

AZURE ACTIVE DIRECTORY QUICK REFERENCE GUIDE GETTING STARTED

February 14, 2019

VERSION 0.03

Revision History

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

INTRODUCTION

Purpose

The California Department of Health Care Services (DHCS) have implemented a robust Enterprise Identity and Access Management (EIAM) solution to address the DHCS need to manage Identity and Access. EIAM enables the right individuals to access the right resources at the right times for the right reasons.

This document describes the steps for internal and external users to access DHCS applications integrated with Microsoft Azure Active Directory (Azure AD or AAD).

Roles and Responsibilities

As a DHCS application user, you must ensure that you only have access to applications that you have a valid business reason to access.

All users must complete any and all Access Review requests in a timely manner. Failure to complete an Access Review may impact your ability to access DHCS applications and continue to have memberships in groups in Azure AD.

During the access reviews, please ensure that you have and document the valid business reason why access is needed based on your current job responsibilities. Provide a high-level description of the applicable job duty the access supports as the reason access is needed when completing the access reviews.

Note: All user access is subject to audits.

Contact Us

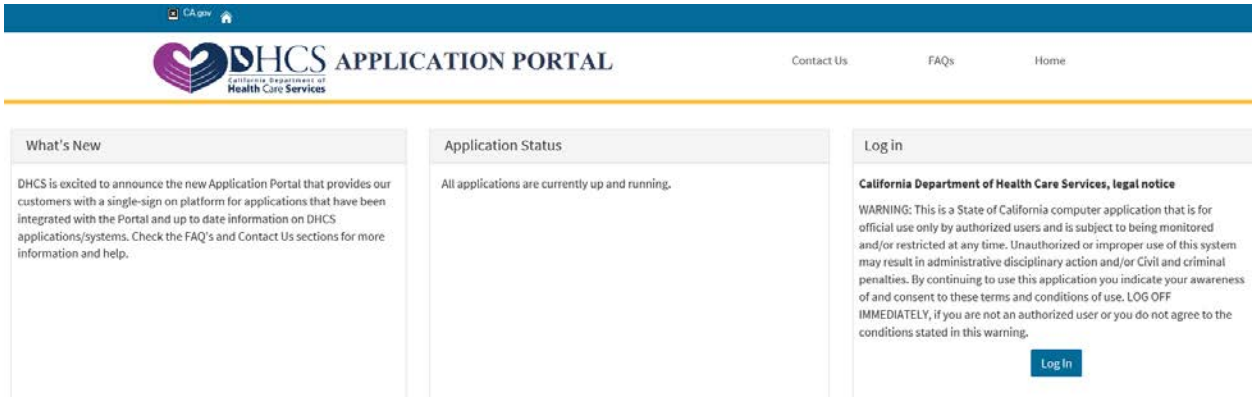
EITS CSTS is responsible for the management and operation of the Azure Active Directory solution. If you have any issues with the solution, please contact the DHCS Service Desk.

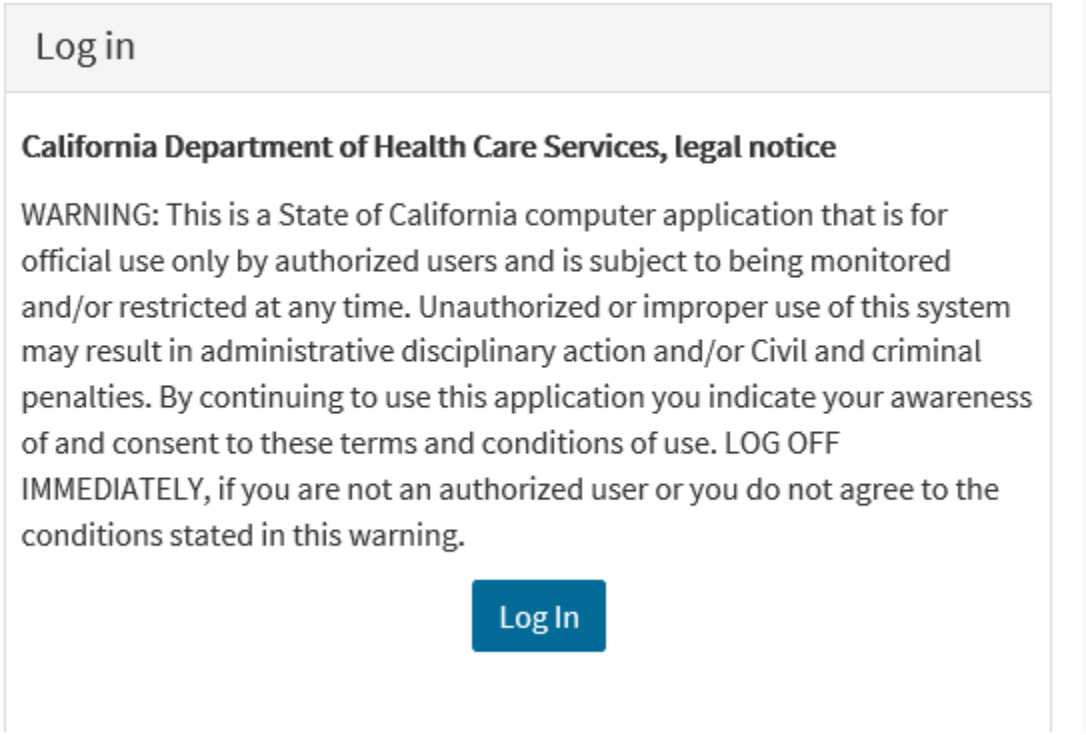
- Internal DHCS staff must create a remedy ticket.
- External users can contact the Service Desk at 916-440-7000 or 1-800-579-0874.

LOGGING IN

Steps

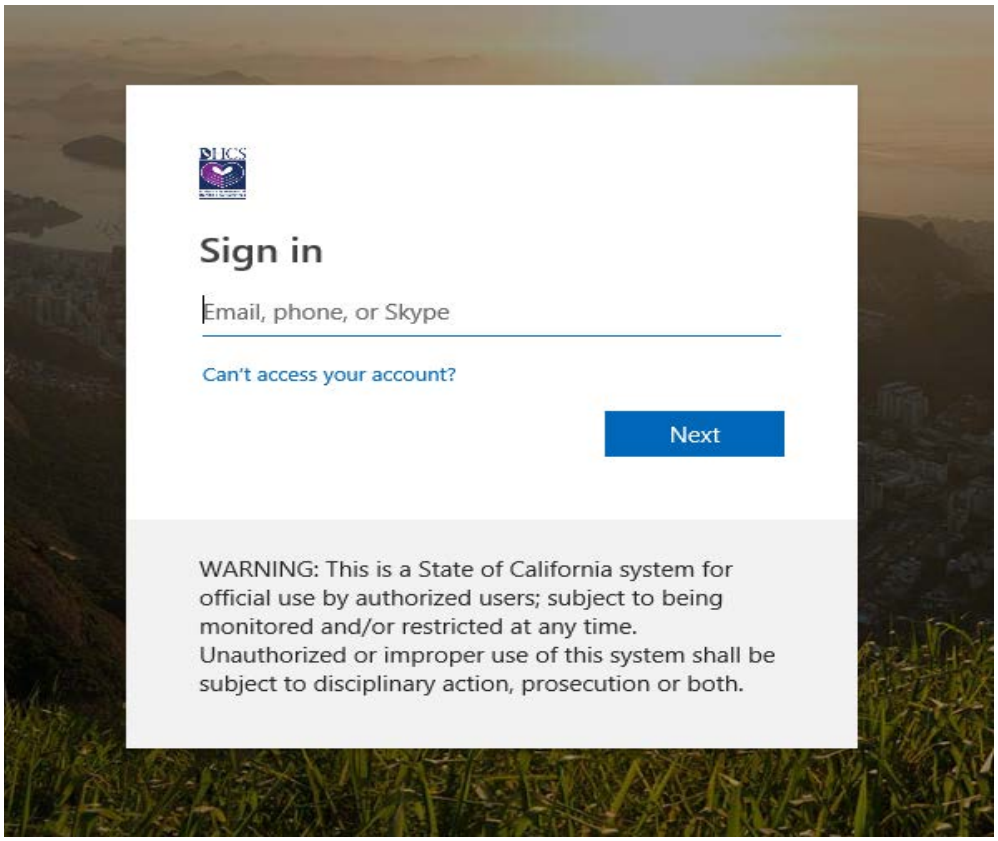
1. From the DHCS Application Portal, click *Log In*



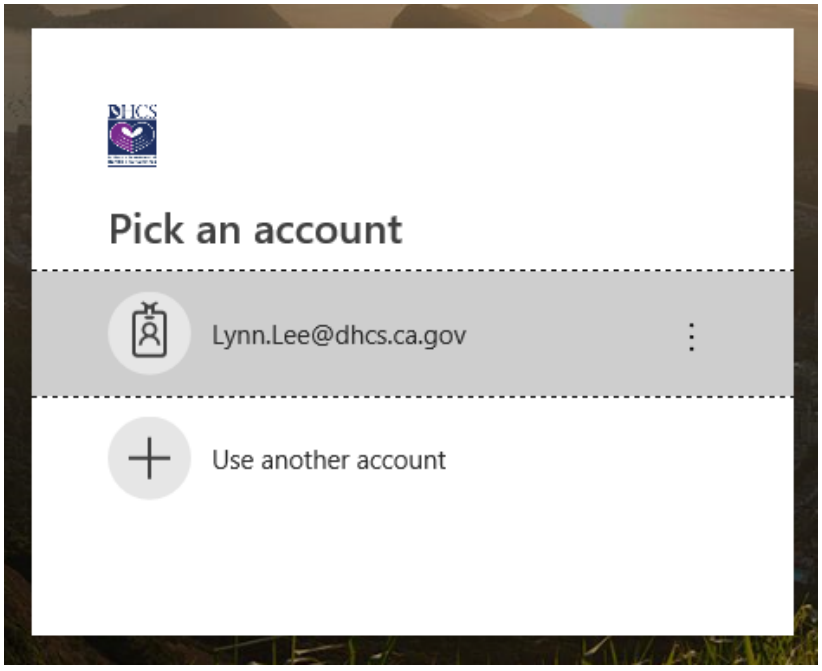


Note: You can also access through the Microsoft My Apps Portal

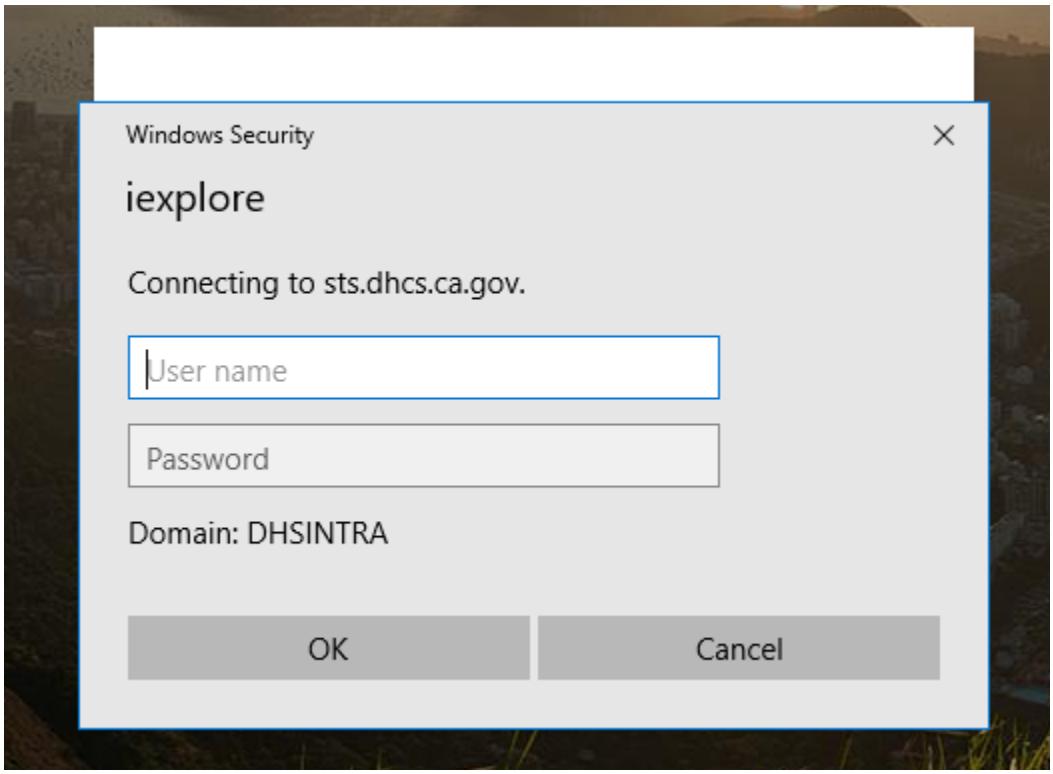
2. When prompted, enter organization email address and click *Next*



