

Microsoft Office365 (O365) API Integration Guide

A step-by-step guide to Securus360's Office365 Integration

Overview

The Securus360 Cyber SOC has the ability to collect log files from Office365. These logs empower Securus360 to monitor and alert on potentially suspicious activity happening in your Office365 environment. For this to work, you will need to configure a few things within your Azure/O365 tenant. This document will walk you through that process.

Please note: Auditing must be enabled for your organization to ensure data collection. For more Information, Click Here <https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-log-enable-disable?view=o365-worldwide>

Installation Steps

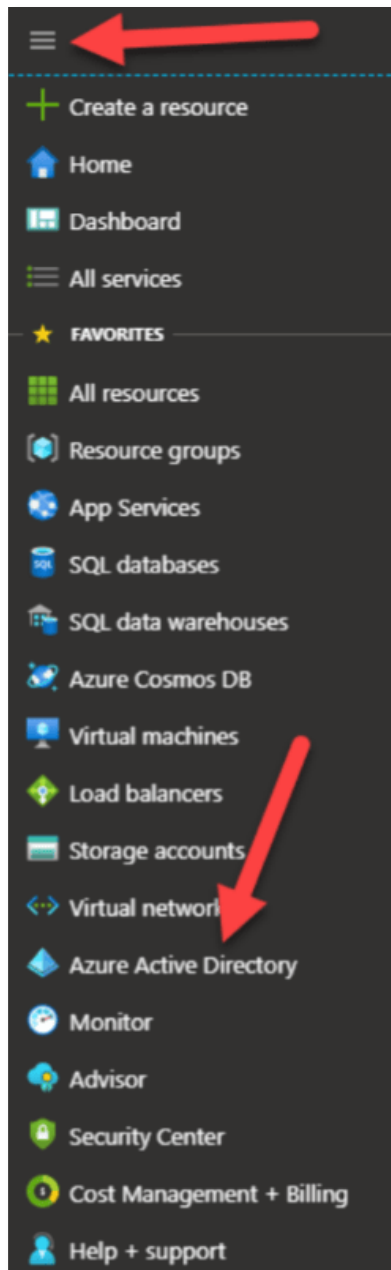
Installing the Office365 collection service is completed by Securus360, however you will need to make some configurations within your Office365 tenant first.

1. Configure the Azure Application

Log in to <https://portal.azure.com> using your Office365 Global Administrator credentials. (E.g. an account that is marked as Global Administrator.)

Microsoft Office365 (O365) API Integration Guide

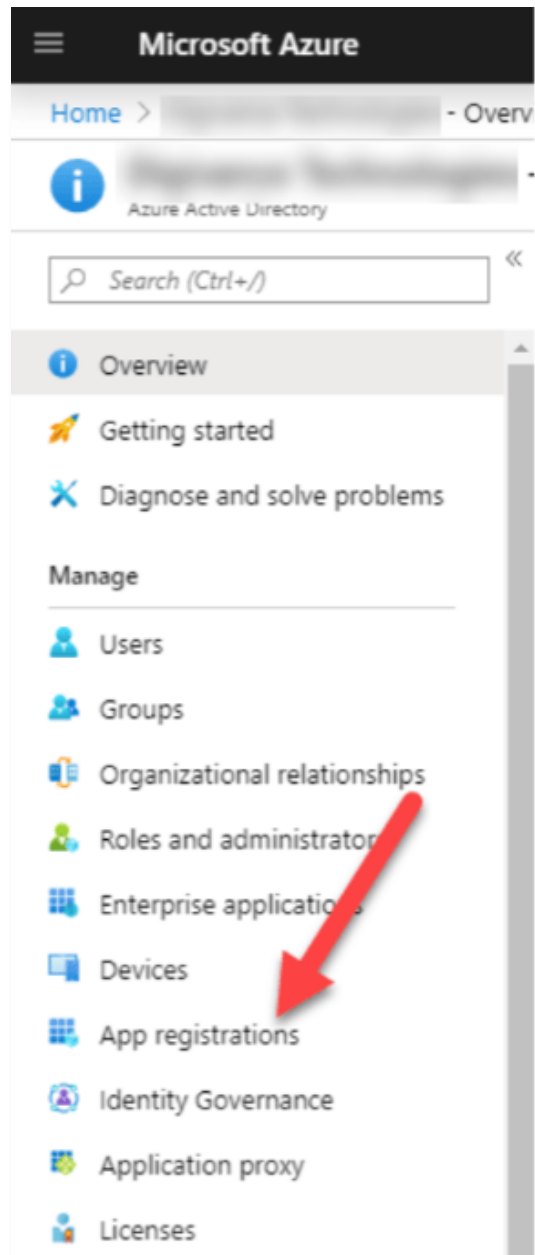
Once logged in, navigate to the **Azure Active Directory** option in the menu:



