

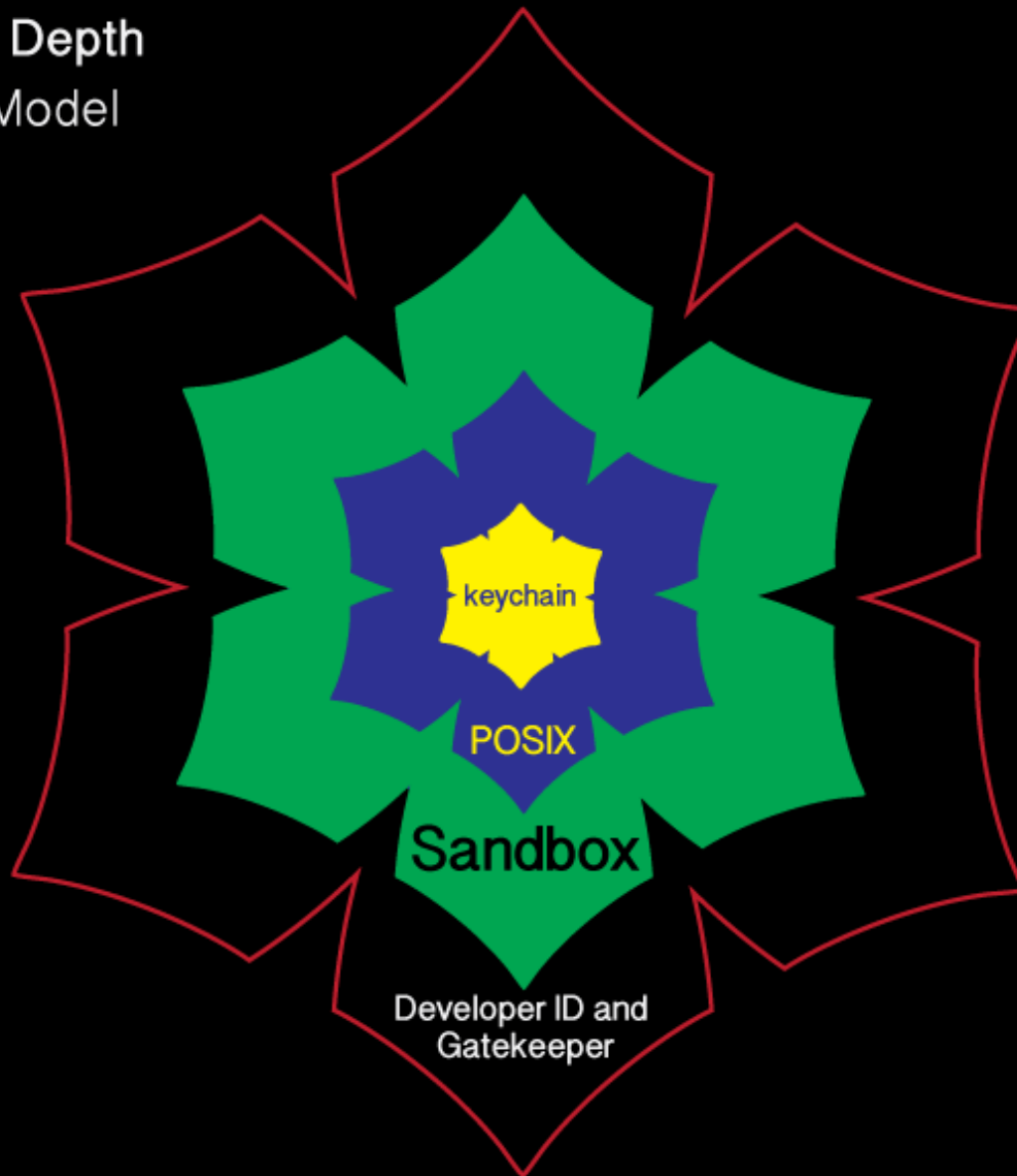
OS X Security: Defense in Depth

Rich Trouton

Howard Hughes Medical Institute,
Janelia Research Campus

Defense in Depth

The OS X Model



Developer ID and Gatekeeper



Developer ID and Gatekeeper

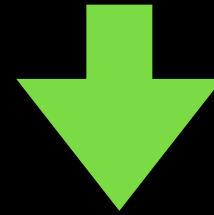
Allow apps downloaded from:

- ☒ Mac App Store
- ☐ Mac App Store and identified developers
- ☐ Anywhere



Allow apps downloaded from:

- ☐ Mac App Store
- ☒ Mac App Store and identified developers
- ☐ Anywhere



"Hello World" can't be opened because it is from an unidentified developer.

Your security preferences allow installation of only apps from the Mac App Store.

Safari downloaded this file today at 11:54 AM from dl.dropboxusercontent.com.



OK



"Hello World" can't be opened because it is from an unidentified developer.

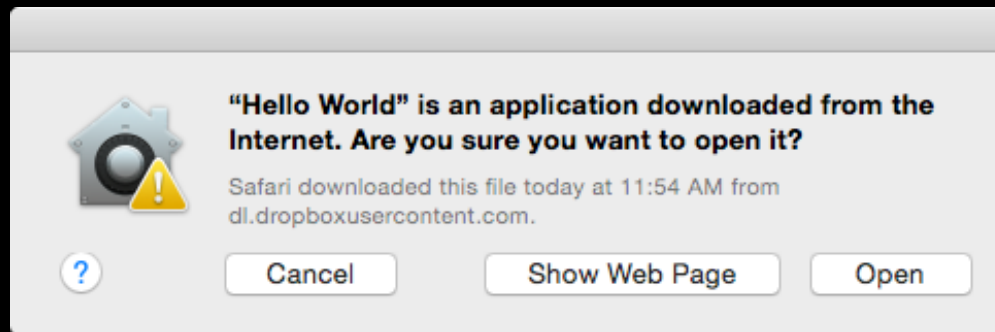
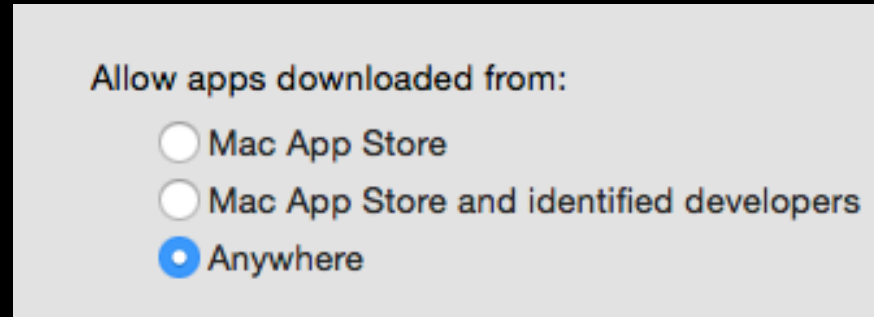
Your security preferences allow installation of only apps from the Mac App Store and identified developers.

Safari downloaded this file today at 11:54 AM from dl.dropboxusercontent.com.

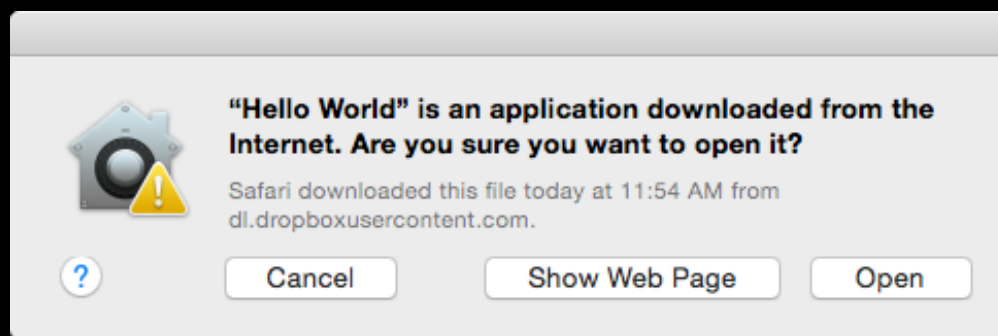
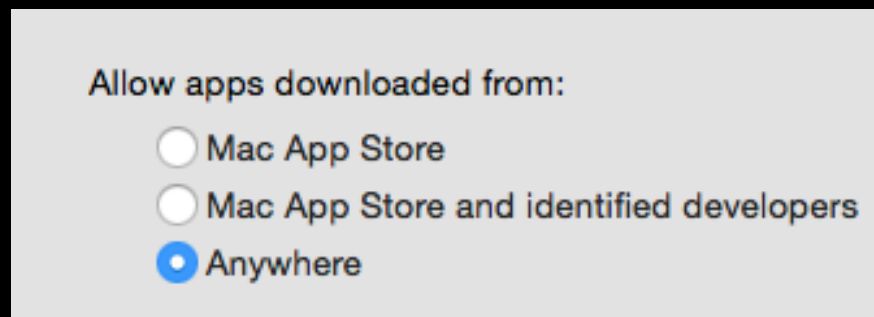


OK

Developer ID and Gatekeeper



File Quarantine and XProtect



File Quarantine and XProtect



**“hello_world.jar” will damage your computer.
You should move it to the Trash.**

It contains the “OSX.OpinionSpy” malware.

Safari downloaded this file today at 3:44 PM from
dl.dropboxusercontent.com.

☒ Report malware to Apple to protect other users



Cancel

Move to Trash

Developer ID and Gatekeeper

```
void doRearmCheck()
{
    // check global preference
    CFRef<CFBooleanRef> rearmPref = (CFBooleanRef)CFPreferencesCopyValue(CFSTR("GKAutoRearm"), CFSTR("com.apple.security"), kCFPreferencesAnyUser, kCFPreferencesCurrentHost);
    if (rearmPref == kCFBooleanFalse)
        return;

    CFBooleanRef status;
    CTimeInterval delta;
    if (SecAssessmentControl(CFSTR("ui-status"), &status, NULL) && status == kCFBooleanFalse)
        if (SecAssessmentControl(CFSTR("rearm-status"), &delta, NULL) && delta > rearmPeriod) {
            SecAssessmentControl(CFSTR("ui-enable"), NULL, NULL); // enable assessments
            SecAssessmentControl(CFSTR("ui-enable-devid"), NULL, NULL); // allow Developer ID
            notify_post("com.apple.security.assessment.rearm");
        }
}
```

<http://tinyurl.com/gkrearm>

Sandboxing

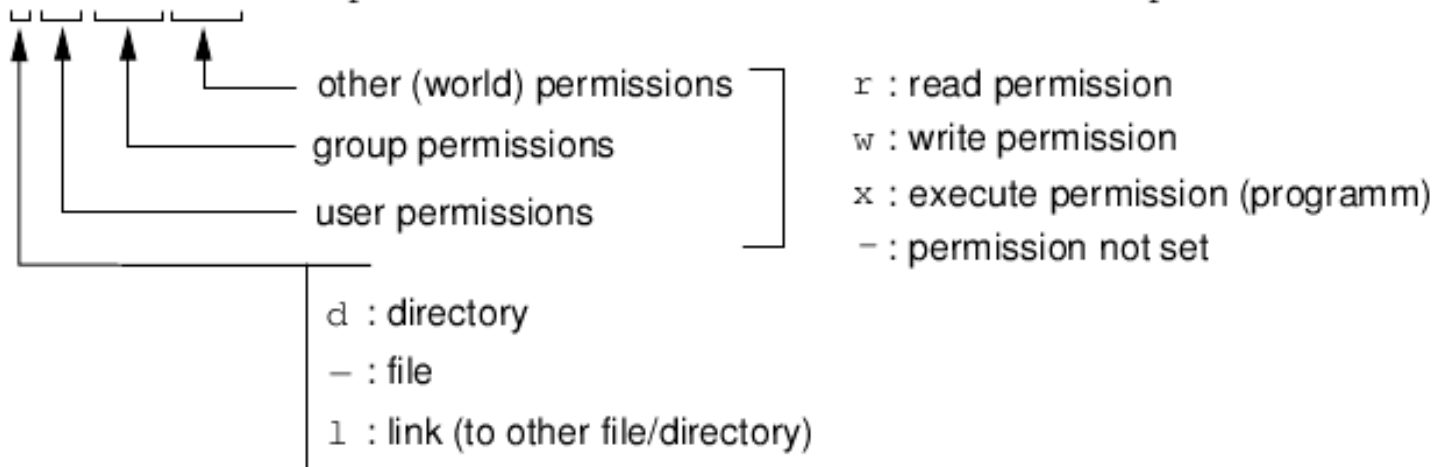


Sandboxing



POSIX Permissions

permissions		user	group	size	date	file/directory
drwxr-xr-x	2	paul	users	1024	Jan 2 23:50	.
drwxr-xr-x	6	root	root	1024	Jan 2 22:51	..
drwxr-xr-x	3	paul	users	1024	Jan 8 11:42	grassdata
lrwxrwxrwx	1	paul	users	13	May 6 1998	latex -> /d2/lt
drwx-----	2	paul	users	1024	Mar 8 17:30	mail
drwx-----	2	paul	users	1024	Feb 4 01:09	projects
-rw-r--r--	1	paul	users	844344	Dec 9 1998	nations.ps
-rw-rw-r--	1	paul	users	21438	Mar 2 21:47	ps4mf.txt

