



Application Portal User Manual



Application Portal User Manual

Table of Contents

Introduction	3
Invitation Email	4
Logging In	5
Steps.....	5
Edge and IE.....	6
Chrome.....	7
Access an Application.....	9
View Group Information	10
Create a New Microsoft Account.....	11
Background.....	11
Steps.....	12
Multi-Factor Authentication (MFA) Setup.....	16
Background.....	16
Steps.....	16



Application Portal User Manual

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.

Application Portal User Manual

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: cadbes.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 (cadbes.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

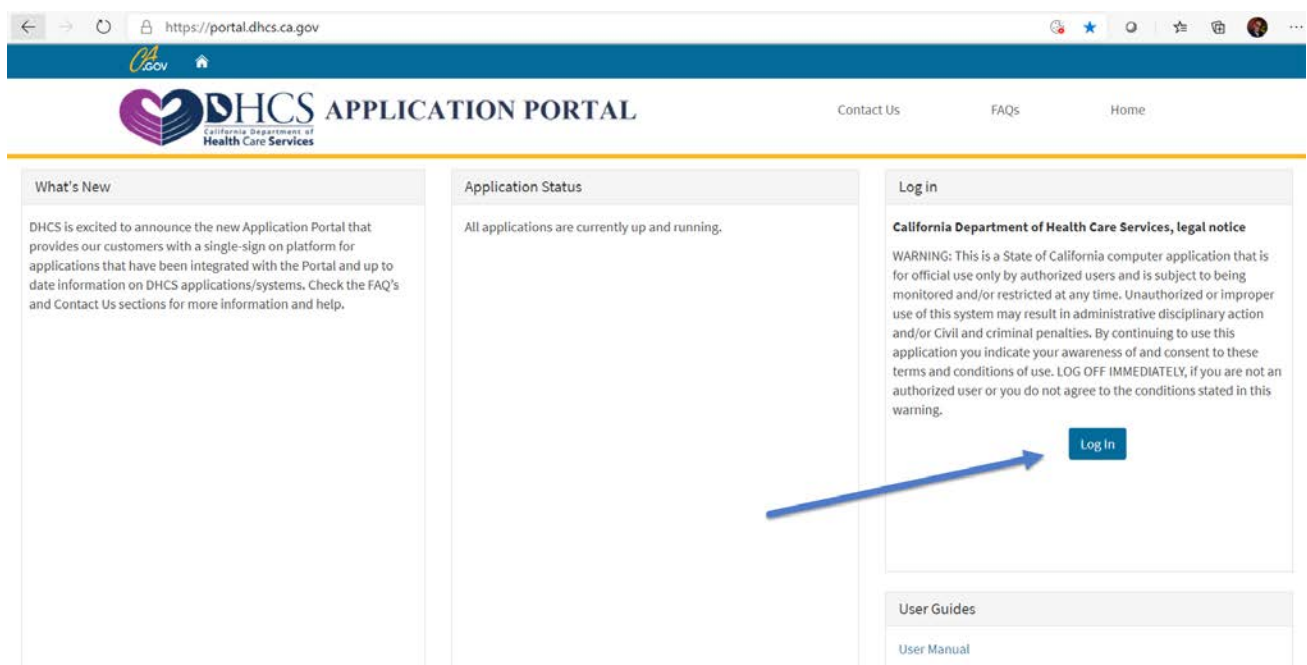


Application Portal User Manual

Logging In

Steps

1. From the [DHCS Application Portal](https://portal.dhcs.ca.gov), select Log In

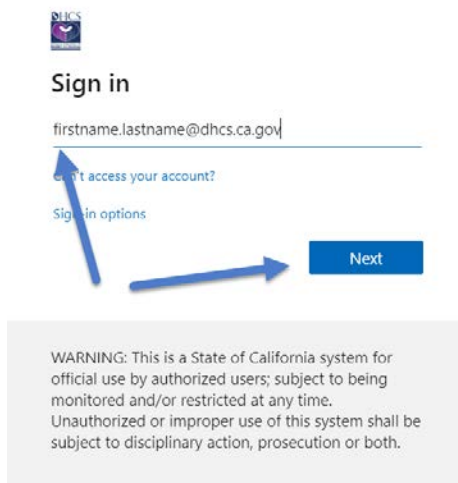


The log in screens may look different based on the browser used and the organizational configuration. Please see the following examples. Your experiences may vary.

