About two-factor authentication

In this article

Two-factor authentication (2FA) is an extra layer of security used when logging into websites or apps. With 2FA, you have to log in with your username and password and provide another form of authentication that only you know or have access to.

For GitHub Enterprise Server, the second form of authentication is a code that's generated by an application on your mobile device. After you enable 2FA, GitHub Enterprise Server generates an authentication code any time someone attempts to sign into your account on your GitHub Enterprise Server instance. The only way someone can sign into your account is if they know both your password and have access to the authentication code on your phone.

After you configure 2FA, using a time-based one-time password (TOTP) mobile app, you can add a security key, like a FIDO2 hardware security key, Apple Touch ID or Windows Hello. The technology that enables authentication with a security key is called WebAuthn. WebAuthn is the successor to U2F and works in all modern browsers. For more information, see "WebAuthn" and "Can I Use."

You can also configure additional recovery methods in case you lose access to your two-factor authentication credentials. For more information on setting up 2FA, see "Configuring two-factor authentication" and "Configuring two-factor authentication recovery methods."

We **strongly** urge you to enable 2FA for the safety of your account, not only on GitHub Enterprise Server, but on other websites and apps that support 2FA. You can enable 2FA to access GitHub Enterprise Server and GitHub Desktop.

For more information, see "Accessing GitHub using two-factor authentication."

Two-factor authentication recovery codes

When you configure two-factor authentication, you'll download and save your 2FA recovery codes. If you lose access to your phone, you can authenticate to GitHub Enterprise Server using your recovery codes. For more information, see "Recovering your account if you lose your 2FA credentials."

Requiring two-factor authentication in your organization

Organization owners can require that organization members and outside collaborators use two-factor authentication to secure their personal accounts. For more information, see "Requiring two-factor authentication in your organization."

Authentication methods that support 2FA

Authentication Method	Description	Two-factor authentication support
Built-in	Authentication is performed against personal accounts that are stored on the GitHub Enterprise Server appliance.	Supported and managed on the GitHub Enterprise Server appliance. Organization owners can require 2FA to be enabled for members of the organization.
Built-in authentication with an identity provider	Authentication is performed against accounts that are stored on the identity provider.	Dependent on the identity provider.
LDAP	Allows integration with your company directory service for authentication.	Supported and managed on the GitHub Enterprise Server appliance. Organization owners can require 2FA to be enabled for members of the organization.
SAML	Authentication is performed on an external identity provider.	Not supported or managed on the GitHub Enterprise Server appliance, but may be supported by the external authentication provider. Two-factor authentication enforcement on organizations is not available.
CAS	Single sign-on service is provided by an external server.	Not supported or managed on the GitHub Enterprise Server appliance, but may be supported by the external authentication provider. Two-factor authentication enforcement on organizations is not available.