



## Identity and Access Management

---

# Security Administrator Guide



June 5, 2015



## CONTENTS

- SECTION 1. SIGN ON TO UMRA / SEARCH FOR AN IAM USERID .....5**
  - Sign On To Production UMRA .....5
  - Search For an IAM Userid.....5
  
- SECTION 2. CREATE A USERID.....8**
  - Sign On To Production UMRA .....8
  - Search For an Existing IAM Userid .....8
  - Search Results Decision Point .....8
  - Creation of New IAM Userid .....8
    - Personal Tab ..... 10
    - Keys Tab..... 11
    - Communication Tab..... 11
    - Location Tab ..... 13
    - State Org Tab ..... 14
    - Finishing The New Userid ..... 14
  - New Userid Activation..... 15
  
- SECTION 3. MANAGE A USER .....17**
  - Sign On To Production UMRA ..... 17
  - Search For an Existing IAM Userid ..... 17
  - Manage an IAM Account ..... 17
    - Modify Personal Tab..... 17
    - Modify Keys Tab ..... 18
    - Modify Communication Tab ..... 19
    - Modify Location Tab ..... 22
    - Modify the State Org Tab ..... 22
    - Save the Modifications ..... 23
  - Status Column ..... 24
  - Control Column ..... 25
  
- SECTION 4. PROCEDURE FOR CHANGING A PASSWORD .....27**
  - Sign On To Production UMRA ..... 27
  - Search For an Existing IAM Userid ..... 27
  - Start the Password Change Process ..... 27
    - Confirm Identity..... 27
    - Change Password..... 28
    - Password Requirements..... 28
    - Handling Locked and Disabled Userids..... 28
  - What Userid Owners Should Do After a Password Change ..... 30
  
- SECTION 5. “LOCKED” VERSUS “BLOCKED” VERSUS “DISABLED” .....31**
  - Sign On To Production UMRA ..... 31
  - Search For an Existing IAM Userid ..... 31
  - Disable a Userid..... 32
  - Enable a Userid..... 34
  - SSRPM Block..... 36
  - Unlock a Userid ..... 36

|   |           |
|---|-----------|
| <b>SECTION 6. DELETING A USERID .....</b>                         | <b>38</b> |
| Sign On To Production UMRA .....                                  | 38        |
| Search For an Existing IAM Userid .....                           | 38        |
| Search Results Decision Point .....                               | 38        |
| Delete a Userid .....   | 38        |
| <b>SECTION 7. CREATING SECONDARY IAM ACCOUNTS (USERIDS) .....</b> | <b>40</b> |
| Sign On To Production UMRA .....                                  | 40        |
| Search For an Existing IAM Userid .....                           | 40        |
| Create Secondary IAM Account (Userid).....                        | 40        |
| Special Issues.....   | 41        |
| Additional Userid Specifications.....                             | 41        |
| <b>SECTION 8. AUDIT LOG.....</b>                                  | <b>43</b> |
| Sign On To Production UMRA .....                                  | 43        |
| Set Audit Listing Parameters .....                                | 43        |
| Audit Action Codes .....  | 45        |
| Audit Listing.....  | 46        |
| Exporting Audit Listing .....                                     | 46        |
| <b>SECTION 9. REPORTS.....</b>                                    | <b>47</b> |
| Sign On To Production UMRA .....                                  | 47        |
| Viewing Report .....  | 47        |
| Exporting Security Report .....                                   | 48        |
| Using Parameters to Search for Security Reports .....             | 48        |
| Available 'Canned' Reports .....                                  | 50        |
| <b>SECTION 10. LIVE DATA QUERIES.....</b>                         | <b>52</b> |
| Sign On To Production UMRA .....                                  | 52        |
| Producing Live Data Queries .....                                 | 52        |
| Direct AD Attributes .....  | 52        |
| Available Direct Attributes .....                                 | 53        |
| Additional Options Under Columns .....                            | 56        |
| Exporting Query Results.....                                      | 56        |
| Special Attributes .....  | 57        |
| Available Special Attributes.....                                 | 59        |
| Locations .....   | 59        |
| <b>SECTION 11. SCHEDULE FUTURE COMMAND EXECUTION.....</b>         | <b>61</b> |
| Commands.....   | 61        |
| Field Modifications NOT Allowed.....                              | 61        |
| Field Modifications Allowed.....                                  | 62        |
| <b>SECTION 12. TRANSFER PROCEDURE .....</b>                       | <b>66</b> |
| Transfer Exemptions .....   | 66        |
| Transfer Scenario .....   | 66        |
| <b>SECTION 13. USERID TRANSFERS .....</b>                         | <b>68</b> |
| Internal Transfer.....  | 68        |
| Inter-Agency Transfer.....  | 71        |



**SECTION 14. REQUESTING NEW SUPPORT STAFF .....75**  
Requesting a New Agency IAM Security Administrator ..... 75  
Requesting a New Agency Delegated Exchange Administrator ..... 75  
Requesting a New Agency Mailbox Auditor ..... 75  
Requesting a New Agency Password Changer (Only) ..... 76  
Requesting the Removal of an Agency IAM Security Administrator ..... 76  
Requesting the Removal of an Agency Delegated Exchange Administrator ..... 76  
Requesting the Removal of an Agency Mailbox Auditor ..... 77  
Requesting the Removal of an Agency Password Changer (Only) ..... 77  
Requesting any other type of Admin access not related to IAM or Exchange ..... 77

**SECTION 15. APPLICATION MANAGEMENT (RBAC / LBAC) .....78**  
Security Administrator Privileges ..... 78  
Add Privilege ..... 78  
Delete Privilege ..... 81  
Other RBAC Roles ..... 82  
Display Current RBAC and LBAC Settings ..... 83

**SECTION 16. OTHER REPORTING .....84**  
Enterprise Email Mailbox Size Report (Run Ad-Hoc) ..... 84

**SECTION 17. IAM USERID FIELD DESCRIPTIONS .....86**  
Personal Tab ..... 86  
Keys Tab ..... 86  
Communication Tab ..... 86  
Location Tab ..... 86  
State Org Tab ..... 87  
Other ..... 87

**SECTION 18. OTHER INFORMATION .....88**  
IAM Administrator Guide ..... 88  
Session Timeout ..... 88  
Session Log Out/Closing Your Browser ..... 88  
Header Drop Down ..... 89  
Tab Count Restriction ..... 89  
Your Account Tab ..... 90  
Locations You Can Administer ..... 90

## SECTION 1. SIGN ON TO UMRA / SEARCH FOR AN IAM USERID

### Sign On To Production UMRA

1. Log on to UMRA at URL is <https://iam.wisconsin.gov/umra> with your IAM Userid and password.

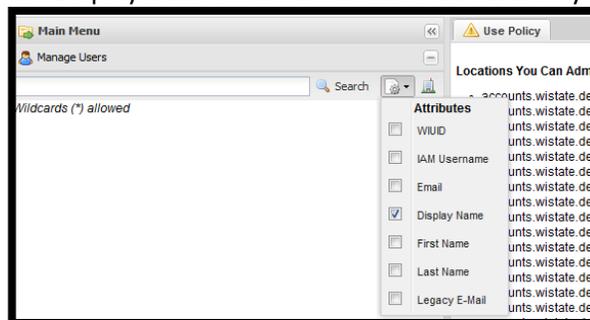


### Search For an IAM Userid

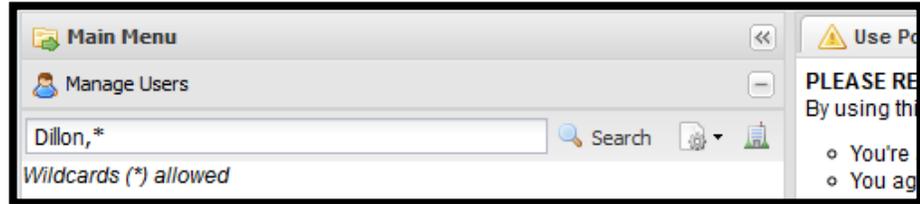
2. Perform a **Search** for an existing IAM userid. Press the **Manage Users** bar.



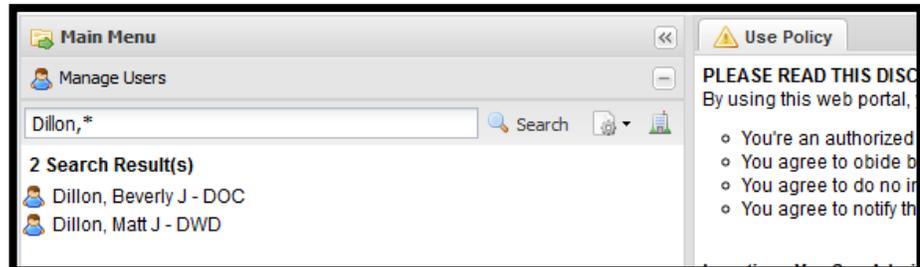
3. Press the **Attributes drop down icon** after Search box and make sure that only the Display name is checked. This value will stay in place until you change it.



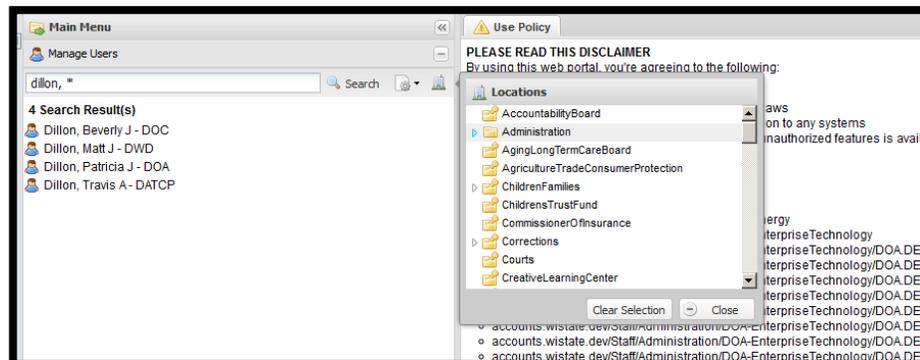
4. In the blank area before the Search button enter in the last name of the individual you are searching for followed by a ',' and a portion of the individuals first name (optional) followed by a '\*'. **Note you are limited to alphanumeric, spaces, dashes, commas, periods, underscores, @, or asterisks (\*)**



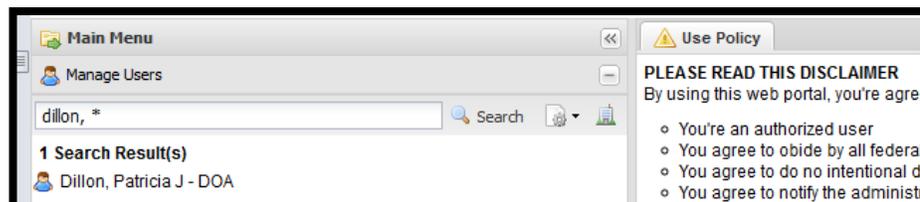
5. Press the **Search** button.



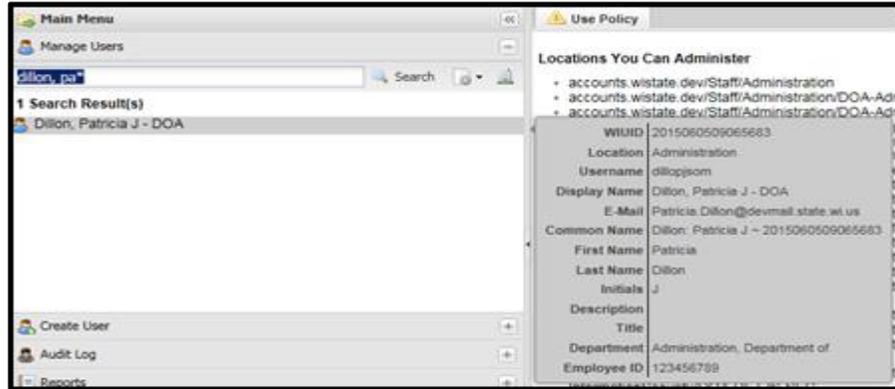
6. You can limit your search within a specific OU by pressing the little hotel icon at the end of the search line. With your mouse click on the OU you wish to restrict your search to. Holding down the **Ctrl** button on your keyboard while selecting agencies with your mouse allows you to select multiple locations. Press the **Close** button. Press the **Search** button.



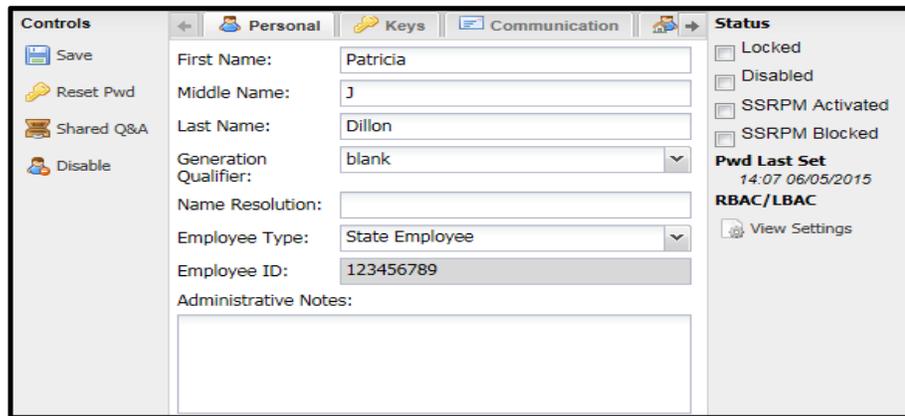
Your search results will be limited to just a specific OU and not all agencies.



7. Using your mouse you can point to a specific individual and see some of the information in their record.



- Click on the individuals name to see their complete information.



## SECTION 2. CREATE A USERID

Follow the procedure below to create a new IAM Userid in UMRA.

### Sign On To Production UMRA

1. See instructions outlined in Section 1, Step 1.

### Search For an Existing IAM Userid

2. Perform a **Search** to make sure that your new individual does not already exist at your agency or another agency. See instructions outlined in Section 1, starting with Step 2.

### Search Results

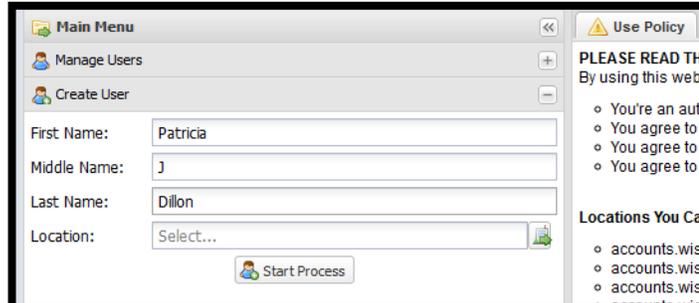
- Individual already exists at another agency: Send an Email to DET IAM Security (*DOA DL IAM Security*) to arrange a transfer (see Section 12) of their IAM Userid to your agency.
- Individual already exists in your agency: Make the necessary changes to their Userid. See Section 3 for managing a Userid and section 13 for internal transfer directions if necessary.
- Individual cannot be found: Continue with Step 3 to create the Userid required.

### Creation of New Userid

3. Click the **Create User** bar (may be on the bottom left hand side of panel).

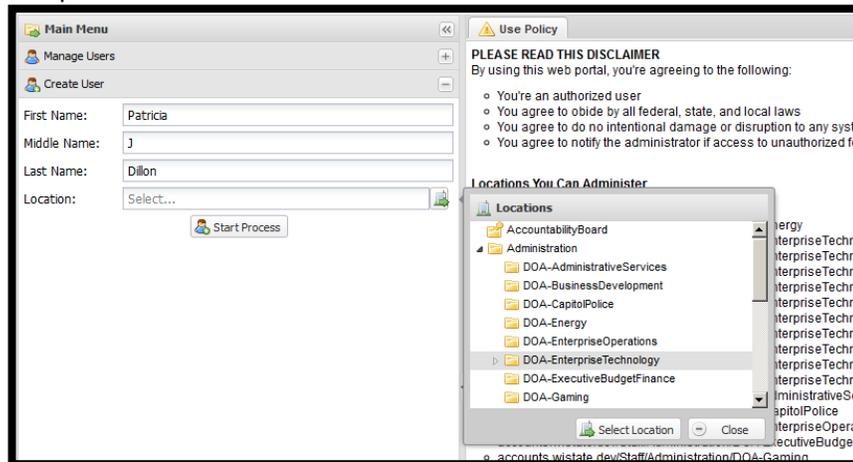


- A drop down of 4 fields will appear. Enter in the new individual's **First Name**, a **Middle Name** (Limit 5 characters or NMN for no middle name), and the **Last Name**.



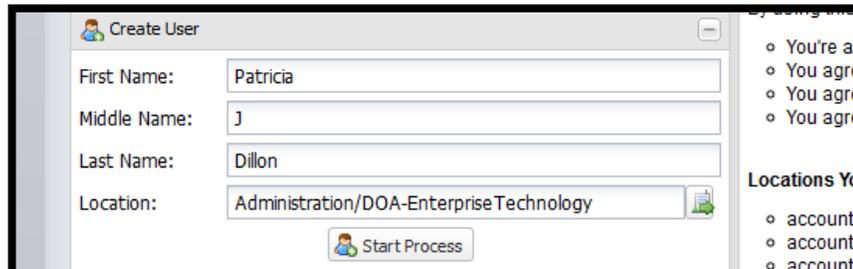
The screenshot shows the 'Create User' form in a web application. The 'First Name' field contains 'Patricia', 'Middle Name' contains 'J', and 'Last Name' contains 'Dillon'. The 'Location' field is a dropdown menu currently showing 'Select...'. A 'Start Process' button is visible at the bottom of the form. To the right, there is a 'Use Policy' section with a disclaimer and a 'Locations You Can Administer' section with a list of locations.

- Press the dropdown button at the end of the Location line. You will see valid locations for a Userid to be placed in. Highlight the location with your mouse and press the **Select Location** button at the bottom of the box.



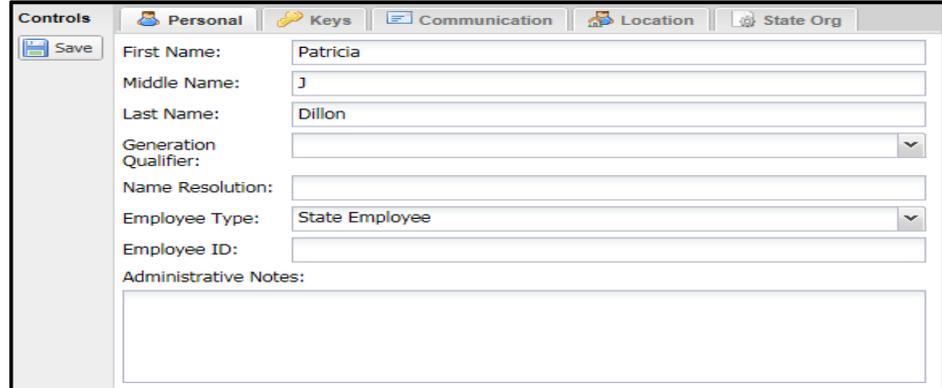
This screenshot shows the 'Create User' form with the 'Locations You Can Administer' dropdown menu open. The menu lists various locations, including 'Administration/DOA-Enterprise Technology', which is highlighted. The 'Start Process' button is still visible at the bottom of the form.

- The location information will fill in the Location field. Press the **Start Process** button.



The final screenshot shows the 'Create User' form with the 'Location' field populated with 'Administration/DOA-Enterprise Technology'. The 'Start Process' button is now the primary action button at the bottom of the form.

- A panel with five tabs will come up on the right side of the screen. You can fill in any remaining fields as needed.

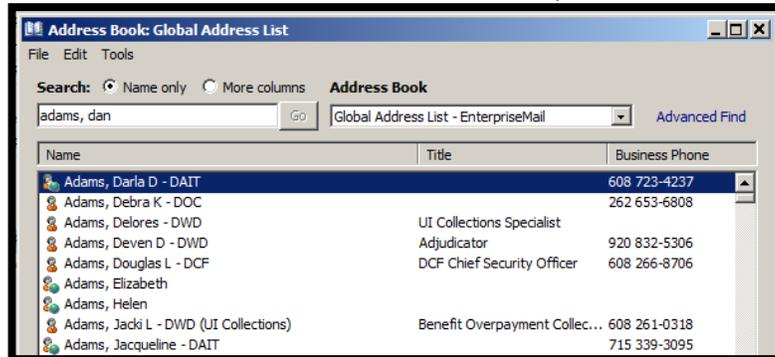


### PERSONAL TAB

- Under the Personal tab you will note a **Generation Qualifier**, **Name Resolution**, **Employee Type** and **Administrative Notes** fields.

**Generation Qualifier:** values available in the dropdown affect the email address but not the Userid.

**Name Resolution:** this can be a common/nickname or bureau location. It will ONLY change the display name in the Enterprise GAL but not the email address or Userid. For example see Jacki L Adams below.



| Name                                  | Title                         | Business Phone |
|---------------------------------------|-------------------------------|----------------|
| Adams, Darla D - DAIT                 |                               | 608 723-4237   |
| Adams, Debra K - DOC                  |                               | 262 653-6808   |
| Adams, Delores - DWD                  | UI Collections Specialist     |                |
| Adams, Deven D - DWD                  | Adjudicator                   | 920 832-5306   |
| Adams, Douglas L - DCF                | DCF Chief Security Officer    | 608 266-8706   |
| Adams, Elizabeth                      |                               |                |
| Adams, Helen                          |                               |                |
| Adams, Jacki L - DWD (UI Collections) | Benefit Overpayment Collec... | 608 261-0318   |
| Adams, Jacqueline - DAIT              |                               | 715 339-3095   |

**Administrative Notes:** this field is for use by agency security administrators to put in notations about changes, transfers or other information.

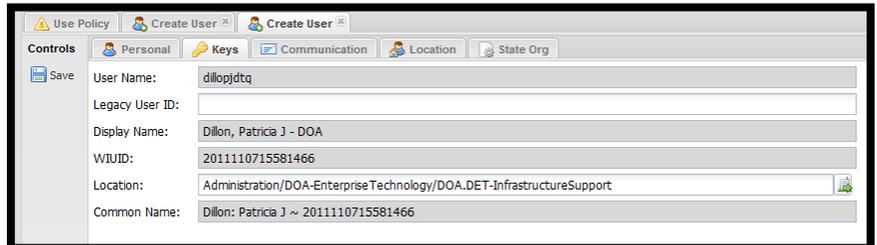
**Employee Type:** A value of **State Employee** is the default value of this field. You can change it to any of the values available in the dropdown list.

**Employee ID:** Key in the Employee ID from the Human Capital Management (HCM) system in STAR. The Employee ID must be numeric and unique. Once the account is Saved, the Employee ID field cannot be modified. If modification of the data in this field is needed, please open a Service Request.

**(06/05/2015 - Until we hear how the Employee ID field will be officially implemented, please leave blank.)**

**KEYS TAB**

- Click on the **Keys** tab. The **User Name**, **Display Name**, **WIUID** and **Common Name** fields are not editable.



- The **Legacy Userid** field is optional, but you can enter in the new individuals LAN account here. The **Location** field has the identical value that you entered in previously when you started the Create Userid process.

**COMMUNICATION TAB**

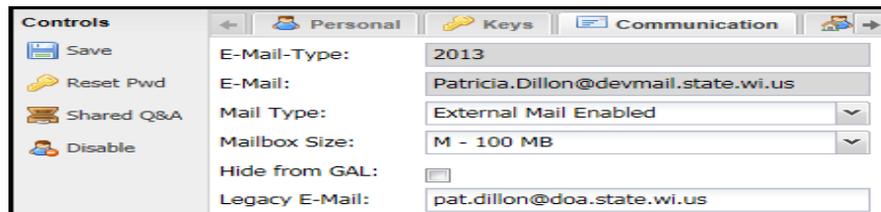
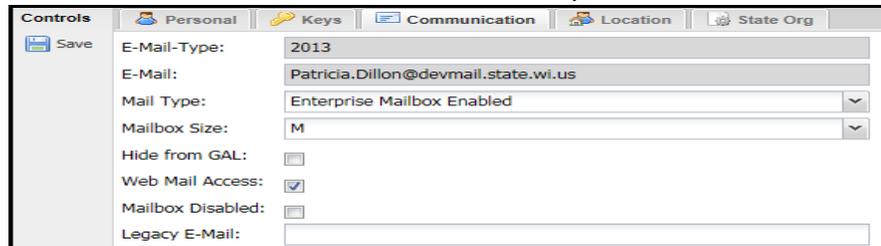
- Click on the **Communication** tab. The **E-Mail Type**, **E-Mail**, **Mail Type**, **Mailbox Size** and **Web Mail Access** fields are automatically filled out for you with values defined for your agency. You can override all except the **E-Mail** field.

- To override the value of **Mail Type**, press the drop down button.

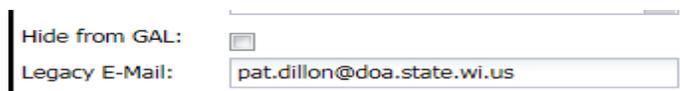
*Enterprise Mailbox Enabled* is for staff using Enterprise Email.

*External Mail Enabled* is for staff using legacy email.

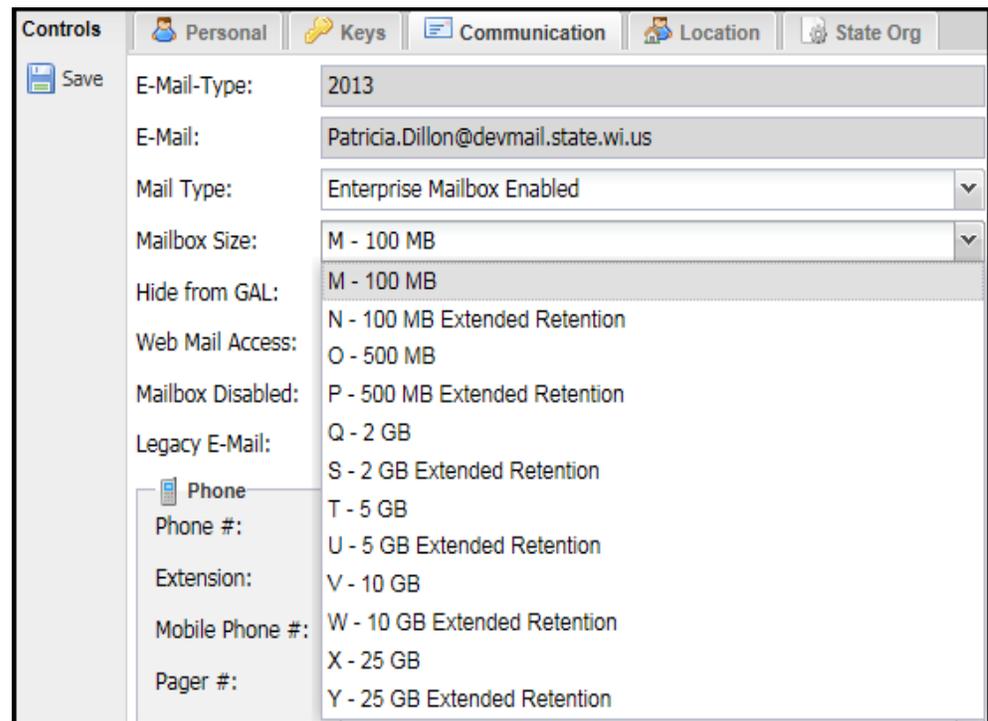
*No-Mail* is for staff with an IAM Userid, but no email account.



All Mail Type entries of External Mail Enable must have a Legacy email address put in the **Legacy E-Mail** field. The values entered in the Legacy E-Mail field must be unique. No two IAM Userids can have the same value in the Legacy E-Mail field.

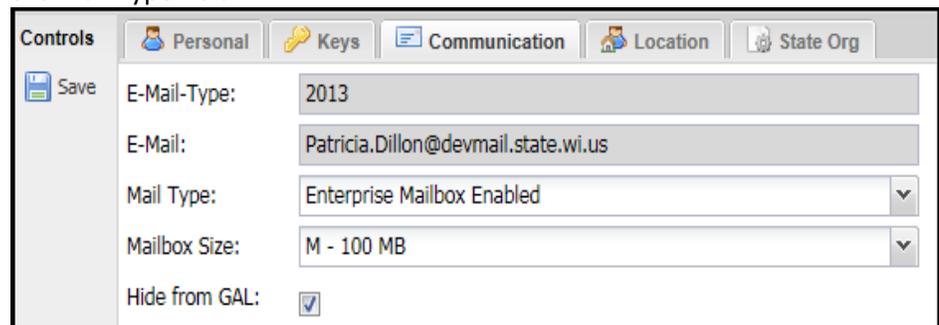


13. The **Mailbox Size** field is specific on IAM Userids that are used for Enterprise Email only. To specify a size (or class) for the **Mailbox Size** press the drop down button. Click on the mailbox size (or class) that is desired. This field will have no impact on mail types of External Mail Enabled or No Mail.



