

Application Portal

User Manual

Table of Contents

Introduction	3
Invitation Email	4
Logging in DHCS Application portal	5
Steps.....	5
Access an Application.....	9
Multi-Factor Authentication (MFA) Setup	10
Background.....	10
Steps.....	10
Navigating to PEDI application	17

Introduction

The DHCS Application Portal uses Microsoft Office 365 / Azure Active Directory (AAD) for providing access to DHCS Applications. This document describes the steps for internal DHCS staff and external users to access DHCS applications that are integrated with the DHCS Application Portal.

Users login to the DHCS Application Portal using their Microsoft Office 365 (AAD) account credentials or accept an invitation from the DHCS Directory Administrator.

More information provided in the "[Logging In](#)" section below.

Also, when first logging into the DHCS Application Portal or when accessing a DHCS Application, users are prompted to set up additional security verification, also referred to as Multi-Factor Authentication (MFA). MFA is an additional security step that helps protect your account by making it harder for other people to break in.

More information provided in the "[Multi-Factor Authentication \(MFA\) Setup](#)" section below.

Invitation Email

When an external member (non-DHCS staff) is given permission to access a DHCS application, the member receives an invitation email with an “Accept Invitation” link to select and “Get Started” link to initiate the login process.

For some applications, the application administrator may choose to send a custom email that will look different from the one below. In these cases, it is recommended that members follow the steps in the [“Logging In”](#) section below.

When a new external member is added to a Security Group, the member receives an invitation email with at “Accept Invitation” link that appears as follows. The member selects the “Accept Invitation” link to initiate the log process.

From: Microsoft Invitations on behalf of California Department of Health Care Services <invites@microsoft.com>

 Please only act on this email if you trust the individual and organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.

Sender: DHCS IT Administrator
Organization: California Department of Health Care Services
Domain: cadhcs.onmicrosoft.com

If you accept this invitation, you'll be sent to [DHCS Azure Application Link](#)

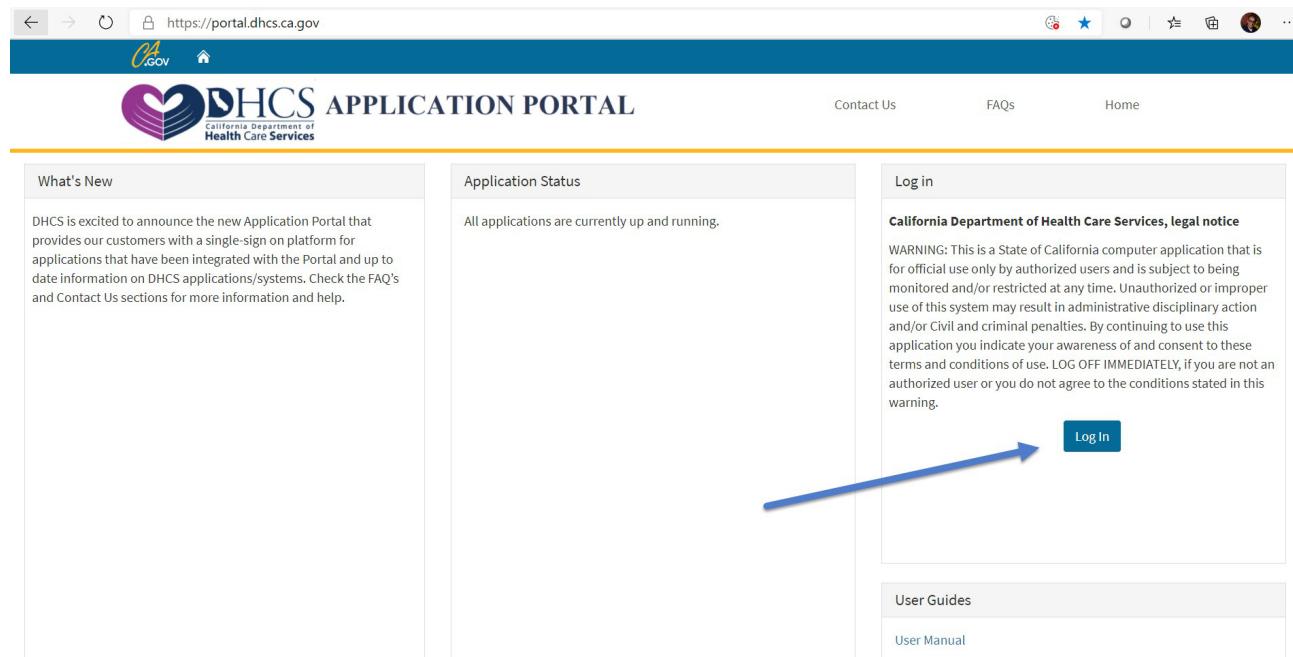
[Accept invitation](#)



