Account Management System (AMS) User Guide for Commons

Latest Update: November 17, 2021
CONTACT US

Document Comments:

We value your feedback on this document.

How are we doing? The Communications & Documentation Team of the electronic Research Administration (eRA) is dedicated to serving our community and welcomes your feedback to assist us in improving our user guides. Please send comments about the user guide to this address: eRACommunications@mail.nih.gov.

Troubleshooting support:

Please contact the eRA Help Desk:

Toll-free: 1-866-504-9552
Phone: 301-402-7469
TTY: 301-451-5939
Web: http://grants.nih.gov/support (Preferred method of contact for external users)
Web: https://inside.era.nih.gov/eRA_helpdesk.cfm (Preferred method of contact for internal users)
Email: commons@od.nih.gov (for Commons Support)
Email: helpdesk@od.nih.gov (for IMPAC II Support)
Hours: Mon-Fri, 7:00 a.m. to 8:00 p.m. Eastern Time

DISCLAIMER STATEMENT

No data shown in illustrations represents any real account, project, or individual. Any resemblance to actual accounts, projects, or individuals is purely coincidental.

TABLE OF CONTENTS

Latest Updates .................................................................................................................. 5
Overview ................................................................. 10
  Commons Management Staff .................................... 10
  User Roles ............................................................ 10
  Commons Management Staff .................................... 10
  Account Statuses ................................................... 10
Accessing AMS ....................................................... 11
  Users Who Create and Manage eRA Commons Accounts 11
Search Accounts .................................................... 13
  User Accounts ....................................................... 13
  System Accounts ................................................... 13
  Certificates ........................................................ 13
  Search for Commons User Accounts .......................... 13
    Accessing Search ............................................... 13
    The Search Accounts screen ................................ 15
  Search Options .................................................... 17
    About Locked Accounts ..................................... 17
    Commons User Account Search Results .................. 17
  Search for System Accounts ................................... 19
    System Account Search Results ............................. 21
  Funding Support Screen ........................................ 23
Create Accounts .................................................. 25
  Create User Accounts .......................................... 25
  Create System Accounts ....................................... 25
  Create a Commons account for an individual(e.g., PD/PI) 25
    Account Invitations from eRA Systems .................... 28
  Add/Delete User Roles ......................................... 29
  Set Primary Organization ...................................... 32
Create System Accounts .......................................... 34
  Add System Roles ................................................ 37
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate Certificate</td>
<td>39</td>
</tr>
<tr>
<td><strong>Manage Accounts</strong></td>
<td>43</td>
</tr>
<tr>
<td>User Accounts</td>
<td>43</td>
</tr>
<tr>
<td>System Accounts</td>
<td>43</td>
</tr>
<tr>
<td>Managing External User Accounts</td>
<td>43</td>
</tr>
<tr>
<td>Actions</td>
<td>45</td>
</tr>
<tr>
<td>Add/Delete User Roles</td>
<td>46</td>
</tr>
<tr>
<td>Affiliate Account</td>
<td>49</td>
</tr>
<tr>
<td>Unaffiliate Account</td>
<td>50</td>
</tr>
<tr>
<td>Reactivate Account</td>
<td>52</td>
</tr>
<tr>
<td>Change Password</td>
<td>53</td>
</tr>
<tr>
<td>Reset Password</td>
<td>55</td>
</tr>
<tr>
<td>Manage System Accounts</td>
<td>55</td>
</tr>
<tr>
<td>Add System Roles</td>
<td>58</td>
</tr>
<tr>
<td><strong>User Reports</strong></td>
<td>61</td>
</tr>
<tr>
<td>All Users Report Screen for External Users</td>
<td>61</td>
</tr>
<tr>
<td>Role Description Report</td>
<td>63</td>
</tr>
<tr>
<td><strong>Report Output</strong></td>
<td>63</td>
</tr>
<tr>
<td>All Users Report output</td>
<td>63</td>
</tr>
<tr>
<td>Role Description Report output</td>
<td>63</td>
</tr>
<tr>
<td>Navigating the report output</td>
<td>63</td>
</tr>
</tbody>
</table>
**Latest Updates**

Updates and new features in AMS:

**November 17, 2021**

- Passwords for eRA user accounts, which previously were required to be 8-16 characters long, must now be 15-64 characters. The full password guidelines are:
  - Password length must be between 15-64 characters
  - First and last characters cannot be numbers
  - Cannot contain username
  - Cannot re-use previous 10 generations of passwords

**September 15, 2021**

- Login via Login.gov — Starting now, users may only associate their login.gov account to a single eRA account. If the user's login.gov account is linked to multiple eRA accounts, at login AMS will prompt them to consolidate those accounts into a single account.

- [Manage Account](#) screen: Changed the label of the "login.gov exemption" field to "2FA exemption."

**Feb 16, 2021**

**Two-Factor Authentication Support:**
• New field in the Commons **Account Search Results** to display **Login via Login.gov** status (Required, Optional, or Exemption):

![Account Search Results](image)

• And in the **Manage Account** screen, two new fields to monitor Login via Login.gov functionality:

![Manage Account](image)

- **Login via Login.gov** — Shows the status of login.gov for this account: "Required," "Optional" or "Exemption."
  
  **Note:** This field is set automatically at the organization level.

- **Login.gov Exemption Expiration Date** — When Login via Login.gov is set to "Exemption," this field displays the end date for the exemption. The user can log in using eRA credentials until this date.
  
  **Note:** Login.gov exemptions are only granted on a limited basis by the eRA Service Desk and only the eRA Service Desk can modify this date.

**Apr 12, 2018**
• eRA Service Desk agents and Grant Solutions account administrators who have the UADM_USER_ROLE and the FOAM_GS_ADMIN or FOAM_GS_AGENCY_ADMIN role can create and manage accounts for GrantSolutions users. See Create GrantSolutions user accounts.