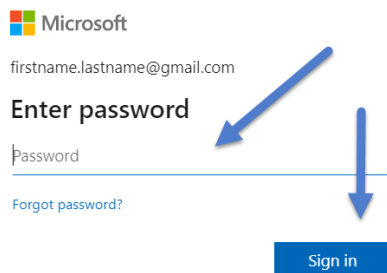
Application Portal User Manual

Edge and IE

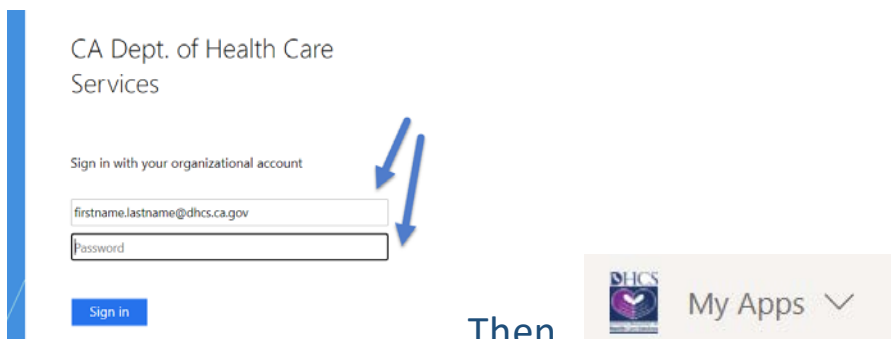
2. Enter work email address, select Next



Enter password



Then...



Then...

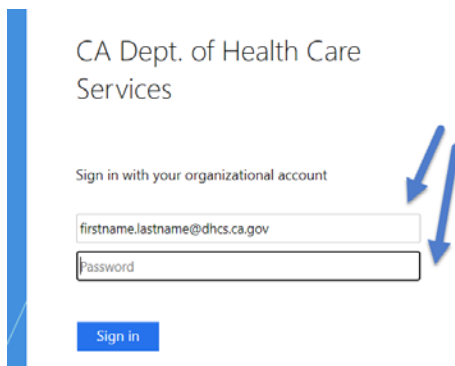
Application Portal User Manual

Chrome

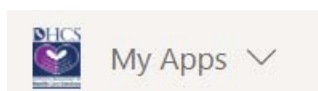
3. Pick an account or Use another account



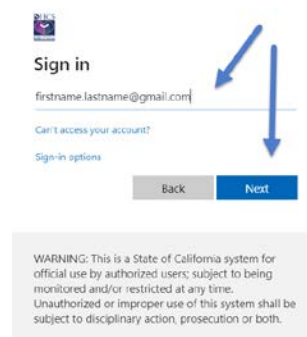
If dhcs.ca.gov or known...



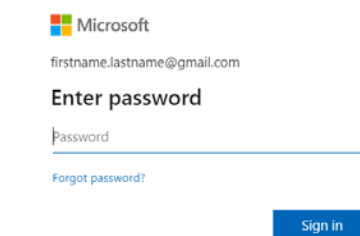
Then...



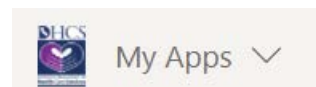
If Using another account unknown to Microsoft...



Then...



Then...



