



Application Notes for Call Management System (CMS) Enterprise Login (using Microsoft Azure) Local Login (using Certificates)

Issue 2.0 28 March, 2022

Abstract

These Application Notes contain information and instructions for using Call Management System (CMS) with Microsoft Azure for the purpose of CMS User login authentication. The integration of CMS with Microsoft Azure is referred to as Enterprise Login.

The Notes also outline how to configure local login authentication via personal certificate. Pre-login banner enablement/modification is also described.

The recommended CMS configuration is reviewed along with all required CMS administration.

It is assumed that the reader has a good working knowledge of Microsoft Azure as well as CMS. Some limited details of Microsoft Azure configuration are provided in this document.

1. Introduction

The purpose of this document is to summarize how CMS integrates with the following authentication methods.

- Microsoft Azure for authentication of CMS User login passwords.
- Login authentication via personal certificate

The document compares and contrasts the different CMS user authentication methods. It also provides instruction on how to administer CMS for integration with Microsoft Azure, and an example of how to configure Microsoft Azure. Similarly, it provides instruction on how to configure login authentication via personal certificate

This document assumes the reader is familiar with Microsoft Azure and therefore does not provide all information and details about how to administer Microsoft Azure.

The enablement/modification of a Pre-login banner is also described.

Document Change History

Issue 1.0	25 October 2021	Original published version for CMS 19.2.0.2
Issue 2.0	28 March 2022	Updated version for CMS 19.2.0.3

Contents

1.	Introduction	2
	Document Change History	2
2.	Types of CMS User Login	3
	Important Information About Security:	3
3.	Web Client User Login Screens	4
	Local Login:	4
	Enterprise Login:.....	4
4.	Authentication Configuration Helper Tool	5
	Example Usage:.....	5
5.	CMS Enterprise Configuration	6
	CMS Configuration Details:	6
6.	Microsoft Azure Example Configuration	8
	Microsoft Azure Configuration Example:	8

7.	Certificate Login Authentication configuration	13
	Cert Setup Details	13
	CMS Configuration Details:	13
8.	Certificate Login Authentication Operation	14
9.	Pre-Login Banner.....	15
10.	Troubleshooting Tips.....	15

2. Types of CMS User Login

Beginning with CMS 19.2.0.2 Service Pack, a new Enterprise Login method is available for CMS. Thus, there are now two login methods available:

- Local Login
 - Users login to CMS using the administered CMS user ID and password.
 - LDAP Password authentication is available for Local Login by:
 - Optionally administering individual users for password authentication via Microsoft Active Directory.

Note that if Microsoft Active Directory is used for password authentication, the LDAP package must first be installed on CMS, and CMS administered to establish connection to the Microsoft Active Directory server.
- Enterprise Login
 - Microsoft Azure is used for login authentication.
 - **Only available for use with CMS Web Client.**
 - Multifactor authentication (MFA) is enforced if Microsoft Azure is configured for MFA.
 - The LDAP package is not required.
 - The user must still have a login ID configured on CMS.
 - Some CMS administration is required to allow CMS to be recognized by Microsoft Azure. See subsequent sections of this document for details on CMS administration.

In the 19.2.0.3 Service Pack support for additional login authentication via personal certificate is available.

Login authentication via personal certificate is a requirement of JITC (The Joint Interoperability Test Command) certification. For Federal and DoD (Department of Defense) employees, personal certificates are encoded and provided by CAC (Common Access Card).

The CMS implementation does not limit support to requiring certificates be on CAC's. Personal certs can be in a regular cert store such as Microsoft Cert Store.

Important Information About Security:

- For both Local and Enterprise Logins, **a CMS User ID must be created.**

The CMS User ID must match **exactly** the User ID in Microsoft Active Directory or Microsoft Azure. As of CMS 19.2.0.0, CMS User IDs may be up to 31 characters long with no special characters in the User ID.

- When using Enterprise Login, no password should be assigned when creating new CMS users. New CMS users are created with non-valid Linux passwords. Therefore, the CMS User will be blocked from logging in with the Local Login method if the CMS User is not administered for LDAP authentication.

CMS users are not restricted to using the Web Client, PC Supervisor client or the ASCII interface. If customers want to restrict users to the Enterprise Login method, do not set the user for LDAP authentication and do not assign a valid Linux password to the user.

