



FOREFRONT IDENTITY MANAGEMENT V3

02.01.2016

MODULE ONE - USER CREATION AND PORTAL OVERVIEW	6
USER CREATION AND SYNCHRONIZATION PROCESS.....	7
AGENCY ROLES AND RESPONSIBILITIES	8
LOGGING INTO FOREFRONT IDENTITY MANAGER – PORTAL (FIMPORTAL)	11
HOME PAGE OVERVIEW	12
MODULE ONE REVIEW	13
MODULE ONE – STUDENT EXERCISE.....	13
MODULE TWO - DISTRIBUTION GROUPS	14
CREATE NEW DISTRIBUTION GROUPS	15
CREATE DYNAMIC DISTRIBUTION GROUPS.....	18
FINDING YOUR AGENCY DISTRIBUTION GROUPS	23
ADVANCED SEARCH FUNCTION	24
MODIFYING DISTRIBUTION GROUPS	25
MANAGING OWNERS AND CO-OWNERS	27
MANAGING CRITERA BASED DISTRIBTION GROUPS.....	28
DELETING DISTRIBUTION GROUPS	31
MODULE TWO REVIEW	32
STUDENT EXERCISES	32
MODULE THREE - SECURITY GROUPS	33
CREATE NEW SECURITY GROUPS	34
CREATE DYNAMIC SECURITY GROUPS.....	38
FINDING YOUR AGENCY SECURITY GROUPS	43
ADVANCED SEARCH FUNCTION	44
MODIFYING SECURITY GROUPS	45
MANAGING OWNERS AND CO-OWNERS	48
MANAGING CRITERA BASED SECURITY GROUPS	49
DELETING SECURITY GROUPS	52
MODULE THREE REVIEW.....	53

STUDENT EXERCISES	53
MODULE FOUR - EMPLOYEE, CONTRACTOR, COUNTY AND OTHER USERS	54
ADD NEW 5X USER ACCOUNTS.....	55
FINDING EMPLOYEE, CONTRACTOR, COUNTY WORKER AND OTHER ACCOUNTS	58
ADVANCED SEARCH FUNCTION	59
EDITING EMPLOYEE, CONTRACTOR AND COUNTY WORKER USER INFORMATION.....	60
ENABLE NEW MAILBOX.....	66
EXCHANGE LICENSING	66
ASSIGNING AND REMOVING FULL ACCESS PERMISSIONS.....	67
ASSIGNING AND REMOVING SEND-AS PERMISSIONS	68
MAILBOX FEATURES TAB	69
MAILBOX ACCESS CONTROL.....	69
MODULE FOUR REVIEW	70
STUDENT EXERCISES	70
MODULE FIVE - RESOURCE ACCOUNTS, ROOM, EQUIPMENT, AND SHARED MAILBOXES	71
CREATING NEW RESOURCE ACCOUNT	72
FINDING RESOURCE ACCOUNTS	73
ADVANCED SEARCH FUNCTION	74
EDITING RESOURCE ACCOUNTS.....	75
ASSIGNING AND REMOVING FULL ACCESS PERMISSIONS.....	78
ASSIGNING AND REMOVING SEND-AS PERMISSIONS	79
HIDING MAILBOX FROM THE GAL.....	79
EQUIPMENT/ROOM SETTINGS.....	80
MODULE FIVE REVIEW	81
STUDENT EXERCISES	81
MODULE SIX - SERVICE AND SERVER ADMIN ACCOUNTS	82
CREATING NEW SERVICE OR SERVER ADMIN ACCOUNT	83
FINDING SERVICE AND ADMIN ACCOUNTS	85

ADVANCED SEARCH FUNCTION	86
EDITING SERVICE ACCOUNTS.....	87
MODULE SIX REVIEW	88
STUDENT EXERCISES	88
MODULE SEVEN - ADMINISTRATOR PASSWORD RESET	89
ACCESSING PASSWORD.OHIO.GOV/ADMIN	90
RESETTING PASSWORDS - ADMINISTRATOR.....	91
CHANGING AN USERS PASSWORD	92
RESETTING ADMIN ACCOUNTS.....	92
RESETTING SERVICE ACCOUNTS	93
MODULE SEVEN REVIEW	95
STUDENT EXERCISES	95
MODULE EIGHT – USER SELF-SERVICE PASSWORD RESET	96
ACCESSING PASSWORD REGISTRATION SITE.....	97
ACCESSING PASSWORD RESET SITE	98
MODULE EIGHT REVIEW	99
STUDENT EXERCISES	99
MODULE NINE - REPORTING	100
ACCESSING THE REPORT SITE	101
NEW HIRE REPORTS	102
NEW HIRES COMPLETED.....	103
TRANSFER REPORTS.....	103
OTHER FIM REPORTS.....	105

MODULE ONE - USER CREATION AND PORTAL OVERVIEW

AGENCY ROLES AND RESPONSIBILITIES

Training time: 5 minutes

- Speak to students about the roles and responsibilities and the agency administration of users, groups, resource, administration, service accounts, and user passwords.
- Clearly define the following:

User accounts

- Basic FIM portal administration level access
- E-mail creation (office 365 and local)
- Office 365 licensing
- Disable mailbox (office 365 and local)
- Enable full and send-as permissions
- Disable full and send-as permissions
- Hide account from global access list
- Enable local Lync
- Administrative password changes

Resource Accounts

- Create Room, Equipment, and Shares
- Modify basic user settings for accounts
- Enable full and send-as permissions
- Disable full and send-as permissions
- Hide account from global access list

Groups – Distribution

- Create distribution groups – manually entered users
- Create distribution groups – criteria based
- Modify criteria and manual based groups
- Delete criteria and manual based groups
- Manage group owners and co-owners

Groups – Security

- Create distribution groups – manually entered users
- Create distribution groups – criteria based
- Modify criteria and manual based groups
- Delete criteria and manual based groups
- Manage group owners and co-owners

Service Accounts

- Create service accounts
- Modify service account information
- Delete service accounts
- Enable – disable service accounts
- Administrative level password administration

Administrator Accounts

- Create administrator accounts
- Modify administrator account information
- Delete administrator accounts
- Enable – disable administrator accounts

Who	Task	Customer function	How
User Administration			
Access Control	Create user accounts	X	Employee
Access Control	Manage editable attributes-user	X	Employee
	Manage administrative agency-user		
Access Control Service Desk	Reset passwords	X	FIM SSPR
Access Control	De-provision user accounts	X	Employee
Special Account Management			
	Create shared resources	X	Shared Resource
	Manage editable attributes-shared resources	X	Shared Resource
	Manage administrative agency-shared resources		
	Create contacts		
	Manage editable attributes-contact	X	Shared Resource
	Create distribution groups	X	Distribution Group
	Manage distribution groups	X	Distribution Group
	Manage administrative agency-distribution groups		
User Self-Service			
	Ensure agency users complete self-registration	X	FIM SSPR
Core Shared Service (CSS)			
Access Control	Enable/disable base email service	X	Employee
Access Control	Enable/disable base <u>lynx</u> service	X	Employee
	Enable/disable base OAKS service	X	TBD
	Enable/disable base <u>sharepoint</u> service	X	TBD
LDAP/LDAPS Authentication			
	Configure application for authentication	X	TBD
	Verify connectivity to LDAP/LDAPS hosts	X	TBD
	Troubleshoot connectivity issues	X	TBD
	Troubleshoot application authentication issues	X	TBD
	Monitor connection for <u>QoS</u> (not done at this time)		
Active Directory Federation Services			
	Configure service for ADFS	X	TBD
	Verify connectivity to ADFS hosts	X	TBD
	Troubleshoot connectivity issues	X	TBD
	Monitor connection for <u>QoS</u> (not done at this time)		
Support / OIT's Customer Service Center (CSC) Footprints			
	Maintain agency points of contact lists	X	TBD
	Maintain agency service notification lists		

LOGGING INTO FOREFRONT IDENTITY MANAGER – PORTAL (FIMPORTAL)

Training time: 5 minutes

➤ Explain browser support for:

- Internet Explorer 9 – 10 – 11 (no mobile support)
- Chrome (no support)
- Firefox (no support)

➤ Demonstrate the FIMPORTAL Login process.

Production: <https://fimportal.ohio.gov/identitymanagement>

Training site: <https://fimportal.training.ohio.gov/identitymanagement>

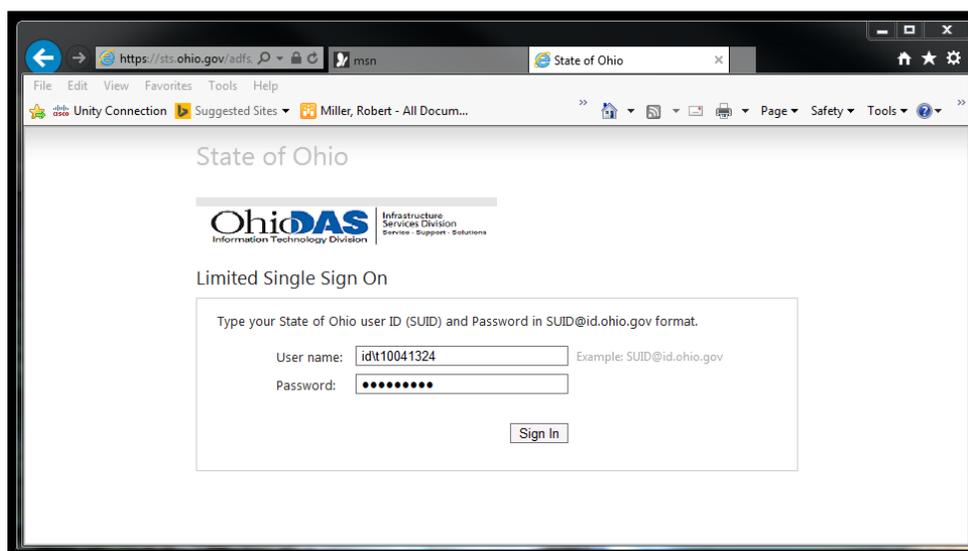
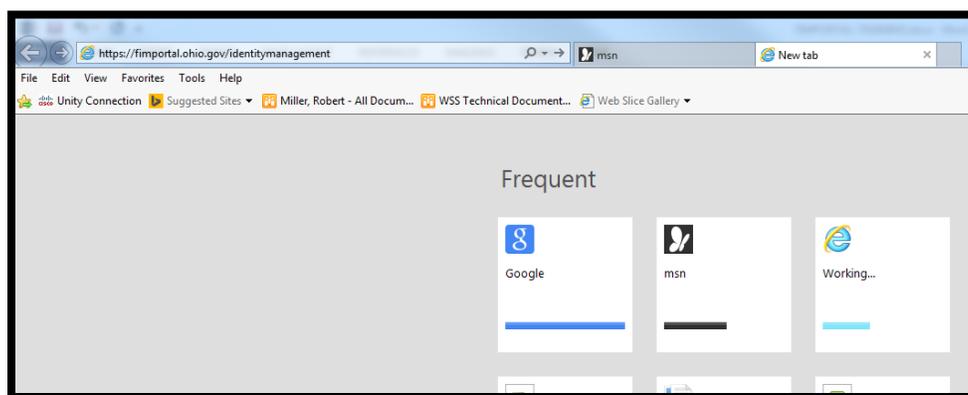


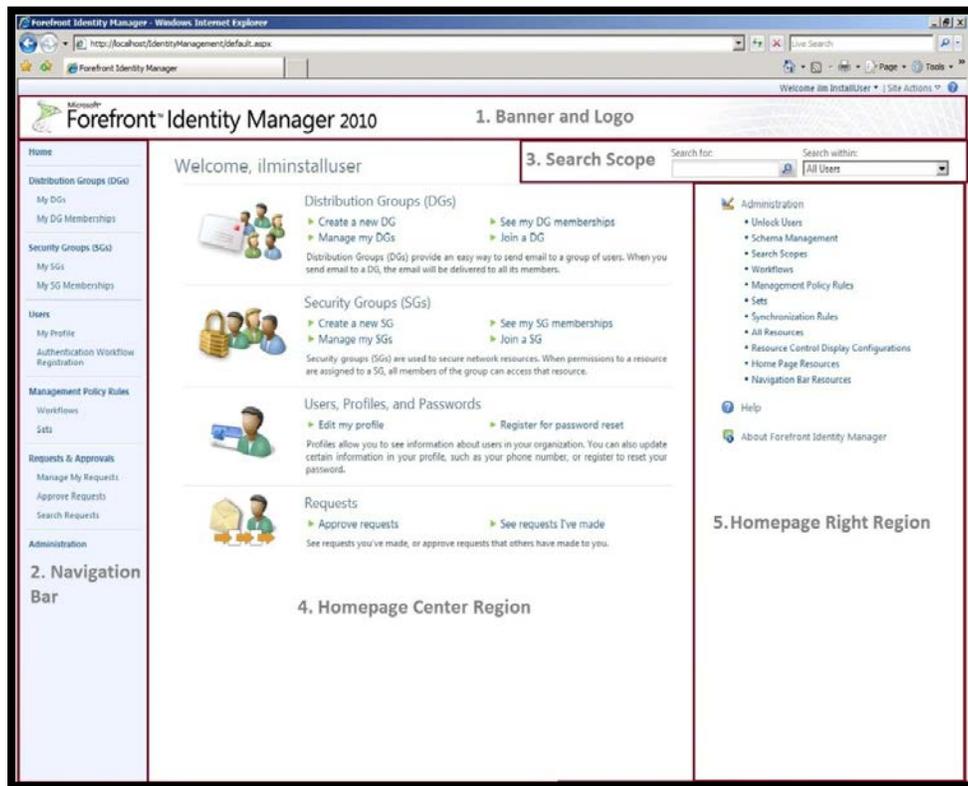
Figure 2 - Active Directory Logon Page

HOME PAGE OVERVIEW

Training time: 5 minutes

Components of the FIM Portal UI

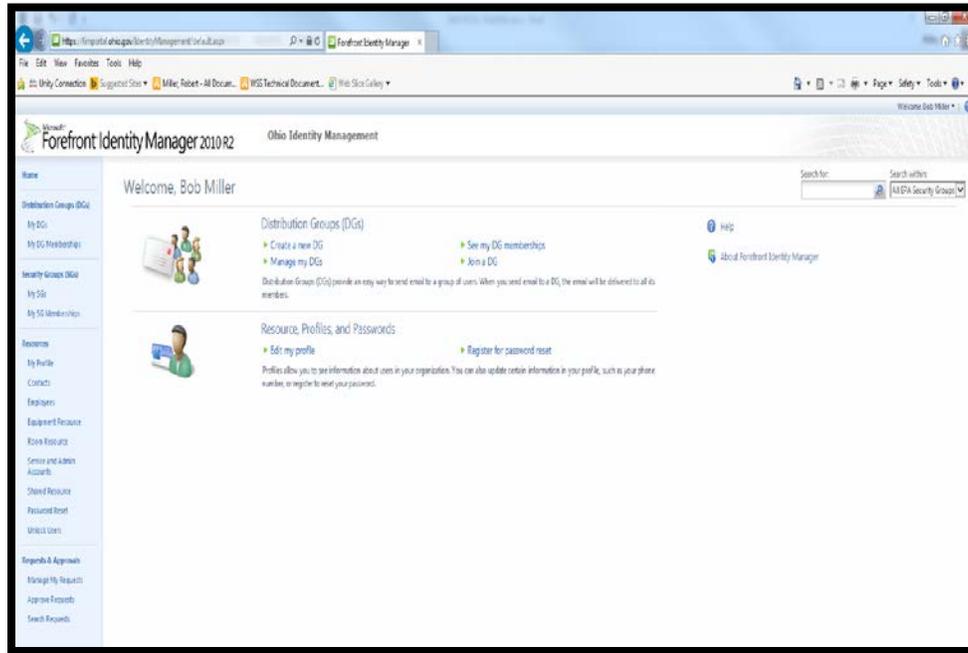
The following figure shows the different parts of the FIM Portal that you can customize by using UI configuration resources.



- The Banner and Logo appear at the top of each FIM Portal page.
- The Navigation Bar is the vertical menu on the left side of the FIM Portal. The Navigation Bar helps the user move among various self-service and information technology professional (IT pro) tasks. The list consists of selected Navigation Bar resources. Each item in the list points to a unique URL.
- Search scopes appear on the upper right area of each FIM Portal page. A search scope includes a search input box and a search scope drop-down list. The search scope is critical for controlling what appears in a page list view, that is, the main area of a portal page where resources are listed. The Homepage includes text and links that lead the end user to explore different features in FIM. It has three areas:
- Center region – work area

The State of Ohio Portal Page has been designed to look like the page below.

- Show students the home page by logging on to:
<https://fimportal.ohio.gov/identitymanagement>



MODULE ONE REVIEW

1. Can someone tell me the name of the Forefront Identity home page?

Answer: <https://fimportal.ohio.gov/identitymanagement>

2. Can some tell me what functions an agency is responsible for on an employee's user account?
3. **Answer:** Basic FIM portal administration level access; e-mail creation (office 365 and local); Office 365 licensing; Disable mailbox (office 365 and local); Enable full and send-as permissions; disable full and send-as permissions; hide account from global access list; enable local Lync; administrative password changes

MODULE ONE – STUDENT EXERCISE

- Have student logon to the FIM Portal training home page:

<https://fimportal.training.ohio.gov/identitymanagement>

MODULE TWO - DISTRIBUTION GROUPS

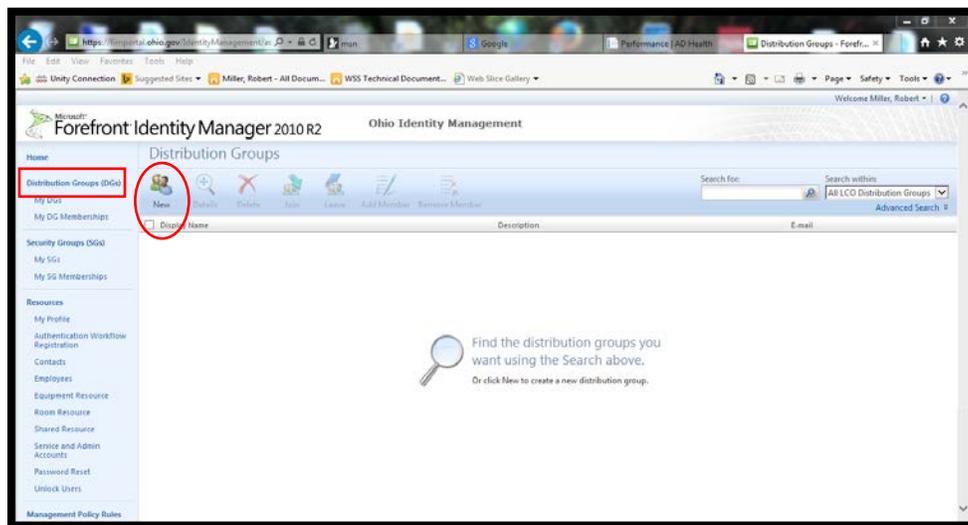
CREATE NEW DISTRIBUTION GROUPS

Training time: 10 minutes

- Create new manually populated distribution group

Rules to creating new distribution groups with manually based users:

- All users or groups you intend to include in the group must be present in FIM Portal.
 - All normal active directory group rules apply. Example you cannot add a domain local mail enabled security group to a distribution group because active directory does not allow this to occur.
 - The group mail alias (nickname) cannot contain invalid characters. Examples of invalid characters are spaces; backslashes; commas. The best solution is to use the common characters such as a period and/or dashes
 - The agency OAKS code will precede the group name upon creation; however this can be changed after the name has been updated.
 - Attribute with a * next to the name are required attributes
 - Distribution groups are created through a synchronization process and can take 30 to 60 minutes to be available in active directory, for these groups to be active in Office365 it can take an additional 30 – 60 minutes
- Begin creating a new distribution list by selecting Distribution Groups from the Navigation panel.



- Select New on the panel

➤ Enter the following information:

- Display Name:

Note: Your agency OAKS code will be inserted automatically upon creation. You can change this once the OAKS code appears by editing the display name.

- **E-mail Alias:** This requires proper formatting.
- **Member Selection:** This will be manual.
- **Application Code:** Choose email from the pull down list.
- **Alternate Agency Code:** Use this field to assign another agency OAKS code to your group
- **Description:** Enter a description.

The screenshot shows a web browser window titled "Forefront Identity Manager -- Webpage Dialog" with the URL "http://fimportal.idga.ohio.gov/identitymanagement/asp/!common/popup.aspx". The page is titled "Create Distribution Group" and has tabs for "General", "Members", "Owners", and "Summary". The "General" tab is active. The form contains the following fields and options:

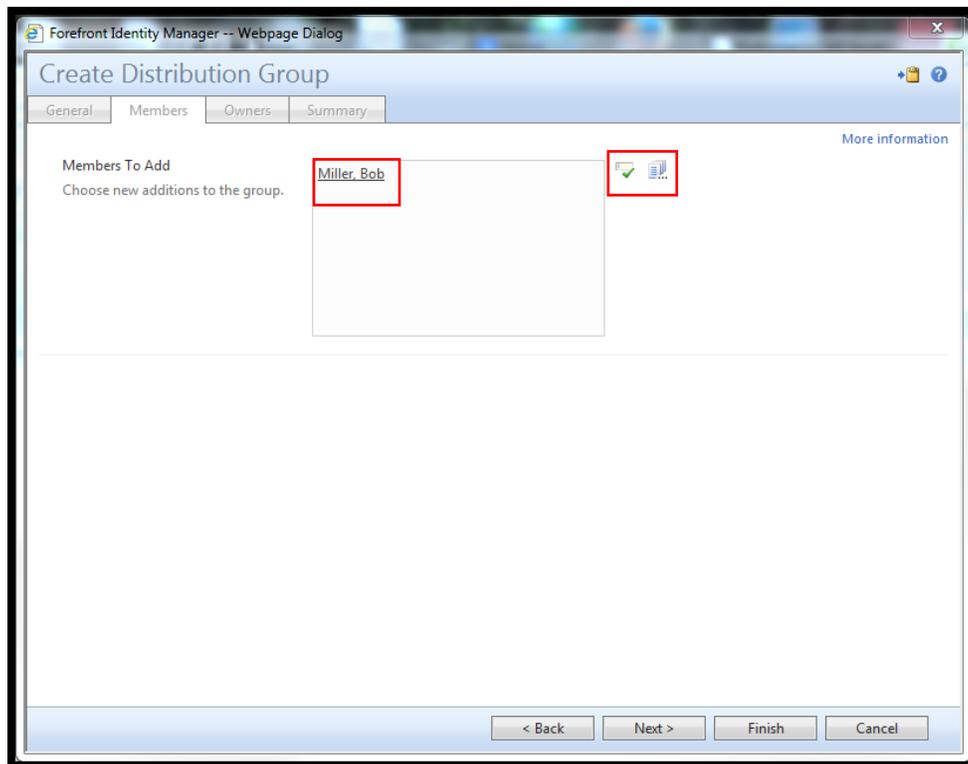
- Display Name ***: A text input field.
- IBM Group**: A checkbox labeled "Group is IBM".
- E-mail Alias ***: A text input field.
- Member Selection ***: Three radio button options:
 - Manual**: Members are manually managed.
 - Manager-based**: Membership is calculated to include a manager, and all people reporting directly to that manager.
 - Criteria-based**: Membership is calculated based on one or more attributes of the members.
- Application Code ***: A dropdown menu with the note "Only applies to Security Groups".
- Alternate Agency Code**: A dropdown menu.
- Description ***: A text area.

