

Leon H. Lincoln III

Leon is a System Administrator for the Broad Institute of MIT and Harvard which is a biomedical and genomic research center located in Cambridge, Massachusetts.

As a Certified Casper Administrator, Certified Casper Mobile Administrator, Apple Certified Technical Coordinator, and Microsoft Mac Office 2015 Expert he designs and implements the Apple environment at the Broad.

Along with the architectural responsibilities he also manages the Google Environment, accounts for users (Active Directory, NIS and Google), maintains the Casper Self Service infrastructure, and provides many other services related to the Windows and Linux environments and acts as the senior escalation point for the Service Desk Team.

A featured speaker at many events including MacTech, MIT Partners and Mass Medical Society, Leon brings his extensive knowledge in the Apple arena to the New England area.



Managing Security with the Growing Threat of Malware

You installed what?!



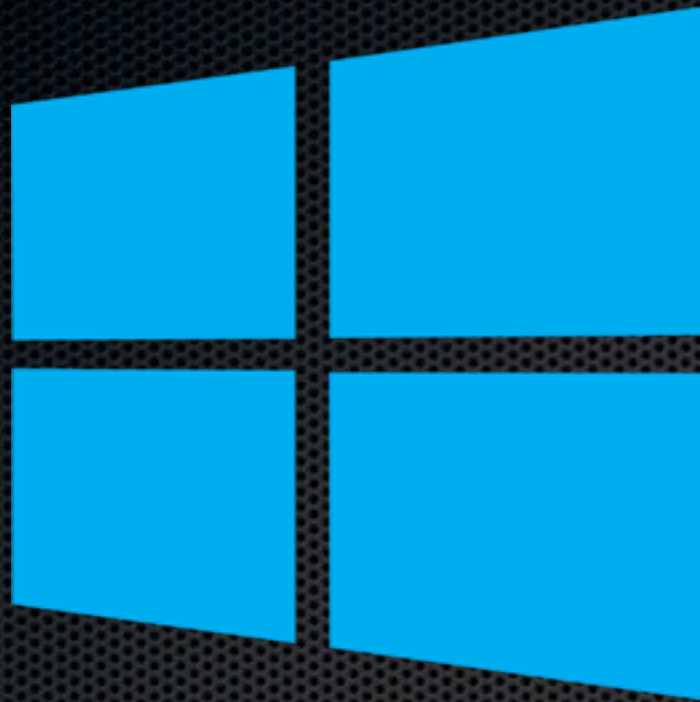
Don't open attachments or click links in emails from unknown or untrusted senders.

Never install dubious software and keep your malware prevention up to date.

Malware: What's the difference?

- Virus
- Adware
- Trojan
- Ransomware
- Windows Viruses

Not Immune



4. .NET Framework Escalation of Privilege Vulnerability (MS15-092)

Custom-crafted .NET applications can cause escalation of privilege exploits to occur. However, users must be first convinced/tricked into running said applications. More information and patch instructions are available on this item's [security bulleting page](#).

3. Microsoft Font Driver Vulnerability (MS15-078)

Windows Adobe Type Manager improperly handles specially-crafted OpenType fonts, which



USN-2989-1: Linux kernel vulnerabilities - 1st June 2016

Justin Yackoski discovered that the Atheros L2 Ethernet Driver in the Linux kernel incorrectly enables scatter/gather I/O. A remote attacker could use this to obtain potentially sensitive information from kernel memory. (CVE-2016-2117) Jason A. Donenfeld discovered multiple out-of-bounds reads in the OZMO USB over wifi device drivers in the Linux ...

