

Duo Installation and Configuration in Linux environment

1. Installation of pam_duo PAM module to protect SSH

Duo can be easily added to any Linux system to protect remote (SSH) with the addition of a simple pam_duo PAM module.

1.1. Install pam_duo

Create /etc/yum.repos.d/duosecurity.repo with the following contents:

```
[duosecurity]
name=Duo Security Repository
baseurl=http://pkg.duosecurity.com/CentOS/$releasever/$basearch
enabled=1
gpgcheck=1
```

Execute the following shell commands:

```
# rpm --import https://duo.com/DUO-GPG-PUBLIC-KEY.asc
# yum install duo_unix
```

Note that the aforementioned GPG key verifies the Duo Unix package only for currently supported OS distributions and versions. If you are running Duo Unix on a distribution that Duo no longer supports, the GPG signatures on these packages will fail to verify.

1.2. Configuration

Once duo_unix is installed, edit /etc/duo/pam_duo.conf to add the **integration key**, **secret key**, and **API hostname**. Please ask Duo administrator for the 3 keys.

```
[duo]
; Duo integration key
ikey = INTEGRATION_KEY
; Duo secret key
skey = SECRET_KEY
; Duo API hostname
host = API_HOSTNAME
prompts = 1
groups = users
```

Remember to put all the users that want to use Duo in the group “users” by updating /etc/group.

1.2.1. SSH Configuration

Update /etc/ssh/sshd_config as follow:

```
ChallengeResponseAuthentication yes
```

1.2.2. PAM Configuration

You’ll need to modify your system’s PAM configuration to include a line like the following:

```
auth required pam_duo.so
```

For example on CentOS 7, to enable Duo for ssh, update /etc/pam.d/sshd as:

Before:

```
##%PAM-1.0
auth    required  pam_sepermit.so
auth    substack  password-auth
auth    include   postlogin
```

After:

```
##%PAM-1.0
auth    required  pam_duo.so
auth    required  pam_sepermit.so
auth    substack  password-auth
auth    include   postlogin
```

2. Login with Duo 2FA

Ssh to the server to login:

```
Login as: xxxxxxxx
Using keyboard-interactive authentication.
Duo two-factor login for yyyyyy

Enter a passcode or select one of the following options:
1. Duo Push to iOS

Passcode or option (1-1):
```

Can then enter 1. for a Duo push to the device enrolled before, or enter the passcode, or enter the bypass code if applied.

3. Notes

Remember user must be enrolled before ssh to the server.

Users must put in group "users" to use Duo, the group can be specified in the pam_duo.conf file as above.

Reference: <https://duo.com/docs/duounix> (Please note the example in this reference link will configure the server to use Duo as the only authentication method, which is not recommended for Linux server, you should configured as the above to use both password and Duo for Two Factor Authentication.)