

Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) is now recommended to secure logins against phishing attacks and credential theft. This authentication method enables two-step verification for the users. The first step would be to fill in the username and password. The second verification step would be to enter a Verification Code aka OTP shared via email, or phone app thereby increasing the security of the user's account at the time of access.

When you work in an organization, the need for two-factor authentication rises significantly, as a single compromised account can put the organization's data security at risk. When 2FA is enabled by the admins, each time a user signs in to Docsvault on a new device, they will need to enter a password and a verification code.

Highlights

- ✓ Adds an extra layer of security to keep hackers out
- ✓ Allows secure access beyond company networks and adds flexibility
- ✓ Allows admins to configure delivery of codes by email only, mobile app only or both
- ✓ Meets regulatory compliance

How Two-Factor Authentication works?

Signing in to your account will work in the following way:



1. Enter your username and password:

Whenever you sign in to Docsvault, as usual, you will enter your username and password.

2. Enter Verification Code

You can get verification code via email or use specialized authenticator apps like Google Authenticator, Microsoft Authenticator, Authy, etc. Once linked to your accounts, the app displays a constantly changing set of codes to utilize whenever needed for verification.

Solutions

- **Business Continuity**
Security is an integral part of business continuity and Docsvault ensures your important documents are secure.
- **Regulatory Compliance**
Prevent users from tampering records and files thus ensuring regulatory compliance.

For More Details, visit:

www.Docsvault.com

Sales(at)Docsvault.com | (888) 819 3035

3. Keeping Sign-in Simple

You can choose to remember your second factor of authentication on your trusted devices for a specific period. From then on, that device will only ask for your password when you sign in.

You will still be covered by 2FA because when anyone else or you try to sign into your account on another device, Two-Factor Authentication will be required.

How Two-Factor Authentication protects you?

Two-Factor authentication adds an extra layer of security while signing into DocsVault. If a hacker hacks through your password, they will still need access to your phone or verification code to get into your account.

Fast Facts

1. Two-Factor authentication implementation allows users to safely access business documents remotely from any device or location without putting sensitive data at risk.
2. As codes are constantly changed, dynamically generated verification codes are safer to use than fixed (static) log-in information.
3. You can allow or disallow your users to skip the second factor of authentication on their trusted devices for a specific period after the initial two step verification.

For More Details, visit:

www.DocsVault.com

Sales(at)DocsVault.com | (888) 819 3035