Oct 26, 2017

• The account unlock operation now requires the user to login that day: When an administrator unlocks an account that's been locked due to inactivity, an email notification is sent that asks the user to login to the account that same day. If the user does not login before the end of the day, the account is locked again.

May 18, 2017

• The temporary passwords used in system-generated Commons account invitations and password reset emails are only valid for one 24 hours: Users must log in the same day they receive the notification email, and those who attempt to login with an expired password will be redirected to the password reset/lost password workflow. For more information see Account Invitations from eRA Systems, Initial Login to eRA Account, and Reset Password.

Feb 16, 2017

• The AMS User Guide has been split into separate documents for each user domain (Agency, Commons, iEdison, State Dept). When you login to AMS, the system recognizes your domain and uses it to select the correct online help package.
• It's now possible to search for system accounts by IMPACII user ID.
• Added a more prominent link to the Person Administration module in the Manage Account and Create Account confirmation screens. Click to manage user names and other personal information.

Dec 22, 2016

• When you unlock an account, the user receives a notification saying that he or she has to login to the account on that same day or the account will be relocked. See Reactivate Account
• eRA Service Desk agents can click the **Add Roles to Other org** button to give a system account roles in another organization. See [Add/Delete System Roles](#).

• Added instructions for verifying a new Commons account when you receive a *Notification of New Account* from eRA. See [Notification of New Account](#).

**Nov 17, 2016**

• Removes all roles associated with an account when Account Coordinators or Service Desk Agents deactivate the account.

• Allows Account Coordinators to re-certify active accounts to prevent the account holder from getting locked out. Note it will be a requirement for Account Coordinators to input a comment and upload an account request form to clarify the Recertification.

• Allows eRA Service Desk Agents to reactivate users and add mapping if no mapping exists.

• Enhances Deactivated Users Report to display correct information, including Deactivated By and Account Deactivation Date.

• Updates the email notifications sent prior to account deactivation to indicate that users should contact their Account Coordinator instead of the eRA Service Desk to request account re-activation.

**Sept 15 2016:**

• The Create Account screen now lets NIH/Agency administrators search the NED system to find user profiles in their organizations. See [Create Agency Accounts](#) for more information.

• Create-Account requests for untrusted Commons accounts can now be approved or rejected automatically. See [Create Commons or external iEdison User Accounts](#) for more information.

**Aug 18 2016:**

• Enhancements to the reporting functionality, including a new internal report on deactivated user accounts. See [User Reports](#).
• Account Coordinators can now upload new or revised account request forms from the Manage Account screen. See Manage Account Request Forms for instructions.

• Account Coordinators and Service Desk agents can now search for accounts that have been locked due to inactivity and reactivate them. See Search by Status for instructions.

• New requirements for accounts with administrative roles: Once a user has held an administrative role (SO/AO, AA, BO, or TTO Admin/User) at one institution, that account cannot be changed to a strictly scientific role, and cannot be affiliated to a different institution in any administrative or scientific role: In these cases, the former administrative user must create a new account to use in his or her new role. See Affiliate Account for more information.

July 22 2016:

• Service Desk Agents can now update User IDs on their accounts.
• In the Search Results screen, the label of the Filter box has been changed to Filter Results.
• Search-by-country functionality is now available for state accounts.

June 23 2016:

• AMS validates users’ affiliations for administrative roles (SO/AO, AA or BO user roles) to make sure users have administrative roles at only one institution.

• The Account Coordinator (or the Service Desk) can now view and if necessary replace an account's Account Request Form (ARF).
Overview

The Account Management System (AMS) facilitates user and system account administration based on assigned user roles. The system provides the ability to search existing accounts. When a search is performed, all records that meet the search criteria are returned on the Search Accounts screen.

Commons Management Staff

Once the institutional account is created, the Signing Official (SO) at each grantee organization is able to establish additional user accounts with various levels of access and capability. The SO or Accounts Administrator (AA) may then create additional accounts for the administrative and scientific staff.

SOs only can also view, create, and maintain system accounts.

User Roles

The following users have the ability to search for, manage and create accounts, and to add or remove roles for user and system accounts:

Commons Management Staff

- Accounts Administrator (AA)
- Administrative Official (AO)
- Business Official (BO)
- Signing Official (SO)

Account Statuses

AMS user accounts can have the following statuses:

- Active — A valid account in good standing.
- Deactivated — Account has been disabled by an administrator
- Locked due to inactivity — Locked by the system due to inactivity (no user activity for 120 days).
- Pending Affiliation — Account has not yet been associated to an organization
- Profile Only — A profile that is not associated to a user account.
Accessing AMS

Users Who Create and Manage eRA Commons Accounts

After logging into Commons, access AMS from the Commons welcome screen by clicking the Account Management (Admin) tile, or selecting Admin from the Apps menu, as shown here:

When you take one of these actions, the AMS Search Accounts screen opens, as shown here.
For instructions on performing a search, see "Search Account."
**Search Accounts**

**User Accounts**

Use the *Search Accounts* screen to search for existing user and system account(s) within or outside of your organization or institution.

See [Search for User Accounts](#)

**System Accounts**

Agency, Commons and external iEdison users can search for system accounts

See [Search for System Accounts](#)

**Certificates**

For information on obtaining and registering a certificate from a Certificate Provider or Authority, please refer to the [Web Services Certificate (S2S) Guide](#): Section 2.4.3 for Commons users

**Search for Commons User Accounts**

**Accessing Search**

1. After logging into [eRA Commons](#), the signing official or other authorized users can access the Account Management System by selecting **Admin** from
the apps icon in the upper left corner, as shown here:

1. Or by clicking the **Account Management (Admin)** button on the [eRA Commons](#) landing page, as shown here:
2. Clicking either **Account Management (Admin)** button opens the AMS Search Accounts screen described below.

From there, they can select the **Manage Accounts** sub-menu.

**The Search Accounts screen**

Clicking on **Account Management (Admin)** opens the AMS Search Account screen shown below.