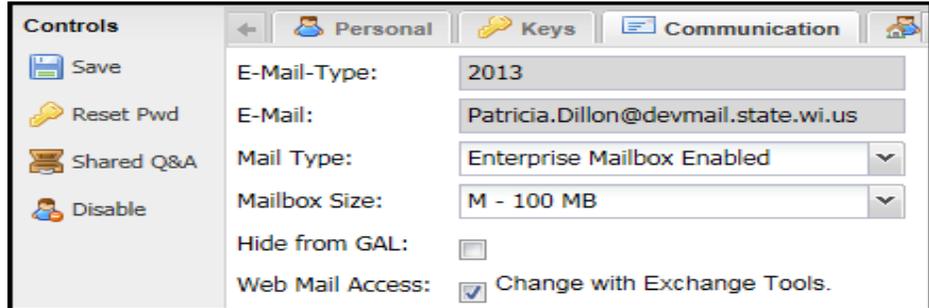
The screenshot shows the 'Controls' window with the 'Communication' tab selected. The 'Mailbox Size' field is set to 'M - 100 MB'. The 'Mail Type' is set to 'Enterprise Mailbox Enabled'. The 'Hide from GAL' field is set to 'M - 100 MB'. The 'Web Mail Access' field is set to 'O - 500 MB'. The 'Mailbox Disabled' field is set to 'P - 500 MB Extended Retention'. The 'Legacy E-Mail' field is set to 'Q - 2 GB'. The 'Phone' field is set to 'T - 5 GB'. The 'Phone #' field is set to 'U - 5 GB Extended Retention'. The 'Extension' field is set to 'V - 10 GB'. The 'Mobile Phone #' field is set to 'W - 10 GB Extended Retention'. The 'Pager #' field is set to 'X - 25 GB'. The 'Pager #' field is also set to 'Y - 25 GB Extended Retention'.

14. The default value for **Hide From GAL** is an unchecked box. You can override this by checking the box with your mouse to not to have an entry for this Email address show up in the Enterprise GAL. This field will not show if No Mail is in the Mail Type field.



The screenshot shows the 'Controls' window with the 'Communication' tab selected. The 'Mailbox Size' field is set to 'M - 100 MB'. The 'Hide from GAL' field is checked, indicating that the email address will not show up in the Enterprise GAL.

15. The default value for **Web Mail Access** is normally a checked box, but this can vary from agency to agency. In order to change this setting, you need to use the Exchange Admin Center (ECP). To obtain access to this application, please refer to section 14 of the IAM Security Admin Guide. This field will not show if External Mail Enabled or No Mail is in the Mail Type field.



The screenshot shows the 'Communication' tab in the ECP. The 'Web Mail Access' checkbox is checked, and the text 'Change with Exchange Tools.' is visible next to it. Other settings include E-Mail-Type: 2013, E-Mail: Patricia.Dillon@devmail.state.wi.us, Mail Type: Enterprise Mailbox Enabled, and Mailbox Size: M - 100 MB.

16. The default value for **Mailbox Disabled** is an unchecked box. This field will not show if External Mail Enabled or No Mail is in the Mail Type field. By checking **Mailbox Disabled** the box after **Hide from GAL** will also become checked. Mailbox Disabled will prevent this id from sending and receiving email.



The screenshot shows the 'Communication' tab in the ECP. The 'Mailbox Disabled' checkbox is checked. Other settings are the same as in the previous screenshot: E-Mail-Type: 2013, E-Mail: Patricia.Dillon@devmail.state.wi.us, Mail Type: Enterprise Mailbox Enabled, and Mailbox Size: M - 100 MB.

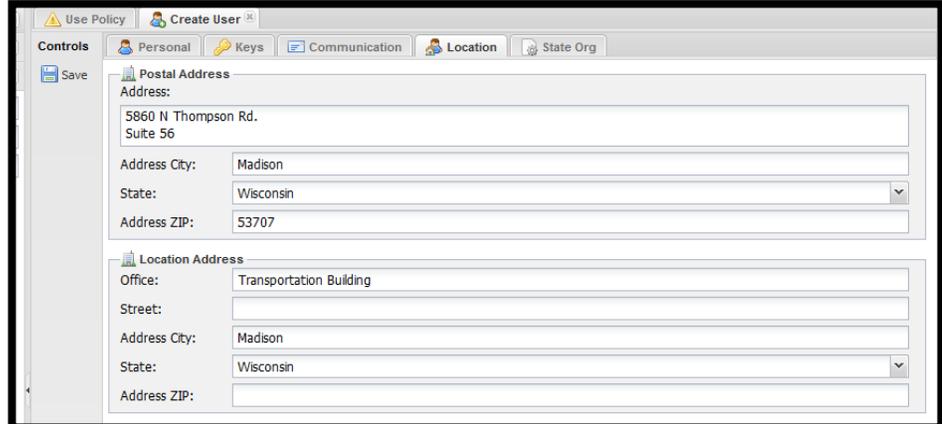
17. In the lower half of the **Communication** tab you will find the **Phone** section. This section consists of the **Phone #**, **Extension**, **Mobile Phone #**, **Pager #** **Fax #** and **Assist. Phone #** fields. All these fields are optional. Each of these fields (except Extension) will expect an **nnn nnn-nnnn** format.



The screenshot shows the 'Phone' section with the following fields and values: Phone #: 999 999-9999, Extension: 9999, Mobile Phone #: 999 999-9999, Pager #: 999 999-9999, Fax #: 999 999-9999, and Assist. Phone #: 999 999-9999.

### LOCATION TAB

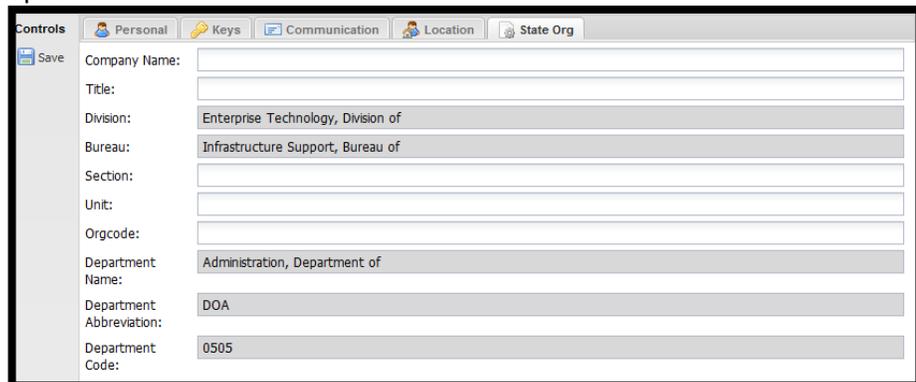
18. Click on the **Location** tab. Two sections are under this tab (Postal Address and Location Address) and all fields in these sections are optional. The Postal Address section reflects an employee's USPS mailing address. The Location Address section reflects an employee's State Inter-d location.



The screenshot shows the 'Postal Address' and 'Location Address' sections of the user creation interface. The 'Postal Address' section includes fields for Address (5860 N Thompson Rd., Suite 56), Address City (Madison), State (Wisconsin), and Address ZIP (53707). The 'Location Address' section includes fields for Office (Transportation Building), Street, Address City (Madison), State (Wisconsin), and Address ZIP.

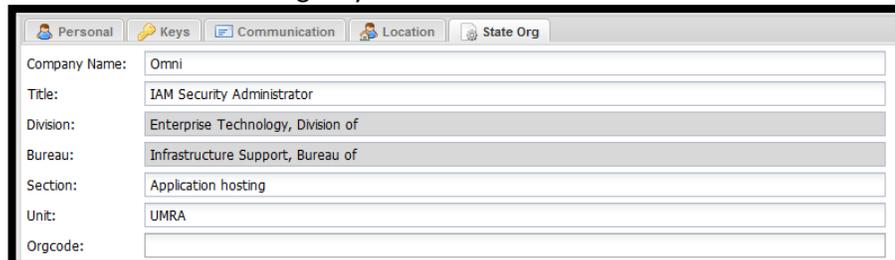
### STATE ORG TAB

- Click on the **State Org** tab. Agencies using sub OU's under their agency OU will find at least the **Division** field filled in for them. They could also see values in the **Bureau** field. Everyone will see that the **Department name, Department Abbreviation** and **Department Code** fields filled in. All remaining fields are optional.



The screenshot shows the 'State Org' tab in the user creation interface. The fields are filled with the following values: Company Name, Title, Division (Enterprise Technology, Division of), Bureau (Infrastructure Support, Bureau of), Section, Unit, Orgcode, Department Name (Administration, Department of), Department Abbreviation (DOA), and Department Code (0505).

- The **Company Name** is best used for the name of consultant firms. The **Title** field is meant to be used for position titles. The **Section** and **Unit** fields are used for further break down of the employee's location within the agency. The **Orgcode** field can be used as an agency desires.



The screenshot shows the 'State Org' tab in the user creation interface with the following values: Company Name (Omni), Title (IAM Security Administrator), Division (Enterprise Technology, Division of), Bureau (Infrastructure Support, Bureau of), Section (Application hosting), Unit (UMRA), and Orgcode.

### FINISHING THE NEW USERID

- Press the **Save** button.



Controls Personal Keys Communication Location

Save Company Name: Omni

Title: IAM Security Administrator

Division: Enterprise Technology, Division of

22. A **Password Options** box pops up. By default the “**I will specify a password**” option is selected. You can accept this default and enter in the initial password twice. Once in the **Password** field, and once in the **Verify** field. Press the **Create User** button.



Password Options

Automatically generate a new password

I will specify a password

Password: \_\_\_\_\_

Verify: \_\_\_\_\_

Create User Cancel

23. By selecting the **Automatically generate a new password** option the system will generate the new password and tell you in the next panel what that password is. Press the **Create User** button.



Unit: UMRA

Password Options

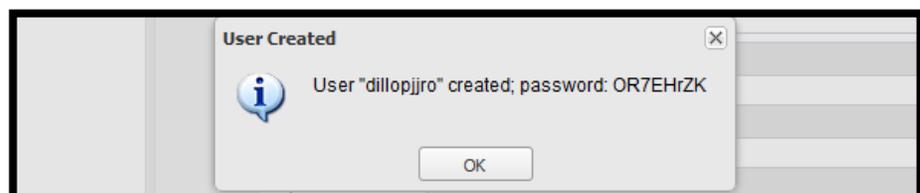
Automatically generate a new password

I will specify a password

Create User Cancel

Code: \_\_\_\_\_

24. The **User Created** box will show you the name of the Userid created along with the initial password for the Userid. Press the **OK** button.



User Created

User "dilloppjro" created; password: OR7EHrZK

OK

### New Userid Activation

25. Follow your agency policy and procedures to provide the owner of the new Userid their IAM Userid and initial password.



- Instruct new Userid owners to go to <https://iam.wisconsin.gov> to ACTIVATE their IAM Userid.
- All new Userid owners should be encouraged to review the **IAM End User Guide**.

## SECTION 3. MANAGE A USER

Follow the procedure below to change a current IAM Userid in UMRA. **This section excludes password changes (covered in section 4) and internal agency Userid transfers (covered in section 13).**

### Sign On To Production UMRA

1. See instructions outlined in Section 1, Step 1.

### Search For an Existing IAM Userid

2. Perform a **Search** to find the person you wish to make changes to. See instructions outlined in Section 1, starting with Step 2.

### Manage an IAM Account

#### MODIFY PERSONAL TAB

**Caution with  
Name Changes**

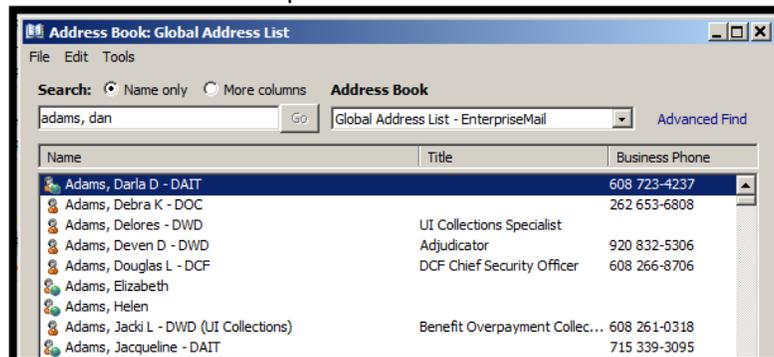
3. On the **Personal** tab you can change the **First Name, Middle Name and Last Name** fields. Keep in mind the following before you do though.
  - a. The **IAM User Name (Userid)** will change if the first 5 characters of the **Last Name** changes, the first initial of the **First Name** changes or the first initial of the **Middle Name** (or sent to NMN) changes. **This cannot be stopped.**
  - b. The **E-Mail** address will change if the **Last Name** or **First Name** of the individual is changed. The **E-Mail** address may also change if the first initial of the **Middle Name** is changed or if **NMN** is added or removed. **This cannot be stopped.**
  - c. A name change that causes the **E-Mail** address to change does NOT mean that the old **E-Mail** address is available for re-assigning. The old **E-Mail** address becomes an alias for the new **E-Mail** address. This is the default action, an agency that wants the old **E-Mail** address removed as an alias, should open up a service request (SR).
  - d. **WARNING:** Tampering with name combinations to get a preferred **E-Mail** address will give you unexpected results. You will be unhappy and your customer will surely be unhappy. Please do not do this.
  - e. The password will not be impacted by an **IAM User Name (Userid)** change. The password will still be the same.

**Timing  
consideration of  
Name Change**

**Should you make a name change that causes the email address to change it can take up to 4 hours before the individuals Exchange SMTP entries are configured correctly. Keep this in mind when doing this change and consider performing such a change during a period of time that the Userid owner is planning on not using their email.**

4. On the **Personal** tab you can change the **Generation Qualifier** and the **Name Resolution** fields.

- a. A **Generation Qualifier** change will impact the **Display Name**, **Common Name** and **E-Mail** fields.
- b. A **Name Resolution** change will impact the **Display Name** and **Common Name** fields. This change will impact the display name in the Enterprise GAL. For example see Jacki L Adams below.



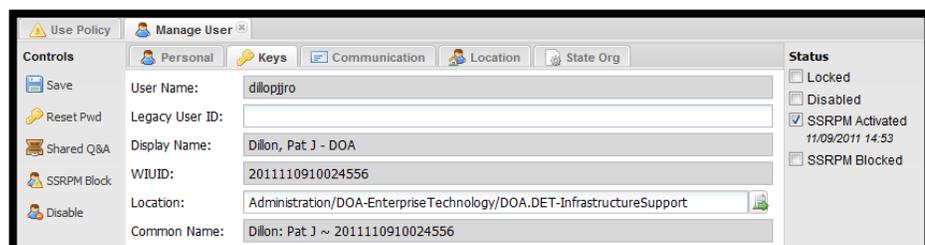
Timing  
consideration of  
Generation  
Qualifier Change.

A **Generation Qualifier** change will cause the email address to change which can take up to 4 hours before the individuals Exchange SMTP entries to be configured correctly. Keep this in mind when doing this change and consider performing such a change during a period of time that the id owner is planning on not using their email.

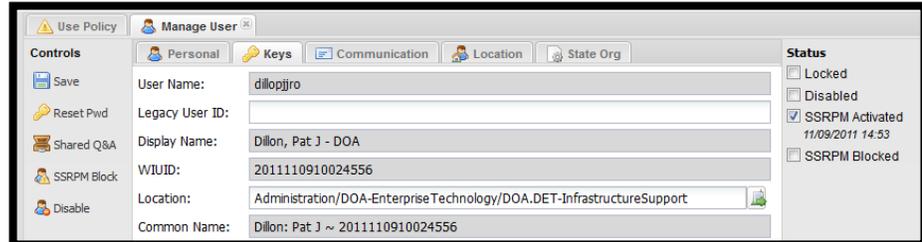
5. On the **Personal** tab you can change the **Employee Type** and **Administrative Notes** fields. Either change will only impact the values in the fields themselves.

#### MODIFY KEYS TAB

6. Click on the **Keys** tab.

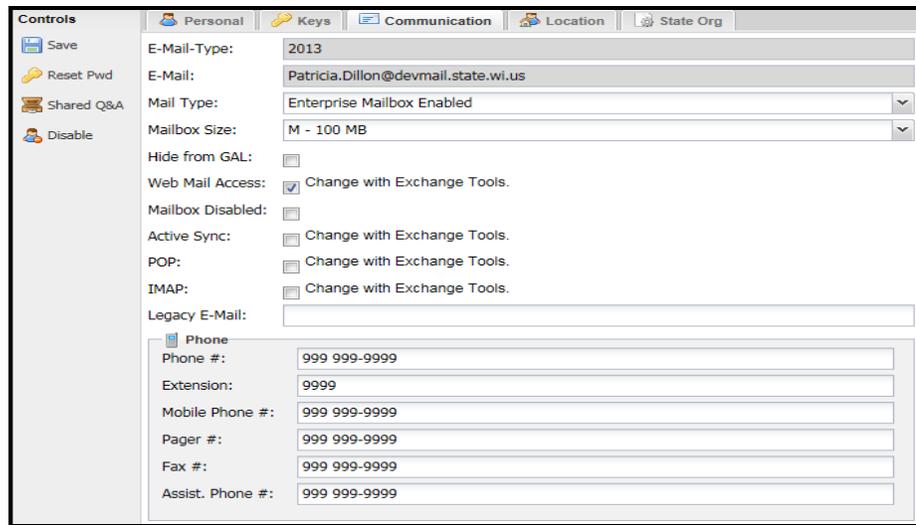


7. Under the **Keys** tab you can change the **Legacy User Id** field. This change will only impact the value in this field.
8. Under the **Keys** tab you can change the **Location** field. This can cause changes in the **Division** and **Bureau** fields under the **State Org**. Please review section 13 of this document going over agency transfers before proceeding with this type of change.

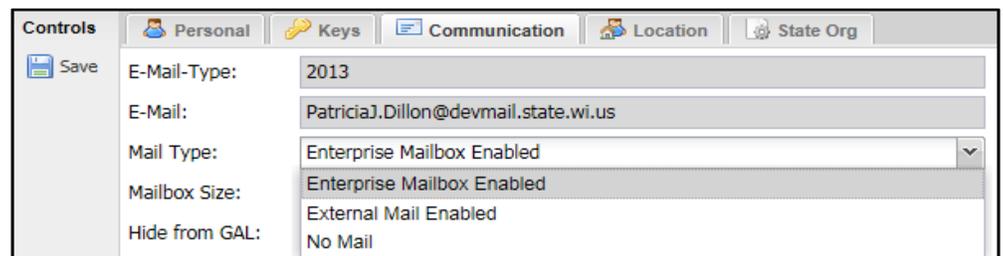


**MODIFY COMMUNICATION TAB**

- Click on the **Communication** tab. The fields in gray are not updateable, as well as checkboxes where “Change with Exchange Tools” are noted.



- To override the value of **Mail Type**, press the drop down button.  
*Enterprise Mailbox Enabled* is for staff using Enterprise Email.  
*External Mail Enabled* is for staff using legacy email.  
*No-Mail* is for staff with an IAM Userid, but no email account.



|      |                |                                      |
|------|----------------|--------------------------------------|
| Save | E-Mail-Type:   | 2013                                 |
|      | E-Mail:        | PatriciaJ.Dillon@devmail.state.wi.us |
|      | Mail Type:     | No Mail                              |
|      | Mailbox Size:  | M - 100 MB                           |
|      | Legacy E-Mail: |                                      |

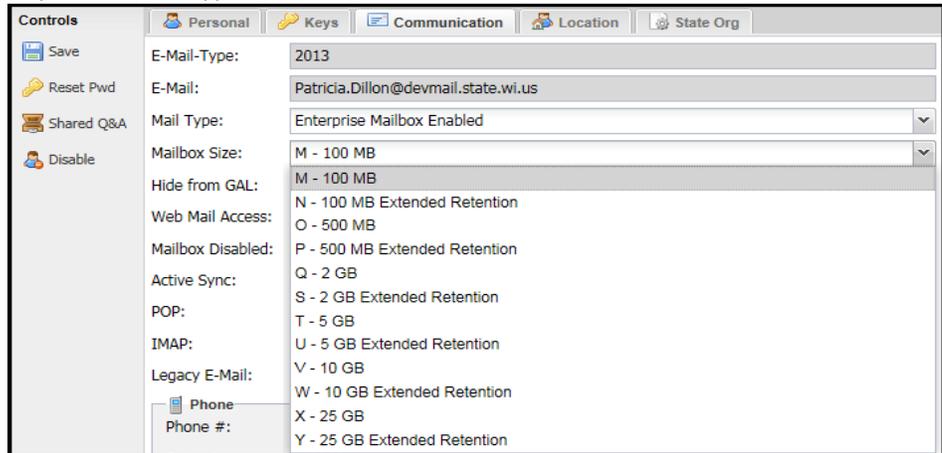
**External Mail Enabled**

A Mail Type value of External Mail Enable must have a Legacy email address put in the **Legacy E-Mail** field. The values entered in the Legacy E-Mail field must be unique. No two IAM Userids can have the same value in the Legacy E-Mail field.

Userids that were created before the agency migrated to Enterprise Email may still have a value in the Legacy E-Mail address. It does not hurt anything.

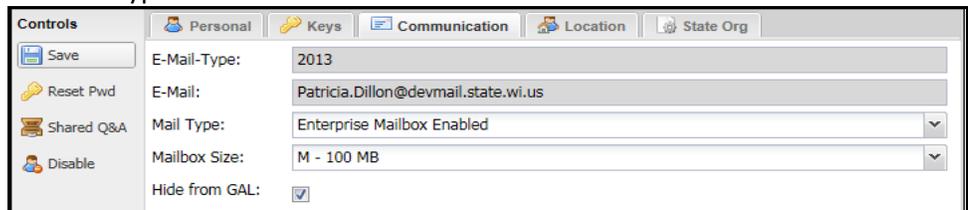
|                 |                |                                      |      |               |          |           |
|-----------------|----------------|--------------------------------------|------|---------------|----------|-----------|
| <b>Controls</b> |                | Personal                             | Keys | Communication | Location | State Org |
| Save            | E-Mail-Type:   | 2013                                 |      |               |          |           |
|                 | E-Mail:        | PatriciaJ.Dillon@devmail.state.wi.us |      |               |          |           |
|                 | Mail Type:     | External Mail Enabled                |      |               |          |           |
|                 | Mailbox Size:  | M - 100 MB                           |      |               |          |           |
|                 | Hide from GAL: | <input type="checkbox"/>             |      |               |          |           |
|                 | Legacy E-Mail: | Patricia.Dillion@doa.state.wi.us     |      |               |          |           |

11. The **Mailbox Size** field is specific on IAM Userids that are used for Enterprise Email only. To specify a size (or class) for the **Mailbox Size** press the drop down button. Click on the mailbox size (or class) that is desired. This field will have no impact on mail types of External Mail Enabled.



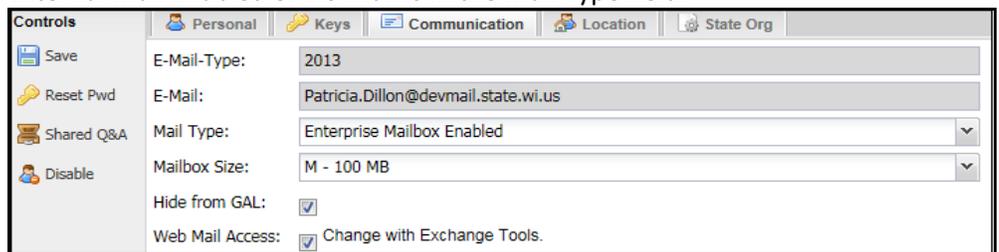
The screenshot shows the 'Communication' tab of the user control panel. The 'Mailbox Size' field is a dropdown menu currently set to 'M - 100 MB'. Other visible fields include 'E-Mail-Type' (2013), 'E-Mail' (Patricia.Dillon@devmail.state.wi.us), 'Mail Type' (Enterprise Mailbox Enabled), 'Hide from GAL' (M - 100 MB), 'Web Mail Access' (O - 500 MB), 'Mailbox Disabled' (P - 500 MB Extended Retention), 'Active Sync' (Q - 2 GB), 'POP' (T - 5 GB), 'IMAP' (U - 5 GB Extended Retention), 'Legacy E-Mail' (V - 10 GB), and 'Phone #' (Y - 25 GB Extended Retention).

12. The default value for **Hide From GAL** is an unchecked box. You can override this by checking the box with your mouse to not to have an entry for this Email address show up in the Enterprise GAL. This field will not show if No Mail is in the Mail Type field.



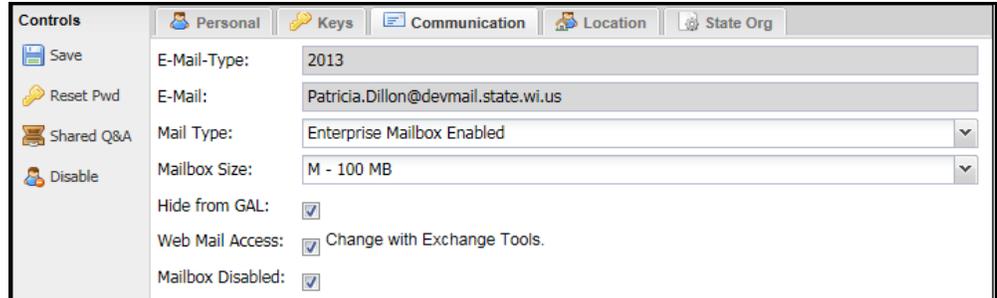
The screenshot shows the 'Communication' tab of the user control panel. The 'Hide from GAL' checkbox is checked. Other visible fields include 'E-Mail-Type' (2013), 'E-Mail' (Patricia.Dillon@devmail.state.wi.us), 'Mail Type' (Enterprise Mailbox Enabled), and 'Mailbox Size' (M - 100 MB).

13. The default value for **Web Mail Access** is normally a checked box, but this can vary from agency to agency. In order to change this setting, you need to use the Exchange Admin Center (ECP). To obtain access to this application, please refer to section 14 of the IAM Security Admin Guide. This field will not show if External Mail Enabled or No Mail is in the Mail Type field.



The screenshot shows the 'Communication' tab of the user control panel. The 'Web Mail Access' checkbox is checked, with the text 'Change with Exchange Tools.' next to it. Other visible fields include 'E-Mail-Type' (2013), 'E-Mail' (Patricia.Dillon@devmail.state.wi.us), 'Mail Type' (Enterprise Mailbox Enabled), 'Mailbox Size' (M - 100 MB), and 'Hide from GAL' (checked).

14. The default value for **Mailbox Disabled** is an unchecked box. This field will not show if External Mail Enabled or No Mail is in the Mail Type field. By checking **Mailbox Disabled** the box after **Hide from GAL** will also become checked.



Controls: Personal, Keys, Communication, Location, State Org

E-Mail-Type: 2013

E-Mail: Patricia.Dillon@devmail.state.wi.us

Mail Type: Enterprise Mailbox Enabled

Mailbox Size: M - 100 MB

Hide from GAL:

Web Mail Access:  Change with Exchange Tools.

Mailbox Disabled:

15. In the lower half of the **Communication** tab you will find the **Phone** section. This section consists of the **Phone #, Extension, Mobile Phone #, Pager # Fax #** and **Assist. Phone #** fields. All these fields are optional. Each of these fields (except Extension) will expect an **nnn nnn-nnnn** format.



