Guidance

End User Devices Security Guidance: Apple OS X 10.11

Published

Contents

This guidance is applicable to all Apple devices running OS X 10.11. This guidance was developed following testing performed on MacBook Pro and MacBook Air devices running OS X 10.11.0.

1. Changes since previous guidance

This document is an update of the previous OS X 10.10 guidance. Changes to the attached configuration script and VPN profiles have been made, and an assessment of the new System Integrity Protection (rootless) feature has been performed.

2. Usage scenario

OS X devices will be used remotely over Ethernet and Wi-Fi networks to connect back to the enterprise over a VPN. This enables a variety of remote working approaches such as:

- accessing OFFICIAL email
- creating, editing, reviewing and commenting on OFFICIAL documents
- accessing OFFICIAL intranet resources, the Internet and other web resources

To support these scenarios, the following architectural choices are recommended:

- All data should be routed over a secure enterprise VPN to ensure the confidentiality and integrity of the traffic, and to benefit from enterprise protective monitoring solutions.
- User accounts should be created locally on the OS X devices and managed remotely using Mobile Device Management (MDM).
- Arbitrary third-party application installation by users should not be permitted on the device. Applications which users require should be pre-installed before users are assigned devices, be provisioned as part of the device image, or installed using MDM.

3. Summary of platform security

This platform has been assessed against each of the 12 security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the platform can best satisfy the security recommendations for more details about how each of the security recommendations is met.

Recommendation	Rationale
1. Assured data-in-transit protection	Whilst the native VPN has not been independently assured to Foundation Grade, third-party VPNs which have are available. Assured products should be used in preference to unassured products.
2. Assured data-at-rest protection	FileVault 2 has not been independently assured to Foundation Grade.
3. Authentication	
4. Secure boot	Secure boot is not supported on this platform.
5. Platform integrity and application sandboxing	
6. Application whitelisting	
7. Malicious code detection and prevention	
8. Security policy enforcement	
9. External interface protection	
10. Device update policy	The enterprise cannot force the user to update their device or software remotely, however, it is possible to turn on automatic updates locally. Third-party utilities may mitigate this issue.

3.1 Significant risks

The following key risks should be read and understood before the platform is deployed.

- The FileVault 2 full-volume encryption product has not been independently assured to Foundation Grade, and does not support some of the mandatory requirements expected from assured full-disk encryption products. Without assurance in FileVault 2 there is a risk that data stored on the device could be compromised.
- FileVault 2 does not use any dedicated hardware to protect its keys. If an attacker can get physical access to the device, they can extract password hashes and perform an offline brute-force attack to recover the encryption password.
- Most OS X devices have external interfaces which permit Direct Memory Access (DMA) from connected peripherals. Whilst the configuration in this section limits DMA to times when the user is logged in and the screen is unlocked, this still presents an opportunity for a local attacker to extract keys and data.

4. How the platform can best satisfy the security recommendations

This section details the platform security mechanisms which best address each of the security recommendations.

4.1 Assured data-in-transit protection

Use a Foundation Grade IPsec VPN client configured as per that product's security procedures to provide data-in-transit protection.

4.2 Assured data-at-rest protection

Use FileVault 2 to provide full-volume encryption. CESG recommends the use of a complex password of at least 9 characters in length, or of at least 6 characters in length when used in conjunction with a second factor.

4.3 Authentication

The user implicitly authenticates to the device by decrypting the disk at boot time.

The user then has a secondary password to authenticate themselves to the device at boot and unlock time. This password also derives a key which encrypts certificates and other credentials, giving access to enterprise services.

4.4 Secure boot

An EFI (firmware) password can make it more difficult for an attacker to modify the boot process. With physical access, the boot process can still be compromised.

4.5 System Integrity Protection

OS X 10.11 introduces a new security policy which extends protection to critical system components, both on disk and at run time.

The new policy prevents users (including root and sudo users) and applications from modifying files in several high-level directories. This feature is enabled by default in the OS and no user configuration is required.

4.6 Platform integrity and application sandboxing

These requirements are met implicitly by the platform. Sandbox profiles limit access to the platform from App Store applications. It is recommended other applications are configured to use the Sandbox features where possible.

4.7 Application whitelisting

The MDM can be used to whitelist default OS X applications. Installation and running of unsigned applications can be prevented with GateKeeper.

4.8 Malicious code detection and prevention

XProtect is built into OS X and has a limited signature set which is maintained by Apple to detect widespread malware. XProtect will also restrict vulnerable plugin versions (such as Java) to limit exposure. Several third-party anti-malware products also exist which attempt to detect malicious code for this platform. An enterprise application catalogue can be used which should only contain vetted apps. Content-based attacks can be filtered by scanning capabilities in the enterprise.

