DHCS

California Department of
Health Care Services

# DHCS APPLICATION PORTAL USER MANUAL

June 04, 2019

VERSION 0.04

# Revision History

| Version Number | Date | Description |
|---|---|---|
| 0.01 | 08/15/2018 | First iteration of working rough draft |
| 0.02 | 09/17/2018 | Updates based on feedback received |
| 0.03 | 02/14/2019 | Updated to include all end user information needed and renamed to Getting Started |
| 0.04 | 06/04/2019 | Updated to include feedback |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Contents

# INTRODUCTION

The DHCS Application Portal uses Microsoft Office 365 (also referred to as 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 existing Office 365 (Azure AD) account credentials or a Microsoft account. For more details, please refer to the “Logging In” section of this document.

When first logging into the DHCS Application Portal, users that belong to organizations that do not have an existing Office 365 (Azure AD) or Microsoft accounts will be asked to create new Microsoft accounts. For more details, please refer to the “Create a New Microsoft Account” section of this document.

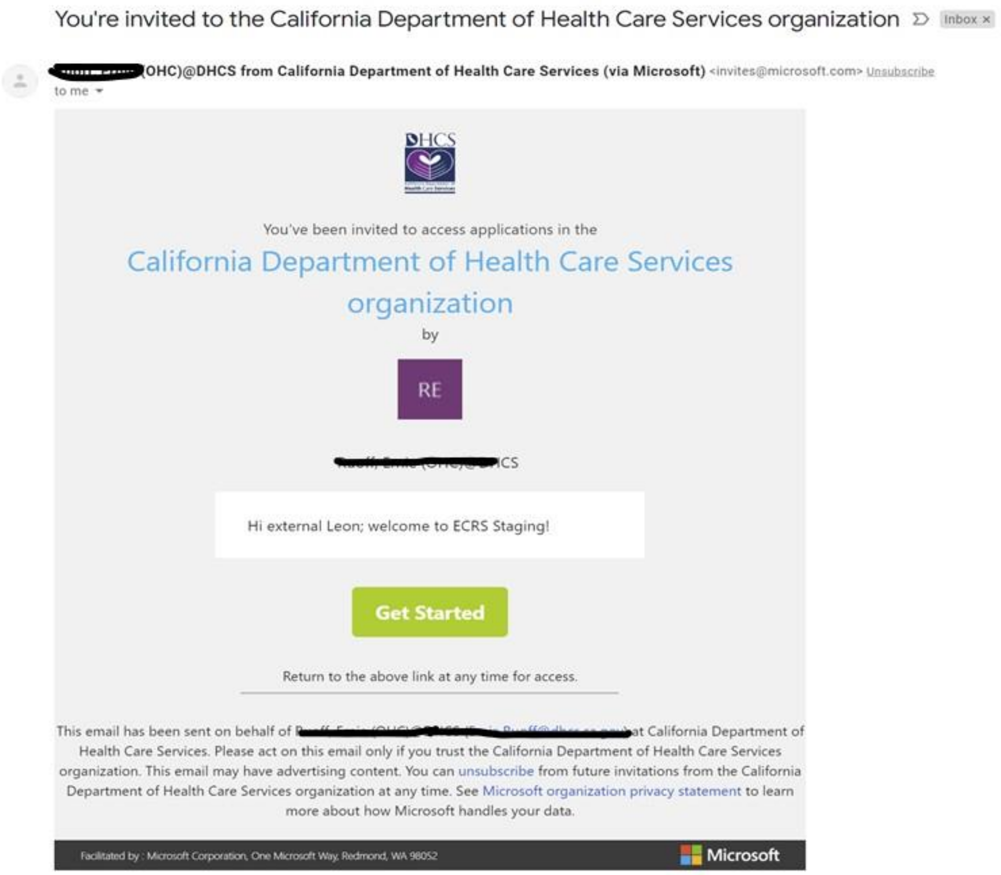
When first logging into the DHCS Application Portal or when first accessing a DHCS Application, users are prompted to set up additional security verification also referred to as Multi-Factor Authentication (MFA). MFA is an additional security step that helps protect your account by making it harder for other people to break in. For more details, please refer to the “Multi Factor Authentication (MFA) Setup” section of this document.

## INVITATION EMAIL

When an external member (non-DHCS staff) is given permission to access a DHCS application, the member receives an invitation email with a "Get Started" link that appears as follows. The member clicks the "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.

DHCS staff will not receive the invitation email. DHCS staff can login following the steps outlined in the "Logging In" section.



You're invited to the California Department of Health Care Services organization

[redacted](OHC)@DHCS from California Department of Health Care Services (via Microsoft) <invites@microsoft.com> Unsubscribe

to me

You've been invited to access applications in the

California Department of Health Care Services organization

by

[redacted]CS

Hi external Leon; welcome to ECRS Staging!

Return to the above link at any time for access.

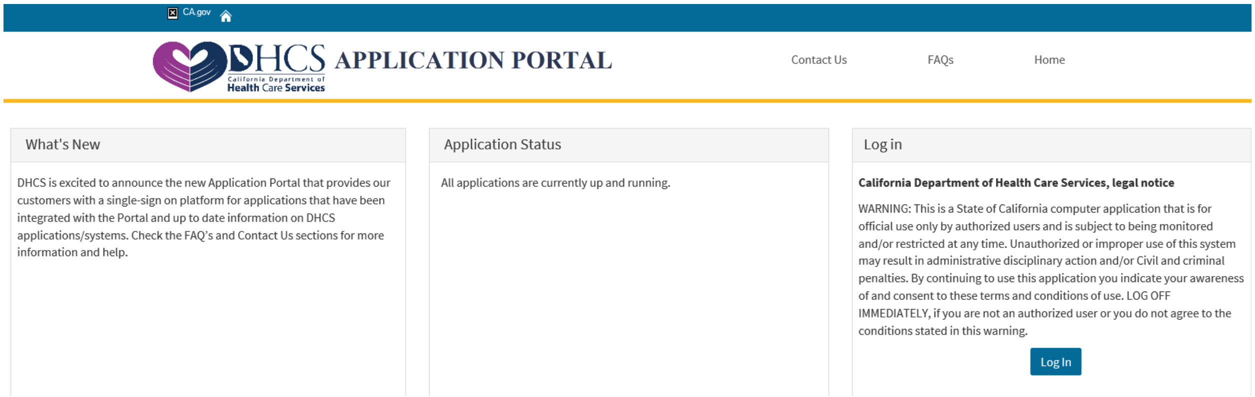
This email has been sent on behalf of [redacted]at California Department of Health Care Services. Please act on this email only if you trust the California Department of Health Care Services organization. This email may have advertising content. You can unsubscribe from future invitations from the California Department of Health Care Services organization at any time. See Microsoft organization privacy statement to learn more about how Microsoft handles your data.

Facilitated by : Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

# LOGGING IN

## Steps

1. From the DHCS Application Portal (https://portal.dhcs.ca.gov/), click *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

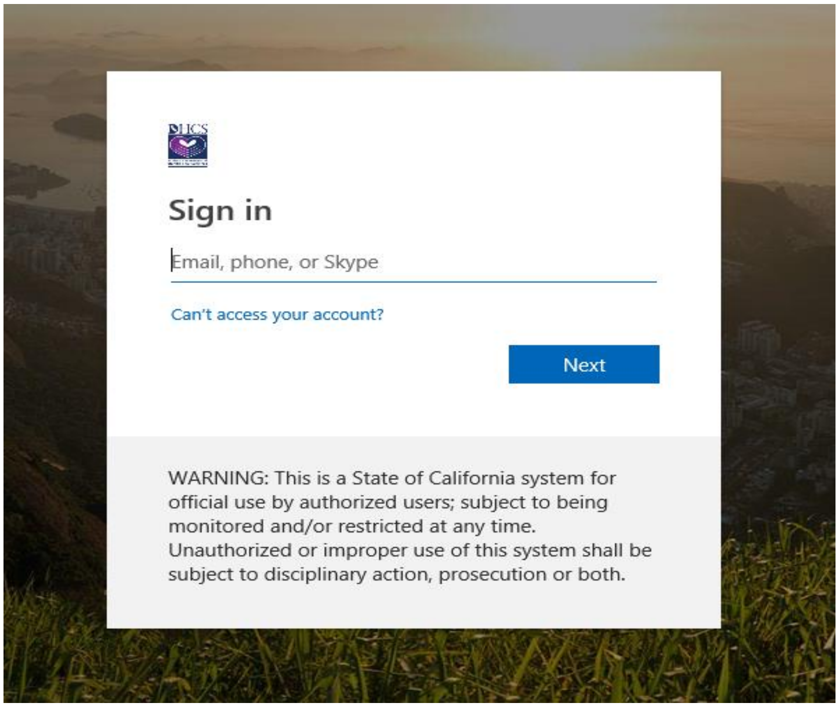
All applications are currently up and running.

Log in

**California Department of Health Care Services, legal notice**

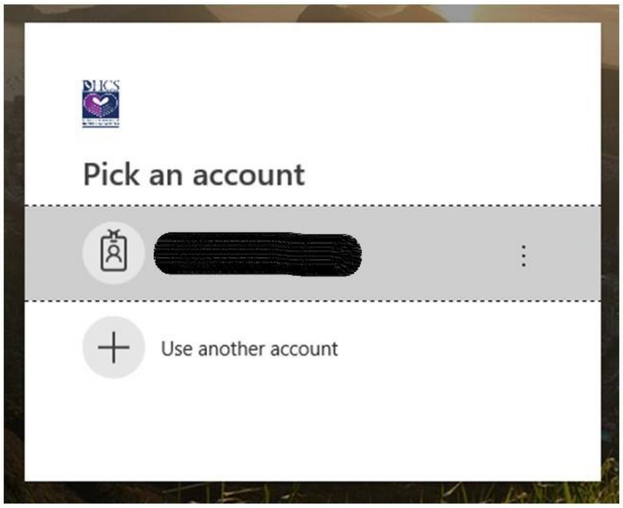
WARNING: This is a State of California computer application that is for official use only by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or Civil and criminal penalties. 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.

2. When prompted, enter your work email address and click *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.

OR when provided a list, choose your organization email address

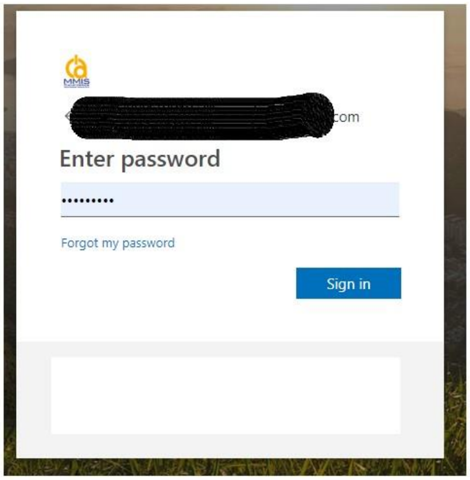


Pick an account

[redacted]

Use another account

3. If prompted, enter the password associated with your email. The password screen may looks different based on the browser you are using and your organization's configuration. Below are some examples of different password screens.