CVE-2015-4004 CVE-2016-2069 CVE-2016-2117 CVE-2016-2187
CVE-2016-3672 CVE-2016-3951 CVE-2016-3955 CVE-2016-4485

CVE-2016-3672 CVE-2016-3951 CVE-2016-3955 CVE-2016-4485
CVE-2016-4004 CVE-2016-5066 CVE-2016-5113 CVE-2016-5183

Also Not Immune

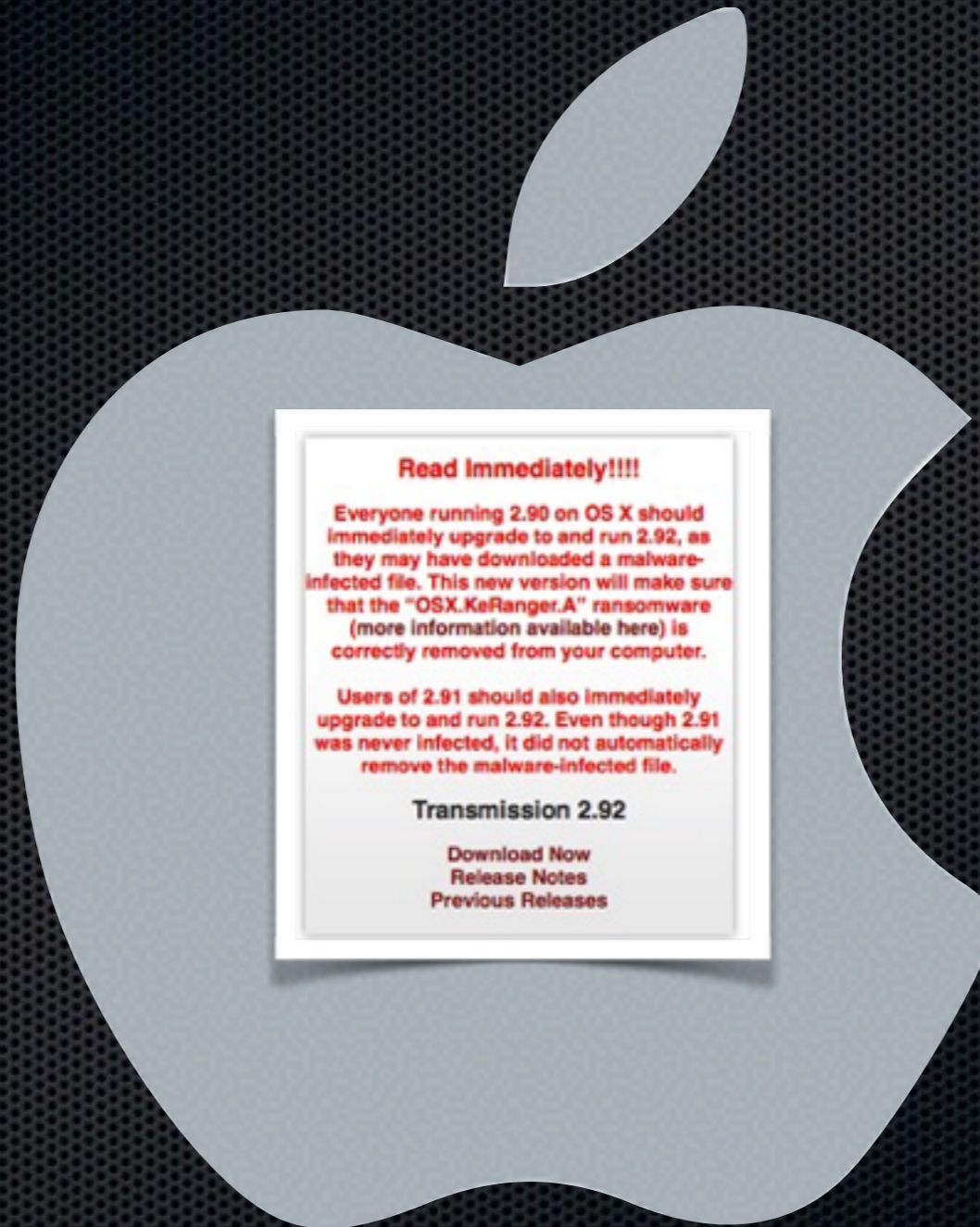


Tethering Controller			
Remote Code Execution in Bluetooth		High	Yes
Elevation of Privilege in Binder	CVE-2016-2440	High	Yes
Elevation of Privilege Vulnerability in Qualcomm Buspm Driver	CVE-2016-2441 CVE-2016-2442	High	Yes
Elevation of Privilege Vulnerability in Qualcomm MDP Driver	CVE-2016-2443	High	Yes
Elevation of Privilege Vulnerability in Qualcomm Wi-Fi Driver	CVE-2015-0571	High	Yes
Elevation of Privilege Vulnerability in NVIDIA Video Driver	CVE-2016-2444 CVE-2016-2445	High	Yes
Elevation of Privilege Vulnerability in NVIDIA Video Driver	CVE-2016-2444 CVE-2016-2445	High	Yes
QUAKE			
Elevation of Privilege Vulnerability in Qualcomm Wi-Fi Driver	CVE-2015-0571	High	Yes



13 CVE-2016-1852 200	WebKit, as used in Apple iOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via crafted web site. CVE-2016-1857.	2016-05-20	2016-05-23	6.8
14 CVE-2016-1852 200		2016-05-20	2016-05-23	2.1
15 CVE-2016-1849 200	+Info	2016-05-20	2016-05-23	2.1
16 CVE-2016-1847 119	DoS Exec Code Overflow Mem. Corr.	2016-05-20	2016-05-23	6.8
17 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
18 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
19 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
20 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
21 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
22 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
23 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
24 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
25 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
26 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
27 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
28 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
29 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0
30 CVE-2016-1842 284	+Info	2016-05-20	2016-05-20	5.0

NOT Immune



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.

We continue till our request be met.

We've obtained all your internal data including your secrets and top secrets.

If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the **24th, 11:00 PM(GMT)**.

Data Link :

<https://www.sony.com/...ata.zip>

<http://d...ata.zip>

<http://www.ntc...SPEData.zip>

<http://www.th...Data.zip>

<http://moodle.u...ch.com.br/SPEDData.zip>

What Can I Do?

