**Introduction**

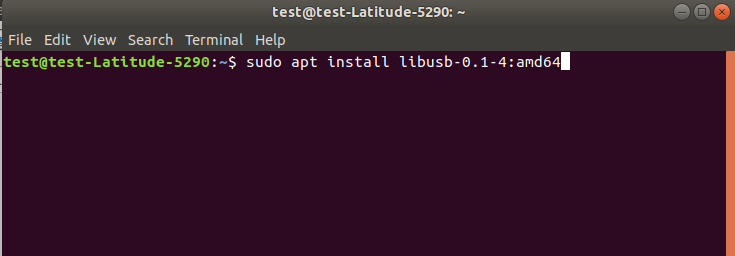
This document outlines the installation of PBS on Ubuntu Linux NMRS systems. The steps are designed for Ubuntu desktop versions 16.04 and 18.04

**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.

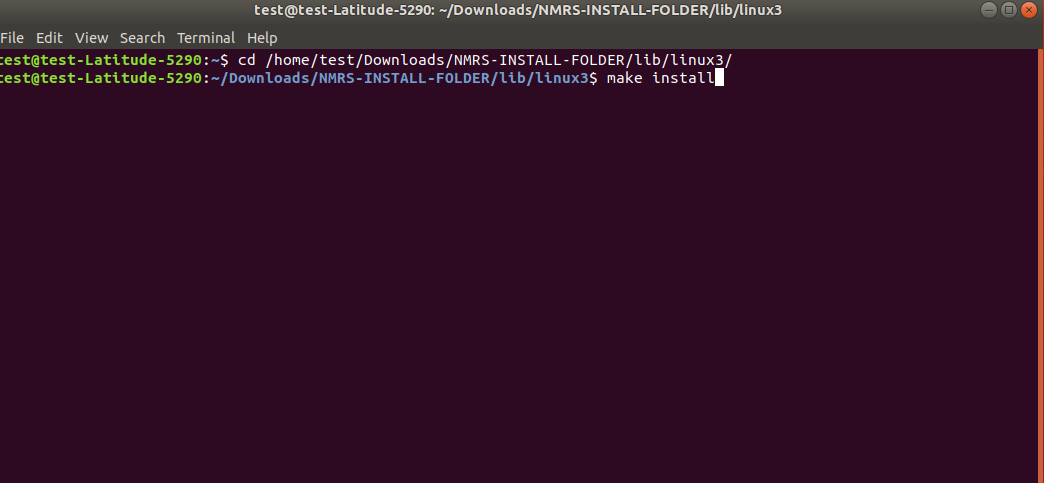
**Step 1. Install standard USB library packages**

|  |  |
| --- | --- |
| Procedure | Command |
| Install the following packages   * libgtk2.0-dev * libusb-0.1-4:amd64 | * sudo apt install libgtk2.0-dev * sudo apt install libusb-0.1-4:amd64 |



**Step 2. Install the Securegen USB Drivers**

|  |  |
| --- | --- |
| Procedure | Command |
| * Navigate to path installation path * <Install Path>/lib/linux3 | * cd /home/test/Downloads/NMRS-INSTALL-FOLDER/lib/linux3/ |
| * Install the Secugen driver | * 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 |
| * Create a SecuGen Group | * sudo groupadd SecuGen |
| * Add fingerprint users to the SecuGen group (substitute user name for myUserID) | * sudo gpasswd -a myUserID SecuGen |
| * Create a file 99SecuGen.rules in   etc /udev/rules.d/ | * cd /etc/udev/rules.d/ * touch 99SecuGen.rules |
|  | |

* 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"

