre-populated content, you are ready to customize the NEO experience for your organization.

Navigation

Site navigation is important because it helps users immediately understand what can be accomplished on a given site. The most effective SharePoint sites help viewers find what they need quickly so that they can use the information to make decisions, learn about what is going on, access the tools they need, or engage with colleagues to help solve a problem. Edit the hub and site navigation for all three NEO site designs to meet the needs of your audience and organization. Learn how to edit site navigation.

Web parts

Customize web parts with images, labels, links, and content that align with your organization's mission. Keep images and descriptions simple and easy to understand for your new-hire audience.

- **Hero web part** - Bring focus and visual interest to your page with the Hero web part. You can display up to five items in the Hero web part and use compelling images, text, and links to draw attention to each.
- **Text web part** - Use the Text web part to add paragraphs to your page. Formatting options like styles, bullets, indentations, highlighting, and links are available.

- **Image web part** – Use the Image web part to add an image to a page.
- **Quick links web part** – Organize and display links to other resources with the Quick links web part.
- **People web part** – Use the People web part to display profile photos, contact information, and organizational information for people at work.
- **Twitter web part** - Use the Twitter web part to highlight topics and conversations on SharePoint pages.
- **YouTube web part** - Use the YouTube web part to embed YouTube videos right on your page.

Site theme and branding

Edit the look of your SharePoint site to align with your organization's brand. Customize the site display name, logo, theme, header layout, navigation style, and more in the Change the look panel.

Hub site settings

SharePoint hub sites help connect and organize sites based on project, department, division, region, etc. making it easier to:

- Discover related content such as news and other site activities
- Apply common navigation, branding, and site structure across associated sites
- Search across all associated sites.

Considering associating your departmental new hire sites to your existing departmental onboarding site. Learn how hub site associations work and how to manage hub settings for your organization. Learn more about SharePoint hub sites.

More customization resources:

- Add a page to a SharePoint site
- How to use web parts on SharePoint pages
- Use the Events web part
- Use the News web part

Step 3: Share the NEO sites with end users

After customizing content, get ready to share the new onboarding experience with new hires. Different permissions will apply to the Pre-onboarding site since users will be external guests. Once new hires start working, use internal permissions sharing instructions to give access to the corporate onboarding site.

Pre-onboarding site: External guest access

> **NOTE**
>
> If you are unable to add visitors (external users, also referred to as guests) to the pre-boarding site, work with your SharePoint administrator to turn on external sharing for a SharePoint site.

As a site owner, you can give external people access to the site by adding them as a **visitor**.

1. Select **Share site** from the right hand corner.
2. In the Share site pane, enter the names of people to add them to the site. The permission level will be ready only.
3. Enter an optional message to send to the person, or clear the Send email box if you don't want to send an email.
4. Select **Share**.

Corporate new hire site and departmental sites

1. Select **Share site** from the right-hand corner.
2. In the **Share site** pane, enter the names of people or groups to add them to the site, or enter "Everyone

except external users" to share the site with everyone in your organization.

3. Change the permission level (Read, Edit, or Full control) as needed.
4. Enter an optional message to send to the person or clear the Send email box if you don't want to send an email.
5. Select **Share**.

Step 4: Measure the impact of your NEO hub

Define NEO hub success metrics

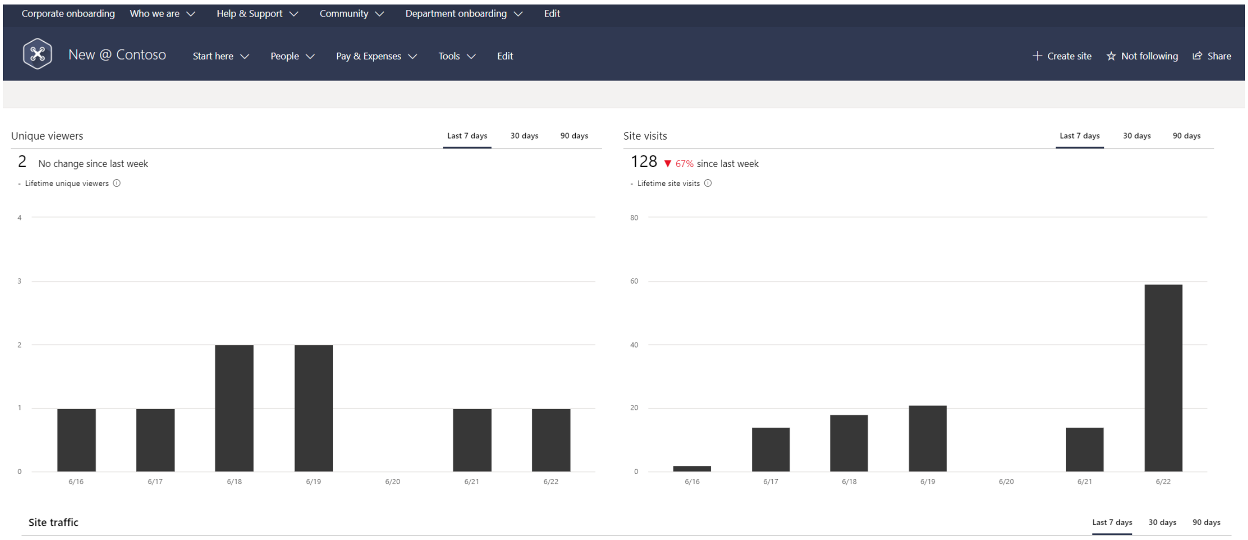
Define site success metrics to measure and optimize your organization's onboarding process. The following is an example of possible metrics for a new employee onboarding hub:

OBJECTIVE	BUSINESS OWNER	KPI MEASURE	DATA SOURCE	KPI FORMULA	KPI BASELINE	KPI TARGET
Help onboard new employees more effectively	Diego Siciliani	New employee satisfaction	Survey data	Average score of new employee satisfaction with NEO Hub	N/A	4.25
Help onboard new employees more effectively	Diego Siciliani	NEO hub usage	Site usage report	Number of unique viewers and visits	N/A	500 unique viewers/month and 1,500 views/month
Increase new employee retention	Alexandre Levesque	New employee retention	HR system retention data	% of new employee cohort that remain with the company after one year	75%	90%
Improve new employee engagement	Diego Siciliani	New employee engagement score	Survey data	Average score of new employee engagement question	3.75	4.25

Leverage site usage data

As a SharePoint site owner, you can view site usage data that shows you how users are interacting with your site. For example, you can see the number of people who have visited the site, how many times people have visited the site, and a list of files that have received the most views. Site owners should utilize SharePoint's built-in site usage reporting capabilities to measure the impact of the NEO hub. Learn how to view usage analytics for your site.

Example of site usage data:



Step 5: Manage and maintain your NEO hub

The NEO Hub should present the most up to date content your organization has to offer, so you'll need to commit to maintaining relevant content throughout the experience. Develop a plan to audit content and refresh web parts as needed to ensure contact information, FAQs, the onboarding checklist, and People web parts are up to date. Learn more about managing communication sites.

- Train site owners and authors. Make sure all site owners and authors have appropriate training and access to maintain the site.
- Update content in web parts. Keep web parts like the People web part updated to ensure you are leveraging the full value of the NEO Hub.
- Review previously established metrics after the launch. Use insights from site analytics to promote content on the home page, update navigation, or re-write content for clarity.
- Establish a schedule to audit content. Plan when site owners should audit content in advance to make sure your sites are always up to date.
- Periodically review your site settings. Make changes to the settings, site information, and permissions for the site as needed.

NEO hub FAQs

Question: What are the requirements for installing the New Employee Onboarding (NEO) Hub into my tenant environment?

Answer:

- SharePoint Online and Communication Sites enabled.
- The individual that will be provisioning CLO365 must be the Global admin of the target tenant for install.

Question: How long will it take to install the site in our tenant environment?

Answer: Based on our testing of the installation, it should take less than 15 minutes. This does not include time required to customize the site to your requirements.

Question: Where can I ask questions or report an issue with the SharePoint provisioning service?

Answer:Post your questions and comments about the provisioning of the NEO hub to the SharePoint provisioning service forum.

Question: Where can I share feedback for ideas on how to improve the SharePoint site experience?

Answer:Post your ideas and comments about SharePoint sites in the [Site and Collaboration User Voice Forum]

(**Question**: Where can I ask questions or report an issue with the SharePoint provisioning service?

Answer:Post your questions and comments about the provisioning of the NEO hub to the SharePoint provisioning service forum.

Sources:

- Gallup, State of the American Workplace, 2017*
- SHRM, Don't Underestimate the Importance of Good Onboarding, 2017**
- Source: Digitate, Super CIO: What the CIO sees—that other people don’t, 2018

Introduction to the SharePoint Success Site

11/2/2020 • 4 minutes to read • Edit Online

The SharePoint Success Site is a ready to deploy and customizable SharePoint communication site that helps your organization maximize the adoption of SharePoint. The SharePoint Success Site is designed to support new SharePoint Site owners in creating high-impact sites to meet the goals of your organization.

The SharePoint Success Site builds on the power of Microsoft 365 learning pathways which allows you to use Microsoft-maintained playlists for training purposes. You can also create custom playlists to meet the unique training requirements of your organization. If you are already using M365 learning pathways and don't want to provision the SharePoint Success Site, you can enable the SharePoint Success Site playlist into learning pathways.

Install the SharePoint Success Site in your tenant environment, customize the pre-populated training and site content, and then make it available to end users.

Ready to get started right away? Next, review the prerequisites and provisioning guidance.

Why invest in a SharePoint Success Site?

The SharePoint Success Site helps Site owners improve the quality and impact of the sites they build in SharePoint for internal audiences, while helping ensure they follow your organization's site usage guidelines.

Use the SharePoint Success Site to:

- **Get more out of SharePoint** - Show new Site owners how to leverage the value behind SharePoint's communication and collaboration features. Help new Site owners understand the ways to work with SharePoint to meet specific business outcomes. Then, show users how to utilize the power behind SharePoint's communication and collaboration features with step-by-step guidance.
- **Enable Site owners to create high-impact sites** - Ensure Site owners have the right information and support to create purposeful sites that are widely adopted by the intended audience.
- **Ensure Site owners follow site creation policies** - Customize the site usage and creation policies page in your SharePoint Success site to communicate organizational policy expectations during the training experience.
- **Provide the most up-to-date content** - Equip Site owners with SharePoint self-help content that is maintained by Microsoft and published as SharePoint evolves.

SharePoint Success Site features

The SharePoint Success Site is designed to reduce the amount of work needed to plan, build, and manage new SharePoint sites for Site owners and content authors.

SharePoint Success Site features:

- **Fast provisioning:** Provision the SharePoint Success Site with just a few steps.
- **Easily customizable:** Edit the site layout, branding, and Microsoft-provided playlist content to align with how you have set up SharePoint in your tenant.
- **Comprehensive Site owner training content:** Training on what makes an effective site and how to build and maintain the site.
- **Site creation guidelines:** Create SharePoint usage guidelines that fit policy requirements for your organization.

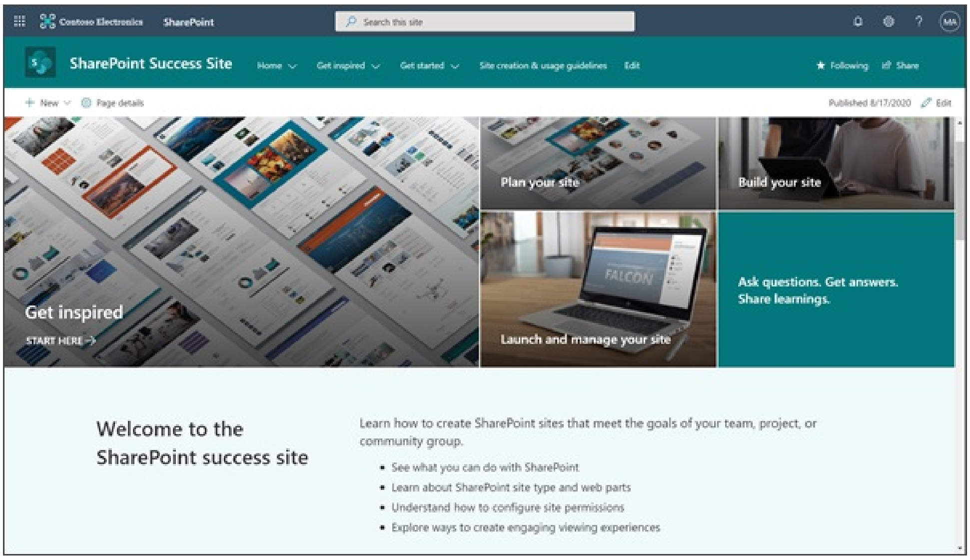
- **Create your own training playlists:** Add your own custom training content and playlists specific to your organization's desired business outcomes outside of SharePoint.

What comes with a SharePoint Success Site

The SharePoint Success Site comes pre-populated with web parts and content to guide your users through the most up-to-date site creation training. There are several opportunities to customize the experience to better suit your organization’s goals, tenant configuration, and usage policy.

SharePoint communication site

The SharePoint Success Site is a SharePoint communication site that includes pre-populated pages, web parts, and site navigation. The site can be customized to incorporate your organization's existing branding, support, and training content.



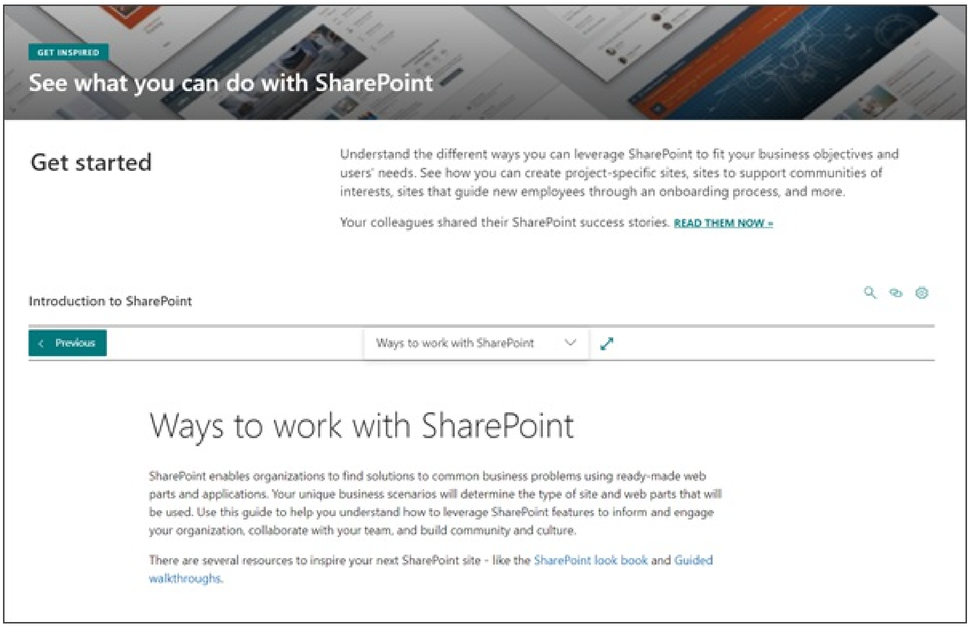
Microsoft-maintained content feed

The SharePoint Success Site’s up-to-date content feed includes a range of content that helps new users and existing site owners plan, build, and manage SharePoint sites:

- **Plan your site:** Guidance on the ways to work with SharePoint, how to plan a site, including what type of SharePoint site to use and how to manage site access and permission strategy.
- **Create your site:** Content that helps new Site owners create their site, add content, customize web parts, and apply brand elements.
- **Share and manage your site:** Guidance to help launch, share, and manage the new site.
- **Advanced site creation:** Content for Site owners who want to learn more about SharePoint beyond site creation basics.

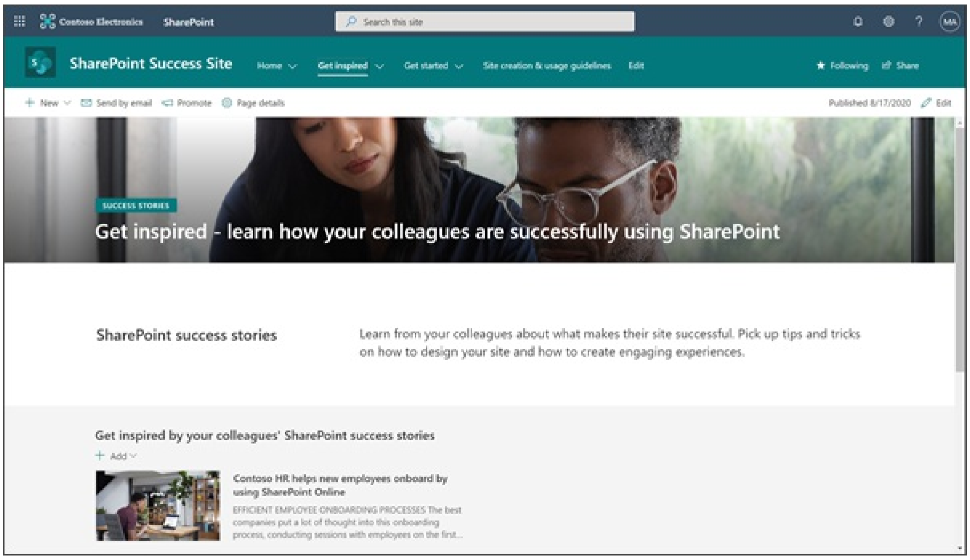
Site inspiration

The introductory content helps new site owners understand the different ways you can leverage SharePoint to meet common business objective through fictional stories that help establish an understanding about the site creation stages and common tasks. Users will have access to stories that illustrate how to build an onboarding site, a project management site, a site that supports a community of interest, and a team collaboration site. These scenarios provide guidance on how to think about the planning, building, and launching phases.



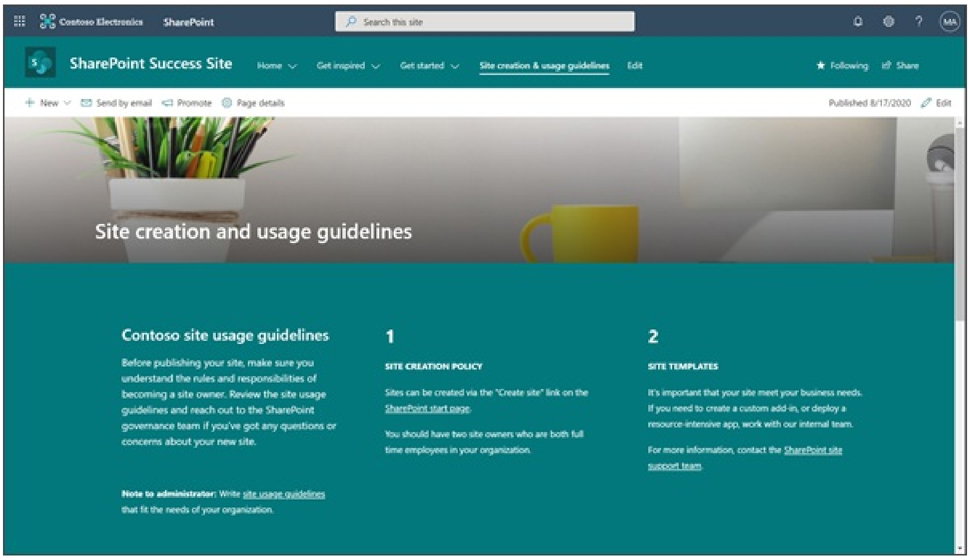
Success stories

The success stories section is a gallery to showcase internal SharePoint site success stories that inspire others in the organization. Learn how to create a Microsoft Form to solicit success stories from site owners and authors, and publish on your SharePoint Success Site to inspire.



Site creation guidelines

The site creation guidelines page provides a starting point to educate new Site owners about SharePoint creation policies for your organization. The guidelines include suggested usage policy topics and questions to prompt consideration of usage policies within your organization. Customize the content in your SharePoint Success Site site creation guidelines page to serve your organization's governance needs.



Summary of how to launch a SharePoint Success Site

Step 1: Meet the pre-requisites and then provision the SharePoint Success Site

Step 2: Customize the site design, playlists, success stories, and site creation guidelines

Step 3: Launch and share the site with others

Next steps - provision the SharePoint Success Site

Review and implement SharePoint Success Site provisioning requirements and instructions.

Frequently asked questions

Question: Who has permission to provision the SharePoint Success Site?
Answer: The Global admin (formerly called the Tenant admin) are required.

Question: Who has permission to customize the site template?
Answer: The Global admin (formerly called the Tenant admin) or Site owner permissions.

Question: Who can create custom playlists and hide or show content in M365 learning pathways?
Answer: The Site collection administrator and Site owner permissions of M365 learning pathways.

Question: Who has permissions to use the SharePoint Success Site as a user?
Answer: Microsoft 365 user permissions or SharePoint Site visitor permissions or higher.

Provision the SharePoint Success Site

1/8/2021 • 7 minutes to read • Edit Online

Start the SharePoint Success Site provisioning process by understanding the prerequisites. We recommend provisioning the SharePoint Success Site from the Microsoft 365 learning pathways administration page per the instructions below. Global administrator (formerly called the Tenant admin) credentials are required to start the provisioning process for the SharePoint Success Site.

Before getting started, watch the provisioning instructional video, follow all steps in the process, and make sure you've met the requirements for provisioning.

Meet the requirements

Before provisioning the SharePoint Success Site, meet the requirements for both the **person** provisioning and the **tenant.** Your tenant's configuration will determine what path you need to take to install the SharePoint Success Site. Start by reviewing the SharePoint Success Site requirements below to prepare your tenant.

TENANT ADMIN ROLE REQUIREMENTS	+	TENANT REQUIREMENTS	=	READY TO PROVISION

Tenant admin requirements

The **person** doing the provisioning must be a Global admin (formerly called the Tenant admin) where the SharePoint Success Site will be provisioned *and must also be* an Administrator of the tenant's App Catalog.

GLOBAL ADMIN ROLE	+	ADMIN OF THE APP CATALOG	=	TENANT ADMIN REQUIREMENTS MET

Are you a Global administrator?

- **Yes** - Next, confirm your tenant has already enabled the App Catalog.
- **No** - Partner with your M365 Global admin to get the site provisioned. Learn more about administrative roles in SharePoint.

  If you are unsure, you can confirm your role by logging into office.com, you'll see an Admin center app icon next to your M365 apps if you have SharePoint administrator credentials.

Are you an Administrator of the App Catalog?

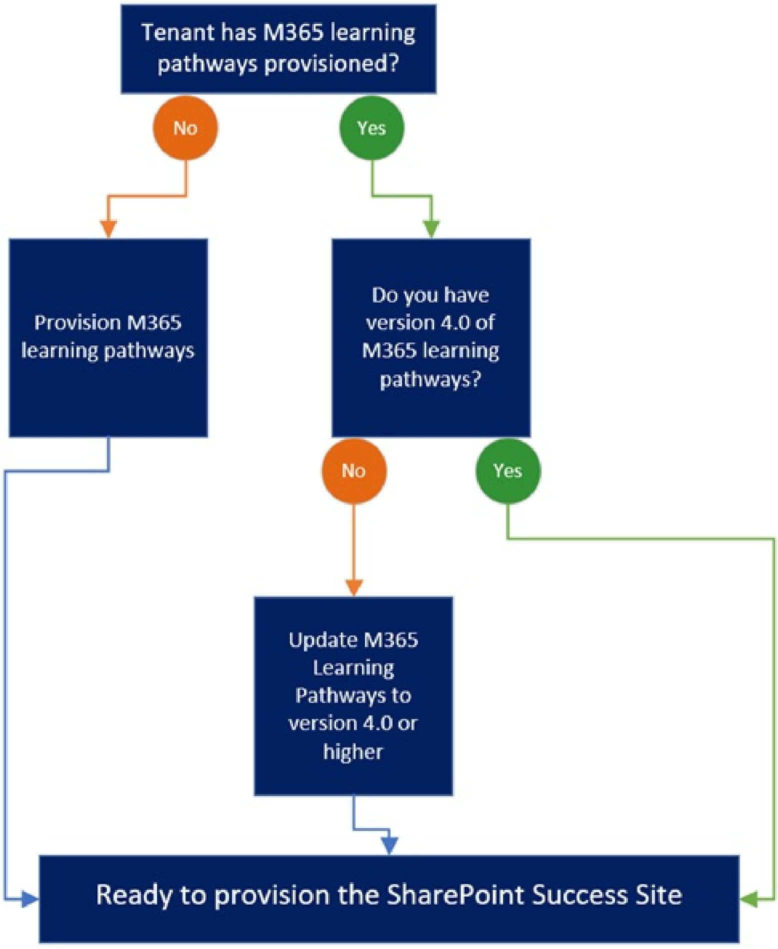
- **Yes** - Next, confirm your tenant has M365 learning Pathways provisioned.
- **No** - Next, ask your Global admin to add you as an App Catalog Administrator.

Tenant requirements

The **tenant** where the site will be provisioned must have the App Catalog installed *and* have the latest version of M365 learning pathways installed. Your tenant must have **version 4.0 or higher** of M365 learning pathways.

APP CATALOG INSTALLED	+	M365 LEARNING PATHWAYS 4.0 OR HIGHER INSTALLED	=	TENANT REQUIREMENTS MET

Use this decision tree to determine your tenant's path to meeting the **tenant** requirements.



Ready to get started provisioning? Review the provisioning instructions.

Does your tenant have the App Catalog installed?

- **Yes** - Next, confirm you are an administrator of the App Catalog.
- **No** - Next, enable the App Catalog (this will take about 30 minutes).

If you are unsure, navigate to the SharePoint admin center, then select **Sites** > **Active sites** and you will see the **App Catalog**

> **IMPORTANT**
>
> If you need to create a App Catalog, wait at least 30 minutes after creating before provisioning M365 learning pathways and the SharePoint Success Site.

Does your tenant have M365 learning pathways provisioned?

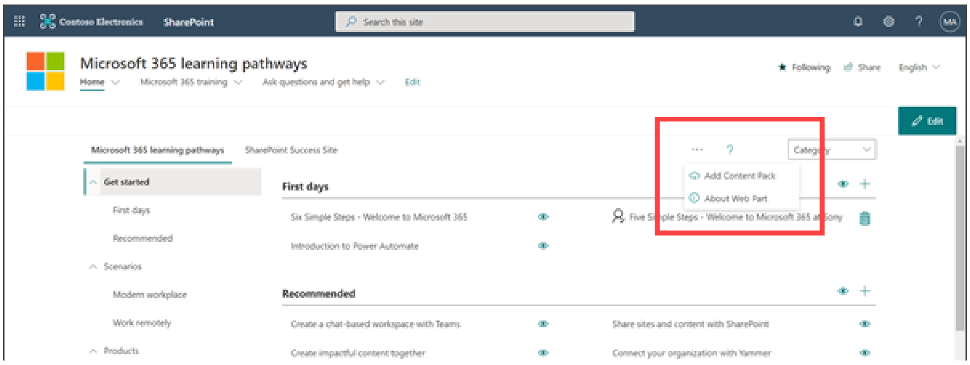
- **Yes** - Next, confirm you are using version 4.0 or higher.
- **No** - Provision M365 learning pathways for the first time.

If you are unsure, navigate to the SharePoint admin center, then select **Sites** > **Active sites** and you will see **Microsoft 365 learning pathways**.

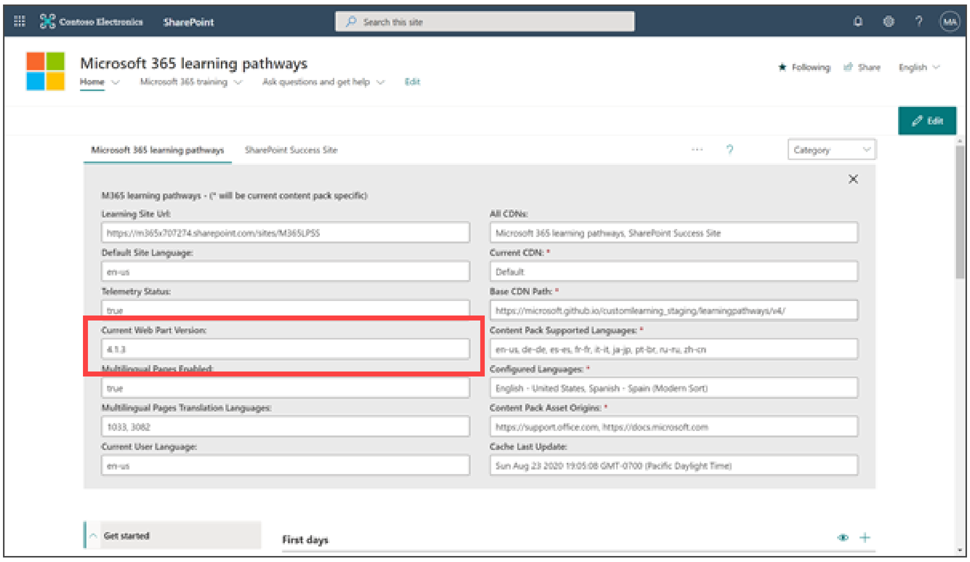
Is your tenant's version of learning pathways version 4.0 or higher?

- **Yes** - You are ready to provision the SharePoint Success Site.
- **No** - Update to version 4.0 or higher and then provision the SharePoint Success Site from the M365 learning pathways administration page.

If you are unsure, navigate to your tenant's **M365 Learning Pathways administration page** and select the ellipses (...)



Then, select **About web part** to confirm the current version.



If you need to, update M365 learning pathways from version 3.0 to version 4.0 or higher

> **IMPORTANT**
>
> The person updating M365 learning pathways must be an Administrator of the tenant's App Catalog. If the person provisioning M365 learning pathways isn't an Administrator of the App Catalog, add an Administrator to the App Catalog and continue.

In this step, you upload the M365 learning pathways 4.0 web part to the SharePoint App Catalog, and then navigate to the M365 learning pathways Administration page to start the update process.

Upload the web part package:

1. Go to the GitHub custom learning repository, select customlearning.sppkg and then download it to a local drive on your PC.
2. If you're not already signed in, sign into your tenant with a Global admin credentials.
3. Select **Admin > Show All > SharePoint > More Features**.
4. Under **Apps**, select **Open**.
5. Select **App Catalog > Distribute Apps for SharePoint**.
6. Select **Upload > Choose Files**.
7. Select the customlearning.sppkg file you downloaded, then select **OK > Deploy**.
8. From the Learning Pathways site, select Learning pathways administration from the Home menu.
9. You'll see a prompt asking if you want to update, then select **Start**.
10. When the update is complete, select **Close**.

Provision the SharePoint Success Site

Once you've confirmed the following, you are ready to provision:

- You are using Global admin (formerly called the Tenant admin) credentials.
- Your tenant has the App Catalog enabled.
- You are an Administrator of the App Catalog.
- Your tenant has version 4.0 or higher of M365 learning pathways provisioned.

It's recommended that you install the SharePoint Success Site using the instructions below. As an alternative you can install the SharePoint Success Site from the look book, just make sure you follow all instructions. Before getting started, watch the provisioning instructions video

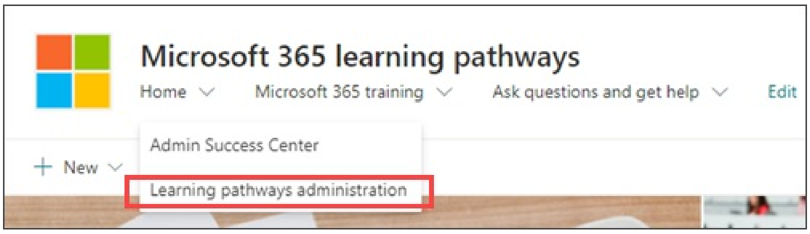
Provision the SharePoint Success Site to your tenant from the Learning pathways administrative page

1. Navigate to office.com or your organization's sign-in location.

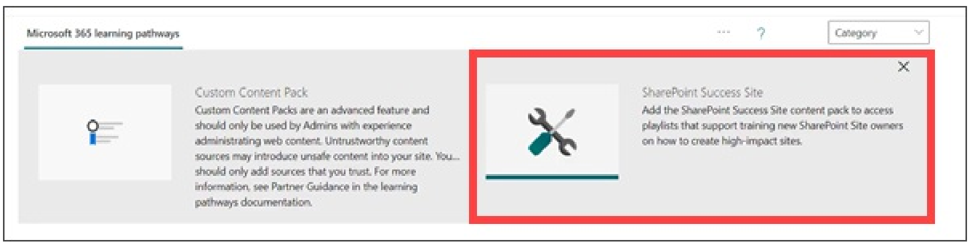
2. Sign in with your username and password.

3. Navigate to the location of the site using the URL supplied by your SharePoint administrator or select SharePoint from the Microsoft 365 home page, and then select the **M365 learning pathways** site.

4. From the learning pathways Home menu, select **Learning Pathways Administration**.



5. Select the ellipses (...) and then select **Add Content Pack**.



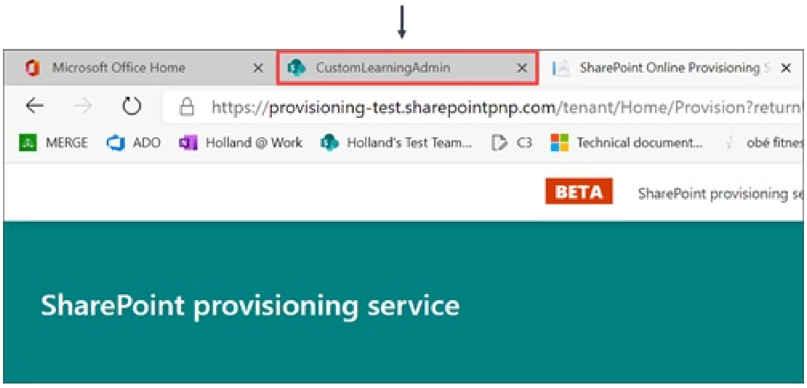
6. Select SharePoint Success Site to open the SharePoint Success Site provisioning page.

7. Select **Add to your tenant**.

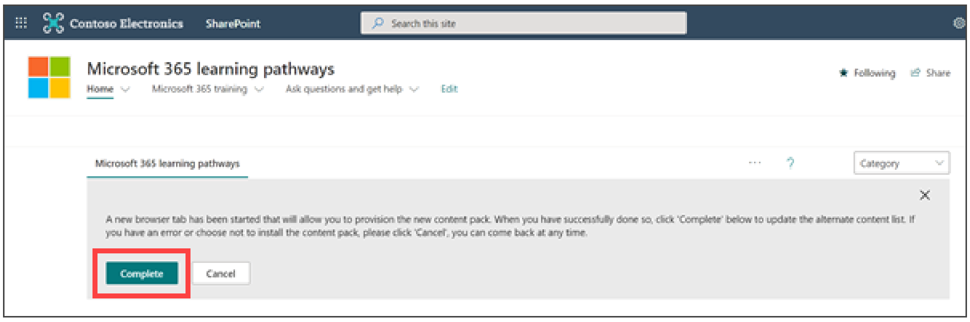
8. Fill out the email address and URL details and then select **Provision**.

9. Select **Complete**.

10. When you see **Provisioning completed** on the provisioning page, you'll see a new tab appear in your browser called **CustomLearningAdmin**. Select the **CustomLearningAdmin** tab as shown in the following image:

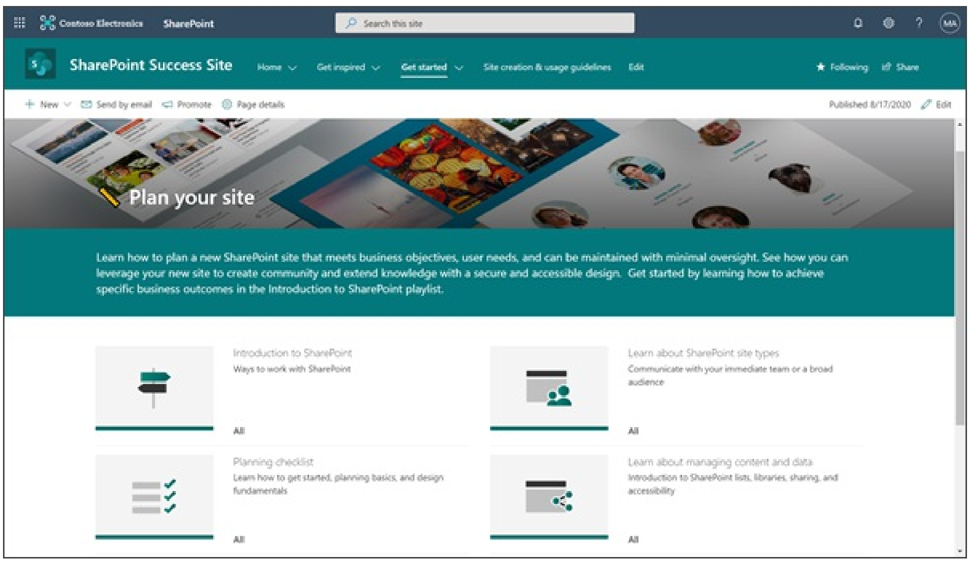


11. Then, select **Complete** as shown in the following image to complete the provisioning process:



> **IMPORTANT**
>
> Make sure to select **Complete** to complete the provisioning process.

12. To confirm the SharePoint Success Site has been successfully provisioned, go to the SharePoint site you provisioned, select **Get Started > Plan your site.** You should see the web part on the page as shown in the following image:



Add Site owners

Assign a few Site owners to grant administrative privileges to customize the site and training content. In order to hide, show, or enable playlists, users will need Site owner or Site member permissions to the M365 learning pathways site. In order to edit the look, navigation, and site content, users will need Site owner or Site member permissions to the SharePoint Success Site.

Add Site owners or members to both sites

1. From the site select **Settings**, then select **Site permissions**.
2. Select **Advanced Permission Settings**.
3. Select **Site owners** or **Site members**
4. Select **New** > **Add users to this group**, and then add the people you want to be Site owners or Site members.
5. Include a link to **Explore the site** in the sharing message, and then select **Share**.

Next steps - customize the SharePoint Success Site

Share the URLs for the M365 learning pathways administration site and the SharePoint Success site with the Site owners and members who will be responsible for customizing the site. Then, customize M365 learning pathways playlist content and the look and feel of your SharePoint Success Site to meet the needs of your organization.

Site provisioning help

- Reference troubleshooting for provisioning help
- See M365 learning pathways FAQs
- Share your feedback with us

Frequently asked questions

Question: What are the requirements for installing the SharePoint Success Site into my tenant environment?

Answer:

- Ensure SharePoint Online is enabled in your environment.
- The individual that will provision the SharePoint Success Site must be the global admin (formerly called the Tenant admin) of the target tenant for install.
- The tenant where the site will be provisioned must have:
  - The App Catalog installed
  - Version 4.0 or higher of M365 learning pathways installed

Question: Can I provision the site from the look book?

Answer: Yes, follow the guidance on how to provision from the look book.

Question: Who has permission to provision the SharePoint Success Site?

Answer: The Global admin (formerly called the Tenant admin) are required.

Question: I have installed the SharePoint Success Site successfully, but I'm not able to get the Success Site content from the M365 learning pathways web part loaded on my site. What should I do?

Answer:

It is likely that the content pack has not been fully installed. You must return to the **CustomLearningAdmin** page that will appear when site provisioning is done to complete the installation. Confirm you have followed steps 10 through 12 above. Review the provisioning video for more detail.

Question: Who has permission to customize the site template?

Answer: The Global admin (formerly called the Tenant admin) or Site owner permissions.

Question: Who can create custom playlists and hide or show content in M365 learning pathways?
Answer: The Site collection administrator and Site owner permissions of M365 learning pathways.

Question: Who has permissions to use the SharePoint Success Site as a user?
Answer: Microsoft 365 user permissions or SharePoint Site visitor permissions or higher.

Customize the SharePoint Success Site

11/2/2020 • 9 minutes to read • Edit Online

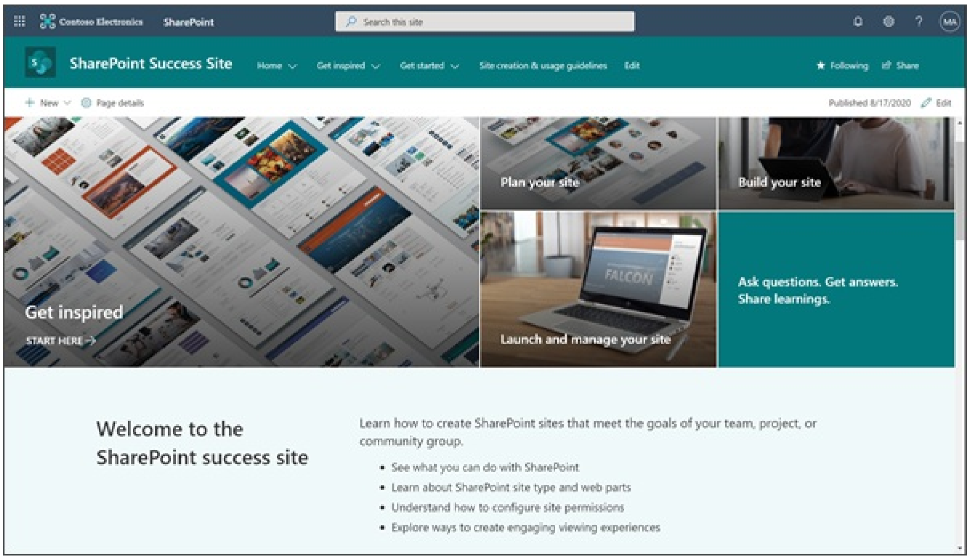
The SharePoint Success Site is a ready to deploy, up-to-date, and customizable SharePoint communication site that helps your organization maximize the adoption of SharePoint. The SharePoint Success Site helps end users improve the quality and impact of the sites they build for internal audiences, while helping ensure they follow your organization's site usage guidelines.

The SharePoint Success Site is pre-populated with web parts and content to guide your viewers through the most up-to-date SharePoint site creation training content. However, there are several opportunities to customize the experience to better suit your organization's goals and usage policy. Learn about what's included in a SharePoint Success Site, and then get started customizing.

> **IMPORTANT**
> You must have Site owner or Site member permissions to the SharePoint Success Site and the M365 learning pathways administrative page in order to make customizations..

The SharePoint Success Site consists of three parts:

1. **SharePoint communication site** - The site comes pre-populated with content and web parts that can be further customized to fit the needs of your organization.
2. **Microsoft 365 learning pathways** - M365 learning pathways is a solution that enables you to leverage existing content produced by Microsoft, as well as the ability to create and enable your own training playlists.
3. **Up-to-date SharePoint training content feed** - Content in the SharePoint Success Site is updated by Microsoft as SharePoint evolves and can be customized to align with your organization's site creation policy.



Before you share the site with end-users

There are several customization opportunities to align the site content, look, and feel with your organization. Before you publish your site and share it with users, review and customize the following elements:

- Training content in M365 learning pathways
- The SharePoint Success Site template
- The Yammer conversation, People, and Forms web parts
- Content in the site usage guidelines page
- Content in the success story page
- Branding details like the site logo and theme
- Navigational elements

Summary of site requirements and permissions

Before getting started customizing, ensure that the SharePoint Success Site has been set up by your SharePoint administrator. You need to be a Site owner or Site member for **both** M365 learning pathways *and* the SharePoint Success Site in order to have permission to make site customizations.

If you're not sure your tenant has the site, contact your SharePoint administrator to verify that the SharePoint Success Site been provisioned and ask for the M365 learning pathways and SharePoint Success Site URLs. If you are the Global admin (formerly called the Tenant admin) and M365 learning pathways has not been provisioned, see the provisioning guidance.

Who has permissions to customize the site template?

- Global admins and SharePoint admins
- SharePoint Site owner or Site member level permissions

Who can create custom playlists and hide or show content in M365 learning pathways?

- The Site collection administrator for M365 learning pathways
- SharePoint Site owner or Site member permissions for M365 learning pathways

Who has permissions to use the SharePoint Success Site as a user?

- Office 365 user permissions or SharePoint Site visitor permissions or higher

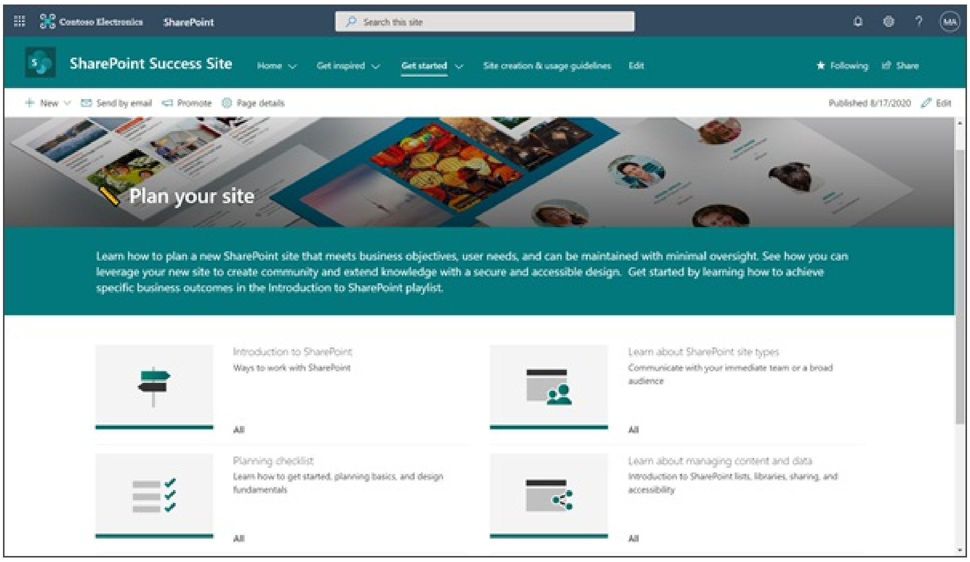
Get started customizing

Once you confirm the necessary access and permission to customize the site, you are ready to get started with the customization process. The SharePoint Success Site is hosted in your Microsoft 365 tenant, so you'll need to sign into Microsoft 365 and then navigate to the site.

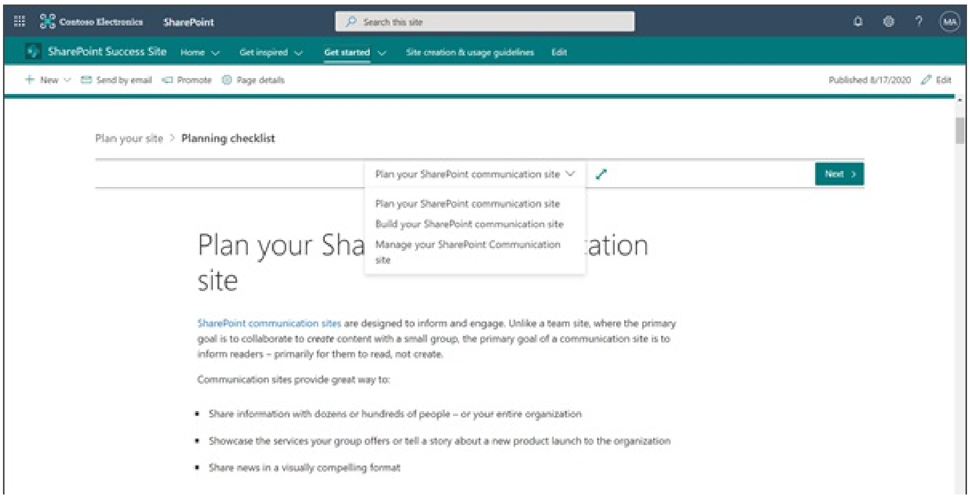
Sign in

1. Open a web browser and navigate to office.com or your organization's sign-in location.
2. Sign in with your username and password.
3. Navigate to the location of the site using the URL supplied by your tenant administrator or select SharePoint from the Microsoft 365 home page, and then select the **SharePoint Success Site**.

Explore and review the pre-populated training content



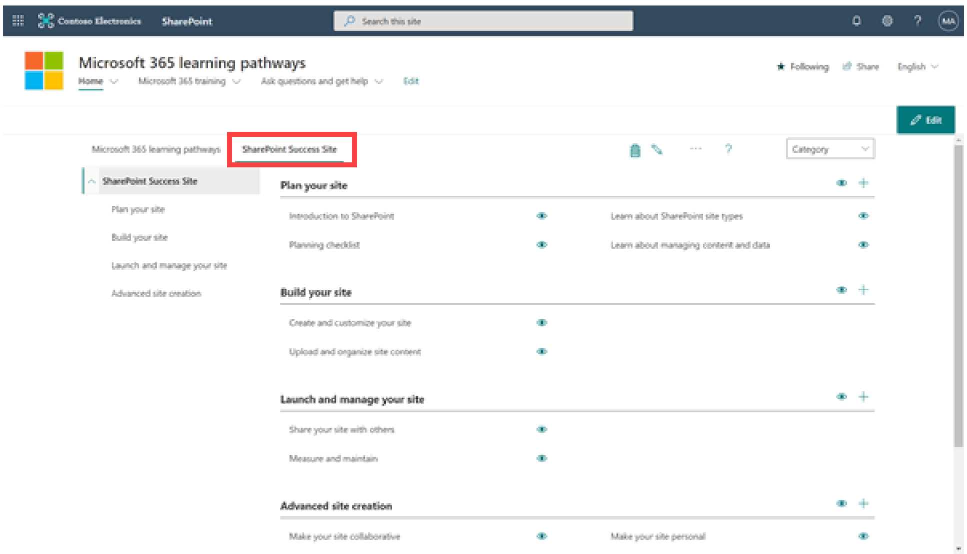
Review the **Plan, Build, Launch and manage, and Advanced** playlist sections to see the full suite of Microsoft curated content available in the SharePoint Success Site.



Select a topic, and navigate through content using controls at the top of the article

Select content categories and subcategories, and then navigate through the playlist using arrows and bread crumbs in the control bar to get a sense for how the SharePoint Success Site content is organized and displayed.

Customize playlist content



Navigate to the Microsoft 365 learning pathways admin page:

1. Navigate to the Microsoft 365 learning pathways by selecting **Home > Administration**.
2. Next, select the **gear icon** in the web part.
3. Then, select **Home > Learning pathways administration**.
4. Select the **SharePoint Success Site** tab.

Show or hide sections to the playlist content

Select which content to display in your SharePoint Success Site by hiding and showing subcategories of content. For example, if you don't want users to have access to the Advanced site creation section, you can hide that subcategory so it won't be visible to end-users. Decide which content is appropriate for the purpose of your SharePoint Success Site.

> **IMPORTANT**
>
> Hiding playlists does not hide the associated page in the SharePoint Success Site, nor will adding custom playlists automatically create site pages for them. Add or delete pages within the site as needed.

Add your own custom playlists

With Microsoft 365 learning pathways, you can create custom playlists that are tailored to the unique needs of your organization. For example, create a playlist for team site integration with Microsoft Teams.

Customize the look and feel of your site

The following sections of the SharePoint Success Site can be customized to meet your requirements, prior to sharing with end users. There are several different ways you can make the SharePoint Success Site template your own. Customize the following elements of your site to fit the need of your organization:

- Update the SharePoint Success Site branding to align with your organization.
- Customize the Hero web part to include images of real sites in your organization where possible.
- Add web parts to your site as needed.
- Customize the page layouts as needed.
- Add new pages to additional support or training resources.

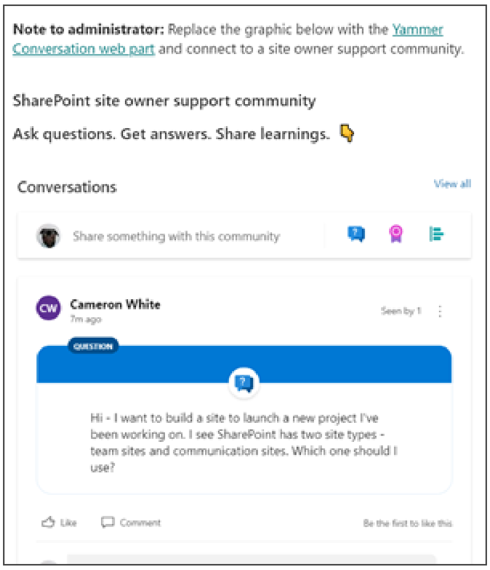
Customize the site navigation

As a Site owner you have full control of the site navigation. Use the following resources to help you make changes that align with business outcomes:

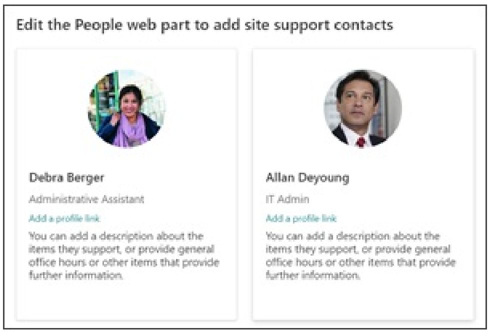
- Customize the site navigation.
- Associate this site with a hub.
- Use audience targeting to target specific navigational links to specific users. For example, in the **Home** navigation drop down you will see a shortcut to the M365 learning pathways administration page. Target that page to Site owners for the SharePoint Success Site to prevent end-users from seeing it.
- Delete unwanted pages if you need to.

Customize specific web parts

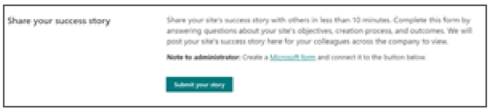
1. **Yammer conversations web part** - Use a Yammer web part to connect new SharePoint Site owners with extra support from current SharePoint Site owners and admins. Connect your Yammer community to the Yammer conversations web part.



2. **People web part** - Edit the People web part to display contact information so new Site owners can reach out for help.

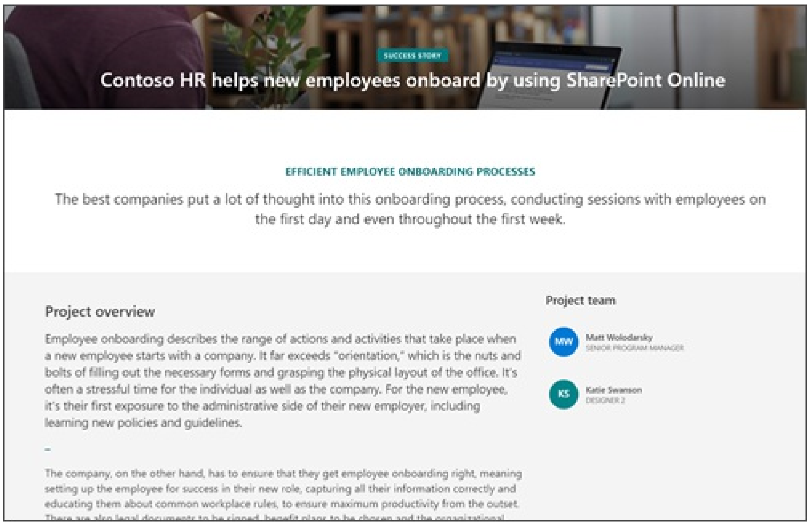


3. **Button web part** - Edit the Button web part to link to a Microsoft Form to collect success stories from Site owners. Consider using the Forms web part to embed a custom form that allows SharePoint Site owners to easily share their success stories.



Customize the Success stories page

The success stories section is a gallery for organizations to showcase internal SharePoint site success stories to inspire new Site owners with their site creation.



If available, add SharePoint success stories to your portal. If there are no ready-to-publish success stories, consider working with internal partners to create SharePoint successes by building high priority sites that align with business outcomes. Highlighting these “early wins” will help inspire others in the organization on the possibilities for using SharePoint themselves to achieve business outcomes.

Here are some sample questions to consider using in your form:

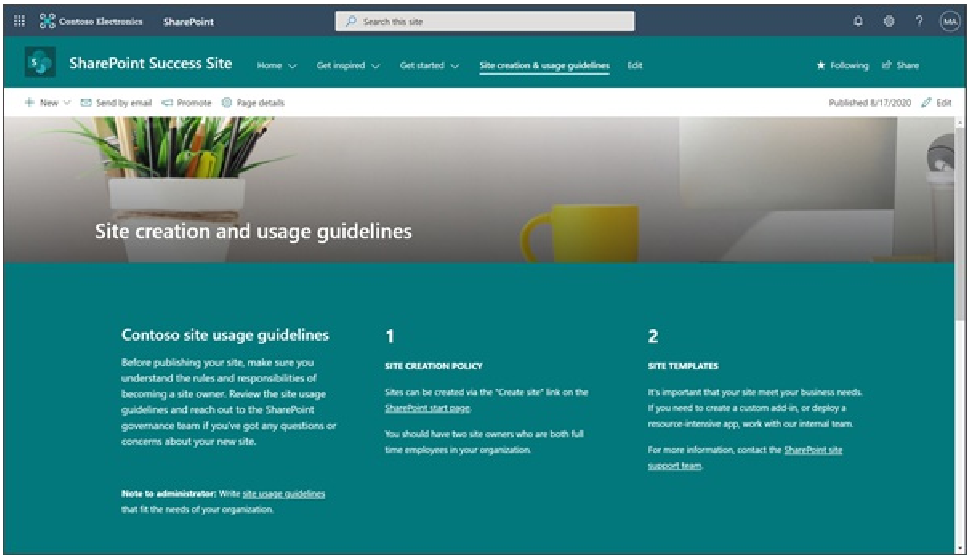
- Name of solution
- Project team members
- Who is the sponsor of the project?
- What Microsoft 365 technologies (e.g., SharePoint, Yammer, Stream, Flow) were used as part of the solution?
- What were the reasons for building the SharePoint site?
- Provide a description of the solution
- What impact or results has the SharePoint site generated?
- What best practices for planning and implementing your solution would you recommend to other who are building their own SharePoint site?

Learn more about how to create a form using Microsoft Forms.

Or, delete unwanted pages if you do not want to include this page in your site.

Customize the Site creation guidelines page

To ensure the proper use of SharePoint in your organization it is important to communicate your site usage guidelines to new and existing site owners. This should include guidelines for how people should create sites in your tenant, design standards, and how people should share information using SharePoint and Microsoft 365.



The example site creation and usage guidelines are not intended to be a final policy document. Once you have created your own unique usage guidelines, remove the content from the Site usage guidelines page and replace it with your organization’s usage guidelines. See how to create and use modern pages on a SharePoint site.

Create site usage guidelines that are appropriate for your organization by reviewing our site usage guidelines checklist that will help you create guidelines that:

- Inspire discussion and consideration amongst your stakeholders on important site usage policies.
- Provide links to resources that can help you better understand the options related to key policy decisions.
- Provide sample text to get you started in creating your own policies.

Here are some topics to consider as you create your own site creation and usage guidelines:

- How to get a new SharePoint site
- Guidelines for using site templates

- Site design, branding, and customization
- Rules for sharing and permissions
- Capacity guidelines
- Site lifecycle policy

Provide contact information for SharePoint support

If your organization has an intranet team that will be supporting site owners, consider profiling the intranet team members on the SharePoint Success Site homepage using the People web part. The home page of the SharePoint Success Site has a People web part you can use to add your own Intranet team. If you will not have a dedicated team supporting site owners, remove the current People web part.

Share the site with end-users

Share your site with others.Partner with others in your organization to ensure the SharePoint Success Site is widely known and adopted.

Key success factors to managing the SharePoint Success Site:

- Celebrate the launch of your SharePoint Success Site.
- Create and post news announcing the new resource.
- Ensure users have an outlet for questions and feedback.
- Plan to review the SharePoint Success site as needed to ensure content and site usage policies are still relevant .
- Build culture and community by integrating a Yammer web part.
- Integrate and customize your organization’s high-value training content.

Adoption and awareness strategy

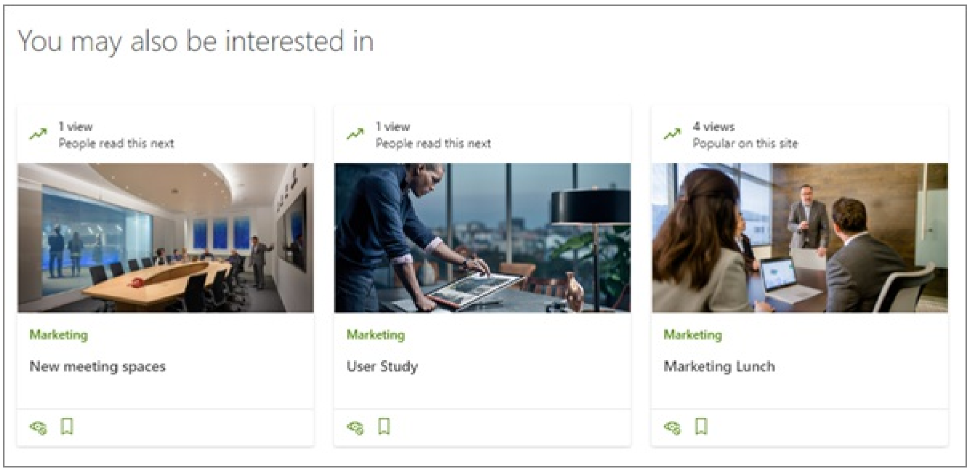
To help build, grow, and sustain your SharePoint adoption efforts, its recommended to create a SharePoint user group community in Yammer. Your SharePoint champions and power users can answer SharePoint related questions posted in the Yammer group and encourage site owners to share their successes and best practices. See the champions guidance for more information on how to identify and build a successful champions program.

To increase visibility and engagement within your portal champions community, integrate the Yammer group hosting your community into the SharePoint Success Site using the Yammer conversations web part.

How SharePoint page recommendations work

1/8/2021 • 2 minutes to read • Edit Online

SharePoint recommendations on modern pages help you and your users discover pages and news in your organization. At the bottom of news posts and pages, you'll see recommendations especially for you or your users. Recommendations show below the heading **You may also be interested in**.



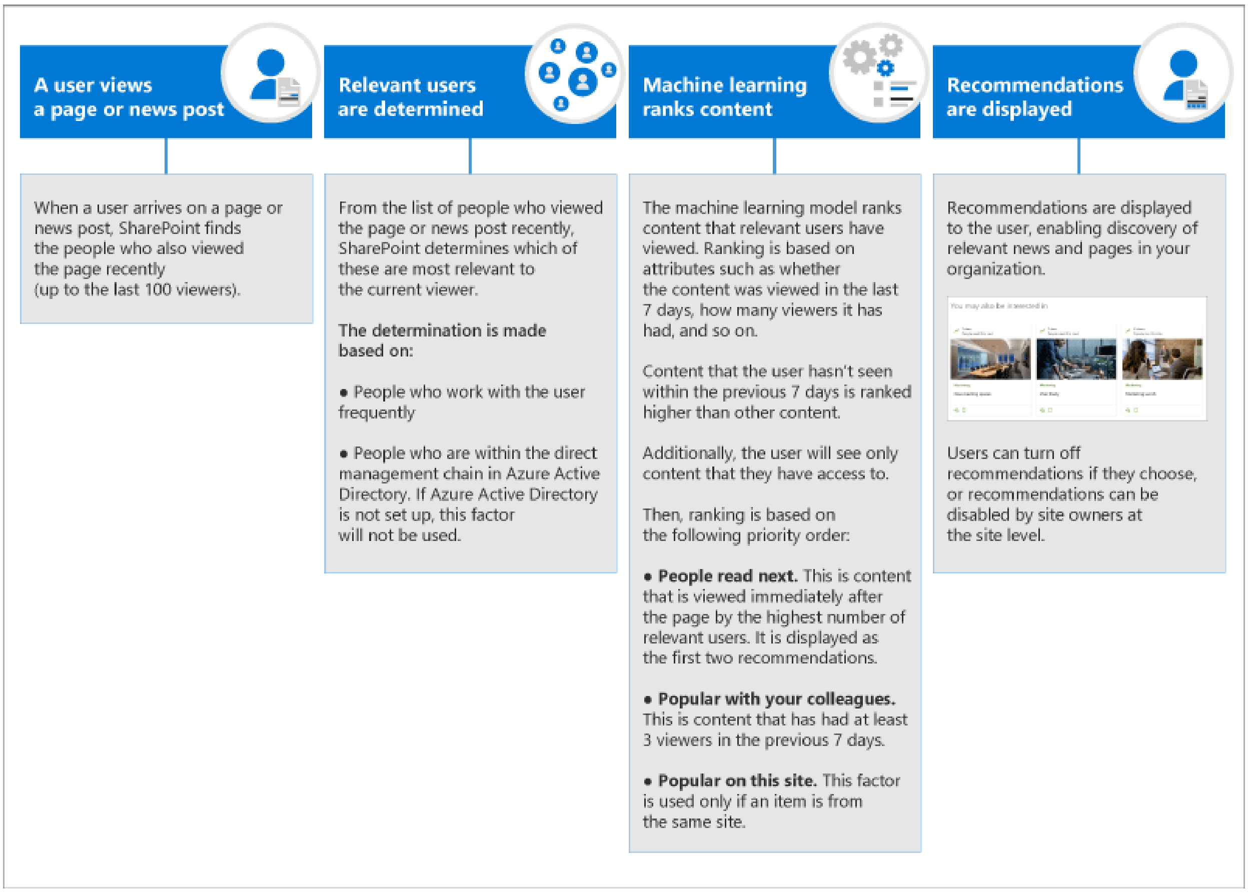
> **NOTE**
> This feature is in an early release phase, and is not yet available to all users.

Recommendations are shown on all newly-created pages and news posts by default.

How are recommendations determined for each user?

The recommendations that users see on their pages are based on what their colleagues have read next; what is popular with their colleagues; and what is popular on the site. Only pages and posts that users have access to are shown.

Here is a diagram that shows how recommendations are determined in more detail (scroll down for a text version of this diagram):



How to disable recommendations

To learn how to disable at the page and site level, see SharePoint page recommendations.

In the article linked above, you'll learn the three different ways to hide or disable recommendations:

- Users can hide individual recommendations
- Page authors can turn off recommendations for the pages they create
- Site owners can disable recommendations at the site level

Recommendations can't be disabled for an entire tenant.

How are recommendations determined for each user?

This is a text version of the diagram above.

A user views a page or news post When a user arrives on a page or news post, SharePoint finds the people who also viewed the page recently (up to the last 100 viewers).

Relevant users are determined From the list of people who viewed the page or news post recently, SharePoint determines which of these are most relevant to the current viewer. The determination is made based on:

- People who work with the user frequently
- People who are within the direct management chain in Azure Active Directory. If Azure Active Directory is not set up, this factor will not be used.

Machine learning ranks content

The machine learning model ranks content that relevant users have consumed according to a variety of attributes, such as whether the content was viewed in the last 7 days, how many viewers it has had, and so on.

Content that the user hasn't seen within the previous 7 days is ranked higher than other content. Additionally, the user will see only content that they have access to Then, ranking is based on the following priority order:

People read next. This is content that is viewed immediately after the page by the highest number of relevant users. It is displayed as the first two recommendations.

Popular with your colleagues. This is content that has had at least 3 viewers in the previous 7 days.

Popular on this site. This factor is used only if an item is from the same site.

Modernize your root site

11/2/2020 • 5 minutes to read • Edit Online

When Microsoft SharePoint is set up for an organization, a root (or top-level) site is created. Before April 2019, the site was created as a classic team site. Now, a communication site is set up as the root site for new organizations. If your environment was set up before April 2019, you can modernize your root site in three ways:

- If you have a different site that you want to use as your root site (a communication site or modern team site that isn't connected to an Office 365 group), replace (swap) the root site with the other site.
- If you want to keep using the classic team site but add a new modern home page and enable full-width pages with horizontal navigation, enable the communication site experience on the site.
- If you want to continue using the classic team site, enable the modern site pages library experience and set a modern page as the home page of the root site. This gives users a modern team site experience with the left navigation.

> **IMPORTANT**
> Before you launch an intranet landing page at your root site location, we strongly encourage you to review the guidance about launching healthy portals.
> Some functionality is introduced gradually to organizations that have opted in to the Targeted release option in Microsoft 365. This means that you might not yet see some features described in this article, or they might look different.

What's the root site?

The root site for your organization is one of the sites that's provisioned automatically when you purchase and set up a Microsoft 365 or Microsoft 365 plan that includes SharePoint. The URL of this site is typically *contoso*.sharepoint.com, the default name is "Communication site," and the owner is Company Administrator (all global admins in the organization). The root site can't be connected to a Microsoft 365 group.

> **WARNING**
> The root (top-level) site for your organization can't be deleted. If you're a global or SharePoint admin in Microsoft 365, you can replace the root site with a different site.

Replace your root site

Before you begin, make sure you:

1. Note any "Featured links" that have been added on the SharePoint start page. You'll need to add them again after you replace the root site. Learn how
2. Review your source site to make sure it has the same policies, permissions, and external sharing settings as your current root site.
3. Communicate the upcoming change to users. This can help reduce user confusion and calls to your help desk. If users are using files on the sites you're replacing, ask them to close the files and check the site recycle bin to make sure it contains no files they want to keep.

By default, a site redirect will be created that will redirect traffic from the source site to the root site. For info about site redirects, see Manage site redirects.

If you've turned on audit log search, the following events can be recorded:

- Scheduled site swap: A site replacement (swap) was scheduled at this time
- Swapped site: A site replacement (swap) completed successfully at this time
- Failed site swap: A site replacement (swap) failed at this time and won't be tried again

Limitations

- The site you select as the new root site must be a communication site (SITEPAGEPUBLISHING#0) or a modern team site that isn't connected to a Microsoft 365 group (STS#3) and where **the publishing feature has never been activated.**
- The current root site can't be connected to a Microsoft 365 group.
- When you replace the root site, both the current site and the new site can't be hub sites or associated with a hub. If either site is a hub site, unregister it as a hub site, replace the root site, and then re-register the site as a hub site. If either site is associated with a hub, disassociate the site, replace the root site, and then reassociate the site. Learn how to manage hubs in the new SharePoint admin center
- Replacing the root site with another site replaces the entire site collection with the new site collection. If your current root site has subsites, they'll be archived.
- The site you select as the new root site must be within the same domain as the current root site.

Use the new SharePoint admin center

We recommend replacing the root site at a time when site usage is low.

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

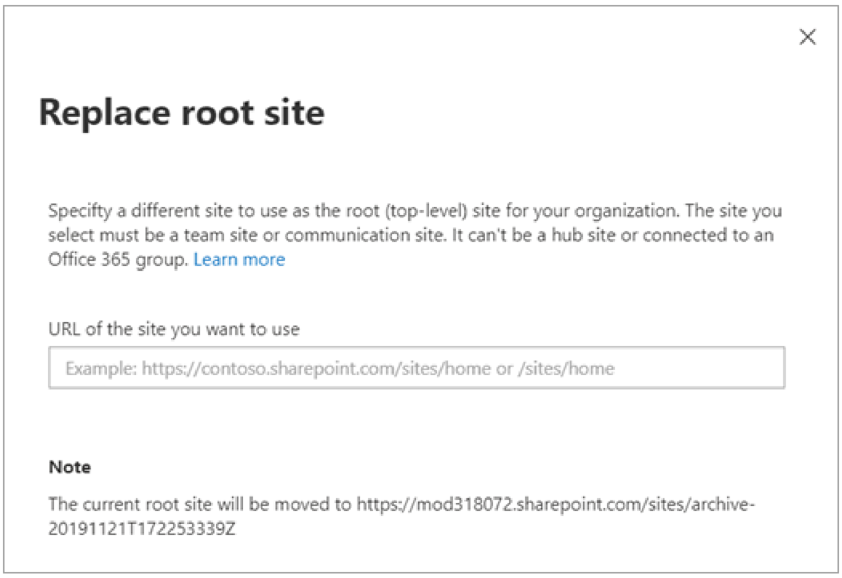
> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. In the upper right, make sure the **All sites** view is selected.

3. In the URL column, select to sort A to Z so the current root site appears at the top of the list.

4. Select the root site (https://contoso.sharepoint.com).

5. Select **Replace site**.



6. In the **URL of the site you want to use** box, enter the full or relative URL of the site that you want to become the new root site.

7. Select **Save**.

   While the root site is being replaced, it might return a "not found" (HTTP 404) error for few minutes.

   After you replace the root site, content must be recrawled to update the search index. This might take some time depending on factors such as the amount of content in these sites. Anything dependent on the search index might return incomplete results until the sites have been recrawled.

8. If the new root site was an organization news site, update the URL. Get a list of all organizational news sites

9. If you disabled site redirects, you'll need to update sharing links and any apps or files (like the OneDrive sync app and OneNote files) to refer to the new URL.

> **NOTE**
>
> For info about using PowerShell to replace (swap) the root site, see Invoke-SPOSiteSwap.
> Project Server sites might need to be validated to make sure they're still associated correctly.

Create a site

4/22/2020 • 3 minutes to read • Edit Online

This article describes how global admins and SharePoint admins in Microsoft 365 can create sites (previously called "site collections").

For info about creating site collections in SharePoint Server, see Create a site collection in SharePoint Server.

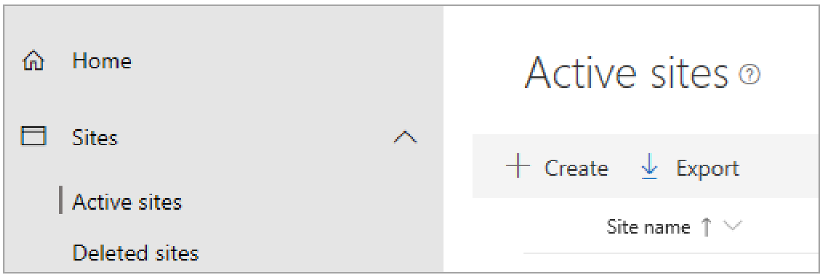
Create a site in the new SharePoint admin center

By using the new SharePoint admin center, you can create sites that use one of the new team site or communication site templates.

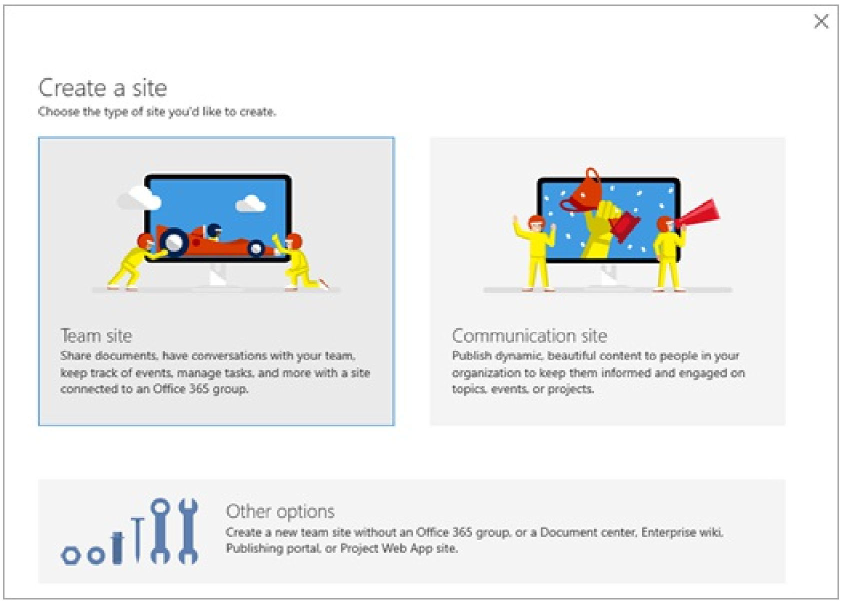
1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select **Create**.



3. Select **Team site** (to create a Microsoft 365 group-connected team site), **Communication site**, or **Other options** (to create a new team site without a Microsoft 365 group, or to create a classic site).



4. Follow the steps to specify a site name, owner, language, and other settings. When you're done, select **Finish**.

> **NOTE**
>
> If you enter a site name and another site already exists at the default address for that name, the site address will automatically be changed to an available address. For example, if you enter "Marketing" as the site name, and you already have a site at /sites/marketing, the new site will be created at /sites/marketing2. If you want to re-use the URL "marketing" for the new site, you need to permanently delete the existing site or delete the redirect at that address.

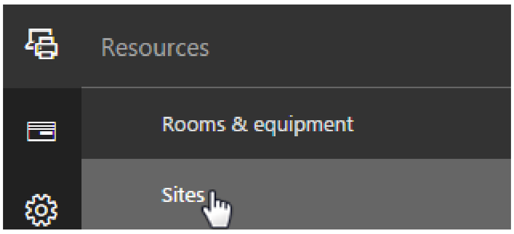
Create a classic site

We recommend using the new site templates for all your new sites. However, if you need to create a site that uses a classic template, you can do so directly from the Microsoft 365 admin center.

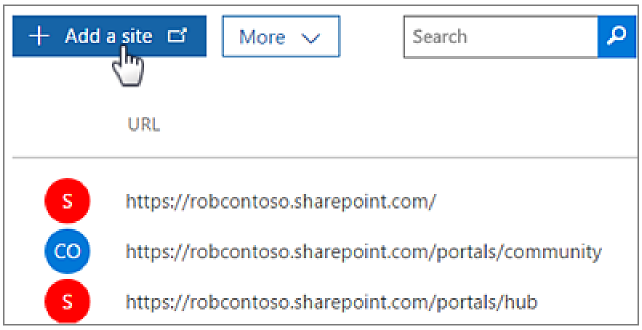
1. Sign in to https://admin.microsoft.com as a global or SharePoint admin. (If you see a message that you don't have permission to access the page, you don't have Microsoft 365 admin permissions in your organization.)

   > **NOTE**
   >
   > If you have Office 365 Germany, sign in at https://portal.office.de. If you have Office 365 operated by 21Vianet (China), sign in at https://login.partner.microsoftonline.cn/. Then select the Admin tile to open the admin center.