The **Search Accounts** screen for external users provides the ability to search for existing user and system account(s):
Search Accounts Screen for External Users

**NOTE:** You must enter at least one search field, besides the **User Type** and **Account Status**.

Wild card characters such as the percent sign (%) can be used to search for a string of characters.

**To Search:**

1. Enter the appropriate search criteria in at least one of the other search fields.
2. Click the **Search** button to execute the search or click **Clear** to clear the search criteria.
3. The system returns the search results. For more information see [Commons User Account Search Results](#).

**NOTE:** Use the **User ID** field to search by IMPACII user ID.
**Search Options**

**Search by Role**

To search by role, select a role from the Roles drop-down menu (to select multiple roles, hold the `<Ctrl>` key as you click the roles).

**NOTE:** When you search by roles, you can only search within your organization. You can select multiple roles, but the default search is for all roles appropriate to the logged in user's account role.

**Search by Status**

You can search by status to locate accounts that have been deactivated (by an administrator or due to inactivity). To do so, select the appropriate status from the **Account Status** drop-down menu:

```
Account Status

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
</tr>
<tr>
<td>Active</td>
</tr>
<tr>
<td>Deactivated</td>
</tr>
<tr>
<td>Locked due to Inactivity</td>
</tr>
<tr>
<td>Pending Affiliation</td>
</tr>
<tr>
<td>Profile Only</td>
</tr>
</tbody>
</table>
```

Make your selection and click **Search** to proceed.

**About Locked Accounts**

The status *Deactivated* indicates that the account has been disabled by an administrator, while the status *Locked due to inactivity* is applied to accounts that have had no activity for 120 days.

For information on reactivating a deactivated account, see [Reactivate or Unlock Account](#).

**Commons User Account Search Results**

When you click the **Search** button, the system displays the **Search Results**
NOTE: The Create New Account button does not display until a search is performed.

The following columns appear in the search results:

- **User ID**
- **Name** - last name, first name
- **Email**
- **Account Status** -
  - *Active* - The Manage button displays in the Action column.
  - *Pending* - The Resend Email button displays in the Action column.
  - *Pending Affiliation* - The Manage button displays in the Action column.
  - *Profile Only* - The Create button displays in the Action column.
• Roles & Affiliations
• Login via Login.gov
• Action - The Action buttons are Manage, Resend Email, and Create.

Perform one or more of the following steps:

1. To view the Search Criteria, click anywhere in the Search Criteria bar.
2. To filter the search results, enter the appropriate value in the Filter Results: text box and hit the <Enter> key.
   a. For example, to view all users with the Internet Assisted Review (IAR) role, type IAR in the Filter Results: text box.

**NOTE:** The default number of records per page is 10.

3. To change the number of records per page, select the appropriate number in the Show per page column.
4. To navigate between pages, perform one of the following options:
   a. Click the appropriate Page Number button.
   b. Click the right double arrows button to go to the end of the list.
   c. Click the left double arrows button to go to the beginning of the list.
5. To sort the search results, click the appropriate column heading name’s down arrow (ascending sort) or the up arrow (descending sort). The default sort is by Name (Last Name, First Name).
6. To view the NIH Support View screen, select the appropriate name hyperlink in the Name column.
   a. For more information, please see the NIH Support View topic.
7. If displayed, click the Read More hyperlink in the Roles and Affiliations column to view a Principal Investigator's (PI) multiple affiliations.
8. To perform one of the options in the Action column, please refer to the Actions Options topic.
9. To create a new account and profile click the Create New Account button at the bottom of the screen.
   a. Please refer to the Create Commons and iEdison User Accounts topic.
10. To return to the top of the screen, click the Back to top hyperlink.

**Search for System Accounts**

Use the , to search for existing user and system account(s).
NOTE: Agency, Commons, and external iEdison users can search for and create system accounts.

Search Accounts Screen Displaying Searching for System Accounts

NOTE: You must enter at least one search field, besides the User Type and Account Status. Wild card characters such as the percent sign (%) can be used to search for a string of characters.

Perform the following steps:

1. To search for a system account, select System from the User Type field's drop-down menu.

2. Enter the appropriate search criteria in at least one of the other search fields besides User Type.

3. Use the User ID field to search by IMPACII user ID

4. If you wish, select a Role from the drop-down menu. (To select multiple roles, hold the <Crtl> key and highlight the desired roles.)

NOTE: When you search by system roles, you can only search within your organization. You can select multiple roles, but the default search is for all roles appropriate to the logged in user's account role.
5. Click Search to execute the search or click Clear to clear the fields and start over.

**System Account Search Results**

When the Search button is clicked, the system displays appropriate system accounts in the Search Results located below the Search Criteria section on the Search Accounts screen. The search results are sorted alphabetically first by last name, first name in the Name field and then by Account Status.

**NOTE:** The Create New Account button does not display until a search is performed.

The following columns appear in the search results:

- **User ID**
- **Name** - last name, first name
- **Organization**
- **Roles & Affiliations**
- **Certification Owner** - The Certificate Owner is the organization who acquired the certificate.
- **Action** - Option button is Manage.
Account Management System (AMS)

Search Accounts Screen Displaying System Accounts Search Results

Perform one or more of the following steps:

1. To view the **Search Criteria**, click anywhere in the **Search Criteria** bar.
2. To filter the search results, enter the appropriate value in the **Filter**: text box and hit the `<Enter>` key.
   a. For example, to view all users with the last name of Salem, type *Salem* in the **Filter**: text box.

**NOTE:** The default number of records per page is 10.

5. To change the number of records per page, select the appropriate number in the **Show per page** column.
6. To navigate between pages, perform one of the following options:
a. Click the appropriate Page Number button.
b. Click the right double arrows button to go to the end of the list.
c. Click the left double arrows button to go to the beginning of the list.

7. If displayed, click the Read More hyperlink in the Roles and Affiliations column to view a system user's multiple affiliations.

