Token expiration and revocation

In this article

Your tokens can expire and can also be revoked by you, applications you have authorized, and GitHub Enterprise Server itself.

When a token has expired or has been revoked, it can no longer be used to authenticate Git and API requests. It is not possible to restore an expired or revoked token, you or the application will need to create a new token.

This article explains the possible reasons your GitHub Enterprise Server token might be revoked or expire.

> **Note:** When a personal access token or OAuth token expires or is revoked, you may see an `oauth_authorization.destroy` action in your security log. For more information, see "Reviewing your security log."

Token revoked after reaching its expiration date

When you create a personal access token, we recommend that you set an expiration for your token. Upon reaching your token's expiration date, the token is automatically revoked. For more information, see "Managing your personal access tokens."

Token revoked by the user

You can revoke your authorization of a GitHub App or OAuth app from your account settings which will revoke any tokens associated with the app. For more information, see "Reviewing and revoking authorization of GitHub Apps" and "Reviewing your authorized OAuth apps."

Once an authorization is revoked, any tokens associated with the authorization will be revoked as well. To reauthorize an application, follow the instructions from the third-party application or website to connect your account on your GitHub Enterprise Server instance again.

Token revoked by the OAuth app

The owner of an OAuth app can revoke an account's authorization of their app, this will also revoke any tokens associated with the authorization. For more information about revoking authorizations of your OAuth app, see "Apps."

OAuth app owners can also revoke individual tokens associated with an authorization. For more information about revoking individual tokens for your OAuth app, see "OAuth Authorizations".

Token revoked due to excess of tokens for an OAuth app with the same scope

There is a limit of ten tokens that are issued per user/application/scope combination, and a rate limit of ten tokens created per hour. If an application creates more than ten tokens for the same user and the same scopes, the oldest tokens with the same user/application/scope combination are revoked. However, hitting the hourly rate limit will not revoke your oldest token. Instead, it will trigger a re-authorization prompt within the browser, asking the user to double check the permissions they're granting your app. This prompt is intended to give a break to any potential infinite loop the app is stuck in, since there's little to no reason for an app to request ten tokens from the user within an hour.

User token revoked due to GitHub App configuration

User access tokens created by a GitHub App will expire after eight hours by default. Owners of GitHub Apps can optionally change the default expiration period for their user access tokens, or configure the tokens to never expire. For more information about configuring your GitHub App's user access tokens, see "Activating optional features for GitHub Apps."

Legal

© 2023 GitHub, Inc. Terms Privacy Status Pricing Expert services Blog