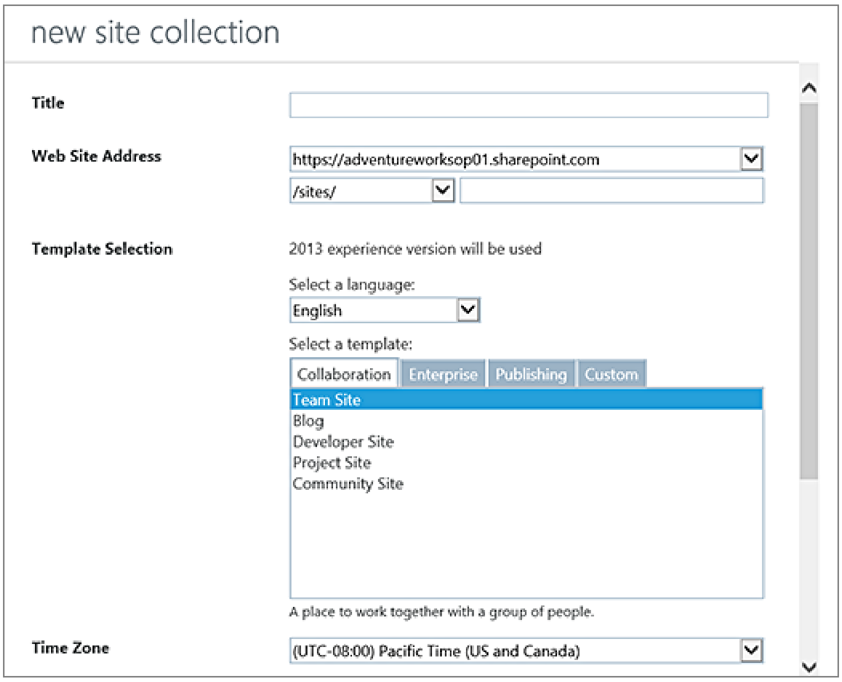
2. In the left pane, select **Resources** > **Sites**. (You may need to select **Show all** to see the Resources option.)



3. Select **Add a site**.



4. Fill out the properties for the site:



- In the **Title** box, enter a name for the site.
- In the **Web Site Address** drop-down lists, select a domain name and a URL path — either **/sites/** or **/teams/** — and then type a URL name for the site.
- In the **Template Selection** section, in the **Select a language** drop-down list, select a language for the site. You can enable the SharePoint multiple language interface on your sites, but the primary language for the site will remain the one you select here.

> **NOTE**
>
> It's important to select the appropriate language for the site, because once it's set, it cannot be changed. After creating a site, verify the locale and regional settings are accurate. (For example, a site created for Chinese will have its locale set to China.)

- In the **Template Selection** section, under **Select a template**, select the template that most closely describes the purpose of your site.

> **TIP**
>
> For more information about the classic templates, see Using templates to create different kinds of SharePoint sites.

- In the **Time Zone** box, select the time zone that's appropriate for the location of the site.
- In the **Administrator** box, enter the user name of the person you want to be the site administrator. You can also use the **Check Names** or **Browse** button to find a user to make site administrator.
- In the **Storage Quota** box, enter the number of megabytes (MB) you want to allocate to this site. Do not exceed the available amount that is displayed next to the box.
- In the **Server Resource Quota** box, accept the resource quota default. This setting no longer affects the resource amounts available for the site.

5. Select **OK**.

Delete a site

6/5/2020 • 4 minutes to read • Edit Online

When you, as a global or SharePoint admin in Microsoft 365, delete a site (previously called a "site collection"), it's retained as a deleted site for 93 days. Deleting a site deletes everything within it, including:

- Document libraries and files.
- Lists and list data.
- Site settings and history.
- Any subsites and their contents.

You should notify the site admins and any subsite owners before you delete a site so they can move their data to another location, and also tell users when the sites will be deleted.

> **WARNING**
> We do not recommend deleting the root site for your organization. If you do, all your SharePoint sites will be inaccessible until you restore the site or create a new root site. Instead of deleting the root site, we recommend replacing it. Learn more about the root site and how to replace it

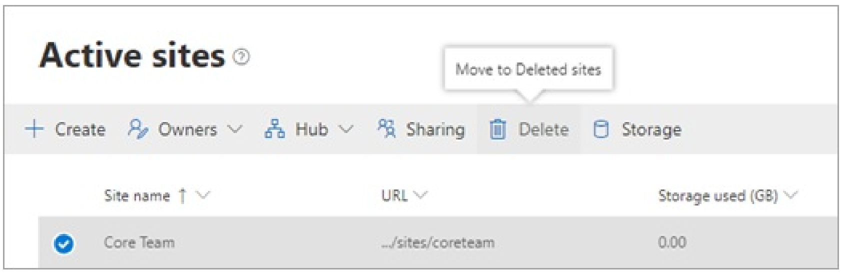
Delete a site in the new SharePoint admin center

By using the new SharePoint admin center, you can delete both classic and modern sites. Both global and SharePoint admins can now delete sites that belong to Microsoft 365 groups. Deleting these sites will delete the group and all its resources, including the Outlook mailbox and calendar, and any Teams channels.

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. In the left column, select a site.
3. Select **Delete**, and to confirm, select **Delete**.



> **NOTE**
>
> To delete a hub site, you first need to unregister it as a hub site.
> Deleted Microsoft 365 groups are retained for only 30 days.
> For info about deleting a site by using PowerShell, see Remove-SPOSite.

Permanently delete a site

To reuse a URL from a deleted site (recreate a site), you need to permanently delete the site. After the site is permanently deleted, it might take up to 24 hours for the URL to become available. On the Deleted sites page of the new SharePoint admin center, you can permanently delete all sites except those that belong to Microsoft 365 groups.

1. Go to the Deleted sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Deleted sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Deleted sites page.

2. In the left column, select a site.

3. Select **Delete**, and to confirm, select **Delete**.

To permanently delete sites (including Microsoft 365 group-connected team sites) by using PowerShell, follow these steps:

1. Download the latest SharePoint Online Management Shell.

   > **NOTE**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
   > On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

```
Remove-SPODeletedSite -Identity https://contoso.sharepoint.com/sites/sitetoremove
```

(Where https://contoso.sharepoint.com/sites/sitetoremove is the URL of the site you want to permanently delete). For more info about using this command, see Remove-SPODeletedSite.

Summary of options

SITE TYPE	HOW TO DELETE	HOW TO PERMANENTLY DELETE
Root site	Not recommended. Replace the root site with a different site. When the site is no longer a root site, its URL will be /sites/archive-*datetime*, and you can delete it from the Active sites page of the new SharePoint admin center or by using PowerShell	From the Deleted sites page of the new SharePoint admin center or by using PowerShell
Communication sites	Delete them from the Active sites page of the new SharePoint admin center or by using PowerShell	From the Deleted sites page of the new SharePoint admin center or by using PowerShell
Microsoft 365 group-connected team sites	Delete Microsoft 365 groups and all their resources from the Microsoft 365 admin center, the Active sites page of the new SharePoint admin center, or by using PowerShell	From PowerShell only
Hub sites (those designated with " (Hub site)" in the Hub column)	Unregister them as hub sites from the Active sites page of the new SharePoint admin center, or by using PowerShell, and then delete them based on their site type	Based on their site type
Classic sites	Delete them from the Active sites page of the new SharePoint admin center or by using PowerShell	From the Deleted sites page of the new SharePoint admin center or by using PowerShell

NOTE

Sites associated with a hub can be deleted like any other site based on their template.

See also

User instructions for deleting sites and subsites

Restore deleted sites

6/5/2020 • 2 minutes to read • Edit Online

Deleted SharePoint sites are retained for 93 days. After 93 days, sites and all their content and settings are permanently deleted, including lists, libraries, pages, and any subsites.

NOTE

If you need to retain content for a minimum period of time to comply with industry regulations or internal policies, you can create a retention policy to keep a copy of it in the Preservation Hold library. For info, see Overview of retention policies.
For info about restoring items within a site, see Restore items in the Recycle Bin of a SharePoint site.
For info about restoring deleted sites in SharePoint Server, see Restore deleted site collections using Microsoft Powershell.

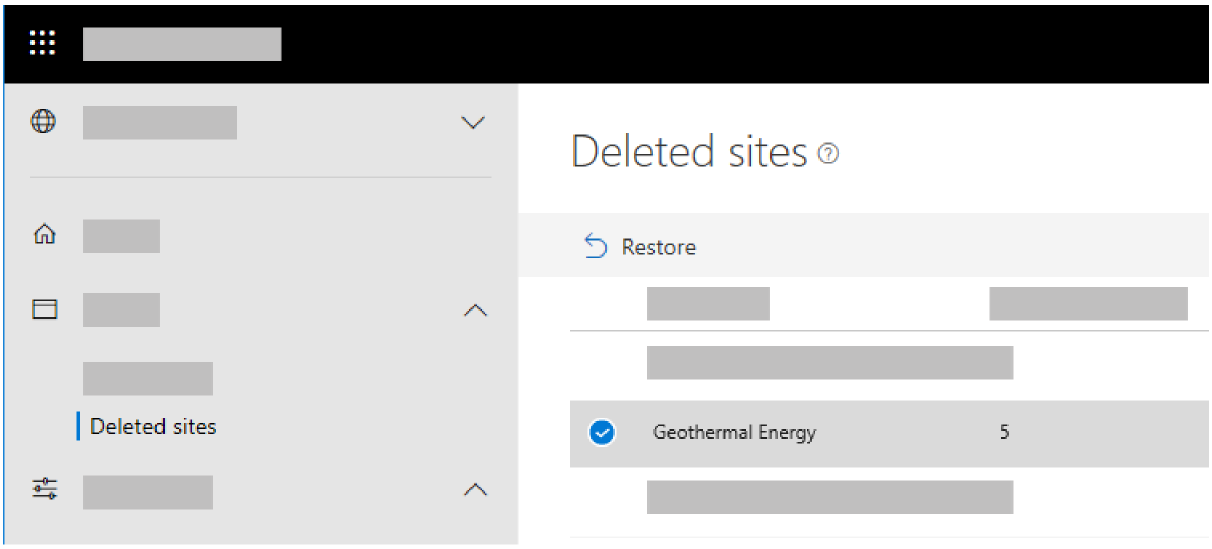
Restore a deleted site in the new SharePoint admin center

In the new SharePoint admin center, you can delete and restore all the new types of sites. You can do this even as a SharePoint admin - you don't need to be a global admin.

1. Go to the Deleted sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

NOTE

If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Deleted sites page.
If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Deleted sites page.



NOTE

You can sort and filter deleted sites the same way you sort and filter sites on the Active sites page. You can also sort and filter deleted sites by Time deleted.

2. Select the site you want to restore.

3. Select **Restore**. (If you don't see the **Restore** button, make sure only one site is selected. The button won't appear if multiple sites are selected.)

> **NOTE**
>
> Restoring a site that belongs to a Microsoft 365 group restores the Microsoft 365 group and all its resources. Note that the other group resources are retained for only 30 days, whereas the site is retained for 93. If the other group resources have been deleted, you can use the PowerShell command Remove-SPODeletedSite to permanently delete the site.
> For info about permanently deleting sites from the Deleted sites page, see Permanently delete a deleted site.

Related topics

Restore deleted items from the site collection recycle bin

Manage site admins

4/22/2020 • 2 minutes to read • Edit Online

This article describes how global admins and SharePoint admins in Microsoft 365 can add and remove site admins (previously called "site collection admins"). If you're an owner of a communication site, or a site that belongs to a Microsoft 365 group, see Manage your SharePoint site settings for info about giving people access to your site. If you're an admin for a classic site, see Manage your SharePoint site settings.

> **NOTE**
> If you're a global admin and want info about assigning other users the SharePoint admin role in Microsoft 365, see Assigning admin permissions.

Add or remove site admins in the new SharePoint admin center

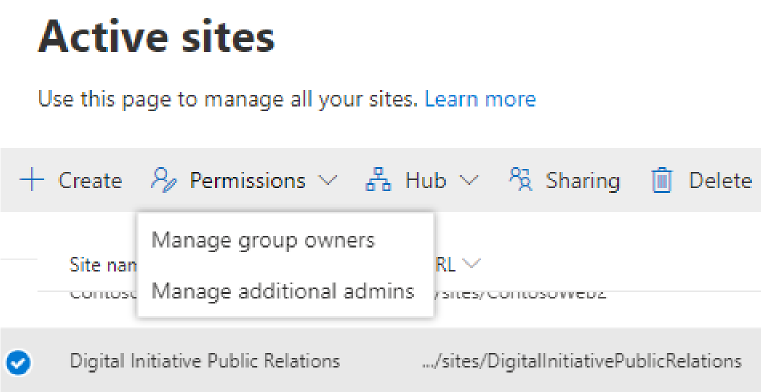
By using the new SharePoint admin center, you can change the owners for sites that use the new team site and communication site templates. You can also add and remove group members in the Microsoft 365 admin center. For info, see Add or remove members from Microsoft 365 groups.

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. In the left column, select a site.

3. Select **Permissions**. For a group-connected team site, you can add and remove group owners and additional site admins. For other sites, you can add and remove site admins and change the primary admin. Note that if you remove a person as a primary admin, they will still be listed as an additional admin. For info about each role, see About site permissions.



Manage site creation in SharePoint

4/22/2020 • 2 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can let your users create and administer their own SharePoint sites, determine what kind of sites they can create, and specify the location of the sites. By default, users can create communication sites and Microsoft 365 group-connected team sites.

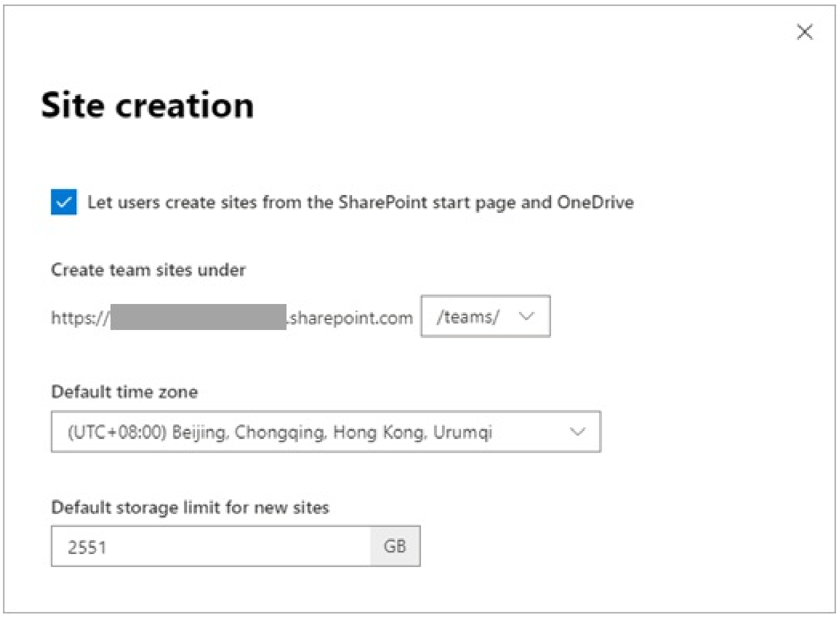
> **NOTE**
>
> Disabling site creation for users does not remove their ability to create Microsoft 365 groups or resources, such as Microsoft Teams, which rely on a group. When a Microsoft 365 group is created, a SharePoint site is also created. To restrict creation of Microsoft 365 groups and the resources that rely on groups see Manage who can create Microsoft 365 Groups.
> Some functionality is introduced gradually to organizations that have opted in to the Targeted release option in Microsoft 365. This means that you might not yet see some features described in this article, or they might look different.

Manage site creation in the new SharePoint admin center

1. Go to the Settings page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.

2. Select **Site creation**.



3. If you want users to be able to create sites from these services, select **Let users create sites from the SharePoint start page and OneDrive**.

> **NOTE**
>
> Even if you clear this check box, users may be able to create Microsoft 365 groups from other places in Microsoft 365. Each group always comes with a team site. Learn how to manage who can create Microsoft 365 groups

4. Under /sites or /teams, select to create Microsoft 365 group-connected team sites, and then select the default time zone and storage limit for new sites.

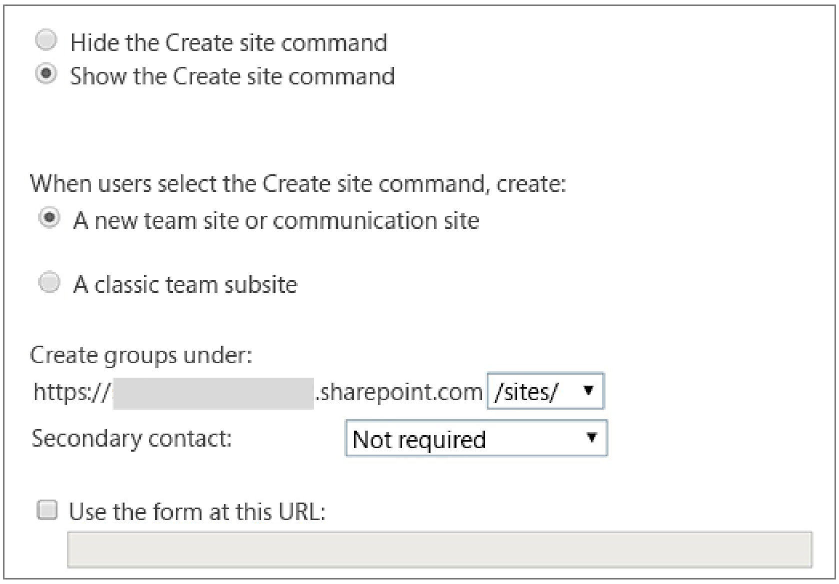
5. Select **Save**.

Manage detailed site and subsite creation settings in the classic SharePoint admin center

1. In the left pane of the new SharePoint admin center, select **Settings**. At the bottom of the page, select **classic settings page**.

2. Under **Site Creation**, select to show or hide the **Create site** command.

3. If you select **Show the Create site command**, specify the type of site that users can create.



- **A new team site or communication site**: Select to create the group-connected team sites under (/sites or /teams) and whether a secondary contact is required. To let users create sites from a custom form you've created, enter its URL in the **Use the form at this URL** box. When users select which type of site they want to create, they'll be able to access the form by clicking "See other options."

- **A classic team subsite**: Use this option to let users create only default classic sites or sites from your custom form. Specify where sites are created, and whether a site classification or secondary contact is required. To specify a custom form, enter the URL for the custom form in the **Use the form at this URL** box.

> **NOTE**
>
> For info about classifying Microsoft 365 groups, see Manage Microsoft 365 Groups with PowerShell.

4. Under **Subsite creation**, on the **Site contents** page, to create a new subsite, specify whether users can select **New** > **Subsite**.

5. Select **OK**.

Manage site storage limits

11/2/2020 • 7 minutes to read • Edit Online

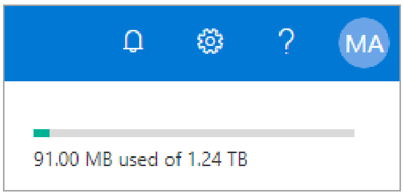
The amount of Microsoft SharePoint space your organization has is based on your number of licenses (see SharePoint Limits). If you're a global admin in Microsoft 365, you can Change storage space for your subscription if you run out.

View the total and available storage space for your organization

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. In the upper right of the page, see the amount of storage used across all sites, and the total storage for your subscription. (If your organization has configured Multi-Geo in Microsoft 365, the bar also shows the amount of storage used across all geo locations.)



> **NOTE**
>
> The storage used doesn't include changes made within the last 24-48 hours.

Set automatic or manual site storage limits

By default, your SharePoint storage is available in a central pool from which all sites can draw. You, as a global or SharePoint admin, don't need to divvy up storage space or reallocate space based on usage. That's all handled automatically: sites use what they need when they need it. If you previously set storage limits manually and switch to using pooled storage, SharePoint resets all the limits to 25 TB (25600 GB). (Note that the total storage for your organization might be less than 25 TB.)

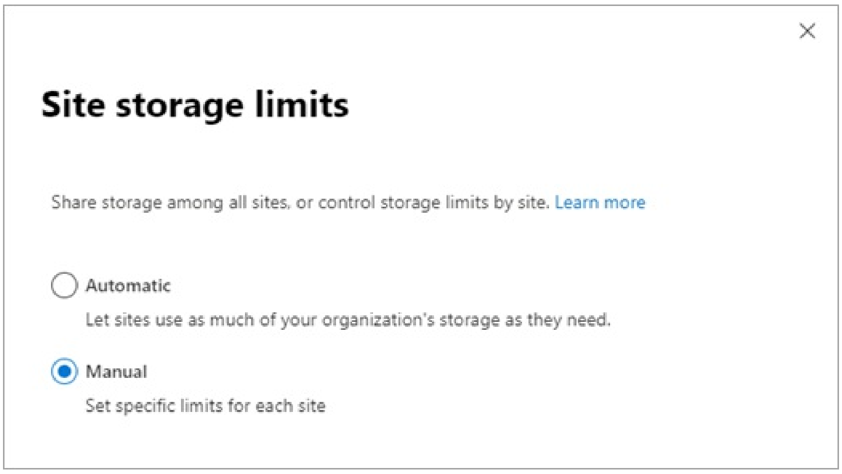
If you prefer to fine tune the storage space allocated to each site, you can set your storage management option to "manual" and specify individual site storage limits.

> **NOTE**
>
> Some functionality is introduced gradually to organizations that have opted in to the Targeted release option in Microsoft 365. This means that you might not yet see some features described in this article, or they might look different.

1. Go to the Settings page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.

2. Select **Site storage limits**.



3. Select **Automatic** or **Manual**, and then select **Save**.

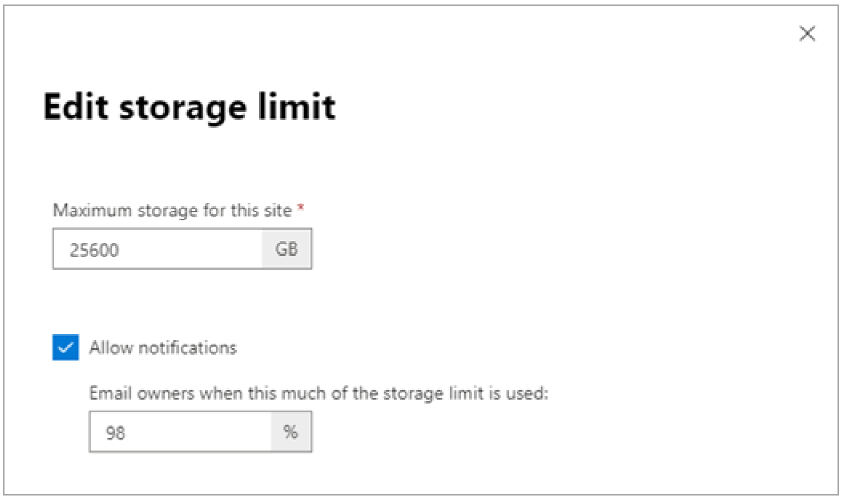
Manage individual site storage limits

Follow these steps to specify individual site storage limits when your storage management option is set to "manual." We recommend that you also set an email alert so that you and other site admins can be notified when sites are nearing the storage limit. To learn how to set the default storage limit for new sites, see Manage site creation.

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select a site, and then select **Storage**.



3. Enter the maximum storage in GB for the site.

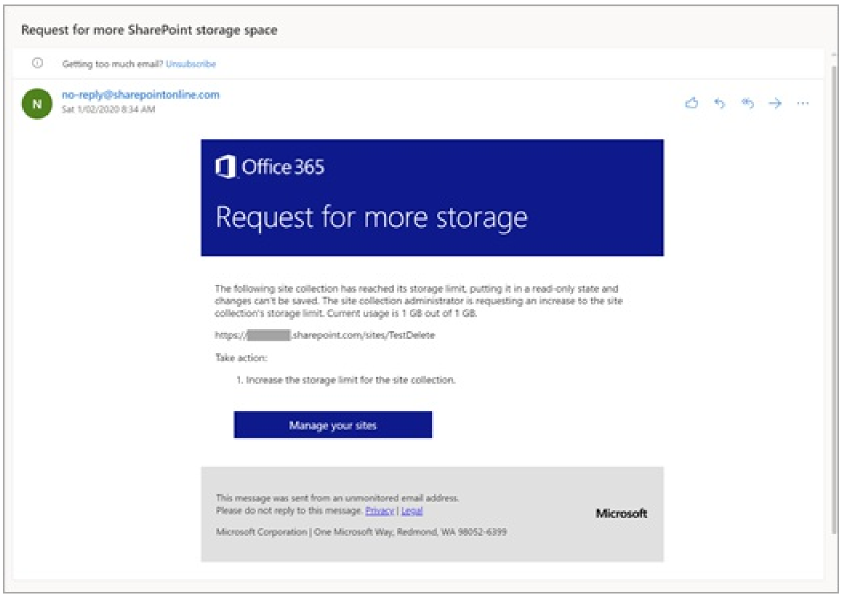
> **NOTE**
>
> The max value you can enter is 25600 GB, although this may be more space than your organization has. To learn how your total storage is calculated, see SharePoint Limits.
> If you set site storage limits in PowerShell, you enter them in MB. The values are converted and rounded down to the nearest integer to appear in GB in both the SharePoint admin center. So a value of 5000 MB becomes 4 GB. The minimum storage limit is 1 GB, so if you set a value of less than 1024 MB by using PowerShell, it will be rounded up to 1 GB.

4. Make sure **Notifications** is turned on to send an email to site admins when the site approaches the storage limit. Then, enter a value as a percent for how full you want the storage to be when the email is sent.
5. Select **Save**.

If a site runs out of storage, site admins can request more by following these steps:

1. Go to the Site Settings page.
2. Under **Site Collection Administration**, select **Storage Metrics**.
3. Select **Request more quota** in the upper right.

This sends a storage request email to the global and SharePoint admins in the organization.



Monitor site storage limits by using PowerShell

If you manage storage limits manually, you need to regularly monitor them to make sure they aren't affecting site performance. We recommend that you also set up your own alert emails to notify site admins before a site reaches the limit. The built-in storage quota warning emails are typically sent weekly for sites that have reached the specified warning level. So site admins often receive the storage quota warning email too late. For example, if the Disk Quota Warning timer job (which triggers the warning email) is scheduled weekly and sends the email warning every Sunday, but a site reaches the quota warning limit on Monday, the site admin doesn't receive the alert email for 6 days. This site could reach the maximum storage limit and be set to read-only before the site admin receives the alert email.

You can use the following Microsoft PowerShell script to monitor your sites. This script pulls the data, composes, and then sends a storage warning alerts to the site admin.

1. Download the latest SharePoint Online Management Shell.

   > **NOTE**
   >
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
   > On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Copy the following text with the variable declarations, and paste it into a text editor, such as Notepad. You must set all of the input values to be specific to your organization. Save the file, and then rename it "GetEmailWarning.ps1".

   > **NOTE**
   >
   > You can use a different file name, but you must save the file as an ANSI-encoded text file with the extension .ps1.

```
#Connect to SharePoint admin center using an admin account
#Specify the URL to your SharePoint admin center site, e.g. https://contoso-admin.sharepoint.com

$url = 'https://contoso-admin.sharepoint.com'

#Specify a folder path to output the results into
$path = '.\'

#SMTP details
$Smtp = '<SmtpServer>'
$From = '<SenderEmailAddress>'
$To = '<RecipientEmailAddress>'
$Subject = 'Site Storage Warning'
$Body = 'Storage Usage Details'

if($url -eq '') {
  $url = Read-Host -Prompt 'Enter the SharePoint admin center URL'
}

Connect-SPOService -Url $url

#Local variable to create and store output file
$filename = (Get-Date -Format o | foreach {$_ -Replace ":", ""})+'.csv'
$fullpath = $path+$filename

#Enumerating all sites and calculating storage usage
$sites = Get-SPOSite
$results = @()

foreach ($site in $sites) {
  $siteStorage = New-Object PSObject

  $percent = $site.StorageUsageCurrent / $site.StorageQuota * 100
  $percentage = [math]::Round($percent,2)

  $siteStorage | Add-Member -MemberType NoteProperty -Name "Site Title" -Value $site.Title
  $siteStorage | Add-Member -MemberType NoteProperty -Name "Site Url" -Value $site.Url
  $siteStorage | Add-Member -MemberType NoteProperty -Name "Percentage Used" -Value $percentage
  $siteStorage | Add-Member -MemberType NoteProperty -Name "Storage Used (MB)" -Value
$site.StorageUsageCurrent
  $siteStorage | Add-Member -MemberType NoteProperty -Name "Storage Quota (MB)" -Value $site.StorageQuota

  $results += $siteStorage
  $siteStorage = $null
}

$results | Export-Csv -Path $fullpath -NoTypeInformation

#Sending email with output file as attachment
Send-MailMessage -SmtpServer $Smtp -To $To -From $From -Subject $Subject -Attachments $fullpath -Body $Body
-Priority high
```

4. Where:

- **$url** is the URL of your SharePoint admin center. If the `$url` variable is left empty, you will be prompted to enter the URL of your admin center site.
- **$path** is the file system path you want the CSV file to output to.
- **<SmtpServer>** is the name of your SharePoint Migration Tool mail server.
- **<SenderEmailAddress>** is the global admin or SharePoint admin account that appears in the From line in the warning email.
- **<RecipientEmailAddress>** is the admin account that will receive the email warning.

5. In SharePoint Online Management Shell, change to the local directory where you saved the script file.

```
./GetEmailWarning.ps1
```

After the script successfully completes, a text file is created in the location that you specified in the `$path` variable in the script.

> **NOTE**
>
> If you get an error message about being unable to run scripts, you might need to change your execution policies. For info, see About Execution Policies.

Change a site address

1/8/2021 • 7 minutes to read • Edit Online

NOTE

This feature is not available for Microsoft 365 Government GCC High customers.

As a global or SharePoint admin in your organization, you can change the URL for the following types of SharePoint sites (previously called "site collections"):

- Microsoft 365 group-connected team sites
- Modern team sites that don't belong to a Microsoft 365 group
- Communication sites
- Classic team sites

NOTE

If the Publishing feature is currently activated or was previously activated for the site, then changing the site address is unsupported.

You can change only the address of the site within the URL, for example:

https://contoso.sharepoint.com/sites/*projectx*
to https://contoso.sharepoint.com/sites/*projecty*

You can't change the domain ("contoso" in the previous example) or any other part of the path. For example, you can't move the site from "/sites" to "/teams."

It can take about 10 minutes to change the site address (depending on the size of the site), and the site will be read-only during this time. We recommend changing addresses during times when site usage is low.

You can change the address of up to 100 sites at a time. To change an additional site address, wait for another change to finish.

Communicate the address change to users

Before you change the address of a site, it's important to communicate the change to site users (generally anyone with the ability to edit or view the site). This can help reduce user confusion and calls to your help desk. Review the effects of changing a site address and let users know the following information:

- When the change will happen
- What the new URL will be
- Users should close their files and not make edits during the address change
- Users should check the site recycle bin to make sure it contains no files they want to keep
- File permissions and sharing won't change

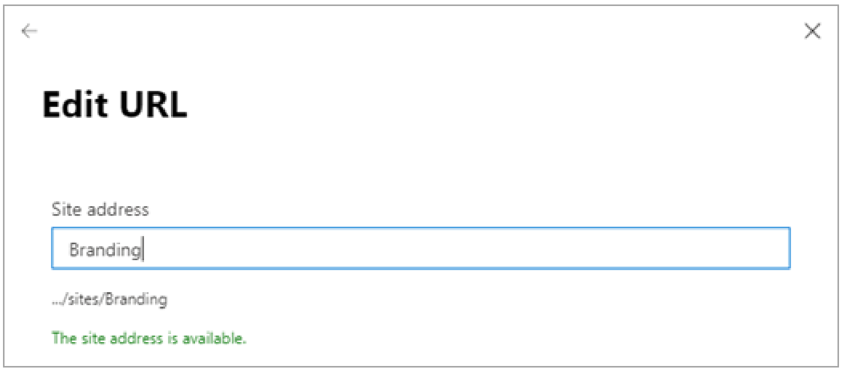
Change a site address in the new SharePoint admin center

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. To open the details pane, select the site name.

3. On the **General** tab, under URL, select **Edit**.



4. Enter the new site address, and then select **Save**.

> **NOTE**
>
> You can't change the address of hub sites, sites that are locked or on hold, Project Web App (PWA) sites, or sites that have BCS connections.
>
> When you change a site address, we create a redirect at the previous address. If you want to reuse the previous address, you need to delete the redirect. Learn how

Change site addresses by using Microsoft PowerShell

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
>
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running? After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command to verify that the site address can be changed:

```
Start-SPOSiteRename -Identity <SiteURL> -NewSiteUrl <NewSiteURl> -ValidationOnly
```

4. Run the following command to change the site address:

```
Start-SPOSiteRename -Identity <SiteURL> -NewSiteUrl <NewSiteURl>
```

For more info about this cmdlet, see Start-SPOSiteRename.

Effects of changing a site address

While the change is in progress, the site is set to read-only, and a redirect is created. After the change is complete, users are redirected to the new URL if they've saved the site as a favorite, or if they select a link to the site.

Apps

If apps in your organization refer to the site's URL, you might need to republish the apps when you change the site's address.

Custom Forms Created in PowerApps

You need to recreate the Custom Form after the site address change.

Hub sites

If the site is associated with a hub, it will need to be reassociated after the site address is changed.

InfoPath forms

InfoPath forms that refer to URLs might not work after the site address is changed.

List View web part

If a List View web part is added to a page and scoped to a specific folder in that list, the web part might display an error after the site URL is changed. To fix this issue, either edit the web part and reset the folder path or remove the web part from the page and then add it again.

Microsoft Forms

If the site is a Microsoft 365 group-connected site that has forms in Microsoft Forms, any File Upload questions in forms will break. To fix this issue, recreate the file upload questions to allow responders to upload files again.

OneNote

If users have a notebook open during the site address change, they'll see a notebook sync error. After the address is changed, the following OneNote apps will automatically detect and seamlessly sync notebooks to the new site URL:

- OneNote desktop app – Version 16.0.8326.2096 and later
- OneNote for Windows 10 – Version 16.0.8431.1006 and later
- OneNote mobile app – Version 16.0.8431.1011 and later

Users don't need to sign in again or take any other action.

Permissions

People who have permission to access the site can access the site during and after the site address change.

Power Apps

You need to reconnect the app or apps to your data source. Start by deleting the existing SharePoint connections to any lists you may have before you reconnect to your data. Once you've done that, reconnect your app to the SharePoint lists you were using. Most fields should update automatically. Certain types seem to have trouble updating and can be fixed by simply deleting the field and then undoing the delete.

Power Automate

Flows will need to be recreated after the site address change.

Recent lists inside Office apps

The Word, Excel, and PowerPoint desktop apps and apps for the web will show the new URL after the change.

Recycle bin Files in the recycle bin will be restorable as per the usual deletion timeframe.

SharePoint mobile apps for Android and iOS

The SharePoint mobile apps will detect the site's new URL. Make sure that users have updated their apps to the latest version.

SharePoint workflow 2013

SharePoint workflow 2013 will need to be republished after the site address is changed.

Sharing links

After the site address is changed, sharing links will automatically redirect to the new URL.

Site customizations and embedded code

Site customizations and embedded code that refer to URLs might need to be fixed after the site address change. Changing the site address will preserve data stored in SharePoint but won't change URL dependencies in custom solutions.

Synced locations

The OneDrive sync app will automatically detect and seamlessly transfer syncing to the new site URL after the site address has been changed. Users don't need to sign in again or take any other action. (Version 17.3.6943.0625 or later of the sync app required.) If a user updates a file while the site address is being changed, they'll see a message that file uploads are pending during the change.

Teams (for Microsoft 365 group-connected sites)

When the site address change is complete, users will be able to access their SharePoint files in the Teams app, with the following limitations.

FUNCTIONALITY	LIMITATION
Files tab in channels	The Files tab will need to be refreshed once after the address change.
Viewing files in Teams	Files shared in channels before the address was changed can be viewed in the Teams app on the channel's Files tab. They can also be viewed in Office apps for the web from the channel's Files tab or the conversation. To view Word, Excel, and PowerPoint files in the desktop apps: Select the "Open in Desktop" option from the channel's Files tab. Open the file in the Office app for the web, and then select "Open in Desktop".
Uploading files to channels	Uploading files from a computer or OneDrive to a channel conversation will work after a user has visited the Files tab for any channel in the site.
File search	Search in Teams will show files only from sites whose addresses have not been changed.
File app – Microsoft Teams page	The Microsoft Teams page in the Teams File app will work after a user has visited the Files tab for any channel in the site.
Teams mobile app	Open and download will continue to work. To edit a Word, Excel, or PowerPoint file in the site, use the Office app for the web or the desktop app. Files shared after the site address was changed can be edited in the Office mobile apps.

Manage site redirects

6/5/2020 • 2 minutes to read • Edit Online

As part of changing a SharePoint site address, moving a site to a different geo location, or swapping a site, we automatically create redirects to ensure that links pointing to the prior URL continue to work. These redirects are sites that use a special site template at the prior site URL.

For example, if you changed a site address from https://contoso.sharepoint.com/sites/*OldSiteName* to https://contoso.sharepoint.com/sites/*NewSiteName* or moved a site from https://*contoso*.sharepoint.com/sites/SiteName to https://*contosoEUR*.sharepoint.com/sites/SiteName, we'll place a redirect (Template type REDIRECTSITE#0) at the old URL, which contains special headers and logic to redirect your browser requests to the new site.

In some cases, you might want to free up the old URL to use it for a new site. To do this, you need to delete the redirect.

> **NOTE**
> After you delete a redirect, any request to that URL won't get redirected. This means that any bookmarks, links, or Shared With Me references will not be routed to the new URL.

To remove a redirect

1. Download the latest SharePoint Online Management Shell.

   > **NOTE**
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
   > On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

```
Remove-SPOSite -Identity https://contoso.sharepoint.com/sites/OldSiteName
```

4. When prompted, confirm that you want to delete the redirect.

To confirm that the redirect has been deleted, browse to the URL. It should return a 404 error. You can also run `Get-SPOSite -Identity https://contoso.sharepoint.com/sites/OldSiteName`. It will return that we cannot get the site.

NOTE

You might need to clear the history in your browser before browsing to the URL.

To get a list of all redirect sites

Run the following command.

```
Get-SPOSite -Template REDIRECTSITE#0
```

Lock and unlock sites

11/2/2020 • 2 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can block access to a site or make a site read-only by using Microsoft PowerShell to change the lock state of the site.

> **NOTE**
> You can't set the lock state on the root site.

Change the lock state for a site

Follow these steps to change the lock state for a site by using PowerShell.

1. Download the latest SharePoint Online Management Shell.

   > **NOTE**
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
   > On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. At the PowerShell command prompt, type the following command, and then press ENTER.

```
Set-SPOSite -Identity "<SiteURL>" -LockState "<State>"
```

Where: *SiteURL* is the URL of the site that you want to lock or unlock and *State* is one of the following values:

- **Unlock** to unlock the site and make it available to users.
- **ReadOnly** to prevent users from adding, updating, or deleting content. A message will appear on the site stating that the site is under maintenance and is read-only.
- **NoAccess** to prevent users from accessing the site and its content. If you've provided a NoAccessRedirectUrl value for your organization (below), traffic will be redirected to the URL you specified. If you haven't set this URL, a 403 error will be displayed.

```
Set-SPOTenant -NoAccessRedirectUrl 'https://www.contoso.com'
```

For more info about the LockState parameter, see Set-SPOSite. For more info about the NoAccessRedirectUrl parameter, see Set-SPOTenant.

Set up a home site for your organization

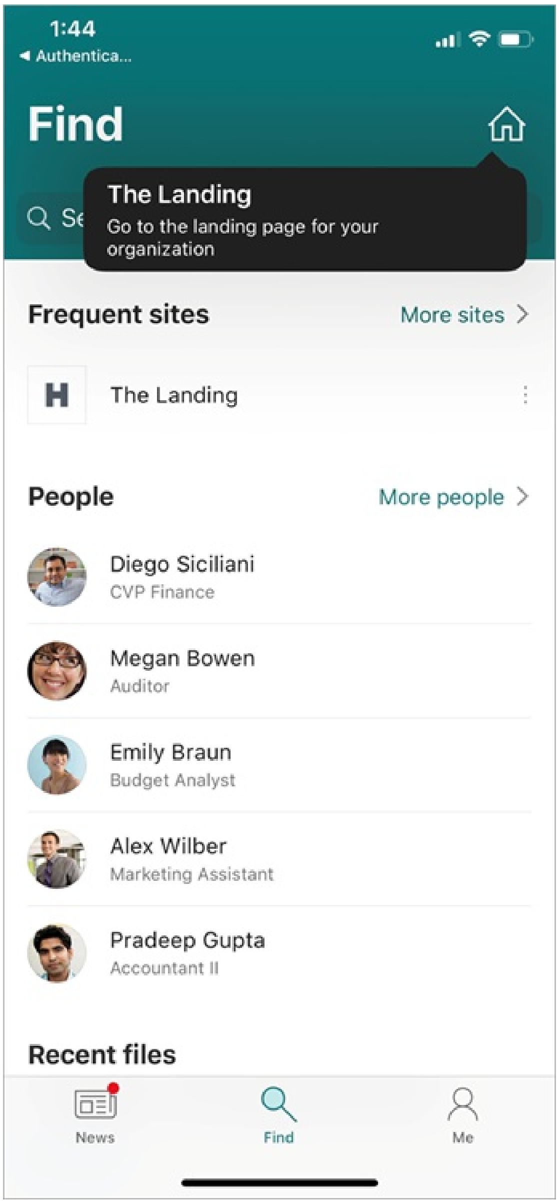
1/8/2021 • 4 minutes to read • Edit Online

A home site is a SharePoint communication site that you create and set as the top landing page for all users in your intranet. It brings together news, events, embedded video and conversations, and other resources to deliver an engaging experience that reflects your organization's voice, priorities, and brand.

Home site capabilities

When you set a site as your home site:

- It's easily accessible from the SharePoint mobile app for Android and iOS. All users that have access to the home site will see a home button on the Find tab of the mobile app. Being communication sites, home sites are designed to be mobile friendly from the start.



- Search for the site is scoped to all sites within the organization. Having a great search experience is critical for the success of the home site. Learn more about Microsoft Search
- The site is automatically set up as an organization news site. (Although you can have only one home site,

you can have multiple organization news sites.)

> **NOTE**
>
> Integration between the home site and SharePoint start page (where the branding, theming, header, navigation, and footer elements from the home site are applied to the start page and users can easily navigate between the pages) is not available at this time. Please watch for updates in the Microsoft 365 roadmap.

Plan and create your home site

To set a site as your organization's home site, you first need to create and customize the site you want to use.

1. When you design your organization's top landing page, consider the goals from the perspective of your IT department, your organization's communications team, and end users of the experience.
2. Create a communication site to use for the home site, and customize it using built-in features as much as possible:
   - Use the megamenu style for navigation and add a site footer. For info, see Change the look of your SharePoint site.
   - Try out various page layouts, including the vertical section. For info, see Add sections and columns.
   - Use audience targeting with SharePoint news and navigation links to tailor the experience for your audiences.
   - Use personalized web parts, preferably in a unique visual location like the vertical section with background color, which allows users to quickly consume organization content and get back to their work.
   - Extend the site as needed by using the SharePoint Framework (SPFx). To get started building custom web parts, see SharePoint Framework Tutorial 1. For info about app extensions, see Getting started with SharePoint Framework Application customizers.
   - Make sure the site is set up for regular content updates. Turn on content approval to ensure high-quality content.
   - Consider making the site a hub site. Your home site can be registered as a hub site, but can't be associated with another hub.
3. Create a launch plan for redirecting from your current solution to the new home site and notifying users of the change. **Important**: Make sure the site adheres to the guidelines for healthy portals.
4. Optional (recommended): When you're ready to launch, replace your root site with the new site.
5. To make the site a home site, follow the steps in the next section.
6. Make sure to customize the Microsoft 365 theme for your organization, adding your logo and linking it to the home site.

Set a site as your home site

After you create and customize the communication site that you want to use as your home site, you need to run a PowerShell cmdlet to set it as your home site. To run this cmdlet, you must be a site admin of the site.

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run `Set-SPOHomeSite -HomeSiteUrl <siteUrl>`.

   (Where siteUrl is the site you want to use)

> **NOTE**
>
> You can set only one site in your organization as a home site. The site can be registered as a hub site, but can't be associated with a hub. The first time you set up a home site, it might take up to several minutes for the changes to take effect. If you run the command again to switch your home site to a different site, it might take up to 2 hours.

Create an organization assets library

1/8/2021 • 3 minutes to read • Edit Online

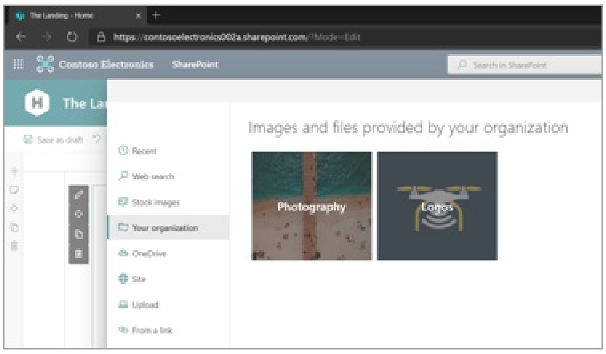
NOTE

This feature is not available for Office 365 Germany, Office 365 operated by 21Vianet (China), or Microsoft 365 US Government plans.

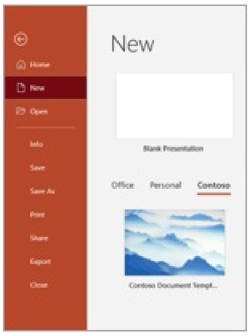
You can specify up to 30 organization asset libraries for a single organization. All of these libraries (regardless of type) must be on the same site. Only libraries (not folders) can be set as organization asset libraries.

If your organization needs to store and manage files for all your users to use, you can specify one or more document libraries on a SharePoint site as an "organization assets library." You can create two types of organization assets:

- **Images such as photos and logos**. When a user adds a web part to any modern page in SharePoint and that web part opens the file picker, the user can select "Your organization" in the left pane to browse the libraries you've specified.



- **Office templates**. When a user selects to create a new PowerPoint presentation (from PowerPoint for the web or the PowerPoint desktop app), the user can select the tab for your organization to see the templates. (To use this feature on PowerPoint for the web, users need to be assigned a license to Office 365 E3 or E5. The templates aren't available from the New menu. To create a file from a template, go to the PowerPoint start page > Office Template Library.)



Use Microsoft PowerShell to specify a library as an organization assets library

1. Select an existing site or create a new site for the organization assets. This can be any type of site, such as a communication site, an Office 365 group-connected team site, or a modern team site that isn't connected to an Office 365 group.

> **NOTE**
>
> All organization asset libraries must be on the same site.

2. **Set the permissions on the site**. Add the people you want to be able to upload files as members or owners of the site or Office 365 group. Add "Everyone except external users" as visitors. If necessary, customize the permissions for the library. You can customize the permissions of up to 100 files and folders in the library.

3. Upload the images or Office templates to a document library.

4. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

5. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

6. Run the following command to designate the document library as an organization assets library:

```
Add-SPOOrgAssetsLibrary -LibraryUrl <URL> [-ThumbnailUrl <URL>] [-OrgAssetType <ImageDocumentLibrary
or OfficeTemplateLibrary>] [-CdnType <Public or Private>]
```

LibraryURL is the absolute URL of the library to be designated as a central location for organization assets. ThumbnailURL is the URL for the image file that you want to appear in the card's background in the file picker; this image must be on the same site as the library. The name publicly displayed for the library will be the name of the library on the SharePoint site. OrgAssetType is either ImageDocumentLibrary or OfficeTemplateLibrary. If you don't specify the OrgAssetType, the library will be designated as an image library by default. If you don't specify the CdnType, it will enable a private CDN by default. Learn more about the Add-SPOOrgAssetsLibrary cmdlet.

Example:

```
Add-SPOOrgAssetsLibrary -LibraryURL https://contoso.sharepoint.com/sites/branding/Assets -ThumbnailURL
https://contoso.sharepoint.com/sites/branding/Assets/contosologo.jpg -OrgAssetType ImageDocumentLibrary
```

> **NOTE**
>
> Adding an organization assets library will enable a content delivery network (CDN) for your organization to provide fast and reliable performance for shared assets. You'll be prompted to enable a CDN for each organization asset library you add. For more information, see Content Delivery Networks (CDNs).

Related commands

- See information about all organization asset libraries on the site:
  `Get-SPOOrgAssetsLibrary`

Learn more about this cmdlet.

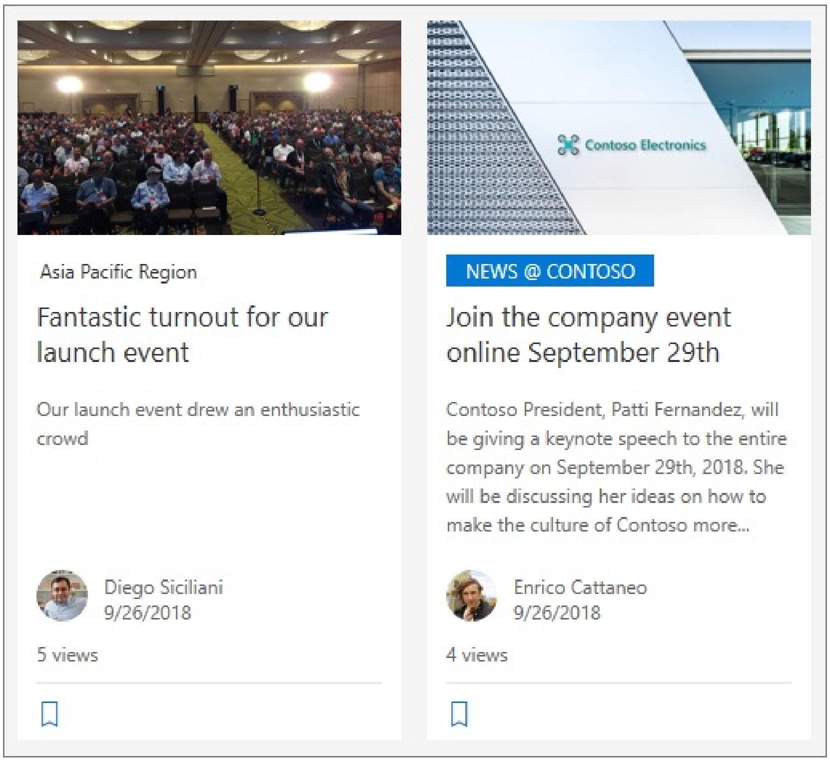
- Update thumbnail URL:
  `Set-SPOOrgAssetsLibrary -LibraryUrl <String> -ThumbnailUrl <String>`
  Learn more about this cmdlet.

- Remove a library:
  `Remove-SPOOrgAssetsLibrary -LibraryUrl <String>`
  Learn more about this cmdlet.

Create an organization news site

6/5/2020 • 2 minutes to read • Edit Online

To specify SharePoint sites as "official" or "authoritative" for news in your organization, mark them as organization news sites. These posts get special visual treatment (see the "NEWS @ CONTOSO" color block below), and appear on the SharePoint start page.



SharePoint admins can specify any number of organization news sites. For multi-geo tenants, organization news sites would have to be set up for each geo location. Each geo location could use the same central organization news site, and/or have its own unique site that shows organization news specific to that region.

> **NOTE**
> When SharePoint home sites are released, they will be automatically configured as organization news sites.

For more info about working with news, see Use the News web part on a SharePoint page and Add news posts.

Use Microsoft PowerShell to specify a site as an organization news site

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command to designate the site as an organization news site:

```
Set-SPOOrgNewsSite -OrgNewsSiteUrl <site URL>
```

Example: `Set-SPOOrgNewsSite -OrgNewsSiteUrl https://contoso.sharepoint.com/sites/Marketing`

Related commands

- View a list of all your organization news sites: Get-SPOOrgNewsSite
- Remove a site from the list of organization news sites: Remove-SPOOrgNewsSite

Retirement of site mailboxes

1/8/2021 • 7 minutes to read • Edit Online

The site mailboxes are being retired and will be out of service and/or removed. Please use the following instructions to identify, backup, and delete site mailboxes.

To view a list of site mailboxes

Run the following command in Exchange PowerShell:

```
Get-SiteMailbox -BypassOwnerCheck -ResultSize Unlimited | ft Name, WhenCreated, ClosedTime, SharePointUrl -AutoSize
```

The 'create' date shows the recently created site mailboxes. The 'ClosedTime' in the output of 'Get-SiteMailbox' refers to the status of the associated SharePoint site. The companies set a SharePoint policy to close sites after a period of time or provide users permission to close the sites. Closing the site generally means it is out of service. Closed site mailboxes are removed from view in the Outlook desktop client, but they are available in the Outlook Web Access.

For more information see, Use policies for site closure and deletion.

To identify active site mailboxes

Run the following command in Exchange PowerShell:

```
# If you run this more than once, delete/rename the output file first because this command appends to it.
# This is a single, long command line. It could take minutes or hours depending on the number of site mailboxes; thus, the countdown.
$sms = Get-SiteMailbox -BypassOwnerCheck -ResultSize unlimited;$count = $sms.Count; $sms | %{ $count-- ; echo "$count";Get-MailboxFolderStatistics $_.Identity -FolderScope Inbox | sort LastModifiedTime -Descending | ft Identity,LastModifiedTime >> c:\temp\sitemailboxes.txt};Write-Host "Open file c:\temp\sitemailboxes.txt to check the result"
```

There are no commands to show if the site mailboxes are still active. The above example lists the number of site mailboxes that were recently updated. The details of the site mailboxes are stored in a file.

> **NOTE**
> The processing time varies based on the number of site mailboxes. You can open the 'sitemailboxes.txt' to view the result of the command.

To Identify the owners of site mailboxes

Run the following command in Exchange PowerShell:

```
Get-SiteMailbox -BypassOwnerCheck -ResultSize unlimited | ft Name, Owners
```

Export site mailboxes through PST (Manually)

You must have Microsoft 365 admin permissions to access the Microsoft 365 compliance center.

For more information, see Permissions and sharing.

1. Go to https://compliance.microsoft.com/ and sign in with an account that has admin permissions for your organization.

2. In the Microsoft 365 compliance center Home page, navigate to **Show all** > **eDiscovery** > **Core**.

   The **Core eDiscovery** page is displayed.

3. Click **Create a case**.

4. In **New case** details pane, enter the following details:

   - Enter the **Case name** (mandatory).
   - Enter the **Case description** (optional).

5. Click **Save**.

6. Select the case that you saved from the list view and click to open the case.

   The case opens in a new window.

7. Click **Search** > **+Guided search**.

   The **New Search** details pane is displayed.

8. In the **New search** details pane, under the following tabs:

   a. In **Name your search** tab, do the following:

      a. Enter the **Name** (mandatory).

      b. Enter **Description** (optional).

      c. Click **Next**.

   b. In **Choose Locations** tab, do the following:

      a. Select **Specific locations**.

      b. In **Location**, click **Choose users, groups, or team**.

         The **Edit locations** window is displayed.

      c. In **Edit locations** window, under **Exchange email**, click **Choose users, groups, or team**.

      d. Enter the name of the site mailbox to be exported.

      e. Check the confirmation box to ensure the site mailbox is added.

      f. Click **Choose** and then click **Done**.

      g. Under **SharePoint sites** option, click **Choose sites** to add the SharePoint site associated with the site mailbox.

      h. To find the SharePoint URL for the site mailbox, run the following command in PowerShell:

         ```
         Get-SiteMailbox -BypassOwnerCheck -ResultSize unlimited
         ```

      i. Enter the URL and check the confirmation box to ensure the URL is added.

j. Click **Choose** and then click **Done**.

k. Click **Next**.

c. In **Create query** tab, click **Finish**.

> **NOTE**
>
> Leave the Condition card blank to ensure the entire mailbox content is searched. The search will take a while based on the amount of content.

9. Once the search is complete, click **More** > **Export results**.

   The **Export results** window is displayed.

10. Select the appropriate options and click **Export**.

> **NOTE**
>
> The export wizard takes a few minutes to launch the Export window.

11. In the **Export** window, under the **Export key** section, click **Copy to clipboard**.
12. Click **Download results**.
13. In the dialog box, click **Open**.

> **NOTE**
>
> This will launch the Microsoft Office 365 eDiscovery Export Tool to export the mailbox to PST.

14. Click **Install** to install the **Export Tool** to export the mailbox to PST.
15. Paste the **Export key**, provide the location to save the PST file locally and then click **Start**.

> **NOTE**
>
> The export will take a while based on the size of the PST file.

16. Click **Close**.

    The PST can be now attached in Outlook.

> **NOTE**
>
> - Folders with no email items inside them will not be exported.
> - The site mailboxes contain a special folder named, "Documents", of type IPF.ShortcutFolder. This contains "links" to files that are on SP sites. The actual SP files must be exported using eDiscovery for SP sites.
> - Outlook shows the items inside the Documents folder as unsafe, this is an expected behavior.
> - The document attachments in the emails of Documents folders are just placeholders, the actual documents are stored in SharePoint.

Export site mailboxes to PST (using script)

1. Copy process-site-mailboxes.ps1 to a working directory.

2. Start Windows PowerShell in administrator mode.

   For more information see, Microsoft 365 admin permissions.

   > **NOTE**
   >
   > Ensure you have admin permissions for the following roles:
   >
   > - Compliance Administrator
   > - eDiscovery Manager
   > - Organization Management

3. Run the script 'process-site-mailboxes.ps1' in PowerShell.

4. Enter the admin username and password when prompted.

5. You can review the list of site mailboxes by opening 'SiteMailboxesList.csv' file on a working directory, when it prompts you to review the file.

6. Remove any site mailbox(es) from the list which you would not like to backup.

7. Save 'SiteMailboxesList.csv', after reviewing it.

8. Press 'y' when prompted "Do you like to proceed further? (Y/N)" to continue.

9. Once you get "Mailboxes content search are complete" message on your screen, access the export results created for each mailbox by going to the compliance center in Microsoft 365 Administrator dashboard.

   > **NOTE**
   >
   > Use Compliance center dashboard to download PST messages on your screen.

> **NOTE**
>
> - Folders with no email items inside them will not be exported.
> - The site mailboxes contain a special folder named, "Documents", of type IPF.ShortcutFolder. This contains "links" to files that are on SP sites. The actual SP files must be exported using eDiscovery for SP sites.
> - Outlook shows the items inside the Documents folder as unsafe, this is an expected behavior.
> - The document attachments in the emails of Documents folders are just placeholders, the actual documents are stored in SharePoint.

Import site mailboxes

For the site mailboxes to be accessible again for site owners, import the PST files to a mailbox. See one of the following topics for detailed, step-by-step instructions for bulk-importing your organization's PST files to Office 365.

- Use network upload to import PST files to Office 365
- Use drive shipping to import PST files

Use Exchange Web Services (EWS) APIs to extract mailbox content

You can also export and import site mailboxes using EWS APIs like any other mailbox. Exporting and importing of appointments, emails, contacts, tasks, and other mailbox items can be done by using the EWS-Managed API or EWS in Exchange.

For more information see, Exporting and importing items by using EWS in Exchange.

See one of the following topics for exporting and importing of mailbox content:

- Export items by using EWS in Exchange
- Import items by using EWS in Exchange

To remove the site mailboxes

Use one of the following options:

Option 1: Hiding the mailbox from a SharePoint site.

You can hide the site mailbox by removing it from the SharePoint site but it will still exist in Exchange. You can access the mailbox through Outlook Web Access if the browser is bookmarked.

1. Navigate to the SharePoint site from which you want to hide the mailbox.
2. Click **Settings** > **Site contents**.
3. Under **Lists, Libraries, and other APPs**, point to **Site Mailbox**, and then click ... for more information.
4. Click **Remove** and then click **OK** to remove the site mailbox app.

> **NOTE**
>
> If you remove a mailbox from a site, it won't be displayed on the site, but it will still be visible in Outlook (if you're using Exchange).

What else do I need to know?

There are a couple of things worth noting about removing a site mailbox:

- The only way to fully delete a site mailbox is to delete the entire site itself. When a site is closed or deleted (either manually, or by following site closure policies), the site mailbox is also closed or deleted.
- After removing the site mailbox app from a site, mail sent to the mailbox will still be stored. If you add the mailbox back to the site later, any mail sent to the site mailbox since it was originally created will still be there.

Option 2: Delete the SharePoint site.

If the SharePoint site is deleted, Exchange is notified to also delete the site mailbox.

1. Navigate to the SharePoint site you want to delete.
2. Select **Settings** at the top of the site and then click **Site information**.

> **NOTE**
>
> If you do not see **Site information** in the **Settings** panel, work with your SharePoint administrator to get access.

3. At the bottom of the **Site Information** panel, select **Delete site**.
4. Check the confirmation box, and then click **Delete**.

Option 3: Delete the site mailbox manually.

For example, run the following command in Exchange PowerShell:

```
Get-Mailbox MDEL:* | ?{$_.RecipientTypeDetails -eq "TeamMailbox"} | Remove-Mailbox -Confirm:$false
```

Use `Remove-Mailbox` to delete a site mailbox. The system removes the site mailbox link from the SharePoint site when a site mailbox is deleted. In the example, change the 'MDEL' to the name of the site mailbox you want to delete.

SharePoint file sync

6/5/2020 • 2 minutes to read • Edit Online

When users install the OneDrive sync app for Windows or Mac, and sync the files on a team site, they can work with the files in File Explorer or Finder. They can also easily save files to the team site from the programs they use.

When users add, change, and delete files and folders on the site, the files and folders are automatically added, changed, or deleted on their computer and vice versa.

To upload files to the team site, users can simply copy or move them to the site in File Explorer or Finder. They can also use File Explorer or Finder to easily organize the document library by creating new folders, and moving and renaming files and folders. All these changes sync automatically.

Windows10 devices come with the OneDrive sync app installed. Office2016 and later installations also have the sync app installed.

Read the release notes and install the latest fully released versions

Invalid file names and file types in OneDrive and SharePoint

Fix OneDrive sync problems

Let users sync SharePoint files with the new OneDrive sync app

6/5/2020 • 2 minutes to read • Edit Online

This article is for IT administrators in large organizations who want to enable users in their organizations to sync SharePoint team sites with the new OneDrive sync app. Smaller organizations and organizations that are new to Microsoft 365 are already set up to sync OneDrive and SharePoint files with the new OneDrive sync app.

When you enable this feature, users will be able to sync the files in a SharePoint team site to their PCs and Macs using the OneDrive sync app (OneDrive.exe). As part of this, they will be able to:

- Browse to a SharePoint site or shared folder and click **Sync** to sync all contents in the document library or only selected folders that are important to them.
- Change the folders they sync directly from their PC or Mac.
- Sync shared folders.
- Sync read-only files and folders.
- Coauthor files in real time with Office 2016 (C2R build 16.0.7167.2xxx or MSI build 16.0.4432.100x)
- Automatically transition from the previous OneDrive sync app (Groove.exe)

Deploy and configure the OneDrive sync app

To enable users in your organization to sync SharePoint team sites with the OneDrive sync app, you first need to deploy the OneDrive sync app to your organization.

See Deploy the new OneDrive sync app using Microsoft Endpoint Configuration Manager

See Deploy and configure the new OneDrive sync app for Mac

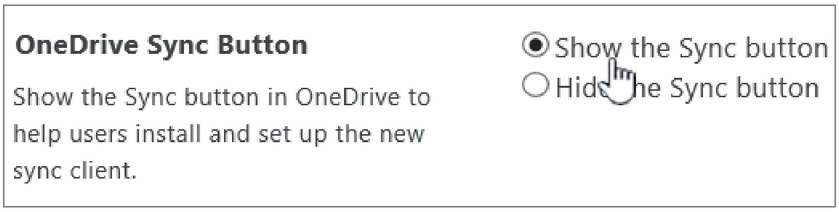
For info about the latest sync app releases, see New OneDrive sync app release notes.

Set SharePoint to sync with the OneDrive sync app

1. Go to the Settings page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

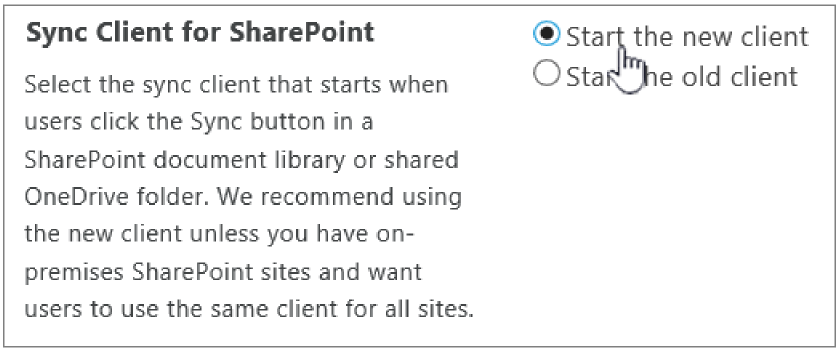
> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.

2. Select **classic settings page**.
3. Make sure "OneDrive Sync Button" is set to "Show the Sync button."



To sync SharePoint files with the new client, you must also sync OneDrive files with the new client.

4. For "Sync Client for SharePoint," select **Start the new client**.



> **NOTE**
>
> If you don't see the "Sync Client for SharePoint" setting on the Settings page, your organization is already set up to use the new OneDrive sync app. When users sign in to the OneDrive sync app (OneDrive.exe), it will automatically take over syncing the site libraries that the previous new OneDrive sync app (Groove.exe) was syncing. For information about how this works, and about the types of libraries that will continue syncing with the previous sync app, see Transition from the previous OneDrive for Business sync app.

5. Select **OK**.

   These changes take several hours to propagate. To check that they've propagated, go to a SharePoint site and select **Sync**. In the browser dialog that confirms the request to open a program, the "Program" should appear as "Microsoft OneDrive" and the "Address" should start with "odopen://"

See also

Sync SharePoint files with the new OneDrive sync app

Let users sync IRM-protected files with the OneDrive sync app

6/5/2020 • 2 minutes to read • Edit Online

This article is for Microsoft 365 global or SharePoint admins who want their users to be able to sync IRM-protected SharePoint document libraries and OneDrive locations using the new OneDrive sync app.

Prerequisites

> **NOTE**
>
> Any IRM-protected files will maintain their IRM protection during the sync process, both during upload and download.

- You've applied Information Rights Management (IRM) to a list or library. (On-premises SharePoint Server libraries can't be synced with the new OneDrive sync app.)
- Your users have disabled syncing using the previous OneDrive for Business sync app

Known issues

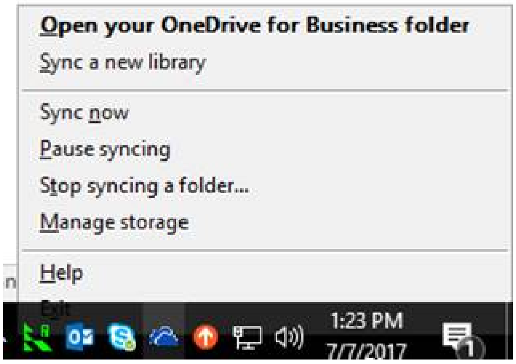
- This feature doesn't support the IRM setting that expires document access rights.

Disabling the previous OneDrive for Business sync app

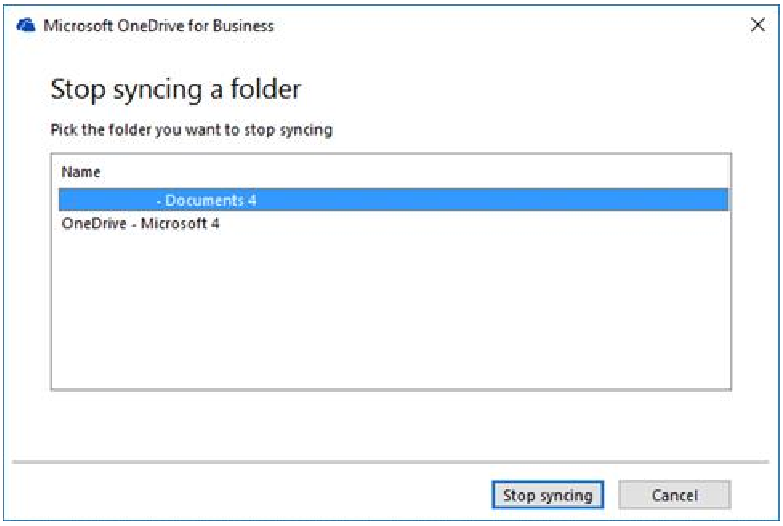
To prevent reliability issues, any users that are using the previous OneDrive for Business sync app (Groove.exe) to sync an IRM-protected library must disable syncing.

1. On a computer that uses the previous sync app to sync IRM-protected libraries, right-click the blue OneDrive icon in the notification area, at the far right of the taskbar:

2. Select **Stop syncing a folder**.



3. Select the IRM-protected library, and select **Stop syncing**.



Setup instructions

To enable this feature, you need to install the RMS client on your users' computers. Download the Rights Management Service client.

To silently install the client on computers, use the /qn switch as part of the command-line options of the Microsoft Windows Installer Tool (Msiexec.exe). For example, the following command shows the silent mode installation (assuming the RMS Client installer package is already downloaded to C:\Downloads).

msiexec /qn c:\downloads\setup.msi

You can have the setup file on a network share and use managed software deployment to run the msiexec command.

To sync an IRM-protected library

Have your users browse to the library in SharePoint and click the Sync button. This will open the OneDrive sync app and create the sync relationship for the location.

File collaboration in SharePoint with Microsoft 365

6/25/2020 • 18 minutes to read • Edit Online

With Microsoft 365 services, you can create a secure and productive file collaboration environment for your users. SharePoint powers much of this, but the capabilities of file collaboration in Microsoft 365 reach far beyond the traditional SharePoint site. Teams, OneDrive, and a variety of governance and security options all play a role in creating a rich environment where users can collaborate easily and where your organization's sensitive content remains secure.

In the sections below, we call out the options and decisions that you as an administrator should consider when setting up a collaboration environment:

- How SharePoint relates to other collaboration services in Microsoft 365, including OneDrive, Microsoft 365 Groups, and Teams.
- How you can create an intuitive and productive collaboration environment for your users.
- How you can protect your organization's data by managing access through permissions, data classifications, governance rules, and monitoring.

We recommend that you download the Microsoft Teams and related productivity services in Microsoft 365 for IT architects poster and refer to it while you read this article. This poster provides detailed illustrations of how the collaboration services in Microsoft 365 relate to each other and interact.

Also see the File Protection Solutions in Microsoft 365 diagram for an overview of recommended solutions to protect your data.

Creating a successful collaboration experience

The technical implementation options that you choose for file collaboration in Microsoft 365 should balance what can seem to be contradictory requirements:

- Protecting your intellectual property
- Enabling self-service
- Creating a smooth user experience

Protecting your intellectual property

There are several options discussed later in this article for protecting your intellectual property. These include limiting who files can be shared with, applying governance policies based on sensitivity labels, and managing the devices that users use to access content.

In considering which options to choose, we recommend a balanced approach:

A configuration that allows users to share content freely can lead to accidental sharing of confidential data. However, a user experience that is difficult to use or too restrictive can lead to users finding alternative collaboration options that circumvent your governance policies, ultimately leading to even greater risk.

By using a combination of features – depending on the sensitivity of your data – you can create a collaboration environment that's easy to use and provides the security and auditing controls that you need.

Enabling self-service

In SharePoint Server on-premises, many organizations chose an IT-focused model where users must request sites and provide a business justification. This was done to prevent site sprawl and to apply governance policies around access to sensitive data.

In Microsoft 365, we recommend allowing users to create Teams, Microsoft 365 Groups, and SharePoint sites as needed. You can use sensitivity labels to enforce permissions governance, take advantage of security features that protect your content, and use expiration and renewal policies to make sure unused sites don't accumulate.

By choosing options that favor user self-service, you can minimize the impact on your IT staff while creating an easier experience for your users.

Creating a smooth user experience

The key to creating a smooth user experience is to avoid creating barriers for your users that they don't understand or that they must escalate to your help desk. For example, turning external sharing off for a site might cause user confusion or frustration; whereas labeling the site and its contents as confidential and using data loss prevention policy tips and emails to educate your users in your governance policies, can lead to a much smoother experience for them.

SharePoint, Microsoft 365 Groups, and Teams

In Microsoft 365, SharePoint is integrated with a variety of other services to provide a much richer experience than is possible with on-premises solutions such as SharePoint Server. These integrations affect how you manage user permissions and what your users can do in a collaboration scenario.

Traditionally, SharePoint permissions have been managed through a set of permissions groups within a site (Owners, Members, Visitors, etc.). In SharePoint in Microsoft 365, each SharePoint team site is part of a Microsoft 365 group. a Microsoft 365 group is a single permissions group that is associated with a variety of Microsoft 365 services, including 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 are given access to the SharePoint site along with the other connected services.

While you can continue to manage SharePoint site permissions separately by using SharePoint groups, we recommend managing permissions for SharePoint by adding people to or removing them from the associated Microsoft 365 group. This provides easier administration as well as giving users access to a host of related services that they can use for better collaboration.

Microsoft Teams provides a hub for collaboration by bringing together all the Microsoft 365 group-related services, plus a variety of Teams-specific services, in a single user experience with persistent chat. Teams uses the associated Microsoft 365 group to manage its permissions. Within the Teams experience, users can directly access SharePoint along with the other services without having to switch applications. This provides a centralized collaboration space with a single place to manage permissions. For collaboration scenarios in your organization, we highly recommend using Teams rather than using services such as SharePoint independently.

For details about how SharePoint and Teams interact, see How SharePoint and OneDrive interact with Microsoft Teams.

Collaboration in client applications

Office applications such as Word, Excel, and PowerPoint provide a wide variety of collaboration features, including co-authoring and @mentions, and are also integrated with sensitivity labels and data loss prevention (discussed below).

We highly recommend deploying Microsoft 365 Apps for enterprise. Microsoft 365 Apps for enterprise provides an always up-to-date experience for your users, with the latest features and updates delivered on a schedule that you can control.

For details about deploying Microsoft 365 Apps for enterprise, see Deployment guide for Microsoft 365 Apps for enterprise.

OneDrive libraries

While SharePoint provides shared libraries for shared files that teams can collaborate on, users also have an individual library in OneDrive where they can store files that they own.

When a user adds a file to their individual library, that file is not shared with anyone else. Users' individual libraries do, however, provide the same sharing capabilities as SharePoint, so users can share files in their individual libraries as needed.

A user's individual library can be accessed from Teams, as well as from the OneDrive web interface and mobile application.

On devices running Windows or macOS, users can install the OneDrive sync app to sync files from both OneDrive and SharePoint to their local disk. This allows them to work on files offline and also provides the convenience of opening files in their native application (such as Word or Excel) without the need of going to the web interface.

The two main decisions to consider for using OneDrive in collaboration scenarios are:

- Do you want to allow Microsoft 365 users to share files in their own library with people outside your organization?
- Do you want to restrict file sync in any way – such as only to managed devices?

These settings are available in the OneDrive admin center.

OneDrive is an important part of the Microsoft 365 collaboration story. For information about how to deploy OneDrive in your organization, see OneDrive guide for enterprises.

Securing your data

A big part of a successful collaboration solution is making sure your organization's data remains secure. Microsoft 365 provides a variety of features to help you keep your data secure while enabling a seamless collaboration experience for your users.

To help protect your organization's information, you can:

- **Control sharing** – by configuring sharing settings for each site that are appropriate to the type of information in the site, you can create a collaboration space for users while securing your intellectual property.
- **Classify and protect information** – by classifying the types of information in your organization, you can create governance policies that provide higher levels of security to information that is confidential compared to information that is meant to be shared freely.
- **Manage devices** – with device management, you can control access to information based on device, location, and other parameters.
- **Monitor activity** – by monitoring the collaboration activity happening in Teams and SharePoint, you can gain insights into how your organization's information is being used. You can also set alerts to flag suspicious activity.
- **Protect against threats** – by using policies to detect malicious files in SharePoint, OneDrive, and Teams, you can help ensure the safety of your organization's data and network.

These are each discussed in more detail below. There are many options to choose from. Depending on the needs of your organization, you can choose the options that give you the best balance of security and usability. If you are in an highly regulated industry or work with highly confidential data, you may want to put more of these controls in place; whereas if your organization's information is not sensitive you may want to rely on basic sharing settings and malicious file alerts.

Control sharing

The sharing settings that you configure for SharePoint and OneDrive determine who your users can collaborate with, both inside and outside your organization. Depending on your business needs and the sensitivity of your data, you can:

- Disallow sharing with people outside your organization.
- Require people outside your organization to authenticate.
- Restrict sharing to specified domains.

You can configure these settings for the entire organization, or for each site independently. For detailed information, see Turn sharing on or off and Turn sharing on or off for a site.

See Limit accidental exposure to files when sharing with guests for additional guidance around sharing with people outside your organization.

When users share files and folders, a shareable link is created which has permissions to the item. There are three primary link types:

- *Anyone* links give access to the item to anyone who has the link. People using an *Anyone* link do not have to authenticate, and their access cannot be audited.

  An *anyone* link is a transferrable, revocable secret key. It's transferrable because it can be forwarded to others. It's revocable because by deleting the link, you can revoke the access of everyone who got it through the link. It's secret because it can't be guessed or derived. The only way to get access is to get the link, and the only way to get the link is for somebody to give it to you.

- *People in your organization* links work for only people inside your Microsoft 365 organization. (They do not work for guests in the directory, only members).

