



Overview of Operating Systems Security Features – Mac OS X

Introduction A key advantage of Mac OS X desktop operating system (OS) is its ease of customization to environment and/or solutions specific requirements, but this can also present security risks. A Mac OS X desktop that is part of the GC network environment may be compromised by malicious software (malware) or other threats that could spread through GC networks. Unsecure installation of Mac OS X desktop OS could either expose stored GC information to unauthorized personnel or make critical information unavailable. For these reasons, departments should ensure that Mac OS X desktop is configured and used securely.

Life Cycle Security should be addressed in each phase of an OS's life cycle: evaluation, configuration, deployment, management and decommissioning.

Working Environments Mac OS X requires different security controls depending on what they will be used for. Deployment environments range from Dedicated Production GC office desktops (most secure) to development GC Office desktops (moderately secure) to mobile desktops (least secure) such as receptions, conference rooms, and printing areas.

Basic Security Recommendations

Identification and Authentication – Strengthen user password & account and remove unwanted user accounts.

Authorization– Enforce minimum access on “root” or administrator account and enforce departmental password security policy.

Access Control – Harden user account access, enforce firmware password, and strengthen system-wide security, including login display lockdown and inactivity passwords.

Confidentiality – Ensure use of proper data encryption.

Integrity – Use up-to-date patch management, anti-virus and malware protection also enable and configure firewall.

Availability – Disable Bluetooth, harden firewall access, and implement lockdown of remote control.

Accountability and Non-Repudiation – Enforce limits on administrator logon, enhance logging and auditing to include authentication, process accounting, improve log data security, and enable time synchronization with a secure authorized time source.

Security Profile	Working Environment
Least Dangerous (Most Secure)	GC Production Desktops
Moderately Dangerous (Moderately Secure)	GC Development Desktops
More Dangerous (Less Secure)	Shared Desktops
Most Dangerous (Least Secure)	Mobile Desktops