The logo features the text "F-SECURE" in a bold, black, sans-serif font, positioned above a stylized shield emblem. The shield is composed of several overlapping, nested shapes in shades of purple and black, creating a complex, geometric design. The entire logo is set against a circular, light-colored background that appears to be a globe or a similar spherical object with a grid pattern.

F-SECURE

F-Secure SSH 2.4

for Macintosh

Secure Remote Login and System Administration

User's Guide

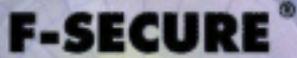
"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

SSH is a registered trademark and Secure Shell is a trademark of SSH Communications Security Corp (www.ssh.com).

Copyright © 2002 F-Secure Corporation. All rights reserved.

#12000057-1L20

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol. Below the text is a stylized, black and white geometric symbol resembling a shield or a stylized letter 'F'.

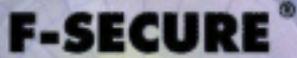
Contents

1. Welcome!	1
1.1 System Requirements	1
1.2 Overview	2
The F-Secure SSH Product Family	2
F-Secure SSH Client	2
1.3 About the SSH Protocol	3
1.4 Public-Key Authentication	3
User Authentication	4
Cryptographic Methods	5
2. F-Secure SSH 2.4 for Macintosh	7
2.1 Overview	7
2.2 Installation Guide	7
2.3 Getting Started With SSH	8
Setting up your preferences	8
Creating a Terminal Connection with SSH	9
Configuring tunneling	11
SSH1 compatibility	13
Conclusion	13
2.4 Using the Menus	14
File Menu	14

Edit Menu	15
SSH Menu	16
Shortcuts Menu	17
Help Menu	17
2.5 Connection Manager	18
Managing Groups	18
Connection Manager Window	19
2.6 Group Properties	21
Group Properties—Document	21
Group Properties—Connect	22
Group Properties—Security	24
2.7 Using Terminals	25
Creating a new Terminal Connection	25
Opening an Existing Terminal Connection	26
Saving a Terminal Connection	26
Selecting a Terminal Window as the Active Window	26
Connecting and Disconnecting from the Host	27
Cloning the Terminal	27
Hiding a Terminal Window	27
Removing a Terminal from the Connection Manager	28
Working with Text in the Terminal Window	28
2.8 Terminal Properties	28
Terminal Properties — Document	29
Terminal Properties—Connect	30
Terminal Properties—Security	32
Terminal Properties—Emulation	33
Terminal Properties—Keyboard	35
Terminal Properties- X11	36
2.9 Tunnels (TCP, E-Mail, FTP)	37
Creating a New Tunnel	37

Opening an Existing Tunnel	38
Saving a Tunnel	38
Selecting a Tunnel	38
Connecting and Disconnecting from the Host	38
Cloning the Tunnel	39
Removing a Tunnel from the Connection Manager	39
2.10 Tunneling Properties (TCP, E-Mail, FTP)	39
Tunneling Properties—Document	40
Tunneling Properties—Connect	41
Tunneling Properties— Security	43
TCP Tunneling Properties - Tunneling	44
E-Mail Tunneling Properties-Services	46
FTP Tunneling Properties-FTP Server	47
Tunneling Properties—Access	48
2.11 F-Secure SSH2 Preferences	49
Connections Preferences	50
Security Preferences	51
Link Sharing Preferences	52
Firewall Preferences	54
Errors Preferences	54
Terminal Preferences	55
Emulation Preferences	57
Keyboard Preferences	58
X11 Preferences	59
Interface Preferences	60
2.12 Public-key authentication	61
Transferring the Public Key	62
Technical Support	65
Web Club	65
Electronic Mail Support	65

About F-Secure Corporation	68
The F-Secure Product Family	69

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol. Below the text is a stylized, dark blue and black shield-like graphic with a white 'F' shape inside.

1. Welcome!

Welcome to F-Secure SSH, the secure remote login program. F-Secure SSH replaces your existing terminal applications to provide you with secure encrypted and authenticated connections to your UNIX host computers.

NOTE:

This chapter discusses generic SSH features that vary slightly between different versions and platforms.

F-Secure SSH provides protection for a wide range of security areas. By encrypting interactive terminal and X-window sessions, eliminating plain text passwords, and providing other services, F-Secure SSH closes the most significant authentication and security holes in a distributed computer environment.

This is achieved using strong encryption in the state-of-the-art security protocol SSH. SSH uses both symmetric and asymmetric encryption algorithms to protect your network connections.

1.1 System Requirements

F-Secure SSH 2.4 for Macintosh requires MacOS 8.x or 9.x. MacOS X is not officially supported yet, but SSH 2.4 appears to function well on it.

1.2 Overview

The F-Secure SSH Product Family

F-Secure SSH products utilize the SSH protocol as a generic transport-layer encryption mechanism, providing both host authentication and user authentication, along with privacy and integrity protection.

F-Secure SSH UNIX Server can be used together with F-Secure SSH Clients for Windows, Macintosh, and UNIX to make secure login connections to remote offices. F-Secure SSH Server for UNIX includes tools for secure systems administration. Tools are provided for secure file transfer and for tunneling of TCP/IP communications.

The encryption technology has been developed in Europe and does not fall under the U.S. ITAR export regulations. F-Secure products can be used globally in every country where encryption is legal, including the USA. F-Secure products are sold with pre-licensed patented encryption algorithms, which provide the strongest security.

F-Secure SSH Client

F-Secure SSH Client provides users with secure login connections over untrusted networks. F-Secure SSH Client acts as a replacement for the telnet protocol, taking advantage of the cryptographic authentication, automatic session encryption, and integrity protection methods defined by the SSH protocol. F-Secure SSH Client supports VT100 terminal emulation and ANSI colors.

F-Secure SSH Client also supports secure TCP/IP port-forwarding technology to connect arbitrary and otherwise insecure connections over a secure channel. TCP/IP port forwarding works by creating a proxy server for a source port that a TCP/IP service uses. The proxy server waits on the local machine for a connection from a client program to the source port. F-Secure SSH then forwards the request and the data over the secure channel to the remote system. The F-Secure SSH server on the remote system makes the final connection to the destination host and the destination port.

Most remote services that use TCP/IP can be secured, including custom client-server applications, database systems, and services such as http, telnet, pop, and smtp. F-Secure SSH also provides automatic forwarding for the X11 Windowing System commonly used on UNIX machines.

1.3 About the SSH Protocol

SSH is a packet-based binary protocol that works on top of any transport that will pass a stream of binary data. Normally, TCP/IP is used as the transport, but the implementation also permits using an arbitrary proxy program to pass data to and from the server. F-Secure SSH supports SOCKS4 proxies.

The packet mechanism and related mechanisms for authentication, key exchange, encryption, and integrity implement a transport-layer security mechanism, which is then used to build secure connections.

1.4 Public-Key Authentication

The industry-standard IP protocol does not provide any security for data being transmitted across networks. It does not provide authentication, privacy, or data integrity. Higher-level protocols do not provide security to the extent that they rely on lower-level protocols to provide that security. Therefore, security measures must be implemented on the application level.

The SSH protocol is an application-level protocol used by all F-Secure SSH products. SSH guarantees authentication of both ends of the connection, and it guarantees the secrecy and integrity of transmitted data.

The server sends its public DSA or RSA host key and a public DSA or RSA “server key” that changes each hour. The client compares the host key it receives against its own database of known host keys. In the SSH1 protocol, RSA is the only option. In the SSH2 protocol, DSA is the default option and RSA is an alternative. In some versions of the SSH2-based software, RSA is not available.

F-Secure SSH Client will normally ask whether to accept the key of an unknown host and if accepted, stores the key in its database for future reference (making SSH practical to use in most environments).

However, F-Secure SSH Client can also be configured to always refuse access to any host that sends an unknown key.

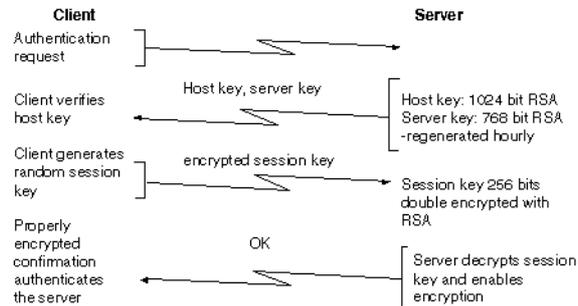


Figure 1: Host Authentication

The client generates a 256-bit random number using a cryptographically strong random number generator, and chooses an encryption algorithm supported by the server (normally Blowfish or three-key triple-des (3des)). The client encrypts the random number (the session key) with RSA, using both the host key and the server key. The client then sends the encrypted key to the server.