8. To manage a system account, click the Manage button in the Action column.
   a. Please refer to the Manage System Accounts topic for more information.

9. To create a new account and profile click the Create New Account button at the bottom of the screen.
   a. Please refer to the Create System Account topic for more information.

10. To return to the top of the screen, click the Back to top hyperlink.

**Funding Support Screen**

The Funding Support screen lists the NIH application information associated with the selected Principal Investigator (PI). Use this information to positively identify PIs associated with your institution.

**NOTE:** The Funding Support screen is for Commons and external iEdison users only.
### Funding Support Screen

The NIH Support page lists the NIH application information associated with the selected Principal Investigator (PI). Use this information to positively identify PIs associated with your institution.

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution Name</th>
<th>Support Type</th>
<th>Support Identification</th>
<th>Support Description</th>
<th>Support Start Date</th>
<th>Support Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dusty Rusty Rhoades</td>
<td>UNIVERSITY OF CALIFORNIA LOS ANGELES</td>
<td>Trainee</td>
<td>5T32CA899969-37</td>
<td>UCLA Tumor Immunology Training Program</td>
<td>2013-04-01</td>
<td>Awarded</td>
</tr>
<tr>
<td>Dusty Rusty Rhoades</td>
<td>UNIVERSITY OF CALIFORNIA LOS ANGELES</td>
<td>Trainee</td>
<td>5T32CA899969-38</td>
<td>UCLA Tumor Immunology Training Program</td>
<td>2014-04-01</td>
<td>Awarded</td>
</tr>
<tr>
<td>Dusty Rusty Rhoades</td>
<td>UNIVERSITY OF CALIFORNIA LOS ANGELES</td>
<td>Trainee</td>
<td>2T32CA999999-36A1</td>
<td>UCLA Tumor Immunology Training Program</td>
<td>2012-04-23</td>
<td>Awarded</td>
</tr>
<tr>
<td>Dusty Rusty Rhoades</td>
<td>UNIVERSITY OF NOTRE DAME</td>
<td>Traineer</td>
<td>5T32GA899999-03</td>
<td>Chemistry-Bohemia-Biology Interface Training Program At Notre Dame</td>
<td>2009-07-01</td>
<td>Awarded</td>
</tr>
<tr>
<td>Dusty Rusty Rhoades</td>
<td>UNIVERSITY OF NOTRE DAME</td>
<td>Traineer</td>
<td>5T32GA899999-02</td>
<td>Chemistry-Bohemia-Biology Interface Training Program At Notre Dame</td>
<td>2008-07-01</td>
<td>Awarded</td>
</tr>
</tbody>
</table>
Create Accounts

You can create the following types of accounts:

Create User Accounts
Create System Accounts

Create a Commons account for an individual (e.g., PD/PI)

If you are a Commons user with an SO, AA or BO role, you have the ability to create new Commons user accounts (such as for a PD/PI).

**IMPORTANT:** PD/PIs cannot create their own accounts: Only an SO or AA Commons user can create this account.

1. To create a new user account, first search AMS to make sure the user doesn't already have an account. For instructions, see Search Account for Commons Accounts.
2. You launch the create-account process from the Search Results screen.
   - In the search results, profiles that are not already associated to a user account display a Create button in the Action column:
     - Click the Create button to create a user account for that profile.
   - Or click the Create New Account button located below the search results:
     - [Create New Account]
3. When you click one of the Create buttons, the Create Account screen opens, as shown below.
Create Account Screen for an External Account

Perform the following steps to create an account:

4. Set **User Type** to Commons.
5. Enter the **User ID** or let the system generate one.
   a. The **User ID** length should be between 6 and 30 characters and should **NOT** contain special characters except the @ sign, the hyphen, the period, and the underscore.
   b. The system can display the following messages: *This User ID is available OR This User ID is already taken, please use another one.*
6. Usually the **Primary Organization** defaults to the logged in user's organization.
   a. If there is no user organization name selected, click the magnifying glass icon to assign a **Primary Organization**. (See [Set Primary Organization](#) for more information.)
7. Perform one of the following options:
   a. When the account information is complete, click **Create** to create the account or click **Clear** to clear all information from the form.

When you click **Create**, the system displays the *Account Details* screen with a success message, as shown here.

![Account Details Screen with success Message](image)

6. Perform one of the following options on the *Account Details* screen:
   a. To return to the *Search Accounts* screen displaying the previous search results, click the **Go Back** hyperlink.
Account Management System (AMS)

b. To edit the account's information, click the Manage button.
   i. For more information, please refer to the Manage Account for Commons Users topic.
c. To return to the Search Accounts screen to enter new search criteria, click the Back to Search button.

Account Invitations from eRA Systems

Create-Account requests for eRA accounts that are validated by invitations from eRA modules can be approved or rejected automatically:

- If the identifying information the new user submits unambiguously matches the profile created by the account requester and the profile is not already associated to another user account, the request is approved automatically.
- If the identifying information is incorrect or an account already exists for the user profile, or if a comment has been entered in the user's funding and committee service history, request is denied and the system sends notifications to the account requester and to the eRA Service Desk.

Examples of system-generated account invitations:

- **SO creates a new PI account in AMS**
  The new PI receives a system-generated invitation to log in to eRA Commons and validate the account.

- **SRO enables a new reviewer in Internet Assisted Review (IAR)**
  The reviewer receives a system-generated invitation to log in to eRA Commons and create an account to access IAR. See the IAR Online Help for information on enabling reviewers

- **PD/PI appoints a new trainee in xTrain**
  The trainee receives a system-generated invitation to log in to eRA Commons and create an account to access xTrain. See xTrain Online Help for information on appointing
trainees.

**Workflow**

The account invitation procedure includes these steps:

1. The account requester creates the new account.
2. The new user receives an email notification that includes the username and other details about the new account.
3. The user receives a second email that includes a temporary password for the new account and instructions for logging into the system. This email explains that the user must login to the system that day or the account will be locked. After an account is locked, any attempt to log in will be redirected to the password reset/lost password workflow. See Initial Login to eRA Account.
4. The user logs in with the provided credentials and is immediately instructed to create a new password for the account.