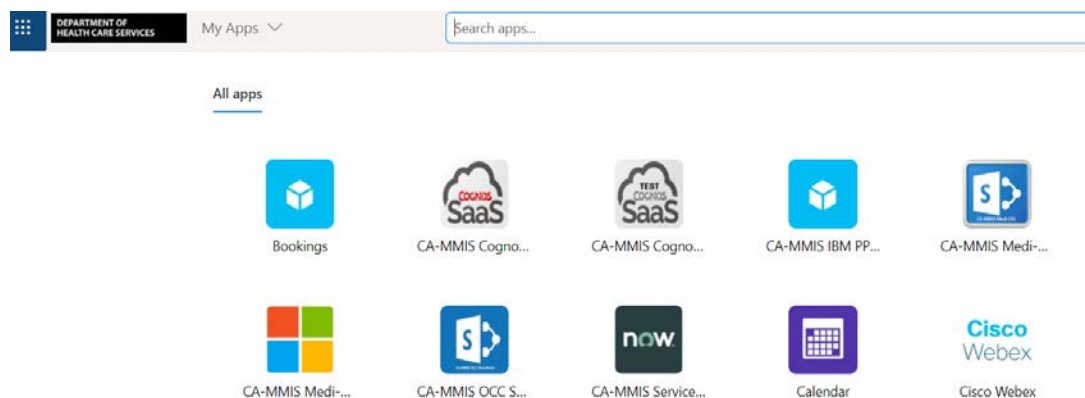
Application Portal User Manual

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.

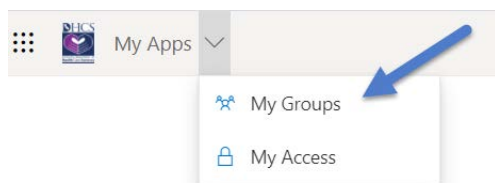
More information provided in the “[Multi-Factor Authentication \(MFA\) Setup](#)” section below.

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.

Application Portal User Manual

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.

Application Portal User Manual

Create a New Microsoft Account

Background

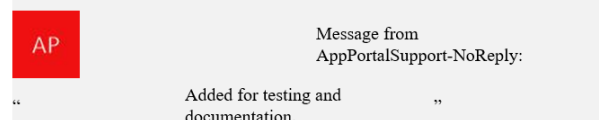
When first logging into the DHCS Application Portal, members are asked to create a new Microsoft account – if belonging to an organization without Microsoft Office 365 / Azure Active Directory (AAD) accounts. An email is received from Microsoft Invitations on behalf of California Department of Health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



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.

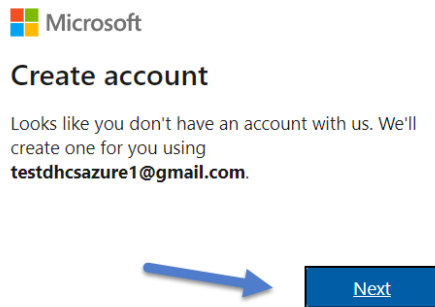


Please see the following for members to create a Microsoft account.

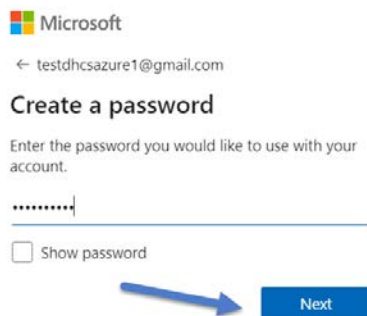
Application Portal User Manual

Steps

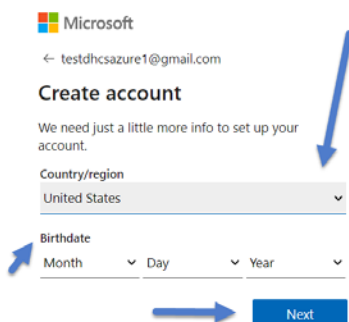
1. When prompted to Create account, select Next