Logging in DHCS Application portal

Steps

1. From the DHCS Application Portal, select Log In



What's New

DHCS is excited to announce the new Application Portal that provides our customers with a single-sign on platform for applications that have been integrated with the Portal and up to date information on DHCS applications/systems. Check the FAQ's and Contact Us sections for more information and help.

Application Status

All applications are currently up and running.

Log in

California Department of Health Care Services, legal notice

WARNING: This is a State of California computer application that is for official use only by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or Civil and criminal penalties. By continuing to use this application you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY, if you are not an authorized user or you do not agree to the conditions stated in this warning.

Log In

User Guides

User Manual

The log in screens may look different based on the browser used and the organizational configuration. Please see the following examples. Your experiences may vary.



CALIFORNIA DEPARTMENT OF
HEALTH CARE SERVICES



Edge and IE

2. Enter work email address, select Next

Sign in

firstname.lastname@dhcs.ca.gov

[Can't access your account?](#)

[Sign in options](#)

[Next](#)

WARNING: This is a State of California system for official use by authorized users; subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system shall be subject to disciplinary action, prosecution or both.

Enter password

Microsoft

firstname.lastname@gmail.com

Enter password

[Forgot password?](#)

[Sign in](#)

Then...

CA Dept. of Health Care Services

[Sign in with your organizational account](#)

firstname.lastname@dhcs.ca.gov

[Sign in](#)

Then... My Apps ▾

Chrome

3. Pick an account or Use another account

Pick an account

 First.Last @dhcs.ca.gov

 Use another account



If dhcs.ca.gov or known...

CA Dept. of Health Care Services

Sign in with your organizational account

Sign in



If Using another account unknown to Microsoft...

Sign in

firstname.lastname@gmail.com

Can't access your account?

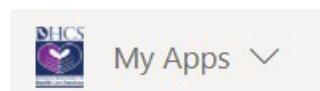
Sign-in options

Back **Next**

WARNING: This is a State of California system for official use by authorized users; subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system shall be subject to disciplinary action, prosecution or both.



Then...



Then...

Microsoft

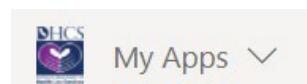
firstname.lastname@gmail.com

Enter password

[Forgot password?](#)

Sign in

Then...

