CPAIS QuickGuide: UMA for UMA Managers

Access the User Management Application

If you do not have any roles or organizations associated with your account, you will be redirected to the User Management Application. If you would like to modify your account or view your account details, you can access UMA from the Main Menu. For more information, see Creating and Modifying Accounts.

To access the User Management Application:

1. Log on to CPAIS.
2. From the Main Menu, click **System Management**.
3. From the list of forms, click **User Management Application**.

Approve Account Requests

You need the UMA Manager role to complete these instructions.

Through UMA, users submit requests for new profiles or changes to their existing profiles. UMA Managers are responsible for reviewing and acting on requests and for renewing accounts that are about to expire or have expired. This topic describes how UMA managers review, edit, and approve/reject account requests.

UMA managers can only approve requests for the roles and organizations authorized by their program areas. If you are an UMA Manager and cannot approve requests for roles and organizations, contact your program area's national program manager.

To approve an account request:

1. Access the User Management Application (UMA). The Personal Information page displays information about your profile.
2. Click the **Manage Users** tab.
3. To search for user profiles, enter search criteria into the three fields in the Users block. You must enter search criteria in all three fields. For more information, see Search for User Profiles.
4. Click **Search**.
5. From the list of search results, select the user profile that you want to work with. The page displays role/organization information in the Roles and Orgs for (user name) block.
6. For both new and existing profile requests, review the requested roles in the Roles and Orgs for (user name) block.
7. To approve a requested role, select it and click **Approve Role**. Repeat with other roles, as necessary. Asterisks (*) display beside each organization for that role to let you know your approval is pending. Re-query the user's profile in a few minutes and the organizations will move to the Assigned Orgs column.
8. To modify a request before approving it, click the **Modify User Requests** tab. For more information, see Modify User Requests.
9. To set expiration dates. see Set Role Expiration Dates.
10. Click **Save**. The user will receive an email notification explaining the action you took.

Reject an Account Request

You need the UMA Manager role to complete these instructions.

As an UMA Manager, you should review all account requests and verify that the user needs all of the roles and organizations he or she has requested. Follow these instructions if you would like to reject a user's request. If a user's request is mostly correct, but he or she has requested an extra role or org, see Modify User Requests and Accounts.

To reject an account request:

1. Access the User Management Application (UMA).
   When the UMA form displays it will default to the Personal Info page, which contains information about your CPAIS profile.
2. Click the **Manage Users** tab.
3. To search for user profiles, type search criteria into the three fields in the Users block. You must enter search criteria in all three fields. See Tips for Searching for Users for more information.
4. Click **Search**.
   All matching user profiles will display in the table immediately below.
5. Select the desired user profile by clicking the corresponding radio button.
   The page will refresh and display role/organization information in the Roles and Orgs for (user name) block below.
6. For both new and existing profile requests, review the requested roles in the Roles and Orgs for (user name) block to ensure the user does indeed need these data editing privileges.
7. To reject a requested role, select it and click **Reject Role**. Repeat with other roles, as necessary.
   The roles will disappear from the Request Add Orgs column. You cannot use the Reject Role button for roles that are already approved/granted as part of the user's profile. Use this button only for new requests.
8. Click **Save**.
   The user will receive an automated email announcing the new status of his or her profile.

Search for User Profiles

You can search for specific user profiles on the Manage Users and Designate Managers pages.

Populate all fields

You must enter search criteria in all three fields (the two drop down lists and one text field). For example, to search for all users whose profiles are about to expire, you cannot select Users Expiring Soon from the Filter Type field's drop down list and then click Search. You must also enter criteria in the Search By field's drop down list (e.g., Username) and accompanying text field (e.g., %).

Searching for exact or partial matches

When selecting criteria from the Search By drop down list, you must type full or partial text into the accompanying text field. Full text must match exactly the information the user provided originally in order to return results.

Use the percent symbol wild card to find partial matches. For example, searching by phone number with %303% in the accompanying text field will return all users whose phone number

contains the numbers 303. Similarly, searching for a first/last name with th% in the accompanying text field will return names that begin with "th" (thomas, theresa, thad, thompson, etc)

Filter Type field

The table below lists and defines all values found in the Filter Type field's drop down list.

Note: These filters are not available on the HelpDesk page.

Filter	Definition
All Users	Broadens your search to all users, whether or not you have the ability to act on their requests
My Users	Limits your search to those users who you can manage in UMA This filter returns only those users with a role and organization combination that you have authorization to manage. In addition, the users returned by the My Users filter must have the role and organization granted to their profile; the filter does not return users with new requests.
Users with Requests	Limits your search to only users who have pending requests (the search results may include users with a status of GRANTED and NEW REQUEST) **Note:** This option is not available when searching for users on the Designate Managers page.
Users Expiring Soon	Limits your search to users who have one or more roles set to expire by the end of the current month When using this filter, Expiration Month End displays the expiration date, rather than "n/a".

