



# CSP PARTNER APPLICATION OVERVIEW

Multi-tenant application model

*The information provided in this document is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.*

© 2018 Microsoft. All rights reserved.

October 2018

Microsoft

## TABLE OF CONTENTS

CSP PARTNER APPLICATION .....	2
CREATE A MICROSOFT PARTNER CENTER SERVICE PRINCIPAL .....	2
CREATE A MULTI-TENANT APPLICATION ON THE CSP PARTNER'S TENANT.....	2
APPLICATION PERMISSIONS .....	3
CONSENT LINK .....	4
KEY VAULT SETUP .....	5
CREATE A NEW WEB APPLICATION IN CSP PARTNER'S TENANT .....	5
AZURE KEY VAULT SETUP .....	5
AZURE KEY VAULT ACCESS .....	6
PROTOTYPE CONFIGURATION .....	7
PROTOTYPE HAS TWO APPLICATIONS:.....	7
CONFIGURATIONS .....	7
PARTNER CONSENT APPLICATION:.....	7
CSP PARTNER APPLICATION: .....	8

## CSP PARTNER APPLICATION

### CREATE A MICROSOFT PARTNER CENTER SERVICE PRINCIPAL

Create a Microsoft Partner Center service principal in the CSP partner's tenant, where the multitenant application is going to be created.

**NOTE:** For CSP partner tenants, this service principal should already exist. If not, please create using the following steps.

In a PowerShell window, run the following admin commands.

1. Install the AzureAD module.
  - `Install-Module "AzureAD"`
2. Run `Connect-AzureAD`, this will prompt for a user name and password. Please enter the tenant admin credentials.
  - `Connect-AzureAD`
3. Create a Microsoft Partner Center service principal.
  - `New-AzureADServicePrincipal -DisplayName "Microsoft Partner Center" -AppId fa3d9a0c-3fb0-42cc-9193-47c7ecd2edbd`

### CREATE A MULTI-TENANT APPLICATION ON THE CSP PARTNER'S TENANT.

Please make sure that the following application properties are set for the newly created multi-tenant application.

1. Have an **Application type** of "Web app / API"
2. The **Home page** URL must be your application redirect URL, which will show the consent success to the partner and collect a refresh token
3. Add a key to the web application

The screenshot displays the Azure portal configuration for a CSP Application. It is divided into three main panes:

- CSP Application (Left Pane):** Shows the application name "CSP Application" and its type "Web app / API". It also lists the "Application ID", "Object ID", and "Home page" (redacted).
- Settings (Middle Pane):** A navigation menu with a search bar "Filter settings". The "Properties" option is selected. Other options include "Reply URLs", "Owners", "Required permissions", "Keys", "Troubleshoot", and "New support request".
- Properties (Right Pane):** Contains various configuration fields:
  - Name:** CSP Application
  - Object ID:** [Redacted]
  - Application ID:** [Redacted]
  - App ID URI:** [Redacted]
  - Logo:** A green square with "CA" in white.
  - Upload new logo:** A button to "Select a file".
  - Home page URL:** [Redacted]
  - Logout URL:** [Empty field]
  - Terms of service URL:** [Empty field]
  - Privacy statement URL:** [Empty field]
  - Application type:** Web app / API
  - Multi-tenanted:** A toggle set to "Yes".

## APPLICATION PERMISSIONS

Please make sure the following permissions are set for the multi-tenant application

1. Windows Azure Active Directory
  - a. There should not be any direct **Application Permissions** to the multi-tenant application.
  - b. **Delegated Permissions** are to be set to access Active Directory as the signed in user.

### Required permissions

+ Add Grant permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	0	2
Microsoft Partner Center	0	1

### Enable Access

Windows Azure Active Directory

Save Delete

APPLICATION PERMISSIONS REQUIRES ADMIN

- Read directory data Yes
- Read and write domains Yes
- Read and write directory data Yes
- Read and write devices Yes
- Read all hidden memberships Yes
- Manage apps that this app creates or owns Yes
- Read and write all applications Yes
- Read and write domains Yes

DELEGATED PERMISSIONS REQUIRES ADMIN

- Access the directory as the signed-in user No
- Read directory data Yes
- Read and write directory data Yes
- Read and write all groups Yes
- Read all groups Yes
- Read all users' full profiles Yes
- Read all users' basic profiles No
- Sign in and read user profile No
- Read hidden memberships Yes

## 2. Microsoft Partner Center

- a. Grant **Access Partner Center** permissions under **Delegated Permissions**.

