Leveling Up

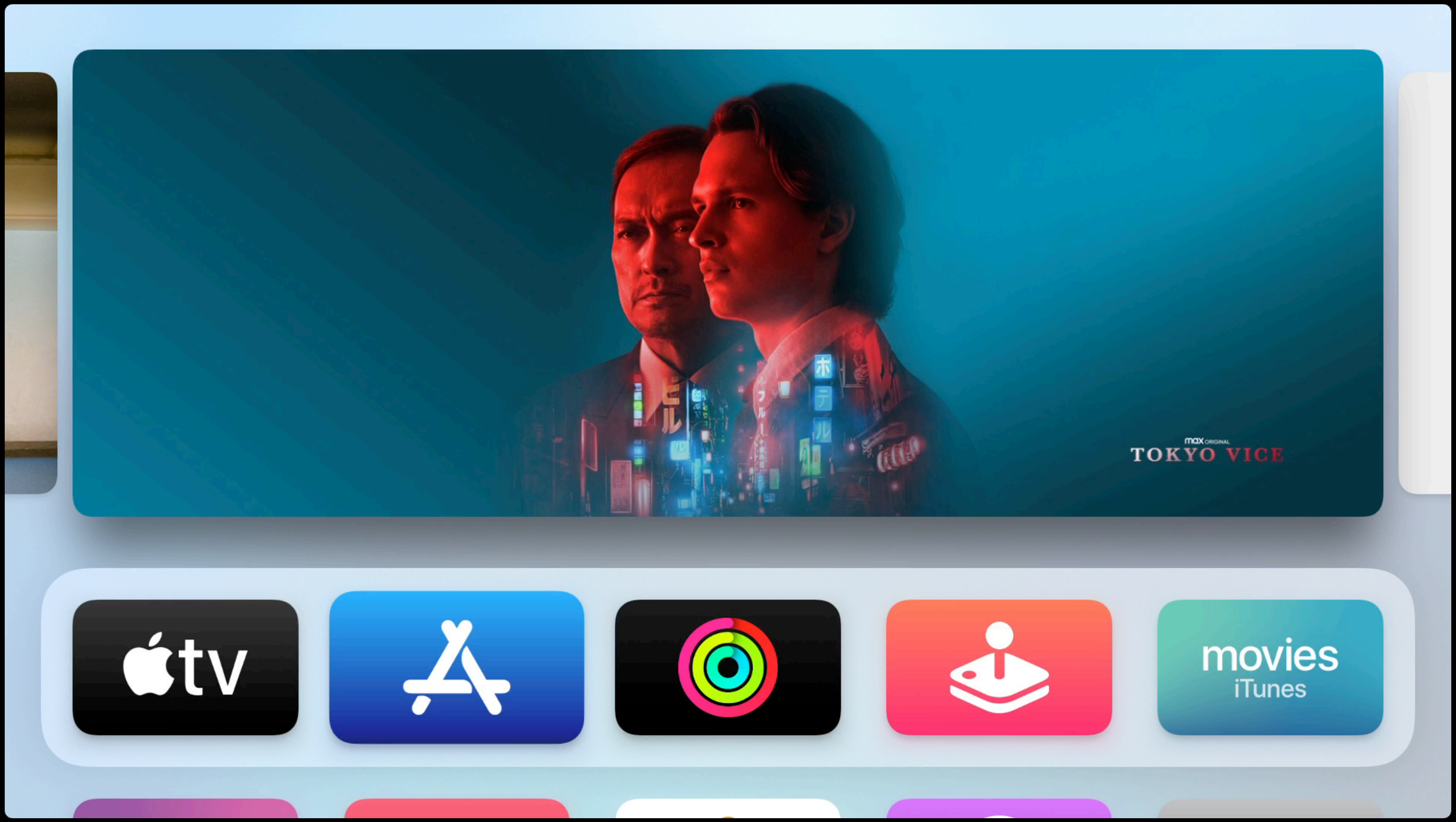
Managing admin rights in the enterprise

Rich Trouton

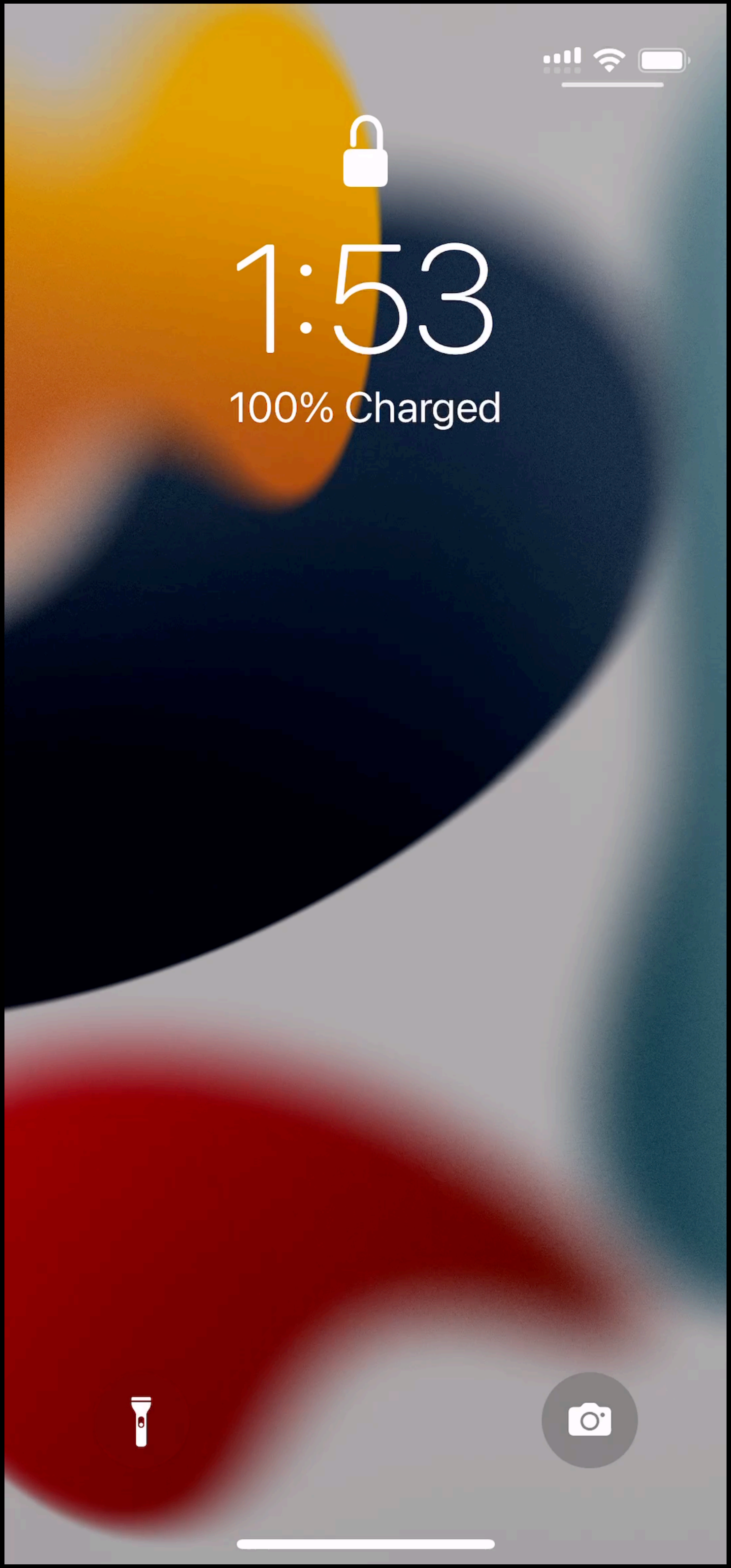
Mac CoE @ SAP

iPhone

tv
MENU

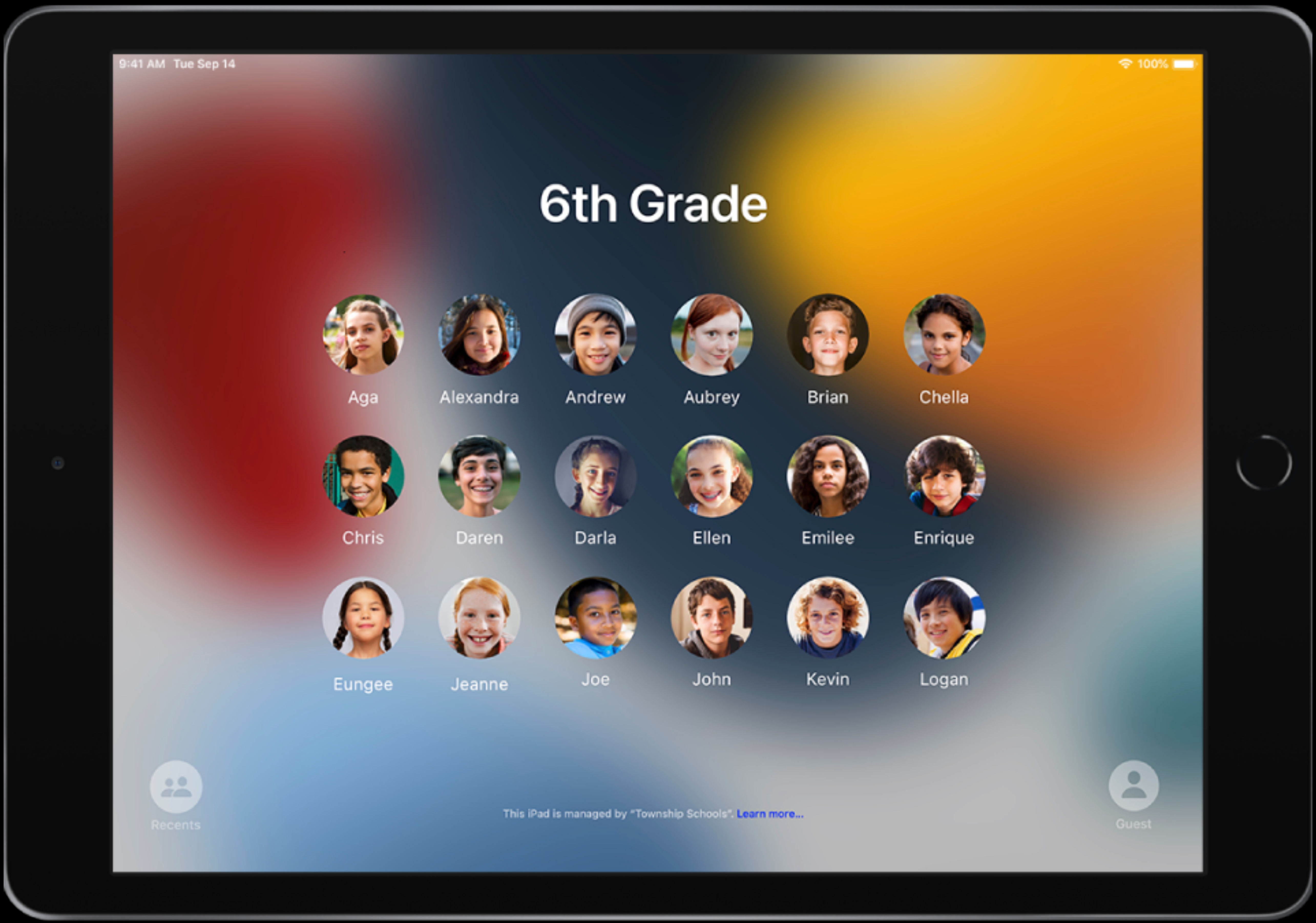

max ORIGINAL
TOKYO VICE
tv
movies
iTunes

Tue
9



1:53

100% Charged

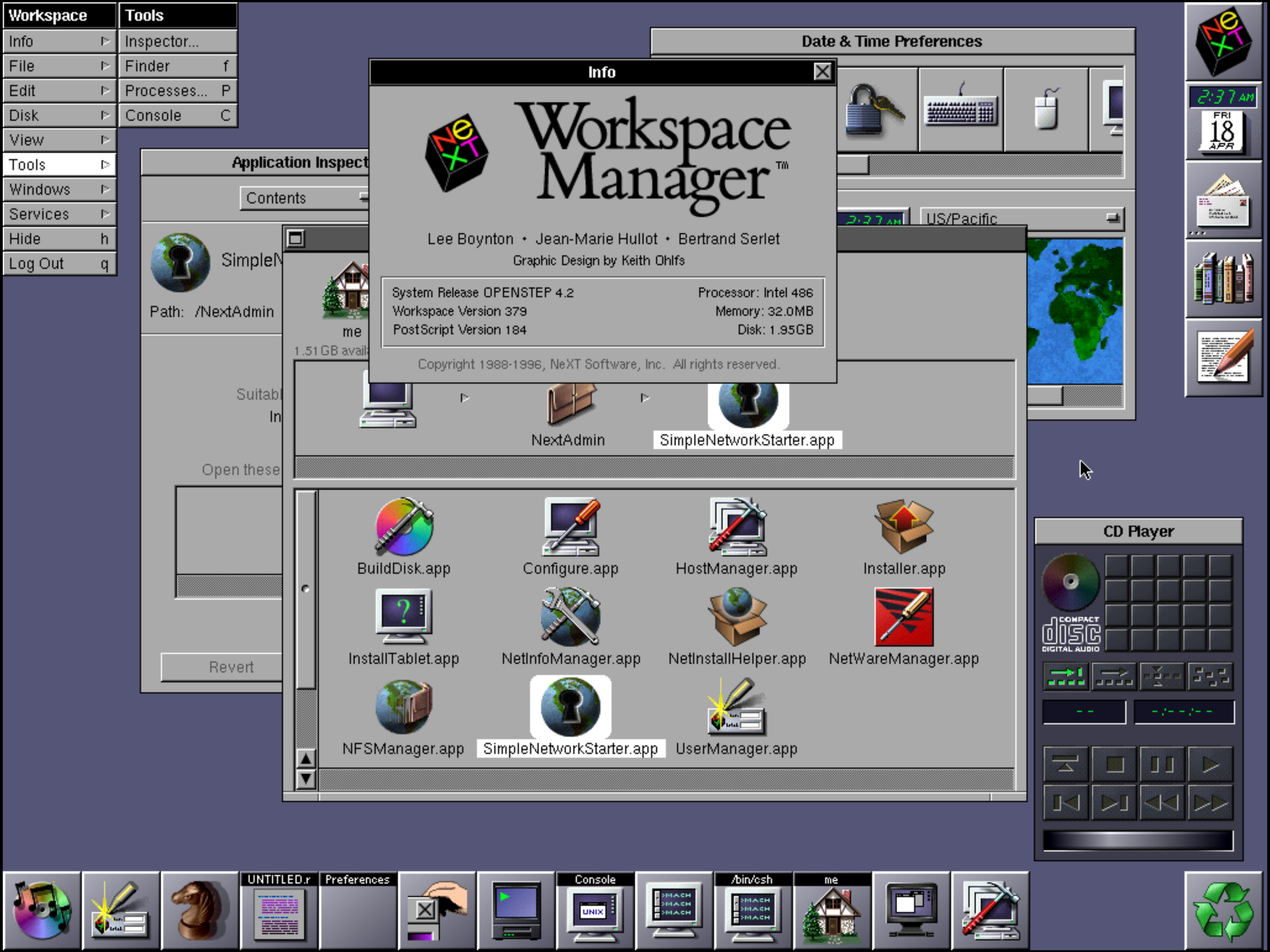


9:41 AM Tue Sep 14

6th Grade

This iPad is managed by "Township Schools". Learn more...

tv
MENU

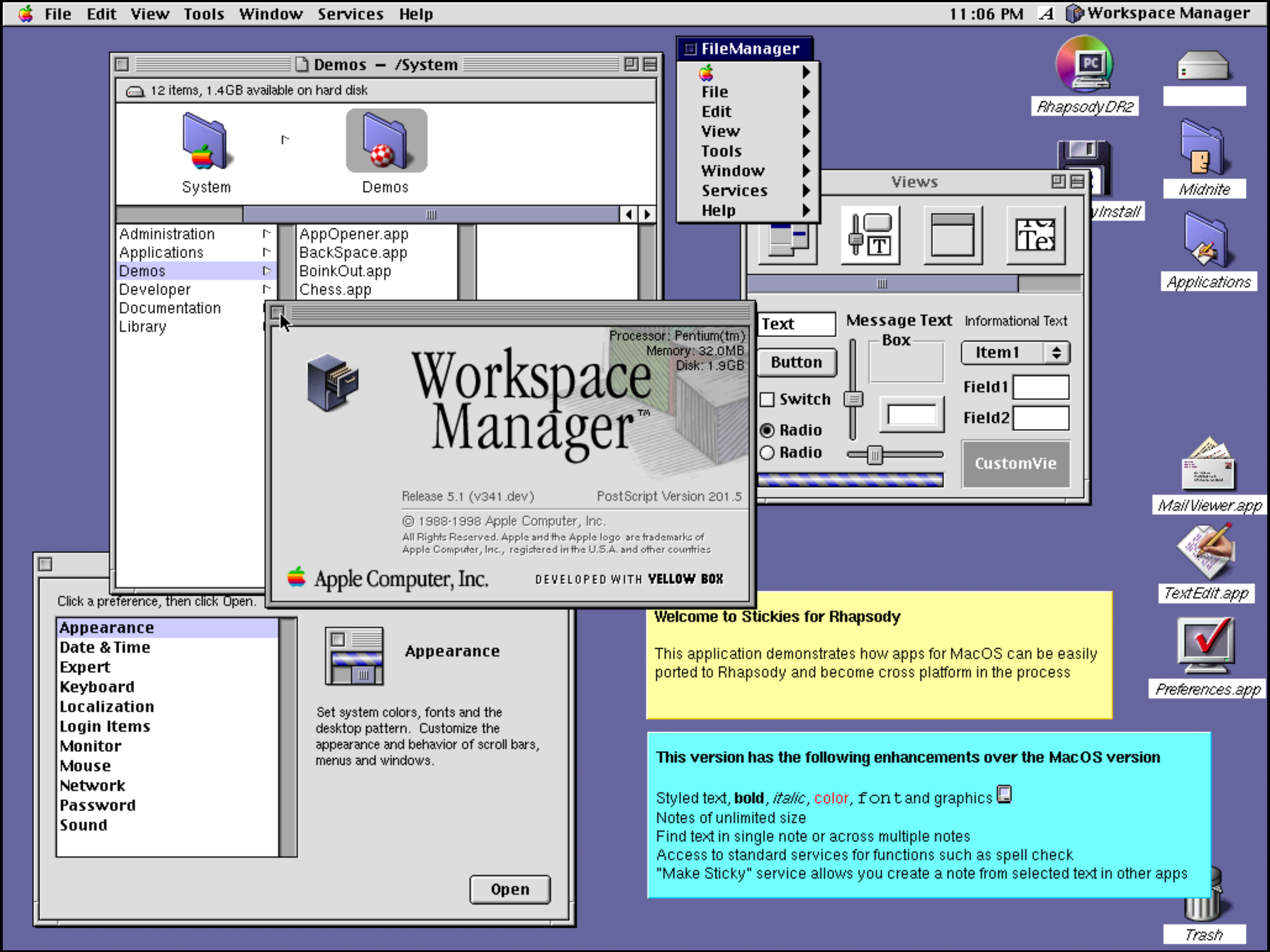


Info

Workspace Manager™

Lee Boynton • Jean-Marie Hullot • Bertrand Serlet
Graphic Design by Keith Ohlfs

```
System Release OPENSTEP 4.2          Processor: Intel 486
Workspace Version 379                Memory: 32.0MB
PostScript Version 184               Disk: 1.95GB
```



12 items, 1.4GB available on hard disk

Workspace Manager™

Processor: Pentium(tm)
Memory: 32.0MB
Disk: 1.9GB

Release 5.1 (v341.dev)   PostScript Version 201.5

© 1988-1998 Apple Computer, Inc.
All Rights Reserved. Apple and the Apple logo are trademarks of Apple Computer, Inc., registered in the U.S.A. and other countries

Apple Computer, Inc.   DEVELOPED WITH YELLOW BOX

Click a preference, then click Open.

Appearance

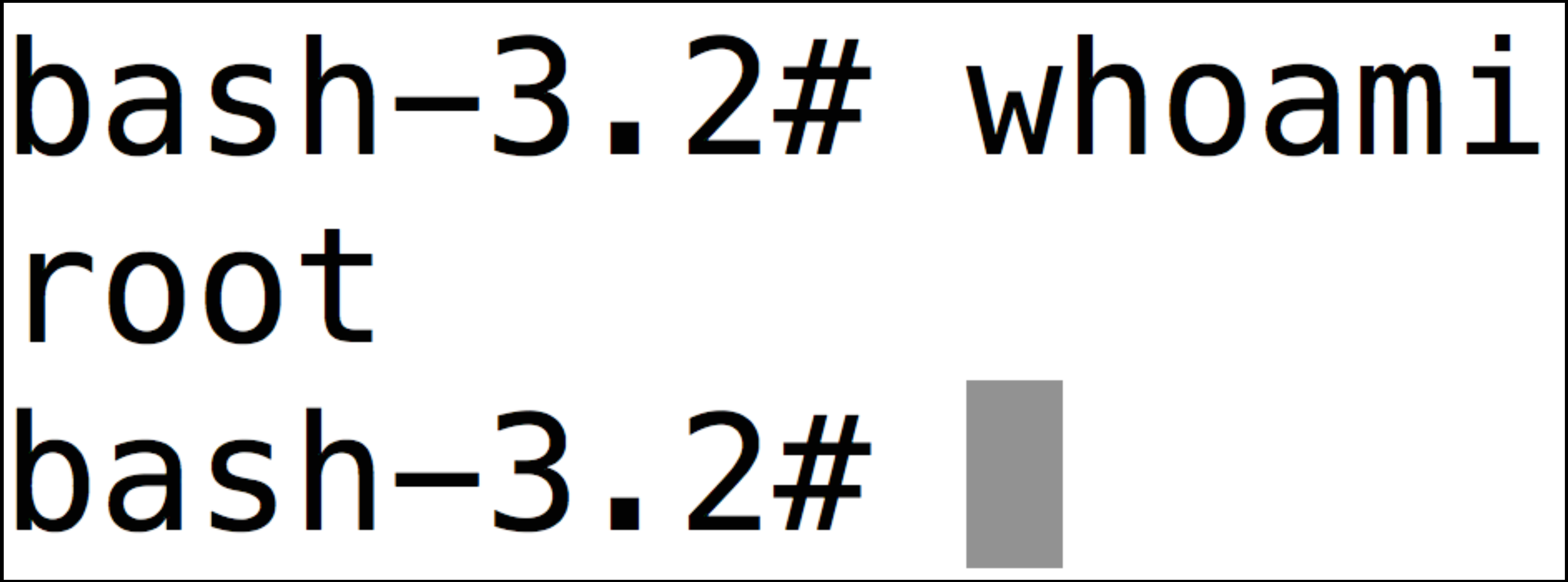
Set system colors, fonts and the desktop pattern. Customize the appearance and behavior of scroll bars, menus and windows.

