Security in Mac OS X

Safety by design.

Features

Security built in
- Communication ports closed by default
- Personal firewall to protect network services
- Open source foundation
- UNIX user-based file permissions
- Common Data Security Architecture (CDSA)
- Systemwide support for X.509 certificates
- Automatic updates via Software Update

Standards-based authentication
- Kerberos for secure single sign-on authentication to network resources
- Directory authentication using any LDAPv3 service or Active Directory
- L2TP or PPTP for accessing virtual private networks (VPNs)
- NTLMv2 support for increased compatibility with Microsoft technology

Confidentiality of data
- Protection of home directory data using FileVault with 128-bit AES encryption
- Highly secure data portability with strong encryption of disk images
- Keychain for securely storing personal passwords, digital certificates, and notes
- Support for multiple users with discrete passwords and home directories on a single computer

Secure network communications
- SSL and TLS for secure, encrypted transport of information
- Encrypted WebDAV via SSL
- S/MIME for signing and encrypting email

Networking security standards
- Built-in 802.1X client for port-based authentication on wireless networks
- SSH for secure remote access to the command line
- Integrated internal firewall based on IPFW

Security has never been a more important consideration when selecting a computer platform. Whether you're a home user with a broadband Internet connection, a professional with a mobile computer, or an IT manager with thousands of networked systems, you need to safeguard the confidentiality of information and the integrity of your computers.

Apple is working to ensure that your Mac is safe and secure by implementing a security strategy that is central to the design of Mac OS X.

- **Secure default settings.** When you take your Mac out of the box, it is configured to be secure on the Internet, so you don't have to be a security expert to set up your system.
- **Modern security architecture.** Mac OS X includes state-of-the-art, standards-based technologies that enable Apple and third-party developers to build secure software for the Mac. These technologies support all aspects of system, data, and networking security required by today's applications.
- **Innovative security applications.** Mac OS X includes features that take the worry out of using a computer. FileVault protects your documents using strong encryption, an integrated VPN client gives you secure access to networks over the Internet, and a powerful firewall secures your home network.
- **Open source foundation.** Using open source methodology makes Mac OS X a more robust, secure operating system, as its core components have been subjected to peer review for decades. Problems can be immediately identified and fixed by Apple and the larger open source community.
- **Rapid response.** Because the security of your system is so important, Apple responds rapidly to provide patches and updates. Apple works with worldwide partners, including the Computer Emergency Response Team (CERT), to notify users of potential threats. Should vulnerabilities be discovered, the built-in Software Update tool automatically notifies users of security updates, which are made available for easy download and installation.

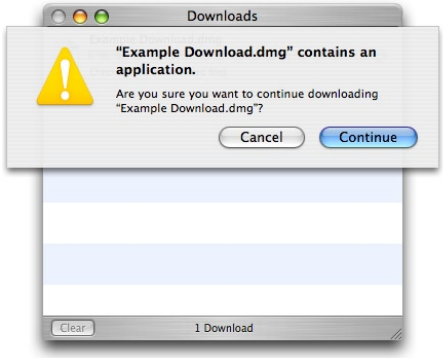
Secure Default Settings

The first time you turn on a Mac, the system is set up securely. Apple sets up the system with secure default settings so you don't need a security expert to keep your data and system safe.

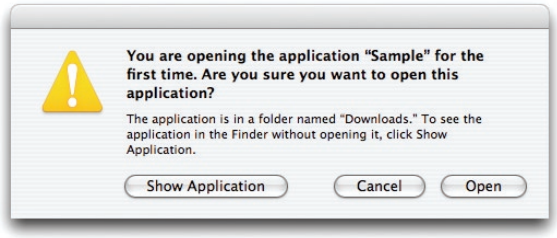
Secured ports. Mac OS X—unlike many operating systems—ships with all communication ports fully secured. Communication ports enable your computer to communicate with other systems on the network via services such as file, web, and printer sharing. Insecure ports can provide an opening into your computer through which intruders can enter. Mac OS X protects your computer and your network by shipping with all ports closed, allowing only an administrator user to open them as needed. Once opened to allow communication between computers, the sharing services in Mac OS X are highly secure, benefiting from years of review by security experts in the open source community.