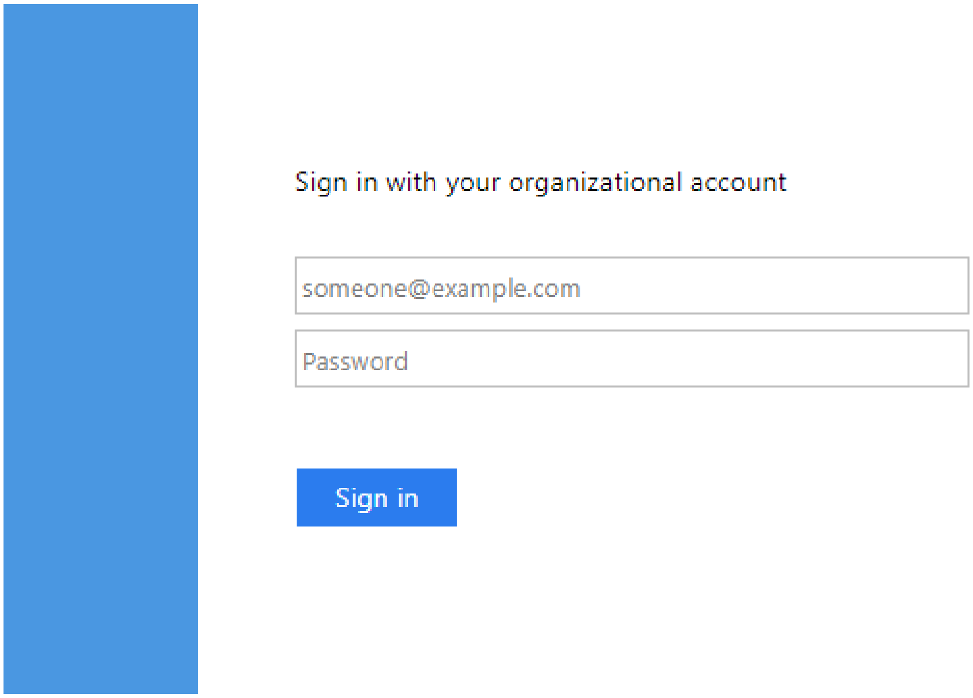


[redacted]com

Enter password

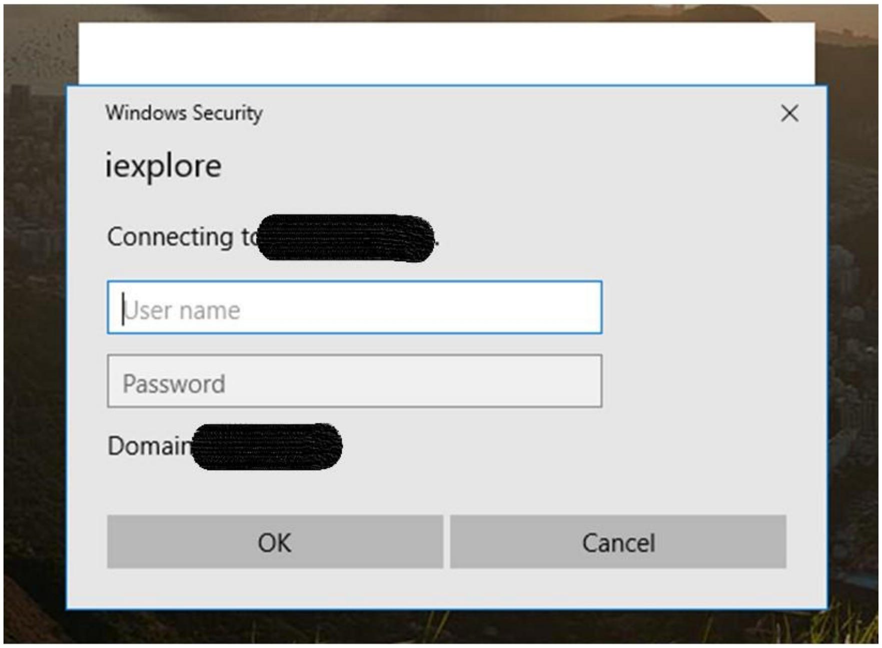
•••••••••

Forgot my password



Sign in with your organizational account

If you are using Internet Explorer (IE) as the browser, depending on your organization’s configuration, you may see this screen. Enter your work username and password.



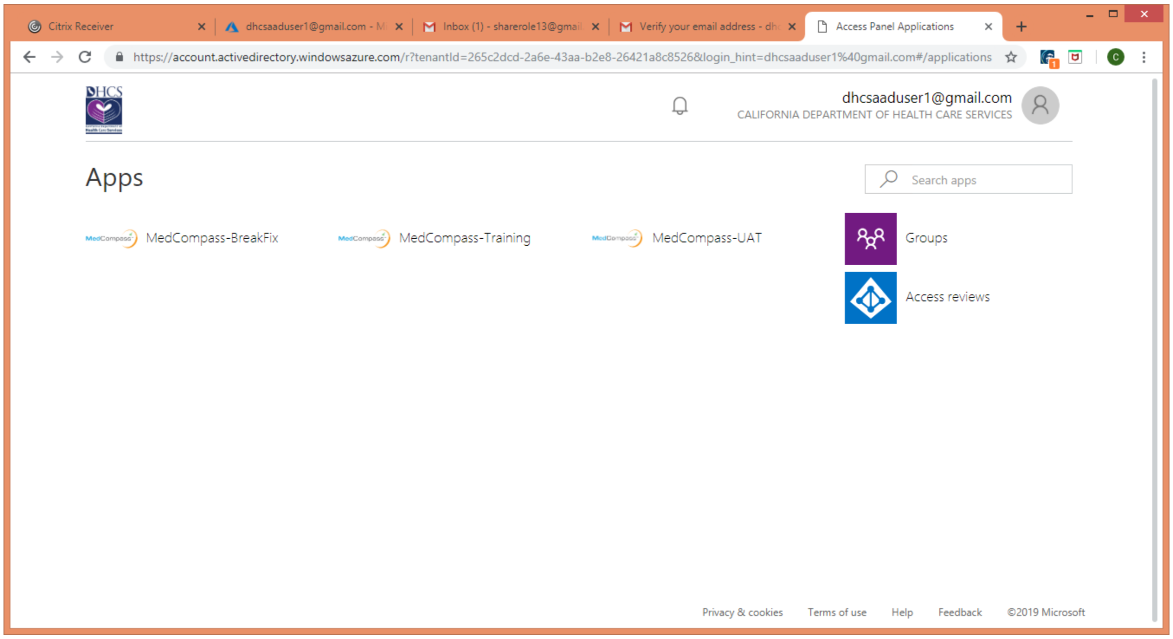
Connecting to [redacted].

Domain: [redacted]

4. If you are logging in for the first time, you may be prompted to set up Additional Security Verification (This is commonly known as Multi-Factor Authentication (MFA). For more information on the MFA setup, please refer to MFA INITIAL SETUP section.

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

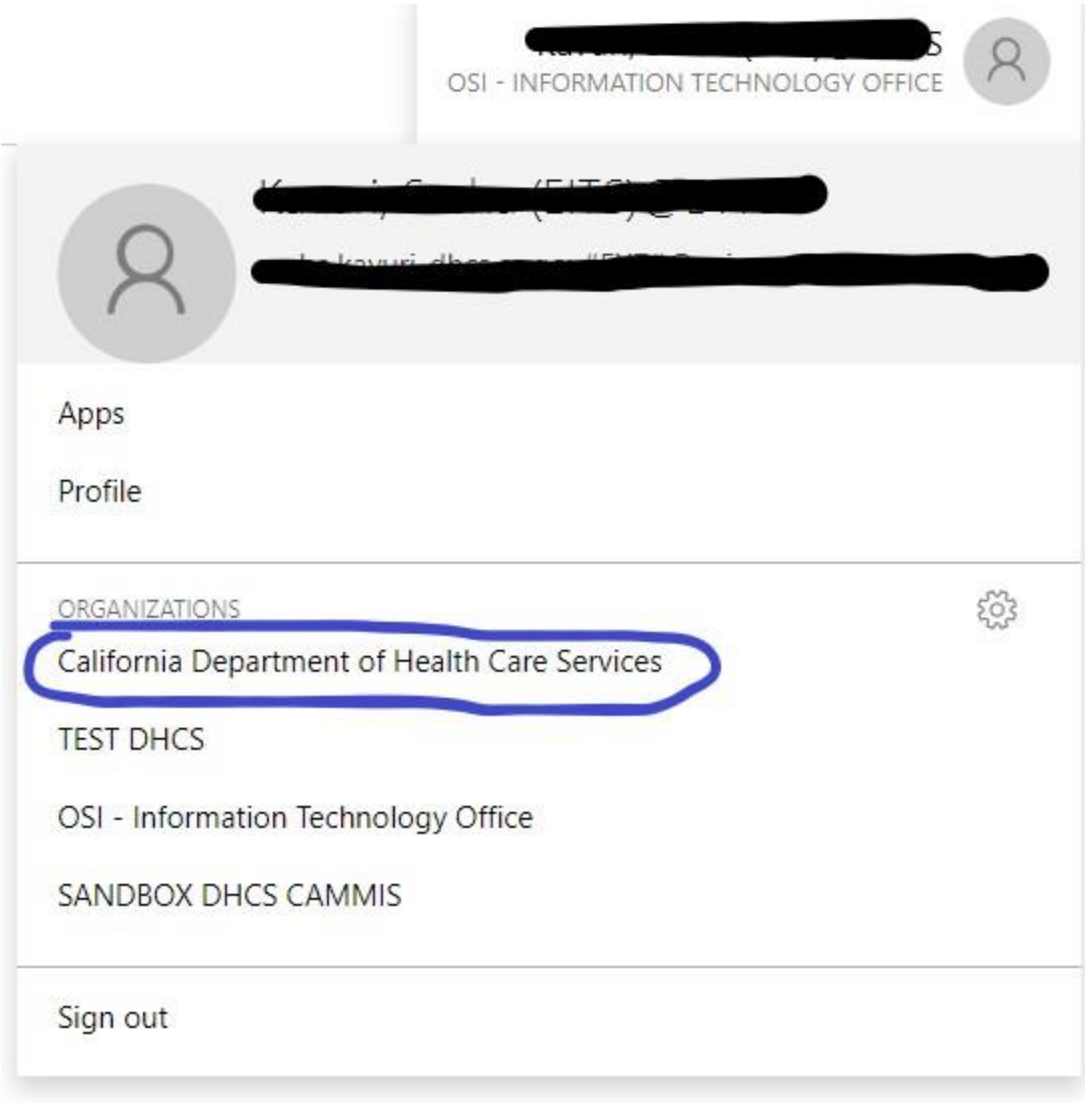
5. Once you are ***SUCCESSFULLY*** logged in, the DHCS Application Gallery (Apps page) is displayed. The Apps page displays all DHCS applications you have access to that have been integrated with the DHCS Application Portal.



https://account.activedirectory.windowsazure.com/r?tenantId=265c2dcd-2a6e-43aa-b2e8-26421a8c8526&login_hint=dhcsaaduser1%40gmail.com#/applications

dhcsaaduser1@gmail.com
CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

6. If you do not see “California Department of Health Care Services” before the user symbol in the upper-right corner of the page, Click the user symbol and click on the “California Department of Health Care Services” under the organizations.



[redacted]
OSI - INFORMATION TECHNOLOGY OFFICE

[redacted]

Apps

Profile

ORGANIZATIONS

[✓ California Department of Health Care Services]

TEST DHCS

OSI - Information Technology Office

SANDBOX DHCS CAMMIS

Sign out

# ACCESS AN APPLICATION

1. On the Apps page, click on the Application you want to access, and the application opens in a new tab.
2. If you are accessing the application for the first time, you may be prompted to setup the Multi-Factor Authentication. For more details, refer to the MFA setup section.

