NCID
Administration Guide

Version 2.12

Department of Information Technology
As of July 14, 2016

Document History

Version	Change Reference	Date	Author
1.0	Initial draft release	5/11/10	Heather Ferrie
1.1	Updated TOC with comments from Brent Roberts	5/12/10	Heather Ferrie
1.2	Updated with comments from Brian Austin and Brent Roberts	6/1/10	Heather Ferrie
1.3	Inserted a new section (1.2 Documentation Organization) and included links to the various sections. Separated the guide into four parts: Part 1: NCID Fundamentals Part 2: Delegated Administrator Functions Part 3: Application Administrator Functions Part 4: Appendixes Inserted a new page at the beginning of each Part to highlight the subsequent sections. Removed “Creating an Acct for State/Local Account” from section 5 into new section 6.	6/23/10	Heather Ferrie
1.4	Updated with team’s comments	6/29/10	Heather Ferrie
1.5	Inserted index, page number references, final edits, updated Transfer, DA Promote/Demote, AA Promote/Demote steps, updated Appendix B w/KB comments	7/9/10	Heather Ferrie
1.6	Updated: Search, Transfer, Promote/Demote DA, Promote/Demote AA, Making Resource Assignments, Appendix B & C, all hyperlinks, screenshots; Added: View My Admin	8/13/10	Heather Ferrie
1.6	Updated Index	8/16/10	Heather Ferrie
1.7	Update: Promote/Demote DA, Transfer, Introduction, Self-Service Account; Add alternative method for assigning application access.	8/25/10	Heather Ferrie
1.8	Update: Part 1, Appendix B, Logout screens, Reactivate Acct: Add note re: State contractor/default 30 day expiration, transfer email notifications	9/10/10	Heather Ferrie
1.9	Minor updates based on edits from User and Service Desk guides	9/17/10	Heather Ferrie
2.0	Document re-organization: Removed 2.3 Using FYP, 2.4 Using FYUID, Section 4: Self-Service Your Acct, Section 5: Self-Reg, Update: 1 Intro, 1.1 User Types, 2.2 Login Screen, 6 Create Employee Acct, Sect7.3 Deact, React, Archive, 7.7 Transfer, 8 Work Dashboard, 8.1 Tasks Add: Sec 7.1 Proc Req Form Overview	10/1/10	Heather Ferrie
	Update w/BR comments: Sec 5.5 Reset, Sec 5.6 Unlock	10/5/10	Heather Ferrie
	Sec 4 Create Employee Acct: Updated Business Tel requirement	10/29/10	
	Removed “Draft” designation. NOTE: This is an early version and is subject to change. Please regularly check the NCID Training and Documentation web page to obtain the most current version. https://www.ncid.its.state.nc.us/TrainingAndDocumentation.asp	10/29/10	Heather Ferrie

	Updated Appendix B: User IDs must contain 6-20 characters. The User ID will now be truncated to 20 characters if it exceeds the maximum length.	11/19/10	Heather Ferrie
	Section 2.1: Added note regarding text size setting. Section 4: Updated note regarding 14 day expiration for unclaimed S&L accounts	12/2/10	Heather Ferrie
2.1	Section 5.3: Renamed section to "Viewing and Updating User Account Information". Updated section intro to reference that a user can view application assignment and administrative role assignments from this form. Also included table to identify form components.	12/16/10	Heather Ferrie
2.2	Section 5.2: Included new note under step 1 to verify that the search criteria the DA enters correlates to the comparison parameter for the attribute they are using in their search. Section 5.2: Updated step 2 to reference that Object Lookup screen opens in separate window and included note to inform that the screen may open behind the main screen. Section 5.5: Included new step to ask the user to close all NCID connected applications (i.e.: Exchange, Beacon). This will prevent password synchronization issues when the user logs back into NCID with the new password.	1/7/11	Heather Ferrie
2.3	Section 4: Updated "Password" definition with password case-sensitivity.	1/26/11	Heather Ferrie
	Section 5.3: Included definition for "Password Policy Type" and new footnote 6 to reference how user can change password exp period from 30 to 90 days in their user profile. Section 5.5: Included new footnote 7 to reference that passwords for some state employees, who have special privileges, might exp in 30 days.	2/3/11	Heather Ferrie
	Section 5.5: Insert note to reference DA password can only be reset by another DA. Section 5.6: Insert note to reference DA account can only be unlocked by another DA. Section 5.6: Insert note to clarify the meaning of receiving a yellow box when attempting to unlock a user account.	2/8/11	Heather Ferrie
2.4	Section 5.8: Update w/new content for "Email Disposition Question" field and updated figures. Removed "NG" reference. Removed Appendix B: Differences b/n 7.x & NG Removed Appendix D: Migration Issues	2/23/11	Heather Ferrie
2.5	NEW Section 10: Downloading Reports	03/11/11	Heather Ferrie
2.6	Section 1.1: Updated definition for Application Administrator. Section 2.2: Updated Figure 2-2; Added "Need Help" feature to "Login Screen Self-Service Features" box.	04/22/11	Heather Ferrie
2.7	Section 1.1: Removed reference that SD cannot unlock DA acct. Section 5.6: Inserted reference that SD can unlock DA acct.	07/13/11	Heather Ferrie

2.8	Section 5.5: Inserted note re: changing password on mobile device	07/26/11	Heather Ferrie
2.9	Updated information about role assignments that exceed 500 members. This change was implemented with IDM 4	07/03/12	Brent Roberts
2.10	Update information about the archive workflow with the new check to see if the account is in transfer status.	02/22/13	Brent Roberts
2.11	Update information about the reactivate workflow with information about 3 extended time period for user to access account.	07/31/13	Brent Roberts
2.12	Added and updated information for new password rules and SSPR (Self-Service Password Rest) information.	07/14/16	Brent Roberts

Table of Contents

About this Guide

This guide is designed as a reference for System Administrators, Delegated Administrators and Application Administrators. Using this guide, the reader will become familiar with NCID features, and learn how to work with those features to manage accounts and resources.

Documentation Organization

This guide is organized into four (4) parts, each containing separate sections.

Part 1: Fundamentals includes an overview of the NCID service, and provides information general to all users, such as steps for accessing and logging in to NCID, and getting familiar with the interface.

Section 1: Introduction provides an overview of the features and functionalities found in NCID, and reviews the several types of users who utilize the service.

Section 2: Getting Started provides steps for accessing and logging in to NCID. This section also reviews the self-service features that are found on the Login screen.

Section 3: Getting Familiar with the Interface introduces the main screen to help familiarize you with how the interface organizes information and displays application features.

Part 2: Delegated Administrator Functions provides instruction on the various administrative tools available to a delegated administrator to manage accounts within his or her organization and division/section.

Section 4: Creating an Employee Account provides delegated administrators with instruction on how to create accounts for users within his or her organization and division/section.

Section 5: Managing User Accounts covers the various administrative operations that a delegated administrator can perform on user accounts.

Section 6: Using the Work Dashboard describes how a delegated administrator can make a process request, and explains how an administrator can check the status of a request he or she made.

Section 7: Managing Delegated Administrators describes the three types of delegated administrators that exist in the NCID environment and reviews the functions that each type can perform. This section also reviews how to promote and demote a user account to delegated administrator.

Part 3: Application Administrator Functions describes how application access is granted in NCID and provides instruction on the various administrative tasks available to an application administrator.

Section 8: Making Resource (Application) Assignments describes how application access is granted in NCID. It introduces the concept of roles (a set of permissions to applications) and illustrates how users are assigned to roles to gain access to applications.

Section 9: Managing Application Administrators reviews how to promote and demote a user account to application administrator.

Part 4: Reporting

Section 10: Downloading a Report describes how to download reports for the users and applications that you manage.

Part 5: Appendixes provides additional reference information for the NCID service.

Appendix A: NCID Terminology provides a list of definitions to commonly used terms.

Appendix B: Function Availability for NCID Users highlights the functions each user type can perform based on their job responsibility and level of authority.

Feedback

Please send your comments and suggestions about this guide to the ITS Service Desk at its.incidents@its.nc.gov.

Documentation Updates

For the most current version of the *NCID Administration Guide* please visit the NCID Training and Documentation web page at:

https://www.ncid.its.state.nc.us/TrainingAndDocumentation.asp

Formatting Conventions

The following formatting conventions are used throughout this guide to enable ease of use and understanding:

- **Bold** – Items that are to be clicked on such as buttons.
    - *Example:* Click on the **Start** button.

- *Italics* – Values that need to be typed in as shown.
    - *Example*: In the “Open:” field, type: *cmd*

- “Quotes” – Items that are selected, but not clicked; field names.
    - *Example:* In the “Filename:” field, type: *File.doc*

- [*Italics with Brackets*] – Values that need to be typed in, but will not always be the same.
    - *Example:* In the “Username:” field, type: [*username*]
      Note: [*username*] will be replaced with the actual username, such as *jdoe*.

Special Notes

The screenshots provided in this guide are for informational purposes. Screen content and feature availability may vary based on individual environments, access permissions and version updates.

This page was intentionally left blank

Part 1: Fundamentals

The following sections include an overview of the NCID service, and provide information general to all users, such as accessing and logging in to NCID, and getting familiar with the interface.

This page was intentionally left blank

1 Introduction

The **North Carolina Identity Management Service (NCID)** is the standard identity and access management platform provided by the Department of Information and Technology. NCID 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.

The NCID service provides administrators with many tools to manage user accounts. Depending on your job responsibility and permissions, you will be able to provision users by performing the following operations:

- Create user accounts for state and local government employees[1]
- Update user account information (i.e.: telephone number, address, etc.)
- Process user requests (i.e.: reset passwords, unlock accounts, deactivate accounts, etc.)
- Perform agency-to-agency transfers for state employee accounts
- View details and status of previously submitted requests
- Make resource assignments (grant access to applications)

Before we look at the various ways you can manage user accounts, we will review some of the NCID fundamentals to help you get started. In this section, we will review the different type of users who utilize the NCID service. You will also learn how to access and log in to NCID, and introduce the main screen to familiarize you with how the interlace organizes information and displays application features.

1.1 User Types

A NCID user can be categorized into one of the following user types:

- **State Government Employee** is a person who is currently employed or assigned to work for an agency within the State of North Carolina government.
- **Local Government Employee** is a person who is currently employed or assigned to work for a North Carolina county, municipality or other local government organization.
- **Business User** is a person who is requesting access to the State of North Carolina services on the behalf of a business.
- **Individual** is a person who is requesting access to the State of North Carolina services as an individual or citizen.

All users are required to have an NCID account so that the person can log in to the service and receive permissions to the appropriate resources. Additionally, depending on job responsibility

[1] Accounts for state and local government employees are created by the delegated administrator associated to the employee's organization, division and/or section. Business, individual and some local government employees (who do not have a delegated administrator) can create a new user account via a self-registration service.

and level of authority, state and/or local government employees might receive additional permissions to hold one of the following positions[2]:

- **Delegated Administrator (DA)** can administer user accounts within the same organization, division(s) and/or section(s) for which he or she has administrative rights.
- **Application Administrator** is responsible for controlling membership access to the roles (applications) that he/she can manage. In addition, this person can promote and demote a user account to application administrator.
- **ITS Service Desk (Global Service Desk**) can unlock accounts for any NCID user, including a delegated administrator. In addition, this person can reset passwords for ITS employees only.
- **Agency Service Desk Administrator** can unlock accounts and reset passwords for a state employee who is a member of the same division(s) and/or section(s) for which he or she has administrator rights. This person cannot reset accounts for delegated administrators.

[2] Please refer to Appendix B on page 101 to see a detailed list of functions that each user type can perform based on their permissions.

2 Getting Started

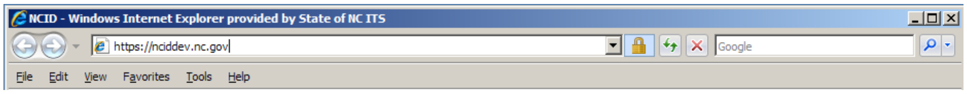
This section describes how to access and log in to NCID, and reviews the self-service features that are found on the Login screen.

2.1 Accessing and Logging In

To begin using the NCID service, you will need to open a Web browser and log in using your NCID user ID and password. Recommended browsers for NCID are: Internet Explorer 10 or higher.

To access and log in to NCID:

1. Open a Web browser and enter the following URL: https://ncid.nc.gov.



NCID - Windows Internet Explorer provided by State of NC ITS

https://nciddev.nc.gov

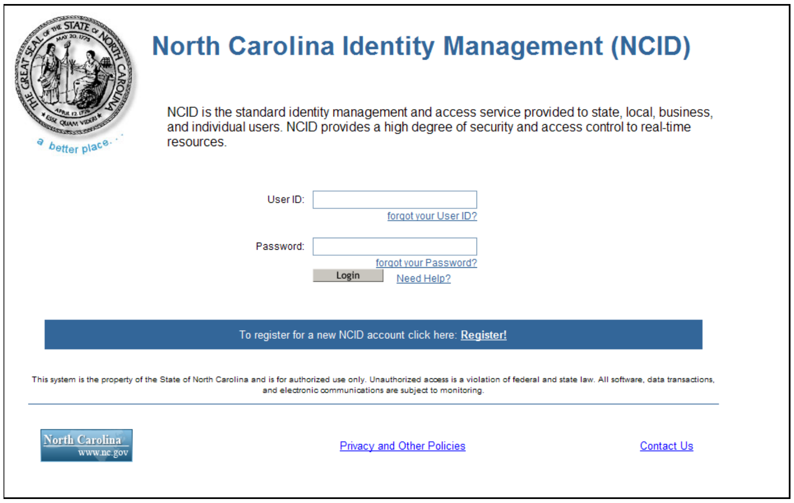
Figure 2-1. Enter URL in the Address Bar

2. The “North Carolina Identity Management (NCID) Login” screen is displayed.

- **Note:** If you cannot view all of the text or buttons on the Login screen, your web browser’s font setting may be too large. You will need to reduce the font size so all of the text and graphics will fit on the screen. To reduce the size in Internet Explorer, click on the **View** menu, and select the **Text Size** option. Click on the desired size (i.e.: Medium). If you have a scroll wheel on your mouse, you can hold the **ctrl** key while turning the wheel toward yourself.

---

3. In the “User ID” field, type [your *NCID user ID*].
4. In the “Password” field, type [your *NCID password*].



North Carolina Identity Management (NCID)

NCID is the standard identity management and access service provided to state, local, business, and individual users. NCID provides a high degree of security and access control to real-time resources.

User ID:

Password:

To register for a new NCID account click here: Register!

This system is the property of the State of North Carolina and is for authorized use only. Unauthorized access is a violation of federal and state law. All software, data transactions, and electronic communications are subject to monitoring.

Figure 2-2 North Carolina Identity Management (NCID) Login Screen

5. Click on **Login**.

6. After successfully logging in, the NCID main screen (also referred to as the "NCID Welcome Page") is displayed. Please refer to the *Getting Familiar with the NCID Interface* section on page 18 for an overview of the application's interface.

> **Important!** Upon logging in to NCID, the system might prompt you to do one of the following:
>
> - Reset your password if it is past its expiration date.
>
>   Note: State and local government users, whose accounts are created by their delegated administrator (not migrated), will need to reset their password and set up their challenge questions upon logging in for the first time.
>
> - Set up your challenge questions if this is your first time logging in to NCID.
>
>   Note: Newly migrated business and individual account holders must update their challenge questions and answers the first time they log in to a protected application. Migrated state and local government users must perform the update the first time their password expires.
>
> Please refer to the *NCID User Guide* for information on how you can manage your challenge questions and reset your password.

2.1.1 Login Screen Self-Service Features

The “Login” screen provides self-service tools which enable all users to reset their password and to lookup a forgotten user ID without seeking assistance from their administrator or the Service Desk. The following table provides a brief description of these tools. For more information, please refer to the *NCID User Guide*.

Self-Service Feature	Description
Forgot Your User ID	This link enables a user to retrieve their user ID. The user must provide some basic information (i.e.: first name, last name) to retrieve the user ID.
Forgot Your Password/Unlock Account	This link allows a user to reset their password if he/she has not recently changed it[3]. The service will also allow the user to unlock their account if it is currently locked. The user must successfully answer all five (5) of their challenge questions before they can create a new password, or unlock their account and log in.
Need Help	This link allows a user to access support resources that are specific to their user type.
Register	This link allows a user to self-register for a NCID account.[4]

[3] Currently a password must be used for 3 days before it can be changed.

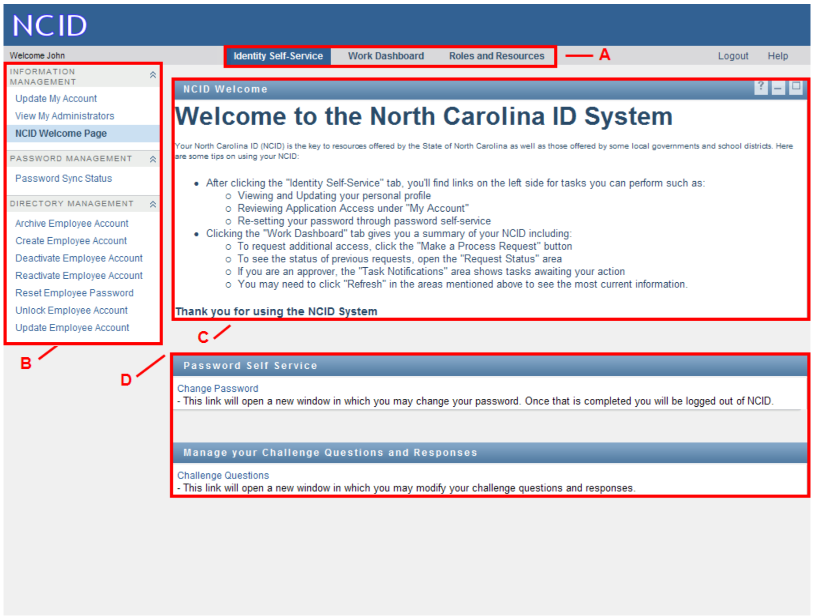
[4] New user accounts for businesses, individuals and local government employees (who do not have a delegated administrator) are created via the self-registration service. Accounts for state and local government employees are created by the delegated administrator associated to the employee’s organization and/or division.

3 Getting Familiar with the Interface

This section describes the layout of the NCID main window to help familiarize you with how the interface organizes information and application features.

3.1 Screen Layout and Features

After logging in to NCID, you will be greeted with the main screen. This screen displays a welcome message and offers some quick tips to help you get started. The following figure illustrates an example of the screen, and highlights its main components.



Welcome to the North Carolina ID System

Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area
  - If you are an approver, the "Task Notifications" area shows tasks awaiting your action
  - You may need to click "Refresh" in the areas mentioned above to see the most current information.

Thank you for using the NCID System

- This link will open a new window in which you may change your password. Once that is completed you will be logged out of NCID.

- This link will open a new window in which you may modify your challenge questions and responses.

Figure 3-1. NCID Main Screen

The screen is separated into the following sections (screen content and feature availability will vary based on job responsibility and access permissions):

A The *tabs* section organizes information and application features. To switch to a different tab, click on the tab you want to see.

- *Identity Self-Service tab* provides access to commonly used workflow links. Workflow links allows you to process requests, such as resetting passwords, reactivating accounts, etc. This tab also provides self-service tools to allow all NCID users to conveniently manage their own account.
- *Work Dashboard tab* provides an alternative method for making a process request. It provides access to every process request that is available to you, and it features a section for viewing the history and status of a submitted request.
- *Roles and Resources tab* allows application administrators assign resources (applications) to users via role assignment. The Roles and Resources tab is viewable to identity delegated administrators; however, they do not have permissions to assign resources.

B The *menu* displays a list of actions that you can perform depending upon your access permissions. Actions are listed by category:

- *Information Management* provides links to help you update your account details, view your administrator(s) contact information and to return you to the main screen.
- *Password Management* provides a link to check if your password has been synchronized across connected systems.
- *Directory Management* provides links to process request forms. Please refer to Appendix B on page 110 to view a list of workflow links that are available to each user type.

C The right-side of the screen displays the details for the action you selected.

D This section contains self-service tools to help you change (reset) your NCID password and manage your challenge questions and responses.

3.2 Getting Help

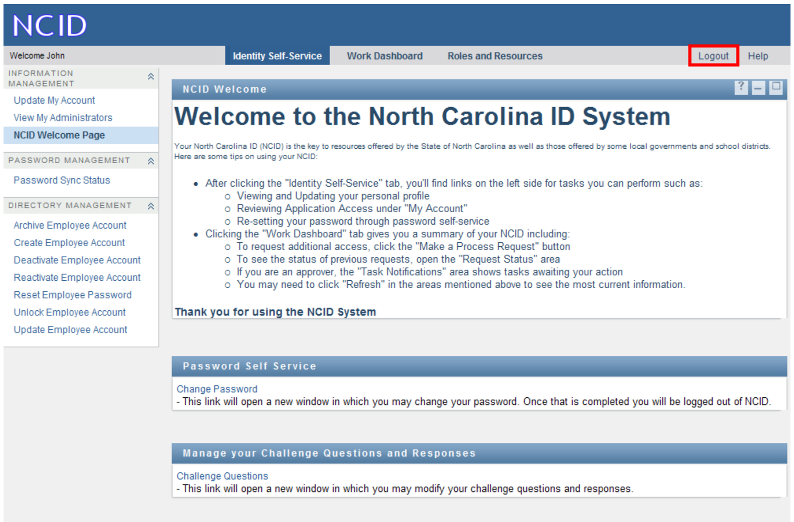
The **Help** Help link, located at the top right corner of the screen, provides access to the most current versions of NCID documentation and training material.

3.3 Logging Out

You may be automatically logged out of NCID after exceeding the state policy's inactivity requirement. You can also log out manually.

To log out of NCID:

1. Click on the **Logout** Logout link located at the top-right section of your screen.



Welcome to the North Carolina ID System

Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area
  - If you are an approver, the "Task Notifications" area shows tasks awaiting your action
  - You may need to click "Refresh" in the areas mentioned above to see the most current information.

Thank you for using the NCID System

Password Self Service

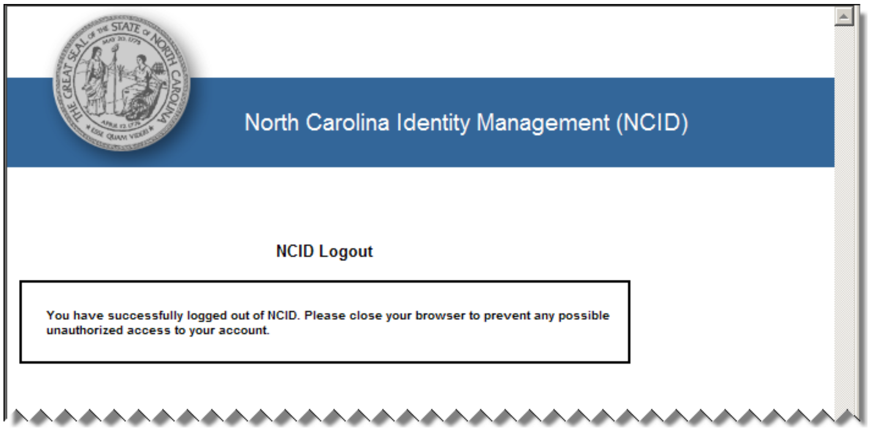
Change Password
- This link will open a new window in which you may change your password. Once that is completed you will be logged out of NCID.

Manage your Challenge Questions and Responses

Challenge Questions
- This link will open a new window in which you may modify your challenge questions and responses.

Figure 3-2. Click "Logout"

2. The “NCID Logout” screen is displayed and indicates that you have successfully logged out of NCID.



NCID Logout

You have successfully logged out of NCID. Please close your browser to prevent any possible unauthorized access to your account.

Figure 3-3. NCID Logout Confirmation Message

3. Close your browser window to prevent any possible unauthorized access to your account.

Part 2: Delegated Administrator Functions

This section provides instruction on the various administrative tasks that a delegated administrator can perform on user accounts within his or her organization and division/section.

This page was intentionally left blank

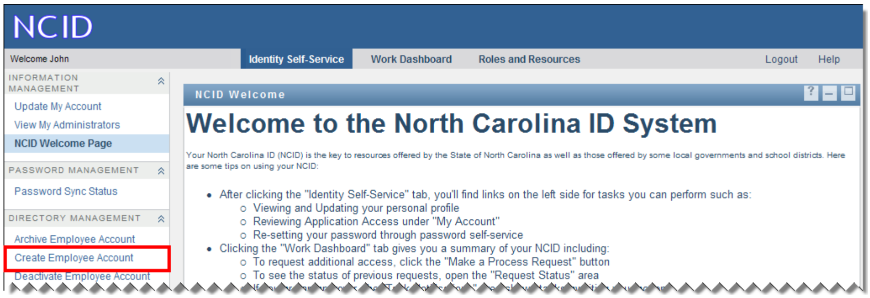
4 Creating an Employee Account

As a delegated administrator, you are responsible for creating new user accounts for any state and local government employee who is a member of the organization, division(s) and/or section(s) which you manage. You can quickly setup a new account via the "Create Employee Account" link on the "Identity Self-Service" tab. This link allows you to access a registration form so that you can enter some basic information about the employee and create a temporary password for the user.

Individual and business users, who need to gain access NCID protected resources, must use the self-registration service on the "NCID Login" screen to create their own accounts. Please refer to the *NCID User Guide* for information on how individual and business users can self-register for an account.

To create an employee account:

1. On the "Identity Self-Service" tab, click on **Create Employee Account** in the menu located on the left side of your screen (this option is listed under the "Directory Management" category).



Welcome to the North Carolina ID System

Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area

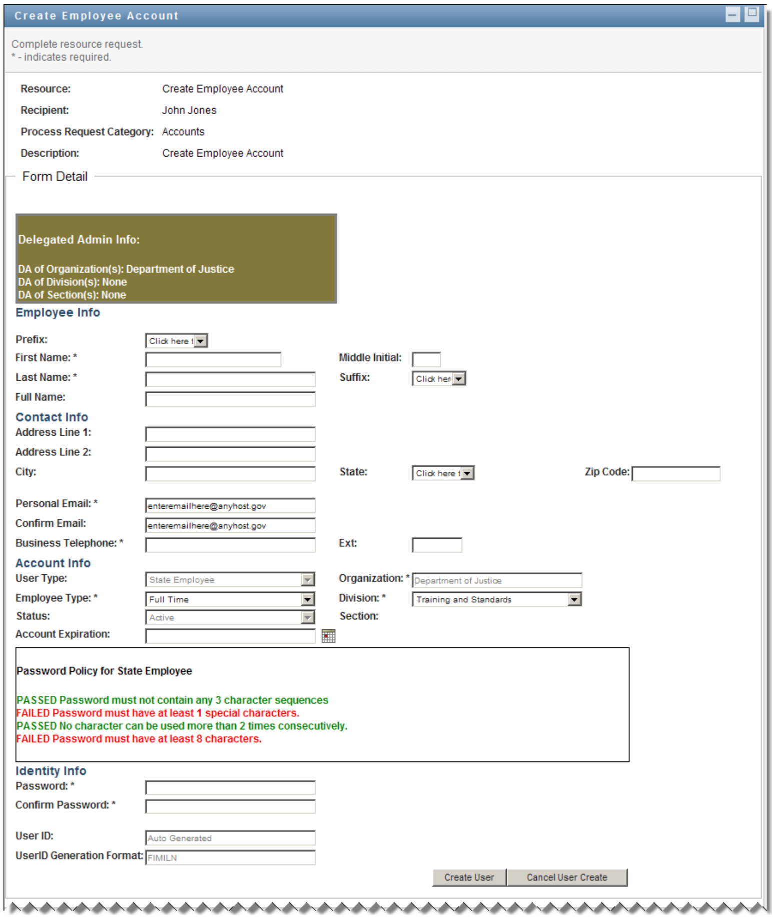
Figure 4-1. Click on "Create Employee Account" Link

2. The "Create Employee Account" screen is displayed. Specify details about this new user. Please note that any field that is followed by an asterisk (*) must be filled out. The system will not let you complete the process until all required information is entered.

Field	Description
"Employee Info" Section	
Prefix	Select one of the listed prefixes, if applicable.
First Name*	Enter the user's first name.
Middle Initial	Enter the initial of the user's middle name.
Last Name*	Enter the user's last name.
Suffix	Select one of the listed suffixes, if applicable.
Full Name	This field is automatically populated with the information entered in the "First Name", "Middle Initial" and "Last Name" fields.

“Contact Info” Section	
Address Line 1	Enter the user’s street address.
Address Line 2	Enter any additional address details.
City	Enter the city name.
State	Select the state.
Zip Code	Enter the zip code.
Personal Email*	By default, this field displays enteremailhere@anyhost.gov. Type over this value to enter the user’s business email address. Upon creating the user account, the system will display the following message: “This is a duplicate email address. Click **OK** if you would still like to proceed with the user creation.” **Important!** A correct and current email address is vital to both creating and managing an NCID account.
Confirm Email*	Re-enter the email address to confirm it matches the value entered in the “Personal Email” field.
Business Telephone*	Enter the10-digit business telephone for the user (ex. 999-999-9999). This number cannot begin with a 0 or 1.
“Account Info” Section	
User Type	This field is pre-populated with one of the following values based upon the administrator’s organization/ division: State Government Employee Local Government Employee
Employee Type*	This field is available when “User Type” = State Government Employee. Select one of the following: ● Contractor ● Full-time ● Part-time
Status	The value for field is system-generated and appears as read-only text.
Account Expiration	This is a required field when “Employee Type” = Contractor. The default expiration is 30 days, but you can click on the **Calendar** icon to select another date. The maximum length is 12 months. **Important!** The system will send reminders to the user and administrator 5 and 15 days prior to the expiration.
Organization*	By default, the organization which you can administer is displayed. Note that if you are an “organization” administrator, all divisions within that organization are available to you in the “Division” dropdown menu below.

Division*	Select the appropriate division for the user. Note that if you are a “division” administrator, you may only assign a user to the division(s) you manage and any of the sections within the division you manage.
Section	Select the section associated to the user. Note that if you are a “section” administrator, you may only create users in the section(s) that you manage.
“Identity Info” Section	
Password Policy Display	This section ensures that the password you enter in the “Password” field complies with the State’s password policy. Notice that when you type the password, each requirement turns from red to green, and the word “Passed” is displayed to indicate that the password has met each policy requirement.
Password*	Enter a temporary password for the user. Passwords are case-sensitive.
Re-enter Password*	Re-enter the password.
User ID	This field is auto-generated for state and local government user accounts.
UserID Generation Format	Identifies the format which is used to generate a user ID. For example, “FIMILN” would include the first initial of the user’s first name, the middle initial (if applicable) and last name to create the user ID (i.e.: John Bernard Smith’s user ID would be: JBSmith). If a User ID matches an existing one, the system will append a number to the User ID. The numbers will increment by 1 for each subsequent User ID (i.e.: JBSmith, JBSmith1, JBSmith 3, etc.).



Complete resource request.
* - indicates required.

Resource: Create Employee Account
Recipient: John Jones
Process Request Category: Accounts
Description: Create Employee Account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Employee Info

Prefix: Click here t
First Name: *
Middle Initial:
Last Name: *
Suffix: Click her
Full Name:

Contact Info

Address Line 1:
Address Line 2:
City:
State: Click here t
Zip Code:
Personal Email: * enteremailhere@anyhost.gov
Confirm Email: enteremailhere@anyhost.gov
Business Telephone: *
Ext:

Account Info

User Type: State Employee
Organization: * Department of Justice
Employee Type: * Full Time
Division: * Training and Standards
Status: Active
Section:
Account Expiration:

Password Policy for State Employee

PASSED Password must not contain any 3 character sequences
FAILED Password must have at least 1 special characters.
PASSED No character can be used more than 2 times consecutively.
FAILED Password must have at least 8 characters.

Identity Info

Password: *
Confirm Password: *
User ID: Auto Generated
UserID Generation Format: FIMILN

Figure 4-2. Create State or Local Gov't User

3. Click on **Create User**. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the "Work Dashboard" tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information

> **Important!** If you attempt to submit the account without entering required information the screen will indicate the error and highlight the problem field(s) in **bold red**.

4. You will need to notify the user that the account was created, and provide the user with the temporary password. Inform the user that he or she must claim the new account within 14 days of it being created or the account will be automatically deleted. To claim the account, the user will need to log in with the temporary password and perform the following actions[5]:
   (1) Set up challenge questions and responses
   (2) Change the password
   (3) Log back into NCID again (the system will log out the user upon setting up the challenge questions and responses)

[5] Please refer the user to the NCID User Guide for information on managing passwords and challenge questions.

5 Managing User Accounts

There are various tools available to delegated administrators to manage employee accounts. In the NCID environment, actions that you can take on an account, such as resetting a password or deactivating an account, are referred to as *process requests*. Your job responsibility and level of permission determines which process requests are available to you.

You can 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. Regardless of the method you choose to access a process request form, information is entered and submitted in the same manner.

