What is Multi-Factor Authentication and why is it important?

First we should define "authentication". Authentication is simply the act of verifying an identity is who they say they are. Commonly this is done using a password to authenticate a username, which theoretically only the owner of the username would know. However this is a low level of assurance, meaning it is possible that another identity could also know that password and impersonate that user. Either the password was weak and simply guessed, brute force attacked, stolen via a keylogger or phishing email, or via a compromise of another system where the password was reused. Whatever the reason, passwords are constantly being compromised which leaves the systems they protect vulnerable to compromise.

The example above is an example of "single-factor" authentication. A "factor" is a type of authentication method, commonly either a knowledge factor (something the user knows), a possession factor (something the user has), or an inherence factor (something the user is, biometrics or location based usually). Using "multi-factor" authentication, requiring two or more of the previously mentioned factors to be verified successfully, offers a much higher level of assurance. When using multi-factor authentication an attacker must both steal a password and also something the user physically has in their possession or impersonate who they physically are, much less likely to occur. It also increases the accountability of the user and helps in auditing as the likelihood that someone was spoofing another account is almost nil.

At UCI the goal is to offer multi-factor authentication to all users and systems, primarily focused first on protecting the most high risk assets from authentication related compromise, because simple password authentication just isn't secure enough anymore. UCI is using Duo Security as its multi-factor authentication solution. With Duo Security, you combine something you know (password) with something you have (mobile device or hardware token) to verify you truly are who you say you are.

Obtaining a Duo Security Token

Enrollment is open to all Employee and Guest type UCInet affiliations. You will need to choose between using a Software Token or Hardware Token. The Software Token is a free app that you install on your phone/tablet, the preferred method if you have a supported mobile device (Android, iOS). The hardware token is a small physical
device to carry with you on a keychain, contact your local computer support to purchase hardware tokens through OIT. Some pro’s and con’s of each below:

<table>
<thead>
<tr>
<th>Pros</th>
<th>Hardware Token</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Free</td>
<td>• Doesn't need a compatible mobile device</td>
</tr>
<tr>
<td>• Supports Duo Passcode (no WiFi or data connection needed)</td>
<td>• Supports Duo Passcode (no WiFi or data connection needed)</td>
</tr>
<tr>
<td>• Supports Duo Push (requires a WiFi or cellular data connection but doesn't use much data)</td>
<td></td>
</tr>
<tr>
<td>• Duo Push doesn’t require you to type a Passcode, but instead just tap to approve a request</td>
<td></td>
</tr>
<tr>
<td>• Duo Push can be used more often than once per 60 seconds</td>
<td></td>
</tr>
<tr>
<td>• Less likely to get damaged or lost</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Cons</td>
<td></td>
</tr>
<tr>
<td>• Requires compatible mobile device (app requires minimal permissions and space)</td>
<td>• Not Free</td>
</tr>
<tr>
<td>• Doesn't support Duo Push</td>
<td>• Doesn't support Duo Push</td>
</tr>
<tr>
<td>• More likely to get damaged or lost</td>
<td>• More likely to get damaged or lost</td>
</tr>
<tr>
<td>• Sometimes needs to be resynced with the server (need to contact HelpDesk)</td>
<td>• Sometimes needs to be resynced with the server (need to contact HelpDesk)</td>
</tr>
<tr>
<td>• Duo Passcode can only be used once per 60 seconds</td>
<td>• Duo Passcode can only be used once per 60 seconds</td>
</tr>
<tr>
<td>• Needs to be replaced every couple of years as the internal battery runs out</td>
<td>• Needs to be replaced every couple of years as the internal battery runs out</td>
</tr>
</tbody>
</table>

Initial Token Setup Instructions

Software Token Setup

1. With your compatible mobile device in hand, on a computer go to https://applications.oit.uci.edu/DuoSupportDesk/enrollment.htm
2. Under Add Software Token click on "Software Token Registration"
   a. [Image]
3. After reading the policy agreement, follow the steps to enter information, download the compatible app, and finally register your phone or tablet with your account.
   a. [Image]
4. You can then test it by going to the Duo-protected test webpage below.

**Duo Hardware Token Setup**

1. You’ll need to contact your local computer support to obtain a hardware token that they can purchase through OIT via **Duo Hardware Token Order Form**. If you work in OIT, have your supervisor contact the security team to get one.

2. With your hardware token in hand, on a computer go to **https://applications.oit.uci.edu/DuoSupportDesk/enrollment.htm**

3. Under “Add Hardware Token” click on “Duo Hardware Token Registration”.
   
   a.