Note: You may have to click the three lines at the top to expand this menu.

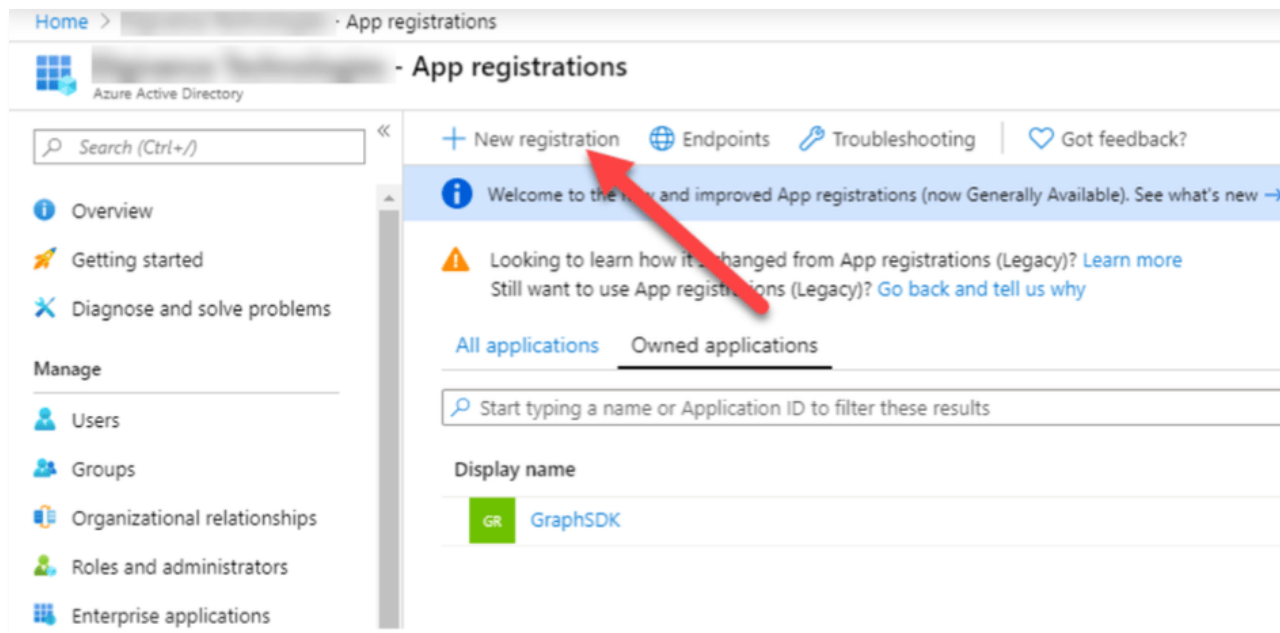
Microsoft Office365 (O365) API Integration Guide

Once you are in the **Azure Active Directory** system, you will need to create a new **App Registration**. To do this, navigate to the **App Registrations** option in the left-hand menu:



Microsoft Office365 (O365) API Integration Guide

Next, click **New registration** in the top menu:



