

## Integrating a multi-tenant Microsoft Defender application

<https://campus.barracuda.com/doc/98224023/>

Follow this procedure to create a multi-tenant application. To create a single-tenant application, see [Integrating a single-tenant Microsoft Defender application](#).

The steps to integrate a multi-tenant Microsoft Defender application are the following:

- Create a multi-tenant application in Azure
- Authorize the MSP Application in each tenant
- Integrate the application with Barracuda XDR

See the procedures below.

### Step One: Create a multi-tenant application in Azure

The following are instructions for creating a multi-tenant application in Azure.


#### To create a multi-tenant application in Azure

The MSP must have a Microsoft Defender for Endpoint subscription.

1. Log in to [Azure](#) with a user that has the **Global Administrator** role.  
The User you use to log in must be the MSP's tenant and not one of the accounts you intend to manage.


2. Navigate to **Azure Active Directory > App registrations > New registration**.


[Home](#) > [MyMsp](#) > [MyMspApplication](#)

 **MyMspApplication** | API permissions ✕ ...


 Refresh |  Got feedback?


 Overview


 Quickstart


 Integration assistant


Manage

 Branding & properties

 Authentication

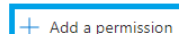

 Certificates & secrets

 Token configuration

 API permissions

#### Configured permissions

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

 Add a permission  Grant admin consent for MyMsp

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

3. On the registration form, write a name for your application, and select **Multi-tenant**.

4. In the **Redirect URI (optional)** section, choose **Web** and type a redirect URI (<https://portal.azure.com>).

[Home](#) > [MyMsp](#) >

## Register an application ...

### \* Name

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

MyMspApplication

### Supported account types

Who can use this application or access this API?

- ☐ Accounts in this organizational directory only (MyMsp only - 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)
- ☐ Personal Microsoft accounts only

[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.

Web

<https://portal.azure.com>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

5. Click **Register**.
6. On your application page, click **API Permissions**.
7. Click **Add permission**.

[Home](#) > [MyMsp](#) > [MyMspApplication](#)

## MyMspApplication | API permissions

Search (Ctrl+/)

Refresh | Got feedback?

Overview

Quickstart

Integration assistant

### Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

### Configured permissions

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

+ Add a permission

Grant admin consent for MyMsp

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

8. Click **APIs my organization uses**. Then type WindowsDefenderATP. Then select **WindowsDefenderATP**.

## Request API permissions




Select an API

 Microsoft APIs   **APIs my organization uses**   My APIs

Apps in your directory that expose APIs are shown below

<input type="text" value="WindowsDefenderATP"/>
Name
WindowsDefenderATP
Application (client) ID
fc780465-2017-40d4-a0c5-307022471b92

9. Click **Application permissions**. Then click **Alert**.
10. Select **Alert.Read.All**. Then click **Add permissions**.

[All APIs](#)

 WindowsDefenderATP  
<https://userrequestsgraphapieprd.trafficmanager.net/>

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](#)

Start typing a permission to filter these results

Permission

Admin consent required

>

AdvancedQuery

▼

Alert (1)

☒

Alert.Read.All ⓘ

Read all alerts

Yes

☐

Alert.ReadWrite.All ⓘ

Read and write all alerts

Yes

[Add permissions](#)
[Discard](#)

11. Select the **Application permission** and click **Grant admin consent**.

[Home](#) > [MyMsp](#) > [MyMspApplication](#)

MyMspApplication | API permissions

[Refresh](#)
[Got feedback?](#)

⚠ You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

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 MyMap](#)

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (1)				...
User.Read	Delegated	Sign in and read user profile	No	...
▼ WindowsDefenderATP (1)				...
Alert.Read.All	Application	Read all alerts	Yes	⚠ Not granted for MyMsp

12. Click **Yes**.

Grant admin consent confirmation.

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

[Yes](#)
[No](#)

13. To add a secret to the application, select **Certificates & secrets**, add a description to the secret.

[Home](#) > [MyMsp](#) > [MyMspApplication](#)

## MyMspApplication | Certificates & secrets

[Got feedback?](#)

Credentials enable confidential applications to identify themselves to the authentication scheme). For a higher level of assurance, we recommend using a certificate (instead of :

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token.

[+ New client secret](#)

Description	Expires	Value ⓘ
No client secrets have been created for this application.		

14. Click **Add**.

### Add a client secret

Description

MyMspSecret

Expires

24 months

Add

Cancel


15. Copy the generated **MSP Secret Key** value.

Make sure you save the **MSP Secret Key**. You won't be able to retrieve this value after you leave.

16. Click **Overview**

17. Copy the **MSP Client ID (Application ID)**.

[Home](#) > [MyMsp](#) > [MyMspApplication](#)

 MyMspApplication | Certificates & secrets

[Got feedback?](#)

**Got a second to give us some feedback? →**

Credentials enable confidential 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 (0) **Client secrets (1)** Federated credentials (0)

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 ID
MyMspSecret	6/22/2024	<b>LOGIb~svWtkmLOGIb~LOGIbGo0bz88Q...</b>	c6aa79ab-4939-49e3-a1d1-53cbc8fc352a

## Step Two: Authorize the MSP Application in each tenant

Because your application interacts with Defender for Endpoint, the next step is to request that an

Admin user each tenant approve the MSP Client ID from the previous procedure.

The Admin user must:

- Be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.
  - Sign in using multi-factor authentication.
1. Send an email to each Admin you want to approve the application. The email must contain the following for approval: `https://login.microsoftonline.com/common/oauth2/authorize?prompt=consent&client_id=<00000000-0000-0000-0000-000000000000>&response_type=code&sso_reload=true`, where `<00000000-0000-0000-0000-000000000000>` is the MSP Client ID you copied from the previous procedure.
  2. Each user that authorizes the MSP Client ID, they must log in to Azure AD and retrieve the **Tenant ID** from the Overview page.

### Step Three: Integrate the application with Barracuda XDR

---

When you've finished the procedure above, complete the integration by entering the Client ID, Secret Key, and Tenant ID in the Barracuda XDR Customer Security Dashboard.

#### To integrate the application with Barracuda XDR Dashboard

1. In the **Account** list, select the name of the company you created in the previous procedure.
2. In **Barracuda XDR Dashboard**, click to **Administration > Integrations**.
3. In the **Microsoft Defender** card, click **Setup**.
4. Enter the **Client ID**, **Secret Key**, and **Tenant ID**.

**Integration: Microsoft Defender for Endpoint** [Help](#)

[Setup Instructions](#)

☒ Enabled

Client ID  
 ✓

Secret Key  
 ✓

Tenant ID  
 ✓

**Test Log:**

2022-06-22T21:47:06	Starting Microsoft Defender for Endpoint test...
2022-06-22T21:47:06	Performing Authorization request...
2022-06-22T21:47:06	Successfully Authorized.
2022-06-22T21:47:06	Performing API request...
2022-06-22T21:47:07	API request succeeded! No alerts have been generated.

Successful test. Remember to save your settings!

5. Click **Save**.

## Figures

1. microsoft.multitenant.permissions1.png
2. microsoft.multitenant.register2.png
3. microsoft.multitenant.permissions1.png
4. microsoft.multitenant.permissions2.png
5. microsoft.multitenant.permissions3.png
6. microsoft.multitenant.grantconsent1.png
7. microsoft.multitenant.grantconsent2.png
8. microsoft.multitenant.secret1.png
9. microsoft.multitenant.secret2.png
10. microsoft.multitenant.secret3.png
11. microsoft.multitenant.save2.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.