A red asterisk indicates that fields marked with a red asterisk require input. At the bottom of the form are buttons for "< Back", "Next >", "Finish", and "Cancel".

Members

➤ Enter Members

The creator of the group will be automatically populated in the **“Members to Add”** attribute and can be removed if needed. Also notice that these are SharePoint picker buttons to the right. Underlining SharePoint controls the selection of the users. Use the people picker to find your group members.



Owners and Co-Owners

The creator of the group is automatically added to the owner and displayed owner attributes; this can be changed as required; however; all FIM Portal administrators have rights to all agency groups. The recommendation is to leave this attribute alone and add all additional owners in the co-owners attribute. All co-owners have rights to change group membership in FIM Portal.

Note: We strongly suggest you keep the Owner to a single user and use CO-Owner for all other users. The behavior in FIM Portal is different for these permissions and for Owner to function you must have FIM PORTAL admin rights.

Join Restrictions

This is not enforced.

The screenshot shows the 'Create Distribution Group' dialog box in Forefront Identity Manager. The 'Join Restriction' field is highlighted with a red box, and the 'Co-Owners' field is also highlighted with a red box. The 'Owner' field contains 'Miller, Bob'. The 'Displayed Owner' field also contains 'Miller, Bob'. The 'Join Restriction' options are 'Owner approval required' (selected) and 'None'. A red asterisk indicates that the 'Join Restriction' field requires input.

CREATE DYNAMIC DISTRIBUTION GROUPS

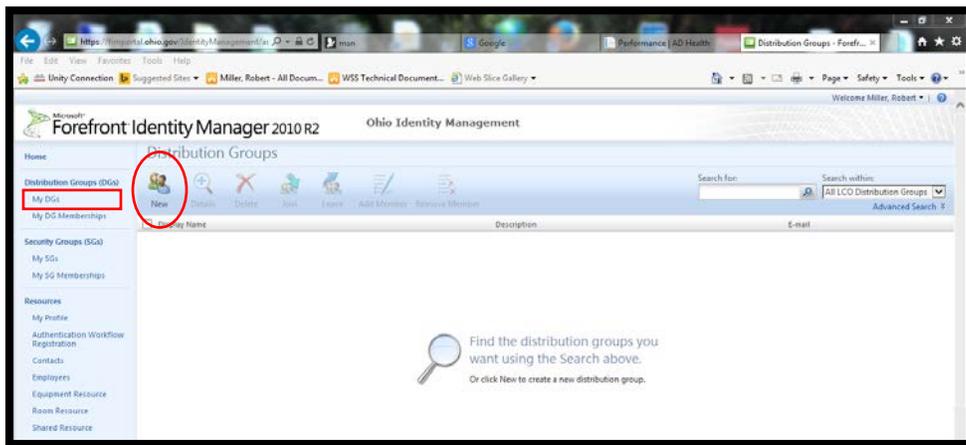
Training Time: 10 minutes

- Create new criteria based distribution groups

Rules for creating new distribution groups with manually based users:

- All users or groups to be included in the group must be present in FIM Portal.
- All normal active directory group rules apply. Example you cannot add a domain local mail enabled security group to a distribution group because active directory does not allow this to occur.
- The group mail alias (nickname) cannot contain invalid characters. Examples of invalid characters are spaces; backslashes; commas. The best solution is to use the common characters such as a period and/or dashes
- The agency OAKS code will precede the group name upon creation; however this can be changed after the name has been updated.

- Attribute with a * next to the name are required attributes
 - You cannot mix criteria based groups and criteria user when building your criteria selection. It must be one or the other.
 - Distribution groups are created through a synchronization process and can take 30 to 60 minutes to be available in active directory, for these groups to be active in Office365 it can take an additional 30 – 60 minutes
 - Criteria based groups are only criteria based within FIM Portal, exchange will contain the actual user accounts when the groups synchronize from Portal to AD and Office365
 - You cannot mix manually selected membership and criteria in the same group
- Begin creating a new distribution list by selecting Distribution Groups from the Navigation panel.



- Select New on the panel
- Enter the following information:
- Display Name:

Note: Your agency OAKS code will be inserted automatically upon creation. You can change this once the OAKS code appears by editing the display name.

- **E-mail Alias:** This requires proper formatting.
- **Member Selection:** This will be criteria.
- **Application Code:** Choose email from the pull down list.
- **Alternate Agency Code:** Use this field to assign another agency OAKS code to your group
- **Description:** Enter a description.

The screenshot shows the 'Create Distribution Group' interface in Forefront Identity Manager. The 'Member Selection' section is highlighted in yellow, and the 'Criteria-based' option is selected. The 'Application Code' and 'Alternate Agency Code' dropdown menus are highlighted with a red box.

CRITERIA SELECTION

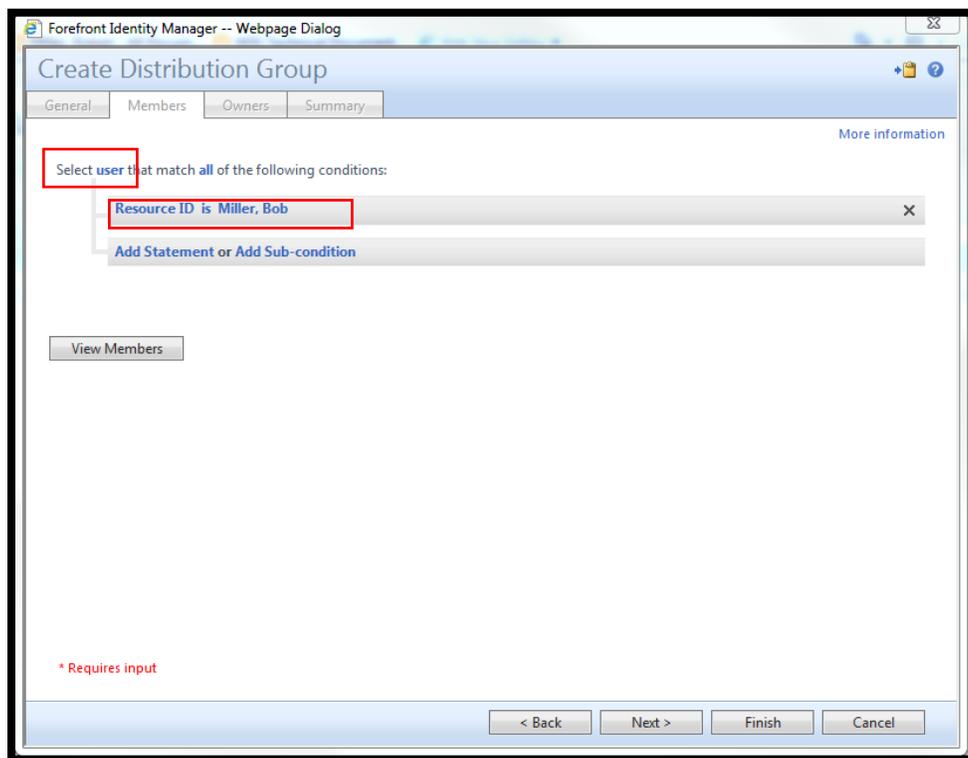
- Next to **“Select”**
- Choose User from the drop down list
- Remove the preselected option of Resource ID
- Click Add Statement
- A line will be inserted – select **Click** to select....

A drop down list of all attributes will be presented.

Common attributes to use include:

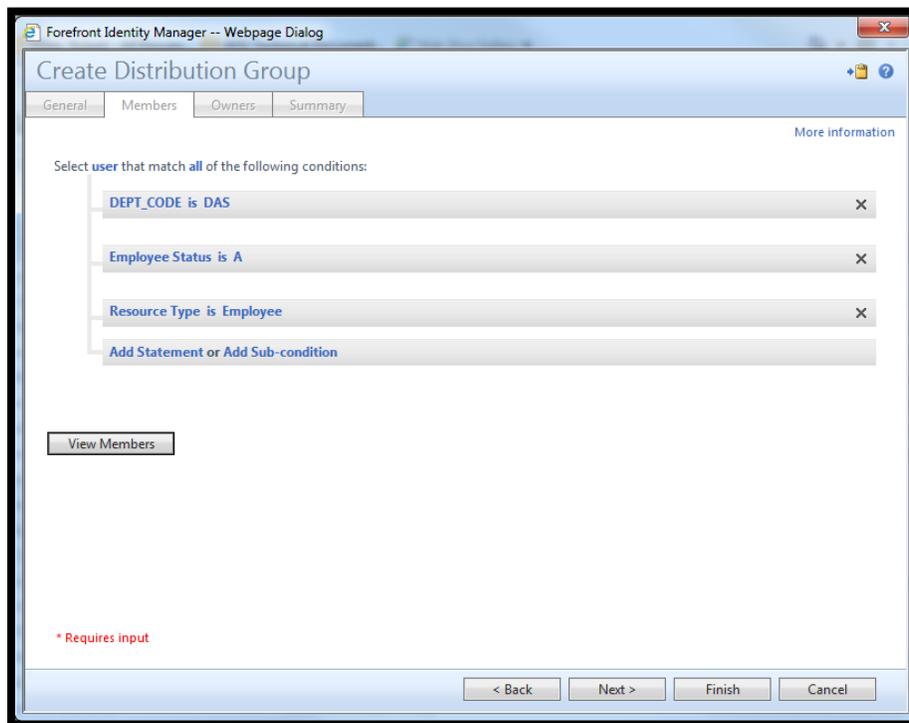
- **Account Name** – (EmployeeID – OAKS ID etc.)
- **DEPT_CODE** – controls all aspects of what data is available to you
- **Employee Status** – Active (A) and Inactive (I)
- **DL Condition 1,2 and 3** – agency Portal admin defined criteria
- **DEPTCODE 2 and 4** – agency HR defined criteria
- **DisplayName** – lastname, firstname
- **Job Title**

- **Logical** – depending on the attribute type appropriately choose the type of logic (is, is not, etc.)
- **Value** – value you are looking for in your search



The example below would produce a distribution group in active directory with all active DAS employees.

Note: As people are moved from Active and Inactive status, they are either added or removed.



Owners and Co-Owners

The creator of the group is automatically added to the owner and displayed owner attributes; this can be changed as required; however; all FIM Portal administrators have rights to all agency groups. The recommendation is to leave this attribute alone and add all additional owners in the co-owners attribute. All co-owners have rights to change group membership in FIM Portal.

Note: We strongly suggest you keep the Owner to a single user and use CO-Owner for all other users. The behavior in FIM Portal is different for these permissions and for Owner to function you must have FIM PORTAL admin rights.

Join Restrictions

This is not enforced.

The screenshot shows the 'Create Distribution Group' dialog box in Forefront Identity Manager. The 'Owners' tab is selected. The 'Owner' field contains 'Miller, Bob'. The 'Co-Owners' field is empty. The 'Displayed Owner' field also contains 'Miller, Bob'. The 'Join Restriction' section has 'Owner approval required' selected, with the description 'A user will become a member of the group only after the group owner has approved the join request.' The 'None' option is also visible, with the description 'Any user can become a member of the group.' At the bottom, there are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'. A red asterisk indicates a required input field.

FINDING YOUR AGENCY DISTRIBUTION GROUPS

Training Time: 5 minutes

From the distribution option – notice the **“Search for”** and **“Search within”** options

These are the two options available to search for distribution groups.

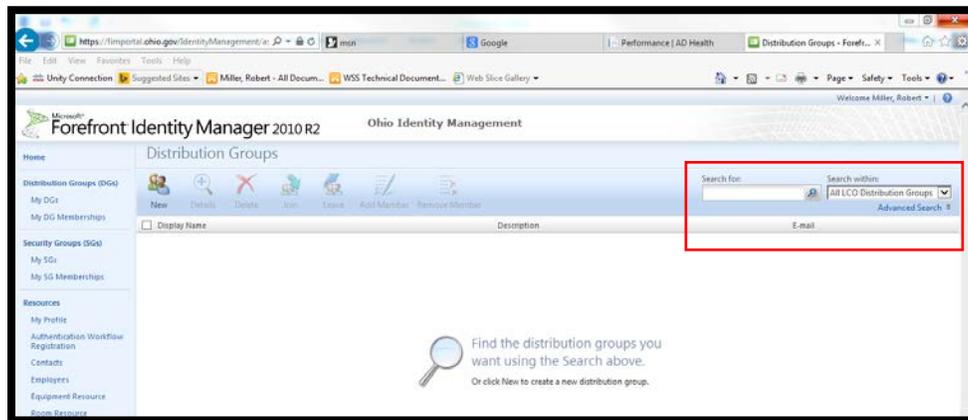
Search for:

Currently you can search by the following criteria:

- **Display Name**
- **Mail NickName** (Alias)
- **Wildcard search option:** FIMPortal is a XML based application the normal **“*”** for wild card is **“%”**, so a search of **%GROU%** will produce a list of groups with those letters together anywhere in the display or alias.

Search Within:

- Pull down with all relative group search scopes that your agency has access to use.
- Agency search scope is the default
- An **“All Distribution Groups”** option is available to all agencies; however this does not mean you will have to edit. It does mean you can add other agency groups to your groups.



ADVANCED SEARCH FUNCTION

Training Time: 5 minutes

As with criteria base groups we can search for groups using the advanced search function .

- Click **Advanced Search**

To return to the basic search;

- Click **Basic Search**

“Group” is already associated.

Also notice it has some basic values already selected – these are those attributes currently being used to create the search scope. You can use these values and add to them or remove and select your own. Use the “X” far right to remove.

To add additional statements;

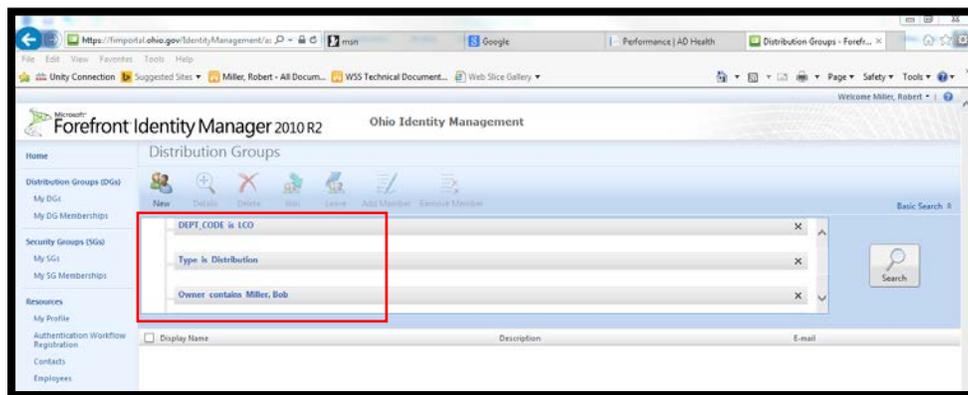
- Click the **“Add Statement”** option

A line will be inserted.

➤ Select **“Click to Select...”**

- **Logical** – depending on the attribute type appropriately choose the type of logic (is, is not, etc.)
- **Value** – value you are looking for in your search

The example below will find all agency **“LCO”** distribution groups that the Owner attribute contains Miller, Bob



MODIFYING DISTRIBUTION GROUPS

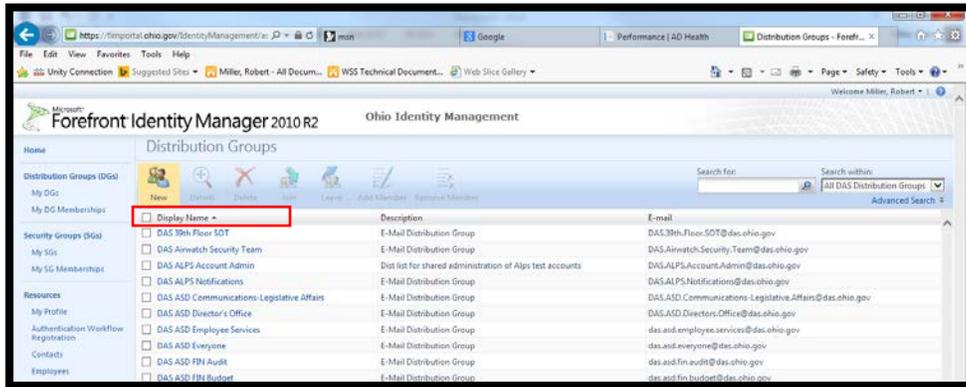
Training Time: 10 minutes

Managing Users

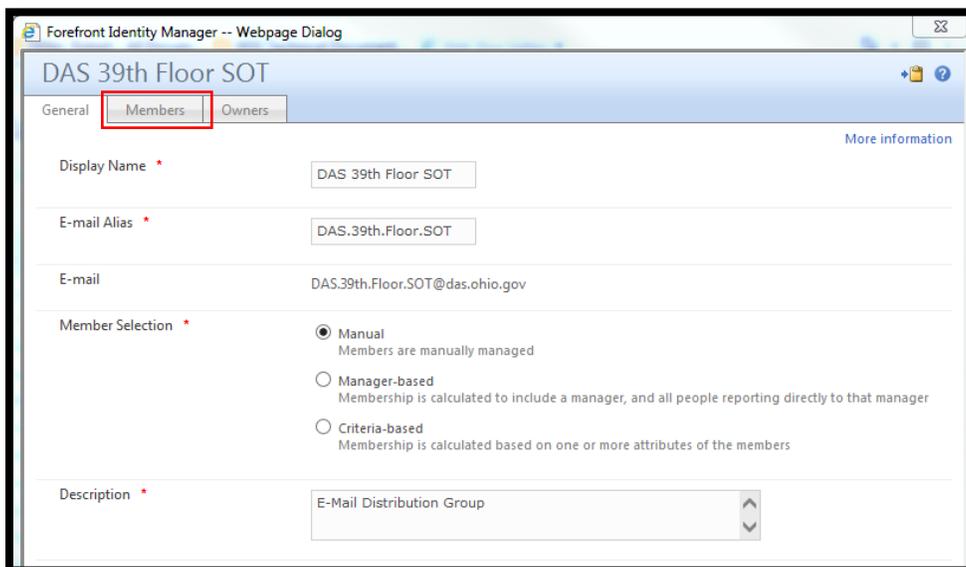
Any owner or co-owner can manage manually created distribution list membership by using FIM Portal.

After the group you are looking to manage has been searched and found;

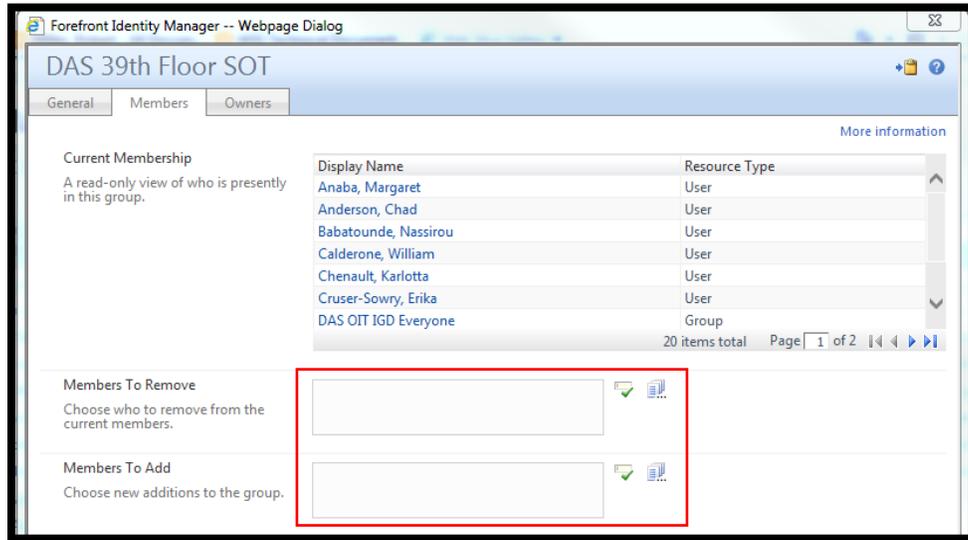
➤ Click on the display name of the group



- Click the Members tab



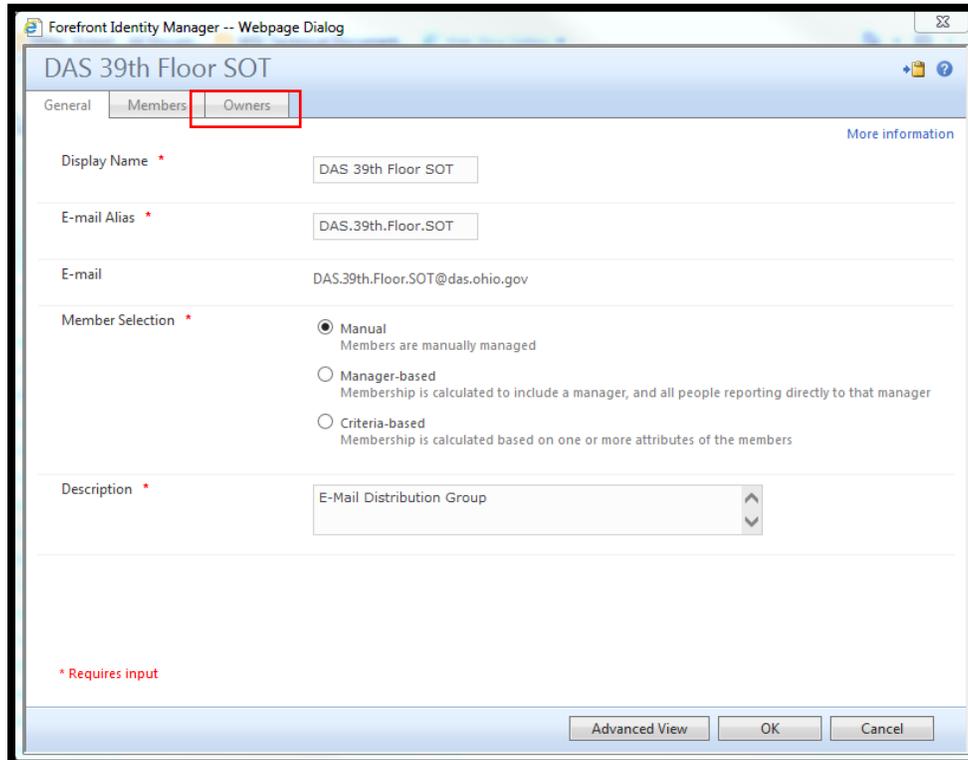
- Current membership is displayed; you cannot add or remove using this attribute.
- **“Members to Remove”** allows you to Remove members.
- The SharePoint picker limits the selection to only those users or groups that are members.
- **“Members to Add”** allows you to Add members
- This is a normal SharePoint picker and you can choose any group or user that is available through the Search option.



