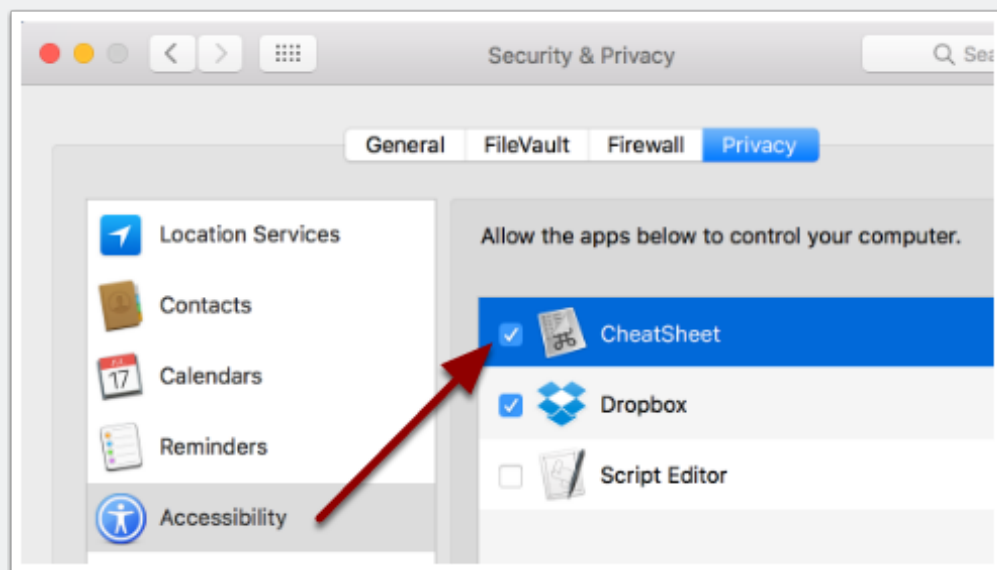


How To Edit The SIP Protected TCC.db File On macOS Sierra 10.12.2 And Later

NOTE: This guide requires macOS Sierra 10.12.2 or later. A command for disabling SIP was added in macOS Sierra 10.12.2 to re enable SIP without the need for booting to the recovery disk. That command is: `csrutil clear`

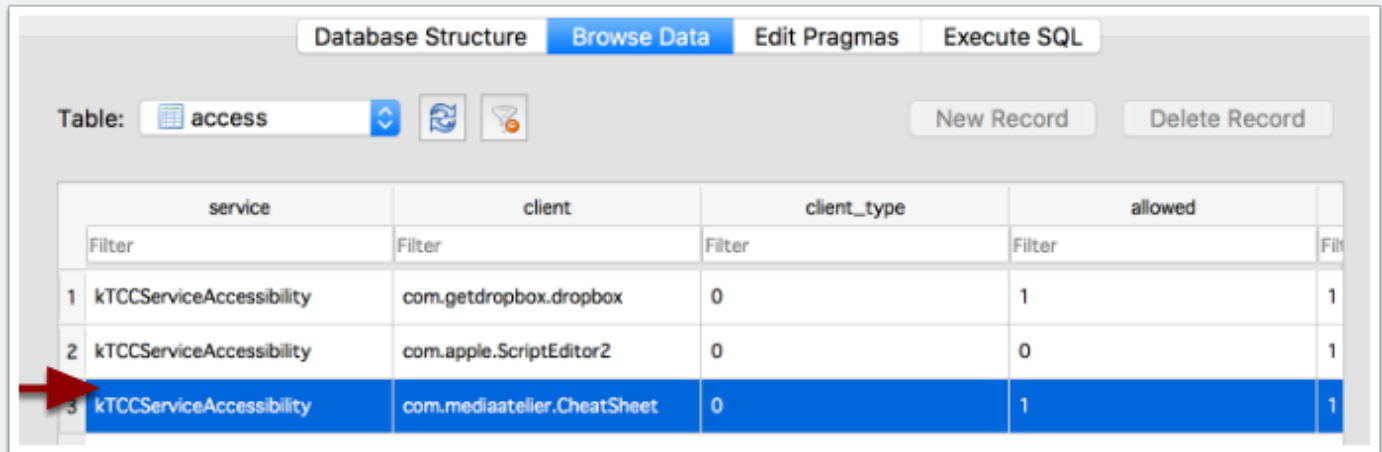
I needed a way to edit the TCC.db file but it is protected by System Integrity Protection (SIP). This means the file cannot be written to even by the root user. The TCC.db stores settings that allow or deny an application to control your computer. I needed to install a program called "CheatSheet" for a client and the program prompts the user for admin credentials to have it allow the app to control the computer. I needed a way to avoid the users getting this prompt. The picture below shows the checkbox that needed to be enabled for the CheatSheet application.