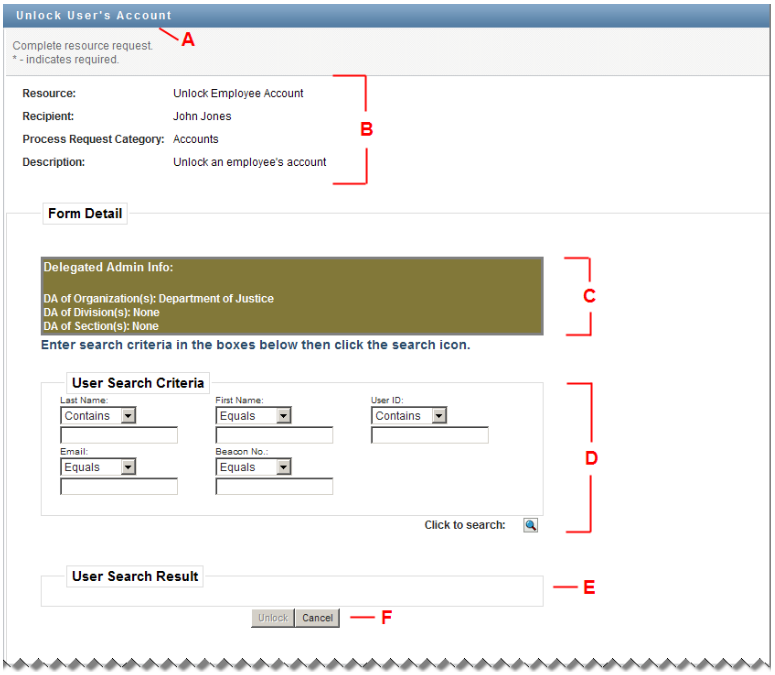
For example, suppose Andrew Jones needs his account unlocked. You would first access the “Unlock Employee Account” request form via the link on the Identity Self-Service tab or from the “Make a Process Request” feature on the Work Dashboard tab. You would then look up Andrew’s account using the search tool on the form, and upon finding Andrew’s account you could then complete the request by clicking on the form’s “Unlock” button.

The following topics in this section demonstrate how to perform process requests via the links on the Identity Self-Service tab, as well as how to make requests which are only available from the Work Dashboard.

- **Note:** Depending on your level of authority, you may perform the actions described in this section on any user within the organization, division(s) and/or section(s) for which you have administrative rights. You can also manage accounts of other administrators who are at your level or lower.

5.1 Process Request Form Overview

Before we demonstrate how to work with request forms, this section will familiarize you with the features that are integral to every form. The following figure illustrates an example of the “Unlock Employee Account” request form and identifies the common components.



Unlock User's Account

Complete resource request.
* - indicates required.

Resource:	Unlock Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Unlock an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to search:

User Search Result

Figure 5-1. Example of a Process Request Form

A This section identifies the name of the process request form you are viewing.

B This section provides general information:

- The **Resource** indicates the name of the process request form.
- The **Recipient** identifies the name of the user who is making the request (you will see your name entered here when you access a form).
- The **Process Request Category** displays the name of the category which the process request is associated.
- The **Description** provides a brief definition of the process request.

C The **Delegated Admin Info** box displays the names of the organization, division(s) and/or section(s) which you can administer.

D The **User Search Criteria** section allows you to find a user account using one or more of the available search fields.

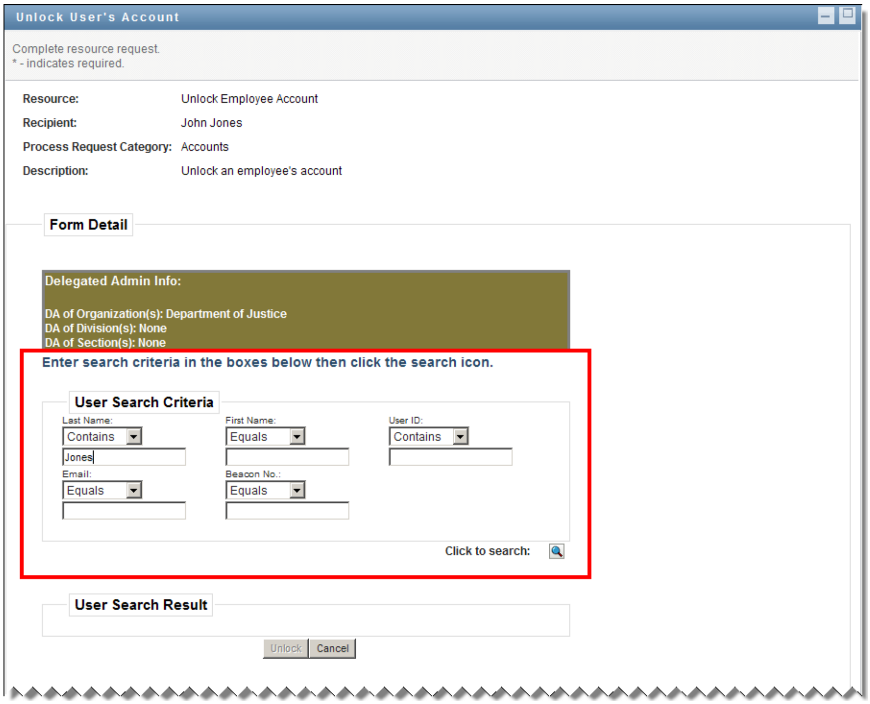
E The **User Search Results** section is updated after a search is performed and a user account is selected. This section displays attributes from the user's profile to let you verify that this is the correct user. Attributes displayed are: Full Name, User ID, Email, Beacon ID and [Account] Status.

F This section contains buttons which allow you to complete or cancel the process request.

5.2 Searching for a User Account

Since the Search feature is common across all process request forms, we will begin by reviewing how to look up a user account.

Upon managing an account, you will need to select the appropriate process request from the Identity Self-Service tab or the 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 "Unlock Employee Account" request form.



Unlock User's Account

Complete resource request.
* - indicates required.

Resource:	Unlock Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Unlock an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains ▾ Jones
First Name: Equals ▾
User ID: Contains ▾
Email: Equals ▾
Beacon No.: Equals ▾

Click to search: 🔍

User Search Result

Figure 5-2. "User Search Criteria" Section

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. Specifying multiple search criteria is helpful in reducing your search results if you think a single field search would result in a very long list. For example, searching for "Last Name" = Jones, might yield many matches, but if we include "First Name" = Andrew our result list would be reduced.

- **Note:** The most effective way to retrieve an account is to search by the User ID field. Since every user has a unique ID the results list will return only one account. This search operation saves you time by eliminating the task of scrolling through a long list of results.

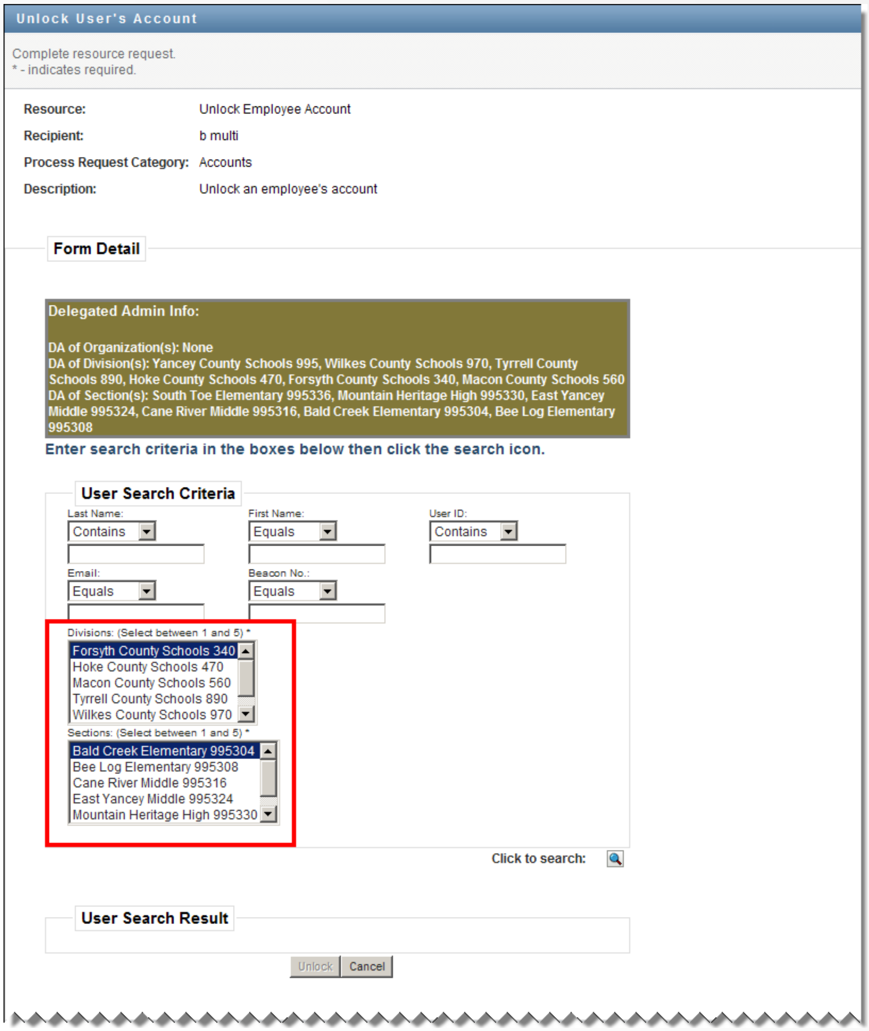
The following table identifies the fields that you can search on.

Last Name	First Name	User ID
Email Address	Beacon Number	

You may also specify a comparison operation to perform against your chosen attribute(s). Each attribute has a dropdown menu to let you select one of the following values: Equals, Contains, Ends With or Starts With.

Important! If you are a delegated administrator of more than 5 divisions or sections, the User Search Criteria will display two additional attribute fields: Divisions and Sections. These fields contain every division and section which you can administer, and let you narrow your search by making up to 5 selections in each field (you must choose at least one division and section).

Indicating a specific division and/or section streamlines your search as your results are displayed faster and are more refined. To make multiple selections, hold CTRL on your keyboard and click on the appropriate selections.



Unlock User's Account

Complete resource request.
* - indicates required.

Resource:	Unlock Employee Account
Recipient:	b multi
Process Request Category:	Accounts
Description:	Unlock an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): None
DA of Division(s): Yancey County Schools 995, Wilkes County Schools 970, Tyrrell County Schools 890, Hoke County Schools 470, Forsyth County Schools 340, Macon County Schools 560
DA of Section(s): South Toe Elementary 995336, Mountain Heritage High 995330, East Yancey Middle 995324, Cane River Middle 995316, Bald Creek Elementary 995304, Bee Log Elementary 995308

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Divisions: (Select between 1 and 5) *
Forsyth County Schools 340
Hoke County Schools 470
Macon County Schools 560
Tyrrell County Schools 890
Wilkes County Schools 970

Sections: (Select between 1 and 5) *
Bald Creek Elementary 995304
Bee Log Elementary 995308
Cane River Middle 995316
East Yancey Middle 995324
Mountain Heritage High 995330

Click to search:

User Search Result

Figure 5-3. Additional Search Options: Divisions & Sections

Performing a search:

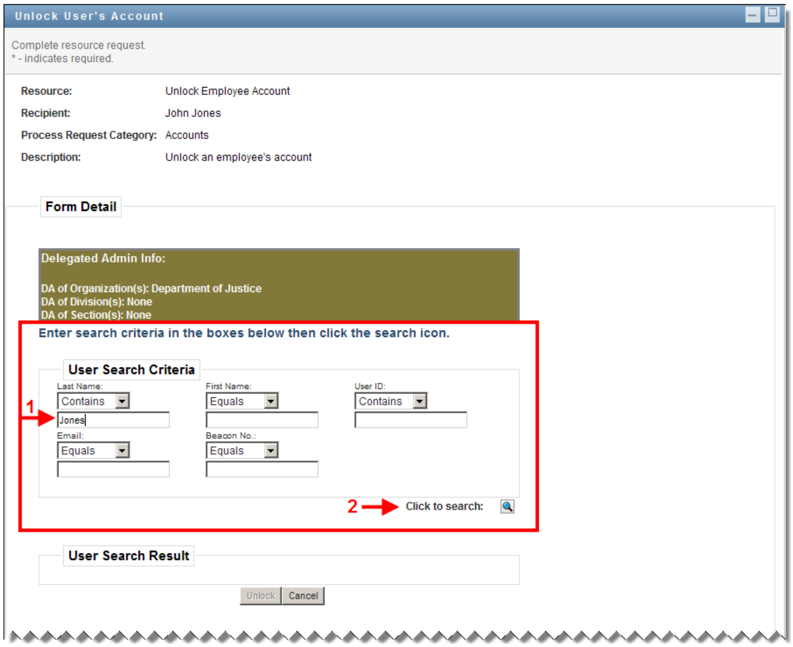
1. From the “User Search Criteria” section, you may either:

   a. Perform an unfiltered search by clicking on the **Search** icon 🔍. This will return a list of all user accounts within your organization, division or section that you can manage.

- **Note:** The system will prompt you to narrow the scope of the search if the number of results exceeds 200 entries.

   b. Filter your search by entering specific criteria into one or more of the available fields, and then clicking on the **Search** icon 🔍.

- **Note:** Before performing your search, please verify that the search criteria you enter correlates to the comparison parameter for the attribute you are using in your search. For example, since the default comparison parameter for the “First Name” attribute is set to “Equals”, you must enter the user’s <u>entire</u> first name in the field. If you enter only part of the user’s first name, the system will search on only those characters you entered and will not get the results you need.



Unlock User's Account

Complete resource request.
* - indicates required.

Resource: Unlock Employee Account
Recipient: John Jones
Process Request Category: Accounts
Description: Unlock an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains — Jones
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to search:

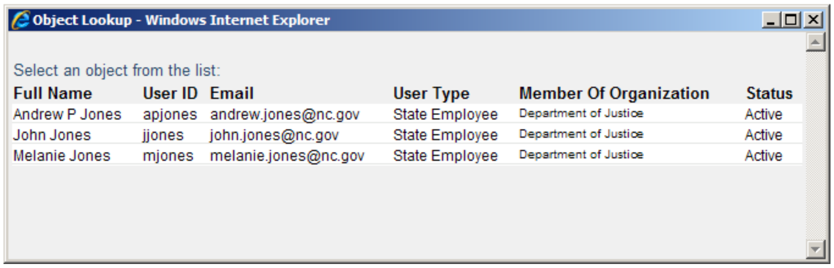
User Search Result

Figure 5-4. Enter Search Criteria

2. The “Object Lookup” screen opens in a separate window and alphabetically displays a list of user accounts which match the search criteria you entered. To help you select the correct user account, the list displays the user(s) full name, user ID and email address. It also indicates the user type, the name of the organization that the user is a member and the status of the account.

- **Note:** If you do not see the “Object Lookup” screen, it may be opened behind your main NCID screen. On the Taskbar, at the bottom of your screen, please click on the "Object Lookup" process to display the window.

3. Scroll through the list and click on the appropriate account to return to the process request form.



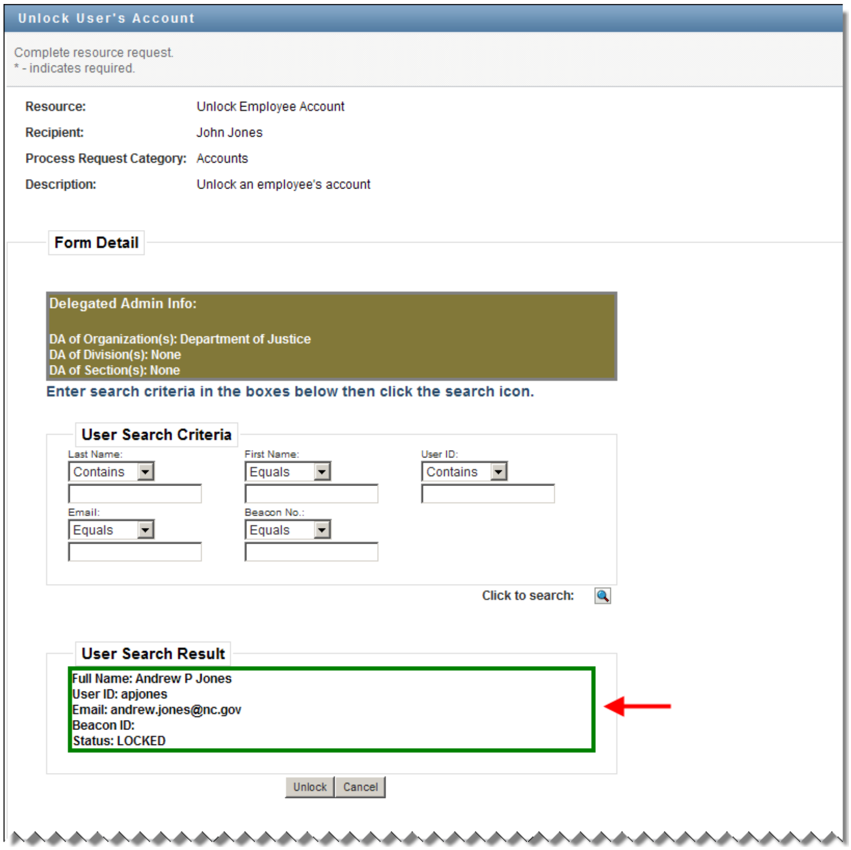
Select an object from the list:

Full Name	User ID	Email	User Type	Member Of Organization	Status
Andrew P Jones	apjones	andrew.jones@nc.gov	State Employee	Department of Justice	Active
John Jones	jjones	john.jones@nc.gov	State Employee	Department of Justice	Active
Melanie Jones	mjones	melanie.jones@nc.gov	State Employee	Department of Justice	Active

Figure 5-5. Example Search Results

4. The request form is updated and attributes stored in the selected user's profile are shown in the "User Search Results" section.

- **Note:** This section is outlined in green to indicate that you can perform this action on the user account. If you do not have permission to perform the action, this section will be highlighted in yellow with a red box.



Unlock User's Account

Complete resource request.
* - indicates required.

Resource:	Unlock Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Unlock an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

User Search Result

Full Name: Andrew P Jones
User ID: apjones
Email: andrew.jones@nc.gov
Beacon ID:
Status: LOCKED

Figure 5-6. "User Search Result" Section

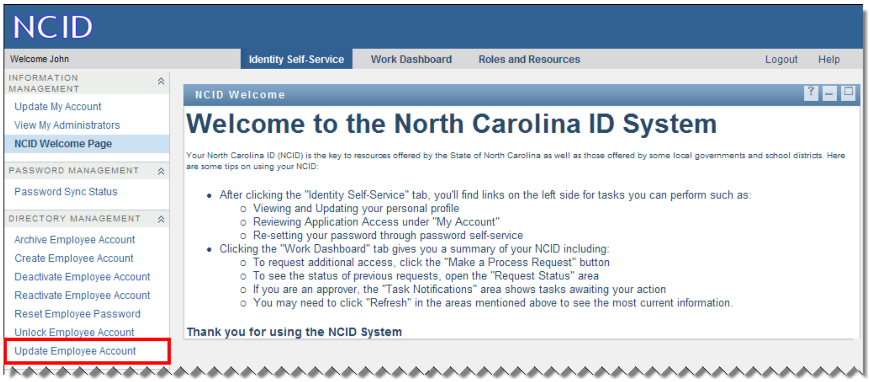
5. You can verify this is the correct user account by checking the name displayed in the “Full Name” field, and verifying the user ID in the “User ID” field. If this is the correct user account that you wish to manage, you can continue processing the request. If this is not the appropriate user, you can clear the fields and perform your search again.

5.3 Viewing and Updating User Account Information

You may view a user’s account profile and update selected information by using the “Update Employee Account” link found on the “Identity Self-Service” tab. This link allows you see general information such as contact details, applications which the user can access, and administrative roles that have been assigned to him or her. This link also allows you to keep the user’s account information current, for example, changing the account expiration date for a contractor whose contract has been extended. Values which appear as read-only text may not be modified.

To view/update user account information:

1. On the “Identity Self-Service” tab, click **Update Employee Account** in the menu located on the left side of your screen (this option is listed under the “Directory Management” category).



Welcome to the North Carolina ID System

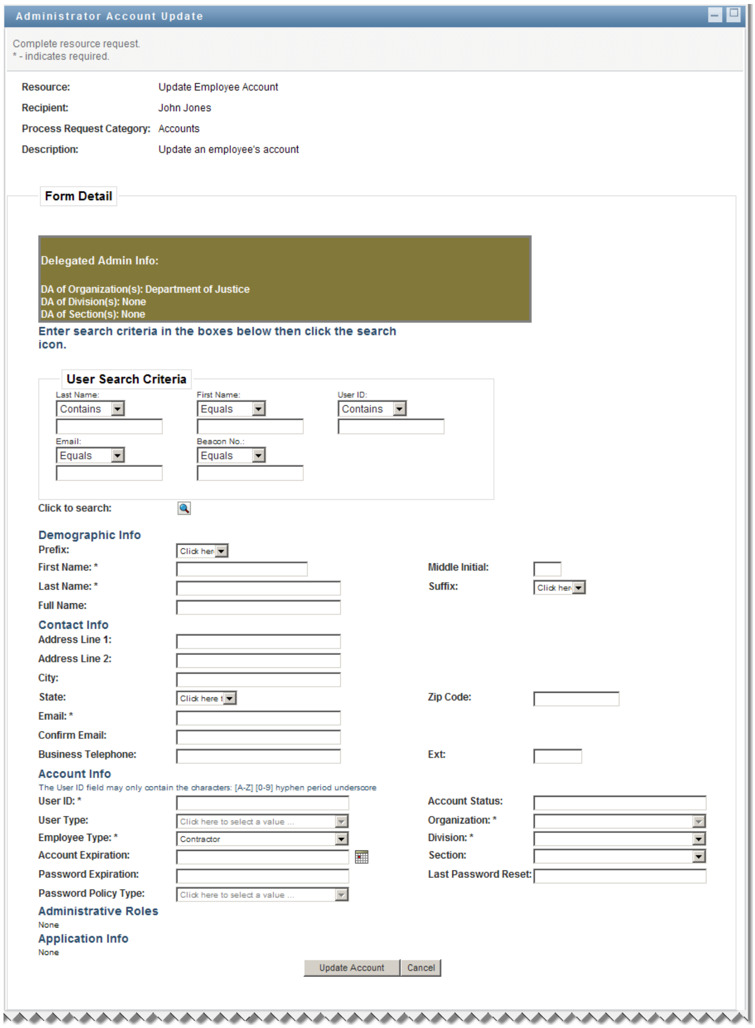
Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area
  - If you are an approver, the "Task Notifications" area shows tasks awaiting your action
  - You may need to click "Refresh" in the areas mentioned above to see the most current information.

Thank you for using the NCID System

Figure 5-7. Click on “Update Employee Account” Link

2. The “Administrator Account Update” request form is displayed. You will need to search for the account you wish to modify. Please refer to the Searching for a User Account section on page 29 for details on how to look up a user account.



Administrator Account Update

Complete resource request.
* - indicates required.

Resource:	Update Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Update an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to search:

Demographic Info

Prefix: Click her
First Name: *
Middle Initial:
Last Name: *
Suffix: Click her
Full Name:

Contact Info

Address Line 1:
Address Line 2:
City:
State: Click here t
Zip Code:
Email: *
Confirm Email:
Business Telephone:
Ext:

Account Info

The User ID field may only contain the characters: [A-Z] [0-9] hyphen period underscore

User ID: *
Account Status:
User Type: Click here to select a value ...
Organization: *
Employee Type: * Contractor
Division: *
Account Expiration:
Section:
Password Expiration:
Last Password Reset:
Password Policy Type: Click here to select a value ...

Administrative Roles

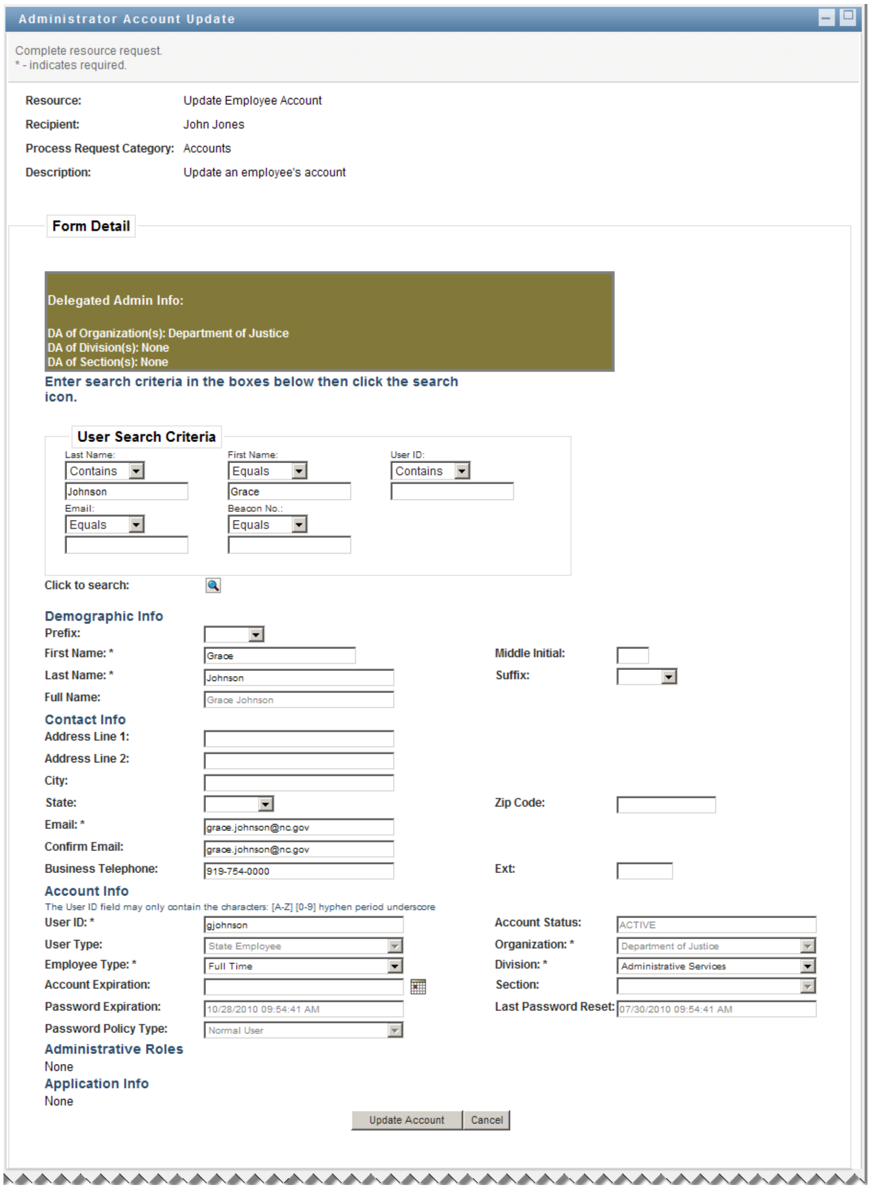
None

Application Info

None

Figure 5-8. “Administrator Account Update” Request Form

3. Once you have selected the account, the request form is updated and displays the user’s profile.
4. Verify that this is the correct user account that you wish to update. If this is not the appropriate user, you can clear the fields and perform your search again.
5. Please refer to the *Creating an Employee Account* section on page 23 for a description of most of the fields displayed on this request form. The following table provides a description of sections/data fields not which have not been discussed.



Administrator Account Update

Complete resource request.
* - indicates required.

Resource:	Update Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Update an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains Johnson
First Name: Equals Grace
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to search:

Demographic Info

Prefix:			
First Name: *	Grace	Middle Initial:	
Last Name: *	Johnson	Suffix:	
Full Name:	Grace Johnson		

Contact Info

Address Line 1:			
Address Line 2:			
City:			
State:		Zip Code:	
Email: *	grace.johnson@nc.gov		
Confirm Email:	grace.johnson@nc.gov		
Business Telephone:	919-754-0000	Ext:	

Account Info

The User ID field may only contain the characters: [A-Z] [0-9] hyphen period underscore

User ID: *	gjohnson	Account Status:	ACTIVE
User Type:	State Employee	Organization: *	Department of Justice
Employee Type: *	Full Time	Division: *	Administrative Services
Account Expiration:		Section:	
Password Expiration:	10/28/2010 09:54:41 AM	Last Password Reset:	07/30/2010 09:54:41 AM
Password Policy Type:	Normal User		

Administrative Roles

None

Application Info

None

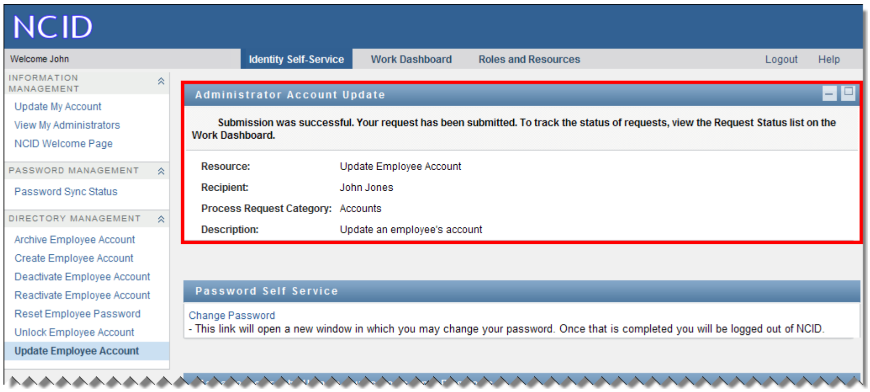
Figure 5-9. Update User Details

Section/Field	Description
"Account Info" Section	
Password Expiration	Shows when the user's password will expire. Passwords for state and local government employees will expire every 90 days.[6] There is no password expiration for business and individual user accounts.
Last Password Reset	Identifies when a user's password was last reset.

[6] Typically, passwords for state and local government employees will expire every 90 days; however, passwords for some state employees, who have more privileges, will expire every 30 days.

Section/Field	Description
Administrative Roles	
This section identifies any delegated administrative role or service desk role that has been assigned to the user. Note that DA roles will be organized by organization, division and section. If the user does not have any DA role assigned to him or her, then "None" will appear in this section.	
Application Info	
This section identifies the applications which the user may access.	
Password Policy Type	Indicates one of the two (2) types of policies that can be applied to a user's password. ● Normal user: applied to typical users and enforces a 90 day expiration policy. ● Administrative user: applied to user accounts with more privileges than those of a typical user and enforces a 30 day expiration policy.

6. Make the appropriate changes and click on **Update Account**.
7. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the "Work Dashboard" tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.



Submission was successful. Your request has been submitted. To track the status of requests, view the Request Status list on the Work Dashboard.

Resource: Update Employee Account

Recipient: John Jones

Process Request Category: Accounts

Description: Update an employee's account

- This link will open a new window in which you may change your password. Once that is completed you will be logged out of NCID.

Figure 5-10. Confirmation Message

5.4 Deactivating, Reactivating and Archiving an Account

You can deactivate a state or local government employee account without deleting or removing the account completely from the system. Deactivation suspends the user's rights or associations so that the user will be unable to log in to NCID and will not be able to access any connected resources.

A deactivated account can be reactivated if the organization wishes to grant the user the ability to access NCID resources. Alternatively, a deactivated account may also be archived; if for example, the user decides to permanently leave state employment.

- **Note:** Business and individual accounts are deactivated and archived by the account holder. Please refer to the *NCID User Guide* for more information.

5.4.1 Deactivating an Account

Deactivating a user account is useful when an employee takes a leave of absence, for example, maternity leave or military service. This prevents the user from logging in to NCID and accessing connected resources while he or she is taking a temporary leave. When the employee returns to work the account can be easily reactivated.

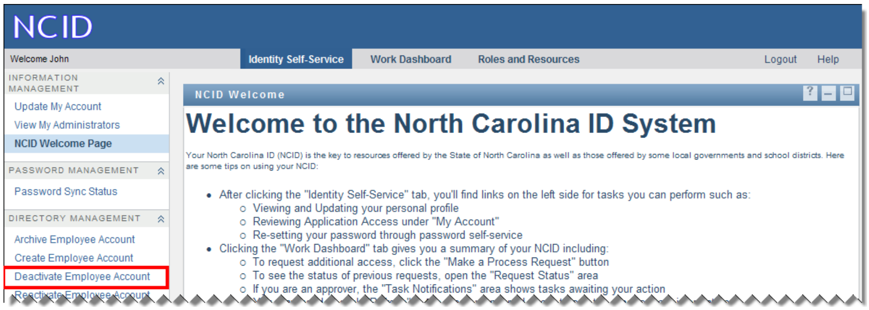
- **Note:** An account will be automatically deactivated after 90 days of inactivity. The employee must contact his or her delegated administrator to reactivate the account.

> **Important!** If a state employee moves to a different agency, you do not need to deactivate and archive the account. You may transfer the user's account to the new agency by using the "Transfer a User Account" process request. Please refer to the *Transferring a State User Account* section on page 53 for more information.