3. Web Client User Login Screens

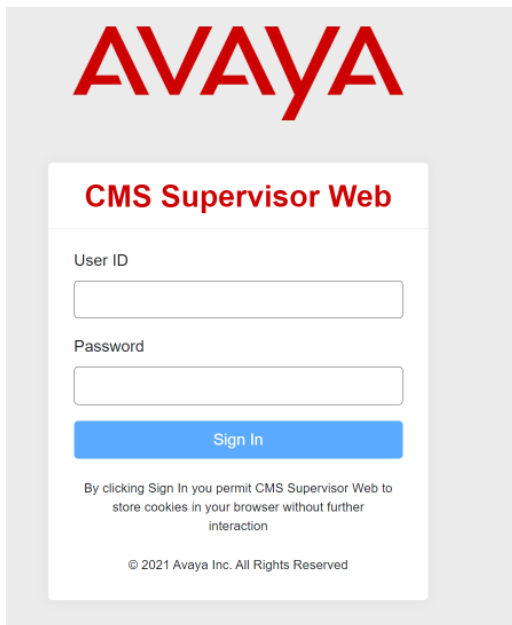
This section reviews what the CMS User sees with Local Login versus Enterprise Login.

Note that Enterprise Login is only available on the CMS Web Client. Therefore, this document only reviews the differences the user will see from the Web Client Login Screens. The PC Client Login has not been changed and does not support Enterprise Login.

Local Login:

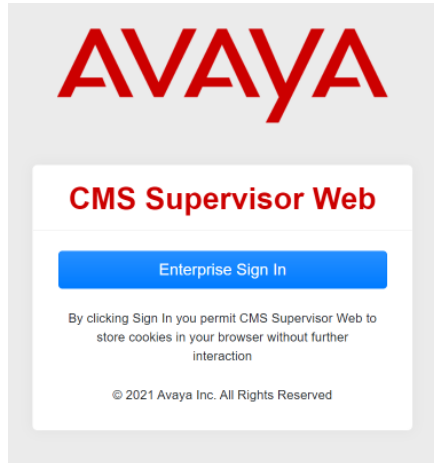
The user sees the following Web Client login screen for local CMS logins, with or without LDAP password authentication.

The user enters their CMS User ID and Password and clicks the 'Sign In' button.



Enterprise Login:

The user sees the following Web Client login screen for Enterprise Login. This screen is new with 19.2.0.2 and the availability of the Enterprise Login method.



When the user clicks the 'Enterprise Sign In' button, the login authentication process is managed by Microsoft Azure. The user is prompted for their login credentials according to how Microsoft Azure is configured. If Microsoft Azure is configured for multifactor authentication, the user will be prompted to enter the pass code sent to the user by Microsoft Azure.

Note that a CMS User ID is still required to be created for Enterprise Login. The User ID must match exactly the Microsoft Azure User ID.

4. Authentication Configuration Helper Tool

A help command line program is available to help with the login.properties configuration.

```
/opt/cmsweb/bin/configlogin.sh
```

This can be used instead of hand crafting the login.properties file.

Example Usage:

```
# ./configlogin.sh

Login option(s) for super users:
  1) Use Linux password? (y/n) default (y):
  2) Use Azure? (y/n) default (n): y
Login option(s) for regular users:
  1) Use Linux password? (y/n) default (y):
  2) Use Azure? (y/n) default (n): y
Enter Azure login URL: (default https://login.microsoftonline.com)
Enter token verificaiton URL: (default https://graph.microsoft.com)
Enter application/client ID: (default xxxxxx-yyyy-zzzz-927f-7c3cc88bblee)
Enter Tenant ID: (default aaaa123-b345-678c-d910-4939248f6b87)
Enter host:port for CMS Web URL : (default cmscms.dr.avaya.com:8443)
```

Enable login certificate checking? (y/n) default (n):

New configuration:

```
login.superUserOption=Password,Azure
login.regularUserOption=Password,Azure
login.aad.clientId= xxxxxx-yyyy-zzzz-927f-7c3cc88bblee
login.aad.authority=https://login.microsoftonline.com/ aaaa123-b345-678c-d910-4939248f6b87
login.aad.msGraphEndpointHost=https://graph.microsoft.com
login.aad.redirectUriSignin=https://cmscms.dr.avaya.com:8443/CMSWeb/
login.aad.postLogoutRedirectUri=https://cmscms.dr.avaya.com:8443/CMSWeb/
login.requiredCertificate=no
Save the new configuration? (y/n) y
```

New configuration saved.

5. CMS Enterprise Configuration

It is assumed that customers implementing Enterprise Login are familiar with Microsoft Azure. It is not the intent of this document to explain how to configure Microsoft Azure nor how to setup Microsoft Azure for multifactor authentication.

It is recommended that the reader review this entire section prior to beginning any administration. It is also recommended to configure Microsoft Azure first, then configure the CMS.

CMS Configuration Details:

The CMS configuration is managed in the `/opt/cmsweb/data/login.properties` file.

Customers must login as the 'root' login on the CMS server and edit the file. This document explains each variable to set and the options available.

In the `/opt/cmsweb/data/login.properties` the following variables should be set:

```
login.superUserOption=<set to desired option>
```

The 'superUserOption' applies ONLY to the 'cms' and 'cmssvc' logins.