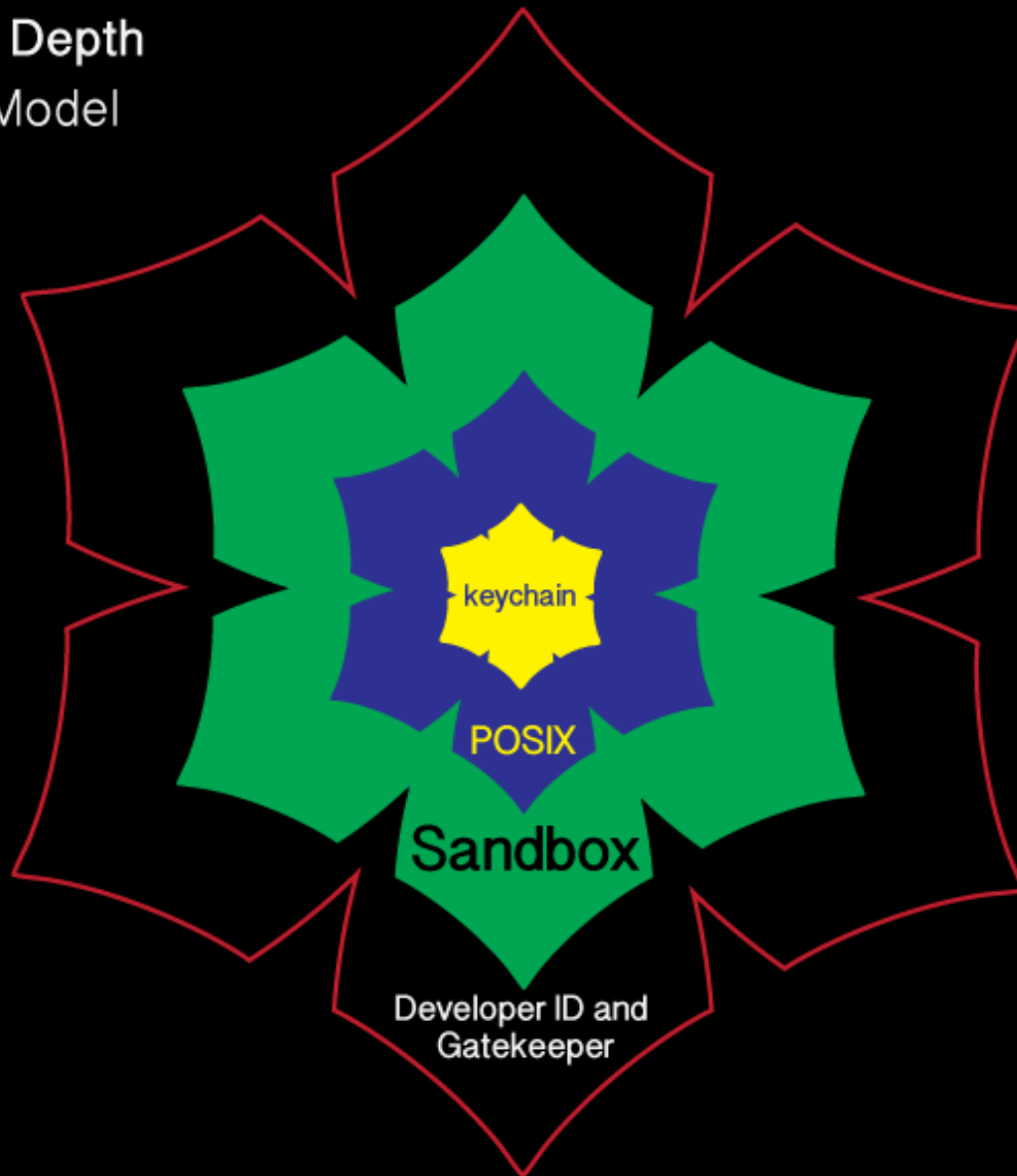


Keychain



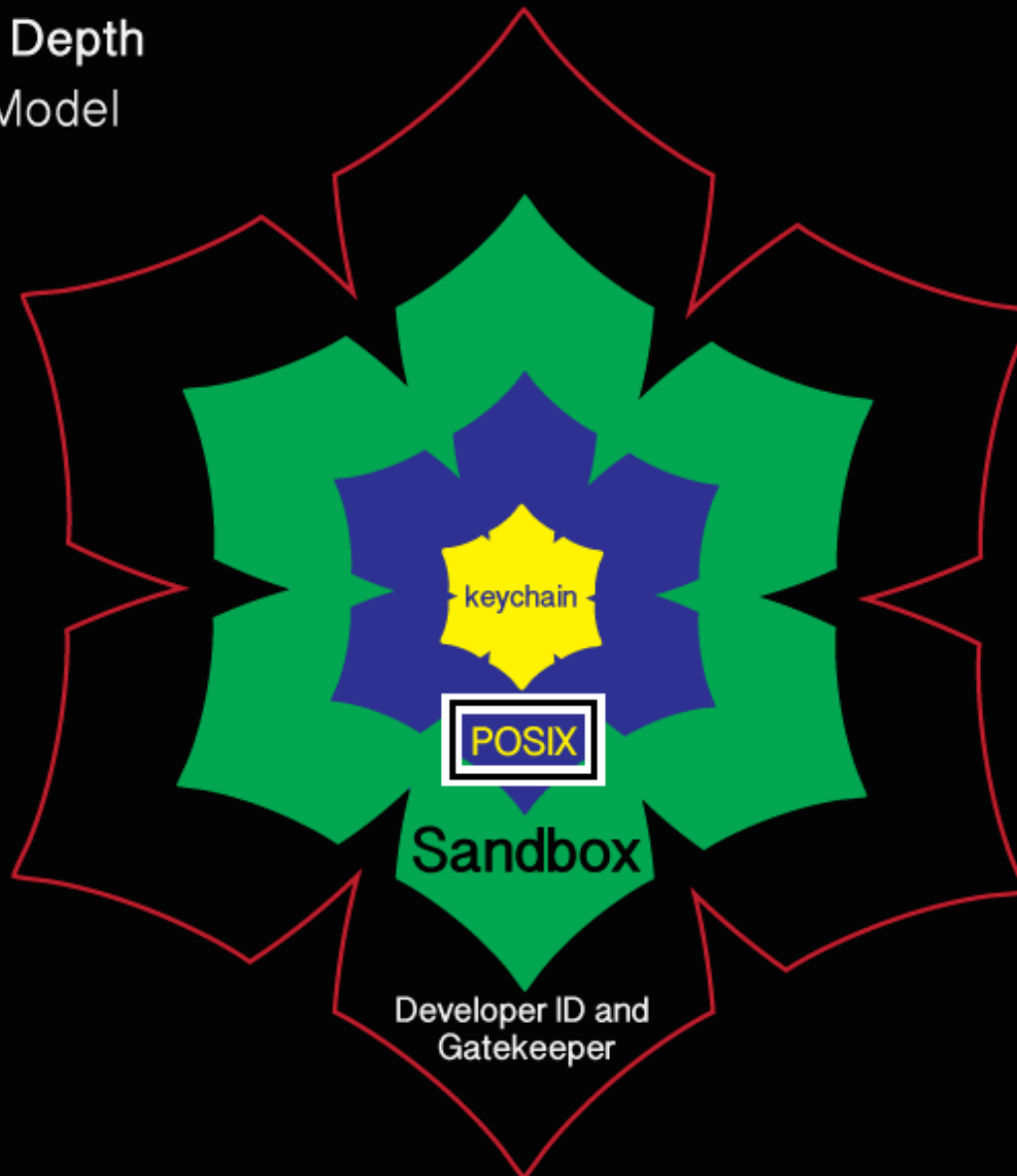
Defense in Depth

The OS X Model



Defense in Depth

The OS X Model



Root

```
bash-3.2# whoami  
root  
bash-3.2# █
```

Root

- Write anywhere on the local filesystem
- Make the OS report anything desired, including that "everything's fine" when it's not.
- Enable or disable all security measures

Root

OS X's compensating security measures

- Disable the root user account
- Discourage enabling root account
- Require an administrator's password to access elevated privileges
- Use **sudo** to run command line applications and process with root privileges

System Integrity Protection

- Limits the power of root
- Protection is on by default
- Only applies to the boot and root volumes.

System Integrity Protection

OS Kernel stops processes from:

- Writing to protected files or folders
- Writing to block devices that back protected content
- Mounting over protected content

System Integrity Protection

System Integrity Protection
configuration is stored in NVRAM

- Applies to the entire machine
- Persistent even when OS is reinstalled

System Integrity Protection

System Integrity Protection's concepts

- File system protection
- Runtime protection
- Kernel extension protection

System Integrity Protection

Protected directories:

- **/System**
- **/bin**
- **/usr**
- **/sbin**

System Integrity Protection

Available to developers

- **~/Library**
- **/Library**
- **/usr/local**
- **/Applications**

System Integrity Protection

Restricted processes:

- `task_for_pid()` / `processor_set_tasks()` fail with `EPERM`
- Mach special ports are reset on `exec(2)`
- dyld environment variables are ignored
- DTrace probes unavailable

<http://tinyurl.com/SIP-Developer-Documentation>

System Integrity Protection

Kernel Extensions

- Must be signed with a **Developer ID for Signing Kexts** certificate
- Must be installed into **/Library/Extensions**

<http://tinyurl.com/SIP-Kernel-Extension>

SIP Configuration

```

/Applications/App Store.app
/Applications/Automator.app
/Applications/Calculator.app
/Applications/Calendar.app
/Applications/Chess.app
/Applications/Contacts.app
/Applications/Dashboard.app
/Applications/Dictionary.app
/Applications/DVD Player.app
/Applications/FaceTime.app
/Applications/Font Book.app
/Applications/Game Center.app
/Applications/Image Capture.app
/Applications/Launchpad.app
/Applications/Mail.app
/Applications/Maps.app
/Applications/Messages.app
/Applications/Mission Control.app
/Applications/Notes.app
/Applications/Photo Booth.app
/Applications/Photos.app
/Applications/Preview.app
/Applications/QuickTime Player.app
/Applications/Reminders.app
/Applications/Safari.app
/Applications/Stickies.app
/Applications/System Preferences.app
/Applications/TextEdit.app
/Applications/Time Machine.app
/Applications/Utilities/Activity Monitor.app
/Applications/Utilities/AirPort Utility.app
/Applications/Utilities/Audio MIDI Setup.app
/Applications/Utilities/Bluetooth File Exchange.app
/Applications/Utilities/Boot Camp Assistant.app
/Applications/Utilities/ColorSync Utility.app
/Applications/Utilities/Console.app
/Applications/Utilities/Digital Color Meter.app
/Applications/Utilities/Disk Utility.app
/Applications/Utilities/Feedback Assistant.app
/Applications/Utilities/Grab.app
/Applications/Utilities/Grapher.app
/Applications/Utilities/Keychain Access.app
/Applications/Utilities/Migration Assistant.app
/Applications/Utilities/Script Editor.app
/Applications/Utilities/System Information.app
/Applications/Utilities/Terminal.app
/Applications/Utilities/VoiceOver Utility.app
/Library/Preferences/SystemConfiguration/com.apple.Boot.plist
/System
/System/Library/Caches
/System/Library/CoreServices
/System/Library/CoreServices/Photo Library Migration Utility.app
/System/Library/CoreServices/RawCamera.bundle
/System/Library/Extensions
/System/Library/Extensions/*
/System/Library/LaunchDaemons/com.apple.UpdateSettings.plist
/System/Library/Speech
/System/Library/User Template
/bin
/private/var/db/dyld
/sbin
/usr
/usr/libexec/cups
/usr/local
/usr/share/man
# symlinks
/etc
/tmp
/var
```

/System/Library/Sandbox/rootless.conf

SIP Configuration

```
/Applications/App Store.app  
/Applications/Automator.app  
/Applications/Calculator.app  
/Applications/Calendar.app  
/Applications/Chess.app  
/Applications/Contacts.app  
/Applications/Dashboard.app  
/Applications/Dictionary.app  
/Applications/DVD Player.app  
/Applications/FaceTime.app  
/Applications/Font Book.app  
/Applications/Game Center.app  
/Applications/Image Capture.app  
/Applications/Launchpad.app  
/Applications/Mail.app  
/Applications/Maps.app  
/Applications/Messages.app  
/Applications/Mission Control.app  
/Applications/Notes.app  
/Applications/Photo Booth.app  
/Applications/Photos.app  
/Applications/Preview.app  
/Applications/QuickTime Player.app  
/Applications/Reminders.app  
/Applications/Safari.app  
/Applications/Stickies.app  
/Applications/System Preferences.app  
/Applications/TextEdit.app  
/Applications/Time Machine.app
```

```
/Applications/Utilities/Activity Monitor.app  
/Applications/Utilities/AirPort Utility.app  
/Applications/Utilities/Audio MIDI Setup.app  
/Applications/Utilities/Bluetooth File Exchange.app  
/Applications/Utilities/Boot Camp Assistant.app  
/Applications/Utilities/ColorSync Utility.app  
/Applications/Utilities/Console.app  
/Applications/Utilities/Digital Color Meter.app  
/Applications/Utilities/Disk Utility.app  
/Applications/Utilities/Feedback Assistant.app  
/Applications/Utilities/Grab.app  
/Applications/Utilities/Grapher.app  
/Applications/Utilities/Keychain Access.app  
/Applications/Utilities/Migration Assistant.app  
/Applications/Utilities/Script Editor.app  
/Applications/Utilities/System Information.app  
/Applications/Utilities/Terminal.app  
/Applications/Utilities/VoiceOver Utility.app
```

SIP Configuration

```

                                /Library/Preferences/SystemConfiguration/com.apple.Boot.plist
                                /System
*                               /System/Library/Caches
booter                         /System/Library/CoreServices
*                               /System/Library/CoreServices/Photo Library Migration Utility.app
                                /System/Library/CoreServices/RawCamera.bundle
*                               /System/Library/Extensions
                                /System/Library/Extensions/*
UpdateSettings                 /System/Library/LaunchDaemons/com.apple.UpdateSettings.plist
*                               /System/Library/Speech
*                               /System/Library/User Template
                                /bin
dyld                           /private/var/db/dyld
                                /sbin
                                /usr
*                               /usr/libexec/cups
*                               /usr/local
*                               /usr/share/man
# symlinks                     /etc
                                /tmp
                                /var
```


SIP Configuration

```
                                /Library/Preferences/SystemConfiguration/com.apple.Boot.plist
                                /System
*                               /System/Library/Caches
booter                         /System/Library/CoreServices
*                               /System/Library/CoreServices/Photo Library Migration Utility.app
                                /System/Library/CoreServices/RawCamera.bundle
*                               /System/Library/Extensions
                                /System/Library/Extensions/*
UpdateSettings                 /System/Library/LaunchDaemons/com.apple.UpdateSettings.plist
*                               /System/Library/Speech
*                               /System/Library/User Template
                                /bin
dyld                           /private/var/db/dyld
                                /sbin
                                /usr
*                               /usr/libexec/cups
*                               /usr/local
*                               /usr/share/man
# symlinks                     /etc
                                /tmp
                                /var
```

SIP Configuration

- **rootless.conf** is Apple's and is not intended for modification by third parties
- Updates to **rootless.conf** are delivered via Software Update, like they are for XProtect and Gatekeeper

SIP Detection

To see which files and folders have been protected by SIP, run the command below:

ls -O (capital letter O)

SIP Detection

```
computername:~ username$ ls -la0 /
total 324
drwxr-xr-x@ 33 root wheel - 1190 Jul 28 21:04 .
drwxr-xr-x@ 33 root wheel - 1190 Jul 28 21:04 ..
-rw-rw-r-- 1 root admin - 6148 Aug 2 17:39 .DS_Store
-rw-r--r-- 1 root wheel - 593 Jun 14 11:39 .OSInstallerMessages
drwxr-xr-x 2 root staff - 68 Jun 14 11:21 .PKInstallSandboxManager
drwx----- 5 root wheel - 170 Jun 14 11:42 .Spotlight-V100
d-wx-wx-wt 2 root staff hidden 68 Aug 27 2008 .Trashes
-rw-r--r--@ 1 1000 staff hidden 130756 Aug 27 2008 .VolumeIcon.icns
----- 1 root admin - 0 Jul 18 14:37 .file
drwx----- 125 root staff - 4250 Jul 28 21:15 .fseventsd
drwxr-xr-x@ 2 root wheel hidden 68 May 10 01:22 .vol
drwxrwxr-x+ 43 root admin - 1462 Jul 28 21:04 Applications
drwxr-xr-x+ 63 root staff - 2142 Jul 28 21:04 Library
drwxr-xr-x@ 2 root wheel hidden 68 May 10 00:28 Network
drwxr-xr-x@ 4 root wheel restricted 136 Jul 28 19:58 System
drwxr-xr-x 6 root admin - 204 Aug 2 17:00 Users
drwxrwxrwt@ 4 root admin hidden 136 Aug 2 17:00 Volumes
drwxr-xr-x@ 39 root wheel restricted,hidden 1326 Jul 28 19:58 bin
drwxrwxr-t@ 2 root admin hidden 68 May 10 00:28 cores
dr-xr-xr-x 3 root wheel hidden 4047 Aug 2 16:59 dev
lrwxr-xr-x@ 1 root wheel restricted,hidden 11 Jun 14 11:34 etc -> private/etc
dr-xr-xr-x 2 root wheel hidden 1 Aug 2 16:59 home
-rw-r--r--@ 1 root wheel hidden 313 May 10 05:55 installer.failurerequests
dr-xr-xr-x 2 root wheel hidden 1 Aug 2 16:59 net
drwxr-xr-x 3 root wheel - 102 Aug 11 2014 opt
drwxrwxrwx 3 root wheel - 102 Jul 28 21:04 path
drwxr-xr-x@ 6 root wheel hidden 204 Jun 14 11:36 private
drwxr-xr-x@ 59 root wheel restricted,hidden 2006 Jul 28 19:58 sbin
lrwxr-xr-x@ 1 root wheel restricted,hidden 11 Jun 14 11:34 tmp -> private/tmp
drwxr-xr-x@ 12 root wheel restricted,hidden 408 Jul 28 20:59 usr
lrwxr-xr-x@ 1 root wheel restricted,hidden 11 Jun 14 11:35 var -> private/var
computername:~ username$
```