- User Education – Practical Security Mindset
- Update Everything
- Protection
- Response
- Backups – Redundant & Offline

Practical Security

- Security can be seen as “sacrificing convenience for safety.” Practical security is finding the right balance between convenience and safety.
- There is no single set of rules that are right for every situation.
- Balance your customers needs and wants with acceptable risk and security.
- Sometimes you have to tell them no.


“Easy” Network Security

- Firewalls
 - The first line of defense
- VPN
 - A secure tunnel through the wall
- Simple solution: OS X Server
 - Offers a full suite of “edge” tools
 - Can be combined with a edge appliance to create a DMZ.

Email Continuity, Spam and Virus filtering

- MXLogic (EOL)
- Proofpoint
- SpamSoap (now Nuvotera)
- MimeCast
- Network appliances (Barracuda's ESS)

Managing Endpoints

- Control Spectrum – Users  Administrators
 - Hands-off
 - Shared
 - Locked Down
- Endpoint/Data Protection
 - Policies
 - Network Access Controls (NAC)
 - Multi-Factor Authentication (MFA)
 - Central Management/Reporting

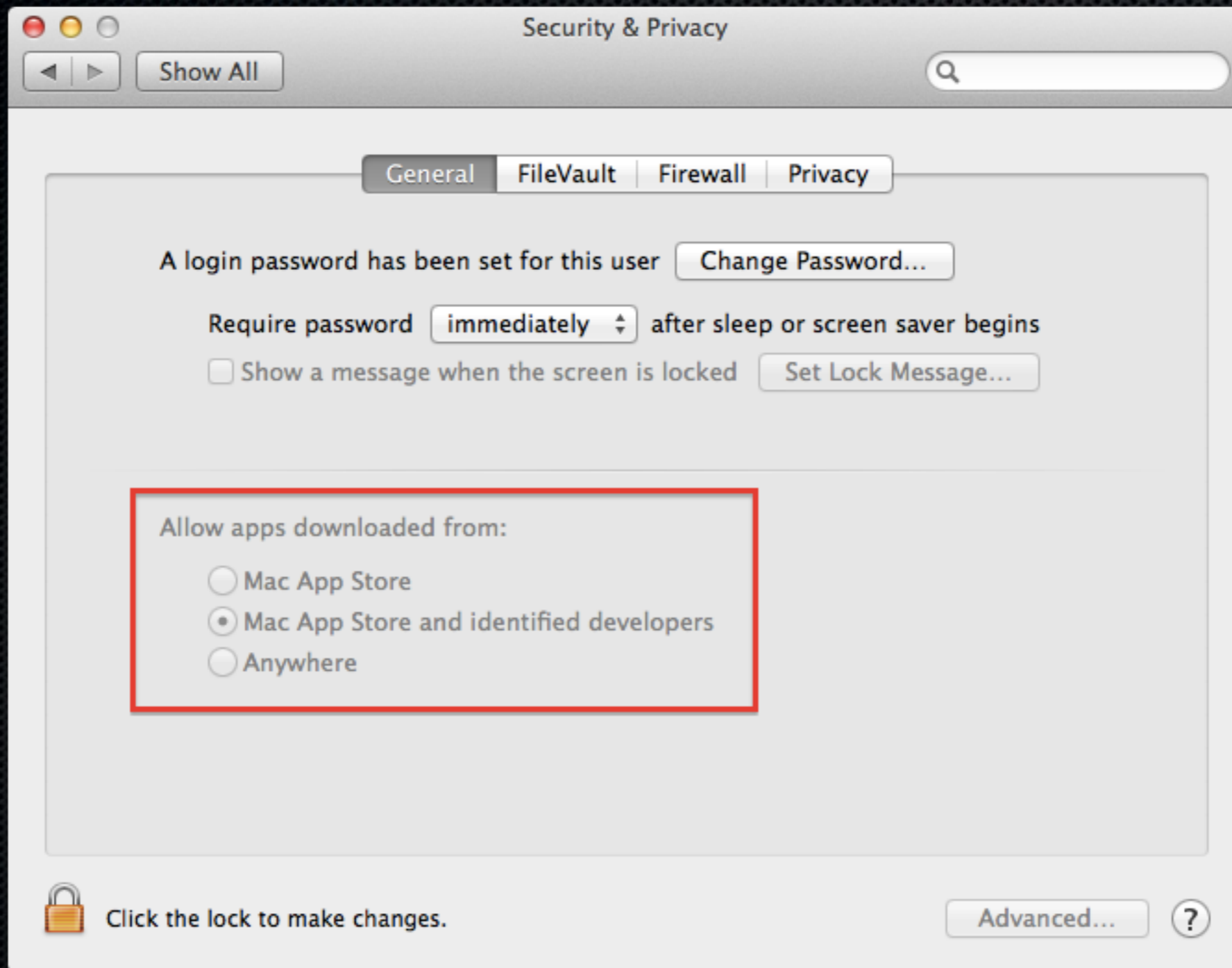
Endpoint Security

- OS X
 - Gatekeeper
 - FileVault
 - Firewall
 - Passwords
 - AdBlockers and AntiVirus
- iOS
 - Passcode
 - VPN