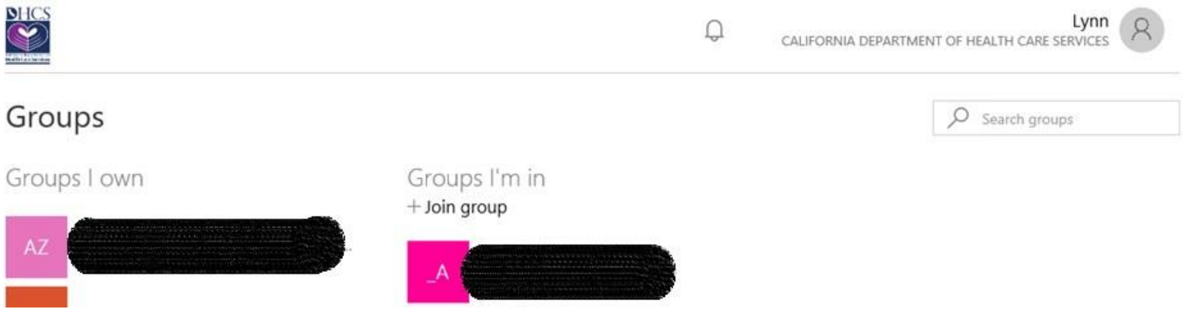
   If you have previously completed the MFA setup, you may be prompted to authenticate using the method you have chosen. Follow the onscreen instructions to complete the MFA verification.

# VIEW GROUP INFORMATION

1. On the Apps Page, Click the Groups tile. You will see the list of Groups you own (under the “Groups I own” column) and the list of Groups you are a member of (under the “Groups I’m in” Column).

   On the Groups page, under Groups I own column, if you see any groups listed, you are a Security Group Owner. Please refer to the “Security Group Owner Manual” for additional information.

   From the “Groups I’m in” column, select the group you want to view the group information. You can view the Group description and the other members of the group.



# CREATE A NEW MICROSOFT ACCOUNT

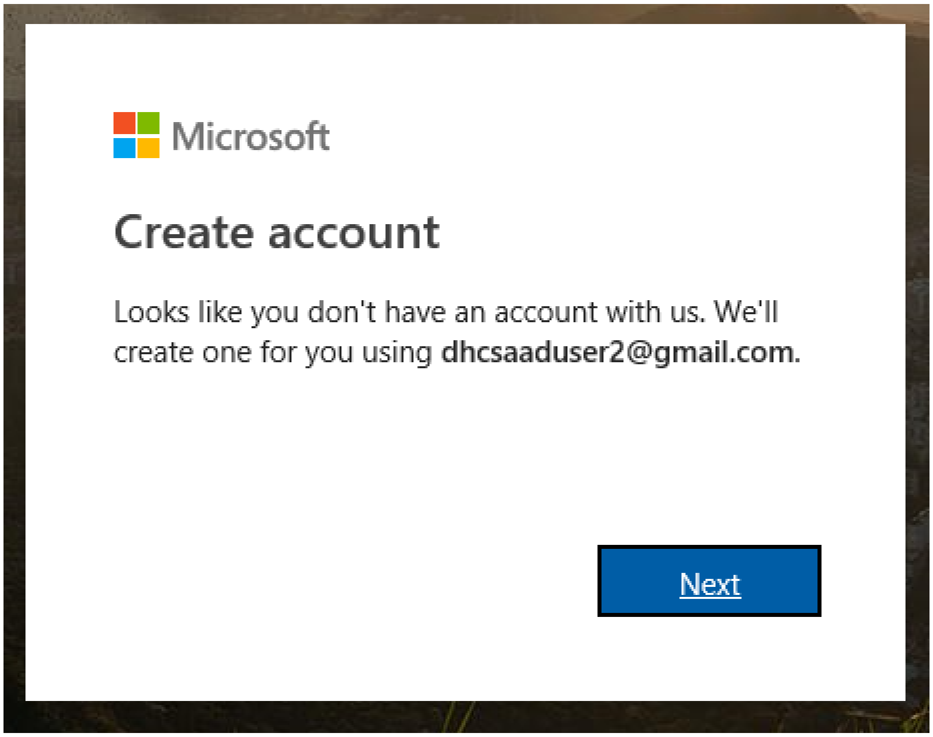
## Background

When first logging into the DHCS Application Portal, members that belong to organizations that do not have existing Office 365 (Azure AD) or Microsoft accounts are asked to create new Microsoft accounts.

Below describes the steps for members to create a Microsoft account.

## Steps

1. When prompted to Create account, click *Next*

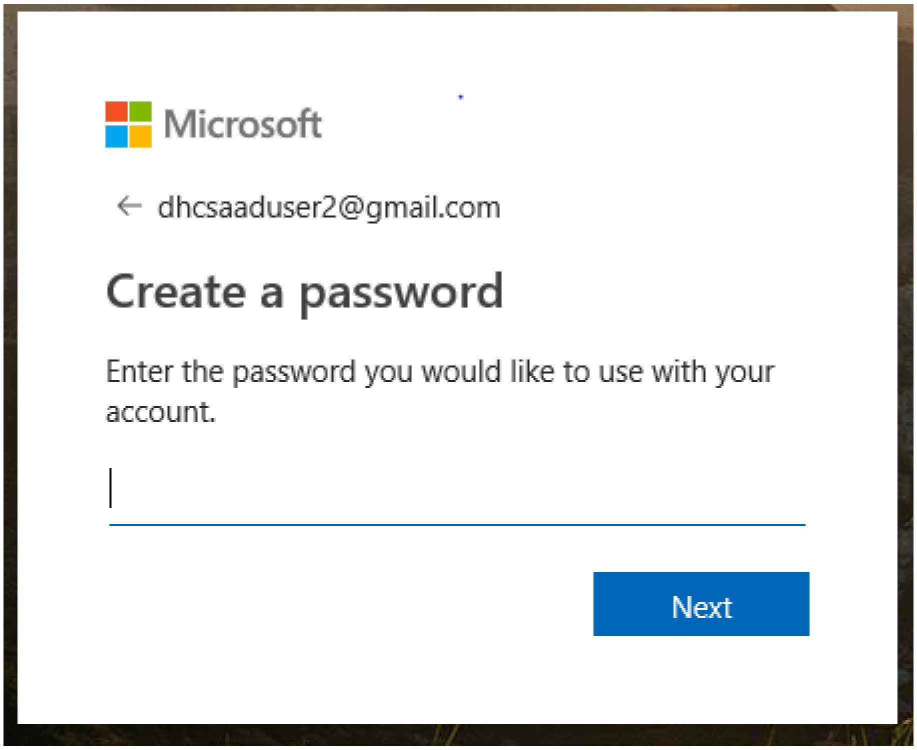


Microsoft

Create account

Looks like you don't have an account with us. We'll create one for you using **dhcsaaduser2@gmail.com**.

2. When prompted to Create a password, enter the password you would like to use for this account, then, click *Next*



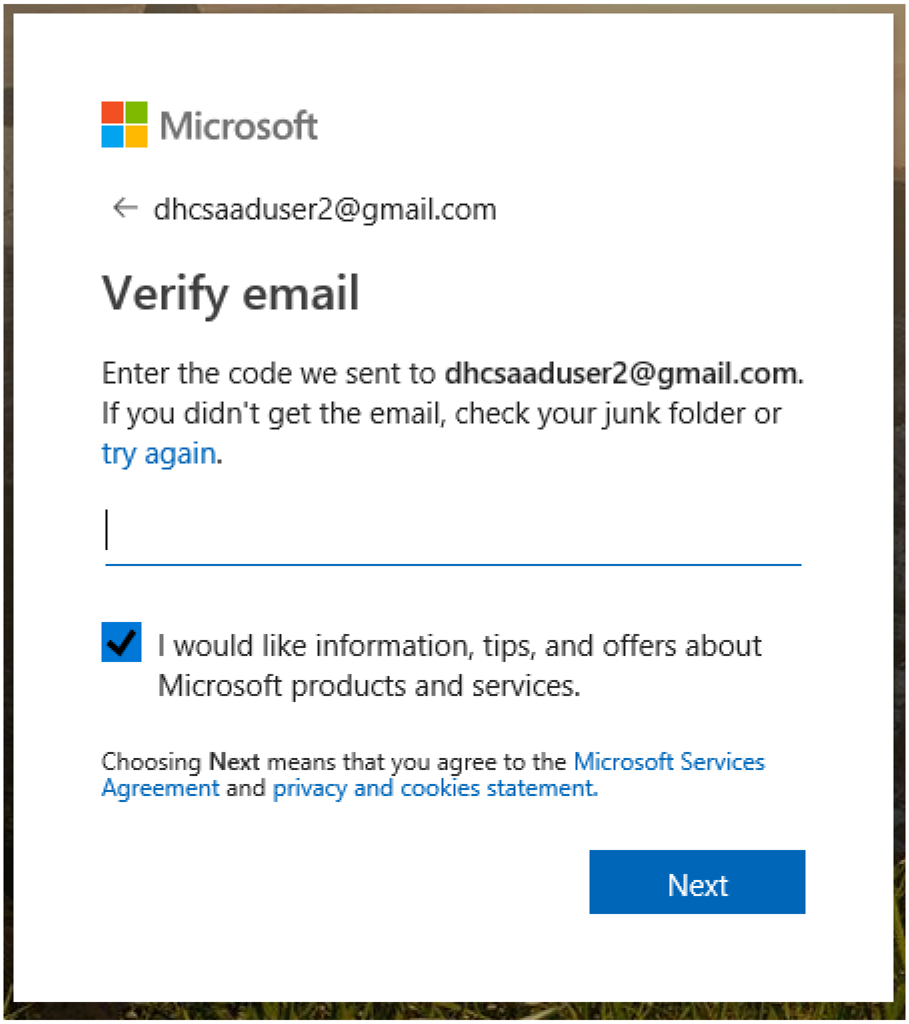
Microsoft

← dhcsaaduser2@gmail.com

Create a password

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

3. When prompted to Verify email, enter the code sent to your email, then, click *Next*



Microsoft

← dhcsaaduser2@gmail.com

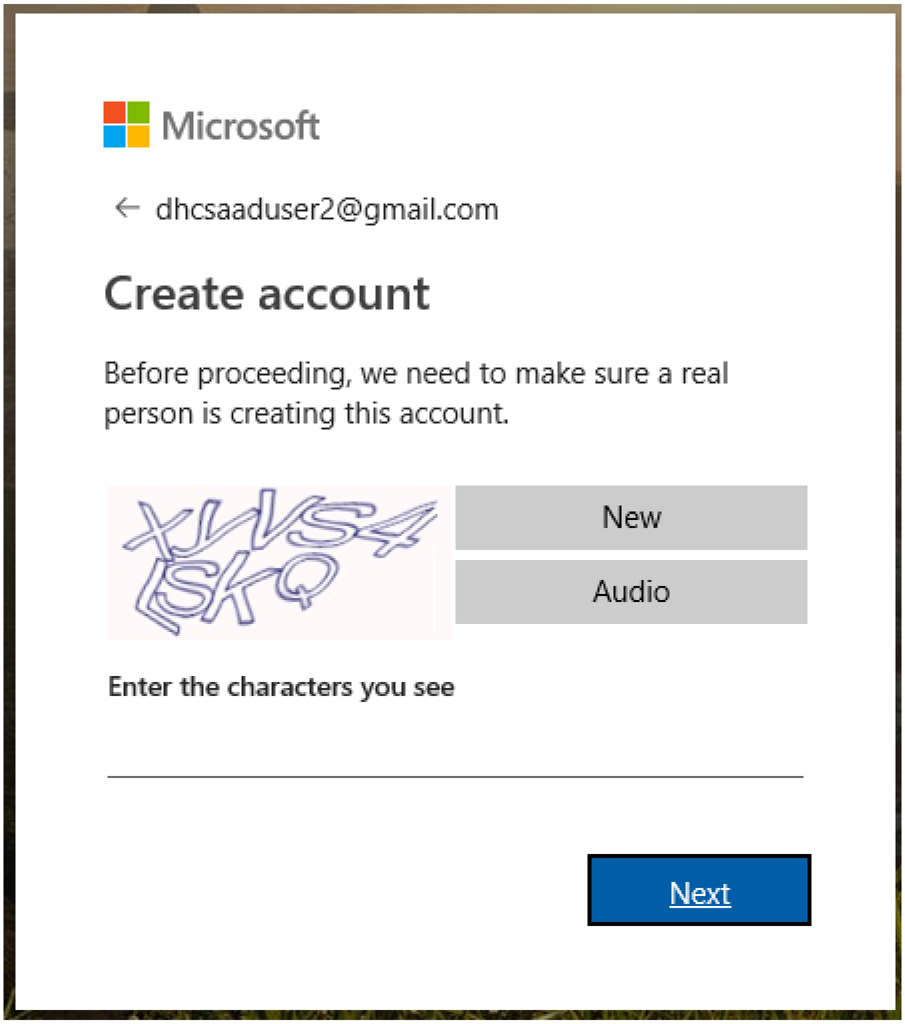
Verify email

Enter the code we sent to **dhcsaaduser2@gmail.com**. If you didn't get the email, check your junk folder or try again.

