

Standard Operating Procedure (SOP)

#23-006

Infrastructure Services Division (ISD)

Table of Contents

MANAGING MICROSOFT ACTIVE DIRECTORY USER ACCOUNTS.....	1
1. Purpose and Scope	1
2. Prerequisites.....	1
3. Procedures	2
3.1 Creating Active Directory User Accounts.....	2
3.2 Provisioning Active Directory User Accounts.....	6
3.3 Configuring Active Directory User Accounts with Entra ID	10
3.4 Adding a User to a Distribution List	15
3.5 Adding a Shared Mailbox	17
3.6 Disabling Active Directory User Accounts	20
3.7 Removing Groups from the Disabled User ID in the Cloud	26
3.8 Granting a Manager Access to a Separated Employee's Contents.....	29
3.9 Managing Deleted Active Directory Objects	32
3.10 Exporting an Active Directory User Creation Report.....	33
4. References	34
4.1 DMHC Active Directory Security Groups	35
4.2 DMHC Distribution Lists	35
5. Revision Log	36

1. Purpose and Scope

This SOP explains how to manage user accounts in Microsoft Active Directory. More specifically, it describes how to create, provision, disable and configure an Active Directory user account, delete Active Directory objects and export an Active Directory user creation report.

2. Prerequisites

To implement this SOP, you need the following:

- A Microsoft Active Directory administrator account.
- Microsoft Remote Server Administration Tools (RSAT) running as an administrator.
You can download RSAT at <https://www.microsoft.com/en-us/download/details.aspx?id=45520>.

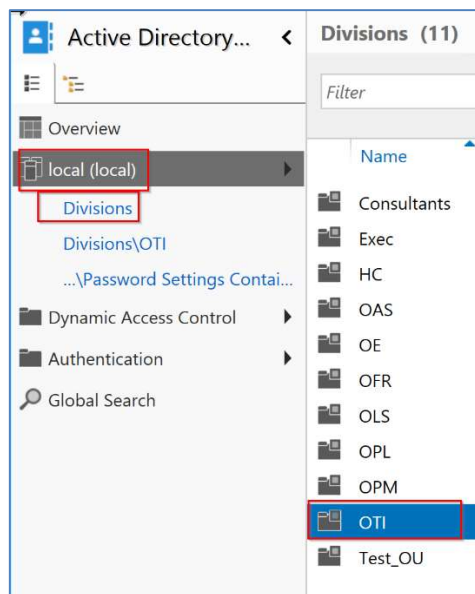
3. Procedures

Perform the procedures in the following sections to implement this SOP. Creating and provisioning a Microsoft Active Directory user account takes place in two phases. The first phase requires on-premises Active Directory to create and provision the user account and the second phase uses Microsoft Entra ID to configure the user account. Section 3.1 explains how to create a user account, Section 3.2 explains how to provision a user account and Section 3.3 explains how to configure a user account using Entra ID. Subsequent procedures in this section describe how to disable a user account, delete Active Directory objects and export an Active Directory user creation report.

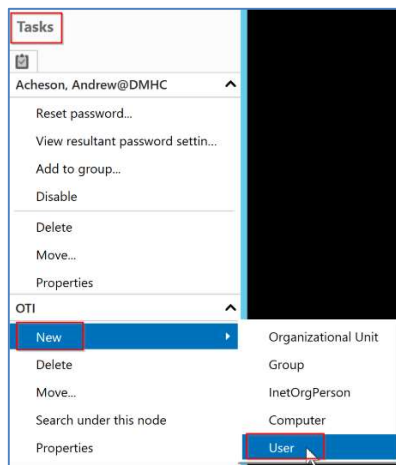
3.1 Creating Active Directory User Accounts

Use the following steps to create a user account with on-premises Active Directory:

1. Open **Active Directory Administrative Center**. Next, click **local (local)** in the left navigation pane, and then click **Divisions**. This example creates a mock user account in the OTI Organizational Unit (OU). In the Divisions column double-click the **OTI OU**.



2. In the screen that opens, click **New** under the Task section, and then click **User**.



3. The **Account** screen appears where you enter basic information about the user. To reduce errors when creating user accounts, copy the new user's name from the Service Request ticket. First, fill out the following fields in the Account screen:

- **First name, and Last name**—Enter the new user's first and last name in their respective fields.
- **Full name**—The format for the full name should be last name, followed by a comma, a space, and then the first name. Then append the @ character with DMHC. For example, Page, Niko@DMHC.
- **User UPN logon**—The format for the user UPN logon should be first name, a period, and then last name. From the drop-down box, select **dmhc.ca.gov**. For example, Niko.Page@dmhc.ca.gov.
- **User SamAccountName login**—Leave the first field set to local. For the username field, enter the user's first name initial, followed by their last name. For example, "local\NPage".

4. Scroll down to the **Organization** section and fill out the following fields:

- **Display name**—Use a pattern of last name, first name with "@DMHC" appended to the name. This convention is standard for domain user accounts and appears in programs like Outlook Web Access (OWA) under the sender or recipient fields.

- **Office**—The division within DMHC where the new user is assigned.
- **E-mail**— The first name is followed by a period and the last name. Capitalization and punctuation are important. Append to the last name the DMHC domain in all capital letters, such as Niko.Page@DMHC.CA.GOV.
- **Main**—The new user’s work phone number in the format +1 916-XXX-XXXX. This must be input correctly to configure multi-factor authentication.
- **Description**—Varies depending in which OU a user account is being created. Refer to another user account in the OU to be consistent. Be sure to note the office or cubicle number from the service request.

Organization

Display name:

Office:

E-mail:

Web page:

[Other web pages...](#)

Phone numbers:

Main:

Home:

Mobile:

Fax:

Pager:

IP Phone:

[Other phone numbers...](#)

Description:

5. Scroll down and enter the information found in the service request:

- **Job title**—Refer to another user account in the OU as an example. Check for spelling and DO NOT abbreviate job titles.
- **Department**—This field should read “DMHC”.
- **Company**—Refers to the unit’s name within the respective office. Utilize the office organizational chart found on the intranet or reach out to the administrative unit for each office. You can also refer to a staff member in the same unit as reference.
- **Address**— The following cities MUST be used, depending on the site where the user will be working. Use only the bolded portion as follows:
 - Sacramento: **DMHC-SO**
 - Rancho Cordova: **DMHC-FB**

- Los Angeles: **DMHC-LA**

Job title: Information Technology Associate

Department: DMHC

Company: Infrastructure Services Division

Manager: Edit... Clear

Direct reports: Add... Remove

Address: Street

DMHC-SO State/Province Zip/Postal code

Country/Region: ▼

- **Manager**—Click the **Edit** button to change the manager’s name for the user account.
- **Direct reports**—This section contains the subordinates that report to the new user account. To update the direct reports, click **Add** to display the Select User or Contact dialog box. Enter each subordinate’s name in the Enter the object name to select box in the format “*last name, first name*”. To input multiple subordinates, separate each name by a semicolon. For example, “Lopez, Daniel; Muslih, Bashar”. Click **Check Names** to resolve the user accounts, and then click **OK** to finalize your additions.

Select User or Contact

Select this object type: User Object Types...

From this location: local.dmhc.ca.gov Locations...

Enter the object name to select (examples): Check Names

Advanced... OK Cancel

6. Click **OK** to create the new user account.

Organization

Display name: Page, Niko@DMHC

Office: Office of Technology and Innovation

E-mail: Niko.Page@DMHC.CA.GOV

Web page:

Phone numbers:

Main:

Home:

Mobile:

Fax:

Pager:

IP Phone:

Description:

Job title: Information Technology Associate

Department: DMHC

Company: Infrastructure Services Division

Manager:

Direct reports:

Address:

Street:

DMHC-SQ State/Province Zip/Postal code

Country/Region:

Member Of

OK Cancel

3.2 Provisioning Active Directory User Accounts

This section describes how to provision a Microsoft user account.

1. After creating a new user in the preceding section, return to the OU where the user was created, and double-click the user account to resume provisioning it.

Filter

Name	Type	Description
1, CND_	User	DISABLED 6/1/23 INC4505...
2, CND_	User	DISABLED 6/1/23 INC4505...
3, CND_	User	DISABLED 6/1/23 INC4505...
Cena, John@DMHC	User	
Page, Niko@DMHC	User	
RedTeam, CND_PT	User	DISABLED 6/1/23 INC4505...
Test, Mr	User	

Page, Niko@DMHC

2. With the account's window open scroll down to the **Member Of** section, which consists of the security groups to which a user account has permissions.

Member Of

Filter

Name

Active Director... Primary

Add...

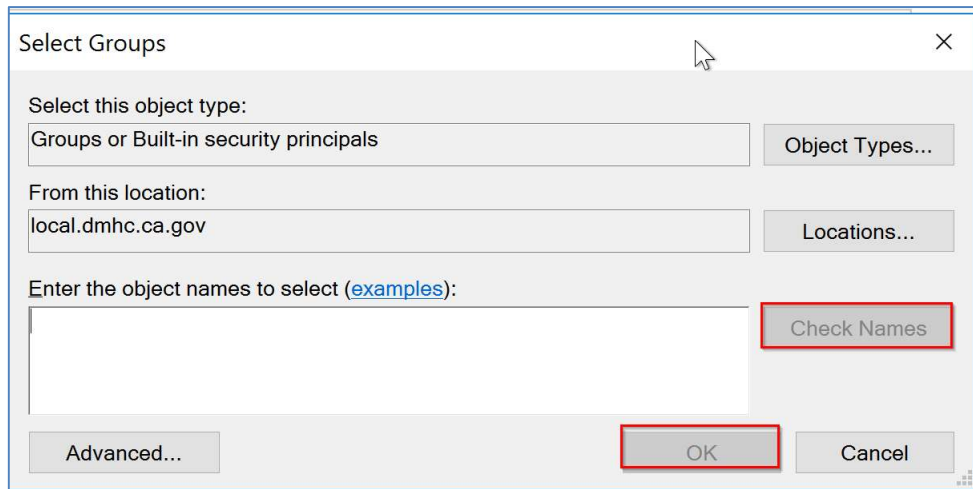
Remove

This object will be added to the default Active Directory group.

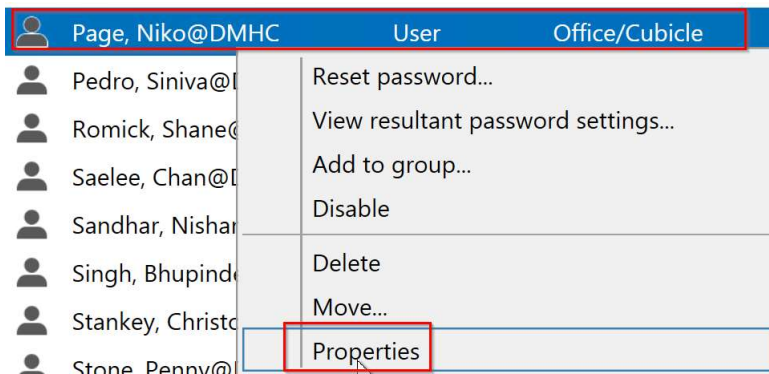
3. Use the filter box to search for the security groups you want to assign to the user account. Select a group from the list, and then click the **Add** button. For descriptions

of the available security groups, refer to DMHC Active Directory Security Groups in the References section.

4. After you click the Add button, the Select Groups dialog box opens. Enter the object names you want to select and click **Check Names**. Click **OK** when you are finished.



5. Refer to the OTI OU and locate Niko Page. **Right-click** the name and select **Properties** from the context menu.



6. Review the user account information and select **Extension** to complete some final details for the Active Directory portion of the provisioning procedure. This step focuses on the **Security**, **Dial-in** and **Attribute Editor** tabs.

Page, Niko@DMHC

Account

Organization

Password Settings

Profile

Policy

Silo

Extensions

Account

First name:

Middle initial:

Last name:

Full name:

User UPN log:

User SamAcc:

☐ Protect fr

- a. **Security**—Click **Authenticated Users** under the **Groups and user names** section. This attribute allows users to authenticate into the network via Cisco ISE. This is vital for user accounts to request access to the domain. Select **Allow** under the checkbox **Allow** under the **Read** permission.

General Address Account Profile Telephones Organization

Security Environment Sessions Remote control

Group or user names:

- Everyone
- SELF
- Authenticated Users**
- SYSTEM
- RTCUniversalUserReadOnlyGroup (DMHC\RTCUniversalUserRe...
- RTCUniversalUserAdmins (DMHC\RTCUniversalUserAdmins)
- OTI_WorkstationAdmins (DMHC\OTI_WorkstationAdmins)

Add... Remove

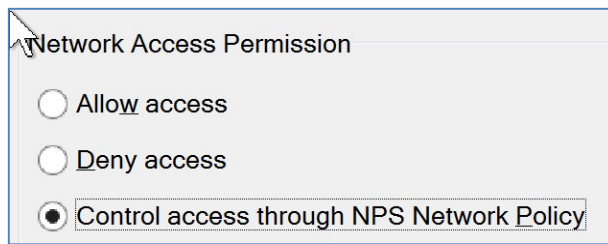
Permissions for Authenticated Users

	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>

Under **Permissions for Authenticated Users** click the **Allow** checkbox for the **Read** permission.