MANAGING OWNERS AND CO-OWNERS

After opening the group you want to edit;

- Choose the **Owner** tab



Owners and Co-Owners are managed in the attributes as presented.

Note: Displayed Owner can only contain a single user; however Owner and Co-Owners can be multiple. We strongly suggest you keep the Owner to a single user and use CO-Owner for all other users. The behavior in FIM Portal is different for these permissions and for Owner to function you must have FIM PORTAL admin rights.

MANAGING CRITERIA BASED DISTRIBUTION GROUPS

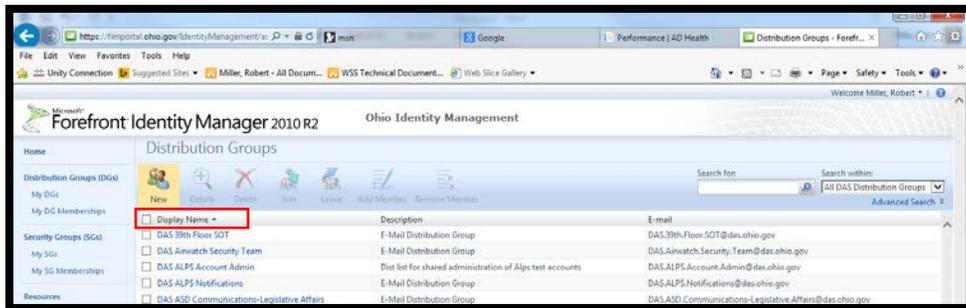
Training Time: 10 minutes

Managing Users

Any owner/co-owner can manage manually created distribution list membership by using FIM Portal.

After finding the searched group;

- Click on the display name of the group



Upon opening if the following is displayed;

- Choose Criteria Based

Forefront Identity Manager -- Webpage Dialog

ODH-AIIODH

General Members Owners More information

Display Name *

E-mail Alias *

E-mail

Member Selection *

Manual
Members are manually managed

Manager-based
Membership is calculated to include a manager, and all people reporting directly to that manager

Criteria-based
Membership is calculated based on one or more attributes of the members

Description *

* Requires input
Static group has a filter.

Advanced View OK Cancel

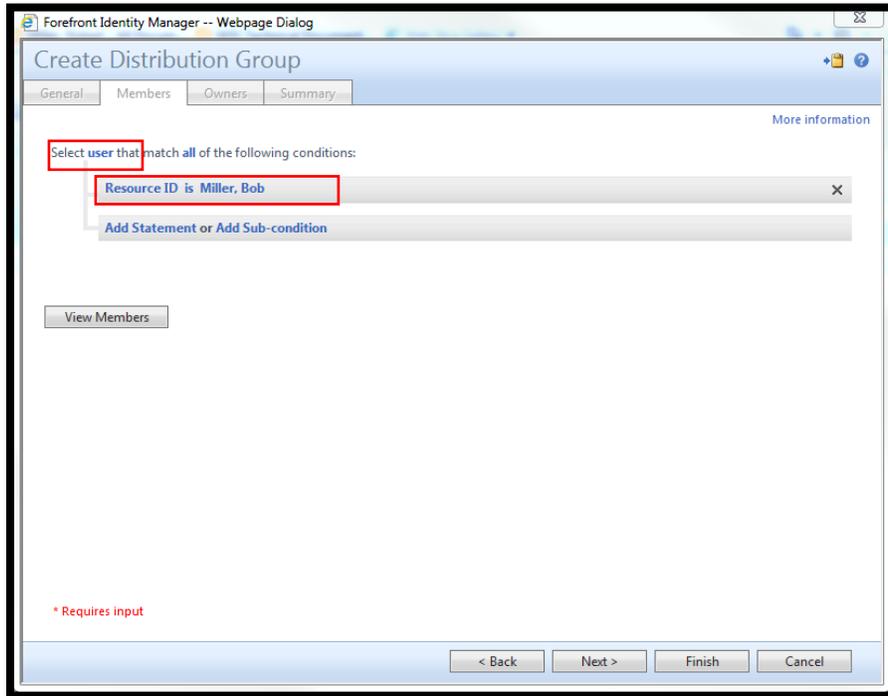
Criteria Selection

- Choose User from the drop down list
- Remove the preselected option of **Resource ID**
- Click **Add Statement**

A drop down with a list of all attributes will be presented.

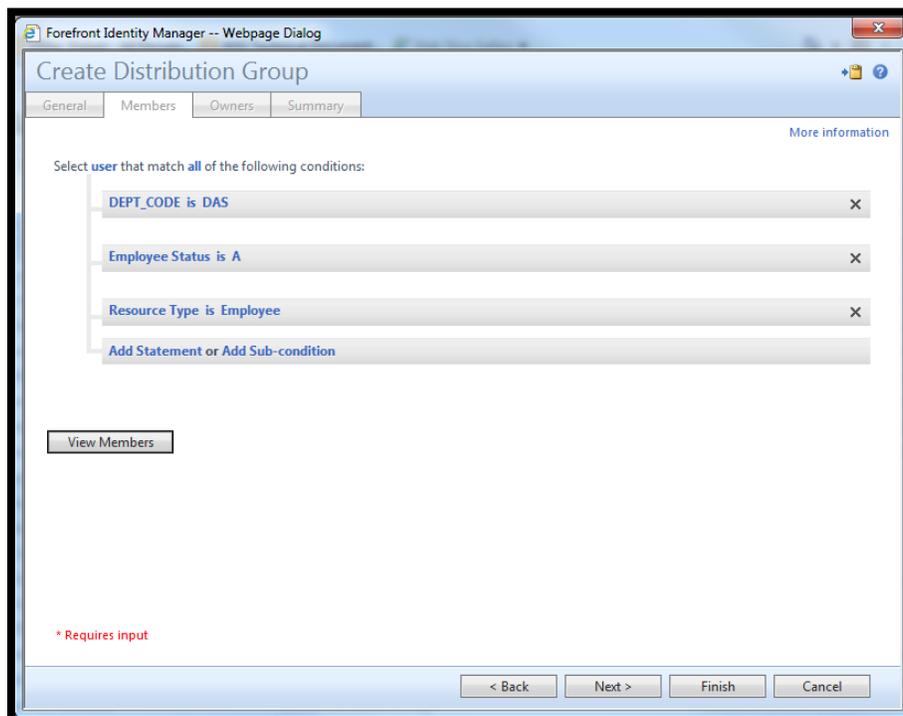
Common attributes to use include:

- **Account Name** – (EmployeeID – OAKS ID etc.)
- **DEPT_CODE** – controls all aspects of what data is available to you
- **Employee Status** – Active (A) and Inactive (I)
- **DL Condition 1,2 and 3** – agency Portal admin defined criteria
- **DEPTCODE 2 and 4** – agency HR defined criteria
- **DisplayName** – lastname, firstname
- **Job Title**
- **Logical** – depending on the attribute type appropriately choose the type of logic (is, is not, etc.)
- **Value** – value you are looking for in your search



The example below produces a distribution group in active directory with all active DAS employees.

Note: As people are moved from Active and Inactive they would either be added or removed.



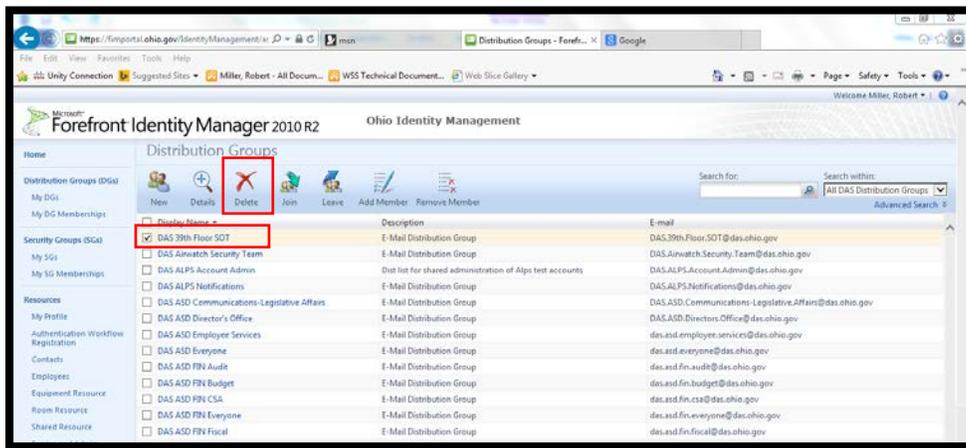
DELETING DISTRIBUTION GROUPS

Training Time: 5 minutes

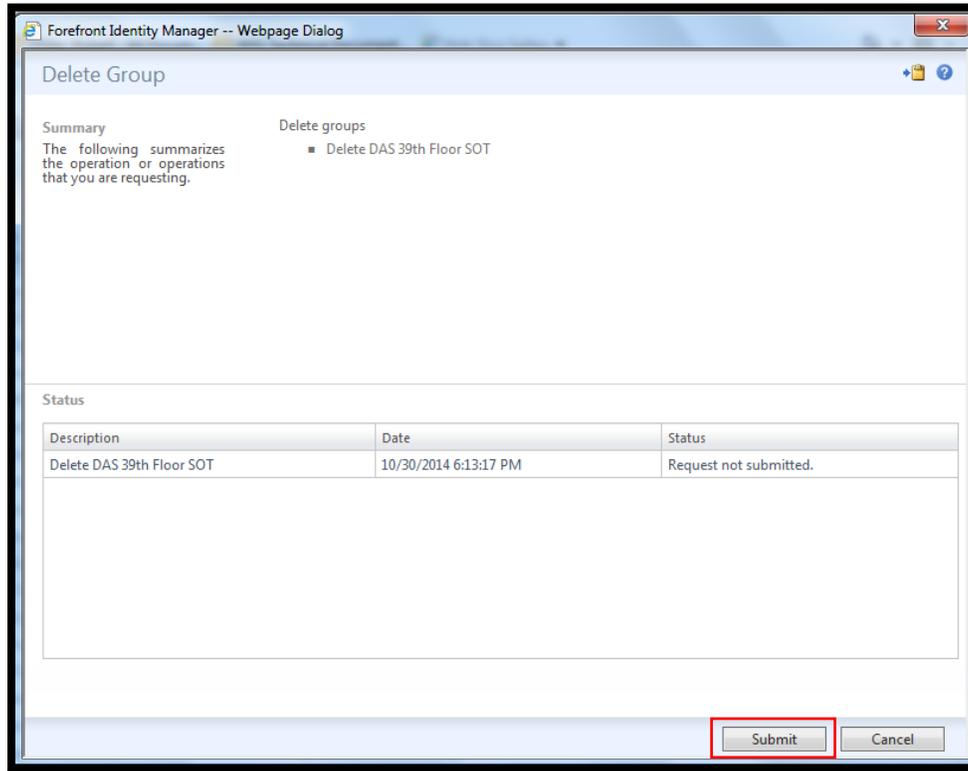
FIM Portal Administrators have the ability to delete distribution groups that have the agencies OAKS department code.

Deleting Distribution Groups:

- Choose the group or groups by first searching for the groups. (see searching for groups)
- Select the checkbox next to the group name
- Choose **Delete** from the buttons at the top of the work area.



- Confirm the deletion



MODULE TWO REVIEW

To create a group of all employees and contractors who work at a particular address you would use which type of group?

Answer Criteria

Explain what the criteria would be: DEPT_CODE = Agency; EMPLOYEE STATUS = "A" and ADDRESS = the address

Are you capable of deleting distribution groups for another agency?

Answer: No

STUDENT EXERCISES

- Create a manual based distribution group
- Create a criteria based distribution group
- Delete the two groups you created

MODULE THREE - SECURITY GROUPS

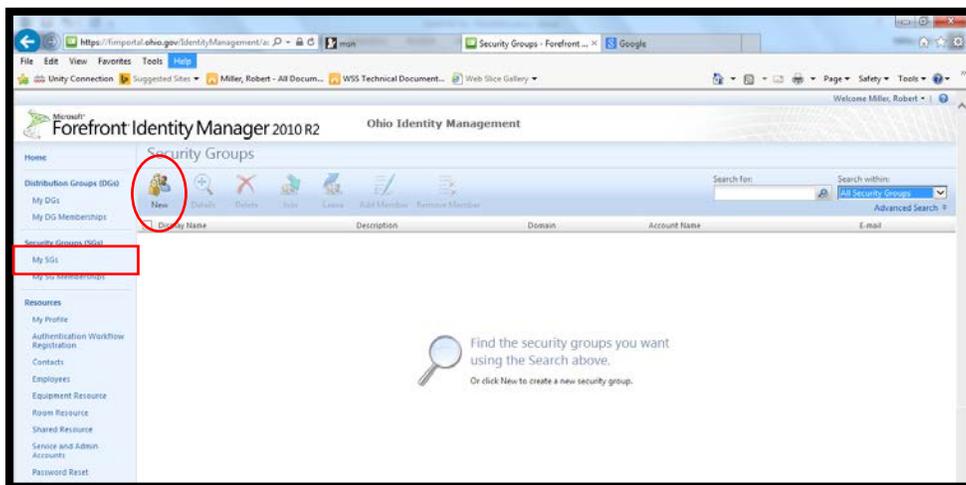
CREATE NEW SECURITY GROUPS

Training time: 10 minutes

- Create new manually populated security groups

Rules to creating new security groups with manually based users:

- All users or groups you intend to include in the group must be present in FIM Portal.
 - All normal active directory group rules apply. Example you cannot add a domain local mail enabled security group to a global group because active directory does not allow this to occur.
 - The group mail alias (nickname) cannot contain invalid characters. Examples of invalid characters are spaces; backslashes; commas. The best solution is to use the common characters such as a period and/or dashes. This is only valid if Mail Enabled is selected.
 - The agency OAKS code will precede the group name upon creation; however this can be changed after the name has been updated.
 - Attribute with a * next to the name are required attributes
 - Security groups are created through a synchronization process and can take 30 to 60 minutes to be available in active directory, for these groups to be active in Office365 it can take an additional 30 – 60 minutes
- Begin creating a new security list by selecting Security Groups from the Navigation panel.



- Select **New** on the panel

Enter the following information:

- Display Name:

Note: Your agency OAKS code will be inserted automatically upon creation. You can change this once the OAKS code appears by editing the display name.

- **E-Mail Enabled:** If e-mail enabled is selected E-mail Alias will appear
- **E-mail Alias:** This requires proper formatting.
- **Domain:** FIM Portal is capable of creating groups in ID.OHIO.GOV and CSS.IS.OHIO.GOV domains
- **Account Name:** This is the active directory samAccountName (25 characters maximum)
- **Scope:** Choose group type (Universal; Global; Domain Local) (Note: if creating a mail enabled security group choose Universal)
- **Member Selection:** This will be manual.
- **Application Code:** Choose email from the pull down list.
- **Alternate Agency Code:** Use this field to assign another agency OAKS code to your group
- **Description:** Enter a description.

Forefront Identity Manager -- Webpage Dialog
http://fimportal.idqa.ohio.gov/identitymanagement/asp/COMMON/popup.aspx

Create Security Group

General Members Owners Summary [More information](#)

Display Name *

IBM Group
Group is IBM

E-mail Enabled Enabled
Enable e-mail on a security group

Domain * IDQA

Account Name *

Scope * Universal
Secures resources in a forest. Members must be in the same forest.

Member Selection * Manual
Members are manually managed
 Manager-based
Membership is calculated to include a manager, and all people reporting directly to that manager
 Criteria-based
Membership is calculated based on one or more attributes of the members

Application Code *
Only applies to Security Groups

Alternate Agency Code

Description *

* Requires input

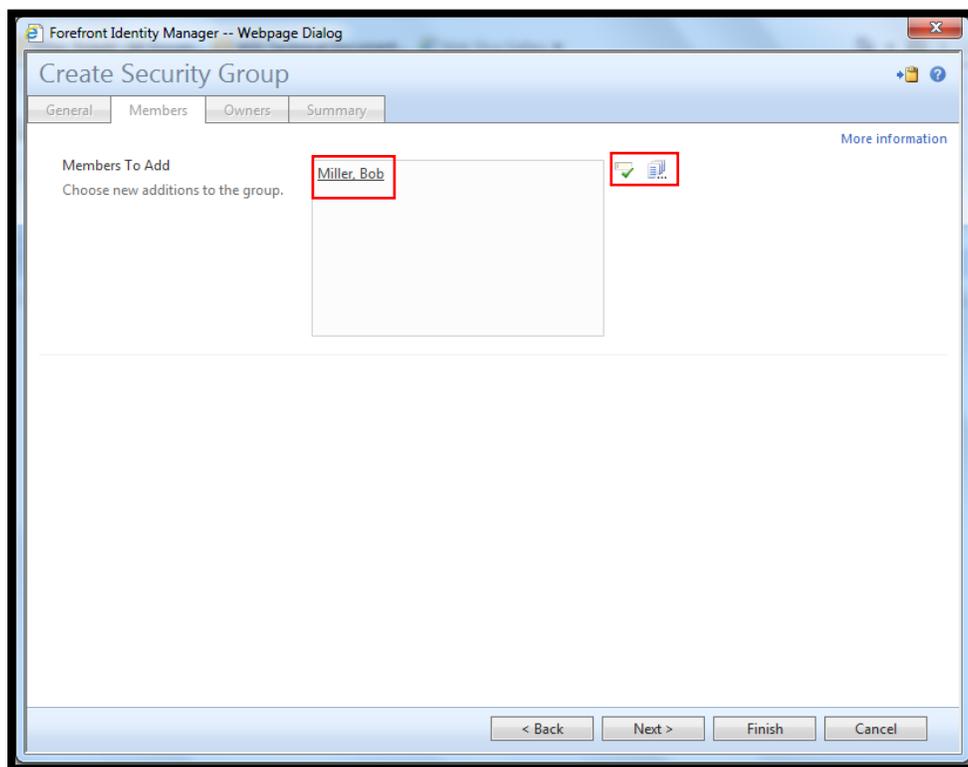
< Back Next > Finish Cancel

Members

- Enter members

The creator of the group will be automatically populated in the **Members to Add** attribute. Remove if needed. Also notice these are SharePoint picker buttons to the right. Underlining SharePoint controls the selection of the users.

- Use the people picker to find your group members.



Owners and Co-Owners

The creator of the group is automatically added to the owner and displayed owner attributes; this can be changed as required; however; all FIM Portal administrators have rights to all agency groups.

Note: The recommendation is to leave this attribute alone and add all additional owners in the co-owners attribute. All co-owners have rights to change group membership in FIM Portal. We strongly suggest you keep the Owner to a single user and use Co-Owner for all other users. The behavior in FIM Portal is different for these permissions and for Owner to function you must have FIM PORTAL admin rights.

Join Restrictions

This is not enforced.

Forefront Identity Manager -- Webpage Dialog

Create Security Group

General Members Owners Summary

More information

Owner * Miller, Bob

Co-Owners
Enter Users who have rights to modify members

Displayed Owner *
The group owner who will be displayed in Outlook or other systems which show only one owner for a group Miller, Bob

Join Restriction *
 Owner approval required
 A user will become a member of the group only after the group owner has approved the join request.
 None
 Any user can become a member of the group.

* Requires input

< Back Next > Finish Cancel

CREATE DYNAMIC SECURITY GROUPS

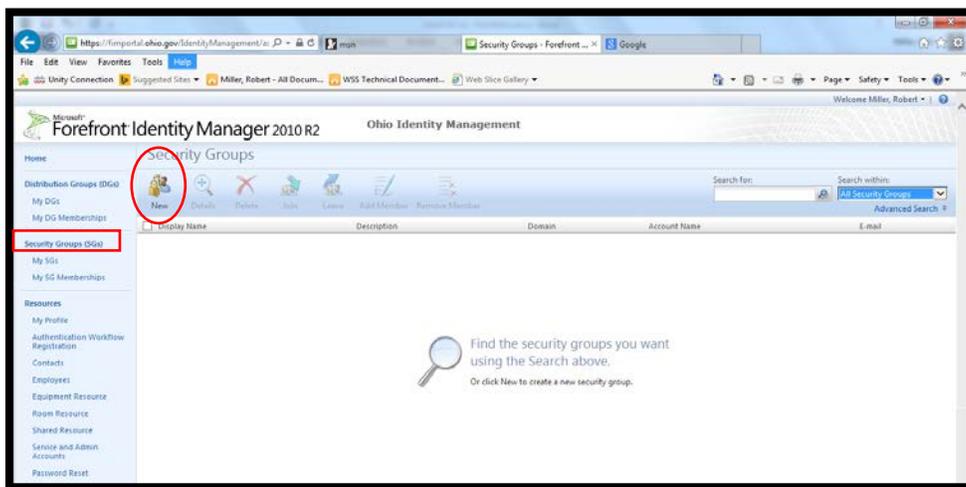
Training Time: 10 minutes

➤ Create new criteria based security group

Rules to creating new security groups with criteria based users:

- All users or groups you intend to include in the group must be present in FIM Portal.
- All normal active directory group rules apply. Example you cannot add a domain local mail enabled security group to a global group because active directory does not allow this to occur.
- The group mail alias (nickname) cannot contain invalid characters. Examples of invalid characters are spaces; backslashes; commas. The best solution is to use the common characters such as a period and/or dashes. This is only valid if Mail Enabled is selected.
- The agency OAKS code will precede the group name upon creation; however this can be changed after the name has been updated.
- Attribute with a * next to the name are required attributes

- You cannot mix criteria based groups and criteria user when building your criteria selection. It must be one or the other.
 - Distribution groups are created through a synchronization process and can take 30 to 60 minutes to be available in active directory, for these groups to be active in Office365 it can take an additional 30 – 60 minutes
 - Criteria based groups are only criteria based within FIM Portal, exchange will contain the actual user accounts when the groups synchronize from Portal to AD and Office365
 - You cannot mix manually selected membership and criteria in the same group
- Begin creating a new distribution list by selecting Distribution Groups from the Navigation panel.



- Select **New** on the panel
- Enter the following information:

- **Display Name:**

Note: Your agency OAKS code will be inserted automatically upon creation. You can change this once the OAKS code appears by editing the display name.

- **E-Mail Enabled:** If e-mail enabled is selected E-mail Alias will appear
- **E-mail Alias:** This requires proper formatting.
- **Domain:** FIM Portal is capable of creating groups in ID.OHIO.GOV and CSS.IS.OHIO.GOV domains
- **Account Name:** This is the active directory samAccountName (25 characters maximum)

- **Scope:** Choose group type (Universal; Global; Domain Local) (Note: if creating a mail enabled security group choose Universal)
- **Member Selection:** This will be manual.
- **Application Code:** Choose email from the pull down list.
- **Alternate Agency Code:** Use this field to assign another agency OAKS code to your group
- **Description:** Enter a description.

The screenshot shows the 'Create Security Group' interface in Forefront Identity Manager. The 'Member Selection' section is highlighted in yellow, and the 'Criteria-based' radio button is selected and enclosed in a red box. The 'Domain' dropdown is set to 'IDQA' and the 'Scope' dropdown is set to 'Universal'. The 'Application Code' and 'Alternate Agency Code' dropdowns are empty. The 'Description' field is also empty. The 'IBM Group' checkbox is unchecked, and the 'E-mail Enabled' checkbox is checked. The 'Display Name' field is empty. The 'Account Name' field is empty. The 'More information' link is visible in the top right corner. The bottom of the page has navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. A red asterisk indicates required input fields.