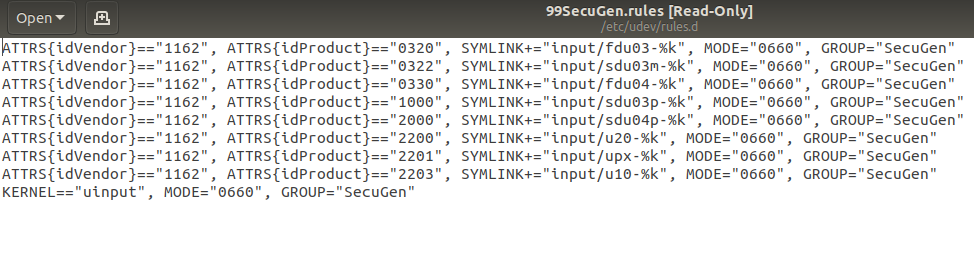
ATTRS{idVendor}=="1162", ATTRS{idProduct}=="2000", SYMLINK+="input/sdu04p-%k", MODE="0660", GROUP="SecuGen"

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"



* 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 |
| * Configuration for Hamster Plus | * cd <install\_dir>/lib/linux3 * sudo cp libjnisgfplib.so.3.8.5.fdu03\_rename libjnisgfplib.so.3.8.5 * make uninstall install |
| * Configuration for Hamster IV | * cd <install\_dir>/lib/linux3 * sudo cp libjnisgfplib.so.3.8.5.fdu04\_rename libjnisgfplib.so.3.8.5 * make uninstall install |
| * Configuration for Hamster PRO 20 | * cd <install\_dir>/lib/linux3 * sudo cp libjnisgfplib.so.3.8.5.fdu05\_rename libjnisgfplib.so.3.8.5 * make uninstall install |
| * Configuration for Hamster PRO | * cd <install\_dir>/lib/linux3 * sudo cp libjnisgfplib.so.3.8.5.fdu06\_rename\_default libjnisgfplib.so.3.8.5 * make uninstall install |

* 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

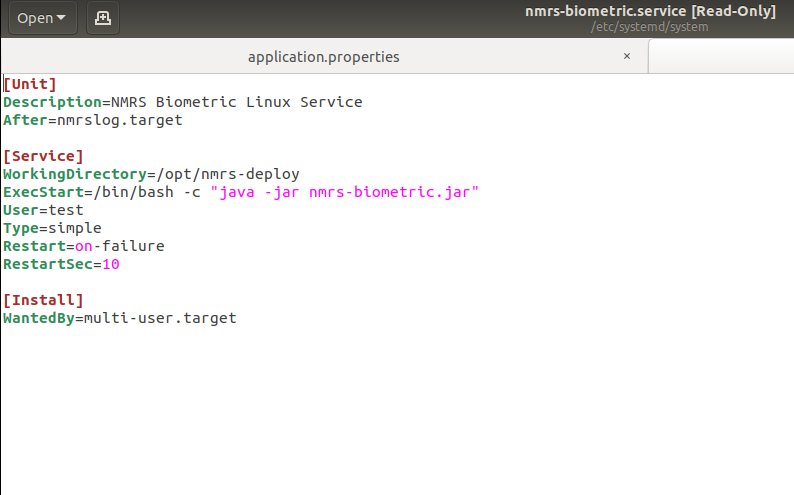
sudo cp sgfdu05mlp.dat /usr/lib

sudo /sbin/ldconfig /usr/lib

**Step 5. Configure permissions for Biometric app**

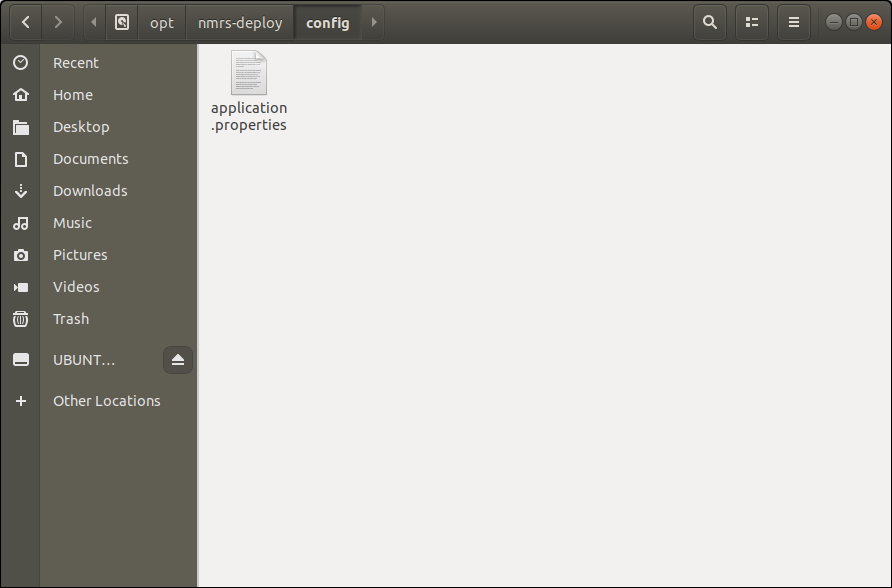
|  |  |
| --- | --- |
| Procedure | Commands |
| * Set permissions for biometric app   Note:  “myUserID” *is the User account at logon. In the command,* myUserID *should be replaced with the correct account name.* | * copy nmrs-deploy folder to /opt * sudo groupadd -r biometricapp * sudo useradd -r -s /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)