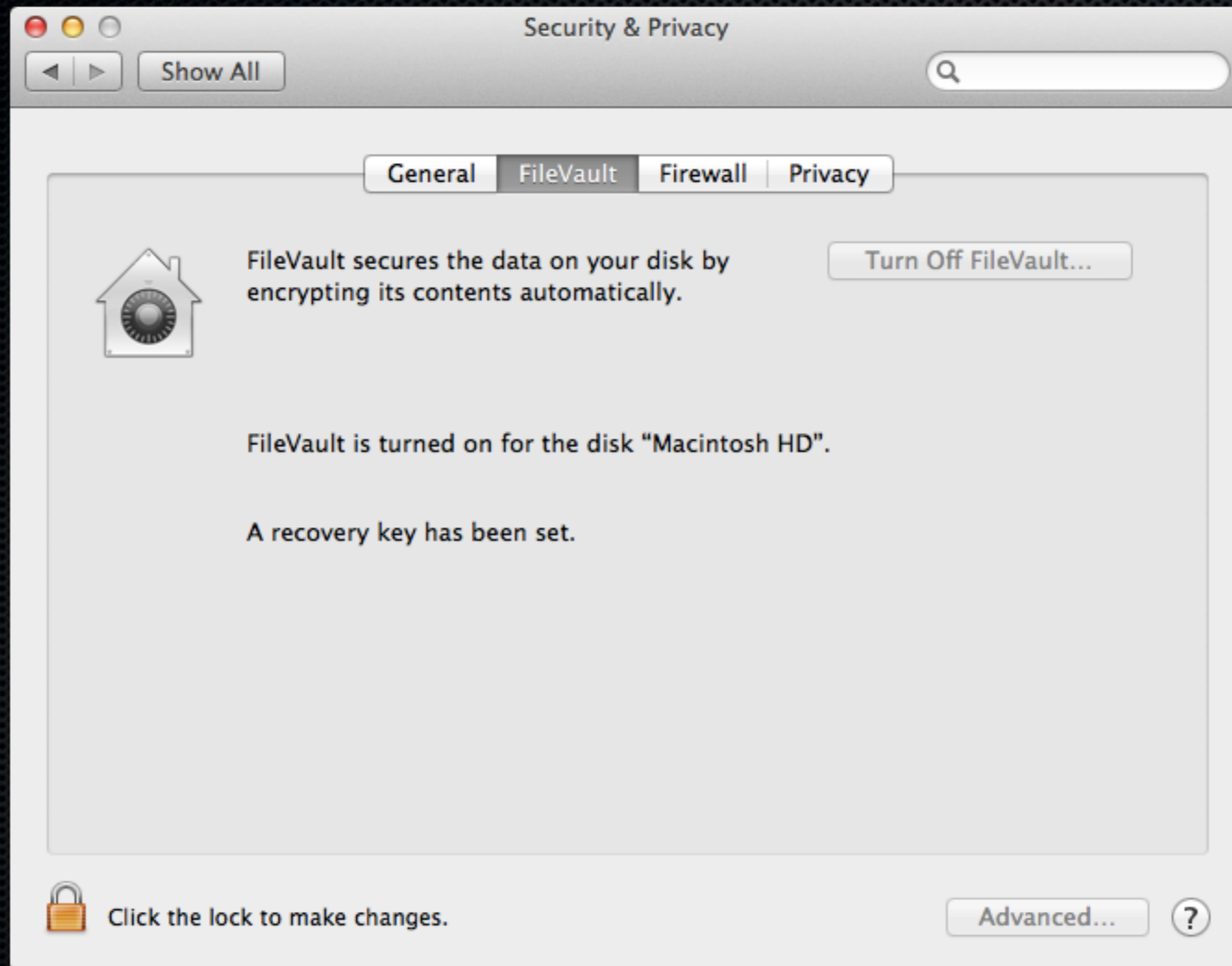
Basic OS X Hardening



Basic OS X Hardening



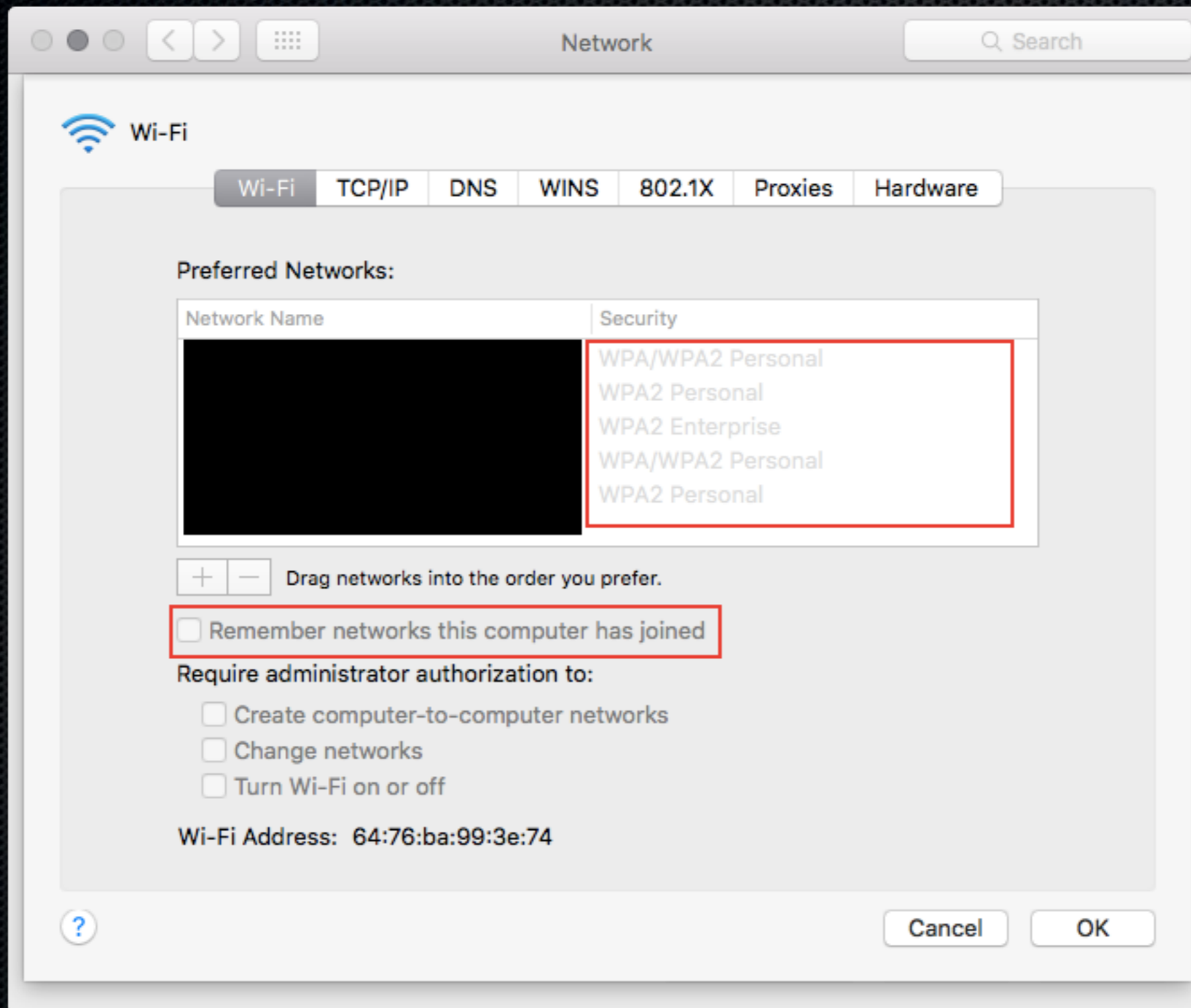
Basic OS X Hardening



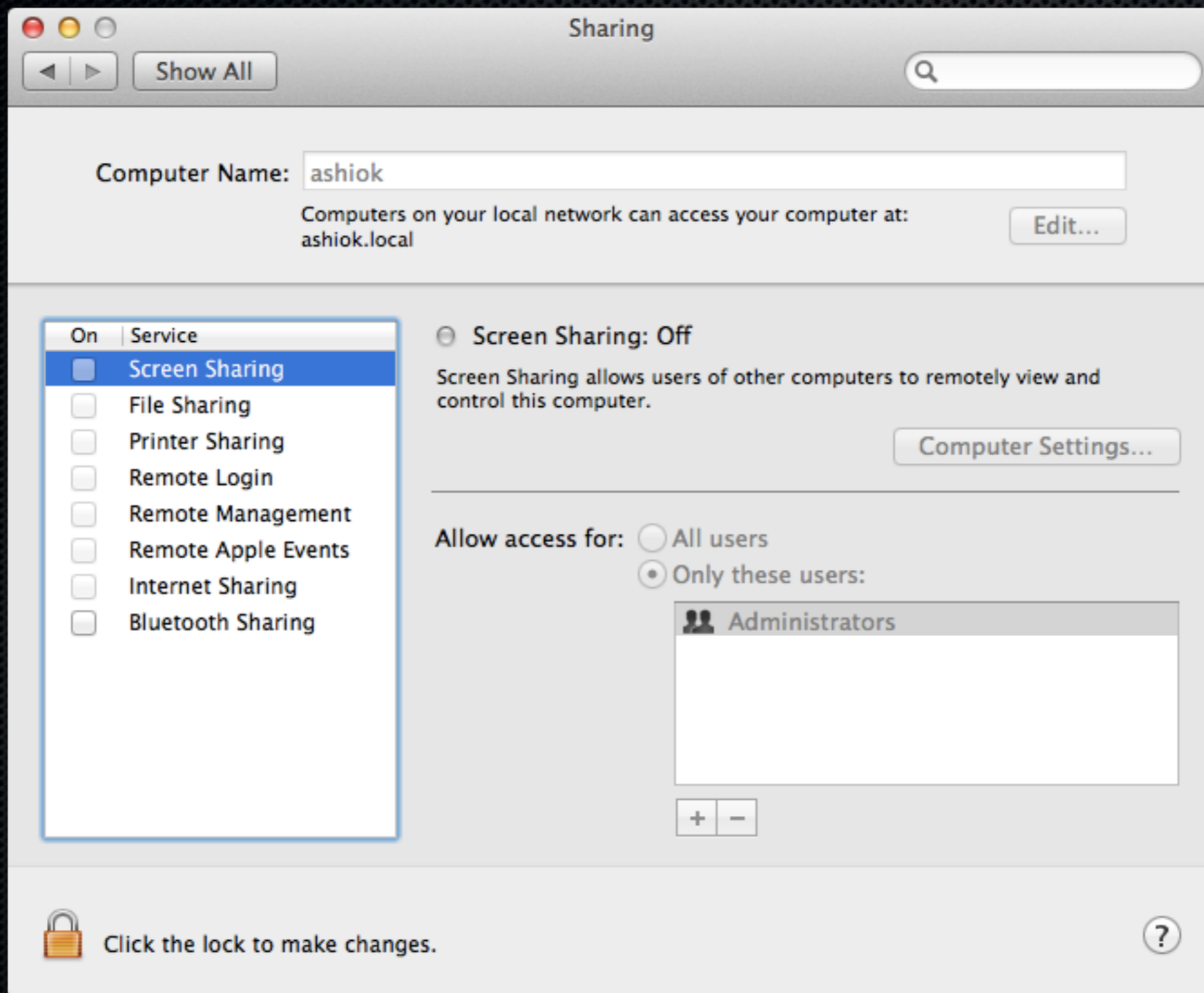
Basic OS X Hardening



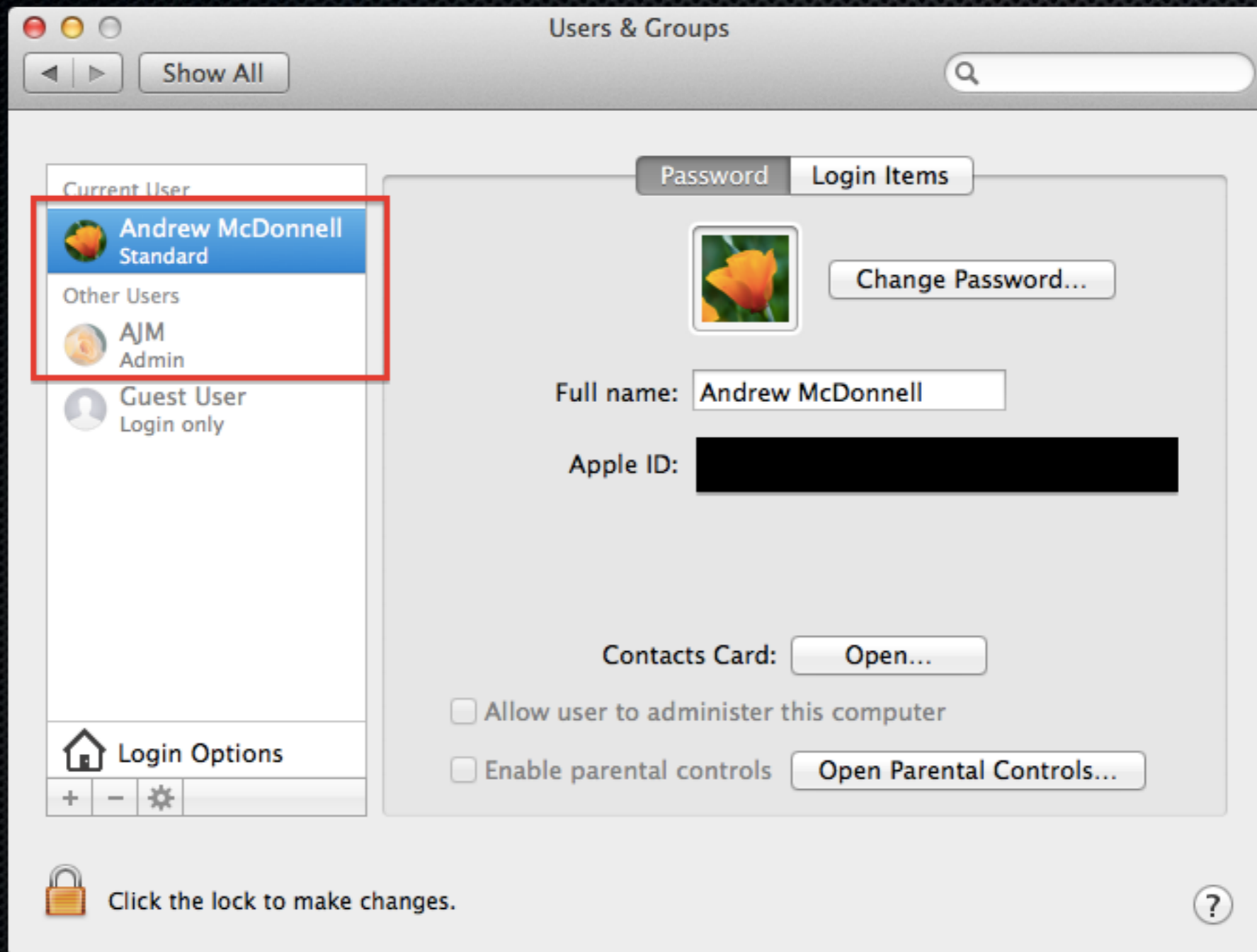
Basic OS X Hardening



