Git

Git "Support for Password Authentication Was Removed" Error

7 months ago • by John Otieno

GitHub is one of the largest and most popular online version control system for any developer and organizations. It contains a large percentage of open source and closed source in the world and facilitates the developers to create and collaborate on various projects.

However, when pushing changes to a GitHub-hosted repository, you might encounter an error such as "support for password authentication was removed. Please use a personal access token instead."

In this tutorial, we will explore the cause/source of this error and how we can fix it when working with a Git repo.

Cause

As of August 2021, GitHub introduced the feature for any user to use the token-based authentication in order to perform various authenticated Git repositories.

This removed the feature of using the account passwords when authenticating to GitHub using REST API.

As a result, attempting to access or perform any authenticated operations on a GitHub-hosted repository using password authentication will result in the said error.

Solution

Let us proceed and discuss how you can quickly fix this error when attempting to push the code on the remote repository.

The method to fix this error is to enable and configure the access token on GitHub which allows us to perform the token-based authentication when running the Git operations.

To enable the access on token-based authentication, start by logging into your GitHub account and head over to the "Settings".
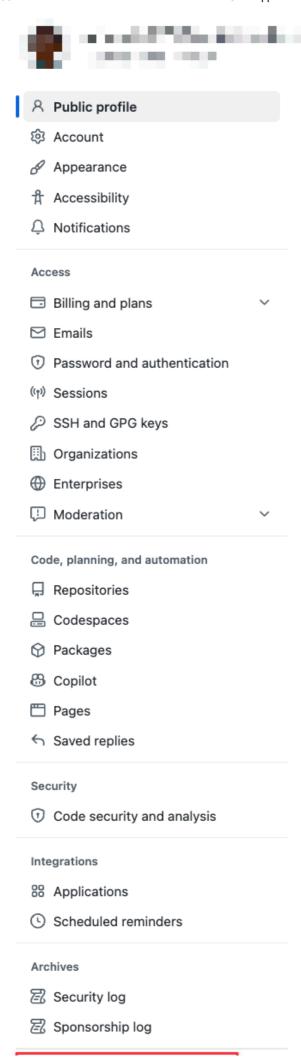
😊 Working, as usual

👤 Your profile

👤⁺ Add account

🔖 Your repositories

📋 Your projects

🏢 Your organizations

🌐 Your enterprises

☆ Your stars

♡ Your sponsors

‹› Your gists

⬆ Upgrade

🌐 Try Enterprise

👥 Copilot

⚗ Feature preview

⚙ Settings

📖 GitHub Docs

🗣 GitHub Support
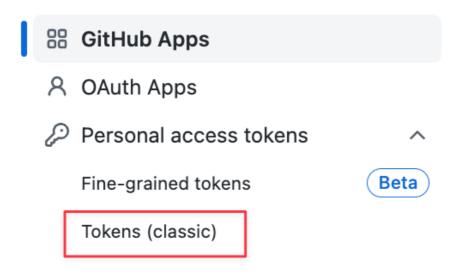
Sign out

In the "Settings" page, scroll down and look for the "Developer Settings" option.

Public profile

Account

Appearance

Accessibility

Notifications

Access

Billing and plans ⌄

Emails

Password and authentication

Sessions

SSH and GPG keys

Organizations

Enterprises

Moderation ⌄

Code, planning, and automation

Repositories

Codespaces

Packages

Copilot

Pages

Saved replies

Security

Code security and analysis

Integrations

Applications

Scheduled reminders

Archives

Security log

Sponsorship log

In the "Developer Settings" window, select "Personal Access Tokens" and choose "Tokens (Classic)".

At the top-right, choose "Generate new token" and select "Generate new token (classic)".
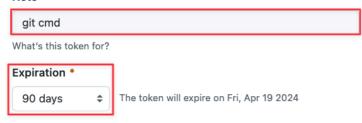
In the next step, fill the details for the "Note" section and then set an expiration date for the access token. It is recommended to set an expiration date although GitHub allows you to create a non-expiring token.
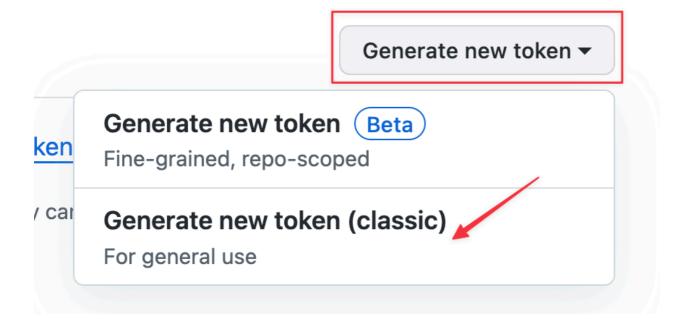
New personal access token (classic)

Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.

