Contents

Overview of Microsoft Search

4/28/2020 • 4 minutes to read • Edit Online

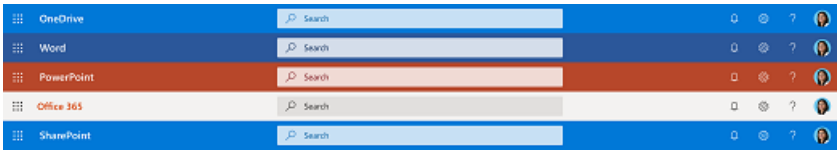
Microsoft Search helps you find what you need to complete what you're working on. Whether you're searching for people, files, org charts, sites, or answers to common questions, you can use Microsoft Search throughout your workday to get answers.

Microsoft Search helps users find the right answers, people, and content to complete their tasks in the app they're already working in.

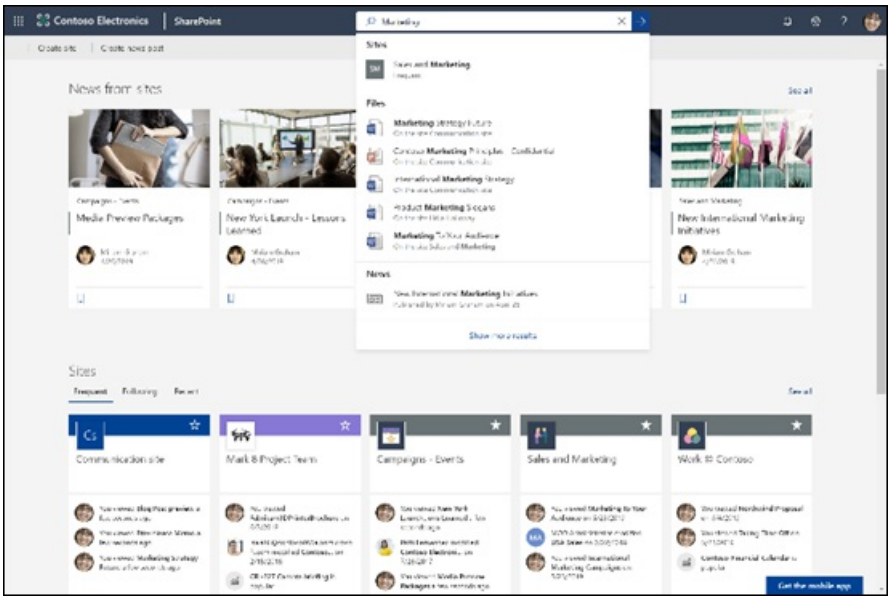
- Users get results that are relevant in the **context** of the app they search from. For example, when they search in Microsoft Outlook, they find emails, and not SharePoint sites. When they search in SharePoint, they find sites, pages, and files.
- Whichever app users are working in; Microsoft Search is **personal**. Microsoft Search uses insights from the Microsoft Graph to show results that are relevant to each user. Each user might see different results, even if they search for the same words. They only see results that they already have access to, Microsoft Search doesn't change permissions.
- Users don't need to remember where the information is located. For example, a user is working in Microsoft Word and wants to reuse information from a presentation that a colleague shared from their OneDrive. There's no need to switch to OneDrive and search for that presentation, they can simply search from Word.
- When in Bing, users get results from within their organization in addition to the public web results.

What users see

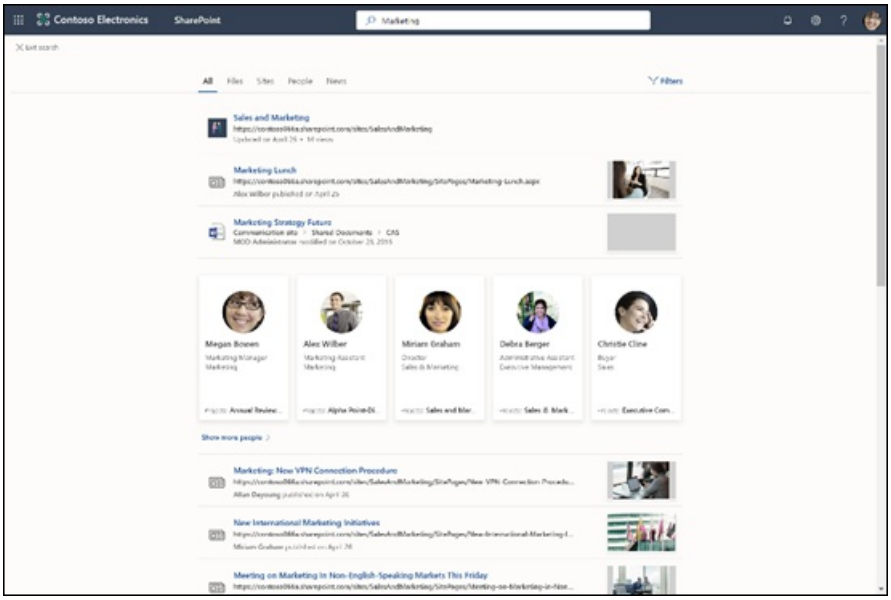
In Bing, users use the same search box as for web searches. In the Office apps, users find the Microsoft Search box in the header bar. It looks like this:



When users click in the **Search** box, search suggests results based on their previous activity in Office 365 and based on content that's trending in your organization. Files they were working on recently, commands they've used recently as well as people they collaborate with are examples of activity that search considers. As users start typing in the **Search** box, the suggested results update. Users can open search results right from the **Search** box. Here's an example of a search in SharePoint.



If the suggestions in the search box aren't what users are looking for, **Enter** opens the full list of results. They can use metadata such as who last modified the item and when, where the items is located, as well as preview it to determine if it's what they're looking for.



Benefits of Microsoft Search

Search across Microsoft 365 from any Microsoft Search box – Users can search from any Microsoft Search box and get quickly back to what they were doing. Microsoft Search brings together results from data sources in Office 365, including SharePoint, Microsoft OneDrive for Business, and Microsoft Exchange Server.

Easy to search – Microsoft Search suggests results based on users' previous activity in Office 365, right in the **Search** box.

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, remote workers, or different geographies.

Administer across all apps – Microsoft Search is **on** by default and any administration you do applies to Microsoft Search in all the apps.

Tailoring Microsoft Search to your organization

As an administrator you can create an amazing Microsoft Search experience for your users.

Show useful content – Answers provide fast, authoritative results to search queries based on keywords. Plan your content.

Add external content – Microsoft Graph Connectors allow you to bring external content into the index. Use connectors to enrich the search experience with data and files from outside of Microsoft 365. Overview of Microsoft Graph connectors

Customize the user experience – You can customize the user experience through the use of verticals and other configurations. Customize the Microsoft Search page

What content is searched

Microsoft Search shows the content that your organization has stored in Microsoft 365 or indexed through connectors. Microsoft Search does not search across tenants or show results from content that's shared by other organizations. If your organization has set up a hybrid SharePoint environment using cloud hybrid search, Microsoft Search returns search results from both online and on-premises SharePoint content, including any external content you've connected to your SharePoint Server environment. Learn more about hybrid search environments.

Users will get the same search results they get from other locations and will also get results from the internet.

How Microsoft Search works

When a user searches, Microsoft Search processes the query and parses search intent from larger phrases, using Artificial Intelligence (AI) to learn common superfluous phrases users add to their queries that don't impact their search intent. For example, when a user searches for "how to change my password" we extract the less important words from the query and trigger based on the relevant ones like "change password".
The search results that the user has **permission** to see are presented on the search results page. Microsoft Search uses intelligent ranking algorithms to order results based on relevance.

How Microsoft Search in Bing protects your company data

Security and Privacy for Microsoft Search in Bing

See also

Set up Microsoft Search

Set up Microsoft Search

11/30/2020 • 2 minutes to read • Edit Online

Microsoft Search provides a user-friendly interface to help users find information like files and documents, internal sites and business tools, people and groups, locations and directions, conversations and answers. It does this by securely accessing all data sources, including emails, files, SharePoint files, OneDrive content, and other shared resources as well. With Microsoft Search in Bing you can get search results from the internet as well.

To learn more about Microsoft Search features, see Microsoft Search Overview.

Get Started

Microsoft Search is turned on by default for all Microsoft apps that supports it, as a part of Microsoft 365. There is no setup required, but you can improve the overall Microsoft Search experience through some basic administrative tasks.

You manage Microsoft Search from Microsoft 365 admin center.

1. In Microsoft 365 admin center, go to **Settings** > **Search & intelligence**.

As an admin you should consider a few things that can make the Microsoft Search experience efficient and user friendly in your organization.

Step 1: Assign Search admin and Search editor

In Microsoft Search, you can manage your organization's search settings and content by assigning these roles to users:

1. **Search admin:** This role can create and manage search result content and define query settings for improved search results within the organization. Search admin manages the Microsoft Search configuration and can perform all of the content-management tasks a Search editor can.
2. **Search editor**: Creates, manages, and deletes content for Microsoft Search in the Microsoft 365 admin center. This role can create and manage editorial content, such as frequently asked questions and answers, important places and locations, frequently searched and used sites and apps.

Currently, the Search admin and Search editor roles must be assigned by a global admin. For more information, see Assign admin roles.

Search administrators directly influence the search experience for end users. This includes choosing the types of results you want to surface to your users. It may be difficult for one person to choose and create authoritative content on many different topics that users search for in an organization. We recommend that you leverage the expertise and knowledge of subject matter experts (SME) and other users by adding them as Search editors.

Step 2: Create answers

Microsoft Search provides administrators with tools that they can use to build a robust search experience for their users. In Microsoft Search, administrators have three different search contents that they can create for a better search experience and to improve the "findability" of content:

Bookmarks are the most commonly used answer type. They promote the best possible results for your users' queries to the top of the search results and make it easy for your users to find what they are looking for. Informational content that is available for everyone; for example, information about the company, help for

Windows and Office apps, etc. Content that people in the organization generally search for in their day-to-day work. Common work-related searches include employee benefits, time and expense reporting, submitting purchase orders, and getting help from IT services.

For creating and managing answers, see Plan your content.

Next steps

If you'd like to learn more about how your users will use Microsoft Search, see the following articles:

- Find what you need with Microsoft Search in Office
- Office 365 Training Center
- Microsoft Search Center

Frequently asked questions

11/30/2020 • 2 minutes to read • Edit Online

Here's a list of the most common questions.

> **TIP**
> Don't see your question answered here? Ask your question in this article's feedback.

Is advanced query understanding supported?

Yes, Microsoft Search parses query intent from larger phrases. This feature uses AI to learn common superfluous phrases users add to their queries that don't impact their search intent. For example, when a user searches for *tell me more about how to change my password please*, we extract the less important words from the query and trigger based on the relevant ones like *change password*.

This feature won't override keywords set in the Microsoft 365 admin center.

Can you search for files on-premises?

Yes. You can search on-premises SharePoint files if you have a hybrid deployment of SharePoint.

How do I make Bing the default search engine for people in my org?

Here's the instructions for setting the default search engine, default homepage, and default browser to give your users the best experience with Microsoft Search in Bing:

- Set Microsoft Edge as your default browser
- Make Bing your default search engine
- Set Bing.com as your enterprise homepage

How are my search results protected?

We require Azure Active Directory authentication to access results from the Trusted Cloud. Authenticated users only see content they have access to. Search queries are de-identified, and logs are separated from public Bing search traffic. This level of protection is unavailable anywhere else in the industry.

Can I search across federated organizations?

No.

Where can I get info about Office 365 security, compliance, and privacy?

Details can be found on the Trust Center pages for Office 365.

Can users earn Microsoft Rewards points with their work or school account?

Microsoft Search requires that enterprise users sign in with a work or school account. But users can't join or sign in to the Microsoft Rewards program with those accounts. However, there is an instance when an enterprise user may

see Rewards points accrue. This can happen when a Microsoft Search user has a Rewards account that was created with a Microsoft account. (The email address associated with a Microsoft account can be from Outlook.com, Hotmail.com, Gmail, Yahoo, or other providers.) If users sign in alternately with both their work account and Microsoft account in the same browser session, they might accrue points to their Rewards account. Users can stop accruing points while searching with Microsoft Search by clearing their cookies.

Can guest users leverage Microsoft Search in my organization?

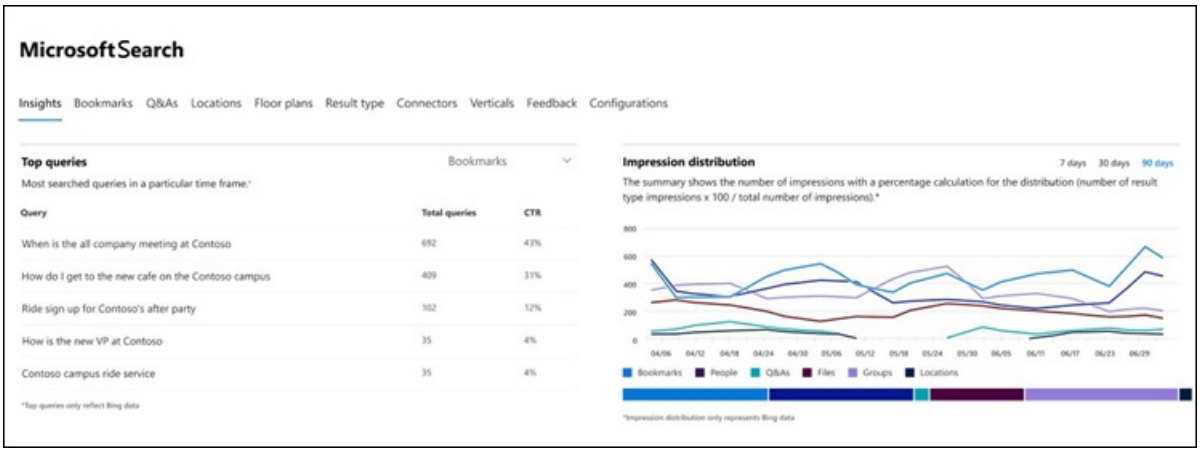
Microsoft 365 enables rich collaboration with people outside of your organization through guest access. These users will be able to perform search operations on documents, sites, groups, lists, and libraries. However, guest users will not get the full, personalized, Microsoft Search experience and may need to leverage the on-page search box instead of the unified Microsoft Search box in the header.

Microsoft Search Insights dashboard reports

11/30/2020 • 2 minutes to read • Edit Online

You can use the Microsoft Search Insights dashboard to manage Bing data for your published answers. This is just one of the steps needed to make content easy to find for your users.

When you first go to Microsoft Search in the Microsoft 365 admin center, you enter on the Insights dashboard.

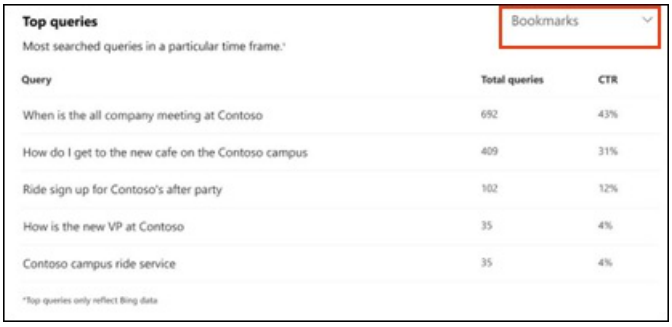


The following reports are available on the Insights dashboard.

> **NOTE**
> The data in the reports only represents Bing data.

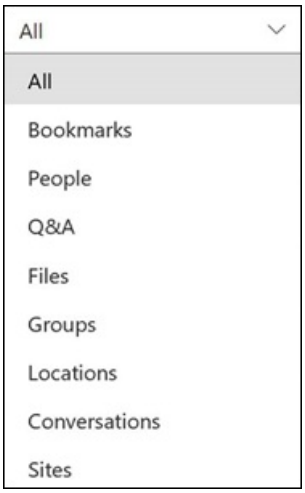
Top queries

This report gives details about the top 2000 Bing search queries that users run. For a query to appear in **Top queries**, the query must get at least three clicks.



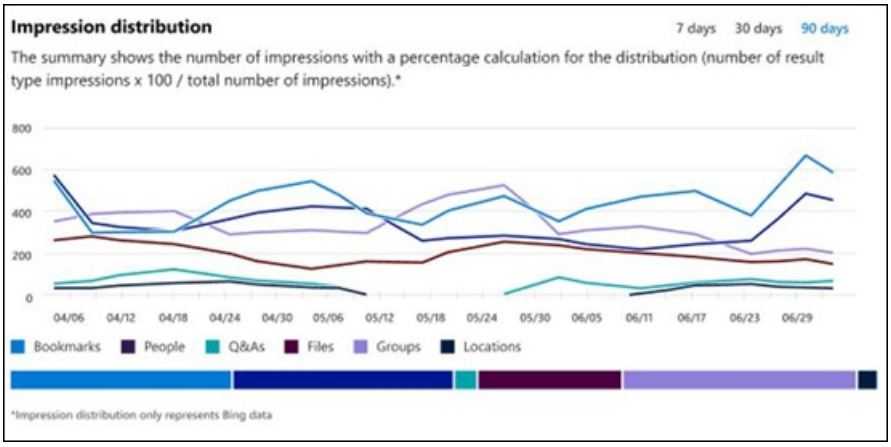
A low click-through rate (CTR) means that users aren't finding what they're looking for.

You can choose different views of the report by filtering on the type of answer. For example, if you just want to view the top queries for Bookmarks, select the drop-down in the upper-right corner of the report, and then select **Bookmarks**. By default, **All** answer types are shown.



Impression distribution

This report shows impression distribution in Bing over time for various answers. Examples are bookmarks, people, Q&A, files, locations, file sites, groups, and conversations.



Impression distribution can help admins understand what users look for during a specified period.

Plan your content

11/30/2020 • 8 minutes to read • Edit Online

Microsoft Search helps users find relevant content. **Microsoft Search** is a secure way to search both your intranet and web content. This kind of integration across web and organization is available only with Microsoft.

Search administrators use their knowledge of the organization and its users to make it easy for users to find the relevant content.

Step 1: Identify information your users need

Find out what your users are searching for and make that easily discoverable. Here are some ideas for finding out what information users need:

- Use intranet search logs to determine sites and pages that get the most traffic.
- Determine apps, sites, and tools that are used on a daily or weekly basis.
- Find direct links for employee benefits.
- Find policies and processes that users need to be aware of.
- Decide 'who' and 'how' users should contact Support.
- Get information that is needed on a recurring basis, either seasonally or based on business cycles; for example, people looking for tools to book time off or quarterly financial updates.
- Collect policies for regional or mobile users, like benefits that vary by location.
- Determine internal sites and information for common web searches; for example, traffic, public transit information, local weather, discounts available from corporate partners, and health and fitness programs.
- Find information about company-sponsored events, conferences, or retreats.
- Research common IT, HR, and support issues and frequently asked questions (FAQs) and answers.

Step 2: Leverage Subject Matter Experts (SMEs) and users

In an organization, users search for a wide range of topics ranging from simple such as office addresses, employee benefits to complex topics such as new work processes, technical information, and how-to-do content. Creating or finding such wide range of content requires knowledge and expertise in different fields, subjects, technologies etc. and a Search administrator may not have the requisite expertise or knowledge. Administrators should leverage expertise and knowledge of others in the organization to scale the amount of available content without additional resources.

Leverage SMEs

Leverage SMEs in the organization including experts from HR, support, sales, technology, and other key areas. To allow your SMEs to contribute content directly, add them as Search editors.

Involve your users

Ask users to suggest resources to bookmark. In addition to suggesting content, ask users to report errors, like broken or invalid links.

Step 3: Improve findability of content

In **Microsoft Search**, Search administrator creates Bookmarks, Q&A, Locations, and PowerApps to improve the findability of content. Each of these search components includes a title, a URL, and a set of keywords that trigger it.

Titles and descriptions

People use titles and descriptions to determine if the result answers their search query, or if they need to try a different search. Titles and descriptions should reflect the core purpose of the result. A good example of a title might be 'Childcare benefits,' with a description - 'Learn about benefits to help pay childcare costs.' This informs the users who search 'childcare' that monetary support benefits are available, and provides them a link to find out more.

Keywords

Keywords are the terms that people in your organization use to find relevant content. Associating the appropriate keywords with search results makes it easier to find the relevant content. **Microsoft Search** suggests keyword based on the title and URL for your content. To identify additional keywords, start by answering these questions:

- Which search terms are used to find the information you've identified?
- Leverage any existing taxonomy your organization uses, as well as related variations, acronyms, subjects, and topics.
- Which other variations or words do people use to talk about this information?
- Leverage your support team to determine these keywords.

For example, if you're creating a result that links to a tool for submitting vacation requests, keywords such as 'vacation' and 'submit vacation request' are good options to include. You may also find that people in your organization use 'holiday' or 'time off' to describe or search vacation related information. Adding keywords like 'holiday,' 'time off,' 'submit holiday request,' and 'request time off' will make it easier for more of your users to find the relevant content.

Reserved keywords

A reserved keyword is a unique term or phrase that triggers a result. Unlike other keywords, a reserved keyword can be associated with one result only. Use reserved keywords sparingly to allow **Microsoft Search** to learn based on usage.

For example, if you create a bookmark for a site for submitting your hours and add “log time” as a reserved keyword, users in your organization who search “log time” see the site for submitting your hours as the only bookmark in the **Microsoft Search** box.

Using keyword to group related content

If you want users to find sets of related content when they search for a term, then try using the same keyword for all related content. For example, if you're adding results about processes and tools around life status changes, you could include a keyword like 'marriage' to group together results about updating benefits, tax information, and name and alias changes.

Search settings

Use search settings to tailor your content and target specific groups of users. **Microsoft Search** has the following settings that give you additional control over when a search result appears and who sees it.

- **Dates:** Set a start date as well as an end date to control when content will be made available or unavailable. For example, time sensitive material appears in search result when it is relevant.
- **Country/region:** Select countries or regions so that only users in those locations will see the content. For example, country specific information appears in search results in those countries only.
- **Groups:** Use the Groups settings to make a result available only to members of a selected group. For example, if you're creating sites that pertain only to employees in the HR department, you could map this setting to the appropriate HR security group.
- **Device & OS:** Select device types or operating systems so that only users searching on those devices or using those systems will see that bookmark.
- **Targeted variations:** Use this setting to vary the content of the bookmark based on a user's device and location.

Step 4: Test your content

After you've created Bookmarks and Q&A, it's important to verify that:

- The correct Bookmark or Q&A appears.
- All content grouped together using keywords appear together as planned.
- No unexpected results appear in search result.
- Review whether the Bookmark or Q&A has enough information.

Users and SMEs who contributed to content creation can help test and validate the search result.

Step 5: Use insights to review and update periodically

It is important that authoritative information such as Bookmarks and Q&A are up to date.

- Fix or remove broken or invalid URL.
- Remove Bookmarks or Q&A that are no longer relevant.
- Check for tool, site name, or team name changes.
- Consider whether the Bookmark or Q&A is authoritative enough or needs a clearer description.

Microsoft Search provides usage statistics for Bookmarks, Q&A, and Locations. The usage statistics shows how users are engaging with your search results and whether users are finding what they are looking for, or are there any gaps in the available content? It helps administrator monitor performance and take appropriate actions to fine tune the search results.

Get details about Bookmarks, Q&A and Locations

See how many Bookmarks, Q&A, and Locations have been published, scheduled, or suggested. Use the dashboard to see Bookmark, Q&A, or Location totals by status:

- **Published:** The number of published results that are available to users.
- **Scheduled:** The number of scheduled results in the publish pipeline.
- **Suggested:** The number of suggestions from users.

Suggested Bookmarks, Q&A, and Locations are a good indicator of gaps in your content. It will help you understand what your users are looking for, and not finding. This could indicate that you need to create more Bookmarks, Q&A, or Locations or you need to update your existing content by using better keywords, reserved keywords, and search strings to improve the discoverability of content.

Review top search queries

Find out which searches have generated the most impressions over the last 90 days. Impression refers to how many times a page was viewed in search result. The **Top Queries** card shows the top 25 user searches for each result type with the total number of searches and their click-through rate (CTR). Use this report to identify search query volume and to determine queries with high and low search activity.

Low search count may indicate user dissatisfaction either because users are not looking for those search content or are using different keywords to find that content. CTR shows how often users select the promoted results and how useful your query rules and results are to users. A low CTR indicates that users are finding the content but are making the determination that the content does not meet their search. In such cases, administrators may decide to review the content and ensure that it corresponds with the user's search and update titles, descriptions, and keywords to align them with the user search queries.

Analyze impressions by result type

Easy-to-read graphs in the **Impression Distribution by Result Type** card show impressions over various timeframes. The timeline shows the daily number of impressions for a result type. Determine which result type is most frequently, or infrequently, used. Infrequent use of particular result type does not necessarily mean that the

result types are not good. It just shows how users are using the search result.

Use this report to understand what result types users are using and any changes in user behavior over a period of time. If a particular result type is preferred by users, administrators may decide to create more search results of the same types or to review the keywords of results types not used by users to ensure that keywords are appropriate.

Manage Acronyms answers in Microsoft Search

11/30/2020 • 4 minutes to read • Edit Online

Users often run into unfamiliar acronyms and abbreviations used by their organization or team. Terms that are specific to organizations or teams might be new to people who move from one team to another, work with internal partner teams, or are new to the organization.

Organizations don't always have a single reference for their standard terminology. Lack of a single reference makes it hard to find definitions or expansions for these acronyms. Microsoft Search solves that problem with Acronyms.

What users experience

Microsoft Search users can get definitions with Acronyms in Bing, SharePoint, and Office 365. In the **Search** box, users enter queries like these examples:

- *What is* DNN
- *Define* DNN
- DNN *definition*
- *Expand* DNN
- DNN *expansion*
- *Meaning of* DNN
- DNN *means*

The result includes all the meanings of DNN that are present within the user's organization.

> **NOTE**
> Users must enter a query that includes the acronym's specified *keywords* to trigger its corresponding answers. Acronym queries are not case sensitive.

Set up Acronyms answers

In the Microsoft 365 admin center, go to **Acronyms**, and then select **Add acronym**.

Microsoft Search queries two data sources to provide Acronyms answers to users' searches:

1. **Editorial acronyms**. Provided by IT administrators in the admin center.
2. **Mined acronyms**. Mined by Microsoft Search from the user's personal email and documents and publicly available data within the organization.

Set up editorial acronyms

Search administrators can set up editorial acronyms on the Acronyms tab in the Microsoft Search admin center. You can add acronyms from any internal site or repository to the admin center. Editorial acronyms can be added to **Published** or **Draft** state:

Published state. Acronyms are available to the organization's employees through Microsoft Search.

> **NOTE**
> It might take up to three days for acronyms added to Published state to become available in Microsoft Search.

Draft state. If admins want to review Acronyms answers before making them available in Microsoft Search, they can add the acronyms to Draft state. Acronyms added to Draft state aren't available in Microsoft Search. Admins need to add the acronyms to Published state to make them available.

Admins can add acronyms individually or bulk import them in a CSV file. Upload a CSV file with the fields shown in the following table:

ACRONYM (MANDATORY)	EXPANSION (MANDATORY)	DESCRIPTION	SOURCE	STATE (MANDATORY)
XXX	*Spelled out abbreviation*		*URL*	*Published or Draft*

CSV fields

Acronym. Contains the actual short form or acronym. An example is *DNN*.

Expansion. Contains the expansion of the acronym. An example is *Deep Neural Network*.

Description. A brief description of the acronym that gives users more info about the acronym and its expansion. For example, *A deep neural network is a neural network with a certain level of complexity, a neural network with more than two layers*.

Source. The URL of the page or website where you want users to go for more information about the acronym.

State. This field can take two values:

- **Draft**. Adds the acronym to the Draft state.
- **Published**. Adds the acronym to the Published state and makes it available in Microsoft Search.

Mined acronyms

It might be a challenge for admins to add all the acronyms used within an organization to Answers. This feature can find acronyms that search administrators aren't even aware of. To do that work, Microsoft Search also mines acronyms from these sources:

- Users' emails.
- Documents in SharePoint, Microsoft OneDrive, and Microsoft OneNote.
- Public documents within the organization that users have access to in SharePoint, OneDrive, or OneNote.

Microsoft Search makes sure that only users with access and permissions to a document can see the acronyms that are mined from it. When an acronym is mined from a user's mailbox, only that user can see that acronym.

> **NOTE**
> No setup is needed for mined acronyms.

Frequently asked questions

Q: How is editorial and mined data ranked?

A: The feature currently ranks editorial acronyms above mined acronyms.

Q: How long does it take for editorial acronyms to be visible in Microsoft Search after they're published?

A: It takes up to three days for acronyms added to Published state to become available in Microsoft Search.

Q: How do users trigger Acronyms answers?

A: To get Acronyms answers, users must enter specific query patterns in a Bing, SharePoint, or Office 365 **Search** box.

Q: How long does it take for mined acronyms to appear after you receive or send a new email or document?

A: Mined acronyms from a new email or document take up to seven days to appear in Microsoft Search results.

Q: Do documents need to be in a specific format for mining to pick them up?

A: No. We support all file types except image, folders, and zip files.

Q: Will Microsoft mine acronyms from documents in all languages?

A: Microsoft only supports mining from documents in English. Support for other languages will be added in phases.

Q: What if my organization doesn't want to show mined acronyms? Can I stop showing mined acronyms in search results?

A: To turn off showing mined acronyms in search results, create a customer support ticket by following the instructions at Contact support for business products. After you create a support ticket, it takes up to 48 hours for mined acronyms to stop appearing in search results.

Manage bookmarks

11/30/2020 • 4 minutes to read • Edit Online

You can create a bookmark in just a few steps. Each bookmark includes a title, a URL, and a set of keywords that trigger it. You can also add categories to a bookmark that can be used for sorting and filtering in the admin portal. A bookmark can have several keywords and bookmarks can share the same keyword, but reserved keyword can't be shared. When a bookmark is created or modified, the search index is refreshed immediately, and the bookmark is available to users immediately.

If your organization set up Promoted Results in SharePoint, you can import the Promoted Results into **Microsoft Search** and make the imported content available to your users. This is an easy way to quickly populate search results as soon as you set up **Microsoft Search** and make it more effective for your users. We recommend using promoted results from SharePoint as a reference to understand how to name and create relevant search results.

Add or edit a single bookmark

1. In the Microsoft 365 admin center, go to **Bookmarks**.
2. To add a bookmark, select **Add**. To edit a bookmark, select the bookmark in the relevant bookmark list.
3. As you add or edit the information, the preview automatically updates.
4. Save your changes.

Add or edit bookmark using browser extensions

Search administrators can create search content easily by using browser extensions. Install the browser extension, go to the site you want to add as bookmark, and add the bookmark.

Currently, browser extensions are available for Edge and Chrome.

- To download Edge extensions, go to Microsoft Store and download the app.
- To download Chrome extensions, go to Chrome web store and download the app.