Safe attachment handling. Files sent to you through mail or other programs are not automatically opened, as they may contain harmful code. This helps you to make sure that the only programs running on your Mac are the ones that you want to run.

Safe-download validation. When you download files in Safari and Mail, Mac OS X analyzes the file to determine whether it contains an application. If the file appears to contain an application, you are asked to confirm whether to continue with the download—giving you the opportunity to avoid inadvertent installations on your system.



New-applications warning. When you open an application manually, you are making an explicit choice. But when you double-click a document or click a URL, you may not know which application will open it. The new-applications warning alerts you before the system opens an application for the first time.



You can either 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 the application. Applications included with your computer are considered trusted and do not trigger the warning.

User permissions model. Mac OS X gains its secure user model from a robust, open source UNIX core. Apple has furthered this security model by disabling the root account by default, a method known as "running with least privileges." By running code with the minimum necessary level of privileges, Mac OS X helps to 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 and cannot affect 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

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

- **Admin.** Mac OS X establishes an admin user account when the system is first installed. The admin user can perform most of the operations normally associated with the root user. The only thing the admin user is prevented from doing is directly adding, modifying, or deleting files in the system domain. However, an administrator can use the Installer or Software Update applications for this purpose. For additional protection, settings that affect the system are locked and can be changed only by an administrator.
- **Root.** Mac OS X defines a superuser, named root, who has full permissions for access to all files on the system. That is, root can 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 approach prevents viruses or unauthorized users from making harmful changes to the operating system.

  In addition to the major types of user accounts, there are system services and software that require specialized access to certain system components, but do not require login access. Mac OS X uses less privileged system accounts to execute these functions.

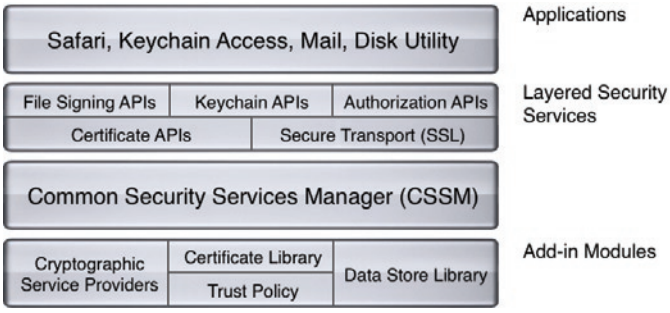
  New-user creation. To prevent unauthorized users from altering the system in an undesirable way, new users do not have administrative privileges unless assigned by the administrator. As users are added to the system, Mac OS X assigns them non-administrative user accounts and prompts them to choose a password, providing a means of authenticating authorized users.

  Safe mail attachment handling. The Mail application built into Mac OS X is designed to handle attachments with extreme caution. It does not run scripts, execute code, or open applications automatically. If you attempt to open an attachment that contains scripts or application code, an appropriate warning is issued and must be acknowledged before the program will proceed.

Modern Security Architecture

Physical security
Security begins with your hardware. To protect your system from theft, all Apple computers have internal slots for inserting Kensington locks. In addition, the Power Mac G5 enclosure has a locking mechanism built into the side panel latch, keeping valuable internal components safe from theft or tampering.

Mac OS X security services are built on the Common Data Security Architecture (CDSA), with support for cryptography, certificate management, trust policy management, and key recovery. This layered security infrastructure makes it easy for Apple and Mac OS X developers to integrate leading-edge security features, such as authentication and encryption, into their applications.



Easy Management Using System Preferences

Privacy controls
Many junk mailers use HTML-based messages to track your email address. When your mail application downloads an image from an HTML message, it tells the sender that your address is valid and ready to receive more junk mail. To protect the privacy of your inbox, you can change your Mail settings to inhibit the display of images in HTML messages—while leaving you the option to load images for individual mail messages.