Valid options for this variable are:

- Password
- Azure

Password: uses the Local Login method (Password administered on the CMS).

Azure: uses the Enterprise Login Method (authentication provided by Microsoft Azure).

```
login.regularUserOption=<set to desired option>
```

The 'regularUserOption' applies to ALL user logins EXCEPT the 'cms' and 'cmssvc' logins.
Valid options for this variable are:

- Password
- Azure

Password: uses the Local Login method (Password administered on the CMS).

Azure: uses the Enterprise Login Method (authentication provided by Microsoft Azure).

```
login.aad.clientId=<application id>
```

This is the Application ID assigned by Microsoft Azure when the CMS application is registered.

See the

Microsoft Azure Example Configuration section of this document. The Application (client) ID is obtained in step 5 of the Microsoft Azure Configuration Example:.

```
login.aad.authority=https://login.microsoftonline.com/<tenant id>
```

This is the Tenant ID assigned by Microsoft Azure where the CMS application is registered.

See the

Microsoft Azure Example Configuration section of this document. The Directory (tenant) ID is obtained in step 5 of the Microsoft Azure Configuration Example:.

```
login.aad.msGraphEndpointHost=https://graph.microsoft.com
```

This is the graph endpoint that is the token verification URL.

```
login.aad.redirectUriSignin=https://<cmshost>:8443/CMSWeb/
```

This is the CMS URL to access the Web Client.

This information shall match the Redirect URI configured in step 9 in the Microsoft Azure Configuration Example: section of this document.

Note: Optionally customers can change the port number to a port other than 8443. The port used for the CMS shall be that administered for the Microsoft Azure integration.

```
login.aad.postLogoutRedirectUri=https://<cmshost>:8443/CMSWeb/
```

This is the CMS URL to access the Web Client.

This value shall match the Front-channel Logout URL configured in step 9 of the Microsoft Azure Configuration Example: section of this document.

Note: Optionally customers can change the port number to a port other than 8443. The port used for CMS shall be that administered for the Microsoft Azure integration.

After edits are completed in the /opt/cmsweb/data/login.properties file, the web client process must be stopped and restarted for changes to take effect.

To stop and start the CMS web process, issue the following commands:

```
# cmsweb stop  
# cmsweb start
```

Note: Restarting the web client process does not require down-time on the CMS. When the web client process is restarted any active web client logins will be canceled, and users can login again and all changes made in the /opt/cmsweb/data/login.properties file will be in effect.

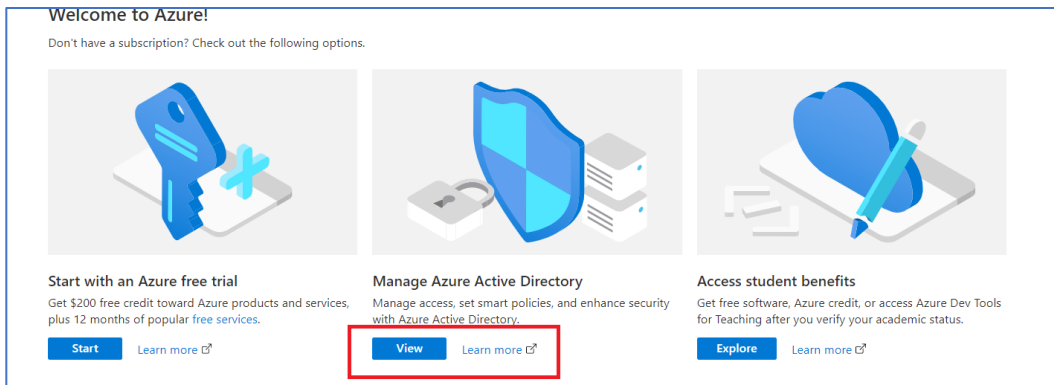
6. Microsoft Azure Example Configuration

This section provides an example of how to configure Microsoft Azure. It is only an example and it not intended to provide full training or explanations of how Microsoft Azure should be configured.