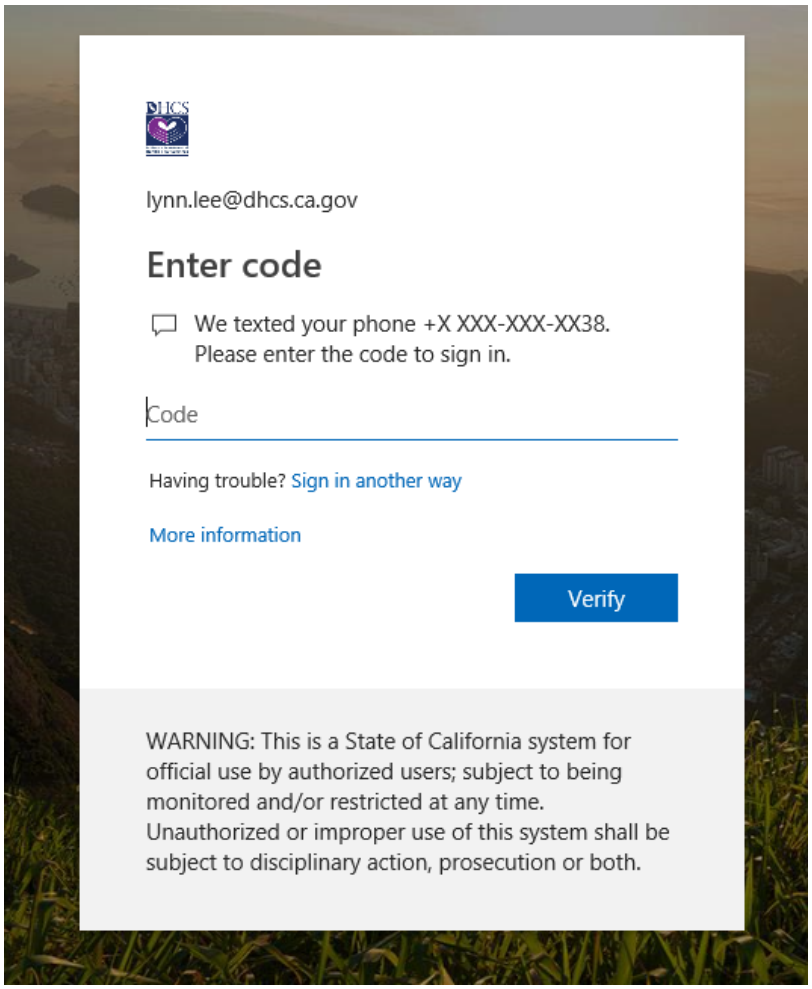
OR when provided a list, choose your organization email address



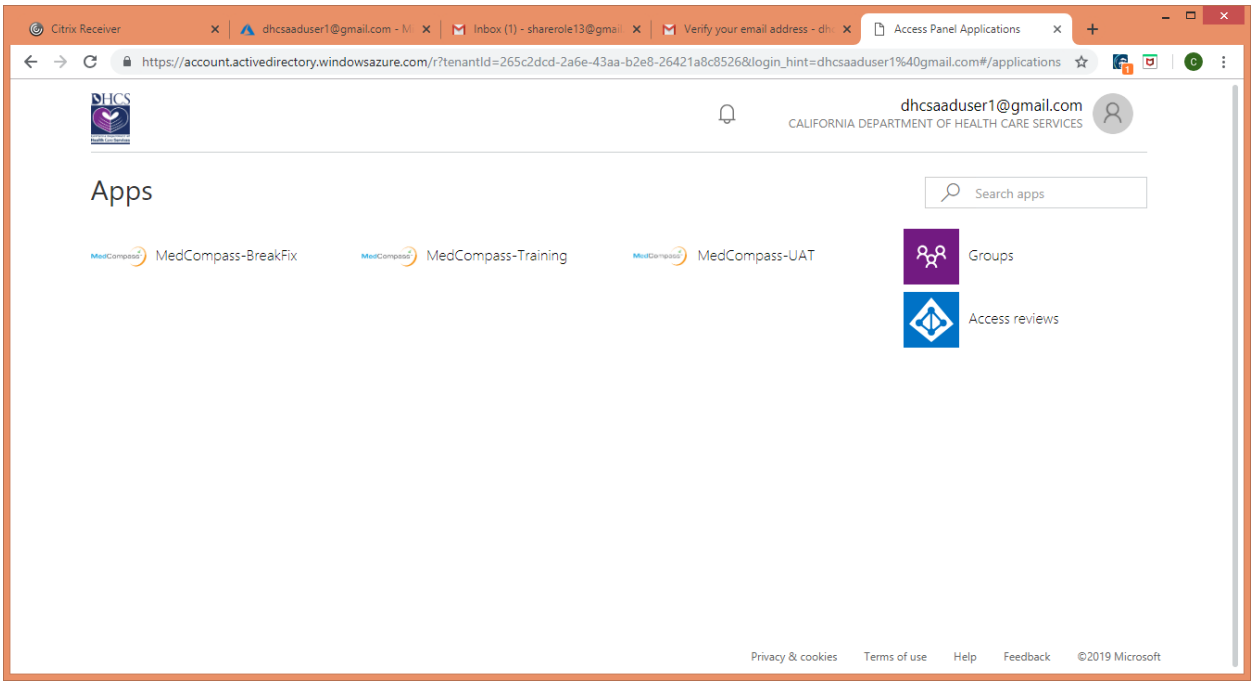
3. If prompted, enter DHCS credentials and click *OK*



4. If prompted, enter MFA code sent and click *Verify*



5. You are now ***SUCCESSFULLY*** logged into the DHCS Application Gallery and can access all DHCS applications you have access to that have been integrated with the Gallery.



EXTERNAL USERS – MICROSOFT ACCOUNT SETUP

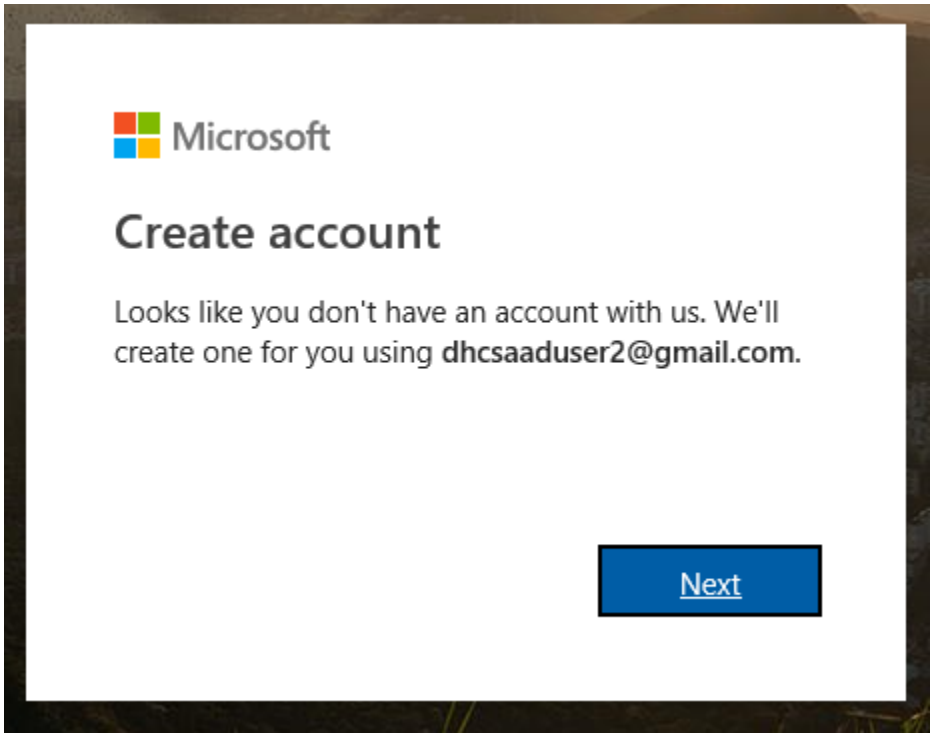
Background

When first logging into Azure Active Directory, users that belong to organizations that do not have existing Microsoft accounts will be asked to create new Microsoft accounts.

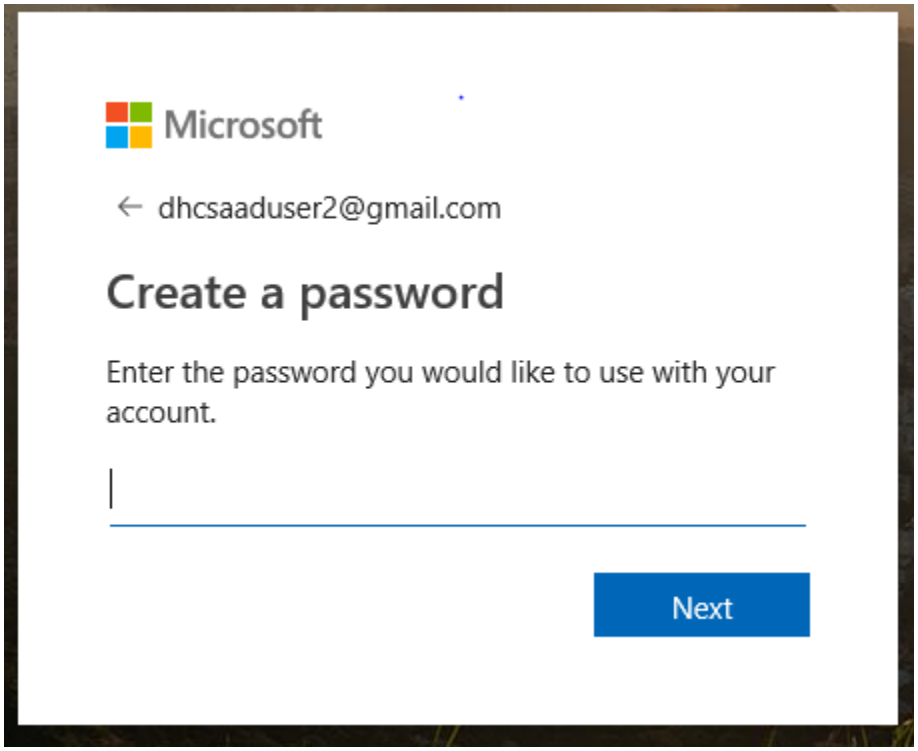
Below describes the steps for users to create their Microsoft account.

