Practical MacAdmin

Andrew Laurence
University of California, Irvine

Practical MacAdmin

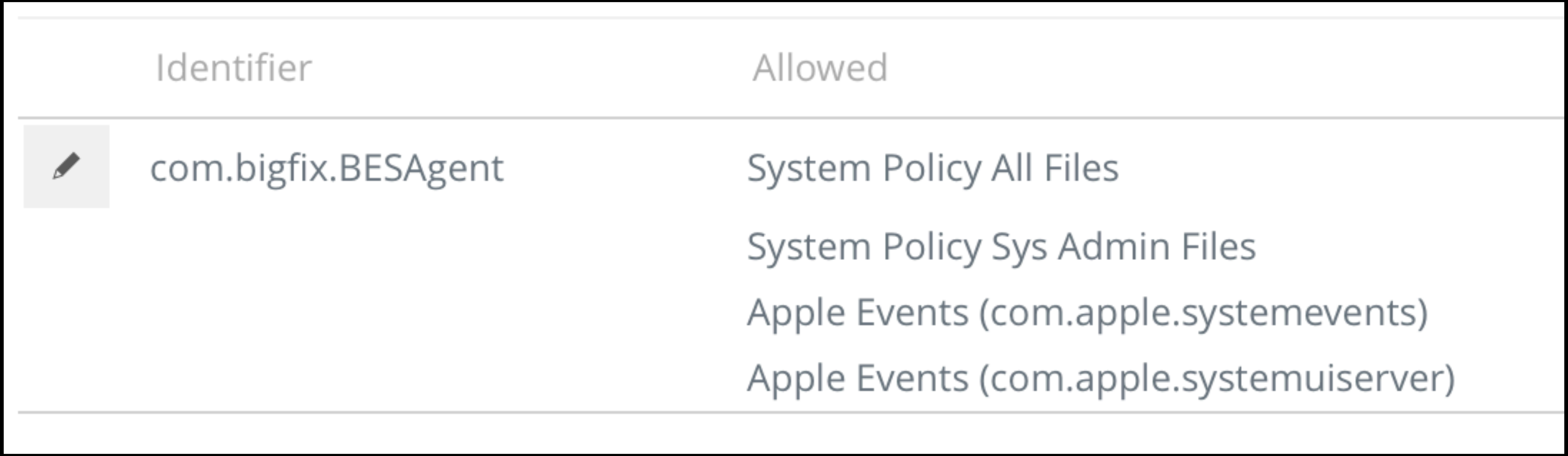
- BigFix runs as root.

- System Integrity Protection
- root isn’t root anymore.

Practical MacAdmin

- Modern MacAdmin requires an MDM system.

- BigFix is not an MDM system.
  - User-Authenticated MDM
  - KEXT whitelisting
  - PPPC payloads



	Identifier	Allowed
✎	com.bigfix.BESAgent	System Policy All Files System Policy Sys Admin Files Apple Events (com.apple.systemevents) Apple Events (com.apple.systemuiserver)

Practical MacAdmin

- Inspector platform parity

  - local group
  - dhcp enabled of network adapter
  - user of process

BigFix: Zoom Remediation

- **RELEVANCE (all must be true)**

```
mac of operating system

exists application ("Zoom.us.app" of "/Applications")

not exists file "/Library/Preferences/us.zoom.config.plist"
  whose (string "ZDisableVideo" of dictionary of it is "1")
```

- **ACTION SCRIPT**

```
wait sudo defaults write /Library/Preferences/us.zoom.config.plist
ZDisableVideo 1
```

BigFix: Zoom 4.4.53932.0709

- **RELEVANCE (all must be true)**

```
mac of operating system

exists application ("Zoom.us.app" of folder "/Applications")
  whose (version of it as string as version < "4.4.53932.0709" )
```

BigFix: Zoom 4.4.53932.0709

- **ACTION SCRIPT (1)**

```
begin prefetch block
 parameter "theURL" = "https://LOCALOBFUSCATED/zoom/zoom.pkg"
 parameter "theSHA" = "21243f5e6bc6921a316ec193c5d5cdec837475c1"
 parameter "theSize" = "11223483"
 parameter "pkgfile" = "{concatenation "_" of (substrings separated
 by "%2520" of (following text of last "/" of parameter "theURL"))}"

 add prefetch item name={parameter "pkgfile"} sha1={parameter
 "theSHA"} size={parameter "theSize"} URL={parameter "theURL"}
  collect prefetch items
end prefetch block
```