Phone

Phone #: 999 999-9999

Extension: 9999

Mobile Phone #: 999 999-9999

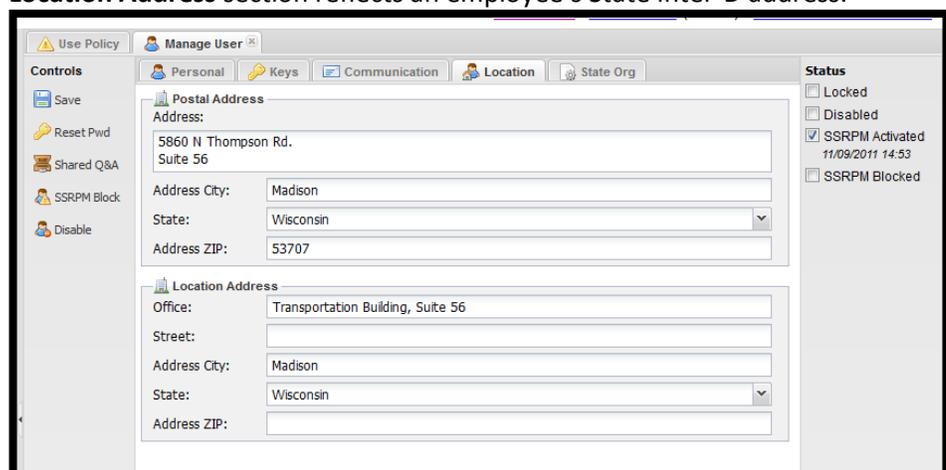
Pager #: 999 999-9999

Fax #: 999 999-9999

Assist. Phone #: 999 999-9999

### MODIFY LOCATION TAB

16. Click on the **Location** tab. Two sections are under this tab (**Postal Address** and **Location Address**) and all fields in these sections are optional.
17. The **Postal Address** section reflects an employee's USPS mailing address. The **Location Address** section reflects an employee's State Inter-D address.



Use Policy Manage User

Controls: Personal, Keys, Communication, Location, State Org

Postal Address

Address: 5860 N Thompson Rd.  
Suite 56

Address City: Madison

State: Wisconsin

Address ZIP: 53707

Location Address

Office: Transportation Building, Suite 56

Street:

Address City: Madison

State: Wisconsin

Address ZIP:

Status

Locked

Disabled

SSRPM Activated  
11/09/2011 14:53

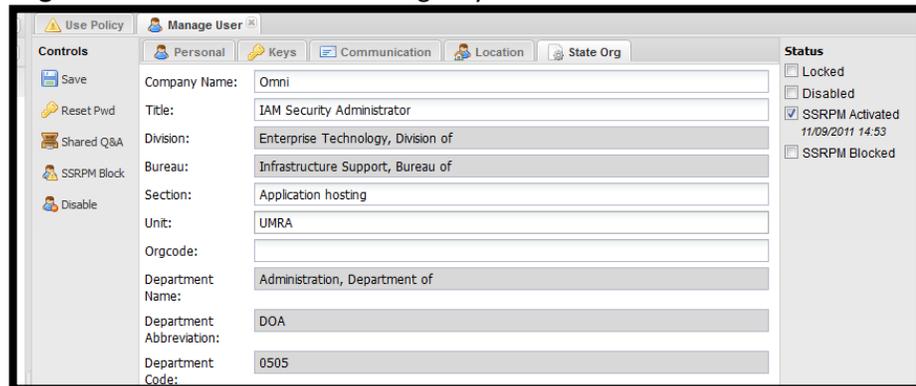
SSRPM Blocked

### MODIFY THE STATE ORG TAB

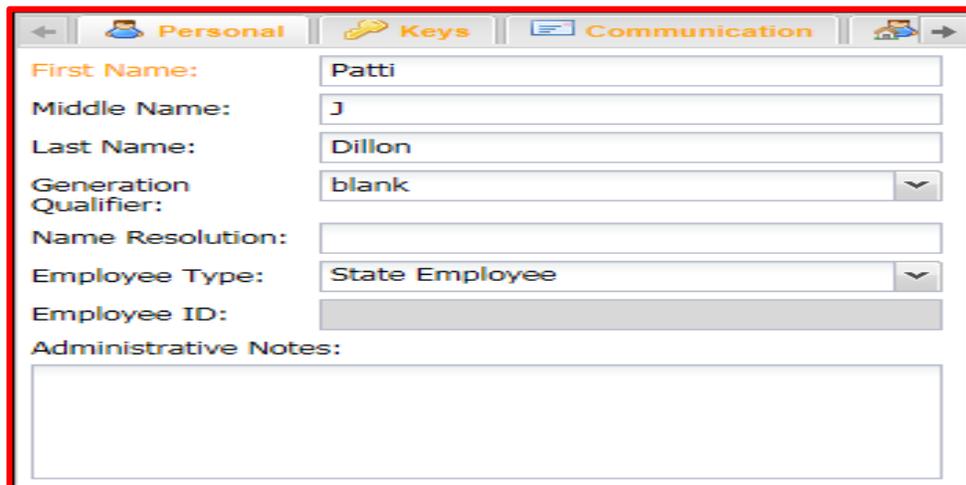
18. Click on the **State Org** tab. Agencies using sub OU's under their agency OU will find at least the **Division** field filled in for them. They could also see values in the

**Bureau** field. These fields are locked if the field is shaded and cannot be edited by the security administrator. These fields are propagated as a result of the value in the **LOCATION** field under the **Keys** tab.

19. On the **State Org** tab everyone will see that the **Department Name**, **Department Abbreviation** and **Department Code** fields filled in. You will also notice that these fields are shaded and cannot be edited by the security administrator.
20. The **Company Name** is best used for the name of a consultant firm. The **Title** field is meant to be used for position titles. The **Section** and **Unit** fields are used for further break down of the employee's location within the agency. The **Orgcode** field can be used as the agency desires.



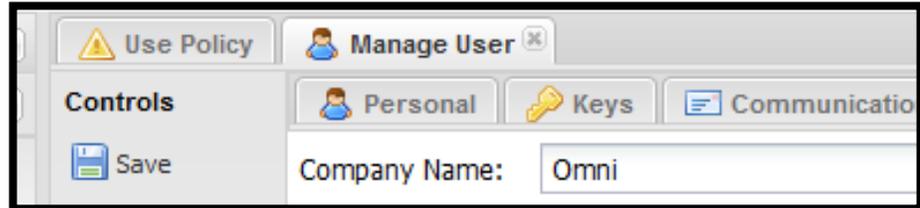
As you make changes to the Userid record you will see that the titles of the fields that are modified change color. You will also notice that tabs that have fields that are modified on them also change colors.



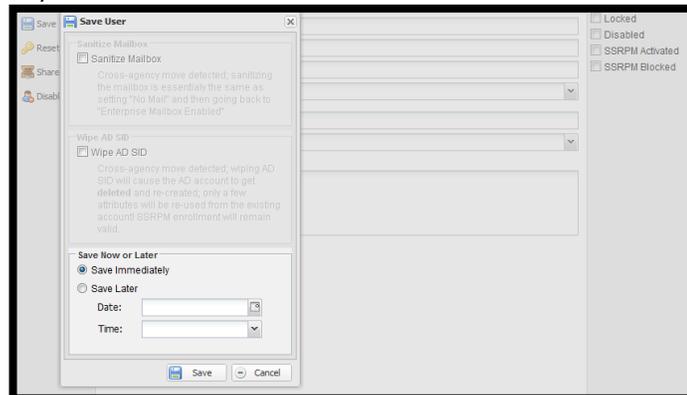
In the example above I have changed the **First Name** from 'Patricia' to 'Patti'. Note that the field name of **First Name** has changed from black to **yellow**. Also notice the color of the tabs of **Personal**, **Keys** and **Communications** has changed from black to **yellow**.

### SAVE THE MODIFICATIONS

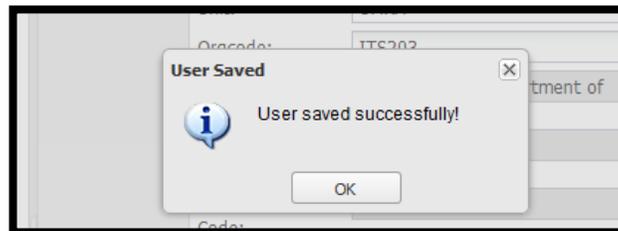
21. Press the **Save** button under the **Controls** column.



22. A **Save User** box pops up giving you the option to **Save Immediately** (by default) or to schedule the change for a **Save Later** date and time (reviewed in section 11). Press the **Save** button.



23. A **User Saved** box comes up stating 'User saved successfully!' Press the **OK** button.



24. **To view your change close all tabs related to this Userid. Repeat the search steps to find this Userid (a new pull) and then select the Userid from the new pull.**

### Status Column

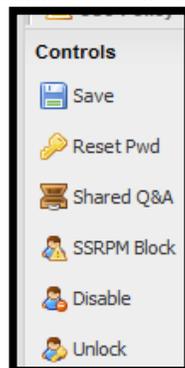
You will notice on the right side of the panel a **Status** column.



- A check in the box before **Locked** means that the Userid is password suspended (too many invalid password attempts). The owner can no longer sign on using this Userid.
- A check in the box before **Disabled** means that the Userid has been disabled by an agency IAM Security Administrator or has been disabled because of lack of use (no Userid usage for over 6 months).
- A check in the box before **SSRPM Activated** means that the Userid has successfully gone through the Account Activation process (via SSRPM). You will also notice the date and time that the owner last made changes to their Challenge Response questions or their Shared Secret question.
- A check in the box before **SSRPM Blocked** means that the Userid made more than 4 invalid attempts to recovery their password using Account Recovery (via SSRPM) within a 20 minute period. The Userid can no longer use Account Recovery to recover their Userid and an agency IAM Security Administrator must assign the Userid a new password.

### Control Column

You will notice in the middle of the screen a column with the title of **Controls**.



- **SAVE:** Save changes you have made to a Userid.
- **Reset Pwd:** Reset the password on the Userid. The password reset process is outlined in Section 4 of this guide.
- **Shared Q&A:** See owner's shared secret question/answer. A box will come up with this information. You will use this information as part of the password reset process that is outlined in Section 4 of this guide.
- **SSRPM Block:** Disable a Userids ability to use IAM Self Care (SSRPM). See Section 5 for more information.
- **Disable:** Prevent a Userid from being used to sign on to an application. A disabled Userid can only be Enabled by an agency security administrator. See Section 5 for more information.
- **Enable:** Allow a Userid that is Disabled to be used (with no password change made). See Section 5 for more information.
- **Unlock:** Allow a Userid that is **Locked** to be used (with no password change made). See Section 5 for more information.



## SECTION 4. PROCEDURE FOR CHANGING A PASSWORD

Follow the procedure below to change the password of a current IAM Userid using UMRA.

### Sign On To Production UMRA

1. See instructions outlined in Section 1, Step 1.

### Search For an Existing IAM Userid

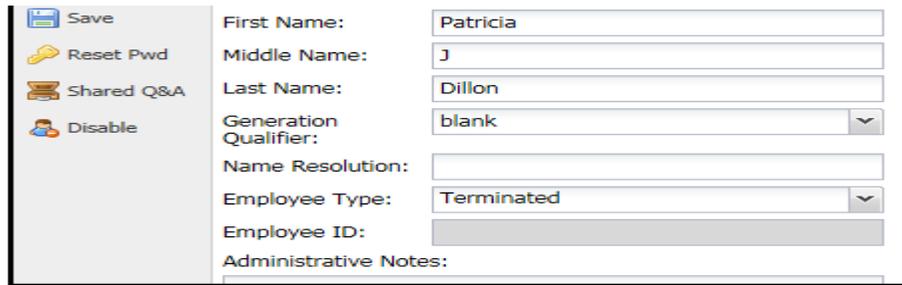
2. Perform a **Search** to find the person you wish to change their password. See instructions outlined in Section 1, starting with Step 2.

**Account Recovery?**

The process below should be followed in the situations that the customer has already attempted and failed Account Recovery (see the IAM End User Guide for instructions). Walk your customer through Account Recovery in SSRPM if they have not attempted already.

**Check this out**

**Do not go any further when the Employee Type field value is TERMINATED until you determine first if this employee is still working for you.**

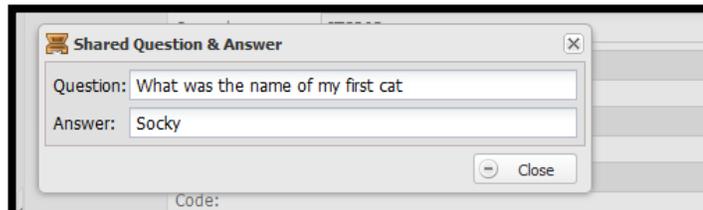


|            |                       |            |
|------------|-----------------------|------------|
| Save       | First Name:           | Patricia   |
| Reset Pwd  | Middle Name:          | J          |
| Shared Q&A | Last Name:            | Dillon     |
| Disable    | Generation Qualifier: | blank      |
|            | Name Resolution:      |            |
|            | Employee Type:        | Terminated |
|            | Employee ID:          |            |
|            | Administrative Notes: |            |

### Start the Password Change Process

#### CONFIRM IDENTITY

3. Press on the **Shared Q&A** button under the **Controls** column in the middle of the screen to see Userid owner's Shared Secret Question & Answer. Ask the caller to confirm the answer to their Shared Secret Question/Answer. Press the **CLOSE** button. **Follow your agency procedures for caller verification if the caller cannot answer their Shared Secret.**



Shared Question & Answer

Question: What was the name of my first cat

Answer: Socky

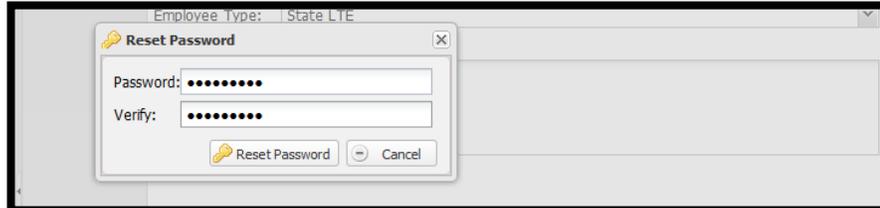
Code: [ ]

Close

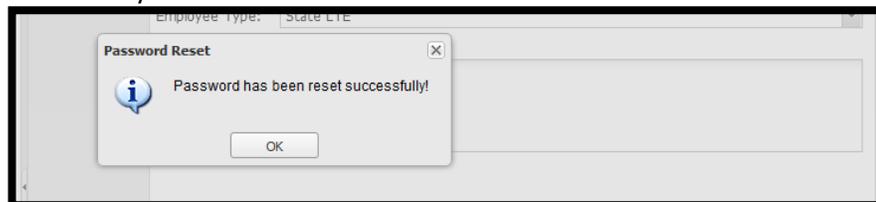
**An IAM Userid that does NOT have a Shared Secret Question & Answer has NOT completed IAM Account Activation. The Userid owner MUST complete their Account Activation. Follow your agency procedures in this situation.**

### CHANGE PASSWORD

4. Press the **Reset Pwd** button under the **Control** column. A '**Reset Password**' will appear. Enter in a new password identically 2 times, once in the **Password:** field and again in the **Verify:** field. Press the **Reset Password** button.



5. A '**Password Reset**' box will come up saying 'Password has been reset successfully'. Press the **OK** button.



### PASSWORD REQUIREMENTS

The IAM technical implementation enforces these requirements:

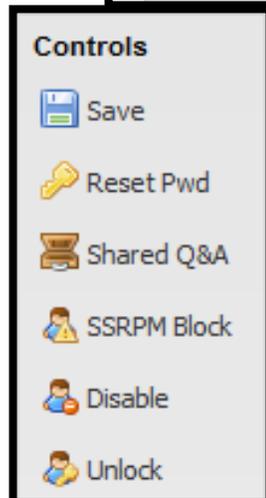
- The last 8 passwords cannot be reused.
- Passwords must be changed every **60 days**.
- Passwords must be 7–20 characters in length.
- Passwords must contain at least three of the following categories of characters:
  - Uppercase letters (ABC...)
  - Lowercase letters (abc...)
  - Numerals 0 to 9
  - Symbols found on the keyboard
- Passwords may not include your user ID or department abbreviation.
- Passwords cannot match your first name, middle name or last name (3 characters or greater).

System administrators, security administrators, or agency IAM password changers are requested to manually and voluntarily follow the following password change requirement

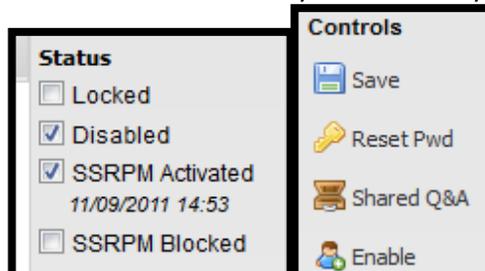
- Passwords must be changed every **30 days**.

### HANDLING LOCKED AND DISABLED USERIDS

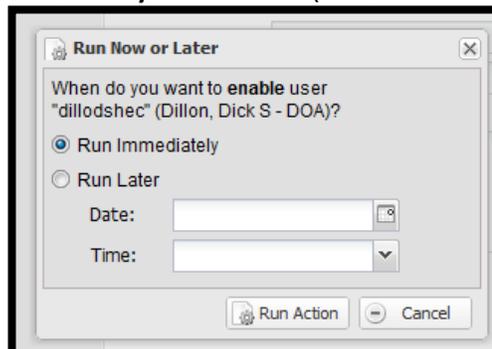
6. Changing a password will automatically **UNLOCK** a Userid that is **Locked** and **UNBLOCK** a Userid that is **SSRPM Blocked**. Using the **Unlock** button under the **Controls** column will **UNLOCK** a userid that is **Locked** and not change the current password. This can be done by both an agency security administrator and a password changer.



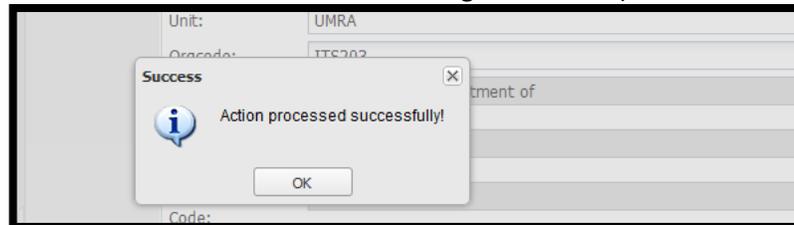
7. Changing a password will not automatically Enable a Userid that is **Disabled**. To enable a Userid you press the **Enable** button that is under the **Controls** column. A Disabled Userid can only be enabled by an agency security administrator.



8. The **Run Now or Later** box will come up. You have the option to **Run Immediately** or **Run Later** (review in Section 11). Press the **Run Action** button.



9. A **Success** box will appear saying 'Action processed successfully!' Press the **OK** button. Note that the Userid is no longer **Disabled** (under the **Status** column).



#### What Userid Owners Should Do After a Password Change

- Instruct Userid owners to change their password after an agency security administrator or password changer has done it for them.
- Instruct Userid owners to recreate their Challenge/Response questions via Account Management. For these instructions go to the IAM End Users Guide.

## SECTION 5. “LOCKED” VERSUS “BLOCKED” VERSUS “DISABLED”

**Disable (step 3) / Enable (step 13):** A Userid that is **disabled** can only be **enabled** by an agency security officer, not a password changer. A Userid can become **disabled** by:

- (1) an agency security officer manually pressing the disabled button in the Userid record. Disabling an IAM Userid may be necessary when staff are on leave of absence, extended sick leave, or at the request of management.
- (2) the weekly inactivity (stale) report showing the Userid has not been used in over 6 months.

**SSRPM Block (step 19):** A **blocked** Userid is caused by more than 4 unsuccessful attempts within a 20 minute period to recover a password using the IAM Home page. An unsuccessful attempt is caused by invalid answers to the Userid owner’s **Challenge Response** questions. An agency security officer can manually block a Userid as well. There are 2 ways to remove a block.

- (1) A password change by an agency security officer will remove the **block**.
- (2) A password change by an agency password changer will remove the **block**.

**Lock / Unlock (step 22):** A **locked** Userid is caused by more than 4 invalid password attempts within a 20 minute period. A Userid that has become **locked** can be:

- (1) **unlocked** by an agency security officer with or without a password change.
- (2) **unlocked** by an agency password changer with or without a password change.
- (3) **unlocked** by the Userid owner using IAM Home to select **Unlock Account** (without a password change) or **Account Recovery** (with a password change).

### Sign On To Production UMRA

1. See instructions outlined in Section 1, Step 1.

### Search For an Existing IAM Userid

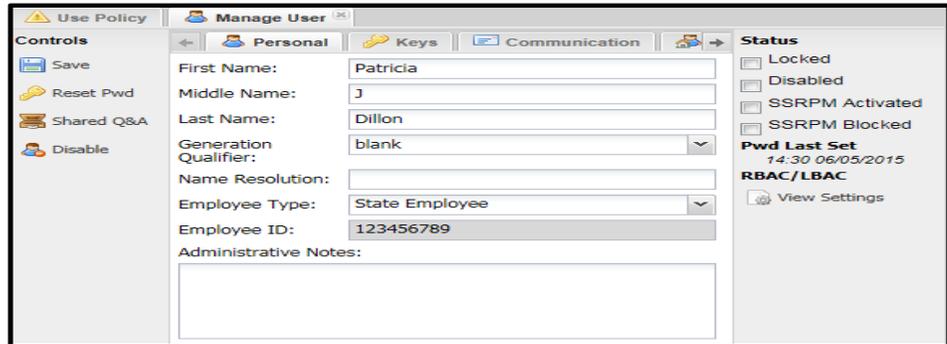
2. Perform a **Search** to find the person you wish to work with. See instructions outlined in Section 1, starting with Step 2.

**STOP**

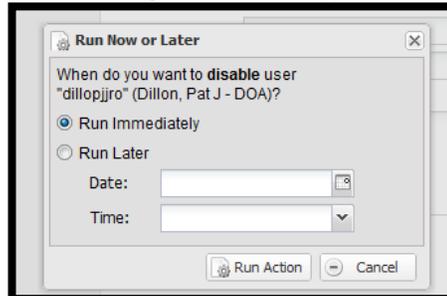
You may not do the following to a Userid that is located under another agency OU that you are not authorized for.

**Disable a Userid**

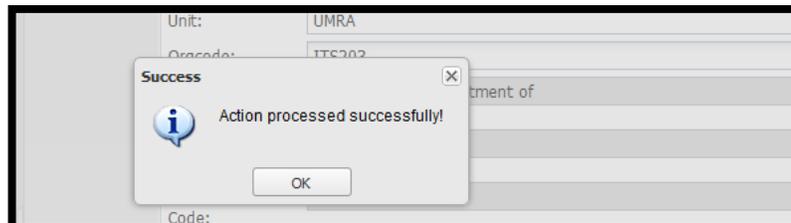
3. Press the **Disable** button on the **Controls** column to disable and active IAM Userid. Keep in mind, only an agency security administrator can enable the Userid.



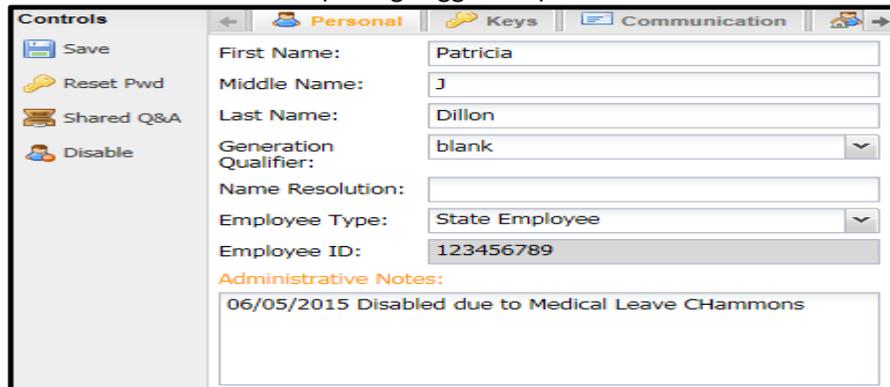
4. The **Run Now or Later** box will come up. You have the option to **Run Immediately** or **Run Later** (reviewed in Section 11). Press the **Run Action** button.



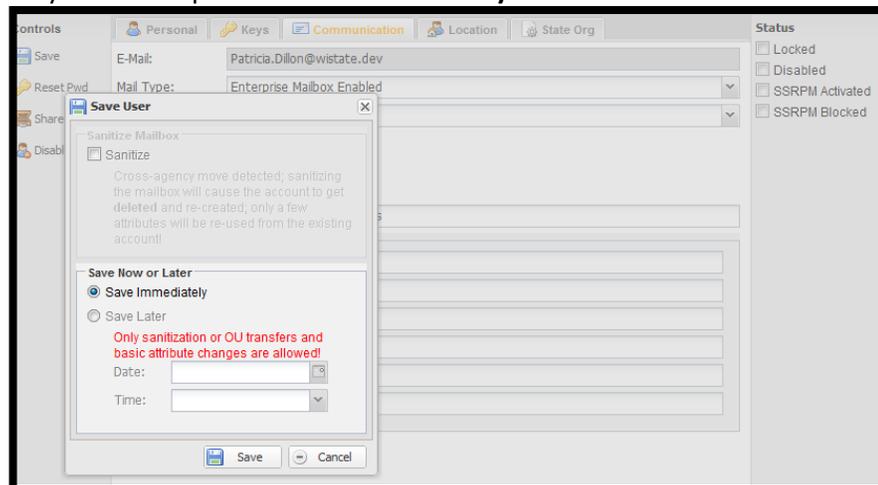
5. A **Success** box will appear saying 'Action processed successfully!' Press the **OK** button.



6. Under the **Personal** tab, put a notation, change date, and initials in the **Administrative Note** field (strong suggestion).



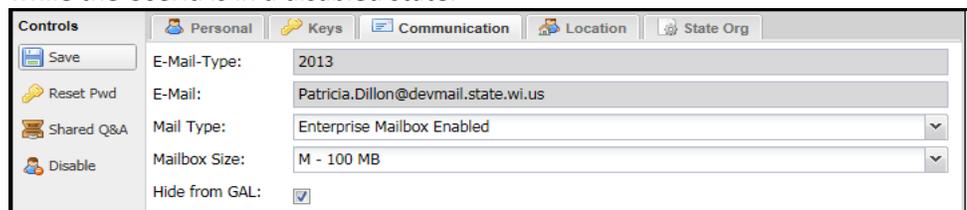
- Press the **SAVE** button. A **Save User / Save Now or Later** box will come up. You only have the option to **Save Immediately**. Press the **Save** button.



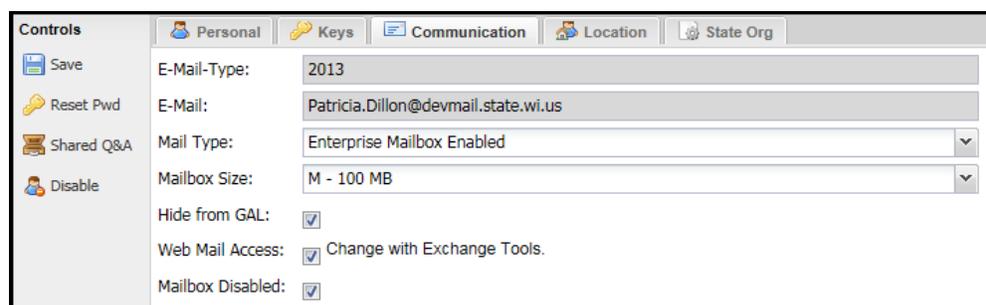
- A **User Saved** box will come up saying 'user saved successfully!' Press the **OK** box.



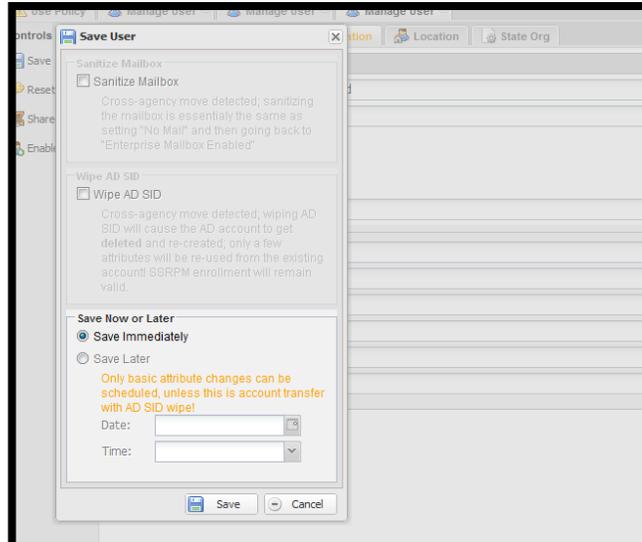
- Under the **Communication** tab, customers using **Mail Type Enterprise Mailbox Enabled** or **External Mail Enabled** can check the box after **Hide from GAL**. This will prevent an entry for this mailbox showing in the Enterprise Exchange GAL while the Userid is in a disabled state.



- Customers that are using **Enterprise Email** can disable the mailbox to keep it from receiving or sending email. This can be done by clicking the box after **Mailbox Disabled**.