Bulk add or edit bookmarks

Use the Import or Export feature to bulk create or edit bookmarks. It makes adding or editing a large number of bookmarks faster and easier. Use it to:

- Bulk add bookmarks - Add details in the bookmark template file, and then import it.
- Bulk edit bookmarks - Export bookmarks to a .csv file, then edit the bookmark details in the exported .csv file, and then import the updated .csv file.
- Import promoted sites from SharePoint.
- Backup bookmarks - Export bookmarks to a .csv file.

To import or export bookmarks:

1. In the upper-right corner of **Bookmarks** tab, select **Import**. Select **Export** to download all the existing bookmarks in a .csv file.
2. In the right pane, choose the option to import using a .csv file or from SharePoint. Download the template file for a list of the required fields and details.
3. Add or edit bookmark details in the template file, and then save it on your computer.
4. In the **Import bookmarks** pane, select **Browse** and then the .csv file that you want to import.

5. Select **Import**.

Here are some important points about the template file:

- Never edit data in these fields: *ID*, *Last Modified*, and *Last Modified By*
- If you include the *ID* of an existing bookmark, it will be replaced with the information in the import file.
- For existing bookmark with the same title or URL, the bookmark will be updated with information in the import file.
- Not all fields in the template file are required and required fields vary depending on the bookmark state.
- Based on the *State* field, bookmarks will be saved as draft, suggested, scheduled, or they'll be published automatically.
- For partners who manage multiple organizations, you can export your bookmarks from one org and import them into another. But you must remove the data in the *ID* column before you import.

Prevent import errors

You'll get an error if any required data is missing or invalid, and a log file is generated with more information about the rows and columns to be corrected. Make necessary edits and try importing the file again. You cannot import or save any bookmarks until all errors are resolved.

To prevent errors, make sure your import file is properly formatted and:

- Includes the header row and all the columns that were in the import template
- The column order is the same as the import template
- All columns have values, except the three that can be empty: *ID*, *Last Modified*, and *Last Modified By*
- The *State* column is not empty, it's required information

To prevent bookmark-to-bookmark duplication errors:

- Don't use duplicate URLS for different bookmarks. If a URL is assigned to another bookmark and you try to add it again from an import file, you'll get an error. This also applies to duplicate URLs for other types of answers.
- When updating existing bookmarks, use the *bookmark ID* column. You can update any other property of an existing bookmark, such as keyword or description, but you should make sure the *bookmark ID* is in the appropriate column of the import file. If the *bookmark ID* is present, it won't be treated as new addition and won't be processed as an error.

Power Apps

Help your users complete tasks, such as entering vacation time or reporting expenses, by adding existing Power Apps to your bookmarks.

Power Apps explained

Power Apps is a service that lets you build business apps that run in a browser or on a phone or tablet with no coding experience required. Power Apps work in any browser and on any device and take less than a minute to add. For more on Power Apps, see:

- Guided Learning
- Documentation
- Power Apps Home

Add a Power App to a bookmark

1. Find the App ID for the Power App that you want to add.
2. In the Microsoft 365 admin center, go to **Bookmarks**.
3. Add a bookmark or find an existing bookmark that you want to add a **Power App** to.
4. In **Bookmark settings**, select **Power App**, and enter or paste the **App ID**. The height and width are

automatically adjusted based on the orientation that was selected when the Power App was created. Bookmarks support both portrait and landscape orientations. The bookmark preview shows a fully functional PowerApp to make it easy to test.

5. Select **Publish** or **Save to Draft**.

Manage floor plans

11/30/2020 • 6 minutes to read • Edit Online

Floor plans in **Microsoft Search** help users find people and meeting rooms within a building. Floor plans answer the following questions:

- Where is Allan Deyoung's office?
- Building 2 floor 3
- Find 2/11173

Add floor plans

Follow these steps to setup floor plans answers in **Microsoft Search**.

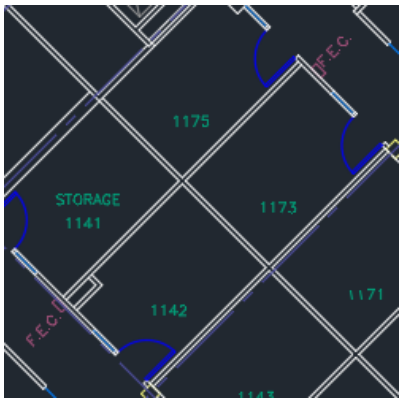
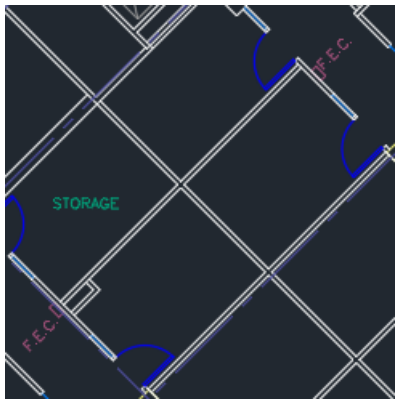
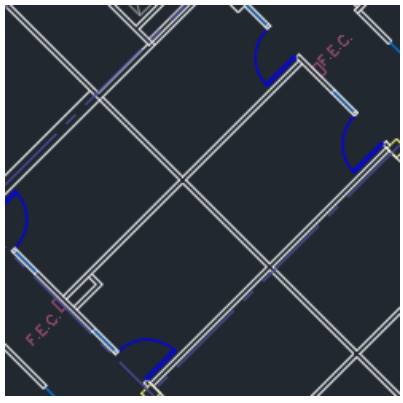
Step 1: Determine your building codes

Building codes are used as part of a user's office location. You'll use these codes when updating user profiles. Let's say your organization has a building at this location: *Building 2, 350 5th Avenue, New York City, NY 10016*

Here are some good examples for this building's code: 2, B2, Building2, Building 2, or NYCB2. Each building must have a unique code.

Step 2: Review your floor plans

Floor plans files must be in DWG format; DWG files can contain text labels. When a text label marks a room, it is called a room label. The DWG file must have **at least 10 rooms** marked with labels. Here are some examples of DWG files with different label types:

TEXT LABELS INCLUDING ROOM LABELS	TEXT LABELS BUT NO ROOM LABELS	NO TEXT LABELS
		

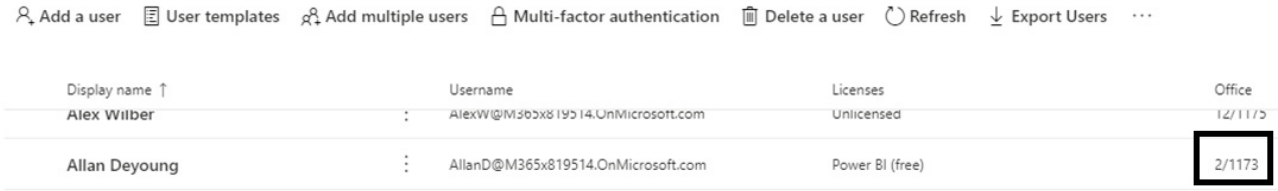
See the FAQ section for information on viewing and updating DWG files.

Step 3: Update office locations on user profiles

A user's office location is a combination of a building code and a room label. For example, if the building code is *2* and the room label is *1173*, the office location would be *2/1173*.

Add or update office locations for each user in your organization. You can change office location on the user profile in the Microsoft 365 admin center or you can change in your on-premises Active Directory to sync into Azure Active Directory. *PhysicalDeliveryOfficeName* is the field that is used for office location. If your room labels do not include floor numbers, see the FAQ for tips.

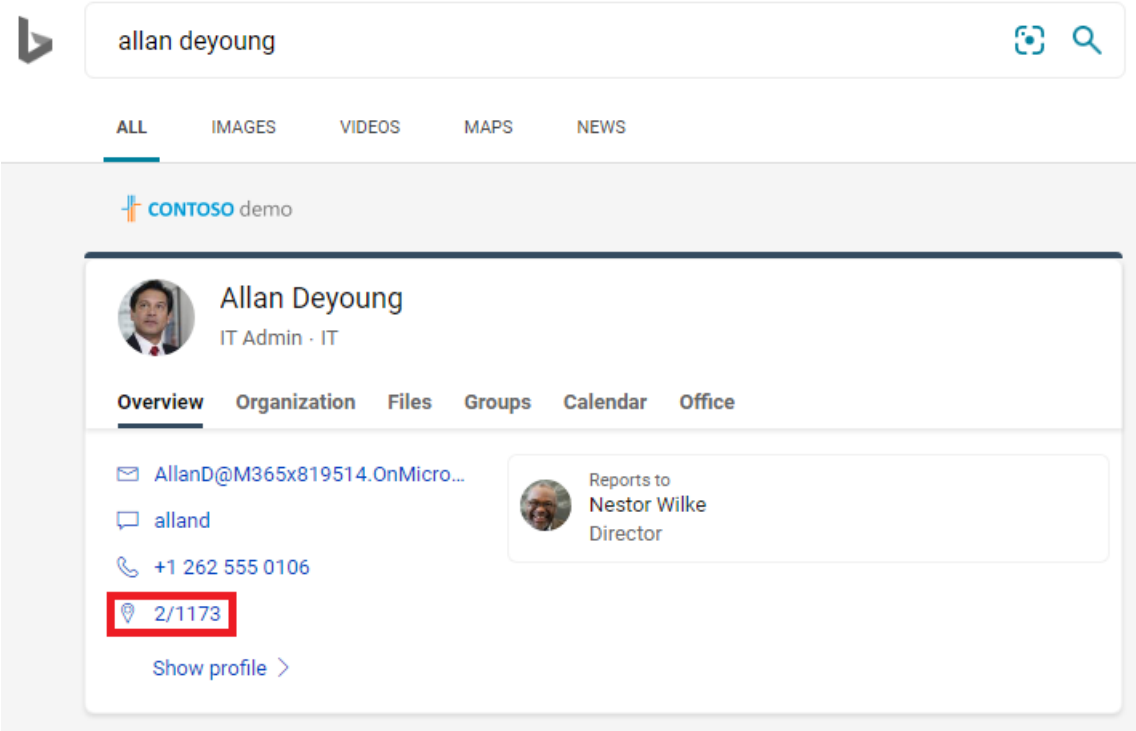
In this example, Allan's office is in room 1173 on floor 1 of building 2.



> **NOTE**
>
> To see updated office locations when searching for floor plans, you must update office locations for **at least 10 people** on each floor.

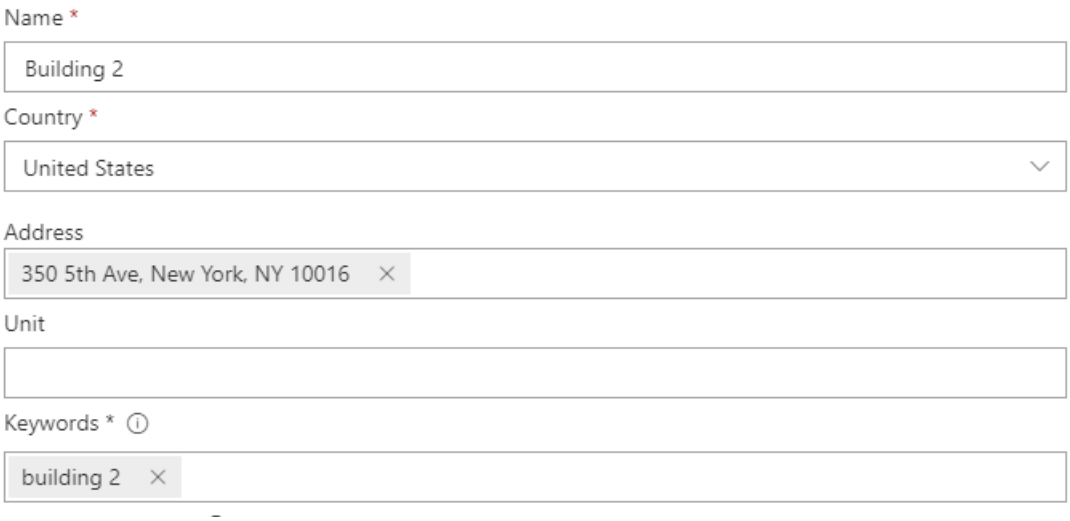
Step 4: Verify office location

Use **Microsoft Search** to find a user and verify that their office location is appearing correctly. If you have just updated locations, you may need to wait up to **72 hours** for the updates to appear in the search results.



Step 5: Add building locations

Floor plans uses Locations to define your buildings. In the Microsoft 365 admin center, go to **Locations**, and then select **Add**. Enter the name, address, and keywords for the building. Add as many buildings as you need.

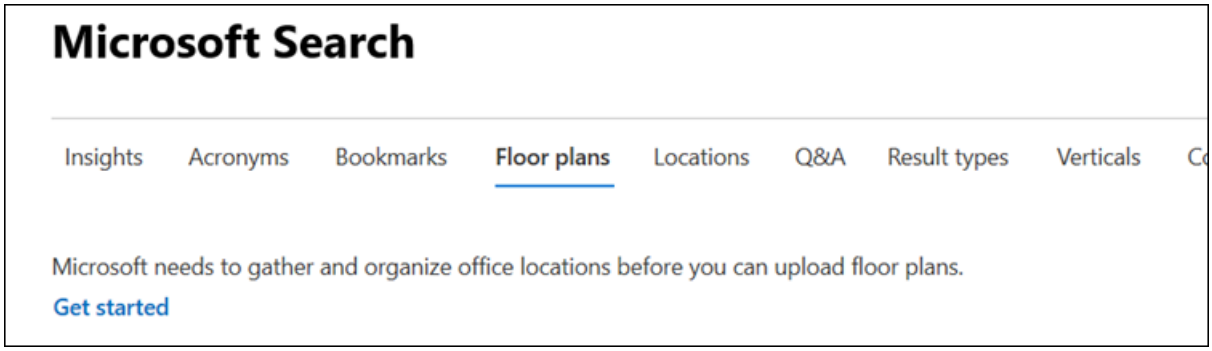


For more details about locations, see Manage Locations

Step 6: Gather and organize office locations

Before you can use floor plans, office locations must be indexed. This is a one-time operation that can take up to 48 hours to complete. The total time will depend on the size of your organization.

In admin center, go to **Floor plans**, and then select **Get started**. If you don't see this notice, this step has already been completed for your organization

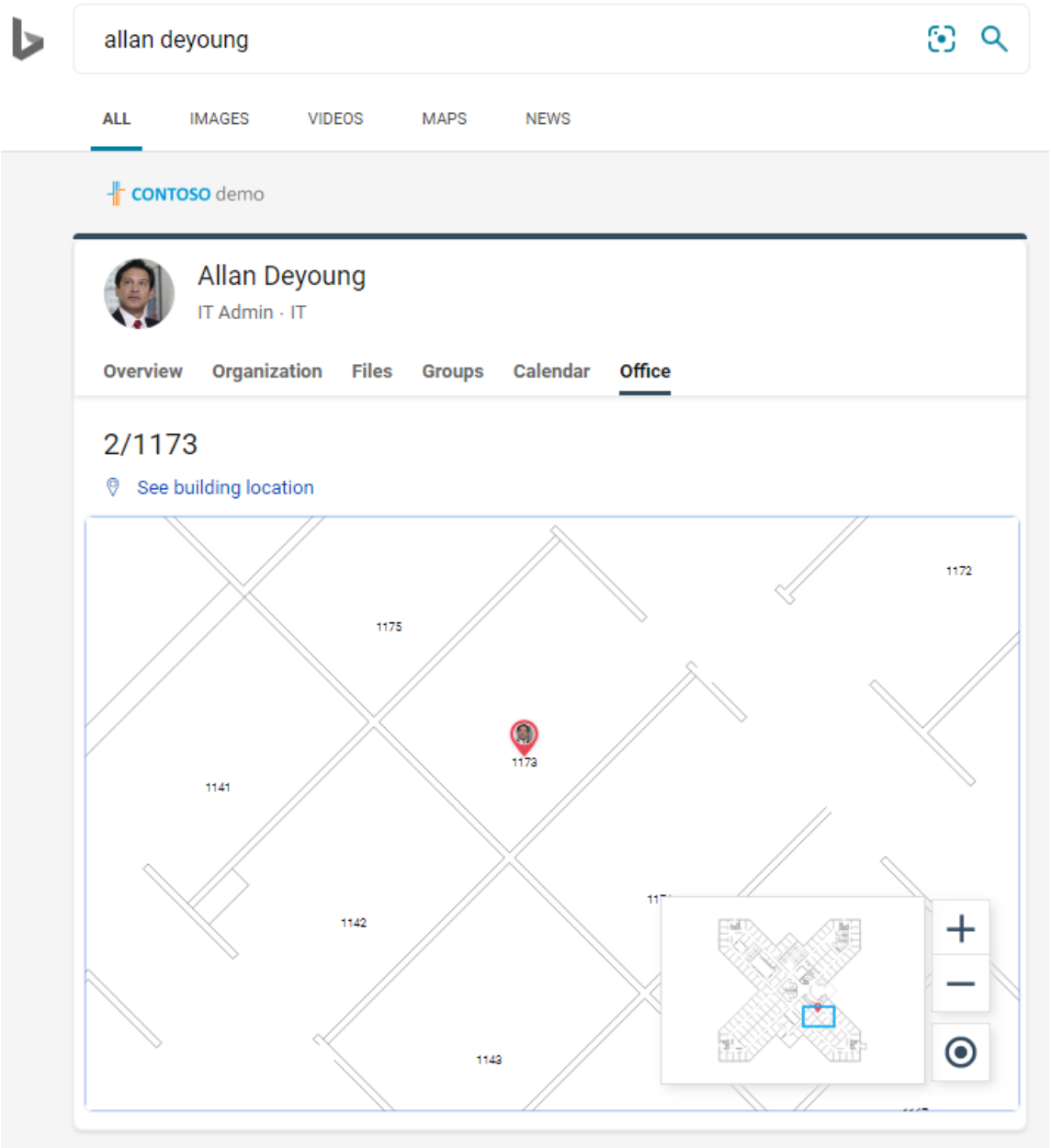


Step 7: Upload floor plans

1. In the admin center, go to **Floor plans**.
2. Select a building in the drop-down list and select **Next**. If the building isn't listed, go back and add building locations.
3. Select **Upload files**, and then choose the floor plan you are uploading.
4. When the upload is complete, you must enter floor number that is represented in the floor plan file. Then select **Next**.
5. (Optional) If your floor has wings or zones, enter that detail.
6. You will see a review screen listing how many office locations were mapped to the floor plans. Select **Details** to ensure the mapping is correct.
   - If no users are mapped or you're not satisfied with the mapping, select **Continue mapping**. To publish, select **Skip and publish**.
7. Enter the building code for this floor plan. The building code can be found on users' office location property. For example, if a user's office location is **2/1173**, then the building code is **2**.
8. On the review screen, repeat step 6 to ensure the mapping is correct.
9. (Optional) Review and identify the location patterns for all uploaded floor plans and then select **Next**.
10. On the review screen, repeat step 6 to ensure the mapping is correct.
11. When you're ready, select **Publish** to make the floor plan available in **Microsoft Search**.

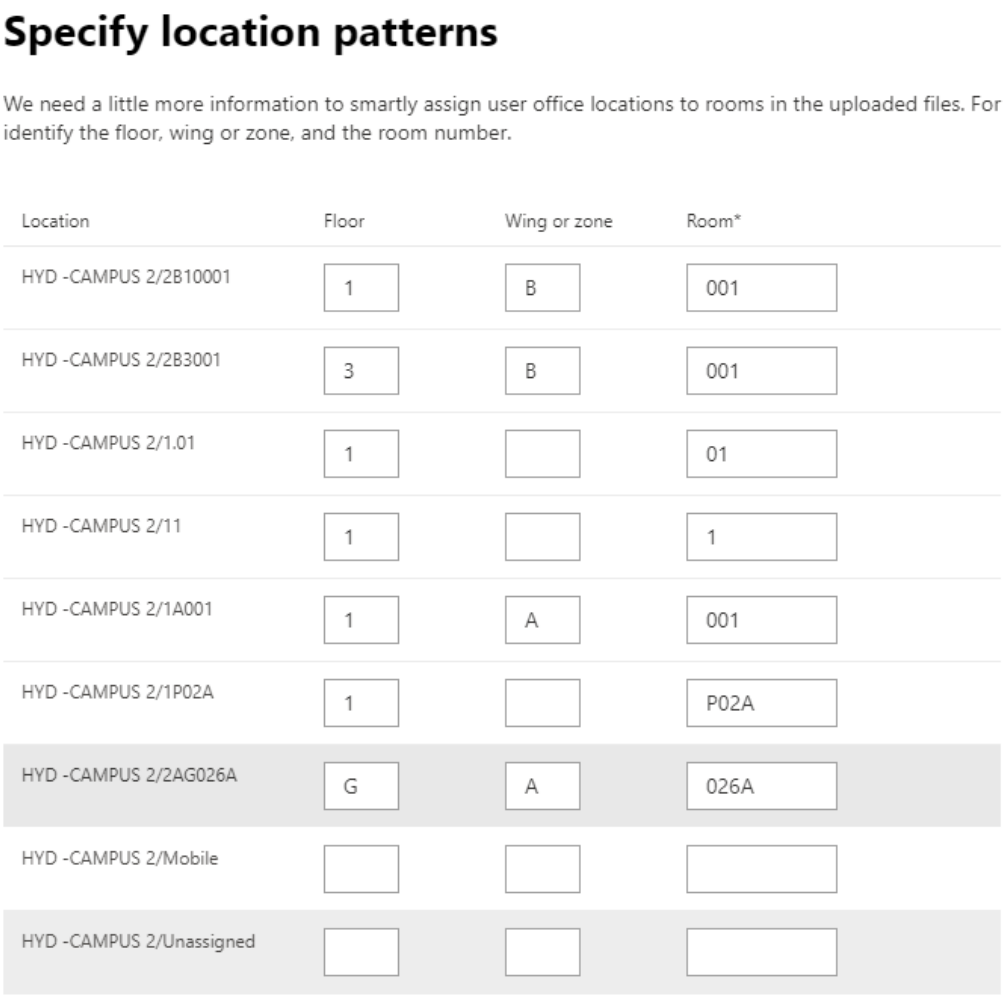
NOTE

It takes 48 hours for the floor plans to be published. After that your users will see a floor plan results similar to the one below when they search for a co-worker's office.



Step 8: (Optional) Specify location patterns

After uploading a floor plan, the text labels will be compared to the office locations in your users' profiles. If there are fewer than 10 matches, the **Specify location patterns** screen appears. Location patterns are used to extract floor, wing, and room information from office locations.



Only room is required, floor and wing are optional, and you can skip locations as needed.

Edit floor plans

To update an existing floor plan, select the floor plan you want to change, and then select **Edit**. Make your changes and save them.

Troubleshooting

STEP	ERROR MESSAGE	TYPE	ACTION
Upload floor plans	Unable to read CC_1.dwg. Please re-upload or delete the floor plan.	Error	Try uploading the file again. If that doesn't work delete the file and try again.
Upload floor plans	There are two files named CC_1.dwg. Please delete one of them or re-upload with another name.	Error	If the file name is incorrect make the file name unique by adding floor or wing information and then upload the file again. If you accidentally added the same file twice just delete it.

STEP	ERROR MESSAGE	TYPE	ACTION
Upload floor plans	No data found.	Error	Check your file to make sure it's the correct one and then upload it again or delete it.
Upload floor plans	External references are missing in this file. Either upload CC_1_furniture.dwg or delete this file.	Warning	Upload external reference files or delete.
Upload floor plans	Could not read room numbers or tags in the DWG file. Please delete this file.	Warning	Check your DWG file to make sure the data is included and then delete the file and try again.
Link office locations	No office locations found in Azure Active Directory. Add location data to Azure Active Directory before setting up floor plans.	Error	Update office locations on user profiles

Frequently asked questions

Q: How do I view and edit DWG files?

A: Use any of these options to view DWG files:

- Upload the file to SharePoint and open it.
- Open the file in Microsoft Visio or Autodesk DWG TrueView.
- Upload the file to Autodesk's Online Viewer.

Q: How do I add text labels to unmarked rooms?

A: Open the DWG file in an editor and add room labels.

Q: How do I create or edit DWG files for testing purposes?

A: Create a DWG file in Microsoft Visio, Autodesk AutoCAD, or any other DWG editor. Make sure 10 or more rooms are labeled in the file.

Q: What's the best format for text labels in DWG files?

A: For the best results, text labels should contain floor numbers and room numbers. The examples below use 2 or SC for the building code.

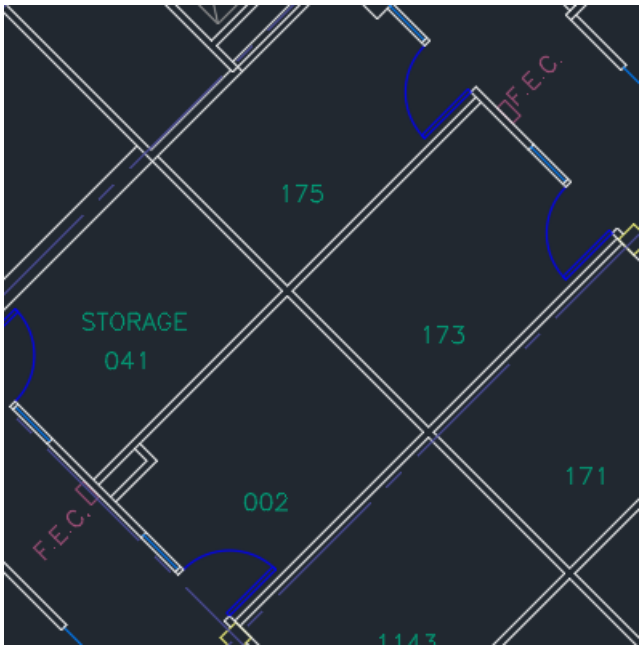
ROOM LABEL TYPES	FLOOR	ROOM	SAMPLE TEXT LABEL	OFFICE LOCATION (BUILDING CODE/TEXT LABEL)
Has floor and room number	1	173	1173	2/1173
	21	45	21045	2/21045
	23	100K	23-100K	2/23-100K
	1	G06-07	1G06-07	2/1G06-07

ROOM LABEL TYPES	FLOOR	ROOM	SAMPLE TEXT LABEL	OFFICE LOCATION (BUILDING CODE/TEXT LABEL)
	2	1024A	02.1024A	2/02.1024A
	2	1024A	02.1024A	2/02.1024A
	2	105.01	2105.01	2/2105.01
Has building code, floor, and room number	0	X-11-M-12	2-0-X-11-M-12	2/2-0-X-11-M-12 2-0-X-11-M-12
	2	128A	22128A	2/22128A 22128A
	1	B2-11	21-B2-11	2/21-B2-11 21-B2-11
	2	45	SC2045	SC/SC2045 SC2045

Q: Can I use a DWG file that doesn't include floor numbers?

A: Yes, you can. When you update office locations in the user's Azure Active Directory profile, include the floor number as part of the room number, even if it's missing from the DWG file. After you upload the file, the Specify location patterns screen will appear and you can indicate both values.

For example, a DWG file that includes room numbers, but no floor numbers, may look similar to this:



The office location in the user's profile should be 2/1175 where '2' is the building code, '1' is the floor number, and '175' is the room number.

Manage locations

11/30/2020 • 2 minutes to read • Edit Online

Location

Location helps your users find addresses and locate your organization's buildings by providing an accurate location for offices, campuses, and buildings, along with directions and navigation. Administrators should add all important locations of your organization. Unlike Bookmarks and Q&A, the index is not refreshed immediately, and it can take several hours for new or changed locations to appear in search results.

Add or edit a single location

1. In the Microsoft 365 admin center, go to **Locations**
2. To add a new location, select **Add**.
3. To edit a location, select the location in the relevant locations list.
4. As you add or edit the information, the preview automatically updates.
5. Save your changes.

Bulk add or edit locations

Administrators can use the Import or Export feature to bulk add or edit locations.

Use the import/export feature to:

1. Bulk add location - Add details in the location template file, and then import it.
2. Bulk edit locations - Export locations to a .csv file, then edit the location details in the exported .csv file, and then import the updated .csv file.
3. Backup locations – Export existing locations to a .csv file.

To export or import locations:

1. In the upper-right corner of the **Locations** tab, select **Import**. Select **Export** to download the existing locations in a .csv file.
2. In the right pane, choose the option to import using a .csv file. Download the template file for a list of the required fields and details.
3. Add or edit location details in the template file, and then save it on your computer.
4. In the **Import** locations pane, select **Browse**, and then the .csv file that you want to import.
5. Select **Import**.

Here are some important points regarding the template file:

- Never edit data in these fields: *Id*, *Last Modified*, and *Last Modified By*
- If you include the *Id* of an existing location, it will be replaced with the information in the import file.
- If there is an existing location with the same name, the location will be updated with information in the import file.
- Not all fields in the template file are required and required fields vary depending on the location state.
- Based on the *State* field, locations will be saved as draft, suggested, scheduled, or they will be published automatically.
- For partners who manage multiple organizations, you can export your locations from one org and import them into another. But you must remove the data in the *Id* column before you import.

NOTE

You cannot import Locations if there are any errors in the template file. To prevent errors, make sure your import file is properly formatted and include all the required information.

For more information on how to prevent error, see Prevent import errors.

Manage Q&As

11/30/2020 • 2 minutes to read • Edit Online

Creating a Q&A is similar to creating bookmarks. Q&As allow you to answer the user's questions instead of just providing a link to a webpage. You can also format the answer in rich text. If a bookmark and a Q&A share the same keyword, the bookmark result is shown first. Like bookmarks, the Q&A index is refreshed immediately after a Q&A is added or changed.

Add or edit a single Q&A

1. In the Microsoft 365 admin center, go to **Q&A**
2. To add a Q&A, select **Add**. To edit a Q&A, select the Q&A in the relevant Q&A list. As you add or edit the information, the preview automatically updates.
3. Save your changes.

Supported HTML tags

You can use existing HTML content or add HTML tags to your answer (description). Unsupported tags are ignored.

The following HTML tags are supported:

- blockquote
- div
- em
- h1, h2, h3, and h4
- ol, ul, and li
- p
- pre
- span
- strong
- table, thead, tbody, tr, th, and td
- u
- a
- code
- br
- hr
- img

Add or edit Q&As using browser extensions

Search administrators can create search content easily by using browser extensions. Install the browser extension, and then go to the site from which you want to generate a Q&A. You can then create the Q&A and include a link to the source site.

Currently, browser extensions are available for Microsoft Edge and Chrome.

- To download extensions for Edge (Legacy), go to Microsoft Store.
- To download extensions Chrome or Edge (Chromium), go to the Chrome web store.

Bulk add or edit Q&As

Administrators can use the Import and Export features to bulk create or edit Q&As.

Use the Import/Export feature to:

- Bulk add Q&As - Add details in the Q&A template file, and then import it.
- Bulk edit Q&As - Export Q&As to a .csv file, edit the Q&A details in the exported file, and then import the file.
- Back up Q&As - Export Q&As to a .csv file.

To import or export Q&As:

1. In the upper-right corner of the Q&A tab, select **Import**. Select **Export** to download all the existing Q&As in a .csv file.
2. In the right pane, select the option to import by using a .csv file. Download the template file to get a list of the required fields and details.
3. Add or edit Q&A details in the template file, and save it on your computer.
4. In the **Import Q&A** pane, select **Browse**, and then select the .csv file that you want to import.
5. Select **Import**.