Welcome to Stickies for Rhapsody

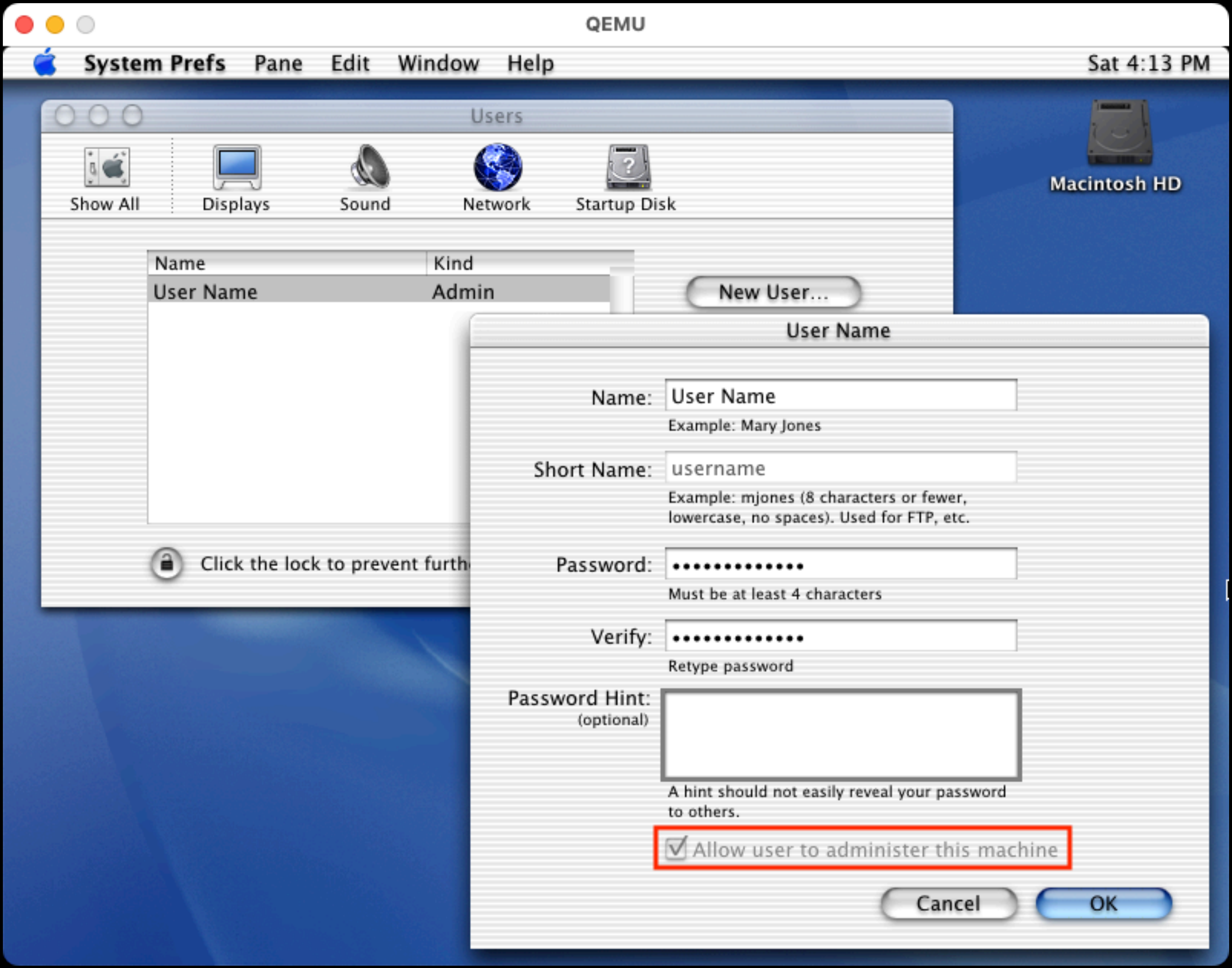
This application demonstrates how apps for MacOS can be easily ported to Rhapsody and become cross platform in the process

This version has the following enhancements over the MacOS version

Styled text, **bold**, *italic*, color, font and graphics
Notes of unlimited size
Find text in single note or across multiple notes
Access to standard services for functions such as spell check
"Make Sticky" service allows you create a note from selected text in other apps



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



Name	Kind
User Name	Admin

Click the lock to prevent furth

User Name

Name: User Name
Example: Mary Jones

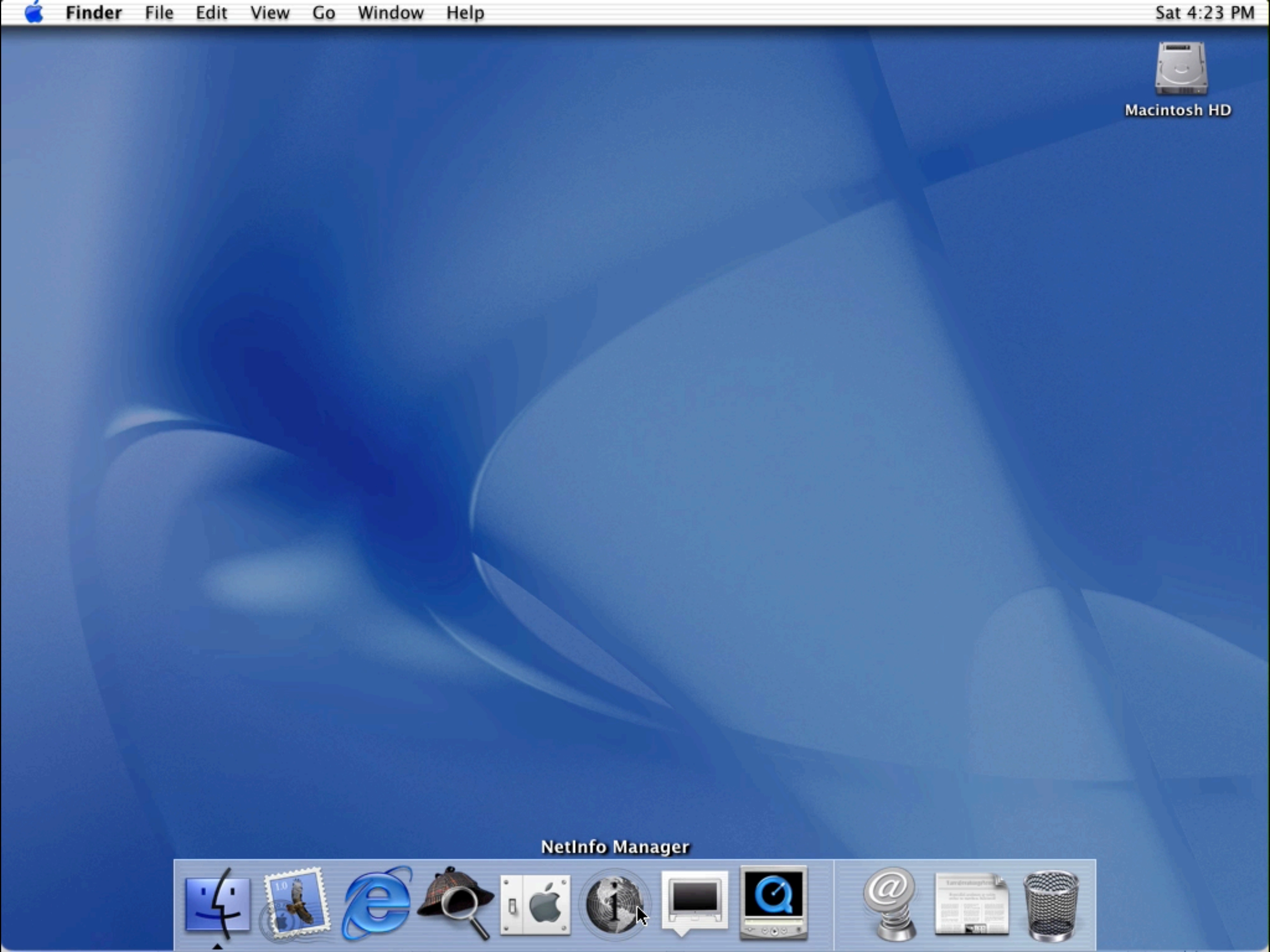
Short Name: username
Example: mjones (8 characters or fewer, lowercase, no spaces). Used for FTP, etc.

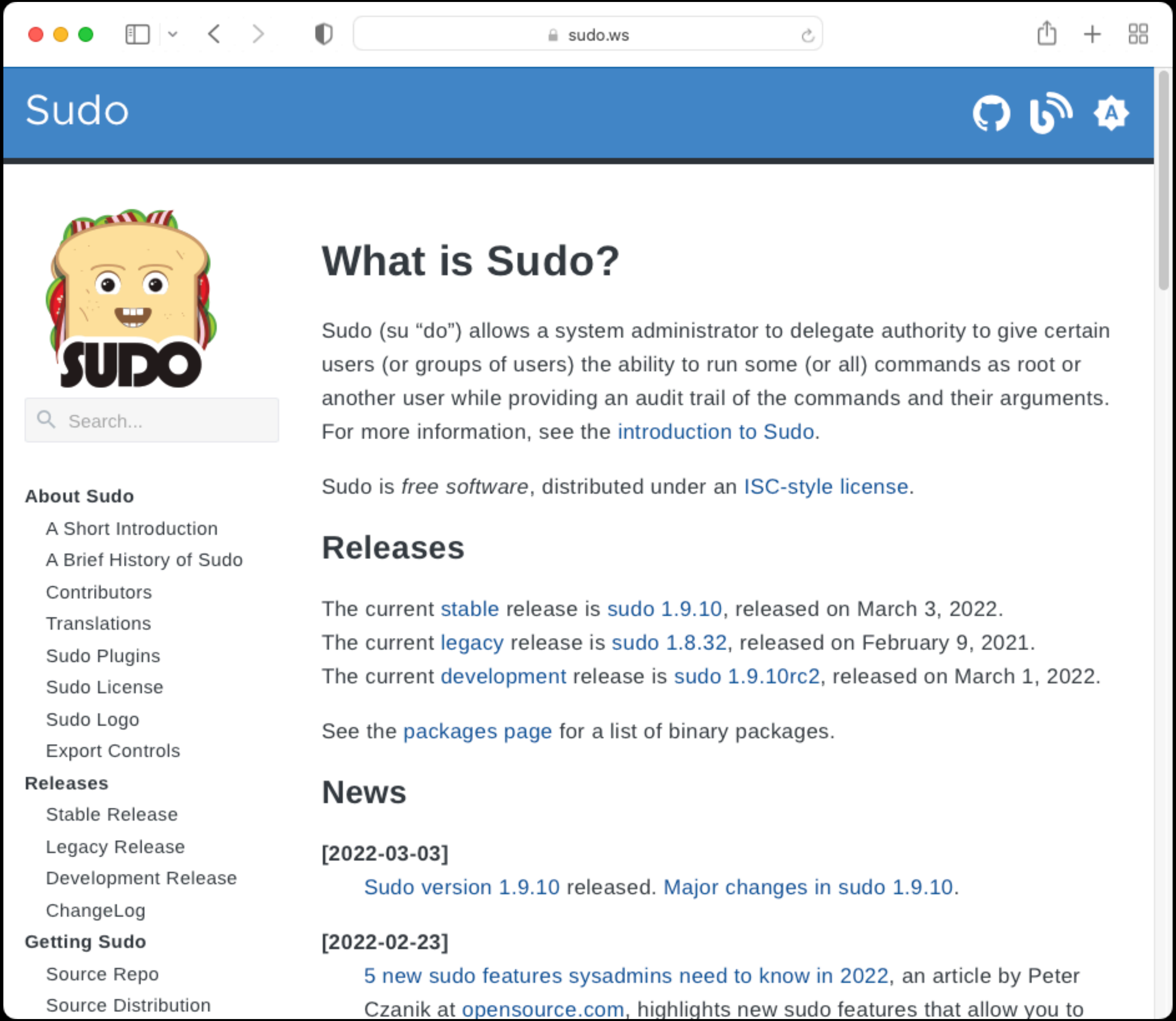
Password: •••••••••••••
Must be at least 4 characters

Verify: •••••••••••••
Retype password

Password Hint: (optional)
A hint should not easily reveal your password to others.

☑ Allow user to administer this machine


Finder
File
Edit
View
Go
Window
Help
Sat 4:23 PM
Macintosh HD
NetInfo Manager



What is Sudo?

Sudo (su "do") allows a system administrator to delegate authority to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while providing an audit trail of the commands and their arguments. For more information, see the introduction to Sudo.

Sudo is *free software*, distributed under an ISC-style license.

Releases

The current stable release is sudo 1.9.10, released on March 3, 2022.
The current legacy release is sudo 1.8.32, released on February 9, 2021.
The current development release is sudo 1.9.10rc2, released on March 1, 2022.

See the packages page for a list of binary packages.

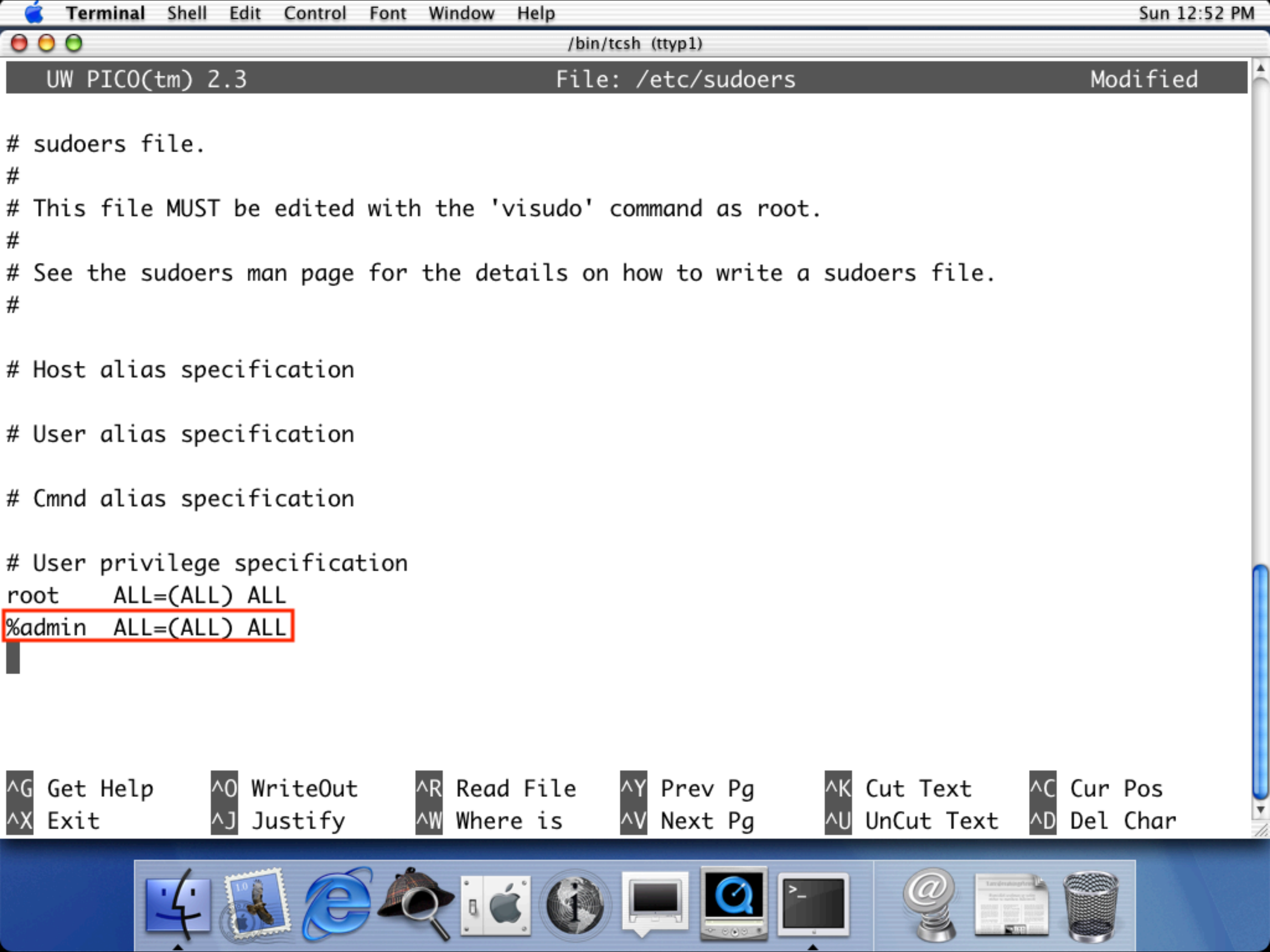
News

[2022-03-03]

Sudo version 1.9.10 released. Major changes in sudo 1.9.10.

[2022-02-23]

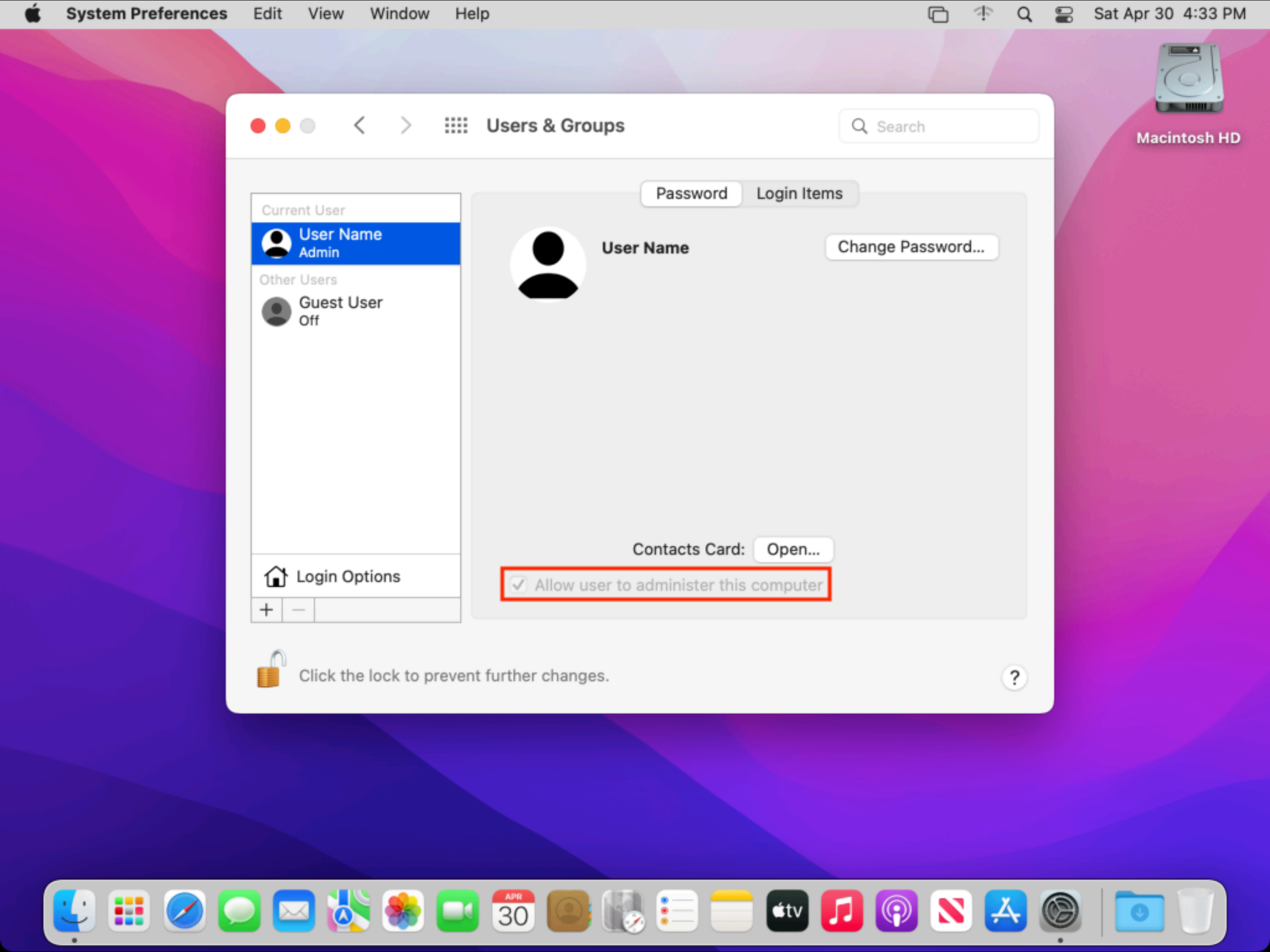
5 new sudo features sysadmins need to know in 2022, an article by Peter Czanik at opensource.com, highlights new sudo features that allow you to



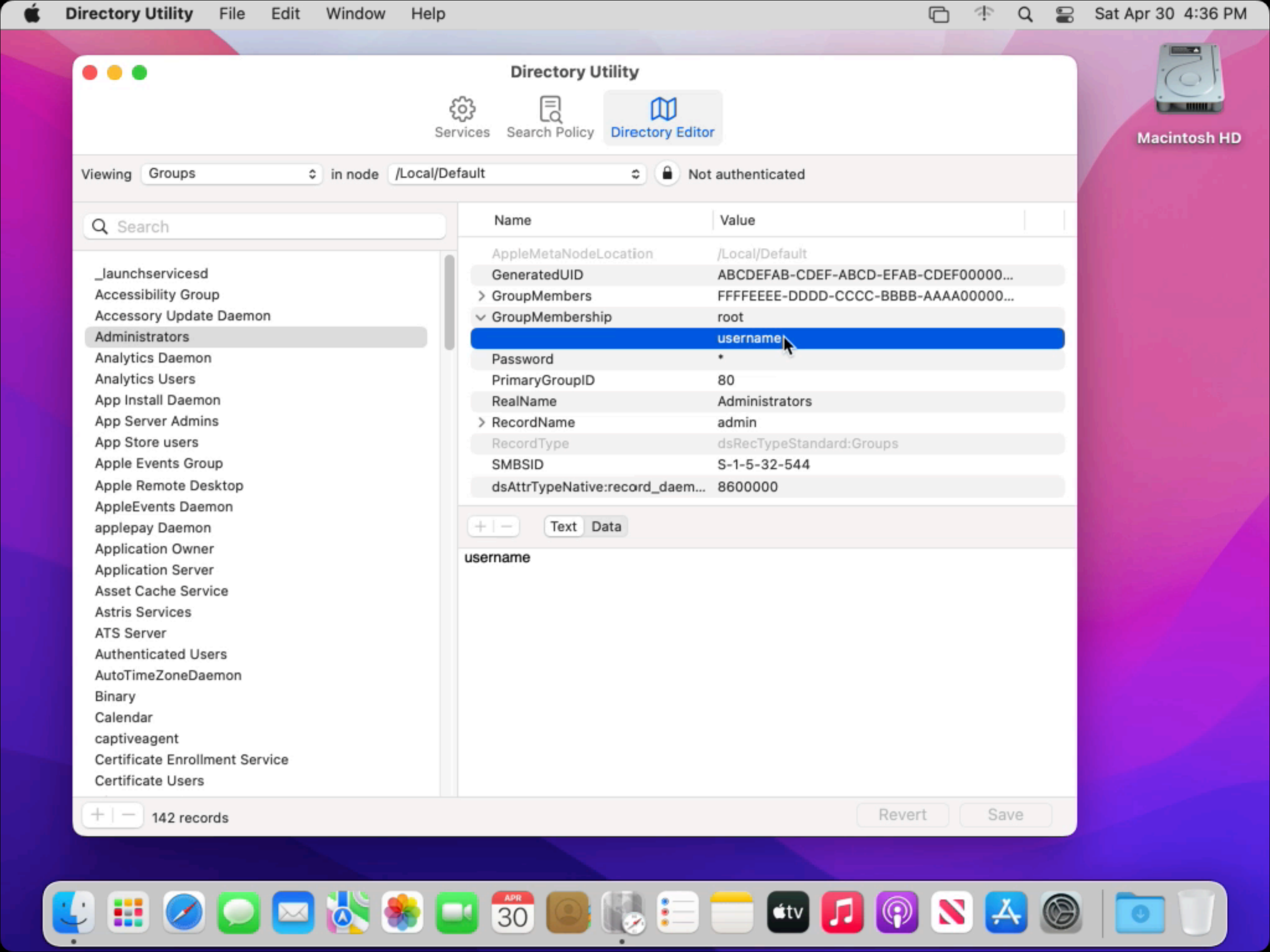
```
  UW PICO(tm) 2.3                  File: /etc/sudoers                  Modified

# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
#

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL
%admin  ALL=(ALL) ALL
```

Root Account

- 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



☑ Allow user to administer this computer



Directory Utility

Viewing Groups in node /Local/Default Not authenticated

Search

_launchservicesd
Accessibility Group
Accessory Update Daemon
Administrators
Analytics Daemon
Analytics Users
App Install Daemon
App Server Admins
App Store users
Apple Events Group
Apple Remote Desktop
AppleEvents Daemon
applepay Daemon
Application Owner
Application Server
Asset Cache Service
Astris Services
ATS Server
Authenticated Users
AutoTimeZoneDaemon
Binary
Calendar
captiveagent
Certificate Enrollment Service
Certificate Users

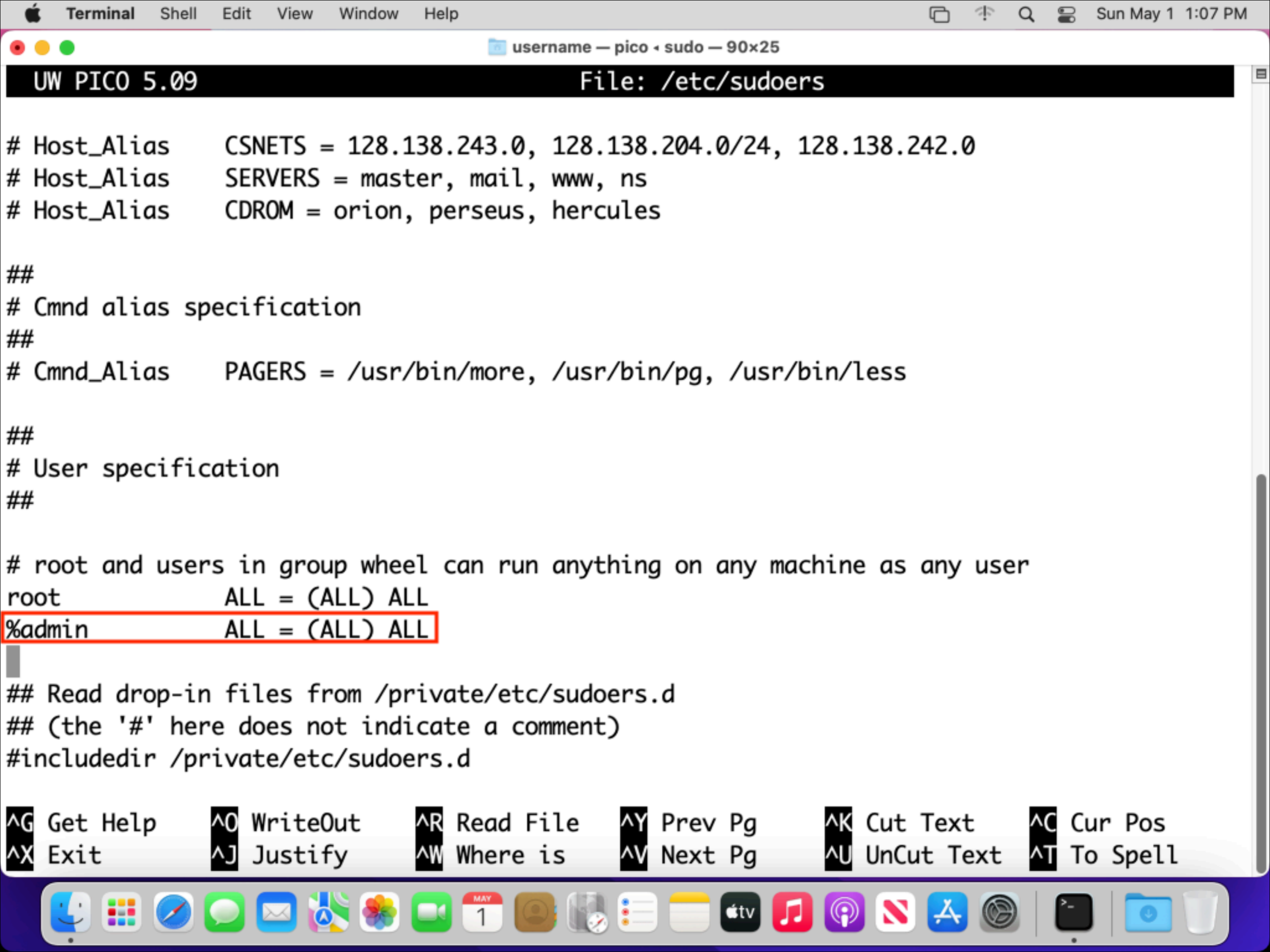
Name	Value
AppleMetaNodeLocation	/Local/Default
GeneratedUID	ABCDEFAB-CDEF-ABCD-EFAB-CDEF00000...
› GroupMembers	FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000...
⌄ GroupMembership	root
	username
Password	*
PrimaryGroupID	80
RealName	Administrators
› RecordName	admin
RecordType	dsRecTypeStandard:Groups
SMBSID	S-1-5-32-544
dsAttrTypeNative:record_daem...	8600000