☑ 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.

4. When prompted to Create account, enter the characters you see, then, click *Next*



Microsoft

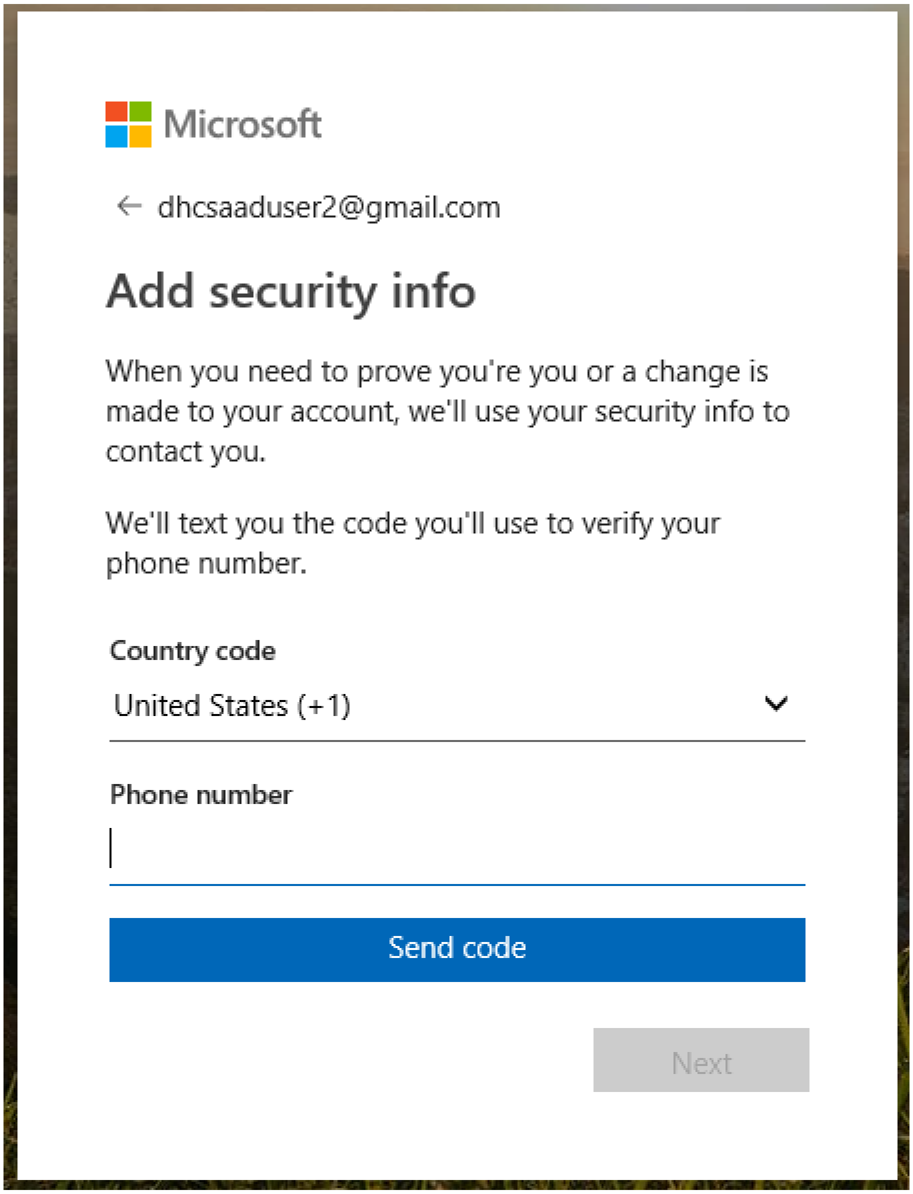
dhcsaaduser2@gmail.com

Create account

Before proceeding, we need to make sure a real person is creating this account.

Enter the characters you see

5. When prompted to Add security info, enter your phone number, then, click *Next*



← dhcsaaduser2@gmail.com

Add security info

When you need to prove you're you or a change is made to your account, we'll use your security info to contact you.

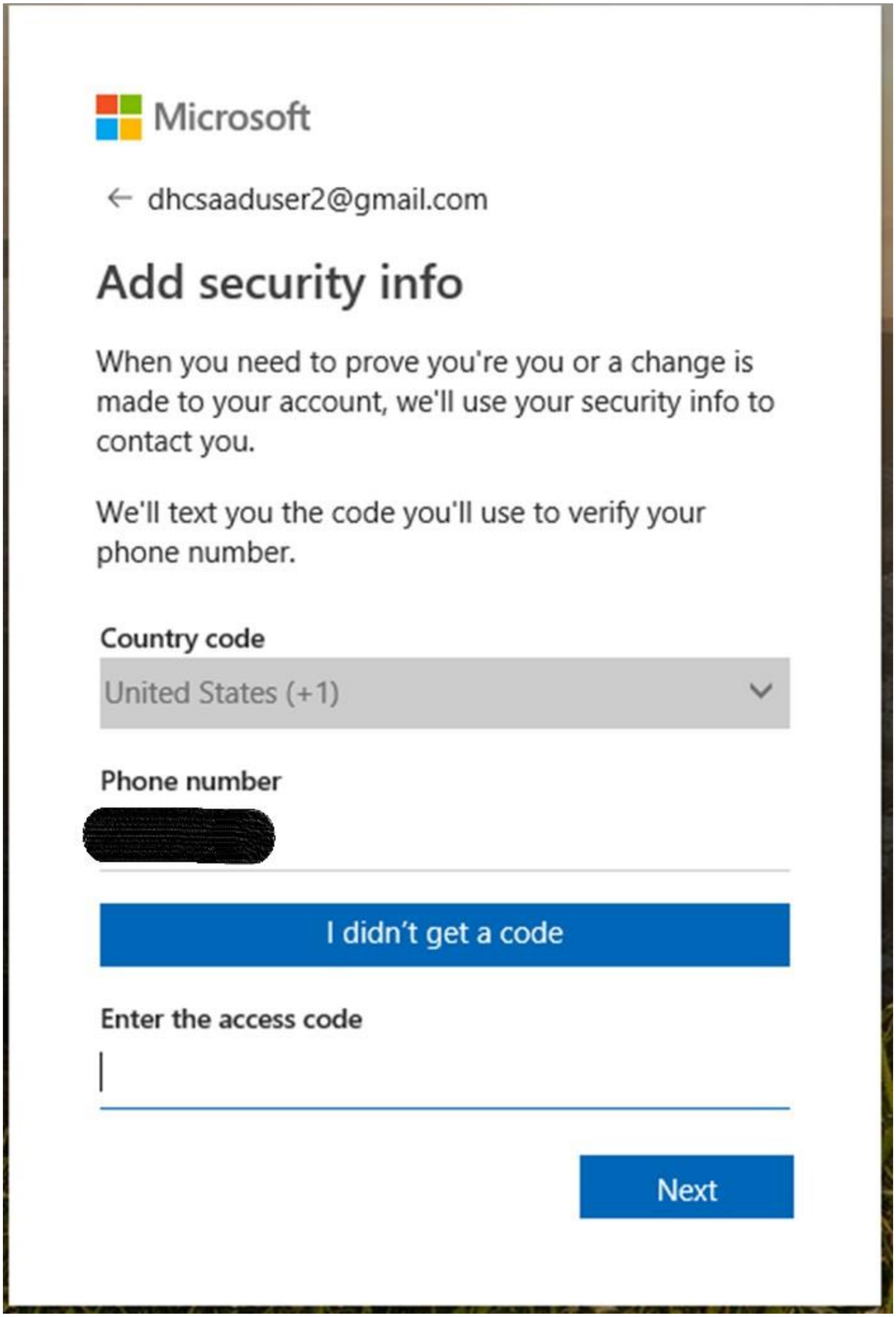
We'll text you the code you'll use to verify your phone number.

Country code

United States (+1)

Phone number

6. When prompted, enter the access code you received, then, click *Next*



← dhcsaaduser2@gmail.com

Add security info

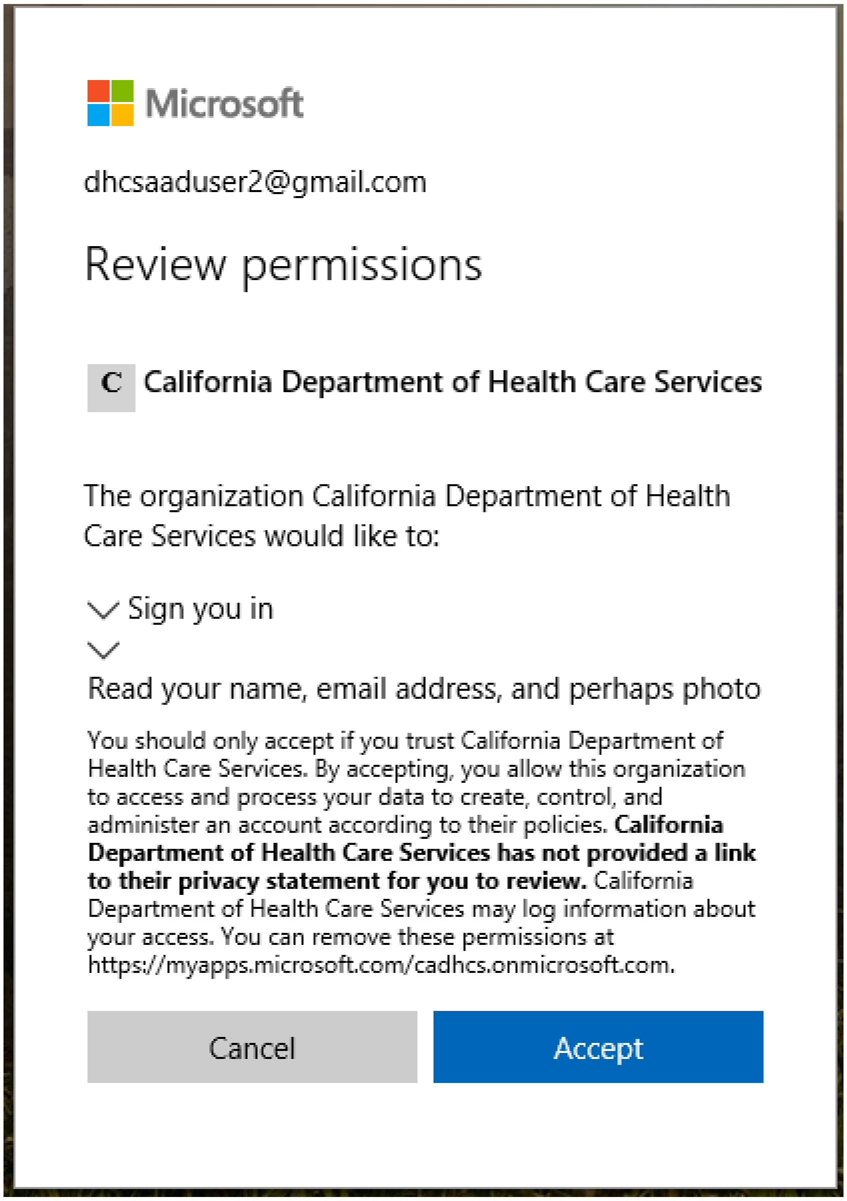
When you need to prove you're you or a change is made to your account, we'll use your security info to contact you.

