

Standard Work: Setting up Multi-Factor Authentication

Role(s) Performing Process: Individual Users

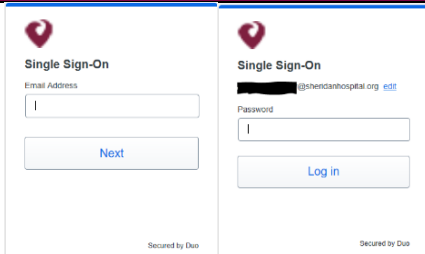
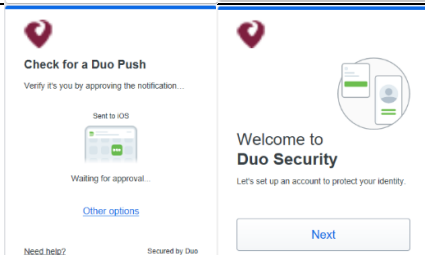
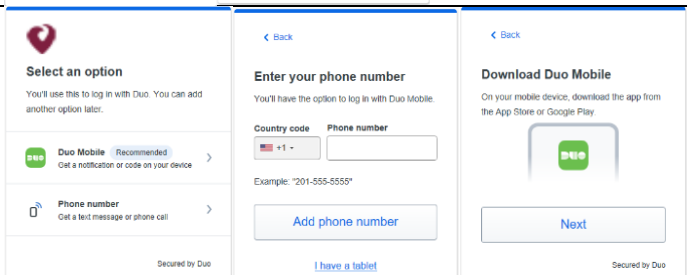
Location(s): Hospital-wide

Department: All

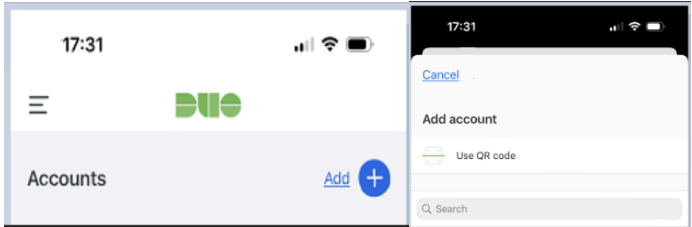
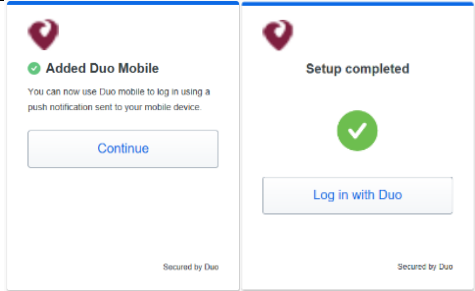
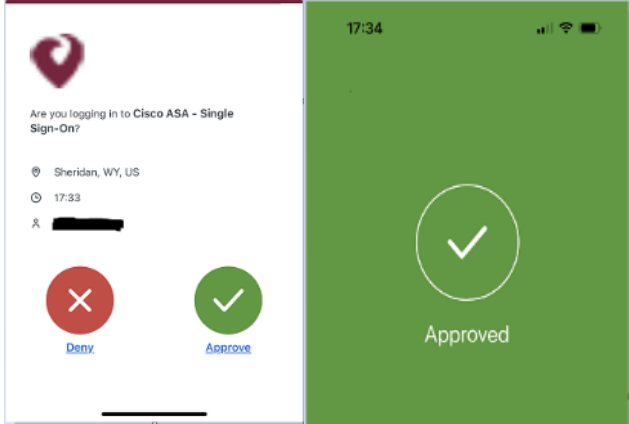
Process Owner: Individual Users

Date Implemented: 6/28/23

Purpose: SMH will be rolling out implementation of Cisco Duo across our remote access login sites to provide Multi-Factor Authentication (MFA) services to the hospital. (VPN, Webmail, Infor, etc)

STEP	TASK / MAJOR STEP (What?) (Add symbols as needed)	KEY POINTS Tools)	(How? Key Tips &	REASON (Why?)
1	After SMH's MFA go-live event when you access an MFA enabled space you will be prompted to enter your email address then password.			
2	Next, Anyconnect will look for an associated account. If this is your first-time utilizing Duo click on "Other options" here.			
3	Please select "Duo Mobile", at the bottom of the next screen, select "I have a tablet", then click "Next".			
4	Visit the App Store or Google Play on your phone and download Duo Mobile.	Duo Mobile - Google Play store (Android) Duo Mobile - App Store (Apple)		

Standard Work: Setting up Multi-Factor Authentication

5	In the app select "add". Select "Use QR code" and scan the QR code presented by Cisco AnyConnect on your pc.		
6	Continue through the remainder of the setup in AnyConnect.		
7	After clicking "Log in with Duo" your phone should buzz with a notification similar to the following: Approve the log in and you should be presented with an approval message and your access will be allowed.		
8	After completing this initial setup, each time you attempt to access an MFA enabled area, after entering your credentials, you will receive a notification on your phone that will prompt for approval and let you in once approval is granted.		
9			