Text Data

username

142 records

Revert Save

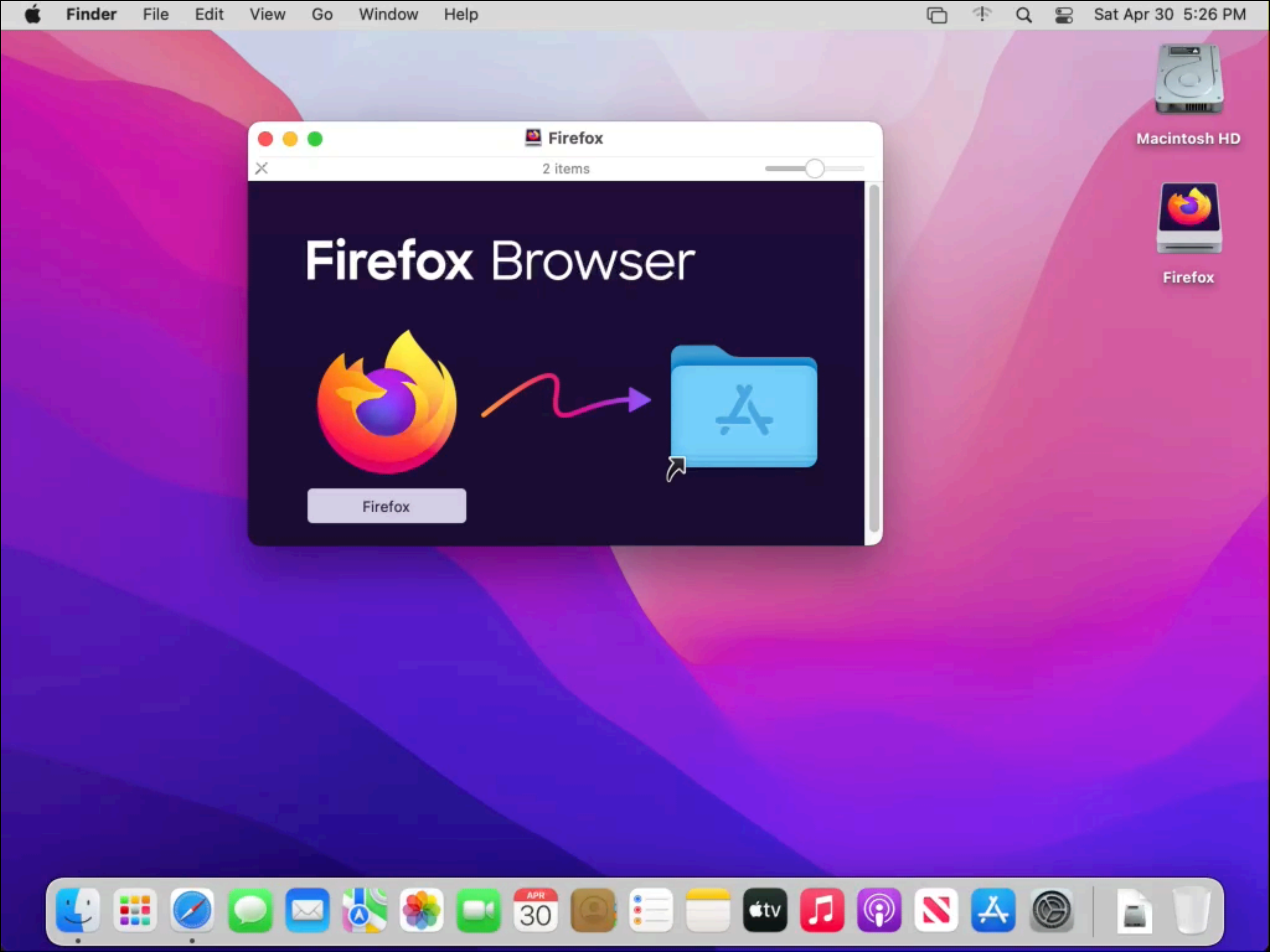


Terminal Shell Edit View Window Help
Sun May 1 1:07 PM
username — pico ◂ sudo — 90×25

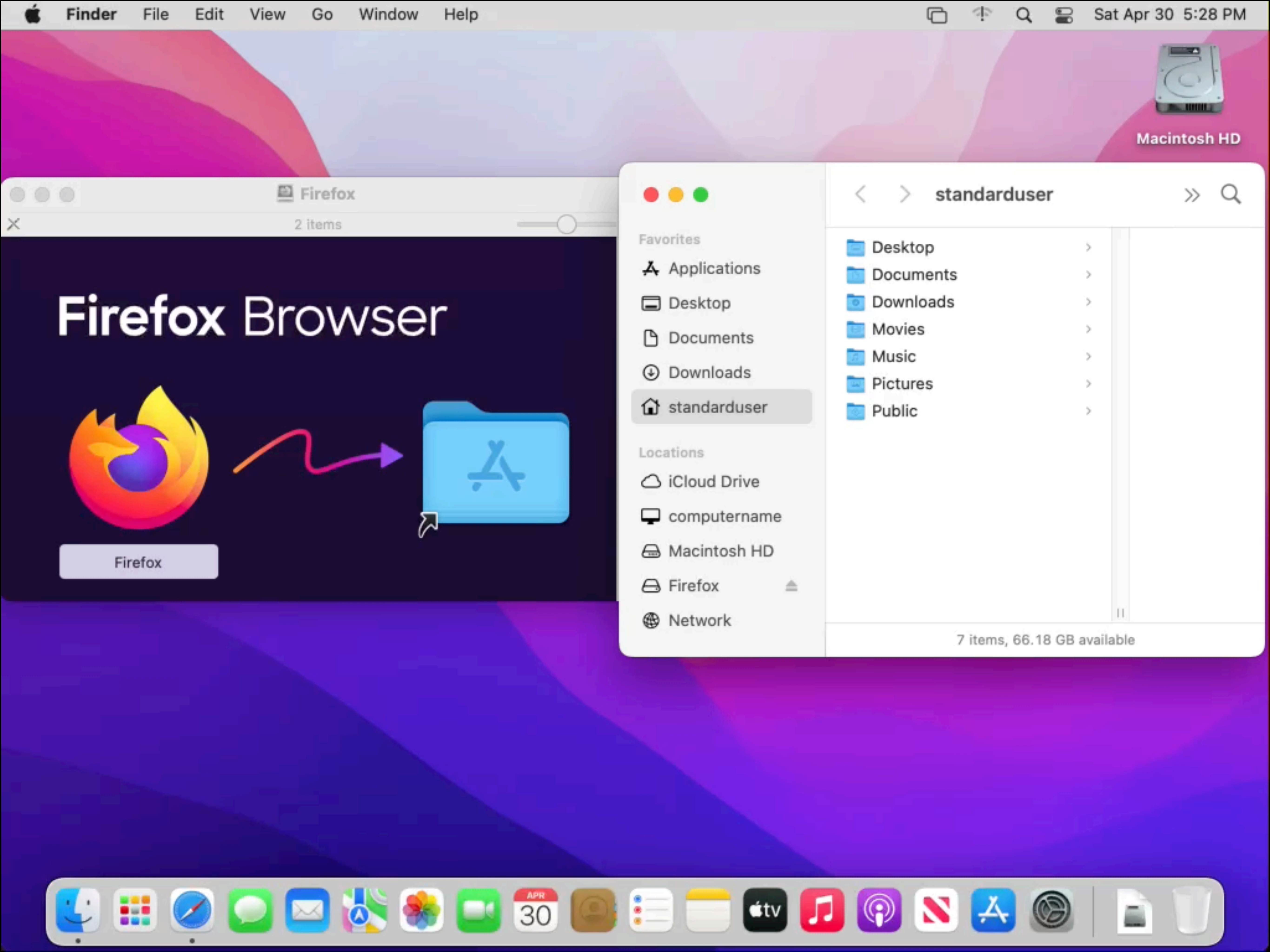
```
  UW PICO 5.09                        File: /etc/sudoers

# Host_Alias    CSNETS = 128.138.243.0, 128.138.204.0/24, 128.138.242.0
# Host_Alias    SERVERS = master, mail, www, ns
# Host_Alias    CDROM = orion, perseus, hercules

##
# Cmnd alias specification
##
# Cmnd_Alias    PAGERS = /usr/bin/more, /usr/bin/pg, /usr/bin/less

##
# User specification
##

# root and users in group wheel can run anything on any machine as any user
root            ALL = (ALL) ALL
%admin          ALL = (ALL) ALL

## Read drop-in files from /private/etc/sudoers.d
## (the '#' here does not indicate a comment)
#includedir /private/etc/sudoers.d

^G Get Help    ^O WriteOut    ^R Read File   ^Y Prev Pg     ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where is    ^V Next Pg     ^U UnCut Text  ^T To Spell
```

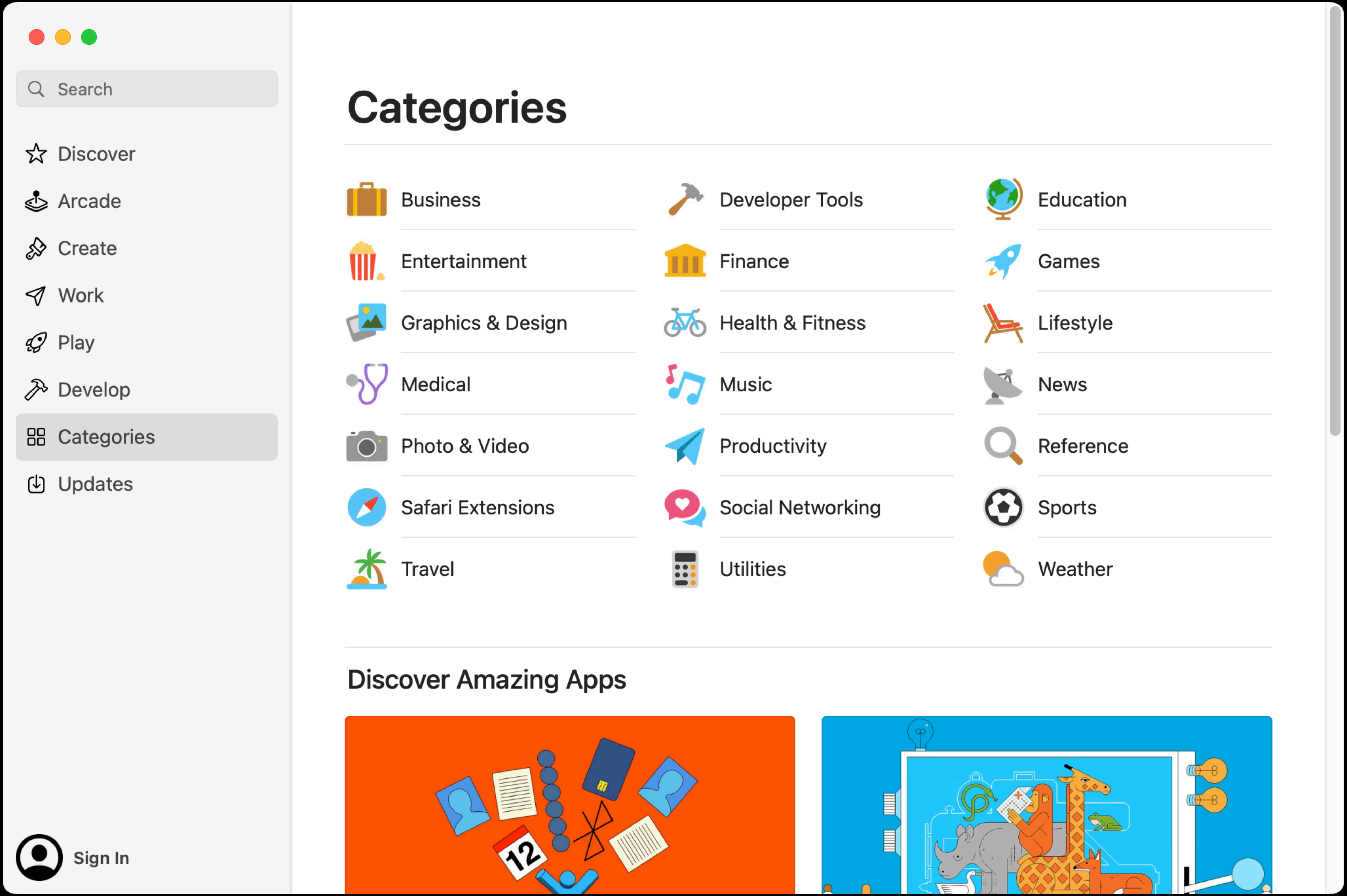
Admin vs. Standard

- Admin
  - Add or manage user accounts
  - Install applications
  - Change account and system settings
- Standard
  - Install applications
  - Change their own account’s settings



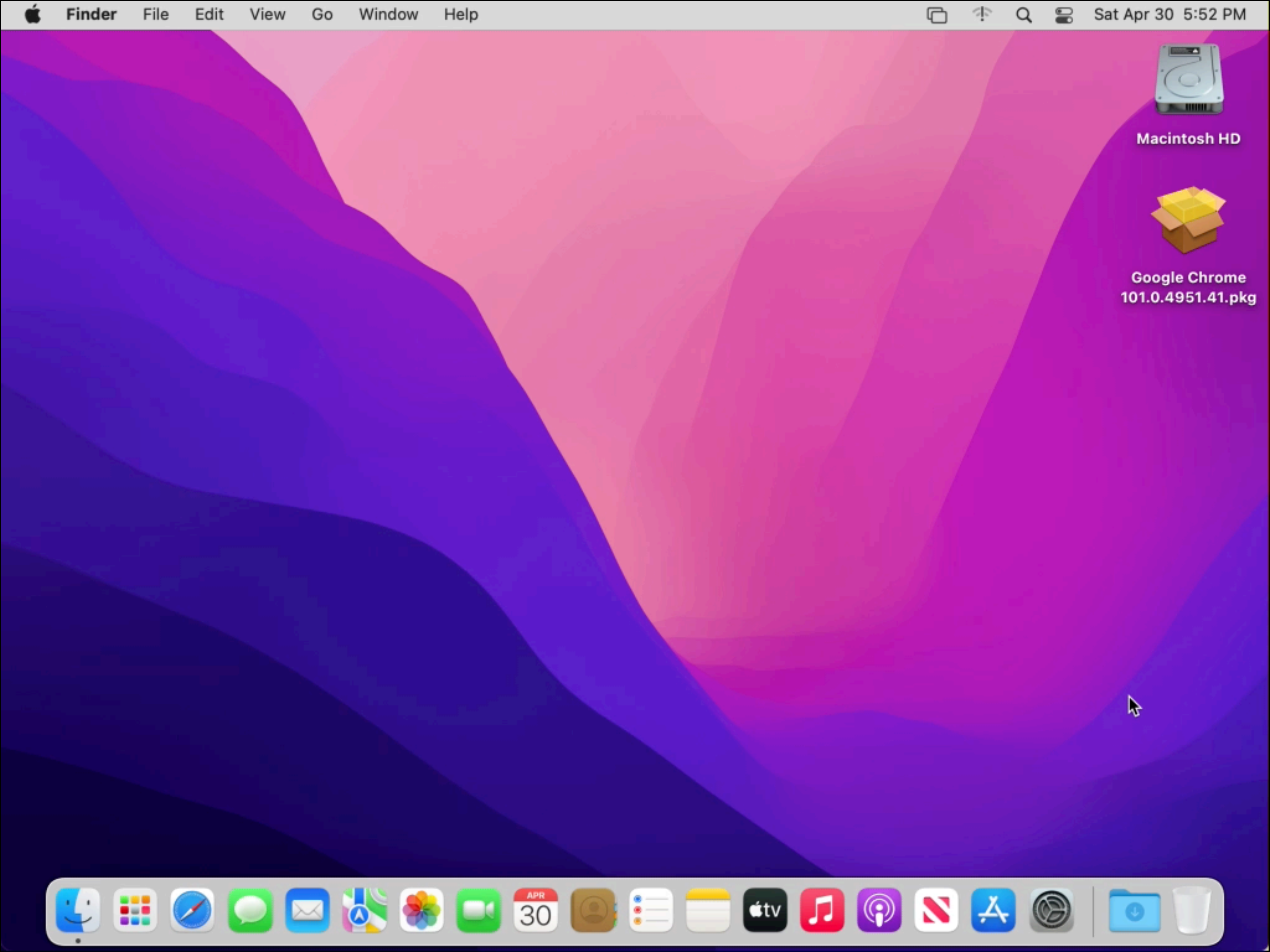
Finder
File
Edit
View
Go
Window
Help
Sat Apr 30 5:26 PM
Macintosh HD
Firefox
Firefox
2 items
Firefox Browser
Firefox
APR
30

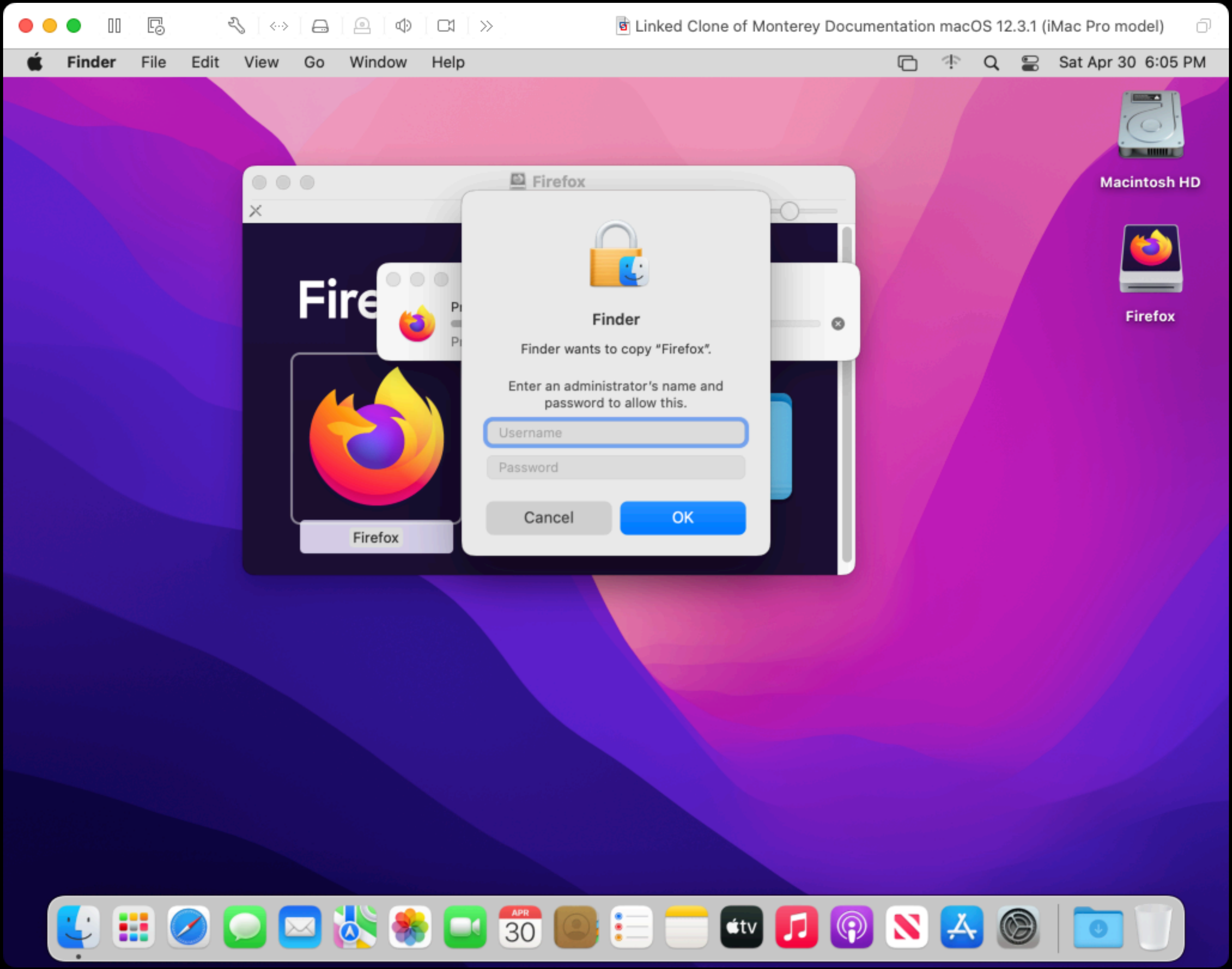

Finder
File
Edit
View
Go
Window
Help
Sat Apr 30 5:28 PM
Macintosh HD
Firefox
2 items
Firefox Browser
Firefox
standarduser
Favorites
Applications
Desktop
Documents
Downloads
standarduser
Locations
iCloud Drive
computername
Macintosh HD
Firefox
Network
Desktop
Documents
Downloads
Movies
Music
Pictures
Public
7 items, 66.18 GB available
APR
30



Categories

Discover Amazing Apps

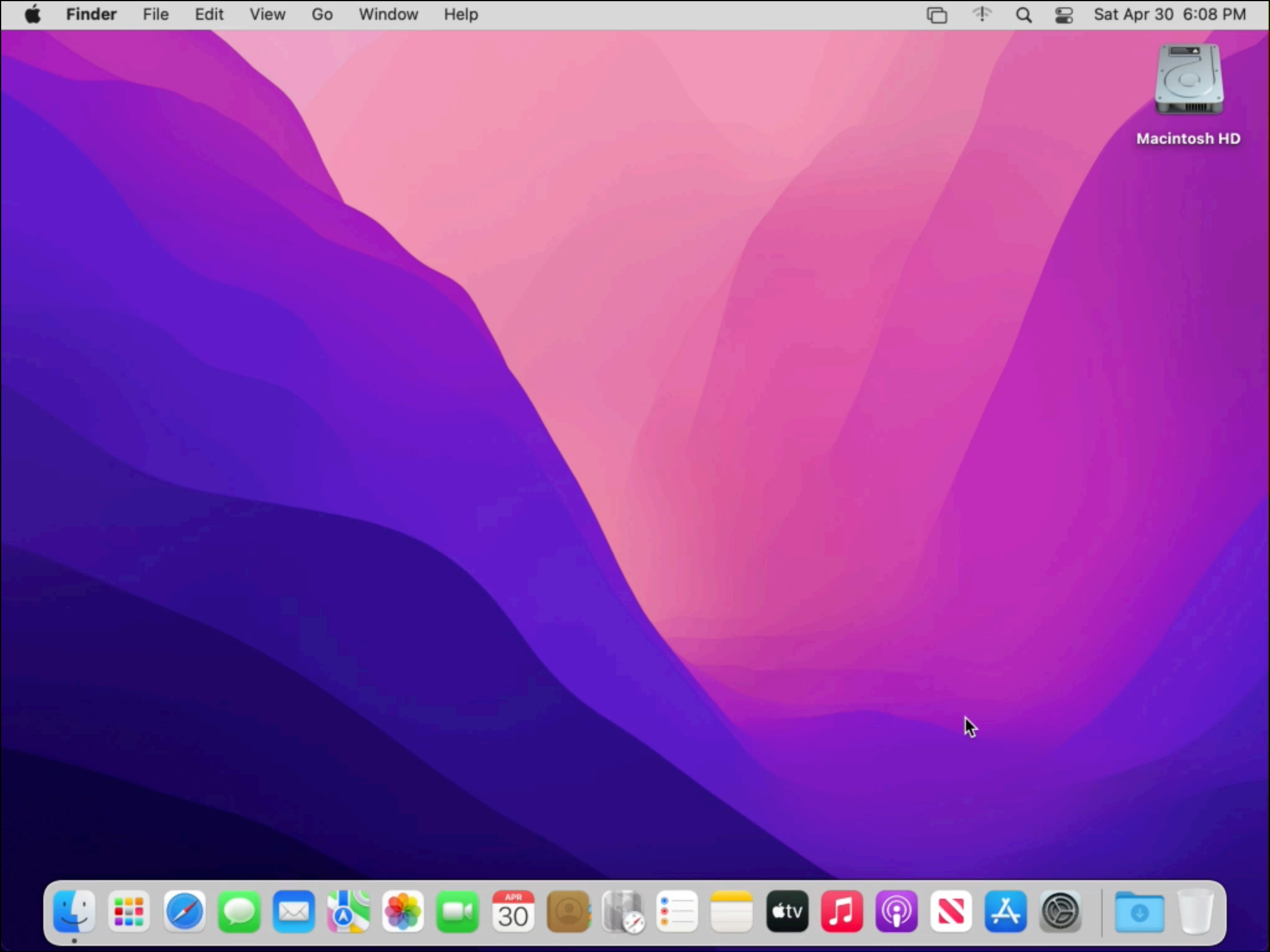

Finder
File
Edit
View
Go
Window
Help
Sat Apr 30 5:52 PM
Macintosh HD
Google Chrome 101.0.4951.41.pkg
APR
30



Finder

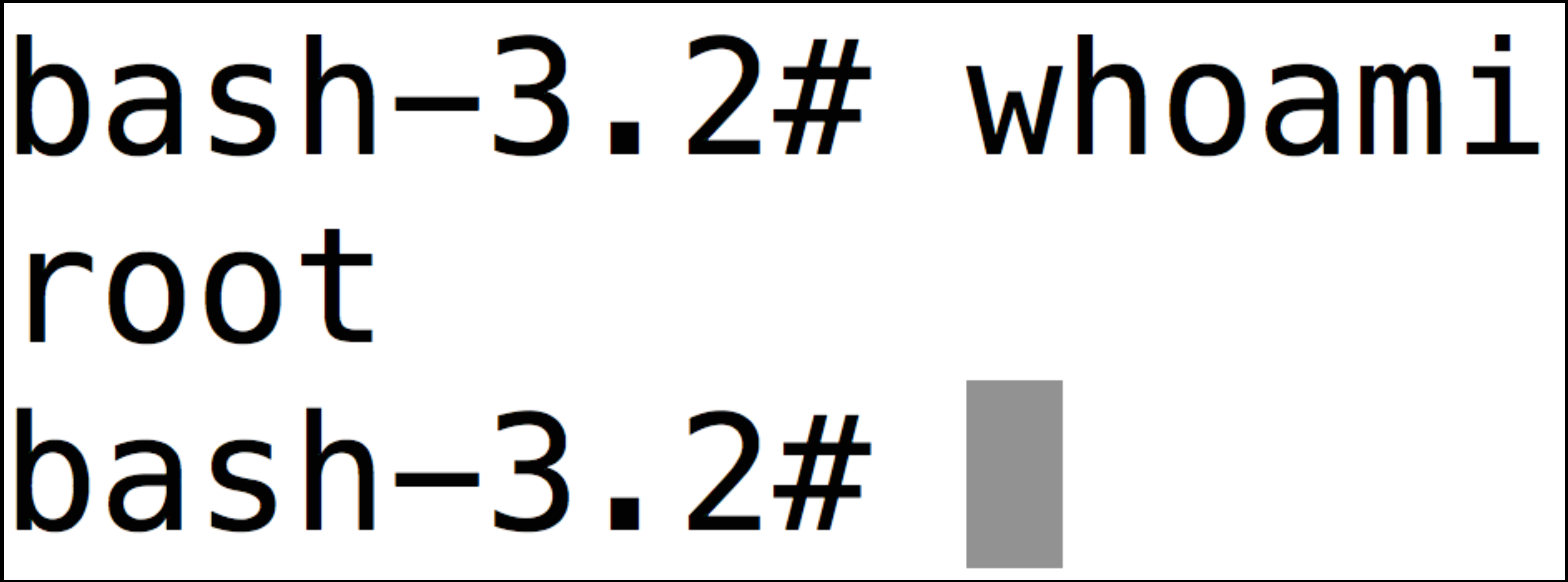
Finder wants to copy “Firefox”.

