



NCID

# NCID

## Quick Start for Developers

### Version 2.9

Department of Information Technology  
As of July 14, 2016

## Document History

| Version | Change Reference   | Date     | Author         |
|---------|--|----------|----------------|
| 1.0     | Initial draft  | 4/28/10  | Heather Ferrie |
| 2.0     | Updated with comments from Review Meeting<br>Removed Part 1 (User Provisioning Before NCID Administrator and User Migration)<br>Introduction: Included reference to 7x docs<br>Section 1: Included Web addresses<br>Section 2: Removed reference to required fields.<br>Section 3.2: Edited typo in step 4<br>Section 3.6: Edited search functionality in step 1<br>Section 5: Updated title: 'Managing Resources ( <a href="#">Applications</a> )'  | 5/6/10   | Heather Ferrie |
| 2.1     | Updated Appendices with content from Brian Austin  | 5/6/10   | Heather Ferrie |
| 2.2     | Updated with comments from Bryn Townsend<br>Section 3.3: Updated 'lock/unlock account' functionality.<br>Section 3.4: Removed 'personal' information reference.<br>Appendix A: Updated title: ' <a href="#">Application</a> Migration Checklist' and formatted tables<br>Section 2.0: Updated title: ' <a href="#">Provisioning</a> <a href="#">Creating</a> User Accounts'  | 5/11/10  | Heather Ferrie |
| 2.4     | New Sections: 3.2.2 Reactivating Account, 3.2.3: Archiving Account<br>3.4: Unlock, 3.6: Transfer Account, 5.1: Granting App Access, 5.2: Remove App Access, Updated Sections: 2 Create Acct, 3.1: Search, 4.1 Promote DA; 4.2: Demote DA   | 10/7/10  | Heather Ferrie |
| 2.5     | Updated: Section 1 (text size setting); Section 2: (14 day expiration for unclaimed S&L accounts ) Inserted new section: 6 Managing Application Administrators<br>Removed "Draft" designation.<br>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.<br><a href="https://www.ncid.its.state.nc.us/TrainingAndDocumentation.asp">https://www.ncid.its.state.nc.us/TrainingAndDocumentation.asp</a>  | 12/10/10 | Heather Ferrie |
| 2.6     | Section 3.1: 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.<br>Section 3.1: Updated step 3 to reference that Object Lookup screen opens in <u>separate</u> window and included note to inform that the screen may open behind the main screen.<br>Section 3.3: 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. | 01/07/11 | Heather Ferrie |
| 2.7     | Section 3.6: Update w/new content for "Email Disposition Question" field and updated figures.<br>Removed "NG" reference.   | 2/23/11  | Heather Ferrie |
| 2.8     | Removed Appendices A: Migration Checklist  | 08/12/11 | Heather Ferrie |



---

|     |   |          |                  |
|-----|---|----------|------------------|
| 2.9 | Updated for SSPR (Self-Service Password Recovery) | 07/14/16 | Brent<br>Roberts |
|-----|---|----------|------------------|

## Table of Contents

|   |    |
|---|----|
| Document History .....  | 2  |
| Table of Contents.....  | 4  |
| Introduction .....  | 5  |
| Feedback.....   | 5  |
| Documentation Updates.....                                      | 5  |
| Formatting Conventions .....                                    | 5  |
| Special Notes .....   | 6  |
| 1 Accessing and Logging in to NCID.....                         | 7  |
| 1.1 Using 'Forgot Your Password' .....                          | 7  |
| 1.2 Using 'Forgot Your User ID' .....                           | 8  |
| 2 Creating an Employee Account.....                             | 9  |
| 3 Managing User Accounts .....                                  | 10 |
| 3.1 Searching for a User Account.....                           | 10 |
| 3.2 Deactivating, Reactivating and Archiving an Account .....   | 11 |
| 3.2.1 Deactivating a User Account.....                          | 12 |
| 3.2.2 Reactivating an Account .....                             | 13 |
| 3.2.3 Archiving an Account .....                                | 13 |
| 3.3 Resetting a User Account .....                              | 14 |
| 3.4 Unlocking a User Account .....                              | 15 |
| 3.5 Recovering a User ID.....                                   | 16 |
| 3.6 Transferring a State User Account .....                     | 16 |
| 3.6.1 Initiating a User Account Transfer to a New Agency .....  | 16 |
| 3.6.2 Claiming and Approving an Agency Account Transfer .....   | 17 |
| 3.6.3 Cancelling an Agency Account Transfer .....               | 18 |
| 3.7 Transferring a State User Account (Intra-Agency) .....      | 19 |
| 3.8 Checking the Status of a Request .....                      | 19 |
| 4 Managing Administrators.....                                  | 21 |
| 4.1 Promoting User Account to Delegated Administrator .....     | 21 |
| 4.2 Demoting a User Account from Delegated Administrator.....   | 22 |
| 5 Making Resource (Application) Assignments.....                | 24 |
| 5.1 Granting Application Access.....                            | 24 |
| 5.2 Removing Application Access .....                           | 24 |
| 6 Managing Application Administrators.....                      | 26 |
| 6.1 Promoting User Account to Application Administrator .....   | 26 |
| 6.2 Demoting a User Account from Application Administrator..... | 26 |

## Introduction

This document will provide steps to managing users in the NCID system.