Mac OS X consolidates all your security settings in one convenient, intuitive interface. The Security preferences pane makes it easy to activate FileVault, require a password to wake the computer or unlock secure system preferences, and set login and logout preferences.

FileVault secures your entire home folder by encrypting its contents.

Strong Authentication

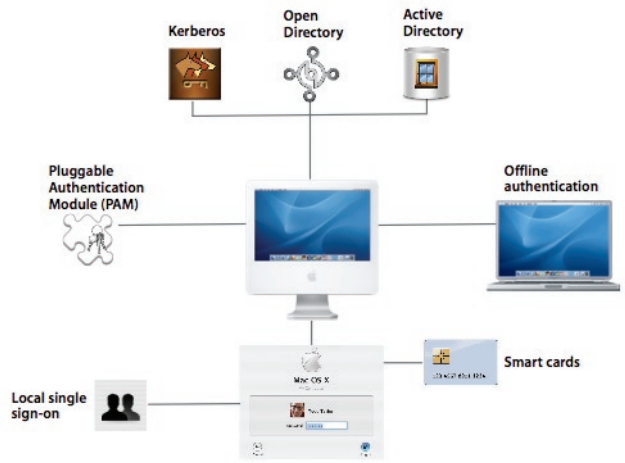
Authentication is the process of verifying the identity of a local or network user. Mac OS X supports local and network-based authentication to ensure that only users with valid authentication credentials can access the computer's data, applications, and network services. Passwords can be required at login, to wake the system from sleep or a screen saver, to install applications, or to change system settings. In addition, Mac OS X supports emerging authentication methods, such as smart cards and biometric readers (for example, thumbprint readers) from third-party developers.

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 authorize individuals to access specified resources, while restricting others from these privileges. Authorizations include permission to change what appears in the Dock, modify system preferences, change passwords, burn CDs or DVDs, install software, launch applications, and access printers.

Biometric devices
Mac OS X supports emerging biometrics-based authentication technologies, such as thumbprint readers. Password-protected websites and applications can now be accessed without having to remember a long list of passwords. Some biometric devices allow you to authenticate simply by placing your finger on the pad. Unlike a password, your fingerprint can never be forgotten or stolen. Fingerprint identity products provide personal authentication and network access, as well as more robust public key infrastructure (PKI) transactions, personal digital certificates, and virtual private networks.

Authentication Methods



Local single sign-on. Mac OS X enables you to sign on only once, obtaining your single sign-on credentials from the keychain for local authentication or from directory services for network authentication. This means you can use the same user name and password combination for all privileges.

Smart cards. USB smart card readers enable you to carry your digital certificates with you. This robust, two-factor authentication mechanism complies with the Department of Defense Common Access Card and Java Card 2.1 standards. Similar to an ATM card and 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.

Pluggable Authentication Modules (PAMs). The Mac OS X security architecture supports Pluggable Authentication Modules, enabling all 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. This means 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 2, the latest version of Apple's standards-based directory services architecture, for storing password enforcement policies and authentication credentials in a robust, central repository. By assigning parameters to the passwords, such as password length, types of characters needed, and expiration time, administrators can require users to pick more secure passwords.

Kerberos. Open Directory integrates MIT's open source Kerberos Key Distribution Center (KDC) for secure access to 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 type in your password only once at login to prove your identity to the Kerberos authentication authority, or KDC. In response, the 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 Safari, SSH, SMB, Mail, Telnet, VPN Client, and the AFP (Apple Filing Protocol) client.

Active Directory. Mac OS X allows users to participate on 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, Mac and Windows, permitting Mac OS X users to log in and authenticate to Microsoft's proprietary Active Directory—without any specific changes to accommodate Mac OS X users.

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

Confidentiality of Data

Mac OS X protects the confidentiality of your data, whether it is stored in your home directory, traveling across the Internet, or shared locally on your network.