Enter an administrator’s name and password to allow this.

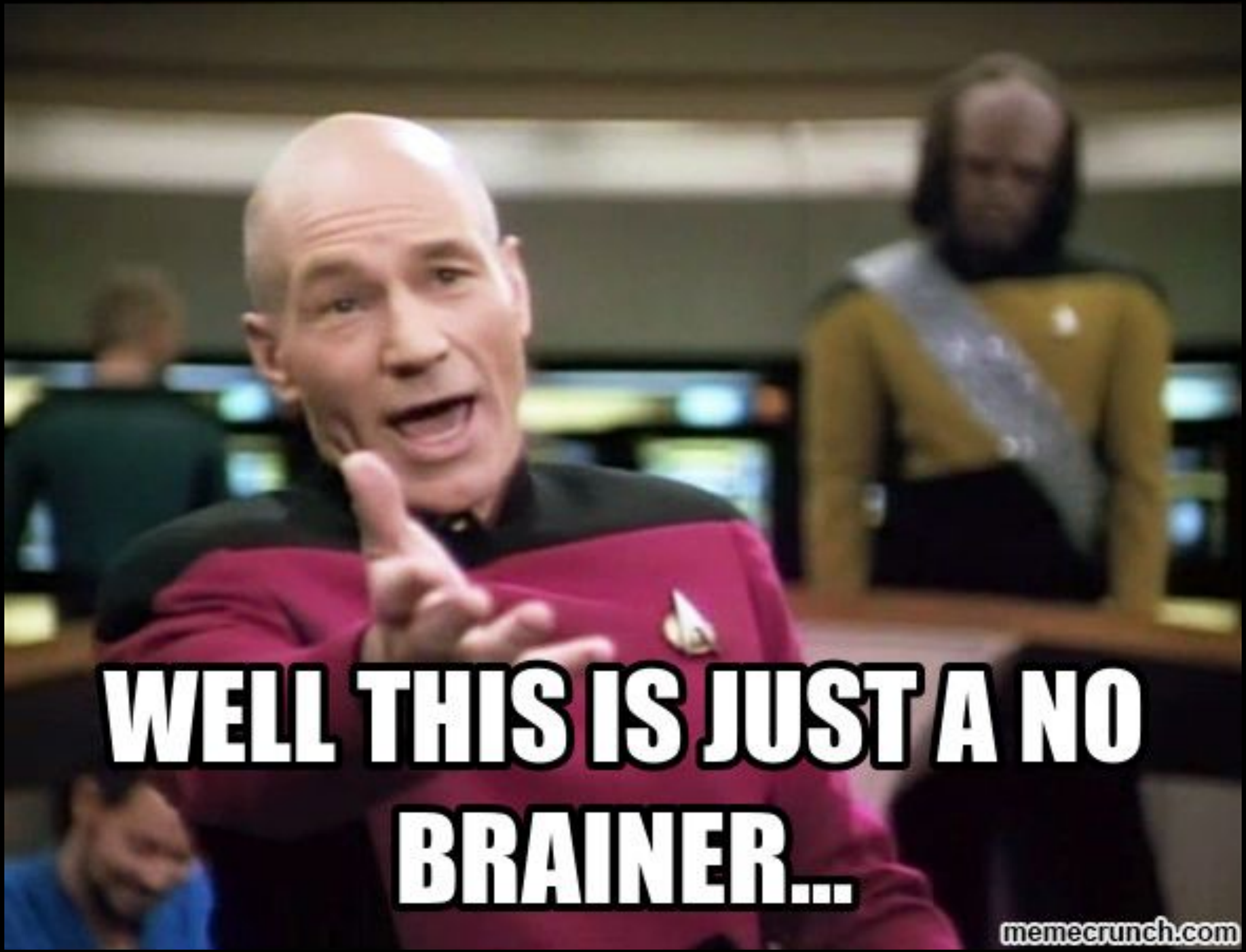

Finder
File
Edit
View
Go
Window
Help
Sat Apr 30 6:08 PM
Macintosh HD
APR
30
tv

COOL STORY, BRO

Anything the root account on macOS can do, an account with administrator rights can do.



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


WELL THIS IS JUST A NO BRAINER...
memecrunch.com

Superuser Limitations

- Read-only Boot Volume
- System Integrity Protection
- User-level privacy protections

Read-only Boot Volume

- Dedicated isolated read-only volume for system software and files.
- Cryptographically signed.
- macOS includes a kernel mechanism which verifies integrity of the system content at runtime.
  - Any data without a valid cryptographic signature from Apple is rejected.
  - As part of macOS installation and updates, the system seal is recomputed entirely on the device from the file system and verified against the Apple-signed seal measurement
  - If system seal verification fails, the startup process fails and the user is prompted to reinstall macOS.

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**
- **/bin**

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

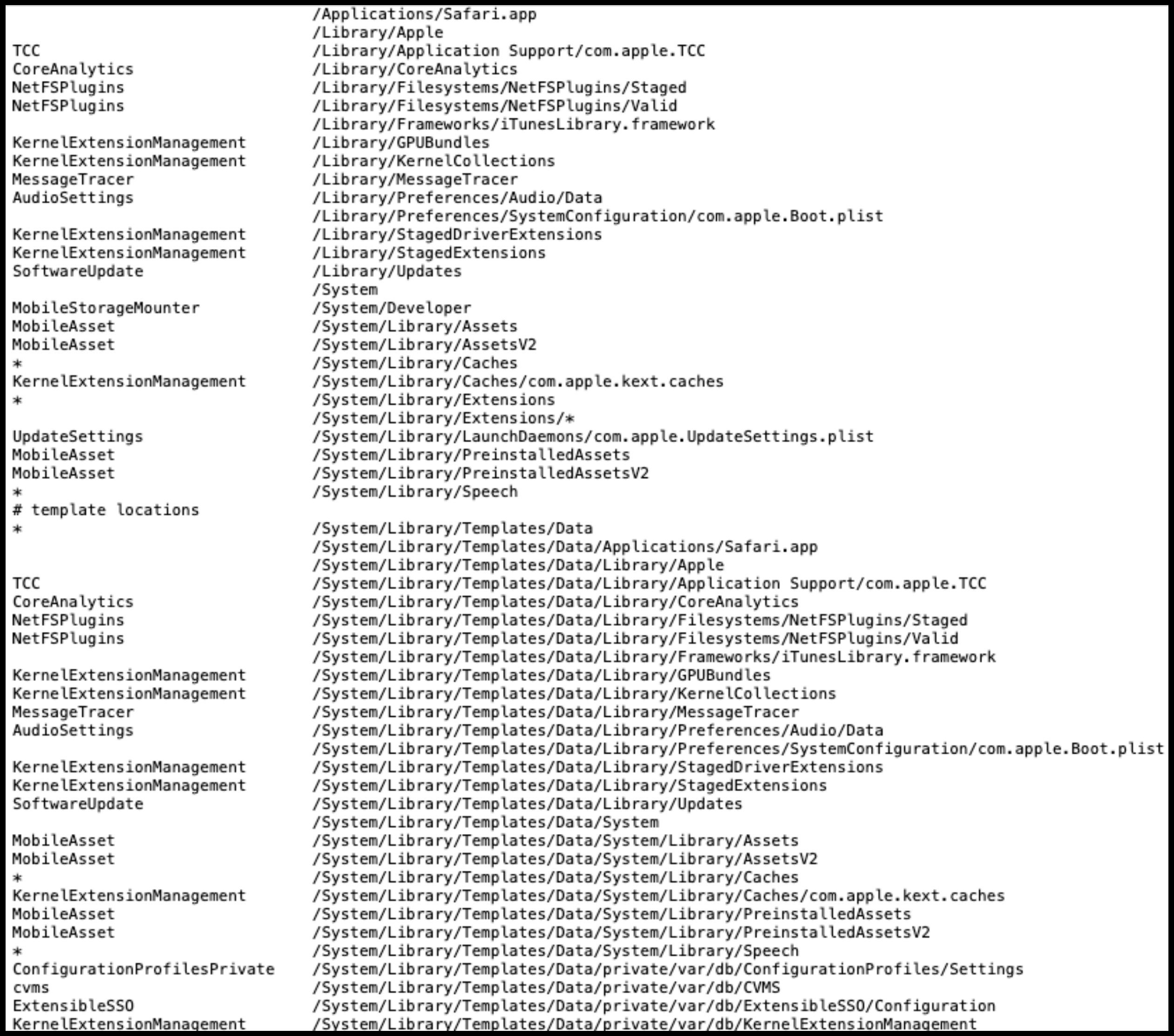
System Integrity Protection

Kernel Extensions

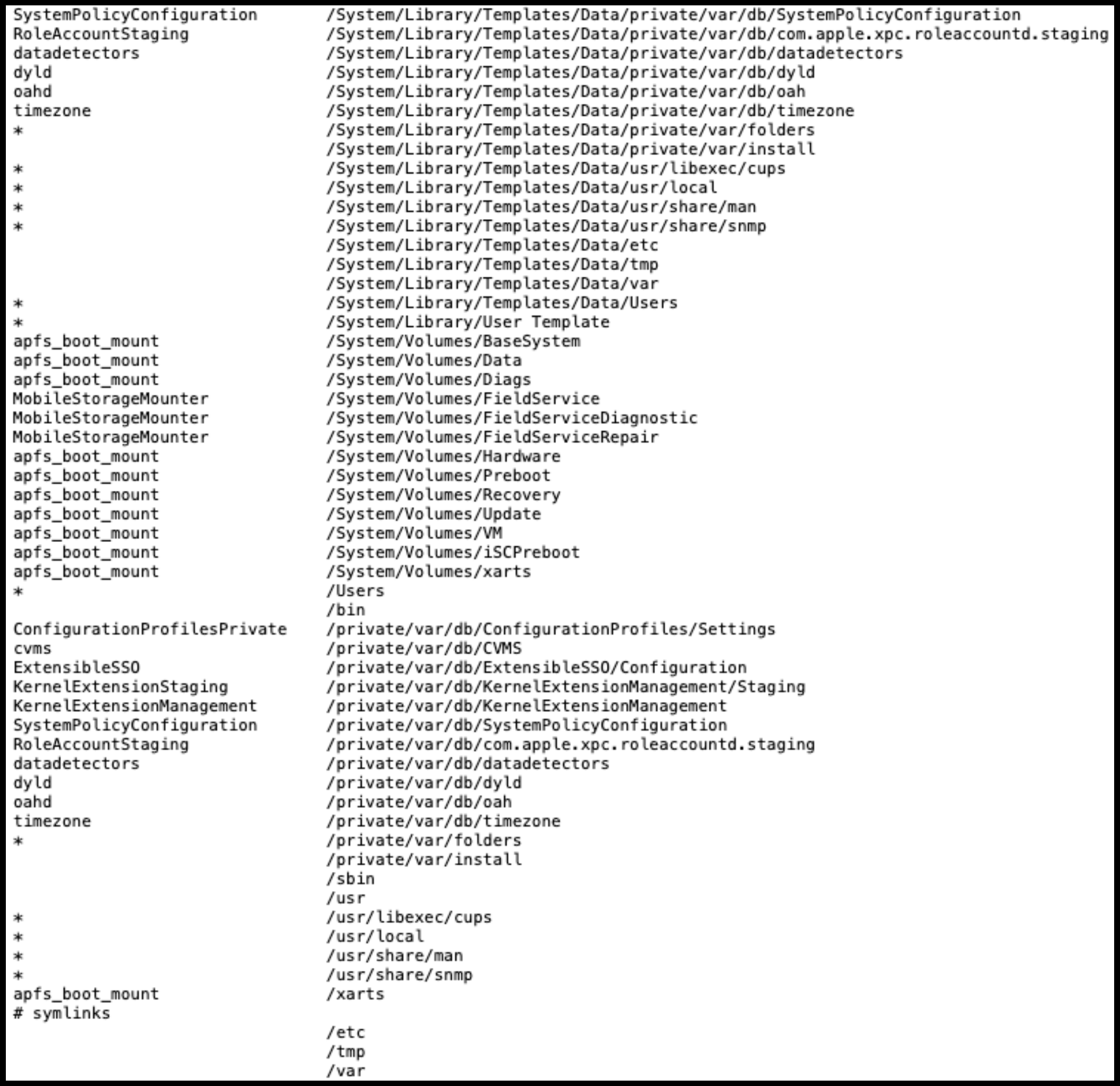
- Must be signed with a **Developer ID for Signing Kexts** certificate
- Must be installed into **/Library/Extensions**

https://tinyurl.com/SIPKext

System Integrity Protection



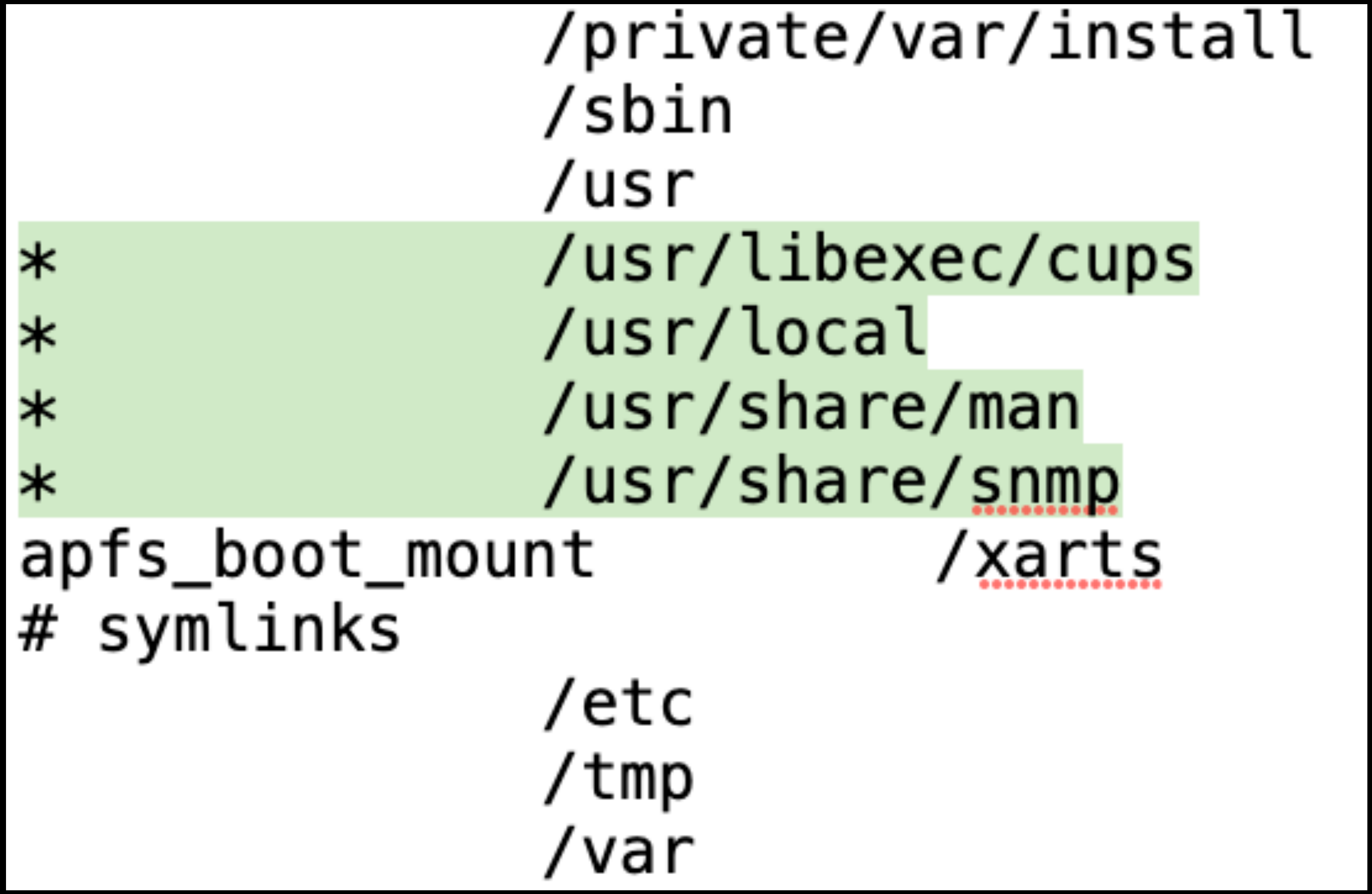
```
                                /Applications/Safari.app
                                /Library/Apple
TCC                             /Library/Application Support/com.apple.TCC
CoreAnalytics                   /Library/CoreAnalytics
NetFSPlugins                    /Library/Filesystems/NetFSPlugins/Staged
NetFSPlugins                    /Library/Filesystems/NetFSPlugins/Valid
                                /Library/Frameworks/iTunesLibrary.framework
KernelExtensionManagement       /Library/GPUBundles
KernelExtensionManagement       /Library/KernelCollections
MessageTracer                   /Library/MessageTracer
AudioSettings                   /Library/Preferences/Audio/Data
                                /Library/Preferences/SystemConfiguration/com.apple.Boot.plist
KernelExtensionManagement       /Library/StagedDriverExtensions
KernelExtensionManagement       /Library/StagedExtensions
SoftwareUpdate                  /Library/Updates
                                /System
MobileStorageMounter            /System/Developer
MobileAsset                     /System/Library/Assets
MobileAsset                     /System/Library/AssetsV2
*                               /System/Library/Caches
KernelExtensionManagement       /System/Library/Caches/com.apple.kext.caches
*                               /System/Library/Extensions
                                /System/Library/Extensions/*
UpdateSettings                  /System/Library/LaunchDaemons/com.apple.UpdateSettings.plist
MobileAsset                     /System/Library/PreinstalledAssets
MobileAsset                     /System/Library/PreinstalledAssetsV2
*                               /System/Library/Speech
# template locations
*                               /System/Library/Templates/Data
                                /System/Library/Templates/Data/Applications/Safari.app
                                /System/Library/Templates/Data/Library/Apple
TCC                             /System/Library/Templates/Data/Library/Application Support/com.apple.TCC
CoreAnalytics                   /System/Library/Templates/Data/Library/CoreAnalytics
NetFSPlugins                    /System/Library/Templates/Data/Library/Filesystems/NetFSPlugins/Staged
NetFSPlugins                    /System/Library/Templates/Data/Library/Filesystems/NetFSPlugins/Valid
                                /System/Library/Templates/Data/Library/Frameworks/iTunesLibrary.framework
KernelExtensionManagement       /System/Library/Templates/Data/Library/GPUBundles
KernelExtensionManagement       /System/Library/Templates/Data/Library/KernelCollections
MessageTracer                   /System/Library/Templates/Data/Library/MessageTracer
AudioSettings                   /System/Library/Templates/Data/Library/Preferences/Audio/Data
                                /System/Library/Templates/Data/Library/Preferences/SystemConfiguration/com.apple.Boot.plist
KernelExtensionManagement       /System/Library/Templates/Data/Library/StagedDriverExtensions
KernelExtensionManagement       /System/Library/Templates/Data/Library/StagedExtensions
SoftwareUpdate                  /System/Library/Templates/Data/Library/Updates
                                /System/Library/Templates/Data/System
MobileAsset                     /System/Library/Templates/Data/System/Library/Assets
MobileAsset                     /System/Library/Templates/Data/System/Library/AssetsV2
*                               /System/Library/Templates/Data/System/Library/Caches
KernelExtensionManagement       /System/Library/Templates/Data/System/Library/Caches/com.apple.kext.caches
MobileAsset                     /System/Library/Templates/Data/System/Library/PreinstalledAssets
MobileAsset                     /System/Library/Templates/Data/System/Library/PreinstalledAssetsV2
*                               /System/Library/Templates/Data/System/Library/Speech
ConfigurationProfilesPrivate    /System/Library/Templates/Data/private/var/db/ConfigurationProfiles/Settings
cvms                            /System/Library/Templates/Data/private/var/db/CVMS
ExtensibleSSO                   /System/Library/Templates/Data/private/var/db/ExtensibleSSO/Configuration
KernelExtensionManagement       /System/Library/Templates/Data/private/var/db/KernelExtensionManagement
```



```
SystemPolicyConfiguration       /System/Library/Templates/Data/private/var/db/SystemPolicyConfiguration
RoleAccountStaging              /System/Library/Templates/Data/private/var/db/com.apple.xpc.roleaccountd.staging
datadetectors                   /System/Library/Templates/Data/private/var/db/datadetectors
dyld                            /System/Library/Templates/Data/private/var/db/dyld
oahd                            /System/Library/Templates/Data/private/var/db/oah
timezone                        /System/Library/Templates/Data/private/var/db/timezone
*                               /System/Library/Templates/Data/private/var/folders
                                /System/Library/Templates/Data/private/var/install
*                               /System/Library/Templates/Data/usr/libexec/cups
*                               /System/Library/Templates/Data/usr/local
*                               /System/Library/Templates/Data/usr/share/man
*                               /System/Library/Templates/Data/usr/share/snmp
                                /System/Library/Templates/Data/etc
                                /System/Library/Templates/Data/tmp
                                /System/Library/Templates/Data/var
*                               /System/Library/Templates/Data/Users
*                               /System/Library/User Template
apfs_boot_mount                 /System/Volumes/BaseSystem
apfs_boot_mount                 /System/Volumes/Data
apfs_boot_mount                 /System/Volumes/Diags
MobileStorageMounter            /System/Volumes/FieldService
MobileStorageMounter            /System/Volumes/FieldServiceDiagnostic
MobileStorageMounter            /System/Volumes/FieldServiceRepair
apfs_boot_mount                 /System/Volumes/Hardware
apfs_boot_mount                 /System/Volumes/Preboot
apfs_boot_mount                 /System/Volumes/Recovery
apfs_boot_mount                 /System/Volumes/Update
apfs_boot_mount                 /System/Volumes/VM
apfs_boot_mount                 /System/Volumes/iSCPreboot
apfs_boot_mount                 /System/Volumes/xarts
*                               /Users
                                /bin
ConfigurationProfilesPrivate    /private/var/db/ConfigurationProfiles/Settings
cvms                            /private/var/db/CVMS
ExtensibleSSO                   /private/var/db/ExtensibleSSO/Configuration
KernelExtensionStaging          /private/var/db/KernelExtensionManagement/Staging
KernelExtensionManagement       /private/var/db/KernelExtensionManagement
SystemPolicyConfiguration       /private/var/db/SystemPolicyConfiguration
RoleAccountStaging              /private/var/db/com.apple.xpc.roleaccountd.staging
datadetectors                   /private/var/db/datadetectors
dyld                            /private/var/db/dyld
oahd                            /private/var/db/oah
timezone                        /private/var/db/timezone
*                               /private/var/folders
                                /private/var/install
                                /sbin
                                /usr
*                               /usr/libexec/cups
*                               /usr/local
*                               /usr/share/man
*                               /usr/share/snmp
apfs_boot_mount                 /xarts
# symlinks
                                /etc
                                /tmp
                                /var
```

/System/Library/Sandbox/rootless.conf

System Integrity Protection

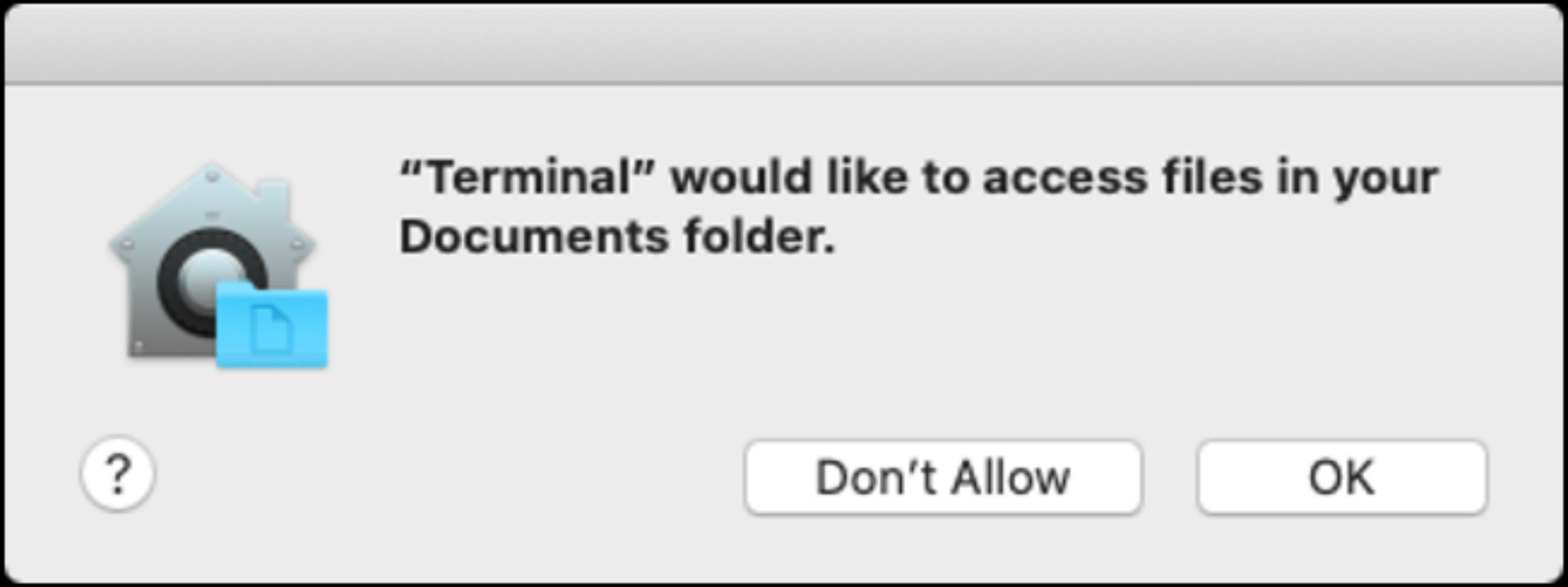


```
              /private/var/install
              /sbin
              /usr
*             /usr/libexec/cups
*             /usr/local
*             /usr/share/man
*             /usr/share/snmp
apfs_boot_mount         /xarts
# symlinks
              /etc
              /tmp
              /var
```