- **Note:** Upon deactivation, the user account status is changed from "Active" to "Disabled".

To deactivate a user account:

1. On the "Identity Self-Service" tab, click **Deactivate Employee Account** in the menu located on the left side of your screen (this option is listed under the "Directory Management" category).



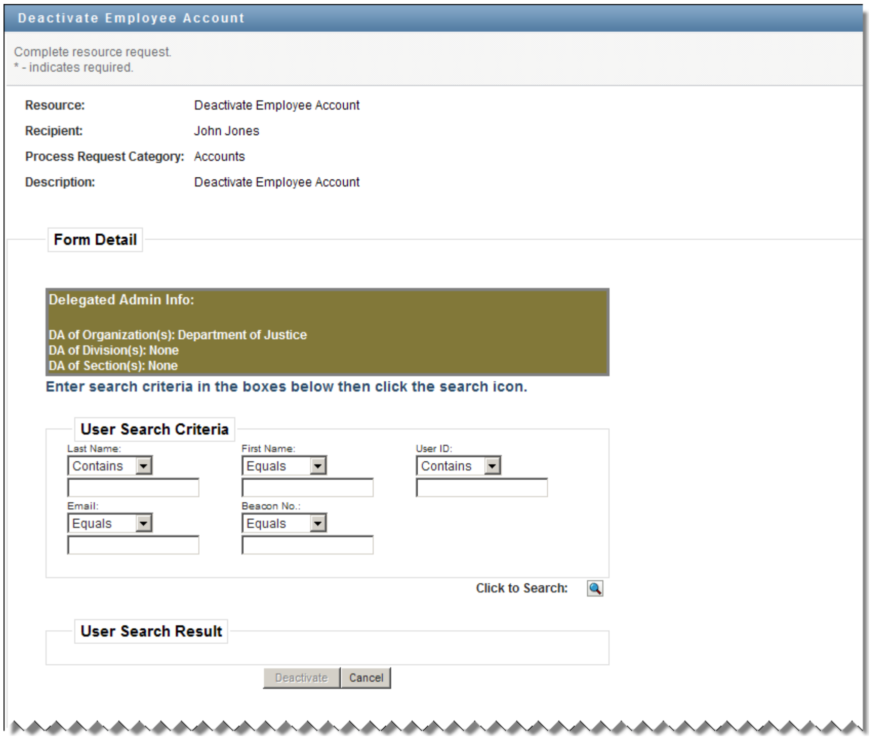
Welcome to the North Carolina ID System

Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area
  - If you are an approver, the "Task Notifications" area shows tasks awaiting your action

Figure 5-11. Click on "Deactivate Employee Account" Link

2. The "Deactivate Employee Account" request form is displayed. You will need to search for the account you wish to deactivate. Note that only active users will be searched. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account.



Deactivate Employee Account

Complete resource request.
* - indicates required.

Resource:	Deactivate Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Deactivate Employee Account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

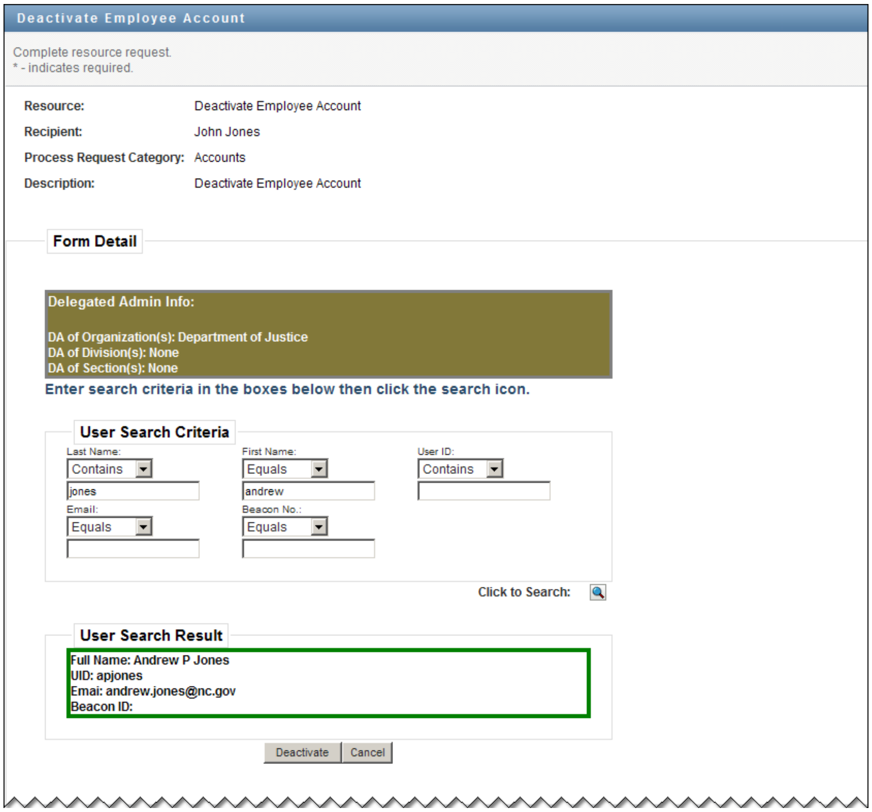
Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Figure 5-12. "Deactivate Employee Account" Request Form

3. Once you have selected the account, the request form is updated and displays selected attributes from the user's profile in the "User Search Result" section.
4. Verify that this is the correct user account that you wish to deactivate. If this is not the appropriate user, you can clear the fields and perform your search again.



Deactivate Employee Account

Complete resource request.
* - indicates required.

Resource:	Deactivate Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Deactivate Employee Account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains jones
First Name: Equals andrew
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to Search:

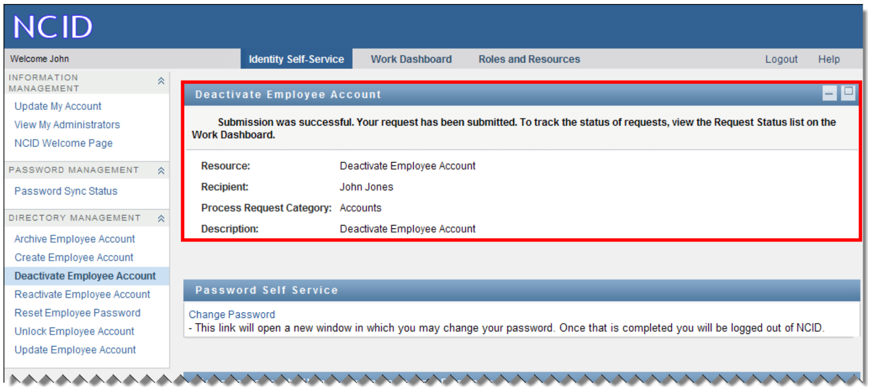
User Search Result

Full Name: Andrew P Jones
UID: apjones
Emai: andrew.jones@nc.gov
Beacon ID:

Figure 5-13. Verify User Details

5. Click on **Deactivate**.
6. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the “Work Dashboard” tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.

- **Note:** To view a list of all deactivated users that you can manage you can use the “Reactivate Employee Account” workflow link to perform an open search. Please refer to the *Reactivating an Account* section on page 40 or more information.



Deactivate Employee Account

Submission was successful. Your request has been submitted. To track the status of requests, view the Request Status list on the Work Dashboard.

Resource:	Deactivate Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Deactivate Employee Account

Password Self Service

Change Password
- This link will open a new window in which you may change your password. Once that is completed you will be logged out of NCID.

Figure 5-14. Confirmation Message

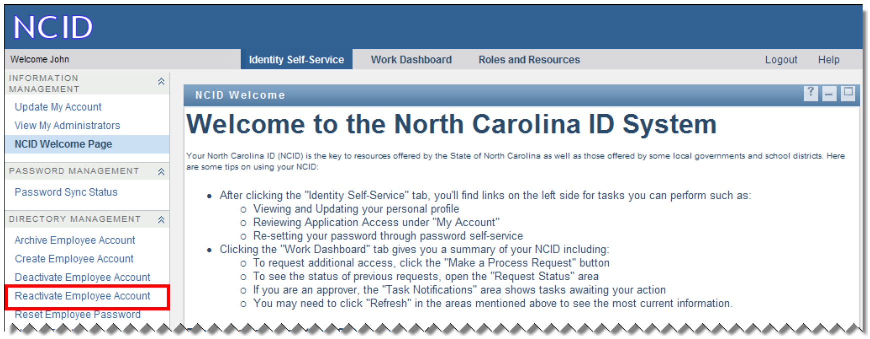
5.4.2 Reactivating an Account

Deactivated accounts can be easily reactivated if the organization wishes to grant the user access NCID resources again. For example, an account can be reactivated for an employee who returns to work after taking a temporary leave of absence.

> Note:
>
> - If an account has not been accessed for over 90 days it is auto disabled. Reactivating the account will set the auto archive timer to 3 days. The user will have 3 days to access the account from any integrated NCID application or it will be auto deactivated again. Once accessed, the timer will be reset to current activity date and time.
>
> - 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.

To reactivate a user account:

1. On the "Identity Self-Service" tab, click **Reactivate Employee Account** in the menu located on the left side of your screen (this option is listed under the "Directory Management" category).



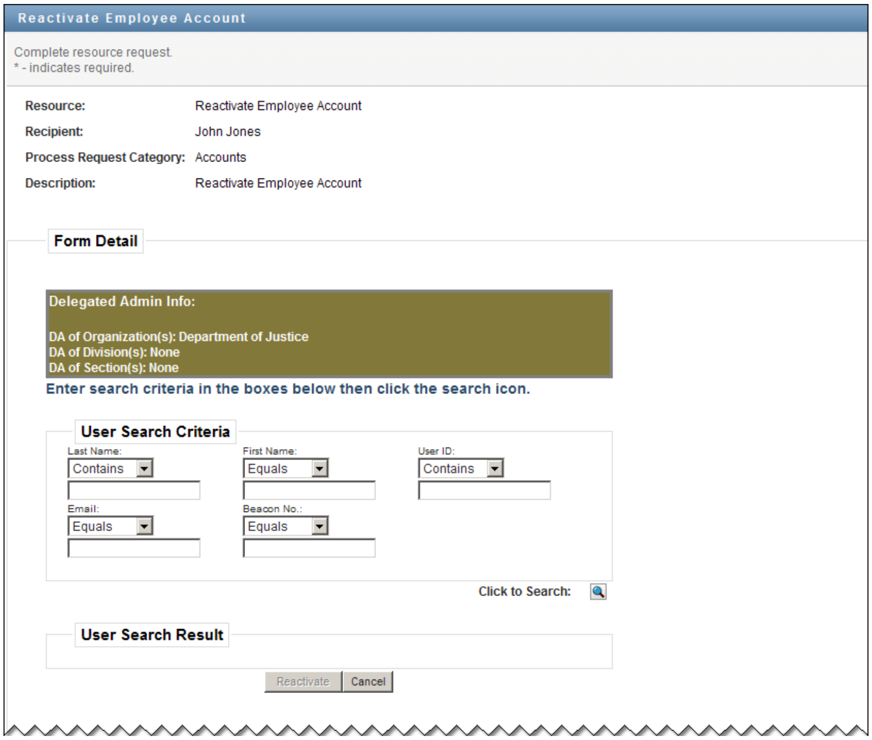
Welcome to the North Carolina ID System

Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area
  - If you are an approver, the "Task Notifications" area shows tasks awaiting your action
  - You may need to click "Refresh" in the areas mentioned above to see the most current information.

Figure 5-15. Click on "Reactivate Employee Account" Link

2. The "Reactivate Employee Account" request form is displayed. You will need to search for the account you wish to reactivate. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account. The search will return a list of deactivated user accounts that you can manage.



Reactivate Employee Account

Complete resource request.
* - indicates required.

Resource:	Reactivate Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Reactivate Employee Account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

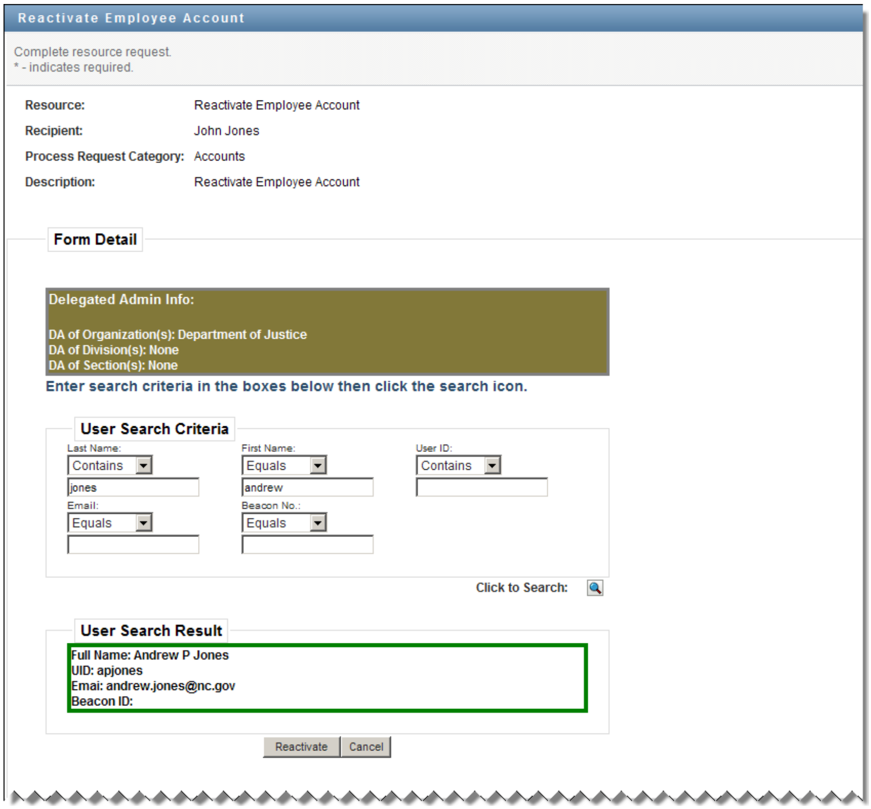
Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to Search:

User Search Result

Figure 5-16. "Reactivate Employee Account" Request Form

3. Once you have selected the account, the request form is updated and displays selected attributes from the user's profile in the "User Search Result" section.
4. Verify that this is the correct user account that you wish to reactivate. If this is not the appropriate user, you can clear the fields and perform your search again.



Complete resource request.
* - indicates required.

Resource: Reactivate Employee Account
Recipient: John Jones
Process Request Category: Accounts
Description: Reactivate Employee Account

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

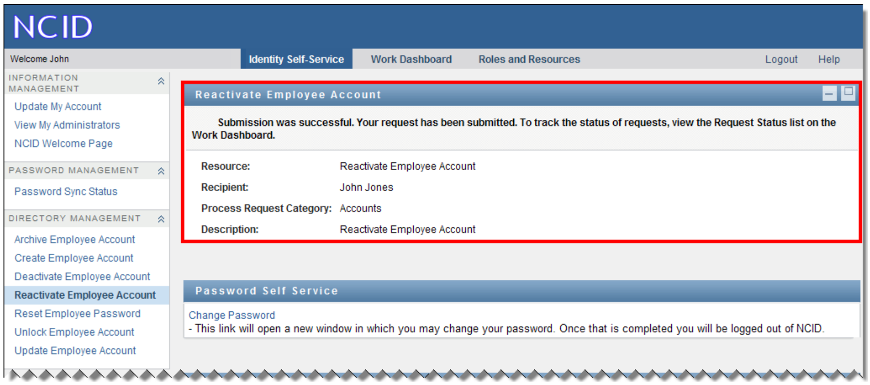
Enter search criteria in the boxes below then click the search icon.

Last Name: Contains jones
First Name: Equals andrew

Full Name: Andrew P Jones
UID: apjones
Emai: andrew.jones@nc.gov
Beacon ID:

Figure 5-17. Verify User Details

5. Click on **Reactivate**.
6. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the "Work Dashboard" tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.



Submission was successful. Your request has been submitted. To track the status of requests, view the Request Status list on the Work Dashboard.

Resource: Reactivate Employee Account
Recipient: John Jones
Process Request Category: Accounts
Description: Reactivate Employee Account

- This link will open a new window in which you may change your password. Once that is completed you will be logged out of NCID.

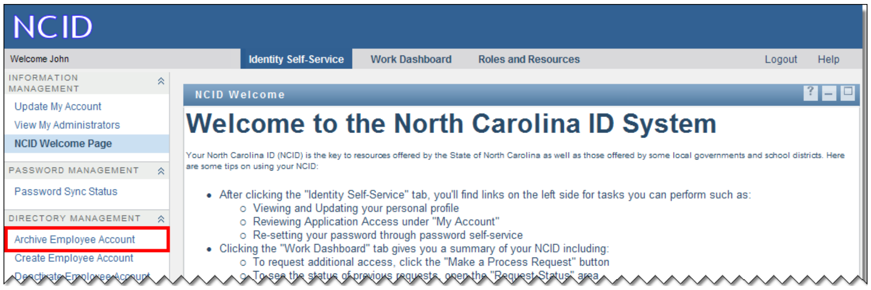
Figure 5-18. Confirmation Message

5.4.3 Archiving an Account

An account may be archived, for example, when an employee is leaving state employment. The account must be deactivated before it can be archived. Please note that once the account is archived it cannot be reinstated. If the user decides to return to state employment, it will be necessary to create a new account for the user to access NCID connected resources again. Additionally, the account cannot currently be in a transfer status.

To archive a user account:

1. On the “Identity Self-Service” tab, click **Archive Employee Account** in the menu located on the left side of your screen (this option is listed under the “Directory Management” category).



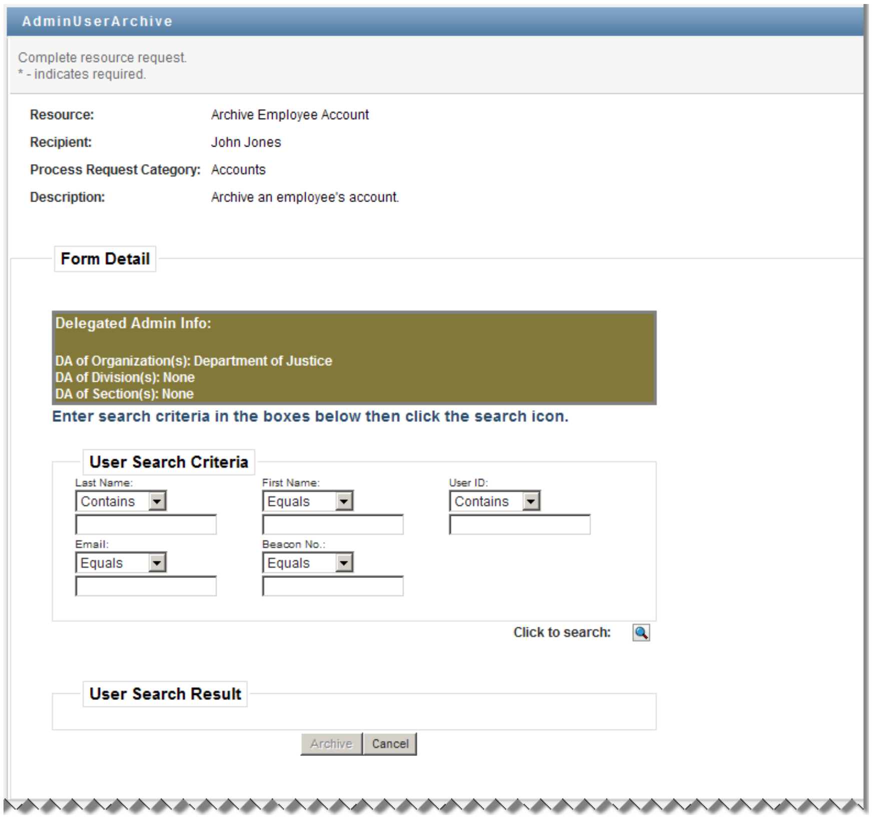
Welcome to the North Carolina ID System

Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area

Figure 5-19. Click on “Archive Employee Account” Link

2. The “Admin User Archive” request form is displayed. You will need to search for the account you wish to archive. Only accounts which are deactivated will be searched. Please refer to the Searching for a User Account section on page 29 for details on how to look up a user account.



Complete resource request.
* - indicates required.

Resource:	Archive Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Archive an employee's account.

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

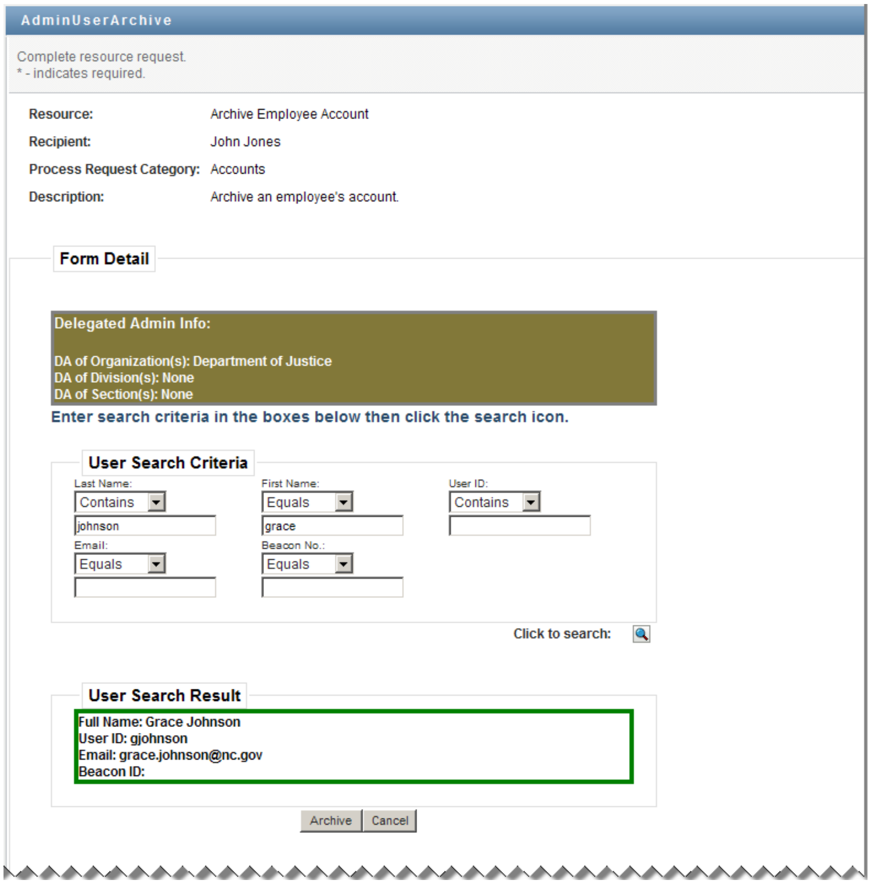
Enter search criteria in the boxes below then click the search icon.

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Figure 5-20. “Archive Employee Account” Request Form

3. Once you have selected the account, the request form is updated and displays selected attributes from the user's profile in the "User Search Result" section.
4. Verify that this is the correct user account that you wish to archive. If this is not the appropriate user, you can clear the fields and perform your search again.

- **Note:** If the account is currently in an active state agency transfer status you will receive an error message and the **Archive** button will be unavailable to select. You will have to complete or cancel the transfer before the account can be archived.



AdminUserArchive

Complete resource request.
* - indicates required.

Resource:	Archive Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Archive an employee's account.

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains johnson
First Name: Equals grace
User ID: Contains
Email: Equals
Beacon No.: Equals

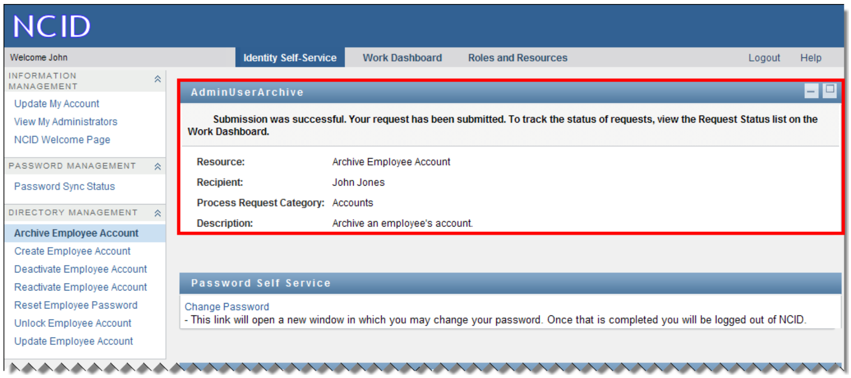
Click to search:

User Search Result

Full Name: Grace Johnson
User ID: gjohnson
Email: grace.johnson@nc.gov
Beacon ID:

Figure 5-21. Verify User Details

5. Click on **Archive**. A message displays to verify that you want to archive the account. Click **OK** to continue.
6. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the "Work Dashboard" tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.



Submission was successful. Your request has been submitted. To track the status of requests, view the Request Status list on the Work Dashboard.

Resource:	Archive Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Archive an employee's account.

- This link will open a new window in which you may change your password. Once that is completed you will be logged out of NCID.

Figure 5-22. Confirmation Message

5.5 Resetting a User Password

You can reset passwords for employees who have trouble using the “Forgot Your Password” self-service feature or whose password has expired.[7]

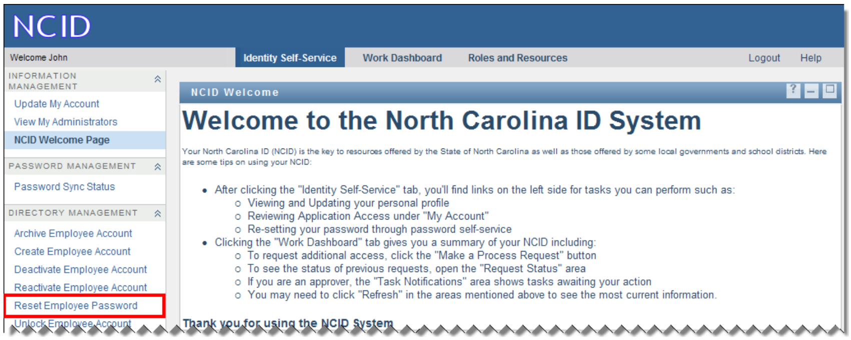
If an employee is unable to change their password, you may reset it using the “Reset Employee Password” link on the “Identity Self-Service tab, and then provide the user with a temporary one. The person may only use the temporary password once to allow the user to log in to NCID and then create a new password.

- **Note:** Delegated administrator passwords can only be reset by another delegated administrator who is at the same level or higher.

To reset a password:

1. Verify that the user is the account holder and that it is acceptable to reset the password.
2. Ask the user to close all NCID connected applications (i.e.: Office-365, Beacon). This will prevent password synchronization issues when the user logs back into NCID with the new password.
3. On the “Identity Self-Service” tab, click **Reset Employee Password** in the menu located on the left side of your screen (this option is listed under the Directory Management category).

[7] Typically, passwords for state and local government employees will expire every 90 days; however, passwords for some state employees, who have more privileges, will expire every 30 days. A user can change the expiration period by setting the “Password Policy Type” field from “Administrative User” to “Normal User” in their account profile. Changing this setting will not impact a DA’s rights.



Welcome to the North Carolina ID System

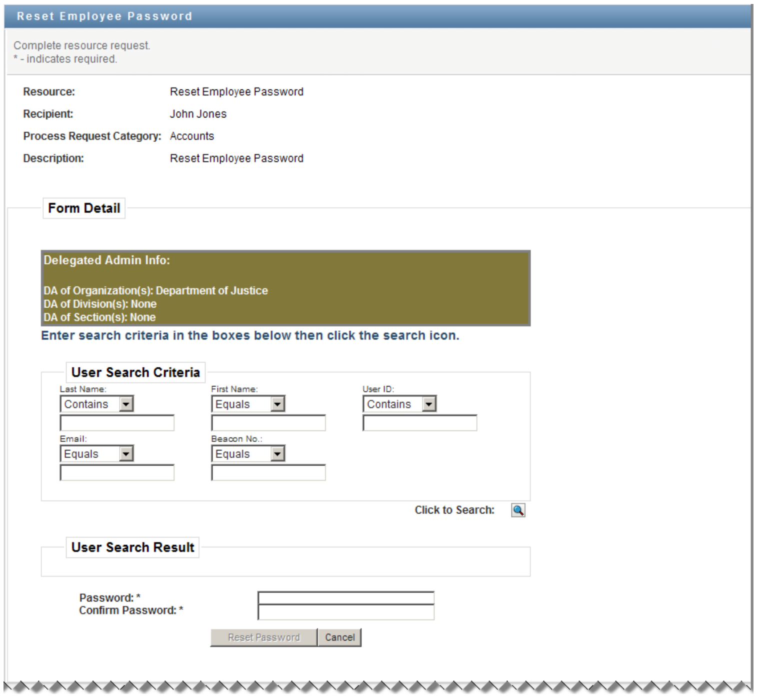
Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area
  - If you are an approver, the "Task Notifications" area shows tasks awaiting your action
  - You may need to click "Refresh" in the areas mentioned above to see the most current information.

Thank you for using the NCID System

Figure 5-23. Click on “Reset Employee Password” Link

4. The “Reset Employee Password” request form is displayed. You will need to search for the account you wish to modify. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account.



Complete resource request.
* - indicates required.

Resource:	Reset Employee Password
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Reset Employee Password

Delegated Admin Info:

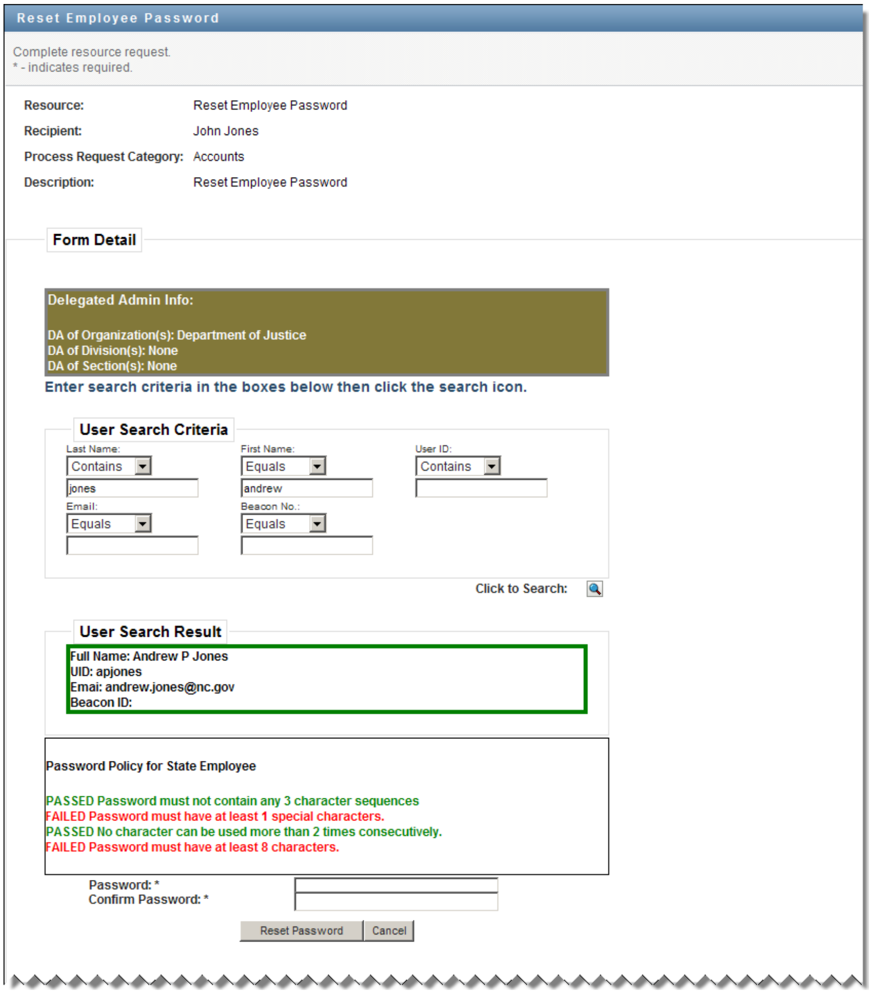
DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

Password: *
Confirm Password: *

Figure 5-24. “Reset Employee Password” Request Form

5. Once you have selected the account, the request form is updated and displays selected attributes from the user’s profile in the “User Search Result” section. You can verify this is the correct user account by checking the name displayed in the “Full Name” field, and by verifying the user ID in the “User ID” field.
6. If this is not the appropriate user, you can clear the fields and perform your search again.



Reset Employee Password

Complete resource request.
* - indicates required.

