



Mac OS X Security and Mobility 10.6 Exam Skills Assessment Guide

To Register

This exam is offered at Apple Authorized Training Centers and Prometric Testing Centers worldwide. For information on exam registration, please visit training.apple.com/certification.

To learn more about Apple training offerings that can help you prepare for certification, please visit training.apple.com/courses.

The Mac OS X Security and Mobility 10.6 Exam (Prometric exam no. 9L0-625) is a computer-based test offered at Apple Authorized Training Centers and Prometric Testing Centers.

The exam is one of three required exams in the Apple Certified Specialist - Security and Mobility 10.6 certification track (ACS - SaM). You must pass this exam, and also earn Apple Certified Technical Coordinator 10.6 certification by passing the Mac OS X Support Essentials 10.6 Exam and the Mac OS X Server Essentials 10.6 Exam to become ACS - SaM 10.6 certified.

The exam is one of four required exams in the Apple Certified System Administrator (ACSA) 10.6 certification track. You must pass this exam, the Mac OS X Server Essentials 10.6 Exam, the Mac OS X Deployment 10.6 Exam, and the Mac OS X Directory Services 10.6 Exam to become ACSA 10.6 certified.

You may take up to two hours to complete the exam, which consists of 71 multiple-choice questions that are based on the objectives listed in this guide.

The score required to pass is 71 percent. Five 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. The primary reference source for this exam is the book: *Apple Training Series: Mac OS X Security and Mobility v10.6* (Peachpit 2010).

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 version 10.6. All references to Mac OS X and Mac OS X Server, unless otherwise stated, refer to version 10.6.

The number of test questions drawn from each knowledge area is indicated below. Please note that although this guide divides the objectives into eight knowledge areas, questions are presented randomly during the exam. Also note that UNIX commands and processes are shown in `monospace font` in the exam. Finally, when the term “by default” is used in the exam, it means using only the settings or values assigned automatically by the operating system or application, without any custom configuration.

Providing Network Services: DNS

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

- Without references, describe security vulnerabilities associated with the DNS service, including: DNS cache poisoning, server mining, DNS server profiling, Denial of Service (DoS), and service piggybacking.
- Given a default installation of Mac OS X Server and a properly formatted export of a DNS configuration file, import a primary zone for a given domain.
- Given a properly configured primary zone and functional DNS services on Mac OS X Server, create a secondary zone for the given domain on a separate installation of Mac OS X Server to establish high availability.
- Given a properly configured primary zone and functional DNS services on Mac OS X Server, a properly configured secondary zone, and functional DNS services on a separate installation of Mac OS X Server, configure a primary zone to accept zone transfer requests from a specific secondary zone (whitelist).
- Given a properly configured primary zone and functional DNS services on a Mac OS X Server computer, verify forward and reverse lookups for a primary zone.
- Without references, define the term “DNS zone”.
- Given a properly configured primary zone and functional DNS services on Mac OS X Server, configure a primary zone to forward requests not contained within its domain to a forward zone.
- Without references, describe three types of DNS zones, including master, slave, and forward.
- Given a properly configured primary zone and functional DNS services on Mac OS X Server configure a DNS sever to provide caching-only name services by clients internal to a company's intranet and refuse all external queries.
- Given a properly configured primary zone and functional DNS services on Mac OS X Server, configure a DNS server to provide authoritative-only name services.
- Given a properly configured primary zone and functional DNS services on Mac OS X Server, update the root zone stored in /var/named/named.ca.
- Given Server Admin and a DNS zone hosted on a Mac OS X Server computer, add mail exchange records to the zone.
- Given a properly formatted DNS configuration and a separate configuration file of unknown origin and content, troubleshoot a broken DNS config by comparing against a known-good config.
- Given Server Admin and a mail exchange record, configure the mail exchange record's priority.
- Without references, define the record types in the DNS system, including: Address (A), Canonical Name (CNAME), Mail Exchanger (MX), Name Server (NS), Pointer (PTR), Text (TXT), Service (SRV), and Hardware Info (HINFO).
- Without references, explain the differences between a fully qualified domain name (FQDN) and a relative domain name.
- Without references, explain the purpose of each of the following types of records that can be added to a DNS zone: address, alias or canonical name, mail exchange, and pointer.
- Given Server Admin and a DNS zone stored on a Mac OS X Server computer, add a new machine record to the DNS zone.
- Given Server Admin and a DNS zone hosted on a Mac OS X Server computer, add a new alias record to the DNS zone.

