Microsoft Office 365 connector

Summary

Connects to an Office 365 application in InTune and pulls in inventory and usage data.This configuration procedure assumes you already have an InTune and Microsoft Office 365 subscription, and you are able to populate the connector with information that is available in an Enterprise Application in your AAD Console.

On this page:

Prerequisites

Before adding a new Office 365 connector, you will to complete the following steps described below:

- Enable PowerShell to connect to Azure via MSOL
- Prepare an AAD application
- Add permissions
- Add a client secret
- Add a user with the necessary permissions to run the PowerShell scripts

You will need the following information from an Enterprise Application created in your AAD console:

- Azure cloud instance URL (optional) if this is not supplied then **AzurePublic** is used as a default
- Azure tenant ID, available in the **Overview** node of your AAD console
- The registered application clientID (a string representing a GUID)
- A client secret value that has been created for your chosen Enterprise Application.
- SingleSignIn enabled Service Account with global reader permissions for running PowerShell cmdlets.

Enable PowerShell to connect to Azure via MSOL

On the Tachyon server where the Office 365 connector will be executed, PowerShell needs to connect to Azure via MSOL, which requires the following two modules to be installed:

```
Install-Module -Name AzureAD
Install-Module -Name MsOnline
```

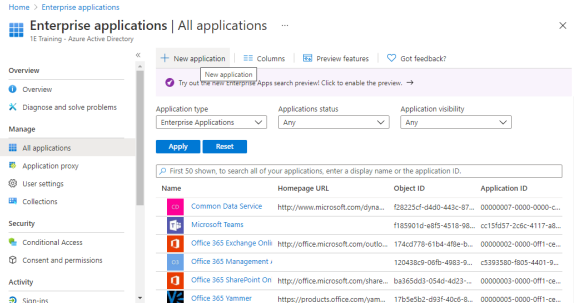
If the following warnings are shown when installing a module, you will need to run the below command first.

WARNING: Unable to download from URI 'https://go.microsoft.com/fwlink/?LinkID=627338&clcid=0x409' to ''.
WARNING: Unable to download the list of available providers. Check your internet connection.