SIP Detection

```
private — -bash — 61x9
computername:private username$ ls -la0 /private
total 0
drwxr-xr-x@  6 root  wheel  hidden  204 Jun 14 11:36 .
drwxr-xr-x@ 33 root  wheel  -       1190 Jul 28 21:04 ..
drwxr-xr-x  89 root  wheel  -       3026 Jul 28 21:15 etc
drwxr-xr-x   2 root  wheel  -         68 May 10 02:30 tftpboot
drwxrwxrwt   5 root  wheel  -        170 Aug  2 17:01 tmp
drwxr-xr-x  25 root  wheel  -        850 Jul 28 21:06 var
computername:private username$
```

Additional SIP Exceptions

/System/Library/Sandbox/Compatibility.bundle/
Contents/Resources/paths

<http://tinyurl.com/SIP-Compatibility-Exceptions>

SIP Management

/usr/bin/csrutil

```
computername:~ username$ /usr/bin/csrutil
usage: csrutil <command>
Modify the System Integrity Protection configuration. All configuration changes apply to the entire machine.
Available commands:

clear
    Clear the existing configuration. Only available in Recovery OS.
disable
    Disable the protection on the machine. Only available in Recovery OS.
enable
    Enable the protection on the machine. Only available in Recovery OS.
status
    Display the current configuration.

netboot
    add <address>
        Insert a new IPv4 address in the list of allowed NetBoot sources.
    list
        Print the list of allowed NetBoot sources.
    remove <address>
        Remove an IPv4 address from the list of allowed NetBoot sources.
computername:~ username$
```

SIP Management

codesign -d --entitlements - /usr/bin/csrutil

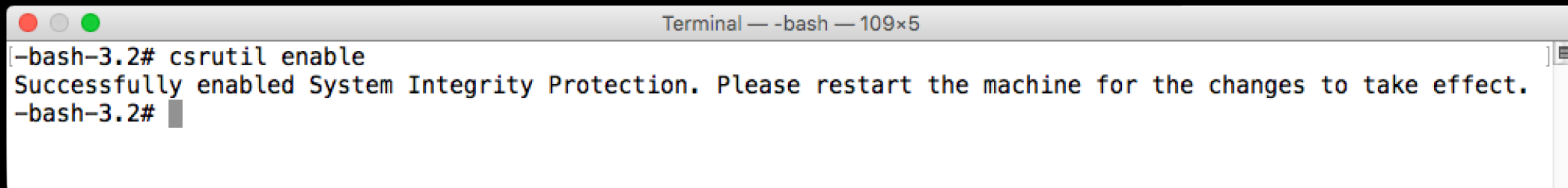
```
username — -bash — 102x11
computername:~ username$ codesign -d --entitlements - /usr/bin/csrutil
Executable=/usr/bin/csrutil
??qq?<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>com.apple.private.iokit.nvram-csr</key>
  <true/>
</dict>
</plist>
computername:~ username$
```


SIP Management



SIP Management

csrutil enable

A screenshot of a macOS Terminal window. The title bar at the top shows three colored window control buttons (red, yellow, green) on the left and the text 'Terminal — -bash — 109x5' on the right. The terminal content shows a prompt '-bash-3.2#' followed by the command 'csrutil enable'. The next line shows the output: 'Successfully enabled System Integrity Protection. Please restart the machine for the changes to take effect.' The prompt '-bash-3.2#' is followed by a small grey cursor block.

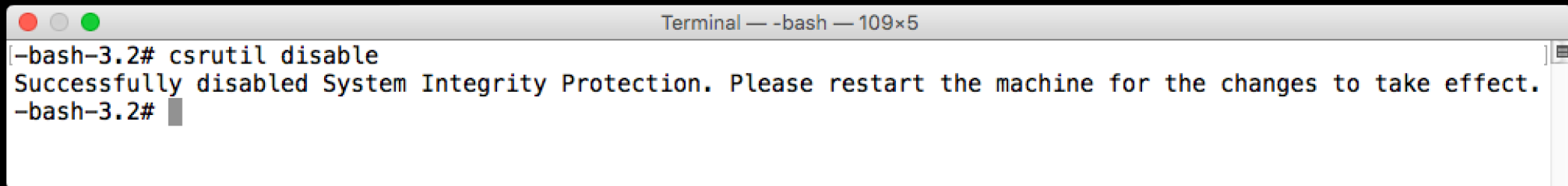
```
Terminal — -bash — 109x5
-bash-3.2# csrutil enable
Successfully enabled System Integrity Protection. Please restart the machine for the changes to take effect.
-bash-3.2#
```

Terminal — -bash — 80×24

-bash-3.2#

SIP Management

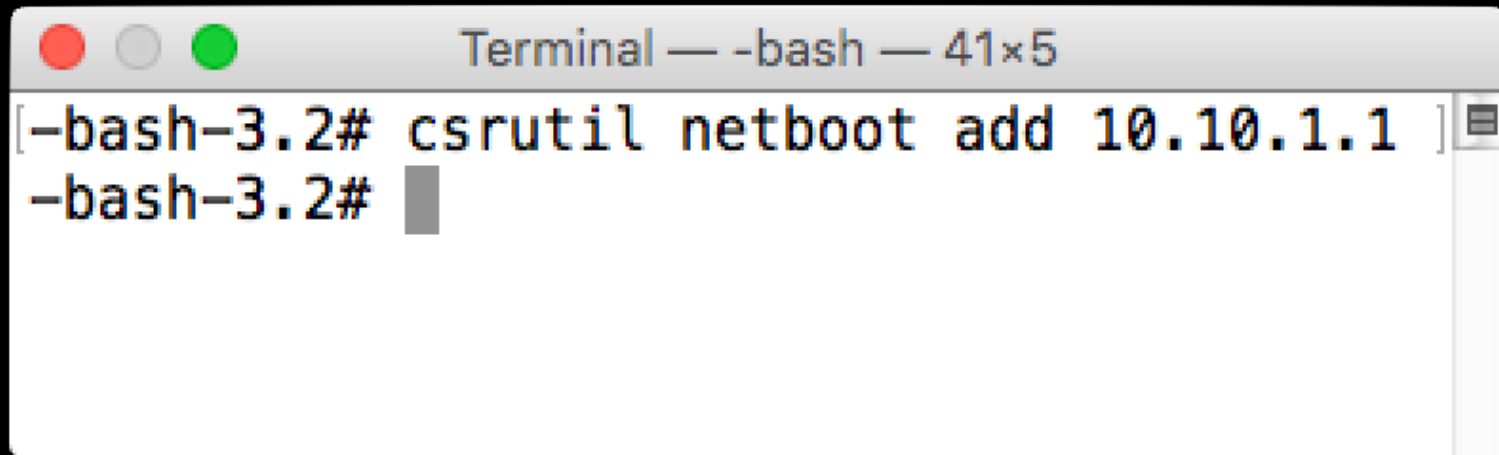
csrutil disable

A screenshot of a macOS Terminal window. The title bar at the top shows three colored window control buttons (red, yellow, green) on the left and the text 'Terminal — -bash — 109x5' on the right. The terminal content shows a prompt '-bash-3.2#' followed by the command 'csrutil disable'. The next line shows the output: 'Successfully disabled System Integrity Protection. Please restart the machine for the changes to take effect.' The prompt '-bash-3.2#' is followed by a small grey rectangular cursor.

```
Terminal — -bash — 109x5
-bash-3.2# csrutil disable
Successfully disabled System Integrity Protection. Please restart the machine for the changes to take effect.
-bash-3.2#
```

SIP Management

csrutil netboot add

A screenshot of a macOS Terminal window. The title bar at the top shows three window control buttons (red, yellow, green) on the left and the text 'Terminal — -bash — 41x5' on the right. The terminal content shows two lines of text: the first line is '[-bash-3.2# csrutil netboot add 10.10.1.1]' followed by a small icon, and the second line is '-bash-3.2#' followed by a grey cursor block.

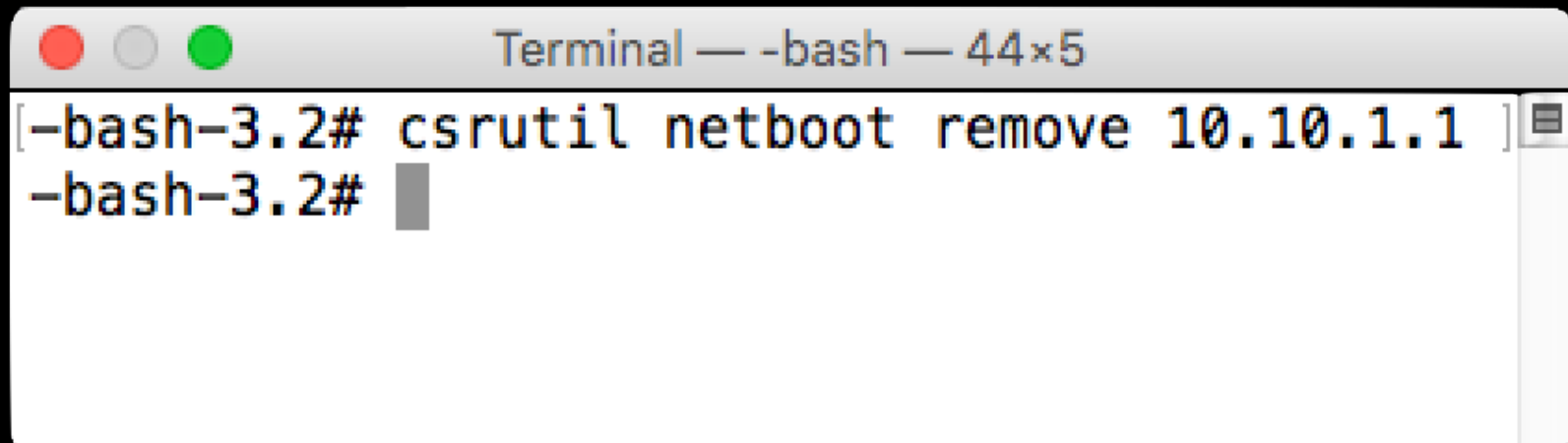
```
Terminal — -bash — 41x5
[ -bash-3.2# csrutil netboot add 10.10.1.1 ]
-bash-3.2#
```

Terminal — -bash — 80×24

-bash-3.2#

SIP Management

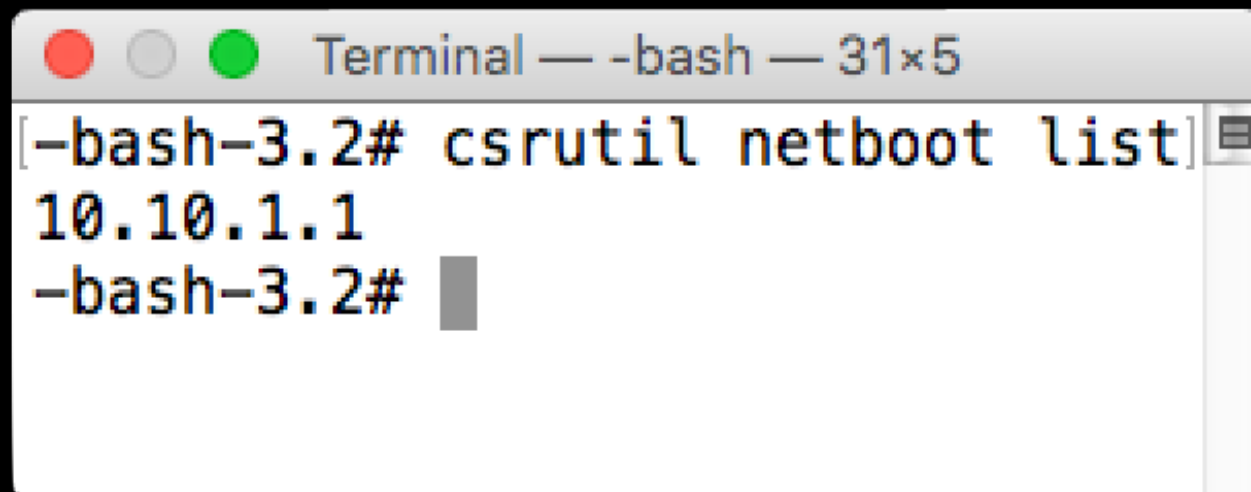
csrutil netboot remove

A screenshot of a macOS Terminal window. The title bar at the top shows three window control buttons (red, yellow, green) and the text "Terminal — -bash — 44x5". The terminal content shows a prompt "[-bash-3.2# " followed by the command "csrutil netboot remove 10.10.1.1" and a closing bracket "]". The second line shows the prompt "-bash-3.2# " followed by a grey cursor block.

```
Terminal — -bash — 44x5  
[ -bash-3.2# csrutil netboot remove 10.10.1.1 ]  
-bash-3.2# █
```

SIP Management

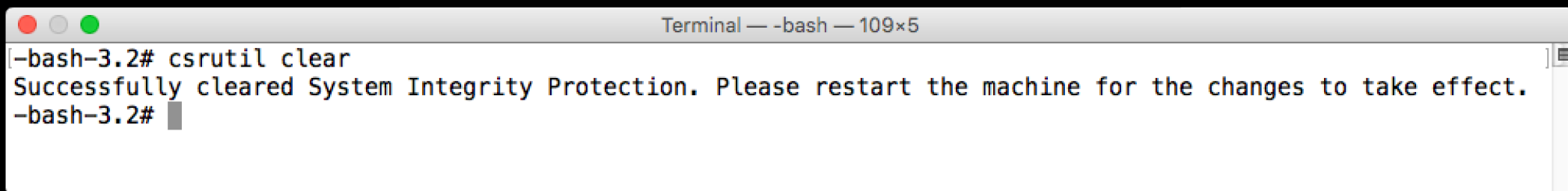
csrutil netboot list



```
Terminal — -bash — 31x5
[-bash-3.2# csrutil netboot list]
10.10.1.1
-bash-3.2#
```


SIP Management

csrutil clear

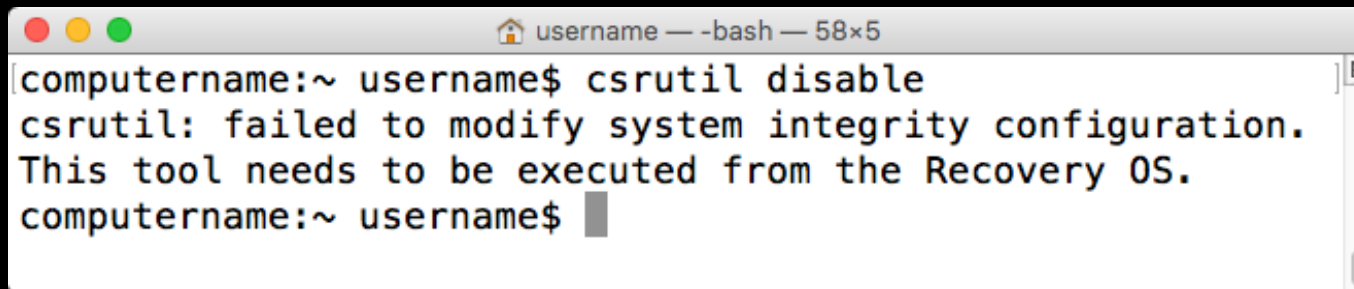
A screenshot of a macOS Terminal window. The title bar at the top reads "Terminal — -bash — 109x5". The terminal content shows the command `csrutil clear` being entered at the `-bash-3.2#` prompt. The output message is "Successfully cleared System Integrity Protection. Please restart the machine for the changes to take effect." followed by a new prompt `-bash-3.2#` with a cursor.

```
Terminal — -bash — 109x5
-bash-3.2# csrutil clear
Successfully cleared System Integrity Protection. Please restart the machine for the changes to take effect.
-bash-3.2#
```

