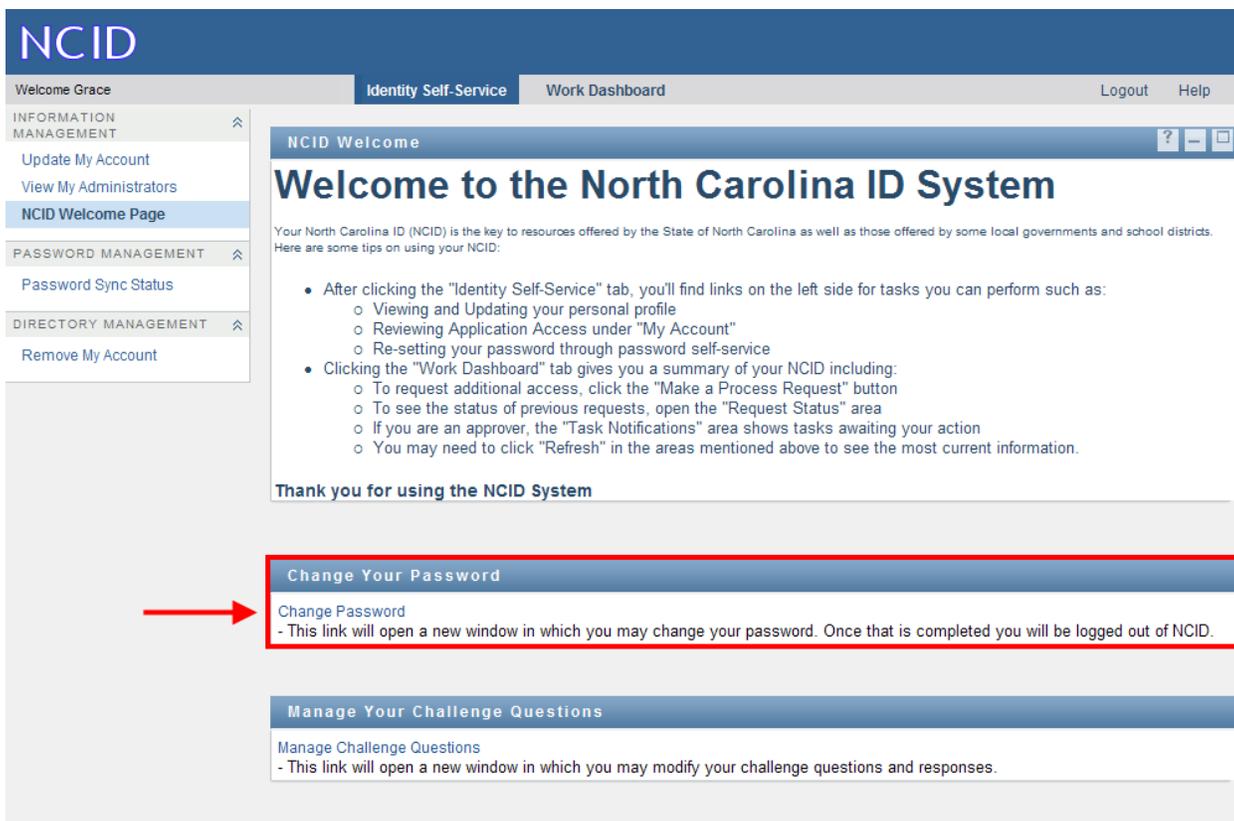# Changing Your NCID Password

You may change your password by using the "Change Password" link featured on the main screen (NCID Welcome Page). Upon making the change, you will be logged out of the system, and must log back into NCID with the new password.