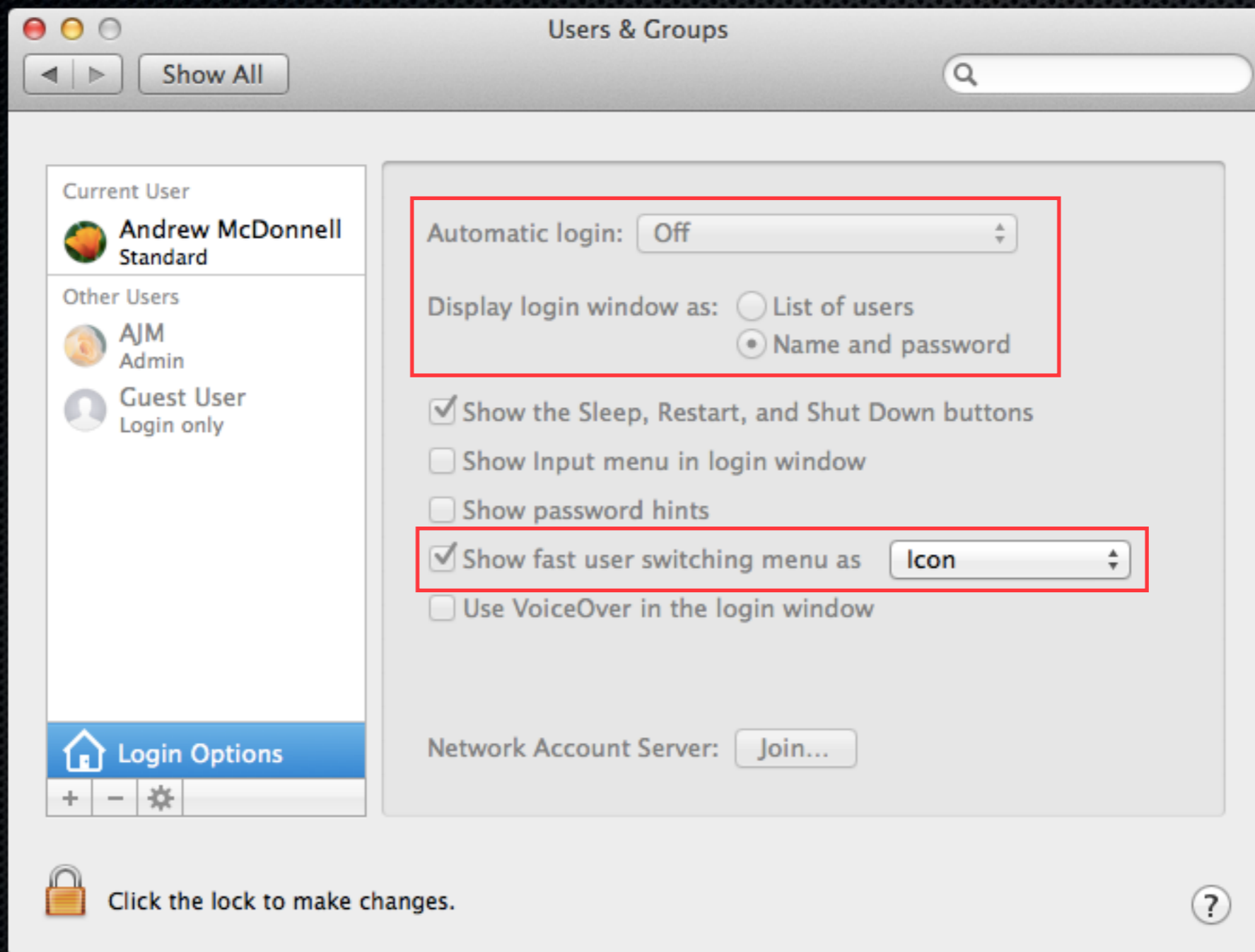
Basic OS X Hardening



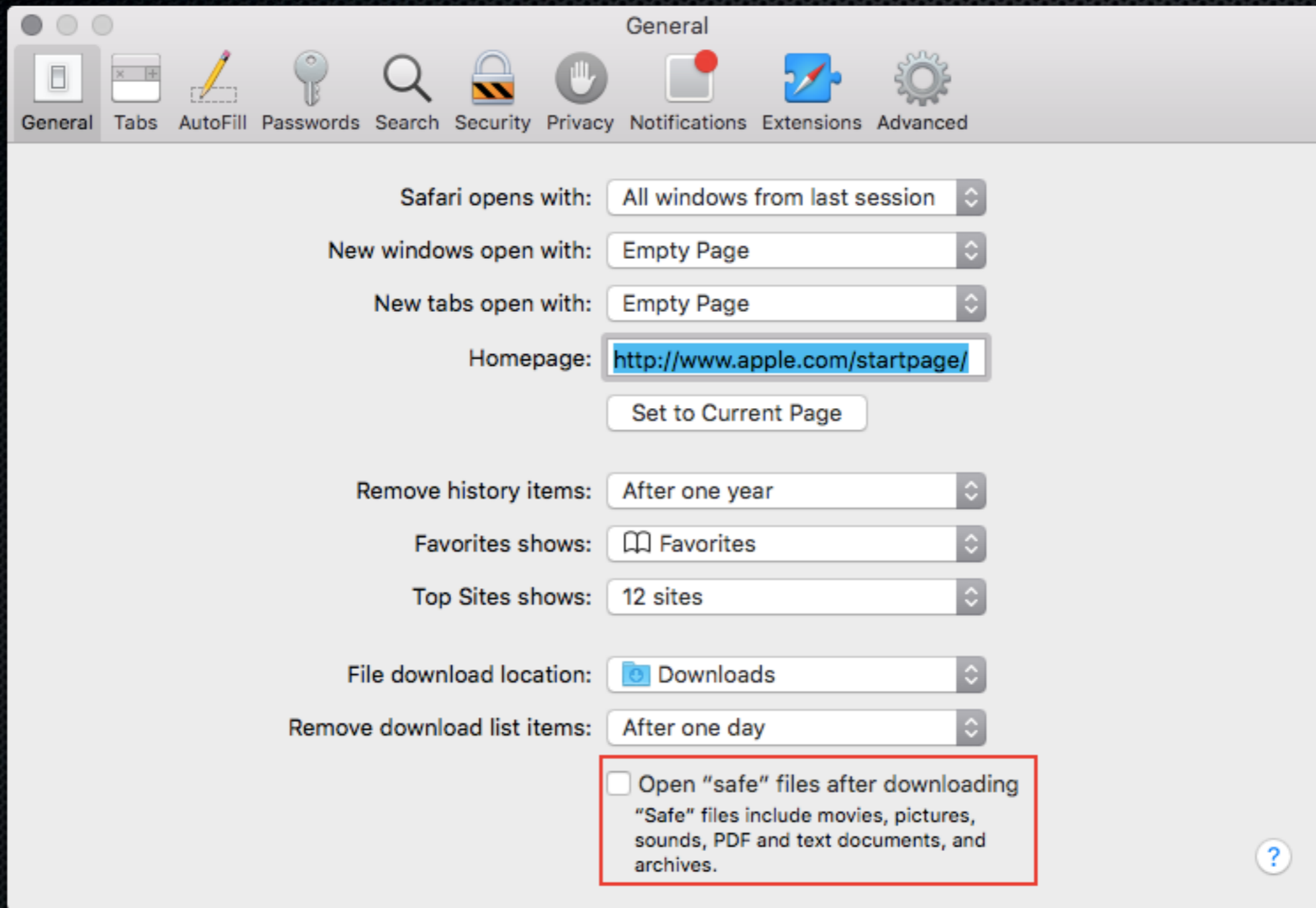
Basic OS X Hardening



Basic OS X Hardening



Basic OS X Hardening



Get These...



Get Rid of These (if you can)



Endpoint Protection Tools

- Active vs. Passive – Performance
- Avira Free Mac Security
- Bitdefender Antivirus
- Avast Free
- Kaspersky
- Sophos
- ClamXav

Next-Generation EPT

- Signature-based AntiVirus is the “old” way
- Advanced Threat Protection (ATP)
 - Extremely lightweight clients
 - Monitors system activity rather than signatures or hashes
 - Behavioral protection
 - Cloud-based “big data” analysis

iOS Security

- Built in hardware encryption
- Complex passcode + Touch ID
- Secure, sandboxed application environment
- Don't get complacent!
- Don't Jailbreak.
- Don't install 3PP App Stores.

Impostors

- Genieo / InstallMac
- MacProtector
- MacKeeper
- Avoid good software from bad sources

More Resources

- csrc.nist.gov
- thesafemac.com
- www.us-cert.gov
- cve.mitre.org
- schneier.com
- arstechnica.com/apple
- krebsonsecurity.com
- astechconsulting.com/blog/

Questions?



@llincoln3

llincoln@broadinstitute.org