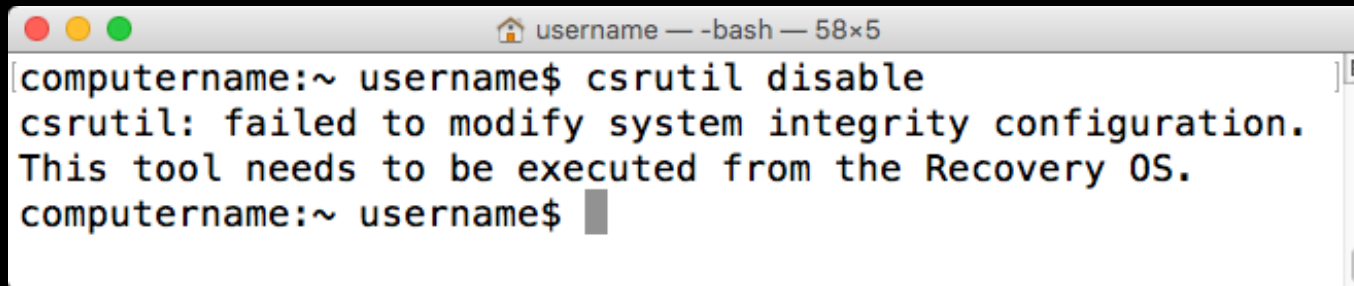
Terminal — -bash — 80×24

-bash-3.2#

SIP Management



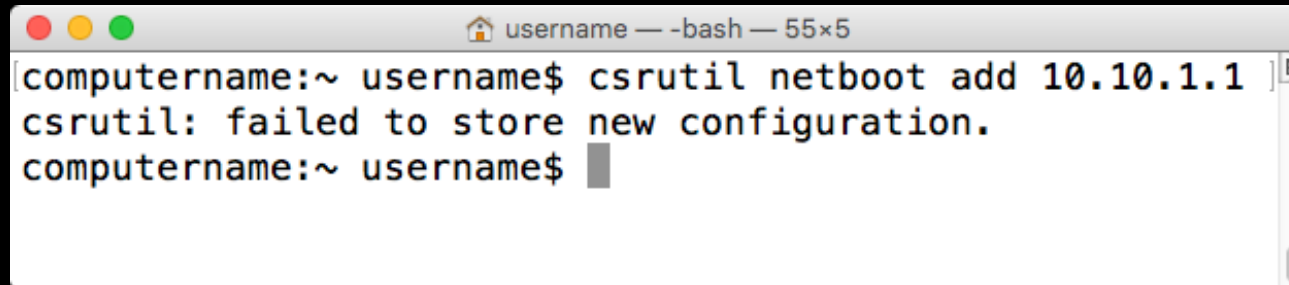
```
username — -bash — 58x5
[computername:~ username$ csrutil disable
csrutil: failed to modify system integrity configuration.
This tool needs to be executed from the Recovery OS.
computername:~ username$
```



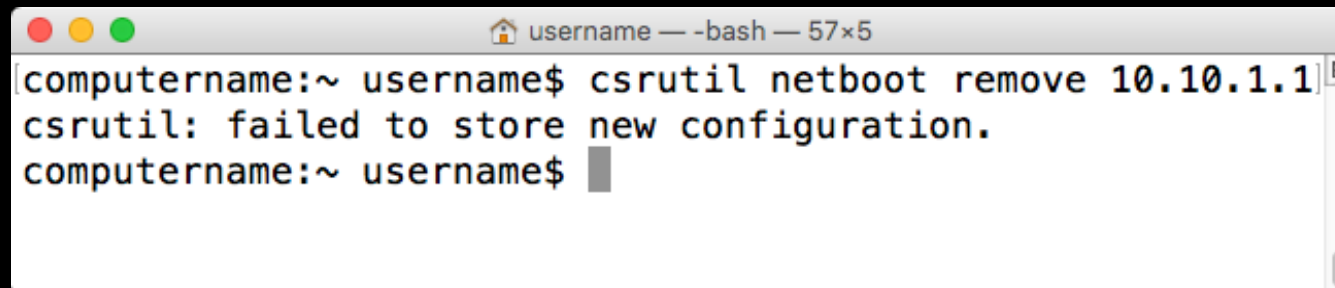
```
username — -bash — 58x5
[computername:~ username$ csrutil disable
csrutil: failed to modify system integrity configuration.
This tool needs to be executed from the Recovery OS.
computername:~ username$
```

csrutil enable and **csrutil disable**
must be run from Recovery

SIP Management

A terminal window with a title bar that says 'username — -bash — 55x5'. The terminal text shows a user at a computer named 'computername' in the home directory (~) running the command 'csrutil netboot add 10.10.1.1'. The output is 'csrutil: failed to store new configuration.' followed by a new prompt.

```
computername:~ username$ csrutil netboot add 10.10.1.1  
csrutil: failed to store new configuration.  
computername:~ username$
```

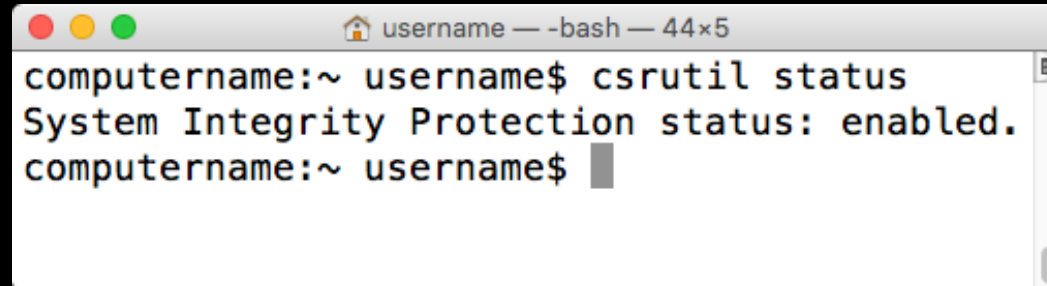
A terminal window with a title bar that says 'username — -bash — 57x5'. The terminal text shows a user at a computer named 'computername' in the home directory (~) running the command 'csrutil netboot remove 10.10.1.1'. The output is 'csrutil: failed to store new configuration.' followed by a new prompt.

```
computername:~ username$ csrutil netboot remove 10.10.1.1  
csrutil: failed to store new configuration.  
computername:~ username$
```

csrutil netbook add and
csrutil netboot remove
must be run from Recovery

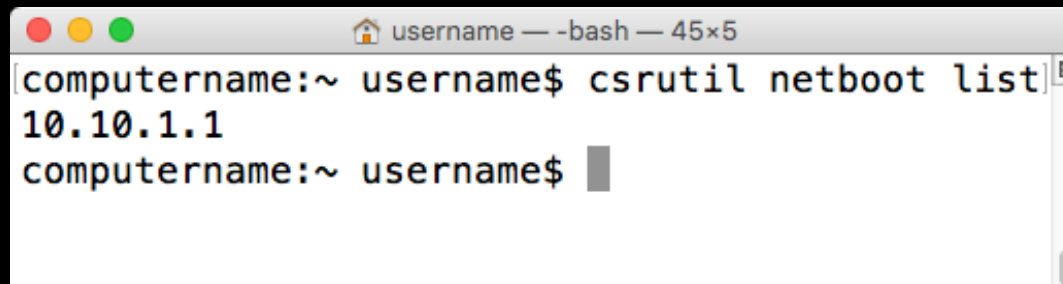
SIP Management

csrutil status

A terminal window titled 'username — -bash — 44x5' showing the command 'csrutil status' being executed. The output is 'System Integrity Protection status: enabled.' followed by a new prompt line.

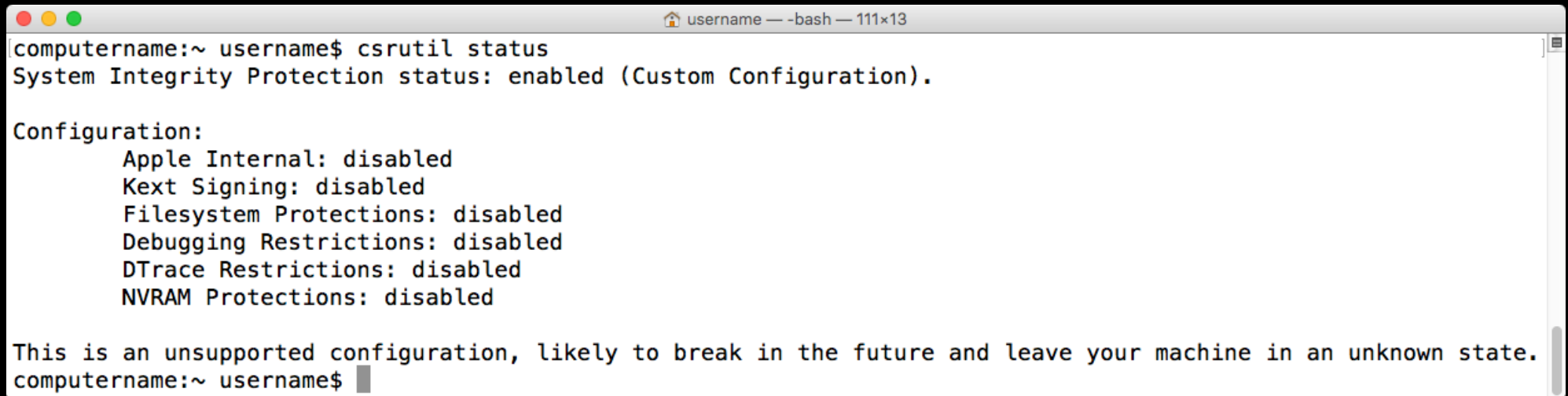
```
computername:~ username$ csrutil status
System Integrity Protection status: enabled.
computername:~ username$
```

csrutil netboot list

A terminal window titled 'username — -bash — 45x5' showing the command 'csrutil netboot list' being executed. The output is '10.10.1.1' followed by a new prompt line.

```
computername:~ username$ csrutil netboot list
10.10.1.1
computername:~ username$
```

SIP Management

A terminal window with a title bar showing 'username — -bash — 111x13'. The terminal output shows the command 'csrutil status' and its output, which indicates that System Integrity Protection is enabled in Custom Configuration. It then lists several configuration items, all of which are disabled: Apple Internal, Kext Signing, Filesystem Protections, Debugging Restrictions, DTrace Restrictions, and NVRAM Protections. A warning message follows, stating that this is an unsupported configuration that could break in the future. The prompt 'computername:~ username\$' is visible at the end of the output.

```
computername:~ username$ csrutil status
System Integrity Protection status: enabled (Custom Configuration).

Configuration:
  Apple Internal: disabled
  Kext Signing: disabled
  Filesystem Protections: disabled
  Debugging Restrictions: disabled
  DTrace Restrictions: disabled
  NVRAM Protections: disabled

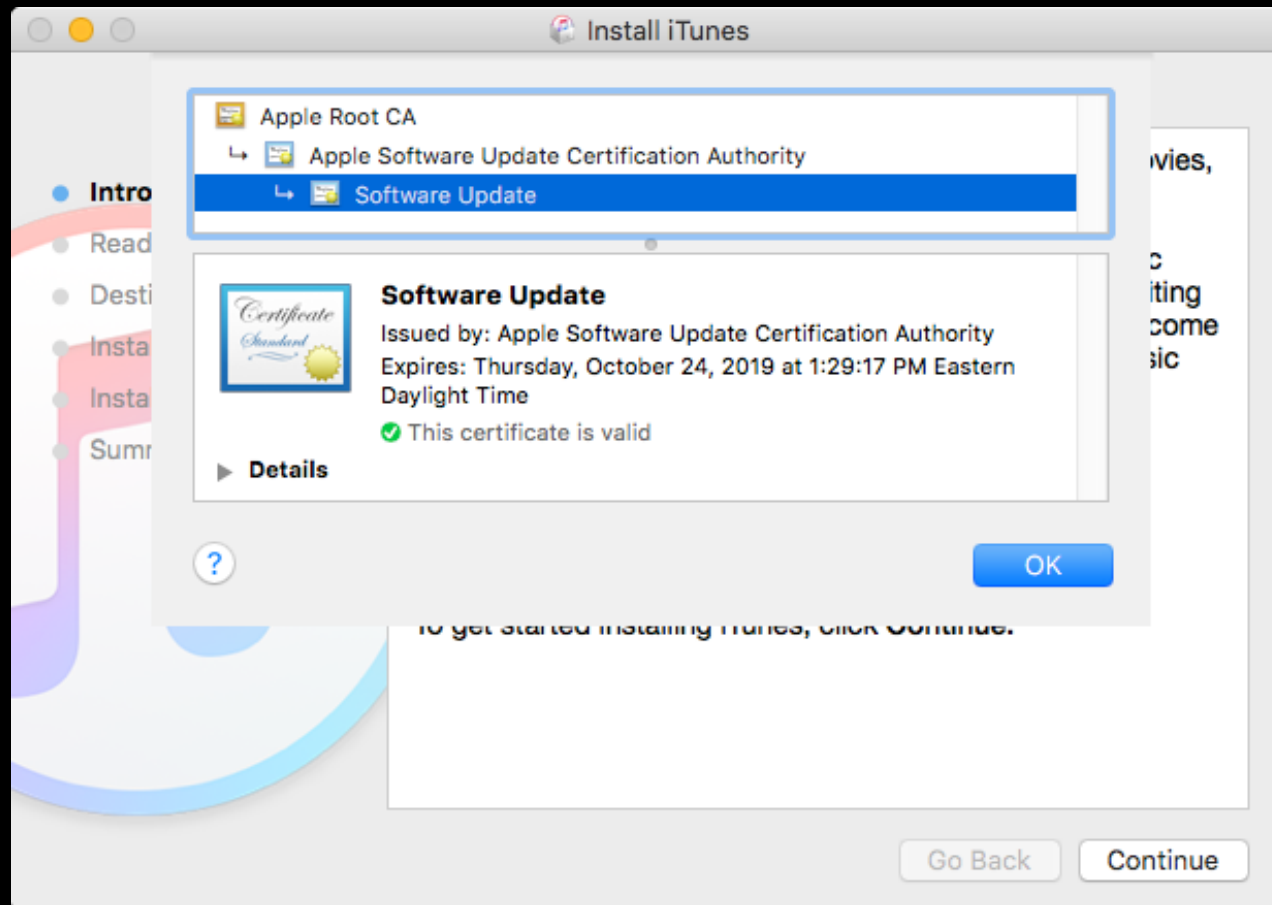
This is an unsupported configuration, likely to break in the future and leave your machine in an unknown state.
computername:~ username$
```

<http://tinyurl.com/bugID22361698>

SIP Management



SIP and Installer





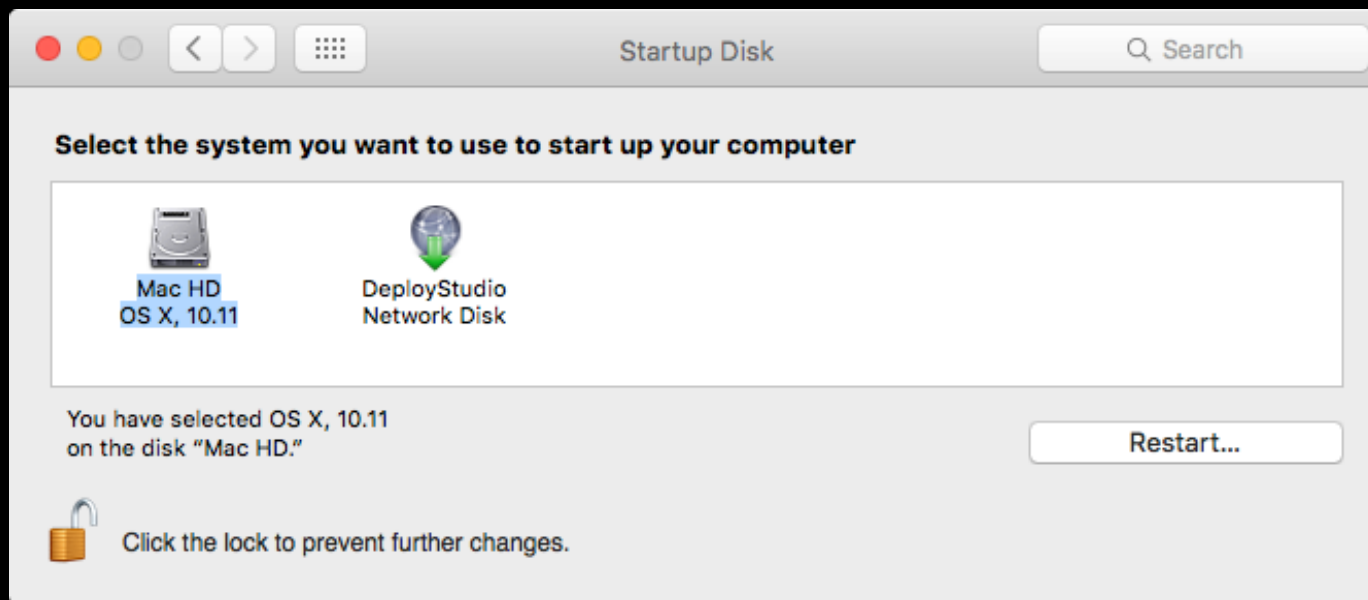
SIP and NetBoot

Do you need to use the **bless** command when NetBooting a Mac in your shop?

