



Application Portal Security Group Owner Manual



Application Portal Security Group Owner Manual

Table of Contents

Introduction.....	3
Purpose	3
Roles and Responsibilities.....	3
View Group Information	4
Add a member	5
Remove a Member	8
Access Reviews.....	9

Application Portal Security Group Owner Manual

Introduction

Purpose

This document describes the steps for users that are a Security Group Owner in Azure Active Directory (AAD) to Add and Remove Members from Security Groups.

Roles and Responsibilities

Currently, a Security Group Owner can perform the following operations:

1. Add Members
2. Remove Members

Do Not Perform the Following Operations:



Edit Details



Delete Group

Editing or Deleting a Group will result in revocation of Security Group Owner permissions.

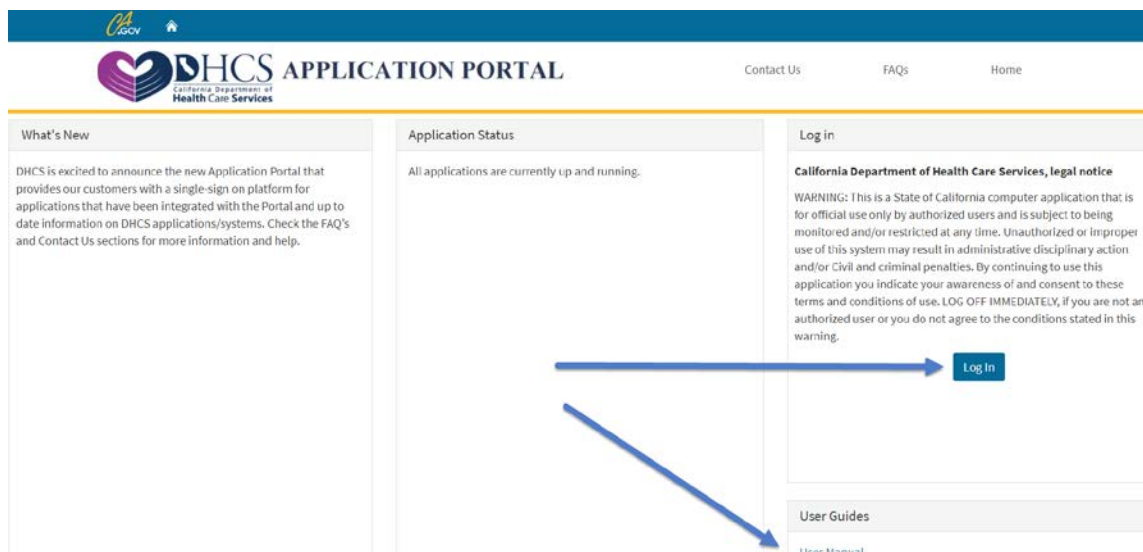
Security Group Owners are responsible for completing Access Reviews. Access Reviews are performed to ensure that users who are invited and/or added to a group and/or application continue to need access. The Security Group Owner must complete any and all Access Review Requests in a timely manner.

If Access Reviews are not completed in time, members will be removed from the Security Group and members will not be able to access the associated DHCS Applications.

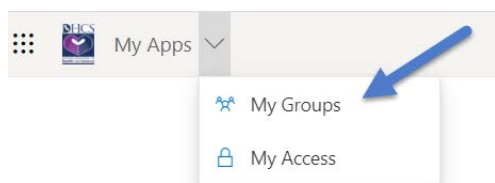
Application Portal Security Group Owner Manual

View Group Information

1. Go to the DHCS Application Portal at [DHCS Portal](#)
2. Select Log In. Detailed steps on how to Log in are found in the Application Portal User Manual document on the home page.

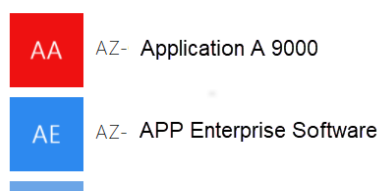


3. On My Apps page, select the caret and choose My Groups



4. Azure Groups page. If Groups are not listed under Groups I Own, you are not a Security Group Owner – and this document does not apply to you.

