TITLE

DUO - Using YubiKey for DUO Authentication

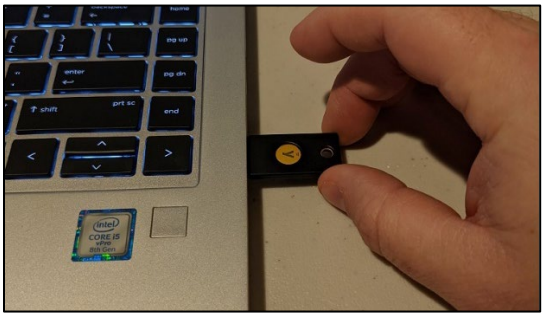
PROCEDURE

DUO is the University of Kansas Health System's **multi-factor authentication** platform (MFA.) MFA's provide an additional layer of security requiring something they know (i.e. a password) and something they have (a physical device.) While the preferred method of authentication with DUO is to register one's smartphone with the **DUO Mobile** app (which would make the user's phone their physical device), some users may need a pre-configured USB token called a YubiKey to serve as the physical device.

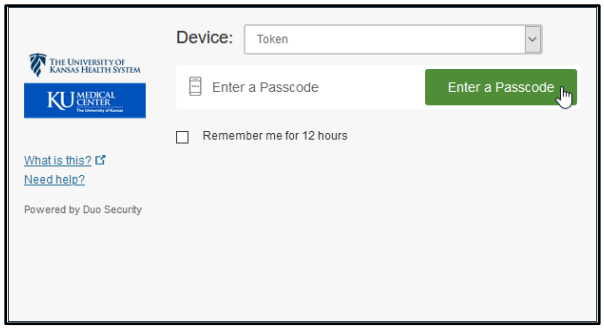
This process defines how to use the physical YubiKey device for authentication. It assumes the user is already in possession of a configured physical device. To obtain a YubiKey submit a request in myIT.

Locate the USB port on your workstation.

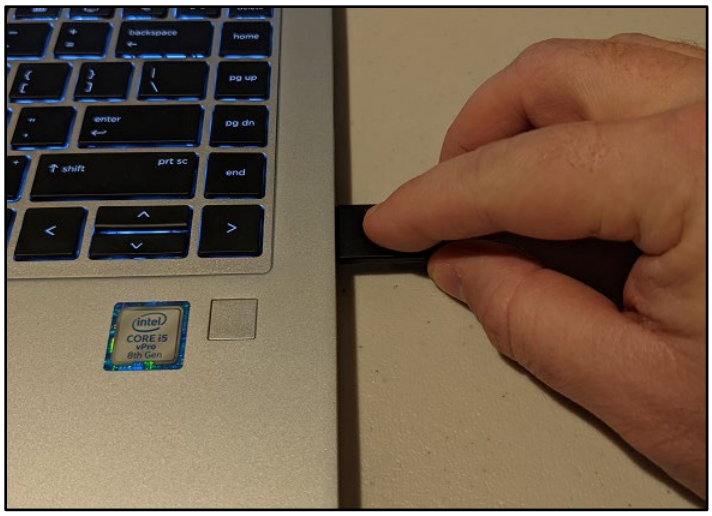
Connect the YubiKey device to your USB port



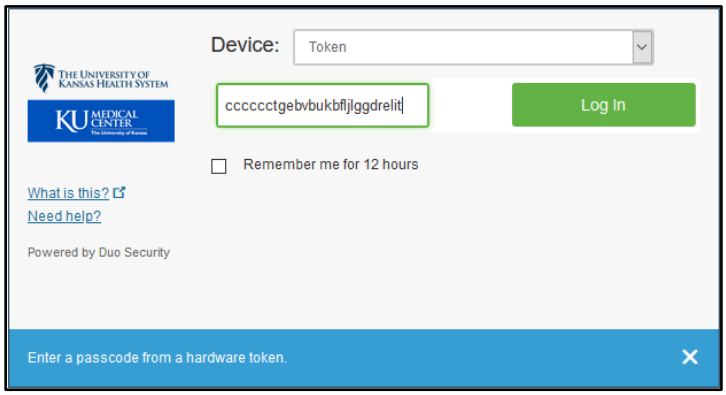
When logging in to a DUO protected app you will see a popup like the menu below. Click the green **Enter a Passcode** button**.**



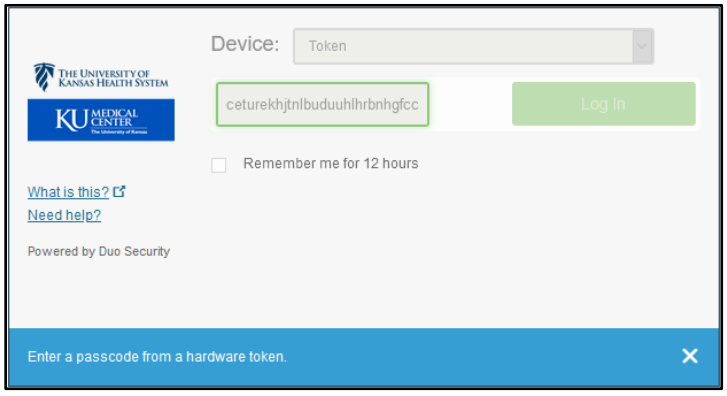
Press the button on the YubiKey device with the Y logo. (Do not hold down the Y button as this has other functionality.)



This will generate a One Time Passcode (OTP) – a random string of characters – in the text field.
Note: If no characters populate that field, remove the device, flip it over and insert it again as it may be in upside down.



Click the green **Log In** button.



RELATED DOCUMENTS

DUO – Using DUO Mobile for Authentication: [Duo (kansashealthsystem.com)]