Yes	No
=	=
SIP Whitelisting required	SIP Whitelisting <u>not</u> required

SIP and NetBoot

If not using the bless
command for NetBoot



SIP and NetBoot

NetBoot
Helper IPs

NetBoot server on
local network
subnet

=

=

SIP Whitelisting
not required*

SIP Whitelisting
not required*

*Unless **bless** is used

NetBoot and Helper IPs

- Layer 3 traffic routing
- Relay all DHCP packets to the target IP
- Set helper IPs on a per-VLAN basis

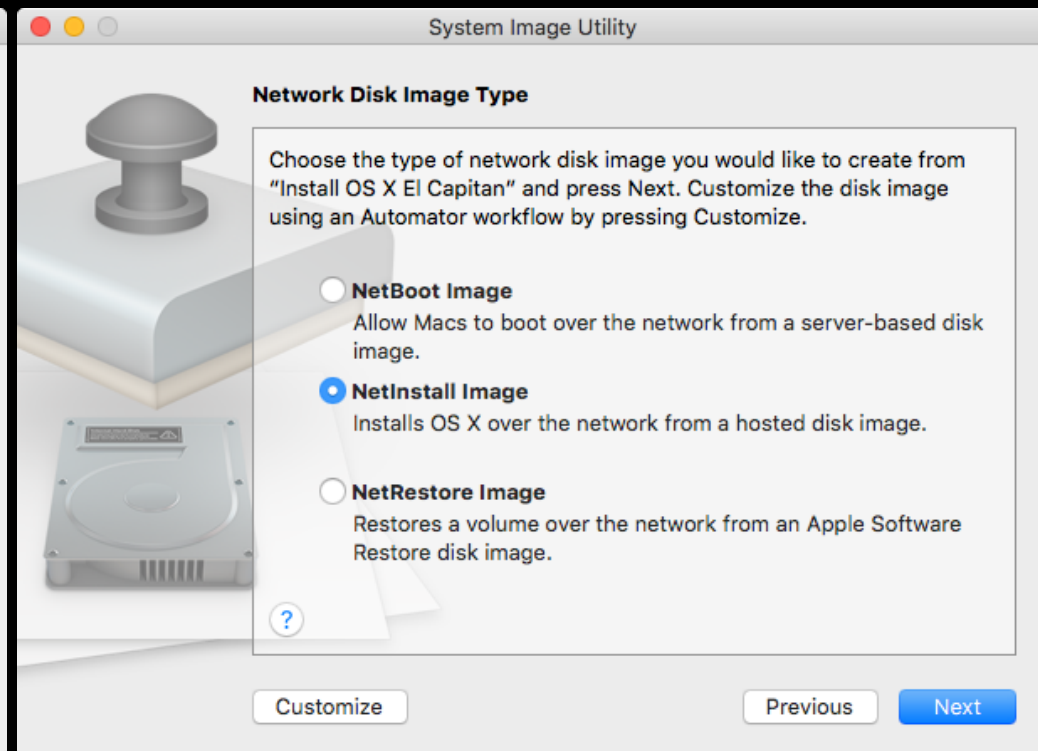
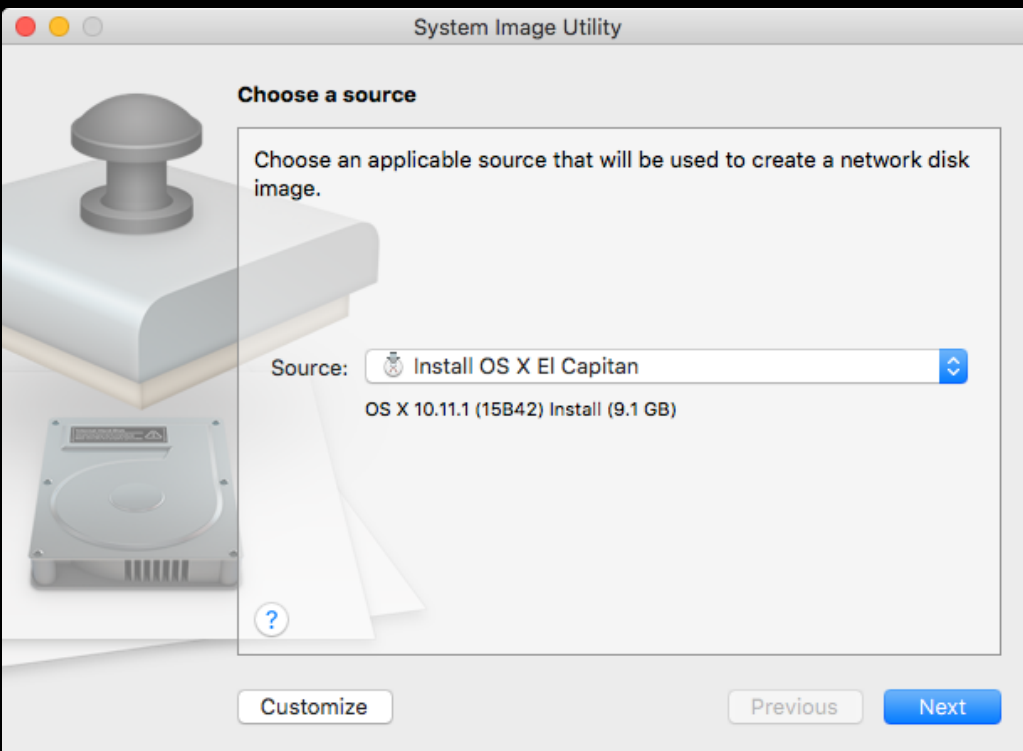
<http://kb.parallels.com/en/118518>

SIP and NetBoot

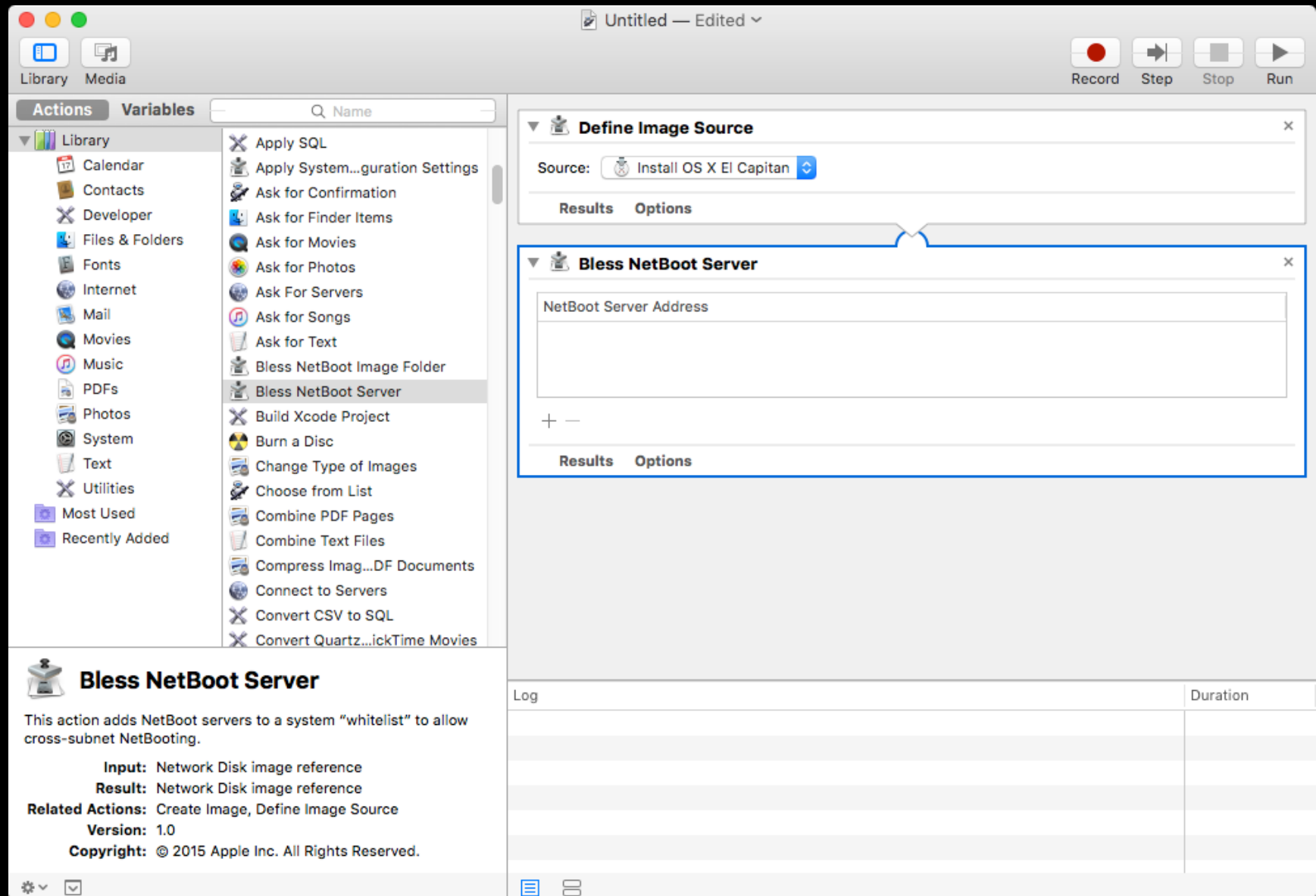
If using the bless command to NetBoot

- Need to whitelist NetBoot server IPs
- **csrutil netboot add** whitelists IPs and stores the whitelist in NVRAM
- Whitelisting can only be done while booted to recovery
- Running **csrutil clear** will reset the NetBoot whitelist and remove all current entries.

SIP and NetBoot



SIP and NetBoot



SIP and NetBoot

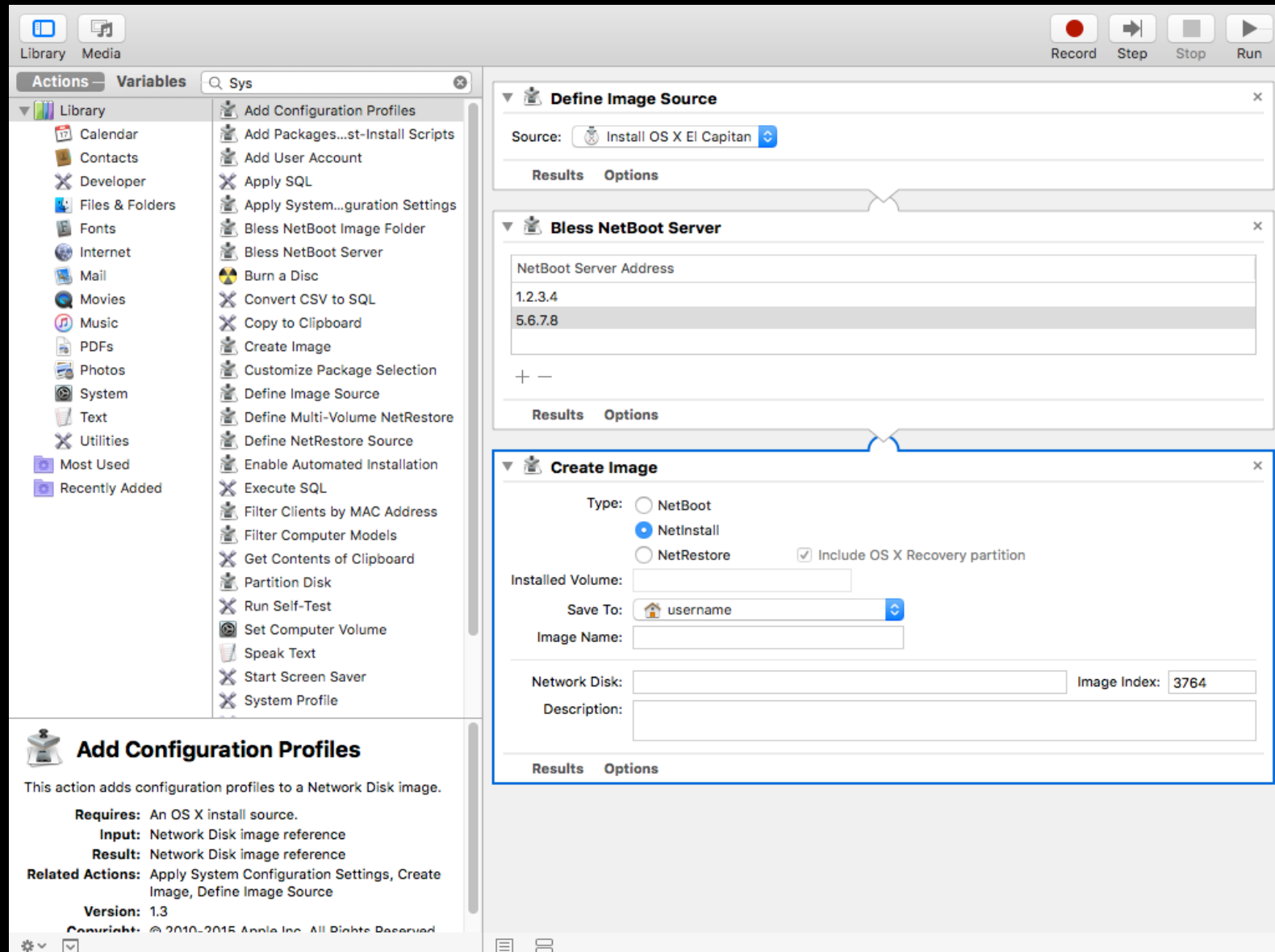
 **Bless NetBoot Server** ×

NetBoot Server Address
1.2.3.4
5.6.7.8

+ —

Results Options

SIP and NetBoot



SIP and NetBoot

```
#!/bin/bash
```

```
csrutil netboot add netboot.ip.address.goes.here  
csrutil netboot add netboot.ip.address.goes.here
```

