Multi-Factor authentication Instructions

Overview

Multi-factor authentication (MFA) is a process of verifying identity of a user based on multiple methods. Methods can be 1) something you know like a password, passphrase or code, 2) something you have like a swipe card or token and 3) something you are such as biometrics (i.e. fingerprint, retina scan). MFA requires that you use one type of authentication from at least two of these three groups as in the following examples:

1) Swipe your ID badge (something you have) and then punch in a code (something you know)
2) Swipe your ID badge (something you have) and then do a fingerprint scan (something you are)
3) Type in your password (something you know) and use a code generated by a token (something you have)

Vendor Selection

The University of Utah UIT group has selected to use DUO Security as its MFA Solution Provider. The DUO Security solution is a cloud-based, hosted solution that means the entire service is installed/running on servers maintained by DUO Security.

The client-end solution has four (4) methods for authentication with the DUO servers:

1) Generate token through an application installed on your phone. Essentially your phone is a “soft token”, meaning your phone generates a login code that is in sync with the DUO cloud server. This generated code is specific to your account and is only valid for 10 seconds before the code is invalid. This requires that you have a smartphone and install the client application. This has been tested and verified with IOS, Android and Windows 8 devices. Because this is generating a code based on a local algorithm on the phone device, no phone connectivity is required. This is a great option for places that have spotty cell phone service.

2) Have the DUO server “push” a confirmation to your phone and you can accept or deny the login request. If you accept the request on your phone, the DUO server sends that acceptance directly to the server and your authentication request is completed (no typing in a code.) This requires that you have a smartphone with the application installed and also cellular reception for your device. This is the most convenient option.
3) Have the DUO server text you a code via SMS. This code will only be good for one login, and also will expire after one minute. This method requires that a person have a cell phone (does not have to be a smartphone and there is no application to install), but the phone must have good enough service to receive the SMS text. This does have an additional cost of $0.01 (one cent) per text. The first two options have no additional cost to the University. The phone will not be charged, those charges come through the account with DUO.

4) Have the DUO server call you on your phone. When it calls you on the phone, you will hear a message stating that you are receiving an authentication request from DUO and to hit any key to accept the request. Once you press any key, the DUO server sends that authorization to the jump box and the authentication request is complete. If you hang up without hitting another button, the request is denied. This does not require a smartphone or application, but does require phone reception and has an additional cost of $0.02 (two cents) per phone authentication.

**Getting Started: Account Creation**

Persons who need DUO accounts must have their departmental manager or delegated admin request an account to be created. Since the account is tied to the user’s cell phone make sure to provide the name, UNID, department and cell phone number of the person the account is being created for with the ticket. Once that account is created, the user will receive an SMS message with their activation information.

**Future Process**

A self-enrollment module will be provided where users can go to a web site and enroll into the University of Utah’s DUO instance.
Installing DUO Application

1) From your appropriate app store, search for DUO Security or DUO Mobile. Here are screen shots from the various storefronts:
2) Install the application.
3) Activate the application by pasting in the message you received via text. When the application comes up there will be an option to read a barcode. Choose “Have an activation code?” and paste in the message.
4) Confirm the activation. You are all done.

**Reporting Issues**

Requests for WIAN AD accounts/objects should go through the help desk. Make sure that you identify the account requests as PCI requests to ensure the work is completed in the appropriate domain.

DUO account requests should also go through the help desk process. Make sure you identify the request as a DUO account request to make sure we are creating the objects in the correct place.