### Required permissions

+ Add Grant permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	0	2
Microsoft Partner Center	0	1

### Enable Access

Microsoft Partner Center

Save Delete

APPLICATION PERMISSIONS REQUIRES ADMIN

No application permissions available.

DELEGATED PERMISSIONS REQUIRES ADMIN

- Access Partner Center No

## CONSENT LINK

Present the partner with the consent link and have them login with their service account to approve the CSP application to act on behalf of the service account on partner tenant.

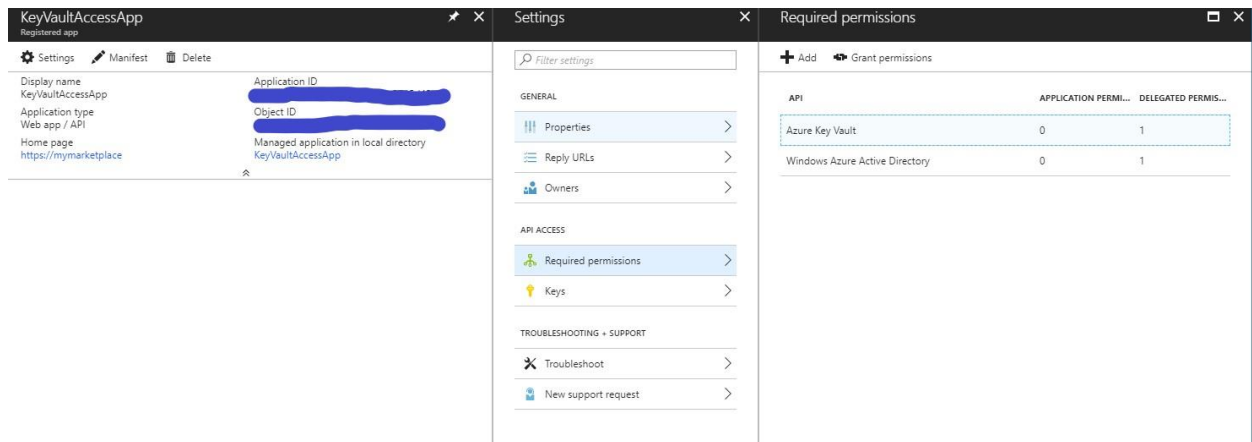
[https://login.microsoftonline.com/common/oauth2/authorize?&client\\_id=<CSPApplicationId>&response\\_type=code&redirect\\_url=https://<CSPApplicationUrl which collects refreshtoken>](https://login.microsoftonline.com/common/oauth2/authorize?&client_id=<CSPApplicationId>&response_type=code&redirect_url=https://<CSPApplicationUrl which collects refreshtoken>)

## KEY VAULT SETUP

### CREATE A NEW WEB APPLICATION IN CSP PARTNER'S TENANT

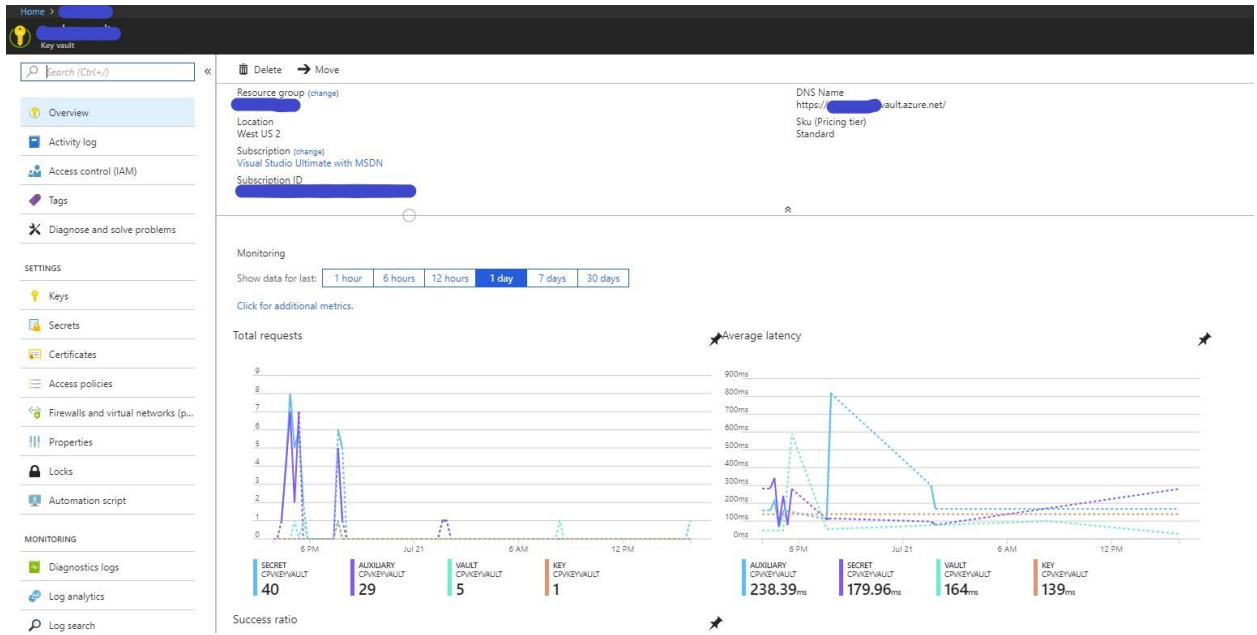
If you are using Azure Key Vault:

1. Add a key to the web application
2. Set application permissions in the **Required Permissions** tab
  - a. For an **Azure Key Vault** app, under the **Delegated Permissions** section, select **Have full access to the Azure Key Vault service**
  - b. For a **Windows Azure Active Directory** app, under the **Delegated Permissions** section, select **Sign in and read user profile**



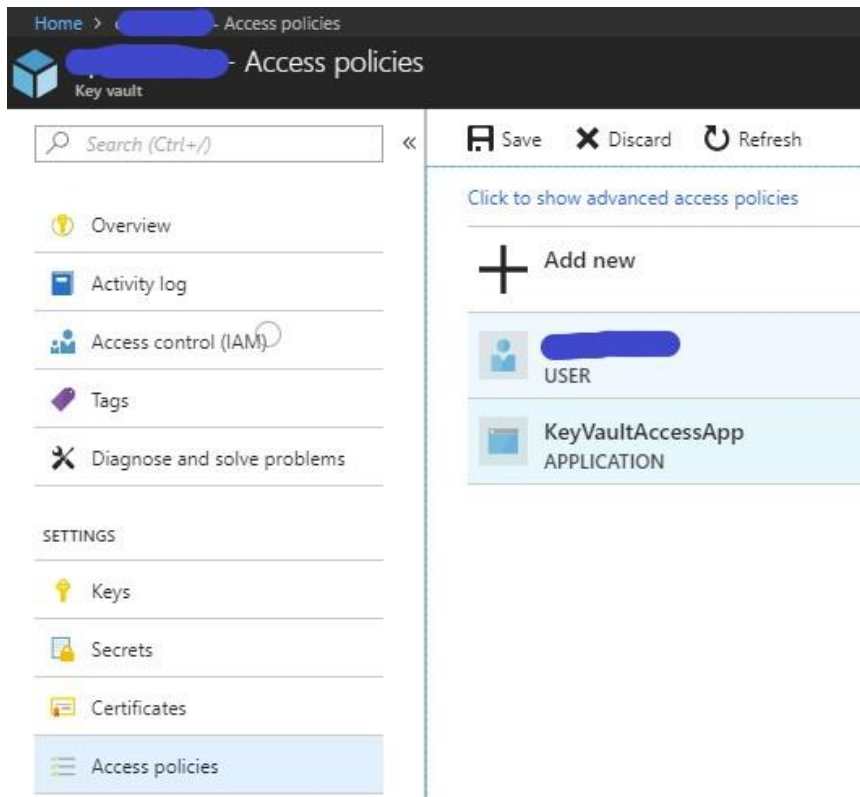
## AZURE KEY VAULT SETUP

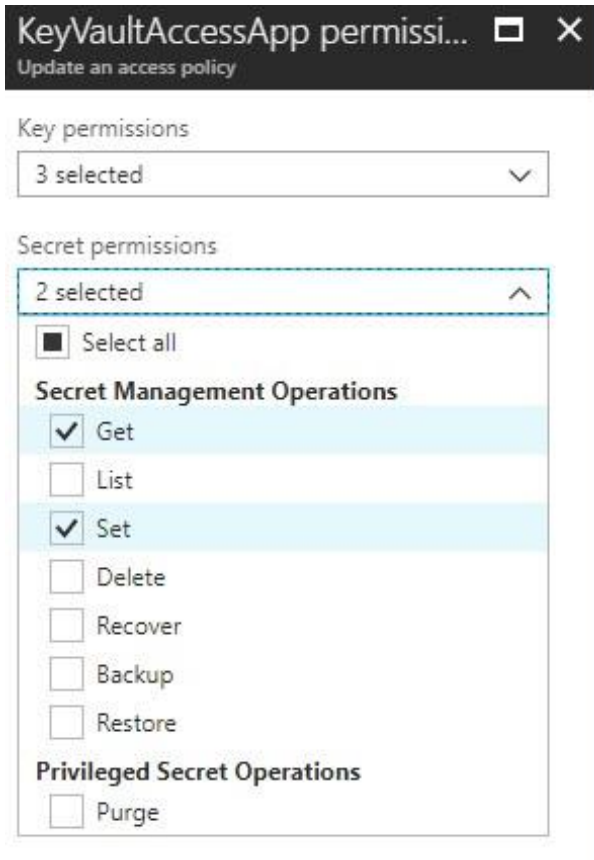
Create the Azure Key Vault with the appropriate <key-vault-name> and it will result in a DNS name like: <https://<key-vault-name>.vault.azure.net>



## AZURE KEY VAULT ACCESS

In the access policies of the key vault, add the **KeyVaultAccessApp** with permissions to only manage the **Get** and **Set** aspects of a **Secret**.





## PROTOTYPE CONFIGURATION

### PROTOTYPE HAS TWO APPLICATIONS:

1. **Partner Consent:** Represents a web application designed to accept consent from a CSP partner and show a success message.
  - a. This application will setup consent and capture the refresh token of the consented user.
  - b. The consented user's refresh token is used for generating the access token for the CSP partner tenant.
2. **CSP application:** Represents a primary CSP application which calls Partner Center APIs and graph APIs to perform commerce and user actions on behalf of the partner
  - a. This application retrieves the access token for a specific audience (Partner Center APIs or graph) before calling respective APIs using the refresh token that is stored securely in the key vault

### CONFIGURATIONS

#### PARTNER CONSENT APPLICATION:

The web.config file has the following sections called out. Please update the values with corresponding application IDs and secrets. For your primary application, please use "certificate" as the web application secret instead of plain secrets because it will provide an additional layer of security.



```

<!-- AppID that represents CSP application -->
<add key="ida:CSPApplicationId" value="CSPApplicationIdValue" />
<!--
Please use certificate as your client secret and deploy the certificate to your environment.
