Practical Paranoia™ macOS 10.13

Marc L. Mintz, MBA-IT, ACTC, ACSP

TPP
The Practical Paranoid

Practical Paranoia: macOS 10.13 Security Essentials

Author: Marc Mintz

Editions: v1.0 20170918

Cover design by Ed Brandt

ISBN-10: 1535579323
ISBN-13: 978-1535579322

Dedication

To Candace,
without whose support and encouragement
this work would not be possible

Contents at A Glance

Contents in Detail

Practical Paranoia macOS 10.13 Security Essentials

Marc L. Mintz, MBA-IT, ACTC, ACSP

1 Thank You for Studying Practical Paranoia!

Dear student,

Thank you for getting this far into this book. Although I can't promise it will be as easy getting all the way through as it was to here, I do promise this is the easiest and most comprehensive book in this category that you can buy.

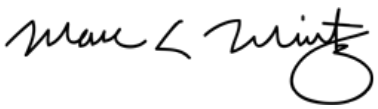
When I wrote the first edition of Practical Paranoia, I received many emails and calls from instructors, students, and fans thanking me for the book. In truth, over half of this book came out of the questions and insights provided by the readers themselves. I love the feedback. I invite you to write to me at *marc@mintzit.com*, and to visit me at *https://mintzit.com/*.

I also ask a favor. Please write a review of *Practical Paranoia*. Loved it, hated it, what worked for you, what you would like to see added or changed–I both enjoy and value your feedback.

Reviews can be difficult to come by these days. You, the reader, have the power now to make, break, and shape the evolution of a book. If you have the time, please visit my author page on Amazon.com[1]. Here you can find all my books, and leave a review.

Thank you so much for studying Practical Paranoia, and for spending time with me.

Warmly,



[1] *https://www.amazon.com/author/marclmintz*

2 Introduction

Just because you're paranoid doesn't mean they aren't after you.
–Joseph Heller[1], *Catch-22*

Everything in life is easy–once you know the how.
–Marc L. Mintz[2]

What You Will Learn In This Chapter

- Who Should Study This Course
- What Is Unique About This Course and Book
- Why Worry?
- Reality Check
- About the Author
- Practical Paranoia Updates
- Practical Paranoia Book Upgrades
- Practical Paranoia Kindle Updates
- Practical Paranoia Online Student Edition Updates
- Notes for Instructors, Teachers, & Professors
- Update Bounty

[1] *https://en.wikipedia.org/wiki/Joseph_Heller*
[2] *https://mintzit.com/*

2.1 Who Should Study This Course

Traditional business thinking holds that products should be tailored to a laser-cut market segment. Something like: *18-25-year-old males, still living at their parents' home, who like to play video games, working a minimum-wage job.* Yup, we all have a pretty clear image of that market segment.

In the case of this course, the market segment is *all users of macOS* and *OS X computers.* Really! From my great-Aunt Rose who is wrestling with using her first computer, to the small business, to the IT staff for major corporations and government agencies.

Even though the military may use better security on their physical front doors–MP's with machine guns protecting the underground bunker–compared to a residential home with a Kwikset deadbolt and a neurotic Chihuahua, the steps to secure macOS for home and business use are almost identical for both. There is little difference between *home-level security* and *military-grade security* when it comes to this technology.

The importance of data held in a personal computer may be every bit as important as the data held by the CEO of a Fortune 500. The data is also every bit as vulnerable to penetration.

2.2 What is Unique About This Course and Book

Practical Paranoia: macOS 10.13 Security Essentials is the first comprehensive macOS security book written with the new to average user in mind–as well as the IT professional. The steps outlined here are the same steps used by my consulting organization when securing systems for hospitals, government agencies, and the military.

By following the easy, illustrated, step-by-step instructions in this book, you will be able to secure your computer to better than National Security Agency (NSA) standards.

Hardening your computer security will help your business protect the valuable information of you and your customers. Should your computer work include HIPAA, SEC, or legal-related information, to be in full compliance with regulations it is likely that you will need to be using at least OS X 10.8, and I recommend macOS 10.13 or higher.

For those of you caught up in the ADHD epidemic, do not let the number of pages here threaten you. This book is a quick read because it has lots of actual screenshots. Written for use in our *Practical Paranoia: Security Essentials Workshops* as well as for college classroom and self-study, this book is the ultimate step-by-step guide for protecting the new macOS user who has no technical background, as well as for the experienced IT consultant. The information and steps outlined are built on guidelines, policies & procedures, and best practices from Apple, the NSA, NIST, US-CERT, and my own 30 years as an IT and Apple consultant, developer, technician and trainer. I have reduced dull background theory to a minimum, including only what is necessary to grasp the need-for and how-to.

The organization of this book is simple. We provide chapters representing each of the major areas of vulnerability, and the tasks you will do to protect your data, device, and personal identity.

Although you may jump in at any section, I recommend you follow the sequence provided to make your system as secure as possible. Remember, the bad guys will not attack your strong points. They seek out your weak points. Leave no obvious weakness and they will most likely move on to an easier target.

To review your work using this guide, use the *macOS Security Checklist* provided at the end of this book.

Theodore Sturgeon, an American science fiction author and critic, stated: *Ninety percent of everything is crap*[3]. Mintz's extrapolation of Sturgeon's Revelation is: *Ninety percent of everything you have learned and think to be true is crap.*

I have spent most of my adult life in exploration of how to distill what is real and accurate from what is, well, Sturgeon's 90%. The organizations I have founded, the workshops I've produced, and the *Practical Paranoia* book series all spring from this pursuit. If you find any area of this workshop or book that you think should be added, expanded, improved, or changed, I invite you to contact me personally with your recommendations.

[3] *https://en.wikipedia.org/wiki/Sturgeon%27s_law*

2.3 Why Worry?

In terms of network, Internet, and data security, macOS users must be vigilant because of the presence of malware[4] such as viruses, Trojan horses, worms, phishing, and key loggers impacting our computers. Attacks on computer and smartphone users by tricksters, criminals, and governments are on a steep rise. In addition to macOS-specific attacks, we are vulnerable at points of entry common to all computer users, including Flash, Java, compromised websites, and phishing, as well as through simple hardware theft. How bad is the situation?

- Per a study by Symantec, an average enterprise-wide data breach has a recovery cost of $5 million.
- Per the FBI, 2 million laptops are stolen or lost in the U.S. each year.
- Of those 2 million stolen or lost, only 3% ever are recovered.
- Out of the box, an macOS computer can be broken into–bypassing password protection–in less than 1 minute.
- The typical email is clearly readable at dozens of points along the Internet highway on its trip to the recipient. Most likely, that email is read by somebody you don't know.
- A popular game played by high school and college students is *war driving*: the act of driving around neighborhoods to find Wi-Fi networks, geographically marking the location for others to use and break into.
- The Cyber Intelligence Sharing and Protection Act (CISPA)[5] allows the government easy access to all your electronic communications. PRISM[6] allows government agencies to collect and track data on any American device.

The list goes on, but we have lives to live and you get the point. It is not a matter of *if* your data will ever be threatened. It is only a matter of *when,* and how often the attempts will be made.

---

[4] *http://en.wikipedia.org/wiki/Malware*
[5] *http://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act*
[6] *http://en.wikipedia.org/wiki/PRISM_ (surveillance_program)*

2.4 Reality Check

Nothing can 100% guarantee 100% security 100% of the time. Even the White House and CIA websites and internal networks have been penetrated. We know that organized crime, as well as the governments of China, North Korea, Russia, Great Britain, United States, and Australia have billions of dollars and tens of thousands of highly skilled security personnel on staff looking for *zero-day exploits*[7]. These are vulnerabilities that have not yet been discovered by the developer. As if this is not enough, the U.S. government influences the development and certification of most security protocols. This means that industry-standard tools used to secure our data often have been found to include vulnerabilities introduced by government agencies.

With these odds against us, should we just throw up our hands and accept that there is no way to ensure our privacy? Well, just because breaking into a locked home only requires a rock through a window, should we give up and not lock our doors?

Of course not. We do everything we can to protect our valuables. When leaving on vacation we lock doors, turn on the motion detectors, notify the police to prompt additional patrols, and stop mail and newspaper delivery.

The same is true with our digital lives. For the very few who are targeted by the NSA or whackadoodle ex, there is little that can be done to completely block them from reading your email, following your chats, and recording your web browsing. But you can make it extremely time and labor intensive for them to do so.

For most of us not subject to an NSA targeted attack, we are rightfully concerned about our digital privacy being penetrated by criminals, pranksters, competitors, nosy people, as well as about the collateral damage caused by malware infestations.

You *can* protect yourself, your data, and your devices from such attack. By following this book, you should be able to secure fully your data and your first device in two days, and any additional devices in a half day. This is a very small price to pay for peace of mind and security.

---

[7] *https://en.wikipedia.org/wiki/Zero-day_(computing)*

Remember, penetration does not occur at your strong points. A home burglar will avoid hacking at a steel door when a simple rock through a window will gain entry. A strong password and encrypted drive by themselves do not mean malware can't slip in with your email, and pass all your keystrokes – including usernames and passwords – to the hacker.

It is imperative that you secure all points of vulnerability.

- Note: Throughout this book we provide suggestions on how to use various free and for-fee applications to help enforce your protection. Neither Marc L. Mintz, Mintz InfoTech, Inc., nor The Practical Paranoid, LLC. receives payment for suggesting them. We have used them with success, and thus feel confident in recommending them.

2.5 About the Author

Marc Louis Mintz is one of the most respected IT consultants and technical trainers in the United States. His technical support services and workshops have been embraced by hundreds of organizations and thousands of individuals over the past 3 decades.

Marc holds an MBA-IT (Masters of Business Administration with specialization in Information Technology), Chauncy Technical Trainer certification, Post-Secondary Education credentials, and over a dozen Apple certifications.

Marc's enthusiasm, humor, and training expertise have been honed on leading edge work in the fields of motivation, management development, and technology. He has been recruited to present software and hardware workshops nationally and internationally. His technical workshops are consistently rated by seminar providers, meeting planners, managers, and participants as *The Best* because he empowers participants to see with new eyes, think in a new light, and problem solve using new strategies.

When away from the podium, Marc is right there in the trenches, working to keep client Android, iOS, macOS, and Windows systems securely connected.

The author may be reached at:
Marc L. Mintz
The Practical Paranoid LLC.
1000 Cordova Pl
#842
Santa Fe, NM 87505
+1 888.504.5591
Email: *marc@thepracticalparanoid.com*
Web: *http://mintzIT.com* • *http://thepracticalparanoid.com*

2.6 Practical Paranoia Updates

Information regarding IT security changes daily, so we offer you newsletter, blog and Facebook updates to keep you on top of everything.

Newsletter

Stay up to date with your Practical Paranoia information by subscribing to our free weekly newsletter.

1. Visit *https://thepracticalparanoid.com*
2. Scroll to the bottom of the home page to the *Newsletter Signup* form.
3. Enter your email and full name, and then click the *Sign Up* button.

Blog

Updates and addendums to this book also will be included in our free *Practical Paranoia blog*. Go to: *https://thepracticalparanoid.com*, and then select the *Security Blog* link.

Facebook

Updates and addendums to this book also will be found in our *Practical Paranoia Facebook Group*. Go to *https://www.facebook.com/groups/PracticalParanoia/*

2.7 Practical Paranoia Paperback Book Upgrades

We are constantly updating *Practical Paranoia* so that you have the latest, most accurate resource available. If at any time you wish to upgrade to the latest version of *Practical Paranoia* at the lowest price we can offer:

1. Tear off the front cover of ***Practical Paranoia***.
2. Make check payable to Mintz InfoTech for $30.
3. Send front cover, check, and mailing information to:
   The Practical Paranoid, LLC.
   1000 Cordova Pl
   #842
   Santa Fe, NM 87505
4. Your new copy of ***Practical Paranoia*** will be sent by USPS. Please allow up to 4 weeks for delivery.

2.8 Practical Paranoia Kindle Updates

We are constantly updating *Practical Paranoia* so that you have the latest, most accurate resource available. If at any time you wish to update to the latest Kindle version of *Practical Paranoia* at no cost:

1. Delete the copy of *Practical Paranoia* currently installed on your Kindle device.
2. Download the current edition of *Practical Paranoia.*

2.9 Practical Paranoia Online Live Student Edition Updates

We are constantly updating *Practical Paranoia* so that you have the latest, most accurate resource available. The Online Student Edition is a streaming pdf version of the book. To update:

1. Quit Google Chrome (the only browser compatible with the Online Student Edition).
2. Launch Google Chrome
3. Go to your *Google Drive* portal > *Shared With Me*
4. The new version will load into your browser

2.10 Notes for Instructors, Teachers, & Professors

If you are conducting IT/CS courses that include Practical Paranoia books, we will provide to you at no charge sample exams (with answers), PowerPoint presentation, as well as voice and email access to the authors. We are committed to keeping the entire Practical Paranoia series the best solution to your security courses.

We strongly recommend opting for the online digital version of the Practical Paranoia books. These allow the students and teacher to always have the most current version (as we update as the technology changes, we often update every month or two), at a lower price than either the paperback or kindle versions.

Please contact our office for details:

Email: info@thepracticalparanoid.com
Voice: +1 888.504.5591

2.11 Update Bounty

Although we work tirelessly to keep the contents of this workbook up to date, every now and then something slips by us. If you discover anything in this workbook that doesn't reflect current reality, *and* you are the first to report it to us, you will receive a free copy of any *Practical Paranoia Security Essentials*.

To make an update bounty report:

Email: info@thepracticalparanoid.com
Voice: +1 888.504.5591

3 Data Loss

Weather forecast for tonight: Dark.

–George Carlin[1]

I know, you want to jump right into cyber security and harden your awesome macOS computer. Sorry to be a Debbie Downer[2], but there is a very real risk of losing data in the process of some of the work ahead of us. Because of this, we must begin our exciting journey into the heart of security with drudgery–backing up your computer.

What You Will Learn In This Chapter

- The need for backups
- Format the backup drive
- Configure Time Machine
- Integrity Test Time Machine
- Install and configure Carbon Copy Cloner
- Integrity test the clone backup

[1] *https://en.wikipedia.org/wiki/George_Carlin*
[2] *https://en.wikipedia.org/wiki/Debbie_Downer*

3.1 The Need for Backups

Data loss is a very real fact of life. It is not a matter of *if* you will experience data loss, just a matter of when, and how often. Only a small percentage of computer users back up on a regular basis. I suspect these are the folks who have experienced catastrophic data loss and never want a repeat.

There are many sources of data loss. The top contenders include:

- Computer theft
- Power surges
- Power sags
- Sabotage
- Fire
- Water damage. I personally have had 3 clients who have lost computers due to cats or dogs marking their territory, and my own cat took out a $4,000 monitor with nothing more than a hairball.
- Entropy / aging of the drive
- Malware
- Terrorist activities
- Criminal activities
- Static electricity
- Physical shock to the drive (banging the computer, dropping, etc.)

Best Practice[3] calls for three backups:

- **One full backup onsite**. This allows for almost immediate recovery of lost or corrupted documents, or full recovery of the OS, applications, and documents in the event of complete loss of the hard drive.

[3] *https://en.wikipedia.org/wiki/Best_practice*

- **One full backup offsite**. This is your *Plan B* in the event of a catastrophic loss of both the computer and the onsite backup. This typically takes the form of fire or theft.
- **One Internet-based backup**. This is your OMG, what do I do now? fallback plan. Many people substitute the Internet backup for the offsite. A potential problem is that your Internet backup may take several days to weeks to download.

Onsite Full Backup with Time Machine

macOS comes with the most advanced backup software for any computer–Time Machine. Time Machine has several advantages over other options, including:

- Free
- Highly reliable and stable
- Low resource requirements
- Maintains document versioning. With each run, Time Machine will back up the latest version of your documents, while maintaining all prior versions as well
- Runs in the background every hour without user intervention
- Works with Migration Assistant (part of the standard macOS installation) to replicate the last backup to another Macintosh.
- Does backup to a FireWire, Thunderbolt, or USB drive attached locally, to an Apple Airport Extreme Base Station, or a computer running macOS Server
- Can create an encrypted backup to a locally attached drive (Mac OS X 10.7 and above, macOS 10.12 and above), or to a drive attached to an Airport Extreme or macOS Server (10.12 and above) or OS X Server (10.8 and above)

As a rule, the backup drive should be at least double the size of your data, preferably quadruple. This allows for future growth and the maintenance of long-term document versioning.

Onsite Full Backup with Carbon Copy Cloner

As great as Time Machine is, there is one critical area in which it fails–it does not create a bootable clone. A bootable clone is an exact duplicate of the original drive. This is where Carbon Copy Cloner comes in. Advantages:

- Commercial software
- Highly reliable and stable
- Low resource requirements
- Maintains document versioning
- Runs on your schedule
- Bootable
- Backs up over FireWire, Thunderbolt, or USB drive attached locally
- Backs up to network drives (not bootable)
- Encrypted

The need for a bootable clone backup becomes clear when you have a hard drive failure. Without a bootable clone, the recovery process looks like this:

1. Call a technician for assistance or rush to the store to buy a new drive.
2. Remove the old drive, install the new drive.
3. Install macOS.
4. Install all updates.
5. Use Migration Assistant to copy over the latest backup from Time Machine.
6. Get back to work–4 to 8 hours after the crash.

With a bootable clone, the recovery process looks like this:

1. Restart your Mac with the option key held down. This triggers the Start Manager, allowing you to select from which drive to boot.
2. Select the bootable clone drive as your boot drive.
3. Get back to work–5 minutes after the crash.

4. Call a technician for assistance. Let them know there is no rush.
5. At a time that is convenient (and not on overtime) the problem drive is replace and all data copied over.

So why use Time Machine? It is the fastest and easiest way to recover lost or damaged documents.

Offsite Full Backup

An offsite full backup is the same as the onsite backup, but after the backup completes, the backup storage device is stored offsite. This should be performed at least once per month, preferably once per week.

A good choice for off-site location is a safety deposit box or a trusted friend's house. The idea is to have easy access to a full backup of your computer in case of a disaster like a fire or robbery that leaves you without your on-site backup. This option will allow much faster recovery than the cloud backup option at the expense of possibly being a week or two out of date. The average user does not create very much data in such a short time frame so you can easily grab your most recent changes from the online backup in case of disaster.

Internet-Based Data Backup

There are several great and unique advantages to Internet-based backups:

- If a small black hole opens devouring your computer, backup and offsite backup, your Internet backup will always be waiting for you. Think disaster recovery after a multi-block explosion, fire destroys your home or business, or terrorist activity that prevents access to either the computer or off-site location.
- Should you find yourself far away from your computer, your data can be accessed from any computer.
- A few of the Internet-based options now include sharing access to any documents that have been backed up.

When looking for the right Internet-based backup service, in addition to cost, features, company and software stability, keep an eye out for document versioning. You want your service to keep at least one month of document versions. If you accidentally delete a document, it will remain on the server for at least a month, or if a document corrupts, you want to be able to go back to a previous (presumably not corrupted) version.

My personal favorites include:

Backblaze[4]. Easy to use, very fast uploads, rock solid stable, 30-day document versioning, backs up all user accounts. For home and business.

Carbonite[5]. Fast uploads, rock solid stable, limited document versioning, backs up all user accounts. 30-day document versioning, family and business accounts make it easier to administer multiple computers.

CrashPlan Pro[6]– for business. Fast upload, rock solid stable, document versioning, lifetime document versioning, individual and business accounts. Can meet your HIPAA or SEC compliance needs.

Google Drive presents a hybrid solution. In addition to providing cloud storage and file sharing, extensions such as *Backupify* provide a cloud-based backup of your cloud-based storage. Google *G-Suite Enterprise* includes cloud-based backup with the package.

3.1.1 Assignment: Format the Backup Drive for Time Machine or Carbon Copy Cloner

Redundancy calls for two on-site backups. My preference is to use two tools, one for each backup–Time Machine and Carbon Copy Cloner.

In this assignment, you format a drive for use with either. If you will be following my approach and have two backups, repeat this process with each of two drives.

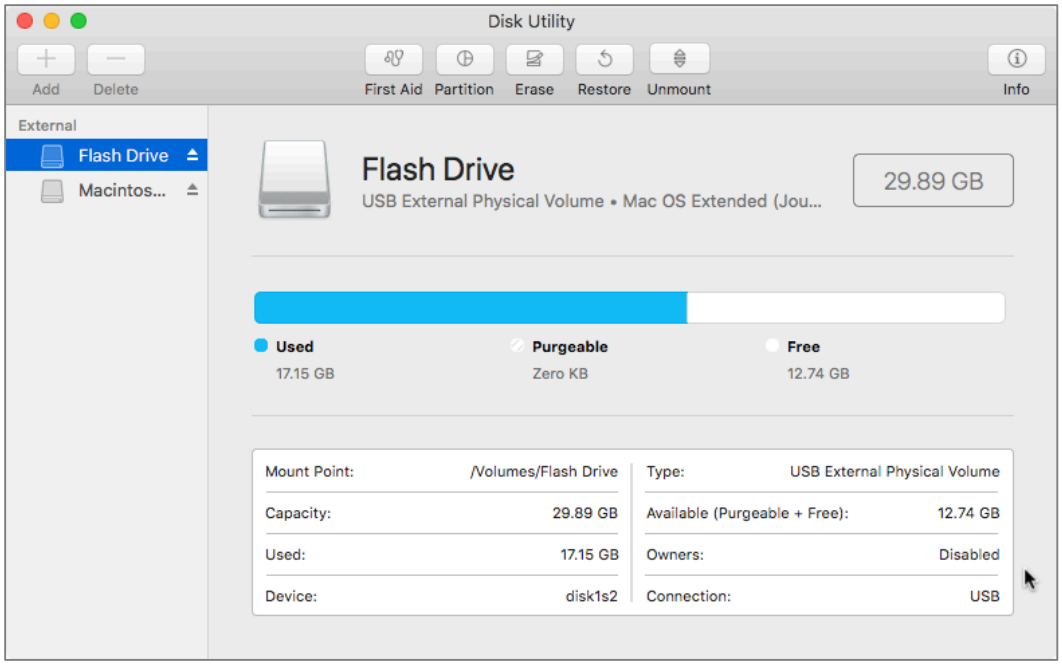
[4] *http://www.backblaze.com*
[5] *http://www.carbonite.com*
[6] *http://www.crashplan.com*

1. Purchase an external hard drive that has at least four times the capacity of the data to be held on the host computer. We strongly recommend purchasing a drive with FireWire 800, USB 3, USB 3.1, or Thunderbolt. Although you pay up to $50 extra upfront, these drives are significantly faster than those with FireWire 400 or USB 2. That speed makes a huge difference as you are sweating blood trying to recover your data.
2. Connect the new drive to your computer.
3. Open Disk Utility, located in your */Applications/Utilities* folder.

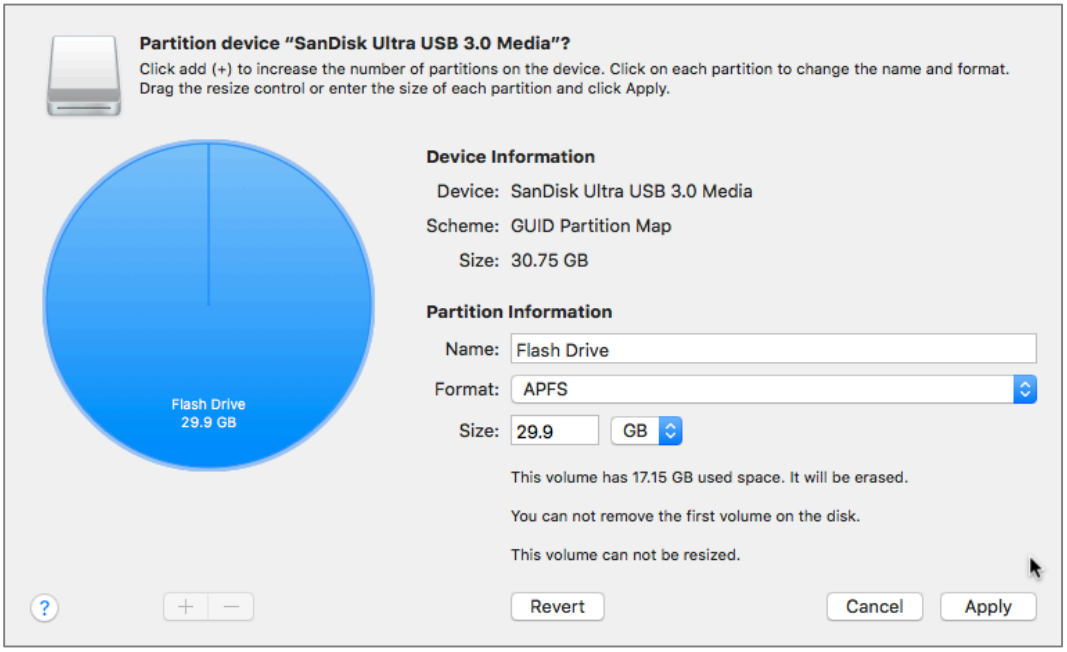
Change Volume format to APFS

It is most likely the drive you have purchased is in either FAT or NTFS format. To be used by Time Machine (or Carbon Copy Cloner), the format of the volume will need to be APFS (macOS 10.13 native) or OS X Extended (Journaled) (macOS 10.12 and earlier native).

4. Select name of the drive from the sidebar, and then select the *Partition* button in the tool bar.

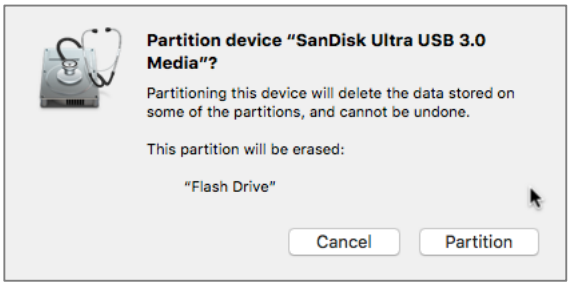


5. The *Partition* window opens.

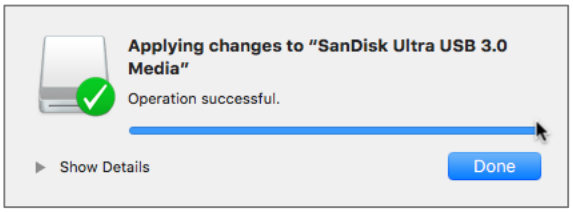


- In the *Name* field, enter the name you want displayed for this drive.
- In the *Format* field, select *APFS*, and then select the *Apply* button.
    - Note: Selecting *OS X Extended (Journaled)* will also work, and maintain compatibility with previous versions of OS X/macOS.

6. In the *Partition device* window, select the *Partition* button.



7. In the *Disk Utility* window, select the *Done* button.



3.1.2 Assignment: Configure Time Machine

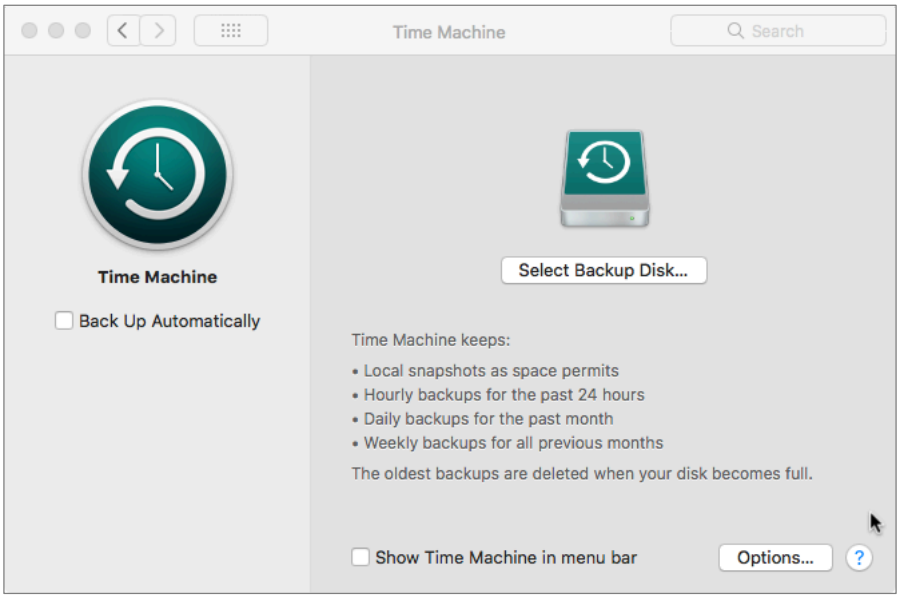
Although Time Machine is designed to auto-configure, that doesn’t mean it has auto-configured correctly.

In this assignment, you configure Time Machine to back up to a drive formatted in the previous assignment

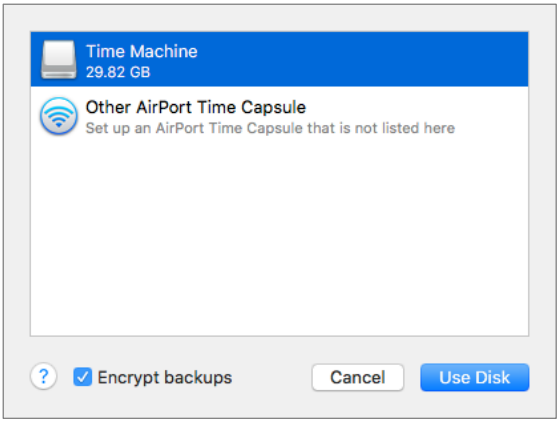
- Prerequisite: Completion of the previous assignment.

1. Attach your Time Machine drive. If you have followed the steps above, it is already attached and mounted.

2. Open *Apple* menu > *System Preferences* > *Time Machine*. Enable the *Back Up Automatically* checkbox.

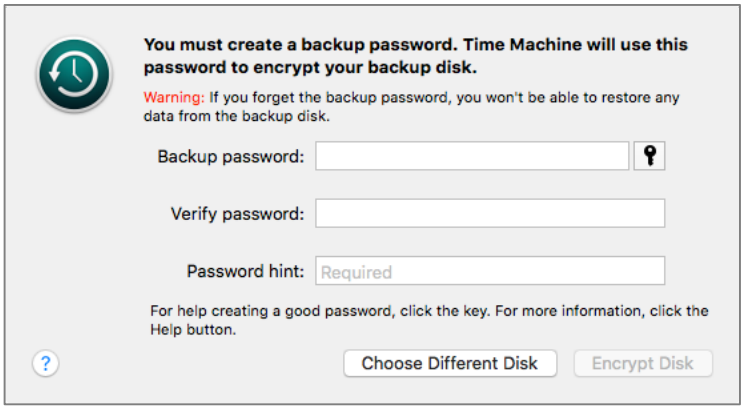


3. All drives available to serve as backup drives appear. Select your Time Machine drive, enable the *Encrypt backups* checkbox, and then select the *Use Disk* button.