Steps

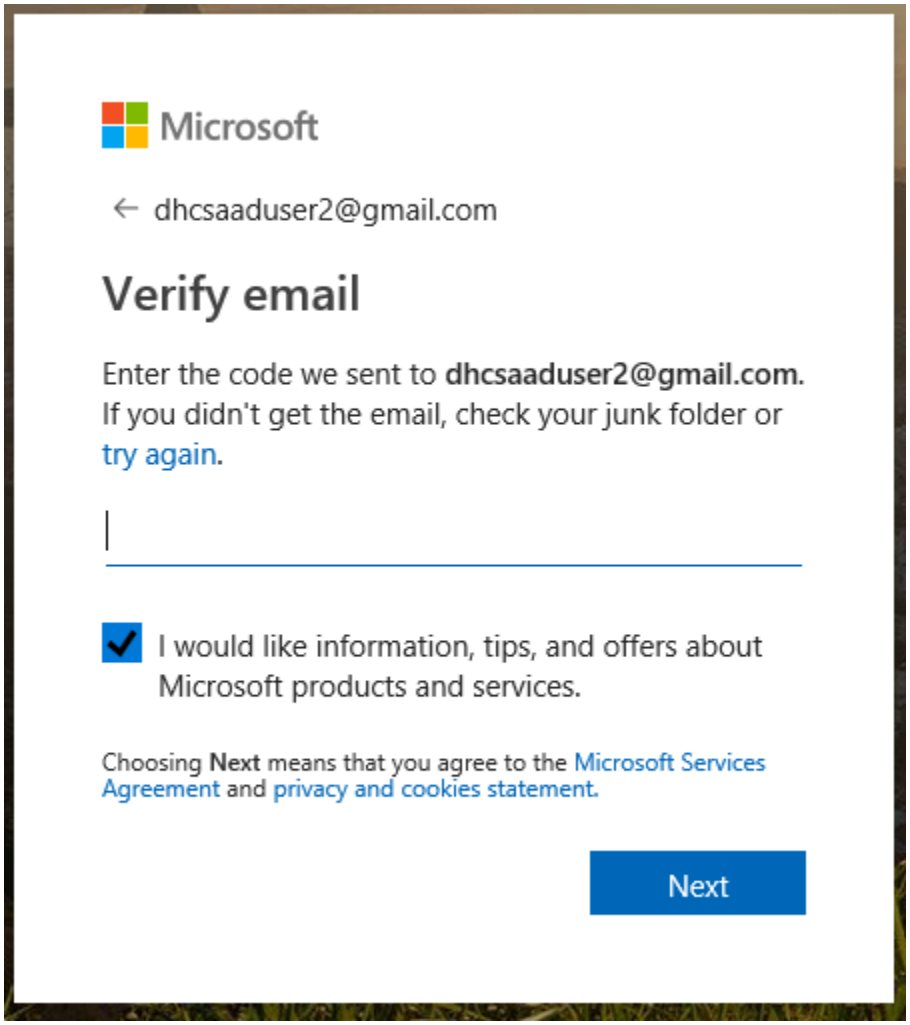
1. When prompted to Create account, click *Next*



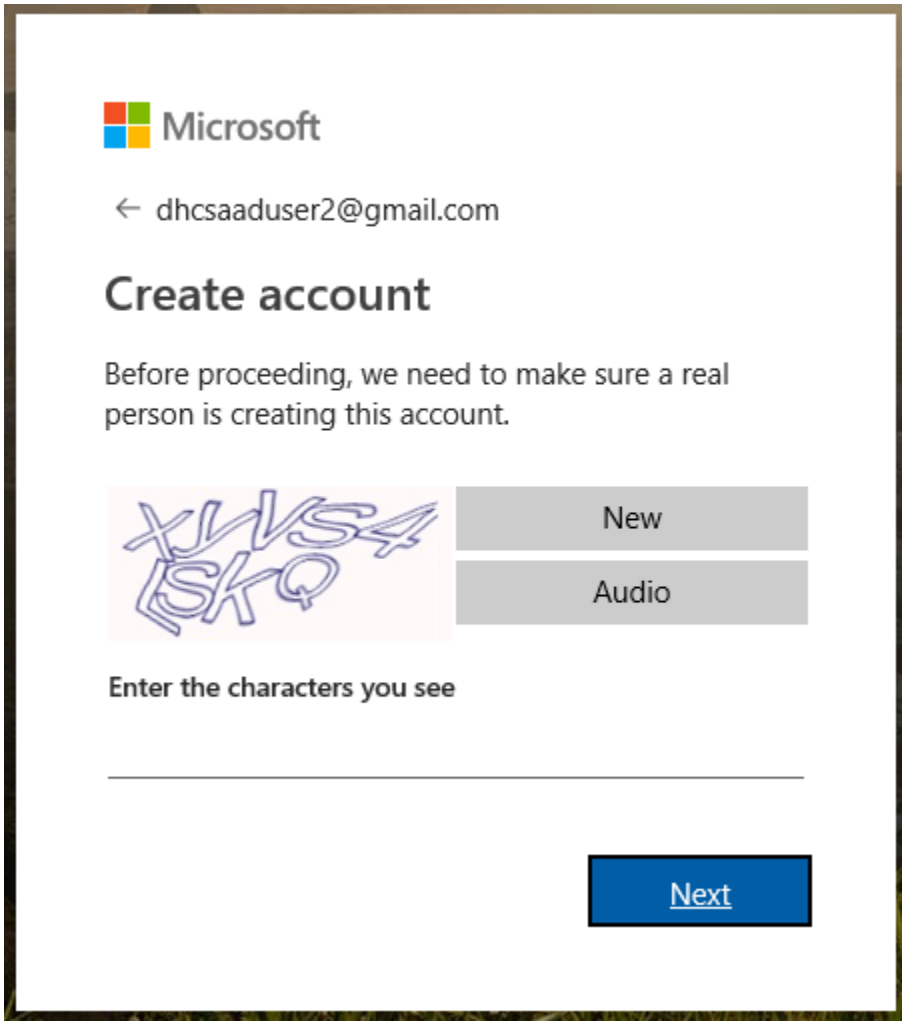
2. When prompted to Create a password, enter the password you would like to use for this account, then, click *Next*



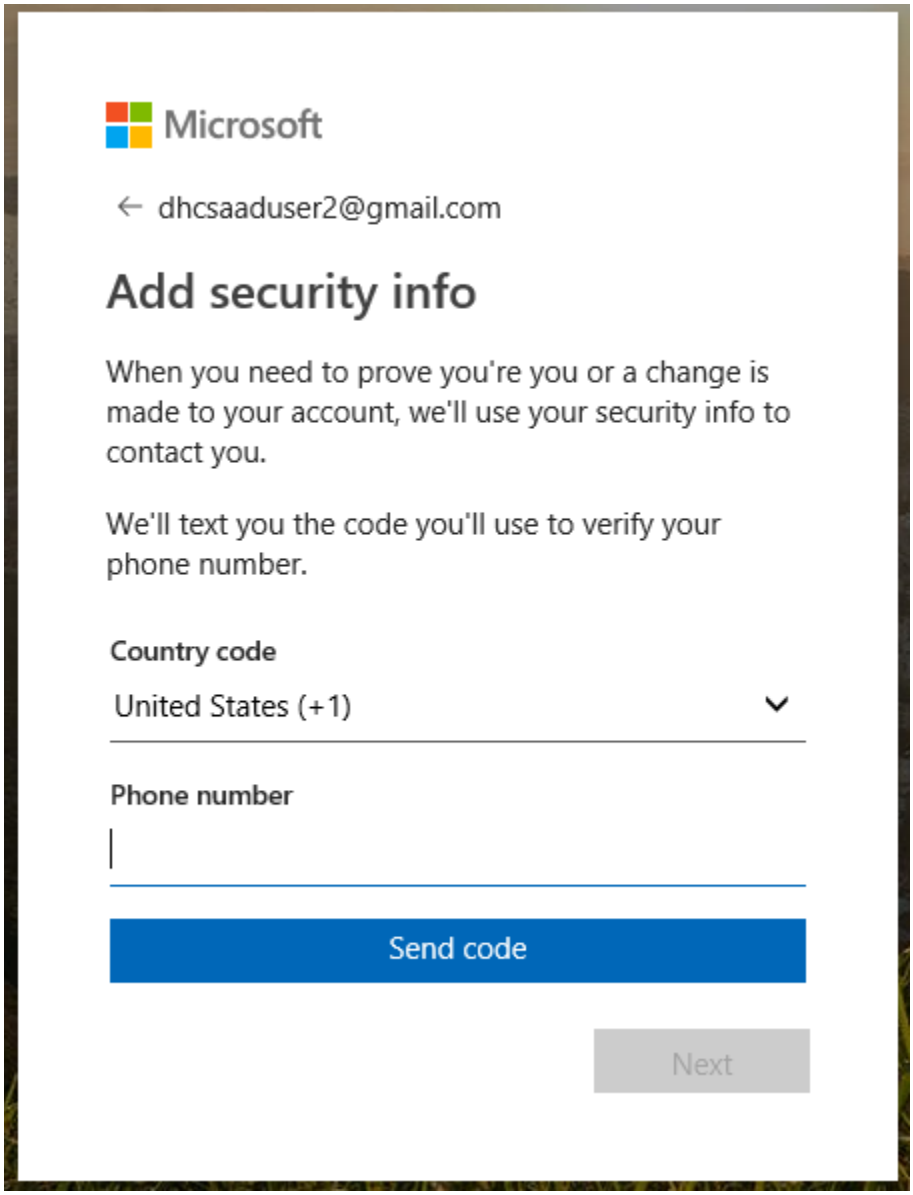
3. When prompted to Verify email, enter the code sent to your email, then, click *Next*



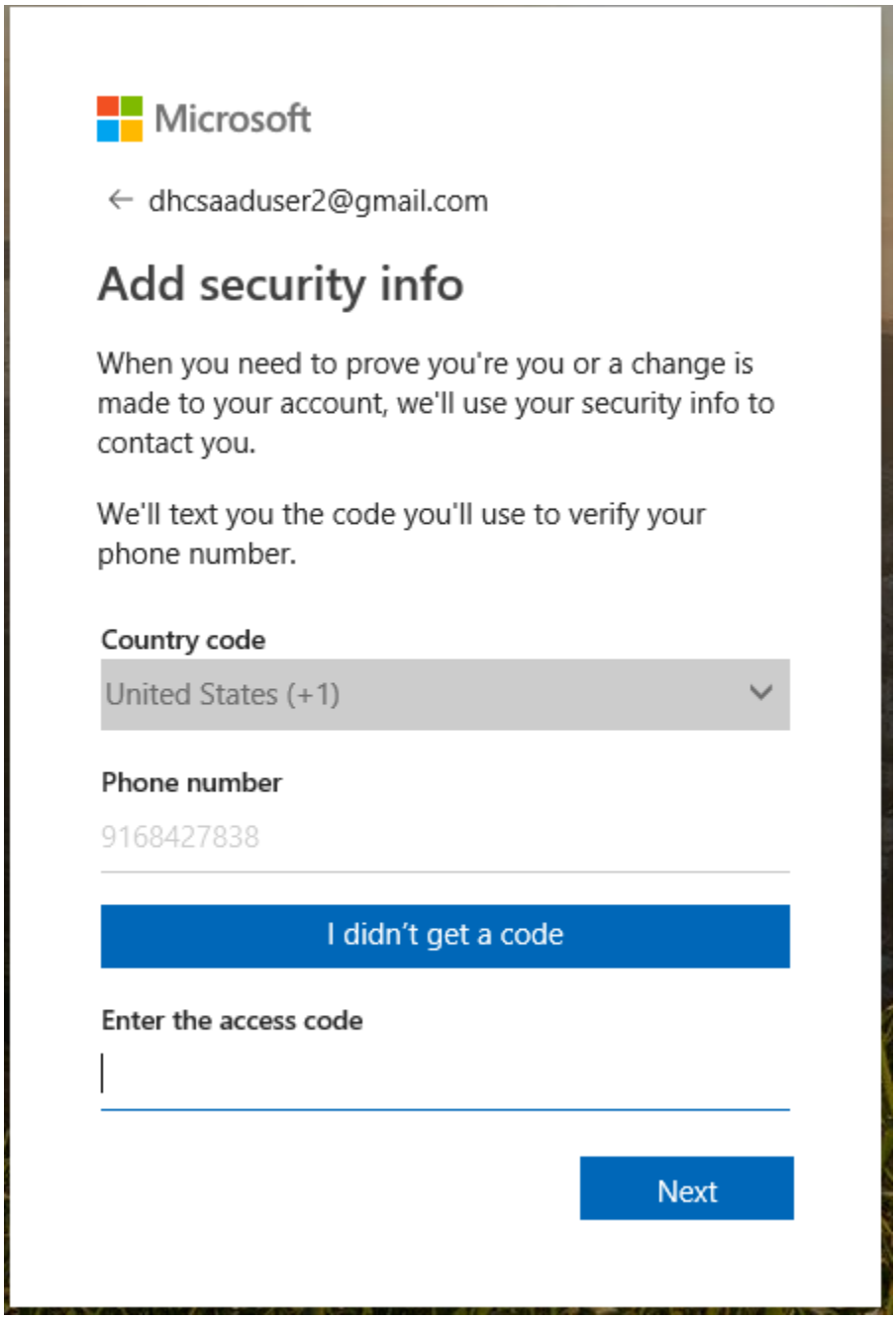
4. When prompted to Create account, enter the characters you see, then, click *Next*