Like an *anyone* link, a *people in my organization* link is a transferrable, revocable secret key. Unlike an *anyone* link, these links only work for people inside your Microsoft 365 organization. When somebody opens a *people in my organization* link, they need to be authenticated as a member in your directory. If they're not currently signed-in, they'll be prompted to sign-in.

- *Specific people* links only work for the people that users specify when they share the item.

A *specific people* link is a non-transferable, revocable secret key. Unlike *anyone* and *people in my organization* links, a *specific people* link will not work if it's opened by anybody except for the person specified by the sender.

Specific people links can be used to share with internal or external users. In both cases, the recipient will need to authenticate as the user specified in the link.

It's important to educate your users in how these sharing links work and which they should use to best maintain the security of your data. Send your users links to Share OneDrive files and folders and Share SharePoint files or folders, and include information about your organization's policies for sharing information.

Unauthenticated access with *Anyone* links

Anyone links are a great way to easily share files and folders with people outside your organization. However, if you're sharing sensitive information, this may not be the best option.

If you require people outside your organization to authenticate, *Anyone* links will not be available to users and you'll be able to audit guest activity on shared files and folders.

Though *Anyone* links do not require people outside your organization to authenticate, you can track the usage of *Anyone* links and revoke access if needed. If people in your organization frequently email documents to people outside your organization, *Anyone* links may be a better option than emailing an attachment.

If you want to allow *Anyone* links, there are several options for a more secure sharing experience.

You can restrict *Anyone* links to read-only. You can also set an expiration time limit, after which the link will stop working.

Another option is to configure a different link type to be displayed to the user by default. This can help minimize the chances of inappropriate sharing. For example, if you want to allow *Anyone* links but are concerned that they only be used for specific purposes, you can set the default link type to *Specific people* links or *People in your organization* links instead of *Anyone* links. Users would then have to explicitly select *Anyone* links when they share a file or folder.

You can also use data loss prevention to restrict *Anyone* link access to files that contain sensitive information.

People in your organization links

People in your organization links are a great way to share information within your organization. *People in your organization* links work for anyone in your organization, so users can share files and folders with people who aren't part of a team or members of a site. The link gives them access to the particular file or folder and can be passed around inside the organization. This allows for easy collaboration with stakeholders from groups that may have separate teams or sites – such as design, marketing, and support groups.

Creating a *People in your organization* link does not cause the file or folder to show up in search or give everyone direct access to the file or folder. Users must have the link in order to access the file or folder. The link does not work for guests or other people outside your organization.

Specific people links

Specific people links are best for circumstances where users want to limit access to a file or folder. The link only works for the person specified and they must authenticate in order to use it. These links can be internal or external (if you've enabled guest sharing).

Classify and protect information

Data loss prevention in Microsoft 365 provides a way to classify your teams, groups, sites, and documents, and to create a series of conditions, actions, and exceptions to govern how they're used and shared.

By classifying your information and creating governance rules around them, you can create a collaboration environment where users can easily work with each other without accidentally or intentionally sharing sensitive information inappropriately.

With data loss prevention policies in place, you can be relatively liberal with your sharing settings for a given site and rely on data loss prevention to enforce your governance requirements. This provides a friendlier user experience and avoids unnecessary restrictions that users might try to work around.

For detailed information about data loss prevention, see Overview of data loss prevention.

Sensitivity labels

Sensitivity labels provide a way to classify teams, groups, sites, and documents with descriptive labels that can then be used to enforce a governance workflow.

Using sensitivity labels helps your users to share information safely and to maintain your governance policies without the need for users to become experts in those policies.

For example, you could configure a policy that requires Microsoft 365 groups classified as confidential to be private rather than public. In such a case, a user creating a group, team, or SharePoint site would only see the "private" option when they choose a classification of confidential. For information about using sensitivity labels with teams, groups, and sites, see Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites

Conditions and actions

With data loss protection conditions and actions, you can enforce a governance workflow when a given condition is met.

Examples include:

- If customer information is detected in a document, then users cannot share that document with guests.
- If a document contains the name of a confidential project, then guests cannot open the document even if it has been shared with them.

Microsoft Cloud App Security offers additional granular conditions, actions, and alerts to help you secure your content. These include the ability to remove a user's permissions or quarantine the user when the specified condition is met.

User notifications

User notifications provide a way to communicate to your users – via email or policy tips – that data loss prevention has detected something that they should be aware of. The user can then decide the best course of action depending on the situation. For example, if a user unknowingly attempts to share a document that contains a credit card number, the user is prompted that a credit card number has been found and advised of your organization's policy regarding this.

Manage access

Microsoft 365 provides a variety of governance features to help you create an intuitive but secure collaboration environment for your users.

- Use device management to ensure your organization's information is accessed only by compliant devices.
- Use conditional access to ensure your confidential data is accessed only from locations and apps that you trust.
- Monitor information sharing in real time and through reports to ensure your governance requirements are met and sensitive information is being kept secure.

Additionally, you can use Azure Active Directory access reviews to automate a periodic review of group and team ownership and membership.

Device Management

Through device management, you can take additional steps to secure your organization's information. You can manage pretty much any device that your users might have – PCs, Macs, mobile devices, and Linux computers.

Examples include:

- Ensure devices have the latest updates before allowing access to Microsoft 365
- Prevent copy and paste of confidential data to personal or unmanaged apps
- Erase company data from managed devices

As you consider your options governing access to information through device management, keep in mind that guest users are likely to have unmanaged devices. For sites where you've enabled guest sharing, be sure to provide the needed access to unmanaged devices, even if that's just web access via a PC or Mac. Azure Active Directory conditional access (discussed below) offers some options to reduce the risk of guest users with unmanaged devices. Some settings can be configured directly from SharePoint.

Intune in Microsoft 365 provides detailed device profiling options and can also deploy and manage individual apps such as Office apps and OneDrive. For detailed information about Intune and device management, see What is Microsoft Intune?.

You can configure device management from the Microsoft 365 Device Management admin center.

Conditional access

Azure Active Directory conditional access provides additional controls to prevent users from accessing your organization's resources in risky situations, such as from untrusted location or from devices that aren't up to date.

Examples include:

- Block guest users from logging in from risky locations
- Require multi-factor authentication for mobile devices

You can create access policies that are specifically for guest users, allowing risk mitigation for users who most likely have unmanaged devices.

For detailed information, see What is Conditional Access?.

Real-time monitoring with alerts

Microsoft Cloud App Security provides an extensive policy infrastructure that you can use to monitor activity that you consider to be risky for your organization's data.

Examples include:

- Raise an alert when a confidential file is shared externally.
- Raise an alert when there's a mass download by a single user.
- Raise an alert when an externally shared file hasn't been updated for a specified period of time.

Cloud App Security can also watch for anomalous behavior such as unusually large uploads or downloads, access from unusual locations, or unusual admin activity.

By configuring alerts in Cloud App Security, you can be more confident in allowing an open sharing experience for your users.

You can see the alerts on the Cloud App Security alerts page.

For detailed information about Cloud App Security, see Microsoft Cloud App Security overview.

Monitoring with reports

A variety of reports are available in Microsoft 365 to help you monitor site usage, document sharing, governance compliance, and a host of other events.

For info about how to view reports on SharePoint site usage, see Microsoft 365 Reports in the Admin Center - SharePoint site usage.

For info about how to view data loss prevention reports, see View the reports for data loss prevention.

For info about how to view Cloud App Security reports, see Generate data management reports.

Manage threats

You can use ATP Safe Attachments (part of Microsoft 365 Advanced Threat Protection) to protect against users uploading malicious files to OneDrive, SharePoint, or Teams.

When ATP discovers a malicious file, that file is locked so that users cannot open, move, or copy the file.

The locked file is included in a list of quarantined items that you can monitor. You can then delete or release the file as appropriate.

For detailed info, see Microsoft 365 ATP for SharePoint, OneDrive, and Microsoft Teams.

Migrate files from on-premises

Microsoft 365 offers much greater versatility in collaboration scenarios than on-premises solutions such as SharePoint Server. If you have files in document libraries on SharePoint Server or in file shares, you can migrate them to SharePoint by using the SharePoint Migration Tool. The SharePoint Migration Tool can move files, OneDrive libraries, and even entire sites to SharePoint.

As part of your migration, you can use the Azure Information Protection scanner to scan and label sensitive information in your on-premises environment. With this information, you can reorganize your data if needed before migrating it to similarly labeled sites in SharePoint.

If the content that your users are collaborating on is located in SharePoint Server or in file shares, we recommend that you migrate it to Microsoft 365 to take advantage of the broader range of collaboration capabilities.

For information on how to migrate content with the SharePoint Migration Tool, see Download and install the SharePoint Migration Tool.

Related topics

Create a secure guest sharing environment

Best practices for sharing files and folders with unauthenticated users

Understanding how Microsoft Information Protection capabilities work together

How to deal with external sharing in Microsoft 365

Tutorial: Automatically apply Azure Information Protection classification labels

What's new in external sharing and collaboration with OneDrive and SharePoint

Protect and collaborate on files in the cloud with OneDrive, SharePoint, and Microsoft Teams

External sharing overview

1/8/2021 • 7 minutes to read • Edit Online

The external sharing features of Microsoft SharePoint let users in your organization share content with people outside the organization (such as partners, vendors, clients, or customers). You can also use external sharing to share between licensed users on multiple Microsoft 365 subscriptions if your organization has more than one subscription. Planning for external sharing should be included as part of your overall permissions planning for SharePoint in Microsoft 365. This article describes what happens when users share, depending on what they're sharing and with whom.

If you want to get straight to setting up sharing, choose the scenario you want to enable:

- Collaborate with guests on a document
- Collaborate with guests in a site
- Collaborate with guests in a team

(If you're trying to share a file or folder, see Share OneDrive files and folders or Share SharePoint files or folders in Microsoft 365.)

> **NOTE**
> External sharing is turned on by default for your entire SharePoint environment and the sites in it. You may want to turn it off globally before people start using sites or until you know exactly how you want to use the feature.

How the external sharing settings work

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. If a site's external sharing option and the organization-level sharing option don't match, the most restrictive value will always be applied.

Whichever option you choose at the organization or site level, the more restrictive functionality is still available. For example, if you choose to allow unauthenticated sharing using "Anyone" links (previously called "shareable" links or "anonymous access" links), users can still share with guests, who sign in, and with internal users.

> **IMPORTANT**
> Even if your organization-level setting allows external sharing, not all new sites allow it by default. The default sharing setting for Microsoft 365 group-connected team sites is "New and existing guests." The default for communication sites and classic sites is "Only people in your organization."

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.

> **NOTE**
>
> To limit *internal* sharing of contents on a site, you can prevent site members from sharing, and enable access requests. For info, see Set up and manage access requests.
>
> When users share a folder with multiple guests, the guests will be able to see each other's names in the Manage Access panel for the folder (and any items within it).

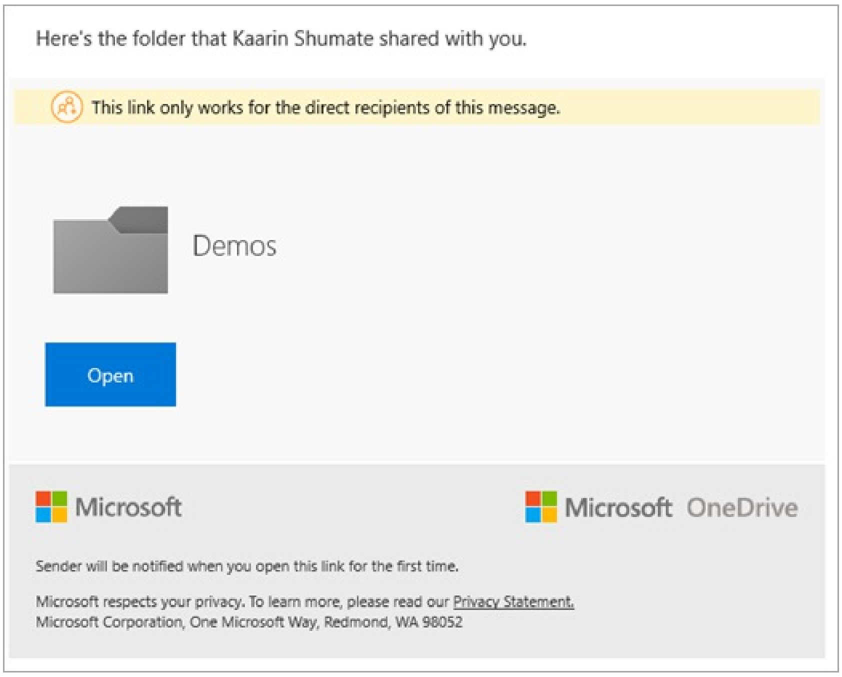
Sharing Microsoft 365 group-connected team sites

When you or your users create Microsoft 365 groups (for example in Outlook, or by creating a team in Microsoft Teams), a SharePoint team site is created. Admins and users can also create team sites in SharePoint, which creates a Microsoft 365 group. For group-connected team sites, the group owners are added as site owners, and the group members are added as site members. In most cases, you'll want to share these sites by adding people to the Microsoft 365 group. However, you can share only the site.

> **IMPORTANT**
>
> It's important that all group members have permission to access the team site. If you remove the group's permission, many collaboration tasks (such as sharing files in Teams chats) won't work. Only add guests to the group if you want them to be able to access the site. For info about guest access to Microsoft 365 groups, see Manage guest access in Groups.

What happens when users share

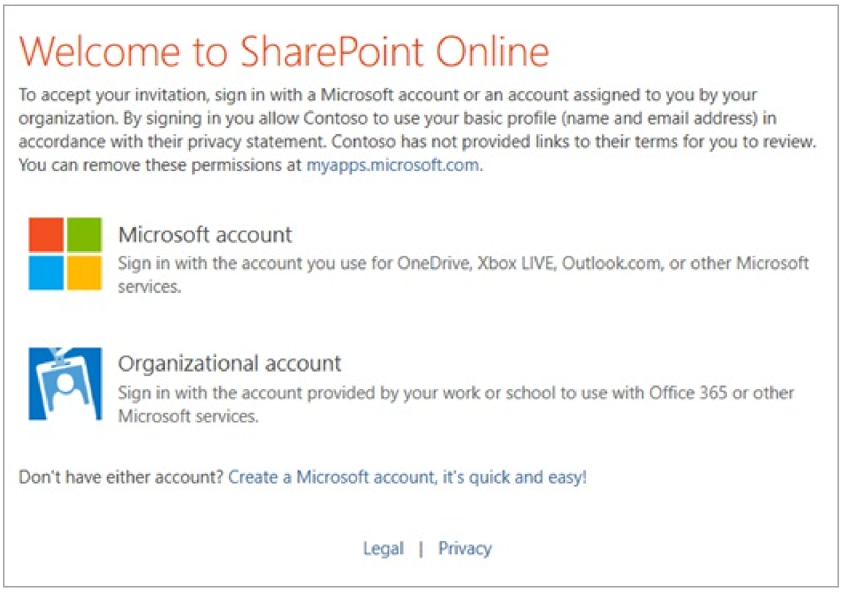
When users share with people outside the organization, an invitation is sent to the person in email, which contains a link to the shared item.



Recipients who sign in

When users share *sites*, recipients will be prompted to sign in with:

- A Microsoft account
- A work or school account in Azure AD from another organization



When users share *files and folders*, recipients will also be prompted to sign in if they have:

- A Microsoft account

These recipients will typically be added to your directory as guests, and then permissions and groups work the same for these guests as they do for internal users. (To ensure that all guests are added to your directory, use the SharePoint and OneDrive integration with Azure AD B2B preview.)

Because these guests do not have a license in your organization, they are limited to basic collaboration tasks:

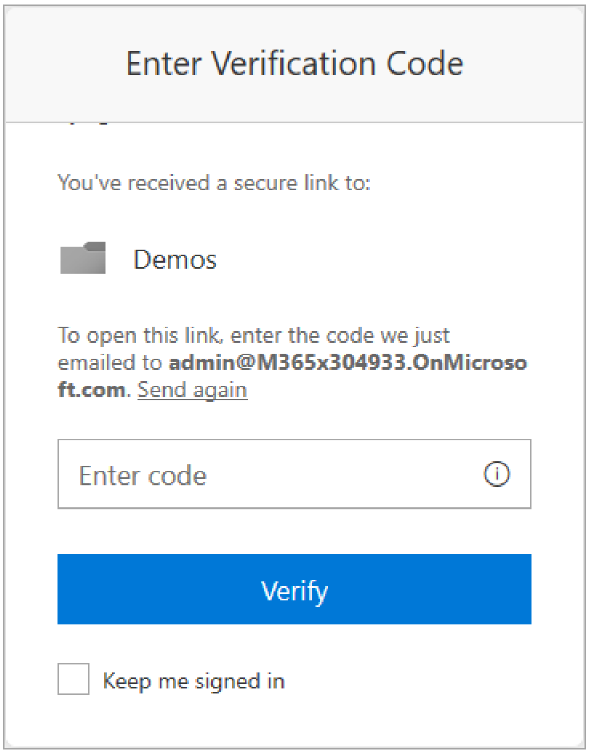
- They can use Office.com for viewing and editing documents. If your plan includes Office Professional Plus, they can't install the desktop version of Office on their own computers unless you assign them a license.
- They can perform tasks on a site based on the permission level that they've been given. For example, if you add a guest as a site member, they will have Edit permissions and they will be able to add, edit and delete lists; they will also be able to view, add, update and delete list items and files.
- They will be able to see other types of content on sites, depending on the permissions they've been given. For example, they can navigate to different subsites within a shared site. They will also be able to do things like view site feeds.

If your authenticated guests need greater capability such as OneDrive storage or creating a Power Automate flow, you must assign them an appropriate license. To do this, sign in to the Microsoft 365 admin center as a global admin, make sure the Preview is off, go to the **Active users** page, select the guest, click **More**, and then click **Edit product licenses**.

Recipients who provide a verification code

When users share files or folders, recipients will be asked to enter a verification code if they have:

- A work or school account in Azure AD from another organization
- An email address that isn't a Microsoft account or a work or school account in Azure AD



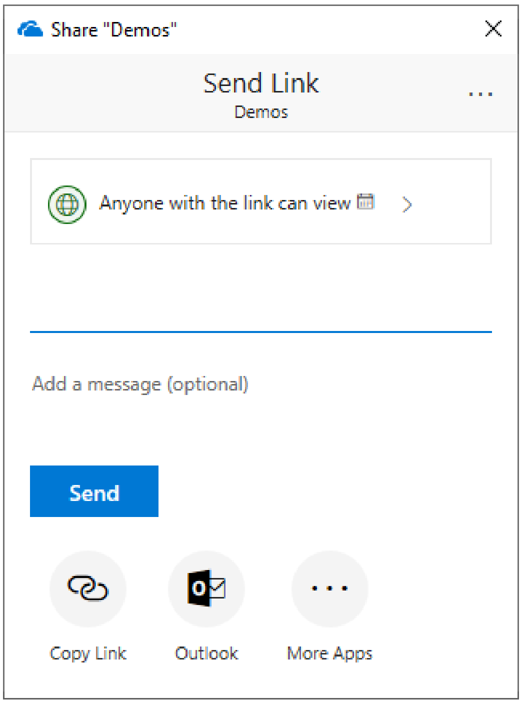
If the recipient has a work or school account, they only need to enter the code the first time. Then they will be added as a guest and can sign in with their organization's user name and password.

If the recipient doesn't have a work or school account, they need to use a code each time they access the file or folder, and they are not added to your directory.

> **NOTE**
>
> Sites can't be shared with people unless they have a Microsoft account or a work or school account in Azure AD.

Recipients who don't need to authenticate

Anyone with the link (inside or outside your organization) can access files and folders without having to sign in or provide a code. These links can be freely passed around and are valid until the link is deleted or expires (if you've set an expiration date). You cannot verify the identity of the people using these links, but their IP address is recorded in audit logs when they access or edit shared content.



People who access files and folders through "Anyone" links aren't added to your organization's directory, and you can't assign them licenses. They also can't access sites using an "Anyone" link. They can only view or edit the specific file or folder for which they have an "Anyone" link.

Stopping sharing

You can stop sharing with guests by removing their permissions from the shared item, or by removing them as a guest in your directory.

You can stop sharing with people who have an "Anyone" link by going to the file or folder that you shared and deleting the link.

Learn how to stop sharing an item

Need more help?

If you have technical questions about this topic, you may find it helpful to post them on the SharePoint discussion forum. It's a great resource for finding others who have worked with similar issues or who have encountered the same situation.

You can also find help on security and permissions in these YouTube videos from SharePoint community experts.

See also

How Microsoft manages and enables external sharing and collaboration with SharePoint (Microsoft Ignite)

Coaching your guests through the external sharing experience

Set up and manage access requests

Searching for site content shared externally

Configure Teams with three tiers of protection

Create a secure guest sharing environment

Settings interactions between Microsoft 365 Groups, Teams and SharePoint

SharePoint and OneDrive integration with Azure AD B2B (Preview)

1/8/2021 • 3 minutes to read • Edit Online

This article describes how to enable Microsoft SharePoint and Microsoft OneDrive integration with Azure AD B2B.

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

With SharePoint and OneDrive integration, the Azure B2B one-time passcode feature is used for external sharing of files, folders, list items, document libraries and sites. This feature provides an upgraded experience from the existing secure external sharing recipient experience.

Enabling the preview does not change your sharing settings. For example, if you have site collections where external sharing is turned off, it will remain off.

Once the preview is enabled you and your users do not have to reshare or do any manual migration for external users previously shared with. Instead, when an external user clicks on a link that was created before the preview was enabled, SharePoint will automatically create a B2B guest account. This guest account is created on behalf of the user who originally created the sharing link. (If the user who created the link is no longer in the organization or no longer has permission to share, the guest user will not be added to the directory and the file will need to be reshared.)

SharePoint and OneDrive integration with the Azure AD B2B one-time passcode feature is currently in preview. After preview, this feature will replace the ad-hoc external sharing experience used in OneDrive and SharePoint today for all tenants.

Advantages of Azure AD B2B include:

- Invited external users are each given an account in the directory and are subject to Azure AD access policies such as multi-factor authentication.
- Invitations to a SharePoint site use Azure AD B2B and no longer require users to have or create a Microsoft account.
- If you have configured Google federation in Azure AD, federated users can now access SharePoint and OneDrive resources that you have shared with them.
- SharePoint and OneDrive sharing is subject to the Azure AD organizational relationships settings, such as **Members can invite** and **Guests can invite**.

This preview is not supported in the following Microsoft 365 services:

- Office 365 Germany
- Office 365 operated by 21Vianet
- GCC High and DoD

Opting in to the preview

This preview requires that your organization also be opted into the Azure AD email one-time passcode authentication preview.

To opt in to the Azure AD passcode authentication preview

1. Sign in to the Azure portal as an Azure AD global admin.
2. In the nav pane, select **Azure Active Directory**.
3. In the **Overview** pane, click **External identities**.
4. In the **Organizational identities** pane, select **External collaboration settings**.
5. Under **Enable Email One-Time Passcode for guests (Preview)**, select **Yes**.
6. Select **Save**.

To opt in to the SharePoint and OneDrive integration with Azure AD B2B

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following cmdlets:

```
Set-SPOTenant -EnableAzureADB2BIntegration $true
Set-SPOTenant -SyncAadB2BManagementPolicy $true
```

Opting out of the preview

You can disable the preview by running `Set-SPOTenant -EnableAzureADB2BIntegration $false`. (You can also opt out of the Azure AD passcode authentication preview.) Content that was shared externally while the preview was enabled will need to be shared again with the specific external users.

Note that after preview, this feature will replace the ad-hoc external sharing experience used in OneDrive and SharePoint today for all tenants and you will not be able to opt out.

See also

Set-SPOTenant

External sharing overview

Manage sharing settings

11/2/2020 • 8 minutes to read • Edit Online

This article describes how global and SharePoint admins in Microsoft 365 can change their organization-level sharing settings for Microsoft SharePoint and Microsoft OneDrive. (If you want to share a file or folder, read Share SharePoint files or folders or Share OneDrive files and folders.)

For end-to-end guidance around how to configure guest sharing in Microsoft 365, see:

- Collaborate with guests on a document
- Collaborate with guests in a site
- Collaborate with guests in a team

To change the sharing settings for a site after you've set the organization-level sharing settings, see Turn external sharing on or off for for a site. To learn how to change the external sharing setting for a user's OneDrive, see Change the external sharing setting for a user's OneDrive.

Video demonstration

This video shows how the settings on the Sharing page in the SharePoint admin center affect the sharing options available to users.

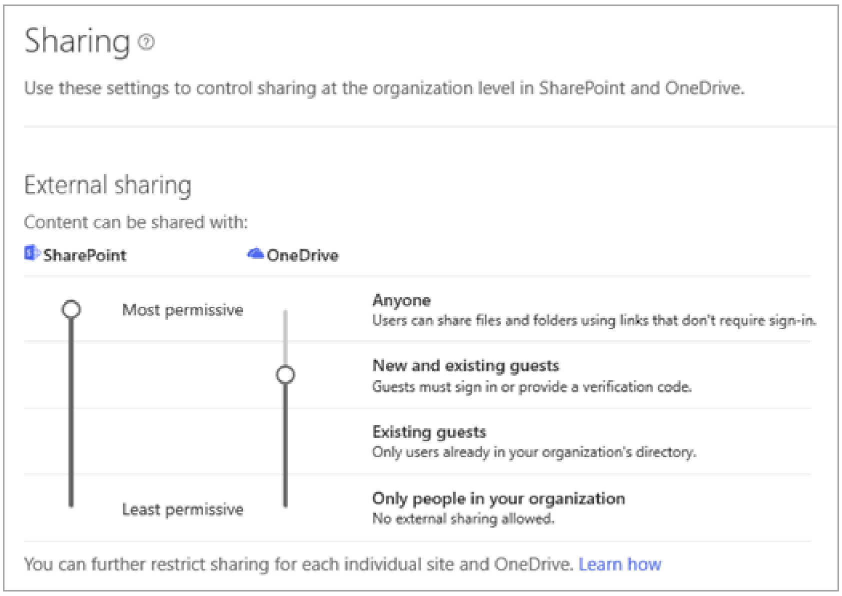
Change the organization-level external sharing setting

1. Go to the Sharing page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **NOTE**
   >
   > If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
   >
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Under **External sharing**, specify your sharing level for SharePoint and OneDrive. The default level for both is "Anyone."

   > **NOTE**
   >
   > The SharePoint setting applies to all site types, including those connected to Microsoft 365 groups.
   >
   > The OneDrive setting can be more restrictive than the SharePoint setting, but not more permissive.
   >
   > The SharePoint external sharing setting on this page is the same as the one in the Microsoft 365 admin center, under **Settings** > **Services & add-ins** > **Sites**. These settings are also the same as those in the OneDrive admin center.



This setting is for your organization overall. Each site has its own sharing setting which you can set independently, though it must be at the same or more restrictive setting as the organization. See Change the external sharing setting for a site for more information.

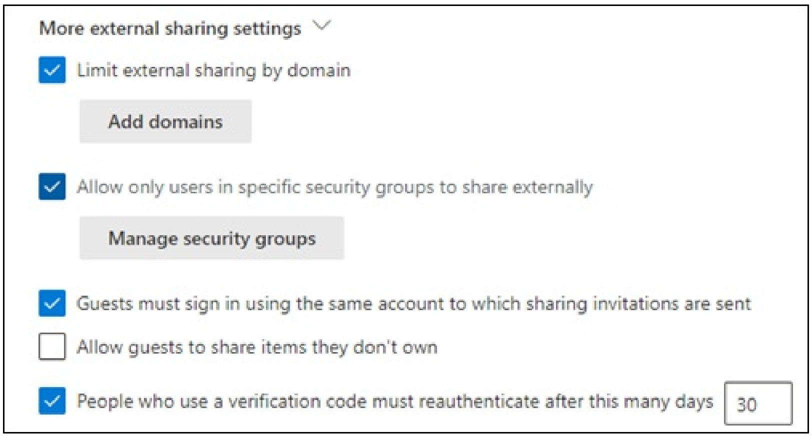
Which option to select...

SELECT THIS OPTION:	IF YOU WANT TO:
Anyone	Allow users to share files and folders by using links that let anyone who has the link access the files or folders without authenticating. This setting also allows users to share sites with new and existing guests who authenticate. If you select this setting, you can restrict the Anyone links so that they must expire within a specific number of days, or so that they can give only View permission. File requests requires that OneDrive be set to **Anyone** and edit permissions for **Anyone** links be enabled. OneDrive settings other than **Anyone** disable file requests. See Best practices for sharing files and folders with unauthenticated users for more information.
New and existing guests	Require people who have received invitations to sign in with their work or school account (if their organization uses Microsoft 365) or a Microsoft account, or to provide a code to verify their identity. Users can share with guests already in your organization's directory, and they can send invitations to people who will be added to the directory if they sign in. For more info about verification codes, see Secure external sharing in SharePoint Invitations to view content can be redeemed only once. After an invitation has been accepted, it can't be shared or used by others to gain access.
Existing guests	Allow sharing only with guests who are already in your directory. These guests may exist in your directory because they previously accepted sharing invitations or because they were manually added, such as through Azure B2B collaboration. (To see the guests in your organization, go to the Guests page in the Microsoft 365 admin center).

SELECT THIS OPTION:	IF YOU WANT TO:
Only people in your organization	Turn off external sharing.

> **NOTE**
>
> If you turn off external sharing for your organization and later turn it back on, guests who previously had access regain it. If you know that external sharing was previously turned on and in use for specific sites and you don't want guests to regain access, first turn off external sharing for those specific sites.
>
> If you restrict or turn off external sharing, guests typically lose access within one hour of the change.

More external sharing settings



Limit external sharing by domain

This is useful if you want to limit sharing with particular partners, or help prevent sharing with people at certain organizations. The organization-level setting on this page affects all SharePoint sites and each user's OneDrive. To use this setting, list the domains (maximum of 3000) in the box, using the format *domain.com*. To list multiple domains, press Enter after adding each domain.

You can also limit external sharing by domain by using the Set-SPOTenant Microsoft PowerShell cmdlet with -SharingDomainRestrictionMode and either -SharingAllowedDomainList or -SharingBlockedDomainList. For info about limiting external sharing by domain at the site level, see Restricted domains sharing.

Allow only users in specific security groups to share externally

For info about this setting, see Manage security groups.

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

By default, guests can receive an invitation at one account but sign in with a different account. After they redeem the invitation, it can't be used with any other account.

Allow guests to share items they don't own

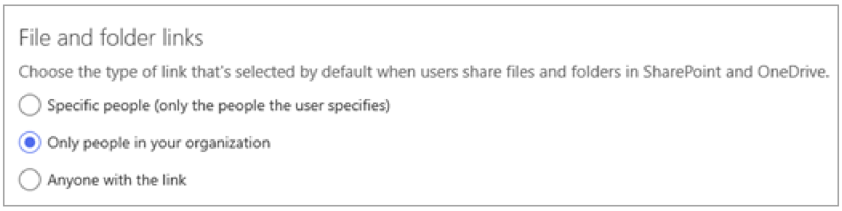
By default, guests must have full control permission to share items externally.

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

If people who use a verification code have selected to "stay signed in" in the browser, they must prove they can still access the account they used to redeem the sharing invitation.

File and folder links

Choose the option you want to show by default when a user gets a link.

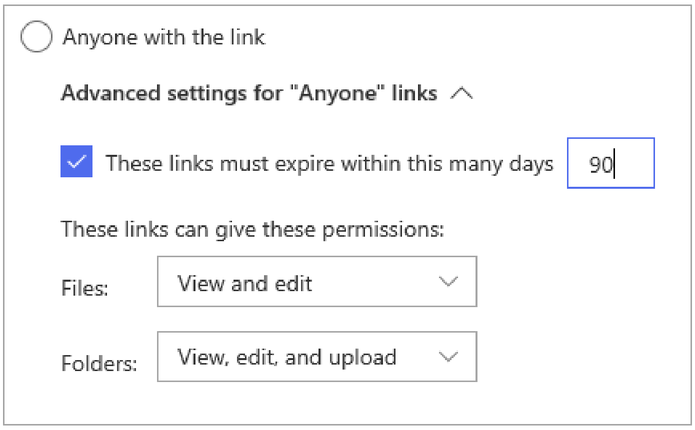


> **NOTE**
> This setting specifies the default for your organization, but site owners can choose a different default link type for a site.

- **Specific people** - This option is most restrictive and impedes broad internal sharing. If you allow external sharing, this option lets users share with specific people outside the organization.
- **Only people in your organization** - If links are forwarded, they'll work for anyone in the organization. This option is best if your organization shares broadly internally and rarely shares externally.
- **Anyone with the link** - This option is available only if your external sharing setting is set to "Anyone." Forwarded links work internally or externally, but you can't track who has access to shared items or who has accessed shared items. This is best for friction-free sharing if most files and folders in SharePoint and OneDrive aren't sensitive.

  > **IMPORTANT**
  > If you select "Anyone with the link," but the site or OneDrive is set to allow sharing only with guests who sign in or provide a verification code, the default link is "Only people in your organization." Users need to change the link type to "Specific people" to share files and folders in the site or OneDrive externally.

Advanced settings for "Anyone" links

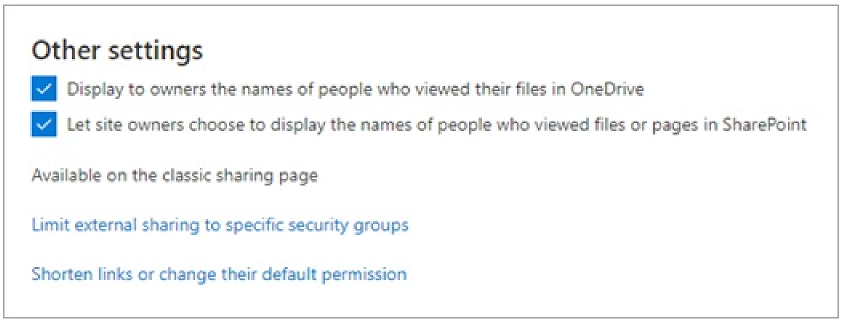


Link expiration - You can require all "Anyone" links to expire, and specify the maximum number of days allowed

Link permissions - You can restrict "Anyone" links so that they can only provide view permission for files or folders.

If you are using file requests, the link permissions must be set for **View and edit** for files and **View, edit, and upload** for folders.

Other



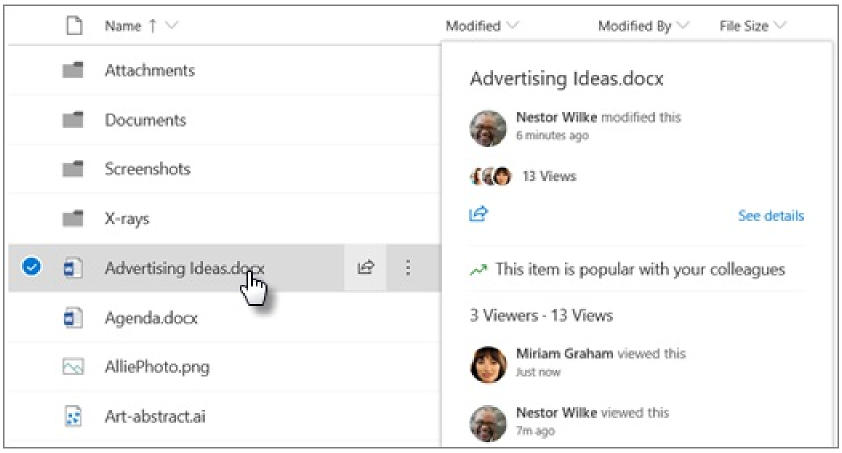
Display to owners the names of people who viewed their files

This setting lets you control whether the owner of a shared file can see on the file card the people who only view (and don't edit) the file in OneDrive. The file card appears when users hover over a file name or thumbnail in OneDrive. The info includes the number of views on the file, the number of people who viewed it, and the list of people who viewed it. To learn more about the file card, see See files you shared in OneDrive.

> **NOTE**
>
> This setting is selected by default. If you clear it, file viewer info is still recorded and available to you to audit as an admin. OneDrive owners can also still see people who have viewed their shared Office files by opening the files from Office.com or from the Office desktop apps.

Let site owners choose to display the names of people who viewed files or pages in SharePoint

This setting lets you specify whether site owners can allow users who have access to a file, page, or news post to see on the file card who has viewed the item.



This setting is turned on by default at the organization level and off at the site level for existing sites. Viewer information is shown only when the setting is on at both the organization and site level. We recommend that site owners turn on this feature only on team sites that don't have sensitive information. Learn how site owners can turn on this feature.

> **NOTE**
>
> Historical data is included when this setting is enabled. Likewise, if the setting is turned off and back on at the organization level or site level, the views during the off period are included in the history.

On the classic Sharing page, you can limit external sharing by security group and shorten sharing links or change their default permission.

Need more help?

If you have technical questions about this topic, you may find it helpful to post them on the SharePoint discussion forum. It's a great resource for finding others who have worked with similar issues or who have encountered the same situation.

You can also find help on security and permissions in these YouTube videos from SharePoint community experts.

See also

Limit accidental exposure to files when sharing with guests

Create a secure guest sharing environment

Stop sharing files or folders or change permissions

External sharing & collaboration with OneDrive, SharePoint & Teams (Ignite 2020)

Turn external sharing on or off for a site

1/8/2021 • 3 minutes to read • Edit Online

You must be a global or SharePoint admin in Microsoft 365 to change the external sharing setting for a site (previously called a "site collection"). Site owners are not allowed to change this setting.

Note that this procedure applies to classic sites, communication sites, and new team sites. To learn how to change the external sharing setting for a user's OneDrive, see Change the external sharing setting for a user's OneDrive. For info about changing your organization-level settings, see Turn external sharing on or off for SharePoint. To change the settings for Teams private channel sites, you must use Set-SPOSite.

For detailed information about how to set up guest access for a site, see Collaborate with guests in a site.

To configure external sharing for a site

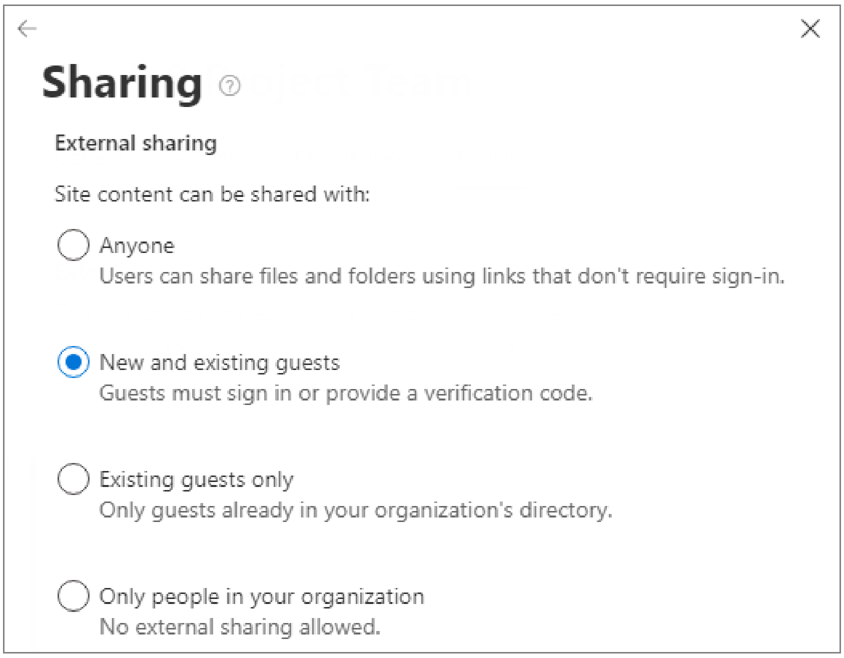
1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. In the left column, select a site.

3. Select **Sharing**.

4. Select an external sharing option (see the following table).



5. If you want to limit the sharing of this site by domain, select the **Limit sharing by domain** check box, and add the domains that you want to allow or block.

6. If you want to change the default sharing link type, permissions, or expiration setting for this site, clear

the **Same as organization-level setting** check box and set the value that you want to use for this site. For more info, see Change the default sharing link for a site.

7. Select **Save**.

Which option to select...

SELECT THIS OPTION:	IF YOU WANT TO:
Anyone	Allow site owners and others with full control permission to share the site with people who authenticate. Allow site users to decide when sharing files and folders to require authentication or allow unauthenticated people to access the item. Anyone links to files and folders can be freely forwarded.
New and existing guests	Allow site owners and others with full control permission to share the site with people outside the organization. These people will need to sign in and will be added to the directory. Allow site users to share files and folders with people who aren't in the organization's directory.
Existing guests	Allow sharing with only people already in your directory. These users may exist in your directory because they previously accepted sharing invitations or because they were manually added. (You can tell an external user because they have **#EXT#** in their user name.)
Only people in your organization	Prevent all site users from sharing any site content externally. (This is the default setting for new classic sites.)

The settings available are dependent on your organization-level setting. If you enable external sharing for a site and it is later turned off for your organization, external sharing will become unavailable at the site level and any shared links will stop working. If it is turned back on for the organization, the site sharing setting will return to what it was before and the shared links will resume working.

> **NOTE**
>
> You might have site content shared with a Microsoft 365 group that has guest members, and the group settings prevent guest members from accessing group resources. In this case, even if you turn on external sharing for the site, guests of the group may not be able to access site content. To enable or disable Microsoft 365 Group guest member access, see Manage guest access in Microsoft 365 Groups.

Related topics

Best practices for sharing files and folders with unauthenticated users

Create a secure guest sharing environment

File collaboration in SharePoint with Microsoft 365

Stop sharing files or folders or change permissions

Mark new files as sensitive by default

7/17/2020 • 2 minutes to read • Edit Online

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

Instead of turning off external sharing entirely, you can address this issue by using a new PowerShell cmdlet. The cmdlet prevents guests from accessing newly added files until at least one Office DLP policy scans the content of the file. If the file has no sensitive content based on the DLP policy, then guests can access the file. If the policy identifies sensitive content, then guests will not be able to access the file. They will receive the following access denied error message: "Due to organizational policies, you can't access this resource."

> **NOTE**
> This cmdlet applies to newly added files in all SharePoint sites and OneDrive accounts. It doesn't block sharing if an existing file is changed.

1. Make sure you have at least one DLP policy turned on for content located in SharePoint. Learn how to create and turn on a DLP policy

   > **IMPORTANT**
   > The DLP policy must include all SharePoint sites and OneDrive accounts and exclude none.

2. Download the latest SharePoint Online Management Shell.

   > **NOTE**
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
   > On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

3. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

4. Run the following command:

   ```
   Set-SPOTenant-MarkNewFilesSensitiveByDefault BlockExternalSharing
   ```

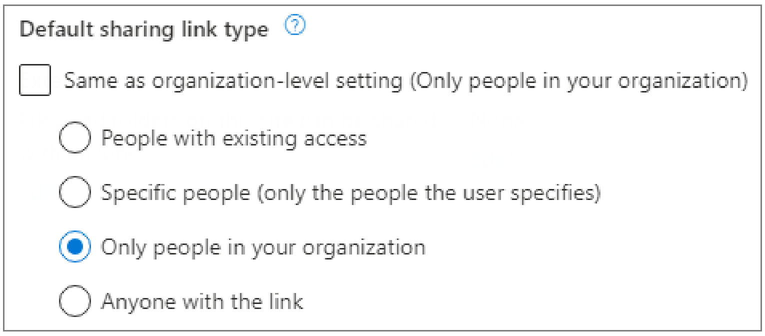
To disable this feature, run `Set-SPOTenant-MarkNewFilesSensitiveByDefault AllowExternalSharing`.

Change the default link type for a site

6/5/2020 • 2 minutes to read • Edit Online

Users can share files and folders in Microsoft SharePoint by sending a link. They should select a link type based on the people to whom they want to give permission. The following link types are available:

- Anyone with the link (previously called "anonymous access" or "shareable")
- People in your organization with the link
- People with existing access
- Specific people



As a global or SharePoint admin, you may want to enable users to send "Anyone" links, but you may not want this to the be the default type of link when users select to share files and folders. You can set the default type of link to something more restrictive, while still allowing users to select other types of links as needed. You can change this setting at the organization level and at the site (previously called "site collection") level.

> **NOTE**
> The default sharing link setting applies only to libraries that use the new experience.
> This setting does not affect Outlook Web App, Outlook 2016, or Office clients prior to Office 2016.

For info about the changing this setting at the organization level, see File and folder links.

Change the default link type for a site

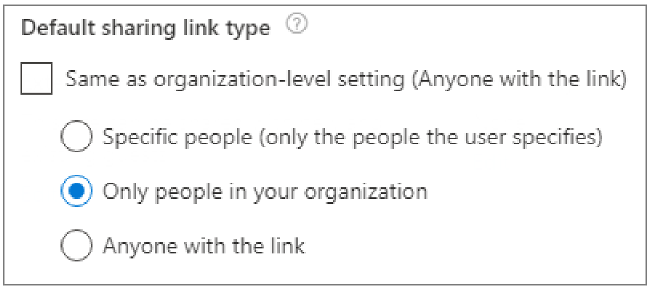
1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **NOTE**
   > If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. In the left column, click to select a site.

3. Select **Sharing**.

4. Under **Default sharing link type**, clear the **Same as organization-level setting** checkbox.



5. Choose the default sharing link setting that you want to use for this site, and then select **Save**.

Related topics

Turn external sharing on or off for a site

Default SharePoint groups

6/26/2020 • 4 minutes to read • Edit Online

The default SharePoint groups are created automatically when you create a site (previously called a "site collection"). The default groups use SharePoint's default permission levels - sometimes called SharePoint roles - to grant users rights and access. The permission levels that these groups have represent common levels of access that users have to have. They are a good place to start when you add users to a SharePoint site.

Administrators can create additional groups to align more closely with specific business needs. Deciding how to design and populate your SharePoint security groups is an important decision that affects security for your site and site content.

Here are links to information on understanding and setting SharePoint permissions.

- Understanding permission levels in SharePoint
- Edit and manage permissions for a SharePoint list or library
- How to create and edit permission levels

Permission levels for default SharePoint groups

SharePoint groups enable you to control access for sets of users instead of individual users. SharePoint groups are usually composed of many individual users. They can also hold Azure Active Directory security groups (created in Microsoft 365 or Azure AD), or can be a combination of individual users and security groups.

Each SharePoint group has a permission level. A permission level is simply a collection of individual permissions, such as Open, View, Edit or Delete. All the users in a group automatically have the permission level of the group. You can organize users into any number of groups, depending on the complexity of your organization, or your needs.

Each site template has a set of SharePoint groups associated with it. When you create a site, you use a site template, and SharePoint automatically creates the correct set of SharePoint groups for the site. The specific collection of groups depends on the type of template that you choose.

For example, the following table shows the groups and permission levels that are created for team sites:

SHAREPOINT GROUPS	DEFAULT PERMISSION LEVEL	APPLIES TO TEAM SITES
Approvers	Approve	No
Designers	Design, Limited Access	No
Hierarchy Managers	Manage Hierarchy	No
<site name> Members	Edit	Yes
<site name> Owners	Full Control	Yes
<site name> Visitors	Read	Yes
Restricted Readers	Restricted Read	No

SHAREPOINT GROUPS	DEFAULT PERMISSION LEVEL	APPLIES TO TEAM SITES
Style Resource Readers	Limited Access	No
Quick Deploy Users	Contribute	No
Translation Mangers	Limited Access	No

Suggested uses for SharePoint groups

The following table describes the SharePoint groups that are created when you use a standard site template to create a site. The table also provides suggested uses for each group.

GROUP NAME	PERMISSION LEVEL)	USE THIS GROUP FOR:
Approvers	Approve	Members of this group can edit and approve pages, list items, and documents.
Designers	Design	Members of this group can edit lists, document libraries, and pages in the site. Designers can create Master Pages and Page Layouts in the Master Page Gallery and can change the behavior and appearance of each subsite by using master pages and CSS files.
Hierarchy Managers	Manage Hierarchy	Members of this group can create sites, lists, list items, and documents.
Owners	Full Control	People who must be able to manage site permissions, settings, and appearance.
Members	Edit or Contribute	People who must be able to edit site content. Permission level depends on the site template that was used to create the site
Visitors	Read	People who must be able to see site content, but not edit it.
Restricted Readers	Restricted Read	People who should be able to view pages and documents but not view versions or permissions.
Style Resource Readers	Restricted Read	People in this group have Limited Access to the Style Library and Master Page Gallery.
Quick Deploy Users	Contribute	These users can schedule Quick Deploy jobs (Content Deployment).
Viewers	View Only	These users see content, but can't edit or download it.

Special SharePoint Groups

"Everyone except external users" is a special group that doesn't appear in the Microsoft 365 admin center, and "Company Administrator" acts like a group but is a role in Azure AD.

Everyone except external users All users added to your organization automatically become members of "Everyone except external users". Please note that you cannot change default permissions granted to "Everyone except external users" on Microsoft 365 group-connected team sites. If a group-connected team site is set to "Public," "Everyone except external users" has a default permission level of "Edit." When a group-connected team site is set to "Private," "Everyone except external users" can't be granted any permission to the site. Although the "Site permissions" tab will allow modifications to be granted, a background job will block such modifications to take effect. To change the privacy setting for a group-connected team site, select the Settings icon, and then select **Site information**.

Company Administrator This group contains all users who are assigned the global admin role. For more info about this role and its permissions in Azure AD, see Company administrator. The root site for your organization is created with "Company Administrator" as the primary admin.

Site administrators

	SHAREPOINT IN MICROSOFT 365	SHAREPOINT SERVER
Who can use this group?	Yes	Yes

A site can have several site admins, but must have one and only one primary administrator. Any site admin can add or remove other admins. Site admins have full control of the site root and any subsites in the site, and can audit all site content.

In SharePoint Server, you designate a site collection administrator when you create a site.

SharePoint admins

	SHAREPOINT IN MICROSOFT 365	SHAREPOINT SERVER
Who can use this group?	Yes	No, by default. Requires special installation.

In SharePoint in Microsoft 365, there is also a SharePoint admin. A SharePoint admin can use the SharePoint admin center or PowerShell to manage settings for all sites. Any global admin in Microsoft 365 also has the permissions of a SharePoint admin. For more info about the SharePoint admin role, see About the SharePoint admin role in Microsoft 365.

If you are using SharePoint Server, you do not have a SharePoint admin or SharePoint admin center.

Sharing errors in SharePoint and OneDrive

4/22/2020 • 11 minutes to read • Edit Online

This article covers the different errors that you might encounter when sharing files or folders from SharePoint or OneDrive in Microsoft 365. You need to be a global or SharePoint admin in your organization to fix these errors. If you are not an administrator, contact your help desk and give them your error code.

Note that changing these settings changes the types of external sharing that are allowed in your organization. In some cases, these settings may have been set by someone in your organization for business reasons.

OSE201

Error OSE201 indicates that external sharing is turned off for all of your SharePoint and OneDrive sites.

First, change the external sharing setting for your organization:

1. Go to the Sharing page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Under **External sharing**, for both SharePoint and OneDrive, select **Anyone** or **New and existing guests**.
3. Select **Save**.

Next, check the external sharing settings for the site that you want to share from.

If you're sharing from a SharePoint site:

1. In the new SharePoint admin center, in the left pane, select **Sites** > **Active sites**.
2. Select the site that you want to share from, and then select **Sharing**.
3. Make sure that either **New and existing guests** or **Anyone** is selected, and if you made changes, select **Save**.

Try sharing again.

If you're sharing from OneDrive:

1. In the Microsoft 365 admin center, in the left pane, under **Users**, select **Active users**.
2. Select the user, and then select the **OneDrive** tab.
3. Select **Manage external sharing**.
4. Make sure **Let people outside your organization access your site** is turned on, and **Allow sharing with anonymous guest links and authenticated users** or **Allow sharing to authenticated guest users with invitations** is selected.

Try sharing again.

OSE202

Error OSE202 indicates that you can only share with guests who are already in your directory. You can add guests directly through Azure Active Directory, or you can change the setting by doing the following:

First, change the external sharing setting for your organization.

1. Go to the Sharing page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Under **External sharing**, select **Anyone** or **New and existing guests** for both SharePoint and OneDrive.
3. Select **Save**.

Next, check the external sharing settings for the site that you want to share from.

If you're sharing from a SharePoint site:

1. In the left pane of the new SharePoint admin center, select **Sites** > **Active sites**.
2. Select the site that you want to share from, and then select **Sharing**.
3. Make sure that either **New and existing guests** or **Anyone** is selected, and if you made changes, select **Save**.

Try sharing again.

If you're sharing from OneDrive:

1. In the Microsoft 365 admin center, in the left pane, under **Users**, select **Active users**.
2. Select the user, and then select the **OneDrive** tab.
3. Select **Manage external sharing**.
4. Make sure **Let people outside your organization access your site** is turned on, and **Allow sharing with anonymous guest links and authenticated users** or **Allow sharing to authenticated guest users with invitations** is selected.

Try sharing again.

OSE204

Error OSE204 indicates that sharing is turned off for the site that you're trying to share from. You can change the setting as follows:

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select the site that you want to share from, and then select **Sharing**.

3. Make sure that either **New and existing guests** or **Anyone** is selected, and then select **Save**.

Try sharing again.

OSE205

Error OSE205 indicates that you can only share the site with guests who are already in your directory. You can add guests directly through Azure Active Directory, or you can change the setting by doing the following:

1. Go to the Active sites page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select the site that you want to share from, and then select **Sharing**.
3. Make sure that either **New and existing guests** or **Anyone** is selected, and then select **Save**.

OSE207

Error OSE207 indicates that external sharing is turned off for OneDrive. You can change this setting as follows:

1. Go to the Sharing page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Under **External sharing**, select **Anyone** or **New and existing guests** for OneDrive.
3. Select **Save**.

Try sharing again.

OSE208

Error OSE208 indicates that you can only share OneDrive files and folders with guests who are already in your directory. You can add guests directly through Azure Active Directory, or you can change the setting by doing the following:

1. Go to the Sharing page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Under **External sharing**, change the OneDrive setting to either **Anyone** or **New and existing external users**.

3. Select **Save**.

Try sharing again.

OSE303

Error OSE303 indicates that the person sharing the file or folder is not a member of the security groups that are allowed to share with guests and by using Anyone links. To change this setting:

1. Go to the Sharing page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Select **Limit external sharing to specific security groups**.

3. Under **Who can share outside your organization**, note the security groups listed for **Let only users in selected security groups share with authenticated external users and using anonymous links**. You need to add the user to one of the listed security groups. (Alternatively, you can clear the check box and remove the sharing restriction.)

To add a user to a security group:

1. On the Groups page of the Microsoft 365 admin center, find the group you want to edit.
2. Select the group, and then on the **Members** tab, select **View all and manage members**.
3. Select **Add members**.
4. Enter the user's name in the search box, select the check box in the results list, and then select **Save**.
5. Select **Close** three times.

Try sharing again.

OSE304

Error OSE304 indicates that the person sharing the file or folder is not a member of the security groups that are allowed to share with guests. To change this setting:

1. Go to the Sharing page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Select **Limit external sharing to specific security groups**.

3. Under **Who can share outside your organization**, note the security groups listed for **Let only users in selected security groups share with authenticated external users**. You need to add the user to one of the listed security groups. (Alternatively, you can clear the check box and remove the sharing restriction.)

To add a user to a security group:

1. On the Groups page of the Microsoft 365 admin center, find the group you want to edit.
2. Select the group, and on the **Members** tab, select **View all and manage members**.
3. Select **Add members**.
4. Enter the user's name in the search box, select the check box in the results list, and then select **Save**.
5. Select **Close** three times.

Try sharing again.

OSE401

Error OSE401 indicates that your organization-level setting lets you share with only people on specific domains. The person you're trying to share with is not on one of the listed domains. To change this setting:

1. Go to the Sharing page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Under **Advanced settings for external sharing**, select **Add domains**, add the domain that you want to share with to the list of allowed domains, and select **OK**. Alternatively, you can turn off domain filtering by clearing the **Limit external sharing by domain** check box.

3. Select **Save**.

Try sharing again.

OSE402

Error OSE402 indicates that your organization-level setting blocks sharing with people on specific domains. The person you're trying to share with is on one of the listed domains. To change this setting:

1. Go to the Sharing page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Under **Advanced settings for external sharing**, select **Add domains**, remove the domain from the list of blocked domains, and select **OK**. Alternatively, you can turn off domain filtering by clearing the **Limit external sharing by domain** check box.

3. Select **Save**.

Try sharing again.

OSE403

Error OSE403 indicates that the site from which you're sharing lets you share with only people on specific domains. The person you're trying to share with is not on one of the listed domains. To change this setting:

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Classic site collections page**, select **Open**.

3. Select the site that you're sharing from, and in the ribbon, select **Sharing**.

4. Under **Site collection additional settings**, add the domain that you want to share with to the list of allowed domains. Alternatively, you can turn off domain filtering by clearing the **Limit external sharing using domains** check box.

5. Select **Save**.

Try sharing again.

OSE404

Error OSE404 indicates that the site from which you're sharing blocks sharing with people on specific domains. The person you're trying to share with is on one of the listed domains. To change this setting:

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Classic site collections page**, select **Open**.

3. Select the site that you're sharing from, and in the ribbon, select **Sharing**.

4. Under **Site collection additional settings**, remove the domain that you want to share with from the list of blocked domains. Alternatively, you can turn off domain filtering by clearing the **Limit external sharing using domains** check box.

5. Select **Save**.

Try sharing again.

See also

External sharing overview

Turn external sharing on or off for SharePoint

Stop sharing files or folders or change permissions

Report on file and folder sharing in a SharePoint site

7/1/2020 • 2 minutes to read • Edit Online

You can create a CSV file of every unique file, user, permission and link on a given SharePoint site or OneDrive. This can help you understand how sharing is being used and if any files or folders are being shared with guests. You must be a site admin to run the report.

When you run the report, the CSV file is saved to a location of your choosing on the site.

In Microsoft SharePoint, if you don't want site members to see the report, consider creating a folder with different permissions where only site owners can access the report.

To run the report (SharePoint)

1. Open the site where you want to run the report
2. On the **Settings** menu, click **Site usage**.
3. In the **Shared with external users** section, click **Run report**.
4. Choose a location to save the report, and then click **Run report**.

To run the report (OneDrive)

1. Open OneDrive.
2. On the **Settings** menu, click **OneDrive settings**.
3. Click **More settings**, and then click **Run sharing report**.
4. Choose a location to save the report, and then click **Save**.

The report may take some time to run depending on the size of the site.

When the report is finished running you will receive an email with a link to the report.

CSV format

For items shared with direct access, the report contains one row for each user / item combination. SharePoint groups are shown in the report, but not individual users inside them.

For items shared with a link, the report contains a row for each signed-in user who has used the link or has been sent the link through the sharing dialog. Links emailed directly that haven't been clicked, and *Anyone* links are not included in the report.

The report contains the following columns:

COLUMN	DESCRIPTION
Resource Path	The relative URL of the item
Item Type	The type of item (web, folder, file, etc.)
Permission	The permission level the user has on this item

COLUMN	DESCRIPTION
User Name	Friendly name of the user or group that has access to this item. If this is a sharing link, the user name is *SharingLink*
User E-mail	The email address of the user who has access to this item. This is blank for SharePoint groups.
User or Group Type	The type of user or group: Member (internal), Guest (external), SharePoint group, Security group or Microsoft 365 group. (Note that *Member* refers to a member in the directory, not a member of the site.)
Link ID	The GUID of the sharing link if user name is *Sharing Link*
Link Type	The type of link (Anonymous, Company, Specific People) if user name is *Sharing Link*
AccessViaLinkID	The **Link ID** used to access the item if a user's permission to an item is via a link.

Restrict sharing of SharePoint and OneDrive content by domain

4/22/2020 • 3 minutes to read • Edit Online

If you want to restrict sharing with other organizations (either at the organization level or site level), you can limit sharing by domain.

> **NOTE**
>
> If you have enrolled in the SharePoint and OneDrive integration with Azure AD B2B Preview, invitations in SharePoint are also subject to any domain restrictions configured in Azure Active Directory.

Limiting domains

You can limit domains by allowing only the domains you specify or by allowing all domains except those you block.

To limit domains at the organization level

1. Go to the Sharing page of the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   > **NOTE**
   >
   > If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Sharing page.

2. Under **Advanced settings for external sharing**, select the **Limit external sharing by domain** check box, and then select **Add domains**.
3. To create an allow list (most restrictive), select **Allow only specific domains**; to block only the domains you specify, select **Block specific domains**.
4. List the domains (maximum of 3000) in the box provided, using the format *domain.com.* If listing more than one domain, enter each domain on a new line.

   > **NOTE**
   >
   > Wildcards are not supported for domain entries.

5. Select **Save**.

You can also configure the organization-wide setting by using the Set-SPOTenant PowerShell cmdlet.

You can also limit domains at the site collection level. Note the following considerations:

- In the case of conflicts, the organization-wide configuration takes precedence over the site collection configuration.

- If an organization-wide allow list is configured, then you can only configure an allow list at the site collection level. The site collection allow list must be a subset of the organization's allow list.
- If an organization-wide deny list is configured, then you can configure either an allow list or a deny list at the site collection level.
- For individual OneDrive site collections, you can only configure this setting by using the Set-SPOSite Windows PowerShell cmdlet.

To limit domains for a site

1. Go to the Active sites page in the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Select the site that you want to restrict domains on.
3. On the **Policies** tab, under **External sharing**, select **Edit**.
4. Under **Advanced settings for external sharing**, select the **Limit external sharing by domain** check box, and then select **Add domains**.
5. Select **Allow only specific domains** to create an allow list (most restrictive), or to block only the domains you specify, select **Block specific domains**.
6. List the domains (maximum of 100) in the box provided, using the format *domain.com.* If listing more than one domain, enter each domain on a new line.

> **NOTE**
> Wildcards are not supported for domain entries.

7. Select **Save**, and then select **Save** again.

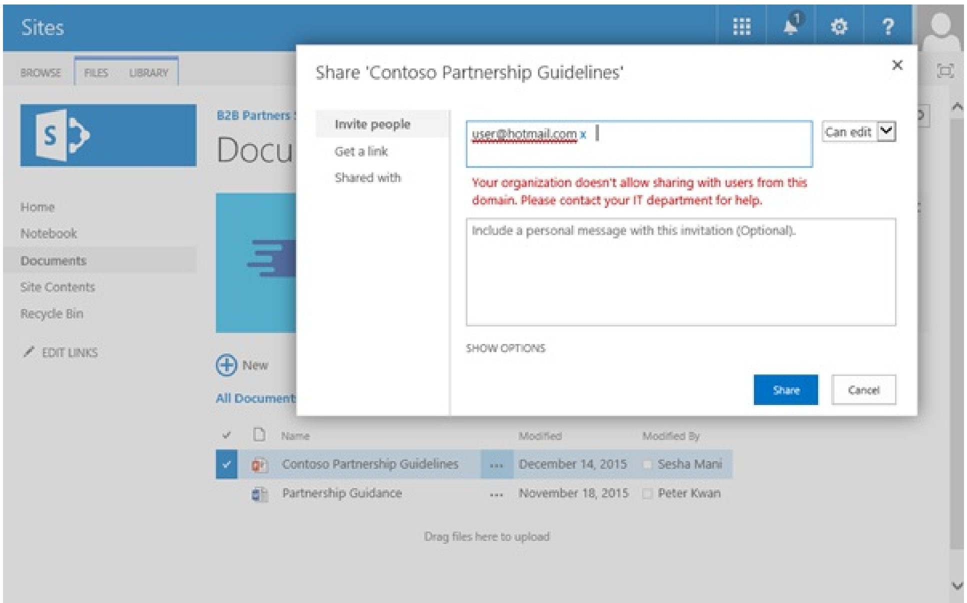
> **NOTE**
> To configure the site collection setting for site collections that do not appear in this list (such as Group-connected sites or individual OneDrive site collections), you must use the Set-SPOSite PowerShell cmdlet.

Sharing experience

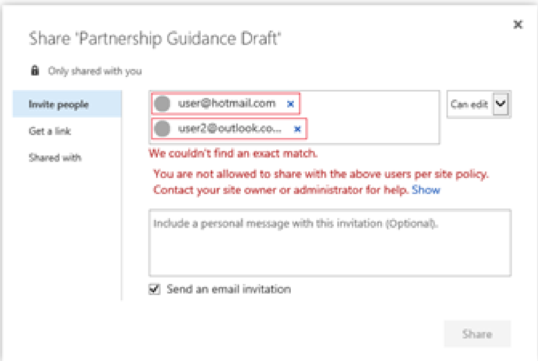
After you limit sharing by domain, here's what you'll see when you share a document:

- **Sharing content with email domains that are not allowed.** If you attempt to share content with a guest whose email address domain isn't allowed, an error message will display and sharing will not be allowed.

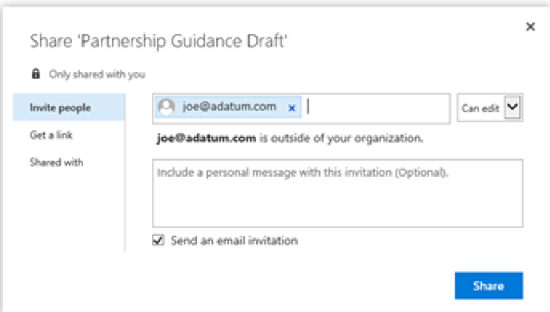
  (If the user is already in your directory, you won't see the error, but they will be blocked if they attempt to access the site.)



- **Sharing OneDrive files with guests on domains that aren't allowed.** If a users tries to share a OneDrive file with a guest whose email domain isn't allowed, an error message will display and sharing will not be allowed.



- **Sharing content with email domains that are allowed.** Users will be able to successfully share the content with the guest. A tooltip will appear to let them know that the guest is outside of their organization.



User auditing and lifecycle management

As with any extranet sharing scenario it's important to consider the lifecycle of your guest users, how to audit their activity, and eventually how to archive the site. See Planning SharePoint business-to-business (B2B) extranet sites for more information.

See also

External sharing overview

Extranet for Partners with Microsoft 365

Set-SPOTenant

Use SharePoint as a business-to-business (B2B) extranet solution

1/8/2021 • 3 minutes to read • Edit Online

An extranet site in Microsoft SharePoint is a site that you create to let external partners have access to specific content, and to collaborate with them. Extranet sites are a way for partners to securely do business with your organization. The content for your partner is kept in one place and they have only the content and access they need. They don't need to email the documents back and forth or use tools that are not sanctioned by your IT department.

Traditionally, deploying a SharePoint *on-premises* extranet site involves complex configuration to establish security measures and governance, including granting access inside the corporate firewall, and expensive initial and on-going cost.

But with Microsoft 365, partners connect directly to a members-only site in SharePoint, without access to your on-premises environment or any other SharePoint sites. Microsoft 365 extranet sites can be accessed anywhere there's an Internet connection.

Depending on your collaboration needs, you can include Microsoft 365 groups or Microsoft Teams as part of your extranet.

Why use Microsoft 365 for a B2B extranet?

Time-to-value and Cost savings: a Microsoft 365 B2B extranet eliminates the need for creating a costly on-premises extranet sites. No additional hardware is required and using Microsoft 365 greatly reduces the resource and labor costs. Your IT department can focus on more important tasks than creating and maintaining extranet infrastructure.

Secure sharing: Microsoft 365 B2B extranet provides a highly secure sharing experience with the IT governance and policies that you require, including:

- The ability to protect yourself against accidental sharing by using owner-approved sharing through Microsoft 365 groups or teams, which prevents users from inviting new users without approval.
- The ability to restrict partner users to a single site or team. They cannot search for or view any content on sites or teams to which they have not been invited.

Seamless collaboration: Collaborate with your partner users as if they are part of your organization, including allowing them chat and conferencing through Teams.

Auditing and reporting. Microsoft 365 B2B extranet offers visibility into the access of your content by external partner users. One of the key IT benefits is to be able to audit usage, including being able to see who is inviting whom and when an external user logs in to access the content. See Search the audit log in the Security & Compliance Center for more information.

Security and governance. Microsoft 365 features such as data loss prevention and Microsoft Cloud App Security provide a robust feature set to help you create a secure guest sharing environment.

Compare Microsoft 365 extranet with a traditional SharePoint on-premises extranet

	Microsoft 365 extranet	SharePoint "on-premises" extranet
Firewall access required for external users	No	Yes
Complex network and infrastructure configuration required	No	Yes
Security hardening	Managed through Microsoft 365 configurations	Manually configured by IT staff
IT labor intensive	No	Yes
Ongoing maintenance needed	Minimal	Considerable
Additional hardware needed	No	Often
Controlling sharing experience for the extranet	Part of Microsoft 365 sites functionality	Often requires custom solutions/apps

Get started

To get started setting up a SharePoint extranet site:

1. Read Collaborate with guests in a site if you want to limit your extranet to a site with a Microsoft 365 group, or Collaborate with guests in a team if you want to include a team.
2. Read Create a B2B extranet with managed guests if you want to delegate guest access management to specific approvers in either your organization or the partner organization.
3. Read Limit accidental exposure to files when sharing with guests and Create a secure guest sharing environment to learn about options for securing your guest sharing environment.

See also

Microsoft 365 guest sharing settings reference

SharePoint site permissions

1/8/2021 • 6 minutes to read • Edit Online

This article contains advanced scenarios for customizing site permissions. Most organizations won't need these options. If you just want to share files or folders, see Share SharePoint files or folders. If you want to share a site, see Share a site.

While SharePoint allows considerable customization of site permissions, we highly recommend using the built-in SharePoint groups for communication site permissions and managing team site permissions through the associated Microsoft 365 group. For information about managing permissions in the SharePoint modern experience, see Sharing and permissions in the SharePoint modern experience.

If you do need to customize SharePoint groups, this article describes how.

Customize site permissions

A SharePoint group is a collection of users who all have the same set of permissions to sites and content. Rather than assign permissions one person at a time, you can use groups to conveniently assign the same permission level to many people at once.

> **NOTE**
> To do the following steps, you need a permission level that includes permissions to *Create Groups* and *Manage Permissions*. The **Full Control** level has both. For more information, see Understanding permission levels in SharePoint.

Create a group

1. On your website or team site, click **Settings** , and click **Site permissions**.
2. On the **Permissions** page, click **Advanced Permissions Settings**.

   The permissions page opens.
3. On the **Permissions** tab, click **Create Group**.
4. On the **Create Group** page, in the **Name** and **About me** boxes, type a name and description for this SharePoint group.
5. In the **Owner** box, specify a single owner of this security group.
6. In the **Group Settings** section, specify who can view and edit the membership of this group.
7. In the **Membership Requests** section, select the settings that you want for requests to join or leave the group. You can specify the email address to which requests should be sent.
8. In the **Give Group Permissions to this Site** section, choose a permission level for this group.
9. Click **Create**.

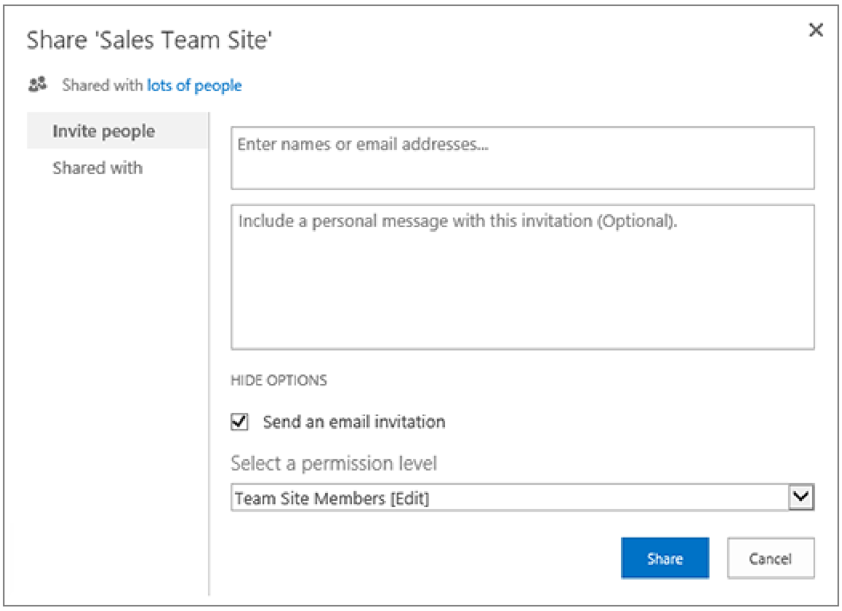
Add users to a group

You can add users to a group at any time.

1. On your website or team site, click **Share**

If you see **Members** instead of **Share**, click **Members**, and then click **Add members**.

2. By default, the **Share** dialog that appears displays the message **Invite people to Edit** or **Invite people**. This invites the users who you add to join the SharePoint Members group. To choose a different group and permission level, click **Show options** and then choose a different SharePoint group or permission level under **Select a group or permission level**.



3. In the **Enter names, email addresses, or Everyone** box, enter the name or email address of the user or group that you want to add. When the name appears in a confirmation box below your entry, select the name to add it to the text box.

4. If you want to add more names, repeat these steps.

5. (Optional) Enter a personalized message to send to the new users in **Include a personal message with this invitation**.

6. Click **Share**.

Remove users from a group

1. On your website or team site, click **Settings** , and click **Site settings**. If you don't see **Site settings**, click **Site information**, and then click **View all site settings**. On some pages, you may need to click **Site contents**, then click **Site settings**.

2. On the **Site Settings** page, under **Users and Permissions**, click **People and Groups**.

3. On the **People and Groups** page, in the Quick Launch, click the name of the group that you want to remove users from.

4. Select the check boxes next to the users who you want to remove, click **Actions**, and then click **Remove Users from Group**.

5. In the confirmation window, click **OK**.

Grant site access to a group

1. On your website or team site, click **Settings** , and click **Site settings**. If you don't see **Site settings**, click **Site information**, and then click **View all site settings**. On some pages, you may need to click

Site contents, then click **Site settings**.

2. On the **Site Settings** page, under **Users and Permissions**, click **Site Permissions**.

3. On the **Permissions** tab, click **Grant Permissions**.

4. In the **Share** dialog, type the name of the SharePoint group that you want to give access to.

5. By default, the **Share** dialog displays the message **Invite people to Edit** or **Invite people** with **Can edit** permissions. This grants permissions in the SharePoint Members group. To choose a different permission level, click **Show options** and then choose a different SharePoint group or permission level under **Select a permission level** or **Select a group or permission level**. The drop-down box shows both groups and individual permission levels, like **Edit** or **View Only**.

6. Click **Share.**

Delete a group

Caution

We recommend that you don't delete any of the default SharePoint groups, because this can make the system unstable. You should only delete group(s) you have created and no longer want to use.

1. On your website or team site, click **Settings** , and click **Site settings**. If you don't see **Site settings**, click **Site information**, and then click **View all site settings**. On some pages, you may need to click **Site contents**, then click **Site settings**.

2. On the **Site Settings** page, under **Users and Permissions**, click **People and Groups**.

3. On the People and Groups page, click the name of the SharePoint group that you want to delete.

4. Click **Settings**, and then click **Group Settings**.

5. At the bottom of the **Change Group Settings** page, click **Delete**.

6. In the confirmation window, click **OK** .

Assign a new permission level to a group

If you have customized a permission level or created a new permission level, you can assign it to groups or users.

1. On your website or team site, click **Settings** , and click **Site settings**. If you don't see **Site settings**, click **Site information**, and then click **View all site settings**. On some pages, you may need to click **Site contents**, then click **Site settings**.

2. On the **Site Settings** page, under **Users and Permissions**, click **Site Permissions**.

3. Select the check box next to the user or group to which you want to assign the new permission level.

4. On the **Permissions** tab, click **Edit User Permissions**.

5. On the **Edit Permissions** page, select the check box next to the name of the new permission level. If you select multiple permission levels, the permission level assigned to the group is the union of the individual permissions in the different levels. That is, if one level includes permissions (A, B, C), and the other level includes permissions (C, D), the new level for the group includes permissions (A, B, C, D).

6. Click **OK**.

> **NOTE**
>
> Permissions for the default SharePoint groups (Owners, Members, and Visitors) for Team sites that are connected to a Microsoft 365 group can't be modified.

Add, change, or remove a site collection administrator

1. On the site, click **Settings**, and click **Site settings**. If you don't see **Site settings**, click **Site information**, and then click **View all site settings**. On some pages, you may need to click **Site contents**, then click **Site settings**.

2. On the **Site Settings** page, under **Users and Permissions**, click **Site Collection Administrators**.

3. In the **Site Collection Administrators** box, do one of the following:

   - To add a site collection administrator, enter the name or user alias of the person who you want to add.

   - To change a site collection administrator, click the **X** next to the name of the person, and then enter a new name.

   - To remove a site collection administrator, click the **X** next to the name of the person.

4. Click **OK**.

   > **NOTE**
   >
   > To see the Site Collection Administrators link, you must be a site collection administrator, or a global or SharePoint admin in your organization. This link is not displayed to site owners.

Permissions inheritance in SharePoint

5/2/2020 • 6 minutes to read • Edit Online

While SharePoint allows considerable customization of site permissions, including changing inheritance, we highly recommend not breaking inheritance. Use the built-in SharePoint groups for communication sites and manage team site permissions through the associated Microsoft 365. Use sharing links to share individual files and folders with people outside the site. This allows for much easier administration. For information about managing permissions in the SharePoint modern experience,see Sharing and permissions in the SharePoint modern experience.

What is permissions inheritance?

Permissions inheritance means that the permission settings of an element in a site collection are passed on to the children of that element. In this way, sites inherit permissions from the root site of the site collection, libraries inherit from the site that contains the library, and so on. Permission inheritance enables you to make a permission assignment once, and have that permission apply to all sites, lists, libraries, folders and items that inherit permissions. This behavior can reduce complexity and the amount of time Administrators and Site Owners spend on security management.

