



# Security in Mac OS X

Advanced security features and a conservative approach ensure the privacy of your data and the integrity of your Mac systems.

## Features

### Security built in

- Open source foundation
- UNIX user-based file permissions
- Common Data Security Architecture (CDSA)
- Communication ports closed by default
- Personal firewall to protect network services
- 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)

### 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
- 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

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.

With Mac OS X, Apple has implemented a security strategy that is central to the design of the operating system, ensuring that your Mac is safe and secure.

- **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.
- **Secure default settings.** When you take your Mac out of the box, it is already configured in the most secure form—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.
- **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 any 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.

## Technology Brief

Mac OS X: Security

## 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 by years of public scrutiny from developers and security experts around the world. Strong security is a benefit of open source software since 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.

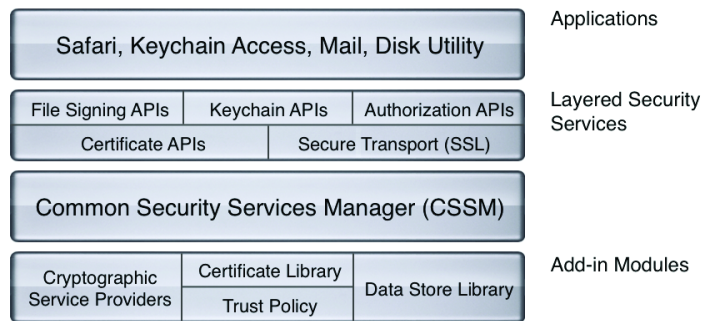
This open approach starkly contrasts with the closed, single-vendor review model, which has a long and well-documented history of exploited vulnerabilities. Instead of depending on private examinations performed by closed source vendors, Mac OS X users can comfortably rely on the ongoing public examination 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.

## Modern Architecture

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.

### 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.



## Secure Default Settings

The first time you turn on a Mac, the system is set up securely. Apple has applied the most secure settings as the default configuration, so you don’t need a security expert to keep your data and system safe.

### 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.

- **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 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.

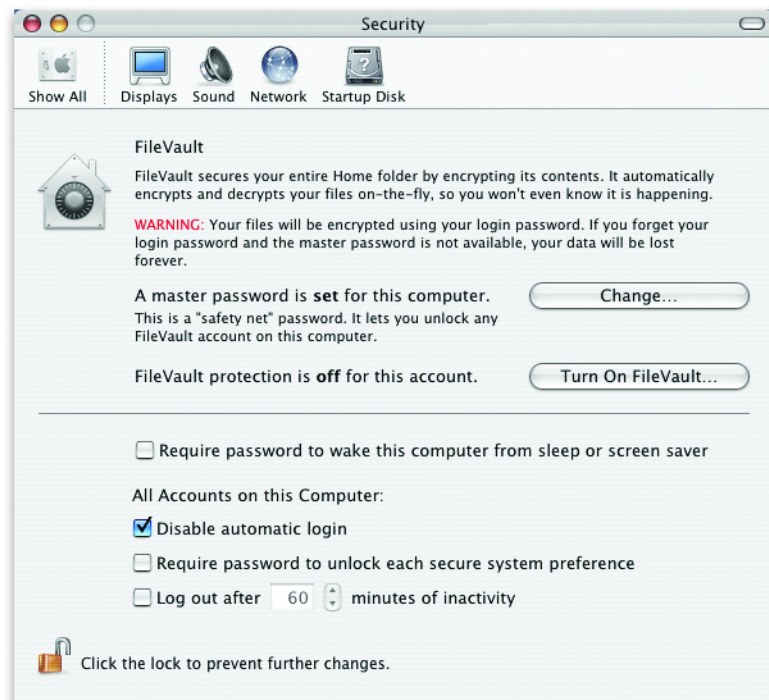
- **Administrative control.** The initial user of any Mac OS X computer is assigned the role of administrator and is granted administrator privileges. The administrator has authorization to install system software or other software that modifies the system files, such as an antivirus utility. For additional protection, settings that affect the system are locked and can be changed only by an administrator.
- **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.
- **Disabled root account.** On UNIX-based systems, the root account is used for configuring and modifying applications and services from the command line—providing unlimited access to the computer. Unlike traditional UNIX systems, Mac OS X disables this powerful account by default. This prevents viruses or unauthorized users from making harmful changes to the operating system.
- **Safe mail attachment handling.** The Mail application built into Mac OS X is designed to handle attachments with extreme caution. It will 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.

### Privacy controls

Many junk mailers use HTML-based messages to track your email address. When your mail application downloads an image from an HTML file, it tells the junk mailer that your address is valid and ready to receive more junk mail. To thwart these intrusions, you can set Mail to never load images that are part of HTML-based messages.

## Easy Management Using System Preferences

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.