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

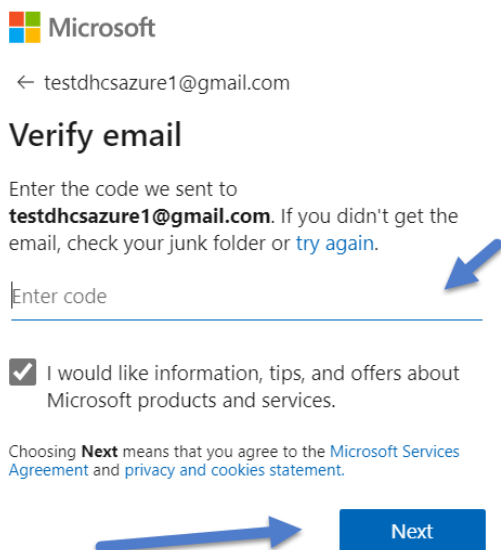


3. When prompted to Create account, enter Country/region and Birthdate, select Next

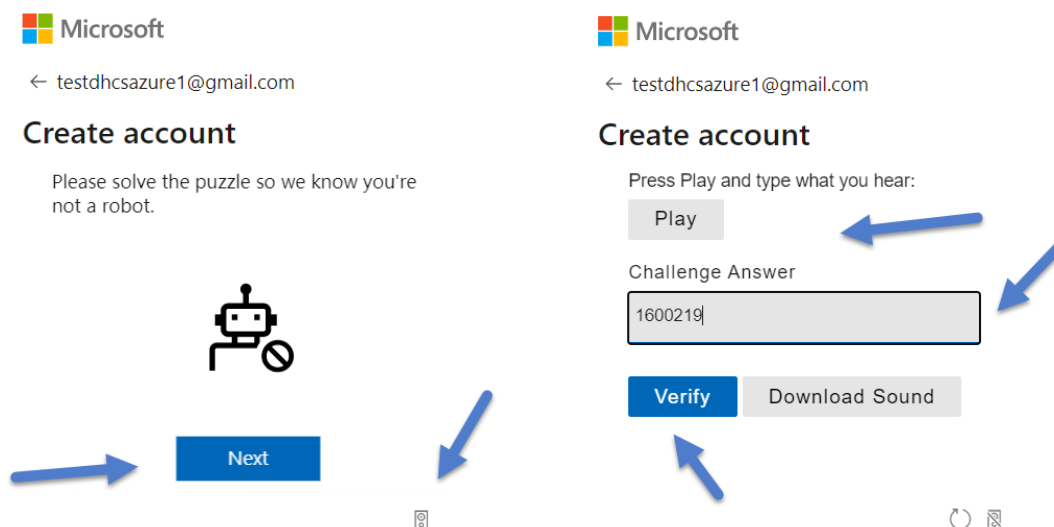


Application Portal User Manual

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

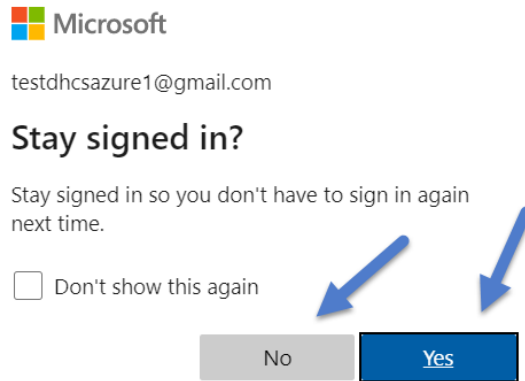


5. When prompted to Create account – Please solve the puzzle so we know you're not a robot. If robot checker not working - Select Audio Speaker, Play, enter the Challenge Answer, select Verify.