4. In the *Backup password* field, enter a password to encrypt the backup drive. I recommend using your account login password for your computer. Enter it again in the *Verify password* field. In the *Password hint* field, enter a character

or two as it is required to have an entry, but, come on, a hint? *Really?!* Then select the *Encrypt Disk* button.



5. Quit System Preferences.

Time Machine will automatically start to back up to this drive within the hour.

3.1.3 Assignment: Integrity Test the Time Machine Backup

To test your Time Machine backup, you need to enter Time Machine, and then verify the existing backups. If you have a portable Mac, it is likely that you have two different backups–one on your Time Machine drive, and the other on your laptop itself. The local snapshots[7] are created when Time Machine auto launches but does not find the Time Machine drive connected.

You can see the two backups in the Time Machine window. Backups that can be restored now from either the snapshot or backup drive appear in bright red. When the backup drive is not connected, only the snapshots are bright red and can be restored, and the backups only available on the backup drive appear in dim red.

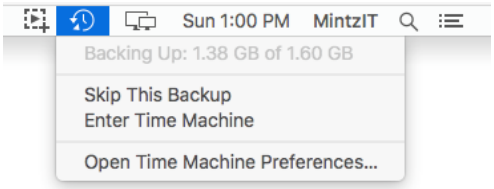
In this assignment, you verify the Time Machine backup.

Verify from the Menu Icon

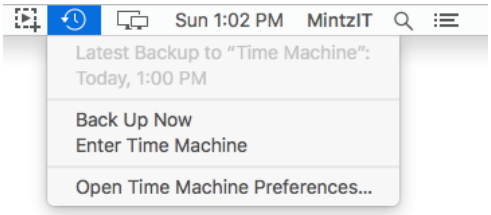
1. From the Finder menu, click the *Time Machine* menu icon.

[7] *https://support.apple.com/en-us/HT204015*

- If it says *Backup Up: X MB of X GB,* Time Machine is currently backing up.



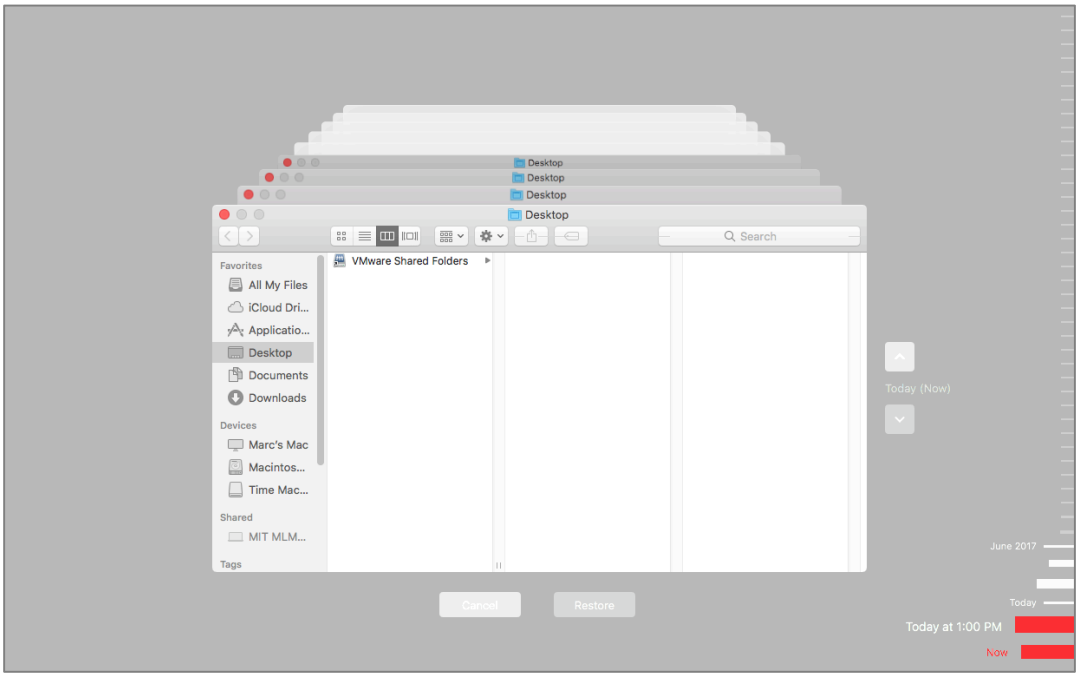
- If it says *Latest Backup…* and reports a date/time within the past couple of hours, it is current.



Verify from Time Machine

2. From the menu bar, select the *Time Machine* icon > *Enter Time Machine* menu.
3. When in Time Machine, look to the right-hand edge of your screen. If you see a series of tick marks that display date and time as the cursor moves over them, Time Machine has performed backups.

4. Verify the latest time stamp (at the bottom) is current.



Congratulations! You have verified your Time Machine backup is working properly.

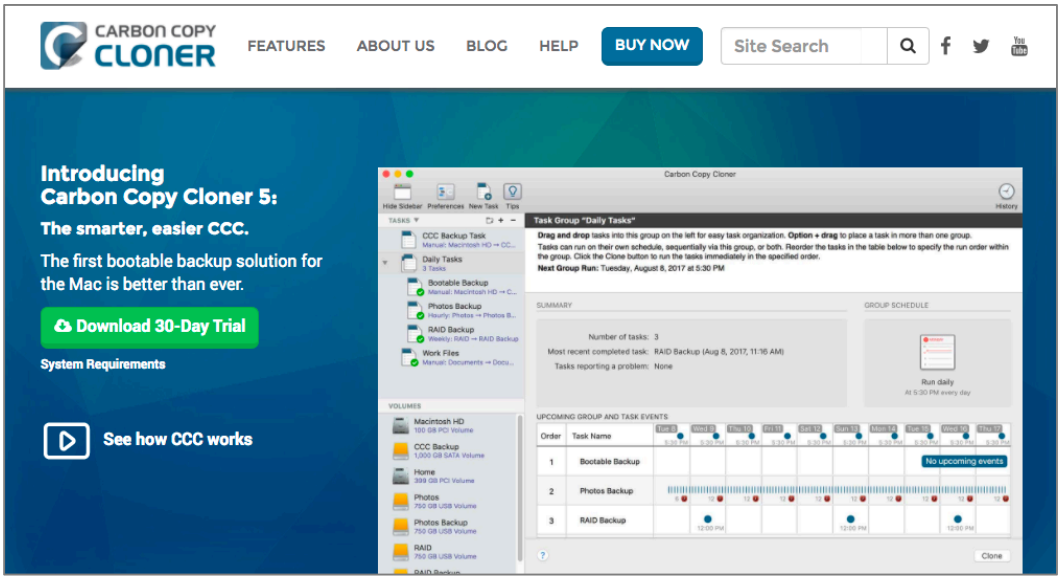
3.1.4 Assignment: Install and Configure Carbon Copy Cloner

In this assignment, you download, install, and then configure Carbon Copy Cloner to create a bootable clone backup of your boot drive.

- Prerequisite: Completion of the previous assignment 3.1.1: *Format the Backup Drive for Time Machine or Carbon Copy Cloner.*
- Note: As of this writing, Carbon Copy Cloner has not been certified to work with macOS 10.13. I anticipate this will be resolved before the final version of 10.13 is released.

Download Carbon Copy Cloner

1. Open a web browser and go to *http://bombich.com*.

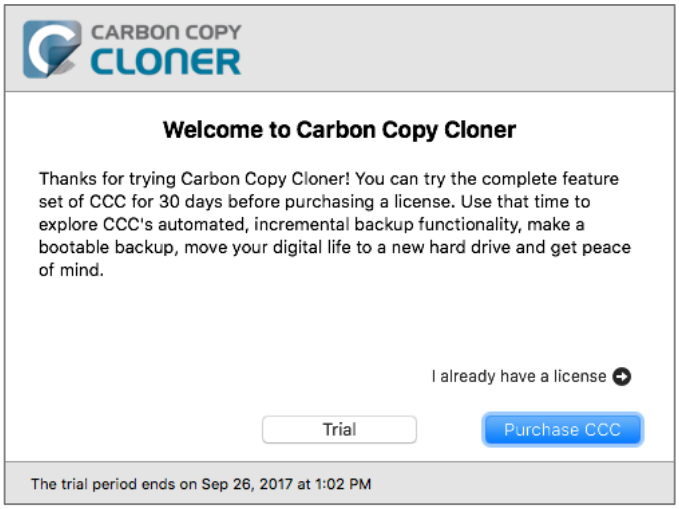


2. Select the *Download 30-Day Trial* button. Carbon Copy Cloner will download. This will be a time-limited full version. Should you wish to purchase CCC, you can do so from within the application.

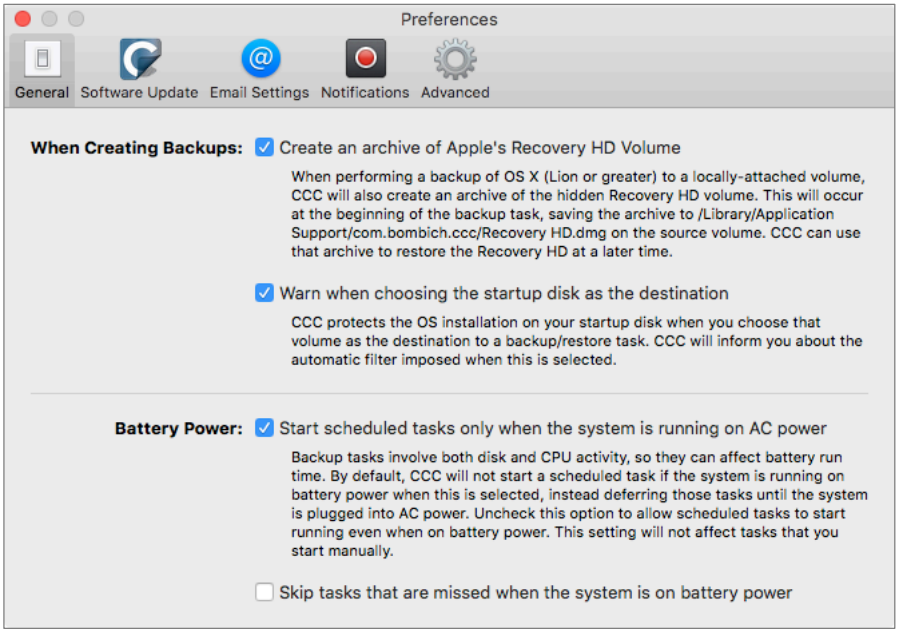
Install Carbon Copy Cloner

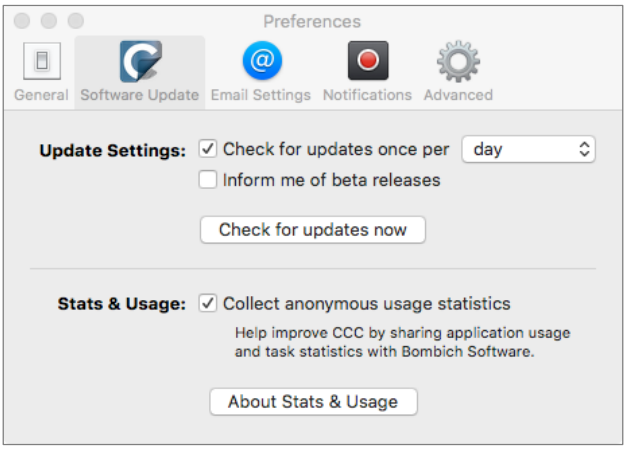
3. Drag Carbon Copy Cloner from the Downloads folder into the Applications folder.
4. Launch Carbon Copy Cloner. If you are logged in with a non-administrator account, enter an administrator *User Name* and *Password* at the

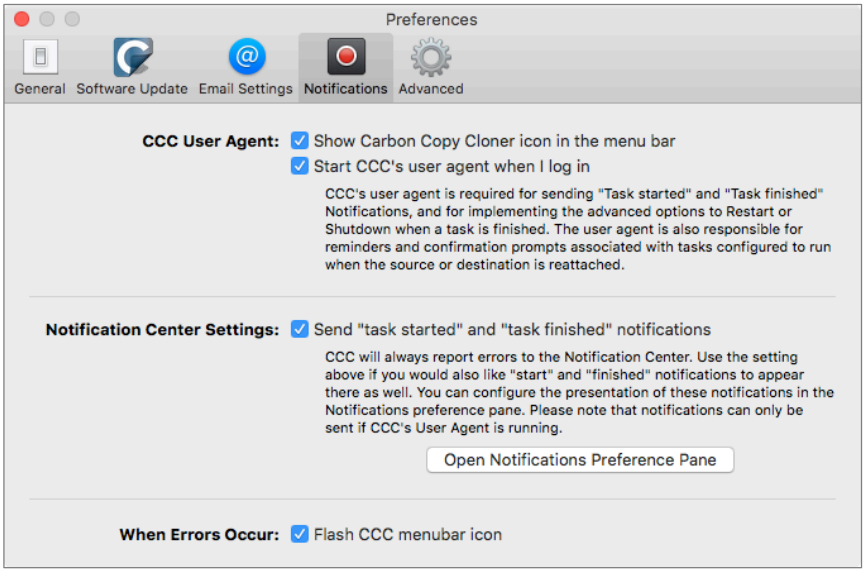
authentication window. At the End User License Agreement window, select *Agree.* At the welcome window, select the *Trial* button.

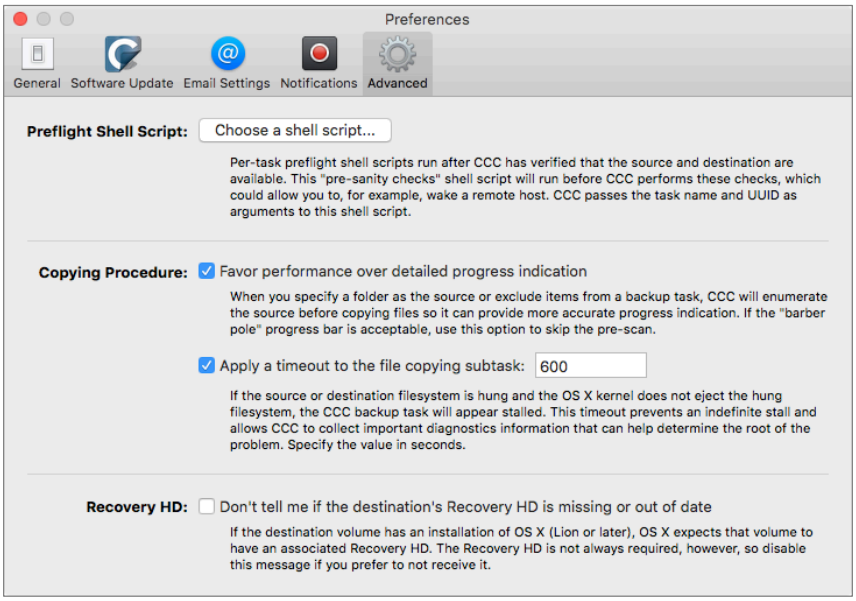


5. The main window opens. It's always a bright idea to configure an application's preferences before having it do heavy lifting. Select the *Carbon Copy Cloner* menu > *Preferences*. Configure each of the preference windows as below.



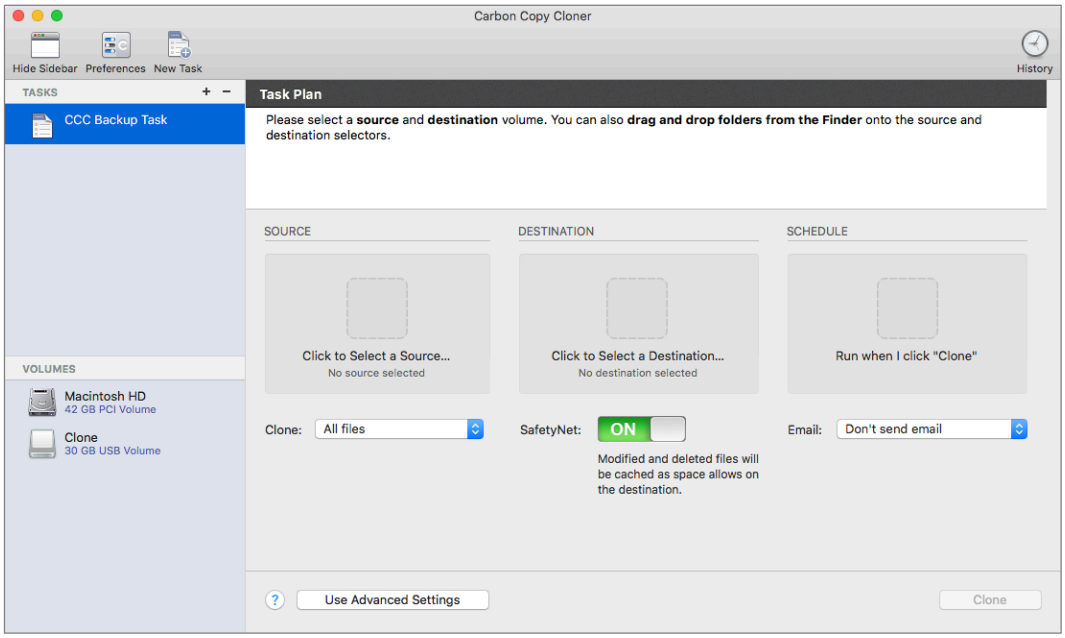

Preferences
General
Software Update
Email Settings
Notifications
Advanced
Update Settings:
Check for updates once per
day
Inform me of beta releases
Check for updates now
Stats & Usage:
Collect anonymous usage statistics
Help improve CCC by sharing application usage and task statistics with Bombich Software.
About Stats & Usage


Preferences
General
Software Update
Email Settings
Notifications
Advanced
CCC User Agent:
Show Carbon Copy Cloner icon in the menu bar
Start CCC's user agent when I log in
CCC's user agent is required for sending "Task started" and "Task finished" Notifications, and for implementing the advanced options to Restart or Shutdown when a task is finished. The user agent is also responsible for reminders and confirmation prompts associated with tasks configured to run when the source or destination is reattached.
Notification Center Settings:
Send "task started" and "task finished" notifications
CCC will always report errors to the Notification Center. Use the setting above if you would also like "start" and "finished" notifications to appear there as well. You can configure the presentation of these notifications in the Notifications preference pane. Please note that notifications can only be sent if CCC's User Agent is running.
Open Notifications Preference Pane
When Errors Occur:
Flash CCC menubar icon



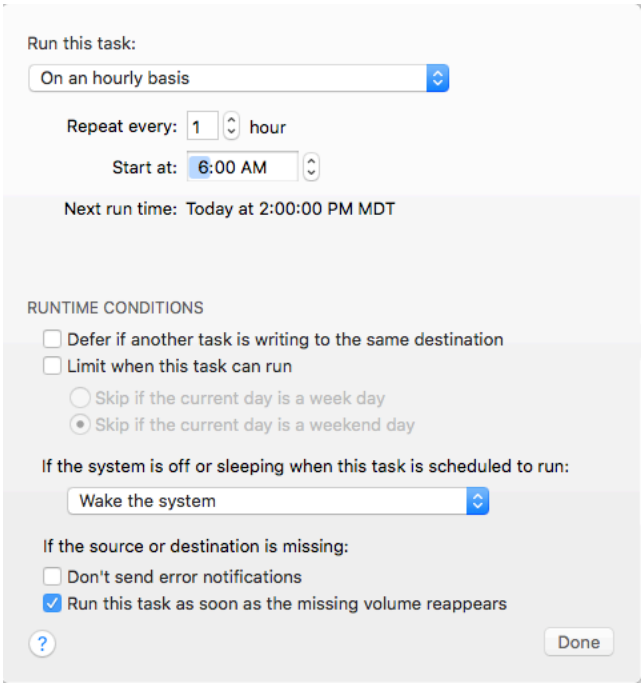
6. Close the *preferences* window.

7. Back at the main window, from the tool bar select the *Show Sidebar* button. The sidebar will slide out.



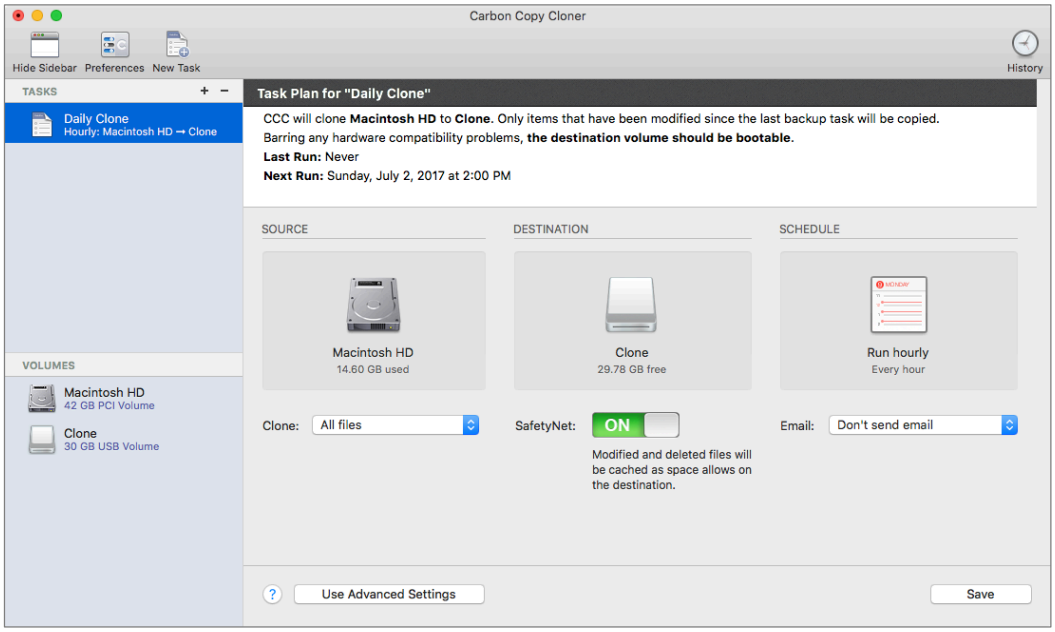
8. From the *Source* area, select the *Click to select a Source* icon, and then select your internal boot hard drive.
9. From the *Destination* area, select the *Click to Select a Destination* icon, and then select the Clone drive.

10. From the *Schedule* area, select the icon, configure as below, and then select the *Done* button.



11. At the main window, in the sidebar, double-click on *CCC Backup Task*, and then rename to *Daily Clone*.

12. Select the *Save* button. Your configuration should look like this:



13. Click the *Save* button.

14. Quit Carbon Copy Cloner.

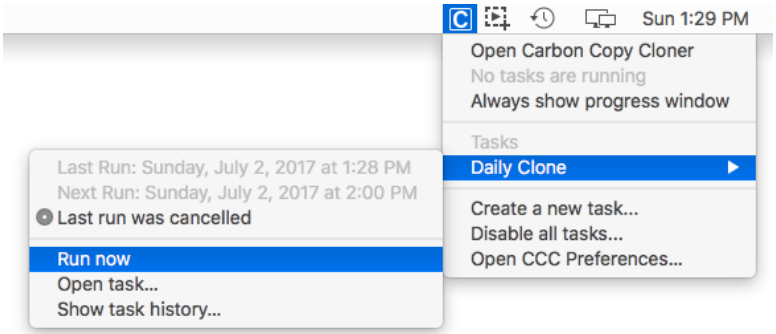
3.1.5 Assignment: Test Run the First Clone Backup

To test your Carbon Copy Cloner script, manually trigger the first backup. It is also necessary to have an initial backup to create a Recovery HD partition onto the drive (required to boot from an encrypted drive), and to then encrypt the drive.

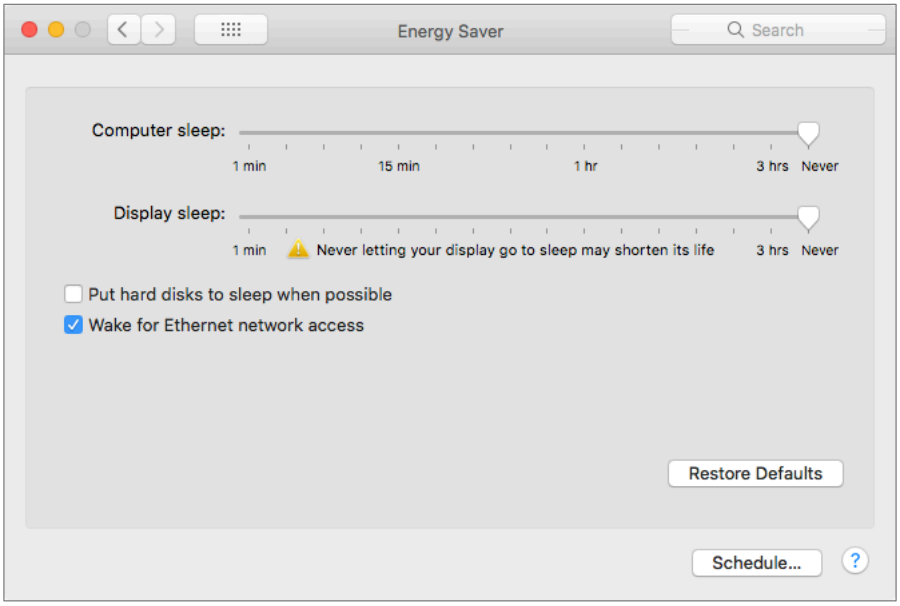
In this assignment, you run the first clone backup.

Run the first clone backup.

1. From the *Carbon Copy Cloner* menu icon, select *Daily Clone* > *Run Now*.

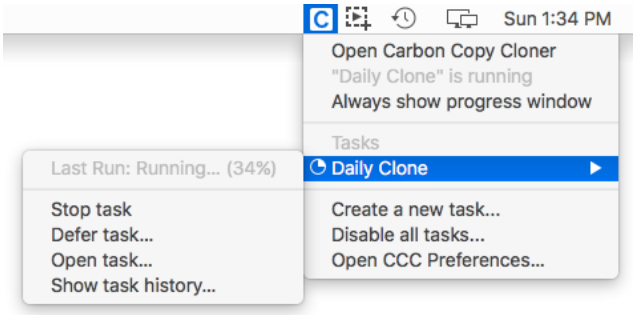


2. Depending on the speed of your computer and the size of the source drive, the first backup may take from 1-12 or more hours. Make certain that your computer will not go into sleep mode during the backup by selecting the *Apple* menu > *System Preferences* > *Energy Saver*. Although it is ok to have your monitor go to sleep, your system must not. Configure your preferences so the computer will not sleep.



3. Close System Preferences.

4. Monitor the progress of the clone by selecting the *Carbon Copy Cloner* menu icon > *Daily Clone* >



Verify Clone is Bootable

5. When the clone completes, go to *Apple* menu > *System Preferences* > *Startup Disk*.
6. Unlock the Startup Disk preference.
7. Select the *Clone* volume, and then click the *Restart…* button.

8. Once at the Desktop, to verify you have booted from the clone, select *Apple* menu > *About This Mac…* If successful, the window will read *Startup Disk Clone.*

9. Close the window.

Boot to Boot Drive

10. To return to the boot drive, select *Apple* menu > *System Preferences* > *Startup Disk.*
11. Unlock the Startup Disk preference.
12. Select the *Macintosh HD* volume, and then click the *Restart…* button.

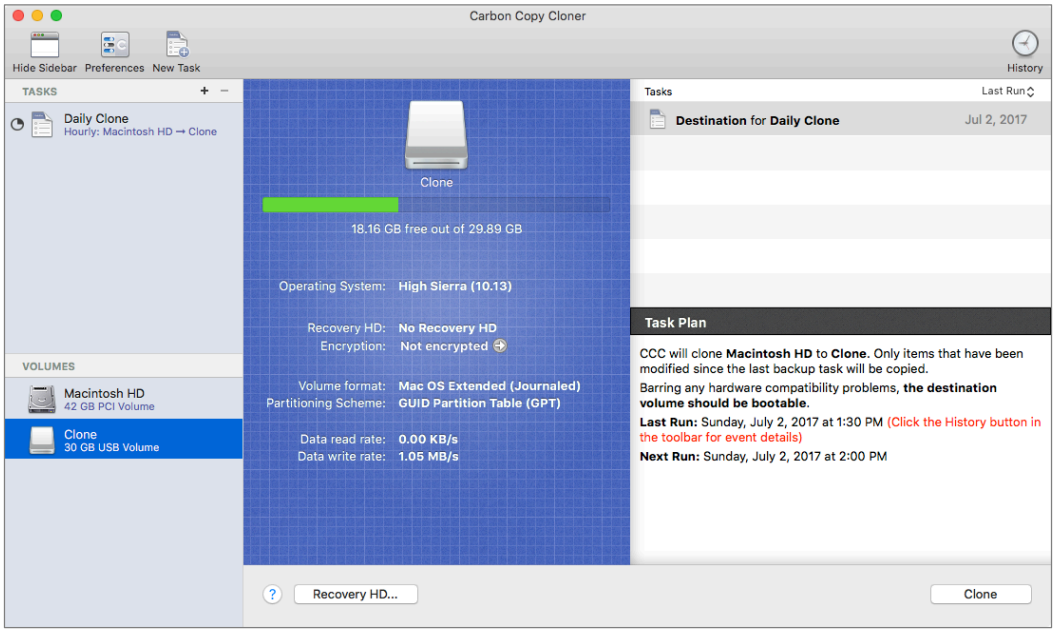
3.1.6 Assignment: Encrypt the Clone Backup.

To have FileVault 2 encryption on a boot volume, it is necessary to add a Recovery HD volume to the drive. The macOS installer performs this task behind the scenes when installing macOS onto a drive. But as you aren't "installing" macOS on the clone, Carbon Copy Clone will do this for you.

