Application Portal User Manual

Table of Contents

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 a Microsoft account.

More information provided in the "Logging In" section below.

When first logging into the DHCS Application Portal, users that belong to organizations that do not have Microsoft Office 365 (AAD) or Microsoft accounts will be asked to create a new Microsoft Account.

More information provided in the "Create a New Microsoft Account" 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

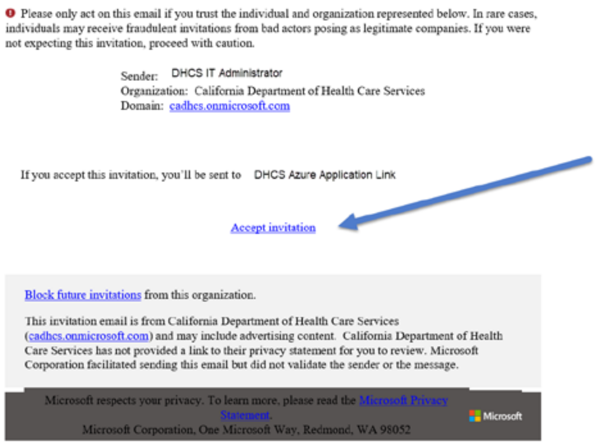
When an external member (non-DHCS staff) is given permission to access a DHCS application, the member receives an invitation email with an “Accept Invitation” link to select and “Get Started” link to initiate the login process.

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.

DHCS staff will not receive the invitation email. DHCS staff can login following the steps outlined 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

Block future invitations from this organization.

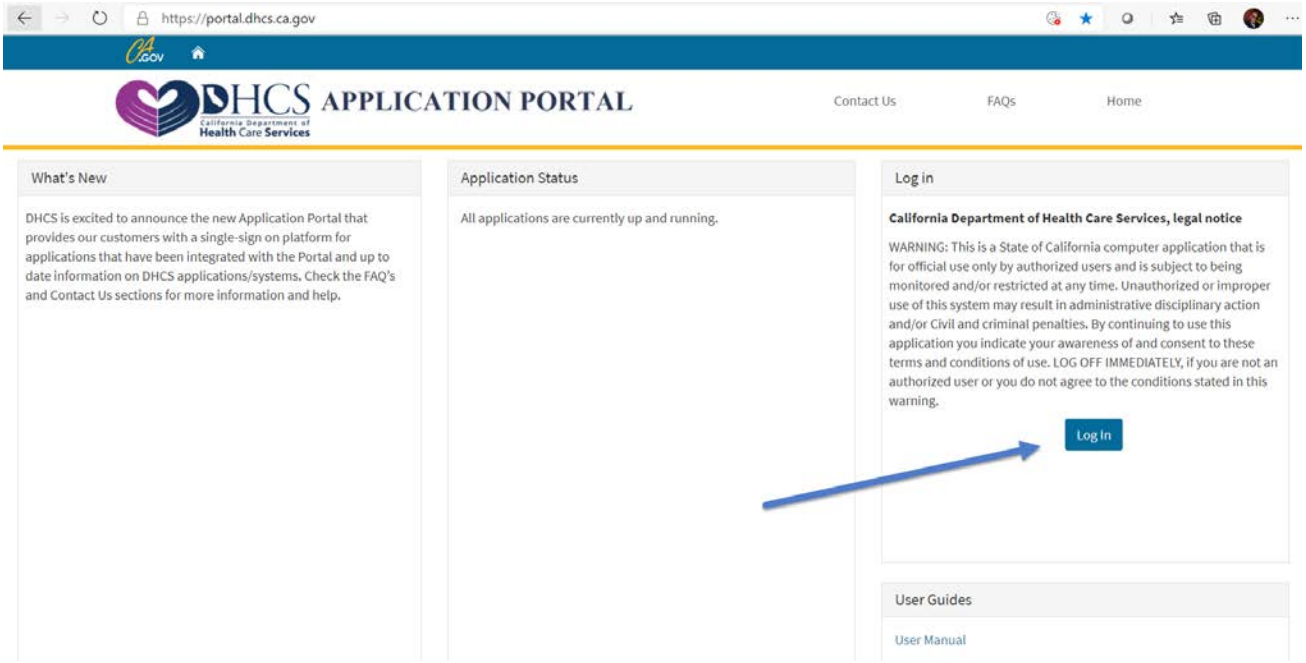
This invitation email is from California Department of Health Care Services (cadhcs.onmicrosoft.com) and may include advertising content. California Department of Health Care Services has not provided a link to their privacy statement for you to review. Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the Microsoft Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Logging In

Steps

1. From the DHCS Application Portal, select Log In


https://portal.dhcs.ca.gov
CA.GOV
DHCS APPLICATION PORTAL
California Department of Health Care Services
Contact Us
FAQs
Home
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.

