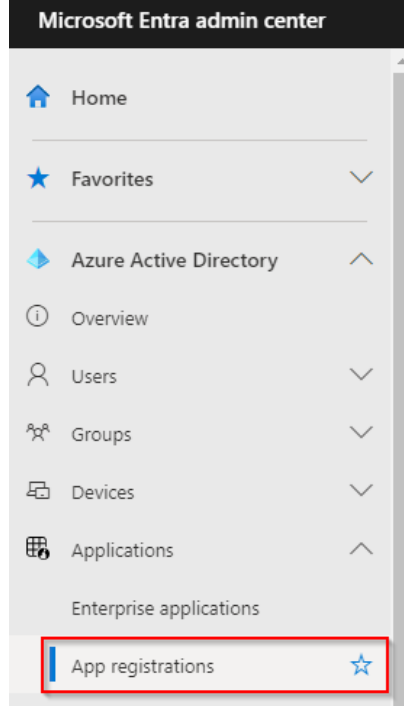


Azure AD application – part 1

Summary

In this post I'm covering how to create an Azure AD app registration to manager Intune Devices using secret as authentication method.

Go to Microsoft Entra Admin center
<https://entra.microsoft.com/>



Home >
App registrations

[+ New registration](#) [Endpoints](#) [Troubleshooting](#) [Refresh](#) [Download](#) [Preview features](#) | [Got feedback?](#)

i Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will upgrade to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Give it a **Name**:

Select "Account in this organization directory only (Your Tenant only – Single tenant" under supported account types

Add

"https://login.microsoftonline.com/common/oauth2/nativeclient"

Then click register to proceed.

Home > App registrations > Register an application

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

Supported account types
Who can use this application or access this API?
☒ Accounts in this organizational directory only (Contoso 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.
 Public client/native (mobile ... | https://login.microsoftonline.com/common/oauth2/nativeclient

Make notes of the:

Application (client) ID

Directory (Tenant) ID

Home > App registrations > Update Autopilot Hashes

Create application
Successfully created application Update Autopilot Hashes.

Search < > Delete Endpoints Preview features

Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Essentials
 Display name : Update Autopilot Hashes
 Application (client) ID : e6b6ebb5-2037-444b-a43f-d65feab...
 Object ID : d544744e-86e6-497d-83f8-9b8447b...
 Directory (tenant) ID : 432f57fd-3a36-4056-ac68-e8e5aa77...
 Supported account types : My organization only
 Client credentials : Add a certificate or secret
 Redirect URIs : @ web, @ spa, @ public client
 Application ID URI : Add an Application ID URI
 Managed application in local directory : Update Autopilot Hashes

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Click on Certificates & secrets under Manage.

Select + New client secret.

Home > App registrations > Update Autopilot Hashes

Update Autopilot Hashes | Certificates & secrets

Search < > Got feedback?

Overview
Quickstart
Integration assistant
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners

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.

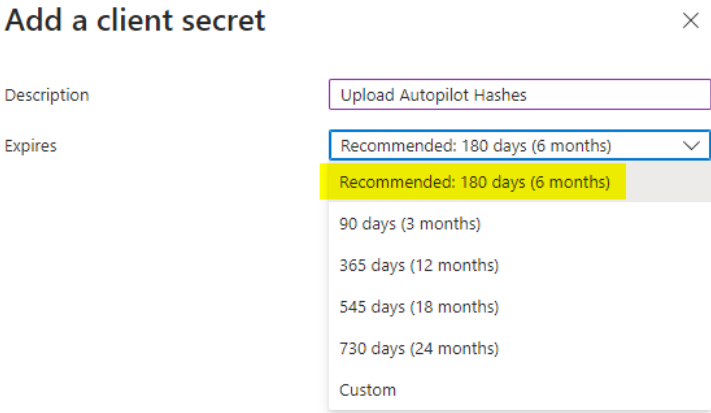
Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) 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
No client secrets have been created for this application.			

<p>Under the new TAB “Add a client secret”</p> <p>Give it a Description:</p> <p>Select your default “Expires” option in months or Custom.</p> <p>For this setup I’m using</p> <p>Recommended: 180 days (6 months)</p>	
<p>Copy value and secret ID</p> <p>Add secret ID to your PowerShell code for authentication</p>	<p>JUe8Q~ETBdaHg8PLy4yX20Cd-6.KfRPdzQ3_WbVH</p> <p>xxxxxxxx-f4d6-4364-a849-aaaaaaaaaaaa</p>

Thiago Beier
Toronto, ON