University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

CU Identity Manager

Process Guide:

Process Guide for Security Coordinators

Contents

Security Coordinator Approvals or Rejections

For Support with CU Identity Manager

For questions or support related to CU Identity Manager functionality contact the UIS Service Desk or Access Management.

Security Coordinator Approvals

If you are a designated Security Coordinator for one of the systems listed above you will approve or reject user access requests via CU Identity Manager. Items that have been approved by the user's manager or sponsor will be assigned to you for approvals and other actions as needed.

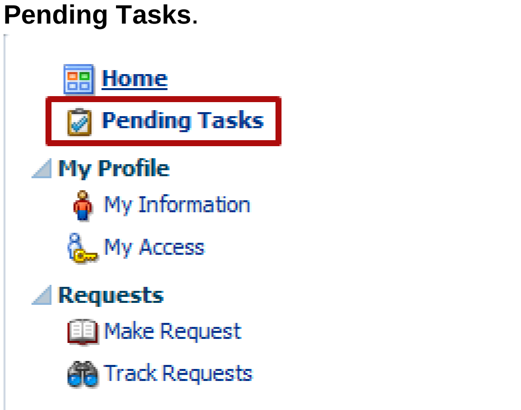
Training Requirements

CU Identity Manager will perform checks for training to ensure required training has been completed for each requested entitlement. The request(s) will fail if training requirements have not been fulfilled and will not be assigned to the manager. Training is checked against SkillSoft directly and against the HCM database for In-Person courses.

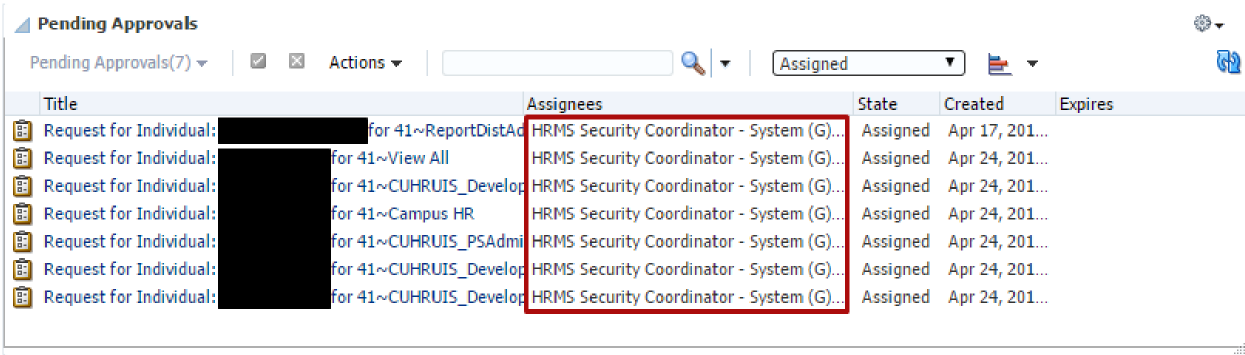
NOTE: Training will need to show as completed in SkillSoft and/or HCM in order for you to receive access to University Systems. Any training not recorded in these systems will not be sufficient for access to be granted.

Approving Requests

1. You should receive an email for any pending request for your application related to jobs or POI statuses associated with your campus. You will receive an email for EACH entitlement requested and must approve or deny each one individually.
2. You may click on the link in the email or log directly into CU Identity Manager.
3. After logging in you will see a **Pending Approvals** section in your **Home** page OR you can click on **Pending Tasks**.

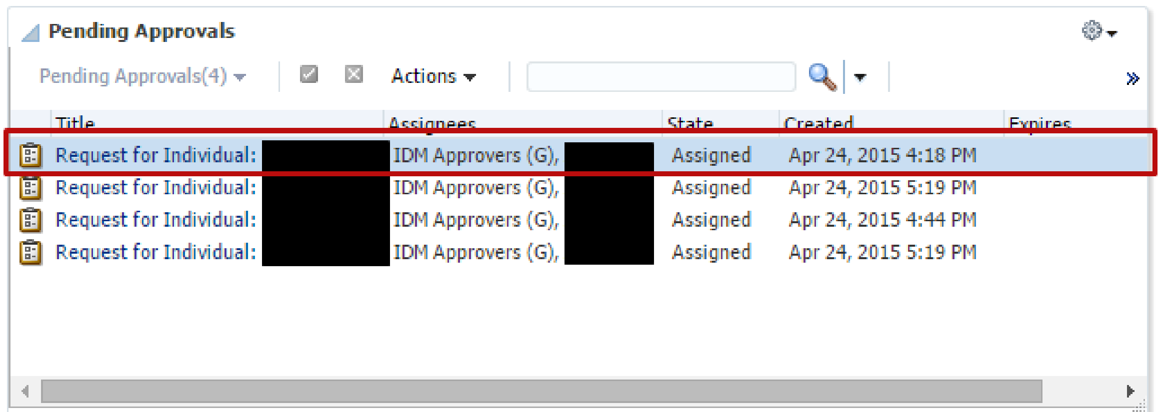


4. In your pending tasks you will see any requests that are waiting for your approval. The pending request will be assigned to your application/Campus security coordinator group.

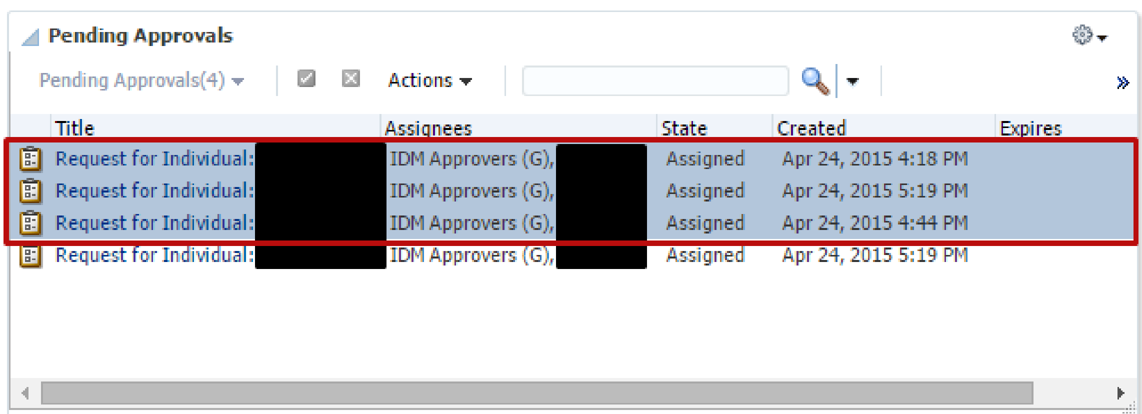


Quick Approvals

a. Select one request by clicking somewhere on the request line other than the title:

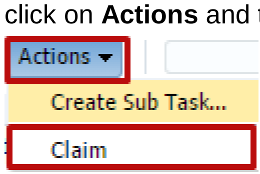


b. Select multiple requests to approve at once by holding shift (for a range) or Ctrl (for individual requests).

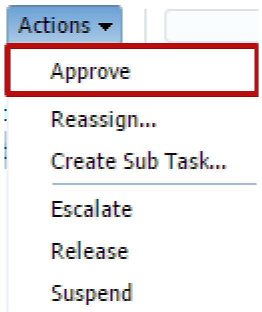


c. Then **Claim** the request(s):

1. click on **Actions** and then **Claim:**



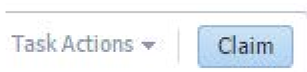
2. Now that you have claimed the request you will see new items in the Actions menu allowing you to approve the request(s):



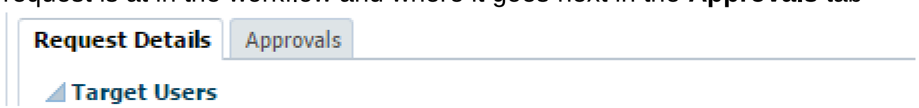
d. Alternatively you may:
   i. **Reassign** the approval to another user (for providing manager/sponsor approval)
   ii. **Escalate** the approval to YOUR manager
   iii. **Suspend** – Pause the request
   iv. **Release** – Un-pause the request
   v. **Create a Sub-Task** – This allows you to create a separate related task to any user.

