CJLEADS

Criminal Justice Law Enforcement Automated Data Services

NCID-NG User Administration

Table of Contents

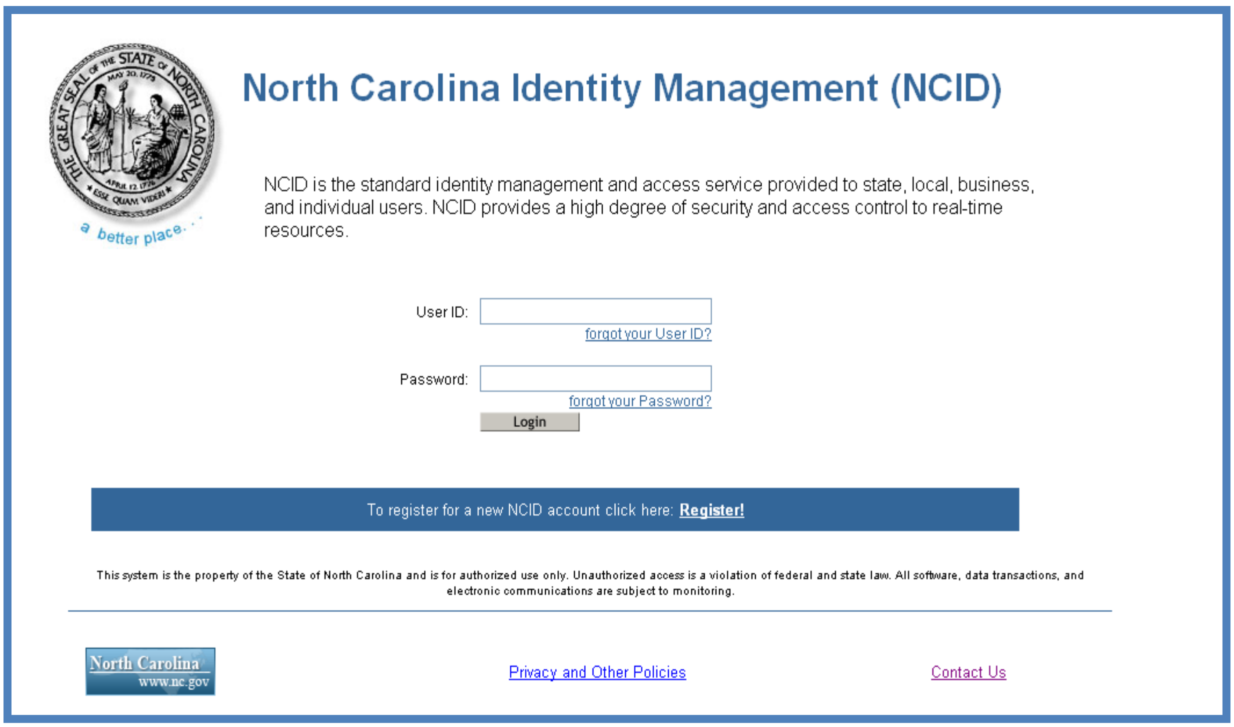
Introduction

The **North Carolina Identity Management Service – Next Generation (NCID-NG)** is the standard identity and access management platform provided by the Office of Information and Technology Services. NCID-NG is a Web-based application that provides a secure environment for state agency, local government, business and individual users to log in and gain access to real-time resources, such as customer-based applications.

CJLEADS is leveraging NCID"s authentication capabilities to ensure that the CJLEADS application is secure. The NCID username and password will be used to access CJLEADS. This document will provide administrators basic instructions for using NCID.

Logging In

Administrators can access the NCID login page at: https://ncid.nc.gov



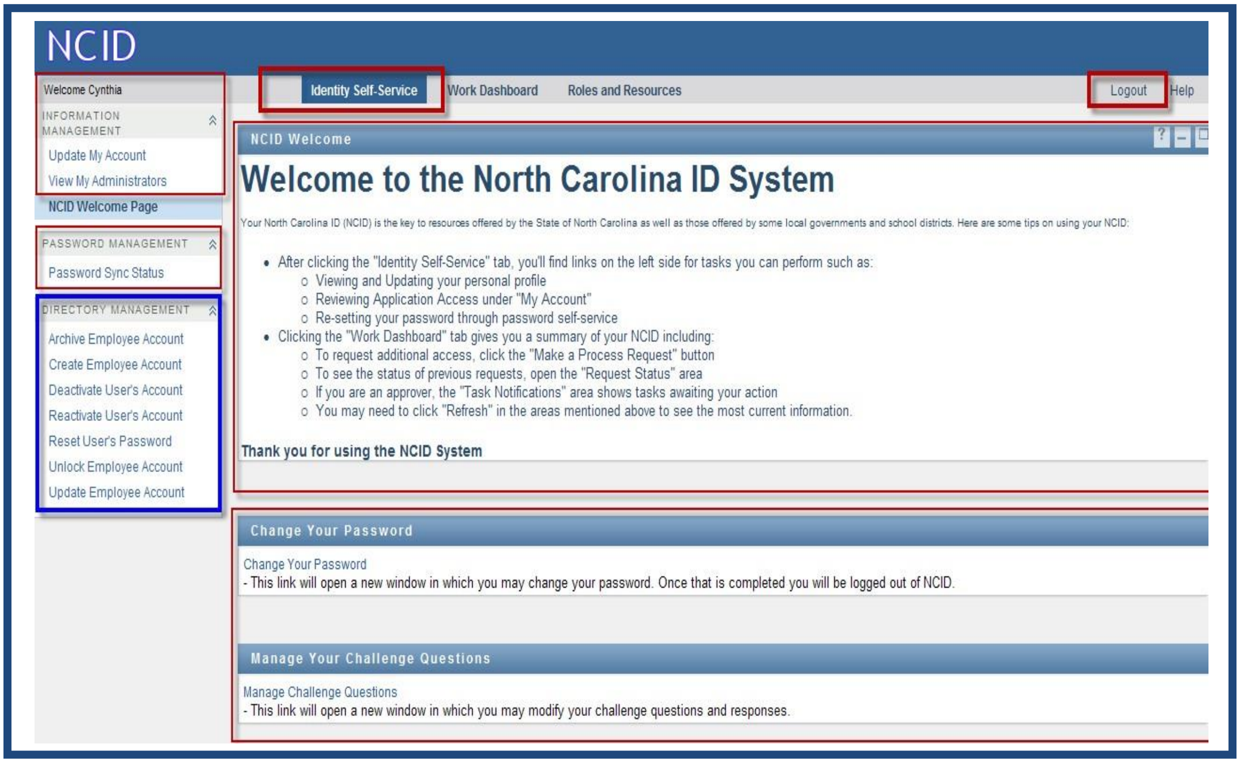
Administrators should already have an NCID. If not, you will need to contact a delegated administrator for your agency to create an account for you. If you do not have a delegated administrator contact ITS at 919 754-6000 or 1-800-800-722-3946. The delegated administrator will also need to promote your account to delegated administrator for your agency, division or section.

Type the **username**.

Type the **password**.

Click **Login**.

The *Welcome to NCID* screen opens.



After logging in to NCID-NG, all users are greeted with the main screen. The delegated administrator screen displays a welcome message, quick tips to help you get started, end user self service tools and a directory management section with links to manage end user accounts.

Managing User Accounts

Administrators manage user accounts from either the "Identity Self-Service" tab or from the "Work Dashboard" tab. The Identity Self-Service tab displays links to the most commonly used process requests; whereas the Work Dashboard tab provides access to every request that is available to you.

Note: (screen content and feature availability will vary based on job responsibility and access permissions.

Self Service Tools:

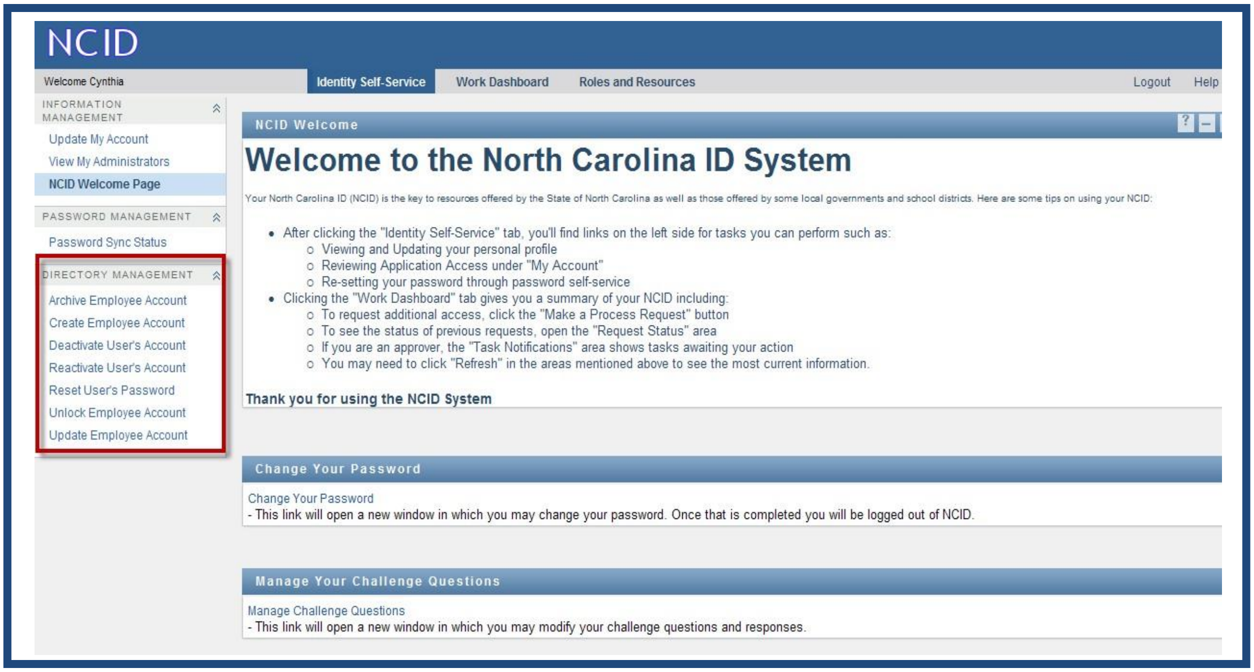
- Identity Self-Service tab - *shows user self-help tools*.
- Update My Account allows user profile edits.
- Password Sync Status shows success/failure of Password Sync to applications.
- Change Password link
- Manage Challenge Questions link
- Logout link

Delegated Administrator Tool – basic tools to manage accounts

- Activate Employee Account
- Create Employee Account
- Deactivate Employee Account

Reactivate Employee Account
Unlock Employee Account
Update Employee Account

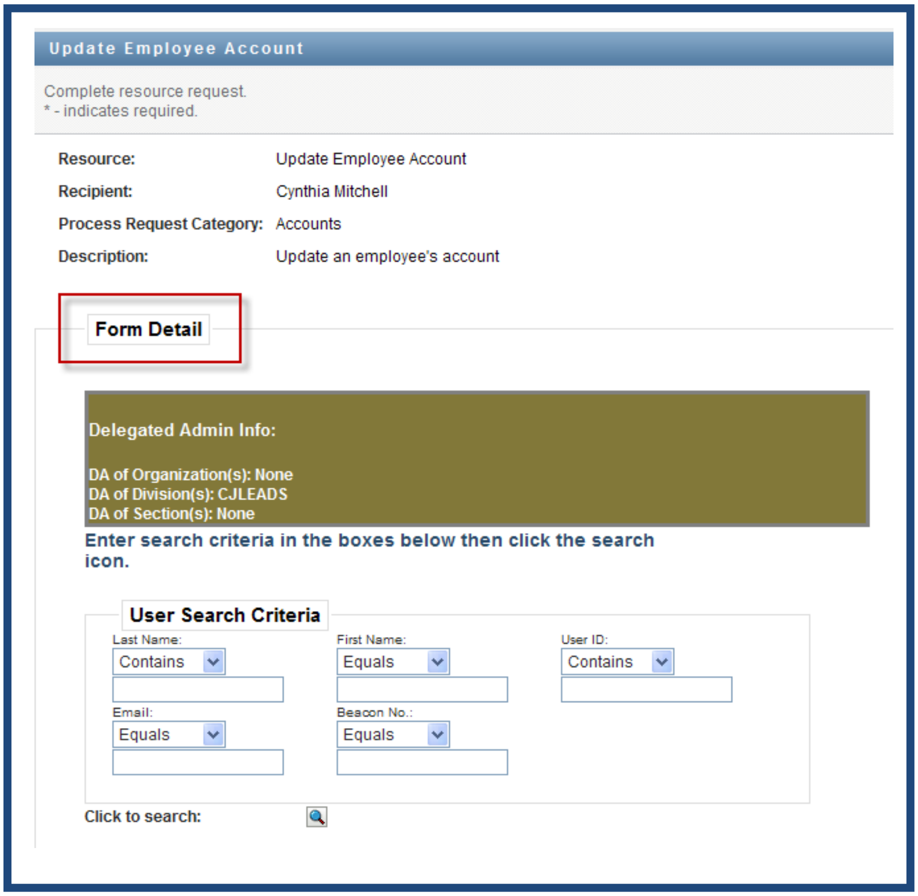
.



Searching for Users:

The Search feature is common across all process request forms. The Administrator will need to select the appropriate process request from the Identity Self-Service tab or Work Dashboard tab, and then look up the account by using the Search feature found on the form. The following figure illustrates an example of the “User Search Criteria” section displayed on the “Update Employee Account” request form.

1. Click **Update Employee Account** link in the Directory Management section.
   Form detail screen displays.

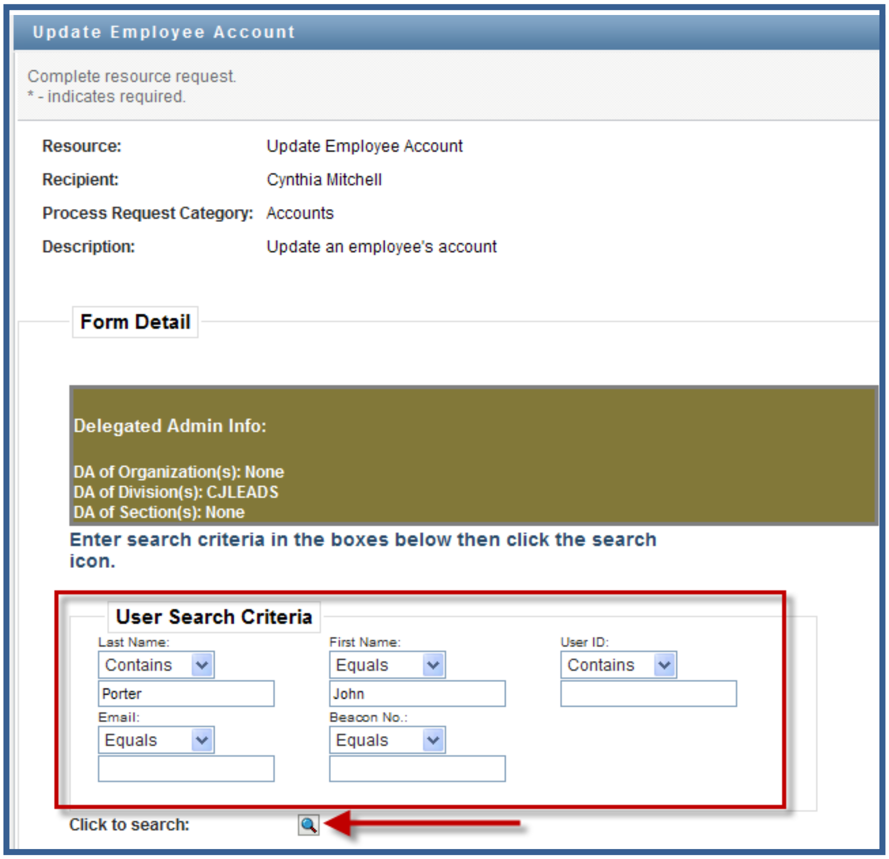


The **User Search Criteria** section provides five (5) user attribute fields to help you retrieve an account. You can search by one field or you can perform multiple field searches.

