NCID
Service Desk Guide
Version 1.10

Department of Information Technology
As of July 14, 2016

Document History

Version	Change Reference	Date	Author
1.0	Initial draft release	8/25/10	Heather Ferrie
1.1	Updated: Documentation Org w/Appendices A & B, Logout screens; Added: Section 2.8 Password Sync	8/31/10	Heather Ferrie
1.2	Updated with references to User Guide	9/20/10	Heather Ferrie
	Added new sections: Helping Users Remove Their account, User Types	9/27/10	Heather Ferrie
	Updated Sec 2.3 "Reset" & Sec 2.4 " Unlock" with BR comments	10/5/10	Heather Ferrie
1.3	Update Sec 2.8:Remove (replaced "NCID NG Resources" with "State applications")	10/08/10	Heather Ferrie
	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	12/2/10	Heather Ferrie
	Section 2.10: New section to assist Service Desk users who do not receive email messages from NCID.	12/21/10	Heather Ferrie
1.4	Section 2.2: 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 2.2: 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 2.3: 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
1.5	Removed "NG" reference. Removed Appendix A: Differences b/n 7.x & NG	2/23/11	Heather Ferrie
1.6	Section 3: This is a new section to reference the "Manage SD Users and Admin" workflow	3/16/11	Heather Ferrie
1.7	Section 1.1: Updated definition for Application Administrator. Section 1.2: Updated Figure 1-2; Added "Need Help" feature to "Login Screen Self-Service Features" box.	4/22/11	Heather Ferrie
1.8	Section 1.0: Removed all reference that SD could not unlock DA accounts Section 2.4: Insert "Locked By Source" note	07/13/11	Heather Ferrie

| 1.9 | Section 2.3: Insert note regarding updating passwords on mobile devices. | 07/26/11 | Heather Ferrie |
| 1.10 | Updated for SSPR (Self-Service Password Rest) and other minor changes. | 07/14/16 | Brent Roberts |

This page was intentionally left blank

Table of Contents

This page was intentionally left blank

About this Guide

This guide is designed as a reference for Agency Service Desk agents and DIT (NCID) Service Desk agents. Using this guide, the reader will become familiar with NCID features, and learn how to work with those features to help users resolve problems with their accounts.

Documentation Organization

This guide is organized into the following sections:

Section 1: Getting Started includes an overview of the NCID service, and provides steps for accessing and logging in to NCID. This section also describes the NCID main screen to help familiarize you with how the interface organizes information and displays application features.

Section 2: Tools for Supporting Users describes the various operations that an Agency Service Desk technician and the DIT (NCID) Service Desk can perform on a user account.

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

Feedback

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

Documentation Updates

For the most current version of the *NCID Service Desk 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 and access permissions.

1 Getting Started

The **North Carolina Identity Management Service – Next Generation (NCID)** is the standard identity and access management platform provided by the Office of Information and Technology Services. 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 Service Desk agents[1] with many tools to help users resolve problems with their accounts. Depending on your job responsibility and permissions, you will be able to assist users by performing the following operations:

- Unlock a user account

- Reset a user password

- Look up a user ID

- Help a user reset their own password

- Help a user view their administrator(s) contact information

Before we look at the various methods that you can use to service an account, we will review some 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 become familiar with the NCID interface.

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

---

[1] There are two types of service desk agents which are responsible for supporting user accounts. An *Agency Service Desk* agent refers to a user who has been designated to reset passwords and unlock accounts for state employees within their agency. An D*IT (NCID) Service Desk* agent has the ability to unlock accounts for all NCID users (business, individual, state and local government employees), and can reset passwords for employees within the DIT agency. Neither service desk agent can reset a password for a delegated administrator.

- **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.

- **DIT Service Desk (Global Service Desk**) can unlock accounts for any NCID user. In addition, this person can reset passwords for DIT 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.

1.2 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 7 or higher.

> **Note:** If you do not have an account, please contact your delegated administrator to create one for you.

To access and log in to NCID:

Open a Web browser and enter the following URL: https://ncid.nc.gov.
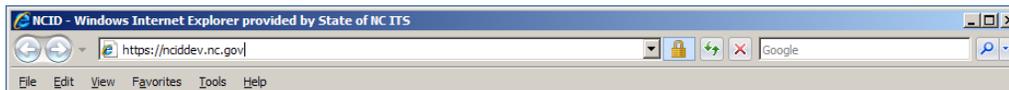
Figure 1-1. Enter URL in the Address Bar

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.

In the "User ID" field, type [your *NCID user ID*].

In the "Password" field, type [your *NCID password*].
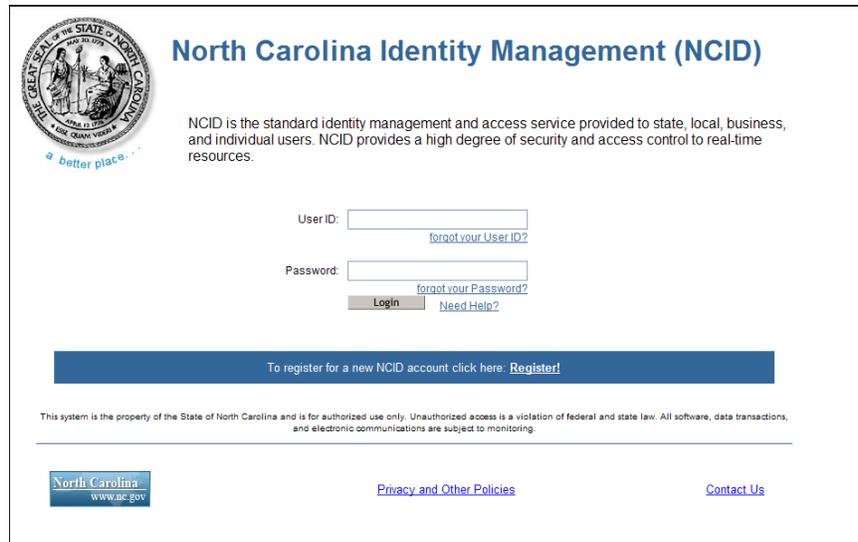
Figure 1-2. North Carolina Identity Management (NCID) Login Screen

Click on **Login**.

After successfully logging in, the NCID main screen is displayed. Please refer to the *Getting Familiar with the Interface* section on page 13 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.