Detailed Approvals and Rejections

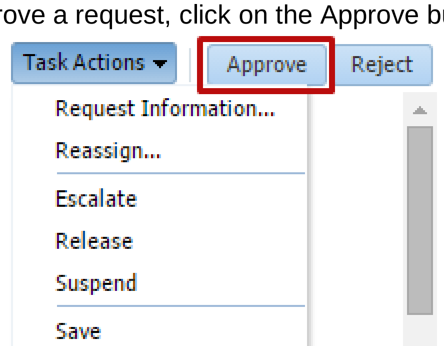
1. Instead of selecting the request(s) to approve, click on the title of the individual request.
2. The request detail tab will open showing detailed information about the request.
3. You may claim the request on this screen if you have not already:



4. After claiming the request you may do the following:
   a. View where the request is at in the workflow and where it goes next in the **Approvals** tab



   b. **Request Additional Information** from the Requestor. See section below on [requesting more information](#).
5. **Approving a Request**
   a. To approve a request, click on the Approve button in the upper right corner:

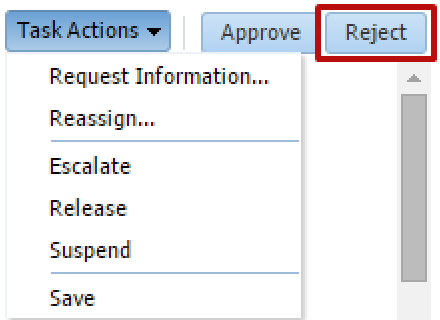


b. The request will be routed to the appropriate application/campus security coordinator for approval.

c. **<u>NOTE:</u>** If you encounter a pop-up error when approving this may be a known CU Identity Manager bug. Despite the error the task was approved. Refresh your pending tasks and ensure that the request is no longer in your pending list.

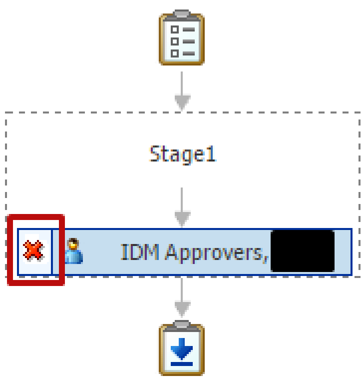
6. Rejecting a Request

a. To reject a request, first add a comment in the comments box explaining the reason for the rejection. Then click on the Reject button.



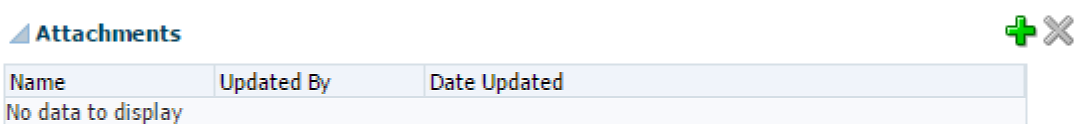
b. You will be routed back to the Inbox/Pending Tasks page. Refresh the page with the icon on the upper right and you should see the request removed from your pending list.

c. The user will receive a notification that request was rejected and you will see in the workflow diagram that the request was rejected:



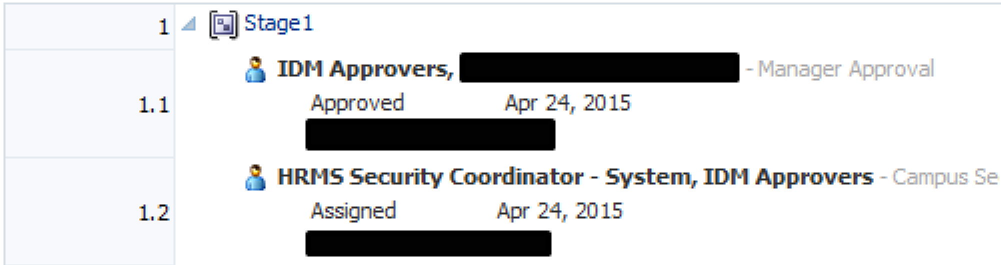
7. Adding an attachment

a. If you need to attach a document for supporting information to a request, you may do so on the Approval tab of the Request Details page:

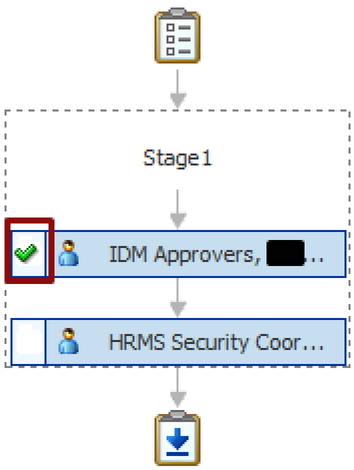


8. Viewing Workflow Status

a. Below you will then see the workflow approval. Most entitlements will be routed to your manager and then to a security coordinator for the system and your campus.



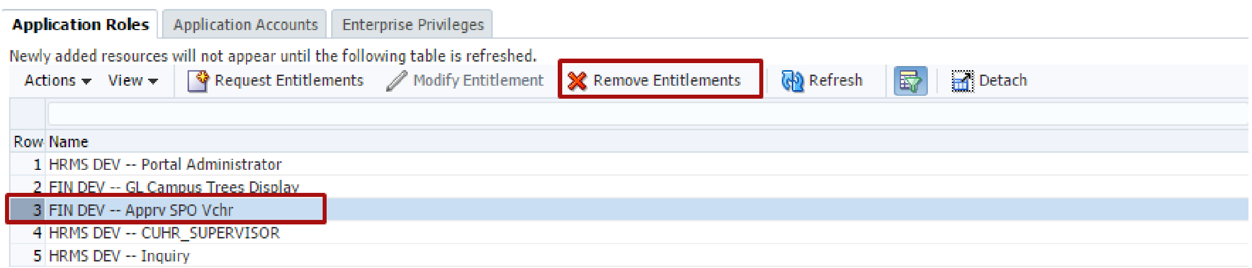
b. In the lower image you will see a green check if the approver has approved the request.



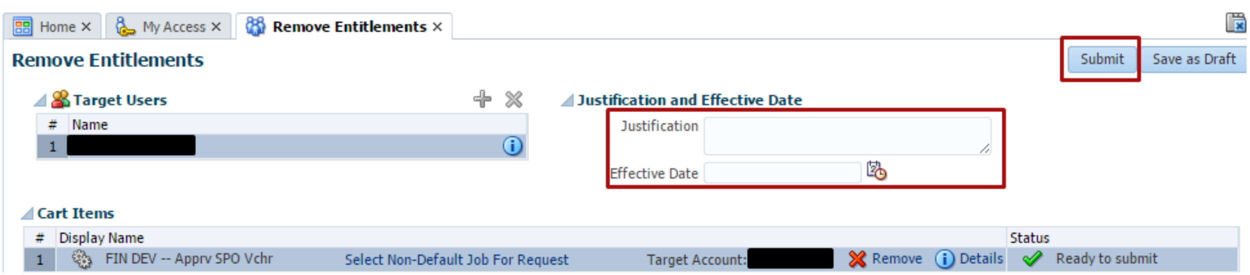
Request to Remove Access

You may initiate a request to remove any of your access. To do so follow these instructions:

1. Log into CU Identity Manager.
2. Click on **Administration > User.**
3. Search for the User – See [**Reviewing Users**](#).
4. Click on the **Application Roles** tab.
5. Select the application roles you want removed and click on **Remove Entitlements**:



6. On the checkout page review your request and add a justification:

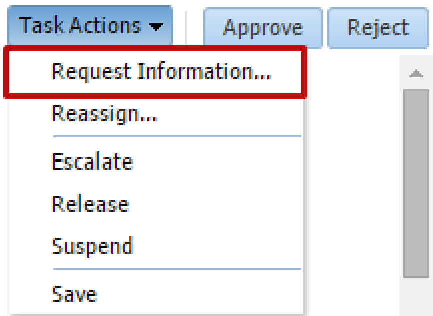


7. Submit your request:

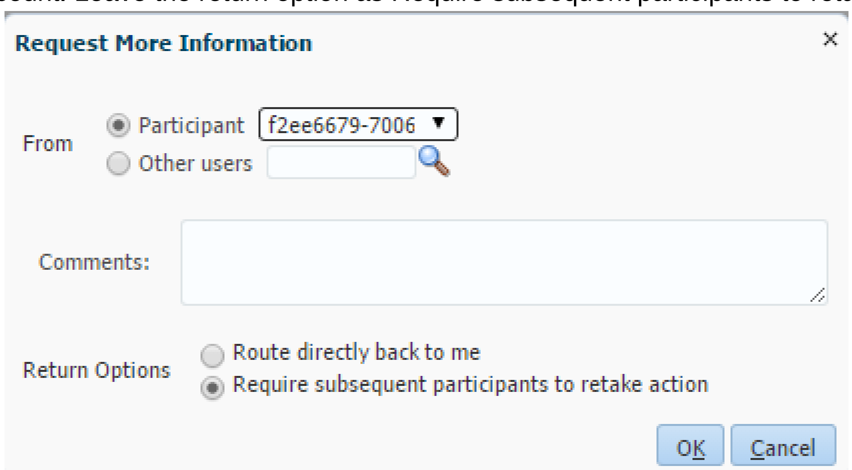
8. As a security coordinator your change will not be routed for approval and the roles will be removed from the target application.

Requesting More Information from the Requestor

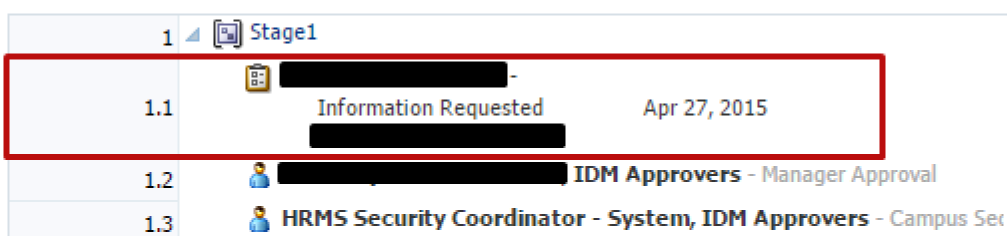
1. In the Request Details screen of a claimed request, instead of approving or rejecting a request you may want to obtain more information for a requestor about what they need. To do this click on Actions and Request Information:

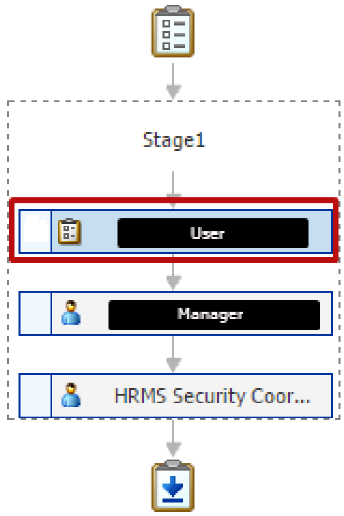


2. A screen will open to enter your information request to the requestor. Enter your question/request and click ok. Do not be concerned with the Participant ID, this is your Constituent ID/ CU Identity Manager sser account. Leave the return option as Require subsequent participants to retake action.

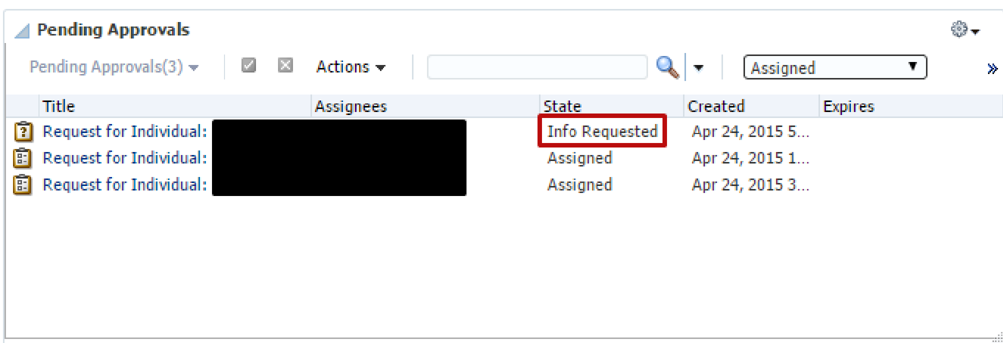


3. The request will be assigned back to the requestor with a task to provide more information about the specific request. You will see this in the workflow diagrams in the **Approval** tab:

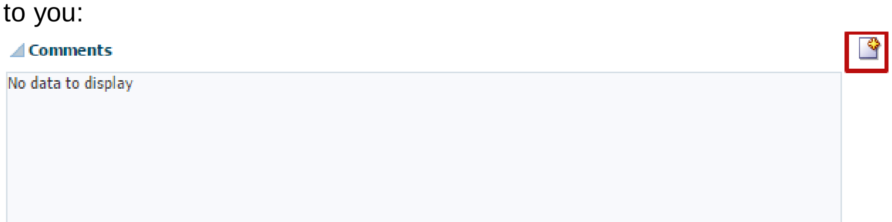




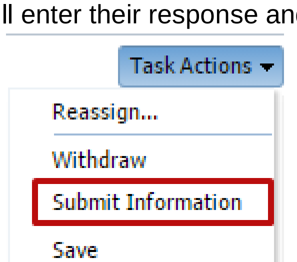
4. After the Requestor has responded to the task, it will be re-assigned to you for further action.
5. The user will see the task –reassigned to them in the **Pending Approvals** section of the **Home** page and in the **Pending Tasks** page:



6. The user will click on the request title to open the details page. They will then enter a comment to respond to you:



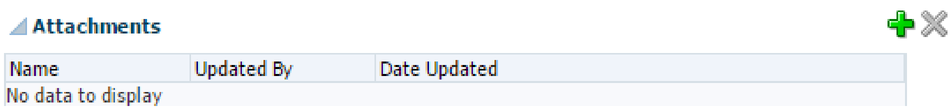
7. They will enter their response and then in the **Actions** menu select **Submit Information**:



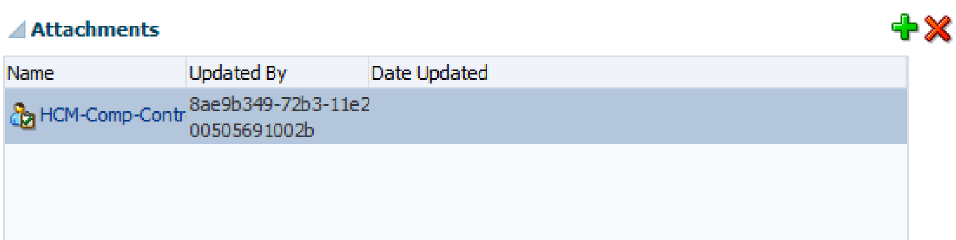
8. Their response will then be assigned to you and their response will be recorded in the **comments** section of the request details page on the **Approvals** tab.