How tight is AES encryption?
128-bit AES encryption uses on the order of 10^{21} times more keys than its predecessor, the Digital Encryption Standard, or DES, which used 56-bit keys, or 7.2 x 10^{16} keys. In the late 1990s, specialized "DES Cracker" machines were built that could recover a DES encryption key after a few hours. Let's imagine a phenomenal machine that could crack a DES key in a second, rather than a few hours. It would take that mythical machine approximately 149 thousand billion (149 trillion) years to crack a 128-bit AES key.

FileVault

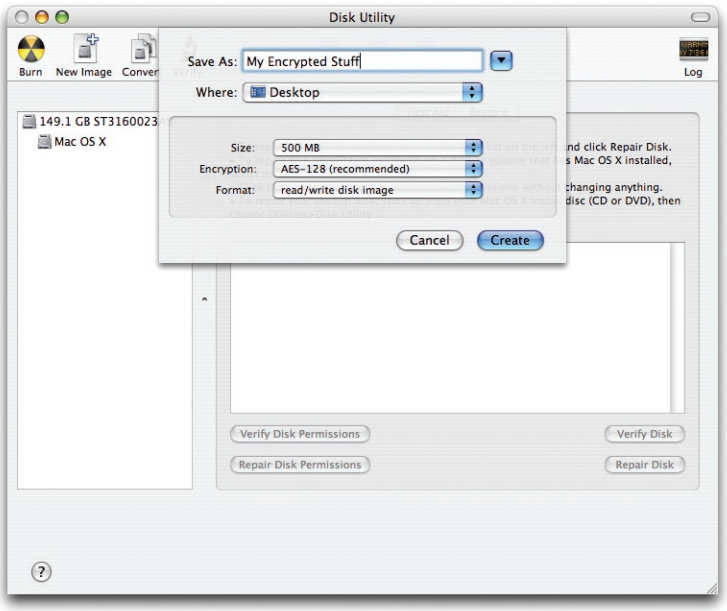
FileVault keeps your documents secure even if your computer is lost or stolen, by storing them in encrypted form in your home directory—preventing unauthorized users, applications, or utilities from reading them. With FileVault enabled, all the information in your home directory is always encrypted. 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 re-encrypted 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 x 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. The result of each pass serves as the origin of the next pass, yielding an encrypted block of data with no known successful method of attack.

Master password
For extra security and control, a master password can unlock your FileVault-protected home directory in case you forget or lose your password. This computerwide password is particularly useful for system administrators who need to keep company data accessible, even if employees forget their password or leave the company. (If the user login password and the master password are both forgotten, the files will be lost forever.)

Encrypted disk images

The Disk Utility tool included in Mac OS X enables you to create encrypted disk images—using the same 128-bit AES encryption as FileVault—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.



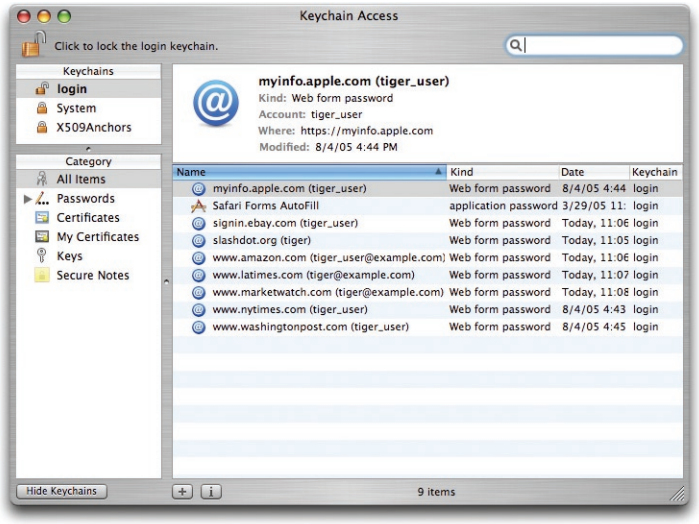
Create encrypted disk images using 128-bit AES encryption.

To see the contents of the disk image, including the metadata, such as file name, 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 playing.

Store more in your keychain
In addition to passwords, keychains can be used to store notes and other 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.

