

Application Note

How to use PAM with Idem Key on Linux

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, contact support@GoTrustID.com.

Date Aug-4-2022



1. Introduction

FIDO is already natively supported by many operating systems, such as Windows, macOS, Linux, iOS, and Android. PAM (Pluggable Authentication Module) is a basic library on Linux for authenticating users. To use Idem Key for PAM, you need to install additional FIDO U2F PAM libraries. This document describes the steps to install and configure on Ubuntu. These steps should also apply to other Linux distributions.

Note that this configuration does not apply to SSH.

2. Install FIDO U2F PAM

Open terminal and run command:

```
sudo apt-get install libpam-u2f
```

```
jeff@jeff-VirtualBox:~$ sudo apt-get install libpam-u2f
[sudo] password for jeff:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfwupdplugin1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libhidapi-hidraw0 libu2f-host0 libu2f-server0 pamu2fcfg
The following NEW packages will be installed:
  libhidapi-hidraw0 libpam-u2f libu2f-host0 libu2f-server0 pamu2fcfg
0 upgraded, 5 newly installed, 0 to remove and 13 not upgraded.
Need to get 81.0 kB of archives.
After this operation, 269 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://tw.archive.ubuntu.com/ubuntu focal/universe amd64 libhidapi-hidraw0
amd64 0.9.0+dfsg-1 [10.7 kB]
Get:2 http://tw.archive.ubuntu.com/ubuntu focal/universe amd64 libu2f-host0 amd6
4 1.1.10-1 [21.6 kB]
Get:3 http://tw.archive.ubuntu.com/ubuntu focal/universe amd64 libu2f-server0 am
```

3. Create U2F Mapping File

Step 1: Run command to create mapping file

```
pamu2fcfg > ~/u2f-keys
```

```
jeff@jeff-VirtualBox:~$ pamu2fcfg > ~/u2f-keys
No U2F device available, please insert one now, you have 3 seconds
```

Step 2: Insert Idem Key and touch it when key is flashing. The mapping file “u2f-keys” will be created in current Home folder and the Idem Key is associated to current user.

Step 3: Create folder “GoTrust” under “/etc”

```
sudo mkdir -p /etc/GoTrust
```

Step 4: For security consideration, suggest moving mapping file “u2f-keys” to “/etc/GoTrust”

```
sudo mv ~/u2f-keys /etc/GoTrust/u2f-keys
```

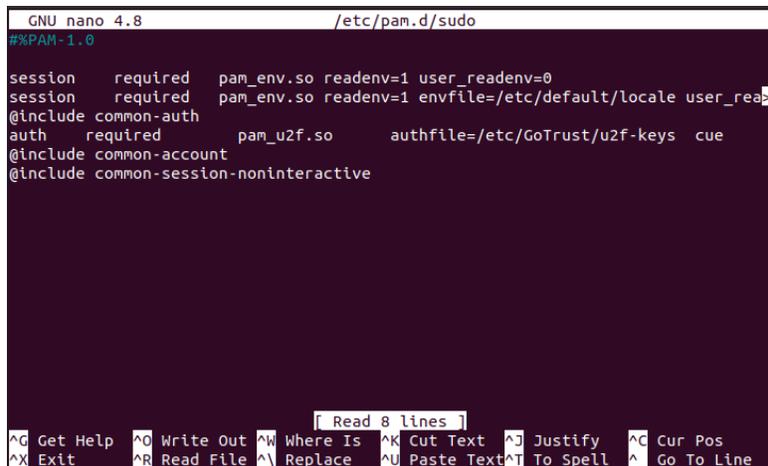
4. Enable Idem Key as 2FA for sudo

Step 1: Edit PAM configuration of sudo

```
sudo nano /etc/pam.d/sudo
```

Step 2: Add new content under the line of “@include common-auth”

```
auth required pam_u2f.so authfile=/etc/GoTrust/u2f-keys
```