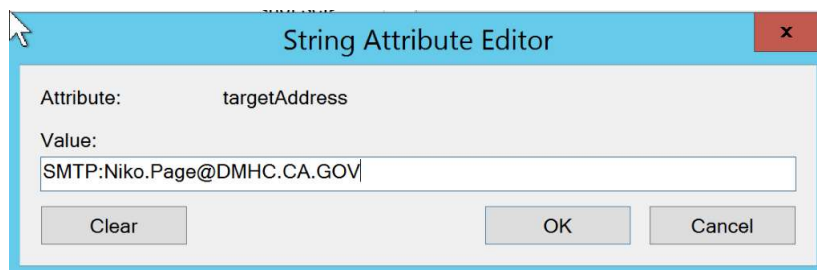
Permissions for Authenticated Users

	Allow
Full control	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>



b. **Attribute Editor**—This setting configures email-related attributes for Entra ID provisioning. Configure these attributes as follows:

- **mailNickname**—Press ‘m’ to locate this attribute. Click **Edit** and then enter the user’s first name, a period and the user’s last name. For example, “Niki.Page”. Click **OK** when completed. This setting appears in Outlook or OWA.
- **targetAddress**—Press ‘t’ to locate this attribute. Click **Edit**, and then enter **SMTP:firstname.lastname@DMHC.CA.GOV** in the **Value** field. For example, SMTP:Niko.Page@DMHC.CA.GOV. Click **OK** when completed. This is the address to where email is routed.



- **proxyAddress**—Press ‘r’ and the up arrow several times to locate this attribute. Click **Edit**. Under **Value to add** enter the following email addresses and click **Add** for each alias. Click **OK** when completed.
 - **Primary address:** SMTP:firstname.lastname@DOMAIN. The domain must be uppercase. For example SMTP:Niko.Page@DMHC.CA.GOV.
 - **SMTP address:** SMTP:firstInitial_lastName@dmhc.ca.gov. The domain must be lowercase. For example. SMTP:NPage@dmhc.ca.gov.

Note: **SMTP address** *must* match the samAccountName shown in Section 3.1, Step 3, appended with the domain dmhc.ca.gov. Failure to do so would impact such apps as **Spotlight**, (etc still need to find out).

Multi-valued String Editor

Attribute: proxyAddresses

Value to add:

Add

Values:

SMTP:Niko.Page@DMHC.CA.GOV
smtp:NPage@dmhc.ca.gov

Remove

OK Cancel

- **extensionAttribute15**—This attribute is used for our WASP ticketing system (Cherwell). Setting the value to **TRUE** flags the user account as a VIP. User accounts that management considers VIP are Director, Deputy Director and Assistant to Director.

String Attribute Editor

Attribute: extensionAttribute15

Value: TRUE

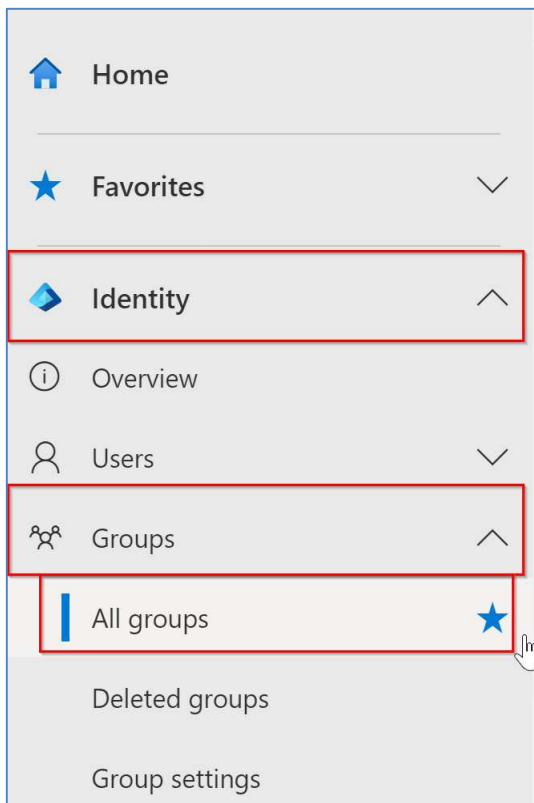
Clear OK Cancel

- c. Press **OK** to finalize the changes to the user account. Note that changes to user accounts first update from on-premises Active Directory, and then synchronize to Entra ID on a half hour basis.

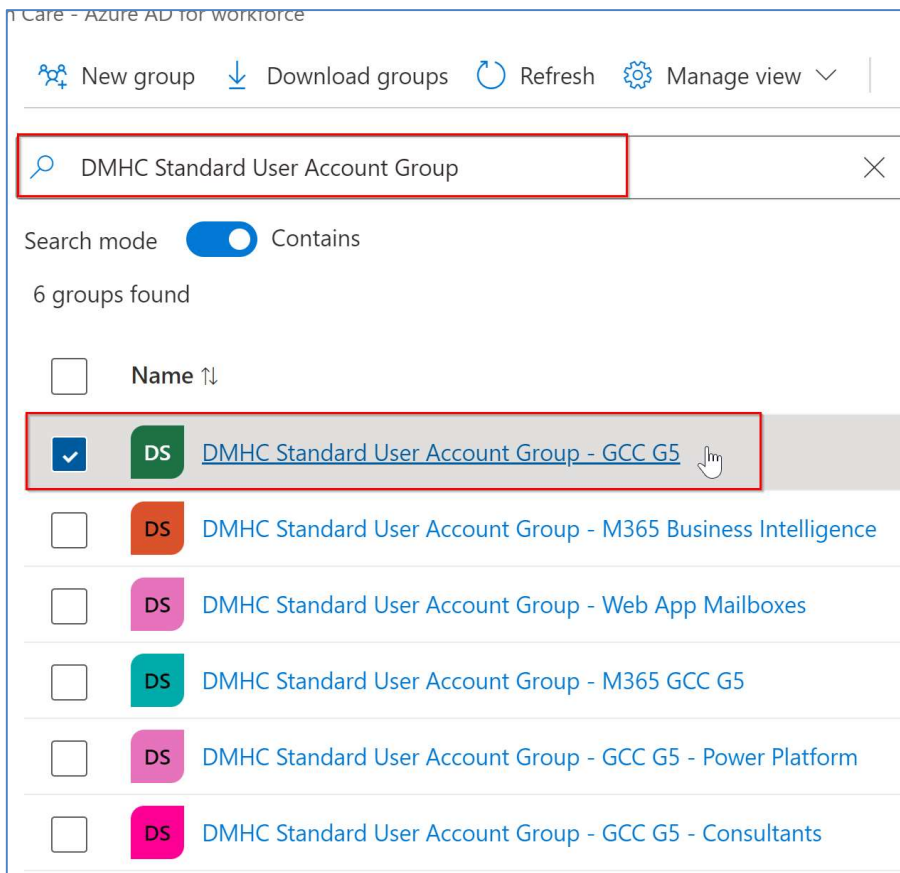
3.3 Configuring Active Directory User Accounts with Entra ID

This section explains how to configure Active Directory user accounts with Entra ID.

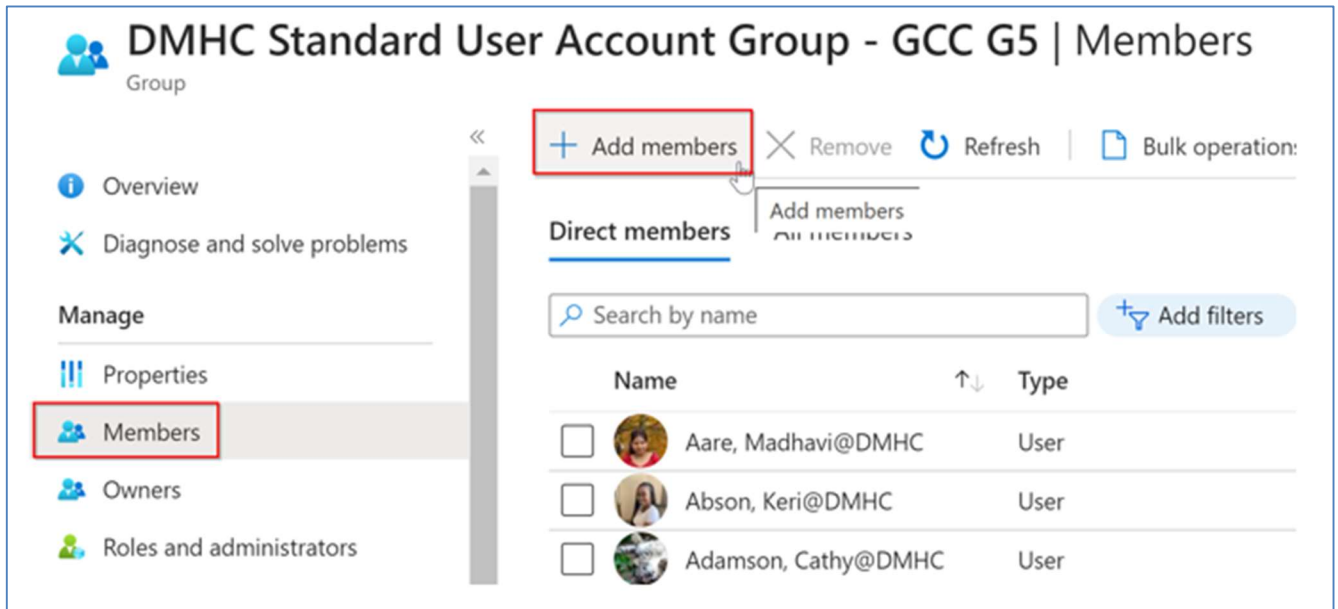
1. Use a cloud admin account to log into Microsoft's Entra Admin Center at <https://entra.microsoft.com/#home>.
2. Click **Identity, Groups** and then **All Groups**.



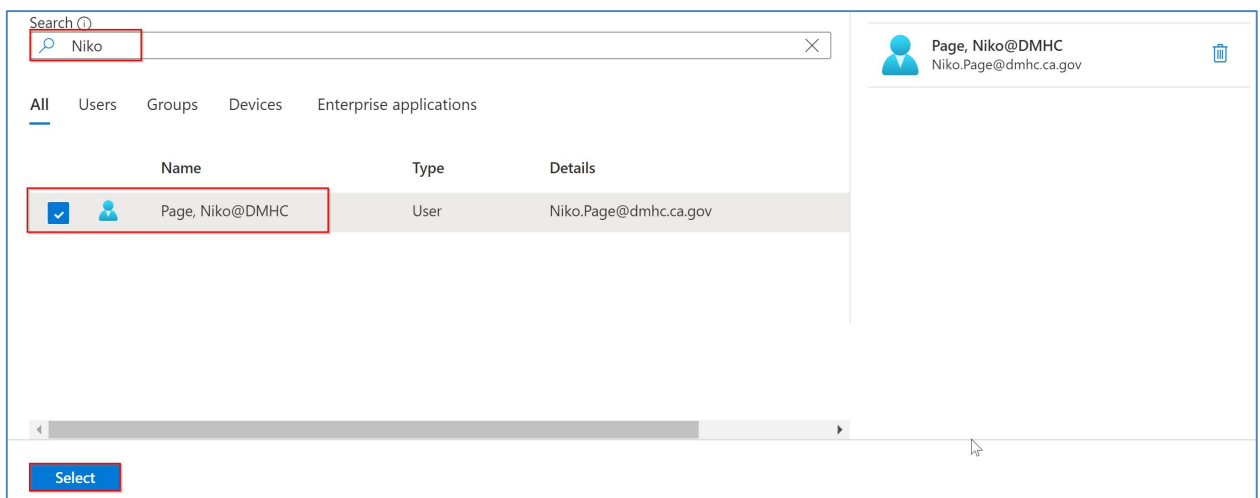
3. In the search box that opens enter **DMHC Standard User Account Group**. The returned results are similarly named security groups that are used to provision a set of Microsoft licenses for a user account. Click **DMHC Standard User Account Group – GCC G5**, which is the most used group.