Important template file tips:

- Never edit data in these fields: **Id**, **Last Modified**, and **Last Modified By**
- If you include the **Id** of an existing bookmark, it will be replaced with the information in the import file.
- If there's an existing bookmark that has the same title or URL, the bookmark will be updated with information in the import file.
- Not all fields in the template file are required, and the required fields vary depending on the bookmark state.
- Based on the **State** field, bookmarks are saved as *draft*, *suggested*, or *scheduled*, or they are published automatically.
- For partners who manage multiple organizations: You can export your bookmarks from one org and import them into another. But you must remove the data in the **Id** column before you import.

> **NOTE**
>
> You can't import Q&As if there are any errors in the template file. To prevent errors, make sure your import file is properly formatted, and include all the required information.

For more information about avoiding errors, see Prevent import errors.

Overview of Microsoft Graph connectors

11/30/2020 • 2 minutes to read • Edit Online

Microsoft Search indexes all your Microsoft 365 data to make it searchable for users. With Microsoft Graph connectors, your organization can index third-party data so it appears in Microsoft Search results. This expands the types of content sources that are searchable in your Microsoft 365 productivity apps and the broader Microsoft ecosystem. The third-party data can be hosted on-premises or in the public or private clouds.

The rest of this article is intended to help Microsoft 365 administrators locate the resources that are avaiable to answer the following questions:

- What data sources can be connected to Microsoft Search?
- How do I manage my connections?
- What are the license requirements and terms of use for Graph connectors?
- How do I customize and configure search results?
- How do I search my connector data from a custom application?

> **IMPORTANT**
> Microsoft Graph connectors and Microsoft Search APIs are now generally available. The first rollouts will be to customers configured for targeted release. If you want to use a Graph connector in your tenant, users and administrators must opt into Targeted release.

What data sources can be connected to Microsoft Search?

Microsoft provides ten Graph connectors and our ecosystem partners have created over 100 additional Graph connectors. You can also build your own Graph connector.

Graph connectors by Microsoft

You can connect to the following data sources using Graph connectors created by Microsoft:

- Azure Data Lake Storage Gen2
- Azure DevOps
- Azure SQL
- Enterprise websites
- MediaWiki
- Microsoft SQL Server
- File share
- Oracle (preview)
- Salesforce (preview)
- ServiceNow

The Graph connectors gallery contains a brief description of each of these Graph connectors. If you are ready to connect one of these data sources to your tenant, be sure to read the Setup overview and any other articles in the Setup connectors by Microsoft section that apply to your data source.

Graph connectors by our partners

The Microsoft Graph connectors gallery includes a brief descriptions of each of the Graph connectors created by our partners and a link to each partner's website. Contact each partner directly to learn more.

Build your own Graph connector

If you plan to build your own Graph connector, see the Overview of the Microsoft Search API in Microsoft Graph for more information.

How do I manage my connections?

You can manage your connections from the Connectors tab in the Microsoft 365 admin center. See Manage your connections for more information.

What are the license requirements and terms of use for Graph connectors?

You need a valid Microsoft 365 or Office 365 license and sufficient Graph Connectors quota for users in your organization to view data from connectors in their search results.

To learn more, see License requirements and pricing and Terms of use.

How do I customize and configure search results?

There are a number of ways to customize and configure search results. See the following articles to learn more:

- Manage verticals and result types
- Manage search result layouts
- Manage result cluster
- Manage custom filters

How do I search my connector data from a custom application?

After custom data is indexed, developers can query this data. You can view your data in any application. For more information, see the Overview of the Microsoft Search API in Microsoft Graph.

Microsoft Graph connectors preview release and features

11/30/2020 • 2 minutes to read • Edit Online

Microsoft Graph connectors and Microsoft Search APIs are now generally available. The initial rollout will be to customers configured for Targeted Release. Upon rollout completion to all tenants, index quota utilization from connectors content will become subject to billing. See Licensing requirements and pricing for more information.

Set up Targeted release

If you want to use Graph connectors in your tenant during rollout, you must opt into Targeted release. To learn more about the Targeted release option and how to set it, see Set up the Standard or Targeted release options in Office 365.

Preview features

Although Microsoft Graph connectors and Microsoft Search APIs are now generally available, there are several features that will remain in preview.

The set of connectors and features in preview include:

- Azure DevOps connector
- Salesforce connector
- ServiceNow connector with search permissions that use source ACLs
- Manage result cluster

In this article

Connectors by Microsoft

Azure Data Lake Storage Gen2

by Microsoft

With this Microsoft Graph connector, users in your organization can search for files and content stored in Azure Blob containers. The Azure Data Lake Storage Gen2 connector also indexes hierarchy-enabled folders in Azure Data Lake Storage Gen2 accounts that you specify.

More details

Azure DevOps

by Microsoft

With this Microsoft Graph connector, users in your organization can search for work items in your Azure DevOps instance.

More details

Azure SQL

by Microsoft

With this Microsoft Graph connector, users in your organization can search for data from your Azure SQL Database.

More details

Enterprise websites

by Microsoft

With this Microsoft Graph connector, users in your organization can search over pages in any non-SharePoint enterprise website.

More details

MediaWiki

by Microsoft

With this Microsoft Graph connector, users can search for knowledge-based articles on wiki sites your organization creates with MediaWiki.

More details

Microsoft SQL

by Microsoft

With this Microsoft Graph connector, users in your organization can search for data in on-premises Microsoft SQL server databases.

More details

Salesforce

by Microsoft

With this Microsoft Graph connector, users in your organization can search for Contacts, Opportunities, Leads and Accounts objects from your Salesforce instance.

More details

ServiceNow

by Microsoft

With this Microsoft Graph connector, users in your organization can search for knowledge-based articles from your ServiceNow instance.

More details

Connectors by our Partners

Aderant

by BA Insight

The Aderant connector honors the security of the source system and provides both full and incremental crawls, so the users have the latest information available to them all the time.

More details

Adobe AEM

by Raytion

Connector for Adobe AEM. Indexes pages, attachments, and other generated document types from Adobe AEM in near real time. The connector fully supports AEM's built-in user and group management, as well as AEM installations based on Active Directory and other directory services. 6th generation Raytion search connector.

More details

Adobe Experience Manager

by Accenture

The Adobe Experience Manager (AEM) connector will crawl content from an Adobe Experience Manager server. The connector fetches access control lists for document level security (currently only Closed Users Groups). It can filter content based on properties using expected values or patterns or pages based on the scheduled on and off time.

More details

Alfresco

by BA Insight

The Alfresco Connector is built on the BAI connector framework, which is the platform used to build all our connectors and provides secure connectivity to enterprise systems.

More details

Alfresco Content Services

by Raytion

Connector for Alfresco One. Indexes documents, folders, and user profiles from Alfresco One in near real time. The connector fully supports Alfresco's built-in user and group management, as well as Alfresco installations based on Active Directory and other directory services. 6th generation Raytion search connector.

More details

Amazon Aurora

by BA Insight

The Amazon Aurora Connector is built upon industry standard database access methods, so it equally supports databases from other systems such as Oracle, MySQL, and IBM DB2.

More details

Amazon RDS

by BA Insight

The Amazon RDS Connector is built upon industry standard database access methods, so it can equally support databases from other systems such as Oracle, MySQL, and IBM DB2.

More details

Amazon S3

by Accenture

The Amazon S3 connector will crawl content from any Amazon Simple Storage Service. Each file is submitted with its metadata (size, location, last accessed, etc.). Updates are discovered automatically.

More details

Amazon S3

by BA Insight

The Amazon S3 Connector works with all content stored in S3. Your organization can use the connector to securely connect to S3 and index content from S3 buckets. Powerful filtering capabilities give your organization control about what content found in S3 should be indexed.

More details

Atlassian Confluence

by Accenture

The Confluence connector will crawl content from any Confluence content repository. The connector retrieves spaces, pages, blogs, attachments and comments. The connector uses the Confluence REST API to crawl Confluence content.

More details

Atlassian Confluence

by Raytion

Connector for Atlassian Confluence. Indexes pages, blog posts, attachments, comments, spaces, profiles and hub sites for tags from on-premise Confluence instances in near real time. The connector fully supports Confluence's built-in user and group management, as well as Confluence installations based on Active Directory and other directory services. 6th generation Raytion search connector.

More details

Atlassian Confluence Cloud

by Raytion

Connector for Atlassian Confluence Cloud. Indexes pages, blog posts, attachments, comments, spaces, profiles and hub sites for tags from on-premise Confluence instances in near real time. The connector fully supports Confluence Cloud's built-in user and group management. 6th generation Raytion search connector.

More details

Atlassian Jira

by Raytion

Connector for Atlassian Jira. Indexes projects, issues, attachments, comments, work logs, issue histories, links, and profiles from on-premise Jira instances in near real time. The connector fully supports Jira's built-in user and group management, as well as Jira installations based on Active Directory and other directory services. 6th generation Raytion search connector.

More details

Atlassian Jira Cloud

by Raytion

Connector for Atlassian Jira Cloud. Indexes projects, issues, attachments, comments, work logs, issue histories, links, and profiles from on-premise Jira instances in near real time. The connector fully supports Jira Cloud's built-in user and group management. 6th generation Raytion search connector.

More details

Azure Blob Storage

by Accenture

The Azure Blob Storage connector will crawl content from the Azure Blob Container. Each blob is submitted with its metadata (size, location, last accessed, etc.). Updates are discovered automatically.

More details

Azure Data Lake

by Accenture

The Azure Data Lake connector will crawl content from the ADLS cloud at either root or specified paths. Each file is submitted with its metadata (size, location, last accessed, etc.). Updates are discovered automatically.

More details

Azure Event Hub

by Accenture

The Event Hub connector fetches events from Azure streams and submits them after performing an optional transform.

More details

Azure SQL Database

by BA Insight

BA Insight's Azure SQL Database Connector is built upon industry standard database access methods, so it can equally support databases from other systems such as Oracle, MySQL, and IBM DB2.

More details

Box

by BA Insight

The Box connector makes it possible to surface content from Box in SharePoint and other portals, enabling users to get integrated search results from SharePoint and Box.

More details

Box

by Raytion

Connector for Box. Indexes files, folders, comments, users, groups, and tasks from Box in near real time. The connector fully supports Box' built-in user and group management. 6th generation Raytion search connector.

More details

Box

by Accenture

Box connector will crawl content from a Box repository. The connector will retrieve the supported elements using the RESTful API (Content API Basics 2.0 version); for authentication, it uses Box API (that uses OAuth 2). Each file is submitted with its metadata (size, location, last accessed, etc.). Updates are discovered automatically.

More details

Confluence

by BA Insight

The Confluence Connector is an enterprise grade indexing connector that enables content stored in Confluence to be crawled and indexed. This enables SharePoint, or any other portal, to serve as the single point from which users can search and retrieve the content they need from multiple content sources.

More details

CuadraSTAR

by BA Insight

The CuadraSTAR Connector crawls content in CuadraSTAR and creates a single index that makes it possible to use Microsoft Search to find relevant information within CuadraSTAR, as well as over 70 other supported repositories, eliminating the need to perform separate searches.

More details

Deltek

by BA Insight

The Deltek Vision Connector honors the security of the source system and provides both full and incremental crawls, so users always have the latest information available to them. It indexes content from Deltek Vision into Azure, SharePoint Online, or SharePoint 2016/2013, surfacing it through BA Insight's SmartHub to provide users with integrated search results.

More details

Documentum / Documentum DQL

by Accenture

The Documentum Connector will crawl content from any Documentum content repository. DQL is a query language that allows you to perform very complex queries involving specialized searching capabilities for document and content management. The Aspire Documentum DQL connector will crawl content from Documentum.

More details

Elasticsearch

by Accenture

The Elasticsearch connector will crawl content from an Elastic index using a user-defined query. It can identify updates automatically or use a timestamp in the index.

More details

Elite / E3

by BA Insight

BA Insight's Elite Connector provides a single point of access for lawyers to access firm content and knowledge in line with Elite content using Microsoft Search.

More details

EMC eRoom

by BA Insight

The eRoom Connector establishes a secure connection to the eRoom application and maps the content, including metadata and attachments, from the eRoom schema to the search engine schema. It then extracts content and feeds it to the search engine in a process called crawling.

More details

eRoom

by Accenture

The eRoom connector will crawl content from an eRoom server instance (site) with an enabled XML Query option (Allow XML queries and commands from external applications).

More details

e-Spirit FirstSpirit

by Raytion

Connector for FirstSpirit. Indexes pages, attachments, and other generated document types from FirstSpirit in near real time. The connector fully supports FirstSpirit's built-in user, group and permission management, as well as FirstSpirit installations based on Active Directory and other directory services. 6th generation Raytion search connector.

More details

Facebook Workplace

by BA Insight

Organizations who leverage Workplace by Facebook can now extend the reach of this data into their existing search indexes via the BA Insight Workplace by Facebook Connector.

More details

Facebook Workplace

by Raytion

Connector for Facebook Workplace. Indexes project groups, conversations and shared documents from Facebook Workplace in near real time. The connector fully supports Facebook Workplace's built-in user and group management. 6th generation Raytion search connector.

More details

File Share

by BA Insight

The File Share Connector makes it possible to surface content from File Shares (Windows, SMB/CIFS) in a single consolidated search index, along with content from other repositories.

More details

File System

by Accenture

The File System connector crawls local file (or locally mounted) systems, traversing folders to build a complete index. It generates a signature for each item to allow incremental updates of only changed items. Each file is submitted with its metadata (size, location, last accessed, etc.).

More details

File System

by Raytion

Connector for local file systems. Indexes files and folders from locally mounted file systems in near real time. 6th generation Raytion search connector.

More details

FTP

by Accenture

The Aspire File Transfer Protocol (FTP) connector provides access to files and folders on an FTP server. Each file is submitted with its metadata (size, location, last accessed, etc.). Updates are discovered automatically.

More details

GitLab

by Raytion

Connector for GitLab. Indexes projects, files, folders, commit messages, issues, and wiki pages from GitLab in near real time. The connector fully supports GitLab's built-in user and group management. 6th generation Raytion search connector.

More details

Google Cloud SQL

by BA Insight

The Google Cloud SQL Connector indexes content from Google Cloud SQL into the Microsoft Search index surfacing it through BA Insight's SmartHub to provide users with integrated search results.

More details

Google Drive

by Raytion

Connector for Google Drive. Indexes files, folders, and comments from Google Drive in near real time. The connector fully supports Google Drive's built-in permission model and the user and group management in the Google Admin Directory. 6th generation Raytion search connector.

More details

Hbase

by Accenture

The HBase connector will crawl data from an HBase Server.

More details

HDFS

by Accenture

The Hadoop Distributed File system (HDFS) connector will crawl content from any given HDFS Cluster using the WebHDFS http interface. Each file is submitted with its metadata (size, location, last accessed, etc.). Updates are discovered automatically.

More details

HP Consolidated Archive (EAS)

by BA Insight

BA Insight's HP Consolidated Archive Connector securely indexes both the full text and metadata of documents in archives into various search engines, including SharePoint Search and Azure Search. This enables a single searchable result set across content from multiple repositories. It allows organizations to tap into the wealth of information accessible within Consolidated Archive, SharePoint and other repositories, making that data instantly actionable to users through search.

More details

IBM Connections

by Accenture

The IBM Connections connector will crawl content from IBM Connections server.

More details

IBM Connections

by BA Insight

The IBM Connections Connector was specifically developed for IBM Connections, establishing a secure connection to the Connections application and mapping the content, including metadata and attachments, from the Connections schema to the search engine schema. It then extracts content and feeds it to the search engine in a process called crawling.

More details

IBM Connections

by Raytion

Connector for IBM Connections. Indexes public and personal files, blogs, wikis, forums, communities, bookmarks, profiles, and status updates from on-premises Connections instances in near real time. The connector fully supports Connection's built-in user and group management, as well as Connections installations based on Active Directory and other directory services. 6th generation Raytion search connector.

More details

IBM Connections Cloud

by Raytion

Connector for IBM Connections Cloud. Indexes public and personal files, blogs, wikis, forums, communities, profiles, and status updates from Connections Cloud in near real time. The connector fully supports Connections Cloud's built-in user and group management. 6th generation Raytion search connector.

More details

IBM Content Manager

by BA Insight

The IBM Content Manager Connector honors the security of source applications and provides both full and incremental crawls, so users always have the latest information available to them.

More details

IBM Db2

by BA Insight

The Db2 Connector allows organizations to tap into the wealth of data stored within DB2 databases and applications and make that data instantly actionable to users through search.

More details

IBM FileNet P8

by BA Insight

The IBM FileNet Content Manager Connector allows SharePoint, as well as other portal users, to securely search for content stored in FileNet repositories. Access to content is determined by security established in FileNet, ensuring that your content is as safe when accessed through any other portal as it is directly within FileNet.

More details

IBM Lotus Notes

by BA Insight

With BA Insight's IBM Notes Email Connector, users have the ability to search Notes emails directly from within SharePoint or another portal. Security defined within IBM Notes is automatically reflected in the search experience, so users will see search results from their own mailbox, public mailboxes, and other mailboxes for which they have been granted access.

More details

IBM Notes

by Raytion

Connector for IBM Notes. Indexes records from a configurable set of databases from Notes instances in near real time. The connector fully supports Notes' built-in user and group management. 6th generation Raytion search connector.

More details

IBM WebSphere

by BA Insight

BA Insight's WebSphere Connector securely indexes both the full text and metadata of WebSphere objects into Microsoft's search engine, enabling a single searchable result set across content from multiple repositories. This allows organizations to tap into the wealth of information accessible within Microsoft platforms, and makes that data instantly actionable to users through search.

More details

iManage Work

by BA Insight

The iManage Work Connector provides full security and operates at high throughput to minimize crawl times while maintaining a low-performance impact on Work. It only requires read access, and there is no need to install client software on any iManage server. This results in seamless and simultaneous access to all content stored in iManage Work.

More details

JIRA Issues

by Accenture

The Jira Issues connector is a simple connector for extracting issues from Jira, either inside the corporate firewall or to Jira cloud.

More details

Jive

by Accenture

The JIVE connector will crawl content from any JIVE Community with an enabled REST API v3. The connector will retrieve documents stored in spaces, groups, projects, and blogs and any sub-folders contained in it.

More details

Jive

by BA Insight

The Jive Connector was specifically developed for Jive, establishing a secure connection to the Jive application and mapping the content including metadata and attachments from the Jive schema to the search engine schema. It then extracts content and feeds it to the search engine in a process called crawling.

More details

Jive

by Raytion

Connector for Jive. Indexes discussions, polls, files, blogs, spaces, groups, projects, tasks, videos, messages, ideas, profiles, and status updates from on-premise and cloud-hosted Jive instances in near real time. The connector fully supports Jive's built-in user and group management and supports Jive's native authentication models, OAuth, and Basic authentication. 6th generation Raytion search connector.

More details

Kafka

by Accenture

The Kafka connector fetches messages from a Kafka message stream and submits them after performing an optional transform.

More details

Kinesis

by Accenture

The Kinesis connector fetches data from Amazon Kinesis Data Streams and submits them after performing an optional transform.

More details

LDAP

by BA Insight

The LDAP Connector enables organizations to connect to any LDAP-compliant directory and index any record from it. Organizations can filter to specific subsets of the directory and retrieve only specific fields, making it simple to search for users, contacts, or groups stored anywhere in your directory.

More details

LDAP

by Raytion

Connector for LDAP-compatible directory services. Indexes LDAP objects from Active Directory, Novell E-Directory, and other LDAP-compatible directory services in near real time. The connector can be used for ingesting principals into

Microsoft Search for use cases like expert, equipment, and location searches, or for implementing security trimming for custom data sources. The connector supports LDAP over SSL. 6th generation Raytion search connector.

More details

LegalKEY

by BA Insight

BA Insight's OpenText LegalKEY Connector securely indexes both the full text and metadata of client and matter records in LegalKEY into the Microsoft search engine, enabling a single searchable result set across content from multiple repositories. This allows organizations to tap into the wealth of information accessible within LegalKEY, SharePoint, and other repositories, making that data instantly actionable to users through search.

More details

LexisNexis InterAction

by BA Insight

The LexisNexis InterAction Connector makes it easier for lawyers and other firm employees throughout the organization to find important information stored in InterAction without the need to directly log in and perform a separate search.

More details

Lotus Notes

by Accenture

The Lotus Notes connector will crawl content and attachments from Lotus Notes.

More details

Lotus Notes Databases

by BA Insight

With the IBM Notes Database Connector, users have the ability to find content stored in Notes databases using Microsoft Search. Security defined within IBM Notes is automatically reflected in the search experience, which ensures that users see content for which they are authorized. Ultimately, users can find everything they need in one place.

More details

MediaPlatform PrimeTime

by BA Insight

BA Insight's MediaPlatform PrimeTime indexing connector makes it possible to make the content accessible to users via an organization's enterprise search platform, combining the connector with BA Insight's SmartHub. The BA Insight MediaPlatform PrimeTime Connector retrieves information about channels and videos from MediaPlatform PrimeTime and indexes them via Microsoft Search.

More details

MediaWiki

by Raytion

Connector for MediaWiki. Indexes pages, discussion pages, and attachments from MediaWiki instances in near real time. The connector fully supports MediaWiki's built-in permission model, as well as MediaWiki installations based on Active Directory and other directory services. 6th generation Raytion search connector.

More details

Micro Focus Content Manager (HPE Records Manager/HP TRIM)

by BA Insight

The HP TRIM Connector was specifically developed for HP Records Manager, establishing a secure connection to the TRIM application and mapping the content, including metadata and attachments, from the TRIM schema to the search engine schema. It then extracts content and feeds it to the search engine in a process called crawling.

More details

Microsoft Azure AD

by Raytion

The connector indexes Azure Active Directory objects via the Graph API. The connector can be used for ingesting principals into Microsoft Search in near real time for use cases like expert, equipment, and location searches, or for implementing early-binding security trimming in conjunction with custom data sources. The connector supports federated authentication against O365. 6th generation Raytion search connector.

More details

Microsoft SharePoint

by Raytion

Connector for SharePoint on-premises instances. Indexes sites, webs, modern (SharePoint 2016 and later) and classic pages, wiki pages, OneNote documents, list items, tasks, calendar items, attachments, and files in near real time. The connector fully supports SharePoint's built-in user and group management, as well as installations with Active Directory but also OAuth providers like SiteMinder and Okta. The connector comes with support for Basic, NTLM, and Kerberos authentication. 6th generation Raytion search connector.

More details

Microsoft SQL Server

by BA Insight

The database connector is built upon industry standard database access methods, so it can equally support databases from other systems such as Oracle, MySQL, and IBM DB2. It honors the security of the source database and provides both full and incremental crawls, so users always have the latest information available to them.

More details

Microsoft Windows File Server

by Raytion

Connector for windows file systems, such as DFS. Indexes files and folders from such file systems in near real time. 6th generation Raytion search connector.

More details

Microsoft Yammer

by Raytion

Connector for Yammer. Indexes channels, posts, replies, attachments, polls, and announcements from Yammer in near real time. The connector fully supports Yammer's built-in user and group management and in particular federated authentication towards O365. 6th generation Raytion search connector.

More details

MySQL

by BA Insight

The MySQL connector is built upon industry standard database access methods, so it can equally support databases from

other systems such as Oracle, MySQL, and IBM DB2. It honors the security of the source database and provides both full and incremental crawls, so users always have the latest information available to them.

More details

NetDocuments

by BA Insight

The NetDocuments Connector indexes content stored in NetDocs so that users can search and retrieve NetDocuments content directly from within their portal. The connector applies document security in NetDocs to Microsoft Search automatically, so user information remains secure. Metadata stored in NetDocuments can be mapped to equivalent terms so that users have a seamless search experience.

More details

Nuxeo

by BA Insight

The Nuxeo connector lets organizations index their Nuxeo content, including both security information and standard and custom metadata set on content into Microsoft Search alongside content present in Office 365. Ultimately, users can find everything they need in one place.

More details

Objective

by BA Insight

The Objective Connector was specifically developed for Objective, establishing a secure connection to Objective and mapping the content including metadata from the Objective schema to the search engine schema. It then extracts content and feeds it to the search engine in a process called crawling.

More details

OneDrive

by Accenture

The OneDrive connector will crawl content from Microsoft OneDrive, traversing folders to find files. It generates a signature for each item to allow incremental updates of only changed items. Each file is submitted with its metadata (size, location, last accessed, etc.) and access control lists.

More details

OpenText Content Server

by Raytion

Connector for OpenText ContentServer. Indexes files, folders, virtual folders, compound documents, news, emails, volumes, collections, classifications, and many more objects from Content Server instances in near real time. The connector fully supports OpenText ContentServer's built-in user and group management. 6th generation Raytion search connector.

More details

OpenText Documentum

by BA Insight

BA Insight's Documentum Connector securely indexes both the full text and metadata of Documentum objects into Microsoft Search, enabling a single searchable result set across content from multiple repositories. This is unlike some other connectors that surface Documentum records with Microsoft Search one at a time for process management.

More details

OpenText Documentum

by Raytion

Connector for Documentum. Indexes repositories, folders, and files together with their metadata and properties from Documentum in near real time. The connector fully supports Documentum's built-in user and group management. 6th generation Raytion search connector.

More details

OpenText eDOCS DM

by BA Insight

Users of the OpenText eDOCS DM Connector are able to search for content housed in eDOCS repositories directly from within Microsoft Search, eliminating the need to perform multiple searches to locate needed content. Security established within eDOCS is maintained by the connector to make certain that content is only seen by those who have been granted access.

More details

OpenText Livelink/RM

by BA Insight

With the OpenText Livelink Connector, users are able to search both Livelink and Microsoft data with a single query. Security defined in Livelink is automatically reflected in the search experience, which ensures that users only see content for which they are authorized. Ultimately, users can find everything they need in one place.

More details

Oracle Database

by BA Insight

The Oracle Database Connector is built upon industry standard database access methods, so it can equally support databases from other systems such as Microsoft SQL Server, MySQL, and IBM DB2.

More details

Oracle Knowledge Advanced Cloud

by Raytion

Connector for Oracle KA. Indexes pages and attachments from Oracle Knowledge Advanced Cloud in near real time. The connector fully supports Oracle KA's built-in user and group management. In particular, the connector handles snippet-based permissions within Oracle KA pages. 6th generation Raytion search connector.

More details

Oracle WebCenter

by BA Insight

The WebCenter Connector integrates WebCenter with Microsoft Search, making it easier for users throughout the organization to find important information stored in WebCenter without the need to directly log in and perform a separate search.

More details

Oracle WebCenter Content (UCM/Stellent

by BA Insight

The WebCenter Content Connector fully supports the underlying security of all content made available to Microsoft Search and keeps this content up to date via scheduled crawls, ensuring users get the most recent updates when performing a

search.

More details

Pironet NDH pirobase CMS

by Raytion

Connector for pirobase CMS. Indexes pages, attachments, and other generated document types from pirobase CMS in near real time. The connector fully supports pirobase CMS' built-in user and group management. 6th generation Raytion search connector.

More details

PostgreSQL

by BA Insight

BA Insight's PostgreSQL Connector honors the security of the source database and provides full and incremental crawls, so users always have the latest information available. It indexes content from PostgreSQL into Microsoft Search, surfacing it through BA Insight's SmartHub to provide users with integrated search results.

More details

RDBMS Server

by Accenture

The Database Server connector will crawl content from a Relational Database server. The crawler discovers databases and tables and indexes all content. Updates are discovered automatically.

More details

Relational databases

by Accenture

Crawls content from relational databases using third-party JDBC drivers. Updates are identified automatically or use an update table. An SQL select statement is used to control the data submitted. Access control lists can be extracted from a returned column.

More details

RSS

by Accenture

The Aspire RSS connector allows you to retrieve feed information and trigger flows when new items are published in an RSS feed.

More details

Salesforce

by Accenture

The Salesforce connector will crawl content from any Salesforce Summer '16 (version 37). The connector will retrieve the supported elements using the SOAP API and the user's Salesforce Chatter feeds using the REST API.

More details

Salesforce

by Raytion

Connector for Salesforce. Indexes accounts, KM, profiles, leads, cases, and all other objects represented by records from Salesforce in near real time. The connector fully supports Salesforce's built-in user and group management. 6th generation

Raytion search connector.

More details

Salesforce

by BA Insight

The Salesforce Connector integrates Salesforce's Service, Sales, and Marketing Cloud with Microsoft Search, making all the content within Salesforce available to all employees through this portal.

More details

SAP ERP

by BA Insight

BA Insight's SAP ERP Connector is designed to bring items from SAP into a search index. This in turn lights up the UI and allows for a unified view across information in SAP, SharePoint, and other systems.

More details

SAP HANA

by BA Insight

The SAP HANA Connector honors the security of the source database and provides both full and incremental crawls, so users always have the latest information available to them. It indexes content from SAP HANA into Microsoft Search, surfacing it through BA Insight's SmartHub to provide users with integrated search results.

More details

SAP NetWeaver Portal

by Raytion

Connector for SAP NetWeaver Portal. Indexes pages, attachments, and other document types from SAP NetWeaver Portal, KMC, and PDC areas in near real time. The connector fully supports SAP NWP's built-in user and group management, as well as NWP installations based on Active Directory and other directory services. 6th generation Raytion search connector.

More details

SAP PLM DMS

by Raytion

Connector for SAP PLM. Indexes documents, attachments, and other records from SAP PLM in near real time. 6th generation Raytion search connector.

More details

ServiceNow

by Accenture

The Service Now connector will crawl content from ServiceNow.

More details

ServiceNow

by BA Insight

The ServiceNow Connector honors the security of the source system and provides both full and incremental crawls, so users always have the latest information available to them.

More details

ServiceNow

by Raytion

Connector for ServiceNow. Indexes issues, tasks, attachments, KM articles, and pages, among others from ServiceNow in near real time. The connector supports ServiceNow's built-in user and group management. 6th generation Raytion search connector.

More details

SharePoint 2013

by Accenture

The SharePoint 2013 connector will crawl content from any SharePoint 2013 site collection URL. The connector supports lists, pages, and sites, and updates are identified either automatically or via the SharePoint change log.

More details

SharePoint 2016

by Accenture

The SharePoint 2016 connector will crawl content from any SharePoint 2016 site collection URL. The connector supports lists, pages, and sites, and updates are identified either automatically or via the SharePoint change log.

More details

SharePoint Online

by Accenture

The SharePoint Online connector will crawl content from any SharePoint Online site collection URL. The connector will retrieve Sites, Lists, Folders, List Items, and Attachments as well as other pages (in .aspx format). This connector supports SharePoint running in the Microsoft O365 offering. Support for crawling the on-premise offerings of SharePoint is supported by SharePoint 2010/2007 Connector and SharePoint 2013 Connector.

More details

Sitecore

by BA Insight

The Sitecore Connector honors the security of the source system and provides both full and incremental crawls, so users always have the latest information available to them.