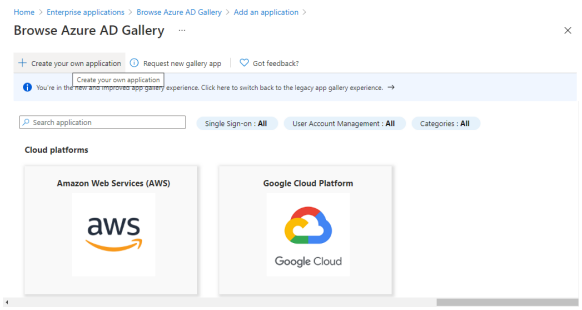
```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Prepare an AAD application

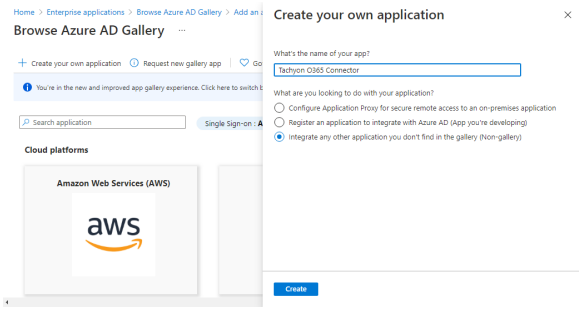
In your Azure Active Directory console, go to the **Enterprise applications** node and click **New application**.



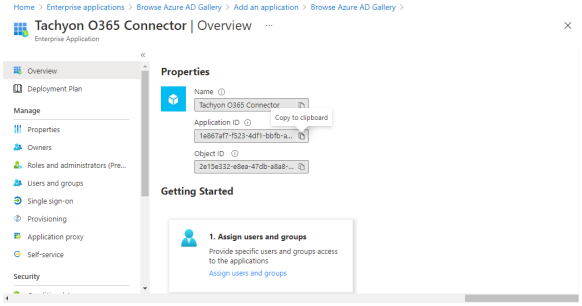
You need to create a non-gallery application, in the version of AAD we're using this is done by clicking the **Create your own application** button.



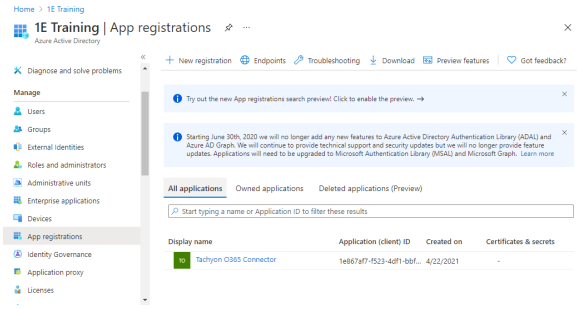
Provide a name for the application. The name of application is not significant however it should be such that it suggests that the application is related to the Office 365 connector, for example: **Tachyon O365 Connector**. In this version of AAD we ensure that the **Integrate any other application you don't find in the gallery (Non-gallery)** option is selected and then click **Create** in the bottom left of the panel.



In the **Overview** tab for the new application, copy the **Application ID** value as this will be required for the connector.



Navigate back to the AAD blade then click the **App registrations** node of AAD.



> ⚠ You may need to change the tab to **All Applications** to see the new application.

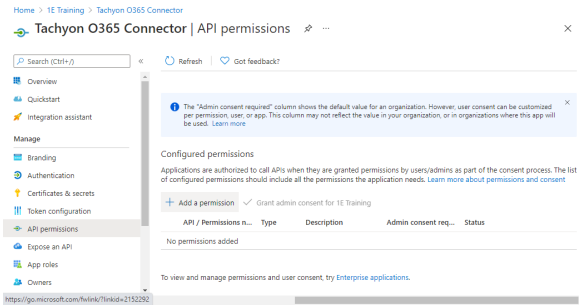
Click on the application name for the new application.

Add permissions

Click on the **API permissions** node under the **Manage** section, then click **Add a permission** .

Click on the **Microsoft Graph** tile and then click on **Application permissions**.

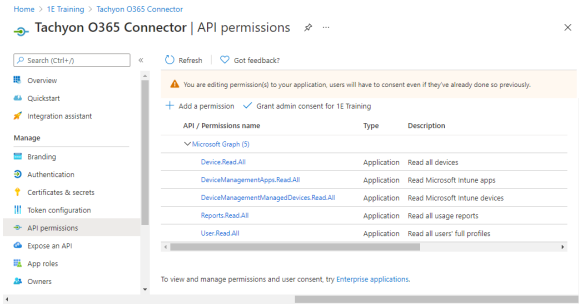
A long list of API permissions will be shown, scroll through them and check as appropriate using the following table.



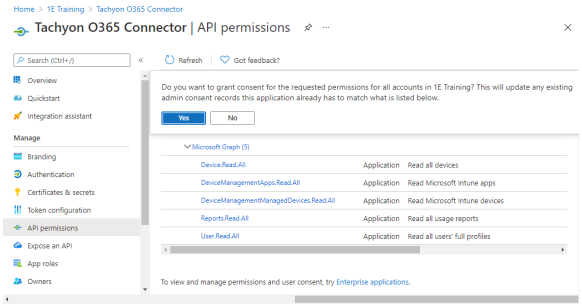
Group	Permission
Device	Read.All
DeviceManagementApps	Read.All
DeviceManagementManagedDevices	Read.All
Reports	Read.All
User	Read.All

When the correct permissions have been selected, click **Add permissions** .

After they've been added the permissions should like the picture shown opposite.



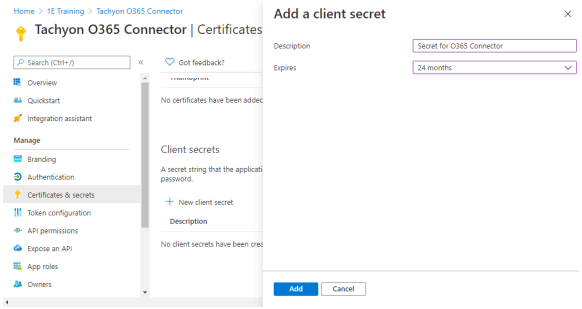
Click **Grant admin consent for <organization>**, where <organization> is the **Organization** you set when your InTune instance was created. Thi s means that as an administrator for your organization, you're consenting that the users of the application can use these permissions. Click **Yes** to confirm.



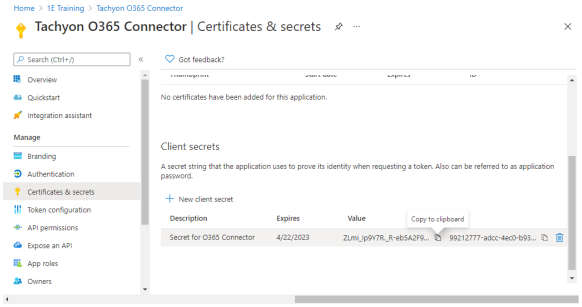
Add a client secret

Click on the **Certificates & secrets** node and then click on **New client secret** button

The **Add a client secret** form will open, add a **description** and select an expiry from the **Expires** radio buttons and then click **Add**.



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



Add a user with the necessary permissions to run the PowerShell scripts