- Press the **SAVE** button. A **Save User / Save Now or Later** box will come up. You only have the option to **Save Immediately**. Press the **Save** button.



- A **User Saved** box will come up saying 'user saved successfully!' Press the **OK** box.

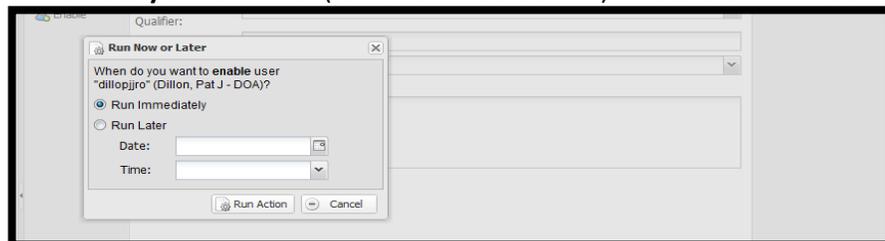


### Enable a Userid

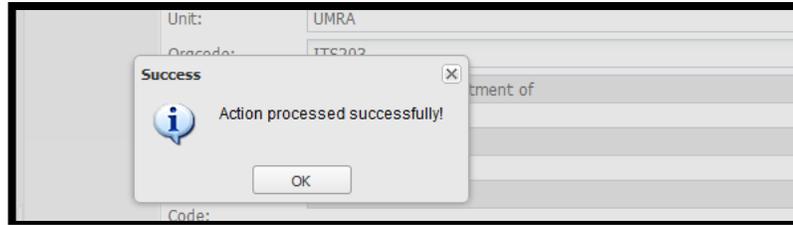
- Press the **Enable** button on the **Controls** column to enable a disabled IAM Userid. Keep in mind, only an agency security administrator can enable the Userid.



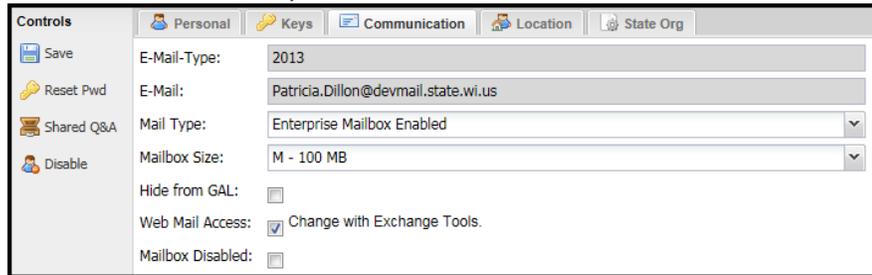
- The **Run Now or Later** box will come up. You have the option to **Run Immediately** or **Run Later** (reviewed in Section 11). Press the **Run Action** button.



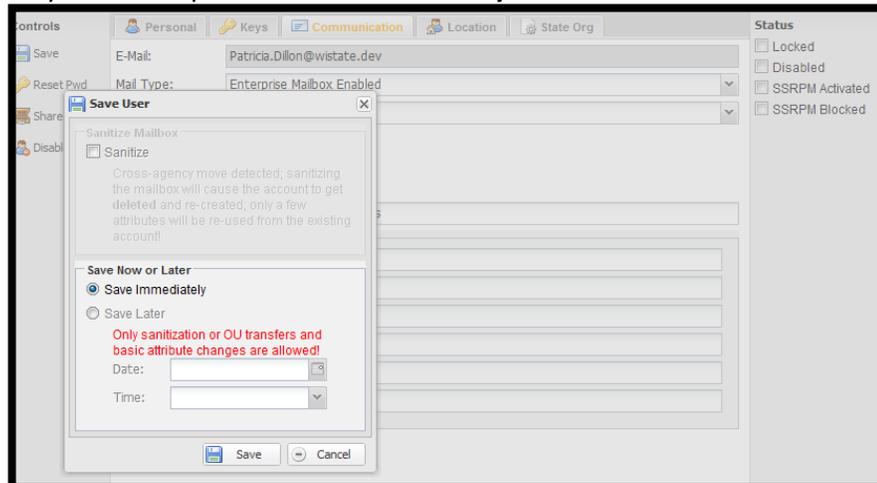
15. A **Success** box will appear saying ‘Action processed successfully!’ Press the **OK** button.



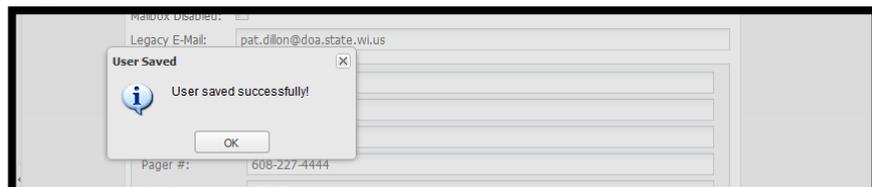
16. Go to the **Communication** tab. Uncheck the boxes after **Hide from GAL** and **Mailbox Disabled** if they are checked.



17. Press the **SAVE** button. A **Save User / Save Now or Later** box will come up. You only have the option to **Save Immediately**. Press the **Save** button.

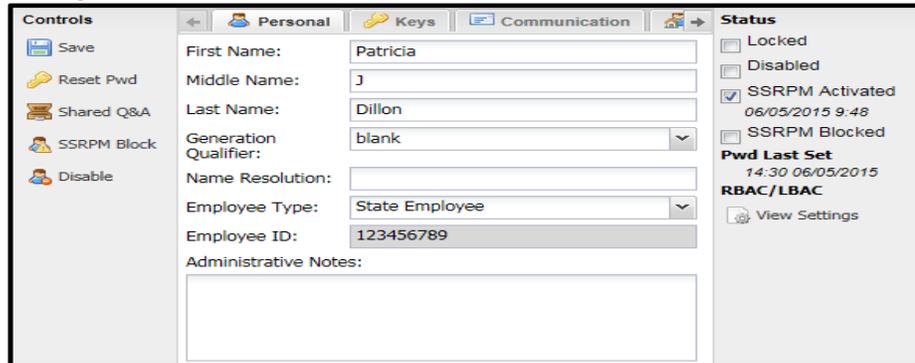


18. A **User Saved** box will come up saying ‘User saved successfully!’ Press the **OK** box.

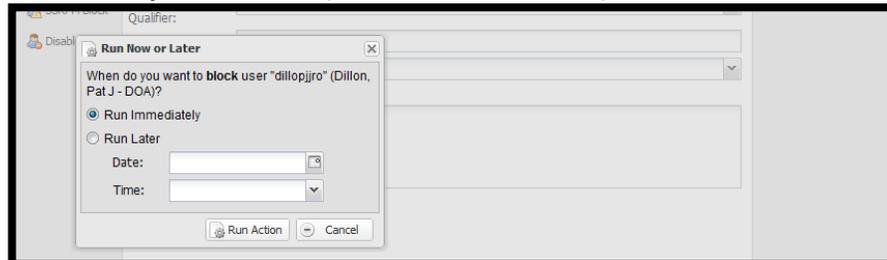


**SSRPM Block**

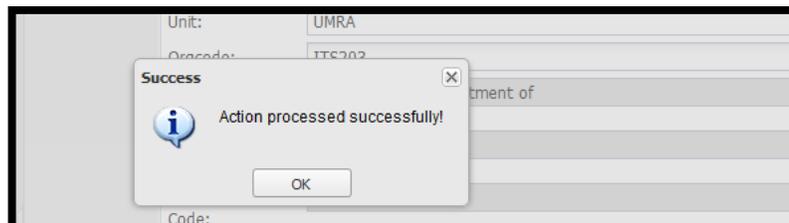
19. To keep a Userid from using the IAM Home page press the **SSRPM Block** button.  
**NOTE: This button will not show if the Userid you are looking at has never gone through Account Activation.**



20. The **Run Now or Later** box will come up. You have the option to **Run Immediately** or **Run Later** (reviewed in Section 11). Press the **Run Action** button.

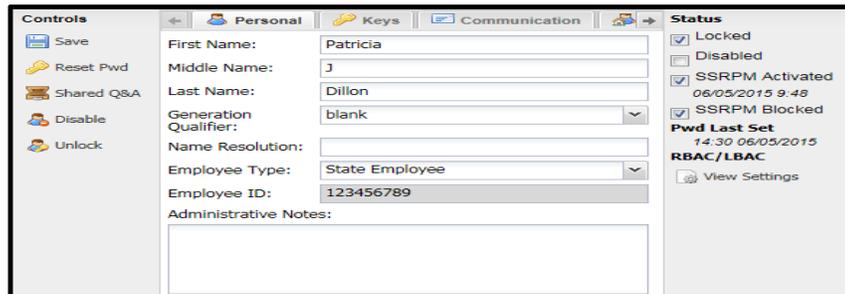


21. A **Success** box will appear saying 'Action processed successfully!' Press the **OK** button.

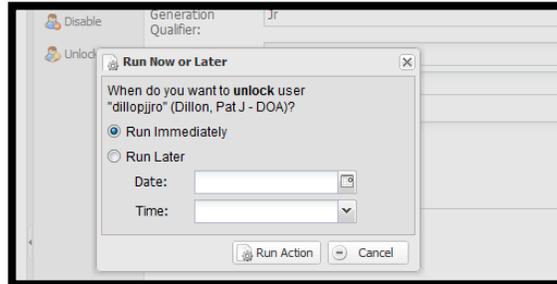


**Unlock a Userid**

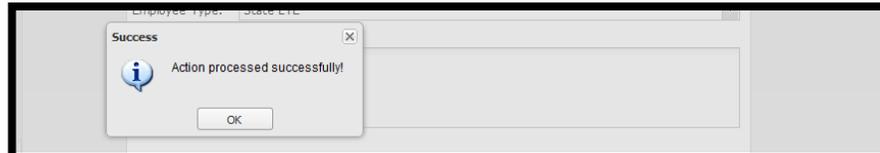
22. Press the **Unlock** button on the **Controls** column to unlock a **Locked** IAM Userid.



23. The **Run Now or Later** box will come up. You have the option to **Run Immediately** or **Run Later** (reviewed in Section 11). Press the **Run Action** button.



24. A **Success** box will appear saying 'Action processed successfully!' Press the **OK** button.



## SECTION 6. DELETING A USERID

Follow these instructions to properly delete an IAM Userid. Please read through this section in its entirety before starting the delete process.

### Sign On To Production UMRA

1. See instructions outlined in Section 1, Step 1.

### Search For an Existing IAM Userid

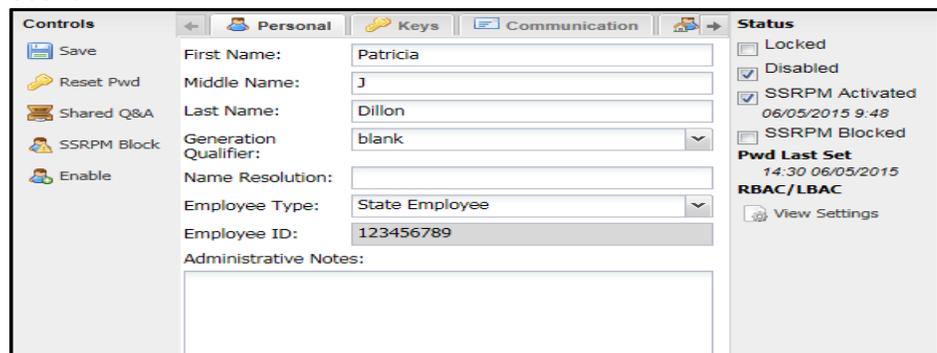
2. Perform a **Search** to find the person you wish to work with. See instructions outlined in Section 1, starting with Step 2.

### Search Results Decision Point

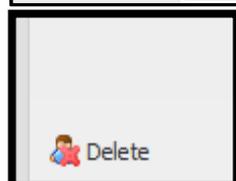
- You may not proceed with a delete if the individual's Userid is located under another agency OU.
- You may disable the Userid (follow direction in Section 5, starting with step 3) if you locate the individual under one of your agencies OU's and you wish to only disable the Userid until you are actually ready to delete the Userid. **Agencies that have migrated to Enterprise Email must work with their agency Delegated Exchange Administrator to make all necessary copies of the mailbox belonging to the individual that is being deleted. This must be completed before the UMRA account is deleted.**
- You may proceed to **Delete a Userid** below if you locate the individual under one of your agencies OU's and you are ready to delete the Userid from UMRA immediately.

### Delete a Userid

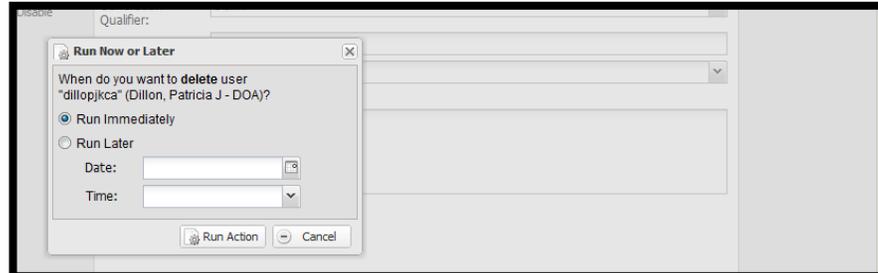
3. Press the **Delete** button on the bottom of the **Controls** column to delete an IAM Userid.



The screenshot shows a user management interface with a 'Controls' column on the left and a 'Status' column on the right. The 'Controls' column contains buttons for 'Save', 'Reset Pwd', 'Shared Q&A', 'SSRPM Block', and 'Enable'. The 'Status' column contains checkboxes for 'Locked', 'Disabled', 'SSRPM Activated', and 'SSRPM Blocked', along with 'Pwd Last Set' and 'RBAC/LBAC' information. The user details for 'Patricia J. Dillon' are displayed in the center, including fields for First Name, Middle Name, Last Name, Generation Qualifier, Name Resolution, Employee Type, and Employee ID (123456789). The 'Delete' button is highlighted in a red box at the bottom of the 'Controls' column.



- The **Run Now or Later** box will come up. You have the option to **Run Immediately** or **Run Later** (reviewed in Section 11). Press the **Run Action** button.



- A **Success** box comes up saying “Action processed successfully!” Press the **OK** button.



- The account is now gone. In the case of an **'OH NO'** moment open an SR for the DET AD team to request that the account be restored from the last backup. Also, the DET Email Team will have to be involved to recover the Enterprise Mailbox if necessary.

## SECTION 7. CREATING SECONDARY IAM ACCOUNTS (USERIDS)

Secondary IAM Accounts (Userid) will be created by the appropriate agency IAM Security Administrator and will reside under the agencies OU or a sub-OU. The agency IAM Security Administrator will continue to maintain the Userid through the life of the Userid. DET IAM Security will not maintain or reset passwords for the Secondary IAM Accounts (Userids) belonging to a customer agency (unless there is an agreement in place).

A secondary IAM account (Userid) is created for someone that has special privileges in an application that would interfere with the workings of their primary IAM Userid. An example of such a situation that requires a secondary IAM account (Userid) is for Agency Email Administrators requiring Delegated Exchange Administration Rights.

### Sign On To Production UMRA

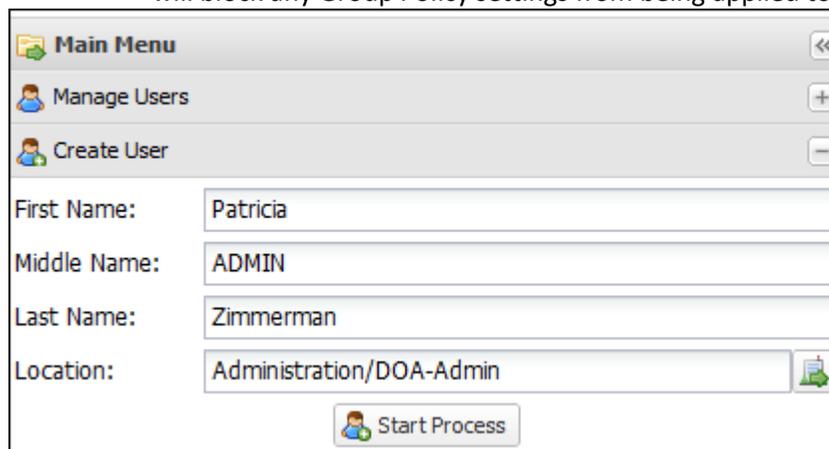
1. See instructions outlined in Section 1, Step 1.

### Search For an Existing IAM Userid

2. Perform a **Search** to confirm that the individual down not already have a Secondary IAM Account (Userid). See instructions outlined in Section 1, starting with Step 2.

### Create Secondary IAM Account (Userid)

3. Follow the Create Userid directions outlined in Section 2 starting at step 3. When creating the new Userid, there are two things to remember:
  - a. The **Middle Name** field should have the value of **Admin**. This will identify Userid that as a Secondary IAM Account (Userid).
  - b. The ID must be created in the **Admin** container for your agency. This will block any Group Policy settings from being applied to the Userid.



The screenshot shows a web-based user creation interface. At the top, there is a 'Main Menu' with three options: 'Main Menu' (with a left arrow), 'Manage Users' (with a plus sign), and 'Create User' (with a minus sign). Below the menu, there are four input fields: 'First Name' with the value 'Patricia', 'Middle Name' with the value 'ADMIN', 'Last Name' with the value 'Zimmerman', and 'Location' with the value 'Administration/DOA-Admin'. A 'Start Process' button is located at the bottom of the form.

Should there be two individuals with the same first and last name, each requiring a Secondary IAM Account (Userid), add their true middle initial after their first name (example: Joe P, Joe J).

### Special Issues

- Should the individual already have a Secondary IAM account (Userid) at another agency (**a secondary IAM account (Userid) can be identified by the term 'admin' in the middle name field**) contact DET IAM Security for assistance.
- Should the individual already have a Secondary IAM account (Userid) within your agency and it is used for Delegated Exchange Administration but not working correctly, contact DET IAM Security for assistance.

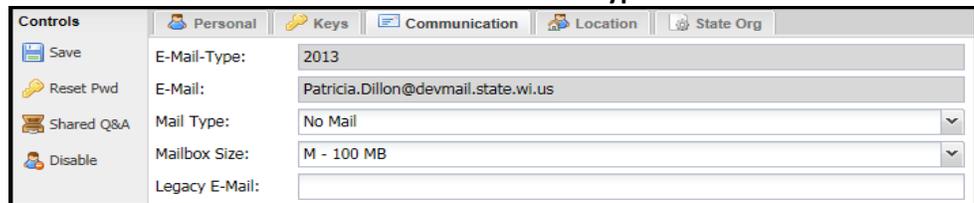
### Additional Userid Specifications

- c. On the **Personal** tab enter '**Secondary IAM Account**' in the **Administrative Notes:** field.



Administrative Notes:  
Secondary IAM Account

- d. On the **Communication** tab the **Mail Type** should be set to **No Mail**.



Controls: Save, Reset Pwd, Shared Q&A, Disable

Personal | Keys | **Communication** | Location | State Org

E-Mail-Type: 2013  
E-Mail: Patricia.Dillon@devmail.state.wi.us  
Mail Type: No Mail  
Mailbox Size: M - 100 MB  
Legacy E-Mail:

- e. There is nothing else special about any of the other fields and they can be filled out as your agency policies dictate. Go ahead and **SAVE** the Userid when you are done.
- f. Provide the owner with their Secondary IAM Account (Userid) and initial password.
- g. The owner will have to activate this Userid like they did their primary IAM Userid.
- h. The password for a Secondary IAM Account (Userid) will expire every 60 days. Where this Userid does not have an associated Email account, it will not be receiving warning emails as the password expiration date draws near. For this reason, it is recommended that the owner change the password of the Secondary IAM Account (Userid) at the same time that they change the password of their Primary IAM Userid.



*Adding Production  
Delegated Exchange  
rights to a  
Production  
Secondary IAM  
Account (Userid)*

- i. After an agency IAM Security Administrator creates a Secondary IAM account (Userid) for Delegated Exchange Admin purposes, follow the directions outlined in **Section 14** for requesting a new agency Delegated Exchange Administrator.

*Adding UAT  
Delegated  
Exchange rights to  
a UAT Secondary  
IAM Account  
(Userid)*

- j. After the agency IAM Security Administrator creates a Secondary IAM account (Userid) in UAT for UAT Delegated Exchange Admin purposes, they should open up a Service Request (SR). State that this Secondary IAM account (Userid) needs to be added as a UAT Delegated Exchange Administrator for the agency. Also state in the SR that it be assigned to the Infrastructure Tools AD team.

## SECTION 8. AUDIT LOG

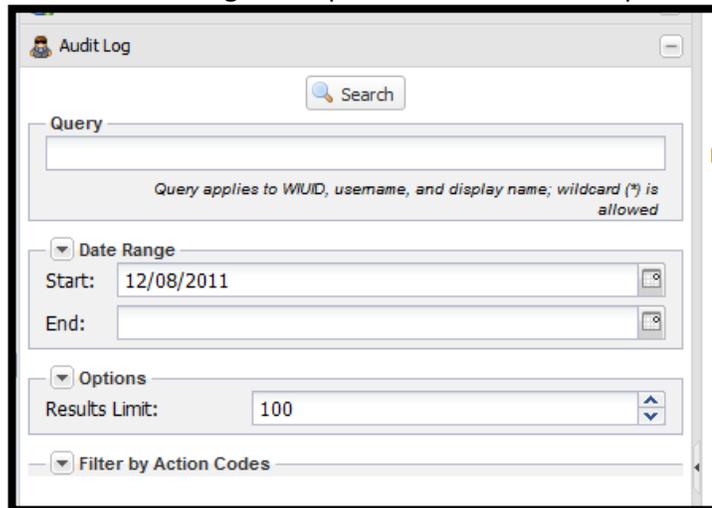
Although you receive immediate confirmation in UMRA on any Userid creation or modification, change, you can review all security changes made through UMRA or SSRPM (IAM Home page).

### Sign On To Production UMRA

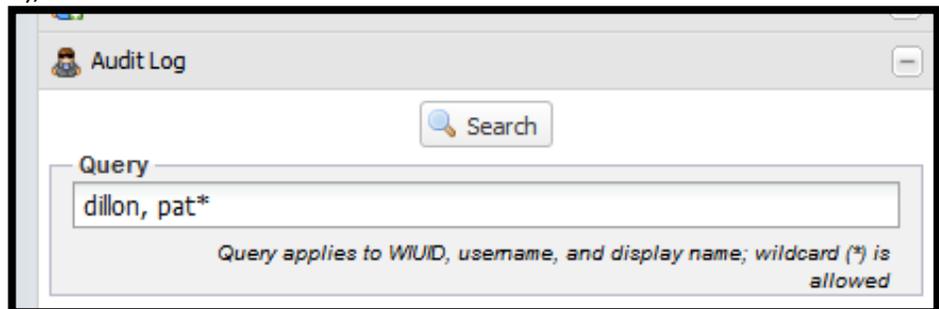
1. See instructions outlined in Section 1, Step 1.

### Set Audit Listing Parameters

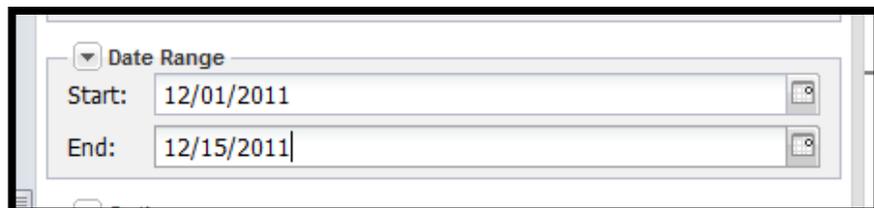
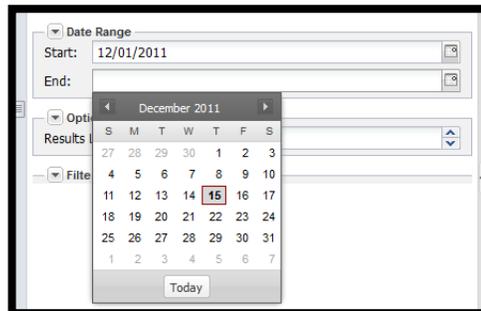
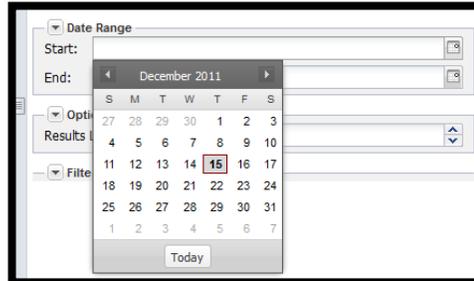
2. Press the **Audit Log** bar. A parameter menu will drop down



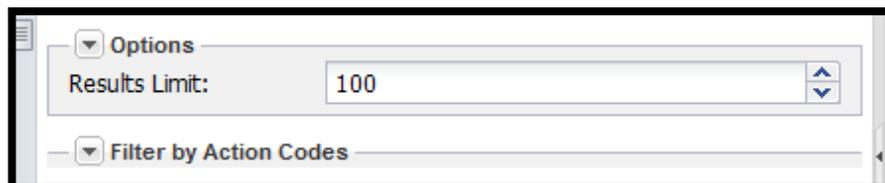
3. In the Query box you can enter in a **Username**, the **Display Name** (or a portion of it), or a **WIUID**.



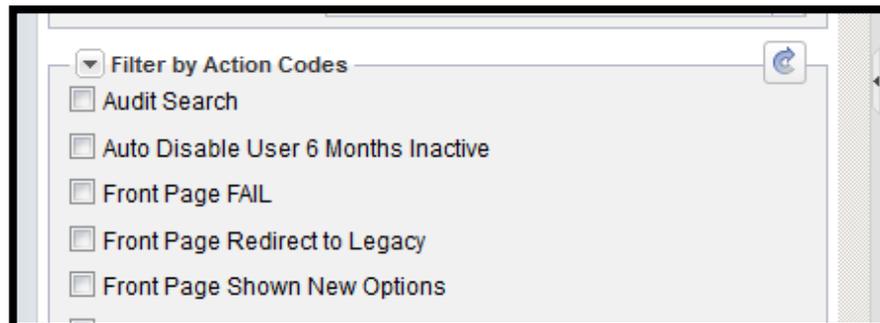
4. In the **Date Range** section you have the option to set a date range, though it is not required. To do this press the little calendar at the end of the **Start** and **End** lines.



- In the **Options** section you can limit the number of lines returned during your inquiry. One hundred (100) is the default value. The maximum that will show in your browser is 500. If you download the output after the log search is completed the maximum line count is 10,000.



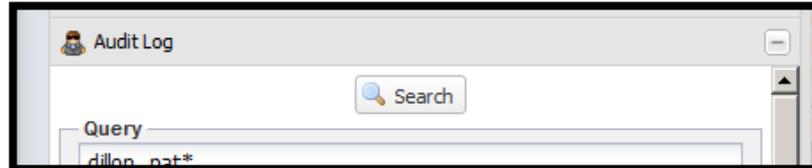
- In the **Filter by Action Codes** section you can specify specific events that you want to audit on. You will notice that there are a number of them which can help you search for specific events. To refresh the Action Code selections, click the refresh button, which is the button with circular arrow to the right of "filter by Action Codes".