More details

Sitecore

by Raytion

Connector for Sitecore. Indexes pages, attachments, and further generated document types in near real time. The connector fully supports Sitecore's permission model and the user and group management in the associated Active Directory. 6th generation Raytion search connector.

More details

Slack

by Raytion

The connector for Slack efficiently and robustly synchronizes Slack content with Microsoft Search. It robustly indexes messages, threads, and shared files from all public channels in near real time. The connector ensures that all documents come with a comprehensive set of metadata, which allows for development of the best search experience. Even in vibrant environments the Slack connector keeps track of all changes and guarantees an updated search index.

More details

SMB

by Accenture

The SMB connector crawls files and directories across shared drives. It generates a signature for each item to allow incremental updates of only changed items. Each file is submitted with its metadata (size, location, last accessed, etc.) and access control lists.

More details

SMB File Share

by Raytion

Connector for SMB File Share indexing. Indexes files and folders in near real time. The current versions of SMB2 and SMB3 are supported. 6th generation Raytion search connector.

More details

SMTP

by Accenture

The SMTP connector will process e-mails sent to it. The email and attachments are submitted with metadata such as to, from, and subject.

More details

SQL Database

by Raytion

Connector for SQL servers, such as Oracle, Microsoft SQL or Postgres. Indexes and interprets records from database tables and views in near real time.

More details

Any SQL-based CRM system

by BA Insight

The SQL Server Connector is built upon industry standard database access methods, so it can equally support databases from other systems such as Oracle, MySQL, and IBM DB2. It honors the security of the source database and provides both full and incremental crawls, so users always have the latest information available to them.

More details

StageR

by Accenture

The StageR connector will crawl content from the StageR (NodeJS) staging repository - an intermediate repository that allows content access without reaching back into original repositories.

More details

Symantec Enterprise Vault

by Raytion

Connector for Enterprise Vault. Indexes archived data, such as e-mails, attachments, files, calendar items, and contacts in near real time. The connector fully supports Enterprise Vault's authentication models Basic, NTLM, and Kerberos authentication. 6th generation Raytion search connector.

More details

TeamForge

by Accenture

The TeamForge connector will crawl content from a TeamForge server through its SOAP services.

More details

Twitter

by Accenture

The Twitter connector will crawl content from Twitter feeds. It collects tweet text and metadata including URL links, geo location, and hashtags

More details

Veeva Vault

by BA Insight

BA Insight's Veeva Vault Connector securely indexes both the full text and metadata of Veeva Vault objects into Microsoft Search. This enables users to retrieve a single result set for content within Veeva Vault and Microsoft 365.

More details

Veritas Enterprise Vault

by Raytion

Connector for Enterprise Vault. Indexes archived data, such as e-mails, attachments, files, calendar items, and contacts in near real time. The connector fully supports Enterprise Vault's authentication models Basic, NTLM, and Kerberos authentication. 6th generation Raytion search connector.

More details

Veritas Enterprise Vault (Symantec eVault)

by BA Insight

The Veritas Enterprise Vault Connector honors the security of the source system and provides full and incremental crawls, so users always have the latest information available to them.

More details

Web Crawler

by Accenture

The Aspider Web Crawler connector will crawl content from one or more websites. The content is submitted along with any metadata provided by the server.

More details

windream ECM-System

by Raytion

Connector for windream ECM-System. Indexes files and folders from windream ECM-System in near real time. 6th generation Raytion search connector.

More details

Xerox DocuShare

by BA Insight

Users of the Xerox DocuShare Connector are able to search for content housed in Docushare repositories directly from within Microsoft Search, eliminating the need to perform multiple searches to locate needed content.

More details

Xerox DocuShare

by Raytion

Connector for Xerox DocuShare. Indexes data repositories, folders, profiles, groups, and files in near real time. The connector fully supports DocuShare's built-in user and group management. 6th generation Raytion search connector.

More details

Yammer

by Accenture

The Yammer connector will crawl content from Yammer messages and metadata including sender, group, and thread details. It runs from any machine with access to the AEM server and optionally supports content fetching and connection throttling.

More details

Yammer

by BA Insight

The Yammer Connector establishes a secure connection to the Yammer application and maps the content including metadata and attachments from the Yammer schema to the search engine schema. It then extracts content and feeds it to the search engine in a process called crawling.

More details

Setup overview for Graph connectors by Microsoft

11/30/2020 • 7 minutes to read • Edit Online

This article summarizes the basic process required to use the Microsoft 365 admin center to setup any of the Graph connectors by Microsoft. The basic process includes the following steps:

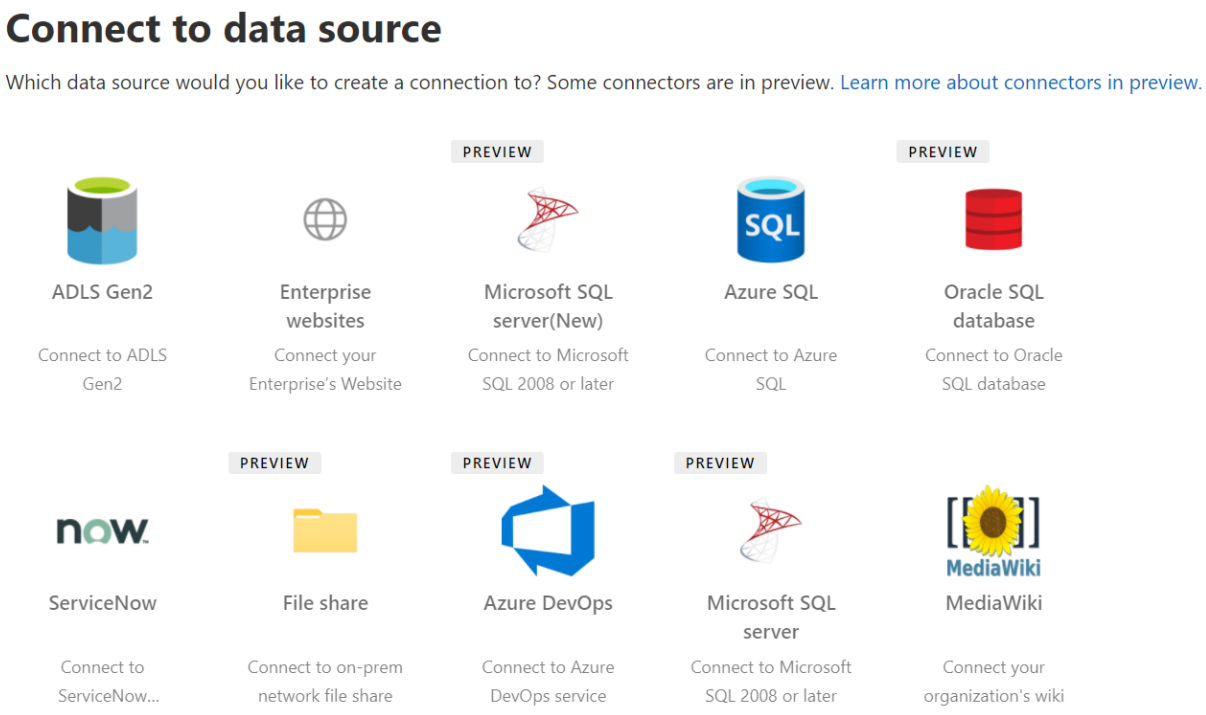
1. Add a Graph connector in the Microsoft 365 admin center.
2. Name the connection.
3. Configure the connection settings.
4. Manage search permissions.
5. Assign property labels.
6. Manage schema.
7. Choose refresh settings.
8. Review the connection.

It is important to note that the setup process is very similar for all the Graph connectors by Microsoft but is not exactly the same. **In addition to reading this article, be sure to read the connector-specific for your data source.**

Step 1: Add a Graph connector in the Microsoft 365 admin center

Complete the following steps to configure any of the Microsoft-built connectors.

1. Sign into your admin account in the Microsoft 365 admin center
2. In the navigation pane, select **Settings**, and then select **Search & intelligence**. Select the Connectors tab.
3. Select **+Add**, and then select the data source of your choice from the menu of available options.



[!Note:] You can add a maximum of ten Graph connections to each tenant.

Step 2: Name the connection

You will need to specify these attributes:

- Name
- Connection ID
- Description (optional)

The connection ID creates implicit properties for your connector. It must contain only alphanumeric characters and be a maximum of 32 characters.

Step 3: Configure the connection settings

The process to configure the Connection settings varies based on the type of data source. See the Connector-specific information for the type of data source you want to add to your tenant to complete this step in the setup process.

To learn more about connecting to an on-premises data source, see Install an on-premises data gateway.

Step 4: Manage search permissions

Access Control Lists (ACLs) determine which users in your organization can access each item of data.

Some connectors like Microsoft SQL and Azure Data Lake Storage Gen2 natively support Azure Active Directory (Azure AD) ACLs.

Other connectors like ServiceNow, Azure DevOps, and Salesforce support syncing of non-Azure AD users and groups.

Step 5: Assign property labels

You can assign semantic labels to your source properties on the "Assign property labels" page. Labels are well known tags provided by Microsoft that provide semantic meaning. They allow Microsoft to integrate your connector data into Microsoft 365 experiences such as enhanced search, people cards, intelligent discovery, and more.

The following table lists the currently supported labels and their descriptions.

LABEL	DESCRIPTION
title	The title for the item that you want shown in search and other experiences
url	The target url of the item in the source system
createdBy	Name of the person who created the item
lastModifiedBy	Name of the person who most recently edited the item
authors	Name of the people who participated/collaborated on the item
createdDateTime	When was the item created
lastModifiedDateTime	When was the item most recently edited

LABEL	DESCRIPTION
fileName	Name of the file item
fileExtension	Type of file item such as .pdf or .word

The properties on this page are pre-selected based on your data source, but you can change this selection if there is a different property that is better suited for a particular label.

The label **title** is the most important label. It is **strongly recommended** that you have a property assigned to this label in order for your connection to participate in the result cluster experience.

Incorrectly mapping labels will cause a deteriorated search experience. It is okay for some labels to not have a property assigned to it.

Step 6: Manage schema

Content property

It is strongly recommended that you select a **Content Property" from the drop-down menu of options, or keep the default if one is present. This property is used for full-text indexing of content, search results page snippet generation, result cluster participation, language detection, HTML/text support, ranking and relevance, and query formulation.

If you select a content property, you will have the option of using the system-generated property **ResultSnippet** when you create your result type. This property serves as a placeholder for the dynamic snippets that are generated from the content property at query time. If you use this property in your result type, snippets will be generated in your search results.

Creating aliases for source properties

You can add aliases to your properties under the "Alias" column on the "Manage schema" page. Aliases are friendly names for your properties. They are used in queries and in the creation of filters. They are also used to normalize source properties from multiple connections such that they have the same name. That way you can create a single filter for a vertical with multiple connections. See Customize the search results page for more information.

Search schema attributes

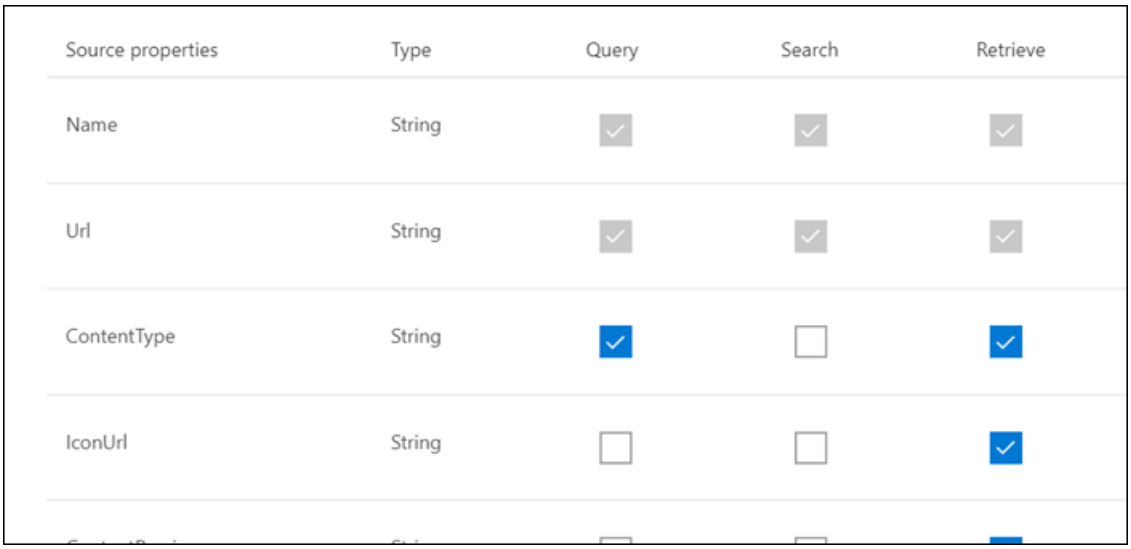
You can set the search schema attributes to control search functionality of each source property. A search schema helps determine what results display on the search results page and what information end users can view and access.

Search schema attributes include **searchable**, **queryable**, **retrievable**, and **refinable**. The following table lists each of the attributes that Microsoft Graph connectors support and explains their functions.

SEARCH SCHEMA ATTRIBUTE	FUNCTION	EXAMPLE
SEARCHABLE	Makes the text content of a property searchable. Property contents are included in the full-text index.	If the property is **title**, a query for **Enterprise** returns answers that contain the word **Enterprise** in any text or title.
QUERYABLE	Searches by query for a match for a particular property. The property name can then be specified in the query either programmatically or verbatim.	If the **Title** property is queryable, then the query **Title: Enterprise** is supported.

SEARCH SCHEMA ATTRIBUTE	FUNCTION	EXAMPLE
RETRIEVABLE	Only retrievable properties can be used in the result type and display in the search result.	
REFINABLE	Refinable properties can be used as in the Microsoft Search results page.	Users in your organization can filter by **lastModifiedDateTime** in the search results page if the property is marked refinable during connection setup

For all connectors except the File share connector, custom types must be set manually. To activate search capabilities for each field, you need a search schema mapped to a list of properties. The connection wizard automatically selects a search schema based on the set of source properties you choose. You can modify this schema by selecting the check boxes for each property and attribute in the search schema page.



Restrictions and recommendations for search schema settings

- The **content** property is searchable only. Once selected in the dropdown, this property cannot be marked **retrievable** or **queryable**.
- Significant performance issues occur when search results render with the **content** property. An example is the **Text** content field for a ServiceNow knowledge-base article.
- Only properties marked as retrievable render in the search results and can be used to create modern result types (MRTs).
- Only string properties can be marked searchable.

> **NOTE**
> After you create a connection, you **can't** modify the schema. To do that, you need to delete your connection and create a new one.

Step 7: Refresh settings

The refresh interval determines how often your data is synced between the data source and Microsoft Search. Each type of data source has a different set of optimal refresh schedules based on how often data is modified and the type of modifications.

There are two types of refresh intervals, which are **Full refresh** and **Incremental refresh**, but incremental

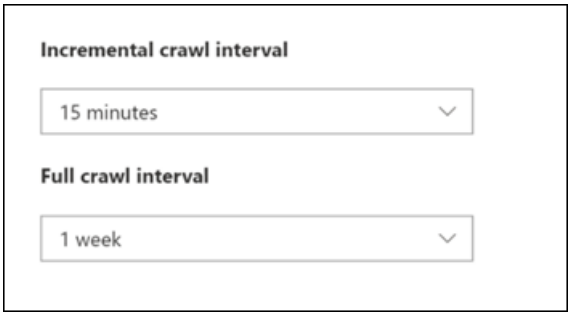
refreshes are not available for some data sources.

With a full refresh, the search engine processes and indexes every item in the content source, regardless of previous crawls. A full refresh works best for these situations:

- Detecting deletions of data.
- The incremental refresh failed to update content due to errors.
- ACLs were modified.
- Crawl rules were modified.
- When schema for the connection has been updated (schema updates are not yet supported)

With an **Incremental refresh**, the search engine can process and index only the items that were created or modified since the last successful crawl. Therefore, not all the data in the content source is re-indexed. Incremental refreshes work best to detect content, metadata, permission, and other updates.

Incremental refreshes are much faster than full refreshes because unchanged items aren't processed. However, if you choose to run incremental refreshes, you will still need to run full refreshes periodically to maintain an accurate data sync between the content source and the search index.



Step 8: Review connection

You can review your entire configuration and edit settings as needed before completing the connection. **Be sure to read the connector-specific information for your data source if you have not already done so.** Select **Finish updating** when you are ready to complete the connection.

How do I know the connection setup worked?

Go to the list of your published connections under the **Connectors** tab in the admin center. To learn how to make updates and deletions, see Manage your connector.

Map your non-Azure AD Identities

11/30/2020 • 3 minutes to read • Edit Online

This article walks you through the steps of mapping your non-Azure AD identities to your Azure AD identities so that people in your Access Control List (ACL) with non-Azure AD identities can see connector search results scoped to them.

These steps are only relevant to search administrators who are setting up a ServiceNow or Salesforce connectors by Microsoft with search permissions for "Only people with access to this data source" and identity type "Non-AAD."

> **NOTE**
>
> If you are setting up a Salesforce connector and select **Only people with access to this data source** and identity type **AAD** on the search permissions screen, refer to the Map your Azure AD Identities article for steps on how to map Azure AD identities.

Steps for mapping your non-Azure AD properties

1. Select an Azure AD user property

You can select the Azure AD user property you are creating the mapping for. This is the target property you are aiming to map your non-Azure AD identities to.

You can select one of the following Azure AD properties:

AZURE AD PROPERTY	DEFINITION	EXAMPLE
User Principal Name (UPN)	A UPN consists of a UPN prefix (the user account name) and a UPN suffix (a DNS domain name). The prefix is joined with the suffix using the "@" symbol.	us1@contoso.onmicrosoft.com
Azure AD ID	An Azure AD ID for a given user is the unique GUID of the user.	58006c96-9e6e-45ea-8c88-4a56851eefad
Active Directory Security ID (SID)	SID (Security Identifier) is a unique identifier that Active Directory uses to identify objects as security principal.	S-1-5-21-453406510-812318184-4183662089

2. Select non-Azure AD user properties to map

You can select non-Azure AD properties pulled from your data source to apply regular expressions on. To learn more about where to find these properties in your data source, see the ServiceNow and Salesforce pages.

You can select a non-Azure AD user property from the dropdown and provide a regular expression to be applied on those user property values. To learn more about regular expressions, see regular expression reference.

Below are some examples of regular expressions and their outputs applied to a sample string:

SAMPLE STRING	REGULAR EXPRESSION	OUTPUT OF REGULAR EXPRESSION ON SAMPLE STRING
Alexis Vasquez	.*	Alexis Vasquez
Alexis Vasquez	..$	ez
Alexis Vasquez	(\w+)$	Vasquez

You can add as many non-Azure AD user properties as you would like expressions for. You can apply different regular expressions to the same user property if your final formula warrants that.

3. Create formula to complete mapping

You can combine the outputs of the regular expressions applied to each of your non-Azure AD user properties to form the Azure AD property selected in step 1.

In the formula box, "{0}" corresponds to the output of the regular expression applied to the *first* non-Azure AD property you selected. "{1}" corresponds to the output of the regular expression applied to the *second* non-Azure AD property you selected. "{2}" corresponds to the output of the regular expression applied to the *third* non-Azure AD property, and so on.

Below are some examples of formulas with sample regular expression outputs and formula outputs:

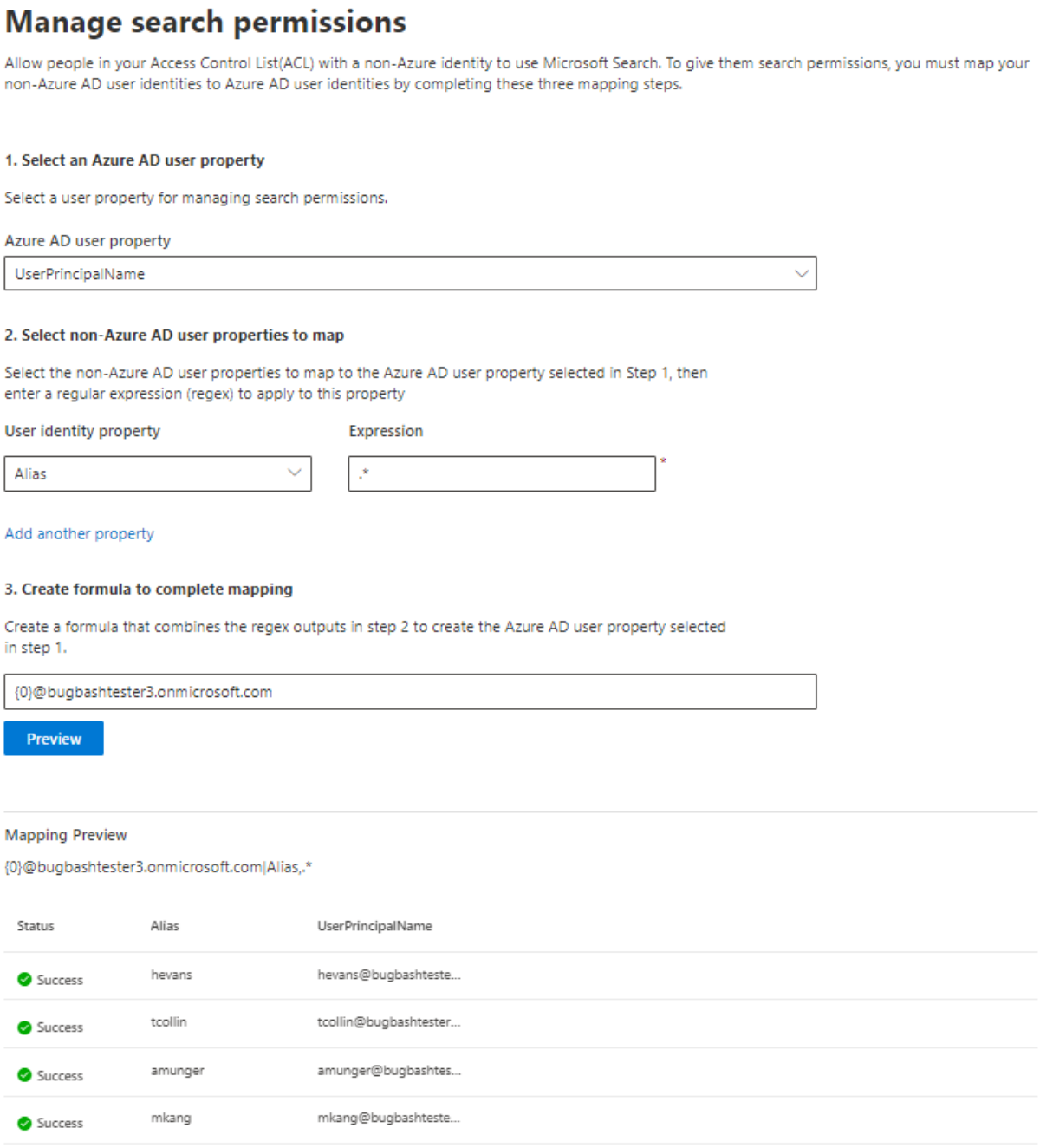
SAMPLE FORMULA	VALUE OF {0} ON SAMPLE USER	VALUE OF {1} ON SAMPLE USER	OUTPUT OF FORMULA
{0}.{1}@contoso.com	firstname	lastname	firstname.lastname@contoso.com
{0}@domain.com	userid		userid@domain.com

After you provide your formula, you can optionally click **Preview** to see a preview of 5 random users from your data source with their respective user mappings applied. The output of the preview includes the value of the non-Azure AD user properties selected in step 2 for those users and the output of the final formula provided in step 3 for that user. It also indicates whether the output of the formula could be resolved to an Azure AD user in your tenant via a "Success" or "Failed" icon.

> **NOTE**
> You can still proceed with creating your connection if one or more user mappings have a "Failed" status after you click **Preview**. The preview shows 5 random users and their mappings from your data source. If the mapping you provide does not map all users, you may experience this case.

Sample non-Azure AD mapping

See the snapshot below for a sample non-Azure AD mapping.



Limitations

- Only one mapping is supported for all users. Conditional mappings are not supported.
- You cannot change your mapping once the connection is published.
- Only regex-based expressions against the non-AAD user properties are currently supported for the transformation.
- There are only 3 Azure AD identities you can choose to map to (UPN, Azure AD ID, and AD SID).

Map your Azure AD Identities

11/30/2020 • 2 minutes to read • Edit Online

This article walks you through the steps of mapping your Azure AD identities to a unique identifier for your data source (non-Azure AD identity) so that people in your Access Control List (ACL) with non-Azure AD identities can see connector search results scoped to them.

These steps are only relevant to search administrators who are setting up a Salesforce connector by Microsoft with search permissions for "Only people with access to this data source" and identity type "AAD." The following steps walk you through how to map your Azure AD user properties to your users' **Federation IDs**.

> **NOTE**
>
> If you are setting up a Salesforce connector and select **Only people with access to this data source** and identity type **non-AAD** on the search permissions screen, refer to the Map your non-Azure AD Identities article for steps on how to map non-Azure AD identities.

Steps for mapping your Azure AD properties

1. Select Azure AD user properties to map

You can select the Azure AD properties you need to map to the Federation ID.

You can select an Azure AD user property from the dropdown. You can also add as many Azure AD user properties as you would like if these properties are necessary to create the Federation ID mapping for your organization.

2. Create formula to complete mapping

You can combine the values of the Azure AD user properties to form the unique Federation ID.

In the formula box, "{0}" corresponds to the *first* Azure AD property you selected. "{1}" corresponds to the *second* Azure AD property you selected. "{2}" corresponds to the *third* Azure AD property, and so on.

Below are some examples of formulas with sample regular expression outputs and formula outputs:

SAMPLE FORMULA	VALUE OF PROPERTY {0} FOR A SAMPLE USER	VALUE OF PROPERTY {1} FOR A SAMPLE USER	OUTPUT OF FORMULA
{0}.{1}@contoso.com	firstname	lastname	firstname.lastname@contoso.com
{0}@domain.com	userid		userid@domain.com

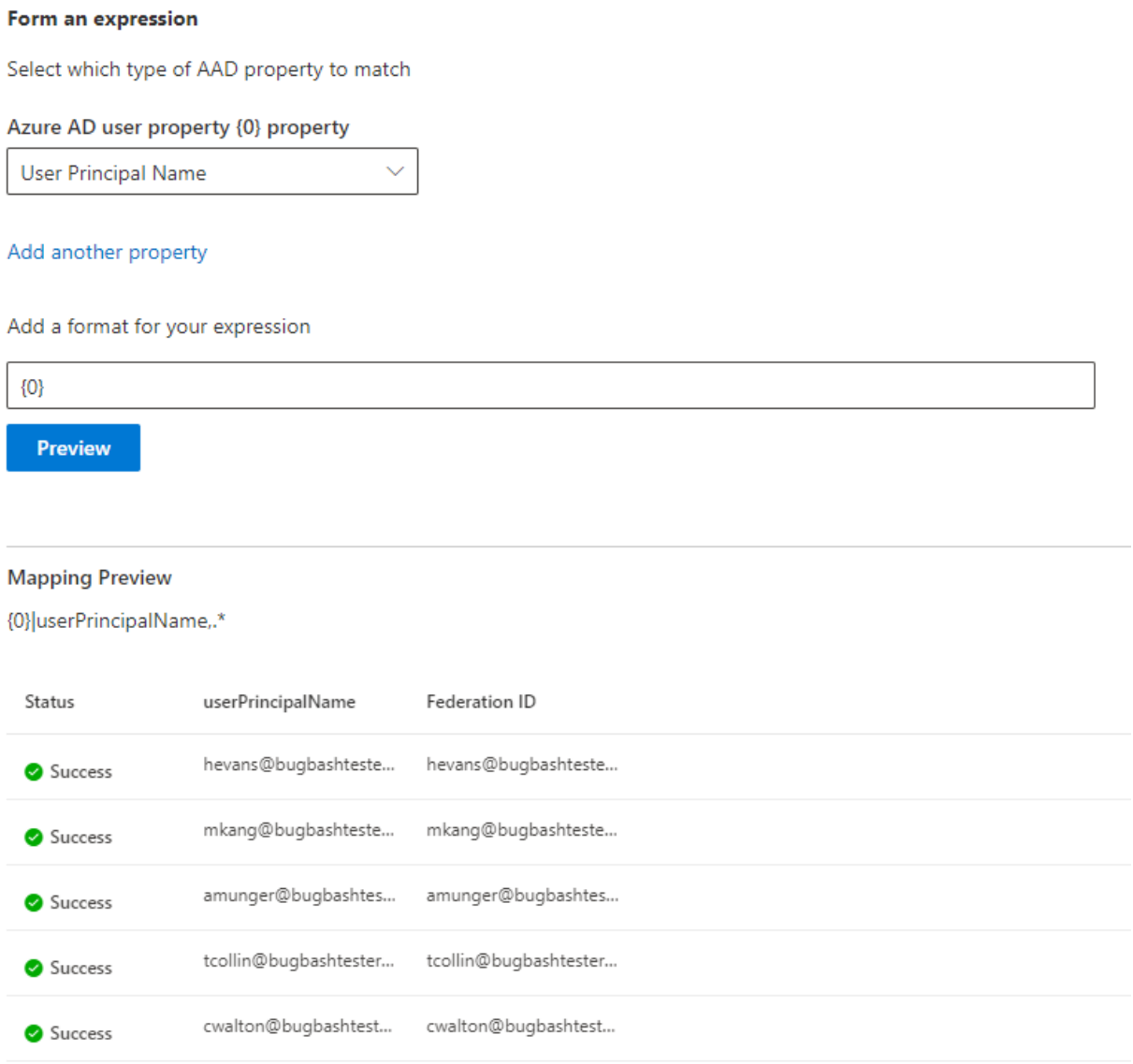
After you provide your formula, you can optionally click **Preview** to see a preview of 5 random users from your data source with their respective user mappings applied. The output of the preview includes the value of the Azure AD user properties selected in step 1 for those users and the output of the final formula provided in step 2 for that user. It also indicates whether the output of the formula could be resolved to an Azure AD user in your tenant via a "Success" or "Failed" icon.

NOTE

You can still proceed with creating your connection if one or more user mappings have a "Failed" status after you click **Preview**. The preview shows 5 random users and their mappings from your data source. If the mapping you provide does not map all users, you may experience this case.

Sample Azure AD mapping

See the snapshot below for a sample Azure AD mapping.



Limitations

- Only one mapping is supported for all users. Conditional mappings are not supported.
- You cannot change your mapping once the connection is published.
- Regex-based expressions against the Azure AD user properties are not supported for the Azure AD to Federation ID transformation.

Azure Data Lake Storage Gen2 connector

11/30/2020 • 3 minutes to read • Edit Online

With the Azure Data Lake Storage Gen2 connector, users in your organization can search for files stored in Azure Blob Storage and Azure Data Lake Gen 2 Storage accounts.

This article is for Microsoft 365 administrators or anyone who configures, runs, and monitors an Azure Data Lake Storage Gen2 connector. It gives an overview of the connector configuration, capabilities, limitations, and troubleshooting techniques. In the article, we use *Azure Storage* as a generic term for Azure Blob Storage and Azure Data Lake Gen 2 Storage.