We'll text you the code you'll use to verify your phone number.

Country code: United States (+1)

Phone number: [redacted]

7. When prompted to Review permissions, click *Accept*



Microsoft

dhcsaaduser2@gmail.com

Review permissions

C California Department of Health Care Services

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

Sign you in

Read your name, email address, and perhaps 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 (Apps page) and can access all DHCS applications you have access to that have been integrated with the Gallery.

# MULTI FACTOR AUTHENTICATION (MFA) SETUP

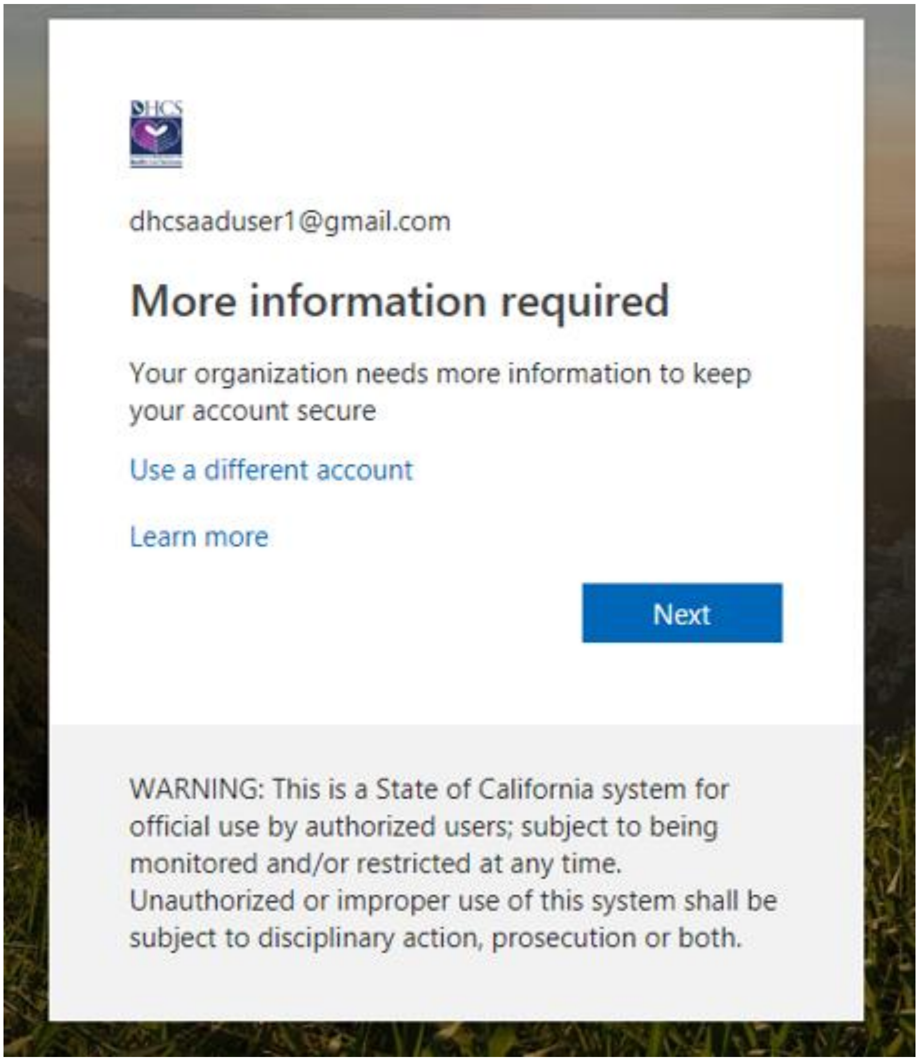
## Background

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 other people to break in.

Below describes the steps for members to set up and update the MFA settings.

## Steps

1. When prompted that more information is required, click *Next*



dhcsaaduser1@gmail.com

More information required

Your organization needs more information to keep your account secure

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.

2. On the Additional Security Verification page, select one of the Contact methods for the additional security verification. Follow the on-screen navigation to complete the setup.

   For more detailed information and screen prints, please refer to Microsoft website

   https://docs.microsoft.com/en-us/azure/active-directory/user-help/multi-factor-authentication-end-user-first-time

| **Contact method** | **Description** |
|---|---|
| Mobile phone call or text | - **Phone call** places an automated voice call to the phone number you provide. Answer the call and press # in the phone keypad to authenticate.<br>- **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 Call | Places an automated voice call to the phone number you provide. Answer the call and presses # in the phone keypad to authenticate. |
| 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.<br>- **Use verification code.** In this mode, the authenticator app generates a verification code that updates every 30 seconds. Enter the most current verification code in the sign-in interface.<br>The Microsoft Authenticator app is available for Android and iOS. |

# MFA ADDITIONS OR CHANGES

## Background

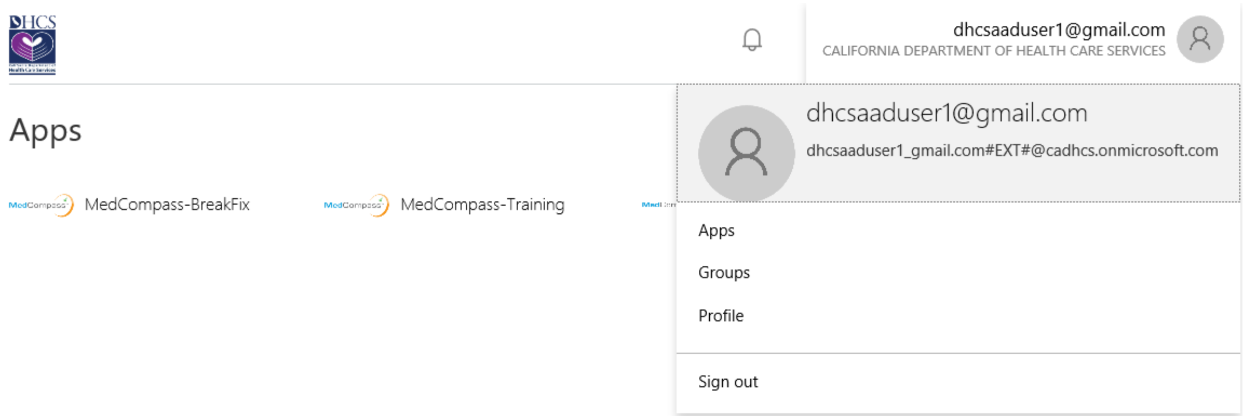
When you want to change your MFA authentication configuration for any reason, you can do this through the DHCS Application Gallery.

Below describes the steps for members to add or update the MFA settings.

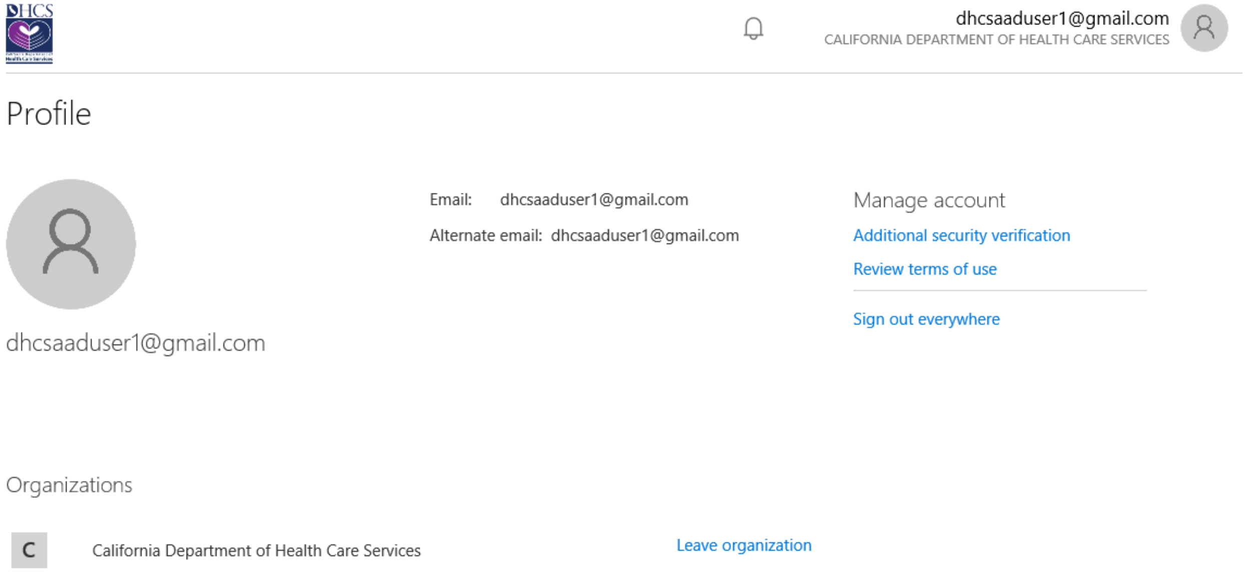
NOTE:  DHCS staff cannot update the office phone through these steps; office phone information must be updated via the Global Address List (GAL) profile update process.