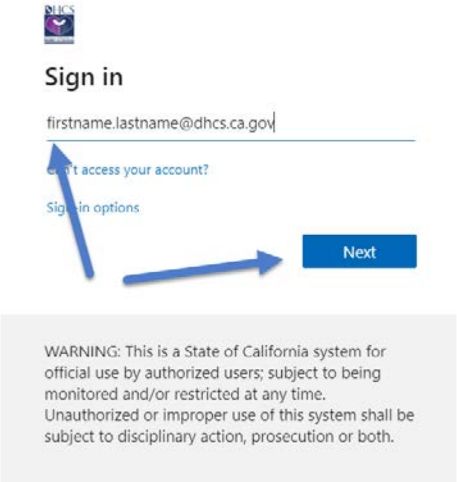
User Guides

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.

Edge and IE

2. Enter work email address, select Next

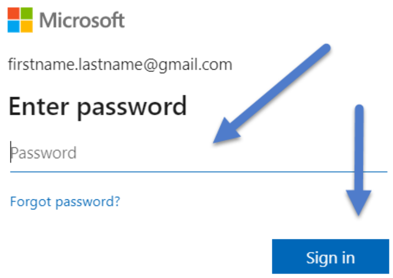


Sign in

firstname.lastname@dhcs.ca.gov

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.

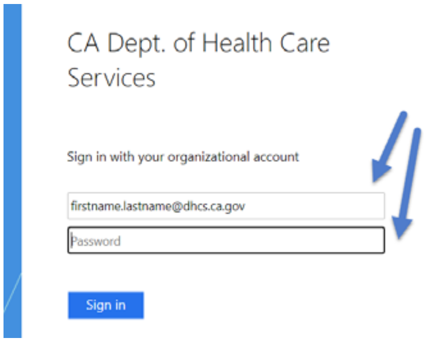
Enter password



firstname.lastname@gmail.com

Enter password

Then…

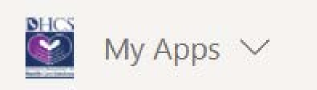


CA Dept. of Health Care Services

Sign in with your organizational account

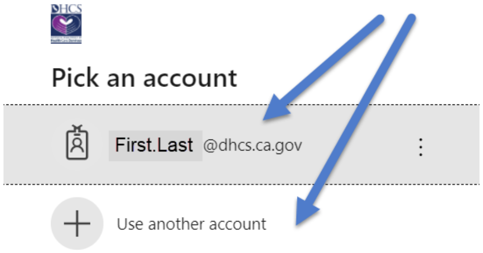
firstname.lastname@dhcs.ca.gov

Then…



Chrome

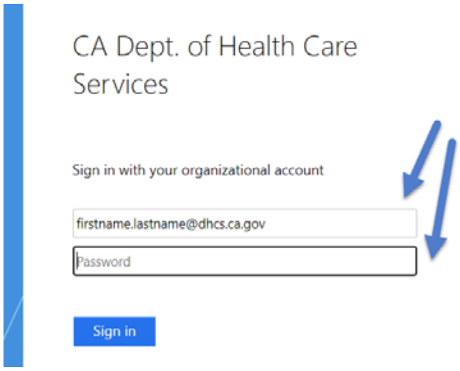
3. Pick an account or Use another account



Pick an account

First.Last @dhcs.ca.gov

If dhcs.ca.gov or known…

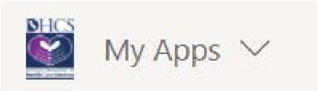


CA Dept. of Health Care Services

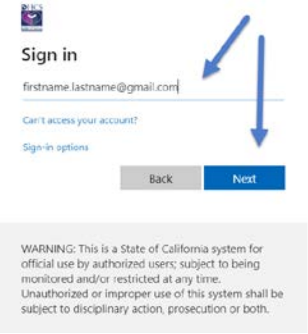
Sign in with your organizational account

