



ERNW
providing security.

OS X Hardening

Mountain Lion 10.8

Version:	1.00
Date:	8/2/2013
Classification:	Public
Author(s):	Florian Grunow, Matthias Luft, Michael Thumann, Michael Schaefer

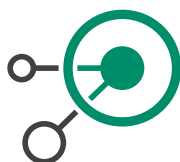
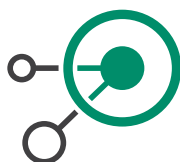


TABLE OF CONTENT

1	INTRODUCTION	4
2	AUTHENTICATION	5
2.1	DISABLE AUTO-LOGIN	5
2.2	ENABLE SINGLE USER MODE AUTHENTICATION	5
2.3	REQUIRE USERNAME AND PASSWORD FOR LOGIN.....	5
2.4	DISABLE PASSWORD HINTS.....	5
2.5	SET SCREENSAVER INACTIVITY INTERVAL	5
2.6	REQUIRE PASSWORD TO UNLOCK SCREENSAVER.....	5
2.7	RESTRICT <code>sudo</code> CONFIGURATION	6
2.8	DISABLE UNAUTHORIZED ADMINISTRATIVE ACCESS FOR SESSIONS LOCKED THROUGH SCREENSAVER	6
3	SYSTEM SECURITY	7
3.1	AUTOMATICALLY LOCK LOGIN KEYCHAIN.....	7
3.2	CHANGE INITIAL PASSWORD FOR LOGIN KEYCHAIN	7
3.3	ENABLE AUTOMATIC UPDATES.....	7
3.4	DISABLE GUEST ACCESS.....	7
3.5	ENABLE GATEKEEPER	7
3.6	SET EFI PASSWORD.....	8
3.7	DISABLE CORE DUMPS	8
3.8	PREVENT SAFARI FROM OPENING KNOWN FILE TYPES	8
3.9	SET STRICT GLOBAL UMASK	8
3.10	SET STRICT HOME DIRECTORY PERMISSIONS.....	8
3.11	ENABLE SECURE ERASE OF DELETED FILES IN TRASH.....	8
3.12	IMPLEMENT HARD DISK ENCRYPTION.....	9
4	NETWORK SECURITY	10
4.1	DISABLE APPLE FILE PROTOCOL (AFP).....	10
4.2	DISABLE FILE TRANSFER PROTOCOL (FTP) DAEMON	10
4.3	DISABLE FILE SHARING	10
4.4	DISABLE PRINTER SHARING	10
4.5	DISABLE ADDITIONAL AND UNNECESSARY SERVICES.....	10

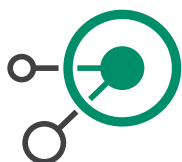


4.6	SET HARDENED TCP/IP KERNEL PARAMETERS	11
4.7	ENABLE NETWORK TIME SYNCHRONIZATION VIA NTP	11
4.8	DISABLE BLUETOOTH	11
4.9	DISABLE LOCATION SERVICES	11
4.10	ENABLE FIREWALL	11
4.11	DISABLE WAKE-ON-LAN.....	12
4.12	LIMIT IPV6 TO LOCAL SUBNET/DISABLE IPV6	12
5	LOGGING & MONITORING	13
5.1	ENABLE BSM AUDIT.....	13
6	APENDIX: LIST OF SERVICES.....	14

1 INTRODUCTION

As no official hardening guide for Apple's OS X Mountain Lion is available yet, ERNW has compiled the most relevant settings into this checklist. While there is a significant amount of controls that can be applied, this document is supposed to provide a solid base of hardening measures. Settings which might have severe impact on the functionality of the operating system and need a lot of further testing are not part of this checklist.

We have marked each recommended setting in this checklist either with "mandatory" or "optional" to make a clear statement, which setting is a MUST (mandatory) or a SHOULD (optional) from our point of view. "Optional" also means that we recommend to apply this setting, but there may be required functionality on the system that will become unavailable once the setting is applied.