The host key is used to bind the connection to the desired server machine. The server key is changed every hour. This key is used to make it impossible to decrypt past recorded traffic if the host key has been compromised. In SSH1, the host key is normally a 1024-bit RSA key, and the server key is a 768-bit key. In SSH2, the host key is by default a 1024-bit DSA key. In some versions of SSH2, RSA keys can be used as an alternative. The keys are generated using a cryptographically strong random number generator.

The server decrypts the session key sent by the client. Both parties start using this session key, and the connection is now encrypted. The server sends an encrypted confirmation to the client. When the client receives the confirmation, it knows that the server had the proper private keys needed to decrypt the session key. The server machine has now been authenticated, and transport-level encryption and integrity protection will be in effect.

User Authentication

The user can be authenticated by the server in a number of ways. The user authentication dialogue is driven by the client, which sends requests to the server. The first request always declares what user name to use when logging on. The server responds to each request with a 'success' or 'failure' response (requiring further authentication).

The following authentication methods are supported:

Traditional password authentication. The password is transmitted over the encrypted channel and cannot be seen by outsiders.

RSA authentication in SSH1 and in some versions of SSH2. Possession of a particular RSA key serves as authentication. The server keeps a list of accepted public keys.

DSA authentication by default in SSH2. Possession of a particular DSA key serves as authentication. The server keeps a list of accepted public keys.

Cryptographic Methods

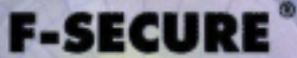
The SSH protocol provides strong security with cryptography. SSH1 uses only RSA for host and user authentication. SSH2 uses DSA by default; RSA is an option. In some versions, RSA is not available.

The server key that changes every hour is 768 bits by default. It is used to protect intercepted past sessions from being decrypted if the host key is later compromised. The server key is never saved on a disk.

Key exchange is performed by encrypting the 256-bit session key twice using RSA. It is padded with non-zero random bytes before each encryption. Server host authentication happens implicitly with the key exchange. Only the holder of the valid private key can decrypt the session key. Receipt of the encrypted confirmation tells the client that the session key was successfully decrypted.

Client-host authentication and RSA user authentication are accomplished using a challenge-response exchange, where the response is MD5 of the decrypted challenge plus data that binds the result to a specific session (host key and anti-spoofing cookie).

The key exchange transfers 256 bits of keying data to the server. Different encryption methods use varying amounts of the key. Blowfish uses 128 bits. Three-key triple-des (3des) uses 168 bits. All random numbers used in SSH are generated with a cryptographically strong random number generator.

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font with a registered trademark symbol. Below the text is a stylized, black and white geometric logo consisting of a large inverted triangle with a smaller, nested triangle inside it, creating a sense of depth and security.

2. F-Secure SSH 2.4 for Macintosh

2.1 Overview

F-Secure Client for Macintosh provides users with secure login connections over untrusted networks. The program supports secure TCP/IP port-forwarding technology to connect arbitrary and otherwise insecure connections over a secure channel.

The F-Secure SSH 2.4 for Macintosh client is compatible with all F-Secure SSH servers.

2.2 Installation Guide

To install F-Secure SSH Client 2.4 for Macintosh, follow these steps:

Double-click the F-Secure Installer icon where you downloaded the application. This opens a simple Save dialog, where you need to enter the keycode for the product and browse for the location to save the product. F-Secure SSH is then installed.

To add an alias to the F-Secure SSH 2.4 Client on the desktop, go to the F-Secure SSH 2.4 folder on your local hard drive and drag the F-Secure SSH 2.4 icon to the desktop while holding down **OPTION+⌘**.

2.3 Getting Started With SSH

The following is a quick walkthrough of the most commonly used SSH features.

Install SSH and launch the application. The Connection Manager window will appear. It's position and size will be remember, so move it to a position of your liking, so that it doesn't obstruct with your workflow and so that it's easily accessible when you need.

Setting up your preferences

Select "Preferences" from the "SSH" menu. A preferences window will open, showing the "Connections" settings.

Enter your most commonly used SSH server name into the default server box.

Enter your most commonly used SSH account name into the default user box. If for instance your name was "Tiffany Rose" and your login name on the SSH server was "trose", you would enter "trose" into that box.

Most of the other preferences are probably going to be OK for now, but you may want to browse through the various preferences panels to see what options are available. Some settings have an immediate effect on the way the program behaves, while others are used to set up default values for new documents and will not affect the way old documents work.

If you would like to use the Keychain manager for storing your passwords and passphrases, move onto the Security panel and click on "Enable keychain". Note that although MacOS stores the passwords and passphrases in encrypted form, they will also be accessible to other applications, if you have configured

your keychain to do make them available. Your user name and hostnames will be accessible to all applications no matter what settings are used, since only the password data is encrypted.

If you commonly use an X11 window server on your Macintosh and wish to secure connections to it, you may want to turn on X11 tunneling by default.

You can now close the preferences window.

Creating a Terminal Connection with SSH

Press command-N to create a new terminal window. The window that opens is the properties window for the terminal. It's similar in appearance to the preferences window, but it directly controls only the settings for this terminal session. These settings can be stored in a connection document for later use.

If you already filled up your favorite host and user names into the preferences, they will appear on the properties window as well. If you are using password authentication, pressing return, enter or ⌘G will connect to the server.



If this is your first time connecting to the server, the SSH client will not know what the public key of the server should be, so it will ask you if it should blindly accept the public key provided by the server as valid and store it for future reference. Server public keys can be imported and exported through the clipboard using the host keys window.

Once a server key is stored, it is remembered and you will only get asked, if it has changed for some reason. If the server key has changed, you should first find out whether it really was changed. If it hasn't

been changed on the server, foul play should be suspected and the connection should be rejected until you can verify that the host you are trying to connect to really is the machine it claims to be.

If the connection succeeds and the host key is accepted, you will then get a dialog prompting you to enter the password.



If keychain use was allowed, the password entry dialog will have a button that allows you to save the entered password into the keychain. To do so, enter the password first and then use the mouse to click on the “store in keychain” button. If you click on “OK” or simply hit enter, the password will not be stored, but you will log in normally.

If SSH1 compatibility had to be used because the server doesn’t support SSH2, you will get a warning message, unless you turned off warnings from the preferences.

If the log in was successful, you should now be connected to your server.

You should save your connection document for future use before closing the window. This will allow you to open the same connection again without having to set up the connection settings manually. To bypass the properties window entirely when the document is opened, go to the “Document” setting panel in the properties and enable “Auto-connect on Open”. The ideal placement for connection documents is in the SSH shortcuts folder. The file will appear in the shortcuts menu the next time you launch SSH.

To disconnect, end the session from the shell (using logout, for instance). You can also use the commands Disconnect (Command-K) or Put Away (Command-Y) from the SSH menus to disconnect from a server.

SSH allows you to clone an existing terminal window simply by pressing Command-D. This will duplicate all the settings in the terminal and automatically connect, if you were already connected. With SSH2, the same authenticated connection can be used for multiple terminal windows. Usually the cloned window will

connect much faster and without any need for authentication and long as one connection with the same settings (user, host, encryption etc) is already open.

Configuring tunneling

Assuming you set up your preferences and you want to connect to your favorite host, tunneling is very easy to set up.

Securing E-mail

First, set up your E-mail program to use 127.0.0.1 as the mail server for SMTP and POP or IMAP (depending on which one you are using).

Then, create an E-mail tunnel using the File->Tunnel->Create E-mail Tunnel command. The default settings will tunnel all three protocols (SMTP, POP and IMAP) and assume that the E-mail server is the same machine as the SSH server. If a different server is used for these protocols, use the “Services” panel to set up the server names before you connect.

Once connected, the connection manager will show the connection status. Traffic is initially 0/0 (zero bytes out and zero bytes in), but will change as soon as a tunnel is used. Observe the traffic status as you use your E-mail client to verify that data is passing through the tunnel (you should usually see traffic even before you need to enter your password for the E-mail server).

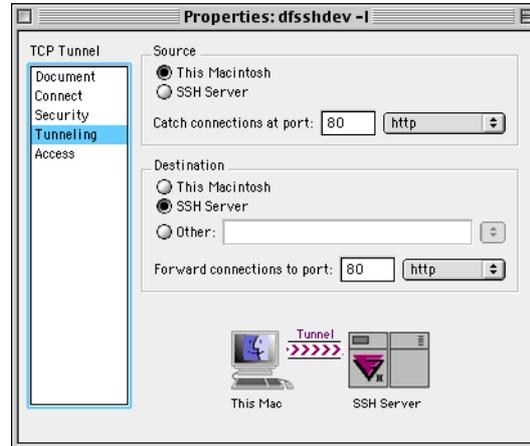
Securing file transfers

While F-Secure SSH 2.4 for Macintosh doesn't provide SFTP (Secure File Transfer Protocol) support, it can entirely secure connections through the older FTP protocol. An ftp client is needed to use this feature and has to be configure to connect to 127.0.0.1 instead of directly to the FTP server.