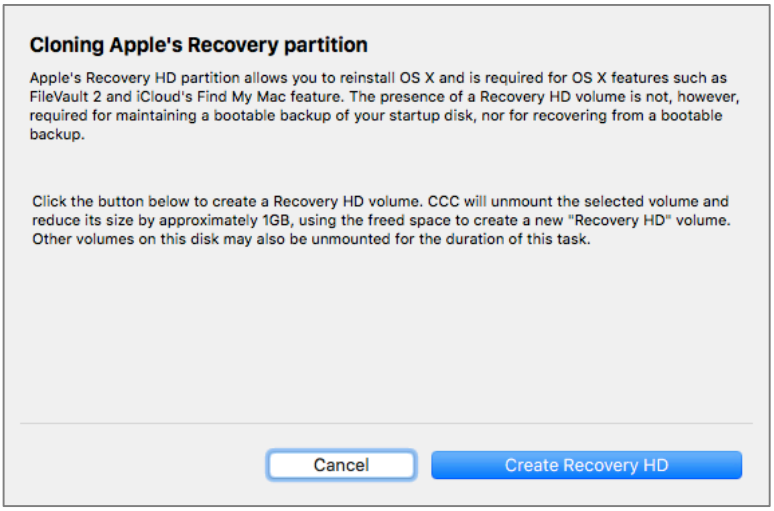
In this assignment, you encrypt the Clone drive.

Add a Recovery HD to the Clone Drive

1. If you are not already logged in with an administrator account, do so now.
2. Open Carbon Copy Cloner.
3. From the side bar, select the Clone volume.
4. Select the Create Recovery HD button.



5. In the *Cloning Apple's Recovery partition* window, select the *Create Recovery HD* button.



6. This process takes only a minute. When complete, return to the main window.

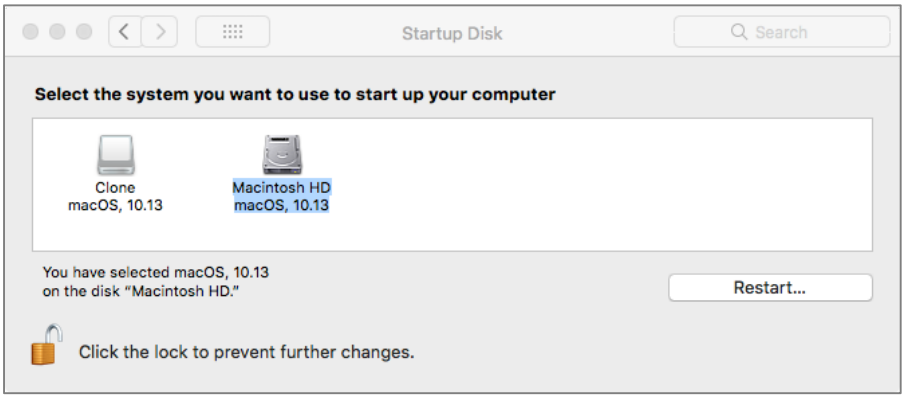
Encrypt the Clone Backup

If an unauthorized person gains access to your clone backup, they will have full access to all your data unless the drive is encrypted.

7. Complete at least one full back up to the clone drive.
8. Restart your computer, booting from the clone drive.
9. Once back at the desktop, start the encryption process for the clone drive by opening *Apple* menu > *System Preferences* > *Security & Privacy* > *FileVault* tab.
10. Click the Lock icon and authenticate as an administrator.
11. Click the *Turn On FileVault* button.
12. Follow the on-screen instructions.
13. Record the *FileVault 2 Recovery Key* in a secure location. I use the Address Book/Contacts application or LastPass. The FileVault 2 Recovery Key is a secondary password used to decrypt and access your boot drive in the event

the user does not remember their account password, or the account password does not work.

14. Click the *Restart* button. FileVault 2 will restart your computer to the clone drive.
15. When back on the desktop, open *Apple* menu > *System Preferences* > *Startup Disk*.
16. Select your normal system/boot drive, which is by default named Macintosh HD.



13. Click the *Restart*… button. The computer will restart, booting from your normal boot drive.

The encryption process for the clone drive will continue. Depending on the size of the drive, the speed of the computer, and if HDD or SSD, it may take from a few hours to a few days to complete the encryption. Although it is ok to let your computer sleep or turn off, this will delay the encryption process.

3.1.7 Assignment: Integrity Test the Clone Backup

The step missed by almost every user is testing the integrity of the backups. This testing process should be performed every month. Not a bad idea to put it on your calendar for the first workday of the month.

Integrity testing requires that your backup has completed at least one full cycle. If you have just completed the previous exercise, allow 24 hours of uptime before

moving on. To test your bootable clone backup, you need to boot from it, and then verify it has been backing up by looking at the history.

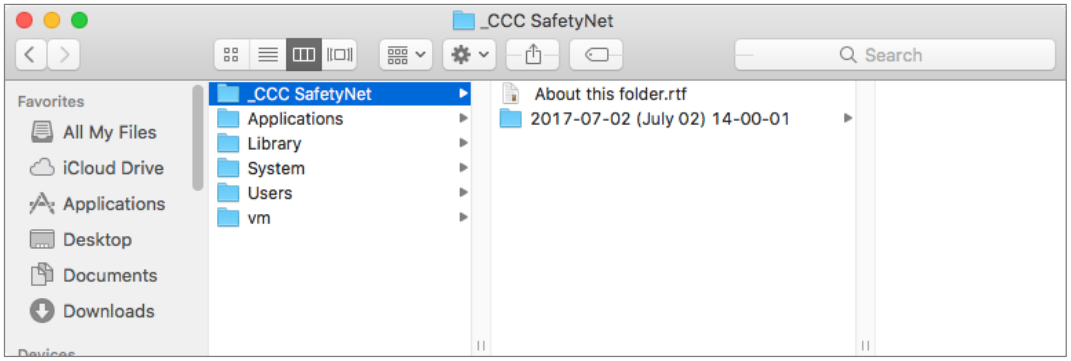
In this assignment, you test the integrity of the clone backup.

1. Select the *Apple* menu > *System Preferences* > *Startup Disk*.
2. Select your clone drive.

3. Click the *Restart* button. Your computer will restart, then boot to the clone drive.
4. Verify that you have booted to the clone drive by selecting the *Apple* menu > *About This Mac*.

5. If the *Startup Disk* field lists the name of your clone drive, you know your clone is bootable and you are half way home.

6. Close the *About This Mac* window.
7. Open the clone drive.
8. Open the *_CCC SafetyNet* folder.
9. A date and time stamp will label each backup. If the most current date and time stamp is what it should be (as opposed to several days or weeks ago), you are good.



10. To restart your Mac into the default boot drive, select the *Apple* menu > *System Preferences* > *Startup Disk*.
11. Select your normal boot drive.
12. Click the *Restart* button. Your computer will restart, and then boot to the normal drive.

Congratulations! You have just verified the integrity of your clone backup.

4 Passwords

For a people who are free, and who mean to remain so, a well-organized and armed militia is their best security.

–Thomas Jefferson[1]

Knowledge, and the willingness to act upon it, is our greatest defense.

–Marc L. Mintz[2]

What You Will Learn In This Chapter

- Create a strong password
- Use the Keychain
- View an existing Keychain record
- Challenge questions
- Store challenge Q&A in Keychain
- Access secure data from Keychain
- Harden the Keychain
- Synchronize Keychain across macOS and iOS devices
- Use LastPass to save website credentials

[1] *https://en.wikipedia.org/wiki/Thomas_Jefferson*
[2] *https://mintzit.com/*

4.1 The Great Awakening

In June 2013, documents of NSA origin were leaked to The Guardian newspaper[3]. The documents provided evidence that the NSA was both legally and illegally spying on United States citizens' cell phone, email, and web usage. These documents, while causing gasps of outrage and shock by the public, revealed little that those of us in the IT field already did not know/suspect for decades: every aspect of our digital lives is subject to eavesdropping.

The more cynical amongst us go even further, stating that *everything* we do on our computers *is* recorded and subject to government scrutiny.

But few of us have anything real to fear from our government. Where the real problems with digital data theft come from are local kids hijacking networks, professional cyber-criminals who have fully automated the process of scanning networks for valuable information, competitors/enemies and malware that finds its way into our systems from criminals, foreign governments, and our own government.

The first step to securing our data is to secure our computers and mobile devices. Remember, we are not in Kansas anymore.

[3] *https://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy*

4.2 Strong Passwords

We all know we need passwords. Right? But do you know that *every* password can be broken? Start by trying *a.* If that does not work, try *b,* and then *c.* Eventually, the correct string of characters will get you into the system. It is only a matter of time.

Way back in your great-great-great grandfather's day, the only way to break into a personal computer was by manually attempting to guess the password. Given that manual attempts could proceed at approximately 1 attempt per second, an 8-character password became the standard. With a typical character set of 24 (a–z) this created a possibility of 24^8 or over 100 billion possible combinations. The thought that anyone could ever break such a password was ridiculous, so your ancestors became complacent.

This is funny when you consider that research has shown that most passwords can be guessed. These passwords include: name of spouse, name of children, name of pets, home address, phone number, Social Security number, and main character names from Star Trek and Star Wars (would I kid you?). Most computer users are unaware that what they thought was an obscure and impossible-to-break password could be cracked in minutes.

It gets worse. A while back the first hacker wrote password-breaking software. Assuming it may have taken 8 CPU cycles to process a single attack event, on an old computer with a blazing 16 KHz CPU that would equate to 2,000 attempts per second. This meant that a password could be broken in less than 2 years. Yikes.

IT directors took notice.

So down came the edict from the IT Director that we *must* create *obscure* passwords: strings that include upper and lower case, numeric, and symbol characters. But in many cases, this was a step backward. Since a computer user could not remember that their password was 8@dC%Z#2, the user often would manually record the password. That urban legend of leaving a password on a sticky note under the keyboard? I have seen it myself more than a hundred times.

Come forward to the present day. A current quad-core Intel i7 with freely available password-cracking software can make over 10 billion password attempts

per second. Create an army of infected computers called a botnet to do your dirty work[4] and you can likely achieve over a hundred trillion attempts per second, unless your system locks out the user after x number of failed log on attempts.

What does this mean for you? The typical password using upper and lower case, number, and symbol now can be cracked with the right tools in under than 2 minutes. If using just a single computer to do the break in, make that a week. Don't believe it? Look at the *haystack*[5] search space calculator.

If we use longer passwords, we can make it too time consuming to break into our system, so the bad guys will move on to someone else.

But you say it is tough enough to remember *8* characters, impossible to remember more?

This is true, but only if we keep doing things as we have always done before. Since virtually all such attacks are now done by automated software, it is only an issue of length of password, not complexity. So, use a passphrase that is easy to remember, such as, "Rocky has brown eyes" (which at 100 trillion attempts per second could take over 1,000,000,000,000,000 centuries to break – provided Rocky is not the name of your beloved pet and thus more guessable).

How long should you make your password, or rather, passphrase? As of this writing, Apple[6], Google[7] and Microsoft[8] recommends a minimum of 8 characters. US-CERT[9] [10] currently recommends at least 15 for administrative accounts, at least 8 for non-administrators. Cisco recommends[11] at least 8. My recommendation to clients is a minimum of 15, in an easy-to-remember, easy-to-enter phrase.

---

[4] *http://en.wikipedia.org/wiki/Botnet*
[5] *https://www.grc.com/haystack.htm*
[6] *https://support.apple.com/en-us/HT201303*
[7] *https://support.google.com/a/answer/33386?hl=en*
[8] *https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf*
[9] *https://security.web.cern.ch/security/recommendations/en/passwords.shtml*
[10] *https://www.us-cert.gov/ncas/alerts/TA11-200A*
[11] *http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec-usr-aaa-15-sy-book/sec-aaa-comm-criteria-pwd.html*

In addition to password length, it is critical to use a variety of passwords. In this way, should a bad entity gain access to your Facebook password, that password cannot be used to access your bank account.

Yes, soon you will have a drawer full of passwords for all your different accounts, email, social networks, financial institutions, etc. How to keep all of them organized and easily accessed amongst all your various computers and devices? More on that later in the *LastPass* section of this *Password* topic.

Apple Password Recommendations

- Maintain an 8-character minimum length
- At least one number
- Include both upper and lowercase letters
- For a stronger password, add additional characters and punctuation marks

Microsoft Password Recommendations

- Maintain an 8-character minimum length
- Eliminate character-composition requirements
- Eliminate mandatory periodic password resets for user accounts
- Ban common passwords, to keep the most vulnerable passwords out of your system
- Educate your users not to re-use their password for non-work-related purposes
- Use multi-factor (2-factor) authentication

US-CERT Password Recommendations

- Private and known only by one person
- Not stored in clear text in any file or program, or on paper
- Easily remembered
- At least 15 characters long for administrators, at least 8 characters long for non-administrators

- A mixture of at least 3 of the following: upper case, lower case, digits, and symbols
- Not listed in a dictionary of any major language
- Not guessable by any program in a reasonable time frame

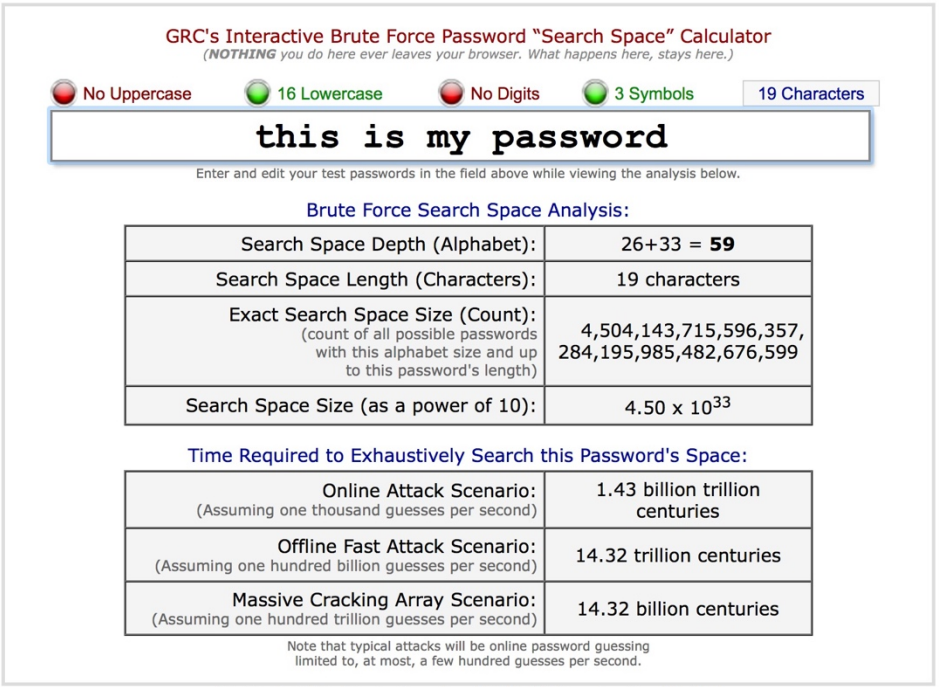
4.2.1 Assignment: Create a Strong User Account Password

As password cracking is now done through automated software, complexity isn't nearly as important as it was when humans were attempting the crack. This is to say that a password of 11111111111111 is about as secure as f^w1&%Ge0*$W18. I recommend using a passphrase–easy to remember, easy to enter, at least 15 characters. For example, *I love brown eyes* is an excellent password.

In this assignment, you create a strong password for your computer account.

1. Think up a password for yourself that is consists of at least 15 easy-to-remember and easy-to-enter characters, and meets the strength/complexity required by your organization.

2. Test how difficult it is to break your password by visiting haystack at *https://www.grc.com/haystack.htm*.



GRC's Interactive Brute Force Password "Search Space" Calculator

(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)

No Uppercase | 16 Lowercase | No Digits | 3 Symbols | 19 Characters

this is my password

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+33 = **59**
Search Space Length (Characters):	19 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	4,504,143,715,596,357, 284,195,985,482,676,599
Search Space Size (as a power of 10):	4.50×10^{33}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	1.43 billion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	14.32 trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	14.32 billion centuries

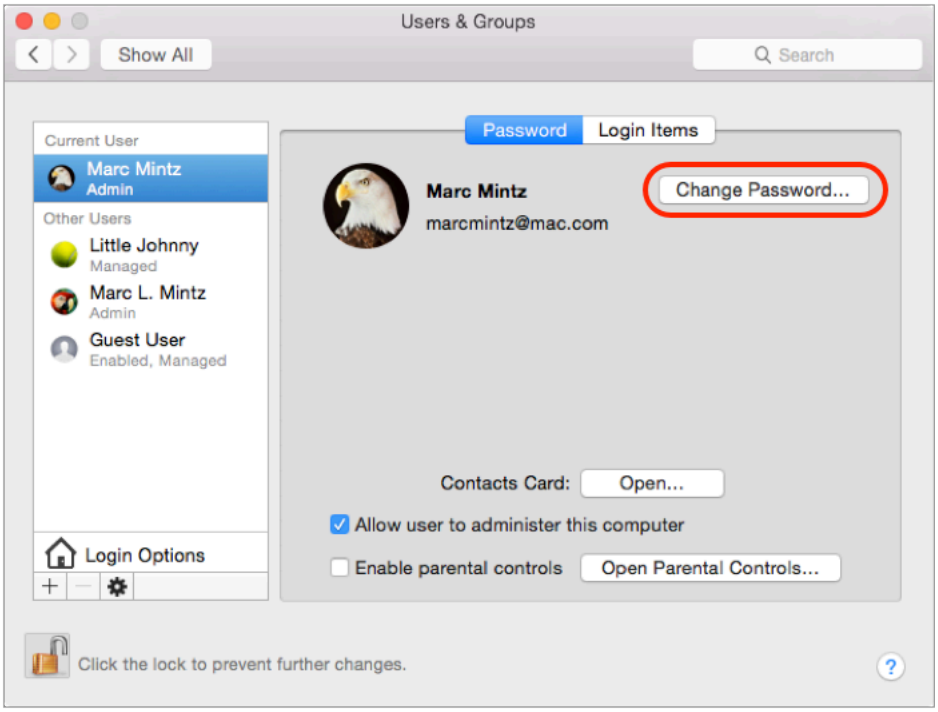
Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

3. Record your new password in a way that is secure, and you can find when you need it. I recommend using LastPass (more on that later in this chapter), or Apple Contacts.
4. Exit the browser.

Change Your Old Password to the Strong Password

5. Log in to your computer using your user account.
6. Click on *Apple* menu > *System Preferences* > *Users and Groups*.

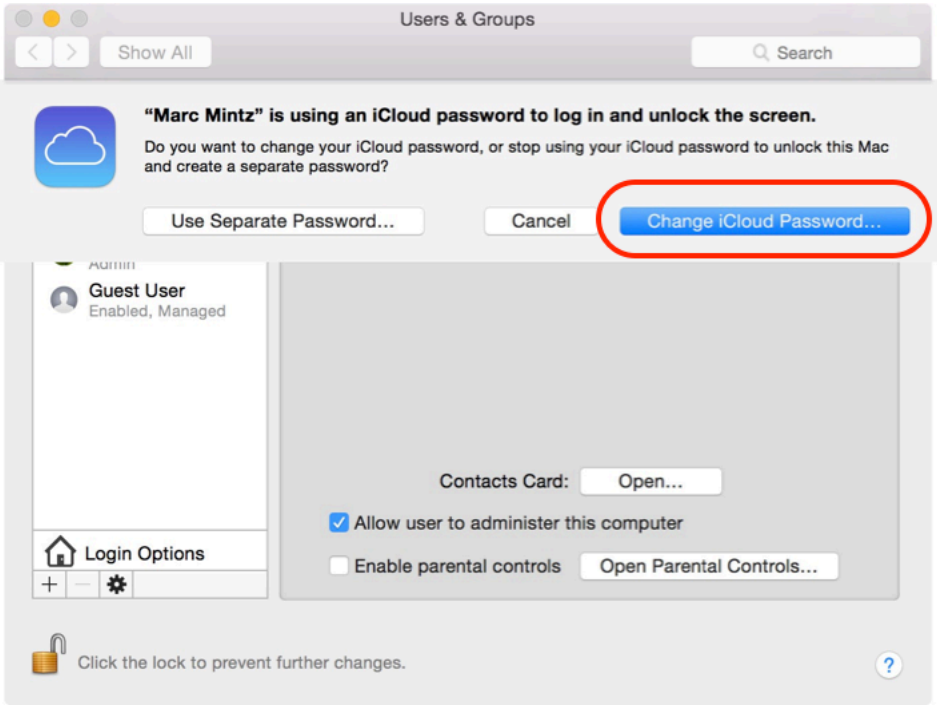
7. Select the Change *Password* button:



- Note: When changing a user/login password, if possible, the change should be made while logged in with that user account. Doing so will simultaneously change the *Keychain* password to match. The Keychain stores usernames and passwords. When changing the user/login password in any other way, the Keychain password remains unchanged. If the user doesn't then know the password to the Keychain, it is impossible to ever open again, and all stored passwords will be lost. More on Keychain later in this chapter.

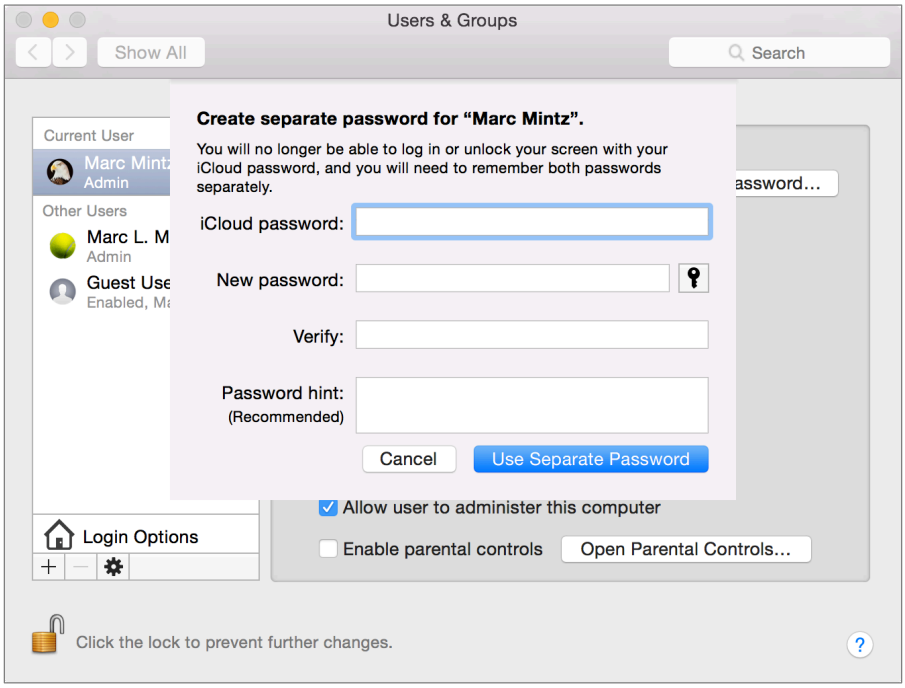
8. By default, your login password is set the same as your iCloud password. You will be asked if you want to *Use Separate Password…*, or to *Change iCloud Password…*

   a. Synchronizing the iCloud and login password makes remembering both easier, and accessing your iCloud data from a new computer easier, but it also presents a roadblock to login should the Apple authentication servers be offline (as has happened at least once).



b. If you select Change iCloud Password, a browser opens to the My Apple ID page at Apple so that you may manage your ID.

c. If you select *Use Separate Password, the Create separate password for "<user name>"* window appears so that you may create a password. At the prompt, enter your *iCloud password, New password, Verify* your new password, and then select the *Use Separate Password* button:



9. Quit System Preferences.

Your new, strong password now is in effect.

4.3 Keychain

In our grandparent's day, life was so much simpler. I'm not talking about politics or sociology, but, well… to give an example: My grandfather had four keys in his pocket at all times: one for home, one for the car, and the other two he could never remember what for.

In today's world, the realm of keys has expanded into the digital world. You now have keys or passwords for logging on to your computer, your phone, your tablet, your email, many of the websites you visit, Wi-Fi access points, servers, your frequent flyer account, etc. In my case, I have 857 passwords in use. I know because they are all neatly stored in a database so that I don't have to remember them.

Unfortunately for most of us, our "keys" are not very well organized, so when we need to access our mail from another computer, or order a book on Amazon, we are stuck.

By default, your Mac stores most usernames and passwords used to access Wi-Fi networks, servers, other computers, and websites. The exceptions are usually websites that are programmed specifically so they do not have credentials saved. These are typically financial institutions.

The built-in tools that store this information automatically can also be used to manually store any text-based data. This includes credit card information, software serial numbers, challenge Q&A, offshore banking information, etc.

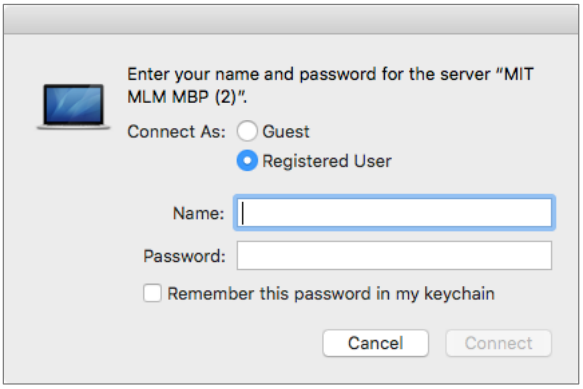
Your Mac has two locations to store keys:

- Safari, which stores only credentials for websites visited with Safari.
- Keychain database, which stores username, password, and URL for websites which request authentication, Wi-Fi networks, servers, other computers you access, email accounts, and encrypted drives.
    - Located at *~/Library/Keychain*
    - Opened with the *Keychain Access* utility

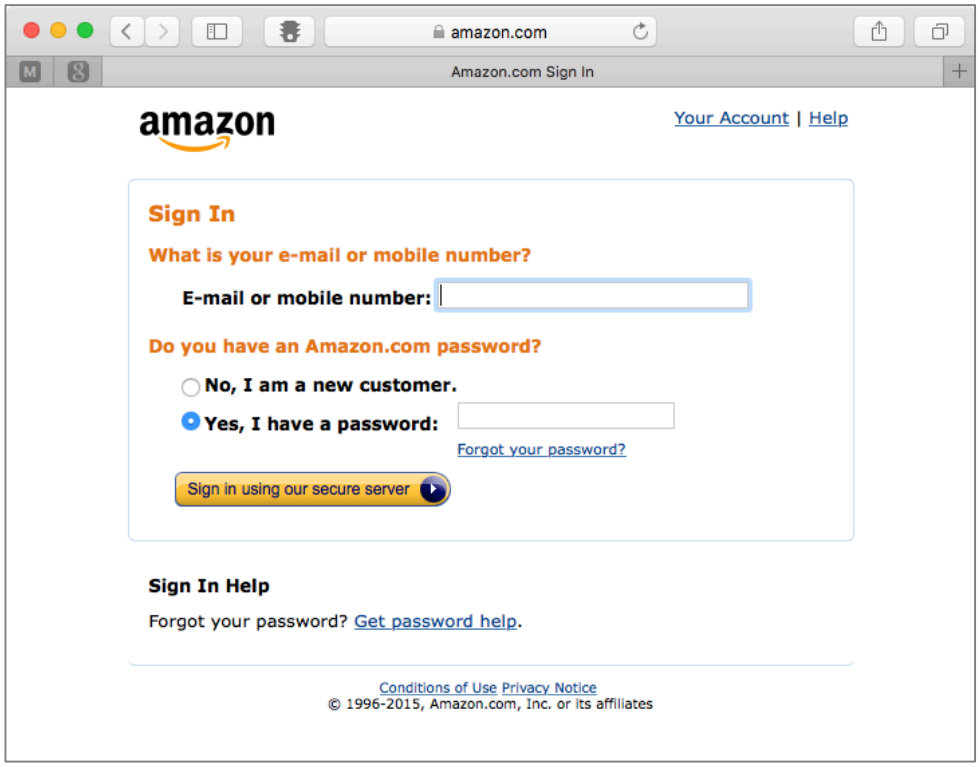
Keychain is what interests us here.

Let's take the case of visiting a website that requires a username and password, connecting to another computer or server, or performing some other action that triggers an authentication request. The following are the steps as they typically occur:

1. A prompt appears requesting a username and password.
    - Typical default authentication window for a server:



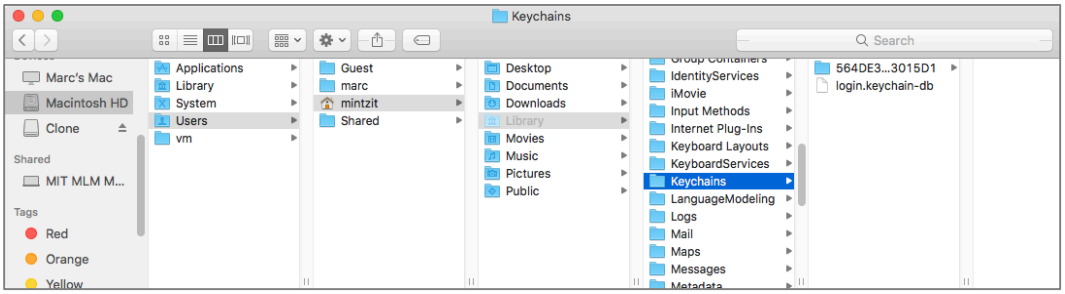
- Typical authentication window for a website:



2. Enter your username and password. In most cases, there is a checkbox to *Remember this password in my Keychain.* Enable that checkbox, and then click Enter or Continue.
3. The website takes you to the appropriate secured page or the other computer mounts a drive on your Mac.

Behind the curtain, your Mac has copied your username and password into the Keychain database, named *Login.Keychain*.

This database is in your Home *Library/Keychains* folder. The database is military grade AES 256 encrypted, safe from prying eyes.



The next time you visit this same website or server, the steps change somewhat:

1. You surf to the website or select a server to access.
2. A prompt appears requesting a username and password.
3. Behind the scenes your web browser or Finder asks: "Has the Keychain stored the credentials for this site or server?"
4. A query is made of the Keychain database based on the URL of the site or the name of the server.
5. If Keychain has stored the username and password associated with the URL or server (it has), the credentials are automatically copied/pasted into the *username* and *password* fields.
6. Select *Enter*.
7. The website takes you to the appropriate secured page or the server share point mounts.

Note that you did not need to know your credentials–Keychain did it all for you.