Groups I own

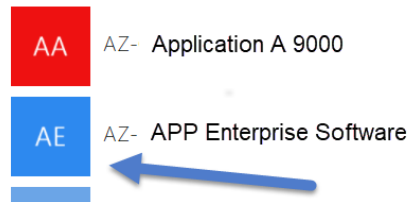


Application Portal Security Group Owner Manual

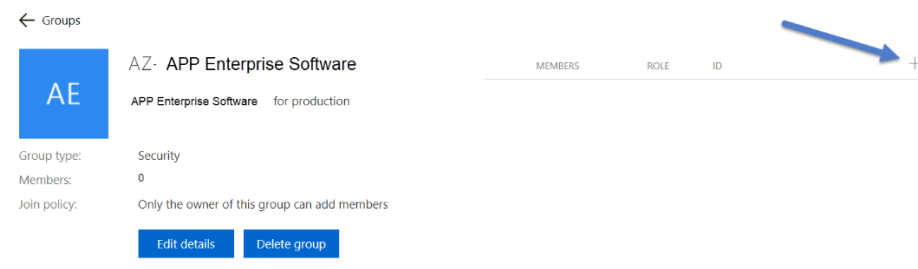
Add a member

1. Under Groups I own, select the Group to add a member(s) to, example Azure Enterprise SharePoint

Groups I own



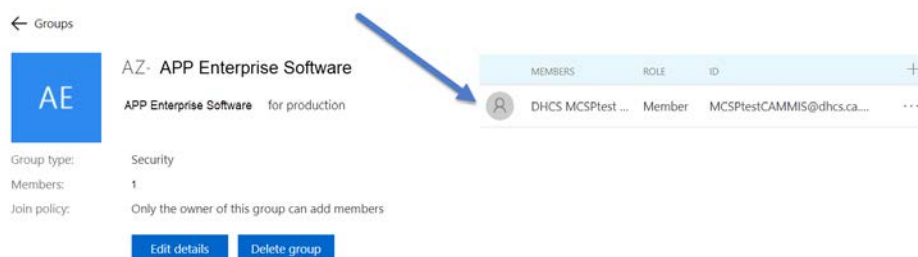
2. On the Security Group page, select the plus +



3. Search for the member, Select the member and choose Add, select OK




Result



Application Portal Security Group Owner Manual

4. If a member is external to DHCS, a dialog box is displayed. You can add a message in the box (Optional). An invitation email will be sent if the member is external to DHCS. If the member is internal to DHCS, an invitation is not sent.


Add members

 a.name@cdph.ca.gov External user ...

Access is now granted to Azure Enterprise Software

The new member added is now listed in the Group. The Role is Invited.

← Groups





AZ- APP Enterprise Software

APP Enterprise Software for production

Group type: Security


Members: 2

Join policy: Only the owner of this group can add members

MEMBERS	ROLE	ID	
 DHCS MCSptest ...	Member	MCSPTtestCMMIS@dhcs.ca...	...
 a.name@cdph.ca.gov	Invited	a.name@cdph.ca.gov	...

Once accepted, the external member becomes a Guest.

← Groups





AZ- APP Enterprise Software

APP Enterprise Software for production

Group type: Security

Members: 2

Join policy: Only the owner of this group can add members

MEMBERS	ROLE	ID	
 DHCS MCSptest ...	Member	MCSPTtestCMMIS@dhcs.ca...	...
 a.name@cdph.ca.gov	Guest	a.name@cdph.ca.gov	...

Application Portal Security Group Owner Manual

When a new external member is added to a Security Group, the member receives an invitation email with an “Accept Invitation” link that appears as follows. The member selects the “Accept Invitation” link to initiate the log in 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



Note: Security Group Owners can only add members if the member’s email domain has been approved by DHCS. If the member’s email domain is not approved, the following error message is displayed.

Add members

Not all members were successfully updated group membership, click OK to see details.

Include a personal message with the invitation for external users only.

OK

Select Ok and the following message will be at the top of the screen:

! User external.user@externaluser.com could not be invited right now. Your organization does not allow collaboration with the domain of the user you're inviting. Contact your admin to allow collaboration with this domain.

To add the email domain of the member to the pre-approved list, contact the application support staff, listed on the [DHCS Application Portal > Contact Us](#).

Application Portal Security Group Owner Manual

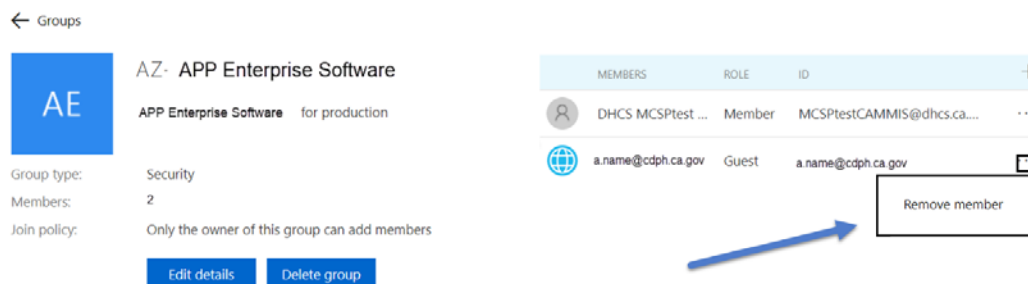
Remove a Member

1. On the Groups page, under the Groups I own column, select a Group

Groups I own



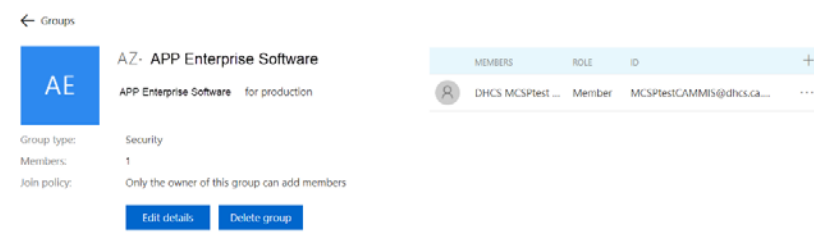
2. On the Group Security page, find the member to be removed
3. Select the three dots (ellipses) next to the member name and choose Remove Member



4. Select Yes



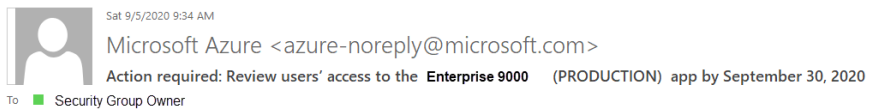
Security Group page will refresh and the member removed is no longer in the Group Members list.