By default, SharePoint sites inherit permissions from a parent site. This means that when you assign a user to the Members group, the user's permissions automatically cascade down through all the sites, lists, libraries, folders and items that inherit the permission level.

What is a parent in SharePoint permissions?

The term parent, when used in SharePoint permissions, is just a way to emphasize inheritance. The parent passes down its permission settings to all its children. By default, the root site of a site collection is the first parent for all the sites and other objects that are below it in the site hierarchy.

The site collection root is not the only parent on a site. Every securable object (sites, libraries, lists, and so on) in a site collection can be a parent. That is, the site collection root is the parent of its subsites, each site is the parent of its libraries and lists, and each list is the parent of the list items in it. In this terminology, an object with a parent is known as a child. So, a subsite is the child of its parent site, a list item is the child of its list parent, and so on.

By default, permissions are inherited from parent to child. That is, if you do not change the permission structure, then a list item inherits permissions (through its parent list) from the top-level site in the collection. However, even if you break inheritance for a list, that list is still a parent for its own list items. The list items for the list inherit the permissions that the list has, and if you change the permissions for the list, the list items inherit the changes.

When you first break this chain of inheritance from parent to child, the child starts with a copy of the parent's permissions. Then, you edit these permissions to make them the way that you want. You can add permissions, remove permissions, create special groups, and so on. None of the changes affect the original parent. And, if you decide that breaking inheritance was the wrong decision, you can resume inheriting permissions at any time.

When a user shares or stops sharing an item that contains other items with broken inheritance, a one-time push down of that permission addition or removal is sent to all child items, even those with broken inheritance. This is true for both direct permissions and sharing links. When managing permissions for an item with broken inheritance, users are able to remove any direct permissions on it. If an item with broken inheritance is accessible by a sharing link that was created on one of its parent folders and a user does not want that link to grant access to the item, then users can either remove the link entirely or they can move the file outside of the folder for which sharing link has permissions.

More about permissions inheritance

Permission inheritance enables an administrator to assign permission levels at one time, and have the permissions apply throughout the site collection. Permissions pass from parent to child throughout the SharePoint hierarchy, from the top level of a site to the bottom. Permission inheritance can save time for site administrators, especially on large or complex site collections.

However, some scenarios have different requirements. In one scenario, you might have to restrict access to a site because it contains sensitive information that you must protect. In a different scenario, you might want to expand access and invite others to share information. If you want, you can break the inheritance behavior (stop inheriting permissions) at any level in the hierarchy.

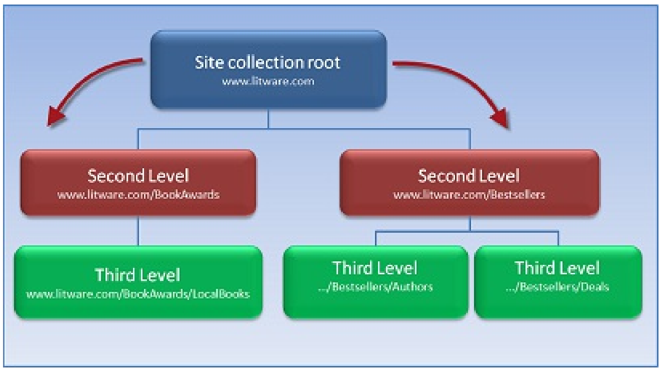
Let's look at examples of these different scenarios.

Suppose that you have a book distribution company called Litware, and that you subscribe to Microsoft 365. You create a SharePoint site named www.litware.com. This is the site collection root. At the site collection root, you set up SharePoint groups, assign permission levels, and add users to the groups.

Suppose then that you create subsites, such as www.Litware.com/BookAwards and www.litware.com/Bestsellers, and that these subsites contain more subsites.

A scenario that uses default behavior

The following illustration shows the default behavior, when permissions pass directly to subsites. That is, the groups and permission levels that you assigned at the site collection root pass down automatically to the subsite for reuse.

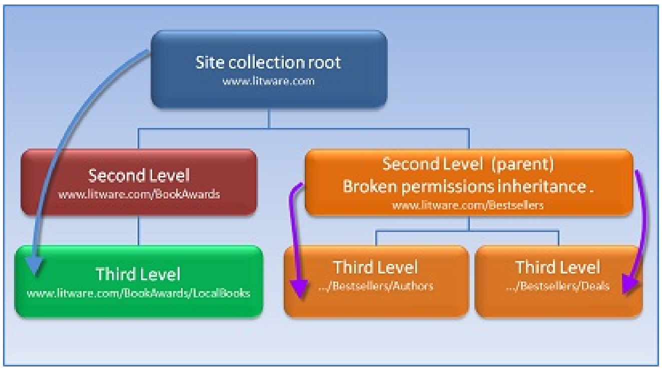


A scenario that restricts access to a site and its children

You might want to do this to restrict access to the separated site and its children.

For example, suppose that your company, Litware, supports active promotional opportunities and deals for bestsellers. Because the deals that the company offers are secret, only certain people in the company can access the information about the bestseller authors and deals. So, the administrators decide to separate the Bestsellers site, and break inheritance.

In the following illustration, the www.Litware.com/Bestsellers breaks inheritance from the parent site, www.litware.com. The site owners for the Best Sellers site change the permissions for the site, removing some groups and creating others. The subsites of the Bestsellers site, Authors and Deals, now inherit permissions only from the Bestsellers subsite. Only the groups and users for Bestsellers can access the lists and libraries that contain sensitive information.



For ease of maintenance, we recommend that you use a similar method to restrict access. That is, organize your site so that sensitive material is in the same place. If you organize the site this way, you only have to break inheritance one time, for that specific site or library. This is much less overhead. It requires much less work than creating separate permission structures in many locations for individual subsites and libraries.

A scenario that shares access for a library and its documents

In this scenario, suppose that Jane is an editor in your Local Books division. Jane is collaborating with an author on a history of the labor union movement. She compiled a research document that she wants to share with the author. The research would be really useful in their collaboration. However, the author does not work for Litware and can't access the information on the Litware site.

Jane has a simple solution - she can just share the document together with the author by clicking a command on the ribbon. SharePoint automatically handles all the details of permissions and access, by breaking inheritance on the document itself. Now, the local author can browse the site to the document location and access the document, but can't view or access any other information on the site.

For more info about inviting an external user to use information on your site, see Share SharePoint files or folders in Microsoft 365.

Permission levels in SharePoint

1/8/2021 • 14 minutes to read • Edit Online

While SharePoint offers a variety of permission levels for sites, we highly recommend using the built-in SharePoint groups for communication sites and managing team site permissions through the associated Microsoft 365 group. This allows for much easier administration. For information about managing permissions in the SharePoint modern experience, see Sharing and permissions in the SharePoint modern experience.

Understanding permission levels

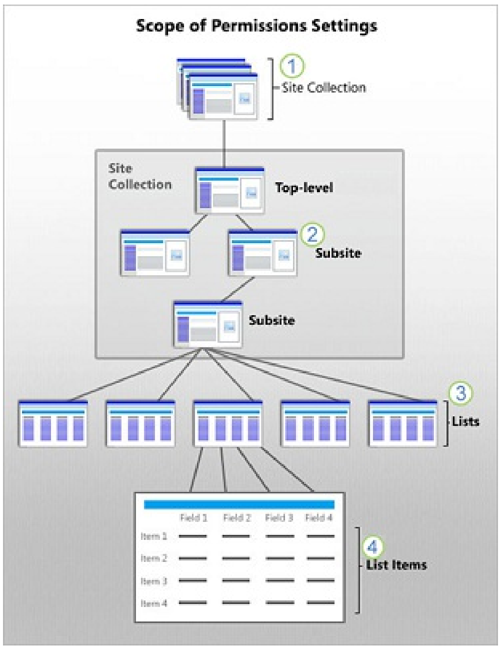
The easiest way to work with permissions is to use the default groups and permissions levels provided, which cover most common scenarios. But, if you need to, you can set more fine-grained permissions beyond the default levels. This article describes the different permissions and permission levels, how SharePoint groups and permissions work together, and how permissions cascade through a site collection.

> **NOTE**
>
> Want to go straight to the steps for changing or setting permission levels? See How to create and edit Permission Levels.

Overview and permissions inheritance

If you work on a site, you are working inside a site collection. Every site exists in a site collection, which is a group of sites under a single top-level site. The top-level site is called the root site of the site collection.

The following illustration of a site collection shows a simple hierarchy of sites, lists and list items. The permissions scopes are numbered, starting at the broadest level at which permissions can be set, and ending at the narrowest level (a single item in a list).



Inheritance

An important concept to understand is permissions inheritance. By design, all the sites and site content in a collection inherit the permissions settings of the root or top-level site. When you assign unique permissions to sites, libraries, and items, those items no longer inherit permissions from their parent site. Here's more information on how permissions work within the hierarchy:

- A site collection administrator configures permissions for the top level site or root site for the whole collection.
- If you are a site owner, you can change permission settings for the site, which stops permission inheritance for the site.
- Lists and libraries inherit permissions from the site to which they belong. If you are a site owner, you can stop permissions inheritance and change the permission settings for the list or library.
- List items and library files inherit permissions from their parent list or library. If you have control of a list or library, you can stop permissions inheritance and change permissions settings directly on a specific item.

  It is important to know that a user can interrupt the default permission inheritance for a list or library item by sharing a document or item with someone who does not have access. In that case, SharePoint automatically stops inheritance on the document.

Default Permission Levels

Default permission levels allow you to quickly and easily provide common levels of permissions for one user or groups of users.

You can make changes to any of the default permissions levels, except **Full Control** and **Limited Access**, both of which are described more fully in the following table.

PERMISSION LEVEL	DESCRIPTION	
Full Control	Contains all available SharePoint permissions. By default, this permission level is assigned to the Owners group. It can't be customized or deleted.	
Design	Create lists and document libraries, edit pages and apply themes, borders, and style sheets on the site. There is no SharePoint group that is assigned this permission level automatically.	
Edit	Add, edit, and delete lists; view, add, update, and delete list items and documents. By default, this permission level is assigned to the Members group.	
Contribute	View, add, update, and delete list items and documents.	
Read	View pages and items in existing lists and document libraries and download documents.	

PERMISSION LEVEL	DESCRIPTION	
Limited Access	Enables a user or group to browse to a site page or library to access a specific content item when they do not have permissions to open or edit any other items in the site or library. This level is automatically assigned by SharePoint when you provide access to one specific item. You cannot assign Limited Access permissions directly to a user or group yourself. Instead, when you assign edit or open permissions to the single item, SharePoint automatically assigns Limited Access to other required locations, such as the site or library in which the single item is located. This allows SharePoint to render the user interface correctly and show the user some context around their location in the site. Limited Access does not grant any additional permissions to the user, so they can't see or access any other content.	
Web-Only Limited Access	Web-Only Limited access is a variant of the ‘Limited Access’ permission level which enables users’ access to the web object only.	
Approve	Edit and approve pages, list items, and documents. By default, the *Approvers* group has this permission.	
Manage Hierarchy	Create sites and edit pages, list items, and documents. By default, this permission level is assigned to the *Hierarchy Managers* group.	
Restricted Read	View pages and documents, but not historical versions or user permissions.	
View Only	View pages, items, and documents. Any document that has a server-side file handler can be viewed in the browser but not downloaded. File types that do not have a server-side file handler (cannot be opened in the browser), such as video files, .pdf files, and .png files, can still be downloaded.	

NOTE

Microsoft 365 subscriptions create a security group called "Everyone except external users" that contains every person you add into the Microsoft 365 directory (except people who you add explicitly as External Users). This security group added to the Members group automatically on Modern Team sites with *Public* privacy settings, so that users in Microsoft 365 can access and edit the SharePoint site. Also, for Modern Team sites created as *Private*, "Everyone except external users" cannot be granted any permissions and people must be explicitly granted permissions. In addition, Microsoft 365 subscriptions create a security group called "Company Administrators", which contains Microsoft 365 Admins (such as Global and Billing Admins). This security group is added to the Site Collection Administrators group. For more info, see Default SharePoint groups.

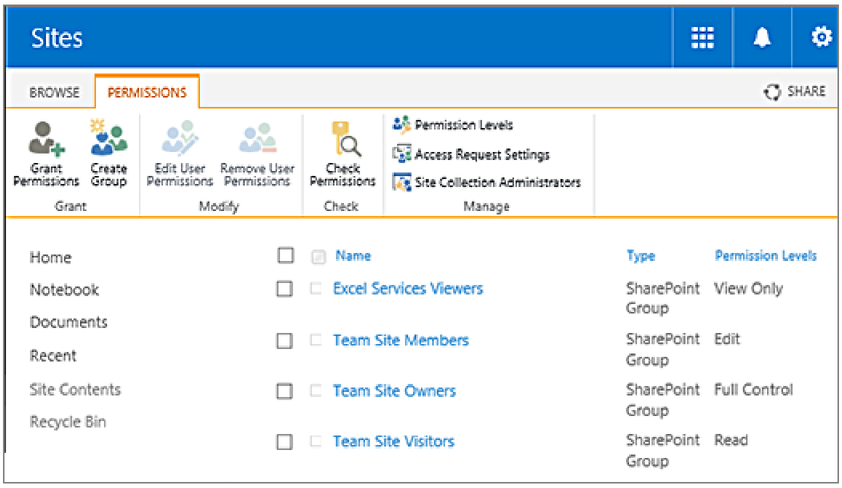
By default, site owners and members can add new users to the site.

To learn more about "Everyone except external users" permission, see Special SharePoint Groups

Permission levels and SharePoint groups

Permission levels work together with SharePoint groups. A SharePoint group is a set of users who all have the same permission level.

The way this works is that you put related permissions together into a permission level. Then you assign that permission level to a SharePoint group.



By default, each kind of SharePoint site includes certain SharePoint groups. For example, a Team Site automatically includes the Owners, Members, and Visitors group. A Publishing Portal site includes those groups and several more, such as Approvers, Designers, Hierarchy Managers, and so on. When you create a site, SharePoint automatically creates a pre-defined set of SharePoint groups for that site. In addition, a SharePoint admin can define custom groups and permission levels.

To learn more about SharePoint groups, see Understanding SharePoint groups.

The SharePoint groups and permission levels that are included by default in your site may differ, depending on:

- The template that you choose for the site
- Whether a SharePoint admin created a unique permissions set on the site that has a specific purpose, such as Search

The following table describes the default permission levels and associated permissions for three standard groups: Visitors, Members, and Owners.

GROUP	PERMISSION LEVEL
Visitors	**Read** This level includes these permissions: Open View Items, Versions, pages, and Application pages Browse User Information Create Alerts Use Self-Service Site Creation Use Remote Interfaces Use Client Integration Features
Members	**Edit** This level includes all permissions in Read, plus: View, add, update and delete Items Add, Edit and Delete Lists Delete Versions Browse Directories Edit Personal User Information Manage Personal Views Add , Update, or Remove Personal Web Parts
Owners	**Full Control** This level includes all available SharePoint permissions.

Site permissions and permission levels

Site permissions apply generally across a SharePoint site. The following table describes the permissions that apply to sites, and show the permission levels that use them.

PERMISSION	FULL CONTROL	DESIGN	EDIT	CONTRIBUTE	READ	LIMITED ACCESS	APPROVE	MANAGE HIERARCHY	RESTRICTED READ	VIEW ONLY
Manage Permissions	X							X		
View Web Analytics Data	X							X		
Create Subsites	X							X		
Manage Web Site	X							X		
Add and Customize Pages	X	X						X		

PERMISSION	FULL CONTROL	DESIGN	EDIT	CONTRIBUTE	READ	LIMITED ACCESS	APPROVE	MANAGE HIERARCHY	RESTRICTED READ	VIEW ONLY
Apply Themes and Borders	X	X								
Apply Style Sheets	X	X								
Create Groups	X									
Browse Directories	X	X	X	X			X	X		
Use Self-Service Site Creation	X	X	X	X	X		X	X		X
View Pages	X	X	X	X	X		X	X	X	X
Enumerate Permissions	X							X		
Browse User Information	X	X	X	X	X	X	X	X		X
Manage Alerts	X							X		
Use Remote Interfaces	X	X	X	X	X		X	X		X
Use Client Integration Features	X	X	X	X	X	X	X	X		X

PERMISSION	FULL CONTROL	DESIGN	EDIT	CONTRIBUTE	READ	LIMITED ACCESS	APPROVE	MANAGE HIERARCHY	RESTRICTED READ	VIEW ONLY
Open	X	X	X	X	X	X	X	X	X	X
Edit Personal User Information	X	X	X	X			X	X		

List permissions and permission levels

List permissions apply to content in lists and libraries. The following table describes the permissions that apply to lists and libraries, and show the permission levels that use them.

PERMISSION	FULL CONTROL	DESIGN	EDIT	CONTRIBUTE	READ	LIMITED ACCESS	APPROVE	MANAGE HIERARCHY	RESTRICTED READ	VIEW ONLY
Manage Lists	X	X	X					X		
Override Check-Out	X	X					X	X		
Add Items	X	X	X	X			X	X		
Edit Items	X	X	X	X			X	X		
Delete Items	X	X	X	X			X	X		
View Items	X	X	X	X	X		X	X	X	X
Approve Items	X	X					X			
Open Items	X	X	X	X	X		X	X	X	
View Versions	X	X	X	X	X		X	X		X
Delete Versions	X	X	X	X			X	X		

PERMISSION	FULL CONTROL	DESIGN	EDIT	CONTRIBUTE	READ	LIMITED ACCESS	APPROVE	MANAGE HIERARCHY	RESTRICTED READ	VIEW ONLY
Create Alerts	X	X	X	X	X		X	X		X
View Application Pages	X	X	X	X	X		X	X		X

Personal permissions and permission levels

Personal permissions apply to content that belongs to a single user. The following table describes the permissions that apply to personal views and web parts, and show the permission levels that use them.

PERMISSION	FULL CONTROL	DESIGN	EDIT	CONTRIBUTE	READ	LIMITED ACCESS	APPROVE	MANAGE HIERARCHY	RESTRICTED READ	VIEW ONLY
Manage Personal Views	X	X	X	X			X	X		
Add/Remove Private Web Parts	X	X	X	X			X	X		
Update Personal Web Parts	X	X	X	X			X	X		

Permissions and dependent permissions

SharePoint permissions can depend on other SharePoint permissions. For example, you must be able to open an item to view it. In this way, View Items permission depends on Open permission.

When you select a SharePoint permission that depends on another, SharePoint automatically selects the associated permission. Similarly, when you clear SharePoint permission, SharePoint automatically clears any SharePoint permission that depends on it. For example, when you clear View Items, SharePoint automatically clears Manage Lists (you can't manage a list if you can't view an item).

> **TIP**
>
> The only SharePoint permission without a dependency is Open. All other SharePoint permissions depend on it. To test a custom permission level, you can just clear "Open". This automatically clears all other permissions.

The following sections contain tables that describe SharePoint permissions for each permission category. For each permission, the table shows the dependent permissions.

- Site permissions and dependent permissions
- List permissions and dependent permissions
- Personal permissions and dependent permissions

Site permissions and dependent permissions

The following table describes the permissions that apply to sites, and show the permissions that depend on them.

PERMISSION	DESCRIPTION	DEPENDENT PERMISSIONS
Manage Permissions	Create and change permission levels on the website and assign permissions to users and groups.	Approve Items, Enumerate Permissions, Open
View Web Analytics Data	View reports on website usage.	Approve Items, Open
Create Subsites	Create subsites such as team sites, Meeting Workspace sites, and Document Workspace sites.	View Pages, Open
Manage website	Perform all administration tasks for the website, which includes managing content.	View Pages, Open
Add and Customize Pages	Add, change, or delete HTML pages or Web Part pages, and edit the website by using a Windows SharePoint Services-compatible editor.	View Items, Browse Directories, View Pages, Open
Apply Themes and Borders	Apply a theme or borders to the whole website.	View Pages, Open
Apply Style Sheets	Apply a style sheet (.css file) to the website.	View Pages, Open
Create Groups	Create a group of users who can be used anywhere within the site collection.	View Pages, Open
Browse Directories	Enumerate files and folders in a website, by using an interface such as SharePoint Designer or web-based Distributed Authoring and Versioning (Web DAV).	View Pages, Open
Use Self-Service Site Creation	Create a website by using Self-Service Site Creation.	View Pages, Open
View Pages	View pages in a website.	Open
Enumerate Permissions	Enumerate permissions on the website, list, folder, document, or list item.	View Items, Open Items, View Versions, Browse Directories, View Pages, Open

PERMISSION	DESCRIPTION	DEPENDENT PERMISSIONS
Browse User Information	View information about users of the website.	Open
Manage Alerts	Manage alerts for all users of the website	View Items, Create Alerts, View Pages, Open
Use Remote Interfaces	Use Simple Object Access Protocol (SOAP), Web DAV, or SharePoint Designer interfaces to access the website.	Open
Open*	Open a website, list, or folder to access items inside that container.	No dependent permissions
Edit Personal User Information	Allow a user to change personal information, such as adding a picture.	Browse User Information, Open

List permissions and dependent permissions

The following table describes the permissions that apply to lists and libraries, and show the permissions that depend on them.

PERMISSION	DESCRIPTION	DEPENDENT PERMISSIONS
Manage Lists	Create and delete lists, add or remove columns in a list, and add or remove public views of a list.	View Items, View Pages, Open, Manage Personal Views
Override Check-Out	Discard or check in a document that is checked out to another user.	View Items, View Pages, Open
Add Items	Add items to lists, add documents to document libraries, and add web discussion comments.	View Items, View Pages, Open
Edit Items	Edit items in lists, edit documents in document libraries, edit web discussion comments in documents, and customize Web Part Pages in document libraries.	View Items, View Pages, Open
Delete Items	Delete items from a list, documents from a document library, and web discussion comments in documents.	View Items, View Pages, Open
View Items	View items in lists, documents in document libraries, and web discussion comments.	View Pages, Open
Approve Items	Approve a minor version of a list item or document.	Edit Items, View Items, View Pages, Open
Open Items	View the source of documents that use server-side file handlers.	View Items, View Pages, Open

PERMISSION	DESCRIPTION	DEPENDENT PERMISSIONS
View Versions	View past versions of a list item or document.	View Items, View Pages, Open
Delete Versions	Delete past versions of a list item or document.	View Items, View Versions, View Pages, Open
Create Alerts	Create e-mail alerts.	View Items, View Pages, Open
View Application Pages	View documents and views in a list or document library.	Open

Personal permissions and dependent permissions

The following table describes the permissions that apply to personal views and web parts, and show the permissions that depend on them.

PERMISSION	DESCRIPTION	DEPENDENT PERMISSIONS
Manage Personal Views	Create, change, and delete personal views of lists.	View Items, View Pages, Open
Add/Remove Private Web Parts	Add or remove private Web Parts on a Web Part Page.	View Items, View Pages, Open, Update Personal Web Parts
Update Personal Web Parts	Update Web Parts to display personalized information.	View Items, View Pages, Open

Lockdown mode

Limited-access user permission lockdown mode is a site collection feature that you can use to secure published sites. When lockdown mode is turned on, fine-grain permissions for the limited access permission level are reduced. The following table details the default permissions of the limited access permission level and the reduced permissions when the lockdown mode feature is turned on.

PERMISSION	LIMITED ACCESS - DEFAULT	LIMITED ACCESS - LOCKDOWN MODE
List permissions: View Application Pages	X	
Site permissions: Browse User Information	X	X
Site permissions: Use Remote Interfaces	X	
Site permissions: Use Client Integration Features	X	X
Site permissions: Open	X	X

Lockdown mode is on by default for all publishing sites, including if a legacy publishing site template was applied to the site collection. Lockdown mode is the recommended configuration if greater security on your sites is a requirement.

If you disable the limited-access user permission lockdown mode site collection feature, users in the "limited access" permissions level (such as Anonymous Users) can gain access to certain areas of your site.

Plan your permission strategy

Now that you have learned about permissions, inheritance, and permission levels, you may want to plan your strategy so that you can set guidelines for your users, minimize maintenance, and ensure compliance with your organization's data governance policies. For tips on planning your strategy, see Plan your permissions strategy.

Permission levels

5/2/2020 • 4 minutes to read • Edit Online

While SharePoint allows considerable customization of site permissions, including custom permission levels, we highly recommend using the built-in SharePoint groups for communication site permissions and managing team site permissions through the associated Microsoft 365 group. This allows for much easier administration. For information about managing permissions in the SharePoint modern experience, see Sharing and permissions in the SharePoint modern experience.

If you do need to create custom permission levels, this article describes how.

How to create and edit permission levels

Permissions allow SharePoint users to perform certain actions, such as edit items in a list or create a site. But you can't assign individual permissions to individual users in SharePoint. Instead, you group related permissions together into a permission level. Then you assign that permission level to a SharePoint group that includes the people you are assigning permissions for.

SharePoint comes with some default permission levels that you can use, such as **Contribute** and **View Only**. But if one of those doesn't meet your needs, you can create a new permissions level. It's easier to keep track of permission levels if you don't change the defaults.

Create a permission level

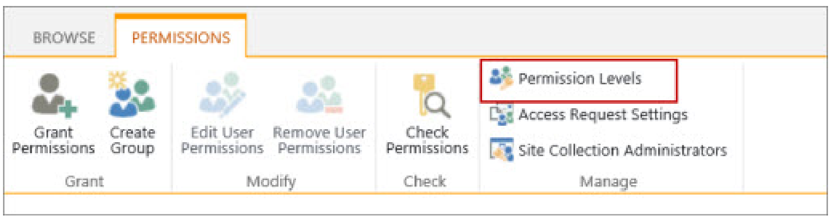
You create and make changes to permission levels on the **Permissions Levels** page.

To create or make changes to permission levels, you must belong to a SharePoint group that includes the permission to Manage Permissions. By default, you have this permission if you belong to the Owners group or if you are a Site Collection Administrator.

1. On the top-level site of the site collection, select **Settings** .

- For a classic site, select **Site settings**. On the **Site Settings** page, in the **Users and Permissions** section, select **Site permissions**.
- For a modern site, select **Site permissions**, and then **Advanced permissions settings**.

2. On the **Permissions** tab, in the Manage group, choose **Permission Levels**.



3. On the **Permission Levels** page, choose **Add a Permission Level**.

4. On the **Add a Permission Level** page provide the name and the description.

5. In the **Permissions area**, select the check boxes next to the list, site, and personal permissions that you want this permission level to include.

6. Click **Create**.

You can make changes to any of the listed permissions levels, except **Full Control** and **Limited Access**.

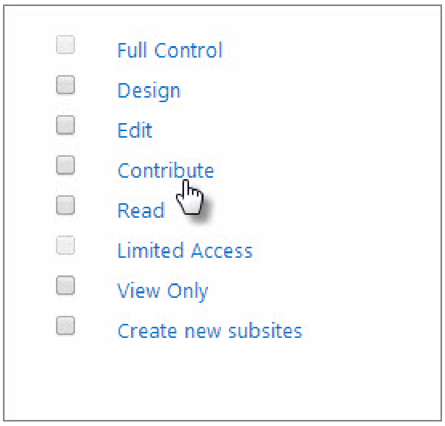
After you create the permission level, assign it to a SharePoint group.

Create a permission level by copying an existing permission level

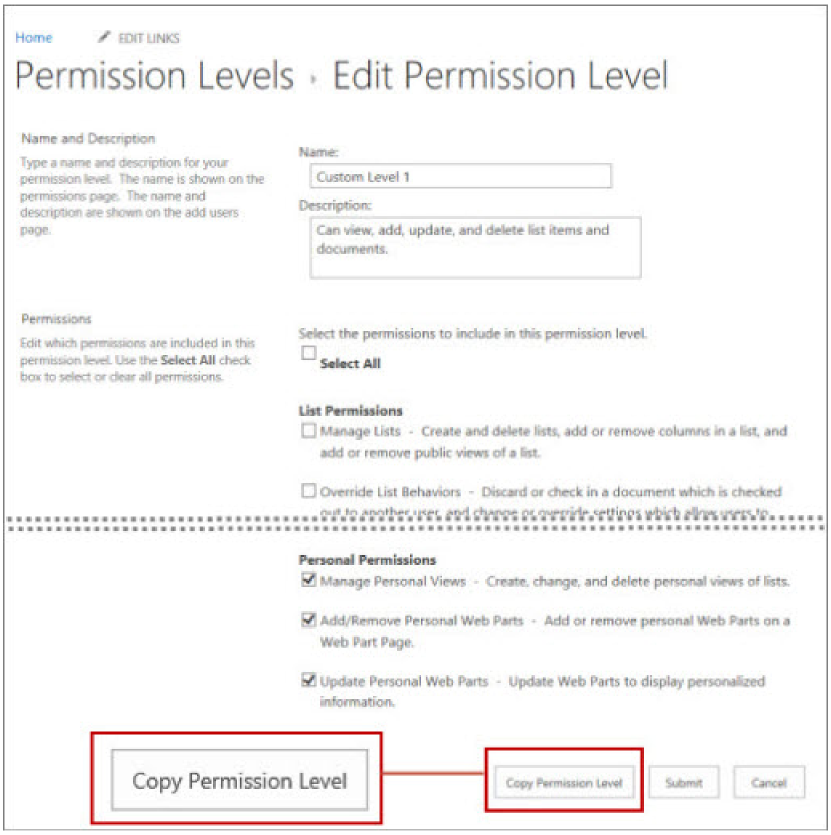
A quick way to create a new permission level is to make a copy of an existing permission level. You might want to do this when the existing permission level has permissions similar to what the new permission level will have. After you make the copy, you can add or remove the permissions you need the new permission level to have.

To copy a permission level:

1. On the **Permission Levels** page, click the name of the permission level that you want to copy. Be sure to click the link; do not select the checkbox next to the name. For example, **Contribute**, as shown in the following figure.



2. On the **Edit Permission Level** page, choose **Copy Permission Level**, which is at the bottom of the page after the **Personal Permissions** section.



3. On the **Copy Permission Level** page, type a name and description for the new permission level.

4. Choose which permissions you want to add or remove, and then choose **Create**

After you create the permission level, assign it to a SharePoint group.

Make changes to a permission level

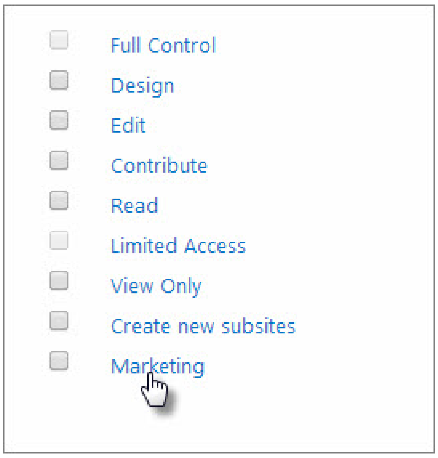
You can make the following changes to a permission level:

- Update the name or description
- Add or remove permissions

We recommend that you don't make any changes to the default permission levels that come with SharePoint. You can't make changes to the **Full Control** and **Limited Access** default permission levels.

To make changes to a permission level:

1. On the **Permission Levels** page, click the name of the permission level you want to edit. Be sure to click the link; do not select the checkbox next to the name. For example, **Marketing**, as shown in the following figure.



2. On **Edit Permission Level** page you can:

- Change the description.
- Add or remove permissions to the level.

3. After you have made you changes, click **Submit**.

You can delete any permission level, except for **Full Control** and **Limited Access**. We don't recommend that you delete a default permission level.

To delete a permission level, on the **Permissions Levels** page, select the check box next to the permission level that you want to delete, and then chose **Delete Selected Permission Levels**.

Best practices for permission levels

Permission levels apply to a specific site collection. This means that any changes you make to a permission level will have an effect throughout the site collection. Therefore, here are some recommendations:

- **Don't edit default permission levels** If you change a default permission level, the changes affect all the built-in SharePoint groups within the site collection. It can also cause confusion if you have two site collections that have permission levels with the same name, but each contains a different set of permissions.
- **Don't delete default permission levels** If you delete a default permission level, it will be removed from all built-in SharePoint groups that contain it within the site collection. This can cause users assigned to those groups to lose critical permissions.

- **Assign permission levels to SharePoint groups** You can assign a permission level to a single SharePoint user, but it's easier to keep track of who has permissions to which sites if you assign permission levels to a SharePoint group, and add that individual to the group. This can also help site performance.

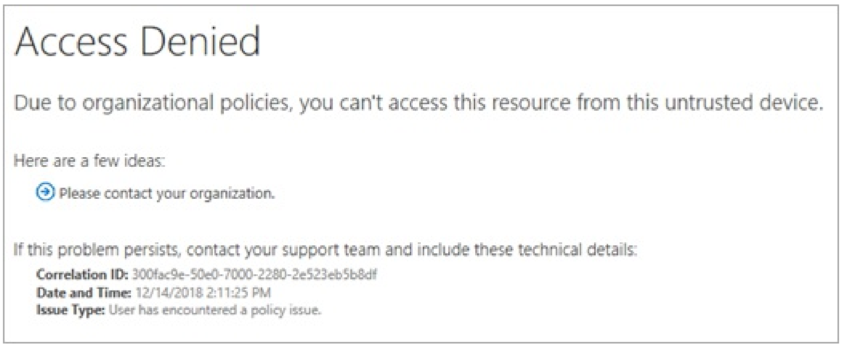
Control access from unmanaged devices

11/2/2020 • 9 minutes to read • Edit Online

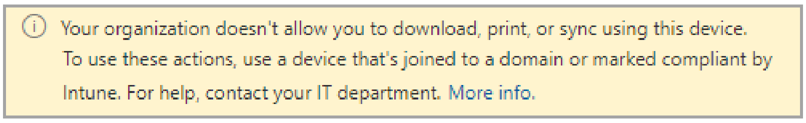
As a SharePoint or global admin in Microsoft 365, you can block or limit access to SharePoint and OneDrive content from unmanaged devices (those not hybrid AD joined or compliant in Intune). You can block or limit access for:

- All users in the organization or only some users or security groups.
- All sites in the organization or only some sites.

Blocking access helps provide security but comes at the cost of usability and productivity. When access is blocked, users will see the following error.



Limiting access allows users to remain productive while addressing the risk of accidental data loss on unmanaged devices. When you limit access, users on managed devices will have full access (unless they use one of the browser and operating system combinations listed below). Users on unmanaged devices will have browser-only access with no ability to download, print, or sync files. They also won't be able to access content through apps, including the Microsoft Office desktop apps. When you limit access, you can choose to allow or block editing files in the browser. When web access is limited, users will see the following message at the top of sites.



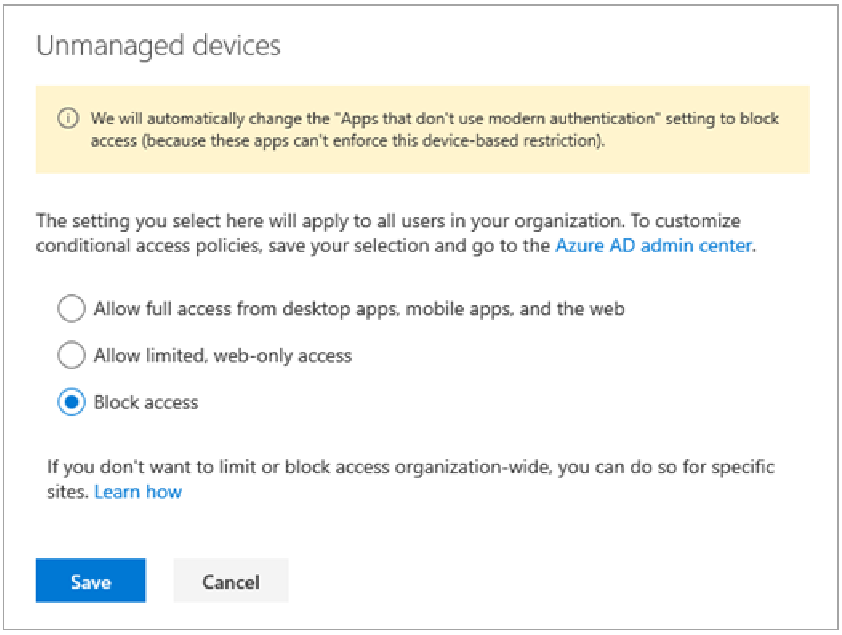
> **NOTE**
>
> Blocking or limiting access on unmanaged devices relies on Azure AD conditional access policies. Learn about Azure AD licensing For an overview of conditional access in Azure AD, see Conditional access in Azure Active Directory. For info about recommended SharePoint access policies, see Policy recommendations for securing SharePoint sites and files. If you limit access on unmanaged devices, users on managed devices must use one of the supported OS and browser combinations, or they will also have limited access.

Block access

1. Go to the Access control page of the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Access control page.
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Access control page.

2. Select **Unmanaged devices**.



3. Select **Block access**, and then select **Save**. (Selecting this option disables any previous conditional access policies you created from this page, and creates a new conditional access policy that applies to all users. Any customizations you made to previous policies will not be carried over.)

> **NOTE**
>
> It can take 5-10 minutes for the policy to take effect. It won't take effect for users who are already signed in from unmanaged devices.

> **IMPORTANT**
>
> If you block or limit access from unmanaged devices, we recommend also blocking access from apps that don't use modern authentication. Some third-party apps and versions of Office prior to Office 2013 don't use modern authentication and can't enforce device-based restrictions. This means they allow users to bypass conditional access policies that you configure in Azure. In the new SharePoint admin center, on the Access control page, select **Apps that don't use modern authentication**, select **Block access**, and then select **Save**.

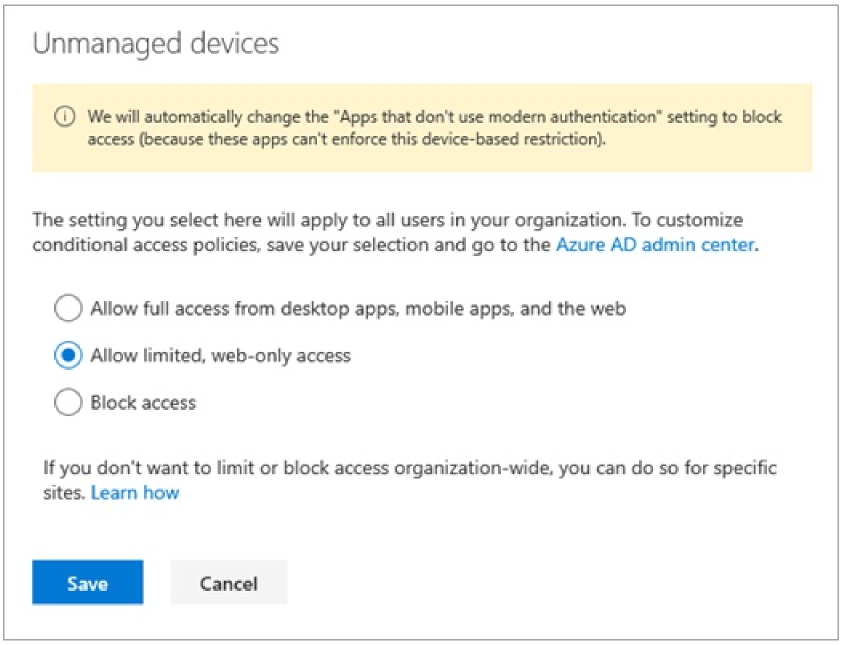
Limit access

1. Go to the Access control page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Active sites page.

2. Select **Unmanaged devices**.

3. Select **Allow limited, web-only access**, and then select **Save**. (Note that selecting this option will disable any previous conditional access policies you created from this page and create a new conditional access policy that applies to all users. Any customizations you made to previous policies will not be carried over.)



> **IMPORTANT**
>
> If you block or limit access from unmanaged devices, we recommend also blocking access from apps that don't use modern authentication. Some third-party apps and versions of Office prior to Office 2013 don't use modern authentication and can't enforce device-based restrictions. This means they allow users to bypass conditional access policies that you configure in Azure. In the new SharePoint admin center, on the Access control page, select **Apps that don't use modern authentication**, select **Block access**, and then select **Save**.

> **NOTE**
>
> If you limit access and edit a site from an unmanaged device, image web parts won't display images that you upload to the site assets library or directly to the web part. To work around this issue, you can use this SPList API to exempt the block download policy on the site assets library. This allows the web part to download images from the site assets library.

> **NOTE**
>
> When Access Control for Unmanaged Devices in SharePoint is set to **Allow limited, web-only access**, SharePoint files cannot be downloaded but they can be previewed. The previews of Office files work in SharePoint but the previews do not work in Microsoft Yammer.

Limit access using PowerShell

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs, and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language, and then select **Download**. You'll be asked to choose between downloading a x64 and x86 .msi file. If you're running the 64-bit version of Windows, download the x64 file; or, if you're running the 32-bit version, download the x86 file. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it, and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

```
Set-SPOTenant -ConditionalAccessPolicy AllowLimitedAccess`
```

> **NOTE**
>
> By default, this policy allows users to view and edit files in their web browser. To change this, see Advanced configurations.

Block or limit access to a specific SharePoint site or OneDrive

To block or limit access to specific sites, follow these steps. If you have configured the organization-wide policy, the site-level setting you specify must be at least as restrictive as the organization-level setting.

1. Manually create a policy in the Azure AD admin center by following the steps in Use app-enforced restrictions.

2. Set the site-level setting by using PowerShell, or a sensitivity label:

   - To use PowerShell, continue to the next step.

   - To use a sensitivity label, see the following instructions and specify the label setting for **Access from unmanaged devices**: Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites.

3. To use PowerShell: Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language, and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. If you're running the 64-bit version of Windows, download the x64 file; or, if you're running the 32-bit version, download the x86 file. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it, and follow the steps in the Setup Wizard.

4. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting

started with SharePoint Online Management Shell.

5. Run one of the following commands.

   To block access to a single site:

```
Set-SPOSite -Identity https://<SharePoint online URL>/sites/<name of site or OneDrive account> -
ConditionalAccessPolicy BlockAccess
```

   To limit access to a single site:

```
Set-SPOSite -Identity https://<SharePoint online URL>/sites/<name of site or OneDrive account> -
ConditionalAccessPolicy AllowLimitedAccess
```

   To update multiple sites at once, use the following command as an example:

```
,(Get-SPOSite -IncludePersonalSite $true -Limit all -Filter "Url -like '-
my.sharepoint.com/personal/'") | Set-SPOTenant -ConditionalAccessPolicy AllowLimitedAccess
```

   This example gets the OneDrive for every user and passes it as an array to Set-SPOTenant to limit access. The initial comma and the parentheses are required for running this cmdlet as a batch request, which is fastest.

NOTE

By default, a setting that includes web access allows users to view and edit files in their web browser. To change this, see Advanced configurations.

Advanced configurations

The following parameters can be used with `-ConditionalAccessPolicy AllowLimitedAccess` for both the organization-wide setting and the site-level setting:

`-AllowEditing $false` Prevents users from editing Office files in the browser and copying and pasting Office file contents out of the browser window.

`-LimitedAccessFileType OfficeOnlineFilesOnly` Allows users to preview only Office files in the browser. This option increases security but may be a barrier to user productivity.

`-LimitedAccessFileType WebPreviewableFiles` (default) Allows users to preview Office files in the browser. This option optimizes for user productivity but offers less security for files that aren't Office files. **Warning:** This option is known to cause problems with PDF and image file types because they can be required to be downloaded to the end user's machine to render in the browser. Plan the use of this control carefully. Otherwise, your users could be faced with unexpected "Access Denied" errors.

`-LimitedAccessFileType OtherFiles` Allows users to download files that can't be previewed, such as .zip and .exe. This option offers less security.

The AllowDownlownloadingNonWebViewableFiles parameter has been discontinued. Please use LimitedAccessFileType instead.

External users will be affected when you use conditional access policies to block or limit access from unmanaged devices. If users have shared items with specific people (who must enter a verification code sent to their email address), you can exempt them from this policy by running the following cmdlet.

```
Set-SPOTenant -ApplyAppEnforcedRestrictionsToAdHocRecipients $false
```

> **NOTE**
>
> "Anyone" links (shareable links that don't require sign-in) are not affected by these policies. People who have an "Anyone" link to a file or folder will be able to download the item. For all sites where you enable conditional access policies, you should disable "Anyone" links.

App impact

Blocking access and blocking download may impact the user experience in some apps, including some Office apps. We recommend that you turn on the policy for some users and test the experience with the apps used in your organization. In Office, make sure to check the behavior in Power Apps and Power Automate when your policy is on.

> **NOTE**
>
> Apps that run in "app-only" mode in the service, like antivirus apps and search crawlers, are exempted from the policy.
>
> If you're using classic SharePoint site templates, site images may not render correctly. This is because the policy prevents the original image files from being downloaded to the browser.
>
> For new tenants, apps using an ACS app-only access token is disabled by default. We recommend using the Azure AD app-only model which is modern and more secure. But you can change the behavior by running 'set-spotenant -DisableCustomAppAuthentication $false' (needs the latest SharePoint admin PowerShell).

Need more help?

If you have technical questions about this topic, you may find it helpful to post them on the SharePoint discussion forum. It's a great resource for finding others who have worked with similar issues or who have encountered the same situation.

See also

Policy recommendations for securing SharePoint sites and files

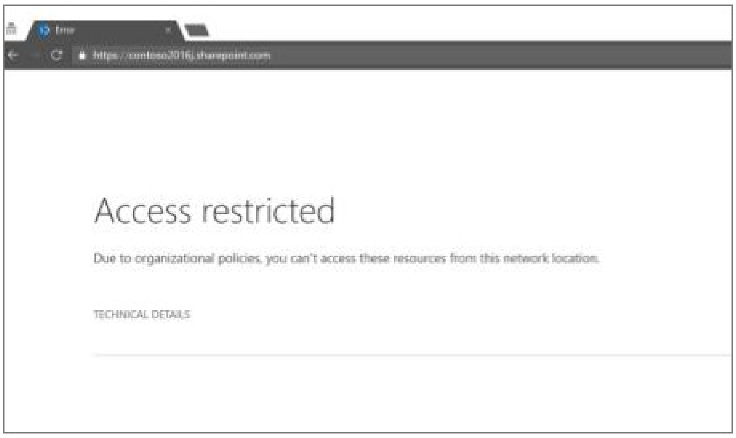
Control access to SharePoint and OneDrive data based on defined network locations

Control access to SharePoint and OneDrive data based on network location

1/8/2021 • 2 minutes to read • Edit Online

As an IT admin, you can control access to SharePoint and OneDrive resources in Microsoft 365 based on defined network locations that you trust. This is also known as location-based policy.

To do this, you define a trusted network boundary by specifying one or more authorized IP address ranges. Any user who attempts to access SharePoint and OneDrive from outside this network boundary (using web browser, desktop app, or mobile app on any device) will be blocked.



Here are some important considerations for setting a location-based policy:

- **External sharing**: If files and folders have been shared with guests who authenticate, they will not be able to access the resources outside of the defined IP address range.
- **Access from first and third-party apps**: Normally, a SharePoint document can be accessed from apps like Exchange, Yammer, Skype, Teams, Planner, Power Automate, PowerBI, Power Apps, OneNote, and so on. When a location-based policy is enabled, apps that do not support location-based policies are blocked. The only apps that currently support location-based policies are Teams, Yammer, and Exchange. This means that all other apps are blocked, even when these apps are hosted within the trusted network boundary. This is because SharePoint cannot determine whether a user of these apps is within the trusted boundary.

> **NOTE**
> We recommend that when a location-based policy is enabled for SharePoint, the same policy and IP address ranges should be configured for Exchange and Yammer. SharePoint relies on these services to enforce that the users of these apps are within the trusted IP range.

- **Access from dynamic IP ranges**: Several services and providers host apps which have dynamic originating IP addresses. For example, a service that accesses SharePoint while running from one Azure data center may start running from a different data center due to a failover condition or other reason, thus dynamically changing its IP address. The location-based conditional access policy relies on fixed, trusted IP address ranges. If the IP address range cannot be determined up front, location-based policy may not be an option for your environment.

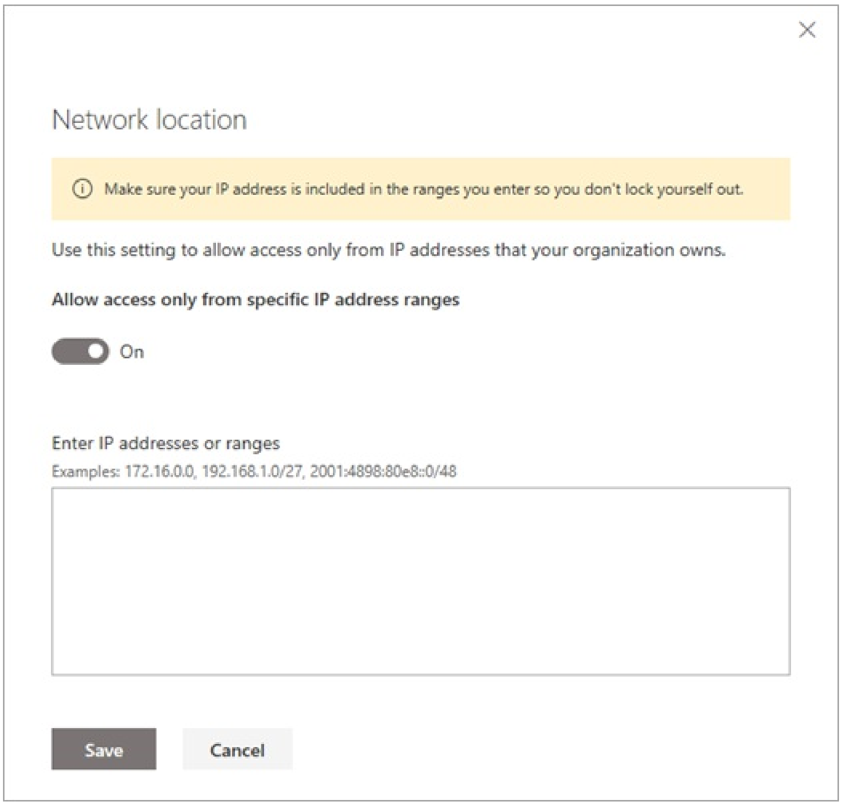
Set a location-based policy in the new SharePoint admin center

> **NOTE**
>
> It can take up to 15 minutes for these settings to take effect.

1. Go to the Access control page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Access control page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Access control page.

2. Select **Network location**, and turn on **Allow access only from specific IP address ranges**.



3. Enter IP addresses and address ranges separated by commas.

> **IMPORTANT**
>
> Make sure you include your own IP address so you don't lock yourself out. This setting not only restricts access to OneDrive and SharePoint sites, but also to the OneDrive and SharePoint admin centers, and to running PowerShell cmdlets. If you lock yourself out and can't connect from an IP address within a range you specified, you will need to contact Support for help.
> If you save overlapping IP addresses, your users will see a generic error message with a correlation ID that points to "The input IP allow list has overlaps."

NOTE

To set a location-based policy by using PowerShell, run Set-SPOTenant with the -IPAddressAllowList parameter. For more info, see Set-SPOTenant.

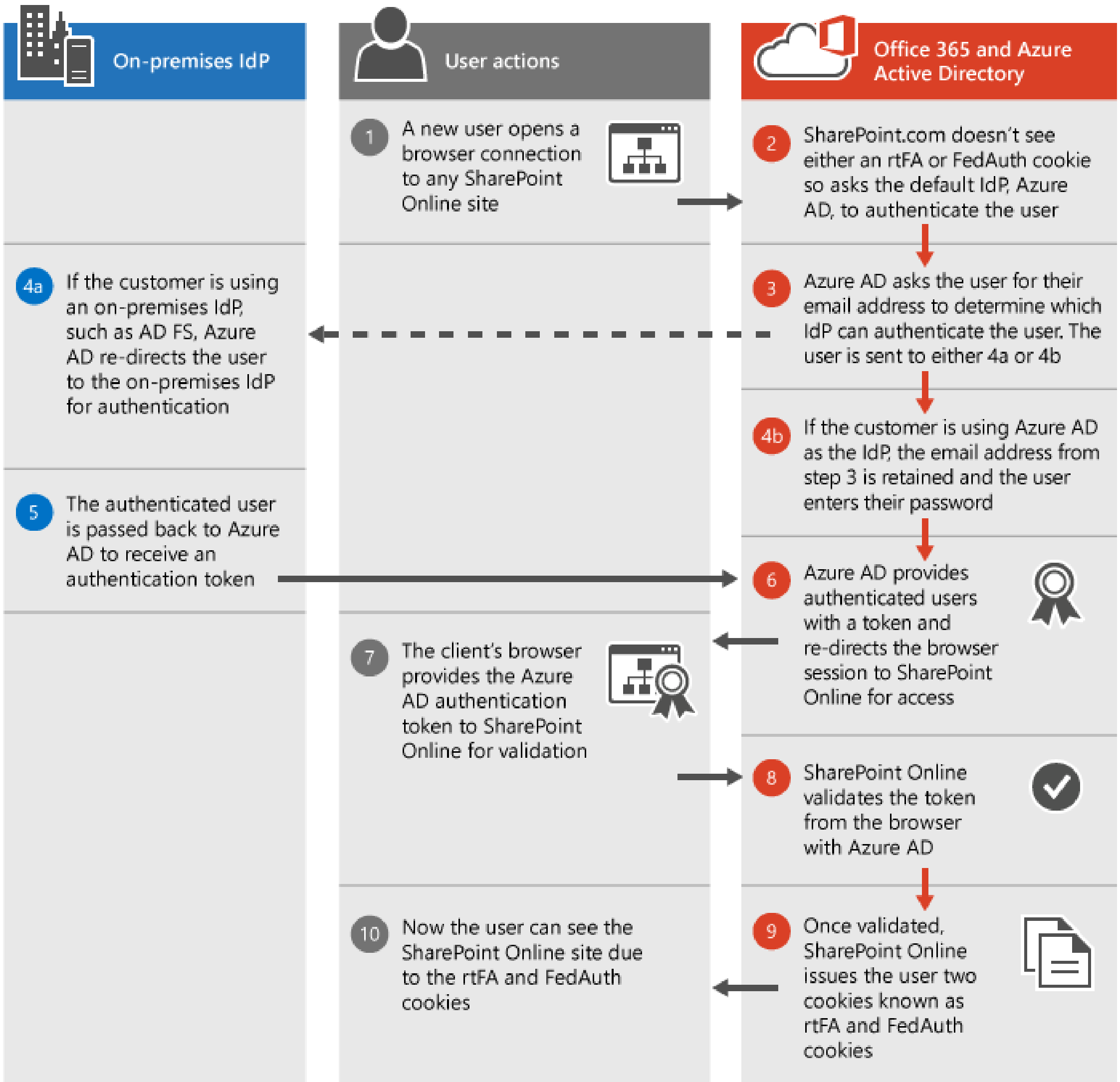
SharePoint authentication

6/26/2020 • 2 minutes to read • Edit Online

SharePoint in Microsoft 365 serves a wide range of customers with a variety of usability and security needs. Some customers don't mind asking users to reauthenticate if it means their data will be more secure. Other customers want to minimize the number of sign-in screens that users see, especially in situations where it seems as though SharePoint should already know who the user is. Luckily, customers don't have to choose usability or security because they work together in a lot of great ways.

The following diagram outlines the SharePoint authentication process. It walks through how the scenario works using either your own Identity Provider (IdP) or the default Azure Active Directory (Azure AD) IdP.

The Federation Authentication (FedAuth) cookie is for each top-level site in SharePoint such as the root site, OneDrive, and the admin center site. The root Federation Authentication (rtFA) cookie is used across all of SharePoint. When a user visits a new top-level site or another company's page, the rtFA cookie is used to authenticate them silently without a prompt. When a user signs out of SharePoint, the rtFA cookie is deleted.



Session and persistent cookies

By default, all SharePoint cookies are **session** cookies. These cookies are not saved to the browser's cookie cache and instead are deleted whenever the browser is closed. Azure AD provides a **Keep Me Signed In** button during login that passes a signal to Microsoft 365 to enable **persistent** cookies. These cookies are saved to the browser's cache and will persist even if the browser is closed or the computer is restarted.

Persistent cookies have a huge impact on the sign-in experience by reducing the number of authentication prompts users see. Persistent cookies are also required for some SharePoint features, such as **Open with Explorer** and **Mapped Drives**.

For more info about session timeouts, see Session timeouts for Microsoft 365.

How SharePoint and OneDrive safeguard your data in the cloud

6/5/2020 • 7 minutes to read • Edit Online

You control your data. When you put your data in SharePoint and OneDrive for Microsoft 365, you remain the owner of the data. For more info about the ownership of your data, see Microsoft 365 Privacy by Design.

How we treat your data

Microsoft engineers administer SharePoint and OneDrive using a PowerShell console that requires two-factor authentication. We perform day-to-day tasks by running workflows so we can rapidly respond to new situations. Check-ins to the service require code review and management approval.

No engineer has standing access to the service. When engineers need access, they must request it. Eligibility is checked, and if engineer access is approved, it's only for a limited time. In rare cases where Microsoft engineers need access to content (for example, if you submit a support ticket because a user can't access an important file that we believe is damaged), the engineers must check in a specific workflow that requires business justification and manager approval. An audit event is generated that you can view in the Microsoft 365 admin center. You can also turn on a feature called Customer Lockbox, so you need to approve the request. The engineer gets access only to the file in question. To learn how to turn on or off Customer Lockbox and approve and deny requests, see Microsoft 365 Customer Lockbox Requests.

How you can safeguard your data

One of the most important things you can do to safeguard your data is to require two-factor authentication for your identities in Microsoft 365. This prevents credentials from being used without a second factor and mitigates the impact of compromised passwords. The second factor can be made through a phone call, text message, or app. When you roll out two-factor authentication, start with your global admins, and then other admins and site collection admins. For info about how to do this, see Set up multi-factor authentication for Microsoft 365 users.

Other things we recommend to increase security:

- Use Azure Active Directory device-based conditional access to block or limit access on unmanaged devices like airport or hotel kiosks. See Control access from unmanaged devices.
- Create policies to sign users out of Microsoft 365 web sessions after a period of inactivity. For information, see Sign out inactive users.
- Evaluate the need for IP-based sessions. These simulate the access model of an on-premises deployment. Read more at Control access based on network location or app.
- Empower workers to share broadly but safely. You can require sign-in or use links that expire or grant limited privileges. See Manage external sharing for your SharePoint environment.
- Prevent accidental exposure of sensitive content. Create DLP policies to identify documents and prevent them from being shared. See Overview of data loss prevention policies.

Protected in transit and at rest

Protected in transit

When data transits into the service from clients, and between datacenters, it's protected using best-in-class encryption. For info, see Data Encryption in OneDrive and SharePoint. We only permit secure access. We won't make authenticated connections over HTTP but, instead, redirect to HTTPS.

Protected at rest

Physical protection: Only a limited number of essential personnel can gain access to datacenters. Their identities are verified with multiple factors of authentication, including smart cards and biometrics. There are on-premises security officers, motion sensors, and video surveillance. Intrusion detection alerts monitor anomalous activity.

Network protection: The networks and identities are isolated from the Microsoft corporate network. We administer the service with dedicated Active Directory domains, we have separate domains for test and production, and the production domain is divided into multiple isolated domains for reliability and security. For more information about the built-in physical and logical security from Microsoft 365, see Built-in security from Microsoft 365.

Application security: Engineers who build features follow the security development lifecycle. Automated and manual analyses help identify possible vulnerabilities. The Microsoft security response center (Microsoft Security Response Center) helps triage incoming vulnerability reports and evaluate mitigations. Through the Microsoft Cloud Bug Bounty, people across the world can earn money by reporting vulnerabilities. Read more about this at Microsoft Cloud Bug Bounty Terms.

Content protection: Your data is encrypted at the disk level using BitLocker encryption and at the file level using keys. For info, see Data Encryption in OneDrive and SharePoint. For information about using Customer Key to provide and control the keys that are used to encrypt your data at rest in Microsoft 365, see Service encryption with Customer Key for Microsoft 365 FAQ.

The Microsoft 365 anti-malware engine scans documents at upload time for content matching an AV signature (updated hourly). For info, see Virus detection in SharePoint. For more advanced protection, use Microsoft 365 Advanced Threat Protection (ATP). ATP analyzes content that's shared and applies threat intelligence and analysis to identify sophisticated threats. For info, see Microsoft 365 Advanced Threat Protection.

To limit the risk of content being downloaded to untrusted devices:

- Limit sync to devices on the domains you specify: Allow syncing only on computers joined to specific domains.
- Use Intune to limit access to content in the OneDrive and SharePoint mobile apps: Control access to features in the OneDrive and SharePoint mobile apps.

To manage content at rest:

- Configure IRM policies on SharePoint document libraries to limit download of content. See Set up Information Rights Management (IRM) in SharePoint admin center.
- Evaluate the use of Azure Information Protection (AIP). Classification and labeling let you track and control how data is used. Visit Azure Information Protection.

Highly available, always recoverable

Our datacenters are geo-distributed within the region and fault tolerant. Data is mirrored in at least two datacenters to mitigate the impact of a natural disaster or service-impacting outage. For more information, see Where's my data?.

Metadata backups are kept for 14 days and can be restored to any point in time within a five-minute window.

In the case of a ransomware attack, you can use Version history (Enable and configure versioning for a list or library) to roll back, and the recycle bin or site collection recycle bin to restore (Restore deleted items from the site collection recycle bin). If an item is removed from the site collection recycle bin, you can call support within 14 days to access a backup. For information about the new Files Restore feature that lets users restore an entire OneDrive to any point within the past 30 days, see Restore your OneDrive.

Continuously validated

We continuously monitor our datacenters to keep them healthy and secure. This starts with inventory. An inventory agent scans each subnet looking for neighbors. For each machine, we perform a state capture.

After we have an inventory, we can monitor and remediate the health of machines. The security patch train applies patches, updates anti-virus signatures, and makes sure we have a known good configuration saved. We have role-specific logic that ensures we only patch or rotate out a certain percentage of machines at a time.

We have an automated workflow to identify machines that don't meet policies and queue them for replacement.

The Microsoft 365 "Red Team" within Microsoft is made up of intrusion specialists. They look for any opportunity to gain unauthorized access. The "Blue Team" is made up of defense engineers who focus on prevention, detection, and recovery. They build intrusion detection and response technologies. To keep up with the learnings of the security teams at Microsoft, see Security, Privacy, and Compliance Blog.

To monitor and observe activity in your Microsoft 365 subscription:

- If you have an on-premises security operations center or SIEM, you can monitor activity with the Management Activity API. For information, see Microsoft 365 Management APIs overview. This will show you activity from across SharePoint, Exchange, Azure Active Directory, DLP, and more. If you don't have an on-premises security operations center or SIEM, you can use Cloud App Security. Cloud App Security uses the Management Activity API. For info, see Overview of Microsoft 365 Cloud App Security. Through Cloud App Security, you can report, search, and alert on activity.
- Use Azure Active Directory identity protection. This applies machine learning to detect suspicious account behavior, for example, simultaneous sign-ins from the same user in different parts of the world. You can configure identity protection to take action to block these sign-ins. For more info, see Azure Active Directory Identity Protection.
- Use Secure Score to evaluate the security profile of your subscription against a known good baseline, and identify opportunities to increase protection. For more info, see Microsoft Secure Score.

Audited and compliant

Regulatory compliance is fundamental to Microsoft 365. We make sure the service complies with regulatory and compliance standards. We also help you meet your audit and compliance obligations. The Service Trust Portal is a one-stop-shop for compliance and trust information for Microsoft enterprise services. The portal contains reports, whitepapers, vulnerability assessments, and compliance guides. The portal also includes the Compliance Manager, which evaluates the configuration of your subscription against a set of compliance criteria. For more info about the Service Trust Portal, see Get started with the Microsoft Service Trust Portal.

To meet your regulatory requirements:

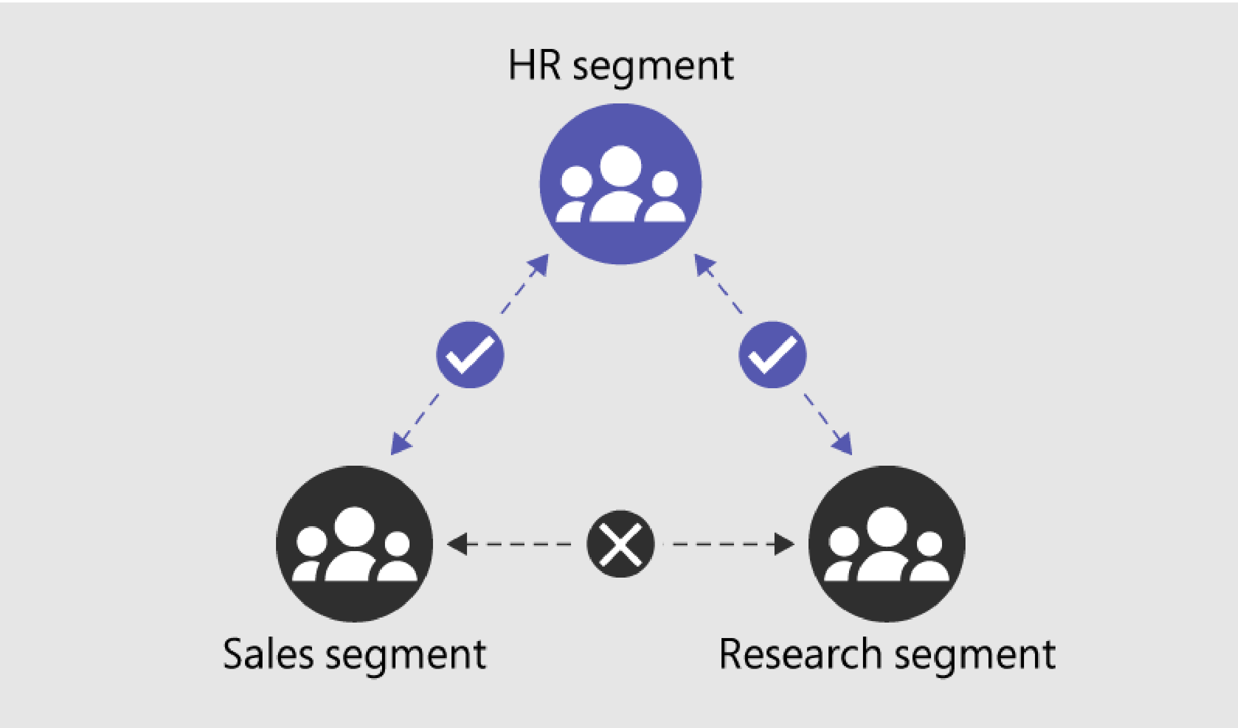
- Audit Microsoft 365 activity in the Security & Compliance Center: Search the audit log in the Microsoft 365 Security & Compliance Center.
- Create eDiscovery cases: Manage eDiscovery cases in the Microsoft 365 Security & Compliance Center
- Apply retention policies: Create and apply information management policies.

Use information barriers with SharePoint

1/8/2021 • 5 minutes to read • Edit Online

Information barriers are policies in Microsoft 365 that a compliance admin can configure to prevent users from communicating and collaborating with each other. This is useful if, for example, one division is handling information that shouldn't be shared with specific other divisions, or a division needs to be prevented, or isolated, from collaborating with all users outside of the division. Information barriers are often used in highly regulated industries and those with compliance requirements, such as finance, legal, and government. Learn more about information barriers.

The following image illustrates three segments in an organization: HR, Sales, and Research. An information barrier policy has been defined that blocks communication and collaboration between the Sales and Research segments. These segments are incompatible.



With SharePoint information barriers, a SharePoint or global admin can associate segments to a site to prevent the site from being shared with or accessed by users outside the segments. Up to 100 compatible segments can be associated with a site. The segments are associated at the site level (previously called site collection level). The Microsoft 365 group connected to the site is also associated with the site's segment.

In the above example, the HR segment is compatible with both Sales and Research. However, because the Sales and Research segments are incompatible, they can't be associated with the same site.

Prerequisites

- Make sure you meet the licensing requirements for information barriers.
- Create segments and define the users in each. Create policies that allow or block communication between the segments, and then set them to active. For info, see Define policies for information barriers.
- Complete the form to enable SharePoint and OneDrive information barriers in your organization. Please note that SharePoint and OneDrive information barriers can only be enabled in your tenant if you already have at least one active information barriers policy.
- After SharePoint and OneDrive information barriers are enabled in your tenant, wait 24 hours for the

changes to propagate through your environment.

Use PowerShell to associate segments with a site

1. Connect to the Security & Compliance Center PowerShell as a global admin.

2. Run the following command to get the list of segments and their GUIDs.

```
Get-OrganizationSegment | ft Name, EXOSegmentID
```

3. Save the list of segments.

NAME	EXOSEGMENTID
Sales	a9592060-c856-4301-b60f-bf9a04990d4d
Research	27d20a85-1c1b-4af2-bf45-a41093b5d111
HR	a17efb47-e3c9-4d85-a188-1cd59c83de32

4. Download the latest SharePoint Online Management Shell.

> **NOTE**
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see https://support.microsoft.com/help/13443/windows-which-operating-system. After the file downloads, run it and follow the steps in the Setup Wizard.

5. Connect to SharePoint Online as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

6. Run the following command:

```
Set-Sposite -Identity <site URL> -AddInformationSegment &lt;segment GUID&gt;
```

Example: Set-SPOSite -Identity https://contoso.sharepoint.com/sites/ResearchTeamSite -AddInformationSegment 27d20a85-1c1b-4af2-bf45-a41093b5d111

An error will appear if you attempt to associate a segment that isn't compatible with the site's existing segments.

To remove segment from a site, run the following command.

```
Set-Sposite -Identity <site URL> -RemoveInformationSegment &lt;segment GUID&gt;
```

Example: Set-SPOSite -Identity https://contoso.sharepoint.com/sites/ResearchTeamSite -RemoveInformationSegment 27d20a85-1c1b-4af2-bf45-a41093b5d111

Segments associated with Microsoft Teams sites

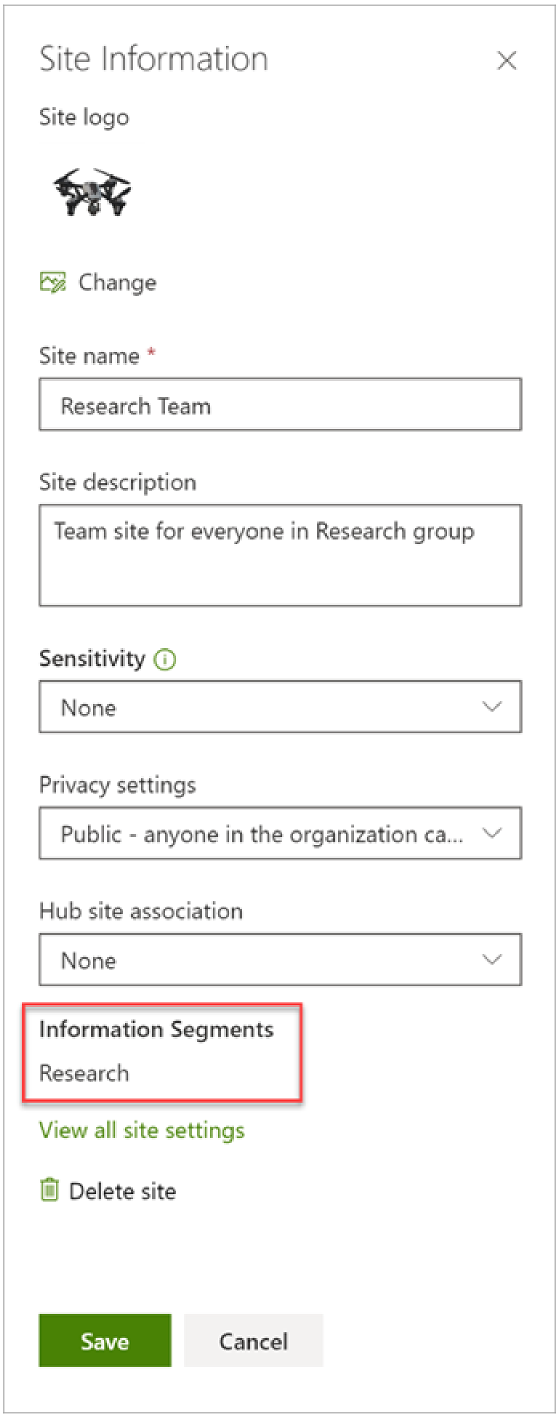
When a team is created in Microsoft Teams, a SharePoint site is automatically created for the team's files. Within 24 hours, the segments associated with the team's members are automatically associated with the site. SharePoint admins can't change the segments associated with a site when the site is connected to a team. Learn more about information barriers in Teams

View the segments associated with a site

Run the following command in the SharePoint Online Management Shell to return the GUIDs of any segments associated with a site.

```
Get-SPOSite -Identity <site URL> | Select InformationSegment
```

Site owners can view the segments associated with a site by selecting **Settings** > **Site information**.



Sharing sites that have segments associated

When a segment is associated with a site:

- The option to share with "Anyone with the link" is disabled.
- The site and its content can be shared only with users whose segment matches that of the site. For example, if a site is associated with only HR, the site can be shared with other HR users only (even though HR is compatible with both Sales and Research).
- New users can be added to the site as site members only if their segment matches that of the site.

When a site has no segments associated:

- The site and its contents can be shared based on the information barrier policy applied to the user. For example, if a user in HR is allowed to communicate with users in Research, the user will be able to share the site with those users.

Access to sites that have segments associated

For a user to access a SharePoint site that segments associated:

- The user's segment must match a segment that is associated with the site.

  AND

- The user must have access permission to the site.

Non-segment users can't access a site that is associated with segments. They will see an error.

Search

Users will see search results from:

- Sites that have an associated segment that matches the user's segment and the user has access permission to the site.
- Sites that don't have associated segments if they have access to the site.

Effects of changes to user segments or information barrier policies

If a SharePoint site owner’s segment changes, the user won't be able to access the site if their segment doesn't match any of the segments associated with the site. To allow the user to access the site, a SharePoint admin must associate the user's new segment with the site.

If a compliance administrator changes an existing policy, the change may impact the compatibility of the segments associated with a site. For example, segments that were once compatible may no longer be compatible. A SharePoint admin must change the segments associated with an affected site accordingly.

Any sharing links will only work if a user's new segment or the new information barrier policy still allows the user to access the site.

See also

Information barriers in OneDrive

Sign out inactive users

1/8/2021 • 4 minutes to read • Edit Online

This article is for global and SharePoint admins in Microsoft 365 who want to control user access to SharePoint and OneDrive data on unmanaged devices. Idle session sign-out lets you specify a time at which users are warned and subsequently signed out of Microsoft 365 after a period of browser inactivity in SharePoint and OneDrive.

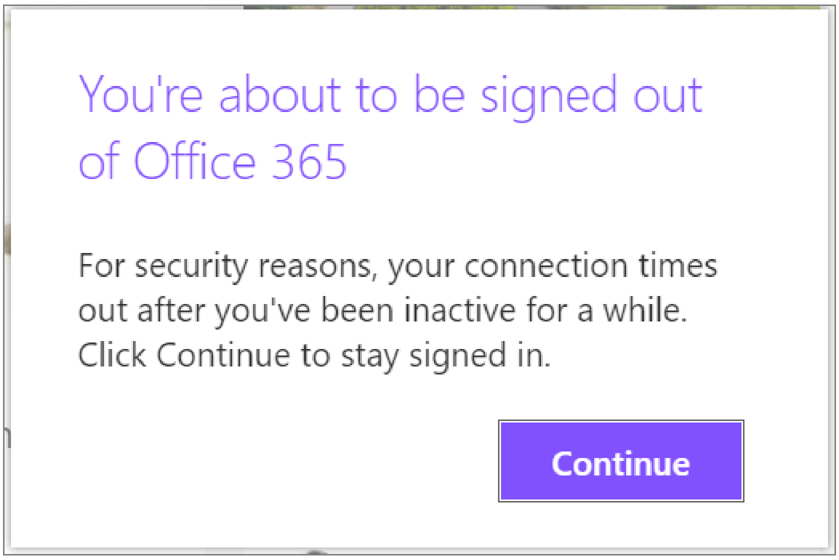
> **NOTE**
> Idle session sign-out applies to the entire organization and can't be set for specific sites or users. To target different settings for different users, use Azure AD Conditional Access policies instead (and see the next important note about the Azure AD Premium requirement).

> **IMPORTANT**
> This feature relies on Azure AD Conditional Access policies being available. You will need an Azure AD Premium P1 or P2 subscription for this to work. For more info about this, refer to the announcement in the Azure Active Directory Identity Blog.

Idle session sign-out is one of a number of policies you can use with SharePoint and OneDrive to balance security and user productivity and help keep your data safe regardless where users access the data, what device they're working on, and how secure their network connection is. For more ways to control access in SharePoint and OneDrive, see How SharePoint and OneDrive safeguard your data in the cloud.

The idle session sign-out experience

When a user is inactive in SharePoint and OneDrive for a period of time you specify, the following message appears:



NOTE

Activity is counted as requests sent to SharePoint, such as mouse clicks on a UI element like a button, list entry, or a link.Moving the mouse and scrolling are not counted as activity.

If users don't select **Continue**, they are automatically signed out, and the following message appears.

NOTE

If a user is active in another Microsoft 365 service (such as Outlook), but inactive in SharePoint and OneDrive, they are signed out across Microsoft 365. If a user has multiple tabs to OneDrive and SharePoint sites open at the same time, they won't be signed out unless they are inactive on all the sites. > Users won't be signed out if they selected to stay signed in when they signed in. For info about hiding this option, see Add company branding to your sign-in page in Azure AD. Users won't be signed out on a managed device (one that is compliant or joined to a domain), unless they're using inPrivate mode or a browser other than Edge or Internet Explorer. If they use Google Chrome, you need to use an extension to pass the device state claim. For more info about device state claims, see Azure AD conditional access settings.