**NOTE:** If the user enters incorrect login information too many times, the account is locked and the user must contact the eRA Service Desk to complete the login process.

**Add/Delete User Roles**

**NOTES:**

- The list of roles displayed is dependent on the logged in user’s role.
- Accounts with scientific roles should be maintained for the career of the scientist and affiliations should be added as necessary.
• Administrative roles cannot be combined with scientific roles on the same user account and accounts with administrative roles cannot be affiliated with more than one institution.

1. To add user roles to an account, click on the + Add Roles button at the bottom of the Create Accounts or Manage Accounts screen, as shown here.

When you click + Add Roles, the Add Roles screen opens, as shown below.

**NOTE:** If you click + Add Roles to other org, the window shown here will open first, so you can search for and select the other organization.

Select the organization and click Next to proceed to the Add Roles screen as described below.
Add Roles screen

1. Scroll through the list and click to select the appropriate role(s).
   **Note:** For reference, here is a [complete list of Commons user roles](#).
2. Click the **Add Role(s)** button.

When you click **Add Roles(s)**, the system returns to the Create Account or Manage Account screen and displays the newly added role(s).

Roles Section on the Create Accounts Screen
3. To add additional roles, click the + Add Roles(s) button and repeat the steps above.
4. To remove a role, click the appropriate Remove button in the Action column.
5. To remove all roles, click the Remove All button.

**NOTE:** You cannot remove Signing Official (SO) role when the Research Performance Progress Report (RPPR) is assigned.

**NOTE:** You cannot add user a role if the account is in deactivated status: You must reactivate the account first.

### Set Primary Organization

**NOTE:** The magnifying glass for the Primary Organization field on the Create Account screen appears if the logged in user is not affiliated with an Organization, IC, or Agency. Usually the Primary Organization defaults to the logged in user's Organization.

<table>
<thead>
<tr>
<th>Primary Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Primary Organization Field

1. To add a primary organization click the magnifying glass icon on the Create Account screen.

When the magnifying glass icon is clicked, the Search Organization and Add Roles screen opens.
Search Organization and Add Roles Screen

2. Enter an **Org ID** or an **Organization Name**.

**NOTE:** Wild card characters such as the percent sign (%) can be used to search for a string of characters.

3. Click the first **Search** button.

When the first **Search** button is clicked, the organization is displayed, if present.

4. To filter the search results, enter the appropriate value in the **Filter:** text box and hit the **<Enter>** key. For example, enter *San Diego* to view only those universities in California.

5. To change the number of records per page, select the appropriate number in the **Show per page** column.
6. To navigate between pages, perform one of the following options:
   a. Click the appropriate Page Number button.
   b. Click the right double arrows button to go to the end of the list.
   c. Click the left double arrows button to go to the beginning of the list.
7. Select the appropriate organization's radio button.
8. Click the second Select button or click the Close button to close the screen.

When the second Select button is clicked, the Create Account screen displays the selected primary organization. For more information see Create External User Accounts.

Create System Accounts

System accounts are used to access eRA Web Services.

Agency, Commons, and external iEdison users can create system accounts.

1. To create a system account, first perform a search to make sure the account you want to create does not already exist.
   a. For instructions see Search System Accounts.

   NOTE: The Create New Account button described below is not available until a search is performed.

2. Review the search results to see if the account you want already exists, and if not, click the Create New Account button that appears below the search results, shown here:

   ![Create New Account Button](image)

   When you click Create New Account, the...

3. Select System in the User Type drop-down menu.
When you select user type *System*, the screen displays the fields you need to complete for a system account.

Create Account Screen Displaying Creating a System Account

4. Type in the owner in the **Certificate Owner** field. The **Certificate Owner** is the organization who acquired the certificate.

5. Select the appropriate **Certificate Provider/Authority** from the drop-down menu.
Account Management System (AMS)

NOTE: Examples of the values that are available for the Certificate Provider/Authority include: Comodo, Digicert, Entrust, Geo Trust, Go Daddy, InCommon, and Thawte.

6. Enter the **Certificate Serial Number** in the format XX:XX:XX:XX:XX:XX:XX:XX.

For information on obtaining and registering a certificate from a Certificate Provider or Authority, refer to one of the [Web Services Certificate (S2S) Guide](#):

- Section 2.4.3 for Commons users - only users with the SO role have the privileges necessary to register the certificate in AMS; Commons users must work with their SO to register their certificate

7. Complete the **Contact Information**.

8. Click the **Add Roles** button to add the roles to the account.
   a. Note the role description on the screen when adding a role.
   b. See [Add System Roles](#) for more information.

9. Select the **Agreement** check box below the **Roles** section.

The **Agreement** check box is mandatory for the user to acknowledge information provided for the system account. If the **Agreement** check box is not checked and the **Save** button is clicked, the system displays the following error message: *User must accept the agreement by checking the field.*

10. Click the **Create** button to create the account or click **Clear** to clear all fields.

When you click **Create**, the system validates the account information. If there are no errors, then the **Account Details** screen opens, displaying a success message.
Account Details screen displaying success message

**Other Actions:**

- Click the **Validate Certificate** button to validate the certificate. See [Validate Certificate](#) for more information.
- Click the **Manage** button if you want to make additional changes. See [Manage System Accounts](#) for more information.
- Click the **Back to Search** button to return to the **Search Account** screen.

**Add System Roles**

**NOTE:** The list of roles is dependent on the logged-in user's role.
1. To add system roles to the account, click on the **Add Roles** button on the *Create Accounts* screen.

![](roles.png)

Add Roles Button on the Create Account Screen

- When the **Add Roles** button is clicked, the pop-up *Add Roles* screen displays.