BigFix: Zoom 4.4.53932.0709

- **ACTION SCRIPT (2)**

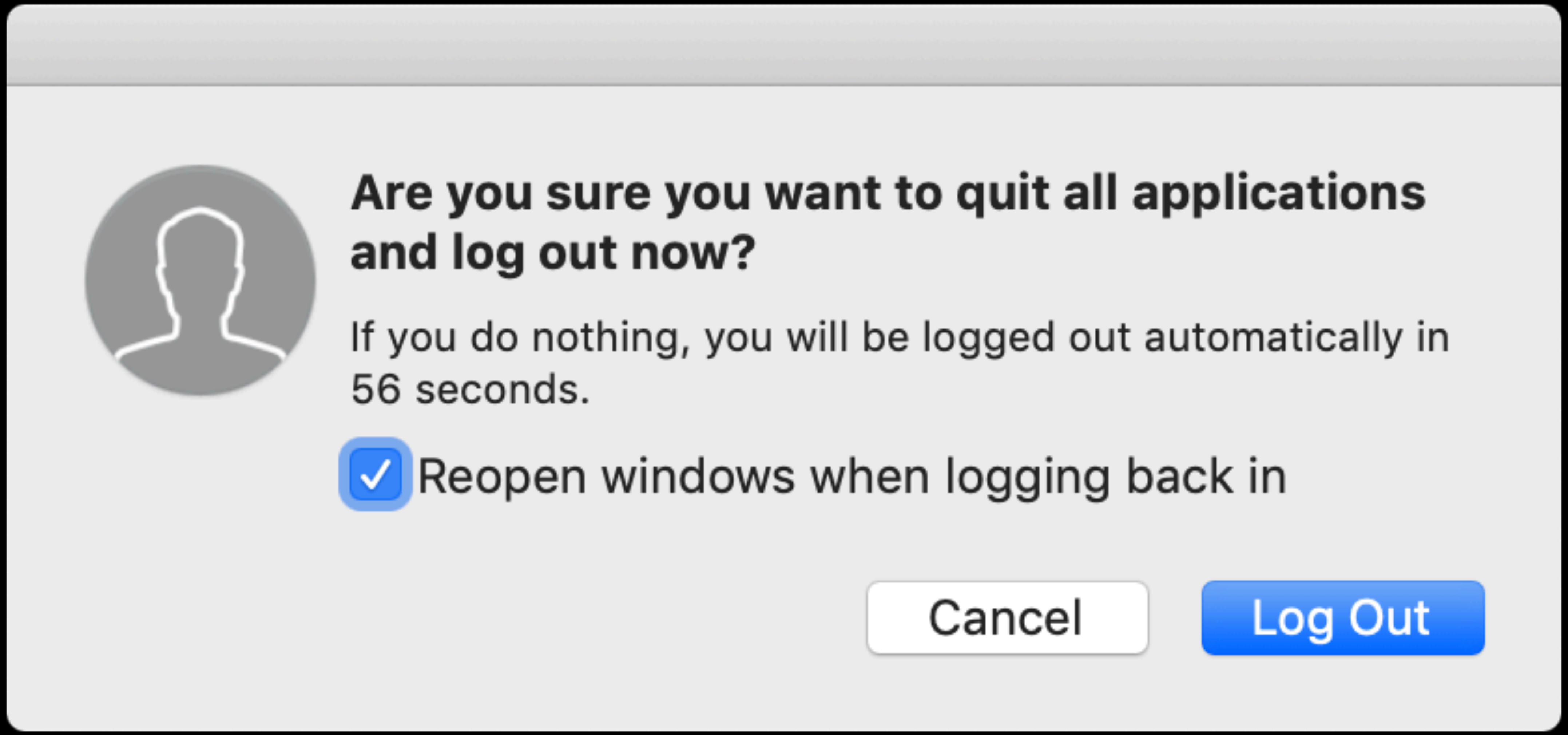
```
wait sudo -i /usr/sbin/installer -package "{download folder}/{parameter "pkgfile"}" -target /
```

BigFix: Log out console user

```
delete __createfile
delete “/tmp/ascript.scpt"
createfile until EOF
#!/usr/bin/osascript
tell application "System Events"
log out
end tell
EOF
move __createfile "/tmp/ascript.scpt"
wait chmod +x "/tmp/ascript.scpt"

parameter "theScript" = "/tmp/ascript.scpt"
parameter "theUser" = "{id of user of current user as string}"

wait launchctl asuser {parameter "theUser"} {parameter "theScript"}
```



Are you sure you want to quit all applications and log out now?

If you do nothing, you will be logged out automatically in 56 seconds.

☑ Reopen windows when logging back in

```
startosinstall
```

@atlauren

atlauren@uci.edu