firstname.lastname@dhcs.ca.gov

Then…



If Using another account unknown to Microsoft…

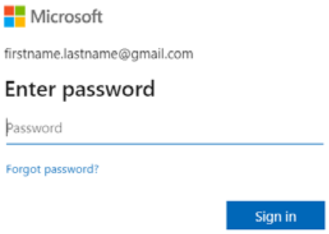


Sign in

firstname.lastname@gmail.com

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…

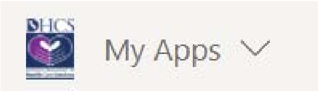


Microsoft

firstname.lastname@gmail.com

Enter password

Then…

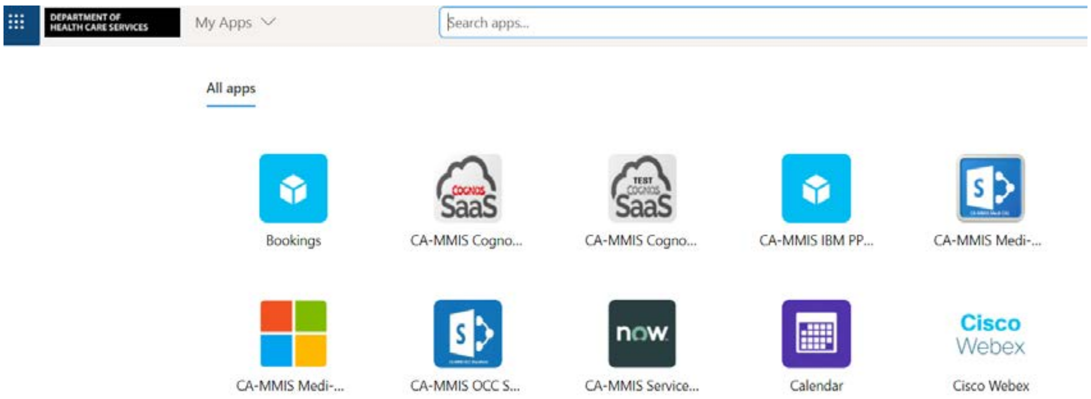


4. If logging in for the first time, you may be prompted to set up Additional Security Verification, commonly known as Multi-Factor Authentication (MFA).

   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.

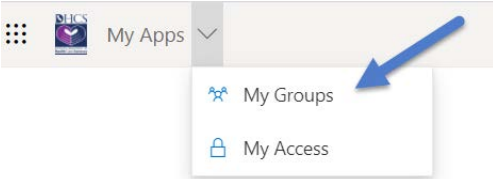
2. If accessing the application for the first time, you may be prompted to set up Multi-Factor Authentication.

   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.

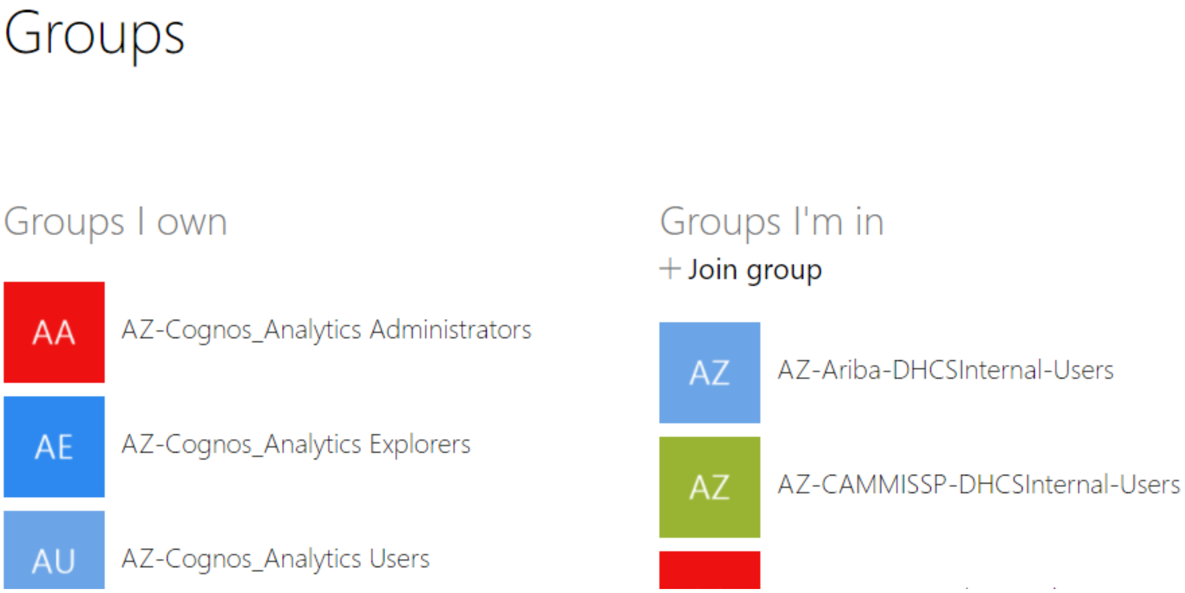
View Group Information

1. On the My Apps page, select the caret and choose My Groups



- Any Groups listed under ‘Groups I own’ indicate you are the Security Group Owner.

- Any Groups listed under ‘Groups I’m in’ indicate you are member of.