### Audit Action Codes

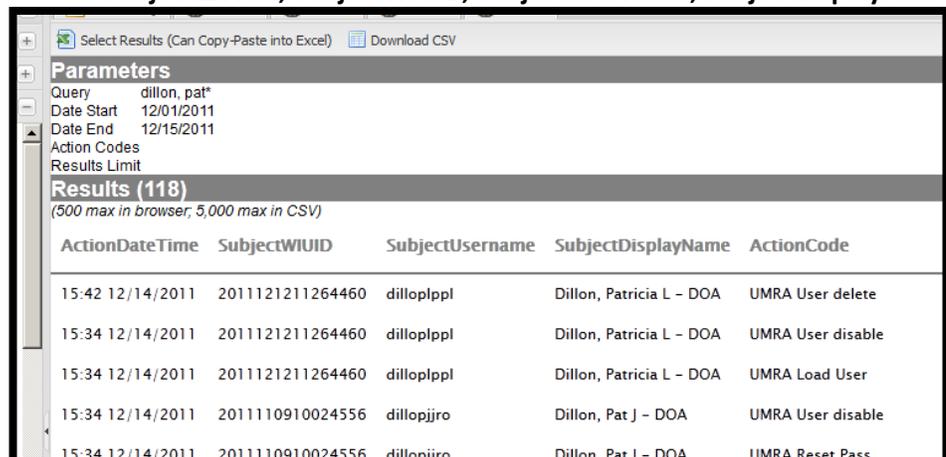
|   |                          |
|---|--------------------------|
| Audit Search                              | UMRA Auth                |
| Auto disable User 6 Months Inactive       | UMRA Auth Fail           |
| Front Page FAIL                           | UMRA Convert to Mailbox  |
| Front Page Redirect to Legacy             | UMRA Convert to Mailuser |
| Front Page Shown Invalid Username         | UMRA Create Mailbox      |
| Front Page Shown new Options              | UMRA Create Mailuser     |
| Front Page Shown New Please               | UMRA Create User         |
| Activate                                  | UMRA LBAC                |
| Pass Reset (using known pass)             | UMRA Load User           |
| Pass Reset (using known pass) FAIL        | UMRA New SMTP Proxy      |
| Pwd Expiration Notification               | UMRA RBAC                |
| Pwd Expiration Notification FAIL          | UMRA RBAC/LBAC Pull      |
| Pwd Expiration Notification SKIPPED       | UMRA Remove Mailbox      |
| Reports Search                            | UMRA Remove Mailuser     |
| Sched. Task Delete                        | UMRA Reset Pass          |
| Self Shared Secret Questions Pull         | UMRA Set Attr            |
| Self Shared Secret Questions Pull<br>FAIL | UMRA Shared Q&A Pull     |
| Self Shared Secret Questions Save         | UMRA Transfer (OU)       |
| SSRPM Activate                            | UMRA Update Mailbox      |
| SSRPM Auth                                | UMRA Update Mailuser     |
| SSRPM Auth (CR-Reset) Fail                | UMRA user block          |
| SSRPM Auth (CR-Unlock) Fail               | UMRA User delete         |
| SSRPM Auth Fail                           | UMRA User disable        |
| SSRPM Auto Unenroll                       | UMRA User enable         |
| SSRPM BLOCK                               | UMRA User unlock         |
| SSRPM RESET                               | UMRA Username Change     |
| SSRPM UNLOCK                              | UMRA Wipe AD SID         |

- Once you have entered in your parameters for your audit search press the **Search** button.



### Audit Listing

8. Your results will appear on the right side of the screen.
  - The **parameters** used to create the listing are in the upper left hand corner of the report.
  - The number of lines of the listing is in the greyed out **Results** line in ( ).
  - The information is under the column heads of **ActionDateTime**, **ActionCode**, **ActionOldValue**, **ActionNewValue**, **ActorCN**, **ActorLBACid**, **ActorWIUID**, **ActorUsername**, **ActorDisplayName**, **SubjectCN**, **SubjectLBACid**, **SubjectWIUID**, **SubjectUsername**, **SubjectDisplayName**



| ActionDateTime   | SubjectWIUID     | SubjectUsername | SubjectDisplayName       | ActionCode        |
|------------------|------------------|-----------------|--------------------------|-------------------|
| 15:42 12/14/2011 | 2011121211264460 | dilloplppl      | Dillon, Patricia L - DOA | UMRA User delete  |
| 15:34 12/14/2011 | 2011121211264460 | dilloplppl      | Dillon, Patricia L - DOA | UMRA User disable |
| 15:34 12/14/2011 | 2011121211264460 | dilloplppl      | Dillon, Patricia L - DOA | UMRA Load User    |
| 15:34 12/14/2011 | 2011110910024556 | dillopjro       | Dillon, Pat J - DOA      | UMRA User disable |
| 15:34 12/14/2011 | 2011110910024556 | dillopjro       | Dillon, Pat J - DOA      | UMRA Reset Pass   |

### Exporting Audit Listing

9. The audit results can be exported to a spread sheet in 3 ways.
  - Use your mouse to highlight the lines you wish to copy and paste into an Excel spread sheet.
  - Press the **Select Results** button and you can copy and paste the whole report into an Excel spreadsheet.
  - Press the **Download CSV**. Screens will follow depending on the browser you are using that lead to a spread sheet with the audit report imported into it.

## SECTION 9. REPORTS

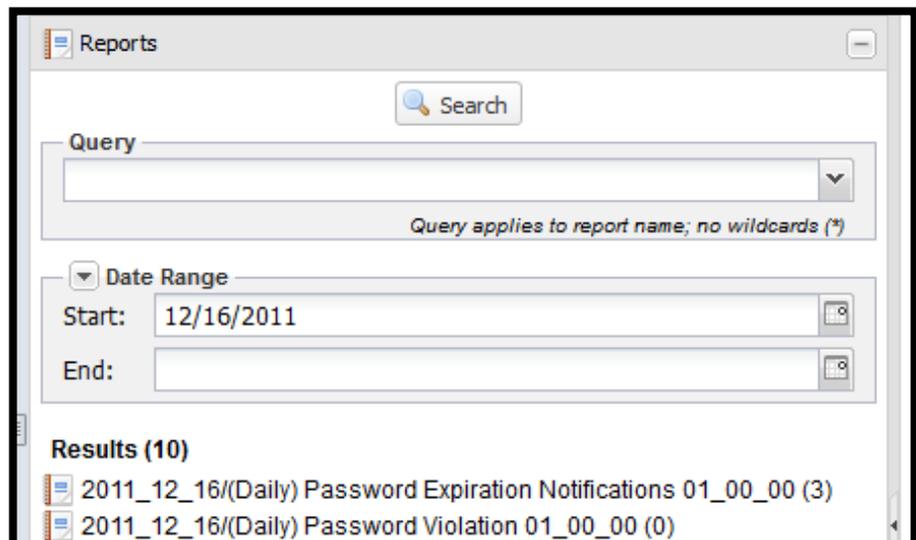
There are a number of ‘canned’ reports available in UMRA for agency security administrator review. It is strongly recommended that someone from each agency review these reports on a regular basis.

### Sign On To Production UMRA

1. See instructions outlined in Section 1, Step 1.

### Viewing Report

2. Press the Reports bar. Parameter fields will drop down under the **Reports** bar. By default the security reports for the current day will also appear.



3. To view reports use your mouse to click on the report under **Results**. You will see the report appear on the right hand side of the screen. The report titles are formatted as follows:

YYYY\_MM\_DD(frequency) Report Name HH\_MM\_SS (# lines)

YYYY\_MM\_DD = Date of run

Frequency = Daily, weekly, monthly, etc

Report name = Name of report

HH\_MM\_SS = Time of run

(# lines) = Number of lines in report

Download CSV

Report: (Daily) UMRA Account Change 01\_00\_00 (74)  
Rows: 74  
Report showing account changes performed in the UMRA Management portal.

| Time                | WIUID            | Display Name                | Username   | Location   | ActionCode                | Notes   | Old Value                         |
|---------------------|------------------|-----------------------------|------------|--|---------------------------|---|-----------------------------------|
| 16:08<br>12/15/2011 | 1111111111111111 | Jouikov,<br>Ivan V -<br>GAB | advtest    | accounts.wistate.dev/Staff<br>/AccountabilityBoard<br>/Jouikov, Ivan V ~<br>1111111111111111 | UMRA<br>User<br>disable   |   |                                   |
| 16:08<br>12/15/2011 | 1111111111111111 | Jouikov,<br>Ivan V -<br>GAB | advtest    | accounts.wistate.dev/Staff<br>/AccountabilityBoard<br>/Jouikov, Ivan V ~<br>1111111111111111 | UMRA<br>User<br>enable    | Also wiStatus is cleared  |                                   |
| 15:27<br>12/15/2011 | 2011121216280487 | Jouikov,<br>Ivan V -<br>DOA | jouikivfnc | accounts.wistate.dev/Staff<br>/Administration/Jouikov,<br>Ivan V ~<br>2011121216280487       | UMRA<br>Sanitize<br>User  | User deleted due to mailbox sanitization<br>due to cross-agency move, new OU:<br>StaffAdministration  | accounts<br>/Account:<br>Ivan V ~ |
| 15:27<br>12/15/2011 | 2011121216280487 | Jouikov,<br>Ivan V -<br>DOA | jouikivfnc | accounts.wistate.dev/Staff<br>/Administration/Jouikov,<br>Ivan V ~<br>2011121216280487       | UMRA<br>Create<br>Mailbox | Size: [C] Alias:<br>[IvanV2.Jouikov@wistate.dev] Web Mail<br>Access: [yes] Hide from GAL: [no]<br>Disabled: [no] Store:<br>[MEWMAD0DC-IN2IONCC01G02SG01d] |                                   |
| 15:27<br>12/15/2011 | 2011121216280487 | Jouikov,<br>Ivan V -<br>DOA | jouikivfnc | accounts.wistate.dev/Staff<br>/Administration/Jouikov,<br>Ivan V ~<br>2011121216280487       | UMRA Set<br>Attr          | wiDepartmentCode  |                                   |
| 15:27<br>12/15/2011 | 2011121216280487 | Jouikov,<br>Ivan V -<br>DOA | jouikivfnc | accounts.wistate.dev/Staff<br>/Administration/Jouikov,<br>Ivan V ~<br>2011121216280487       | UMRA Set<br>Attr          | wiDepartmentAbbrv   |                                   |
| 15:27<br>12/15/2011 | 2011121216280487 | Jouikov,<br>Ivan V -<br>DOA | jouikivfnc | accounts.wistate.dev/Staff<br>/Administration/Jouikov,<br>Ivan V ~<br>2011121216280487       | UMRA Set<br>Attr          | department  |                                   |
| 15:27               | 2011121216280487 | Jouikov,<br>Ivan V -        | jouikivfnc | accounts.wistate.dev/Staff<br>/Administration/Jouikov,                                       | UMRA Set                  | wiSSRPMPEnrollDate  |                                   |

4. In the upper left hand corner of the report you will find additional information about the run.

Download CSV

Report: (Daily) UMRA Account Change 01\_00\_00 (74)  
Rows: 74  
Report showing account changes performed in the UMRA Management portal.

Report: (frequency) Report Name HH\_MM\_SS (# lines)

Rows: NN

Explanation of what information is reflected in the report

Frequency = Daily, weekly, monthly, etc

Report name = Name of report

HH\_MM\_SS = Time of run

(# lines) = Number of lines in report

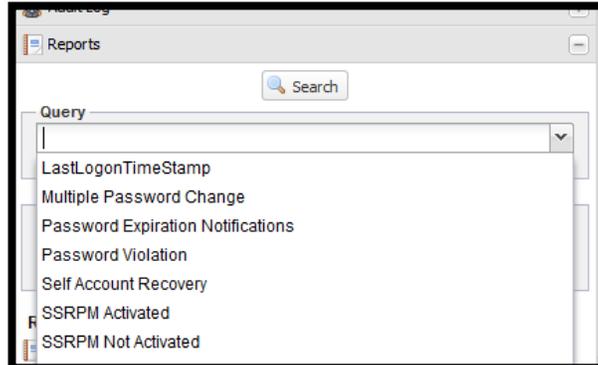
NN = Number of lines in report

### Exporting Security Report

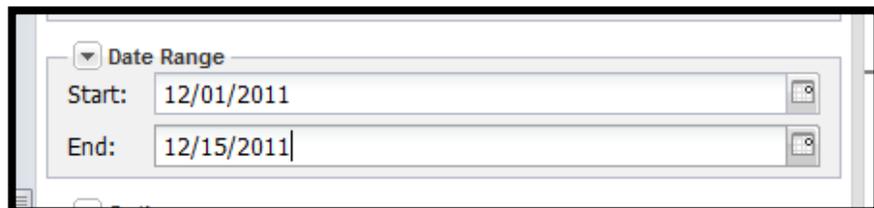
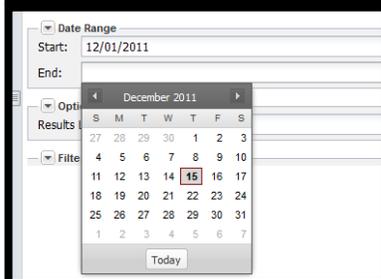
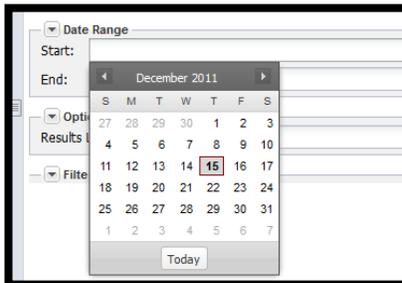
5. The audit results can be exported to a spread sheet by pressing the Download CSV in the upper left hand corner of the report. Screens will follow depending on the browser you are using that lead to a spread sheet with the security report imported into it.

### Using Parameters to Search for Security Reports

6. Using the **Query** parameter you can select the specific report that you are looking to view. You can either enter in a query manually or drop down the listing of reports is available. With your mouse click on the report you want.



7. In the **Date Range** section you have the option to set a date range, though it is not required. To do this press the little calendar at the end of the **Start** and **End** lines.



Available 'Canned' Reports

**Weekly**

|                          |  |
|--------------------------|--|
| Last Logon Time Stamp    | Weekly report showing inactive accounts defined as accounts that have not signed on in over 30 days (but no more than 180 days) or never at all, or have not changed their password in over 60 days (but no more than 180 days) or never at all. |
| Multiple Password Change | Report showing accounts that have had more than 3 password changes or have gone through 3 or more Account Recoveries in the past week.   |
| Password Violation       | Report outlining Bad Password Attempt violations by the account. This applies to the self-password reset page only.  |
| Self-Account Recovery    | Report showing which accounts went through account recovery and were successful or unsuccessful  |
| SSRPM Activated          | Accounts in deployed OUs that have gone through the activation process.  |
| SSRPM Not Activated      | Accounts in deployed OUs that have not gone through the activation process   |
| Stale Accounts           | Weekly inactivity report showing which accounts have not been used in over 6 months  |
| UMRA Account Change      | Report showing account changes performed in the UMRA Management portal   |
| UMRA Delete User         | Report showing accounts deleted in the UMRA Management portal  |
| UMRA New User            | Report showing accounts created in the UMRA Management portal  |
| UMRA Password Reset      | Security Officer performs a Password Change through UMRA management portal.  |
| UMRA Restore Account     | Users reset own password using good known password   |
| UMRA Suspend Account     | Report showing accounts that were SSRPM Blocked in the UMRA Management portal  |

**Daily**

|                                   |  |
|-----------------------------------|--|
| Password Expiration Notifications | Daily report showing which accounts were sent Userid password expiration warning letters |
|-----------------------------------|--|

|                          |  |
|--------------------------|--|
| Password Violation       | Report outlining Bad Password Attempt violations by accounts. This applies to the self-password reset page only. |
| RBAC-LBAC Groups Members | Report showing access granted to UMRA administrators. See Section 15 for more information regarding RBAC roles.  |
| Self-Account Recovery    | Report showing which accounts went through account recovery (SSRPM) and were successful or unsuccessful          |
| SSRPM Activated          | Accounts in deployed OUs that have gone through the activation process.  |
| SSRPM Not Activated      | Accounts in deployed OUs that have not gone through the activation process                                       |
| UMRA Account Change      | Report showing account changes performed in the UMRA Management portal   |
| UMRA Delete User         | Report showing accounts deleted in the UMRA Management portal  |
| UMRA New User            | Report showing accounts created in the UMRA Management portal  |
| UMRA Password Reset      | Security Officer performs a Password Change through UMRA management portal                                       |
| UMRA Restore Account     | Users reset own password using good known password   |
| UMRA Suspend Account     | Report showing accounts that were SSRPM Blocked in the UMRA Management portal                                    |

## SECTION 10. LIVE DATA QUERIES

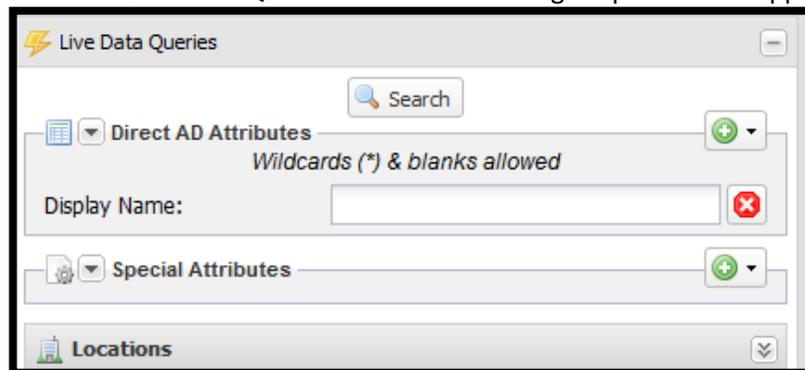
Within UMRA there is the capability to produce reports using the contents of the Enterprise AD (IAM Userids) database. You can produce reports depending on values in certain fields to be executed on an ad-hoc (as needed) basis.

### Sign On To Production UMRA

1. See instructions outlined in Section 1, Step 1.

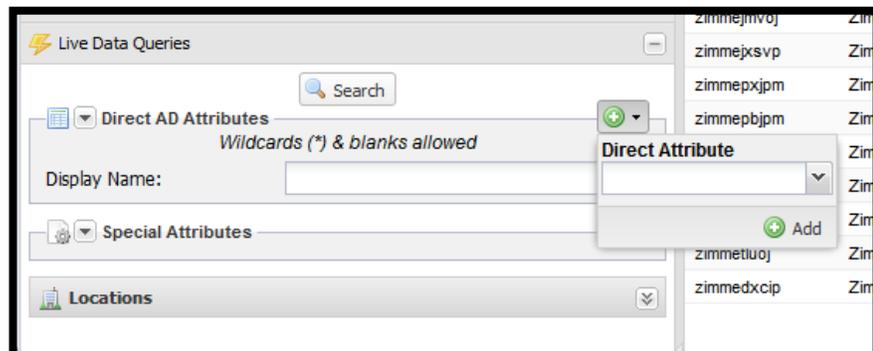
### Producing Live Data Queries

2. Press the **Live Data Queries** bar. The following drop down will appear.

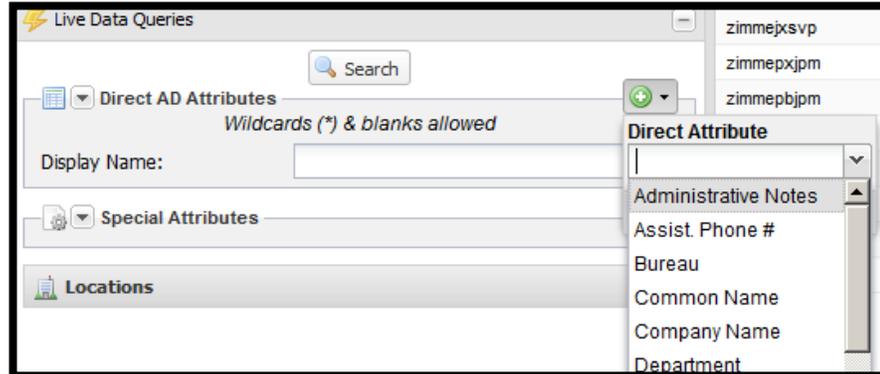


### Direct AD Attributes

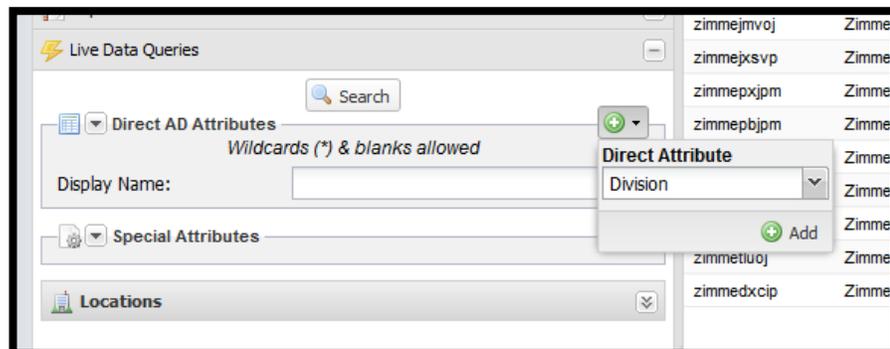
3. Press on the green circle drop down directly across from the 'Direct AD Attributes' heading. A drop down will appear with an empty field.



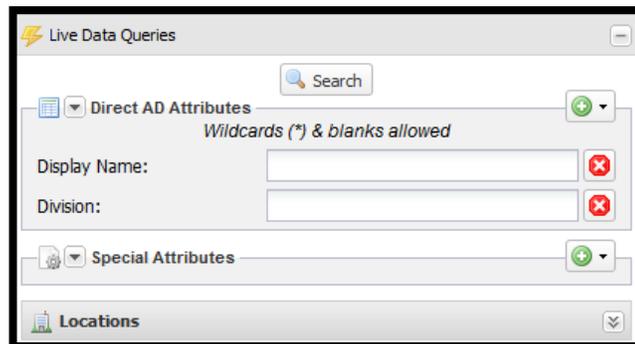
4. Press the drop down button on the right to select which Userid fields you wish to query.



5. Select the field you wish to query by clicking on it with your mouse



6. Press the green circle with the work **Add** after it.



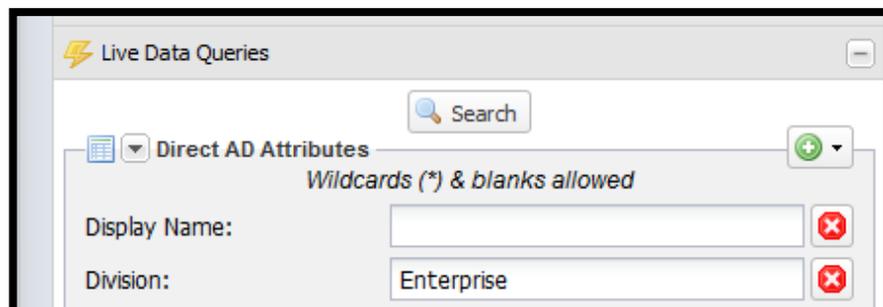
7. Notice that under 'Display Name:' the field you selected (Division in this case) appears. You can repeat steps 3 – 6 if you wish to perform a more complex query.

#### Available Direct Attributes

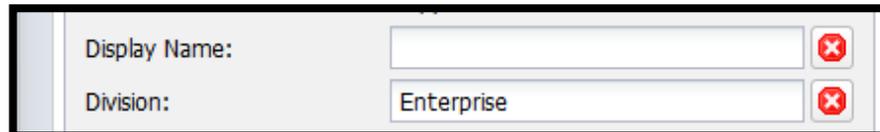
Admin. Notes  
Assist. Phone #  
Bureau  
Common Name  
Company Name

Depart. Abb.  
Department Code  
Department Name  
Division  
E-Mail  
Employee Type  
Extension  
Fax #  
First Name  
Last Name  
Legacy E-Mail  
Legacy Userid  
Loc. Address    City  
Loc. Addr. Office  
Loc. Addr. State  
Loc. Addr. Street  
Loc. Address ZIP  
Middle Name  
Mobile Phone #  
Name resolution  
Orgcode  
Pager #  
Phone #  
Postal Address  
Postal Addr. City  
Postal Addr. State  
Postal Addr. ZIP  
Section  
Title  
Unit  
User Name  
WIUID

8. Once you have added all the fields to your query you can enter your search criteria.

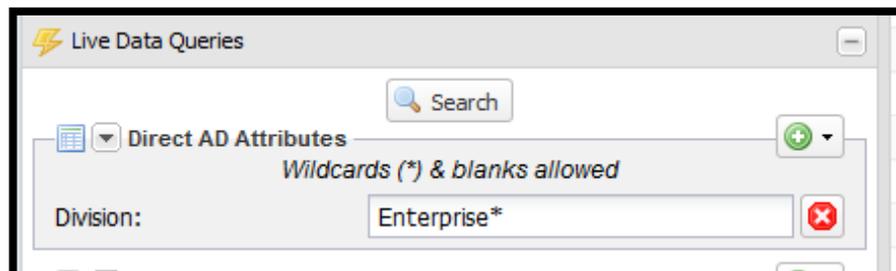


9. To delete a field from the query press the red X box after the field name.



Display Name:  ✕  
 Division:  ✕

10. Now that your query parameters are done press the **Search** button to execute the query.



Live Data Queries

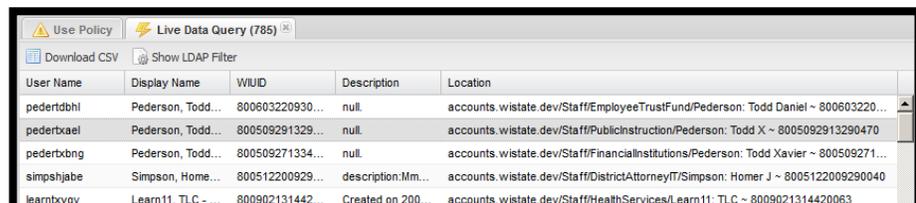
Search

Direct AD Attributes +

Wildcards (\*) & blanks allowed

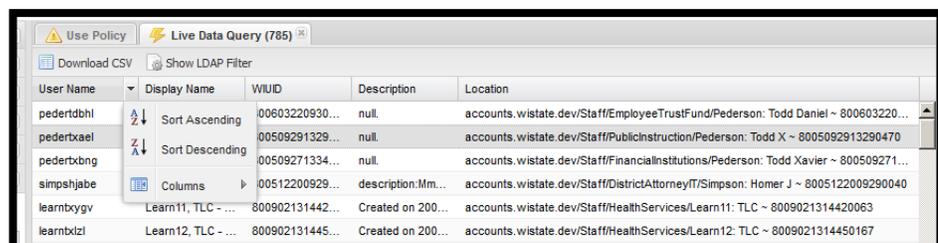
Division:  ✕

11. The query results will appear on the right side of your screen. **The first 500 lines will appear only. You can download the full report (max. 100,000 lines) into a spread sheet.**



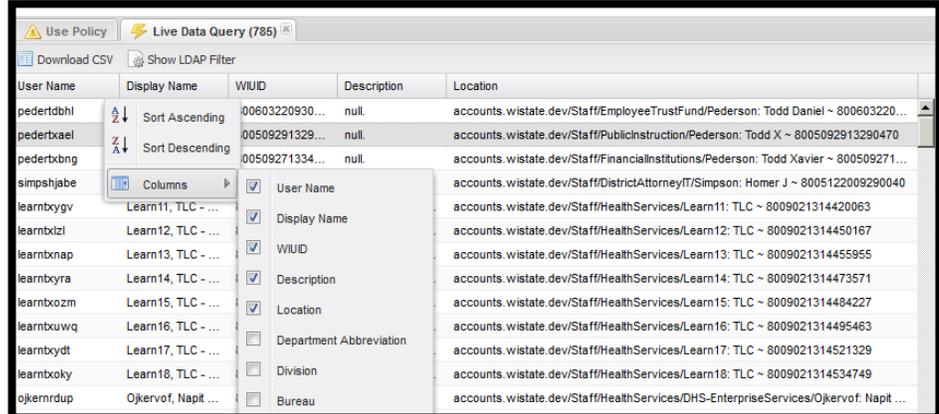
| User Name  | Display Name       | WIUID           | Description       | Location  |
|------------|--------------------|-----------------|-------------------|---|
| pedertdbhl | Pederson, Todd...  | 800603220930... | null              | accounts.wistate.dev/Staff/EmployeeTrustFund/Pederson: Todd Daniel ~ 800603220...     |
| pedertxae  | Pederson, Todd...  | 800509291329... | null              | accounts.wistate.dev/Staff/PublicInstruction/Pederson: Todd X ~ 8005092913290470      |
| pedertxbng | Pederson, Todd...  | 800509271334... | null              | accounts.wistate.dev/Staff/FinancialInstitutions/Pederson: Todd Xavier ~ 800509271... |
| simpshjabe | Simpson, Home...   | 800512200929... | description.Mm... | accounts.wistate.dev/Staff/DistrictAttorneyIT/Simpson: Homer J ~ 8005122009290040     |
| learnbygv  | Learn11, TLC - ... | 800902131442... | Created on 200... | accounts.wistate.dev/Staff/HealthServices/Learn11: TLC ~ 8009021314420063             |

