

Getting Started With Microsoft SharePoint Online Connector

The GoAnywhere MFT Microsoft SharePoint Online Connector allows you to integrate with Microsoft SharePoint via the Microsoft Graph API. Actions supported by this cloud connector include uploading, downloading, moving, renaming, and deleting files and folders.

Prior to integrating GoAnywhere MFT with Microsoft SharePoint Online Connector, use the following instructions to create a SharePoint site and configure and retrieve the Microsoft SharePoint settings to add a Cloud Connector Resource in GoAnywhere MFT.

Step 1: Register GoAnywhere as an Application with Microsoft Azure

Registering with Microsoft Azure will create the Application (client) ID, which will be used later when adding a Cloud Connector Resource in GoAnywhere MFT.

1. Log in to the Microsoft Azure portal at <https://portal.azure.com>.
2. Select **App registrations**.
3. Select **New registration**.
4. Define the **Name** for the application, which is the user-facing display name. This name can be changed later.
5. In the Supported account types section, choose who can use this application or access this API by selecting the radio button next to one of the three account types. **The Help me choose...** link supplies definitions for the different account types.
6. Select **Register** to register your new application.
7. On the Overview page, you will see your **Application (client) ID**.

Step 2: Create a Client Secret

The client secret will be used later as the Application Password when adding a Cloud Connector Resource in GoAnywhere MFT.

1. Select **Certificates and secrets** in the leftmost panel.
2. In the Client secrets section, select **New client secret**.
3. Enter a description into the **Description** field.
4. Select when the client secret expires.
5. Copy the generated client secret into a text editor. The value will be hidden on return to this screen.

Step 3: Add API Permissions

Adding API permissions will allow applications to access the Sharepoint account on behalf of the signed-in user.

1. Select **API permissions** in the leftmost panel.
2. Select **Add a permission**.

3. Select **Microsoft Graph**.
4. Select **Application permissions**.
5. Select **Sites.ReadWrite.All** to give GoAnywhere MFT access to files that are accessible in Sharepoint Sites.
6. Select **Add permissions**.
7. After adding permissions, grant admin consent by clicking the checkmark above the permissions table. Make sure the **Sites.ReadWrite.All** shows a Status of "Granted".

+ Add a permission		✓ Grant admin consent for HelpSystems		
API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (1)				
Sites.ReadWrite.All	Application	Read and write items in all site collections	Yes	✓ Granted

Step 4: Identify the Tenant Name/Cloud Subdomain

The tenant name created in SharePoint will be used as the Cloud Subdomain later in the authentication process when adding a Cloud Connector Resource in GoAnywhere MFT. Use the Microsoft instructions at <https://o365hq.com/faq/how-to-find-your-office-365-tenant-name> to find your tenant name/Cloud Subdomain.

Step 5: Configure the Microsoft SharePoint Online Connector Resource

Follow the instructions on the Cloud Connector Resource topic to add a Microsoft SharePoint Online Connector.

On the Microsoft SharePoint Online Connector, specify the following fields:

- **Name** - A name for the Cloud Connector Resource.
- **Domain** - The domain identifies the primary location of your instance. For example, if you access your site with "https://example.companyname.com" then your domain would be "companyname.com".
- **Subdomain** - The location of your cloud instance. For example, if you access your site with 'https://example.sharepoint.com' then your subdomain would be 'example'. This will only be used if 'cloud' was selected for SharePoint Location.
- **Root Path** - The Root Path in SharePoint to use, sites or teams. **Default Value:** sites
- **Site** - The site in SharePoint to use.
- **Library** - The document library in SharePoint to use. The document library 'Shared Documents' will be used by default. Use the Microsoft instructions at <https://support.office.com/en-us/article/create-a-document-library-in-sharepoint-306728fe-0325-4b28-b60d-f902e1d75939> to create a new document library.
- **Tenant ID** - Your unique Azure Tenant ID.
- **Client ID** - The ID provided from the Microsoft Azure portal.
- **Client Secret** - The password provided from the Microsoft Azure portal.
- **User** - The user name of the SharePoint account to use during authentication.
- **Password** - The password of the SharePoint user.

NOTE:

Microsoft is deprecating Password based authentication. We recommend switching to OAuth Access Token based authentication to avoid any service interruption. Doing so will not require any changes to Projects that use this Resource.

Add Cloud Connector
✓ Save
🔍 Test
↺ Exit

Basic Proxy Contacts

Name *

SharePoint Online

Description

Cloud Connector

Microsoft SharePoint Online Connector

Domain

sharepoint.com

Subdomain *

mysubdomain

Root Path

sites

Site *

examplesite

Library

Shared Documents

Tenant ID

f4e13607-8639-4d26-82c0-3dc262e8c

Client ID

1e656907-4cce-502e-ba75-b8ae50a9i

Client Secret

Change Client Secret

User

Password

Okta API Token

Okta Base URL

Click the **Save** button to save the Microsoft SharePoint Online Connector.