Last Name
First Name
User ID
Email
Beacon Number

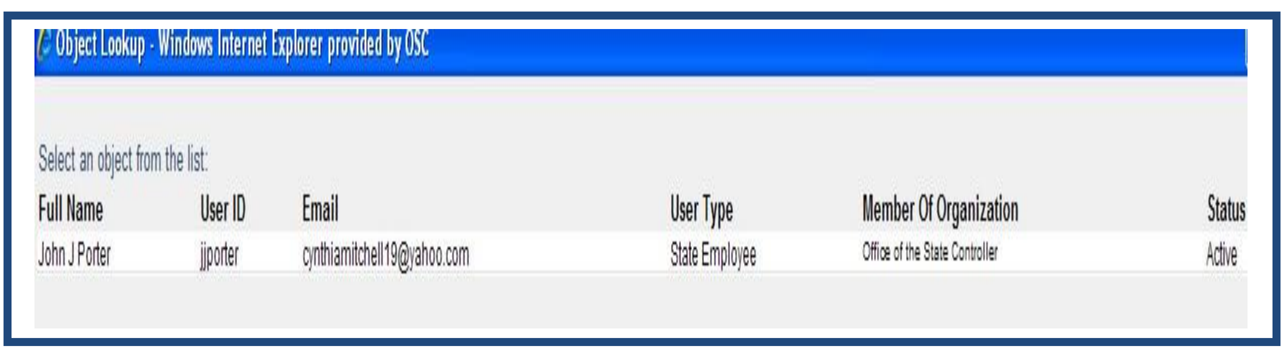
The dropdown menus provide four (4) characteristics to perform a match type.

Contains
Equals
Ends With
Starts With

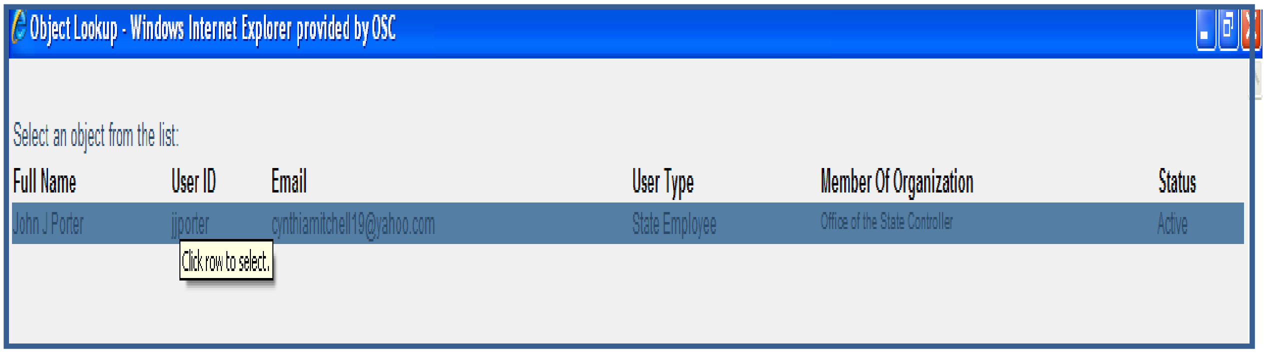


2. Type the user information to search for in the appropriate fields.

3. Select appropriate **match type** from dropdown menus.

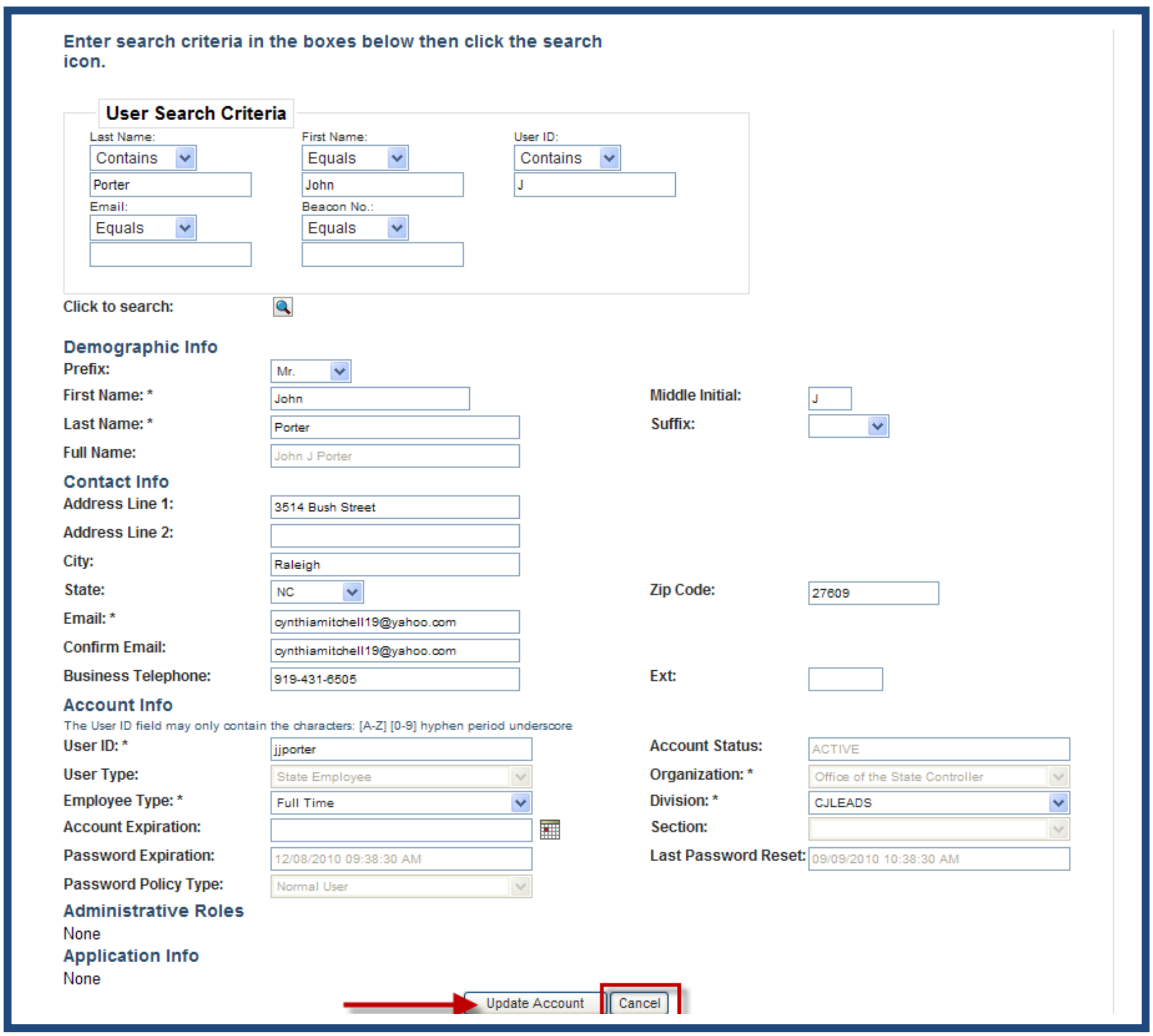


4. Click **Search.**
The *Object Lookup* results screen displays user account to update.



5. **Click** the selected user account.
   The *Form Details* screen displays with demographic information stored in the user"s profile

6. **View** or **Update** the user"s profile.



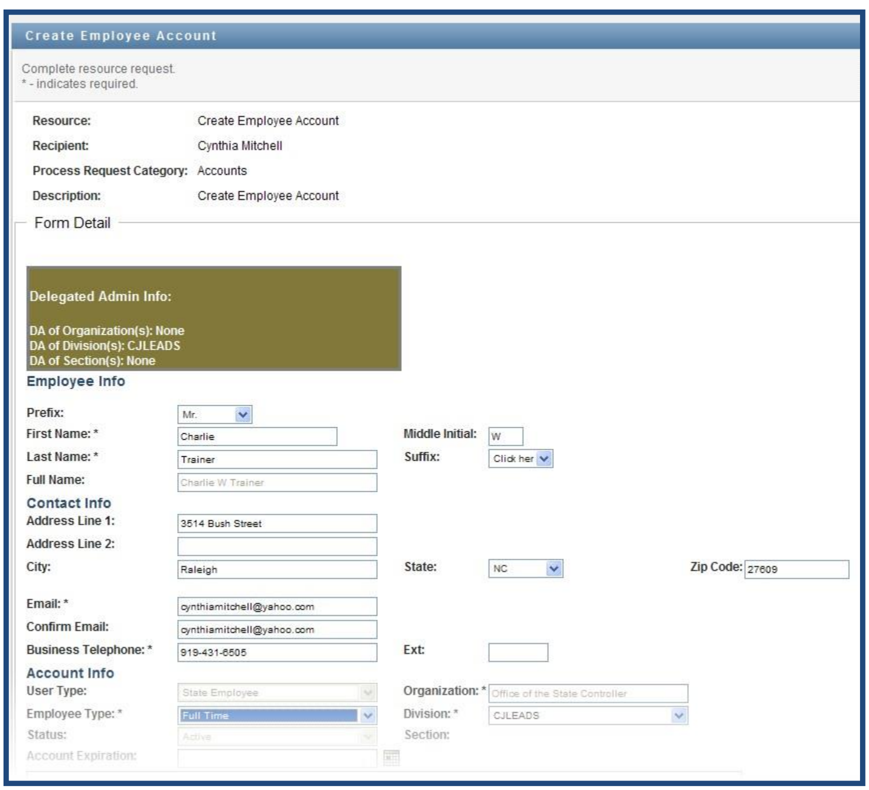
7. Click **Update Account** if modifying user demographic information or

8. Click **Cancel** to clear screen.

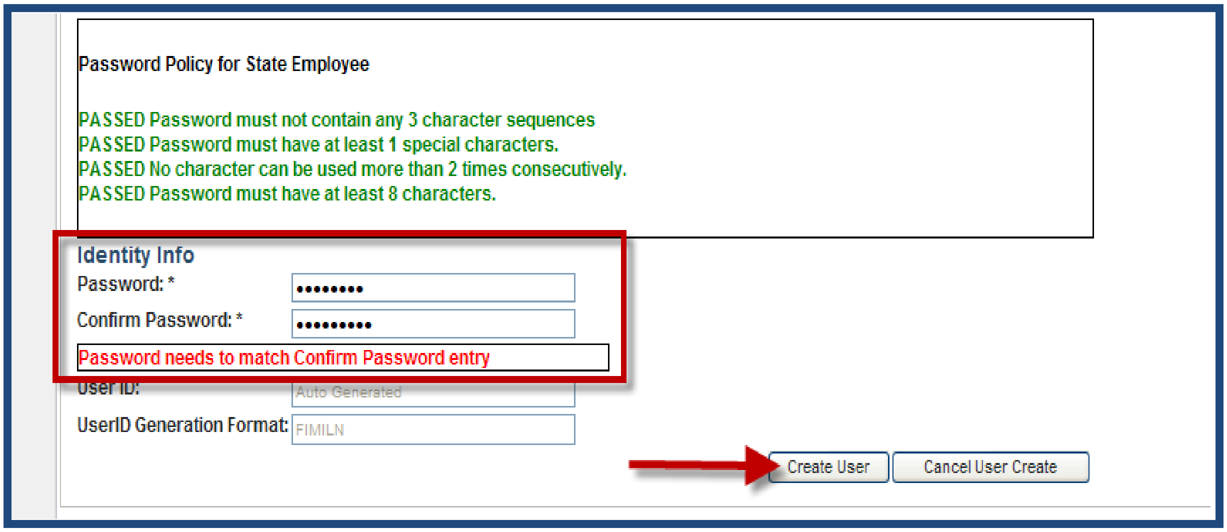
Creating New Accounts

Administrators are responsible for creating all new user accounts in NCID-NG.

1. Click Create **Employee Account** link in the **Directory Management** section.
   The Create Employee Account form displays.



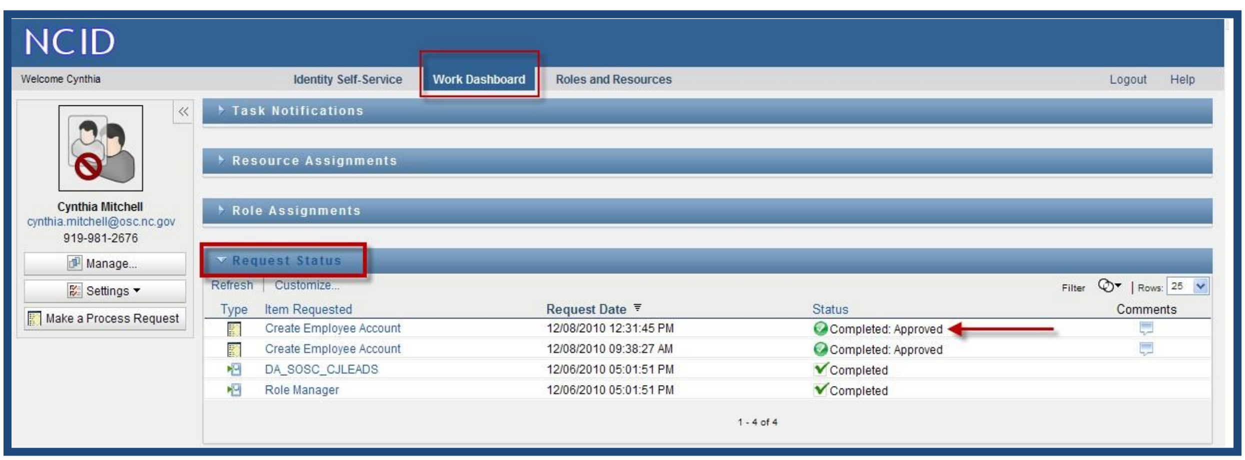
2. Fill in all of the required fields (marked with an *).



If password meets password policy criteria, password policy message will change from red to green.

3. Create one-time temporary password.

4. Click **Create User** to finish.



To confirm account creation status completed.

1. Click on **Work Dashboard**.

2. Click **Request Status**.
   The *Item Request* screen will display with account status listing as *Completed.*

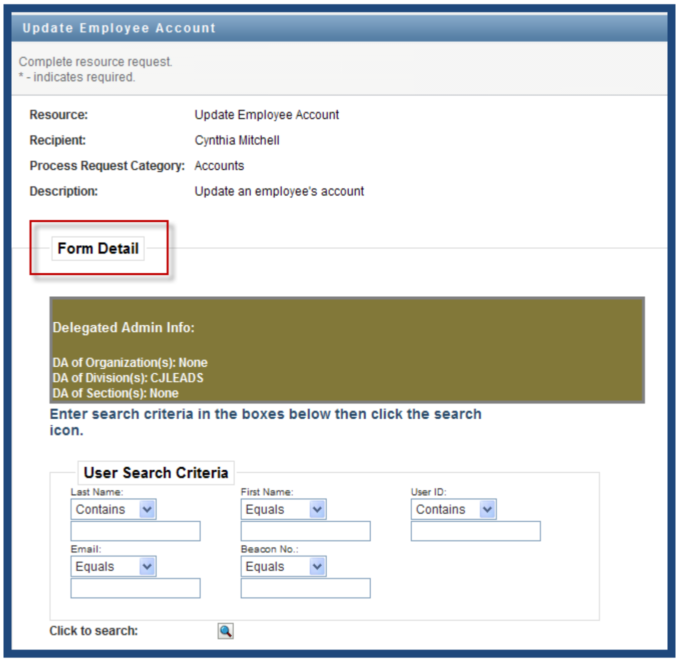
The administrator must notify user that account was created and provide one-time temporary password to login to NCID. The user must perform the following actions upon logging in NCID for the first time:

Change password
Set up challenge questions and responses
Log back into NCID.

