

EETI Android SELinux Config Guide

TABLE OF CONTENTS

TABLE OF CONTENTS.....	0
SELinux Permission Setting.	1

All information provided in this document is for reference only and is tested on Android 7. User shall modify the contents based on the operating system and its environment.

SELinux Permission Setting.

1. Define the SELinux type

Add the string in the “/device/manufacturer/device-name/sepolicy/file.te”

```
type eGalax_data_file, file_type, data_file_type, mltrustedobject;
```

2. Bind file for eGTouchD Service:

Add the string in the “Android/device/manufacturer/device-name/sepolicy/file_contexts”

```
/system/bin/eGTouchD u:object_r:eGTouchD_exec:s0
```

```
/data/eGalax(/.*)? u:object_r:eGalax_data_file:s0
```

3. Add eGTouchD permission:

Add the file “Android/device/manufacturer/device-name/sepolicy/eGTouchD.te

```
# File types must be defined for file_contexts.

type eGTouchD, domain;

type eGTouchD_exec, exec_type, file_type;

init_daemon_domain(eGTouchD)

##

allow eGTouchD shell_exec:file { open read execute getattr execute_no_trans };

allow eGTouchD eGalax_data_file:dir { open read write add_name remove_name search };

allow eGTouchD eGalax_data_file:file { open read write getattr unlink create ioctl };

allow eGTouchD eGalax_data_file:fifo_file { open read write getattr create setattr };

allow eGTouchD toolbox_exec:file { open read execute getattr execute_no_trans };

allow eGTouchD proc:file { open read getattr };

allow eGTouchD sysfs:dir { open read };

allow eGTouchD sysfs:file { open read write getattr };

allow eGTouchD sysfs:lnk_file { getattr };

allow eGTouchD rootfs:lnk_file { getattr };

allow eGTouchD device:chr_file { open read write ioctl };

allow eGTouchD uhid_device:chr_file { open read write ioctl };

allow eGTouchD input_device:dir { open read search };

allow eGTouchD input_device:chr_file { getattr setattr };

allow eGTouchD eGTouchD:capability { dac_override fsetid dac_read_search };

allow eGTouchD system_file:file { execute_no_trans };

allow eGTouchD perfprofd:process { signull };

allow eGTouchD eGTouchD:capability { kill };
```

4. Add Exceptions permission rules:

After adding these permissions, errors may occur during compilation.

This may be due to the conflict between some neverallow rules such as eGTouchD.te and domain.te

You may need to add some exceptions to the rules of:

AndroidSource/system/sepolicy/domain.te”

```
# Don't allow raw read/write/open access to generic devices.
# Rather force a relabel to a more specific type.
# init is exempt from this as there are character devices that only it uses.
# ueventd is exempt from this, as it is managing these devices.
neverallow { domain -init -ueventd eGTouchD } device:chr_file { open read write };
```

```
# Only system_app and system_server should be creating or writing
# their files. The proper way to share files is to setup
# type transitions to a more specific type or assigning a type
# to its parent directory via a file_contexts entry.
# Example type transition:
# mydomain.te:file_type_auto_trans(mydomain, system_data_file, new_file_type)
#
neverallow {
    domain
    -shell
    -usbmuxd
    -system_server
    -system_app
    -init
    -installld # for relabelfrom and unlink, check for this in explicit neverallow
    -eGTouchD
} system_data_file:file no_w_file_perms;
```

5. Add EETI Android APK Tool permission:

Add the string in the “Android/device/manufacturer/device-name/sepolicy/eGTouchD.te”

```
allow untrusted_app eGalax_data_file:fifo_file { open read write };
```

```
allow untrusted_app eGalax_data_file:dir { open read write search };
```