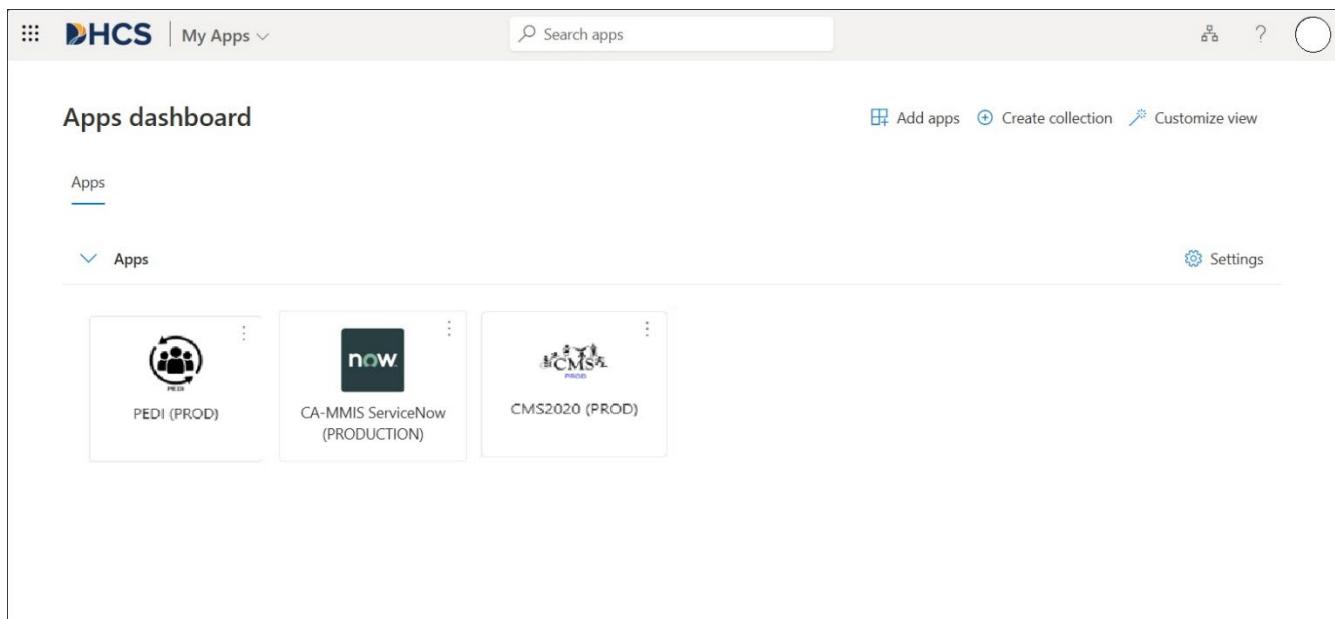


4. If logging in for the first time, you may be prompted to set up Additional Security Verification, commonly known as Multi-Factor Authentication (MFA).

More information provided in the "[Multi-Factor Authentication \(MFA\) Setup](#)" section below.

If MFA setup was previously completed, you may be prompted to authenticate using the method chosen. Follow the onscreen instructions to complete the MFA verification.

5. Once successfully logged in, the DHCS Application Gallery (My Apps page) is displayed. The My Apps page displays all the DHCS applications you have access to. Only applications that have been integrated with the DHCS Application Portal are displayed.



Access an Application

1. On the My Apps page, click on an application you want to access.
The application opens in a new tab in the browser.
2. If accessing the application for the first time, you may be prompted to set up Multi-Factor Authentication.

More information provided in the "[Multi-Factor Authentication \(MFA\) Setup](#)" section below.

If a user has previously completed the MFA setup, you may be prompted to authenticate using the method chosen. Follow onscreen instructions to complete the MFA verification.

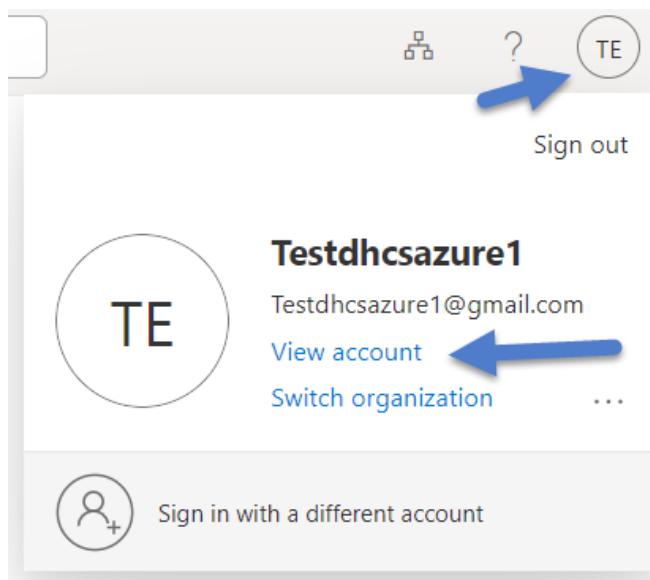
Multi-Factor Authentication (MFA) Setup

Background

When first logging into the DHCS Application Portal, members are prompted to set up additional security verification also referred to as Multi-Factor Authentication (MFA). MFA is an additional security step that helps protect your account by making it harder for others to break in. The following steps describe how to set up and update MFA settings.

