



The Security Best Practices for Mac OS X v10.4 Exam Skills Assessment Guide

To Register

You are required to have an Apple Tech ID number before registering for an exam. You can apply for a Tech ID by following the instructions at certifications.apple.com. Then, to register for an exam, call Prometric toll-free at 888-APL-EXAM (888-275-3926) or register online at 2test.com.

To register for an Apple Training course, please visit www.apple.com/training or call 800-848-6398. To schedule an onsite course at your organization's location, please call 800-848-6398 or email abouttraining@apple.com.

The Security Best Practices for Mac OS X v10.4 Exam (Prometric exam no. 9L0-612) is a computer-based test offered at Authorized Prometric Testing Centers.

The exam is an elective in the Apple Certified System Administrator (ACSA) track. Successful completion of the exam earns Security Best Practices for Mac OS X 10.4 certification and also contributes 3 credits, valid for 2 years, towards Apple Certified System Administrator (ACSA) certification.

The exam lasts two hours and consists of 73 multiple-choice questions that are based on the knowledge-area objectives listed in this guide.

The score required to pass is 54 percent (40 items correct out of 73). Eight demographic questions are presented but are not scored.

To prepare for the exam, read through the objectives in this guide to determine which areas you need to review. You will not have access to any resources or references during the exam. Please note that the exam is based on Mac OS X and Mac OS X Server versions 10.4.

Please note also that if the Peachpit Apple Training Series: Mac OS X System Administration Reference, Volume 1 (which includes the Security Best Practices chapters) has been updated, a Corrections document will be available at <http://www.peachpit.com/ats.sysadmin>. Ensure that you have the most up-to-date information available on the exam content by reviewing any Corrections documented by Peachpit.

The number of test questions drawn from each knowledge area is indicated below. Please note that although this guide divides the objectives into ten knowledge areas, questions are presented randomly during the exam. Also note that UNIX commands and processes are shown in `monospace` in the exam.

Mac OS X Security Overview

This topic has 4 items, drawn randomly from the following objectives:

- Describe the Apple authorization philosophy.
- Identify the components of the security process.

- Describe the function of each component of the Mac OS X security architecture.
- Describe an IT security policy document and how it is developed.

Securing the Local System

This topic has 7 items, drawn randomly from the following objectives:

- Identify the four layers of the Mac OS X local security model.
- Describe how to set Open Firmware restrictions.
- Identify elements of a secure Mac OS X installation, including hard disk formats, passwords, and user-account based access controls.
- Describe the role of Disk Utility in creating a secure local system.
- Describe security options and vulnerabilities related to Mac OS 9 (Classic).
- Describe how the Mac OS X firewall functions.
- Describe how FileVault secures users' documents.

Optimizing Data Confidentiality

This topic has 14 items, drawn randomly from the following objectives:

- Outline standard UNIX permissions.
- Describe how to configure appropriate file-system permissions and ACLs to provide data security.
- Identify when to use SUID and GUID permissions.
- Describe how to audit for inappropriate SUID and GUID permissions.
- Describe how to restrict the administrator's home folder permissions so that other users cannot browse it.
- Identify the location and function of file-system access control lists.
- Describe how to configure Mac OS X computers for optimum data confidentiality by encrypting sensitive data on the local file system.
- Recognize the encryption features of FileVault.
- Describe how to create a secure documents folder by encrypting a disk image.
- Describe how to disable possible data leaks by encrypting the swap space, wiping clean free space, and using secure empty trash.

Mobility Security Concerns

This topic has 7 items, drawn randomly from the following objectives:

- Identify the features and security risks of Bluetooth and 802.11 WLANs.
- Describe how to configure Mac OS X Bluetooth for security.
- Identify similarities and differences between the features and level of security provided by WEP, 802.1X/WEP, WPA Enterprise, and WPA Personal.

- Describe how to configure Mac OS X for WEP, 802.1X/WEP, WPA Enterprise, and WPA Personal.

Secure Network Connections

This topic has 6 items, drawn randomly from the following objectives:

- Describe open ports.
- Describe how to implement SSH, SCP, and SFTP.
- Describe how to set up a VPN client.

Secure Authentication

This topic has 10 items, drawn randomly from the following objectives:

- Recognize the concepts behind authentication.
- Outline how to use Mac OS X Server to provide SASL-based encryption.
- Recognize the role Kerberos plays in Mac OS X and Mac OS X Server.

Secure Network Configuration

This topic has 1 item, drawn randomly from the following objectives:

- Recognize network security design principles.
- Identify methods for implementing a secure network design, including NAT, VPNs, and firewalls.
- Describe how to use the Mac OS X Gateway Setup Assistant to enable and configure routing, NAT, and VPN services.
- Describe how to use the Mac OS X Server Admin application to configure the firewall service.
- Describe how to create firewall rules to lock down traffic to and through a Mac OS X server, including remote administration traffic, Web and e-mail traffic, DNS zone transfers, pings, and ping replies.
- Describe how to configure Mac OS X firewall service for stealth mode.
- Outline how to analyze firewall rules with the UNIX `ipfw show` command.
- Identify how to monitor network security with logging.

Mail Security

This topic has 9 items, drawn randomly from the following objectives:

- Identify methods to reduce spam and virus email.
- Describe methods to secure email.
- Recognize ways to protect email servers.
- Describe how to bring up a chat server.
- Outline how to maintain physical security.

Web Security

This topic has 5 items, drawn randomly from the following objectives:

- Describe how to configure security features in Safari.
- Outline how to establish a secure website using SSL.
- Identify how to redirect from an HTTP site to an HTTPS site.
- Describe how to set up WebMail securely with SSL.
- Describe how to set up WebDAV securely with SSL.
- Describe how to set up a proxy server to block selected sites.

Maintenance, Intrusion Detection, and Auditing

This topic has 10 items, drawn randomly from the following objectives:

- Recognize which files to watch for unauthorized modification.
- Describe methods to detect malicious software.
- Describe varieties of malicious software, including Trojan Horses, Viruses, Worms, and Spyware.
- Describe how to use virus protection software.
- Describe how to use rootkit safely.
- Describe how to use Apple's Common Criteria auditing tools.

For More Information

Please visit www.apple.com/training or call 800-848-6398 for more information about all Apple Training courses and certification programs.