CU Identity Manager

Process Guide:

Process Guide for Requesting Access

Contents

Requesting Access in CU Identity Manager

For Support with CU Identity Manager

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

Application Access Requested Through Identity Manager

This document details the process of using CU Identity Manager to request entitlements that provide access to the following systems:

- Human Capital Management system (HCM)
- Finance System (FIN)
- CU Marketplace – (ePro* entitlements in FIN)

POI Access

For POIs only POI type 15 can request access to CU applications and IT resources.

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.

You will need to complete the required training for each application role you request BEFORE you make your request. If you do not complete the required training the request will fail and you will need to start your request again after completing the required training.

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.

Making a Request

1. If you are requesting entitlements for yourself, click on **Make Request**. Note: If you are requesting entitlements for someone else see Initiating Requests for Others.
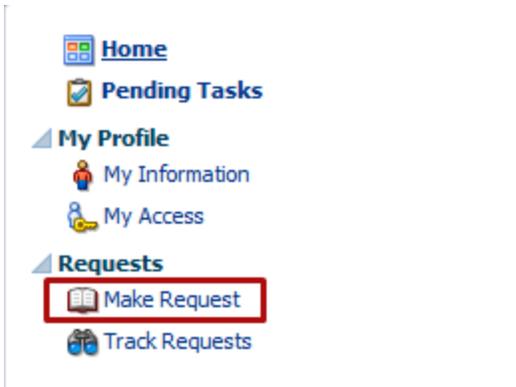
2. In the catalog, search for all entitlements or enter a role name and search.

3. Update the **Sort By** option to Display name to list entitlements in alphabetical order.


4. Look at the entitlement prefix to find the application environment you are requesting access for. Examples: FIN DEV for FIN Development Environment, FIN for FIN Production access, HCM for HCM Production.

5. Add individual entitlement to your shopping cart by clicking on the **Add to Cart** button to the right, OR select all the roles you need and use the **Add Selected to Cart** in the upper left to add multiple entitlements at once. If you encounter a >> symbol where the **Add to Cart** button should be, just click on it to reveal the **Add to Cart** button.

6. You may add entitlements for multiple applications environments. When you are done click on **Checkout**.
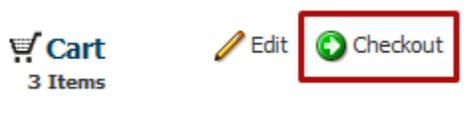
7. On the Checkout page you can enter information for approvers in the **Justification** field.

Justification and Effective Date

Justification

Effective Date

8. For multiple Jobs or Job and POI status:
    a. If you have multiple Jobs or a Job AND a POI status your request by default will be associated with your primary Job. To change which job the access is associated with click on **Select Non-Default Job for Request** for EACH entitlement.

| 2 | FIN DEV -- AR Receivables Entry | Select Non-Default Job For Request | Target Account: In Cart | Remove | Details | Ready to submit |
| 3 | FIN DEV -- AM Asset Inquiry | Select Non-Default Job For Request | Target Account: In Cart | Remove | Details | Ready to submit |

    b. Remove any entitlements from your request by clicking **Remove**.
9. When you are satisfied with the items in your cart, **Submit** your request or save it as a draft to return to it later.

Submit   Save as Draft

10. Once you have submitted your request, you will arrive to a **Request Summary** page. Your request has been successfully submitted!
11. On the Request Summary page wait a few seconds and then refresh the page to check the status.

Summary Information   Refresh   Withdraw Request

Request Id	318	Requester	DARSWeb Z9VSRSYS02
Requested Date	4/24/2015	Status	Obtaining Request Approval
Effective Date		Parent Request ID	
Justification		Request Type	Heterogeneous Request

    a. If the status shows **Request Failed**, you may not have completed the training course required for your access. Click on the words **Request Failed** and the popup will tell you the reason.

Summary Information

Request Id	330	Requester	
Requested Date	4/24/2015	Status	Request Failed
Effective Date		Parent Request ID	314
Justification		Request Type	Provision Entitlement