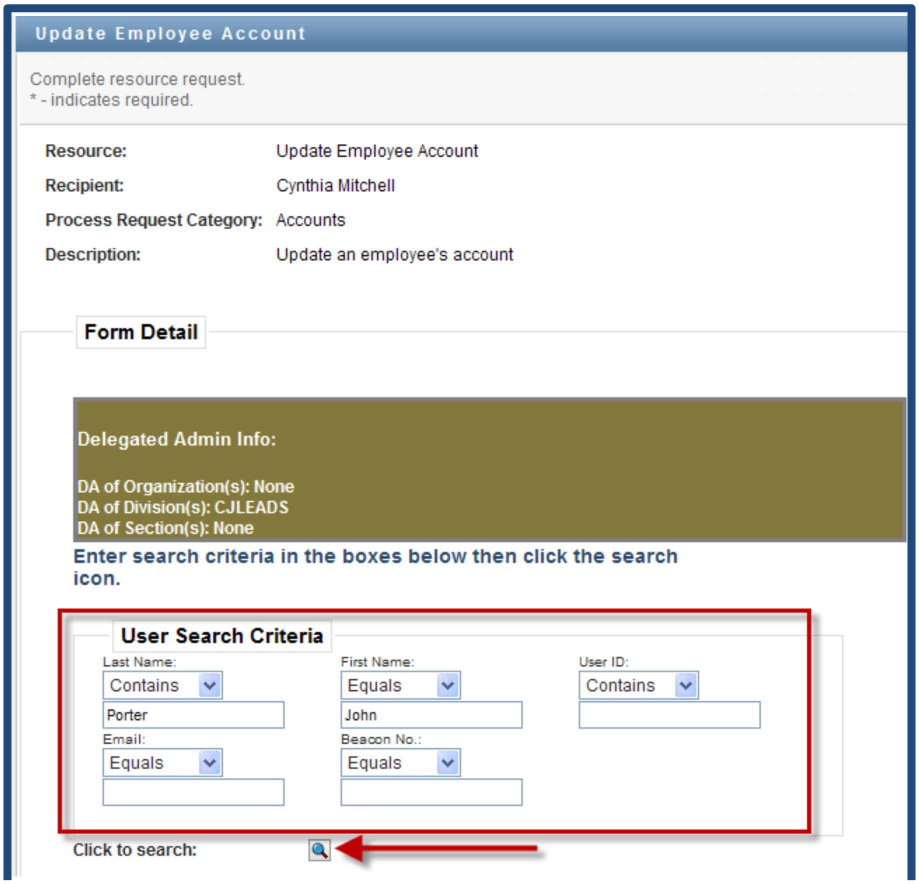
Updating Employee Accounts

The Updating Employee Accounts link is used to modify user account information. The Administrator will need to search for the account to be modified. Values which appear as read-only text may not be modified.

1. Click **Update Employee Account** link in the Directory Management section. *Form Detail screen* displays.



2. Type the user information to search for in the appropriate fields to retrieve account information.



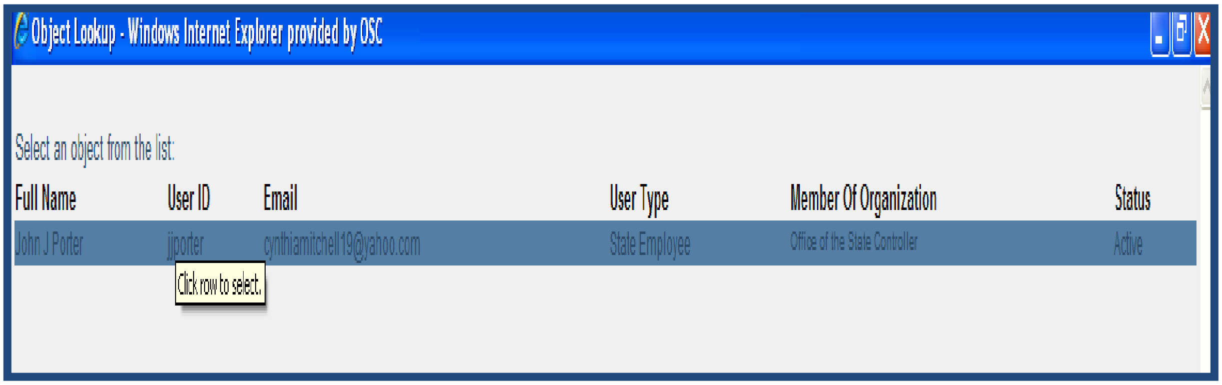
3. Select appropriate **match type** from dropdown menus.


Object Lookup - Windows Internet Explorer provided by OSC

Select an object from the list:

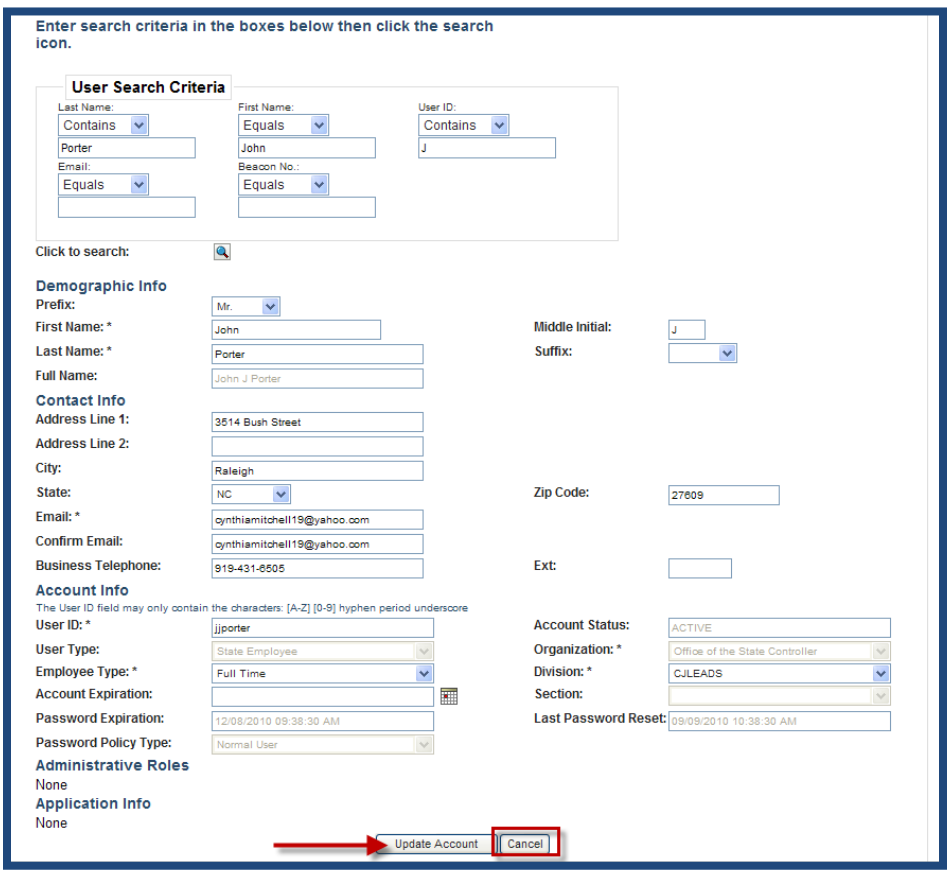
Full Name	User ID	Email	User Type	Member Of Organization	Status
John J Porter	jjporter	cynthiamitchell19@yahoo.com	State Employee	Office of the State Controller	Active

4. Click **Search**
   The *Object Lookup* results screen displays user to be updated.



5. **Click** the selected user account.
   The *Form Details* screen displays with demographic information stored in the user"s profile.

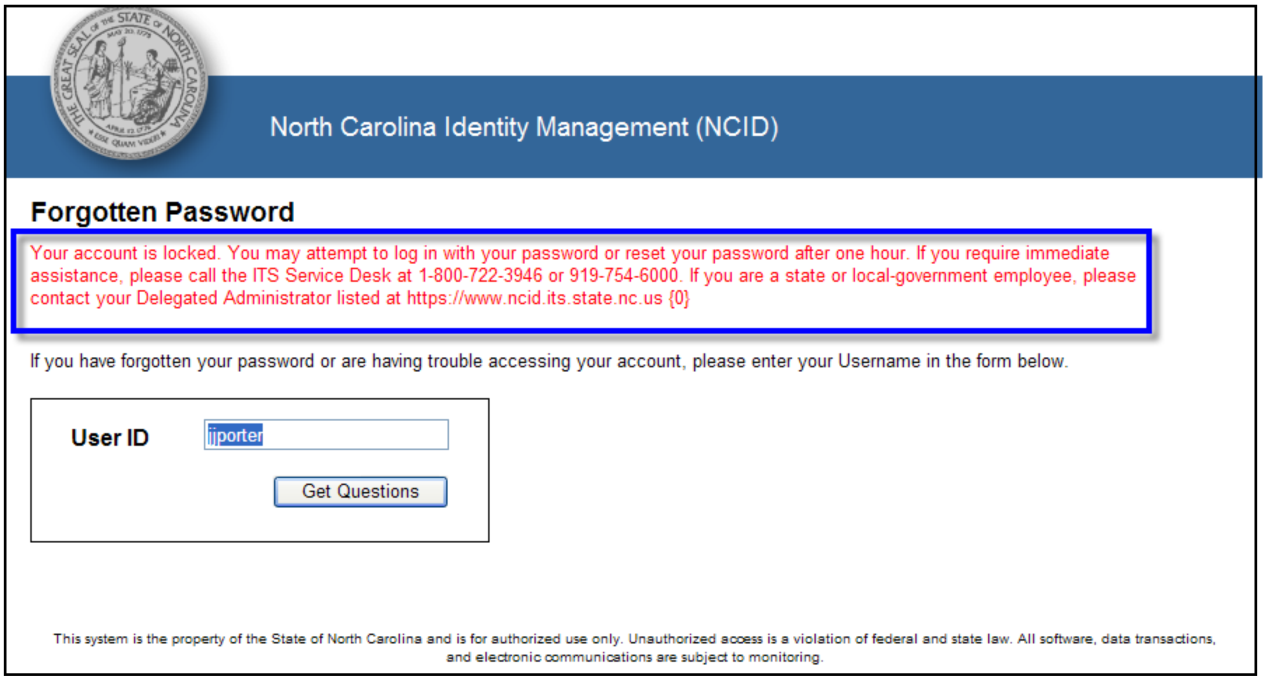
6. **View** or **Update** the user"s account profile.



7. Click **Update Account**
   The user"s account information has been updated.

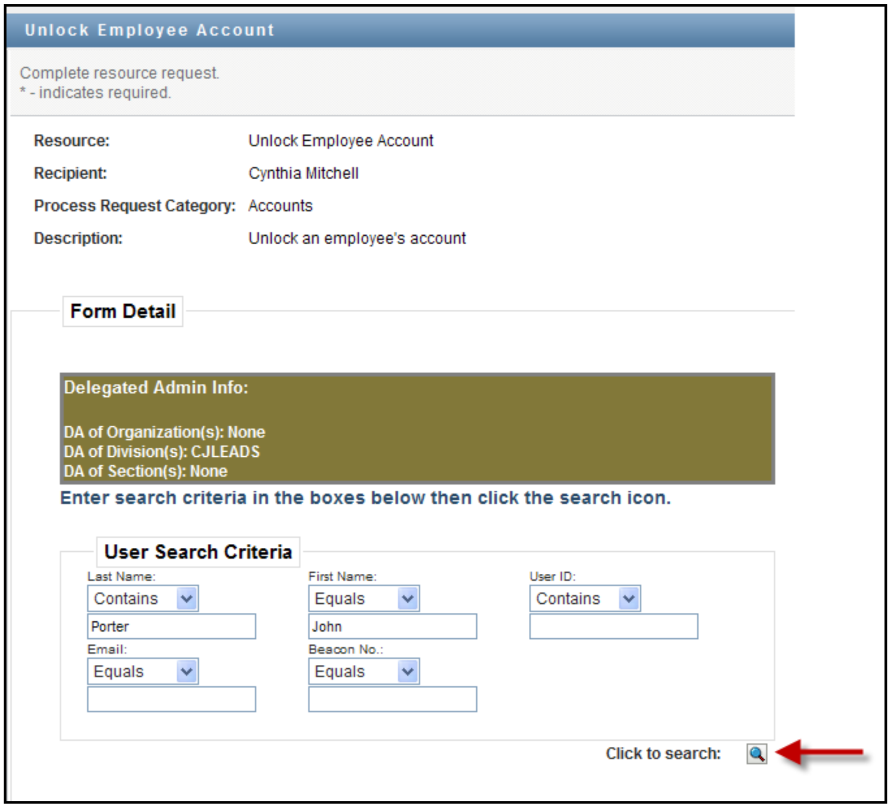
8. Click **Cancel** to clear screen.

Unlocking User Accounts

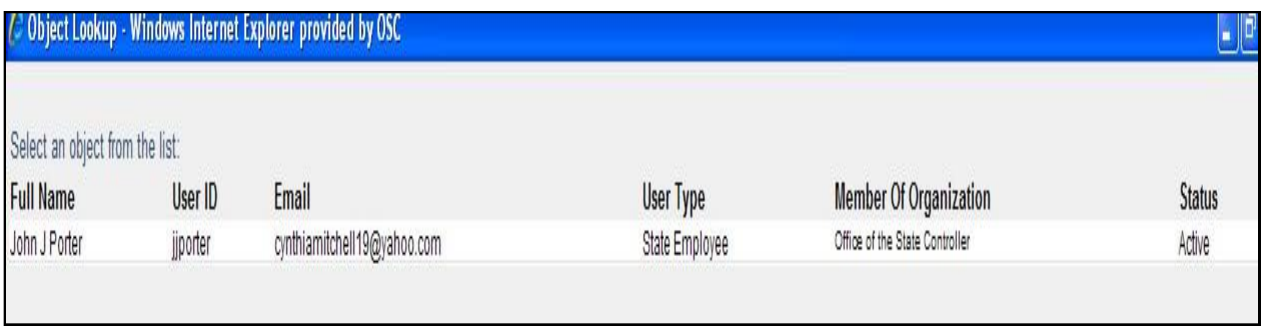


When a user attempts to access a NCID protected application and fails three (3) times in a row, the user"s account will be locked. The user account will automatically unlock after **one (1) hour** from the time it was locked. However, if the user requires immediate assistance, the administrator can manually unlock the account before the lockout period expires.

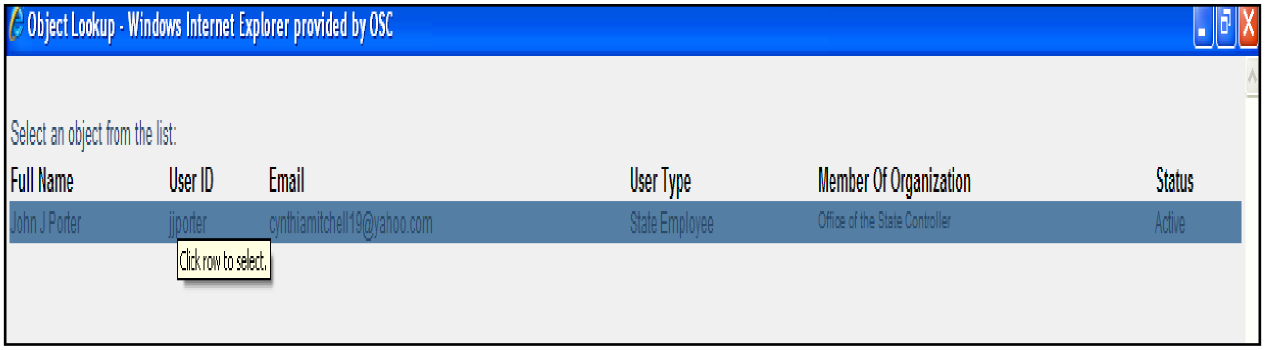
1. Click **Unlock Employee Account**.
   The *Unlock Employee Account* request form displays.



