



PBS INSTALLATION GUIDE FOR LINUX OPERATING SYSTEM

Version 1.1

Introduction

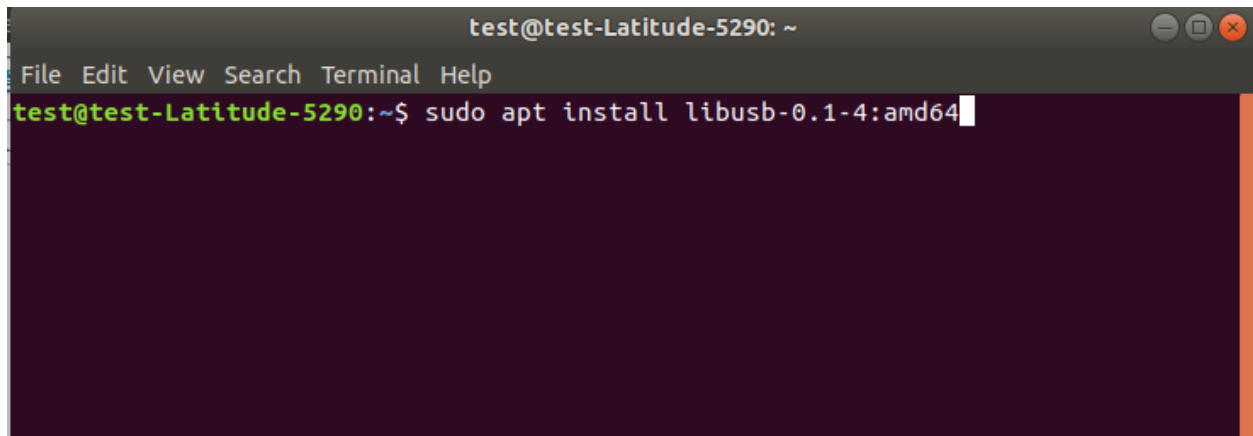
This document outlines the installation of PBS on Ubuntu Linux NMRS systems. The steps are designed for Ubuntu desktop versions 16.04 and 18.04

Requirements and Dependencies

- Ubuntu Desktop 1604/ 1804
- Oracle java JRE 1.8
- Standard USB libraries
- Text Editors
- Sudo User account
- Existing and functional OpenNMRS Installation.

Step 1. Install standard USB library packages

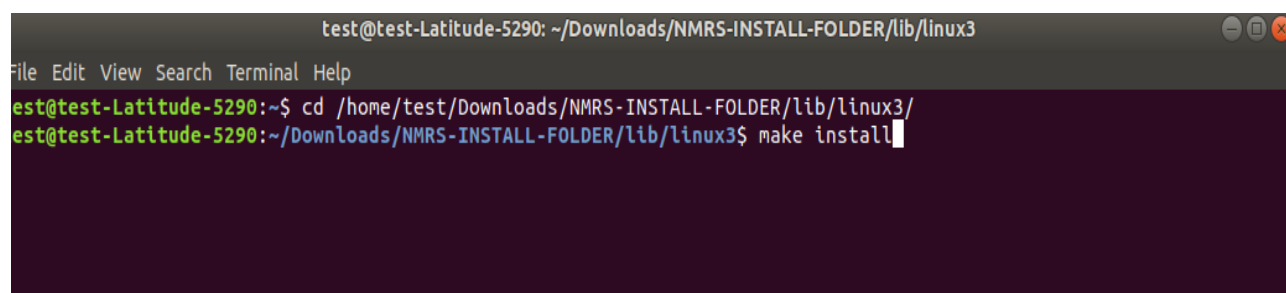
Procedure	Command
Install the following packages <ul style="list-style-type: none">• libgtk2.0-dev• libusb-0.1-4:amd64	<ul style="list-style-type: none">• <code>sudo apt install libgtk2.0-dev</code>• <code>sudo apt install libusb-0.1-4:amd64</code>