1.2.1 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[2]. The user must successfully answer all five (5) of their challenge questions before they can create a new password and log in. This will also allow them to unlock their account if locked.
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.[3]

---

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

1.3 Getting Familiar with the Interface

After logging in to NCID, all users are 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.
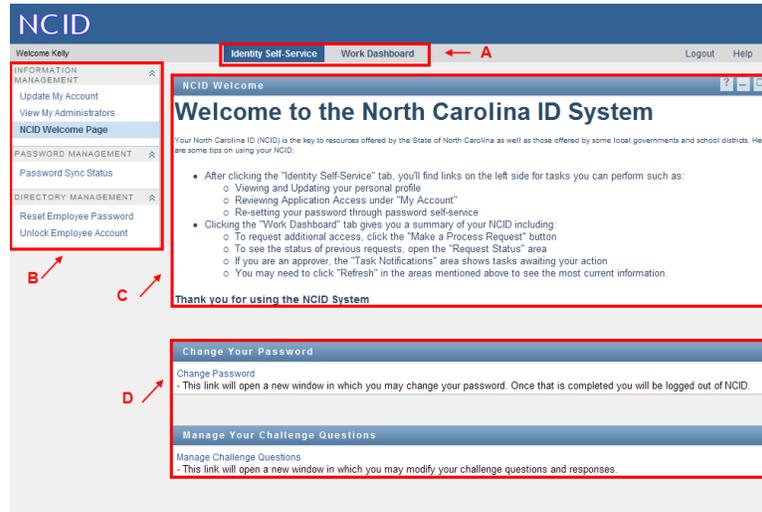
Figure 1-3. NCID Main Screen

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 one 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, unlocking accounts, etc. This tab also provides self-service tools to allow all NCID users 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.

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 access process request forms. The following table highlights the workflow links available to each type of Service Desk agent.

Workflow Link	Service Desk Agent Type	
	Agency Service Desk	DIT (NCID) Service Desk
DIT Service Desk Administration		✓
Reset Employee Password	✓	✓
Unlock Employee Account	✓	

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.

1.4 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.

1.5 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:

Click on the **Logout** Logout link located at the top-right section of your screen.
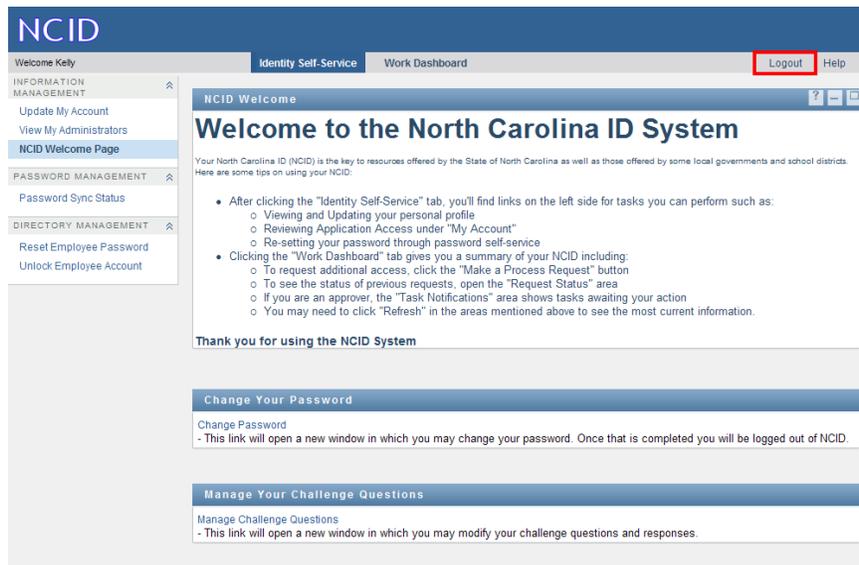
Figure 1-4. Click "Logout"

The "NCID Logout" screen is displayed and indicates that you have successfully logged out of NCID.
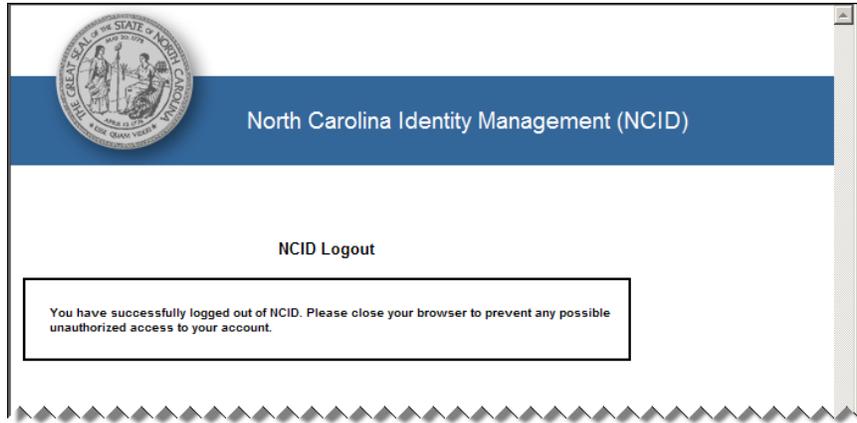
Figure 1-5. NCID Logout Confirmation Message

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

This page was intentionally left blank

2 Tools for Supporting Users

There are various tools available to Service Desk agents to help resolve problems with user accounts. In NCID, actions that you can perform on a user account are categorized as *process requests* and depending on your job responsibility you can perform specific process requests on a user account (i.e.: reset password or unlock account). You can make a process requests via the links on the Identity Self-Service tab or using the "Make a Process Request" feature on the Work Dashboard. Each process request has its own unique form which allows you to lookup the user account that you need to service, and then submit the form to complete the request.

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 using the "Make a Process Request" feature on the Work Dashboard. 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 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. All of the links that you will need are found on the Identity Self-Service tab. This allows you to quickly access process request forms and resolve user problems in a timely manner.

This section describes how you can service a user account using the links found on the Identity Self-Service tab. Please refer the *NCID Administration Guide* if you would like to learn more about how you can service accounts from the Work Dashboard.

2.1 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.
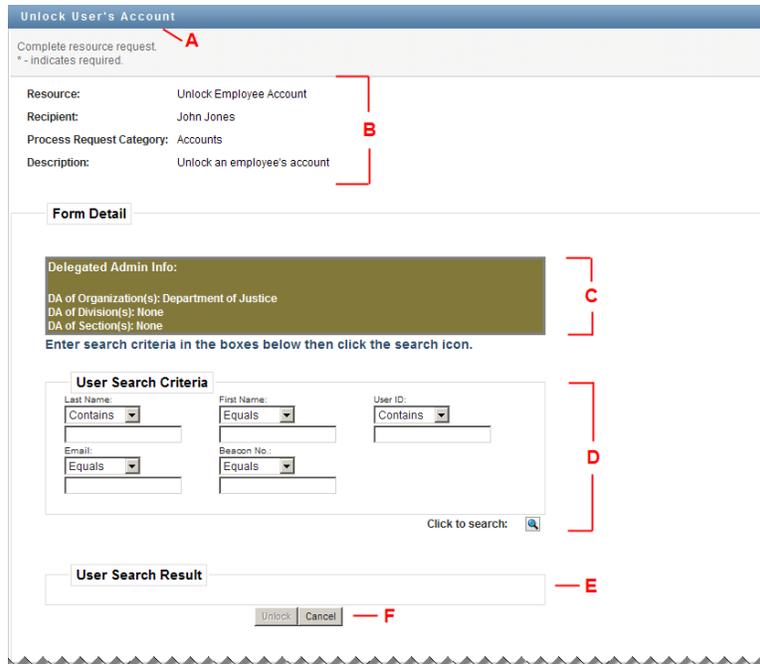
Figure 2-1. Example of a Process Request Form

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

B   This section provides general information about the form:

- 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 information if you a delegated administrator. The names of the organization, division(s) and/or section(s) which you can administer will be shown.

