Duo at NCSA

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

Duo at NCSA accounts are available to all NCSA Kerberos account holders.

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.

[ Prerequisites ] [ Enrollment Steps ] [ FAQ ]

Prerequisites

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

1. Know your NCSA Kerberos username and password.
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
   • For more information about Duo's support for security keys, see https://guide.duo.com/security-keys
   • In some cases, NCSA can provide a Duo hardware token for you.
     • NCSA employees: contact help+duo@ncsa.illinois.edu.
     • Industry Partners: contact your Industry program representative.
     • LSST Staff: contact your project manager.
     • Blue Waters users: Contact the BW Project Office - help+bw@ncsa.illinois.edu
     • Others: please purchase a security key (e.g., https://www.yubico.com/product/security-key-by-yubico).

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.
2. Log in with your NCSA Kerberos username and password.
   • If you need to reset your password, use the NCSA Identity service at https://identity.ncsa.illinois.edu/
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:

1. First complete the Prerequisites listed above to prepare your new device/token.
2. Next, visit https://duo.security.ncsa.illinois.edu.
4. Click the "Enter a Passcode" button.
5. Enter your backup code and then click "Login".
6. 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?

- 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
- 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.

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!