



icam
YOUR KEY TO USDA

Office of the Chief Information Officer
Identity, Credential, and Access Management Program

Identity Manager User Guide

Access Role Administrator

January 2020

Document Revision and History

TABLE 1: Document Revision and Version Information

VERSION NO.	DATE	DESCRIPTION	AUTHOR/APPROVAL
1.0	08.2017	Initial Draft	J.G.
1.0	08.2017	Branding, 508 Compliance	G.R.
2.0	04.2019	Support section update	J.G.
2.0	04.2019	508 Compliance	G.R.
2.1	07.2019	Changed role name to remove agency specific designation	J.G.
2.2	01.2020	Updated Support Information	J.G.
2.2	01.2020	Review, 508 Compliance	G.R.

Table of Contents

1.	Introduction	4
2.	Log into Identity Manager	5
3.	Users Tab	6
4.	Roles and Tasks Tab	13
5.	Support	16

1. Introduction

1.1 Document Purpose

This document is a reference guide for using the access role management capabilities of EEMS. This document provides detailed instructions for:

- Logging into the EEMS Identity Manager interface
- Viewing the access roles in your management scope
- Searching for end-users in your management scope
- Modifying the membership of the access roles in your management scope
- Assigning roles to users in your management scope

This document demonstrates how an IT Support Administrator can assign the MobileLinc IT Support Specialist role to IT Support Specialists, so they can assign the role of MobileLinc user to personnel within their agency.

1.2 Audience

This document is intended for USDA Agency access role managers. Agency access role managers are responsible for managing the membership of the roles defined in EEMS that are used to access the Agency's applications or systems.

1.3 Scope

This document provides information on the access role management capabilities of EEMS only. This document is not a comprehensive guide for all EEMS administrative functionality. This document should be used by those meeting the "Audience" description and is not intended for dissemination to end-users.

1.4 Terms & Definitions

For definitions see the [Identity, Credential, and Access Management \(ICAM\) Glossary](#) located on the [ICAM USDA Connect site](#).

2. Log into Identity Manager

2.1 Access the Identity Manager User Interface

To access EEMS Identity Manager, go to the following URL: <https://www.eauth.usda.gov>