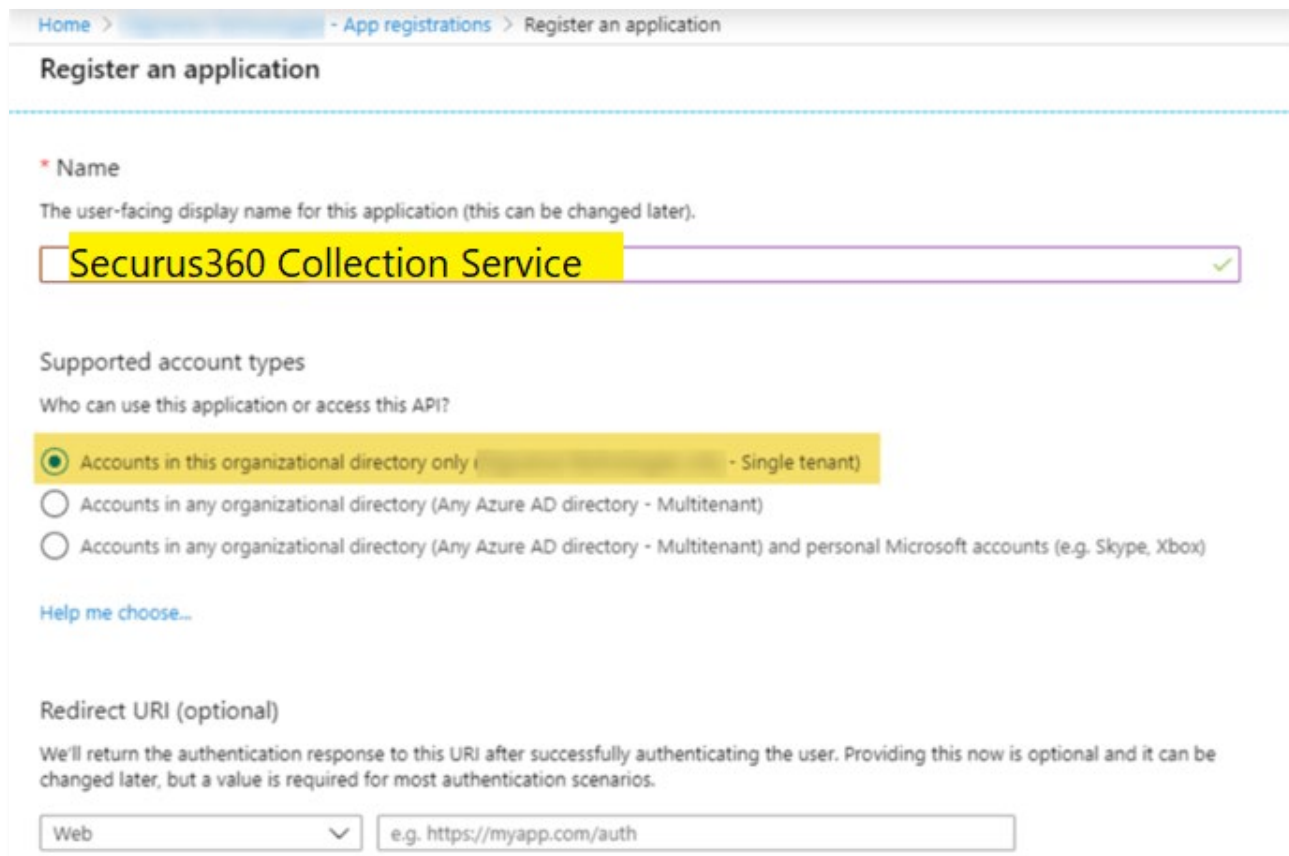
Microsoft Office365 (O365) API Integration Guide

Configure the options for this "App Registration" as shown below:

Name: Securus360 Collection Service

Supported account types: Accounts in this organizational directory only (Your tenant only - Single tenant)

Redirect URI: No value, not needed



Home > App registrations > Register an application

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (Any Azure AD directory - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

