Installing certificates on a Webhook (Azure Function)

Last updated by | Alan Parsons | 4 Dec 2023 at 16:19 GMT

Steps

1. Register Custom Domain in the Azure Function.

- Navigate to the required Function App from within the Azure Portal, and then navigate to **Settings** -> **Custom Domains** in the left-hand pane..
- Click on **Add Custom Domain**
- In the "Add Custom Domain" dialogue window, select:
  - Domain Provider: **All other domain services**
  - TLS/SSL certificate: **Add certificate later**
  - TLS/SSL type: **SNI SSL**
  - Domain: <**SAN entry, as per configured in certificate>**
- Two DNS entries need to be made prior to clicking validate

Note: *the "Domain" entry above can be either of the 2 Subject alternative Names (SAN) configured in the certificate.*

2. Create entries in DNS:

Registering a Custom Domain in Azure will prompt you to create two DNS entries in DNS:

- **CNAME record** - a record **that** repoints/redirects the custom domain name to the fully qualified domain name (FQDN) of the Function App. The CNAME "Name" entry must be configured to be the same as one of the SAN entries configured in the certificate, and the "Alias" configured as the FQDN of the Function App.
- **TXT record** - used to confirm ownership of the domain. The Azure portal will advise on the value that needs to be set in this record.

Once the above entries have been created in DNS, switch back to the "Add Custom Domain" dialogue window in Azure portal, and click **Validate**. The Custom Domain entry will be validated and then created.

3. Bind the mTLS certificate to the Custom Domain.

- Navigate to the required Function App from within the Azure Portal, and then navigate to **Settings** -> **Custom Domains** in the left hand pane.
- Click on the "**Add binding**" link located next to the Custom Domain entry.
  - At this point, there are two of options to choose from whilst in the **Add TLS/SSL Binding** dialogue window:

Option 1 - Import from Key Vault

For this option to be available, the following criteria needs to be met first:

- The certificate has to be pre-uploaded into the target Key Vault in PFX format.
- The System Managed Identity of the Function App requires GET, LIST Certificates and GET, LIST secrets privileges on the target Key Vault. Please note that RBAC cannot be used.
  - Navigate to the **Certificate** drop down list, and select **Add Certificate.**
  - Navigate to the **Source** drop down list, and select **Import from Key Vault.**
  - Click **Select Key Vault Certificate** and select the required certificate using the wizard.
  - Click **Select** and then **Add.**

Option 2 - Upload Certificate

If the certificate has created and is stored outside of a Key Vault, then it can be uploaded as a PFX file.

- Navigate to the **Certificate** drop down list, and select **Add Certificate.**
- Navigate to the **Source** drop down list, and select **Upload Certificate (.pfx)**.
- Click on **Browse**, and use file manager to navigate to the .pfx file. Click **Open.**
- Click **Add**

If required, the below PowerShell can be used to create a full PFX with password:

```
param (
    [Parameter(Mandatory=$true, Position=0)]
    [string] $importPath,

    [Parameter(Mandatory=$true, Position=1)]
    [string] $exportPath,

    [Parameter(Mandatory=$true, Position=2)]
    [string] $pwd
)

$imported = Import-PfxCertificate -FilePath $importPath -CertStoreLocation Cert:\LocalMachine\My -Exportable
$thumb = $imported.Thumbprint
Export-PfxCertificate -Cert Microsoft.PowerShell.Security\Certificate::LocalMachine\My\$thumb -FilePath $expor
```

Once the TLS certificate is bound to the Custom Domain, the process of installing a certificate on a Webhook is complete

Microsoft: https://learn.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-domain?tabs=root%2Cazurecli