Select **Update** your account and log in with your eAuthentication credentials

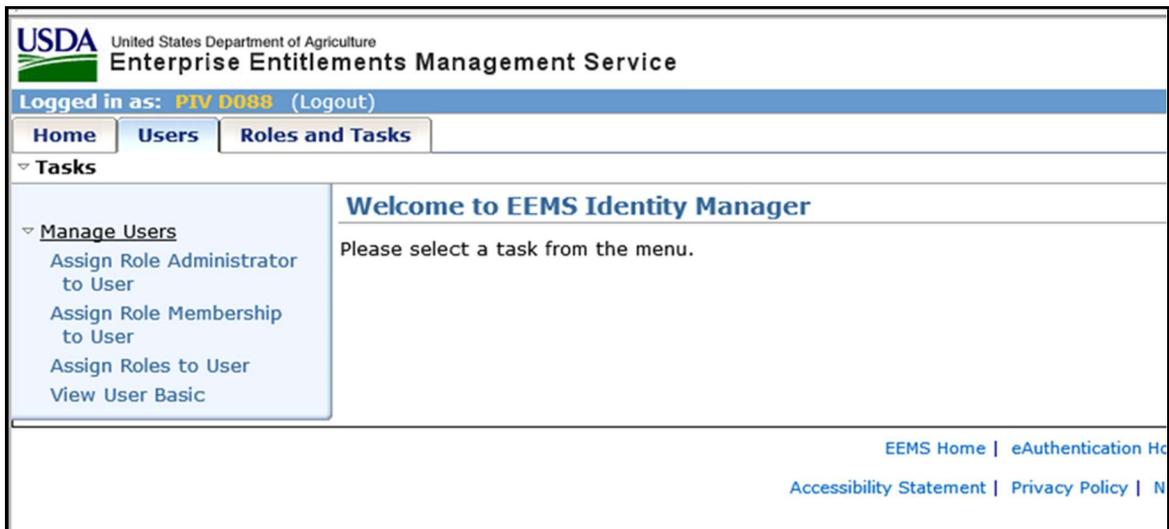
2.2 View Your Tasks

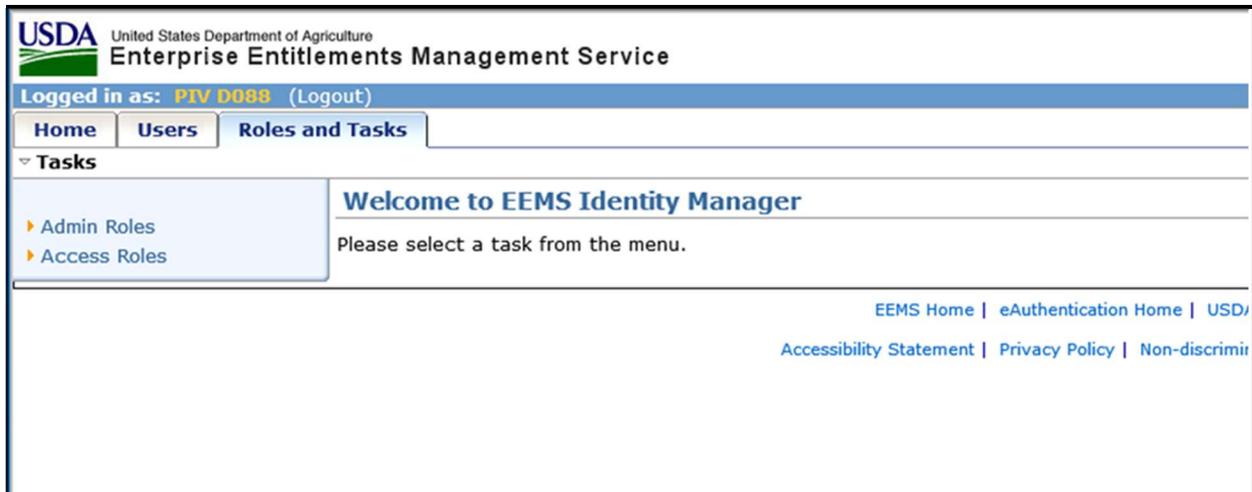
Upon login, you will see a “Welcome to CA Identity Manager” message

Click on the functional navigation tabs at the top of the screen to view your tasks (Figure 1). As an “Access Role Manager” you will have at least the following tasks available to you:

TA	TASK	DESCRIPTION
Home	View My Roles	View your own role membership
Home	View My Submitted Tasks	Search and view tasks or changes you have submitted
Users	View User Basic	Perform a basic user search
Users	Assign Roles to User	Assign Admin, Access, and Provisioning Roles
Roles & Tasks	View Access Role Members/Administrators	View the members and administrators for a role
Roles & Tasks	Modify Access Role Members/Administrators	Modify the members and administrators for a role

FIGURE 1: Welcome to Identity Manager





3. Users Tab

3.1 View User Basic Task

This task will allow you to search for users and view limited profile information. If you are familiar with EEMS searching, you may skip to section 3.2

1. To begin, click on the **Users** tab at the top of the screen
2. Click on the **Manage Users** link to expand the list of tasks
3. Select the **View User Basic** task to search for a user

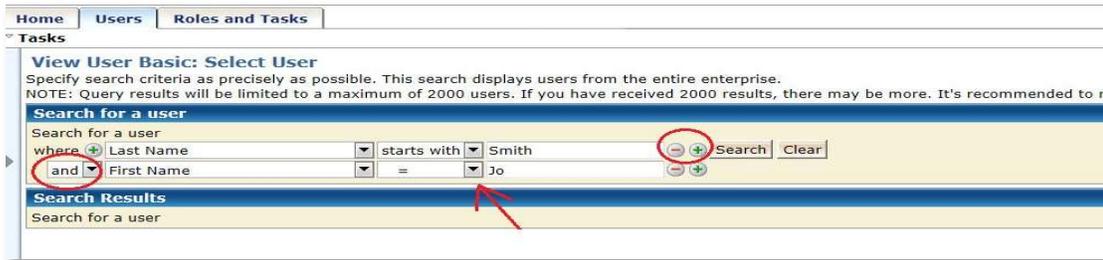


3.1.1 User Search Screen

A user search screen will appear with several search options (Figure 2)

You can search for a user by choosing from a list of pre-defined search attributes (e.g. “Last Name”) and a list of search operators (e.g. “equals,” “starts with,” etc.)

