## Revision History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01</td>
<td>08/15/2018</td>
<td>First iteration of working rough draft</td>
</tr>
<tr>
<td>0.02</td>
<td>09/17/2018</td>
<td>Updates based on feedback received</td>
</tr>
<tr>
<td>0.03</td>
<td>02/14/2019</td>
<td>Updated to include all end user information needed and renamed to Getting Started</td>
</tr>
<tr>
<td>0.04</td>
<td>06/04/2019</td>
<td>Updated to include feedback</td>
</tr>
</tbody>
</table>
Contents

INTRODUCTION.................................................................................................................................................. 3
INVITATION EMAIL .............................................................................................................................................. 4
LOGGING IN .................................................................................................................................................. 5
ACCESS AN APPLICATION ...................................................................................................................................... 10
VIEW GROUP INFORMATION .......................................................................................................................... 10
MULTI FACTOR AUTHENTICATION (MFA) SETUP ......................................................................................... 18
MFA ADDITIONS OR CHANGES .......................................................................................................................... 20
ACCESS REVIEWS ........................................................................................................................................... 24
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.
LOGGING IN

Steps

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

2. When prompted, enter your work email address and click *Next*
OR when provided a list, choose your organization email address

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

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.
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
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

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.

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

Create account

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

Enter the characters you see

← dhcsaaduser2@gmail.com

New
Audio

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 (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

![DHCS Application Portal MFA setup screen](image-url)
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


<table>
<thead>
<tr>
<th>Contact method</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.  
                           - **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.  
                           - **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.  
                           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

<table>
<thead>
<tr>
<th>Apps</th>
<th><a href="mailto:dhcsaaduser1@gmail.com">dhcsaaduser1@gmail.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:dhcsaaduser1@gmail.com">dhcsaaduser1@gmail.com</a></td>
<td><a href="mailto:dhcsaaduser1@gmail.com">dhcsaaduser1@gmail.com</a>#EXT#@cadhcs.onmicrosoft.com</td>
</tr>
</tbody>
</table>

Sign out
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

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.
2. Click *Start Review* link in email

**OR** Access Reviews in DHCS Application Gallery

dhcsaaduser1@gmail.com
RNIA DEPARTMENT OF HEALTH CARE SERVICES

---

Search apps

- Groups
- Access reviews

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*
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.

**YOU HAVE SUCCESSFULLY COMPLETED THE MEMBER ACCESS REVIEW**
Update Access Review

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

2. Update response and Click *Submit Changes*
View Status of an Access Review

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.