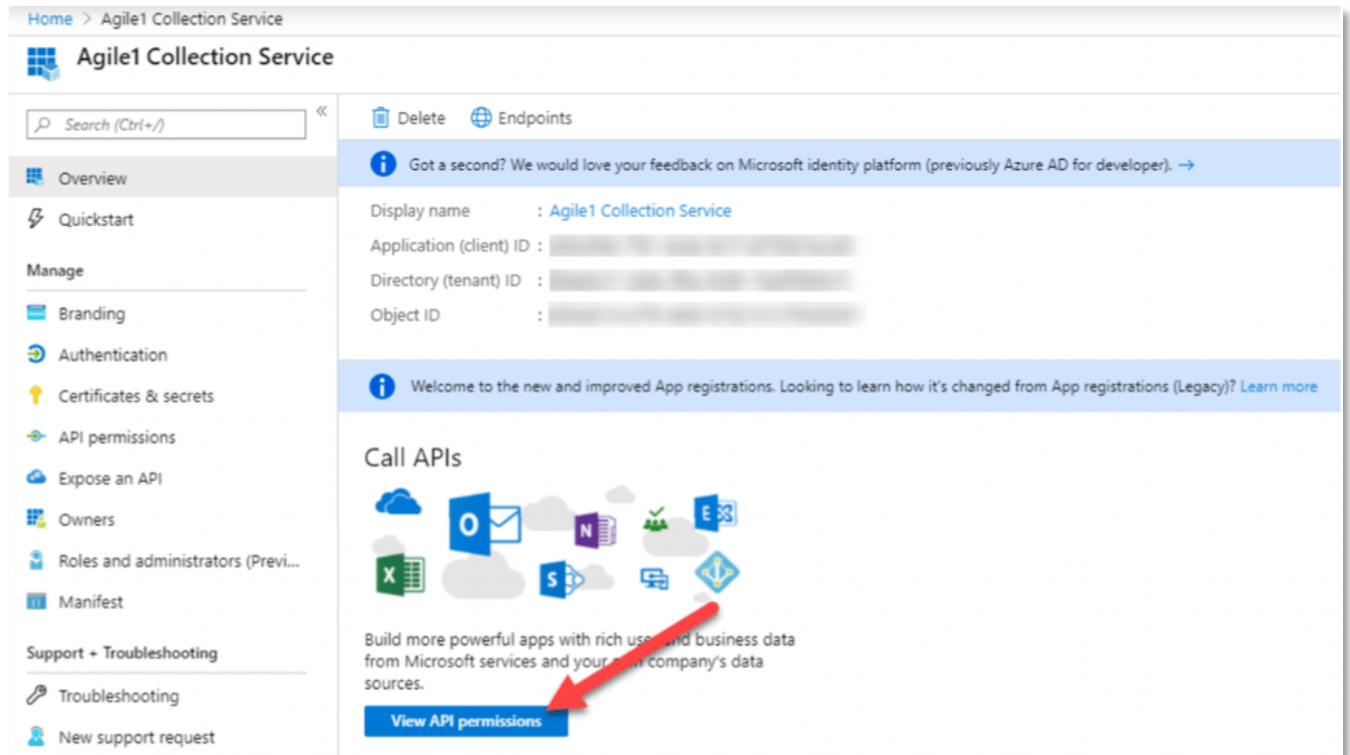
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Microsoft Office365 (O365) API Integration Guide

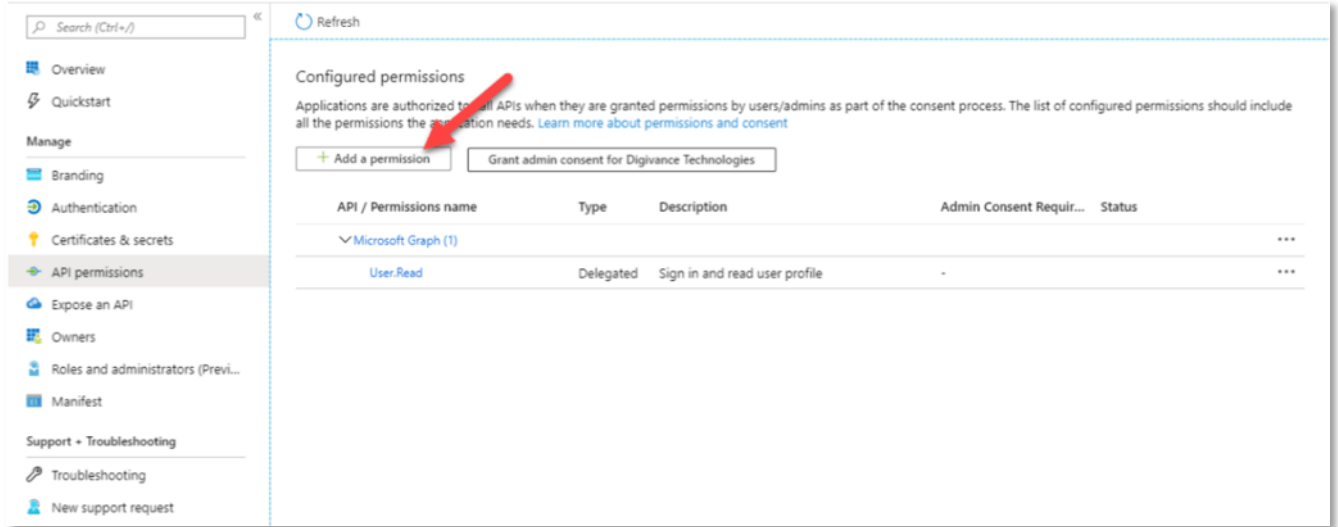
2. Configure permissions for your app registrations