1. Input values to search for in the free form text field (*remember to remove the default value*)
2. To add or remove additional search criteria, click the  or the  button
3. Change the “and/or” field as necessary
4. Click on the **Search** button

FIGURE 2: User Search Screen


Home Users Roles and Tasks

Tasks

View User Basic: Select User

Specify search criteria as precisely as possible. This search displays users from the entire enterprise.
 NOTE: Query results will be limited to a maximum of 2000 users. If you have received 2000 results, there may be more. It's recommended to r

Search for a user

Search for a user

where Last Name starts with Smith Search Clear

and First Name = Jo

Search Results

Search for a user

Tips:

- Searching by Last Name “starts with” will include users with suffixes (e.g., Jr, Sr, III, etc.)
- Searching by Last Name (rather than Login ID) will help you identify the correct account if a user has multiple accounts

3.1.2 Search Results

A search results screen will display a list of registered users who match your search criteria, along with a summary of their profile information

1. If there are a large number of users returned, click the arrows (> >>) at the bottom of the page to view additional users
2. Select a user by clicking the radio button next to the *Login ID* and then press the **Select** button (Figure 3)

Note: You must click on the button; if you press **Enter** on your keyboard you will get an error message

FIGURE 3: User Search Results


View User Basic: Select User

Specify search criteria as precisely as possible. This search displays users from the entire enterprise.
 NOTE: Query results will be limited to a maximum of 2000 users.

Search for a user

Search for a user

where Login ID = eems.doc Search Clear

Search Results

1-1 of 1

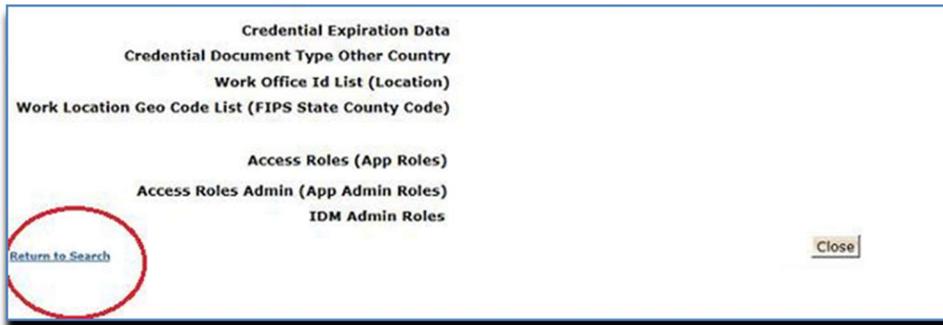
Select	Login ID	Last Name	First Name	Agency Abbreviation List	Agency Status List	Email	eAuth Internal ID	HSPD12 PID	State	eAuthentication Assurance Level
<input checked="" type="radio"/>	eems.doc	Documentation	EEMS	C_IT:OCIO	C_IT:A				TestState	2

1-1 of 1

Select Cancel

3.1.3 User Profile Details

After selecting a user, you will be able to view additional limited profile information. To return to the search screen click the **Return to Search** link at the bottom left of the screen (Figure 4)

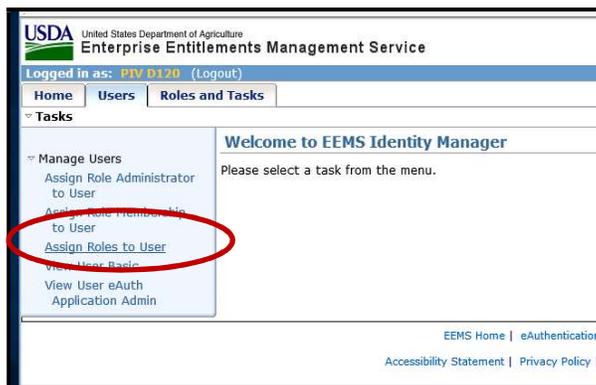
FIGURE 4: User Profile Details


3.2 Assign Role to User

This task will allow you to view /assign roles within your management scope. This is the preferred task for assigning access roles to a single user

NOTE: Not all roles may be visible to you, nor will all users populate when searching for a user after the role has been selected. This is due to your permission level and properties of the user

1. To begin, click on the **Users** tab at the top of the screen
2. Clicking on the **Manage Users** link
3. Select the **Assign Role to User** task (Figure 5)