User-level privacy protections

Individual user account permissions needed for the following user data:

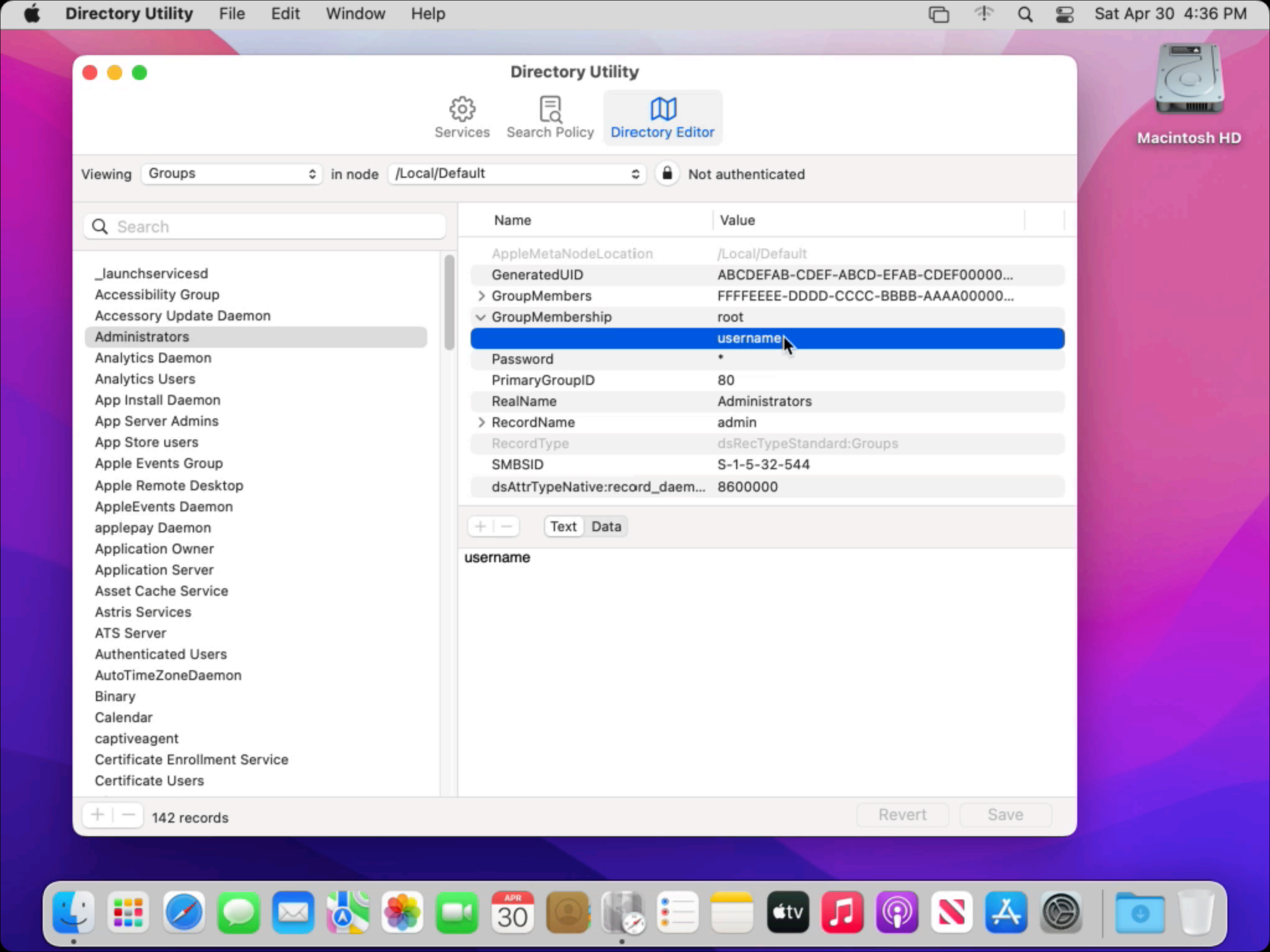
- Calendars
- Camera
- Contacts
- Microphone
- Photos
- Reminders
- Speech recognition
- Input monitoring (for example, keyboard strokes)
- Prompt
- Screen recording (for example, static screen shots and video)
- System Preferences



"Terminal" would like to access files in your Documents folder.

Anything the root account on macOS can do, an account with administrator rights can do.

Managing admin rights



Directory Utility

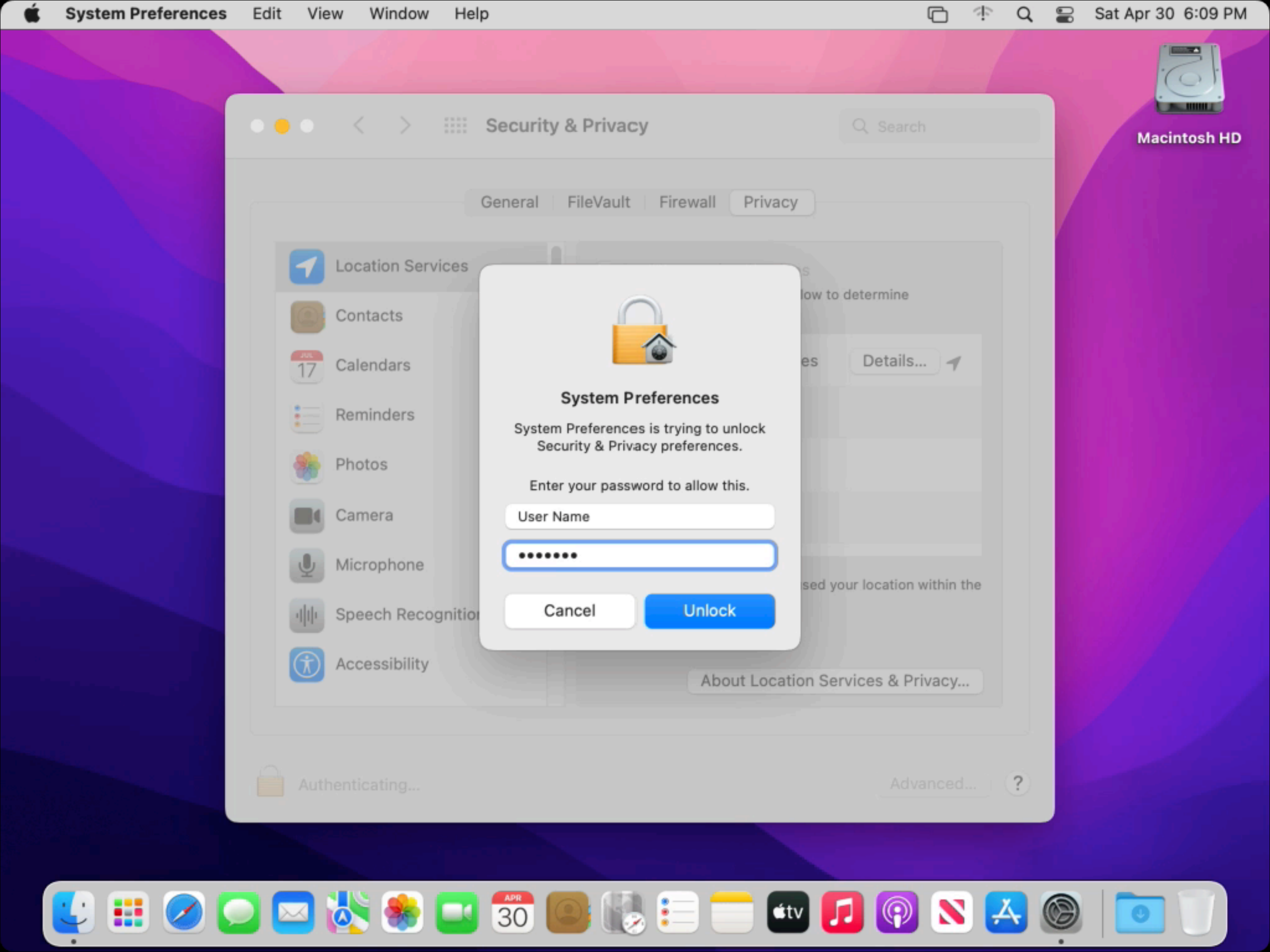
Viewing Groups in node /Local/Default 🔒 Not authenticated

_launchservicesd
Accessibility Group
Accessory Update Daemon
Administrators
Analytics Daemon
Analytics Users
App Install Daemon
App Server Admins
App Store users
Apple Events Group
Apple Remote Desktop
AppleEvents Daemon
applepay Daemon
Application Owner
Application Server
Asset Cache Service
Astris Services
ATS Server
Authenticated Users
AutoTimeZoneDaemon
Binary
Calendar
captiveagent
Certificate Enrollment Service
Certificate Users

142 records

Name	Value
AppleMetaNodeLocation	/Local/Default
GeneratedUID	ABCDEFAB-CDEF-ABCD-EFAB-CDEF00000...
› GroupMembers	FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000...
⌄ GroupMembership	root
	username
Password	*
PrimaryGroupID	80
RealName	Administrators
› RecordName	admin
RecordType	dsRecTypeStandard:Groups
SMBSID	S-1-5-32-544
dsAttrTypeNative:record_daem...	8600000

username



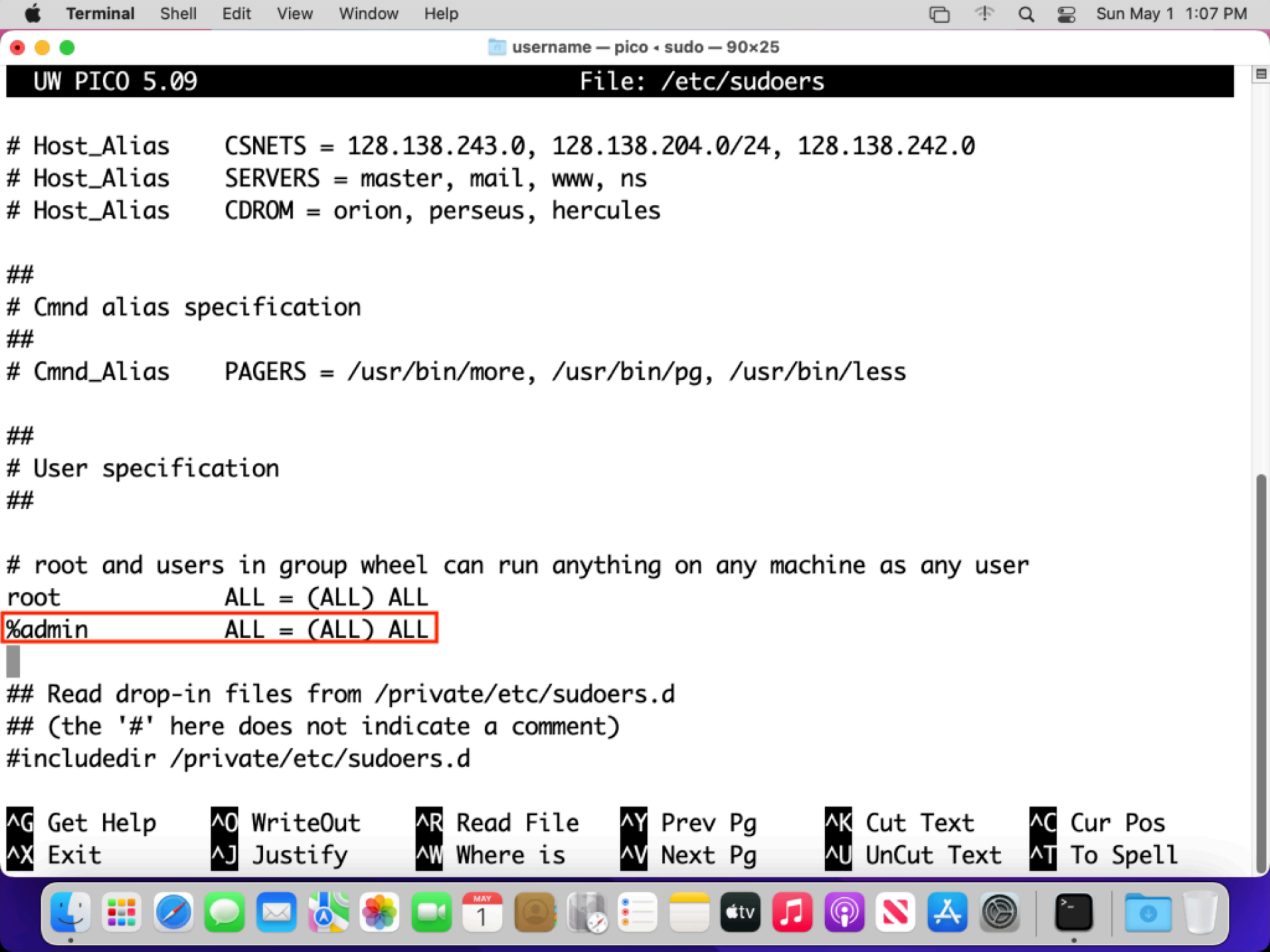
System Preferences

System Preferences is trying to unlock Security & Privacy preferences.

Enter your password to allow this.

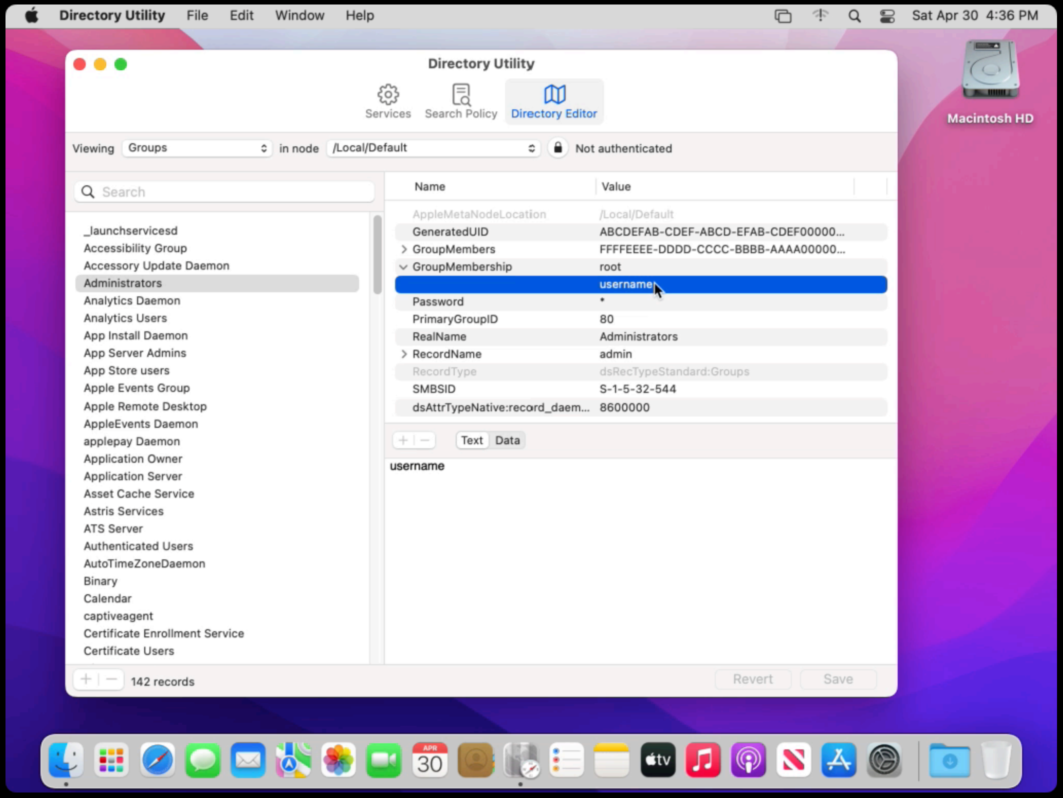
User Name

••••••••



```
  UW PICO 5.09                              File: /etc/sudoers

# Host_Alias    CSNETS = 128.138.243.0, 128.138.204.0/24, 128.138.242.0
# Host_Alias    SERVERS = master, mail, www, ns
# Host_Alias    CDROM = orion, perseus, hercules

##
# Cmnd alias specification
##
# Cmnd_Alias    PAGERS = /usr/bin/more, /usr/bin/pg, /usr/bin/less

##
# User specification
##

# root and users in group wheel can run anything on any machine as any user
root            ALL = (ALL) ALL
%admin          ALL = (ALL) ALL

## Read drop-in files from /private/etc/sudoers.d
## (the '#' here does not indicate a comment)
#includedir /private/etc/sudoers.d

^G Get Help     ^O WriteOut     ^R Read File    ^Y Prev Pg      ^K Cut Text     ^C Cur Pos
^X Exit         ^J Justify      ^W Where is     ^V Next Pg      ^U UnCut Text   ^T To Spell
```

Two places to manage admin rights



Viewing Groups in node /Local/Default 🔒 Not authenticated

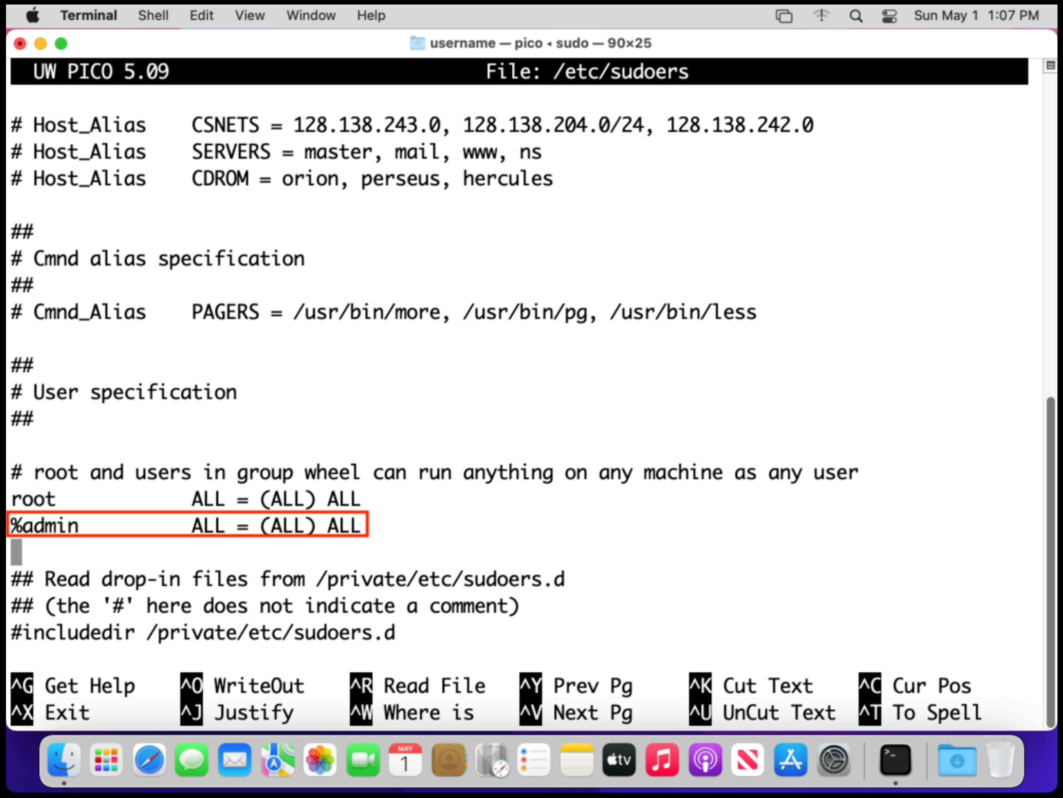
_launchservicesd
Accessibility Group
Accessory Update Daemon
Administrators
Analytics Daemon
Analytics Users
App Install Daemon
App Server Admins
App Store users
Apple Events Group
Apple Remote Desktop
AppleEvents Daemon
applepay Daemon
Application Owner
Application Server
Asset Cache Service
Astris Services
ATS Server
Authenticated Users
AutoTimeZoneDaemon
Binary
Calendar
captiveagent
Certificate Enrollment Service
Certificate Users

142 records

Name	Value
AppleMetaNodeLocation	/Local/Default
GeneratedUID	ABCDEFAB-CDEF-ABCD-EFAB-CDEF00000...
› GroupMembers	FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000...
⌄ GroupMembership	root
	username
Password	*
PrimaryGroupID	80
RealName	Administrators
› RecordName	admin
RecordType	dsRecTypeStandard:Groups
SMBSID	S-1-5-32-544
dsAttrTypeNative:record_daem...	8600000

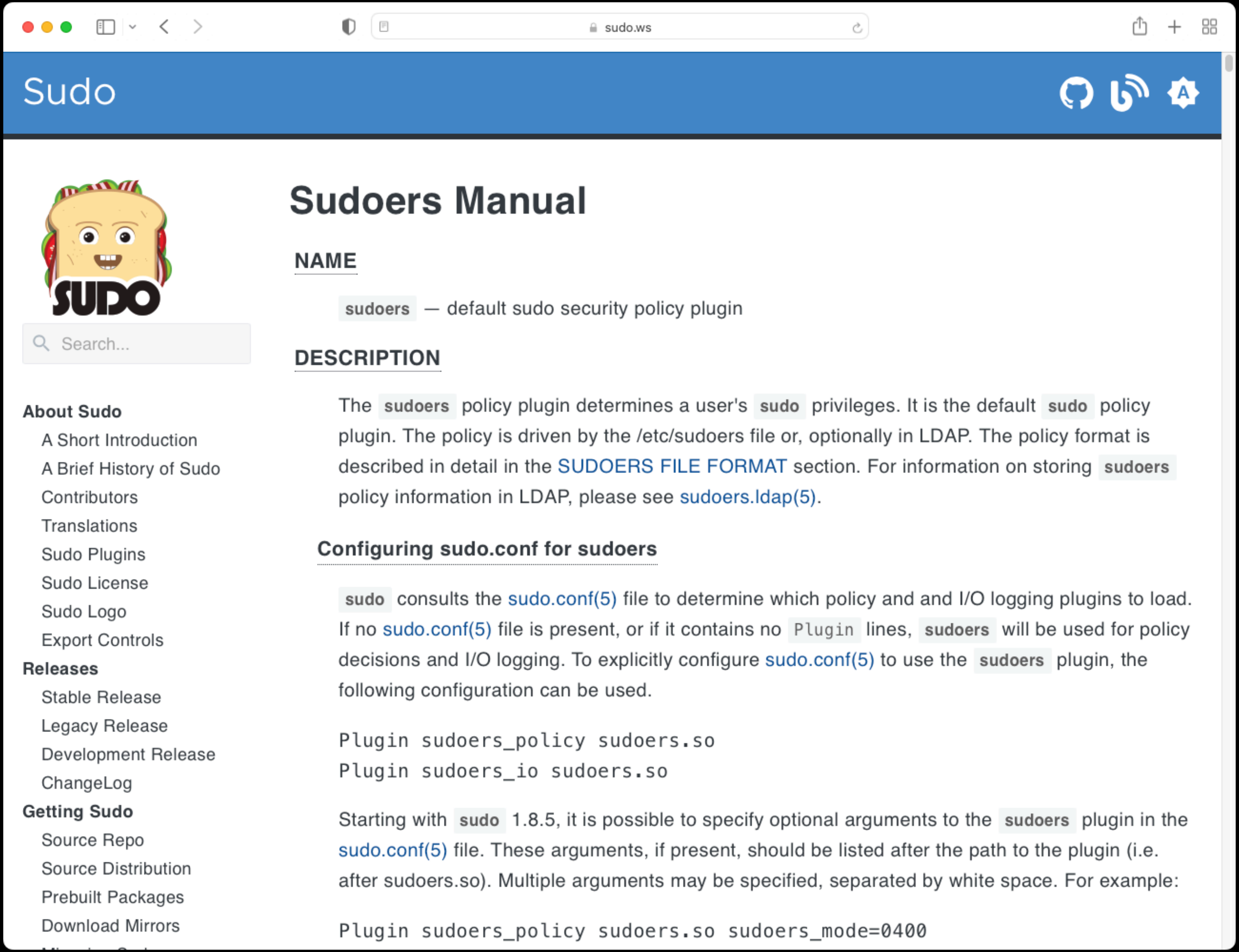
Text Data

username



```
  UW PICO 5.09                                  File: /etc/sudoers

# Host_Alias    CSNETS = 128.138.243.0, 128.138.204.0/24, 128.138.242.0
# Host_Alias    SERVERS = master, mail, www, ns
# Host_Alias    CDROM = orion, perseus, hercules

##
# Cmnd alias specification
##
# Cmnd_Alias    PAGERS = /usr/bin/more, /usr/bin/pg, /usr/bin/less

##
# User specification
##

# root and users in group wheel can run anything on any machine as any user
root            ALL = (ALL) ALL
%admin          ALL = (ALL) ALL

## Read drop-in files from /private/etc/sudoers.d
## (the '#' here does not indicate a comment)
#includedir /private/etc/sudoers.d

^G Get Help    ^O WriteOut    ^R Read File   ^Y Prev Pg     ^K Cut Text    ^C Cur Pos
^X Exit        ^J Justify     ^W Where is    ^V Next Pg     ^U UnCut Text  ^T To Spell
```

Admin rights for GUI and command line can be managed separately



Sudoers Manual

NAME

`sudoers` — default sudo security policy plugin

DESCRIPTION

The `sudoers` policy plugin determines a user's `sudo` privileges. It is the default `sudo` policy plugin. The policy is driven by the /etc/sudoers file or, optionally in LDAP. The policy format is described in detail in the SUDOERS FILE FORMAT section. For information on storing `sudoers` policy information in LDAP, please see sudoers.ldap(5).