CRITERIA SELECTION

- Choose User from the drop down list
- Remove the preselected option of **Resource ID**
- Click **Add Statement**

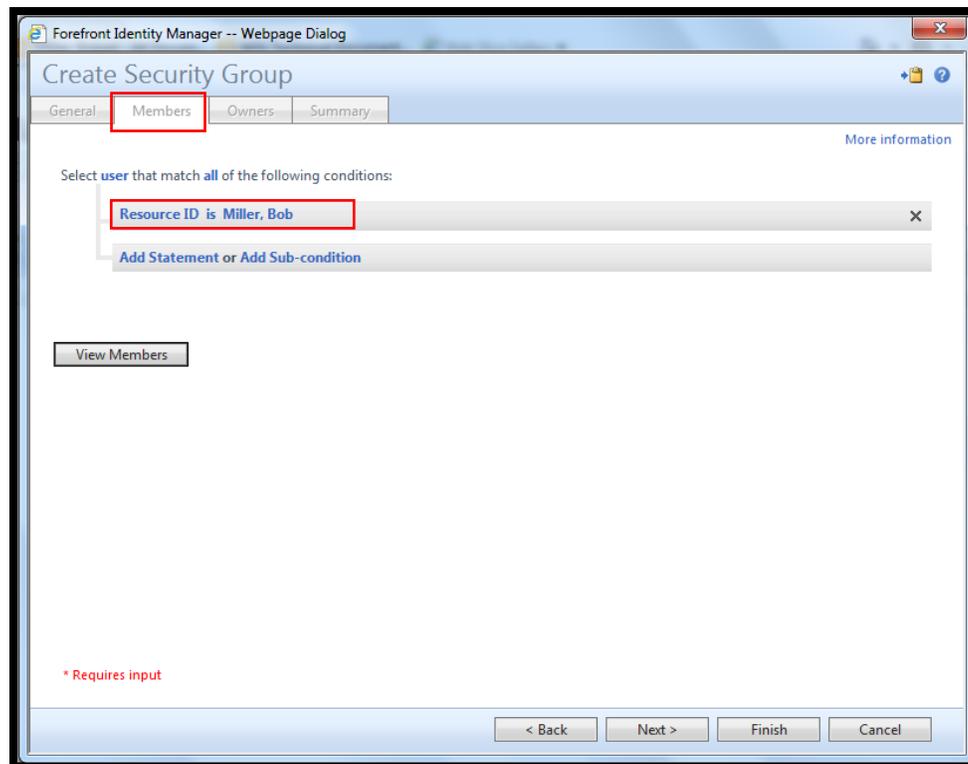
A line will be inserted.

- Click to select....

A drop down will be presented.

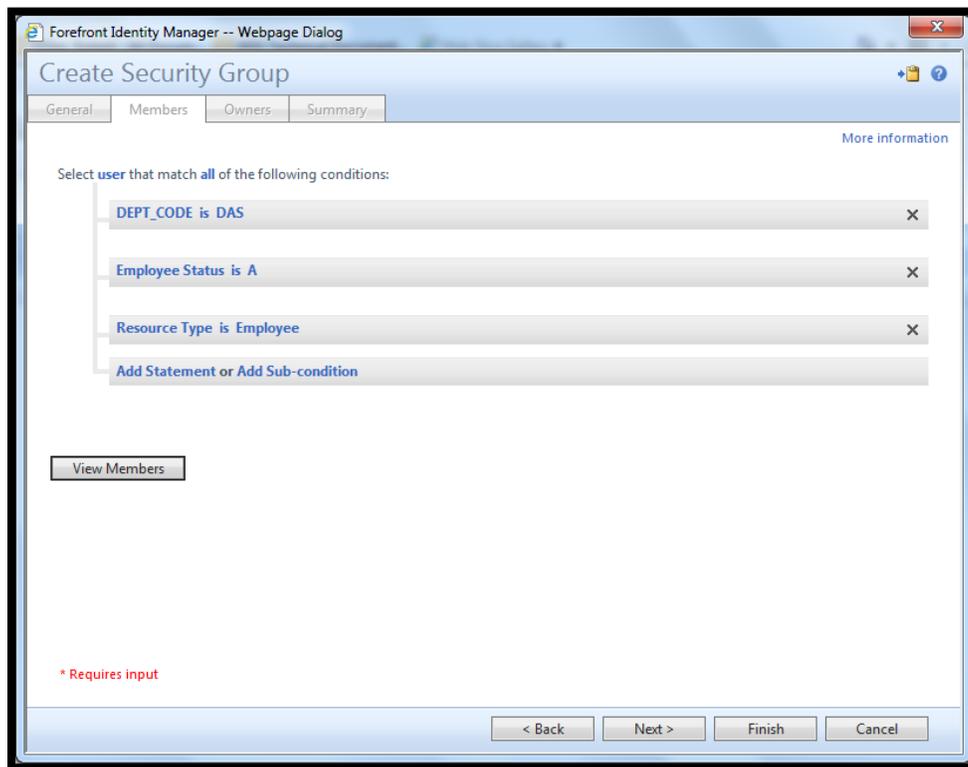
A list of all attribute will be presented; some common attributes to use include:

- **Account Name** – (EmployeeID – OAKS ID etc.)
- **DEPT_CODE** – controls all aspects of what data is available to you
- **Employee Status** – Active (A) and Inactive (I)
- **DL Condition 1, 2 and 3** – agency Portal admin defined criteria
- **DEPTCODE 2 and 4** – agency HR defined criteria
- **DisplayName** – lastname, firstname
- Job Title
- **Logical** – depending on the attribute type appropriately choose the type of logic (is, is not, etc.)
- **Value** – value you are looking for in your search



The following example would produce a security group in active directory with all active DAS employees.

Note: As people are moved from Active and Inactive they would either be added or removed.



Owners and Co-Owners

The creator of the group is automatically added to the owner and displayed owner attributes; this can be changed as required; however; all FIM Portal administrators have rights to all agency groups.

Note: The recommendation is to leave this attribute alone and add all additional owners in the co-owners attribute. All co-owners have rights to change group membership in FIM Portal. We strongly suggest you keep the Owner to a single user and use CO-Owner for all other users. The behavior in FIM Portal is different for these permissions and for Owner to function you must have FIM PORTAL admin rights.

Join Restrictions

This is not enforced.

FINDING YOUR AGENCY SECURITY GROUPS

Training Time: 5 minutes

From the security option – notice the **“Search for”** and **“Search within”** options

These are the two options available to search for distribution groups

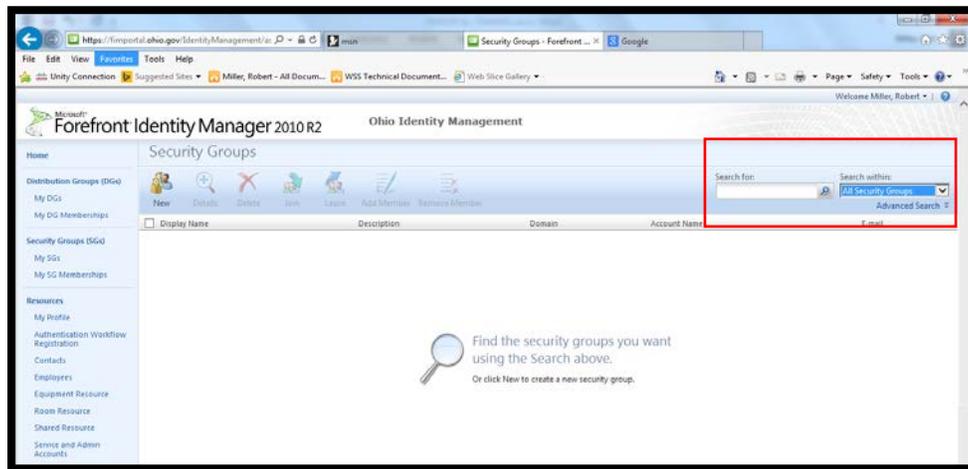
Search for:

Currently you can search by the following criteria

- **Display Name**
- **Mail NickName** (Alias)
- **Wildcard search option:** FIMPortal is a XML based application the normal **“*”** for wild card is **“%”**, so a search of **%GROU%** will produce a list of groups with those letters together anywhere in the display or alias.

Search Within:

- Drop down with all relative group search scopes that your agency has access to use.
- Agency search scope is the default
- An **“All Distribution Groups”** option is available to all agencies; however this does not mean you will have to edit. It does mean you can add other agency groups to your groups.



ADVANCED SEARCH FUNCTION

Training Time: 5 minutes

As with criteria base groups we can search for groups using the advanced search function

- Click **Advanced Search**

To return to the basic search;

- Choose **Basic Search**

Select has **“group”** already associated and it has some basic values already selected – these are those attributes currently being used to create the search scope. You can use these values and add to them or remove and select your own. Use the “X” far right to remove.

To add additional statements;

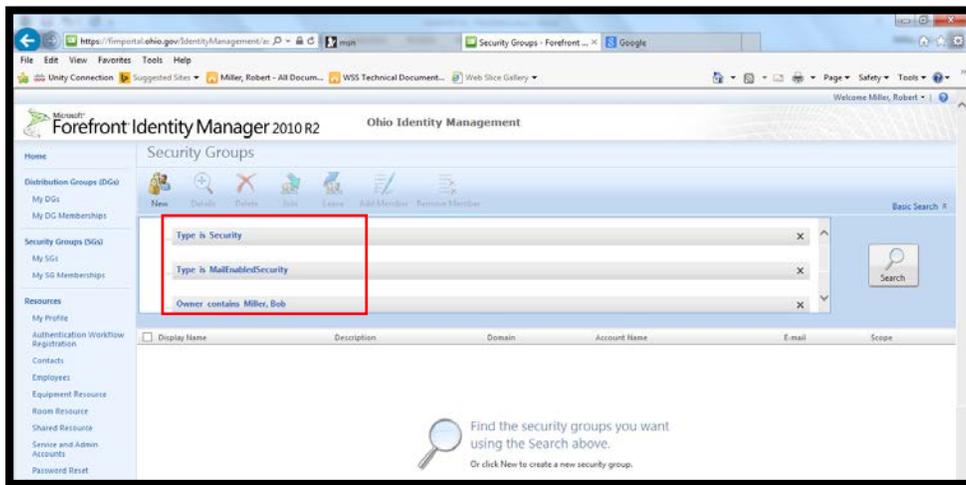
- Click the **“Add Statement”** option

A line will be inserted.

➤ Select **“Click to Select...”**

- **Logical** – depending on the attribute type appropriately choose the type of logic (is, is not, etc.)
- **Value** – value you are looking for in your search

The example below will find all agency **“LCO”** distribution groups that the Owner attribute contains Miller, Bob



MODIFYING SECURITY GROUPS

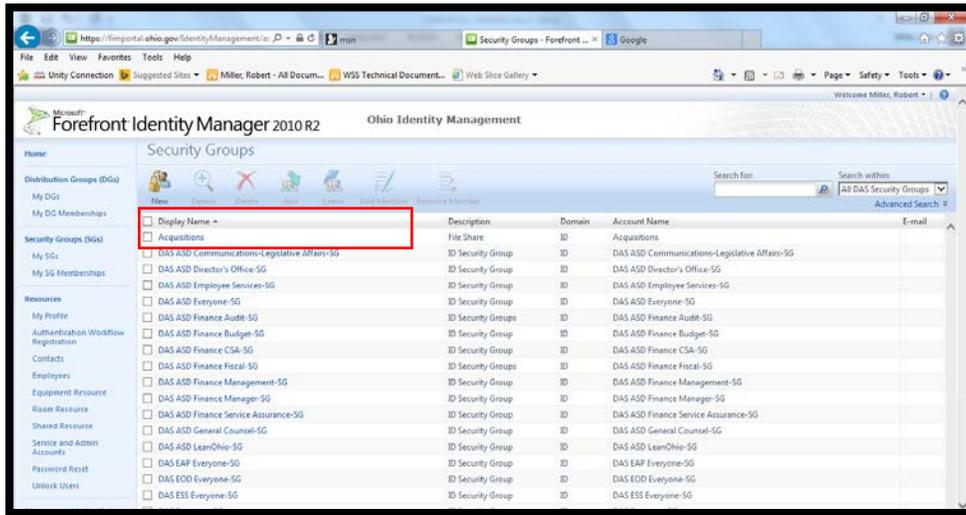
Training Time: 10 minutes

Managing Users

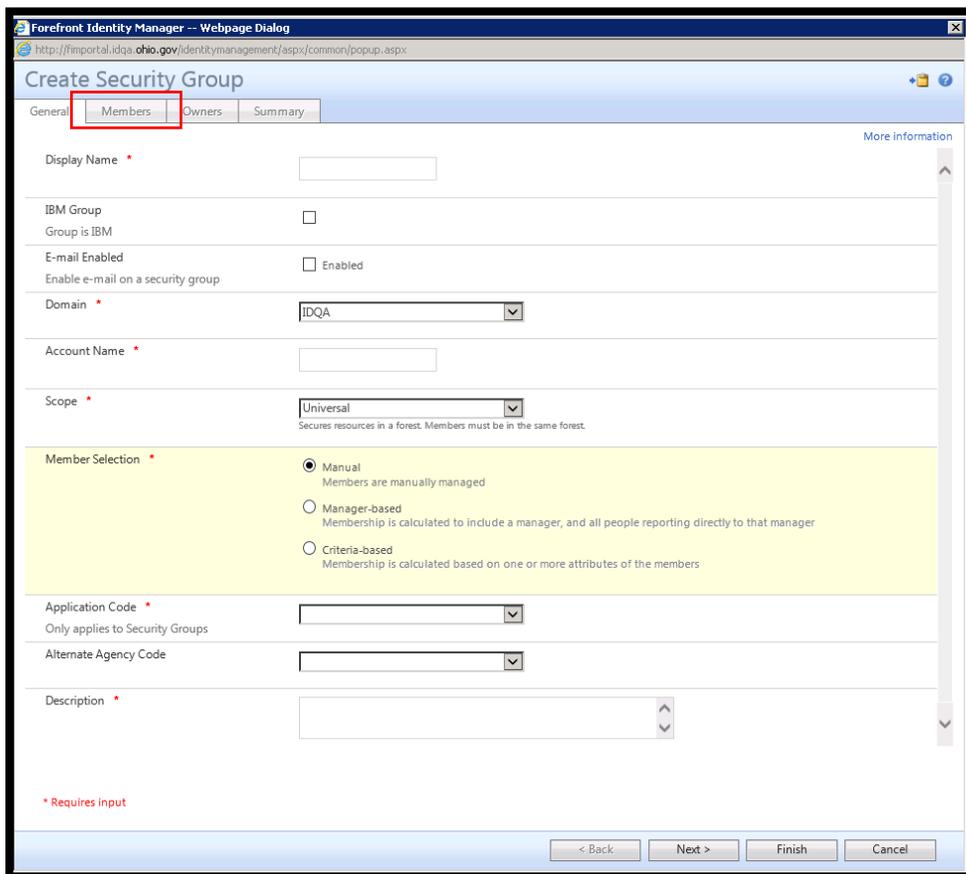
Any owner or co-owner can manage manually created security groups membership by using FIM Portal.

After the group you are looking to manage has been searched and found;

- Click on the display name of the group

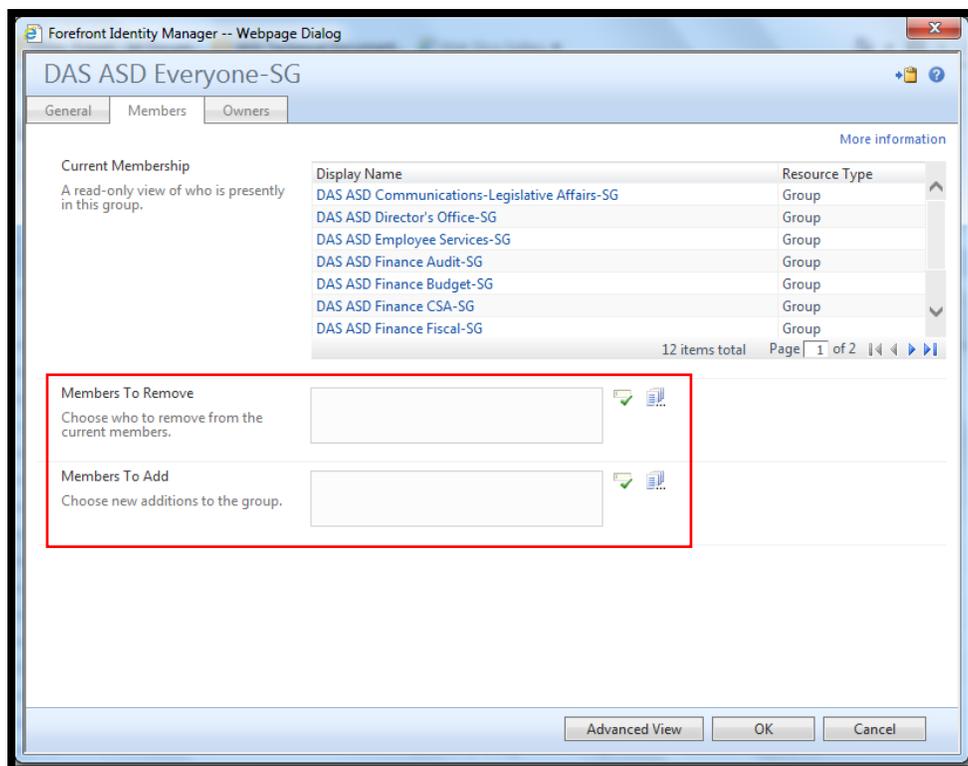


➤ Click the Members tab



The current membership is displayed; you cannot add or remove using this attribute.

- **“Members to Remove”** allows you to Remove members.
- The SharePoint picker limits the selection to only those users or groups that are members.
- **“Members to Add”** allows you to Add members
- This is a normal SharePoint picker and you can choose any group or user that is available through the Search option.



MANAGING OWNERS AND CO-OWNERS

After opening the group;

- Choose the Owner tab

The screenshot shows the 'Create Security Group' interface in the Forefront Identity Manager web portal. The 'Owners' tab is selected and highlighted with a red box. The page contains several configuration fields and options:

- Display Name**: A text input field.
- IBM Group**: A checkbox labeled 'Group is IBM'.
- E-mail Enabled**: A checkbox labeled 'Enable e-mail on a security group'.
- Domain**: A dropdown menu with 'IDQA' selected.
- Account Name**: A text input field.
- Scope**: A dropdown menu with 'Universal' selected. Below it, a note reads: 'Secures resources in a forest. Members must be in the same forest.'
- Member Selection**: A section with three radio button options:
 - Manual**: Selected. Description: 'Members are manually managed.'
 - Manager-based**: Description: 'Membership is calculated to include a manager, and all people reporting directly to that manager.'
 - Criteria-based**: Description: 'Membership is calculated based on one or more attributes of the members.'
- Application Code**: A dropdown menu.
- Alternate Agency Code**: A dropdown menu.
- Description**: A text area.

At the bottom of the page, there are four navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. A red asterisk icon is visible near the bottom left, indicating required input fields.

Owners and Co-Owners are managed in the attributes as presented.

Note: Displayed Owner can only contain a single user; however Owner and Co-Owners can be multiple. We strongly suggest you keep the Owner to a single user and use CO-Owner for all other users. The behavior in FIM Portal is different for these permissions and for Owner to function you must have FIM PORTAL admin rights.

MANAGING CRITERIA BASED SECURITY GROUPS

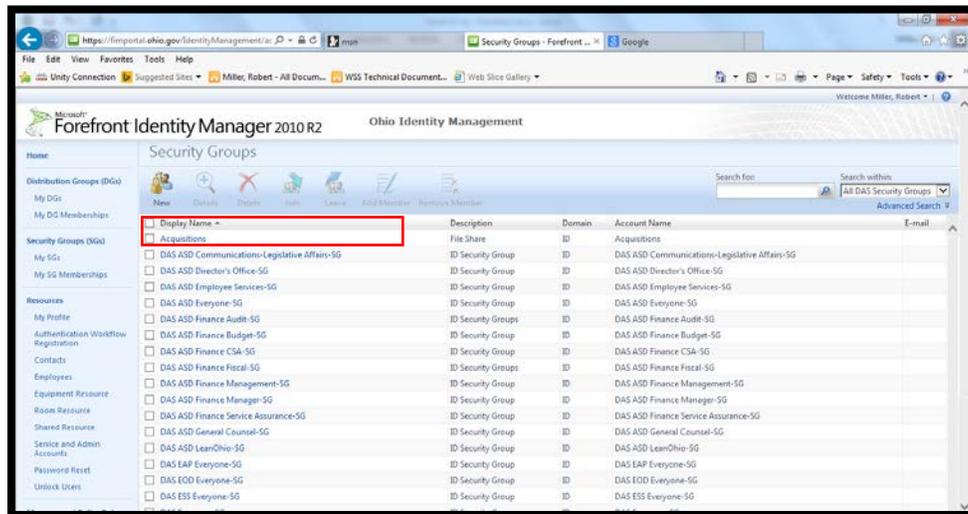
Training Time: 10 minutes

Managing Users

Any owner or co-owner can manage manually created security group membership by using FIM Portal.

After the group you are looking to manage has been searched and found;

- Click on the display name of the group



Upon opening if the following is displayed;

- Choose Criteria Based

The screenshot shows the 'Create Security Group' dialog in Forefront Identity Manager. The 'Member Selection' section is highlighted in yellow, and the 'Criteria-based' radio button is selected and enclosed in a red box. Below this, there is a red box containing the text '* Requires input'. The 'Domain' dropdown is set to 'IDQA'. At the bottom of the dialog, there are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

CRITERIA SELECTION

- Choose User from the drop down list
- Remove the preselected option of **Resource ID**
- Click **Add Statement**

A line will be inserted.