FIGURE 5: Assign Role Administrator to User


3.2.1 Search for a User

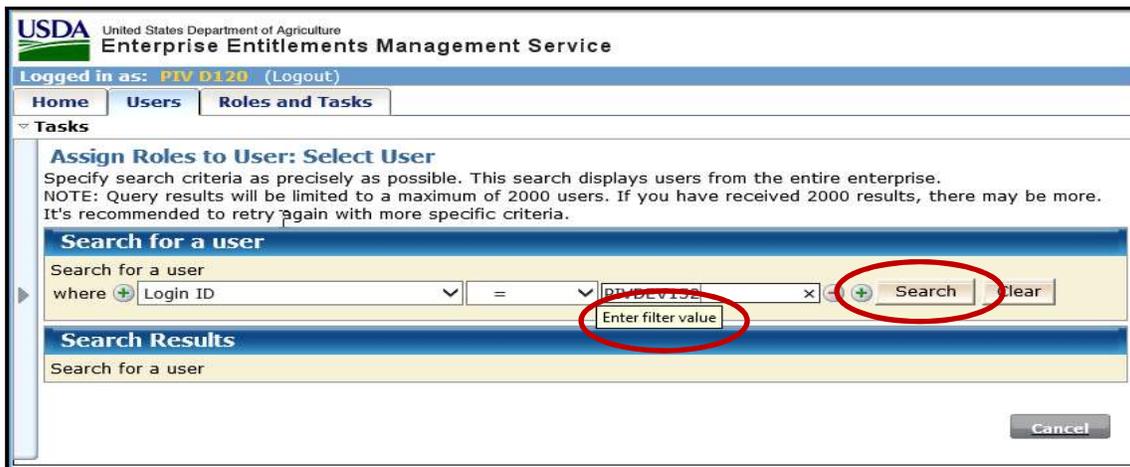
Like the **View User Basic** task described in section 3.1.1, a user search screen will appear with several search options (Figure 6)

You can search for a user by choosing from a list of pre-defined search attributes (e.g. "Last Name") and a list of search operators (e.g. "equals," "starts with," etc.)

1. Input values to search for in the free form text field
(remember to remove the default value)

2. To add or remove additional search criteria, click on the  or the  button
3. Change the “and\or” field as necessary
4. Click on the **Search** button

FIGURE 6: View Basic User



Tips:

- Searching by Last Name “starts with” will include users with suffixes (e.g., Jr, Sr, III, etc.)
- Searching by Last Name (rather than Login ID) will help you identify the correct account if a user has multiple accounts

Note: If you wish to confirm the list of members or administrators of a specific role, please reference section 4.1.

3.2.2 Type of Roles

Once you have selected the user you wish to assign a role to, search for the role itself.

There are three types of roles: “Provisioning”, “Access”, and “Admin”.

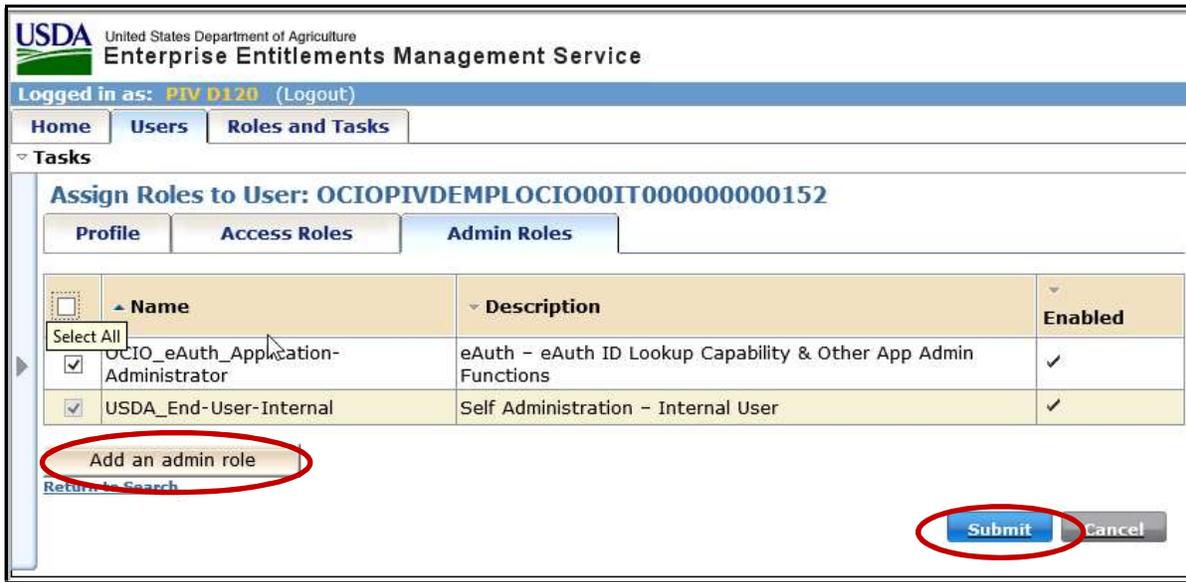
Note: Depending upon your management scope you may not see the *Provisioning* or *Admin* tabs. Also, if a user is not permitted to have a role, it will not show up as an available option.