Securing HTTP connections

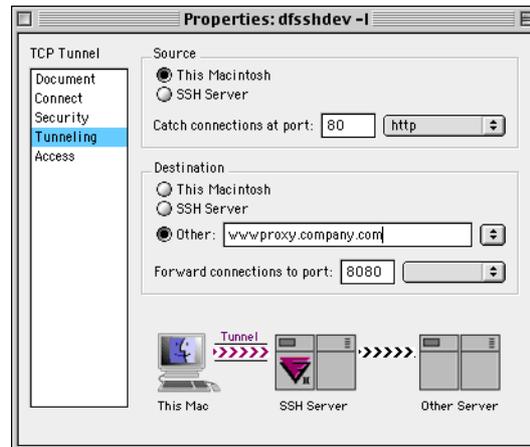
One of the most common uses for tunneling with SSH is to get access to a firewalled company intranet server from outside the firewall. Your SSH server has to be inside the firewall as well for this to work. If

there's also an HTTP proxy server inside the firewall, it can be used to make the tunneling work even better.



The default TCP tunnel setting is for tunneling HTTP connections. You can tunnel connections directly to the web server or you could tunnel a connection from your browser to the proxy.

If you are already using a web proxy that is outside your firewall, proxy use should be disabled at least for host 127.0.0.1, if you wish to tunnel directly to a web server. Also, some web pages may be designed so that they access the server by name, in which case these links may appear broken or the data they reference may not be tunneled.



If you wish to tunnel your connection to a web proxy, the web browser should be configured (use your Internet settings to set up a proxy) to connect to 127.0.0.1 and a port of your choice: 80 works quite well, although higher port numbers are usually used for proxy servers. The server end of the tunnel should point to your normal proxy settings, such as: wwwproxy.company.com and port 8080.

Tunneling to a proxy server usually works better than tunneling to a company intranet server directly, since it allows all web pages to function correctly regardless of their design. Since you can only select one proxy server at a time, all or most of your connections will now go through the SSH connection. Disable the use of proxies for servers that need not be accessed through the SSH tunnel.

SSH1 compatibility

SSH1 is the original protocol on which SSH2 is based. F-Secure SSH 2.4 for Macintosh supports both, although SSH2 is highly recommended, because:

- It provides a higher level of security and flow control of data
- SSH1 connections can not be used for “remote forwarding” (tunneling) using this client and because of this only passive mode FTP tunneling is supported. With SSH2, remote tunneling and both FTP modes of transfer are supported.
- SSH1 is also limited to one shell session per authenticated connection, so connection cloning is not as efficient
- An open terminal session is required for any kind of tunneling to work with SSH1. There are no such limitations with SSH2.

Conclusion

To integrate SSH into your daily tasks as smoothly as possible, you should:

- Set up the preferences to your liking
- Save connection documents in the shortcuts folder for easy access
- At least browse through the rest of this manual to learn what other settings are available.

Technical support contacts are listed at the end of this manual.

2.4 Using the Menus

File Menu

Menu Item	Description
New Group	Create a new group in the Connection Manager. Selecting this item adds a new group to the Connection Manager. See Section “Managing Groups” on page 18.
New Terminal	Create a new terminal connection to an SSH server. Opens the Terminal Properties dialog box. For more information, see “ Creating a new Terminal Connection ” on page 25.
Tunnel	
TCP Tunnel	Create a new TCP tunnel. Opens the TCP Tunnel Properties dialog box. For more information, see “ Creating a New Tunnel ” on page 37.
E-Mail Tunnel	Create a new e-mail tunnel. Opens the E-Mail Tunnel Properties dialog box. For more information, see “ Creating a New Tunnel ” on page 37.
FTP Tunnel	Create a new FTP tunnel. Opens the FTP Tunnel Properties dialog box. For more information, see “ Creating a New Tunnel ” on page 37.
Open	Open an existing group, terminal, or tunnel.
Close	Hide the currently active window.
Save	Save a group, terminal, or tunnel connection. Only top-level items can be saved. If you want to save an item that is within a lower-level group, either move it to the top level first or select it and choose Put Away, in which case you will be prompted to save it. The Put Away command removes the selected item and everything underneath it from the Connection Manager, and the change will be saved along with the top-level group.
Save As...	Save a group, terminal, or tunnel that you have opened from a file under a different name.

Menu Item	Description
Clone	Make an exact copy of the selected group, terminal, or tunnel in the Connection Manager.
Put Away	Remove the selected group, terminal, or tunnel from the Connection Manager.
Create Public Key	Create a key-pair for public-key authentication. For more information on public-key authentication, see Section 2.12, "Public-key authentication" on page 61.
Quit	Close all connections and quit SSH.

Edit Menu

The Edit menu is a standard Macintosh menu. The Undo command has no application in F-Secure SSH 2.4 Client and the Cut command can only be used in the text entry fields of dialog boxes.

Menu Item	Description
Undo	Undo has no application in F-Secure SSH 2.4 Client.
Cut	Cut the selected contents of a text entry field in a dialog box to the Clipboard. Text displayed in the terminal window cannot be cut; it can only be copied.
Copy	Copy the selected text in any window to the Clipboard.
Paste	Paste text from the Clipboard to the terminal prompt, to a text entry field in the dialog boxes or to the Known Host Keys window.
Clear	Delete the selected text in a text entry field in the Properties or Preferences dialog boxes.
Copy Table	Copy the selected text from the terminal to the Clipboard in tabulated format.
Select All	Selects all the text in the active terminal window for copying.

SSH Menu

Menu Item	Description
Known Host Keys	Show a list of hosts whose host keys you have verified and accepted. You can also cut/copy/paste keys and if necessary store them in the scrapbook. This allows them to be moved from one machine to another. Host keys may also be distributed to multiple client machines simply by copying the SSH2 preferences file from the system preferences folder at: <i>System Folder:Preferences:SSH2 Preferences</i>
Connection Manager	Shows the Connection Manager as the active window.
Preferences	Opens the general SSH preferences dialog box. For more information on SSH preferences, see Section 2.11, "F-Secure SSH2 Preferences," on page 49.
Show Properties/ Show Terminal	Open the Properties dialog box of the currently selected group, terminal, or tunnel. If a Terminal Properties dialog box is the active window, the menu item is Show Terminal. If any other Properties dialog box is the active window, this menu item is disabled. For more information on terminal properties, see " Terminal Properties " on page 28. For information on tunneling properties, see " Tunnels (TCP, E-Mail, FTP) " on page 37.
Connect	Connect the selected group, terminal, or tunnel to the server defined in its Properties dialog box. This option is only available if the active group, terminal, or tunnel is not connected to the server.
Disconnect	Disconnect the selected group, terminal, or tunnel from the server. This option is only available if the selected group, terminal, or tunnel is connected to the server.
Switch Back	Switch to previous terminal in the Connection Manager.
Switch Forward	Switch to next terminal in the Connection Manager.
Open connections	A list of all the terminal connections you have open. You can select the active terminal from this list. The active terminal is checked.

Shortcuts Menu

You can save groups, terminals, and tunnels in the Shortcuts folder under the F-Secure SSH 2.4 Client for Macintosh folder, and they will appear in the Shortcuts menu. When saving the file, if you add /[ANY CHARACTER] after the name, you can open the item at any time by pressing ⌘[CHARACTER]. For example, saving a terminal with the name *myterm/J* in the Shortcuts folder will enable you to open the terminal from the F-Secure SSH 2.4 Client by pressing ⌘J. The Shortcuts menu is rebuilt each time the application is started. Quit and restart F-Secure SSH to rebuild it.

If you create new folders inside the *Shortcuts* folder, the contents of each folder are separated from other shortcuts in the *Shortcuts* menu with a horizontal line.

The *Shortcuts* folder is located in the same folder with the SSH application. It can also be an alias to a folder located somewhere else. Using an alias, you can store your connection documents in your Documents folder and still access them from the shortcuts menu.

The shortcuts menu can also contain applications, documents or aliases to just about any object. It may be convenient to create a folder with aliases to your favorite Internet applications inside the *Shortcuts* folder. You can then access these applications from the shortcuts menu from within SSH. The *Shortcuts* folder is in effect very much like an application-specific version of the *Apple Menu Items Folder*.