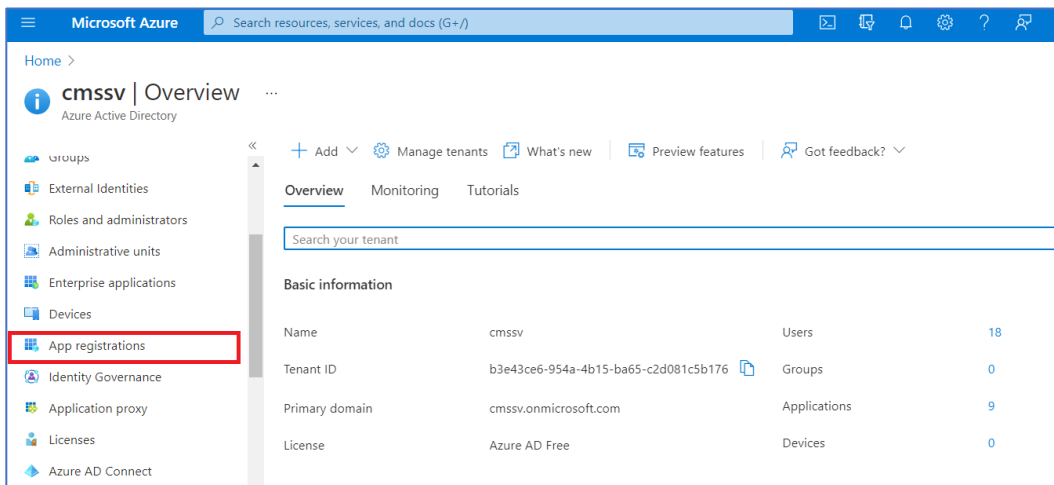
Microsoft Azure should be configured to add a Single-Page application for CMS Web Client and to set the Redirect URI value to match the CMS Web Client URL configured on the customer CMS system.

Microsoft Azure Configuration Example:

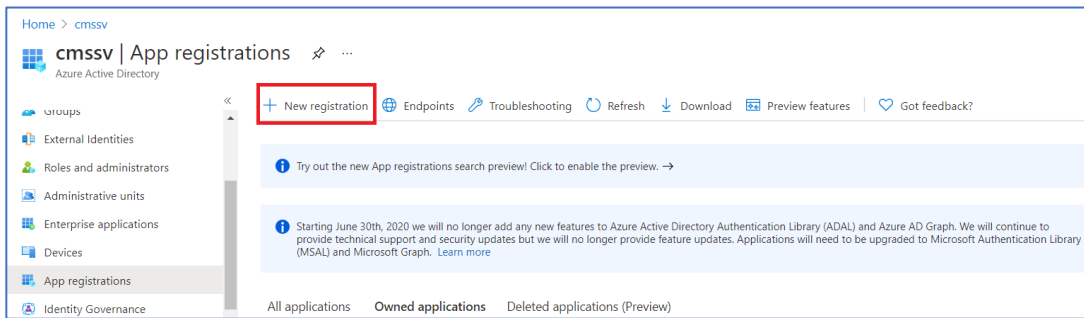
- 1) Login to Microsoft Azure portal. On the home page click on view button of “Manage Azure Active directory”.



- 2) On the left side of the screen, click on “App registrations”.

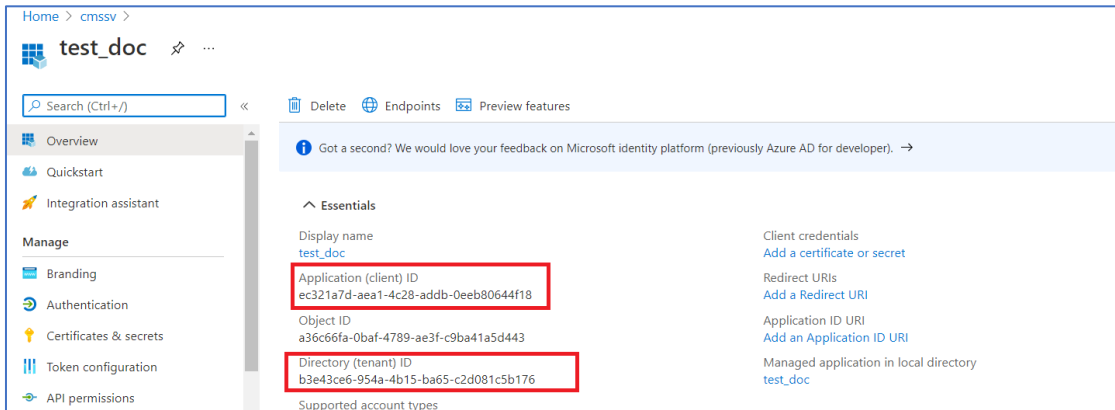


3) Then click on “New registration”.

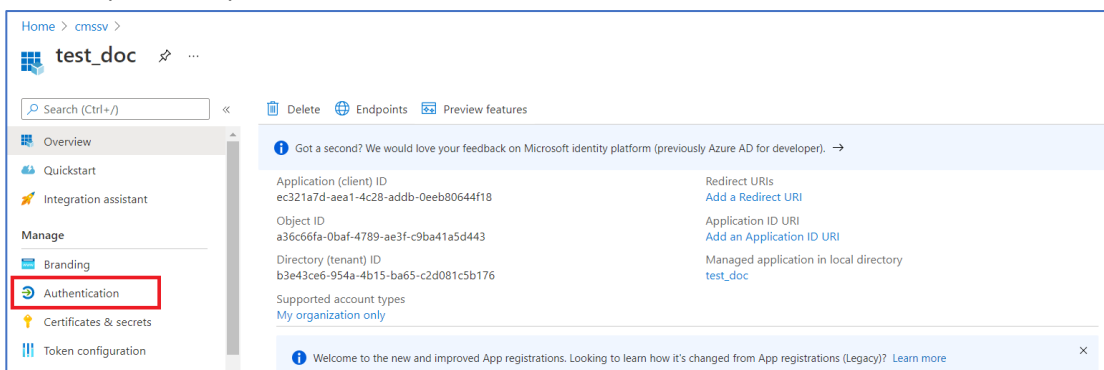


4) The “Register an application” window is displayed. Now provide the application name and supported account types. Then click on “Register”.