A screenshot of a terminal window titled 'test@test-Latitude-5290: ~'. The terminal has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The prompt is 'test@test-Latitude-5290:~\$' and the command 'sudo apt install libusb-0.1-4:amd64' is entered, followed by a cursor. The terminal background is dark purple, and the command text is green and white. The window has standard Ubuntu window controls (minimize, maximize, close) in the top right corner.

```
test@test-Latitude-5290: ~
File Edit View Search Terminal Help
test@test-Latitude-5290:~$ sudo apt install libusb-0.1-4:amd64
```

Step 2. Install the Securegen USB Drivers

Procedure	Command
<ul style="list-style-type: none">• Navigate to path installation path• <code><Install Path>/lib/linux3</code>	<ul style="list-style-type: none">• <code>cd /home/test/Downloads/NMRS-INSTALL-FOLDER/lib/linux3/</code>
<ul style="list-style-type: none">• Install the Secugen driver	<ul style="list-style-type: none">• <code>make install</code>



```
test@test-Latitude-5290: ~/Downloads/NMRS-INSTALL-FOLDER/lib/linux3
File Edit View Search Terminal Help
est@test-Latitude-5290:~$ cd /home/test/Downloads/NMRS-INSTALL-FOLDER/lib/linux3/
est@test-Latitude-5290:~/Downloads/NMRS-INSTALL-FOLDER/lib/linux3$ make install
```

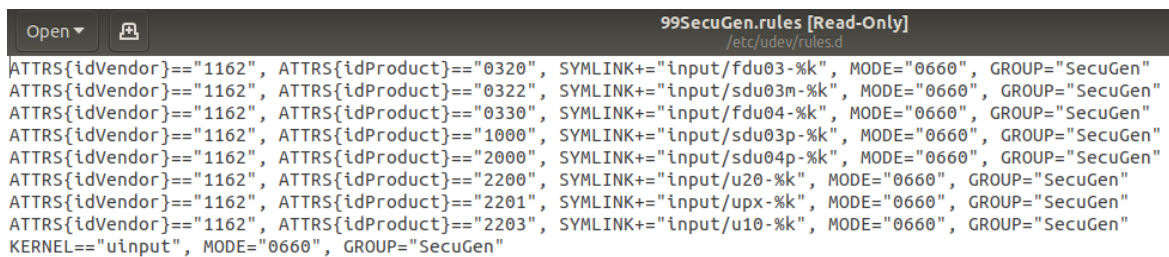
Step 3. Set USB device permissions


By default, only the root user can access the SecuGen USB device because the device requires write permissions, to allow non-root users to use the device, perform the following steps:

Procedure	Command
<ul style="list-style-type: none">• Create a SecuGen Group	<ul style="list-style-type: none">• <code>sudo groupadd SecuGen</code>
<ul style="list-style-type: none">• Add fingerprint users to the SecuGen group (substitute user name for myUserID)	<ul style="list-style-type: none">• <code>sudo gpasswd -a myUserID SecuGen</code>
<ul style="list-style-type: none">• Create a file <code>99SecuGen.rules</code> in <code>etc /udev/rules.d/</code>	<ul style="list-style-type: none">• <code>cd /etc/udev/rules.d/</code>• <code>touch 99SecuGen.rules</code>

- Open the file **99SecuGen.rules** and add the following lines:

```
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="0320",
SYMLINK+="input/fdu03-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="0322",
SYMLINK+="input/sdu03m-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="0330",
SYMLINK+="input/fdu04-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="1000",
SYMLINK+="input/sdu03p-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="2000",
SYMLINK+="input/sdu04p-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="2200",
SYMLINK+="input/u20-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="2201",
SYMLINK+="input/upx-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="2203",
SYMLINK+="input/u10-%k", MODE="0660", GROUP="SecuGen"
KERNEL=="uinput", MODE="0660", GROUP="SecuGen"
```



```
Open ▾  99SecuGen.rules [Read-Only]
/etc/udev/rules.d
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="0320", SYMLINK+="input/fdu03-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="0322", SYMLINK+="input/sdu03m-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="0330", SYMLINK+="input/fdu04-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="1000", SYMLINK+="input/sdu03p-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="2000", SYMLINK+="input/sdu04p-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="2200", SYMLINK+="input/u20-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="2201", SYMLINK+="input/upx-%k", MODE="0660", GROUP="SecuGen"
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="2203", SYMLINK+="input/u10-%k", MODE="0660", GROUP="SecuGen"
KERNEL=="uinput", MODE="0660", GROUP="SecuGen"
```