Resource:	Reset Employee Password
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Reset Employee Password

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains jones
First Name: Equals andrew
User ID: Contains
Email: Equals
Beacon No.: Equals

User Search Result

Full Name: Andrew P Jones
UID: apjones
Email: andrew.jones@nc.gov
Beacon ID:

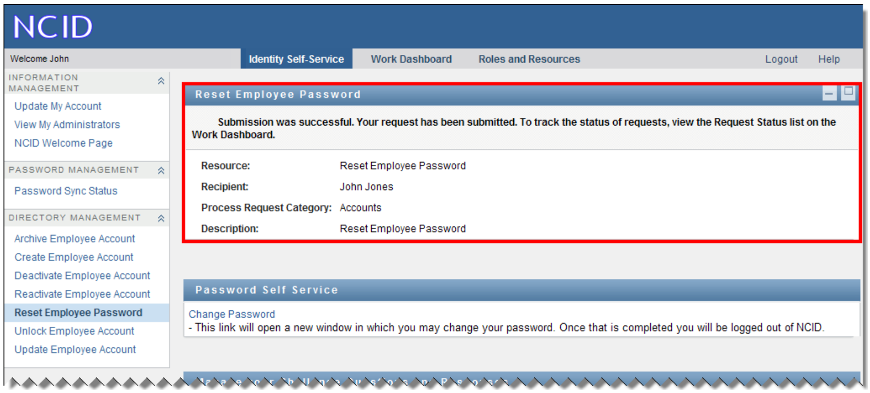
Password Policy for State Employee

PASSED Password must not contain any 3 character sequences
FAILED Password must have at least 1 special characters.
PASSED No character can be used more than 2 times consecutively.
FAILED Password must have at least 8 characters.

Password: *
Confirm Password: *

Figure 5-25. Verify User Details

7. A "Password Policy" box is displayed to ensure that the password you enter complies with the State's password policy. Notice that 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.
8. Enter a temporary password in the "Password" field and re-enter it in the "Confirm Password" field. Please remember to check the "Password Policy" box to verify that each requirement has been met.
9. For security reasons, please do not use passwords that you previously used when resetting another employee's password. Ensure that the password is unique.
10. Click on Reset Password.
11. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the "Work Dashboard" tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.



Submission was successful. Your request has been submitted. To track the status of requests, view the Request Status list on the Work Dashboard.

Resource: Reset Employee Password
Recipient: John Jones
Process Request Category: Accounts
Description: Reset Employee Password

- This link will open a new window in which you may change your password. Once that is completed you will be logged out of NCID.

Figure 5-26. Confirmation Message

12. You will need to provide the user with the temporary password, and tell him or her to log in to NCID at https://ncid.nc.gov. The user will need to access the website from a computer that is already logged in to the network.
13. In addition, explain to the user that upon logging in the system will display the “Change Password” screen forcing him or her to create a new password. Remind the user to follow the password policy rules, and that NCID passwords are case-sensitive. You should emphasis that passwords must be entered exactly as they were originally entered.

    In addition, make the user aware that after changing the password, he or she will be automatically logged out of the system.

> **Important!** Ask the user if he or she uses a mobile device to connect to a NCID application. For example, a user may connect to Office-365 to access their email via a mobile phone or PDA. In this case, instruct the user to also change the password on each device. If the password is not changed, the user will be unable to log in. Note that the user’s NCID account will lock after 3 failed login attempts.

5.6 Unlocking a User Account

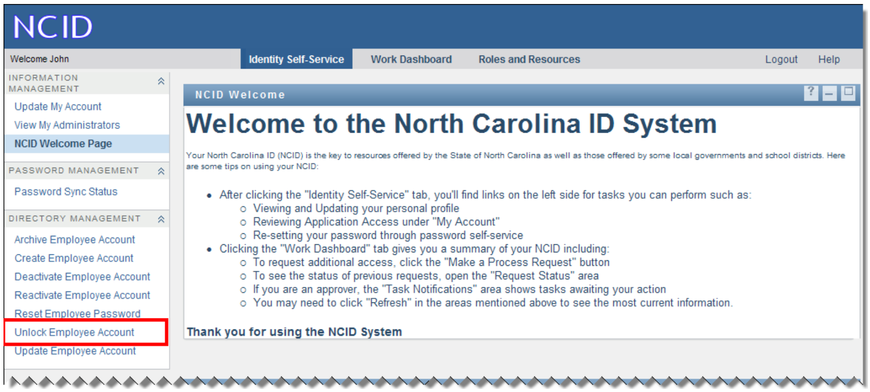
You can unlock any employee account within your organization, division or section for which you have administrative rights.

If a user has tried to access a protected application and failed after three (3) attempts, his or her account will lock. Note that the account will automatically unlock after 30 minutes from the time it was locked. **After the lockout period expires, the user will need to log in to NCID and then continue to the application that they were trying to access.** However, if the user requires immediate assistance, you can manually unlock the account before the lockout period expires.

- **Note:** Delegated administrator accounts can be unlocked by another delegated administrator who is at the same level or higher. A delegated administrator can also request an unlock from a Service Desk agent.

To unlock an account:

1. On the “Identity Self-Service” tab, click **Unlock Employee Account** in the menu located on the left side of your screen (this option is listed under the Directory Management category).



Welcome to the North Carolina ID System

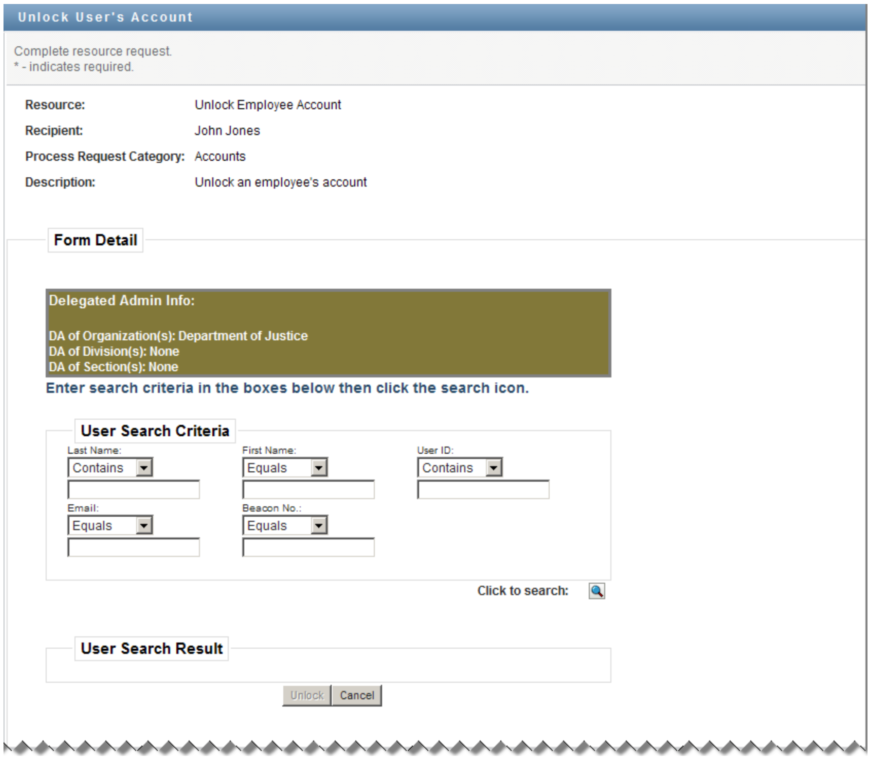
Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area
  - If you are an approver, the "Task Notifications" area shows tasks awaiting your action
  - You may need to click "Refresh" in the areas mentioned above to see the most current information.

Thank you for using the NCID System

Figure 5-27. Click on “Unlock Employee Account” Link

2. The “Unlock Employee Account” request form is displayed. You will need to search for the account you wish to unlock. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account.



Complete resource request.
* - indicates required.

Resource:	Unlock Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Unlock an employee's account

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

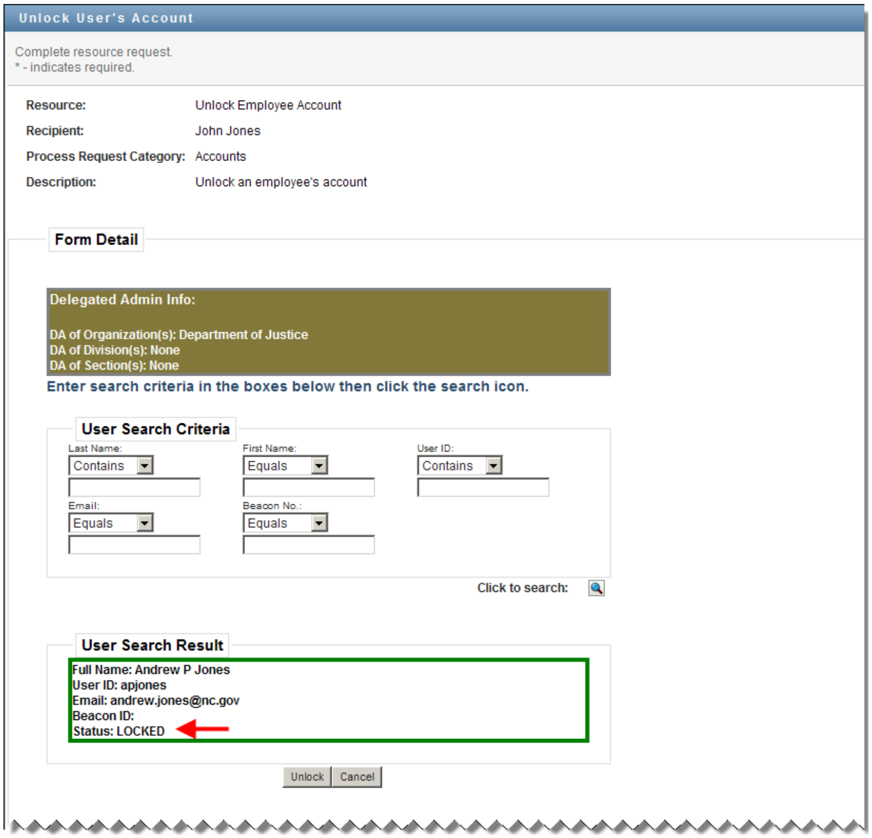
Enter search criteria in the boxes below then click the search icon.

Figure 5-28. “Unlock Employee Account” Request Form

3. Once you have selected the account, the request form is updated and displays selected attributes from the user's profile in the "User Search Result" section. You can verify this is the correct user account by checking the name displayed in the "Full Name" field, and verifying the user ID in the "User ID" field. You will also notice that the "Status" field indicates that the account is "Locked".

- **Note:** If this section is highlighted in yellow, a message will display to alert you that you do not have permission to perform the action on the account. Additionally, this section may be highlighted if the account is not locked. In this case, the "Status" field will indicate that the account is "Active".

4. If this is not the appropriate user, you can clear the fields and perform your search again.



Unlock User's Account

Complete resource request.
* - indicates required.

Resource:	Unlock Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Unlock an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

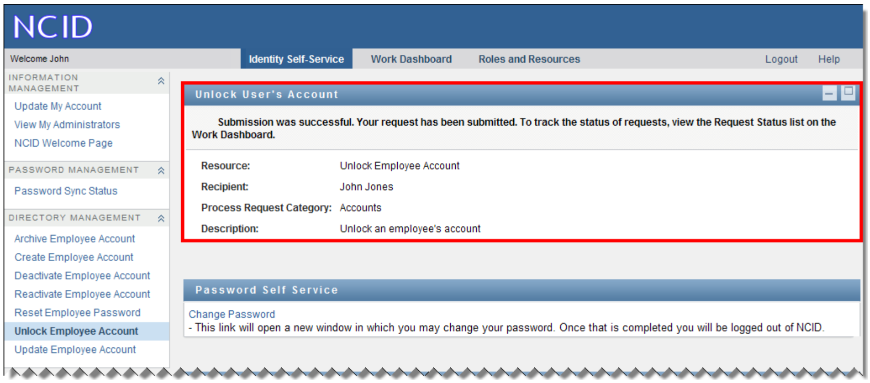
Click to search:

User Search Result

Full Name: Andrew P Jones
User ID: apjones
Email: andrew.jones@nc.gov
Beacon ID:
Status: LOCKED

Figure 5-29. Verify User Details

5. Click on **Unlock**.
6. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the "Work Dashboard" tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.



Submission was successful. Your request has been submitted. To track the status of requests, view the Request Status list on the Work Dashboard.

Resource: Unlock Employee Account
Recipient: John Jones
Process Request Category: Accounts
Description: Unlock an employee's account

- This link will open a new window in which you may change your password. Once that is completed you will be logged out of NCID.

Figure 5-30.Confirmation Message

7. Inform the user that he or she will need to log in to NCID at https://ncid.nc.gov before continuing to the application that they were trying to access.

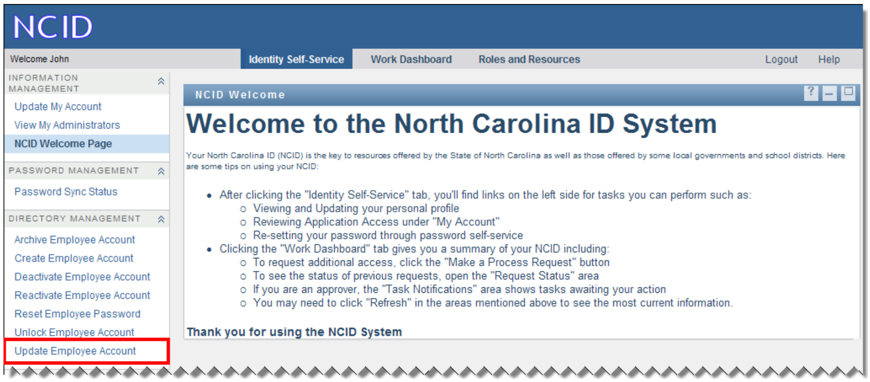
5.7 Recovering a User ID

If a user cannot remember his or her user ID, you should direct the user to the “Forgot Your User ID” self-service feature on the “Login” screen. The user will need to provide some basic information (i.e.: first name, last name) to retrieve the user ID.

If the user is unable to recover the user ID you can look it up by using the “Update Employee Account” link. Upon finding the correct account, the user ID is displayed on the form’s “Account Info” section.

To look up a user ID:

1. On the “Identity Self-Service” tab, click **Update Employee Account** in the menu located on the left side of your screen (this option is listed under the “Directory Management” category).



Welcome to the North Carolina ID System

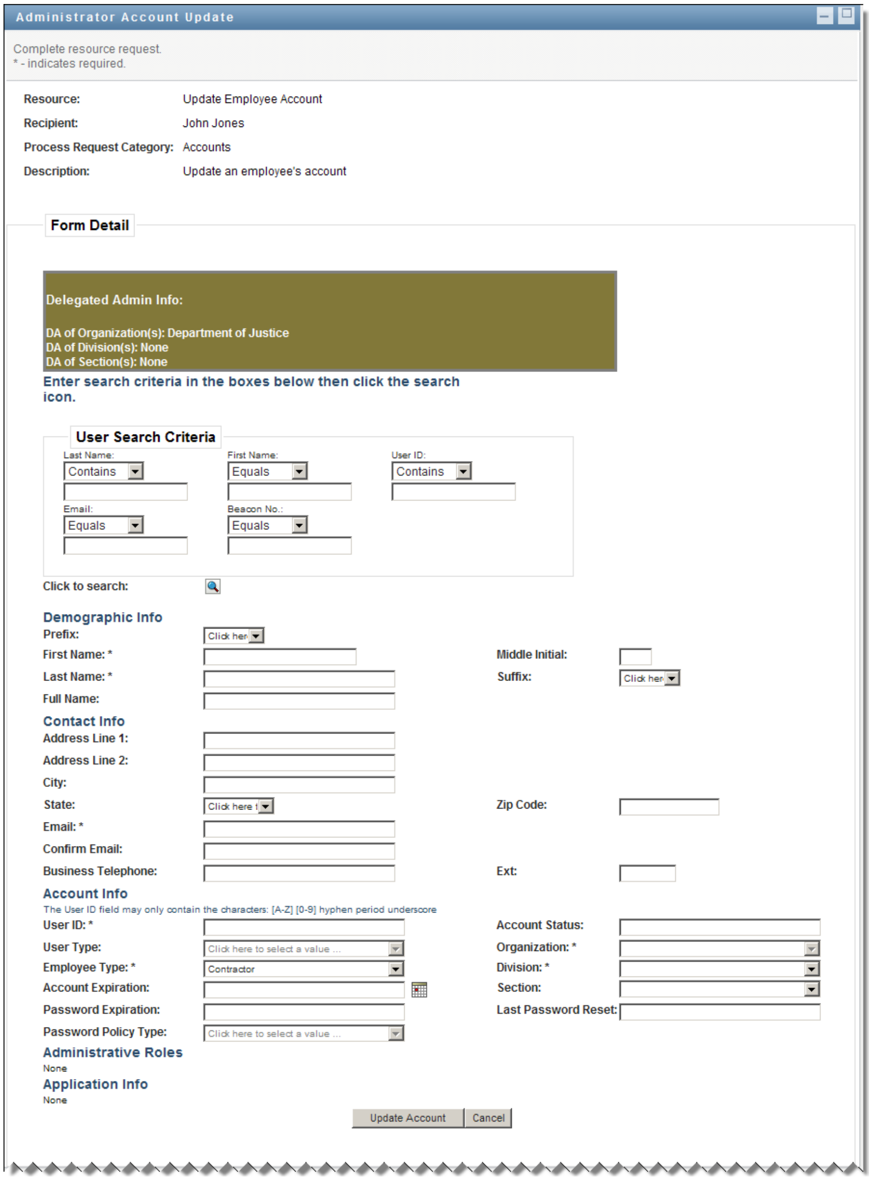
Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area
  - If you are an approver, the "Task Notifications" area shows tasks awaiting your action
  - You may need to click "Refresh" in the areas mentioned above to see the most current information.

Thank you for using the NCID System

Figure 5-31. Click on “Update Employee Account” Link

2. Look up the user’s account. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account.



Administrator Account Update

Complete resource request.
* - indicates required.

Resource:	Update Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Update an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to search:

Demographic Info
Prefix: Click her
First Name: *
Middle Initial:
Last Name: *
Suffix: Click her
Full Name:

Contact Info
Address Line 1:
Address Line 2:
City:
State: Click here t
Zip Code:
Email: *
Confirm Email:
Business Telephone:
Ext:

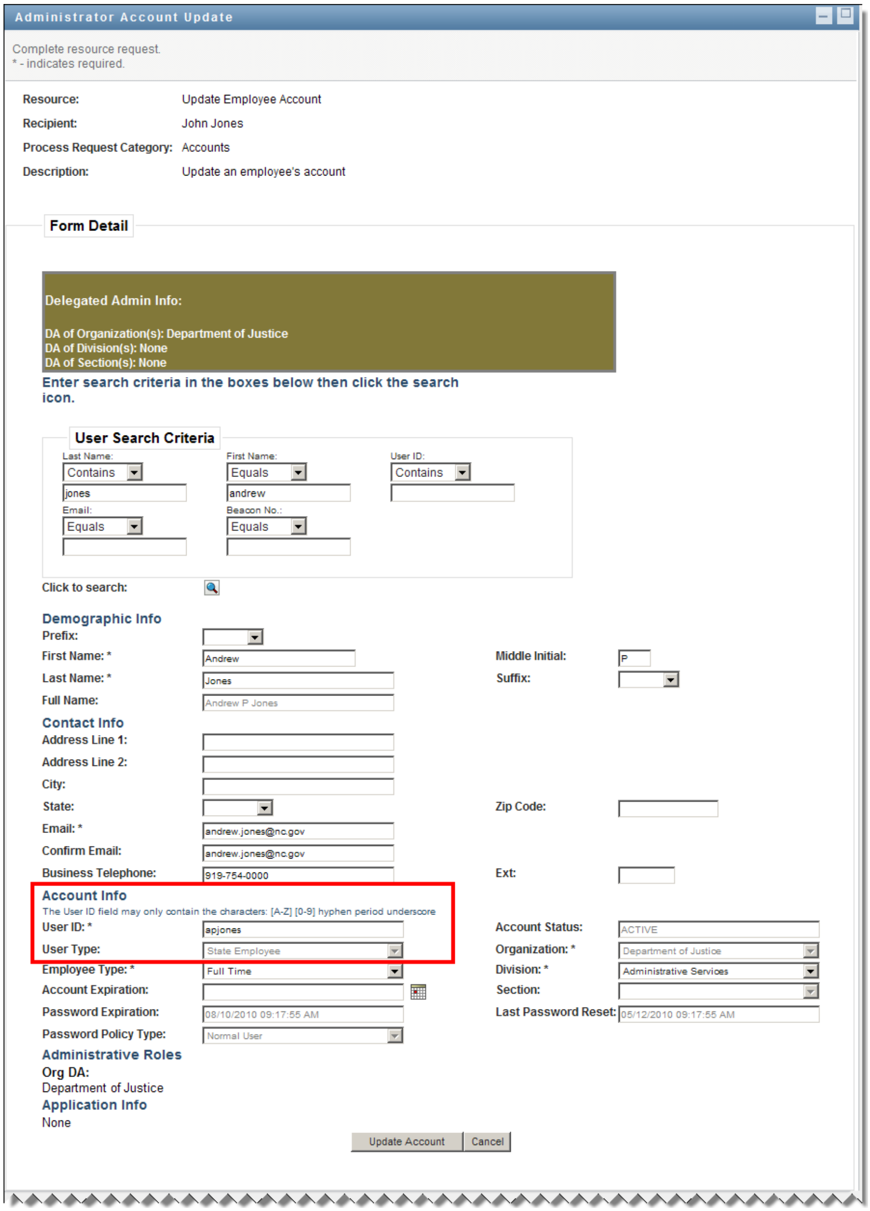
Account Info
The User ID field may only contain the characters: [A-Z] [0-9] hyphen period underscore
User ID: *
Account Status:
User Type: Click here to select a value ...
Organization: *
Employee Type: * Contractor
Division: *
Account Expiration:
Section:
Password Expiration:
Last Password Reset:
Password Policy Type: Click here to select a value ...

Administrative Roles
None

Application Info
None

Figure 5-32. "Administrator Account Update" Request Form

3. Once you have selected the account, the request form is updated and displays the user's profile. You will be able to see the user's ID in the "Account Info" section.



Administrator Account Update

Complete resource request.
* - indicates required.

Resource:	Update Employee Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Update an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): None
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains jones
First Name: Equals andrew
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to search: 🔍

Demographic Info

Prefix:			
First Name: *	Andrew	Middle Initial:	P
Last Name: *	Jones	Suffix:	
Full Name:	Andrew P Jones		

Contact Info

Address Line 1:			
Address Line 2:			
City:			
State:		Zip Code:	
Email: *	andrew.jones@nc.gov		
Confirm Email:	andrew.jones@nc.gov		
Business Telephone:	919-754-0000	Ext:	

Account Info

The User ID field may only contain the characters: [A-Z] [0-9] hyphen period underscore

User ID: *	apjones	Account Status:	ACTIVE
User Type:	State Employee	Organization: *	Department of Justice
Employee Type: *	Full Time	Division: *	Administrative Services
Account Expiration:		Section:	
Password Expiration:	08/10/2010 09:17:55 AM	Last Password Reset:	05/12/2010 09:17:55 AM
Password Policy Type:	Normal User		

Administrative Roles

Org DA:
Department of Justice

Application Info

None

Figure 5-33. View User ID in "Account Info" Section

5.8 Transferring a State User Account

Transferring a state user account to a different agency is a multi-step process performed by the user's current administrator and the administrator of the receiving agency. When the current administrator is notified that an employee is moving to another state agency, he or she will initiate the transfer request in NCID. Upon submitting the request, an email notification is sent to the receiving administrator(s) to alert him or her of the pending transfer. The receiving administrator can then either approve or deny the request. If it is approved, the transferred account maintains the user's name, user ID, password and Beacon number; however, the address and email fields are cleared and the user's previous permissions and roles are removed. If a transfer request is denied, the user account remains in the current agency, and the agency's administrator will be notified of the rejection.

Important!

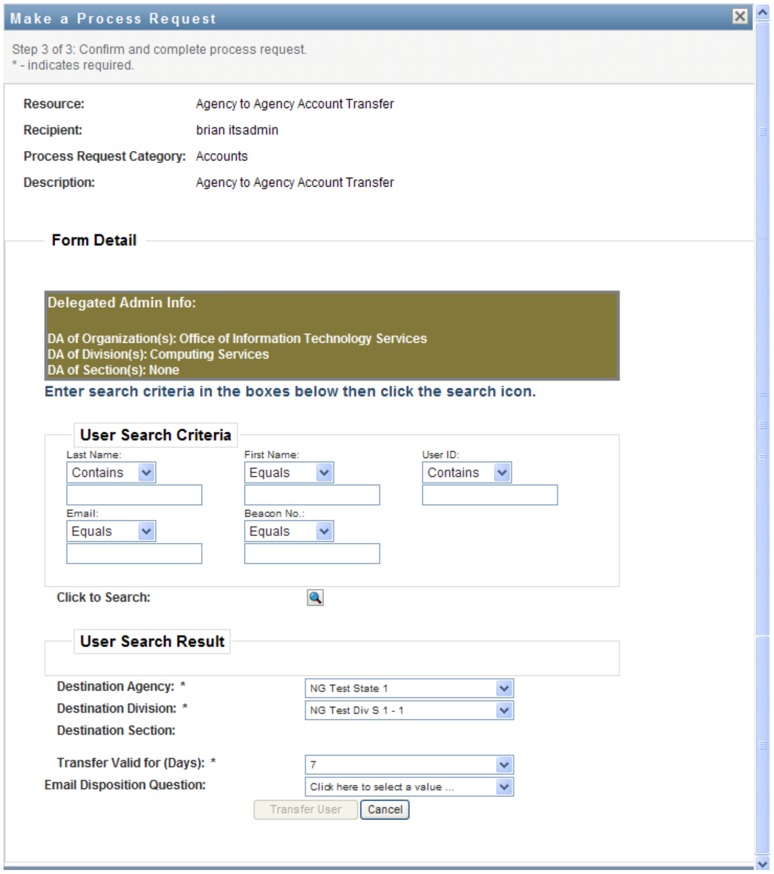
- Only delegated administrators who are state employees can perform an agency to agency transfer for users within their organization, division and/or section.
- If both agencies use Office-365, the current administrator can select what will happen to the user's email account. Upon transfer approval, a system generated email is sent to the Remedy team to open a ticket for the Unified Communications team. The Remedy ticket notifies the Unified Communications team of the transfer and indicates the action they should take on the user's email account. Actions include: delete the user's mailbox, export the mailbox items to a PST file and move the mailbox to new agency.
- A transfer request will expire if it is not approved within the time period set by the current administrator. If the receiving agency does not take action on the request, the account will remain in the current agency, and the current administrator will be notified by email of the expiration.
- Deactivated user accounts can be transferred. The account remains deactivated until the receiving administrator reactivates it.

5.8.1 Initiating a User Account Transfer to a New Agency

The following steps are performed by the employee's current administrator, and begin the transfer process.

To make an agency account transfer request:

1. On the "Work Dashboard" tab, click on the **Make a Process Request** button to display the "Make a Process Request" screen.
2. Click on **Continue** to view a list of workflow processes available to you, and select **Agency to Agency Account Transfer**.
3. The "Agency to Agency Account Transfer" request form is displayed. You will need to search for the account. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account.



Make a Process Request

Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource:	Agency to Agency Account Transfer
Recipient:	brian itsadmin
Process Request Category:	Accounts
Description:	Agency to Agency Account Transfer

Form Detail

Delegated Admin Info:

DA of Organization(s): Office of Information Technology Services
DA of Division(s): Computing Services
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to Search:

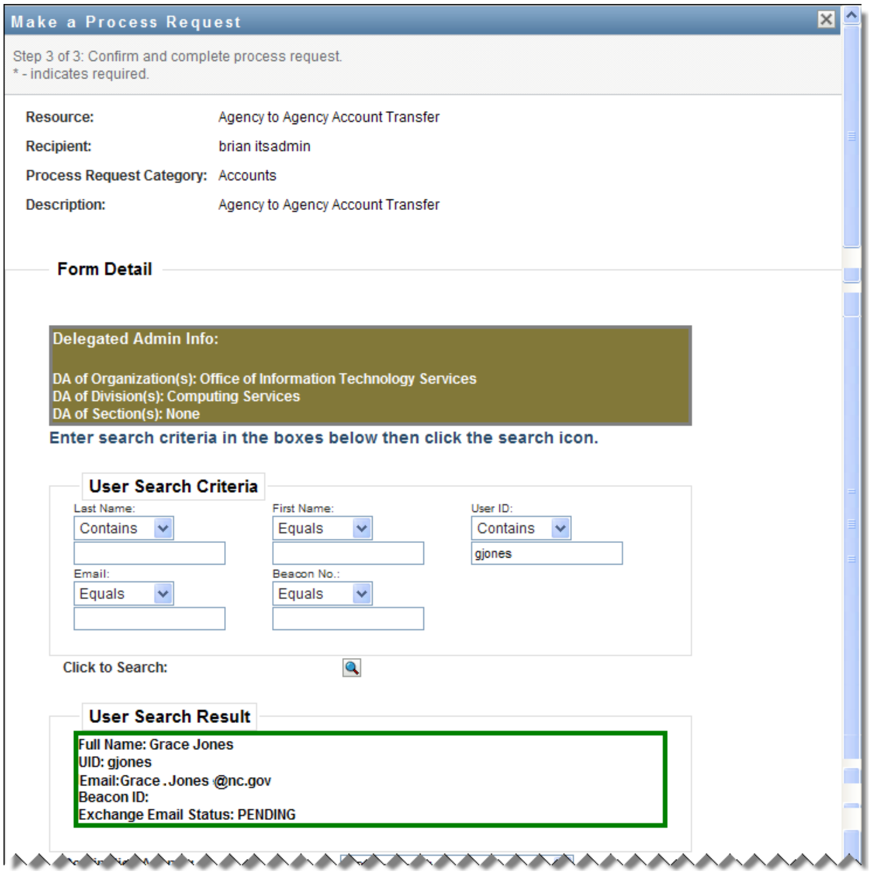
User Search Result

Destination Agency: * NG Test State 1
Destination Division: * NG Test Div S 1 - 1
Destination Section:

Transfer Valid for (Days): * 7
Email Disposition Question: Click here to select a value ...

Figure 5-34. "Agency to Agency Account Transfer" Request Form

4. Once you have selected the account, the request form is updated and displays selected attributes from the user's profile in the "User Search Result" section.
5. Verify that this is the correct user account that you wish to transfer. If this is not the appropriate user, you can clear the fields and perform your search again.



Make a Process Request

Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource:	Agency to Agency Account Transfer
Recipient:	brian itsadmin
Process Request Category:	Accounts
Description:	Agency to Agency Account Transfer

Form Detail

Delegated Admin Info:

DA of Organization(s): Office of Information Technology Services
DA of Division(s): Computing Services
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains	First Name: Equals	User ID: Contains gjones
Email: Equals	Beacon No.: Equals	

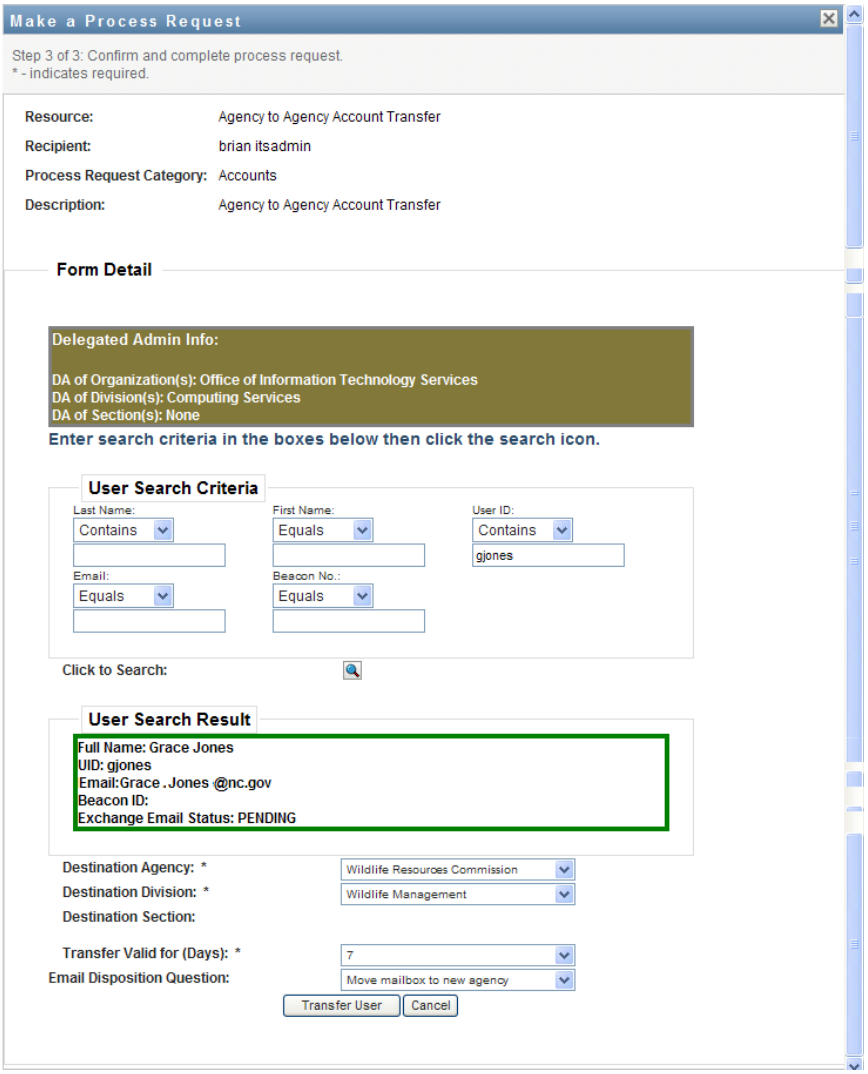
Click to Search:

User Search Result

Full Name: Grace Jones
UID: gjones
Email:Grace .Jones @nc.gov
Beacon ID:
Exchange Email Status: PENDING

Figure 5-35. Verify User Details

6. Select the appropriate destination information from the **Destination Agency, Destination Division** and **Destination Section** dropdown menus. The “Destination Section” menu is available when the user is moving to a division that has one or more sections.



Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource: Agency to Agency Account Transfer
Recipient: brian itsadmin
Process Request Category: Accounts
Description: Agency to Agency Account Transfer

Form Detail

Delegated Admin Info:

DA of Organization(s): Office of Information Technology Services
DA of Division(s): Computing Services
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains gjones
Email: Equals
Beacon No.: Equals

Click to Search:

User Search Result

Full Name: Grace Jones
UID: gjones
Email:Grace . Jones @nc.gov
Beacon ID:
Exchange Email Status: PENDING

Destination Agency: * Wildlife Resources Commission
Destination Division: * Wildlife Management
Destination Section:

Transfer Valid for (Days): * 7
Email Disposition Question: Move mailbox to new agency

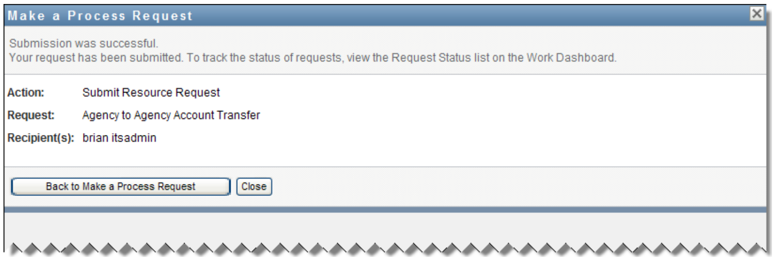
Figure 5-36. Enter New Agency Details

7. In the **Transfer Validate for (Days)** field, select the length of time the destination administrator has to approve the transfer. If it is not approved within the specified time period, the request will expire and the account will remain in the current agency. You will receive an email notification if the request expires.
8. The **Email Disposition Question** field will be available if both agencies use Office-365. You may select what will happen to the user's email account when the transfer is approved by the destination administrator. Actions include: delete the user's mailbox, export the mailbox items to a PST file and move the mailbox to new agency.

- **Note:** Upon transfer approval, a system generated email is sent to the DIT Service Desk team to open a ticket for the Unified Communications team. The ticket notifies the Office-365 team of the transfer and indicates the action they should take on the user's email account.

9. Click on Transfer User.

10. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the “Work Dashboard” tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.



Make a Process Request

Submission was successful.
Your request has been submitted. To track the status of requests, view the Request Status list on the Work Dashboard.

Action:	Submit Resource Request
Request:	Agency to Agency Account Transfer
Recipient(s):	brian itsadmin

Figure 5-37. Confirmation Message

11. An email message is sent to the receiving administrator to alert him or her that a request has been submitted which requires approval. The email indicates who submitted the transfer request and the name and user ID of the employee who is attempting to move into the agency. The email also provides two URL links to let the administrator view: (1) the details of the request in his or her task list and (2) a list of all pending requests requiring approval.

- **Note:** The receiving administrator can also look at the Work Dashboard tab to view all pending requests. Please refer to the following section for more information on viewing requests via the Work Dashboard.

5.8.2 Claiming and Approving an Agency Account Transfer

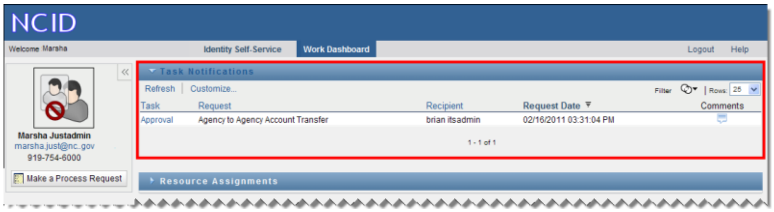
When a transfer request is submitted, the receiving administrator will receive an email notification of the employee’s pending move. The email indicates that there is a request in his or her task list which requires approval, and it also contains URL links which allow the administrator to quickly access the request or to see a list of all requests pending approval. To complete the transfer process, the administrator must retrieve (claim) the request from his or her task list and then approve it.

To claim and approve an agency account transfer request (the following steps must be performed by the receiving administrator):

1. Access the transfer request by either:
2. Clicking on the link in the notification email.

Or

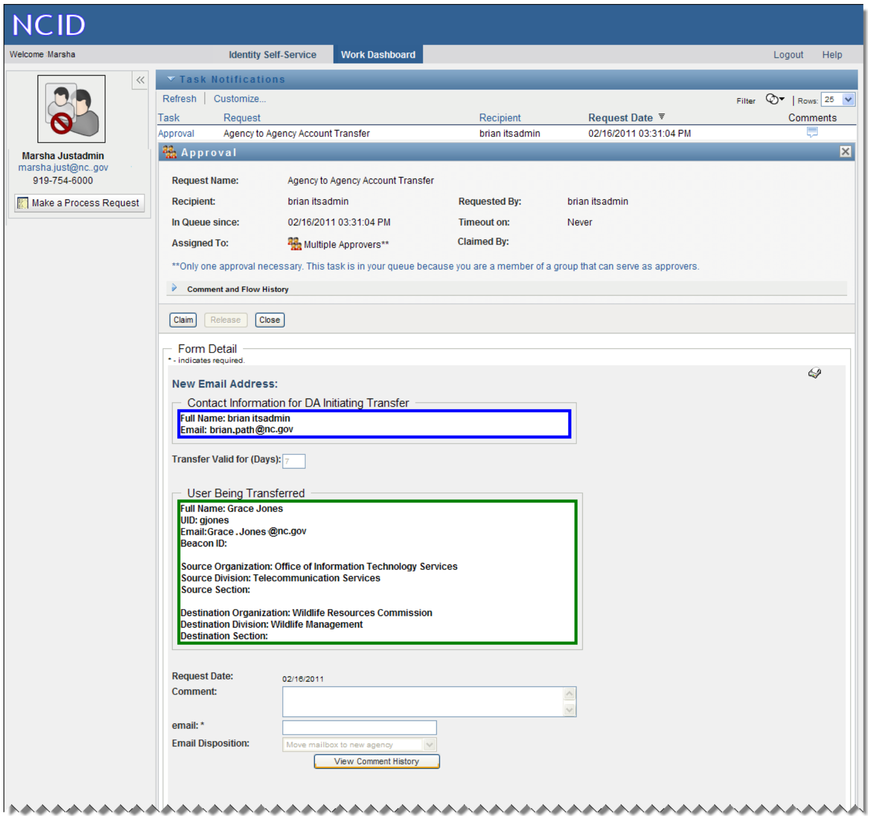
3. Moving to the “Work Dashboard” tab and clicking on the ▶ icon in front of **Task Notifications**.



Task	Request	Recipient	Request Date	Comments
Approval	Agency to Agency Account Transfer	brian itsadmin	02/16/2011 03:31:04 PM	

Figure 5-38. Viewing Transfer Request from Task List

4. A list of tasks appears in the "Task Notification" section. You can click on the appropriate task to expand the line item and view details, such as the name and email address of the administrator who initiated the transfer, the date the request was made, and information about the employee who is moving to the new agency.



Task	Request	Recipient	Request Date	Comments
Approval	Agency to Agency Account Transfer	brian itsadmin	02/16/2011 03:31:04 PM	

Request Name: Agency to Agency Account Transfer

Recipient: brian itsadmin
Requested By: brian itsadmin

In Queue since: 02/16/2011 03:31:04 PM
Timeout on: Never

Assigned To: Multiple Approvers**
Claimed By:

**Only one approval necessary. This task is in your queue because you are a member of a group that can serve as approvers.

Form Detail

* - indicates required.

New Email Address:

Contact Information for DA Initiating Transfer

Full Name: brian itsadmin
Email: brian.path@nc.gov

Transfer Valid for (Days): 7

User Being Transferred

Full Name: Grace Jones
UID: gjones
Email:Grace .Jones @nc.gov
Beacon ID:

Source Organization: Office of Information Technology Services
Source Division: Telecommunication Services
Source Section:

Destination Organization: Wildlife Resources Commission
Destination Division: Wildlife Management
Destination Section:

Request Date: 02/16/2011

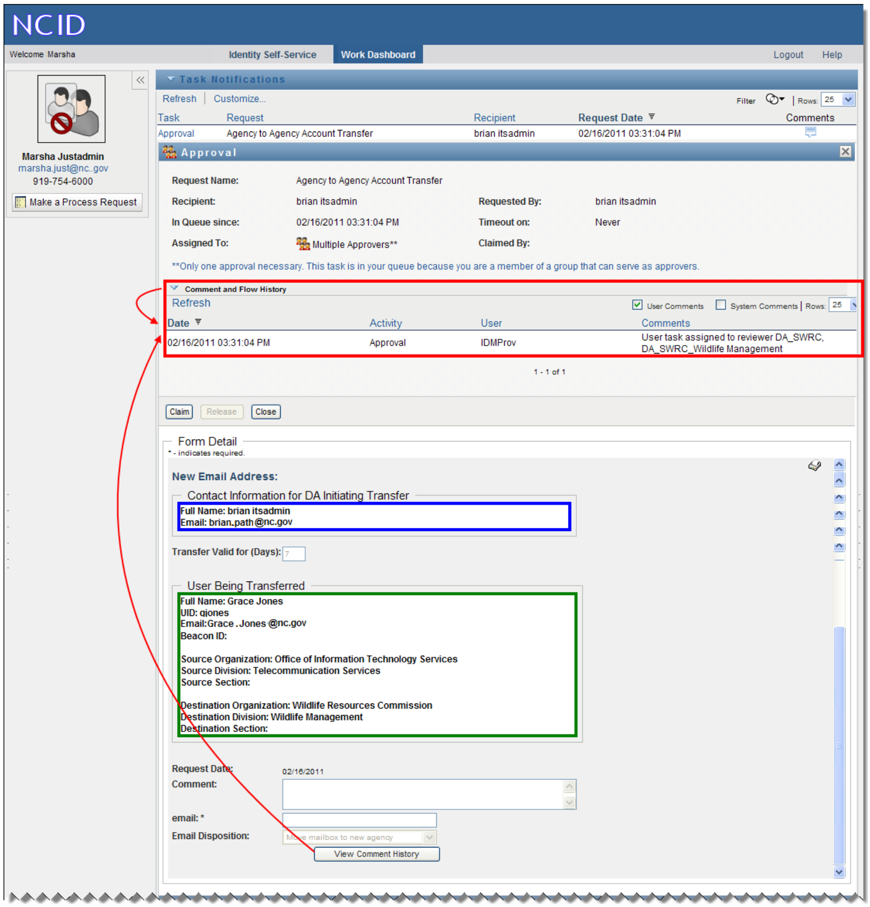
Comment:

email: *

Email Disposition: Move mailbox to new agency

Figure 5-39. Viewing Request that Requires Approval

5. You may also view a list of steps performed during the transfer process by clicking on the **View Comment History** button.



Task	Request	Recipient	Request Date	Comments
Approval	Agency to Agency Account Transfer	brian itsadmin	02/16/2011 03:31:04 PM	

Request Name: Agency to Agency Account Transfer

Recipient: brian itsadmin

Requested By: brian itsadmin

In Queue since: 02/16/2011 03:31:04 PM

Timeout on: Never

Assigned To: Multiple Approvers**

Claimed By:

**Only one approval necessary. This task is in your queue because you are a member of a group that can serve as approvers.

Comment and Flow History

Refresh ☑ User Comments ☐ System Comments | Rows: 25

Date	Activity	User	Comments
02/16/2011 03:31:04 PM	Approval	IDMProv	User task assigned to reviewer DA_SWRC, DA_SWRC_Wildlife Management

1 - 1 of 1

Form Detail

* - indicates required.

New Email Address:

Contact Information for DA Initiating Transfer

Full Name: brian itsadmin
Email: brian.path@nc.gov

Transfer Valid for (Days): 7

User Being Transferred

Full Name: Grace Jones
UID: gjones
Email:Grace.Jones@nc.gov
Beacon ID:

Source Organization: Office of Information Technology Services
Source Division: Telecommunication Services
Source Section:

Destination Organization: Wildlife Resources Commission
Destination Division: Wildlife Management
Destination Section:

Request Date: 02/16/2011

Comment:

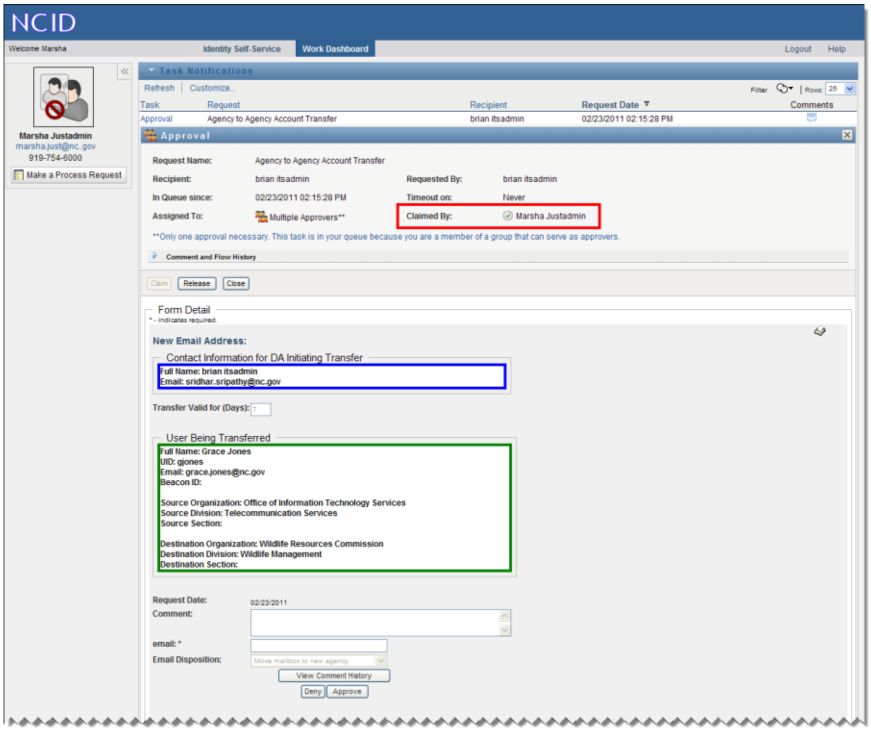
email: *

Email Disposition: Move mailbox to new agency

Figure 5-40. Viewing Task History

6. In some cases, there are multiple administrators available to approve a transfer. Click on the **Claim** button which will alert any other approvers that you are granting the approval. The screen will display your name next to the "Claimed By" field to indicate that you have claimed the task.

- **Note:** Should you change your mind, you can release the task back to the task list by clicking on the **Release** button.



Task	Request	Recipient	Request Date	Comments
Approval	Agency to Agency Account Transfer	brian itsadmin	02/23/2011 02:15:28 PM	

Request Name: Agency to Agency Account Transfer

Recipient: brian itsadmin
Requested By: brian itsadmin

In Queue since: 02/23/2011 02:15:28 PM
Timeout on: Never

Assigned To: Multiple Approvers**
Claimed By: Marsha Justadmin

**Only one approval necessary. This task is in your queue because you are a member of a group that can serve as approvers.

* - indicates required.

New Email Address:

Contact Information for DA Initiating Transfer
Full Name: brian itsadmin
Email: sridhar.sripathy@nc.gov

Transfer Valid for (Days): 7

User Being Transferred
Full Name: Grace Jones
UID: gjones
Email: grace.jones@nc.gov
Beacon ID:

Source Organization: Office of Information Technology Services
Source Division: Telecommunication Services
Source Section:

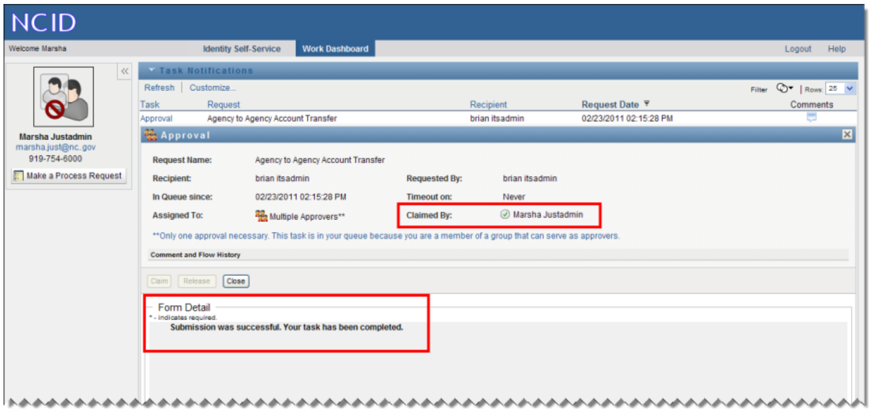
Destination Organization: Wildlife Resources Commission
Destination Division: Wildlife Management
Destination Section:

Request Date: 02/23/2011
Comment:
email: *
Email Disposition: Move mailbox to new agency

Figure 5-41. Example of a “Claimed” Task

7. After claiming the task, you may enter notes or remarks in the “Comments” textbox. You will need to enter an email address for the user in the “Email” field. You can enter the user’s new address, if it is known, or you can enter what you anticipate it to be. (Note: An incorrect email address will not impact the completion of the transfer request. This field can be updated on the user’s account profile, if the email is incorrect or changes.)
8. Two additional action buttons are available at the bottom of the window: **Deny** and **Approve**. Click on **Approve** to complete the transfer process. Upon approval, the task list is refreshed and indicates that the request was successful.
9. You can update the user’s new business telephone number on his or her profile, if it is known.

- **Note:** You can cancel a request by clicking on **Deny**, for example, if you were notified that the user will not be transferring into your agency. The employee’s current administrator would receive an email notification, and the transfer would be cancelled.



Task	Request	Recipient	Request Date	Comments
Approval	Agency to Agency Account Transfer	brian itsadmin	02/23/2011 02:15:28 PM	

Request Name: Agency to Agency Account Transfer
Recipient: brian itsadmin
Requested By: brian itsadmin
In Queue since: 02/23/2011 02:15:28 PM
Timeout on: Never
Assigned To: Multiple Approvers**
Claimed By: Marsha Justadmin

**Only one approval necessary. This task is in your queue because you are a member of a group that can serve as approvers.

Comment and Flow History

Form Detail
* - indicates required.
Submission was successful. Your task has been completed.

Figure 5-42.Approval for Transfer Successful

5.8.3 Cancelling an Agency Account Transfer

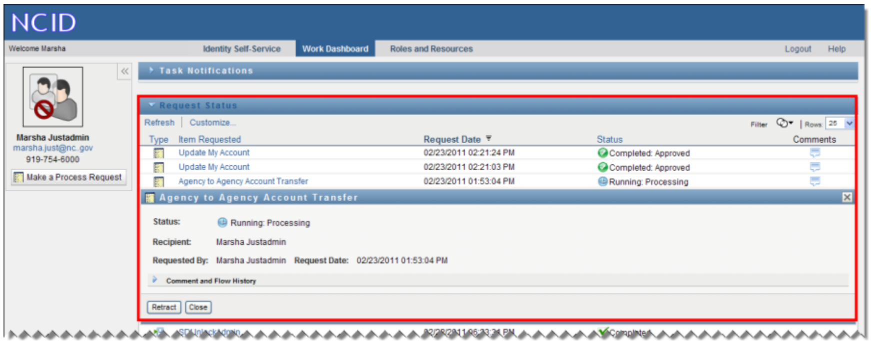
A transfer request can be cancelled by the employee's current administrator if it has not been approved by an administrator at the destination agency.

The request will remain on the current administrator's Work Dashboard tab until the transfer is approved. From the Work Dashboard, the current administrator can review the status of the pending request, as well as retract the request if the transfer needs to be cancelled.

- **Note:** A transfer request which has been "claimed" by the receiving administrator may still be cancelled by the employee's current administrator.

To cancel an agency account transfer request (the following steps must be performed by the administrator who initiated the transfer request):

1. On the "Work Dashboard" tab, click on the ▶ icon in front of **Request Status**.
2. A list of process requests is displayed. Click on the appropriate **Agency to Agency Account Transfer** request to expand the line item and view its details.



Type	Item Requested	Request Date	Status	Comments
	Update My Account	02/23/2011 02:21:24 PM	Completed: Approved	
	Update My Account	02/23/2011 02:21:03 PM	Completed: Approved	
	Agency to Agency Account Transfer	02/23/2011 01:53:04 PM	Running: Processing	

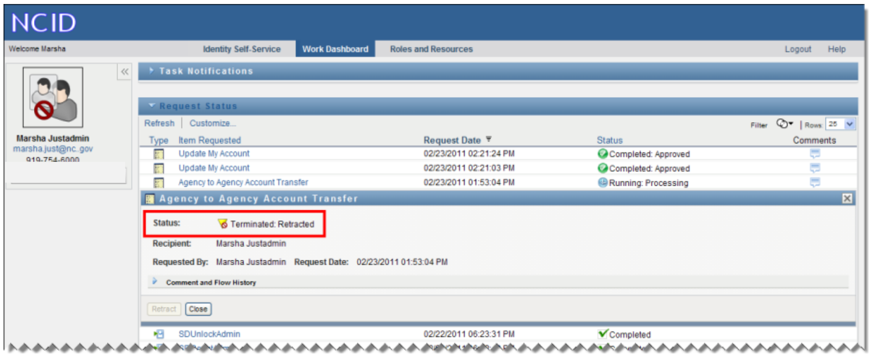
Status: Running: Processing
Recipient: Marsha Justadmin
Requested By: Marsha Justadmin Request Date: 02/23/2011 01:53:04 PM

Comment and Flow History

Figure 5-43. Viewing the Agency Account Transfer Details

3. Click on **Retract**.
4. A message displays to verify that you want to retract the request. Click on **OK** to continue the cancellation, or click on **Cancel** to keep the request.

5. Upon clicking OK, the status is updated to “Terminated: Retracted”, and the request is removed from the new administrator’s task list.



Type	Item Requested	Request Date	Status	Comments
	Update My Account	02/23/2011 02:21:24 PM	Completed: Approved	
	Update My Account	02/23/2011 02:21:03 PM	Completed: Approved	
	Agency to Agency Account Transfer	02/23/2011 01:53:04 PM	Running: Processing	
	SDUnlockAdmin	02/22/2011 06:23:31 PM	Completed	

Agency to Agency Account Transfer

Status: Terminated: Retracted

Recipient: Marsha Justadmin

Requested By: Marsha Justadmin Request Date: 02/23/2011 01:53:04 PM

Comment and Flow History

Figure 5-44. Viewing Terminated:Retracted Transfer Status

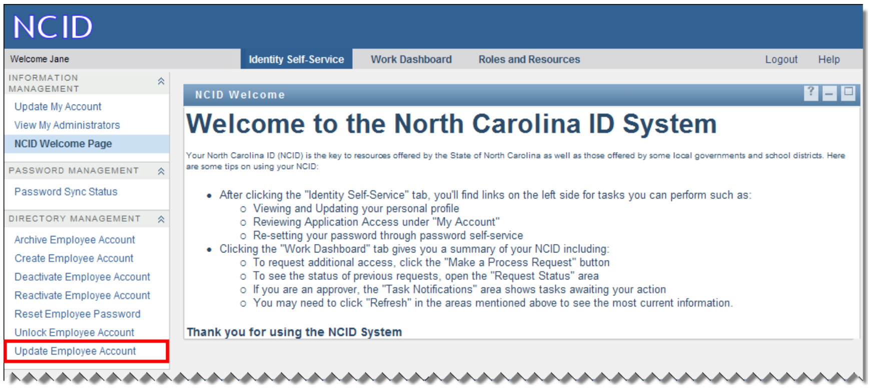
5.9 Transferring a State User Account (Intra-Agency)

If a state employee moves to another division within his or her agency, you can move the user by specifying the new division on the user’s account profile.

- **Note:** An intra-agency transfer does not affect linked email accounts since this type of transfer is a “move” within the same agency.

To transfer a user account within an agency:

1. On the “Identity Self-Service” tab, click **Update Employee Account** in the menu located on the left side of your screen (this option is listed under the “Directory Management” category).



Welcome to the North Carolina ID System

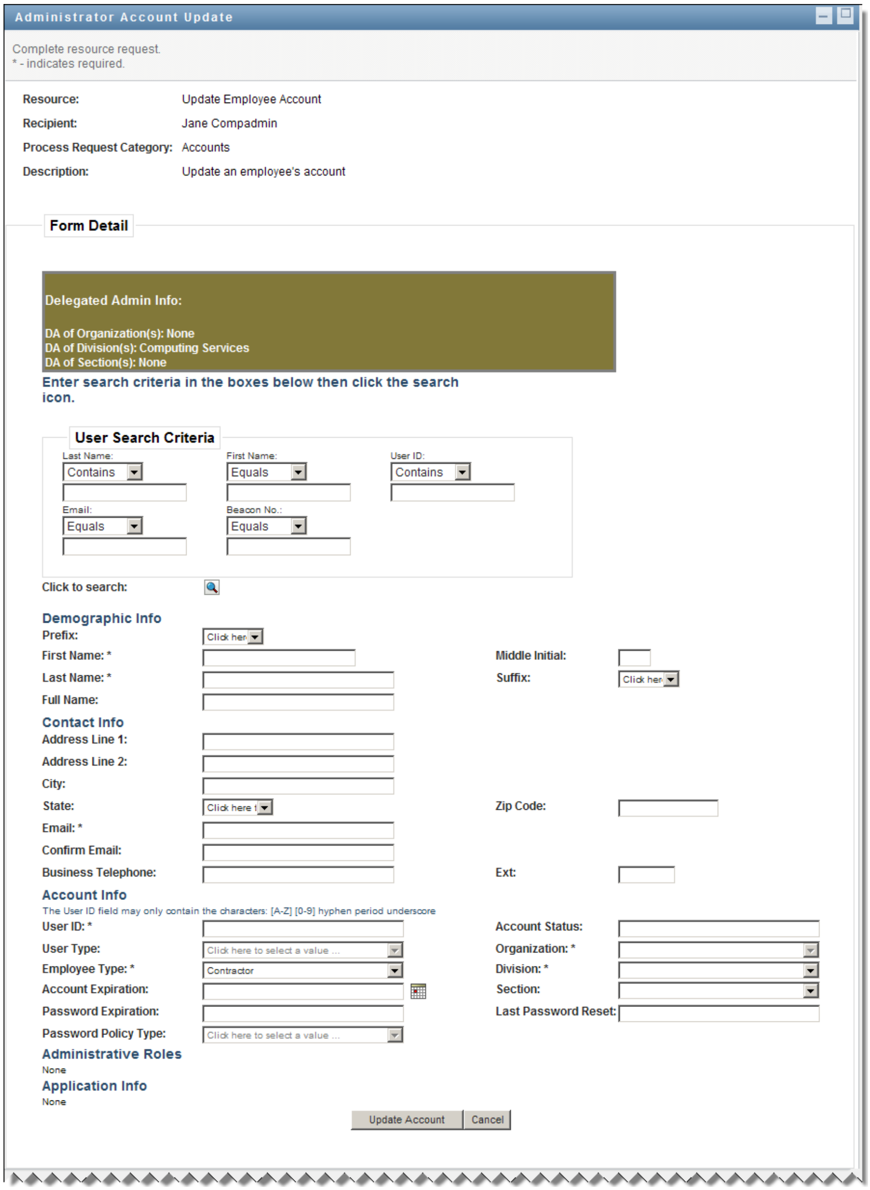
Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

- After clicking the "Identity Self-Service" tab, you'll find links on the left side for tasks you can perform such as:
  - Viewing and Updating your personal profile
  - Reviewing Application Access under "My Account"
  - Re-setting your password through password self-service
- Clicking the "Work Dashboard" tab gives you a summary of your NCID including:
  - To request additional access, click the "Make a Process Request" button
  - To see the status of previous requests, open the "Request Status" area
  - If you are an approver, the "Task Notifications" area shows tasks awaiting your action
  - You may need to click "Refresh" in the areas mentioned above to see the most current information.

Thank you for using the NCID System

Figure 5-45. Click on “Update Employee Account” Link

2. The “Administrator Account Update” request form is displayed. You will need to search for the account you wish to modify. Please refer to the Searching for a User Account section on page 29 for details on how to look up a user account.



Complete resource request.
* - indicates required.

Resource:	Update Employee Account
Recipient:	Jane Compadmin
Process Request Category:	Accounts
Description:	Update an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): None
DA of Division(s): Computing Services
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to search:

Demographic Info

Prefix: Click her
First Name: *
Middle Initial:
Last Name: *
Suffix: Click her
Full Name:

Contact Info

Address Line 1:
Address Line 2:
City:
State: Click here t
Zip Code:
Email: *
Confirm Email:
Business Telephone:
Ext:

Account Info

The User ID field may only contain the characters: [A-Z] [0-9] hyphen period underscore

User ID: *
Account Status:
User Type: Click here to select a value ...
Organization: *
Employee Type: * Contractor
Division: *
Account Expiration:
Section:
Password Expiration:
Last Password Reset:
Password Policy Type: Click here to select a value ...

Administrative Roles

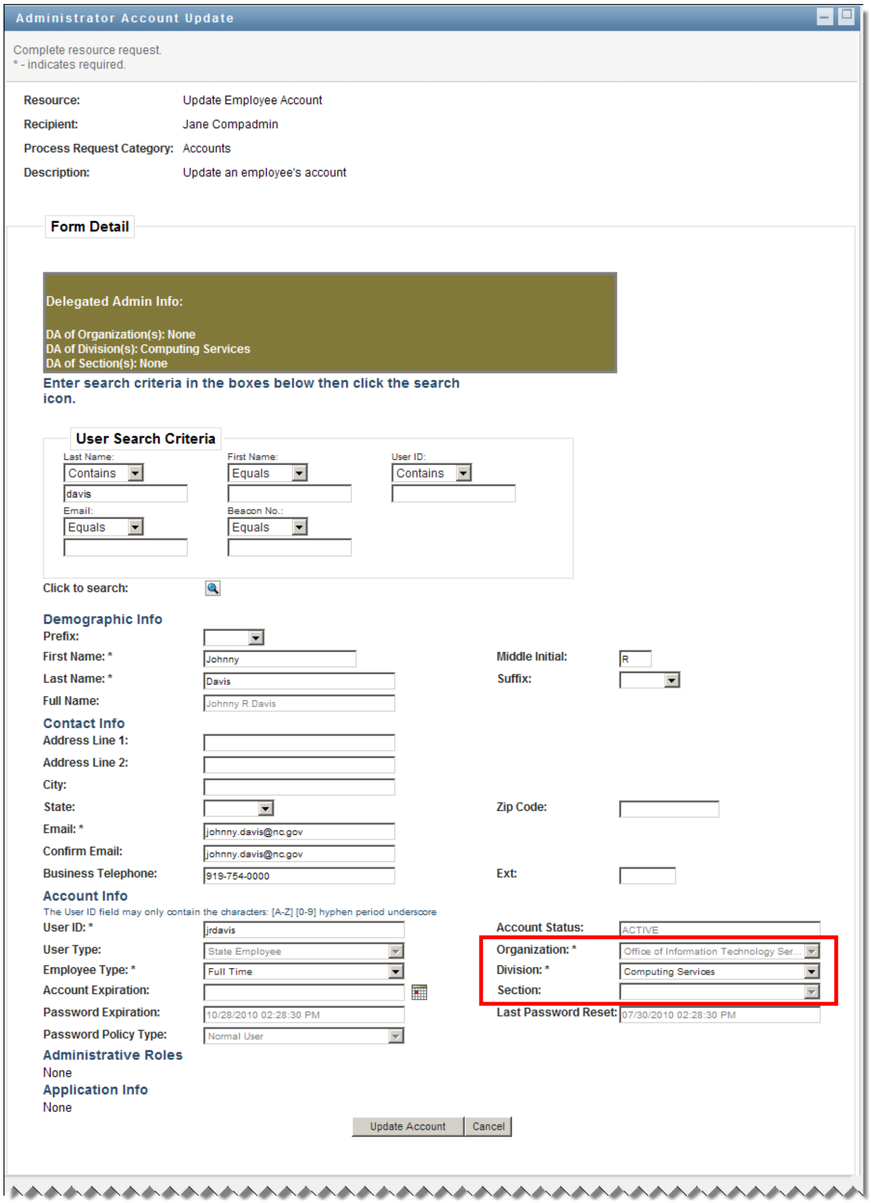
None

Application Info

None

Figure 5-46. "Administrator Account Update" Request Form

3. Once you have selected the account, the request form is updated and displays the user's profile.
4. Verify that this is the correct user account that you wish to modify. If this is not the appropriate user, you can clear the fields and perform your search again.
5. From the **Division** and/or **Section** dropdown menus, select the name(s) of the division and/or section the user is moving to and click on **Update Account**.



