About two-factor authentication and SAML single sign-on

Organization owners can enable both SAML single sign-on and two-factor authentication to add additional authentication measures for their organization members.

Two-factor authentication (2FA) provides basic authentication for organization members. By enabling 2FA, organization owners limit the likelihood that a member's account on GitHub.com could be compromised. For more information on 2FA, see "About two-factor authentication."

To add additional authentication measures, organization owners can also enable SAML single sign-on (SSO) so that organization members must use single sign-on to access an organization. For more information on SAML SSO, see "About identity and access management with SAML single sign-on."

If both 2FA and SAML SSO are enabled, organization members must do the following:

- Use 2FA to log in to their account on GitHub.com
- Use single sign-on to access the organization
- Use an authorized token for API or Git access and use single sign-on to authorize the token

Further reading

- "Enforcing SAML single sign-on for your organization"