

# Azure AD application – part 2

## Contents

Summary .....	1
Code .....	1
Configuring Azure AD application .....	2

## Summary

In this post I'm covering how to create an Azure AD app registration to manage Intune Devices hash import to windows autopilot through this app using certificate as authentication method.

You need a certificate for this. If you do not have a purchased certificate, you can generate a self-signed certificate.

1. Create the Azure AD App
2. Configure the App to support Certificate authentication.

## Code

PowerShell code to create the certificate and its PFX file

```
#Azure AD APP certificate authentication
#Create and export your public certificate
$certname = "UpdateAutopilotHashes" ## Replace {certificateName}
$cert = New-SelfSignedCertificate -Subject "CN=$certname" -CertStoreLocation
"Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature -KeyLength 2048
-KeyAlgorithm RSA -HashAlgorithm SHA256
Export-Certificate -Cert $cert -FilePath "C:\BLOG\$certname.cer" ## Specify your
preferred location

#(Optional): Export your public certificate with its private key
$mypwd = ConvertTo-SecureString -String "funnyPan+her95" -Force -AsPlainText ##
Replace {myPassword}
Export-PfxCertificate -Cert $cert -FilePath "C:\BLOG\$certname.pfx" -Password $mypwd
## Specify your preferred location
```

You can use Windows Terminal on Windows 11 to perform the certificate creation

```
PS C:\BLOG> .\1-cert-create-and-export.ps1

Directory: C:\BLOG

Mode                LastWriteTime         Length Name
----                -
-a----            3/13/2023   1:23 AM             798 UpdateAutopilotHashes.cer
-a----            3/13/2023   1:23 AM            2652 UpdateAutopilotHashes.pfx
```

## Configuring Azure AD application

1. Go back to Azure AD app
2. Click on Certificates & secrets under Manage

Home > App registrations > Update Autopilot Hashes

### Update Autopilot Hashes | Certificates & secrets

<< [Got feedback?](#)

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Related administration

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 (1)   Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

Thumbprint	Description	Start date	Expires	Certificate ID
No certificates have been added for this application.				


3. Under Certificates tab
4. Click upload certificate.
5. Under upload certificate click on browse then select the .cer file (certificate)

## Upload certificate

✓ Upload Completed for  
UpdateAutopilotHashes.cer  
798 B | "Streaming upload"

✕

Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt



Description

- Click “add” and make sure Certificate Thumbprint, Description, Start date, Expires and Certificate ID corresponds to your imported certificate.

Home > App registrations > Update Autopilot Hashes

### Update Autopilot Hashes | Certificates & secrets

Search

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

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.

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

Certificates (3) Client secrets (1) Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Description	Start date	Expires	Certificate ID
...	CN=PnPowerShell	3/12/2023	3/12/2024	e4b28910-a7a3-4209...
D3E447E1F3868207A3E734965D64E1...	CN=UpdateAutopilotHashes	3/13/2023	3/13/2024	8dea01e4-20dc-4962...
...	CN=PnPowerShell	9/29/2022	9/29/2032	d1061f69-cc26-4222-...

Update application credentials  
Successfully updated application Update Autopilot Hashes credentials

## Reference

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-self-signed-certificate>

Cheers,

**Thiago Beier**  
Toronto, ON