
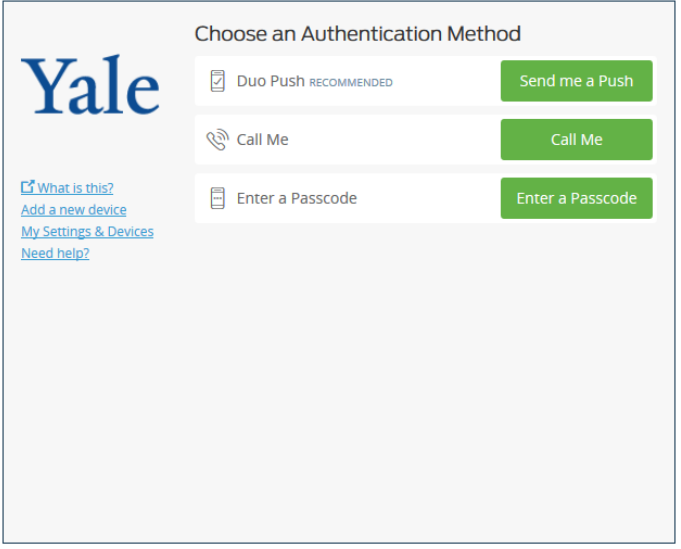
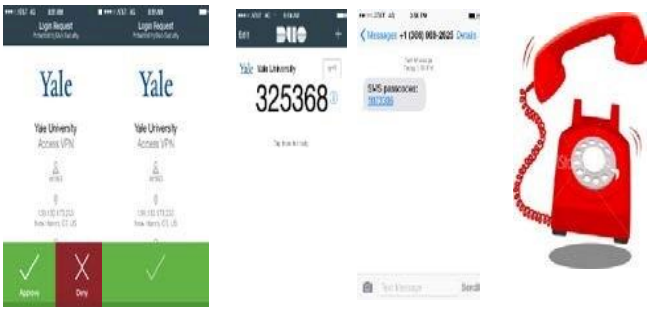



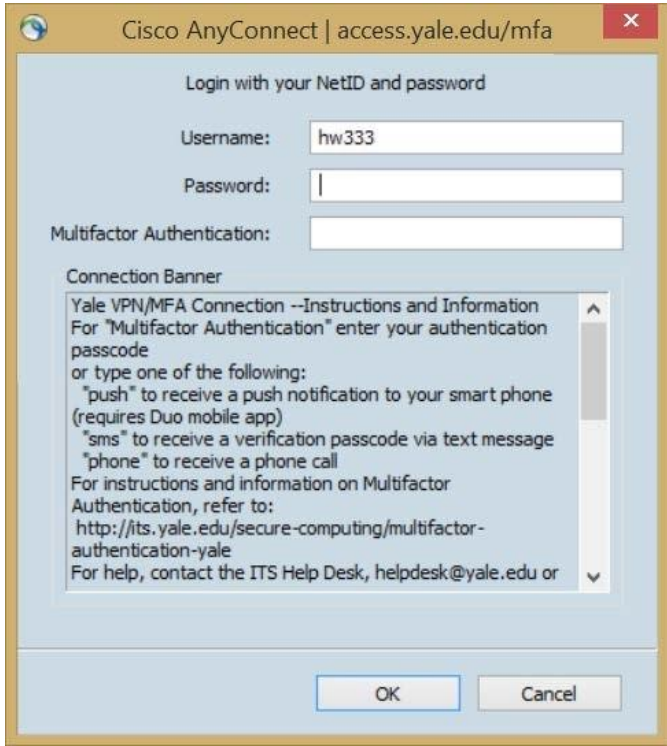

Instructions for logging into CAS and VPN (via a web browser) using Multifactor Authentication (MFA).

MFA is currently required when using CAS or YaleConnect from *off campus and VPN

Step	Action/Result	
1	<p>Follow the instructions below for your specific situation.</p> <ul style="list-style-type: none"> • CAS: Log in as usual with your netID and password. This will launch the Duo Multifactor Authentication Screen. • VPN from the browser: Type <code>access.yale.edu</code> into your web browser. This will launch the log in screen. Log in with your netID and password. This will launch the Duo Multifactor Authentication Screen. 	
2	<p>Log in with your second factor by telling Duo how you want to authenticate. You can</p> <ul style="list-style-type: none"> • Push a login request to your phone if you have the Duo Mobile app. <i>This is the recommended and simplest way to authenticate.</i> • Log in by typing a Passcode received via SMS, a hardware token, or your administrator. You can also generate a new passcode sent via SMS from this screen. • Generate a phone call to a landline or mobile phone. 	
3	<p>Depending on what you choose in Step 2 you will be prompted to authenticate via a second authentication result.</p> <ul style="list-style-type: none"> • If you chose “push” simply tap “Approve” on your mobile device you will be logged in to your desired application. • If you chose to type a passcode you will be logged in to your desired application. • If you chose “Phone call” follow the prompts when you are called and you will be logged in to your desired application. 	 <p style="text-align: center;">DUO Push Passcode SMS Phone</p>

Yale Information Technology Services

Notes	<ul style="list-style-type: none"> • For CAS and YaleConnect you may choose to remember your device for 1 day. This is browser specific, cookie based functionality. You will need to remember the device in all browsers where you use your second factor, and if you delete your cookies you will be prompted to use your second factor the next time you log in • If you have authenticated via VPN you will not have to authenticate a second time for CAS.
-------	--

Logging into VPN from the Cisco Client with Multifactor Authentication (MFA)		
Step	Action/Result	
1	Launch the Cisco Client and click connect .	
2	<p>Log in with your netID and password. In the remaining field Type “push”, “SMS”, or “phone” to tell Duo how you want to authenticate or enter a passcode.</p> <ul style="list-style-type: none"> • Push a login request to your phone if you have the Duo Mobile app. <i>This is the recommended and simplest way to authenticate.</i> • Log in by typing a Passcode received via SMS, a hardware token, or your administrator. You can also generate a new passcode sent via SMS from this screen. • Generate a phone call to a landline or mobile phone. This will generate a phone call to the FIRST number on your list of devices. To call the second or third number on your registered devices list type Phone2, Phone3, etc. 	
3	<p>Depending on what you choose in Step 2 you will be prompted to authenticate via a second authentication result.</p> <ul style="list-style-type: none"> • If you chose “push” simply tap “Approve” on your mobile device you will be logged in to VPN. • If you chose to type “SMS” you will receive a text message with your passcode enter you passcode and you will be logged in to VPN. • If you chose “Phone call” follow the prompts when you are called and you will be logged in to VPN. 	<p>DUO Push Passcode SMS Phone</p> 
Note	If you have authenticated via VPN you will not have to authenticate a second time for CAS .	

- Off Campus is defined as anything other than Yale Secure Wireless, Yale Wireless, or Yale hard wired network. Note: There are a few physically / geographically remote offices (medical) which are connected via Aruba Networks however they are considered on Campus and they will see no change. “Yale Guest” is an Off Campus network.