IMPORTANT

Microsoft 365 apps and services will not support Internet Explorer 11 starting August 17, 2021 (Microsoft Teams will not support Internet Explorer 11 earlier, starting November 30, 2020). Learn more. Please note that Internet Explorer 11 will remain a supported browser. Internet Explorer 11 is a component of the Windows operating system and follows the Lifecycle Policy for the product on which it is installed.

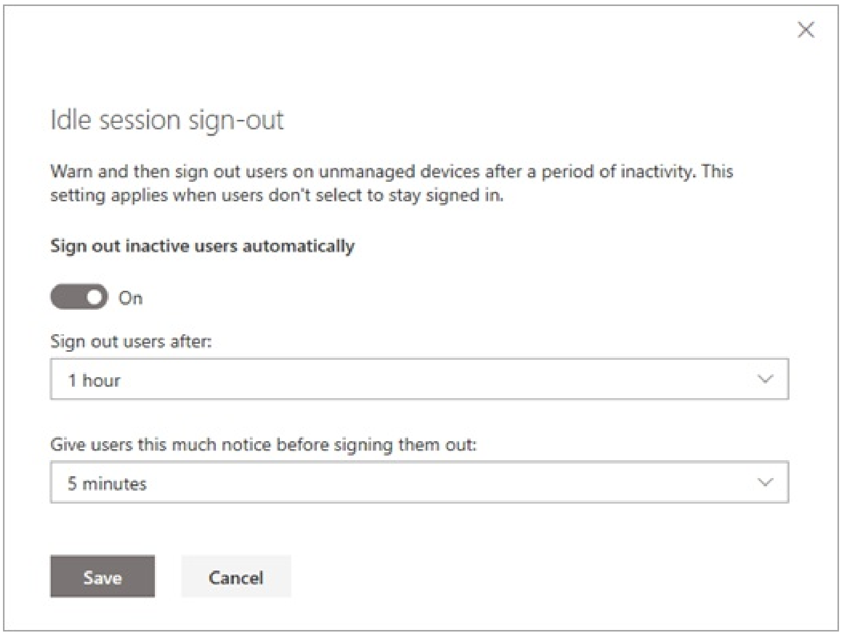
Specify idle session sign-out settings in the new SharePoint admin center

1. Go to the Access control page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

   NOTE

   If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Access control page.
   If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Access control page.

2. Select **Idle session sign-out**.



3. Turn on **Sign out inactive users automatically**, and then select when you want to sign out users and how much notice you want to give them before signing them out.

4. Select **Save**.

Specify idle session sign-out settings by using PowerShell

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running? After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

```
Set-SPOBrowserIdleSignOut -Enabled $true -WarnAfter (New-TimeSpan -Seconds 2700) -SignOutAfter (New-
TimeSpan -Seconds 3600)
```

Where:

- **-Enabled** specifies whether idle session sign-out is enabled or disabled by using **$true** or **$false**.

- **-WarnAfter** specifies the amount of after which a user is notified that they will be signed out after a period of inactivity as a **New-TimeSpan** which can be configured in seconds, minutes, or hours.

- **-SignOutAfter** specifies the amount of time after which is a user is signed out of Microsoft 365 if they do not respond to the **-WarnAfter** prompt.

NOTE

You must specify values for both **WarnAfter** and **SignOutAfter**. The **SignOutAfter** must be greater than the **WarnAfter** value.

It takes about 15 minutes for the policy to take effect across your organization. The policy doesn't affect existing sessions. To view the idle session sign-out values you've set, use **Get-SPOBrowserIdleSignOut**.

For info about Microsoft 365 session lengths (regardless of activity), see Session timeouts for Microsoft 365.

Introduction to managed metadata

6/5/2020 • 11 minutes to read • Edit Online

Metadata is information about information. For example, a book's title and author is metadata. Metadata can be many kinds of information -- a location, a date, or a catalog item number. When you use SharePoint products, you can manage the metadata centrally. You can organize the metadata in a way that makes sense in your business and use the metadata to make it easier to find what you want.

This article describes some important terminology of managed metadata, and gives you a quick look at how you can use the tools in SharePoint to manage metadata.

Important terminology

This section contains definitions of some key terminology. These terms and concepts appear frequently in articles about managed metadata.

Taxonomy

A taxonomy is a formal classification system. A taxonomy groups the words, labels, and terms that describe something, and then arranges the groups into a hierarchy.

People construct taxonomies for almost any kind of information, from biological systems to organizational structures. For example, biologists group living organisms into four major classifications: animal, plant, fungus, and microbe. Each of these major groups has many subdivisions. Together, the whole system is a taxonomy.

Organizations create taxonomies in too many ways to list. They create Chart of Accounts taxonomies to manage accounting systems, organization charts and job classifications to manage employees, product catalogs and so on. All these taxonomies are structured hierarchies of information; formal classification systems that help people handle information.

Folksonomy

A folksonomy is an informal classification system. It evolves gradually as web site users collaborate on words, labels, and terms on a site. Originally, folksonomies developed from popular applications such as bookmarking.

If you have ever seen a tag cloud on a website, then you have seen a visualization of a folksonomy. The following figure shows a tag cloud on a SharePoint site.

A folksonomy-based approach to metadata can be useful. It creates a way to share the knowledge and expertise of site users. By using a folksonomy, content classification can evolve together with changing business needs and user interests.

Term Set

A Term set is a group of related terms.

Terms sets can have different scope, depending on where you create the term set.

- **Local term sets** are created within the context of a site collection, and are available for use (and visible) only to users of that site collection. For example, when you create a term set for a metadata column in a list or library, then the term set is local. It is available only in the site collection that contains this list or library. For example, a media library might have a metadata column that shows the kind of media (diagram, photograph, screen shot, video, etc.). The list of permitted terms is relevant only to this library, and available for use in the library.

- **Global term sets** are available for use across all sites that subscribe to a specific Managed Metadata Service application. For example, an organization might create a term set that lists names of business units in the organization, such as Human Resources, Marketing, Information Technology, and so on.

In addition, you can configure a term set as closed or open. In a closed term set, users can't add new terms unless they have appropriate permissions. In an open term set, users can add new terms in a column that is mapped to the term set.

Terms

A term is a specific word or phrase that you associated with an item on a SharePoint site. It is a single item in a term set. A term has a unique ID and it can have many text labels (synonyms). If you work on a multilingual site, the term can have labels in different languages.

There are two types of terms:

- **Managed terms** Managed terms are terms that are pre-defined. Term Store administrators organize managed terms into a hierarchical term set.

- **Enterprise keywords** An enterprise keyword is a word or phrase that a user adds to items on a SharePoint site. The collection of enterprise keywords is known as the Keywords set. Typically, users can add any word or phrase to an item as a keyword. This means that you can use enterprise keywords for folksonomy-style tagging. Sometimes, Term Store administrators move enterprise keywords into a specific managed term set. When they are part of a managed term set, keywords become available in the context of that term set.

To learn more about how to create and manage terms, see Create and manage terms in a term set.

Group

In SharePoint products, group is a security term. With respect to managed metadata, a group is a set of term sets that all share common security requirements. Only users who have contributor permissions for a specific group can manage term sets that belong to the group or create new term sets within it. Organizations should create groups for term sets that will have unique access or security needs.

To learn more about how to create a group for term sets, see Set up a new group for term sets.

Term Store management tool

The Term Store management tool is the tool that people who manage taxonomies use to create or manage term sets and the terms within them. The Term Store management tool displays all the global term sets and any local term sets available for the site collection from which you access the Term Store management tool.

Managed Metadata column

A Managed Metadata column is a special kind of column that you can add to lists or libraries. It enables site users to select terms from a specific term set. A Managed Metadata column can map to an existing term set, or you can create a local term set specifically for the column.

To learn how to work with a Managed Metadata column, see Create a managed metadata column

Enterprise Keywords column

The enterprise Keywords column is a column that you can add to content types, lists, or libraries to enable users to tag items with words or phrases that they choose. By default, it is a multi-value column. When users type a word or phrase into the column, SharePoint presents type-ahead suggestions. Type-ahead suggestions might include items from managed term sets and the Keywords term set. Users can select an existing value, or enter something new.

List or library owners can enable or disable metadata publishing by updating the **Enterprise Metadata and Keywords Settings** for a list or library.

To learn how to add a special keywords column, see Add an enterprise keywords column to a list or library.

Tagging

In a general sense, tagging refers to the act of applying managed metadata to an item.

Metadata scenarios: from taxonomies to folksonomies

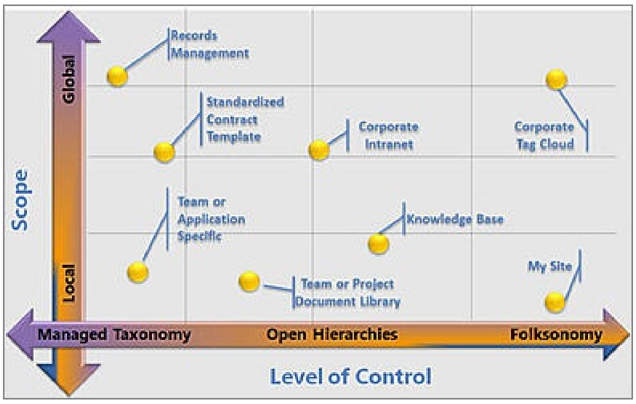
SharePoint metadata management supports a range of approaches to metadata, from formal taxonomies to user-driven folksonomies. You can implement formal taxonomies through managed terms and term sets. You can also use enterprise keywords which enable site users to tag content with keywords that they choose.

In addition, SharePoint products offer flexibility. You can choose how much structure and control to use with metadata, and you can choose the scope of control and structure. For example:

- You can apply control globally across sites, or make local to specific sites.
- You can configure term sets to be closed or open to user contributions.
- You can choose to use enterprise keywords with managed terms, or not.

SharePoint products enable organizations to combine the advantages of formal, managed taxonomies with the dynamic benefits of user-driven tagging in customized ways.

The following diagram shows how different requirements might use different levels of scope and control.



Benefits of managed metadata

There are several advantages to using managed metadata across the sites in an organization:

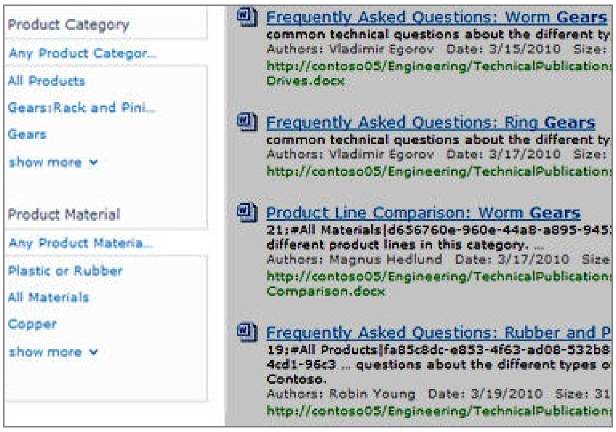
Consistent use of metadata

The managed metadata features in SharePoint products enable you to control how users add metadata to content. For example, by using term sets and managed terms, you can control which terms users can add to content, and you can control who can add new terms. You can also limit enterprise keywords to a specific list by configuring the Keywords term set as closed.

When the same terms are used consistently across sites, it is easier to build robust processes or solutions that rely on metadata. Additionally, it is easier for site users to apply metadata consistently to their content.

Improved content discoverability

When the content across sites in an organization has consistent metadata, it is easier to find business information and data by using search. Search features such as the refinement panel, which displays on the left-hand side of the search results page, enable users to filter search results based on metadata.



Metadata navigation for sites

Metadata navigation for sites enables a site administrator to create navigation elements based on metadata terms. For more information including performance recommendations, see Navigation options for SharePoint.

Metadata navigation for lists and libraries

Metadata navigation enables users to create views of information dynamically, based on specific metadata fields. Then, users can locate libraries by using folders or by using metadata pivots, and refine the results by using additional Key Filters. To learn how to set this up, see Set up metadata navigation for a list or library and Use grouping to modify a SharePoint view.

Increased flexibility

Managed metadata makes it easier for Term Store Administrators to maintain and adapt your metadata as business needs evolve. You can update a term set easily. And, new or updated terms automatically become available when you associate a Managed Metadata column with that term set. For example, if you merge multiple terms into one term, content that is tagged with these terms is automatically updated to reflect this change. You can specify multiple synonyms (or labels) for individual terms. If your site is multilingual, you can also specify multilingual labels for individual terms.

Managing metadata

Managing metadata effectively requires careful thought and planning. Think about the kind of information that you want to manage the content of lists and libraries, and think about the way that the information is used in the organization. You can create term sets of metadata terms for lots of different information.

For example, you might have a single content type for a document. Each document can have metadata that identifies many of the relevant facts about it, such as these examples:

- Document purpose - Is it a sales proposal? An engineering specification? A Human Resources procedure?
- Document author, and names of people who changed it
- Date of creation, date of approval, date of most recent modification
- Department responsible for any budgetary implications of the document

- Audience

Here are some important activities that are involved with managing metadata:

- Planning and configuring
- Managing terms, term sets, and groups
- Specifying properties for metadata

Planning and configuring managed metadata

Your organization may want to do careful planning before you start to use managed metadata. The amount of planning that you must do depends on how formal your taxonomy is. It also depends on how much control that you want to impose on metadata.

If you want to let users help develop your taxonomy, then you can just have users add keywords to items, and then organize these into term sets as necessary.

If your organization wants to use managed term sets to implement formal taxonomies, then it is important to involve key stakeholders in planning and development. After the key stakeholders in the organization agree upon the required term sets, you can use the Term Store management tool to import or create your term sets. To learn how to access the tool, see Open the Term Store management tool

Managing terms, term sets, and groups

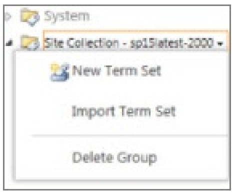
The Term Store management tool provides a tree control that you can use to perform most tasks. Your user role for this tool determines the tasks that you can perform. To work on global terms in the Term Store management tool, you must be a global admin or SharePoint admin in Microsoft 365, or a Term Store Administrator in SharePoint. To work on terms for a site, you can be a designated Group Manager or Contributor for term sets.

For more information, see Create and manage groups and term sets.

To take actions on an item in the hierarchy, follow these steps.

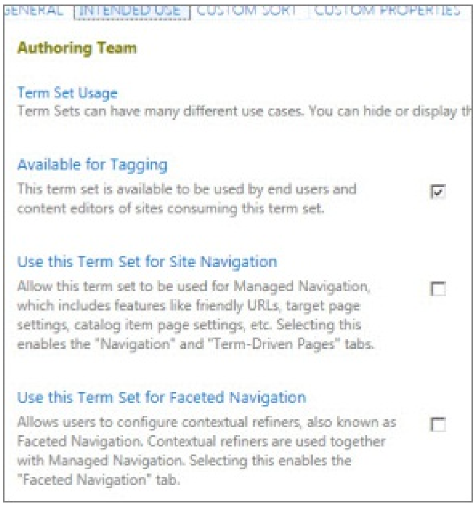
1. Point to the name of the Managed Metadata Service application, group, term set, or term that you want to change, and then click the arrow that appears.
2. Select the actions that you want from the menu.

For example, if you are a Term Store Administrator or a Group Manager you can create, import, or delete term sets in a group. Term set contributors can create new term sets.



Properties for terms and term sets

At each level of the hierarchy, you can configure specific properties for a group, term set, or term by using the properties pane in the Term Store management tool. For example, if you are configuring a term set, you can specify information such as Name, Description, Owner, Contact, and Stakeholders in pane available on the **General** tab. You can also specify whether you want a term set to be open or closed to new submissions from users. Or, you can choose the **Intended Use** tab, and specify whether the term set should be available for tagging or site navigation.



See also

Introduction to managed metadata in SharePoint Server

Set up metadata navigation for a list or library

Configure metadata navigation for a list or library

Add an enterprise keywords column to a list or library

Create a Managed Metadata column

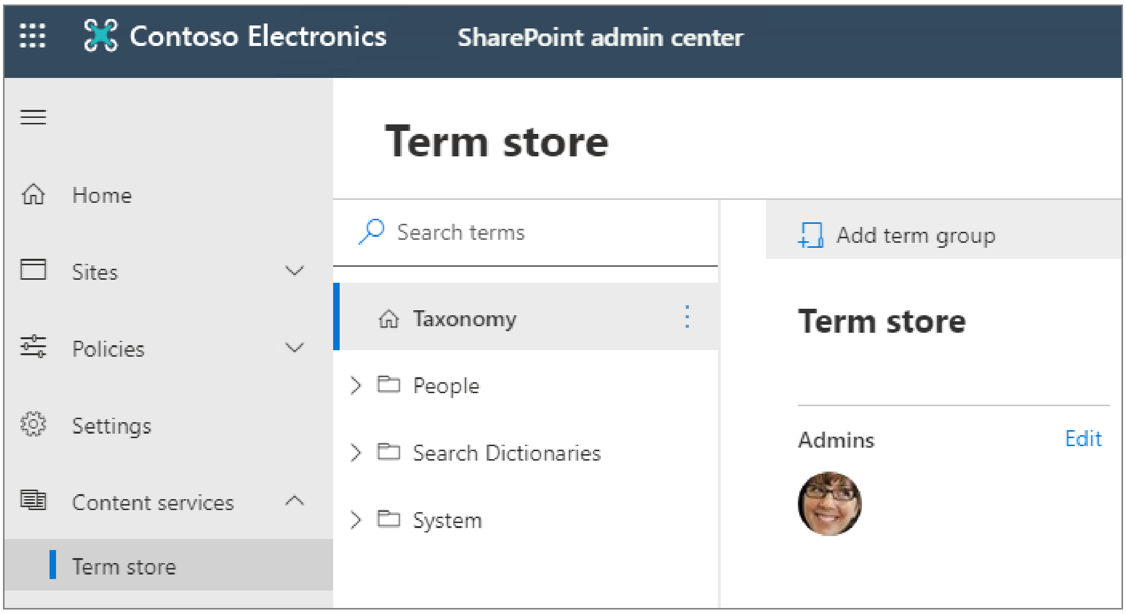
Import term sets

Open the Term Store Management Tool

6/2/2020 • 2 minutes to read • Edit Online

If you're a global or SharePoint admin in Microsoft 365, you can access the Term Store Management Tool from the SharePoint admin center.

1. Open the SharePoint admin center.
2. In the left navigation, under **Content services**, choose **Term store**.



Open term store management for a site

If you need to edit the local taxonomy for a site, you can open the terms tore management tool from the site.

1. For a site that you own, go to the **Site Settings** page.
2. Under **Site Administration**, select **Term store management**.

Set up a new group for term sets

6/2/2020 • 2 minutes to read • Edit Online

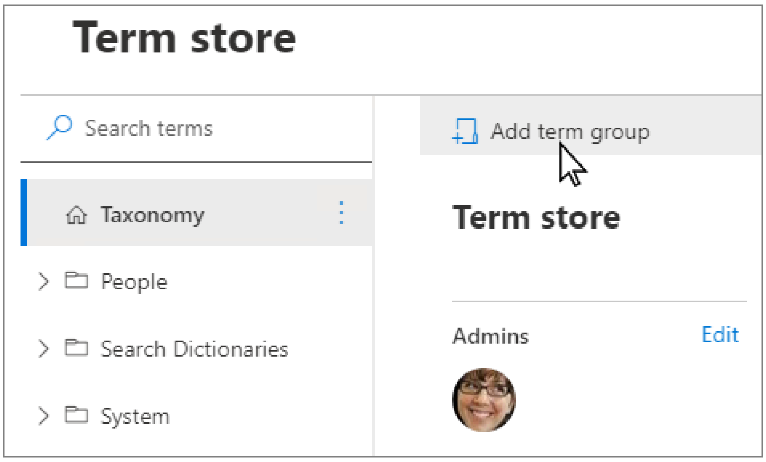
A term group is a set of term sets that all share common security requirements. Only users who are designated as contributors to a specific group can manage term sets that belong to the group or create new term sets within it. Organizations should create unique groups for term sets that will have unique access or security needs. For information about how to create a term set, see Set up a new term set.

> **IMPORTANT**
> To create a new term set group, you must be a term store admin.

To set up a new group for term sets, follow these steps.

1. In the SharePoint admin center, under **Content services**, click **Term store**.

2. In the right pane, click **Add term group**.



3. Enter a name for your new group, and then press ENTER.

4. To edit the Term group **name** and **description**, select **Edit** next to the group name. The **Edit name and description** panel appears. Enter a description to help users understand the purpose of this term group. Select **Save**.

5. To edit the group managers or contributors, select **Edit** next to **Group managers**. The **Edit admins** panel appears. Enter the names or email addresses of the people you want to add, assign them to a role, and then click **Save**.

6. To copy the unique identifier for this term group, select **Copy**.

Create and manage terms in a term set

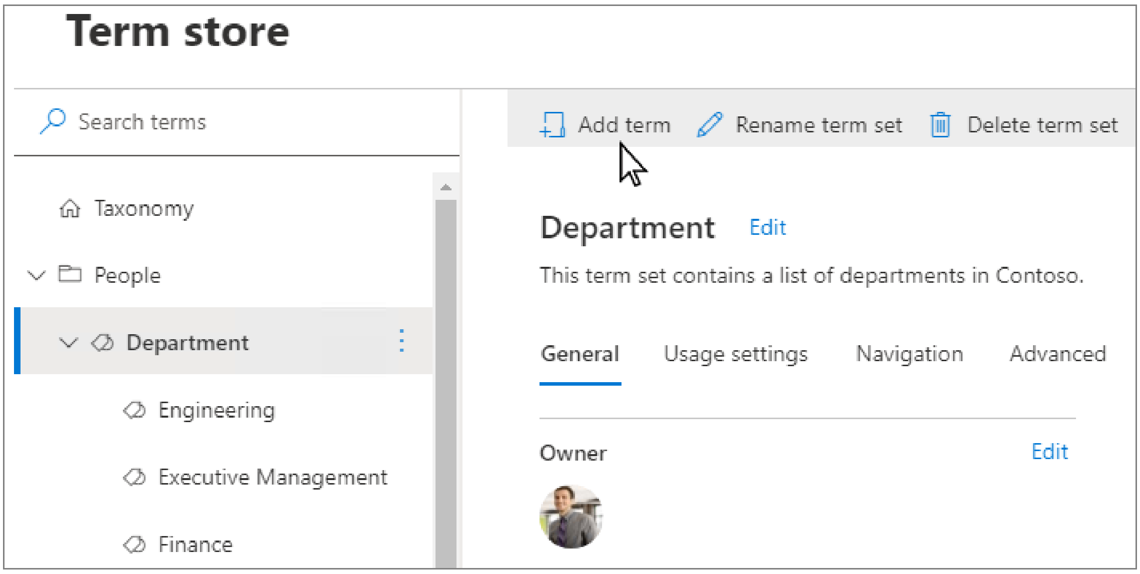
6/2/2020 • 2 minutes to read • Edit Online

To create and manage terms, you must be a contributor, a group manager, or a term store admin. (If you have many terms that you want to add, consider importing them.)

> **NOTE**
> If you are adding a term to a local term set, you must open term store management at the site level.

To create a term in a term set

1. In the SharePoint admin center, under **Content services**, click **Term store**.
2. In the tree-view pane, select the term set to which you want to add a term.
3. Click **Add term**.



4. Type a name for the term and press ENTER.
5. Update the term settings as needed:

- On the **General** tab, to add languages, translations, and synonyms, select **Add**. The **Add translation and synonyms** panel appears. Select your language, translation, description, and add synonyms. Select **Save**.
- On the **Usage settings** tab, to make the term available to the users and content editors of sites consuming this term set, select **Edit**. The **Available for tagging** panel appears. By default, the term is enabled for tagging. To disable, select the **Enable** checkbox. Select **Save**.
- On the **Advanced** tab, to use shared or local custom properties to store additional data about a term sets, select **Edit**. The **Edit shared custom properties** panel appears. Add property names and values. Select **Save**.

Take another action with terms

There are several actions that you can take on terms that will help you build and manage term sets as the business needs of your organization evolve.

To take any of the following actions, first select the term that you want to update.

Rename term

- Select **Rename term**.

Copy term

- Select **Copy term**. This action shows the name of the new term as **Copy of <original term name>**. No child terms for the source term are copied.

Move term

1. Select **Move term**. The **Move to** panel appears.
2. Select the target term set or term.
3. Select **Move**.

Delete term

If you delete this term, any terms below it will also be deleted. Terms that are shared with other term sets will be placed in the Orphaned terms term set under System.

1. Select **Delete term**.
2. Select **Delete**.

Pin term

Pinning a term makes linked copies of the term and its children available at the destination. You can only create or edit the children of a pinned term at the source and the changes will reflect everywhere the term is used.

1. Select **Pin term**. The **Pin term to** panel appears.
2. Select the target term set or term where you want to pin the term.
3. Select **Pin**.

Reuse term

Reusing a term makes linked copies of the term and its children available at the destination. You can create children for a reused term anywhere it is used but will exist only in the term set they were created.

1. Select **Reuse term**. The **Reuse term to** panel appears.
2. Select the target term set or term where you want to reuse the term.
3. Select the term, and then select **Reuse**.

Merge term

Merging this term with another will collapse its synonyms, translations and custom properties into the other term.

1. Select **Merge term**. The **Merge to** panel appears.
2. Select the target term set or term where you want to merge the term.
3. Select **Merge**.

Deprecate term

This action makes any instances of this term in any term set to which it belongs unavailable for tagging. Child terms of the term are not deprecated.

- Select **Deprecate term**.

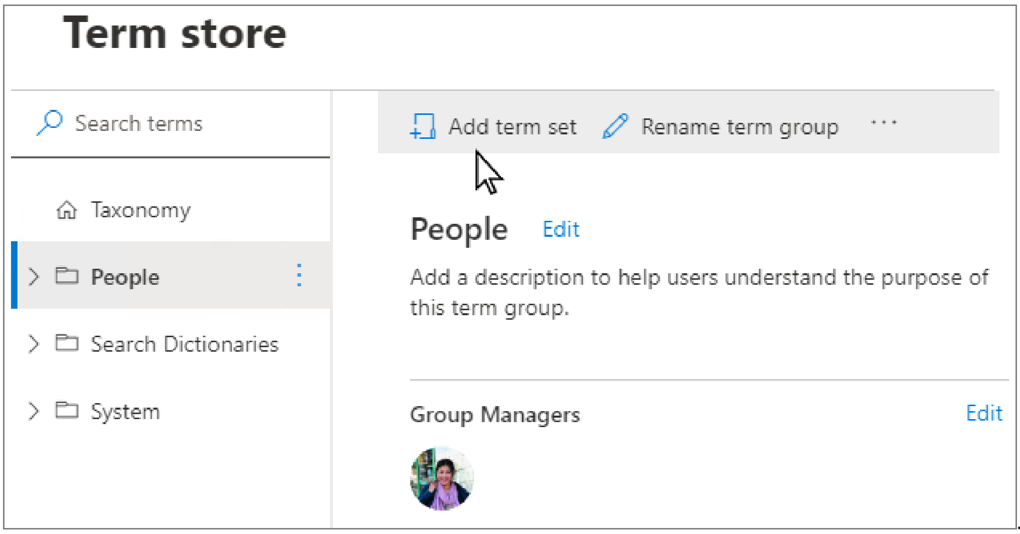
Set up a new term set

6/2/2020 • 3 minutes to read • Edit Online

To add a term set, you must be a contributor, group manager or a term store admin.

To set up a new term set

1. In the SharePoint admin center, under **Content services**, click **Term store**.
2. In the tree-view navigation pane, expand the groups to select the group to which you want to add a term set.
3. Click **Add term set**.



4. Type a name for the term set and press ENTER.

General tab

1. On the **General** tab, for **Owner**, select **Edit**. The **Edit Properties** panel appears. Specify the following information about who owns and maintains this term set:
   - **Term Set owner**: If you want the owner of the term set to be someone other than you, enter the person, group, or email address for who will maintain this term set.
   - **Stakeholders**: Add the names of users, groups, or email addresses that should be notified before major changes are made to the term set.
   - **Contact**: If you want site users to be able to provide feedback on the term set, enter an email address.
2. Click **Save**.

Usage settings tab

To configure the term submission policy

1. On the **Usage settings** tab, for **Submission policy**, select **Edit**. The **Edit submission policy** panel appears.
2. Specify whether you want the term set to be **Closed** or **Open**. If you select **Closed**, only people with contribute permissions can add terms to this term set. If you select **Open**, users can add terms from a

tagging application.

3. Click **Save**.

To configure the tagging policy

1. Under the **Usage settings** tab, for **Available for tagging**, select **Edit**. The **Available for tagging** panel appears.

2. Select the **Enable** check box to make the terms in the term set available for tagging. If you clear the **Enable** check box, this term set won't be visible to most users. If the term set is still in development, or is not otherwise ready for use, you might want to clear the **Enable** check box.

3. Select **Save**.

Usage navigation tab

Enabling site navigation means you can use the terms in this term set for site navigation links with friendly URLs and dynamic content. Enabling faceted navigation means users can use refiners based on managed metadata from the search index to quickly browse to specific content

1. Under the **Usage Navigation** tab, for **Use term set for site navigation**, select **Edit**. The **Edit Properties** panel appears.

2. Click the **Enable** check boxes to use this term set for site or faceted navigation.

3. Click **Save.**

Enabling either using the term set for site or faceted navigation enables options to set a custom target page and a custom catalog item page.

You can choose a custom target page if you want to display a specific page. Custom target pages that you set for individual terms will override this setting.

To set a custom target page

1. For **Custom target page**, select **Edit**. The **Edit term set target page** panel appears.
2. Move the toggle switch to enable **Use a custom target page**.
3. Click **Select**, and then select **Save**. The target page appears when users navigate to a friendly URL in this term set.

If terms in this term set are used as catalog categories, you can select the page used to render catalog data for items under those categories.

To set a custom catalog item page

1. For **Custom catalog item page**, select **Edit**. The **Edit term set catalog item page** panel appears.
2. Move the toggle switch to enable **Use a custom catalog item page**.
3. Click **Select** and then select **Save**.

Advanced tab

You can use machine translation to translate your terms, or you can export and import XLIFF files. You must repeat the translation each time you update the term set.

To configure translations

1. Under the **Advanced** tab, for **Translation**, select **Manage**. The **Translation** panel appears.
2. To use machine translation to translate this term set into the working languages for the term store, select **Start**. The **Machine translation** panel appears.

3. For the terms you want to translate, select either **All terms**, or **Only the terms updated since the last translation**.
4. From both the **Translate from** and **Translate to** dropdowns, select a language.
5. Click **Translate.**

You can use custom properties to store additional data about a term set.

To edit custom properties

1. For **Custom properties**, select **Edit**. The **Edit Custom properties** panel appears.
2. Enter a **Property name** and **Value**, and then select **Add**.\
3. Click **Save.**

To learn how to add a term to the new term set, see Create and manage terms in a term set.

Assign roles and permissions to manage term sets

6/2/2020 • 3 minutes to read • Edit Online

The tasks that you can do in the term store are determined by the specific role that you're assigned.

To be able to create or change a term, you must have one of three specific roles: term store admin, group manager, or contributor.

A term store admin can do these tasks:

- Create or delete term set groups.
- Add or remove group managers or contributors, or other term store admins
- Change the working languages for the term store.
- Any task that a group manager or contributor can do.

When you set up a term set, you can designate a group or a person as an Owner, Contact, or Stakeholders for the term set. These labels do not grant any specific permission to work with the term set. Instead, they provide a useful way to track the business owners or stakeholders for a term set.

Add term store admins

1. In the SharePoint admin center, under **Content services**, click **Term store**.
2. In the tree view pane on the left, select the taxonomy.
3. In the **Term store** page, for **Admins**, select **Edit**. The **Edit term store admin** panel appears. Enter the names or email addresses of the people who you want to add as term store admins. Select **Save**.

Add group managers

A group manager can do these tasks:

- Add or remove contributors.
- Any task that a contributor can do.

> **IMPORTANT**
> You must be a term store admin to add new Group Managers.

To add a group manager:

1. In the SharePoint admin center, under **Content services**, click **Term store**.
2. In the tree view pane on the left, select the Group for which you want to add a Group Manager.
3. From the **People** page, select **Edit**. The **Edit name and description** panel appears. Add a term group name and description to help users understand the purpose of this term group. Select **Save**.
4. For **Group Managers**, to add people who can create new term groups, set and assign users to the group manager and contributor role, select **Edit**. The **Edit admins** panel appears. Enter the names or email addresses of the people who you want to add as Group Managers. Select **Save**.

Add contributors

A contributor can create or change a term set.

You must be either a term store admin or a group manager of a specific group to add contributors to that group.

1. In the SharePoint admin center, under **Content services**, click **Term store**.
2. In the tree view pane on the left, select the Group to which you want to add a Contributor.
3. For **Contributors**, set and assign users to the group manager and contributor role, select **Edit**. The **Edit contributors** panel appears. Enter the names or email addresses of the people who you want to add as Contributors. Select **Save**.

Metadata tasks that site users can perform

Site users who do not have an assigned role in the term store can use terms and terms sets in other ways.

Site members can do the following tasks with managed metadata:

- Update values in managed metadata columns (if terms sets associated with the columns are open and if the column lets fill-in choices).
- Add new terms to a term set when they update the value for a managed metadata column.
- Create new enterprise keywords when they update the enterprise keywords column for a list or library.
- Use metadata navigation in lists or libraries to filter the display of items.
- Use managed terms or enterprise keywords in search queries, and then refine search results based on these terms.

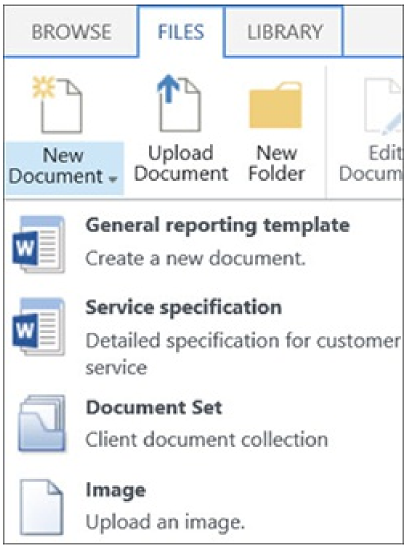
In addition, site users who have appropriate permissions (such as site owners) can create new managed metadata columns for lists, libraries, or content types. When site users create these columns, they can create new term sets that apply only to the site (previously called "site collection"), and they can manage the terms within these term sets.

Create or customize a content type

11/2/2020 • 3 minutes to read • Edit Online

Content types help make it easy to provide consistency across a site. You create or customize a content type with the characteristics that you want, such as a certain template, specific metadata, and so on. For example, when a user chooses an item from the **New Item** or **New Document** menu, you can ensure that customized content is used.

Content types created in SharePoint admin center are saved to the SharePoint content type hub located at /sites/ContentTypeHub.



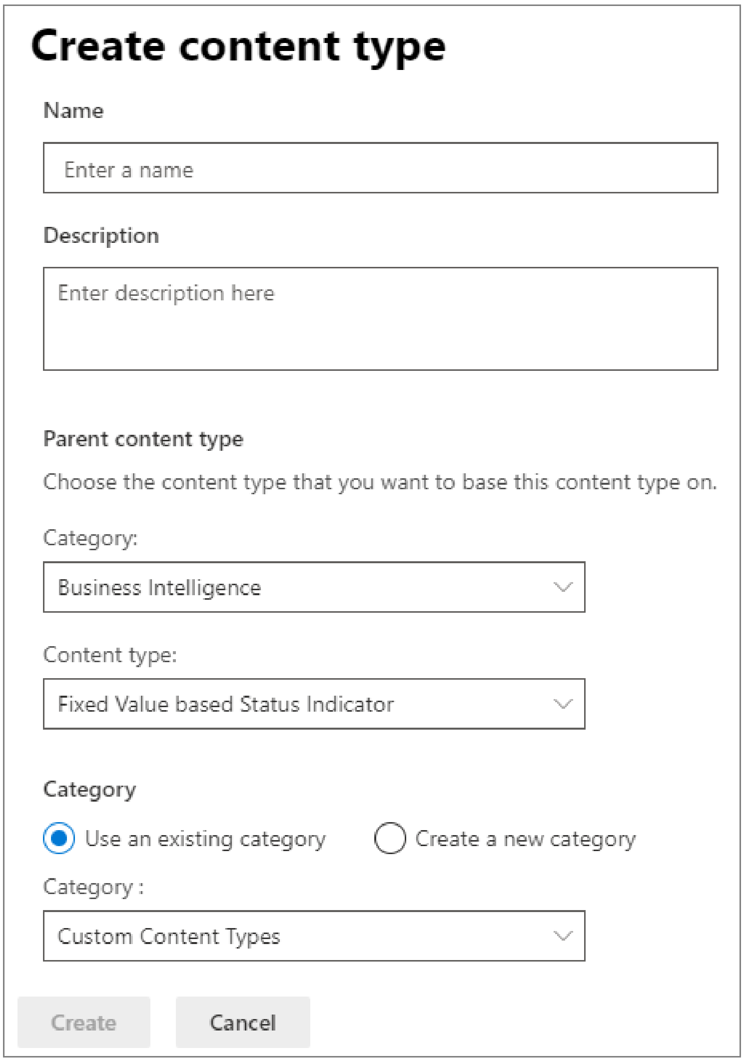
To learn more about content types, see Introduction to content types and content type publishing.

To understand how the built-in content types relate to each other, see SharePoint in Microsoft 365 default content type hierarchy.

To create a content type, follow these steps:

To create a content type

1. Go to the SharePoint admin center.
2. Under **Content services**, select **Content type gallery**.
3. Select **Create content type**. The **Create content type** panel appears.
4. On the **Create content type** panel, provide a name and description for the new content type.



5. In the **Parent content type** section, from the **Category** and **Content type** dropdowns, select the content type that you want to base this content type on.

6. In the **Category** section, you are provided two choices:

   - To put the new content type in an existing category, select **Use an existing category**, and from the **Category** dropdown, select a category.

   - To put the content in a new category, select **Create a new category**, and in the **Category name** box, provide a name.

7. Select **Create**.

The new content type appears in the **Content type gallery**.

To change the name of a content type

1. Go to the SharePoint admin center.

2. Under **Content services**, select **Content type gallery**.

3. On the **Content type gallery** page, under the **Site content type** column, select the name of the site content type that you want to change.

4. On the content type page, on the menu bar, select **Edit**. The **Edit content type** panel appears.

5. In the **Name** text box, change the name of the content type.

6. When done, select **Save**.

Associate a document template with a content type

To make sure that documents have consistent content across a site, you can associate a Word, Excel, or PowerPoint template with a site content type.

For example, you might want employees to use a standard Excel template when they create a weekly time sheet. If you associate the template with a Timesheet content type, every time someone uses the Timesheet content type, the correct template is automatically loaded in the worksheet.

You can make it even easier for users by adding the Timesheet content type to a library. Then, users can open the correct timesheet just by selecting **Timesheet** on the **New Documents** menu. To learn how to do this, see Add a content type to a list or library.

To associate a template with a content type

1. Go to the SharePoint admin center.
2. Under **Content services**, select **Content type gallery**.
3. On the **Content type gallery** page, under the **Site content type** column, select the name of the document-based content type that you want to change by associating a Word, Excel, or PowerPoint template.
4. In the menu bar, under **Settings**, select **Advanced Settings**. The **Advanced Settings** panel appears.
5. Enter the location of the template:
    - If the template is stored on your site, select **Use an existing template**, and then enter the URL for the template that you want to use. To edit the template, select **Edit template**.
    - If the document template is stored on your local computer, select **Upload a new document template**, and then select **Upload**. From the explorer page, locate the file that you want to use, select it, and then select **Open**.
6. Under **Permissions**, to select whether the content type can be modified, select either **Read** or **Edit**. You can change this setting later from this page by anyone with permissions to edit this content type.
7. Under **Update site and lists**, if you want to update all site and list content types that inherit from this content type with the settings on this page, select **Enable**.
8. Select **Save**.

Related topics

Add columns to a content type

Create or customize a site content type

Add columns to a content type

7/15/2020 • 3 minutes to read • Edit Online

The columns for a content type represent metadata. To add a metadata element, add a new column.

For example, your organization might want to track specific metadata for purchase orders, such as account number, project number, and project manager. If you add columns for this information to the purchase order content type, SharePoint prompts users to provide the information when they save their work. In addition, if you add the content type to a list or library, you can define a view to display the columns.

You can customize content types by adding columns of the types you need. You can also change the order of columns and specify if they are required fields.

Add a column to a content type

To add a column to a content type, follow these steps:

1. Go to the SharePoint admin center.
2. Under **Content services**, select **Content type gallery**.
3. On the **Content type gallery** page, under the **Site content type** column, select the name of the site content type to which you want to add a column.
4. Under **Site columns**, from the **Add site column** dropdown, select **Add from existing site columns**. The **Add from existing site columns** panel appears.
5. In the **Select site columns from existing category** section, select **Add** or **Remove** to add or remove columns from the choices that appear. You can choose a category to narrow the list of available columns.
6. In the **Update List and Site Content Types** section, decide whether you want to update all site and content types that inherit from this content type with the settings on this page.
7. Select **Save**.

Change column order

To change column order for a content type, follow these steps.

To change column order on a content type

1. Go to the SharePoint admin center.
2. Under **Content services**, select **Content type gallery**.
3. On the **Content type gallery** page, under the **Site content type** column, select the name of the site content type to which you want to change a column's order. That site content type page appears.
4. Under **Site columns**, in the **Name** column, select the column that you want to change its order.
5. Select the vertical ellipsis to the right of the site column name you selected, and from the dropdown, select **Reorder site columns** and then select from the following four choices:
   - **Move to top**
   - **Move up**

- **Move down**
- **Move to bottom**

Make a column required, optional, or hidden

To make a column required, optional or hidden, follow these steps.

To make a column required, optional, or hidden

1. Go to the SharePoint admin center.
2. Under **Content services**, select **Content type gallery**.
3. On the **Content type gallery** page, under the **Site content type** column, select the name of the site content type that you want to change a site content type by adding a column. That site content type page appears.
4. Under **Site columns**, in the **Name** column, select the name of the column that you want to make optional, required, or hidden.
5. Select **Edit site column settings**. The **Edit site column settings** panel appears.
6. In the **Show or hide site column** section, do one of the following:
    - To show or hide this column in lists, check or clear **Show this column in lists**, respectively.
    - To make it optional for users to specify information for a column, select **Optional (may contain information)**.
    - To require users to specify information for a column, select **Required (must contain information)**.
7. Under **Update sites and lists**, if you want to update all site and list content types that inherit from this content type with the settings on this page, check the box.
8. Select **Save**.

Related topics

Remove columns from a content type

Add columns to a content type

Add a content type to a list or library

Create, change, or delete a view of a list or library

Remove columns from a content type

7/15/2020 • 2 minutes to read • Edit Online

Columns can be added and removed from content types as necessary. To remove a column from a content type, follow these steps:

To remove a column from a content type

1. Go to the SharePoint admin center.
2. Under **Content services**, select **Content type gallery**.
3. On the **Content type gallery** page, under the **Site content type** column, select the name of the site content type to which you want to remove a column.
4. Under **Site columns**, select the column name you want to remove.
5. Select the vertical ellipsis to the right of the site column name you selected, and from the dropdown, select **Delete**. A **Delete site column** dialog box appears prompting you that this action will remove the column from the content type.
6. Select **Delete** to confirm.

Related topics

Add columns to a content type

Create or customize a site content type

Add a content type to a list or library

Remove columns from a content type

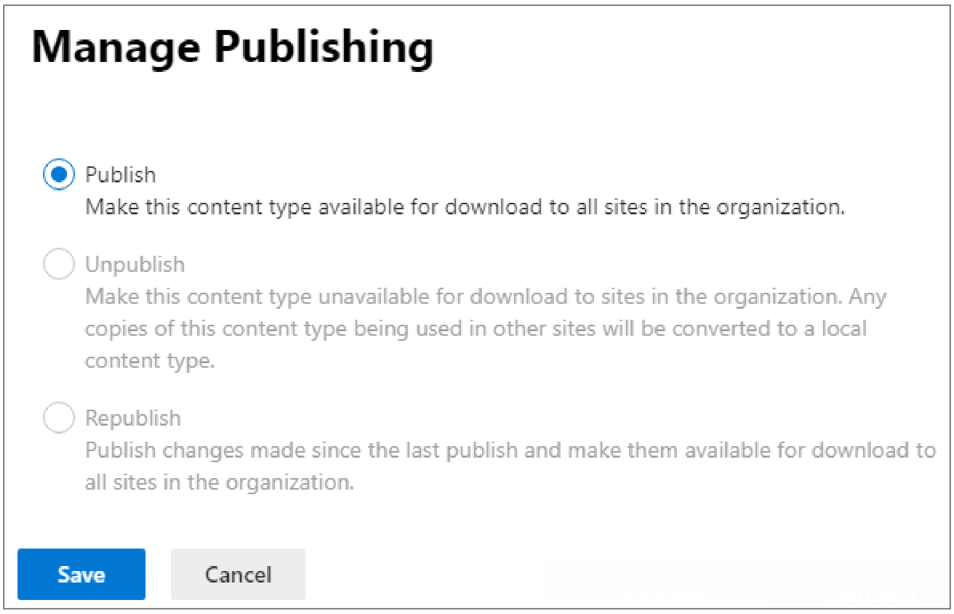
Publish a content type

1/8/2021 • 2 minutes to read • Edit Online

You can publish, unpublish, or republish content types in the content type hub at /sites/ContentTypeHub or from the SharePoint admin center.

To publish, republish, or unpublish a content type

1. Go to the SharePoint admin center.
2. Under **Content services**, select **Content type gallery**.
3. On the **Content type gallery** page, under the **Site content type** column, select the name of the site content type for which you want to manage updates. That site content type page appears.
4. In the menu bar, select **Publish**. The **Manage Publishing** panel appears.



5. On the **Manage Publishing** page, do one of the following:
   - To make this content type available for download to all sites in the organization, select **Publish**.
   - To publish updates to this content type, select **Republish**.
   - To make this content type unavailable for download to sites in the organization, select **Unpublish**. Any copies of this content type being used in other sites will be converted to a local content type.
6. Select **Save**.

Related topics

Publish a content type from a content publishing hub

Introduction to content types and content type publishing

Search experiences in SharePoint

1/8/2021 • 3 minutes to read • Edit Online

Microsoft Search is the modern search experience in SharePoint in Microsoft 365 and is a personalized experience. It uses the insights of the Microsoft Graph to show results that are relevant to you. Routine tasks such as finding the right version of a document, getting back to a presentation you were editing, or a document you were collaborating with others on, are easy. Learn more about Microsoft Search for users. The classic search experience, on the other hand, can be tailored more to your organization. Learn about the differences between the search experiences.

Both search experiences are turned on by default and as a search administrator you can't turn either search experience off. Which search experience your users see depends on where they search from:

- Users get the classic search experience on publishing sites, classic team sites, and in the Search Center.
- Users get the Microsoft Search experience on the SharePoint start page, hub sites, communication sites, and modern team sites. Learn about classic and modern sites.

  If you're in a document library, the search box shows **Search this library**. If you're in the home page of the site, the box shows **Search this site**. In all other locations, the search box shows **Search**.

Benefits of Microsoft Search in SharePoint

Easy to search - Microsoft Search suggests results based on users' previous activity in Microsoft 365, right in the search box. On the search results page the results are ordered by relevance.

Find shared files - Microsoft Search uses advanced query understanding to make finding shared files simple. Users can easily find files they're collaborating on.

Show relevant content - Promote the information and answers your users need to complete tasks, for example policies, benefits, resources, tools, and more. You can also target specific groups, like new hires or remote workers.

Administer across all apps - Microsoft Search is on by default and any administration you do applies to Microsoft Search in all the apps.

Easy to explore results - Users can explore results without leaving search. They can for example browse through a presentation directly in the search results page and quickly assess if it's the right result.

Mobile friendly - The Microsoft Search results page is mobile friendly.

User friendly interface - Microsoft Search offers a great user interface without a search administrator configuring anything. Learn more

Microsoft Search evolves - The set of content types users can search for and the intelligence of the search box will grow over time. Learn what's coming next in Microsoft Search

When to use which search experience?

Which experience your users see depends on whether your organization mostly uses classic or modern sites. If you believe that Microsoft Search gives your users the best experience, learn how to get started with Microsoft Search in SharePoint.

Should you use the Search Center or the SharePoint start page as your portal?

If you need custom refiners or search verticals for organization-specific content, or you need to display results for organization-specific content differently than other content. Use the Search Center (classic search) as your portal. If not, we recommend promoting the SharePoint start page (Microsoft Search) to your users.

Is the search experience impacted if you migrate from classic to modern sites?

Yes, if you have customized search. A classic site has a classic search box. For example, you've set up the search box to redirect to a custom Search Center in order show results that are filtered and formatted for organization-specific content types. The modern site has the Microsoft Search box. You can't customize the Microsoft Search experience like that. If you don't need to customize search, we recommend using modern sites.

Can users search across all sites of an administrative unit?

It's possible, but it takes some effort to do this with classic search. It's better to use a hub site to organize the sites. Hub sites use Microsoft Search, which is scoped to search for news, people, files, and sites across all sites that are associated with the hub. Learn more about hub sites

Can you use Microsoft Search in combination with cloud hybrid search?

Yes. With cloud hybrid search, both on-premises and online content go into the same index, which both the classic and Microsoft Search experiences use.

Overview of search in SharePoint

11/2/2020 • 3 minutes to read • Edit Online

If you're responsible for search in your organization, learn how you can tailor the search experience to your organization and make search even better for your users.

SharePoint in Microsoft 365 has both a classic and a modern search experience, where Microsoft Search in SharePoint is the modern search experience. The most visible difference is that the Microsoft Search box is placed at the top of SharePoint, in the header bar. Another difference is that Microsoft Search is personal. The results one user sees are different from what other users see, even when they search for the same words. Users see results before they start typing in the search box, based on their previous activity and trending content in Microsoft 365, and the results update as they type. The search results are easy to explore without any effort from you as an admin. Learn more about the Microsoft Search experience for users in Find what you need with Microsoft Search.

Both search experiences use the same search index to find search results. You can customize and tailor the classic search experience more tha Microsoft Search in SharePoint. Some classic search settings can impact both experiences, learn how to avoid impacting Microsoft Search. Read When to use which search experience to decide which experience is best for your organization.

See the following main areas where you can customize and impact the search experience and make sure that search is performing the way you want. The high-level overview of How search works can also help you understand where and how you can impact the search experience in SharePoint.

Many of the classic search features are available on the search administration page in the SharePoint admin center.

1. Make sure the content can be found

The content must be crawled and added to the search index for your users to find what they're looking for when they search in SharePoint. Microsoft Search uses the same index of SharePoint content as classic search does.

See how you can make content searchable, and how you can crawl content to get it into the search index. Also, see how you can help users search for content across Microsoft 365 and on-premises SharePoint Server at the same time. Learn more

2. Make the search results look great

Presenting the search results the right way makes content easier to find.

See how you can manage the classic experience in the Search Center in SharePoint, and how you can use the different search Web Parts to help each user find what they're looking for. See Make the search results look great

3. Show relevant search results

All search results are not relevant to everyone all the time.

See how you can show each user exactly the results they're looking for. See Show the right search results

4. Check logs, limits and reports

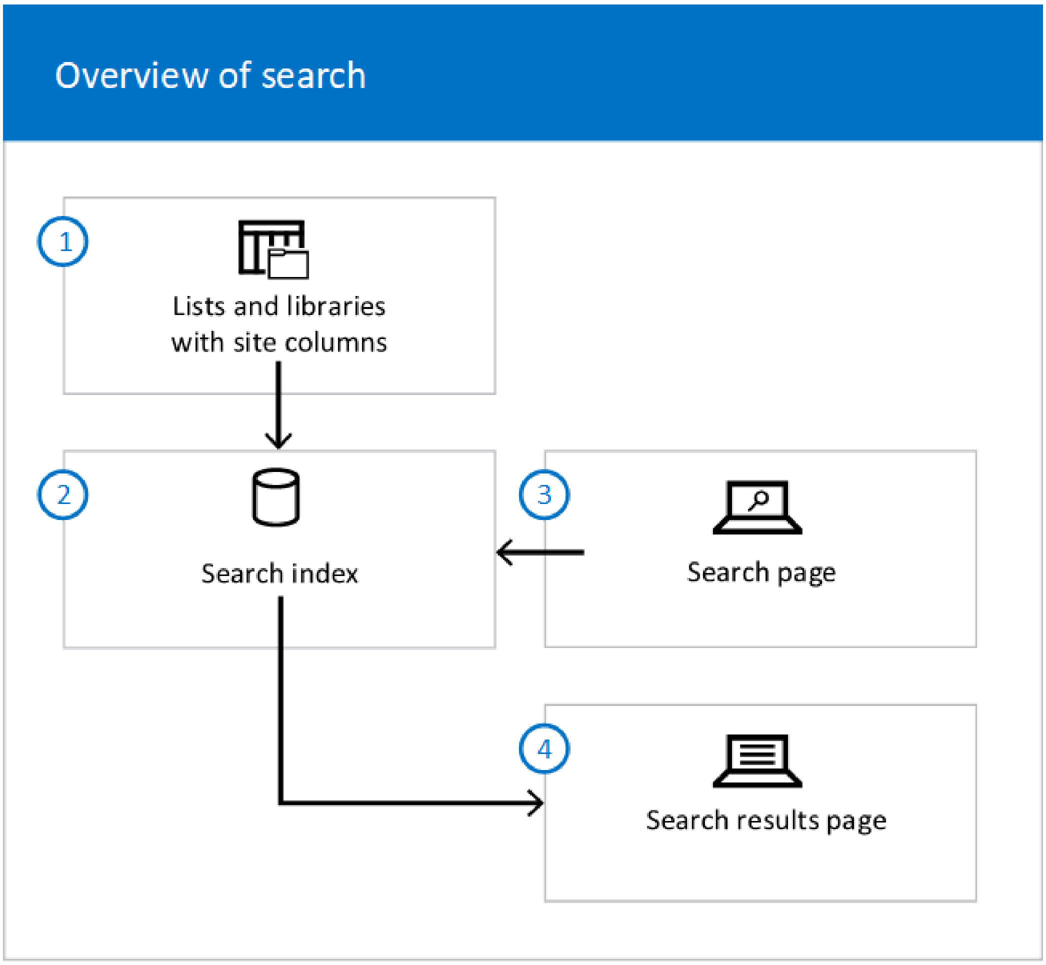
See how you can check if the crawler has added content to the search index, and if your users are finding what they're looking for. Look up the limits for search, for example how many entries you can have in a custom search dictionary. See Check logs, limits and reports

How search works

This high-level overview of how search works can help you understand where and how you can customize the search in SharePoint.

In lists and libraries, site columns store detailed information about each document.

1. Search **crawls** the lists and libraries and adds the site columns and values to the search index.
2. In the **search index**, site columns are mapped to managed properties.
3. When a user enters a **query** in a search box, the query is sent to the search index.
4. The search engine finds **matching results**, and sends them to a search results page.



See also

Learn about Microsoft Search

Get started with Microsoft Search in SharePoint

SharePoint classic search administration overview

11/2/2020 • 3 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can customize and impact the search experiences for your users. You can define searchable managed properties in the search schema, identify high-quality pages to improve relevance, manage query rules and result sources, and remove individual results. You can also evaluate any changes by viewing reports about usage and search.

The changes you make from the search administration page are valid for the whole tenant, but you can also customize search on site collection level and on site level.

You can customize and tailor the classic search experience more than Microsoft Search in SharePoint. Some classic search settings can impact both experiences, learn how to avoid impacting Microsoft Search.

How to get to the classic search administration page

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

What do you want to do?

CHOOSE THIS OPTION:	TO DO THIS:
Manage the search schema	Learn how to create a customized search experience by changing the search schema. In the search schema, you can view, create, or change managed properties, and map crawled properties to managed properties.
Manage search dictionaries	Learn how to manage search dictionaries for classic search. You can use search dictionaries to include or exclude company names to be extracted from the content of your indexed documents, or you can include or exclude words for query spelling correction.
Manage authoritative pages	Influence the pages or documents that should appear at the top of the search results by identifying high-quality pages, also known as authoritative pages, for the classic search experience.

CHOOSE THIS OPTION:	TO DO THIS:
Manage query suggestion settings	Learn how to add phrases that you want the system to suggest to users as they search for an item using classic search, and how to add phrases that you don't want the system to suggest to users. Also, learn how to turn this feature on or off.
Manage result sources	Result sources limit searches to certain content or to a subset of search results. Learn how to create your own result sources, or change the predefined result sources.
Manage query rules	Improve search results in the classic search experience by creating and managing query rules. Query rules can help searches respond to the intent of users.
Manage query client types	Learn how query client types decide in which order queries are performed in the classic search experience.
Remove search results	Learn how you can temporarily remove items from the search results with immediate effect. These items can be documents, pages, or sites that you don't want users to see when they search.
View usage and search reports	View usage reports and search reports and see how often your users search, what their top queries are, and which queries they're having trouble getting answers for.
Manage Search Center settings	Choose where searches in the classic search experience should go by specifying the URL of your Search Center.
Import and export customized search configuration settings	Learn how to export and import customized search configuration settings between tenants, site collections, and sites.
Manage crawl log permissions	Learn how to grant users or groups read access to crawl log information for the tenant. A typical use case is in eDiscovery, where users may need to check whether crawled content was in fact added to the search index.

NOTE

Thesaurus isn't available in SharePoint in Microsoft 365.

See also

Search limits for SharePoint

Make sure content can be found

11/2/2020 • 2 minutes to read • Edit Online

The content must be crawled and added to the search index for your users to find what they're searching for in Microsoft SharePoint. SharePoint in Microsoft 365 has both a classic and a modern search experience, both use the same search index. Learn about the differences between the classic and modern search experiences in SharePoint

Make site content searchable

When users search on a site, results can come from many places such as columns, libraries, and pages. A site owner can change search settings to decide whether or not content should appear in search results.

Users only see search results for content they have access to. Setting the right permissions for content ensure that people can see the right documents and sites in the search results. Learn more.

Crawl site content

In SharePoint, content is automatically crawled based on a defined crawl schedule. The crawler picks up content that has changed since the last crawl and updates the index.

In some cases, you may want to manually request crawling and full re-indexing of a site, a document library, or a list. Learn more.

Search across on-premises and online content

Hybrid search in SharePoint lets your users search for files and documents across SharePoint Server and Microsoft 365 at the same time. With cloud hybrid search, both on-premises and online content go into the index that both the classic and Microsoft Search experiences use.

Remove search results temporarily

You can **temporarily** remove documents, pages and sites from search results with immediate effect. Learn more.

Enable content on a site to be searchable

11/2/2020 • 8 minutes to read • Edit Online

When users search on a site, results can come from many places such as columns, libraries, and pages. A site owner can change search settings to decide whether content is allowed to appear in search results. Permissions on content also affect whether users are allowed to see the content in search results. A good understanding of how permissions and search settings work can help you ensure that users can see the right documents and sites in the search results.

> **NOTE**
>
> Search results are always security trimmed, so users will only see content they have permission to see. The search settings only define what content is included in the search index.

Plan to make your content available in search results

As a site owner, you can use settings to control whether content can appear in search results. Content is stored in many places including sites, lists, libraries, Web Parts, and columns. By default, most content contained in a site, list, library, Web Part page, or column will be crawled and added to the search index. What's in the search index decides what content can appear in search results both in the **classic** and **modern** search experiences. The permissions that are set on items, lists, libraries, sites, and so forth, also affect whether users can see the content in search results.

Site owners and site collection administrators can choose whether content can appear in search results. By default, the content of a site can appear in search results. If a site owner or site collection administrator specifies that the content from a particular site can't appear in search results, then the other search results settings such as those for lists, libraries, ASPX pages, and columns set on that site wouldn't have any effect.

Similarly, if a site owner or site collection administrator prevents list or library content from appearing in search results, then excluding columns wouldn't have any effect. It's important to know what settings are inherited from higher levels in order to plan search effectively.

Understand search settings and permissions

One of the responsibilities of a site owner is to control who has access to content. You can give some people permission to read and change content, allow others to only read content, and prevent others from viewing content entirely. In order to accommodate this flexibility, you use permissions groups, which are assigned specific permission levels. To allow users access to the site or to content on that site, a site owner assigns users to one or more security groups. By using permissions settings in conjunction with search results settings, the site owner can manage whether users can see content in search results.

For example, let's say Joe is working on a Request for Proposal (RFP) in Microsoft Office Word and is collaborating with a team of 10 people. His team site has 50 users, all of whom are Site Members. Joe isn't ready for the whole team to view the RFP. Therefore, when he uploads it to the team site, he sets the permissions so that only the team of 10 can view and edit it. Until he grants all 50 people read permissions, only the 10 people who have permission to view the document will see it listed in search results.

Permissions can be applied to lists, sites, views, and Web Parts. Also, permissions can be dependent on other permissions. All of this can affect what the user sees in search results. Therefore, before adding any content to your site, you may want to familiarize yourself with SharePoint's permissions model, the permissions model of your site or organization, or to plan what the permissions model will be for your site.

See also: Default SharePoint Groups in SharePoint

Show content on a site in search results

As a site owner, you can choose whether the content on your site can appear in search results. By default, all site content can appear in search results. The person who's viewing search results must have permission to view the content.

> **NOTE**
> To change this setting, you must have the Manage Permissions permission level. This permission level is included in the " *Site Name* " Owner group.

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Search**, click **Search and offline availability**.

3. In the **Indexing Site Content** section, under **Allow this site to appear in Search results**, select **Yes** to allow the content of the site to appear in search results.

To prevent the content from appearing in search results, select **No**.

Show content from lists or libraries in search results

As a site owner, you can decide whether items in lists and libraries on your site are included in search results. By default every list and library is set to include all items in search results.

> **NOTE**
> To change this setting, you must have the Manage Lists permission level. The Designer and " *Site Name* " Owner groups contain this permission level. When you do not have Manage Lists permissions, the menus described in this procedure aren't available.

1. On the site, find and click the list or library you want to customize.

2. Select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

3. Under **Site Administration**, click **Site Libraries and lists**.

4. Click an item from the list, for example, **Customize "Shared Documents."**

5. On the List Settings page, under **General Settings**, click **Advanced settings**.

6. In the **Search** section, under **Allow items from this document library to appear in search results**, select **Yes** to include all of the items in the list or library in search result.

To prevent items from the list or library to appear in search results, select **No**.

Show contents of ASPX pages in search results

You can control whether the content of ASPX pages is included in search results. When you create a site, many content pages are created automatically. For example, default.aspx, allitems.aspx for your Web Part gallery, and several others are automatically created pages. You can also create custom ASPX pages.

By default, when a Web Part displayed on an ASPX page uses information from a list or library that contains restricted permissions, also known as fine-grained permissions, none of the content in any of the ASPX pages on the site is included in search results. This prevents non-authorized users from viewing content.

For example, let's say five documents are displayed in a Shared Documents Web Part on a team site with 50 members. One of the documents has restricted permissions; only a few people are allowed to see it. Content is automatically hidden from that site in search results so that the content from that document does not appear when users search. This prevents the content of the ASPX page from unintentionally being exposed to people who are not supposed to see it.

You have the option of ignoring this setting to display all content in search results regardless of permissions. In this case, all content can appear in the search results, but unauthorized users will not be able to access the actual documents. Another option is to not include any ASPX content in search results, regardless of permissions.

> **NOTE**
> To change this setting, you must have the Manage Permissions permission level. This permission level is included in the " *Site Name* " Owner group.

1. On the site, select **Settings** ⚙, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Search**, click **Search and offline availability**.

3. In the **Indexing ASPX Page Content** section, select one of the following options:

OPTION	DESCRIPTION
Do not index Web Parts if this site contains fine-grained permissions	When permissions of the ASPX page are different from the parent site, no content on the site appears in search results.
Always index all Web Parts on this site	Show content of all ASPX pages on the site in search results regardless of permissions.
Never index any Web Parts on this site	Hide content of all ASPX pages on the site from search results regardless of permissions.

Exclude content in columns from search results

As a site owner you can control whether the content in specific columns in lists or libraries appears in search results. By default, all content is included in search results. This setting is useful when you want to prevent sensitive data from appearing in search results.

> **NOTE**
> To change this setting, you must have the Manage Permissions permission level. This permission level is included in the *"Site Name"* Owner group.

1. On the site that contains the list or library, select **Settings** ⚙, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Search**, click **Searchable columns**.

3. In the **Excluded Columns from Search Indexing** section, under **Excluded**, check the box next to the

Column Name for the column you want to exclude in search results.

> **NOTE**
>
> Columns that appear are those that belong to the current site.

Crawl and re-index a site

When people search for content on your SharePoint sites, what's in your search index decides what they'll find. The search index contains information from all documents and pages on your site. In SharePoint, content is automatically crawled based on a defined crawl schedule. The crawler picks up content that has changed since the last crawl and updates the index.

For cases in which the Search schema has changed where a managed property has been added/removed/changed, you will want to specifically request a full re-indexing of a site. See Manually request crawling and re-indexing of a site for more information.

Manually request crawling and re-indexing of a site, a library or a list

11/2/2020 • 2 minutes to read • Edit Online

In SharePoint, content is automatically crawled based on a defined crawl schedule. The crawler picks up content that has changed since the last crawl and updates the index. You will want to manually request crawling and full re-indexing of a site, a document library, or a list after a schema change has occurred.

Caution

Re-indexing a site can cause a massive load on the search system. Don't re-index your site unless you've made changes that require all items to be re-indexed.

Re-index after changing managed properties

When people search for content on your SharePoint sites, what's in your search index decides what they'll find. The search index contains information from all documents and pages on your site.

The search index is built up by crawling the content on your SharePoint site. The crawler picks up content and metadata from the documents in the form of crawled properties. To get the content and metadata from the documents into the search index, the crawled properties must be mapped to managed properties. Only managed properties are kept in the index. This means that users can only search on managed properties.

When you have changed a managed property, or when you have changed the mapping of crawled and managed properties, the site must be re-crawled before your changes will be reflected in the search index. Because your changes are made in the search schema, and not to the actual site, the crawler will not automatically re-index the site. To make sure that your changes are crawled and fully re-indexed, you must request a re-indexing of the site. The site content will be re-crawled and re-indexed so that you can start using the managed properties in queries, query rules and display templates.

You can also choose to only re-index a document library or a list. When you have changed a managed property that's used in a library or list, or changed the mapping of crawled and managed properties, you can specifically request a re-indexing of that library or list only. All of the content in that library or list is marked as changed, and the content is picked up during the next scheduled crawl and re-indexed.

Learn more about search and crawled and managed properties in Manage the search schema in SharePoint.

See also: Enable content on a site to be searchable

Re-index a site

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Search**, click **Search and offline availability**.
3. In the **Reindex site** section, click **Reindex site**.
4. A warning appears, click **Reindex site** again to confirm. The content will be re-indexed during the next scheduled crawl.

Re-index a document library or a list

1. On the site, go to the list or library that you want to re-index.
2. In the ribbon, click the **Library** tab or the **List** tab.
3. In the **Library** ribbon, choose **Library Settings**. Or, in the **List** ribbon, choose **List Settings**.
4. On the Settings page, under **General Settings**, choose **Advanced settings**.
5. Scroll down to **Reindex Document Library** or **Reindex List**, and click the button. The content will be re-indexed during the next scheduled crawl.

See also

Get-PnPSearchCrawlLog

Remove search results

11/2/2020 • 2 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can temporarily remove items from search results with immediate effect. The items that you can remove can be documents, pages, or sites that you don't want users to see. An example of this could be a Word document containing an invitation to an event that has been cancelled, but the organizer has not removed the document from the site yet. Removing a result removes it from both classic and modern search results.

> **IMPORTANT**
>
> This is only a quick fix! Unless you delete the items or change the permissions of items manually, they will show up again in your search results after the next crawl.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. On the **search administration** page, select **Remove Search Results**.
4. On the **Remove Search Results** page, in the **URLs to remove** box, enter the URLs that you want to remove from the search results. Enter one URL on each line.
5. Select **Remove Now**. The URLs are immediately removed from your search results.

Make the search results look great

11/2/2020 • 2 minutes to read • Edit Online

Presenting the search results the right way makes content easier to find for users.

SharePoint has both a classic and a modern search experience, where Microsoft Search in SharePoint is the modern search experience. Learn about the differences between the search experiences in SharePoint.

If you're responsible for search in your organization, you can customize how results are presented on classic search results pages. Read about how you can use the search web parts in SharePoint to make it easier for users find what they're looking for in the classic search experience.

Manage the Search Center

A Search Center is a classic site where users can enter search queries and view search results. Learn more.

Specify the default Search Center URL

Choose where searches should go by specifying the URL of your default Search Center. Learn more.

Specify the Search Center URL for a site or subsite

For each site or subsite, you can specify the URL of the Search Center where you want the search results from the site to be displayed. Learn more.

The Search Box Web Part

The Search Box Web Part shows a text box where users can enter words or phrases to search for information. Learn more.

The Search Results Web Part

The Search Results Web Part shows the search results of a query that was entered in a Search Box Web Part. Change settings for the Search Results Web Part

The Search Navigation Web Part

The Search Navigation Web Part lets users move quickly between search verticals, for example between **People** and **Videos**. Learn more.

The Refinement Web Part

The Refinement Web Part filters search results into categories called refiners. The refiners help users drill into the search results to find what they're looking for. About configuring the Refinement Web Part.

The Content Search Web Part

When visitors browse to a page that contains a Content Search Web Part, the Web Part automatically issues a query. The search results are displayed within the Web Part. Configure a Content Search Web Part in SharePoint.

Use result types and display types to change how search results look

To help users quickly distinguish between different types of results, you can use *result types* and *display templates* to show important information directly in the search results. Users don't have to click on each result to see if they've found what they're looking for. Learn more.

Manage the Search Center in SharePoint

11/2/2020 • 2 minutes to read • Edit Online

The Search Center is a classic search experience. The Search Center is a site or site collection that has a starting page where users enter search queries and a search results page where users can drill into and refine search results, or run a new query.

SharePoint offers two types of Search Centers: the **Basic** Search Center and the **Enterprise** Search Center. By default, SharePoint is set up with the Basic Search Center.

Both Search Centers search the same content and show the same search results. The main difference is that the Enterprise Search Center comes with the search verticals People, Conversations, and Videos. Search verticals are pages that are tailored for displaying search results that are filtered and formatted for a specific content type or class. Search verticals help users move quickly between such different types and classes of content. Also, as a search administrator you have more options for tailoring the look and feel of the Enterprise Search Center.

If your organization needs an enterprise-wide search experience, evaluate first whether the modern search experience covers your needs. Modern search also comes with verticals, it doesn't require any set up, and the results are personal. Learn about the modern search experience for users.

If modern search doesn't cover you needs, you can switch from the Basic Search Center to an Enterprise Search Center.

Search Center pages

These pages are located in the **Pages** library, and they contain predefined Web Parts that you can customize to improve the end user's search experience.

PAGE	DESCRIPTION
default.aspx	The home page for Search Centers, and the page where users enter their queries.
results.aspx	The default search results page for the Search Centers. If you have an Enterprise Search Center, this is also the search results page for the **Everything** search vertical.
peopleresults.aspx	If you have an Enterprise Search Center, this is the search results page for the **People** search vertical.
conversationresults.aspx	If you have an Enterprise Search Center, this is the search results page for the **Conversations** search vertical.
videoresults.aspx	If you have an Enterprise Search Center, this is the search results page for the **Videos** search vertical.
advanced.aspx	This is the search page where users can apply some restrictions to their search phrases — for example, they can limit the search to an exact phrase.

As a global or SharePoint admin, you can also create your own search pages and add them to the Enterprise Search Center as search verticals, see Add a search vertical to the Search Navigation Web Part.

About the Web Parts used on Search Center pages

The Search Center pages contain the following predefined Web Parts: Search Box Web Part, Search Results Web Part, Search Navigation Web Part, and Refinement Web Part.

If you have an Enterprise Search Center, the Web Parts on the search result pages are by default set up the same way. The only difference is that the query in the **Search Results** Web Part is directed to different result sources for each search vertical page. For example, for the **People** search vertical page, the query in the **Search Results** Web Part is limited to the **Local People Results** result source. For the **Videos** search vertical page, the query in the **Search Results** Web Part is limited to the **Local Video Results**.

For information about how to customize the Search Center Web Parts, see the following articles:

- Change settings for the Search Box Web Part
- Change settings for the Search Results Web Part
- Change settings for the Search Navigation Web Part
- Change settings for the Refinement Web Part

Search Center settings

11/2/2020 • 2 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can specify where searches should go for your classic site collection or site by specifying the URL of your Search Center. For example, if you have created an Enterprise Search Center where users can search everything in your company, you can enter the URL of that site here.

Enter the address of your Search Center

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. On the **search administration** page, select **Search Center Settings**.
4. In the **Search Center URL** box, enter the URL of the Search Center site.

   Example: http://companyportal/searchcenter/pages.

5. Select **OK**.

> **NOTE**
> It may take up to 30 minutes before changes take effect.

Specify search settings for a site collection or a site

11/2/2020 • 3 minutes to read • Edit Online

As a global or SharePoint admin, you can specify how search should behave for a classic site collection or a site. The shared Search Box at the top of most classic pages uses these search settings. Any settings you specify on site collection level applies to all sites within that site collection, unless you specify other settings for the site.

You can specify where searches should go for your classic site collection or site by specifying the URL of your Search Center. For example, if you have created an Enterprise Search Center on your site where users can search everything in your company, you can enter the URL of that site here. If you do not enter a Search Center URL, searches will go to the default Search Center, available at <host_name>/search/.

When you create an Enterprise Search Center site collection SharePoint creates a default search home page and a default search results page. In addition, several pages known as search verticals are also created. Search verticals are customized for searching specific content, such as People, Conversations, and Videos, and they display search results that are filtered and formatted for a specific content type or class.

For more on creating and customizing a search center for your site, see Manage the Search Center in SharePoint.

You can change which search results page queries are sent to. By default, queries are sent to the same search results page as the parent, but you can override this for a site collection or a site.

You can also configure search navigation for a site. With search navigation, users can move quickly between different search vertical pages. Navigation links are shown in the Search Navigation Web Part on search result pages, and can also be shown as a drop-down menu in the search box.

> **NOTE**
> It may take up to 30 minutes before changes take effect.

Specify search settings for a site collection

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Site Collection Administration**, click **Search Settings**.
3. To specify a Search Center, in the **Search Center URL** box, type the URL of the Search Center site.
4. To change which search result page queries are sent to, in the section **Which search results page should queries be sent to?**, clear **Use the same results page settings as my parent**, and then select one of the following:

- **Send queries to a custom results page URL**. Enter the URL. Custom URLs can be relative or absolute, and can also include special tokens, such as {SearchCenterURL}.

  Example: /SearchCenter/Pages/results.aspx or http://server/sites/SearchCenter/Pages/results.aspx.

- **Turn on the drop-down menu inside the search box, and use the first Search Navigation node as the destination results page**. If you choose this option, users can choose search vertical in the search box when they enter a query.

5. Click **OK**.

Specify search settings for a site

By default, a site has the same search settings as the site collection that the site belongs to. You can, however, override these settings by defining specific search settings for the site.

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Search**, click **Search Settings**.

3. To specify a Search Center, in the **Search Center URL** box, type the URL of the Search Center site.

4. To change which search result page queries are sent to, in the section **Which search results page should queries be sent to?**, clear **Use the same results page settings as my parent**, and then select one of the following:

- **Send queries to a custom results page URL**. Enter the URL. Custom URLs can be relative or absolute, and can also include special tokens, such as {SearchCenterURL}.

  Example: /SearchCenter/Pages/results.aspx or http://server/sites/SearchCenter/Pages/results.aspx.

- **Turn on the drop-down menu inside the search box, and use the first Search Navigation node as the destination results page**. Make sure that the search vertical you want as a default is the first option in the **Configure Search Navigation** section.

5. To configure search navigation, edit settings in the **Configure Search Navigation** section as required. You can, for example:

- Change the display name or the URL of a search vertical

- Change the order of the search vertical links

- Add a search vertical

  See Change settings for the Search Navigation Web Part for steps.

6. Click **OK**.

Change settings for the Search Box Web Part

11/2/2020 • 3 minutes to read • Edit Online

The Search Box Web Part shows a text box where users can enter words or phrases to search for information. By default, the Search Box Web Part is used on the home page for the Search Center (default.aspx), and all default search results pages (**Everything**, **People**, **Conversations**, and **Videos**).

As a global or SharePoint admin in Microsoft 365, you can change settings in the Search Box Web Part. You can:

- Change where the search results should be displayed — for example, show results in a custom Search Results Web Part or a custom search results page.
- Turn off query suggestions and people suggestions.
- Show links to a search preference page and an advanced search page.
- Change the display template that is used for the Web Part.

Change where search results are displayed

1. On the Search Center site home page, click the **Settings** menu, and then click **Edit Page**.
2. In the Web Part, click the **Search Box Web Part Menu** arrow, and then click **Edit Web Part**.
3. In the **Search Box** tool pane, under **Properties for Search Box**, expand **Which search results page should queries be sent to**.