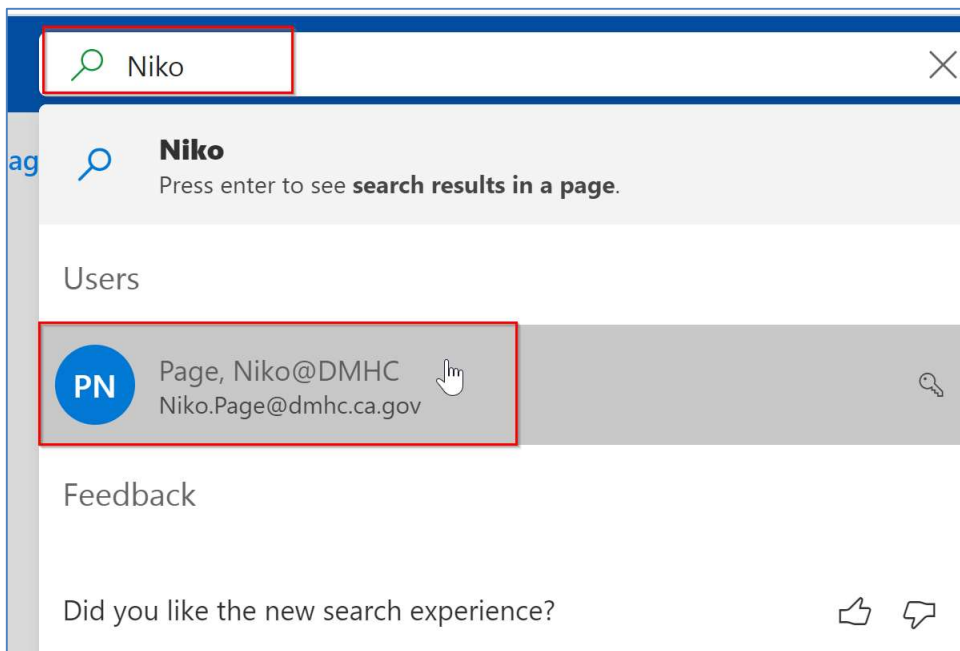
4. In the screen that opens, click **Members**, and then click **Add members**.



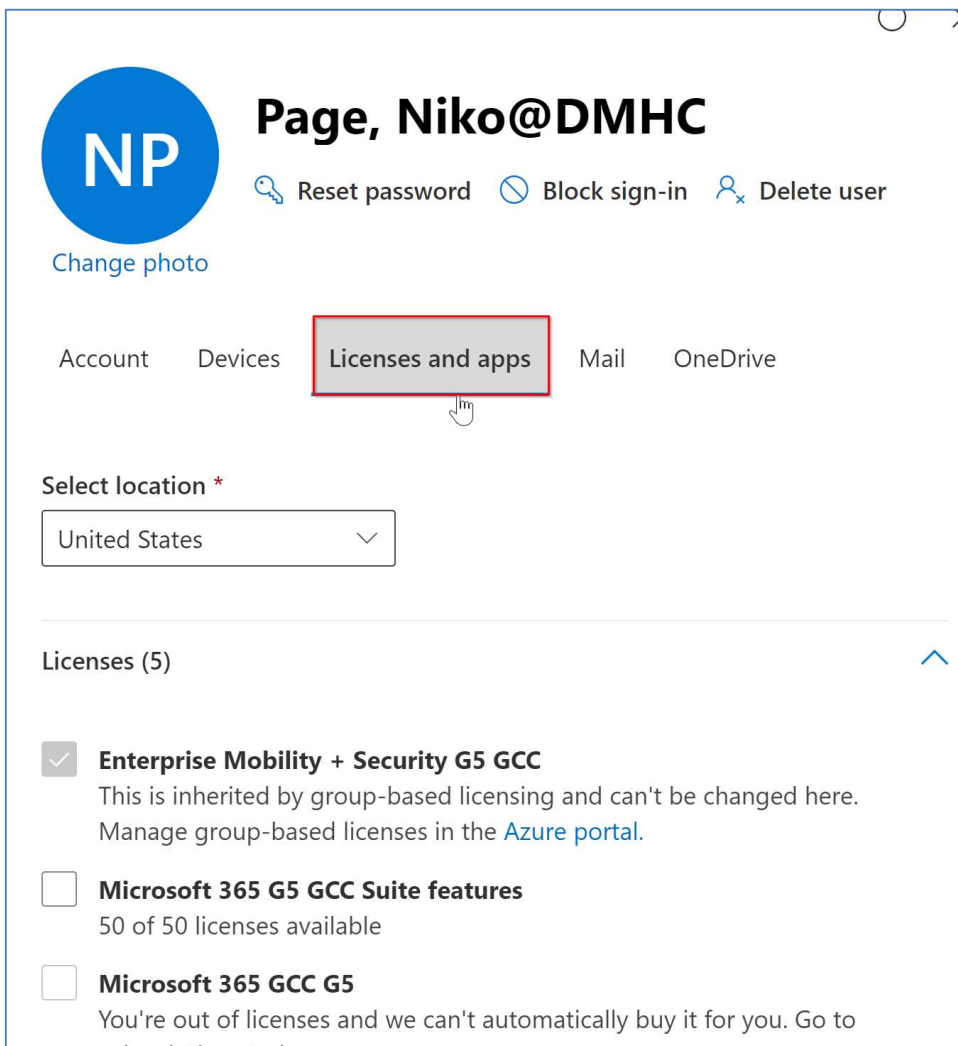
5. A side pane opens where you can add members. In the search box enter the name of the user, then select the checkbox associated with the user account. Finally, click **Select**.



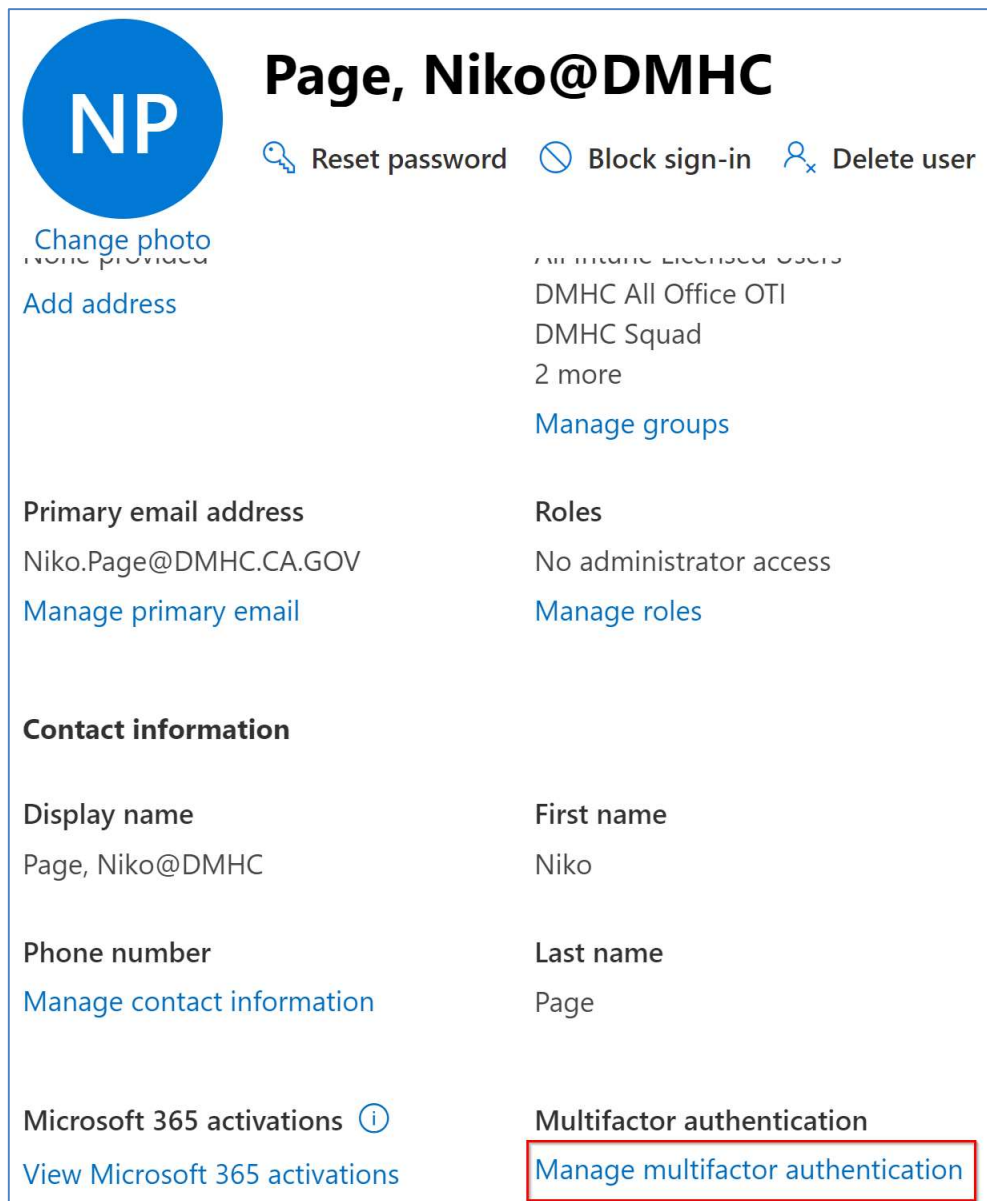
6. Open the Microsoft 365 Admin Center at <https://admin.microsoft.com/Adminportal/Home#/homepage> to review the account and verify the licenses that have been provisioned. Enter the user account name in the search box and click it in the returned search list.



7. Next click on the **License and apps** tab and confirm the licenses under the Licenses section. After confirming the provisioned licenses, click on the **Account** tab.



8. Scroll to the bottom of the **Account** screen and click **Manage multifactor authentication** to enable it for the user account.



The image shows a user account management page for 'Page, Niko@DMHC'. At the top left is a blue circular profile picture with the letters 'NP'. To the right of the profile picture is the user's name 'Page, Niko@DMHC'. Below the name are three links: 'Reset password', 'Block sign-in', and 'Delete user'. Below the profile picture are links for 'Change photo' and 'Add address'. To the right of these links is a section for 'Assigned licenses' which lists 'DMHC All Office OTI', 'DMHC Squad', and '2 more', with a link to 'Manage groups'. Below the 'Change photo' link is the 'Primary email address' section, which shows 'Niko.Page@DMHC.CA.GOV' and a link to 'Manage primary email'. To the right of this is the 'Roles' section, which shows 'No administrator access' and a link to 'Manage roles'. Below the 'Primary email address' section is the 'Contact information' section. It has two columns: 'Display name' (Page, Niko@DMHC) and 'First name' (Niko). Below 'Display name' is 'Phone number' and a link to 'Manage contact information'. Below 'First name' is 'Last name' (Page). At the bottom left is 'Microsoft 365 activations' with an information icon and a link to 'View Microsoft 365 activations'. At the bottom right is 'Multifactor authentication' with a link to 'Manage multifactor authentication' which is highlighted with a red box.

Page, Niko@DMHC

[Reset password](#) [Block sign-in](#) [Delete user](#)

[Change photo](#)
None provided

[Add address](#)

Assigned licenses
DMHC All Office OTI
DMHC Squad
2 more
[Manage groups](#)

Primary email address
Niko.Page@DMHC.CA.GOV
[Manage primary email](#)

Roles
No administrator access
[Manage roles](#)

Contact information

Display name
Page, Niko@DMHC

First name
Niko

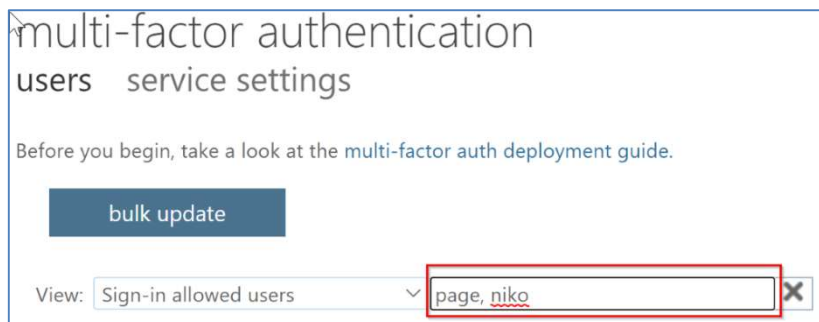
Phone number
[Manage contact information](#)

Last name
Page

Microsoft 365 activations ⓘ
[View Microsoft 365 activations](#)

Multifactor authentication
[Manage multifactor authentication](#)

7. On the **Multifactor authentication** page, enter the user account name in the search box and press **Enter**.



The image shows the 'Multi-factor authentication' page. At the top is a search bar with the text 'multi-factor authentication' and 'users service settings'. Below the search bar is a link to 'Before you begin, take a look at the multi-factor auth deployment guide.' Below this is a 'bulk update' button. At the bottom is a 'View:' dropdown menu set to 'Sign-in allowed users'. To the right of the dropdown is a search box containing the text 'page, niko' which is highlighted with a red box. To the right of the search box is a close button (X).

multi-factor authentication
users service settings

Before you begin, take a look at the multi-factor auth deployment guide.