Connect to a data source

Primary storage connection string

On the **Authentication and config** screen, provide the Primary Storage Connection String. That string is required to allow access to your storage account. To find your connection string, go to the Azure portal and navigate to the **Keys** section of your relevant Azure Storage account. Copy and paste the connection string in the appropriate field on the screen.

If you do not prefer to provide the **AccountKey** (a parameter in the primary storage connection string), you will need to grant access to our Graph Connectors Service for the following roles.

- Storage Blob Data Reader
- Storage Queue Data Contributor
- Storage Blob Delegator (only for hierarchical storage)

Navigate to the **Access Control** tab of your Azure Storage account, and follow the instructions there to grant access to the following app:

- **First Party App ID:** 56c1da01-2129-48f7-9355-af6d59d42766
- **First Party App Name:** Graph Connector Service

Storage account and queue notifications (Optional)

Support to process changes in real time in the Graph Connectors Service might be added in the future. In that case, we'll monitor Azure Storage change notifications stored in a queue. You'll need to create a queue in the same account as your Azure Storage account.

After you create a queue, go to the **Events** tab on the queue page to configure **Event Subscription**. Choose all the Blob events that the queue will receive, and connect the queue to the Azure Storage account.

Manage search permissions

Azure Data Lake Gen 2

On the **Manage search permissions** screen, you can choose to ingest the Access Control Lists (ACLs) from your Azure Data Lake Gen 2 Storage account. When these search permissions are set, search content is trimmed based on the permissions assigned to the signed-in Azure Active Directory user searching the content. Alternatively, you can choose to make all the content indexed from your storage account visible to everyone in your organization. In this case, everyone in your organization will have access to all the data in your storage account.

Azure Blob Storage

For a connection to Azure Blob Storage, all the content indexed from the configured source is visible to everyone

in your organization. Access control lists are not supported at Blob level in Azure Blob Storage.

Manage search permissions

The Azure Data Lake Storage Gen2 connector supports search permissions visible to **Everyone** or **Only people with access to this data source**. Indexed data that appears in the search results could be visible to all users in the organization or only to users who have access to each item.

Assign property labels

You can assign a source property to each label by choosing from a menu of options. While this step is not mandatory, having some property labels will improve the search relevance and ensure more accurate search results for end users.

Manage schema

On the **Manage Schema** screen, you have the option to change the schema attributes (**queryable**, **searchable**, **retrievable**, and **refinable**) associated with the properties, add optional aliases, and choose the **Content** property.

Set the refresh schedule

On the **Refresh Settings** screen, you can set the incremental crawl interval and the full crawl interval. The default intervals for the Azure Data Lake Storage Gen2 connector are 15 minutes for an incremental crawl and one week for a full crawl.

Limitations

A published connection for Azure Blob Storage cannot be reconfigured for Azure Data Lake Storage Gen2 source and vice-versa. In such scenarios, it is recommended to configure a new connection.

Azure DevOps connector (preview)

11/30/2020 • 3 minutes to read • Edit Online

With the Azure DevOps connector, your organization can index work items in its instance of the Azure DevOps service. After you configure the connector and index content from Azure DevOps, end users can search for those items in Microsoft Search.

This article is for Microsoft 365 administrators or anyone who configures, runs, and monitors an Azure DevOps connector. It explains how to configure your connector and connector capabilities, limitations, and troubleshooting techniques.

> **IMPORTANT**
> The Azure DevOps connector supports only the Azure DevOps cloud service. Azure DevOps Server 2019, TFS 2018, TFS 2017, TFS 2015, and TFS 2013 are not supported by this connector.

Connect to a data source

To connect to your Azure DevOps instance, you need your Azure DevOps organization name, its App ID, and client secret for OAuth authentication.

Register an app

You must register an app in Azure DevOps so that the Microsoft Search app can access the instance. To learn more, see Azure DevOps documentation on how to register an app.

The following table provides guidance on how to fill out the app registration form:

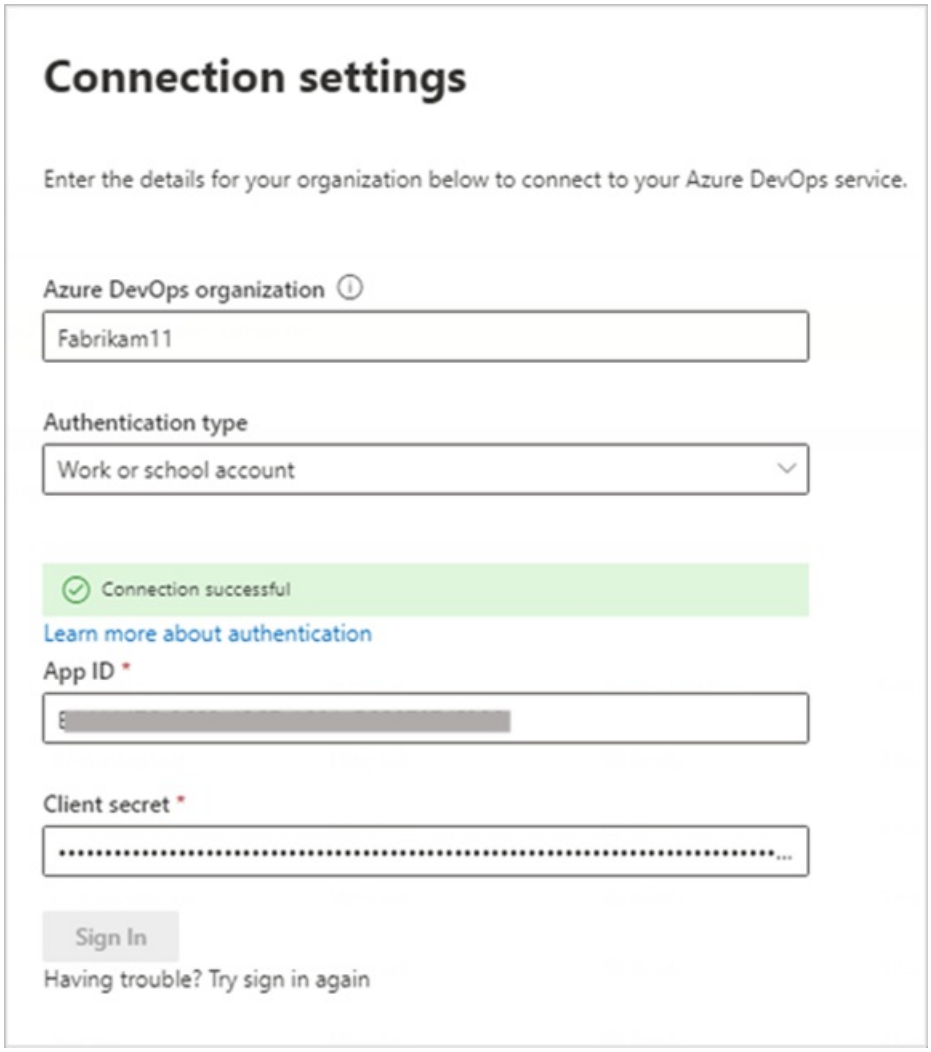
MANDATORY FIELDS	DESCRIPTION	RECOMMENDED VALUE
Company Name	This is the name of your company.	Use an appropriate value
Application name	This unique value identifies the application that you're authorizing.	Microsoft Search
Application website	This required field is the URL of the application that will request access to your Azure DevOps instance during connector setup.	https://gcs.office.com/
Authorization callback URL	A required callback URL that the authorization server redirects to.	https://gcs.office.com/v1.0/admin/oauth/callback
Authorized scopes	This is the scope of access for the application	Select the following scopes: Identity (read), Work Items (read), Variable Groups (read), Project and team (read), Graph (read)

On registering the app with the details above, you will get the **App ID** and **Client Secret** that will be used to configure the connector.

> **NOTE**
>
> To revoke access to any app registered in Azure DevOps, go to User settings at the right top of your Azure DevOps instance. Click on Profile and then click on Authorizations in the Security section of the side pane. Hover over an authorized OAuth app to see the Revoke button at the corner of the app details.

Connection settings

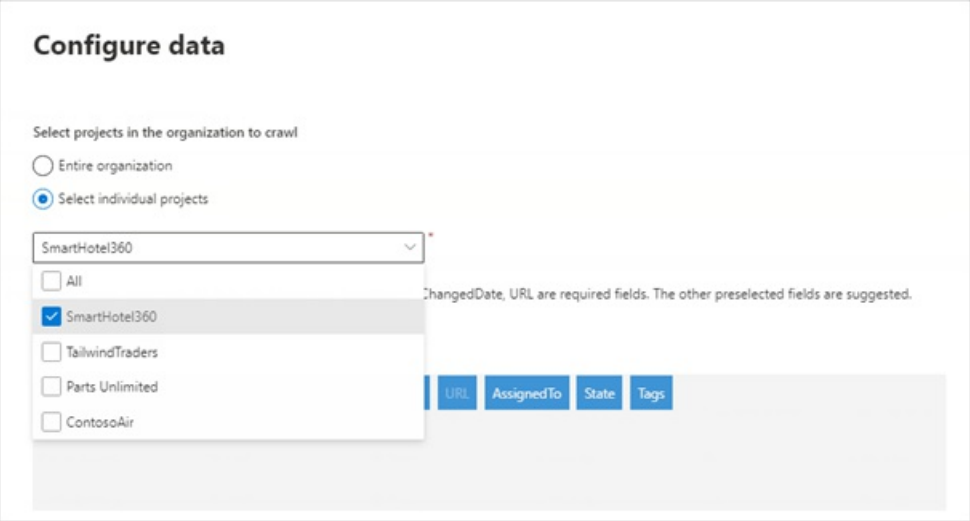
After registering the Microsoft Search app with Azure DevOps, you can complete the connection settings step. Enter your organization name, App ID, and Client secret.



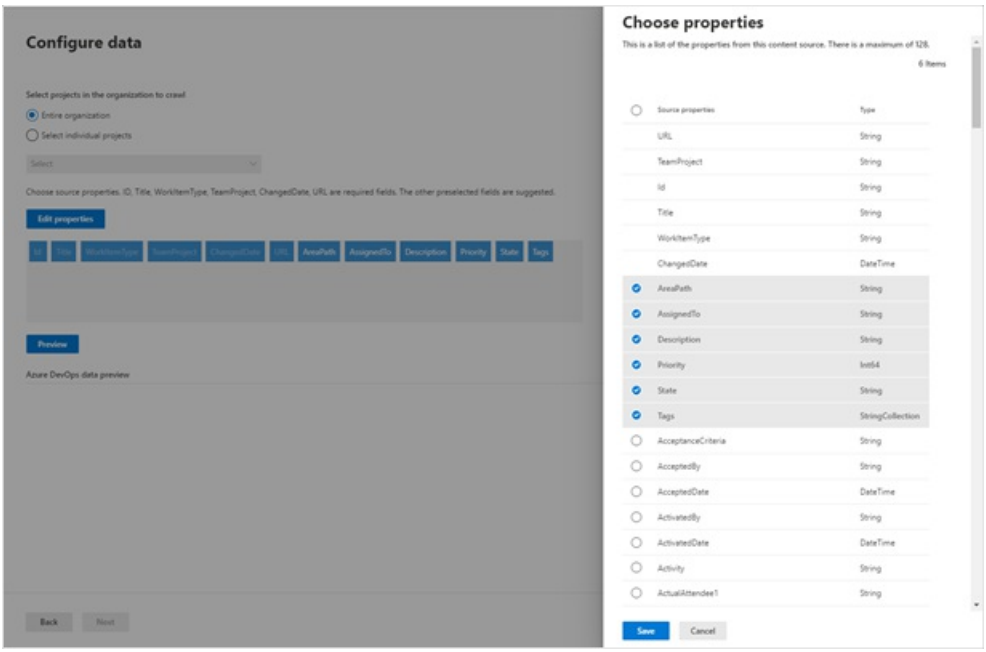
Select projects and fields

You can choose for the connection to index either the entire organization or specific projects.

If you choose to index the entire organization, items in all projects in the organization will get indexed. New projects and items will be indexed during the next crawl after they are created. If you choose individual projects, only work items in those projects will be indexed.



Next, select which fields you want the connection to index and preview data in these fields before proceeding.



Manage search permissions

The Azure DevOps connector supports search permissions visible to**Only people with access to this data source** or **Everyone**. If you choose **Only people with access to this data source**,indexed data will appear in the search results for users who have access to them based on permissions to users or groups at the Organization, Project or Area path level in Azure DevOps. If you choose **Everyone**, indexed data will appear in the search results for all users.

Assign property labels

You can assign a source property to each label by choosing from a menu of options. While this step is not mandatory, having some property labels will improve the search relevance and ensure more accurate search results for end users.

Manage schema

On the **Manage Schema** screen, you have the option to change the schema attributes (**queryable**, **searchable**, **retrievable**, and **refinable**) associated with the properties, add optional aliases, and choose the **Content** property.

Set the refresh schedule

The Azure DevOps connector supports refresh schedules for both full and incremental crawls. A full crawl finds deleted work items that were previously synced to the Microsoft Search index. A full crawl runs to sync all the work items. To sync new work items and updates to existing work items, you need to schedule incremental crawls.

The recommended schedule is one hour for an incremental crawl and one day for a full crawl.

Azure SQL and Microsoft SQL server connectors

11/30/2020 • 8 minutes to read • Edit Online

With a Microsoft SQL server or Azure SQL connector, your organization can discover and index data from an on-premises SQL Server database or a database hosted in your Azure SQL instance in the cloud. The connector indexes specified content into Microsoft Search. To keep the index up to date with source data, it supports periodic full and incremental crawls. With these SQL connectors, you can also restrict access to search results for certain users.

This article is for Microsoft 365 administrators or anyone who configures, runs, and monitors a Microsoft SQL server or Azure SQL connector. It explains how to configure your connector and connector capabilities, limitations, and troubleshooting techniques.

Install the Graph connector agent (required for on-premises Microsoft SQL server connector only)

In order to access your on-premises third-party data, you must install and configure the Graph connector agent. See Install the Graph connector agent to learn more.

Register an app (for Azure SQL connector only)

For Azure SQL connector, you must register an app in Azure Active Directory to allow Microsoft Search app to access data for indexing. To learn more about registering an app, refer Microsoft Graph documentation on how to register an app.

After completing the app registration and taking note of the app name, application (client) ID and tenant ID, you need to generate a new client secret. The client secret will only be displayed once. Remember to note & store the client secret securely. Use the client ID and client secret while configuring a new connection in Microsoft Search.

To add the registered app to your Azure SQL Database, you need to:

- Log in to your Azure SQL DB
- Open a new query window
- Create a new user by running the command 'CREATE USER [app name] FROM EXTERNAL PROVIDER'
- Add user to role by running command 'exec sp_addrolemember 'db_datareader', [app name]' Or 'ALTER ROLE db_datareader ADD MEMBER [app name]'

> **NOTE**
>
> To revoke access to any app registered in Azure Active Directory, refer the Azure documentation on removing a registered app.

Connect to a data source

To connect your Microsoft SQL server connector to a data source, you must configure the database server you want crawled and the on-prem agent. You can then connect to the database with the required authentication method.

> **NOTE**
> Your database must run SQL server version 2008 or later for the Microsoft SQL server connector to be able to connect.

For the Azure SQL connector, you only need to specify the server name or IP address you want to connect to. Azure SQL connector only supports Azure Active Directory Open ID connect (OIDC) authentication to connect to the database.

For added security, you may configure IP firewall rules for your Azure SQL server or database. To learn more about setting up IP firewall rules, refer documentation on IP firewall rules. Add the following client IP ranges in the firewall settings.

REGION	IP RANGE
NAM	52.250.92.252/30, 52.224.250.216/30
EUR	20.54.41.208/30, 51.105.159.88/30
APC	52.139.188.212/30, 20.43.146.44/30

To search your database content, you must specify SQL queries when you configure the connector. These SQL queries need to name all the database columns that you want to index (i.e. source properties), including any SQL joins that need to be performed to get all the columns. To restrict access to search results, you must specify Access Control Lists (ACLs) within SQL queries when you configure the connector.

Full crawl (Required)

In this step, you configure the SQL query that runs a full crawl of the database. The full crawl selects all the columns or properties you want to be made **queryable**, **searchable**, or **retrievable**. You can also specify ACL columns to restrict access of search results to specific users or groups.

> **TIP**
> To get all the columns that you need, you can join multiple tables.

Example: SELECT OrderId, OrderTitle, OrderDesc, AllowedUsers, AllowedGroups, DeniedUsers, DeniedGroups, CreatedDateTime, IsDeleted

FROM OrderTable, AclTable
WHERE (CreatedDateTime > @watermark) && (OrderTable.OrderId = AclTable.OrderId) && (IsDeleted <> 0)
ORDER BY CreatedDateTime ASC

Select data columns (Required) and ACL columns (Optional)

The example demonstrates selection of five data columns that hold the data for the search: OrderId, OrderTitle, OrderDesc, CreatedDateTime, and IsDeleted. To set view permissions for each row of data, you can optionally select these ACL columns: AllowedUsers, AllowedGroups, DeniedUsers, and DeniedGroups. All these data columns can be made **queryable**, **searchable**, or **retrievable**.

Select data columns as shown in this example query:

```
SELECT OrderId, OrderTitle, OrderDesc, AllowedUsers, AllowedGroups, DeniedUsers, DeniedGroups, CreatedDateTime, IsDeleted
```

To manage access to the search results, you can specify one or more ACL columns in the query. The SQL connector allows you to control access at per record level. You can choose to have the same access control for all records in a table. If the ACL information is stored in a separate table, you might have to do a join with those tables in your

query.

The use of each of the ACL columns in the above query is described below. The following list explains the 4 **access control mechanisms**.

- **AllowedUsers**: This specifies the list of user IDs who will be able to access the search results. In the following example, list of users: john@contoso.com, keith@contoso.com, and lisa@contoso.com would only have access to a record with OrderId = 12.
- **AllowedGroups**: This specifies the group of users who will be able to access the search results. In the following example, group sales-team@contoso.com would only have access to record with OrderId = 12.
- **DeniedUsers**: This specifies the list of users who do **not** have access to the search results. In the following example, users john@contoso.com and keith@contoso.com do not have access to record with OrderId = 13, whereas everyone else has access to this record.
- **DeniedGroups**: This specifies the group of users who do **not** have access to the search results. In the following example, groups engg-team@contoso.com and pm-team@contoso.com do not have access to record with OrderId = 15, whereas everyone else has access to this record.

OrderId	OrderTitle	OrderDesc	AllowedUsers	AllowedGroups	DeniedUsers	DeniedGroups	CreatedDateTime
12	Order for windows	Windows 10 for corp...	john@contoso.com; keith@contoso.com	sales-team@contoso.com	null	null	06/11/2016 01:00
13	Contoso lathe order	Lathe for the inventory...	null	null	john@contoso.com; keith@contoso.com	null	07/12/2016 13:00
15	Fabrikam order for mcb	MCBs for the store room...	null	null	null	engg-team@contoso.com; pm-team@contoso.com	07/01/2017 15:00

Supported data types

The below table summarizes the SQL data types that are supported in the MS SQL and Azure SQL connectors. The table also summarizes the indexing data type for the supported SQL data type. To learn more about Microsoft Graph connectors supported data types for indexing, refer documentation on property resource types.

CATEGORY	SOURCE DATA TYPE	INDEXING DATA TYPE
Date and time	date datetime datetime2 smalldatetime	datetime
Exact numeric	bigint int smallint tinyint	int64
Exact numeric	bit	boolean
Approximate numeric	float real	double
Character string	char varchar text	string
Unicode character strings	nchar nvarchar ntext	string
Other data types	uniqueidentifier	string

For any other data type currently not directly supported, the column needs to be explicitly cast to a supported data

type.

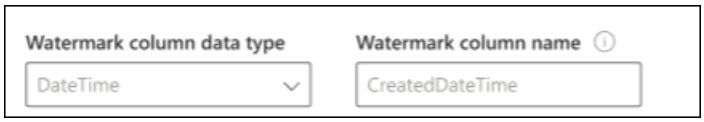
Watermark (Required)

To prevent overloading the database, the connector batches and resumes full-crawl queries with a full-crawl watermark column. By using the value of the watermark column, each subsequent batch is fetched, and querying is resumed from the last checkpoint. Essentially this is a mechanism to control data refresh for full crawls.

Create query snippets for watermarks as shown in these examples:

- `WHERE (CreatedDateTime > @watermark)`. Cite the watermark column name with the reserved keyword `@watermark`. If the sort order of the watermark column is ascending, use `>`; otherwise, use `<`.
- `ORDER BY CreatedDateTime ASC`. Sort on the watermark column in ascending or descending order.

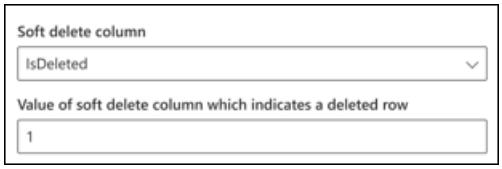
In the configuration shown in the following image, `CreatedDateTime` is the selected watermark column. To fetch the first batch of rows, specify the data type of the watermark column. In this case, the data type is `DateTime`.



The first query fetches the first **N** number of rows by using: "CreatedDateTime > January 1, 1753 00:00:00" (min value of DateTime data type). After the first batch is fetched, the highest value of `CreatedDateTime` returned in the batch is saved as the checkpoint if the rows are sorted in ascending order. An example is March 1, 2019 03:00:00. Then the next batch of **N** rows is fetched by using "CreatedDateTime > March 1, 2019 03:00:00" in the query.

Skipping soft-deleted rows (Optional)

To exclude soft-deleted rows in your database from being indexed, specify the soft-delete column name and value that indicates the row is deleted.



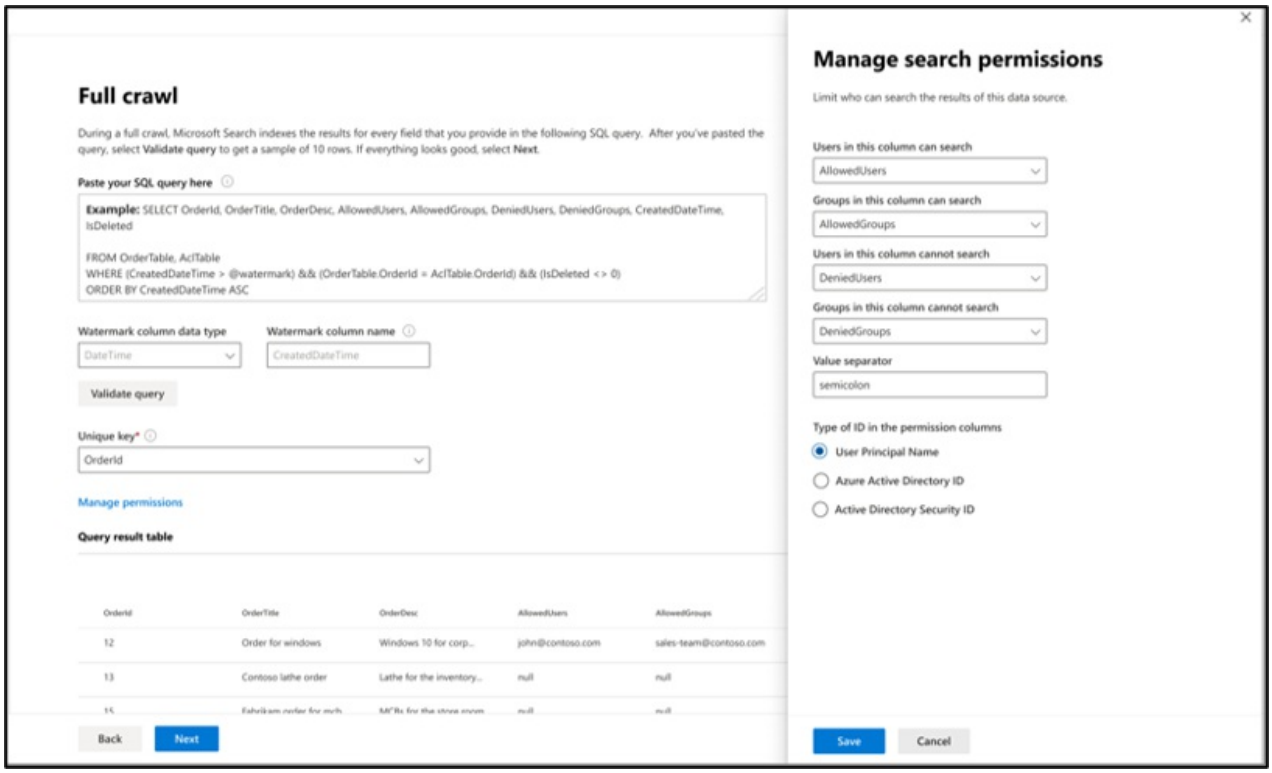
Full crawl: Manage search permissions

Click **Manage permissions** to select the various access control (ACL) columns which specify the access control mechanism. Select the column name you specified in the full crawl SQL query.

Each of the ACL columns is expected to be a multi-valued column. These multiple ID values can be separated by separators such as semicolon (;), comma (,), and so on. You need to specify this separator in the **value separator** field.

The following ID types are supported for using as ACLs:

- **User Principal Name (UPN)**: AUser Principal Name (UPN)is the name of a system user in an email address format. A UPN (for example:john.doe@domain.com) consists of theusername(logon name),separator(the @ symbol), anddomain name(UPN suffix).
- **Azure Active Directory (AAD) ID**: In Azure AD, every user or group has an object ID which looks something like 'e0d3ad3d-0000-1111-2222-3c5f5c52ab9b'
- **Active Directory (AD) Security ID**: In an on-premises AD setup, every user and group have an immutable, unique security identifier which looks something like 'S-1-5-21-3878594291-2115959936-132693609-65242.'



Incremental crawl (Optional)

In this optional step, provide a SQL query to run an incremental crawl of the database. With this query, the SQL connector determines any changes to the data since the last incremental crawl. As in the full crawl, select all columns that you want to be made **queryable**, **searchable**, or **retrievable**. Specify the same set of ACL columns that you specified in the full crawl query.

The components in the following image resemble the full crawl components with one exception. In this case, "ModifiedDateTime" is the selected watermark column. Review the full crawl steps to learn how to write your incremental crawl query and see the following image as an example.

Manage search permissions

You can choose to use the ACLs specified in the full crawl screen or you can override them to make your content visible to everyone.

Next steps: Customize the search results page

Create your own verticals and result types, so end users can view search results from new connections. Without this step, data from your connection won't show up on the search results page.

To learn more about how to create your verticals and MRTs, see Search results page customization.

Limitations

The SQL connectors have these limitations in the preview release:

- Microsoft SQL server connector: The on-premises database must run SQL server version 2008 or later.
- ACLs are only supported by using a User Principal Name (UPN), Azure Active Directory (Azure AD), or Active

Directory Security.

- Indexing rich content inside database columns is not supported. Examples of such content are HTML, JSON, XML, blobs, and document parsings that exist as links inside the database columns.

Enterprise websites connector

11/30/2020 • 3 minutes to read • Edit Online

With the Enterprise websites connector, your organization can index articles and **content from its internal-facing websites**. After you configure the connector and sync content from the website, end users can search for that content from any Microsoft Search client.

This article is for Microsoft 365 administrators or anyone who configures, runs, and monitors an Enterprise websites connector. It explains how to configure your connector and connector capabilities, limitations, and troubleshooting techniques.

Connect to a data source

To connect to your data source, you need to fill in the root URL of the website and the type of authentication you'd like to use: None, Basic Authentication, or OAuth 2.0 with Azure Active Directory (Azure AD).

URL

Use the URL field to specify the root of the website that you'd like to crawl. The enterprise websites connector will use this URL as the starting point and follow all the links from this URL for its crawl.

Authentication

Basic Authentication requires a username and password. Create this bot account by using the Microsoft 365 admin center.

OAuth 2.0 with Azure AD requires a resource ID, Client ID, and Client Secret.

For more information, see Authorize access to Azure Active Directory web applications using OAuth 2.0 code grant flow. Register with the following values:

Name: Microsoft Search
Redirect_URI: `https://gcs.office.com/v1.0/admin/oauth/callback`

To get the values for the resource, client_id, and client_secret, go to **Use the authorization code to request an access token** on the redirect URL webpage.

For even more information, see Quickstart: Register an application with the Microsoft identity platform.

Add URLs to exclude

You can optionally create an **Exclusion list** to exclude some URLs from getting crawled if that content is sensitive or not worth crawling. To create an exclusion list, browse through the root URL. You have the option to add the excluded URLs to the list during the configuration process.

Manage search permissions

The Enterprise websites connector only supports search permissions visible to **Everyone**. Indexed data appears in the search results and is visible to all users in the organization.

Assign property labels

You can assign a source property to each label by choosing from a menu of options. While this step is not mandatory, having some property labels will improve the search relevance and ensure more accurate search

results for end users.

Manage schema

On the **Manage Schema** screen, you have the option to change the schema attributes (**queryable**, **searchable**, **retrievable**, and **refinable**) associated with the properties, add optional aliases, and choose the **Content** property.

Set the refresh schedule

The Enterprise websites connector only supports a full refresh. This means that the connector will recrawl all the website's content during every refresh. To make sure the connector gets enough time to crawl the content, we recommend that you set a large refresh schedule interval. We recommend a scheduled refresh between one and two weeks.

Troubleshooting

When reading the website's content, the crawl may encounter some source errors which are represented by the detailed error codes below. To get more information on the types of errors, go to the **error details** page after selecting the connection. Click on the **error code** to see more detailed errors. Also refer to Manage your connector to learn more.

DETAILED ERROR CODE	ERROR MESSAGE
6001	The site that is being tried to index is not reachable
6005	The source page that is being tried to index has been blocked by as per robots.txt configuration.
6008	Unable to resolve the DNS
6009	For all client side errors (Except HTTP 404, 408), please refer to HTTP 4xx error codes for details.
6013	The source page that is being tried to index could not be found. (HTTP 404 error)
6018	The source page is not responding, and the request has timed out. (HTTP 408 error)
6021	The source page that is being tried to index has no textual content on the page.
6023	The source page that is being tried to index is unsupported (not a HTML page)
6024	The source page that is being tried to index has unsupported content.

- Errors 6001-6013 occur when the data source is not reachable due to a network issue or when the data source itself is deleted, moved, or renamed. Check if the data source details provided are still valid.
- Errors 6021-6024 error occur when the data source contains non-textual content on the page or when the page is not an HTML. Please check the data source and add this page in exclusion list or ignore the error.

Limitations

The Enterprise websites connector doesn't support searching data on **dynamic webpages**. Examples of those webpages live in content management systems like Confluence and Unily or databases that store website content.

MediaWiki connector

11/30/2020 • 2 minutes to read • Edit Online

With the MediaWiki connector, your organization can discover and index data from a wiki created by using MediaWiki software. This connector indexes specified content into Microsoft Search and supports periodic crawls to keep the index up to date.