Menu Item	Description
Read Me	Opens the F-Secure SSH 2.4 Client Readme file.

Help Menu

Menu Item	Description
About Balloon Help	View information about Balloon Help.
Show/Hide Balloons	Select whether or not you want to use Balloon Help. There is no SSH-specific Balloon Help available in this version of the program.

2.5 Connection Manager

The Connection Manager is a utility for managing all your terminal connections and TCP tunnels from a single window. By grouping tunnels and terminals together, you can open them all by opening the group. Groups can include other groups.

Managing Groups

To create a new group, go to the *File* menu and select *New Group*, or click the **New Group** button on the Connection Manager. The new group will be placed in the Connection Manager. The first group will be placed on the left side of the Connection Manager.

All items in the Connection Manager can be arranged hierarchically. The hierarchy runs from left to right in the Connection Manager; the main group is on the left. New items will appear on the same level as the selected item when the new item is added. If the Connection Manager is empty, the new item will be placed on the top level (the left side of the Connection Manager). Opened items will always appear on the top level.

This hierarchy allows you to simultaneously open several terminals and tunnels and groups of terminals and tunnels. The number of levels is limited by the width of the screen. If you need to edit deeper hierarchies, you can move embedded groups to the top level, edit them and move them back to their place.

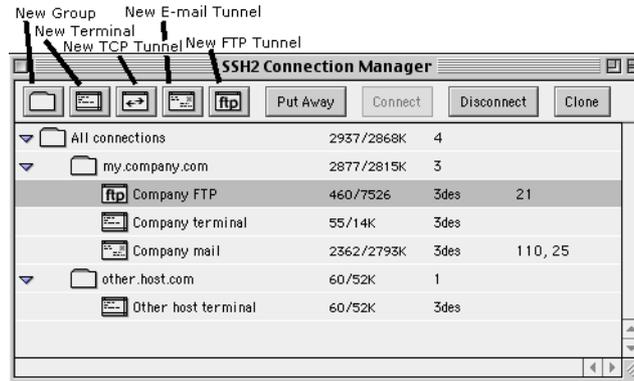
Tunnels and terminals can only be created inside a group or as stand-alone items at the top level; not inside each other.

You can move an item to a different level by dragging it to a group or to the top level.

In the following section you have an example of a two-level grouping. The smaller groups, *my.company.com* and *other.host.com*, can be opened separately if only one group is needed, as long as they have been saved separately. If all connections are needed at the same time, a top-level group called 'All connections' can be created to include both groups. In this way, all of the connections can be opened at once simply by opening the 'All connections' group.

Connection Manager Window

The Connection Manager window consists of the connection information screen and a toolbar with the following buttons:



Button	Description
New Group	Create a new group in the Connection Manager. Selecting this item adds a new group to the Connection Manager. See Section “Group Properties” on page 21.
New Terminal	Create a new terminal connection to an SSH server. Opens the terminal properties dialog box. See Section “Creating a new Terminal Connection” on page 25.
New TCP Tunnel	Create a new TCP tunnel. Opens the TCP Tunnel Properties dialog box. See Section 2.9, “Tunnels (TCP, E-Mail, FTP)” on page 37.
New E-Mail Tunnel	Create a new a-mail tunnel. Opens the E-Mail Tunnel Properties dialog box. See Section 2.9, “Tunnels (TCP, E-Mail, FTP)” on page 37.
New FTP Tunnel	Create a new FTP tunnel. Opens the FTP Tunnel Properties dialog box. See Section 2.9, “Tunnels (TCP, E-Mail, FTP)” on page 37.
Put Away	Remove the selected group, terminal or tunnel from the Connection Manager.

Button	Description
Connect	Connect the selected group, terminal or tunnel to the server defined in its Properties dialog box. This option is only available if the active group, terminal or tunnel has not yet been connected to the server.
Disconnect	Disconnect the selected group, terminal or tunnel from the server. This option is only available if the selected group, terminal, or tunnel is connected to the server.
Clone	Make an exact copy of the selected group, terminal, or tunnel in the Connection Manager.

The connection information screen shows all currently opened items and information about their connection status.

For groups, you are shown an outline triangle for expanding and collapsing the contents of the group. When the triangle is pointing to the right, the group is collapsed, hiding its contents. When the triangle points down, the group is expanded, displaying its contents.

After the group icon you see the name you have given to the group, or the address of the host you are connected to, if no name has been given. If no tunnels or terminals inside that group, or in any groups inside the group, are connected to a host, no further information is shown. If there are one or more connections, you will see the combined amount of data transferred in/out through all the connections within that group hierarchy, followed by the number of open connections within that group hierarchy.

The item's name is displayed next to the icons. If the item has not been named, the address of the host it is connected to is displayed. If the terminal or tunnel is connected, the amount of data transferred in and out through that connection will also be shown, as well as the cipher used for encrypting the data, followed by the port numbers that the tunnel is forwarding.

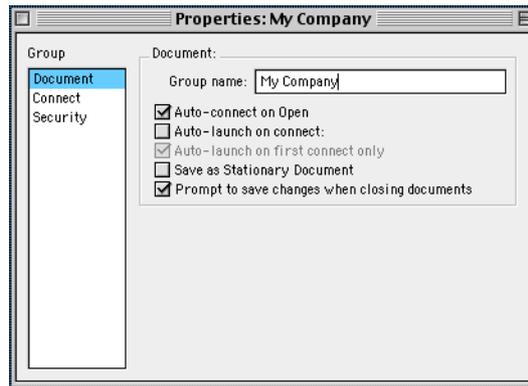
The data in/out transfer indicator is especially useful when setting up tunnels. When a tunnel is first opened, the indicator will show 0/0. When the tunnel is being accessed, the indicator immediately changes. The indicator will remain at 0/0 if the tunnel is never accessed, which can happen if your Web browser or e-mail client is not correctly configured to use the tunnel.

To select an item in the Connection Manager window, use the up and down arrow keys. To open a terminal screen, select the terminal and press `ENTER` or double-click on it. To open the terminal's Properties dialog box, press `⌘-ENTER` or press `OPTION-ENTER`. You can also open a terminal's Properties dialog box by clicking on the status box in the bottom left of the terminal window.

To open the Properties box for a tunnel or a group, select it and press ENTER, or double-click on it.

2.6 Group Properties

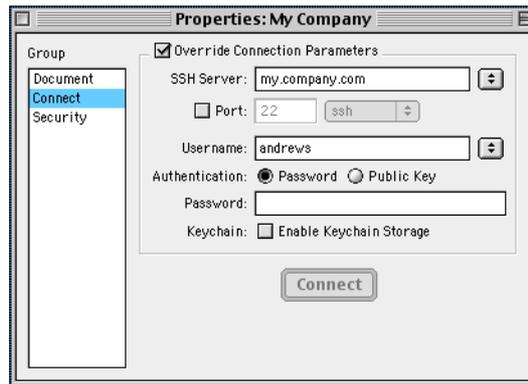
Group Properties—Document



Properties Item	Description
Group Name	Give a name to the group. This name will be shown beside the icon of the group in the Connection Manager. The name can be used to quickly identify the group. If no name is given, the address of the host being connected to is shown instead.
Auto-connect on Open	This option applies to groups that have been saved as files that can be opened in SSH. When this option is selected, opening a file will automatically connect you to the server named in the <i>Connect</i> page of the Properties dialog box. If you leave the <i>SSH Server</i> , <i>Username</i> and <i>Password</i> fields blank on the <i>Connect</i> page, you will be prompted for them while the connection is being initiated.
Auto-launch on connect:	When checked, the selected application will automatically be launched as soon as the connection has been established.

Properties Item	Description
Auto-launch on first connect only	When checked, the application selected in the previous item will only be opened once as long as the group remains open in the Connection Manager.
Save as Stationary Document	Save the groups as a stationary document. When you open a group saved like this, you will be taken to the Properties page of the group just as if you were creating a new group, but the properties are by default as you saved them. This option is cleared when the document is opened again, so you will need to select this option again if you want to make changes to the stationary document.
Prompt to save changes when closing a document	Select this check box if you want the client to ask you whether to save a document when you close one. This setting allows you to automatically discard changes made to the document/stationary, such as resizing a window or changing the host/username.