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.

2.2 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 receiving a service desk call, you will need to select the appropriate process request form from the Identity Self-Service 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.

Figure 2-2. "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" = Johnson, might yield many matches, but if we include "First Name" = Daisy 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.

Performing a search:

From the "User Search Criteria" section, you may either:

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 service.

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

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 entire 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.

Figure 2-3. Enter Search Criteria

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.

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

Figure 2-4. Example Search Results

The request form is updated and attributes stored in the selected user's profile are shown in the "User Search Results" section. This section is outlined in green to indicate that you can perform this action on the user account. If the section is highlighted in red, a message alerts you that the action cannot be performed.

Figure 2-5. "User Search Result" Section

If this is the correct user account that you wish to service, you can continue processing the request. If it is not the correct user, you can clear the fields and perform your search again.

2.3 Resetting a User Password

DIT (NCID) Service Desk and Agency Service Desk agents can reset passwords for employees within their agency who have trouble using the "Forgot Your Password" self-service feature. This feature is unavailable to employees who have recently changed their password (within 3 days), or if their account is locked.

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:** DIT Service Desk and Agency Service Desk agents may not reset passwords for delegated administrators. Administrator passwords can only be reset by another delegated administrator who is at the same level or higher.
>
> Additionally, if you receive a service desk call from an employee who is not a member of your agency, please advise the user to contact their agency's delegated administrator or agency's service desk for assistance.

Important Information for DIT Service Desk Agents: You cannot reset passwords for individual and business account holders; however, you can guide the person through the "Forgot Your Password" self-service feature. Please refer to the *Helping User Utilize "Forgot Your Password" Feature* section on page 35 for more information. If the person is unable to successfully answer their Challenge Questions, please advise the user to self-register for a new account.

In the event the user's account is locked, you can unlock it and then ask the user to try resetting the password using the "Forgot Your Password" self-service feature. If the person recently changed their password with 3 days, you can run the workflow to allow the user to reset their password. Customers can also use the SSPR (Self-Service Password Recovery) to unlock their account if they remember the answers to their security questions.

To reset a password:

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.

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).

Figure 2-6. Click on "Reset Employee Password" Link

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 19 for details on how to look up a user account.

Figure 2-7. "Reset Employee Password" Request Form

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.

> **Important!** You will not be able to reset a password for a deactivated account. If the account you selected is deactivated, the "User Search Result" will indicate that the account is "Disabled" in the "Status" field. Please inform the user that he or she must contact their delegated administrator for assistance.

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

Figure 2-8. Verify User Details

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.

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.

Click on Reset Password.

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 the *NCID Administration Guide* for information on using the Work Dashboard.
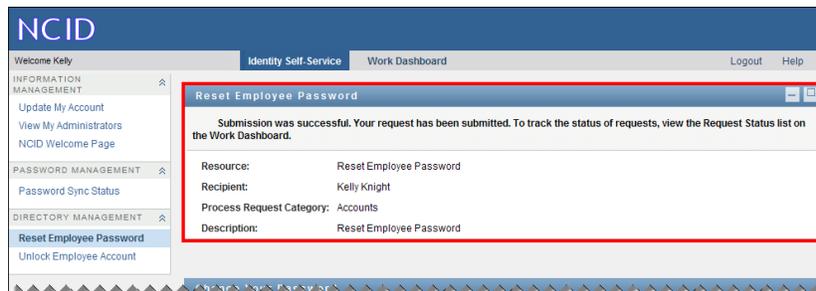
Figure 2-9. Confirmation Message

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.

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.

Please make the user aware that after changing the password, he or she will be automatically logged out of the system, and must log back into NCID with the new password.

> **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 Exchange 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.

2.4 Unlocking a User Account

DIT (NCID) Service Desk and Agency Service Desk agents use different process request forms to unlock an account. This section demonstrates the unlock process for each type of Service Desk agent. Customer who know the answers to all five (5) of their challenge questions and use self-service to unlock their own account.

> **Note:** DIT (NCID) Service Desk agents have permission to unlock accounts for <u>all</u> NCID users, whereas Agency Service Desk agents are permitted to unlock accounts for employees within their agency.

For DIT (NCID) Service Desk Agents:

On the "Identity Self-Service" tab, click D**IT Service Desk Administration** in the menu located on the left side of your screen (this option is listed under the Directory Management category).
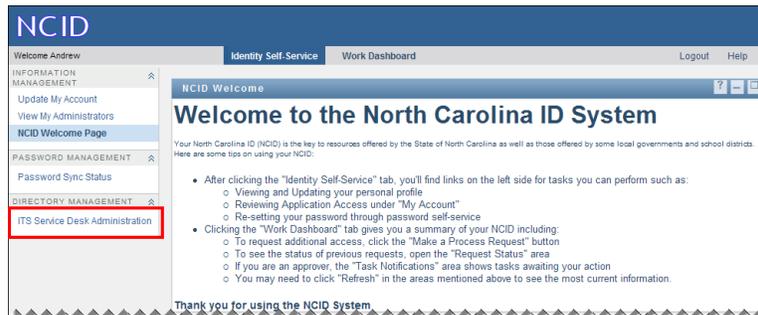
Figure 2-10. Click on "DIT Service Desk Administration" Link

The "Global Service Desk" 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 19 for details on how to look up a user account.

Figure 2-11. "Global Service Desk" Request Form

Once you have selected the account, the request form is updated and displays the user's profile. 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 "Active-Locked" appears in the "Account Status" field to confirm that this is a locked account.

> **Important!** You will not be able to unlock a deactivated account. If the account you selected is deactivated, the user's profile will indicate the account is "Disabled" in the "Account Status" field. Please inform the user that he or she must contact their delegated administrator for assistance.

Note: The "Locked By Source" field provides historical information which identifies the application that locked out a user and when the lockout happened. Reviewing this information can help you see trends of multiple locks and assist with assignment of any resulting tickets.

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

Figure 2-12. Verify User Details

Click on Unlock Account.

