GOOGLE AUTHENTICATION

MFA Linux Configuration

Thomas Potgieter

Achieve more.

Disclaimer

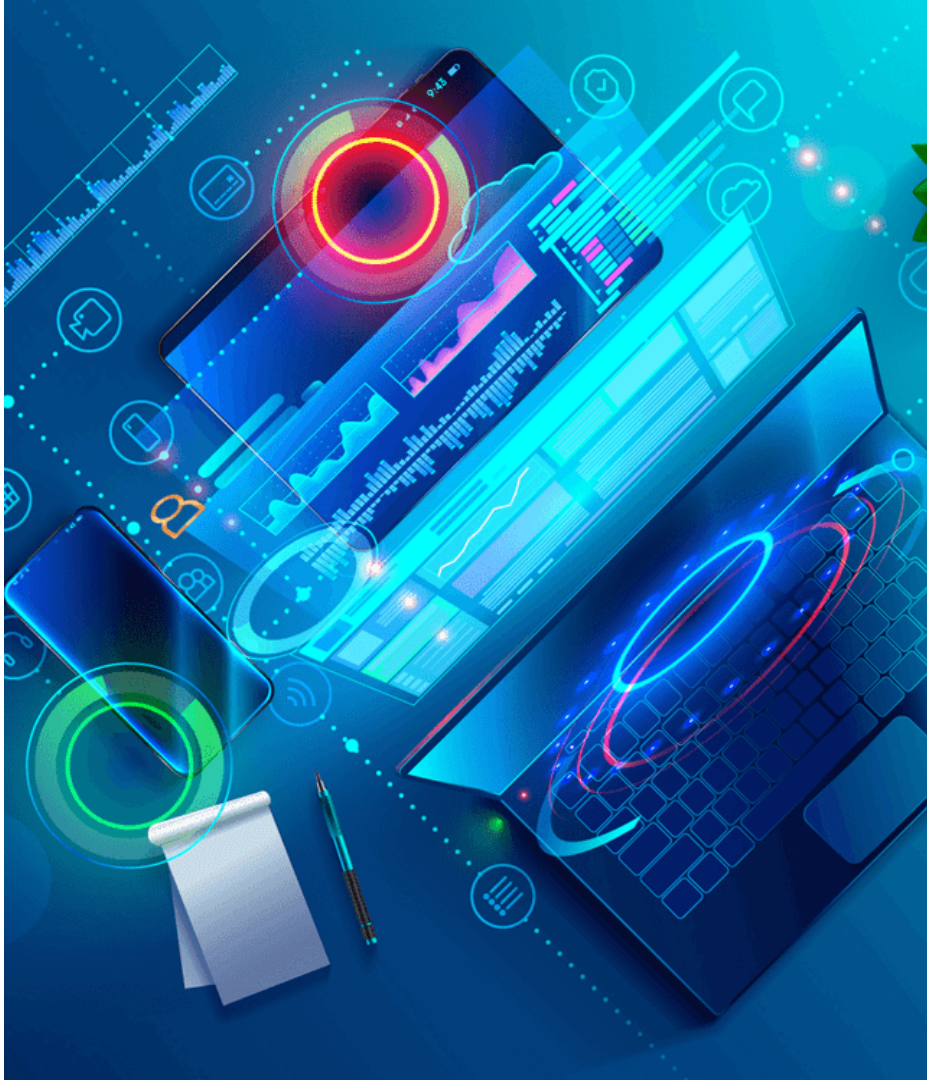
- This presentation is only a summary of some of Adapt IT's products, features and their latest developments.
- Adapt IT only intends for the information to give you an overview, and not a complete and comprehensive statement that necessarily suits your purposes.
- Adapt IT reserves the right to change any information contained in this presentation and is not responsible for any loss that results from inaccuracies in the information.
- You may not distribute or reproduce the information without Adapt IT's written permission.

