Terminal - Error GitHub Credenciales Token

Es posible que te hayas encontrado con el siguiente **error** al intentar hacer "`push`" en tu primer **repositorio de GitHub**:

```
remote: Support for password authentication was removed on August 13, 2021. Please use
a personal access token instead.

remote: Please see https://github.blog/2020-12-15-token-authentication-requirements-
for-git-operations/ for more information.

fatal: Authentication failed for 'https://github.com/<username>/<reponame>.git/'
```

Este error ocurre porque **GitHub ya no permite autenticación con contraseña** para realizar operaciones desde la línea de comandos o desde la API. En su lugar, debes utilizar un **Personal Access Token** (PAT) que actúa como una contraseña para autenticarte de forma segura en GitHub.

Aquí tienes el **enlace** a la documentación de GitHub **para solucionar este error**.

Resumen en español y un paso a paso.

Aunque en las siguientes líneas encuentras un resumen y paso a paso de cómo solucionarlo, siempre es recomendable leer la documentación para habituarse a ella, además, con el paso del tiempo es posible que la actualicen y en su web siempre será un recurso más fiable.

¿Por qué ocurre el error?

GitHub eliminó el soporte para la autenticación mediante contraseña en 2021, lo cual significa que **necesitas un token de acceso personal** (PAT) para realizar acciones como ***push, pull y clone*** en **repositorios remotos** a través de HTTPS. Este cambio **mejora la seguridad**, ya que el token puede ser controlado, revocado y ajustado con permisos específicos, a diferencia de una contraseña general.

Cómo solucionar el error

OPCIÓN 1. Personal Access Token

Sigue estos pasos para crear y usar un Personal Access Token en lugar de una contraseña:

1. Generar el Personal Access Token (PAT) en GitHub:

- Accede a tu cuenta de GitHub.
- En la esquina superior derecha, haz clic en tu foto de perfil y selecciona **Settings** (Configuración).
- En el menú izquierdo, haz clic en **Developer settings** (Configuración de desarrollador).
- Selecciona **Personal access tokens** y luego:
- **Tokens (classic)** si quieres uno amplio.
- **Fine-grained tokens** para un token con permisos específicos.
- Haz clic en **Generate new token** (Generar nuevo token).
- Dale un nombre al token y elige una fecha de expiración (es recomendable que expiren por seguridad).
- En los **Scopes**, selecciona los permisos que necesitas. Para repositorios, selecciona `repo`.
- Haz clic en **Generate token**. **Copia el token** ya que **solo lo verás una vez**.

2. Configurar Git para usar el token:

- Cuando hagas ***push, pull o clone*** en el terminal con HTTPS, Git te pedirá usuario y contraseña:
- Escribe tu nombre de usuario de GitHub.
- Cuando te pida la contraseña, **introduce el Personal Access Token** en vez de tu contraseña habitual.

Ejemplo:

```
git clone https://github.com/USERNAME/REPO.git
Username: YOUR-USERNAME
Password: YOUR-PERSONAL-ACCESS-TOKEN
```

3. Almacenar el token para no introducirlo cada vez (opcional):

Para evitar introducir el token cada vez, puedes almacenar las credenciales:

- En macOS: `git credential-osxkeychain`
- En Windows: `git credential-manager-core`

Esto almacenará tu token de acceso de manera segura.

OPCIÓN 2. Alternativa: Autenticación SSH

Si prefieres **evitar los tokens de acceso personal**, puedes configurar la **autenticación SSH** en lugar de HTTPS. GitHub ofrece una guía para configurar una clave SSH y asociarla con tu cuenta de GitHub.

Siguiendo estos pasos podrás evitar el error de autenticación y realizar operaciones con GitHub sin problemas.