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 the *NCID Administration Guide* for information on using the Work Dashboard.

Figure 2-13.Confirmation Message

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.

For Agency Service Desk Agents:

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).
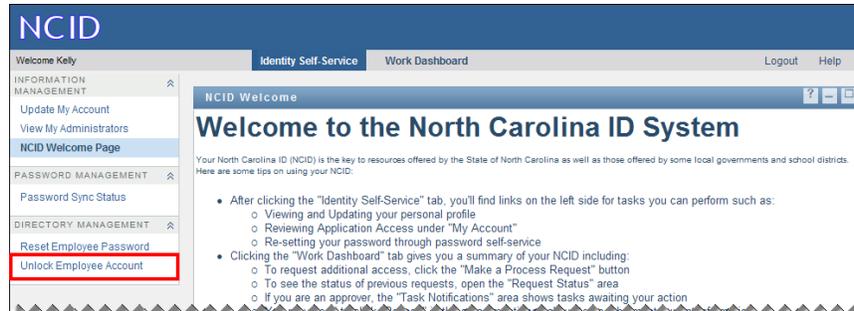

Figure 2-14. Click on "Unlock Employee Account" Link

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 19 for details on how to look up a user account.
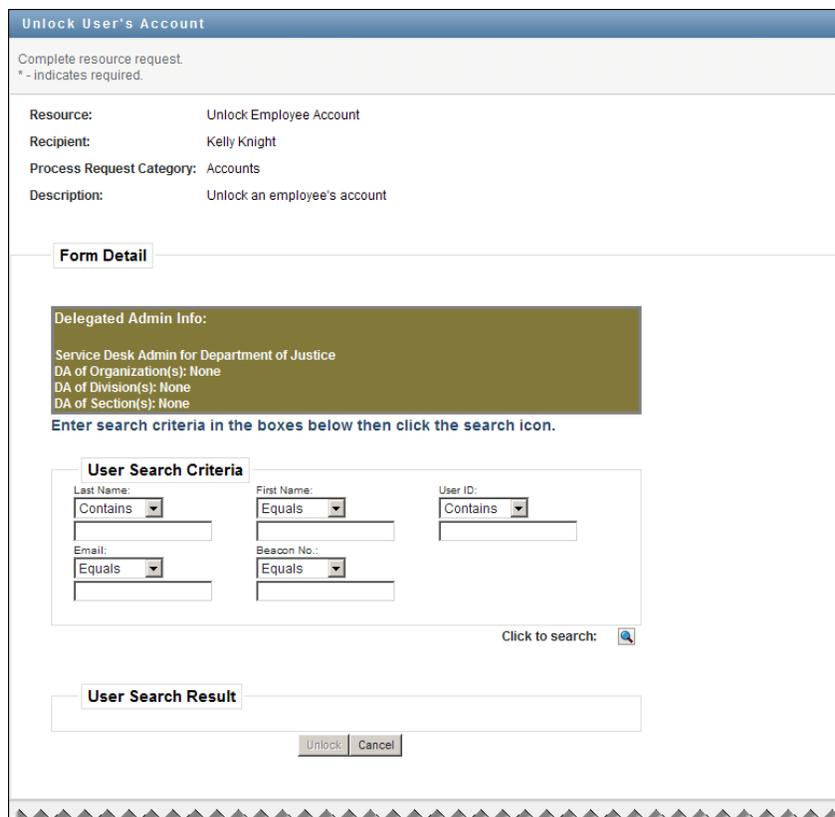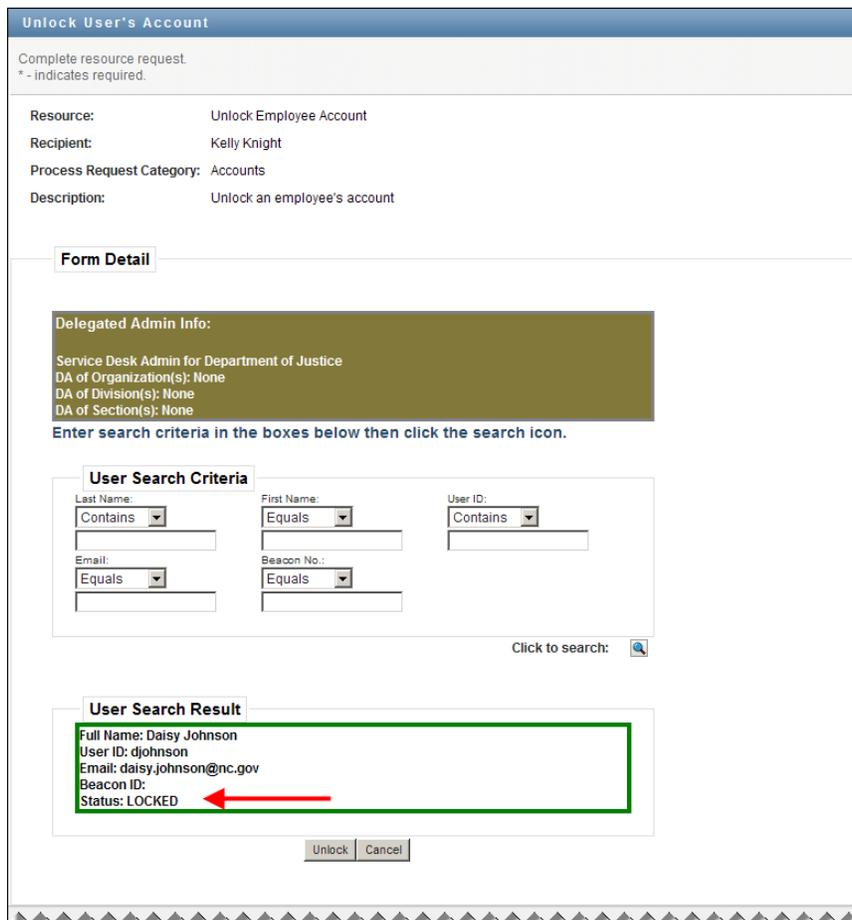

Figure 2-15. "Unlock Employee Account" Request Form

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".

> **Important!** You will not be able to unlock a deactivated account. If the account you selected is deactivated, the "User Search Result" will indicate that the account is "Disabled in the "Status" field". Please inform the user that he or she must contact their delegated administrator for assistance.

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

Figure 2-16. Verify User Details

Click on **Unlock**.