Groups

Groups I own

AA AZ-Cognos_Analytics Administrators

AE AZ-Cognos_Analytics Explorers

AU AZ-Cognos_Analytics Users

Groups I'm in

+ Join group

AZ AZ-Ariba-DHCSInternal-Users

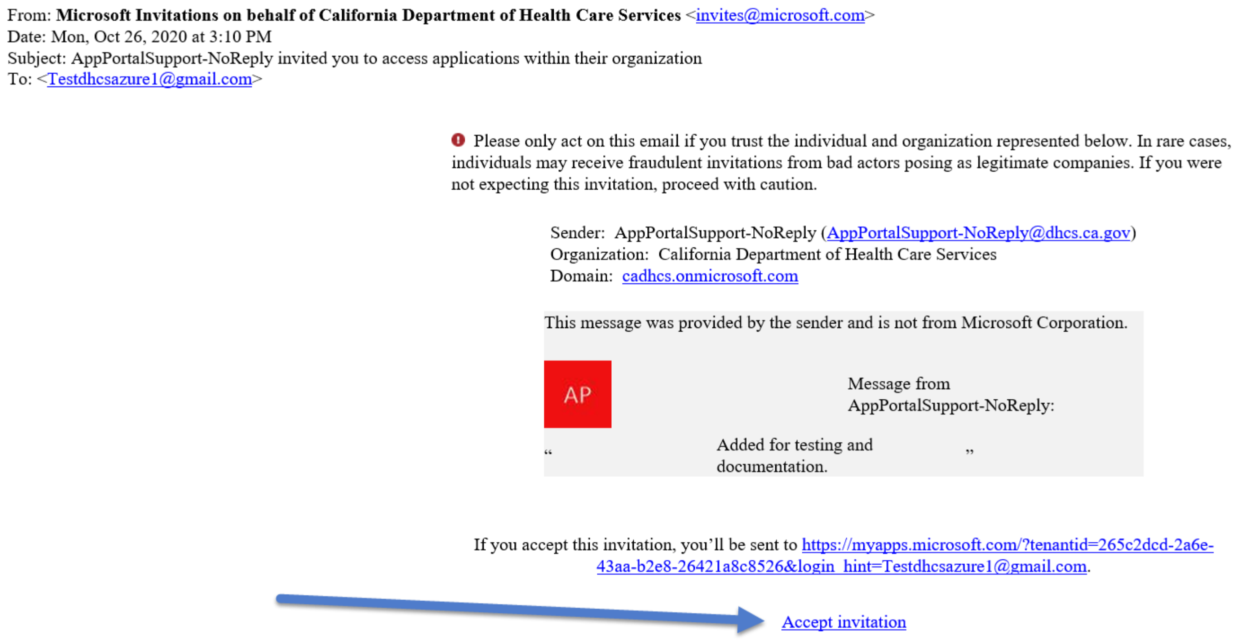
AZ AZ-CAMMISSP-DHCSInternal-Users

Select an Application tile in the ‘Groups I’m in’ to view the Group’s description and members.

Create a New Microsoft Account

Background

When first logging into the DHCS Application Portal, members are asked to create a new Microsoft account – if belonging to an organization without Microsoft Office 365 / Azure Active Directory (AAD) accounts. An email is received from Microsoft Invitations on behalf of California Department of Health Care Services. Select ‘Accept invitation’.



From: **Microsoft Invitations on behalf of California Department of Health Care Services** <invites@microsoft.com>
Date: Mon, Oct 26, 2020 at 3:10 PM
Subject: AppPortalSupport-NoReply invited you to access applications within their organization
To: <Testdhcsazure1@gmail.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: AppPortalSupport-NoReply (AppPortalSupport-NoReply@dhcs.ca.gov)
Organization: California Department of Health Care Services
Domain: cadhcs.onmicrosoft.com

This message was provided by the sender and is not from Microsoft Corporation.

Message from AppPortalSupport-NoReply:

“ Added for testing and documentation. ”

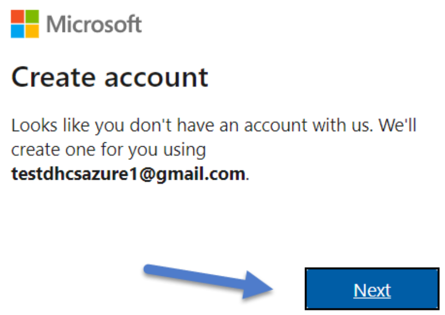
If you accept this invitation, you’ll be sent to https://myapps.microsoft.com/?tenantid=265c2dcd-2a6e-43aa-b2e8-26421a8c8526&login_hint=Testdhcsazure1@gmail.com.

Accept invitation

Please see the following for members to create a Microsoft account.

Steps

1. When prompted to Create account, select Next

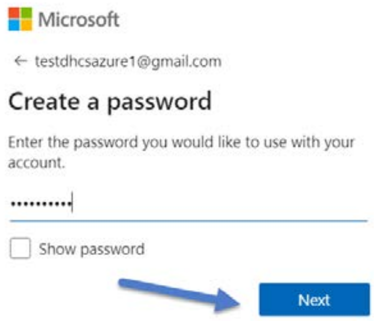


Microsoft

Create account

Looks like you don't have an account with us. We'll create one for you using **testdhcsazure1@gmail.com**.

