# AppArmor

## What is AppArmor?

AppArmor is MAC style security extension for the Linux kernel. It implements a task centered policy, with task "profiles" being created and loaded from user space. Tasks on the system that do not have a profile defined for them run in an unconfined state which is equivalent to standard Linux DAC permissions.

## How to enable/disable

set `CONFIG_SECURITY_APPARMOR=y`

If AppArmor should be selected as the default security module then set:

```
CONFIG_DEFAULT_SECURITY="apparmor"
CONFIG_SECURITY_APPARMOR_BOOTPARAM_VALUE=1
```

Build the kernel

If AppArmor is not the default security module it can be enabled by passing `security=apparmor` on the kernel's command line.

If AppArmor is the default security module it can be disabled by passing `apparmor=0, security=XXXX` (where `XXXX` is valid security module), on the kernel's command line.

For AppArmor to enforce any restrictions beyond standard Linux DAC permissions policy must be loaded into the kernel from user space (see the Documentation and tools links).

## Documentation

Documentation can be found on the wiki, linked below.

## Links

Mailing List - apparmor@lists.ubuntu.com

Wiki - http://wiki.apparmor.net

User space tools - https://gitlab.com/apparmor

Kernel module - git://git.kernel.org/pub/scm/linux/kernel/git/jj/linux-apparmor