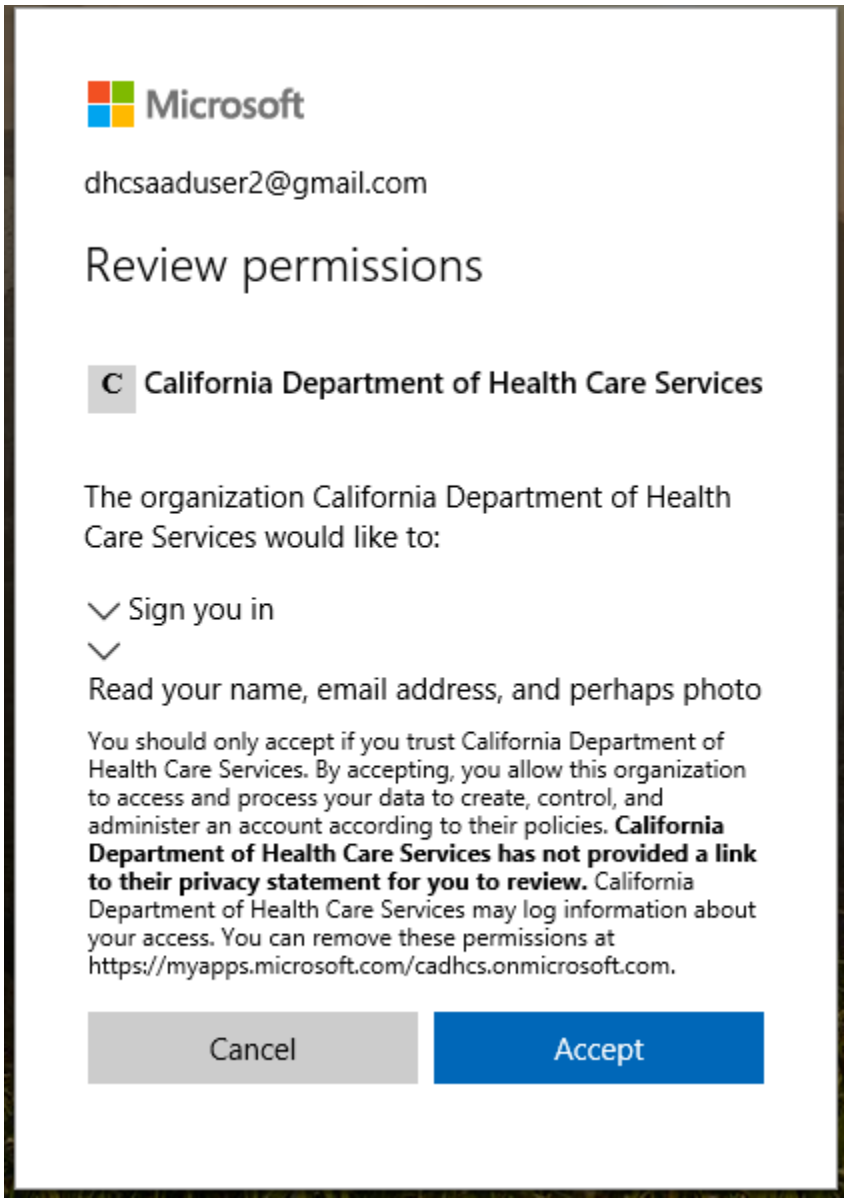
5. When prompted to Add security info, enter your phone number, then, click *Next*



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



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



8. You are now ***SUCCESSFULLY*** logged into the DHCS Application Gallery and can access all DHCS applications you have access to that have been integrated with the Gallery.

MFA INITIAL STEP UP

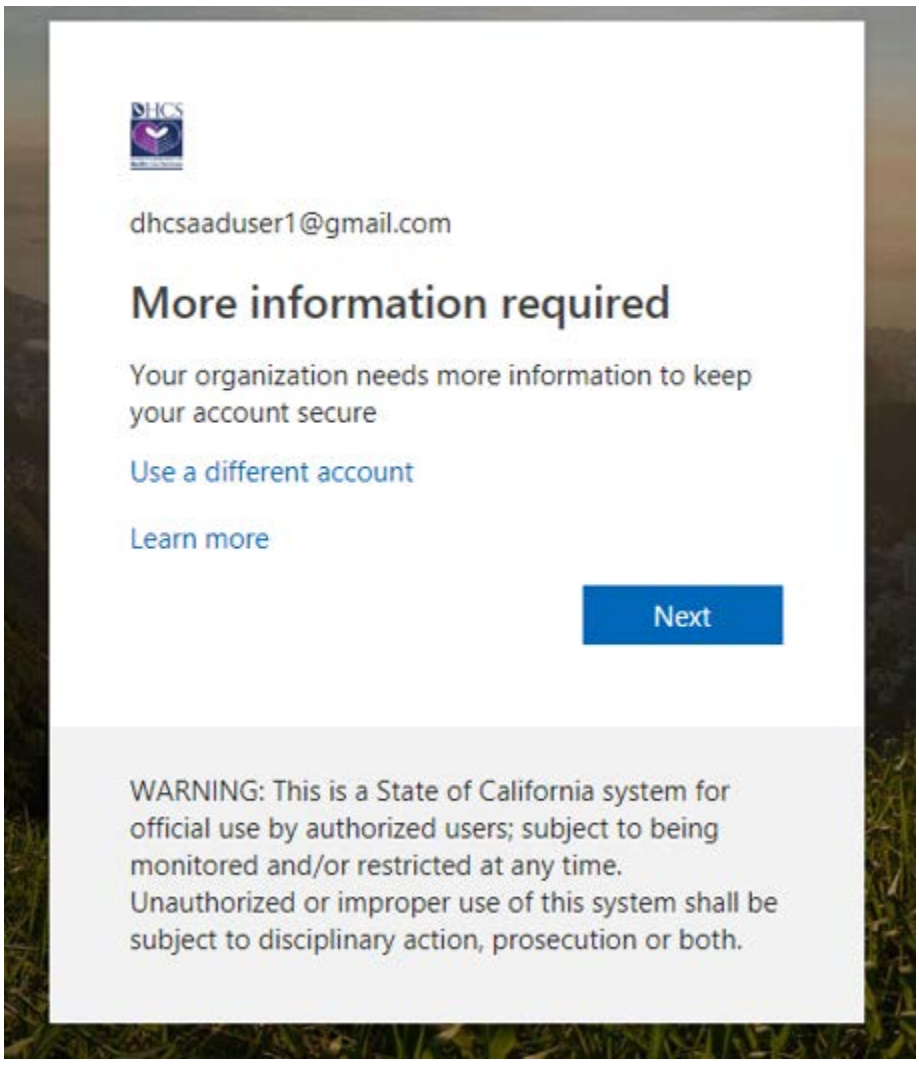
Background

When first logging into Azure Active Directory, users will be prompted to set up additional security verification also referred to as Multi-Factor Authentication (MFA).

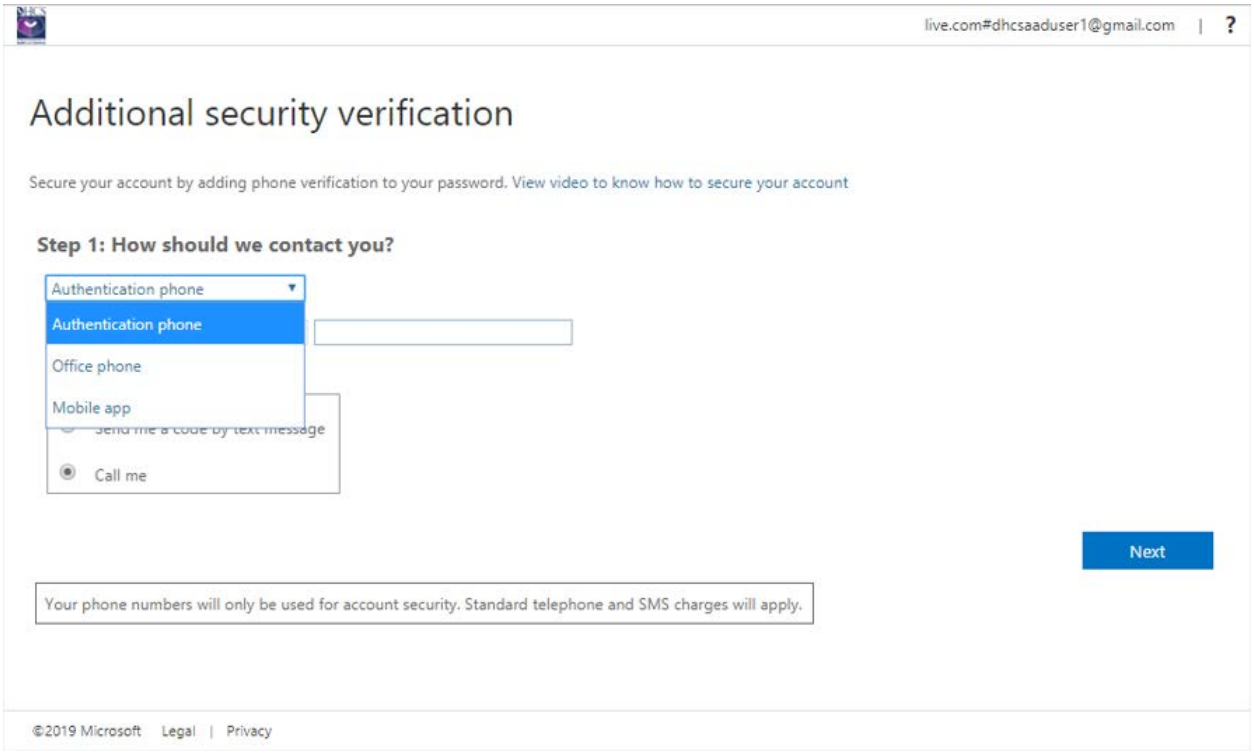
Below describes the steps for users to set up and update their MFA settings.