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 the *NCID Administration Guide* for information on using the Work Dashboard.
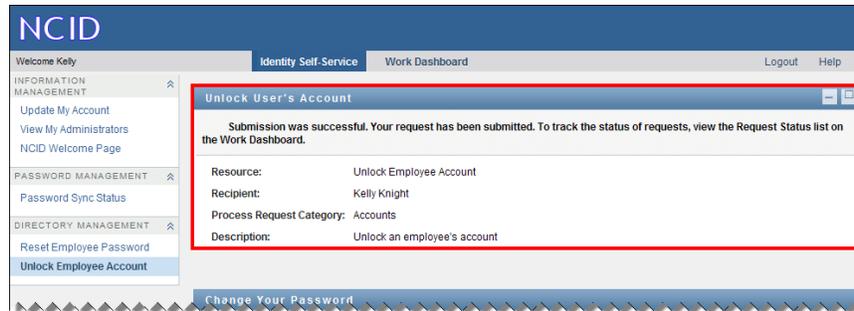
Figure 2-17.Confirmation Message

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.

2.5 Recovering a User ID

If a user cannot remember his or her user ID, you can look it up by using the "Search" feature found on any of the process request forms. Upon finding the correct account, the user ID is displayed in the form's "User Search Results" section.

To look up a user ID:

On the "Identity Self-Service" tab, click on one of the links under the Directory Management category to open a process request form. For our example, we will use the "Unlock Employee Account" link.
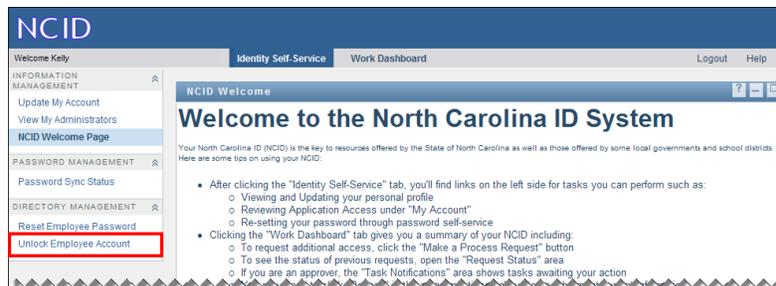

Figure 2-18. Click on "Unlock Employee Account" Link

Look up the user's account. Please refer to the *Searching for a User Account* section on page 19 for details on how to look up a user account.
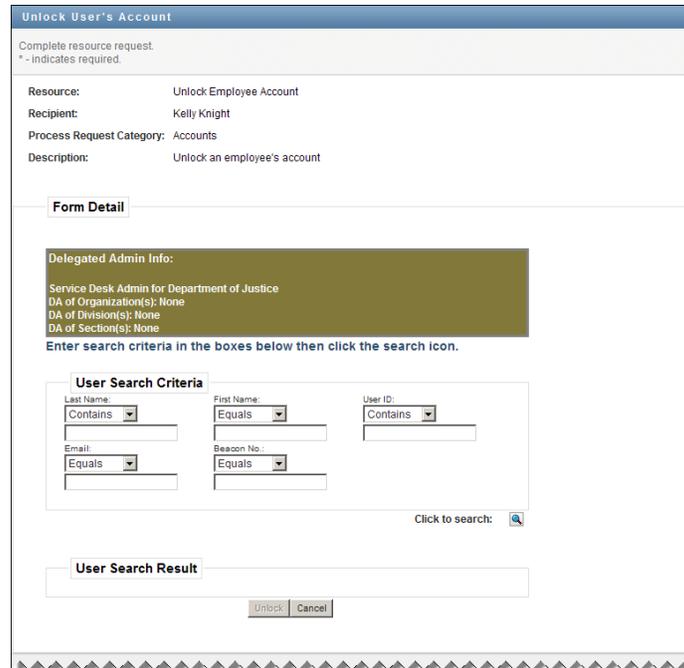
Figure 2-19. "Unlock Employee Account" Request Form

Once you have selected the account, the request form is updated and you will be able to see the user's ID in the "User Search Results" section.
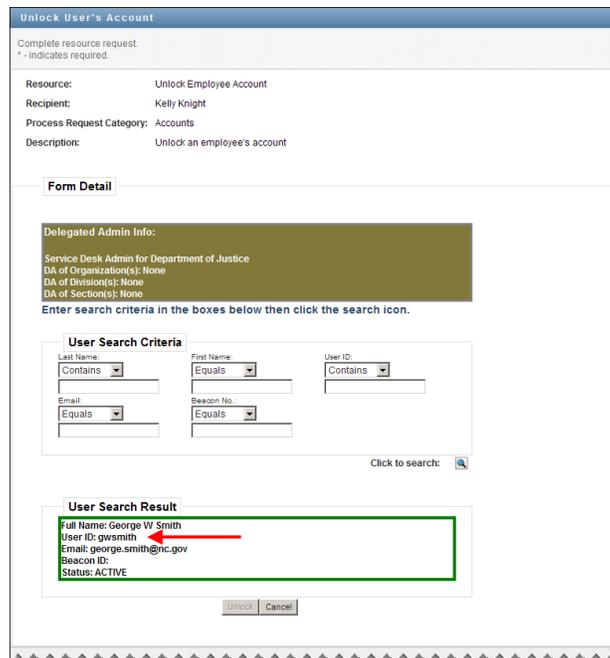

Figure 2-20. View User ID in "User Search Result" Section

Important for DIT (NCID) Service Desk Agents: DIT (NCID) Service Desk agents can look up a user ID on the Global Service Desk form; however, the user ID is displayed on the form's "Account Info" section.

Figure 2-21. Look Up User ID in the "Account Info" Section

2.6 Helping Users Find Their Administrator's Contact Info

You can help users find the name and contact information for each administrator within their agency, division and/or section. This information is available via the link on the user's Identity Self-Service tab.

To assist users finding contact information for their administrators:

Verify that the user is logged into NCID, and the user is on the "Identity Self-Service" tab.

Ask the user to click on the **View My Administrators** link in the menu located on the left side of the screen.

Figure 2-22. Click "View My Administrators" Link

Verify that the "View My Administrators" screen is displayed. Direct the user to the "Administrator Contact Info" section to see a list of names and telephone numbers for administrators in their organization, division and/or section.
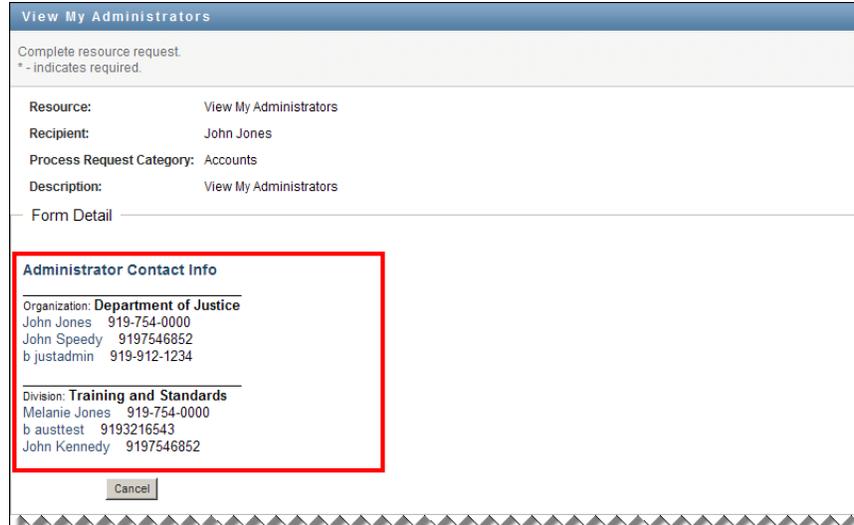

Figure 2-23. View Administrator Contact Information

2.7 Helping Users Utilize "Forgot Your Password" Feature

This section provides a brief overview of the "Forgot Your Password" feature that is located on the "Login" screen. It is important to familiarize yourself with the feature's various screens in the event a user has trouble resetting their password and requests assistance from the Service Desk.

