# Mac OS X Security

Keeping safety simple.

## Features

**System security**

- Mandatory access controls
- Application signing
- System library randomization
- No-execute stack for all applications
- Stack canaries
- No-execute heap for 64-bit applications
- Tagging and first-run warning for downloaded applications
- Cryptographic verification of software update packages

**Data protection and privacy**

- 256-bit AES disk image encryption
- 128-bit AES FileVault home directory encryption
- Guest user account

**Network security**

- Application firewall
- Kerberos for NFS
- SMB packet signing
- VPN: L2TP over IPSec
- VPN: PPTP
- VPN: Cisco IPSec
- Access control lists for shared files and folders
- Kerberos KDC

**Authentication and smart cards**

- Smart card keychain unlock
- Screen lock on smart card removal
- Support for U.S. federal government Personal ID Verification (PIV) standard
- Null or empty passwords disallowed for remote access
- Keychain Access that can associate selected user certificates with services and applications

The Mac computer has a great track record for security, thanks not only to a development process that includes security from the design phase, but also to a commitment to making security features easy to use. Security in Mac OS X is grounded in a few simple principles:

- **Highly secure from the start.** You don't have to be a security expert to configure your Mac to be secure at home or on the road—you just need to know how to turn on the computer. That's because the default settings safely restrict how your Mac communicates on the network.
- **Easy to keep up to date.** Apple makes it easy to keep your Mac up to date with digitally signed automatic software updates. Mac checks for updates every week by default, but you can set it to check as frequently as every day.
- **Easy to make even more secure.** With tools to help you create strong passwords, FileVault to encrypt the contents of your home directory, and a firewall to provide an added measure of network protection, Mac OS X makes it easy to enhance the security of your Mac.

## Improvements in Snow Leopard

Mac OS X version 10.6 Snow Leopard includes a host of new security features and technologies designed to enhance the protection of your Mac and your personal information. The goal is to strengthen Mac security with features that are as invisible and intuitive as possible, while giving you easy tools to help make your Mac even more secure.

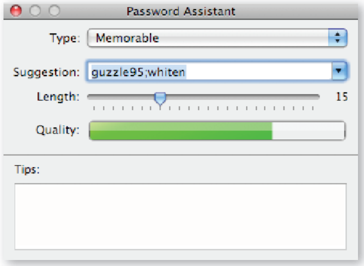
- **Stronger runtime security.** Improved runtime protection for data such as stack canaries, heap corruption checks, and sandboxed system services helps to stymie attacks that try to hijack or modify the software on your system.
- **Browser plug-ins in a separate process.** On 64-bit Mac computers, Safari runs certain plug-ins in a separate process. This not only keeps an errant plug-in from crashing Safari, but it also takes advantage of more secure system routines for managing data.
- **64-bit applications.** All the key system applications in Snow Leopard run 64 bit by default on 64-bit Mac computers. The 64-bit runtime system in Mac OS X provides enhanced security thanks to features such as no-execute data on the system heap, as well as architectural advantages such as passing arguments to functions in registers rather than on the stack.
- **Improved secure connectivity.** Virtual private network (VPN) support has been enhanced to connect to Cisco IPSec VPN servers—without additional software.

## Layers of Protection

Mac OS X is designed to provide defense in depth against outside security threats with a series of protective measures and systems. These include authentication and access control systems, protection from network-borne threats, and runtime mechanisms such as library randomization and sandboxing.

### Strong authentication

Authentication is the process of verifying the identity of a local or network user. Mac OS X supports local and network-based authentication to help ensure that only users with valid authentication credentials can access the computer's data, applications, and network services. Passwords and other credentials can be required to log in, wake the system from sleep or a screen saver, install applications, or change system settings. Mac OS X also supports smart cards for authentication.



Password Assistant

Type: Memorable

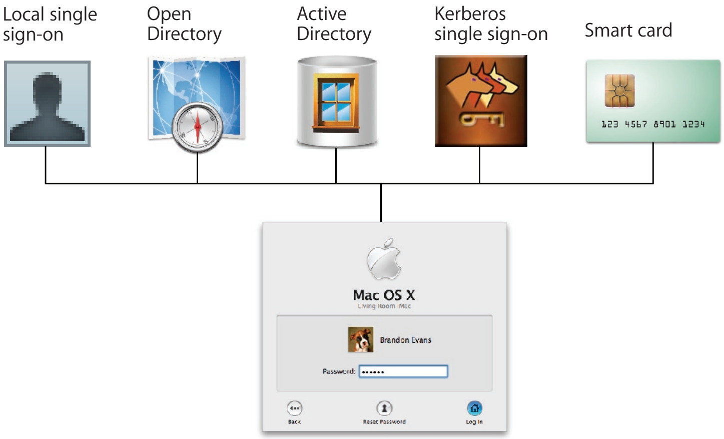
Suggestion: guzzle95;whiten

Length: 15

Quality:

Tips:

**Building a better password**
The Password Assistant can help you create a password that's both strong and memorable. To display the Password Assistant panel, click the key icon next to the Password field in the Accounts preference pane. The Password Assistant is also available in Disk Utility to help you create strong passwords for encrypted disk images.



**Local single sign-on.** Mac OS X enables you to sign on just once, obtaining your application- or site-specific credentials from the system's keychain for local authentication or from directory services for network authentication. This means that you can use one name and password combination for all privileges.

