How to install Google authenticator on Centos/Ubuntu?

323 Manu Chacko October 31, 2024 General, Technical 28693

Install Google Authenticator on Centos/Ubuntu

Overview: This article describes how to install Google Authenticator on CentOS/Ubuntu and addresses issues related to the deprecation of the Google Image Charts API affecting QR code generation.

1. Add the EPEL repo

```
:~# yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

2. Install Google Authenticator

```
root@localhost:~ yum install google-authenticator          (Cent OS)

root@localhost:~ apt install libpam-google-authenticator    (Ubuntu)
```

3. Run the initialization app.

```
root@localhost:~ google-authenticator
```

4. After you run the command, you'll be asked a few questions.

```
Do you want authentication tokens to be time-based (y/n) y

Do you want me to update your "/root/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication token? This restricts you to one login about every 30s, but it increases your chances to notice or even prevent man-in-the-middle attacks (y/n) y


By default, a new token is generated every 30 seconds by the mobile app.
```

In order to compensate for possible time-skew between the client and the server,we allow an extra token before and after the current time. This allows for a time skew of up to 30 seconds between authentication server and client. If you experience problems with poor time synchronization, you can increase the window from its default size of 3 permitted codes (one previous code, the current code, the next code) to 17 permitted codes (the 8 previous codes, the current code, and the 8 next codes). This will permit for a time skew of up to 4 minutes between client and server.

Do you want to do so? (y/n) **y**

If the computer that you are logging into isn't hardened against brute-force login attempts, you can enable rate-limiting for the authentication module. By default, this limits attackers to no more than 3 login attempts every 30s.

Do you want to enable rate-limiting? (y/n) **y**

5. Configure openssh (SSHD)

```
:~   vi /etc/pam.d/sshd
```

Scroll down to the bottom of the file and add the following line:

```
auth required pam_google_authenticator.so
```

6. Edit the SSH configuration file.

```
root@localhost:~  vi /etc/ssh/sshd_config
```

Enable 2-factor Challenge Response Authentication:

```
ChallengeResponseAuthentication yes

#ChallengeResponseAuthentication no
```

7. Restart SSHD service

```
:~ systemctl restart sshd
```

Related Articles:

Enable Google 2fa in Ezeelogin.

Error: No 2fa configured.

Online URL: https://www.ezeelogin.com/kb/article/how-to-install-google-authenticator-on-centos-ubuntu-323.html