How do I register my YubiKey for use with Duo 2FA?

Q: How do I register my YubiKey for use with Duo 2FA?

- · How can I register my hardware token for use with Duo?
- Can I use a hardware token with Duo 2FA?

Context

You can use a Yubikey USB hardware token to generate a One Time Passcode (OTP) for use with Duo. This is useful if you don't have a smartphone, prefer a physical token for your second factor, or as a secondary backup option in case you don't have access to your phone.

If you would like to request a Yubikey, please submit the Yubikey Request Form.

Registering a Yubikey with Duo Security requires two steps:

- · Configuring the Yubikey hardware token
- Registering it with Duo Two-Factor authentication

Configuring the Yubikey hardware token

The following steps will erase and reconfigure your Yubikey. If you received a new Yubikey from IS&T, it is safe to follow the steps. If you already had your own Yubikey and were using it for non-MIT services, be aware that erasing and reconfiguring your Yubikey will probably make it stop working for your other services. For safety we recommend getting a new Yubikey from IS&T.

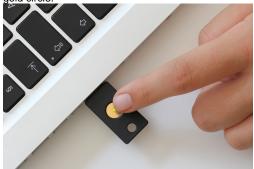
It should be possible to use a single Yubikey for multiple services if you:

- · Remove the Yubikey from all services that use it.
- Reconfigure it following the instructions below.
- Upload the configuration information to Yubico at https://upload.yubico.com/
- Upload the configuration information to MIT's Duo portal: Registering it with Duo Two-Factor authentication
- Re-attach the Yubikey to your other non-MIT services.

IS&T does not support the above steps, and will not be able to help if things don't work. Using a single Yubikey with multiple services (MIT/Duo and non-MIT/Yubico) weakens the security of the key. IS&T recommends getting a dedicated Yubikey for MIT/Duo logins.

To configure your Yubikey with One Time Passcode:

- 1. Download and install the Yubikey Personalization Tool from the Yubico website.
- 2. Once installed, insert your Yubikey into the USB port. Verify it is plugged in correctly by the solid/blinking green light in the middle of the gold circle.



Mac OS X users might encounter a prompt to set up a new keyboard the first time a Yubikey is connected. If you encounter this prompt, close the window and continue with the setup.

3. Open the Yubikey Personalization Tool. Under Personalize your Yubikey in select Yubico OTP Mode.

Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings	Tools	About	Exit
			nife for the YubiK				YubiKey is insert
	ize your YubiKey ubico OTP Mode DATH-HOTP Mode tatic Password Mor hallenge-Response ipdate Settings nd discussion, head t	de • Mode		-			Programming statu Not configured Firmware Version: 2.5.1 Serial Number Dec: 3262790 Hex: 31c946 Modhex: ebrkfh Features Support Yubico OTP
http://yu	<u>bi.co/forum</u>		Application Vers				2 Configurations OATH-HOTP Static Password Scan Code Mode
Copyright	© 2011-2015 Yubico). All Rights Reserved.	Library Version:	1.17.1			Challenge-Response Updatable Ndef Universal 2nd Factor
							yubic

4. Select Quick for program mode.

			YubiKey Personalization Too	bl					
Yubico OTP	ОАТН-НОТР	Static Password	Challenge-Response	Settings	Tools	About	Exit		
		Program in Yu	ibico OTP mode				Yubi	Key is inser	ted
Quick Quickly progra	am a YubiKey for use	e with Yubico Validation S	erver					•	
Advance Allows you to		e YubiKeys with greater o	control over the configuration v	alues			Program Not cont	mming statu figured	18:
							2.5.1	ve Version:	
							Dec:	3262790	r
							Hex:	3262790 31c946	1 [
							Modhex	:: ebrkfh	C
							Featu	res Supporte	ed
							Yubico	ОТР	
							2 Config	gurations	
							OATH-H	IOTP	
							Static P	assword	
								ode Mode	
								ge-Response	
							Updata	ble	
							Ndef		
							Univers	al 2nd Factor	114
							γι	ıbic	

- 5. Next, select Configuration Slot 1 and uncheck the Hide values box to reveal the Private Identity and Secret Key.
- 6. Click Write configuration.