The following application secret is for sample application only. please do not use secret directly from the
config file.
-->
<add key="ida:CSPApplicationSecret" value="CSPApplicationSecretValue" />

<!-- AppID that is given access for keyvault to store the refresh tokens -->
<add key="ida:KeyVaultClientId" value="KeyVaultClientIdValue" />

<!--
Please use certificate as your client secret and deploy the certificate to your environment.
The following application secret is for sample application only. please do not use secret directly from the
config file.
-->
<add key="ida:KeyVaultClientSecret" value="KeyVaultClientSecretValue" />

<!-- AAD instance: Global is .com, for different national clouds it changes German cloud: .de, China cloud: .cn
-->
<add key="ida:AADInstance" value="https://login.microsoftonline.com/" />

```

---

#### CSP PARTNER APPLICATION:

The app.config file has the following sections called out. Please update the values with the corresponding application IDs and secrets. For your primary application, please use "certificate" as the web application secret instead of plain secrets because it will provide an additional layer of security.

```

<!-- AppID that represents CSP application -->
<add key="ida:CSPApplicationId" value="CSPApplicationIdValue" />
<!--
Please use certificate as your client secret and deploy the certificate to your environment.
The following application secret is for sample application only. please do not use secret directly
from the config file.
-->
<add key="ida:CSPApplicationSecret" value="CSPApplicationSecretValue" />
<!-- AppID that is given access for keyvault to store the refresh tokens -->

<add key="ida:KeyVaultClientId" value="KeyVaultClientIdValue" />
<!--
Please use certificate as your client secret and deploy the certificate to your environment.
The following application secret is for sample application only. please do not use secret directly
from the config file.
-->
<add key="ida:KeyVaultClientSecret" value="KeyVaultClientSecretValue" />

<!-- AAD instance: Global is .com, for different national clouds it changes German cloud: .de,
China cloud: .cn -->
<add key="ida:AADInstance" value="https://login.microsoftonline.com/" />

```