Configuring sudo.conf for sudoers

`sudo` consults the sudo.conf(5) file to determine which policy and and I/O logging plugins to load. If no sudo.conf(5) file is present, or if it contains no `Plugin` lines, `sudoers` will be used for policy decisions and I/O logging. To explicitly configure sudo.conf(5) to use the `sudoers` plugin, the following configuration can be used.

```
Plugin sudoers_policy sudoers.so
Plugin sudoers_io sudoers.so
```

Starting with `sudo` 1.8.5, it is possible to specify optional arguments to the `sudoers` plugin in the sudo.conf(5) file. These arguments, if present, should be listed after the path to the plugin (i.e. after sudoers.so). Multiple arguments may be specified, separated by white space. For example:

```
Plugin sudoers_policy sudoers.so sudoers_mode=0400
```

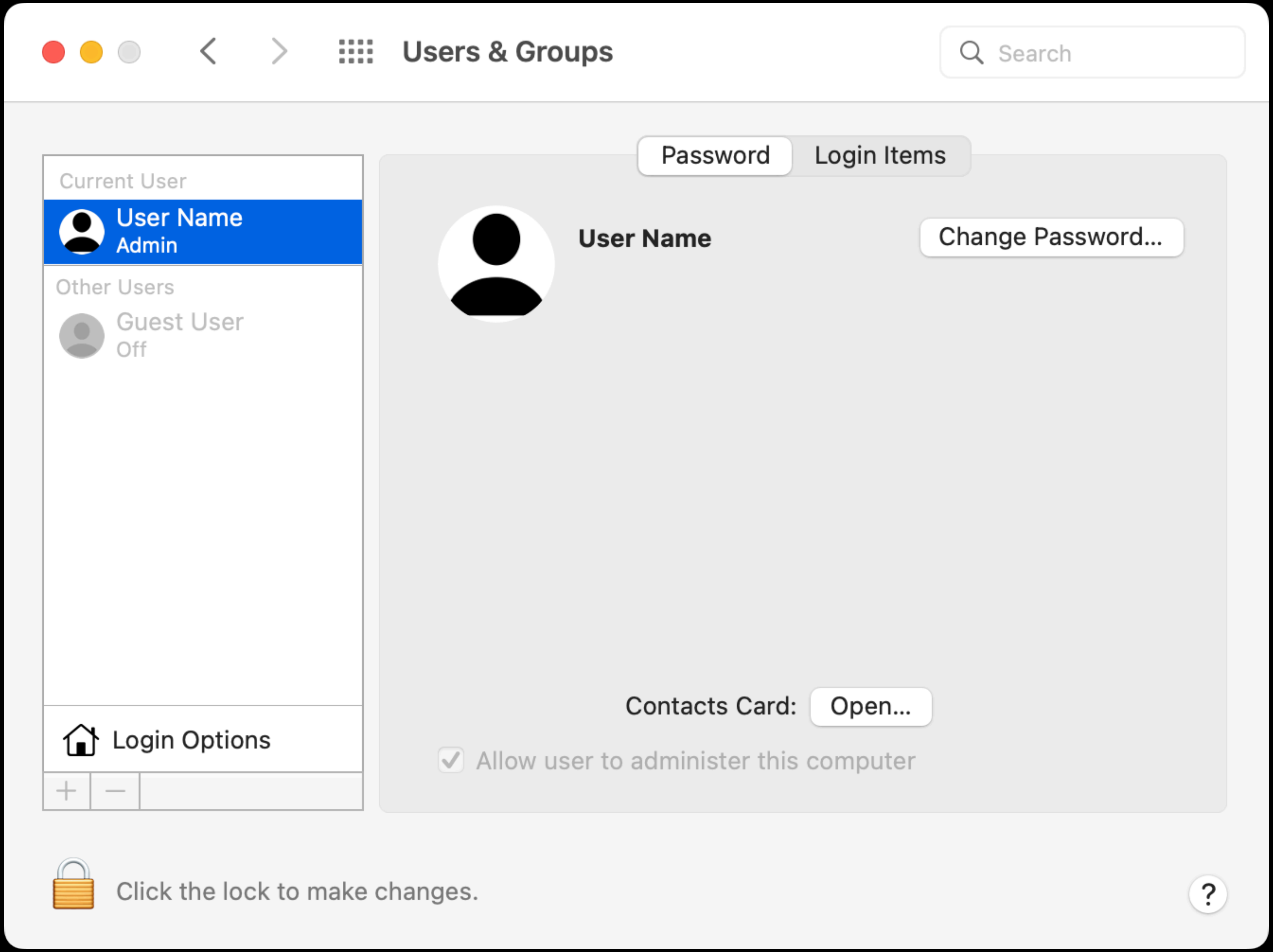
https://www.sudo.ws/docs/man/1.8.17/sudoers.man/

Admin rights management

- Permanent admin rights
- No admin rights
- Allow admin rights on non-permanent basis

Admin rights management

Permanent Admin rights



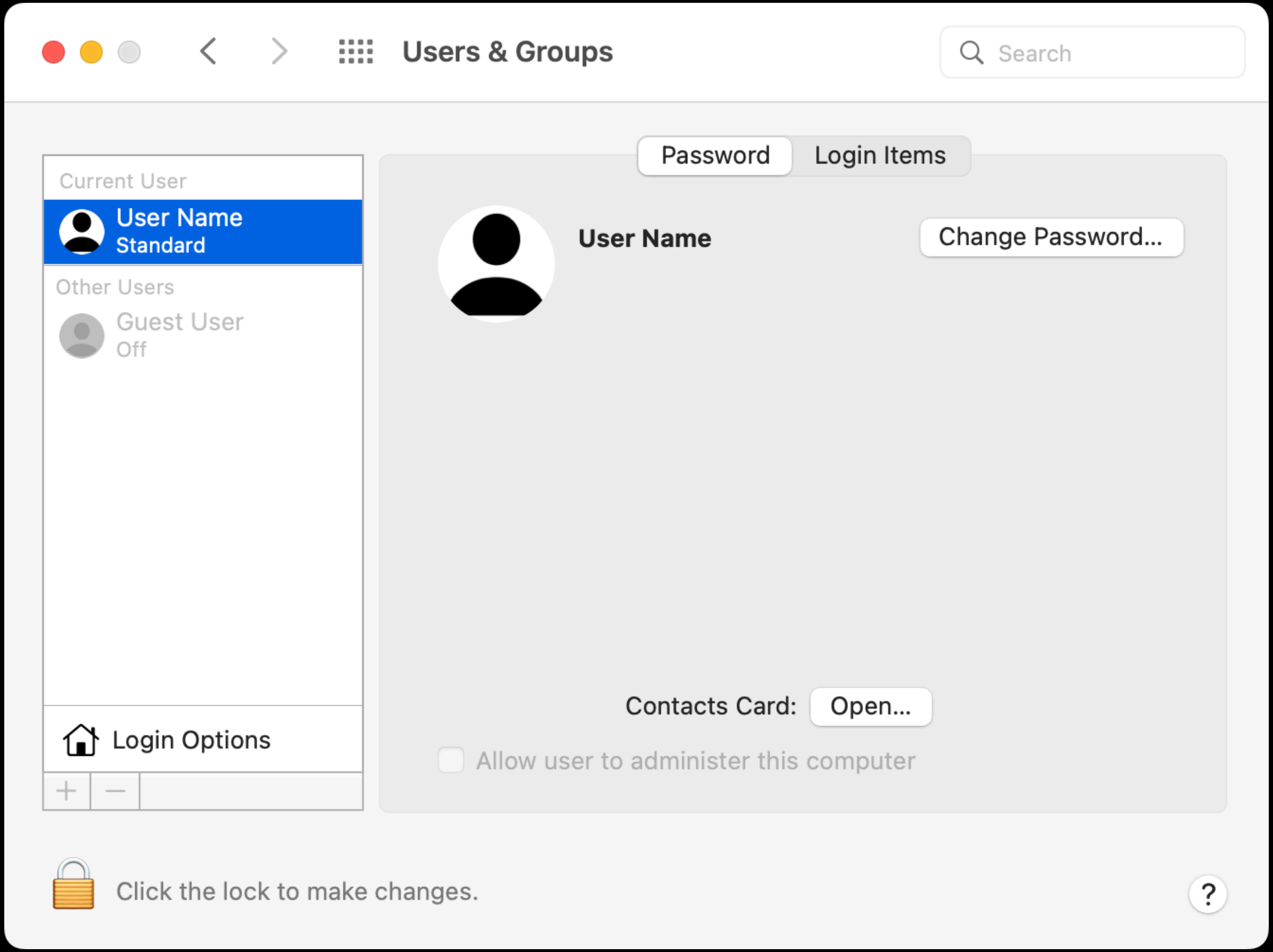
☑ Allow user to administer this computer

Click the lock to make changes.

Anything the root account on macOS can do, an account with administrator rights can do.

Admin rights management

No Admin rights



□ Allow user to administer this computer

Click the lock to make changes.

Admin vs. Standard

- Admin
  - Add or manage user accounts
  - Install applications
  - Change account and system settings
- Standard
  - Install applications
  - Change their own account’s settings

Admin rights management

Allow non-permanent
admin rights

Admin rights management

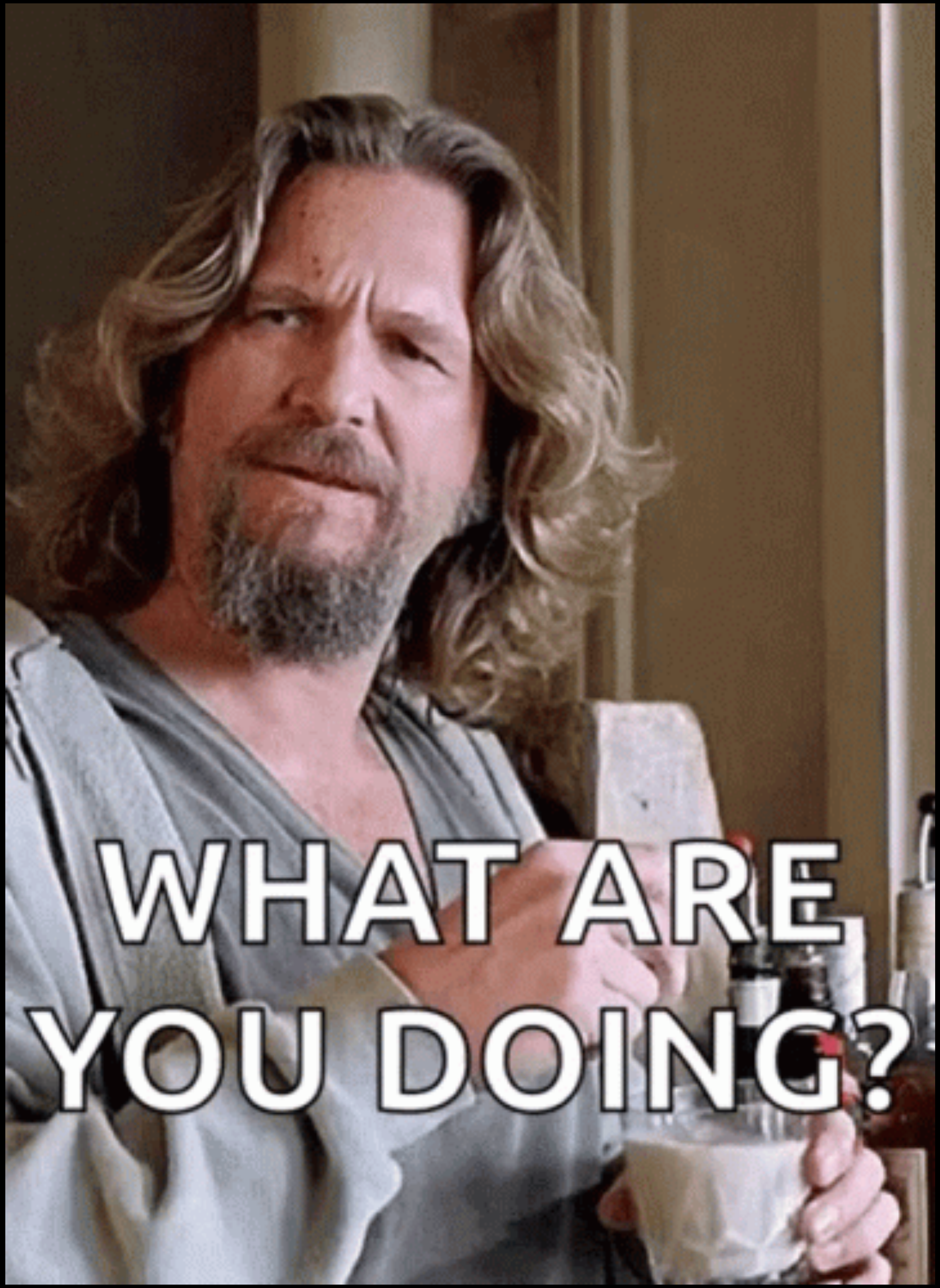
What’s the best way?

Different answers for different situations

What affects the answer?

- Legal requirements
- External standard requirements
- Internal policy requirements
- Operational requirements

POWERED BY
TRUST
S


WHAT ARE
YOU DOING?