2. When prompted to Create a password, enter a password and select Next



Microsoft

← testdhcsazure1@gmail.com

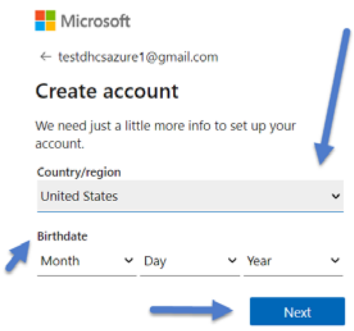
Create a password

Enter the password you would like to use with your account.

••••••••••

□ Show password

3. When prompted to Create account, enter Country/region and Birthdate, select Next



Microsoft

← testdhcsazure1@gmail.com

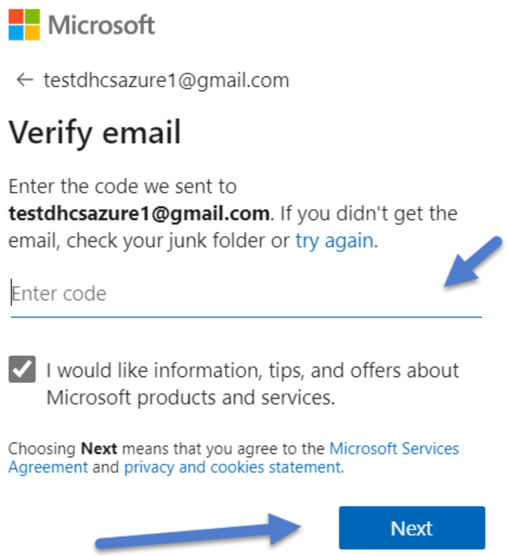
Create account

We need just a little more info to set up your account.

Country/region: United States

Birthdate: Month Day Year

4. When prompted to Verify email, enter the code sent to your email, select Next



Microsoft

← testdhcsazure1@gmail.com

Verify email

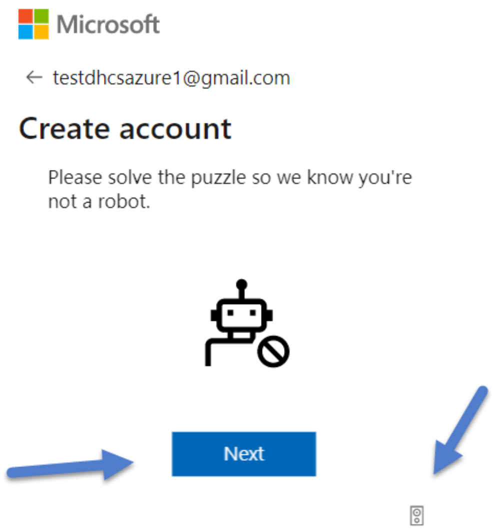
Enter the code we sent to **testdhcsazure1@gmail.com**. If you didn't get the email, check your junk folder or try again.

Enter code

☑ I would like information, tips, and offers about Microsoft products and services.

Choosing **Next** means that you agree to the Microsoft Services Agreement and privacy and cookies statement.

5. When prompted to Create account – Please solve the puzzle so we know you're not a robot. If robot checker not working - Select Audio Speaker, Play, enter the Challenge Answer, select Verify.

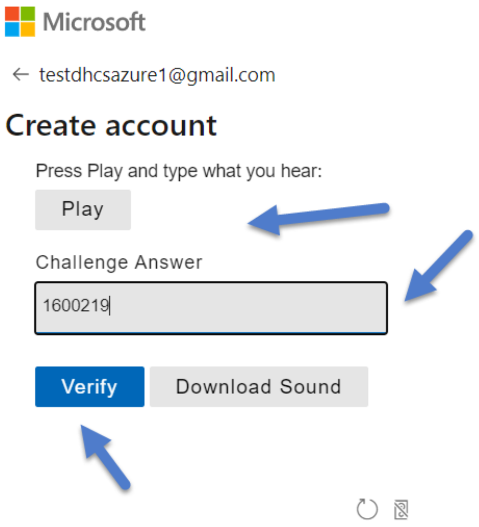


Microsoft

← testdhcsazure1@gmail.com

Create account

Please solve the puzzle so we know you're not a robot.