- To use the settings that are defined on the **Search Settings** page, select the **Use this site's Search Settings** check box.
- To override the settings that are defined on the **Search Settings** page, clear the **Use this site's Search Settings** check box.
- To show search results in a Web Part on the page, in the section **Send queries to other Web Parts on this page**, select a Web Part.

> **NOTE**
>
> If there are no other Web Parts on a page, search results will be sent to the search results page that is specified on the **Search Settings** page.

- To send queries to a different search results page, select **Send queries to a custom results page URL**, and then type the URL of the custom search results page.

> **NOTE**
>
> You can't send queries to a custom search results page that uses a friendly URL.

4. Click **OK**.

Change settings for query suggestions, people suggestions, and personal favorites results

Personal favorites results are suggestions based on search results that the user has clicked before. Query suggestions are turned on by default.

As a global or SharePoint admin in Microsoft 365, you can turn off or on query suggestions, people suggestions, and personal favorites results, or edit the different settings for query suggestions.

1. On the Search Center site home page, click the **Settings** menu, and then click **Edit Page**.
2. In the Web Part, click the **Search Box Web Part Menu** arrow, and then click **Edit Web Part**.
3. In the **Search Box** tool pane, under **Properties for Search Box**, expand the **Query Suggestions** section.

- To turn off query suggestions, clear the **Show suggestions** check box.
- To change how many query suggestions to show, type the maximum number in the **Number of query suggestions** box.
- To change how many characters the user must type before query suggestions are shown, edit the number in the **Minimum number of characters** box.
- To change how many milliseconds elapse before query suggestions are shown, edit the number in the **Suggestions delay (in milliseconds)** box.
- To change how many query suggestions are shown under the text **Are you looking for these again?** in the search results, change the value for **Number of personal favorites**: Personal favorite results are based on search results that the user has clicked before. To disable personal favorite results, clear **Show personal favorite results**.
- To turn on people name suggestions, select **Show people name suggestions**.

4. Click **OK**.

Show links or change the display template

1. On the Search Center site home page, click the **Settings** menu, and then click **Edit Page**.
2. In the Web Part, click the **Search Box Web Part Menu** arrow, and then click **Edit Web Part**.
3. In the **Search Box** tool pane, under **Properties for Search Box**, expand the **Settings** section:

- To show a link to a search preference page, select **Show preferences link**.
- To show a link to an advanced search page, select **Show advanced link**, and then in the **Advanced search page URL** box, type the URL of the advanced search page that you want to link to.
- To apply another display template, in the **Search box control Display Template** list, select the display template that you want to apply to the Web Part.
- Select the **Make the search box have focus when the page is loaded** check box so that users can immediately type a query in the search box when the page is loaded without first having to click the search box. This option is selected by default.

4. Click **OK**.

See also

[Manage the Search Center in SharePoint]

[Change settings for the Search Navigation Web Part]

Change settings for the Refinement Web Part

Change settings for the Search Results Web Part

Change settings for the Search Navigation Web Part

11/2/2020 • 4 minutes to read • Edit Online

The Search Navigation Web Parts shows links that let users move quickly between the different search pages, known as search verticals. Search verticals are predesigned to give users different search experiences depending on what they are looking for. For example, if users click the **People** link, they are taken to the people search vertical, which is a search page specifically set up to display people information.

By default, the Search Navigation Web Part is set up to show links to the search verticals **Everything**, **People**, **Conversations** and **Videos**. The Search Navigation Web Part uses search results from the Search Results Web Part so that when users click a search vertical link, the search results are filtered and displayed according to how the search vertical is set up.

As a global or SharePoint admin in Microsoft 365, you can change how the Search Navigation Web Part is set up by specifying a different Web Part to get the results from, change how many links to show, and change the appearance and layout of the Web Part. You make these changes by editing the properties in the Web Part tool pane.

To make other changes, such as changing display names for the links, or change their order, go to the **Search Settings** for the corresponding site. Here, you can also add a link to a new search vertical to be shown in the Web Part.

Change the settings for the Search Navigation Web Part

Here's how you can change the set-up of the Search Navigation Web Part. You can specify a different Web Part to get the results from, change how many links to show, and change the appearance and layout of the Web Part.

1. On the search results page, click the **Settings** menu, and then click **Edit Page**.
2. In the Search Navigation Web Part, click the **Search Navigation Web Part** menu arrow, and then click **Edit Web Part**.
3. In the Web Part tool pane, in the **Control** section:

- To receive search results from another Web Part on the page, in the **Use Current Query from** list, select a Web Part.
- To change the number of search vertical links to display before overflowing, in the **Maximum Links Before Overflow** box, type a number.

4. To change how the Web Part looks, edit the settings in the **Appearance** and **Layout** sections.
5. Click **OK**.

Change the display name or the URL of a search vertical

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Search** section, click **Search Settings**.
3. On the **Search Settings** page, in the **Configure Search Navigation** section, click to select the search

vertical that you want to change, and then click **Edit**.

4. In the **Navigation Link** dialog:

- To change the display name of a search vertical, in the **Title** field, type a display name.
- To change the URL of the search vertical, in the **URL** field, type a URL.

> **NOTE**
>
> You can't use a page that uses a friendly URL for your search vertical.

5. Click **OK**.

Change the order of the search vertical links

1. On the site, select **Settings** ⚙, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Search** section, click **Search Settings**.
3. On the **Search Settings** page, in the **Configure Search Navigation** section, click to select a search vertical.
4. Click **Move Up** or **Move Down** to change the display order.
5. Click **OK**.

Add a search vertical to the Search Navigation Web Part

As a global or SharePoint admin in Microsoft 365, you can create a new search vertical page and add it to the Search Navigation Web Part. When you create a new page, we recommend that you copy one of the existing search vertical pages — for example, **results.aspx**, and then modify the copy to create a new page.

Here's how you can add a link to the new search vertical page in the Web Part:

1. On the site, select **Settings** ⚙, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Search** section, click **Search Settings**.
3. On the **Search Settings** page, in the **Configure Search Navigation** section, click **Add Link**.
4. In the **Navigation Link** dialog:

- In the **Title** field, type a display name.
- In the **URL** field, type the URL of the new search vertical.
- Click **OK** to save the new search vertical.

5. To change the display order, use the **Move Up** or **Move Down** buttons.
6. Click **OK**.

See also

[Manage the Search Center in SharePoint]

[Change settings for the Search Box Web Part]

Change settings for the Refinement Web Part

Change settings for the Search Results Web Part

Change settings for the Refinement Web Part

11/2/2020 • 3 minutes to read • Edit Online

The Refinement Web Part filters search results into categories called refiners. Users can click these refiners to narrow search results to find what they're looking for more easily.

By default, the Refinement Web Part is used on all default search vertical pages in the Enterprise Search Center, which are the search results pages for **Everything**, **People**, **Conversations**, and **Videos**.

As a global or SharePoint admin in Microsoft 365, you can change how the Refinement Web Part is set up. You can:

- Filter search results from a different Search Results Web Part.
- Specify which refiners to show.

> **NOTE**
> Any managed properties that you want to use as refiners must be set to refinable and queryable in the search schema. Also, the content source that contains the managed properties must have been crawled before the properties can be used as refiners.

- Change the display template for a refiner.
- Change display names for refiners.
- Add counts to refiners.

Change how the Refinement Web Part behaves and looks

1. On the page that contains the Refinement Web Part, on the **Settings** menu, click **Edit Page**.
2. In the Web Part, click the **Refinement Web Part Menu** arrow, and then click **Edit Web Part**.
3. In the Web Part tool pane, in the **Refinement Target** section, select the Web Part that you want to filter search results from. By default, the Search Results Web Part is selected.
4. In the Web Part tool pane, verify that the **Choose Refiners in this Web Part** is selected.
5. Click **Choose Refiners**.
6. On the **Refinement configuration** page, from the **Available refiners** section, use the buttons to choose which refiners to show in the Web Part, and also in what order to show them. If you have specified an **Alias** for a refinable managed property, this alias is shown in the **Configuration for** section.
7. In the **Configuration for** section, choose how you want each refiner to look.

> **NOTE**
> If you've a single language site, you can change the refiner display name in the **Display name** section. For multilingual sites, change the refiner display language as described under Change the display name for a refiner.

8. Click **OK**.

Change the display name for a refiner in the classic search experience

By default, the name of the managed property will be used as a display name for the refiner. In many cases, the managed property name is hard to understand—for example, **RefinableString00** or **ColorOWSTEXT**. You can fix this by changing the name of the refiner in a JavaScript file.

1. On the page that contains the Refinement Web Part, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Web Designer Galleries** section, click **Master pages and page layouts**.
3. On the **Master Page Gallery** page, click **Display Templates**.
4. On the **Display Templates** page, click **Language Files**.
5. On the **Language Files** page, click the folder for the relevant language.
6. Open the **CustomStrings.js** file.
7. Add one line for each managed property that you want to change the display name for. Use this syntax:

   ```
   "rf_RefinementTitle_ManagedPropertyName": "Sample Refinement Title for ManagedPropertyName"
   ```

   For example, add this line to change the display name for the managed property **RefinableInt00** to **Price**:

   ```
   "rf_RefinementTitle_RefinableInt00": "Price"
   ```

8. Save the file.

Add refiner counts

By default, the Refinement Web Part doesn't show refiner counts — that is, the number of results for each refiner value. For example, if you've enabled the managed property Color as a refiner, the refiner values will be colors, such as Red, Green, and Blue. You can add refiner counts by changing a value in an HTML file so that the refiner values are shown as Red (10), Green (12), and Blue (8).

1. On the page that contains the Refinement Web Part, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Web Designer Galleries** section, click **Master pages and page layouts**.
3. On the **Master Page Gallery** page, click **Display Templates**.
4. On the **Display Templates** page, click **Filters**.
5. Open the **Filter_Default.html** file.
6. Change the value for **ShowCounts** to **true**.
7. Save the file.

See also

Manage the Search Center in SharePoint

Change settings for the Search Box Web Part

Change settings for the Search Navigation Web Part

Change settings for the Search Results Web Part

Change how search results look by using result types and display templates

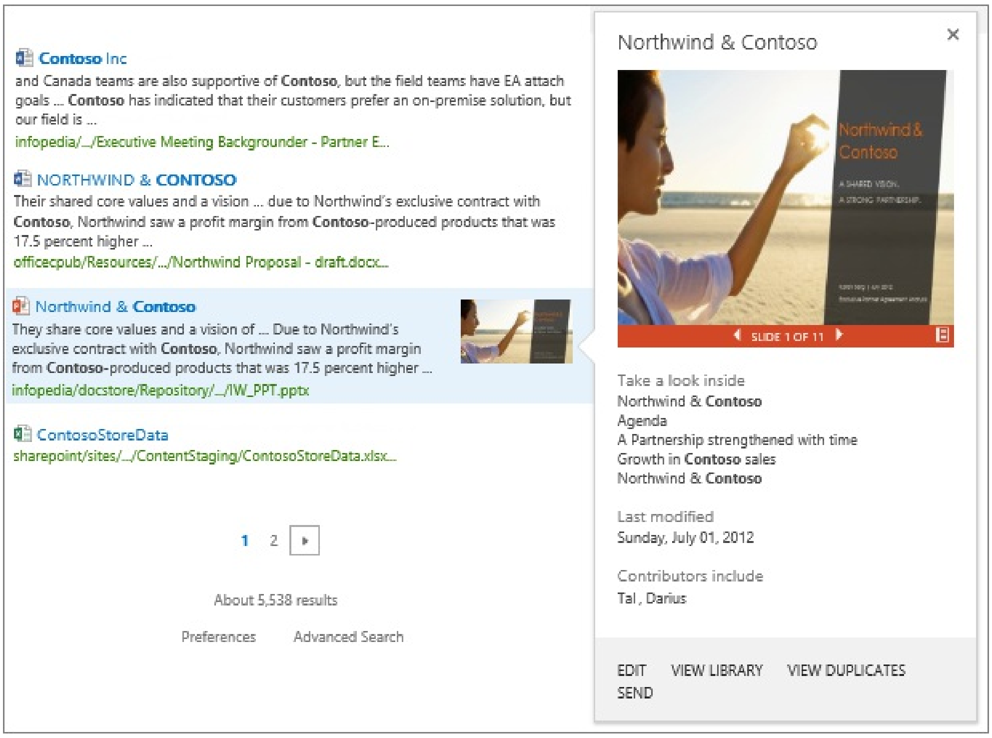
11/2/2020 • 3 minutes to read • Edit Online

To help users quickly distinguish between different types of results when they search for something in the classic search experience, we use *result types* and *display templates*. Important information is shown directly in the search results, so that users don't have to click on each result to see if they've found what they're looking for.

By default, the Search Results Web Part in your Search Center is set up to use different display templates according to the result type of the search result. Result types define when to use which display template, and the *display template* defines what information to show in the search results.

For example, there's a display template for PowerPoint files and another display template for Word documents. A result type says that if the search term is found in a PowerPoint file, then use the PowerPoint display template when showing that result. The users can see right away that this result is a PowerPoint file, and they can also see other information that helps them see whether this result is what they're looking for. When users hover over the result, they'll see a preview of the PowerPoint in the hover panel, together with more details about it. The hover panel also lets users perform *actions,* such as **Edit** or **Send**. The same way, the result type for Word documents uses a Word display template to show information.

Results look different based on result type and display template. This picture shows item display templates for Word, PowerPoint and Excel on the left side, and a hover panel display template for PowerPoint on the right side.



Types of display templates used in the Search Results Web Part

The default Search Center on your site consists of different Web Parts: a Search Box Web Part, a Search Results Web Part, a Search Navigation Web Part, and a Refinement Web Part. The actual search results are shown in the **Search Results Web Part**, All these Web Parts can also be added to any of your site's pages.

For the Search Results Web Part, there are three main types of display templates you should know about, Control display templates, Item result templates, and Hover panel templates.

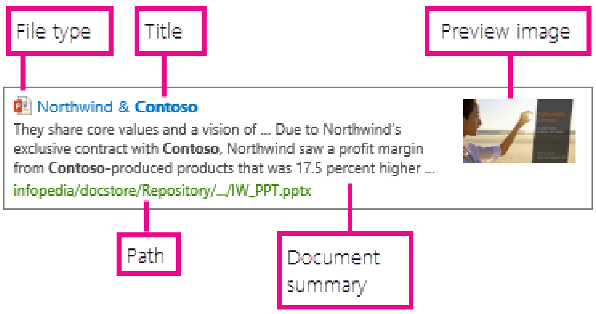
The *Control display template* decides the overall structure of how the results are presented. It contains the things "around" the individual results, such as a heading, numbering, next and previous page buttons, and a "no results found" message.

An *Item display template* defines how each result is displayed. It defines the managed properties you want to show and how they're displayed. You can have different item display templates for different result types.

The *Hover panel display template* typically shows a preview of the item or document when the users hover over the search result. The hover panel display template also contains actions such as **Edit** or **Send**, and other information about the search result.

How display templates show information about search results

The search results contain information that'll help users identify whether the result is what they're looking for. The display templates show this information by surfacing *managed properties* . Managed properties are content and metadata stored in the search index, for example the author and the title of a document. The display templates show a selection of the managed properties in the search results, such as file type, title, document summary, path, and image.



You can create your own display templates that show information that's important to your users, for specific types of results.

- For more information about managed properties, see Manage the search schema in SharePoint.
- For information about the Search Center and how to set it up, see Manage the Search Center in

SharePoint.

- For a full list of available display templates, see **Display templates for the Search Results Web Part** in Display template reference in SharePoint Server 2013.

About display templates in the Content Search Web Part and other search-driven Web Parts

11/2/2020 • 2 minutes to read • Edit Online

The Content Search Web Part and the other search-driven Web Parts use display templates to control how the search results appear in the Web Part. By using display templates, you can control the ways in which search results appear and behave in search-driven Web Parts.

Display templates are HTML files that specify which managed properties from the search result to display, and also how these properties should be displayed. For example, a display template could specify that the managed property PublishingImage displays a 100x100 pixel picture, and the managed property Title appears in bold to the left of the image. You can use any of the pre-configured display templates, or create your own.

The different search-driven Web Parts have different default display template settings that are optimized for the intended use of that Web Part. For example, by default, the Content Search Web Part displays a list of items where each item has a picture on the left side and three lines of text on the right.

To change display template settings

1. In the **Control** list, select a display template to control the organization and layout of your search results and the overall look of the Web Part.

2. In the **Item** list, select a display template for the individual items that are displayed in the search results within the Web Part.

3. Select the **Don't show anything when there are no results** check box if you don't want to display the Web Part at all if there are no search results returned by the query in that Web Part.

   If you clear the check box, the Web Part is displayed even if there are no search results, and the Web Part will show the "No results" message in the selected Control display template.

To change which managed properties are displayed in the fields in the Item Display Template

By default, display templates have a set of property mappings in them that were defined when the display template was created. However, you can override these settings in a particular Content Search Web Part.

1. Under **Property Mappings**, select the check box **Change the mapping of managed properties for the fields in the Item Display Template**.

2. In the different lists below the check box, enter the managed property to use for that field in the Item Display Template.

   If you enter multiple managed property names in a list, separate the managed properties by using semicolon. When displaying content, SharePoint will use the first property that is not empty.

For more information, see:

- About search criteria for the Content Search Web Part and other search-driven Web Parts

Make pages load faster with caching in the Content Search Web Part

11/2/2020 • 7 minutes to read • Edit Online

Configure a Content Search Web Part in SharePoint (CSWP) offers a lot of flexibility for configuring the query it contains. However, if you configure the Web Part to use a very complex query, or if you have many CSWPs on a page, the page can take longer time to load. To make the page load faster, you can configure the CSWP to cache search results for users who belong to the same AD security groups. Because it's faster to look up search results in the cache than in the search index, the page loads faster.

When you have configured a CSWP to use caching, it will first look in the cache for existing search results that match the query and the AD security group. If it doesn't find any search results in the cache, it will look in the search index.

We recommend that you use caching only in CSWPs that are on pages that have more than 10 page loads per 15 minutes, for example on popular home pages or on category pages that are starting points for navigating to more detailed catalog pages.

> **TIP**
>
> See Configure a Content Search Web Part in SharePoint for other things you can do to make pages load faster.

Configure a Content Search Web Part (CSWP) to use caching

1. Make sure that you're a member of the Designers SharePoint group on the site that contains the CSWP.
2. Go to the page that contains the CSWP.
3. From **Settings**, select **Edit Page**.
4. Select the CSWP that you want to configure.
5. In the Web Part tool pane, in the **Properties** section, in the **Search Criteria** section, select **Change query**.
6. Go to the **SETTINGS** tab.
7. In the **Caching** section, select **Group: Everyone except external users**, or select **Group:** and then enter the name of the AD security group you want to use.

   > **NOTE**
   >
   > To test that the CSWP returns the expected results, you have to be member of the AD security group that you select.

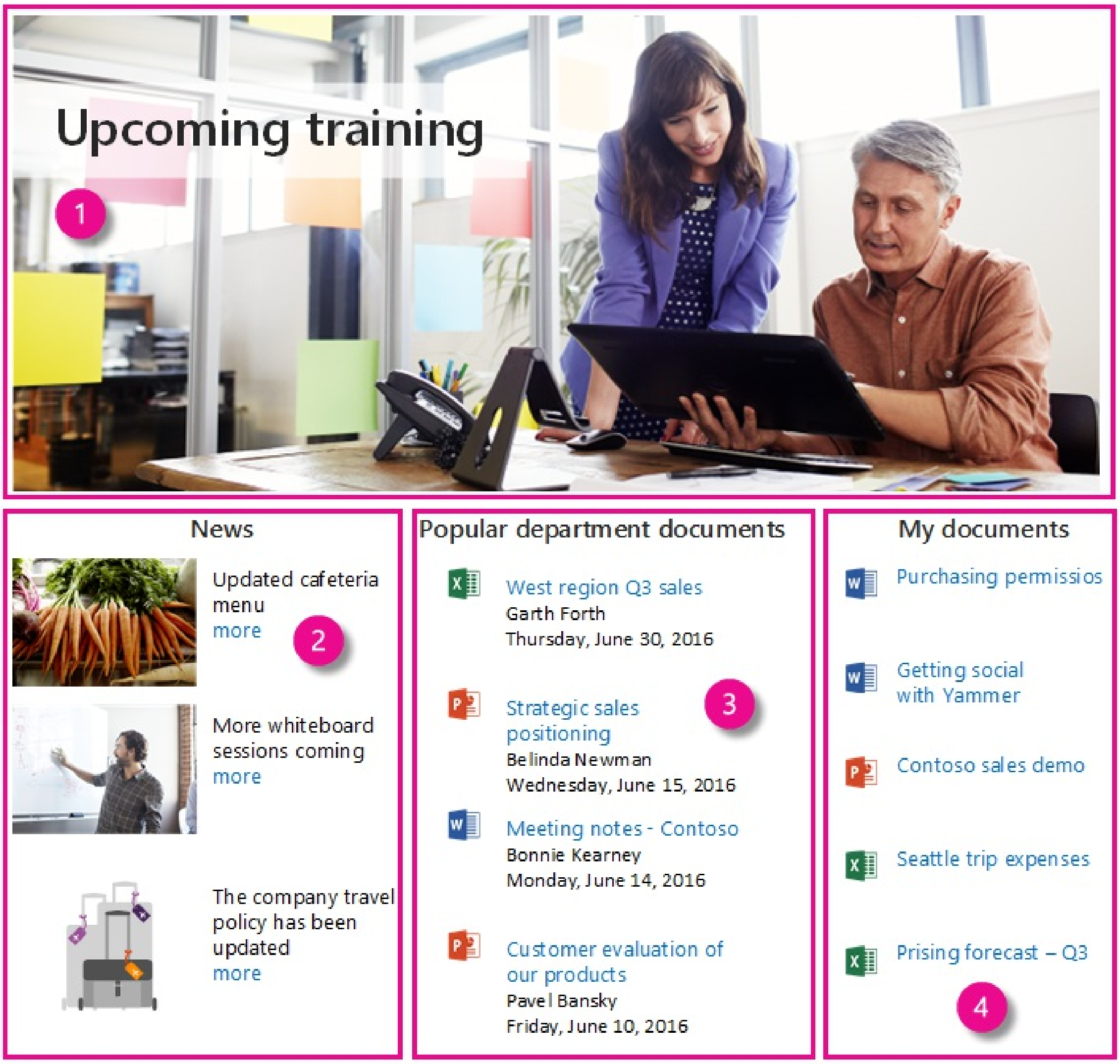
> **TIP**
>
> You can't look up the name of your AD security groups from the CSWP. To look up your AD security groups, go to your Azure classic portal. For more information, see Managing groups in Azure Active Directory

When should I use caching?

Before you change all your Content Search Web Parts (CSWP) to use caching, you should consider the characteristics of the page where the CSWPs are used:

- **What type of page is the CSWP on?** Caching works great in CSWPs that are on home pages or pages that many users have as a starting point when they browse for information. CSWPs on category pages that are starting points for navigating to more detailed catalog pages, can also benefit from caching.
- **How many page loads does the page have?** We recommend that you use caching only in CSWPs that are on pages with more than 10 page loads per 15 minutes.
- **Is the CSWP configured to show different results to different users?** If the CSWP query involves too many user groups, the search result combinations can overload the cache, and the page load time will not be reduced, or may even increase.

The example below shows an intranet page with four CSWPs. On average, the page has 38 page loads per 15 minutes. These page characteristics suggest that the page can load faster if you configure some of the CSWPs to use caching.



Let's look at the individual CSWPs:

- CSWP 1 shows a featured company news story, in this case a news story about upcoming training.
- CSWP 2 shows other company news stories.
- CSWP 3 shows popular documents in your department.

- CSWP 4 shows the documents you have been working on recently.

The queries in **CSWP 1 and 2** are configured to **show the same results to all users**. That means you can probably make the page load faster by configuring these two CSWPs to use caching.

The queries in **CSWP 3 and 4** are configured to **show different results to different users**.

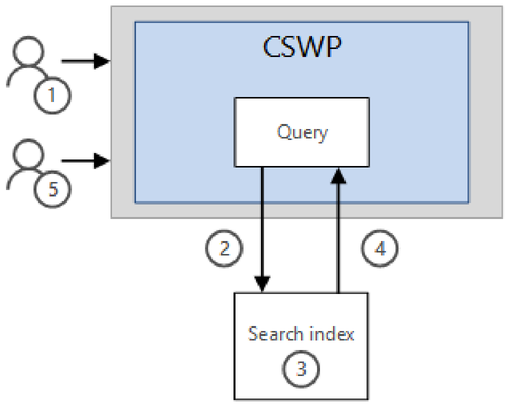
CSWP 3 shows one set of results to people who work in the HR department, and another set of results to people who work in the Sales department. In most cases, you can make the page load faster by using caching in this Web Part. However, if you have many small departments with only a few employees in each department, the number of search results that'll be stored in the cache could overload the cache and actually increase the page load time.

CSWP 4 shows which documents the logged-in user has worked on recently. You should not use caching in this Web Part. Because the query is tailored to each user, all individual search results will be stored in the cache. This will overload the cache and might increase the page load time.

How does caching make web pages load faster?

First, let's look at how search results are displayed in a Content Search Web Part (CSWP) **without** caching:

1. A user goes to a page that has a CSWP.
2. The query in the CSWP is sent to the search index.
3. Search finds results in the search index, and removes any search results that the users in the assigned AD security group are not allowed to see.
4. The search results are sent from the search index to the CSWP, where the user sees the results.
5. A second user goes to the same page, and steps 2 - 4 are repeated.



Now let's look at how results are displayed in a Content Search Web Part (CSWP) **with** caching:

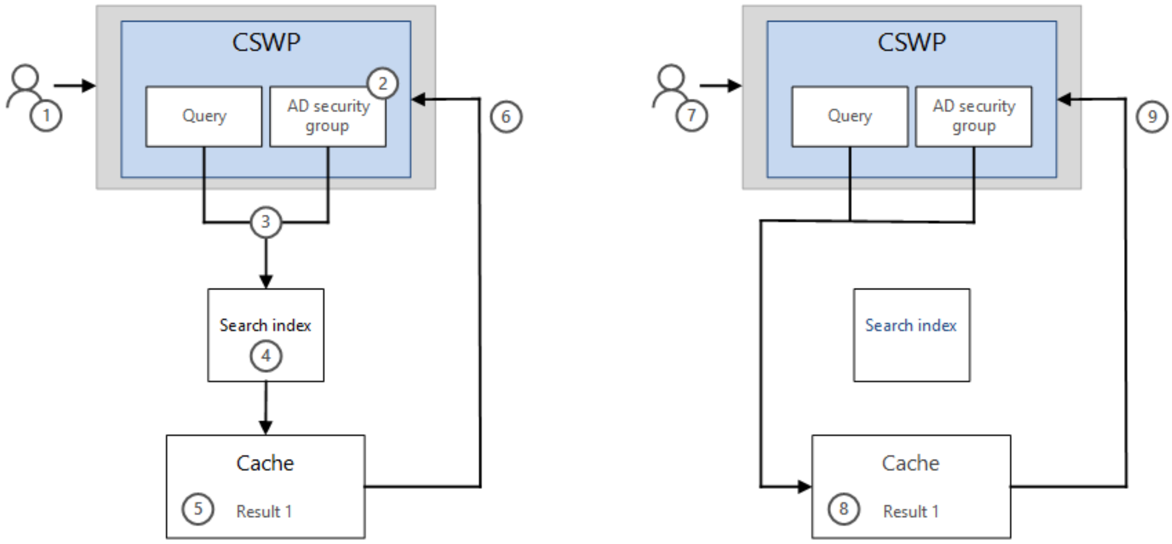
1. A user goes to a page that has a CSWP.
2. An AD security group, for example **Everyone except external users**, is assigned in the CSWP. This example assumes that the user who visits the page belongs to the assigned AD security group.
3. The query and the assigned AD security group in the CSWP is combined, and search first looks for a matching query and security group in the cache. If it doesn't find any matching results in the cache, the query is sent to the search index.
4. Search finds results in the search index, and removes any results that the users in the assigned AD security group are not allowed to see.
5. The search result is sent from the search index to the cache where it is stored (Result 1).

6. The search result is served from the cache to the CSWP, where the user sees the result.

7. A second user goes to the same page. The second user belongs to the same AD security group as the first user.

8. Search finds existing search results for the combination of the query and the AD security group in the cache.

9. The search result is served from the cache to the CSWP where the users sees the result.



Because it's quicker to look up search results in the cache than in the search index, the page loads faster.

> **IMPORTANT**
>
> The cache expires after 15 minutes. It's repopulated by the first user that goes to the page after the cache has expired, so page load time might be longer for the first user that repopulates the cache after an expiration.

Troubleshooting: newly added content does not show up in CSWP results

The Content Search Web Part (CSWP) shows search results from content that has been crawled and added to the search index. When you configure the CSWP to use caching, it shows matching results from the cache, and not from the search index. Search results, **also empty search results**, are stored in the cache for a maximum of 15 minutes before the cache expires.

If you search for newly added content before the content has been crawled and included in the search index, the cache will contain an **empty search result** for the query until the cache expires, and the content will not show up in the CSWP results.

If newly added content does not show up in the CSWP:

1. Make sure that the content has been crawled and added to the search index. Search for the content in a search box, or in a CSWP that does not use caching, until you can find the content.

2. Wait for at least 15 minutes to let the CSWP cache expire, and try again.

3. If you still don't see any results, check that you're a member of the AD security group that has been assigned to the CSWP. If you're not a member of the AD security group, you will not see any search results.

NOTE

SharePoint automatically crawls and adds new content to the search index at scheduled intervals, but you can also manually request crawling and re-indexing of a site, a library or a list.

Switch from an Enterprise Search Center to Basic in SharePoint

11/2/2020 • 2 minutes to read • Edit Online

> **IMPORTANT**
> This feature is gradually rolling out and might not be available yet for your organization.

The Basic Search Center is a classic search experience. To offer your users a richer search experience, you can either switch from a Basic Search Center to an Enterprise Search Center or rely on the modern search experience that SharePoint comes with. Learn about differences between classic and modern search and when to choose which search experience for your organization.

If you are currently using the Enterprise Search Center, you can easily replace (swap) it with the Basic Search Center if needed. This will result in your users seeing the classic search experience in their default search home page and default search results page. You can use the Invoke-SPOSiteSwap PowerShell cmdlet to do this.

How to use Invoke-SPOSiteSwap to swap your Search Center sites

1. Download the latest SharePoint Online Management Shell.

   > **NOTE**
   > If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
   > On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the Invoke-SPOSiteSwap cmdlet.

```
Invoke-SPOSiteSwap
  -SourceUrl <string>
  -TargetUrl <string>
  -ArchiveUrl <string>
```

PARAMATER	DESCRIPTION
-SourceUrl	The site you want to promote.
-TargetUrl	The site you want to replace.
-ArchiveUrl	URL that the target site will be archived to.

Here's an example of how to use these parameters when swapping an existing Enterprise Search Center to Basic:

- **For your -SourceUrl**, you need the URL of your Basic Search Center site. The site must exist before running the cmdlet. For our example, we'll use https://contoso.sharepoint.com/sites/SiteSearch.

  You can create a Basic Search Center site from an Enterprise site template.

- **For your -TargetUrl**, you need the URL of your Enterprise Search Center site that you want to replace. For our example, we'll use https://contoso.sharepoint.com/search.

- **For your -ArchiveUrl**, use a Url that does not currently exist at the location. Your Enterprise Search Center site will be archived to this site location. For our example, we'll use https://contoso.sharepoint.com/sites/ArchivedEntSearch.

Here's how to use the examples above in the Invoke-SPOSiteSwap cmdlet:

```
Invoke-SPOSiteSwap -SourceUrl https://contoso.sharepoint.com/sites/SearchSite -TargetUrl
https://contoso.sharepoint.com/search -ArchiveUrl https://contoso.sharepoint.com/sites/ArchivedEntSearch
```

Successfully running the cmdlet above would result in:

- Basic Search will be the default Search Center experience. When users go to https://contoso.sharepoint.com/search, they will now be using the Basic Search Center.
- The Enterprise Search Center site will no longer be available as the default Search Center experience.

See also

Manage the Search Center in SharePoint

Show the right search results

11/2/2020 • 2 minutes to read • Edit Online

All search results are not relevant to everyone all the time. Learn how you can help users find exactly the results they're looking for in SharePoint. SharePoint has both a classic and a modern search experience, learn about the differences between the classic and modern search experiences in SharePoint.

Manage the search schema

The search schema controls what users can search for, how they can search it, and how the results get presented on your search websites. In the search schema, you can view, create, or change managed properties, and map crawled properties to managed properties. Learn about the search schema.

Manage query rules

Query rules apply to the classic search experience. They consist of conditions and associated actions. When a query meets the conditions in a query rule, the search system performs the actions specified in the rule. Query rules can be used to promote results to the top of the result list.Learn about managing query rules.

Manage query suggestions

Query suggestions are words that appear below the search box as a user types a query. SharePoint automatically creates a query suggestion when you've clicked a search result for a query at least six times. In the classic search experience you can also import your own lists of query suggestions to SharePoint. Learn about managing query suggestions.

Using query transforms

Query transforms apply to the classic search experience. You can configure a query transform to replace properties of a query, such as the result source that the query will use to get search results, or the sort order that it will use when it displays search results. Read Understanding query transforms to learn more.

Manage result sources

Result sources limit searches to certain content, or to a subset of search results. You can also use result sources to send queries to external providers such as Bing. Learn about managing result sources

Manage result types

Results types apply to the classic search experience. A result type specifies one or more conditions to compare search results against, and an action to take if a search result meets those conditions. The action specifies the display template to use for the search result. Learn about managing result types.

Manage search dictionaries

Search dictionaries apply to the classic search experience. You can use search dictionaries to include or exclude words for query spelling correction, and you can include or exclude company names to be extracted from the content of indexed documents. Learn about managing search dictionaries.

Manage authoritative pages

You can influence the pages or documents that should appear at the top of your list of search results by identifying authoritative pages - high-quality pages that link to the most relevant information. Authoritative pages apply to the classic search experience. Learn about managing authoritative pages.

Export and import search settings

You can export and import customized search configuration settings between tenants, site collections, and sites. The settings include all customized query rules, result sources, result types, ranking models and site search settings. Learn about exporting and importing search settings.

Manage the search schema in SharePoint

11/2/2020 • 21 minutes to read • Edit Online

The search schema controls what users can search for, how users can search it, and how you can present the results on your search websites. By changing the search schema, you can customize the search experience in SharePoint in Microsoft 365.

About the search schema

When a user searches for content on SharePoint sites, search only finds what's in the **search index**, and only shows results that the user has permission to see.

Search discovers information by crawling items on your site. The discovered content and metadata are called **properties** of the item. The **search schema** has a list of **crawled properties** that helps the crawler decide what content and metadata to extract.

Not all crawled content or metadata is useful to have in the search index, so the search schema has a list of useful types of content and metadata, called **managed properties**. The index only includes content and metadata from the managed properties. Examples of useful metadata for the index are the author and the title of a document.

Search comes with relevant crawled properties mapped to managed properties. For example, crawled properties related to author map to a managed property related to author. If you add a managed property, you must map it to a crawled property to get content into the index. After the site, library, or list has been crawled, users can search for the content and metadata of new, or changed managed properties. See Introducing Search Schema for SharePoint for more info.

> **NOTE**
> Numeric data in Microsoft Excel files isn't indexed. For example, the number "123456789" isn't indexed, but the string "PO123456789" is indexed.

Managed properties and search

Each managed property has settings that determine how users can search for the content of that managed property, and how the content can be shown in the search results.

You can create new, **custom** managed properties, but these can only contain text or Yes/No. If you need other content types in your custom managed property, then use one of the unused, **built-in** managed properties that search comes with. These managed properties can contain information in integer, decimal, date and time, double precision float, or binary format. You can "rename" these unused managed properties by using the alias setting.

For the built-in managed properties, you can change their mappings to crawled properties, but the only setting you can change is the alias.

Define which content that users can search and get results for

If you set a managed property to be **searchable**, the content is added to the index. This means that a simple query for "Smith" returns items that contain the word "Smith" and also items whose "author" property contains "Smith". If you want users to be able to "only search for items that have this specific author", set the author property to be **queryable**. Then, to find only items that have an author named Smith, users can query for "author:Smith".

If you want to prevent the content in a managed property from showing up as search results, you can disable the **retrievable** setting for the managed property.

If you don't want anonymous users to see the information in a managed property, for example who has authored an item, disable the "Safe for Anonymous" setting for the managed property.

Get better search results when you have multi-lingual content and metadata with special characters

When search indexes content or when it processes queries, it breaks a stream of text into smaller parts such as words, phrases, symbols, or other meaningful elements. These parts are called tokens. When users enter a query, search tries to find tokens in the index that match the tokens of the query.

For most languages, search changes text to lower-case, removes diacritics, replaces special characters, such as punctuation, with white space, and then breaks on white spaces.

Breaking on white spaces works fine for a language like English, but not so well for East Asian languages. Let's say you have a document library that contains product datasheets both in English and Chinese. Each datasheet has a product identifier with non-alphanumerical characters, such as "11.132-84-115#4". When search processes the datasheet, it **detects** its language, and tokenizes everything in it according to that language. So, the product identifier in a Chinese data sheet is tokenized as if it was Chinese text, and in an English data sheet the product identifier is tokenized as if it was English text. When users search for a product identifier, search tokenizes their query according to the language setting of the SharePoint site they're on. If the site is set to English, and the user searches for a product identifier that was tokenized as Chinese text, the tokens might not match, and the users get no results.

Here's how you can make results better for users: When search crawls the datasheet, it extracts the product identifier. Map the crawled property for the product identifier to a new managed property, "ProductID". Enable **language neutral tokenization** for the "ProductID" managed property, and instruct users to search for product identifiers against the "ProductID" managed property, like this: *ProductID:"11.132-8"*. Because you've enabled language neutral tokenization for "ProductID", search uses language neutral tokenization for the query and can find matching results for the query.

Get better search results when you have metadata with special characters

To help users get better search results when they search in managed properties that contain metadata with non-alphanumeric characters, you can enable the **finer tokenization** setting for the managed property.

Let's look at the example with a product datasheet library again.

Users who prefer to quickly enter a query and then browse the results to find the datasheet they're looking for, typically enter queries like ProductID:"132-884". Because search breaks content for the **search index** into smaller parts than it does for **queries**, search might not find matches for these queries. When the query is tokenized finer, it's more likely that there are matches between the tokens in the search index and in the query. Users can also query for the middle or last part of the product identifier.

Users who search for a datasheet and expect to only get results that match the full product identifier, typically write queries like *ProductID:"11.132-884-115#4"*. Finer query tokenization doesn't make a difference for such queries.

Determine which title to show in results

A single crawled property can be mapped to multiple managed properties. Or, multiple crawled properties can be mapped to a single managed property, for example both the "Writer" and "Author" crawled properties can be mapped to the "Author" managed property.

For example, a document in a library can have a SharePoint title, a title in the file metadata, and the content can have a title formatted with the style "Title". All these are mapped to the "Title" managed property. It's the title from the crawled property that's highest on the mapping list and that has a value that's included in the index.

Auto-generated managed properties

Some managed properties are generated automatically. One example is when you add a site column to a SharePoint library or list. When search crawls that list it automatically generates a crawled and a managed property for the site column, and a mapping between them. Another example is when crawling finds metadata in a document you've uploaded to SharePoint. If there isn't already a mapping to a managed property for that metadata, such as 'Title', search auto-generates a managed property. The type of crawled property determines the settings of the auto-generated managed property.

The search schema displays the name of auto-generated managed properties and their mappings to crawled properties in grey in the search schema. The search schema doesn't hold the settings of the managed auto-generated managed properties. The settings exist, but they're hidden from the search schema. You can add mappings to other managed properties for the crawled properties, but if you change any other setting, you override the other (hidden) settings and the auto-generated managed property is converted to a regular managed property. If you decide to **change** an auto-generated managed property, review **all** the settings carefully, just as you would when you create a new property manually.

> **IMPORTANT**
>
> Auto-generated managed properties are case-sensitive. When accessing auto-generated managed properties, such as through a REST query, verify the casing is correct. If the casing is incorrect, no value will be returned.

Refine on managed properties

If you want to use a managed property as a refiner on the search results page, use the setting **refinable**. This setting is only available on the built-in managed properties, and only affects the classic search experience. If you need to use a new managed property, or an auto-generated managed property, as a refiner, rename an existing, unused managed property (that's refinable) by using an alias. There are quite a few managed properties available for this purpose. They have names such as "RefinableString00" and "RefinableDate19."

For example, you create a new site column called "NewColors", and you want users to be able to use "NewColors" as an option when they refine on the search results. In the search schema, you choose an unused managed property, for example "RefinableString00", and rename the property to "NewColors" by using the Alias setting. Then, you map this new managed property to the relevant crawled property.

Change the search schema on tenant level or on site collection level

Usually, you don't have to change the default search schema for the tenant unless you want to create a more advanced or customized search experience.

You can change the search schema for the whole tenant or for a specific site collection only. The search schema for the site collection is based on the search schema for the tenant, so typically, you would make changes on the tenant level first, and then on the site collection level. Any changes you make on a site collection, only apply to that site collection.

Crawling and re-indexing

When you change managed properties or add new ones, the changes take effect only after the content has been re-crawled. In SharePoint in Microsoft 365, crawling happens automatically based on the defined crawl schedule.

When you have added a new property to a list or to a library, or when you have changed properties that are used in a list or library, search has to re-crawl the content before your changes will be reflected in the search index. Because your changes are made in the search schema, and not to the actual site, the search will not automatically re-crawl the list or the library. To make sure that your changes are crawled, you can specifically request a re-indexing of the list or library. When you do this, the list or library content will be re-crawled so that you can start using your new managed properties in queries, query rules and display templates.

Managed properties and Delve

Delve uses managed properties to query the Office graph and to display content cards in Delve. For example, you can see managed properties like Author, Filename, ModifiedBy and LastModifiedTime on the Delve content cards.

Any document that a user can view or edit in Microsoft 365, can also appear in Delve. Delve doesn't change any permissions and users will only see documents they already have access to. Sometimes, though, you may want to prevent a document from appearing in Delve.

You can use the HideFromDelve managed property to hide a document from Delve. You can keep storing the document in Office 365, and people can still find it through search - it just won't show up in Delve anymore. See Hide documents from Delve.

For more info about Delve, see Office Delve for Office 365 admins

Create a new managed property

> **NOTE**
> Not all options are available in SharePoint in Microsoft 365. Refinable Managed Properties cannot be created. Instead use the existing Refinable Managed Properties, e.g. RefinableString00 or RefinableInt00. Searching "Refinable" will show all of the usable Refinable Managed Properties available.

In SharePoint in Microsoft 365, when you create a new managed property, it will have some limitations. For example, the property can only be of type **Text** or **Yes/No**, and it can't be refinable or sortable.

If you need a property of a different type, or one that has different characteristics than what is available, follow the steps under Create a managed property by renaming an existing one.

Go to the Search Schema page for the tenant

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings** ⚙, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. Select **Managed Properties**.

4. On the **Managed Properties** page, select **New Managed Property**.

5. In the **Name and description** section, in the **Property name** box, enter the name of the new managed property. Optionally, enter a description.

6. In the **Type** section, select one of the available options for the property:

- Yes/No.

- Text.

7. In the **Main characteristics** section, select one or several of the available options.

8. In the **Mappings to crawled properties** section, select **Add a mapping**.

9. In the **crawled property selection** dialog, select a crawled property to map to the managed property, and then select **OK**. If you want to map more crawled properties to the same managed property, repeat this step.

10. In the **Mappings to crawled properties** section, specify if you want to include:

- All content from all crawled properties mapped to this managed property.

- Content from the first crawled property that contains a value and, optionally, in which order.

11. Select **OK**.

Create a managed property by renaming an existing one

Go to the Search Schema page for the tenant

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. On the **Managed Properties** page, find an unused managed property. By unused, we mean that the property is not mapped to a crawled property: the **Mapped Crawled Properties** column is empty. See the Default unused managed properties table for more details.

   > **IMPORTANT**
   >
   > To be able to use the property as a refiner later, choose a managed property that is marked with **Refine**.

4. Point to the managed property, select the arrow, and then select **Edit/Map property**.

5. On the **Edit Managed Property** page, under **Main characteristics**, in the **Alias** section, in the **Alias** box, enter the new name for the property.

6. In the **Mappings to crawled properties** section, select **Add a mapping**.

7. On the **Crawled property selection** page, select a crawled property to map to the managed property, and then select **OK**. Repeat this step to map more crawled properties to this managed property.

8. Select **OK**.

> **IMPORTANT**
> When you have created a new managed property this way, the library or list that will use the refiner must be re-crawled and re-indexed before the property will appear as an option in the refinement configuration. See Request re-indexing of a document library or list.

View crawled properties and managed properties

Go to the Search Schema page for the tenant

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. On the **Managed Properties** tab, you see all the managed properties, the settings on the managed properties, and the crawled properties they are mapped to.

4. To view crawled properties and the managed properties they are mapped to, select **Crawled Properties**.

5. To view crawled property categories, select **Categories**.

Edit a managed property

> **NOTE**
> Not all options are available in SharePoint.

Go to the Search Schema page for the tenant

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. On the **Managed Properties** tab, in the **Property Name** column, find the managed property that you want to edit, or in the **Filter** box, enter the name.

4. Point to the managed property in the list, select the arrow, and then select **Edit/Map property**.

5. On the **Edit Managed Property** page, edit the settings, and then select **OK**.

Delete a managed property

Go to the Search Schema page for the tenant

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. On the **Managed Properties** tab, find the managed property that you want to delete, or in the **Filter** box, enter its name.

4. Point to the managed property that you want to delete, select the arrow, and then select **Delete**.

5. Select **OK**.

> **IMPORTANT**
>
> If you delete a managed property: > Users can't search on the property. > A query rule that uses the property no longer works. > A custom web part that uses the property no longer works.

Map a crawled property to a managed property

Go to the Search Schema page for the tenant

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. Choose **Crawled Properties**.

4. On the **Crawled Properties** page, find the crawled property that you want to map to a managed property, or under **Filters**, enter its name in the **Crawled properties** box.

5. Point to the crawled property that you want to map, select the arrow, and then select **Edit/Map property**.

6. On the **Edit Crawled Property** page, in the **Mappings to managed properties** section, select **Add a Mapping**.

7. In the **managed property selection** dialog, select a managed property to map to the crawled property, and then select **OK**. Repeat this step to map more managed properties to this crawled property.

8. In the **Include in full-text index** section, if you want to include the content of this crawled property in the full-text index, select the box.

9. Select **OK**.

View or edit crawled property categories

Go to the Search Schema page for the tenant

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has

admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Search Schema**.

Go to the Search Schema page for a site collection

1. On the site, select **Settings** ⚙, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. Under **Site Collection Administration**, select **Search Schema**.

3. Select **Categories**.

4. On the Categories page, find the crawled property category that you want to view or edit.

5. Do one of the following:

   - To view which crawled properties belong to a category, and which managed properties they are mapped to, click the crawled property category in the Categories page.

   - To edit a category, point to the crawled property category that you want to edit, click the arrow, and then click **Edit category**.

Default unused managed properties

The following table provides an overview of the default unused managed properties that you can reuse and rename using an Alias.

MANAGED PROPERTY TYPE	COUNT	MANAGED PROPERTY CHARACTERISTICS	MANAGED PROPERTY NAME RANGE
Date	10	Queryable	Date00 to Date09
Date	20	Multivalued, Queryable, Refinable, Sortable, Retrievable	RefinableDate00 to RefinableDate19
Date	2	Queryable, Refinable, Sortable, Retrievable	RefinableDateInvariant00 to RefinableDateInvariant01
Date	5	Queryable, Refinable, Sortable, Retrievable	RefinableDateSingle00 to RefinableDateSingle04
Decimal	10	Queryable	Decimal00 to Decimal09
Decimal	10	Multivalued, Queryable, Refinable, Sortable, Retrievable	RefinableDecimal00 to RefinableDecimal09

MANAGED PROPERTY TYPE	COUNT	MANAGED PROPERTY CHARACTERISTICS	MANAGED PROPERTY NAME RANGE
Double	10	Queryable	Double00 to Double09
Double	10	Multivalued, Queryable, Refinable, Sortable, Retrievable	RefinableDouble00 to RefinableDouble09
Integer	50	Queryable	Int00 to Int49
Integer	50	Multivalued, Queryable, Refinable, Sortable, Retrievable	RefinableInt00 to RefinableInt49
String	200	Multivalued, Queryable, Refinable, Sortable, Retrievable	RefinableString00 to RefinableString199

Hide documents from Delve

If you don't want a document to show up in Delve, you can create a HideFromDelve site column of the type **Yes/No**. This site column creates a new crawled property, ows_HideFromDelve, which is automatically mapped to the HideFromDelve managed property.

Add a site column to the library or list where the document is stored

1. Sign in as a site collection administrator, and go to the site where the document that you want to hide from Delve is stored.
2. On the ribbon, select the **List** or **Library** tab.
3. In the **Manage Views** group, select **Create Column**.
4. Under the **Name and Type** section, in the **Column name** box, enter HideFromDelve, and then select **Yes/No** (check box)*

   > **IMPORTANT**
   >
   > In the **Additional Column Settings** section, in the **Default value** dropdown, select **No**. If you select **Yes**, all new documents are hidden from Delve.

5. Do one of the following:

- For SharePoint 2016 or SharePoint in Microsoft 365, clear the **Add to all content types** check box.
- For SharePoint 2013, clear the **Add to default view** check box.

6. Select **OK**.

Mark the document you want to hide from Delve

1. Go to the site where the document that you want to hide from Delve is stored.
2. Find the document that you want to hide in the library or list, select **edit properties**, and then check **HideFromDelve**.
3. Select **OK**.

After the next scheduled crawl, or after you Request re-indexing of a document library or list, the document is hidden from Delve. If you want the document to show up in Delve again, uncheck the **HideFromDelve** column for the hidden document.

Request re-indexing of a document library or list

1. On your site, go to the list or library where you have added the new property, and select the title. The **Library** or **List** tabs appear.
2. On the ribbon, select the **Library** tab or the **List** tab.
3. Under the **Settings** section, select **Library settings** or **List settings**.
4. On the **Settings** page, under **General Settings**, select **Advanced settings**.
5. Scroll down to **Reindex Document Library** or **Reindex List**, and select the button. All of the content in the document library or list are re-indexed during the next scheduled crawl.

> **NOTE**
>
> This may cause a massive load on the search system, so be sure to re-index only after you've made all the changes you want to be re-indexed.

Related Topics

Overview of crawled and managed properties in SharePoint Server 2013

Overview of the search schema in SharePoint Server

Manually request crawling and re-indexing of a site

Manage query rules

1/8/2021 • 18 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can improve search results in the classic search experience by creating and managing query rules. Query rules help searches respond to the intent of users.

In a query rule, you specify conditions and associated actions. When a query meets the conditions in a query rule, the search system performs the actions specified in the rule to improve the relevance of the search results. This could be by narrowing results or changing the order in which results are displayed. For example, a query rule condition could be that a term in a query matches a particular term in a SharePoint term set, or that a query is frequently performed on a particular result source in a search system, such as videos. When the query rule condition is met, an associated action could be to show a specific item at the top of the search results. Say you have an intranet site where all company events are maintained in a library, and you want to promote a first-aid seminar. To do this, you create a query rule that boosts the first-aid seminar to the top of the search results when someone searches for "seminar" or "event."

A query rule can specify the following three types of actions:

- Promote a search result to appear above ranked results. For example, for the query "sick leave", a query rule could specify a particular result, such as a link to a site that has a statement of company policy regarding time off work.
- Add one or more groups of search results, called result blocks. For example, for a query that contains “Fabrikam sales report”, a query rule might use a taxonomy dictionary to recognize “Fabrikam” as a customer, and then display a result block with pertinent results about Fabrikam from your customer relationship management (CRM) system.
- Change the ranking of search results. For example, for a query that contains “download toolbox”, a query rule could recognize the word “download” as an action term and boost search results that point to a particular download site on your intranet.

You can create query rules at different levels: for the whole tenant, for a site collection, or for a site. When you create query rules at tenant level, the query rules can be used in all site collections. When you create query rules at site collection level, the rules can be used on all sites in the site collection. When you create query rules at site level, the rules can only be used on that site.

You can configure query rules for one or more result sources, and you can specify a time period for when the query rule is active.

SharePoint has both a classic and a modern search experience. Only query rules that return promoted results and that are defined for the default result source can affect the modern search experience. Query rules which do query re-writes are not supported for modern experiences. Users might see such promoted results on the **All** tab on the search results page when they search across all of SharePoint. Learn more about the differences between the classic and modern search experiences in SharePoint.

Promote a search result

You can add several individual promoted results. When there is more than one promoted result, you can specify the relative ranking.

1. Go to the **Manage Query Rules** page for the tenant, for a site collection, or a site:

- For a tenant, in the new SharePoint admin center, select **More features**. Under **Search**, select **Open**, and then on the search administration page, select **Manage Query Rules**.

- For a site collection, in your site collection, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Site Collection Administration**, select **Search Query Rules**.
- For a site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Search**, select **Query Rules**.

2. On the **Manage Query Rules** page, in the **Select a Result Source** list, select a result source for the new query rule.
3. Select **New Query Rule**.
4. On the **Add Query Rule** page, in the **General Information** section, in the **Rule name** field, type the name for the query rule.
5. Select to expand the **Context** section.
6. In the **Context** section, do one of the following:

- To apply the query rule to all result sources, select **All sources**.
- To apply the query rule to one or more specific result sources, select **One of these sources**. By default, the result source that you specified earlier is selected. To add a result source to the query rule, select **Add Source**, select a result source in the dialog, and then select **Save**.

7. To restrict the query rule to categories—for example, that a query rule should fire only when a term from your managed navigation term set is included in the query, do as follows:

- To restrict the query rule to a category, select **Add category**. In the **Import from term store** dialog, select a term which, when you include it in a query, will cause the query rule to fire, and then select **Save**.
- To restrict the query rule to a user segment, select **Add User Segment**. In the dialog, in the **Title** field, type the name for this rule, and then select **Add user segment term**. In the **Import from term store** dialog, select a term that represents a user segment that will cause the query rule to fire when it appears in a query. Select **Save**

8. In the **Query Conditions** section, do one of the following:

- Select one of the conditions listed in Overview of conditions that make a query rule fire.

  > **NOTE**
  >
  > The rule fires when any condition is true.

  To add more conditions, select **Add Alternate Condition**

- Select **Remove Condition** to configure this query rule to fire for every query that users type at the level at which you are creating the rule, and then go to the next step. For example, if you are creating this rule for a site collection, select **Remove Condition** if you want this rule to fire for every query that users type inside any search box in the site collection.

9. In the **Actions** section, specify the action to take when the query rule fires. Specify one of the following:

- To promote individual results so that they appear towards the top of search results, select **Add Promoted Result** (in SharePoint 2010 Products this was called Best Bets). In the dialog, in the **Title** field, type the name that you want to give this promoted result. In the **URL** field, type the URL of the result that should be promoted. Choose **Render the URL as a banner instead of as a hyperlink**. Select **Save**.

  You can add several individual promoted results. When there's more than one promoted result, specify the relative ranking.

- To promote a group of search results, select **Add Result Block**. For more information, see Create and display a result block a bit further down.
- To change ranked search results, select **Change ranked results by changing the query**. For more information, see Change ranked search results by changing the query a bit further down.

10. To make the query rule active during a particular time period, select **Publishing**, and then specify the period.
11. Select **Save**.

Create and display a result block

A result block contains a small subset of results that are related to a query in a particular way. Like individual results, you can promote a result block or rank it with other search results.

When you configure a query condition for a result block, you use *query variables*. Query variables are like placeholders for values that you don't yet know, when you specify the query. However, when the query's run, this information is available and the system uses it to send the query to the index. For example, {User.Name} stands for the display name of the user who typed in the query. Another one's {searchBoxQuery}, which stands for the query a user typed in a search box. When you use the Query Builder to configure the query, a list of query variables is shown. (See step 3 in the procedure right below.)

1. In step 9 of the procedure Create a query rule, on the **Add Query Rule** page, in the **Actions** section, click **Add Result Block**.
2. Enter the title that shall appear in the result block in the **Title** field in the **Block Title** section.
3. Configure the query that gives results for the block. In the **Query** section, click **Launch Query Builder** and on the **BASICS** tab do the following:

- Select which content to search by selecting a result source from the drop-down list in the **Select a query** section
- Specify your query. See Query variables in SharePoint Server 2013 for a list of available query variables. You can select pre-defined query variables from the **Keyword filter** drop-down list, and then add them to the Query text box by clicking **Add keyword filter**
- If relevant, use property filters to query the content of managed properties that are set to queryable in the search schema. You can select managed properties from the **Property filter** drop-down list. Click **Add property filter** to add the filter to the query.

> **NOTE**
>
> Custom managed properties are not shown in the **Property filter** list. To add a custom managed property to your query, in the **Query text** box, enter the name of your custom managed property followed by the query condition, for example *MyCustomColorProperty:Green*

4. Specify how the search results within your result block should be sorted. Sorting of search results is case sensitive. On the **SORTING** tab, in the **Sort by drop-down list**, select a managed property, and then select **Descending** or **Ascending**. The list only contains managed properties that are set as sortable in the search schema. You can also sort by rank. To add more sorting levels, click **Add sort level**.
5. If you chose to sort by rank, you can optionally:

- Select which model to use for ranking search results (this selection is optional). Use the **Ranking Model** drop-down list.

- Define rules for dynamically changing the ordering of results. In the **Dynamic ordering** section, define when to change ranking by selecting a condition from the drop-down list and then specifying whether to **promote** or **demote** the result. To add more rules, click **Add dynamic ordering rules**

6. Preview the final query that will be run by the Content Search Web Part, on the **TEST** tab. The preview is based on the original query template where dynamic variables are substituted with current values. Other changes to the query may have to be made as part of query rules. Click **Show more** to display additional information.

- The **Query text** shows the final query that'll be run by the Content Search Web Part. It's based on the original query template where dynamic variables are replaced with current values. You might end up making other changes to the query as part of query rules.

- The **Query template** box shows the content of the query template that is applied to the query.

- The **Query template variables** section shows the query variables that will be applied to the query, and the values of the variables that apply to the current page. You can type other values to test the effect they will have on the query. Click the **Test Query** button to preview the search results.

7. Click **OK** to close the **build your query** dialog.

8. Define which result source this result block should be applied to. Use the **Search this Source** drop-down list in the **Query** section

9. In the **Items** drop-down list, select how many results to show in the result block.

10. Click to expand the **Settings** section.

    The result block only displays the number of search results that you specified in the previous step. However, you can add a **Show more** link at the bottom of the result block that'll show all search results for the result block. To add a **Show more** link, select **"More" link goes to the following URL**, and then type a URL. You can use query variables in this URL—for example, .

11. Click **OK**.

Change ranked search results by changing the query

The ranking model calculates a ranking order of search results. You can change this ranking by promoting or demoting items within the search results. For example, for a query that contains "download toolbox", you can create a query rule that recognizes the word "download" as an action term. Once you've done this, you can change the ranked search results and this will promote the URL of a specific download site on your intranet.

You can also dynamically change the sorting order of the search results, based on several variables such as file name extension or specific keywords. When you change ranked search results by changing the query, you'll see that your results are security trimmed and refinable. Moreover, the search results don't show up if the document's no longer there.

1. In step 9 of the procedure Create a query rule, on the **Add Query Rule** page, in the **Actions** section, click **Change ranked results by changing the query**. The **build your query** dialog appears

2. On the **BASICS** tab, do the following:

- Select which content to search by selecting a result source from the drop-down list in the **Select a query** section

- Specify your query. See Query variables in SharePoint Server 2013 for a list of available query variables. You can select pre-defined query variables from the **Keyword filter** drop-down list, and then add them to the Query text box by clicking **Add keyword filter**

- If relevant, use property filters to query the content of managed properties that are set to queryable in the search schema. You can select managed properties from the **Property filter** drop-down list. Click **Add property filter** to add the filter to the query.

3. Specify how the search results within your result block should be sorted. Sorting of search results is case sensitive. On the **SORTING** tab, in the **Sort by drop-down list**, select a managed property, and then select **Descending** or **Ascending**. The list only contains managed properties that are set as sortable in the search schema. You can also sort by rank. To add more sorting levels, click **Add sort level**.

4. If you chose to sort by rank, you can optionally:

- Select which model to use for ranking search results (this selection is optional). Use the **Ranking Model** drop-down list.

- Define rules for dynamically changing the ordering of results. In the **Dynamic ordering** section, define when to change ranking by selecting a condition from the drop-down list and then specifying whether to **promote** or **demote** the result. To add more rules, click **Add dynamic ordering rules**

5. Preview the final query that will be run by the Content Search Web Part, on the **TEST** tab. The preview is based on the original query template where dynamic variables are substituted with current values. Other changes to the query may have to be made as part of query rules. Click **Show more** to display additional information.

- The **Query text** shows the final query that'll be run by the Content Search Web Part. It's based on the original query template where dynamic variables are replaced with current values. You might end up making other changes to the query as part of query rules.

- The **Query template** box shows the content of the query template that is applied to the query.

- The **Query template variables** section shows the query variables that will be applied to the query, and the values of the variables that apply to the current page. You can type other values to test the effect they will have on the query. Click the **Test Query** button to preview the search results.

6. Click **OK** to close the **Build Your Query** dialog.

7. Click **Save**.

Make a query rule inactive on a site

Query rules that are created at the tenant level are inherited by site collections and sites. Similarly, query rules that are created at the site collection level are inherited by sites in the site collection. If you don't want a query rule to apply to a site that inherits it, you can make the query rule inactive for the site.

1. On your site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Search** section, click **Query Rules**.

3. On the **Manage Query Rules** page, on the **Select a Result Source** menu, select the result source that contains the query rule that you want to make inactive.

4. In the **Name** column, point to the query rule that you want to make inactive, click the arrow that appears, and then click **Make Inactive**.

Rank query rules for a site collection

When multiple query rules are active for a tenant, a site collection, or a site, more than one rule can fire for a query that is performed at that level. By default, the rules don't fire in a given order. However, if you want to control the order in which the rules fire, you have to add the query rules that you create to query groups. To do this, you select rules to add to a group, and then you specify the order in which the rules in the group will fire if they're triggered. You can also prevent query rules that rank lowest in a group from firing even if they do get triggered.

1. In the site collection, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Site Collection Administration** section, click **Search Query Rules**.
3. On the **Manage Query Rules** page, on the **Select a Result Source** menu, select the result source that contains the query rules that you want to group.
4. For each query rule that you created that you want to add to a group, point to the rule and select the check box.

> **NOTE**
> Query rules that you created for this site collection are listed in the **Defined for this site collection** section.

5. Click **Order Selected Rules**.
6. In the **Order Selected Rules** dialog, do either of the following, and then click **OK**:

- Select **Move rules to new group with this name**, and then type a name for the group.
- Select **Move rules to existing group** and select a group in the list.

7. On the **Manage Query Rules** page:

- To change the order in which a rule in a group will fire if it's triggered, change the number ordering of the rule.
- To prevent query rules that are ranked lowest in the group from firing, go to the row for the group's query rule that should fire last, and then in the **Actions** column, in the **Continue/Stop** list, select **Stop**.

Overview of conditions that make a query rule fire

QUERY CONDITION	DESCRIPTION	CONFIGURATION	EXAMPLE
Query Matches Keyword Exactly	The query rule fires when a query exactly matches a word or phrase that you specify.	In the **Query exactly matches one of these phrases** text box, type one or more phrases separated by semicolons.	Type "picture; pic" in the box. The query rule fires when a user types "picture" or "pic" in a search box. The rule doesn't fire if a user types "pictures" or "sunny picture."

QUERY CONDITION	DESCRIPTION	CONFIGURATION	EXAMPLE
Query Contains Action Term	The query rule fires when a query contains a term for something that the user wants to do. The term must be at the beginning or end of the query.	Enter the action term that causes the query rule to fire by doing one of the following: Select **Action term is one of these phrases**, and type one or more phrases. Select **Action term is an entry in this dictionary**, and then click **Import from term store**. In the dialog, select a term from a term set, and then click **Save**.	Type the word "download" in the **Action term is one of these phrases** box. When a user types "download Contoso Electronics datasheet" in a search box, there are chances the user isn't searching for a document that contains the words "download," "Contoso," "Electronics," and "datasheet." Instead, the user most likely wants to download a Contoso Electronics datasheet. The query rule fires, and only the words "Contoso," "Electronics," and "datasheet" are sent to the search index.
Query Matches Dictionary Exactly	The query rule fires when the query is an exact match of a dictionary entry.	From the **Query exactly matches an entry in this dictionary** list, select a dictionary. To specify a different dictionary, click **Import from term store**, select a term from a term set in the dialog, and then click **Save**.	A word that a user types in a search box perfectly matches an entry in the preconfigured **People Names** dictionary.
Query More Common in Source	The query rule fires if users frequently sent this query from another source that you have already specified.	In the **Query is more likely to be used in this source** list, select a result source.	You selected **Local Video Results** in the list. The query rule fires if a user types the word "training" in a search box and if that word had already been frequently typed in a search box in the Videos vertical.
Result Type Commonly Clicked	The query rule fires if other users frequently clicked a particular result type after typing the same query.	In the **Commonly clicked results match result type** list, select a result type.	You selected **SharePoint MicroBlog Post** in the list. If users frequently click a microblog post in search results, consider configuring the most recent microblog post as the first promoted result, and the next most recent microblog post as the second promoted result (in the **Actions** section).

QUERY CONDITION	DESCRIPTION	CONFIGURATION	EXAMPLE
Advanced Query Text Match	You want to use a phrase or a dictionary entry that causes the query rule to fire, and then define more detailed conditions for when the query rule fires.	Enter the phrase or term that causes the query rule to fire by doing one of the following: Select **Query contains one of these phrases**, and type one or more phrases. Select **Query contains an entry in this dictionary**, and then click **Import from term store**. In the dialog, select a term from a term set, and then click **Save**. Then, add more conditions by checking off options in the lists.	You selected **Query contains one of these phrases**, and then chose **Start of query matches, but not entire query**. The query rule fires only if the phrase is at the beginning of a query, not if it's at the end.

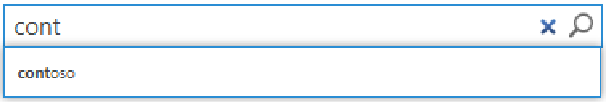
Customize query suggestions in SharePoint search

11/2/2020 • 3 minutes to read • Edit Online

Query spelling suggestions are words that appear below the search box as a user types a query. SharePoint automatically creates a query suggestion when you've clicked a search result for a query at least six times. For example, if you've entered the query word "coffee" and then clicked a search result six times, "coffee" automatically becomes a query suggestion.

Automatic query suggestions are generated daily for each result source and each site collection, so the query suggestions can be different for different result sources and site collections.

For example, in the following screenshot, "contoso" is automatically suggested.



SharePoint has both a classic and a modern search experience, learn about the differences between the classic and modern search experiences in SharePoint. The modern search experience uses the same default result source as the classic search experience. Automatic query suggestions for the default result source appear in both the classic and modern search experiences.

You can manually create your own lists of query suggestions and import them to SharePoint. Manual query suggestions apply to **all** result sources, **all** site collections, and to **both** search experiences.

To create query suggestions for multiple languages, you'll need to create a separate file for each language. The language determines how the query suggestions are processed internally in the search system. All manual query suggestions are always displayed for **all** languages. Add each phrase as a separate line in the text file that you create and save the file in UTF-8 encoding.

Query suggestions are turned on by default. To turn them off, go to **Search Suggestions**, and clear **Show search suggestions**.

To create query suggestions in SharePoint search

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Query Suggestion Settings**.

4. Open a text editor of your choice, and enter a list of terms that you want the system to always suggest to users. Only add one term per line to the text file, and don't mix languages in the text file.

5. Save the text file to a location that's accessible from SharePoint.

6. To import a list of query suggestions to SharePoint search, go to **Always suggest phrases** > **Import from text file**. When you import query suggestions, any existing ones will be overwritten.
7. Browse to the file that you want to import.
8. Go to **Language for suggestion phrases**, and select the processing language of your query suggestions. It should match the language of the terms in the text file.
9. Select **Save Settings**.

Related tasks

You can edit a list of query suggestions that you've manually created. To edit a list that you've already imported in to SharePoint, choose **Export to text file**, update the text file with your changes, and then re-import it. After you've uploaded your query suggestions file, it might take a few hours until your query suggestions are displayed. You can check that they're working properly by entering a phrase from your list of query suggestions in the search box. The query suggestion should appear below the search box.

To get rid of a list of query terms, you must overwrite it. Do this by importing an empty text file.

You can also prevent terms from appearing in the search box. To do this, create a text file with the query terms that you never want users to see below the search box, and then import it to **Never suggest phrases**.

Manage result sources

11/2/2020 • 5 minutes to read • Edit Online

Result sources limit searches to certain content or to a subset of search results. You can also use result sources to send queries to external providers such as Bing.

A global or SharePoint admin can manage result sources for all site collections and sites in the tenant. A site collection administrator or a site owner can manage result sources for a site collection or a site, respectively.

SharePoint has both a classic and a modern search experience. The modern search experience gets results from the default result source. If you change the default result source, this impacts both the classic and modern search experiences. Learn more about the differences between the classic and modern search experiences in SharePoint.

For the classic search experience, you can create your own result sources, or use the predefined result sources. After you create a result source, you configure Search Web Parts and query-rule actions to use it.

Create a new result source

1. Go to the **Manage Result Sources** page for the tenant, for a site collection, or a site:

- For a tenant, in the new SharePoint admin center, select **More features**. Under **Search**, select **Open**, and then on the search administration page, select **Manage Result Sources**.
- For a site collection, in your site collection, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Site Collection Administration**, select **Search Result Sources**.
- For a site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Search**, select **Result Sources**.

2. On the **Manage Result Sources** page, select **New Result Source**.
3. In the **General Information** section, type a name and a description for the new result source.
4. In the **Protocol** section, select one of the following protocols for retrieving search results:

- **Local SharePoint**, the default protocol, provides results from the search index of this tenant (Search Service).
- **Remote SharePoint** provides results from the index of a search service in a different farm (external source). In the **Remote Service URL** box, type the address of the root site collection of the remote SharePoint farm.
- **OpenSearch 1.0/1.1** provides results from a search engine that uses the OpenSearch 1.0/1.1 protocol.
- **Exchange** provides results from Microsoft Exchange Server. Select **Use AutoDiscover** to have the search system find an Exchange Server endpoint automatically, or type the URL of the Exchange web service to retrieve results from — for example, https://contoso.com/ews/exchange.asmx

> **NOTE**
> The Exchange Web Services Managed API must be installed on the computer where the search service is running.

5. If you choose **Local SharePoint** or **Remote SharePoint** for protocol, choose a **Type**:

- **SharePoint Search Results** to search the whole index.
- **People Search Results** to search in people profiles and enable query processing that is specific to people search, such as phonetic name matching or nickname matching.

6. In the **Query Transform** section, you can change incoming queries to use a new query text instead. Choose one of these options:

- Leave the default query transform (**searchTerms**) as is. The query will be unchanged since the previous transform.
- Type a different query transform in the box. See Understanding query transforms.
- Build your own query. Select **Launch Query Builder** and build your query by specifying filters on the **BASICS**, sorting on the **SORTING** tab, and then testing the query on the **TEST** tab. Each of these tabs are described in the following sections.

7. In the **Credentials Information** section, choose an authentication type for users to connect to the result source.

8. Select **Save**.

The BASICS tab

CHOOSE THIS OPTION	TO DO THIS
Keyword filter	Use keyword filters to add predefined query variables to the query transform. Select query variables from the list, and add them to the query by clicking **Add keyword filter**.
Property filter	Use property filters to query the content of managed properties that are set to **queryable** in the search schema. Select managed properties from the **Property filter** list. Click **Add property filter** to add the filter to the query. **NOTE**: Custom managed properties are not shown in the **Property filter** list. To add a custom managed property to your query, in the **Query text** box, enter the name of your custom managed property followed by the query condition, for example *MyCustomColorProperty:Green*

The SORTING tab

CHOOSE THIS OPTION	TO DO THIS
Sort results	Define sorting for results. The **Sort by** list contains managed properties that are set as sortable in the search schema. Select a property to sort by, and then select **Descending** or **Ascending**. To sort by relevance, select **Rank**. Click **Add sort level** if you want to specify more levels of sorting.
Ranking model	If you selected **Rank** from the **Sort by** list, choose the ranking model to use for sorting.

CHOOSE THIS OPTION	TO DO THIS
Dynamic ordering	Click **Add dynamic ordering rule** to specify additional ranking by adding rules that change the order of results within the result block when certain conditions are met. You can add conditions by choosing from the lists that appears.

The TEST tab

CHOOSE THIS OPTION	TO DO THIS
Query text	See the final query text, which is based on the original query template, the applicable query rules, and the variable values.
Show more	Click the link to show more options.
Query template	See the query as it is defined in the **BASICS** tab or in the text box in the **Query transform** section on the Add Result Source page.
Query template variables	Test the query template by specifying values for the query variables. Click **Test query** to see the results.

Set a result source as default

The default result source is **Local SharePoint Results**, but you can choose to set a different one as the default. By doing this, it will be easier to edit the query in Search Web Parts. For example, when you add a Content Search Web Part to a page, the Web Part automatically uses the default result source.

1. Go to the **Manage Result Sources** page for the tenant, for a site collection, or a site:
    - For a **tenant**, in the new SharePoint admin center, select **More features**. Under **Search**, select **Open**, and then on the search administration page, select **Manage Result Sources**.
    - For a site collection, in your site collection, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Site Collection Administration**, select **Search Result Sources**.
    - For a site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Search**, select **Result Sources**.
2. On the **Manage Result Sources** page, point to the result source that you want to set as the default, select the arrow that appears, and then select **Set as Default**.

See also

Understanding result sources

Understanding query transforms

Manage result types

11/2/2020 • 3 minutes to read • Edit Online

As a site collection administrator or site owner, you can create and use result types to customize how results are displayed for particular types of documents.

SharePoint has both a classic and a modern search experience. For the classic search experience, you use a result type to specify a display template that the search system should use for a particular type of document or search result. As documents aren't all the same, search results shouldn't be either. By using result types and display templates, it's much easier for users to find the results they are looking for. You can't customize how results are displayed for the modern search experience. Learn about the differences between the classic and modern search experiences in SharePoint.

A result type specifies one or more conditions to compare search results against, such as the type or the result source of the search result, and an action to take if a search result meets those conditions. The action specifies the display template to use for the search result.

For example, a preconfigured result type named **Person** specifies that if a search result comes from the result source **Local People Results**, then use the **People Item** display template. The **People Item** display template shows information in the hover panel such as documents the person's authored and gives you quick access to those documents.

Another example is to have a result type that fires if the **ContentType** property **contains** *Sales Report*, and then have a specific display template for sales reports. Users will identify the search result as a sales report right away.

See Change how search results look by using result types and display templates for more information.

There are many preconfigured result types to choose from, and you can also create new custom result types. You can configure result types at site collection level and at site level.

Add a new result type

1. Go to the **Manage Result Types** page for a site collection or a site:

- For a site collection, in your site collection, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Site Collection Administration**, select **Search Result Types**.
- For a site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**. Under **Search**, select **Result Types**.

2. On the **Manage Result Types** page, do one of the following:

- Click **New Result Type**, or
- In the list of existing result types, click the name of a result type, such as **Person**, and then click **Copy** so that you can modify the copy to create a new result type.

3. In the **General Information** section, in the **Give it a name** box, type a name for the result type.
4. In the **Conditions** section, in the first list, choose a result source that the results should match.
5. In the **Conditions** section, in the second list, choose which types of content should match. To match all

content, skip the rule. To add more content types, click **Add value**.

6. To add more advanced conditions related to managed properties, expand **Show more conditions**.
7. In the first list, choose a property to match.
8. Choose how the property should relate to one or more values.
9. Enter one or more values for the property in the box. Separate by using semicolons.
10. To add more properties to match, click **Add property**.
11. In the **Actions** section, select a display template. The URL of the display template is shown under **Display template URL**.
12. Check the **Optimize for frequent use** box if the result type will be among the most frequently used result types.
13. Click **Save**.

Manage search dictionaries

11/2/2020 • 6 minutes to read • Edit Online

You can use search dictionaries to include or exclude company names to be extracted from the contents of your indexed documents, or you can include or exclude words for query spelling correction.

Manage company name extraction

> **NOTE**
>
> Beginning on November 15th, 2019, we'll be removing Company Name Extraction from SharePoint in Microsoft 365. This will only impact you if you have configured company name extraction to be surfaced in the classic Enterprise Search Center as a refiner. Learn more about the specifics and other options by reading Changes to company name extraction in SharePoint.

For company name extraction to work, that is, for a company name to be pulled from your content and for it to be mapped to the managed property **companies**, you have to make sure that:

- The managed property setting **Company name extraction** is enabled on the managed property that you want to extract company names from. This setting is available for the managed properties **Title**, **Body** and **Notes**. See also Manage the search schema in SharePoint.
- The name of the company that you want to extract is in the prepopulated company name dictionary or in the **Company Inclusions** list.

After you have done this, you can then use the managed property **companies** to create refiners based on the extracted company name in the **Refinement Web Part**, on the search results page.

Include company names

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**, and to open the term store, select **Manage Search Dictionaries**.
3. On the **Site Settings: Term Store Management Tool** page, to expand the **Search Dictionaries** menu, select the arrow.
4. Select **Company Inclusions**, then select the arrow, and then select **Create Term**.
5. Enter the name of the company that you want to include in the box that appears.
6. To add the term to the **Company Inclusions** list, select anywhere on the page.

