

Microsoft 365[®] Integration Instructions

SAFARI Montage[®] v6.5.28



Note: The Microsoft 365[®] Integration must be configured by an administrator

SAFARI Montage now offers a powerful new integration option that links directly with Microsoft's cloud-hosted Microsoft 365[®], OneDrive[®] for Business, and Azure[®] Active Directory[®], providing:

- Single Sign-On to SAFARI Montage
- Seamless access to Microsoft OneDrive and Microsoft 365 Apps from within SAFARI Montage
- Federated search of Microsoft OneDrive from within SAFARI Montage with one-click support to:
 - Upload files from Microsoft OneDrive to SAFARI Montage in any of 50+ supported file formats
 - Auto-convert Office[®] formats to universally accessible PDF formats
- Ability to save Microsoft OneDrive search results to the SAFARI Montage Learning Object Repository™ (LOR) as live web links, allowing continual collaboration
- **New in v7.3.41** – Ability to share content, playlists, and lessons from SAFARI Montage to Microsoft Teams

Requirements:

- SAFARI Montage v6.5.28 or greater for Single Sign On, OneDrive and Microsoft 365 Integration (excluding Teams)
- SAFARI Montage v7.3.41 or greater required for Teams Integration
- SAFARI Montage Interoperability Support Services
- SAFARI Montage server(s) must be publicly accessible and configured with an SSL certificate with a full Certificate Chain
- Microsoft 365 for Education Tenant

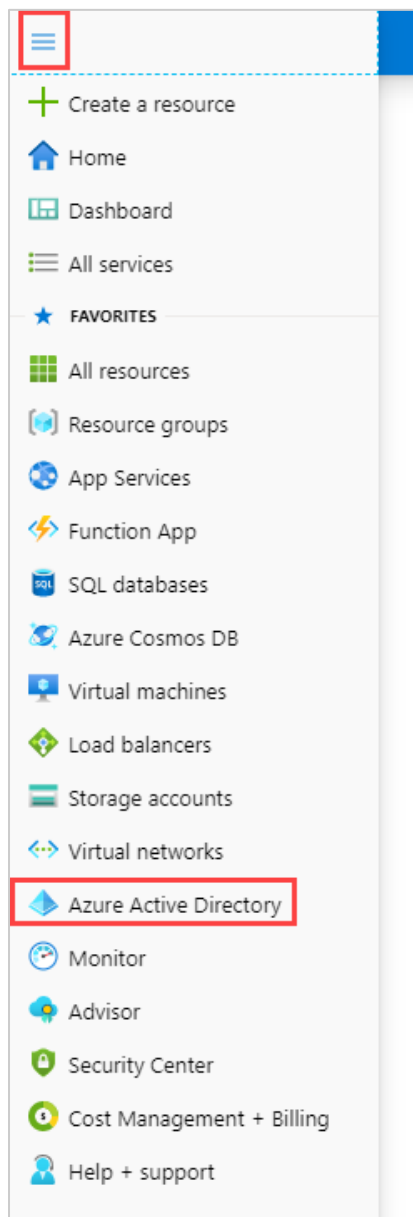
Note:

- Microsoft SSO, OneDrive, Microsoft 365, and Teams Integrations can be enabled independently of each other.
- SAFARI Montage remote servers must have the Microsoft Integration enabled locally.
- Contact SAFARI Montage Technical Support with questions pertaining to these instructions. SAFARI Montage Technical Support is available Monday - Friday from 8 a.m. to 6 p.m. Eastern Time, and they may be contacted by telephone at 800-782-7230 or online via <http://www.safarimontage.com/support>.

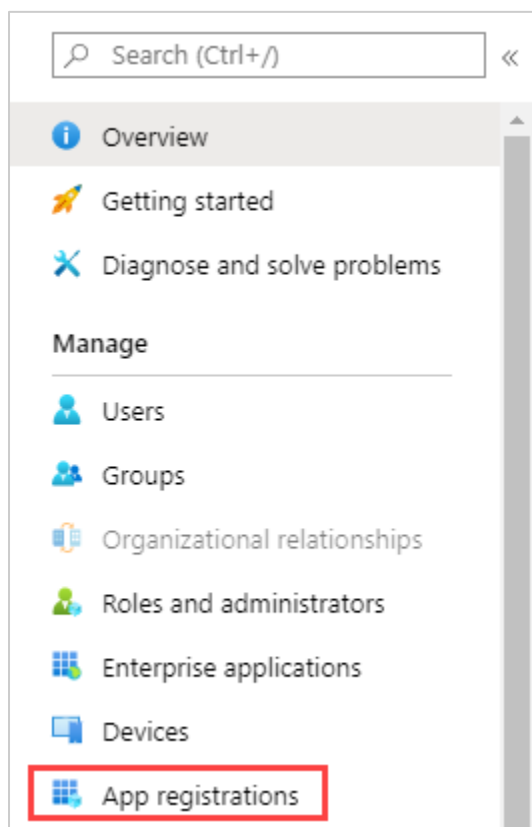
Microsoft Azure Configuration Instructions