2 AUTHENTICATION

2.1 Disable Auto-login

- Go to *Security and Privacy* settings in the *System Preferences* menu
- Check *Disable automatic login*

Mandatory

2.2 Enable Single User Mode Authentication

- Change *secure* to *insecure* in `/etc/ttytys`
-  If the root account is disabled, booting into single user mode is not possible.

Optional

2.3 Require Username *and* Password for Login

- Go to *Users & Groups* settings in the *System Preferences* menu.
- At *Display login window as* select *Name and password*.

Mandatory


2.4 Disable Password Hints

- Go to *Users & Groups* settings in the *System Preferences* menu.
- Choose *Login options*.
- Uncheck *Show password hints*.

Mandatory

2.5 Set Screensaver Inactivity Interval

- Set the inactivity interval to 5min.

 `defaults -currentHost write com.apple.screensaver idleTime -int 300`

Mandatory

2.6 Require Password to Unlock Screensaver

- Go to *Security & Privacy* settings in the *System Preferences* menu.
- Choose tab *General*.
- Check *Require password [...] after sleep or screen saver begins*.
- Set duration to *immediately*.

Mandatory

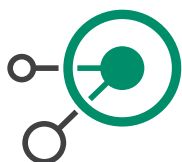
2.7 Restrict sudo Configuration

<ul style="list-style-type: none"> • Open the sudo configuration file: <pre>sudo visudo</pre> • Restrict sudo usage to one single command and to the authenticated terminal only: <pre>Defaults timestamp timeout=0 Defaults tty_tickets¹</pre> 	Mandatory
--	------------------

2.8 Disable Unauthorized Administrative Access for Sessions Locked Through Screensaver

<ul style="list-style-type: none"> • In <code>/etc/authorization</code> edit the section <code>system.login.screensaver</code> as follows: <pre><key>system.login.screensaver</key> <dict> <key>class</key> <string>rule</string> <key>comment</key> <string>The owner can unlock the screensaver.</string> <key>rule</key> <string>authenticate-session-owner-or-group</string> Go to the rules section and add the following element: <key>authenticate-session-owner-or-group</key> <dict> <key>allow-root</key> <false/> <key>class</key> <string>user</string> <key>comment</key> <string><i>your comment</i></string> <key>group</key> <string>MAC-ADMIN-GROUP</string> <key>session-owner</key> <true/> <key>shared</key> <false/> </dict></pre> 	Mandatory
--	------------------

¹ In combination with the previous line, this option does not have any effect, yet we recommended it in case `timestamp_timeout` will be changed.



3 SYSTEM SECURITY

3.1 Automatically Lock Login Keychain

- Open *Keychain Acces* and select the *login* keychain.
- Choose *Edit* → *Change Settings for Keychain* "login".
- Set *Lock after [...] minutes of inactivity* to 10.
- Check *Lock when sleeping*.

Mandatory

3.2 Change Initial Password for Login Keychain

- Open *Keychain Acces* and select the *login* keychain.
- Choose *Edit* → *Change Password for Keychain* "login".
- Set a new password different to the login password.

Mandatory

3.3 Enable Automatic Updates

- Go to *App Store* settings in the *System Preferences* menu.
- Check *Automatically check for updates*.
- Check *Download newly available updates in the background*.
- Check *Install app updates*.
- Check *Install system data files and security updates*.²

Mandatory

3.4 Disable Guest Access

- Go to *Users & Groups* settings in the *System Preferences* menu.
- Choose the *Guest User*.
- Uncheck *Allow guests to login into this computer*.

Mandatory

3.5 Enable Gatekeeper

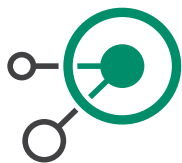
- Go to *System Preferences* → *Security & Privacy*.
- Choose tab *General*.
- Set *Allow applications downloaded from* to *Mac App Store and identified Developers*.