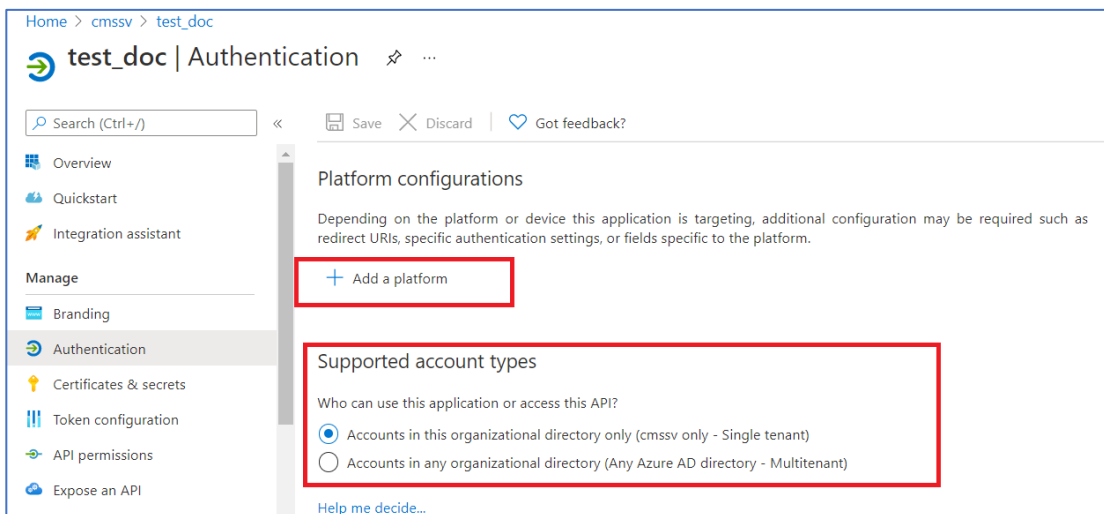
5) After clicking on the *Register* button, the application is created and the information in the screenshot below is displayed. It is recommended the user write down the Application (client) ID and Directory (tenant) ID. These values will be required for configuration of the CMS.



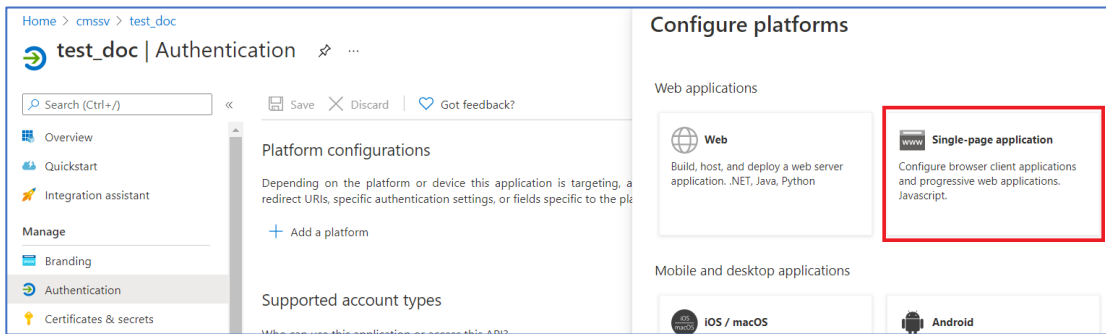
6) Once step 5 is completed click on the “Authentication” button on the left side of the screen.