Steps

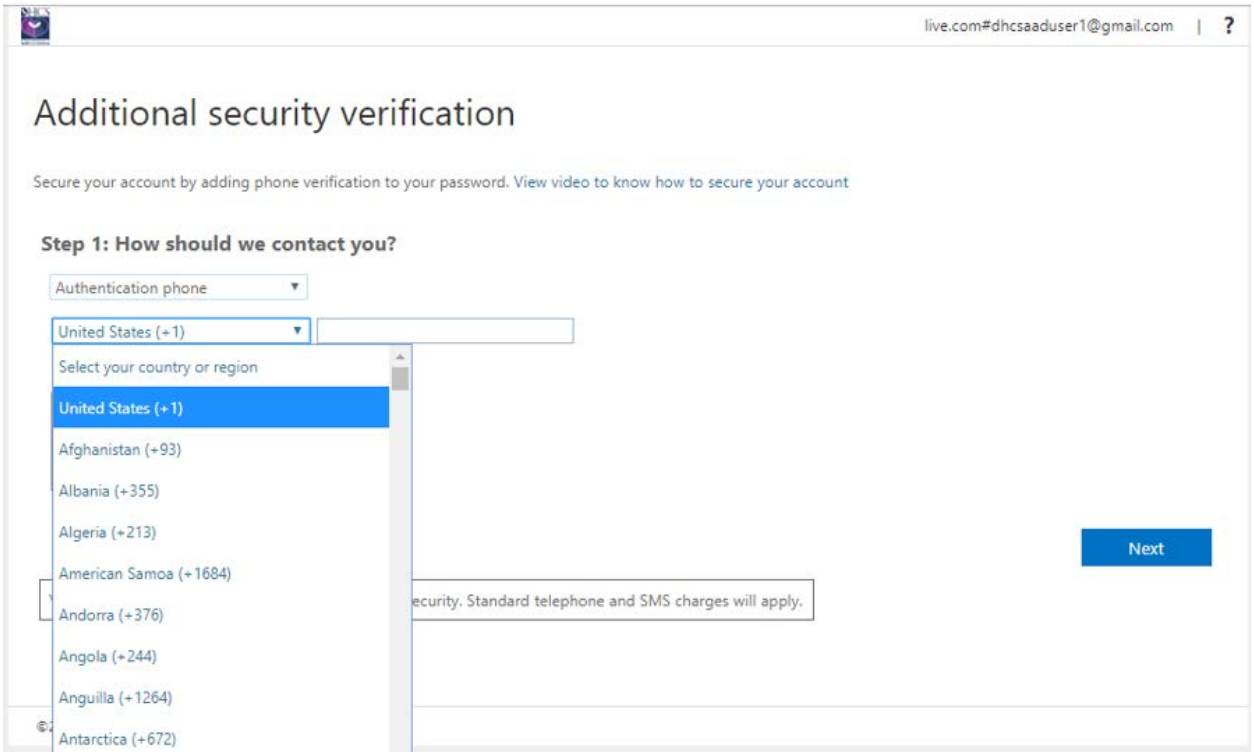
9. When prompted that more information is required, click *Next*



10. On the Additional Security Verification page, select one of the following:
    - Authentication phone (for mobile devices) OR
    - Office phone (for landlines)

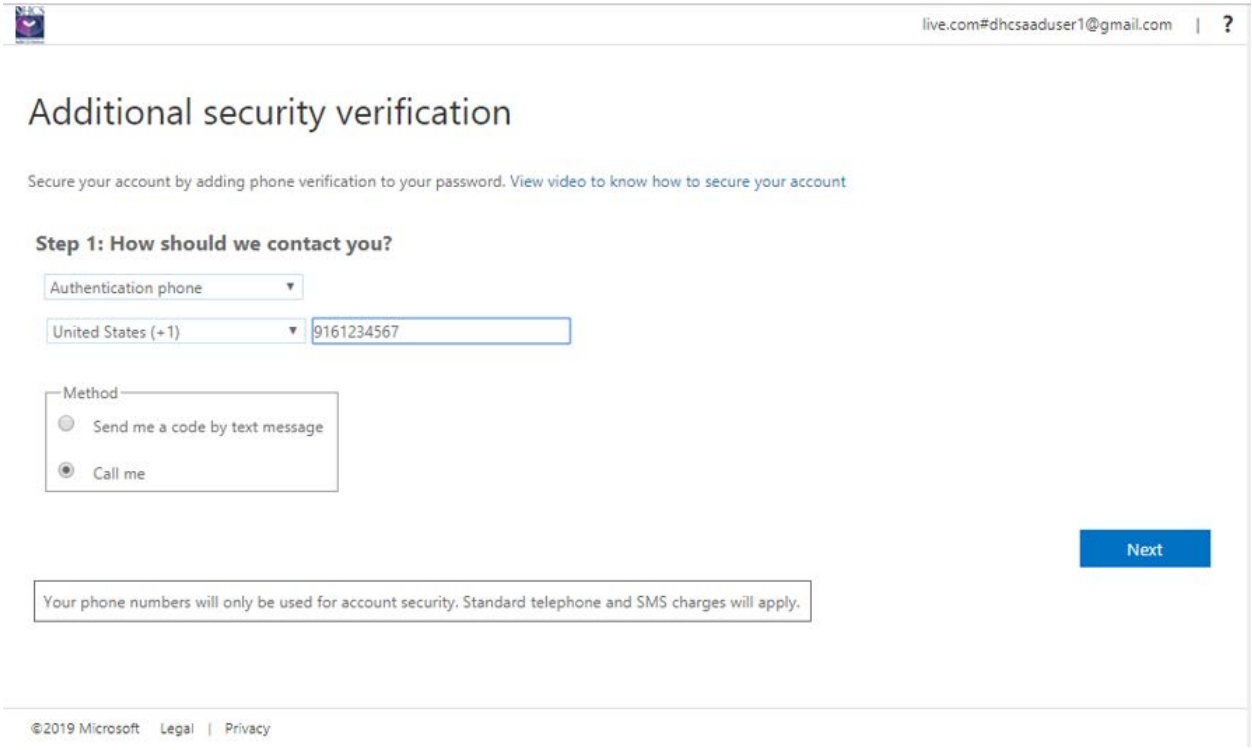


a. Next, select United States and enter your number

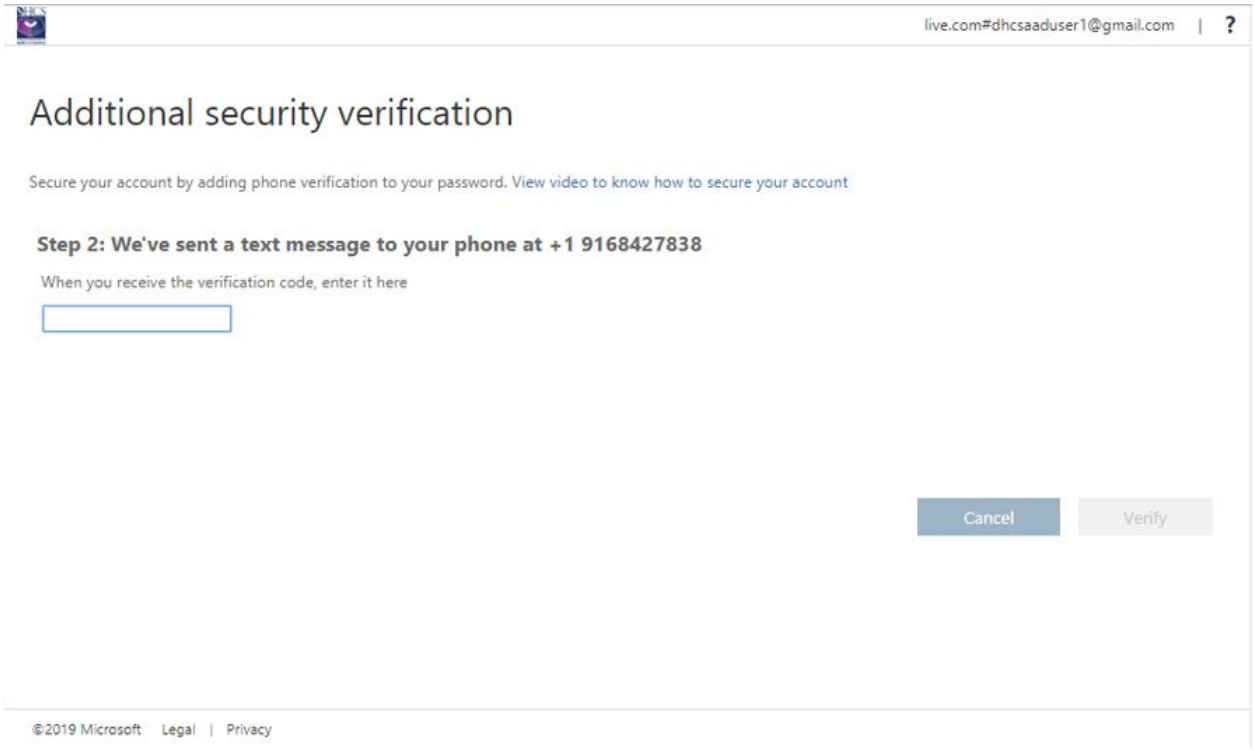


b. Lastly, select one of the following methods and click *Next*

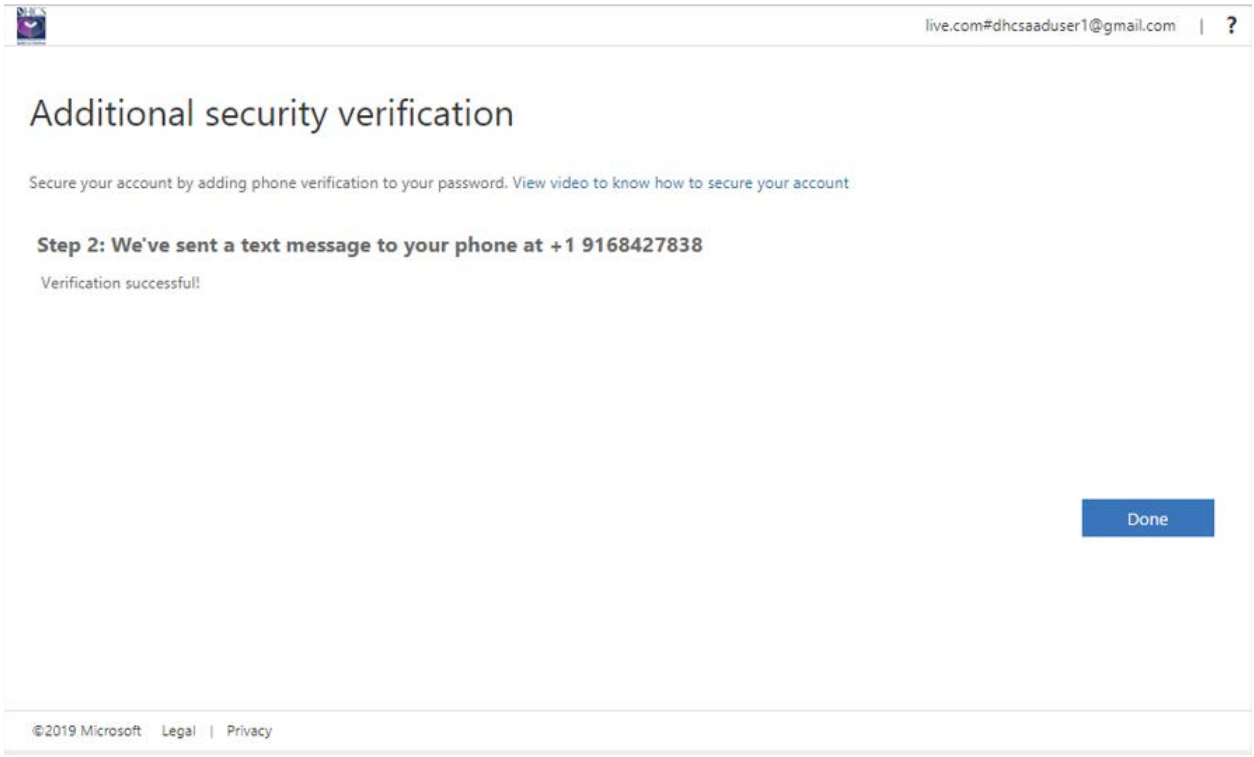
- Send me a code by text message (for mobile devices) OR
- Call me (for office phones/landlines)



11. On the Additional Security Verification page, enter the verification code received and click *Verify*



12. On the Additional Security Verification page, when verification is successful you will receive a confirmation, click *Done*



13. Once verified, you are now SUCCESSFULLY logged into the DHCS Application Gallery or the Application you selected to access.

