Duo at NCSA



Short link to this page: https://go.ncsa.illinois.edu/2fa

NCSA offers the Duo multi-factor authentication solution as a method of protecting and securing NCSA's resources.

Duo for NCSA accounts is available to all NCSA Kerberos account holders.

Duo for NCSA accounts is separate from Duo for University of Illinois NetIDs. For help with Duo for University of Illinois NetIDs, please visit the NetID Center.

IMPORTANT: You must enroll with Duo using either a mobile app or a security key before attempting to log in. Keep reading below for details.

Table of Contents

- Prerequisites
- Enrollment Steps
- FAQ
  - How do I use a backup code to recover access?
  - How do I transfer my Duo setup to a new phone?
  - Can I use SMS as a Duo authentication method?
  - My passcodes aren't working even though I'm pretty sure they should. What can I do?
  - Duo account recovery process
  - Protecting your system or application with NCSA Duo
  - How does NCSA Duo relate to my campus Duo?
  - Where can I get additional help?

Prerequisites

Prior to beginning Duo enrollment for your NCSA account, take care of the following prerequisites.

1. Know your NCSA Kerberos username and password.
   - If you need to reset your password, use the NCSA Identity service at https://identity.ncsa.illinois.edu/
2. Install the Duo mobile app on your iOS/Android device or obtain a security key.
   - To install on iOS, find Duo Mobile in the App Store.
     - For more information about Duo on iOS, see: https://guide.duo.com/iphone
   - To install on Android, find Duo Mobile in Google Play.
     - For more information about Duo on Android, see: https://guide.duo.com/android
   - To purchase a security key, visit: https://www.yubico.com/product/security-key-by-yubico
     - **Note Security keys are not compatible with non-web based authentication at this time**.
     - For more information about Duo's support for security keys, see https://guide.duo.com/security-keys
     - Tokens are useful for recovering your NCSA Duo account and logging into the NCSA IDP service.
     - If you require a hardware token for any other use or project at NCSA please contact the project to be assigned a token
       - NCSA employees: contact help+duo@ncsa.illinois.edu.
       - Industry Partners: contact your Industry program representative.

Enrollment Steps

With the above prerequisites satisfied, follow these steps to enroll using your iOS/Android device or security key.

1. Visit https://duo.security.ncsa.illinois.edu in your web browser.
   - If using a security key, be sure to use one of the web browsers that support U2F (e.g., Chrome).
2. Log in with your NCSA Kerberos username and password.
   - If you have trouble logging in with your username and password, visit https://identity.ncsa.illinois.edu/ or contact help+its@ncsa.illinois.edu.
3. Select **Launch Device Management Portal**.
4. Follow the Duo process for enrollment. See https://guide.duo.com/enrollment for details.
5. Generate and save 2 non-expiring one-time-use backup codes.
   - Visit https://duo.security.ncsa.illinois.edu/ and select **Manage Backup Codes and Tokens**. Then select **Generate replacement backup codes**.
   - Write down the codes and place them in a safe location or store them in your password vault.
   - Whenever you use one of the backup codes, it is a good idea to generate 2 new backup codes, so you always have 2 backup codes available to use.
6. (Optional) Add additional devices (phones, tablets, security keys).
   - Visit https://duo.security.ncsa.illinois.edu/portal, select **+Add another device,** and follow the instructions.

FAQ

How do I use a backup code to recover access?

To use a backup code to add a new device/token:

- First complete the Prerequisites listed above to prepare your new device/token.
- Next, visit https://duo.security.ncsa.illinois.edu.
- Select **Launch Device Management Portal**.
- Click the "Enter a Passcode" button
- Enter your backup code and then click "Login"
- Click the "Add another device" link and follow the instructions.
- Lastly, return to https://duo.security.ncsa.illinois.edu/ and select **Manage Backup Codes and Tokens**. Then select **Generate replacement backup codes** to generate 2 new backup codes (and save them in a safe location like before).

How do I transfer my Duo setup to a new phone?

- **Prerequisite**: Have access to your two NCSA Duo backup codes.
    - If you do not have these please generate new ones.
    - Visit https://duo.security.ncsa.illinois.edu/ and select **Manage Backup Codes and Tokens**. Then select **Generate replacement backup codes**.

- First, install the Duo mobile app on your iOS/Android device.
    - To install on iOS, see: https://guide.duo.com/iphone
    - To install on Android, see: https://guide.duo.com/android
- You may be able to use Instant Restore
    - iPhone: https://duo.com/blog/new-phone-who-dis-how-to-instantly-restore-2fa-settings
    - If this does not work proceed to next step.
- Next, visit https://duo.security.ncsa.illinois.edu.
- Select **Launch Device Management Portal**.
- Log in with one of the following options:
    - If you still have your old phone, use the "Send me a Push" or "Enter a Passcode" option with your old phone.
    - If you have a security key, use that to log in.
    - If you have a backup code, use that to log in.
- Set up your new phone using one of the following options:
    - Select "Device Options" to "Reactivate Duo Mobile" on your new phone.
    - Delete your old phone from the list, then select "Add another device" to add your new phone.