Now that you have registered the Securus360 Collection Service application, you will need to give it permissions to your tenant. These permissions can be applied by selecting the **View API permissions** option:



Microsoft Office365 (O365) API Integration Guide

From the **API permissions** page, you can add necessary permissions. To do this, click on **Add a permission**. This expands a pop out on the right side of the screen.



The screenshot shows the 'API permissions' page in the Microsoft Azure portal. The left sidebar contains navigation options: Overview, Quickstart, Manage (Branding, Authentication, Certificates & secrets, API permissions, Expose an API, Owners, Roles and administrators (Previous), Manifest), Support + Troubleshooting (Troubleshooting, New support request). The main content area is titled 'Configured permissions' and includes a 'Refresh' button. Below the title is a paragraph explaining that applications are authorized to call APIs when granted permissions by users/admins. A red arrow points to the '+ Add a permission' button. To its right is a button for 'Grant admin consent for Digivance Technologies'. Below these buttons is a table of configured permissions:

API / Permissions name	Type	Description	Admin Consent Requir...	Status
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	...

Microsoft Office365 (O365) API Integration Guide

On the pop out, select **Office 365 Management APIs** then **Application permissions**

Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Dynamics 365 Business Central
Programmatic access to data and functionality in Dynamics 365 Business Central

Flow Service
Embed flow templates and manage flows

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

Request API permissions

< All APIs

Office 365 Management APIs
<https://manage.office.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.

Microsoft Office365 (O365) API Integration Guide

Under Office365 Application APIs Application permissions, expand and check the following options, then click **Add permissions** at the bottom of the pop out to save your changes.

Request API permissions

< All APIs

Office 365 Management APIs
<https://manage.office.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