Steps

1. Select your Account Manager icon and choose View account:

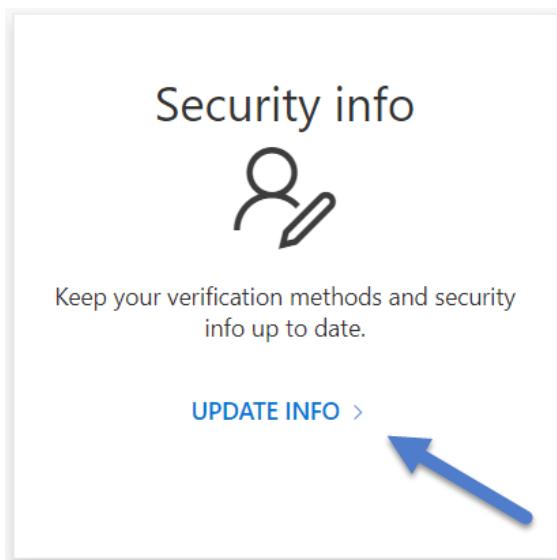




CALIFORNIA DEPARTMENT OF
HEALTH CARE SERVICES



2. Select UPDATE INFO >



3. From the Security info page, add, change or delete a method. In this example, a Default sign-in method of Phone-text is set. Select + Add method

Note: DHCS staff cannot update the office phone through these steps. Office phone information must be updated through the Global Address List (GAL) profile update process.

4. From Add a method, select the drop-down list and a method.
Follow the onscreen navigation to complete the setup.

Add a sign-in method X

 Microsoft Authenticator	Approve sign-in requests or use one-time codes
 Phone	Get a call or text to sign in with a code
 Alternate phone	Get a call or text to sign in with a code
 Office phone	Get a call or text to sign in with a code

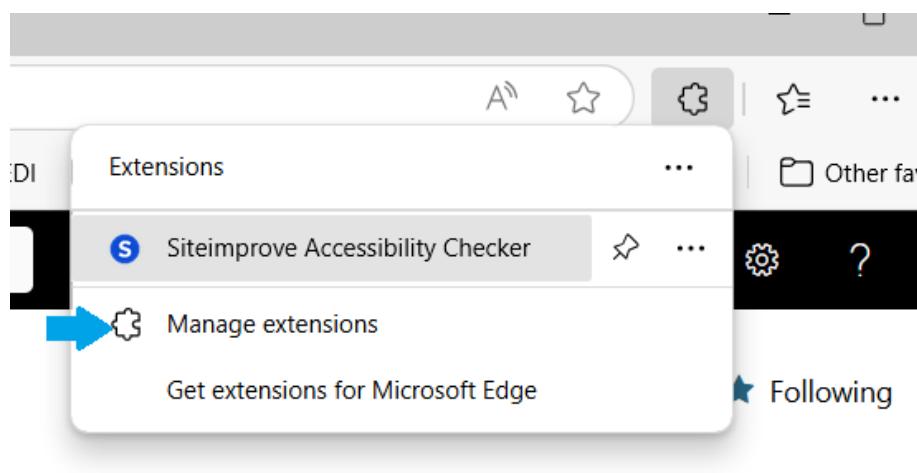
For more detailed information and screen prints, please refer to
[Microsoft Multi-Factor Authentication end user first time web article](#)