Note: The Azure Portal has many configurations, and your screen may not match exactly what is shown here

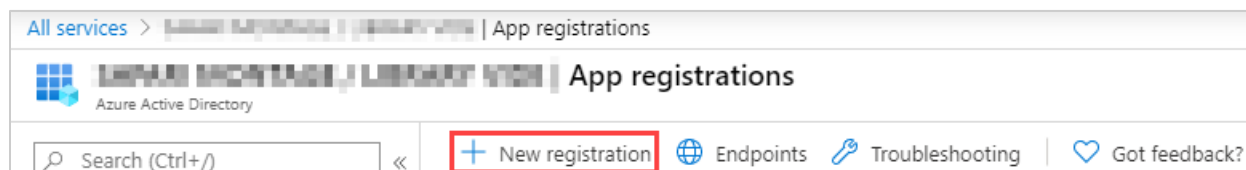
1. Log in to the Microsoft Azure portal at <https://portal.azure.com> as an administrator
2. From the **Dashboard** click the collapsed menu icon in the upper left corner of the screen and select **Azure Active Directory**



3. In the menu sidebar under **Manage** click **App registrations**



4. Add a new application:
 - a. Click **New registration** at the top of the page to add a new application



- b. Fill in the fields for the new registration
 - i. Enter a display name in the **Name** field, e.g., SAFARI Montage
 - ii. Most use cases will leave **Supported account types** as the default **Single tenant** option
 - iii. Select **Web** and enter the **Redirect URI**, replacing <YOUR SERVER> with the publicly accessible fully qualified domain name of your SAFARI Montage Server

https://<YOURSERVER>/SAFARI/montage/login/microsoft.php

- c. Click the **Register** button at the bottom of the page

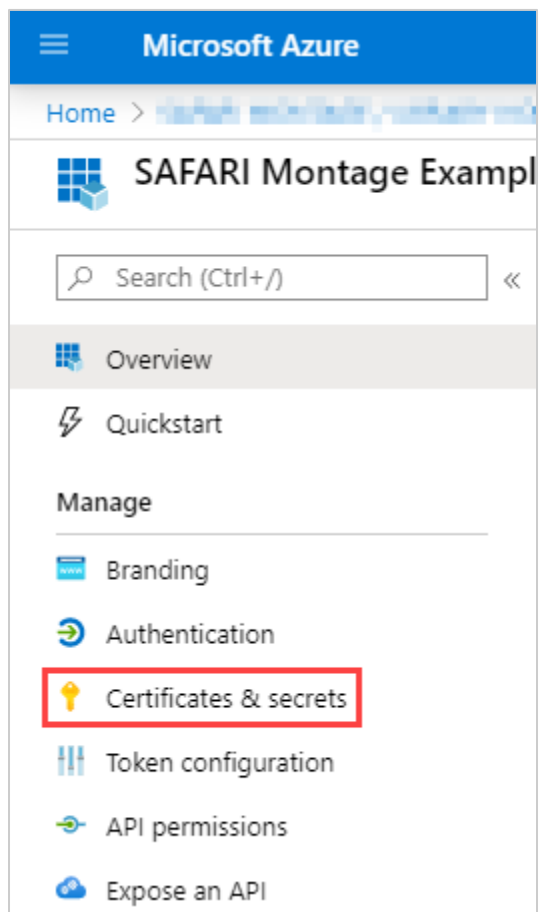
The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The 'Name' field is filled with 'SAFARI Montage Example Application'. Under 'Supported account types', the 'Single tenant' option is selected. Under 'Redirect URI (optional)', the 'Web' option is selected and the URI is 'https://smtraining.safarimontage.com/SAFARI/montage/login/mic...'. A red box highlights the 'Register' button at the bottom.

- 5. Copy/write down the **Application (client) ID** on the **Overview** page. This information will be used later when configuring the integration in SAFARI Montage

Application ID: _____

The screenshot shows the 'Overview' page for the application. The 'Application (client) ID' is highlighted with a red box.

6. Create the **Secret** for the application:
 - a. Under **Manage** select **Certificates & secrets**



- b. Under **Client secrets** click the **New client secret** button

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as applicatio

+ New client secret

Description	Expires	Value
Example Secret	Expires	Value

- Enter a name in the **Description** field, e.g., SAFARI Montage Secret
- Select an expiration date
Note: Consult your district policy regarding the appropriate expiration date for the client secret
- Click **Add**

Add a client secret

Description

SAFARI Montage Example Secret

Expires

In 1 year

In 2 years

Never

Add Cancel

- Copy/write down the **Secret** displayed under the **Value** column. This information will be used later when configuring the integration in SAFARI Montage.