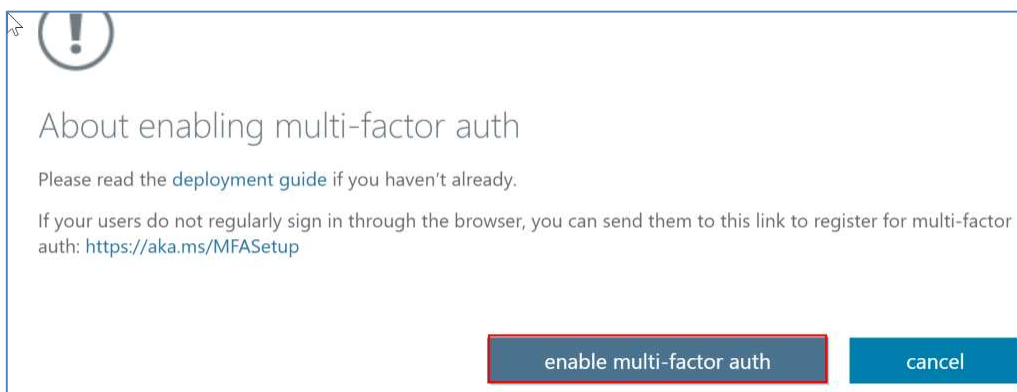
[bulk update](#)

View: Sign-in allowed users

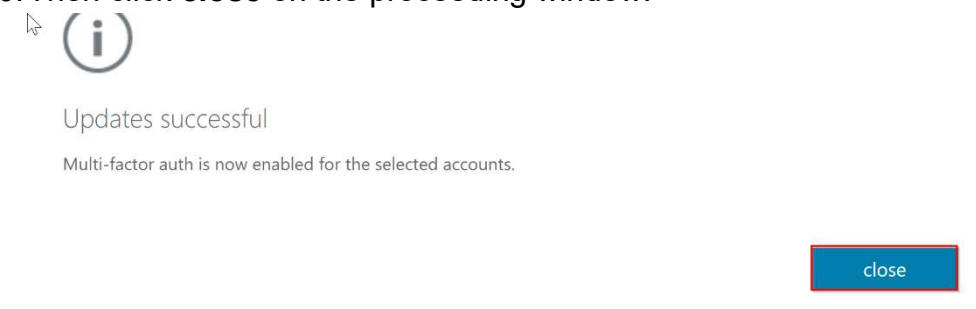
8. After locating the user account, select it and click **Enable**.



9. Click **enable multi-factor auth**.



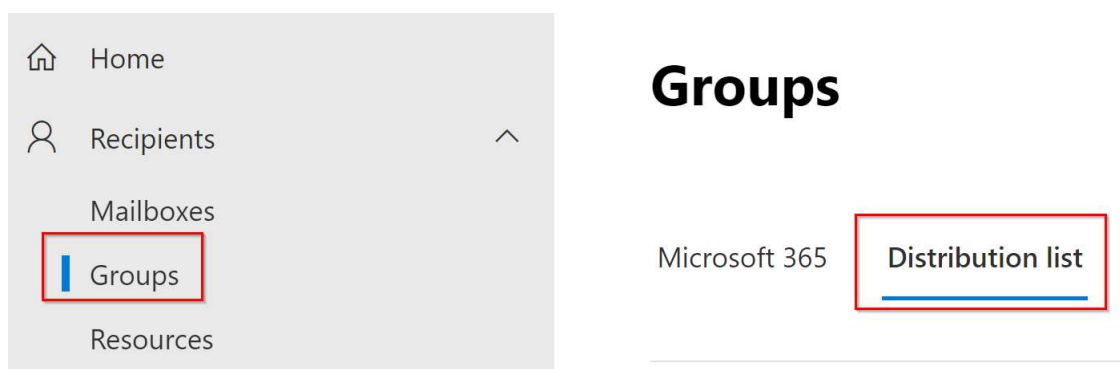
10. Then click **close** on the proceeding window.



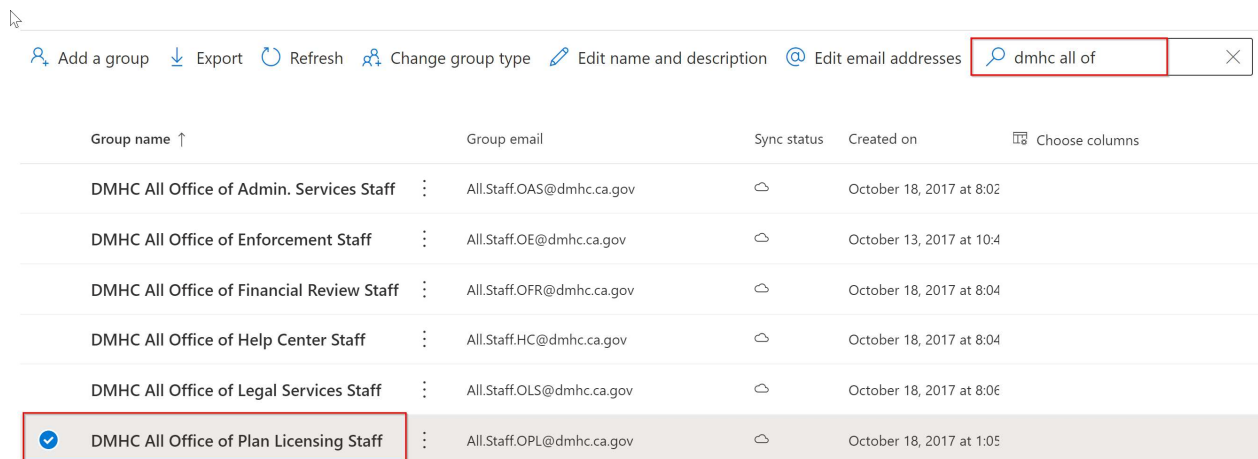
3.4 Adding a User to a Distribution List

1. Navigate to Exchange admin center <https://admin.exchange.microsoft.com/> click **Groups** and then click **Distribution list**.

There will be office specific distributions lists that a user account will need to be added to. For a more in-depth explanation of the office distributions lists please refer to the Reference section 4.2. The following steps will provide instructions on how to add a user to a distribution list.

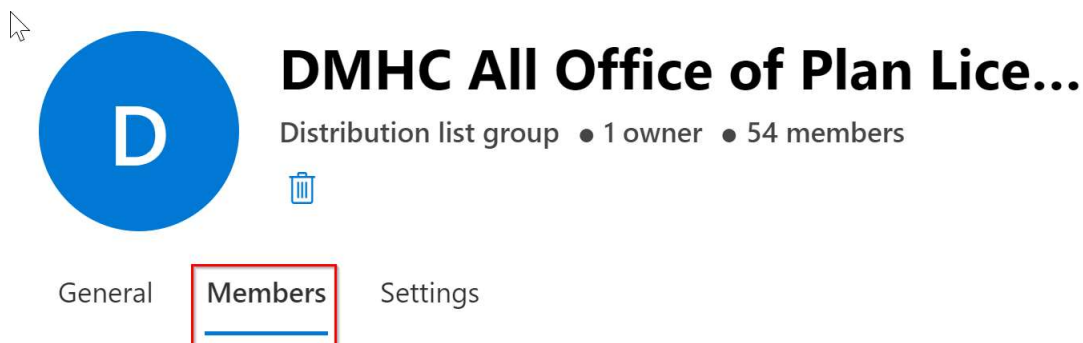


- Typically, a user account would be added to the office they're hired in, however OTI's distribution list's functions differently than the others. Therefore, as an example, we'll add the user account to the distribution list **DMHC All Office of Plan License**. First search for the distribution list in question. Then select the distribution list.



Add a group Export Refresh Change group type Edit name and description Edit email addresses dmhc all of			
Group name ↑	Group email	Sync status	Created on
DMHC All Office of Admin. Services Staff	All.Staff.OAS@dmhc.ca.gov	☁	October 18, 2017 at 8:02
DMHC All Office of Enforcement Staff	All.Staff.OE@dmhc.ca.gov	☁	October 13, 2017 at 10:4
DMHC All Office of Financial Review Staff	All.Staff.OFR@dmhc.ca.gov	☁	October 18, 2017 at 8:04
DMHC All Office of Help Center Staff	All.Staff.HC@dmhc.ca.gov	☁	October 18, 2017 at 8:04
DMHC All Office of Legal Services Staff	All.Staff.OLS@dmhc.ca.gov	☁	October 18, 2017 at 8:06
DMHC All Office of Plan Licensing Staff	All.Staff.OPL@dmhc.ca.gov	☁	October 18, 2017 at 1:05

- With the side pane open for **DMHC All Office of Plan Licensing** click the **Members** section

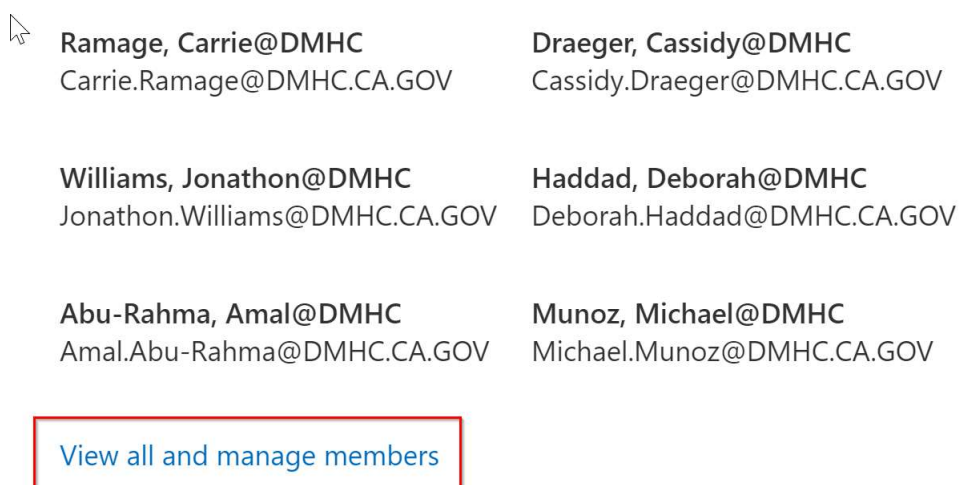


DMHC All Office of Plan Lice...

Distribution list group • 1 owner • 54 members

General **Members** Settings

- Next scroll down to **View all and manage members** and click it.



Ramage, Carrie@DMHC
Carrie.Ramage@DMHC.CA.GOV

Draeger, Cassidy@DMHC
Cassidy.Draeger@DMHC.CA.GOV

Williams, Jonathon@DMHC
Jonathon.Williams@DMHC.CA.GOV

Haddad, Deborah@DMHC
Deborah.Haddad@DMHC.CA.GOV

Abu-Rahma, Amal@DMHC
Amal.Abu-Rahma@DMHC.CA.GOV

Munoz, Michael@DMHC
Michael.Munoz@DMHC.CA.GOV

[View all and manage members](#)

- Next click **Add members**.

+ Add members

Search members list

6. In the search box type the user's name. Allow the interface time to return results. Next click the checkbox next to the user's name and click **Add**.

←

×

Add members

page, niko

×

☒ Display name

☒

PN

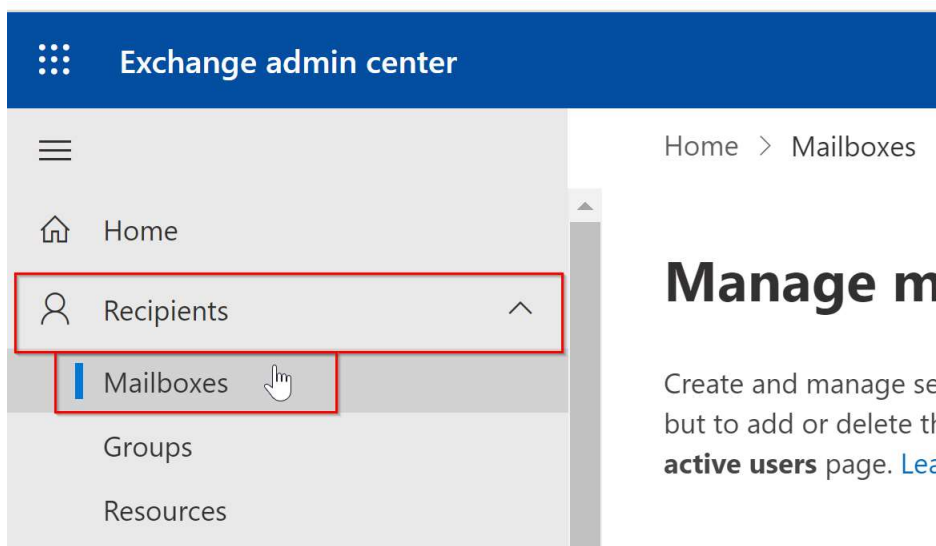
Page, Niko@DMHC
Niko.Page@DMHC.CA.GOV

Add (1)

Cancel

3.5 Adding a Shared Mailbox

1. Navigate to the link <https://admin.exchange.microsoft.com/#/mailboxes> to open the Exchange admin center. Click **Recipients** and then **Mailboxes**.