### 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.

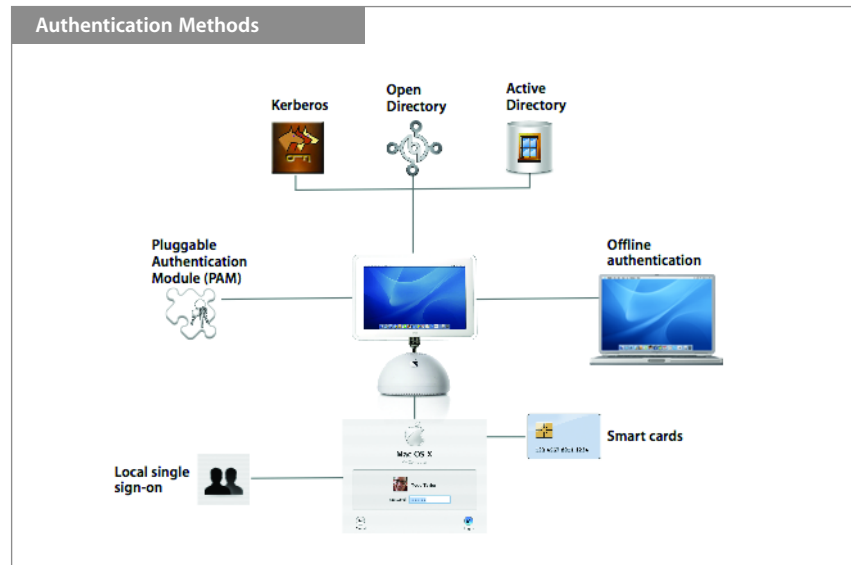
For added control, the administrator can authorize individuals to access specified resources, while restricting others from these privileges. Authorizations include permission to change what appears in the Dock, modify system preferences, change passwords, burn CDs or DVDs, install software, launch applications,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

## 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 authorized users 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 from third-party developers (for example, thumbprint readers).



- **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 standards-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 version 10.3 “Panther” 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, 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.

## Confidentiality of Data

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

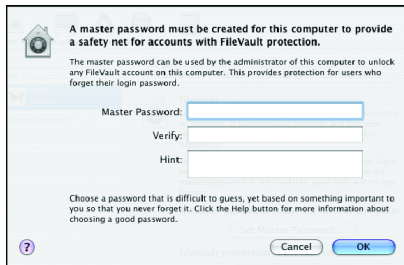
### FileVault

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 times  $10^{38}$  possible keys for FileVault. (Before AES was developed, the Digital Encryption Standard, or DES, used 56-bit keys, or 7.2 times  $10^{16}$  keys.) 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.

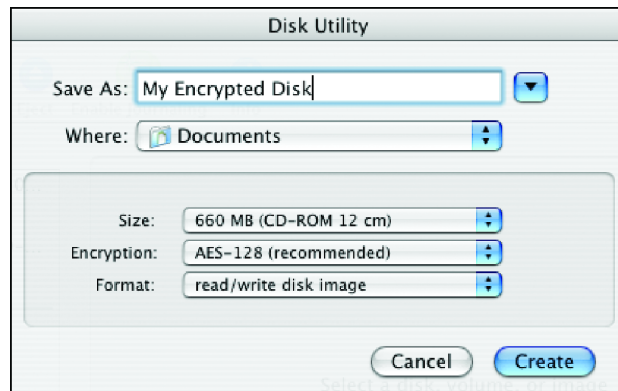
### Encrypted disk images

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.



### 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 computer-wide 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.)



Create encrypted disk images using 128-bit AES encryption.

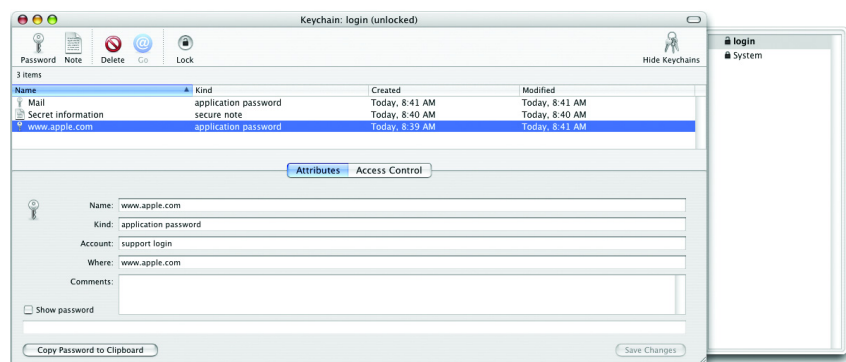
To see the contents of the disk image, including the metadata, such as file name, date, size, or any other properties, a user must enter your chosen password or have a keychain with the correct password. The file is decrypted in real time, only as the application needs it. For example, if you open a 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

The Mac OS X keychain provides a convenient, secure repository for your various user names and passwords. With one login password, your keychain is unlocked, allowing you to 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.