Important*! You will not be permitted to change your password if you have recently changed it. Currently, for state and local government employees, a password must be used for 15 days before it can be changed. Individuals and business users can reset their password after 3 days. Typically, passwords for state and local government employees will expire every 90 days; however, passwords for some state employees, who have more privileges, will expire every 30 days.*

To reset/change a password:
1. Go to https://ncidp.nc.gov .Log on using your NCID user id and password. On the main screen, click on the Change Password link (this option is located in the middle of the screen in the "Change Your Password" section).
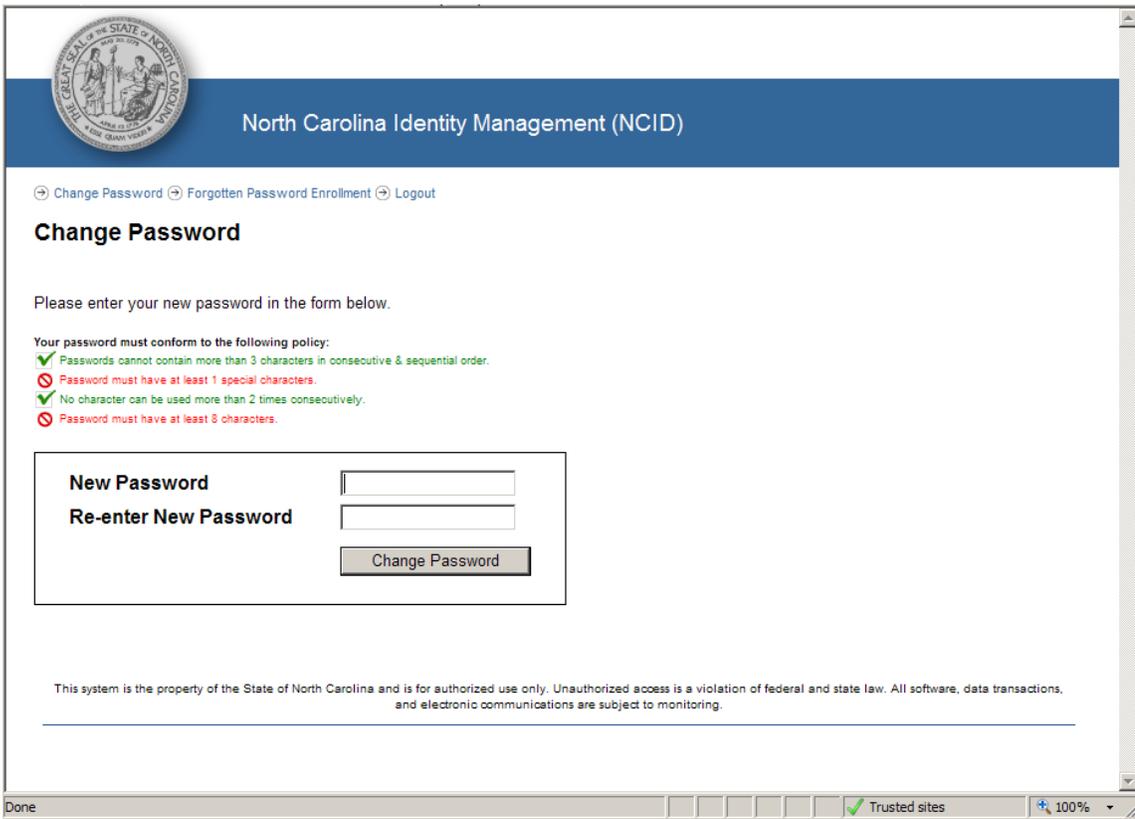

Click on "Change Password" Link Screen

2. The "Change Password" screen is displayed and prompts you to enter a password in the "New Password" field.

Note: The screen indicates whether the password complies with the State's password policy. Notice that as you type the password, each requirement listed on the screen turns from red to green and the screen displays either ✔ or ⊘ to indicate whether the password has met each policy requirement.

Change Password" Screen

3. Type the password again in the "Re-enter New Password" field.
4. Click on Change Password.

Note: A message will alert you that you cannot change your password if you try to change it before the minimum password age has expired.

