

App-only certificate

Author: Tyler Lu

Contents

[1. Prerequisite 2](#_Toc498098771)

[2. Generate a self-signed certificate 2](#_Toc498098772)

[2.1. Generate a self-signed certificate with PowerShell 2](#_Toc498098773)

[2.2. Get thumbprint 2](#_Toc498098774)

[2.3. Get keyCredential 2](#_Toc498098775)

[2.4. Export the certification 3](#_Toc498098776)

[3. Use keyCredential in Azure App Registration 6](#_Toc498098777)

[4. Use the certificate in Azure Web App 7](#_Toc498098778)

[4.1 Upload the certificate 7](#_Toc498098779)

[4.2 Add App Settings 8](#_Toc498098780)

# Prerequisite

We will create a self-signed certification for application permissions. PowerShell with administrative privilege is required.

# Generate a self-signed certificate

## Generate a self-signed certificate with PowerShell

Run PowerShell as administrator. Then execute the command below:

|  |
| --- |
| $cert = New-SelfSignedCertificate -Type Custom –KeyExportPolicy Exportable -KeySpec Signature -Subject "CN=Huddle App-only Cert" -NotAfter (Get-Date).AddYears(20) -CertStoreLocation "cert:\CurrentUser\My" -KeyLength 2048 |

Note: Keep the PowerShell open.

## Get thumbprint

Run the command below in the same PowerShell window.

|  |
| --- |
| Write-Host $cert.Thumbprint |

Copy the output value. It will be used as the value of **WEBSITE\_LOAD\_CERTIFICATES** and ida:**ClientCertThumbprint** app settings.

Note: Keep the PowerShell open.

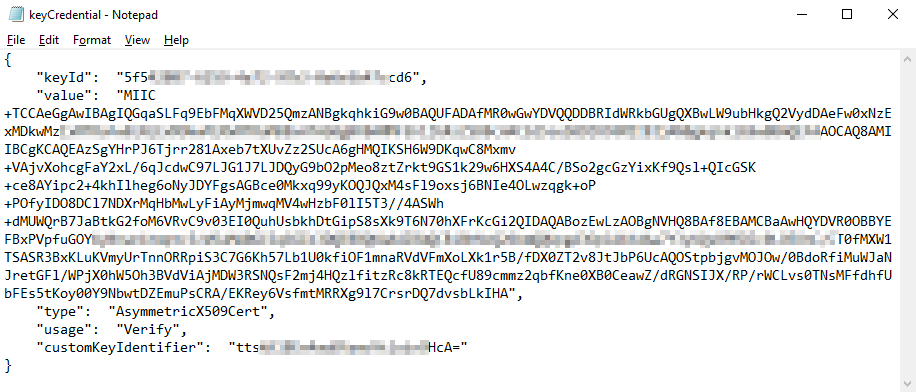
## Get keyCredential

The following command will create the keyCredential and save it to c:\keyCredential.txt.

Feel free to change the file path.

|  |
| --- |
| $keyCredential = @{}  $keyCredential.customKeyIdentifier = [System.Convert]::ToBase64String($cert.GetCertHash())  $keyCredential.keyId = [System.Guid]::NewGuid().ToString()  $keyCredential.type = "AsymmetricX509Cert"  $keyCredential.usage = "Verify"  $keyCredential.value = [System.Convert]::ToBase64String($cert.GetRawCertData())  $keyCredential | ConvertTo-Json > c:\keyCredential.txt |

Execute the command in the same PowerShell window. Then open the txt file:

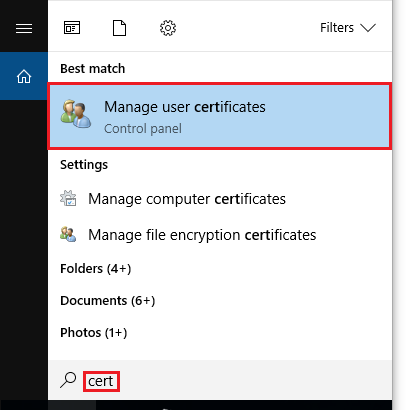


The text in it is a JSON fragment containing the public key, and will be used in Azure App Registrations.

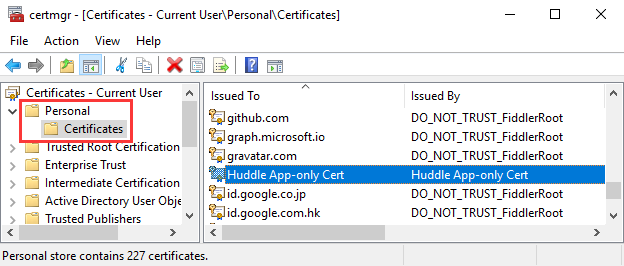
Note: You can close PowerShell now.

## Export the certification

Search “cert”.

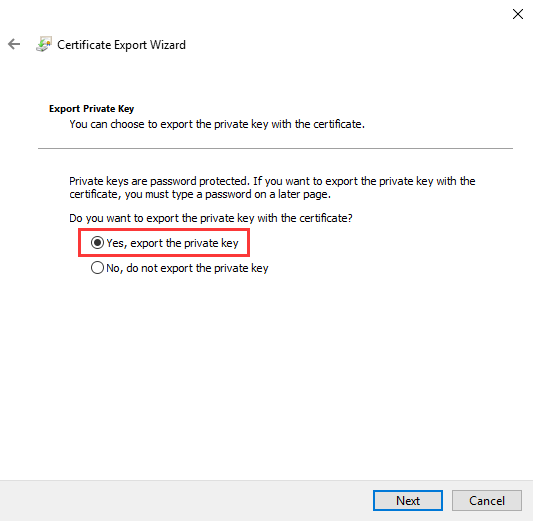


Then click **Manage user certificates**.