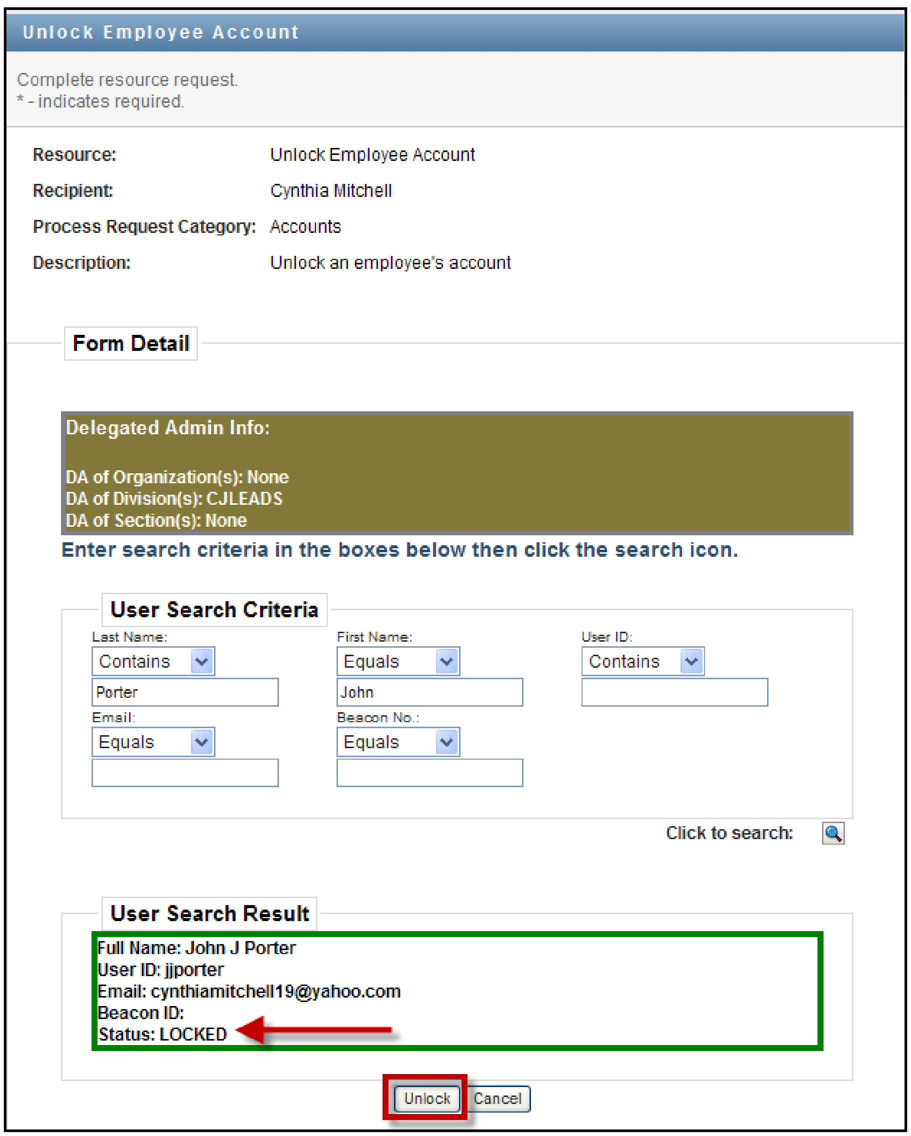
2. Select appropriate criteria to search for the user‟s account that needs to be unlocked.



3. Click **Search.**
The *Object Lookup* screen displays user account to be unlocked.



4. Select user account.
   Selected *User's Account Detail* form displays. Under *User Search Results* the status field should indicate user account as "**Locked**".



5. Click **Unlock**.
A *confirmation message* displays that your request was successful.

To track the status of request, view the request status list on the Work Dashboard.

Recovering a User ID

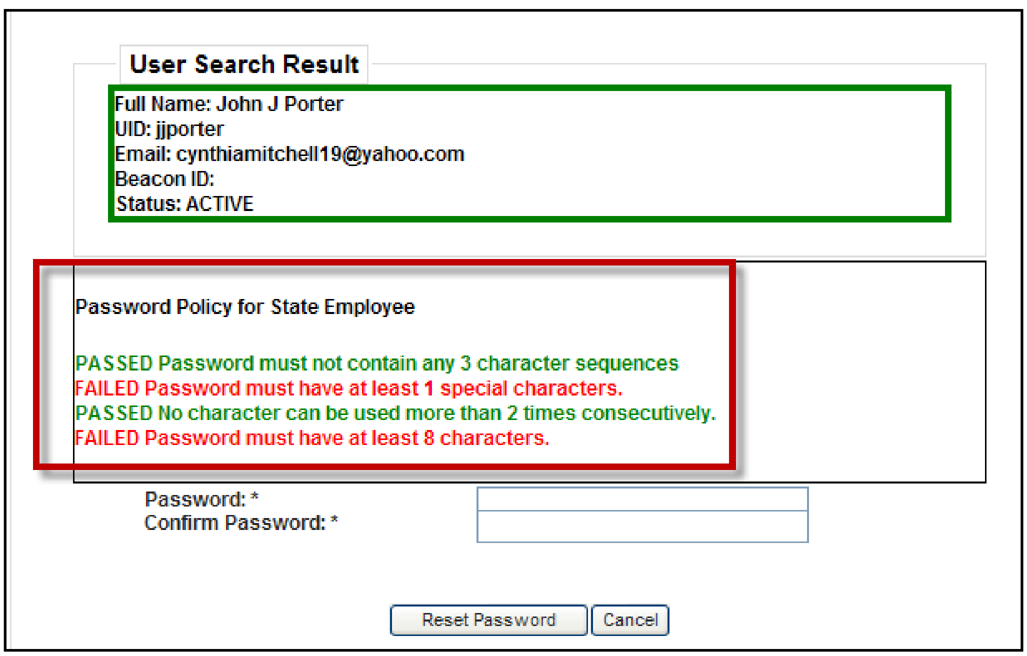
Occasionally users will need to recover their user ID. If a user cannot remember his or her user ID, then the administrator should direct the user to the **'Forgot Your User ID?**" link on the login page to perform a user ID recovery search. The Administrator can also recover the user ID by accessing the Update Employee Account link. Please refer to "Updating Employee Account" on page ( ) of this document.

The User ID displays in the User ID field in the Account Info section on the Update Employee Account form.

Resetting User Passwords

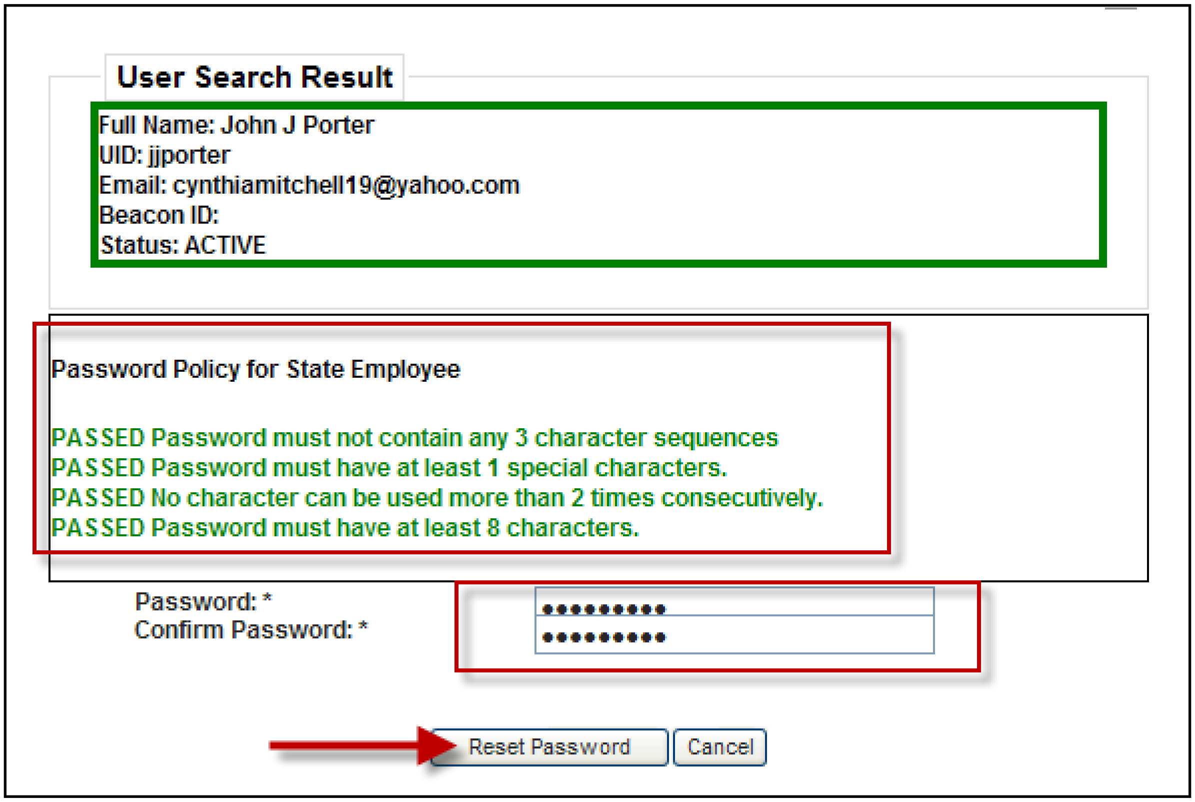
Occasionally users will need to have a password reset performed. Ensure that the user has attempted and failed to reset the password first using the „Forgot Your Password?" link on the login page. If the user is not able to answers the questions correctly, then an administrator will need to reset the user"s password. This feature is unavailable to employees who have recently changed their password (within 15 days), or if their account is locked

1. Click **Reset Employees' Password**.
   The *Reset Employee Password request* form displays.



2. Select appropriate criteria and search for the user account that needs to be reset.
   Selected user account details and *Password Policy Box* are displayed.

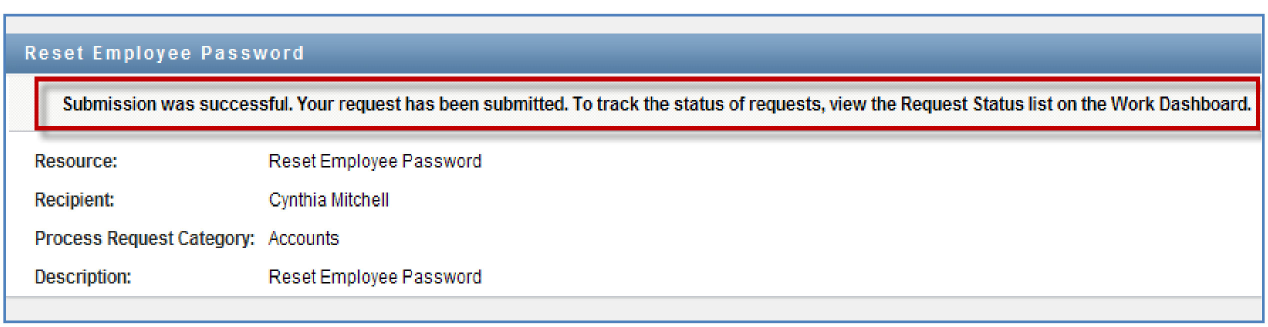
As you type the password, each requirement turns from red to green and the word "Passed" is displayed to indicate that the password meets the policy criteria.



3. Enter **temporary password** in Password field**.**

4. Re-enter **temporary password** in Confirm Password field.

5. Click **Reset Password.**
   A *confirmation message* displays that your request was successful.



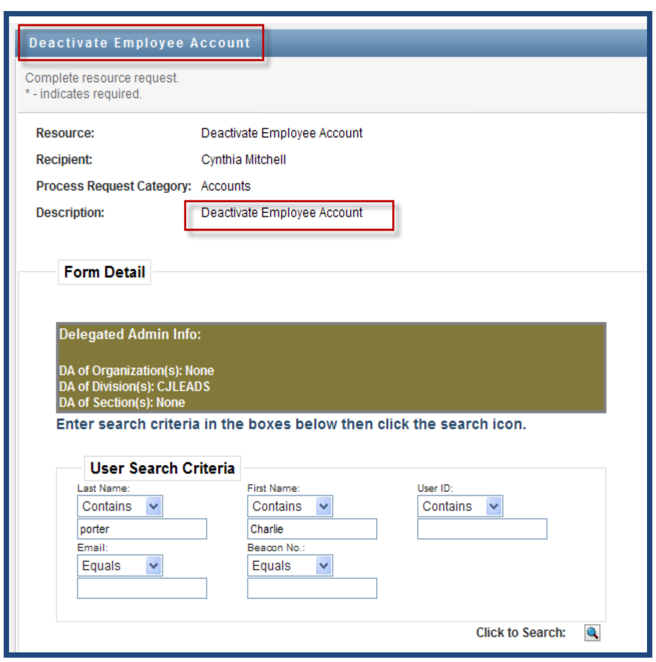
6. Contact the user via telephone with the new password.

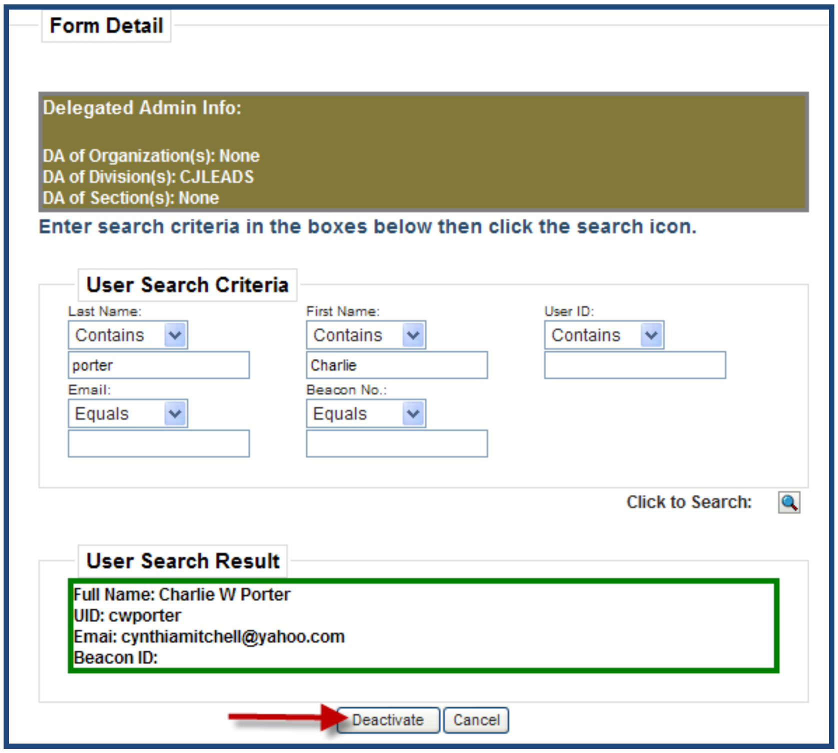
The user will need this password once to login to the NCID login page to reset their password.