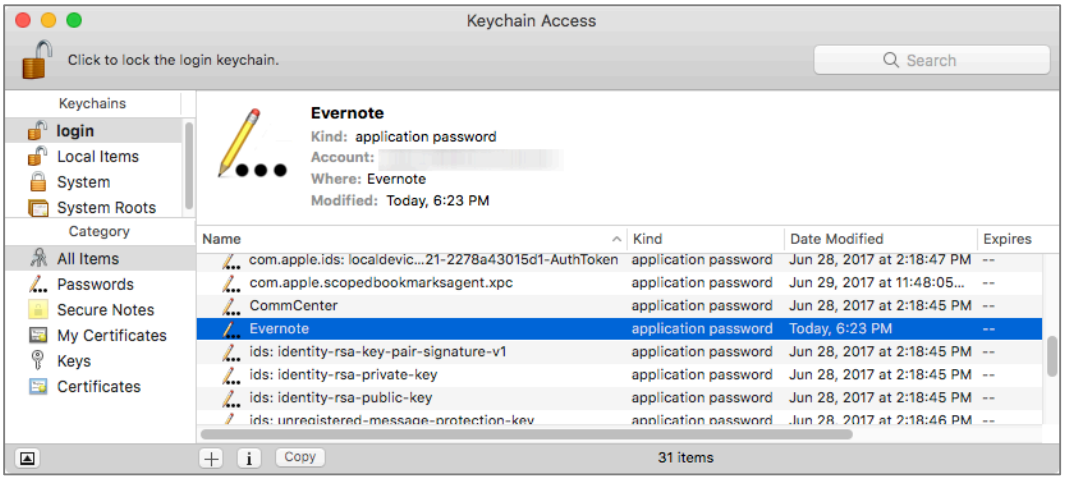
macOS ships with a tool allowing the user full access to the database, named *Keychain Access*, located in the /Applications/Utilities folder.

4.3.1 Assignment: View an Existing Keychain Record

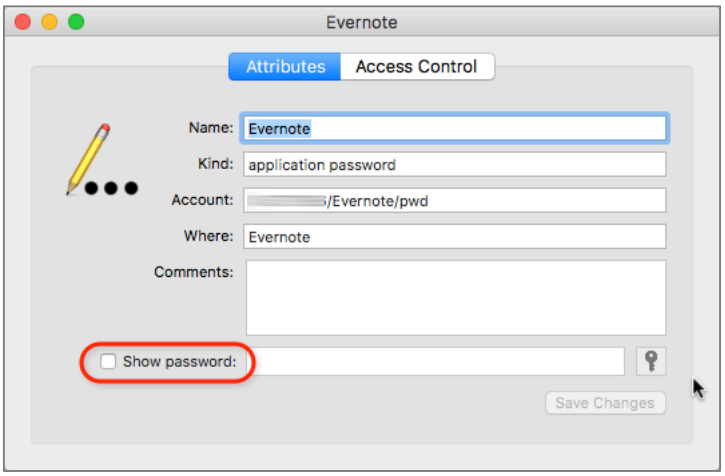
Perhaps a trusted visitor needs access to your Wi-Fi network, and you have forgotten the password to that network. The Keychain database has it stored, you just need to look for it.

In this assignment, you examine a record in the Keychain.

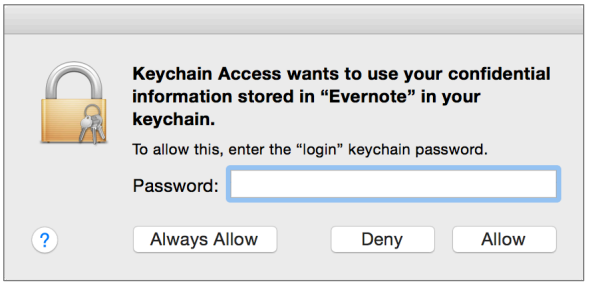
1. Launch *Keychain Access* (located in /Applications/Utilities/).
2. From the sidebar, in the *Keychains* field, select log in. This is the database that holds your secure information.
3. From the sidebar, in the *Category* field, select *All Items*.
4. In the center, main area of the window, double-click on the *target record*, in this example, *Evernote*.



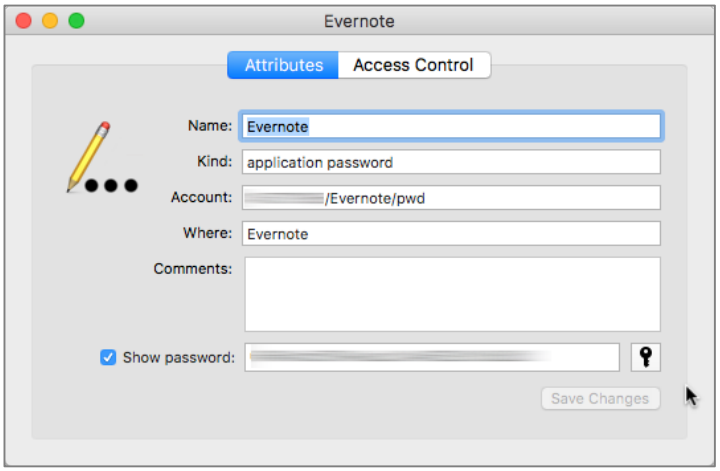
5. The records *Attributes* window will open. At the bottom of the *Attributes* window you will see *Show Password*. Enable the checkbox. This will open the authentication window.



6. At the prompt, enter your Keychain password. By default, this is the same as your user account password. This will authorize Keychain to show you the password. Then click the *Allow* button.



7. The *Show Password* field will now display the needed password.



8. Quit Keychain Access.

4.4 Challenge Questions

A Challenge Question is a way for websites to authenticate who you claim to be when you contact support because of a lost or compromised password.

For example, when registering at a website you may see: *Question – Where did your mother and father meet?*

The problem with this strategy is that most answers easily are discovered with an Internet search of your personal information, or a bit of social engineering.

The solution is to give bogus answers. For example, my answer to the question; *Where did your mother and father meet?* may be; *1954 Plymouth back seat.* It would not be possible for a hacker to discover this answer, as it is completely bogus. My mother tells me it was a 1952 Dodge.

Unless you are some type of savant, there is no way you will remember the answers to your challenge questions. But, there is no need to remember. We already have a built-in utility that is highly secure and designed to hold secrets such as passwords–Keychain Access!

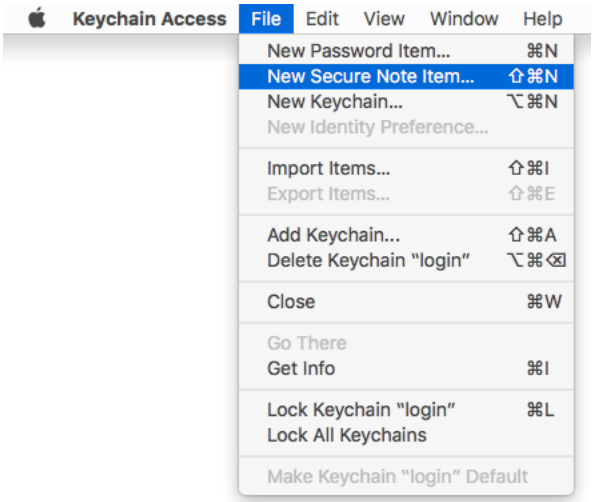
Although Keychain can automatically record and auto fill usernames and passwords, it will require manually entering other data such as challenge Q&A.

4.4.1 Assignment: Store Challenge Q&A in the Keychain

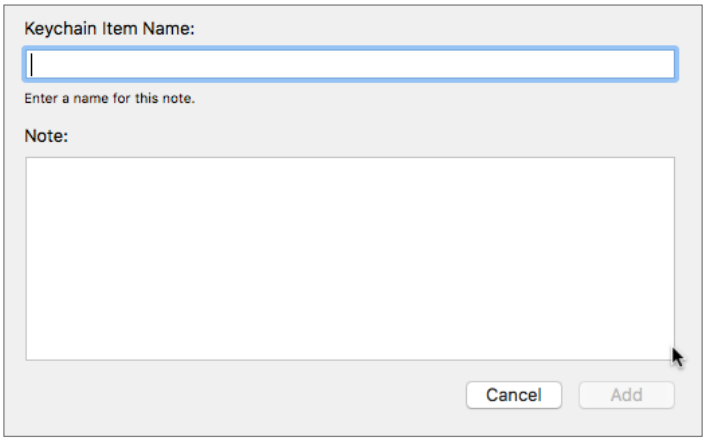
In this assignment, you manually store the challenge Q&A for a pretend website, myteddybear.com.

1. Open *Keychain Access.app*, located in */Applications/Utilities.*

2. Select the Keychain Access *File* menu > *New Secure Note item*…



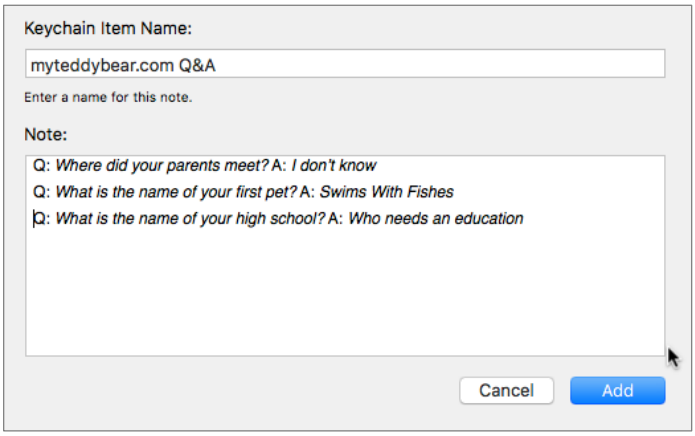
3. The Keychain *Item Name* window appears.



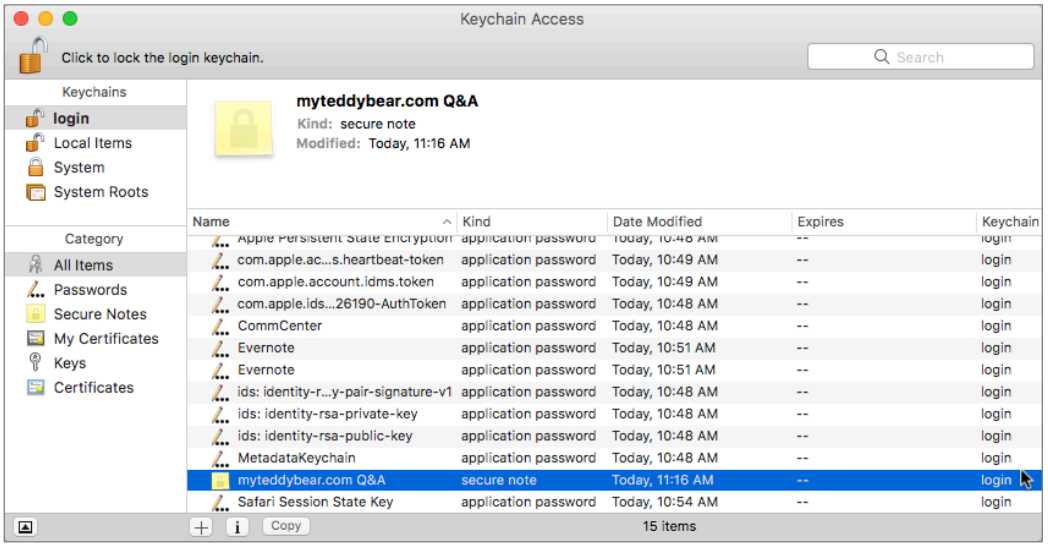
4. In the *Keychain Item Name* field, enter: *myteddybear.com Q&A*.

5. In the *Note* field, enter:
Q: *Where did your parents meet?* A: *I don't know*

Q: *What is the name of your first pet?* A: *Swims With Fishes*
Q: *What is the name of your high school?* A: *Who needs an education*



6. Select the *Add* button.
7. You will find your new Secure Note within all your other Keychain items.



8. Quit Keychain Access.

Your challenge questions and answers are now securely stored.

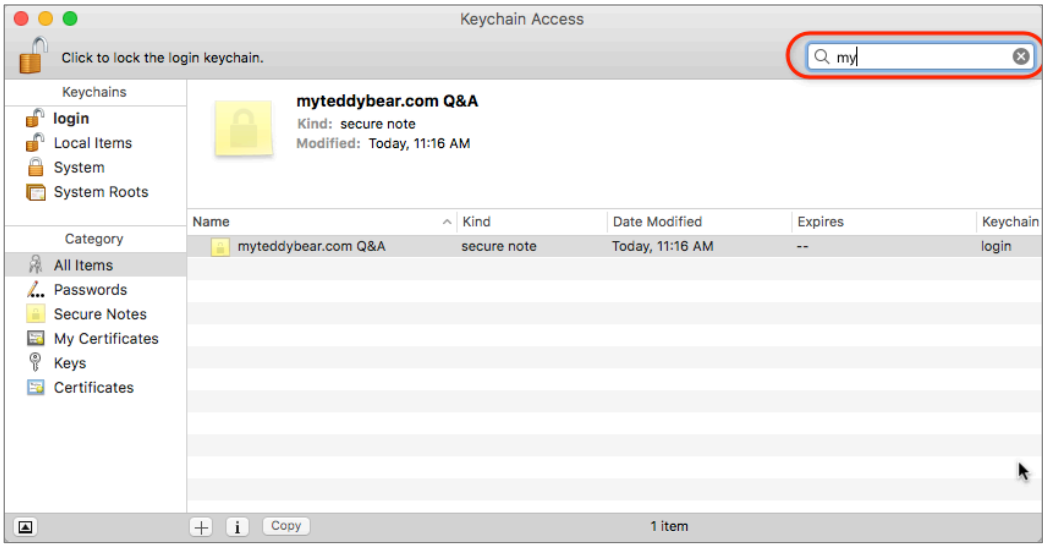
4.4.2 Assignment: Access Secure Data from Keychain

There may come a time that you forget your password to myteddybear.com. A call to technical support with a request to either retrieve or reset your password is met with a challenge question. If you are like me, your synapses holding that memory have long died out.

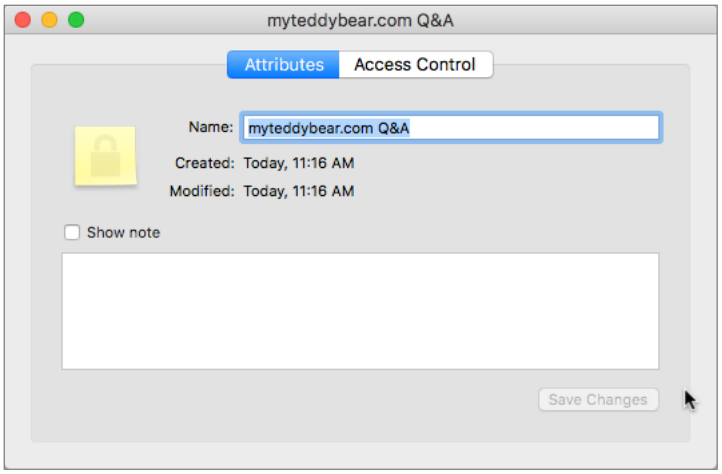
But, no worries! You do remember that you have the habit of storing all your important data securely in your Keychain.

In this assignment, you retrieve your challenge Q&A for myteddybear.com.

1. Open Keychain Access.app, located in */Applications/Utilities*.
2. Click in the *search* field at the top right corner of the *Keychain Access* window.
3. Enter: *myteddybear*. As you type, only those records matching your search string appear, until only the proper record shows.

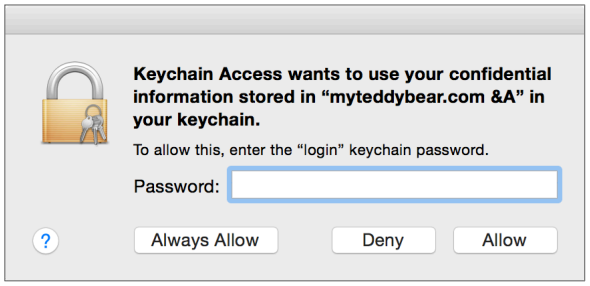


4. Double-click on the myteddybear.com record to open it. Your password is not initially displayed. This is intentional, doubly protecting your data.

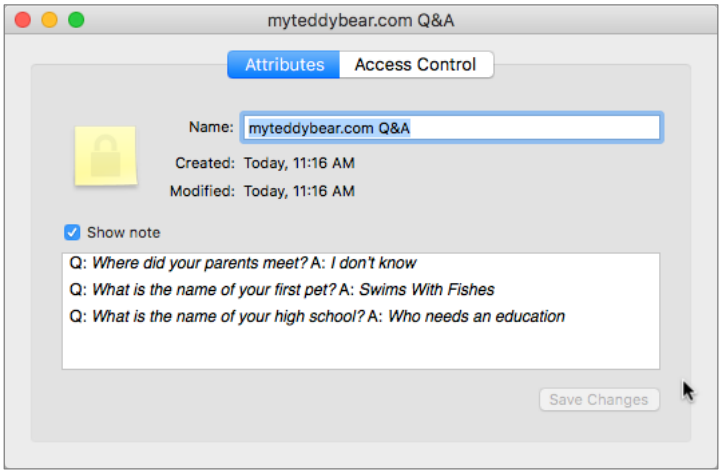


5. Enable the *Show note* checkbox.

6. You are prompted to enter your Keychain password. By default, this is the same as your log in password. Enter your Keychain password, and then click either the *Always Allow*, or *Allow*, button. By selecting *Always Allow*, you will not be asked to verify your Keychain password for this record in the future. If you select *Allow*, you have access to your data, but you will be prompted for your Keychain password in the future.



7. After selecting either *Always Allow* or *Allow,* you see your challenge Q&A.



8. Close the window and Quit *Keychain Access.*

4.5 Harden the Keychain

The work we have done so far in Keychain Access is all that is necessary for almost every environment. Some situations call for even greater levels of security– think military bases, the computer used by the CEO, and my aunt Rose who needs to protect her secret recipe for kosher raisin noodle Koogle.

There are two options to further protect the Keychain, which may be used separately or in tandem:

- Change your Keychain password to be different than your log in password
- Have your Keychain automatically log off after X minutes of inactivity.

By default, your Keychain password matches your login password. With this configuration, in the process of logging in to your computer the Keychain is automatically unlocked. If you give your Keychain a different password, it will remain locked after log in. Where you see this is when you attempt to access a website or connect with another computer and you have the authentication credentials stored in Keychain. Instead of auto filling as usual, you are prompted to enter the password for the Keychain. This unlocks the Keychain, allowing it to continue the auto fill process.

By default, the Keychain remains unlocked if the user remains logged in. There is also the option to set the Keychain to automatically lock after a specified amount of inactivity time.

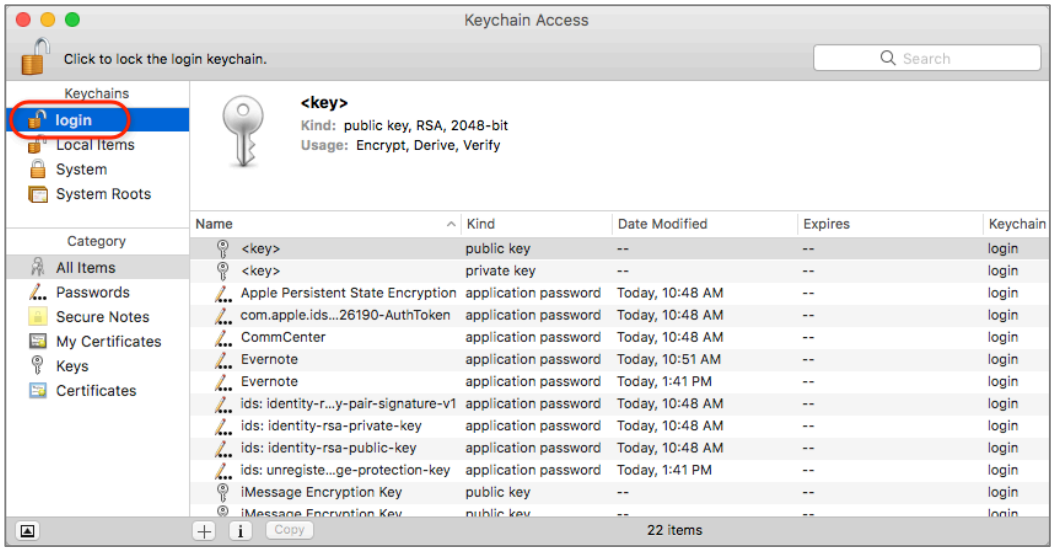
Let's say Keychain Access to automatically lock the Keychain after 5 minutes of inactivity. Upon log in, if the Keychain password is the same as the log in password, the Keychain will unlock and remain unlocked for 5 minutes. If you need an auto fill from data held in Keychain after that 5 minutes, you are prompted for the Keychain password. If within 5 minutes another auto fill is needed, the data is pulled from Keychain automatically. But when 5 minutes or more has passed, the Keychain will lock automatically.

4.5.1 Assignment: Harden the Keychain with a Different Password

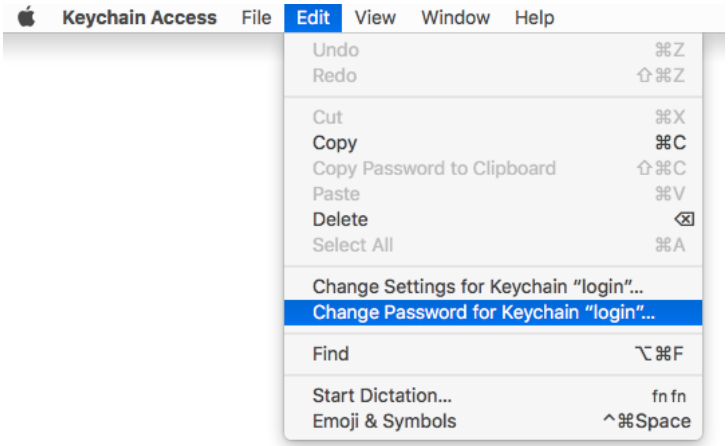
By default, the Keychain password is the same as the user login password. Under this condition, the Keychain automatically unlocks when the user logs in. An additional layer of security may be gained by giving Keychain a different password. If this is done, the Keychain remains locked at login. When called upon to provide a password, it prompts the user for the Keychain password so that it may unlock.

In this assignment, you give your Keychain a password different than your user account login password.

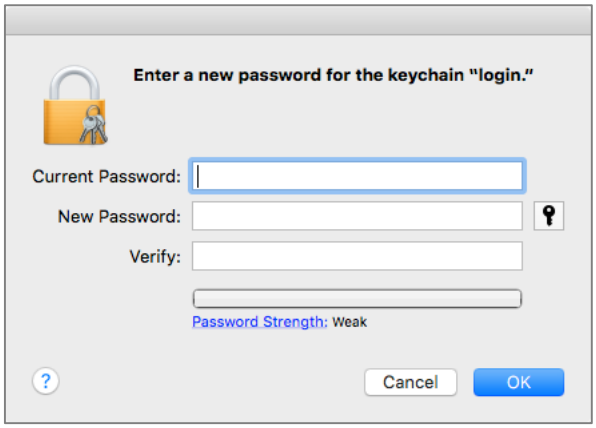
1. Open Keychain Access.app, located in */Applications/Utilities*. From the top of the sidebar, select the *login* keychain.



2. Select the Keychain *Edit* menu > *Change Password for Keychain "login"*.



3. This opens the Enter a new password for the *Keychain "login"* window. Enter the following:



- In the *Current Password* field, enter your current Keychain password. By default, this is your user account log in password.
- In the *New Password* and *Verify* fields, enter your new strong password for Keychain. Write it down so it is not forgotten. I keep this in my Address Book / Contacts application.

4. Select the *OK* button.

5. Select the Lock icon in the top left corner of the Keychain Access window. This locks the log in Keychain.
6. Quit Keychain Access.

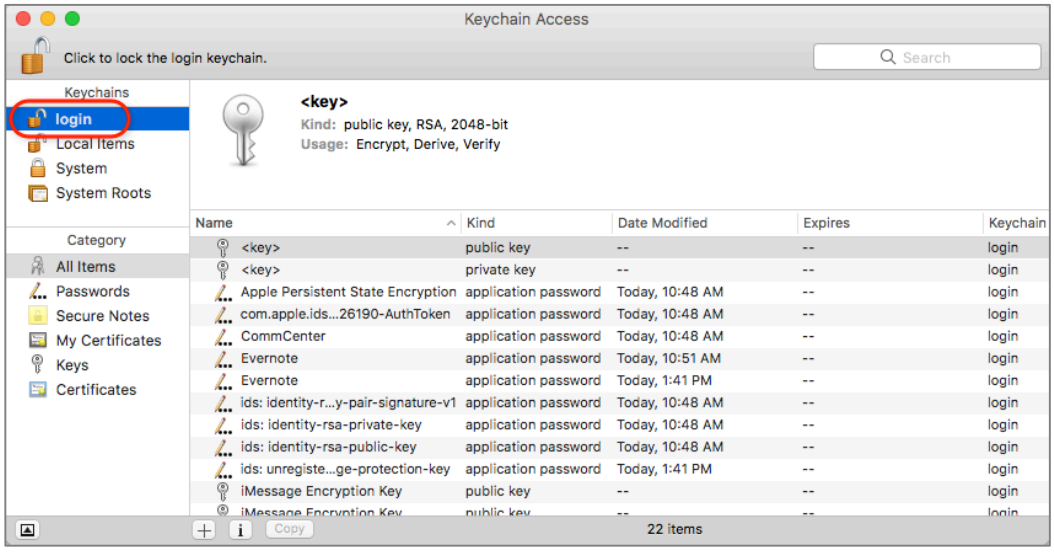
Because your login Keychain now has a different password than your user account password, it will not automatically unlock when you log in to your computer. Attempting to access the Keychain through *Keychain Access* requires that you manually unlock it. Also, the first time that an autofill is attempted, you are prompted to enter the Keychain password.

7. If you do not wish to have a hardened Keychain, repeat steps 1–9, changing the password back to your user account password.

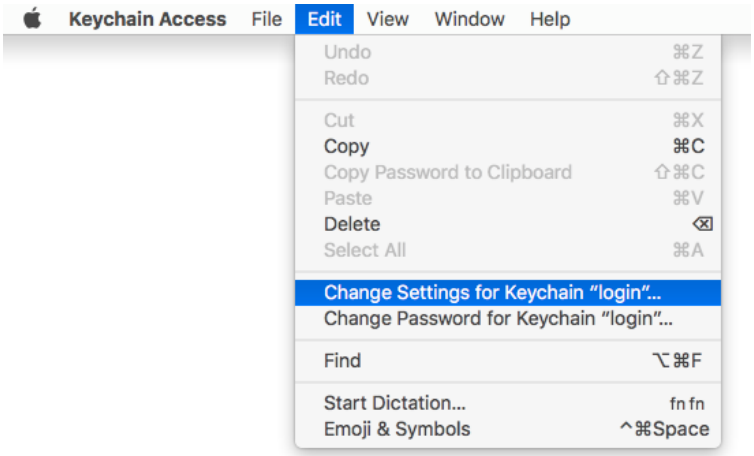
4.5.2 Assignment: Harden the Keychain With a Timed Lock

In this assignment, you give your Keychain a timeout to automatically lock after it has not been used for 1 minute.

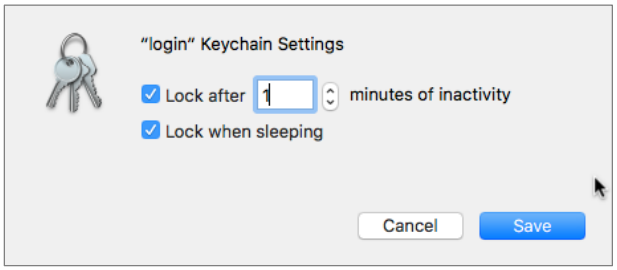
1. Open Keychain Access, located in */Applications/Utilities*. From the top of the sidebar, select the *login* keychain.



2. Select the Keychain Access *Edit* menu > *Change Settings for Keychain "login."*



3. The *Login Keychain Settings* window will open. Configure as follows:



   - Enable the *Lock after ___ minutes of inactivity* checkbox, and then set this to 1 minute.
   - Enable the *Lock when sleeping* checkbox.
4. Select the *Save* button.
5. Quit Keychain Access.
6. Sit on your thumbs for 60 seconds–time enough for the Keychain to lock.
7. Open a browser and visit a website or connect to another computer on your network that you frequent with a password that otherwise auto fills. You find you now are prompted to enter the password for the Keychain it to open.

8. If you do not need a hardened Keychain, repeat steps 1–3, and then when the *Login Keychain Settings* window appears, disable the checkboxes. Then select the *Save* button.
9. Quit Keychain Access.

Your Keychain will now automatically lock, preventing anyone from accessing all your passwords should you step away from your desk with your system awake and no screen saver in place.

4.6 Synchronize Keychain Across macOS and iOS Devices

Perhaps like me, you have a need to access most of these passwords and challenge answers anywhere, anytime. When I have my computer with me, no worries. But what if I don't? It would be a rare event indeed for me to be without my computer or my iPhone, so I keep my Keychain on my iPhone as well.

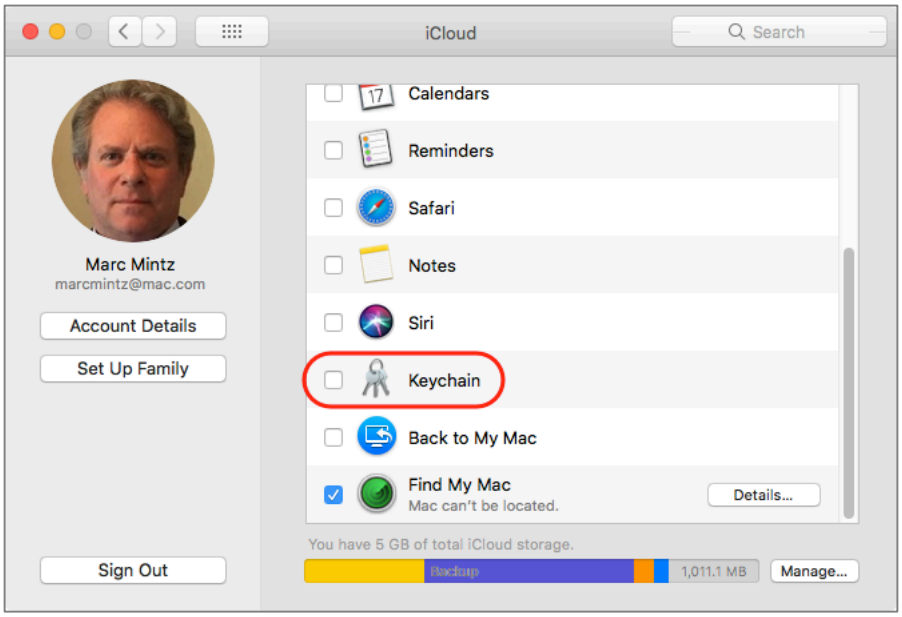
If you have upgraded to macOS 10.12 or higher, OS X 10.9 or higher, and iOS 7 or higher, Apple has you handled. With the most recent incarnations of both operating systems, Apple has added *Keychain* to the iCloud synchronization scheme. This allows your Keychain database to be synchronized between all your computers, iPhones, and iPads.

