About support for your IdP's Conditional Access Policy

In this article

When your enterprise uses OIDC SSO, GitHub can validate access to your enterprise and its resources using your IdP's Conditional Access Policy (CAP).

To manage users in your enterprise with your identity provider, your enterprise must be enabled for Enterprise Managed Users, which is available with GitHub Enterprise Cloud. For more information, see "About Enterprise Managed Users."

Note: OpenID Connect (OIDC) and Conditional Access Policy (CAP) support for Enterprise Managed Users is only available for Azure AD.

About support for Conditional Access Policies

When your enterprise uses OIDC SSO, GitHub will automatically use your IdP's conditional access policy (CAP) IP conditions to validate user interactions with GitHub, when members change IP addresses, and each time a personal access token or SSH key is used.

GitHub Enterprise Cloud supports CAP for any enterprise with managed users where OIDC SSO is enabled. GitHub Enterprise Cloud enforces your IdP's IP conditions but cannot enforce your device compliance conditions. Enterprise owners can choose to use this IP allow list configuration instead of GitHub Enterprise Cloud's IP allow list, and can do so once OIDC SSO is configured. For more information about IP allow lists, see "Restricting network traffic to your enterprise with an IP allow list" and "Managing allowed IP addresses for your organization."

For more information about using OIDC with Enterprise Managed Users, see "Configuring OIDC for Enterprise Managed Users" and "Migrating from SAML to OIDC."

Considerations for integrations and automations

GitHub sends the originating IP address to your IdP for validation against your CAP. To make sure actions and apps are not blocked by your IdP's CAP, you will need to make changes to your configuration.

Warning: If you use GitHub Enterprise Importer to migrate an organization from your GitHub Enterprise Server instance, make sure to use a service account that is exempt from Azure AD's CAP otherwise your migration may be blocked.

GitHub Actions

Actions that use a personal access token will likely be blocked by your IdP's CAP. We recommend that personal access tokens are created by a service account which is then exempted from IP controls in your IdP's CAP.

If you're unable to use a service account, another option for unblocking actions that use personal access tokens is to allow the IP ranges used by GitHub Actions. For more information, see "About GitHub's IP addresses."

GitHub Codespaces

GitHub Codespaces may not be available if your enterprise uses OIDC SSO with CAP to restrict access by IP addresses. This is because codespaces are created with dynamic IP addresses which it's likely your IdP's CAP will block. Other CAP policies may also affect GitHub Codespaces's availability, depending on the policy's specific setup.

GitHub Apps and OAuth apps

When GitHub Apps and OAuth apps sign a user in and make requests on that user's behalf, GitHub will send the IP address of the app's server to your IdP for validation. If the IP address of the app's server is not validated by your IdP's CAP, the request will fail.

When GitHub Apps call GitHub APIs acting either as the app itself or as an installation, these calls are not performed on behalf of a user. Since your IdP's CAP executes and applies policies to user accounts, these application requests cannot be validated against CAP and are always allowed through. For more information on GitHub Apps authenticating as themselves or as an installation, see "About authentication with a GitHub App".

You can contact the owners of the apps you want to use, ask for their IP ranges, and configure your IdP's CAP to allow access from those IP ranges. If you're unable to contact the owners, you can review your IdP sign-in logs to review the IP addresses seen in the requests, then allow-list those addresses.

If you do not wish to allow all of the IP ranges for all of your enterprise's apps, you can also exempt installed GitHub Apps and authorized OAuth apps from the IdP allow list. If you do so, these apps will continue working regardless of the originating IP address. For more information, see "Enforcing policies for security settings in your enterprise."