Microsoft

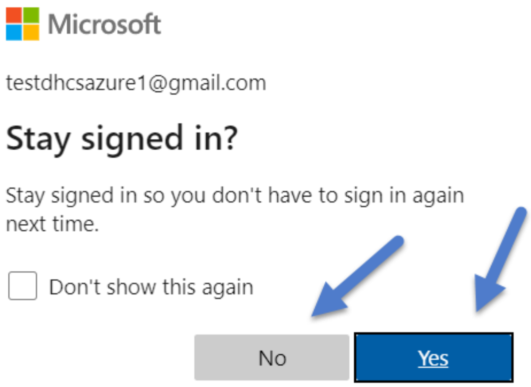
← testdhcsazure1@gmail.com

Create account

Press Play and type what you hear:

Challenge Answer: 1600219

6. When prompted to Stay signed in?, select No or Yes



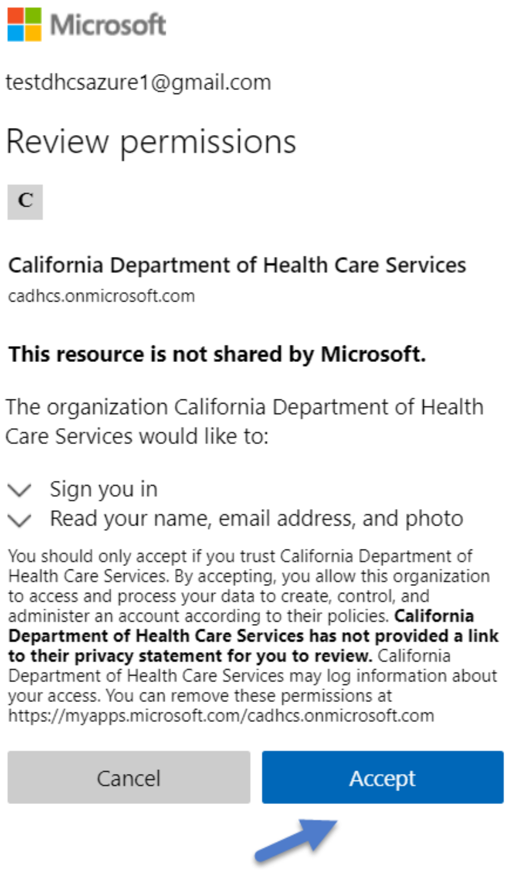
testdhcsazure1@gmail.com

Stay signed in?

Stay signed in so you don't have to sign in again next time.

□ Don't show this again

7. When prompted to Review permissions, select Accept



testdhcsazure1@gmail.com

Review permissions

California Department of Health Care Services
cadhcs.onmicrosoft.com

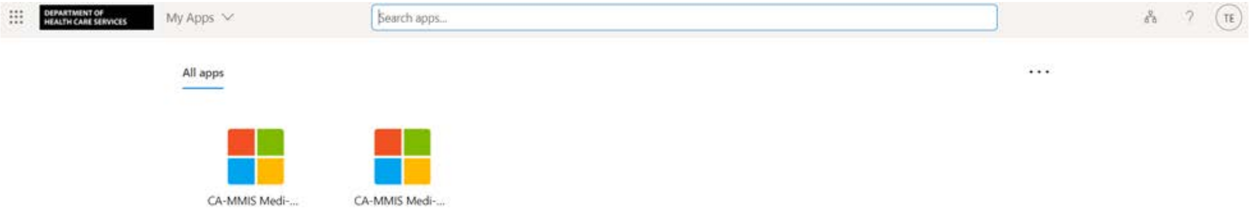
This resource is not shared by Microsoft.

The organization California Department of Health Care Services would like to:

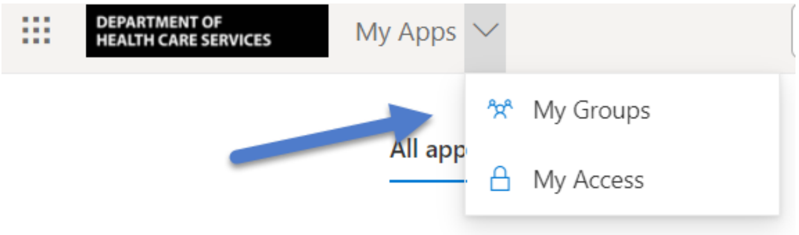
- Sign you in
- Read your name, email address, and photo

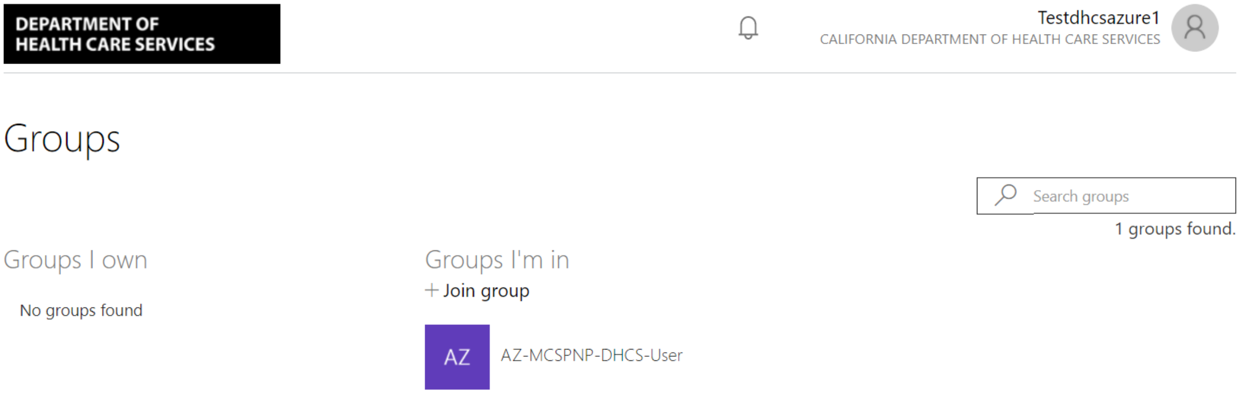
You should only accept if you trust California Department of Health Care Services. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. **California Department of Health Care Services has not provided a link to their privacy statement for you to review.** California Department of Health Care Services may log information about your access. You can remove these permissions at https://myapps.microsoft.com/cadhcs.onmicrosoft.com