Step 1. I enabled the checkbox manually for CheatSheet, then I used a program called "DB Browser for SQLite" to view the TCC.db file which is located at: `/Library/`

How To Edit The SIP Protected TCC.db File On macOS Sierra 10.12.2 And Later

Application Support/com.apple.TCC. This allowed me to see the items that get written to the TCC.db database.



Database Structure | Browse Data | Edit Pragmas | Execute SQL

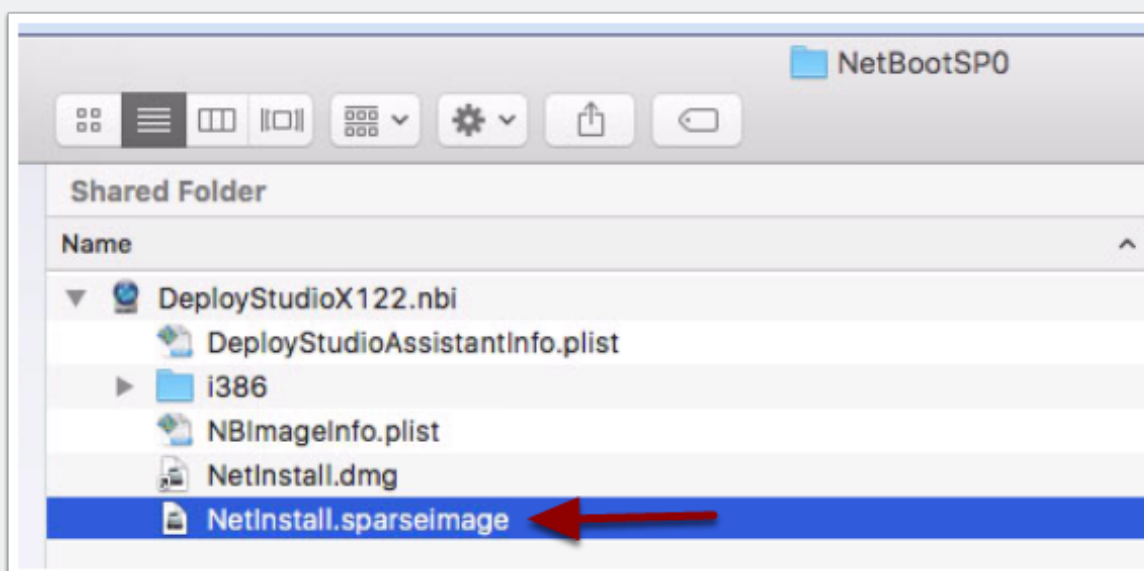
Table: **access** [Icons] [New Record] [Delete Record]

	service	client	client_type	allowed	
	Filter	Filter	Filter	Filter	Filter
1	kTCCServiceAccessibility	com.getdropbox.dropbox	0	1	1
2	kTCCServiceAccessibility	com.apple.ScriptEditor2	0	0	1
3	kTCCServiceAccessibility	com.mediaatelier.CheatSheet	0	1	1