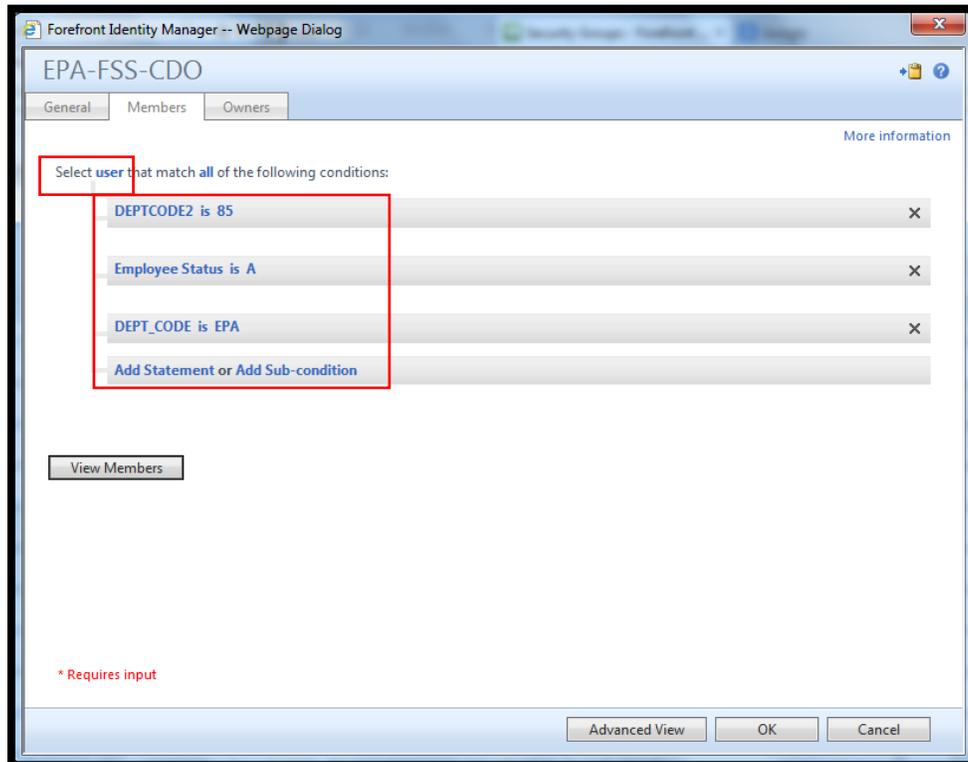
- Click to select....

A drop down will be presented with a list of all attributes.

Common attributes to use include:

- **Account Name** – (EmployeeID – OAKS ID etc.)
- **DEPT_CODE** – controls all aspects of what data is available to you
- **Employee Status** – Active (A) and Inactive (I)
- **DL Condition 1,2 and 3** – agency Portal admin defined criteria

- **DEPTCODE 2 and 4** – agency HR defined criteria
- **DisplayName** – lastname, firstname
- Job Title
- **Logical** – depending on the attribute type appropriately choose the type of logic (is, is not, etc.)
- **Value** – value you are looking for in your search



The example above would produce a security group in active directory with active EPA employees with DEPTCODE2 equal to 85.

Note: As people are moved from Active and Inactive they would either be added or removed.

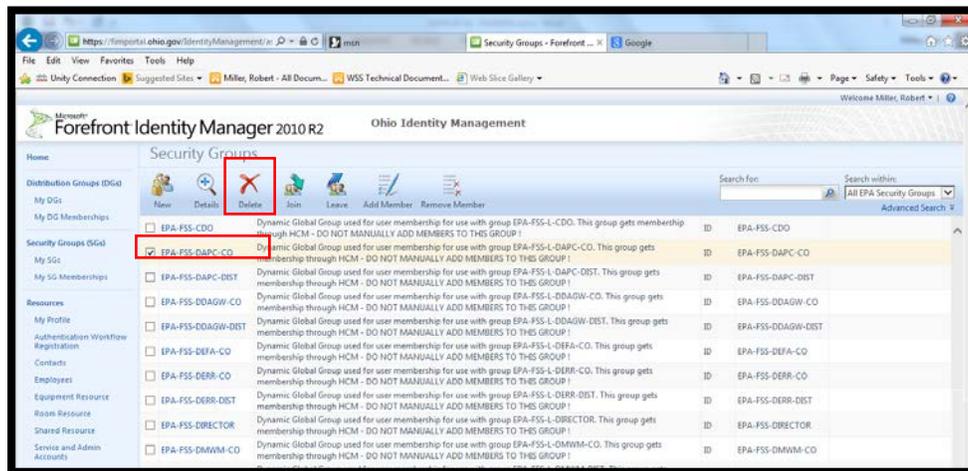
DELETING SECURITY GROUPS

Training Time: 5 minutes

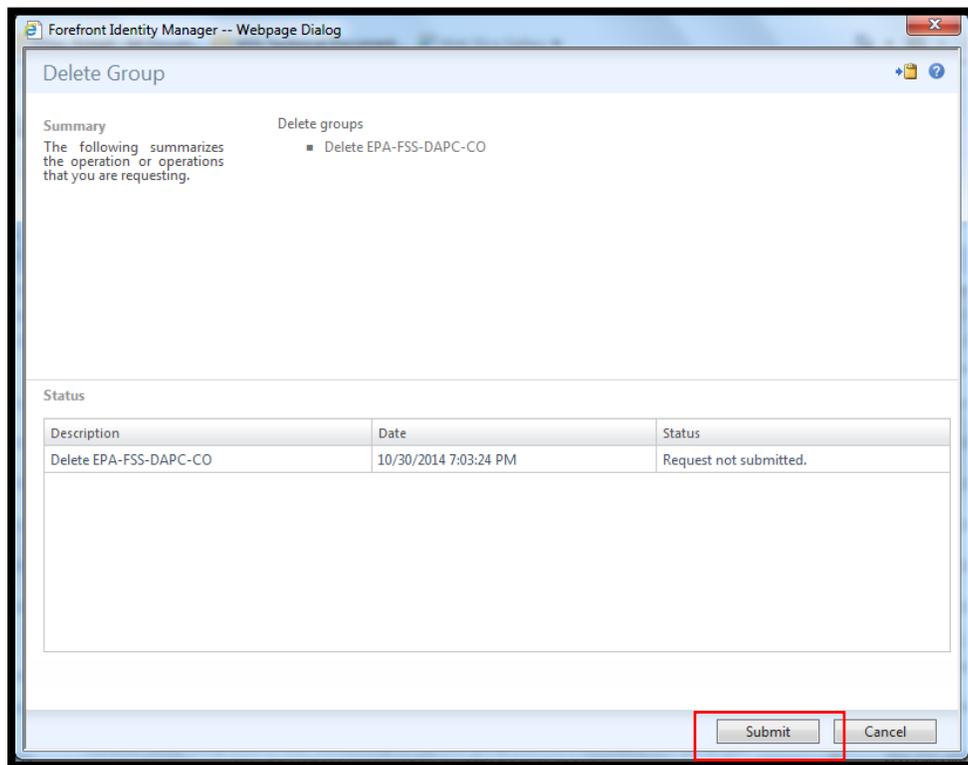
FIM Portal administrators have the ability to delete security groups that have the agencies OAKS department code.

Deleting Security Groups:

- Choose the group or groups by first searching for the groups. (See *Searching for Groups*)
- Select the checkbox next to the group name
- Choose **Delete** from the buttons at the top of the work area



- Confirm the deletion



MODULE THREE REVIEW

Can you create a mail enabled security group that contains both manual and criteria based information?

Answer: No

Do users with Co-owner rights have the ability to delete groups?

Answer: No

STUDENT EXERCISES

- Create a global scope manual based security group
- Create a domain local manual based security group – add the global group you just created to the domain local group as a member.

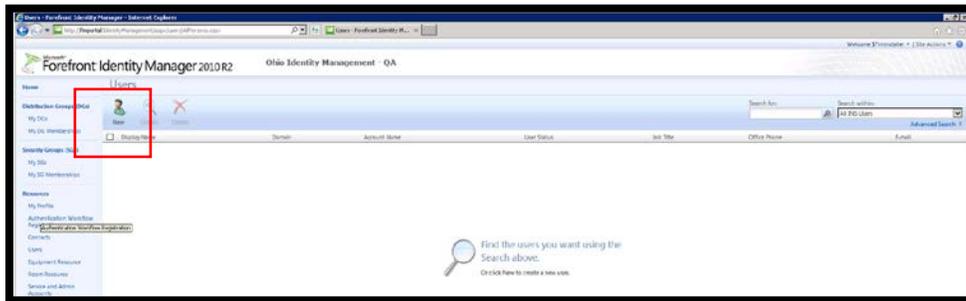
**MODULE FOUR - EMPLOYEE,
CONTRACTOR, COUNTY AND OTHER
USERS**

ADD NEW 5X USER ACCOUNTS

Training Time: 10 minutes

From the Users option;

- Click **Users**
- Click **New**



When creating a new user you will see the following form.

- Start by entering basic information concerning the user.

A screenshot of the "Create User" form in the Forefront Identity Manager portal. The form is titled "Create User" and has tabs for "General", "Work Info", "Contact Info", and "Summary". The "General" tab is active. The form contains the following fields:

- First Name * (Required): Text box containing "James".
- Last Name * (Required): Text box containing "Doolittle".
- Middle Name: Text box.
- Agency * (Required): Drop-down menu with "Administrative Services" selected. Below it, "DAS" is listed.
- Agency User Type * (Required): Drop-down menu with "Generic User" selected. Below it, "Generic" is listed.

At the bottom left, there is a red asterisk and the text "* Requires input". At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

General Tab

- **First Name** – this is the employee’s first name as it appears on his or hers W2 form. We will discuss changing the name later. Note: this is a required attribute.
- **Last Name** - this is the employee’s last name as it appears on his or hers W2 form. We will discuss changing the name later. Note: this is a required attribute.
- **Middle Name** - this is the employee’s middle name as it appears on his or hers W2 form. We will discuss changing the name later.
- **Display Name** – at the time of this writing the display name is a calculated value from last name, first name attributes. Enter the displayname as last name, comma, and first name. Note: this is a required attribute.
- **Agency Code** – from the drop down choose the agency the user account will be assigned. Note: this is a required attribute.
- **Agency User Type** – from the drop down menu select a user type of Business Partner (vendor), City Worker, County Worker, Federal Worker, or Generic User (those accounts need for non-people)

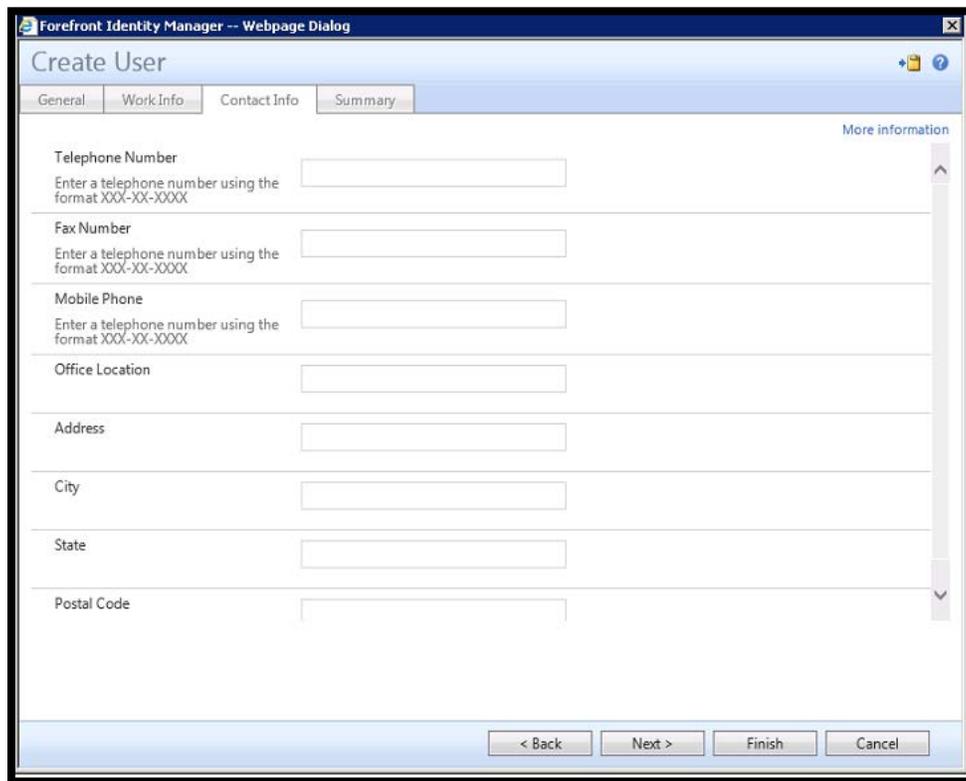
The screenshot shows a web browser window titled "Forefront Identity Manager -- Webpage Dialog" with a "Create User" page. The page has a navigation bar with tabs for "General", "Work Info", "Contact Info", and "Summary". The "General" tab is active. Below the tabs, there are several input fields with labels and instructions:

- Title**: Enter the peron's title
- Password Reset Date**: Enter a date for password reset - format is yyyy-mm-dd
- Password Reset Pin**: Enter a pin for password reset
- User Start Date**: Format as M/d/yyyy h:mm tt
- User End Date**: Format as M/d/yyyy h:mm tt

At the bottom left, there is a red asterisk and the text "* Requires input". At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Work Info Tab

- **Title** – Enter the user accounts working title.
- **Password Date** – Enter in a date that the user will use when requesting a password reset from the help desk. This is a required attribute.
- **Password PIN** – Enter in a PIN that the user will use when requesting a password reset from the help desk. This is a required attribute.
- **User Start Date** – enter in the date that the user will start working. Leave blank if not applicable.
- **User End Date** – enter in a date that the user will end working. Leave blank if not applicable.



The screenshot shows a web browser window titled "Forefront Identity Manager -- Webpage Dialog" with a "Create User" form. The form has four tabs: "General", "Work Info", "Contact Info", and "Summary". The "Work Info" tab is selected. The form contains several input fields with labels and instructions:

- Telephone Number**: Enter a telephone number using the format XXX-XX-XXXX
- Fax Number**: Enter a telephone number using the format XXX-XX-XXXX
- Mobile Phone**: Enter a telephone number using the format XXX-XX-XXXX
- Office Location**
- Address**
- City**
- State**
- Postal Code**

At the bottom of the form, there are four buttons: "< Back", "Next >", "Finish", and "Cancel". A "More information" link is visible on the right side of the form.

Contact Info Tab

- **Telephone Number** – enter in the user’s telephone number. Please remember this is the telephone number that will appear in the global address list for e-mail.
- **Fax Number** – enter in the user’s fax number, if any.
- **Mobile Phone** – enter the user mobile phone, if any. Please remember this will appear in the global address list in e-mail.
- **Office Location** – enter the user office location.
- **Address** – enter the user address.
- **City** – enter the user city.
- **State** – enter the user state.
- **Postal Code** – enter the user postal code.

Once completed;

- Click the **Finish** button and then
- Click submit

FINDING EMPLOYEE, CONTRACTOR, COUNTY WORKER AND OTHER ACCOUNTS

Training Time: 10 minutes

From the User option (if you select Resources or Employees you will be redirected to the same location) – notice the **“Search for”** and **“Search within”** options

These are the two options available to search for distribution groups

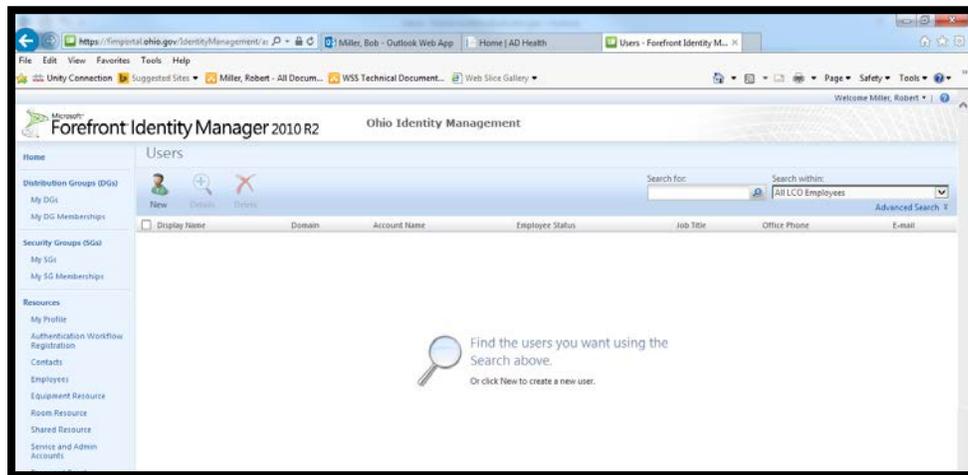
Search for:

Currently you can search by the following criteria

- Display Name
- EmployeeID (OAKS ID; State of Ohio User ID)
- Mail NickName (Alias)
- First Name
- Last Name
- **Wildcard search option:** FIMPortal is a XML based application the normal **“*”** for wild card is **“%”**, so a search of **%GROU%** will produce a list of groups with those letters together anywhere in the display or alias.

Search Within:

- Pull down with all relative group search scopes that your agency has access to use.
- Agency search scope is the default
- An **“All Users and All Employee”** option is available to all agencies; however this does not mean you will have to edit. It does mean you can add other agency groups to your groups.



ADVANCED SEARCH FUNCTION

Training Time: 5 minutes

To search for users using the Advanced Search function;

- Click Advanced Search (note to return to the basic search choose Basic Search)
- Notice this time that nothing has been preselected and in most cases an error appears (the error is a bug in Microsoft code and a fix is scheduled to be released in the future – you can remove the error by clicking search)
- Choose User

The Match is All or Any (the Any function is like an “or” statement) in fact you can get fairly complex by using the “any” function

To add additional statements;

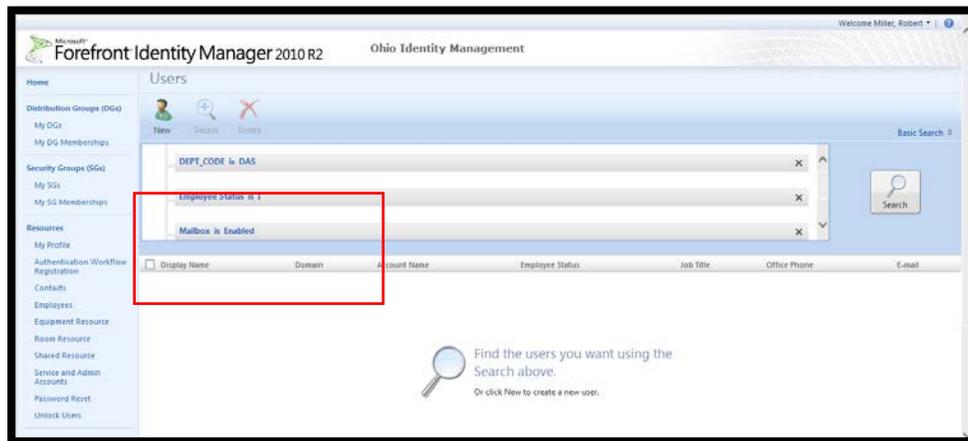
- Click the **Add Statement** option

A line will be inserted.

➤ Click to select....

- **Logical** – depending on the attribute type appropriately choose the type of logic (is, is not, etc.)
- **Value** – value you are looking for in your search

The example below will find all DAS users who are inactive but have an enabled mailbox, which allows you a quick way to find those mailboxes you are paying for that are not being used.



EDITING EMPLOYEE, CONTRACTOR AND COUNTY WORKER USER INFORMATION

Training Time: 30 minutes

The user environment is broken by where your mailbox is located. For all agencies other than JFS your mailboxes are or will be in Office365 and that is where we will focus our attention.

Let's start by taking a look at those attributes that are synchronized from OAKS or HCM. This is information that is entered by the agency human services division into the HCM system.

General Tab

- **First Name** – this is the employee's first name as it appears on his or hers W2 form. We will discuss changing the name later.
- **Last Name** - this is the employee's last name as it appears on his or hers W2 form. We will discuss changing the name later.
- **Middle Name** - this is the employee's middle name as it appears on his or hers W2 form. We will discuss changing the name later.

- Display Name – at the time of this writing the display name is a calculated value from last name, first name attributes
- Account Name – the person's State of Ohio User ID

The screenshot shows the 'Forefront Identity Manager -- Webpage Dialog' window for user 'Boyd, Bill'. The 'General' tab is selected, displaying the following information:

- Photo:** Active Directory Photo. A placeholder image is shown with the text 'No photo specified.' and buttons for 'Browse...' and 'Clear'.
- IBM Employee:** A checkbox labeled 'Employee is IBM' which is currently unchecked.
- First Name:** Text box containing 'Bill'.
- Last Name:** Text box containing 'Boyd'.
- Middle Name:** Text box containing 'J'.
- Display Name:** Text box containing 'Boyd, Bill'.
- Account Name:** Text box containing '80041324'.
- Oaks ID:** (Label visible below the Account Name field).

At the bottom of the dialog, there are buttons for 'Advanced View', 'OK', and 'Cancel'.

Work Info Tab

- **Employee Type** - Employee, Contingent (contractor), County, or Generic (this attribute has been removed from display)
- **Job Title** – Official job title
- **Department** – Users associated department (this is an OAKS code and it is not always a representation of the department code)
- **Search Criteria One** – agency administrator controlled, allows for dynamic groups or filtering
- **Search Criteria Two** – agency administrator controlled, allows for dynamic groups or filtering
- **Search Criteria Three** – agency administrator controlled, allows for dynamic groups or filtering
- **Search Criteria Taxation** – taxation agency administrator controlled, allows for dynamic groups or filtering
- **Search Criteria Four** – agency HR controlled
- **Search Criteria Five** – agency HR controlled
- **Employee ID** – State of Ohio User ID

- **User Home Directory** – based on active directory home directory attribute – allows agency admin the ability to assign a home director via active directory
- **User Home Drive** – based on active directory home directory attribute – allows agency admin the ability to assign a home drive via active directory
- **Manager** – allows for a manager to be entered (HR sync dependent)
- **Assistant** - allows for an assistant to be entered (HR sync dependent)
- **Agency Admin** – designates the person as a FIM Portal admin
- **Helpdesk Admin** – designates the person as an agency password manager
- **Password Date*** – used exclusively when a user accounts is created in FIM Portal – this is viewable only by the designated portal administrator for the agency that the account was created. Enter a date that will be used for password reset functionality.
- **Password Pin*** – used exclusively when a user accounts is created in FIM Portal – this is viewable only by the designated portal administrator for the agency that the account was created. Enter a four digit pin that will be used for password reset functionality.
- **User Status*** - used exclusively when a user accounts is created in FIM Portal – this is viewable only by the designated portal administrator for the agency that the account was created. Enter an “A” for active and an “I” for Inactive. Enables and disables a user account.

***Note:** Password Date, Password Pin, and User Status attributes will not be seen if the user was not created in FIM Portal.

