

Integrating a single-tenant Microsoft Defender application

<https://campus.barracuda.com/doc/98224018/>

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

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

- Create a single-tenant application in Azure
- Integrate the application with Barracuda XDR

See the procedures below.

Creating a single-tenant application in Azure

Follow this procedure to create a single-tenant application or see below to create a multi-tenant application.

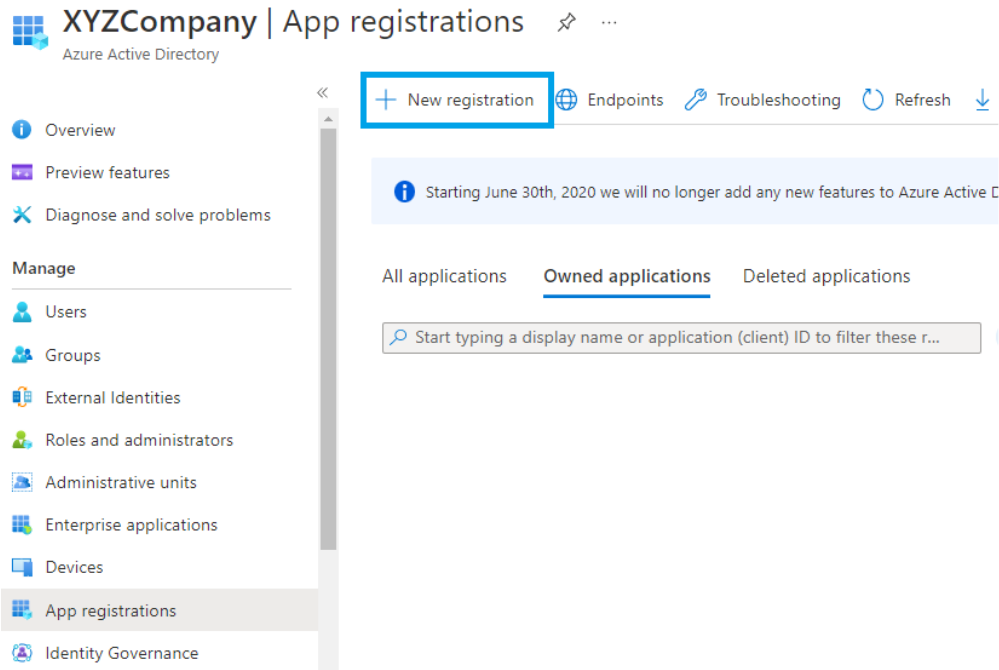
Creating a single-tenant application in Azure involves doing the following:

1. Creating an application in Azure Active Directory.
2. Adding API permissions and grant admin consent.
3. Creating a Secret Key.

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

To create a single-tenant application in Azure

1. Log in to [Azure](#) with a user that has the Global Administrator role.
2. Click **Azure Active Directory** > **App registrations**.
3. Click **New registration**.



4. On the registration form, choose a name for your application, select **Account in this organizational directory only (single-tenant)**, then click **Register**.

[Home](#) > [XYZCompany](#) >

Register an application

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

XYZCompanyApplication ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (XYZCompany 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.

Select a platform ▼ e.g. <https://example.com/auth>

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. On your application page, select **API Permissions** > **Add a permission** > **APIs my organization uses**.

Home > XYZCompany > XYZCompanyApplication

XYZCompanyApplication | API permissions

Search (Ctrl+/) << Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles

The "Admin consent required" column shows the default value for an organization. However [more](#)

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 XYZCompany

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

6. Type *WindowsDefenderATP*, and 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

WindowsDefenderATP

Name	Application (client) ID
WindowsDefenderATP	fc780465-2017-40d4-a0c5-307022471b92

7. Click **Application permissions** > **Alert**. Click **Alert.Read.All**. Then click **Add permissions**.

Request API permissions


[← All APIs](#)


WindowsDefenderATP

https://userrequestsgraphapi-prd.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)	
<input checked="" type="checkbox"/> Alert.Read.All ⓘ Read all alerts	Yes
<input type="checkbox"/> Alert.ReadWrite.All ⓘ Read and write all alerts	Yes

Add permissions

Discard

8. Select the **Application permission** and click **Grant admin consent for your company name**.

[Home](#) > [XYZCompany](#) > [XYZCompanyApplication](#)

XYZCompanyApplication | API permissions

Search (Ctrl+/)

[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 XYZCompany

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 XYZCompany

Grant admin consent confirmation.

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

Yes
 No

9. To add a secret to the application, select **Certificates & secrets**, add a description to the secret, and then click **Add**.

[Home](#) > [XYZCompany](#) > [XYZCompanyApplication](#)

XYZCompanyApplication | Certificates & secrets

[Got feedback?](#)

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions

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

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.

Add a client secret

Description

Expires

[Add](#)[Cancel](#)

10. After you click **Add**, copy the generated **Secret Key** value.

Make a copy of the **Secret Key** value. You won't be able to retrieve this value after you leave.

[Home](#) > [XYZCompany](#) > [XYZCompanyApplication](#)

XYZCompanyApplication | Certificates & secrets

[Got feedback?](#)

- Overview
- Quickstart
- Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions

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
XYZCompanySecret	6/22/2024	rOn8Q~CokWnthskC_4pboBwkXuxHdp...	80cb42fc-1c66-45ba-b3a4-25eaa5d7667f

11. Select **Overview** and copy the **Application (client) ID** and **Directory (tenant) ID**.

[Home](#) > [XYZCompany](#) >

XYZCompanyApplication ...

 Delete  Endpoints  Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

^ Essentials

Display name : [XYZCompanyApplication](#)

Application (client) ID : [6ba1a2b3-5be5-4ad1-880c-24c4cb02667a](#)

Object ID : 5bc93006-50bb-4a8c-982a-ee3ad6a26ac2

Directory (tenant) ID : [ee50daaf-ea51-476b-962f-9ca83bb9e8ea](#)

Supported account types : [My organization only](#)

12. Proceed to the **To integrate the application with Barracuda XDR Dashboard** procedure below.

Integrating 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

6ba1a2b3-5be5-4ad1-880c-24c4cb02667a ✓

Secret Key

..... ✓

Tenant ID

ee50daaf-ea51-476b-962f-9ca83bb9e8ea ✓

Test **Save**

Test Log:
2022-06-22T21:43:27 Starting Microsoft Defender for Endpoint test...
2022-06-22T21:43:27 Performing Authorization request...
2022-06-22T21:43:27 Successfully Authorized.
2022-06-22T21:43:27 Performing API request...
2022-06-22T21:43:28 API request succeeded! No alerts have been generated.

Successful test. Remember to save your settings!

5. Click **Save**.

Figures

1. microsoft.singletenant.register1.png
2. microsoft.singletenant.register2.png
3. microsoft.singletenant.permission1.png
4. microsoft.singletenant.permission2.png
5. microsoft.singletenant.permission3.png
6. microsoft.singletenant.grantconsent1.png
7. microsoft.singletenant.grantconsent2.png
8. microsoft.singletenant.newsecret1.png
9. microsoft.singletenant.newsecret2.png
10. microsoft.singletenant.newsecret3.png
11. microsoft.singletenant.overview.png
12. microsoft.singletenant.save.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.