Step 6: Configure the GoAnywhere Project

Microsoft SharePoint Online Connector actions are added to a Project like other file transfer tasks. Use the following instructions to use a Microsoft SharePoint Online Connector action in a Project workflow.

1. From within the Project Designer page, expand the **Cloud Connectors** folder in the **Component Library**, expand the **Microsoft SharePoint Online Connector** menu, and then drag the **Authenticate** action to the **Project Outline**.

2. On the Authenticate action, specify a value for the following fields:
 - **Microsoft SharePoint Online Connector Resource** - A pre-configured Microsoft SharePoint Online Connector Resource from the drop-down list.
 - **Access Token** - A Variable in which to store the Access Token.

The screenshot shows a project outline on the left with a tree structure: 'Example' (blue icon) containing 'Main' (red icon) which contains 'Authenticate' (green icon). The main panel is titled 'Microsoft SharePoint Online Connector - Authenticate' with an 'Edit' button. It contains the following fields:

Label	
Microsoft SharePoint Online Connector Resource	SharePoint Online
Output Variables	
Access Token	accessToken
Session ID	
Request Digest	
▶ Microsoft SharePoint Online Connector Resource	
▶ Comment	
▶ Control	
▶ On Error	

3. Specify any additional actions for the Project. In the following example, the List Directory action is used to pull a list of files and directories from a specified directory in a SharePoint library. For this action, the Microsoft SharePoint Online Connector Resource and Access Token variables are required as well as the name of the output variable that will contain the retrieved JSON data.

The screenshot shows the same project outline as before, but the 'List Directory' (green icon) action is now selected under 'Main'. The main panel is titled 'Microsoft SharePoint Online Connector - List Directory' with an 'Edit' button. It contains the following fields:

Label	
Microsoft SharePoint Online Connector Resource	SharePoint Online
Access Token	\${accessToken}
Session ID	
Request Digest	
Directory	/
Output Variables	
Results JSON *	results
▶ Microsoft SharePoint Online Connector Resource	
▶ Comment	
▶ Control	
▶ On Error	

4. Click the **Save** button when finished.

Using Okta to Authenticate

Use the following instructions to authenticate with SharePoint using an Okta API token and Base URL.

1. From within the Project Designer page, expand the **Cloud Connectors** folder in the **Component Library**, expand the **Microsoft SharePoint Online Connector** menu, and then drag the **Authenticate** action to the **Project Outline**.
2. On the **Authenticate** action, specify a value for the following fields:
 - **Microsoft SharePoint Online Connector Resource** - A pre-configured Microsoft SharePoint Online Connector Resource from the drop-down list.
 - **Session ID** - A Variable in which to store the session information.
 - **Request Digest** - A Variable that will contain the unique request digest value to authenticate subsequent requests.

The screenshot shows the 'Project Outline' on the left with a tree structure: 'Example' > 'Main' > 'Authenticate'. The main panel is titled 'Microsoft SharePoint Online Connector - Authenticate' and contains the following fields:

- Label**: An empty text box.
- Microsoft SharePoint Online Connector Resource**: A dropdown menu with 'SharePoint Online' selected.
- Output Variables**: A section header.
- Access Token**: A text box containing 'accessToken'.
- Session ID**: An empty text box.
- Request Digest**: An empty text box.
- Microsoft SharePoint Online Connector Resource**: A collapsed expandable section.
- Comment**: A collapsed expandable section.
- Control**: A collapsed expandable section.
- On Error**: A collapsed expandable section.

3. Expand the **Microsoft SharePoint > Basic** panel and specify the following fields:
 - **Okta API Token** - The API Token created for your organization. Visit <https://developer.okta.com/docs/guides/create-an-api-token/overview> for instructions on how to create an API token.
 - **Okta Base URL** - The base URL for the Okta authorization server. For single sign-on to Okta, the base URL is `https://{yourOktaDomain}/oauth2/`. For a Custom Authorization Server, the Base URL is `https://{yourOktaDomain}/oauth2/${authServerId}/`. For more information on the base URL, visit <https://developer.okta.com/docs/reference/api/oidc/#endpoints>.

The screenshot shows the configuration fields for the Okta API Token and Base URL:

- Okta API Token**: A text box containing '.0sdErHy9Jf1sijEGexYZlSdGr9a4QjKS' and a variable placeholder '\$ {var}'.
- Okta Base URL**: A text box containing 'https://myOktaDomain/oauth2'.

TIP:

The Okta API Token and Base URL can be specified on the Sharepoint Resource for reuse.