An AAD user with global Reports Reader permissions must be made available in your organization's blade. The credentials for this user will be set in the Microsoft Office 365 connector when it is created in Tachyon.

Configuring the Office 365 connector

These instructions show how to create an Office 365 connector in the Tachyon Settings application.

Adding, testing and running an Office 365 connector

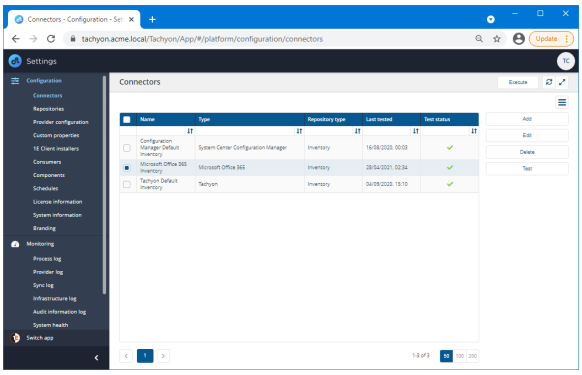
These are the steps to add, test and run an Office 365 connector

Adding an Office 365 connector

1. In the Tachyon portal, navigate to **SettingsConfigurationConnectors**.
2. Click on the **Add** button.

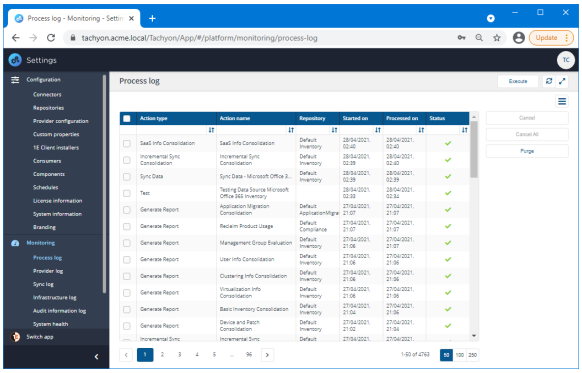
3. In the **Add connector** popup select the **Intune** type.
4. In **Connector name**, enter a logical name for this connector. In our example we choose the name **Microsoft Office 365 Inventory** .
5. **Azure Cloud Instance** can be set to the URL for your InTune implementation. If you leave this field blank **AzurePublic** is used as a default.
6. In Azure **Tenant Id**, enter your Azure tenant ID, available in the **Overview** node of your AAD console
7. **Client Id** this should be set to your registered application clientID.
8. **Client Secret** this should be set to the specific client secret value that has been created for your chosen Enterprise Application
9. **Login Email** - set this to the permissioned user.
10. **Login Password** - set this to the password for the permissioned user.
11. Click **Add**.

The new connector has now been added and a new action that can be used to run the connector has been created in the background, called **Sync Data - Microsoft Office 365 Inventory**.



Testing an Office 365 connector

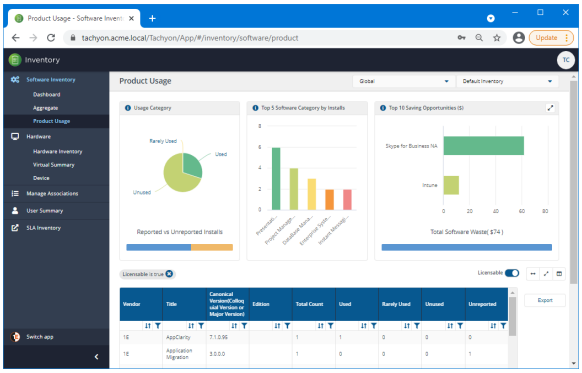
1. Select the Office 365 connector by checking the box at the left-hand end of its entry in the **Connectors** table.
2. Click the **Test** button.
    a. The **Test status** column for the connector will display a clock icon indicating that the test has been queued for executing.
    b. If the test succeeds **Test status** will display a check icon, and the **Last tested** column will display the date and time the test succeeded.
    c. If the test fails the **Test status** will display a failed icon, and you'll need to check the details you entered for the connector.
3. If the test succeeds you can proceed to run the connector to populate an inventory repository.



Running an Office 365 connector

1. Click the **Execute** button.
2. In the **Execute action** popup subsequently displayed, use the **Repository** menu to select the inventory repository you want to populate.
3. Once the repository has been selected you can then select the action to run. In the case of inventory repositories the actions will be restricted to inventory related actions. For a connector you will be looking for an action with the form **Sync Data - <connector name>**.