Can I use SMS as a Duo authentication method?

No, NCSA has disabled the SMS authentication method for our Duo deployment due to the security weaknesses of that method. See NIST is No Longer Recommending Two-Factor Authentication Using SMS for references on this topic.

My passcodes aren't working even though I'm pretty sure they should. What can I do?

- Attempt to authenticate with three correct passcodes in five minutes. This process will resynchronize your Duo app or hardware token with your Duo-protected account.

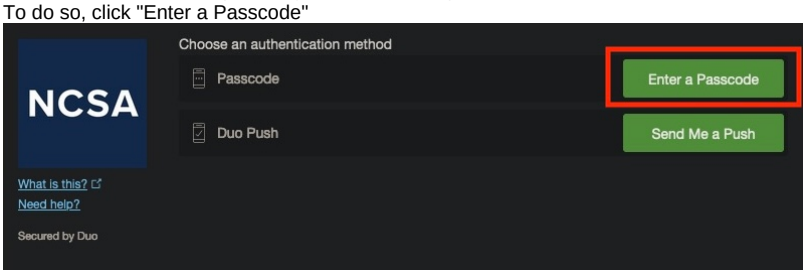
If your passcodes have gotten out of sync with the Duo service, Duo supports the standard resynchronization algorithm which allows a user to provide multiple valid one time passcodes (OTPs) to get the remote server's counter back in sync with the local device. This is a secure method of resynchronization and does not pose a security risk because the OTP seed is not changed. Resynchronization may be needed because server's counter value is only incremented after a successful authentication where as the counter on the device is incremented with every request by the user. Because of this, the counter values on the server and on the token might be out of synchronization.

Duo account recovery process

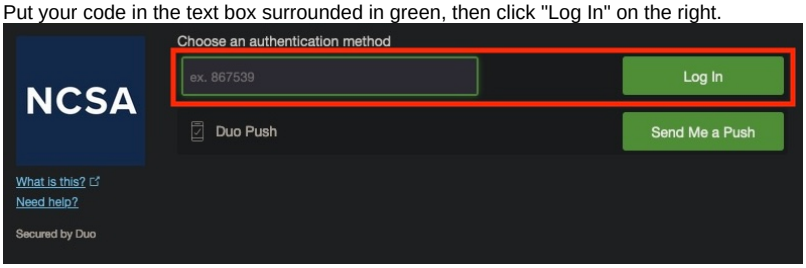
If you no longer have access to your phone/security key or backup codes for your NCSA Duo account you may be able to use the NCSA Duo recovery process.

1. Go to https://identity.ncsa.illinois.edu/manage . If you are not already logged in, you will be prompted to log in with your username and password. Scroll to the bottom of the page and look for the "Other Actions" section. Once there, click the "**Initiate Duo Account Recovery**" button.
2. On the "Request new Duo recovery codes" page, select a manager or group owner for your project. Select a contact who you think may be available to assist you, then click the "Begin recovery" button. If you do not recognize any of the contacts listed, open a Help+Duo ticket stating you do not recognize any PIs and require help.
3. An email will be sent to the contact you selected, and you should receive an email acknowledging the request to recover your Duo account. You must now wait for the manager or group owner to respond to your request.
4. The manager or group owner will arrange to contact you via a synchronous communication channel such as in-person, telephone or video chat in order to verify your identity and give you a one-time code for Duo authentication.
5. Go to https://duo.security.ncsa.illinois.edu/portal
    a. Log in with your NCSA username and password

b. enter the one-time code that was given to you in order to log in to Duo.
    i. To do so, click "Enter a Passcode"



    ii. Put your code in the text box surrounded in green, then click "Log In" on the right.



6. Select "Add another device" to add your new phone / security key for Duo authentication.
7. Go to https://duo.security.ncsa.illinois.edu/
    a. select "Manage Backup Codes and Tokens", then select "Generate replacement backup codes" to generate two backup codes in case you lose your phone / security key again.

Protecting your system or application with NCSA Duo

If you are the manager of an NCSA system or application and would like to use NCSA Duo to add multi-factor protection to your system please contact us at help+duo@ncsa.illinois.edu with your request.

How does NCSA Duo relate to my campus Duo?

NCSA Duo is separate from Duo at the University of Illinois or other universities or organizations. If you use Duo with multiple organizations, you'll need to enroll separately in each organization's Duo, then each organization will be listed separately in your Duo mobile app. If you need to recover your Duo account(s), the recovery steps will differ for each of your Duo accounts. The instructions on this page apply only to Duo at NCSA used with NCSA systems.

For information about Duo at the University of Illinois, please visit https://identity.uillinois.edu/.

For information about Duo for ACCESS, please visit https://identity.access-ci.org/manage-mfa.html

Where can I get additional help?

Send your questions, comments, suggestions, etc. to help+duo@ncsa.illinois.edu.

Corrections and suggestions for improvement to the above documentation are very welcome!