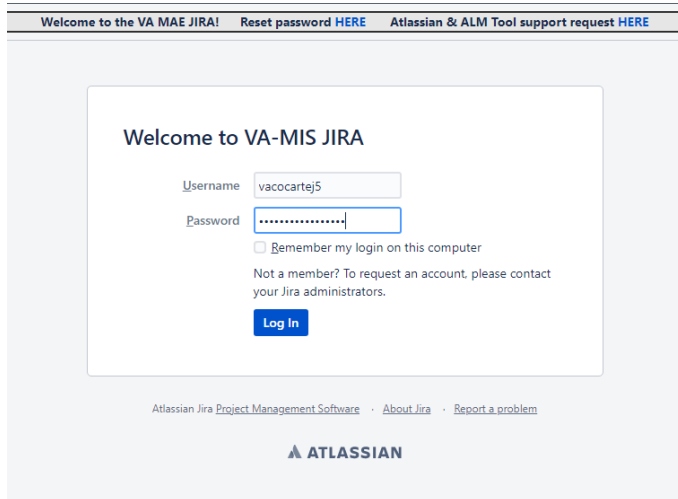


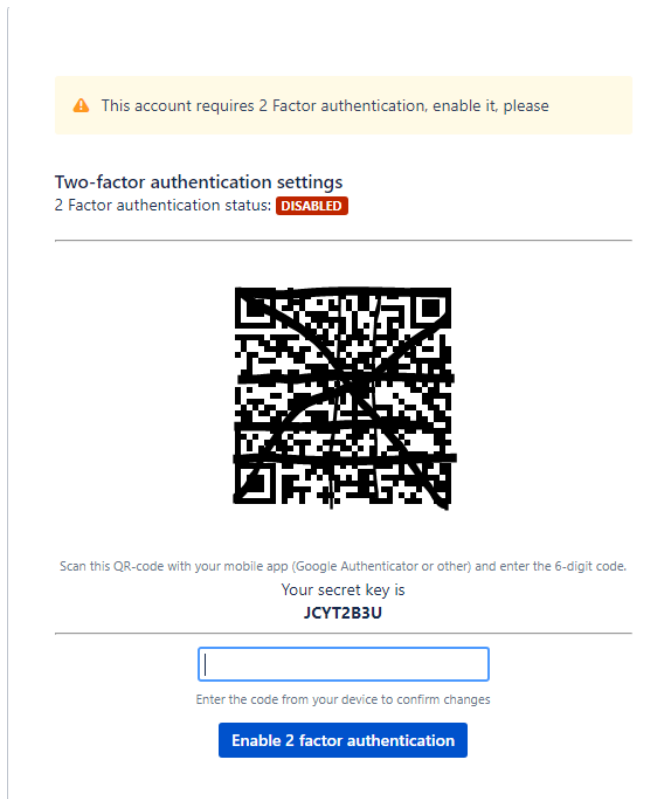
Atlassian 2FA Guide

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



The screenshot shows the login interface for 'VA-MIS JIRA'. At the top, there are links: 'Welcome to the VA MAE JIRA!', 'Reset password HERE', and 'Atlassian & ALM Tool support request HERE'. The main login box contains the title 'Welcome to VA-MIS JIRA', a 'Username' field with 'vacocartej5', a 'Password' field with masked characters, a 'Remember my login on this computer' checkbox, and a 'Log In' button. Below the login box, there are links for 'Atlassian Jira Project Management Software', 'About Jira', and 'Report a problem', followed by the Atlassian logo.

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")



The screenshot shows the 'Two-factor authentication settings' page. It starts with a yellow warning box stating 'This account requires 2 Factor authentication, enable it, please'. Below this, the '2 Factor authentication status' is shown as 'DISABLED'. A QR code is displayed for scanning with a mobile app. Below the QR code, the text 'Scan this QR-code with your mobile app (Google Authenticator or other) and enter the 6-digit code.' is followed by 'Your secret key is JCYT2B3U'. A text input field is provided for entering the 6-digit code from the device. At the bottom, there is a blue button labeled '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

- i** 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.



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).

i 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 |
|---|------|-------|--------|
|---|------|-------|--------|

i 2FA is already enabled.

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](#)