Linux SSH ?? OTP ????

??Qrencode?OATH?pam

```
apt install qrencode oathtool libpam-oath
```

??oathtool

□□□□□□□□□□□□□□□□□□□□□□□□□□□□ `HEX_SECRET`

```
export HEX_SECRET=$(head -15 /dev/urandom | sha256sum | cut -b 1-30)
```

□□□□□ OTP□□

```
oathtool --totp=SHA256 --verbose --digits=6 $HEX_SECRET
```

□□ Base32 secret□□□□ Qrencode□□□□□□□□□

```
root@ssh:~#  oathtool --totp=SHA256 --verbose --digits=6 $HEX_SECRET
Hex secret: 2180dcb885c46412345674e3aa4dba
Base32 secret: EGANZOEFYRddasdsa5STR2UTN2
Digits: 6
Window size: 0
TOTP mode: SHA256
Step size (seconds): 30
Start time: 1970-01-01 00:00:00 UTC (0)
Current time: 2025-10-07 14:56:47 UTC (1759849007)
Counter: 0x37F1B01 (58661633)

961769
```

□□ oath□□

```
touch /etc/users.oath
chmod 0600 /etc/users.oath
```

□□ oath□□

```
echo HOTP/T30 $USER - $HEX_SECRET \ >> /etc/users.oath
```

□□□□□

```
unset HEX_SECRET
```

SSH ??

□ `/etc/pam.d/sshd` □□□□

```
auth required pam_oath.so usersfile=/etc/users.oath
```

□□ `/etc/ssh/sshd_config`

```
ChallengeResponseAuthentication yes
AuthenticationMethods keyboard-interactive:pam
KbdInteractiveAuthentication yes
```

```
service ssh restart
```

??Qrencode

□□ **otp.sh□□□□**

secret□□□ Base32 secret□□

```
#!/bin/bash
secret=EGANZOEFYRddasdsa5STR2UTN2
echo $secret
qrencode -o - $(echo
otpauth://totp/test:test123?secret=${secret}&issuer=test&algorithm=SHA256&digits=6&period=30)
-o qrcode.png -t png -s 5
```

```
test:test123  □□□□
issuer □□□□□
algorithm □□□
digits OTP□□
```

```
period □□□□
```

□□ otp.sh□□□□□□ qrcode□□□□□ OTP APP□□□□

????

□□□□□□□□□ otp□□

```
root@server:~# ssh 192.168.100.100
(root@192.168.100.100) One-time password (OATH) for `root':
(root@192.168.100.100) Password:
```

Revision #2
Created 7 October 2025 22:40:51 by Jason
Updated 7 October 2025 23:37:35 by Jason