4. After reading the policy agreement, enter the serial number found on the hardware token and click “Register”.
   
   a.
5. You can then test it by going to the Duo-protected test webpage below.
6. **Note**: The hardware token has a button on it that displays the token code when it is pressed. If the button is pressed too many times without the token code being used to log in, the token will get out of sync and you won’t be able to log in until it is resynced. Having the token in your pocket or backpack with keys or other objects that could press on the button will cause this to happen. Contact the [OIT Help Desk](mailto:oithelpdesk@uci.edu) to get the token resynced.

**YubiKey Hardware Token Setup**

1. With your hardware token in hand, on a computer go to https://applications.oit.uci.edu/DuoSupportDesk/enrollment.htm
2. Under "Add YubiKey Hardware Token" click on "YubiKey Hardware Token Registration".
   a. 

3. After reading the policy agreement, enter the YubiKey’s serial number, private identity, and secret key and click "Register".
   a. 
4. You can then test it by going to the Duo-protected test webpage below.

Testing Your Token

1. The following Duo-protected webpage can be used to verify your token is working: https://applications.oit.uci.edu/DuoSupportDesk/testToken.htm. You can also visit the DuoSupportDesk home page and click "Test Token" found on the navigation bar.
   a.
   b.
Removing Your Token

1. To remove your software or hardware token, go to https://applications.oit.uci.edu/DuoSupportDesk/enrollment.htm
2. Under "Remove Token" click on "Remove Registration".
   a.
3. Authenticate
   a.
4. Click "My Settings & Devices" first and enter a passcode/push to verify authentication
   a.
5. Click "Device Options" for the device you want to remove
   a.  

6. Click the trash can icon and then click "Remove" (you can't remove a device if it is your only one)
   a.  
   b.  
7. Your token is now successfully removed. It can be re-registered to any account.
   a. 

   Emergency Backup Codes

   1. To generate emergency backup codes, go to https://applications.oit.uci.edu/DuoSupportDesk/enrollment.htm
   2. Under “Emergency Backup Codes” click on “Generate Emergency Backup Codes”.
      a. 

   3. After reading the disclaimers, click “Generate”.
      a. 
4. Securely store your backup codes for use when your software or hardware tokens are unavailable.
   a. New Phone / Software Token Replacement

If you still have the old device with an activated software token, you can go to https://applications.oit.uci.edu/DuoSupportDesk/enrollment.htm and click on the manage software tokens link to enroll the new device and delete the old one. Otherwise contact the OIT Help Desk and ask them to delete the old device, then you can go to the enrollment page and register the new device by following the “Software Token Setup” steps above.

General Usage Information

- **Duo Guide to Two-Factor Authentication**
- Keep your Duo Security token in a safe place, either with you at all times or somewhere you won't forget it, when you need access to systems from work or home
- Duo Security requires two factors being authenticated before you are allowed to progress:
  - First Factor = the normal native password you have been using to access the system
  - Second Factor = the Duo Security Passcode or Duo Push Response
    - Example Duo Passcode using hardware token:
• Example Duo Passcode using Android mobile app:

• Example Duo Push using Android mobile app:

• A Passcode on a Duo Security token changes every 60 seconds.
• A Passcode can only be used once, you must wait until the passcode changes before attempting to use the Duo Security token for authentication again.
• Duo Push requests can be initiated and approved sequentially multiple times regardless of time.
• Accounts get locked out after 5 failed login attempts by policy.
• If you need your account reactivated after a lockout, or you’ve lost or forgotten your Duo Security Hardware or Software token, or have any problems related to Duo Security Authentication, please contact the OIT Help Desk.
• Duo Security tokens do not communicate to a central server and do not need internet connectivity for standard use. However, if you wish to use the Duo Push feature of the software device token, that does require a data connection on the mobile device.
• Here is **generic information** (.pdf) about Two-Factor Authentication via SANS (calling the process two-step verification)

Common Usage Step-by-step

WebAuth

1. When you get redirected to WebAuth from a web application that is enforcing multi-factor authentication, you will first see a WebAuth login page. Login with your UCInetID and Password.
2. After successful login using first factor, you will be presented with the second factor login. You will have an option to choose your type of phone device and either Duo Push or to enter in a Passcode. The example that is shown uses "Android" as a device. If you choose to select Duo Push, then press the "Log in" button. Otherwise you can select "Passcode" and enter the passcode that is currently being displayed on your hardware token or mobile app, then press the "Log in" button.

3. Once you enter the correct passcode, or approve the push request, the WebAuth page will redirect you back to the application you came from successfully authenticated.