8. You are now successfully logged into the DHCS Application Gallery (My Apps page) and can access all the integrated DHCS applications you have access to.



- Select My Apps > My Groups





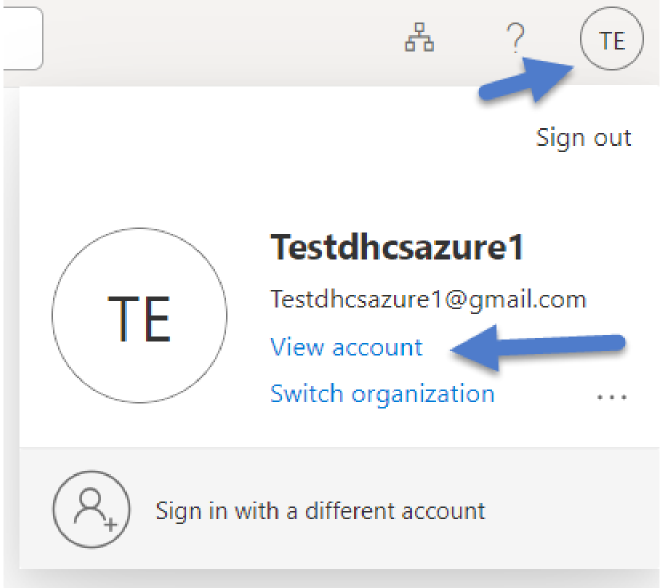
Multi-Factor Authentication (MFA) Setup

Background

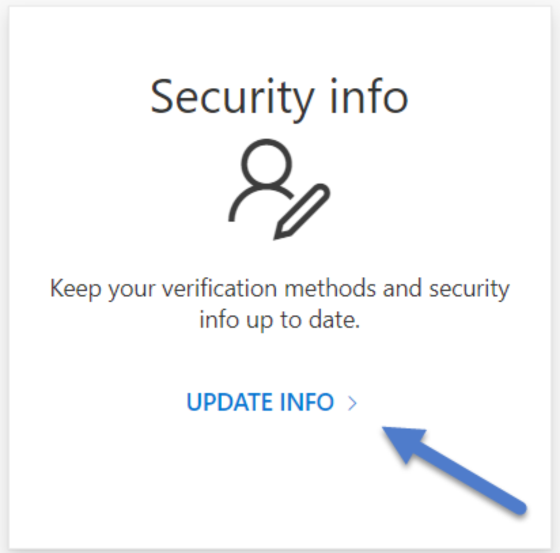
When first logging in to the DHCS Application Portal, members are prompted to set up additional security verification also referred to as Multi-Factor Authentication (MFA). MFA is an additional security step that helps protect your account by making it harder for others to break in. The following steps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

Steps

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



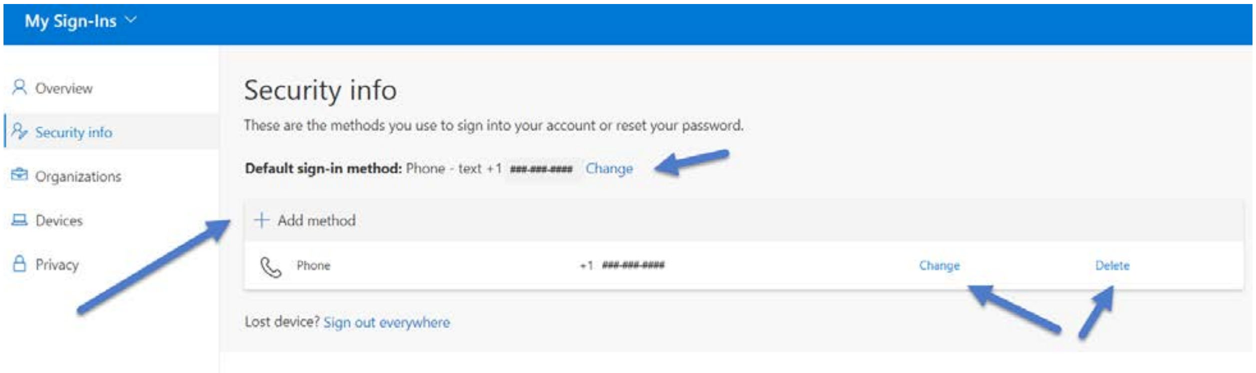
2. Select UPDATE INFO >



Security info

Keep your verification methods and security info up to date.