### 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 Panther 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. 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 in Panther removes all traces of your deleted files from your hard drive. Permanent file deletion uses a rigorous protocol that follows the U.S. Department of Defense standard for the sanitization of magnetic media.

## 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

Panther 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.

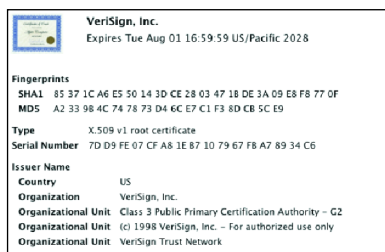
### Digital certificates for encrypting email and web communications

The Secure Multipurpose Internet Mail Extensions (S/MIME) specification enables Apple's Mail application to support digital certificates for securing email 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, ensuring that only authorized recipients are able to read them.
- **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 on the Internet. Easy to deploy and highly scalable, digital certificates can be implemented systemwide and shared among



### 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.

multiple applications. With support for the X.509 standard, Mac OS X now 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 Panther 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.



### Configuring 802.1X clients

Mac OS X Panther 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 Tunnled 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.



### SecureID

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

### Secure Shell (SSH)

For secure command-line access to remote systems, Panther 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.

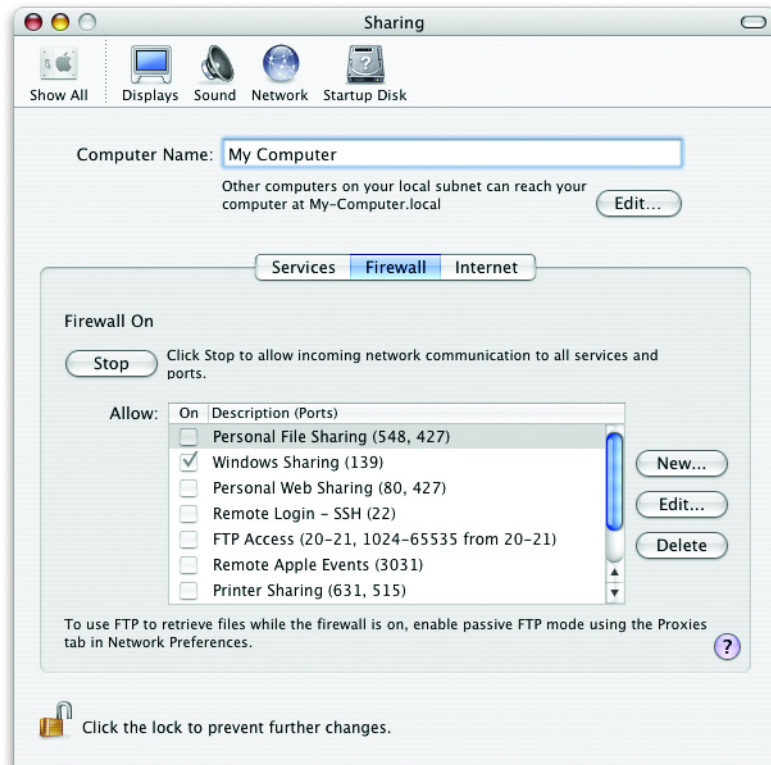
### Virtual Private Network (VPN)

Mac OS X includes a Virtual Private Network (VPN) client for secure remote access to your corporate or home network over the Internet. The standards-based VPN client supports L2TP and PPTP for compatibility with most VPN servers, including those from Apple, Microsoft, and Cisco.

The L2TP VPN client features integrated support for RSA's SecureID system, combining user passwords with randomly generated numbers. In addition, any number of VPN connection settings can be saved as "locations," so you don't have to reconfigure your system each time you connect to a different network.

### 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 preferences 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.



Set up a personal firewall to protect your home network.

## 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 Version 10.3 "Panther": Power of UNIX, Simplicity of Macintosh

Security features in Mac OS X Panther provide solutions for securing data at all levels—from the operating system to applications to networks such as the Internet—whether you are wired to a network or wireless and on the go. Panther is secure right out of the box. In addition, Panther offers more than 150 new features and innovations, including iChat AV for personal video conferencing, Exposé for instantly finding any window, and a new Finder for easy access to everything you need. It's like having an all-new Mac.

## For More Information

For more information on security in Mac OS X, visit [www.apple.com/security](http://www.apple.com/security).  
For more information about Mac OS X Panther, visit [www.apple.com/macosex](http://www.apple.com/macosex).

© 2004 Apple Computer, Inc. All rights reserved. Apple, the Apple logo, Keychain, Mac, Macintosh, Mac OS, Power Mac, and QuickTime are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Exposé, Finder, iChat, Panther, and Safari are trademarks of Apple Computer, Inc. Mac is a service mark of Apple Computer, Inc. Java is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies. Product specifications are subject to change without notice. This material is provided for information purposes only; Apple assumes no liability related to its use. March 2004 L302768A