**UNIX® Pluggable Authentication Modules.** The Mac OS X security architecture supports Pluggable Authentication Modules (PAMs), enabling PAM-based UNIX applications to access its authentication mechanisms.

**Offline authentication.** By securely caching network-based credentials, Mac OS X allows you to authenticate offline. So you can disconnect your notebook computer from your office network and work offline—at home or on the road—using the same user name and password.

**Open Directory.** Mac OS X supports Open Directory 4, the latest version of Apple's standards-based directory services architecture, for storing password enforcement policies and authentication credentials in a robust, central repository. Built into Open Directory is an authentication server that uses Kerberos Key Distribution Center (KDC) to provide strong authentication with support for secure single sign-on. Users need to authenticate only once, with a single user name and password pair, for access to a broad range of Kerberized network services. For services that have not been Kerberized, the integrated SASL service automatically negotiates the strongest possible authentication protocol.

**Kerberos.** Like previous versions of Mac OS X, Snow Leopard integrates open source Kerberos KDC for secure access to and collaboration with network resources. This robust, directory-based authentication mechanism enables single sign-on to all authorized systems and services. Instead of authenticating to each service individually, you enter your password only once at login to prove your identity to the Kerberos authentication authority or KDC. In response, KDC issues strongly encrypted electronic "tickets," which are used to assure all participating applications and services that you have been authenticated securely. Kerberized applications and services include NFSv3, Safari, SSH, SMB, Mail, Telnet, VPN client, and the AFP (Apple Filing Protocol) client.

**Active Directory.** Mac OS X allows users to participate in Windows-managed networks, with a single home directory, on either a Mac or a Windows-based computer. Network administrators can set one authentication policy for all users, both Mac and Windows, that enables Mac OS X users to log in and authenticate to Microsoft's proprietary Active Directory—without any specific changes needed to accommodate them.

**NTLMv2.** Mac OS X supports Microsoft's NTLM version 2 authentication protocol for increased compatibility.

**Smart cards.** Mac OS X allows you to use your smart card whenever an authentication dialog is presented. This robust, two-factor authentication mechanism offers built-in support for Department of Defense Common Access Card, U.S. PIV, Belgium National Identification Card, Japanese government PKI, and Java Card 2.1 standards. Similar to an ATM card and a PIN code, two-factor authentication relies on something you have and something you know. If your smart card is lost or stolen, it cannot be used unless your PIN is also known.

Mac OS X has additional functionality for smart card use such as:

- **Lock screen access on smart card removal.** You can configure your Mac to automatically lock the screen whenever you remove your smart card.
- **Unlock keychain.** When you insert a smart card, the keychain can be unlocked, and your stored information and credentials can be used.

### Firmware password protection

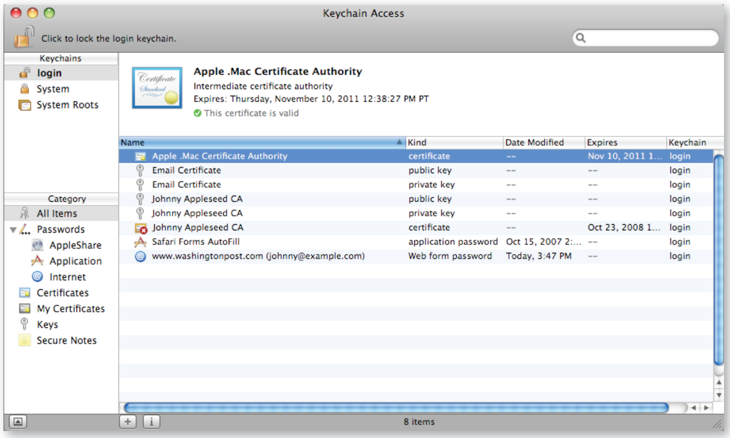
You can use passwords to prevent system startup from unauthorized disks by restricting access to the Startup Manager and disabling hot keys, so the computer cannot be booted from a CD, DVD, NetBoot disk image, or another hard drive using target disk mode. Firmware password protection is especially valuable for public kiosks or computer labs, where computer access is unmonitored.

### Keychain for storing credentials

The Mac OS X Keychain provides a convenient, secure repository for your various user names and passwords, as well as other authentication credentials. While it's a good security practice to use a unique password for each resource, most users find it impossible to remember so many passwords. Use a single login password to unlock your keychain and authenticate automatically to file servers, FTP servers, websites, your .Mac account, email accounts, encrypted files, and other password-protected resources. There's no need to enter—or even remember—the user name and password for each resource. You can choose which items to store in your keychain or require specific applications to request authentication, even if your keychain contains the necessary information.

### Store more in your keychain

In addition to storing passwords and other credentials, keychains can be used to store notes and confidential information, such as ATM and credit card PINs. You can even create multiple keychains to store passwords for different purposes—for example, one for work and one for online shopping—or copy your keychain from one computer to another.