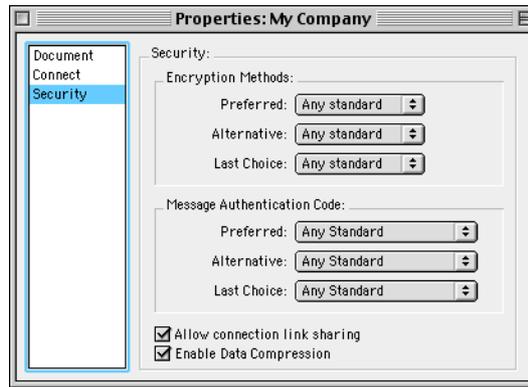
Group Properties —Connect



Connect Item	Description
Override Connection Parameters	Values given in the Connect Properties of the group will override all the Connect and Security Properties in the groups, tunnels, and terminals beneath it in the Connection Manager hierarchy.

Connect Item	Description
SSH Server	Give the DNS or IP address of the server you are connecting to, or select it from the list of your favorite servers. For information on setting your favorite servers, see “ Connections Preferences ” on page 50.
Port	Enter the port number if the SSH2 server you are connecting to is listening to a port other than the standard port 22.
User name	Enter your user name on the server you are connecting to, or select it from your list of user names. For information on setting the list of user names, see “ Connections Preferences ” on page 50.
Authentication	Select whether to use password authentication or public-key authentication. For information on how to setup your account for public-key authentication, see Section 2.12, “Public-key authentication,” on page 61.
Password	If you selected password authentication, enter your password here.
Keychain: Enable Keychain Storage	When selected, you can add your login passwords and public key passphrases to the MacOS keychain. For more information on the keychain feature introduced in MacOS 9, refer to your MacOS documentation.
Connect	When you have given all the required information, click Connect to connect to the server.

Group Properties—Security



Security Option	Description
Encryption Methods	Select your preferred encryption methods from the pop-up menus. To force SSH to use a specific encryption method, select the same item from all three menus:
	Preferred — Your preferred cipher Alternative — Your second choice Last Choice — Used if the above ciphers are not available
Message Authentication Code	Select your preferred methods for message authentication from the pop-up menus:
	Preferred — Your preferred cryptographic hash Alternative — Your second choice Last Choice — Used if the above hashes are not available

Security Option	Description
Allow connection link sharing	Allow terminals and tunnels connecting to the same host to use the same connection. When using connection link sharing, you need to authenticate yourself to the server only once for multiple connections that use the same authentication and security parameters. If the connection has hung for some reason, and you want to open a new connection, disable connection link sharing before opening the connection, so that a new TCP connection will be created. However, when connecting to SSH1 servers, you are restricted to one terminal per connection, but can still use connection link sharing for tunnels.
Enable Data Compression	When this box is checked, all data travelling through any items in the group will be compressed to speed up the connection.

2.7 Using Terminals

Creating a new Terminal Connection

To create a new terminal connection in F-Secure SSH2, click the **New Terminal** button in the Connection Manager, press **⌘N**, or select *New Terminal* from the *File* menu. This will open the Properties dialog box for the new terminal connection.

The Properties dialog box will open on the Connect page. The simplest way to connect is to just enter all the required information on this page and click **Connect**. However, by going through all the pages, you can change several properties of the terminal connection.

For information on terminal properties, see “[Terminal Properties](#)” on page 28.

Opening an Existing Terminal Connection

You can open an existing connection in the following ways:

- Choose *Open* from the *File* menu, or press ⌘O, and select the file you want to open.
- Choose the connection you want to open from the Shortcuts menu. For more information on using shortcuts, see “[Shortcuts Menu](#)” on page 17.
- Double-click on the icon of the file you want to open.
- Drag the icon of the file you want to open onto the F-Secure SSH2 icon.

Saving a Terminal Connection

After you have entered all the required information in the Terminal Properties dialog box, you can save the properties in a file by doing one of the following:

- Choose *Save* from the File menu, or press ⌘S.
- Choose *Save As* from the File menu if you want to save an existing connection under a new name.

The file will be associated with SSH, so you can open it later by just double-clicking it.

The *Shortcuts* folder is a very convenient place for frequently used connection documents. Settings that are stored there will appear in the Shortcuts menu the next time you launch SSH. For more information, see “[Shortcuts Menu](#)” on page 17.

Selecting a Terminal Window as the Active Window

To select a terminal window that has been opened, do one of the following.

- Select it from the SSH menu, or press the ⌘ key and the number assigned to the terminal window.
- Click on its icon in the Connection Manager.
- Switch between the terminal windows by pressing the ⌘= key. You can change back to using the ⌘+ and ⌘- keys from *Preferences-Keyboards*.

Connecting and Disconnecting from the Host

To connect to the host defined in the Properties dialog box, select the terminal window, and do one of the following.

- Choose *Connect* from the SSH menu, or press ⌘G.
- Select the terminal and click the **Connect** button in the Connection Manager.
- Click on the word “Disconnected” in the status bar at the bottom of the terminal window.
- Open the terminal Properties dialog box, and click the **Connect** button.

To disconnect from a host, do one of the following.

- Choose *Disconnect* from the SSH menu, or press ⌘K.
- Log out from the host with the usual UNIX commands (logout, exit, or quit).
- Click the **Disconnect** button in the Connection Manager.

Cloning the Terminal

To clone a terminal, select the terminal and do one of the following.

- Choose *Clone* from the File menu, or press ⌘D.
- Click the **Clone** button in the Connection Manager.

If the original terminal is already connected to a server, cloning the terminal will automatically connect the cloned terminal to the server as well.

Hiding a Terminal Window

To hide a terminal window, select the terminal and do one of the following:

- Choose *Close* from the File menu, or press ⌘W.
- Click the Close box in the upper left corner of the terminal window. If you select the “Put away’ When a Terminal Window is Closed” option in the Interface page of the Preferences dialog box, the terminal will be closed and removed from the Connection Manager.

Removing a Terminal from the Connection Manager

To disconnect a terminal from a host and remove the terminal from the Connection Manager, select the terminal and do one of the following.

- Choose *Put Away* from the File menu, or press ⌘Y.
- Click the **Put Away** button in the Connection Manager.

Working with Text in the Terminal Window

You can scroll the terminal and the scrollback buffer with the mouse. Pressing ⌘ and the up or down arrow at the same time will scroll the terminal up or down one screen at a time.

To select text in the terminal window, drag your mouse over the text. To select a single word, double-click on the word. To select a line of text, click three times anywhere in the line. To select a paragraph, click four times anywhere in the paragraph.

You can extend your previous selection by pressing SHIFT when selecting text. You can select URLs by pressing OPTION or ⌘ and clicking on the URL. Using the ⌘ key opens the URL in a browser.

To copy text from the terminal window to the Clipboard, select the text you want to copy and either choose Copy from the Edit menu or press ⌘C.

To copy text in a tabulated format, select the text you want to copy and choose Copy Table from the Edit menu. Text in tabulated format can be properly pasted into a spreadsheet.

To paste text into the terminal window, either choose Paste from the Edit menu or press ⌘V.

You can also select text and drag it with your mouse to another document.

2.8 Terminal Properties

To edit the terminal properties, do one of the following.

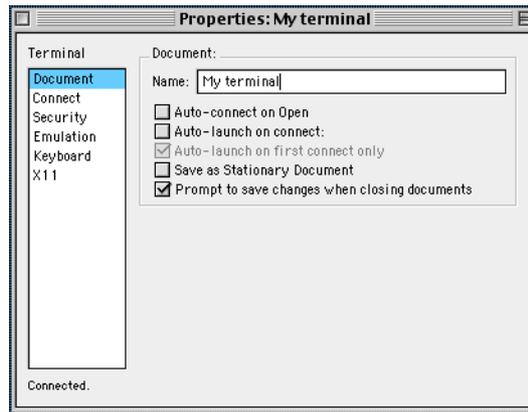
- Select the terminal and choose *Show Properties* from the SSH menu, or press ⌘P.
- Double-click on the terminal in the Connection Manager.

To toggle between the terminal and its properties, press ⌘P.

NOTE:

You can override terminal preferences with group preferences. Select the *Override connection properties* check box in the *Connect* page of the group properties to do so.

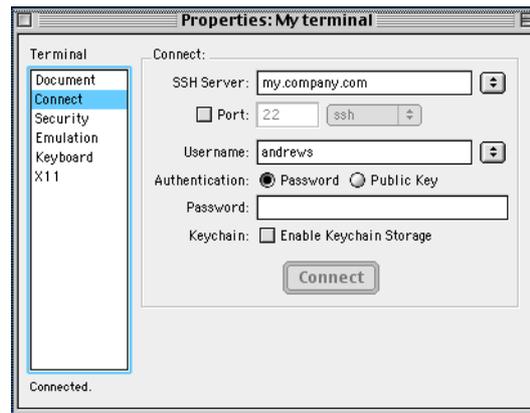
Terminal Properties — Document



Properties Item	Description
Name	Give a name to the connection. This name will be shown on the title bar of the terminal window and beside the icon of the terminal in the Connection Manager. The name can be used to quickly identify the connection.
Auto-connect on Open	This option applies to terminal connections that have been saved as files that can be opened in SSH. When this option is selected, opening a file will automatically connect you to the server.
Auto-launch on Connect	When checked, the selected application or document will automatically be launched as soon as the connection has been established. For example, you could launch a Web browser when the connection is established, or you can open a specific URL file.