SIP and NetBoot

```
username — less — man bless — 80x24

MOUNT MODE
To set a volume containing either Mac OS 9 and Mac OS X to be the active
volume:

    bless --mount "/Volumes/Mac OS" --setBoot

NETBOOT MODE
To set the system to NetBoot and broadcast for an available server:

    bless --netboot --server bsdp://255.255.255.255

INFO MODE
To gather information about the currently selected volume (as determined
by the firmware), suitable for piping to a program capable of parsing
Property Lists:

    bless --info --plist

SEE ALSO
    mount(8), newfs(8), nvram(8)

Mac OS X                               May 24, 2013                               Mac OS X
(END)
```

Terminal — -bash — 80×24

-bash-3.2#

SIP and Imaging





Mac HD



SIP and Installer

Project

Settings

Payload

Scripts

Comments

Settings

Type: Internal ☒ Split Forks if needed

Default Destination: / Set

Contents

Filename	Owner	Group	Permissions
/	root	wheel	drwxr-xr-x
Applications	root	admin	drwxrwxr-x
Utilities	root	admin	drwxr-xr-x
Library	root	wheel	drwxr-xr-x
Application Support	root	admin	drwxr-xr-x
Automator	root	wheel	drwxr-xr-x
Documentation	root	wheel	drwxr-xr-x
Filesystems	root	wheel	drwxr-xr-x
Frameworks	root	wheel	drwxr-xr-x
Input Methods	root	wheel	drwxr-xr-x
Internet Plug-Ins	root	wheel	drwxr-xr-x
LaunchAgents	root	wheel	drwxr-xr-x
LaunchDaemons	root	wheel	drwxr-xr-x
PreferencePanes	root	wheel	drwxr-xr-x
Preferences	root	wheel	drwxr-xr-x
Printers	root	admin	drwxr-xr-x
PrivilegedHelperTools	root	wheel	drwxr-xr-x
QuickLook	root	wheel	drwxr-xr-x
QuickTime	root	wheel	drwxr-xr-x
Screen Savers	root	wheel	drwxr-xr-x
Scripts	root	wheel	drwxr-xr-x
Services	root	wheel	drwxr-xr-x
Widgets	root	wheel	drwxr-xr-x
System	root	wheel	drwxr-xr-x
Library	root	wheel	drwxr-xr-x
very_important_file.txt	root	wheel	-rw-r--r--
Users	root	admin	drwxr-xr-x

+ -

very_important_file.txt

Modified: Aug 4, 2015, 7:43 PM

Architectures: -

Kind: File

Reference: R Relative to Project

Source: resources/very_important_file.txt

Destination: /System/very_important_file.txt

Attributes

Name: very_important_file.txt

Owner: root

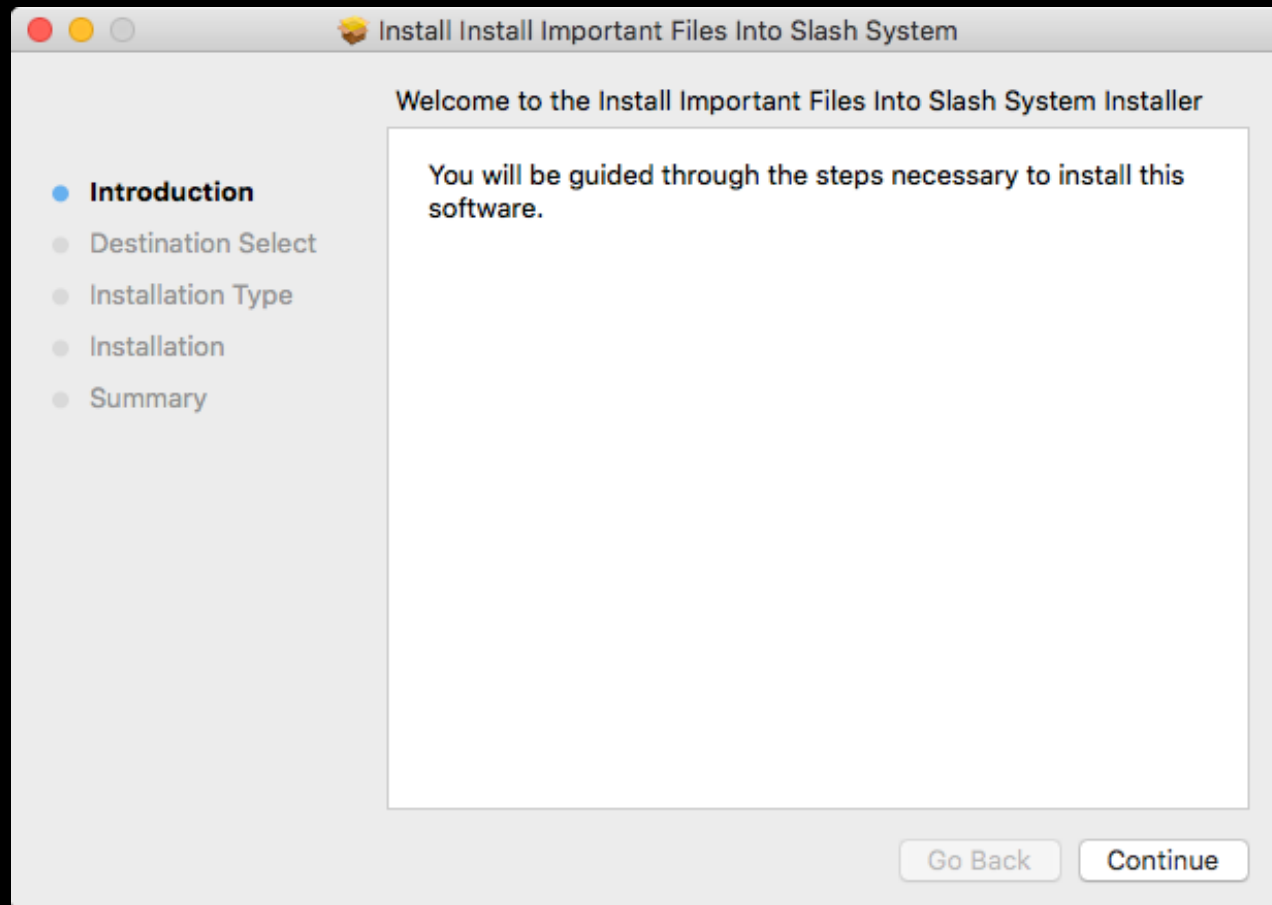
Group: wheel

Access: -rw-r--r--

	Read	Write	Exec	Bit	
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	SetUID
Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	SetGID
Others	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sticky

Build succeeded

SIP and Installer





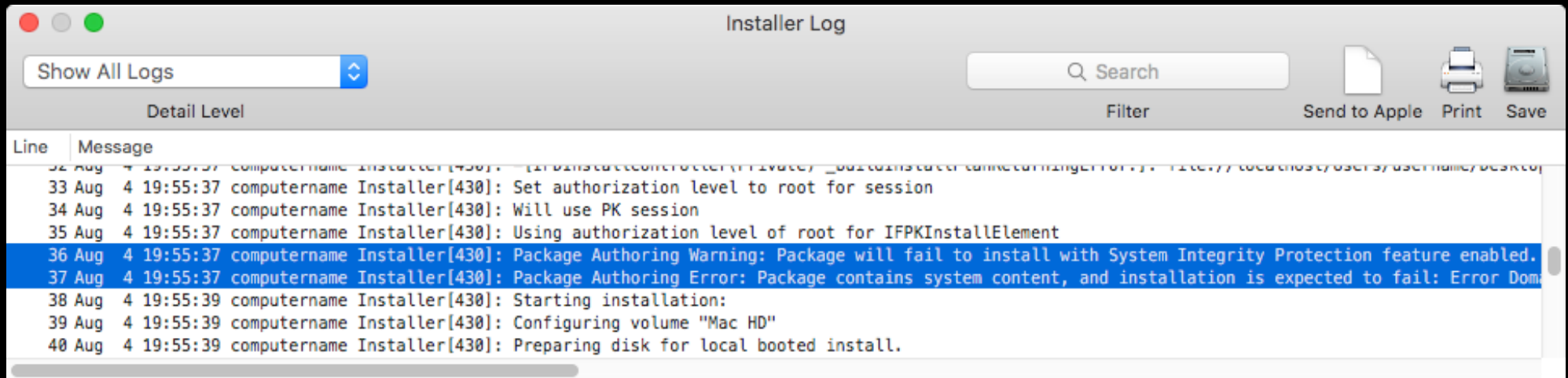
Mac HD



Install Important Files Into
Slash System.pkg



SIP and Installer



SIP and User Templates

```

/System
* /System/Library/Caches
booter /System/Library/CoreServices
* /System/Library/CoreServices/Photo Library Migration Utility.app
* /System/Library/CoreServices/RawCamera.bundle
* /System/Library/Extensions
/System/Library/Extensions/*
UpdateSettings /System/Library/LaunchDaemons/com.apple.UpdateSettings.plist
* /System/Library/Speech
* /System/Library/User Template
/bin
dyld /private/var/db/dyld
/sbin
/usr
* /usr/libexec/cups
* /usr/local
* /usr/share/man
# symlinks
/etc
/tmp
/var
```


SIP and Software





SIP and Software



SIP and Software



SIP and XProtect



Rich Trouton

@rtrouton

 Follow

XProtect has been updated to set Flash 19.0.0.226 and Flash ESR 18.0.0.255 as the minimum versions allowed. [#macadmin](#)
[#macadmins](#)

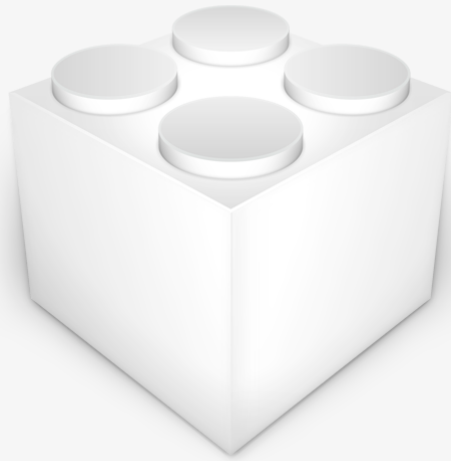
RETWEETS

5



11:03 AM - 20 Oct 2015

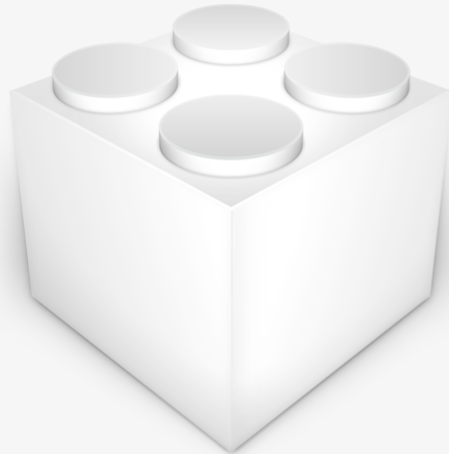
SIP and XProtect



JavaAppletPlugin.plugin

177.8 MB

Last modified Nov 17, 2014, 7:38:08 PM

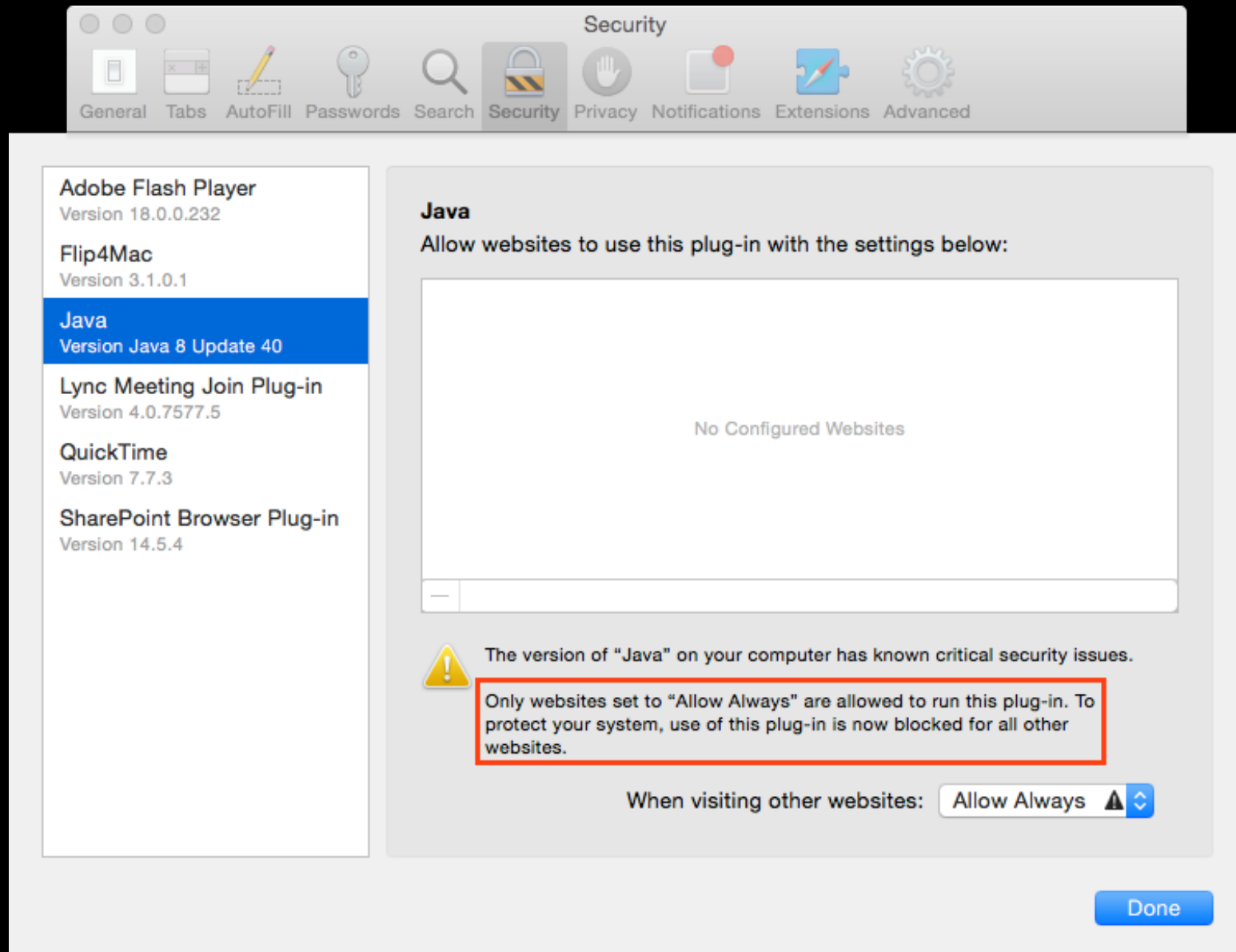


Flash Player.plugin

46 MB

Last modified Aug 12, 2015, 6:39:11 PM

SIP and XProtect



SIP and NVRAM Reset

NVRAM Reset

=

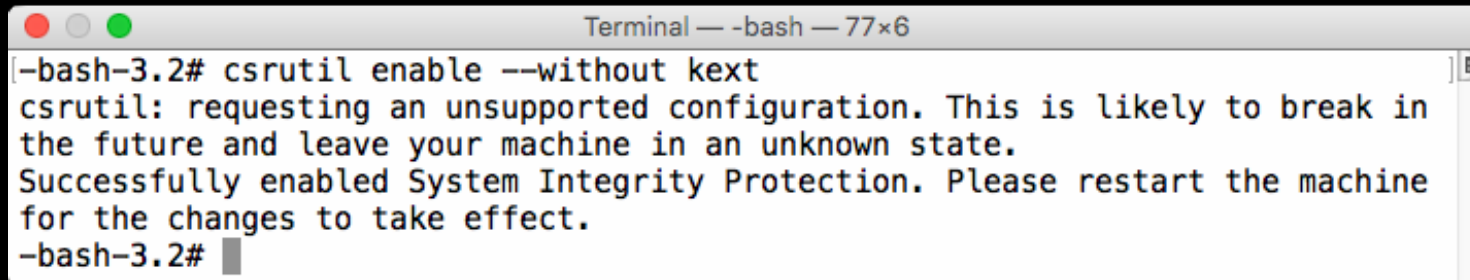
SIP resets to factory default:
SIP enabled, NetBoot whitelist cleared