© Copyright 2022 Adapt IT (Pty) Ltd. All rights reserved. www.adaptit.com

Required Software / Linux Setup

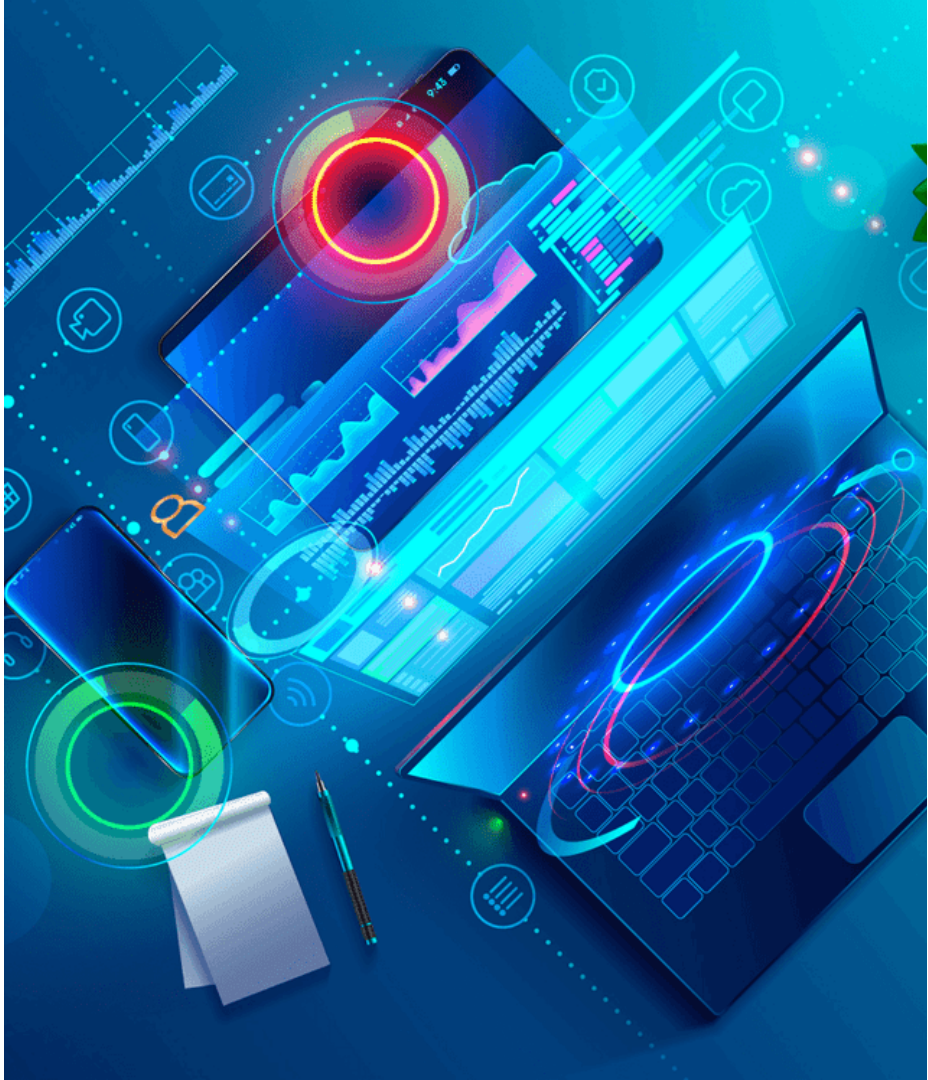
- yum install **https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm**
- yum install google-authenticator
- **vi /etc/pam.d/sshd**
- # Used with polkit to reauthorize users in remote sessions