This will prevent unsigned application bundles from being executed. This does not cover applications/binaries that are not bundles. Unsigned application bundles from trusted sources can be executed by performing a right-click on the application bundle, choose *Open*, and confirm the warning dialog with *Open*. An exception for this bundle will be generated automatically.

Optional

² This setting only enables automatic updates for the system and system software. Updates for 3rd party software must be installed manually/in another way.



3.6 Set EFI Password

Prevent unauthorized access to the EFI of the system by setting a firmware password.

- Use the Firmware Password Utility to set a firmware password.



This will require the password to be entered when booting into Single User, Verbose or Target Disk mode as well as booting into the recovery mode (command-r).

Mandatory

3.7 Disable Core Dumps



```
launchctl limit core 0
```

Optional

3.8 Prevent Safari from Opening Known File Types

- Launch the *Safari* browser application.
- Choose *Preferences*.
- Choose tab *General*.
- Uncheck *Open safe files after downloading*.

Mandatory

3.9 Set Strict Global umask



```
sudo echo "umask 027" >> /etc/launchd.conf
```



This might break the installation of additional software that relies on a less strict umask.

Optional

3.10 Set Strict Home Directory Permissions



```
sudo chmod 700 /Users/<username>
```

Optional

3.11 Enable Secure Erase of Deleted Files in Trash

- Launch the *Finder* application.
- Choose *Preferences*.
- Click *Advanced...*
- Check *Empty Trash securely*.

Mandatory



3.12 Implement Hard Disk Encryption

- Launch the *System preferences* application.
- Choose *Security & Privacy*.
- Click *FileVault...*
- Turn FileVault on.

Optional





4 NETWORK SECURITY

4.1 Disable Apple File Protocol (AFP)

- Go to *System Preferences* → *Sharing*.
- Select *File Sharing*.
- Click *Options*.
- Uncheck *Share files and folders using AFP*.


- Alternatively AFP can be disabled using the command line interface:


```
 sudo launchctl unload -w /System/Library/LaunchDaemons/AppleFileServer.plist
```

 Disabled per default on OS X 10.8.

Optional

4.2 Disable File Transfer Protocol (FTP) daemon

```
 sudo launchctl unload -w /System/Library/LaunchDaemons/ftp.plist
```

 Disabled per default on OS X 10.8.

Optional


4.3 Disable File Sharing

- Go to *System Preferences* → *Sharing*.
- Uncheck *File Sharing*.

Optional

4.4 Disable Printer Sharing


- Go to *System Preferences* → *Sharing*.
- Uncheck *Printer Sharing*.

 Disabled per default on OS X 10.8.


Optional

4.5 Disable Additional and Unnecessary Services

- Disable services which are not needed or required by other applications/services.

```
 sudo launchctl unload -w <FullPathToPlistFile>
```

- Servicefiles (Plistfiles) are located in
 - /System/Library/LaunchDaemons
 - /System/Library/LaunchAgents
 - /Library/LaunchDaemons
 - /Library/LaunchAgents
 - /Users/USERNAME/Library/LaunchDaemons
 - /Users/USERNAME/Library/LaunchAgents

 Before disabling a service it must be ensured that its functionality is not required by other software components or services.

Mandatory



4.6 Set Hardened TCP/IP Kernel Parameters

- Set kernel parameters in `/etc/sysctl.conf`:
 - `net.inet.ip.fw.verbose = 1`
 - `net.inet.ip.fw.verbose_limit = 65535`
 - `net.inet.icmp.icmplim = 1024`
 - `net.inet.icmp.drop_redirect = 1`
 - `net.inet.icmp.log_redirect = 1`
 - `net.inet.ip.redirect = 0`
 - `net.inet.ip.sourceroute = 0`
 - `net.inet.ip.accept_sourceroute = 0`
 - `net.inet.icmp.bmcastecho = 0`
 - `net.inet.icmp.maskrepl = 0`
 - `net.inet.tcp.delayed_ack = 0`
 - `net.inet.ip.forwarding = 0`
 - `net.inet.tcp.strict_rfc1948 = 1`

The system must be restarted before these changes become active.