**Apple .Mac Certificate Authority**
Intermediate certificate authority
Expires: Thursday, November 10, 2011 12:38:27 PM PT
This certificate is valid

| Name | Kind | Date Modified | Expires | Keychain |
|---|---|---|---|---|
| Apple .Mac Certificate Authority | certificate | -- | Nov 10, 2011 1... | login |
| Email Certificate | public key | -- | -- | login |
| Email Certificate | private key | -- | -- | login |
| Johnny Appleseed CA | public key | -- | -- | login |
| Johnny Appleseed CA | private key | -- | -- | login |
| Johnny Appleseed CA | certificate | -- | Oct 23, 2008 1... | login |
| Safari Forms AutoFill | application password | Oct 15, 2007 2:... | -- | login |
| www.washingtonpost.com (johnny@example.com) | Web form password | Today, 3:47 PM | -- | login |

The keychain securely stores user names and passwords. All the password data in the keychain is protected using the Triple Digital Encryption Standard (3DES). For added protection, Mac OS X locks your keychain when you log out. You can also set Mac OS X to lock your keychain when the system sleeps or after a specified time of inactivity, and you can lock your keychain manually at any time. If you store your home directory on a network server, your keychain remains safe because all keychain information is provided only on the local client system as applications request it. You can synchronize the keychains on all your Mac systems with iSync. Using more than one Mac has never been so easy and secure.

### User permissions model

Mac OS X inherits its permissions model from UNIX. Apple has enhanced this security model by disabling the root account by default. Running code with the minimum necessary level of privileges helps protect the system from inadvertent or deliberate damage.

There are three types of user accounts in Mac OS X:

**User.** The user account is the least privileged account in the Mac OS X system. The user can modify settings only for his or her account, not the entire system. It is considered a good security practice to have all users operate at this level of permissions. If further privileges are required to install software or modify system settings, an administrator can be authenticated when needed. Additional limits can be placed on user accounts to prevent them from:

- Opening System Preferences
- Removing items from the Dock
- Changing passwords
- Burning CDs or DVDs
- Using certain installed applications

These limits can be managed using either parental controls in Snow Leopard or managed preferences in Mac OS X Server version 10.6 Snow Leopard.

**Administrator.** Mac OS X establishes an administrator user account when the system is first installed. An admin user can perform most of the operations normally associated with the root user, except directly adding, modifying, or deleting files in the system domain. However, an administrator can use the Installer or Software Update applications for this purpose.

**Root.** Mac OS X (like most UNIX operating systems) has a superuser, named root, who has full permissions for access to all files on the system. Specifically, root can—with a few limited exceptions—execute any file that has any of its execute permissions turned on and can access, read, modify, or delete any file and any directory. Unlike traditional UNIX systems, Mac OS X disables this powerful account by default. This precaution helps to limit the extent of harmful changes that viruses or unauthorized users could make to the operating system.

In addition to user accounts, Mac OS X uses less privileged system accounts for some system services and software that require specialized access to certain system components, but not login access.

To prevent unauthorized users from altering the system in an undesirable way, new users do not have administrative privileges unless they are assigned to them by the administrator. As users are added to the system, Mac OS X assigns them nonadministrative user accounts and prompts them to choose a password, providing a means of authentication. Remote access is not allowed for users with no password.

**Support for multiple users**

Mac OS X makes it easy and secure for multiple users to use a single computer, whether at home or in workgroups or labs. Each user can have a unique user name, password, keychain, and home directory, while UNIX-based access controls prevent unauthorized users from accessing another user’s private data.

For added control, the administrator can grant certain individuals access to specified capabilities, while restricting others. Capabilities can include permission to change the appearance of the Dock, modify system preferences, change passwords, burn CDs or DVDs, install software, launch applications, and access printers.

### Physical security

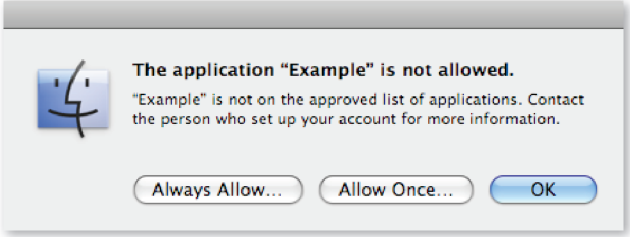
Security begins with hardware. To protect your system from theft, all Apple computers have internal slots for inserting Kensington locks. In addition, the Mac Pro enclosure has a locking mechanism built into the side panel latch, keeping valuable internal components safe from theft or tampering.

### Mandatory access controls

The Mac OS X kernel provides mandatory access controls. These controls enforce restrictions on access to system resources (such as networking, file systems, and process execution) so that resources are available only to processes that are explicitly granted access. Mandatory access controls in Mac OS X aren't directly visible to users, but they are the underlying technology for several important features in Mac OS X, including sandboxing, parental controls, managed preferences, and a "safety net" feature for Time Machine.

The Time Machine feature clearly illustrates the contrast between mandatory access controls and the user privilege model: It allows files within Time Machine backups to be deleted only by programs related to the Time Machine feature. From the command line, no user—even one logged in as root—can delete the files within a Time Machine backup.

Mandatory access controls are integrated with the exec system service to prevent the execution of applications that aren't authorized. This is the basis for the application controls in both parental controls in Mac OS X and managed preferences in Mac OS X Server.



**The application "Example" is not allowed.**

"Example" is not on the approved list of applications. Contact the person who set up your account for more information.