5. The "NCID Logout" screen is displayed. A message informs you that your security credentials have been successfully updated and asks you to wait a few seconds while your password is synchronized across the applications that you are permitted to access.
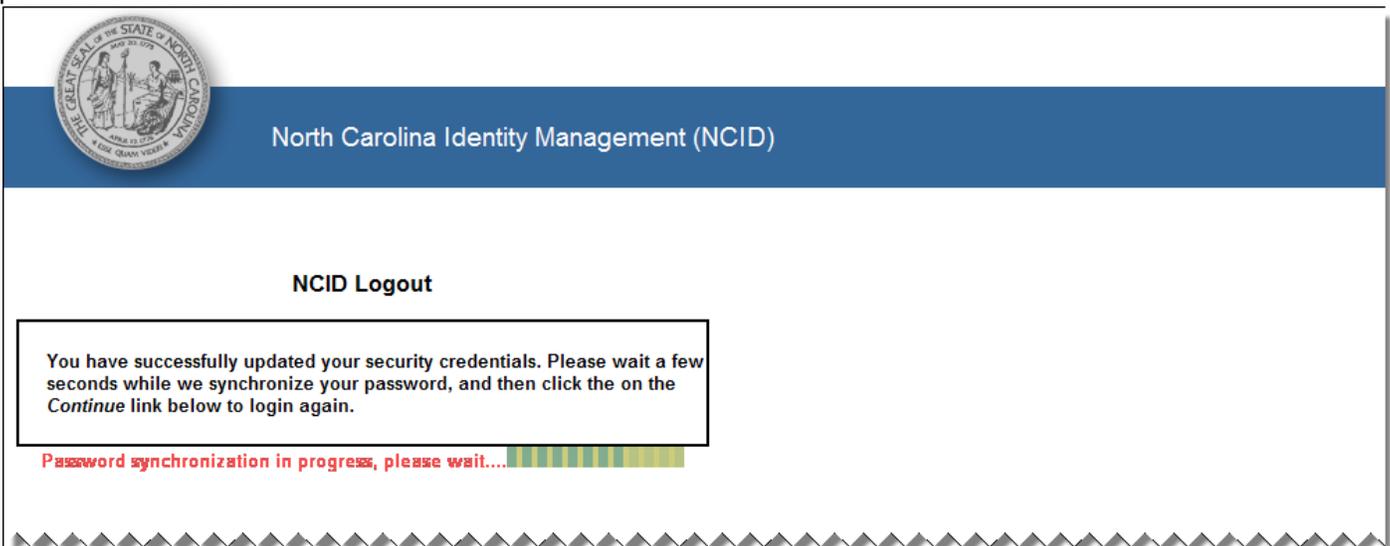
NCID Logout" Screen – Password Synchronization in Progress

6. The Continue link appears when the password synchronization is complete. Click on the link to log in to NCID again.

Note: You will also receive an email message to notify you that your password has been successfully changed.
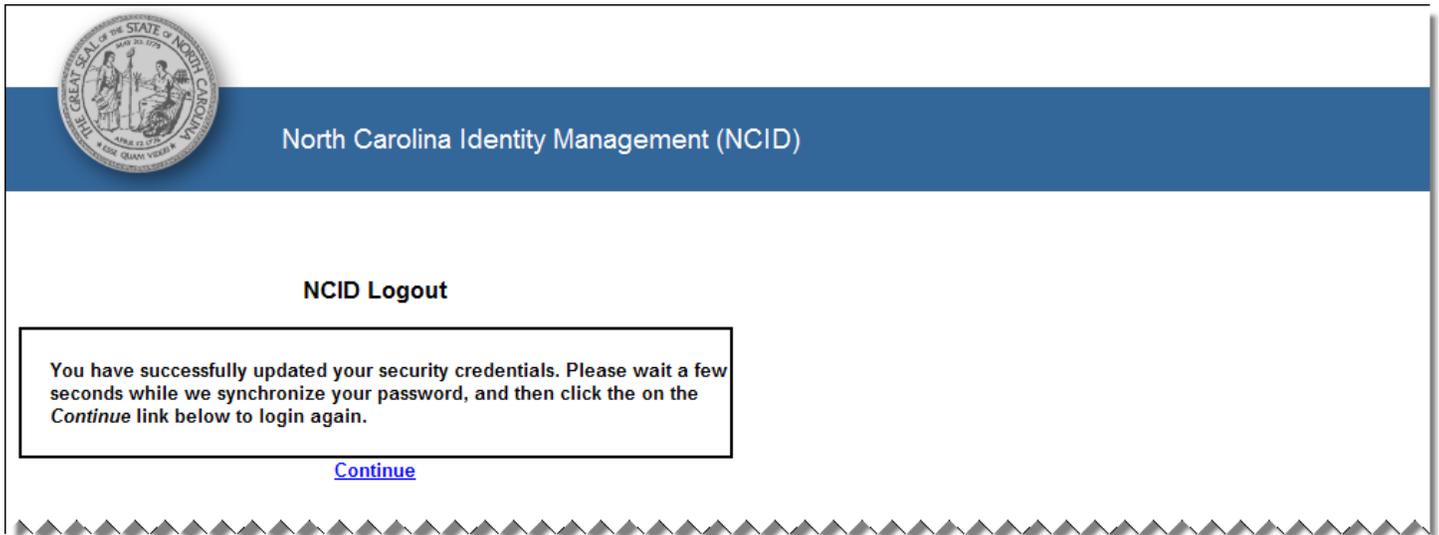
NCID Logout" Screen – Click "Continue" to Login