2. In the search box, enter the name of a given mailbox specified in. In this example we're looking for **DMHC OTI Receiving**, therefore we enter "oti". In the search results click **DMHC OTI Receiving**



11. With the side pane for **DMHC OTI Receiving** opened, click **Delegation**. The user account will be given both **Send as** and **Full Access** permissions. The provisioning procedure is similar for either case. Click **Edit** for one of the permissions.



DMHC OTI Receiving

Shared mailbox

Hide mailbox Email forwarding Send on behalf

General

Organization

Delegation

Mailbox

Others

Send as (11)

The Send as permission allows the delegate to send an email from this mailbox. Message will appear to have been sent from this mailbox owner.

Edit

Read and manage (Full Access) (12)

The Full Access permission allows a delegate to open this mailbox and behave as the mailbox owner.

Edit

12. Click **Add members**.

Manage mailbox delegation

The Full Access permission allows a delegate to the mailbox owner.

Add members Delete(0) 12 items

13. Enter the name of the user account, select the account, and then click **Save**.

Add read and manage permissions

The Full Access permission allows a delegate to open this mailbox and behave as a mailbox owner.

Added(1)

☒ Display Name

<input checked="" type="checkbox"/>	<div><div>PN</div><div>Page, Niko@DMHC Niko.Page@DMHC.CA.GOV</div></div>	
-------------------------------------	------------------------------------------------------------------------------	--



14. On the **Add delegate permission** page click **Confirm** to add the permission being added to the user account.

←

×

Add delegate permissions?

Are you sure you want to add delegate permission for these mailboxes?

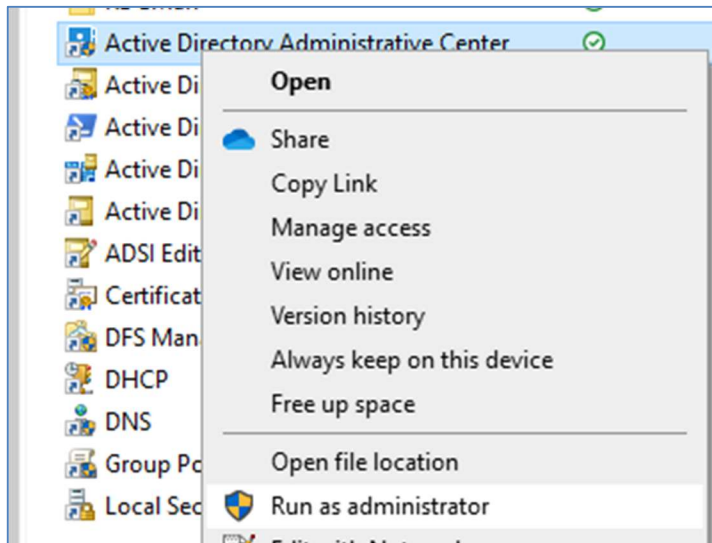
Confirm

3.6 Disabling Active Directory User Accounts

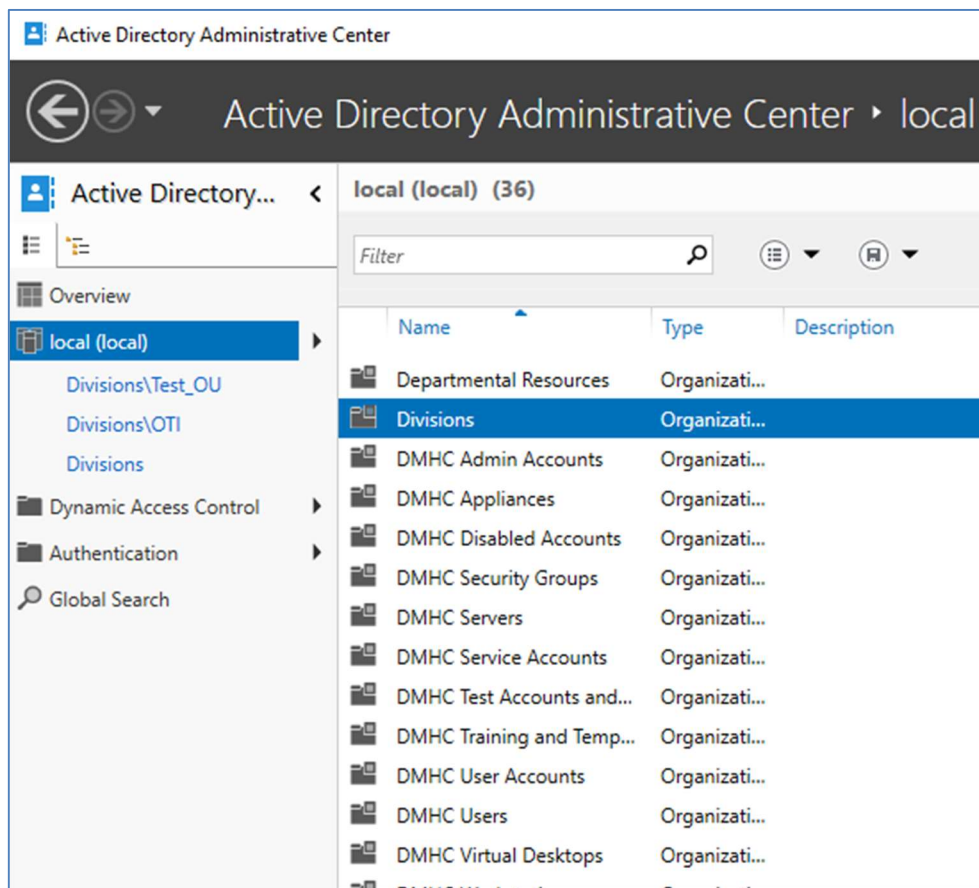
Except for OTI staff members, and some consultants, the following steps should encompass the process for separating user accounts for your typical user. For OTI staff or consultants, create a task associated with the separating ticket for administrator accounts and Entra ID admin accounts with a prefix of gla, csa and spa. Assign the task to ISD's System Admins queue in Cherwell.

Note that this SOP does not discuss deleting user accounts due to requirements from Legal that user accounts, I: drives and mailboxes be retained.

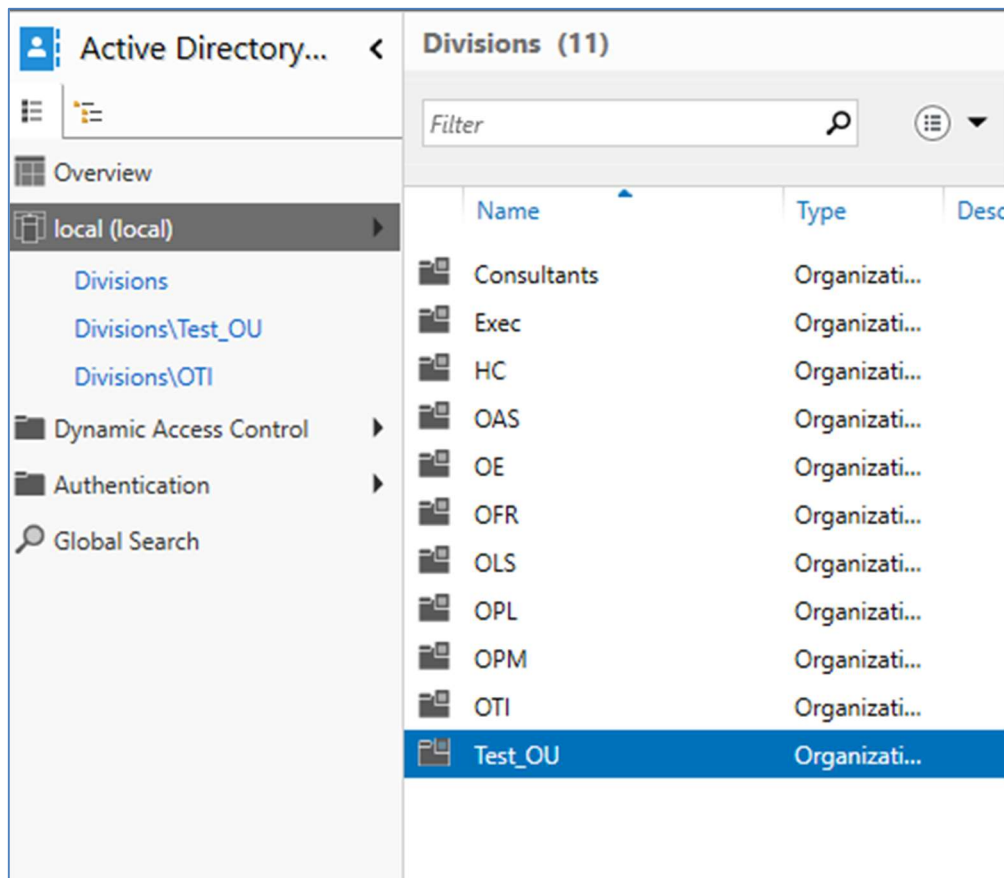
1. Running as an administrator, open **Microsoft Remote Server Administration Tools (RSAT)** and right-click **Active Directory Administrative Center**. Then, click **Run as administrator** from the context menu.



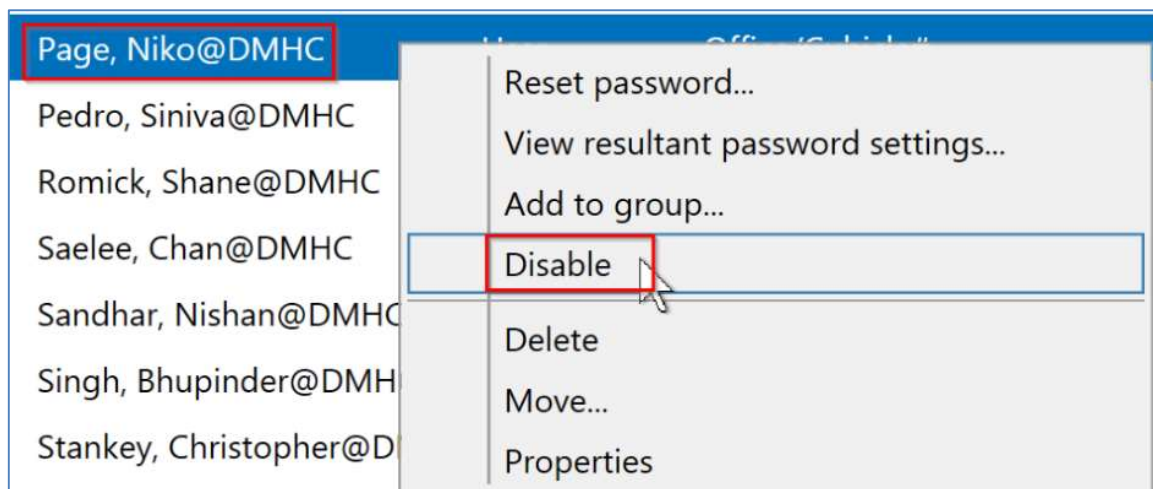
2. Click **local (local)** in the left navigation pane and then click the **Divisions Organization Unit**.



3. Click the department organizational unit containing the user you want to disable.

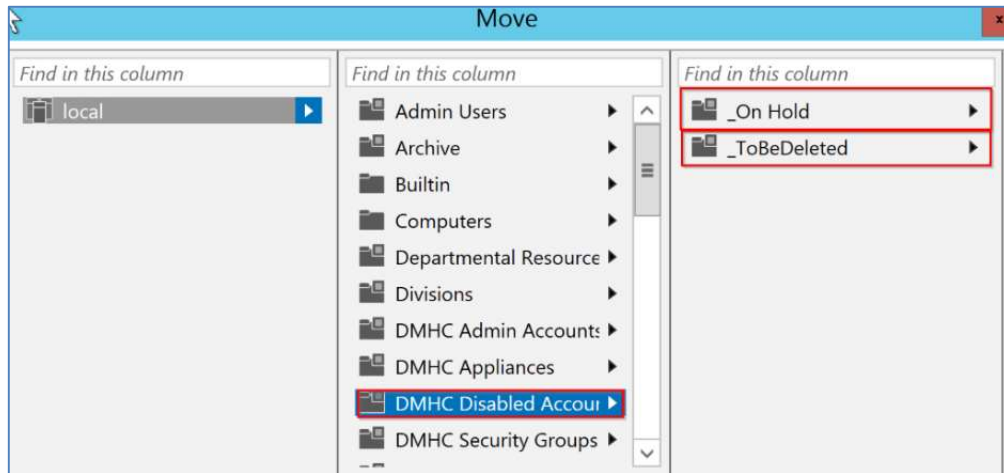


4. Locate the user account you want to disable, right-click it and then click **Disable** from the context menu. Be sure to note the date and time that you disabled the user account.