Keychain for storing passwords

With a greatly improved interface, the Mac OS X keychain provides a convenient, secure repository for your various user names and passwords. 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. With the keychain, it has never been easier to be secure. 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 type in—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.



The keychain securely stores user names and passwords.

All of 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. This is because all keychain information is decrypted only on the local client system as applications request it; it is never transmitted over the network.

You can synchronize the keychains on all of your Mac systems with iSync. Using more than one Mac has never been so easy and secure.

Secure Empty Trash
Each time you securely empty the Trash, Mac OS X uses a seven-step algorithm to prevent the data from ever being recovered:

- Overwrite file with a single character
- Overwrite file with zeroes
- Overwrite file with a single character
- Overwrite file with random characters
- Overwrite file with zeroes
- Overwrite file with a single character
- Overwrite file with random characters

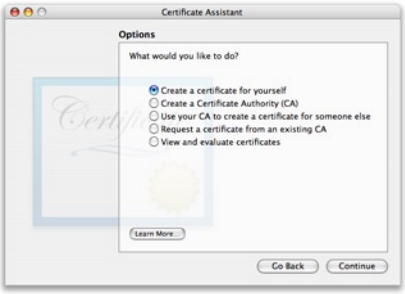
Permanent file deletion

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—presenting a security risk if the deleted file is recovered by unauthorized users. The Secure Empty Trash command removes all traces of your deleted files from your hard drive. Secure Empty Trash uses a rigorous protocol that follows the U.S. Department of Defense standard for the sanitization of magnetic media.

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. This optional setting is available in the Security pane of System Preferences.

Obtaining a digital certificate
Before you can start sending digitally signed messages, you must obtain a digital certificate that identifies you and copy it to the keychain. Certificates can be obtained from your system administrator, public Certificate Authorities (CAs), or special CAs within your organization.



Certificate Assistant
Certificate Assistant is an easy-to-use utility that helps you request, issue, and manage certificates. It contains all of 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 with none of the cost. The certificates created by Certificate Assistant can be used to send encrypted email, log in to protected websites, or participate in secure chat sessions with iChat.

Technology in Mac OS X that can use digital certificates
Safari
Keychain
VPN Client
Mail
Apache
iChat
Certificate Assistant
Login window with a smart card
Address Book
Access control lists (ACLs)

Secure Network Communications

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

Secure Internet communications with SSL and TLS
Mac OS X includes SSL versions 2 and 3, today's most common transport mechanism, as well as Transport Layer Security (TLS), the next-generation security standard for the Internet. Safari and other Internet applications automatically start these transport layer mechanisms to provide a secure, encrypted channel between two systems and to protect the information in the channel from eavesdroppers. For maximum protection, Safari and Mail support 40- and 128-bit SSL encryption.

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 at a later time.

Digital certificates
The use of digital certificates enables Mac OS X to support secure communications. Similar to showing a driver's license, digital certificates enable these important security services:

- **Authentication.** Digital certificates guarantee the identity of the author or "signer."
- **Data integrity.** Digital certificates ensure that messages have not been changed or altered, whether accidentally or maliciously.
- **Encryption.** Digital certificates can encrypt messages to help protect confidential or private information.
- **Nonrepudiation.** Digital certificates enable the recipient to verify the identity of the signer in connection with 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 keychain of the sender must contain a digital certificate for the recipient; 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 your public key are included with the message, allowing recipients to send you encrypted messages in reply.

For secure 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 set up the secure session with SSL encryption, to verify the site's identity and that your communication with the website in 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.

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 over email, you can import the certificate into your keychain for later use. If a certificate's authenticity cannot be verified, you will be presented with a warning before it is added to your keychain.

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 ensures data security while traversing local area networks as well as the Internet. In addition, virtual private networking (VPN) uses Layer 2 Tunneling Protocol (L2TP) or Point-to-Point Tunneling Protocol (PPTP) to support secure communications to your work or home network.

Secure Mac OS X Networking

Configuring 802.1X clients
Mac OS X makes it easy to set up authenticated users on wireless networks.

Secure 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), Transport Layer Security (TLS), and Tunneled Transport Layer Security (TTLS).