- Given Server Admin and a Macintosh OS X Server computer, start and stop DNS service on the server.
- Given the Lookup pane in Network Utility and a Macintosh OS X Server computer, verify that the DNS service on the server is correctly resolving domain names and IP addresses.
- Without references, list the address for the official BIND documentation.
- Given a default installation of Mac OS X Server, describe describe the underlying configuration/directory file structure for DNS services.
- Given an unconfigured installation of Mac OS X Server and an existing DNS server providing valid and accurate DNS services, describe the impact of pre-existing DNS on initial server setup.
- Without references, describe the purpose and benefit of DNS caching.
- Without references, describe how Domain Name System (DNS) associates computer host names with IP addresses on a network.
- Without references, describe the purposes of a DNS server, including translating between domain names and IP addresses, and acting as a cache and relay for translations provided by other DNS servers.
- Without references, describe how a DNS server uses a hierarchy of DNS servers to resolve a domain name that is not stored locally.
- Without references, list the four steps necessary to configure a new DNS service for an organization, including registering a domain name, creating DNS zones, adding DNS records to the zones, and starting the DNS service.

Providing Network Services: DHCP

This topic has 8 items, drawn from the following objectives:

- Without references, describe the security implications of deploying the DHCP service on Mac OS X Server v10.6, and strategies to mitigate the risks based on those implications.
- Given Server Admin, display the log files for the DHCP service.
- Without references, describe the function of the DHCP service in Mac OS X Server.
- Identify the DHCP log messages that indicate a lease was acquired from Mac OS X Server by a DHCP client.
- Given the log file for the DHCP service on a Mac OS X Server computer, identify the entries associated with a specified client computer.
- Given the server administration tools and system logs, isolate and resolve DHCP issues with a DHCP client or with the DHCP server on Mac OS X Server.
- Without references, list the 4 primary steps that occur when a client computer requests an address from a DHCP server.
- Given Server Admin, configure the lease and renewal times for a DHCP subrange in the DHCP service.
- Given Server Admin connected to a Mac OS X Server, configure the DNS information that will be provided to a given subrange by the DHCP service.
- Given Server Admin connected to a Mac OS X Server, configure the IP addressing information that will be provided to a given subrange by the DHCP service.
- Given Server Admin connected to a Mac OS X Server computer, specify over which network interfaces the DHCP service will provide addresses.

- Given Server Admin, display a list of the current client computers of the DHCP service on a Mac OS X Server computer.
- Given Server Admin, configure the DHCP service to assign a specific IP address to a specific computer based on the computer's hardware (MAC) address.
- Identify whether a network port has received an IP address from a DHCP server or is using a link-local address.
- Given Server Admin, configure the logging detail level for the DHCP service.

Providing Network Services: NAT/Gateway

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

- Without references, describe the security implications of deploying the NAT service on Mac OS X Server v10.6 and strategies to mitigate the risks based on those implications.
- Without references, describe how port forwarding is configured for and implemented by the NAT service on Mac OS X Server v10.6.
- Define the terms “static NAT”, “dynamic NAT”, and “Port Address Translation”.
- Given Server Admin, configure Mac OS X Server to provide multiple computers on a private LAN access to the Internet using a single assigned public IP address.
- Describe how an outbound NAT connection works on Mac OS X v10.6.
- Given a Mac OS X Server computer configured to act as a gateway between two networks, configure the NAT service to port forward incoming IP traffic to computers based upon the IP port of the incoming traffic.
- Without references, describe the relationship between IP ports and services on an IP host.
- Without references, define the term “port forwarding” as implemented in Mac OS X Server.
- Given Gateway Setup Assistant on a Mac OS X Server computer, configure the server to give multiple computers on a private LAN access to the Internet using a single assigned public IP address.
- Given a Mac OS X Server computer configured as a gateway server, troubleshoot a situation where a computer on the private network is unable to access services on the public network.
- Given a properly configured primary zone, functional DNS services, and NAT services on Mac OS X Server, create a namespace behind a NAT gateway.

Securing Systems and Services: Firewalls

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

- Without references, describe security considerations related to deploying the Firewall service on Mac OS X Server.
- Without references, explain the purpose of Stealth Mode in the Firewall service on a Mac OS X Server computer.
- Without references, explain how to enable Stealth Mode for TCP or UDP packets in the Firewall service on a Mac OS X Server computer.
- Without references, describe the architecture and configuration options of the Firewall service in Mac OS X Server.