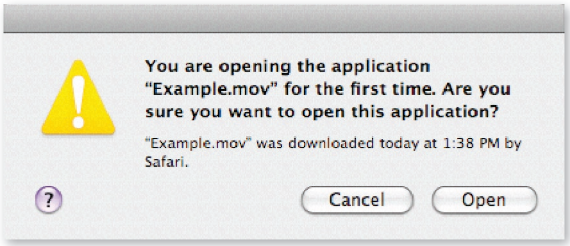
Mandatory access controls enable strong parental controls in Mac OS X.

In the case of the sandboxing facility in Mac OS X, mandatory access controls restrict access to system resources as determined by a special sandboxing profile that is provided for each sandboxed application. This means that even processes running as root can have extremely limited access to system resources.

### Protection against Trojan horse downloads

Files downloaded using Safari, Mail, and iChat are automatically tagged with metadata indicating that they are downloaded files and referring to the URL, date, and time of the download. This metadata is propagated from any archives that are downloaded (such as ZIP or DMG files) so that any file extracted from the archive is also tagged with the same information. Files copied from USB drives are also tagged with this metadata.

The first time you try to run an application that has been tagged, you are prompted by a warning asking whether you want to run the application and displaying the information on the date, time, and location of the download.



**You are opening the application "Example.mov" for the first time. Are you sure you want to open this application?**

"Example.mov" was downloaded today at 1:38 PM by Safari.

You can either continue to open the application or cancel the attempt, which is appropriate if you don't recognize or trust the application. Once an application has been opened, this message does not appear again for that application.

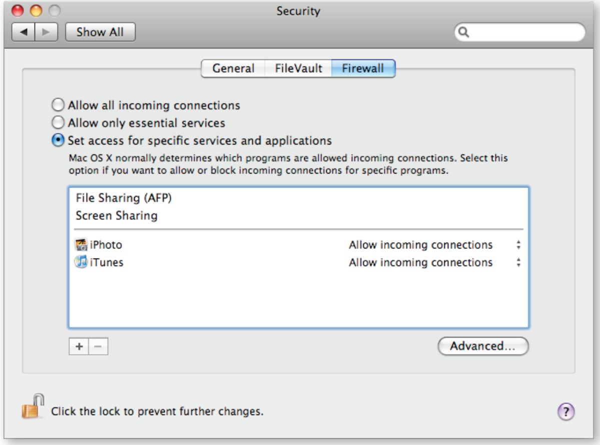
This new mechanism dramatically reduces the number of warnings related to downloads that you see. Such messages now appear only when you attempt to launch a downloaded application. When you do see a warning, you are given useful information about the source of the download that can help you make an informed decision about whether to proceed.

## Network Communications

For communications over the web and in email, Mac OS X integrates robust security standards into its Safari web browser and Mail application, including Transport Layer Security (TLS) and support for digital certificates. In addition, Mail supports a choice of local and network-based authentication methods.

### Firewalls

The application-based firewall in Mac OS X makes it easy for nonexperts to get the benefits of firewall protection. The application firewall allows or blocks incoming connections on a per-application basis rather than on a per-port basis.



○ Allow all incoming connections
○ Allow only essential services
● Set access for specific services and applications

Mac OS X normally determines which programs are allowed incoming connections. Select this option if you want to allow or block incoming connections for specific programs.

File Sharing (AFP)
Screen Sharing

| | |
|---|---|
| iPhoto | Allow incoming connections |
| iTunes | Allow incoming connections |

Click the lock to prevent further changes.

The application firewall allows or blocks access on a per-application basis.

Users can restrict firewall access to just essential network services (such as those needed for DHCP, BOOTP, IPSec VPNs, and Bonjour), or they can allow (or block) access to selected applications on an individual basis. The application firewall uses digital signatures to verify the integrity of applications. If you select an unsigned application, Mac OS X will sign that application in order to uniquely identify it.

For expert users, the IPFW firewall is still available on the system. Since IPFW handles packets at a lower level of the networking stack than the application firewall, its rules take precedence.

### Networking security standards

Whether communications are taking place over wired or wireless networks, Mac OS X provides secure access to network resources and protection against unauthorized use. Using highly secure networking protocols that are based on open standards, such as OpenSSL and OpenSSH, Mac OS X helps ensure data security while traversing local area networks as well as the Internet. In addition, VPN uses the Layer 2 Tunneling Protocol (L2TP), Cisco IPSec, or Point-to-Point Tunneling Protocol (PPTP) to support secure communications to your work or home network.

### Encrypted Internet communications with TLS and SSL

Mac OS X includes TLS as well as SSL versions 2 and 3 for compatibility. Safari and other Internet applications automatically start these transport layer mechanisms to provide an encrypted channel between two systems and to protect the information in the channel from eavesdroppers. For maximum protection, Safari and Mail support 128-bit TLS encryption.

### Back to My Mac

Back to My Mac lets MobileMe subscribers see their registered computers from anywhere on the Internet. It uses advanced authentication and security technologies to help prevent unauthorized access to your data and protect it while it's in transit over the Internet. When you first sign in to MobileMe, you receive a digital certificate and private key for your "MobileMe Sharing Identity." When you connect to another system using Back to My Mac, authentication is performed using the standard Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) protocol with the MobileMe Sharing Identity.

Communication between Back to My Mac computers over the public Internet is encrypted using IPSec.