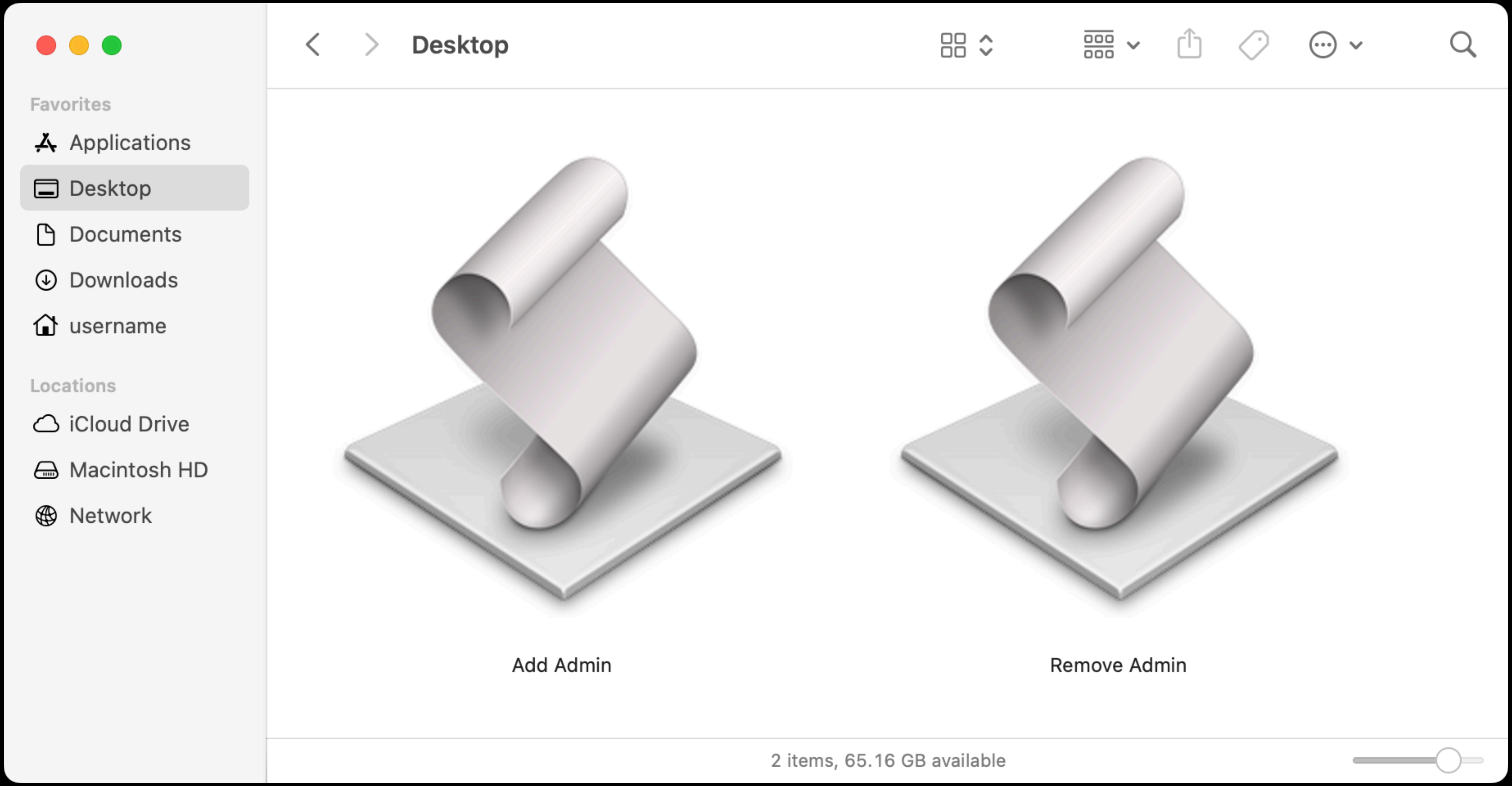
Allow non-permanent admin rights

SAP®

Allow non-permanent admin rights

https://github.com/SAP/macOS-enterprise-privileges

WHERE DID THAT
COME FROM
makeameme.org



Add Admin

Remove Admin

2 items, 65.16 GB available

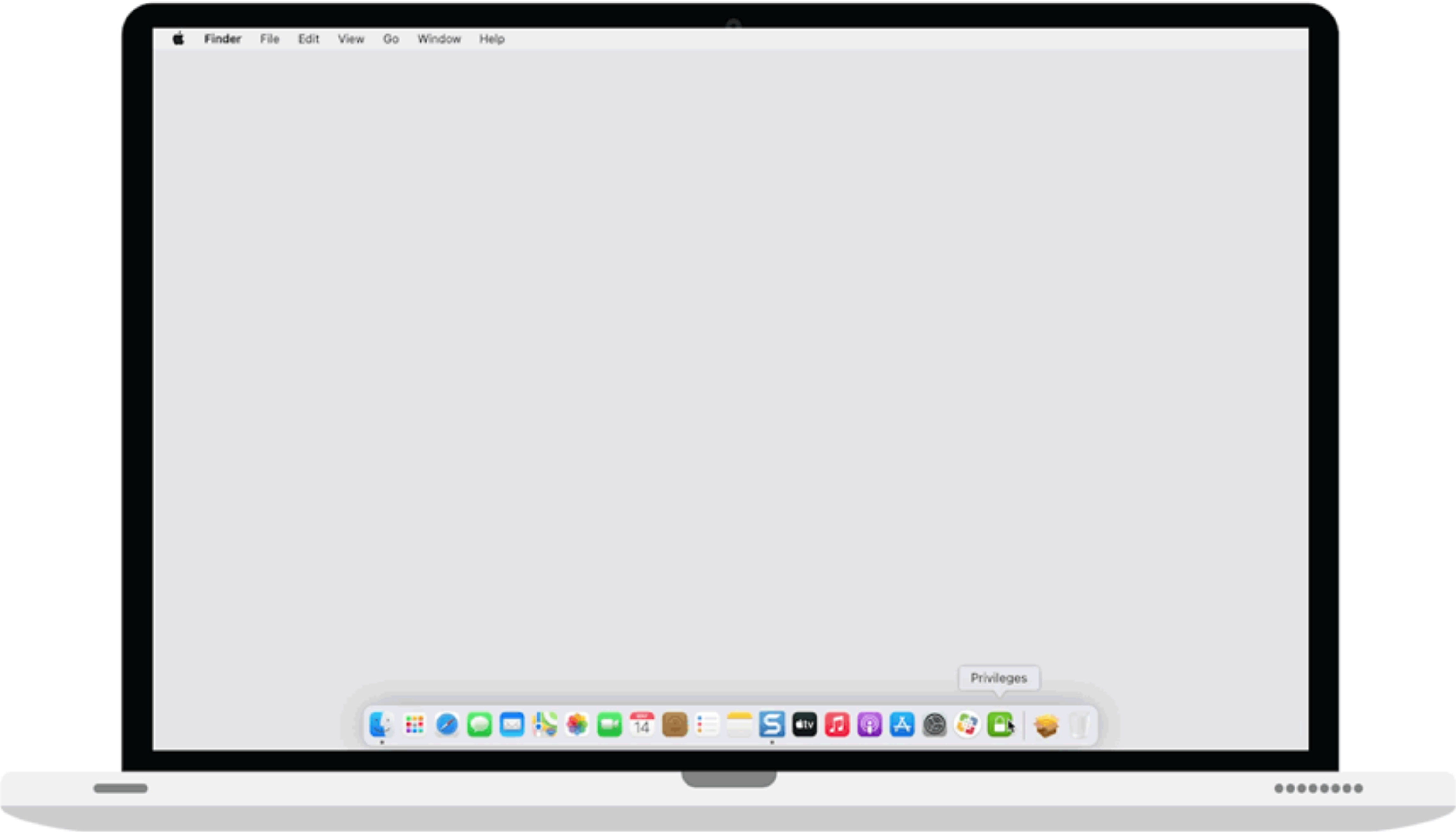
SAP®

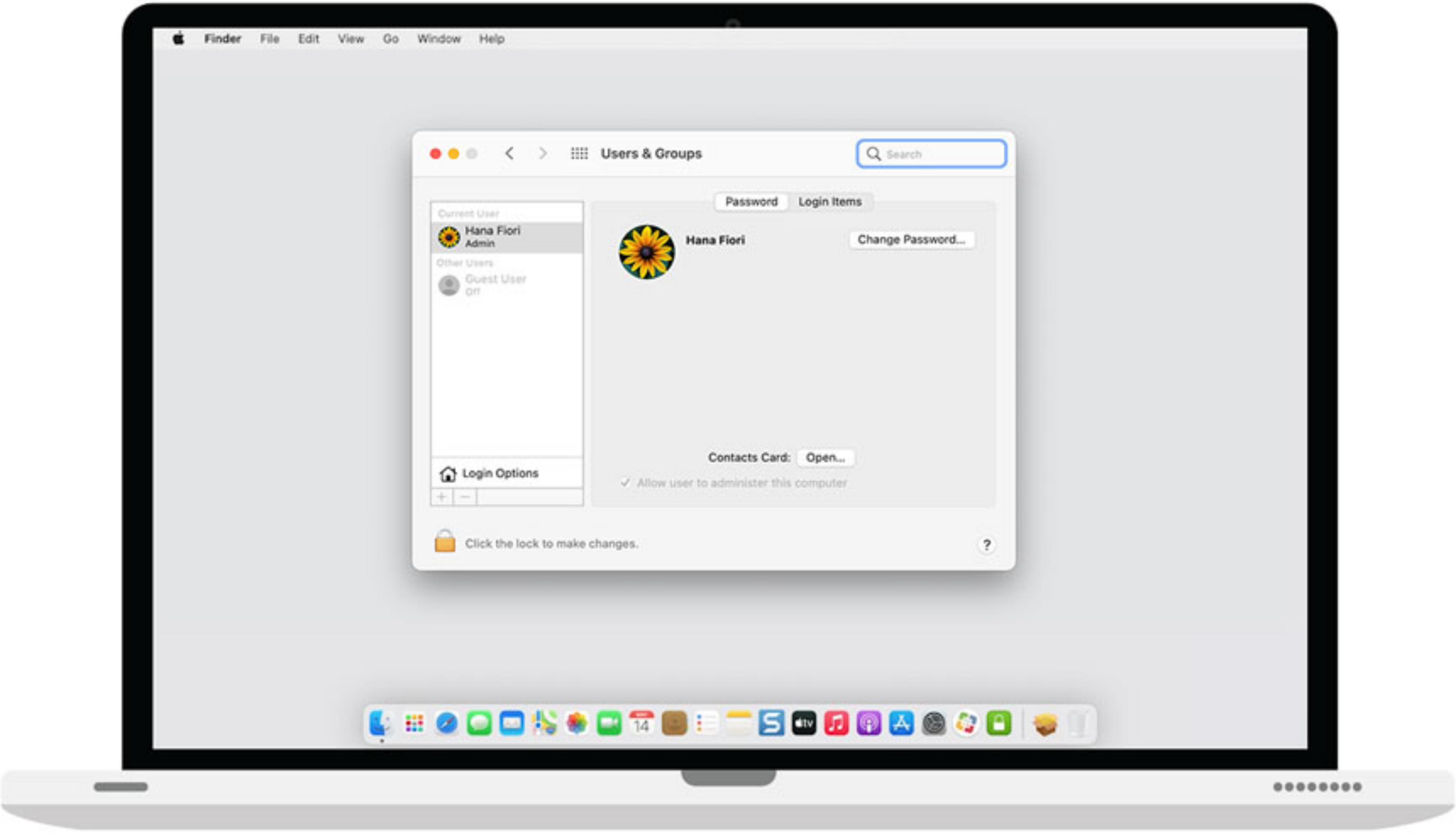
Auditor

Privileges

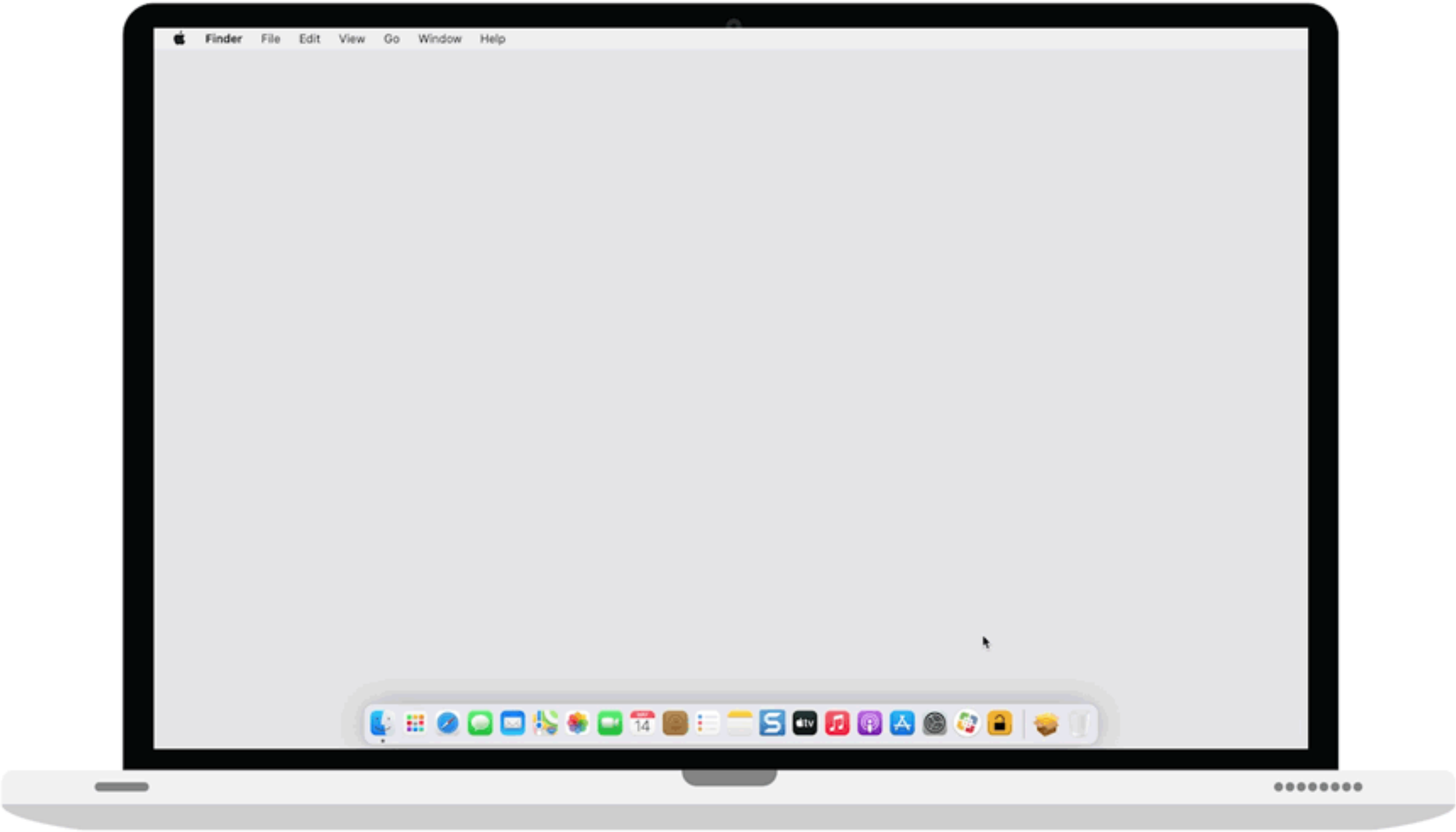
Admin user vs. standard user

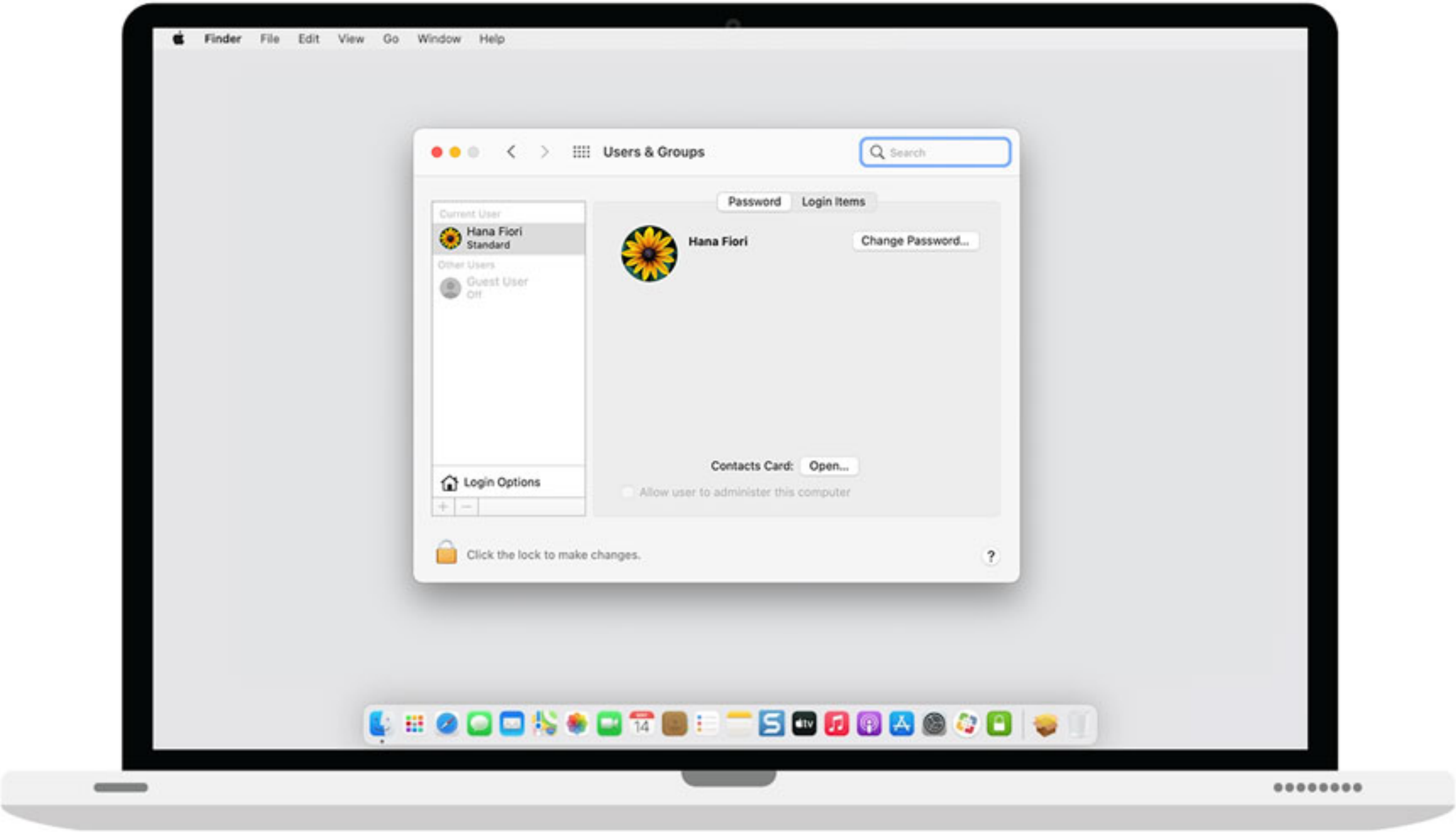
Standard User ?


Finder
File
Edit
View
Go
Window
Help
Privileges

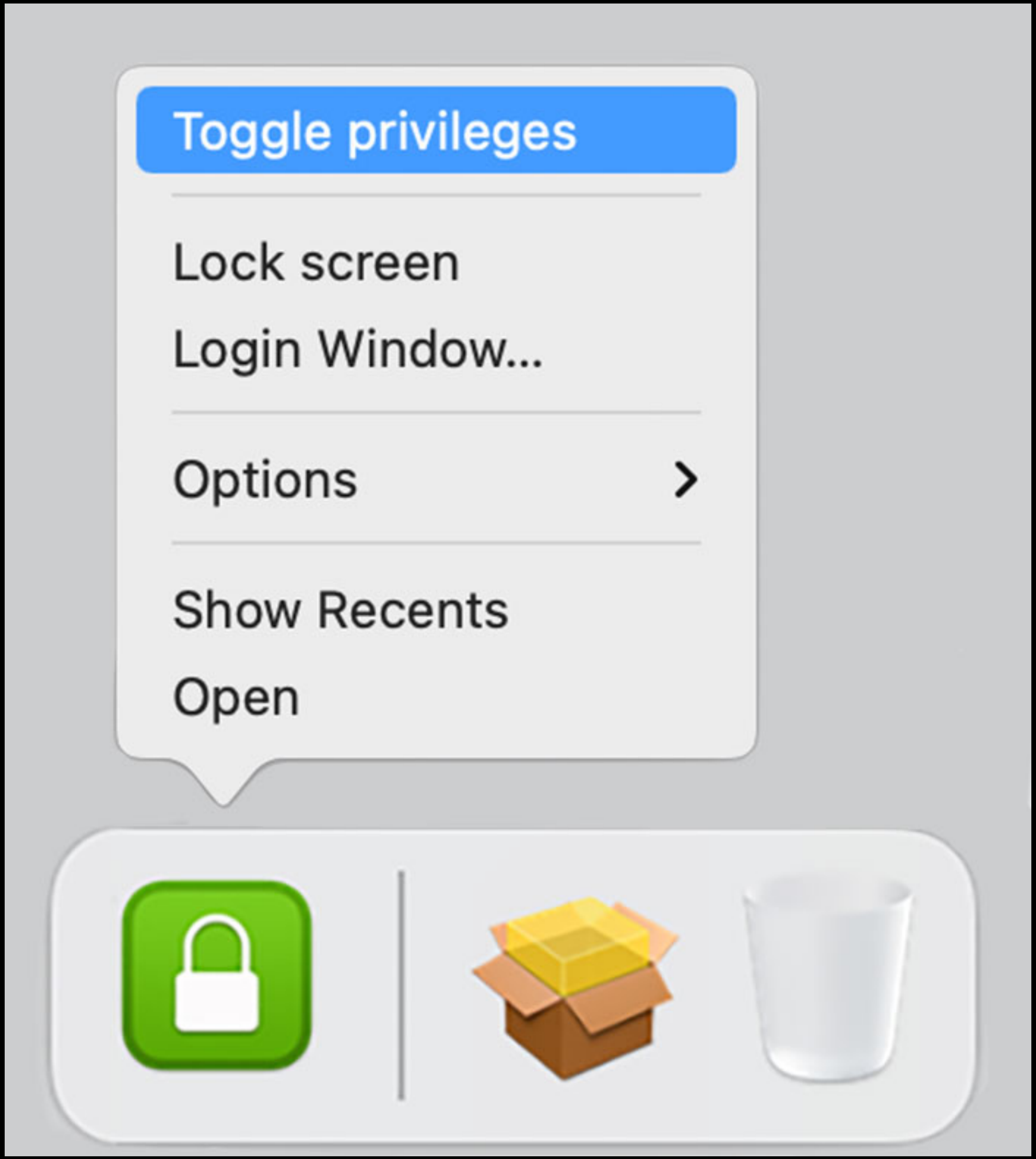


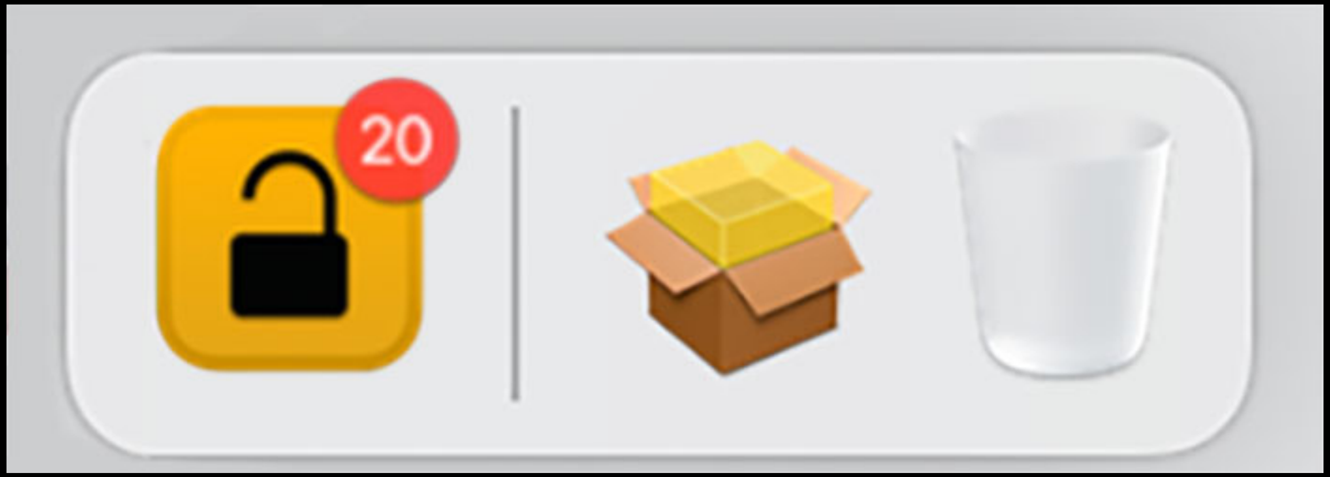
Click the lock to make changes.

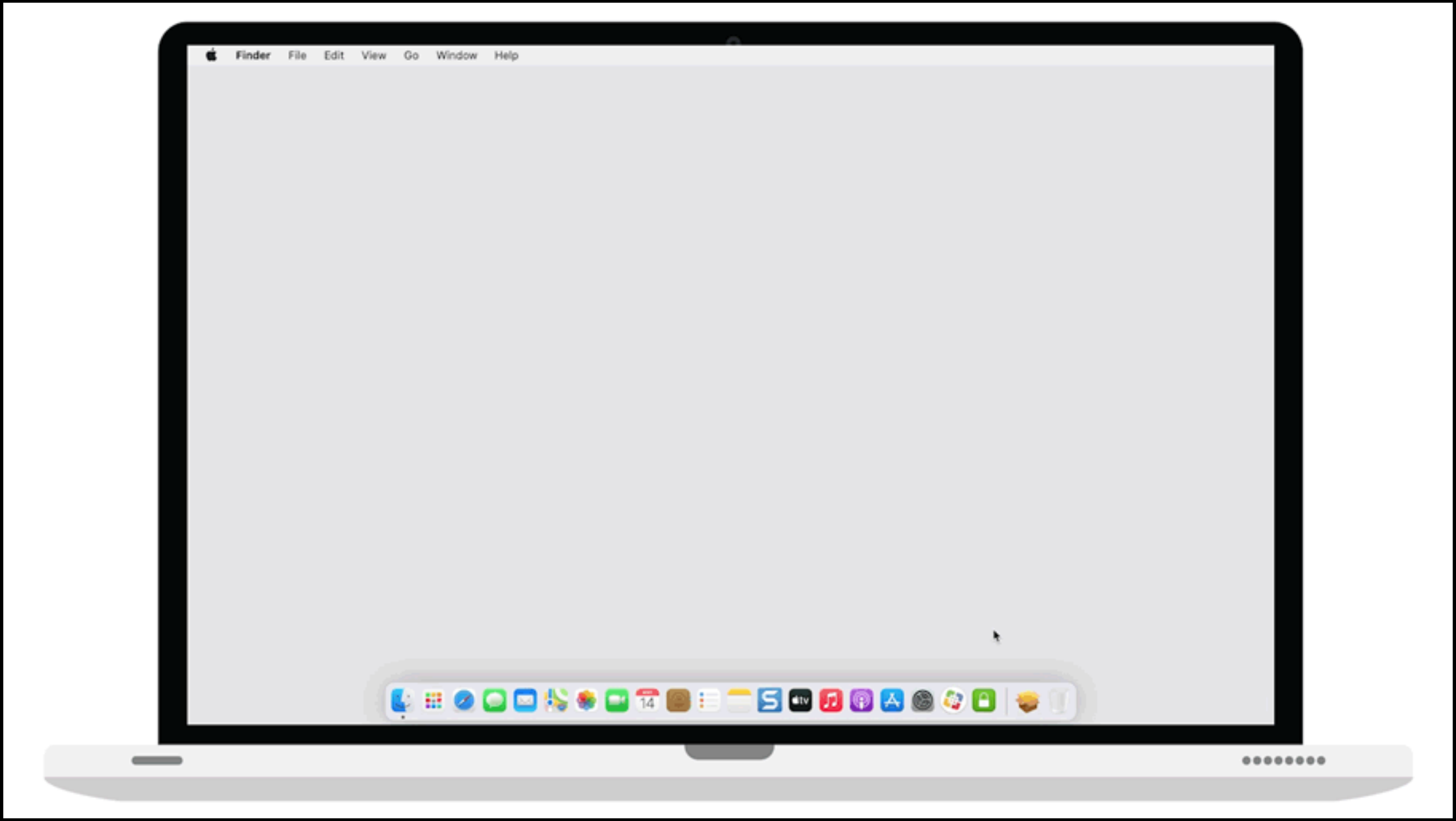

Finder
File
Edit
View
Go
Window
Help
14



Click the lock to make changes.

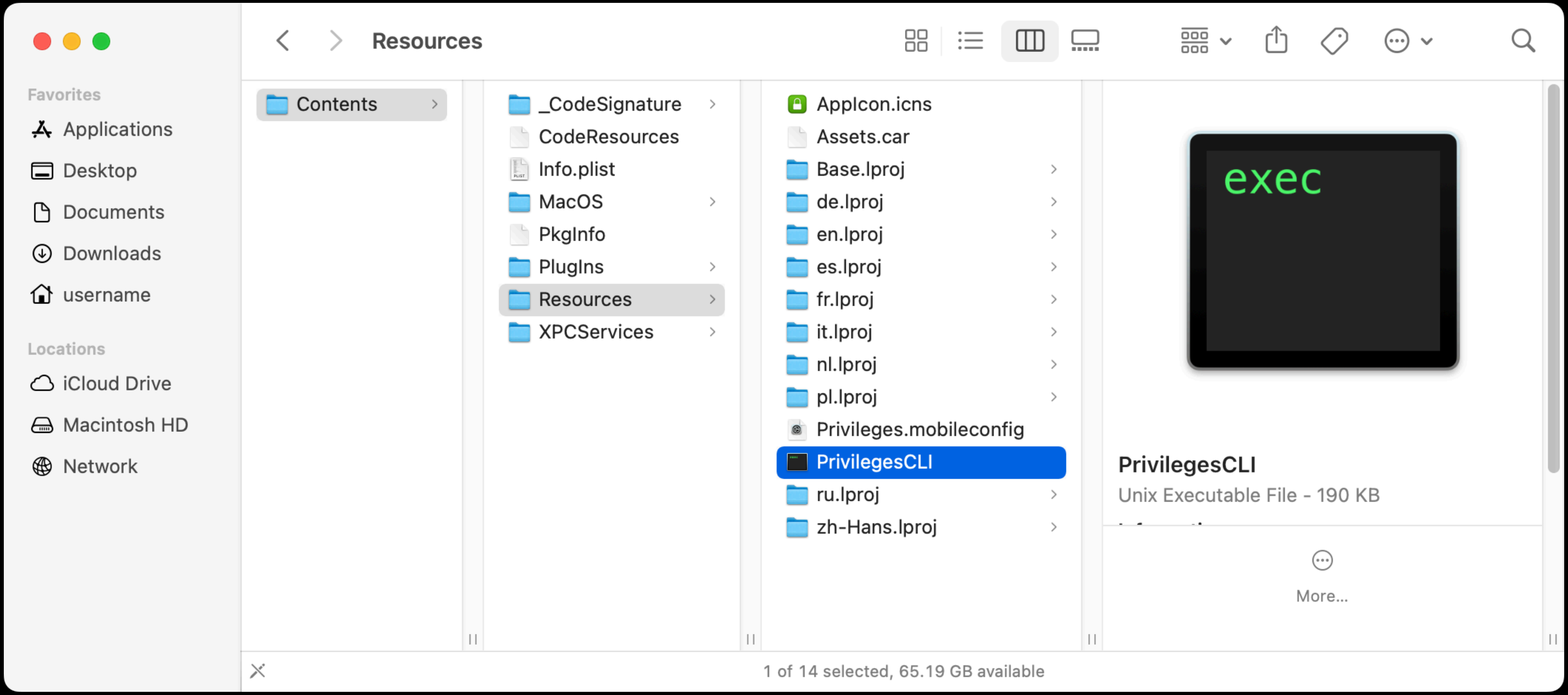

Toggle privileges
Lock screen
Login Window...
Options
Show Recents
Open


20



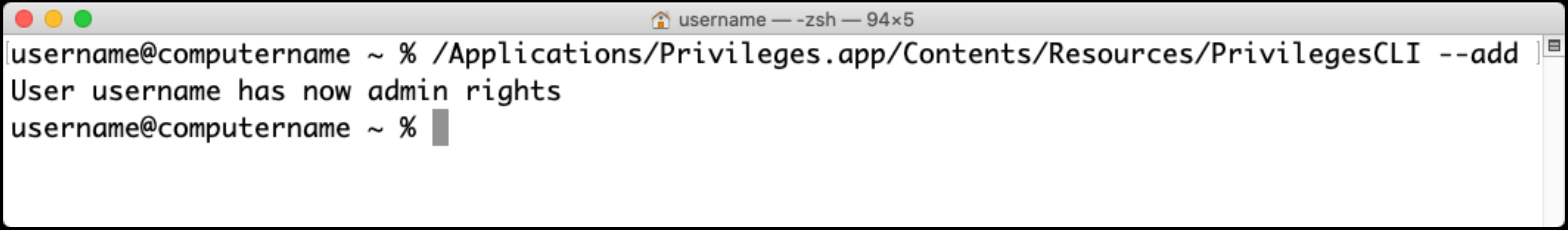
https://github.com/SAP/macOS-enterprise-privileges/wiki/Frequently-Asked-Questions

PrivilegesCLI



/Applications/Privileges.app/Contents/Resources/PrivilegesCLI

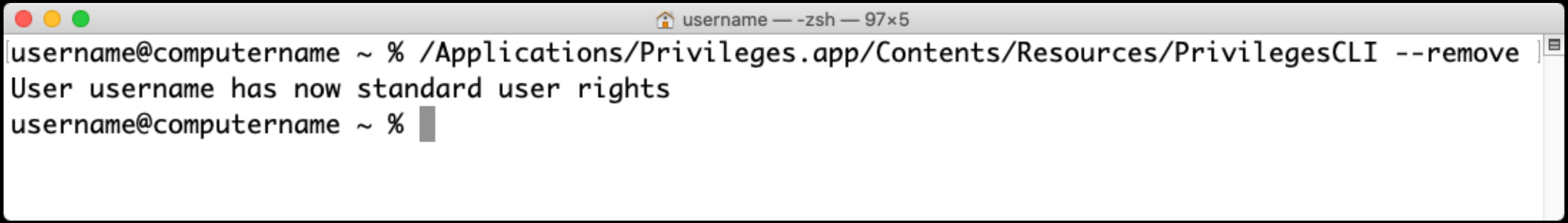
PrivilegesCLI



```
username@computername ~ % /Applications/Privileges.app/Contents/Resources/PrivilegesCLI --add
User username has now admin rights
username@computername ~ %
```

/Applications/Privileges.app/Contents/Resources/PrivilegesCLI - -add

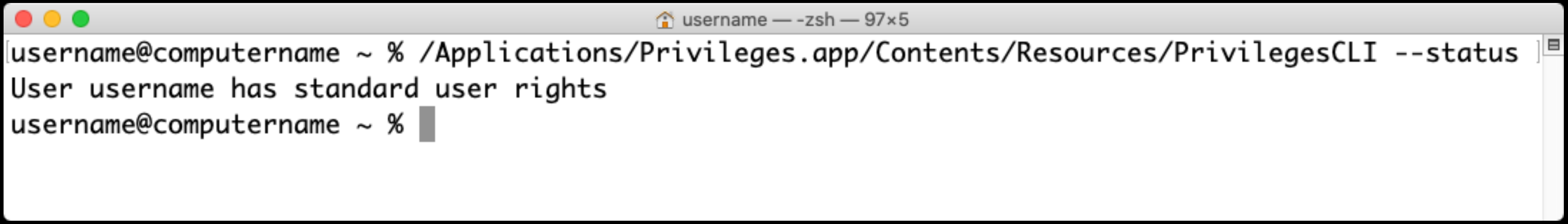
PrivilegesCLI



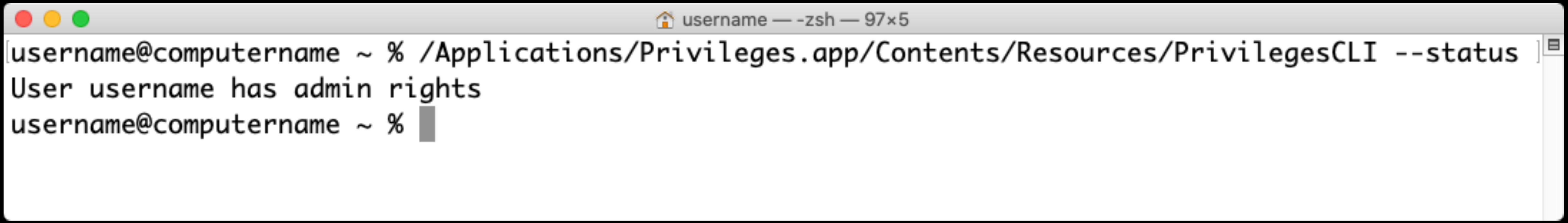
```
username@computername ~ % /Applications/Privileges.app/Contents/Resources/PrivilegesCLI --remove
User username has now standard user rights
username@computername ~ %
```

/Applications/Privileges.app/Contents/Resources/PrivilegesCLI - -remove

PrivilegesCLI



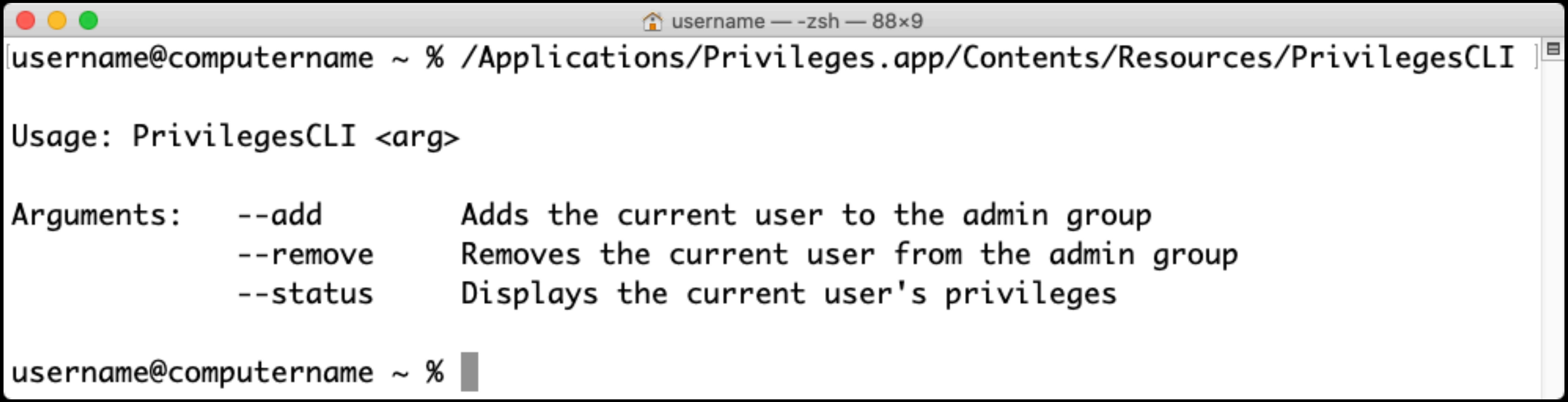
```
username@computername ~ % /Applications/Privileges.app/Contents/Resources/PrivilegesCLI --status
User username has standard user rights
username@computername ~ %
```



```
username@computername ~ % /Applications/Privileges.app/Contents/Resources/PrivilegesCLI --status
User username has admin rights
username@computername ~ %
```