This article is for Microsoft 365 administrators or anyone who configures, runs, and monitors a MediaWiki connector. It explains how to configure your connector and connector capabilities, limitations, and troubleshooting techniques.

Connect to a data source

Enter your MediaWiki URL and credentials for authenticating the connection. You'll need the following information: **Tenant ID**, **Resource ID**, **Client ID**, and the **Client Secret**.

Manage search permissions

The MediaWiki connector only supports search permissions visible to **Everyone**. Indexed data appears in the search results and is visible to all users in the organization.

Assign property labels

You can assign a source property to each label by choosing from a menu of options. While this step is not mandatory, having some property labels will improve the search relevance and ensure more accurate search results for end users.

Manage schema

On the **Manage Schema** screen, you have the option to change the schema attributes (**queryable**, **searchable**, **retrievable**, and **refinable**) associated with the properties, add optional aliases, and choose the **Content** property.

Set the refresh schedule

This schedule refreshes indexed data, so changes to the wiki are reflected in Microsoft Search. All new pages, deleted pages, page content, or metadata changes appear in search results after the specified refresh interval. The crawl time is dependent on the size of the wiki. Currently the connector crawls at around 50 pages per minute.

Limitations

The MediaWiki connector has these limitations in the preview release:

- Supports only cloud-based wikis.
- Supports only Basic or OAuth 2.0 with Azure Active Directory or Azure authentication.
- Doesn't support namespace selection for indexing. Indexes only **Main**, **Category**, and **File** namespaces.
- Doesn't support Access Control Lists (ACLs). Thus, indexed pages are visible to all users in the organization.

Salesforce connector (preview)

11/30/2020 • 5 minutes to read • Edit Online

With the Salesforce Graph connector, your organization can index Contacts, Opportunities, Leads and Accounts objects in your Salesforce instance. After you configure the connector and index content from Salesforce, end users can search for those items from any Microsoft Search client.

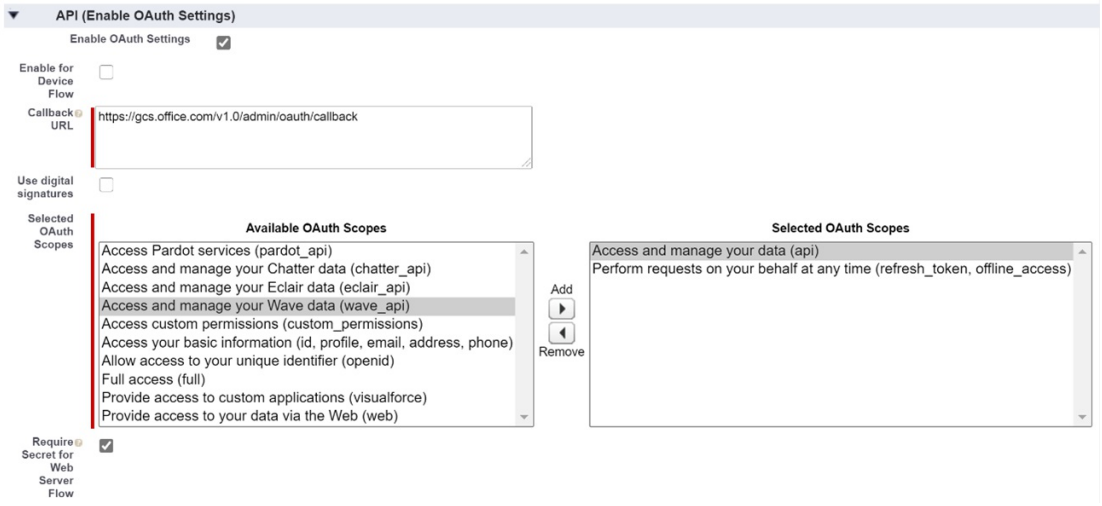
This article is for Microsoft 365 administrators or anyone who configures, runs, and monitors a Salesforce connector. It explains how to configure your connector and connector capabilities, limitations, and troubleshooting techniques.

> **IMPORTANT**
> The Salesforce Graph connector currently supports Summer '19 or later.

Connection settings

To connect to your Salesforce instance, you need your Salesforce instance URL, the Client ID, and Client Secret for OAuth authentication. The following steps explain how you or your Salesforce administrator can get this information from your Salesforce account:

- Log in to your Salesforce instance and go to Setup
- Navigate to Apps -> App Manager.
- Select **New connected app**.
- Complete the API section as follows:
  - Select the checkbox for **Enable Oauth Settings**.
  - Specify the Callback URL as: https://gcs.office.com/v1.0/admin/oauth/callback
  - Select these required OAuth scopes.
    - Access and manage your data (api)
    - Perform requests on your behalf at any time (refresh_token, offline_access)
  - Select the checkbox for **Require secret for web server flow**.
  - Save the app.



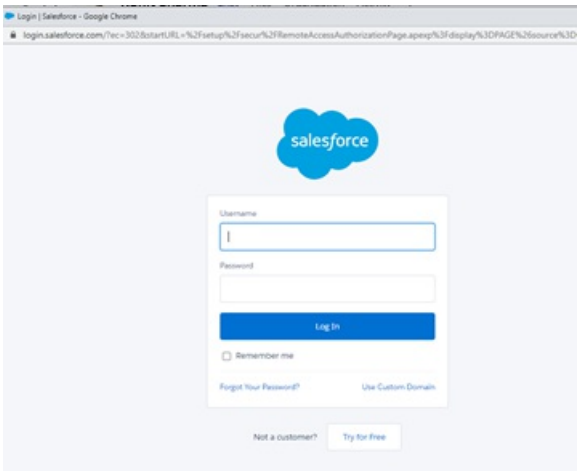
- Copy the consumer key and the consumer secret. These will be used as the Client ID and the Client Secret when you configure the Connection Settings for your Graph Connector in the Microsoft 365 admin portal.

- Before closing your Salesforce instance, perform the following steps to ensure that refresh tokens do not expire:
  - Go to Apps -> App Manager
  - Find the app you just created and select the drop down on the right. Select **Manage**
  - Select **edit policies**
  - For refresh token policy, select **Refresh token is valid until revoked**

You can now use the M365 Admin Center to complete the rest of the setup process for your Graph connector.

Configure the Connection settings for your Graph connector as follows:

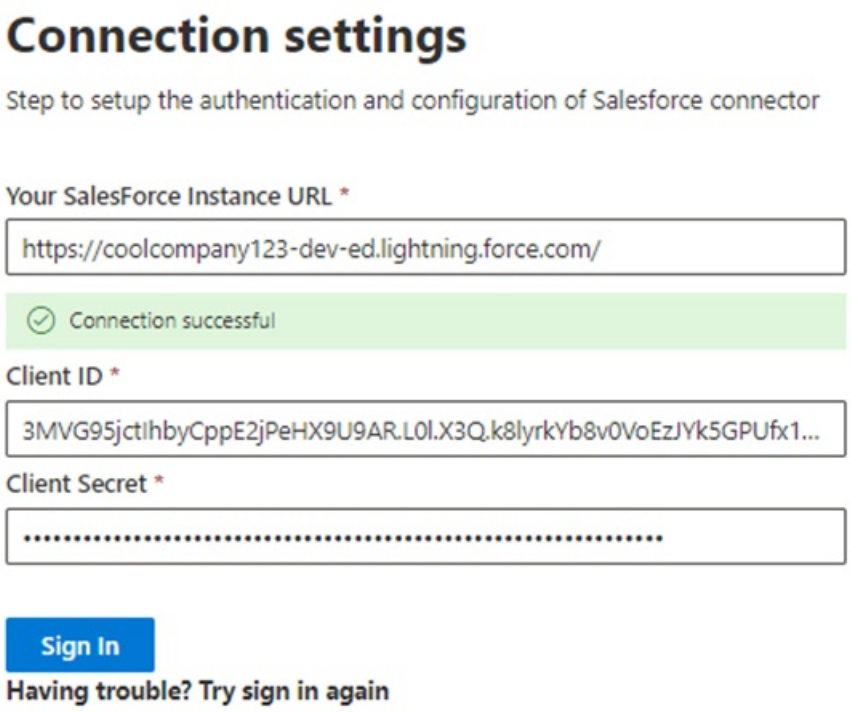
- For the Instance URL, use https://[domain].my.salesforce.com where domain would be the Salesforce domain for your organization.
- Enter the Client ID and Client Secret you obtained from your Salesforce instance and select Sign in.
- If this is the first time you have attempted to Sign in with these settings, you will get a pop up asking you to login to Salesforce with your admin username and password. The screenshot below shows the popup. Enter your credentials and select Log in.



> **NOTE**
>
> If the pop up does not appear, it might be getting blocked in your browser, so you must allow pop-ups and redirects.

> **NOTE**
>
> If your organization uses single sign-on (SSO), you can select **Use Custom Domain** in the bottom, right-hand corner of the login interface. Enter the domain and then select **Continue**. It will go to your organization specific login page where you will have an option to login with SSO.

- Check that the connection was successful by searching for a green banner that says "Connection successful" as show in the screenshot below.

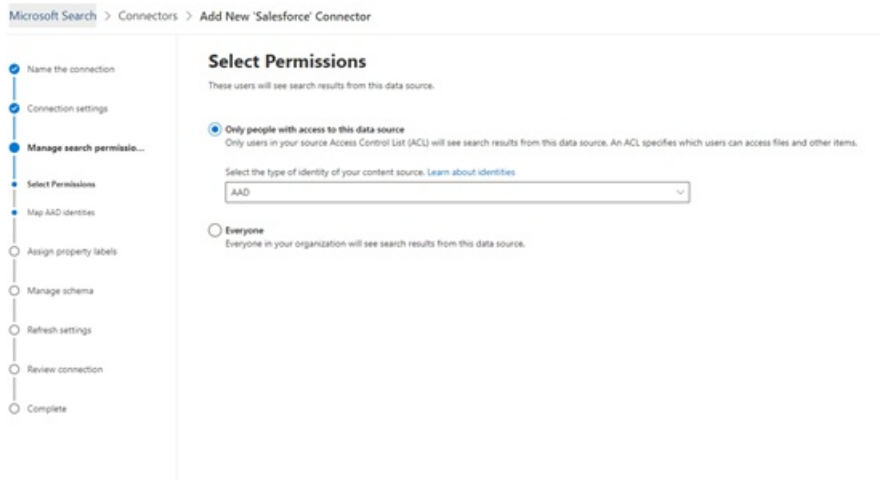


Manage search permissions

You will need to choose which users will see search results from this data source. If you allow only certain Azure Active Directory (Azure AD) or Non-Azure AD users to see the search results, you will then need to map the identities.

Select Permissions

You can choose to ingest Access Control Lists (ACLs) from your Salesforce instance, or you can allow everyone in your organization to see search results from this data source. ACLs can include Azure Active Directory (AAD) identities (users who are federated from Azure AD to Salesforce), non-Azure AD identities (native Salesforce users who have corresponding identities in Azure AD), or both.



Map non-AAD identities

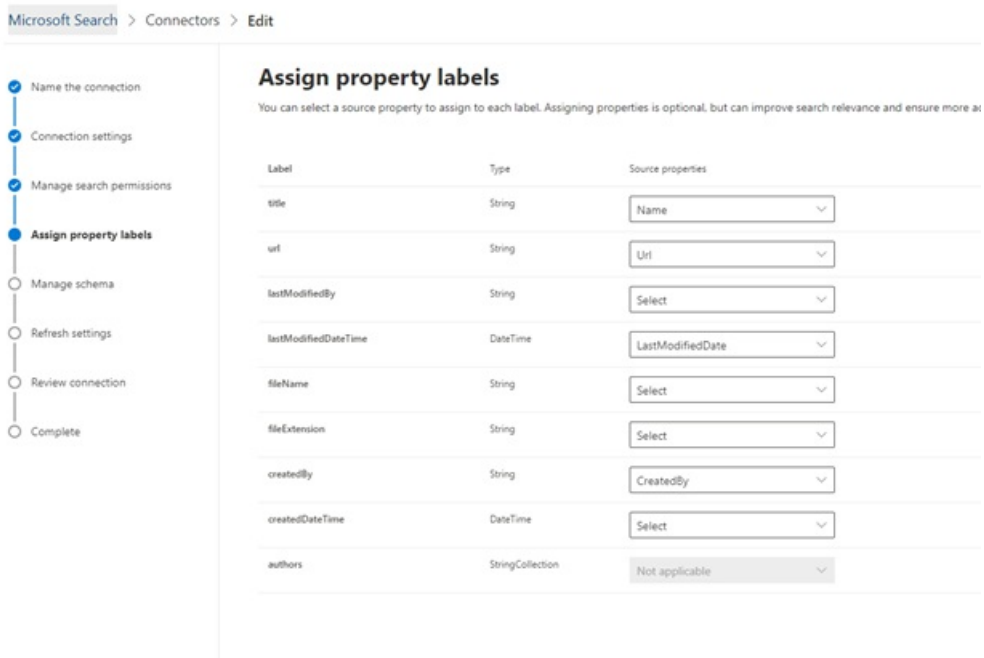
If you chose to ingest an ACL from your Salesforce instance and selected "non-AAD" for the identity type see Map your non-Azure AD Identities for instructions on mapping the identities.

Map AAD identities

If you chose to ingest an ACL from your Salesforce instance and selected "AAD" for the identity type see Map your Azure AD Identities for instructions on mapping the identities. To learn how to set up Azure AD SSO for Salesforce, see this tutorial.

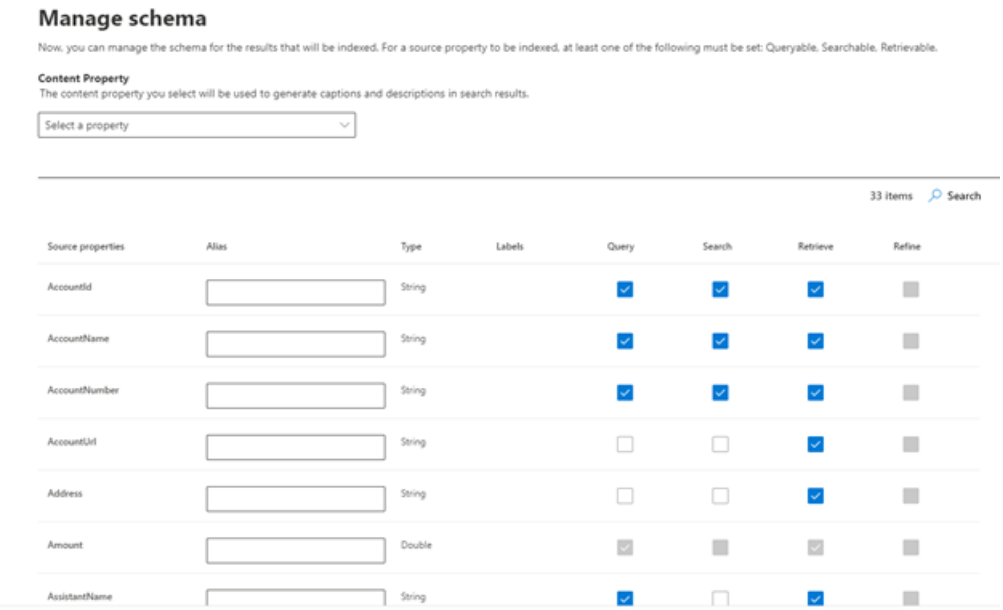
Assign property labels

You can assign a source property to each label by choosing from a menu of options. While this step is not mandatory, having some property labels will improve the search relevance and ensure more accurate search results for end users. By default, some of the Labels like "Title," "URL," "CreatedBy," and "LastModifiedBy" have already been assigned source properties.



Manage Schema

You can select what source properties should be indexed so that they can show up in search results. The connection wizard by default selects a search schema based on a set of source properties. You can modify it by selecting the check boxes for each property and attribute in the search schema page. Search schema attributes include Search, Query, Retrieve and Refine. Refine allows you to define the properties which can be later used as custom refiners or filters in the search experience.



Set the refresh schedule

The Salesforce connector only supports refresh schedules for full crawls currently.

> **IMPORTANT**
>
> A full crawl finds deleted objects and users that were previously synced to the Microsoft Search index.

The recommended schedule is one week for a full crawl.

Limitations

- The Graph connector does not currently support Apex based , territory-based sharing and sharing using personal groups from Salesforce.
- There is a known bug in the Salesforce API that the Graph connector uses where the private org wide defaults for leads is not honored currently.
- If a field has field level security (FLS) set for a profile, the Graph connector will not ingest that field for any profiles in that Salesforce org. Users will thus not be able to search on values for those fields, nor will it show up in the results.
- In the Manage Schema screen these common standard property names are listed once and the selection done to make them queryable, searchable and retrievable apply to all or none.
  - Name
  - Url
  - Description
  - Fax
  - Phone
  - MobilePhone

- Email
- Type
- Title
- AccountId
- AccountName
- AccountUrl
- AccountOwner
- AccountOwnerUrl
- Owner
- OwnerUrl
- CreatedBy
- CreatedByUrl
- LastModifiedBy
- LastModifiedByUrl
- LastModifiedDate
- ObjectName

ServiceNow connector

11/30/2020 • 8 minutes to read • Edit Online

With the ServiceNow connector, your organization can index knowledge-base articles that are visible to all users or restricted with user criteria permissions within your organization. After you configure the connector and index content from ServiceNow, end users can search for those articles from any Microsoft Search client.

This article is for Microsoft 365 administrators or anyone who configures, runs, and monitors a ServiceNow connector. It explains how to configure your connector and connector capabilities, limitations, and troubleshooting techniques.

Learn how to access Microsoft built connectors from Set up your Microsoft-built connector for Microsoft Search. ServiceNow connector specific configuration is explained in the article below.

Connection Settings

To connect to your ServiceNow data, you need your organization's **ServiceNow instance URL**, credentials for this account, and the Client ID and Client Secret for OAuth authentication.

Your organization's **ServiceNow instance URL** typically looks like **https://<your-organization-domain>.service-now.com**. Along with this URL, you will need an account for setting up the connection to ServiceNow as well as for allowing Microsoft Search to periodically update the articles from ServiceNow based on the refresh schedule. The account should at least have *knowledge* role. Learn how to assign role for ServiceNow accounts.

> **NOTE**
>
> If you want to crawl user and group identities to honor access permissions of knowledge articles in Microsoft Search results, the account should have access to read the following table records in ServiceNow:
>
> - kb_uc_can_contribute_mtom
> - kb_uc_can_read_mtom
> - kb_uc_cannot_read_mtom
> - kb_uc_cannot_contribute_mtom
> - sys_user
> - sys_user_has_role
> - sys_user_grmember
> - user_criteria
> - kb_knowledge_base
>
> You can create and assign a role for the account you use to connect with Microsoft Search. Read access to the tables can be assigned on that role. To learn about setting read access to table records, see Securing Table Records.

To authenticate and sync content from ServiceNow, choose **one of three** supported methods:

1. Basic authentication
2. ServiceNow OAuth (recommended)
3. Azure AD OpenID Connect

Basic authentication

Enter the username and password of ServiceNow account with **knowledge** role to authenticate to your instance.

ServiceNow OAuth

To use ServiceNow OAuth for authentication, a ServiceNow admin needs to provision an endpoint in your ServiceNow instance, so that the Microsoft Search app can access the instance. To learn more, see Create an endpoint for clients to access the instance in the ServiceNow documentation.

The following table provides guidance on how to fill out the endpoint creation form:

FIELD	DESCRIPTION	RECOMMENDED VALUE
Name	This unique value identifies the application that you require OAuth access for.	Microsoft Search
Client ID	A read-only, auto-generated unique ID for the application. The instance uses the client ID when it requests an access token.	NA
Client secret	With this shared secret string, the ServiceNow instance and Microsoft Search authorize communications with each other.	Follow security best-practices by treating this as a password.
Redirect URL	A required callback URL that the authorization server redirects to.	https://gcs.office.com/v1.0/admin/oauth/callback
Logo URL	A URL that contains the image for the application logo.	NA
Active	Select the check box to make the application registry active.	Set to active
Refresh token lifespan	The number of seconds that a refresh token is valid. By default, refresh tokens expire in 100 days (8640000 seconds).	31,536,000 (1 year)
Access token lifespan	The number of seconds that an access token is valid.	43,200 (12 hours)

Enter the client id and client secret to connect to your instance. After connecting, use a ServiceNow account credential to authenticate permission to crawl. The account should at least have **knowledge** role.

Azure AD OpenID Connect

To use Azure AD OpenID Connect for authentication, follow the steps below.

Step 1: Register a new application in Azure Active Directory

To learn about registering a new application in Azure Active Directory, see Register an application. Select single tenant organizational directory. Redirect URI is not needed. After registration, note down the Application (client) ID and Directory (tenant) ID.

Step 2: Create a client secret

To learn about creating a client secret, see Creating a client secret. Take a note of client secret.

Step 3: Retrieve Service Principal Object Identifier

Follow the steps to retrieve Service Principal Object Identifier

1. Run PowerShell
2. Install Azure PowerShell using the following command

```
Install-Module -Name Az -AllowClobber -Scope CurrentUser
```

3. Connect to Azure

```
Connect-AzAccount
```

4. Get Service Principal Object Identifier

```
Get-AzADServicePrincipal -ApplicationId "Application-ID"
```

Replace "Application-ID" with Application (client) ID (without quotes) of the application you registered in step 1. Note the value of ID object from PowerShell output. It is the Service Principal ID.

Now you have all the information required from Azure portal. A quick summary of the information is given in the table below.

PROPERTY	DESCRIPTION
Directory ID (Tenant ID)	This is a unique ID referring the Azure Active Directory tenant (from step 1).
Application ID (Client ID)	This is a unique ID referring the application registered in step 1.
Client Secret	This is the secret key of the application (from step 2). Treat it like a password.
Service Principal ID	An identity for the application running as a service. (from step 3)

Step 4: Register ServiceNow Application

The following configuration need to be done in the ServiceNow instance.

1. Register a new OAuth OIDC entity. To learn, see Create an OAuth OIDC provider.
2. The following table provides guidance on how to fill out OIDC provider registration form

FIELD	DESCRIPTION	RECOMMENDED VALUE
Name	A unique name that identifies the OAuth OIDC entity.	Azure AD
Client ID	The client ID of the application registered in the third-party OAuth OIDC server. The instance uses the client ID when requesting an access token.	Application (Client) ID from step 1
Client Secret	The client secret of the application registered in the third-party OAuth OIDC server.	Client Secret from step 2

All other values can be default.

3. In the OIDC provider registration form, you need to add a new OIDC provider configuration. Click the search icon against *OAuth OIDC Provider Configuration* field to open the records of OIDC configurations. Click New.

4. The following table provides guidance on how to fill out OIDC provider configuration form

FIELD	RECOMMENDED VALUE
OIDC Provider	Azure AD
OIDC Metadata URL	This must be in the form https://login.microsoftonline.com/"tenandId"/.well-known/openid-configuration Replace "tenantID" with Directory (tenant) ID from step 1 (without quotes).
OIDC Configuration Cache Life Span	120
Application	Global
User Claim	sub
User Field	User ID
Enable JTI claim verification	Disabled

5. Click Submit and Update the OAuth OIDC Entity form.

Step 5: Create a ServiceNow account

Refer the instructions to create a ServiceNow account, create a user in ServiceNow.

The following table provides guidance on how to fill out the ServiceNow user account registration

FIELD	RECOMMENDED VALUE
User ID	Service Principal ID from step 3
Web service access only	Checked

All other values can be left to default.

Step 6: Enable Knowledge role for the ServiceNow account

Access the ServiceNow account you created with ServiceNow Principal ID as User ID and assign the knowledge role. Instructions to assigning a role to a ServiceNow account can be found here, assign a role to a user.

Use Application ID as Client ID (from step 1), and Client secret (from step 2) in admin center configuration wizard to authenticate to your ServiceNow instance using Azure AD OpenID Connect.

Filter data

With a ServiceNow query string, you can specify conditions for syncing articles. It's like a **Where** clause in a **SQL Select** statement. For example, you can choose to index only articles that are published and active. To learn about creating your own query string, see Generate an encoded query string using a filter.

Manage search permissions

The ServiceNow connector supports search permissions visible to **Everyone** or **Only people with access to this data source**. Indexed data appears in the search results and is visible to all users in the organization or users who have access to them respectively. ServiceNow Connector supports default user criteria permissions without advanced scripts. When the connector encounters a user criteria with advanced script, all data using that user criteria will not be showed in search results.

If you choose **Only people with access to this data source**, you need to further choose whether your ServiceNow instance has Azure Active Directory (AAD) provisioned users or Non-AAD users.

> **NOTE**
> The ServiceNow connector is in **preview** if you choose **Only people with access to this data source**.

> **NOTE**
> If you choose AAD as the type of identity source, make sure you are assigning UPN source property to email targeted property in ServiceNow. To verify or change your mappings, see Customizing user provisioning attribute-mappings for SaaS applications in Azure Active Directory.

If you chose to ingest an ACL from your ServiceNow instance and selected "non-AAD" for the identity type see Map your non-Azure AD Identities for instructions on mapping the identities.

Assign property labels

You can assign a source property to each label by choosing from a menu of options. While this step is not mandatory, having some property labels will improve the search relevance and ensure more accurate search results for end users.

Manage schema

On the **Manage Schema** screen, you have the option to change the schema attributes (**queryable**, **searchable**, **retrievable**, and **refinable**) associated with the properties, add optional aliases, and choose the **Content** property.

Set the refresh schedule

The ServiceNow connector supports refresh schedules for both full and incremental crawls. We recommend that you set both.

A full crawl schedule finds deleted articles that were previously synced to the Microsoft Search index and any articles that moved out of the sync filter. When you first connect to ServiceNow, a full crawl runs to sync all the knowledge-base articles. To sync new items and make updates, you need to schedule incremental crawls.

The recommended default is one day for a full crawl and four hours for an incremental crawl.

> **NOTE**
> For identities, only full crawl scheduled will be applied.

Review and publish

After you configure your connector, you can review and publish the connection.

Next steps

After publishing the connection, you need to customize the search results page. To learn about customizing search results, see Customize the search results page.

Manage your connections for Microsoft Search

11/30/2020 • 7 minutes to read • Edit Online

To access and manage your connectors, you must be designated as a search administrator for your tenant. Contact your tenant administrator to provision you for the search administrator role.

Get started

Navigate to the Connectors tab in the Microsoft 365 admin center.

For each connector type, the Microsoft 365 admin center supports the operations shown in the following table:

OPERATION	MICROSOFT-BUILT CONNECTOR	PARTNER OR CUSTOM-BUILT CONNECTOR
Add a connection	✔ (See Configure your Microsoft-built connector)	✘ (Refer to your partner or custom-built connector admin UX)
Delete a connection	✔	✔
Edit a published connection	✔ Name ✔ Description ✔ Authentication credentials for your external data source ✔ Gateway credentials for your on-premises data source ✔ Refresh schedule	✔ Name ✔ Description
Edit a draft connection	✔	✘

Monitor your connection status

After you create a connection, the number of processed items shows on the **Connectors** tab on the **Microsoft Search** page. After the initial full crawl completes successfully, the progress for periodic incremental crawls displays. This page provides information about the connector's day-to-day operations and an overview of the logs and error history.

Four states show up in the **Status** column against each connection:

- **Syncing**. The connector is crawling the data from the source to index the existing items and make any updates.
- **Enabled**: The connection is enabled, and there's no active crawl running against it. **Last sync time** indicates when the last successful crawl happened. The connection is as fresh as the last sync time.
- **Paused**. The crawls are paused by the admins through the pause option. The next crawl runs only when it's manually resumed. However, the data from this connection continues to be searchable.
- **Failed**. The connection had a critical failure. This error requires manual intervention. The admin needs to take appropriate action based on the error message shown. Data that was indexed until the error occurred is searchable.

View your last crawl info

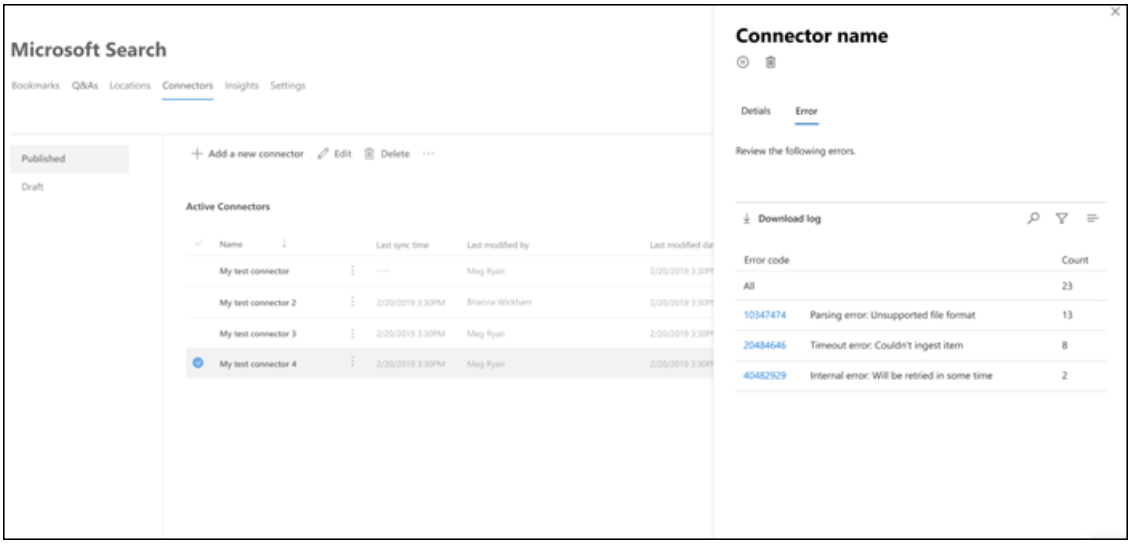
After the first initial incremental or full crawl completes successfully, the last crawl data values are displayed under the last crawl header in the detail pane. If there was no last crawl that ran, you will not see any information under the last crawl header. This information about last crawl will help you gain insights into how the crawl performed and take necessary steps wherever required.