5. Right-click the user account again and click **Move**. Select the **DMHC Disabled Account** container, and then select one of the following containers where you want to move the disabled account and click **OK**:
 - **_On Hold**—Contains user accounts that potentially have institutional knowledge about DMHC based on position or tenure with the department.

- **_ToBeDeleted**—Stores user account that are to be deleted. However, due to legal requirements, user accounts moved to this container are not likely to be deleted. Nonetheless, move user accounts here that you want to disable.

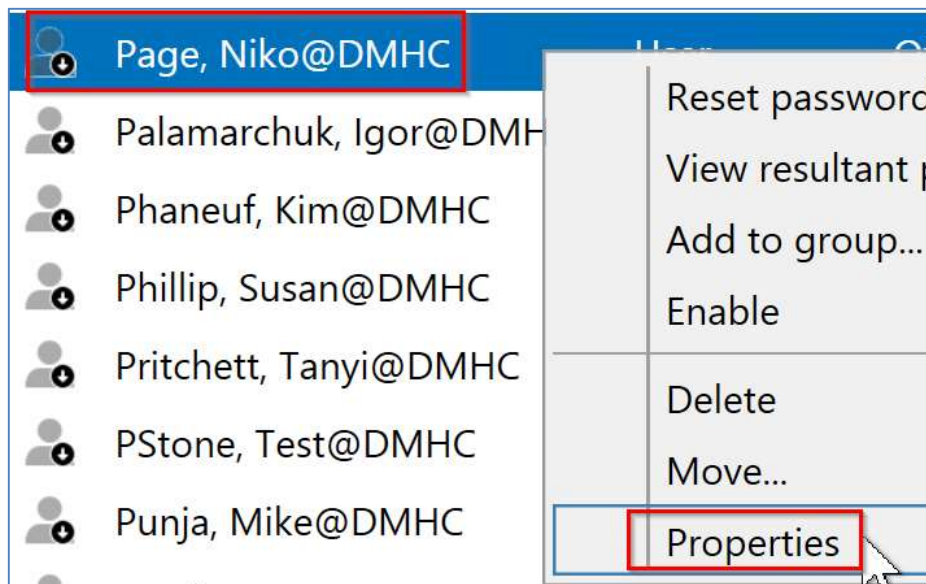


6. Click **local (local)** to return to the root of the domain.
7. Double-click the **DMHC Disabled Accounts** container. Select the container where you moved the user account (**_On Hold** or **_ToBeDeleted**).



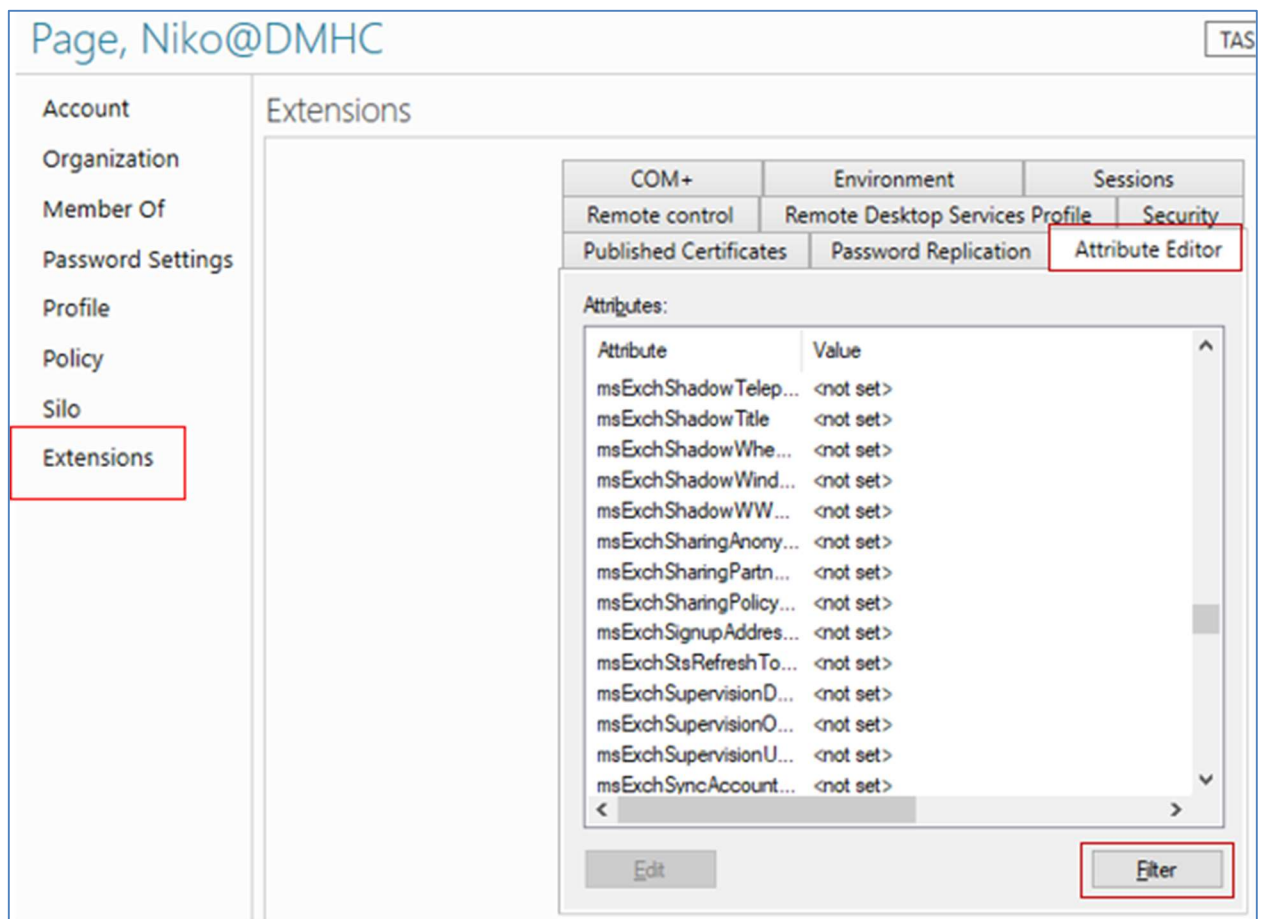
At the end of the week, a schedule task runs to remove security groups on the **Member Of** section for accounts place in the **DMHC Disabled Accounts** container. The security groups are documented in a log file. Reach out to server team for service requests to mirror a separated user's permissions.

8. Right-click the user account and then click **Properties** from the context menu.

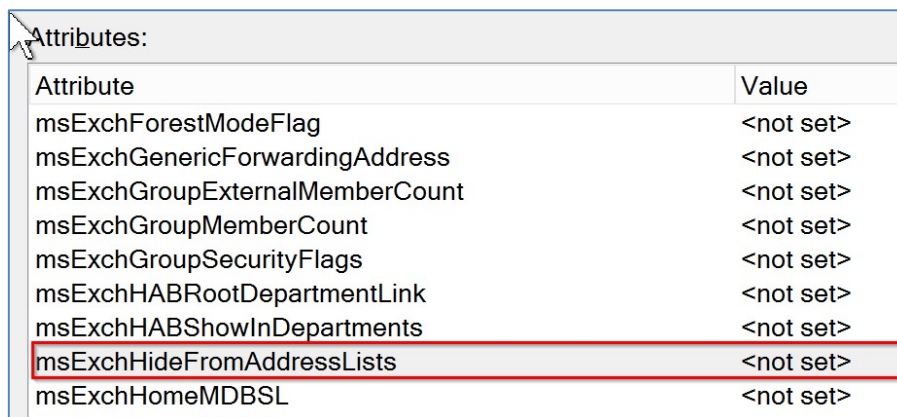


9. In the **Organization** section of the **Properties** screen, input the date and time in the **Description** field.

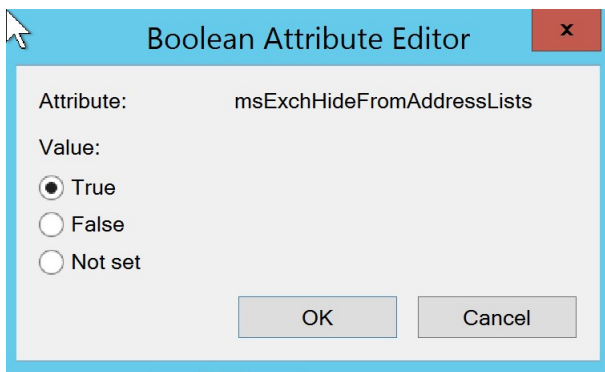
10. Click **Extensions** in the left navigation pane of the **Properties** screen, and then click the **Attribute Editor** tab.



- On the **Attributes** screen, click **Filter** and then click to uncheck **Show only attributes that have values**. Scroll down until you locate the attribute **msExchHideFromAddressLists** and double-click it.

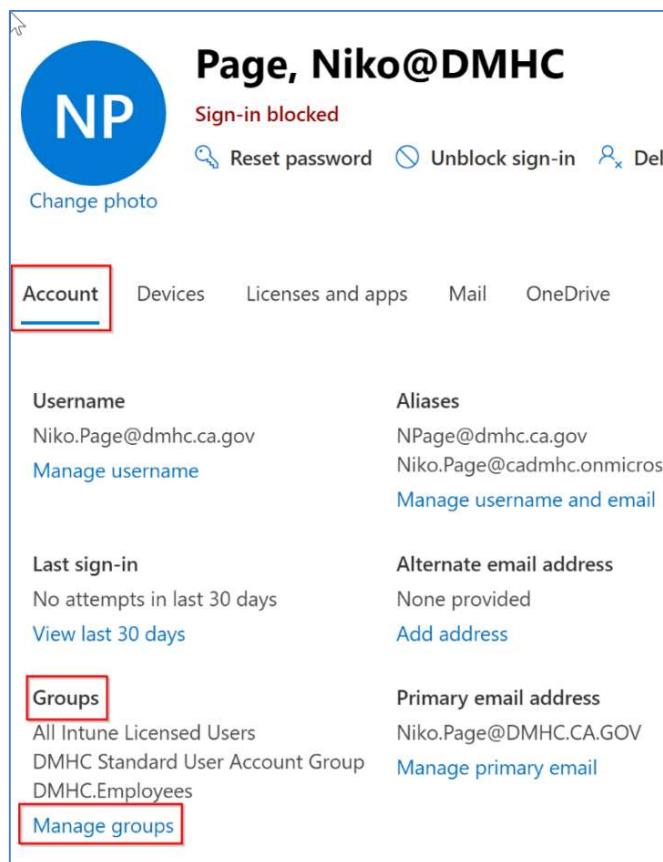


- In the **Boolean Attribute Editor** dialog box, click **True**. This hides the email address from Outlook's Global Address List (GAL). Click **OK** to close the dialog box, and then click **OK** once more to complete the changes to the user account.

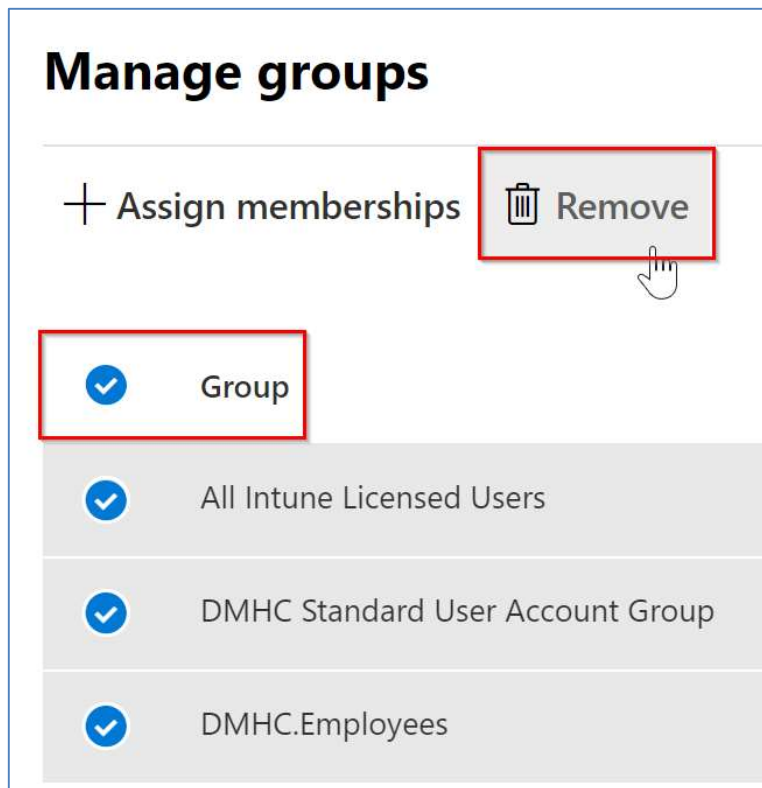


3.7 Removing Groups from the Disabled User ID in the Cloud

1. Open your browser to **Microsoft 365 Admin Center** (<https://admin.microsoft.com/#/homepage>). Search for the user account with the Admin Center's search input field. Select the user account, and from their settings section, click the **Account** tab, and then click **Manage groups**.