Deactivating User Accounts

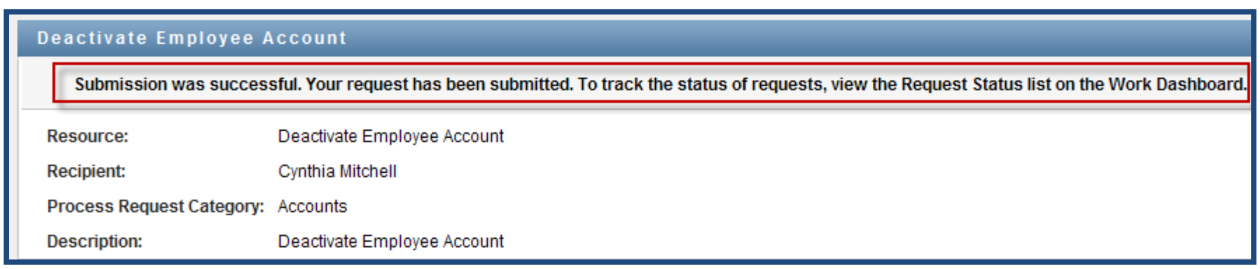
If a user is temporarily or permanently leaving an agency the user"s NCID account needs to be deactivated. Deactivation suspends the user"s rights or associations so that the user will be unable to log in to NCID-NG or any connected applications. The Administrator can deactivate a user account without deleting or removing the account completely from the system. Deactivated accounts can be reactivated if a user needs to regain access to NCID or any connected applications. A deactivated account may also be archived if the user permanently leaving the agency.

1. **Deactivate Employee Account**.
   The *Deactivate Employee Account* form displays.





2. Search for the user account using the steps outlined previously in this document.
   User's account profile displays.



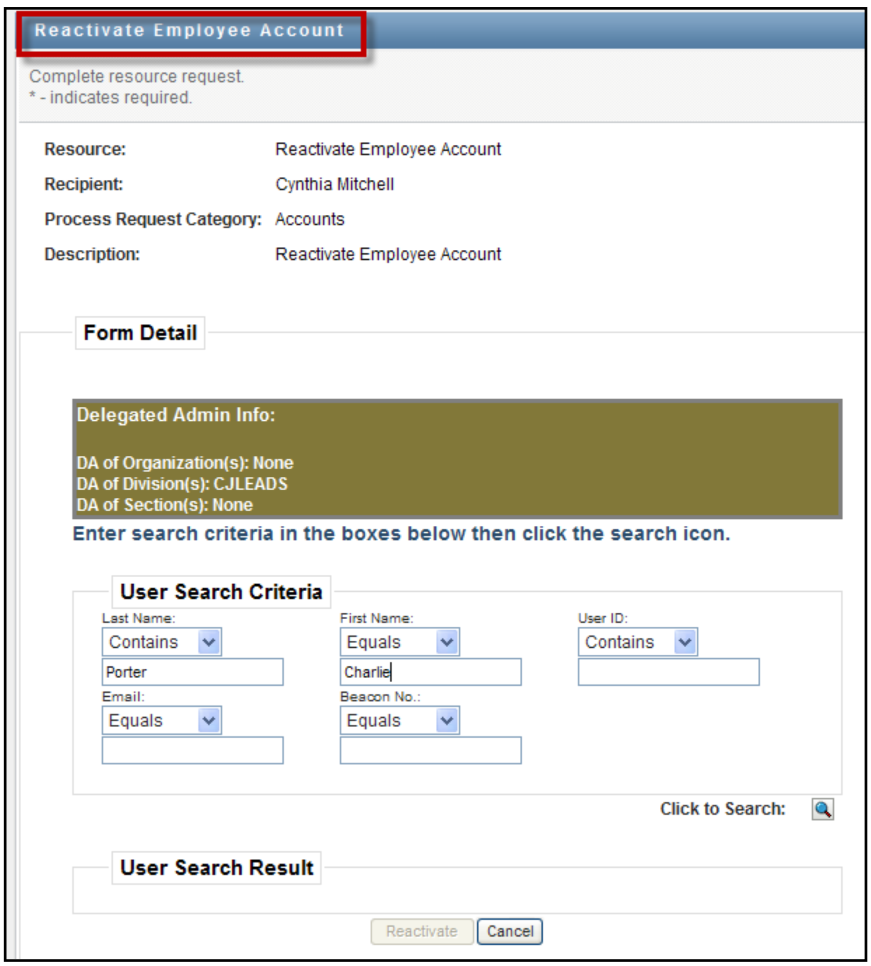
3. Click **Deactivate.**
   A *confirmation message* displays that your request was successful.

Reactivating User Accounts

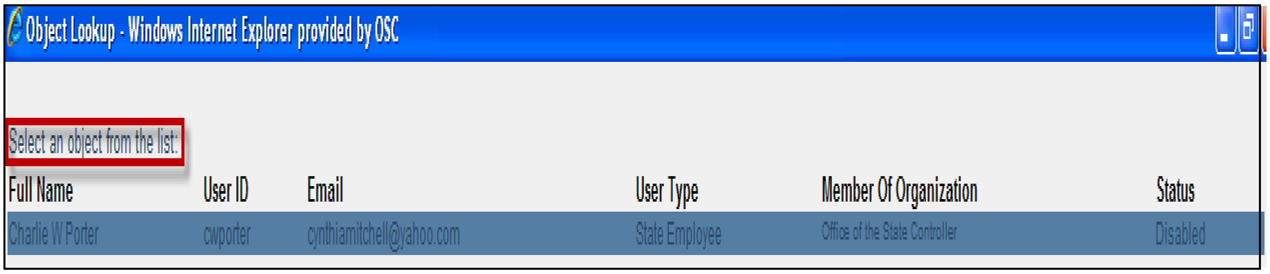
After a user account is deactivated, it is sometimes necessary to reactivate the account. For example, an account can be reactivated for an employee who returns to work after taking a temporary leave of absence. The steps listed below outline the reactivation process.

If a state employee contractor is reactivated, the system will automatically add 30 days from the current date as the new account expiration date. You may change this value in the user"s account by specifying a different date in the "Account Expiration" field.

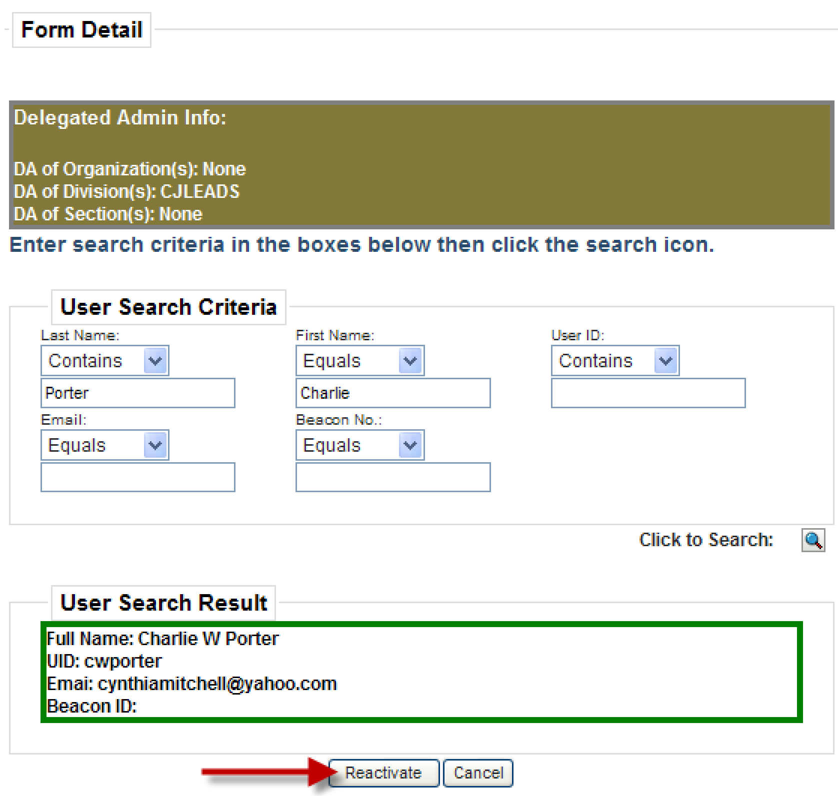
1. Click **Reactive Employee Account**.
   The *Reactivate Employee Account* form displays.



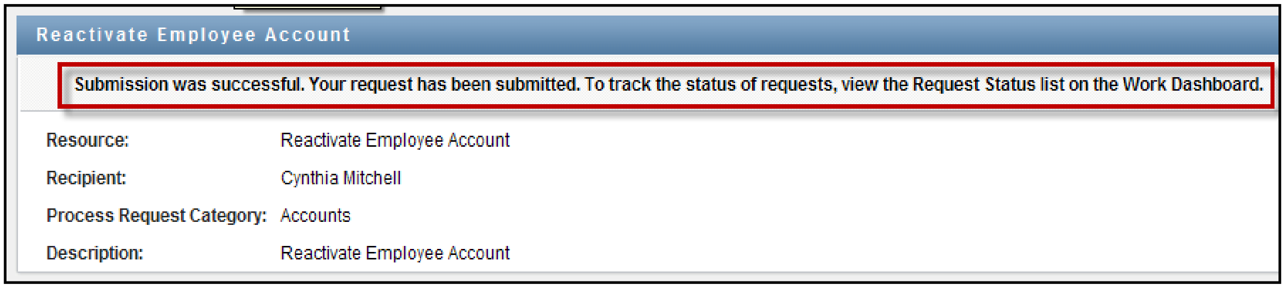
2. Search for the user account using the steps outlined previously in this document. The *Object Lookup* screen displays a list of *deactivated user accounts*.



3. Select user account to be reactivated.



4. Click **Reactivate**.
   A *confirmation message* displays that your request was successful.



The user account is now reactivated. Reactivated accounts should automatically be activated in the CJLEADS application. The CJLEADS User Administrator will now need to verify if the user account is activated and granted access in CJLEADS. If account is not granted access, the CJLEADS Administrator will need to grant user account access to the CJLEADS application.

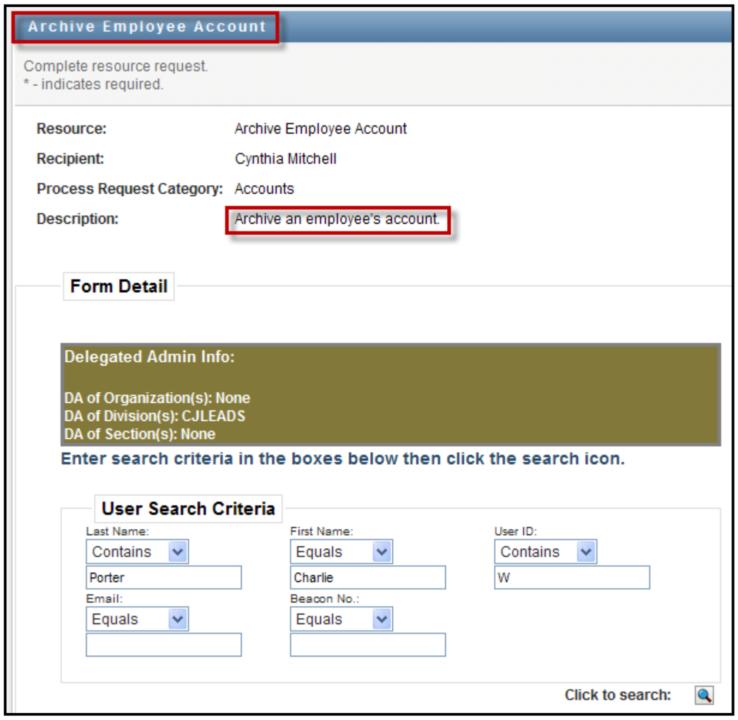
For information on how to restore and/or revoke CJLEADS access, please refer to the *CJLEADS User Administration* document.

Removing User Accounts

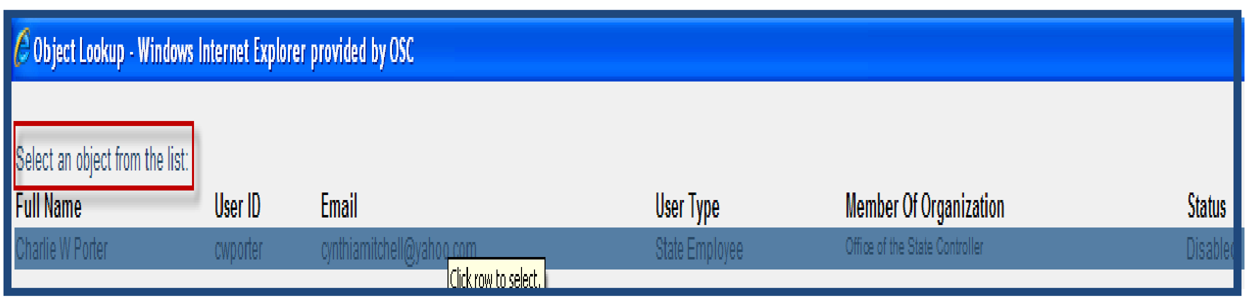
If a user is permanently leaving the agency, the NCID user account needs to be **deactivated** and **archived**. Refer to "Deactivating User Account" previously outlined in this document. Please note that once the account is archived it cannot be reinstated. If the user decides to return to the agency, it will be necessary for the Administrator to create a new account for the user to access NCID-NG and any connected resources again.

1. **Deactivate** user account.

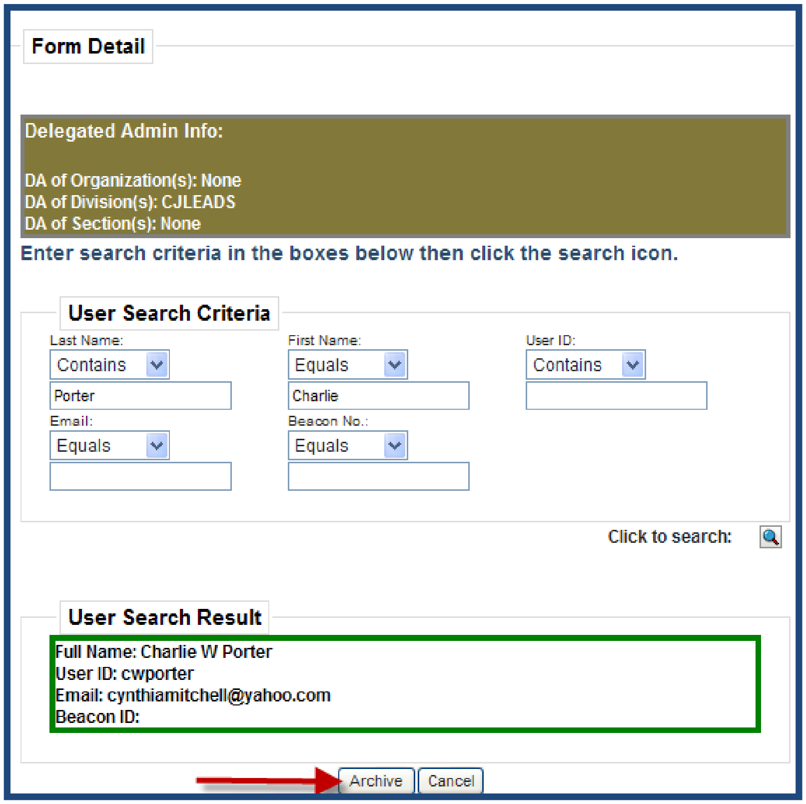
2. Click on **Archive Employee Account**.
   The *Archive Employee Account* form displays.