### Authentication with 802.1X

The 802.1X standard enhances security by requiring users to authenticate before connecting to a wired or wireless network. 802.1X ties the Extensible Authentication Protocol (EAP) to both wired and wireless networks with support for multiple authentication methods: Lightweight Extensible Authentication Protocol (LEAP), Protected Extensible Authentication Protocol (PEAP), TLS, and Tunneled Transport Layer Security (TTLS).

802.1X configuration in Mac OS X is extremely easy to deploy, even for large numbers of network users. Client configurations can be exported as an Internet Connect file and distributed via email, on a secure website, or using other out-of-band methods. When the user opens the file, all necessary settings are imported into Internet Connect, so the client is configured instantly for wireless communications.

### Secure Shell

For command-line access to remote systems, Mac OS X uses Secure Shell (SSH) in place of clear-text Telnet sessions (which are disabled by default). SSH encrypts remote command-line data, such as passwords, to help eliminate eavesdropping and other network-level intrusions. In Mac OS X, SSH is integrated with the system keychain.

### Virtual private network

Mac OS X includes a universal VPN client with support built into the Network preference pane, so you have everything you need to establish an encrypted connection. The VPN client supports L2TP over IPSec, Cisco IPSec, and PPTP, which make Apple's VPN client compatible with the most popular VPN servers, including those from Microsoft and Cisco.

You can also use digital certificates and one-time password tokens from RSA or CryptoCARD for authentication in conjunction with the VPN client. The one-time password tokens provide a pseudo–randomly generated passcode number that must be entered along with the VPN password—a great option for those who require extremely robust security. In addition, the L2TP VPN client can be authenticated using credentials from a Kerberos server. In either case, you can save the settings for each VPN server you routinely use as a "location," so you can reconnect without having to reconfigure your system each time.

**Ticket Viewer**

Mac OS X includes a utility for working with Kerberos tickets. You can access the Ticket Viewer application by launching the Keychain Access application and choosing Ticket Viewer from the Keychain Access application menu. Ticket Viewer allows you to see detailed information on current Kerberos tickets, as well as renew or destroy tickets.

**Certificate Assistant**

Certificate Assistant is an easy-to-use utility that helps you request, issue, and manage certificates. It contains all the functionality to create, manage, and issue certificates to a small group of friends or a small office. Certificate Assistant includes many features of a commercial Certificate Authority at no cost. The certificates created by Certificate Assistant can be used to send encrypted email, log in to protected websites, or participate in encrypted chat sessions with iChat.

Apple’s L2TP VPN client can connect you to protected networks automatically by using its “VPN on demand” feature. VPN on demand can automatically establish a VPN connection for you when you need to connect to a specified domain. This results in increased security because VPN connections can be closed when not in use, and you can work more efficiently.

The VPN client includes support for Cisco Group Filtering as well as DHCP over PPP to dynamically acquire additional configuration options such as Static Routes and Search Domains.

### Windows SMB packet signing

The Windows network file system (SMB) client supports the signing of SMB packets. SMB packet signing is a security mechanism in the SMB protocol that allows network traffic to be signed and verified, providing improved compatibility and security when connecting to Windows-based servers.

### Digital certificates

The use of digital certificates enables Mac OS X to support secure communications. Similar to a driver’s license, digital certificates are a form of identification that enables the following important security services:

- **Authentication.** Digital certificates guarantee the identity of the author or “signer.”
- **Data integrity.** Signatures facilitated by certificates ensure that messages have not been changed or altered, whether accidentally or maliciously.
- **Encryption.** Digital certificates facilitate the encryption of messages to help protect confidential or private information.
- **Nonrepudiation.** Digital certificates enable the recipient to verify the identity of the signature accompanying a particular message, similar to a witnessed signature on a paper document.

A digital certificate is composed of a public key and a private key, along with other information about you and the Certificate Authority (CA) that issued the certificate. To send encrypted messages, the sender must be able to access the recipient’s public key either from the sender’s keychain or from a directory server; this enables Mac OS X to use the recipient’s public key for encryption. When the encrypted message is received, the recipient’s private key is used to decrypt the message. Every time you send digitally signed email, your certificate and public key are included with the message, allowing recipients to send you encrypted messages in reply.

For web transactions, the Safari web browser in Mac OS X uses X.509 digital certificates to validate users and hosts, as well as to encrypt the communication on the Internet. An example is online banking. Your bank is issued an identifying certificate from a well-known CA. This allows your browser to check the validity of the certificate being presented and to set up the secure session with TLS or SSL encryption, verifying that the site’s identity is legitimate and that your communication with the website is encrypted to help prevent interception of personal or confidential data. Easy to deploy and highly scalable, digital certificates are implemented systemwide and shared among multiple applications. With support for the X.509 standard, Mac OS X provides a full application programming interface (API) that enables developers to leverage system-level certificate support.