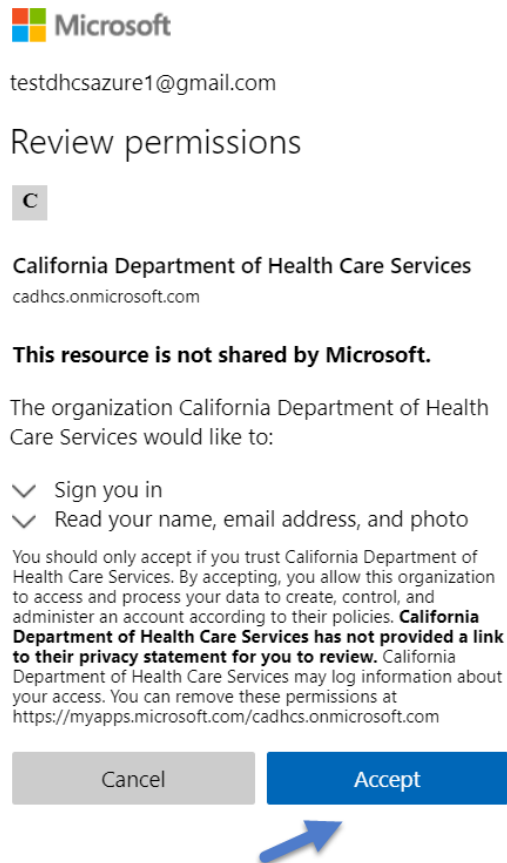


Application Portal User Manual

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

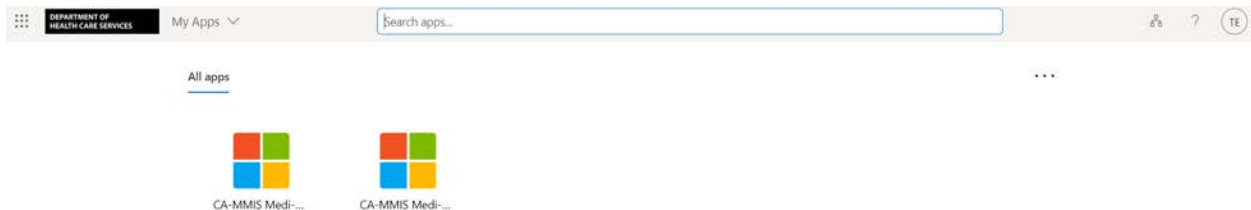


7. When prompted to Review permissions, select Accept

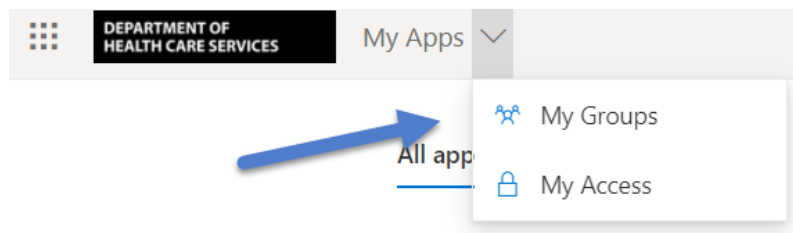


Application Portal User Manual

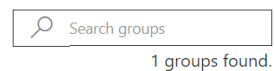
8. You are now successfully logged into the DHCS Application Gallery (My Apps page) and can access all the integrated DHCS applications you have access to.



- Select My Apps > My Groups




Groups



Groups I own
No groups found

Groups I'm in
+ Join group



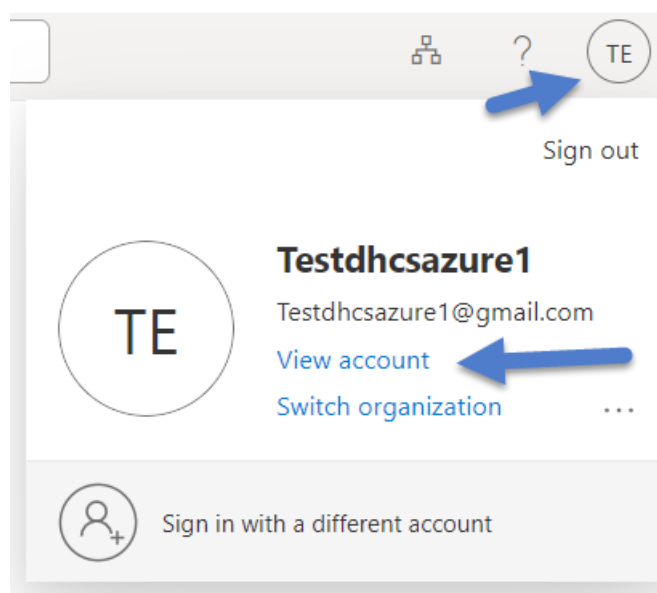
Multi-Factor Authentication (MFA) Setup

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.