Using the "Forgot Your Password" option

You can reset your password if you have forgotten it by using the "Forgot Your Password" link is featured on the "NCID Login" screen. You will need to provide your user ID and answer three of your challenge questions so that the system can confirm you are an account holder.

Important: This feature will be unavailable to you if:
- Your account is locked. If you attempt to change the password, a message displays to advise you to reset it after one hour, or to contact your administrator or the Service Desk for immediate assistance.

- You have recently changed your password. State and local government employees must use their password for 15 days before it can be changed.

To use the "Forgot Your Password" feature:

1. Go to https://ncidp.nc.gov . On the "NCID Login" screen, type your user ID in the "User ID" field. This information must be entered before you can proceed to the next step. The system cannot reset your password without a valid user ID.

Enter "User ID" and Click "Forgot Your Password"

2. Click on the **Forgot Your Password** link.

3. The "Forgotten Password" screen is displayed. Your user ID should appear in the "User ID" field. If it is not displayed, type it in the field.

"Forgotten Password" Screen

4. Click on **Get Questions** to display the "**Forgotten Password – Challenge Questions"** screen.

5. Answer the three **(3)** challenge questions presented on the screen. The answers are not case-sensitive; however, the answer must include every character (including punctuation) that you specified when you set up your challenge questions. (They are randomly selected from the five (5) questions you selected.)
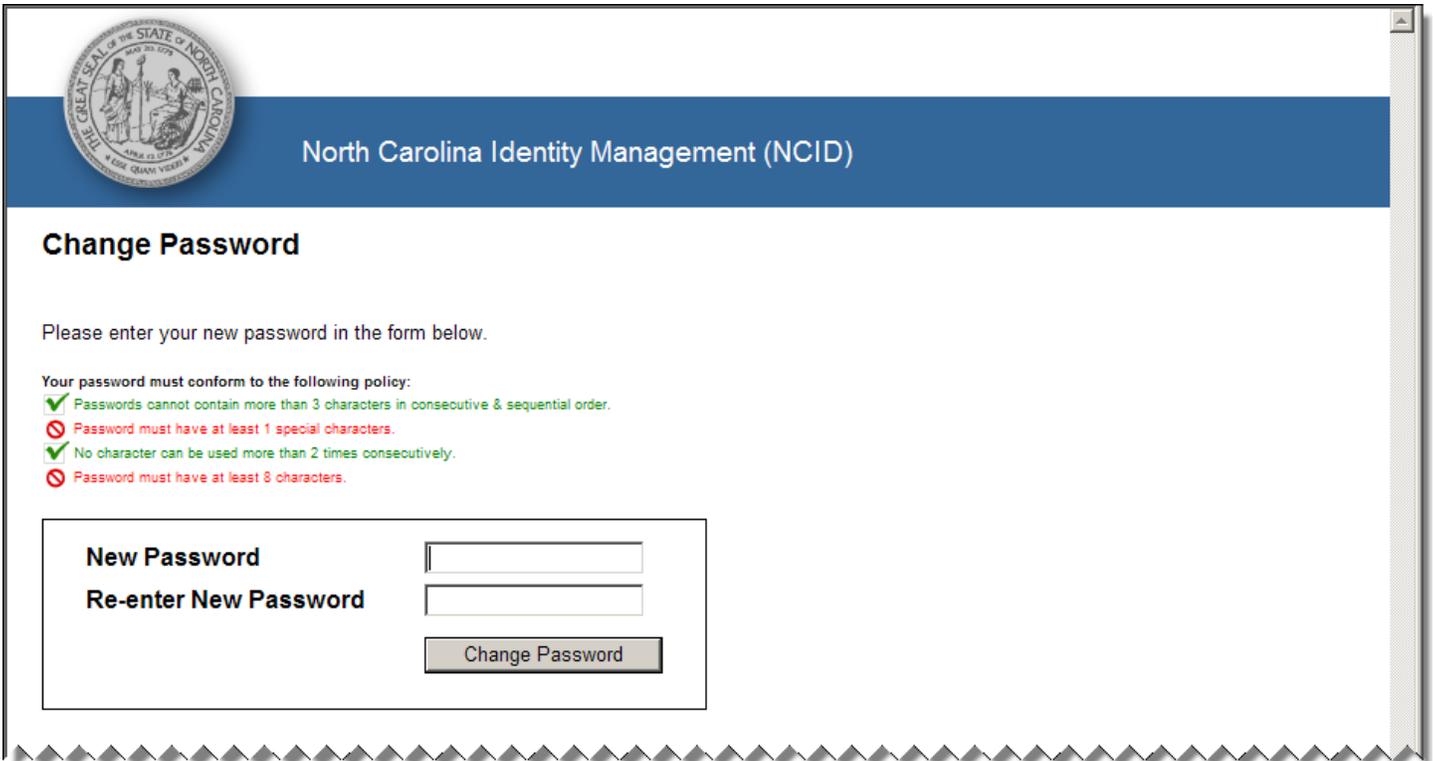

Answer Your Challenge Questions

6. Click on **Login**.