Secret: _____

Expiration Date: _____

IMPORTANT: You will not be able to retrieve the Secret after you perform another operation or leave this blade. Make sure to copy the Secret before proceeding to the next steps.

i Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

Thumbprint	Start date	Expires
No certificates have been added for this application.		

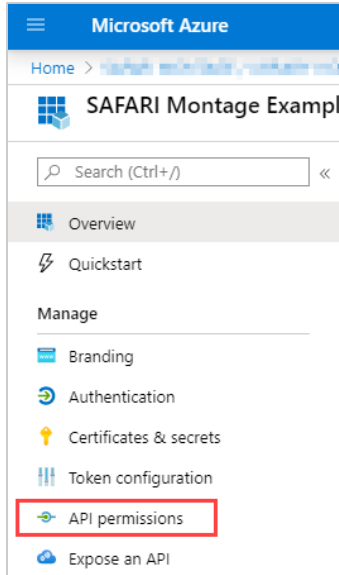
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value	
Secret	4/13/2021	[REDACTED]	
SAFARI Montage Example Secret	4/13/2021	[REDACTED]	

8. Configure the API Permissions:
 - a. Under **Manage** select **API Permissions**



- b. Under **API / Permissions name** click **Microsoft Graph**

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) Grant admin consent for SAFARI MONTAGE / LIBRARY VIDE

API / Permissions name	Type	Description	Admin consent req
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

- c. From the **Delegated Permissions** and **Application Permissions** selections, select the following permissions:

Note: User.Read is selected by default under Delegated

Type	Permission name	Description
Delegated	Files.Read	Read user files
Delegated	User.Read	Sign in and read user profile
Application	Directory.Read.All	Read directory data
Application	Group.Read.All	Read all groups

Request API permissions

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Files.Read ✓

Permission	Admin consent required
Files (1)	
<input checked="" type="checkbox"/> Files.Read Read user files ⓘ	-
<input type="checkbox"/> Files.Read.All Read all files that user can access ⓘ	-

- d. Click **Update permissions**

Update permissions Discard

9. Grant admin consent for this app:
 - Note:** You must be logged in as an administrator for this step
 - a. From the **API Permissions** page, click **Grant admin consent**

ons

Refresh

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission **Grant admin consent for SAFARI MONTAGE**

API / Permissions name	Type	Description	Admin consent req...	Status
------------------------	------	-------------	----------------------	--------

- b. Click **Yes** to grant consent for the requested permissions

ons

Refresh

Do you want to grant consent for the requested permissions for all accounts in SAFARI MONTAGE? This will update any existing admin consent records this application already has to match what is listed below.

Yes No

+ Add a permission Grant admin consent for SAFARI MONTAGE

API / Permissions name	Type	Description	Admin consent req...	Status
------------------------	------	-------------	----------------------	--------

- c. Verify that the permissions have been granted, as shown below

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

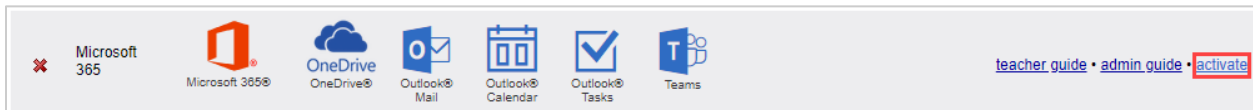
+ Add a permission ✓ Grant admin consent for SAFARI MONTAGE / SAFARI MONTAGE

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (4)				
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for SAFARI MO_ ...
Files.Read	Delegated	Read user files	-	✓ Granted for SAFARI MO_ ...
Group.Read.All	Application	Read all groups	Yes	✓ Granted for SAFARI MO_ ...
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for SAFARI MO_ ...

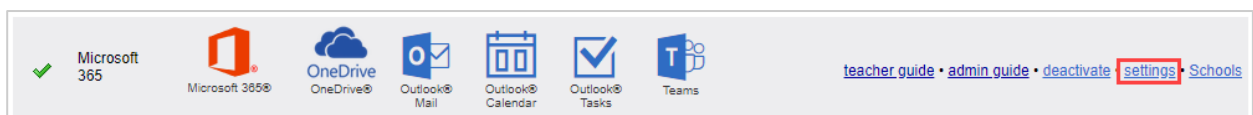
SAFARI Montage Configuration Instructions

