GitHub Docs

Enterprise administrators / Identity and access management / Manage IAM for your enterprise / Change authentication methods

Changing authentication methods

You can change the way GitHub Enterprise Server authenticates with your existing accounts at any time.

User accounts on your GitHub Enterprise Server instance are preserved when you change the authentication method and users will continue to log into the same account as long as their username doesn't change.

If the new method of authentication changes usernames, new accounts will be created. As an administrator, you can rename users through the site admin settings or by using the User Administration API.

Other issues you should take into consideration include:

- **Passwords:** If you switch to using built-in authentication for your instance, users must set a password after the change is completed.

- **Site administrators:** Administrative privileges are controlled by your identity provider when you use SAML and can be controlled by group membership when you use LDAP.

- **Team membership:** Only LDAP lets you control team membership from your directory server.

- **User suspension:** When you use LDAP to authenticate, access to GitHub Enterprise Server can be controlled via *restricted groups*. After switching to LDAP, if restricted groups are configured, existing users who are not in one of those groups will be suspended. Suspension will occur either when they log in or during the next LDAP Sync.

- **Group membership:** When you use LDAP to authenticate, users are automatically suspended and unsuspended based on restricted group membership and account status with Active Directory.

- **Git authentication:** SAML and CAS only supports Git authentication over HTTP or HTTPS using a personal access token. Password authentication over HTTP or HTTPS is not supported. LDAP supports password-based Git authentication by default, but we recommend that you disable that method and force authentication via a personal access token or SSH key.

- **API authentication:** SAML and CAS only supports API authentication using a personal access token. Basic authentication is not supported.

- **Two-factor authentication:** When using SAML or CAS, two-factor authentication is not supported or managed on the GitHub Enterprise Server instance, but may be supported by the external authentication provider. Two-factor authentication enforcement on organizations is not available. For more information about enforcing two-factor authentication on organizations, see "Requiring two-factor authentication in your organization."

- **Fallback authentication for users with no account on your external authentication provider:** You can invite users to authenticate to your GitHub Enterprise Server instance without adding them to your identity provider. For more

information, see "[Allowing built-in authentication for users outside your provider](#)."