Administrator Account Update

Complete resource request.
* - indicates required.

Resource:	Update Employee Account
Recipient:	Jane Compadmin
Process Request Category:	Accounts
Description:	Update an employee's account

Form Detail

Delegated Admin Info:

DA of Organization(s): None
DA of Division(s): Computing Services
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains davis
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to search:

Demographic Info

Prefix:			
First Name: *	Johnny	Middle Initial:	R
Last Name: *	Davis	Suffix:	
Full Name:	Johnny R Davis		

Contact Info

Address Line 1:			
Address Line 2:			
City:			
State:		Zip Code:	
Email: *	johnny.davis@nc.gov		
Confirm Email:	johnny.davis@nc.gov		
Business Telephone:	919-754-0000	Ext:	

Account Info

The User ID field may only contain the characters: [A-Z] [0-9] hyphen period underscore

User ID: *	jrdavis	Account Status:	ACTIVE
User Type:	State Employee	Organization: *	Office of Information Technology Ser...
Employee Type: *	Full Time	Division: *	Computing Services
Account Expiration:		Section:	
Password Expiration:	10/28/2010 02:28:30 PM	Last Password Reset:	07/30/2010 02:28:30 PM
Password Policy Type:	Normal User		

Administrative Roles
None

Application Info
None

Figure 5-47. Select New Division and Section

6. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the “Work Dashboard” tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.

This page was intentionally left blank

6 Using the Work Dashboard

The Work Dashboard tab provides you with a centralized area to manage user accounts. From this tab you can make a process request from a list of actions that you are permitted to perform, and then view the details and status of the requests you made. Additionally, you can access tasks that have been assigned to you which require your approval, for example, state agency-to-agency employee transfer requests.

6.1 Work Dashboard Overview

Before we introduce the features and functionalities found on the Work Dashboard tab, this section will familiarize you with the tab's main components. The following figure illustrates an example of the Work Dashboard and identifies its components.

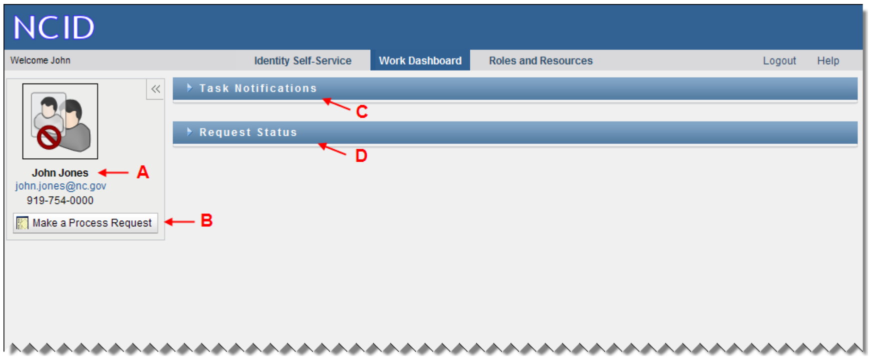


Figure 6-1. Example of the Work Dashboard Tab

A This section displays your name and contact information.

B The Make a Process Request button allows you to access a list of actions that you can perform on a user account (i.e.: Deactivate an Employee Account, Transfer an Employee Account, etc).

C The Task Notifications section allows you to view and work on tasks that have been assigned to you.

D The Request Status section allows you to see the details and status of requests you have made.

6.2 Managing Tasks

The "Task Notifications" section is used when you need to access transfer requests for state employees moving into your agency. Clicking on the ▶ icon in front of **Task Notifications** will expand the section and show a list of transfer requests requiring your approval. For information on how this section is used to view and work with transfer requests, please refer to the *Transferring a State User Account* section on page 53.

6.3 Making a Process Request

The Work Dashboard allows you to manage user accounts by making a process request from a comprehensive list of actions which are available to you. Upon selecting an action the appropriate process request form is displayed and lets you specify the information needed to complete the request.

- **Note:** Depending on how your application has been configured, some of actions on the Work Dashboard tab might be available to you as *links* on the Identity Self-Service tab.

To make a process request:

1. On the "Work Dashboard" tab, click on the **Make a Process Request** Make a Process Request button located on the left side of the screen to begin the workflow process.

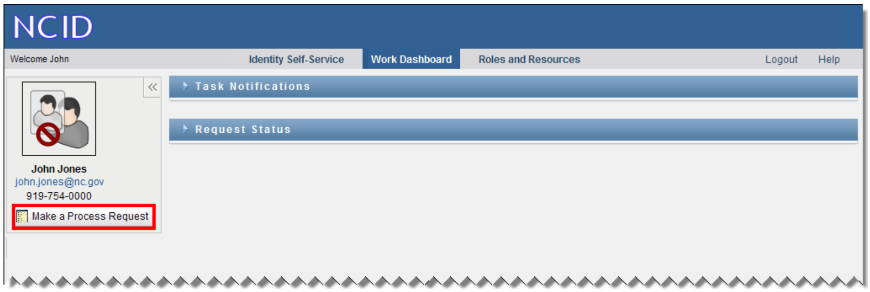
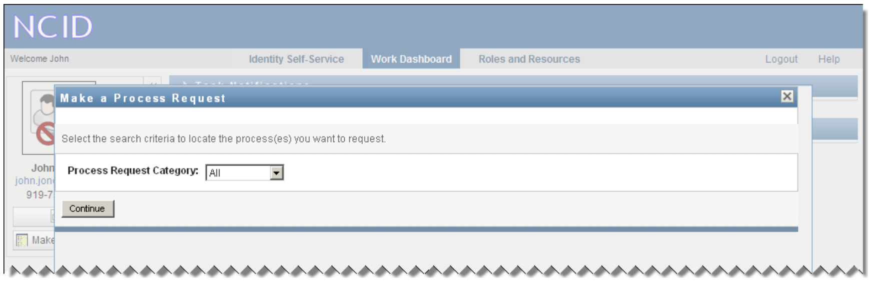


Figure 6-2. Click on "Make a Process Request"

2. The "Make a Process Request" screen is displayed. The "Process Request Category" dropdown menu lets you search by category for the request you want to make.

- **Note:** A *category* is a way to organize requests. Currently, requests are organized under the "Accounts" and "Roles" categories.

3. By default, **All** is displayed in the menu. You can accept this value or you can select **Accounts** to return a filtered list of process requests used for managing user accounts.
4. Click on **Continue**.

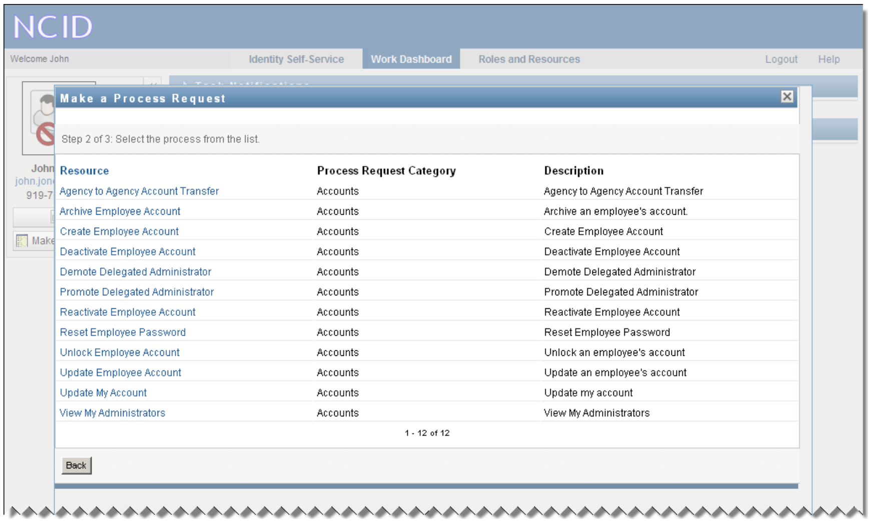


Select the search criteria to locate the process(es) you want to request.

Process Request Category: All

Figure 6-3. Select a Process Request Category

5. The following screen alphabetically displays a list of process requests that are available to you. Click on the appropriate selection to access its process request form.



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
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 - 12 of 12

Figure 6-4. List of Available Process Requests

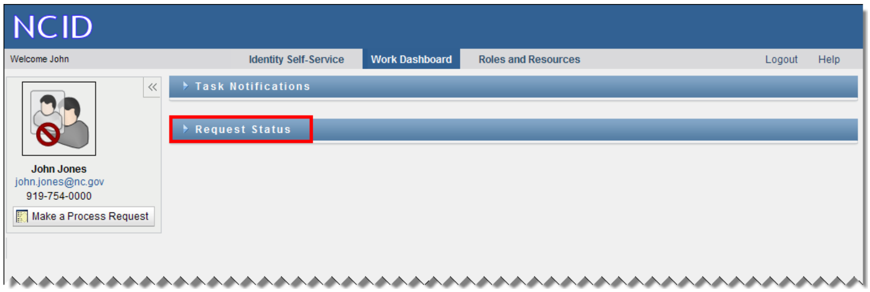
Please refer to the *Managing User Accounts* section on page 27 for information on how to work with each process request form.

6.4 Checking the Status of a Process Request

The "Request Status" section on the Work Dashboard tab allows you to view the details and status of process requests you made. This feature is helpful if there is a problem with a request and you need to troubleshoot the issues.

To check the status of a request:

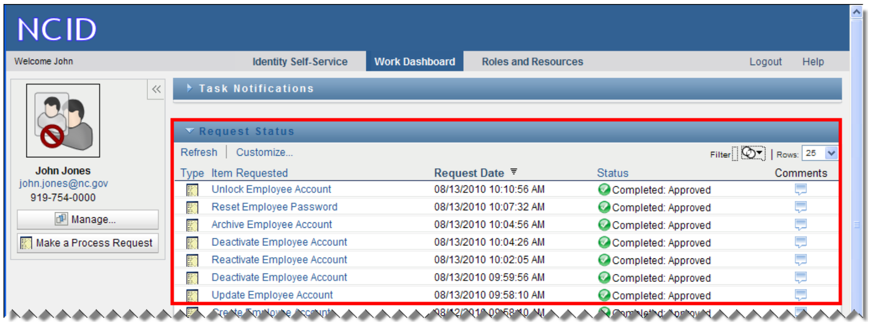
1. On the "Work Dashboard" tab, click on the ▶ icon in front of **Request Status**.



John Jones
john.jones@nc.gov
919-754-0000

Figure 6-5. Click on "Request Status"

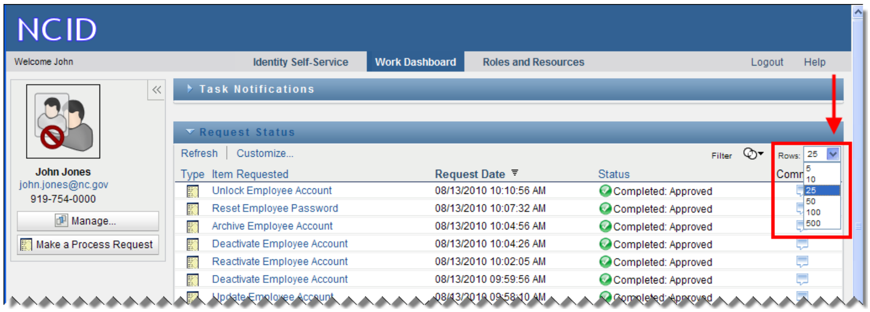
2. A list of process requests is displayed. Requested items are displayed chronologically from the most recent request. You may resort the list by "Item Requested" or by "Status".



Type	Item Requested	Request Date	Status	Comments
	Unlock Employee Account	08/13/2010 10:10:56 AM	Completed: Approved	
	Reset Employee Password	08/13/2010 10:07:32 AM	Completed: Approved	
	Archive Employee Account	08/13/2010 10:04:56 AM	Completed: Approved	
	Deactivate Employee Account	08/13/2010 10:04:26 AM	Completed: Approved	
	Reactivate Employee Account	08/13/2010 10:02:05 AM	Completed: Approved	
	Deactivate Employee Account	08/13/2010 09:59:56 AM	Completed: Approved	
	Update Employee Account	08/13/2010 09:58:10 AM	Completed: Approved	

Figure 6-6. List of Requested Items

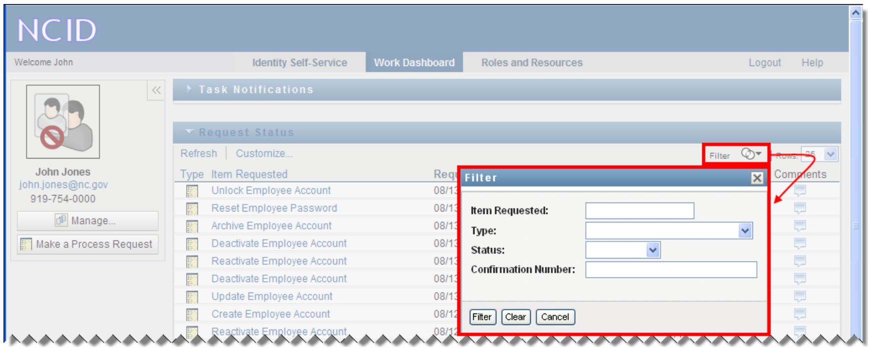
3. By default, this screen displays up to 25 requests at a time. You may change the number by clicking on the **Rows** dropdown menu and choosing from one of the following values: 5, 15, 25, 50, 100 and 500.



Type	Item Requested	Request Date	Status	Comm
	Unlock Employee Account	08/13/2010 10:10:56 AM	Completed: Approved	
	Reset Employee Password	08/13/2010 10:07:32 AM	Completed: Approved	
	Archive Employee Account	08/13/2010 10:04:56 AM	Completed: Approved	
	Deactivate Employee Account	08/13/2010 10:04:26 AM	Completed: Approved	
	Reactivate Employee Account	08/13/2010 10:02:05 AM	Completed: Approved	
	Deactivate Employee Account	08/13/2010 09:59:56 AM	Completed: Approved	
	Update Employee Account	08/13/2010 09:58:10 AM	Completed: Approved	

Figure 6-7. Change Row Display

4. In addition, you may filter the list of requests by its name, type or status by clicking on the **Filter** icon. This is helpful if, for example, you would like to see any transfer requests which are still processing or which have been retracted.

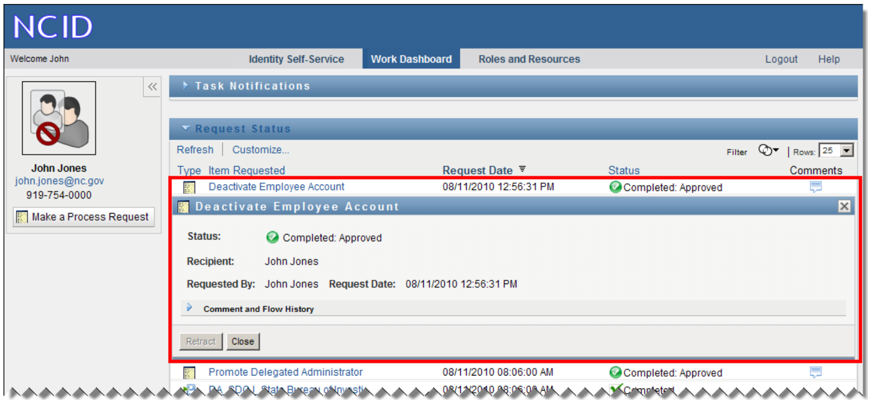


Type	Item Requested	Req
	Unlock Employee Account	08/13
	Reset Employee Password	08/13
	Archive Employee Account	08/13
	Deactivate Employee Account	08/13
	Reactivate Employee Account	08/13
	Deactivate Employee Account	08/13
	Update Employee Account	08/13
	Create Employee Account	08/12
	Reactivate Employee Account	08/12

Item Requested:
Type:
Status:
Confirmation Number:

Figure 6-8. Set Filter Options

5. To view details about a particular request, click on its name. The line item expands and shows details such as the date and time the request was initiated, the recipient’s name and the current state of the request.



John Jones
john.jones@nc.gov
919-754-0000

Type	Item Requested	Request Date	Status	Comments
	Deactivate Employee Account	08/11/2010 12:56:31 PM	Completed: Approved	
	Promote Delegated Administrator	08/11/2010 08:06:00 AM	Completed: Approved	
	DA, SDOI, State Bureau of Investi	08/11/2010 08:06:00 AM	Completed	

Deactivate Employee Account

Status: Completed: Approved

Recipient: John Jones

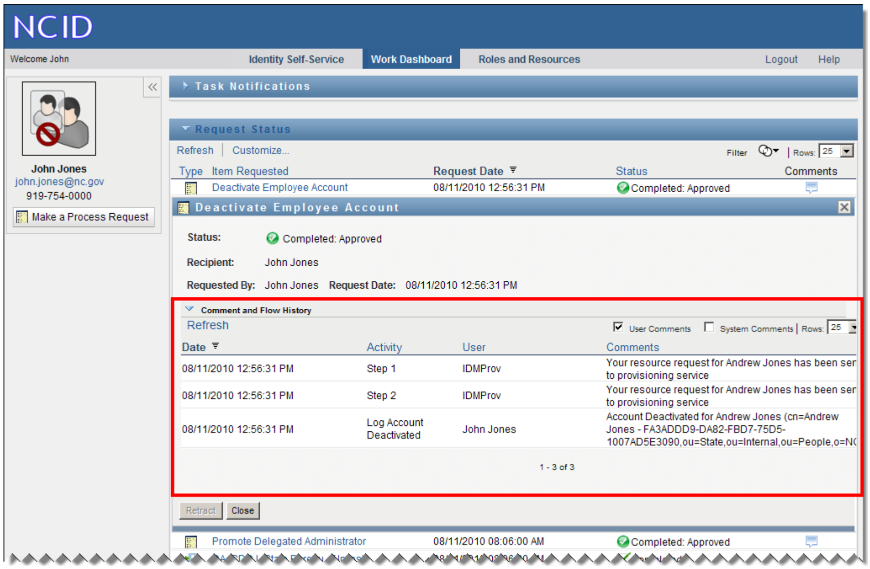
Requested By: John Jones Request Date: 08/11/2010 12:56:31 PM

Comment and Flow History

Figure 6-9.Request Details

6. You can view additional details about a request by clicking on the ▶ icon next to **Comment and Flow History**. The view expands to let you see comments for each activity associated with the request. By default, user comments are displayed. If there is a problem with a request, you might want to see system comments to help troubleshoot the issue. Click on the **System Comments** checkbox to turn on this feature.
7. The following table provides a description of the information displayed in the Comment and Flow History section.

Column Heading	Description
Date	Displays the date and time when each comment was added.
Activity	The name of the activity to which each comment applies.
User	The name of the user who made the activity. If an activity was generated automatically by the system, the following is displayed in the User column: `IDMProv`.
Comments	Summarizes the activity and includes the name of the user who is the currently assigned to the activity. If the System Comments checkbox is enabled, this column will indicate what action was taken for the activity.



John Jones
john.jones@nc.gov
919-754-0000

Request Status

Refresh | Customize... Rows: 25

Type	Item Requested	Request Date	Status	Comments
	Deactivate Employee Account	08/11/2010 12:56:31 PM	Completed: Approved	

Deactivate Employee Account

Status: Completed: Approved

Recipient: John Jones

Requested By: John Jones Request Date: 08/11/2010 12:56:31 PM

Comment and Flow History

Refresh ☑ User Comments ☐ System Comments | Rows: 25

Date	Activity	User	Comments
08/11/2010 12:56:31 PM	Step 1	IDMProv	Your resource request for Andrew Jones has been ser to provisioning service
08/11/2010 12:56:31 PM	Step 2	IDMProv	Your resource request for Andrew Jones has been ser to provisioning service
08/11/2010 12:56:31 PM	Log Account Deactivated	John Jones	Account Deactivated for Andrew Jones (cn=Andrew Jones - FA3ADDD9-DA82-FBD7-75D5-1007AD5E3090,ou=State,ou=Internal,ou=People,o=N(

1 - 3 of 3

	Promote Delegated Administrator	08/11/2010 08:06:00 AM	Completed: Approved	

Figure 6-10.Comment and Flow History

7 Managing Delegated Administrators

There are three types of delegated administrators that exist in the NCID-NG environment:

- The *Organization DA* is the highest-level delegated administrator who has the ability to administer and perform all operations on user accounts within his or her organization.
- The *Division DA* is the second-highest level delegated administrator who can perform the same operations as the Organization DA, but their administration capabilities are limited to the division level. A Division DA can only administer and perform operations on user accounts that are in the same division(s) for which they have administrative rights.
- The *Section DA* is the third-highest level delegated administrator who can perform the same operations as the Organization and Division DA, but their administration capabilities are limited to the section level. A Section DA can only administer and perform operations on user accounts that are in the same section(s) for which they have administrative rights.

The level of administration is determined by the role assigned to the user account. The NCID system contains multiple delegated administrative roles, each having been created with permissions to different organizations, divisions and sections. A delegated administrator can be assigned to one or more roles depending upon their level of responsibility.

The following table highlights the operations common to each type of delegated administrator.

- **Note:** Although they can perform the same administrative functions, their scope is limited to the organization, division and/or section for which they have administrator rights.

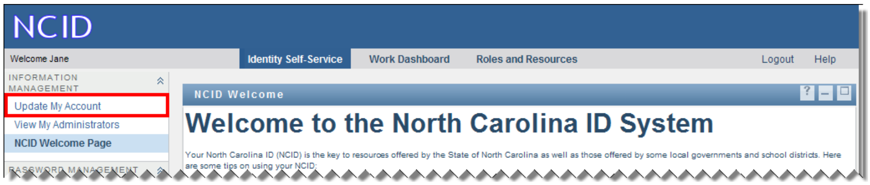
Functions
• Create state and local government employee accounts • Update selected profile information in employee accounts • Deactivate/reactivate employee accounts • Archive deactivated employee account • Reset employee password • Unlock employee account • Promote/demote delegated administrator • Agency to agency account transfer (State DA only)

7.1 Viewing DA Roles Assigned to Your Account

You can view the DA role(s) which have been assigned to your account on the “Identity Self-Service” tab. The “Administrative Roles” section provides a list of your DA roles assignments.

To view delegated administrative roles assigned to your account:

1. On the “Identity Self-Service” tab, click on **Update My Account** in the menu located on the left side of your screen (this option is listed under the “Information Management” category).

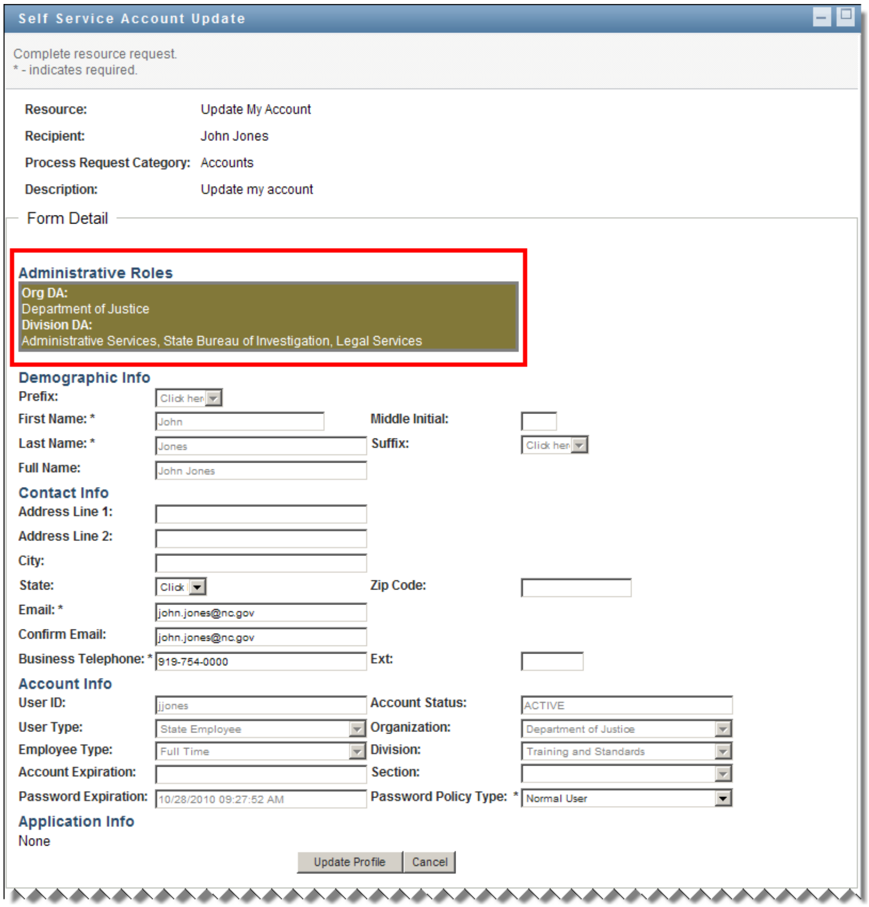


Welcome to the North Carolina ID System

Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are some tips on using your NCID:

Figure 7-1. Click “Update My Account” Link

2. The “Self-Service Account Update” screen is displayed. The “Administrative Roles” section displays the name(s) of the delegated administrative role(s) which you have been assigned.


Self Service Account Update

Complete resource request.
* - indicates required.

Resource:	Update My Account
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Update my account

Form Detail

Administrative Roles

Org DA:
Department of Justice
Division DA:
Administrative Services, State Bureau of Investigation, Legal Services

Demographic Info

Prefix:	Click her		
First Name: *	John	Middle Initial:	
Last Name: *	Jones	Suffix:	Click her
Full Name:	John Jones		

Contact Info

Address Line 1:			
Address Line 2:			
City:			
State:	Click	Zip Code:	
Email: *	john.jones@nc.gov		
Confirm Email:	john.jones@nc.gov		
Business Telephone: *	919-754-0000	Ext:	

Account Info

User ID:	jjones	Account Status:	ACTIVE
User Type:	State Employee	Organization:	Department of Justice
Employee Type:	Full Time	Division:	Training and Standards
Account Expiration:		Section:	
Password Expiration:	10/28/2010 09:27:52 AM	Password Policy Type: *	Normal User

Application Info

None

Figure 7-2. “Administrative Roles” Section

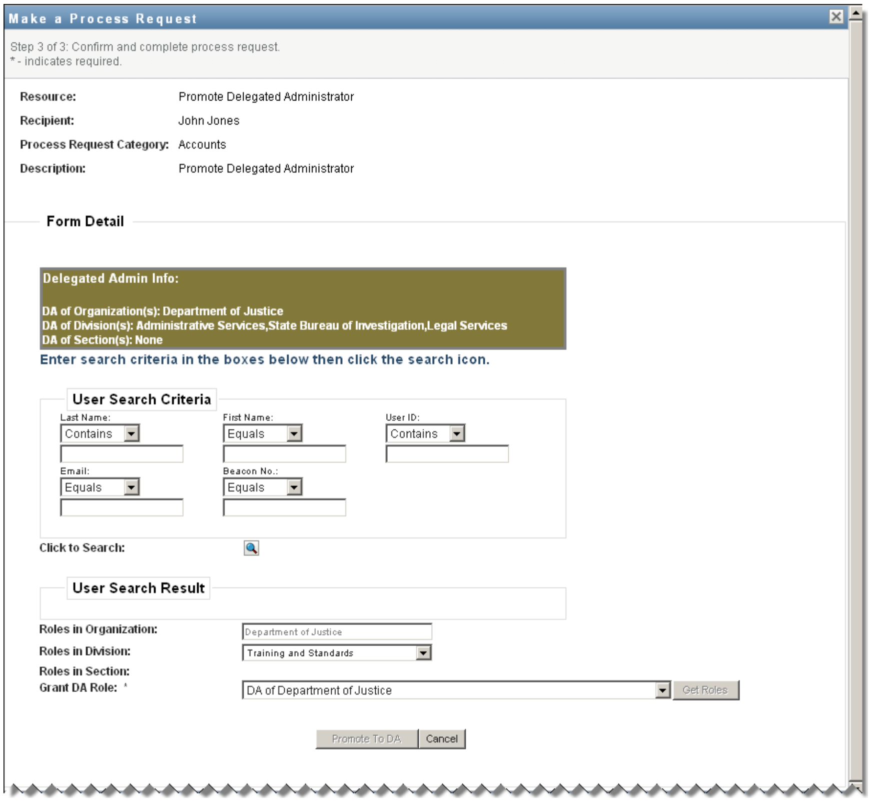
7.2 Promoting a User Account to a Delegated Administrator

You can promote a user account to a delegated administrator by assigning the appropriate administrative role to the account.

> **Important!** It is strongly recommended that your agency has at least two (2) delegated administrators. In the event that an administrator transfers or takes a leave of absence, the remaining administrator will be able to create additional DAs. In addition, actions on an administrator's account can only be performed by another delegated administrator who is at the same level or lower. Service Desk agents are not permitted to unlock a DA's account or reset a DA's password.

To promote a user to a delegated administrator:

1. On the "Work Dashboard" tab, click on the **Make a Process Request** button to display the "Make a Process Request" screen.
2. Click on **Continue** to view a list of workflow processes available to you, and select **Promote Delegated Administrator**.
3. The "Promote Delegated Administrator" request form is displayed. You will need to search for the account you wish to promote. Note that only active users will be searched. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account.



Make a Process Request

Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource:	Promote Delegated Administrator
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Promote Delegated Administrator

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): Administrative Services,State Bureau of Investigation,Legal Services
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to Search:

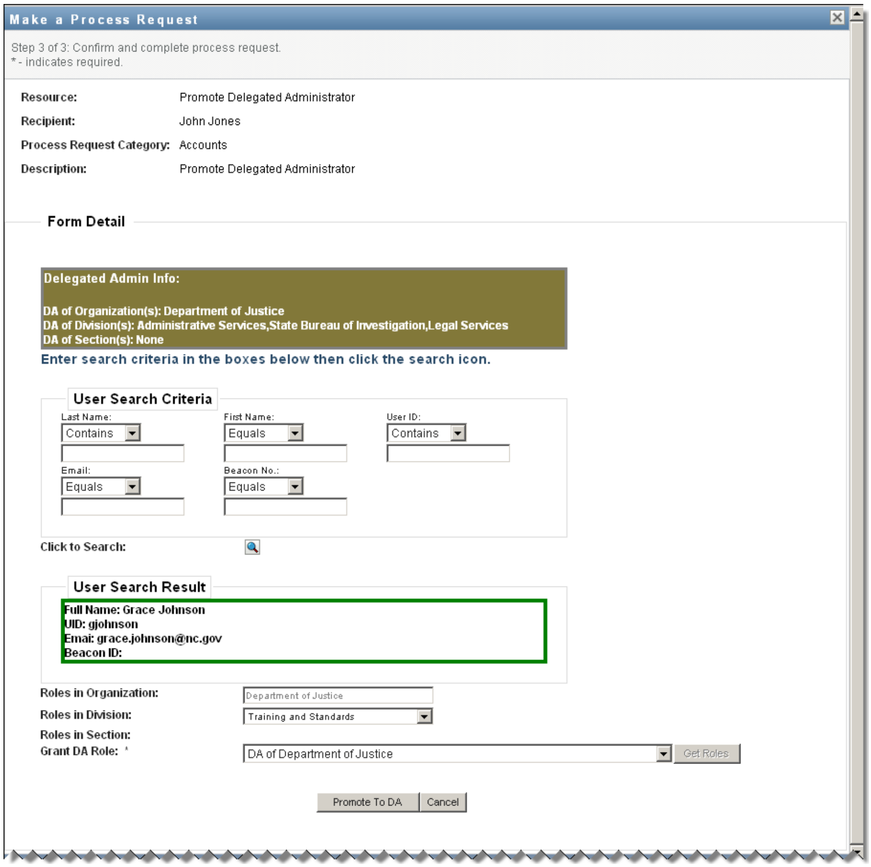
User Search Result

Roles in Organization: Department of Justice
Roles in Division: Training and Standards
Roles in Section:
Grant DA Role: * DA of Department of Justice

Figure 7-3. "Promote Delegated Administrator" Request Form

4. Once you have selected the account, the request form is updated and displays selected attributes from the user's profile in the "User Search Result" section.

- **Note:** By default, the "Grant DA Role" dropdown menu appearing below this section displays the first role included on its menu. As a result, the User Search Criteria section may be highlighted in yellow if the user already has this default role. Alternatively, the section might be outlined in green if the user has not been assigned to the default role. In either case, you will need to assign the appropriate DA role to the user, as explained in the next step.