> **Note:** The "Forgot Your Password" feature can only be performed by an account holder. A person will not be able to use this feature if the password was recently changed (the minimum password expiration requirement 3 days). The user will need to provide his or her user ID and answer their challenge questions so that the system can confirm the person is an account holder.

To use the "Forgot Your Password" feature:

On the "NCID Login" screen, the user must type their user ID in the "User ID" field. The system cannot reset the password without a valid user ID.
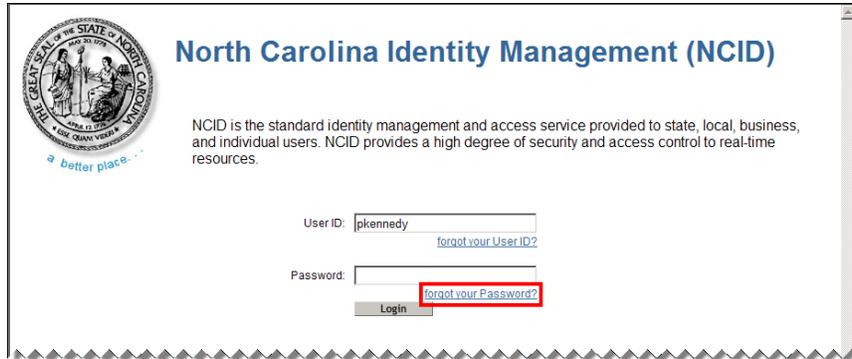

Figure 2-24. Enter "User ID" and Click "Forgot Your Password"

Upon clicking on the **Forgot Your Password/Unlock Account** link, the "Forgotten Password" screen is displayed. The user ID appears in the "User ID" field.
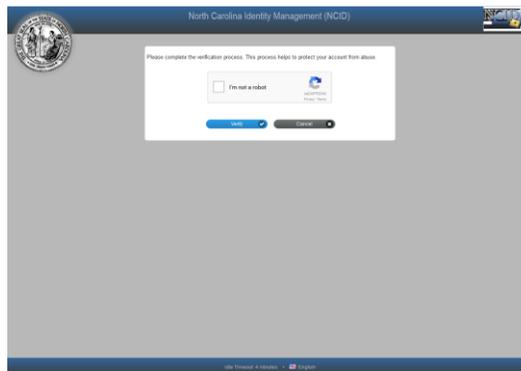

Figure 2-25. "Forgotten Password" Screen

The user will select the correct information and pictures once they click on **Verify** to display the "Forgotten Password – Challenge Questions" screen.

> **Note:** If the user has not set up his or her challenge questions and responses, a message alerts the user to call the Service Desk for assistance. You will need to reset the user's password, and provide him or her with the temporary one. Inform the user that upon logging in he or she will be prompted to change the password and then set up questions.
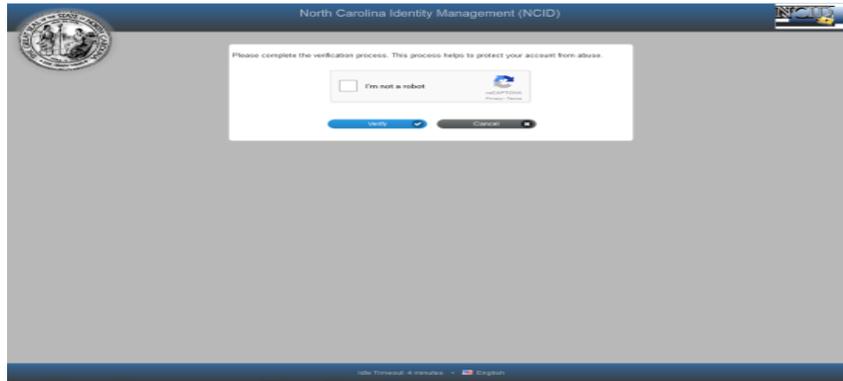
Figure 2-26.Call Service Desk Message

The user must answer the challenge questions presented on the screen. The answers are not case-sensitive; however, the answer must include every character (including punctuation) that were specified when the challenge questions were setup.
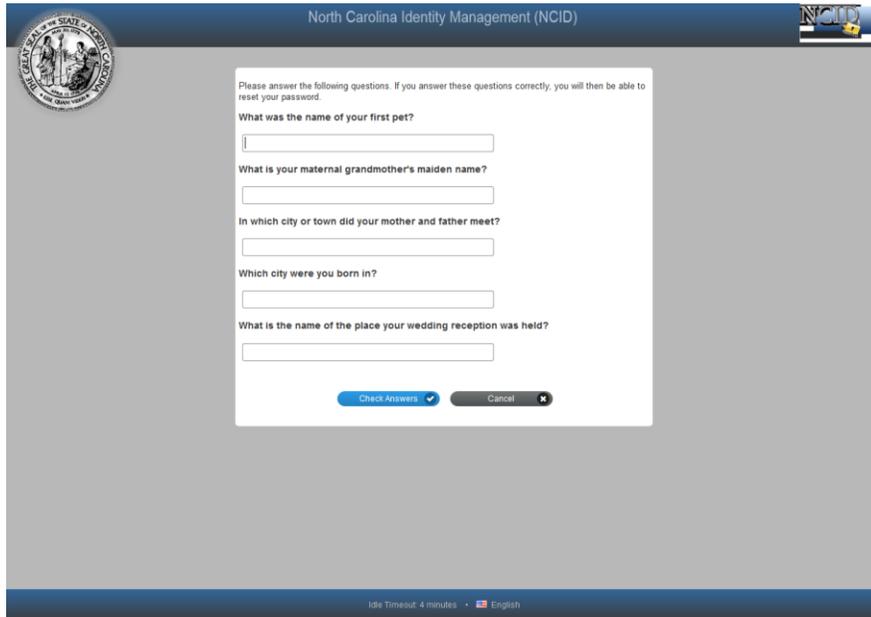

Figure 2-27. Answer Your Challenge Questions

Click on **Login**.