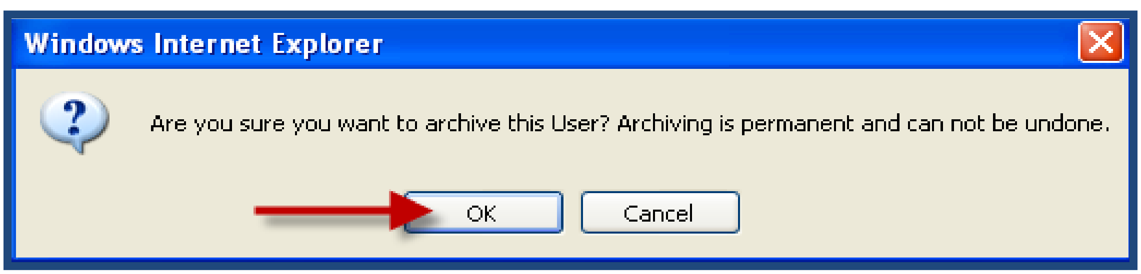
3. Search for the user account using the steps outlined previously in this document. The *Object Lookup* screen display list of users to be archived



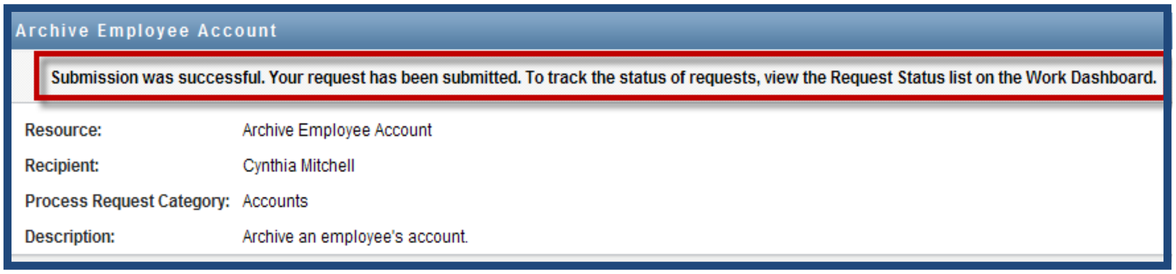
4. Select user account to be **archived**.



5. Click **Archive.**
   The system will ask for a confirmation



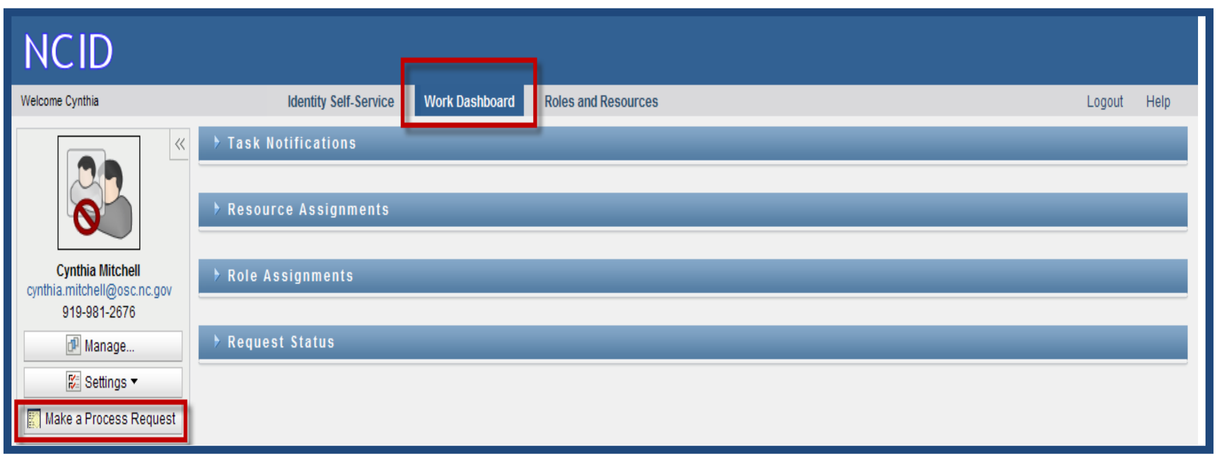
6. Click **Ok**.
   A *confirmation message* displays that your request was successful



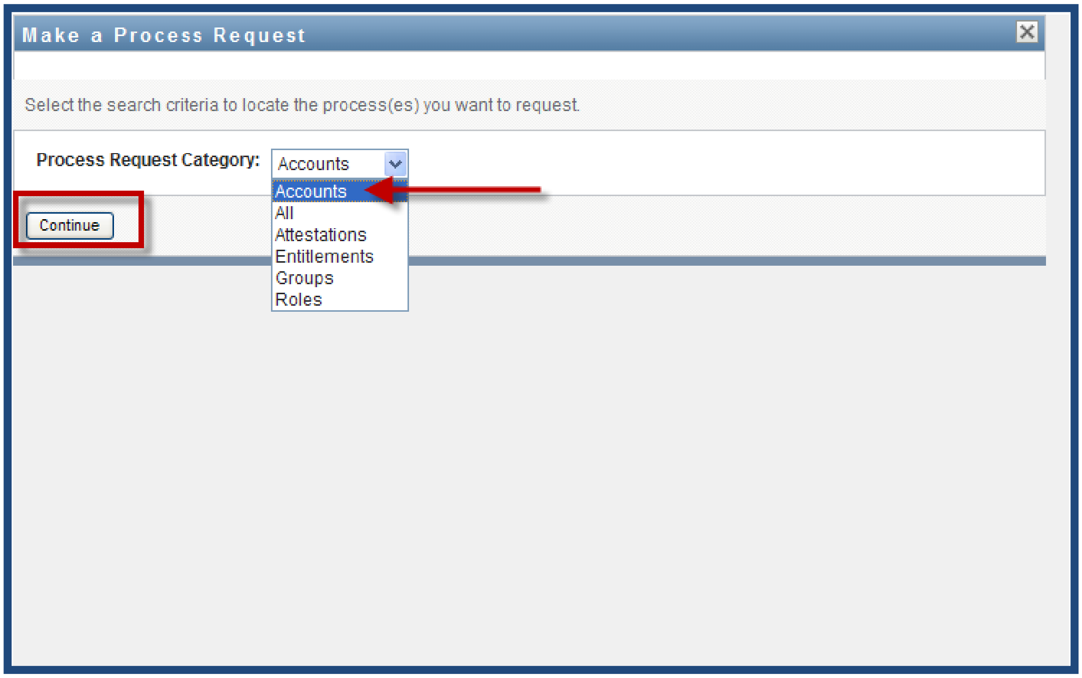
The user account is now archived. Archived user accounts should automatically be removed in the CJLEADS application. The CJLEADS User Administrator will now need to verify account is removed from the CJLEADS Utility Administrator tool.

Promote Delegated Administrator

It may be necessary to assign a user as an additional administrator to assist with managing agency user accounts or demote a user from that role. The Administrator can promote a user account to delegated administrator by assigning the appropriate administrative role.



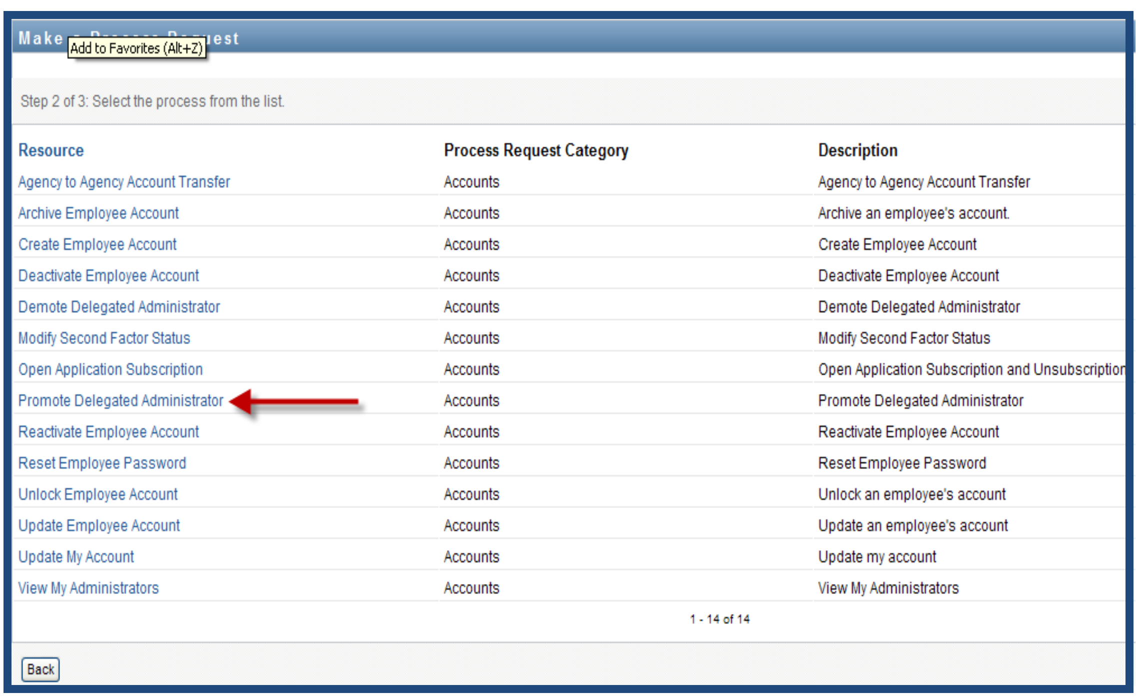
1. Click **Work Dashboard** tab.



2. Click **Make a Process Request**.

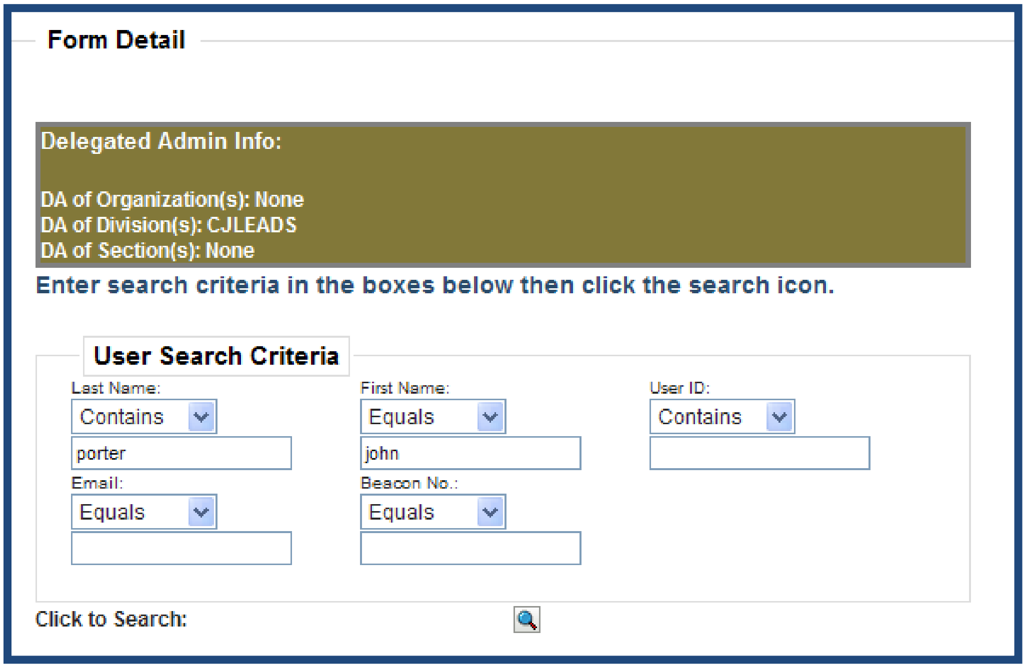
3. Click **Accounts** from the **Process Request Category** dropdown menu.

4. Click **Continue.**
   The *Make A Process Request* screen displays.



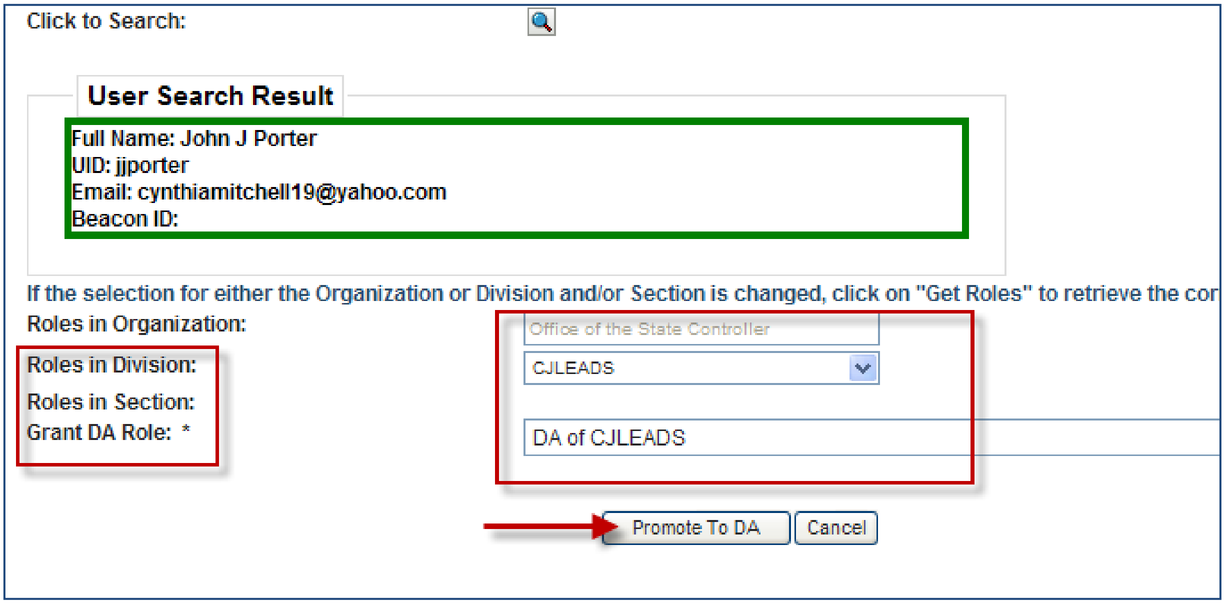
Resource	Process Request Category	Description
Agency to Agency Account Transfer	Accounts	Agency to Agency Account Transfer
Archive Employee Account	Accounts	Archive an employee's account.
Create Employee Account	Accounts	Create Employee Account
Deactivate Employee Account	Accounts	Deactivate Employee Account
Demote Delegated Administrator	Accounts	Demote Delegated Administrator
Modify Second Factor Status	Accounts	Modify Second Factor Status
Open Application Subscription	Accounts	Open Application Subscription and Unsubscription
Promote Delegated Administrator	Accounts	Promote Delegated Administrator
Reactivate Employee Account	Accounts	Reactivate Employee Account
Reset Employee Password	Accounts	Reset Employee Password
Unlock Employee Account	Accounts	Unlock an employee's account
Update Employee Account	Accounts	Update an employee's account
Update My Account	Accounts	Update my account
View My Administrators	Accounts	View My Administrators

5. Click **Promote Delegated Administrator**.
   Form Detail screen displays.



6. Search for and locate user.
   Object Lookup screen displays

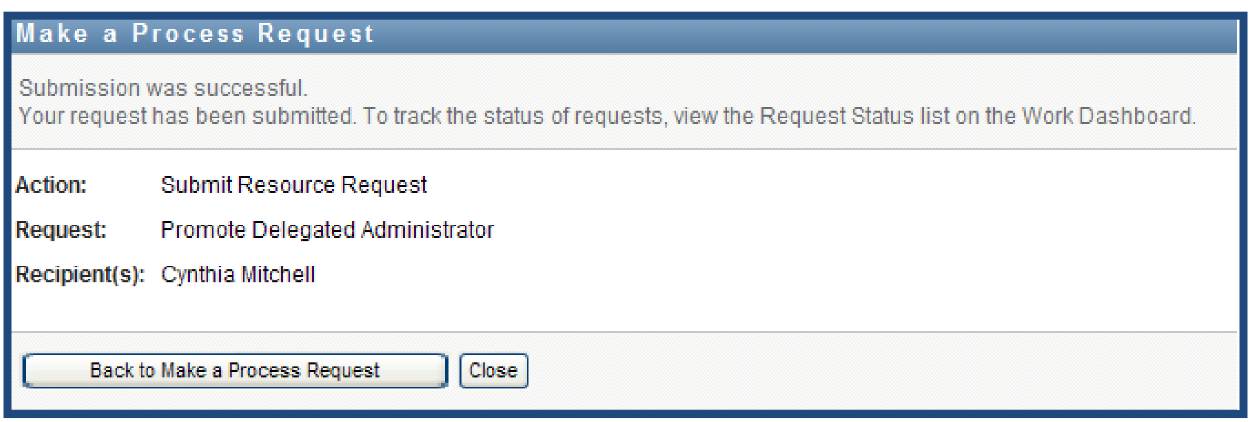
7. Select user account to be promoted.