Properties Item	Description
Auto-launch on first connect only	When checked, the application selected in the previous item will only be opened once as long as the group remains open in the Connection Manager. This will disable switching to the application for example when the group is cloned.
Save as Stationary Document	Save the terminal as a stationary document. When you open a terminal saved like this, you will be taken to the Properties page of the terminal just as if you were creating a new terminal, but the properties are by default as you saved them. This option is cleared when the document is opened again, so you will need to select this option again if you want to make changes to the stationary document.

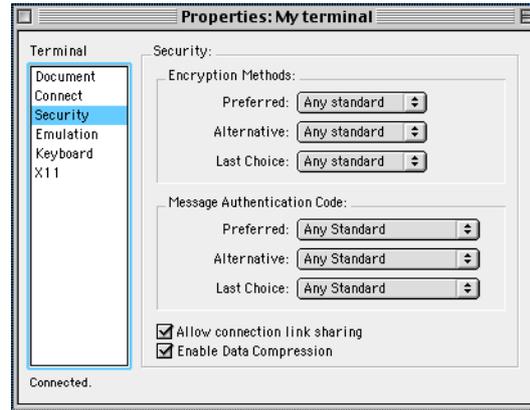
Terminal Properties—Connect



Connect Item	Description
SSH Server	Give the DNS or IP address of the server you are connecting to, or select it from the list of your favorite servers. For information on setting your favorite servers, see “ F-Secure SSH2 Preferences ” on page 49.
Port	Enter the port number if the SSH2 server you are connecting to is listening to a port other than the standard port 22.

Connect Item	Description
User name	Select whether to use password authentication or public-key authentication. For information on how to setup your account for public-key authentication, see “ Public-key authentication ” on page 61.
Authentication	Select whether to use password authentication or public-key authentication. For information on how to setup your account for public-key authentication, see “ Public-key authentication ” on page 61.
Password	If you selected password authentication, enter your password here.
Keychain: Enable Keychain Storage	When selected, you can add your login passwords and public key passphrases to the MacOS keychain. For more information on the keychain feature introduced in MacOS 9, refer to your MacOS documentation.
Connect button	When you have given all the required information, click Connect to connect to the server.

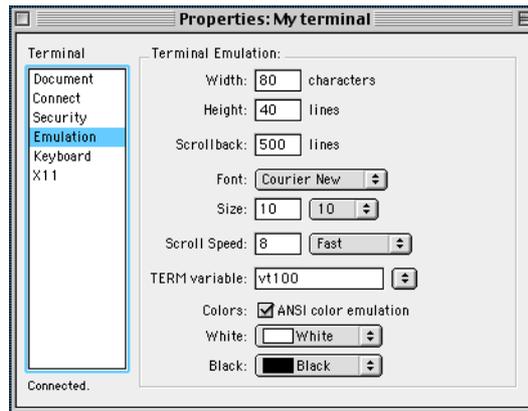
Terminal Properties—Security



Security Option	Description
Encryption Methods	Select your preferred encryption methods from the pop-up menus. To force SSH to use a specific encryption method, select the same item from all three menus:
	Preferred — Your preferred cipher Alternative — Your second choice Last Choice — Used if the above ciphers are not available
Message Authentication Code	Select your preferred methods for message authentication from the pop-up menus:
	Preferred — Your preferred cryptographic hash Alternative — Your second choice Last Choice — Used if the above hashes are not available

Security Option	Description
Allow connection link sharing	<p>Allow terminals and tunnels connecting to the same host to use the same connection. When using connection link sharing, you only need to authenticate yourself to the server once for multiple connections using the same authentication and security parameters.</p> <p>If the connection has hung for some reason, and you want to open a new one, disable connection link sharing before opening the connection, so that a new TCP connection will be created.</p>
Enable Data Compression	When this box is checked, all data traveling through the terminal will be compressed to speed up the connection.

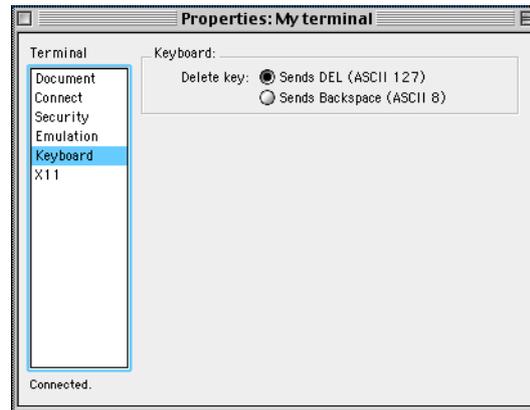
Terminal Properties—Emulation



Emulation Option	Description
Width:	Enter the width of the terminal window in characters.
Height:	Enter the height of the terminal window in lines.

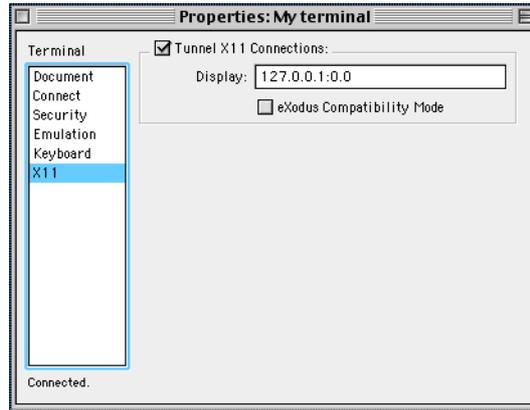
Emulation Option	Description
Scrollback:	Enter the number of lines to have in the scrollback buffer. If memory is low, the F-Secure SSH Client may limit the number of scrollback lines to conserve memory.
Font:	Select the font you want to use in the terminal from the pop-up menu.
Size:	Enter the size of the font, or select it from the pop-up menu.
Scroll Speed:	Enter the maximum number of lines to scroll at a time, or select it from the pop-up menu.
TERM variable:	Select your preferred mode of terminal emulation from the pop-up menu.
Colors:	Checking the box selects ANSI color emulation.
White/Black	Select your terminal colors by changing these settings.

Terminal Properties—Keyboard



Keyboard Option	Description
Delete key:	Select whether pressing the <code>DELETE</code> key on the keyboard sends <code>DEL</code> or <code>BACKSPACE</code> to the terminal. By default, pressing <code>SHIFT+DELETE</code> sends <code>BACKSPACE</code> , and pressing <code>DELETE</code> by itself sends <code>DEL</code> . You can use this option to reverse this action.

Terminal Properties- X11



X11 Option	Description
Tunnel X11 Connections:	Select this check box if you want to enable X11 tunneling.
Display:	Enter the display variable for your local X11 window server. SSH will replace this with a virtual display variable at the SSH server end. Most of the time you do not need to change this field.
eXodus Compatibility Mode	Select this check box if you are using eXodus for viewing the forwarded X11 content on your machine. Using this option will automatically replace <i>127.0.0.1</i> with your actual IP number.

NOTE:

X11 tunneling must be enabled when the connection is opened in order for it to work.

2.9 Tunnels (TCP, E-Mail, FTP)

Tunnels encrypt all TCP traffic going through them. With the FTP tunnel introduced in version 2.1 it is possible to encrypt all FTP traffic, usernames, passwords and commands by forwarding them through a tunnel.

SSH tunneling can also be used to encrypt the Appleshare IP protocol. To do so, create a local tunnel that connects port 548 on your machine to port 548 on the AFP server. To use the encrypted connection to the server, open the "Chooser", select AppleShare and click on the "Server IP Address..." button. Enter *127.0.0.1* as the server address and proceed normally with your login to the server. You can use the connection manager statistics to verify that data is actually going through SSH.

Appleshare IP servers are available as standard features on MacOS X and MacOS 9.

If your Unix system has "netatalk" installed and afpd is running, it is possible to access the Unix file system in a secure and encrypted fashion using this tunnel.

For more information on netatalk, you can consult the following web pages:

<http://www.umich.edu/~rsug/netatalk/>

<http://thehamptons.com/anders/netatalk/>

F-Secure makes no guarantees on the accuracy or availability of the above web pages. The links are provided for informational purposes only and are not meant as an endorsement of those web sites or the products or services described within.

