

Configurations Complement of Harden Secure Shell

1. To disabled SELINUX, Edit /etc/selinux/config, change enforcing to disabled

SELINUX=disabled

After that, restart the server

2. If you want to apply MFA only to some users, edit /etc/pam.d/sshd file and add nullok.

auth required pam_google_authenticator.so nullok

After that, restart Secure shell service

For Debian Family : systemctl restart ssh

For RedHat Family : systemctl restart sshd

3. I limited SSH connection only to members of the sshgroup, add user to group

usermod -aG sshgroup username

4. If you want to use publickey authentication method, generate sshkey on your management host and copy it to the remote server

ssh-keygen -t ed25519 -C "your_email@example.com"

ssh-copy-id username@remote_host

Edit /etc/ssh/sshd_config and change some parameters

PasswordAuthentication no

PubkeyAuthentication yes

Match Group sshgroup

 PubkeyAuthentication yes

 KbdInteractiveAuthentication yes

 AuthenticationMethods publickey keyboard-interactive

5. Restart Secure Shell service

For Debian Family : systemctl restart ssh

For RedHat Family : systemctl restart sshd

Screenshots

A simple step can stop a cyberattack before they start

By Marlyns NKUNGA, Oct. 2025

- 1) Harden Secure Shell
 - 2) Configure SSH MFA
 - 0) Exit

Enter choice [0-2]:

A simple step can stop a cyberattack before they start
By Marlyns NKUNGA, Oct. 2025

- 1) Harden Secure Shell
 - 2) Configure SSH MFA
 - 0) Exit

Enter choice [0-2]: 1

Information

You want to harden the security of Secure Shell, the Secure Shell configuration will be modified.
If you perform this script, the login behavior of the Secure Shell will be changed.
You must be sure that all SSH users are members of the sshgroup to connect via Secure Shell.
By default password authentication is used, if you want to use pubkey, read the README.md file.

Do you want to continue (y/n)? █

Do you want to continue (y/n)? y

```
[Task 1] : Gathering Operating system and Secure Shell information
[Task 2] : Creating Secure shell and SSH group variables
[Task 3] : Creating SSH Connexion group
Linux distribution redhat
[Task 4] : Updating Operating System and Installing requirement packages
[Task 5] : Hardening Secure Shell
PasswordAuthentication yes : [Pass]
[Task 6] : Restarting Secure Shell service
[Task 7] : Sucessful
```

```
Enter choice [0-2]: 2
```

Information

```
You want to configure secure shell multifactor authentication.  
Keep in mind that, this script enforce multifactor authentication by default for all users.  
You can modify this configuration, for more information read the README.md file.
```

```
Do you want to continue (y/n)? 
```

```
Do you want to continue (y/n)? y
```

```
[Task 0] : Gathering operating system and Secure Shell information
```

```
[Task 1] : Installing google-authenticator packages
```

```
Rocky distribution
```

```
[Task 2] : Checking if UsePAM yes and SELINUX is disabled
```

```
[Task 3] : Configuring Secure shell and PAM Secure Shell
```

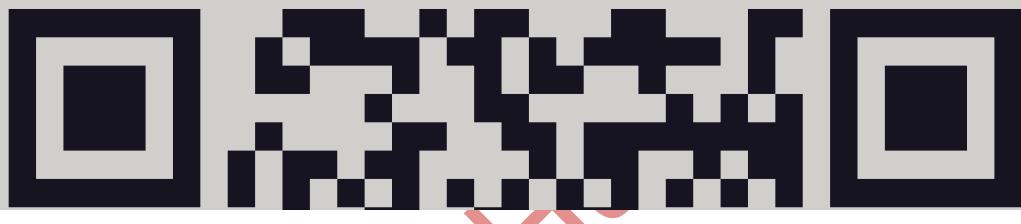
```
[Task 4] : Restarting Secure Shell Service
```

```
[Task 5] : Configuring MFA Google Authenticator
```

```
Enter username : rocky
```

```
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/rocky@lab1%3Fsec26issuer%3Dlab1
```



```
Your new secret key is: IAFVXA3Z4NYWK2VXSIYTPXWP04
```

```
Enter code from app (-1 to skip): 195356
```

```
Code confirmed
```

```
Your emergency scratch codes are:
```

```
51001842
```

```
30572356
```

```
34767809
```

```
98754997
```

```
88009633
```

```
45869342
```

```
48899242
```

```
89696365
```

```
77177153
```

```
64343365
```

```
MFA Configured for rocky
```

```
[Task 6] : Successful
```

```
Do you want to continue (y/n)? y  
[Task 0] : Gathering operating system and Secure Shell information  
[Task 1] : Installing google-authenticator packages  
Rocky distribution  
[Task 2] : Checking if UsePAM yes and SELINUX is disabled  
[Task 3] : Configuring Secure shell and PAM Secure Shell  
[Task 4] : Restarting Secure Shell Service  
[Task 5] : Configuring MFA Google Authenticator  
Enter username : secops  
User secops does not exist  
[Task 6] : Successful
```

```
:~$ ssh rocky@192.168 [REDACTED] 157  
/____|____/____|____|____\____|____|____|____|____|____|____|____|  
 \____\____|____|____|____|____|____|____|____|____|____|____|____|  
  ____|____|____|____|____|____|____|____|____|____|____|____|____|  
 |____/|____\____\____/|____\____|____/|____|____|____|____|____|  
  
Welcome to the Secure Shell, All activity is monitored and recorded.  
If you are not an authorized person, please log out immediately.  
Unauthorized access will be investigated and punished according of the law.  
  
(rocky@192.168 [REDACTED] 157) Password:  
(rocky@192.168 [REDACTED] 157) Verification code:  
Last failed login: Sat Nov  1 07:47:45 CET 2025 from 192.168 [REDACTED] 186 on ssh:notty  
There was 1 failed login attempt since the last successful login.  
[rocky@lab1 ~]$ █
```