The following last crawl values will be available for each connection:

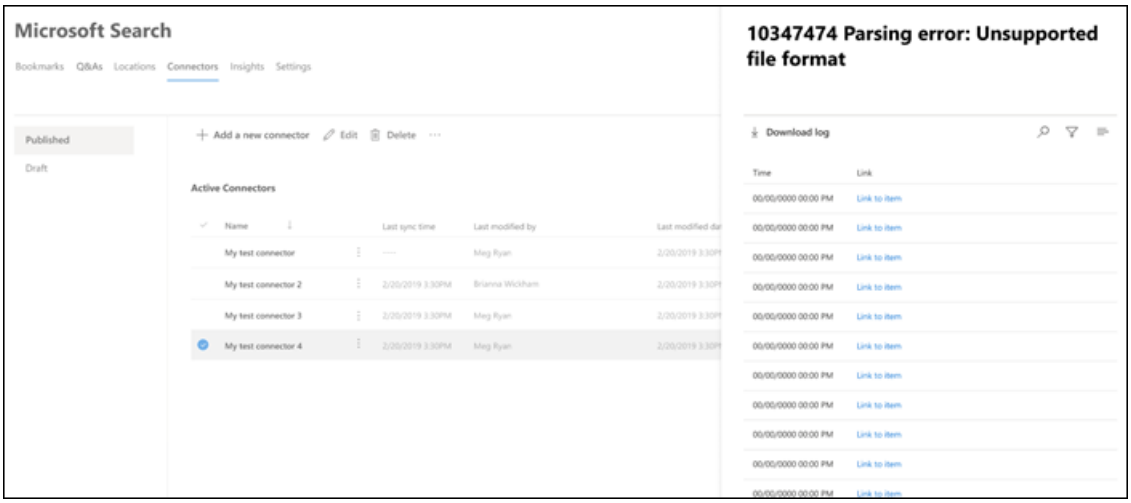
VALUE	DESCRIPTION
Completed at	Date and time the last crawl got completed
Type	Incremental or full crawl
Duration	how much time did the last crawl take to complete
Successes	Number of items that have been successfully ingested in the last crawl
Errors	Number of items that errored in the last crawl

Monitor errors

For each **Active Connector** on the **Connectors** tab, any existing crawl errors show under the **Error** tab. The tab lists error codes, the count of each, and error log download options. See the example in the following image. Select an **error code** to view the error's details.



To view an error's specific details, select its error code. A screen appears with error details and a link. The most recent errors appear at the top. See the example in the following table.



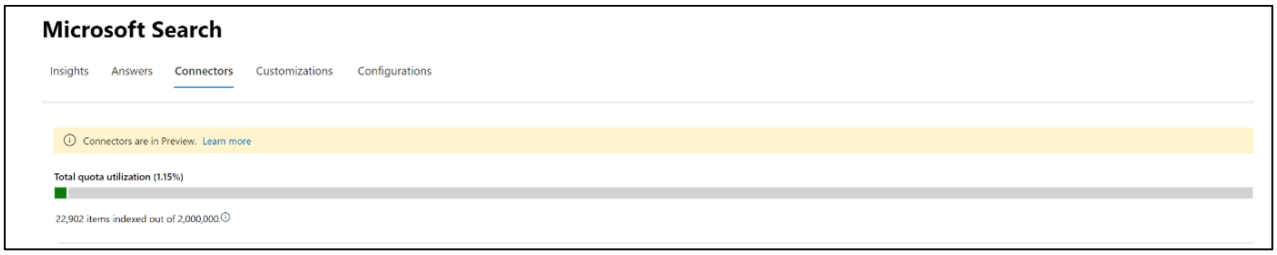
Below is the list of different errors that can appear against any connection. If these solutions don't work, contact support or send us feedback.

ERROR CODE	ERROR MESSAGE	SOLUTION
1000	The data source isn't available. Check your internet connection or make sure the data source is still accessible by the connector.	This error occurs when the data source is not reachable due to a network issue or when the data source itself is deleted, moved, or renamed. Check if the data source details provided are still valid.
1001	Can't update the data, because the data source is throttling the connector.	To unthrottle the data source, check if its scale limits can be increased or wait until a less traffic-heavy time of the day.
1002	Can't authenticate with the data source. Verify that the credentials associated with this data source are correct.	Click **Edit** to update the authentication credentials.
1003	The account associated with the connector doesn't have permission to access the item.	Ensure the proper account has access to the item you want indexed.
1004	Unable to reach the on-premises data gateway. Make sure the gateway service is running and the gateway details are updated in the connection configuration.	Check the computer with the gateway, open the Power BI Gateway application and make sure the gateway is running. Verify that the gateway is using the same admin account as Microsoft Search, then make sure all the gateway details are all updated in the connection configuration.
1005	Credentials associated with this data source have expired. Renew the credentials and update the connection.	Click **Edit** to update the authentication credentials.
1006	Your gateway version is out of date and doesn't support this connector anymore. You will need to update the gateway.	Please visit Install an on-premises data gateway to download and install the latest version of the Power BI gateway on the machine containing the gateway.

ERROR CODE	ERROR MESSAGE	SOLUTION
1007	No valid Power BI license detected. You need a valid Power BI license to perform this crawl.	You need a valid Power BI license to perform this crawl. Check that your organization has a valid license. If it does, try again. If it doesn't, obtain a license and then try again.
1008	The total quota utilization of your tenant has reached its limit. Try deleting a connection to free up some of your quota or adjusting your ingestion filters to bring in less data.	Try deleting a connection to free up some of your quota or adjusting your ingestion filters to bring in less data. If these don't solve the issue, contact Microsoft support.
2001	Indexing is throttled because of alarge number of updates in the queue. Depending on the queue, it can take some time for the updates to complete.	Please wait until the queue gets cleared.
2002	Indexing failed due to unsupported item formatting.	See connector-specific documentation for more information.
2003	Indexing failed due to unsupported item content.	See connector-specific documentation for more information.
2010	This connection is no longer valid because of an update made by Microsoft. Please delete the connection and create a new one.	Please delete the connection and create a new one.
5000	Something went wrong. If this continues, contact support.	

Monitor your index quota utilization

The available index quota and consumption is displayed on the connectors landing page.



NOTE

During the preview period, every organization trying out Graph connectors was provided a free fixed quota of up to 2 million items across all connections. With Graph connectors being generally available, the free quota will expire on Feb 1st, 2021 for those organizations who have been using Graph connectors in preview. Microsoft-built Graph connectors labeled as "Preview" will not be included in the total charged index quota for your organization. However, it will count towards the max number of 10 connections you can configure for your organization and the max number of 7 million items your organization can index across connections.

The quota utilization bar will indicate various states based on consumption of quota by your organization:

STATE	QUOTA CONSUMPTION
Normal	1-69%
High	70-89%
Critical	90%-99%
Full	100%

The number of items indexed will also be displayed with each connection. The number of items indexed by each connection contributes to the total quota available for your organization.

When index quota is exceeded for your organization, all active connections will be impacted, and those connections will operate in **limit exceeded** state. In this state, your active connections

- Will not be able to add new items.
- Will be able to update or delete existing items.

To fix this, you can do any of the following:

- Learn how to purchase index quota for your organization at Licensing requirements and pricing.
- Identify connections which have too much content being ingested and update them to index fewer items to make room for quota. To update the connection, you must delete and create a new connection with a new ingestion filter which brings in fewer items.
- Permanently delete one or more connections

Limitations

- When you **publish** a Microsoft-built connector, it might take a few minutes for the connection to be created. During that time, the connection will show its status as pending.
- The Microsoft 365 admin center doesn't support editing the **search schema** after a connection is published. To edit the search schema, delete your connection and then create a new one.
- Ingestion throughput is throttled at about four items per second.
- There is no support for schema updates. After you create a connection setup, there's no way to update the schema. You can only delete and re-create the connection.
- There is a connections limit. Each tenant can create up to 10 connections.
- Edit support for connection is not available. Once the connection has been created, you cannot edit or change it. If you need to change any details, you must delete and recreate the connection.

License requirements and pricing

11/30/2020 • 2 minutes to read • Edit Online

This article is intended for Global or Billing Admins who want to learn about how to purchase additional Graph connectors quota for their organization.

You need a valid Microsoft 365 or Office 365 license and sufficient Graph connectors quota for your organization to view data from connectors in your search results. All of the Graph connectors by Microsoft are free. However, you need to have sufficient index quota to ingest content from those connectors.

Each Microsoft 365 or Office 365 E5 license includes 500 items of index quota, which counts towards your organization's quota for ingesting content from Graph connectors. For example, if your organization has 100 Microsoft 365 E5 licenses, then your organization has 100 x 500 = 50,000 items worth of Graph connectors index quota.

To purchase additional Graph connectors quota, get in touch with your Microsoft Account Manager or complete the following steps:

1. In the Microsoft 365 admin center navigation menu, go to **Billing > Purchase services**.
2. At the bottom of thePurchase servicespage, select **Add-ons**.
3. Select **Extra Graph Connector Capacity**.
4. Select **Buy** then complete your order preferences.
5. Select **Check out now**.

> **NOTE**
> Currently Graph connectors only support up to 7 million items of total index quota, which includes any built-in quota bundled into Microsoft 365 or Office 365 E5 licenses. The platform will support higher limits in the future. Please contact Microsoft support or your Microsoft account manager if you have any questions.

Provide feedback for Microsoft Graph connectors

11/30/2020 • 2 minutes to read • Edit Online

The Microsoft Graph connectors team responds to the search admin community across several channels:

- **Documentation feedback:** If you have questions about the Microsoft Graph connectors documentation or want to tell us what you like or don't like, you can provide feedback at the bottom of any article.
- **Feature requests:** If our platform doesn't empower you to do what you need, make your feature suggestions under the category **Connectors** on Microsoft User Voice.

Microsoft Graph connectors: Terms of Use

11/30/2020 • 2 minutes to read • Edit Online

Your use of Microsoft Graph Connectors may be subject to third party terms and conditions. Microsoft is not a party to your agreement(s) with third parties and any concerns or questions regarding third party terms or services should be directed to the third party. You, as the data controller for your data, are responsible for the indexing of data into your Microsoft 365 tenant.

Microsoft makes no representation, warranty, or guarantee in relation to the third party data prior to indexing into your Microsoft 365 tenant. Microsoft assumes no liability for errors that may occur during the indexing of third party data. You agree that any data sourced from a third party provider is provided "as is," and with respect to the index, is provided subject to your configuration. Indexed data in your Microsoft 365 tenant will be considered "Customer Data" for purposes of the Online Services Terms, Privacy Statement, and Microsoft's other data obligations.

For further information on how we use Customer Data in M365, please consult the Online Services Terms and Privacy Statement. You can also find out more about Microsoft's commitments to data protection and privacy by visiting our Trust Center.

Customize the search results page

11/30/2020 • 6 minutes to read • Edit Online

You can create search verticals and result types to customize the search results that users see when they search in Microsoft SharePoint, Microsoft Office, and Microsoft Search in Bing. Verticals make it easier for users to find the information that they have permission to see. For example, you could create a search vertical for marketing analysis data from third-party software for your users in the marketing department. You can also define result types and customize the layout for this data.

You can create verticals and result types at these levels:

- **Organization level** – When you add a vertical at the organization level, it appears on the search results page when users search from their SharePoint start page, on Office, or on Bing.
- **Site level** – For example, you might want to enable your customer service employees to search for *Severity 1* incidents directly from their department's SharePoint site.

Search verticals explained

At the top of the Microsoft Search results page, there's a row of tabs. These are the search verticals. A search vertical only shows results of a certain type or from certain content. Examples are **Files** or **News**. By default, Microsoft Search shows the verticals **All**, **People**, **Files**, **Sites**, and **News**.

You can add search verticals that are relevant to your organization. These will appear on the Microsoft Search results page in SharePoint, Office, and Bing. For example, you could create a vertical for marketing-related content and another for sales, based on the type of information that each group needs. You can add verticals to show results only from content indexed via connectors.

Multiple connections in a vertical

A search vertical can now surface results from multiple connector sources. This provides greater flexibility in designing your search result page. The existing administrative experience of vertical setup allows you to select multiple connections in the "Content Source" step. If you accurately appoint as many semantic labels as possible, this experience will be enhanced. You can add semantic labels upon schema definition and ingestion.

Here is additional information on how to create and manage semantic labels.

Things you should know

1. A connection can be added as a content source only under one vertical. Reusing connections under multiple verticals is not allowed.
2. If you need to setup a query for a search vertical where multiple connection sources have been added, common source properties should be used to create a such a query.

Things to consider

Before you start, make sure that the connector has been indexed. This can take up to 48 hours, depending on the file size.

You can't create a vertical for content that resides in SharePoint.

There are three basic steps to add a vertical:

1. Create the vertical. In this step, you define the vertical's name, content source, and scope of the content to search.

2. Define what the results for this vertical will look like.
3. Enable the vertical (to be displayed) from the vertical list page.

STEP 1: Create the search vertical

After you start the wizard, you're guided through the steps to define the vertical's name, content source, and scope of the content to search. The vertical is created in a disabled state. You'll enable it later.

You can use a limited set of Keyword Query Language (KQL) to narrow the scope. This page lists the properties that are available. We recommend that you use freetext keywords and property restrictions with boolean operators for creating the KQL.

Create a vertical at the organization level

To create the vertical on Microsoft Search in SharePoint home, Office, or Bing, follow these steps:

1. In the Microsoft 365 admin center, go to **Verticals**.
2. Select **Add** to get started.

Create a vertical at the site level

1. On the SharePoint site where you want the vertical, go to **Settings**.
2. Select **Site information** and then **View all site settings**.
3. Look for the **Microsoft Search** section, and then select **Configure Microsoft Search for this site collection**.
4. In the navigation pane, go to **Custom experience**, and then select the **Verticals** tab.
5. To add a vertical, select **Add**. Or, to edit a vertical, select it in the list.

Remember, verticals are created in a disabled state. They must be enabled before users can see them.

STEP 2: Create the result types

You can define how results are displayed in the vertical by designing the layout using result types. The result layout lets you show important information directly in the search results, so users don't have to select each result to see if they found what they're looking for.

Default search result layout

A default search result layout will be shown for Connector content if **labels** and **content** property have been mapped correctly to the source properties at the time of configuring the connector. The label **title** is the most important label. It is **strongly recommended** that you have a property assigned to this label to use default search result layout.

Create your own result type

You can decide to create your own search result layout and override the default search result layout by creating a **result type**. A search result type is a rule that causes distinct kinds of search results to be displayed in different ways. It consists of the following:

- **One or more conditions** to compare each search result against, such as the content source of the search result.
- A **result layout** to use for search results that meet the conditions. The result layout controls the way that all results that meet the conditions appear and behave on a search results page.

If appropriate mapping is not done to show default search result layout, Yyou must create at least one result type for results to display on the vertical. You can create multiple result types for each vertical, which allows you to use different layouts for different type of results. For example, you can customize *Severity 1* incidents to have more prominent colors and a larger font compared to *Severity 3* incidents.

After you start the wizard, you're guided through the steps to define the name, content source, and conditions for the result type. You can define the priority of the result type from the list view.

Create a result type at the organization level

1. In the Microsoft 365 admin center, go to **Result types**.
2. To add a **Result type**, select **Add**. To edit a result type, select the result type in the relevant list.

Create a results type at the site level

1. On the SharePoint site where you want to create the result type, go to **Settings**.
2. Select **Site information** and then **View all site settings**.
3. Look for the Microsoft Search section, and then select **Configure Microsoft Search for this site collection**.
4. In the navigation pane, go to **Custom experience**, and select **Result type** tab.
5. To add a result type, select **Add**. Or, to edit a result type, select the result type in the list.

STEP 3: View the vertical after it's enabled

After you enable the vertical, it might take a while before you can view it. If you don't want to wait after enabling it, you can append **cacheClear=true** to the URL in SharePoint and Office to view the vertical immediately.

Troubleshooting

Here's a list of common issues you might encounter and actions to fix them.

ERROR	ACTION
I see a "Something went wrong" error message on the vertical.	Both the vertical and result types are needed to complete the setup. Make sure you have created both for the same content source.
I don't see my result layout, although I created one.	It takes a few minutes because these settings are generally cached. Wait for a few minutes and try again.
I don't see any content sources on the vertical or result type page.	Make sure you have configured connectors and indexed data.

Next steps

STEP 3: Customize the results layout

Create a layout to customize search results

11/30/2020 • 4 minutes to read • Edit Online

You can design the result layout for a custom vertical using the search layout designer. You can start designing the layout by choosing templates offered in the layout designer and using them if they fit your requirements. Or you can choose to edit these templates in various ways to fit your requirements. For example, add/remove images, add/remove text, and modify text. If none of the templates meet your requirements, you can choose to start designing your layout using a blank template.

After the layout is ready, use the Adaptive Cards Template language to create a result layout JSON that's used to define a result type. You map the result properties to the layout using the Mapping step in the layout designer.

Create a layout on your own

Creating a layout on your own requires knowledge of adaptive cards and their schema. Search result layout uses a subset of the elements offered by adaptive cards, and you can use the layout designer to learn about the supported set of elements.

While creating your own layout, create the adaptive card layout using data from your connector, and then finalize the layout. There are two main steps in creating your own layout:

- Design the layout.
- Separate the data from the template.

Design the layout

In this example, we show a layout with a header, link, and descriptive text.

And here's the layout's associated JSON file:

```
{
    "type": "AdaptiveCard",
    "version": "1.0",
     "body": [
{

            "type": "ColumnSet",
             "columns": [
                 {
                     "type": "Column",
                     "width": 8,
                     "items": [
                         {
                             "type": "TextBlock",
                             "text": "Contoso Marketing Analysis - Q3 FY18",
                             "color": "Accent",
                             "size": "Medium",
                             "spacing": "None",
                             "$when": "{title != \"\"}",
                             "weight": "Bolder"
                        },
                        {
      "type": "TextBlock",
      "text": "https://contoso.com/hr/link",
      "spacing": "None",
      "color": "Dark",
      "weight": "Bolder"

                        },

                        {
      "type": "TextBlock",
      "text": "Marketing team at Contoso.., and looking at the Contoso Marketing documents on the team site.
This contains the data from FY20 and will taken over to FY21...Marketing Planning is ongoing for FY20..",
      "wrap": true,
      "maxLines": 2,
      "spacing": "Medium"
      }
      ],

     "horizontalAlignment": "Center",
     "spacing": "None"

                }

            ]

        }
  ],

    "$schema": "http://adaptivecards.io/schemas/adaptive-card.json"
}
```

Separate the data from the layout

You can separate the data from the layout and bind the data.

Here's Layout JSON after binding the data:

```
{

    "type": "AdaptiveCard",
 "version": "1.0",
 "body": [
 {
 "type": "ColumnSet",
"columns": [

                {
    "type": "Column",
    "width": 8,
    "items": [
    {
    "type": "TextBlock",
    "text": "[{title}]({titleUrl})",
    "color": "Accent",
    "size": "Medium",
    "spacing": "None",
    "weight": "Bolder"

                },
     {
     "type": "TextBlock",
     "text": "{link}",
     "spacing": "None",
     "color": "Dark",
     "weight": "Bolder"
     },
     {
     "type": "TextBlock",
     "text": "{description}",
     "wrap": true,
     "maxLines": 2,
     "spacing": "Medium"
     }
     ],
     "horizontalAlignment": "Center",
     "spacing": "None"
     }
     ]

        }

    ],

    "$schema": "http://adaptivecards.io/schemas/adaptive-card.json"
}
```

Sample data: Specify sample data in the **Sample Data Editor** to view the data-bound card when in **Preview Mode**.

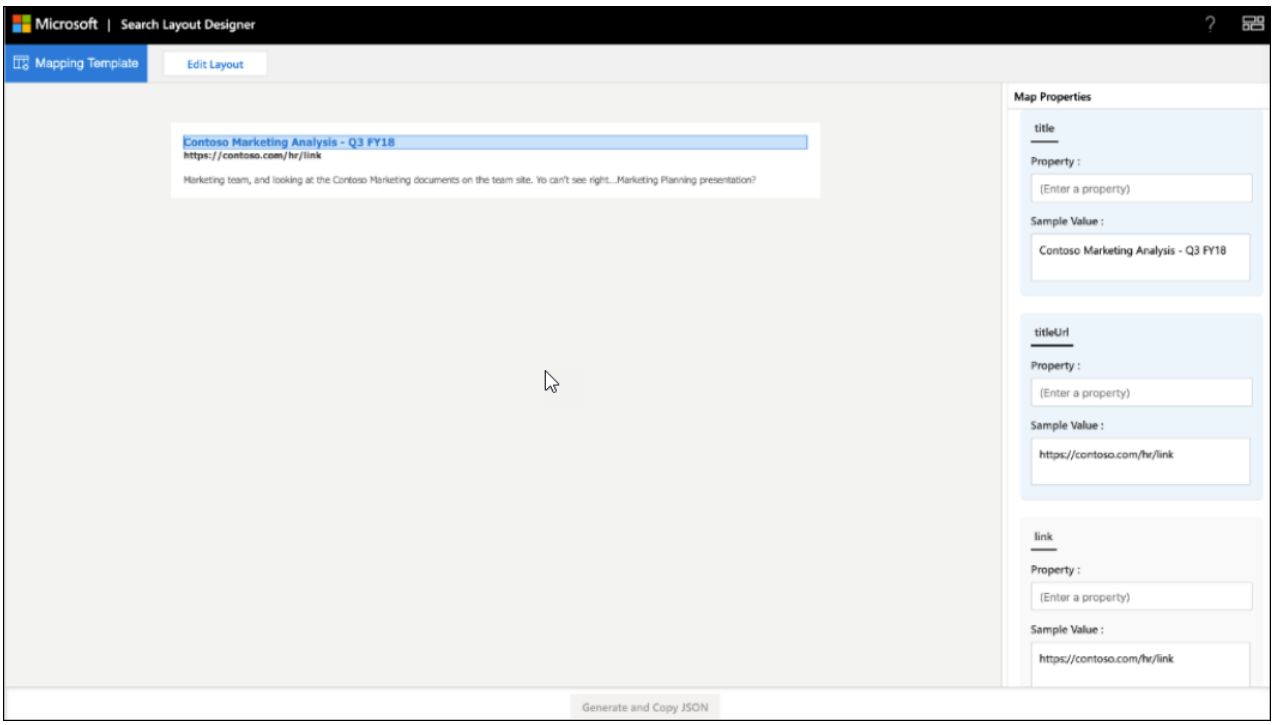
```
{

    "title": "Contoso Marketing Analysis - Q3 FY18",
    "titleUrl": "https://contoso.com/hr/link",
    "link": "https://contoso.com/hr/link",
    "description": "Marketing team, and looking at the Contoso Marketing documents on the team site. Yo can't
see right...Marketing Planning presentation?"

}
```

Map the layout to the result properties

You must map each field of the layout to a result property or a connector property to generate the result layout JSON.



Select a field in the layout to highlight the variables that need to be mapped. You can use multiple variables for a single field, and all fields must be mapped to the result properties.

Show snippet on search result

Dynamic snippets generated on the **content** property of the connector result can be shown on the search result. **ResultSnippet** is the system property that acts as a placeholder property for the snippets generated for each Connector result. To show the snippets on the result layout, the **ResultSnippet** system property must be mapped to an appropriate field, for example Description, in the search result layout. Snippets generated on each result also highlight the matches in the Snippet with the query term entered by the user.

Things to consider

Before you get started, there are a few things that you should do and a few things you should avoid to ensure that your layouts will be successful.

Do

- Edit a template to provide the logo link in the layout if you're using static links for logos and not result properties.
- Validate the result layout for scenarios where no data is returned for a result property used in the result JSON. Use the `$when` condition to hide an element if the property doesn't contain data.
- Make sure that data types of the `$when` condition and the result property match. For example, don't compare `Number` with `Text` in the `$when` condition.
- Think of theme requirements when designing a result layout.
- Make sure that the `Textblock` element can handle dynamic content. You can use the `wrap` and `maxLines` element properties for this purpose.
- Properly format the date when using `{DATE()}` in Markdown.

Don't

- Don't define invalid data types when binding values. For more information about data types, see Manage the Search schema.
- Avoid cropping the result on the result page by following the maximum height of the result layout JSON. If you

exceed the maximum height of the result layout, the result will be cropped on the result page.

- Don't use `px` values in element properties.
- Don't use markdown with the **ResultSnippet** property in the result layout to highlight query match in the search result.

Resources

Customize search result page

Adaptive cards

Adaptive Cards Template language

Adaptive card schema

Graph connectors result cluster

11/30/2020 • 2 minutes to read • Edit Online

Overview of the Graph connectors result cluster (Preview)

With Graph connectors result clusters, enterprises can search for content from third party data sources in their default view (the All tab) in SharePoint and Office.com.

Result clusters help users discover all third party content (previoulsy tied to a single connector and vertical) in one place. The results shown in a result cluster are grouped together based on how the tenant administrator configures them in a search vertical.

How connector results are selected and displayed

Connector results provided in the result cluster are derived from individual search verticals with connector content. Each search vertical provides a set of relevant results which becomes a candidate result cluster. Relevant results are chosen based on the "title" property, result snippet, and content component of each item.

To ensure discovery of content from the search verticals, we recommend providing meaningful titles for your items. This positively impacts the arbitration of result cluster candidates and the likelihood of your content showing up in a result cluster. For example, avoid the use of IDs as values for the property "title" unless your users are using IDs to look for content.

How often a result cluster is shown varies on factors such as the number of search verticals that you configure and the type of content. By either selecting or ignoring result cluster results, you will implicitly provide hints that will adjust the triggering of result clusters over time.

The search result experience for connector items shown in your result cluster is system generated and does not use custom result layouts. You must declare the "title" property and item content during connection registration if you want results to appear in your result cluster.

Enable result clusters

The result cluster experience is turned off by default.

Follow these steps to turn on the experience at the organization level:

1. In the Microsoft 365 admin center, go to **Settings** > **Search & intelligence** > **Customization** > **Verticals**.
2. Select the **All** vertical, then enable **Show connector results**.

Follow these steps to turn on the experience at the site level:

1. On the SharePoint site where you want the result cluster experience, go to **Settings**.
2. Go to **Site information**>**View all site settings**.
3. Go to the Microsoft Search section, then select **Configure Microsoft Search for this site collection**.
4. In the navigation pane, go to **Custom experience**, then select **Verticals**.
5. Select the **All** vertical, then enable **Show connector results**.

View the result cluster experience after it is enabled

After you turn on the result cluster experience, it might take a few minutes before you can view it. If you want the experience immediately, you can append *cacheClear=true* to the URL in SharePoint and Office.

Create custom Filters

11/30/2020 • 2 minutes to read • Edit Online

You can create filters to customize the search experience that users see when they search in Microsoft SharePoint, Microsoft Office, and Microsoft Search in Bing. Filters lets users quickly refine the set of results from their search query.

A custom filter can be created inside a vertical based on a connection property. For example, you can create a **Published On** filter for ServiceNow connection inside a custom vertical.

Things to consider

1. For creating custom filter on connection content source, some additional capabilities are provided:

- You can also create filter on an alias to connector source properties
- In case your vertical has multiple connections then you can create a common filter across these connections. This can be done by creating the filter on an common alias which aliases source properties across across different connections. For example you can create an **Author** filter across a ServiceNow & a Jira connection by creating aliases as follows:

CONNECTION	PROPERTY	ALIAS
Service Now	Owner	Author
Jira	Publisher	Author

2. Filters exist within the scope of the vertical. Hence,

- If a filter is created in a vertical which is at organizational level, then the filter would only be visible at the organizational level
- If a filter is created in a vertical which is at site level, then the filter would only be visible at the site level.

Steps to Create custom filter

Create filter in organizational level vertical:

To create a filter on Microsoft search follow these steps:

1. In the Microsoft 365 admin center, go to the Verticals page.
2. Create/Edit the vertical in which you want to create the filter
3. Navigate to the 'Filters' step in the wizard
4. Click on 'Add Filter' and get started After adding filters, you can review and save the vertical.

Known Limitations

1. You can currently create filters only on String & Date type managed properties.
2. You cannot create hierarchical filters

Resources

Customize search result page

Get started with Microsoft Search in SharePoint

11/18/2019 • 2 minutes to read • Edit Online

Microsoft Search in SharePoint is the modern search experience in SharePoint Online. SharePoint Online also offers a classic search experience. As a search administrator, you can't turn either of these search experiences on or off. They're both on by default. Which search experience your users get depends on where they search from:

- Users get the Microsoft Search box on the SharePoint start page, hub sites, communication sites, and modern team sites.
- Users get the classic search box on publishing sites, classic team sites, and in the SharePoint Search Center.

To get your organization going with Microsoft Search in SharePoint, take the steps in the following sections.

Prepare for Microsoft Search in SharePoint

Users can only find SharePoint content that's been indexed. Microsoft Search and classic search share the same index for SharePoint content, which is crawled and indexed automatically.

Some organizations use both classic search and Microsoft Search in SharePoint. To learn how to avoid impact from classic search settings on Microsoft Search in SharePoint, see Differences between the classic and modern search experiences in SharePoint Online.

Follow the guidelines to set up Microsoft Search.

Get your organization to adopt modern sites

For a better search experience, influence your organization to try modern instead of classic sites. To learn more, see SharePoint classic and modern experiences.

Promote searching from the SharePoint start page

Teach your users to search from the SharePoint start page instead of from the classic Search Center. Consider hiding your classic Search Center from users.

See also

Overview of Microsoft Search

Overview of search in SharePoint Online

Search experiences in SharePoint

Create a custom search results page in SharePoint Online

11/30/2020 • 2 minutes to read • Edit Online

One way to customize the search experience in SharePoint is to create a custom search results page for a site. This allows you to use a page that you created, rather than the default in Microsoft Search results page. This gives you more flexibility on how the search results experience looks for your users.

> **NOTE**
>
> To make changes to the default Microsoft Search results page that is available by default, please see Customize the search results page.

With a custom results page you can create a new page that can be used to control the layout and design of search results to support your organization's needs. You can use any built-in web parts, open-source search web parts from SharePoint Patterns and Practices community, as well as any custom web parts that you may have developed using SharePoint Framework.

Configure a results page

To configure a custom results page in SharePoint Online follow the steps below:

1. Browse to the site where you would like to configure a custom results page and go to **Site Settings > Site Collection Settings > Search Settings**.
2. In Search Settings, clear selection from **Use the same results page settings as my parent**, choose **Send queries to a custom results page**, and provide a value for **Results page URL:**. Then, save your changes. The URL you use here should be for the page that you created to use as your custom results page.

> **NOTE**
>
> The custom results page needs to be on the same domain as your site, but it does not have to be in the same site collection.

Alternatively, you can use the Set-PnPSearchSettings SharePoint PnP PowerShell command to set the value instead of using the Site Settings page.

Once set, the custom search results page is displayed when you search using the Microsoft Search box that appears in the navigation bar on top of the page and is used when you enter search from site pages or the home page of the site. It is not used when you are searching within a list, library, or the site contents page. You may use the link to expand your search from search results in lists and libraries to get to the custom results page.

Change the layout of your custom results page

A page layout named **HeaderlessSearchResults** can be used to make the search results page appear closer to our out of box search results experience. This new layout can only be active for the pages that are set to be the custom search results page.

To set the page layout, you can use the Set-PnPClientSidePageSharePoint PnP PowerShell command with -LayoutType HeaderlessSearchResults.

Use SharePoint Framework Query extensions

Custom search results pages can also make use of the SharePoint Framework Query Extension to modify the query before it gets sent to the search engine.

Additional resources

To learn more about custom results page, check out our Ignite 2019 Search Customization and Development session.

For open source projects, getting started with our Microsoft Search APIs, and more customization and extensibility samples, visit Microsoft Search on GitHub.

Security and Privacy for Microsoft Search in Bing

2/4/2020 • 3 minutes to read • Edit Online

With enhanced privacy and security measures, Microsoft Search in Bing helps protect your users and workplace data.

Secure by default

Microsoft Search in Bing requests are made over HTTPS. The connection is encrypted end-to-end for enhanced security.