Request Error Details   ✕

IAM-2050126 : Invalid outcome Required training not complete. Request requires completion of: A00029,A00030,F00001 received from SOA for the request id 330.
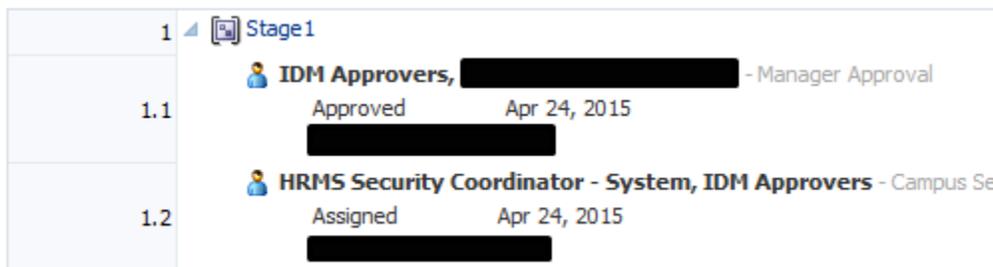
b. If you requested multiple Entitlements, the main request is a parent request and each entitlement is a child request. You can see the status of all the individual requests in the Request Details tab in the Related Requests box. Click on the Request ID of the child request to see its status.

| Request Details | Approval Details |

Target Users

Display Name	E-mail
▓▓▓▓▓▓▓▓▓▓▓▓ ⓘ	▓▓▓▓▓▓▓▓▓▓

Related Requests

Beneficiary	Request Id	Requested Item	Status
F2EE6679-7006-1...	352	HRMS DEV -- CUHRUIS QA Engine...	Request Created
F2EE6679-7006-1...	353	HRMS DEV -- CUHRUIS Portal Int...	Request Created

Cart Items

#	Display Name			
1	HRMS DEV -- CUHRUIS Portal Integration NP	Select Non-Default Job For Request	Target Account: MCCA000394	ⓘ Details
2	HRMS DEV -- CUHRUIS QA Engineer NP	Select Non-Default Job For Request	Target Account: MCCA000394	ⓘ Details

c. To check who the request was assigned to click on the **Approval Details** tab. Under Assignees you will see IDM Approvers and the manager your request went to for approval (redacted in the screen shot below). Double click on the request title for more details.

| Request Details | Approval Details |

View ▾   🔄 Refresh   📄 Detach

Row	Title	Task Status	Assignees
1	Request for Individual: ▓▓▓▓▓ for 41~CUHRUIS_QA_Engineer_NP	Assigned	IDM Approvers, ▓▓▓▓▓▓▓

Columns Hidden   1
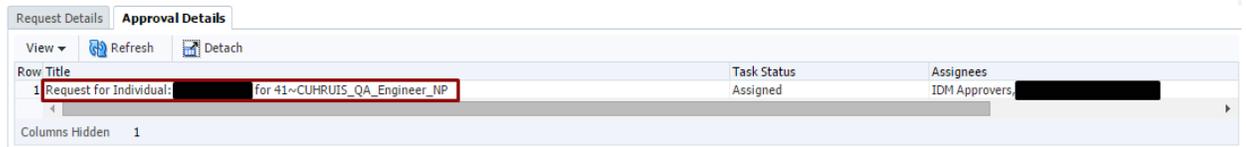
d. Below you will then see the workflow approval. Most entitlements will be routed to your manager and then to a security coordinator for the system and your campus.

1	⊿ 🔲 Stage1
	👤 **IDM Approvers,** ▓▓▓▓▓▓▓▓▓▓▓▓▓ - Manager Approval
1.1	Approved Apr 24, 2015
	▓▓▓▓▓▓▓▓▓
	👤 **HRMS Security Coordinator - System, IDM Approvers** - Campus Se
1.2	Assigned Apr 24, 2015
	▓▓▓▓▓▓▓▓

e. In the lower image you will see a green check if the approver has approved the request.
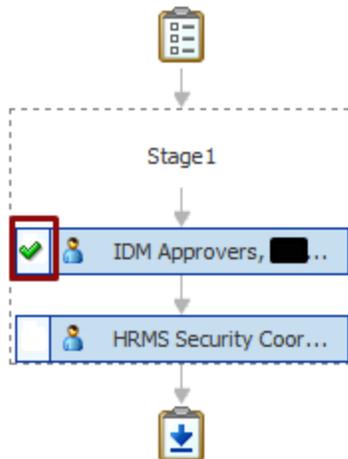
12. You will receive an email when your request has been completed or if it is denied by an approver. To check on the status of your request by following the **Track a Request** instructions.
13. If you receive an email indicating that one of your entitlements will result in incompatible access, follow the instructions in the email or in the **Incompatible Access** directions.
14. Also see the related instructions:
    a. **Requesting Department Security (HCM Only).**

Request to Remove Access

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

1. Log into OIM.

2. Click on **My Profile > My Access.**

3. Click on the **Application Roles** tab.

4. Select the application roles you want removed and click on **Remove Entitlements**:

5. On the checkout page review your request and add a justification if needed:

6. Submit your request:

7. Your request will be routed to an administrator for approval after which the access will be removed.

Requesting Department Security (HCM Only)

1. When do you need to request Department Security Access?
    a. When you are making your initial HCM access request.
    b. When you need to change your department security.
2. **NOTE:** If you do not specifically request department level access, you will automatically be granted access to your own department of employment.
3. You will need to specify what level of department access you require by requesting one of the following HRMS entitlements. In the Make Request page search for and request 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**, you will need to list what departments you need access to. If you do not provide this in the **justification** field of the request, then you may be asked to provide this information 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 HRMS Security Coordinator. OIM will route the request to that security coordinator after the approval of the primary campus security coordinator.