Processing Incompatible Access Requests (CU Marketplace Only)

1. When a user requests roles deemed to be incompatible with other roles that the user already has, in another pending request, or in the same request, CU Identity Manager will flag the request as representing Incompatible Access and will do the following:
    a. Assign the request to the user for an additional self- approval
    b. Send an email to the user explaining that the role is incompatible with another role including instructions to do the following:
        i. The email has a link to a Compensating Controls Form (PDF) that the user must complete.
            1. FIN Compensating Controls
        ii. They user must send the form to a reviewer who will sign the form and send it back to the users.
        iii. The user must then log into CU Identity Manager and look up the request. In the request approval tab, they must attach the completed Compensating Controls form to the request and then self-approve the request.



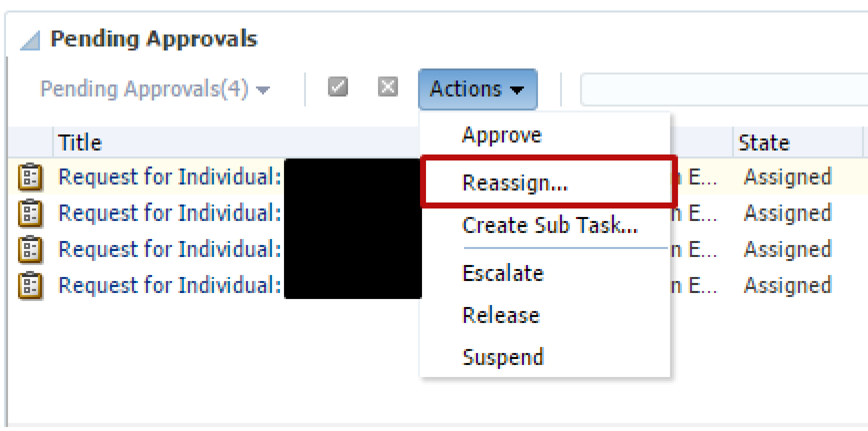
        iv. The request will then be assigned to the manager/sponsor and complete the rest of the normal approval process.
2. When the request is assigned to you as the coordinator, it will have an attachment shown in the attachments section of the details approval tab.



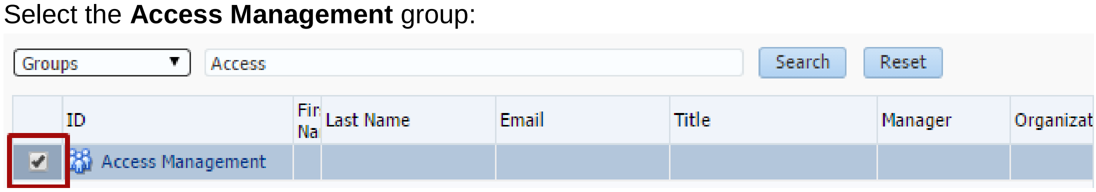
3. Open the form and record the reviewer as you normally would:
    a. FIN: enter the reviewer in the reviewer page in FIN8
        i. Setup Financials/Supply Chain > Security > Incompatible Access
    b. HCM: Record the reviewer as you do now.
4. You may now approve the request.

Processing Department Security (Row Level) Requests (HCM Only)

1. Users will request their required **Department Security** by looking up and requesting an entitlement beginning with "Dept Access":
    a. Dept Access – My Dept Only
    b. Dept Access – All Anschutz
    c. Dept Access – All Boulder
    d. Dept Access – All Denver
    e. Dept Access – All Springs
    f. Dept Access – All System
    g. Dept Access – Custom
        i. For the *Dept Access – Custom* entitlement **only**, the user will need to list what departments they need access to. If they have not provided this in the justification field of the request, then you will need to request the information from them using the Request Additional Information process.
    h. Dept Access – All Campuses
        i. The All Campus department security requires an additional approval from the System Campus HCM Security Coordinator. CU Identity Manager will route the request to that security coordinator after the approval of the primary campus security coordinator.
2. **NOTE:** If the user does not specifically request department level access, they will automatically be granted access to their own department of employment.
3. When you receive a request for **any** of these you must **reassign** it to **Access Management**::
    a. After claiming the request, select **Actions: Reassign**:



    b. A **Reassign Task** screen will open and you will need to do the following:
        i. Set the drop down to **Groups** and search for "Access"
        ii. Select the **Access Management** group:



        iii. Click Ok
    c. The task will be assigned to Access Management for action.
    d. Access Management will update the HCM system with the requested department security.

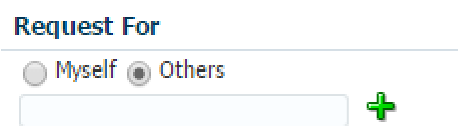
Granting Access for Other Users

To enter a request directly into the target application without training checks, Incompatible Access checks, manager approval, or additional security coordinator approval: log in as yourself with your campus credentials and initiate a request with the following procedures.

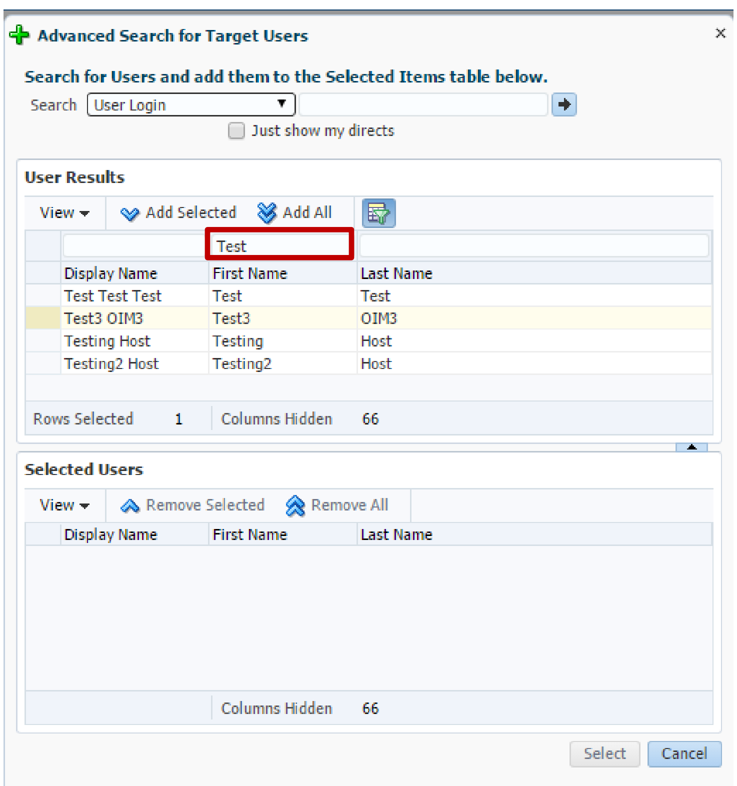
You will primarily use this process to add roles for a user that they did not originally request, but do not need to go through the normal approval process AND to waive training requirements or grant temporary access for future scheduled training.