---

Note: For detailed instruction on how to manage accounts and grant application access to users, please refer to the *NCID Administration Guide* at: [https://www.ncid.its.state.nc.us/NCID\\_Training\\_Materials.asp](https://www.ncid.its.state.nc.us/NCID_Training_Materials.asp)

---

Topics included in this document:

- Accessing & Logging in to NCID
- Creating a User Account
- Managing User Accounts
- Managing Administrators
- Managing Resource (Application) Assignment
- Managing Application Administrators

## Feedback

Please send your comments and suggestions about this guide to the ITS Service Desk at [its.incidents@its.nc.gov](mailto:its.incidents@its.nc.gov).

## Documentation Updates

For the most current version of the *NCID Quick Start for Developers* 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 Accessing and Logging in to NCID

To begin using the NCID service, you will need to open a Web browser and log in using your existing NCID user ID and password. Your user credentials and attributes have been migrated to the new system to allow you access to the NCID environment.

**Note:** Recommended browsers for NCID are Internet Explorer 10 or higher.

## To access and log in to NCID:

1. Open a Web browser and enter one of the following in the address bar:
2. <https://nciddev.nc.gov> (NCID development environment)
3. <https://ncidpp.nc.gov> (NCID pre-production environment)
4. 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.

5. In the “User ID” field, type [NCID user ID].
6. In the “Password” field, type [NCID password].
7. Click on **Login**.
8. After successfully logging in, the main screen (also referred to as the “NCID Welcome Page”) is displayed.

**Important!** Upon logging in to NCID, the system might prompt you to Reset your password if it is past its expiration date and set up your challenge questions and responses.

## 1.1 Using ‘Forgot Your Password’

The functionality of this self-service feature in the NCID system is identical to the current system. Please refer the *NCID User Guide* for information on using this service.

### Important!

- A user is allowed three (3) attempts to reset their password using this feature. The account will lock if the user cannot successfully answer the challenge questions after the third attempt. The system will automatically unlock the account after 30 minutes. Once the account is unlocked, the user can attempt to use the “Forgot Your Password” feature again or try to log in to NCID if he or she remembered their password. If the user continues to have a problem logging in or resetting the password, you can reset it for him or her.
- A user will not be able to use this feature if the password was recently changed (the minimum password expiration requirement is 3 days for state and local government employees).

## 1.2 Using 'Forgot Your User ID'

The functionality of this self-service feature in the NCID system is identical to the current system. Please refer the *NCID User Guide* for information on using this service.



## 2 Creating an Employee Account

This section describes how to create a user account for a state or local government employee. In the new NCID environment, accounts for state and local government employees are no longer created via the self-registration process. These account types are created by the Delegated Administrators (DAs) associated to the employee's organization/division and/or section.

---

**Note:** New user accounts for business users, individuals and some local government agency employees will continue to be created via the self-registration service. Upon self-registering, the user will receive an email which contains an activation URL link needed to complete registration.

Accounts that are self-registered will not be vetted or approved and will not be managed by an administrator. Self-service tools are available to help users manage their accounts such as, permitting users to update their account with new information, resetting passwords and recovering user ID. Please refer to the *NCID User Guide* for more information.

---

### To create an employee account:

1. On the “Identity Self-Service” tab, click **Create Employee Account** in the menu located on the left side of your screen (this option is listed under the “Directory Management” category).
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.
3. Click on **Create User**. 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<sup>1</sup>:
  - (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)

---

<sup>1</sup> Please refer the user to the NCID User Guide for information on managing passwords and challenge questions.

### 3 Managing User 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.

---

#### 3.1 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 Work Dashboard tab, and then look up the account by using the Search feature found on the form.

The Search utility 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 Utility provides 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.

#### Performing a search:

1. Enter your search criteria into the appropriate fields.

**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.

2. Click on the **Search** icon .
3. The “Search Results” screen opens in a separate window and alphabetically displays a list of user accounts which match the search criteria you entered.

**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.

4. Click on the appropriate user account and you will return to the process request form.
5. 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 the section is highlighted in red, a message alerts you that the action cannot be performed

6. 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.

## 3.2 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 use any NCID resource including the password reset feature.

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; for example, if 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.

