

com.apple.driver.AppleBCMWLANCore performJoin apple80211 assoc candidates

"[ik] %s@%d:%s: Disable roaming when joining an RSN\_AKM\_PSK network in lockdown mode\n"

com.apple.driver.AppleCredentialManager

unsigned char const unsigned int

```
kernel_thread_start enable_lockdown_mode disable_lockdown_mode

performCommandGated
```

commandProcessedGated acm command t const unsigned long





## com.apple.driver.AppleLockdownMode

bool AppleLockdownMode::start(IOService \*a1, IOService \*a2)

```
start
if
  IOLog "LockdownMode: started (no-op)\n"
else
  IOLog "LockdownMode: failed to start"
return
```





## How Bad Is It?

## not that bad

In the KEXT com.apple.driver.AppleLockdownMode

```
bool AppleLockdownMode::start(IOService *a1, IOService *a2)
{
    v2 = IOService::start(a1, a2);
    if ( v2 )
        IOLog("LockdownMode: started (no-op)\n");
    else
        IOLog("LockdownMode: failed to start");
    return v2;
}
```

Appears to be a no-op for now

In the KEXT com.apple.driver.AppleCredentialManager

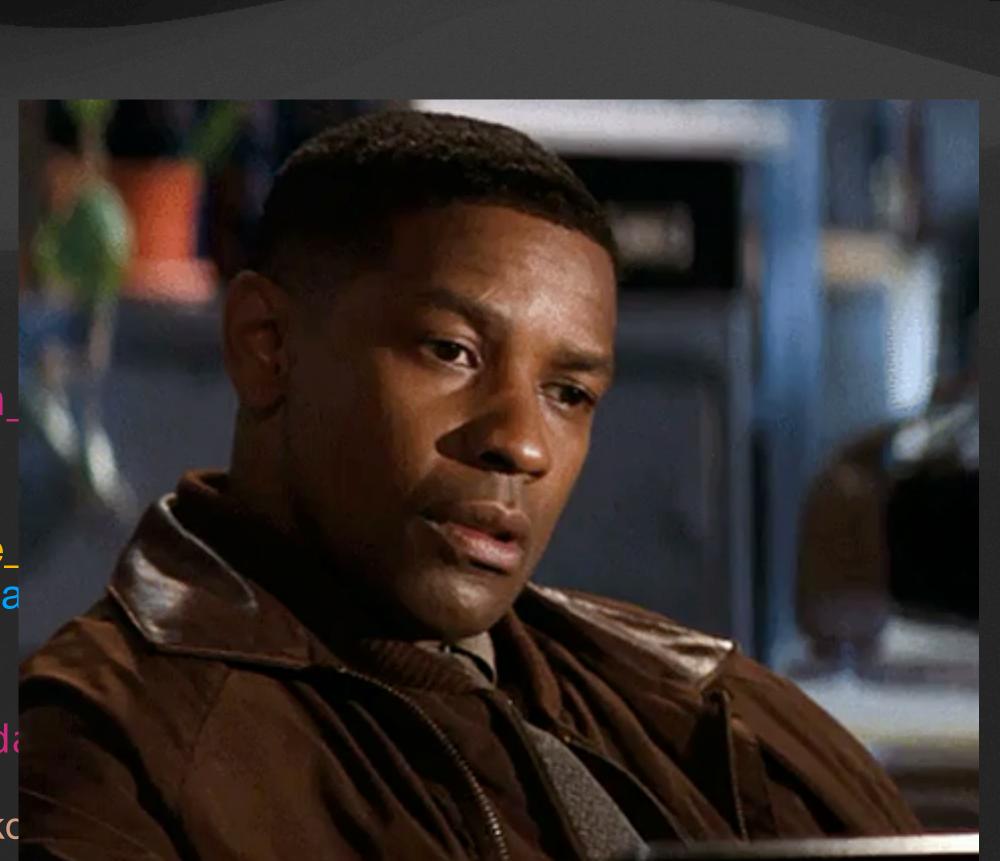
ACMLockdownModeKernelService::commandProcessedGated(acm\_unsigned char const\*, unsigned int)

This function calls via kernel\_thread\_start enable\_lockdown\_mode or disable\_input struct and is called from AppleCredentialManager::performCommandGa

In the KEXT com.apple.driver.AppleBCMWLANCore

AppleBCMWLANJoinAdapter::performJoin(apple80211\_assoc\_candidate)

"[ik] %s@%d:%s: Disable roaming when joining an RSN\_AKM\_PSK network in lockc



## ... for now