4.9 Security policy enforcement

MDM profiles can be marked as non-removable so the user cannot remove them and alter the configuration.

4.10 External interface protection

USB removable media can be blocked through MDM if required. If an EFI password is set, DMA is only possible when the device is booted and unlocked. Kernel Modules for other interfaces (eg Firewire) can be removed if required, but will be re-installed during OS updates.

4.11 Device update policy

MDM can be used to audit which App Store software and OS versions are installed on a device. The attached script will turn on automatic updates, but this cannot be achieved remotely with MDM.

4.12 Event collection for enterprise analysis

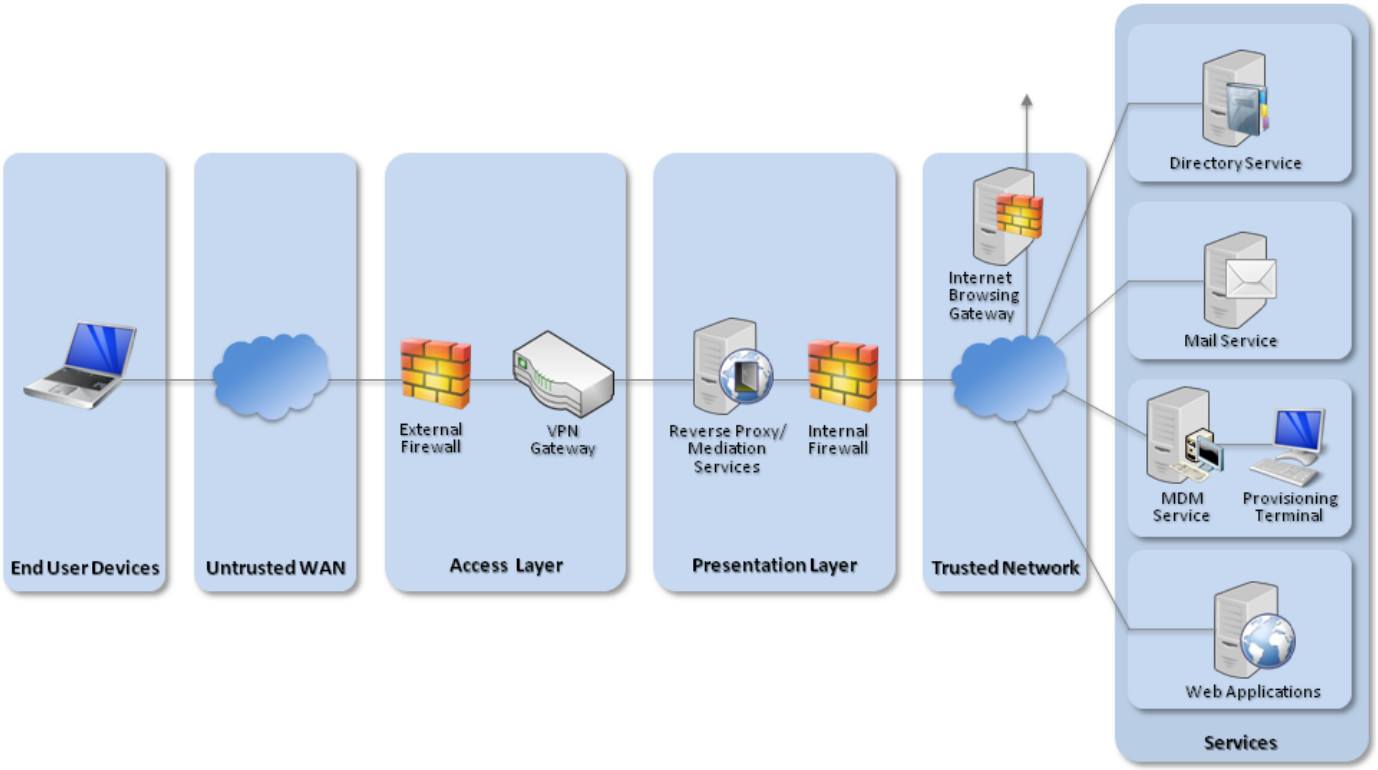
OS X logs can be viewed by a local administrator on device, or viewed remotely using remote administration tools. Third-party software can also be used to automate log collection.

4.13 Incident response

OS X devices can be locked, wiped, and configured remotely by their MDM.

5. Network architecture

All remote or mobile working scenarios should use a typical remote access architecture based on the Walled Garden Architectural Pattern. The following network diagram describes the recommended architecture for this platform.



Recommended network architecture for deployments of OS X

A Mobile Device Management server is required. Apple's OS X Server Profile Manager is sufficient for this purpose. Alternatively, third-party products exist which may offer additional functionality over and above Profile Manager.