> **Note:** A message will display if the user failed to correctly answer any of the challenge questions. The account will lock after three (3) failed attempts; however, the user can try to log in again after 30 minutes, or he or she may request that their account be unlocked sooner by a delegated administrator or the Service Desk.

The "Change Password" screen is displayed, and he or she can enter a password in the "New Password" field. Tell the user that screen indicates whether the password conforms to the State's password policy. As the

password is entered, the screen indicates whether the password has met each policy requirement by displaying either ✔ or ⊘ .

> **Note:** Remind the user that NCID passwords are case-sensitive, and must be entered <u>exactly</u> as they were originally entered.

The user must retype the password in the "Re-Enter New Password" field.

After clicking on **Change Password**, the "NCID Logout" screen is displayed. Ask the user to wait a few seconds while their existing password is synchronized across the applications that they are permitted to access.

Inform the user that a **Continue** link will appear when the password synchronization is complete, and he or she will need to click on it to log in to NCID again.

> **Note:** Inform the user that he or she will receive email message to notify them that the password has been successfully changed.
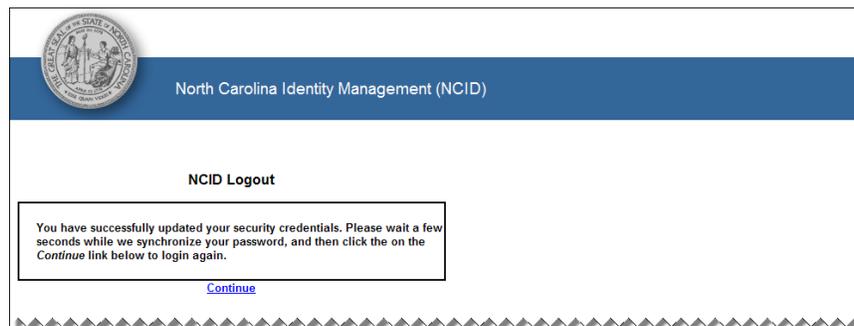

Figure 2-28. "NCID Logout" Screen

2.8 Helping Users Remove Their User Account

This section provides a brief overview of the "Remove My Account" link that is located on the "Identity Self-Service" screen. This feature is only available to individual and business account holders so they can remove (archive) their account when they no longer need to access State applications. It is important to familiarize yourself with the feature's various screens in the event a user has trouble removing his or her account and requests assistance from the Service Desk.

> **Note:** State or local government employee accounts must be deactivated and then archived by the account holder's administrator.

To assist individual and business account holders remove their account:

Verify that the user is logged into NCID, and the user is on the "Identity Self-Service" tab.

Ask the user to click on the **Remove My Account** link in the menu located on the left side of the screen.
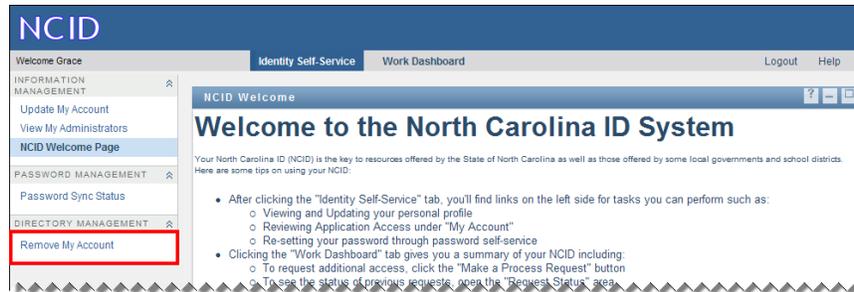
Figure 2-29. Click "Remove My Account" Link

Verify that the "Self Service User Archive" screen is displayed. Remind the user that once the account is removed it cannot be reinstated, and he or she will need to self-register for a new account if they need to access NCID resources again. Tell the user to click on **Remove my Account** to delete the account, or click on **Cancel** stop the operation.
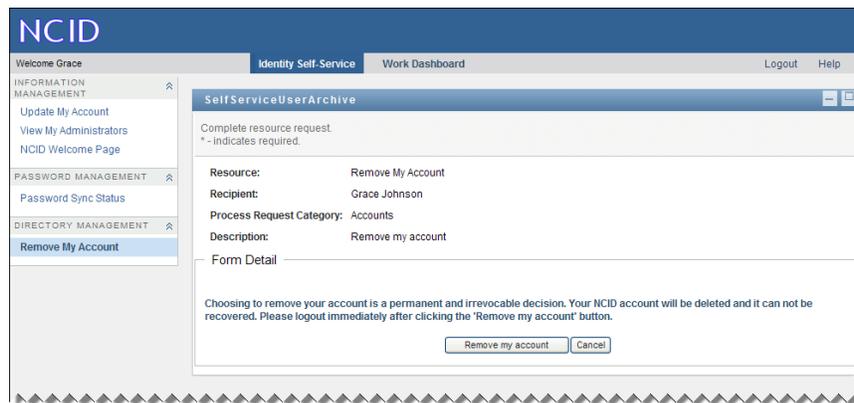

Figure 2-30. "Self-Service User Archive" Screen

Instruct the user to close the browser window.

2.9 Helping Users Who Do Not Receive Email Messages from NCID

Some users may not receive NCID messages in their Inboxes, because their email account is most likely treating the message from NCID as spam. To ensure that NCID messages will always be delivered to the user's Inbox, please ask the user to verify that their email client and email provider are set up to accept messages from **ncid.notifications@nc.gov**.

> **Note:** For users who have just registered for a new account, and have not received the activation email in their Inbox, please ask the user to verify that the message was not marked as spam and sent to the Junk Email folder. If this happens, instruct the user to move the message to their Inbox so they can validate the new account.

3 Managing Service Desk Users and Administrators

The "Manage Service Desk Users and Admin" workflow allows you to grant users permission to perform Service Desk functions, as well as allows you to manage the actions that existing agents can take on a user account. To use this workflow you must be a Service Desk administrator that is assigned to manage one or both Service Desk roles. Depending upon your permissions, you may be able to assign (or remove) a user to a role which permits (or prohibits) the agent to reset passwords and/or unlock accounts for users that they manage.

This workflow is beneficial, because it allows you to independently manage Service Desk agents without assistance from the NCID team. It also provides the flexibility to let you assign a peer as an administrator to one or both Service Desk roles so that the person can then manage Service Desk members and/or administrators.

This section demonstrates how you can assign and manage Service Desk agents and administrators to the following roles:

- Service Desk Password Reset
- Service Desk Unlock Account

Assigning and managing Service Desk agents and administrators:

Note: You must be a Service Desk administrator of the role you wish to assign/manage.