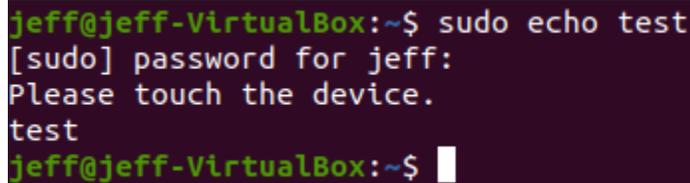
```
GNU nano 4.8 /etc/pam.d/sudo
#%PAM-1.0
session required pam_env.so readenv=1 user_readenv=0
session required pam_env.so readenv=1 envfile=/etc/default/locale user_rea>
@include common-auth
auth required pam_u2f.so authfile=/etc/GoTrust/u2f-keys cue
@include common-account
@include common-session-noninteractive

[ Read 8 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

Step 3: Open a new terminal and run test command. When prompted, enter your password and press Enter.

```
sudo echo test
```

Step 4: Insert Idem Key and touch metal area when flashing. If you can see the echo text “test” after touching Idem Key, it means the setting is successfully configured.



```
jeff@jeff-VirtualBox:~$ sudo echo test
[sudo] password for jeff:
Please touch the device.
test
jeff@jeff-VirtualBox:~$
```

Please keep original terminal of editing PAM sudo configuration on. When this sudo setting is failed, you can still use the terminal to recover the configuration by deleting the newly added configuration.

5. Enable Idem Key as 2FA for Linux login

Step 1: Edit PAM configuration of sudo

- If your system is Ubuntu 17.10 or newer, run:

```
sudo nano /etc/pam.d/gdm-password
```

- If your system is Ubuntu 17.04 or older, run:

```
sudo nano /etc/pam.d/lightdm
```

Step 2: Add new content under the line of “@include comman-auth”

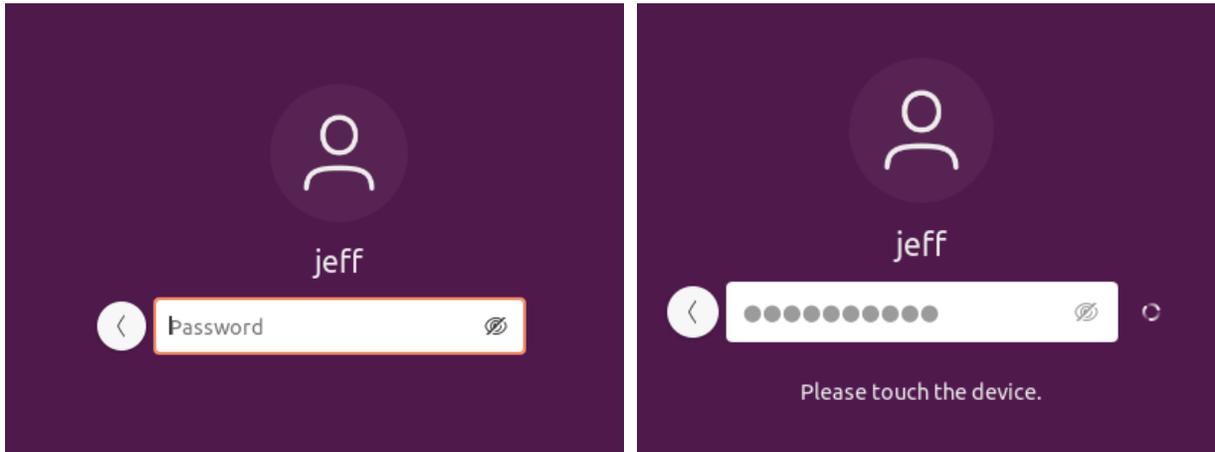
```
auth required pam_u2f.so authfile=/etc/GoTrust/u2f-keys cue
```

```

GNU nano 4.8 /etc/pam.d/gdm-password Modified
#%PAM-1.0
auth requisite pam_nologin.so
auth required pam_succeed_if.so user != root quiet_success
@include common-auth
auth required pam_u2f.so authfile=/etc/GoTrust/u2f-keys cue
auth optional pam_gnome_keyring.so
@include common-account
# SELinux needs to be the first session rule. This ensures that any
# lingering context has been cleared. Without this it is possible
# that a module could execute code in the wrong domain.
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam
session required pam_loginuid.so
# SELinux needs to intervene at login time to ensure that the process
# starts in the proper default security context. Only sessions which are
# intended to run in the user's context should be run after this.
# pam_selinux.so changes the SELinux context of the used TTY and configures
# SELinux in order to transition to the user context with the next execve()
# call.
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam
session optional pam_keyinit.so force revoke