Requesting Incompatible Access (CU Marketplace Only)

If you request roles that constitute Incompatible Access, you will have to identify a Reviewer who will approve your Incompatible Access. They will need to sign the Compensating Controls form for the system you are requesting the IA access and you will need to attach the form to your OIM request before it will go to your manager for approval.

1. Log into OIM and request the access for CU Marketplace

2. If the request includes application roles that will result in Incompatible Access, the request will NOT be assigned to your manager/sponsor for approval, but will be assigned to you for action.

3. You will receive an email from the system with instructions.

    a. The email will include a link to the Compensating Controls Forms.

        i. FIN Compensating Controls
    b. Fill out the user portion of the form, provide the Reviewer information, and sign the form.

    c. Send the form to the Reviewer.

        i. The Reviewer will have to sign the form and return it to you.

4. Log into OIM

5. Open your pending request in the Pending Tasks page.
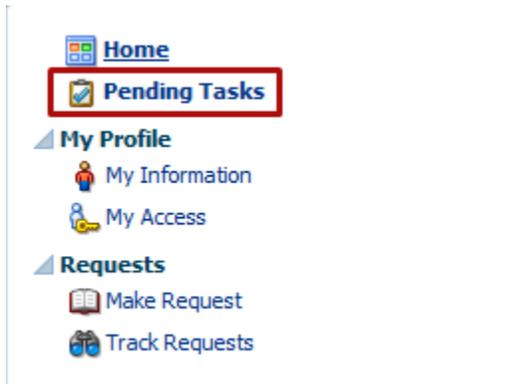
6. Open the request by clicking on the Request Title.

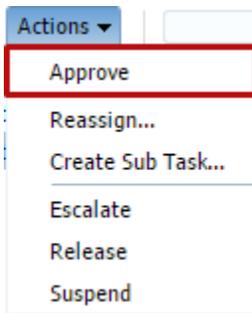
7. Claim the request

8. On the Approval Details Tab, use the Add Attachments section in the lower right corner.
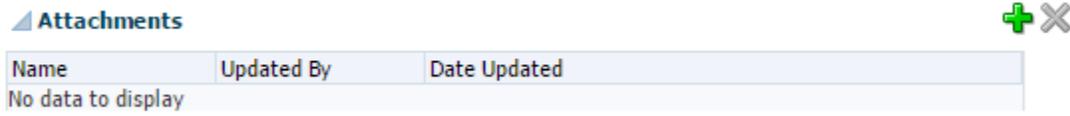
9. Add the PDF form as an attachment.

10. Approve the request to send it on to your manager/sponsor for approval.

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 OIM 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:
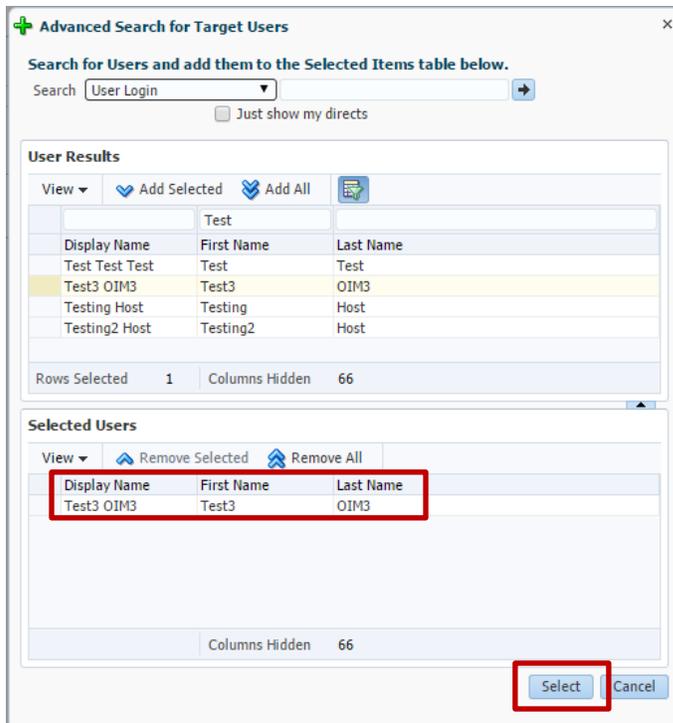
7. You will now see the users added to the request:
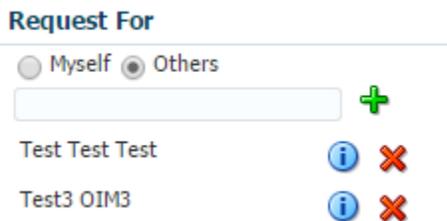
8. When you have selected the users and the application roles (entitlements) to the shopping cart, checkout.