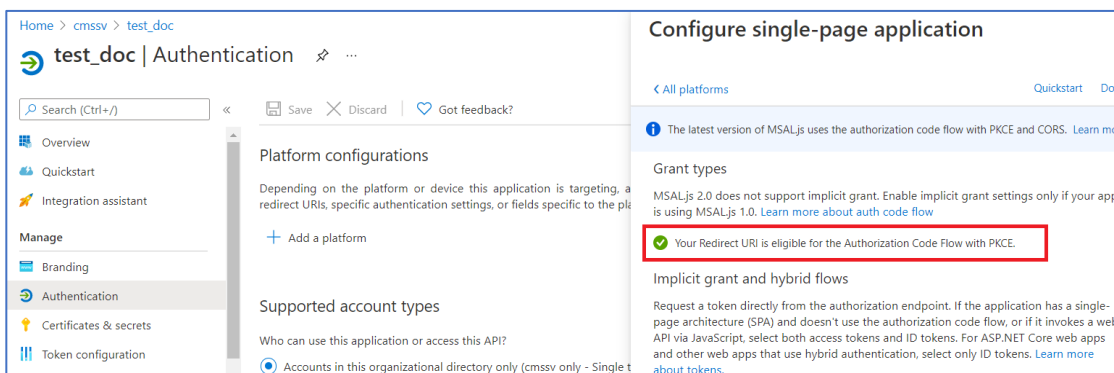
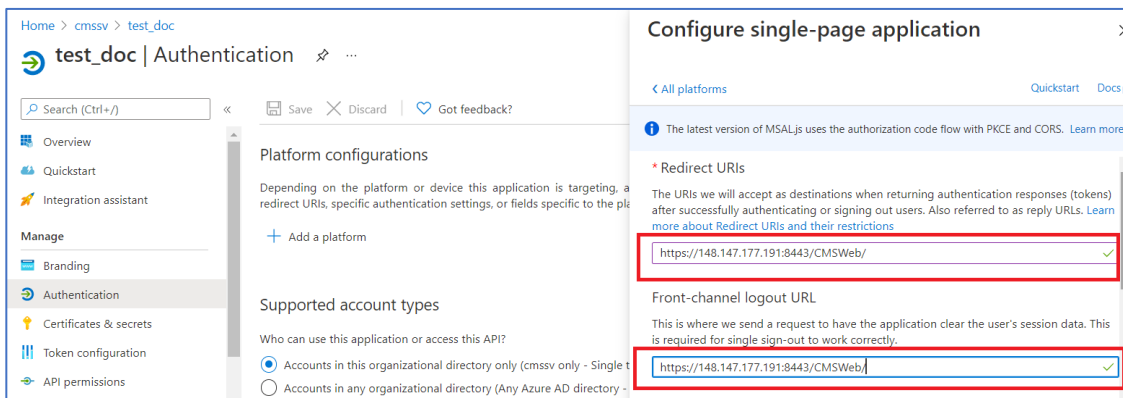
7) Next select “Supported account types” based on your requirements. Then click on “Add a platform”.



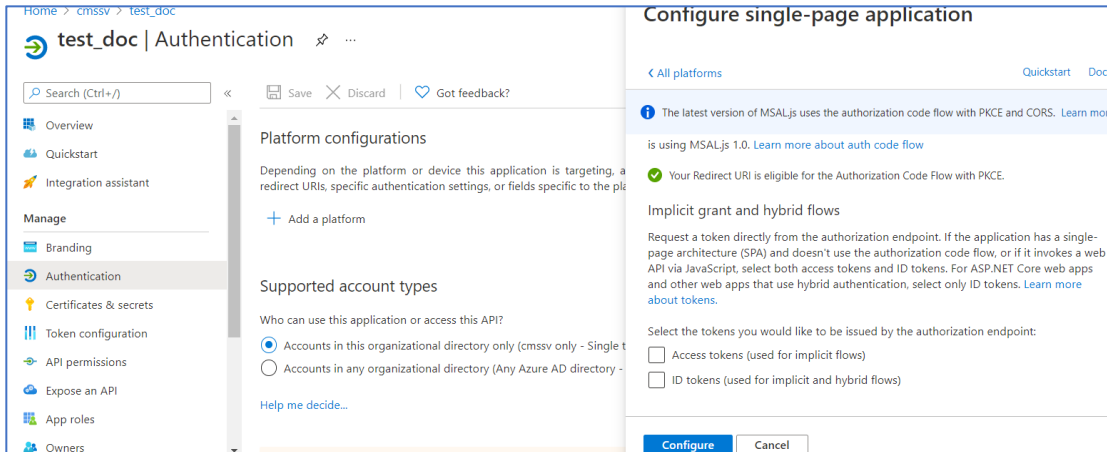
8) Next click on “Single-page application”.



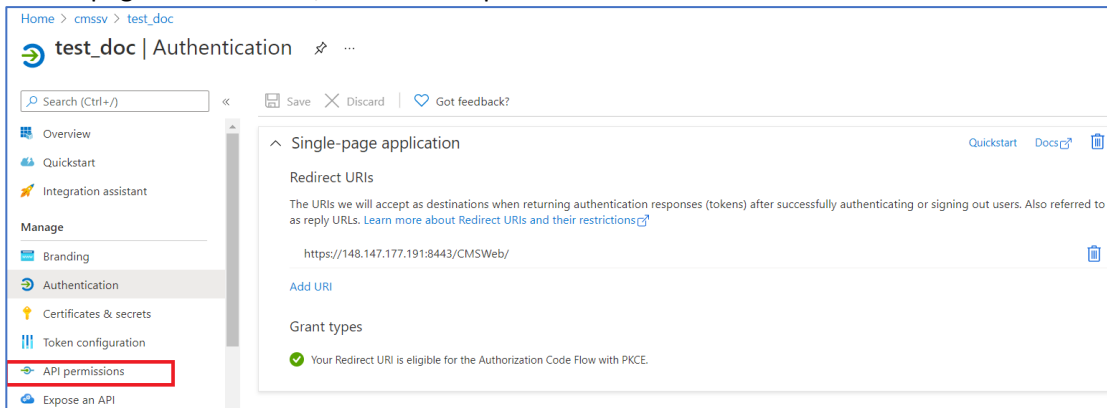
9) After clicking on “Single-page application”, the configuration for single-page application is presented. See below. The values entered here are the values required for configuring the CMS login.properties file.