---

### 3.2.1 Deactivating a User Account

When a user is no longer associated to your organization, their account should be deactivated to prevent the person from accessing the NCID service. Deactivation ensures that your organization does not allow unauthorized users to have access to NCID protected resources.

---

**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 16 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).
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 10 for details on how to look up a user account.
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.
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 19 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 for more information

---

### 3.2.2 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 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).
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 10 for details on how to look up a user account. The search will return a list of deactivated user accounts that you can manage.
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.
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 19 for more information.

### 3.2.3 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.

**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).
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 10 for details on how to look up a user account.
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.
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 19 for more information.

### 3.3 Resetting a User Account

You can reset passwords for employees 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:** You must be an administrator of the user or be assigned to a role that can reset passwords for your organization.

---

#### 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).
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 10 for details on how to look up a user account.
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
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.
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 19 for more information.

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 emphasize that passwords must be entered exactly as they were originally entered.

**Important!** 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.

### 3.4 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:** You must be an administrator of the user or be assigned to a role that can unlock a user account for your organization.

#### 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).
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 10 for details on how to look up a user account.
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”.
4. If this is not the appropriate user, you can clear the fields and perform your search again.
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 19 for more information.
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.

### 3.5 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).
2. Look up the user’s account. Please refer to the [Searching for a User Account](#) section on page 10 for details on how to look up a user account.
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.

### 3.6 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.

**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.

#### 3.6.1 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 10 for details on how to look up a user account.
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.
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.
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.
9. Note: 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.
10. Click on **Transfer User**.
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 19 for more information.
12. 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.


### 3.6.2 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:
  - a. Clicking on the link in the notification email.

Or

  - b. Moving to the “Work Dashboard” tab and clicking on the  icon in front of **Task Notifications**.
2. 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.
3. You may also view a list of steps performed during the transfer process by clicking on the **View Comment History** button.
4. 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. Should you change your mind, you can release the task back to the task list by clicking on the **Release** button.
5. The screen will display your name next to the “Claimed By” field to indicate that you have claimed the task.
6. 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.)
7. 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.
8. 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

---

### 3.6.3 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.
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.

### 3.7 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).
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 10 for details on how to look up a user account.
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**.
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 for more information.

### 3.8 Checking the Status of a Request

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**.
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”.
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.

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.
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.
6. You can view additional details about a request by clicking on the  icon next to **Comment and Flow History**.

## 4 Managing 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)

### 4.1 Promoting User Account to Delegated Administrator

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

---

**Note:** It is 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.

---

**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 10 for details on how to look up a user account.
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.

---

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 19 for more information.

## 4.2 Demoting a User Account from Delegated Administrator

Administrator rights can be taken away from a user by removing the administrator role(s) assigned to the user account.

**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 10 for details on how to look up a user account

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.

---

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 19 for more information.

## 5 Making Resource (Application) Assignments

In the NCID environment access to system resources (applications) is assigned via roles. A *role* defines a set of permissions to resources, and *role assignments* can be directly associated to a user. Roles to resources (applications) are managed on the “Roles and Resources” tab.


### 5.1 Granting Application Access

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. If you are an Application Administrator, click on the **Roles and Resources** tab.
2. The “Role Catalog” section alphabetically displays a list of roles that have been created in the system. Each role’s level and associated category are identified.

---

**Note:** The screen displays up to 25 roles at a time. To page through the list, click on the **Next** icon . You may also change the number of roles displayed on a page, by selecting a number in the “Rows” dropdown menu at the top of the screen.

---

3. You will need to choose the appropriate role. To filter the list of roles:
4. Click on the **Filter** icon  at the top of the screen to display the “Filter” pop-up window.
5. Enter or select filter criteria into one or more of the fields or menus.
6. Click **Filter**. The “Role Catalog” screen displays an updated list of roles matching the filter criteria you selected.
7. Click on the checkbox next to the appropriate Role and click on **Assign**. The “Assign Role” pop-up window is displayed.
8. Specify the following details for the assignment:
9. In the “Initial Request Description” field, enter a brief reason for the assignment request.
10. In the “Type of Assignment” dropdown menu, select **User**.
11. Click on the **Search** icon next to the “Select User(s)” field. You may specify one or more users to assign the role.
12. Optionally, you may specify the date when you want the assignment to take effect, and/or you can indicate whether you want the assignment to have an expiration date.
13. Click on **Assign**.
14. 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.

---

### 5.2 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” section. You can search for the role by scrolling through the list, or you can specify filter criteria to quickly find the role.
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.
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.
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.

## 6 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.

---

### 6.1 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 10 for details on how to look up a user account.
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.

---

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 19 for more information.

### 6.2 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 10 for details on how to look up a user account.
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.
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 19 for more information.