Make a Process Request

Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource:	Promote Delegated Administrator
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Promote Delegated Administrator

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): Administrative Services,State Bureau of Investigation,Legal Services
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains | First Name: Equals | User ID: Contains
Email: Equals | Beacon No.: Equals

Click to Search:

User Search Result

Full Name: Grace Johnson
UID: gjohnson
Email: grace.johnson@nc.gov
Beacon ID:

Roles in Organization: Department of Justice
Roles in Division: Training and Standards
Roles in Section:
Grant DA Role: * DA of Department of Justice

Figure 7-4. Verify User Details

5. 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 available), and click on the **Get Roles** button. The "Grant DA Role" dropdown menu will display a list of DA roles associated to the division/section that you had selected.

- **Note:** 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.

6. In the "Grant DA Role" dropdown menu, select the appropriate DA role to assign to the user. The User Search Result section will be outlined in green if the role can be assigned to the user.

- **Note:** The section will be highlighted in yellow if the user already has the role. You can either select another DA role to assign to the user, or you can click on **Cancel** to end the request.

7. Click on Promote to DA.
8. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the "Work Dashboard" tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.

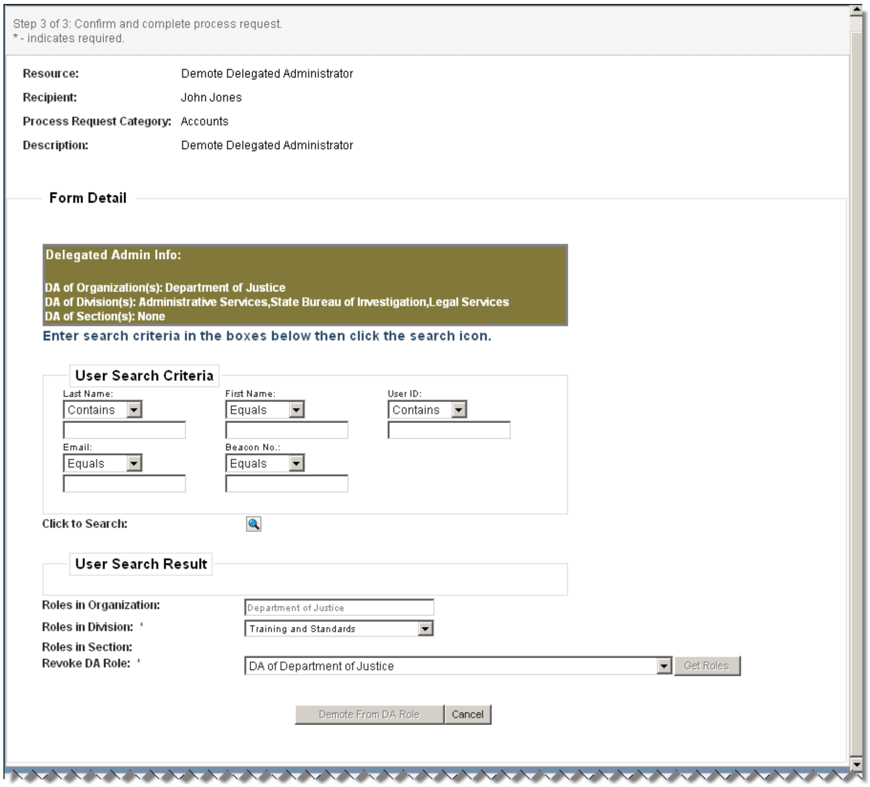
7.3 Demoting a User Account from Delegated Administrator

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

- **Note:** You must be an organization-level administrator to remove rights from the organization. If you are not an organizational administrator, you can remove rights only from the user accounts which belong to the division(s) and section(s) that you administer.

To demote a user account from a delegated administrator:

1. On the "Work Dashboard" tab, click on the **Make a Process Request** button to display the "Make a Process Request" screen.
2. Click on **Continue** to view a list of workflow processes available to you, and select **Demote Delegated Administrator**.
3. The "Demote Delegated Administrator" request form is displayed. You will need to search for the account you wish to demote. Note that only active users will be searched. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account.



Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource:	Demote Delegated Administrator
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Demote Delegated Administrator

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): Administrative Services,State Bureau of Investigation,Legal Services
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to Search:

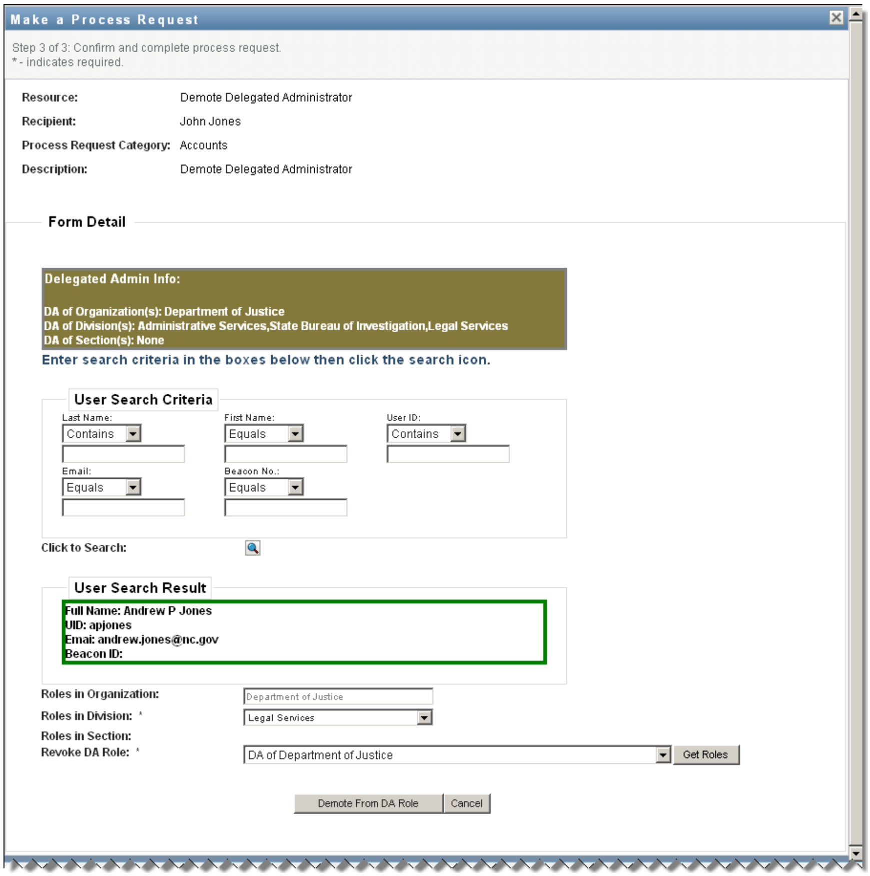
User Search Result

Roles in Organization: Department of Justice
Roles in Division: * Training and Standards
Roles in Section:
Revoke DA Role: * DA of Department of Justice

Figure 7-5. “Demote Delegated Administrator” Request Form

4. Once you have selected the account, the request form is updated and displays selected attributes from the user’s profile in the “User Search Result” section.

- **Note:** By default, the “Grant DA Role” dropdown menu appearing below this section displays the first role included on its menu. As a result, the User Search Criteria section may be highlighted in yellow if the user has not been assigned to this default role. Alternatively, the section might be outlined in green if the user has been assigned to the default role. In either case, you will need to revoke the appropriate DA role from the user, as explained in the next step.



Make a Process Request

Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource:	Demote Delegated Administrator
Recipient:	John Jones
Process Request Category:	Accounts
Description:	Demote Delegated Administrator

Form Detail

Delegated Admin Info:

DA of Organization(s): Department of Justice
DA of Division(s): Administrative Services,State Bureau of Investigation,Legal Services
DA of Section(s): None

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to Search:

User Search Result

Full Name: Andrew P Jones
UID: apjones
Email: andrew.jones@nc.gov
Beacon ID:

Roles in Organization: Department of Justice
Roles in Division: * Legal Services
Roles in Section:
Revoke DA Role: * DA of Department of Justice

Figure 7-6. Verify User Details

5. 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 available), and click on the **Get Roles** button. The “Revoke DA Role” dropdown menu will display a list of DA roles associated to the division/section that you had selected.

- **Note:** 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.

6. In the “Revoke DA Role” dropdown menu, select the appropriate DA role to remove.
7. Click on Demote from DA Role.
8. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the “Work Dashboard” tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.

This page was intentionally left blank

Part 3: Application Administrator Functions

This section describes how application access is granted in NCID and provides instruction on the various administrative tasks available to an application administrator.

Section 8: Making Resource (Application) Assignments

Section 9: Managing Application Administrators

This page was intentionally left blank

8 Making Resource (Application) Assignments

As application administrator, you can grant users access to their applications via role assignments. In NCID, a role defines a set of permissions to an application (or *resource*), and users are granted access to resources via *role assignments*.

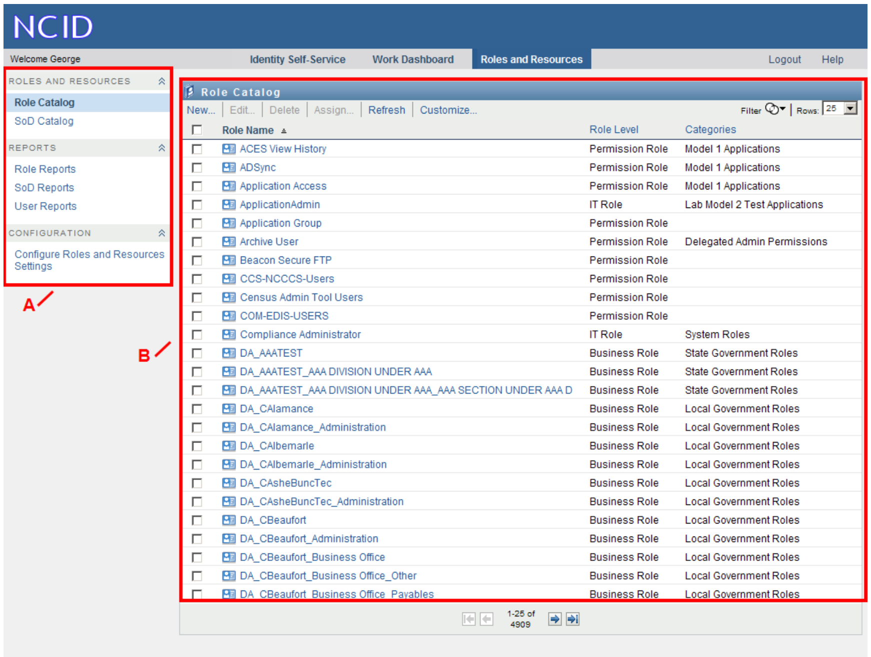
The NCID group creates the roles that you can assign to users within the division(s) and/or section(s) you manage. Roles can be given directly to a user, in which case you can give a user explicit access to a resource associated with the role, or a user may receive a role indirectly by being a member of a group or related role.

All roles are stored in the *Role Catalog*, which can be viewed on the “Roles and Resources” tab. The Role Catalog lets you sort and filter roles by their name, level and/or category, and it provides tools to create new roles, modify existing ones and/or assign a role to a user (tool availability is dependent on your access permissions).

The following topics in this section demonstrate how to navigate around the Role Catalog and instruct how to grant and revoke application access via role assignments.

8.1 Roles and Resources Overview

Before we describe the Role Catalog and demonstrate how to make role assignments, this section will familiarize you with the Roles and Resources tab. This tab is separated into the following sections (screen content and feature availability will vary based on job responsibility and access permissions):



□	Role Name ▲	Role Level	Categories
□	ACES View History	Permission Role	Model 1 Applications
□	ADSync	Permission Role	Model 1 Applications
□	Application Access	Permission Role	Model 1 Applications
□	ApplicationAdmin	IT Role	Lab Model 2 Test Applications
□	Application Group	Permission Role	
□	Archive User	Permission Role	Delegated Admin Permissions
□	Beacon Secure FTP	Permission Role	
□	CCS-NCCCS-Users	Permission Role	
□	Census Admin Tool Users	Permission Role	
□	COM-EDIS-USERS	Permission Role	
□	Compliance Administrator	IT Role	System Roles
□	DA_AAATEST	Business Role	State Government Roles
□	DA_AAATEST_AAA DIVISION UNDER AAA	Business Role	State Government Roles
□	DA_AAATEST_AAA DIVISION UNDER AAA_AAA SECTION UNDER AAA D	Business Role	State Government Roles
□	DA_CAlamance	Business Role	Local Government Roles
□	DA_CAlamance_Administration	Business Role	Local Government Roles
□	DA_CAlbemarle	Business Role	Local Government Roles
□	DA_CAlbemarle_Administration	Business Role	Local Government Roles
□	DA_CAsheBuncTec	Business Role	Local Government Roles
□	DA_CAsheBuncTec_Administration	Business Role	Local Government Roles
□	DA_CBeaufort	Business Role	Local Government Roles
□	DA_CBeaufort_Administration	Business Role	Local Government Roles
□	DA_CBeaufort_Business Office	Business Role	Local Government Roles
□	DA_CBeaufort_Business Office_Other	Business Role	Local Government Roles
□	DA_CBeaufort_Business Office_Payables	Business Role	Local Government Roles

Figure 8-1. Roles and Resources Tab

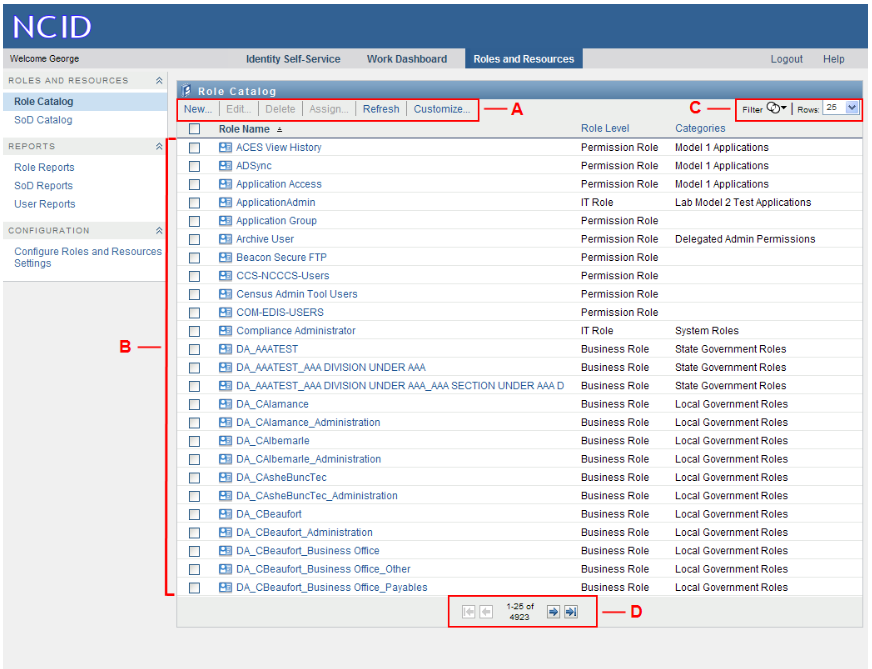
A The *menu* displays a list of actions that you can perform. Actions are listed by category: Roles and Resources, Reports and Configuration. Menu categories and actions are dependent on the tab you are viewing and your access permissions.

- **Note:** Only the "Roles Catalog" option under the "Roles and Resources" category will be used in this current release of NCID

B The right-side of the screen displays a window which shows the details for the action you selected.

8.2 Role Catalog

By default, the Role Catalog is displayed when the Roles and Resources tab is accessed. This feature provides a centralized area for managing roles and making role assignments for users who need access to applications. The following figure illustrates an example of the Role Catalog, and highlights its main components (feature availability will vary based on job responsibility and access permissions).



□	Role Name	Role Level	Categories
□	ACES View History	Permission Role	Model 1 Applications
□	ADSync	Permission Role	Model 1 Applications
□	Application Access	Permission Role	Model 1 Applications
□	ApplicationAdmin	IT Role	Lab Model 2 Test Applications
□	Application Group	Permission Role	
□	Archive User	Permission Role	Delegated Admin Permissions
□	Beacon Secure FTP	Permission Role	
□	CCS-NCCCS-Users	Permission Role	
□	Census Admin Tool Users	Permission Role	
□	COM-EDIS-USERS	Permission Role	
□	Compliance Administrator	IT Role	System Roles
□	DA_AAATEST	Business Role	State Government Roles
□	DA_AAATEST_AAA DIVISION UNDER AAA	Business Role	State Government Roles
□	DA_AAATEST_AAA DIVISION UNDER AAA_AAA SECTION UNDER AAA D	Business Role	State Government Roles
□	DA_CAlamance	Business Role	Local Government Roles
□	DA_CAlamance_Administration	Business Role	Local Government Roles
□	DA_CAlbemarle	Business Role	Local Government Roles
□	DA_CAlbemarle_Administration	Business Role	Local Government Roles
□	DA_CAsheBuncTec	Business Role	Local Government Roles
□	DA_CAsheBuncTec_Administration	Business Role	Local Government Roles
□	DA_CBeaufort	Business Role	Local Government Roles
□	DA_CBeaufort_Administration	Business Role	Local Government Roles
□	DA_CBeaufort_Business Office	Business Role	Local Government Roles
□	DA_CBeaufort_Business Office_Other	Business Role	Local Government Roles
□	DA_CBeaufort_Business Office_Payables	Business Role	Local Government Roles

Figure 8-2. Example of the Role Catalog

A This section provides action buttons which let you create, manage and assign roles, as well as customize how information is displayed in the Role Catalog.

B This section displays a list of roles that have been created in the NCID system. Roles are displayed alphabetically and each role's level and associated category are identified. You may sort the list by name, level or category by clicking on the appropriate column heading.

C This section provides a filter so you can display only the roles that you are interested in viewing. Additionally, you can set the amount of roles which are displayed on the screen by using the "Rows" dropdown menu.

D This section lets you page through the list of roles.

To view roles:

1. On the "**Roles and Resource**" tab, click **Role Catalog** in the menu located on the left side of your screen (this option is listed under the Roles and Resources category).

- **Note:** Upon clicking on the Roles and Resources tab, a message informs you that you might experience a short delay while the system loads the existing roles into the catalog. Click on **OK** to continue, or click on **Cancel** to enter filter criteria. Please refer to steps 3 and 4 for instruction on how to filter, or move to step 5 if you choose to view the entire list.

2. The "Role Catalog" opens and alphabetically displays a list of roles that have been created in the system. The catalog presents role information in the following columns:

- **Note:** Columns can be sorted in ascending or descending order to help you locate and organize roles. Click on the appropriate column heading to perform this operation.

Role Name displays the name of each role in the catalog.

Level indicates the level of the role within the catalog. The following levels make up the *roles hierarchy* which establishes relationships between roles in the catalog. This hierarchy helps simplify the task of granting permissions through role assignments.

Business Role is the highest level in the roles hierarchy. This role defines operations that have business meaning within the organization. For example, a role which is assigned to a delegated administrator is at a Business Role level.

IT Role is the middle level in the roles hierarchy. This role supports technology functions, for example, an application administrator. For example, a role which is assigned to an application administrator is at an IT Role level.

Permission Role is the lowest level in the roles hierarchy, and defines lower-level permissions. For example, a role which is assigned to an end-user is at a Permission Role level.

- **Note:** A higher-level role includes permissions from lower-level roles that it contains. Lower-level roles cannot contain high-level roles.

Categories column lists the categories associated to the roles. When a role is created, it can be associated with a category. Specifying a role category is helpful when viewing the Role Catalog as you can organize and filter roles by category.

3. The Role Catalog displays up to 25 roles at a time. To page through the list, click on the **Next** icon ➡ . You may change the number of roles displayed on a page by selecting another value in the "Rows" dropdown menu at the top of the screen.

To filter the list of roles:

4. Click on the **Filter** icon Filter at the top of the screen to display the “Filter” pop-up window. You can filter on one or more of the following filter options.

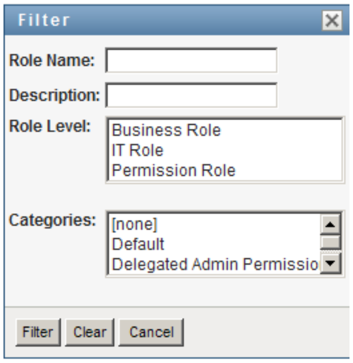


Figure 8-3. Role Filter Options

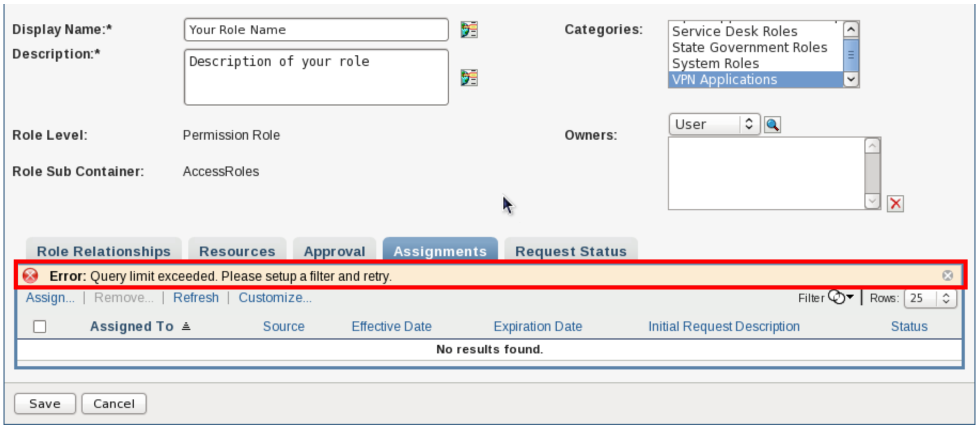
5. To filter on a role name: In the **Role Name** field, you can enter role’s full name or only a part of it. The system will show only those roles that begin with the characters that you entered. You may also use the asterisk (*) as a wildcard in your text.
6. To filter on roles which have a specific role level(s): Click on the appropriate level in the **Role Level** selection box. To select more than one level, hold the <Shift> key or <Ctrl> key as you click on your selections.
7. To filter on roles which are associated to a particular category(s): Click on the appropriate category in the **Categories** selection box. To select more than one category, hold the <Shift> key or <Ctrl> key as you click on your selections.
8. Click on **Filter** to apply the filter criteria.

- **Note:** You may also click on **Clear** to reset the filter criteria, or click on **Cancel** to return to the role catalog without applying the filter criteria.

9. The “Role Catalog” screen displays an updated list of roles matching the filter criteria you selected.
10. To view details of a role, click on the role name in the “Role Name” column.

To view users assigned to a role:

1. To view a list of user with the assigned role, click on **Refresh**. If the role exceeds 500 users, the following message will be displayed (outlined in red below.)



Display Name:* Your Role Name

Description:* Description of your role

Categories: Service Desk Roles, State Government Roles, System Roles, VPN Applications

Role Level: Permission Role

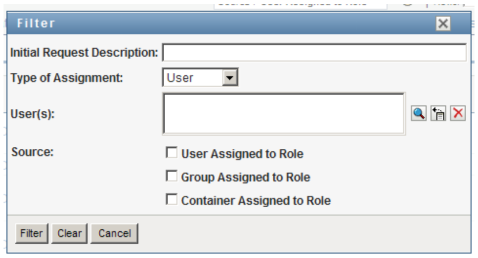
Owners: User

Role Sub Container: AccessRoles

Error: Query limit exceeded. Please setup a filter and retry.

☐	Assigned To	Source	Effective Date	Expiration Date	Initial Request Description	Status
No results found.						

2. Click on the **Filter** icon Filter below the **Error:** message to display the “Filter” pop-up window.
3. You can filter on one or more of the following filter options.



Initial Request Description:

Type of Assignment: User

User(s):

Source:
☐ User Assigned to Role
☐ Group Assigned to Role
☐ Container Assigned to Role

4. In the “Type of Assignment” dropdown menu, select **User**.

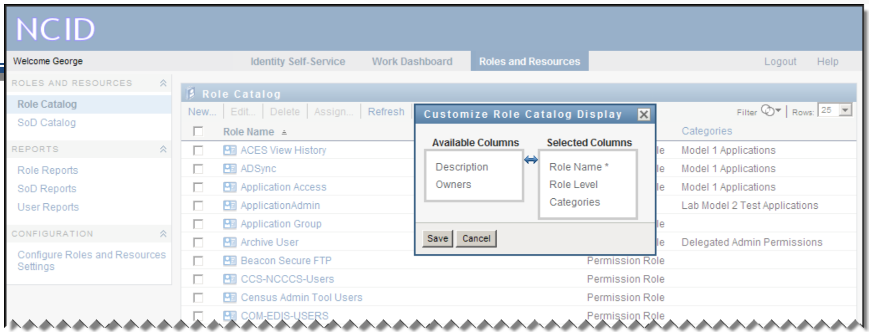
- **NOTE:** To see all role assignments refer to chapter 10 – Reporting for instructions on retrieving a full report of users assigned to a role.

5. Click on the **Search** icon next to the “Select User(s)” field. You may specify one or more users in your search.
6. Click on **Filter** to search the selected role for users that match the filter.

Tip! You can customize the type of information that is presented in the Role Catalog by hiding or displaying column headings.

To hide/display column heading(s):

1. From the Role Catalog menu, click on Customize Customize...
2. The "Customize Role Catalog Display" pop-up window is displayed. The window presents "Available Columns" and "Selected Columns" in two selection boxes.
3. To add a new column: Click on the column name from the "Available Columns" selection box. The name appears in the "Selected Columns" box.
4. To remove a column: Click on the column name from the "Selected Columns" selection box. The name appears in the "Available Columns" box.
5. Click on Save to apply the customization to the Role Catalog screen.
6. Click on Cancel to return to the role catalog without applying the customization.



□	Role Name		Categories
□	ACES View History	le	Model 1 Applications
□	ADSync	le	Model 1 Applications
□	Application Access	le	Model 1 Applications
□	ApplicationAdmin		Lab Model 2 Test Applications
□	Application Group	le	
□	Archive User	le	Delegated Admin Permissions
□	Beacon Secure FTP	Permission Role	
□	CCS-NCCCS-Users	Permission Role	
□	Census Admin Tool Users	Permission Role	
□	COM-EDIS-USERS	Permission Role	

Figure 8-4. Customize Role Catalog Display

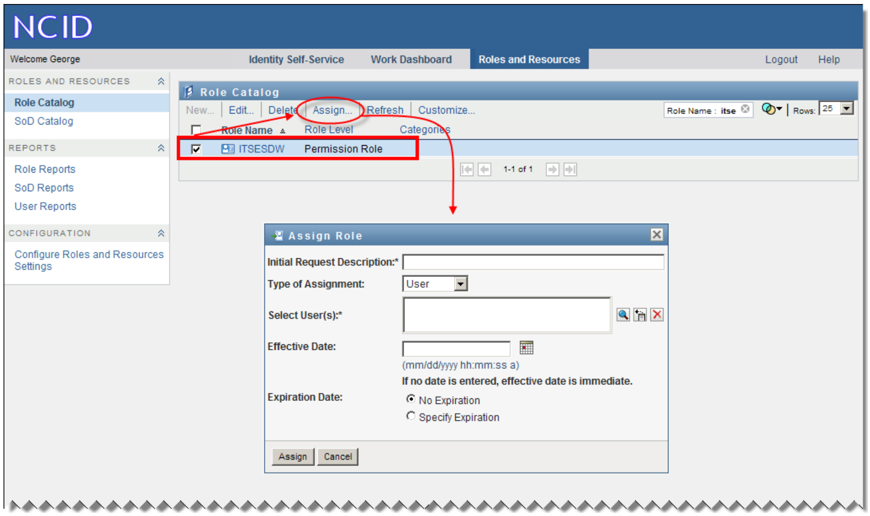
8.3 Granting Application Access via Role Assignments

To grant a user access to an application, you will need to locate the role which contains permissions to the application, and then assign the role to the user account.

To grant application access via a role assignment:

1. Click on the **Roles and Resources** tab.
2. Locate the appropriate role from the Role Catalog. You can search for the role by scrolling through the list, or you can specify filter criteria to quickly find the role. Please refer to the *Role Catalog* section on page 84 for steps on how to specify filter criteria.
3. Click on the checkbox next to the appropriate role and click on **Assign**. The "Assign Role" pop-up window is displayed.

> **Good to Know!** You can also access the “Assign Role” window by clicking on the role name from the list on the Role Catalog. The role’s property window displays. Click on the Assignments tab and then click on **Assign** to access the “Assign Role” window.



Role Name : itse

Rows: 25

☐	Role Name	Role Level	Categories
☑	ITSESDW	Permission Role	

1-1 of 1

Initial Request Description:*

Type of Assignment: User

Select User(s):*

Effective Date:

(mm/dd/yyyy hh:mm:ss a)

If no date is entered, effective date is immediate.

Expiration Date: ● No Expiration ○ Specify Expiration

Figure 8-5. “Assign Role” Pop-Up Window

4. The “Initial Request Description” is a required field, so you will need to enter a brief reason for the assignment request.
5. In the “Type of Assignment” dropdown menu, select **User**.
6. Click on the **Search** icon next to the “Select User(s)” field. You may specify one or more users to assign the role.
7. Optionally, you may specify effective and expiration dates for the role assignment. If you don’t specify an effective date, the assignment is immediate.
8. Click on Assign.
9. The screen displays a confirmation message that the role assignment was successful.

- **Note:** A message alerts you if you are unauthorized to assign a role to a user.

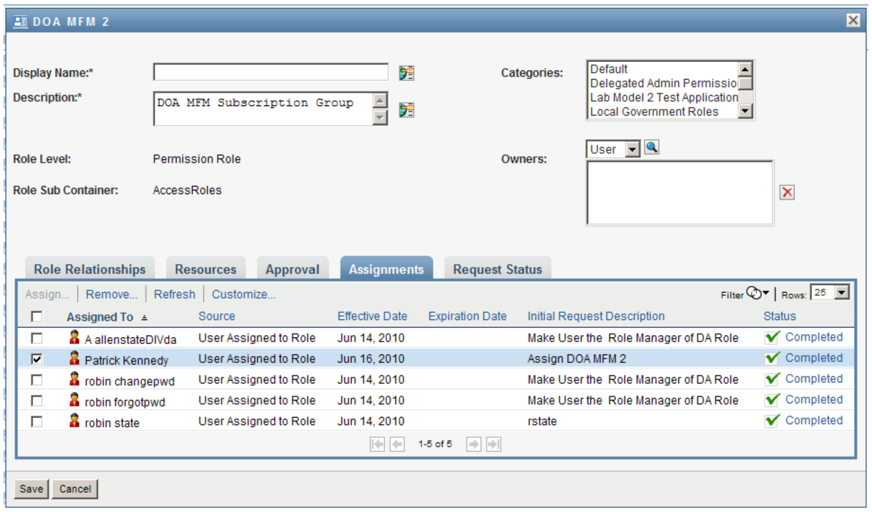
8.4 Removing Application Access

If a user’s responsibilities change, you can revoke user access to an application. You will need to locate the role which has permissions to the application, and then remove the role assignment from the user account.

To remove application access from a user account:

1. Click on the **Roles and Resources** tab.
2. Locate the appropriate role from the Role Catalog. You can search for the role by scrolling through the list, or you can specify filter criteria to quickly find the role. Please refer to the *Role Catalog* section on page 84 for steps on how to specify filter criteria.

3. Click on the checkbox next to the appropriate Role and click on **Edit**. The role's property window is displayed.
4. Click on the **Assignments** tab to view a list of user accounts that are assigned to this role.



DOA MFM 2

Display Name:*

Description:* DOA MFM Subscription Group

Categories: Default, Delegated Admin Permissio, Lab Model 2 Test Application, Local Government Roles

Role Level: Permission Role

Owners: User

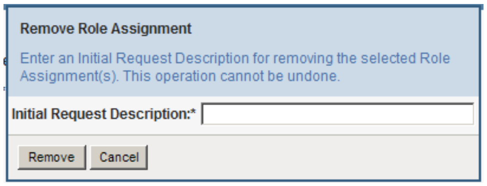
Role Sub Container: AccessRoles

□	Assigned To	Source	Effective Date	Expiration Date	Initial Request Description	Status
□	A allenstateDIVda	User Assigned to Role	Jun 14, 2010		Make User the Role Manager of DA Role	✓ Completed
☑	Patrick Kennedy	User Assigned to Role	Jun 16, 2010		Assign DOA MFM 2	✓ Completed
□	robin changepwd	User Assigned to Role	Jun 14, 2010		Make User the Role Manager of DA Role	✓ Completed
□	robin forgotpwd	User Assigned to Role	Jun 14, 2010		Make User the Role Manager of DA Role	✓ Completed
□	robin state	User Assigned to Role	Jun 14, 2010		rstate	✓ Completed

Figure 8-6. Role Property Window

- **NOTE:** If the role membership exceeds 500 you will need to apply a filter to view assignments for users that match the filter. See "To view users assigned to a role:" above.

5. Locate the user account. You can scroll through the list of user accounts, or specify filter criteria to find the user.
6. Click on the checkbox next to the appropriate user and click on **Remove**. The "Remove Role Assignment" pop-up window is displayed.