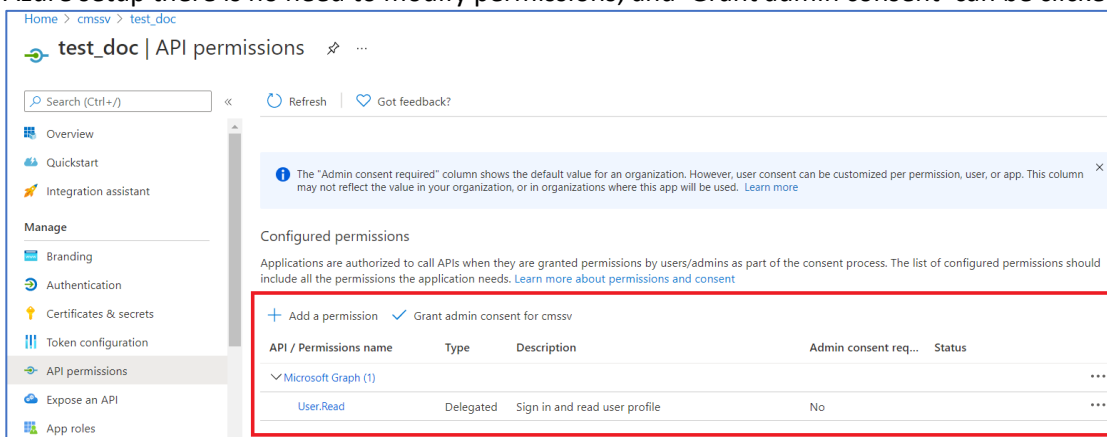
10) On the same page, scroll down and check that the “Implicit grant and hybrid flows” settings match those shown here. Once verified, click on “Configure” button.



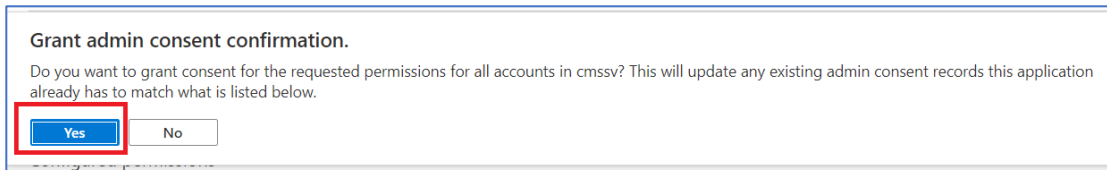
11) On the page shown below, click on “API permissions”.



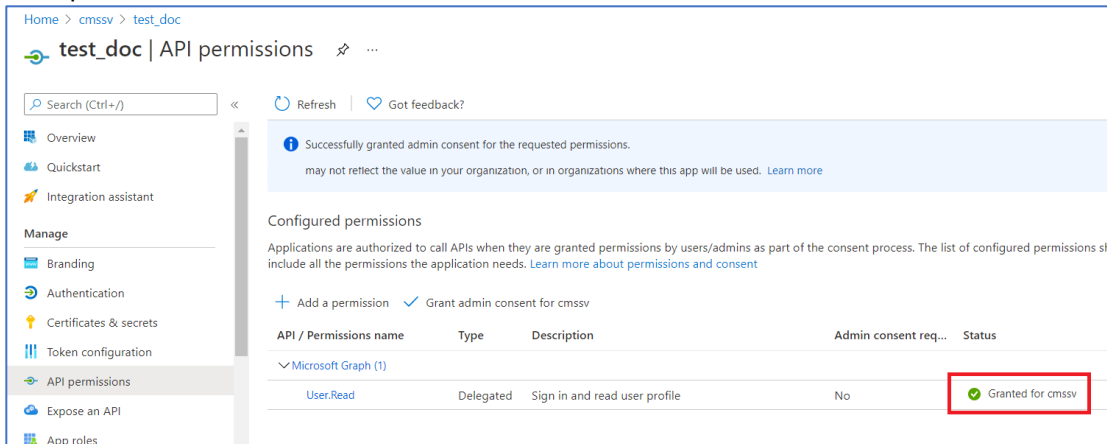
12) Initially the permission will look like the following screen shot. If the same permission is seen on the Azure setup there is no need to modify permissions, and ‘Grant admin consent’ can be clicked.