**External System Roles**

![](external_roles.png)

Add Roles Screen for External System Roles

- Highlight the appropriate role(s).
- Click the **Add Role(s)** button.
When the **Add Roles(s)** button is clicked, the system returns to the *Create Account* or *Manage Account* screen and displays the newly added role(s).

![Roles section](image)

Roles Section on the Create Accounts Screen for Agency Users

3. To add additional roles, click the **+ Add Roles(s)** button. Repeat the steps above.
4. To remove a role click the appropriate **Remove** button in the **Action** column.
5. To remove all roles click the **Remove All** button.

**Validate Certificate**

When the **Validate Certificate** button is clicked on either the *Manage Account* or *Account Details* confirmation screen, the system displays the *AMS | Validate Certificate* screen with hyperlinks to instructions for the different browsers (i.e. Internet Explorer, Firefox, and Safari, etc.) for uploading a certificate file.

1. Perform one of the following options:
   a. To validate the certificate, click the **Validate** button on the **Validate Certificate** screen.
   b. Click the **Cancel** button to cancel the certificate validation.
Validate Certificate Screen

When the **Validate** button is clicked, the system performs the certificate validation.

If the browser call does go through to the certificate provider, but the details of the uploaded certificate do not match the details entered in AMS, then the following warning message opens:
Warning! - This certificate works with eRA systems correctly, but the certificate details you entered in the account do not match information in the certificate you are trying to validate. Certificate information in the account must match certificate you are trying to validate.

If there are no validation errors, a second Validate Certificate screen displays the following success message: Success! Your certification works with the eRA systems as expected.

Validate Certificate Screen Displaying the Success Message

2. Click the Close button to close the screen.
The following audit information is audited and stored in the database:

- **Certificate Number** – Certificate Number of the uploaded certificate during validation
- **Certificate Provider** – Common Name of the uploaded certificate during validation
- **Certificate Owner** – The Certificate Owner that was entered during validation. The Certificate Owner is the organization who acquired the certificate.
- **Time of Validation** – Format: DD/MM/YYYY HH:MM:SS
- **Result of Validation Attempt**
  - Success
  - Validation is successful but the certificate details does not match the user entered details
Manage Accounts

User Accounts

Once an account is created it can be maintained via the Manage Accounts screen.

- Manage User Accounts

System Accounts

Agency, Commons, and iEdison external users can modify system accounts.

- Manage System Accounts

For information on obtaining and registering a certificate from a Certificate Provider or Authority, please refer to the Web Services Certificate (S2S) Guide:

- Section 2.4.3 for Commons users

Managing External User Accounts

The following roles can manage accounts:

- Account Administrator (AA)
- Administrative Official (AO)
- Business Official (BO)
- Signing Official (SO)
- TTO Administrator

1. Perform one of the following steps to manage a user account:
   a. Click the Manage button for an account on the Search Accounts screen.
   b. Click the Manage button on the Account Details screen after an account have been created or saved (edited).

When either Manage button is clicked, the Manage Account screen opens, as shown here.
Manage Account

Note: Changes to the account are not saved until you hit the save button.
- For example, if you affiliate someone, he/she is not actually affiliated until you hit the save button.

All fields are required unless they're marked (Optional)

User Information
Account Status: Active
User Type: Commons
User ID: SJR
Primary Organization: FASGEN, INC.
Login via 2FA: OPTIONAL
2FA Exemption Expiration Date:
2FA Mapping Completion Status: NOT MAPPED

Contact Information
Last Name: Ons
First Name: Art
Middle Name: H.
Email: eRATest@email.nih.gov
Confirm Email: eRATest@email.nih.gov

Roles
+ Add Roles  + Add Roles to other org.  ✗ Unaffiliate

<table>
<thead>
<tr>
<th>Role(s)</th>
<th>Organization(s)</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSR</td>
<td>FASGEN, INC.</td>
<td>Remove</td>
</tr>
<tr>
<td>SO</td>
<td>FASGEN, INC.</td>
<td></td>
</tr>
</tbody>
</table>

Save  Close  Reset Password  Deactivate

Showing 1 - 2 of total 2
**Actions**

You can perform these actions:

- Edit the **Email** addresses if necessary.
- Add Roles. To add or delete roles click the **+ Add Roles** button. For more information, see *Add/Delete Roles*.
- To affiliate an account with an organization, click the **Affiliate** button, if displayed. (An affiliation can be created for accounts that are either not currently associated with an institution, such as an account solely with the Internet Assisted Reviewer (IAR) authority role, or for accounts that need to be associated with multiple institutions. Users with the AA or SO role may create an affiliation for their organization only. For more information, see *Affiliate Account*.
- If the **Unaffiliate** button is present, you can click it to unaffiliate an account. For more information, see *Unaffiliate Account*.
- If the account has been deactivated, a **Reactivate** button will be present at the bottom of the screen. Click it to reactivate the account. For more information, see *Reactivate Account*.
- Two-Factor Authentication:
Account Management System (AMS)

- **Login via Login.gov** — Shows the status of login.gov for this account: "Required," "Optional" or "Exemption."
  
  **Note:** This field is set automatically at the organization level.

- **Login.gov Exemption Expiration Date** — When Login via Login.gov is set to "Exemption," this field displays the end date for the exemption. The user can log in using eRA credentials until this date.
  
  **Note:** Login.gov exemptions are only granted on a limited basis by the eRA Service Desk and only the eRA Service Desk can modify this date.

**Account Statuses**

AMS user accounts can have the following statuses:

- Active — A valid account in good standing.
- Deactivated — Account has been disabled by an administrator
- Locked due to inactivity — Locked by the system due to inactivity (no user activity for 120 days)
- Pending Affiliation — An individual account that has not been linked to an organization
- Profile Only — A user ID that is not associated to an account

**NOTES:**

- Administrative and reporting roles such as SO, AA, AO, FSR, etc., cannot be combined with Scientific roles such as PI, TRAINEE, ASST, etc.
- Only accounts with scientific roles such as IAR, PI, TRAINEE, POSTDOC, etc., may have multiple affiliations. If an account has any roles in addition to these, additional affiliations cannot be added.
- Fields grayed out cannot be edited.