## Steps

1. From the Apps page, click on your email in the upper right corner to get the following drop down selections and select Profile



2. From the Profile page, under Manage Account, click Additional security verification

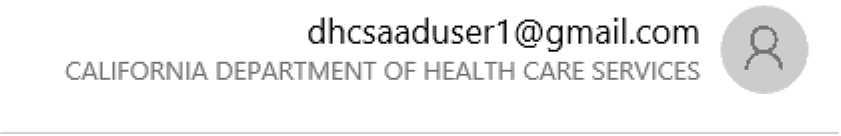


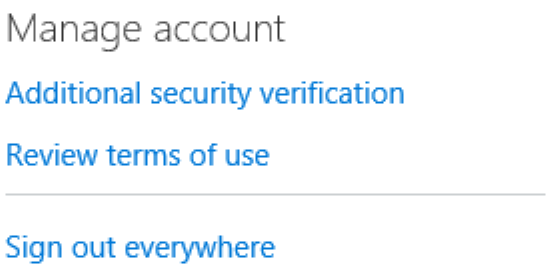
dhcsaaduser1@gmail.com

Email: dhcsaaduser1@gmail.com

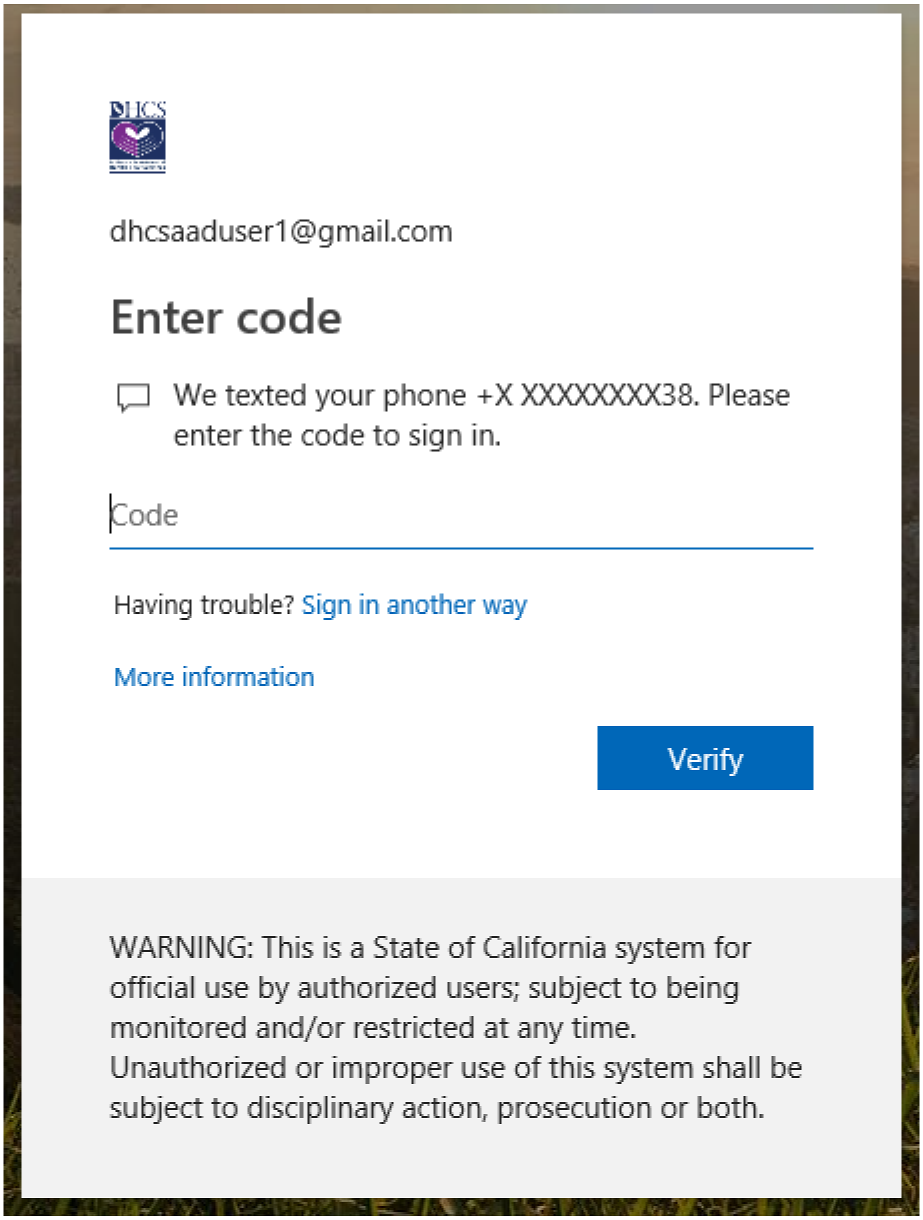
Alternate email: dhcsaaduser1@gmail.com

California Department of Health Care Services





3. If prompted for MFA, enter the verification code received and click *Verify*



dhcsaaduser1@gmail.com

Enter code

We texted your phone +X XXXXXXXX38. Please enter the code to sign in.

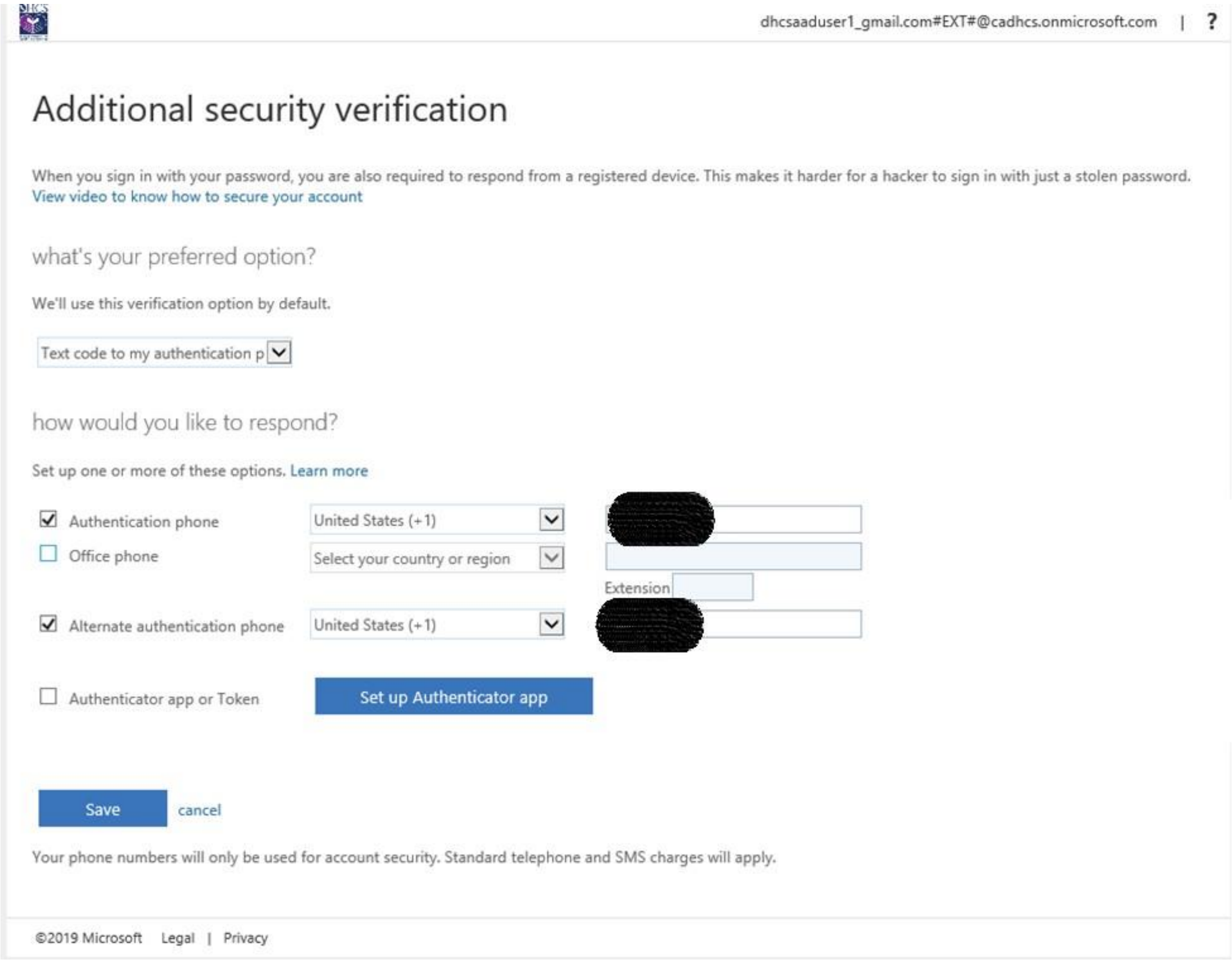
Code

Having trouble? Sign in another way

More information

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.

4. On the Additional Security Verification page, enter additional or update existing authentication phone information and click *Save*



dhcsaaduser1_gmail.com#EXT#@cadhcs.onmicrosoft.com | ?

## Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
View video to know how to secure your account

what's your preferred option?

We'll use this verification option by default.

Text code to my authentication p

how would you like to respond?

Set up one or more of these options. Learn more

☑ Authentication phone — United States (+1) — [redacted]

□ Office phone — Select your country or region — Extension

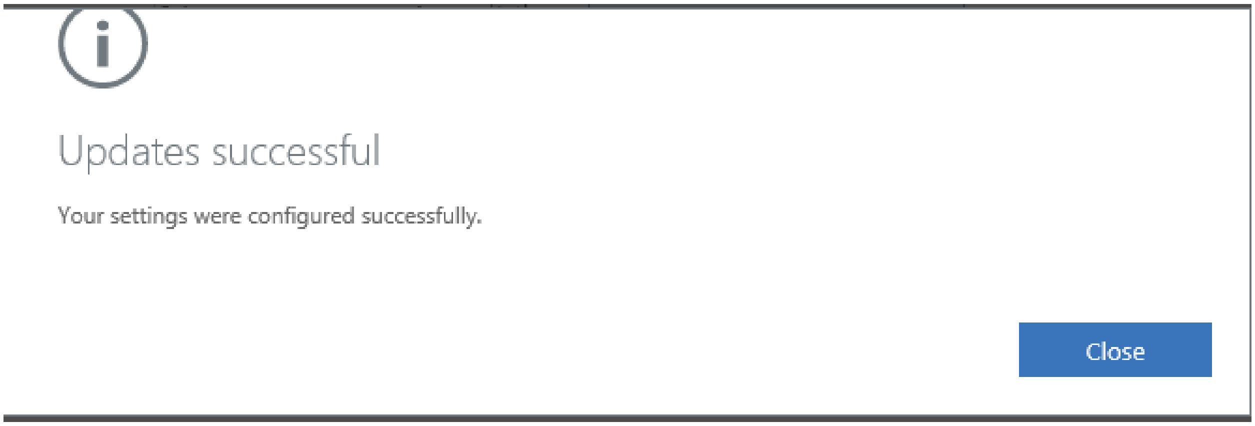
☑ Alternate authentication phone — United States (+1) — [redacted]

□ Authenticator app or Token — Set up Authenticator app

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2019 Microsoft Legal | Privacy