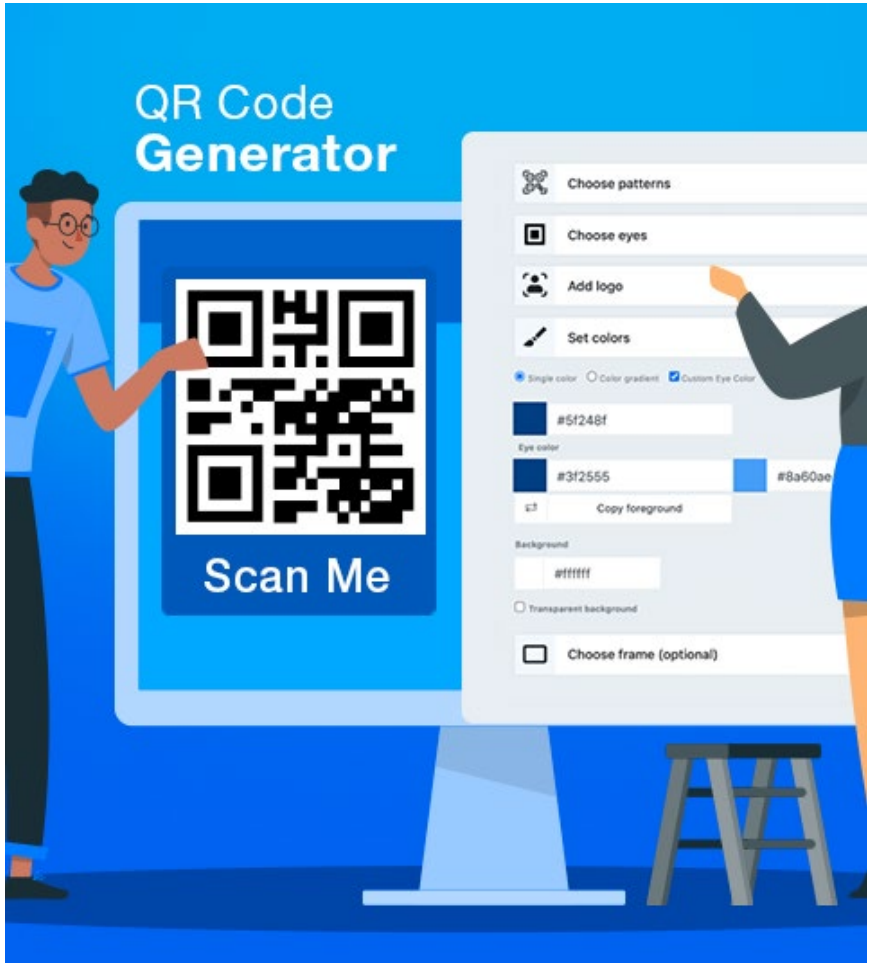
  -session optional pam_reauthorize.so prepare auth required pam_google_authenticator.so nullok



