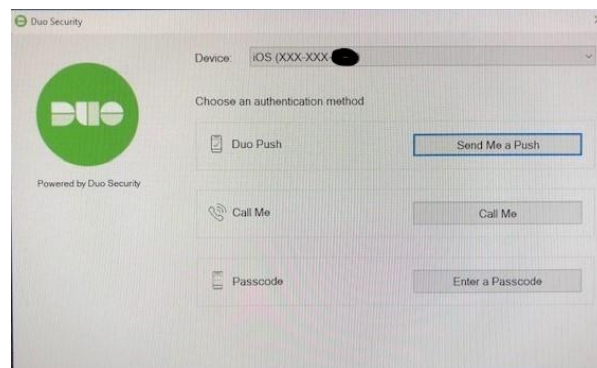


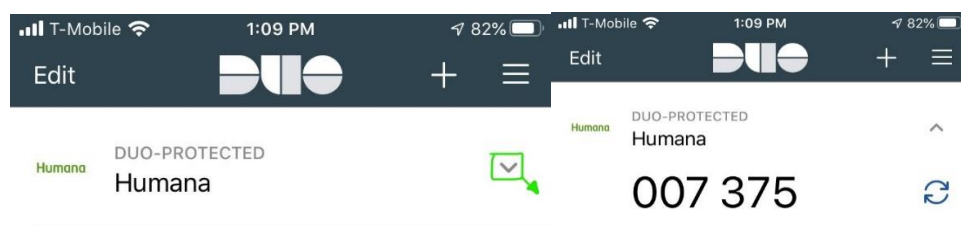
Glossary

2FA (two-factor authentication): an additional layer of authentication beyond a username and password. 2FA involves something you know (password) plus something you have with you (like Duo Mobile on your smartphone) to prevent someone from logging in with only your password. With Duo 2FA, you still enter your username and password. The second factor provided by Duo is simply an added layer of security on top of your existing credentials.

Duo Prompt: this interactive prompt lets you choose how to verify your identity each time you log in (e.g. “Duo Push” or “Call Me”) to a web-based application. The Duo Prompt allows you to enroll and authenticate.



Passcode: these are numeric codes that can be generated either via the Duo Mobile app, SMS (text message), or a hardware token. Passcodes may be used at any time and are particularly handy for authenticating when your 2FA device doesn't have internet or cellular service.



Push Notification (Duo Push): a push authentication request that is sent to the Duo Mobile App on an enrolled device. Push notifications include information like the geographical location of the access device, IP address of the access device, and the application being accessed so you can verify whether the push is real or fraudulent.



What devices does Humana Military support?

Humana Military supports Duo on smartphones and the Duo hardware token.



HGB Duo Token

What difference between Humana Military's token and WPS' token?

Humana Military's token is Duo while WPS' token is RSA (picture below):



WPS RSA token

How can I get the hardware token?

The HMHSSecurity team will be mailing it to your home. Be sure to update your home mailing address in Workday so they have the correct address.

What should I do when I received the token?

Access HGB Sharepoint at **go/duotoken**. Enter your name, email address and click submit.

How long does the battery on the token last?

Minimum 2 years and up to 7 years

What shall I do if my token stops working?

Contact CSS or HMHS Security for a replacement

What if my token gets damaged or is lost?

Contact CSS or HMHS Security for a replacement

How do I log into my workstation with DUO?

Watch the video: <https://www.youtube.com/watch?v=wiNBvWK0eKw>

Do I need to use DUO to unlock my physical workstation?

Yes. The DUO prompt will come up whenever you unlock your workstation.

Do I need to use DUO to unlock my Virtual workstation (VDI)?

No.

With DUO, do I still log in to the Array and Citrix Launchpad with SyferLock gridpin?

No, DUO replaces Syferlock. You will get the DUO prompt during the login process.

Do I require to have a smart device or data plan to use two-factor authentication?

No. Smart device is recommended but not require. Smart device is used as a backup plan in case you lose your hardware token. You can always use the Humana supplied DUO Token to authenticate.

What is Duo Mobile?

Duo Mobile is a mobile application (app) that you install on your smartphone or tablet to generate

passcodes for login or receive push notifications for easy, one-tap authentication on your mobile device. It works with Duo Security's two-factor authentication (2FA) service to make your logins more secure.

How much data does a Duo Push request use?

Duo Push authentication requests require a minimal amount of data -- less than 2KB per authentication. For example, you would only consume 1 megabyte (MB) of data if you were to authenticate 500 times in a given month.

What should I do if I lost my Humana phone?

Please contact CSS.

Can Duo see my password?

No. Your password is only verified by your organization and never sent to Duo. Duo provides only the second factor, using your enrolled device to verify it's actually you who is logging in.

Does using Duo give up control of my smartphone?

No. The Duo Mobile app has no access to change settings or remotely wipe your phone. The visibility Duo Mobile requires is to verify the security of your device, such as OS version, device encryption status, screen lock, etc. We use this to help recommend security improvements to your device. You always are in control of whether or not you take action on these recommendations.