Creating a strong password

Secure your account on your GitHub Enterprise Server instance with a strong and unique password using a password manager.

You must choose or generate a password for your account on your GitHub Enterprise Server instance that is at least:

- Seven characters long, if it includes a number and a lowercase letter, or
- 15 characters long with any combination of characters

To keep your account secure, we recommend you follow these best practices:

- Use a password manager to generate a password of at least 15 characters.
- Generate a unique password for GitHub Enterprise Server. If you use your GitHub Enterprise Server password elsewhere and that service is compromised, then attackers or other malicious actors could use that information to access your account on your GitHub Enterprise Server instance.
- Configure two-factor authentication for your personal account. For more information, see "About two-factor authentication."
- Never share your password, even with a potential collaborator. Each person should use their own personal account on GitHub Enterprise Server. For more information on ways to collaborate, see: "Inviting collaborators to a personal repository," "About collaborative development models," or "Collaborating with groups in organizations."

You can only use your password to log on to GitHub Enterprise Server using your browser. When you authenticate to GitHub Enterprise Server with other means, such as the command line or API, you should use other credentials. For more information, see "About authentication to GitHub."

Further reading

- "Caching your GitHub credentials in Git"
- "Keeping your account and data secure"