6. Deployment process

The following steps should be followed to prepare the enterprise infrastructure for hosting a deployment of these devices:

- Set up an MDM server (eg Profile Manager on OS X Server). This may require setting up the Open Directory component of an OS X Server.
- Ensure all Configuration Profiles are signed to prevent modification in transit or once they are installed
- Create policies on Profile Manager for:
  - VPN
  - Passcode
  - Exchange/Mail/Calendar Settings.

    - Ensure ‘Use SSL’ is selected for all server settings
- Disabling access to the Preference Panes in Restrictions (OS X) for iCloud and Network as access to these could be used to disable the VPN.

See the Policy Recommendations section for more detail on the above.

You can also consider creating policies in other sections of Profile Manager. In particular, CESG recommend that administrators:

- Whitelist applications to further reduce the risk of malicious code being executed.
- Tighten permissions on USB mass storage and optical devices to help prevent data loss through removable media.
- Use Restrictions to blacklist locations users should not run applications from, or whitelist trusted applications that users are allowed to run.
- Include internal CA Certificates where appropriate to ensure users can authenticate network services
- Include corporate network profiles (eg 802.1X or Wi-Fi) to ensure that network access credentials are distributed securely

7. Provisioning steps

The following steps should be followed to provision each end user device onto the enterprise network to prepare it for distribution to end users.

These instructions assume the device is new or the operating system has been wiped and reinstalled.

- On first boot, the device will present a number of prompts. In these prompts:
    - Firstly, create a local Administrator account. This will be used to locally manage the device and credentials should not be given to the end user. A strong password should be entered at this stage.
    - Secondly, skip the Apple ID creation and entry.
    - Location Services can be enabled if required.
    - The device can be registered with Apple if required.
- Local settings should now be set. A script is provided at the end of this section to automatically provision these settings, but they can also be configured manually.
    - Disable any non-required services (eg IPv6, infrared);
    - Enable low-overhead security features (eg firewall, updates);

- Set user security policies (eg timeouts, screen lock, password hints);
- Create a standard user account;
- Make the user's home folder accessible only to that user;
- Lock down the user's Terminal/Shell access. The user should have a limited Bash profile, which can be set as part of .bash_profile. This file should be owned by the root user so that modifications cannot be made. The user's PATH should be set to a folder in the user's directory and required applications symlinked to this directory.
- Create a Disk Encryption user which will have a strong password that can decrypt the disk. Part of this password could be from a password entry token such as a YubiKey. The Disk Encryption password should be at least 9-characters long, or 6-characters plus a longer fixed string from the Password Entry Token (>16 characters recommended).
    - Alternatively, increase the password complexity of the primary user to >9 characters so that there is only one password required to decrypt and log in. A 6 character password with 16 characters from a password entry token could be used here instead of the 9-character password.
- Enable FileVault 2 and encrypt the disk; only give the Disk Encryption user access to decrypt the disk;
- Turn on automatic updates via System Settings -> App store settings;
- Turn off initial iCloud login prompt for first user login. This will stop the user being prompted to use iCloud;
- Set FileVault 2 to remove the key on sleep, and set the sleep mode to Hibernate;
- To help prevent DMA and cold-boot attacks, set a Firmware Password.

- The device should now be enrolled with the MDM server and the configuration profiles applied.
- At this stage, any additional third-party applications can be installed (eg productivity apps)
- Distribute the device, disk encryption password and user password separately to the user.
- The user should then change their password and skip the Apple ID registration step at the next time they log on.

7.1 Device Imaging

Instead of provisioning each device individually, an alternative option is to produce a master device image which can be deployed onto devices. The recommended approach for creating a standard disk image is to install the OS, create a local admin account and apply local policies, then install any required applications on a client machine.

The client machine is then connected to an imaging server in target disk mode. Apple's System Image Utility can then be used to create a NetRestore or NetBoot image of the device. The image can then be used to provision other machines. NetBoot images can also be created from OS X installers downloaded from Apple, though care should be taken to ensure that the version downloaded can be deployed on the specific hardware to be used.

Note that enabling FileVault 2 and MDM enrolment must only be done after the device has been imaged. This ensures that the cryptographic keys involved in these security features are different.

Apple's website has a support article that contains details about creating images for device-specific versions of OS X. The article can be found at http://support.apple.com/kb/HT5599.

8. Policy recommendations

This section details important security policy settings which are recommended for an OS X deployment. Other settings (eg server address etc.) should be chosen according to the relevant network configuration. These settings should be applied through a profile (or combination of profiles) created on the MDM server.

The settings below are named as they appear in Apple Configurator and Profile Manager. Other products may use different names for these settings.