Application Portal Security Group Owner Manual

Access Reviews

1. When an Access Review is initiated, Security Group Owners or Selected Users will receive an email from Microsoft Azure AD (example email modified for Enterprise 9000 test app). Access Review reminders will be sent close to the due date and must be completed on time.
2. Click “Start Review” link



Please review users' access to the Enterprise 9000 (PRODUCTION) app in California Department of Health Care Services

Security Group Owner, your organization requested that you approve or deny continued access for one or more users to the **Enterprise 9000 (PRODUCTION)** app in the **Quarterly-Production Application Access-All Members (Enterprise 9000)** review. The review period will end on **September 30, 2020**.

[Start review >](#)

Learn how to [perform an access review](#) and more about [Azure Active Directory access reviews](#).

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

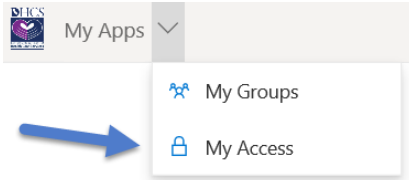
Facilitated by



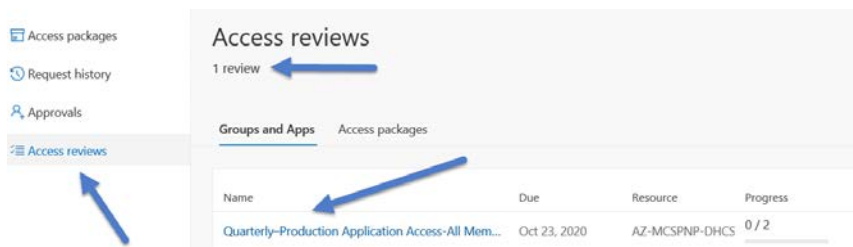
Application Portal Security Group Owner Manual

Access Reviews can be accessed from the MyApps page.

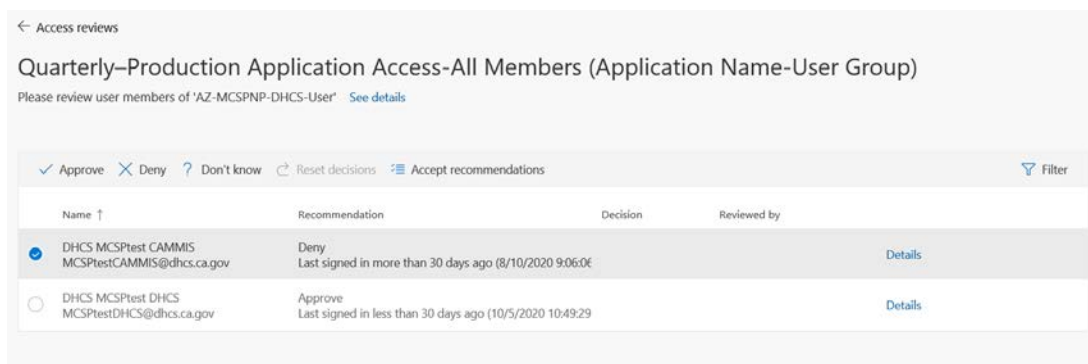
1. Select MyApps caret dropdown and select My Access:



2. Select Access Reviews and choose any active reviews



3. View members to be reviewed. Reviews can have 1 to many members to review. When a member is selected, choices include Approve, Deny, Don't know or Accept recommendations. Recommendations are not always an option, depending on the Application configuration.



- a. When Accept Recommendations is chosen, select the Submit button



Application Portal Security Group Owner Manual

b. When Approve is chosen, enter a Reason and select Submit

Approve continued access ×

You and other reviewers can make changes until the review ends.

1 approval

Reason *

Validated access with ITMO manager

Submit
Cancel

c. When Deny is chosen, enter a Reason and select Submit

Deny continued access ×

You and other reviewers can make changes until the review ends.

1 denial

Reason

No longer requires access; validated with BusOps vendor manager

Submit
Cancel

d. When Don't know is chosen, select Submit. Reason is optional.

Don't know ×

You and other reviewers can make changes until the review ends.

1 marked 'Don't know'

Reason

Submit
Cancel

4. After all Access Reviews are complete, exit.

Name	Due	Resource	Progress
Quarterly-Production Application Access-All Mem...	Oct 23, 2020	AZ-MCSPNP-DHCS	2 / 2