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



Security info

These are the methods you use to sign into your account or reset your password.

Default sign-in method: Phone - text +1 ###-###-#### Change

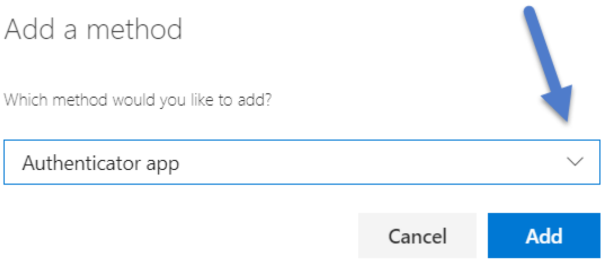
+ Add method

Phone +1 ###-###-#### Change Delete

Lost device? Sign out everywhere

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.

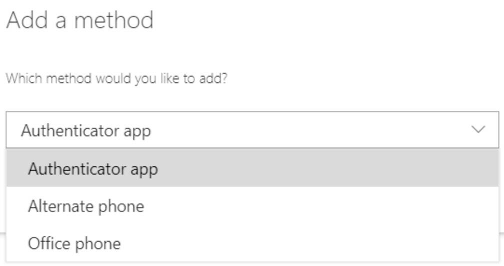
4. From Add a method, select the drop down list and a method. Follow the onscreen navigation to complete the setup.



Add a method

Which method would you like to add?

Authenticator app



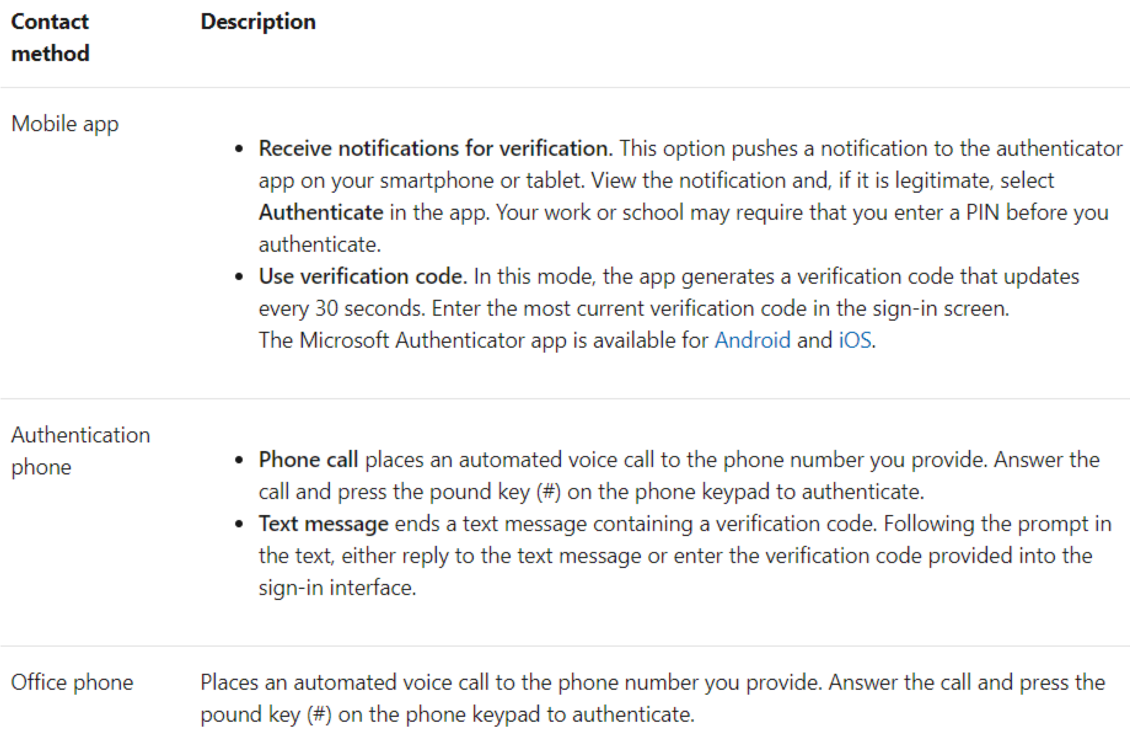
Add a method

Which method would you like to add?

Authenticator app

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	• **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	• **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.