MFA ADDITIONS OR CHANGES

Background

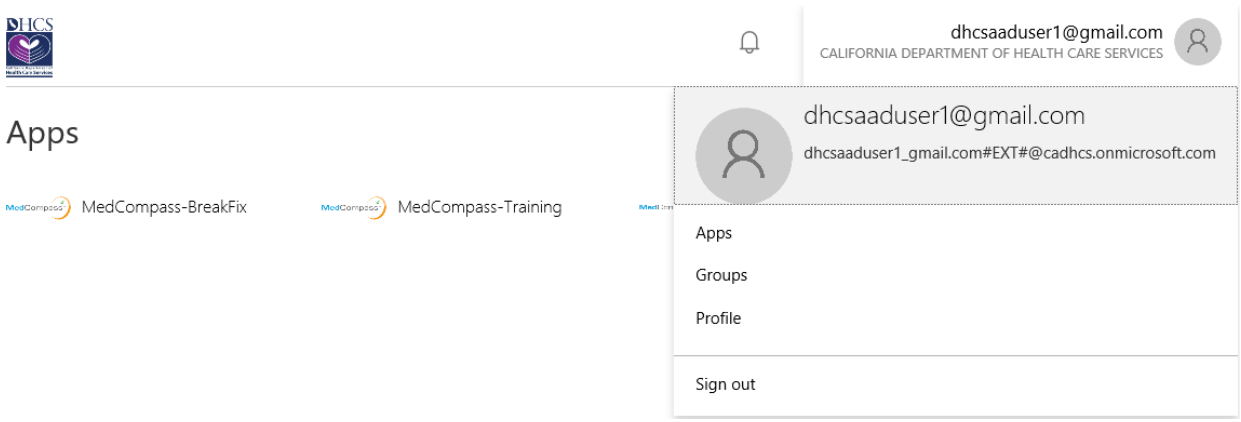
When you want to change your MFA authentication phone for any reason, you can do this through the DHCS Application Gallery.

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

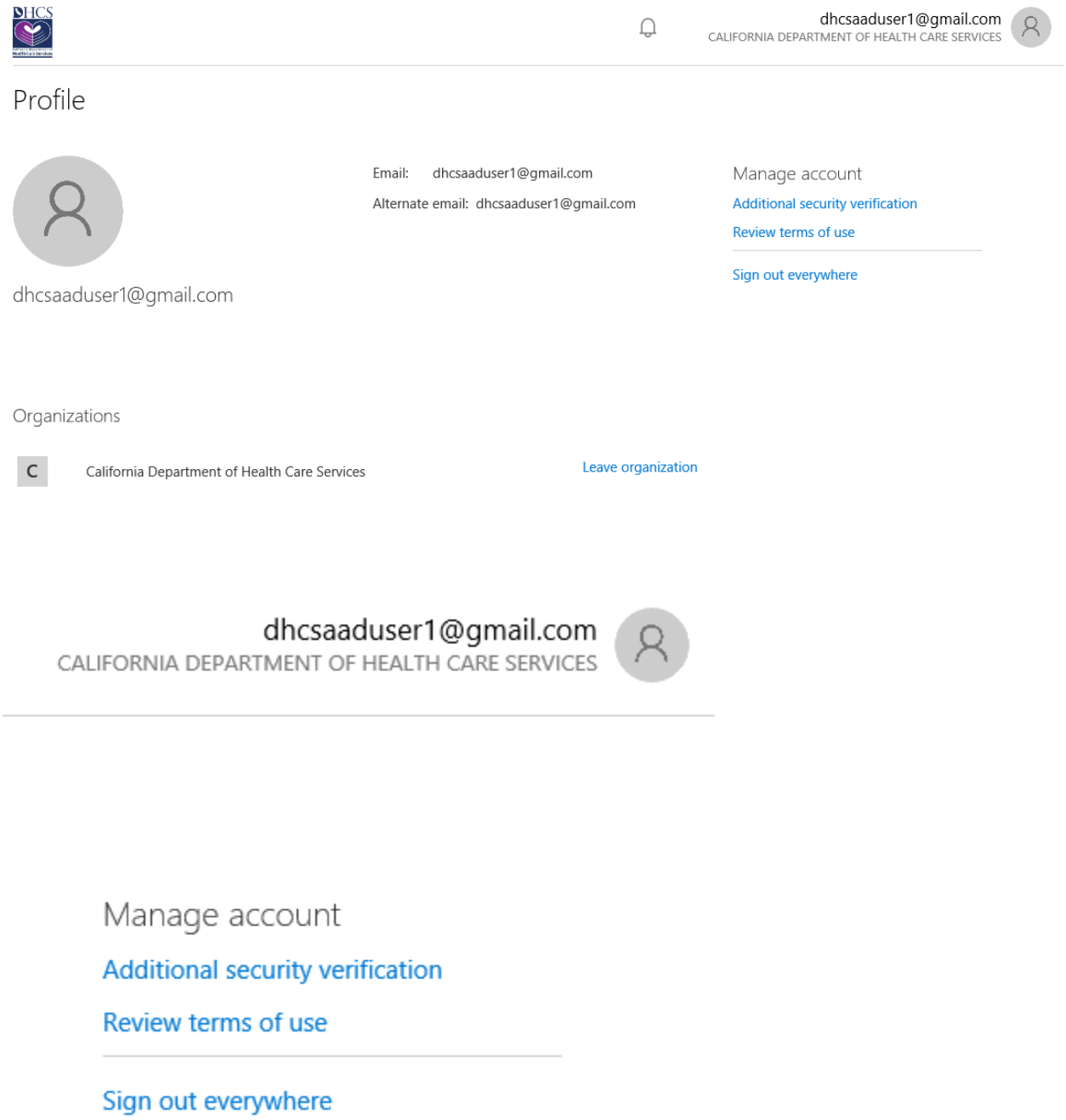
> NOTE: Office phone cannot be updated through these steps; office phone information must be updated via Global Address List (GAL) profile update process.

Steps

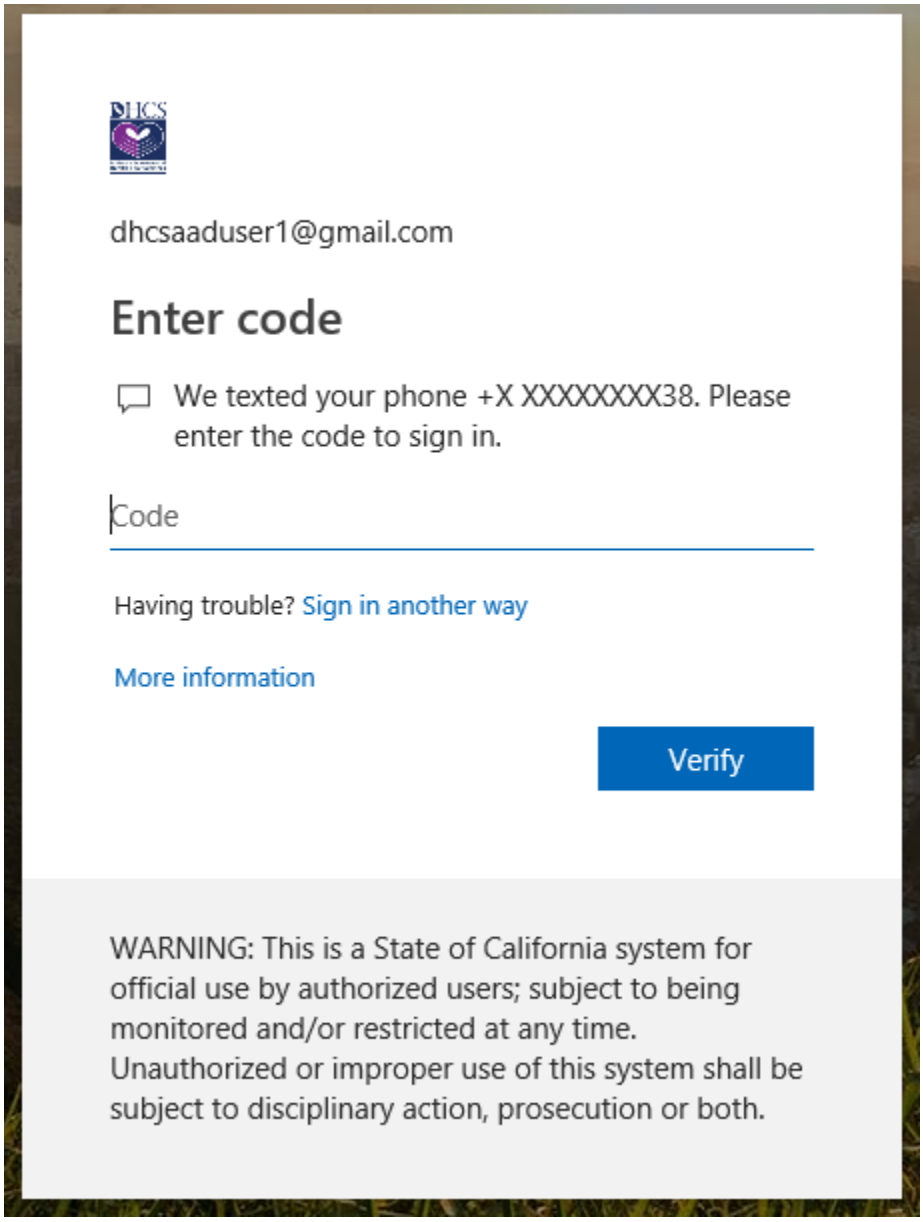
1. From the DHCS Application Gallery page, click on your email in the upper right corner to get the following drop down selections and select Profile



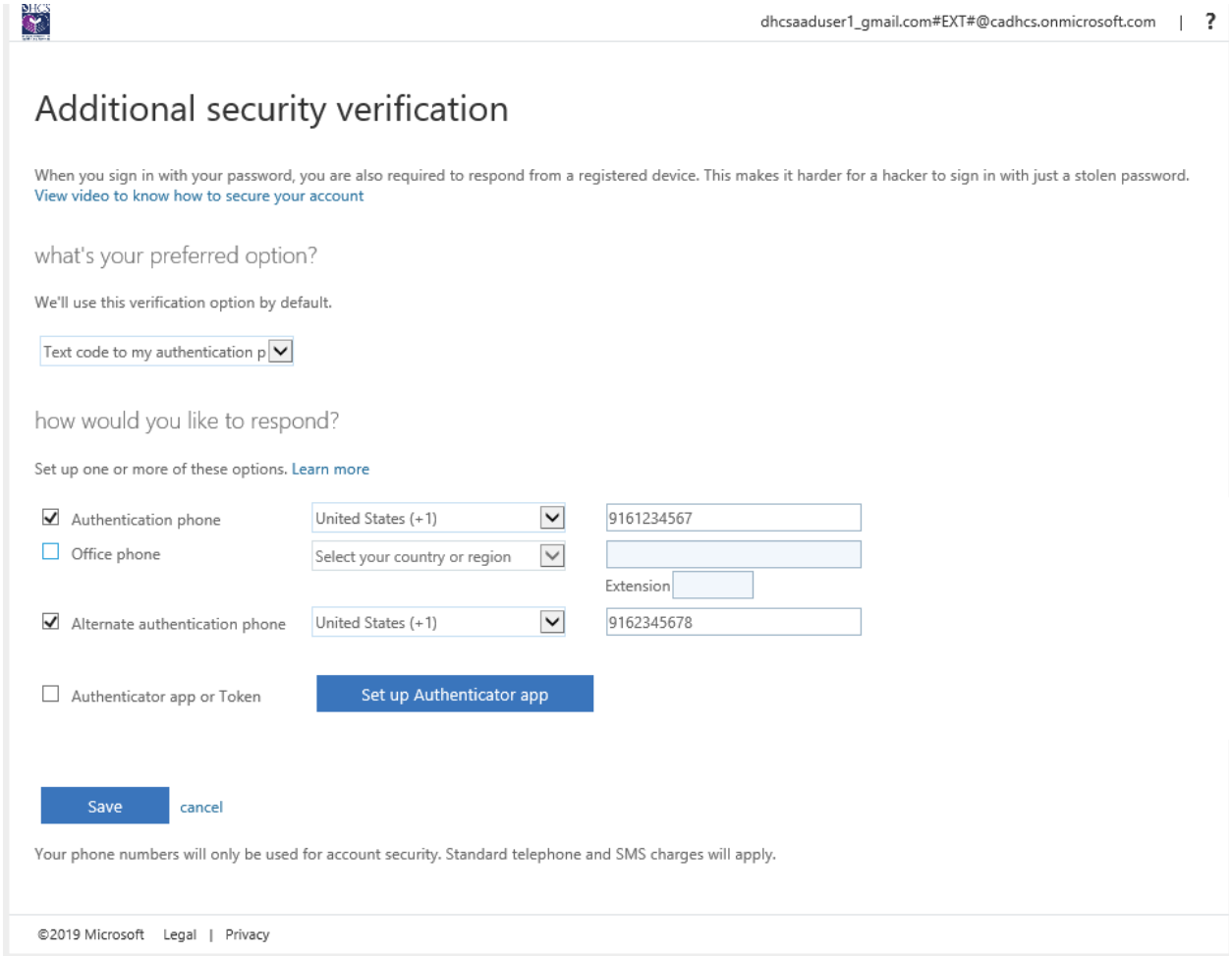
2. From the Profile page, under Manage Account, click Additional security verification