The screenshot shows the 'Forefront Identity Manager -- Webpage Dialog' for user 'Starr, John'. The dialog has several tabs: General, Work Info, Contact Info, Account Info, Mailbox Maintenance, Mailbox Delegates, Mailbox Features, MITS Access Control, and Provisioning. The 'Contact Info' tab is selected. The user's name is 'Starr, John'. Below the tabs, there are several sections of user attributes:

- User Type:** User Resource Type
- Job Title:** Test User
- Department:** DAS
- Agency Code of User:** DAS
- Search Criteria One:** Dynamic Group Search Criteria
- Search Criteria Two:** Dynamic Group Search Criteria
- Search Criteria Three:** Dynamic Group Search Criteria
- DEPTCODE2:** Oaqs Source - Entered by HR
- DEPTCODE4:** Oaqs Source - Entered by HR
- User ID:** 58000005
- State of Ohio User ID:** 58000005
- User Home Directory:**
- User Home Drive:**
- Manager:**
- Assistant:**
- Agency Admin:** Agency Administrator Indicator (checkbox)

Helpdesk Admin

Helpdesk Administrator Indicator

Password Last Set 12/28/2015 1:09:07 PM
Date the password was last reset Format as M/d/yyyy h:mm tt

Employee Status
Enter A for Active (enabled) and I for Inactive (Disabled) - Ss User's created in FIM Portal

Disable User Access
Disables account from Office 365 - Local Ss User Accounts set Inactive

OK Cancel

Contact Info Tab

Office Phone – employee updated on the MyOhio website

- Office Location
- Address
- Address Line 2
- City
- State
- Postal Code

Forefront Identity Manager – Webpage Dialog

https://fimportal.ohio.gov/identitymanagement/aspx/common/popup.aspx

Miller, Bob

General Work Info Contact Info Exchange Online Local Mailbox General Local Lync Provisioning

More information

Office Phone 614-914-4202
Enter as XXX-XXX-XXXX

Fax
Enter as XXX-XXX-XXXX

Mobile Phone 614-307-9788
Enter as XXX-XXX-XXXX

Office Location SOCC03

Address Line One

Address Line Two 1320 Arthur E Adams Dr
Enter the person's address information

City Columbus

State OH
Enter state OH

Postal Code 43221-3560

Note: On these same tabs we also have attributes that agency admin are responsible to update and maintain.

General Tab

- **Photo** – this photo is written to active directory and synchronized to Office 365. This picture will appear in Lync and Outlook. Note the picture size is limited to 96dpi.
- **First Name*** – Once the first name is synchronized from OAKS the agency admin can modify the name.
- **Last Name*** – Once the first name is synchronized from OAKS the agency admin can modify the name.
- **Middle Name*** – Once the first name is synchronized from OAKS the agency admin can modify the name.

*To return to the OAKS supplied name;

- Clear the first, last and middle names.

Note: The OAKS name is only synced one time all subsequent changes must be completed by the portal admin.

To change a second time;

- Return to the OAKS supplied name then you do additional updates.

Work Info Tab

- **Agency Admin** – assign portal admin rights
- **Helpdesk Admin** – assign rights to user to change user password. Please note this is agency wide.
- **Search Criteria One** – allows the agency admin to create criteria for advance searches and criteria based groups
- **Search Criteria Two** – allows the agency admin to create criteria for advance searches and criteria based groups
- **Search Criteria Three** – allows the agency admin to create criteria for advance searches and criteria based groups
- **User Home Directory** – used for home folders
- **User Home Drive** – drive designation for home folders

Account Information Tab

The account information tab is newly added to FIM Portal. This is an information tab items on this tab are not editable by agency administrators.

- **E-Mail** – current user e-mail address
- **E-Mail Alias** – current user mail nickname
- **Preferred Nickname** – allows the administrator to choose an alias for the mailbox.

Note: This will update the e-mail address as long as the mailbox is set to automatically update the e-mail address.

- **BWC User ID SMTP address** – although this states BWC it can be used by any agency. Allows the administrator enter in a proxy address for the users mailbox.
- **Member of Security Group** – list of security groups this user belongs to
- **Member of Distribution Group** – list of distribution groups this user belongs to

Forefront Identity Manager — Webpage Dialog

Miller, Bob

General | Work Info | Contact Info | **Account Info** | Mailbox Maintenance | MITS Access Control | Provisioning

E-mail
Primary e-mail address for the user: bob.miller@mail.assure.ohio.gov

E-mail Alias
E-mail alias. It is used to create the e-mail address:

Preferred Nickname:

BWC User ID SMTP address
Please enter the entire SMTP address - i.e., bwc@bwc.state.oh.us:

Member Of Security Groups
This User Is A Member Of The Following Security Groups...

Display Name	Account Name	Domain	Type	Scope	Membership Locked	Owner
The User Is NOT A Member Of Any Security Group...						

0 items total Page 1 of 1

Member Of Distribution Groups
This User Is A Member Of The Following Distribution Groups...

Display Name	Account Name	Domain	Type	Scope	Membership Locked	Owner
The User Is NOT A Member Of Any Distribution Group...						

0 items total Page 1 of 1

Advanced View | OK | Cancel

ENABLE NEW MAILBOX

The new version of FIM Portal has simplified how a mailbox is enabled. Prior to this release an extra attribute must be checked. The new option allows a pull down but no additional requirements are needed.

Note: If an e-mail address exists for the user the system will not attempt to create a new mailbox. The system also checks if you are JFS or not and displays the proper tab on the form for that type of user.

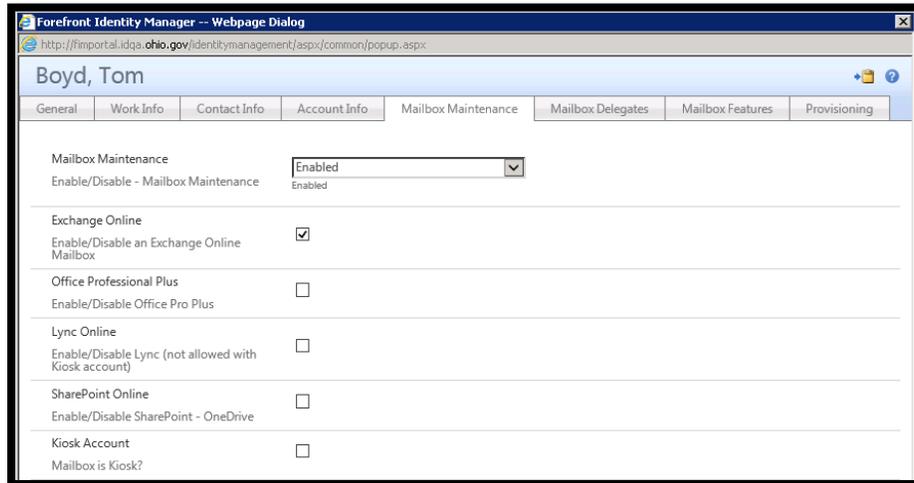
EXCHANGE LICENSING

- Exchange Online
- Lync Online
- SharePoint Online
- Kiosk Account

The type of licensing is reduced to those items that are configurable by an agency. When creating a mailbox, the mailbox itself must be created but before the user can access the mailbox on-line it must be licensed. The licensing structure is to give the agency control where control may be needed for example:

A regular exchange user with mailbox will have the exchange on-line option selected, if you want to add SharePoint and Lync you would also select those licenses. However you are not required to have an exchange mailbox to have SharePoint or Lync these options can be selected on a as need basis with or without and exchange mailbox.

A Kiosk user is limited to 2 GB in their mailbox to select a Kiosk license first check the exchange on-line license and also check the kiosk license. A Kiosk user is also allowed to have SharePoint but not Lync. Please be aware you cannot select a Kiosk user with having a mailbox for that user, a SharePoint license by itself is a full license.



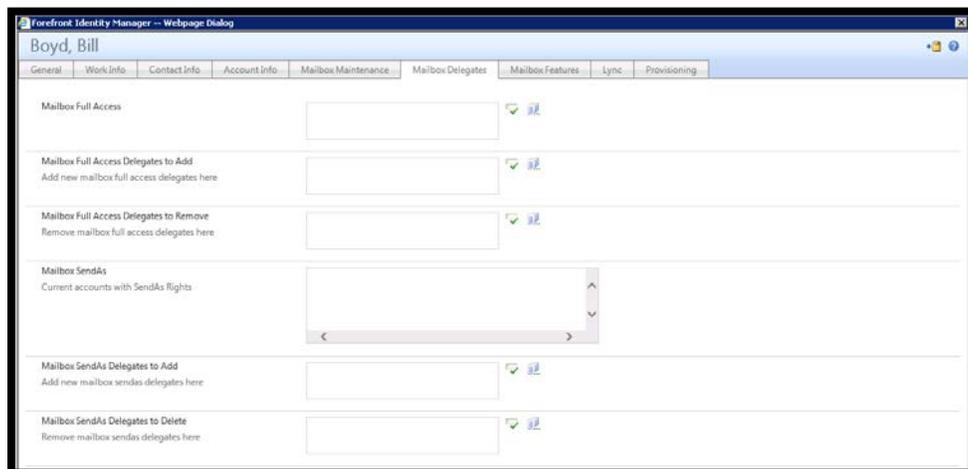
ASSIGNING AND REMOVING FULL ACCESS PERMISSIONS

The assigning and removing of full access permission is completed through the Mailbox Delegates tab within a user account edit. Note: this tab will not show until a mailbox has been created either in the cloud or on-premises. To complete the operation you will use two attributes, one for adding and one for removal.

A third attribute is available that will display the current permissions as they are recorded in active directory. Please note: full access permissions are applied to user's mailbox and can contain data that is not present in Active Directory. For example if a ticket is entered to have full access permissions applied or removed and these are completed directly on the account in Office365 they will not be represented in FIM Portal.

Full Access

- **Mailbox Full Access Delegates to Add** – use this attribute to add full access rights
- **Mailbox Full Access Delegates to Remove** – use this attribute to remove full access rights



ASSIGNING AND REMOVING SEND-AS PERMISSIONS

The assigning and removing of send-as permission is completed through the Mailbox Delegates tab within a user account edit. Note: this tab will not show until a mailbox has been created either in the cloud or on-premises. To complete the operation you will use two attributes, one for adding and one for removal.

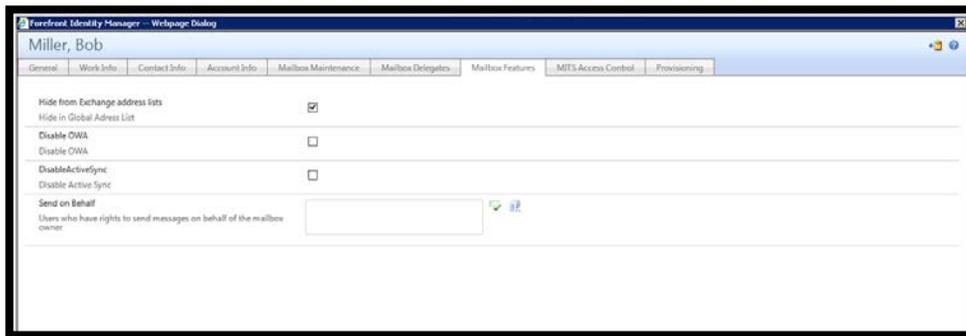
A third attribute is available that will display the current permissions as they are recorded in active directory. Please note: send-as permissions are applied to user's mailbox and can contain data that is not present in Active Directory. For example if a ticket is entered to have send-as permissions applied or removed and these are completed directly on the account in Office365 they will not be represented in FIM Portal.

Send-As Access

- **Mailbox Full Access Delegates to Add** – use this attribute to add full access rights
- **Mailbox Full Access Delegates to Remove** – use this attribute to remove full access rights

MAILBOX FEATURES TAB

- **Hide from Exchange Address List** – click for true and un-check for false
- **Disable OWA** – click to disable OWA, uncheck to enable. OWA is enabled on a mailbox by default (unchecked).
- **Disable ActiveSync** - click to disable ActiveSync, uncheck to enable. OWA is enabled on a mailbox by default (unchecked).
- **Send on Behalf** – agency administrators can configure send on behalf for a user mailbox by adding the users SUID to this option.

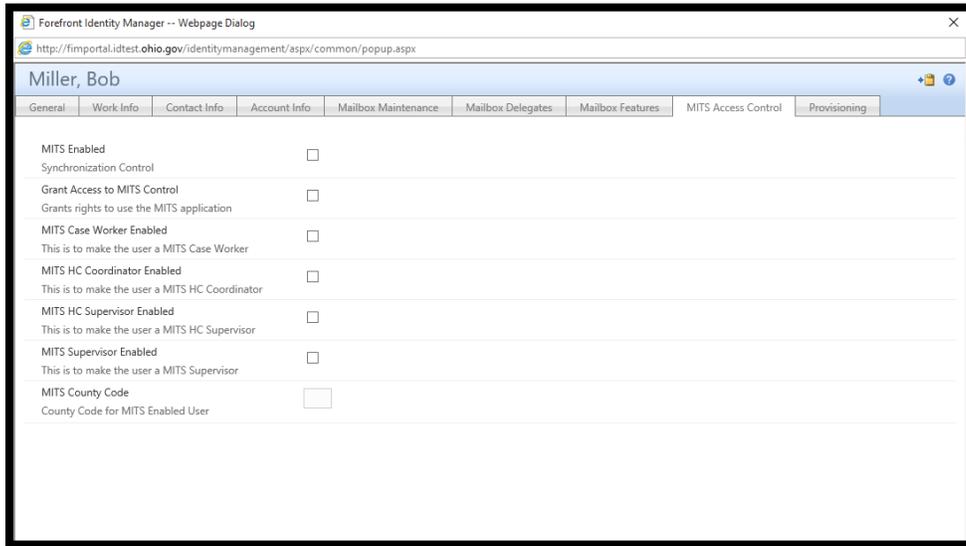


IMITS ACCESS CONTROL

Specifically designed for Medicaid's MITS application this tab allows Medicaid administrators (those enabled for MITS admin rights) to see this tab.

Note: This tab is not available if you are not a MITS administrator.

- **Grant Access to MITS Control** – this option is used to tell the system that this person needs to be synchronized with the MITS system.
- **MITS Enabled** – this option allows the administrator to configure synchronization to the MITS LDS server
- **Grant Access to MITS Control** – This option enables or disables MITS access.
- **MITS Case Worker Enabled** – enables a user to be in the case worker role.
- **MITS HC Coordinator Enabled** - enables a user to be in the case HC coordinator role.
- **MITS HC Supervisor Enabled** - enables a user to be in the case supervisor role.
- **MITS Supervisor Enabled** – enabled MITS supervisor role
- **MITS County Code** – codes the user to the proper county.



MODULE FOUR REVIEW

Can you configure full access and send-as rights prior to a mailbox being created?

Answer: No – the account must first be created

Can you add a new employee user account through FIM Portal?

Answer: No – each agencies HR is responsible for creating user accounts by entering into HCM

Can you delete employee or contractor user accounts?

Answer: No

STUDENT EXERCISES

- Enable a user for e-mail
- Add full access and send-as rights to the user account you just created
- Hid the user from the GAL

**MODULE FIVE - RESOURCE ACCOUNTS,
ROOM, EQUIPMENT, AND SHARED
MAILBOXES**

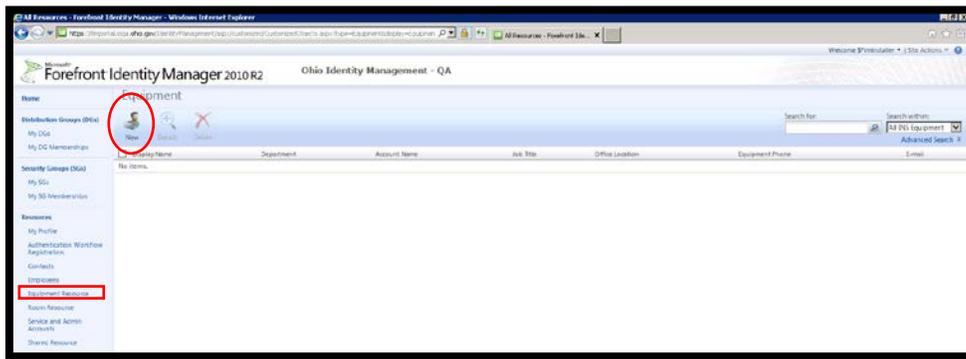
CREATING NEW RESOURCE ACCOUNT

Training Time: 30 minutes

Begin creating a new security list by selecting Security Groups from the Navigation panel.

When creating a new account the system first synchronizes the user account information to the Identity domain and to Office365. This process can take 30 – 90 minutes depending on the sync cycle. Once FIM Portal has detected that a user account has been create on both on-premises and in the cloud it will perform the mailbox creation process. All resource accounts (other than JFS) are created in Office365.

Note: This guide will only show one type of resource account. All resource accounts work exactly alike other than Shared which does not have calendar options.



- Select **New** on the panel
- Enter the following information:
 - **Equipment Name:** This will be the name in active directory (not display). The application automatically adds the agency department code per OAKS.
 - **Display Name:** name you will see in Exchange global address list
 - **Preferred Email and Alias Name:** Enter the alias for the account which will also be used as the primary SMTP address
 - **Alternate Agency Code:** used when you are creating a Resource that is not your own agency. (Example I work for DAS but if I wanted to create a resource for Insurance I would use this option to choose INS.)

FINDING RESOURCE ACCOUNTS

Training Time: 10 minutes

From the Equipment/Room/Shared option – notice the Search for and Search within options. These are the two options available to search for resource accounts.

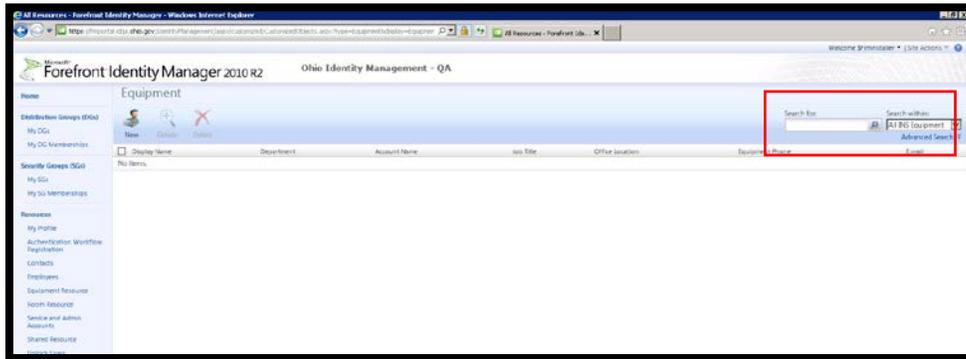
Search for:

Currently you can search by the following criteria:

- Display Name
- Mail NickName (Alias)
- First Name
- Last Name
- **Wildcard search option:** FIMPortal is a XML based application the normal “*” for wild card is “%”, so a search of %GROU% will produce a list of groups with those letters together anywhere in the display or alias.

Search Within:

- Pull down with all relative group search scopes that your agency has access to use.
- Agency search scope is the default
- An **“All Equipment/All Room/All Shared”** option is available to all agencies; however this does not mean you will have to edit.



ADVANCED SEARCH FUNCTION

Training Time: 5 minutes

To search for users using the advanced search function;

- Click Advanced Search

To return to the basic search;

- Choose Basic Search

Notice this time that nothing has been preselected and in most cases an error appears (the error is a bug in Microsoft code and a fix is scheduled to be released in the future – you can remove the error by clicking search).

- Choose User next to “Select”

The Match is All or Any (the Any function is like an “or” statement) in fact you can get fairly complex by using the “any” function

To add additional statements;

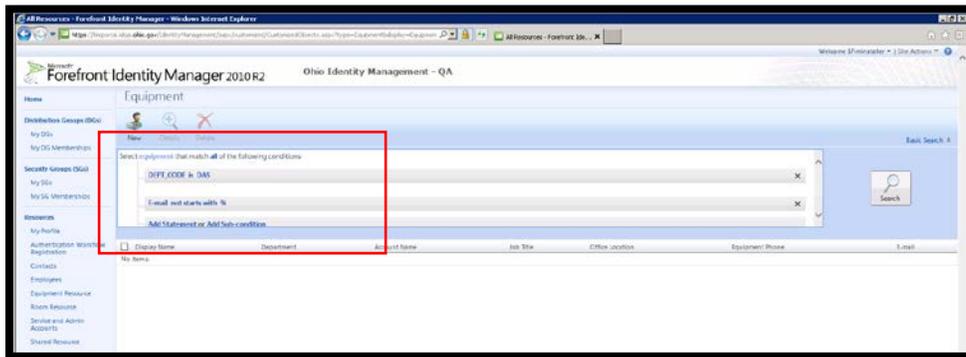
- Click the Add Statement option

A line will be inserted.

➤ Click to select....

- **Logical** – depending on the attribute type appropriately choose the type of logic (is, is not, etc.)
- **Value** – value you are looking for in your search

The example below will find all DAS equipment resources that are missing an e-mail address.



EDITING RESOURCE ACCOUNTS

Training Time: 10 minutes

To edit a resource account;

➤ Click on the resource name.

With a new resource a minimal amount of data is entered to create the account, once the mailbox and account has been created all of the basic data along with certain exchange attributes are available for change. Please note: the edit screen will not display all tabs until the mailbox has been created and synchronization has taken place to FIM Portal.

Forefront Identity Manager -- Webpage Dialog

DAS Test Equip 85

BasicInfo | WorkInfo | ContactInfo | Resource Info | Mailbox Delegates | Mailbox Features | Equipment Settings

Equipment Name: DAS-Test-Equip-85

Account Name: [Empty]

Display Name: DAS Test Equip 85

Advanced View | OK | Cancel

- **Account Name:** This is not edible after the initial create
- **Display Name:** You can change the display name as needed
- **WorkInfo**
- **Department:** This is the agency department code
- **Search Criteria One, Two, and Three:** Agency portal admin, criteria related searches

Forefront Identity Manager -- Webpage Dialog

DAS Test Equip 85

BasicInfo | WorkInfo | ContactInfo | Resource Info | Mailbox Delegates | Mailbox Features | Equipment Settings

Department: DAS

Agency Code: [Empty]

Search Criteria One: [Empty]
Dynamic Group Search Criteria: [Empty]

Search Criteria Two: [Empty]
Dynamic Group Search Criteria: [Empty]

Search Criteria Three: [Empty]
Dynamic Group Search Criteria: [Empty]

Manager: [Empty] ✓ [Empty]

Assistant: [Empty] ✓ [Empty]

Advanced View | OK | Cancel

Contact Information

This is standard active directory attributes used for general information. All are edible attributes by agency portal administrators.

The screenshot shows a web browser window titled "Forefront Identity Manager -- Webpage Dialog" with the URL "DAS Test Equip 85". The interface has several tabs: "BasicInfo", "WorkInfo", "ContactInfo", "Resource Info", "Mailbox Delegates", "Mailbox Features", and "Equipment Settings". The "ContactInfo" tab is active, displaying a form with the following fields:

- Equipment Phone:
- Office Location:
- Address:
- City:
- Postal Code:

Resource Information

General information about the resource account; e-mail address, alias, and any security or distribution groups the mailbox is a member of.

The screenshot shows the same web browser window as above, but with the "Resource Info" tab selected. The "E-mail" field is populated with "DAS-Test-Equip-85@idga.ohio.gov". The "E-mail Alias" field contains "DAS-Test-Equip-85". Below these are two sections for group membership:

Member Of Security Groups
This User is A Member Of The Following Security Groups...
The User is NOT A Member Of Any Security Group...

0 Items total Page 1 of 1 [< >]

Member Of Distribution Groups
This User is A Member Of The Following Distribution Groups...
The User is NOT A Member Of Any Distribution Group...