Enabling Auto-Push for Web Logins

1. Go to https://applications.oit.uci.edu/DuoSupportDesk/enrollmentDuo.htm
2. Click on the "My Settings & Devices" link
3. Use Duo authentication to confirm your device
4. Change the "When I log in" selection for your device to automatically send a Duo push (or the opposite to disable)
5. Click Save

Toggling Remember Me feature when Auto-Push is enabled for Web Logins

1. Click the "Cancel" button on the web page screen where it says "Pushed a login request to your device..."
2. The "Remember me" checkbox should now be editable
   a. Note: Using this feature requires your browser to accept 3rd party cookies
3. Change option as desired and click Push, after which it will Auto-Push again with new setting
Windows RDP/Console

Note: This is a preview of what it may look like, contact your system administrator about the current status of your systems.

1. Remote Desktop or get Console access to the Windows system you want to log into. You will first be presented with the familiar Windows login dialog box. Here enter your Windows username and password (domain or local account, depending).

2. After successful login using first factor, you will be presented with the second factor login. You can enter the passcode that is currently being displayed on your hardware token or mobile app, or if you have Duo Push enabled you can type "push" and the request will be sent to your mobile device to approve.

3. Once you enter the correct passcode, or approve the push request, you will have successfully authenticated into the Windows system.

Unix/Linux SSH

Note: This is a preview of what it may look like, contact your system administrator about the current status of your systems.
1. Open up an SSH terminal session to the Unix system you want to log into. You will first be presented with the familiar Unix login prompt. Here enter your Unix username and password (how first factor Unix authentication is setup varies between environments, ask your system administrator for specifics).

2. After successful login using first factor, you will be presented with the second factor login. You can enter the passcode that is currently being displayed on your hardware token or mobile app, or if you have Duo Push enabled you can type “1” and the request will be sent to your mobile device to approve.

3. Once you enter the correct passcode, or approve the push request, you will have successfully authenticated into the Unix system.

Departmental VPN

1. Start the AnyConnect client, type in the address of the multi-factor enabled VPN server you want to connect to, and click Connect.
1. On the next screen, choose the tunnel group from the Group dropdown that you need to connect to. Enter your username and both first and second factor authentication in the same window. The first factor is your UCInet password. The second factor is your Duo Passcode (or you can type "push" if you have a Duo software token).

2. Once you enter the correct credentials, or approve the push request, you will have successfully authenticated into the VPN.

User Opt-In Available Services

WebAuth

http://www.oit.uci.edu/help/duo/webauth-duo/

Office 365

http://www.oit.uci.edu/help/duo/office-365-duo/

Login failures and Lockouts

Your Duo token/account will be disabled ("locked-out") automatically when you have five (5) consecutive authentication failures in a row. It does not matter how far apart the failures are. However, if you have a successful authentication before you hit five failures, the count resets back to zero. There are other reasons why you may be unable to login -- See the next section about troubleshooting login failures. If you are sure that you have caused your token/account to become disabled, contact the OIT Help Desk at 42222 for assistance.

Troubleshooting login failures

- If you are using "push" and your phone turns off WiFi when it is locked, unlock your phone and let it connect
to the WiFi network before you try to log in. The Duo app may get the push request from the cell network, the phone connects to the wireless network and tries to reply over the wireless network, and your login may time out.

- If you are using "push" and are in an area where there is "free" WiFi (hotel, airport, etc) where you have to click thru an agreement to use the network, either do that to get fully connected or turn off WiFi before you try to log in. Most phones prefer WiFi over the cell network for data, and if you are not completely connected to the internet because you haven't clicked thru the agreement, the Duo app won't be able to talk to the Duo infrastructure to authenticate you.
- If you are in an area with poor or no cell and WiFi coverage, use a token code instead of typing "push". Start the Duo app and click on the key to get the token code. If the service you are connecting to uses "autopush" this won't work for you, and you won't be able to log in until you can get on a cell or WiFi network. If the service uses autopush and you will need to use a token code to get to it because you don't have good cell/WiFi coverage, talk to the administrator of that service to see if it autopush can be turned off.

Using the Duo Software Token App for Other Two-Factor Authentication Third-Party Accounts

The Duo Software Token App supports working with any two-factor authentication solution that uses the TOTP protocol (popularized by Google Authenticator). Cut down on the number of apps you have to install and manage all of your other compatible third-party accounts within the Duo mobile app.

Popular TOTP compatible two-factor authentication third-party accounts include (based on https://twofactorauth.org/ )

- Google Drive / Gmail
- Amazon Web Services (AWS) Console
- LastPass
- Github
- Dropbox
- Slack

See https://www.turnon2fa.com/ for specific setup instructions.

***Please be sure to follow the recommended backup directions for your third-party accounts, e.g., a phone number or backup code.***