Exclude company names

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. To open the term store, select **Manage Search Dictionaries**.
4. On the **Taxonomy Term Store** page, to expand the **Search Dictionaries** menu, select the arrow.
5. Select **Company Exclusions**, then select the arrow, and then select **Create Term**.
6. Enter the name of the company that you want to exclude in the box that appears.
7. To add the term to the **Company Exclusions** list, select anywhere on the page.

Manage query spelling correction

> **NOTE**
>
> Beginning on December 8, 2020, we'll be removing Query Spelling Suggestions (inclusion and exclusion lists) from SharePoint in Microsoft 365. This will only impact you if you have configured Query Spelling Suggestions. Query Spelling Suggestions will be replaced with a native learning platform to provide automatic spelling suggestions across Microsoft Search (initially in SharePoint and Outlook).

If you or another user enters a word in a search query that appears to be misspelled, the search results page helps you out by displaying query spelling corrections. These are important words in your indexed documents. This is also known as "Did you mean?".

For example, if you enter a query that contains the word "ampitheater", the query spelling correction would show "amphitheater" if this term is available in many places in your indexed documents. You can add terms such as the one just shown to the **Query Spelling Inclusions** list, or to the **Query Spelling Exclusions** list to influence how you want query spelling corrections to be applied or not. It takes up to 10 minutes for any changes to the **Query Spelling Inclusions** or the **Query Spelling Exclusions** list to take effect.

Include a term in query spelling corrections

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. To open the term store, select **Manage Search Dictionaries**.

4. On the **Site Settings: Term Store Management Tool** page, to expand the **Search Dictionaries** menu, select the arrow.

5. Select **Query Spelling Inclusions**, then select the arrow, and then select **Create Term**.

6. Enter the query spelling that you want to include in the box that appears.

7. To add the term to the **Query Spelling Inclusions**, select anywhere on the page.

Exclude a term from query spelling corrections

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. To open the term store, select **Manage Search Dictionaries**.

4. On the **Site Settings: Term Store Management Tool** page, to expand the **Search Dictionaries** menu, select the arrow.

5. Select **Query Spelling Exclusions**, then select the arrow, and then select **Create Term**.

6. Enter the query spelling that you want to exclude in the box that appears.

7. To add the term to the **Query Spelling Exclusions** list, select anywhere on the page.

Edit query spelling corrections or company names

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. To open the term store, select **Manage Search Dictionaries**.

4. On the **Site Settings: Term Store Management Tool** page, to expand the **Search Dictionaries** menu, select the arrow.

5. Depending on which dictionary the term is in, select **Company Exclusions**, **Company Inclusions**,

Query Spelling Exclusions, or **Query Spelling Inclusions**.

6. Double-click the term that you want to edit.
7. Enter the new name for the term.
8. To save the edited term, select anywhere on the page.

Manage authoritative pages

11/2/2020 • 2 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can influence the pages or documents that should appear at the top of your list of search results by identifying high-quality pages, also known as authoritative pages. Authoritative pages link to the most relevant information. A typical example of an authoritative page could be the home page of your company portal.

Authoritative pages only work for **classic** search and only for web parts that use the **default** ranking model.

If you have specific knowledge of an area, you can influence the relative importance of pages by adding more levels of authoritative pages (second-level and third-level).

In the same way, you can also add non-authoritative pages. A typical example of a non-authoritative page could be the URL of a site that contains outdated information.

Specify authoritative or non-authoritative pages

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the search administration page, select **Manage Authoritative Pages**.

4. In the **Authoritative Web Pages** section, in the **Most authoritative pages** box, enter the URLs of pages that are the most important. Separate the URLs with returns so that there is one URL per line.

5. In the **Second-level authoritative pages** box, enter the URLs of any pages that should be seen as second-level.

6. In the **Third-level authoritative pages** box, enter the URLs of any pages that should be seen as third-level.

7. In the **Non-authoritative Sites** section, in the **Sites to demote** box, enter the URLs of any sites that you want to be ranked lower than all of the other sites. Type one URL per line.

   > **TIP**
   >
   > All URLs whose prefix matches the prefix of a URL in the **Sites to demote** box are demoted. Example: Entering http://archive/ demotes the rank of all URLs that begin with http://archive/.

8. Select **OK**.

How results are ranked

Classic search uses the list of authoritative pages to calculate the ranking of results. Static rank determines the relative importance of a page. Static rank is calculated as the smallest number of clicks that it would take a user to navigate from an authoritative page to a document. The closer a document is to the most authoritative page, the higher the static rank of the page is.

Export and import customized search configuration settings

11/2/2020 • 7 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can export and import customized search configuration settings between tenants, site collections, and sites. The settings that you export and import include all customized query rules, result sources, result types, ranking models and site search settings. It's also possible to export customized search configuration settings from a Search service application and import the settings to tenants, site collections, or sites. You can't export the default configuration settings.

Overview

When you export customized search configuration settings, SharePoint creates a search configuration file in XML format. This search configuration file includes all exportable customized search configuration settings at the tenant, site collection, or site level from where you start the export. A search configuration file for a site collection doesn't contain search configuration settings from the individual sites within the site collection.

When you import a search configuration file, SharePoint creates and enables each customized search configuration setting in the tenant, site collection or site from where you start the import.

This table shows the settings that you can export or import. For each setting, you'll find dependencies on other customized search configuration settings. If the customized search configuration settings depend on a customized search configuration setting at a different level, for example, if a site query rule depends on a result source at site collection level, you must export and import settings at all of the relevant levels.

CUSTOMIZED SEARCH CONFIGURATION SETTING	DEPENDENCY ON OTHER CUSTOMIZED SEARCH CONFIGURATION SETTINGS
Query rules. These include result blocks, promoted results, and user segments.	Result sources, result types, search schema, ranking model.
Result sources	Search schema
Result types	Search schema, result sources, display templates
Search schema	None
Ranking model	Search schema

Conditions that can cause the import to fail

If the search configuration file and the target for your import have settings with the same name, the import of the search configuration file fails when it encounters this setting. There are exceptions however:

- If you reimport a search configuration file, the settings that have the same name in the search configuration file and on the target do not cause the import to fail.
- Managed properties with the same name do not cause an import to fail if the individual managed property settings are the same on the property in the search configuration file and on the target property.

- Managed properties with the same name do not cause an import to fail if the aliases and mappings to crawled properties are different on the managed property in the search configuration file and on the target managed property. The import adds the aliases and mappings on the managed property in the search configuration file to the aliases and mappings on the target managed property.

If the search configuration file contains managed property names or aliases that contain invalid characters, the import fails when it encounters that managed property name or alias.

The managed property names and aliases of a search schema must be unique for a site and its parent site collection. This means:

- If your search configuration file has a managed property that has the same name as an alias for a managed property on your target site or the parent site collection of your target site, then the import fails.
- If your search configuration file has a managed property with an alias that has the same name as a managed property on your target site or the parent site collection of your target site, then the import fails.

> **NOTE**
> Any customized search settings that were created and enabled by SharePoint before the import failed, remain enabled.

If the import fails, remove the condition that caused the failure and reimport the search configuration file. For example, if the Notes column states that there is already a query rule with the same name as the query rule that you are trying to import, then you should remove that query rule either from the target or from the import file, and then reimport the file. See Invalid characters causing your import to fail later in this article.

Export customized search configuration settings from a tenant

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select Open.
3. Select **Export Search Configuration**.
4. In the dialog, select **Save**.

Export customized search configuration settings from a site

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Search** section, select **Configuration Export**.
3. In the dialog, select **Save**.

Export customized search configuration settings from a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Site Collection Administration** section, select **Search Configuration Export**.

3. In the dialog, select **Save**.

Import customized search configuration settings to a tenant

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.

3. On the **Import Search Configuration** page, browse to the file you want to import.

4. Select **Import**.

5. On the **Search Config List** page, verify that:

6. The search configuration file you imported is in the list, and that its status is **Imported Successfully**.

   If the file hasn't been imported successfully, then the **Notes** column provides more details about what happened.

7. The **Scope** column shows that the settings you imported are at the right level, that is, at the level you meant to import the file to. For example, if you imported your settings at the site collection level instead of at the site level, you'd see this information in the **Scope** column. The **Scope** column shows at which level the search configuration settings were enabled. The levels are: tenant (Tenant), site collection (SPSite), or site level (SPWeb).

Import customized search configuration settings to a site

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.

2. On the **Site Settings** page, in the **Search** section, select **Configuration Import**.

3. On the **Import Search Configuration** page, browse to the file you want to import.

4. Select **Import**.

5. On the **Search Config List** page, verify that:

6. The search configuration file you imported is in the list, and that its status is **Imported Successfully**.

   If the file hasn't imported successfully, then the **Notes** column provides more details about what happened.

7. The **Scope** column shows that the settings you imported are at the right level, that is, at the level you meant to import the file to. For example, if you imported your settings at the site collection level instead of at the site level, you'd see this information in the **Scope** column. The **Scope** column shows at which level the search configuration settings were enabled. The levels are: tenant (Tenant), site collection (SPSite), or site level (SPWeb).

Import customized search configuration settings to a site collection

1. On the site, select **Settings**, and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. On the **Site Settings** page, in the **Site Collection Administration** section, select **Search Configuration Import**.
3. On the **Import Search Configuration** page, browse to the file you want to import.
4. Select **Import**.
5. On the **Search Config List** page, verify that:
6. The search configuration file you imported is in the list, and its status is **Imported Successfully**.

   If the file hasn't imported successfully, then the **Notes** column provides more details about what happened.

7. The **Scope** column shows that the settings you imported are at the right level, that is, at the level you meant to import the file to. For example, if you imported your settings at the site collection level instead of at the site level, you'd see this information in the **Scope** column. The **Scope** column shows at which level the search configuration settings were enabled. The levels are: tenant (Tenant), site collection (SPSite), or site level (SPWeb).

Invalid characters causing your import to fail

If managed properties or aliases contain any of the listed characters, the import of the customized search schema that contains these properties will fail.

CHARACTER	NAME
	space
:	colon
;	semicolon
,	comma
(	opening parenthesis
)	closing parenthesis
[	opening bracket
]	closing bracket
{	opening brace

CHARACTER	NAME
}	closing brace
%	percent
$	dollar sign
_	underscore
+	plus sign
!	exclamation point
*	asterisk
=	equal sign
&	ampersand
?	question mark
@	at sign
#	number sign
\	backslash
~	tilde
<	opening angle bracket
>	closing angle bracket
|	pipe
`	grave accent
^	caret
'	escape sequence
"	escape sequence

Check logs, limits and reports

11/2/2020 • 2 minutes to read • Edit Online

See if the crawler has added content to the search index, and if your users are finding what they're looking for in SharePoint.

View search usage reports

This article describes how you can use search reports in the SharePoint admin center to find answers to questions about how search is being used in your organization. You can for example see the number of queries and the top queries. Learn more.

Query throttling

In SharePoint, you can't turn query throttling on or off, but you can use client-type information to make sure lower-priority clients like automated queries don't squeeze out higher-priority clients like UI. Learn more.

Set crawl log permissions

Use the crawl log to see if crawled content was successfully added to the search index, if it was excluded because of a crawl rule, or if indexing failed because of an error. Learn more.

Search limits

Look up the limits to SharePoint search. For example, there are limits to the number of entries you can have in a custom search dictionary and the number of results that can be returned for a query. Learn more.

View search usage reports

1/8/2021 • 3 minutes to read • Edit Online

NOTE

Beginning on January 11, 2021, we'll be retiring classic tenant-wide search usage reports in SharePoint Online. After this change, you will be able to discover site collection search usage data through the classic site collection usage reports under the **Site** > **Site Settings** > **Site collection Administration** > **Search Reports** where you can access and download usage data for the last 31 days and past 12 months. For administrators of Microsoft Search you can access the tenant usage analytics reports through the Microsoft 365 admin center under **Settings** > **Search and Intelligence** > **Insights**.

If you're a SharePoint admin in your organization, you're probably asked questions about search usage, such as:

- What are the top queries on my site per day or per month?
- How many search queries are users performing on average?
- Which queries are getting low clicks as they're simply not showing up in any results?
- How often are query rules firing and how often are people clicking promoted results?

This article describes how you can use search reports in the SharePoint admin center to find answers to these questions.

To view a report

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

NOTE

If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. Select **View Usage Reports**.
4. To retrieve a report, select a link on the page. The report opens in an Excel spreadsheet or in another program that you can find online.

Overview of search reports

REPORT	DESCRIPTION
Number of Queries	This report shows the number of search queries performed. Use this report to identify search query volume trends and to determine times of high and low search activity.

REPORT	DESCRIPTION
Top Queries by Day	This report shows the most popular search queries. Use this report to understand what types of information visitors are seeking.
Top Queries by Month	This report shows the most popular search queries. Use this report to understand what types of information visitors are seeking.
Abandoned Queries by Day	This report shows popular search queries that received low click-through. Use this report to identify search queries that might create user dissatisfaction and to improve the discoverability of content. Then, consider using query rules to improve the query's results.
Abandoned Queries by Month	This report shows popular search queries that received low click-through. Use this report to identify search queries that might create user dissatisfaction and to improve the discoverability of content. Then, consider using query rules to improve the query's results.
No Result Queries by Day	This report shows popular search queries that returned no results. Use this report to identify search queries that might create user dissatisfaction and to improve the discoverability of content. Then, consider using query rules to improve the query's results.
No Result Queries by Month	This report shows popular search queries that returned no results. Use this report to identify search queries that might create user dissatisfaction and to improve the discoverability of content. Then, consider using query rules to improve the query's results.
Query Rule Usage by Day	This report shows how often query rules trigger, how many dictionary terms they use, and how often users click their promoted results. Use this report to see how useful your query rules and promoted results are to users.
Query Rule Usage by Month	This report shows how often query rules trigger, how many dictionary terms they use, and how often users click their promoted results. Use this report to see how useful your query rules and promoted results are to users.

Related topics

Microsoft 365 Reports in the Admin Center - SharePoint site usage

Microsoft 365 Reports in the Admin Center - SharePoint activity

Crawl log permissions

11/2/2020 • 2 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can grant users read access to crawl log information for the tenant. The crawl log tracks information about the status of crawled content.

A typical use case is in eDiscovery, where you can grant a security group permission to view the crawl log information for the tenant. The users in the security group can view the crawl log data via the eDiscovery portal to check whether crawled content was successfully added to the search index, or whether indexing failed because of an error.

Grant users permission to view the crawl log information

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. On the **search administration** page, select **Crawl Log Permissions**.
4. In the **Crawl Log Permissions** box, enter names or email addresses. The names of valid users or user groups appear in the list as you enter letters in the box.
5. Select **OK**.

Manage query client types

11/2/2020 • 2 minutes to read • Edit Online

Learn how query client types decide in which order queries are performed.

A query client type is how a client performing a query tells the system what type of client it is. For example, a client might tell us it is UI, or an automated query. Query throttling monitors the use of resources and protects the search system. Administrators can use client-type information for throttling, to make sure lower-priority clients like automated queries don't squeeze out higher-priority clients like UI. Query client types are also used for things like logging, reports, and determining relevance.

The client sets the client type as a label in the query. The administrator configures the valid client types (though some are default and mandatory), and the client chooses one for each query.

> **NOTE**
> You can't turn query throttling on or off.

Add a query client type

> **NOTE**
> You can change the name of a client type that has been created for your tenant only.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. On the search administration page, select **Manage Query Client Types**.
4. To add a client type, select **New Client Type**.
5. On the **Edit a client type** page, in the **Query Client Type** field, for the client type, enter a name.
6. From the **Throttling Tier** list, select either **Top**, **Middle**, or **Bottom**.

   > **NOTE**
   > Lower priority queries are throttled first. The search system processes queries from top tier to bottom tier.

7. Select **OK**.

Prioritize a client query type

You can use throttling tiers to prioritize query processing. When the resource limit is reached, query throttling kicks in, and the search system processes queries, starting from the top tier, right through to the bottom tier.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Search**, select **Open**.
3. On the search administration page, select **Manage Query Client Types**.
4. Go to the **Client Type** section, and select the **System Type** that you want to change.
5. From the **Throttling Tier** list, select either **Top**, **Middle**, or **Bottom**.

   > **NOTE**
   >
   > Lower priority queries are throttled first. The search system processes queries from top tier to bottom tier.

6. Select **OK**.

Search limits for SharePoint

11/2/2020 • 4 minutes to read • Edit Online

As an admin who manages SharePoint (for more info, see SharePoint search administration overview), you should also be aware of limits to search. For example, there are limits to the number of entries you can have in a custom search dictionary or the number of rows that are returned as part of a search.

There are two types of limits:

- **Boundary** A number that can't be exceeded.
- **Supported** A recommended number, based on testing that Microsoft has done, that shouldn't be exceeded. If you exceed a supported limit, you might encounter unexpected results or see a significant decrease in performance.

These limits apply to all SharePoint plans.

The following table lists the limits for SharePoint search.

LIMIT	MAXIMUM VALUE	LIMIT TYPE	NOTES	
Size of document that can be downloaded by the crawl components	150 MB	Boundary	Search downloads metadata and content from a document until it reaches the maximum document size. The rest of the content is not downloaded.	
Parsed content size	2 million characters	Boundary	Search stops parsing an item after it has parsed up to 2 million characters of content from it, including the item's attachments. The actual amount of parsed characters can be lower than this limit because search uses a maximum of 30 seconds on parsing a single item and its attachments. When search stops parsing an item, the item is marked as partially processed. Any unparsed content isn't processed and therefore isn't indexed.	

LIMIT	MAXIMUM VALUE	LIMIT TYPE	NOTES	
Characters processed by the word breaker	1,000,000	Boundary	Search breaks content into individual words (tokens). The word breaker produces tokens from the first 1,000,000 characters of a single item, including the item's attachments. The actual amount of tokens can be lower than this limit because search uses a maximum of 30 seconds on word breaking. Any remaining content isn't processed.	
Indexed managed property size	512 KB per managed property that is set to either "searchable" or "queryable"	Boundary		
Retrievable managed property size	16 KB per managed property	Boundary		
Sortable and refinable managed property size	16 KB per managed property	Boundary		
Token size	Variable - the size depends on the word breaker, and the word-breaker is language-dependent.	Boundary	Search can index tokens of any length but the word breaker that is used to produce tokens can limit the token length. Word breakers are language-aware components that break content into single words (tokens).	

LIMIT	MAXIMUM VALUE	LIMIT TYPE	NOTES	
Unique indexed tokens per managed property	10,000	Boundary	This is the maximum number of unique tokens that can be added to the search index per managed property. If the limit is exceeded, the index will contain the first 10,000 tokens from the managed property and the file will be marked as partially processed by setting the IsPartiallyProcessed property to true.	
Distinct users or AD/AAD security groups having access to an item	10,000	Boundary	When more than 10,000 distinct users or AD/AAD security groups have access to an item, the item isn't searchable by any user. Such items will only be returned as part of an eDiscovery query through the Security & Compliance center.	
Number of entries in a custom search dictionary	5,000 terms per tenant	Boundary	This limits the number of terms allowed for inclusions and exclusions dictionaries for query spelling correction and company extraction. You can store more terms than this limit in the term store, but search only uses 5,000 terms per tenant.	
Managed property mappings	100 per managed property	Supported	Crawled properties can be mapped to managed properties. Exceeding this limit may decrease crawl speed and query performance.	

LIMIT	MAXIMUM VALUE	LIMIT TYPE	NOTES	
Values per managed property	1,000	Boundary	A managed property can have multiple values of the same type. This is the maximum number of values per managed multi-valued managed property per document. If this number is exceeded, the remaining values are discarded.	
Unique contexts used for ranking	15 unique contexts per rank model	Boundary		
Authoritative pages	1 top level and minimal second- and third-level pages per tenant	Supported	Use as few second- and third-level pages as possible while still achieving the desired relevance. If you add additional pages you may not achieve the desired relevance. Add the key site to the first relevance level. Add more key sites at either second or third relevance levels, one at a time. Evaluate relevance after each addition to ensure that you have achieved the desired relevance effect.	
Text length for queries using Keyword Query Language	4 KB (4,096 characters)	Boundary		
Number of rows in a result set	500	Boundary	To display the entire result set, issue more paging queries. For Discovery queries the maximum number of rows in a result set is 10,000.	
User-defined full-text indexes	3	Boundary		

LIMIT	MAXIMUM VALUE	LIMIT TYPE	NOTES	
Maximum number of on-premises items indexed in Microsoft 365	20 million items	Threshold	For each 1 TB of storage space your tenant has in Microsoft 365, you can index 1 million items of on-premises content in your tenant's search index in Office 365 with the cloud hybrid search solution. This quota is by default limited upwards to 20 million items. To increase the number of items that can be indexed beyond 20 million items, contact Microsoft Support.	

See also

- SharePoint Limit
- SharePoint Service Description
- Overview of the search schema in SharePoint Server 2013
- SharePoint feature availability across Office 365 plans

View Popularity Trends and Most Popular Items

11/2/2020 • 2 minutes to read • Edit Online

To identify usage trends and find out at what times activity is high or low, you can view **Popularity Trends** reports for a site or a site collection. The reports show historical usage information, such as number of views (hits) and unique users per day or month. Popularity Trends for a page or item in a library in a library show how many views the page or item has had recently.

You can also view the most popular items in a library. You'll see which items have the most views, either recently or ever (from the first time the item became available.)

> **NOTE**
> For SharePoint Modern sites, please see View usage data for your SharePoint site.

View Popularity Trends for a site

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Site Administration**, click **Popularity Trends**.
3. Click **Usage**.
4. Click Open to open the report in Excel.

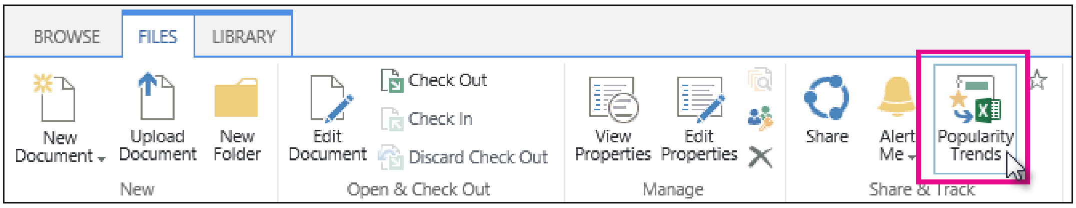
View Popularity Trends for a site collection

1. On the site, select **Settings** , and then select **Site settings**. If you don't see **Site settings**, select **Site information**, and then select **View all site settings**.
2. Under **Site Collection Administration**, click **Popularity and Search Reports**.
3. Under **Usage Reports**, click **Usage**.
4. Click Open to open the report in Excel.

You can also view other reports for the site collection, see View usage and search reports.

View Popularity Trends for a page or item in a library

1. On your site, navigate to the relevant document library.
2. Select one or more pages or items that you want to look at trends for.
3. Click the **FILES** tab.
4. On the ribbon, click **Popularity Trends**.



5. Click Open to open the **Usage Details** report in Excel. There's one tab in the report for each item you selected.

You can also see popularity trends for a page or item from the **Most Popular Items** view.

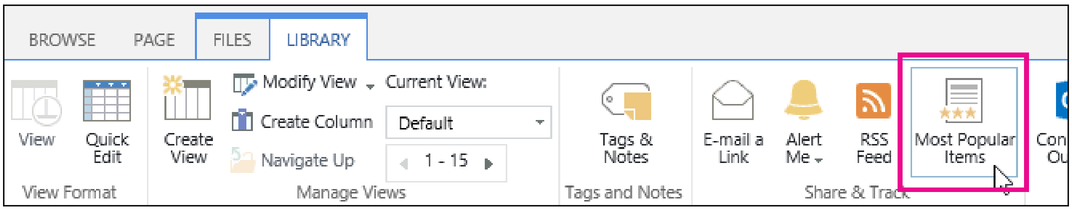
Or, you can go to an individual page and select the **PAGE** tab > **Popularity Trends**.

View the Most Popular Items in a library

1. On your site, go to the relevant document library.

2. Click the **LIBRARY** tab.

3. On the ribbon, click **Most Popular Items**.



You can sort the list by **Recent** (views the last 14 days), or **Ever** (views from the first time the item became available).

To see more details for each item, click the **Popularity Trends** link under each item URL.

View Usage and Search reports for all sites

If you're a global or SharePoint admin in Microsoft 365, you can view search usage reports for the whole organization. See View usage and search reports.

Manage user profiles in the SharePoint admin center

11/2/2020 • 4 minutes to read • Edit Online

This article is for global admins and SharePoint admins in Microsoft 365.

- If you're running SharePoint Server, see Administer the User Profile service in SharePoint Server.
- If you're not an admin, see View and update your profile in Office Delve for info about changing your profile.

Most organizations don't need to change any user profile settings in the SharePoint admin center. For the organizations that do need to work with user profile settings, this article describes the most common tasks.

Create and edit custom user properties

In Microsoft 365, identity is managed by Azure Active Directory. For info about this, see Understanding Microsoft 365 identity and Azure Active Directory. SharePoint receives this profile information as described in About user profile synchronization. If you need to store additional info about your users, you can create custom properties in the classic SharePoint admin center. For info about doing this, see Add and edit user profile properties in SharePoint.

> **NOTE**
> Instead of creating user sub-types in the SharePoint admin center, we recommend using the Microsoft 365 admin center to Compare groups or using the Azure AD admin center to create groups with dynamic membership.

Add and remove admins for a user's OneDrive

Follow these steps to transfer ownership of a OneDrive to a different user, or give a user full control over another user's OneDrive.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the the SharePoint admin center and open the More features page.

2. Under **User profiles**, select **Open**.
3. Under **People**, select **Manage User Profiles**.

4. Enter the user's name and select **Find**.

5. Right-click the user, and then select **Manage site collection owners**.

6. Add and remove admins for the OneDrive, and then select **OK**.

WARNING

Do not remove a user as the admin of their own OneDrive. Doing this causes many experiences to break.

For info about automatically transferring ownership of OneDrive to a user's manager when the user account is marked for deletion, see Set up access delegation.

Manage audiences

Audiences let you customize content on pages so that it appears only to particular people based on their:

- Membership in a distribution list or security group
- Location in the reporting structure or public info in the user profile

For example, you can display a navigational link to only people in a particular geographic location. For info about using audiences, see Target content to specific audiences.

NOTE

Only sites that use classic templates can be customized based on audience.
Audiences are not a security feature. They help you deliver relevant content to specific groups of people, but don't prevent content from being available to anyone with the appropriate permissions.

To add, edit, or delete an audience or an audience rule, go to the Manage Audiences page:

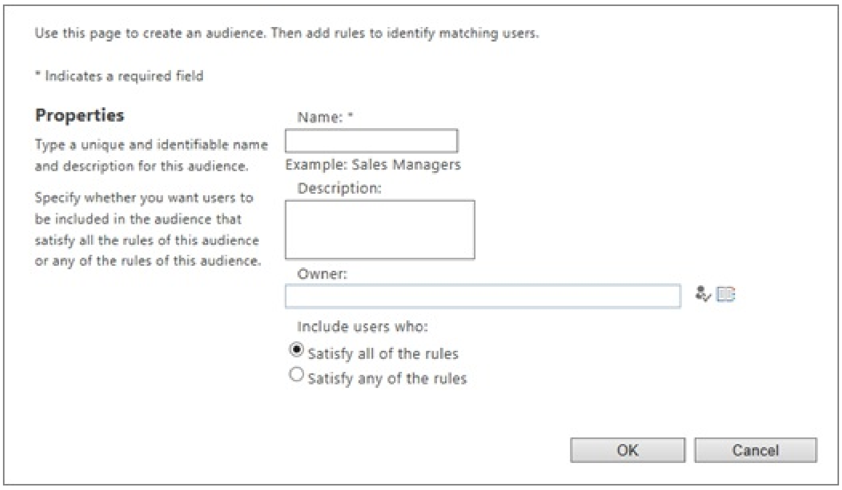
1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

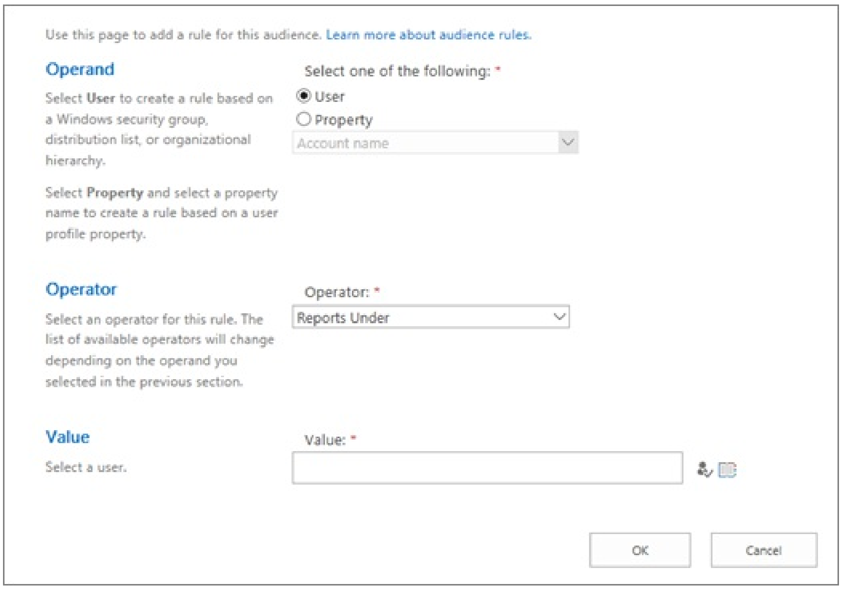
2. Under **User profiles**, select **Open**.

3. Under **People**, select **Manage Audiences**.

Creating a new audience:



Creating a new rule for the audience:



Audiences compile approximately weekly, and you can only view audience members after the audience compiles. The user profiles page shows the number of audiences, the number of uncompiled audiences, and the compilation status and time.

Disable OneDrive creation for some users

If some users are licensed to use OneDrive, but you don't want them to create a OneDrive (perhaps for regulatory reasons), you can prevent them from doing so.

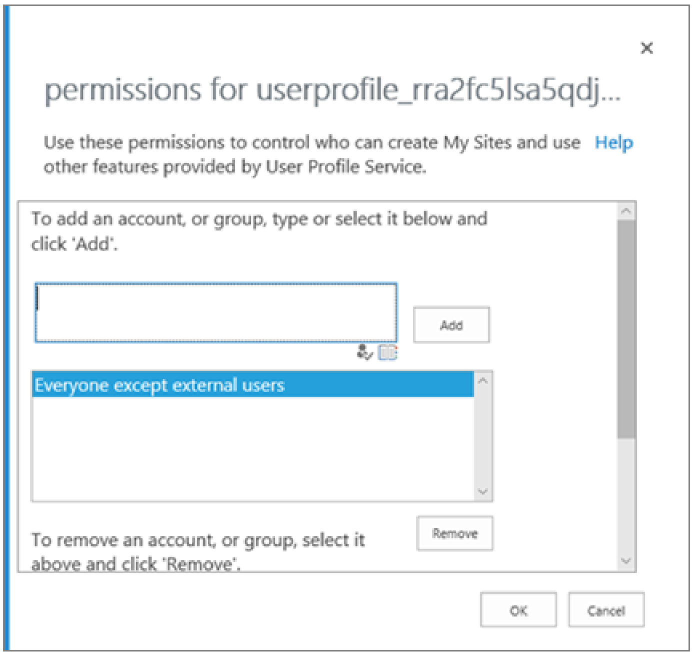
> **NOTE**
>
> If a user already created a OneDrive, changing the following setting won't delete it.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **User profiles**, select **Open**.
3. Under **People**, select **Manage User Permissions**.

4. By default, "Everyone except external users" has permission to "Create Personal Site" (which includes creating a OneDrive and saving user data such as followed and frequent sites). Remove that group and add specific groups to allow only a subset of licensed users to create a OneDrive.



> **NOTE**
>
> The **Disable OneDrive** check box has no effect. Use the "Create Personal Site" check box to specify the security groups that have permission to create a OneDrive.

5. Select **OK**.

Add and edit user profile properties in SharePoint

11/2/2020 • 4 minutes to read • Edit Online

If your organization uses the cloud identity model, your user accounts are stored in Azure AD and you can manage most user profile info in the Microsoft 365 admin center. For info, see Edit or change a user in Microsoft 365. You can also manage user profiles (including adding user pictures and defining user managers) in the Azure AD admin center. For info, see Add or change profile information for a user in Azure Active Directory. If you need to create custom user profile properties, such as languages spoken, emergency contact info, or sales account, you can use user properties in SharePoint. Note that these properties are NOT synced back to Azure AD.

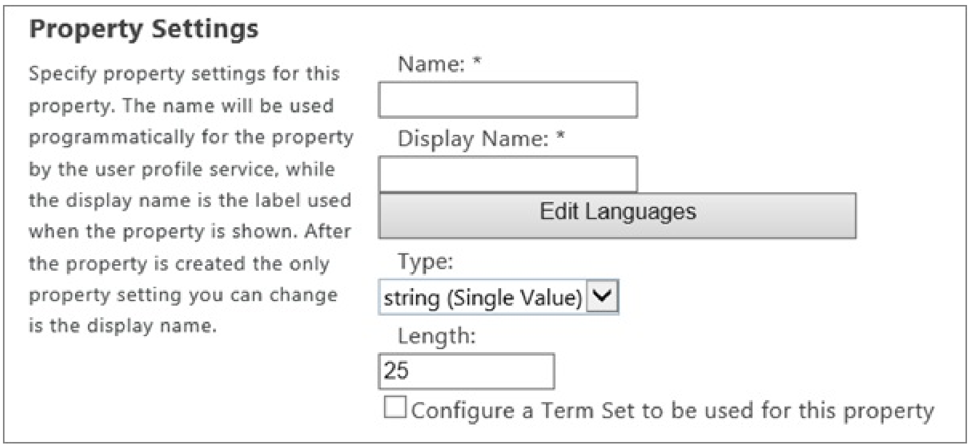
Add a property for a user profile

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **User profiles**, select **Open**.
3. Under **People**, select **Manage User Properties**.

4. Select **New Property**.
5. In the **Name** box, enter a unique name for the property.



6. In the **Display Name** box, enter the profile property name that will be displayed to all users. (This name doesn't have to be unique.)

7. In the **Type** list, select the data type for the property.

> **NOTE**
>
> If you select **string (Multi Value)**, the property will be permanently set as a multi-valued property. You cannot change this setting after you select **OK**. You can only delete the property and add it again as a new single-value property.

8. If you selected binary, HTML, or string, use the **Length** box to enter the maximum number of characters allowed for property values.

9. If you selected string and want to associate the profile property with a managed metadata term set, select **Configure a Term Set to be used for this property**. Then select a term set from the list.

10. Make sure **Default User Profile Subtype** is selected so the default user profile subtype is associated with this user profile property.

11. In the **Description** box, enter the instructions or information that is displayed to users about this profile property.

12. In the **Policy Settings** section, select the policy setting and default privacy setting that you want for this property. Select the **User can override** box to enable users to override these settings.

13. If you want users to be able to change this profile information for themselves, select **Allow users to edit values for this property**.

14. In the **Display Settings** section, specify whether and how the property will be viewed by users.

15. In the **Search Settings** section, select **Alias** if the property is the equivalent of a user's name. For example, you might do this if you create a property for a "Stage name" and want searches for all documents by John Kane to return the same results as searches for the user's real name. Select the **Indexed** if you want searches to return all the user profiles matching that property. For example, if you have a property for "University," a search for that value would return all alumni from that university.

> **NOTE**
>
> The **Alias** check box is available only if you set the **Default Privacy Setting** > **Everyone**.

16. Select **OK**.

Edit or delete a property you added

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Select **User profiles**, and then select **Open**. Under **People**, choose **Manage User Properties**.

3. In the **Property Name** column, select the profile property that you want to change, and then select **Edit** or **Delete**.

4. Edit the elements you want to change.

> **NOTE**
>
> Some elements of profile properties, such as the **Type** element, are unavailable because they can't be edited. To define these elements, create a new property. The exception is the Source Data Connection property. It's predefined in SharePoint and can't be changed.

5. When you're done, select **OK**.

Synchronize custom properties

Custom properties from Active Directory or Azure AD are not synchronized with SharePoint. For info about bulk updating custom user profile properties by using PowerShell, see Call the import API from PowerShell.

Need more help?

If you have technical questions about this topic, you may find it helpful to post them on the SharePoint discussion forum. It's a great resource for finding others who have worked with similar issues or who have encountered the same situation.

User profile synchronization

1/8/2021 • 3 minutes to read • Edit Online

Microsoft SharePoint uses the Active Directory synchronization job to import user and group attribute information into the User Profile Application (UPA).When a new user is added to Azure Active Directory (Azure AD), the user account information is sent to the SharePoint directory store and the UPA sync process creates a profile in the User Profile Application based on a predetermined set of attributes. Once the profile has been created, any modifications to these attributes will be synced as part of regularly scheduled sync process.

NOTE

The profile properties that are synced by the UPA sync process are not configurable. Synchronization times will vary based on workloads.

Sync process

There are four steps in the sync process.

STEP	DESCRIPTION
1. Active Directory to Azure AD	Azure AD Connect syncs data from on-premises Active Directory to Azure AD. For more info, seeWhat is hybrid identity with Azure Active Directory? and Attributes synchronized.
2. Azure AD to SharePoint	Azure AD syncs data from Azure AD to the SharePoint directory store.
3. SharePoint to UPA	The UPA sync process syncs user account information in SharePoint directory store to the User Profile Application (UPA).
4. UPA to sites	User account information from the UPA is synced to SharePoint sites (previously called “site collections”).

Typically, user profiles are created automatically for all accounts that are created in Microsoft 365. For organizations that have a Microsoft 365 Education subscription, user profiles are not created for new accounts by default. The user must access SharePoint once, at which time a basic stub profile will be created for the user account. The stub profile will be updated with all remaining data as part of the sync process.

If block sign-in is set on the user account in Azure AD or disabled accounts are synced from Active Directory on premises, those user accounts will not be processed as part of the UPA sync process. The user must be enabled and licensed for changes to be processed.

Properties that are synced into SharePoint user profiles

The following Azure AD user attributes are synced to the UPA.

AZURE AD ATTRIBUTE	USER PROFILE PROPERTY DISPLAY NAMES	NOTES	SYNC TO SITES
UserPrincipalName	Account Name User Name User Principal Name	Example: `i:0#.f <|> membership <|>` gherrera@contoso.com gherrera@contoso.com	Yes
DisplayName	Name		Yes
GivenName	FirstName		Yes
sn	LastName		Yes
telephoneNumber	Work phone	Example: (123) 456-7890	Yes
proxyAddresses	Work Email SIP Address	Work Email is set to the value prefixed withSMTP.(SMTP:gherrera@contoso.com) Example: gherrera@contoso.com	Yes
PhysicalDeliveryOfficeName	Office		Yes
Title	Title Job Title	Job Title contains the same value as Title and is connected to a term set.	Yes
Department	Department	Department is connected to a term set.	Yes
WWWHomePage	Public site redirect		No
PreferredLanguage	Language Preferences	Used bySharePoint to determine language for the user when the multilingual user interface (MUI) feature is enabled.	Yes
msExchHideFromAddressList	SPS-HideFromAddressLists		No
Manager	Manager	User Manager for organization hierarchy	Yes

NOTE

To update additional or custom properties, see Bulk update custom user profile properties.

Frequentlyasked questions (FAQs)

How often are changes synced into the User Profile Application?

User account attribute changes are collected in batches and processed for UPA synchronization. Times will vary based on the amount of changes requested in a single batch. The UPA synchronization is schedule to run at regular intervals.

Will UPA synchronization overwrite existing properties in SharePoint user profiles?

For the default properties that are synced by UPA synchronization, values will be overwritten to align with Azure AD.

Does UPA synchronization update only properties that have changed?

UPA synchronization is driven primarily by changes that are made Azure AD, including adding new users. A full import can occur under certain maintenance events.

Why isn't it possible to map additional properties for UPA synchronization to sync from Azure AD to the User Profile Application?

UPA synchronization is limited to a preconfigured set of properties to guarantee consistent performance across the service.

How to remove deleted users from SharePoint

1/8/2021 • 3 minutes to read • Edit Online

This article describes how to remove deleted users so they no longer appear in SharePoint. It should be used to troubleshoot Profile Property synchronization or mismatched ID issues only as advised by Microsoft Customer Support Services.

- **Scenario 1: Someone is deleted from the Microsoft 365 admin center but still appears in SharePoint.**

  When a user or guest browses to a SharePoint site, their user information is cached in the UserInfo list. When the user or guest is deleted, their related UserInfo information is not removed. Their profile still appears, which may cause confusion when people view the people picker.

- **Scenario 2: Site User ID Mismatch.**

  This issue most frequently occurs when a user is deleted and the account is then re-created with the same user name. The account in the Microsoft 365 admin center or Active Directory (in directory synchronization scenarios) is deleted and re-created with the same user principal name (UPN). The new account is created by using a different ID value. When the user tries to access a site collection or their OneDrive, the user has an incorrect ID. A second scenario involves directory synchronization with an Active Directory organizational unit (OU). If users have already signed in to SharePoint, and then are moved to a different OU and resynced with SharePoint, they may experience this problem.

Delete a user from the Microsoft 365 admin center

For the steps to delete a user in the Microsoft 365 admin center, see Delete a user from your organization.

> **NOTE**
> If you're using directory synchronization, you must remove the user from the on-premises Active Directory environment.

After you delete a user, a series of jobs will remove the user from SharePoint. After the next incremental profile import job, the user (or users) will be marked as deleted, the user's profile page will be deleted, and the user's OneDrive will be marked for deletion by the MySite cleanup job.

Delete a guest from the Microsoft 365 admin center

1. Sign in to https://admin.microsoft.com as a global or SharePoint admin. (If you see a message that you don't have permission to access the page, you don't have Microsoft 365 admin permissions in your organization.)

   > **NOTE**
   > If you have Office 365 Germany, sign in at https://portal.office.de. If you have Office 365 operated by 21Vianet (China), sign in at https://login.partner.microsoftonline.cn/. Then select the Admin tile to open the admin center.

2. In the left pane, select **Users** > **Guest users**.

3. Select **Delete a user**.

4. Select the user, click **Select**, and then click **Delete**.

Delete a guest by using the SharePoint Online Management Shell

1. Install the SharePoint Online Management Shell.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command:

```
Connect-SPOService -Url https://fabrikam-admin.sharepoint.com -Credential $cred
```

4. Remove the guest from each site collection by using the following command:

```
$ExtUser = Get-SPOExternalUser -filter jondoe@fabrikam.com
```

> **NOTE**
>
> Replace the **jondoe@fabrikam.com** placeholder with the account for your scenario.

5. Enter the following command:

```
Remove-SPOExternalUser -UniqueIDs @($ExtUser.UniqueId)
```

Remove people from the UserInfo list

The preceding steps removed access to Microsoft 365 and SharePoint. However, the user or guest still appears in people searches and in the SharePoint Online Management Shell when you use the Get-SPOUser cmdlet. To completely remove people from SharePoint, you must remove them from the UserInfo list. There are two ways to do this:

Site by site in SharePoint

You'll have to browse to each site collection that the user or guest visited, and then follow these steps:

> **NOTE**
>
> This option is available only if the user previously browsed to the site collection. They won't be listed if they were granted access but never visited the site.

1. Browse to the site and edit the URL by adding the following string to the end of it: **/_layouts/15/people.aspx?MembershipGroupId=0**

   For example, the full URL will resemble the following: **https://fabrikam.sharepoint.com/_layouts/15/people.aspx/membershipGroupId=0**

2. Select the person from the list, and then on the **Actions** menu, select **Delete Users from Site Collection**.

Using the SharePoint Online Management Shell

1. Install the SharePoint Online Management Shell.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting

started with SharePoint Online Management Shell.

3. Run the following command:

```
Remove-SPOUser -Site https://fabrikam.sharepoint.com -LoginName jondoe@fabrikam.com
```

> **NOTE**
>
> Replace the *jondoe@fabrikam.com* placeholder with the person in question.

Clear browser history

SharePoint uses browser caching in several scenarios, including in the people picker. Even when a user is fully removed, he or she may still remain in the browser cache. Clearing the browser history resolves this issue. For info about doing this in Edge, see View and delete browser history in Microsoft Edge.

When you clear the browser history, make sure that you also select to clear cookies and website data.

Manage Business Connectivity Service Applications

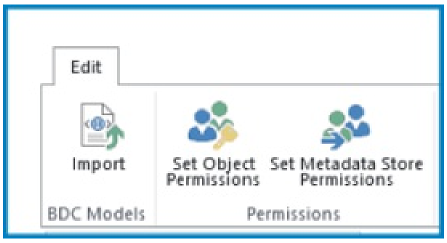
11/2/2020 • 13 minutes to read • Edit Online

In SharePoint in Microsoft 365, you can create Business Connectivity Services (BCS) connections to data sources, such as SQL Azure databases or Windows Communication Foundation (WCF) web services, that are outside the SharePoint site. Once you've created these connections, you can manage or edit BCS information in the SharePoint admin center. Microsoft SharePoint uses BCS together with Secure Store Services to access and retrieve data such as BDC Models from external data systems. See also Deploy a Business Connectivity Services hybrid solution in SharePoint.

Manage BCS permissions

After setup is complete, user permissions control access to the data that the connection provides. BCS has two types of permissions:

- Object permissions
- Metadata Store permissions



Object permissions

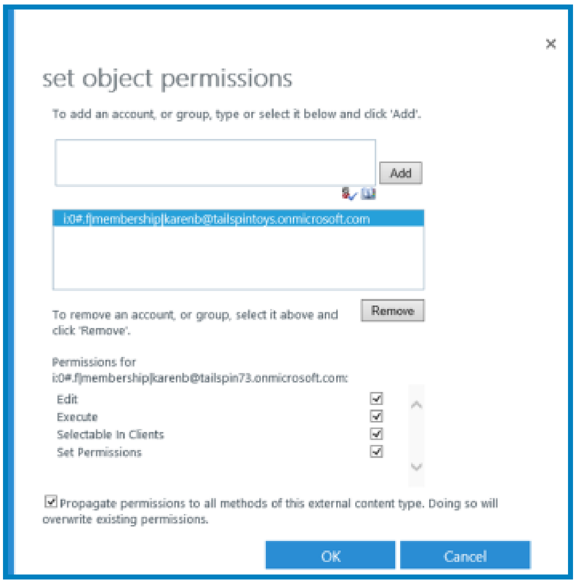
Object permissions apply only to a specific External System, BDC Model, or External Content Type (ECT). Each ECT is a securable object. For example, if you have an ECT called WCFBookSales, object permissions apply only to the WCFBookSales object, and not to any other ECT that might be defined.

To set object permissions for an object, follow these steps.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **BCS**, select **Open**.
3. In the **business data catalog** section, select **Manage BDC Models and External Content Types**.
4. Select the check box next to the name of the ECT or external system that you want to manage.
5. On the ribbon, select **Set Object Permissions**.



6. Enter a user account or group name in the text box, and then select **Add**. You can also select **Browse** to look for the name that you want.

7. Select the name of the account or group for which you want to set access to the ECT or external system. You can set permissions for only one account at a time. If you have multiple accounts or groups, you have to set levels of access for each account separately, by selecting them one at a time.

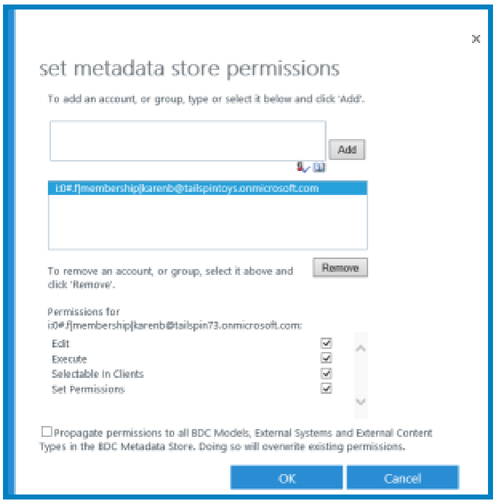
   The following table describes the permissions and their associated access levels.

PERMISSION	NOTES
Edit	Allows the user or group to create External Systems and BDC Models, to import BDC Models, and to Export BDC Models. This setting should be reserved for highly privileged users.
Execute	Allows the user or group to execute operations (create, read, update, delete, or query) on ECTs.
Selectable in clients	Allows the user or group to create external lists for any ECTs, and to view the ECTs in the external item picker.
Set permissions	Allows the user, group, or claim to set permissions on the Metadata Store. At least one user or group must have this permission on every BCS connection so that permissions management can occur. With this permission, a user can grant **Edit** permissions to the Metadata Store. This setting should be reserved for highly privileged users

Metadata Store Permissions

Metadata Store permissions apply globally to the whole BCS store. That is, they apply to all BDC Models, external systems, ECTs, methods, and methods instances that are defined for that external data system. You can set permissions on the metadata store to determine who can edit items and set permissions for the store.

Metadata Store permissions apply to many objects, such as BDC Models, ECTs, and external systems. Because Metadata Store permissions can replace object permissions, they must be managed carefully. When applied with forethought, Metadata Store permissions can grant access quickly and completely.



To set Metadata Store permissions, follow these steps.

1. In the left pane of the new SharePoint admin center, select **More features**.
2. Under **BCS**, select **Open**.
3. Select **Manage BDC Models and External Content Types**.
4. On the ribbon, select **Set Metadata Store Permissions**.
5. Enter a user account or group into the text box, and then select **Add**. You can also select **Browse** to look for the account that you want.
6. The account or group will appear in the second text box. If you have multiple accounts or groups, you must select them one at a time to set the level of access.

PERMISSION	NOTES
Edit	Allows the user or group to create External Systems and BDC Models, to import BDC Models, and to export BDC Models. This setting should be reserved for highly privileged users.
Execute	Allows the user or group to execute operations (create, read, update, delete, or query) on ECTs.
Selectable in clients	Allow the user or group to create external lists for any ECTs, and to view the ECTs in the external item picker.
Set Permissions	Allows the user, group, or claim to set permissions on the Metadata Store. At least one user or group must have this permission on every BCS connection so that permissions management can occur. With this permission, a user can grant Edit permissions to the Metadata Store. This setting should be reserved for highly privileged users.

7. To propagate permissions to all items in the Metadata Store, select **Propagate permissions to all BDC Models, External Systems and External content types in the BDC Metadata Store**. If you select this option, you'll replace all existing permissions (including object permissions) that you may have set anywhere else in your selected BCS Application.

Import or export a Business Data Connectivity (BDC) Model

The BDC Model view allows a user to import and export the underlying framework for the business data connection. This is very useful if you have to re-create the connection in a new environment. A BDC Model file can be imported to create an ECT connection to an external system.

You can import or export two types of model files:

Model Exports the XML metadata for a selected system.

Resource Exports the localized names, properties, and permissions for a selected system.

> **NOTE**
> You can create a BDC Model using XML code. If you do so, it's important to know that you cannot use the authentication modes **RevertToSelf** and **PassThrough** with SharePoint. Although you might be able to import a BDC Model that was written in XML, the connection will not be usable.

Import a BDC Model

When you import a BDC Model, you also import its specified permissions. Before you import a BDC Model, it's a good idea to understand how imported permissions interact with existing permissions.

Imported permissions for a BDC Model are added to the store of existing permissions in the BDC service. If an entry for an object already exists in the access control list, the existing value is overwritten with the permissions information from the imported file.

To import a BDC Model, follow these steps:

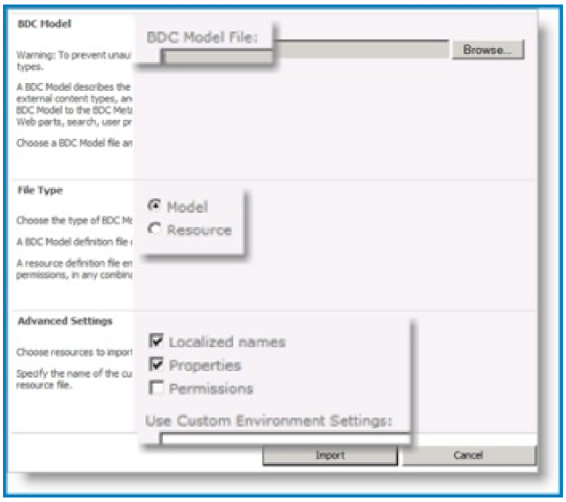
1. In the left pane of the new SharePoint admin center, select **More features**.

2. Under **BCS**, select **Open**.

3. In the business connectivity services section, select **Manage BDC Models and External Content Types**.

4. On the ribbon, select **Import**.

5. In the **BDC Model** section, enter the name of the BDC Model File. The Model name must not include any special characters, such as ~ " # % & * : < > ? \ { | } or the character 0x7f. You can also select **Browse** to locate the *.bdcm file for a BDC Model.



6. In the **File Type** section, select **Model** or **Resource** as the file type that you want to import.

7. In the **Advanced Settings** section, select one or more of the following resources to import:

8. **Localized names** to import localized names for the ECTs in a particular locale. Imported localized names

are merged with the existing localized names by Business Data Connectivity.

9. **Properties** to import properties for ECTs. Imported properties are merged with the existing property descriptions by Business Data Connectivity.
10. **Permissions** to import permissions for ECTs and other securable objects in the model.
11. (Optional) To save the resource settings in a file for later use, type a name for the resource file in the **Use Custom Environment Settings** text box.
12. Select **Import**.

Export a BDC Model

You can export a BDC Model and then read its contents to determine differences between connections. This can be useful if you are troubleshooting. You can also import an exported BDC Model file into another environment for testing or reuse.

To export a BDC Model or Resource file, follow these steps:

1. In the left pane of the new SharePoint admin center, select **More features**.
2. Under **BCS**, select **Open**.
3. Select **Manage BDC Models and External Content Types**.
4. Select the dropdown, and in the **View** group, select **BDC Model**.
5. Select the name of the BDC Model that you want to export, on the ribbon, select **Export**.
6. On the Business Data Connectivity Models page, select the model or resource file to export.
7. On the Export page, in the **File Type** section, to specify the type of file that you want to export, select **Model** or **Resource**.
8. In the **Advanced Settings** section, to further refine the data export, select one or more of the following:

- To export localized names for the ECTs in a particular locale, select**Localized names**.
- To export properties for ECTs, select **Properties**.
- To export permissions for ECTs, select **Permissions**.
- To export an implementation-specific proxy that is used to connect to the external system, select **Proxies**.
  .

9. If you saved a file of resource settings for later use, enter the name of the file to export in the **Use Custom Environment Settings** field.
10. Select **Export** to start a dialog that enables you to save a *.bdcm file to your local drive. You can open the *.bdcm file in a text editor.

Add actions to external content types

By adding actions to ECTs, administrators associate a uniform resource locator (URL) with an ECT. This automatically starts a specified program or opens a specified web page.

Actions can specify parameters that are based on one or more fields in an ECT. For example, you can create an action for an ECT that specifies a Search page URL. The parameter for this action might be the ID of an item in the external data source. This would allow you to specify a custom action for the ECT that automates search for this item.

> **NOTE**
>
> When you add a new action to an ECT, that action is not added to existing external lists for that ECT. The action is only available in new external lists for the ECT.

To add an action to an ECT, follow these steps.

1. In the left pane of the new SharePoint admin center, select **More features**.
2. Under **BCS**, select **Open**.
3. Select **Manage BDC Models and External Content Types**.
4. Point to the name of the ECT to which you want to add an action, and then select the arrow that appears. From the menu, to open the **Add Action** page, select **Add Action**.
5. In the **Name** field, give the action a meaningful name.
6. In the URL field, for the action you want to open, enter the URL.

    > **NOTE**
    >
    > Under the control, you can find an example URL. The example shows how to add one (or more) parameter place-holders such as {0}, or {1} (http://www.adventure-works.com/sample.aspx?p0={0}&p1={1}).

7. If you want web parts on the site to be able to use this new action, select one of the following options:

COMMAND	ACTION
Yes	Starts the action in a new browser window (preserves the page context).
No	Starts the action in the same browser window.

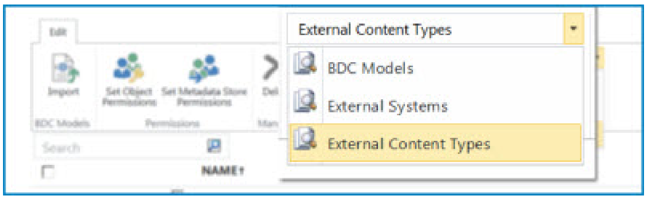
8. In the **URL Parameters** field, specify any parameters that are required by the URL. These are numbered in the interface starting at 0.
9. Decide if you want to use an **Icon** or not. This field also allows you to use Standard icons.
10. If you want the action to be the default action, select the **Default Action** check box.

    > **IMPORTANT**
    >
    > Parameters can contain personally identifying information such as names and Social Security numbers. When you design an action, be careful not to use fields that display personally identifying information.

View external data and external data settings

You use the **View** section of the ribbon to choose different views of BCS connections. The three views display information about the BCS connection in different ways, and give you access to different actions. It is important to become familiar with these views because some tasks are available only in specific views.

The three view options are BDC Models, External Systems, and External Content Types, as shown in the following illustration.

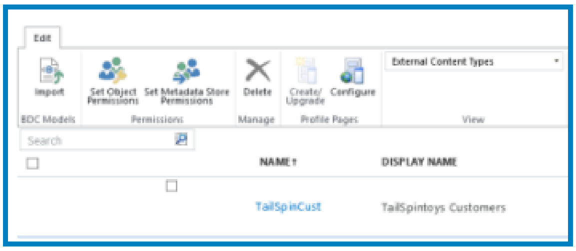


For more information about how you can use these views to help manage BCS, see the sections that follow.

External Content Types view

By default, the BCS connection uses the **External Content Types** view. This view shows Service Application Information, and lists the following information:

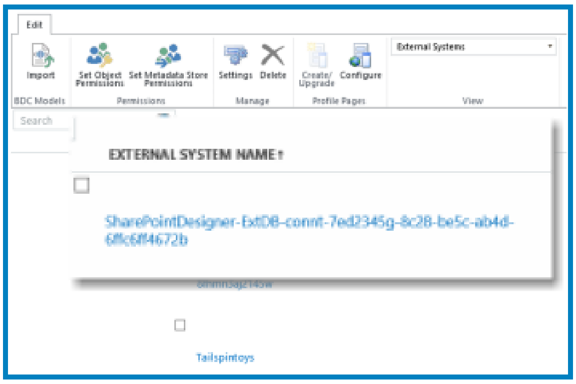
- ECT name
- ECT display name
- ECT type namespace
- Namespace version
- External system name



For most processes in BCS, this view is sufficient. However, if there are many ECTs, this view can be difficult to navigate.

External Systems view

The **External Systems** view shows a BCS connection in terms of its system of origin. This view is useful if you want to know the BCS connection information after you create the BCS. In this view, you can see the property settings for a named External System. In addition, you can configure some of the property settings.



View property settings

The name of the External System appears on this page as a selectable link (a navigable URL). You can select the URL to open a window that shows the original property settings for that store. In addition, if you are connected to SQL Azure, you can see the database server name and database, in this view.

Depending on the type of BCS connection, the property settings can include any combination of the following items:

- Access Provider (such as WCF Service)

- Authentication Mode (such as User's Identity)
- Database Server
- Impersonation Level (such as None, Anonymous, Identification, Impersonation, Delegation)
- Initial Database name
- Integrated Security (such as SSPI)
- Secure Store Implementation
- Secure Store Target Application ID (as the ID entered in Secure Store)
- Service EndPoint Address (such as the URL pointing to SomeWCFService.svc)
- Connection Pooling (Active/Inactive)
- Secondary Secure Store Target Application ID
- Secure Store Implementation

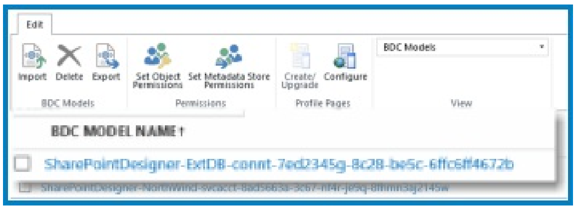
Configure property settings

If you point to an External System Name, you can open a shortcut menu that includes a **Settings** command. This is useful for SharePoint connections that use Windows Communication Foundation (WCF) Web Services. By selecting the **Settings** option from the menu, you can configure any of the following settings:

- Metadata Exchange URL
- Metadata Exchange Discovery Mode
- Web Services Description Language (WDSL) Authentication Mode
- WSDL Secure Store Target Application Id
- Secure Store Implementation.

BDC Model view

The **BDC Model** view offers ribbon commands that enable you to import or export BDC Models. In addition, the BDC Model view can make it easier to move around in a very large collection of ECTs. Because the BDC Model shows hyperlinks for each distinct connection, rather than showing all ECTs for each connection, it can make a more manageable list.



If you want to see all the ECTs for a BDC Model, select the name of the Model. If you select the name of an ECT, open a table that shows the fields that are defined for the ECT. It resembles the following table.

NAME	TYPE	DISPLAY BY DEFAULT
Order Id	System.String	No
Employee Id	System.String	No
Freight	System.Nullable '1[[System.Decimal, ...	No

This display can closely mirror the layout of the data source connected via an ECT, and give better insight into the structure of the underlying data.

Also, at the bottom of the page, any Associations, Actions, or Filters for this ECT appear.

Create or edit a Secure Store Target Application

11/2/2020 • 6 minutes to read • Edit Online

When you want to use external data (such as data from your other business applications or partner resources) in SharePoint, you can use Business Connectivity Services (BCS) together with Secure Store. And, you can manage BCS and Secure Store right in the SharePoint admin center. The external data source that you can connect to is called a Secure Store Target Application, or just a Target Application.

BCS makes it possible for you to set up a connection to the Target Application, and the Secure Store enables you to manage the credentials that are required by the external data source.

> **NOTE**
> To access the Secure Store, you must have the SharePoint Admin role or Global Admin role.

How the Secure Store Service Works

This SharePoint service makes access to external business application data easier. In order to understand why the Secure Store Service offers this benefit, it's important to understand that the username and password used to access external data stores may not be the same as the username and password used to access SharePoint. When a user accesses a SharePoint page that displays information from an external data system, SharePoint must make a separate request to retrieve information from the external data system. This must be made with credentials that are known to the external data system in order for the request for content to be successful. Only then can SharePoint display the information from the external data system on the page. The Secure Store Service stores the external data system credentials for this reason.

The Secure Store Service is designed to create a background mapping between a group of users in SharePoint, and a single user known to the external data system. When the Secure Store Service is properly configured, the following occurs:

- A user authenticates through Internet Information Services (the web server technology underlying SharePoint technologies) to SharePoint via valid credentials.
- Inside SharePoint, the Secure Store Service uses mapped credentials known to the external business application to render any necessary external data on the site for the authenticated user.

Another benefit of the Secure Store Service is that it eliminates authentication prompts for users. When users navigate to SharePoint pages that access external data systems, the Secure Store Service is active in the background, checking user rights and providing mapped credentials to the external data when appropriate. This allows users to access the required data without prompting them to enter usernames and passwords specific to the external application.

Create a Target Application

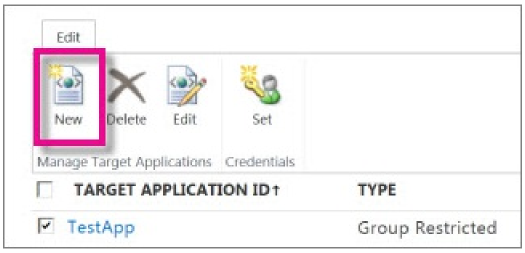
1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

NOTE

If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Secure store**, select **Open**.

3. In the **Manage Target Applications** group on the ribbon, select **New**.



4. In the **Target Application Settings** section, enter values for the following fields:

5. **Target Application ID**. You might find it useful to assign a meaningful name. For example, if you are connecting to source that contains employee data, you might enter EmployeeTargetApp.

6. Display Name. This field should be a user-friendly name for the Target Application. For example, you might use Employee Data.

7. **Contact E-mail** Enter a valid email address for people to use when they have questions.

8. **Target Application Type**. By default, SharePoint uses type **Group Restricted**.

9. In the **Credential Fields** section, for the credentials that are required to access data in the Target Application, enter the **Field Names** and **Field Types**. These fields determine how you will map identity in the Secure Store Service. By default, the Credential Fields list the Windows User Name and Windows Password with matching Field Types (User Name and Password), and specifies that the password is masked.

10. In the **Target Application Administrators** section, enter a list of users, or to search for the name of a group, select **Browse**. This section usually contains the account of the SharePoint admin, or a global admin.

11. In the **Members** section, enter a list of users or SharePoint groups of users who need to access the target app. Or, to search for the name of a group that you want to map to the Target Application, select **Browse**.

12. Select **OK** to accept this configuration and return to the Secure Storage Service page. The new Target Application appears on the page.

Edit settings for a Target Application

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Secure store**, select **Open**.

3. From the list of Target Applications, select an existing Target Application.

4. On the ribbon, select **Edit**.

> **NOTE**
>
> Some fields on the Edit page are not available. These elements cannot be edited. After you create a Target Application, you can't change the **Target Application ID**, **Target Application Type**, or **Credentials Fields**.

5. Select any of the following to edit the contents:

- Display Name
- Contact E-mail
- Target Application Administrators
- Members

6. Select **OK**.

Set credentials for a Target Application

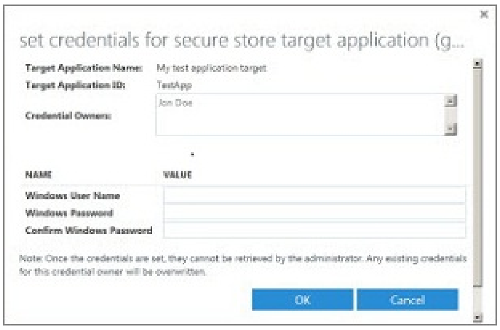
1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Secure store**, select **Open**.

3. Select a single Target Application from the list if you have created more than one.

4. In the **Credentials** group on the ribbon, select **Set**. This opens the **Set Credentials for Secure Store Target Application (Group)** dialog. When you set credentials, you map a Target Application Group to a single set of credentials for an external data system.



5. In the **Set Credentials for Secure Store Target Application (Group)** dialog, enter the credential values that you want. The credential fields that you enter apply to the external data system.

> **NOTE**
>
> The following fields cannot be edited. These fields specify the Secure Store mapping for the Target Application: **Target Application Name**, **Target Application ID**, and **Credential Owners**.

> **IMPORTANT**
>
> Be careful when you enter the password. If you enter a password that is incorrect, you won't see a message about the error. Instead, you'll be able to continue with configuration. However, errors can occur later, when you attempt to access data through BCS. Also, if the password for the external data source is updated, you have to return to this page to manually update the password credentials.

6. When you finish entering values for credential fields, select **OK**.

Make an External List from a SQL Azure table with Business Connectivity Services and Secure Store

1/8/2021 • 13 minutes to read • Edit Online

As a SharePoint or global admin in Microsoft 365, you can use services in Microsoft SharePoint to access data from a Microsoft SQL Azure database. Because SQL Azure is a cloud-based relational database technology, the connection works completely in the cloud. This article describes how to use SharePoint technologies to access data from a SQL Azure database without having to write code.

To use data from a SQL Azure database, you have to create an External List by using Business Connectivity Services (BCS) and Secure Store. BCS connects SharePoint solutions to external data, and Secure Store enables user authentication for the data. By using an External List, you can display the contents of a table from SQL Azure in SharePoint. Users can read, edit, and update the data, all in SharePoint.

For more information about how to use BCS to use external data, see Introduction to external data.

SQL Azure databases are cloud-based relational databases that are created by using SQL Server technology. To learn how to get started with these databases, see Getting Started with Microsoft Azure SQL Database Using the Microsoft Azure Platform Management Portal

Overview of steps in the process

To create an External List that enables you to access data from SQL Azure, you have to complete a sequence of separate steps.

The following table lists the steps and the required software for that step.

WHAT TO DO:	WHERE TO DO IT:
Step 1: Set permissions on the BCS Metadata Store	SharePoint admin center
Step 2: Create a Secure Store Mapping	SharePoint admin center
Step 3: Create an External Content Type (ECT)	SharePoint Designer 2010 OR Visual Studio
Step 4: Create an External List	SharePoint admin center
Step 5: Grant permissions to manage your ECT	SharePoint admin center

How BCS and Secure Store work together

Business Connectivity Services (BCS) connects to data in an external data store. You can display the data in an External List, and maintain the data elsewhere. BCS enables you to connect SharePoint solutions to two kinds of resources:

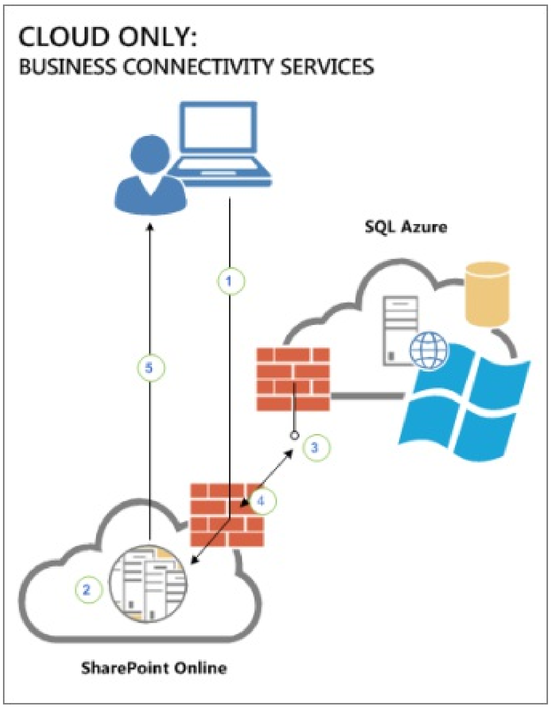
- A SQL Azure database
- A WCF web service that acts as an end-point for some other kind of data store

BCS enables you to access an external data source by using the Secure Store. Secure Store keeps encrypted copies of credentials. It enables a SharePoint admin to associate a SharePoint group that uses a single SQL Azure account that can access the target database. When a SharePoint user browses the data in the External List, Secure Store uses the associated SQL Azure account to request the data from SQL.

To make this possible, a SharePoint admin defines an External Content Type (ECT) in SharePoint Designer or in Visual Studio. Then, someone with appropriate permissions creates an External List on a SharePoint site by referencing the ECT. Users who have appropriate permission can view or update the list.

> **NOTE**
>
> SharePoint in Microsoft 365 doesn't support offline use of external lists.

This illustration shows how the connections between the different elements occur:



The following list describes the steps in the connectivity process. Each step in this list corresponds to a number in the previous diagram.

1. The user signs in to SharePoint and opens an External List. The Business Data Connectivity (BDC) service in SharePoint queries External Content Type for that list in the BDC metadata store that contains the list. The query asks for the following information: how to access the external system, which operations are supported, and what credentials to use.

2. The BDC service runtime sends the request (SOAP over HTTP) to the endpoint of the SQL Azure Windows Communication Foundation (WCF) service.

3. The SQL Azure service returns the data in a SOAP envelope.

4. The SharePoint site displays the external list in the user's browser. The user can then perform all the configured operations on the data source for which the user has permissions.

Step 1: Set permissions on the BCS Metadata store

To do this step, follow the procedure in Set permissions on the BCS Metadata Store for a Business Connectivity Services on-premises solution in SharePoint 2013.

When you finish the steps in that procedure, return to this page and start Step 2: Create a Secure Store credentials mapping.

Step 2: Create a Secure Store credentials mapping

Typically, when you create a credentials mapping in Secure Store, you map multiple SharePoint users to a single SQL Azure account. You might use a SharePoint group, or just list all the user names. The SQL Azure account has appropriate permissions to access the target database table. The database that you target in SQL Azure is known as the Secure Store Target Application, or just the Target Application.

> **TIP**
>
> Make sure that you have SQL Azure credentials ready. You'll use these credentials when you create the mapping between SharePoint users and a SQL Azure account.

Create the Secure Store Target Application

To create a Secure Store Target Application, follow these steps.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Secure store**, select **Open**.

3. On the ribbon, to open the page where you can specify settings for a Target Application, select **New**.

4. In the **Target Application Settings** section, do the following:

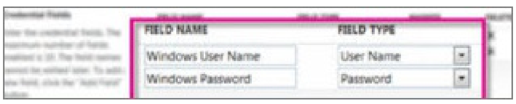
- Under **Target Application ID**, specify a value for a unique ID. This ID maps the External Content type to credentials that are required to authenticate the user. You cannot change the Target Application ID once you create the Target Application.

- Under **Display Name**, specify a user-friendly name for referring to the Target Application.

- Under **Contact E-mail**, specify the email address that you want people to use when they have a question about the Target Application (external data system).

- Under **Target Application Type**, verify that the value is set to **Group Restricted**. Group Restricted means that the Secure Store contains a mapping that connects a group of SharePoint users to a single, external data account that can act on their behalf. In addition, a Group Restricted application type is restricted to the specified external data system.

5. In **Credential Fields** section, enter the field names that you want to use for the user name and password of the external data system. By default, the Secure Store uses the **Windows User Name** and **Windows Password**. We recommend that you accept these values. You cannot edit these Field Types after you finish creating the application.



6. In the **Target Application Administrators** section, in the **Target Application Administrators** field, enter the name of a group or a list of users who can edit this Target Application. You can also search for

the name of a group in Microsoft Online Directory Server. Typically, this section usually contains the name of the SharePoint or global admin.

7. In the **Members** section, in the **Members** field, enter the name of the group that will use the Target Application. Generally, this is a group from the Microsoft Online Directory Service (MSODS).

   If you are a global admin, you can create groups in MSODS in the Microsoft 365 admin center.

8. To create the Target Application, and return to the **Secure Store Service** page, select **OK**.

Store credentials for the Target Application

After you create the Target Application, you are ready to enter the credentials that Secure Store uses to access the external data. To set the credentials, follow these steps

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

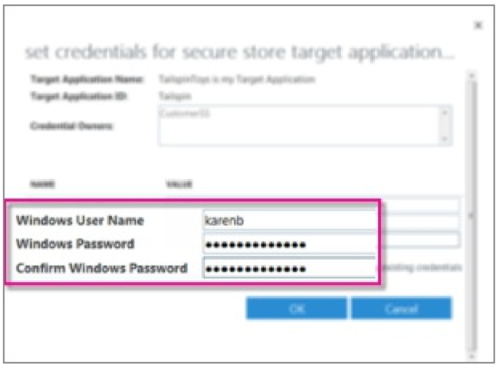
> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Secure store**, select **Open**.

3. Select the arrow next to the new Target Application, and then select **Set Credentials**.

4. In the **Set Credentials for Secure Store Target Applications (Group)** dialog, enter the user name and password of the account. The account must have access to the target database. In the following image, the username is **Windows User Name**, and the password is **Windows Password**.

   > **IMPORTANT**
   > Keep a secure record of this information. After you set these credentials, an administrator cannot retrieve them.



Step 3: Create the External Content Type

You can create an External Content Type (ECT) by using Microsoft Visual Studio, or by using Microsoft SharePoint Designer 2010. This procedure describes how to create an ECT in SharePoint Designer 2010. Microsoft SharePoint Designer 2010 is available as a free download from the Microsoft Download Center.

You must be a SharePoint or global admin in your organization to perform this task.

To create an ECT, follow these steps.

1. Start Microsoft SharePoint Designer.

2. To open the SharePoint team site at the root collection, select **Open Site**. The URL for the root collection will resemble this example URL: https://tailspintoys.sharepoint.com. SharePoint might display a prompt for valid credentials.

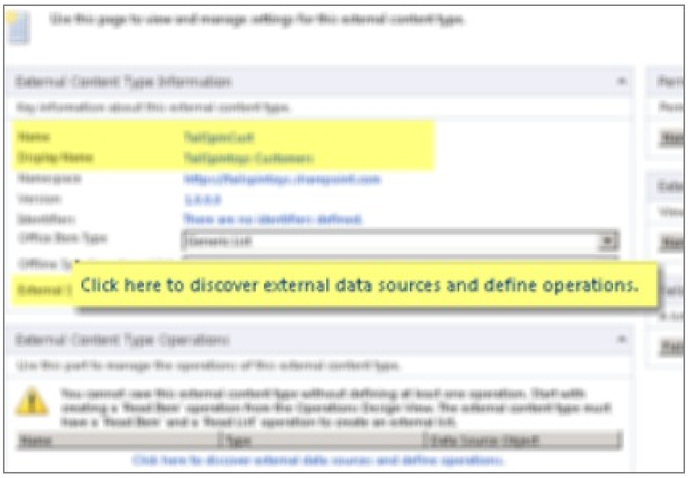
> **NOTE**
>
> If SharePoint displays a prompt for you to add a new user, ensure the user account you use has sufficient permissions. The user account must be able to make and test BCS changes to the SharePoint site. Typically, a SharePoint or global admin performs these steps.
> If you want to change to a different user, select **Add a new user**, select **Personal** or **Organization**, sign in to the site as the SharePoint or global admin, and select **Sign In**.

3. After the site opens, in the **Site Objects** tree on the left of the application window, select **External Content Types**.

4. Select the **External Content Types** tab, and in the ribbon, to begin the creation process, select **External Content Type**.