SIP and NVRAM Reset



Zapping PRAM = NVRAM Reset

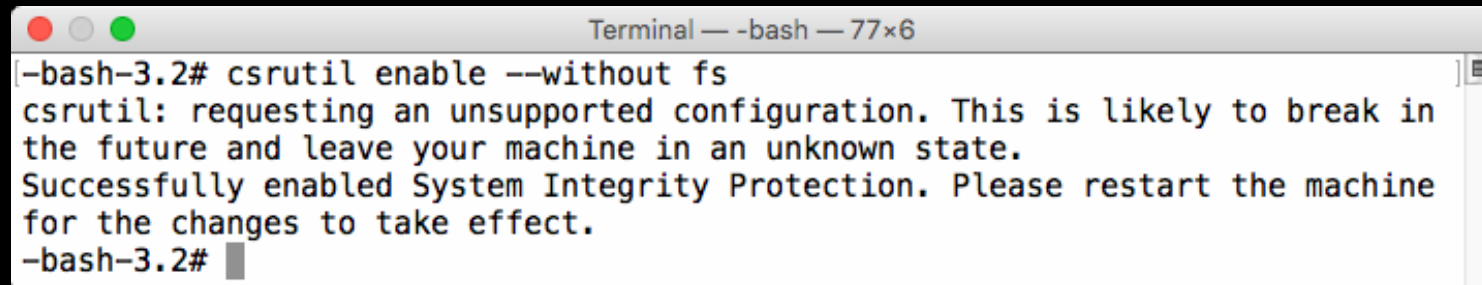
Custom SLP configurations



```
Terminal — -bash — 77x6
[-bash-3.2# csrutil enable --without kext
csrutil: requesting an unsupported configuration. This is likely to break in
the future and leave your machine in an unknown state.
Successfully enabled System Integrity Protection. Please restart the machine
for the changes to take effect.
-bash-3.2#
```

csrutil enable --without kext

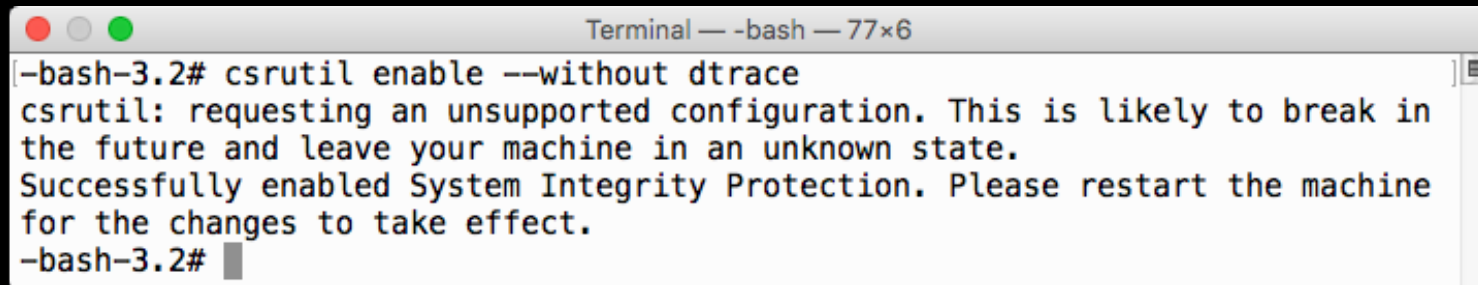
Custom SLP configurations

A screenshot of a macOS Terminal window. The title bar reads "Terminal — -bash — 77x6". The terminal content shows the command `csrutil enable --without fs` being executed. The output consists of three lines: a warning about an unsupported configuration, a confirmation that System Integrity Protection is enabled, and a request to restart the machine. The prompt `-bash-3.2#` is visible at the end of the output.

```
Terminal — -bash — 77x6
[-bash-3.2# csrutil enable --without fs
csrutil: requesting an unsupported configuration. This is likely to break in
the future and leave your machine in an unknown state.
Successfully enabled System Integrity Protection. Please restart the machine
for the changes to take effect.
-bash-3.2#
```

csrutil enable --without fs

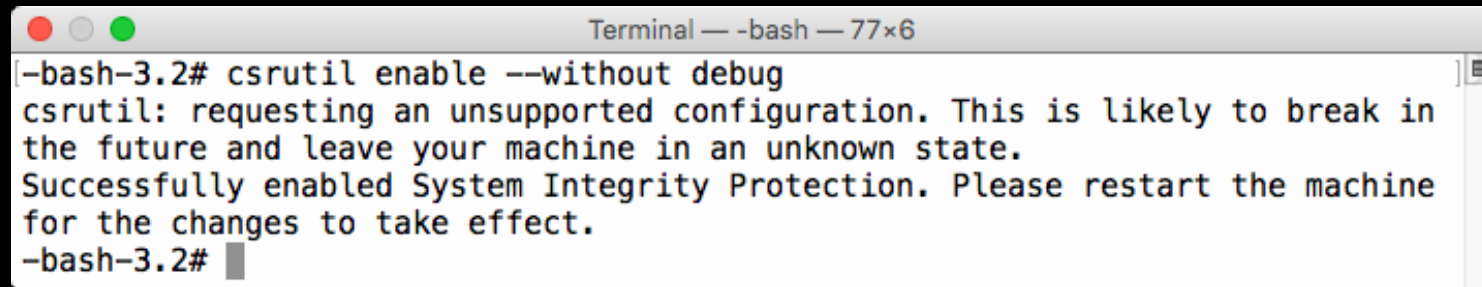
Custom SLP configurations

A screenshot of a macOS Terminal window. The title bar reads "Terminal — -bash — 77x6". The terminal content shows the command `csrutil enable --without dtrace` being executed. The output consists of three lines: a warning about an unsupported configuration, a confirmation that System Integrity Protection is enabled, and a request to restart the machine. The prompt `-bash-3.2#` is visible at the end of the command line.

```
Terminal — -bash — 77x6
-bash-3.2# csrutil enable --without dtrace
csrutil: requesting an unsupported configuration. This is likely to break in
the future and leave your machine in an unknown state.
Successfully enabled System Integrity Protection. Please restart the machine
for the changes to take effect.
-bash-3.2#
```

csrutil enable --without dtrace

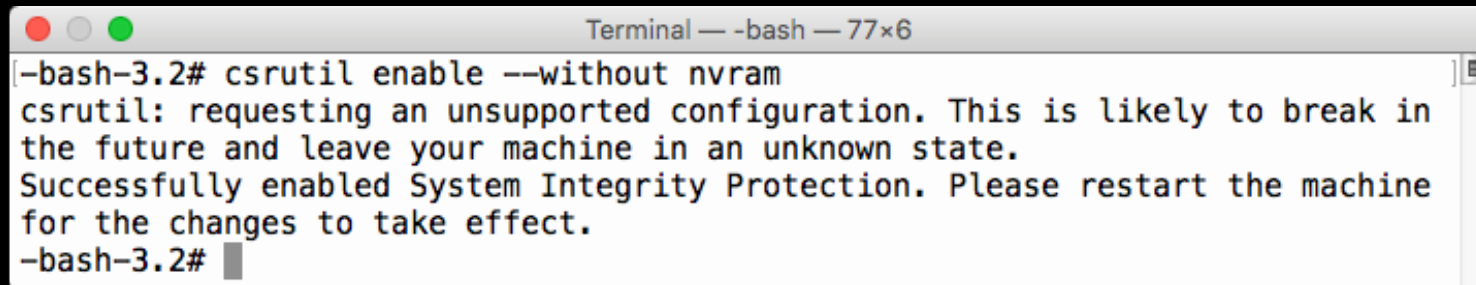
Custom SLP configurations

A screenshot of a macOS Terminal window. The title bar reads "Terminal — -bash — 77x6". The terminal content shows a root prompt "[~]#", followed by the command "csrutil enable --without debug". The output consists of three lines: "csrutil: requesting an unsupported configuration. This is likely to break in the future and leave your machine in an unknown state.", "Successfully enabled System Integrity Protection. Please restart the machine for the changes to take effect.", and a new root prompt "[~]#".

```
[~]# csrutil enable --without debug
csrutil: requesting an unsupported configuration. This is likely to break in
the future and leave your machine in an unknown state.
Successfully enabled System Integrity Protection. Please restart the machine
for the changes to take effect.
[~]#
```

csrutil enable --without debug

Custom SLP configurations

A screenshot of a macOS Terminal window. The title bar at the top reads "Terminal — -bash — 77x6". The terminal content shows a root shell prompt "[~]#". The user enters the command "csrutil enable --without nvram". The system responds with a warning: "csrutil: requesting an unsupported configuration. This is likely to break in the future and leave your machine in an unknown state." followed by a confirmation: "Successfully enabled System Integrity Protection. Please restart the machine for the changes to take effect." The prompt returns to "[~]#".

```
[~]# csrutil enable --without nvram
csrutil: requesting an unsupported configuration. This is likely to break in
the future and leave your machine in an unknown state.
Successfully enabled System Integrity Protection. Please restart the machine
for the changes to take effect.
[~]#
```

csrutil enable --without nvram

Custom SIP configurations

```
computername:~ username$ csrutil status
System Integrity Protection status: enabled (Custom Configuration).

Configuration:
  Apple Internal: disabled
  Kext Signing: enabled
  Filesystem Protections: enabled
  Debugging Restrictions: enabled
  DTrace Restrictions: enabled
  NVRAM Protections: disabled

This is an unsupported configuration, likely to break in the future and leave your machine in an unknown state.
computername:~ username$
```

Configuring SIP without Recovery

The screenshot shows a web browser window with the address bar displaying "Apple Inc. developer.apple.com/library/prerelease/mac/document:". The page title is "Mac Developer Library — Prerelease". The main content area is titled "System Integrity Protection Guide" and includes a "PDF" icon. A left sidebar contains a table of contents with the following items: "Table of Contents", "Introduction", "File System Protections" (expanded), "Migration of Third-Party Content", "Scripting Languages", "Runtime Protections", "Kernel Extensions", "Configuring System Integrity Protection", and "Revision History". The main content area shows the word "required." followed by a blue-bordered box containing a note: "Note: For certain enterprise configurations that do not allow booting to Recovery OS, System Integrity Protection can be configured by other means." Below the note are links for "Previous" and "Next". At the bottom, a footer contains the copyright notice "Copyright © 2015 Apple Inc. All Rights Reserved." followed by links for "Terms of Use" and "Privacy Policy", and the date "Updated: 2015-09-16". A "Feedback" button is located in the bottom right corner.

Mac Developer Library — Prerelease

System Integrity Protection Guide PDF

▼ Table of Contents

- Introduction
- ▼ File System Protections
 - Migration of Third-Party Content
 - Scripting Languages
- Runtime Protections
- Kernel Extensions
- Configuring System Integrity Protection
- Revision History

required.

Note: For certain enterprise configurations that do not allow booting to Recovery OS, System Integrity Protection can be configured by other means.

[Previous](#) [Next](#)

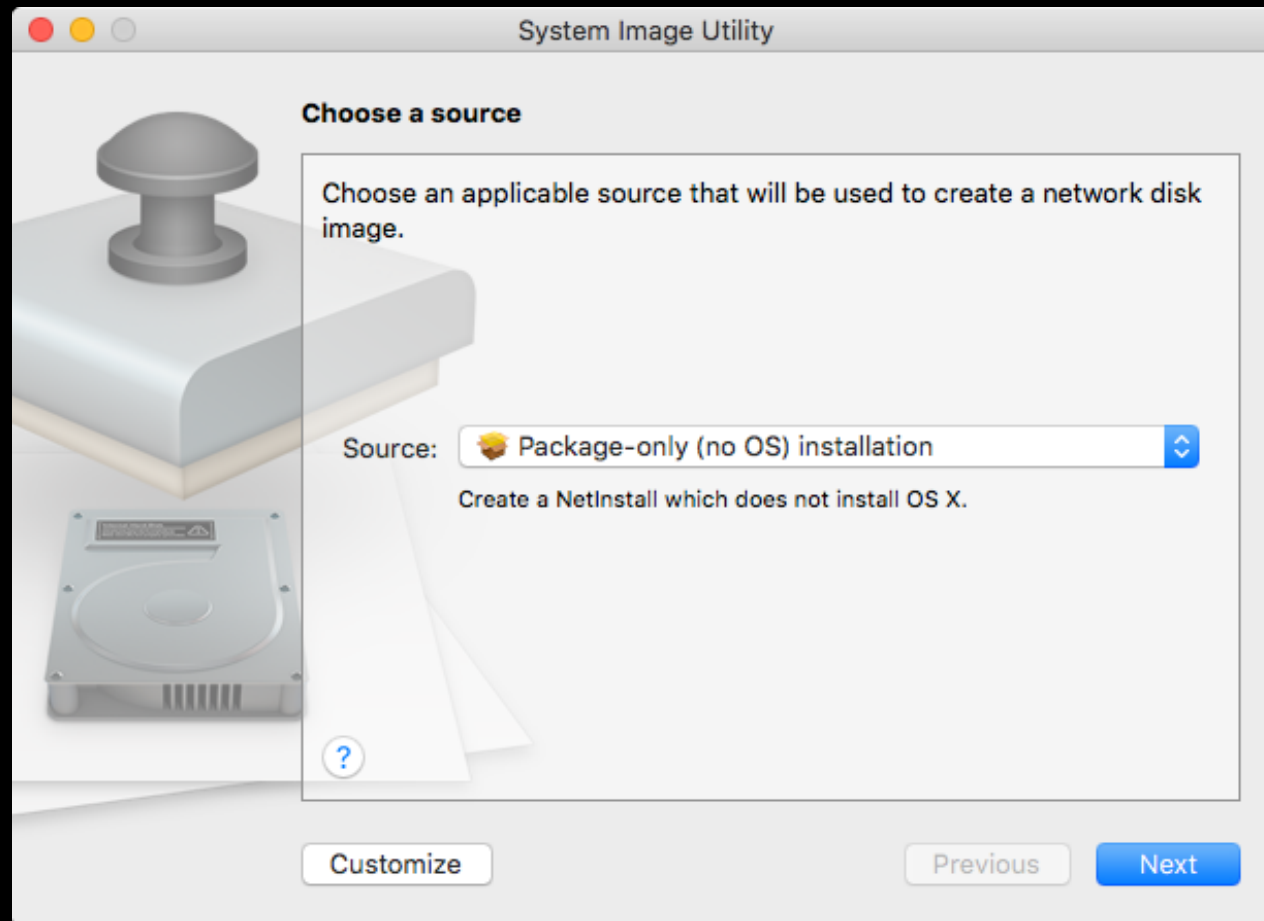
Copyright © 2015 Apple Inc. All Rights Reserved. [Terms of Use](#) | [Privacy Policy](#) | Updated: 2015-09-16

[Feedback](#)