4.6.1 Assignment: Activate iCloud Keychain Synchronization

Synchronizing your Keychain with iCloud allows all your macOS 10.12 and higher, OS X 10.9 and higher, and iOS 7 and higher devices share your keychain.

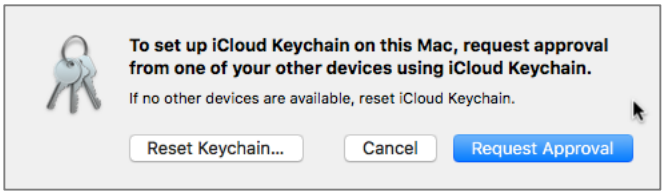
In this assignment, you enable iCloud Keychain synchronization.

1. Open the *Apple* menu > *System Preferences* > *iCloud*.

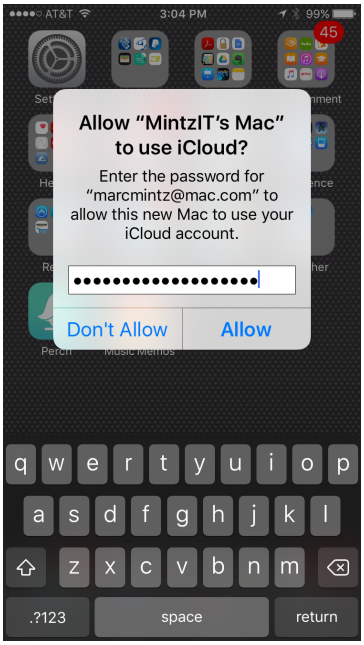


2. Select the *Keychain* checkbox. The *Enter your Apple ID password to setup iCloud Keychain* dialog box appears.
3. Enter your Apple ID password, and then select the *OK* button.

4. If you have previously created a 2-step verification for your Apple ID, the *Keychain Setup* dialog box opens. Select the *Request Approval* button.



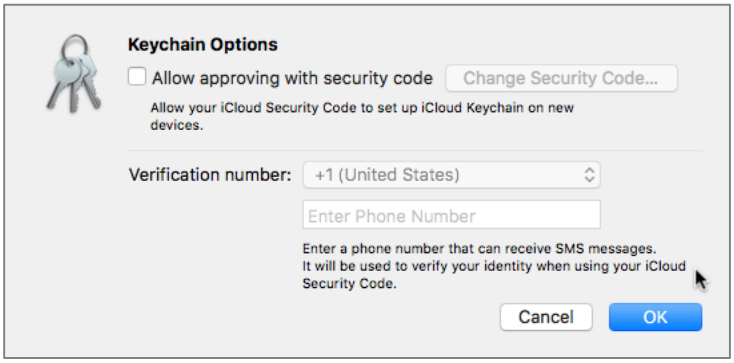
5. A request will be sent to the other devices currently approved on your account to approve this device. Enter your Apple ID password, and then click *Allow*.



6. Go back to *System Preferences,* and notice that the *Keychain* is now enabled.

Further secure your keychain:

7. In the *iCloud Preferences*, select the Keychain *Options* button.
8. The *Keychain Options* window opens:



9. Enable the *Allow approving with security code* checkbox.

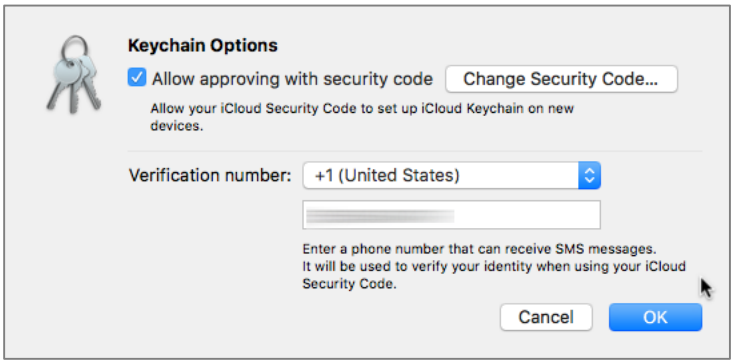
10. The *Create an iCloud Security Code* window opens. Enter a 6-character code that can be used to enable your other Apple devices to share and synchronize Keychains, and then select the *Next* button.

    - Notes: If you would like a more complex code, you can select the *Advanced…* button instead.

11. The same security window appears again to verify your security code. Reenter the code, and then select the *Next* button.

12. The *Enter a phone number that can receive SMS messages* window opens. This will be used by Apple to verify your identity when using the security code. Enter your phone number, and then select the *Done* button.

13. You are returned to the *Keychain Options* window. Select the *Done* button.



14. At the *Enter your Apple ID password to update your account settings* window, enter your Apple ID password, and then select the *OK* button.

15. *Quit* System Preferences.

Your Keychain on this computer will now synchronize automatically with your iCloud account, and therefore with all other OS X, macOS, and iOS devices synchronizing on the same account.

4.7 LastPass

A great solution to the problem of password management is *LastPass*[12].

There are three important advantages of LastPass:

- You no longer must concern yourself with Internet passwords–the correct response becomes automatic. LastPass will keep your Internet passwords available in each of your browsers.
- Stores and share your passwords with all your devices–even across operating systems. It also securely stores manually entered data such as challenge questions.
- The for-fee version allows sharing of selected passwords with others in the group.

LastPass provides the following solutions:

- Provides free (ad supported) and premium (no ads) options
- Automatically remembers your Internet passwords, fully encrypted
- Auto fills web-based forms and authentication fields
- Stores notes and challenge questions and answers (Q&A), fully encrypted
- Synchronizes across multiple browsers
- Synchronizes across multiple computers
- Synchronizes across Android, BlackBerry, iOS, Linux, macOS, Windows
- Automatically generates very strong passwords, which since you do not need to remember them, provide even greater online security.

4.7.1 Assignment: Install LastPass

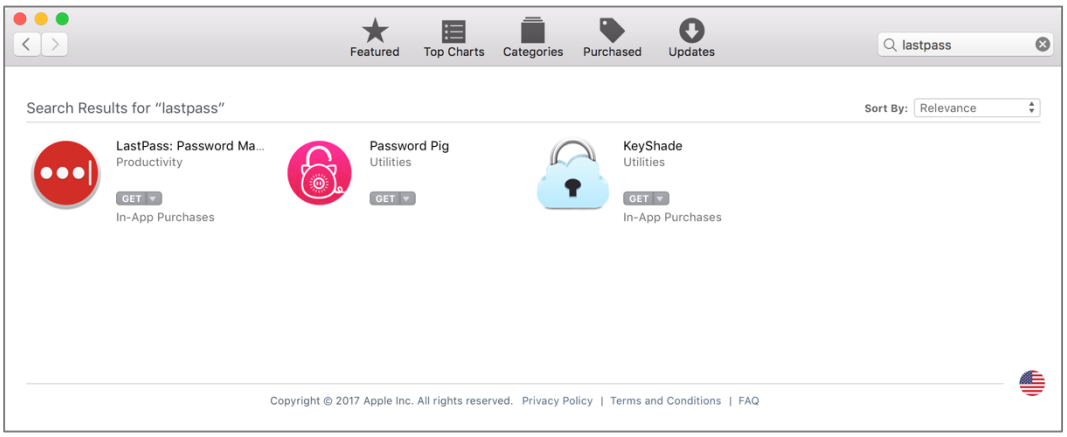
The free version of LastPass works indefinitely across devices.

[12] *http://www.LastPass.com*

In this assignment, you download and install LastPass on your macOS computer.

Download the LastPass Installer

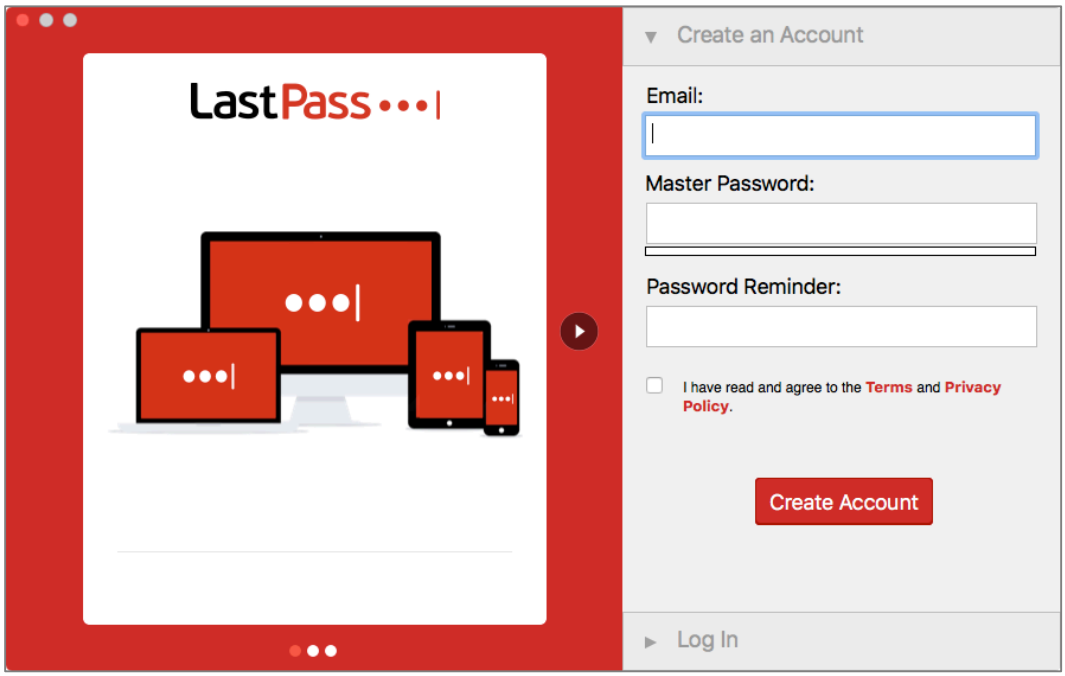
1. Open the *App Store.*
2. In the *Search Field,* enter *LastPass,* and then tap the *Return/Enter* key.
3. In the *LastPass* area, select *Get.* LastPass will download.



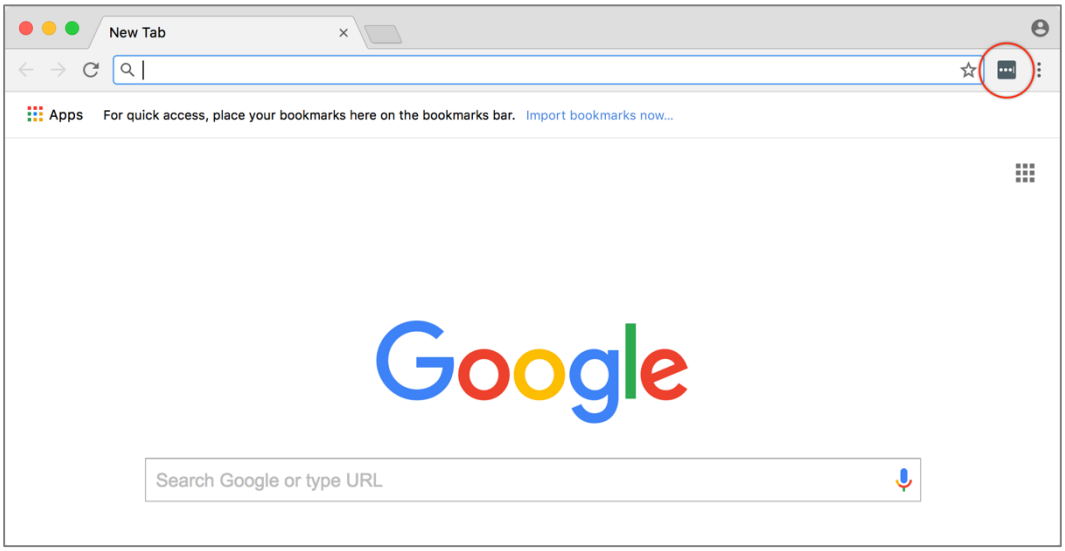
Install LastPass

4. Once LastPass has downloaded, double-click to launch it.

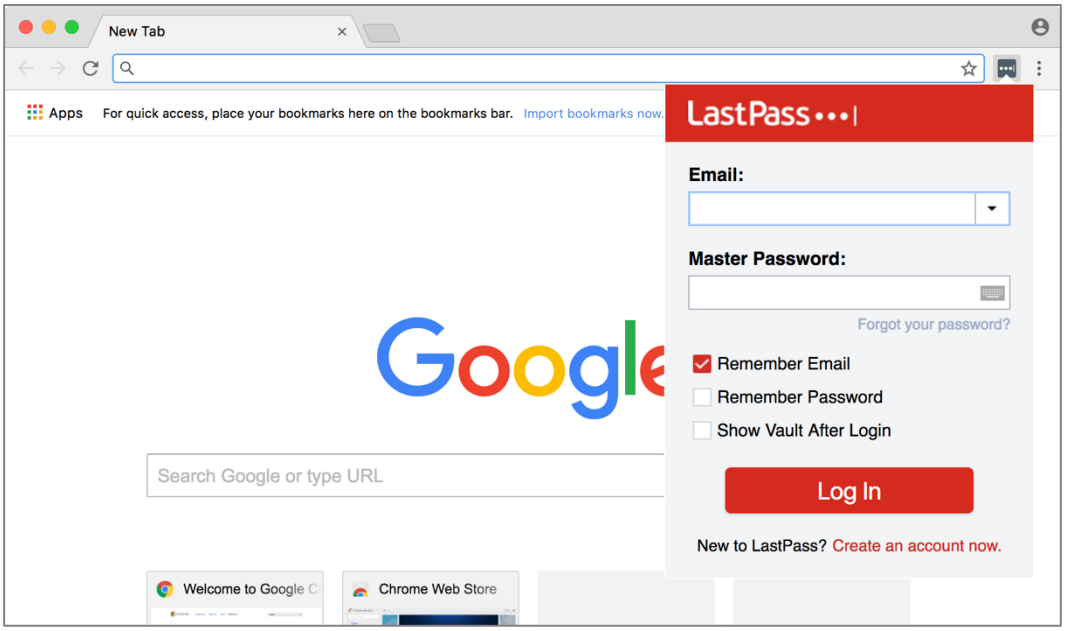
5. Select *Create an Account,* and then enter your *Email* address, a password in the *Master Password* field, a *Password Reminder*, and then click *Create Account*.



6. LastPass automatically installs its extension into Chrome, Edge, Internet Explorer, Firefox, Opera, and Safari. Open a browser. In this example, it is Chrome. The LastPass extension displays as three dots …



7. In your browser, click the LastPass extension icon. The LastPass window opens.



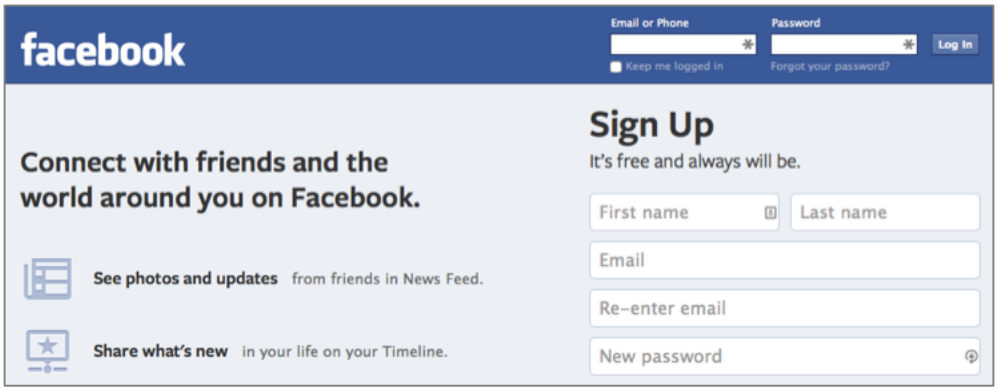
8. Enter the *email* address to be linked to LastPass, and then the *Master Password* you created in an earlier step, and then click *Log In.*
9. The LastPass window goes away, and LastPass is now active within your browser.
10. If you use multiple browsers, repeat steps 6-9 with each.

4.7.2 Assignment: Use LastPass to Save Website Authentication Credentials

Once you have LastPass installed, it's time to put it to use.

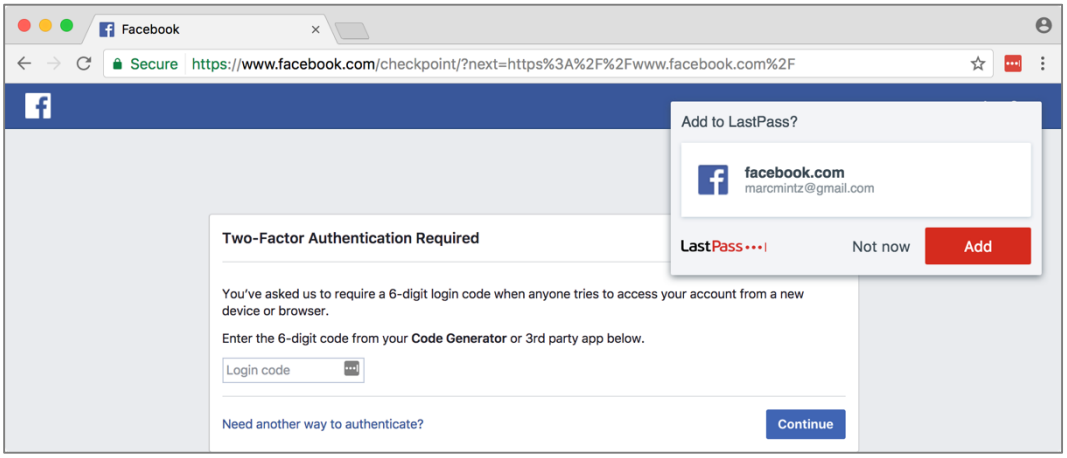
In this assignment, you use LastPass to store the user name and password for Facebook.

1. Use your browser to visit Facebook *https://facebook.com*.



2. As this is the first time you have visited Facebook since installing LastPass, your log in credentials have not yet been stored in LastPass. Enter your Email or Phone and Password information, and then select the *Log in* button.

3. LastPass will detect that there is a form on this page, and present an option to remember your credentials. This will appear just under the navigation bar. Select the *Add* button.



4. Quit your web browser.

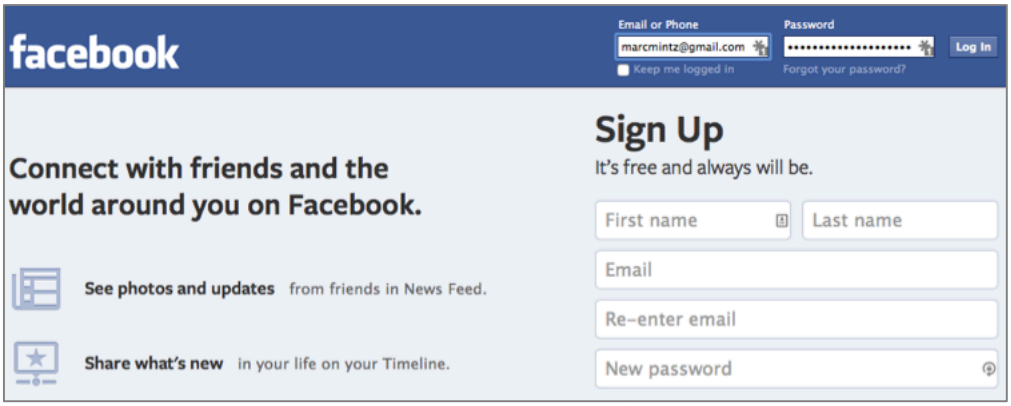
Your Facebook account credentials are now stored in LastPass, so you do not need to remember them.

4.7.3 Assignment: Use LastPass to Auto Fill Website Authentication

When LastPass has saved user name and password information for a site, you will never need to manually enter that information again.

In this assignment, you revisit Facebook and allow LastPass to enter your credentials.

1. Launch your browser and then go to *Facebook* at *https://facebook.com.* Take note that your authentication credentials have been automatically entered for you by LastPass.



2. Quit your browser.

You have just successfully proved that LastPass is saving your credentials.

5 System and Application Updates

Every new beginning comes from some other beginning's end.

–Seneca[1], Roman philosopher, statesman, and dramatist

What You Will Learn In This Chapter

- Configure Apple system and application update schedule
- Manage application updates with MacUpdate Desktop

[1] *https://en.wikipedia.org/wiki/Seneca_the_Elder*

5.1 System Updates

Most computer and mobile device users simply fail to update their systems. Many say the reason is updates slow down the device, or they are concerned about introducing instability to their systems.

Updates rarely significantly change performance, although upgrades often do–a larger code base, requiring more RAM and CPU–will slow down a system. And while it is occasionally true that updates introduce instability–it is far more likely that not updating will create greater instability.

More important is that many updates are about patching vulnerabilities and security holes in the system. Fixing these security issues is so important that US-CERT (Homeland Security division responsible for cyber terrorism and IT security) strongly recommends that all users update all computers and mobile devices "as soon as possible[234].

There are fundamentally three reasons for updates and upgrades:

- **Bug fixes**. All software and hardware have bugs. We simply never will be rid of them. Developers do want to squash as many as possible so that you are so happy with their product and will continue to pay for upgrades.
- **Monetization**. Updates to operating systems and applications almost always are free, or included in the price of the original purchase. Upgrades typically are for fee. But developers will include significant new features in an upgrade to encourage the market to purchase, so the developers can afford to stay in business.
- **Security patches**. Although rarely talked about, one of the most important reasons for an update is to patch newly discovered security holes. Without the update, your computer may be highly vulnerable to attack.

---

[2] *https://www.us-cert.gov/ncas/tips/ST04-006*

[3] *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf* (Appendix D–Bibliography)

[4] *https://www.cisecurity.org/critical-controls/documents/TheASD35andCISControls.pdf*

It is for this last reason alone that I implore clients to be consistent with the update process.

To protect your computer from security holes in the operating system, it is critical to check for updates daily. Fortunately, we can automate this process.

5.1.1 Assignment: Configure Apple System and Application Update Schedule

In this assignment, you automate the process of updating the macOS operating system, as well as Apple software.

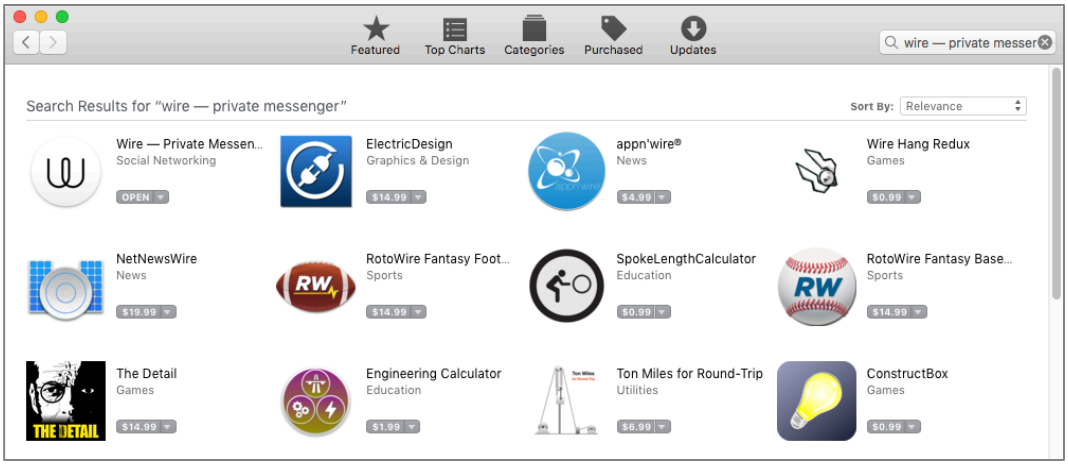
1. Open *Apple* menu > *System Preferences* > *App Store*. Configure as shown below:

- Enable *Automatically check for updates.* That is why we are here!
- Enable *Download newly available updates in the background.* With this option active, the updates are downloaded without you knowing it. An alert will appear telling you updates are ready to be installed. Installation will start immediately upon you clicking *OK* or *Install.*
- Enable *Install system data files and security updates.* I cannot imagine why you would not want to have the most current macOS anti-malware installed.
- Enable *Automatically download apps purchased on other Macs.* If you own multiple macOS or OS X machines, and have the same Apple ID in use for the Mac App Store on each, this will automatically install applications on this Mac even if they were purchased on one of the others.

2. Close System Preferences.
3. When new system or Apple software updates are available, the *App Store Dock* icon will display a red dot with the number of updates available.

4. Select the *App Store* icon to launch the App Store Application. Select the *Updates* button in the navigation bar to display the available updates.

Depending on your Internet connection speed, this may take several minutes to display.



5. Select the *Update All* button to download and install all available updates.
6. Quit the App Store application.

Your macOS system and Apple Store applications will now automatically alert you when updates are available.

5.2 Manage Application Updates With MacUpdate Desktop

macOS, Apple applications, and apps downloaded from the Apple App Store can be updated through the App Store app. Although some other applications have built-in automatic updating, it is still not the norm. Also, system preferences, plug-ins, and other software do not typically automatically update.

Recently, Adobe Flash and Oracle Java have been used by criminal elements to gain control over computers to access user data. Apple has taken the offensive by blocking older susceptible versions from running on macOS and OS X 10.7 and higher. There are many other software points that have been, can, and will be exploited. It is critical to keep all your software up-to-date so that security holes can be secured.

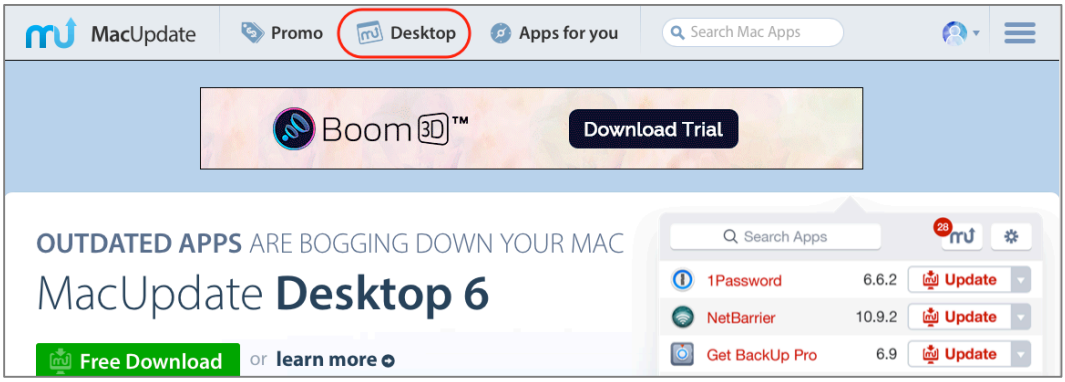
As the typical user has over 100 applications, plug-ins, extensions, etc., by far the fastest, easiest, and most cost-effective way to do this is to automate the process using MacUpdate Desktop[5] (approximately $40/year).

5.2.1 Assignment: Install and Configure MacUpdate Desktop

In this assignment, you download, install, and configure MacUpdate Desktop with a 7-day free trial.

[5] *http://www.macupdate.com/desktop*

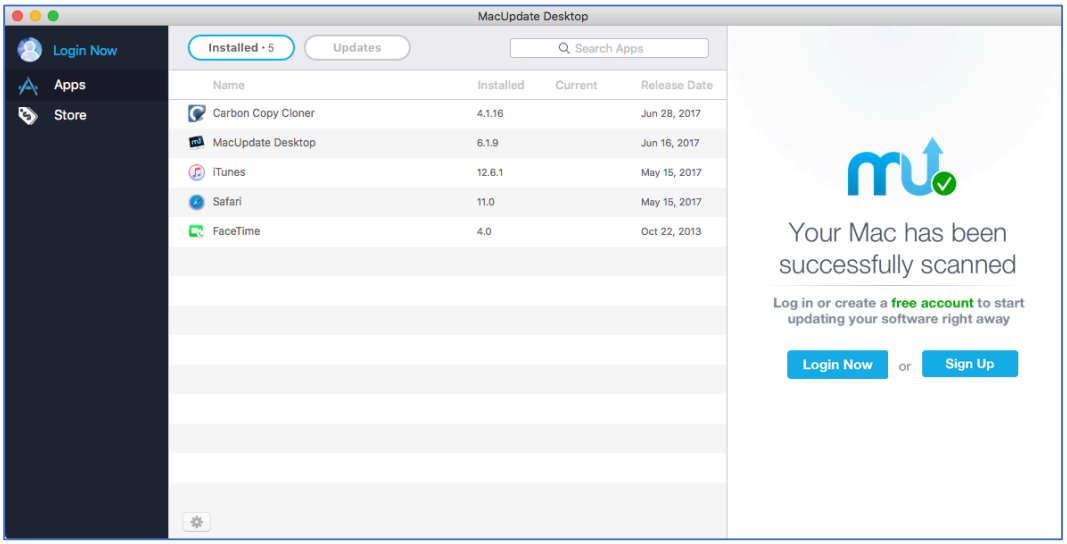
1. Open a browser to surf to the *MacUpdate* home page at *https://macupdate.com*. Select the *Desktop* button at the top of the page.