Required Software / Linux Setup

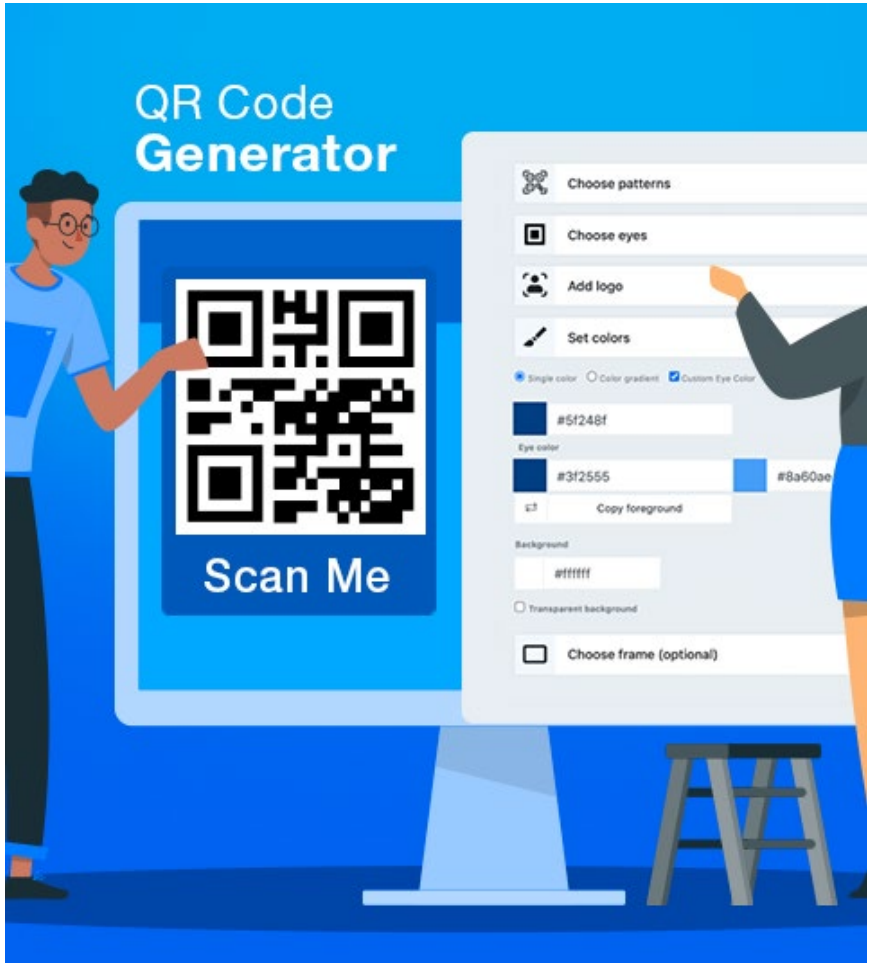
- vi /etc/ssh/sshd_config
- # Change to no to disable s/key passwords
- ChallengeResponseAuthentication yes
- #ChallengeResponseAuthentication no
- **service sshd restart**





Generate QR and Secret

- **#google-authenticator – Run this command**
- Do you want authentication tokens to be time-based (y/n) y
- Warning: pasting the following URL into your browser exposes the OTP secret to Google:
- https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/oraias@rela.adaptit.com%3Fsecret%3DVWMHHZHXI6J2HKLH5DMLKM57QIXXE%26issuer%3Drela.adaptit.com



Generate QR and Secret

- Your new secret key is: **ZZRWWBJP745HZ3OAOGNXHULAYM**
- Your verification code is: **305842**
- Your emergency scratch codes are:

  14005407

  70550776

  52549314

  78890838

  79436102

Verify Response

- **Do you want me to update your** "/oraias/app/oracle/product/.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