Mandatory

4.7 Enable Network Time Synchronization via NTP

- Edit `/private/etc/hostconfig` and change `TIMESYNC` to `YES`.
- Configure the desired NTP server in `/private/etc/ntp.conf` through a corresponding server entry.
- Restart the NTP daemon.



```
sudo launchctl load -w /System/Library/LaunchDaemons/org.ntpd.ntpd.plist
```

Mandatory

4.8 Disable Bluetooth

- Disable Bluetooth in *System Preferences* → *Bluetooth*.

Optional

4.9 Disable Location Services

- Go to *System Preferences* → *Security & Privacy*.
- Choose tab *Privacy*.
- Uncheck *Enable Location Services* or uncheck applications which should NOT be able to access location services.

Mandatory

4.10 Enable Firewall

- Go to *System Preferences* → *Security & Privacy*.
- Choose tab *Firewall*.
- Click *Turn On Firewall*.
- Click *Firewall Options...*
- Check *Block all incoming connections*.
- Check *Automatically allow signed software to receive incoming connections* only, if you're not familiar with firewall configurations and you want to make sure, that all functionality will be available.
- Check *Enable stealth mode*.

Mandatory



4.11 Disable Wake-on-LAN

- Go to *System Preferences* → *Energy Saver*
- Choose tab *Options*
- Uncheck *Wake for network access*.

Mandatory

4.12 Limit IPv6 to Local Subnet/Disable IPv6³

- Go to *System Preferences* → *Network*.
- For all relevant interfaces click *Advanced...*
- For *Configure IPv6* select *Link-local only*.

This will ensure that IPv6 is only used in the local subnet. If you would like to disable IPv6 completely, enter the following commands:

- To list all network devices: `networksetup -listallnetworkservices`.
- To disable IPv6 on a specific network device: `networksetup -setv6off Wi-Fi`

Optional

³ While IPv6 is not in use in many environments yet, we basically recommend to gather operational and security requirements for future deployments:
<http://blog.ipSPACE.net/2013/05/the-dangers-of-ignoring-ipv6.html>


5 LOGGING & MONITORING


5.1 Enable BSM Audit

- Edit `/etc/security/audit_control` and include the following lines:

```
dir:/var/audit
flags:all
minfree:5
naflags:lo,aa,pc,nt
policy:cnt,argv
filesz:1G
expire-after:5G
superuser-set-sflags-mask:has_authenticated,has_console_access
superuser-clear-sflags-mask:has_authenticated,has_console_access
member-set-sflags-mask:
member-clear-sflags-mask:has_authenticated
```

- Start a new audit trail using the adjusted configuration:

```
 sudo audit -n
```

 As only new processes will be audited, the system must be restarted.

Optional

6 APENDIX: LIST OF SERVICES

The following table lists service files and the corresponding functionality that should be disabled/must not be enabled unless required.

Filename	Functionality
com.apple.AppleFileServer.plist	AFP
ftp.plist	FTP
smbd.plist	SMB
org.apache.httpd.plist	HTTP Server
eppc.plist	Remote Apple Events
com.apple.xgridagentd.plist	Xgrid
com.apple.xgridcontrollerd.plist	Xgrid
com.apple.InternetSharing.plist	Internet Sharing
com.apple.dashboard.advisory.fetch.plist	Dashboard Auto-Update
com.apple.UserNotificationCenter.plist	User notifications
com.apple.RemoteDesktop.PrivilegeProxy.plist	ARD
com.apple.RemoteDesktop.plist	ARD
com.apple.IIDCAssistant.plist	iSight
com.apple.blued.plist	Bluetooth
com.apple.RemoteUI.plist	Remote Control