1. Select the type of role by clicking on the **Provisioning Roles**, **Access Roles**, or **Admin roles** tab at the top of the user’s profile (Figure 7). In this case, select the Admin Roles tab.

Note: Each tab shows currently assigned roles.

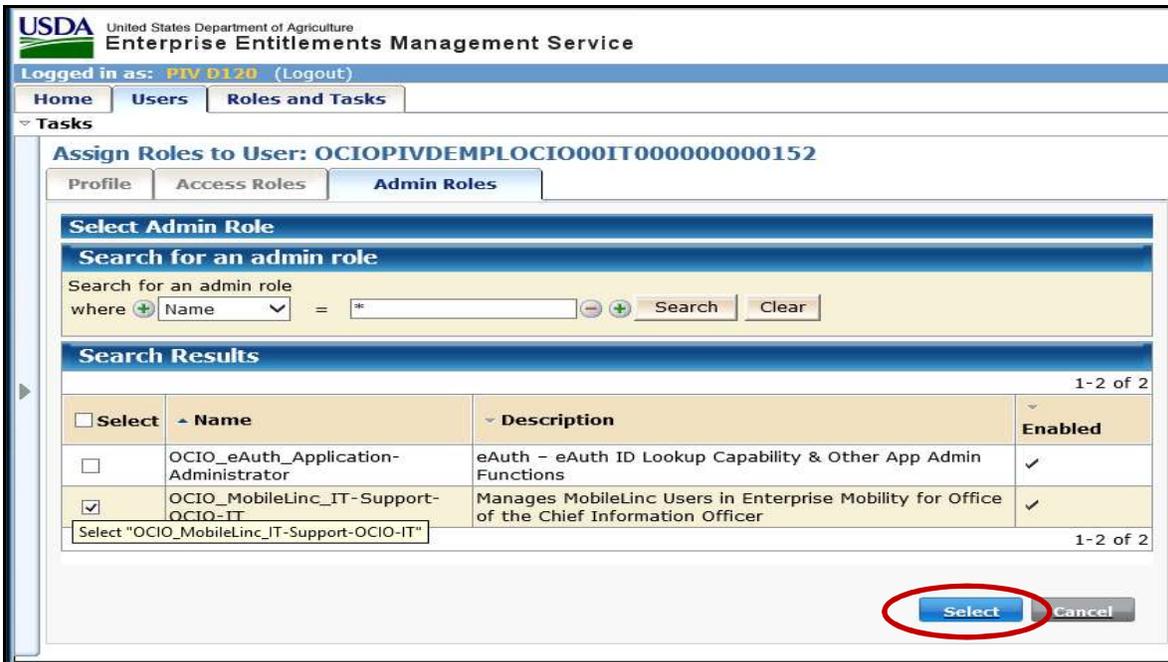
2. Select the **Add a xxxxxx Role** button. (The button name depends on the type of role you selected)

FIGURE 7: Types of Roles



- If you did not know the role name you could leave the asterisk (*) in place and click the **Search** button (Figure 8). In this case the role name is defined in 3.2.3.

FIGURE 8: Find the Role



3.2.3 Assign the Administrator Role

Find the role you wish to assign. In this case, the role name will be **OCIO_MobileLinc_IT-Support-xxx-##**.

Note: The Agency initials will be in the “xxx” and the Agency number will be “##”. All available options will have an open box next to them.