Verify Response

- 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

© Copyright 2022 Adapt IT (Pty) Ltd. All rights reserved. www.adaptit.com

Verify Response

- 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

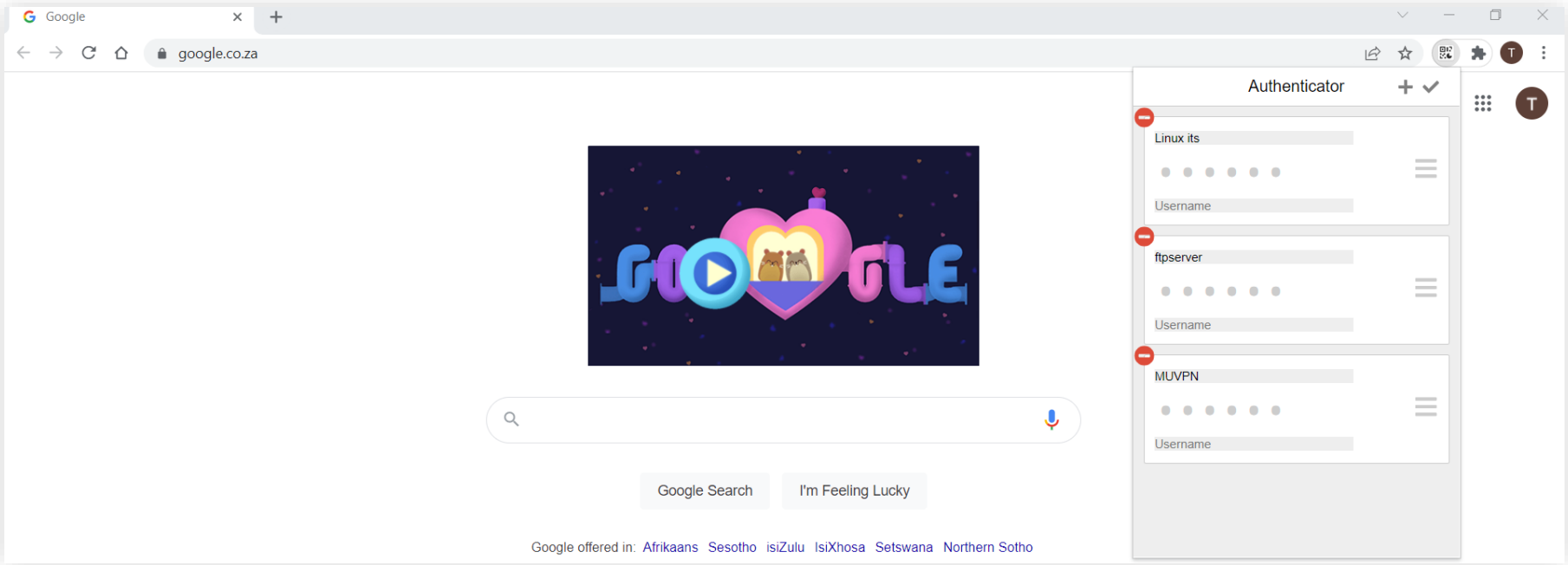
© Copyright 2022 Adapt IT (Pty) Ltd. All rights reserved. www.adaptit.com

QR Codes and Scratch Codes

- Scan the QR code with Google Authenticator OR use manual entry.
- You will need to enlarge the terminal window to scan the full QR code.
- The QR code represents a secret key, which is only known by the SSH server on which the QR code was generated.
- Once you have scanned the QR code , you will see a six-digit one-time password on your device. The password changes every 30 seconds.
- You need to enter this one-time password into the terminal to complete the Two Factor Installation process.
- Emergency scratch codes. (Five)
- Save this information to a secure place or location in case you lose access to your device.
- **Emergency scratch codes can ONLY be used ONCE.**