2. Click **Group** and then click **Remove**. Click **OK** when prompted.






Not all groups are distribution lists. Some like **DMHC Standard User Account Group**, are Entra ID groups, while other groups are SharePoint sites or Microsoft Teams/Channels. **Be sure to remove all distribution lists or groups from a disabled user's Entra ID account so that they don't continue to appear in e-mails.** Towards the end of the week, sac-task01 runs a weekly automated task that first records the group memberships for the disabled user accounts within the DMHC disable user accounts OU for future reference. Then it strips all groups from the disabled user accounts. If you need to review the past group memberships, make a request to the ISD server team.



Note: For section 3.8 when granting a manager access to a user's contents, specifically their mailbox. It must be converted from a user mailbox to a shared mailbox for the mailbox to remain visible. The reason being is because "DMHC Standard User Account Group" provisions license one of which grants the user access to their mailbox. The following steps should be completed prior to removing the groups in step 14 above.



- a. Navigate to the URL: <https://admin.exchange.microsoft.com/#!/mailboxes> and then search for the user's accounts name in the searchbox. Next click the DisplayName associated with user account.

Manage mailboxes


Create and manage settings for shared mailboxes. You can also manage settings for user mailb but to add or delete them you must go to the [Microsoft 365 admin center](#) and do this on the **active users** page. [Learn more about mailboxes](#)



 Mailflow setting  Hide from address list  Edit

 niko  ...

 Display name ↑	Email address
<div> Page, Niko@DMHC</div> <div>Page, Niko@DMHC</div>	Niko.Page@DMHC.CA.GOV

b. Next click the **Others** section followed by clicking **Convert to shared mailbox**.



Page, Niko@DMHC
User mailbox
 Hide mailbox  Email forwarding ...

General

Organization

Delegation

Mailbox

Others

Custom attributes
[Custom attributes](#)

Automatic replies
[Manage automatic replies](#)

Convert to shared mailbox
[Convert to shared mailbox](#)

Member of
[Group membership](#)

Recover deleted items
[Recover deleted items](#)

Litigation hold
[Manage litigation hold](#)

c. Lastly to convert the user mailbox to a shared mailbox click **Confirm**. With the mailbox converted proceed onto doing section 3.8



Convert mailbox from regular to shared

Do you want to convert the mailbox ?

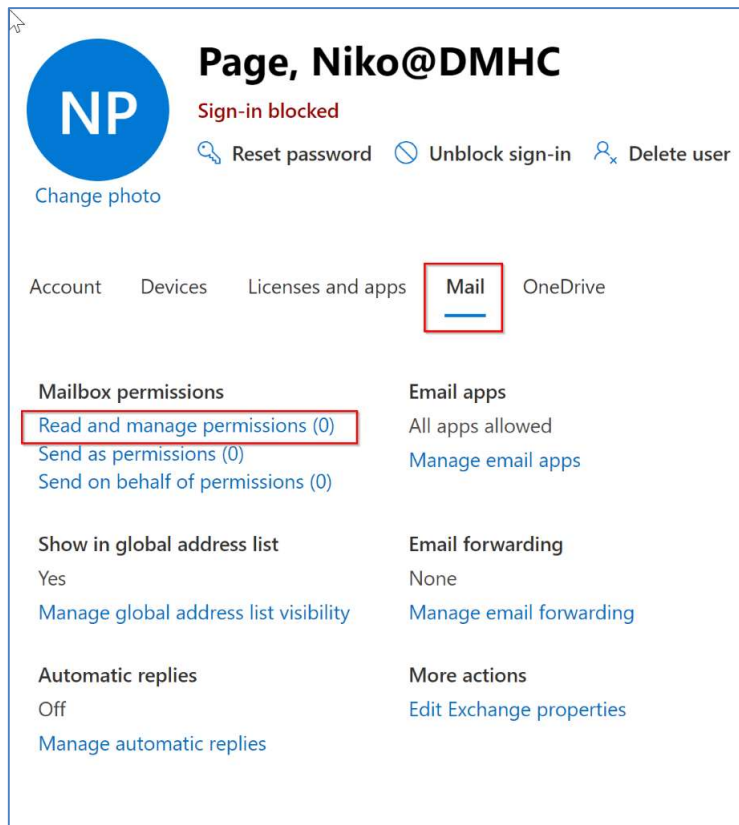
Confirm



3.8 Granting a Manager Access to a Separated Employee's Contents

Depending on whether the Cherwell ticket for separated employees indicates that the user account contents should be granted to their direct manager, follow these steps:

1. From the Admin Center, navigate to the properties of the user account. Then click the **Mail** tab and, if requested, grant permission to the employee's manager by clicking **Read and manage permission**.



2. Input the user account name that the requester specified should have permission to the separated user's mailbox. Then click **Save changes**.


Read and manage permissions




Set the permissions for users that can read, send as, or send on behalf of this mailbox. Changes can take up to 60 minutes to take effect.

Add read and manage permissions

LD Lopez, Daniel@DMHC X

3. From the Admin Center, search for the disabled user's name and select the account. Click the **OneDrive** tab. Next click **Create link to files**. Once the link is created, click it, and browse to the user's OneDrive location.

**Lopez, Daniel@DMHC**

 Reset password  Block sign-in  Delete user

[Change photo](#)

Account Devices Licenses and apps Mail **OneDrive**

Get access to files

Create a link to view and edit Lopez, Daniel@DMHC's OneDrive files.

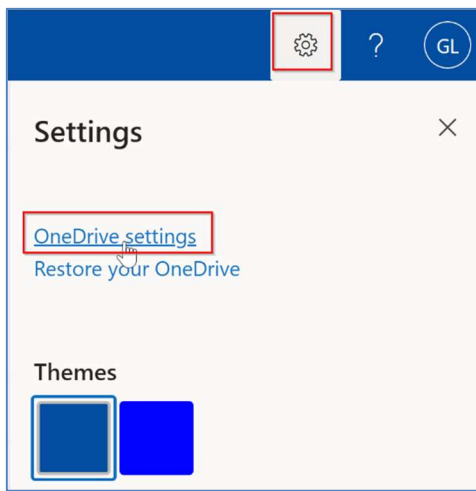
Create link to files

Storage used

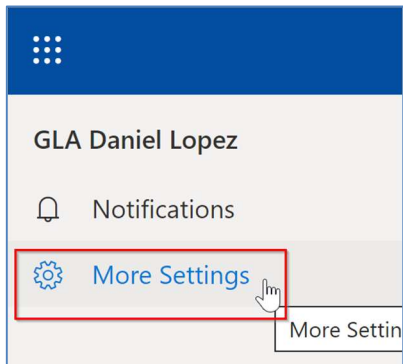
0.05% (524.288 MB of 1024 GB)

[Edit](#)

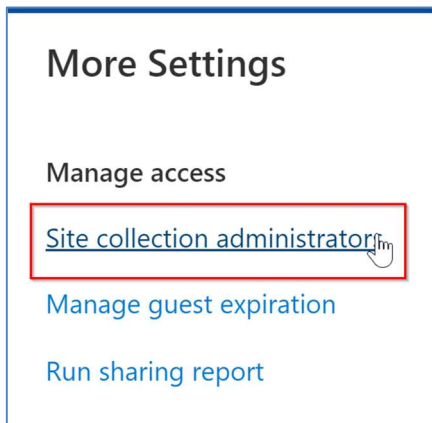
4. Once on the user's OneDrive site click on the **Cog Wheel** icon to view the settings and then click **OneDrive settings**.



5. On the OneDrive Settings page click **More Settings**.



6. While viewing More Settings click **Site collection administrators**.



7. Enter the name of the user who will need access to the recently separated employee. Select the user and click **OK**.

Permissions ▸ Site Collection Administrators ⓘ

Site Collection Administrators

Site Collection Administrators are given full control over all Web sites in the site collection. They may also receive site use confirmation mail. Enter users separated by semicolons.

Admin DLopez x GLA Daniel Lopez x Lopez, Daniel@DMHC x Muslih

GLA Bashar Muslih

Muslih, Bashar@DMHC
Student Assistant

Showing 2 results

Bashar.Muslih@DMHC.CA.GOV

8. Finally, send an e-mail to the employee's manager/requester, informing them that they now have access to the separated user's mailbox, and home folder in OneDrive.
9. Upon adding permission to the separated user's mailbox, anticipate for it to take approximately 30 minutes for it to show up in their manager's mailbox.

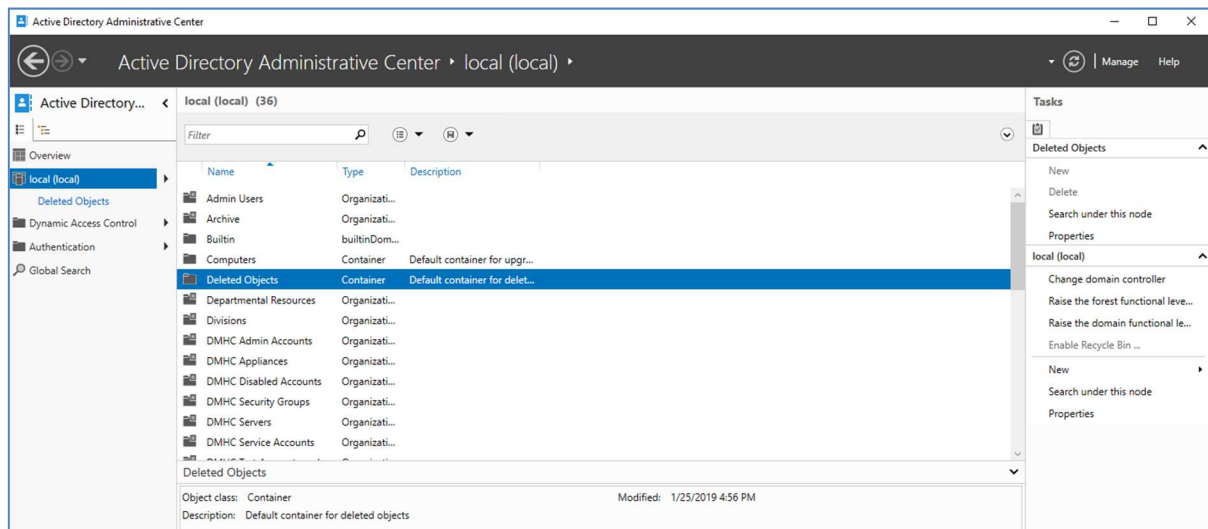
Notice that there is an account, GLA Daniel Lopez, that was automatically added due to creating a link to the user's OneDrive. After giving access to the manager, remove your own account that was used to manage the user's OneDrive permissions.

Note the date of how long a manager requests their employee's content and reach out to clarify whether they still need access, or should it be removed.

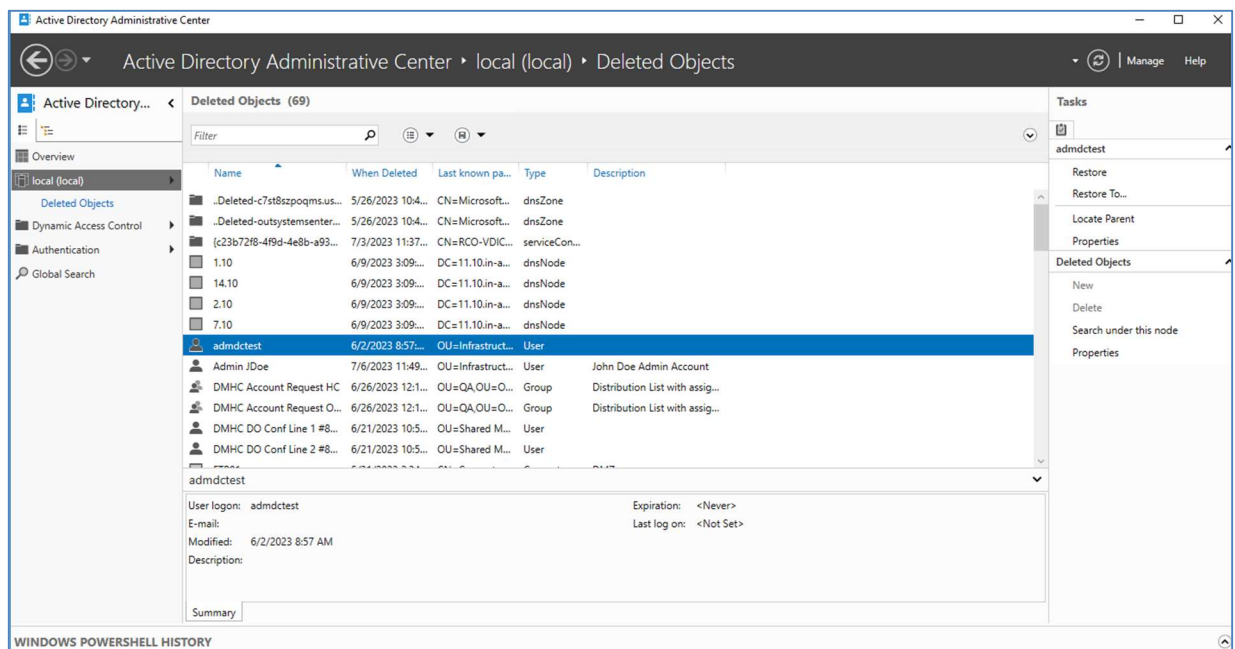
3.9 Managing Deleted Active Directory Objects

This procedure explains how to manage deleted Active Directory objects.