Contact method	Description
Mobile app	<ul style="list-style-type: none"> Receive notifications for verification. This option pushes a notification to the authenticator app on your smartphone or tablet. View the notification and, if it is legitimate, select Authenticate in the app. Your work or school may require that you enter a PIN before you authenticate. Use verification code. In this mode, the app generates a verification code that updates every 30 seconds. Enter the most current verification code in the sign-in screen. The Microsoft Authenticator app is available for Android and iOS.
Authentication phone	<ul style="list-style-type: none"> Phone call places an automated voice call to the phone number you provide. Answer the call and press the pound key (#) on the phone keypad to authenticate. Text message ends a text message containing a verification code. Following the prompt in the text, either reply to the text message or enter the verification code provided into the sign-in interface.
Office phone	Places an automated voice call to the phone number you provide. Answer the call and press the pound key (#) on the phone keypad to authenticate.

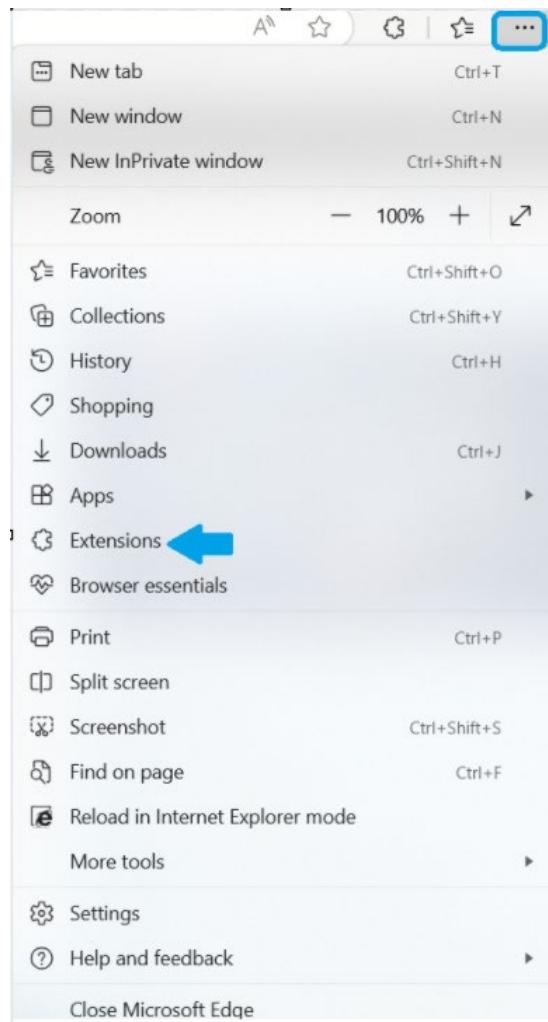
DHCS uses Microsoft Multi-Factor Authenticator application to receive an approved sign-in request. Check with your organization to decide whether Microsoft Authenticator application is the best option for you.

Also, Edge and Chrome browsers do have extensions to add a third-party multi-factor authenticator application to the browser themselves that do not require the application to be installed on your own mobile device.

Edge and Chrome browser extension are located by clicking the puzzle icon

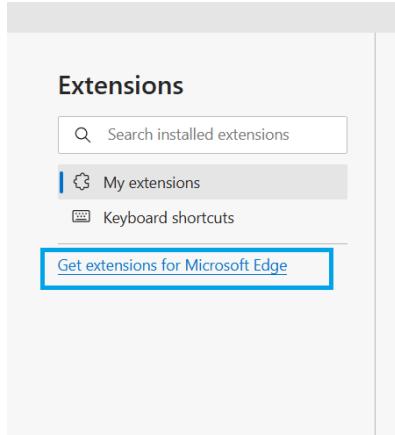


Or by clicking the three dots to select the settings and more drop down.



Select “Extensions” and you will be brought to manage extensions page choose “Get extensions for Microsoft Edge”, you will be redirected to the Microsoft Edge Add-ons page. Within the search field type “Authenticator” to search for third-party authenticator apps.