5. When update is successful you will receive the following confirmation, click *Close*



Updates successful

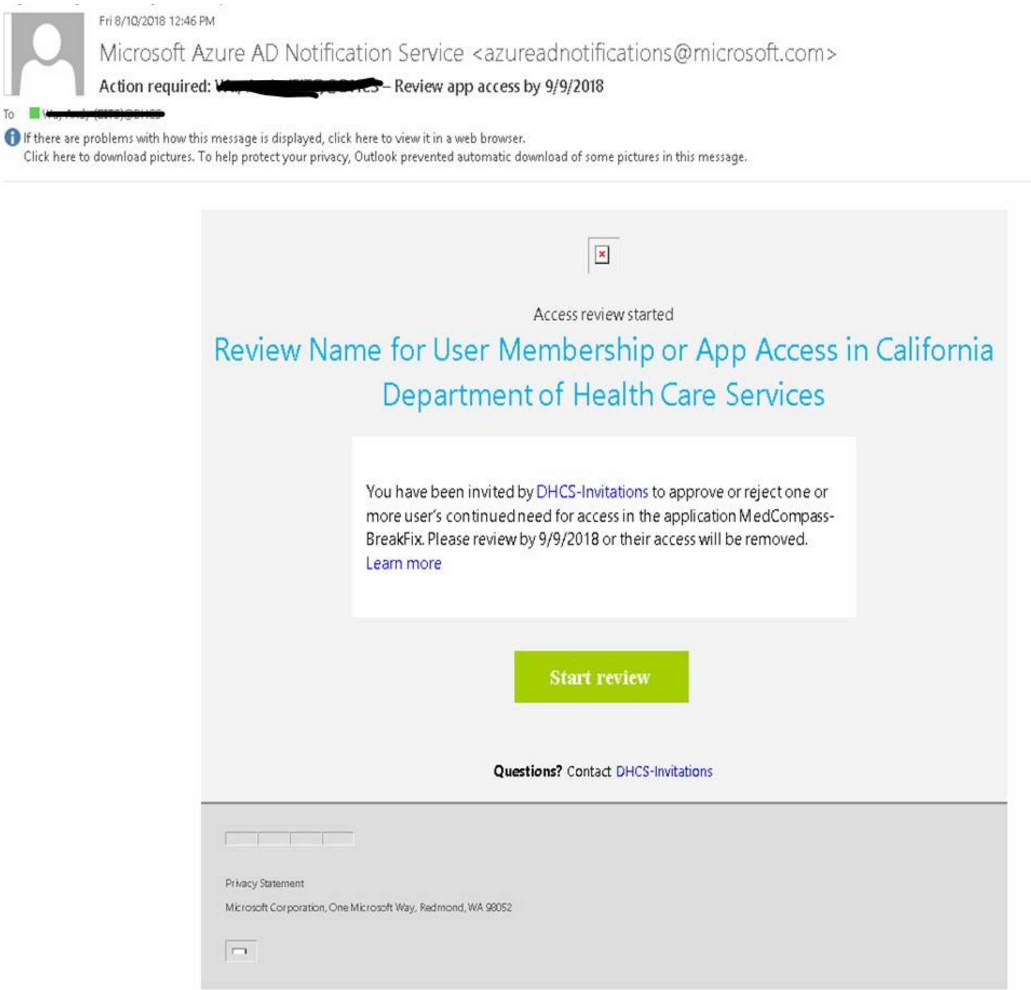
Your settings were configured successfully.

# ACCESS REVIEWS

Access Reviews are performed to ensure that members who were added to a security group and/or application continue to need access. DHCS Application administrator require all members to complete the Access Reviews periodically. As a member, you must complete any and all Access Review requests in a timely manner.  If Access Reviews are not completed in time, members will be removed from the Security Group/Application and members will not be able to access the DHCS application(s) in scope for the Access Review(s).

## Member Access Review

1. Receive an email from Microsoft or DHCS that asks you to review access for yourself, members of a group or users with access to an application.



Fri 8/10/2018 12:46 PM

Microsoft Azure AD Notification Service <azureadnotifications@microsoft.com>

Action required: [redacted] – Review app access by 9/9/2018

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Access review started

Review Name for User Membership or App Access in California Department of Health Care Services

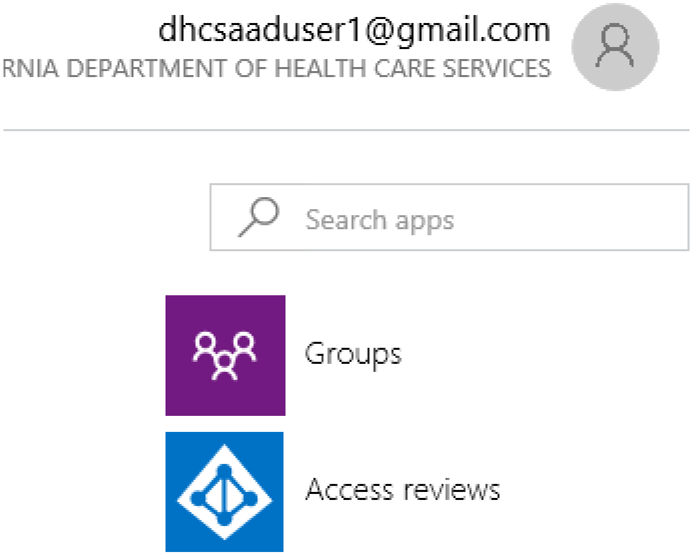
You have been invited by DHCS-Invitations to approve or reject one or more user's continued need for access in the application MedCompass-BreakFix. Please review by 9/9/2018 or their access will be removed.
Learn more

**Questions?** Contact DHCS-Invitations

Privacy Statement
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

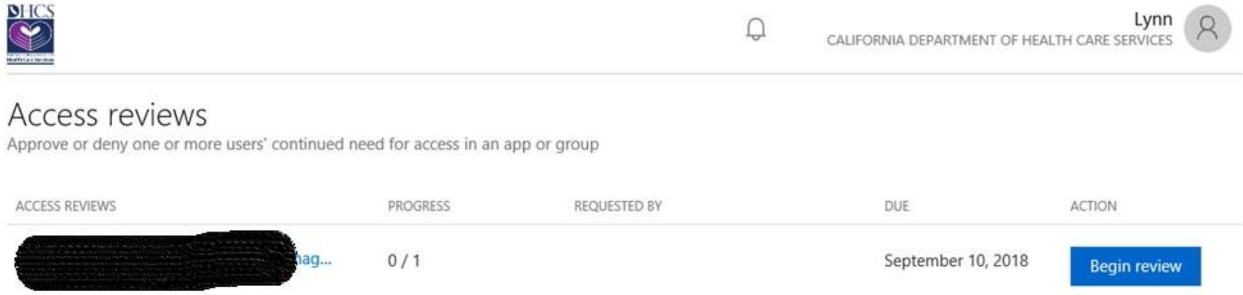
## 2. Click *Start Review* link in email

## OR Access Reviews in DHCS Application Gallery



Note: If a tile labeled Access reviews is on the right side of the page, select it. If the tile isn't visible, there are no access reviews to perform for that organization and no action is needed at this time.

## 3. Click *Begin Review*



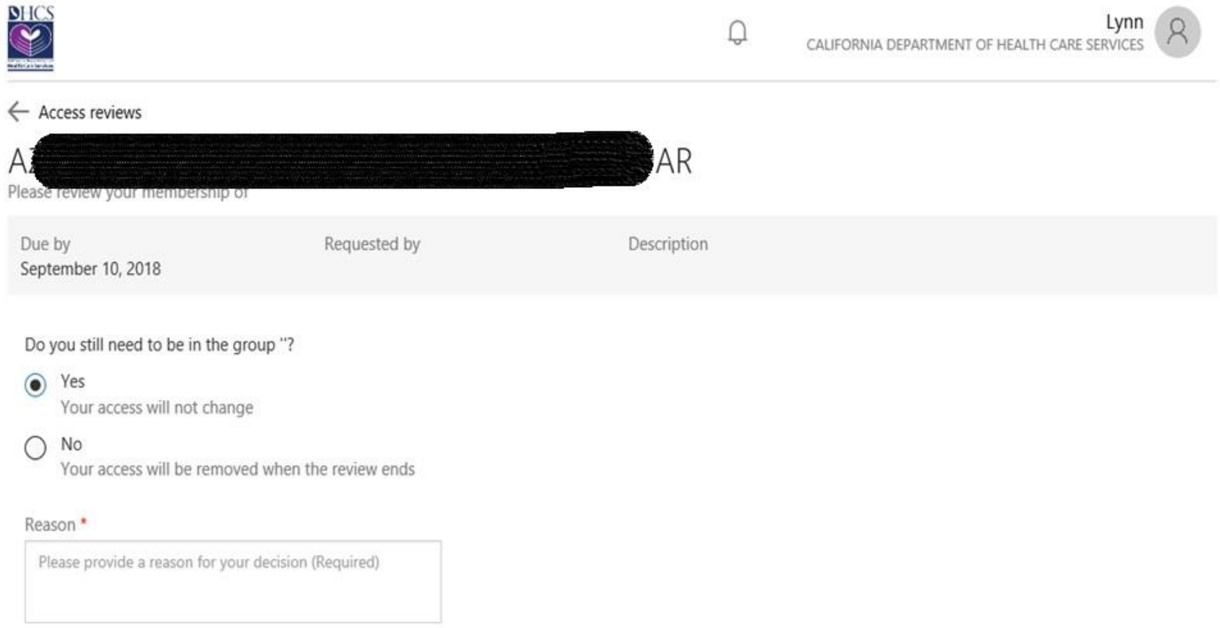
Access reviews

Approve or deny one or more users' continued need for access in an app or group

| ACCESS REVIEWS | PROGRESS | REQUESTED BY | DUE | ACTION |
|---|---|---|---|---|
| [redacted] nag... | 0 / 1 | | September 10, 2018 | Begin review |

4. Select *Yes* and provide a Reason (*Required*) why you still require access.

   Select *No* and provide a Reason (*Optional*) if you no longer require access.



Lynn
CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

← Access reviews

A[redacted]AR

| | | |
|---|---|---|
| Due by<br>September 10, 2018 | Requested by | Description |

Do you still need to be in the group ''?

● Yes
Your access will not change

○ No
Your access will be removed when the review ends

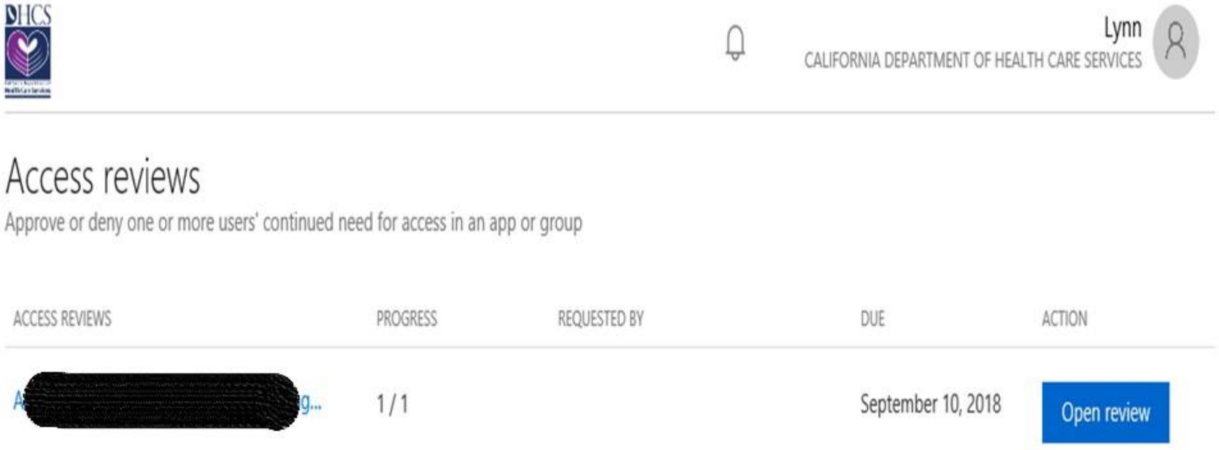
Reason *

Please provide a reason for your decision (Required)

