FAQ- DUO and Partners SharePoint sites

Contents

What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is a method of confirming a user's identity by utilizing a combination of different components to verify your identity. This adds an additional layer of protection to your accounts and the data that is accessed through them. An everyday example is using an ATM: only the correct combination of your bank card (something you have) and your PIN (something you know) allows a transaction to be carried out.

Why do we need to use Multi-Factor Authentication to login?

Johns Hopkins Applied Physics Laboratory (JHAPL) must comply with a new mandated federal government requirement promulgated by a Defense Federal Acquisition Regulation Supplement (DFARS) for protection of unclassified sensitive data resident on IT systems and networks. To fulfill two of the requirements of the ongoing implementation of NIST 800-171, all federal contractors are required to use Multi-Factor Authentication to access network services by Dec 31, 2017.

What is a token?

A token is a physical device or software application that provide the user with a second form of authentication. The username and password would be considered something you know, and the token would be considered something you have which meets the Multi-Factor Authentication requirement.

When is a token needed?

A token will be needed each time you attempt to access a JHAPL Partners SharePoint site.
You will begin with entering your username and password. You will then be prompted to enter a passcode. This can be generated via hard token, soft token, text message or landline phone call.
Note: Tokens are not needed to access Secure File Transfer Protocol (SFTP).

What devices can I use to generate a DUO passcode?

- Hard Tokens
- Soft tokens can be installed on
  - iOS devices (iPhone and iPad)
  - Android devices
  - Windows Phone
- Mobile phones can be used to receive a text message with a passcode
- Landlines and mobile phones can be used to receive a phone call with a passcode

What kind of authentication methods are available?

Hard tokens are physical tokens. They are devices a little smaller than a thumb drive. They generate a passcode using a preconfigured algorithm that you will be able to enter when accessing the Partners SharePoint site.
If you typically work in a closed area, a hard token is a good option.

Soft token is a mobile application that can be installed on an iOS or Android device. Once an outer domain account has been created you will be able to complete a soft token self-enrollment by navigating to the Partners SharePoint site. The self-enrollment guides you through the process of installing the application and completing the soft token enrollment. Soft tokens utilize DUO Push and passcodes for authentication.

DUO passcodes can also be generated via a **Phone call** or **Text Message**. To use the phone call option, the landline option can be selected during the initial DUO setup. To use the text message option, a mobile device needs to be set up.

What is DUO Push?

Duo Push is the easiest and quickest way of authenticating. When this option is selected, you'll get a login request sent to your mobile phone — just press Approve to authenticate and you will be logged into the SharePoint site.
This is the recommended way to complete DUO authentication.

How do I login to a Partners SharePoint site with a token?

When accessing a Partners SharePoint site, you will first enter your username and password. Once you have authenticated with something you know, you will be asked for the DUO passcode. This can be generated from a hard token, the DUO Mobile smart phone app, a text message or landline phone call. You will enter the passcode on the site and will be allowed access to the SharePoint site.

Can hard tokens be reassigned?

Tokens can be reassigned. If an individual no longer needs access to a Partners SharePoint site, the token can be deleted in order to remove access. The token can then be reassigned to another account.

What do I do if I lose my hard token?

Please contact your site owner (external users) or the APL Help desk (internal users). The token can be unassigned and a new token can be assigned and sent to you or picked up from the APL Help desk.

What should be done with hard tokens that are no longer being used?

Tokens that are not being used any longer should be sent back to the site owner.