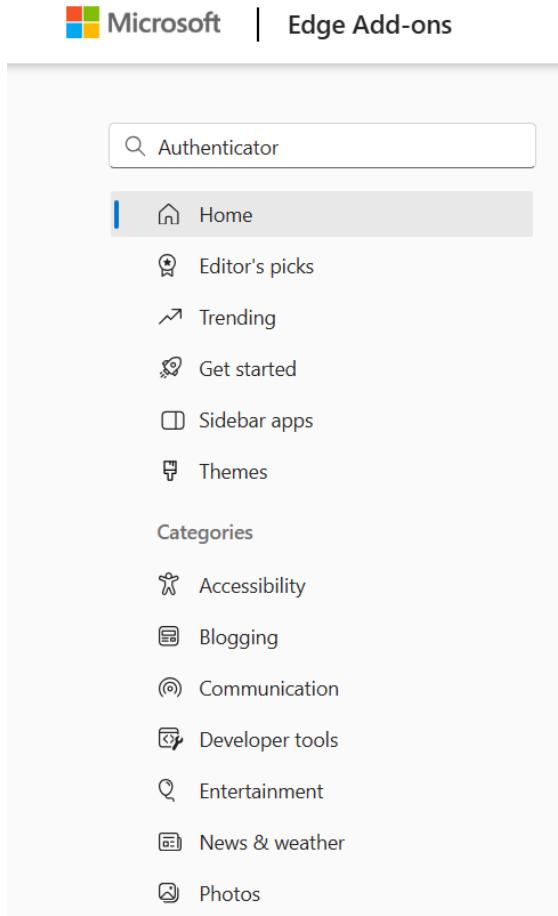
Mange Extensions page



Extensions

- Search installed extensions
- My extensions **Get extensions for Microsoft Edge**
- Keyboard shortcuts

Microsoft Edge Add-ons page



Microsoft | Edge Add-ons

Authenticator

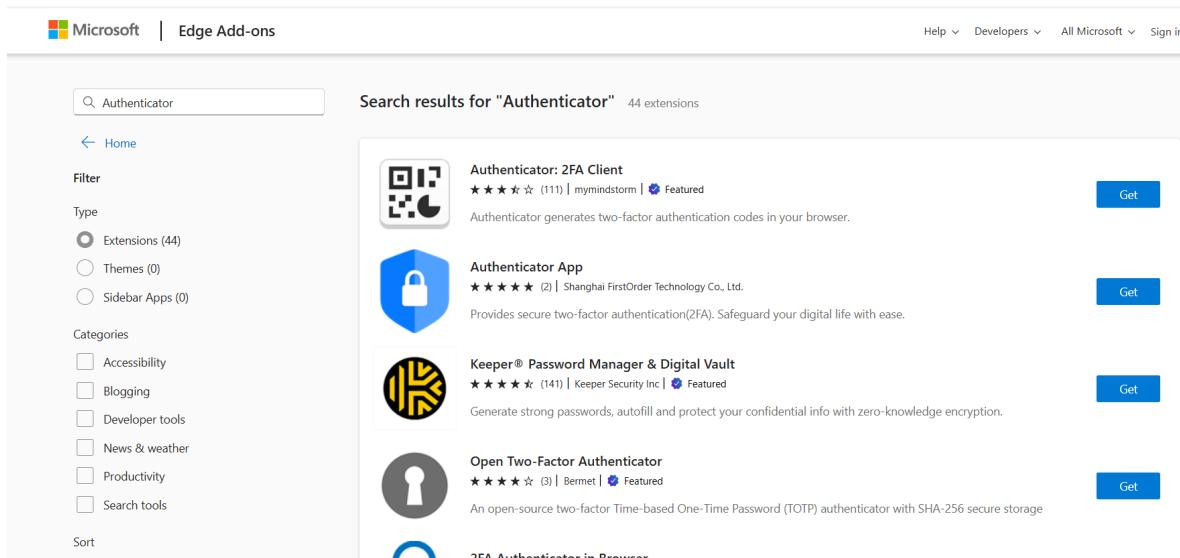
Home

- Editor's picks
- Trending
- Get started
- Sidebar apps
- Themes

Categories

- Accessibility
- Blogging
- Communication
- Developer tools
- Entertainment
- News & weather
- Photos