12. You can change the sort of any of the columns by placing your mouse over the column name and press the drop down.



| User Name  | Display Name       | WIUID           | Description       | Location  |
|------------|--------------------|-----------------|-------------------|---|
| pedertdbhl | Pederson, Todd...  | 800603220930... | null              | accounts.wistate.dev/Staff/EmployeeTrustFund/Pederson: Todd Daniel ~ 800603220...     |
| pedertxae  | Pederson, Todd...  | 800509291329... | null              | accounts.wistate.dev/Staff/PublicInstruction/Pederson: Todd X ~ 8005092913290470      |
| pedertxbng | Pederson, Todd...  | 800509271334... | null              | accounts.wistate.dev/Staff/FinancialInstitutions/Pederson: Todd Xavier ~ 800509271... |
| simpshjabe | Simpson, Home...   | 800512200929... | description.Mm... | accounts.wistate.dev/Staff/DistrictAttorneyIT/Simpson: Homer J ~ 8005122009290040     |
| learnbygv  | Learn11, TLC - ... | 800902131442... | Created on 200... | accounts.wistate.dev/Staff/HealthServices/Learn11: TLC ~ 8009021314420063             |
| learnbzil  | Learn12, TLC - ... | 800902131445... | Created on 200... | accounts.wistate.dev/Staff/HealthServices/Learn12: TLC ~ 8009021314450167             |

13. You can further change the fields shown by pressing the arrow after the **Columns** selection.



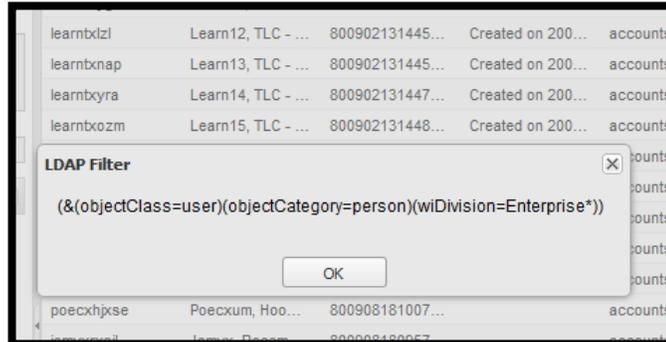
| User Name  | Display Name        | WIUID          | Description | Location  |
|------------|---------------------|----------------|-------------|---|
| pedertdbhl | Sort Ascending      | 00603220930... | null        | accounts.wistate.dev/Staff/EmployeeTrustFund/Pederson: Todd Daniel ~ 800603220...     |
| pedertxael | Sort Descending     | 00509291329... | null        | accounts.wistate.dev/Staff/PublicInstruction/Pederson: Todd X ~ 8005092913290470      |
| pedertxbng |                     | 00509271334... | null        | accounts.wistate.dev/Staff/FinancialInstitutions/Pederson: Todd Xavier ~ 800509271... |
| simpshjabe |                     |                |             | accounts.wistate.dev/Staff/DistrictAttorneyIT/Simpson: Homer J ~ 8005122009290040     |
| learnbygv  | Learn11, TLC - ...  |                |             | accounts.wistate.dev/Staff/HealthServices/Learn11: TLC ~ 8009021314420063             |
| learnbizi  | Learn12, TLC - ...  |                |             | accounts.wistate.dev/Staff/HealthServices/Learn12: TLC ~ 8009021314450167             |
| learnbnap  | Learn13, TLC - ...  |                |             | accounts.wistate.dev/Staff/HealthServices/Learn13: TLC ~ 8009021314455955             |
| learnbyra  | Learn14, TLC - ...  |                |             | accounts.wistate.dev/Staff/HealthServices/Learn14: TLC ~ 8009021314473571             |
| learnbozm  | Learn15, TLC - ...  |                |             | accounts.wistate.dev/Staff/HealthServices/Learn15: TLC ~ 8009021314484227             |
| learnbuwq  | Learn16, TLC - ...  |                |             | accounts.wistate.dev/Staff/HealthServices/Learn16: TLC ~ 8009021314495463             |
| learnbydt  | Learn17, TLC - ...  |                |             | accounts.wistate.dev/Staff/HealthServices/Learn17: TLC ~ 8009021314521329             |
| learnboky  | Learn18, TLC - ...  |                |             | accounts.wistate.dev/Staff/HealthServices/Learn18: TLC ~ 8009021314534749             |
| ojkernrdup | Ojkervof, Napit ... |                |             | accounts.wistate.dev/Staff/HealthServices/DHS-EnterpriseServices/Ojkervof: Napit ...  |

### Additional Options Under Columns

- Department Abbreviation
- Division
- Bureau
- SSRPM Blocked
- AD Disabled
- AD Locked
- Last Logon
- Pswd Expires in X Days
- Password Expires On
- Password Last Set On
- Mail Type
- Mailbox Size
- Hide From GAL
- Web Mail Access
- Mailbox Disabled

### Exporting Query Results

14. The full query results (**max. 100,000 lines**) can be exported to a spread sheet by pressing the **Download CSV** in the upper left hand corner of the report. Screens will follow depending on the browser you are using that lead to a spread sheet with the security report imported into it.
15. To view your query parameters press **Show LDAP filter** near the upper left hand corner of the report. Press the **OK** button to close the **LDAP Filter** box.



### Special Attributes

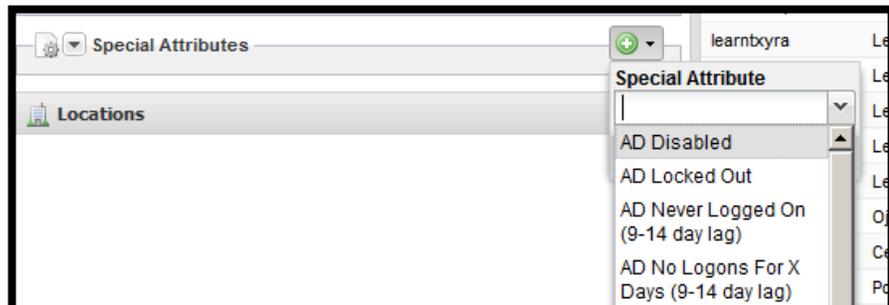
16. You add special attributes to the AD Attributes you specified above or you can run the **Special Attributes** on their own.
17. Press on the green circle drop down directly across from the 'Special Attributes' heading.



18. A drop down will appear with an empty field.



19. Press the drop down button on the right to select which special attributes you wish to use.



20. Select the special attribute you wish to execute by clicking your mouse on it.



21. Press the green circle with the word **Add** after it.

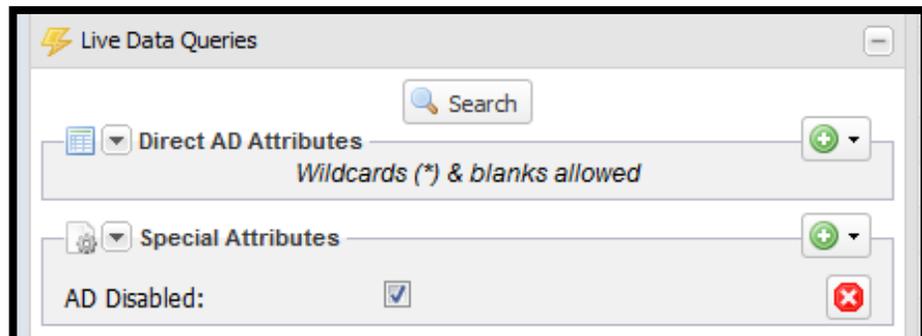


22. You will notice that under 'Special Attributes' the attribute you selected (AD Disabled in this case) appears. You can repeat steps 17 – 21 if you wish to perform a more complex query.

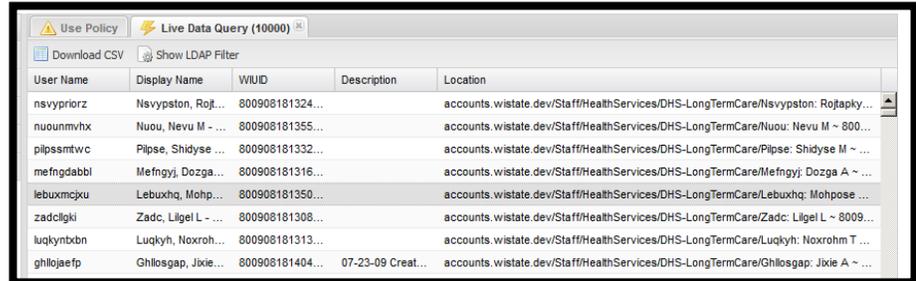
23. To delete a special attribute from the query press the red X box after the field name.



24. Now that your special attributes are done press the **Search** button to execute the query.



25. The query results will appear on the right side of your screen.



| User Name  | Display Name         | WUID            | Description       | Location  |
|------------|----------------------|-----------------|-------------------|---|
| nsvypriorz | Nsvypston, Rojt...   | 800908181324... |                   | accounts.wistate.dev/Staff/HealthServices/DHS-LongTermCare/Nsvypston: Rojtapy...    |
| nuounmvhx  | Nuou, Nevu M - ...   | 800908181355... |                   | accounts.wistate.dev/Staff/HealthServices/DHS-LongTermCare/Nuou: Nevu M ~ 800...    |
| pilpsmtwc  | Pilpse, Shidyse ...  | 800908181332... |                   | accounts.wistate.dev/Staff/HealthServices/DHS-LongTermCare/Pilpse: Shidyse M ~ ...  |
| mefngdabbl | Mefngyj, Dozga...    | 800908181316... |                   | accounts.wistate.dev/Staff/HealthServices/DHS-LongTermCare/Mefngyj: Dozga A ~ ...   |
| lebuxmcjcu | Lebuxhq, Mohp...     | 800908181350... |                   | accounts.wistate.dev/Staff/HealthServices/DHS-LongTermCare/Lebuxhq: Mohpose ...     |
| zadcligki  | Zadc, Lilgel L - ... | 800908181308... |                   | accounts.wistate.dev/Staff/HealthServices/DHS-LongTermCare/Zadc: Lilgel L ~ 8009... |
| luqkymbxn  | Luqkyh, Noxroh...    | 800908181313... |                   | accounts.wistate.dev/Staff/HealthServices/DHS-LongTermCare/Luqkyh: Noxrohm T ...    |
| ghllojaefp | Ghllosgap, Jixie...  | 800908181404... | 07-23-09 Creat... | accounts.wistate.dev/Staff/HealthServices/DHS-LongTermCare/Ghllosgap: Jixie A ~ ... |

26. The option described in steps 13 – 15 above work for special Attribute listings as well.

#### Available Special Attributes

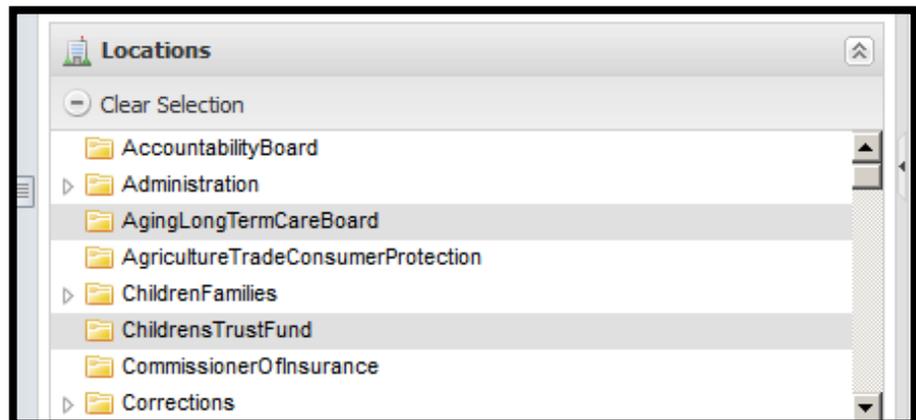
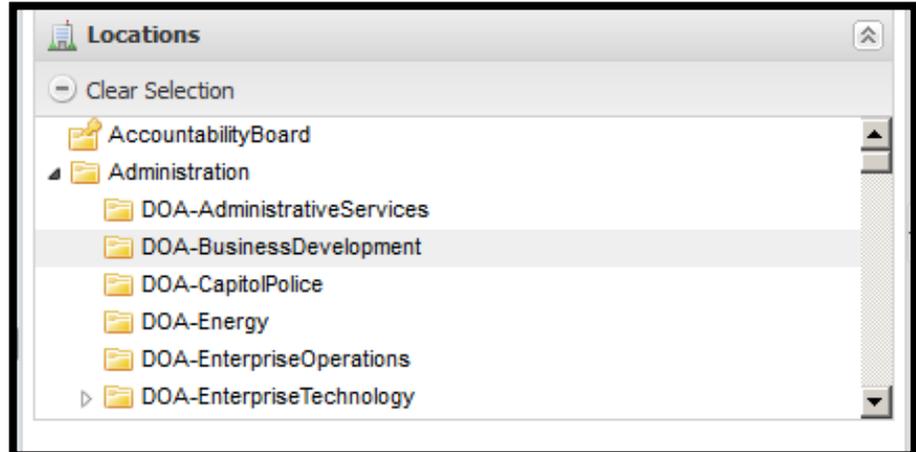
- AD Disabled
- AD Locked Out
- AD Never Logged On
- AD No Logons for X Days
- Exchange Hide from GAL
- Exchange Mail Type
- Exchange Mailbox Disabled
- Exchange Mailbox Size
- Exchange Web Mail Access
- Password Expires After
- Password Expires Before
- SSRPM Blocked

#### Locations

27. To reduce the size of your queries you can specify the location(s) that you want to execute with. Press the drop down arrows across from the **Locations** heading.



28. With your mouse click on the agency or agency sub OU to which you wish to limit your query to. You can select multiple locations by pressing down the **CTRL** button when using your mouse to click on the agency or agency sub OU.



## SECTION 11. SCHEDULE FUTURE COMMAND EXECUTION

UMRA allows you to schedule many of the manage user commands and inter-agency transfers to run at a later date.

### Commands

You are allowed to schedule the following commands under the **Controls** column in **Managed Users**.

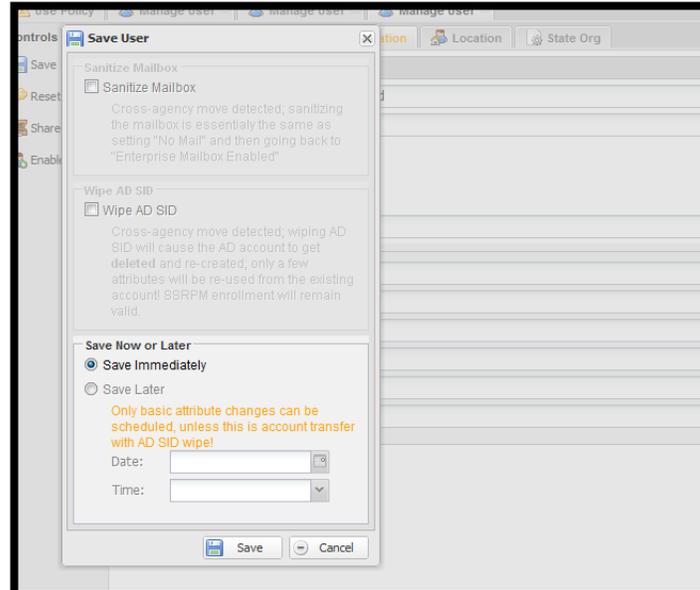
SSRPM Block  
Disable  
Enable  
Unlock  
Delete

### Field Modifications **NOT** Allowed

You are **NOT** allowed to schedule modifications to the following fields.

First name  
Middle name  
Last Name  
Generation Qualifier  
Name Resolution  
WIUID  
Common Name  
E-Mail  
Mail Type  
Mailbox Size  
Hide from Gal  
Web mail Access  
Mailbox disable  
Legacy E-Mail

When you **SAVE** a Userid modification that cannot be scheduled, the **Save User** box will open. Notice the **Save Later** option is shaded and in red it states 'Only sanitization or OU transfers and basic attribute changes are allowed'. Press the **SAVE** button to continue and your modification will be executed immediately.



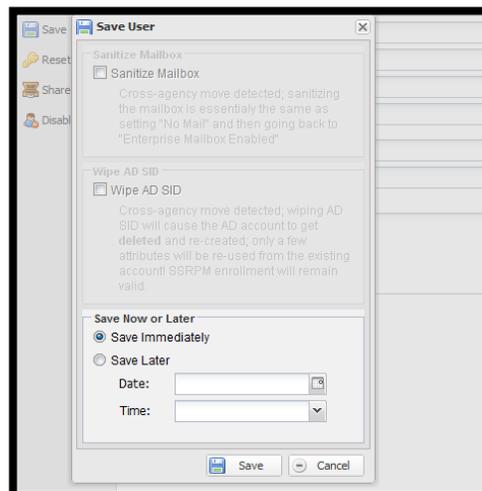
### Field Modifications Allowed

You are allowed to schedule modifications to the following fields.

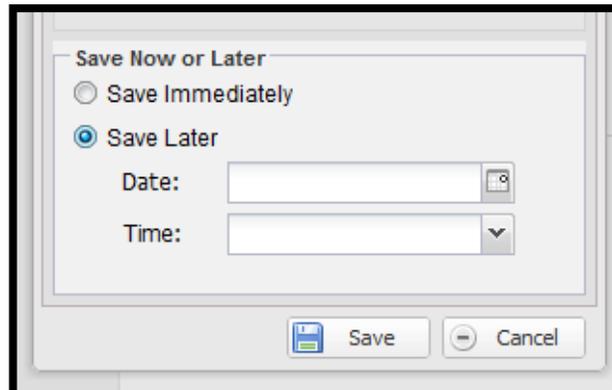
- Employee Type
- Administrative Notes
- Legacy Userid
- Display Name
- Location
- Phone #
- Extension
- Mobile Phone #
- Pager #
- Fax #
- Assist. Phone #
- Postal Address
- Postal Address City
- Postal Address State
- Postal Address ZIP
- Location Address Office
- Location Address Street
- Location Address City
- Location Address State
- Location Address ZIP
- Company name
- Title
- Division
- Bureau

Section  
Unit  
Orgcode  
Department Name  
Department Abbreviation  
Department Code

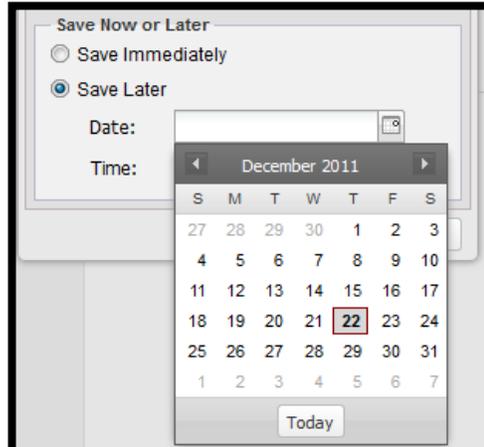
1. When you **SAVE** an allowed Userid modification or a command that can be scheduled, the **Save User** box will open and you will note the option to **Save Later**.



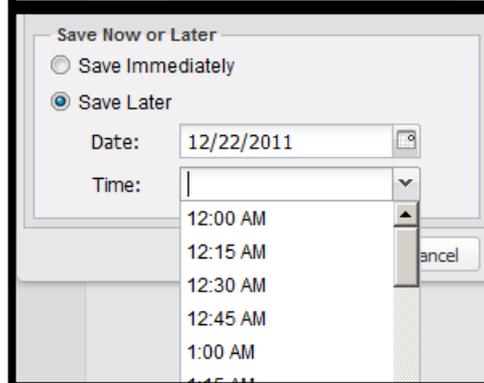
2. Press the radio button in front of **Save Later** and fill in the **Date** and **Time** fields.



3. You can use the drop downs at the end of each field to assist you with selecting the field values.

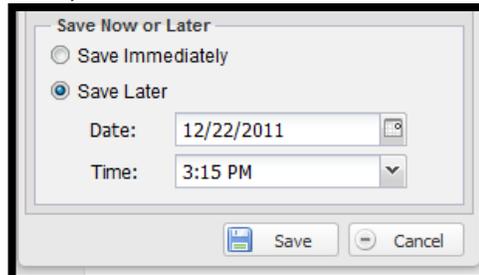


The screenshot shows a dialog box titled "Save Now or Later" with two radio buttons: "Save Immediately" (unselected) and "Save Later" (selected). Below the radio buttons are "Date:" and "Time:" labels. A calendar for December 2011 is overlaid on the "Date:" field, with the date "22" highlighted in a red box. The "Time:" field is currently empty.



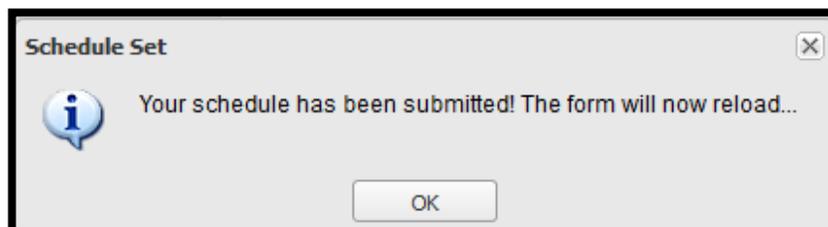
The screenshot shows the "Save Now or Later" dialog box with "Save Later" selected. The "Date:" field now contains "12/22/2011". The "Time:" field has a dropdown menu open, showing a list of times: "12:00 AM", "12:15 AM", "12:30 AM", "12:45 AM", and "1:00 AM". A "Cancel" button is visible on the right side of the dialog.

4. Press the **SAVE** button. The command will execute within a 5 minute time frame of the time you select.



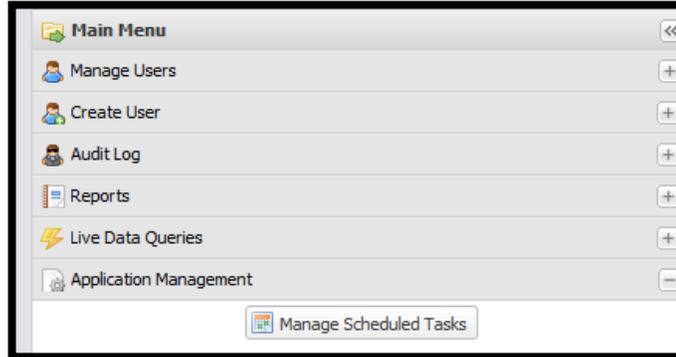
The screenshot shows the "Save Now or Later" dialog box with "Save Later" selected. The "Date:" field contains "12/22/2011" and the "Time:" field contains "3:15 PM". At the bottom of the dialog are "Save" and "Cancel" buttons.

5. The **Schedule Set** box will come up telling you that 'Your schedule has been submitted! The form will now reload...' Press the **OK** button.



The screenshot shows a dialog box titled "Schedule Set" with a close button (X) in the top right corner. On the left is an information icon (i). The main text reads: "Your schedule has been submitted! The form will now reload...". At the bottom center is an "OK" button.

6. You will notice that the Userid you are working on will return all fields to their original values and will wait until the scheduled time to actually execute the change.
7. To view all scheduled events press the **Application Management** box on the left of your panel. Press the **Manage Scheduled Tasks** box.



8. On the right side of your panel all scheduled changes impacting the agency(ies) that you are authorized to support will appear.

| De | Runs             | Action | Actor Username | Actor Display Name   | Subject Username | Subject Display Name | Description                               |
|----|------------------|--------|----------------|----------------------|------------------|----------------------|---|
|    | 12/22/2011 03:15 | save   | zimmepxjpm     | Zimmerman, Pat...    | dillopjro        | Dillon, Pat J - DOA  | Sanitize? False; Changed Attrs: emplo...  |
|    | 12/27/2011 12:15 | manage | zimmepxjpm     | Zimmerman, Pat...    | zimmetluoj       | Zimmerman, Ter...    | delete                                    |
|    | 12/29/2011 01:00 | save   | advtest2       | Jouikov, Ivan J -... | Error            | Error                | Sanitize? False; Changed Attrs: displa... |
|    | 12/30/2011 12:15 | manage | zimmepxjpm     | Zimmerman, Pat...    | zimmesgkwe       | Zimmerman, Sa...     | enable                                    |

- An agency security officer can delete any change that involves their agency by pressing the **red icon with the white X** in the **Delete** column.
- The word 'ERROR' in either the **Actor Username**, **Actor Display Name**, **Subject Username** or **Subject Display Name** fields mean that the Userid associated with those fields is no longer defined on the system.
- In the case of the word 'ERROR' in the **Subject Username** and **Subject Display Name** fields, these scheduled actions will **FAIL** and an email will be sent to the System Administrators.

## SECTION 12. TRANSFER PROCEDURE

### Transfer Exemptions

**Department of Children and Families** is exempt from having IAM Userids transferred out.

**Department of Revenue** is exempt from having IAM Userids transferred out.

**Department of Transportation** is exempt from having IAM Userids transferred in or out.

**Department of Workforce Development, Deloitte Consulting & Labor Industry Review** (all administered by DWD) is exempt from having IAM Userids transferred in or out.

### Transfer Scenario

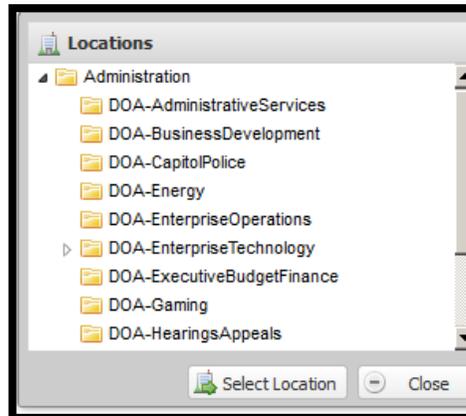
1. Agency security administrator checks to see if a new IAM Userid request is for an individual that already has an IAM Userid at any other agency.
2. The sending or receiving agency IAM Security Administrator sends an email with the following information to DET IAM Security (DOA DL IAM Security) to request a transfer.
  - Name of the individual being transferred
  - Name of Sending Agency and Receiving Agency
  - Date the transfer should be completed

NOTE: Enterprise Mailboxes are SANITIZED by default. If the employee wishes to take their Email (messages, calendar appointments, contacts, etc) to the new agency, please indicate this in the message. Any agency considering the transfer of Email from one agency to another should consult with their legal team.
3. DET IAM Security verifies via Email with both the sending/receiving agency IAM Security Administrator of the pending transfer.
4. If the sending agency uses Enterprise Email and they wish to have a copy of the mailbox contents for business purposes or to send a copy along with the employee, the sending agency Exchange Administrator must export the contents of Enterprise Email mailbox to a .PST file. If the employee is taking a copy of their mailbox data to the new agency, the file must be placed on portable media and given to the employee. **Note: this must be completed before DET IAM Security transfer's the IAM Userid to the new agency.**
5. DET IAM Security executes or schedules the transfer on the agreed on date and notifies the receiving agency IAM Security Administrator when done. DET IAM Security will normally be using an automated process that will:
  - Clear any values from most fields and change the Userid password
  - Create a new IAM Userid with the same WIUID, Userid, First name, Last Name, Middle Name, and E-Mail address.
  - Sanitize (empty) Enterprise Mailboxes
  - Transfer the IAM Userid to the receiving (new) agency.
6. When the transfer is completed, receiving agencies that use a legacy email system will have to replace **Mail Type: No Mail** to **Mail Type: External Mail Enabled**. They will also need to populate the **Legacy E-Mail** field with the correct **Legacy Email ID**.

7. When the transfer is complete, the receiving agency IAM Security Administrator will make necessary changes to the IAM Userid and assign the Userid a new password.
8. If there is an agreement between the sending & receiving agency allowing the transferred employee to bring their mailbox data with them to the new agency, the employee will provide the file on portable media. The mailbox data is imported into the new mailbox by an Exchange Administrator.
9. For a user that has never activated their IAM Userid:
  - The agency IAM Security Administrator must provide the Userid owner with their IAM Userid and password along with Account Activation instructions.
  - The Userid owner must go through IAM Account Activation.

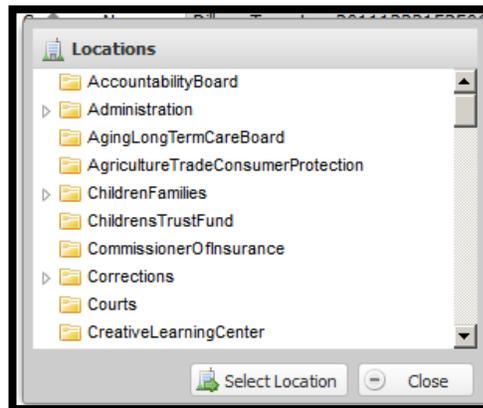
## SECTION 13. USERID TRANSFERS

There are two types of Userid transfers. An **Internal** transfer is transferring a Userid within the same agency OU from one division or bureau to another. An **Inter-Agency** transfer is transferring a Userid from one agency level OU to another agency level OU.