Search By field

The table below defines all values found in the Search By list. This field is paired with the text field that displays to the right of the drop down list. You must type text that further specifies the value you choose from the drop down list. See above for tips for searching for exact or partial matches.

Filter	Definition
Username	Lets you search by user name
Last/First Name	Lets you search by first or last name In most cases, you need to use the wildcard character (%) in combination with your search parameters when using this search field
Email	Lets you search by email address **Note:** Enter a full email address (user@usda.gov).
Phone Number	Lets you search for a user by phone number The user you are searching for may not have entered their phone number using the standard format. Consider typing partial text and the percent symbol (%) wild card in the accompanying text field.
Home Org	Lets you search for a user by the home organization

	The user you are searching for may not have entered a home organization using a standard format. Consider typing partial text and the percent symbol (%) wild card in the accompanying text field (e.g., %Arapaho% or 01%).
Supervisor	Lets you search for users by their supervisor's name
Status	Lets you search for a user by one of the following statuses: • GRANTED • APPROVED • NEW REQUEST
All Fields (slow)	Lets you search for users by any field **Note:** This search method will take longer to return results.

Set Role Expiration Dates

You need the UMA Manager role to complete these instructions.

Roles expire one year after an account is approved. UMA managers can set the expiration date to a length of time less than one year. Expiration dates can be the same for all roles in a user's profile or each role can have a separate expiration date. You will be notified by email when a user's role is about to expire. It is your responsibility to evaluate if the user needs access and, if necessary, extend expiration dates.

Note: The Expiration Month End field normally displays "n/a". This field is only populated with the actual Expiration Month End when searching for Users Expiring Soon. You can also view expiration dates by searching for a user, selecting a specific role, and clicking View Details.

To set or extend expiration dates for all roles in a user's profile:

1. Search for and select the user's profile in the Users block. For more information, see Search for User Profiles.
2. To view expiration dates, select the role in the Roles and Orgs for (USER) block and click **View Details**.
3. Enter a new expiration date in the New User Expiration Month field (Users block). You can either type the date using the MM-YYYY format or select a date using the calendar.
4. Click **Set All Expiration Dates for User**.
5. In the confirmation window, click **OK** if you are sure you want to change the expiration date.
6. Click **Save**.

To set or extend expiration dates for a single role:

1. Search for and select the user's profile in the Users block. For more information, see Search for User Profiles.
2. Select an individual role in the Roles and Orgs block.
3. To view expiration dates, select the role in the Roles and Orgs for (USER) block and click **View Details**.
4. Enter a new expiration date in the New Role Expiration Month field (Roles and Orgs block). You can either type the date using the MM-YYYY format or select a date using the calendar.

5. Click **Set Role Expiration Date**.
6. In the confirmation window, click **OK** if you are sure you want to change the expiration date.
7. Click **Save**.

Modify User Requests and Accounts

You need the UMA Manager role to complete these instructions.

While reviewing user profile requests, you might find that the user failed to request certain roles or the correct number or organizations for a role. You do not need to postpone the review process and wait for the user to submit another request. As an UMA manager, you can modify the user's request and then approve those changes.

UMA managers can only approve requests for the roles and organizations authorized by their program areas. Contact your program area's national program manager if you find that you do not have sufficient privileges to approve requests.

To modify a user request/account:

1. Access the User Management Application.
2. Click **Manage Users**.
3. Search for and select the user's profile.
4. Click the **Modify User Requests** tab.
5. Select an application from the Application Name list.
6. Select the role from the Role Name list that you want to add or remove from the user's request.
7. Select the user's agency from the Agency list.
8. In the Available Orgs box, search for organizations using the Filter list.
9. Select the organizations you want to add or remove.
10. Use the **Move** or **Move All** links to pass those organizations to the Requested Orgs box.
11. Click **Add Selected Orgs** to add those organizations to the role or **Remove Selected Orgs** to remove those organizations from the role.
12. Repeat Steps 5 through 11 for other roles, if necessary.
13. Click **Save**.
14. Click the **Manage Requests**.
15. In the Roles and Orgs block, select the role for which you initiated a change.
16. Set the Expiration Date. For more information, see Set Role Expiration Dates.
17. Click **Approve Role**.
18. Repeat Steps 14 through 17 for any other roles for which you requested a change.
19. Click **Save**. The user will receive an email notification explaining the changes to his or her profile.

Promote a User to UMA Manager

You need the UMA Manager role to complete these instructions.

You can promote other users to UMA Manager. When you promote a user, you are not giving them the ability to edit or view data; you are only granting them the ability to approve requests from users requesting roles and organizations.