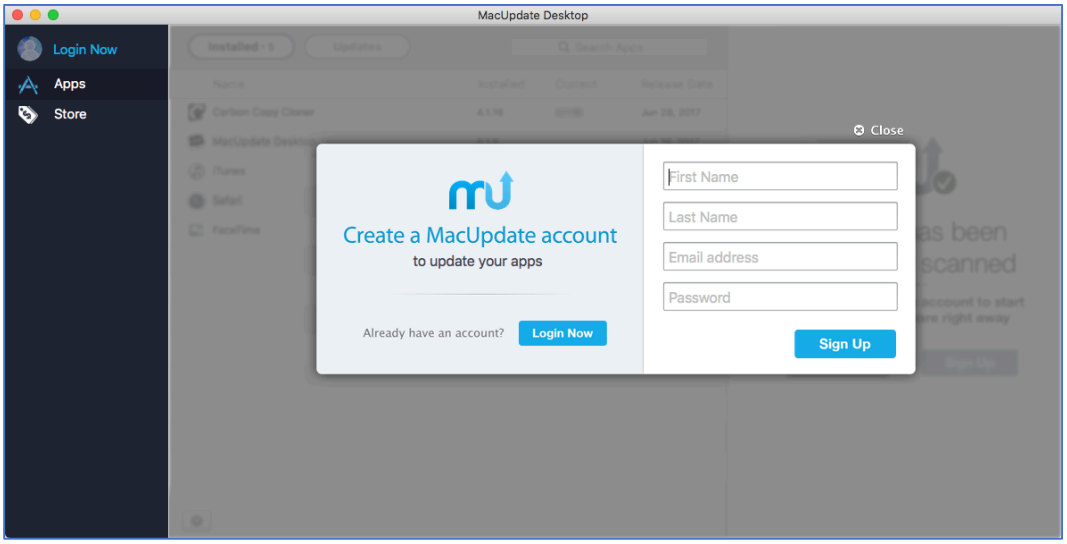
2. The *MacUpdate Desktop 6* page opens. Click the *Free Download* button. The MacUpdate Desktop app downloads to your computer.

3. Move MacUpdate Desktop from the Downloads folder, to the Applications folder.
4. Launch MacUpdate Desktop. The home window opens.

5. Click the *Sign Up* button.



6. The *Create a MacUpdate account* window opens. Complete the required fields:



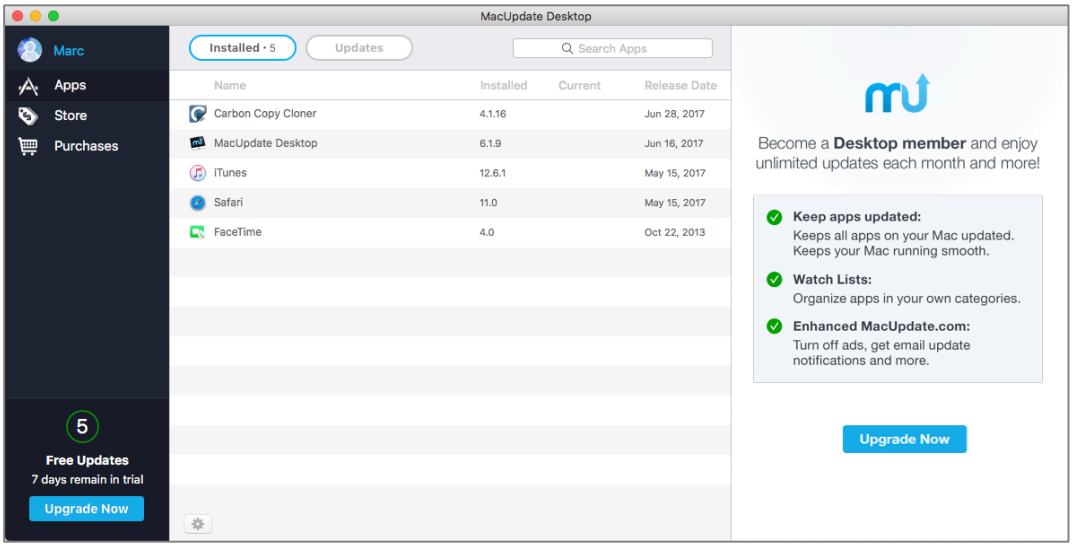
a. Enter your First name.

b. Enter your Last name.

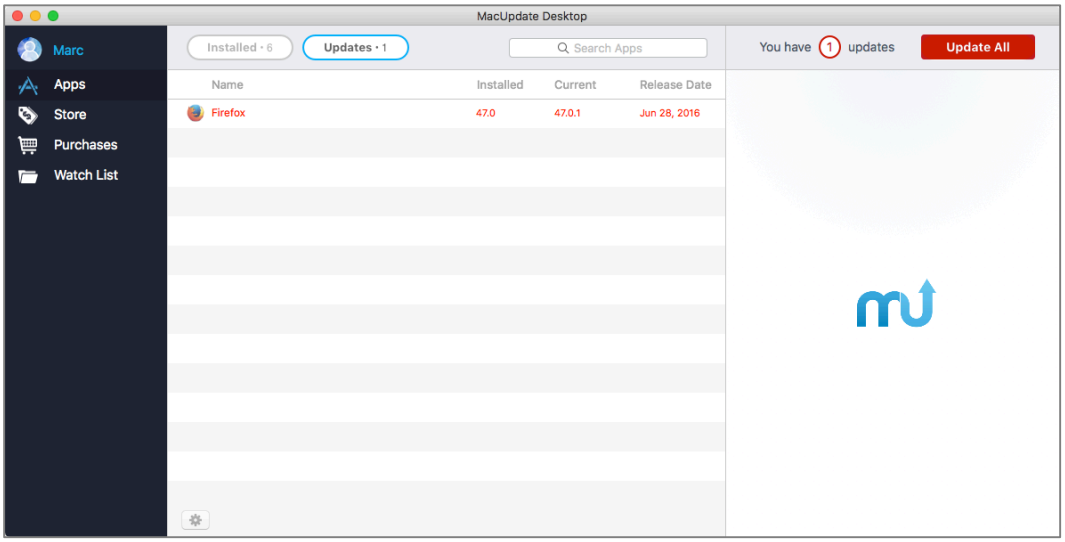
c. Enter your Email address.

d. Create a Password.

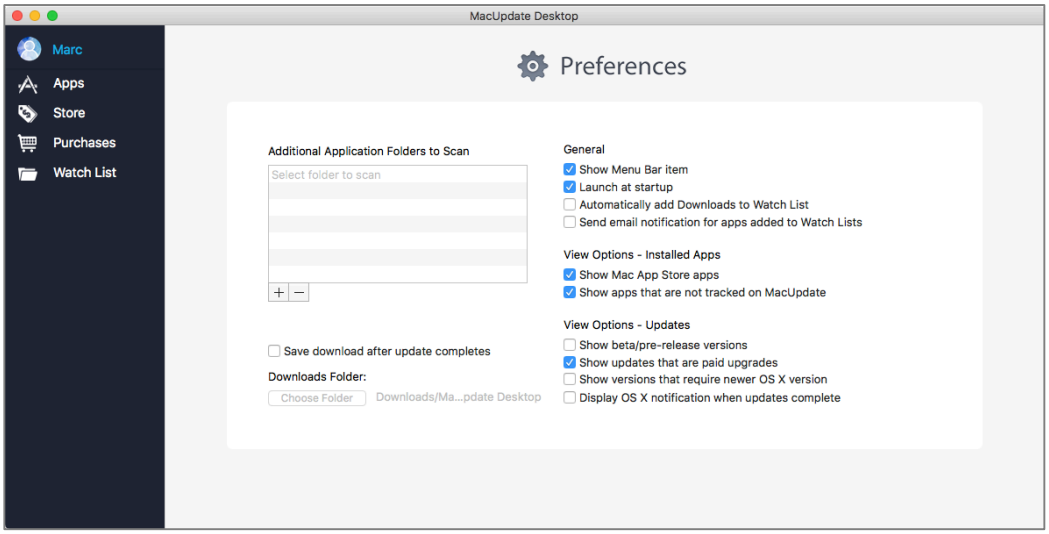
7. Click the *Sign Up* button.
8. The app will open.



9. MacUpdate Desktop will automatically scan your computer for all installed applications, check for any available updates, and then display them for you. Available updates will appear in red.



10. Select the *MacUpdate Desktop* menu > *Preferences.* Configure the main window as below:



11. Quit MacUpdate Desktop to save your preferences.

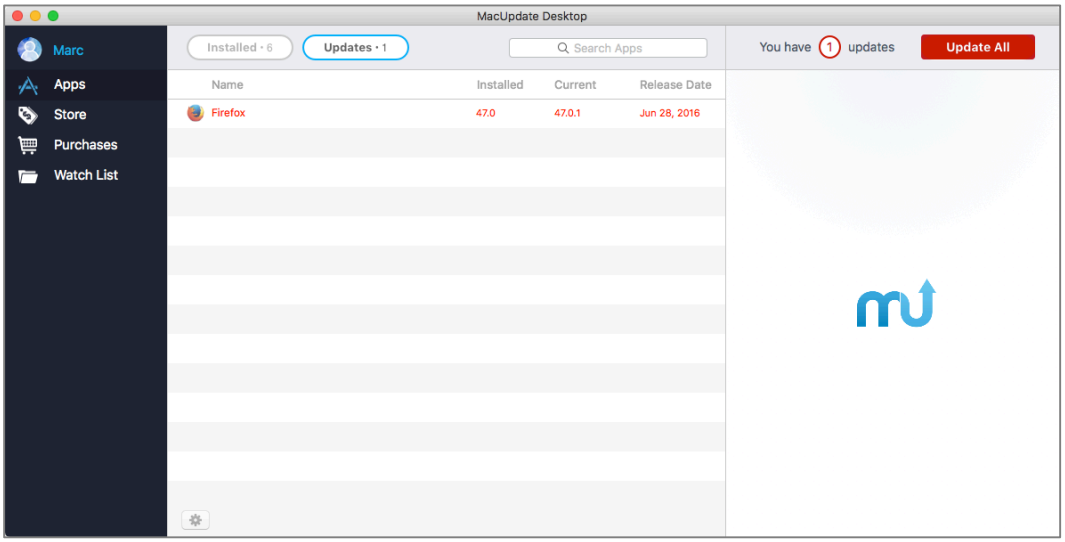
You have successfully installed and configured MacUpdate Desktop on your computer.

5.2.2 Assignment: Application Updates with MacUpdate Desktop

Once you have MacUpdate Desktop installed and configured, it will notify you daily of available Apple and third-party application updates.

In this assignment, you use MacUpdate Desktop to manually scan, download, and install updates.

1. From the *Applications* folder, launch MacUpdate Desktop. It will automatically begin scanning for available updates.
2. From the sidebar, select *Apps*.
3. Select the *Apps* menu > *Check for Updates*.
4. Select the *Updates* button in the navigation bar. This will filter out any applications that don't have updates. Then select the *Name* column to sort alphabetically:



5. From the top right corner of the windows, select *Update All* to, well, download and install all updates.
    - Note: If you prefer to hand-select which updates to install, double-click the target update from the main window.
6. Most updates require authorization to install. At the prompts, enter an administrator name and password.
7. When all desired updates are complete, Quit MacUpdate Desktop.

Can it get any easier or faster than this?

5.3 Additional Reading

Souppaya, Murugiah, and Karen Scarfone. "Guide to Enterprise Patch Management Technologies." NIST Special Publication 800-40, Revision 3. July 2013. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf>

Liu, Simon, Rick Kuhn, and Hart Rossman. "Surviving Insecure IT: Effective Patch Management." Insecure IT. 2009. <http://csrc.nist.gov/staff/Kuhn/liu-kuhn-rossman-v11-n2.pdf>

6 User Accounts

Those who desire to give up freedom in order to gain security will not have, nor do they deserve, either one.

–Benjamin Franklin[1]

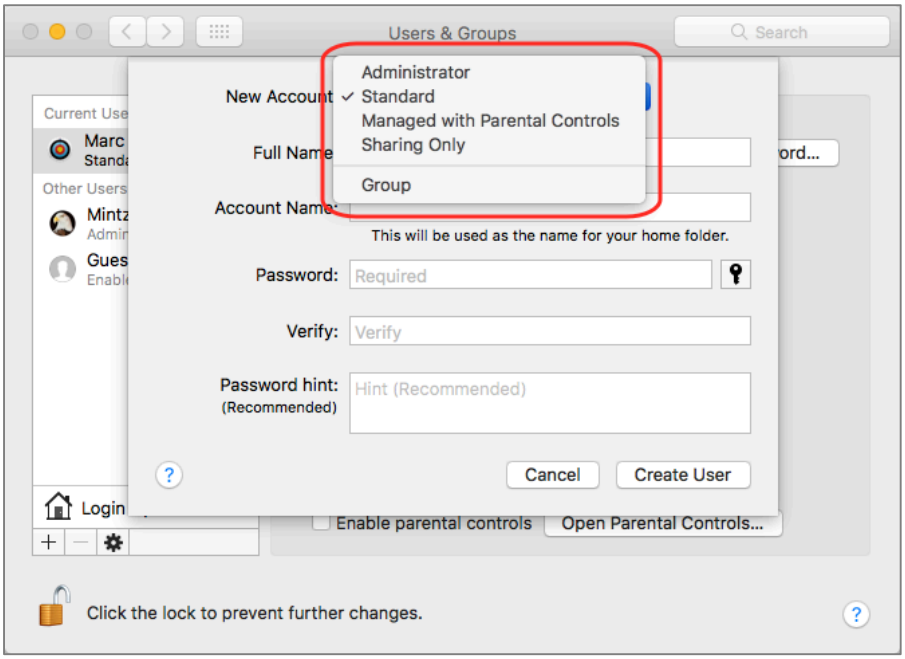
What You Will Learn In This Chapter

- Why never log in as an administrator
- Enable the root user
- Login as the root user
- Change the root user password
- Disable the root user
- Create an administrative user account
- Change from administrator to standard user
- Enable whitelisting with parental controls
- View parental controls logs
- Create a policy banner

[1] *https://en.wikipedia.org/wiki/Benjamin_Franklin*

6.1 User Accounts

macOS allows six different types of user accounts, each with its own pros and cons, powers and limitations. Most of these may be designated from the *Users & Groups System Preference.*



- **Root**. The Root account cannot be created or enabled from System Preferences. There can be one, and only one root account ever on any computer. Root is the ultimate lord over the system, with unquestioned power and control. If root does something dangerous–say, issues a command to erase the entire drive–the system will not even issue a *Danger, Will Robinson* alert, it will simply dutifully erase the drive. Root is present out of the box, but is disabled by not having a password assigned. It would be rare to ever need to enable the root user, as any administrator account can assume the powers of root.
- **Administrator**. There must always be at least one, and may be an unlimited number of administrators, or administrative user accounts, each having identical power over the computer. What makes an Administrator unique

above the Standard, Sharing, and Guest user accounts are its abilities to: Create new user accounts, delete user accounts, modify the contents of restricted folders (System, Library, Applications), authorize the installation or removal of applications and system updates, and take on the powers of root from the command line by issuing *sudo* and *su* commands.

- **Standard**. There can be an unlimited number of Standard accounts. This is the recommended account level for most users working locally on the computer. Standard accounts can open and work without limitations with any application installed on your Mac. The advantage of working as a Standard account is that it is not possible to damage the operating system or applications.
- **Managed with Parental Controls**. This account is typically a Standard account that has had Parental Controls assigned to it. Parental Controls further restrict the powers of the account by limiting: Access to specific applications, access to specific websites or any adult site, who can communicate with the user via Apple Mail and Messages/iChat, the hours for which the user may stay logged in, etc. Although this account level was originally intended to protect children from the darker areas of the Internet, and the computer from the children, it is a powerful tool for use with employees (guess how many billions of dollars a year in wasted productivity are spent on Facebook?)
- **Sharing Only**. There can be an unlimited number of Sharing Only accounts. This type of account cannot log in locally to the computer. The only access is via the network and file sharing. It is highly useful if you need to work with someone else on the same network and share files with them. This allows them to access your computer and files over the network, but only those files.
- **Guest**. There is only one Guest account. With Guest enabled, anyone may access your computer, either locally or via file sharing over the network. The Guest only has access to folders and files that have been shared as either read or read & write for everyone. If a Guest logs in locally, any documents the Guest creates and saves in the Guest home folder are deleted upon log off. Unless you are certain of your file-sharing configuration, it is unsecure to allow Guest access.

6.2 Never Log in As an Administrator

Maybe it is the human condition. We want power, authority, and more power! This carries over into how we log in to the computer. Everyone wants to be the administrator of his or her computer! Apple enables this. When the owner of a new Mac boots up for the first time, that person is prompted to create a user account, which is by default an administrator account.

But this is bad juju.

If you have the bad luck of launching a malware attack on your computer (most often unknowingly) while you are logged in as an administrator, the malware will take on your user account power. This means the malware has full control and power over the computer–including all other user accounts. Yikes.

On the other hand, if you have the same lousy luck to launch a malware attack while logged in as a non-administrative user, the malware will typically take on your non-admin power. Under this scenario, the malware has full control over your home folder and nothing else.

I can hear the wailing from here: *But I need to be an administrator. How else will I be able to install software and updates, and perform maintenance*?

Fear not. In macOS you do not need to be logged in as an administrator to perform administrator tasks (adding/deleting user accounts, installing/updating the system and applications, and running system diagnostic and repair utilities). You can be logged in with any type of user account. You only need to authenticate with an administrator name and password when prompted.

To do this, you need to have an administrative user account on the computer, but log in with a non-admin (standard) user account. Then when you are prompted for an admin name and password while performing admin duties, just enter them.

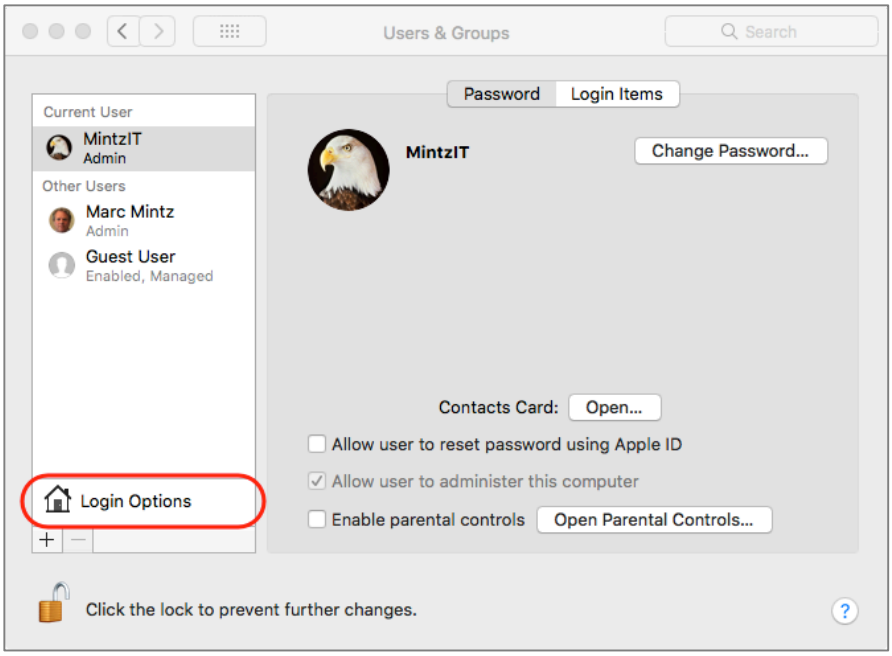
6.2.1 Assignment: Enable the Root User

As mentioned earlier, the root user account is present right out of the box, but it is disabled. The way Apple has disabled the account is by not assigning a password. That's right–all that is needed to enable root is to assign the account a password!

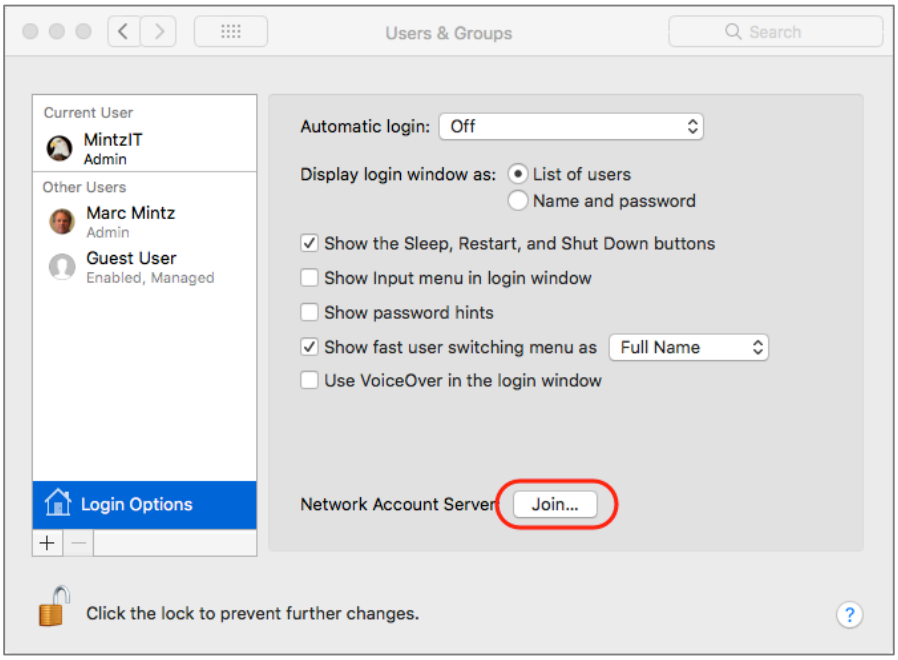
Before jumping in and assigning a password, give thought to why you want to enable root. Any administrative account can assume the powers of root whenever needed. I've also seen far too many users send their data to the cornfield when logged in as root and then making a simple keystroke error.

However, if you would like to experiment with root powers, here we go…

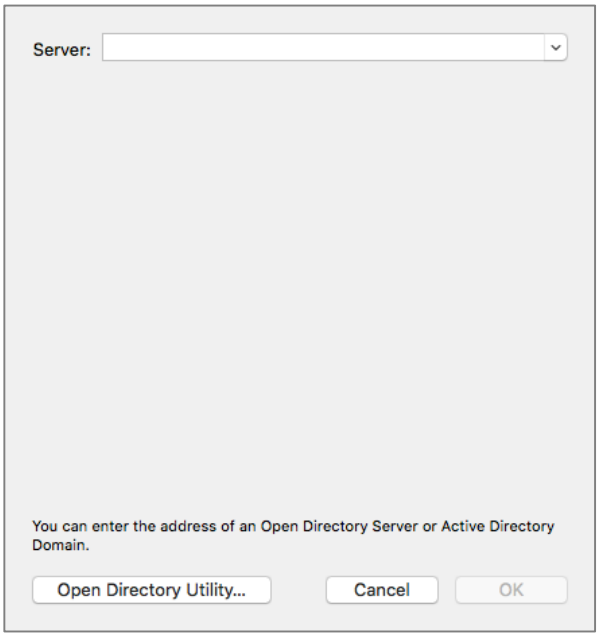
1. Select *Apple* menu > *System Preferences* > *Users & Groups*.
2. Authenticate.
3. Select the *Login Options* button.



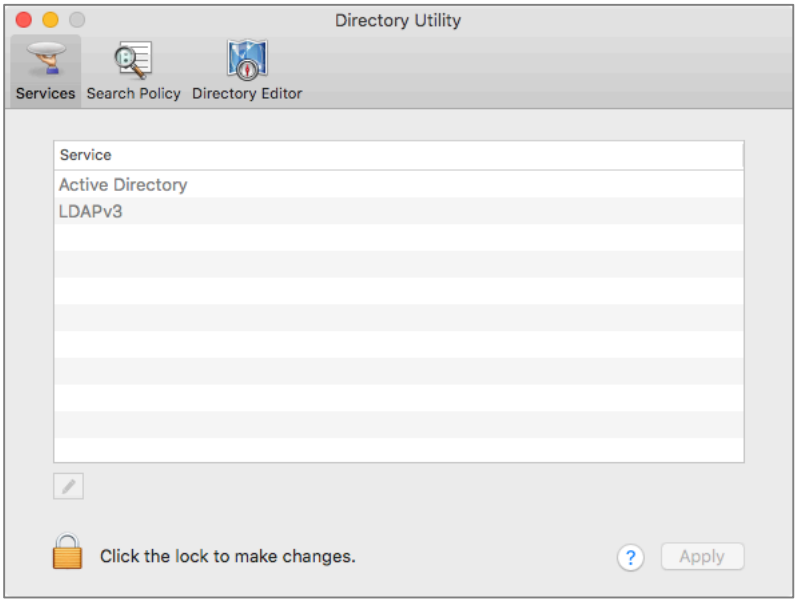
4. Select the *Network Account Server: Join* or *Edit button*.



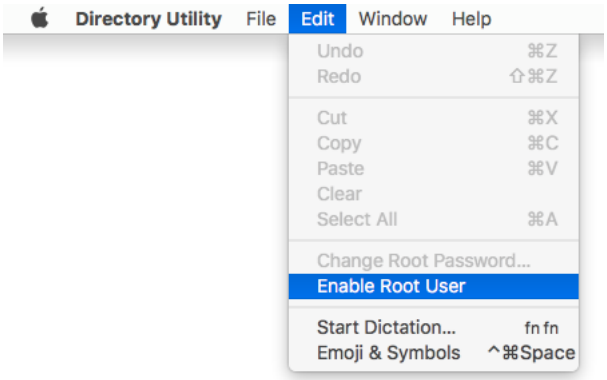
5. Select the *Open Directory Utility* button.



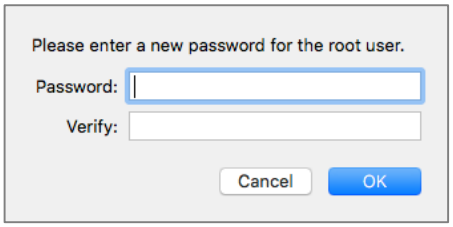
6. Click the lock icon, and then authenticate with administrator credentials.



7. Select the *Edit* menu > *Enable Root User*.



8. In the *Please enter a new password for the root user* window, enter a strong password, verify, and then click the *OK* button.



9. Quit Directory Utility.
10. Quit System Preferences.

Root was on the computer from the moment the system was installed. Giving root a password enabled it.

6.2.2 Assignment: Login as the Root User

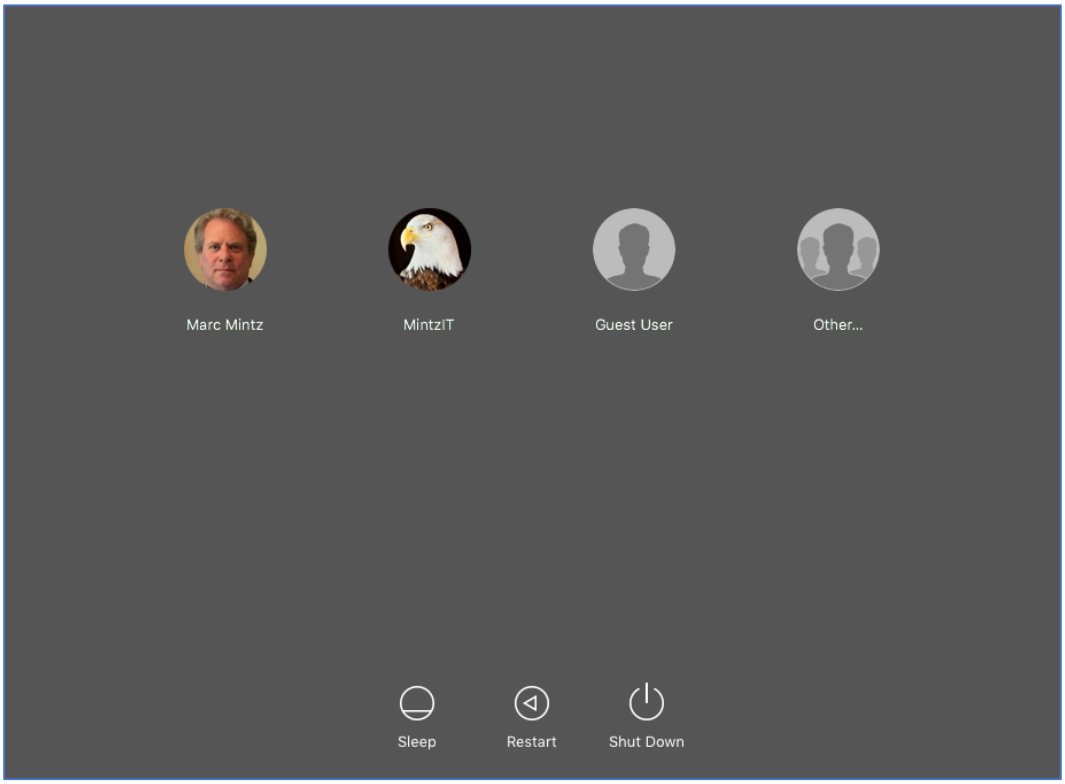
To see how the macOS landscape appears to root user, simply log in as root.

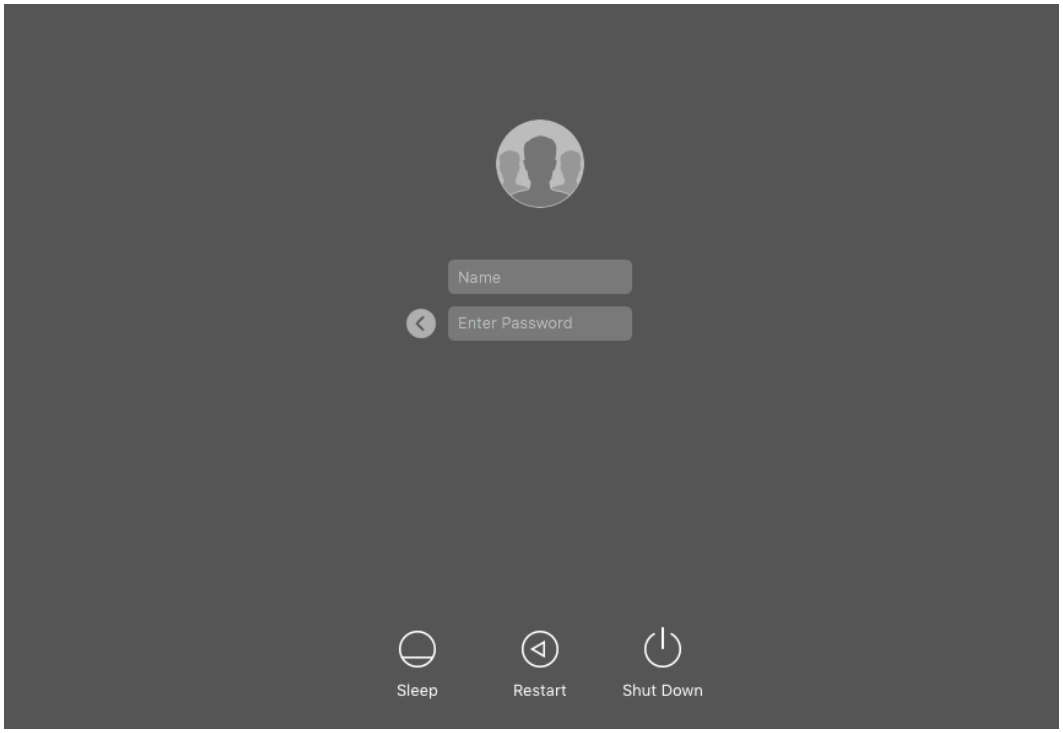
In this assignment, you log in as the root user

- Prerequisite: Completion of the previous assignment.