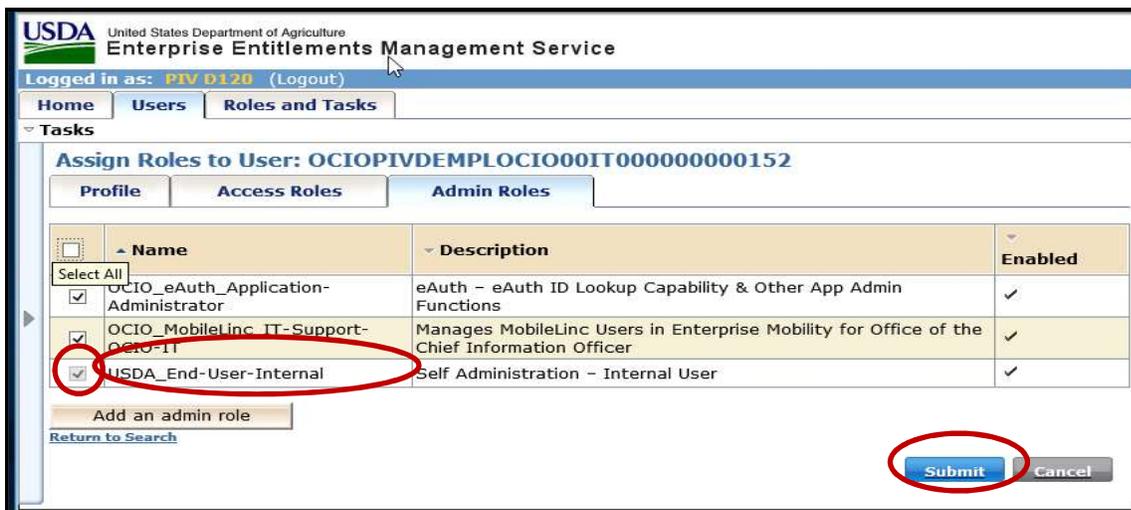
To assign the role, click the **checkbox** next to the role and click the **Select** button (Figure 9)

FIGURE 9: Select the Role



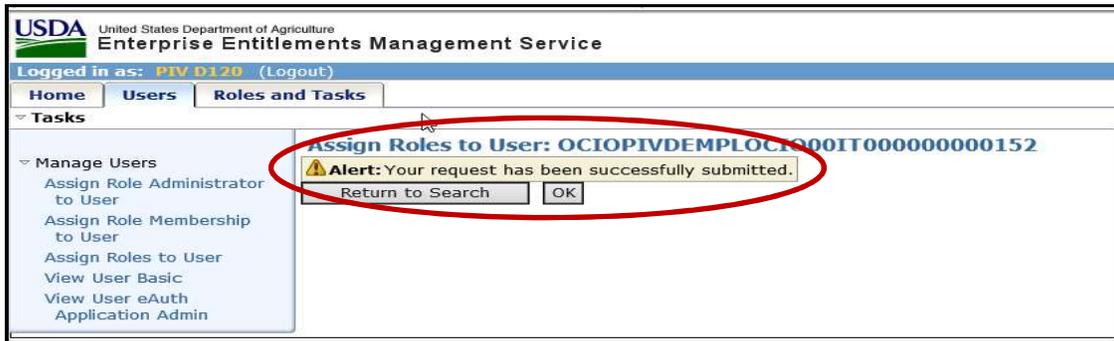
You will be returned to the list of the user’s roles (Figure 10). Confirm the new role is there and click the **Submit** button

FIGURE 10: Roles Assigned



On the next screen, you should see a success message (Figure 11)