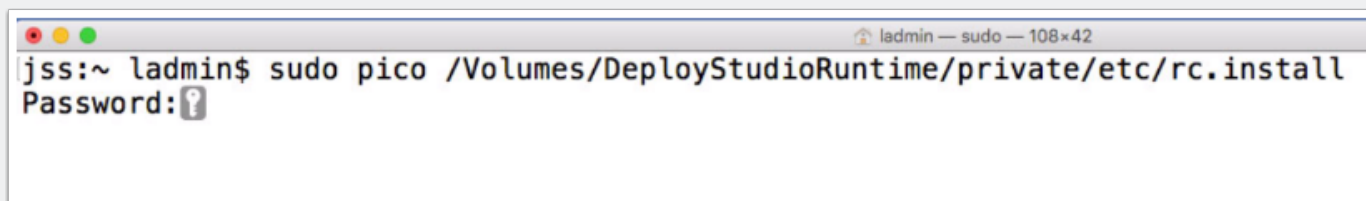
How To Edit The SIP Protected TCC.db File On macOS Sierra 10.12.2 And Later

Step 2. In order to disable SIP, you need to boot into Recovery Mode. I needed a way to disable SIP during the imaging process, then edit the TCC.db file to enable the checkbox for CheatSheet, then re enable SIP. I needed to get all of this done before the first login to the Mac. I had a DeployStudio Netboot server setup at this client.

Since the DeployStudio Netboot Set is a NetInstall.sparseimage, It's very similar to booting into Recovery Mode. On the DeployStudio Server, I went to /Library/NetBoot/NetBooSP0, then I mounted the "NetInstall.sparseimage" to have a look at the "rc.install" file.



Step 3. I opened "Terminal.app" then entered the following command: `sudo pico /Volumes/DeployStudioRuntime/private/etc/rc.install`. When prompted, I entered my admin password.



How To Edit The SIP Protected TCC.db File On macOS Sierra 10.12.2 And Later

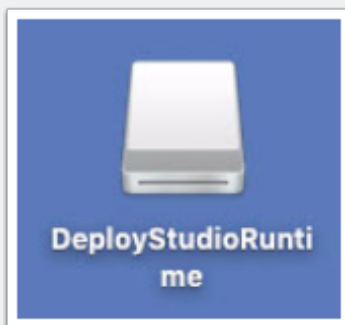
Step 4. The "rc.install" file is used during the DeployStudio Netboot process. I added: /usr/bin/csrutil disable to the "rc.install" file right before the "Launch DeployStudio Runtime" entry. Since the DeployStudio NetBoot image is actually a NetInstall image, the system thinks it's booted into Recovery Mode and will allow SIP to be disabled. I pressed the Control and X keys to save this file.

```
#
# Launch a VNC server
#
if [ -e /Library/Preferences/com.apple.
then
    launchctl load /System/Library/Launch/
fi

#
# Update Disk Utility preferences to di
#
defaults write com.apple.DiskUtility DU

# Disable SIP
/usr/bin/csrutil disable
#
# Launch DeployStudio Runtime
#
DS_APP="/Applications/Utilities/DeployS
```

Step 5. Unmount the "DeployStudioRuntime" from the Desktop.



How To Edit The SIP Protected TCC.db File On macOS Sierra 10.12.2 And Later

Step 6. I created a bash script that does the following:

- Launch "CheatSheet.app" - This needs to be done to create the TCC.db entry for CheatSheet. By default it's not checked.
- sleep 5 - This will pause the script for 5 seconds.
- Enter the sqlite3 command to enable the checkbox for CheatSheet - This is the info that I got in step 1 using "DB Browser for SQLite"
- sleep 5 - This will pause the script for 5 seconds.
- Re Enable SIP.

```
#!/bin/bash

/usr/bin/open /Applications/CheatSheet.app

sleep 5

#This will enable the Accessibility Setting for Cheat Sheet

/usr/bin/sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db "INSERT or REPLACE INTO access
VALUES('kTCCServiceAccessibility','com.mediaatelier.CheatSheet',0,1,1,NULL,NULL)"

sleep 5

#This will re enable SIP on 10.12.2 or later

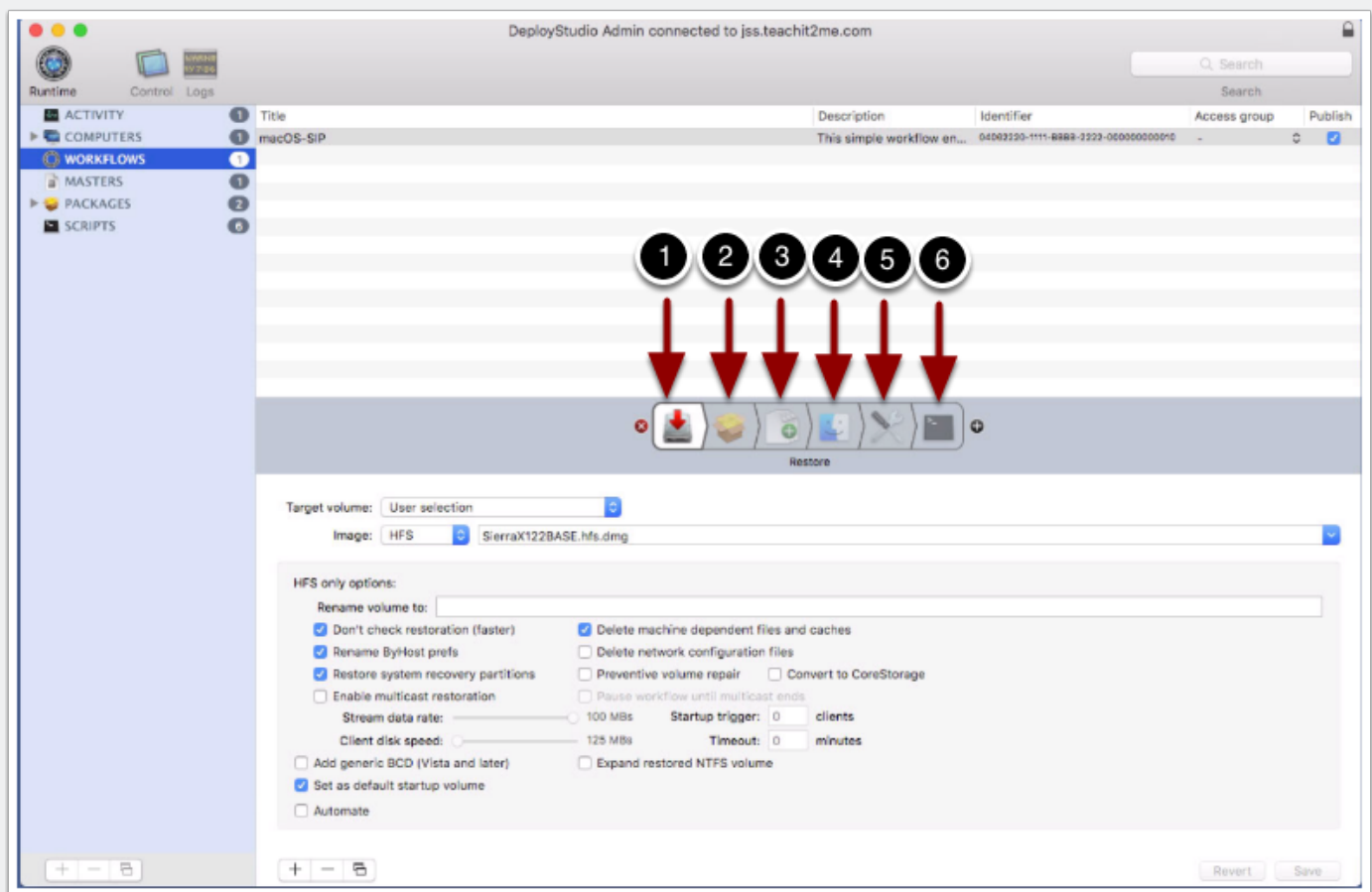
/usr/bin/csrutil clear
```

How To Edit The SIP Protected TCC.db File On macOS Sierra 10.12.2 And Later

Step 7. I created a workflow in DeployStudio that does the following:

1. Applies macOS Sierra BASE Image
2. Creates the first user
3. Puts the "CheatSheet" application in /Applications
4. Asks user to name the computer
5. Applies the computer name and disables the first run assistant.
6. Runs the script I created in step 6 on first boot.