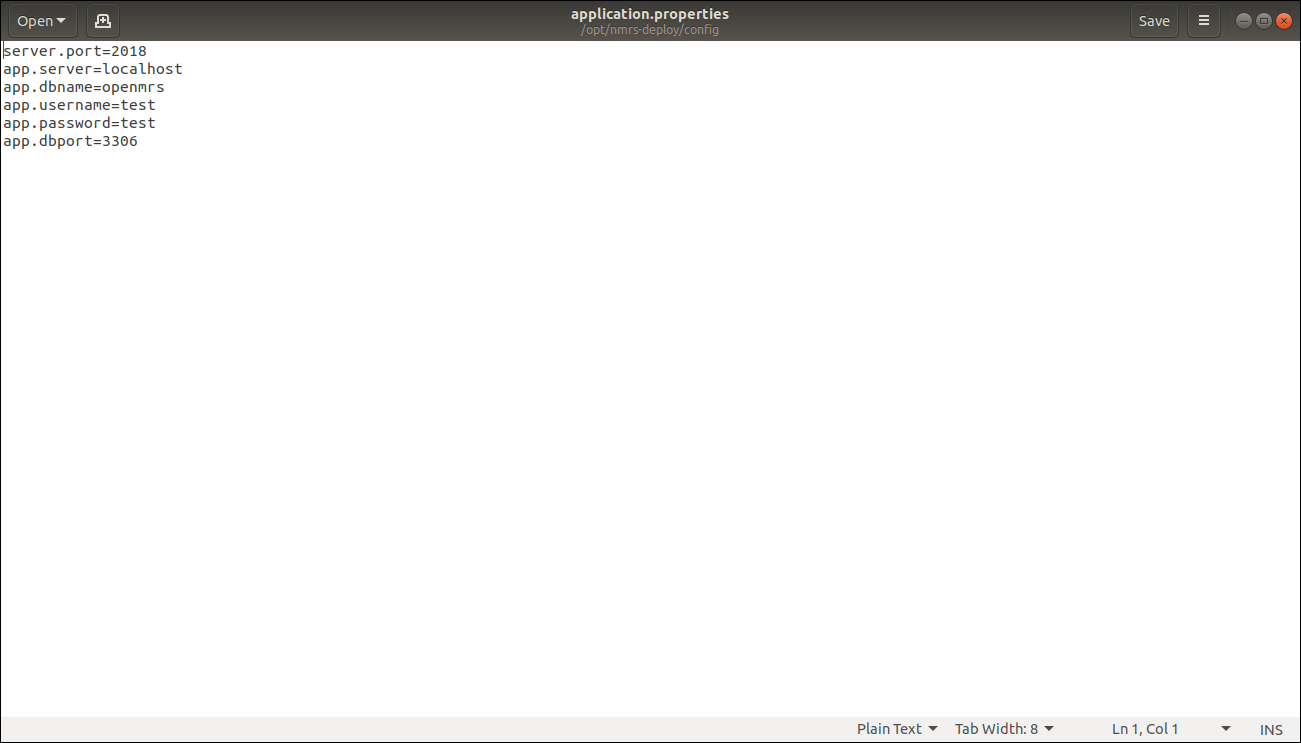


**Step 6. Set up the Biometric Service**

* 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.