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.

Tracking a Request

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

1. Log into OIM using your normal account.
2. Click on **Requests > Track Requests**
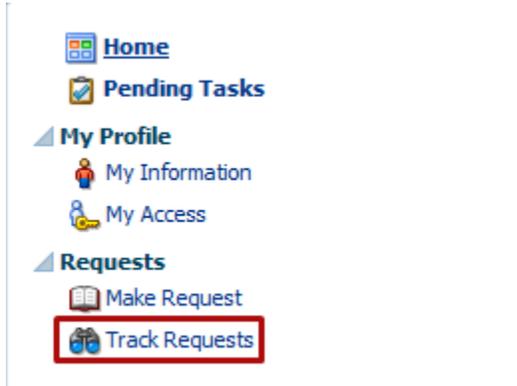
3. The **Show** field defaults to **Requests Raised by Me**. To look up requests for others or requests for you that were created by others change this setting before searching.
    a. **Requests Raised By Me**
    b. **Requests Raised For Me**
    c. **For a User** (Search All for Security Coordinators, HelpDesk, 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:

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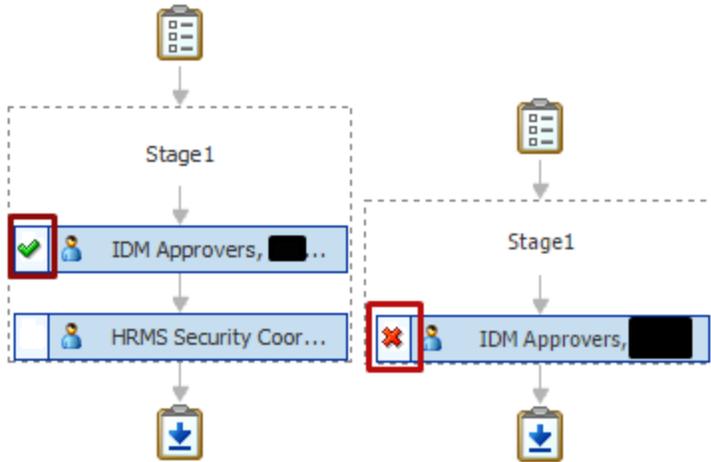
10. You can review any comments.
      a. Reason for rejection
      b. Request for information

11. And review any attachments

My Access

You can review your existing access using the **My Profile > My Access** page.

1. Click on My Access in the left-hand navigation:
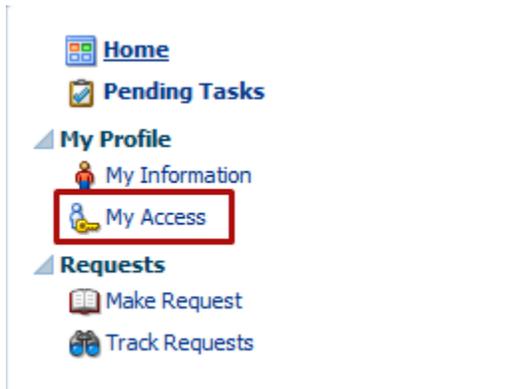
2. You will have four (4) tabs in the My Access page:

   a. Application Roles

   b. Application Accounts

   c. Enterprise Privileges (For OIM Only)

   d. OIM Admin Roles (For OIM Only)

3. **Application Roles**

   a. This tab will show your existing application roles listed by **Application Instance** (HCM DEV) and **Account Name** (SMIT000001).

   b. From here you can request additional access by clicking on the **Request Entitlements** button. This will take you to the Make Request page to start a new request.

4. **Application Accounts**

   a. This tab will show the accounts you have in various applications and IT Resources.

   b. There is a Request Accounts button, but you should not use this. Requests will be denied.

Appendix

URLs

- [CU Identity Manager Links, Information, and Guides](#)
- [UIS Service Desk](#)

CU Identity Manager Process Guide
February 2016 | Prepared by: UIS-Identity and Access Management