Authentication and authorization with Azure Active Directory

Authentication for Microsoft Search in Bing is tied to Azure Active Directory. When Microsoft Search users go to Bing, the Bing header will show sign-in options for a Microsoft account as well as a work or school account. If Bing can't determine whether a user is an eligible participant, users can go to the Explore Microsoft Search page, where they'll be automatically redirected to your organization's sign-in page.

Users can access Microsoft Search only through a work or school account. They need to sign in with the same credentials they use to access Office 365 services such as SharePoint or Outlook. A personal Microsoft account can't be used to sign in to Microsoft Search.

Single sign-on

If a user is already authenticated with their work or school account in another service, such as Outlook or SharePoint, they'll be automatically signed into the same work or school account when they go to Bing in the same browser. Also, when the user signs out of their work or school account, they'll be automatically signed out from other Microsoft Office services in the same browser.

Communicates with the Microsoft cloud from the browser

When a user signs in with their work or school account, Bing will download the necessary client libraries to the browser to enable Microsoft Search results. Then, when they search, the in-browser code calls the Office 365 cloud to get work results. To do this, Microsoft Search uses a dedicated API that is operated in accordance with the control objectives of SSAE 18 SOC2 Type 1. This means work results and work data do not flow through Bing systems that are subject to less stringent data processing control objectives than the work results themselves are subject to when processed in Office 365 Core Online Services.

Permissions

Work results retrieved from Office 365 workloads such as SharePoint and OneDrive for Business are security trimmed at the source. Users can't see resources such as Word documents or PowerPoint presentations they can't see and access through Office 365. They can only see their own files and files that have been shared with them by the author explicitly or implicitly (through a group membership, for example) in SharePoint.

Microsoft Search in Bing protects workplace searches

When a user enters a search query in Microsoft Search in Bing, two simultaneous search requests occur:

- A search of your organization's internal resources.

- A separate search of public results from Bing.com.

Because workplace searches might be sensitive, Microsoft Search has implemented a set of trust measures that describe how the separate search of public results from Bing.com is handled.

Logging

- All Bing.com search logs that pertain to Microsoft Search in Bing traffic are disassociated from your workplace identity.
- If a set of restrictions or frequency thresholds are met which give us confidence that the query is not specific to a particular organization, the query will be treated as described in the Search and artificial intelligence section of the Privacy Statement. For example, such queries will be used to model and train public features, such as autosuggest or related searches.
- Queries that do not meet the set of restrictions or frequency thresholds will be stored separately from public, non-Microsoft Search traffic.

Advertising

Advertising shown on Bing.com in connection with workplace searches is solely related to the content of the search queries. Ads are never targeted to users based on their workplace identity.

GDPR

The May 21, 2018, blog post from Microsoft reflects our commitment to GDPR compliance and how Microsoft helps businesses and organizations with their own GDPR compliance obligations. You can find additional detail in the Microsoft Trust Center FAQ.

Microsoft Search queries executed against a customer's internal resources and results returned are considered Customer Data and, as such, also meet the processor commitments outlined in Article 28 as reflected in the Trust Center FAQ. With respect to queries from Microsoft Search that go to public Bing, Microsoft complies with its GDPR obligations as a data controller.

Add a search box to your intranet site

11/30/2020 • 2 minutes to read • Edit Online

To provide your users with easy access to results from your organization, add a Microsoft Search in Bing search box to any intranet site or page. These are some of the benefits:

- A search box on your SharePoint or intranet portal provides a familiar, trusted entry point to start searching
- Supports all major web browsers, including Google Chrome and Microsoft Edge
- Only search suggestions from your organization appear, web suggestions are never included
- Takes users to a Microsoft Search in Bing work results page, which excludes ads and web results
- You control the appearance and behavior of the search box

Add a search box to an intranet page

You need to add two elements to the page: a container for the search box and the script that powers it.

```
<div id="bfb_searchbox"></div>
<script>
    var bfbSearchBoxConfig = {
        containerSelector: "bfb_searchbox"
    };
</script>
<script async src="https://www.bing.com/business/s?k=sb"></script>
```

On a SharePoint classic site, add a Script Editor Web Part and drop the script in it.

Enable the search box for mobile

For intranet sites or pages available to mobile users, add isMobile: true to the settings object:

```
<div id="bfb_searchbox"></div>
<script>
    var bfbSearchBoxConfig = {
        containerSelector: "bfb_searchbox",
        isMobile: true
    };
</script>
<script async src="https://www.bing.com/business/s?k=sb"></script>
```

Put focus on the search box by default

To help users search faster, when the page or site loads place the cursor in the search box by adding focus: true to the settings object:

```
<div id="bfb_searchbox"></div>
<script>
    var bfbSearchBoxConfig = {
        containerSelector: "bfb_searchbox",
        focus: true
    };
</script>
<script async src="https://www.bing.com/business/s?k=sb"></script>
```

Customize the appearance of the search box

To help the search box better fit with the style of your intranet, there are a variety of configuration options you can use. Mix and match options to suit your needs.

```
<div id="bfb_searchbox"></div>
<script>
    var bfbSearchBoxConfig = {
        containerSelector: "bfb_searchbox",
        width: 560,                             // default: 560, min: 360, max: 650
        height: 40,                             // default: 40, min: 40, max: 72
        cornerRadius: 6,                        // default: 6, min: 0, max: 25
        strokeOutline: true,                    // default: true
        dropShadow: true,                       // default: true
        iconColor: "#067FA6",                   // default: #067FA6
        companyNameInGhostText: "Contoso"       // default: not specified
                                                // when absent, ghost text will be "Search work"
                                                // when specified, text will be "Search
<companyNameInGhostText>"
    };
</script>
<script async src="https://www.bing.com/business/s?k=sb"></script>
```

Use an iFrame to embed a search box

If embedding a script isn't an option for the site, use an iFrame to add the search box. You won't be able to customize the appearance of the search box.

```
<iframe width="564" height="400" src="https://www.bing.com/business/searchbox"></iframe>
```

Make Microsoft Edge the default browser

11/14/2019 • 2 minutes to read • Edit Online

To give your users the best experience with Microsoft Search, you can make Microsoft Edge the default browser. This will only set Microsoft Edge as the default browser for users in your org, individual users can still select a different browser.

Windows 8 and later

These instructions show you how to make Microsoft Edge or Internet Explorer as the default browser for computers running Windows 8 or later. Users will be able to change the browser after this policy is set.

STEP 1: Create the default associations file

Create the default associations file in the SYSVOL folder of the domain controller.

1. Open an administrative PowerShell console.
2. `New-Item -Path "\\$env:USERDOMAIN\SYSVOL\$env:USERDNSDOMAIN" -Type Directory -Name "Settings"`
3. `$SettingsPath="\\$env:USERDOMAIN\SYSVOL\$env:USERDNSDOMAIN\Settings"`
4. `Start-Process Dism.exe -PassThru "/Online /Export-DefaultAppAssociations:$SettingsPath\AppAssoc.xml"`

STEP 2. Add or edit the default associations file

1. `Notepad "$SettingsPath\AppAssoc.xml"`
2. Edit the following entries (.htm, .html, http, https), and remove other entries if they're not needed.

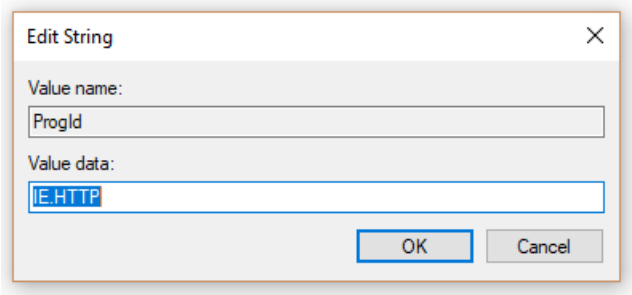
- Microsoft Edge
  - ```
    <Association Identifier=".htm" ProgId="AppX4hxtad77fbk3jkkeerkrm0ze94wjf3s9"
    ApplicationName="Microsoft Edge" />
    ```
  - ```
    <Association Identifier=".html" ProgId="AppX4hxtad77fbk3jkkeerkrm0ze94wjf3s9"
    ApplicationName="Microsoft Edge" />
    ```
  - ```
    <Association Identifier="http" ProgId="AppXq0fevzme2pys62n3e0fbqa7peapykr8v"
    ApplicationName="Microsoft Edge" />
    ```
- Internet Explorer
  - `<Association Identifier=".htm" ProgId="htmlfile" ApplicationName="Internet Explorer" />`
  - `<Association Identifier=".html" ProgId="htmlfile" ApplicationName="Internet Explorer" />`
  - `<Association Identifier="http" ProgId="IE.HTTP" ApplicationName="Internet Explorer" />`
  - `<Association Identifier="https" ProgId="IE.HTTPS" ApplicationName="Internet Explorer" />`

Step 3. Edit the Group Policy

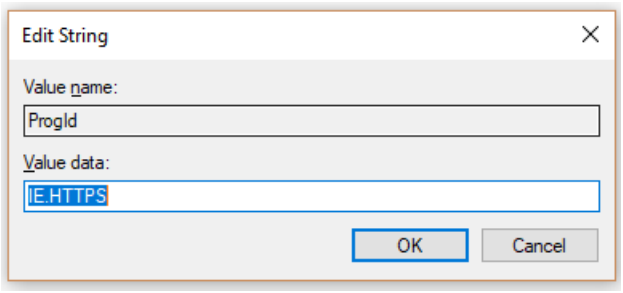
1. Open **Group Policy Management Console** (gpmc.msc) and switch to editing any existing policy or creating a new one.
2. Navigate to **Computer Configuration\Administrative Templates\Windows Components\File Explorer**.
3. Double-click **Set a default associations configuration file**, set it to **Enabled**, and enter the path to AppAssoc.xml (for example %USERDOMAIN%\SYSVOL%USERDNSDOMAIN%\Settings\AppAssoc.xml) Enforce the resultant GPO by linking it to the appropriate domain.

Windows 7
    ```

1. Configure the local machine that will be used to set the GPO.
2. Open **Control Panel\Programs\Default Programs\Set Default Programs** and set Internet Explorer as the default.
3. Open Group Policy Management Console (gpmc.msc) and switch to editing any existing policy or creating a new one.
4. Navigate to **<Computer/User> Configuration\Policies\Preferences\Windows Settings**.
5. Right-click on **Registry\New** and select **Registry Wizard**.
6. From the Registry Browser window, select **Local Computer** and click **Next**.
7. Navigate to **HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\https** and select the ProgId value. Make sure the value looks like the one below:



8. Navigate to **HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\https** and select the ProgId value. Make sure that the value looks like the one below:



9. Enforce the resultant GPO by linking it to the appropriate domain.

Make Bing the default search engine

11/14/2019 • 4 minutes to read • Edit Online

This article explains how you can make Bing the default search engine for Microsoft Edge, Google Chrome, and Internet Explorer.

Microsoft Edge on Windows 10, Version 1703 or later

Although you'll set Bing as the default search engine, Microsoft Edge allows users to change their settings to use a different search engine.

For the latest ADMX files for various versions of Windows, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows.

If the setting described in this section cannot be found inside of GPMC, download the appropriate ADMX and copy them to the central store. For more information, see Editing Domain-Based GPOs Using ADMX Files. Central store on the controller is a folder with the following naming convention:

%systemroot%\sysvol\<domain>\policies\PolicyDefinitions

Each domain that your controller handles should get a separate folder. The following command can be used to copy the ADMX file from the command prompt:

```
Copy <path_to_ADMX.ADMX> %systemroot%\sysvol\<domain>\policies\PolicyDefinitions
```

1. Open the Group Policy Management Console (gpmc.msc) and switch to editing an existing policy or creating a new one.
2. Navigate to **<Computer/User Configuration>\Administrative Templates\Windows Components\Microsoft Edge**.
3. Double-click **Set default search engine**, set to **Enabled**, and enter `https://www.bing.com/sa/osd/bfb.xml`
4. Enforce the resultant GPO by linking it to the appropriate domain.

Google Chrome on Windows XP SP2 or later

Users won't be able to change the default search engine after this policy is set.

Chrome comes with its own set of group policy settings which can be downloaded in the form of an ADMX file from Google Chrome Enterprise Help. If operating systems Windows Vista/Server 2008 or later are used to manage GPO's for the domain, the ADMX file provided in this package takes care of Chrome settings on Windows XP SP2 or later.

Copy the template file to a central store for ADMX files on the domain controller. For more information, see Editing Domain-Based GPOs Using ADMX Files. Central store on the controller is a folder with the following naming convention:

%systemroot%\sysvol\<domain>\policies\PolicyDefinitions

Each domain that your controller handles should get a separate folder. The following command can be used to copy the ADMX file from the command prompt:

```
Copy <path_to_Chrome.ADMX> %systemroot%\sysvol\<domain>\policies\PolicyDefinitions
```

1. Open the Group Policy Management Console (gpmc.msc) and switch to editing any existing policy or creating a new one.
2. Make sure the following folders appear in the Administrative Templates section of both User/Computer Configuration: Google Chrome and Google Chrome - Default Settings.

- The settings of the first section are fixed and local administrators won't be able to change them in the browser.
- The settings of the latter section of policies can be changed by users in the browser settings.

3. Navigate to **<Computer/User> Configuration\Administrative Templates\Google Chrome\Default search provider**
4. Double-click **Enable the default search provider**, and set it to **Enabled**.
5. Double-click **Default search provider icon**, set it to **Enabled**, and enter `https://www.bing.com/sa/simg/bb.ico`
6. Double-click **Default search provider instant URL**, and enter `https://www.bing.com/business/search?q={searchTerms}&form=BFBSPR`
7. Double-click **Default search provider name**, set it to Enabled, and enter 'Microsoft Search in Bing'
8. Double-click **Default search provider search URL**, set it to **Enabled**, and enter `https://www.bing.com/business/search?q={searchTerms}&form=BFBSPR`
9. Double-click **Default search provider suggest URL**, set it to **Enabled**, and enter `https://business.bing.com/api/v2/browser/suggest?q={searchTerms}&form=BFBSPA`
10. Enforce the resultant GPO by linking it to the appropriate domain.

Setting the default search engine will add the Microsoft Search search suggestions feature in the browser address bar. Currently, this supports bookmarks only. Users will see the top two bookmark suggestions above public web suggestions as they type in the address bar.

Internet Explorer 11 or later

Users will be able to change the search provider after this policy is set.

STEP 1. Configure the local machine that will be used to set the GPO

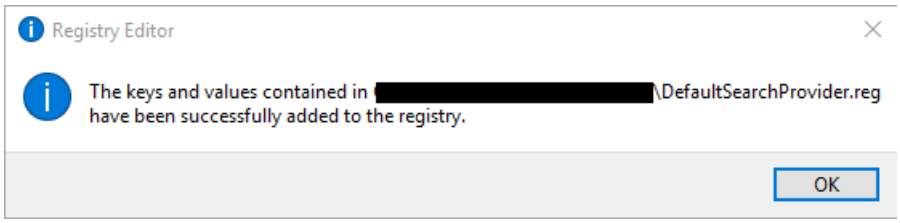
Paste the following text into a reg(*.reg) file.

Windows Registry Editor Version 5.00

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes]
"DefaultScope"="{D54CD0C8-C007-4BC4-B2DD-1E4896B8406D}"
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\{D54CD0C8-C007-4BC4-B2DD-
1E4896B8406D}]
"Codepage"=dword:0000fde9
"DisplayName"="Microsoft Search in Bing"
"OSDFileURL"="https://www.bing.com/sa/osd/bfb.xml"
"FaviconURL"="https://www.bing.com/sa/simg/bb.ico"
"SuggestionsURL_JSON"="https://business.ing.com/api/v2/browser/suggest?q=
{searchTerms}&form=BFBSPA"
"ShowSearchSuggestions"=dword:00000001
"URL"="https://www.bing.com/business/search?q={searchTerms}&form=BFBSPR"
```

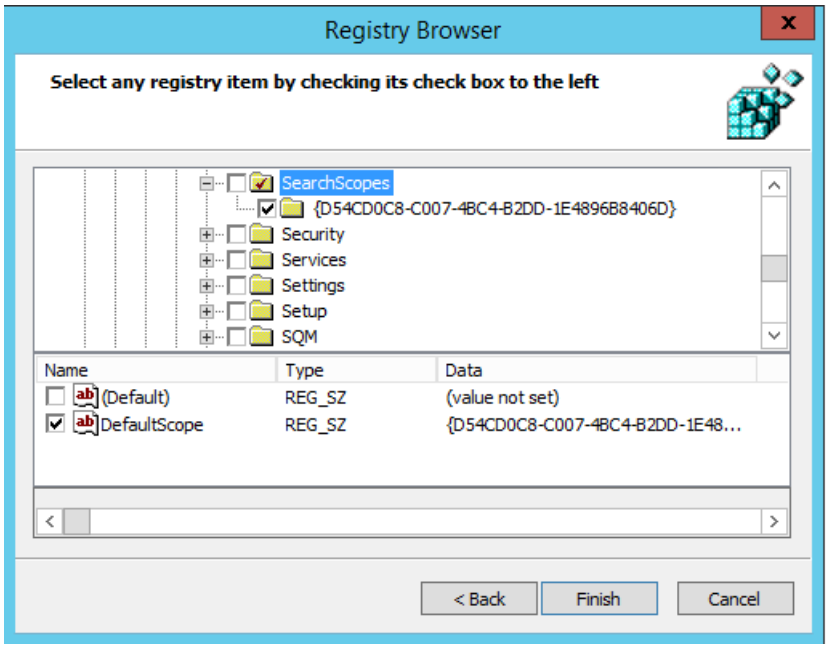
Double-click the file created and follow the steps to import the file. A successful import should result in the

following dialog:

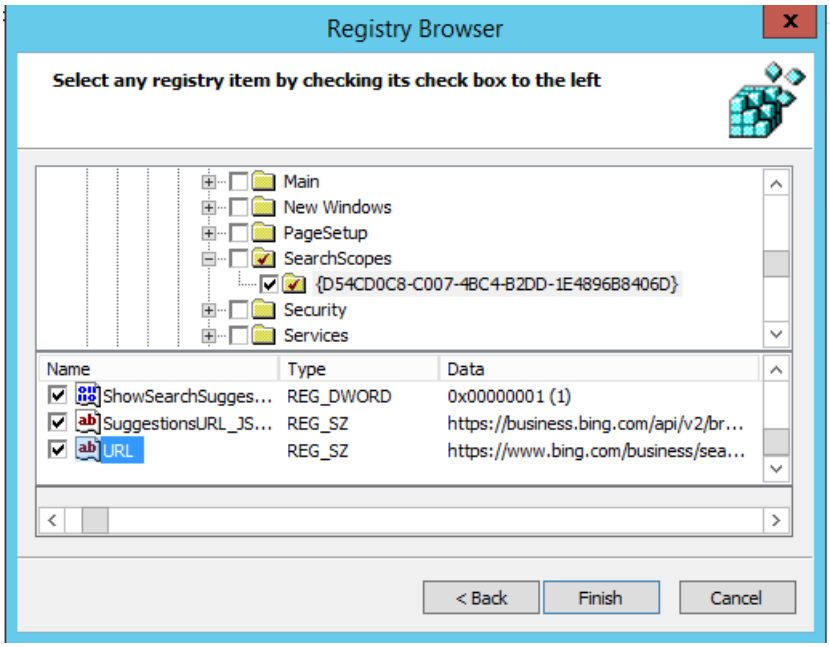


STEP 2. Open the Group Policy Management Console (gpmc.msc) and switch to editing an existing policy or creating a new one

1. Navigate to **User Configuration\Policies\Preferences\Windows Settings**.
2. Right-click on **Registry\New** and select **Registry Wizard**. From the Registry Browser window, select **Local Computer** and click **Next**.
3. Navigate to **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\SearchScopes**.
4. From this key, make sure to select DefaultScope.



5. Check all sub keys containing the GUID for Microsoft Search in Bing and every value under the key except any path to user profiles. Scroll down to select other items.



6. Click Finish to complete this configuration.

STEP 3. Set up User Preferences to help eliminate a warning the user may get when DefaultScope search is enforced

This warning is by design and alerts users of a program trying to modify their settings.

1. Within the same GPO, right click on **Registry\New** and select **Registry Wizard**.
2. Navigate to **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\User Preferences**.
3. Select the **User Preference** key.
4. Click **Finish**.
5. Click on the newly created object. On the right-side pane double click on the User Preferences object, change the **Action** to **Delete and Save**.
6. Enforce the resultant GPO by linking it to the appropriate domain.

Make Bing.com the default home page

11/14/2019 • 2 minutes to read • Edit Online

This article explains how to set Bing.com as the default home page for Microsoft Edge, Google Chrome, and Internet Explorer browsers.

Microsoft Edge on Windows 10, Version 1511 or later

Users won't be able to change this once this policy is set.

1. Open the Group Policy Management Console (gpmc.msc) and switch to editing any existing policy or creating a new one.
2. Navigate to **Administrative Templates\Windows Components\Microsoft Edge**.
3. Double-click **Configure Start pages**, set it to **Enabled**, and enter `https://www.bing.com/business`
4. Enforce the resultant GPO by linking it to the appropriate domain.

Google Chrome on Windows XP SP2 or later

The Windows Support article on managing ADMX files and the latest ADMX files for different versions of Windows can be found on Microsoft Support.

You'll also need the latest Google policy file, which you can find on Google Chrome Enterprise Help.

If the settings described in this section can't be found inside of GPMC, download the appropriate ADMX and copy them to the central store. Central store on the controller is a folder with the following naming convention:

%systemroot%\sysvol\<domain>\policies\PolicyDefinitions

Each domain your controller handles should get a separate folder. The following command can be used to copy the ADMX file from the command prompt:

```
Copy <path_to_ADMX.ADMX> %systemroot%\sysvol\<domain>\policies\PolicyDefinitions
```

1. Open the Group Policy Management Console (gpmc.msc) and switch to editing any existing policy or creating a new one.
2. Make sure the following folders appear in the **Administrative Templates** section of both *User/Computer Configuration*: Google Chrome and Google Chrome - Default Settings (users can override).
   - The settings of the first section are fixed and the local administrator won't be able to change them.
   - The settings of the latter section of policies can be changed by users in their browser settings. You should decide if users can override your default setting. In the following steps, change in the setting in the folder that corresponds to your organization policy and needs. The steps below use the Google Chrome - Default Settings as the default.
3. Navigate to **<Computer/User Configuration>\Administrative Templates\Google Chrome - Default Settings\Home Page**.
4. Double-click **Use New Tab Page as homepage**, and set it to **Enabled**.
5. Navigate to **<Computer/User Configuration>\Administrative Templates\Google Chrome - Default Settings\New Tab Page**.
6. Double-click **Configure the New Tab Page URL**, set it to **Enabled**, and enter

`https://www.bing.com/business?form=BFBSPR`

7. Enforce the resultant GPO by linking it to the appropriate domain.

Internet Explorer 5.0 or later

Users can still change the home page after this policy is set.

1. Open the Group Policy Management Console (gpmc.msc) and switch to editing any existing policy or creating a new one.
2. Navigate to **User Configuration\Preferences\Control Panel Settings\Internet Settings**.
3. Right-click on **Internet Settings** and select **Internet Explorer 10**.

> **NOTE**
> You need to select the option of Internet Explorer 10 to apply the settings for Internet Explorer 11 as the same settings apply to Internet Explorer 11.

4. Settings which are underlined in red are not configured at the target machine, while settings underlined in green are configured at the target machine. To change the underlining, use the following function keys:

   F5 - Enable all settings on the current tab

   F6 - Enable the currently selected setting

   F7 - Disable the currently selected setting

   F8 - Disable all settings on the current tab

5. Press **F8** to disable all settings before configuring anything. The screen should look like this:

6. Press **F6** on the Home page setting and enter `https://www.bing.com/business?form=BFBSPR`
7. Enforce the resultant GPO by linking it to the appropriate domain.

User adoption guide

11/30/2020 • 7 minutes to read • Edit Online

This information is intended for Microsoft Search admins, change management leaders, and business owners.

To roll out and ensure the successful adoption of Microsoft Search across your organization, we recommend this four-stage process.

Stage 1: Stakeholders

To ensure a seamless rollout and increase user adoption of Microsoft Search, identify people who can help support and drive the process.

The table shows the team hierarchy and what each person contributes.

User adoption team roles and responsibilities

ROLE	RESPONSIBILITIES	DEPARTMENT
Executive sponsor	Understand the high-level vision and value of Microsoft Search for your organization. Provide leadership support to IT/business team. Allocate resources. Communicate directly with employees.	Executive leadership
Business owner	Identify product and user scenarios. Determine success metrics for departments and the organization.	Any
Change management team	Ensure product value is easy to understand. Create a plan for the roll out.	IT
Champions	Evangelize the product to peers and teams.	Any (staff)
Search administrator	Identify user adoption core team members. Administrate Microsoft Search, including look and feel of the experience and ongoing management. Drive discussions to show the value of Microsoft Search.	IT
Editors	Create content in the Microsoft 365 admin center.	IT/Any

Stage 2: Scenarios

To ensure user adoption, it's critical to determine and define end-user scenarios. These should include real-world examples of how people can use Microsoft Search to find the information they need, answer questions, and complete tasks faster. In order to measure the success of your roll out and user adoption, it's also important to

determine the metrics you'll use before you begin.

Understand what your users need and want

When it comes to finding information and getting answers, knowing your user's needs and pain points is key. You can use quantitative methods, like data from Office 365 and SharePoint search usage, or qualitative methods, like surveys and user focus groups to get this data. This will help you determine when, where, and how Microsoft Search can provide value.

For various roles and teams across your organization, consider:

- Existing user pain points when searching for information.
- Frequently used apps, tools, sites, and other information sources.
- What users would like to see when it comes to searching for information.
- How the benefits of Microsoft Search apply to your organization. For more information, see Microsoft Search Overview.

Choose the user scenarios that will have the biggest positive impact for your users.

Identify success metrics

To help you meet your roll-out goals and show a positive impact for your organization, it's critical to determine your key success metrics before you start. Keep your goals simple and measurable, and assess performance on a regular basis, so you can respond quickly if needed.

1. **Change management:** Determine how you'll measure awareness of Microsoft Search and the success of communications about it.
2. **Usage:** You can leverage data from your Insights Dashboard including daily and monthly active users (DAU and MAU), the content types that are getting the most views, and top search keywords to measure usage over time. For more information, see Microsoft Search Insights dashboard reports.
3. **User satisfaction:** Use the data you gathered from surveys and user focus groups to determine your baseline. Net satisfaction (NSAT) and Net Promoter Scores (NPS) can also provide helpful measurements. Regardless of the method you use, keep it consistent, so you can see impact over time.
4. **Other measurements:** Use historical and/or current data for support requests and the amount of time spent searching.

Stage 3: Readiness

Investing time in preparing for your Microsoft Search rollout will result in a positive impact for your organization. Microsoft provides an Adoption Kit that contains an announcement email template, lightweight, visual content created for sharing on your internal communication sites, and a training presentation. There's also a Microsoft Search Resource Center where you can find other training and adoption resources designed to help make your Microsoft Search rollout a successful one.

Product and content readiness

Administrators directly influence the search experience for end users and determine how Microsoft Search looks for the organization. This includes choosing the types of results you want to surface to your users. These results can include links—also known as bookmarks—to documents, sites, people, groups, locations, conversations, and other workplace resources.

For more information, see Set up Microsoft Search.

Editors are subject matter experts who help manage bookmarks and Q&As within their areas of expertise. Editors should create content that addresses the user scenarios that you identified earlier.

For more information, see Plan your content.

Signing in

Microsoft Search users must sign in to Bing with a work or school account. To make signing in as seamless as possible for your users:

- To make sure Azure Active Directory configurations are correctly set, have a few users try to sign in. For more information, see Test single sign-on.
- Set browser defaults for company-managed devices to Bing. For more information, see Set default browser.
- Deploy search extensions for Microsoft Edge and Google Chrome users via Group Policy. For more information, see Microsoft Search Overview.

Draft communications

Use your real-world scenarios to tell users about Microsoft Search and how it will help them save time. Your change management team can help create a rollout strategy and prepare collateral and campaigns for end-user readiness.

Begin planning communications and events for your organization:

- Place banners, posters, or leaflets in prominent locations.
- In-person product demos or booths.
- Online events for local and remote teams.
- Have your executive sponsor host a town hall meeting or send an announcement email.
- Share self-help documentation about using Microsoft Search.

All communications should educate users about how they can sign in to Bing to find work results.

Engage partner teams

As an integral part of Microsoft 365, Microsoft Search complies with GDPR and Tier-C guidelines. Depending on your organization, it might be necessary to share information about Microsoft Search with your privacy and security teams. For more information, see Security and Privacy for Microsoft Search in Bing.

Make sure your help desk knows about the features and functionality of Microsoft Search, as well as the user requirements to sign in, so they can more effectively support users. For more information, see Learn about Microsoft Search in Microsoft 365 and FAQs.

Evaluate with pilot users

Start with a small group of users to evaluate the impact of Microsoft Search and gather early feedback. This gives you time to change content, update your communications, and set expectations for the broad rollout. Search power users or early adopters are great candidates for this.

To help find pilot users:

- Partner with a business sponsor within your organization.
- Identify a group of early adopters.
- Identify groups that do high volumes of enterprise searches.
- Identify users in other geographical locations, including international.

Ask your pilot users to provide input using the feedback options in Microsoft Search or via simple surveys.

Survey questions to ask:

- Do you understand how to sign in and use Microsoft Search?

- Does it work as expected?
- Which features do you like?
- Were you able to find work results?
- Were the work results helpful?
- Are the communications about Microsoft Search clear and understandable?

This is a great time to begin measuring the effectiveness of the metrics identified in Stage 2.

When you start the pilot phase, consider sharing a sneak peek of Microsoft Search with the wider organization.

Stage 4: Roll out

Every organization thinks about product rollouts differently. Here are a few things to consider.

Broad deployment

When you're ready, either allow all users in your organization access to Microsoft Search, or use a phased approach to roll out more slowly.

Generate awareness

Build excitement in your organization about Microsoft Search:

- Enlist pilot users to provide peer-to-peer assistance and expertise.
- Follow through on the communications and events you planned in Stage 3.

Ongoing communication

For the first few weeks and months, maintain a rhythm of communications to encourage engagement with Microsoft Search. This keeps users informed and engages new users. Each communication should explain why Microsoft Search can be helpful to their work.

Send ongoing communications that highlight features and searches to try, as well as user success stories.

Gather feedback and improve

Support users and let them know you care by listening to them and acting on their feedback.

Use the insights dashboard to see how the product and the content is performing. Leverage this information to update bookmarks, Q&As, and other communications. This will also help you:

- Improve the content quality: review titles, descriptions, and URLs, optimize keywords, remove obsolete information, and add new information.
2. Determine which features are most frequently or infrequently used.
3. Conduct surveys, focus groups, and feedback sessions to understand what users think of Microsoft Search, increase adoption, and identify improvement areas.

Education and feedback is an iterative process. It might be necessary to make changes to content and communications as your users adopt Microsoft Search.