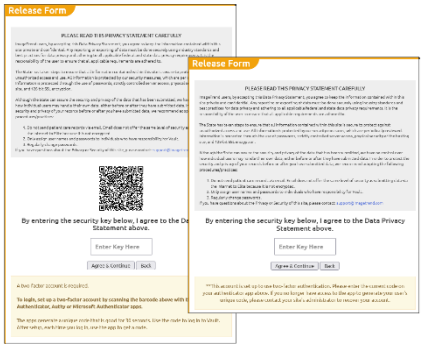
Article: Users > About Two-Factor Authentication

Two-Factor Authentication



Two-factor authentication is an additional safeguard to the configurable password settings for protecting access to your agency's historical data. Vault's two-factor authentication uses approved third-party applications that generate a unique six-digit code every 60 seconds for users to enter into Vault when logging in.

Vault requires all users to log in using two-factor authentication for increased login security.

> **NOTE:** Two-factor authentication is **not** a configurable option; all users must log in to Vault using two-factor authentication

How Does Two-Factor Authentication Work?

Setup

Two-factor authentication is setup on a user's first time logging in to Vault and each time their two-factor authentication is reset. After logging in to Vault, users scan a QR code using one of the approved two-factor authenticator apps: Google Authenticator, Microsoft Authenticator or Authy. The apps generate a unique code every 60 seconds.

MIEMSS does not endorse any specific two-factor authenticator app available.

Logging In

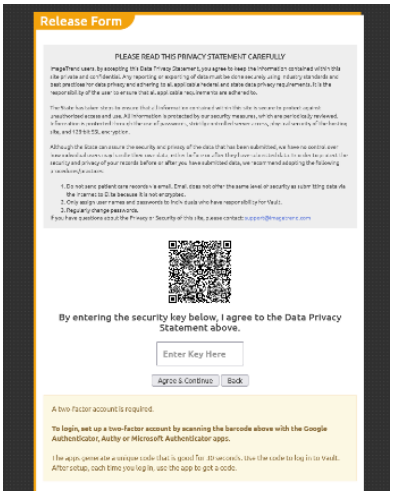
Users must authenticate themselves by entering a code from the authenticator app each time they log in to Vault. After entering their username and password, users can enter the code form the authenticator app into the Enter Key Here field on the Release Form.

Managing Two-Factor Authentication

Two-factor authentication can be reset when users get a new mobile device or if they lose their device. Resetting two-factor authentication requires the user to set up two-factor again the next time they log in to Vault.

To reset an account's Two-Factor Authentication, send request to eMEDS® Support

Setting Up Two-Factor Authentication



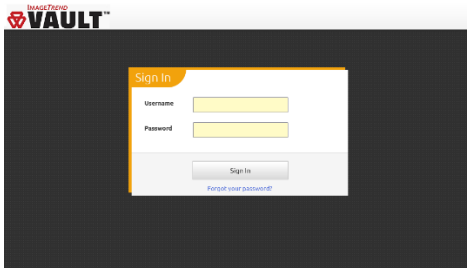
On your first time logging in to Vault or if your two-factor authentication is reset, you must set up two-factor authentication. There are three different apps you can use for two-factor authentication: (1) Google Authenticator, (2) Microsoft Authenticator and (3) Authy. The approved apps provide a unique code for you to enter on the Release Form to set up two-factor authentication and each time you log in to Vault.

After two-factor is setup, you must use the authenticator app to get a code each time you log in to Vault.

How to Set Up Two-Factor Authentication

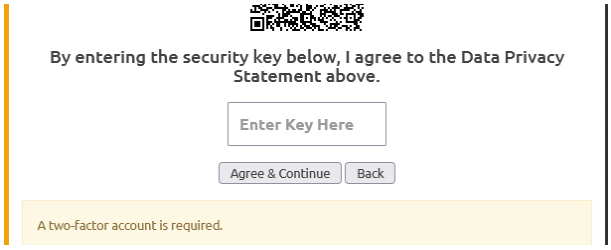
IMPORTANT! Set up requires a mobile device capable of downloading an authentication app: Google Authenticator, Microsoft Authenticator or Authy.

1. In a web browser, navigate to the Vault URL provided to you by your administrators
2. Enter your username and password.



> **HINT:** If you do not remember your password, click Forgot Password. Forgot password emails are sent to your Vault email address.

3. Click Sign In.
4. Using your mobile device, open the authenticator app Google Authenticator, Microsoft Authenticator or Authy) and scan the QR code in the Release Form.
5. Enter the two-factor authentication code into the Enter Key Here box.



6. Click Agree & Continue.