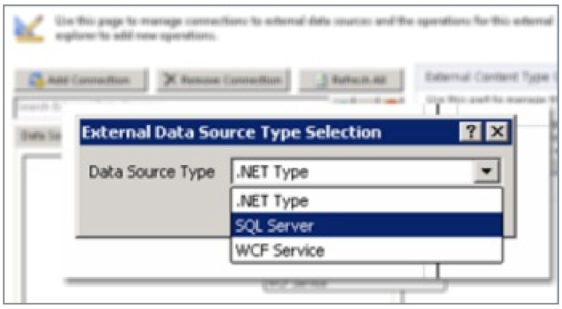
5. In the **External Content Type Information** section of the page, change the **Name** and **Display Name**. Make certain that the **Name** is descriptive. The **Display Name** is a friendly name for the ECT.

6. To open the Operation Designer page, select the link **Click here to discover external data sources and define operations**.



7. To open the **External Data Source Type Selection** dialog, select **Add Connection**.

8. To access the SQL Azure database, select **SQL Server**.



NOTE

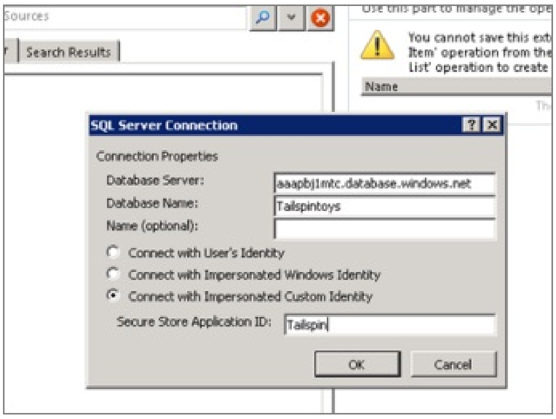
You cannot use on-premises data sources, such as .NET Type, with SharePoint in Microsoft 365. In addition, you cannot use a SQL Server data source that is on-premises with SharePoint in Microsoft 365.

9. When you select SQL Server, specify the following:

   - **Database Server name**
   - **Database Name**
   - **Name**

IMPORTANT

The URL you use to access the database contains the Fully Qualified Server Name. For example, if you access the database via https://aaapbj1mtc.database.windows.net your Fully Qualified Server Name is **aaapbj1mtc.database.windows.net**. > If you log on at a higher level, such as the Management Portal for Microsoft Azure, you can discover the Fully Qualified Server Name. On the portal page, under **Subscriptions**, select the name of your subscription. Then, under **Fully Qualified Server Name**, expand your subscription and the server name. Names of databases appear under each server name.

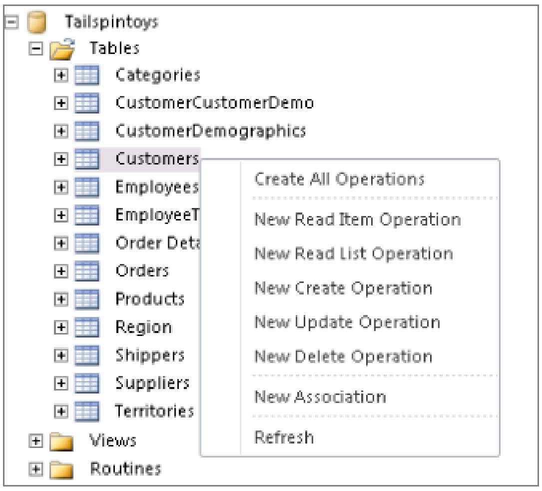


In the **SQL Server Connection** dialog, select **Connect with Impersonated Custom Identity**. Then, in the **Secure Store Application ID** text box, type the Secure Store Application ID that stores credentials for the target database and then select **OK**.

10. If you see a prompt for credentials to access the external data source, to access the external data system, enter the correct **User name** and **Password** credentials. Then, to connect, select **OK**.

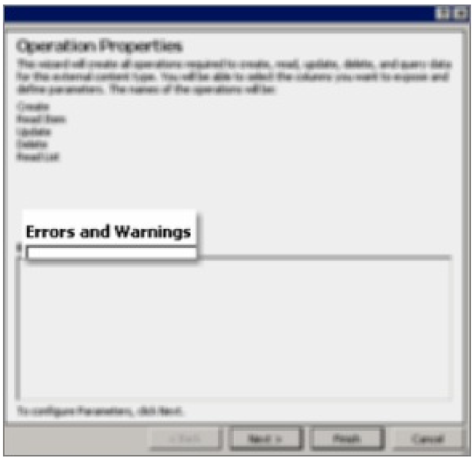
    The **Data Source Explorer** tab, you can view a list of tables that are available from the SQL Azure database. To see a list of possible operations for this table, open the shortcut menu for the table.

    You can select specific options such as New Read Item Operation and New Update Operation for the table. Or, you can just select **Create All Operations**.

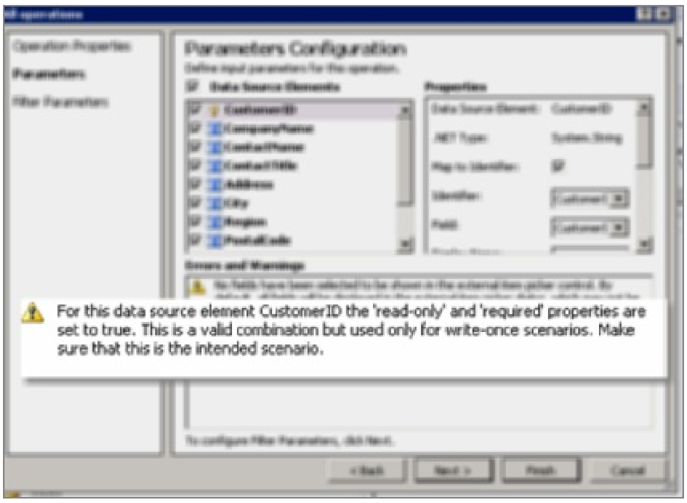


11. To open a wizard, select **Create All Operations**, and then select **Next**.

    On the **Operation Properties** page of the wizard, in the **Errors and Warnings** pane, read about any issues. It is important to resolve reported issues that you see. For example, you may have to choose a field to show in an external item picker control. For a customer table, you could choose the customer name.



> **IMPORTANT**
>
> The wizard may display a warning message if unique, required fields, such as 'CustomerID', exist in the target table. This is valid if the specified field is required and unique in the table, such as a primary key.



> **NOTE**
>
> For more information about how to define filters in external content types, see How to: Define filters for External Item Picker controls .

12. To accept the operations properties that you configured, select **Finish**. SharePoint Designer displays the operations as a list of ECT Operations.

When this step is complete, you are ready to create an External List to use the data from the external source.

Step 4: Create an External List

You can create an External List by using SharePoint Designer, or by adding an External List as an app on the SharePoint team site. This procedure describes how to create an External List from the team site in SharePoint.

Create an External List by using SharePoint

1. Go to the home page of the SharePoint team site.
2. Select **Settings** > **Add an app**.
3. On the **Your Apps** page, in the search dialog, enter **External List**, and search.
4. To open the **Adding External List** dialog, double-click the **External List** tile.
5. In the **Name** box, enter a name for the list.
6. In the **External Content Type** box, enter the name that you want to use. For example, you might use the name of the ECT that you created in SharePoint Designer. Alternatively, you can select the database icon to browse for the name of an ECT.
7. Select **Create**.

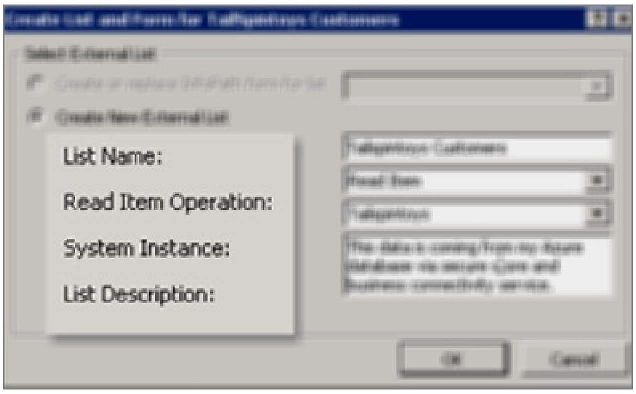
Create an External List by Using SharePoint Designer 2010

1. In SharePoint Designer 2010, on the ribbon, select **Create Lists and Forms**.

   SharePoint Designer may display a message that states, "Creating lists and forms requires the external content type to be saved". select **Yes** to save the ECT.

   In the **Create List and Forms for databasename Customers** dialog, in the **List Name** text box, enter a meaningful name for the External List. For example, if you created an ECT for the "Customers" database table, you might use "Tailspintoys Customers" in the list name.

2. From the list of Operations, select a **Read Item Operation**.
3. In the **System Instance** text box, enter the name of the SQL Azure database.



4. To create the External List in the SharePoint site, select **OK**, and then select **Save**.

Step 5: Grant permissions to manage the ECT

To finish setting up the External List, you have to grant permissions to the people who will use the list. To grant permissions, follow these steps.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

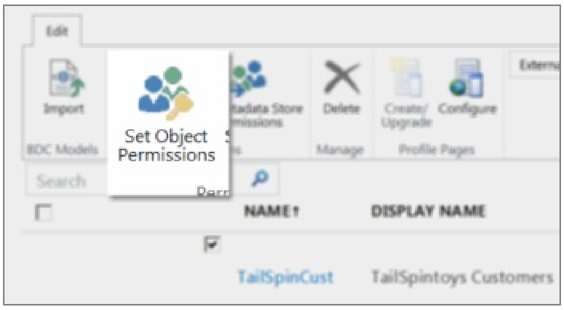
> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **BCS**, select **Open**.

3. Select **Manage BDC Models and External Content Types**.

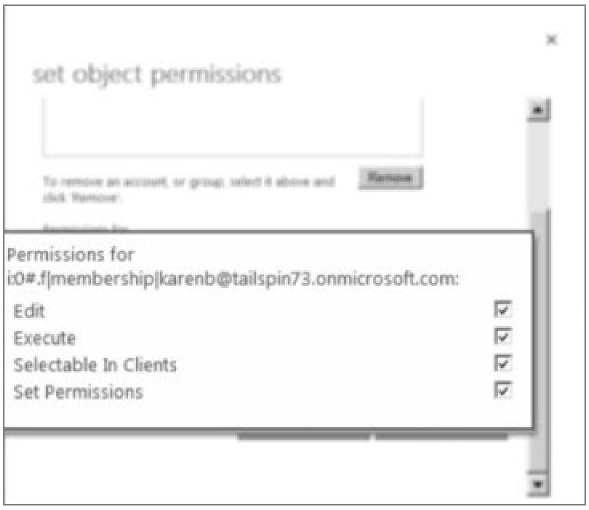
4. Select the check box next to the name of the ECT that you just created, and then select **Set Object Permissions**.

> **IMPORTANT**
>
> You must manually assign permissions to manage the ECT to a global or SharePoint admin by using the **Set Object Permissions** command. If you do not assign these permissions explicitly, the admins won't have permission to manage the ECT.



5. In the **set object permissions** dialog, select the check boxes for all the permissions ((**Edit, Execute, Selectable in Clients, and Set Permissions**) that the SharePoint admin needs.

> **NOTE**
>
> Make sure that at least one user or group has **Set Permissions** rights. If you don't assign someone this right, you might create an unmanageable BCS connection.



6. Select **Propagate permissions to all methods of this external content type**. Doing this overwrites any existing permissions.

> **NOTE**
>
> If you want to add a group that can use the External Lists, you must also give the group **Execute** rights. That enables users in the group to run a query to the external source, and view the results in SharePoint.

Manage app licenses for a SharePoint environment

4/22/2020 • 3 minutes to read • Edit Online

As a SharePoint or global admin in Microsoft 365, you can use the SharePoint admin center to manage licenses for apps purchased from the SharePoint Store, regardless of whether you purchased them. All apps available from the SharePoint Store have built-in licenses that SharePoint recognizes. An app license provides digital verification of a user's right to use an app.

It is important to keep track of the number of licenses that are available for each app so that the number of app users does not exceed the number of available licenses. If necessary, you can buy additional licenses for an app.

From the admin center, you can also add users to an app, or delegate management of a license to someone else.

> **NOTE**
> The Office and SharePoint App Stores are optional services operated by Microsoft Corporation or its affiliate from any of Microsoft's worldwide facilities. The apps available in the Store are provided by various app publishers, and are subject to the app publisher's terms and conditions and privacy statement. Your use of any of these apps may result in your data being transferred to, stored, or processed in any country where the app publisher, its affiliates or service providers maintain facilities. Availability of specific apps and payment methods depends on your region and service. You can review the app publisher's terms and conditions and privacy statements before downloading and using such apps.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Apps**, select **Open**.
3. Select **Manage Licenses**.
4. In the list of apps, select the app you want to update or view.
5. On the Manage App License page, you can review the details about the app license, such as the number of licenses available for users or the license type. You can also take a number of actions.
6. Do any of the following:

TO DO THIS:	DO THIS:
Assign licenses to specific users	Under **People with a License**, select **assign licenses**, enter the name(s) of the people you want to add, and then select **Add User**.
Buy more licenses	Under **People with a License**, select **buy**, and then follow the steps to sign in with your Microsoft account to buy the additional number of licenses than you want.

TO DO THIS:	DO THIS:
Remove app licenses	Under **View a purchase**, select the arrow next to **Actions** and then select **Remove this license**.
Recover app licenses	When you recover a license, you basically reacquire it from the SharePoint Store. You might need to do this if your license gets out of sync with Office.com or if you are moving the license to a new deployment (for example, in a disaster recovery scenario).
Under View a purchase, select the arrow next to Actions, and then select Recover license. On the Details page for the app in the SharePoint Store, select More Actions, and then select Recover license again. When prompted, sign-in with your Microsoft account.	
Add a License Manager	
In the License Managers section, select add manager. Type the name(s) of the people you want to add (or select the address book icon to select people). When you have finished typing or selecting names, select Add Manager underneath the text box.	

NOTE

If this is a free app, some of the actions in the table above will not apply.

A user cannot grant an app permissions to do more than that user has permissions to do.

See also

Add an app to a site

Buy an app from the SharePoint Store

Monitor apps for your SharePoint environment

4/22/2020 • 2 minutes to read • Edit Online

As a SharePoint or global admin in Microsoft 365, you can monitor information such as app usage and error information for the apps that are in use in your SharePoint environment. Before you can monitor information about an app, you need to add it to the list of apps you want to monitor.

Select apps to monitor

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Apps**, select **Open**.
3. Select **Monitor Apps**.
4. To add apps to the list, select **Add App**.
5. Search for the app(s) you want to add, or select from the list of available apps, and then select **Add**.

View app details or errors

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Apps**, select **Open**.
3. Select **Monitor Apps**.
4. Point to the app for which you want to view info, select the check box that appears, and then do one of the following:

TO DO THIS:	DO THIS:
View the details about the app such as: number of licenses purchased or used counts of errors and installs usage info	On the ribbon, select **View Details**. In the **Usage** section, to change the timeframe for the usage info that displays in the chart, select **Days**, **Months**, or **Years**.
View error information for an app	On the ribbon, select **View Errors**. To find the errors in the error log, use the Correlation ID. In the **Location** column, to view more error details for this app, select the URL.

NOTE

If you no longer want to monitor an app, you can select it on the Monitor Apps page, and on the ribbonm select **Remove App**.

App usage and error detail info is processed by different timer jobs that are pre-configured to run at set times for SharePoint. These timer jobs pick up events for the previous day. For this reason, the data visible on the Monitor Apps page may be delayed for up to 29 hours.

Request app installation permissions

4/22/2020 • 3 minutes to read • Edit Online

Apps are small, easy-to-use web applications that add functionality to SharePoint sites. They offer unlimited possibilities for customizing your sites in ways that are specific to your organization. For example, you can add apps that perform general tasks such as time and expense tracking, or apps that make it easy for customers to contact you, or productivity apps that enable you to establish data connections and develop reports for your stakeholders.

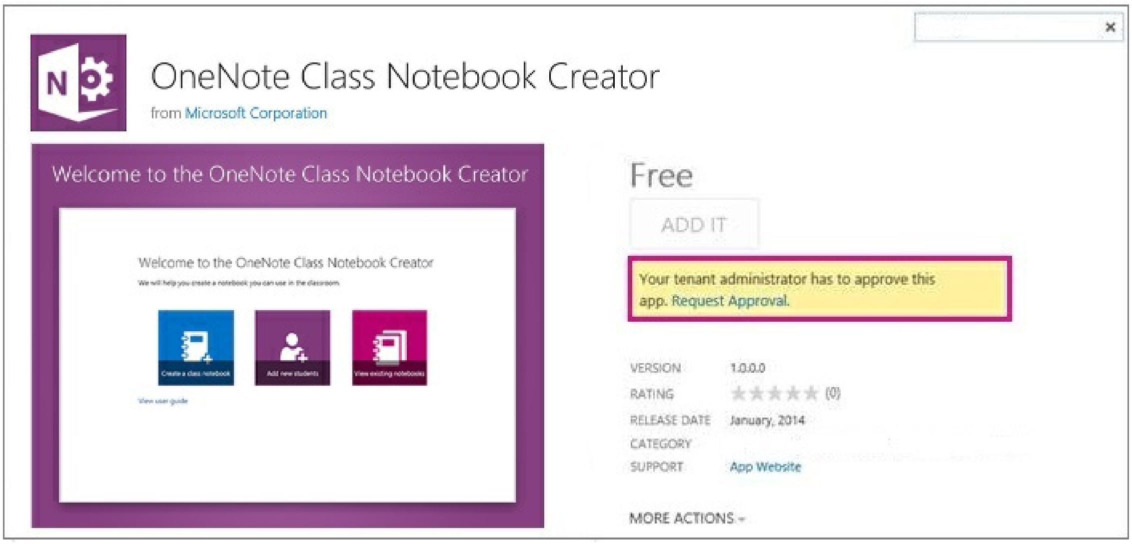
Some apps are included with SharePoint, others might be developed by your organization, and still others are created by third-party developers and available for purchase from the SharePoint Store.

Only those users who have the appropriate permission level can add apps to a site. Typically, Full Control permission (or membership in the Site Owners group) is the minimum requirement. But some apps require access to data sources or web services to read data required for the app. This kind of app has permissions associated with it. When the app requires organization-level permissions, the requestor will need approval from a Microsoft 365 admin to continue with the installation. The approval process includes a workflow, called the permission request flow, which ensures installation requests are directed to the right person.

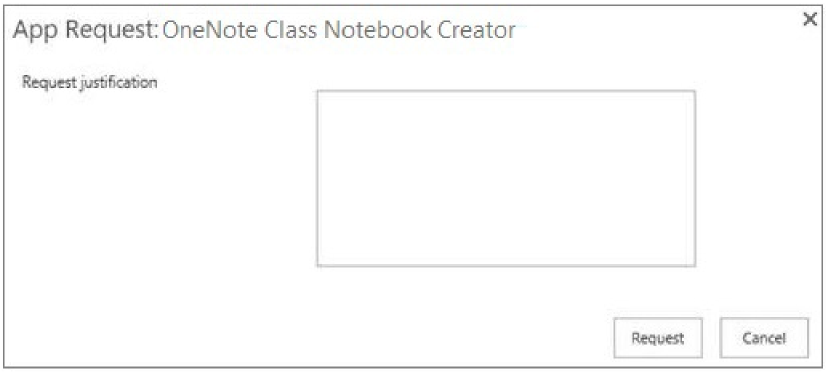
This article is intended for global admins and SharePoint admins at the organization level who receive requests for app installation.

How the permission request flow works

When users encounter an app that requires admin permission to install, they'll see a **Request Approval** link on the app details page.



Clicking the link displays an **App Request** dialog where they provide justification for the request.



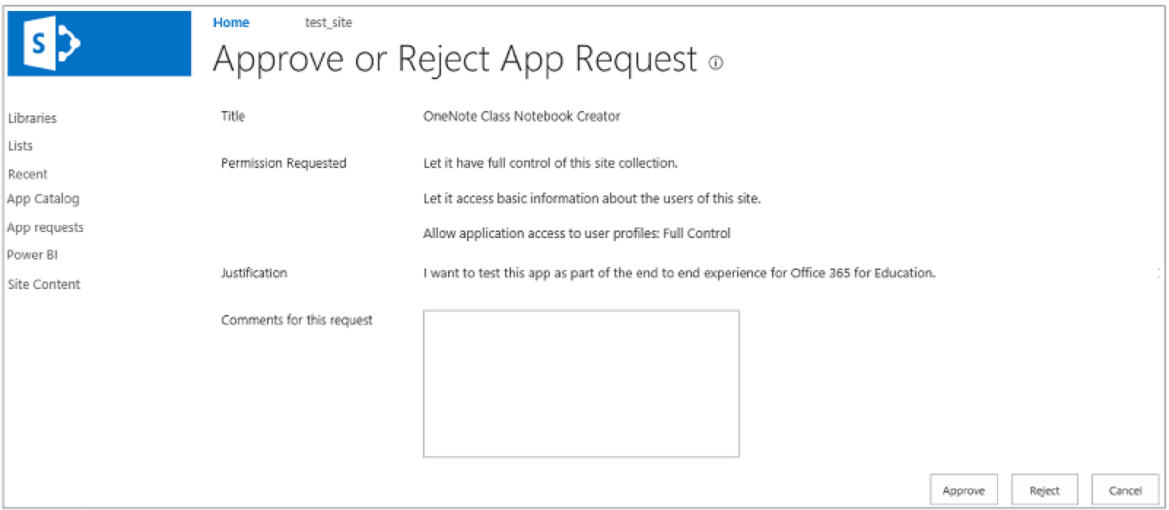
When they click **Request**, an automated email is sent to everyone who is a site collection admin for the app catalog.

> **NOTE**
>
> Sometimes, depending on the Office Store settings, the **App Request** dialog will include a place for users to indicate the number of licenses required along with the justification. See Configure settings for the SharePoint Store for more information.

Approve or deny requests

1. In the auto-generated email that you receive for the request, click **You can now approve or reject the request here**.
2. On the **Approve or Reject App Request** screen, in the **Comments** box, provide relevant information about your decision.
3. Either select:

- **Approve** to approve the request and send an auto-generated email to the requester.
- **Reject** to deny the request and send an auto-generated email to the requester.

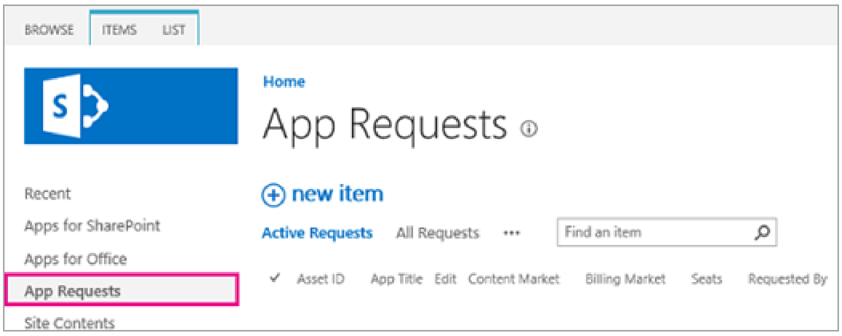


The app catalog is where you store and manage all apps for the organization. There you can see a list of all pending app installation requests.

View all requests

1. Browse to your app catalog. (In the SharePoint admin center, select **apps** in the left pane and then click the **App Catalog** link.)
2. Click **Settings** > **Site settings** > **Site Collection Administration** > **Manage App Requests**.

3. In the left nav, select **App Requests**.



4. Click the title of each pending request to review it. Once the request is approved or denied, it is removed from the view. If you change your mind about allowing an app or apps to be added to you sites, you can revoke approval on the request. To revoke approval for a request, choose the request and click **Remove Approvals**.

Make the application available

Once the status has been changed to **Approved**, go to the SharePoint Store and acquire the app. This is done by clicking the link next to **View App Details** on the App Request entry.

At this point, site owners can check the **Your Requests** list to view the status of their request. After the application has been acquired and approved, it will show up in the **Apps you've requested** list.

Delegate approval authority

As a global admin or SharePoint admin in your organization, you can delegate app approval authority as a way of spreading the approval work around, or alleviating approval bottlenecks. Remember that apps are stored and managed in the app catalog, and the app catalog is a site collection. Therefore, to grant app approval permission to select users, you add them to the site collection administrator group on the app catalog.

Caution

When you promote users to site collection administrators on the app catalog site collection, you are giving them the ability to approve the installation of apps that have organization-wide impact. Consider this decision carefully.

Add site collection admins to the app catalog

1. Browse to your app catalog. (In the SharePoint admin center, select **apps** in the left pane and then click the **App Catalog** link.)

2. Select **Settings** > **Site settings** > **Users and Permissions** > **Site collection administrators**.

3. Type the name of the group or individuals who you want to add as site collection administrators.

4. Select **OK**.

Use the App Catalog to make custom business apps available for your SharePoint environment

6/30/2020 • 7 minutes to read • Edit Online

As a SharePoint or global admin in Microsoft 365, you can create an App Catalog site to make internally developed custom apps available for users to install when they browse apps under the **From Your Organization** filter on the Site Contents page. Site owners can then add these apps to customize sites with specific functionality or to display information.

After the App Catalog site has been created, you can use it to upload any custom apps that your organization has developed. Uploading custom apps isn't much more complicated than uploading a document to a library and setting some properties. You can use the App Catalog site to do things like install custom or third-party apps on sites for users (also called app deployment). You can also manage app requests from users.

For more information about your options for developing custom apps for SharePoint, see: Build apps for SharePoint and Apps for SharePoint compared with SharePoint solutions.

Step 1: Create the App Catalog site collection

The first step is to create the App Catalog site collection if it hasn't already been created.

Even if you don't plan to make internal custom apps available, you will not be able to do things like change the purchase settings for the SharePoint Store until you create the App Catalog site collection. You can have only one App Catalog site collection for your organization, and you only need to create it once.

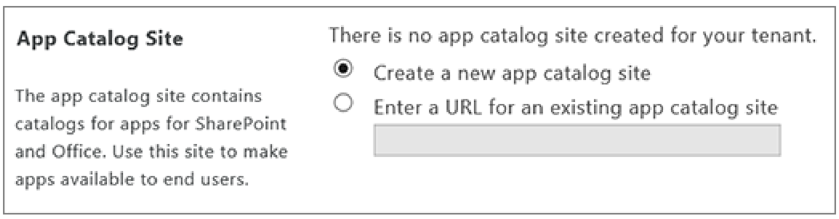
1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

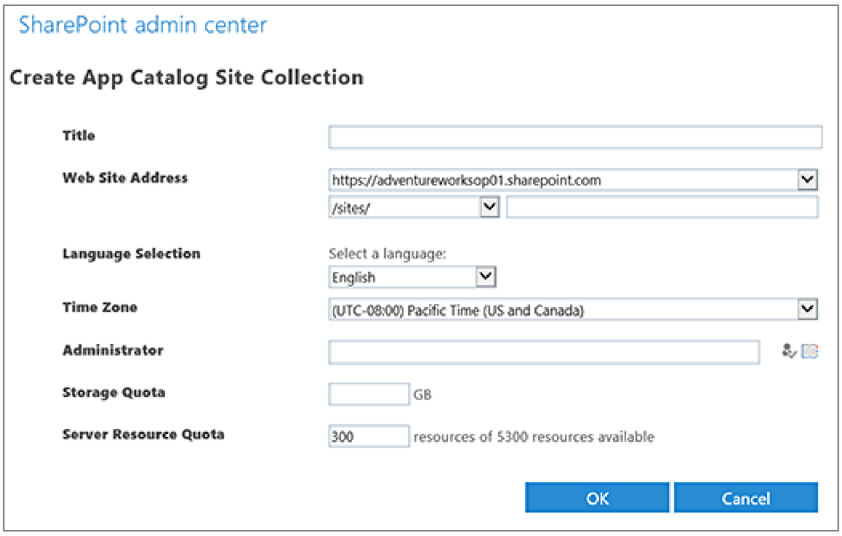
2. Under **Apps**, select **Open**.

3. Select **App Catalog**.

4. If the **App Catalog** site doesn't open, select **Create a new app catalog site**, and then select **OK**.

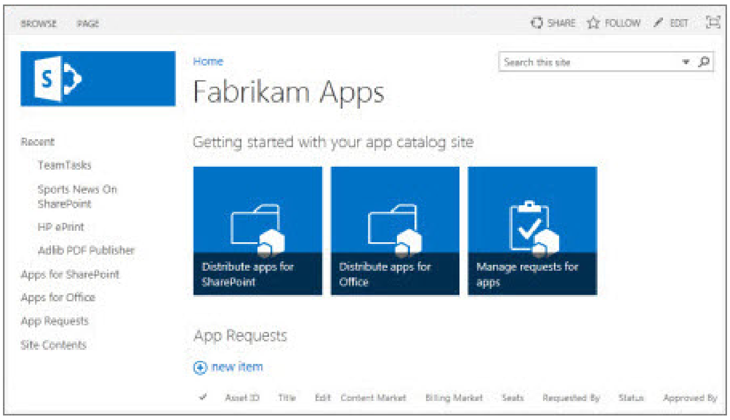


5. On the **Create App Catalog Site Collection** page, enter the required info, and then select **OK**.

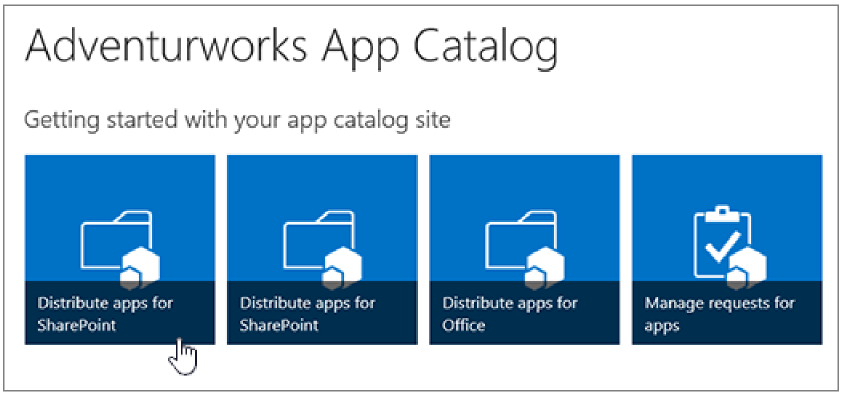


Step 2: Add custom apps to the App Catalog site

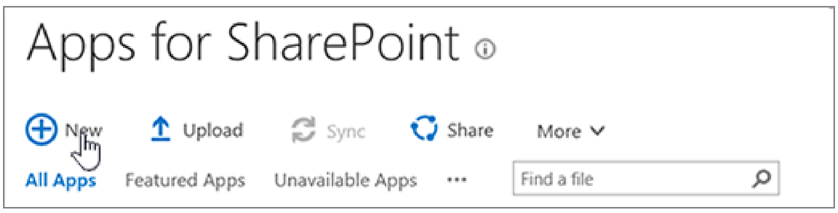
To get to the App Catalog site once it's been created, follow steps 1 and 2 in the previous section. The site may take a little time to appear. The App Catalog site will have a document library for Apps for Office and a document library for Apps for SharePoint, as well as a list that tracks App Requests from site users.



1. On the home page of the **App Catalog** site, select the tile labeled either **Distribute apps for SharePoint** or **Distribute apps for Office**, depending on which type of app you are uploading.



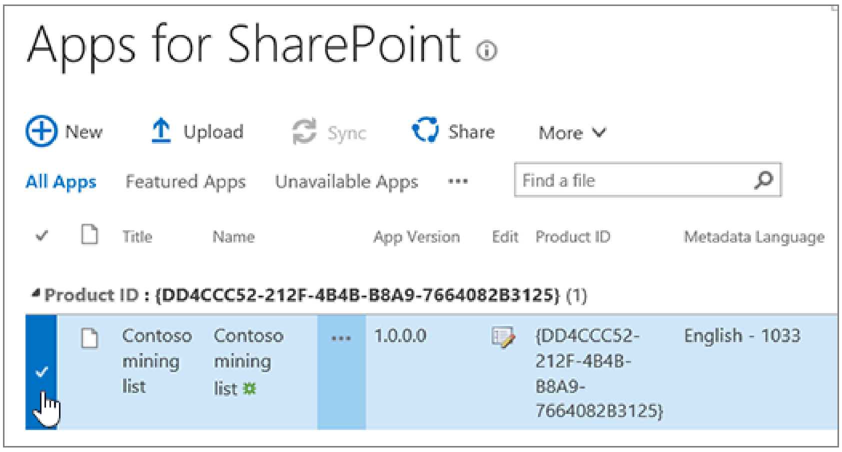
2. Select **New**, and browse to the app you want upload, or drag the app into the library.



NOTE

Depending on the functionality that the app provides, the developer can set a flag that allows you to make the app available to all sites in the organization. If the app builds something (for example, it creates a new list), you can't make it available to all sites and will need to deploy it as described in the next section under "Deploy a custom app." We always recommend testing solutions before deploying them more broadly. If the "Do you trust" dialog appears when you upload the app, and you want to make the app available to all sites in your organization, select **Make this solution available to all sites in the organization**, and then click **Deploy**.

3. To help site owners identify and use the app, right-click it, and then select **Properties**.



4. In the properties dialog form, you can change the **Name** for the app and enter optional information like a description, images, category, publisher, and support URL. Follow the instructions on the screen for details like image size.

5. Make sure the **Enabled** check box is selected so that users are able to add this app to sites.

6. If it appears, in the **Hosting Licenses** box, specify the number of licenses you think you will need.

7. Select **Save**.

NOTE

If you want to make third-party apps available for users to find and install, you simply need to buy a site license for them. When you buy a site license for a third-party app from the SharePoint store, the apps will automatically display under **Apps You Can Add**.

Step 3 (optional): Install an app for users

If you want all users to use an app, you can deploy it to specific site collections, managed paths, or site templates. Deploying an app essentially installs that app on a site for users so that is available for use. Deployed apps appear on the Site Contents page for a site.

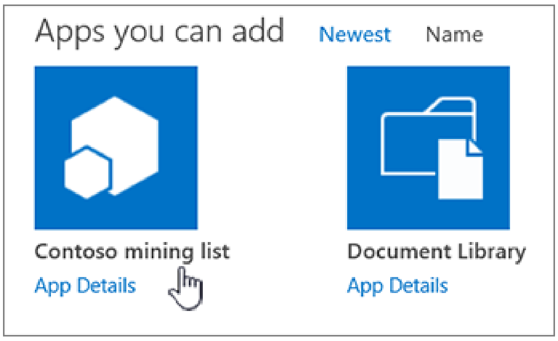
You can deploy a third-party app, or you can deploy a custom app.

NOTE

This option is only available for SharePoint add-ins. To see tenant-scoped deployment options for SharePoint Framework solutions, see Tenant-scoped solution deployment for SharePoint Framework solutions.

Deploy a third-party app

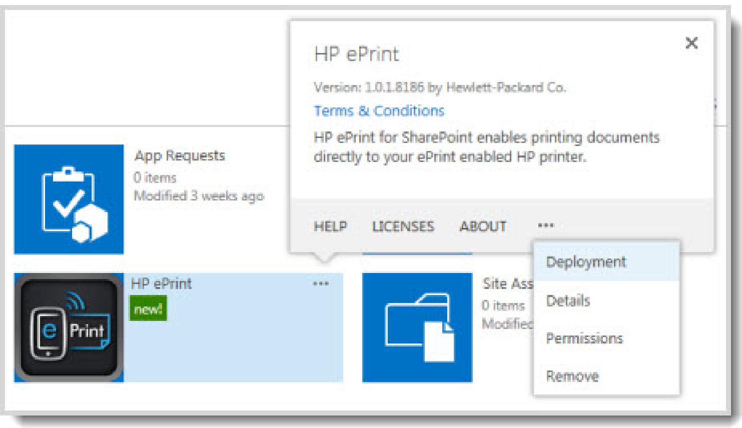
If you buy a site license for a third-party app, then that app is automatically available for users to install when they browse apps under **Apps You Can Add**.



However, if you want to make the app available for use without requiring users to find and install it, you can deploy it.

1. If you have not already purchased the app, you must buy it first. For info about how to do this, see Buy an app from the SharePoint Store.
2. On the **App Catalog** site, select **Settings**, and then select **Add an app**.
3. Select the app you want to add, and when prompted, select **Trust It**.

4. On the **Site Contents** page, find the app you want to deploy.
5. Select ... (ellipses icon) next to the app, and to view the menu, select ... (ellipses icon) again in the callout, and then select **Deployment**. (For some apps, the **Deployment** command may appear on the first callout.)



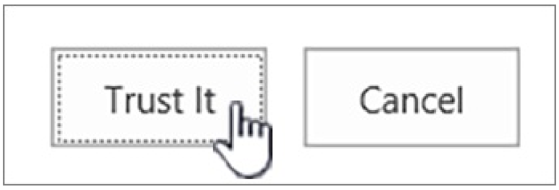
6. On the **Manage App Deployments** page, enter the URL for each site collections to which you want to deploy the app, and to add it to the list, select **Add** .

7. In the **Managed Paths** section, to specify which managed paths should have this app available, select **Add**.
8. In the **Site Templates** section, to specify which site templates should have this app available, select **Add**.
9. Select **OK**.
10. If you are prompted to Trust the app, select **Trust It**.

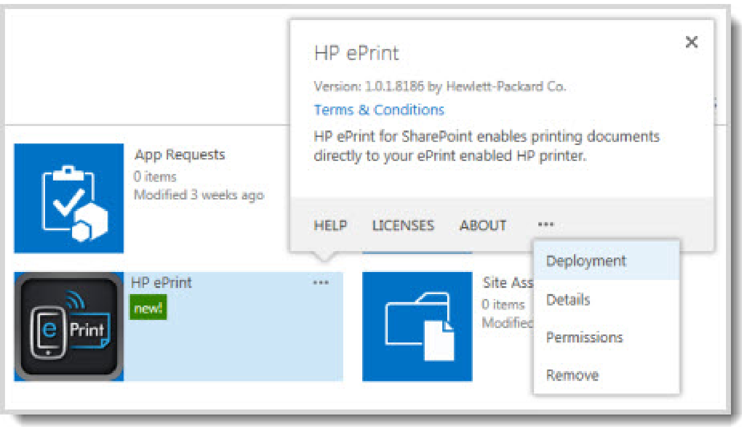
Deploy a custom app

If you upload a custom app to the App Catalog, it is automatically available for users to install when they browse apps under **From Your Organization**. If you want you want the app to be available for use without the need for site users to install it, you can deploy it.

1. Before you can deploy a custom app, you must first upload it to the **App Catalog** site. For step-by-step guidance about how to do this, see the previous section, Step 2: Add custom apps to the App Catalog site.
2. After you have uploaded the app, you then must add it as an app to the App Catalog site so that it appears on the Site Contents page for the App Catalog itself. On the App Catalog site, go to **Settings** and then click **Add an app**.
3. Select the app you want to add, and when prompted, select **Trust It**.



4. On the **Site Contents** page, find the app you want to deploy.
5. Next to the app, select ... (ellipses icon), and to view the menu, select ... (ellipses icon) again in the callout, and then select **Deployment**. (For some apps the **Deployment** command may appear on the first callout.)



6. On the **Manage App Deployments** page, enter the URL for each site collections to which you want to deploy the app, and to add it to the list, select **Add**.
7. In the **Managed Paths** section, to specify which managed paths should have this app available, select **Add**.
8. In the **Site Templates** section, to specify which site templates should have this app available, select **Add**.
9. Select **OK**.
10. If you are prompted to Trust the app, select **Trust It**.

NOTE

It may take up to 30 minutes for an app to deploy.
If you deploy an app that adds commands to the item callout for document libraries or lists, then those commands are visible to users. However, if you deploy an app that features custom ribbon controls or an App Part, additional steps may be required to make the user interface commands for the app appear.

Remove an app from the App Catalog

If you no longer want a specific app to be available for users to install, you can remove it from the App Catalog. Any instances of the app that have already been added to sites by users will remain, but the app will no longer be available for users to add to additional sites.

1. On the **App Catalog** site, select the **Apps for SharePoint** list.
2. Right-click the app that you want to remove, and select **Delete**.
3. In the dialog, to confirm that you want to send the item to the site Recycle Bin, select **OK**.

See also

Configure settings for the SharePoint Store

Manage app licenses for a SharePoint environment

Monitor apps for your SharePoint environment

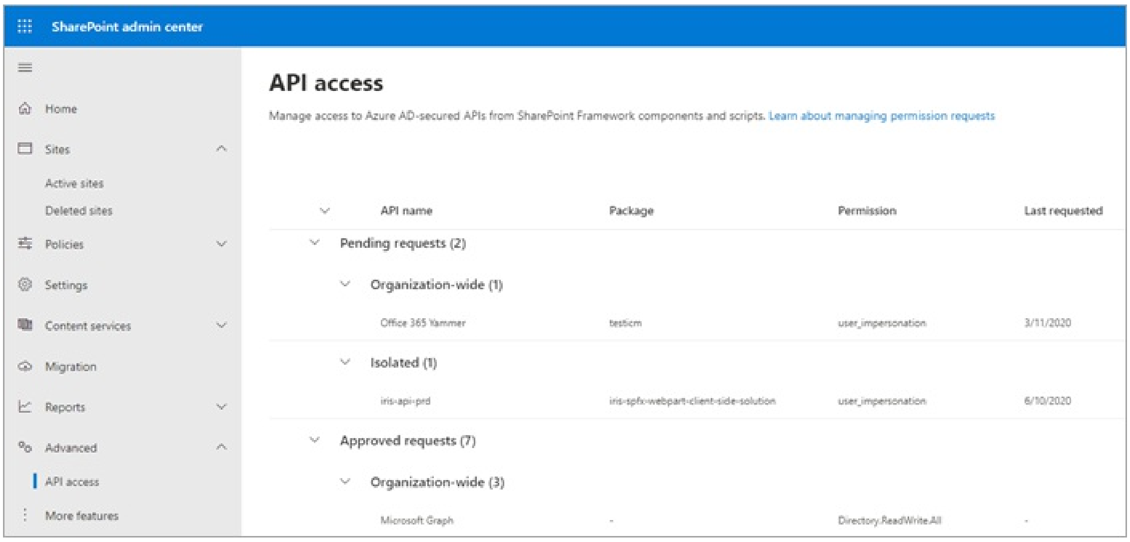
Add an app to a site

Manage access to Azure AD-secured APIs

1/8/2021 • 2 minutes to read • Edit Online

When developers build SharePoint Framework solutions, they might need to connect to an API that's secured through Azure Active Directory (Azure AD). Developers can specify which Azure AD applications and permissions their solution requires, and an administrator can manage the permission request from the API access page of the new SharePoint admin center.

Learn more about building SharePoint Framework solutions that connect to Azure-AD secured APIs.

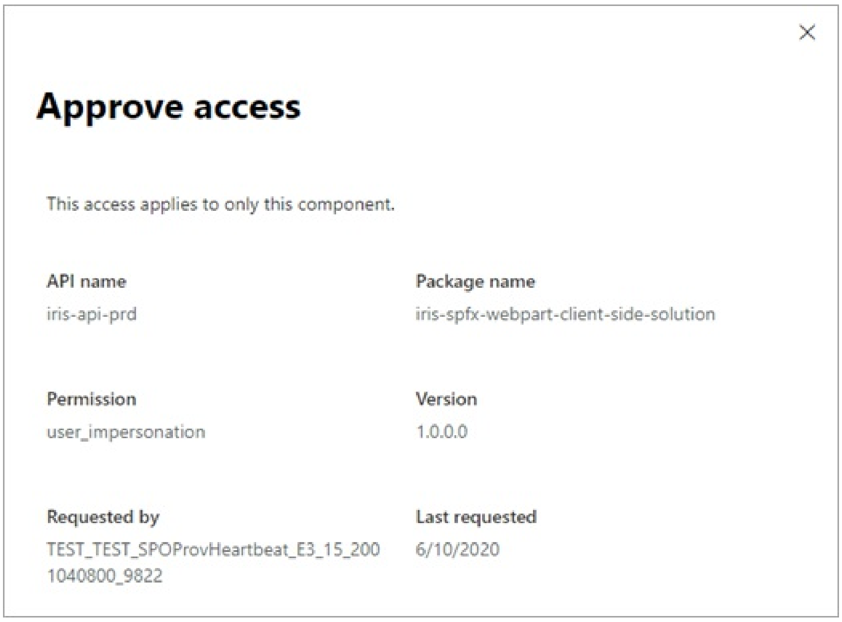


The API access page shows pending and approved requests. It also shows which requests apply to any SharePoint Framework component or custom script in your organization (organization-wide) and which requests apply to only the specific component (isolated).

> **NOTE**
>
> The admin role that's required to approve permissions depends on the API. To approve permissions to any of the third-party APIs registered in the tenant, the application administrator role is sufficient. To approve permissions for Microsoft Graph or any other Microsoft API, the global admin role is required.

Approve a pending request

1. Select the request, and then select **Approve** to see details about the request.
2. In the **Approve access** panel, select **Approve**.



After you approve a request, it moves to the Approved requests list.

> **NOTE**
> If you try to approve a permission request for a resource that already has some permissions granted (for example, granting additional permissions to the Microsoft Graph), the requested scopes are added to the previously granted permissions.

Reject a pending request

1. Select the request, and select **Reject**.
2. Select **Reject** again to confirm.

Rejecting access doesn't remove the app from the App Catalog. If the app is used on any sites, it might not work as expected. After you reject the request, it's removed from the page and the developer will need to issue a new request with the same resource and scope.

Remove access to a previously approved request

1. Select the request, and then select **Remove access**.
2. Select **Remove** again to confirm.

When you remove access, solutions and custom scripts that rely on the permission might not work as expected. After you remove access, the request is removed from the page and the developer will need to issue a new request with the same resource and scope.

Manage access by using Microsoft PowerShell

You can also use PowerShell to manage permission requests.

- To view pending requests, use the cmdlet Get-SPOTenantServicePrincipalPermissionRequests.
- To approve a request, use the cmdlet Approve-SPOTenantServicePrincipalPermissionRequest.
- To reject a request, use the cmdlet Deny-SPOTenantServicePrincipalPermissionRequest.
- To remove access to a previously approved request, use the cmdlet Revoke-SPOTenantServicePrincipalPermission.

Allow or prevent custom script

11/2/2020 • 6 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can allow custom script as a way of letting users change the look, feel, and behavior of sites and pages to meet organizational objectives or individual needs. If you allow custom script, all users who have "Add and Customize Pages" permission to a site or page can add any script they want. (By default, users who create sites are site owners and therefore have this permission. For more info about SharePoint permission levels, see Understanding permission levels in SharePoint.)

> **NOTE**
> For simple ways to change the look and feel of a site, see Change the look of your SharePoint site.

By default, script is allowed on most sites that admins create. It is not allowed on OneDrive, on sites users create themselves, on modern team and communication sites, and on the root site for your organization. You'll probably want to limit the amount of script you allow for security reasons. For more info about the security implications of custom script, see Security considerations of allowing custom script.

> **IMPORTANT**
> If SharePoint was set up for your organization before 2015, your custom script settings might still be set to "Not Configured" even though in the SharePoint admin center they appear to be set to prevent users from running custom script. In this case, users won't be able to copy items between SharePoint sites and between OneDrive and SharePoint. On the Settings page of the SharePoint admin center, to accept the custom script settings as they appear, select **OK**, and enable cross-site copying. For more info about copying items between OneDrive and SharePoint, see Copy files and folders between OneDrive and SharePoint sites.

To allow custom script on OneDrive or user-created sites

In the SharePoint admin center, you can choose to allow users to run custom script on OneDrive (referred to as "personal sites") or on all classic team sites they create. For info about letting users create their own sites, see Manage site creation in SharePoint.

Caution

Before you allow custom script on sites in your organization, make sure you understand the security implications.

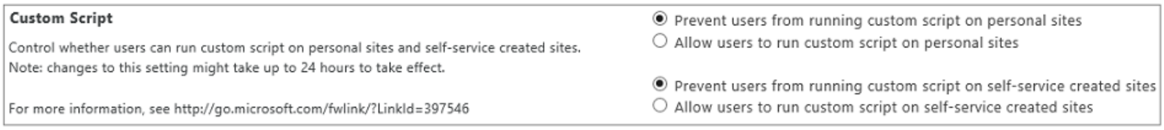
1. Go to the Settings page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the **Settings** page.

2. At the bottom of the page, select **classic settings page**.

3. Under **Custom Script**, select:

- Allow users to run custom script on personal sites.
- Allow users to run custom script on self-service created sites.


Custom Script

Control whether users can run custom script on personal sites and self-service created sites.
Note: changes to this setting might take up to 24 hours to take effect.

For more information, see http://go.microsoft.com/fwlink/?LinkId=397546

(•) Prevent users from running custom script on personal sites
( ) Allow users to run custom script on personal sites

(•) Prevent users from running custom script on self-service created sites
( ) Allow users to run custom script on self-service created sites

> **NOTE**
>
> Because self-service site creation points to your organization's root site by default, changing the Custom Script setting allows custom script on your organization's root site. For info about changing where sites are created, see Manage site creation in SharePoint.

4. Select **OK**. It can take up to 24 hours for the change to take effect.

To allow custom script on other SharePoint sites

Caution

Before you allow custom script on sites in your organization, make sure you understand the security implications.

To allow custom script on a particular site (previously called "site collection") immediately, follow these steps:

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

3. Run the following command.

```
Set-SPOsite <SiteURL> -DenyAddAndCustomizePages 0
```

If you change this setting for a user's OneDrive or a classic team site, it will be overridden by the Custom Script setting in the admin center within 24 hours.

Features affected when custom script is blocked

When users are prevented from running custom script on OneDrive or the classic team sites they create, site admins and owners won't be able to create new items such as templates, solutions, themes, and help file collections. If you allowed custom script in the past, items that were already created will still work.

The following site settings are unavailable when users are prevented from running custom script:

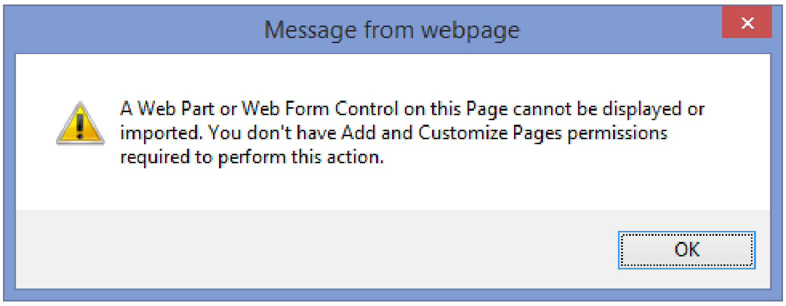
SITE FEATURE	BEHAVIOR	NOTES
Save Site as Template	No longer available in Site Settings	Users can still build sites from templates created before custom script was blocked.
Save document library as template	No longer available in Library Settings	Users can still build document libraries from templates created before custom script was blocked.
Solution Gallery	No longer available in Site Settings	Users can still use solutions created before custom script was blocked.
Theme Gallery	No longer available in Site Settings	Users can still use themes created before custom script was blocked.
Help Settings	No longer available in Site Settings	Users can still access help file collections available before custom script was blocked.
HTML Field Security	Still available in Site Settings, but changes made will not take effect	Users can still use HTML field security that they set up before custom script was blocked.
Sandbox solutions	Solution Gallery is no longer available in Site Settings	Users can't add, manage, or upgrade sandbox solutions. They can still run sandbox solutions that were deployed before custom script was blocked.
SharePoint Designer	Pages that are not HTML can no longer be updated. Handling List: **Create Form** and **Custom Action** will no longer work. Subsites: **New Subsite** and **Delete Site** redirect to the **Site Settings** page in the browser. Data Sources: **Properties** button is no longer available.	Users can still open some data sources. To open a site that does not allow custom script in SharePoint Designer, you must first open a site that does allow custom script.
Uploading files that potentially include script	The following file types can no longer be uploaded to a library .asmx .ascx .aspx .htc .jar .master .swf .xap .xsf	Existing files in the library are not impacted.
Uploading Documents to Content Types	Access denied message when attempting to attach a document template to a Content Type.	We recommend using Document Library document templates.
Publishing of SharePoint 2010 Workflows	Access denied message when attempting to publish a SharePoint 2010 Workflow.	

The following web parts and features are unavailable to site admins and owners when you prevent them from running custom script.

WEB PART CATEGORY	WEB PART
Business Data	Business Data Actions Business Data Item Business Data Item Builder Business Data List Business Data Related List Excel Web Access Indicator Details Status List Visio Web Access
Community	About This Community Join My Membership Tools What's Happening
Content Rollup	Categories Project Summary Relevant Documents RSS Viewer Site Aggregator Sites in Category Term Property Timeline WSRP Viewer XML Viewer
Document Sets	Document Set Contents Document Set Properties
Forms	HTML Form Web Part
Media and Content	Content Editor Script Editor Silverlight Web Part
Search	Refinement Search Box Search Navigation Search Results
Search-Driven Content	Catalog-Item Reuse
Social Collaboration	Contact Details Note Board Organization Browser Site Feed Tag Cloud User Tasks
Master Page Gallery	Can't create or edit master pages
Publishing Sites	Can't create or edit master pages and page layouts

Best practice for communicating script setting changes to users

Before you prevent custom script on sites where you previously allowed it, we recommend communicating the change well in advance so users can understand the impact of it. Otherwise, users who are accustomed to changing themes or adding web parts on their sites will suddenly not be able to and will see the following error message.



Communicating the change in advance can reduce user frustration and support calls.

Security considerations of allowing custom script

6/30/2020 • 3 minutes to read • Edit Online

Allowing users to customize sites and pages in SharePoint by inserting script can give them the flexibility to address different needs in your organization. However, you should be aware of the security implications of custom script. When you allow users to run custom script, you can no longer enforce governance, scope the capabilities of inserted code, block specific parts of code, or block all custom code that has been deployed. Instead of allowing custom script, we recommend using the SharePoint Framework. For more info, see An alternative to custom script.

What custom script can do

Every script that runs in a SharePoint page (whether it's an HTML page in a document library or a JavaScript in a Script Editor Web Part) always runs in the context of the user visiting the page and the SharePoint application. This means:

- Scripts have access to everything the user has access to.
- Scripts can access content across several Microsoft 365 services and even beyond with Microsoft Graph integration.

You can't audit the insertion of script

As a global admin, security admin, or SharePoint admin, you can allow or block custom script capabilities for the whole organization or for specific site collections. (For info on how to do this, see Allow or prevent custom script.) However, once you allow scripting, you can't identify:

- What code has been inserted
- Where the code has been inserted
- Who inserted the code

Any user who has "Add and Customize Pages" permission (part of the Design and Full Control permission levels) to any page or document library can insert code that can potentially have a powerful effect on all users and resources in the organization. The script has access to more than just the page or site - it can access content across all site collections and other Microsoft 365 services in the organization. There are no boundaries for executing script. For info about site activity you can audit, see Configure audit settings for a site collection.

You can't block or remove inserted script

If you've allowed custom script, you can change the setting to later prevent users from adding custom script, but you can't block the execution of script that has already been inserted. If dangerous or malicious script was inserted, the only way you can stop it is to delete the page that hosts it. This might result in data loss.

An alternative to custom script

The SharePoint Framework is a page and web part model that provides a governed and fully supported way to build solutions using scripting technologies with support for open source tooling. Key features of the SharePoint Framework:

- The framework runs in the context of the current user and connection in the browser. It doesn't use iFrames.

- The controls are rendered in the normal page Document Object Model (DOM).
- The controls are responsive and accessible.
- Developers can access the lifecycle. In addition to render, they can access load, serialize and deserialize, configuration changes, and more.
- You can use any browser framework you like: React, Handlebars, Knockout, AngularJS, and more.
- The toolchain is based on common open source client development tools like npm, TypeScript, Yeoman, webpack, and gulp.
- Admins have governance tools to immediately disable solutions regardless of the number of instances that have been used and the number of pages or sites across which they've been used.
- Solutions can be deployed in web parts and pages that use the classic experience or the new experience.
- Only global admins, SharePoint admins, and people who have been given permission to manage the App Catalog can add solutions. For info about giving users permission to manage the app catalog, see Request app installation permissions.

Configure settings for the SharePoint Store

4/22/2020 • 4 minutes to read • Edit Online

The SharePoint Store is an Internet-based service that offers apps for Office, SharePoint, Exchange, Access, and Project. Site users can access the SharePoint Store directly from a SharePoint site in order to browse for and buy third-party apps. If a SharePoint environment has been configured to prevent users from getting apps from the SharePoint Store, users can still browse for and request apps. These requests are added to the App Requests list in the App Catalog.

For more information about the SharePoint Store, see Office Store and SharePoint Store Terms of Use.

For more information about how to buy apps, see Buy an app from the SharePoint Store.

Specify whether users can get apps from the SharePoint Store

By default, SharePoint is configured to allow users to get or request apps from the SharePoint Store. The option to change this setting will not be enabled if you have not yet created an App Catalog site. For information about how to create an App Catalog site, see Use the App Catalog to make custom business apps available for your SharePoint environment.

Even if you choose not to allow users to buy apps from the SharePoint Store, they will still be able to browse the SharePoint Store and request apps.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Apps**, select **Open**, and then select **Configure Store Settings**.

3. Next to **App Purchases**, do one of the following:

- If you want users to be able to get free, trial, or paid third-party apps from the SharePoint store, select **Yes**.

- If you do not want users to be able to get third-party apps, select **No**.

View or manage app requests

When users request an app, they are requesting that an admin buys that app on their behalf. In an app request, users can request a specific number of licenses, and they can provide a business justification for why they need the app. App requests are saved to the App Requests list in the App Catalog site.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

NOTE

If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **Apps**, select **Open**, and then select **Configure Store Settings**.

3. Next to **App Requests**, select the link **Select here to view app requests**.

4. In the **App Requests** list, select a request, and then select **Edit**.

5. In the **Status** list, do one of the following:

- To approve the request, select **Approved**. If you approve the app request and you want to purchase the app immediately, select the link next to **View App Details**. The app details page in the SharePoint store will open in another tab in your browser, and you can follow the steps to purchase the app. For more information about buying apps, see Buy an app from the SharePoint Store. Note that the app must be purchased from the store before it will be available for the user in their site.

- To decline the request, select **Declined**.

6. On the app request form, add any comments in the **Approvers Comments** field, and then select **Save**.

7. After the status has been changed to **Approved**, if the app wasn't purchased during the previous approval process, the global admin or SharePoint admin must go to the SharePoint Store and acquire the app to make it available for the user. See Buy an app from the SharePoint Store.

Site users who request apps can view their requests by going to **Settings** > **Add an app** > **Your Requests**.

Specify whether to allow apps for Office to start in documents

Documents stored on sites may contain apps for Office from several sources. You can specify whether or not you want to allow these apps to work when documents are opened in the browser.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

NOTE

If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the **More features** page.

2. Under **Apps**, select **Open**, and then select **Configure Store Settings**.

3. Next to **Apps for Office from the Store**, do one of the following:

- If you want to allow apps for Office to start when documents are opened in the browser, select **Yes**.

- If you do not want to allow apps for Office to start when documents are opened in the browser, select **No**.

Configure InfoPath Forms Services

4/22/2020 • 3 minutes to read • Edit Online

InfoPath Forms Services in SharePoint lets you deploy your organization's forms to your sites, enabling users fill out these forms in a web browser. You can configure InfoPath Forms Services in any of several ways, depending on the needs of your organization.

> **NOTE**
> InfoPath Forms Services 2013 is the last release of InfoPath Forms Services. Microsoft Power Apps is the recommended solution for creating and delivering custom forms for SharePoint lists. Create new forms with Power Apps from the command bar or the **Customize** button on SharePoint list forms. Support for InfoPath Forms Services will match the support lifecycle for SharePoint Server 2016.

Overview

This article discusses settings that apply only to user form templates, which are form templates that are not deployed by a developer. User form templates don't require Full Trust, and they don't contain code or other business logic.

Form designers can publish user form templates to a list or a form library in a SharePoint site collection. Because user form templates can be deployed by many users, a server can potentially host thousands of user form templates. In large numbers, even form templates that contain no business logic can put a heavy load on the server.

Configure browser-enabled user form templates

When form templates are published to a server that is running InfoPath Forms Services, the designer of the form template can choose to make the form template browser-enabled. This allows a user to fill out the form in a web browser.

As an administrator, you can configure the following template settings for browser-enabled user form templates:

- **Enable or disable publishing of browser-enabled form templates.** If you disable publishing, form designers can publish only form templates that are not browser-enabled. In this case, all browser-compatible features are disabled in the form template.
- **Enable or disable rendering of browser-enabled form templates.** If you disable rendering, users cannot use a web browser to fill out the form and must use Microsoft InfoPath Filler 2013 to open the form.

By default, browser-enabled user form templates can be published and rendered.

To configure browser-enabled user form templates

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

2. Under **InfoPath**, select **Open**.

3. In the **User Browser-enabled Form Templates** section, specify how you want user form templates to be processed by InfoPath Forms Services by completing the following steps:

   > **NOTE**
   >
   > These settings apply only to form templates published to form libraries. Workflow form templates and list forms are not affected.

   a. Select the **Allow users to browser-enable form templates** check box to allow users to publish browser-enabled form templates.

   > **NOTE**
   >
   > Clearing this check box disables browser-enabled form templates across the entire site collection.

   b. Select the **Render form templates that are browser-enabled by users** check box to allow browser-enabled form templates that users publish to be rendered in a web browser.

   > **NOTE**
   >
   > If this option is not selected, users can still publish browser-compatible form templates to form libraries, but these form templates cannot be filled out in a web browser.

4. Select **OK**.

Configure exempt user agents

To make indexing InfoPath forms faster and easier, you can specify which user agents to exempt from receiving an entire webpage to index. This means that when a user agent you've specified as exempt encounters an InfoPath form, the form will be returned as an XML file (which looks like a hierarchical text file) instead of an entire webpage. You can use the procedure below to select this option and populate the agent list.

1. Go to the More features page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the More features page.

3. Under **InfoPath**, select **Open**.

4. In the **Exempt User Agents** section, select the **Customize the list of exempt user agents** check box, and then do one of the following:

5. To add a user agent to the exempt list, in the **Name** box, enter a name, and then select **Add**.

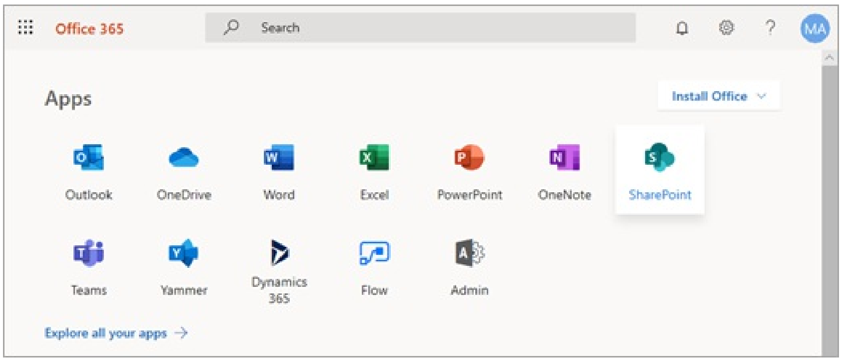
6. To remove a user agent from the list, select the name, and then select **Remove**.

7. Select **OK**.

Hide the OneDrive and SharePoint app tiles

6/5/2020 • 2 minutes to read • Edit Online

By default, the OneDrive and SharePoint app tiles appear in the app launcher and on the Microsoft 365 admin center. If your subscription doesn't include one of these services, or if you don't want users using one of them, you can hide the app tile for it.



> **NOTE**
>
> Hiding these services doesn't remove them for users. If users have saved the address of the service, they will still be able to access it.
>
> If users click a tile for a service they don't have, they will see an Access Denied message.

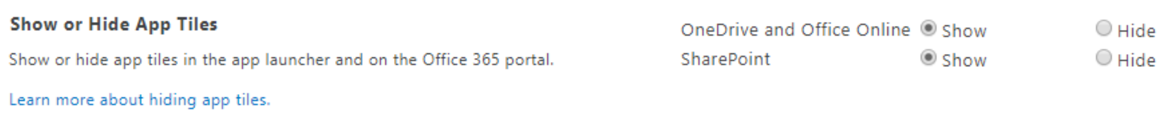
To hide app tiles

1. Go to the Settings page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
>
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.
>
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.

2. At the bottom of the page, select **classic settings page**.

3. In **Show or Hide App Tiles**, select the tile you want to hide.



> **NOTE**
>
> If you have an Office 365 Education subscription, you also have the option to hide **OneNote Class Notebooks** and **OneNote Staff Notebooks**.
>
> Hiding the OneDrive tile also hides the tiles for Word, Excel, PowerPoint, and OneNote.

4. To save the settings, select **OK**.

See also

Customize the navigation on your SharePoint site

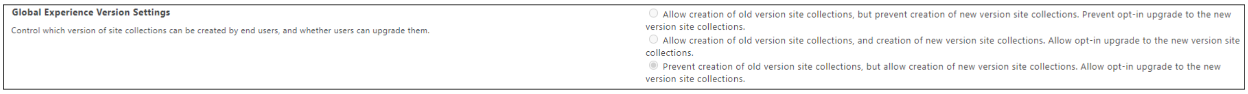
Customize the Microsoft 365 theme for your organization

Add custom tiles to the app launcher

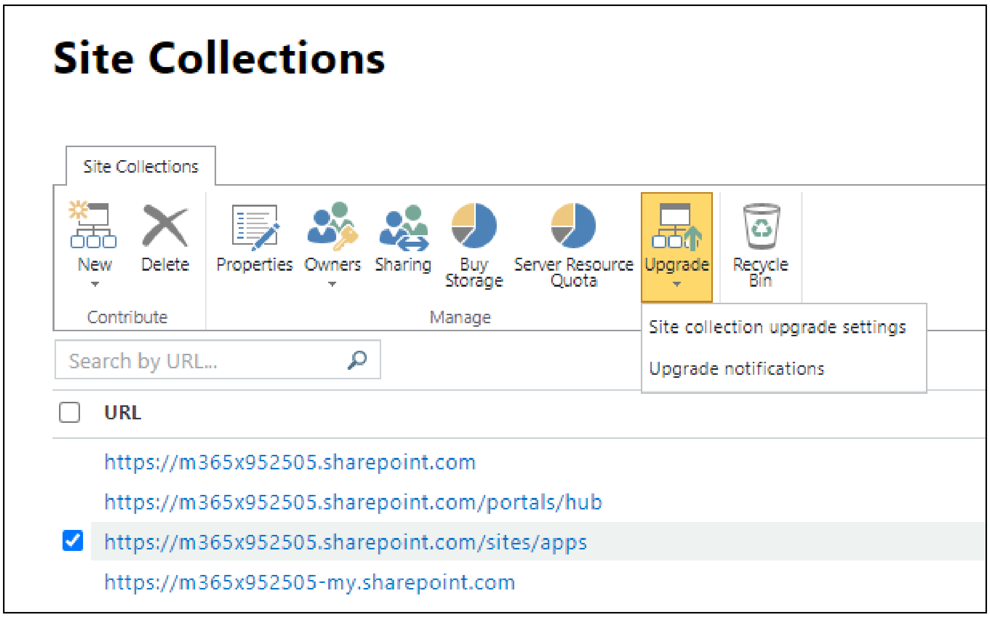
Change site collection version and upgrade settings

6/17/2020 • 2 minutes to read • Edit Online

The **Global Experience Version Settings** on the settings page of the classic SharePoint admin center are no longer in use.



The **Upgrade** settings on the site collections page of the classic SharePoint admin center are no longer in use.



Allow users to create modern pages

6/5/2020 • 5 minutes to read • Edit Online

Using modern pages in Microsoft SharePoint is a great way to share ideas using images, Office files, video, and more. Users can Add a page to a site quickly and easily, and modern pages look great on any device.

If you're a global or SharePoint admin in Microsoft 365, you can allow or prevent users from creating modern pages. You can do this at the organization level by changing settings in the SharePoint admin center. If you allow the creation of site pages as the organization level, site owners can turn it of or off at the site level.

> **NOTE**
>
> If you want to prevent members from creating or modifying any SharePoint pages on a site, go to Site Pages, select **Settings** > **Library settings** > **Permissions for this document library**, and then set the Members group to Read.

Change page creation settings at the organization level

1. Go to the Settings page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

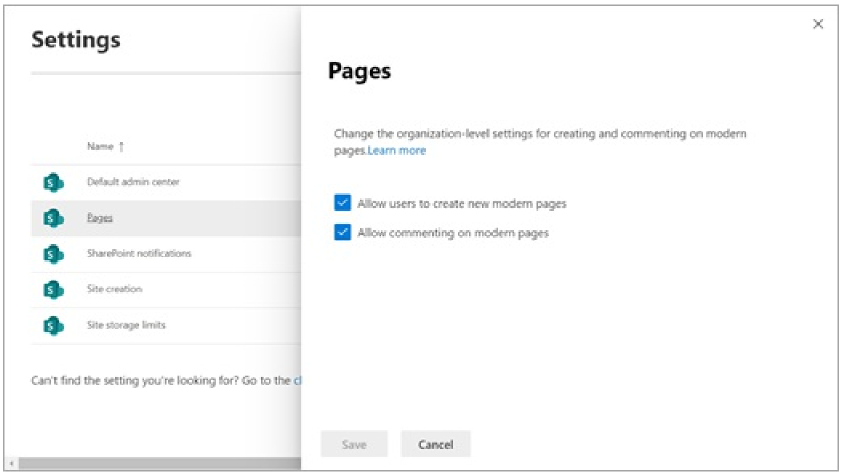
   > **NOTE**
   >
   > If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.
   > If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.

2. Select **Pages**.

3. Select or clear **Allow users to create new modern pages**.

   > **NOTE**
   >
   > Preventing users from creating modern pages hides the following options:
   > - On the Site Pages and Site contents pages > **New** > **Page**.
   > - **Settings** > **Add a page**.
   > Users can still add pages from other modern pages, either from the New menu or from modern webparts (such as News).

4. You can also select to allow or prevent commenting on modern pages. If you allow commenting, it can be turned on or off at the page level.



Prevent users from creating modern pages on a specific site by using PowerShell

1. Download the latest SharePoint Online Management Shell.

> **NOTE**
>
> If you installed a previous version of the SharePoint Online Management Shell, go to Add or remove programs and uninstall "SharePoint Online Management Shell."
> On the Download Center page, select your language and then click the Download button. You'll be asked to choose between downloading a x64 and x86 .msi file. Download the x64 file if you're running the 64-bit version of Windows or the x86 file if you're running the 32-bit version. If you don't know, see Which version of Windows operating system am I running?. After the file downloads, run it and follow the steps in the Setup Wizard.

2. Install the SharePoint Online Client Components SDK.

3. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

> **NOTE**
>
> Read About Execution Policies and make sure you run the SharePoint Online Management Shell as an administrator and the correct execution policy to run unsigned scripts.

4. Copy the following code and paste it into a text editor, such as Notepad.

```
# Load SharePoint Online Client Components SDK Module
Import-Module 'C:\Program Files\Common Files\microsoft shared\Web Server
Extensions\16\ISAPI\Microsoft.SharePoint.Client.dll'

# Set script constants
$sitePagesFeatureIdString = 'B6917CB1-93A0-4B97-A84D-7CF49975D4EC'

# Set up client context
$userName = Read-Host "Username"
$password = Read-Host "Password" -AsSecureString
$siteUrl = Read-Host "Site Url"
$webUrl = Read-Host "Server-Relative Web Url"
$context = New-Object Microsoft.SharePoint.Client.ClientContext($siteUrl)
$credentials = New-Object Microsoft.SharePoint.Client.SharePointOnlineCredentials($userName,
$password)
$context.Credentials = $credentials

# Get the list of existing features
$web = $context.Site.OpenWeb($webUrl)
$features = $web.Features
$context.Load($features)
$context.ExecuteQuery()

# Verify that the Site Pages feature is present in the web
if(($features | ? { $_.DefinitionId -eq $sitePagesFeatureIdString }).Count -eq 0)
{
    Write-Host "The Site Pages feature is already disabled in this web"
    return
}

# Remove the Site Pages feature from the web
$features.Remove((new-object 'System.Guid' $sitePagesFeatureIdString), $false)
$context.ExecuteQuery()

# Verify that the Site Pages feature is no longer present in the Web
$web = $context.Site.OpenWeb($webUrl)
$features = $web.Features
$context.Load($features)
$context.ExecuteQuery()
if(($features | ? { $_.DefinitionId -eq $sitePagesFeatureIdString }).Count -eq 0)
{
    Write-Host "The Site Pages feature has been successfully disabled"
}
else
{
    throw "The Site Pages feature failed to be disabled"
}
```

5. Save the text file, and then change its extension. In this example, we name it SitePagesOut.ps1.

> **NOTE**
>
> You can use a different file name, but you must save the file as an ANSI-encoded text file whose extension is .ps1.

6. Change to the directory where you saved the file.

7. Run the following command:

```
./SitePagesOut.ps1
```

8. The script will prompt you for a **SiteUrl** and **WebUrl**.

If you have a site such as "https://contoso.sharepoint.com/sites/marketing/northwindcompete"

For the **SiteUrl** you would enter: `https://contoso.sharepoint.com/sites/marketing`

And for the **WebUrl** you would enter `sites/marketing/northwindcompete`

Allow users to create modern pages on a specific site by using PowerShell

1. Download the latest SharePoint Online Management Shell.

2. Install the SharePoint Client Components SDK.

3. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365. To learn how, see Getting started with SharePoint Online Management Shell.

   > **NOTE**
   >
   > Read About Execution Policies and make sure you run the SharePoint Online Management Shell as an administrator and the correct execution policy to run unsigned scripts.

4. Copy the following code and paste it into a text editor, such as Notepad.

```
# Load SharePoint Online Client Components SDK Module
Import-Module 'C:\Program Files\Common Files\microsoft shared\Web Server
Extensions\16\ISAPI\Microsoft.SharePoint.Client.dll'

# Set script constants
$sitePagesFeatureIdString = 'B6917CB1-93A0-4B97-A84D-7CF49975D4EC'

# Set up client context
$userName = Read-Host "Username"
$password = Read-Host "Password" -AsSecureString
$siteUrl = Read-Host "Site Url"
$webUrl = Read-Host "Server-Relative Web Url"
$context = New-Object Microsoft.SharePoint.Client.ClientContext($siteUrl)
$credentials = New-Object Microsoft.SharePoint.Client.SharePointOnlineCredentials($userName,
$password)
$context.Credentials = $credentials

# Get the list of existing features
$web = $context.Site.OpenWeb($webUrl)
$features = $web.Features
$context.Load($features)
$context.ExecuteQuery()

# Verify that the Site Pages feature is not present in the web
if(($features | ? { $_.DefinitionId -eq $sitePagesFeatureIdString }).Count -gt 0)
{
    Write-Host "The Site Pages feature is already enabled in this web"
    return
}

# Add the Site Pages feature back to the web
$features.Add((new-object 'System.Guid' $sitePagesFeatureIdString), $false,
[Microsoft.SharePoint.Client.FeatureDefinitionScope]::None)
$context.ExecuteQuery()

# Verify that the Site Pages feature is now present in the web
$web = $context.Site.OpenWeb($webUrl)
$features = $web.Features
$context.Load($features)
$context.ExecuteQuery()
if(($features | ? { $_.DefinitionId -eq $sitePagesFeatureIdString }).Count -gt 0)
{
    Write-Host "The Site Pages feature has been successfully enabled"
}
else
{
    throw "The Site Pages feature failed to be enabled"
}
```

5. Save the text file, and then change its extension. In this example, we name it SitePagesIn.ps1.

> **NOTE**
>
> You can use a different file name, but you must save the file as an ANSI-encoded text file whose extension is .ps1.

6. Change to the directory where you saved the file.

7. Run the following command:

```
./SitePagesIn.ps1
```

8. The script will prompt you for a **SiteUrl** and **WebUrl**.

If you have a site such as "https://contoso.sharepoint.com/sites/marketing/northwindcompete"

For the **SiteUrl** you would enter: `https://contoso.sharepoint.com/sites/marketing`

And for the **WebUrl** you would enter `sites/marketing/northwindcompete`

Let users connect classic team sites to new Microsoft 365 groups

7/10/2020 • 2 minutes to read • Edit Online

As a global or SharePoint admin in Microsoft 365, you can allow or prevent site collection administrators from connecting classic team sites to new Microsoft 365 groups. You can also use Microsoft PowerShell or the API to connect sites to new Microsoft 365 groups.

Allow or prevent site collection administrators from connecting classic team sites to new Microsoft 365 groups

1. Go to the Settings page of the new SharePoint admin center, and sign in with an account that has admin permissions for your organization.

> **NOTE**
> If you have Office 365 Germany, sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the Settings page.
> If you have Office 365 operated by 21Vianet (China), sign in to the Microsoft 365 admin center, then browse to the SharePoint admin center and open the **Settings** page.

2. Select **classic settings page**.
3. Next to "Allow site owners to create Microsoft 365 groups and attach them to existing sites," select **Do not allow site owners to create new Microsoft 365 groups for their existing sites.** or **Allow site owners to create new Microsoft 365 groups for their existing sites.**

When this setting is on, and the site collection administrator for a classic team site (with the template STS#0) is allowed to create groups, they will see the "Connect to a new Microsoft 365 Group" option in settings. For more info, see:

- Manage who can create Microsoft 365 Groups
- Connect sites to new Microsoft 365 groups using PowerShell: Set-SPOSiteOffice365Group
- Connect sites to new Microsoft 365 groups using the CSOM API: CreateGroupForSite method
- SharePoint modernization scanner tool

> **NOTE**
> If your organization has set up OneDrive and SharePoint Multi-Geo, site collection administrators can connect a site to a new Microsoft 365 group only if the site's location matches the user's preferred data location.