Note

git cmd

What's this token for?

Expiration *

90 days ⇕   The token will expire on Fri, Apr 19 2024

Under the "Scope" section, enable the following scopes for your token:

1. workflow
2. delete:packages
3. admin:org
4. admin:public_key
5. delete_repo
6. admin:enterprise
7. project
8. admin:gpg_key
9. admin:ssh_signing_key

Click on "Generate Token" with the selected scope.

☑ **delete_repo**	Delete repositories
☐ **write:discussion**	Read and write team discussions
☐ read:discussion	Read team discussions
☑ **admin:enterprise**	Full control of enterprises
☑ manage_runners:enterprise	Manage enterprise runners and runner groups
☑ manage_billing:enterprise	Read and write enterprise billing data
☑ read:enterprise	Read enterprise profile data
☐ **audit_log**	Full control of audit log
☐ read:audit_log	Read access of audit log
☐ **codespace**	Full control of codespaces
☐ codespace:secrets	Ability to create, read, update, and delete codespace secrets
☐ **copilot**	Full control of GitHub Copilot settings and seat assignments
☐ manage_billing:copilot	View and edit Copilot Business seat assignments
☑ **project**	Full control of projects
☑ read:project	Read access of projects
☑ **admin:gpg_key**	Full control of public user GPG keys
☑ write:gpg_key	Write public user GPG keys
☑ read:gpg_key	Read public user GPG keys
☑ **admin:ssh_signing_key**	Full control of public user SSH signing keys
☑ write:ssh_signing_key	Write public user SSH signing keys
☑ read:ssh_signing_key	Read public user SSH signing keys

Generate token   Cancel

Next, copy the resulting token.

Personal access tokens (classic)   Generate new token ▾   Revoke all

---

Tokens you have generated that can be used to access the GitHub API.

> Make sure to copy your personal access token now. You won't be able to see it again!

✓ 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 🗐   Delete

Personal access tokens (classic) function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to authenticate to the API over Basic Authentication.
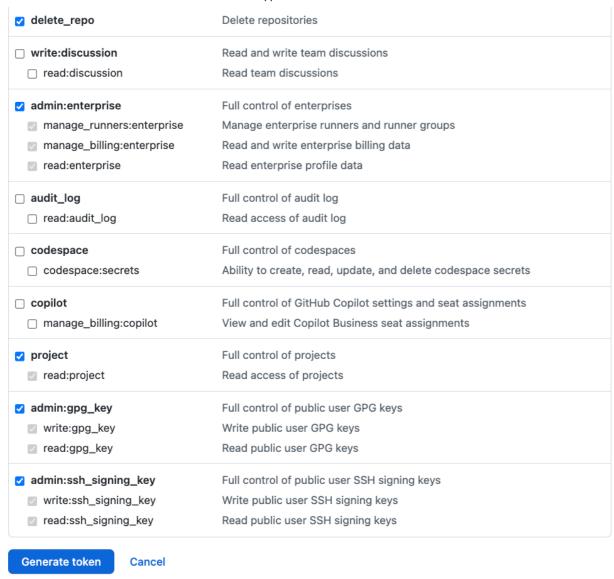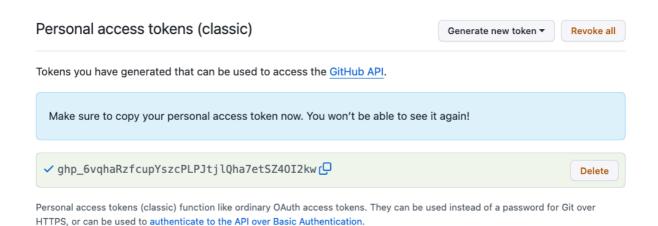
Paste it into the password field when running the Git command.

This should help you fix the "please use a personal access token instead" error when performing the changes to a remote GitHub repository.