The 802.1X solution 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 over 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 secure wireless communications.

Secure Shell (SSH)
For secure command-line access to remote systems, Mac OS X uses SSH in place of clear-text Telnet sessions. SSH encrypts remote command-line data, such as passwords, to help eliminate eavesdropping and other network-level intrusions.

SecureID
RSA offers several types of SecureID hardware tokens, including one that can be attached to a keychain so it's always handy.

Virtual private network (VPN)

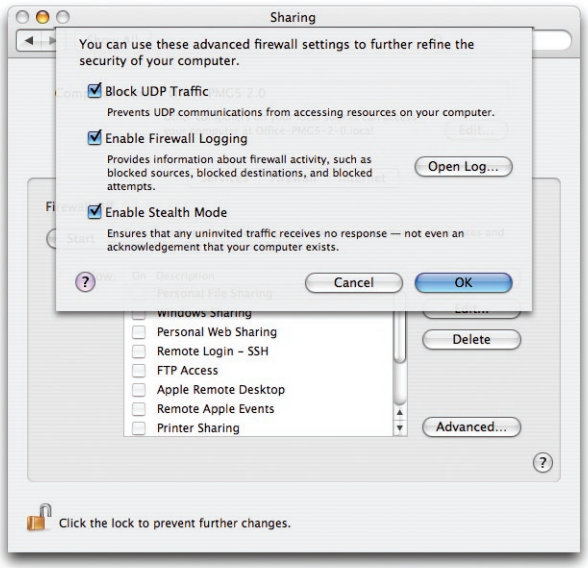
Mac OS X Tiger includes a universal VPN client with RSA SecureID support built into Internet Connect, so you have everything you need to establish a secure connection. The VPN client supports L2TP over IPSec and PPTP, which make Apple's VPN client compatible with most VPN servers, including those from Microsoft and Cisco. You can also use digital certificates and RSA SecureID hardware tokens for authentication in conjunction with the VPN client. SecureID 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.

Apple's L2TP VPN client can connect you to protected networks automatically by using its "VPN on demand" feature. VPN on demand can detect when you want to access a network that is protected by a VPN server and automatically start the connection process for you. This means that your security is increased because VPN connections can be closed when not in use, and you can work more efficiently.

Personal firewall

By monitoring incoming network traffic, Mac OS X can act as a firewall to protect your home network from unauthorized access. The integrated firewall is based on IPFW, a FreeBSD technology that protects the most mission-critical UNIX computers on the Internet. Personal firewall settings are defined in the Sharing preference pane, with simple checkboxes to enable or disable monitoring of services. In addition, the personal firewall can be customized for communications such as Internet Relay Chat (IRC), games, or other user-definable services.

For increased protection, advanced firewall features are available through easy-to-configure checkboxes. Stealth mode hides your Mac on the Internet by dropping unsolicited communication packets, making it appear as though no Mac is present. UDP packets can be blocked, restricting network traffic to TCP packets only for open ports. The firewall also supports logging, an important tool for checking on unwanted activity.



Set up a personal firewall to protect your home network.

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 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 ensure that Mac OS X is truly secure.

This open approach starkly contrasts with the closed, single-vendor review model, which has a long and well-documented history of exploited vulnerabilities. Instead of depending on private examinations performed by closed source vendors, Mac OS X users can comfortably rely on the ongoing public examination by large numbers of security experts, which is made possible by Apple's open approach to software development. The result is an operating system that is inherently more 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 to 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.

Mac OS X: Power of UNIX, Simplicity of Macintosh

Security features in Mac OS X provide solutions for securing 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 secure right out of the box. In addition, Mac OS X Tiger offers more than 200 innovative new features, including Spotlight, a desktop search technology that instantly finds anything on your computer; Automator, for easily automating complex or repetitive tasks; and Dashboard, which provides desktop accessories that instantly appear on your screen with the touch of a key.

For More Information

For more information on security in Mac OS X, visit www.apple.com/security. For more information about Mac OS X, visit www.apple.com/macosx.