Use the **Roles in Division** and **Roles in Section** dropdown menus to return a filtered list of DA roles specific to a division and section within your organization. Select the appropriate division and section (if applicable), and click on the **Get Roles** button.

The **Grant DA Role** or **Revoke DA Role** dropdown menus will display a list of DA roles associated to the division/section that you had selected. If you need to choose a different division/section, you must re-click the **Get Roles** button to obtain the roles associated with your new selection.

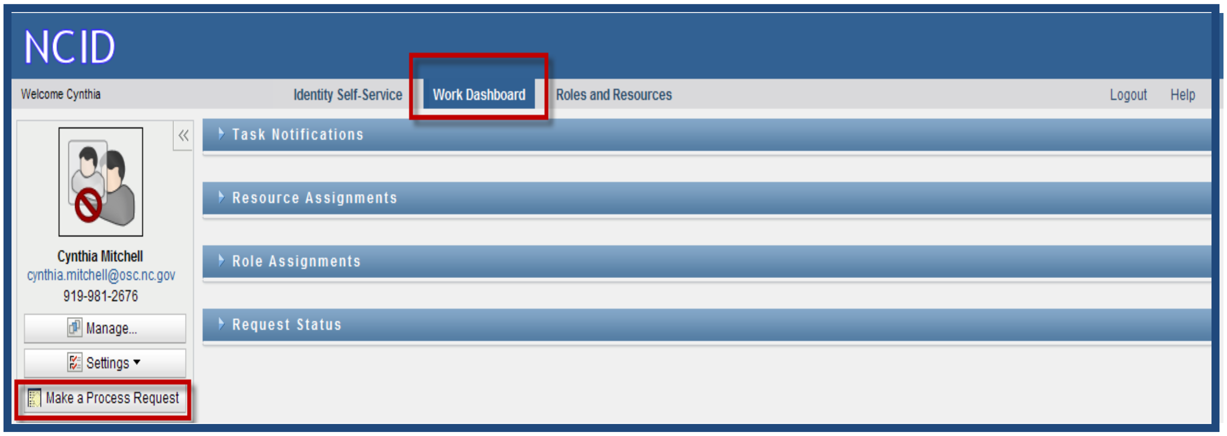
8. Click **Promote to DA** button to promote user.



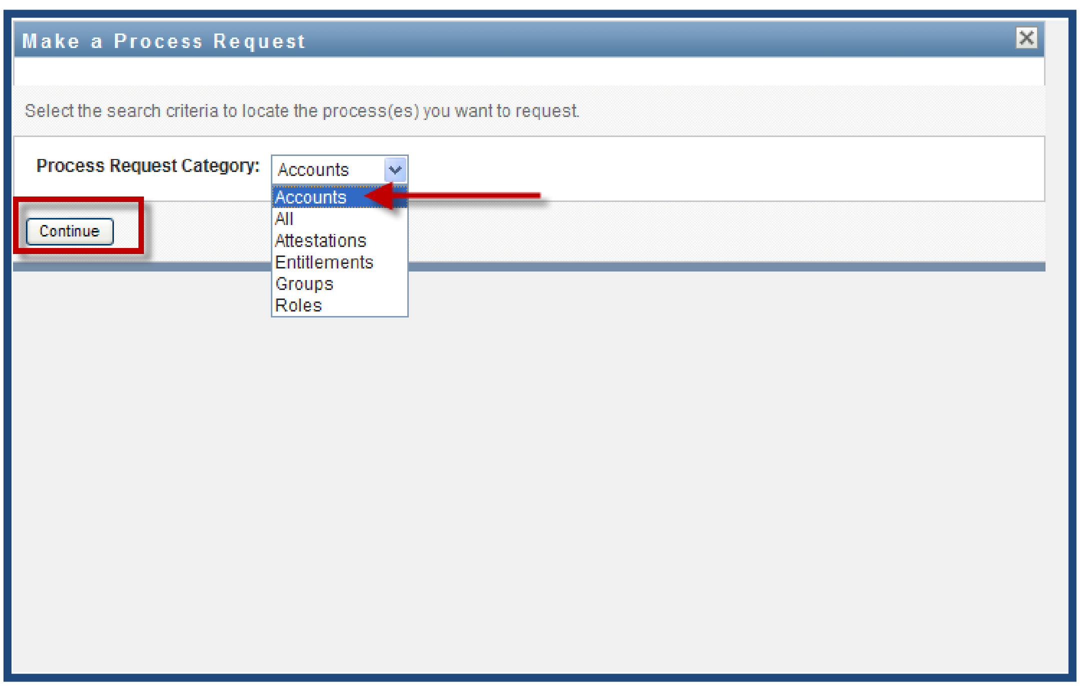
9. System confirms your request was successful.

Demote Delegated Administrator

If a user"s responsibilities change, administrator rights can be taken away by removing the administrator role(s) assigned to the user account.

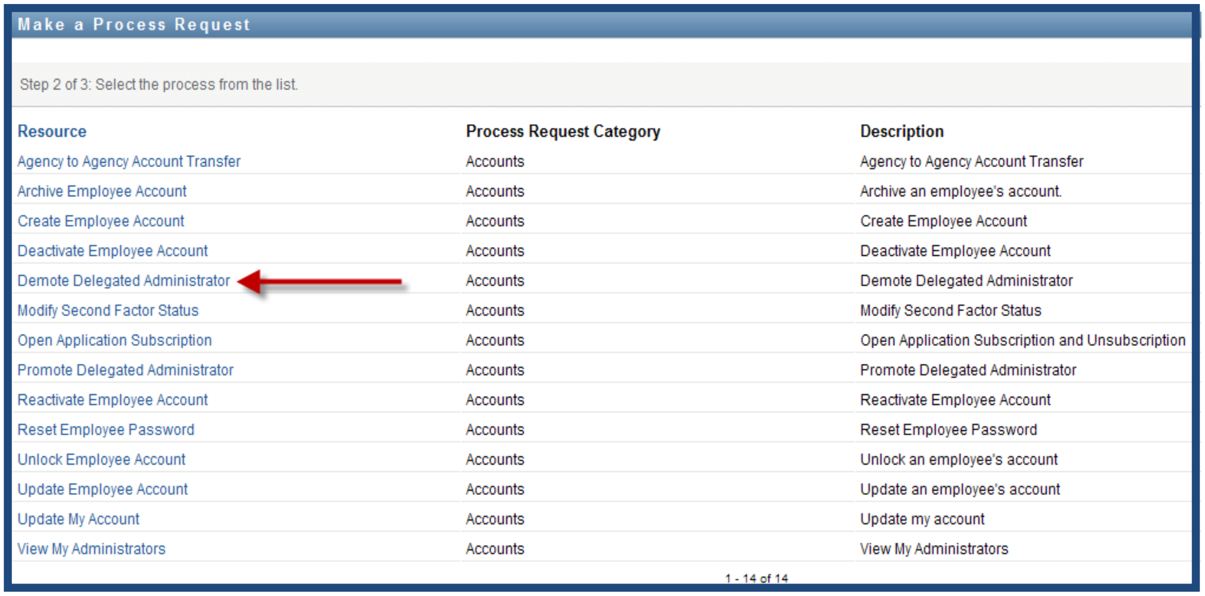


1. Click **Work Dashboard** tab.
2. Click **Make a Process Request**.



3. Click **Accounts** from the **Process Request Category** dropdown menu.

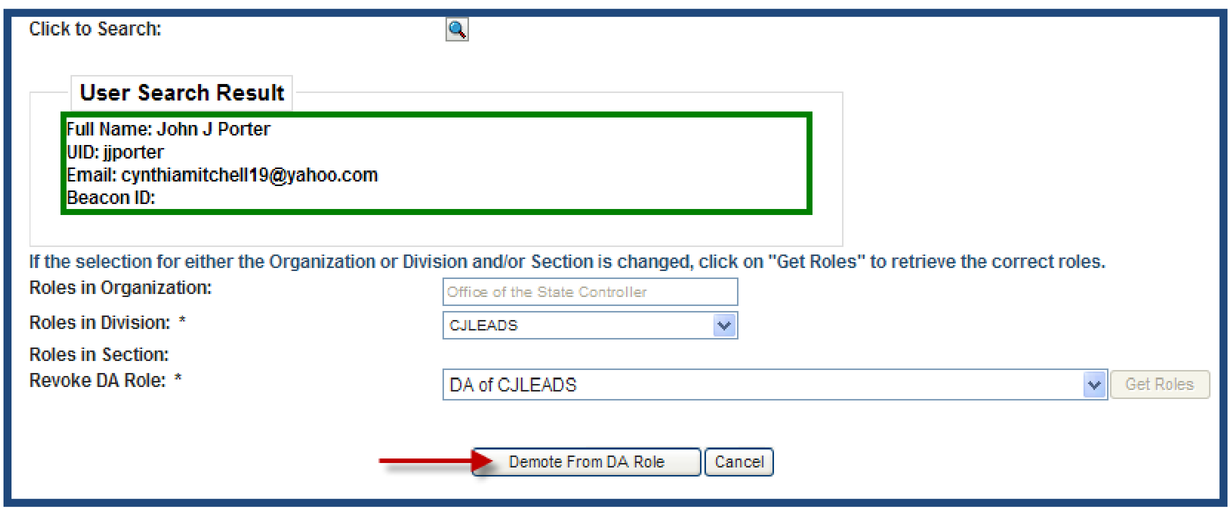
4. Click **Continue**.
   The *Make A Process Request* screen opens.


Make a Process Request

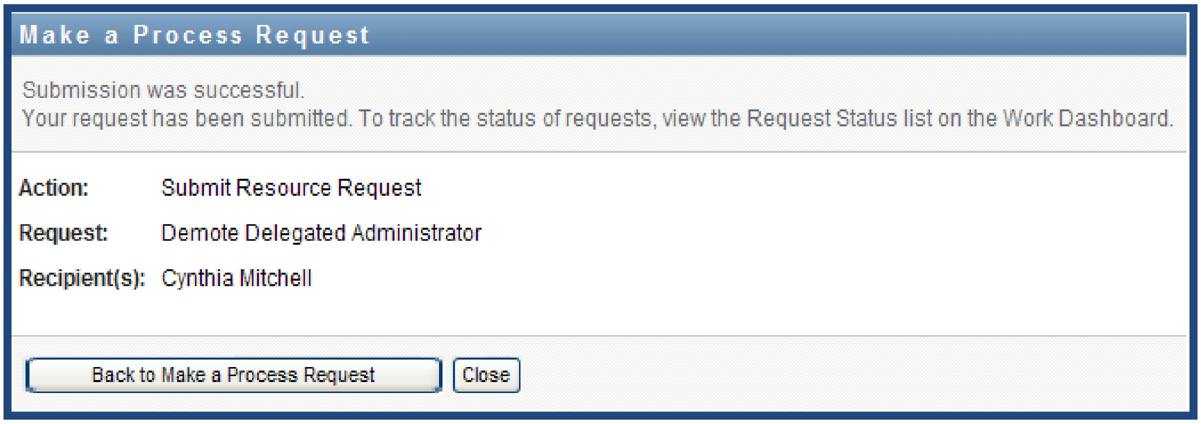
Step 2 of 3: Select the process from the list.

Resource	Process Request Category	Description
Agency to Agency Account Transfer	Accounts	Agency to Agency Account Transfer
Archive Employee Account	Accounts	Archive an employee's account.
Create Employee Account	Accounts	Create Employee Account
Deactivate Employee Account	Accounts	Deactivate Employee Account
Demote Delegated Administrator	Accounts	Demote Delegated Administrator
Modify Second Factor Status	Accounts	Modify Second Factor Status
Open Application Subscription	Accounts	Open Application Subscription and Unsubscription
Promote Delegated Administrator	Accounts	Promote Delegated Administrator
Reactivate Employee Account	Accounts	Reactivate Employee Account
Reset Employee Password	Accounts	Reset Employee Password
Unlock Employee Account	Accounts	Unlock an employee's account
Update Employee Account	Accounts	Update an employee's account
Update My Account	Accounts	Update my account
View My Administrators	Accounts	View My Administrators

