🎅 Malware Blacklisting Tool

IT: (212) 555 – 1212

For macOS

Admin Guide for Santa

Common interactions to address concerns for Santa binary white/blacklisting tool

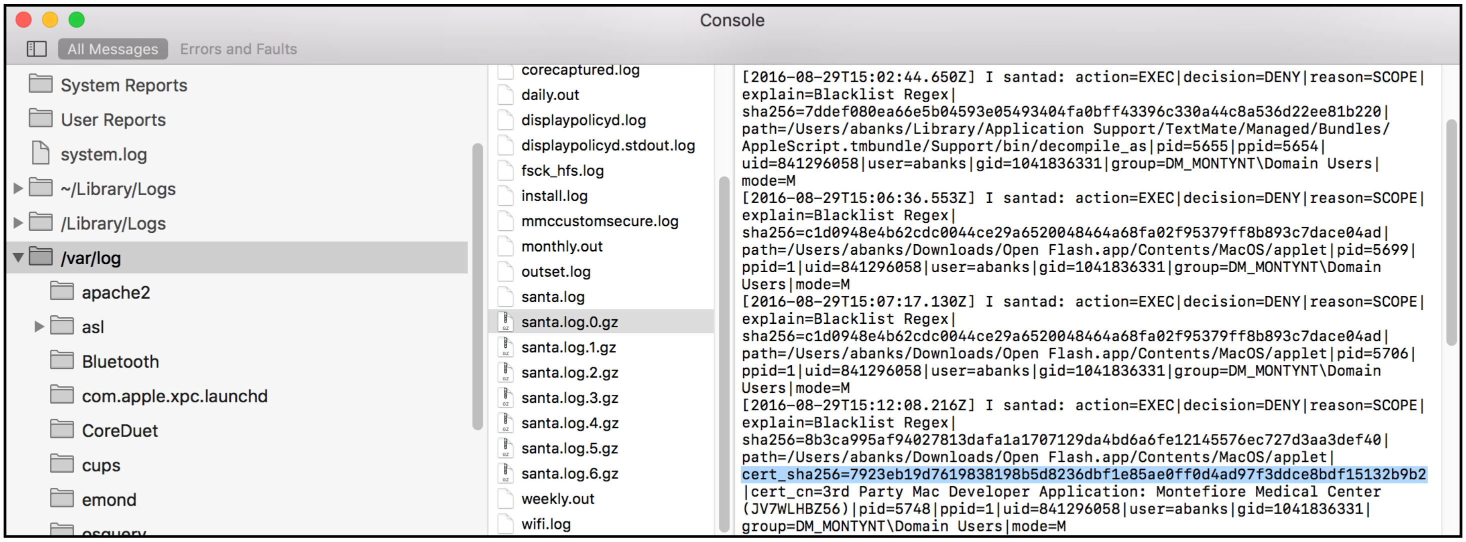
---

We are (<date>) rolling out Santa app blacklisting tool, first by stopping users from launching apps from their home folders, then by only allowing the launch of whitelisted apps. The goal is to stop ransomware or other badware from ever being launched in the first place.

You should understand the app from the customers perspective, but there's a separate intranet document for that. More importantly, for details about how 🎅 rules work and its operation, please review this article: https://www.afp548.com/2016/09/06/proactive-mac-security-santa

When we get a call/report from a customer that they tried to use a ***legitimate*** app and were blocked, please check with <Approval People> that you have the go-ahead based on business-use case approval, and that the app is/will be loaded into Munki.

The dialog that appears telling customers an app is blocked allows them to mute further notifications for 24 hours, they don't need it visible and screenshots don't help. The quickest method is to 1. screenshare w/ the computer 2. open /var/log/santa.log in Console and filter by DENY. ***If you do not see a cert_sha256= field in the logline, 🚧 STOP! 🚧***
An app without a cert will be a pain to update/maintain - an alternative should be found.



```
[2016-08-29T15:02:44.650Z] I santad: action=EXEC|decision=DENY|reason=SCOPE|
explain=Blacklist Regex|
sha256=7ddef080ea66e5b04593e05493404fa0bff43396c330a44c8a536d22ee81b220|
path=/Users/abanks/Library/Application Support/TextMate/Managed/Bundles/
AppleScript.tmbundle/Support/bin/decompile_as|pid=5655|ppid=5654|
uid=841296058|user=abanks|gid=1041836331|group=DM_MONTYNT\Domain Users|
mode=M
[2016-08-29T15:06:36.553Z] I santad: action=EXEC|decision=DENY|reason=SCOPE|
explain=Blacklist Regex|
sha256=c1d0948e4b62cdc0044ce29a6520048464a68fa02f95379ff8b893c7dace04ad|
path=/Users/abanks/Downloads/Open Flash.app/Contents/MacOS/applet|pid=5699|
ppid=1|uid=841296058|user=abanks|gid=1041836331|group=DM_MONTYNT\Domain
Users|mode=M
[2016-08-29T15:07:17.130Z] I santad: action=EXEC|decision=DENY|reason=SCOPE|
explain=Blacklist Regex|
sha256=c1d0948e4b62cdc0044ce29a6520048464a68fa02f95379ff8b893c7dace04ad|
path=/Users/abanks/Downloads/Open Flash.app/Contents/MacOS/applet|pid=5706|
ppid=1|uid=841296058|user=abanks|gid=1041836331|group=DM_MONTYNT\Domain
Users|mode=M
[2016-08-29T15:12:08.216Z] I santad: action=EXEC|decision=DENY|reason=SCOPE|
explain=Blacklist Regex|
sha256=8b3ca995af94027813dafa1a1707129da4bd6a6fe12145576ec727d3aa3def40|
path=/Users/abanks/Downloads/Open Flash.app/Contents/MacOS/applet|
cert_sha256=7923eb19d7619838198b5d8236dbf1e85ae0ff0d4ad97f3ddce8bdf15132b9b2
|cert_cn=3rd Party Mac Developer Application: Montefiore Medical Center
(JV7WLHBZ56)|pid=5748|ppid=1|uid=841296058|user=abanks|gid=1041836331|
group=DM_MONTYNT\Domain Users|mode=M
```

Copy the 'path' and 'cert_sha256' sections, and record/send to the Santa admin:

In Terminal, run the following command, pasting just the <certsha256> where shown:

```
$ sudo santactl rule --whitelist --certificate --sha256 <paste>
Password:
Added rule for SHA-256:
062e73a81e5b9f72e363e59f664f7462e42769d9946fe6cf9b56dab7ca760848
```

This will take effect immediately.

To Disable Controls (If approved/for troubleshooting)

To turn off the path-based blacklisting, run the following command:

```
sudo defaults delete /var/db/santa/config.plist BlacklistRegex
```

(Re-enable with `sudo defaults write /var/db/santa/config.plist BlacklistRegex "'^(?:/Users)/.*'"`

When active, turn off LOCKDOWN mode by running the following command:

```
sudo defaults write /var/db/santa/config.plist ClientMode -int 1
```

(Re-enable with `sudo defaults write /var/db/santa/config.plist ClientMode -int 2`

You can also TEMPORARILY disable 🎅 with the following command:

```
sudo launchctl unload /Library/LaunchDaemons/com.google.santad.plists
```