WARNING: ***When you use this process, it will be YOUR responsibility to check Incompatible Access rules, and track temporary access.***

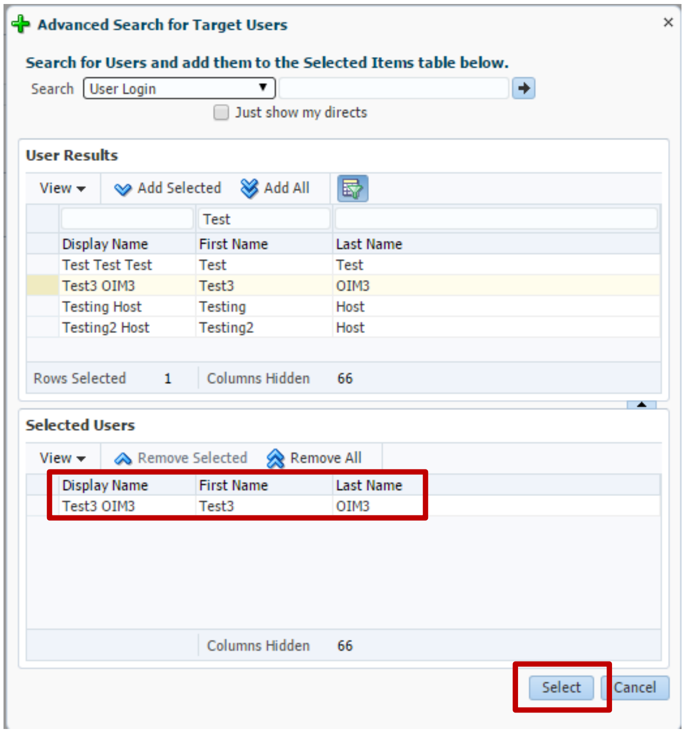
1. Login to CU Identity Manager using the bypass login: https://identity.prod.cu.edu/identity
2. Use your **campus credentials** to log in.
3. Search and Sort the catalog in **Make Request** as you normally would.
4. Set the **Request For** value to **Others** and click on the **green plus** to add users**:**



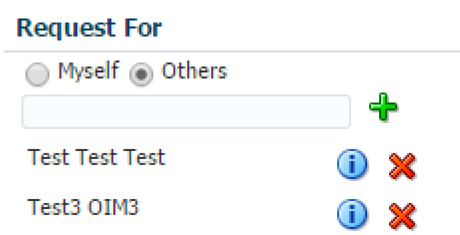
5. In the Search Users window you can search by a variety of fields such as Employee Number (hremplid), First Name, and Last Name. You may also type into the search space above the columns in the User Results.



6. You may select one or more user and Add them by clicking on  such that they are added to the Selected Users section:



7. You will now see the users added to the request:



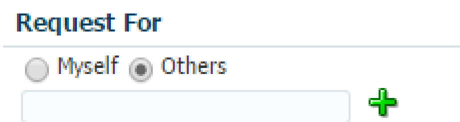
8. When you have selected the users and the application roles (entitlements) to the shopping cart, checkout.
9. On the checkout page you have another opportunity to add users to the request by adding rows with the Target Users:

10. ALL the users added to the cart will have requests for ALL the roles (entitlements) requested. The request will be broken up and assigned to the correct manager and security coordinator based on each user’s job, campus, and the application.
11. Submit the request.

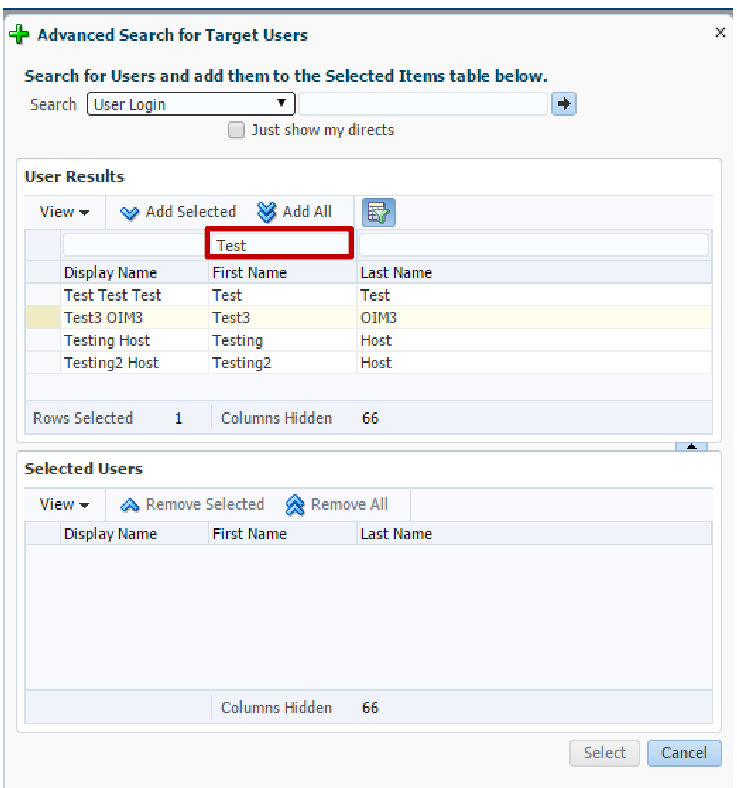
Initiating Requests for Others

To initiate an Access Request for other users that will flow through the complete workflow rather than being auto-approved: log in with your **init-name** account. This will log you in without the extended privileges of a security coordinator and allow you to start a request on behalf of another user.

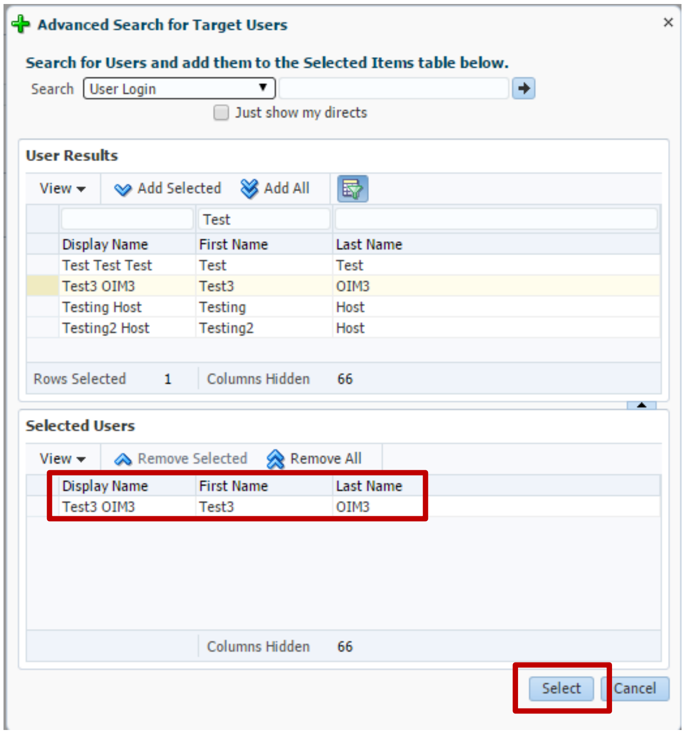
1. Login to CU Identity Manager using the bypass login: https://identity.prod.cu.edu/identity/faces/signin
2. Use your **init-name** account and password to log in.
3. Search and Sort the catalog in **Make Request** as you normally would.
4. Set the **Request For** value to **Others** and click on the **green plus** to add users**:**



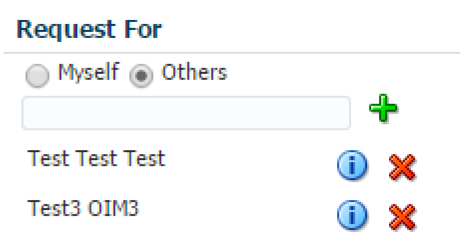
5. In the Search Users window you can search by a variety of fields such as Employee Number (hremplid), First Name, and Last Name. You may also type into the search space above the columns in the User Results.



6. You may select one or more user and Add them by clicking on  such that they are added to the Selected Users section:



7. You will now see the users added to the request:



8. When you have selected the users and the application roles (entitlements) to the shopping cart, checkout.
9. On the checkout page you have another opportunity to add users to the request by adding rows with the Target Users:

10. ALL the users added to the cart will have requests for ALL the roles (entitlements) requested. The request will be broken up and assigned to the correct manager and security coordinator based on each user’s job, campus, and the application.
11. Submit the request.