***<u>YOU HAVE SUCCESSFULLY COMPLETED THE MEMBER ACCESS REVIEW</u>***

## Update Access Review

### 1. Click *Open Review* to submit changes, if needed.



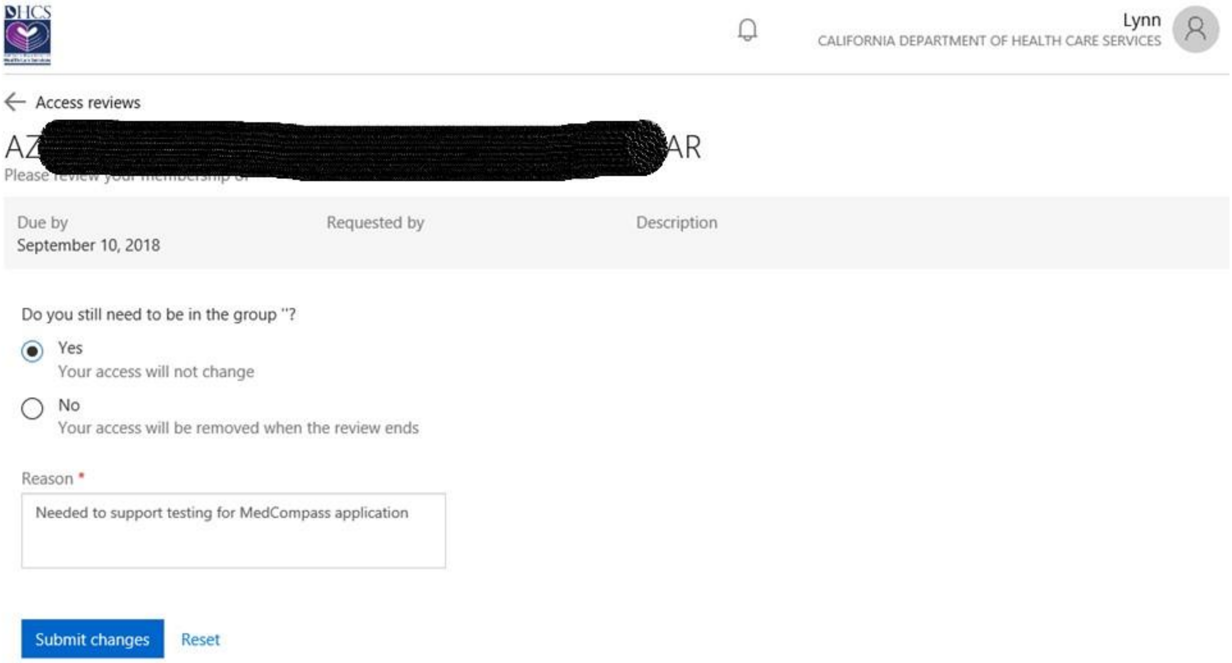
Lynn
CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

Access reviews

Approve or deny one or more users' continued need for access in an app or group

| ACCESS REVIEWS | PROGRESS | REQUESTED BY | DUE | ACTION |
|---|---|---|---|---|
| A[redacted]g... | 1 / 1 | | September 10, 2018 | Open review |

### 2. Update response and Click *Submit Changes*



Lynn
CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

← Access reviews

AZ[redacted]AR

Please [redacted]

| Due by | Requested by | Description |
|---|---|---|
| September 10, 2018 | | |

Do you still need to be in the group ''?

● Yes
Your access will not change

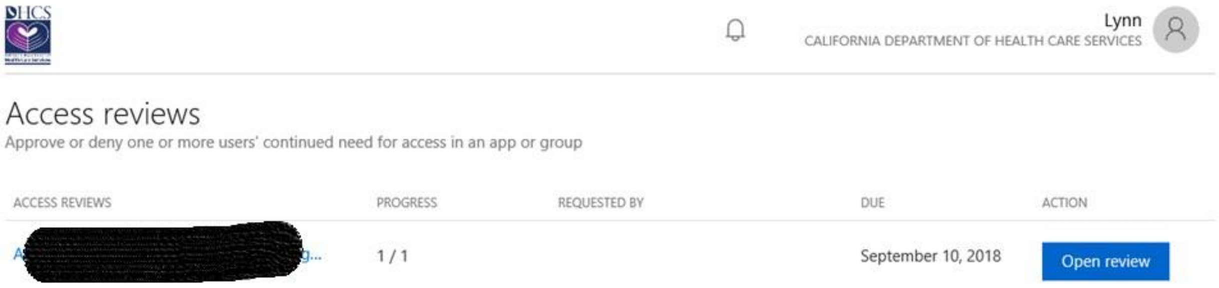
○ No
Your access will be removed when the review ends

Reason *

Needed to support testing for MedCompass application

## View Status of an Access Review

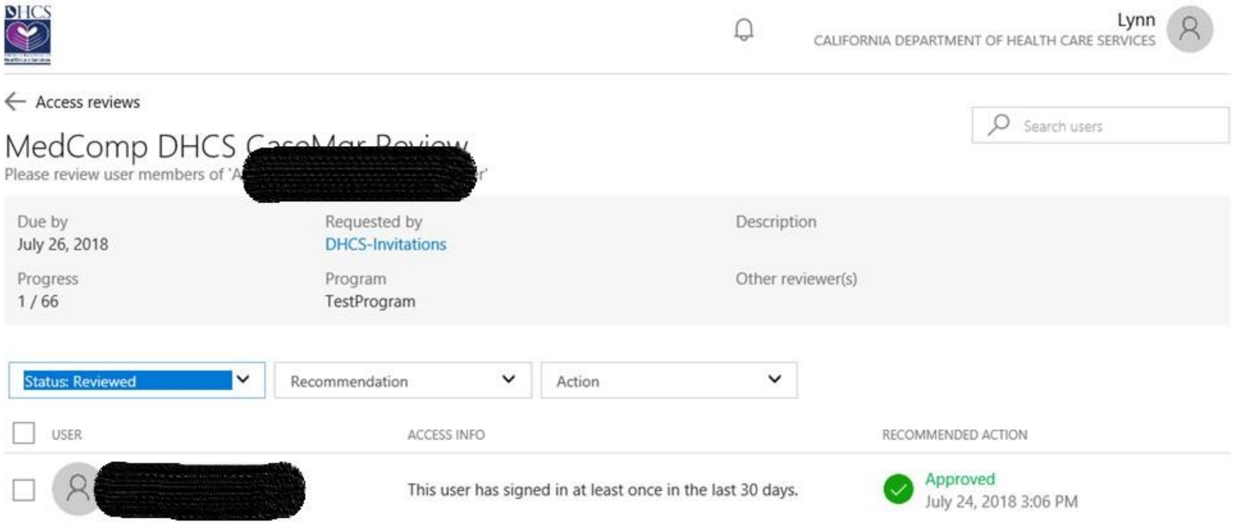
### 1. Click *Open Review* to view Status of Access Review



Lynn
CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

Access reviews
Approve or deny one or more users' continued need for access in an app or group

| ACCESS REVIEWS | PROGRESS | REQUESTED BY | DUE | ACTION |
|---|---|---|---|---|
| A[redacted]g... | 1 / 1 | | September 10, 2018 | Open review |



Lynn
CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES

← Access reviews

Search users

MedComp DHCS [redacted]
Please review user members of 'A

Due by
July 26, 2018

Requested by
DHCS-Invitations

Description

Progress
1 / 66

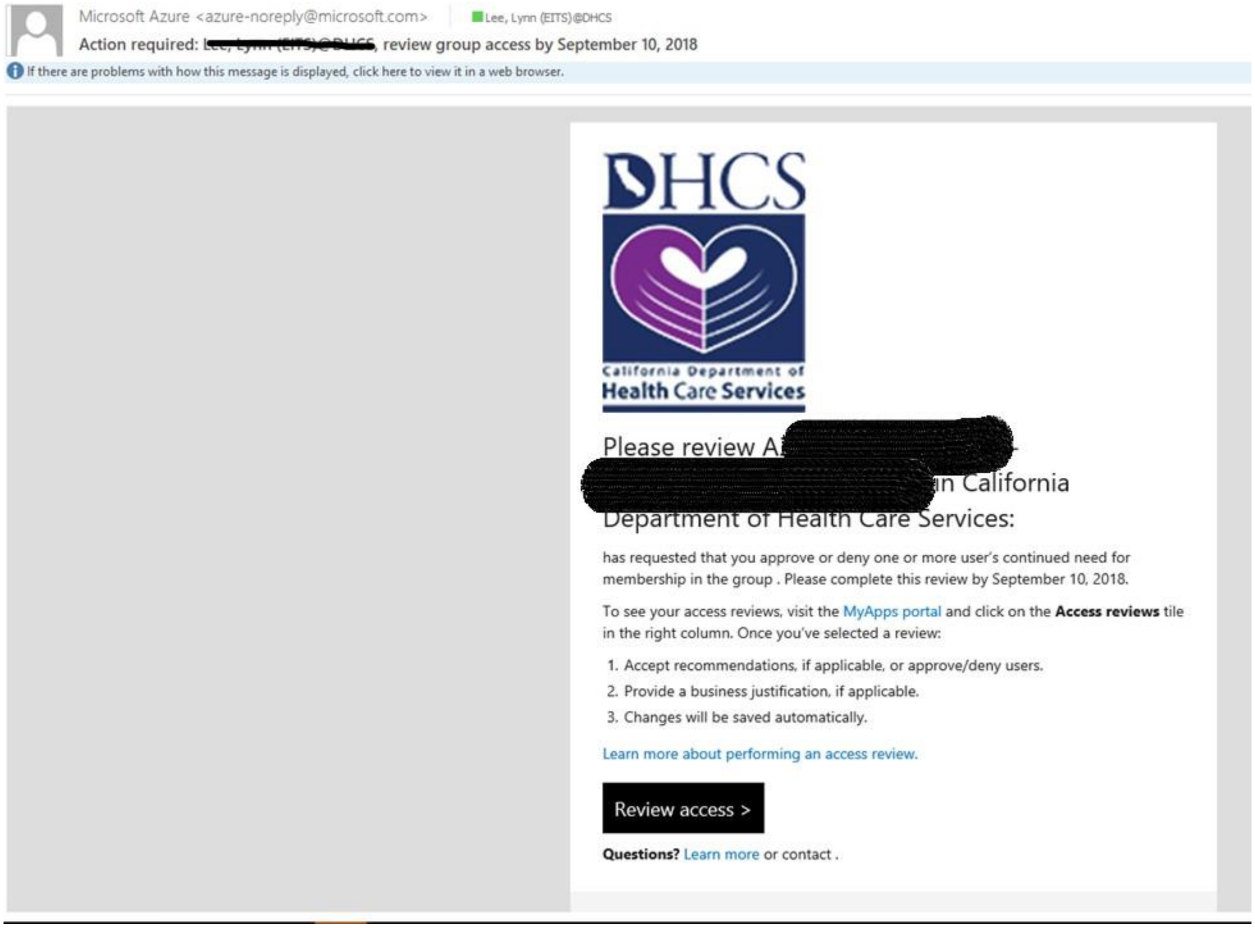
Program
TestProgram

Other reviewer(s)

Status: Reviewed | Recommendation | Action

| □ USER | ACCESS INFO | RECOMMENDED ACTION |
|---|---|---|
| □ [redacted] | This user has signed in at least once in the last 30 days. | ✓ Approved<br>July 24, 2018 3:06 PM |

# Examples of follow up emails sent by Microsoft Azure when access review(s) are still outstanding.



Microsoft Azure <azure-noreply@microsoft.com> | 🟩Lee, Lynn (EITS)@DHCS

Action required: [redacted], review group access by September 10, 2018

If there are problems with how this message is displayed, click here to view it in a web browser.

DHCS

California Department of Health Care Services

Please review A[redacted] [redacted]n California Department of Health Care Services:

has requested that you approve or deny one or more user's continued need for membership in the group . Please complete this review by September 10, 2018.

To see your access reviews, visit the MyApps portal and click on the **Access reviews** tile in the right column. Once you've selected a review:

1. Accept recommendations, if applicable, or approve/deny users.
2. Provide a business justification, if applicable.
3. Changes will be saved automatically.

Learn more about performing an access review.

**Questions?** Learn more or contact .