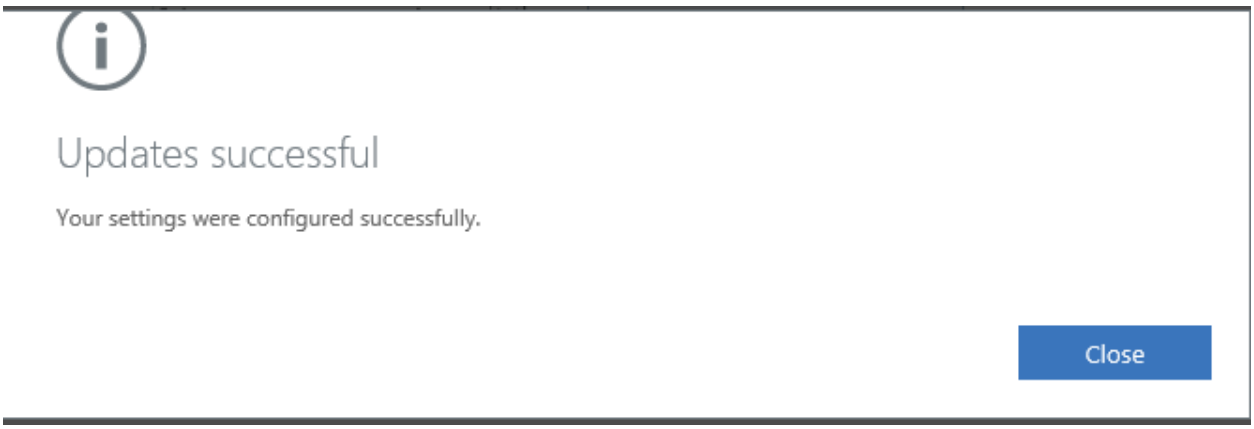
3. If prompted for MFA, enter the verification code received and click *Verify*



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



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



ACCESS REVIEWS

Background

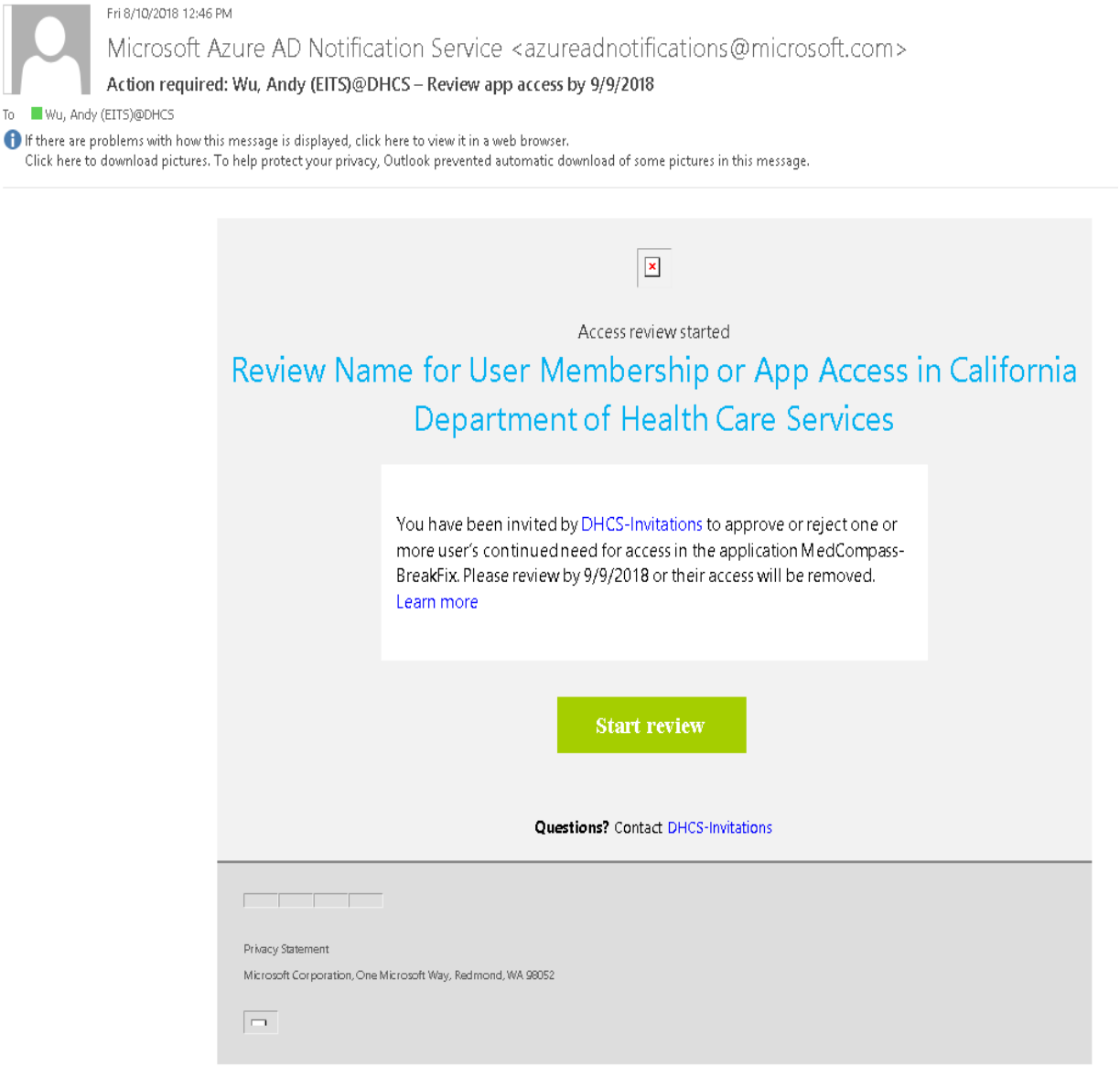
Azure Active Directory (Azure AD) Access Reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and privileged role assignments. Azure AD simplifies how enterprises manage access to applications and members of groups in Azure AD and other Microsoft Online Services with a feature called Access Reviews.

Access Reviews ensure that all users have appropriate access to complete their business function. Access Reviews are to ensure that users who were invited and/or added to a group and/or application continue to need access.

Below describes the steps for users that have access to applications and memberships in groups in Azure AD to complete Access Reviews.

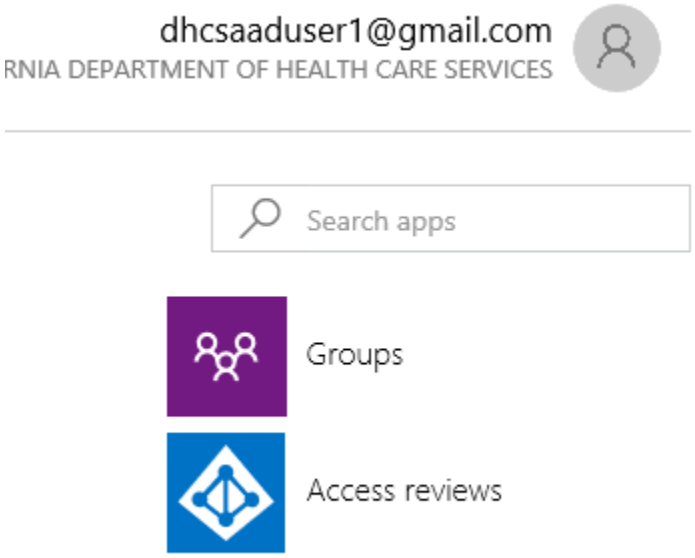
Steps

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.



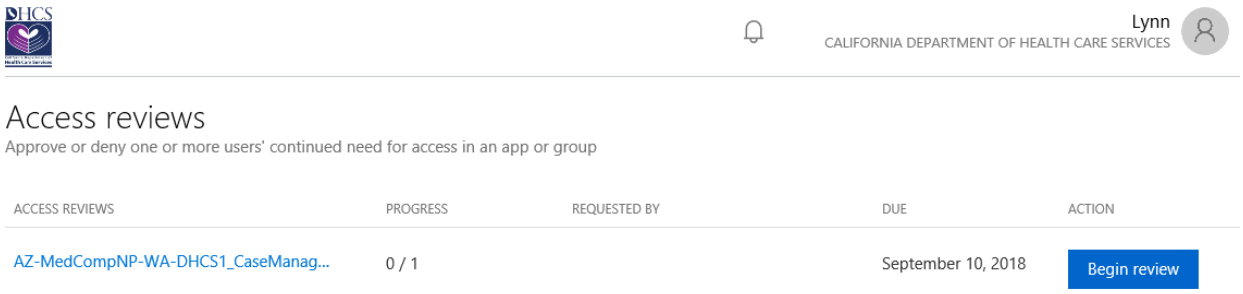
2. Click *Start Review* link in email

OR Access Reviews in DHCS Application Gallery



Note: If you have access to more than one organization, select the user symbol in the upper-right corner of the page, which displays your name and default organization. Then, select the organization that requested an access review. 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*