WARNING:

Important: Installation of the netatalk system requires extensive experience with the Unix operating system and should not be attempted without the necessary skills. For security reasons, access to the AFP server should be restricted to connections from the SSH server only.

Creating a New Tunnel

To create a new TCP, e-mail or FTP tunnel in F-Secure SSH2, select *Tunnel*, and the *type of tunnel you want to create*, from the *File* menu, or click on the respective button in the connection manager. This will open the Properties dialog box for the new tunnel.

The Properties dialog box will open on the *Tunneling* page. The simplest way to connect is to just enter all the required information on this page, switch to the *Connect* page and click the **Connect** button. However, you can change several properties of the tunnel by going through all the pages.

Opening an Existing Tunnel

To open an existing connection, do one of the following.

- Choose *Open* from the *File* menu (or press ⌘O), and select the file you want to open.
- Double-click on the icon of the file you want to open.
- Drag the icon of the file you want to open onto the F-Secure SSH2 icon.

Saving a Tunnel

After you have entered all the required information in the Tunnel Properties dialog box, save the properties in a file by one of the following methods.

- Choose *Save* from the File menu, or press ⌘S.
- Choosing *Save As* from the File menu if you want to save an existing connection under a new name.

The file will be associated with SSH, so you can open it later by just double-clicking it.

Selecting a Tunnel

To select a tunnel that has been opened, click on its icon in the Connection Manager.

Connecting and Disconnecting from the Host

To connect to the host defined in the Properties dialog box, select the tunnel and do one of the following:

- Choose *Connect* from the SSH menu, or press ⌘G.
- Select the tunnel and click the **Connect** button in the Connection Manager.
- Open the tunnel Properties dialog box and click the **Connect** button.

To disconnect from a host, do one of the following.

- Choose *Disconnect* from the SSH menu, or press ⌘K.
- Log out from the host with the usual UNIX commands (logout, exit, or quit).
- Click the **Disconnect** button in the Connection Manager.

Cloning the Tunnel

To clone a tunnel, select the tunnel and do one of the following.

- Choose Clone from the File menu, or press ⌘D.
- Click the **Clone** button in the Connection Manager.

NOTE:

Only a single port listener can be open for each socket number, so if a tunnel is cloned, the port number that it is listening on should be changed on one copy before both are opened.

Use a port number of 0 to let SSH allocate a listener on any available port number. The actual port number will be displayed in the connection manager.

Removing a Tunnel from the Connection Manager

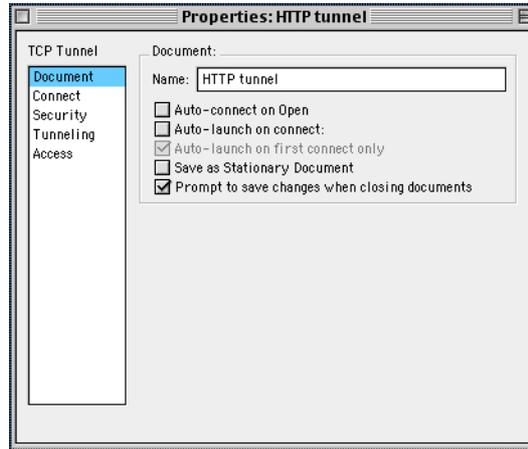
To disconnect a tunnel from a host and remove the tunnel from the Connection Manager, select it and do one of the following.

- Choose Put Away from the File menu, or press ⌘Y.
- Click the **Put Away** button in the Connection Manager.

2.10 Tunneling Properties (TCP, E-Mail, FTP)

All pages of the Properties windows of the three different kinds of tunnels are the same, except the Tunneling page. In TCP tunnels it is named Tunneling, in E-Mail tunnels it is Services and in FTP tunnels it is FTP Server. These pages differ from each other, and they are documented here successively according to their respective place in the Properties window.

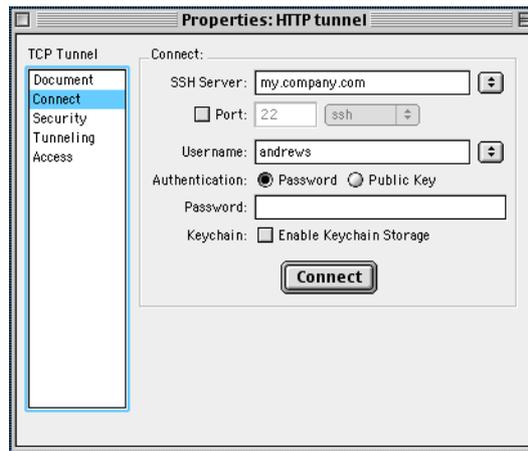
Tunneling Properties—Document



Document Option	Description
Name	Name of the connection. Displayed next to the icon for the tunnel in the Connection Manager.
Auto-connect on Open	This option applies to tunnels that have been saved as files that can be opened in SSH. When this option is selected, opening a file will automatically connect you to the server.
Auto-launch on connect	When checked, the application or document you select will automatically be launched as soon as the connection has been established. For example, you can open a URL file that uses the tunnel for transferring data.
Auto-launch on First Connect Only	When checked, the application selected in the previous item will only be opened once as long as the document remains open.

Document Option	Description
Save as Stationary Document	Save the tunnel as a stationary document. When you open a tunnel saved like this, you will be taken to the properties page of the tunnel just as if you were creating a new tunnel, but the properties are the same as when you saved it. This option is cleared when the document is opened again, so you will need to select this option again if you want to make changes to the stationary document.

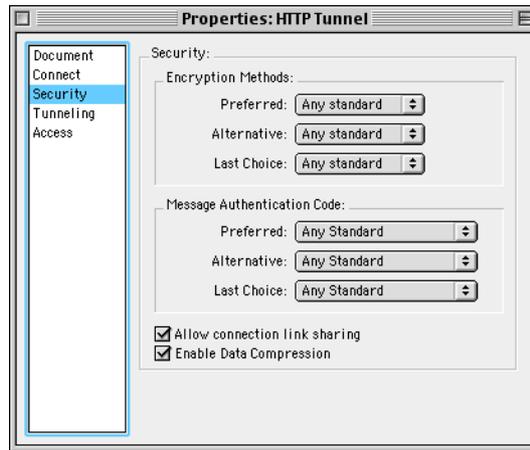
Tunneling Properties—Connect



Connect Item	Description
SSH Server	Give the DNS or IP address of the server you are connecting the tunnel to, or select it from the list of your favorite servers. For information on setting your favorite servers, see Section 2.11, "F-Secure SSH2 Preferences," on page 49.
Port	If the SSH2 server you are connecting the tunnel to is listening to some other port than the standard 22, you can enter the port number here.

Connect Item	Description
User name	Enter your user name on the server you are connecting the tunnel to, or select it from your list of user names. See Section 2.11, "F-Secure SSH2 Preferences," on page 49 for information on setting the list of user names.
Authentication	Select whether to use password authentication or public-key authentication. For information on how to set up your account for public-key authentication, see Section 2.12, "Public-key authentication," on page 61.
Password	If you selected password authentication, enter your password here.
Keychain: Enable Keychain Storage	When selected, you can add your login passwords and public key passphrases to the MacOS keychain. For more information on the keychain feature introduced in MacOS 9, refer to your MacOS documentation.
Connect	When you have given all the required information, click Connect to connect the tunnel to the server.

Tunneling Properties— Security

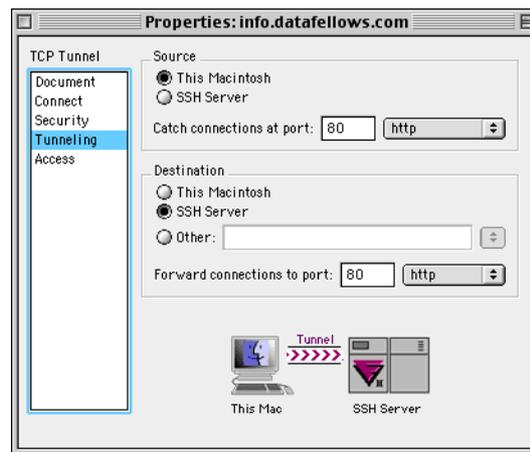


Security Option	Description
Encryption Methods	Select your preferred encryption methods from the pop-up menus. To force SSH to use a specific encryption method, select the same item from all three menus:
	Preferred — Your preferred cipher Alternative — Your second choice Last Choice — Used if the above ciphers are not available
Message Authentication Code	Select your preferred methods for message authentication from the pop-up menus:
	Preferred — Your preferred cryptographic hash Alternative — Your second choice Last Choice — Used if the above hashes are not available

Security Option	Description
Allow connection link sharing	<p>Allow terminals and tunnels connecting to the same host to use the same connection. When using connection link sharing, you only need to authenticate yourself to the server once for multiple connections using the same authentication and security parameters.</p> <p>If the connection has hung for some reason, and you want to open a new one, disable connection link sharing before opening the connection, so that a new TCP connection will be created.</p>
Enable Data Compression	When this box is checked, all data traveling through the tunnel will be compressed to speed up the connection.