Note: A message will display if you failed to correctly answer any of your challenge questions. Your account will lock after three (3) failed attempts; however, you may try to log in again after one hour, or you may request that your account be unlocked sooner by your administrator or the Service Desk.

7. The "Change Password" screen is displayed, and prompts you to enter a password in the "New Password" field. The screen indicates whether the password complies with the State"s password policy. Notice that as you type the password, each requirement listed on the screen turns from red to green and the screen displays either ✔ or ⊘ to indicate whether the password has met each policy requirement.

Note: NCID passwords are case-sensitive, and must be entered exactly as they were originally entered.

Enter and Confirm New Password

8. Retype the password in the "Re-Enter New Password" field.

9. Click on **Change Password** to display the "NCID Logout" screen. The message indicates that you have successfully updated your security credentials and asks you to wait a few seconds while your password is synchronized across the applications that you are permitted to access.

"NCID Logout" Screen – Password Synchronization in Progress

10. The **Continue** link appears when the password synchronization is complete. Click on the link to log in to NCID again.
Note: You will also receive an email message to notify you that your password has been successfully changed.

"NCID Logout" Screen – Click "Continue" to Login

Important information for State and Local Government Users If you connect to NCID applications via a mobile device (e.g.: if you connect to Exchange to access email via a mobile phone or PDA) you must also change the password on each device. If the password is not changed, you will be unable to log in. Note that your NCID account will lock after 3 failed login attempts.

Frequently Asked Questions (FAQs)

1) What is the expiration date on passwords?