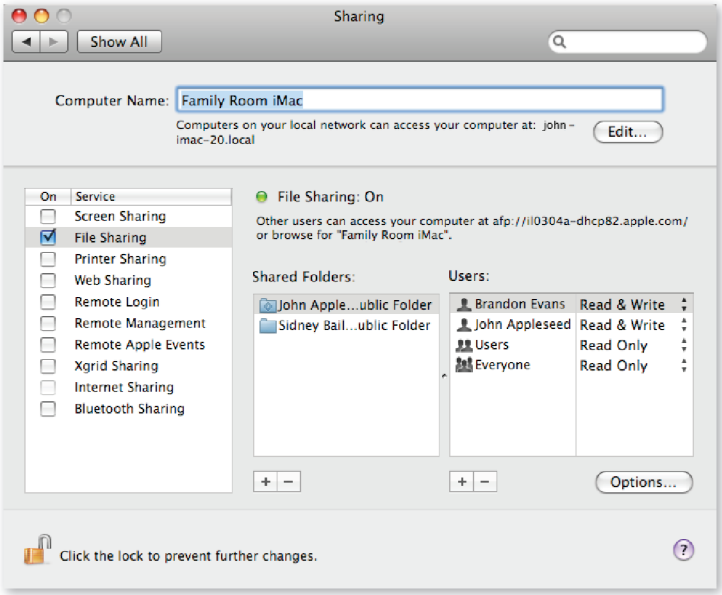
Technologies in Mac OS X that can use digital certificates include:

- FileVault
- Login window
- Screen saver
- NFSv3
- Safari
- Keychain
- VPN client
- Mail
- Apache
- iChat
- Certificate Assistant
- Smart cards
- Address Book
- Access control lists

For quick access to secure websites and email messages, you can add digital certificates to your keychain. Whenever you receive a certificate, on the web or via email, you can import the certificate into your keychain for later use.

### Sharing and collaboration configuration

In Mac OS X, the sharing services that you enable can be configured to allow access only to users that you specify through access control lists (ACLs). You can create user accounts for sharing based on existing user accounts on the system, as well as entries in your address book.



Computer Name: Family Room iMac

Computers on your local network can access your computer at: john-imac-20.local

| On | Service |
|---|---|
| □ | Screen Sharing |
| ☑ | File Sharing |
| □ | Printer Sharing |
| □ | Web Sharing |
| □ | Remote Login |
| □ | Remote Management |
| □ | Remote Apple Events |
| □ | Xgrid Sharing |
| □ | Internet Sharing |
| □ | Bluetooth Sharing |

● File Sharing: On

Other users can access your computer at afp://il0304a-dhcp82.apple.com/ or browse for "Family Room iMac".

Shared Folders:

- John Apple…ublic Folder
- Sidney Bail…ublic Folder

Users:

| | |
|---|---|
| Brandon Evans | Read & Write |
| John Appleseed | Read & Write |
| Users | Read Only |
| Everyone | Read Only |

Click the lock to prevent further changes.

Sharing services become more secure with access control lists.

## Runtime Protection

Snow Leopard offers several new features designed to help protect your Mac from some of the most common techniques used by malicious software to hijack software running on your system.

### Execute disable

One of the most common techniques used by developers of malicious software to gain unauthorized access to systems is known as buffer overflow. A buffer overflow can occur when the developer of a piece of software erroneously allocates a fixed amount of memory as a buffer for an input that can be of arbitrary length. For example, a program might process a string of text such as a filename and be written in a way that assumes that the filename will never exceed 256 characters. If the buffer for the string representing the filename has a fixed length of 256 characters and a longer input is provided to the buffer, a buffer overflow can result. Software trying to hijack the system can use a buffer overflow to execute its own malicious code (often referred to as shellcode).

**Developer options**
With Xcode in Snow Leopard, developers can add enhanced runtime security to their applications with a number of features. Applications built with Xcode can use stack "canaries" that cause an application to terminate if there is a stack buffer overflow. In addition, applications can be built as position-independent executables so that their own library addresses are randomized as well as those of the system libraries. Finally, the Xcode compiler provides several options for checking developers' code at compile time to scan for common mistakes that could make code vulnerable to buffer overflows.

Since the release of Mac OS X version 10.4 Tiger on Intel processor–based Mac systems, Mac OS X has provided no-execute stack protection by taking advantage of the execute disable (XD) function available in recent Intel microprocessors. With execute disable, the compiler marks certain regions of a program as containing data only at the time a piece of software is compiled into object code. The processor then refuses to execute instructions in those regions that are designated as data only.

In Snow Leopard, stack execute disable is available for both 32- and 64-bit applications. For 64-bit processes, Snow Leopard provides protection from code execution in both heap and stack data areas.

### System library randomization

While the execute disable feature provides some measure of protection from buffer overflow exploits, there is a well-known technique for circumventing stack execute disable called "return to libc." The essence of a return to libc attack is to replace a legitimate return memory address on the stack with the known memory address of a system function. The technique gets its name from the practice of calling functions such as system() in the system's C library.

System libraries are assigned random addresses when the system is installed and when library prebinding is updated on the system (typically after system software updates, though you can manually force an update by running the "`update_dyld_shared_cache -force`" command). For any given Mac, the address of a particular library function will be fixed in one of thousands of random locations between system updates, but across all Mac systems, the address is different. This makes it much more difficult to use return to libc exploits, since for any given Mac it is difficult to know the address of the system library function.

### Sandboxing

Sandboxing helps ensure that applications do only what they're intended to do by placing controls on applications that restrict which files they can access, whether they can talk to the network, and whether they can be used to launch other applications. In Snow Leopard, many of the system's helper applications that normally communicate with the network—such as mDNSResponder (the software underlying Bonjour) and the Kerberos KDC—are sandboxed to guard them from abuse by attackers trying to access the system. In addition, other programs that routinely take untrusted input (for instance, arbitrary files or network connections) such as the H.264 codec, Xgrid, and the Quick Look and Spotlight background daemons are sandboxed.