### Internal Transfer Example:

Transfer Userid from DOA-Gaming to DOA-Energy



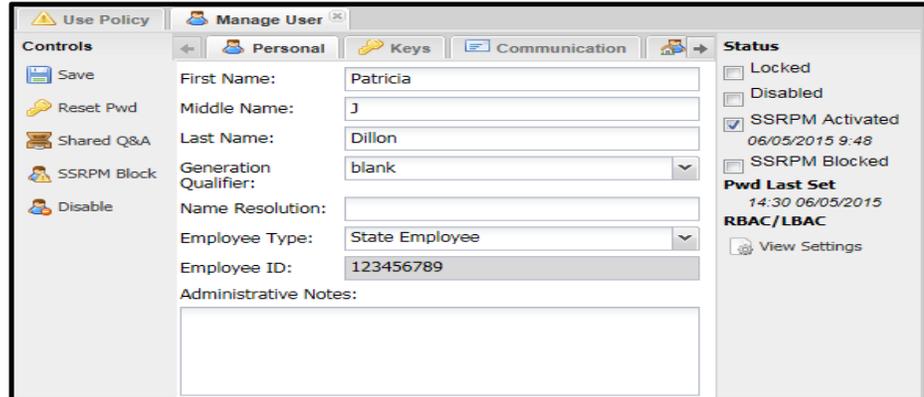
### Inter-Agency Transfer Example:

Transfer Userid from Administration to Corrections

### Internal Transfer

You may proceed to transfer the Userid if you locate the individual under one of your agency OU's. You are not able to transfer the Userid if you located it under another agency OU. You must then contact DET Security (DOA DL IAM Security or [DOADLIAMSecurity@wisconsin.gov](mailto:DOADLIAMSecurity@wisconsin.gov)) for assistance.

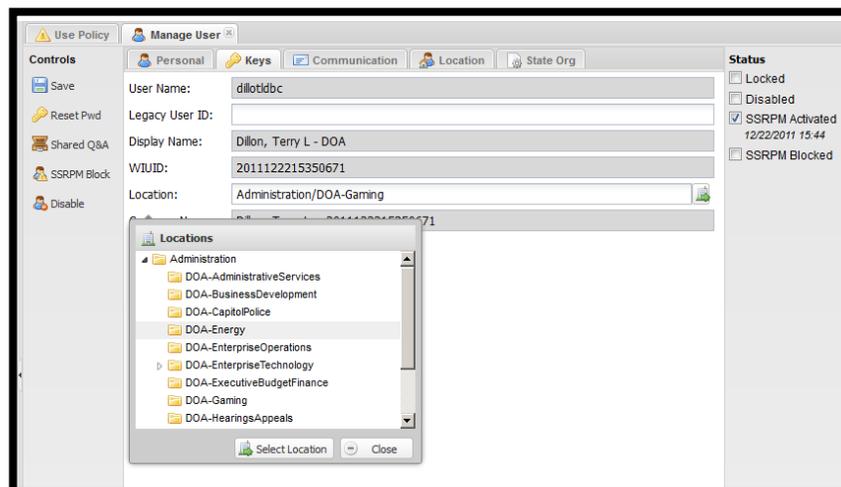
1. An Internal Transfer can be done by any agency Security Administrator that has sub OU's under their agency OU. Follow the steps in Section 1 of this document to bring up the Userid you wish to transfer. In the following example we are transferring Terry L Dillon from Administration/DOA-Gaming to Administration/DOA-Energy



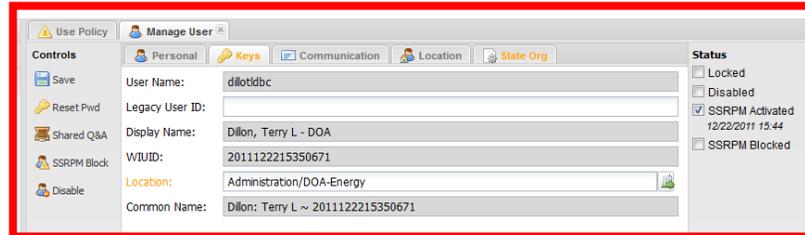
2. Press the **Keys** tab.



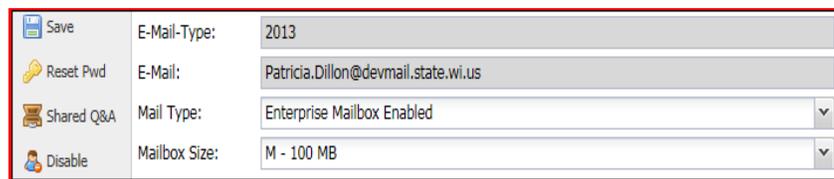
3. Press the drop down button to the right of the **Location** field. With your mouse select the location where you want the Userid transferred to. In this example the destination is DOA-Energy. Press the **Select Location** button.



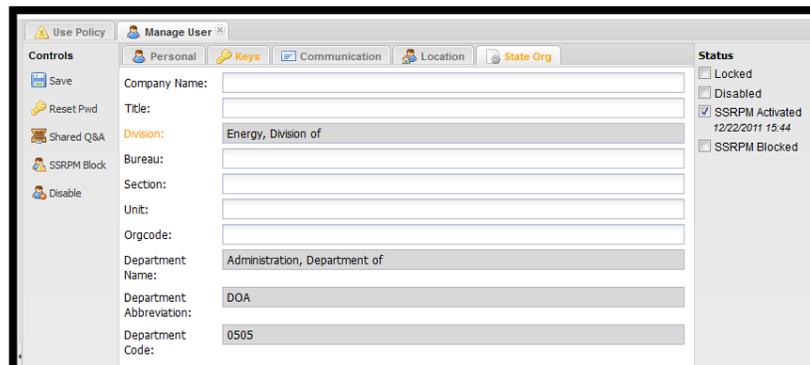
4. You will notice that the **Location** field title has changed color and the new location of Administration/DOA-Energy is in the field. You will also notice that the **State Org** tab has changed color. This is telling you that a field under this tab has changed.



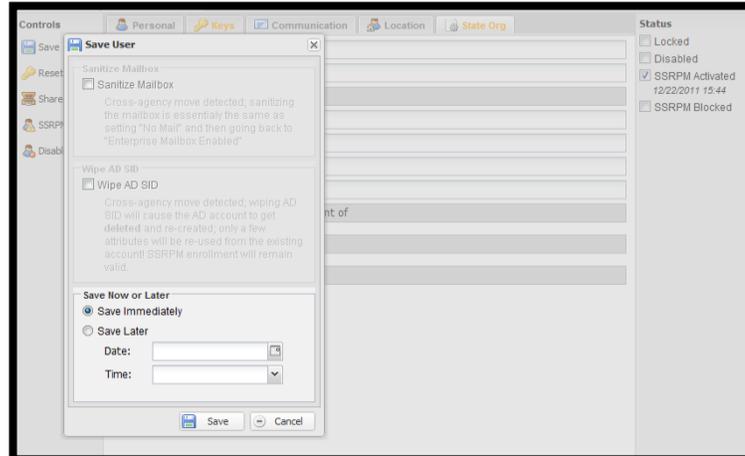
5. Press the **Communication** tab. It has been encountered that the when doing an internal transfer, the Mailbox Size will revert back to the agencies original Mailbox Size setting. Confirm that the mailbox size is correct for this userid.



6. Press the **State Org** tab. You will notice that the **Division** field title has changed color and the field contents have changed to reflect the new division contents.

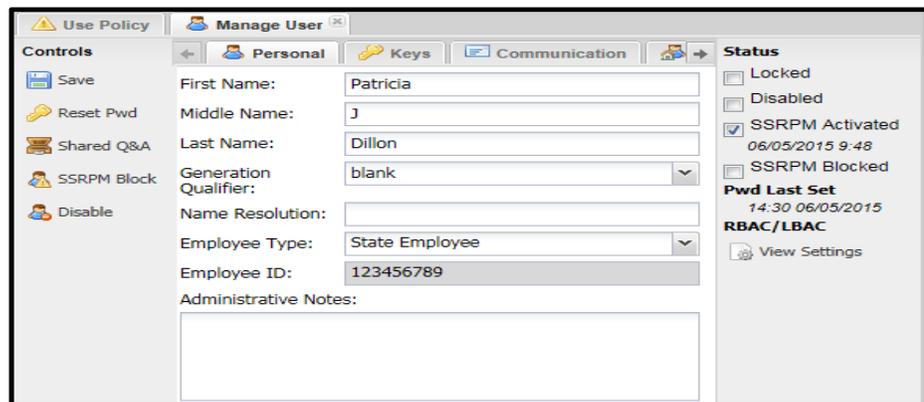


7. Press the **SAVE** button. The **Save User** box will come up. You will have the option to **Save Immediately** or schedule the save for later with **Save Later**. See Section 11 about scheduling your change

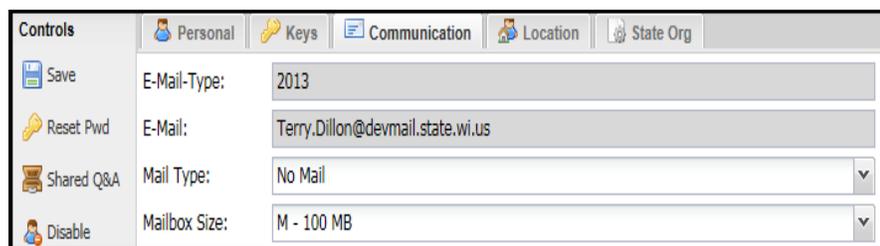


### Inter-Agency Transfer

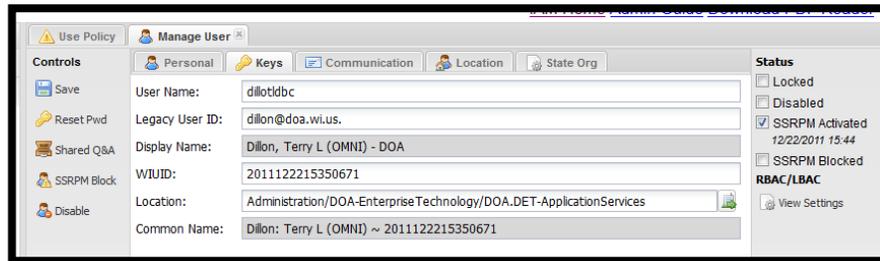
1. An Inter-Agency Transfer is a transfer of a Userid from one agency level OU to another agency level OU and is normally done by a DET IAM Security Administrator. It can also be done by an agency Security Administrator who has authority over multiple agency level OU's. Follow the steps in Section 1 of this document to bring up the Userid you wish to transfer. In the following example we are transferring Terry L Dillon from Administration/DOA-Enterprise Technology/DOA.DET-Application Services to Corrections.



2. Press the **Communications** tab. Change the Mail Type to No Mail, then **SAVE**. This will break the connection to the mailbox.



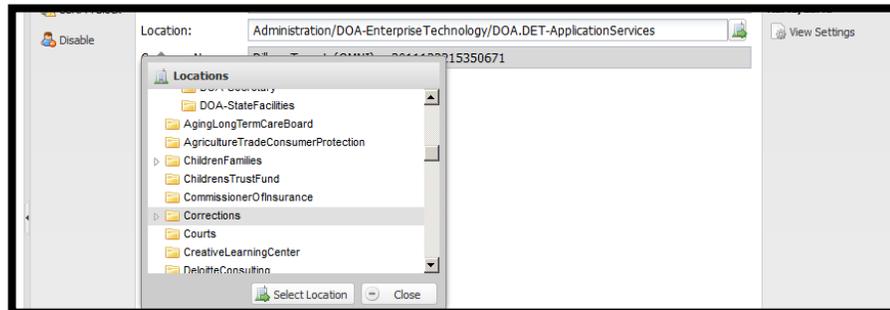
3. Press the **Keys** tab.



The screenshot shows the 'Manage User' interface with the 'Keys' tab selected. The 'Location' field is highlighted in blue. The user information is as follows:

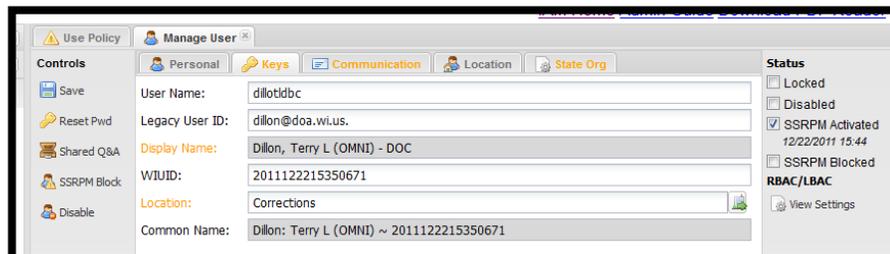
|                 |   |
|-----------------|---|
| User Name:      | dilottdbc   |
| Legacy User ID: | dillon@doa.wi.us.   |
| Display Name:   | Dillon, Terry L (OMNI) - DOA  |
| WIUID:          | 2011122215350671  |
| Location:       | Administration/DOA-EnterpriseTechnology/DOA.DET-ApplicationServices |
| Common Name:    | Dillon: Terry L (OMNI) ~ 2011122215350671                           |

4. Press the drop down button to the right of the **Location** field. With your mouse select the location where you want the Userid transferred to. In this example the destination is Corrections. Press the **Select Location** button.



The screenshot shows the 'Locations' dropdown menu open. The 'Corrections' option is selected. The 'Location' field in the background is highlighted in blue.

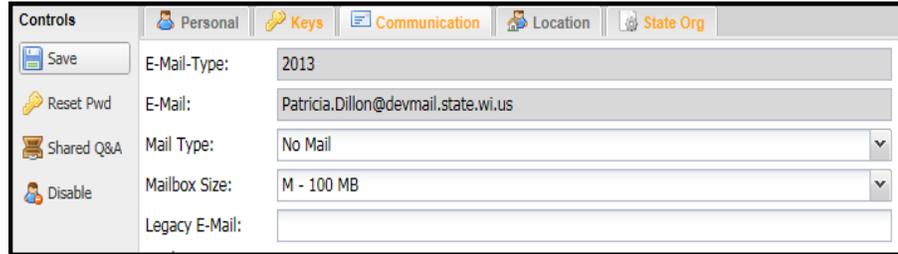
5. You will notice that the **Location** field title has changed color and the new location of Corrections is in the field. You will also notice that the **Display Name** field has changed to show the new agency in the display name. The **Communication** (not always) and the **State Org** tabs have changed color as well. This is telling you that fields under these tabs have changed.



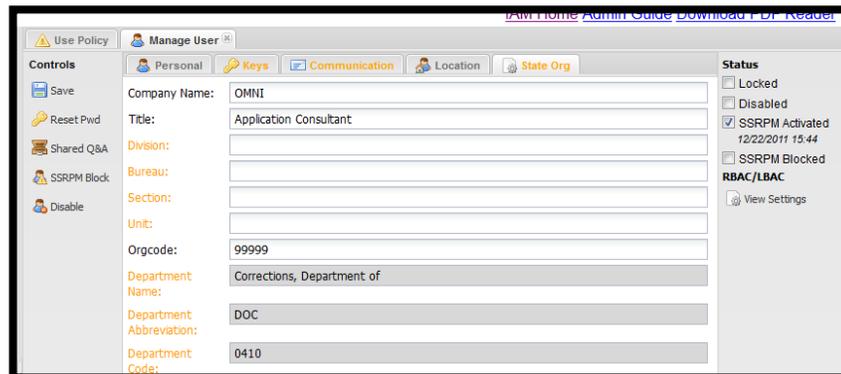
The screenshot shows the 'Manage User' interface with the 'Communication' tab selected. The 'Location' field is highlighted in blue. The user information is as follows:

|                 |   |
|-----------------|---|
| User Name:      | dilottdbc                                 |
| Legacy User ID: | dillon@doa.wi.us.                         |
| Display Name:   | Dillon, Terry L (OMNI) - DOC              |
| WIUID:          | 2011122215350671                          |
| Location:       | Corrections                               |
| Common Name:    | Dillon: Terry L (OMNI) ~ 2011122215350671 |

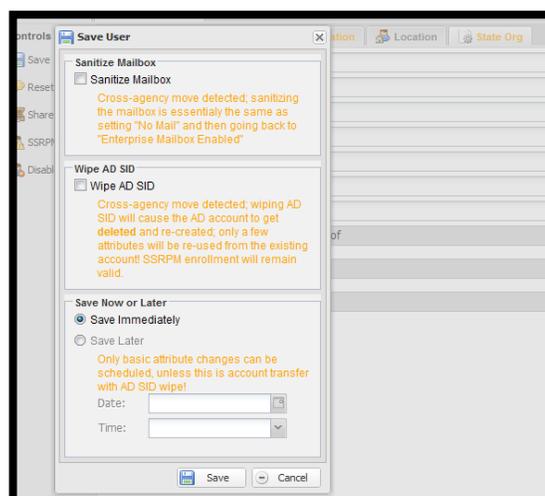
6. Press the **Communication** tab. You will notice that the **Web Mail Access** field titles has changed color and the field contents have changed to reflect the new values in this example. This tab does not always have changes.



7. When transferring from an agency with **Mail Type: Enterprise Mailbox Enabled** to an agency with **Mail Type: External Mail Enabled**, over-ride the value with **Mail Type: No Mail**.
8. Press the **State Org** tab. You will notice that the **Division, Bureau, Section, Unit, Department Name, Department Abbreviation** and **Department Code** field titles have changed color and the field contents have changed to reflect the new contents.



9. Press the **SAVE** button. The **Save User** box will come up.



- a. Click on the box in front of **Sanitize Mailbox** if you want the Emailbox sanitized.

- b. Click on the box in front of **Wipe AD SID** to get a new AD Userid created with a new SID and new password. This is the norm and would be very unusual if not checked.
  - c. You will have the option to **Save Immediately** or schedule the save for later with **Save Later**. See Section 11 about scheduling your change
  - d. Press the **SAVE** button.
10. Once the transfer is complete, agency security administrators can make all necessary informational changes to the Userid.



## SECTION 14. REQUESTING NEW SUPPORT STAFF

### Requesting a New Agency IAM Security Administrator

Current agency IAM Security Administrator

Create an IAM Userid for the new IAM Security Administrator.

Current agency IAM Security Administrator

Submit a properly filled out **Customer Data Security Officer /Representative/Authorization/ Attributes (DOA-10359)** to DET IAM Security.

DET IAM Security

Add the proper authority to the new agency IAM Security Administrator's IAM Userid.

### Requesting a New Agency Delegated Exchange Administrator

Agency IAM Security Administrator

Create a Secondary IAM Userid for the new agency Delegated Exchange Administrator.

Agency IAM Security Administrator

Send an email to DET IAM Security (DOA DL IAM Security). Provide the Secondary IAM Userid and state that the Userid be given access to the agencies Delegated Exchange group.

DOA IAM Security

Confirm authority and open a Service Request for Onestop to add the secondary IAM ID to the agencies Delegated Exchange Administrator group.

Onestop

(1) Add this Userid to the proper delegated Exchange group.  
(2) Under the Terminal Service Profile tab on the secondary IAM Userid enter in Profile Path: \\accounts\profiles\metaframe\%username%.

### Requesting a New Agency Mailbox Auditor

Agency IAM Security Administrator

Create a Secondary IAM Userid for the new agency Mailbox Auditor.

|                                   |   |
|-----------------------------------|---|
| Agency IAM Security Administrator | Send an email to DET IAM Security (DOA DL IAM Security). Provide the <u>Secondary IAM Userid</u> and state that the Userid be given access to the agencies Mailbox Auditor group.                   |
| DOA IAM Security                  | Confirm authority and open a Service Request for the AD Team to add the secondary IAM ID to the agencies Mailbox Auditor group.   |
| DOA AD Team                       | (1) Add this Userid to the proper Mailbox Auditor group.<br>(2) Under the Terminal Service Profile tab on the secondary IAM Userid enter in Profile Path: \\accounts\profiles\metaframe\%username%. |

**Requesting a New Agency Password Changer (Only)**

|                                   |   |
|-----------------------------------|---|
| Agency IAM Security Administrator | Create a Userid for the new password changer.   |
| Agency IAM Security Administrator | Send an email to DET IAM Security (DOA DL IAM Security) with the new password changer's name and IAM Userid. Add the proper authority to the new password changer's IAM Userid. |
| DET IAM Security                  |   |

**Requesting the Removal of an Agency IAM Security Administrator**

|   |  |
|---|--|
| Current agency IAM Security Administrator | Send an email to DET IAM Security (DOA DL IAM Security) requesting that IAM Security Administrator privileges be removed. Provide the former Security Administrator's name and IAM Userid. |
| DET IAM Security                          | Remove the privileges from the former IAM Security Administrator's IAM Userid.   |

**Requesting the Removal of an Agency Delegated Exchange Administrator**

|   |  |
|---|--|
| Current agency IAM Security Administrator | Delete the individuals secondary IAM Userid. This will |
|---|--|

automatically clean up their access.

**Requesting the Removal of an Agency Mailbox Auditor**

Current agency IAM Security Administrator

Delete the individual's secondary IAM Userid. This will automatically clean up their access.

**Requesting the Removal of an Agency Password Changer (Only)**

Current agency IAM Security Administrator

Send an e-mail to DET Security (DOA DL IAM Security) requesting that the IAM password changer capabilities be removed. Provide the former password changer's name and IAM Userid.

DET IAM Security

Remove authority to the former password changer's IAM Userid.

**Requesting any other type of Admin access not related to IAM or Exchange**

Current agency IAM Security Administrator

Create a Secondary IAM Userid for the new administrator.

Current agency IAM Security Administrator

Follow this link to request admin access: [Support \[ADMIN\] Account Request](#)

## SECTION 15. APPLICATION MANAGEMENT (RBAC / LBAC)

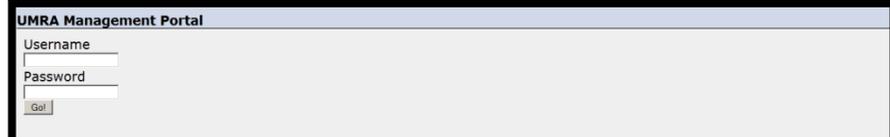
Functions in this section are performed by a Level 0 or Level 1 Security Administrator. Agency Security Administrators will not see these functions on their UMRA panel.

### Security Administrator Privileges

#### Add Privilege

To add Security Administrator privileges you must first receive a properly filled out **Customer Data Security Officer/Representative/Authorization/Attributes (DOA-10359)** form. To remove this privilege an Email must have received by DET IAM Security from an appropriate agency IAM Security Administrator.

1. Log on to UMRA at URL is <https://iam.wisconsin.gov/umra> with your IAM Userid and password.



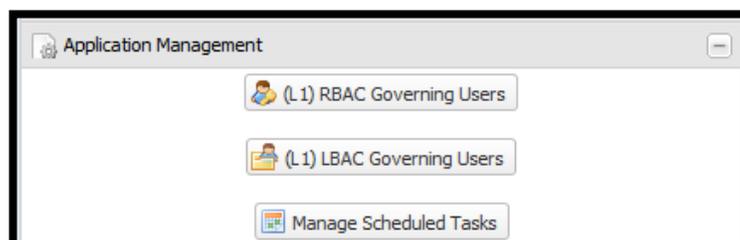
UMRA Management Portal

Username  
Password  
Go!

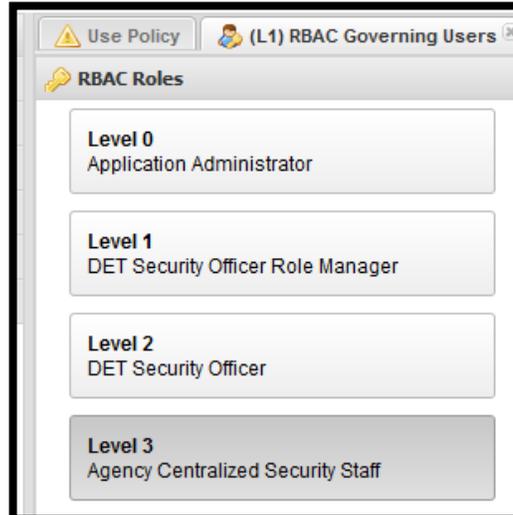
2. Press the **Application Management** bar.



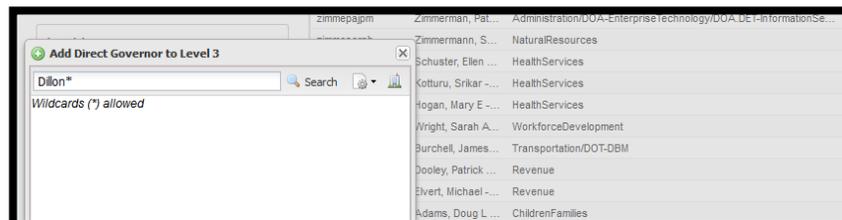
3. Press the **(L1) RBAC Governing Users** button



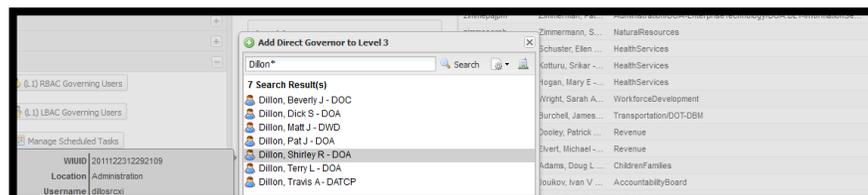
4. Press the **Level 3 (Agency Centralized Security Staff)** button. **NOTE: A single Userid can only be a member of ONE RBAC role level.**



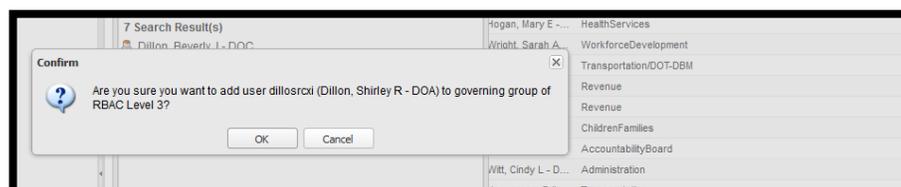
- You will see a listing of current Level 3 User on the right side of your panel. To add an individual press the **Add** button. Enter in a partial **Display Name** in the **Search** field of the individual you wish to add. Press the **Search** button. **Note you are limited to alphanumeric, spaces, dashes, commas, periods, underscores, @, or asterisks (\*)**



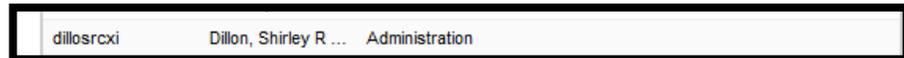
- With your mouse click on the name of the individual you wish to add.



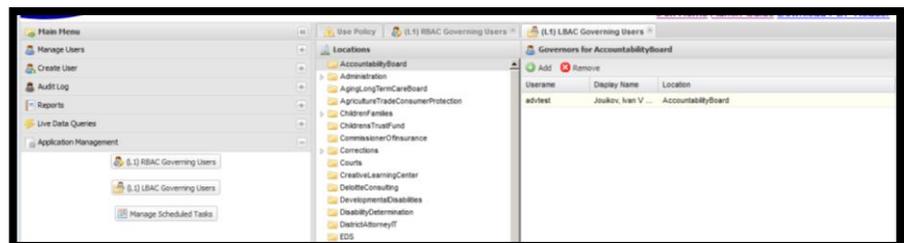
- Press the **OK** button in the **Confirm** box in reply to the question 'Are you sure you want to add user xxxxxxxxx (display name) to governing group of RBAC Level 3?'



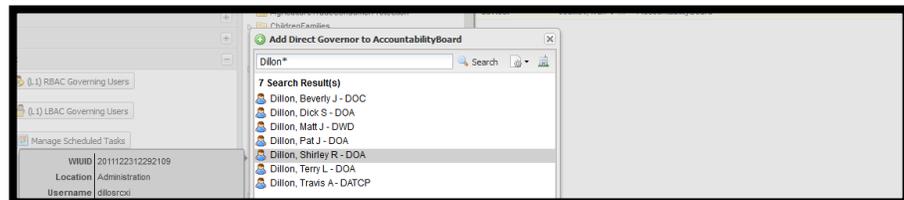
- You will notice that the user has been added to the bottom of the list. You can press the **Username, Display Name, or location** column headings to resort the listing.



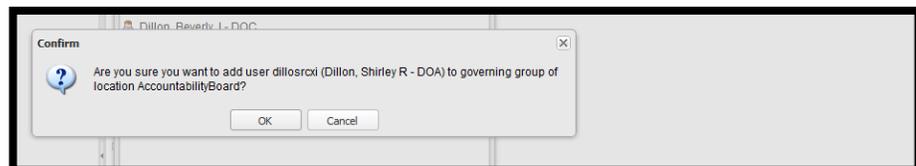
- Press the **(L1) LBAC Governing Users** button under **Application Management**. With your mouse highlight the agency you wish to add this person to as an agency security administrator. The current agency security administrators will show up on the right.