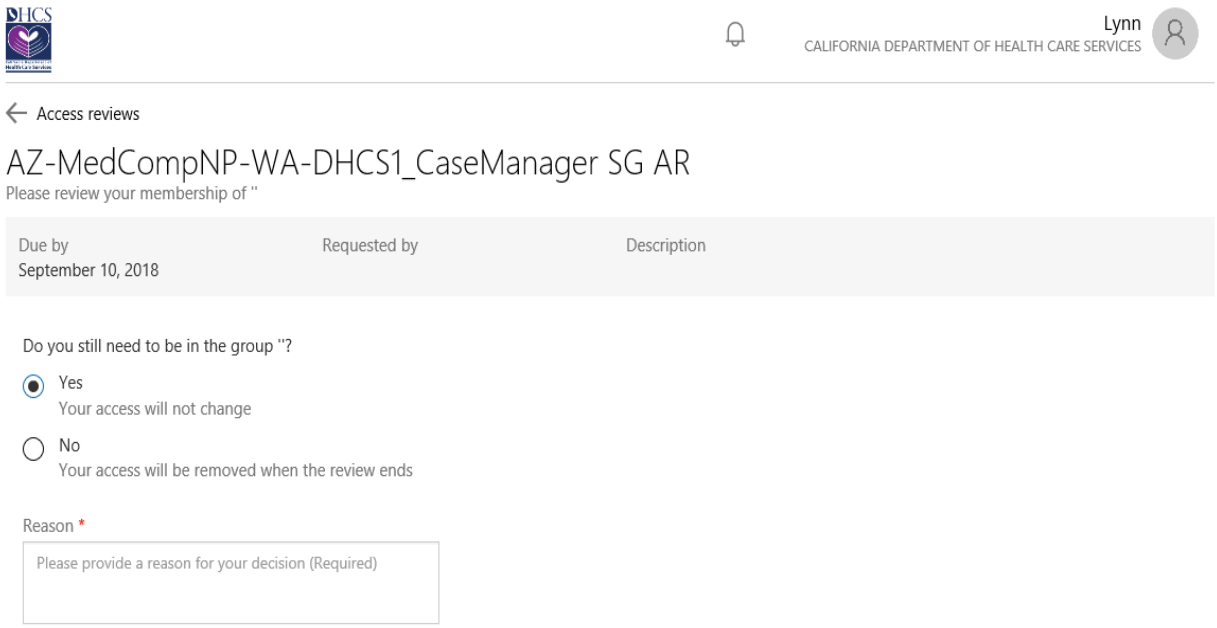
INDIVIDUAL MEMBER (USER) ACCESS REVIEWS

4. If review is for Members (i.e. individual users), the following will display.

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

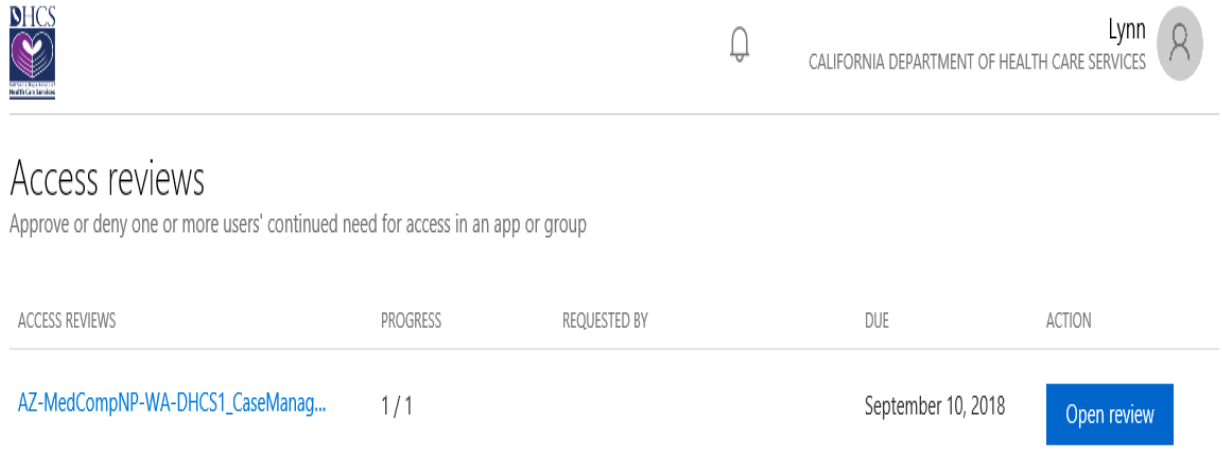
Examples:	Needed to perform Help Desk Support
	Needed to perform Case Management duties
	Needed to audit external vendor activities

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

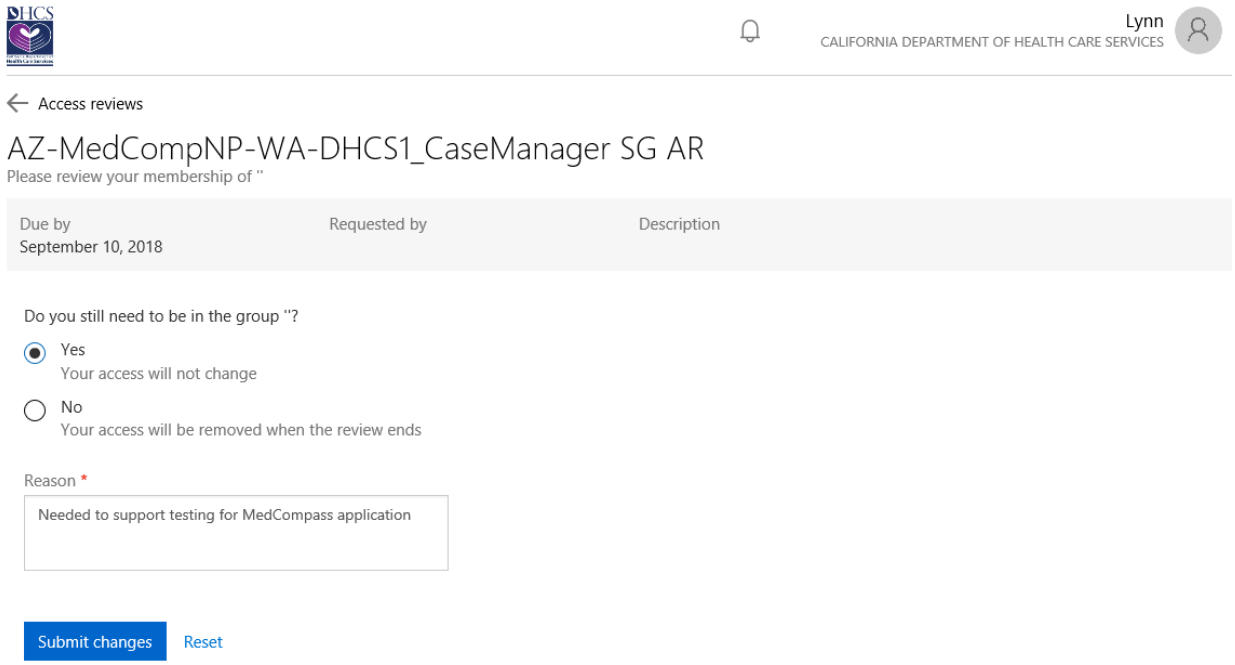


YOU HAVE SUCCESSFULLY COMPLETED THE MEMBER ACCESS REVIEW

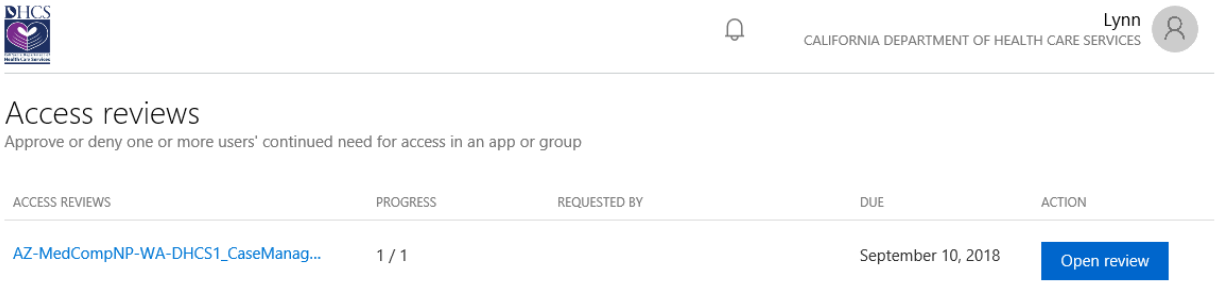
1. Click *Open Review* to submit changes, if needed.

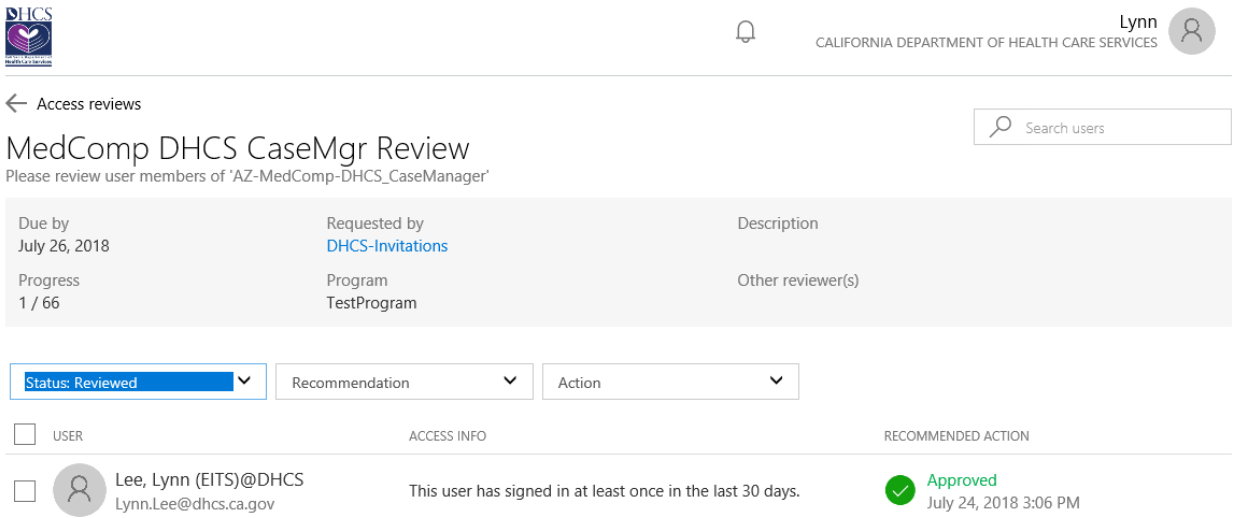


2. Update response and Click *Submit Changes*

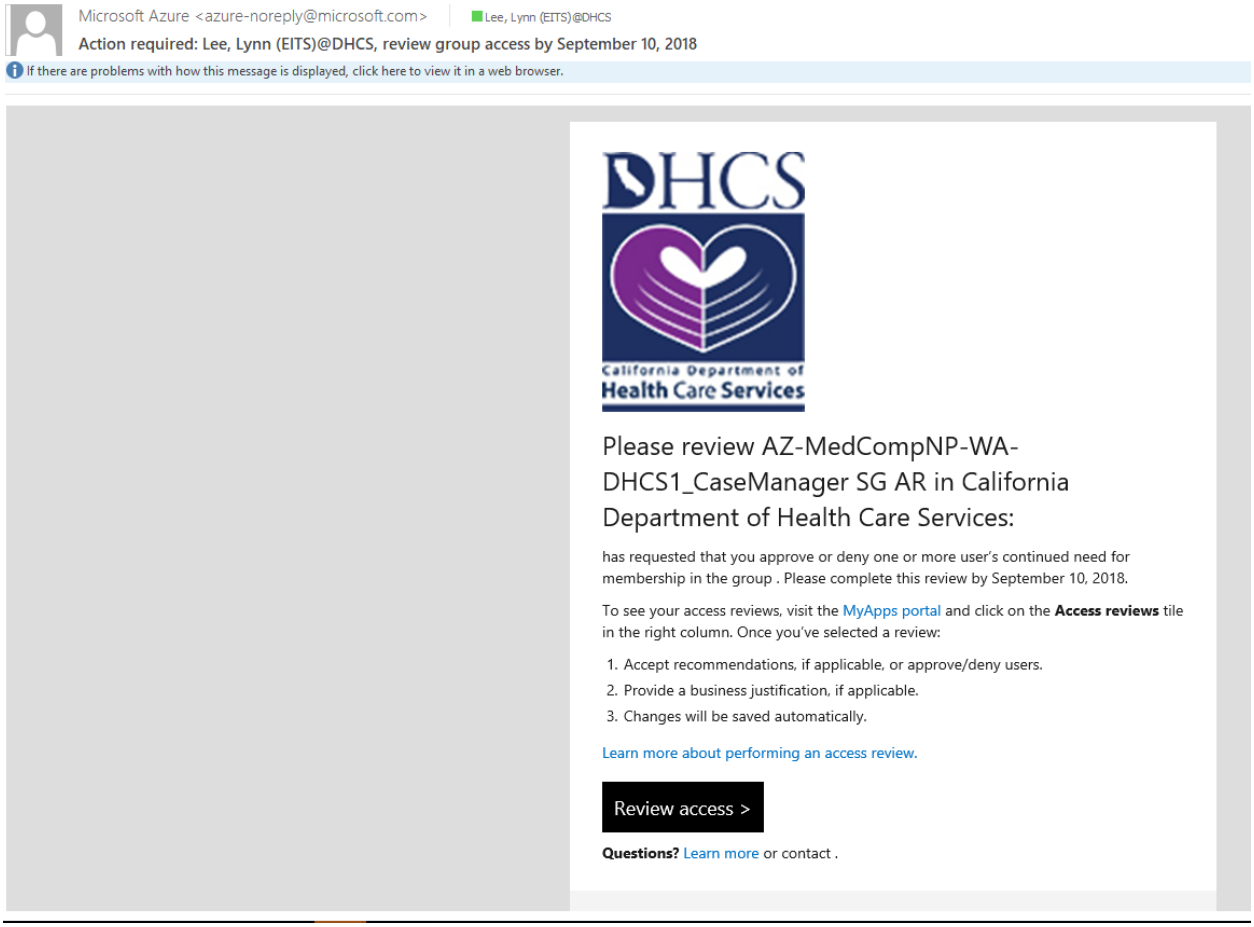


1. Click *Open Review* to view Status of Access Review





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: Lee, Lynn (EITS)@DHCS, 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 AZ-MedCompNP-WA-DHCS1_CaseManager SG AR in 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.

Review access >

Questions? Learn more or contact .