1 - 14 of 14



5. Click **Demote Administrator**.
   Form Detail screen displays.

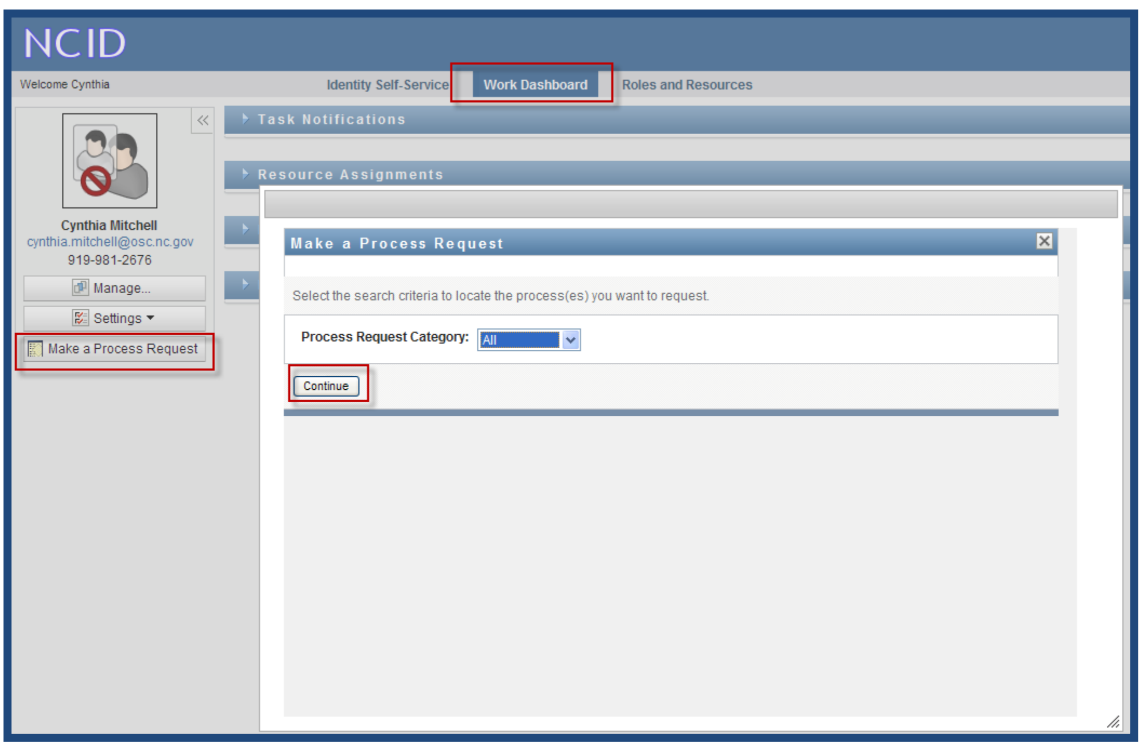


6. System confirms your request was successful.

Performing Agency to Agency Transfers

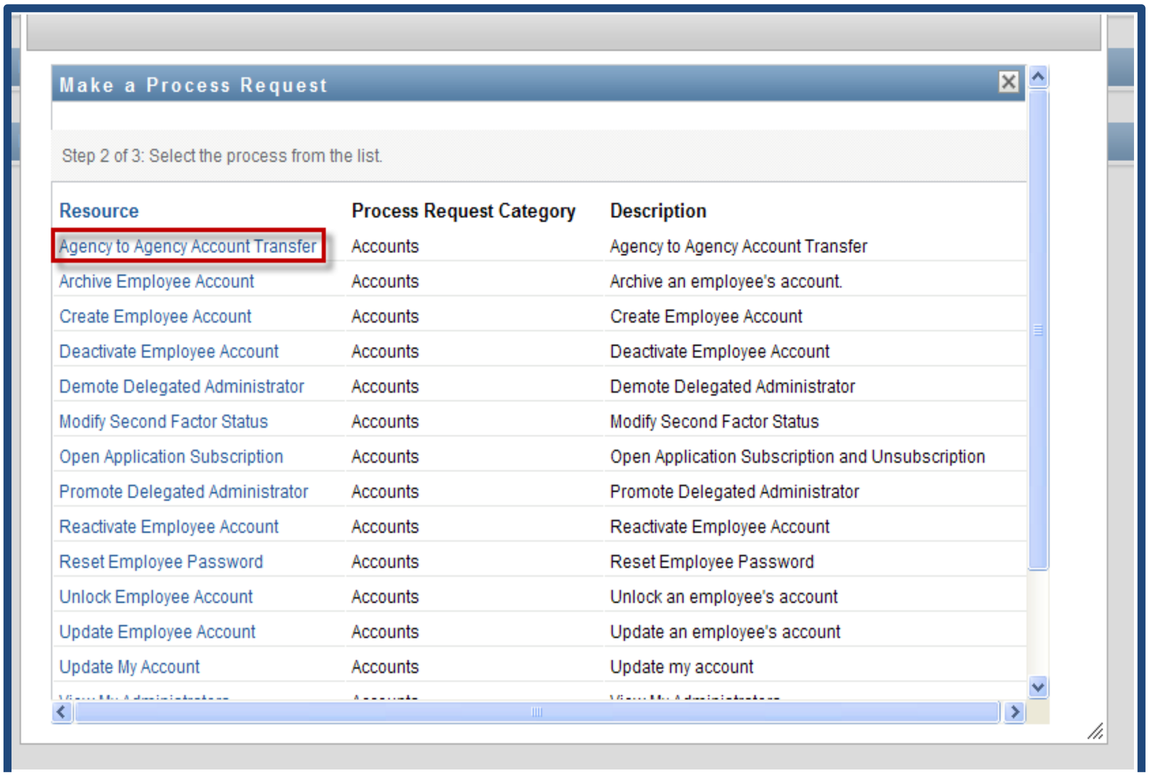
Performing an agency to agency transfer is a multi-step process that is performed by the employee‟s current administrator and the destination administrator. This process can only be performed with state employees transferring to another state agency. The agency to agency transfer cannot be performed with employees transferring between local government agencies.

Phase 1 is performed by the current administrator:



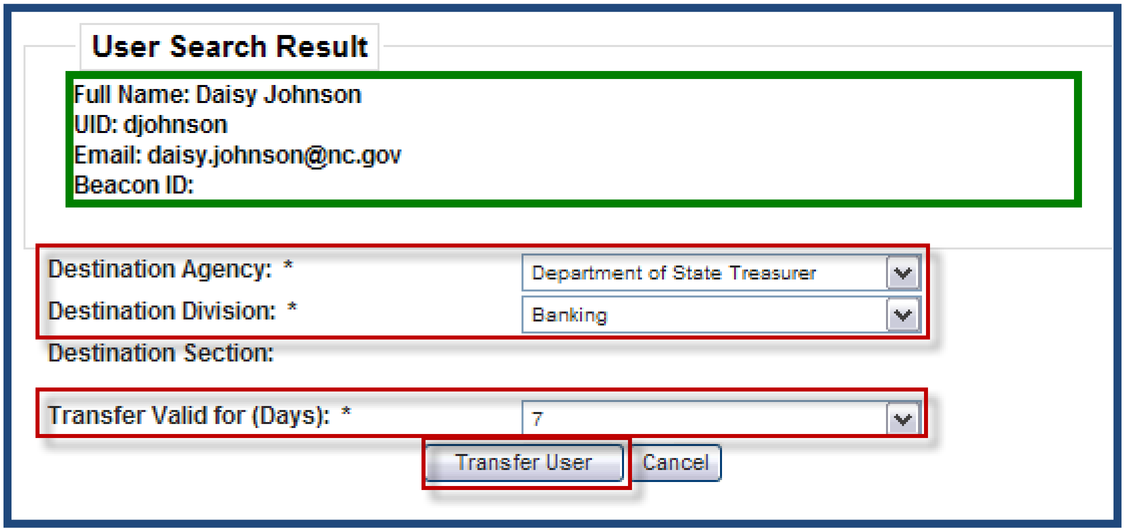
1. On the **Work Dashboard** tab, click on the **Make a Process Request** button.

2. Click **Continue** to view a list of workflow processes and select **Agency to Agency Account Transfer**.



3. The **Agency to Agency Account Transfer** request form is displayed.

4. Search for the employee you wish to transfer.

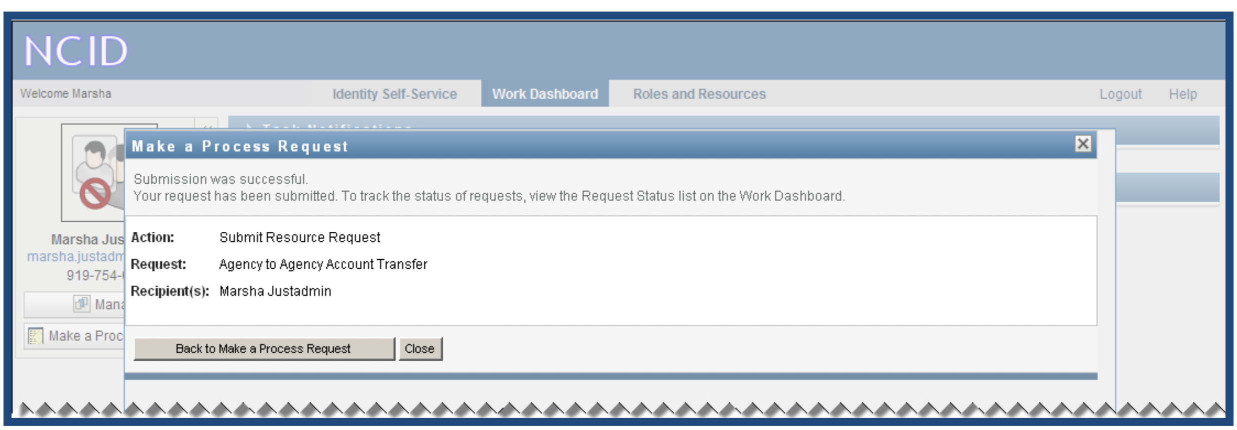


5. Select the agency, division (and section, if applicable) to which the user is transferring from the **Destination Agency**, **Destination Division**, and **Destination Section** dropdown menus. (The **Destination Section** menu is visible only if the user is moving to a division that has one or more sections.)

6. In the **Transfer Validate for (Days)** field, select the length of time required for the destination administrator approve the transfer.

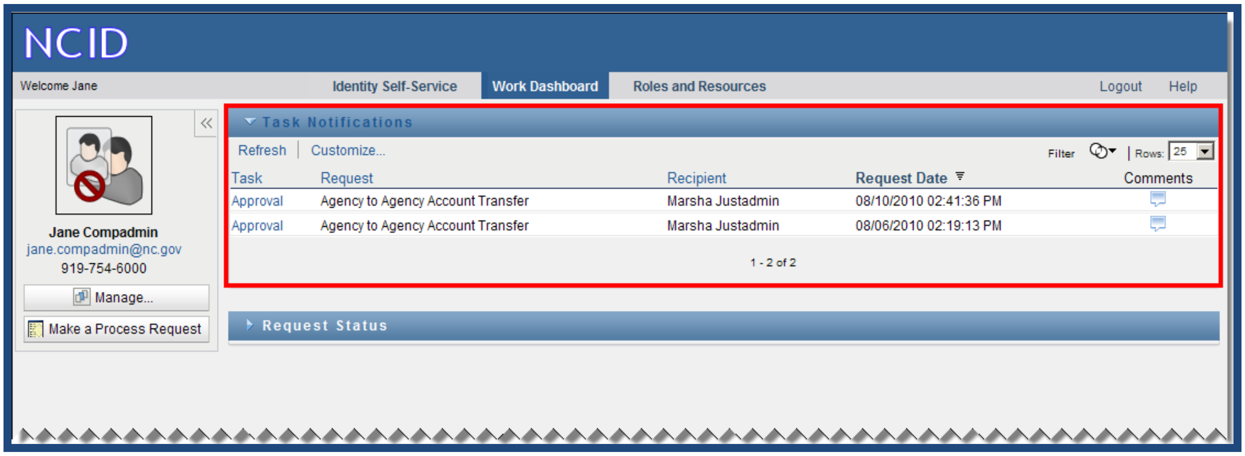
7. Click the **Transfer User** button.

If the request not approved within the specified time period, it will expire and the account will remain in the current agency. You will receive an email notification if the request expires.

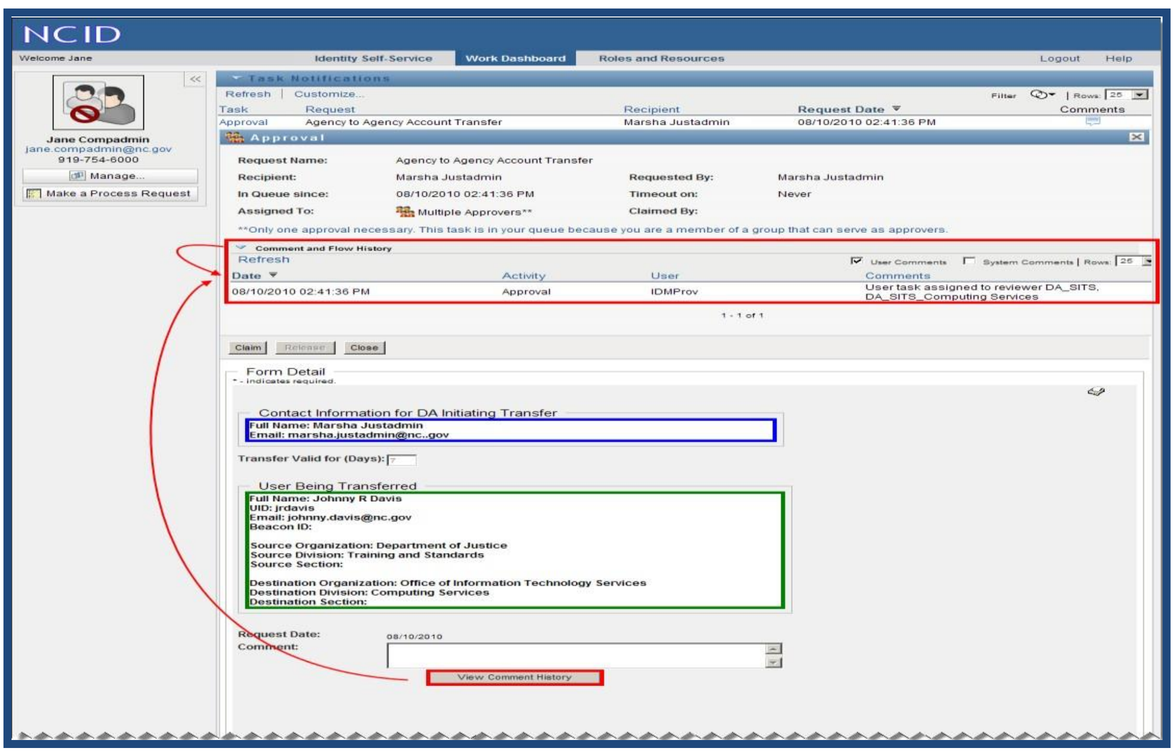


Phase 2 is performed by the destination administrator:

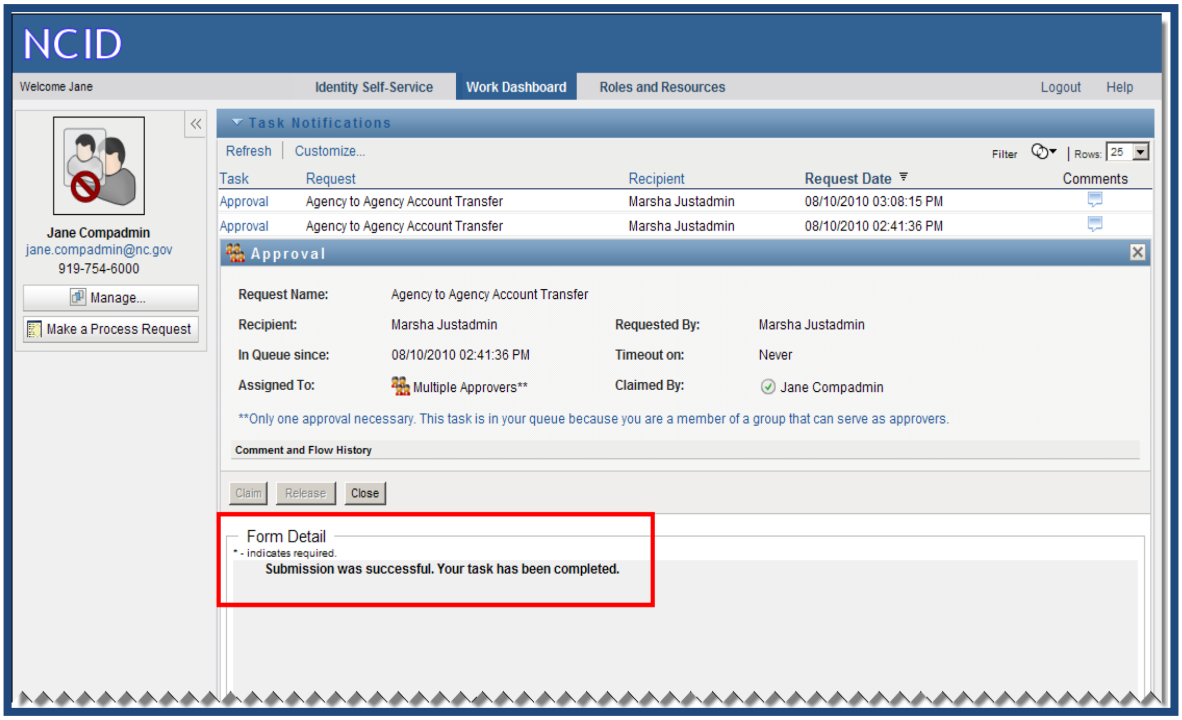
When a transfer request is submitted, the receiving administrator will receive an email notification of the employee's pending move.



1. Access the transfer request on the Work Dashboard tab.
2. Click on the icon in front of **Task Notifications**. A list of tasks is displayed.
3. Click the **Approval** button on the appropriate task to expand the line item and view details.
4. Click the **Claim** button.



If there are multiple DAs in the destination division you must first claim the task. The claim button alerts other approvers that you are granting the approval. After claiming the task, two additional action buttons are available at the bottom of the window: **Deny** and **Approve**.



5. Click the **Approve** button to complete the transfer process. (Or you can cancel a request by clicking **Deny** . The employee"s current administrator will receive an email notification, and the transfer is cancelled.

If you need additional assistance with performing an agency to agency transfer, please contact CJLEADS User Administration at 919-707-6949 or email cjleadshelp@nc.gov.

Some information in this document was taken directly from the NCI D A dmi nist rat or"s Guide document which is maintained by the North Carolina Office of Information Technology Services.