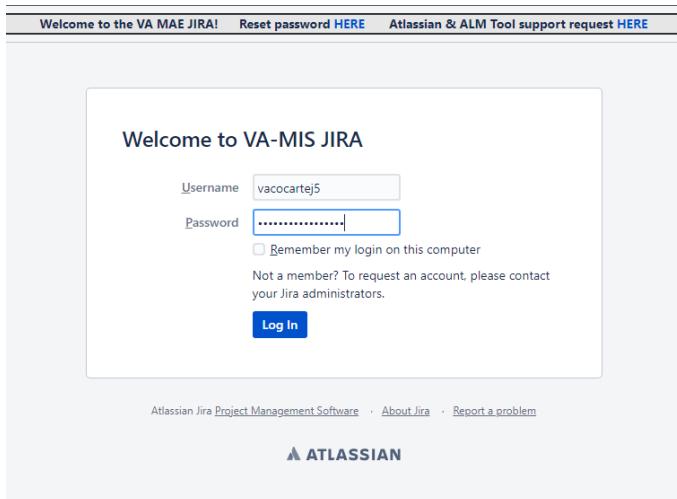
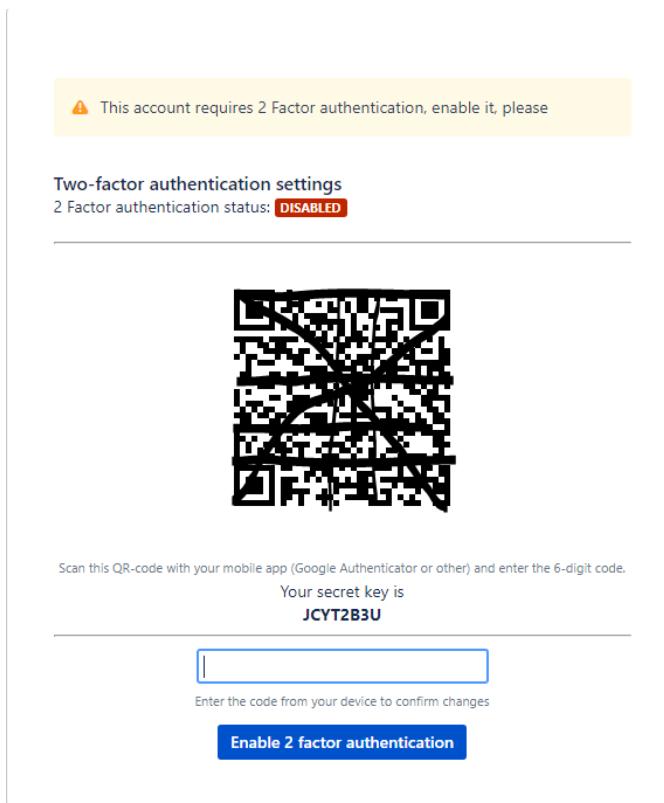


Atlassian 2FA Guide

1. Enter Username/Password and Log In. You will be prompted to enable 2FA:



2FA Enable: Google Authenticator is recommended but other MFA applications work. (Enter in 6 digit pin that is provided from application and click "Enable 2 factor authentication")



2. After you enable 2 factor authentication you will get to a screen where you can download backup codes (recommended).

Backup codes

ⓘ In case you lose your phone or access to your one-time password, each of these recovery codes can be used once to regain access to your account. Please save them in a secure place, otherwise you will lose access to your account.

[REDACTED]

[Download codes](#)

[Continue](#)

3. After you click continue you will get a U2F devices page (you can skip this step as it is not necessary).

ⓘ As U2F devices are only supported by a few browsers.
We require you to set up a two-factor authentication app before a U2F device. Thus you'll always be able to log in, even when you use an unsupported browser.

Two-factor authentication settings

2 Factor authentication status: **ENABLED**

[Deactivate 2FA Protection](#)

Increase security of your account by enabling 2FA.

Register U2F Hardware Security Keys

U2F Hardware Security keys can be used as your second factor of authentication instead of a verification code.

[Add U2F Device](#)

#	Name	Added	Delete
---	------	-------	--------

ⓘ 2FA is already enabled.

Additionally, you can add U2F devices as an alternative to TOTP, or you may [skip adding U2F devices](#) at all or add them later.

4. You have successfully enabled 2 factor authentication and will be logged into the application.

Important note: Since 2 factor authentication is now enabled, for our Bitbucket application (coderepo.mobilehealth.va.gov) you will need to create a Personal Access Token to use any GIT Related commands (i.e git clone, git pull, git push) wiki page: [2 Factor Authentication - Bitbucket Personal Access Token Use](#)