Third party authenticator application results page

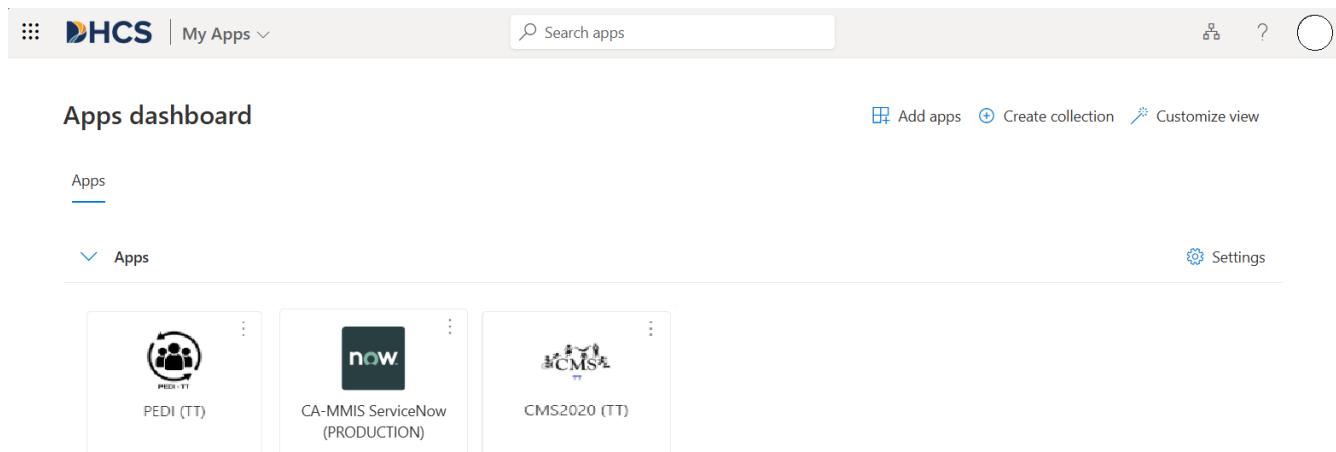


The screenshot shows the Microsoft Edge Add-ons search results for "Authenticator". The search bar at the top contains "Authenticator". Below the search bar, the text "Search results for 'Authenticator'" and "44 extensions" are displayed. The results list four items, each with a "Get" button:

- Authenticator: 2FA Client**
★ ★ ★ ★ ☆ (111) | mymindstorm | Featured
Authenticator generates two-factor authentication codes in your browser.
- Authenticator App**
★ ★ ★ ★ (2) | Shanghai FirstOrder Technology Co., Ltd.
Provides secure two-factor authentication(2FA). Safeguard your digital life with ease.
- Keeper® Password Manager & Digital Vault**
★ ★ ★ ★ ☆ (141) | Keeper Security Inc | Featured
Generate strong passwords, autofill and protect your confidential info with zero-knowledge encryption.
- Open Two-Factor Authenticator**
★ ★ ★ ☆ (3) | Bermet | Featured
An open-source two-factor Time-based One-Time Password (TOTP) authenticator with SHA-256 secure storage.

Navigating to PEDI application

Once logged into the DHCS Application portal the user will land on My Apps-Apps Dashboard. From the apps dashboard the user will select the PEDI tile to open PEDI homepage. Users will notice the login page has been removed due to the user now accessing PEDI through the DHCS application portal using the multi-factor authentication single sign-on.



(Similar icons will display based on security role)

Please note to register a new organization a new link will be updated on [CMS Net Provider Electronic Data Interchange](#) page.