0 Items total Page 1 of 1 [< >]

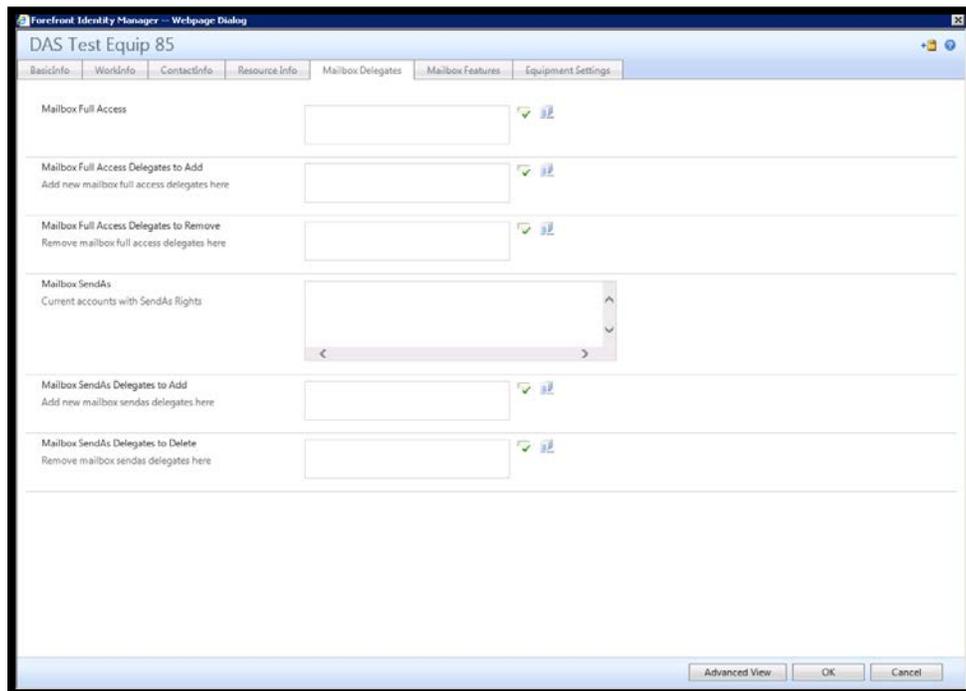
ASSIGNING AND REMOVING FULL ACCESS PERMISSIONS

The assigning and removing of full access permission is completed through the Mailbox Delegates tab within a user account edit. Note: this tab will not show until a mailbox has been created either in the cloud or on-premises. To complete the operation you will use two attributes, one for adding and one for removal.

A third attribute is available that will display the current permissions as they are recorded in active directory. Please note: full access permissions are applied to user's mailbox and can contain data that is not present in Active Directory. For example if a ticket is entered to have full access permissions applied or removed and these are completed directly on the account in Office365 they will not be represented in FIM Portal.

Full Access

- **Mailbox Full Access Delegates to Add** – use this attribute to add full access rights
- **Mailbox Full Access Delegates to Remove** – use this attribute to remove full access rights



ASSIGNING AND REMOVING SEND-AS PERMISSIONS

The assigning and removing of send-as permission is completed through the Mailbox Delegates tab within a user account edit. Note: this tab will not show until a mailbox has been created either in the cloud or on-premises. To complete the operation you will use two attributes, one for adding and one for removal.

A third attribute is available that will display the current permissions as they are recorded in active directory. Please note: send-as permissions are applied to user's mailbox and can contain data that is not present in Active Directory. For example if a ticket is entered to have send-as permissions applied or removed and these are completed directly on the account in Office365 they will not be represented in FIM Portal.

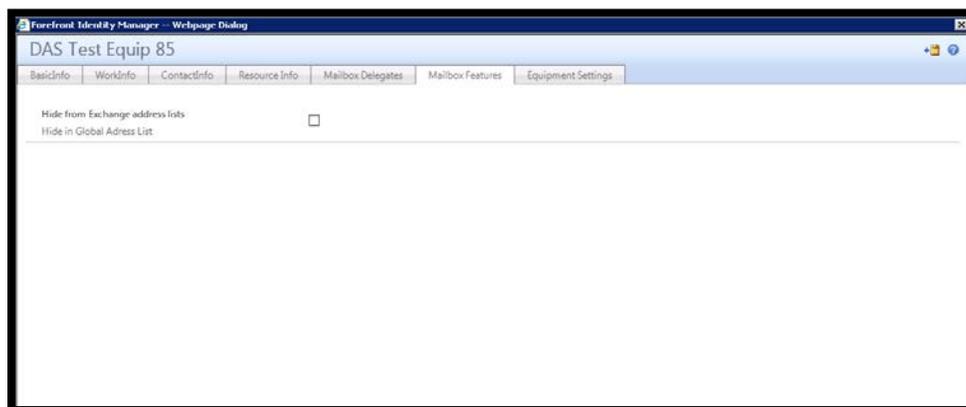
Send-As Access:

- **Mailbox Full Access Delegates to Add** – use this attribute to add full access rights
- **Mailbox Full Access Delegates to Remove** – use this attribute to remove full access rights

HIDING MAILBOX FROM THE GAL

Currently the only option on the Mailbox Features tab is the ability to hide the mailbox from the GAL. This is a synchronization attribute and will take a short amount of time before syncing. Also if the mailbox is in Office365, addition sync will need to take place.

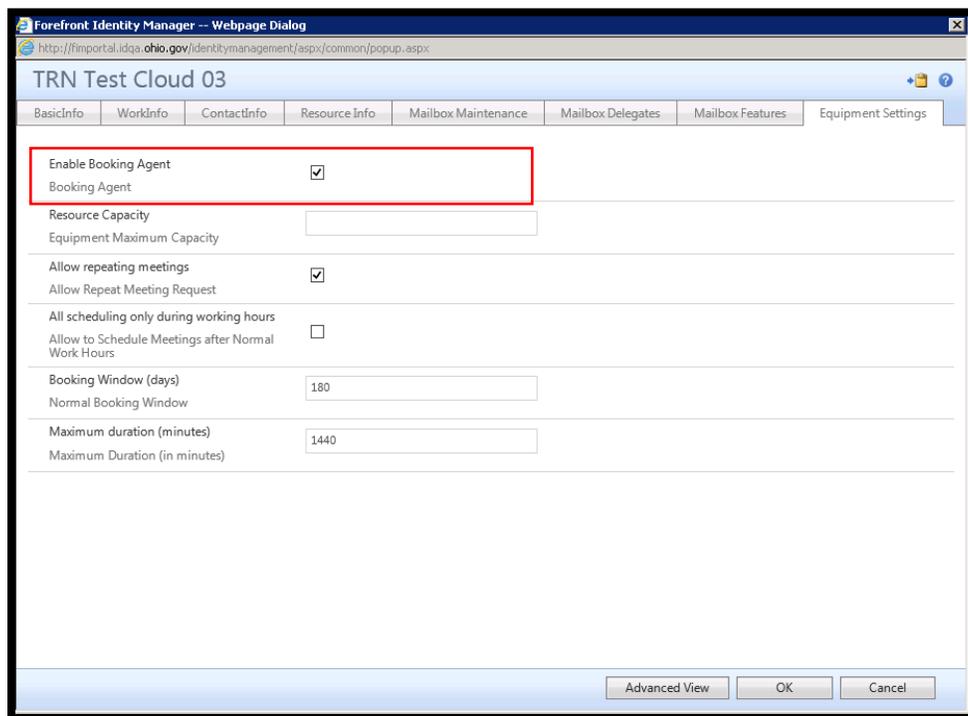
Hide from Exchange Address List – click for true and un-check for false



EQUIPMENT/ROOM SETTINGS

An option that you have with Equipment and Rooms is calendar settings. Because the nature of FIM Portal and how updates work there is an option at the top the screen that is required for calendar updates to occur. Please be sure to check the box when submit the changes for calendar changes to take place. The identity team has pre-populated those calendars setting with default values. The one addition or change is **enable booking agent**. This is normally not a default value however we configure this during resource creation since it is a normal option that is requested. Any one item can be change or all at one time.

Further explanation of these options is available.



The screenshot shows a web browser window titled "Forefront Identity Manager -- Webpage Dialog" with the URL "http://fimportal.idqa.ohio.gov/identitymanagement/asp/COMMON/popup.aspx". The page is titled "TRN Test Cloud 03" and has several tabs: "BasicInfo", "WorkInfo", "ContactInfo", "Resource Info", "Mailbox Maintenance", "Mailbox Delegates", "Mailbox Features", and "Equipment Settings". The "Equipment Settings" tab is active. The settings are as follows:

Setting	Value
Enable Booking Agent	<input checked="" type="checkbox"/>
Booking Agent	
Resource Capacity	
Equipment Maximum Capacity	
Allow repeating meetings	<input checked="" type="checkbox"/>
Allow Repeat Meeting Request	
All scheduling only during working hours	<input type="checkbox"/>
Allow to Schedule Meetings after Normal Work Hours	
Booking Window (days)	180
Normal Booking Window	
Maximum duration (minutes)	1440
Maximum Duration (in minutes)	

At the bottom of the page, there are three buttons: "Advanced View", "OK", and "Cancel".

MODULE FIVE REVIEW

How long must you wait until a resource mailbox can be created?

Answer: Until the synchronization process has completed, typically 60 to 90 minutes.

What information is required to create a new resource account?

Answer: Resource Name and Display Name

What is the difference between the Resource Name and Display Name?

Answer – The resource name is the active directory name and the display name is the name as seen in the global address list.

STUDENT EXERCISES

- Create a new resource account (room, equipment, and share)
- Add full access and send-as rights to one of the resource accounts
- Change calendar settings on the resource account.

MODULE SIX - SERVICE AND SERVER ADMIN ACCOUNTS

CREATING NEW SERVICE OR SERVER ADMIN ACCOUNT

Training Time: 10 minutes

Service accounts are those accounts being used for applications for support of the applications.

- Service accounts have a non-expiring password.
- Service account password management can be done by group or individual user but the password is managed through password.ohio.gov/admin.
- All service accounts begin with a "\$". For certain Unix or Lynx servers beginning with a \$ is an invalid name.
- You do not use service accounts as normal application management accounts.
- Password registration / Reset is not available for Admin or Service Accounts.

Administrator (Admin) Accounts are those accounts specifically created for server management. These accounts are not your normal logon accounts for separation of authority purposes.

- For the CSS domain the admin account will begin with an "A" followed by your State of Ohio User ID.
- For the ID domain the admin account will begin with an "I" followed by your State of Ohio User ID.
- You must manage your own admin account passwords using the password.ohio.gov/admin website.
- When creating an "Admin" account check the box that it is an Admin and have the person's State of Ohio User ID available. You will need to supply the ID.
- Password registration / Reset is not available for Admin or Service Accounts.

General Information

- **Admin Account** – designate that the account is an admin
- **IBM Account** – if this is an IBM employee please designate with this checkbox
- **First Name** – Person’s name
- **Last Name** – Person’s name
- **Agency** – enter the agency for the account
- **Domain** – CSS or ID
- **Manager** – the person’s manager
- **Application Code** – choose the appropriate application code
- **Enable Account** – this is enable / disable in AD. You can disable an account at any time by unchecking. Be sure to check when creating a new account.
- **Description** – what the account is for.

The screenshot shows a web browser window titled "Forefront Identity Manager -- Webpage Dialog" with the URL "http://fimportal.idqa.ohio.gov/identitymanagement.aspx/common/popup.aspx". The page content is titled "Create SrvAcct" and has two tabs: "General Information" (selected) and "Summary".

The form fields are as follows:

- Admin Account**: "Is this an Admin Account?" with an unchecked checkbox.
- IBM Admin Account**: "Employee is IBM" with an unchecked checkbox.
- First Name**: A text input field with a red asterisk.
- Last Name**: A text input field with a red asterisk.
- Password Reset E-Mail Address**: "E-mail address for password reset letter" with a text input field.
- Agency**: A dropdown menu with a red asterisk.
- Domain**: A dropdown menu with "CSSQA" selected and a red asterisk.
- Manager**: A text input field with a red asterisk, a green checkmark icon, and a document icon.
- Application Code**: A dropdown menu with a red asterisk.
- Enable Account**: "Enable or Disable Account in Active Directory" with an unchecked checkbox.
- Description**: A text area with a red asterisk.

A legend at the bottom left states: "* Requires input". At the bottom right, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

FINDING SERVICE AND ADMIN ACCOUNTS

Training Time: 5 minutes

From the Service and Admin option – notice the Search for and Search within options

These are the two options available to search for resource accounts

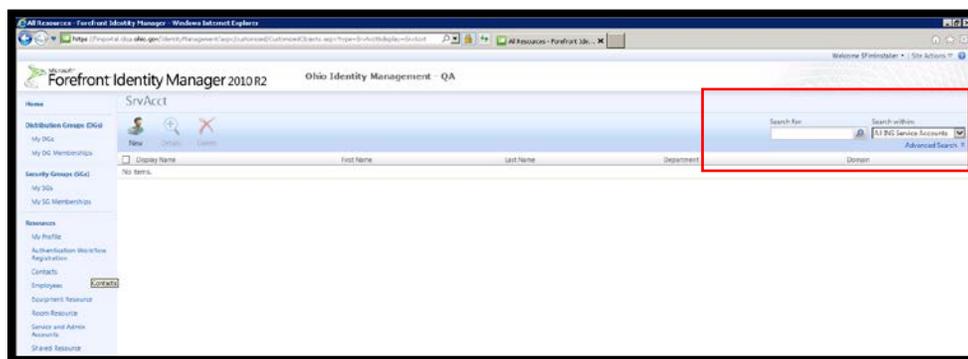
Search for:

Currently you can search by the following criteria:

- Display Name
- First Name
- Last Name
- **Wildcard search option:** FIMPortal is a XML based application the normal “*” for wild card is “%”, so a search of %GROU% will produce a list of groups with those letters together anywhere in the display or alias.

Search Within:

- Pull down with all relative group search scopes that your agency has access to use.
- Agency search scope is the default
- An **“All Service Account”** option is available to all agencies; however this does not mean you will have edit access.



ADVANCED SEARCH FUNCTION

Training Time: 5 minutes

As with criteria base groups we can search using the advanced search function

➤ Click Advanced Search

Notice this time that nothing has been preselected and in most cases an error appears (the error is a bug in Microsoft code and a fix is scheduled to be released in the future – you can remove the error by clicking search)

➤ Choose User next to “Select”

The Match is All or Any (the Any function is like an “or” statement) in fact you can get fairly complex by using the “any” function

To add additional statements;

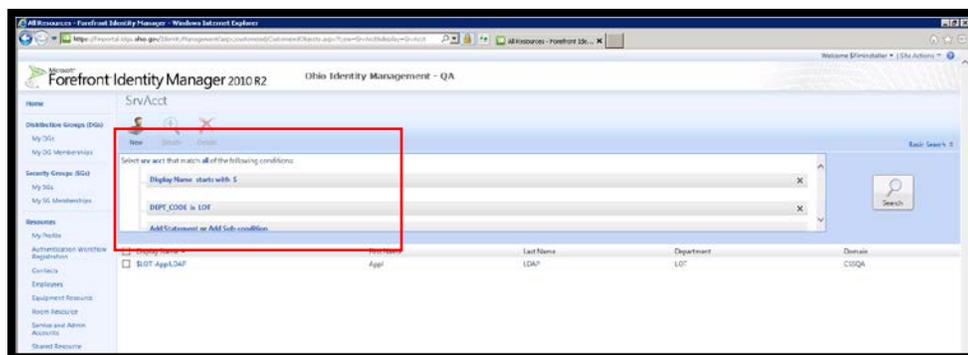
➤ Click the Add Statement option

A line will be inserted.

➤ Select Click to select....

- **Logical** – depending on the attribute type appropriately choose the type of logic (is, is not, etc.)
- **Value** – value you are looking for in your search

The example below will find all service accounts for LOT.



EDITING SERVICE ACCOUNTS

Training Time: 5 minutes

Once the account has been found you can edit information related to the account when first entering.

The following attributes have editable criteria:

- IBM Admin Account
- First Name
- Last Name
- Manager
- Enable-Disable
- Description

The screenshot shows a web browser window titled "Forefront Identity Manager -- Webpage Dialog" displaying the "General Information" tab for a service account named "\$LOT-AppLDAP". The form contains the following fields and options:

- Account Name ***: \$LOT-AppLDAP
- Admin Account**: Is this an Admin Account?
- IBM Admin Account**: Employee is IBM
- First Name ***: Appl
- Last Name ***: LDAP
- Agency Code**: Lottery Commission (dropdown menu, with "LOT" listed below)
- Domain**: CSSQA
- Manager**: [Empty text box] with a green checkmark icon and a document icon to the right.
- Application Code ***: LDAP Connectivity (dropdown menu, with "LDP" listed below)
- Enable Account**: Enable or Disable Account in Active Directory
- Description ***: [Empty text box]

A red asterisk indicates required input. At the bottom of the dialog are buttons for "Advanced View", "OK", and "Cancel".

MODULE SIX REVIEW

What character will be added to all service accounts?

Answer: \$

Who can change an administrators password?

Answer: The user themselves, they will use their State of Ohio User ID to change.

What information is required to create an admin account?

Answer – First Name, Last Name, Agency, SUID, Domain, Manager, Application Code, and Description

STUDENT EXERCISES

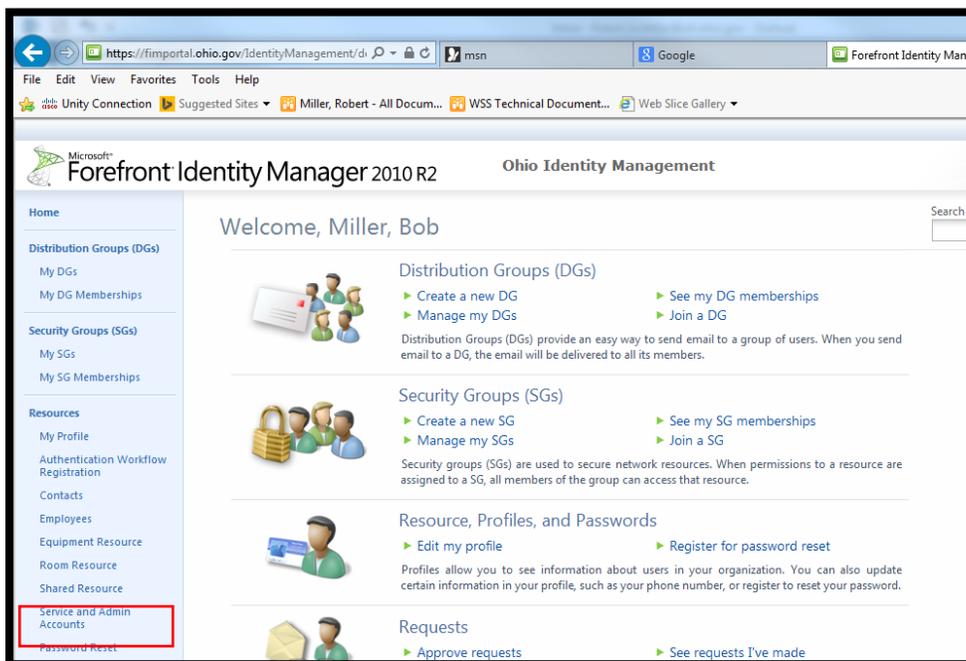
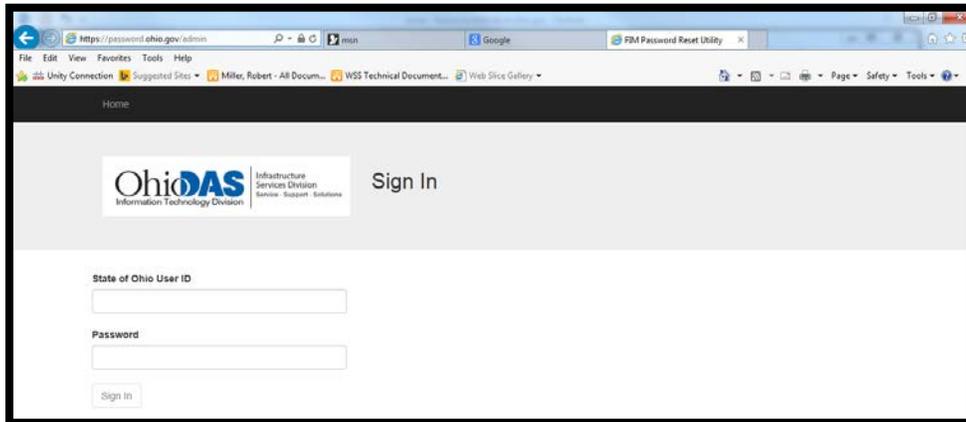
- Create a new service account.
- Create a new admin account.
- Disable the admin account.

MODULE SEVEN - ADMINISTRATOR PASSWORD RESET

ACCESSING PASSWORD.OHIO.GOV/ADMIN

Training Time: 5 minute

Accessing the administrator password reset site can be accomplished by opening IE, Chrome, and/or Firefox and going to <https://password.ohio.gov/admin> or by clicking the link from FIM Portal.

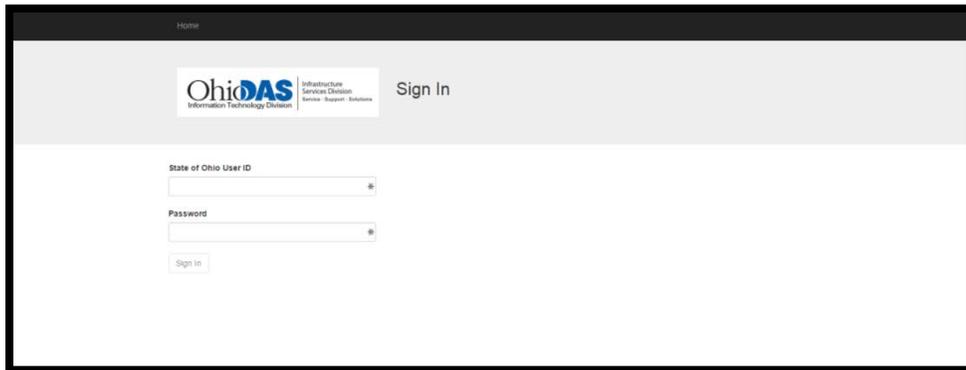


RESETTING PASSWORDS - ADMINISTRATOR

Training Time: 10 minutes

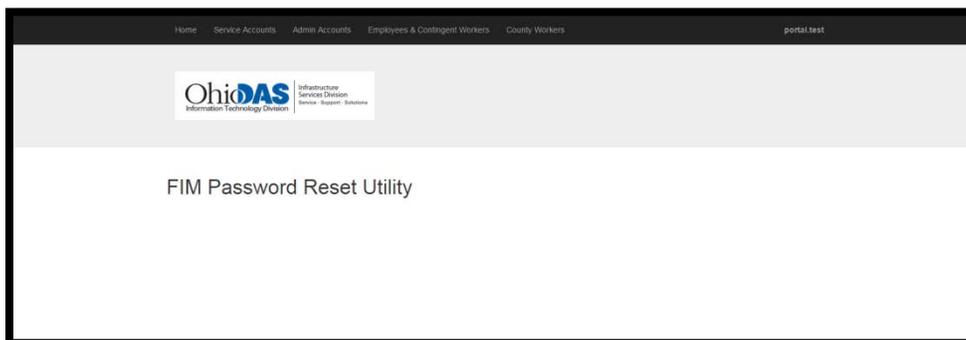
To access the password reset site please use the URL – <https://password.ohio.gov/admin> this site is available to all internal IP subnets and selected external subnets.