© Copyright 2022 Adapt IT (Pty) Ltd. All rights reserved. www.adaptit.com

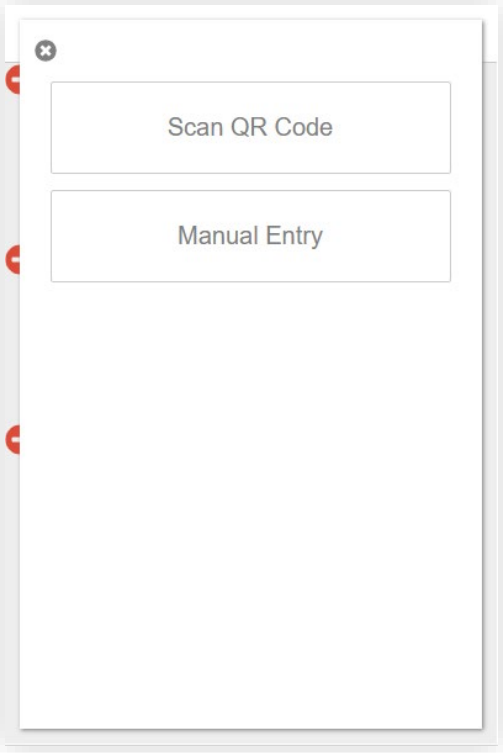
Add Server to Authenticator

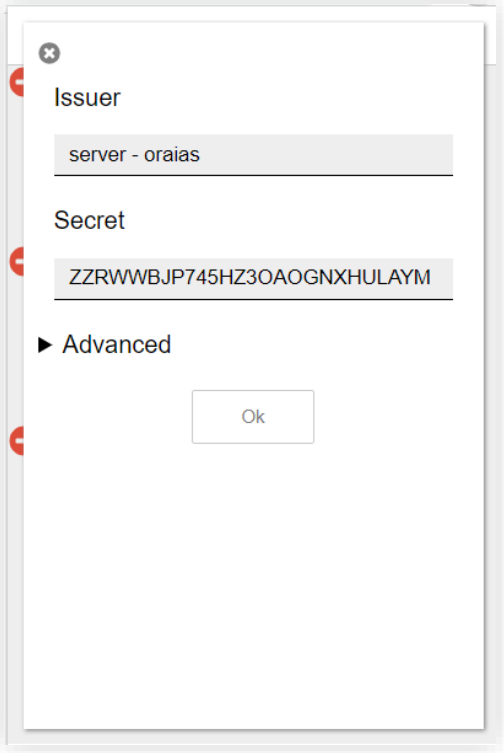


© Copyright 2022 Adapt IT (Pty) Ltd. All rights reserved. www.adaptit.com

Achieve more.

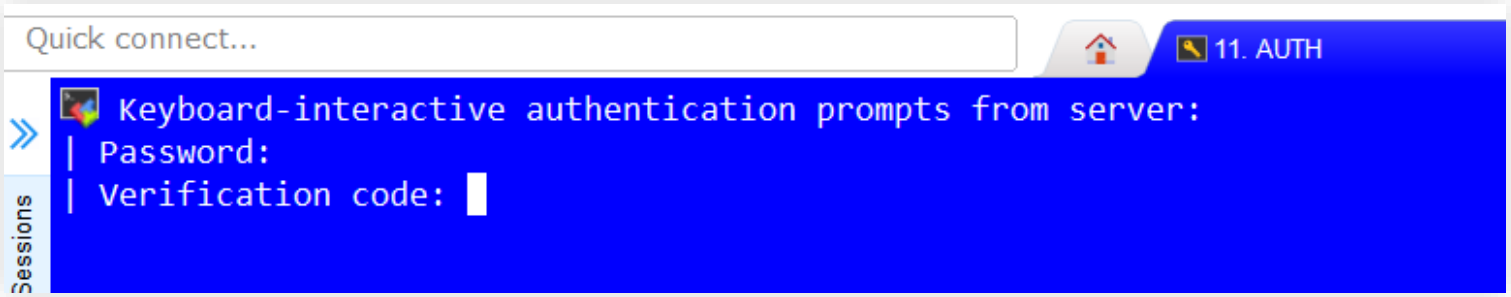
Add Server to Authenticator

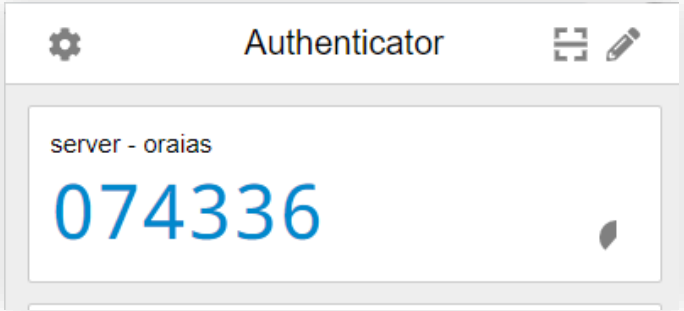




© Copyright 2022 Adapt IT (Pty) Ltd. All rights reserved. www.adaptit.com

Login





© Copyright 2022 Adapt IT (Pty) Ltd. All rights reserved. www.adaptit.com

References and to Consider

- References - www
- Multiple authenticated UNIX users or single user
- Same authentication code across multiple servers
- AD authentication only multiple users per server
- Support access from Adapt IT
- Sudo access

© Copyright 2022 Adapt IT (Pty) Ltd. All rights reserved. www.adaptit.com

QUESTIONS?

THANK YOU

Achieve more with Adapt IT