4. Select whether you want to clear any existing data in the repository by checking the **Clean sync** checkbox.
5. Click **Execute** button in the **Execute action** popup to start the sync.
6. When the sync starts a number of actions are queued to be performed on the selected repository. To check the progress of the sync actions:
    a. Navigate to the **MonitoringProcess log** page.
    b. Here you can see the sequence of actions that have been queued for the selected repository related to the **Sync Data** action selected.
    c. When each action has finished running you'll see a check icon appear in the **Status** column if it succeeds or a failed icon if it fails.

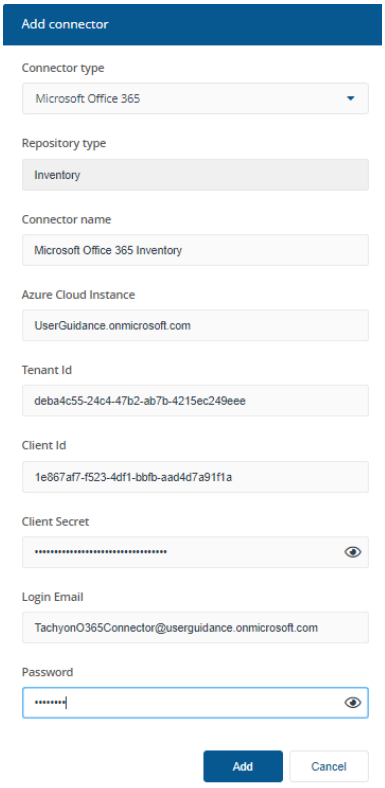
Viewing the Office 365 information in the Inventory application



1. Use the **Switch app** menu to open the **Inventory** application.
2. Navigate to **Software InventoryProduct Usage** page.
3. On this page you should see software items that are coming from your AAD environment.

The Office 365 connector parameters

The following fields are available in the **Add connector** and **Edit connector** popups when the **Microsoft Office 365 Connector type** is selected, as shown in the picture opposite:



Field	Description
Connector type	Shows the connector type: **Microsoft Office 365**.
Repository type	Shows which type of repository the connector works with. For the **Microsoft Office 365 Connector type** this is always **Inventory**.
Connector name	Here you set the logical name for the connector. You should use a naming convention for connector names: <connector type> <scope> <RCR> **Scope** describes where data is coming from or what it's being used for. For example Demo, Test, Lab, Q2 Audit. Include **RCR** in the name if you have enabled **Run Consolidation Reports**.
Azure Cloud Instance	Azure cloud instance URL (optional) if this is not supplied the **AzurePublic** is used as a default.
Tenant Id	Azure tenant ID, available in the **Overview** node of your AAD console.
Client Id	The registered application clientID.
Client Secret	A client secret value that has been created for your chosen Enterprise Application.
Login Email	The user login name for the permissioned user.
Password	The password for the permissioned user.
Run Consolidation Reports	Check the **Run Consolidation Reports** checkbox if you want consolidation actions to be processed each time the **Sync Data** action is executed for the connector. This can lead to unnecessary processing if you enable this on more than one connector. The recommended method of processing consolidation actions is to schedule the action **Generate Report - Basic Inventory Consolidation** to execute after the **Sync Data** actions have run for all connectors. This will execute the remaining consolidation actions. Alternatively check the **Run Consolidation Reports** checkbox on one of your connectors. You can view action processes in **SettingsProcess log**.