Sandboxing is based on the system's mandatory access controls mechanism, which is implemented at the kernel level. Sandboxing profiles are developed for each application that runs in a sandbox, describing precisely which resources are accessible to the application.

## Application Signing

By signing applications, your Mac can verify the identity of an application and ensure its integrity. All applications shipped with Mac OS X are signed by Apple. In addition, third-party software developers can sign their software for the Mac. Application signing doesn't provide any intrinsic protection, but it integrates with several other Mac OS X features to enhance security.

Signing is used by features—such as parental controls, managed preferences, Keychain, and the firewall—that need to verify that the applications they are working with are the correct, unmodified versions. With Keychain, the use of signing dramatically reduces the number of Keychain dialogs presented to users since the system can validate the integrity of an application that uses a keychain. With parental controls and managed preferences, the system uses signatures to make sure that an application that is allowed to run is unmodified. With the application firewall, signatures are used to identify and verify the integrity of applications that are granted network access. In the case of parental controls and the firewall, unsigned applications are signed by the system on an ad hoc basis in order to identify them and verify that they remain unmodified.

## Protecting Private Data

Mac OS X has a number of features designed to protect the confidentiality of your data, whether it is stored in your home directory, traveling across the Internet, or shared locally on your network.

**Master password**
For extra security and control, a master password can help you to change your FileVault password in the event you lose or forget it. The master password is particularly useful for system administrators who need to keep company data accessible, even if employees forget their passwords or leave the company.

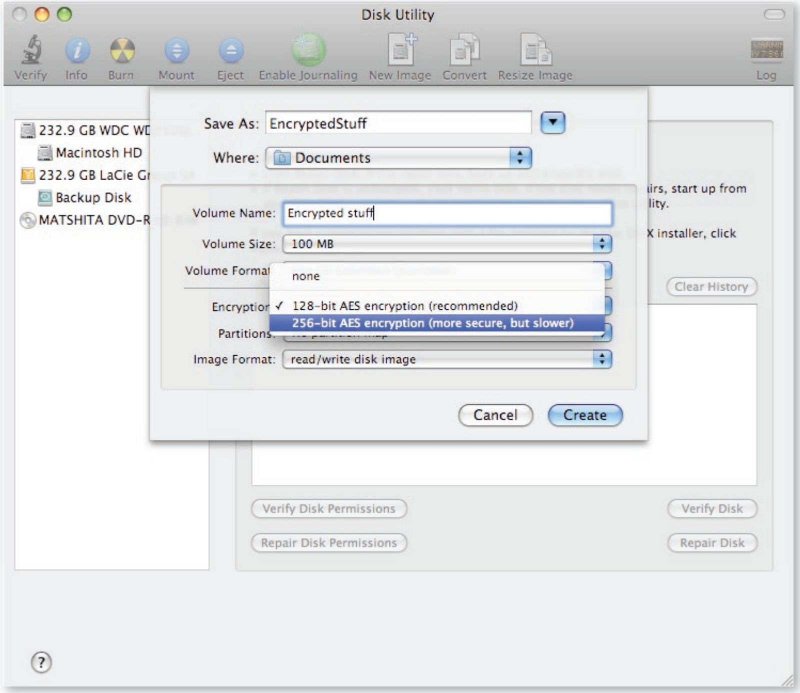
### FileVault

FileVault keeps your documents secure, even if your computer is lost or stolen, by storing them in an encrypted form in your home directory—preventing unauthorized users, applications, or utilities from reading them. With FileVault enabled, all the information in your home directory is always encrypted. By logging in and authenticating, you provide the key to access your encrypted documents. Documents are decrypted on the fly as you open them and reencrypted as you save them to disk.

FileVault encrypts files with the robust Advanced Encryption Standard (AES), the same cryptography technology recommended by the federal government to secure sensitive documents. AES uses a 128-bit key length, which means there are $3.4 \times 10^{38}$ possible keys for FileVault. In addition, AES relies on a symmetric key cryptographic algorithm that turns the data into cipher text using a four-step transformation process. It performs this transformation 10 times for 128-bit encryption and 14 times for 256-bit encryption.

### Encrypted disk images

The Disk Utility tool included in Mac OS X enables you to create encrypted disk images—using 128-bit or even stronger 256-bit AES encryption—so you can safely email valuable documents, files, and folders to friends and colleagues; save the encrypted disk image to CD or DVD; or store it on the local system or a network file server. A disk image is a file that appears as a volume on your hard drive; it can be copied, moved, or opened. When the disk image is encrypted, any files or folders placed in it are encrypted automatically.



Save As: EncryptedStuff
Where: Documents
Volume Name: Encrypted stuff
Volume Size: 100 MB
Volume Format
Encryption: ✓ 128-bit AES encryption (recommended)
none
256-bit AES encryption (more secure, but slower)
Partitions:
Image Format: read/write disk image

Create encrypted disk images using strong 128- or 256-bit AES encryption.

To see the contents of the disk image, including metadata such as filename, date, size, or any other properties, a user must enter your chosen password or have a keychain with the correct password. The file is decrypted in real time, only as the application needs it. For example, if you open a QuickTime movie from an encrypted disk image, Mac OS X decrypts only the portion of the movie currently being read from disk.