Remove Role Assignment

Enter an Initial Request Description for removing the selected Role Assignment(s). This operation cannot be undone.

Initial Request Description:*

Figure 8-7. "Remove Role Assignment" Window

7. In the "Initial Request Description" field, enter a brief reason for the role removal.
8. Click on **Remove** to return to the role's property window.
9. Click on **Save** to save the changes made to the role.

This page was intentionally left blank

9 Managing Application Administrators

The NCID system contains multiple application administrators who are responsible for granting application access to users within their organization, division and/or section. The applications which an administrator can grant permission are determined by the application role assigned to his or her account.

A user is promoted to application administrator by an existing application administrator. If an administrator does not exist for an organization, the user can open a ticket to the NCID group and make a request to become an application administrator for the organization. Once the user is assigned the application administrator role, he or she can promote other users.

- **Note:** A user can be both an application administrator and a delegated administrator, depending on the role(s) assigned to their user account.

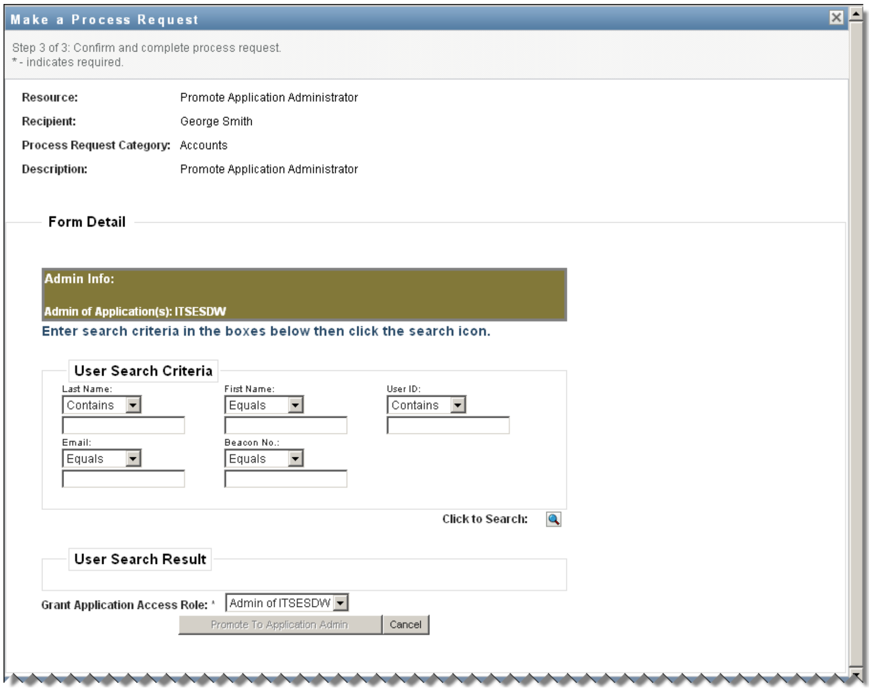
This section provides instruction on the various administrative tasks that are available for managing application administrators.

9.1 Promoting User Account to Application Administrator

You can promote a user account to application administrator by assigning the appropriate role to the account.

To promote a user to an application administrator:

1. On the “Work Dashboard” tab, click on the Make a Process Request button to display the “Make a Process Request” screen.
2. Click on **Continue** to view a list of workflow processes available to you, and select **Promote Application Administrator**.
3. The “Promote Application Administrator” request form is displayed. You will need to search for the account you wish to promote. Note that only active users will be searched. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account.



Make a Process Request

Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource: Promote Application Administrator
Recipient: George Smith
Process Request Category: Accounts
Description: Promote Application Administrator

Form Detail

Admin Info:

Admin of Application(s): ITSESDW

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

Click to Search:

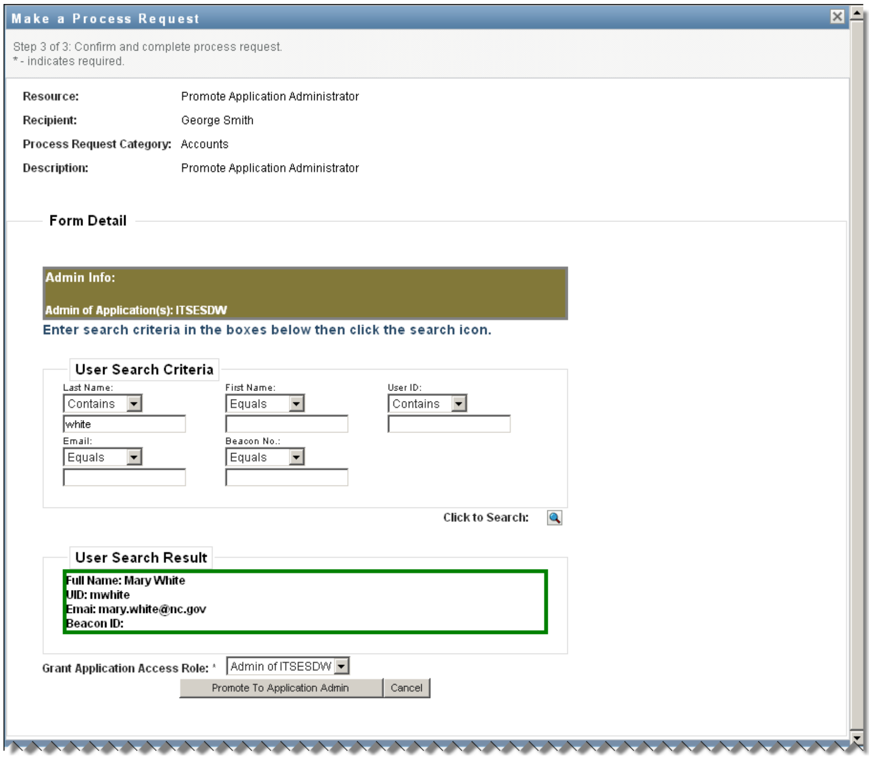
User Search Result

Grant Application Access Role: * Admin of ITSESDW

Figure 9-1. "Promote Application Administrator" Request Form

4. Once you have selected the account, the request form is updated and displays selected attributes from the user's profile in the "User Search Result" section.

- **Note:** This section is outlined in green if the user has not been already promoted to administrator. If the user has been promoted, the section is highlighted in red and a message alerts you that the user already has the application administrator role.



Make a Process Request

Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource:	Promote Application Administrator
Recipient:	George Smith
Process Request Category:	Accounts
Description:	Promote Application Administrator

Form Detail

Admin Info:

Admin of Application(s): ITSESDW

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains white

First Name: Equals

User ID: Contains

Email: Equals

Beacon No.: Equals

Click to Search:

User Search Result

Full Name: Mary White
UID: mwhite
Emai: mary.white@nc.gov
Beacon ID:

Grant Application Access Role: * Admin of ITSESDW

Figure 9-2. Updated User Search Result Section

5. Verify that this is the correct user account that you wish to promote. If this is not the appropriate user, you can clear the fields and perform your search again.
6. In the “Grant Application Access Role” dropdown menu, select the appropriate application administrator role to assign to the user.
7. Click on Promote to Application Admin.
8. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the “Work Dashboard” tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.

9.2 Demoting a User Account from Application Administrator

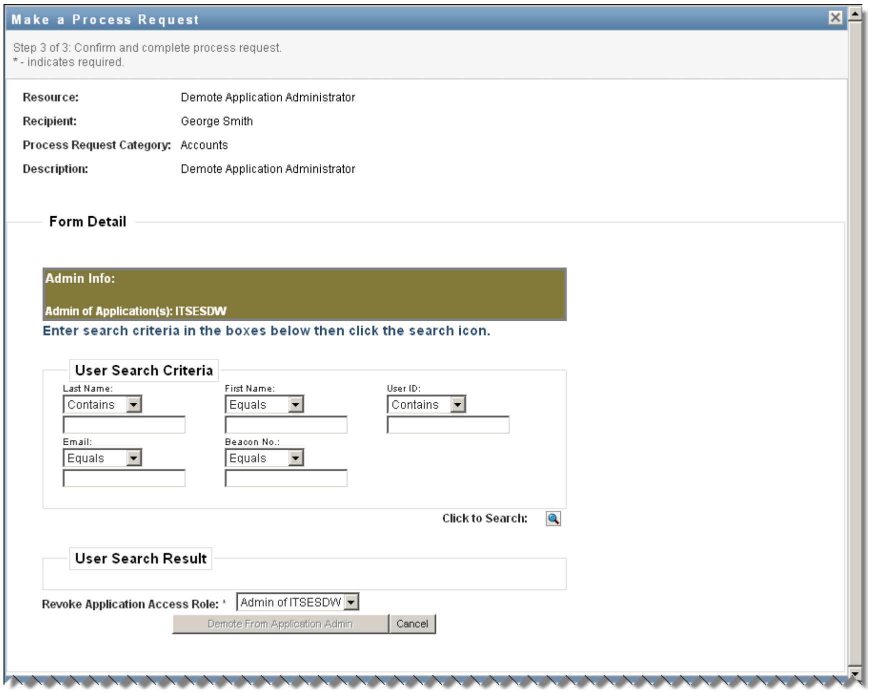
If a user’s responsibilities change, administrator rights can be taken away by removing the administrator role(s) assigned to the user account.

- **Note:** You must be an application administrator to remove rights from a user account.

To demote a user account from application administrator:

1. On the “Work Dashboard” tab, click on the **Make a Process Request** button to display the “Make a Process Request” screen.
2. Click on **Continue** to view a list of workflow processes available to you, and select **Demote Application Administrator**.
3. The “Demote Application Administrator” request form is displayed. You will need to search for the account you wish to demote. Note that only active users will be

searched. Please refer to the *Searching for a User Account* section on page 29 for details on how to look up a user account.



Make a Process Request

Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource: Demote Application Administrator
Recipient: George Smith
Process Request Category: Accounts
Description: Demote Application Administrator

Form Detail

Admin Info:

Admin of Application(s): ITSESDW

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

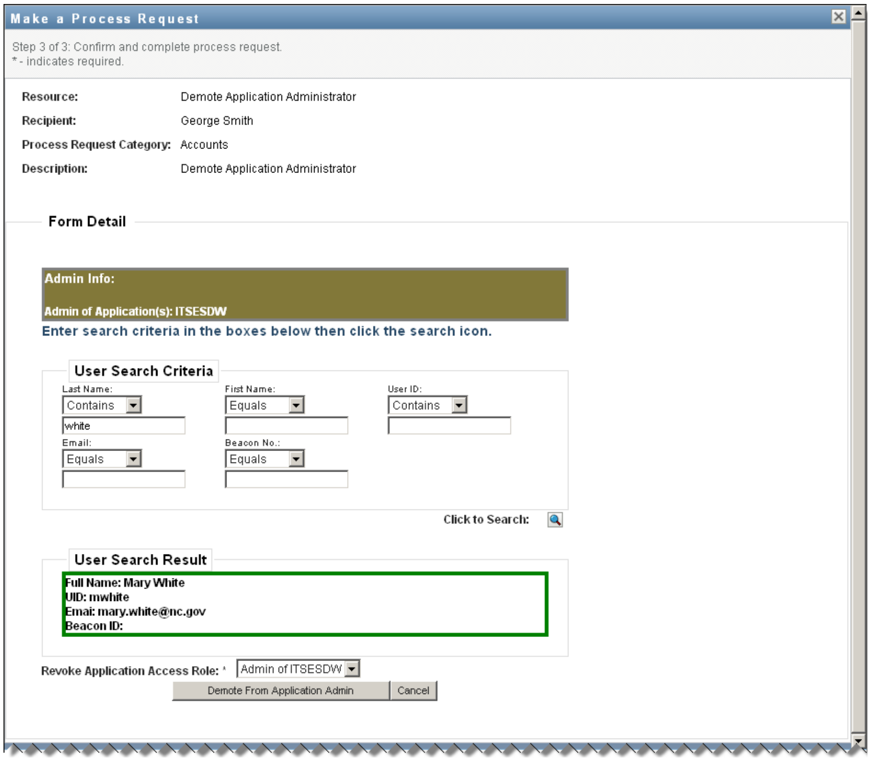
Click to Search:

User Search Result

Revoke Application Access Role: * Admin of ITSESDW

Figure 9-3."Demote Application Administrator" Request Form

4. Once you have selected the account, the request form is updated and displays selected attributes from the user's profile in the "User Search Result" section.
5. Verify that this is the correct user account that you wish to remove administrator rights from. If this is not the appropriate user, you can clear the fields and perform your search again.
6. In the "Grant Application Access Role" dropdown menu, select the appropriate role associated to remove.



Step 3 of 3: Confirm and complete process request.
* - indicates required.

Resource: Demote Application Administrator
Recipient: George Smith
Process Request Category: Accounts
Description: Demote Application Administrator

Form Detail

Admin Info:

Admin of Application(s): ITSESDW

Enter search criteria in the boxes below then click the search icon.

User Search Criteria

Last Name: Contains white
First Name: Equals
User ID: Contains
Email: Equals
Beacon No.: Equals

User Search Result

Full Name: Mary White
UID: mwhite
Emai: mary.white@nc.gov
Beacon ID:

Revoke Application Access Role: * Admin of ITSESDW

Figure 9-4. Updated User Search Results Section

7. Click on Demote from Application Admin.
8. The screen displays a confirmation message that your request was successful, and states that you can also check the status of the request on the “Work Dashboard” tab. Please refer to the *Checking the Status of a Request* section on page 69 for more information.

This page was intentionally left blank

Part 4: Reporting

This section describes how to download reports for the users and applications that you manage.

This page was intentionally left blank

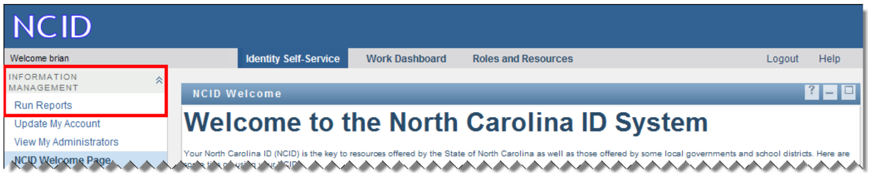
10 Downloading a Report

The NCID Report application allows you to download pre-defined reports for the users and applications that you manage. You must be either a state agency delegated administrator and/or an application administrator to use this feature. Report availability is based on the administrative role assigned to your user account.

Report information is exported as a single Comma Separated Values file (.CSV file), which can saved to your computer. Please note that report data is generated in the early morning each day. Updates to an account made earlier in the day will not be reflected in the data exported to the file until the following day.

To download a report:

1. On the “Identity Self-Service” tab, click **Run Reports** in the menu located on the left side of your screen (this option is listed under the Information Management category).

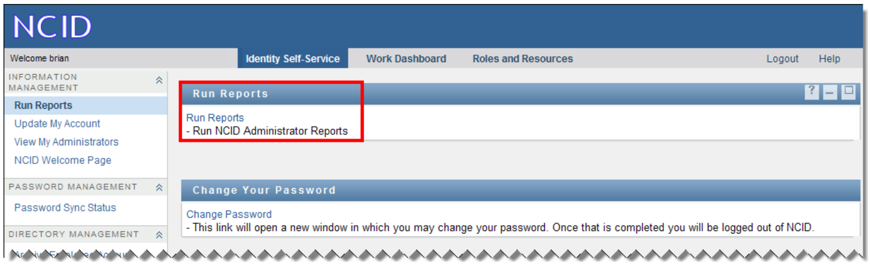


Welcome to the North Carolina ID System

Your North Carolina ID (NCID) is the key to resources offered by the State of North Carolina as well as those offered by some local governments and school districts. Here are

Figure 10-1. Click on “Run Reports”

2. The “Identity Self-Service” tab is refreshed. From the “Run Reports” section, click on the link to access the reporting screens.

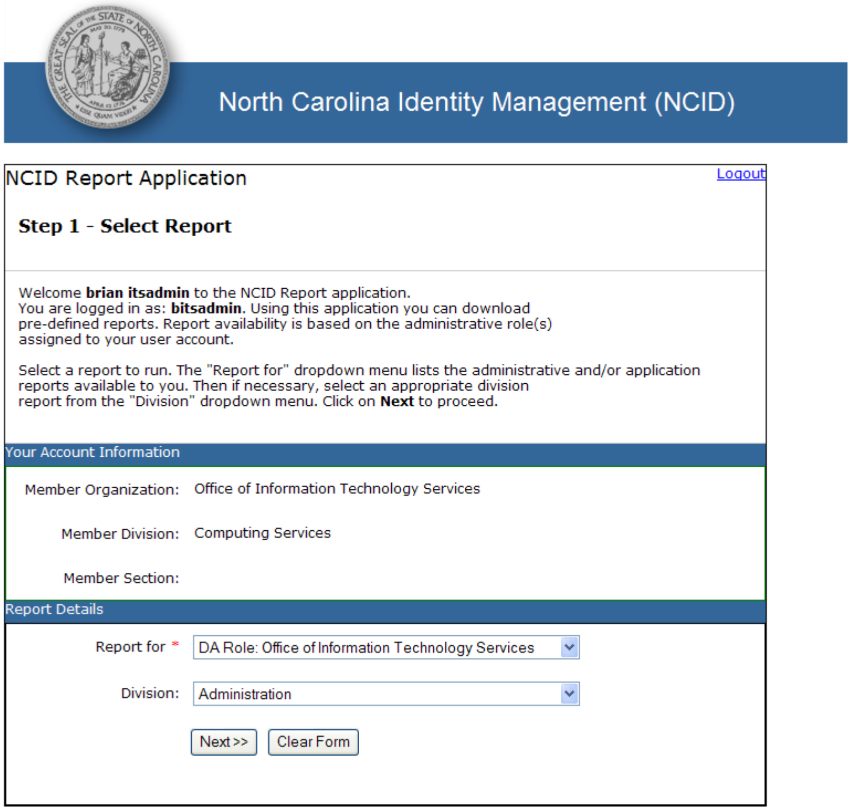


- Run NCID Administrator Reports

- This link will open a new window in which you may change your password. Once that is completed you will be logged out of NCID.

Figure 10-2. Click on “Run Reports”

3. The “Step 1 – Select Report” screen is displayed. The names of the organization, division(s) and/or section(s) of which you are a member are displayed in the “Your Account Information” section.



North Carolina Identity Management (NCID)

NCID Report Application

Step 1 - Select Report

Welcome **brian itsadmin** to the NCID Report application.
You are logged in as: **bitsadmin**. Using this application you can download pre-defined reports. Report availability is based on the administrative role(s) assigned to your user account.

Select a report to run. The "Report for" dropdown menu lists the administrative and/or application reports available to you. Then if necessary, select an appropriate division report from the "Division" dropdown menu. Click on **Next** to proceed.

Your Account Information

Member Organization: Office of Information Technology Services

Member Division: Computing Services

Member Section:

Report Details

Report for *: DA Role: Office of Information Technology Services

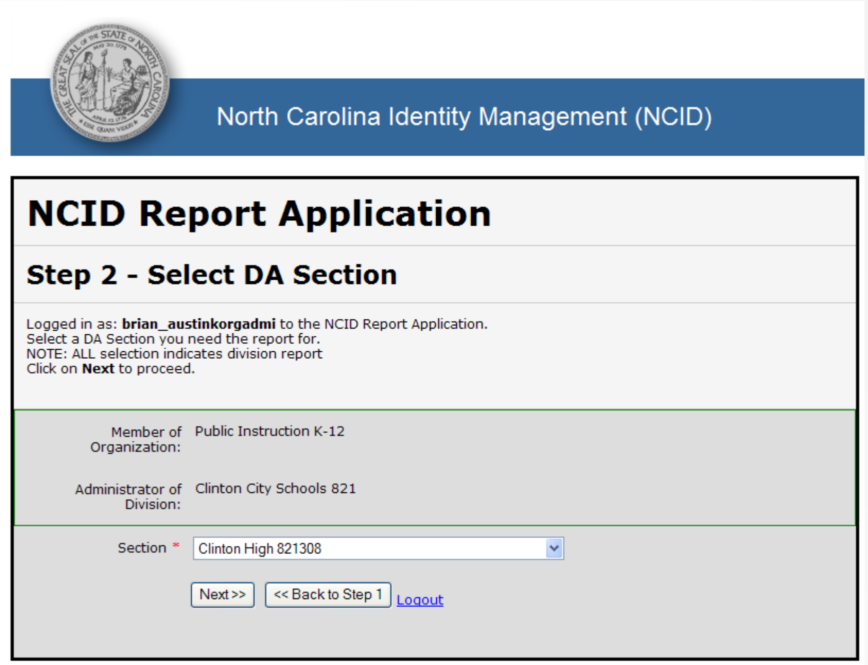
Division: Administration

Figure 10-3. Step 1 – Select Report

4. Depending upon your administrative permissions, the “Report for” dropdown menu displays a list of DA (Delegated Administrator) and/or AA (Application Administrator) reports that are available to you. Select the report that you wish run.
5. If applicable, you may select a division report from the “Division” dropdown menu, or select **All** to generate a report for the organization.
6. Click on **Next** to proceed.

Note: The following screen will be displayed if the division you selected contains section reports.

- Select the appropriate report from the “Section” dropdown menu, or select **All** to generate a report for the entire division.
- Click on **Next** to proceed, or click on **Back to Step 1** if you need to select a report for a different division.



North Carolina Identity Management (NCID)

NCID Report Application

Step 2 - Select DA Section

Logged in as: **brian_austinkorgadmi** to the NCID Report Application.
Select a DA Section you need the report for.
NOTE: ALL selection indicates division report
Click on **Next** to proceed.

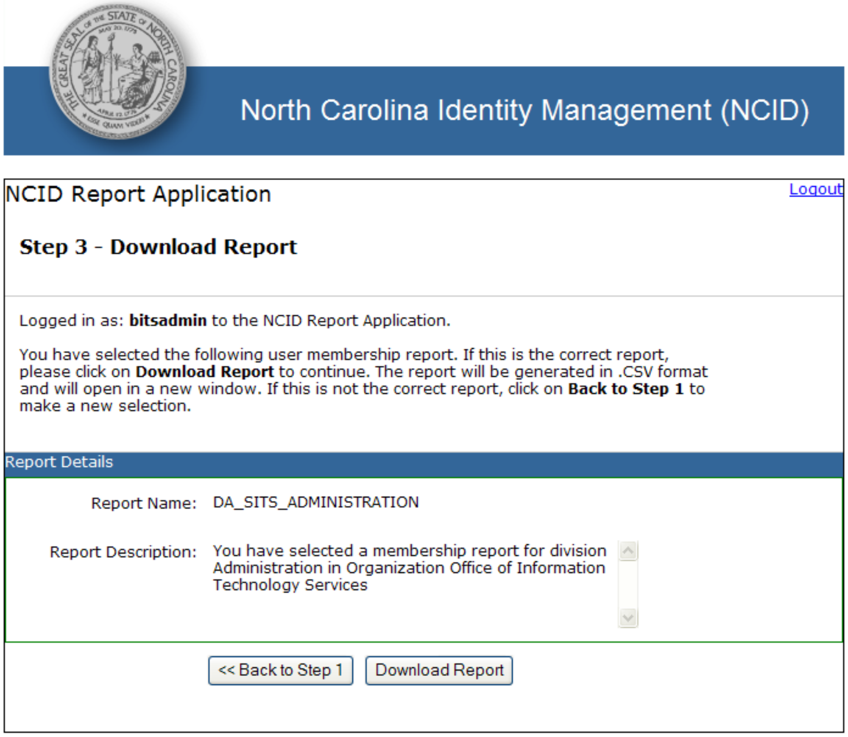
Member of Organization: Public Instruction K-12

Administrator of Division: Clinton City Schools 821

Section *: Clinton High 821308

Figure 10-4. Step 2 – Select DA Section Report

7. The “Step 3 – Download Report” screen is displayed, and provides a summary of the report you selected to generate. If the information is correct, click on **Download Report** to continue, or click on **Back to Step 1** if you need to select a different report.



North Carolina Identity Management (NCID)

NCID Report Application

Step 3 - Download Report

Logged in as: **bitsadmin** to the NCID Report Application.

You have selected the following user membership report. If this is the correct report, please click on **Download Report** to continue. The report will be generated in .CSV format and will open in a new window. If this is not the correct report, click on **Back to Step 1** to make a new selection.

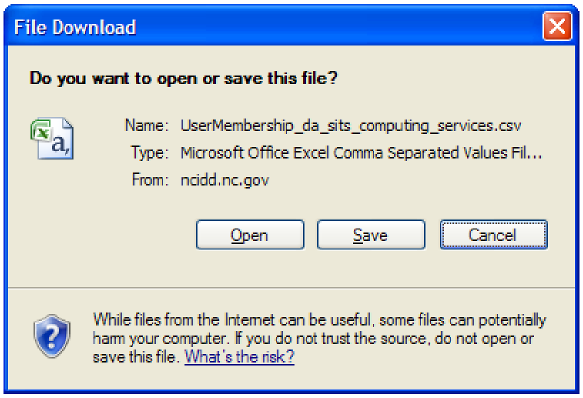
Report Details

Report Name: DA_SITS_ADMINISTRATION

Report Description: You have selected a membership report for division Administration in Organization Office of Information Technology Services

Figure 10-5. Confirm Report Details

8. The “File Download” screen prompts you to open the .CSV file or to save it on your computer or network.



File Download

Do you want to open or save this file?

Name: UserMembership_da_sits_computing_services.csv
Type: Microsoft Office Excel Comma Separated Values Fil...
From: ncidd.nc.gov

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 10-6. File Download Window

Part 5: Appendixes

The following sections provide additional reference information for the NCID service.

Appendix A: NCID Terminology

Appendix B: Function Availability for NCID Users

This page was intentionally left blank

Appendix A: NCID Terminology

Archiving [Account]	The process of decommissioning a user account. An archived account cannot be reinstated. A new user account must be created if the user needs to access NCID connected resources again.
Authentication	The process of identifying an individual to NCID based on user ID and password.
Authorization	The process of giving an individual access to system resources, such as customer-based applications.
Business Role	The highest level in the roles hierarchy. This role defines operations that have business meaning within the organization.
Challenge Questions	NCID password policy requires that users set up security questions and responses. A subset of these questions will be used to verify identity during login when a user has forgotten his or her password.
Deactivating [Account]	The process of preventing a user from logging in to NCID and accessing connected resources. Deactivating an account suspends the user's rights or associations. Deactivated accounts can be reactivated by the user's administrator.
Division Delegated Administrator (DA)	A person who can only administer user accounts which are in the same division(s) for which he or she has administrative rights. This person may manage another administrator who is at their level or below. Note: A division DA may administer more than one division; however, these divisions must be part of the same organization.
Forgot Your Password?	A self-service feature which permits a user to reset his or her password without assistance from the Service Desk.
Forgot Your User ID?	A self-service feature which permits a user to recover his or her user ID without assistance from the Service Desk.
End-User	A state or local government employee, a citizen or business person who is authenticated to access NCID. User capabilities are dependent upon the permissions assigned to them by the administrator. NCID self-service features are available to all end-users.
Global Service Desk	A person who can unlock accounts for any user account, excluding a delegated administrator. (Also referred to as ITS Service Desk.)
Identity Self-Service Tab	Provides self-service tools for users to conveniently manage their own account. It also provides access to workflow links to allow delegated administrators and the Service Desk to administer user accounts.
IT Role	The middle level in the roles hierarchy. This role supports technology functions, for example, an application administrator.
ITS Service Desk	A person who can unlock accounts for any user account, excluding a delegated administrator. (Also referred to as Global Service Desk.)
Login	Performs user authentication to NCID.
Minimum Password Age	State password policy requires that a state and local government employee keep a new password for 15 days before it can be changed. Individuals and business users can reset their password after 3 days.

Organizational Delegated Administrator (DA)	A person who can administer user accounts within his or her organization. This person may administer another delegated administrator who is at their same level, but not above them.
Organization Service Desk Administrator	A person who can unlock accounts and reset passwords for any user account that is a member of the same organization. This person may not act upon an account for a delegated administrator.
Password	A user's unique string of characters that is used to authenticate to NCID.
Permission Role	The lowest level in the roles hierarchy, and defines lower-level permissions.
Resource	A NCID connected application, such as Beacon.
Role	A set of permissions related to one or more resources (applications).
Role Assignment	The method of granting a user access to one or more resources (applications). A role assignment can be made directly to a user, in which case a user is given explicit access to a resource associated with the role. A user may also receive a role indirectly by being a member of a group, container or related role.
[Role] Category	A label used to classify a role. Associating a role to a category is not mandatory, but it is helpful when viewing the Role Catalog as you can organize and filter roles by category.
Role Catalog	Contains all of the roles definitions that have been created in the NCID system. Roles are alphabetically displayed and each role's level and associated category are identified. Roles may be sorted and filtered by name, level and/or category.
Roles Hierarchy	Establishes relationships between roles in the catalog. The hierarchy helps simplify the task of granting permissions through role assignments.
Role Level	Indicates the level of the role within the catalog. The following levels (highest to lowest) make up the roles hierarchy: Business Role, IT Role and Permission Role.
Role Reports	Provide designated administrators with the ability to analyze the current state of roles and role assignments. Role reports include: Role List Report and Role Assignment Report.
Role Manager (previously Group Administrator)	A person who can define and modify a role (a set of permissions related to one or more applications), and grant role assignments to users. A role manager also has access to reports to help them analyze the current state of role assignments and user entitlements.
Roles and Resources Tab	Allows application administrators assign resources (applications) to users via role assignment, and access reports to analyze the current state of role assignment and user entitlements.
Section Delegated Administrator (DA)	A person who can only administer user accounts which are in the same section(s) for which he or she has administrative rights. This person may manage another administrator who is at their level or below.
System Administrator	A person who has rights to configure and manage all aspects of the NCID application.

Tabs	The way in which information and application features are organized and displayed in NCID. Currently, the application uses three tabs to present information: *Identity Self-Service*, *Work Dashboard* and *Roles and Resources*. Tab availability will vary based on job responsibility and access permissions.
User ID	A user's unique account ID that is required to authenticate him or her to NCID.
Work Dashboard Tab	Provides a centralized area for users to make a process request, and view the history and status of a request they made.

This page was intentionally left blank

Appendix B: Function Availability for NCID Users

There are several kinds of users in NCID, and what a user can see and do is determined by their job responsibility and level of authority. The following table highlights the functions each user type can perform based on their permissions.

User Type	End-user	ITS Service Desk (Global Service Desk)	Organizational DA Division DA Section DA	Agency Service Desk Administrator	Application Administrator
Identity Self-Service Tab					
Information Management Category					
Run Reports			✓		✓
Update My Account	✓	✓	✓	✓	✓
View My Administrators	✓	✓	✓	✓	✓
NCID Welcome Page	✓	✓	✓	✓	✓
Remove My Account	✓[8]				
Password Management Category					
Password Sync Status	✓	✓	✓	✓	✓
Directory Management Category					
Archive Employee Account			✓		
Create Employee Account			✓		
Deactivate Employee Account			✓		
ITS Service Desk Administration		✓			
Reactivate Employee Account			✓		

[8] The "Remove My Account" function is available to only business and individual account holders. Since these account types are not managed by delegated administrators, this function allows non-employees to deactivate and archive their accounts.

User Type	End-user	ITS Service Desk (Global Service Desk)	Organizational DA Division DA Section DA	Agency Service Desk Administrator	Application Administrator
Identity Self-Service Tab					
Directory Management Category *(continued)*					
Reset Employee Password		✓ (for ITS employees only)	✓	✓	
Unlock Employee Account		✓	✓	✓	
Update Employee Account			✓		
Work Dashboard Tab					
Make a Process Request					
Agency to Agency Account Transfer			✓[9]		
Archive Employee Account			✓		
Create Employee Account			✓		
Deactivate Employee Account			✓		
Demote Application Administrator					✓
Demote Delegated Administrator			✓		
ITS Service Desk Administration		✓			
Promote Application Administrator					✓
Promote Delegated Administrator			✓		
Reactivate Employee Account		✓ (for local government DAs only)	✓		
Reset Employee Password		✓ (for ITS employees only)	✓	✓	
Unlock Employee Account		✓	✓	✓	

[9] Only delegated administrators who are state employees can perform agency to agency account transfers.

User Type	End-user	ITS Service Desk (Global Service Desk)	Organizational DA Division DA Section DA	Agency Service Desk Administrator	Application Administrator
Work Dashboard Tab					
Make a Process Request *(continued)*					
Update Employee Account			✓		
Update My Account	✓	✓	✓	✓	✓
View My Administrators	✓	✓	✓	✓	✓
View Task Notification	✓	✓	✓	✓	✓
Check Request Status	✓	✓	✓	✓	✓
Roles & Resources Tab					
View Role Catalog					✓
View SoD Catalog	Currently unavailable in this NCID release				
Run Role Reports	Currently unavailable in this NCID release				
Run SoD Reports	Currently unavailable in this NCID release				
Run User Reports	Currently unavailable in this NCID release				
Configure Roles and Resources Settings	Utilized by the NCID Administrator only				

This page was intentionally left blank

Index