On the "Work Dashboard" tab, click on the **Make a Process Request** button to display the "Make a Process Request" screen.
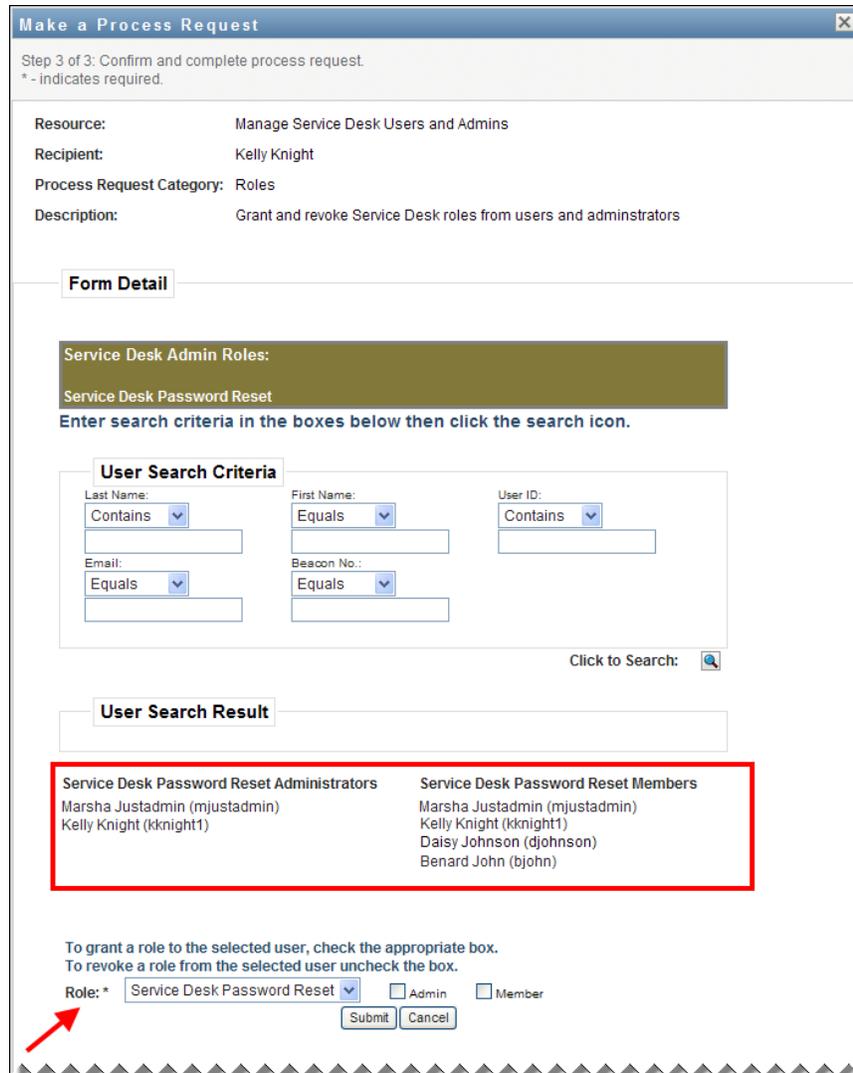
Click on **Continue** to view a list of workflow processes available to you, and select **Manage Service Desk Users and Admins**.
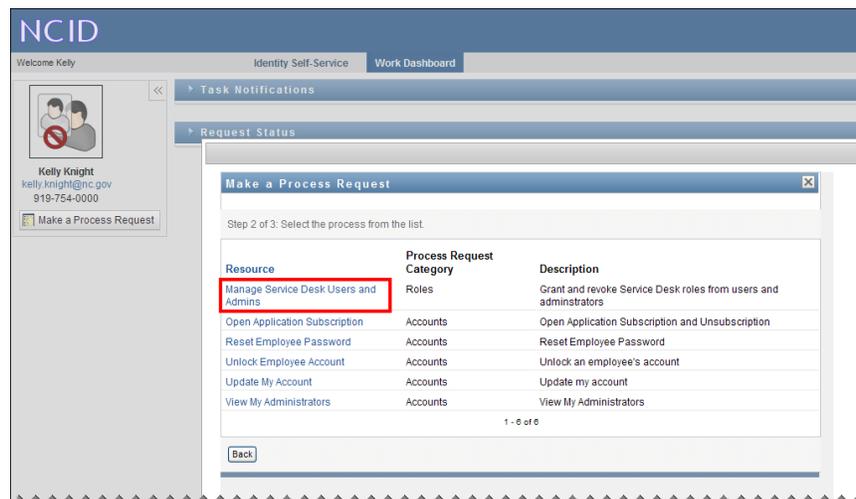
3-1. Select 'Manage Service Desk Users and Admins'

The "Manage Service Desk Users and Admins" request form is displayed.

> **Important!** By default, the request form identifies a list of administrators and members (agents) who have been assigned to the "Service Desk Password Reset" role (refer to the figure below). To see a list of administrators and members assigned to the "Service Desk Unlock Account" role, select it from the "Role" dropdown menu. The screen refreshes and shows the names of the administrators and members assigned to that role.

Figure 3-2. Viewing Role Administrators and Members

1. You will need to search for the account you wish to manage. In the "User Search Criteria" section, filter your search by entering specific criteria into one or more of the available fields, and click on the **Search** icon 🔍. (Please refer to the *Searching for a User Account* section on page 19 for details on how to look up a user account.)

> **Note:** The value displayed in the "Role" field will not affect your search results.

Figure 3-3. "Manage Service Desk Users and Admins" Request Form

Click on the appropriate account on "Search Results" screen.

The request form is updated and displays selected attributes from the user's profile in the "User Search Result" section.

A checkmark will be displayed in the "Admin" and/or "Member" checkboxes if the user has already received one or both of these designations.

Figure 3-4. Updated User Search Result Section

To grant access to a role, select the appropriate role from the "Role" dropdown menu, and then click on the **Admin** and/or **Member** checkbox. Click on **Submit**.

Selecting "Admin" allows the user access to the "Manage Service Desk User and Admin" workflow, and permits the user to manage the role that was specified in the dropdown menu.

Selecting "Member" allows the user access to the "Reset Employee Password" workflow or the "Unlock Employee Account" workflow, depending on the role that was specified in the dropdown menu.

To revoke access from a role, select the appropriate role from the "Role" dropdown menu and click on the **Admin** and/or **User** checkbox to remove the checkmark. Click on **Submit**.

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 the *NCID Administration Guide* for information on using the Work Dashboard.

Note: The process request form will only let you submit a request for one role at a time. You will need to submit a separate request form if the user needs to be a member and/or admin for another Service Desk role.

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.
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 DIT 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.
DIT 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.
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.

Index