- Reboot System

Step 4. Driver Library Configuration

- Driver Library Configuration for java applications libjnisgfplib.so supports only one class of SecuGen device at a time.

The default configuration is for the SecuGen UPx device.

Procedure	Commands
<ul style="list-style-type: none">• Configuration for Hamster Plus	<ul style="list-style-type: none">• <code>cd <install_dir>/lib/linux3</code>• <code>sudo cp libjnisgfplib.so.3.8.5.fdu03_rename libjnisgfplib.so.3.8.5</code>• <code>make uninstall install</code>
<ul style="list-style-type: none">• Configuration for Hamster IV	<ul style="list-style-type: none">• <code>cd <install_dir>/lib/linux3</code>• <code>sudo cp libjnisgfplib.so.3.8.5.fdu04_rename libjnisgfplib.so.3.8.5</code>• <code>make uninstall install</code>
<ul style="list-style-type: none">• Configuration for Hamster PRO 20	<ul style="list-style-type: none">• <code>cd <install_dir>/lib/linux3</code>• <code>sudo cp libjnisgfplib.so.3.8.5.fdu05_rename libjnisgfplib.so.3.8.5</code>• <code>make uninstall install</code>
<ul style="list-style-type: none">• Configuration for Hamster PRO	<ul style="list-style-type: none">• <code>cd <install_dir>/lib/linux3</code>• <code>sudo cp libjnisgfplib.so.3.8.5.fdu06_rename_default libjnisgfplib.so.3.8.5</code>• <code>make uninstall install</code>

- Run the following commands:

```
sudo cp libsgfdu07.so.1.0.0 /usr/lib
sudo cp libsgfdu06.so.1.0.0 /usr/lib
sudo cp libsgfdu05.so.1.0.2 /usr/lib
sudo cp libsgfdu04.so.1.0.4 /usr/lib
sudo cp libsgfdu03.so.2.0.7 /usr/lib
sudo cp libsgfplib.so.3.8.5 /usr/lib
sudo cp libsgfpamx.so.3.5.2 /usr/lib
sudo cp libjnisgfplib.so.3.8.5 /usr/lib
sudo cp libpysgfplib.so.1.0.1 /usr/lib
sudo cp libsgnfiq.so.1.0.0 /usr/lib
sudo cp libsgimage.so.1.0.0 /usr/lib
sudo cp libnxsdk.so /usr/lib
sudo cp sgfdu05mlp.dat /usr/lib
sudo /sbin/ldconfig /usr/lib
```

Step 5. Configure permissions for Biometric app

Procedure	Commands
<ul style="list-style-type: none"> • Set permissions for biometric app <u>Note:</u> <i>"myUserID" is the User account at logon. In the command, myUserID should be replaced with the correct account name.</i> 	<ul style="list-style-type: none"> • copy nmrs-deploy folder to /opt • sudo groupadd -r biometricapp • sudo useradd -r -s /bin/false -g biometricapp myUserID • sudo chown -R myUserId:biometricapp /opt/nmrs-deploy/

- Edit the nmrs-biometric.service and change the user the current user account (account at logon)