To access the site enter your State of Ohio User ID and Password



The screenshot shows the OhioDAS Sign In page. At the top left is the OhioDAS logo with the tagline 'Information Technology Division'. To the right of the logo is the text 'Infrastructure Services Division Service · Support · Solutions' and a 'Sign In' link. Below the logo is a form with two input fields: 'State of Ohio User ID' and 'Password'. Each field has a small eye icon to its right. Below the password field is a 'Sign In' button.

Once logged onto the site you will components that you have access to use. Please note the example below shows all components and your option may not be the same.

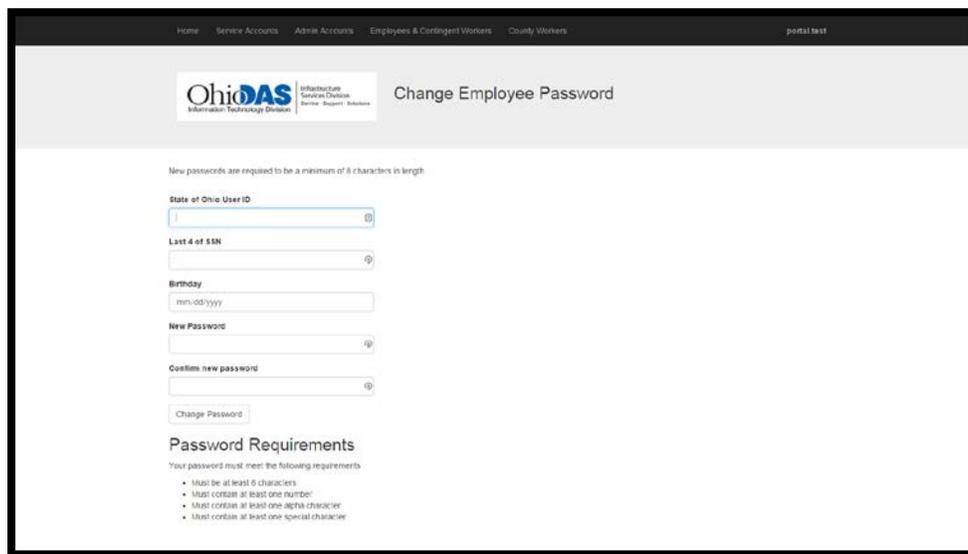


The screenshot shows the FIM Password Reset Utility page. At the top is a navigation bar with links: 'Home', 'Service Accounts', 'Admin Accounts', 'Employees & Contingent Workers', 'County Workers', and 'portal.test'. Below the navigation bar is the OhioDAS logo and the text 'Infrastructure Services Division Service · Support · Solutions'. The main content area displays 'FIM Password Reset Utility'.

CHANGING AN USERS PASSWORD

To reset an employee, contractor, or generic user you must know the following pieces of information:

- The persons State of Ohio User ID
- The last four numbers of their social security
- Their date of birth (Note: the birthdate must be entered in Year-Month-Day order (1945-12-12))
- New passwords – 8 characters long, must contain a letter, number, and special character.



The screenshot shows the 'Change Employee Password' page in the OhioDAS portal. The page has a navigation bar at the top with links for Home, Service Accounts, Admin Accounts, Employees & Contingent Workers, and County Workers. The main content area features the OhioDAS logo and the title 'Change Employee Password'. Below the title, there is a note: 'New passwords are required to be a minimum of 8 characters in length.' The form includes several input fields: 'State of Ohio User ID', 'Last 4 of SSN', 'Birthday' (with a date mask 'mm-dd-yyyy'), 'New Password', and 'Confirm new password'. A 'Change Password' button is located below the form. At the bottom, there is a 'Password Requirements' section with a list of requirements: 'Your password must meet the following requirements: • Must be at least 8 characters • Must contain at least one number • Must contain at least one alpha character • Must contain at least one special character'.

RESETTING ADMIN ACCOUNTS

Training Time: 5 minutes

To reset an admin account from the landing page;

- Choose Admin Accounts

To reset an admin password you must know the following pieces of information:

- The admin or service account name
- New passwords – 8 characters long, must contain a letter, number, and special character.

- The person resetting the admin account must be logged on with the SUID that matches the admin account.

The screenshot displays the 'Change Admin Account Password' interface. At the top, there is a navigation bar with links for Home, Service Accounts, Admin Accounts, Employees & Contingent Workers, and County Workers. The main content area features the OhioDAS logo and the title 'Change Admin Account Password'. A note states: 'New passwords are required to be a minimum of 8 characters.' The form includes three input fields: 'Admin Account', 'New Password', and 'Confirm New Password', each with a small icon to its right. Below the fields is a 'Change Password' button. Underneath the button, the 'Password Requirements' are listed: 'Your password must meet the following requirements: • Must be at least 8 characters • Must contain at least one number • Must contain at least one alpha character • Must contain at least one special character'.

RESETTING SERVICE ACCOUNTS

Training Time: 5 minutes

To reset a service account from the landing page;

- Choose Service Accounts

To reset a service account password you must be the owner of that account as entered in FIM Portal service and admin accounts:

- The service account name
- New passwords – 8 characters long, must contain a letter, number, and special character.
- The person resetting the admin account must be the owner of that account.

OhioDAS Infrastructure Services Division Service Support Solutions

Change Service Account Password

New passwords are required to be a minimum of 8 characters.

Service Account

New Password

Confirm New password

Change Password

Password Requirements

Your password must meet the following requirements

- Must be at least 8 characters
- Must contain at least one number
- Must contain at least one alpha character
- Must contain at least one special character

MODULE SEVEN REVIEW

Who has the authority to change an Admin password?

Answer: The user themselves

What attributes are required to change an employee's password?

Answer: SUID; last four of social security; date of birth

STUDENT EXERCISES

- Reset the password for Admin account you created for yourself

MODULE EIGHT – USER SELF-SERVICE PASSWORD RESET

ACCESSING PASSWORD REGISTRATION SITE

Training Time: 10 minutes

To access the password registration site enter <https://passwordregistration.ohio.gov>

If prompted for a user name and password enter your State of Ohio User ID and password. The format for the username is either id\suid or suid@id.ohio.gov.

You will see the following screen:



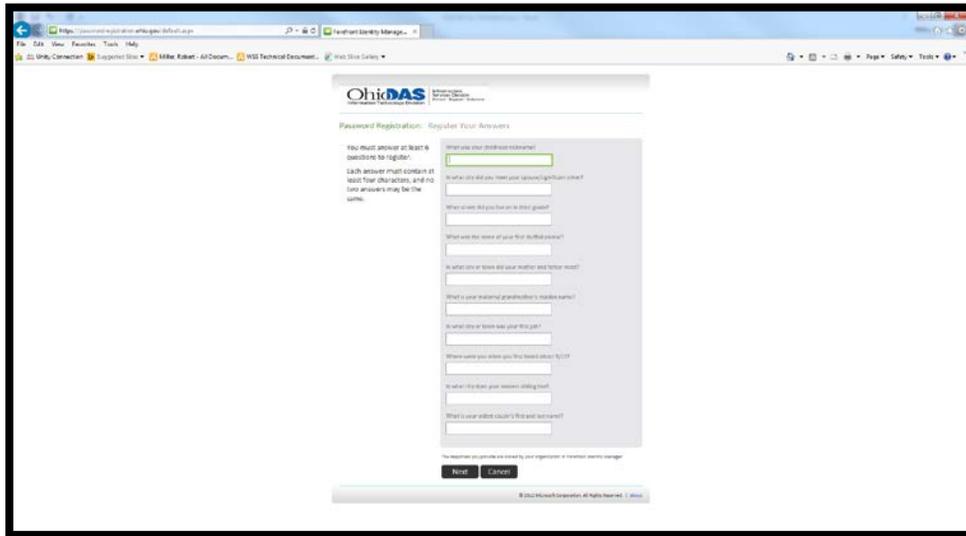
- Click Next

You will be prompted for your password again,

- Confirm it is your user name on the screen:



You must answer 6 of the 10 questions



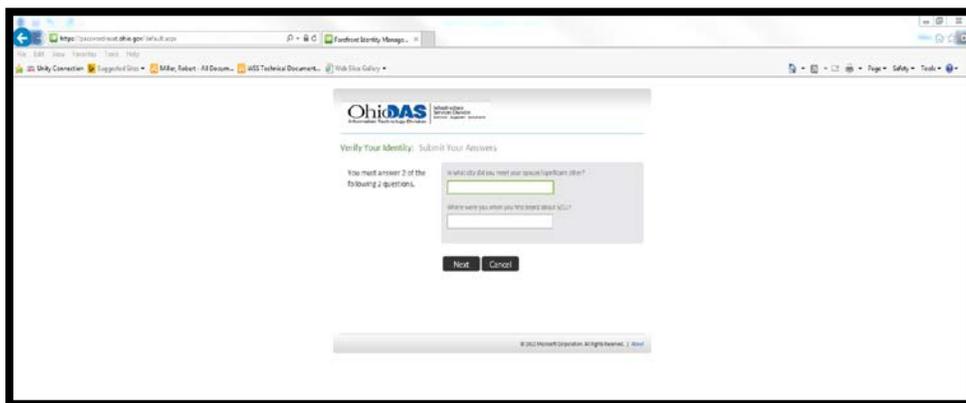
ACCESSING PASSWORD RESET SITE

Training Time: 5 minutes

To access the password registration site enter <https://passwordreset.ohio.gov>. Enter your username in id\suid format.



Answer the questions when prompted, this is time limited.



Enter a new password:



MODULE EIGHT REVIEW

How many questions must you answer to register?

Answer: 6

STUDENT EXERCISES

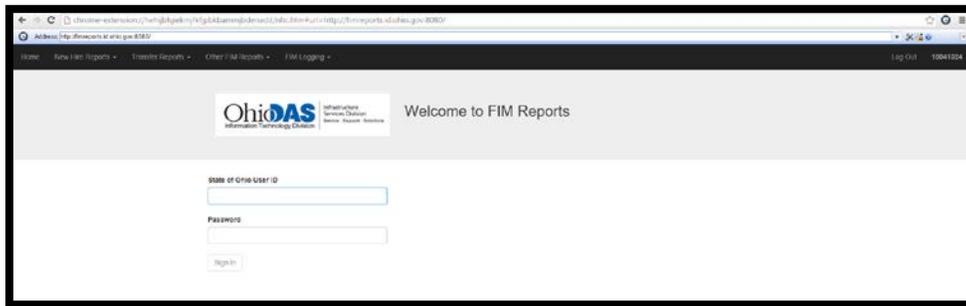
- Access the registration page and register your State of Ohio User ID

MODULE NINE - REPORTING

ACCESSING THE REPORT SITE

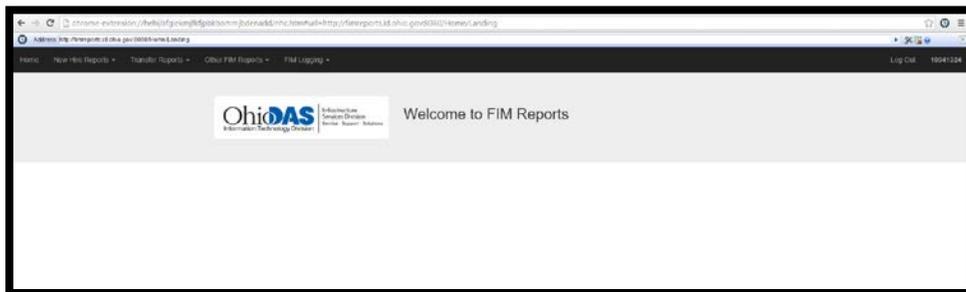
Training Time: 5 minutes

To access the report site login to <https://fimportal.ohio.gov/identitymanagement> and select User Reports from the menu list.



➤ Enter your State of Ohio User ID and password.

Once you have been authenticated the menu options will be available. (Your username and password are required because the site is separate from FIM Portal and to limit your view to only your agency a username is required.)

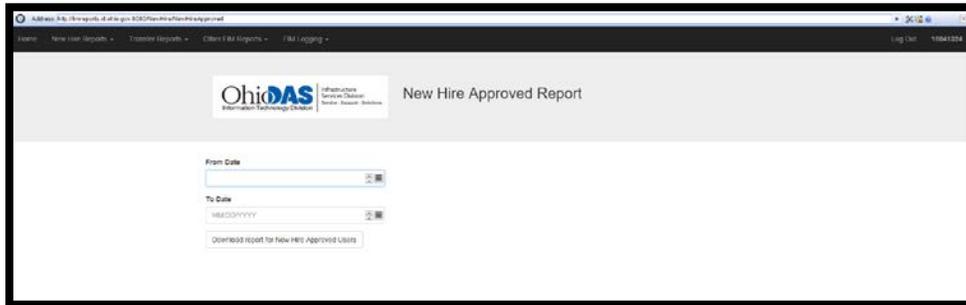


Options at the top of the screen with pull-down for each category of NewHire Reports - Transfer Reports – and – Other FIM Reports.

NEW HIRE REPORTS

Approved New Hires

This report will display new hires for your agency that have been approved and available in FIM Portal.

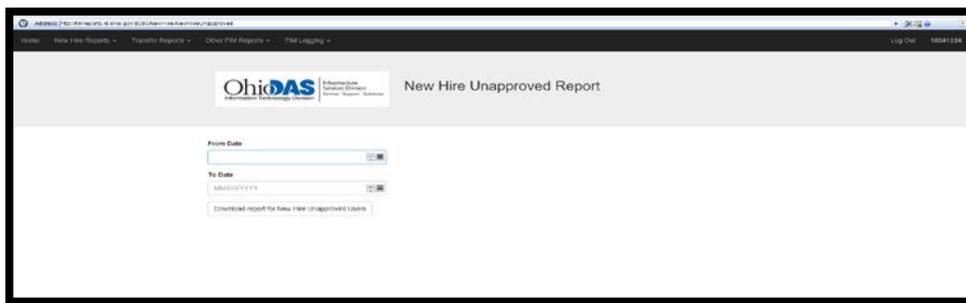


- Enter starting date range for new hires, picker is available on right.
- Enter ending date range for new hires, picker is available on right.

Once the report displays the Download report for New Hire Approved Users will be available. The download is in CSV format which can be opened using Microsoft Excel.

New Hire Unapproved Report

This report will display new hires for your agency that have not been approved and are not available in FIM Portal. These users will not appear in FIM Portal until the hire process has completed.

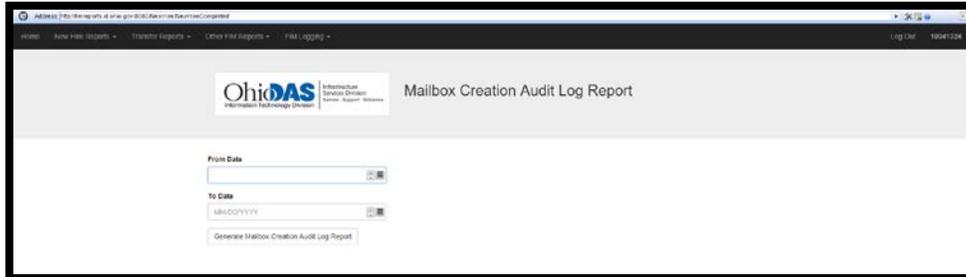


- Enter starting date range for new hires, picker is available on right.
- Enter ending date range for new hires, picker is available on right.

Once the report displays the Download report for New Hire UnApproved Users will be available. The download is in CSV format which can be opened using Microsoft Excel.

NEW HIRES COMPLETED

This report will display new hires that are available in FIM Portal and the date the mailbox was created. It is an audit report that can be used to track mailbox creation.



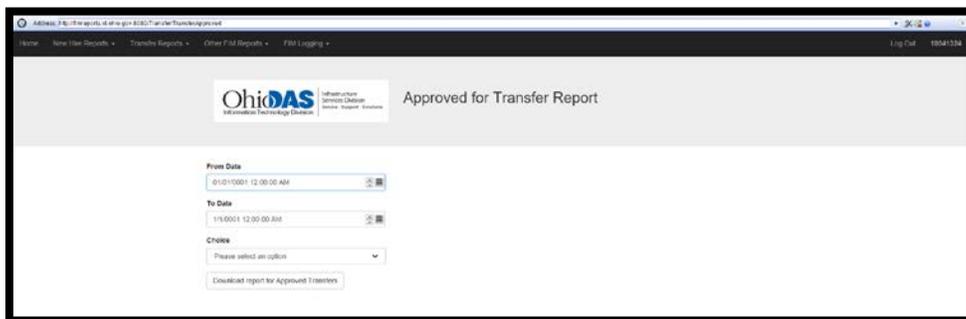
- Enter starting date range for new hires, picker is available on right.
- Enter ending date range for new hires, picker is available on right.

Once the report displays the Download report for Generate Mailbox Creation Audit Log Report will be available. The download is in CSV format which can be opened using Microsoft Excel.

TRANSFER REPORTS

Approved Transfers

The approved transfer report will display a list of user either transferring to your agency or from your agency (a selector is available) that have been approved for the transfer and will be processed by the exchange team on the day of their transfer.

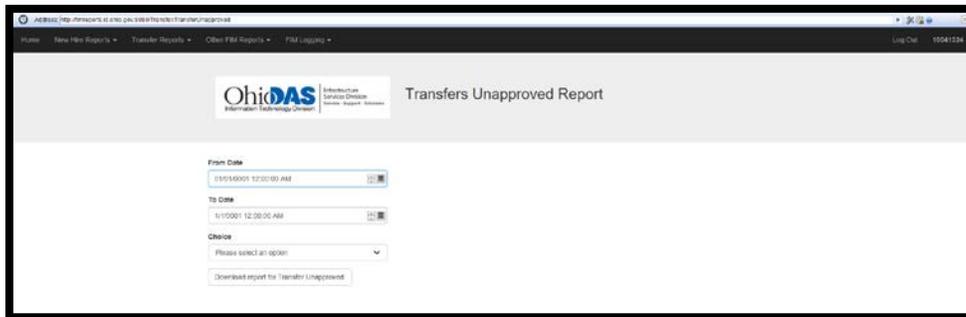


- Enter starting date range for new hires, picker is available on right.
- Enter ending date range for new hires, picker is available on right.
- Select either Transferring or Receiving

Once the report displays the Download report Approved Transfers will be available. The download is in CSV format which can be opened using Microsoft Excel.

Unapproved Transfers

The unapproved transfer report will display a list of user that have not been approved for transfer either transferring to your agency or from your agency (a selector is available) that have been approved for the transfer and will be processed by the exchange team on the day of their transfer.

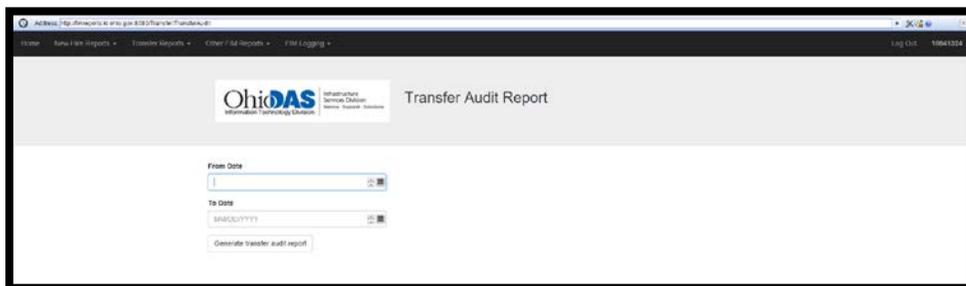


- Enter starting date range for new hires, picker is available on right.
- Enter ending date range for new hires, picker is available on right.
- Select either Transferring or Receiving

Once the report displays the Download report for Transfers Unapproved will be available. The download is in CSV format which can be opened using Microsoft Excel.

Transfer Audit

The transfer audit report is an auditing report which will allow you to see information regarding the processing of the transfer.

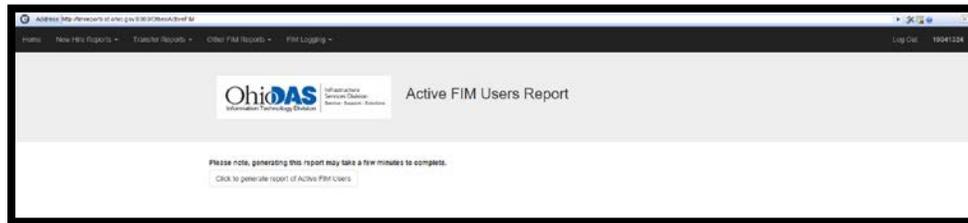


- Enter starting date range for new hires, picker is available on right.
- Enter ending date range for new hires, picker is available on right.
- Select either Transferring or Receiving

OTHER FIM REPORTS

Active FIM Users

The active FIM users report will allow the agency to dump all users in FIM Portal that are currently active to a CSV file. Please note this report takes a long time to generate.



There are no options in the report.

Inactive FIM Users Report

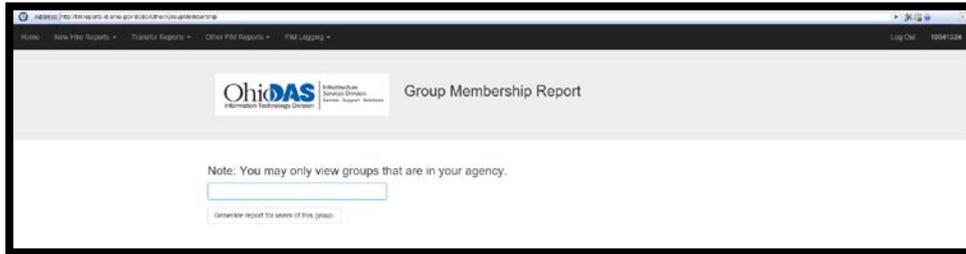
The active FIM users report will allow the agency to dump all users in FIM Portal that are currently inactive to a CSV file. Please note this report takes a long time to generate.



There are no options in the report.

Group Membership

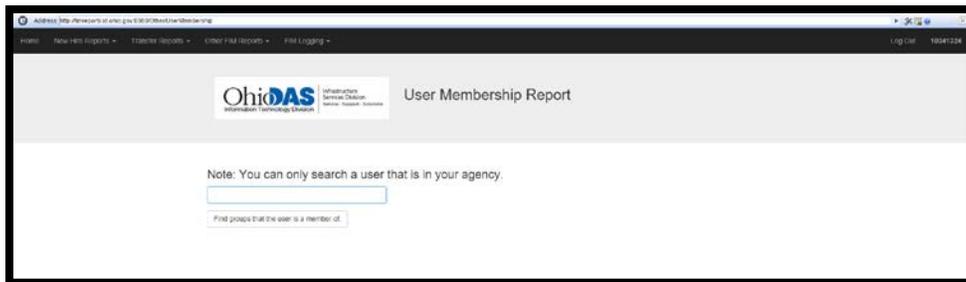
This report will allow the agency to export the membership of a group to a CSV file.



- Enter the group name.

User Membership

This report allows an agency to export group membership for a user.



- Enter the user State of Ohio user ID.