



CONTROL PANEL VENDOR 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

CONTROL PANEL VENDOR APPLICATION	2
CREATE A MICROSOFT PARTNER CENTER SERVICE PRINCIPAL	2
CREATE A MULTI-TENANT APPLICATION ON THE CONTROL PANEL VENDOR'S TENANT.....	2
APPLICATION PERMISSIONS	3
CONSENT LINK	4
KEY VAULT SETUP	5
CREATE A NEW WEB APPLICATION IN CONTROL PANEL VENDOR 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:.....	8
CONTROL PANEL VENDOR APPLICATION:	8

CONTROL PANEL VENDOR APPLICATION

CREATE A MICROSOFT PARTNER CENTER SERVICE PRINCIPAL

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

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 CONTROL PANEL VENDOR'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

CPV Application

Registered app

Settings Manifest Delete

Display name

CPV Application

Application type

Web app / API

Home page

Application ID

Object ID

Managed application in local directory

CPV Application

Settings

Filter settings

GENERAL

Properties

Reply URLs

Owners

API ACCESS

Required permissions

Keys

TROUBLESHOOTING + SUPPORT

Troubleshoot

New support request

Save Discard

Name

CPV Application

Object ID

Application ID

App ID URI

Logo

CA

Upload new logo

Select a file

Home page URL

Logout URL

Terms of service URL

Privacy statement URL

Application type

Web app / API

Multi-tenanted

Yes No

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 Control Panel vendor application to act on behalf of the service account.

https://login.microsoftonline.com/common/oauth2/authorize?&client_id=<CPVApplicationId>&response_type=code&redirect_url=https://<CPVApplicationUrl which collects refreshtoken>

China:https://login.microsoftonline.com/common/oauth2/authorize?&client_id=<CPVApplicationId>&response_type=code&redirect_url=https://<CPVApplicationUrl which collects refreshtoken>

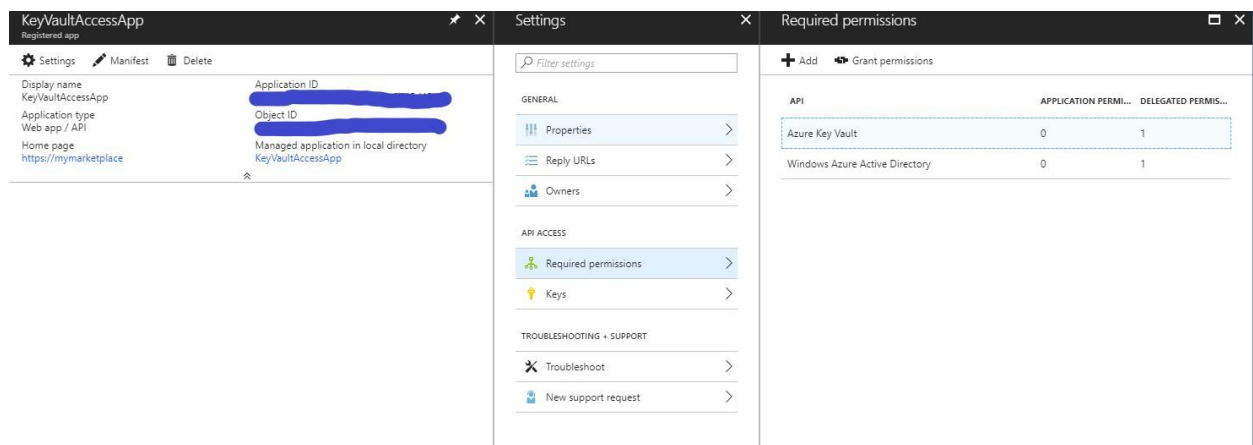
4

KEY VAULT SETUP

CREATE A NEW WEB APPLICATION IN CONTROL PANEL VENDOR TENANT

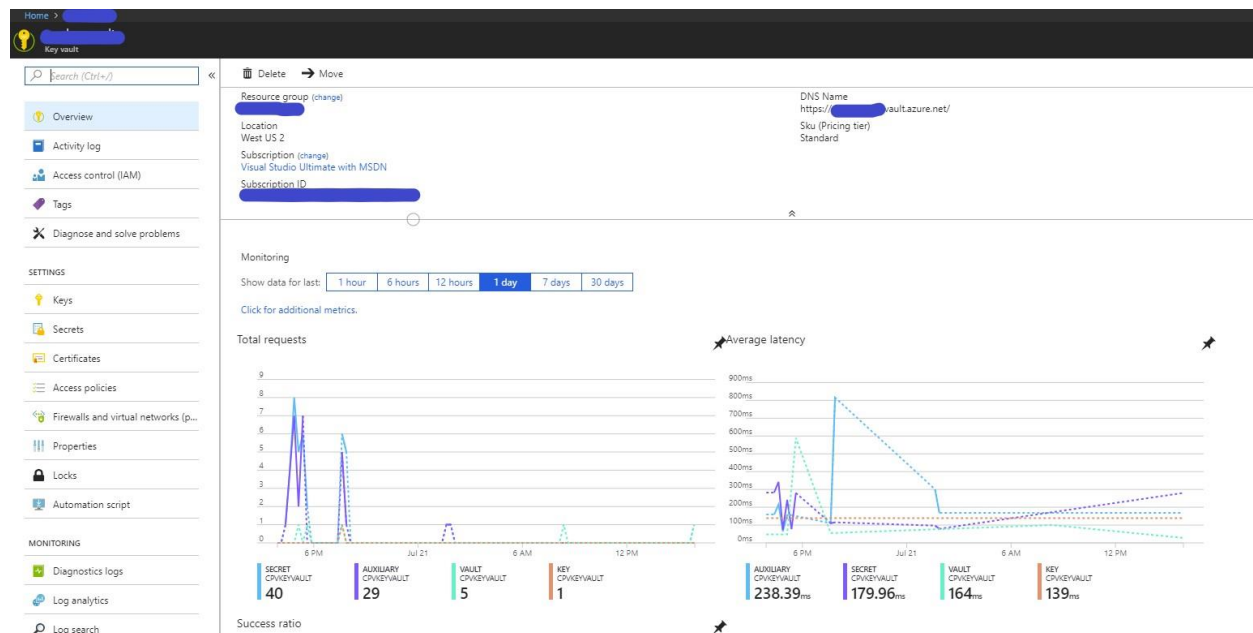
If you are using Azure Key Vault:

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**



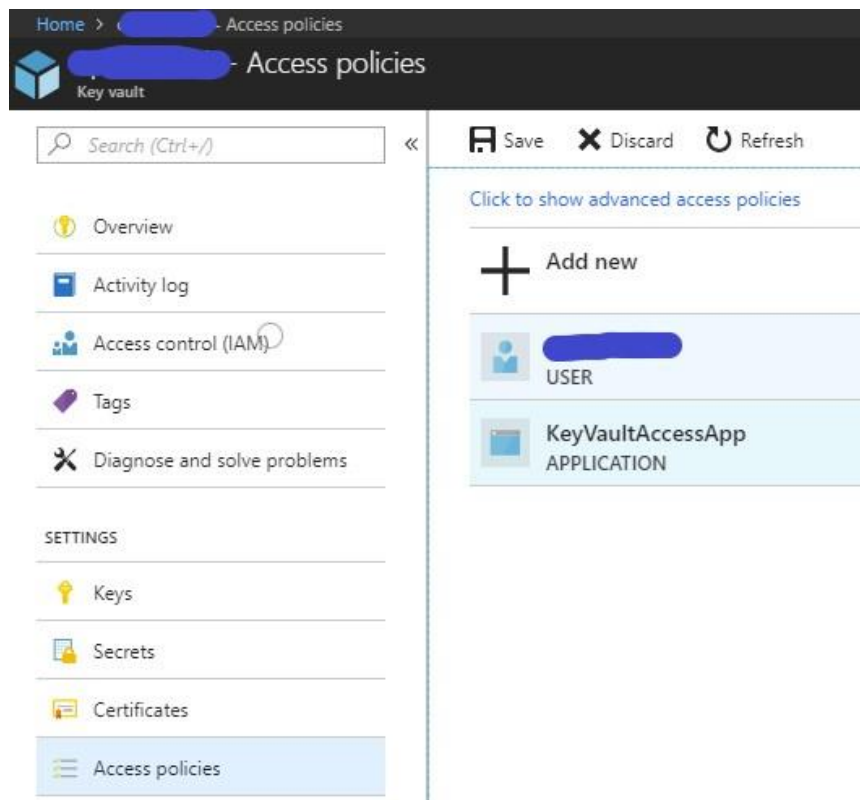
AZURE KEY VAULT SETUP

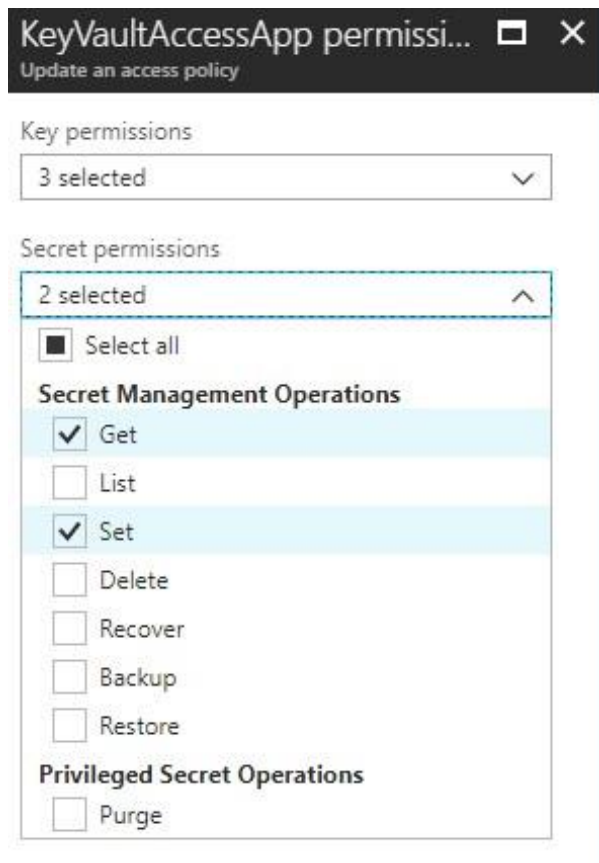
Create the Azure Key Vault with the appropriate <key-vault-name> and it will result in a DNS name like: <https://<key-vault-name>.vault.azure.net>



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 Control Panel vendor application.
2. **Control Panel vendor application:** Represents a primary Control Panel vendor 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 Control panel vendor application -->
<add key="ida:CPVApplicationId" value="CPVApplicationIdValue" />
<!--
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:CPVApplicationSecret" value="CPVApplicationSecretValue" />

<!-- 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: login.chinacloudapi.cn -->
<add key="ida:AADInstance" value="https://login.microsoftonline.com/" />
```

CONTROL PANEL VENDOR 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 Control panel vendor application -->
<add key="ida:CPVApplicationId" value="CPVApplicationIdValue" />
<!--
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:CPVApplicationSecret" value="CPVApplicationSecretValue" />

<!-- 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: login.chinacloudapi.cn -->
<add key="ida:AADInstance" value="https://login.microsoftonline.com/" />
```