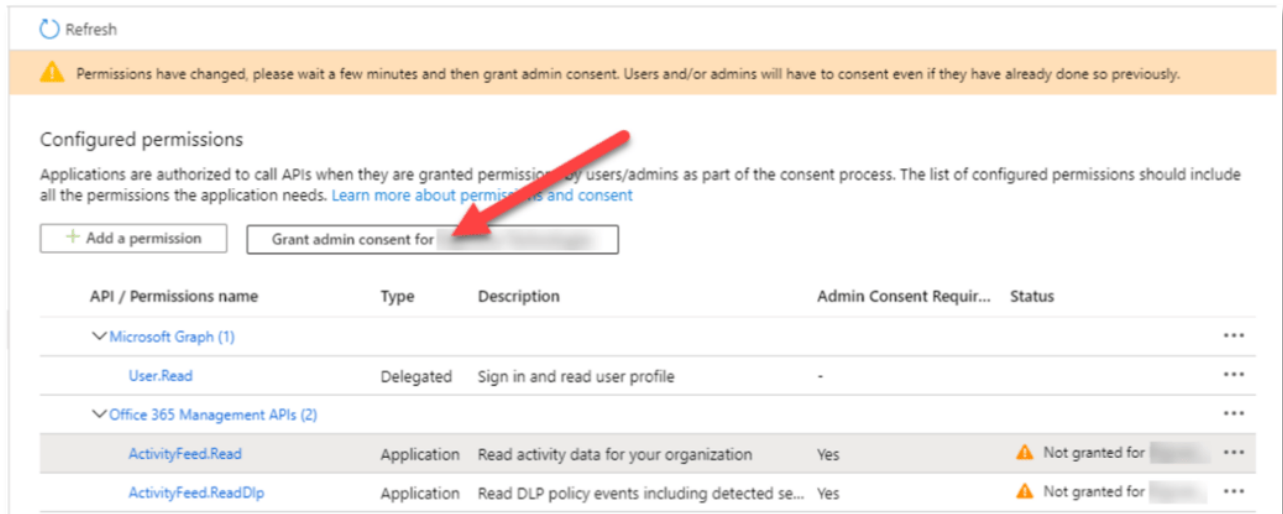
Type to search

Permission	Admin Consent Required
ActivityFeed (2)	
<input checked="" type="checkbox"/> ActivityFeed.Read Read activity data for your organization	Yes
<input checked="" type="checkbox"/> ActivityFeed.ReadDlp Read DLP policy events including detected sensitive data	Yes
> ActivityReports	
> ServiceHealth	
> ThreatIntelligence	

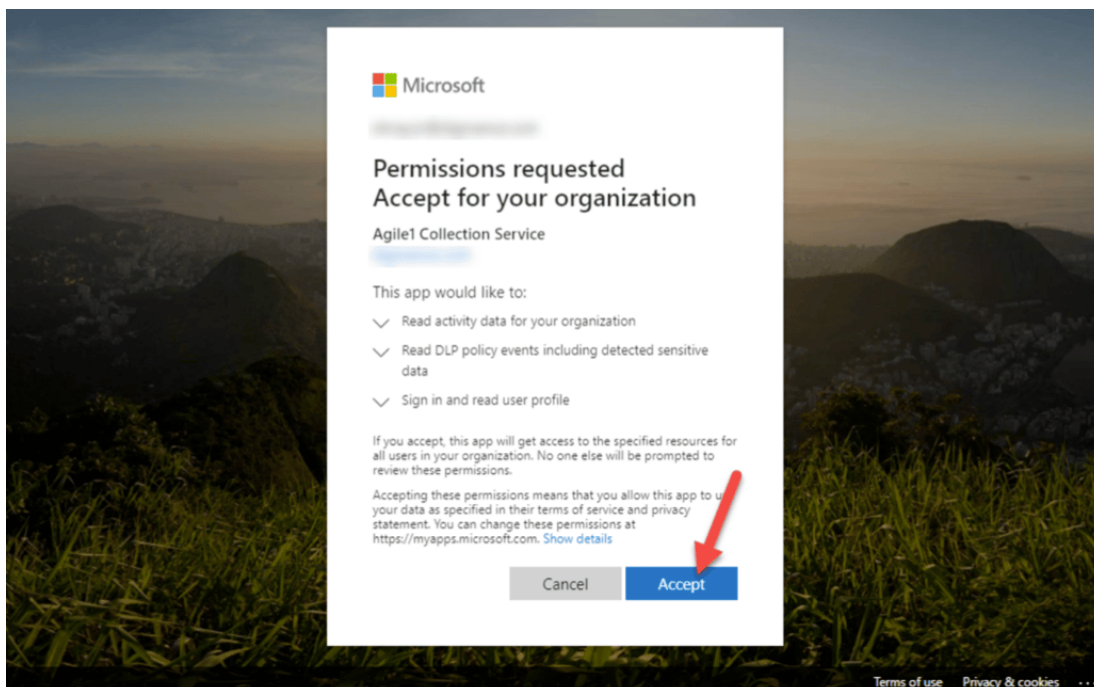
Add permissions Discard

Microsoft Office365 (O365) API Integration Guide

Now that your permissions are configured, you will need to grant administrative consent. To do this, click **Grant admin consent for [your tenant name]**.