> *The password expiration policy is 90 days for state and local government employees.*

2) When a password is reset by a DA or the Service Desk, how many days does a user have to change the temporary password before it expires?

> *A user can change the temporary password from the time it was created up to 90 days. If a user does not log in, the account will deactivate after 90 days of non-use.*

3) Will users be permitted to log in to other applications (i.e.; BEACON, Exchange) using a temporary password?

> *No, the temporary password is a "one time use password"; therefore, users must first log in to NCID and reset their password before proceeding to other applications.*

4) Are there any 'special characters' that cannot be used in passwords?

> *Yes, the following characters may not be used: Forward Slash (/), Backward Slash (\), Double Quotation ("), Single Quotation ('), Reverse Quotation (`) and Plus (+). Additionally, a password cannot contain spaces.*

5) Will users be able to see the number of days remaining before they need to change their password, or will they able to see the date the password needs to be changed?

> *A user can see their password expiration date on their profile. The user's DA will be able to see when the password was last changed and when it's due to expire on the "Update Employee Account" screen.*

6) Although temporary passwords should follow password policies, does anything prevent DA's from using the same temporary password for every account?

> *No, the system allows the administrator to reuse the password each time he/she performs a password reset. From a security point of view, it is good practice to use different passwords each time a reset is performed.*

7) Is one-time password considered a security risk if the DA is consistently utilizing same password?

> *Yes, but needs to be addressed by agency policies.*

8) Have password strength rules been considered?

> *Yes, they are the same as what we currently have; however, there is one difference: passwords are case-sensitive, and they must be entered exactly as they were originally entered.*

9) Are passwords case-sensitive?

> *Yes, NCID enforces case sensitivity.*

10) Once a user resets the password, if they forget it, is there a time period when they can use the "Forgot Password" link again?

> *Yes, federal regulations require a 15 day period for a user to change their password; however, they can contact the AGR help desk to reset it before the minimum age requirement expires.*

11) Will passwords reset after 1 hour?

No, an account will be unlocked after one hour, and the user will need to log in to NCID.

12) How will color-blind users distinguish between red and green password rules?

The screen displays "Passed" and "Failed" next to each rule.

13) Will there be a way to verify if a user with an expired account was sent an email requesting them to change their password? A majority of users don't seem to get the 10-day warning message.

The password expiration warning email message is a convenience feature, not a guarantee. There is no way for NCID to check if emails are received and the email may go to spam or junk folders, etc. Most Model 2 and web service applications do not display warning messages about upcoming password expiration, but a warning message is displayed for users who log in to NCID directly or a Model 1 application. Note that password expiration dates are included in the report, so DA's could extract this information to implement their own warning process.

14) Can users change their password before it expires?

Yes, a user can change their password via the "Change Password" link displayed on the "Identity Self-Service" tab. Please be advised that the minimum password expiration policy requires state and local government employees to use their password for 15 days until it can be changed.

15) Regarding the NCID password policy, what is the difference between not containing 3 or more character sequences and not using a character 3 or more times consecutively?

The following are examples of 3 characters sequences: 123, abc, ABC. Therefore, password123 would not be permitted due to the '123' sequence. The following password is acceptable: password12.

*The following are examples of using a character 3 or more times consecutively: 111, aaa, AAA, ***. Therefore, password111, would not be permitted due to '1' being used more than three consecutive times. The following password is acceptable: password11.*

16) If a staff member is on medical leave for more than 15 days, will the user's password expire because the user has not logged into NCID?

The password expiration policy is 90 days so the user will be able to log into NCID if it's within 90 days.

17) Is it correct that a temporary password is no longer auto-generated upon resetting a password in NCID?

Yes, that is correct. The administrator will need to enter a temporary password.

18) Will NCID passwords and NCMail passwords sync for the same expiration date?

No.

19) Is the Password Synchronization feature available to all NCID users, or only to Delegated Administrators?

The Password Synchronization feature is available to all NCID users via the link on the "Identity Self-Service" tab.

20) How long does it take for an account to synchronize between NCID and Beacon?

Approximately 5 minutes.