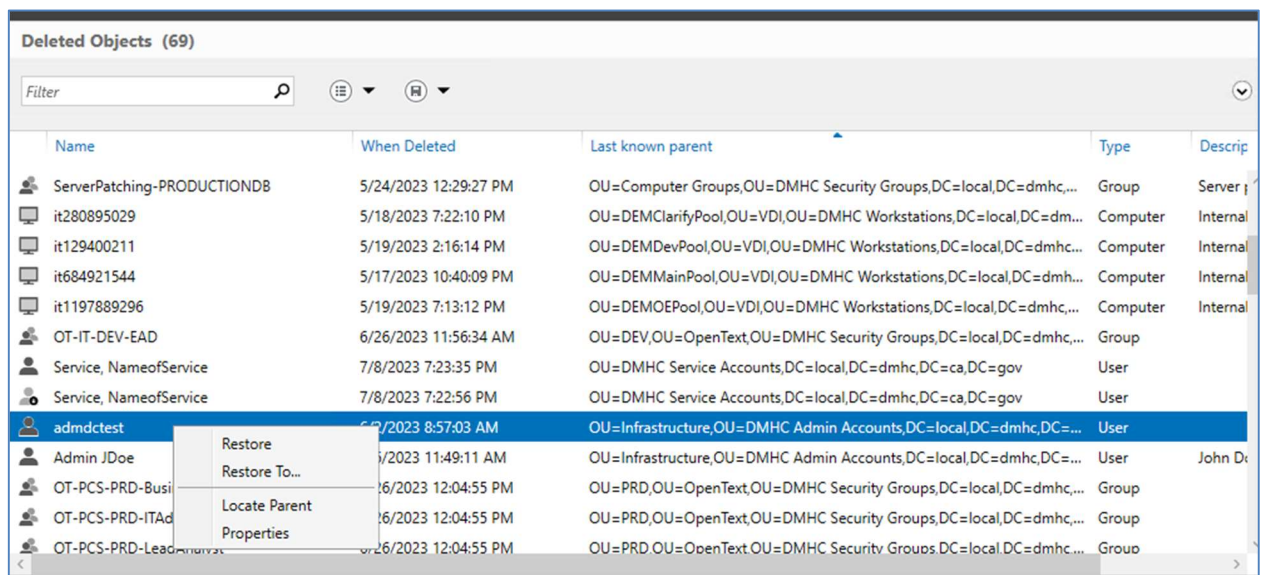
1. Open **Active Directory Administrative Center**. Next, click **local (local)** in the left navigation pane, and then click **Deleted Objects**.



2. Click **Deleted Objects** in the right pane.



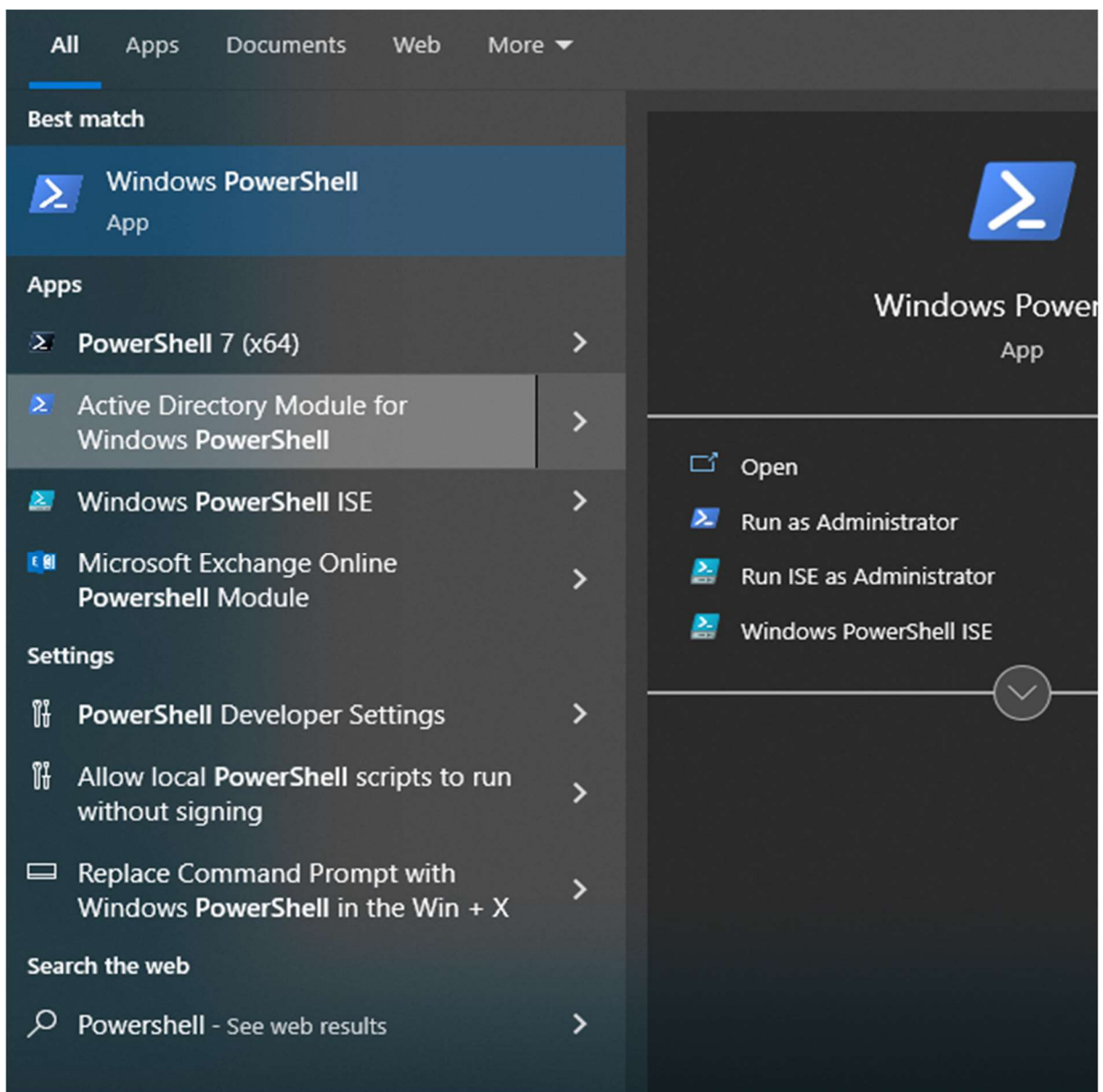
3. The Deleted Objects window displays where you can view, browse and review deleted objects. Note that there is a 60-day default lifecycle before system purges. Right-click a deleted object to view its properties, locate the parent or restore the object.



3.10 Exporting an Active Directory User Creation Report

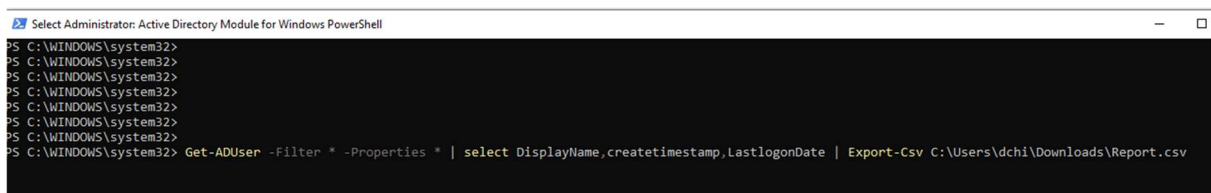
Use the following steps to export an Active Directory user creation report that will display the Active Directory display name, creation date and last login for all users:

1. Open **Active Directory Module for Windows PowerShell**, and then click **Run as Administrator**. Note that if you don't have the module, go to <https://learn.microsoft.com/en-us/powershell/module/activedirectory/?view=windowsserver2022-ps>, and follow the instructions.



2. In the PowerShell window, enter a command like the following to export a CSV file to a target folder location:

```
Get-ADUser -Filter * -Properties * | select
DisplayName,CreateTimeStamp,LastlogonDate | Export-Csv
C:\yourfolder\creationreport.csv
```



4. References

The following sections contain the sources of reference for this SOP.

4.1 DMHC Active Directory Security Groups

When provisioning users as described in Provisioning Active Directory User Accounts in the Procedures section, you have the option of adding security groups to the user profile. Typically, the requestor of a service account refers to another employee's account as an example. Or the requestor may refer to his or her respective office's folders. If unsure, refer to your system administrator for guidance.

Note that when you provide a user to a security group while logged in, the user must log out and log back in with internal network/VPN access to update permissions.

The following table lists the base security groups which you should assign to a new user account:

	Root Folder	SharePoint Hub Access Group
Office Name		
Director's Office	Exec_DO	DMHC.Exec
Help Center	HMOHC	DMHC.HMOHC
Office of Administrative Services	Admin	DMHC.OAS
Office of Enforcement	ENF	DMHC.ENF
Office of Financial Review	OFR	DMHC.OFR
Office of Legal Services	OLS	DMHC.OLS
Office of Plan Licensing	OPL	DMHC.OPL
Office of Plan Monitoring	OPM	DMHC.OPM

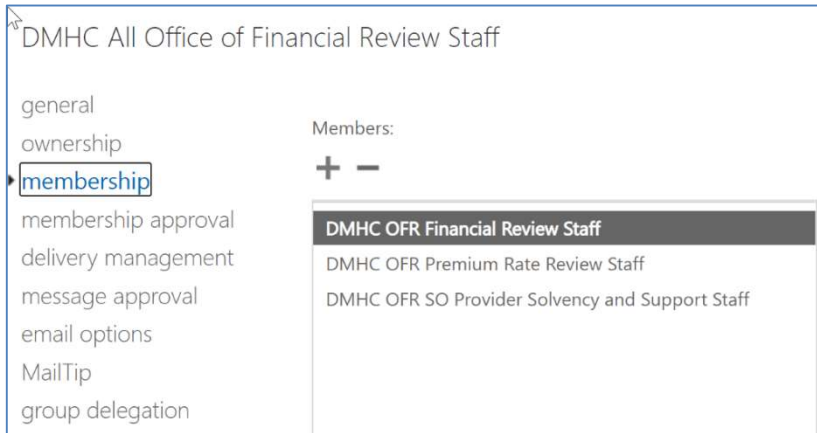
The following list describes additional security groups that you can assign to a user account:

- **Aspire**—SO, FB, or LA; Allows users to access the Aspire Training app.
- **Management Distribution List**—All supervisors and managers.
- **Tableau's Manager Dashboard**—Tableau Reader Active Directory. Note that if a user belongs to the Management Distribution List, Technology Services Division (TSD) must install Tableau Reader and grant access to the Tableau site.
- **VPN Access**—PANVPNUUsers
- **VDI Access**
 - **Main Pool**: VDI Win10 Main Pool
 - **Help Center/Office of Enforcement Pool**: VDI Win10 HCOE Pool,
 - **Maximus Pool**: VDI Win10 Maximus Pool
 - **ProLaw**: OE Pool
 - **EAD Pool**: EAD Pool
- **Spotlight Access**—Clarify HC Users and Clarify Project Users.

4.2 DMHC Distribution Lists

Distribution lists and their configurations vary from office-to-office. Office specific groups have the following naming format, **DMHC All Office of _____**.

- Within OTI, the distribution list is configured as a dynamic distribution list. User accounts whose **Office** field is **Office of Technology and Innovation** are automatically added to the distribution list, **DMHC All Office of Technology and Innovation Staff**.
- Distribution lists for other offices are designed with nested distribution lists. For instance, **DMHC All Office of Financial Review Staff** is made up of three smaller distributions lists, as shown in the following image. Therefore, administrators only need to alter the small groups to affect the larger group.



- There are distribution lists that are simply made-up user accounts, without a nested or dynamic assignment structure. One office's distribution that has such a structure is **DMHC All Office of Plan Licensing Staff**.
- The distribution list, **DMHC All Counsel**, is made up of individuals with the following titles: Attorney (I, III, IV), Special Investigator, Assistant Chief Counsel and General Counsel. By default, these user accounts are assigned to this distribution list.
- Some office distribution lists are managed by administrative support staff using Outlook's Global Address List. For this reason, administrative support staff simply need to delegate ownership access.

5. Revision Log

Version #	Date	Author	Key Differences