NOTE: You can add as much to the workflow as you want but for this test I wanted to keep it simple.



How To Edit The SIP Protected TCC.db File On macOS Sierra 10.12.2 And Later

Step 8. How it all works.

Boot your Mac from the DeployStudio Netboot Set. This will disable SIP because of the edit we made the "rc.install" file.

Log in to DeployStudio and select the workflow.

Select the hard drive.

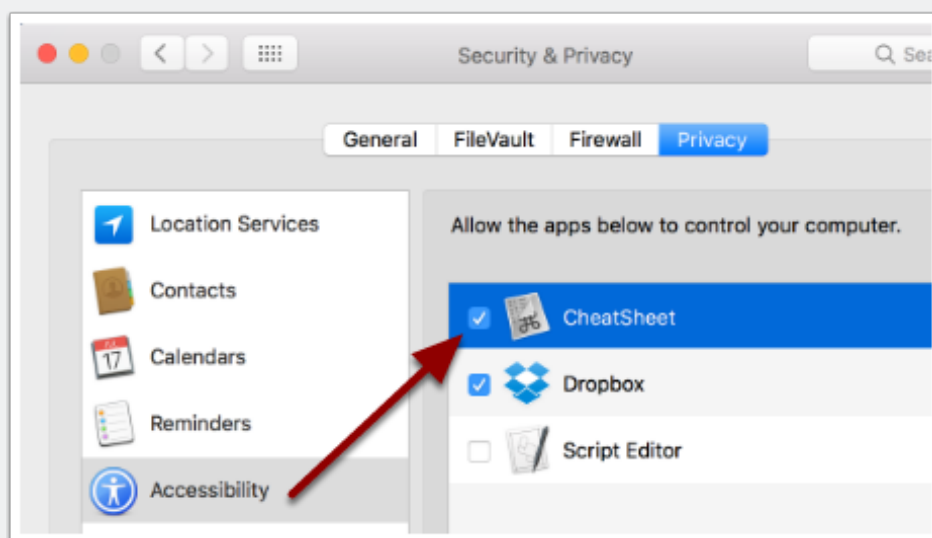
Name the computer when prompted.

Reboot the computer when prompted.

When the computer boots up, it will run the script that we added to the workflow. This script will silently launch the CheatSheet app to create the TCC.db database entry, then it will run the sqlite command to edit the entry to the TCC.db for CheatSheet, once done, it will re enable SIP and reboot the computer.

How To Edit The SIP Protected TCC.db File On macOS Sierra 10.12.2 And Later

Step 9. Log in to the computer, then open "System Preferences" and select "Security & Privacy", select the "Privacy" tab then select "Accessibility". The CheatSheet application will be checked. Quit "System Preferences".



Step 10. Open "Terminal.app". Enter the following command: `csrutil status`. The SIP status will be enabled. We have successfully enabled and disabled SIP and edited the TCC.db before the first user login.

```
admin$ csrutil status
System Integrity Protection status: enabled.
```


How To Edit The SIP Protected TCC.db File On macOS Sierra 10.12.2 And Later

Step 11. More information on SIP and the TCC.db

The TCC.db was added to SIP because DropBox was editing the file and bypassing user permission. Users must approve permission for an application to control the computer. Apple saw that as a security risk so they added it to SIP.

To see a listing of everything that is protected by SIP, have a look at the "rootless.conf file": `/System/Library/Sandbox/rootless.conf`.

rootless.conf file defines an exception for the TCC system. (Allow file-write* (subpath (string-append home "/Library/Application Support/com.apple.TCC"))

See the seatbelt config at `/System/Library/Sandbox/Profiles/com.apple.tccd.sb`

This completes the how to guide.