**Add/Delete User Roles**

**NOTES:**

- The list of roles displayed is dependent on the logged in user's role.
- Accounts with scientific roles should be maintained for the career of the scientist and affiliations should be added as necessary.
Account Management System (AMS)

- Administrative roles cannot be combined with scientific roles on the same user account and accounts with administrative roles cannot be affiliated with more than one institution.

1. To add user roles to an account, click on the + Add Roles button at the bottom of the Create Accounts or Manage Accounts screen, as shown here.

When you click + Add Roles, the Add Roles screen opens, as shown below.

NOTE: If you click + Add Roles to other org, the window shown here will open first, so you can search for and select the other organization.

Select the organization and click Next to proceed to the Add Roles screen as described below.
Add Roles screen

1. Scroll through the list and click to select the appropriate role(s).
   Note: For reference, here is a complete list of Commons user roles.
2. Click the Add Role(s) button.

When you click Add Roles(s), the system returns to the Create Account or Manage Account screen and displays the newly added role(s).

Roles Section on the Create Accounts Screen
3. To add additional roles, click the + Add Roles(s) button and repeat the steps above.
4. To remove a role, click the appropriate Remove button in the Action column.
5. To remove all roles, click the Remove All button.

**NOTE:** You cannot remove Signing Official (SO) role when the Research Performance Progress Report (RPPR) is assigned.

**NOTE:** You cannot add user a role if the account is in deactivated status: You must reactivate the account first.

**Affiliate Account**

1. To affiliate an existing account with an organization, search for the user account in AMS and select the Manage action for the account
2. Click the Affiliate button under Roles on the Manage Account screen, as shown here:

![Affiliate button on Manage Account screen](image)

When the Affiliate button is clicked, the Add Roles screen opens, as shown here:
NOTE: The list of roles is dependent on the logged in user's role.

Add Roles screen

1. Highlight the appropriate role(s).
2. Click the Add Role(s) button.

When the Add Role(s) button is clicked, the role is added, the account is placed in 'Active' status, and the Unaffiliate button appears in the Roles section, as shown here:

Roles section on the Manage Account screen

Unaffiliate Account

1. To unaffiliate an account, click the Unaffiliate button in the Roles section of the Manage Account screen.
When the **Unaffiliate** button is clicked, an *Account Unaffiliation* pop-up screen displays.

![Account Unaffiliation Screen](image)

**Account Unaffiliation Screen**

2. Click the **Yes** button to unaffiliate the account, or click **No** to cancel the unaffiliation.

When the **Yes** button is clicked, all roles assigned to the account are removed, the account is placed in ‘Pending Affiliation’ status, and the **Affiliate** button appears in the *Roles* section of the *Manage Account* screen, as shown here:

![Roles Section](image)

**IC Transfer Process**

1. The Account Coordinator will un-affiliate the account by removing all roles for their IC.
2. The account will go into ‘Pending Affiliation’ Status, in which there are no roles associated with the account, and the user cannot perform any functions.
3. An Account Coordinator from the new IC will search for accounts in ‘Pending Affiliation’ status and select an account to affiliate.

For information on Affiliating an account, see [Affiliate Account](#).

**Affiliate Button in Roles Section on Manage Account Screen**
Reactivate Account

Follow these steps to reactivate an account that has been deactivated by an administrator.

**NOTE:** Commons users are required to reset their passwords after a defined time period. The system locks the account if the user fails to rest the password. Use the **Reset Password** function to unlock these accounts.

1. Open the account in the *Manage Account* screen.

2. If an account is deactivated, a **Reactivate** button will be present at the bottom of the *Manage Account* screen, as shown here. Click this button to proceed.

3. When you click **Reactivate**, the *Reactivate Account* screen opens, as shown here.

Reactivate Account screen
4. In this screen, take these steps:
   a. **Mandatory**: Enter comments in the comments field to inform the user about this action.
   b. Click **Reactivate** to reactivate the account, or click **Close** to cancel.

5. When you click **Reactivate**, the system reactivates the account and displays a confirmation message. And the account owner receives an email notification that includes the text you entered in the **Comments** field.

**NOTE**: The unlock notification asks the user to login to the account that same day. If the user does not login before the end of the day, the account is locked again.

**Change Password**

1. Perform one of the following options:
   a. For external iEdison users, click the **Change Your Password** hyperlink on the **Main Menu** screen.
   b. For Commons users, click the **Change Password** tab.

**Modify Your iEdison Account Information**

- **Change Your Password**
- **Change Your User Preferences**

iEdison Main Menu Screen Displaying Change Your Password Hyperlink

Commons Menu Tabs Displaying the Change Password Tab
For iEdison users, when the **Change Your Password** hyperlink is clicked, a pop-up screen displays.

![Message from webpage]

Accessing AMS Pop-up Screen

When the **OK** button is clicked on the pop-up screen or the **Change Password** tab is clicked, the **Change Password** screen displays in a separate browser window.

![Change Password Screen]

Change Password Screen

2. Enter your **Current Password**.
3. Enter a **New Password**.
4. Type your new password a second time in the **Confirm New Password** field.
5. Perform one of the following options:
   a. Click the **Save** button to save the changes.
   b. Click the **Clear** button to clear the fields.

Use your new password the next time that you log into Commons or iEdison.

**NOTE:** The password guidelines are:

- Password length must be between 15-64 characters
- First and last characters cannot be numbers
- Cannot contain username
- Cannot re-use previous 10 generations of passwords

**Reset Password**

**NOTE:** Users are required to reset their passwords after a defined time period. The system locks the account is if the user fails to reset the password. Use this procedure to unlock these accounts.