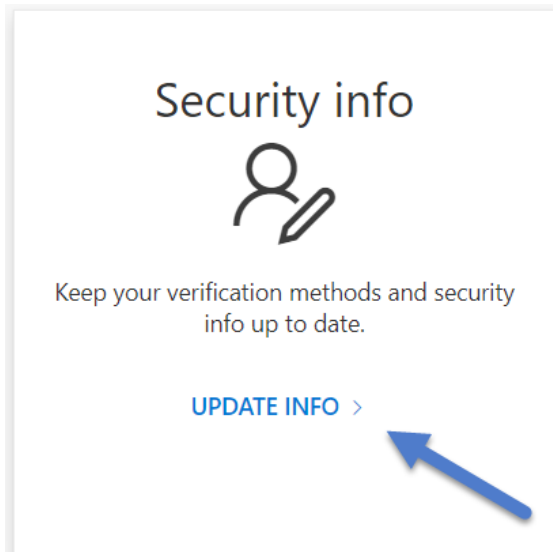
Steps

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

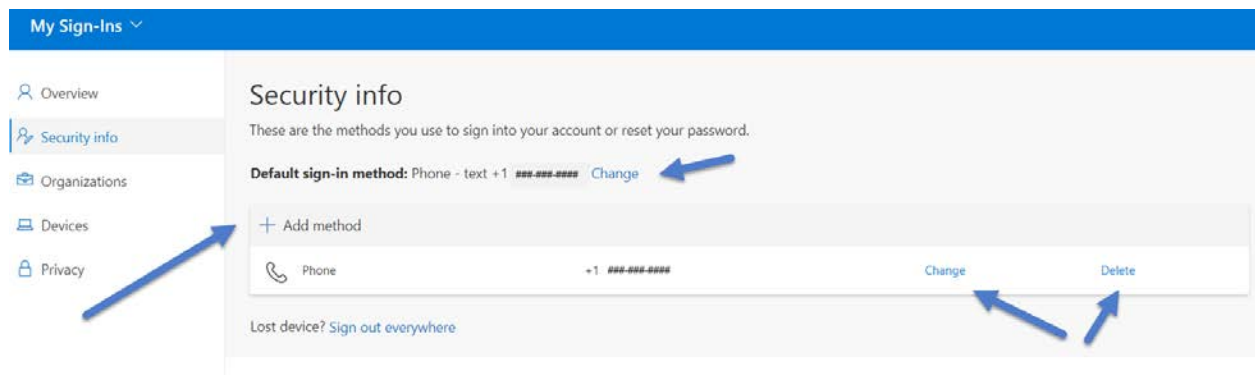


Application Portal User Manual

2. Select UPDATE INFO >



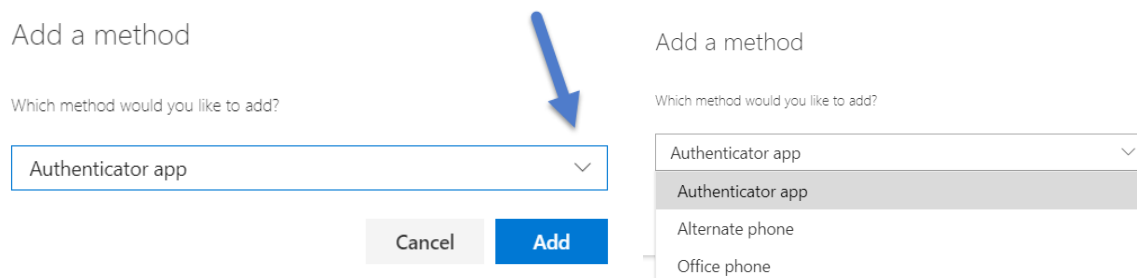
3. From the Security info page, add, change or delete a method. In this example, a Default sign-in method of Phone-text is set. Select + Add method



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.

Application Portal User Manual

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



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.