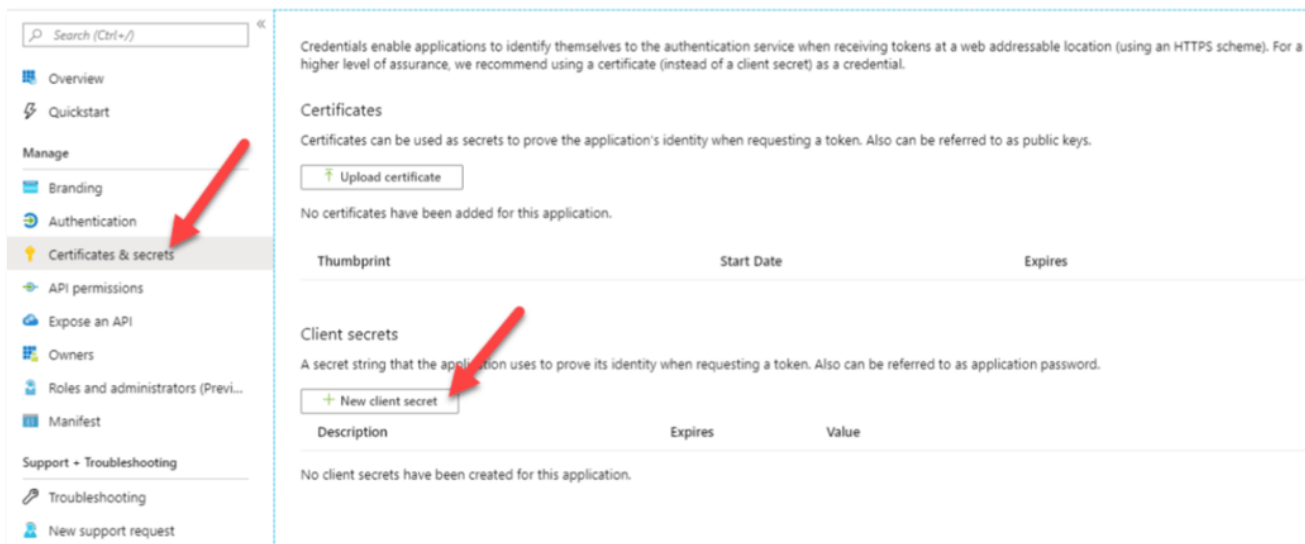
Note: To provide consent, you will be asked to sign in again. Make sure you are using the same credentials you first used to sign in as you will need Global Admin privileges to assign consent. Click **Accept** when asked to allow the permissions previously set.



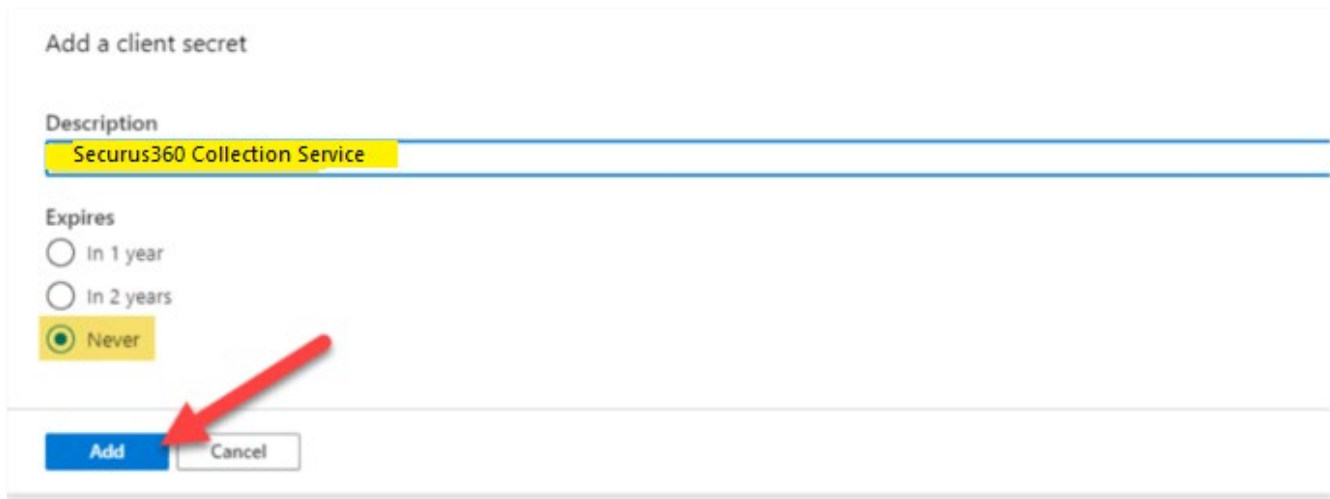
Microsoft Office365 (O365) API Integration Guide

3. Create client secret keys & collect necessary IDs

The next step is to create a client secret key and collect the IDs that Securus360 needs to collect logs from your Office365/Azure services. To do this, select **Certificates & secrets** from the left-hand menu. Once the page loads, click **New client secret**:



5
On the pop out that appears, provide a **Description** of **Securus360 Collection Service** and select **Never** for expiration, then click **Add**.