1. To reset a user's account password, open account in the the **Manage Accounts** screen and click the **Reset Password** button located on the lower right side of the screen.
2. A pop-up confirmation screen opens. Click **Close** to close it.

![ AMS | Reset Password ]

Password for this account has been reset successfully! An email with temporary password was sent to the account holder.

3. When you complete the password reset, an email notification with a temporary password is sent to the account holder.

**Manage System Accounts**

System accounts are used to access eRA **Web Services**.
Agency, Commons and external iEdison users can manage system accounts in their organizations.

For information on obtaining and registering a certificate from a Certificate Provider or Authority, please refer to the Web Services Certificate (S2S) Guide:

- Section 2.4.3 for Commons users

Perform the following steps:

1. To manage a system account, first perform a search to locate the account.
   a. See Search for System Accounts for more information.

2. On the Search Results screen, click the Manage button for the system account you want to manage.

When the Manage button is clicked, the Manage Account screen opens, as shown below.
Manage Account Screen for external accounts

**NOTE:** Fields that are grayed out cannot be edited.

3. Edit the non-gray fields as needed.

4. Click the Add Roles button to add the roles to the account. See Add System Roles for more information.

5. To remove a role, click the Remove button. To remove all roles, click the Remove All button.

6. Click Deactivate to deactivate an account. See Deactivate Account for more
7. Click **Save** to save the changes or click **Cancel** to cancel.

When you click **Save**, the *Account Details* screen opens and displays a success message, as shown below

![Account Details Screen](image)

Account Details Screen for external users

Account Details Screen for Agency Management Staff

8. You can perform these additional actions in the *Account Details* screen:
   - If the certificate needs to be validated, click the **Validate Certificate** button. See [Validate Certificate](#) for more information.
   - To return to the *Manage Accounts* screen, click the **Manage** button or the **Go Back** hyperlink.
   - To return to the *Search Accounts* screen to enter new search criteria, click the **Back to Search** button.

### Add System Roles
NOTE: The list of roles is dependent on the logged-in user's role.

1. To add system roles to the account, click on the + Add Roles button on the Create Accounts screen.

Add Roles Button on the Create Account Screen

When the + Add Roles button is clicked, the pop-up Add Roles screen displays.

External System Roles

Add Roles Screen for External System Roles

1. Highlight the appropriate role(s).
2. Click the Add Role(s) button.
When the **Add Roles(s)** button is clicked, the system returns to the *Create Account* or *Manage Account* screen and displays the newly added role(s).

Roles Section on the Create Accounts Screen for Agency Users

3. To add additional roles, click the **+ Add Roles(s)** button. Repeat the steps above.

4. To remove a role click the appropriate **Remove** button in the **Action** column.

5. To remove all roles click the **Remove All** button.
**User Reports**

AMS includes the following reports capabilities:

- **All Users Report** — Information on all user accounts in your organization
- **Inactive Users Report** — lists user accounts that have been locked due to inactivity (note: for internal users only)
- **Deactivated Users Report** — lists user accounts that have been deactivated by an administrator (note: for internal users only)
- **Role Description Report** — lists all roles, role descriptions, and associated privileges for any business area (note: for internal users only)

To open the reporting functions, click the **AMS User Reports** tab.

The *All Users Report* screen opens. There are two versions of this screen, as shown below. The version you see depends on the organization you belong to.

### All Users Report Screen for External Users

*All Users Report* screen for Commons, external iEdison, and State Department users

All Users Report Screen for External Users

Use this screen to run an All Users Report on external users.

The **All Users Report** button is selected by default, as shown below. Follow the steps below to launch the report.

![All Users Report Button](image)
1. Select "Commons" in the **User Type** field and set the search criteria in the other fields as follows:

2. **Organization** — This field displays your organization name. Service Desk agents, to select an organization, begin typing its name or ID number in this field. The live search function displays organization names as you type. When the one you want appears, scroll down and click to select it, as shown below.  
   *(note: To select multiple organizations, hold the <Ctrl> key as you click.)*  
   **Note:** This field is mandatory.

![Organization field, external](image)

3. **Roles** — Leave this field blank to report all user roles. To limit the report to one or more user roles, click this field to open the drop-down menu or begin typing the name of a role. The live search function displays roles as you type. When the one you want appears, scroll down and click to select it, as shown below. *(Note: To select multiple roles, hold the <Ctrl> key as you click.)*

![Roles](image)

4. **Account Creation Start Date/End Date** — Leave these fields blank to report all time periods. To limit the report to a certain time period, enter a start date, end date, or start and end dates. Enter dates in MM/DD/YYYY format or click the calendar icon to select them from the calendar.

5. When you finish entering search criteria, click **Search** to run the report. See **Report Output** below.
Role Description Report

Report Output

All Users Report output
To run the All Users report, click the **All Users report** button and enter search criteria as described above. When you click the **Search** button for the All Users report, the report output displays.

![All Users Report output](image)

Navigating the report output
These tips for browsing, filtering and exporting the report output apply to all report types.

The report output displays include the controls shown here.
To filter the report, type some text in the **Filter** field, such as a name. Only rows that contain the filter term will be displayed, and all instances of the filter text will be highlighted in yellow, as shown below:

![Filter Example](image)

To adjust the number of records displayed, select a number in the **Show per page** drop-down menu.

To navigate the report pages, click a **Page Number** or use the left and right arrow buttons.

To re-sort the report columns in ascending or descending order, click the up/down arrows in the column headers.

To export the report output as an Excel spreadsheet or PDF, click the appropriate **Export** button, shown here:

![Export Buttons](image)

- **Export to Excel**

  When you click this button, an open-or-save dialog opens, as shown here.
Click **Open** to open the report data in Excel. A new Excel window opens. Go to it and click the **Enable Editing** button in the yellow bar at the top of the worksheet, then work with the spreadsheet as usual.

- **Export to PDF**

Click this button to save the report as a PDF file. A save dialog opens. Choose a location and save the file.