1. Enable the Microsoft 365 Integration:

a. Navigate to **Admin > Interoperability Support > Services** and click on the **Activate** link



b. Click on the **Settings** link

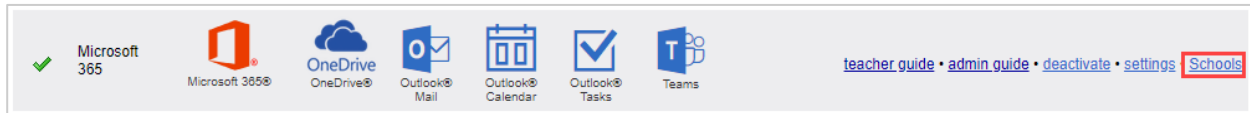


- i. Enable or disable **Microsoft 365**, **Microsoft OneDrive**, and **Microsoft SSO** per district preferences
- ii. Enter the **Application ID** in the **Client ID** field, and the **Secret** in the **Secret** field
- iii. Ensure that the **Hostname** field contains the publicly accessible fully qualified domain name of your SAFARI Montage server

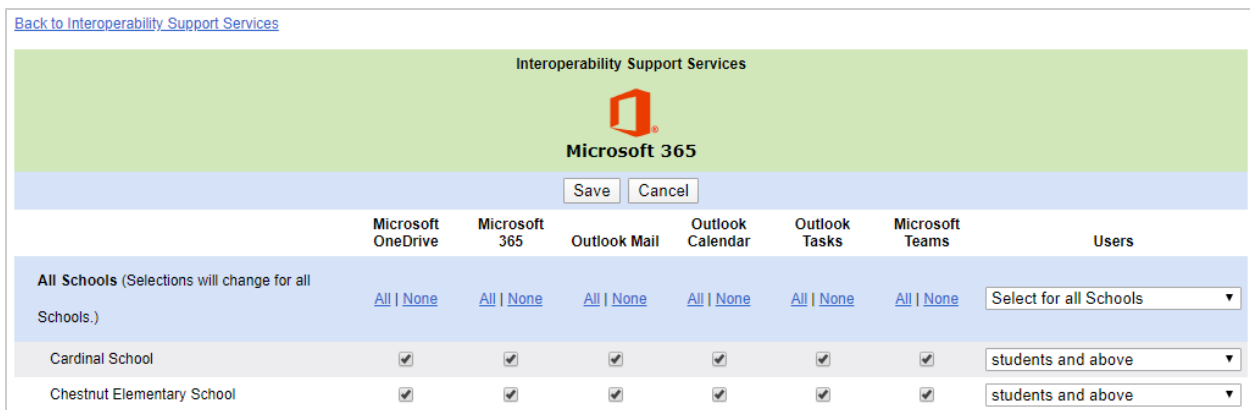
A screenshot of the 'Microsoft Settings' configuration form. At the top, there are links for 'Back to Services' and 'Create New Integration Profile'. The form has a green header 'Microsoft Settings'. It contains several fields: 'Microsoft 365:' with a checked checkbox, 'Microsoft OneDrive:' with a checked checkbox, 'Microsoft SSO:' with a checked checkbox, 'Client ID:' with a text input field containing a long alphanumeric string, 'Secret:' with a text input field containing a long alphanumeric string, 'Hostname:' with a text input field containing 'smtraining.safarimontage.com', and 'Microsoft Teams:' with a button labeled 'Azure AD Permissions'. At the bottom of the form are 'Save' and 'Reset' buttons.

- c. To authorize the **Microsoft Teams** integration, click the **Azure AD Permissions** button
Note: You must be logged in with an account that has administrator permissions within Azure for this step
 - i. Click the **Agree** button in the resulting window to grant consent
- d. Click on the **Save** button to save the configuration

2. Configure the Microsoft Integration for each School
 - a. After activation, administrators can configure which **Schools** and **User Types** will be able to access the integration by clicking on the **Admin > Interoperability Support > Services > Microsoft 365 > Schools** link



- b. Each School can be configured to enable or disable access to **Microsoft OneDrive**, **Microsoft 365**, **Outlook Mail**, **Outlook Calendar**, **Outlook Tasks** and **Microsoft Teams**, as well as restrict which user types are allowed access to the integration
 - c. Click on **Save** for the settings to take effect



Note: By default, Microsoft OneDrive, Microsoft 365, Mail, Calendar, and Tasks integration are enabled for Student and Teachers (and above)

Note: Microsoft OneDrive must be assigned to the school to enable the OneDrive search tab in the federated search for that school's users

Microsoft, Microsoft 365, the Microsoft 365 logo, OneDrive, the OneDrive logo, the Outlook Mail logo, the Outlook Calendar logo, the Outlook Tasks logo, Azure, Active Directory, Microsoft Teams, the Microsoft Teams logo and Microsoft Office are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.