Processing PDF Forms

For a grace period after CU Identity Manager go-live (and through Year-End 2015 for FIN) we will continue to process PDF request forms for the following reasons:

- The request was already in process when CU Identity Manager went live
  - The user should be instructed to use CU Identity Manager in the future
- The user used a form they had stored locally
  - The user should be instructed to use CU Identity Manager in the future
- There was a problem with requesting access via CU Identity Manager.
  - The issue should be reported to access@cu.edu immediately.

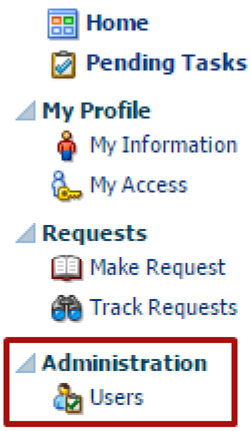
To process the PDF form in CU Identity Manager, follow these instructions:

1. Log into CU Identity Manager using your normal account
2. Use the Make Request page to select the user.
3. Enter the roles from the PDF form.
4. Checkout and select alternate job data if needed.
5. Submit the request.
6. Archive the PDF form in singularity or send to access@cu.edu requesting to have it archived. Please indicate that the form was already processed.

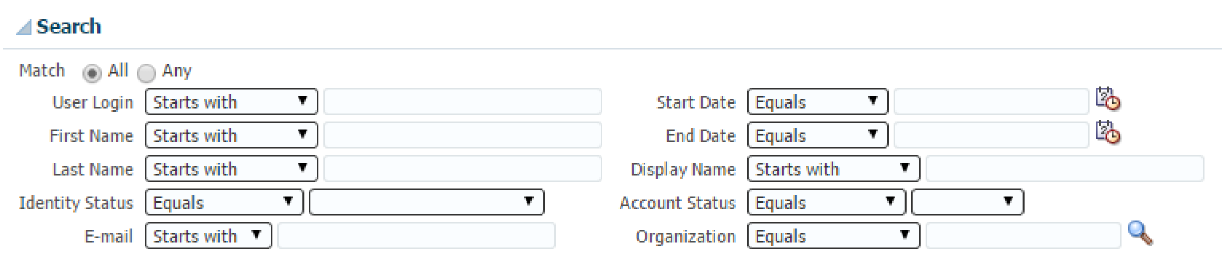
Reviewing Users

To review existing accounts and access for a user follow these instructions:

1. Log into CU Identity Manager using your normal account
2. Click on the **Administration > Users** link in the left-hand navigation:

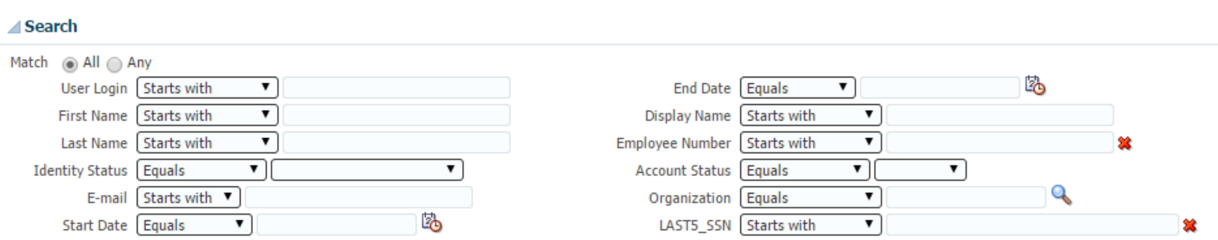


3. Search for the user. Do not use the **User Login** field as that will be the user **Constituent ID**:

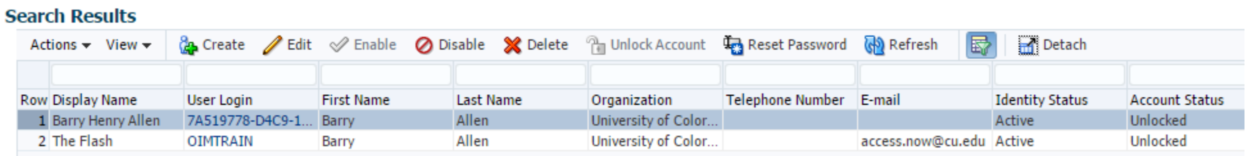


4. You may add search fields to those shown with the **Add Fields** button:

5. Not all the fields available are populated with information in CU Identity Manager, but **Employee Number** and Last5_SSN may be useful:

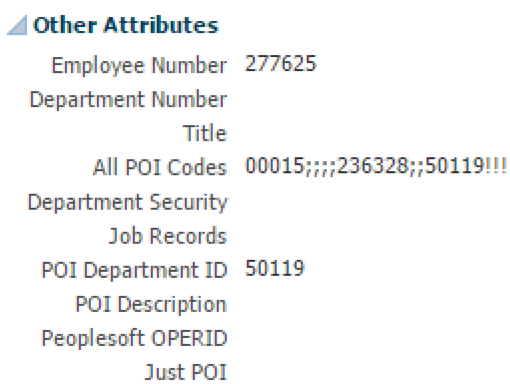


6. You should receive results. If you do not, make sure the search did not save data from a previous search. You may click **Reset** to clear all the search fields.

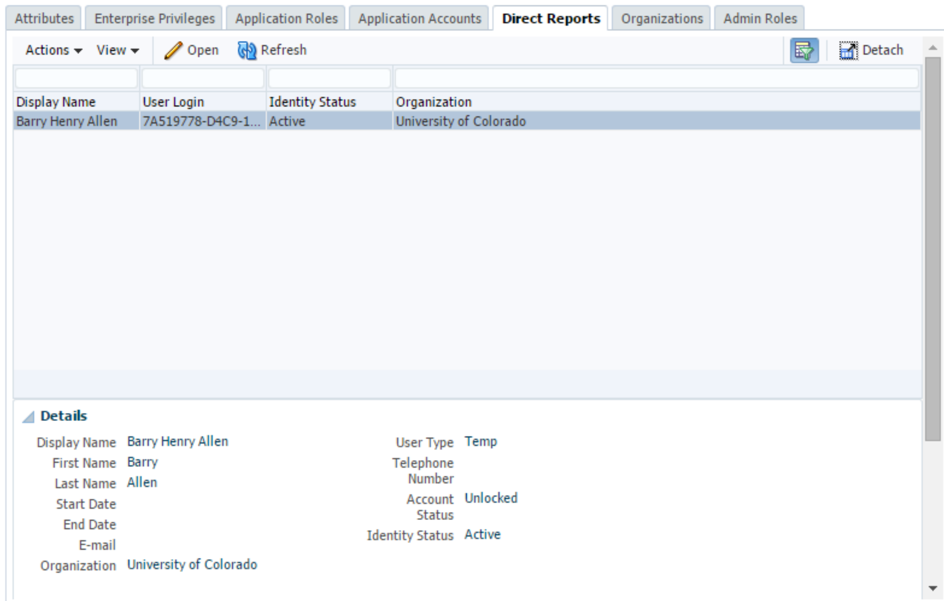


7. Click on the **User Login value** to open the desired user.
8. In the User information you will see several tabs:
    a. User Attributes:
        i. Basic Info:

        ii. Other Attributes including:
            1. Employee Number
            2. HCM Department security by Node
            3. Department Code
            4. POI and Job Information

