# Security Best Practices for Mac OS X v10.4

## Ensure optimum security and data confidentiality on your Mac OS X network.

### What You Will Learn

- To identify security needs and implement appropriately secure Mac OS X computers
- How to customize the security settings in Mac OS X for your network
- How to configure Mac OS X Server Open Directory Masters to provide secure authentication for an organization's particular clients
- How to protect Mac OS X Server Mail and Web services
- How to implement specific security configurations for mobile computers
- How to audit security using Apple's Common Criteria auditing tools
- How to publish and maintain security policies

### Course Description

The three-day Security Best Practices course provides system and security administrators with the knowledge and tools necessary to secure Mac OS X and Mac OS X Server against local and network attacks. Solutions covered in the class include Mac OS X specific features as well as third party tools for monitoring and analysis. Students will design a security policy template in class to be used as a starting point for their IT security decisions. This course is a combination of lecture and hands-on case study exercises that provide practical real-world experience.

### Who Should Attend?

This class is for anyone responsible for administering Mac OS X computers or servers, and providing the proactive security measures necessary for the integrity and confidentiality of all computer systems and their data. Some understanding of file systems, directory services, and networking is necessary. Command-line options for graphical utilities are covered, so a familiarity with terminal is also desired.

### Certification

The Security Best Practices v10.4 Exam (9L0-612) covers the knowledge necessary to secure Mac OS X and Mac OS X Server against local and network attacks. Solutions include using Mac OS X specific features as well as third-party tools for monitoring and analysis. For specific exam objectives, see the Skills Assessment Guide for the Security Best Practices for Mac OS X v10.4 Exam.

Successful completion of this exam earns Security Best Practices for Mac OS X 10.4 certification and also earns 3 credits toward Apple Certified System Administrator (ACSA) certification.

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

**Fact Sheet**
MacOS 340
Security Best Practices for Mac OS X v10.4

## To Register

To register for an Apple Training course, please visit train.apple.com or call 800-848-6398 in the US and Canada. To schedule an onsite course at your organization's location, please call 800-848-6398 or email abouttraining@apple.com.

**Apple Training Center Course**
Order number D3534Z/A

**Onsite Course**
Order number D3536Z/A

**Coordinated Onsite Course**
Order number D3535Z/A

## Prerequisites

Students should have the following prerequisite knowledge prior to attending the course:

- Completion of Mac OS X Support Essentials v10.4 and Mac OS X Server Essentials v10.4, or equivalent knowledge
- Experience with LDAP-based directory services
- Network and Internet topical knowledge

## Course Outline

| Topic | Description |
|---|---|
| Chapter 1<br>Overview/Architecture | Introduction to the basics of risk analysis and to Apple's security architecture. |
| Chapter 2<br>Securing the Local System | Using the NSA Security Document to refine the security settings in Mac OS X for local systems. |
| Chapter 3<br>Data Confidentiality | Keeping data confidential on local drives through the use of FileVault, file system permissions, and encrypted disk images. |
| Chapter 4<br>Mobility Security Issues | Wireless security for Bluetooth and 802.11, and physical security issues specific to mobile devices. |
| Chapter 5<br>Secure Network Connections | Comparing commonly used secure client protocols. Creating ssh tunnels, and configure VPN clients. |
| Chapter 6<br>Secure Authentication | Secure local authentication using different shadow hashes, smart cards, and biometrics. Secure network authentication using certificates and Open Directory security. |
| Chapter 7<br>Secure Network Configuration | Configuring Mac OS X Server for NAT, port forwarding, firewall, and VPN server. |
| Chapter 8<br>Mail Security | Security options in Mail.app, as well as configuring certificates and real-time blacklists on Mac OS X server, and Clam/AV for mail-borne virus detection. |
| Chapter 9<br>Web Security | Security options in Safari, as well as Apache web server security issues. Covers web server-specific file system security considerations, PHP vulnerabilities, and logging. |
| Chapter 10<br>Maintenance, Intrusion Detection, and Auditing | Apple certification compliance with various agencies, Common Criteria auditing tools, Apple's security update process. Analyzing Viruses, Macro Viruses, Trojans, and Worms, and exploring potential risks involved on Mac OS X. |

## For More Information

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