You can only grant UMA Manager privileges to other users for the roles and organizations you manage in UMA and that you are allowed to grant to others. To view the roles and orgs that you are allowed to grant to others, click the Review My Manager Role-Orgs tab then click View Details for each role. If the Grant column is Y, you can promote other users to UMA Manager; if it is N, you cannot promote other users.

To promote a user to UMA Manager:

1. Access the User Management Application (UMA).
2. Click the **Designate Managers** tab.
3. Enter search criteria in all three of the fields in the Users block. For more information, see Search for User Profiles.
4. Click **Search**.
5. Select the user you want to promote to UMA Manager. Any roles and organizations for which this user is currently an UMA manager appear in the UMA Manager Roles and Orgs block. In the next few steps, you will assign the roles and organizations for which this UMA Manager can approve requests.
6. Select an application from the Application Name list.
7. Select the role from the Role Name list that you want to add to the user's request.
8. Select the user's agency from the Agency list.
9. In the Available Orgs box, search for organizations using the Filter list.
10. Select the organizations you want to add.
11. Use the **Move** or **Move All** links to pass those organizations to the Requested Orgs box.
12. Select Yes in the Grant Option field to indicate whether this user can promote other users to UMA Manager. Select No if you do not want the user to be able to promote other users.
13. Use the New Expiration Month End field to set an expiration date for this user's UMA manager privileges.
14. Click **Add Selected Orgs**.
15. Repeat Steps 6 through 14 for other roles, if necessary.
16. Click **Save**. The user will receive an email notification explaining the changes you made to his or her profile.

CPAIS User Roles

To access CPAIS and view or edit data, you need a valid user account and password. Your account has roles that let you work with certain types of data. When you apply for a user account and password, you will request the roles and organizations that you need access to. Speak with your manager or your agency's CPAIS HelpDesk point of contact if you are not sure which roles or organizations you need to request. For more information, see Request a New Account or Modify an Existing Account.

Real Property Accounting Roles

Role	Description
RPA Stream Manager	Role allows user to create or update current year adjustment transactions using the Value Stream screen. Assumes RPA_DISPOSAL_MGR, as needed, to perform responsibilities. Limited number of access privileges for this role in each agency. Users having this access should be limited to one primary and a backup. Users in this role are also allowed to place an asset in service.
RPA Disposal Manager	Role allows the user to create or update subledger accounts, and create write-off transactions for disposed assets using the Value Stream screen. Assumes the RPA_LOCAL_MGR role, as needed, to perform responsibilities. ** If write-offs are performed at the Department level, this role may not be needed at the agency level.
RPA Local Manager	Role provides access to create and maintain subledgers, and set development status. Users having this access are normally operational accountants who deal with real property
RECON_USER	Role provides access to query records related to a rejected transaction and edit any missing or incorrect data in the record
RPA Reconciliation Manager	Role provides access to query records related to a rejected transaction and approve records that have been edited.

Real Property Management Roles

Role	Description
RPM Lease Manager	Role allows the user to create, update, and delete lease records and the authority to issue GSA OA billing adjustment requests. Assumes RPM_PROPERTY_MGR role, if needed, to perform responsibilities. A Property Manager is normally assigned this role.
RPM Property Manager	Role allows the user to create, update, and delete assets and link the assets to GSA sites. This role can be assigned to a facility engineer, fiscal manager, or property manager.
RPM Work Item Manager	Role allows user to enter and update deferred maintenance work items and facility master plan information. This role can be assigned to a facility engineer, fiscal manager, or property manager.
RPM Occupancy Manager	Role allows the user to enter occupancy information for assigned properties or the collocation property managed by other agencies.
RPM Collocation Manager	Role allows the user to manage collocation agreements.

Generic Roles

Role	Description
Contact Manager	Role allows the user to enter different type of contact data into CPAIS. This role is already inherited by all RPA/RPM roles.
FRPP Manager	Role allows an agency user to certify agency data by re-calculating the summary data and updating the status for accuracy and completion.
Read Only	Role allows the user to select all objects for viewing and/or reporting.

Super User Roles

Role	Description
Headquarters Manager	Role assumes all RPA/RPM/Generic roles, as needed, to perform responsibilities. Users having this role should be limited to the Agency Real Property Management POC and Real Property Accounting POC with one back-up person. Users assigned this role will also run security reports for quarterly certifications. May also have limited Department-level personnel (i.e. COD-PRB) assigned to this role for high-level transactions.
SECURITY_ADMN_MGR	Role allows the user to extract the CPAIS user information obtained from the User Access Form. Using a Discoverer report this user can identify all CPAIS users and their level of access to create a security report. This role is only assigned by a system database administrator.