13) The “Grant admin consent confirmation” window will open. Click on “Yes” to confirm.



14) Then permission will look like the below screen shot.



This completes the Microsoft Azure example. The CMS configuration steps can now proceed.

7. Certificate Login Authentication configuration

It is assumed that customers implementing Certificate Login Authentication are familiar with Cert management and if required CAC's. It is not the intent of this document to explain how to configure or obtain personal certs.

Cert Setup Details

1. The root certificate of the relevant Certificate Authority has to be imported into the CMS web key store. This is located at:
 - `/opt/cmsweb/cert/cmsweb.jks`

An example command to perform this import is as follows:

- `keytool -import -trustcacerts -alias <alias> -file <cert file> -keystore /opt/cmsweb/cert/cmsweb.jks`

CMS Configuration Details:

The CMS configuration is managed in the `/opt/cmsweb/data/login.properties` file.

Customers must login as the 'root' login on the CMS server and edit the file. This document explains each variable to set and the options available.

In the `/opt/cmsweb/data/login.properties` the following variables should be set:

`login.requireCertificate=<Yes/No>`

Set to 'Yes'

After edits are completed in the `/opt/cmsweb/data/login.properties` file, the web client process must be stopped and restarted for changes to take effect.

To stop and start the CMS web process, issue the following commands:

```
# cmsweb stop
# cmsweb start
```

Note: Restarting the web client process does not require down-time on the CMS. When the web client process is restarted any active web client logins will be canceled, and users can login again and all changes made in the `/opt/cmsweb/data/login.properties` file will be in effect.

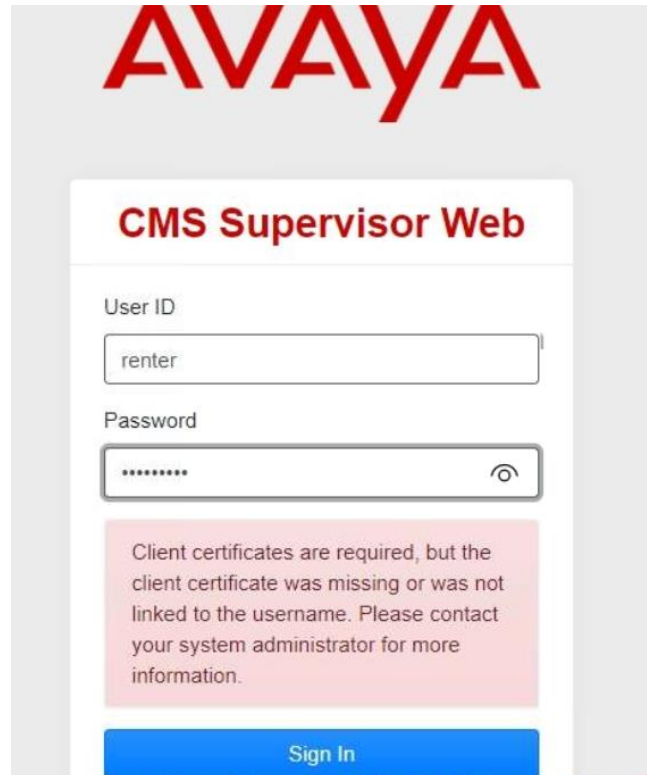
8. Certificate Login Authentication Operation

When the feature is activated, CMS will send the browser a list of trusted certificate authorities stored in the `cmsweb.jks` file. The browser will select or prompt the user to select a personal certificate to send to the CMS. This personal certificate may be stored on a CAC or in another location, possibly on the user's PC. If there is no matching personal certificate, the user will not be able to access the CMS login page. An error like the following will be displayed.



During login, CMS will obtain the client personal certificate from the browser request and verify the CN (common name) in the certificate against the user id and the username. If the CN does not match either the user id or the username, the login will be rejected.

An error like the following will be displayed.



9. Pre-Login Banner

It is possible to enable/modify the banner message displayed before being presented with the login screen to the CMS Supervisor Web Client interface. To enable/modify the pre-login message, you must edit the following file and add the desired message:

`/opt/cmsweb/preloginbanner/banner.txt`

10. Troubleshooting Tips

After following all the configuration steps, if CMS users see the Enterprise Login screen, yet cannot successfully login, the following should be verified:

- Verify the CMS can connect to the network using the DNS. If the CMS cannot be recognized by DNS, or the CMS and Microsoft Azure cannot 'see' each other on the network, the login cannot succeed.
- Verify that the user is created in BOTH CMS and in Microsoft Azure.
- Verify the username is EXACTLY the same on both products.

©2022 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.