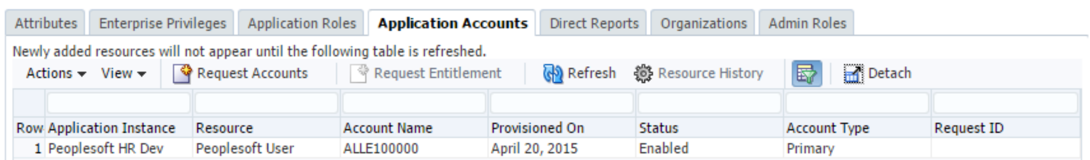


        iii. The user's direct reports if they are a manager or POI sponsor:



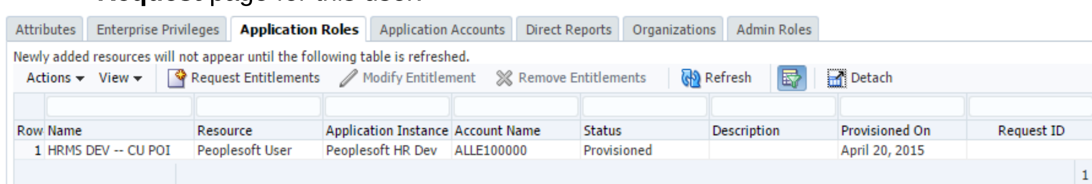
iv. User Accounts

1. Listed by Application Instance:



v. User Application Roles for all application instances:

1. Notice you may request application roles (entitlements) for this user by using the **Request Entitlements** button. This will take you to the **Make Request** page for this user.



vi. Enterprise Privileges

1. This is for CU Identity Manager use only.
2. This will show you if the user is setup as a security coordinator.

vii. Organization

1. This will show the organization the user is associated with.

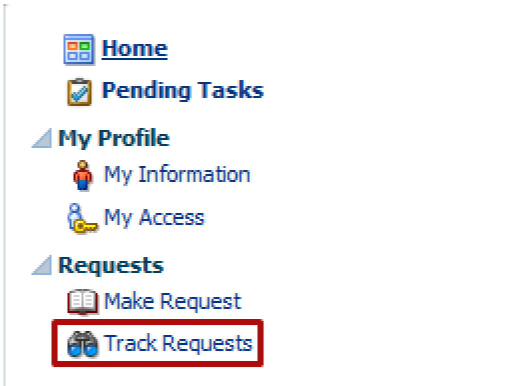
viii. Admin Roles

1. This is for CU Identity Manager users only.
2. This will show you if the user has Help Desk access or other special privileges in CU Identity Manager.

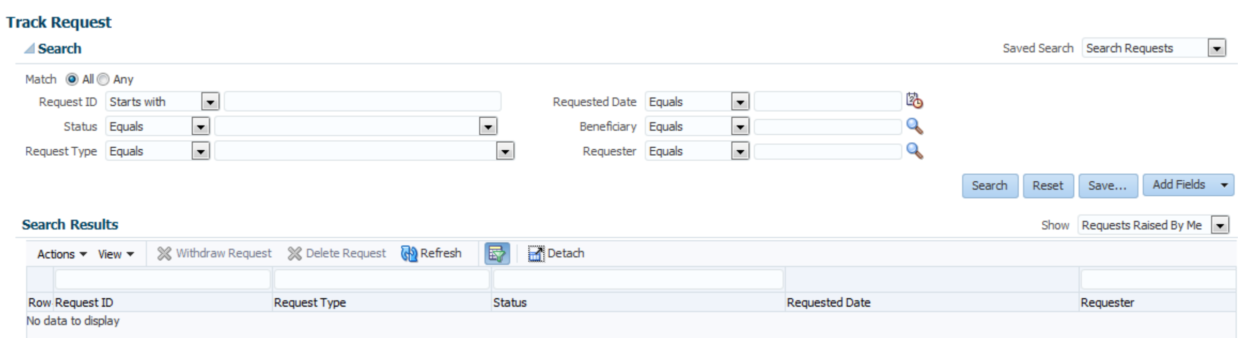
Tracking Requests

To check on the status of an existing request follow these instructions.

1. Log into CU Identity Manager using your normal account.
2. Click on **Requests > Track Requests**



3. The **Show** field defaults to **Requests Raised by Me**. To look up requests for others or requests for you that were created by others change this setting before searching.
    a. **Requests Raised By Me**
    b. **Requests Raised For Me**
    c. **For a User** (Search All for Security Coordinators, Help Desk, and Admins only)
        i. You must enter a requestor or beneficiary for the **For a User** option.



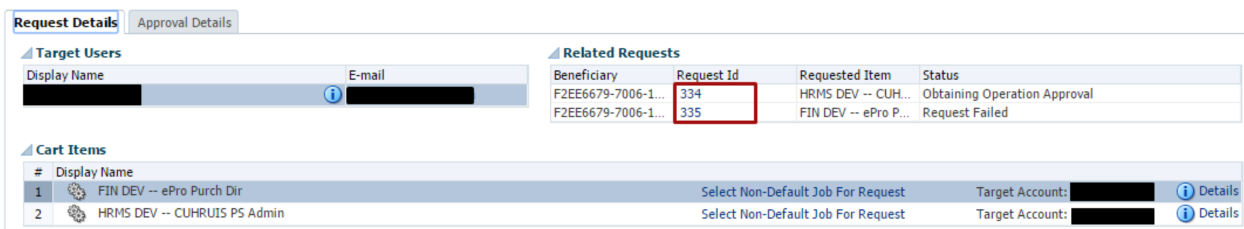
4. The result will show request IDs and their status. Click on a request ID to review the details:

Actions ▾ View ▾ Withdraw Request Delete Request Refresh Detach

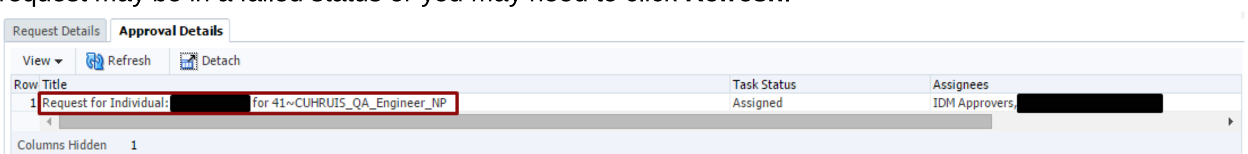
Row	Request ID	Request Type	Status	Requested Date
1	Request ID: 328	Provision Entitlement	Obtaining Operation Approval	April 24, 2015
2	Request ID: 329	Provision Entitlement	Request Completed	April 24, 2015
3	Request ID: 330	Provision Entitlement	Request Failed	April 24, 2015
4	Request ID: 321	Provision Entitlement	Request Failed	April 23, 2015
5	Request ID: 319	Provision Entitlement	Obtaining Operation Approval	April 24, 2015
6	Request ID: 314	Provision Entitlement	Request Awaiting child Requests Completion	April 24, 2015
7	Request ID: 315	Provision Entitlement	Request Failed	April 24, 2015
8	Request ID: 317	Provision Entitlement	Obtaining Operation Approval	April 24, 2015
9	Request ID: 316	Provision Entitlement	Request Failed	April 24, 2015

5. If the request has failed, click on the Request Failed link to see why:

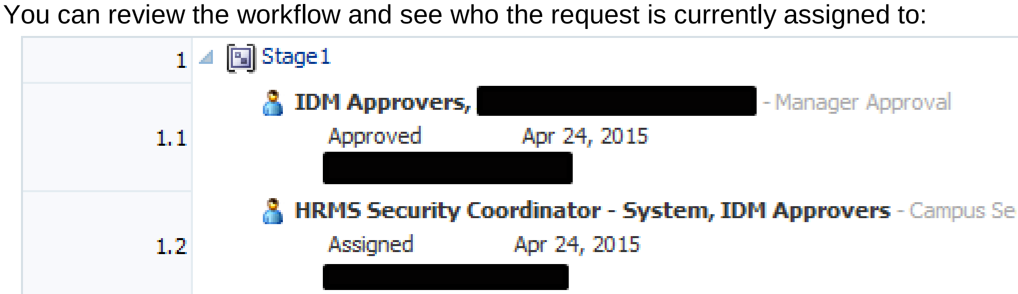
6. In the Request Details tab you can see information about the request.
   a. If the request is a parent request, it will have multiple Request ID listed under Related Requests. If it is a child request, it will list the parent. You can switch back and forth by clicking on the related request ID.