Configuring SIP without Recovery



Configuring SIP without Recovery



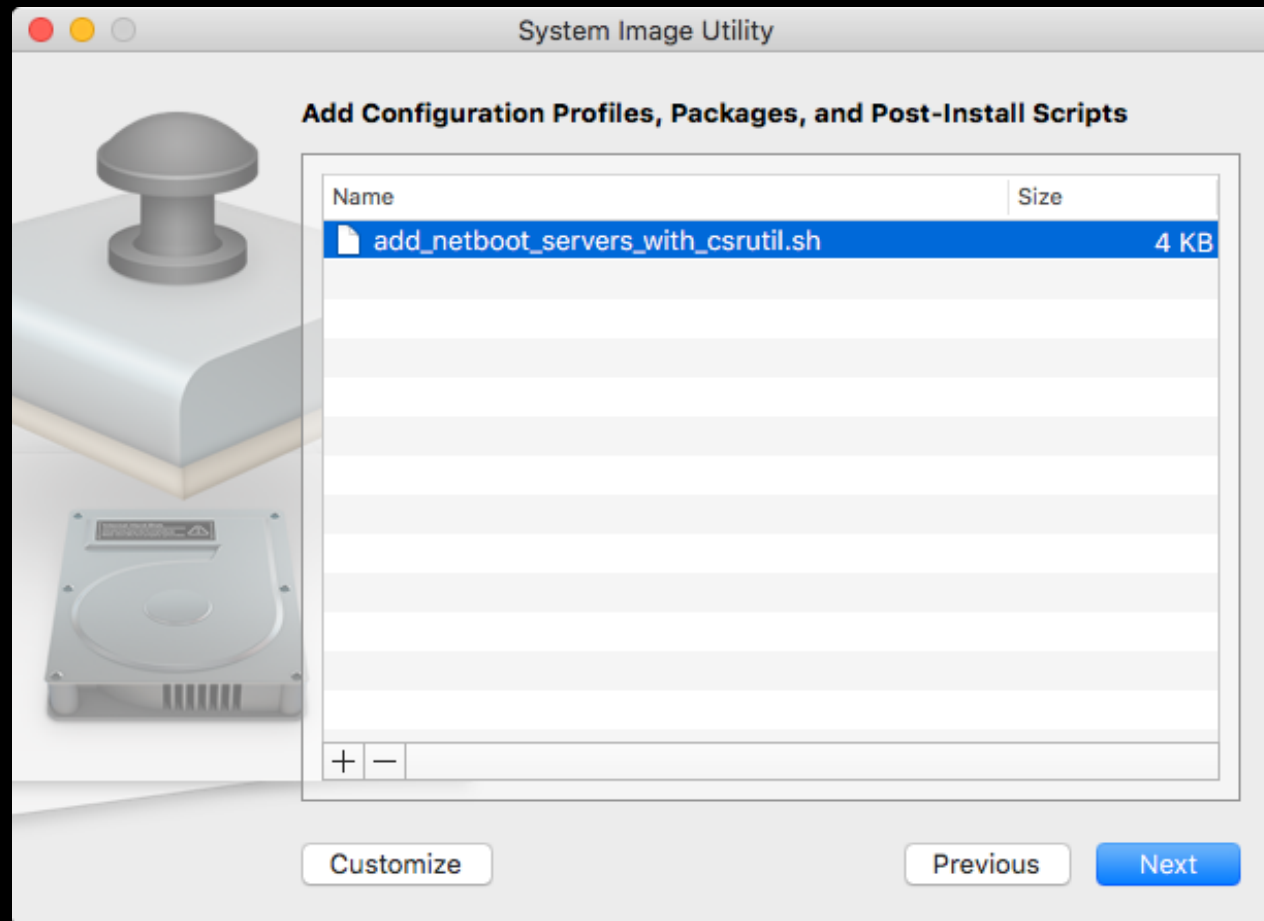
Configuring SLP without Recovery

```
#!/bin/bash
```

```
/usr/bin/csrutil netboot add 10.10.10.100
```

```
/usr/bin/csrutil netboot add 10.10.10.101
```

Configuring SLP without Recovery





Mac HD

username — -bash — 47x7

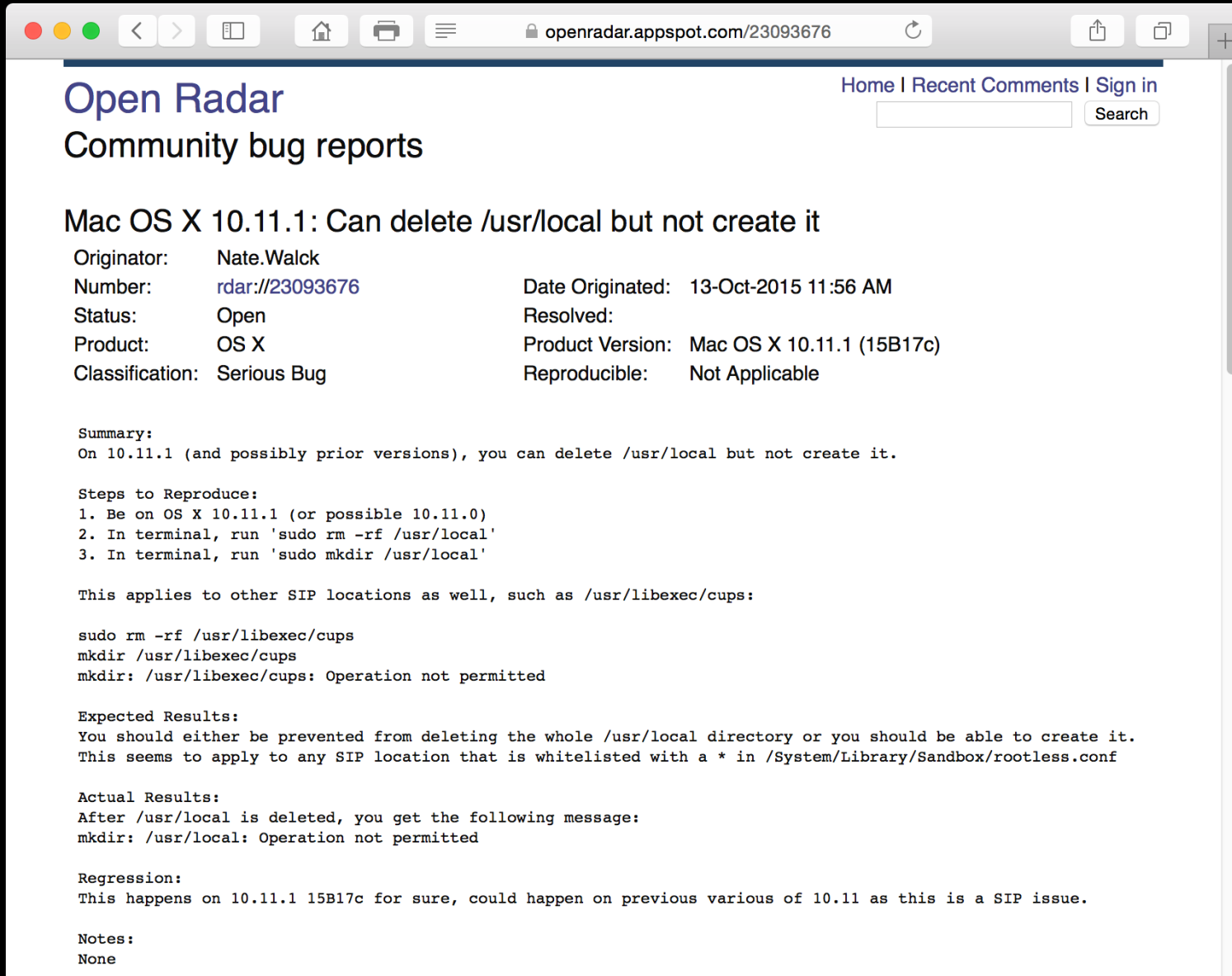
computername:~ username\$



SIP: Work in Progress



SIP: Work in Progress



The screenshot shows a web browser window with the address bar displaying `openradar.appspot.com/23093676`. The page title is "Open Radar" and the subtitle is "Community bug reports". In the top right corner, there are links for "Home", "Recent Comments", and "Sign in", along with a search bar. The main content area displays a bug report for "Mac OS X 10.11.1: Can delete /usr/local but not create it". The report includes fields for Originator (Nate.Walck), Number (rdar://23093676), Status (Open), Product (OS X), Classification (Serious Bug), Date Originated (13-Oct-2015 11:56 AM), Resolved (empty), Product Version (Mac OS X 10.11.1 (15B17c)), and Reproducible (Not Applicable). The summary states: "On 10.11.1 (and possibly prior versions), you can delete /usr/local but not create it." The steps to reproduce are listed as: 1. Be on OS X 10.11.1 (or possible 10.11.0), 2. In terminal, run 'sudo rm -rf /usr/local', and 3. In terminal, run 'sudo mkdir /usr/local'. The report notes that this applies to other SIP locations as well, such as /usr/libexec/cups, and provides a terminal snippet showing the error "mkdir: /usr/libexec/cups: Operation not permitted". The expected results are that the user should be prevented from deleting the whole /usr/local directory or should be able to create it. The actual results show that after deleting /usr/local, the user gets the message "mkdir: /usr/local: Operation not permitted". The regression section states that this happens on 10.11.1 15B17c for sure, but could happen on previous versions of 10.11 as this is a SIP issue. The notes section is empty.

Open Radar
Community bug reports

Home | Recent Comments | Sign in

Search

Mac OS X 10.11.1: Can delete /usr/local but not create it

Originator: Nate.Walck
Number: [rdar://23093676](#)
Status: Open
Product: OS X
Classification: Serious Bug

Date Originated: 13-Oct-2015 11:56 AM
Resolved:
Product Version: Mac OS X 10.11.1 (15B17c)
Reproducible: Not Applicable

Summary:
On 10.11.1 (and possibly prior versions), you can delete /usr/local but not create it.

Steps to Reproduce:
1. Be on OS X 10.11.1 (or possible 10.11.0)
2. In terminal, run 'sudo rm -rf /usr/local'
3. In terminal, run 'sudo mkdir /usr/local'

This applies to other SIP locations as well, such as /usr/libexec/cups:

```
sudo rm -rf /usr/libexec/cups
mkdir /usr/libexec/cups
mkdir: /usr/libexec/cups: Operation not permitted
```

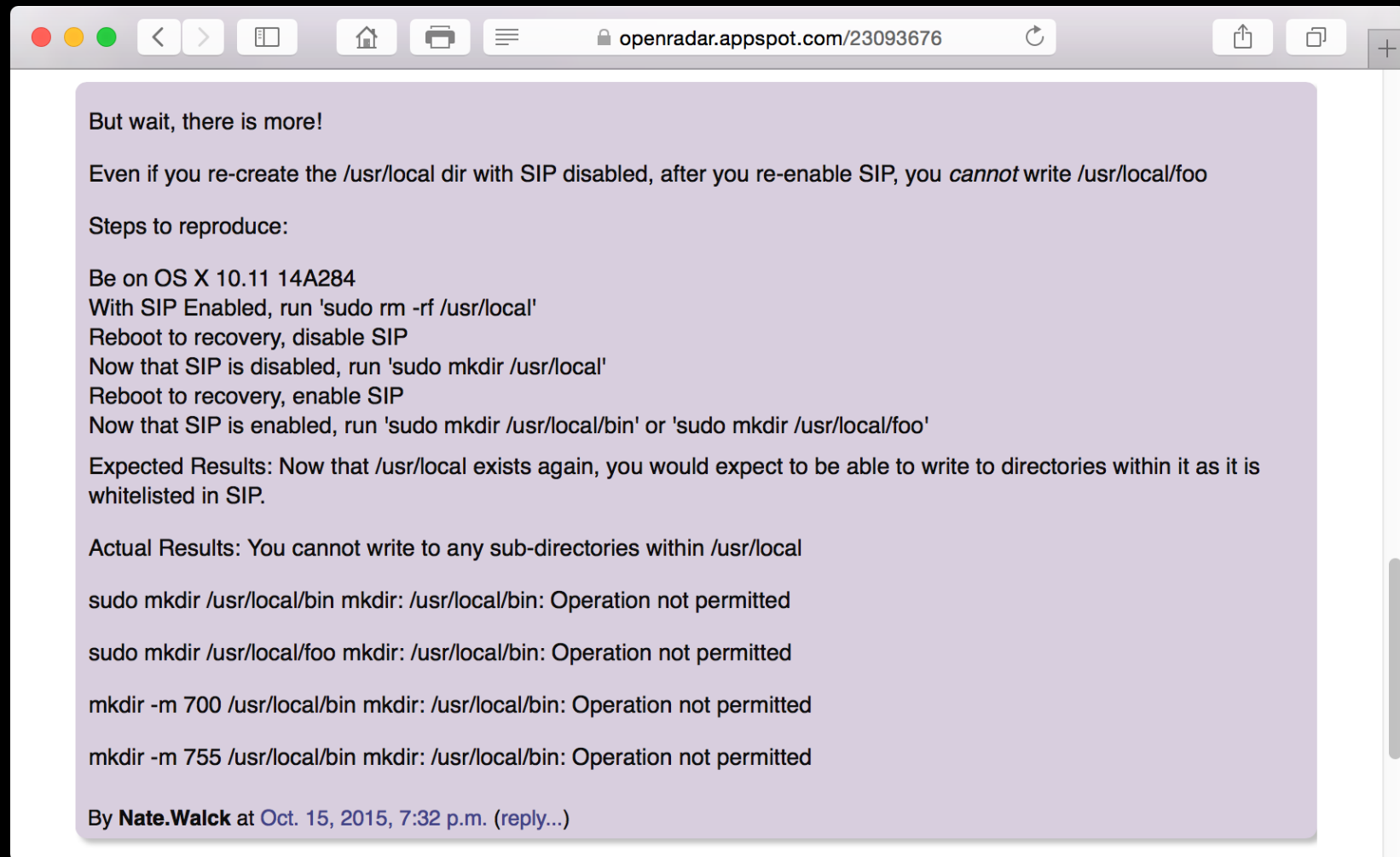
Expected Results:
You should either be prevented from deleting the whole /usr/local directory or you should be able to create it. This seems to apply to any SIP location that is whitelisted with a * in /System/Library/Sandbox/rootless.conf

Actual Results:
After /usr/local is deleted, you get the following message:
mkdir: /usr/local: Operation not permitted

Regression:
This happens on 10.11.1 15B17c for sure, could happen on previous versions of 10.11 as this is a SIP issue.

Notes:
None

SIP: Work in Progress



<https://openradar.appspot.com/23093676>

Useful Links

- ✦ The Fight For Root: <https://medium.com/@FredericJacobs/the-fight-for-root-13934b12e831>
- ✦ System Integrity Protection – Adding another layer to Apple's security model: <https://derflounder.wordpress.com/2015/10/01/system-integrity-protection-adding-another-layer-to-apples-security-model/>
- ✦ System Integrity Protection and resetting NVRAM: <https://derflounder.wordpress.com/2015/09/21/system-integrity-protection-and-resetting-nvram/>
- ✦ About System Integrity Protection on your Mac: <https://support.apple.com/en-us/HT204899>
- ✦ System Integrity Protection (a.k.a. Rootless): <http://mjtsai.com/blog/2015/07/12/system-integrity-protection-a-k-a-rootless/>

Useful Links

- NetBoot, NetInstall, and NetRestore requirements in OS X El Capitan: <https://support.apple.com/HT205054>
- NetBooting and System Integrity Protection: <https://derflounder.wordpress.com/2015/09/05/netbooting-and-system-integrity-protection/>
- Analysis of the Use of the Boot Server Discovery Protocol in NetBoot: <https://static.afp548.com/mactips/bootpd.html>
- Helper Addresses: <http://www.ciscopress.com/articles/article.asp?p=330807&seqNum=9>
- Setting Up Network Environment for NetBoot Server: <http://kb.parallels.com/en/118518>

Downloads

PDF available from the following link:

<http://tinyurl.com/MT2015SecurityPDF>

Keynote slides available from the
following link:

<http://tinyurl.com/MT2015SecurityKeynote>