- Given the Server Admin application, configure firewall logs in Mac OS X Server 10.6.
- Without references, describe the type, purpose, and benefit of Firewall services in Mac OS X Server.
- Given properly configured services running on a default installation of Mac OS X Server v10.6.x, network access, and a valid URL that accurately resolves to the Mac OS X Server v10.6, configure the Mac OS X Server's v10.6.x firewall to restrict access to certain services on certain IP addresses if that service doesn't support binding (AFP).
- Without references, explain the function of the adaptive firewall in Mac OS X.
- Given a default installation of Mac OS X Server v10.6.x with a misconfigured firewall service configuration and a valid network connection, troubleshoot an `ipfw` configuration.
- Given an firewall rule on a Mac OS X Server computer and an IP address, determine if the rule applies to the given IP address.
- Given a default installation of Mac OS X Server v10.6.x with a misconfigured firewall service and a valid network connection, troubleshoot the service by using `ping`, `telnet`, `tcpdump`, and Network Utility to verify packets based on rules established in firewall configuration.
- Given a default installation of Mac OS X v10.6, display the application firewall log.
- Given Server Admin, a Mac OS X Server computer and a range of IP addresses, create an address group to allow the Firewall service to control network access to computers using the given IP addresses.
- Given the Server Admin application, view firewall logs and identify connection attempts and failures in Mac OS X Server 10.6.
- Given Server Admin, a Mac OS X Server computer, a range of IP addresses, an action (either allow or deny), and a service name or port number and protocol (TCP/UDP), create a rule for the Firewall service that allows or denies IP traffic for the given service or port number through the firewall.
- Given Server Admin and a Mac OS X Server computer, configure the Firewall service to simply drop denied packets rather than sending a failure notification to the requesting computer.

Securing Systems and Services: VPN

This topic has 11 items, drawn from the following objectives:

- Without references, list the two encrypted transport protocols supported by the VPN service on Mac OS X Server.
- Without references, compare and contrast the two encrypted transport protocols supported by the VPN service on Mac OS X Server.
- Without references, list the three authentication options available for the Mac OS X Server L2TP VPN service.
- Without references, list the two authentication options available for the Mac OS X Server PPTP VPN service.
- Given a computer with a default installation of Mac OS X Server v10.6, , configure the computer's VPN service to provide valid IP addresses and require secure authentication.
- Without references, state the requirements for establishing IP addresses for VPN services on Mac OS X Server v10.6.

- Given a computer running Mac OS X v10.6 and a computer running Mac OS X Server v10.6, configure them to connect to each other via VPN service.
- Without references, identify the locations of the VPN log file on a Mac OS X computer.
- Without references, identify the locations of the VPN service log file on a Mac OS X Server computer.
- Without references, compare and contrast authentication mechanisms that can be used with Mac OS X Server's VPN service for both users and devices.
- Without references, state the requirements for integrating firewall services with VPN services on Mac OS X Server v10.6.
- Without references, describe the features, architecture, and options of the VPN service in Mac OS X Server v10.6.
- Without references, describe the features and options of the VPN client in Mac OS X v10.6.
- Without references, describe the features and options of the VPN client in iPhone OS.
- Without references, describe how the `ssh` tool in Mac OS X Server v10.6 can be used to tunnel unencrypted traffic over a network through an encrypted SSH channel.
- Given two computers running Mac OS X Server v10.6 and a functional network connection between them, configure an SSH tunnel between the two computers.

Securing Systems and Services: Keys and Certificates

This topic has 12 items, drawn from the following objectives:

- Without references, describe how 802.1x is implemented on Mac OS X, Mac OS X Server, and iPhone OS.
- Without references, describe the features and function of 802.1x as a network access control mechanism.
- Given a default installation of Mac OS X and Mac OS X Server and a functioning network connection between them, configure Mac OS X to connect to Mac OS X Server using 802.1x.
- Given a device running iPhone OS and Mac OS X Server and a functioning network connection between them, configure the iPhone OS device to connect to Mac OS X Server using 802.1x.
- Without references, describe the features and function of RADIUS on Mac OS X Server.
- Given a default installation of Mac OS X Server, an Airport Base Station, Mac OS X and a functioning network connection between them, configure the devices to connect using 802.1x/RADIUS.
- Without references, define the term "certificate" as it applies to computer security.
- Given a default installation of Mac OS X Server v10.6.x, configure the server's services to use a trusted certificate from an issuing authority.
- Given a default installation of Mac OS X Server v10.6.x, a default installation of Mac OS X v10.6.x with an expired key/certificate from the server, and a functional network connection between the server and client, troubleshoot the source and cause of the expired key/certificate, and then generate a new key/certificate to replace the expired key/certificate.