FIGURE 11: Success Message

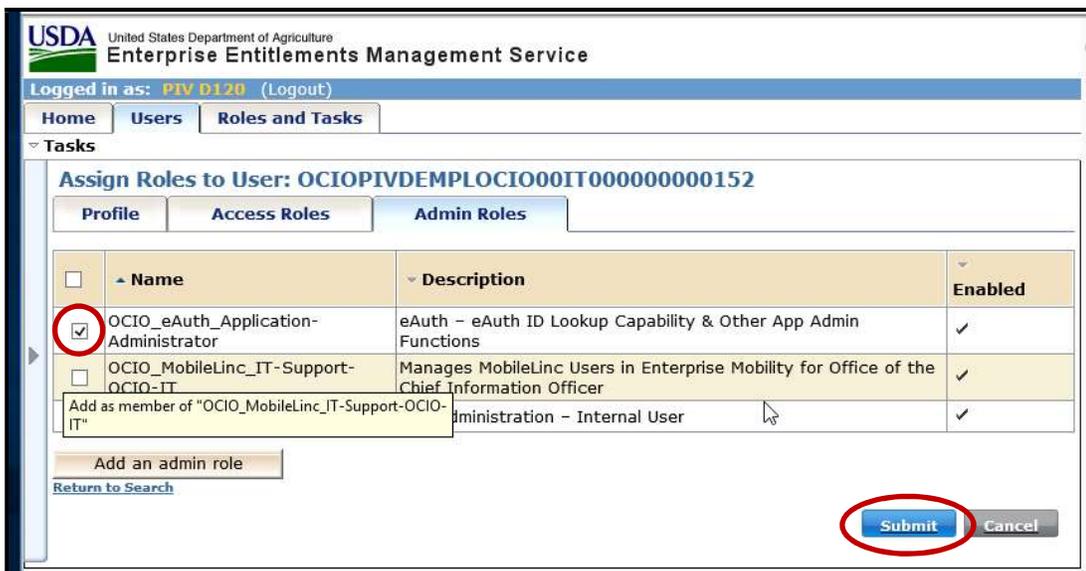


To assign roles to additional users, select the **Return to Search** button, otherwise select the OK button to return to the main screen

3.2.4 Remove the Administrator Role

1. To remove the administrative role from a user, simply uncheck the **checkbox** next to a admin role name for that user (Figure 12)
2. Click the **Submit** button

FIGURE 12: Select Users to Remove from Role



3. The next screen will indicate that the request has been successfully submitted (Figure 13)

FIGURE 13: Success Message

4. Roles and Tasks Tab

4.1 View All Access Roles Members/Administrators

The **View Access Role Members/Administrators** task will allow you to view all the members of a specific access role within your management scope. This task is often used when a list of users is needed (e.g., for reporting).



1. To begin, click on the **Roles and Tasks** tab at the top of the screen
2. Click on the **Access Roles** link
3. Select **View Access Role Members/Administrators**
4. You will be presented with a listing of each role for which you are an administrator
5. Select the role you wish to manage by selecting the radio button to the left of the role name (Figure 14)
6. If there are a large number of roles returned, click the arrows (> >>) at the bottom of the page to view additional roles
7. Click the **Select** button

FIGURE 14: Role Selection Screen



4.1.1 View Members of a Role

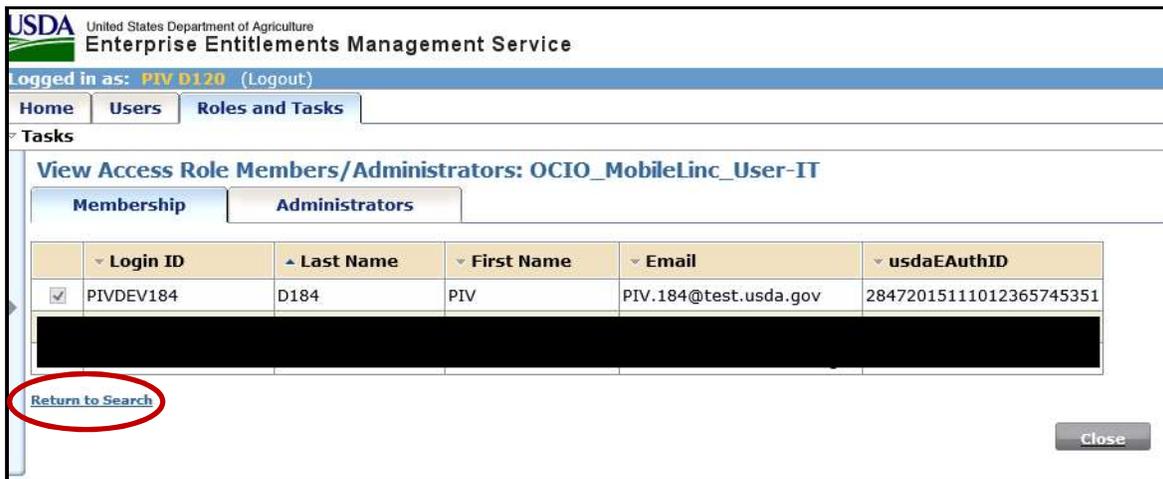
Members of the role you selected will be displayed with the following attributes for unique identification:

- Login ID (User ID)
- Last Name
- First Name
- Email
- eAuth Internal ID

If there are a large number of users returned, click the arrows (> >>) at the bottom of the page to view additional users

To view the membership of a different role, click on the **Return to Search** link (Figure 15)