Microsoft Office365 (O365) API Integration Guide

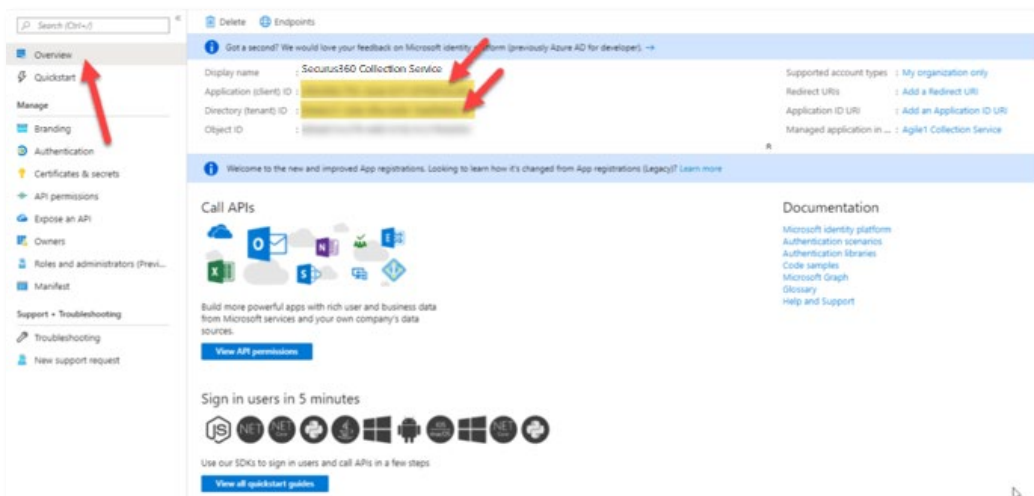
CAUTION! Depending on your version of Azure/Office365 and/or your security configurations, you may only have ONE CHANCE to grab this value. Be sure to copy this value and store it somewhere safe immediately!

Collect the **value** of the client secret that you created. To do this, copy and paste the value into a secure location.



Note: We masked the value in this example, but it should look something like `ifr=j8GjN_JZ/wqCN]sQXFTUrVcPU827`

Now that you have the client secret value ready, you will need to collect your **Application (client) ID** and **Directory (tenant) ID** values. To get these, navigate back to the **Overview** page and copy them from the top portion of the page.



Microsoft Office365 (O365) API Integration Guide

Note: We mask the values in this example. They should look like:

- **Application (client) ID:** a8967919-b638-4aa5-acc-afc28bfedb3b
- **Directory (tenant) ID:** ce58a858-12c6-4de5-9620-2a6b24a71ad4

4. Submitting Sensitive Data

The final step is to submit these sensitive details to Securus360.

To ensure the secure transfer of sensitive information beyond basic email security measures, Securus360 will provide you with a link to a Sharepoint folder that's unique to your site, and is accessible only to you and Securus360.

Please create a text file which includes the following values:

- a) Secret Value
- b) Application (client) ID
- c) Directory (tenant) ID
- d) Tenant Name (Ex. securus360.onmicrosoft.com)

Example:

- a) Secret Value - ifr=j8GjN_JZ/wqCN]sQXFTUrVcPU827
- b) Application (client) ID - a8967919-b638-4aa5-acc-afc28bfedb3b
- c) Directory (tenant) ID - ce58a858-12c6-4de5-9620-2a6b24a71ad4
- d) Tenant Name - securus360.onmicrosoft.com

Note: If you wish to secure this even further, such as encrypting the text file with 7-Zip, please provide Securus360 with the password to decrypt/extract the archive.

Once complete, please upload the file containing these values to the Sharepoint link provided by Securus360. Then send an email to support@securus360.com to let us know that it has been successfully uploaded. Securus360 will confirm we have received the file as quickly as possible. After we confirm receipt, you can then opt to securely delete the file from wherever it was saved locally, such as an internal disk or a flash drive.

If you have any questions or concerns regarding this procedure, please reach out to either your preferred contact or to support@securus360.com

Lastly, if you would prefer a different method of sending us this information, Securus360 is more than willing to accommodate whichever method adheres to your preferences and security policies.