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
  
```

Step 3: Logout Linux and login again. Enter password, insert Idem Key, and touch metal area when flashing.



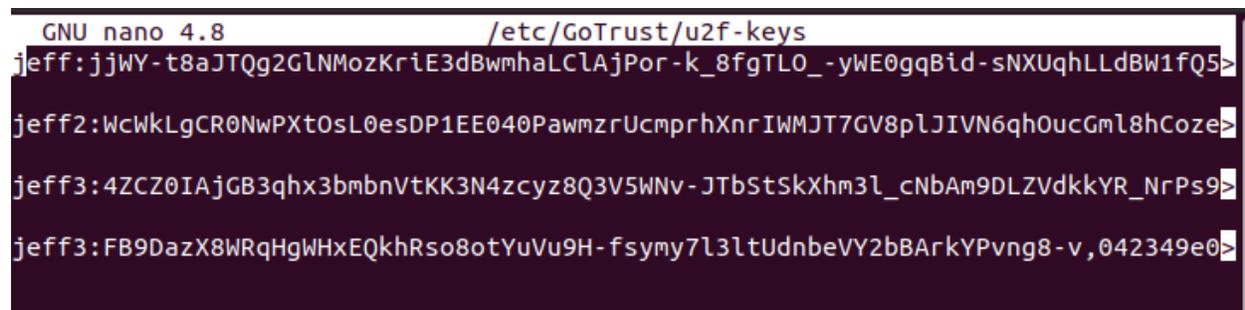
6. Configuration for multiple users and Idem Keys

Configure more users:

Run u2f configuration command. Replace username as real login account. If “u2f-keys” is already moved to /etc/GoTrust folder, change the path by your own case.

```
pamu2fcfg -u username > ~/u2f-keys  
echo -e “\n” >> ~/u2f-keys
```

After the configurations for more users, you can see the mapping file like this



```
GNU nano 4.8 /etc/GoTrust/u2f-keys  
jeff:jjWY-t8aJTQg2GlnMozKriE3dBwmhaLClAjPor-k_8fgTLO_-yWE0gqBid-sNXUqhLLdBW1fQ5>  
jeff2:WcWkLgCR0NwPXt0sL0esDP1EE040PawmzrUcmprhXnrIWMJT7GV8pLJIVN6qhOucGml8hCoze>  
jeff3:4ZCZ0IAjGB3qhx3bmbnVtKK3N4zcyz8Q3V5WNv-JTbStSkXhm3l_cNbAm9DLZVdkkYR_NrPs9>  
jeff3:FB9DazX8WRqHgWHxEQkhRso8otYuVu9H-fsymy7l3ltUdnbeVY2bBArkYPvng8-v,042349e0>
```

The format will be like this:

```
jeff:something1,something2  
jeff1:something3,something4  
jeff2:something5,something6
```

Configure one user with multiple keys:

Run configuration command with same user name multiple times with different Idem Key.

```
pamu2fcfg -u jeff > ~/u2f-keys  
echo -e “\n” >> ~/u2f-keys  
pamu2fcfg -u jeff > ~/u2f-keys  
echo -e “\n” >> ~/u2f-keys
```

You will then get the mapping file “u2f-keys” like this:

```
jeff:something1,something2  
jeff:something3,something4
```

Modify mapping file manually to this format.

```
jeff:something1,something2:something3,something4
```

Now, you can use user name “jeff” to login with 2 different Idem Keys.

Configure multiple users with single Idem Key:

Modify mapping file manually by this format

```
jeff:something1,something2  
jeff1:something1,something2  
jeff2:something1,something2
```

Now, you can use jeff, jeff1, or jeff2 to login with same Idem Key.