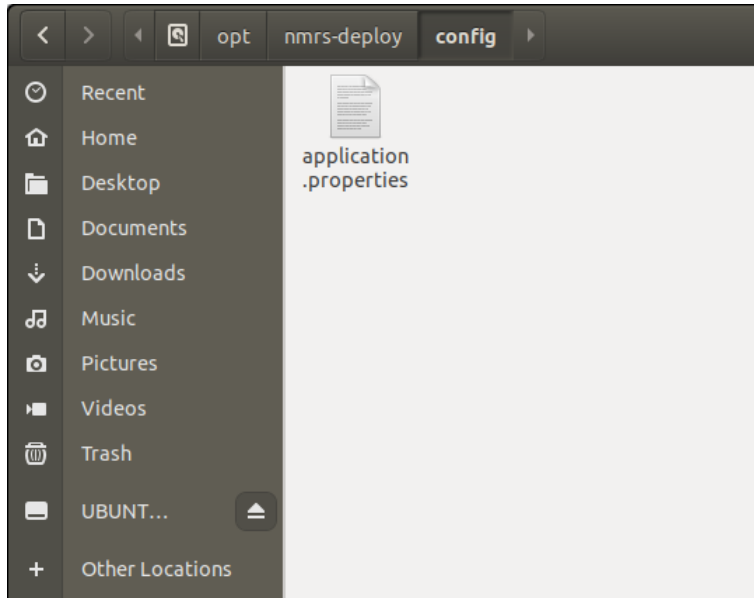
```
[Unit]
Description=NMRS Biometric Linux Service
After=nmrslog.target

[Service]
WorkingDirectory=/opt/nmrs-deploy
ExecStart=/bin/bash -c "java -jar nmrs-biometric.jar"
User=test
Type=simple
Restart=on-failure
RestartSec=10

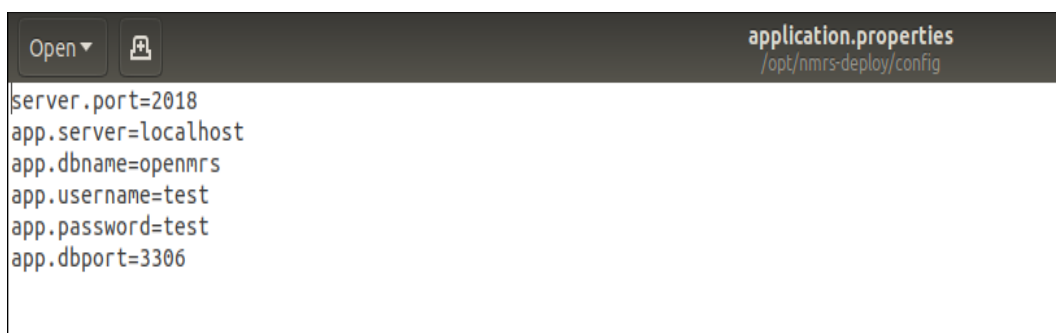
[Install]
WantedBy=multi-user.target
```

Step 6. Set up the Biometric Service

- Copy the nmrs-biometric.service file to /etc/systemd/system
- Run `sudo systemctl daemon-reload`.
- Navigate to /opt/nmrs-deploy/config.



- Configure the `application.properties` file.



- Run `sudo systemctl enable nmrs-biometric.service` to enable service at startup.
- Reboot System

Step 7. Initialize the device

- Connect the Fingerprint scanner device
- Check status of the biometric service
Run `sudo systemctl status nmrs-biometric.service`
- Confirm service above is running.
- Proceed to scan Clients' Fingerprints in NMRS

Step 8. Extras

Cockpit makes it easy to administer your GNU/Linux servers via a web browser. NMRS biometric service restart and other service actions are available on Cockpit. The steps below will get cockpit running

- Install cockpit by running `sudo apt-get install cockpit`
- Access cockpit on the web browser via `localhost:9090`
- Provide system user account and password
- Check "reuse my password" and click on login
- Navigate to services, locate and click on NMRS Biometric Linux Service
- Click on the drop-down menu to select desired service actions. (restart, stop, disable, start)

Notes

- Fingerprint scanner device must be unplugged during setup.
- Switching USB ports will require biometric service restart.
- Avoid switching USB ports when fingerprint capture is in progress.
- Apply lotion/water on dry fingers, clean wet fingers to effective fingerprint capture.
- Ensure that fingerprint capture devices are firmly connected to USB ports.