General Group	
Security (when can profile be removed)	Never
Automatic profile removal	Never
Passcode Group	
Allow simple value	No
Require alpha-numeric value	Yes
Minimum passcode length	7 This is for the login password if using separate passwords for encryption and login. The disk encryption password is managed elsewhere.
Minimum number of complex characters	1
Maximum passcode age	90 (days)
Maximum Auto-Lock	5 (minutes)

Maximum number of failed attempts	5
Mail/Exchange/Calendar Groups (as appropriate)	
Allow messages to be moved	No
Use Only in Mail	Yes
Use SSL (for internal and external host)	Yes
VPN Group	
Connection Type	IPsec (Cisco)
Machine Authentication	Certificate
Enable VPN on Demand	Yes
Security & Privacy Group	
Send diagnostic and usage data to Apple	No
Do not allow user to override Gatekeeper setting	Yes
Restrictions Group	
Restrict which system preferences are enabled	Yes Network, Profiles, Sharing and iCloud should be disallowed. Other panes may be disabled at the organisation's discretion.
Allow use of Game Center	No
Allow only the following Dashboard widgets to run	Yes Do not add any widgets. This will stop any widgets from being able to access the Dashboard.
Select services that should be available in the share menu	Untick all

The media access settings can be used to limit user access to removable media such as USB drives, writeable optical media and AirDrop.

8.1 VPN profile

Setting	Value

Certificate type	ECDSA256
Encryption algorithm	AES-128-GCM
Integrity algorithm	SHA2-256
Diffie-Hellman group	19
Dead peer detection interval	Medium
Enable perfect forward secrecy	True
Disable redirects	False
Disable mobility and multihoming	True
Enable certificate revocation check	True
VPN On Demand	Always

In OS X 10.9, the mechanism for configuring the VPN On Demand settings changed, and none of the tested MDM utilities currently has a GUI for this new mechanism. To configure the VPN On Demand to trigger for all outgoing connections, follow the steps below:

- Configure the VPN settings using the MDM and test the profile on the device to ensure it connects manually
- Export the VPN configuration profile (unsigned) from the MDM as a .mobileconfig file. Convert this to text using `plutil` if required.
- Using a text editor, modify the XML configuration inside the exported file. In the IPSec key, change:

```
<key>OnDemandEnabled</key>
<integer>1</integer>
```

to

```
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>OnDemandRules</key>
<array>
<dict>
<key>Action</key>
<string>Connect</string>
</dict>
</array>
```

- Import the modified configuration to the MDM and deploy to the device

In profile manager, it is possible to set ‘Always on VPN (iOS supervised only)’. However, this causes the profile to fail to install on an OS X device so the approach described above should be used instead.

Note that for an OS X device to successfully verify the VPN server certificate, the certificate must have a Subject Alternative Name (SAN) entry that matches the common name.

8.2 Other settings

If not required, Bluetooth and Wi-Fi should be turned off before giving the device to the user. The user will be able to turn Wi-Fi back on if they need it.

Kernel Modules can be removed to prevent access to removable media and network interfaces, but this is unsupported and will be reset during some software updates. Instructions on how to do this can be found on pages 249 onwards of https://ssl.apple.com/support/security/guides/docs/SnowLeopard_Security_Config_v10.6.pdf

9. Enterprise considerations

The following points are in addition to the common enterprise considerations, and contain specific issues for OS X deployments.

9.1 iCloud

Users must not enable iCloud as this provides device control to Apple and may allow data to leak through iCloud backup and application storage. This can be achieved by not signing into the Apple ID when prompted by the operating system. Other Apple applications such as iTunes can be used with an Apple ID without enabling iCloud integration if this is required.

9.2 FileVault

In order for the enterprise to retain the ability to access the device in the event the FileVault 2 encryption password is lost, it should be ensured that the local administrator user has permission to unlock the FileVault encryption. This option is available within the Security & Privacy section of System Settings, under FileVault. A keychain can also be created by setting a Master Password (from the Users & Groups service menu). This keychain can be distributed to all managed OS X devices before enabling FileVault and will be acknowledged during the process of enabling FileVault. More information on this process can be found at http://support.apple.com/kb/ht5077 and pages 15 onwards of

http://training.apple.com/pdf/WP_FileVault2.pdf.

9.3 Extensions

In OS X 10.10, a new concept known as extensions was added. This allows application developers to extend the functionality of their application beyond the original application. As an example, the sharing extension could allow a user to share information to social network sites from an application. It is recommended that the enterprise controls what applications are installed in the environment and limit the ability for applications to interface to the user via Extensions. This can partially be configured as part of the enterprise MDM solution.

9.4 Handoff

A new feature which was introduced in iOS 8 and OSX 10.10 is Handoff. This allows a user to push documents being read from an iOS device to an OSX device to continue reading. As an example, a user can open a webpage on Safari on an iOS device and then continue reading the webpage on an OSX device using Handoff. This requires a user to login with an Apple ID. It is recommended that users are asked not to use this feature, as information and data is sent to Apple servers.

Legal information