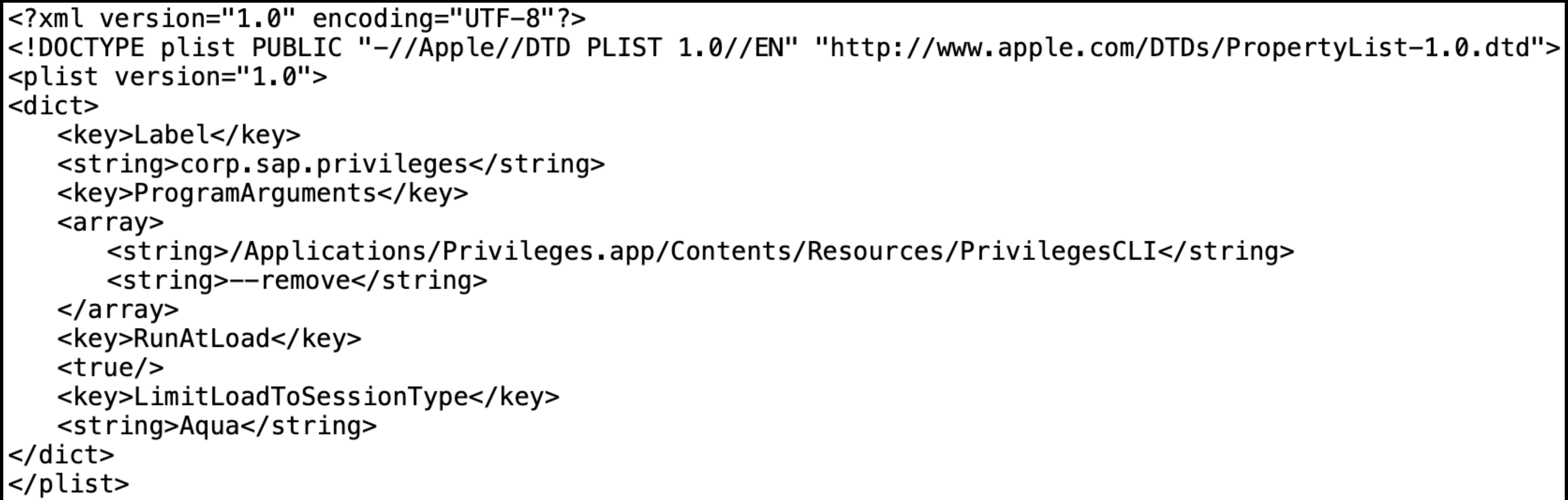
/Applications/Privileges.app/Contents/Resources/PrivilegesCLI - -status

PrivilegesCLI



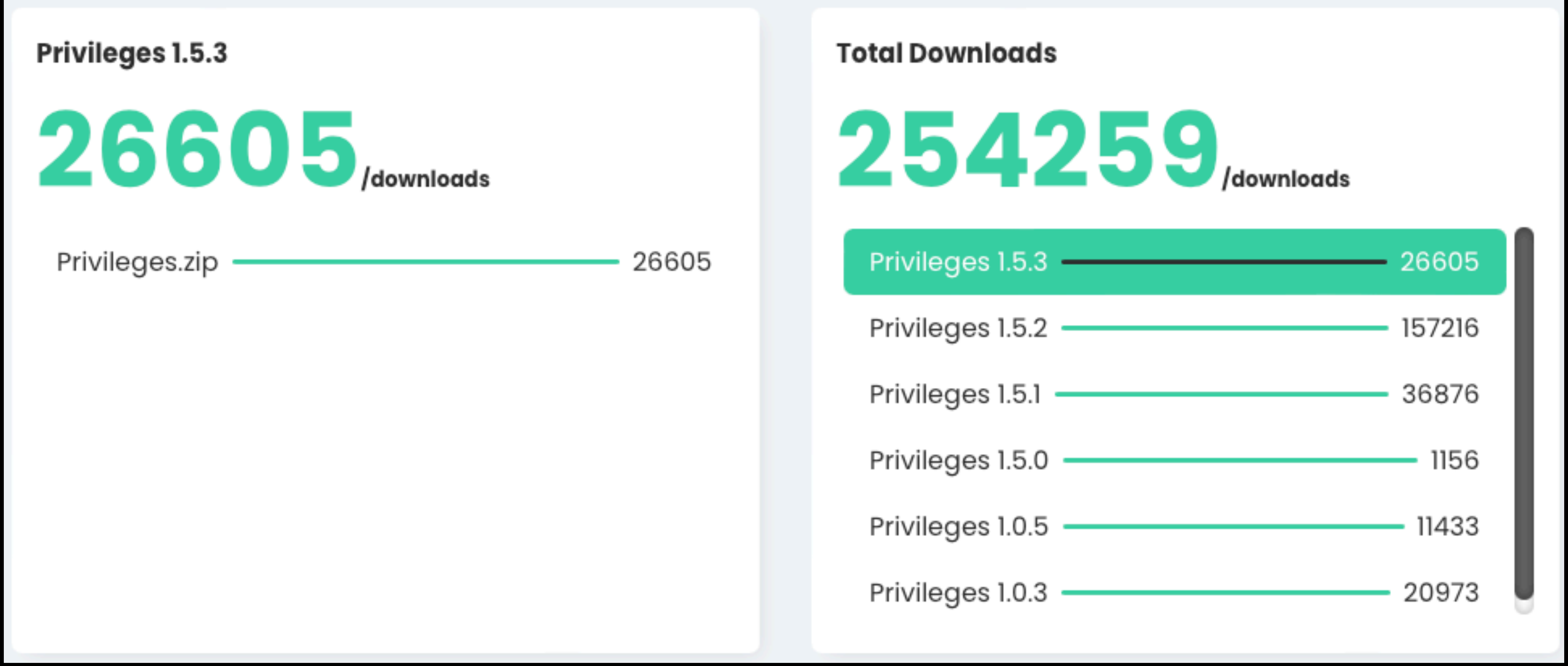
```
username@computername ~ % /Applications/Privileges.app/Contents/Resources/PrivilegesCLI

Usage: PrivilegesCLI <arg>

Arguments:    --add        Adds the current user to the admin group
              --remove     Removes the current user from the admin group
              --status     Displays the current user's privileges

username@computername ~ %
```

/Applications/Privileges.app/Contents/Resources/PrivilegesCLI



```
<?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>Label</key>
   <string>corp.sap.privileges</string>
   <key>ProgramArguments</key>
   <array>
      <string>/Applications/Privileges.app/Contents/Resources/PrivilegesCLI</string>
      <string>--remove</string>
   </array>
   <key>RunAtLoad</key>
   <true/>
   <key>LimitLoadToSessionType</key>
   <string>Aqua</string>
</dict>
</plist>
```

https://github.com/SAP/macOS-enterprise-privileges/tree/main/sample_launchagent



Privileges 1.5.3

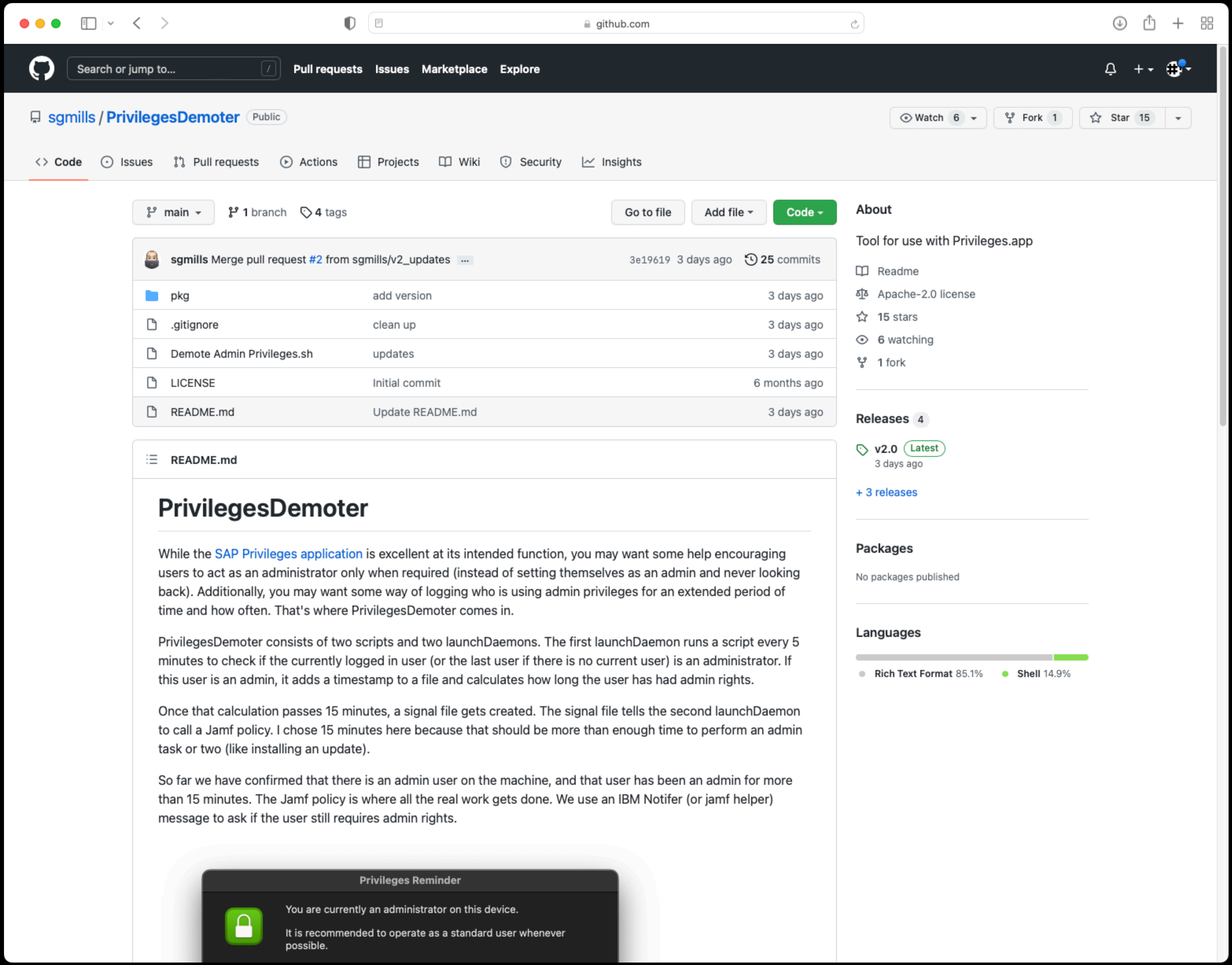
26605/downloads

Privileges.zip	26605

Total Downloads

254259/downloads

Privileges 1.5.3	26605
Privileges 1.5.2	157216
Privileges 1.5.1	36876
Privileges 1.5.0	1156
Privileges 1.0.5	11433
Privileges 1.0.3	20973



Tool for use with Privileges.app

sgmills Merge pull request #2 from sgmills/v2_updates … 3e19619 3 days ago 25 commits

pkg	add version	3 days ago
.gitignore	clean up	3 days ago
Demote Admin Privileges.sh	updates	3 days ago
LICENSE	Initial commit	6 months ago
README.md	Update README.md	3 days ago

README.md

PrivilegesDemoter

While the SAP Privileges application is excellent at its intended function, you may want some help encouraging users to act as an administrator only when required (instead of setting themselves as an admin and never looking back). Additionally, you may want some way of logging who is using admin privileges for an extended period of time and how often. That's where PrivilegesDemoter comes in.

PrivilegesDemoter consists of two scripts and two launchDaemons. The first launchDaemon runs a script every 5 minutes to check if the currently logged in user (or the last user if there is no current user) is an administrator. If this user is an admin, it adds a timestamp to a file and calculates how long the user has had admin rights.

Once that calculation passes 15 minutes, a signal file gets created. The signal file tells the second launchDaemon to call a Jamf policy. I chose 15 minutes here because that should be more than enough time to perform an admin task or two (like installing an update).

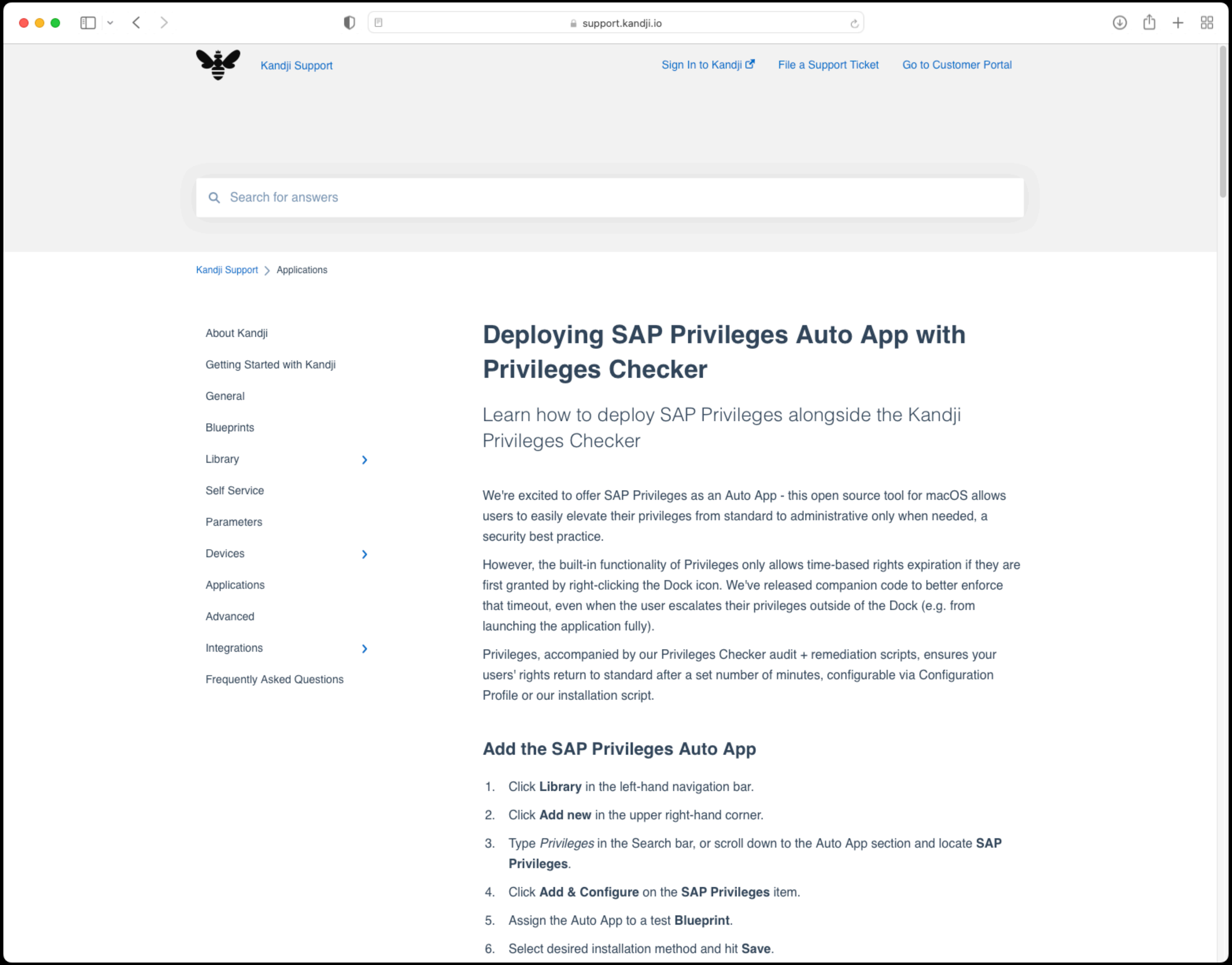
So far we have confirmed that there is an admin user on the machine, and that user has been an admin for more than 15 minutes. The Jamf policy is where all the real work gets done. We use an IBM Notifer (or jamf helper) message to ask if the user still requires admin rights.

Privileges Reminder

You are currently an administrator on this device.

It is recommended to operate as a standard user whenever possible.

https://github.com/sgmills/PrivilegesDemoter



Deploying SAP Privileges Auto App with Privileges Checker

Learn how to deploy SAP Privileges alongside the Kandji Privileges Checker

We're excited to offer SAP Privileges as an Auto App - this open source tool for macOS allows users to easily elevate their privileges from standard to administrative only when needed, a security best practice.

However, the built-in functionality of Privileges only allows time-based rights expiration if they are first granted by right-clicking the Dock icon. We've released companion code to better enforce that timeout, even when the user escalates their privileges outside of the Dock (e.g. from launching the application fully).

Privileges, accompanied by our Privileges Checker audit + remediation scripts, ensures your users' rights return to standard after a set number of minutes, configurable via Configuration Profile or our installation script.

Add the SAP Privileges Auto App

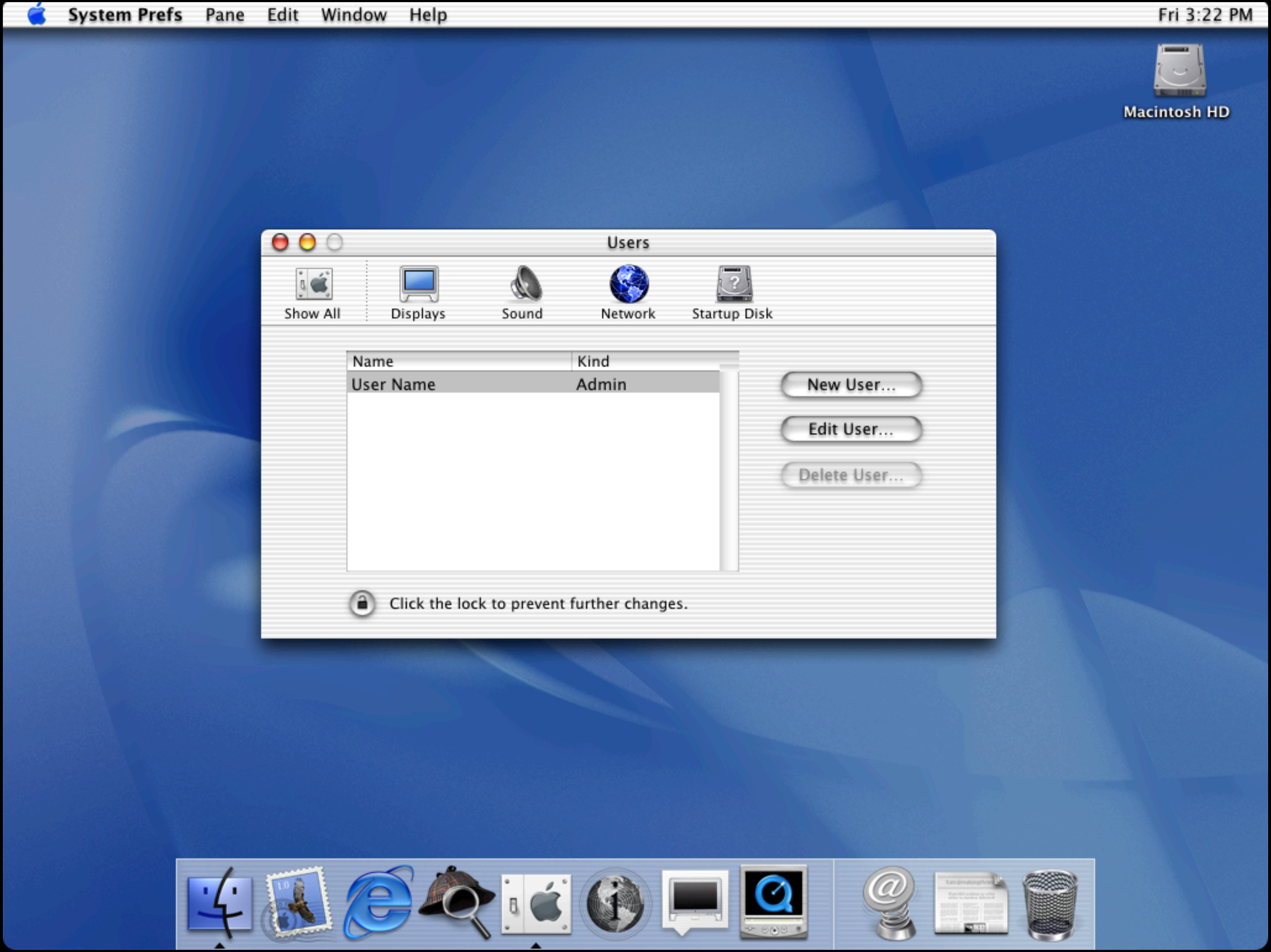
1. Click **Library** in the left-hand navigation bar.
2. Click **Add new** in the upper right-hand corner.
3. Type *Privileges* in the Search bar, or scroll down to the Auto App section and locate **SAP Privileges**.
4. Click **Add & Configure** on the **SAP Privileges** item.
5. Assign the Auto App to a test **Blueprint**.
6. Select desired installation method and hit **Save**.

https://support.kandji.io/sap-privileges

Privileges

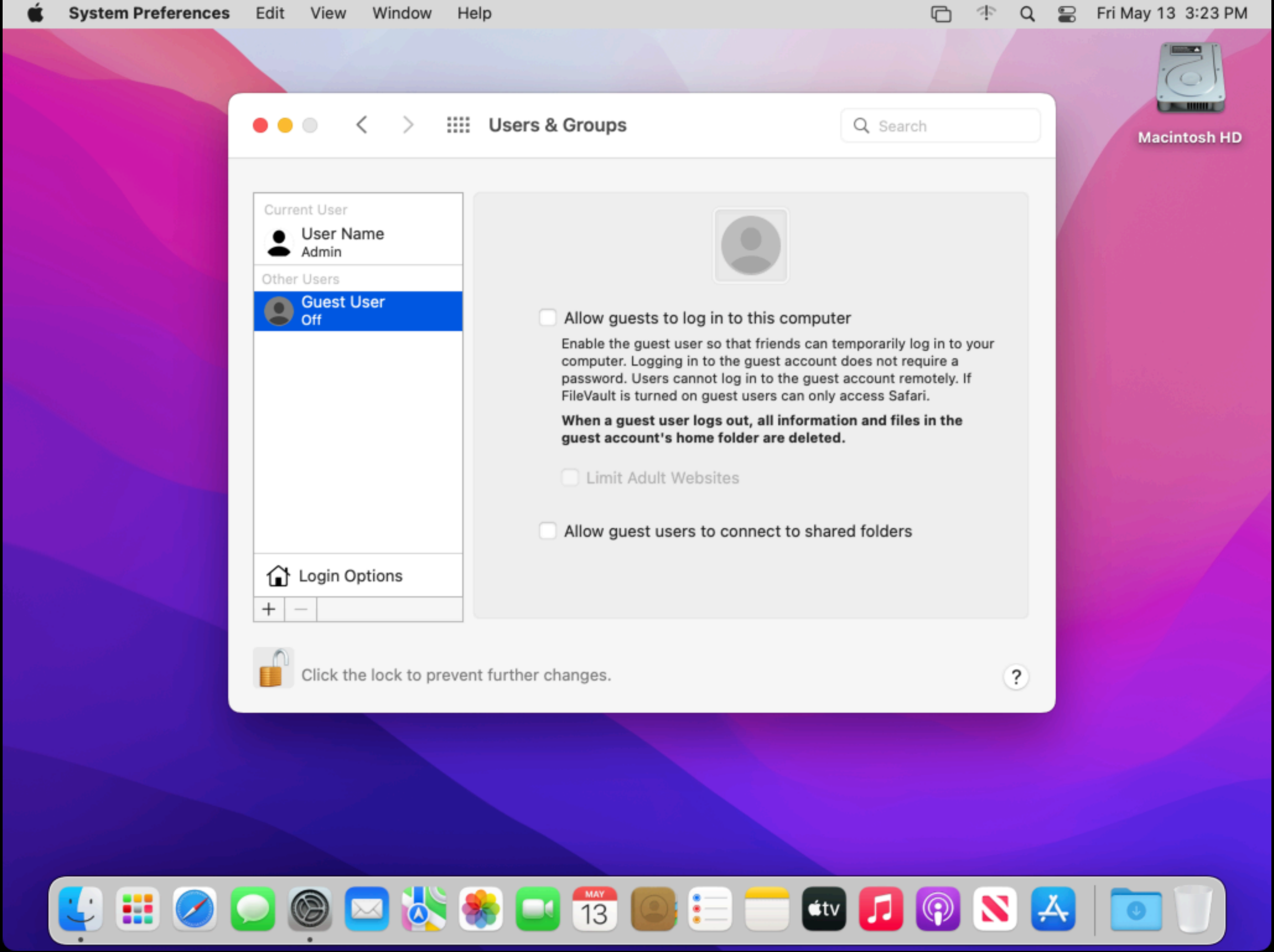
POWERED BY
TRUST
S

Anything the root account on macOS can do, an account with administrator rights can do.



Name	Kind
User Name	Admin

Click the lock to prevent further changes.



□ Allow guests to log in to this computer

Enable the guest user so that friends can temporarily log in to your computer. Logging in to the guest account does not require a password. Users cannot log in to the guest account remotely. If FileVault is turned on guest users can only access Safari.

When a guest user logs out, all information and files in the guest account's home folder are deleted.

□ Limit Adult Websites

□ Allow guest users to connect to shared folders

Click the lock to prevent further changes.

Downloads

PDF available from the following link:

https://tinyurl.com/macsysadmin2022pdf

Keynote slides available from the following link:

https://tinyurl.com/macsysadmin2022pdf