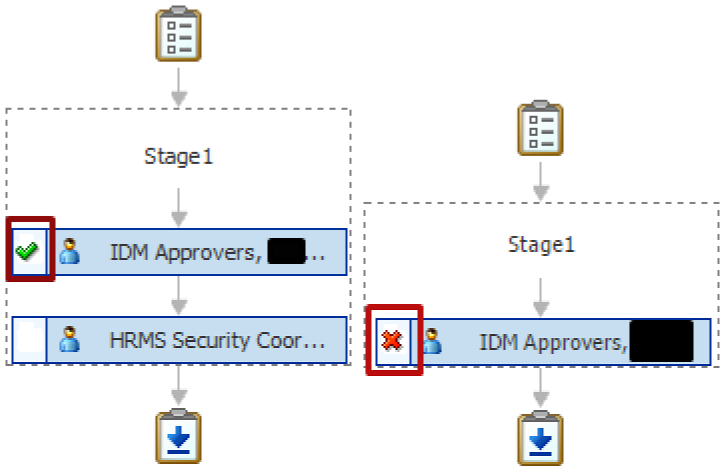
7. In the **Approval Details** tab, double click on the title of the request. If the title does not appear, the request may be in a failed status or you may need to click **Refresh**.



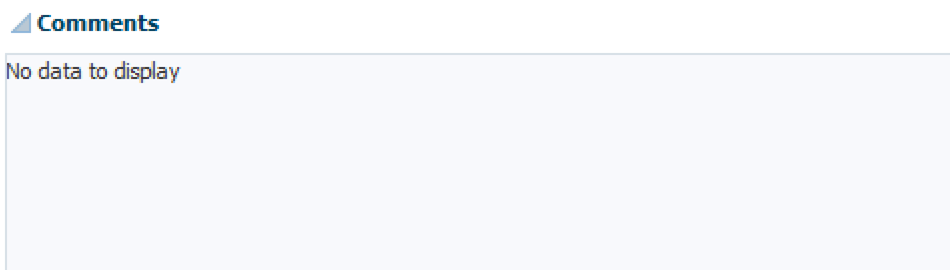
8. You can review the workflow and see who the request is currently assigned to:



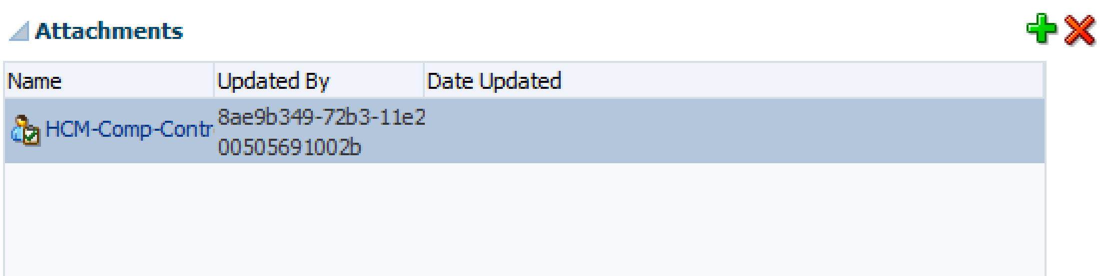
9. And see who has approved or rejected the request:



10. You can review any comments:
    a. Reason for rejection
    b. Request for information



11. And review any attachments

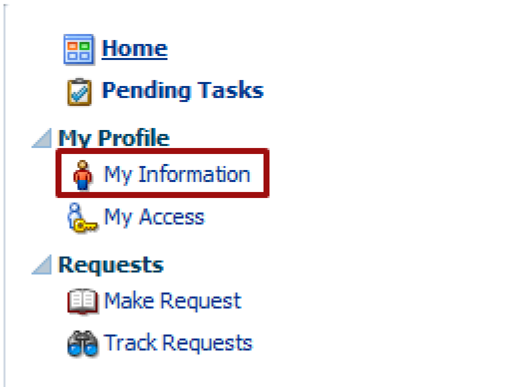


:

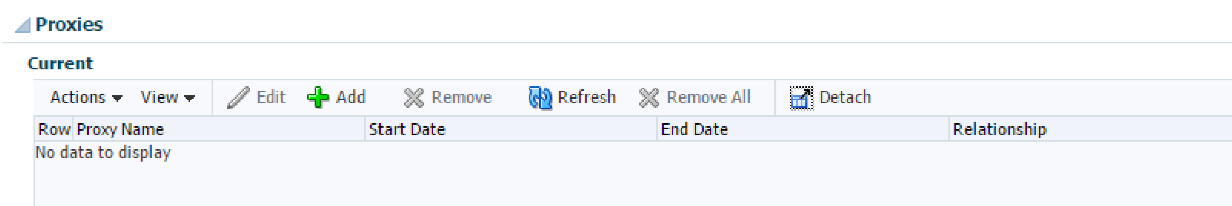
Assign a Proxy

If you are going to be out of the office and would like to assign a proxy to approve access requests on your behalf, you may do so in CU Identity Manager. You may also define a long-term proxy to approve requests on your behalf simply by using a longer date range.

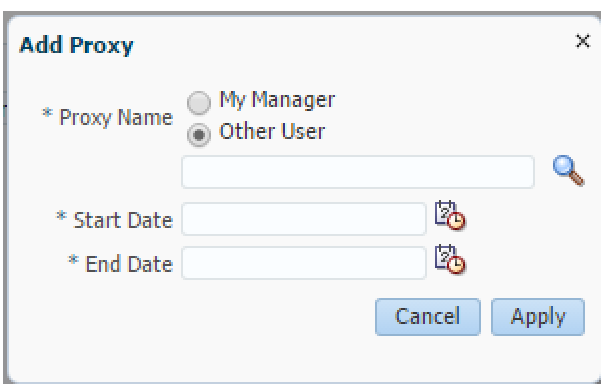
1. Log into CU Identity Manager.
2. Go to the **My Profile > My Information** page:



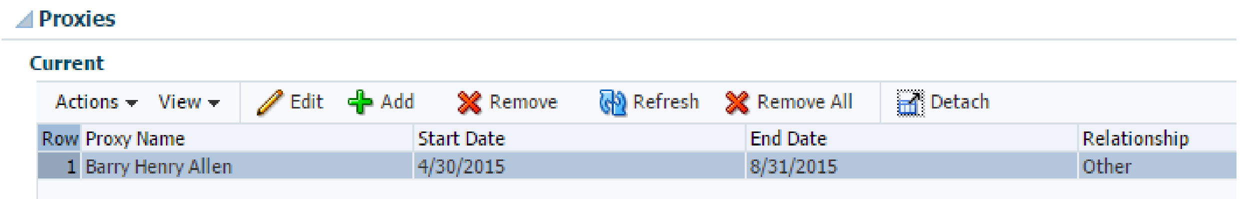
3. Scroll down to the Proxy section.



4. Add a proxy:



5. You may select the manager associated with your primary job, or you may look up another user.
6. Set a start and end date. During this period the proxy will have access to your pending approvals and can claim them and approve or reject as you would.



7. The proxy will expire at the end date set, or you can remove them to inactivate their proxy status.

Appendix

URLs

- CU Identity Manager Links, Information, and Guides
- UIS Service Desk