### Secure Empty Trash

Mac OS X includes a Secure Empty Trash command that removes all traces of deleted files from your hard drive, preventing them from being recovered by unauthorized users. In most cases, when a file is deleted from a personal computer, the file's name and location are removed from the disk's directory. However, the file itself remains intact until the space it occupies on the hard drive is needed to store another file. To safeguard against accidental erasures, several commercial utilities enable you to search for and recover these "deleted" files, which presents a security risk if the deleted file is recovered by unauthorized users. The Secure Empty Trash command overwrites the area of the hard drive used by the recently deleted file, making it virtually impossible to recover the original data. Secure Empty Trash uses a rigorous protocol that takes seven successive passes to overwrite the data.

### Encrypted virtual memory

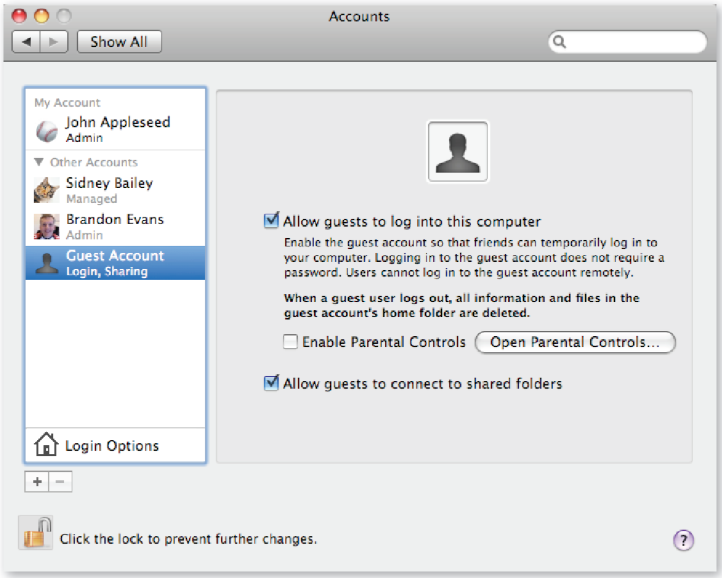
Virtual memory is used like random-access memory (RAM) to store temporarily needed information on your disk drive for quick retrieval. This virtual or "swap" memory area can contain important, confidential information. With Mac OS X, you can encrypt this area of memory so that it remains protected and not visible to others. Encrypted virtual memory is enabled by default for all current portable systems running Mac OS X.

### Private Browsing

The Safari web browser in Mac OS X saves the contents of web pages you open in a cache so that it's faster to visit them again. With the optional Private Browsing feature, the history and cached information about your surfing habits are not stored or recorded. This provides a way to keep your surfing habits private and not recoverable later.

### Guest account

In Mac OS X, you can use the new guest user account to allow anyone to surf the web and check email as a guest on your Mac. When a user logs out of the guest account, Mac OS X deletes the account, removing all files associated with the user's activity. Each time someone logs in as a guest, he or she gets a fresh, unused account.



☑ Allow guests to log into this computer

Enable the guest account so that friends can temporarily log in to your computer. Logging in to the guest account does not require a password. Users cannot log in to the guest account remotely.

**When a guest user logs out, all information and files in the guest account's home folder are deleted.**

□ Enable Parental Controls

☑ Allow guests to connect to shared folders

Click the lock to prevent further changes.

## Open Source Software

Apple built the foundation of Mac OS X and many of its integrated services with open source software—such as FreeBSD, Apache, and Kerberos, among many others—that has been made more secure through years of public scrutiny by developers and security experts around the world. Strong security is a benefit of open source software because anyone can freely inspect the source code, identify theoretical vulnerabilities, and take steps to strengthen the software. Apple actively participates with the open source community by routinely releasing updates of Mac OS X that are subject to independent developers' ongoing review and by incorporating improvements. An open source software development approach provides the transparency necessary to help ensure that Mac OS X is truly secure.

## Rapid Response

Apple works with the incident response community, including the Forum of Incident Response and Security Teams (FIRST) and the FreeBSD Security team, to proactively identify and quickly correct operating system vulnerabilities. In addition, Apple cooperates closely with organizations such as the Computer Emergency Response Team Coordination Center (CERT/CC), so security notifications are distributed to their security constituents at the same time they are sent to Apple customers.

Up-to-date security-related information is posted on the Apple website and distributed to mailing list members via digitally signed email. Mac OS X also includes Software Update, a mechanism that automatically notifies you when security patches are available. These updates are digitally signed, so you can be sure they're coming from a trusted source when you install them. For additional protection, Apple does not disclose, discuss, or confirm security issues until a full investigation has occurred and any necessary updates are available. Additional information is available at www.apple.com/support/security/.

## Security Configuration Guidance

Apple works together with a number of agencies in the U.S. government to develop guidance for the secure configuration of Mac OS X. The most recent security configuration guide for Mac OS X is located at www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml.

## Mac OS X: The Power of UNIX, the Simplicity of Mac

Security features in Mac OS X provide solutions for protecting data at all levels—from the operating system to applications to networks such as the Internet. Whether you are connected to a wired network or are wireless and on the go, your Mac is highly secure right out of the box.

## For More Information

To find out more about Mac OS X, visit www.apple.com/macosx.

August 2009 L416018A