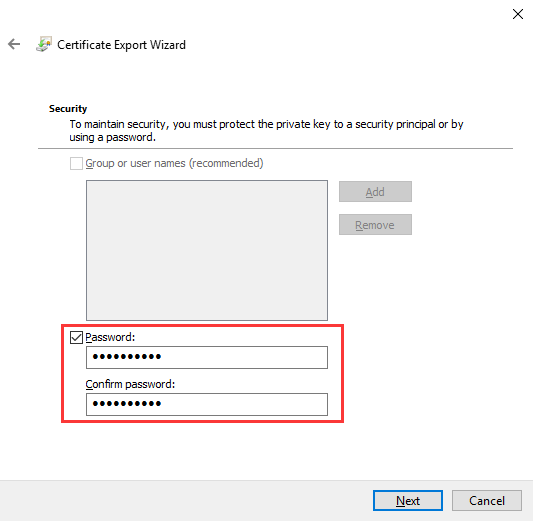


Click **Personal** -> **Certificates** at the left, then find the certificate at the right.

Right click it, then click **All Tasks** -> **Export…**



Export the private key, you need to specify a password:



Name the file as “Huddle App-only Cert”.

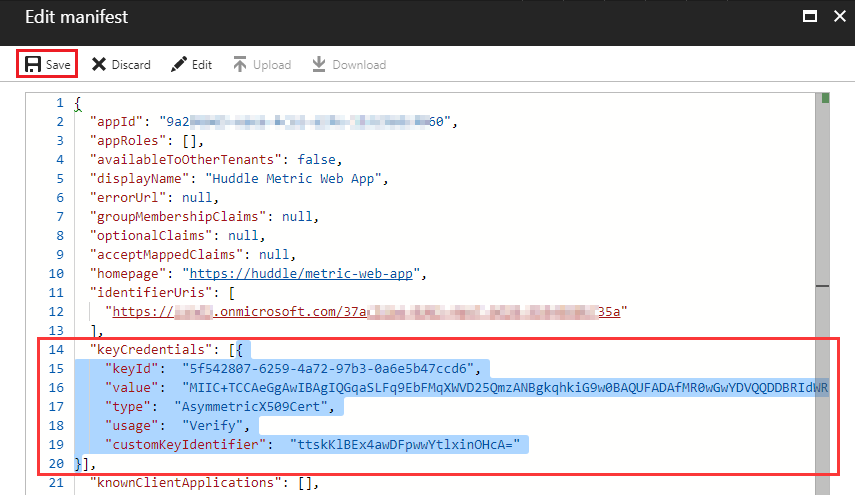
Keep the exported certificate file and the private key password. They will be used when uploading certificate to an Azure Web App.

# Use keyCredential in Azure App Registration

Find the App Registration in Azure Portal.



Click **Manifest**.



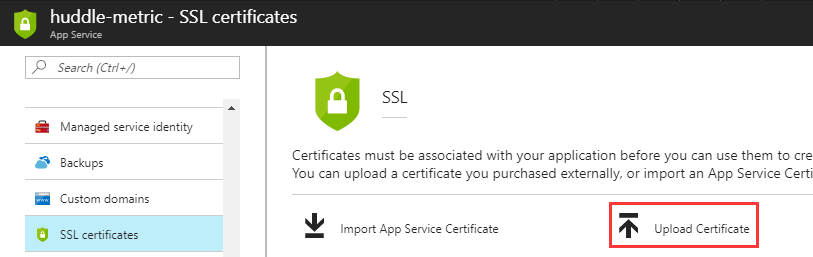
Insert the keyCredential JSON part into the square brackets of **keyCredentials** node.

Click **Save**.

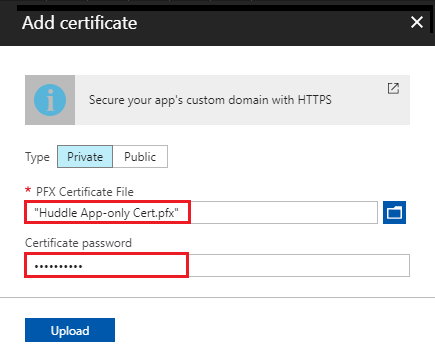
# Use the certificate in Azure Web App

### 4.1 Upload the certificate

Find the Web App in Azure Portal. Click **SSL certificates**:



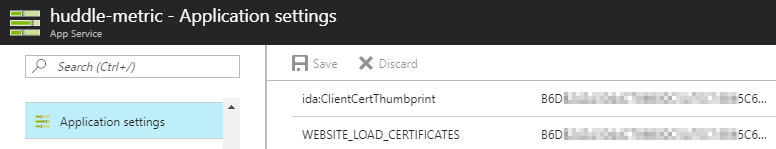
Click **Upload Certificate**.



Select the ***Huddle App-only Cert Dev.pfx*** certificate file, input the password, then click **Upload**.

### 4.2 Add App Settings

Click **Application Settings**. Make sure the following App settings are added.



|  |  |
| --- | --- |
| Key | Value |
| WEBSITE\_LOAD\_CERTIFICATES | Thumbprint of the certificate |
| ida:ClientCertThumbprint | Thumbprint of the certificate |