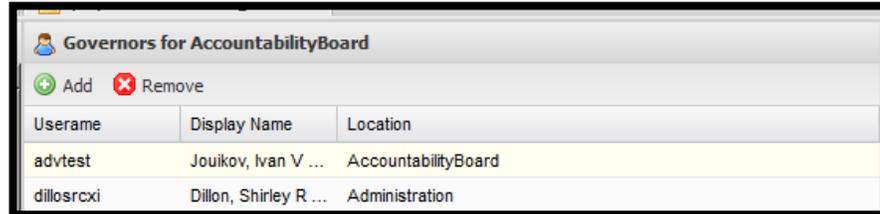
- Press the **Add** button. A search box will come up. Enter the partial display name of the individual you wish to add and press the **Search** button. With your mouse click on the individual you wish to add.



- The **Confirm** box will appear. Press the **OK** button to answer 'Are you sure you want to add user xxxxxxxxx (display name) to governing group of location "agency here"?'



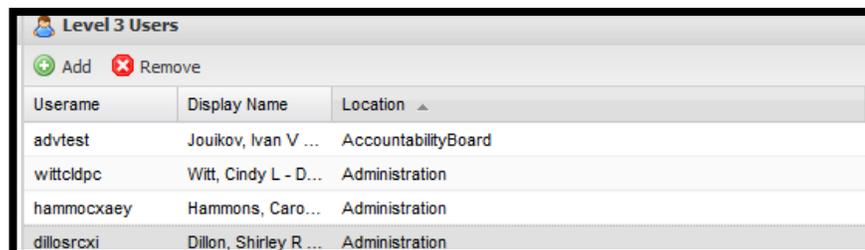
- You will notice that your new person has been added.



| Username   | Display Name          | Location            |
|------------|-----------------------|---------------------|
| advtest    | Jouikov, Ivan V ...   | AccountabilityBoard |
| dillosrcxi | Dillon, Shirley R ... | Administration      |

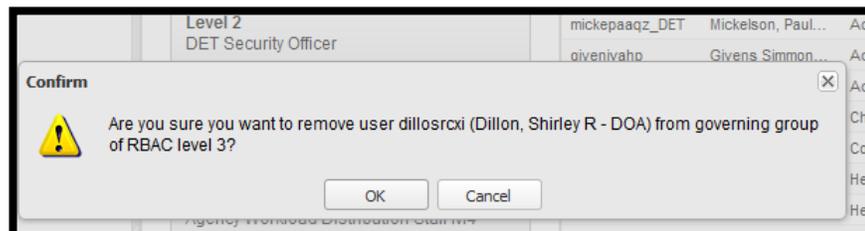
### Delete Privilege

1. Repeat steps 1 through 4 above.
2. To delete user as an Agency Security Administrator highlight their name and press the REMOVE button.

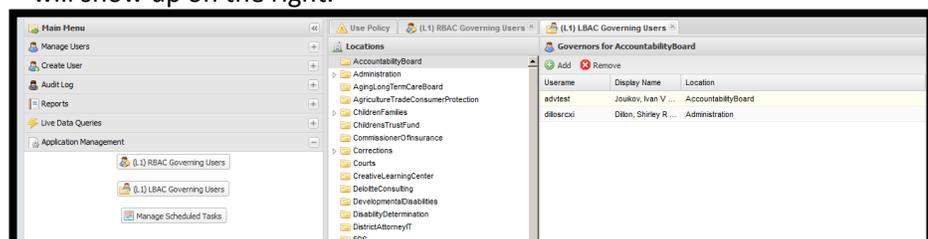


| Username   | Display Name          | Location            |
|------------|-----------------------|---------------------|
| advtest    | Jouikov, Ivan V ...   | AccountabilityBoard |
| wittclpdc  | Witt, Cindy L - D...  | Administration      |
| hammocxaey | Hammons, Caro...      | Administration      |
| dillosrcxi | Dillon, Shirley R ... | Administration      |

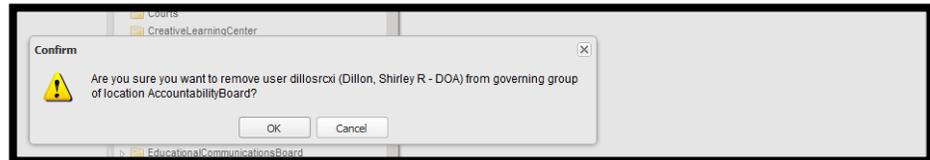
3. In the **Confirm** box answer 'Are you sure you want to remove user xxxxxxxxx (display name) from governing group of RBAC level 3 by pressing the **OK** button.



4. You will note that the individuals name has disappeared from the list.
5. Press the **(L1) LBAC Governing Users** button under **Application Management**. With your mouse highlight the agency you wish to remove this person from as an agency security administrator. The current agency security administrators will show up on the right.



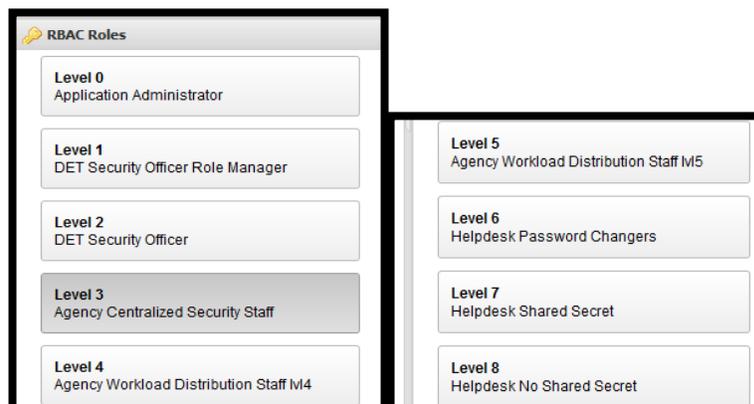
- With your mouse highlight the name of the individual you wish to remove. Press the **REMOVE** button. The **Confirm** box will come up and press the **OK** button in answer to the question 'Are you sure you want to remove user xxxxxxxxx (display name) from governing group of location 'agency name here'?'



- You will note that the individuals name has disappeared from the list.

### Other RBAC Roles

There are other RBAC Roles that a Level 0 and Level 1 Administrator could be adding and removing. The process to do this would all following the same format as steps 1 – 19 above which covered adding and deleting an agency security administrator. Levels 1 through 4 require a **Data Security Officer/Representative/Authorization/Attributes (DOA-10359)** form. Levels 5 through 8 require an email from the appropriate authoritative party. **NOTE: A single Userid can only be a member of ONE RBAC Roles level**



Level 0 – UMRA Technical Support Staff

Level 1 – Enterprise Security Administrator (Manage Roles)

Level 2 – Enterprise Security Administrator

Level 3 – Agency Security Administrator (Centralized)

Level 4 – Agency Security Administrator (Distributed)

**Same as level 3 without the capability to perform TRANSFER's or view SCHEDULED changes.**

Level 5 – Agency support for specific field

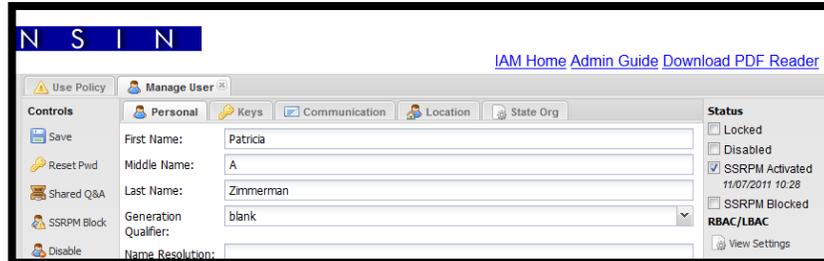
Level 6 – Password Changers

Level 7 – Browse Userids (including Shared Secret Question/Answer)

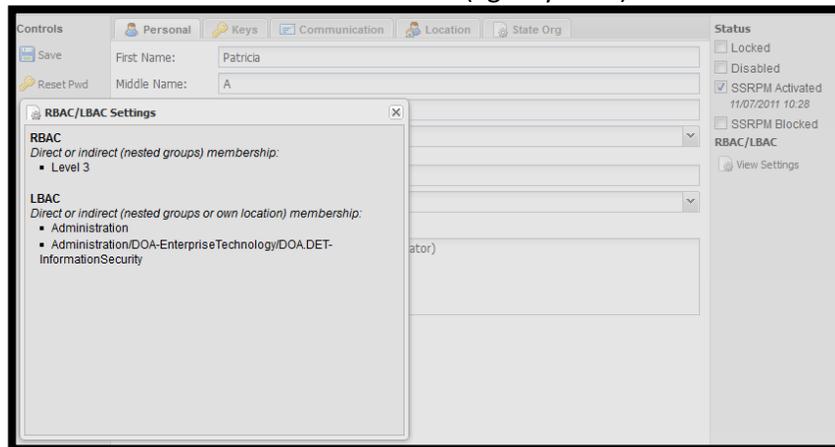
Level 8 – Browse Userids (excluding Shared Secret Question/Answer)

**Display Current RBAC and LBAC Settings**

1. Follow the steps in section 1 to retrieve the Userid you wish to view.



2. On the right side of the panel click on the **View Settings** button. The **RBAC/LBAC Settings** box will open up showing you the RBAC levels that the Userid is a member of and the LBAC (agency OU's) that the Userid can manage.



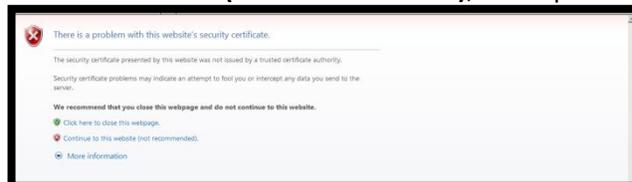
## SECTION 16. OTHER REPORTING

This section provides information on other reports that are currently available or generated.

### Enterprise Email Mailbox Size Report (Run Ad-Hoc)

This report is available to each agency IAM Security Administrator in Ad Hoc mode (run as you need it). It is a listing of each Enterprise mailbox and its current size. The layout is similar to below.

1. Go to URL [https://stateftp.wi.gov/DOA/statenet/iam\\_reports/](https://stateftp.wi.gov/DOA/statenet/iam_reports/)
2. Press **Continue to this website (not recommended)**, if this panel comes up



3. Press the **YES** button in the Security Warning box, (if this panel comes up)



4. Enter in your IAM Userid and password. Then press the OK box.



5. Right click on **MailboxSize.csv**.



## Enterprise FTP Services

WARNING: ACCESS IS RESTRICTED TO AUTHORIZED USERS ONLY.  
ALL ACCESS TO THIS SYSTEM IS RECORDED AND MONITORED.  
Please contact the DET helpdesk if you have any problems.



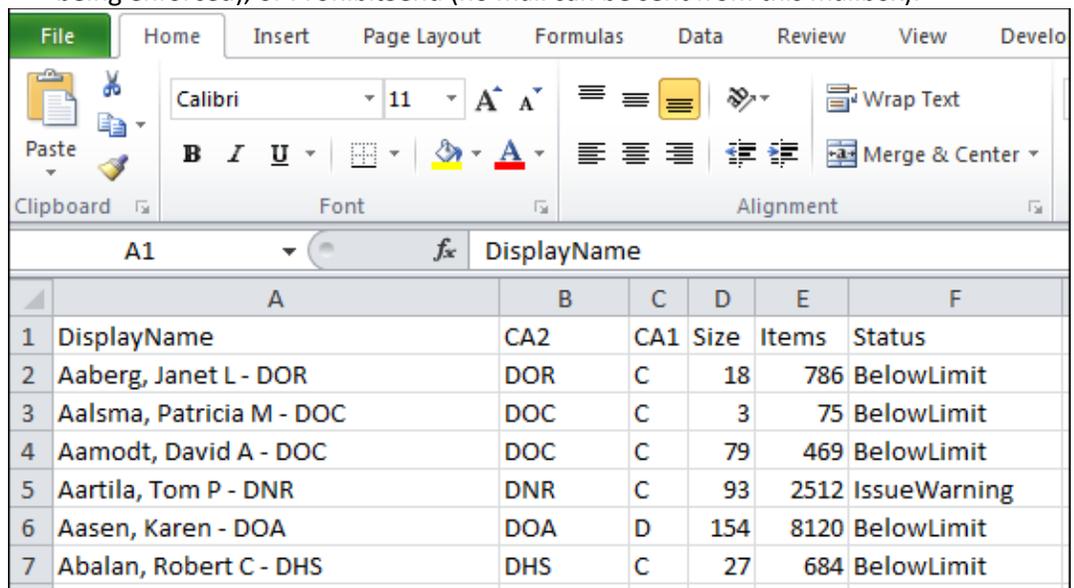
stateftp.wi.gov - /DOA/statenet/iam\_reports/

---

[To Parent Directory]

|             |       |  |
|-------------|-------|--|
| 12 Sep 2013 | 08:43 | 2026626 MailboxSize.csv                |
| 13 Jun 2011 | 14:12 | 40336485 WI-DOA DET Exchange Archiving |

6. Select SAVE TARGET As... and download the report to your machine. Press the SAVE button.
7. Once the download is complete open the .CSV file with Excel.
8. A formatted report looking similar to the one below will be displayed. The report is sorted by name (lastname, firstname). Columns are Displayname (as in the GAL), agency associated with the email account (CA2), the mailbox class size (CA1), the size of the mailbox (in MBs), the number of items in the mailbox, and the status. The status can be BelowLimit (under the restricted mailbox size), IssueWarning (size warning email sent to mailbox owner), MailboxDisabled, NoChecking (no size limit being enforced), or ProhibitSend (no mail can be sent from this mailbox).



|   | A                        | B   | C   | D    | E     | F            |
|---|--------------------------|-----|-----|------|-------|--------------|
| 1 | DisplayName              | CA2 | CA1 | Size | Items | Status       |
| 2 | Aaberg, Janet L - DOR    | DOR | C   | 18   | 786   | BelowLimit   |
| 3 | Aalsma, Patricia M - DOC | DOC | C   | 3    | 75    | BelowLimit   |
| 4 | Aamodt, David A - DOC    | DOC | C   | 79   | 469   | BelowLimit   |
| 5 | Aartila, Tom P - DNR     | DNR | C   | 93   | 2512  | IssueWarning |
| 6 | Aasen, Karen - DOA       | DOA | D   | 154  | 8120  | BelowLimit   |
| 7 | Abalan, Robert C - DHS   | DHS | C   | 27   | 684   | BelowLimit   |

## SECTION 17. IAM USERID FIELD DESCRIPTIONS

### Personal Tab

#### UMRA Fields

First Name  
Middle Name  
Last Name  
Generation Qualifier  
Name Resolution  
Employee Type  
Administrative Notes

#### AD Attributes

givenname required  
initials required  
sn required  
generationqualifier  
wiNamereresolution  
employeeType required  
Description

### Keys Tab

#### UMRA Fields

User Name  
Legacy Userid  
Display Name  
WIUID  
Location  
Common Name

#### AD Attributes

SamAccountName required  
wiLegacyUId  
DisplayName required  
wiUID required  
wiContainer required  
cn required

### Communication Tab

#### UMRA Fields

E-Mail  
Mail Type  
Mailbox Size  
Hide from GAL  
  
Web Mail Access  
Mailbox Disabled  
  
Legacy E-Mail  
Phone #  
Extension  
Mobil Phone #  
Pager #  
Fax #  
Assist. Phone #

#### AD Attributes

mail required  
  
required  
extensionAttribute1 required  
msExchHideFromAddressLists  
extensionAttribute2  
protocolSettings  
msExchHideFromAddressLists  
nDBoverHardQuotaLimit  
wiLegacyMail  
telephoneNumber  
Appends to *telephoneNumber*  
mobile  
pager  
facsimileTelephoneNumber  
telephoneAssistant

### Location Tab

#### UMRA Fields

Address  
Address City  
Address State

#### AD Attributes

streetAddress  
l  
st



|                 |                  |
|-----------------|------------------|
| Address ZIP     | postalCode       |
| Office          | wiLocationOffice |
| Location Street | wiMailAddrLine1  |
| Location City   | wiLocationCity   |
| Location State  | wiLocationState  |
| Location ZIP    | wiLocationZip    |

**State Org Tab**

**UMRA Fields**

|                         |
|-------------------------|
| Company Name            |
| Title                   |
| Division                |
| Bureau                  |
| Section                 |
| Unit                    |
| Orgcode                 |
| Department Name         |
| Department Abbreviation |
| Department Code         |

**AD Attributes**

|                    |              |
|--------------------|--------------|
| company            |              |
| title              |              |
| wiDivision         | OU Dependant |
| wiBureau           | OU Dependant |
| wiSection          | OU Dependant |
| wiUnit             |              |
| wiOrgCode          |              |
| department         | Required     |
| wiDepartmentAbbrev | Required     |
| wiDepartmentCode   | Required     |

**Other**

**UMRA Fields**

|                 |
|-----------------|
| SSRPM Activated |
| Block           |
| Disable/Enable  |
| Lock/Unlock     |
| Password        |

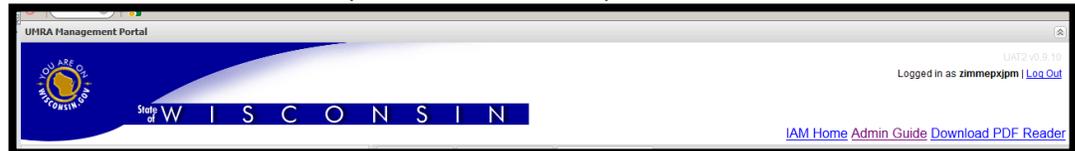
**AD Attributes**

|                    |          |
|--------------------|----------|
| wiSSRPMEnrollDate  |          |
| wiStatus           |          |
| UserAccountControl | Required |
| UserAccountcontrol | Required |
| userPassword       | Required |

## SECTION 18. OTHER INFORMATION

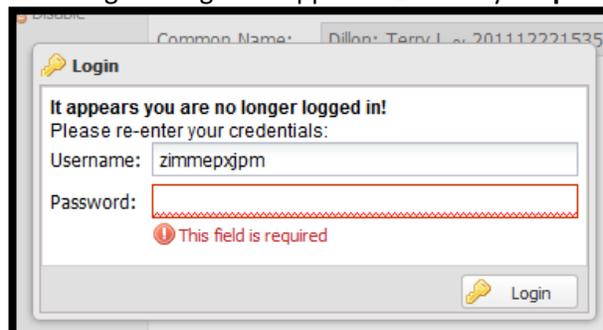
### IAM Administrator Guide

A current copy of the IAM Administrator guide is available in UMRA in the upper right hand corner. It is a PDF and you can download or print it.

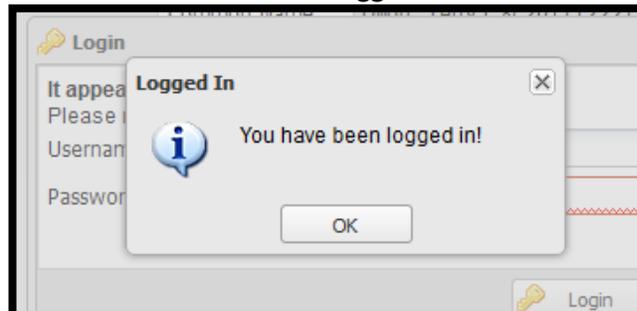


### Session Timeout

A UMRA session will timeout in 20 minutes, but it will not automatically log you off. Your last window will stay open. When you come back and attempt to do something the following message will appear. Enter in your **password** and press the **Login** button.

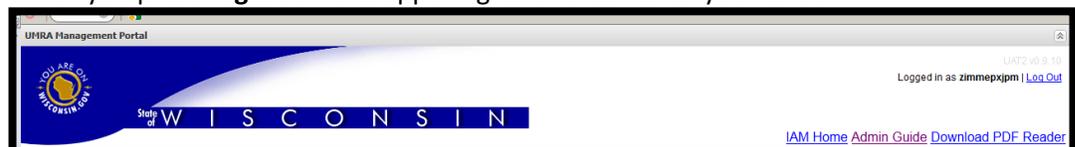


Press the **OK** button in the **Logged In** box. You can now continue working.

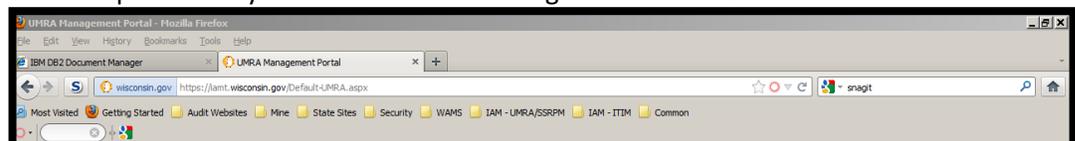


### Session Log Out/Closing Your Browser

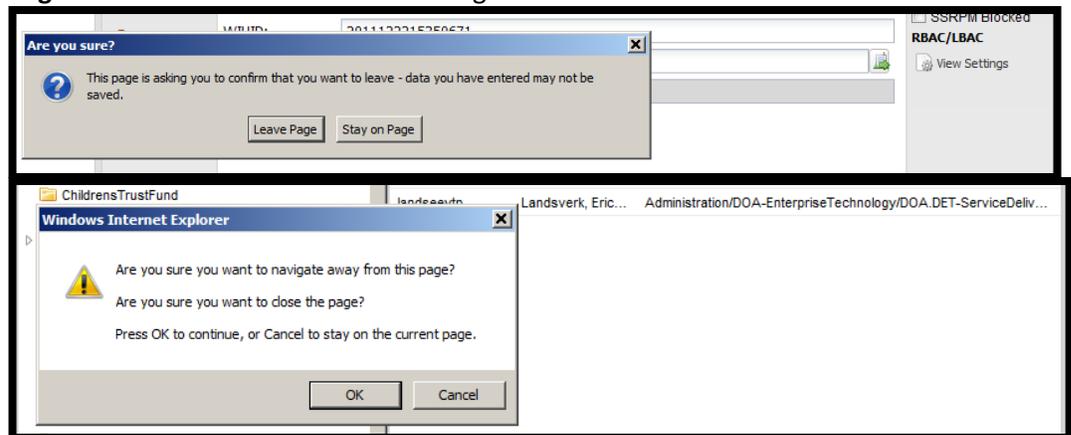
When you press **Log Out** in the upper right hand corner of your screen



Or attempt to close your browser window or go to a new URL

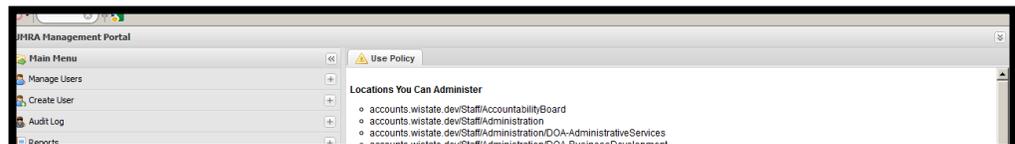
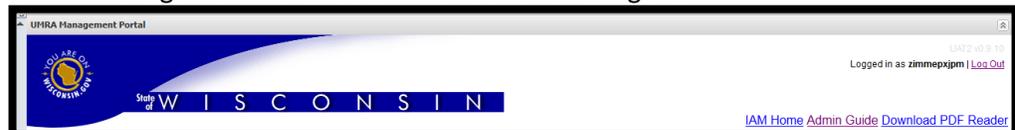


The **Are you sure?** or **Windows Internet Explorer** box will come up. Press the **Leave Page** or **OK** button. Your session will log out.



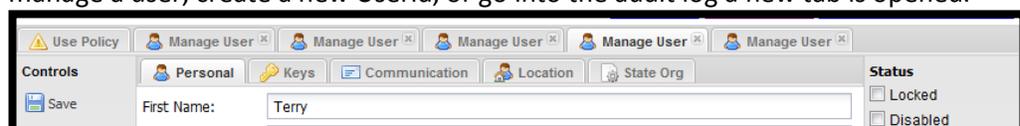
### Header Drop Down

Some monitors have a shortage of screen space when working with UMRA. You can reduce the size of the UMRA panel by closing down the header. To do this press the button with two upward arrows in the upper right hand corner (directly across from the UMRA Management Portal title). The header is now gone.

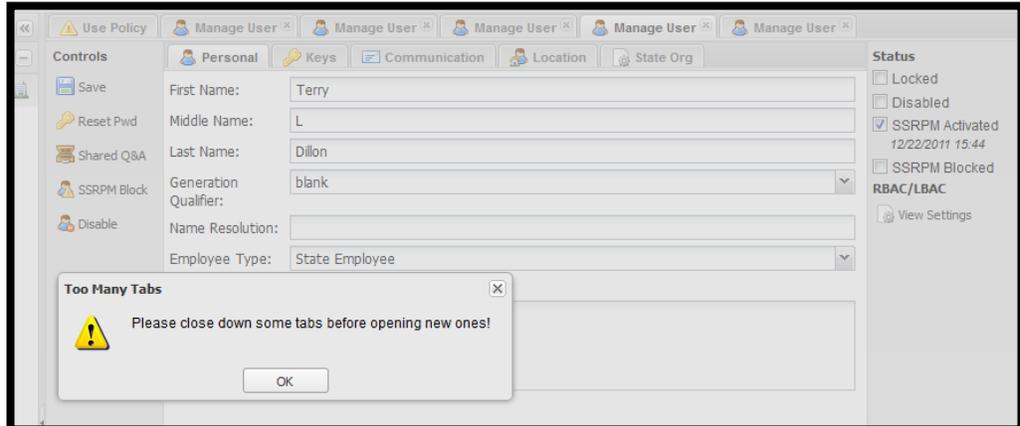


### Tab Count Restriction

Near the top of the UMRA panel under the heading you will notice that each time you manage a user, create a new Userid, or go into the audit log a new tab is opened.



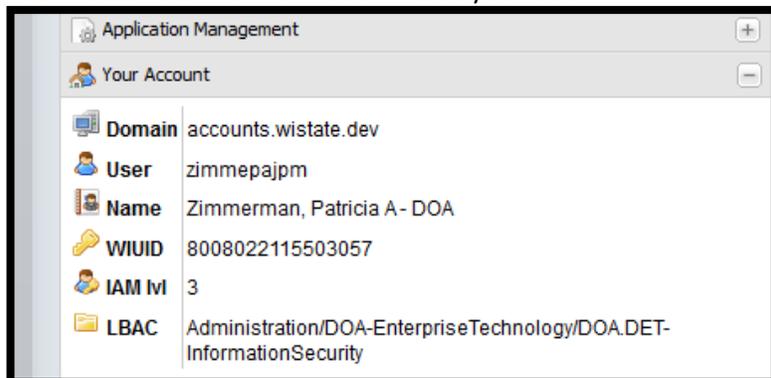
You are limited to a maximum of 5 tabs (not counting the **Use Policy** tab). When you perform an UMRA function that would open a 6<sup>th</sup> tab you will receive the error 'Please close down some tabs before opening new ones'. Press the **OK** button in the **Too Many Tabs** box to continue. Then close some of your tabs.



The reason for this restriction is that the number of open tabs has an impact your UMRA session performance.

### Your Account Tab

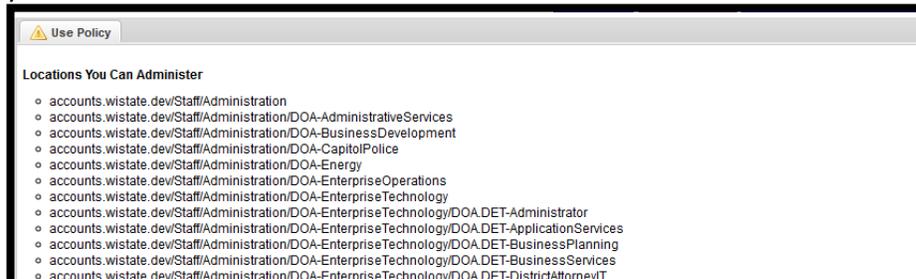
When you sign on to UMRA you will notice in the lower left side of the panel under the **Your Account** tab is information about your Userid.



You will see your **Domain**, **User** (Userid), **Name** (Display Name), and **WIUID**. The **IAM lvl** is the security role that your Userid is using. The **LBAC** is the location of your Userid in the tree.

### Locations You Can Administer

When you sign on to UMRA under the **Use Policy** tab you will see a listing of OU's that your Userid is authorized for administer.



\*\*\*\*\* End of Manual \*\*\*\*\*