ubico OTP	OATH-HOTP	Static Password	Challenge-Response	Settings	Tools	About	Exi	t	
		gram in Yubico	o OTP mode - Qui	ck			Yubi	Key is inser	ted
Configuration !									
	guration slot to be p	-				-	1.5		
Configuratio	n Slot 1	Configuration SI	ot 2			0		n -	
Yubico OTP Pa	rameters (auto ge	nerated)					~		
Public Identity (6 bytes Modhex)	vv uj fr el ne rh				0			
Hide values							Not con	mming statu	JS:
Private Identity	(6 bytes Hex)	a2 c3 f9 8d 67 cd						ngureu are Version:	
Secret Key (16	bytes Hex)	55 c1 90 4e 7b 96	e6 7d 4a 10 02 99 c6 2a 4e 33			0	2.5.1		
							Serial	Number	
Actions						\rightarrow	Dec:	3262790	J
Press Write Con	figuration button to	program your YubiKey's s	elected configuration slot				Hex:	31c946	1
Write Con	figuration	Upload to Yubico	Regenerate	Back			Modhey	k: ebrkfh	1
							Featu	res Supporte	ed
							Yubico	ОТР	
							2 Confi	gurations	
							OATH-H	HOTP	
								Password	
								ode Mode	
								ige-Response	
							Updata	ole	
							Ndef		
								al 2nd Factor	

۸	Keep this window and information open in order to register your token with Duo
0	Some users may encounter the following warning about overwriting the configuration in Slot 1. This is normal as some Yubikeys come pre-configured with YubiCloud credentials in slot 1.
	Confirm: Overwrite configuration slot 1?
	If you have a YubiKey VIP, this slot should contain a Symantec VIP credential by default. You should refrain from rewriting this Slot as a Symantec VIP credential can only be programmed during manufacture - you will thus not be able to get a new one. If you have any other YubiKey, this slot should contain a Yubico OTP credential by default. This credential is required for using the YubiKey with many of our services and that of our partners. If you overwrite this and want to use it again later, you will need to reprogram it and upload the new one to our YubiCloud validation service. Are you sure you want to overwrite the configuration slot 1? Don't show this message again No

7. You **may** be prompted to save the log file.

Save As:	yubiconfig.csv	·
Tags:		
Where:	📓 Macintosh HD	٢
		Cancel Save

Registering it with Duo Two-Factor authentication

Once you have the token configured, you can add it to your Duo devices:

- 1. Navigate to https://duo.mit.edu.
- 2. Once signed in, click on **Register a new hardware token**. *Result*: You are brought to the registration page.

C 🔅 https://d	luo.mit.edu/newtoken/		2
	IIIIT IST Information Systems and Technology		Search
	MIT Duo Sec	curity Account Ma	nagement
1	Please enter the information about your hardware to	ken below.	
	Type: YubiKey S Serial Number:		
	Private Identity:		
:	Secret Key:		
	Submit		

- 3. Make sure the appropriate token type is selected. For any model YubiKey, select Yubikey.
- 4. Enter (copy & paste) the Serial Number (in Decimal format), Private Identity, and Secret Key you generated when configuring your Yubikey and select Submit.

Result: You will be returned to the Duo settings page with a message saying the enrollment was successful.

000	8T Duo Security Account x	Eran
← → C 🕅	https://duo.mit.edu/verifysuccess/	☆ 🏭 =
	IVIIT IST Internation Systems and Technology	
	MIT Duo Security Account Management	
	You have successfully enrolled a new device with MIT's Duo Security two-factor authentication service.	
	Duo authentication is currently required for your account. You may change this setting below.	
	 Disable Duo for my account 	
	© Enable Duo for my account (recommended)	
	Submit	

You can now test your hardware token by authenticating to an MIT service..

Troubleshooting

If you repeatedly get the error "Invalid Yubikey private ID or secret key." when attempting to register a YubiKey, you might inadvertently have two configurations set up in your YubiKey and be triggering the wrong one during verification. Recent models of YubiKeys can store two configurations: you trigger the first by a short press of 0.3-1.5 seconds, and you trigger the second by a long press of 2.5-5 seconds. YubiKeys are easier to use if only configuration 1 is set up, so you should delete configuration 2 if you are certain that nothing else needs it.