FIGURE 15: View Role Membership



4.1.2 View Administrators of a Role

To view administrators of the role you selected, click the **Administrators** tab from the *View Admin Role Members/Administrators* screen (Figure 16a)

Select the radio button next to the role whose administrators you want to view. (Figure 16b), and press *Select*. Active administrators of the role will be displayed (Figure 16c) with the following attributes for unique identification:

- Login ID (User ID)
- Last Name
- First Name
- Email
- eAuth Internal ID

If there are many users returned, click the arrows (> >>) at the bottom of the page to view additional users

FIGURE 16 A: View Role Administrators



FIGURE 16 B: View Role Administrators

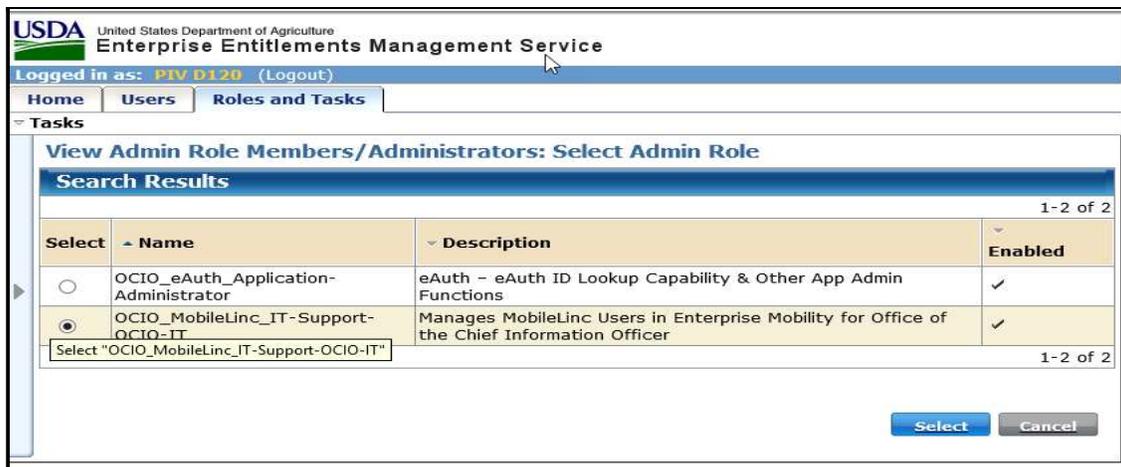
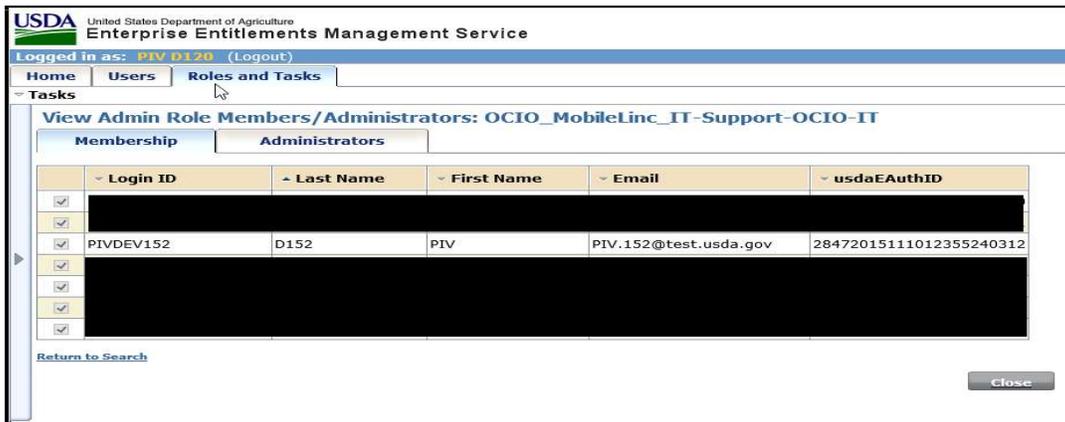


FIGURE 16 C: View Role Administrators



5. Support

Escalate unresolved through your agencies Help Desk escalation process. Include the incident ID and details and results of all troubleshooting steps.

Important Note: Internal USDA workers listed in search results may not have a fully registered account for use in accessing eAuthentication-protected applications, however roles can still be added to the user’s record and then access will be permitted once they register. Also, users must use their LincPass to log on to MobileLinc Identity Guard.