- Without references, describe the purpose and operation of keys and certificates as utilized in Mac OS X v10.6's implementation of the Public Key Infrastructure (PKI).
- Given a default installation of Mac OS X v10.6.x running the Terminal application, a default installation of Mac OS X Server v10.6.x, and functional network connections, configure an SSH key pair between the client and server machines so that an SSH connection can be made between them.
- Given an installation of Mac OS X Server v10.6.x with a valid certificate from a trusted certificate authority (CA), view the certificate and determine the granting certificate authority.
- Given a default installation of Mac OS X Server v10.6.x, display the built-in certificate(s).
- Given an installation of Mac OS X Server v10.6.x with a certificate issued by a certificate authority (CA), determine whether the computer trusts the certificate authority that issued the certificate.
- Without references, explain how trust of a certificate is granted.
- Given a default installation of Mac OS X Server v10.6.x, create a certificate signing request (CSR).
- Given a default installation of Mac OS X Server v10.6.x, create a self-signed certificate.
- Without references, list the services capable of using certificates in Mac OS X Server v10.6.
- Given an installation of Mac OS X Server v10.6.x with a certificate issued by a certificate authority (CA), validate the certificate using the appropriate tool.
- Without references, describe the function of the Certificate Authority (CA) as it applies to the Public Key Infrastructure (PKI).

Working with Mobile Devices: Providing iPhone Applications

This topic has 8 items, drawn from the following objectives:

- Given access to the iPhone SDK and a Mac OS X system, install the SDK so that the primary development tools can be used to create iPhone applications.
- Without references, state which iPhone SDK utilities are used to create an iPhone web application.
- Given a system with the iPhone SDK installed, create a simple iPhone Web application.
- Without references, state which iPhone SDK utilities are used to create an iPhone native application.
- Given a system with the iPhone SDK installed, create a simple iPhone native application.
- Without references, state how a developer gains access to the iPhone SDK.
- Without references, state what is required by a developer in order to install a native application on an iPhone.
- Without references, state the options for deploying a native iPhone application within an organization.
- Without references, compare the benefits of deploying an iPhone web application compared to a native iPhone application.
- Without references, explain what a provisioning profile is.

- Without references, explain how to install a provisioning profile.
- Without references, state which utility is used to distribute and manage iPhone configuration profiles.
- Given the iPhone Configuration Utility installer package and a Mac OS X computer, install the iPhone Configuration Utility.
- Without references, explain how to use the iPhone Configuration Utility to create a configuration profile.
- Without references, explain how to distribute and install a configuration profile on an iPhone.
- Without references, explain where to get the iPhone Configuration Utility.

Working with Mobile Devices: Mobile Access Server

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

- Without references, explain the function of the Mobile Access service on Mac OS X Server.
- Given Server Admin, a Mobile Access server and an iCal server, configure the Mobile Access server to route external iCal traffic to the internal iCal server.
- Without references, explain the benefits of using Mobile Access service as compared to VPN.
- Given Server Admin, a Mobile Access server and a Mail server, configure the Mobile Access server to route external mail traffic to the internal Mail server.
- Without references, list the services to which the Mobile Access service provides proxy access.
- Given Server Admin, a Mobile Access server and a private Web server, configure the Mobile Access server to forward Web traffic to the internal Web server.
- Without references, explain how Mobile Access service provides access to private resources.
- Given Server Admin and a Mobile Access server, start and stop the Mobile Access service.
- Without references, compare and contrast the three methods for using certificates with proxied services.
- Given Server Admin and a Mobile Access server, display the Mobile Access service logs.
- Without references, list the client OS requirements to allow a client computer to access services on a private network via the Mobile Access service.
- Given Server Admin and a Mobile Access server, display the status of the Mobile Access service, including which proxy services are running and the number of requests made on each proxy service.

For More Information

Please visit training.apple.com for more information about all Apple training courses and certification programs.