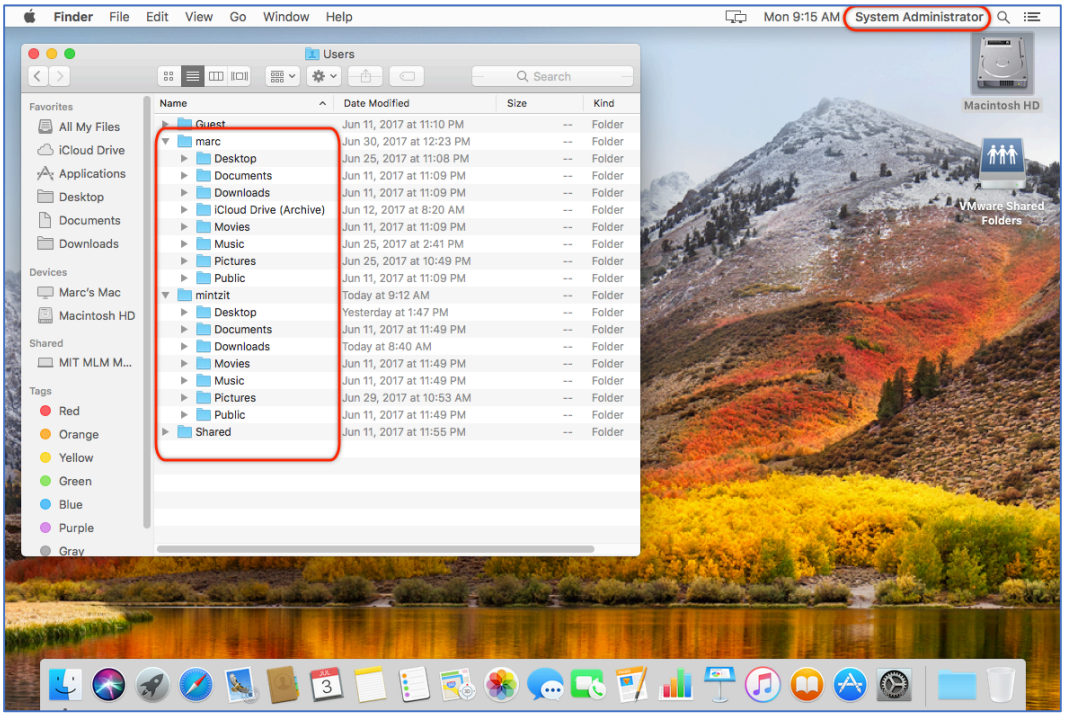
1. Log out of the current user account.

2. At the Login Window, log in as *root*. If you don't see the *root* user, select *Other…* From here you may enter the username "root", and the password you assigned for root.




Name
Enter Password
Sleep
Restart
Shut Down

3. Once at the Desktop, navigate to the */Users/<username>* folders. Notice that you can access any user folder with read and write permissions, and that the user name is *System Administrator.*



4. To log out, select the *Apple* menu > *Log Out.*
5. At the *Login Window,* log in with your standard account.

6.2.3 Assignment: Change the Root User Password

In this assignment, you change the root user password

1. Select *Apple* menu > *System Preferences* > *Users & Groups.*
2. Authenticate.
3. Select the *Network Account Server Join* or *Edit button.*
4. Authenticate.

5. Select the *Edit* menu > *Change Root Password.*
6. Enter a strong password
7. Quit Directory Utility.
8. Quit System Preferences.

6.2.4 Assignment: Disable the Root User

In this assignment, you disable the root user account.

1. Select *Apple* menu > *System Preferences* > *Users & Groups*.
2. Authenticate.
3. Select the *Network Account Server Join* or *Edit button.*
4. Authenticate.
5. Select the *Edit* menu > *Disable Root User.*
6. Quit Directory Utility.
7. Quit System Preferences.

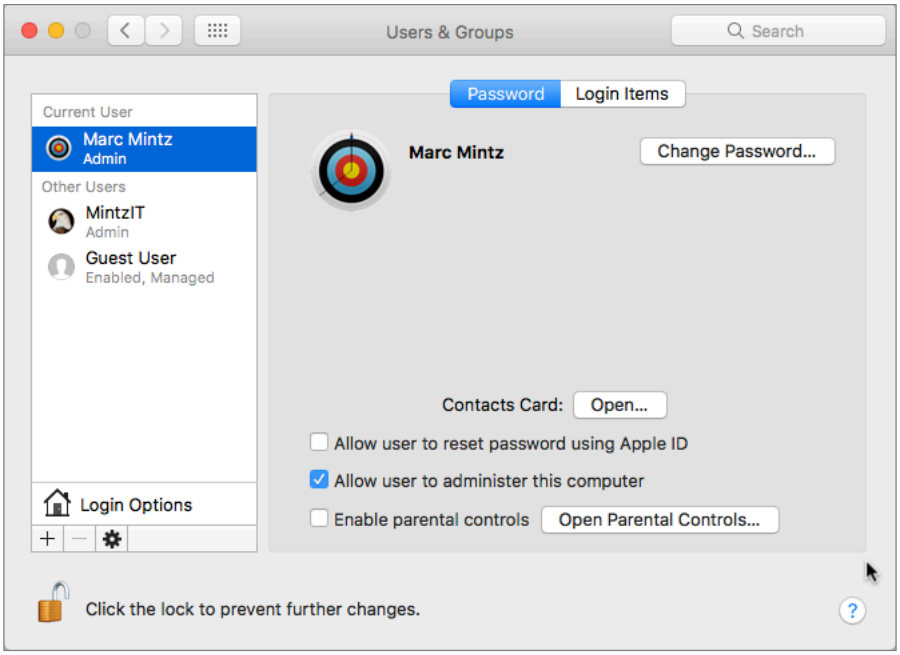
6.2.5 Assignment: Create an Administrative User Account

One of the most important rules in IT security is to log in with a non-administrative account, not an administrative account. However, the very first account created when you initially boot up your computer *is* an administrator!

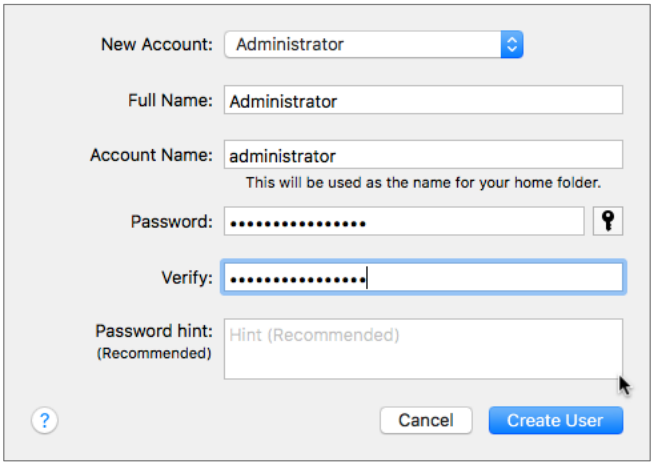
In this assignment, you create an administrative user account on the computer. In the next assignment, you will change your own account to a standard user account so that you will no longer be in violation of this rule.

1. Log in to the computer with your normal administrator account.

2. Open *Apple* menu > *System Preferences* > *Users & Groups*. Click the *Lock* icon in the bottom left corner, and then authenticate with an administrator name and password.



3. Click the + *(add user)* button at the bottom of the side bar. The *Create a New Account* window will open.



- From the *New Account* pop-up menu, select *Administrator*.
- In the *Full Name* field, enter "Administrator".
- In the *Account Name* field, enter "administrator".
- In the *Password* field, enter a strong password.
- In the *Verify* field, reenter the strong password.
- I'm not fond of entering anything in the *Password Hint* field, as this will be of assistance to hackers as well.

4. When done, click the *Create User* button. You are returned to the *Users & Groups* preference.
5. *Quit* System Preferences.

You have successfully created a new administrator account.

6.2.6 Assignment: Change from Administrator to Standard User

In the previous assignment, you created an administrative user account whose name and password can be used when needed.

In this assignment, you change your own account to a standard user account, which will remain your regular log in account.

1. Log out of your account.
2. Log in as the new administrator account.
3. Select the *Apple* menu > *System Preferences* > *Users & Groups*.
4. Unlock the Lock icon, and authenticate with administrator credentials.
5. Select your account in the side bar.

6. Disable the *Allow user to administer this computer* check box:

7. At the prompt informing you that the change will take place after a restart, select the *OK* button.
8. Select *Apple* menu > *Restart*.
9. Log in with your everyday account (now a Standard account).

Whenever you need to perform administrative tasks, use the name and password of the new administrator account you have just created. No need to login as an administrator!

6.3 Application Whitelisting and More with Parental Controls

In 2014, Target, Home Depot, and other major retailers were hacked for their customer databases. Although there were multiple breakdowns in the security protocols of these organizations, one step would likely have prevented all of them–*Application whitelisting.* This same strategy should be used by both home and business systems to help secure computer systems.

Application whitelisting is a process that allows only authorized applications to run on a computer, blocking any executable that is not on the list. This is a vital ingredient to system security because even the very best anti-malware catches only 99.9% of the *known* bugs. And what if your computer is penetrated by *unknown* malware? Anti-malware is of no use here. However, if your computer has application whitelisting in place, the unknown malware is blocked from executing! In macOS, *Parental Controls* can be used to perform application whitelisting.

Parental Controls allow an Administrator to restrict access to specific applications and services to a non-administrative user account. As the name implies, this feature was originally intended as a way for parents to better manage their children's account. It also has its place in the business setting by restricting specific applications (disallowing Spotify, etc.), restricting access to specific websites (pornography, Facebook, etc.), or allowing access to the account only during work hours.

Once Parental Controls has been used to implement application whitelisting, it will be necessary for the administrator to be available for a brief time while the unintended consequences shake out. It is common for some permitted applications to require the use of a restricted application or process. An administrator will need to be available to provide authorization.

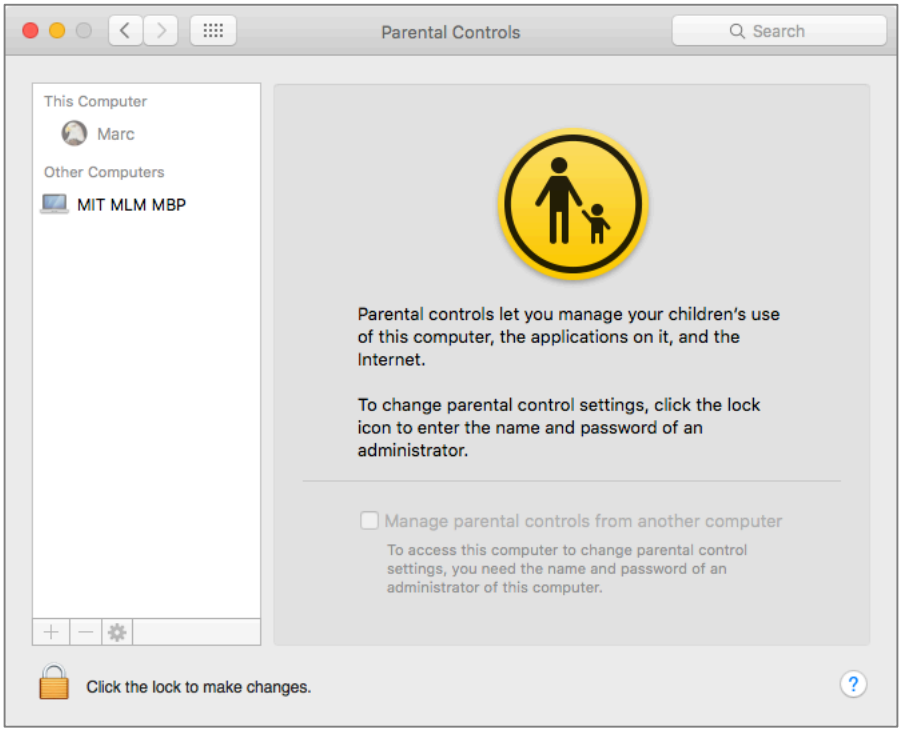
Once Parental Controls are established for a user account, the account is referred to as *Managed with Parental Controls,* or as a *managed* account. Only non-administrative accounts may be managed. If creating a new user account, it can be initially setup as *Managed with Parental Controls.* If the account already exists as a

Standard account, it can be converted to managed. The *Guest* account can also have parental controls assigned.

6.3.1 Assignment: Configure a Managed with Parental Controls Account

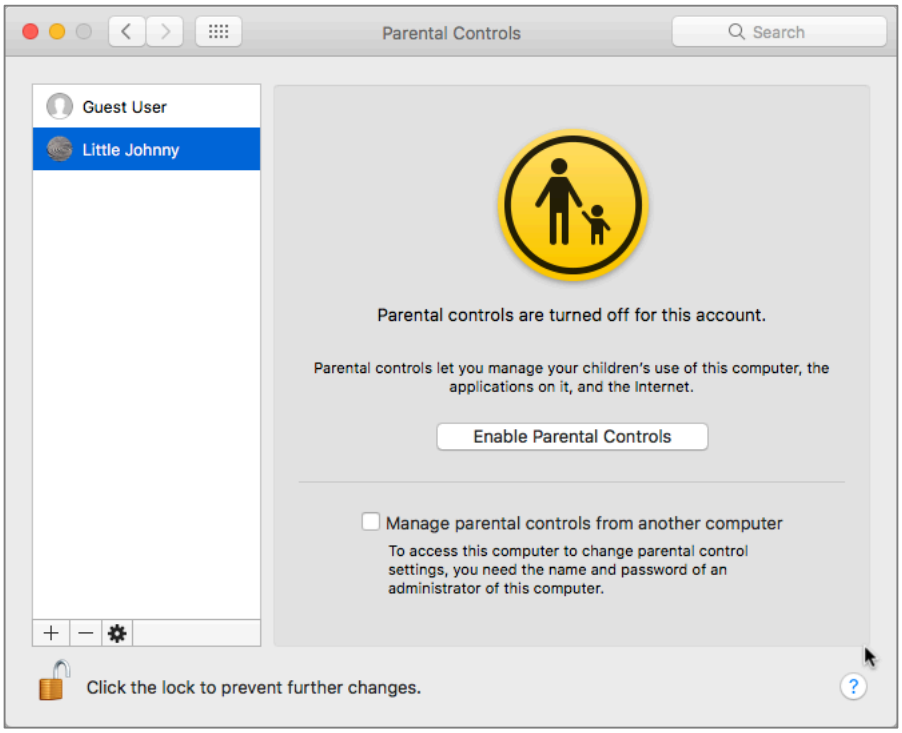
For this assignment, you configure your own account to have the added security of application whitelisting. These same steps should be taken for all non-administrative accounts on your computer, and all computers in your household or business. Understand that best practices hold that *all* your non-administrative accounts should have application whitelisting enabled–and that you never login with an administrative account.

1. On the computer hosting the user account to be managed, open *Apple* menu > *System Preferences* > *Parental Controls.*

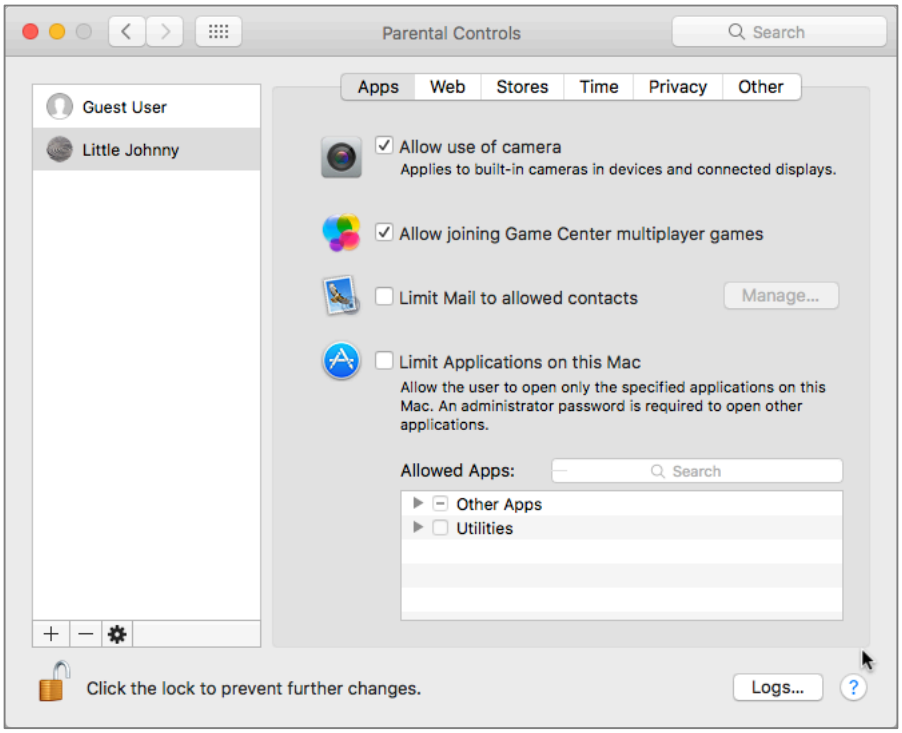


2. Select the *Lock* icon to authenticate as an administrator.

3. In the sidebar select the target account to manage, and then select the *Enable Parental Controls* button.
    - Note: If you want to manage parental controls from another computer on the same network, enable the *Manage parental controls from another computer* checkbox.

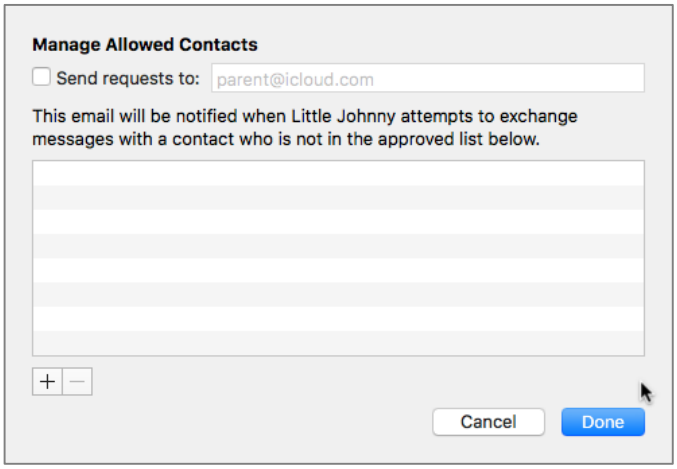


4. The *Parental Controls* System Preference pane opens. Unlock the pane.



- *Allow use of camera* is self-explanatory.
- *Allow joining Game Center multiplayer games* is self-explanatory.

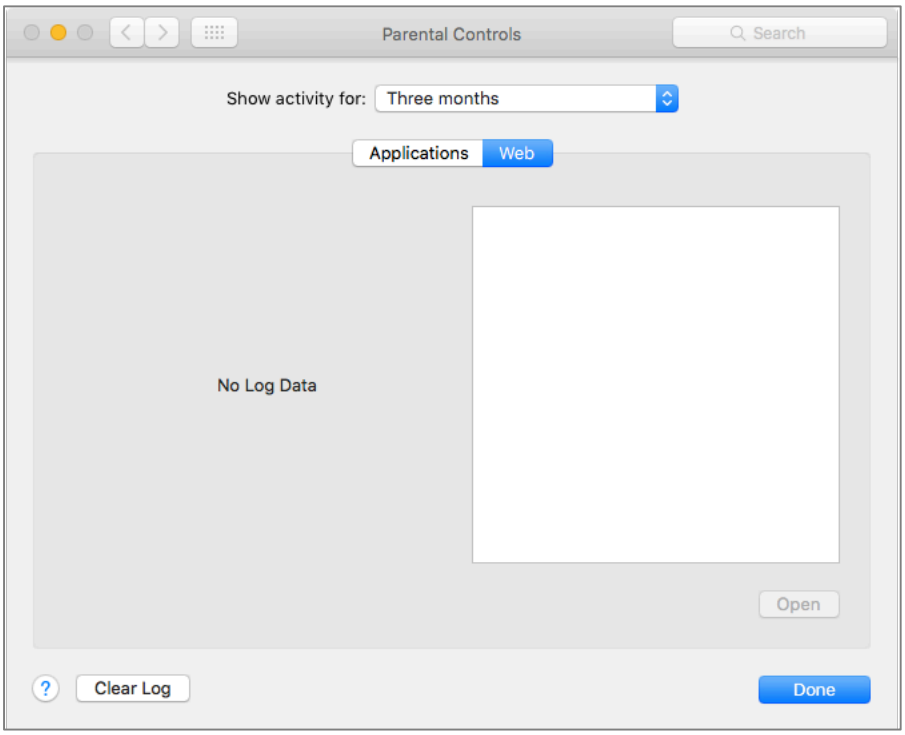
- *Limit Mail to allowed contacts* helps to prevent unknown and unwanted people from exchanging email with the user. Selecting the *Manage* button opens a configuration window for this option.



- *Limit Applications on this Mac* activates application whitelisting. It allows picking which specific applications the account will have access.

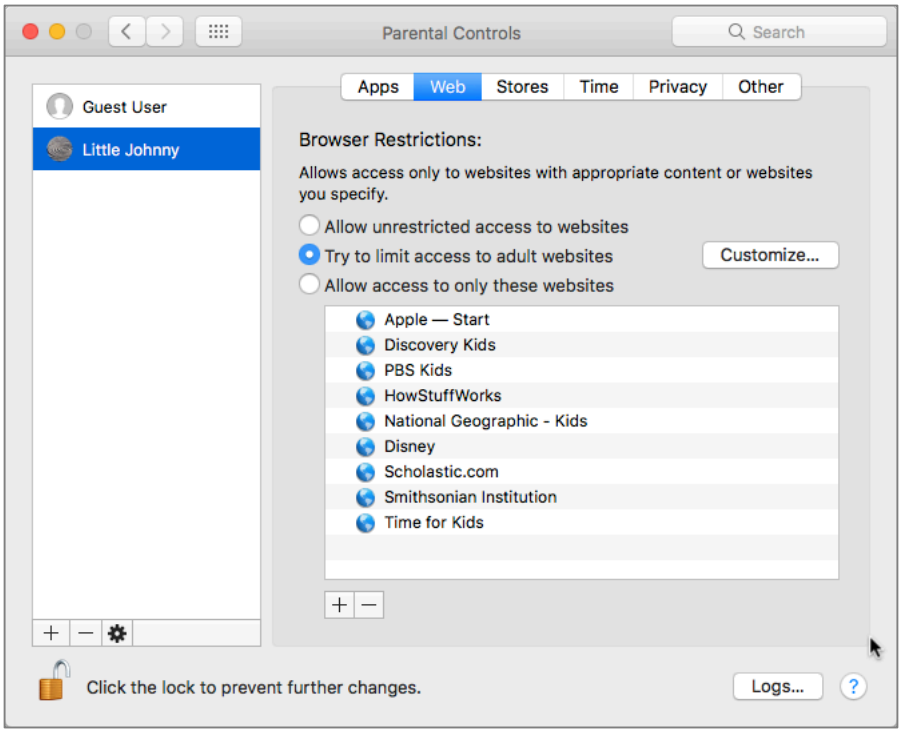
5. Expand *Other Apps*. Enable the checkbox for applications this account needs, but do not enable the *Other Apps* checkbox as this will allow any application to run. Keep in mind we are attempting to prevent unwanted malware from launching.
6. Expand the Utilities checkbox. Pick which utilities should be allowed access by this user.

7. By selecting the *Logs* button, the administrator can view the activities of the managed user. Logs may be viewed from any other computer on the same network.



8. Select the *Done* button to return to Parental Controls.

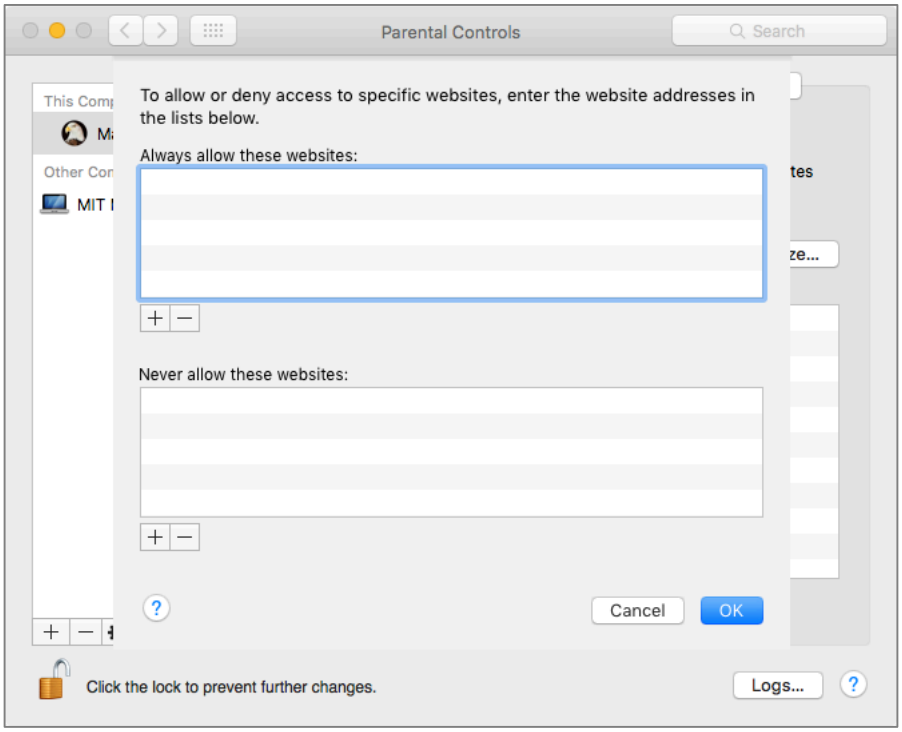
9. Select the *Web* tab to view the managed web options.



- *Allow unrestricted access to websites* eliminates any filtering of website access. Less than 5% of the businesses with which we hold an initial consult restrict web use. This is due primarily from leadership not understanding the consequences of doing so. Per a recent sarlary.com survey[2] 64% of employees visit non-work-related websites *every day*. This is a costly misuse of company resources. It is also a significant source of malware infections. We do not recommend this option without a demonstrated business need.
- *Try to limit access to adult websites automatically* is our recommendation for business environments. Selecting the *Customize* button opens the

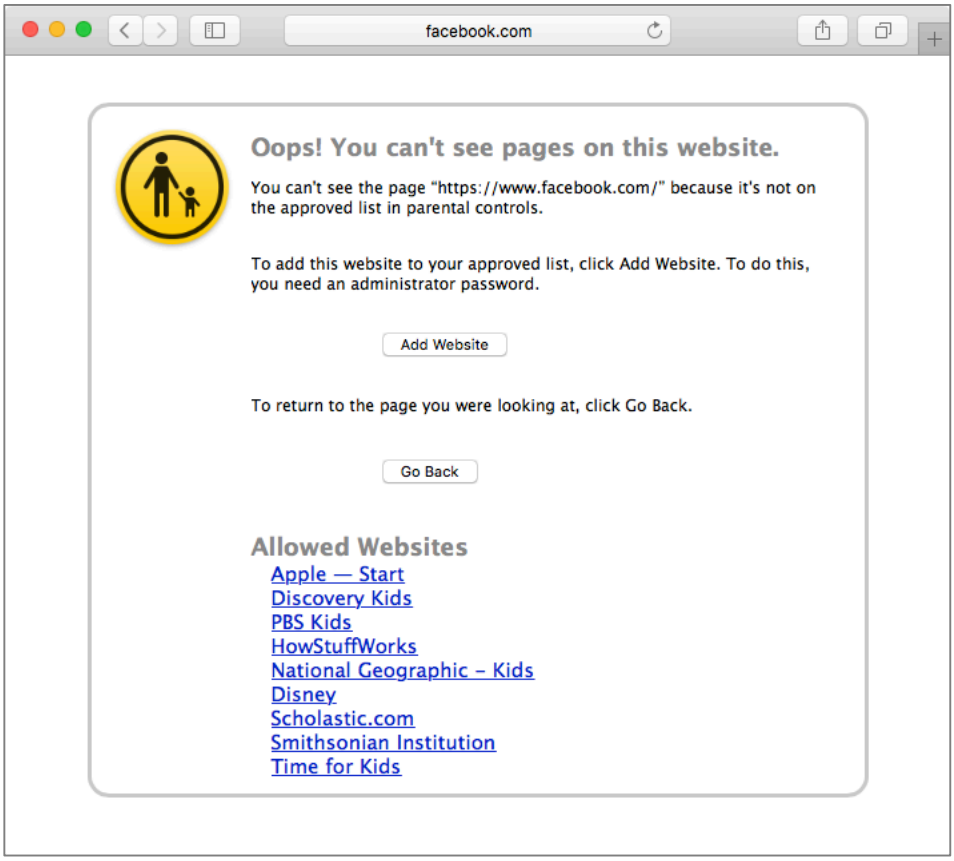
[2] *http://www.salary.com/wasting-time-at-work-2012/*

configuration window. When done looking it over, select the *OK* button to return to Parental Controls.

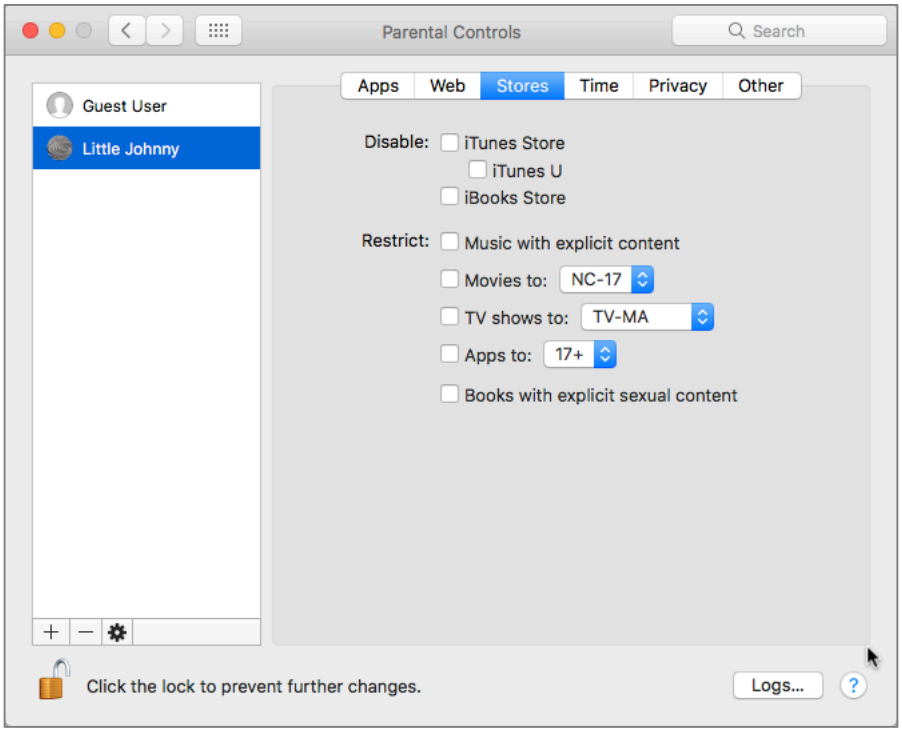


- *Allow access to only these websites* is the most restrictive, and may find its niche with young children.
- If the user attempts to visit a site that is restricted, they receive notice of such. If the user has access to administrative credentials, or if an

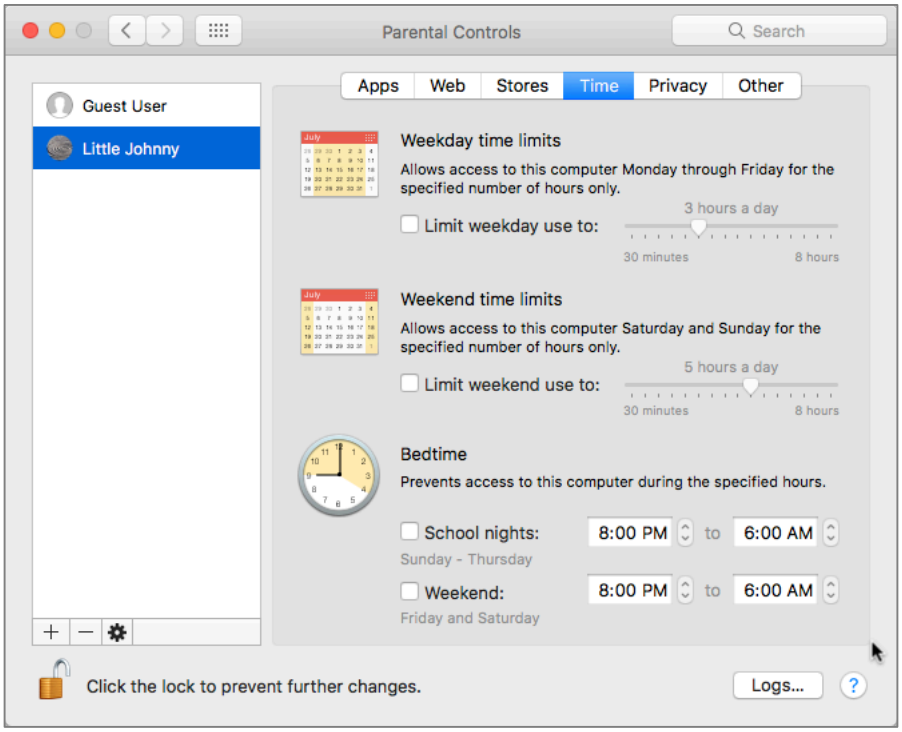
administrative user is available, selecting the *Add Website* button will make this website accessible.



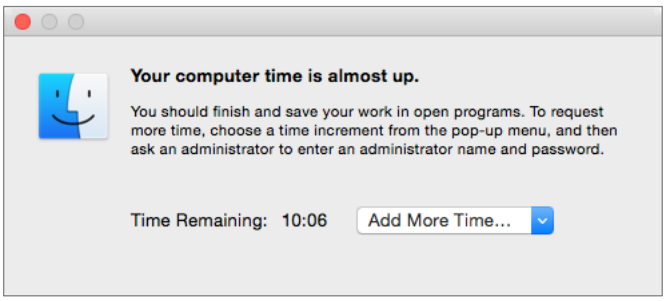
10. Selecting the *Stores* tab allows configuring access to all the various Apple commercial offerings.



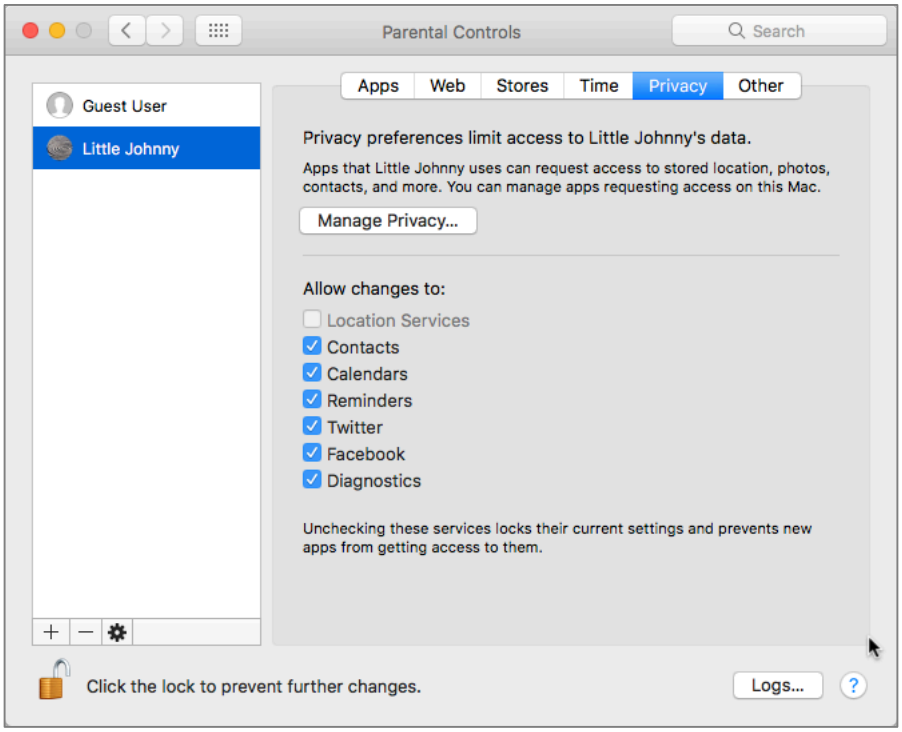
11. Selecting the *Time* tab allows configuration of when the account can use the computer:



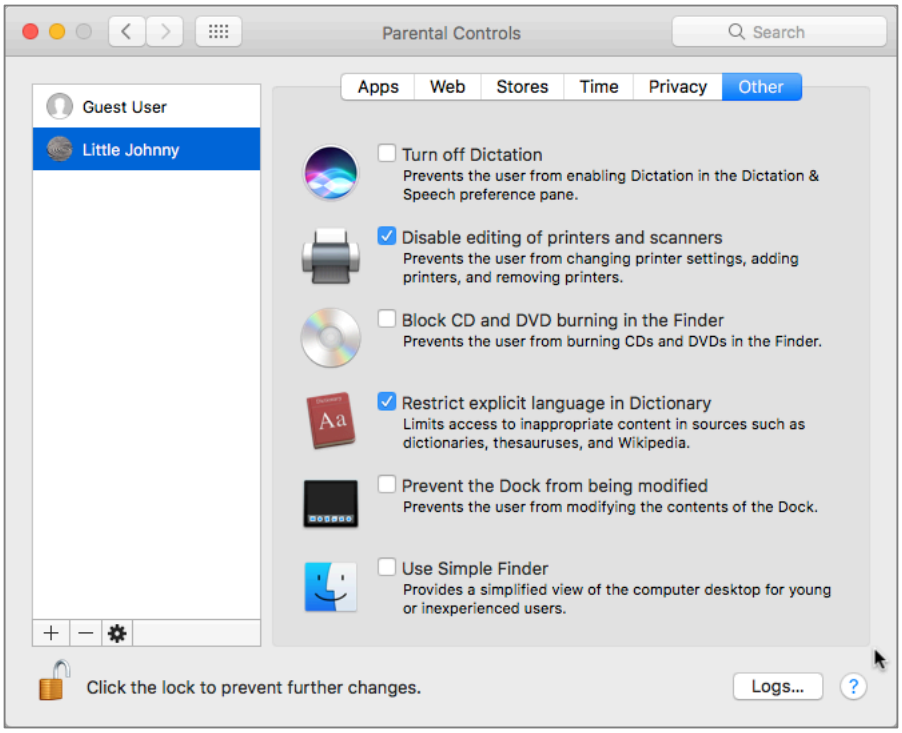
- As the end of their time approaches, an alert appears, allowing any administrative user to extend the managed user time for this session only:



12. Selecting the *Privacy* tab allows configuration of privacy settings for this account.



13. Selecting *Other* allows configuration of the odds and ends.



14. Quit System Preferences.

You have successfully created a Managed user account with Parental Controls.

6.3.2 Assignment: View Parental Controls Logs

If the managed user has an account on the same computer as the administrator, viewing the logs is just a couple of clicks away.

In this assignment, you view the Parental Control logs

1. Log in as the administrator.
2. Select the *Apple* menu > *System Preferences* > *Parental Controls*.
3. Click the *Lock* icon and then authenticate as an administrator.
4. Select the targeted managed account.

5. Select the *Logs* button.
6. In the *Logs* window, you can choose to view the *Websites Visited, Websites Blocked, Applications,* and *Messages*. When selecting the specific log files, each event is listed individually, along with time stamps. In the case of websites, they will be grouped by category.
7. *Quit* Parental Controls.
8. Take your sweet time torturing the managed user with the knowledge you have gleamed about them.

Viewing the logs from another macOS computer on the same network is almost identical. The only difference is that when opening *Parental Controls* on your own Mac to view the logs of the managed user on the remote Mac, you will see the user account under *Other Computers*.

6.4 Policy Banner

Within some organizations, the legal department specifies there must be a *Policy Banner* present at startup. This will alert any would-be hackers or criminals that proceeding into the computer is considered a criminal offense. It is possible having a policy banner in place may prevent the "I didn't know I was doing anything wrong" defense in court.

6.4.1 Assignment: Create a Policy Banner

In this assignment, you create a policy banner that will display upon startup.

1. Log in with an administrative account.
2. Open a word processor or text editor that can create a plain text (.txt) or rich text (.rtf) file format.
3. Create a new document with the specifics required for your policy banner. A sample policy banner is listed below:

   *** WARNING***

   This is a <organization name> computer system. <Organization name> computer systems are provided for processing of official <organization name> information only. All data contained on this system is owned by the <organization name> and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel.

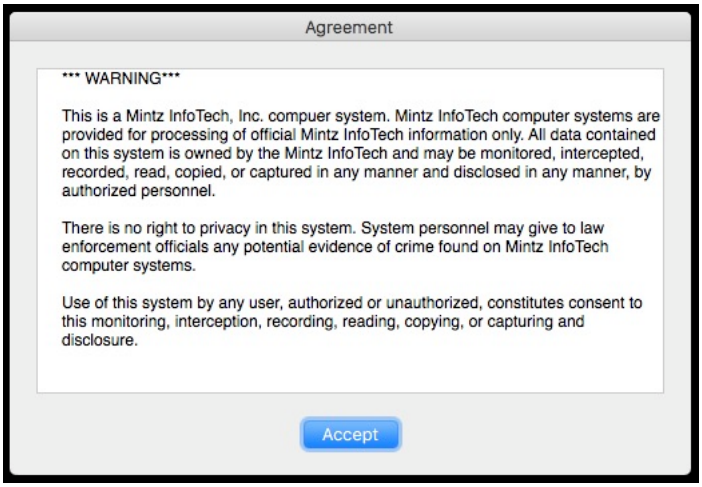
   There is no right to privacy in this system. System personnel may give to law enforcement officials any potential evidence of crime found on <organization name> computer systems.

   Use of this system by any user, authorized or unauthorized, constitutes consent to this monitoring, interception, recording, reading, copying, or capturing and disclosure.

4. Save the file as *PolicyBanner* in either .txt or .rtf, to the Desktop.
5. Drag and drop the PolicyBanner file into the */Library/Security* folder.
6. At the prompt, enter your administrator credentials to authorized the copy.
7. Open Terminal to adjust permissions so that Everyone (Other) has read and execute privileges. Enter:
    - For .txt: `sudo chmod o+rx /Library/Security/PolicyBanner.txt`
    - For .rtf: `sudo chmod -R o+rx /Library/Security/PolicyBanner.rtf`
8. At the prompt, enter your password.
9. Quit Terminal.

Test the Policy Banner

10. Restart.
11. Before the login window, you should see the policy banner appear:



12. Select the *Accept* button.
13. Continue log in as normal.

7 Storage Device

I am disturbed by how states abuse laws on Internet access. I am concerned that surveillance programs are becoming too aggressive. I understand that national security and criminal activity may justify some exceptional and narrowly tailored use of surveillance. But that is more reason to safeguard human rights and fundamental freedoms.

–Ban Ki-moon[1], Secretary General of the United Nations

What You Will Learn In This Chapter

- Disable USB, FireWire, and Thunderbolt storage device access
- Boot into Target Disk Mode
- Boot into Recovery HD Mode
- Boot into Single-User Mode
- Enable FileVault 2
- Remotely access and reboot a FileVault drive

[1] *https://en.wikipedia.org/wiki/Ban_Ki-moon*

7.1 Block Access to Storage Devices

In some environments, it is appropriate to block access to USB, FireWire, or Thunderbolt storage devices. This may be required so that users cannot copy sensitive data. There are two ways to accomplish this:

- Disable the software controlling USB, FireWire, or Thunderbolt storage devices. Advantages: Free, takes a minute to accomplish. Disadvantages: Difficult to undo, impacts all users equally.
- Install a utility to control access. We recommend *DeviceLock*[2]. Advantages: Granular control over any storage device from thumb drive to iPhone, controllable user by user. Disadvantages: Must be run from a Windows computer to control macOS, OS X and Windows clients.

7.1.1 Assignment: Disable USB, FireWire, and Thunderbolt Storage Device Access

Within a few rarified, high-security environments, it is necessary to ensure that users are unable to use USB or FireWire storage devices. This can be accomplished by removing the drivers for such devices

In this assignment, you disable the drivers for USB, FireWire, and Thunderbolt storage devices

1. Log in as Root.
2. Navigate to the */System/Library/Extensions* folder.
3. Rename *IOUSBMassStorageClass.kext* to *IOUSBMassStorageClass.kext.disabled.*
4. Rename *IOFireWireSerialBusProtocolTransport.kext* to *IOFireWireSerialBussProtocolTransport.kext.disabled*.
5. Rename *IOThunderboltFamily.kext* to *IOThunderboltFamily.kext.disabled.*
6. Reboot.

[2] *http://www.devicelock.com*

7. Connect either a USB or FireWire storage device to the computer. Note that it will not mount, and that no user has access.

You have successfully blocked any user on this computer (including yourself, all administrators, and even root) from being able to "steal" data from this computer onto any USB, FireWire, or Thunderbolt storage device.

7.1.2 Assignment: Enable USB, FireWire, and Thunderbolt Storage Device Access

In this assignment, you reverse the work performed in the previous assignment, enabling storage device access

1. Log in as Root.
2. Navigate to the */System/Library/Extensions* folder.
3. Rename *IOUSBMassStorageClass.kext.disabled* to *IOUSBMassStorageClass.kext*.
4. Rename *IOFireWireSerialBusProtocolTransport.kext.disabled* to *IOFireWireSerialBussProtocolTransport.kext*.
5. Rename *IOThunderboltFamily.kext.disabled* to *IOThunderboltFamily.kext.*
6. Reboot.
7. Connect either a USB, FireWire, or Thunderbolt storage device to the computer. Note that it will now mount, and all users have access.

You have successfully returned your computer to default functionality.

7.2 FileVault 2 Full Disk Encryption

Strong passwords keep the network and Internet-based password attacks at bay, but should someone have physical access to your computer, they may be able to perform a brute force attack on your login password.

Prior to Mac OS X 10.7, the system included home directory encryption using *FileVault*, now referred to as *Legacy FileVault.* This was enabled on a user-by-user basis.

Starting with Mac OS X 10.7, and continuing with macOS, we now have FileVault 2[3] (normally referred to as simply *FileVault*), which enables military-grade AES-256 full disk encryption. With FileVault configured, your drive has a secure wall around it that can only be penetrated by entering an account password.

Once FileVault has been enabled, it may take 1–5 days for the encryption to complete on a spinning hard disk drive, as little as 30 minutes on a Solid-State Drive or Flash Drive. During this time, you can continue working normally, although your computer may be sluggish as it is doing both your work and the encryption process.

Enabling FileVault has an additional advantage: Boot time keyboard commands require authenticating at the Login Window. This has significance for three keyboard commands.

Target Disk Mode allows booting with macOS functionally disabled, with only Firewire and Thunderbolt active for storage devices. This effectively turns the computer into an external drive that can connect via Firewire or Thunderbolt.

Recovery HD Mode allows booting into the otherwise invisible Recovery HD partition, to perform directory repair with Disk Utility, reinstall macOS, enable Firmware password, etc.

Single-User Mode allows booting into a command line state, prior to loading of Open Directory (the database holding all user accounts) and the entire OS. In this state, only the Root user account is active, hence the term *Single-User Mode.*

[3] *http://en.wikipedia.org/wiki/FileVault*

7.2.1 Assignment: Boot into Target Disk Mode

In this assignment, you boot into Target Disk Mode (TDM).

1. Power off your computer.
2. Power on your computer, and then immediately (before the appearance of the Apple logo) hold down the *T* key, and keep held down.
3. If your computer does not have FileVault enabled, skip to step 7. If FileVault is enabled:
4. The login window will appear.
5. Release the T key.
6. Select your account, enter your password, and then tap the Return/Enter key.
7. The Firewire or Thunderbolt icon will appear moving around your screen. You are now in TDM.
8. To verify this, you may connect your computer to another Mac via Firewire or Thunderbolt, and it will mount on the other computer.
9. To exit TDM, press and hold the power button to power off, and then power on as normal.

7.2.2 Assignment: Boot into Recovery HD Mode

In this assignment, you will boot into Recovery HD Mode.

1. Power off your computer.
2. Power on your computer, and then immediately (before the appearance of the Apple logo) hold down the *cmd* + *R* keys, and keep held down.
3. If your computer does not have FileVault enabled, skip to step 7. If FileVault is enabled:
4. The Login Window appears.
5. Release the cmd + R keys.
6. Select your account, enter your password, and then tap the Return/Enter key.

7. The Recovery HD home screen will appear, displaying a list of available *Utilities*.
    a. If you wish, you may experiment with the various utilities.
8. To exit Recovery HD Mode, select the *Apple* menu > *Restart*.

7.2.3 Assignment: Boot into Single-User Mode

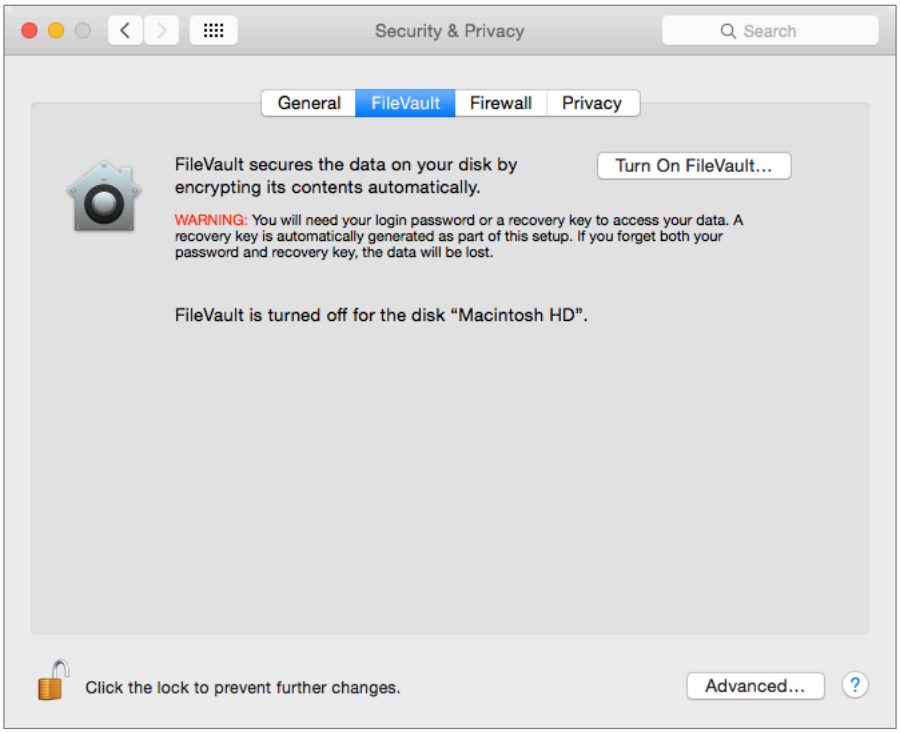
In this assignment, you boot into Single-User Mode.

1. Power off your computer.
2. Power on your computer, and then immediately (before the appearance of the Apple logo) hold down the cmd + S keys, and keep held down.
3. If your computer does not have FileVault enabled, skip to step 7. If FileVault is enabled:
4. The Login Window appears.
5. Release the cmd + S keys.
6. Select your account, enter your password, and then tap the Return/Enter key.
7. The Single-User Mode screen will appear, displaying a list all the commands and activity that is occurring.
8. Within a minute or so the scrolling list of activities will stop at a command line prompt. If you are familiar with Linux, Unix, or the bash shell, you can issue commands and look around the drive from here .
9. To exit Single-User Mode, enter *exit* at the prompt, and then tap the Return/Enter key. The system will continue to the normal login window.

7.2.4 Assignment: Enable and Configure FileVault 2

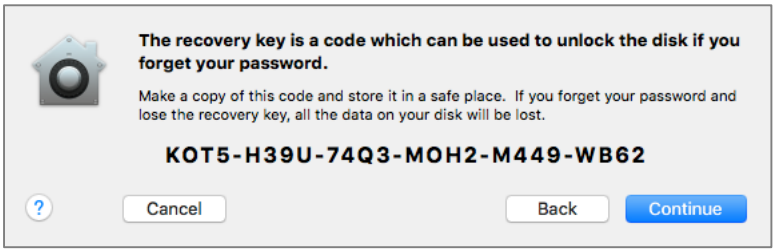
In this assignment, you enable full disk encryption on your boot drive using FileVault 2.

1. Open *Apple* menu > *System Preferences* > *Security & Privacy*, and then select the *FileVault* tab.

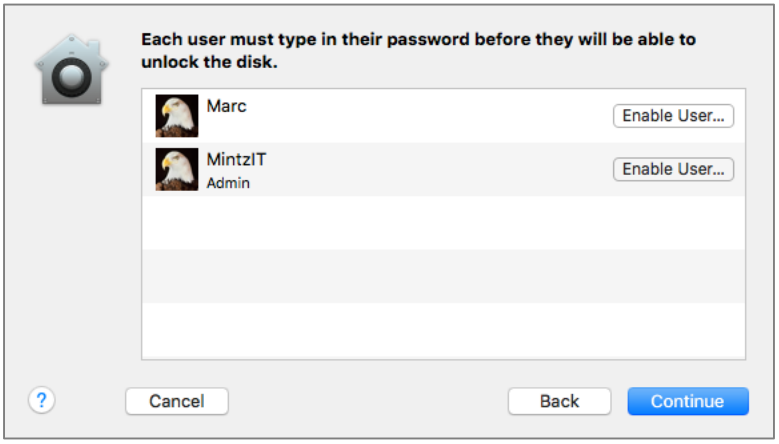


2. Unlock the *FileVault* lock icon.
3. Select the *Turn On FileVault…* button.
4. A dialog box appears to select using either your iCloud account or a recovery key to unlock the disk in the event your login password is forgotten.

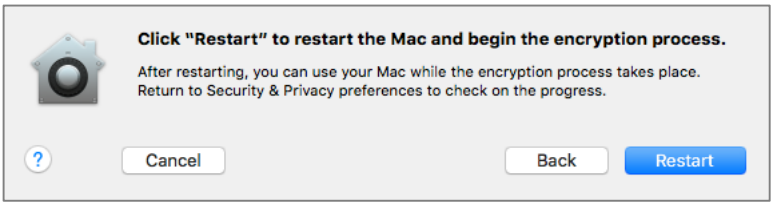
- Selecting *Allow my iCloud account…* allows you to use your iCloud account password to be used, and then select the *Continue* button.
- Selecting *Create a recovery key…* presents a randomly generated password. Store this key in a secure location. I recommend in your Address Book / Contacts application, and then select the *Continue* button.



5. If there are multiple user accounts on this machine, you are asked to enable the user accounts that are to be allowed to unlock the encrypted boot drive to boot up. For each of these accounts, click the *Enable User…* button, and enter the account password. (Users that have not been enabled can still access their accounts via *Fast User Switching* after the drive is unlocked by one of the authorized accounts.) Then click *Continue*.



6. Select the Restart button to restart the Mac and begin the encryption process.



7. When your Mac returns to the Desktop, the *Security & Privacy* preference window will reopen, providing a progress indicator for the encryption process. You may close this window if desired.

The encryption process may take as little as an hour (small flash drive in a MacBook Air), or more than a day (4TB hard disk drive in an older, slower computer.) Though encryption will start again after the computer has been sleeping or turned off, to have it complete faster, set *Energy Saver* System Preferences to *Never Sleep*.

Enabling FileVault 2 is only half of the solution. The other half is to enable the Firmware Password. More on that later.

7.3 FileVault Resistance to Brute Force Attack

Apple claims there is no back door or golden key to FileVault 2. If there is a way to hack into a FileVault-protected volume, only one group is laying claim to it. *Passware*[4] says their software can break into a FileVault 2 drive in 40 minutes. The author has not tested this claim.

It is recommended that in addition to using FileVault to encrypt the drive, the EFI chip (firmware chip) on the motherboard also have a password in place, called a *Firmware Password*. More on that later.

[4] *https://www.passware.com/*

7.4 Remotely Access and Reboot a FileVault Drive

When a drive is protected with FileVault, remote support that requires a reboot may become an issue. The reason is that the macOS will reboot into an encrypted mode, which most remote support software cannot communicate with. So, once the technician has rebooted the machine, they have lost control over it.

A workaround for this situation is to temporarily disable FileVault. This can be done using the Terminal to enter the appropriate command.

7.4.1 Assignment: Temporarily Disable FileVault

In this assignment, you temporarily disable FileVault during a macOS restart. This will allow remote support software to regain control over the computer after a restart.

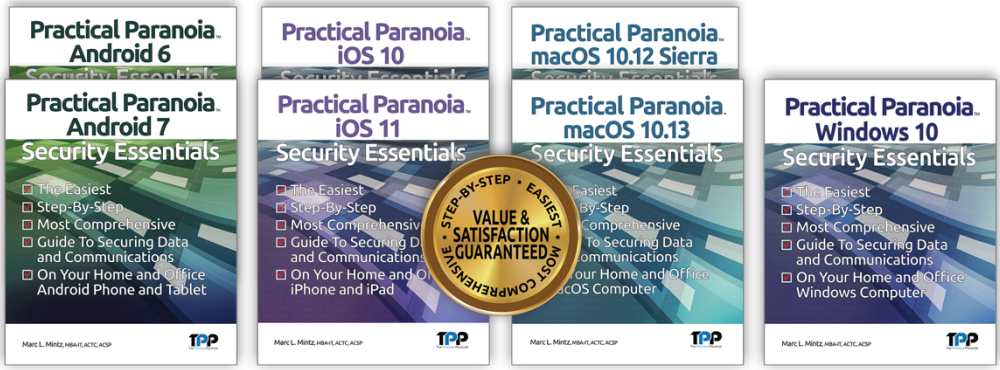
- Prerequisite: The computer must have the Root user account enabled, and you must know the Root password.

1. Login to an administrative account.
2. Open Terminal.app.
3. Enter the command: `sudo fdesetup authrestart`
4. At the authentication prompt, enter your administrative password.
5. At the prompt: *Enter a password for '/', or the recovery key,* enter the Root password.
6. The computer will restart with FileVault disabled.
7. At the login screen, enter your *user name* and *password*. You will be able to work remotely on the computer.
8. On the next boot, FileVault will be enabled as normal.

Index

Practical Paranoia Workshops & Books

4 Years Undisputed #1 Best, Easiest, & Most Comprehensive Cybersecurity Series



This is an age of government intrusion into every aspect of our digital lives, criminals using your own data against you, and teenagers competing to see who can crack your password the fastest. Every organization, every computer user, everyone should be taking steps to protect and secure their digital lives.

The *Practical Paranoia: Security Essentials Workshop* is the perfect environment in which to learn not only *how*, but to actually *do* the work to harden the security of your macOS and Windows computers, and iPhone, iPad, and Android devices.

Workshops are available online and instructor-led at your venue, as well as tailored for on-site company events.

Each Book is designed for classroom, workshop, and self-study. Includes all instructor presentations, hands-on assignments, software links, and security checklist. Available from Amazon (both print and Kindle format), and all fine booksellers, with inscribed copies available from the author.

Call for more information, to schedule your workshop, or order your books!

The Practical Paranoid, LLC
+1 888.504.5591 • info@thepracticalparanoid.com
https://thepracticalparanoid.com