TCP Tunneling Properties - Tunneling

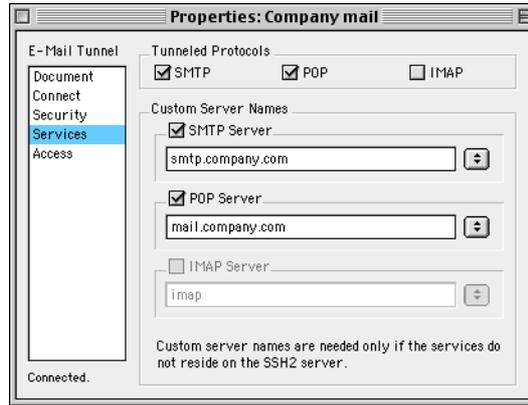
For more information on tunneling, see “[Tunnels \(TCP, E-Mail, FTP\)](#)” on page 37.



Tunneling Option	Description
Source	Select the source of the tunnel. You can select either This Macintosh for local tunneling, or SSH Server for remote tunneling. Remote tunneling is not supported for SSH1 servers.

Tunneling Option	Description
Catch connections at port:	<p>Select which port F-Secure SSH2 will listen to on your Macintosh or the remote SSH Server. You can enter the port number manually or you can select one of the predefined ports from the pop-up menu.</p> <p>Using 0 as a port number will allocate a port number dynamically from the available free ports. The port number will be displayed in the connection manager once it is known.</p>
Destination	<p>Select the destination of the tunnel. For creating a local tunnel, you can select the SSH2 server you are connecting to as the destination server of the tunnel, or you can select a different destination. For remote tunneling, select This Macintosh or a third host.</p>
Forward connections to port	<p>Select which port on the selected destination host the tunnel is connected to. You can enter the port number manually or select one of the predefined ports from the pop-up menu.</p>

E-Mail Tunneling Properties-Services

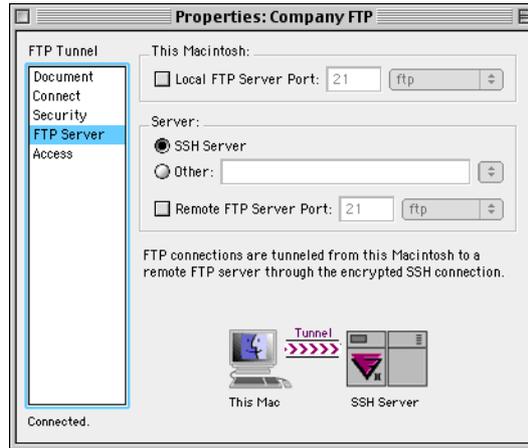


Services Option	Description
Tunneled Protocols	Select which e-mail protocols you wish to forward through an SSH tunnel. The available protocols are SMTP, POP and IMAP. Normally, when you forward your incoming and outgoing e-mail on a single e-mail server, you need SMTP and either POP or IMAP.
Custom Server Names	You only need to give the server names if the e-mail services reside on another host than the server you are connecting to. If that is the case, select the appropriate check boxes and enter the name of the respective e-mail server.

FTP Tunneling Properties-FTP Server

NOTE:

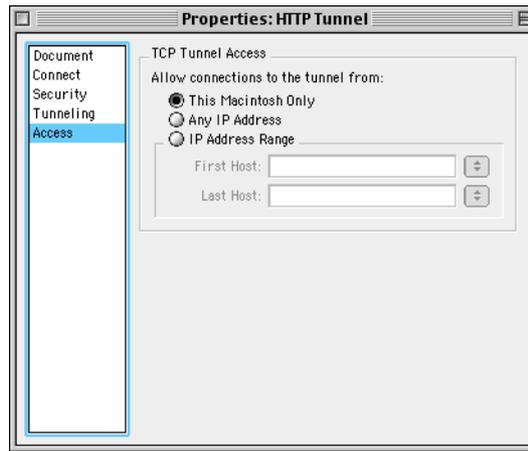
FTP tunneling with SSH1 only supports passive FTP. SSH2 supports both active and passive FTP.



FTP Server Options	Description
This Macintosh:	
Local FTP Server Port	Give the port number you want to connect to on your local computer when making a forwarded connection to the FTP site this tunnel is created to. If you create several FTP tunnels, remember that you need to give each one a different port number. You then connect to the server with your FTP client by defining the FTP server as '127.0.0.1' and using the port number you have assigned for it here.
Server:	
SSH Server	Select this radio button if the FTP server resides on the same server that you are connecting to with SSH.

FTP Server Options	Description
Other:	Select this radio button if the FTP server resides on another host. Give the IP address or the DNS name of the other host here.
Remote FTP Server Port	If the remote FTP server port is other than the default 21, select this check box and enter the port number in the field or select it from the available services.

Tunneling Properties—Access



Access Option	Description
Allow connections to the tunnel from:	
This Macintosh only	Do not allow connections to the tunnel from anywhere else but the Macintosh you are creating the tunnel from.

Access Option	Description
Any IP Address	Allow anyone to use the tunnel you create from any computer in the world that can access the source of the tunnel. This is not recommended as it poses a high security risk for your network.
IP Address Range	Give a range of IP addresses or DNS names from which the tunnel can be accessed (for example 10.10.10.1 and 10.10.10.255). You can also define a single IP address or DNS name to allow connections only from that address.

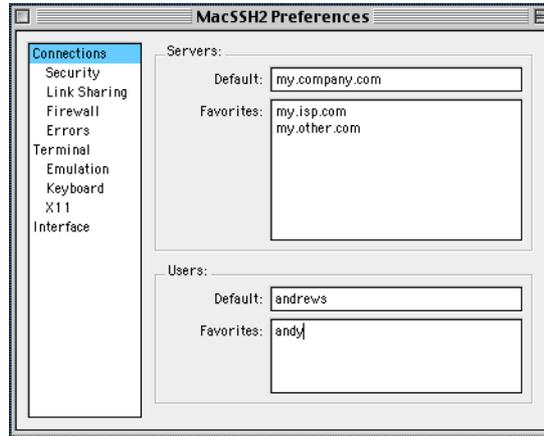
2.11 F-Secure SSH2 Preferences

You can edit the general preferences of F-Secure SSH2 for MAC by selecting *Preferences* from the *SSH* menu. The Preferences dialog box and Properties dialog box share many of the same options. The preferences set in the Preferences dialog box are used as defaults for all your connections.

NOTE:

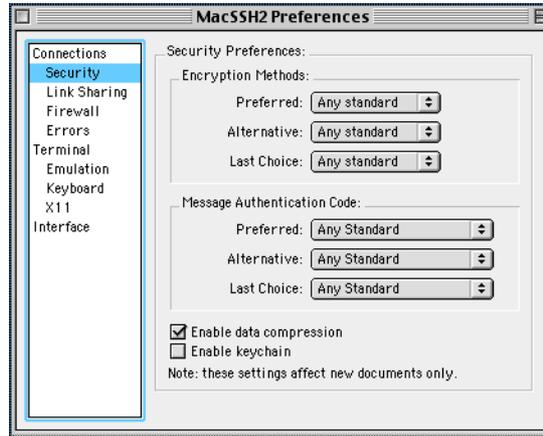
Some settings are presets for new documents, i.e. new documents will have the settings that are defined in the preferences. Other settings are global and immediate and affect old documents as well. These global settings can only be changed from the preferences and do not have corresponding items in the properties panels.

Connections Preferences



Connections Option	Description
Servers: Default:	Enter your default server address. This will then be used as the default address in all new terminals and tunnels that you create.
Servers: Favorites:	List your other favorite server addresses. You can then select them from a pop-up menu in the Properties dialog box of any new terminal or tunnel. Use - (on its own to insert a line between choices.
Users: Default:	Enter your default user name. This will be used as the default user name in all new terminals and tunnels that you create.
Users: Favorites:	List the user names you use often. You can then select them from a pop-up menu in the Properties dialog box of any new terminal or tunnel. Use - on its own to insert a line between choices.

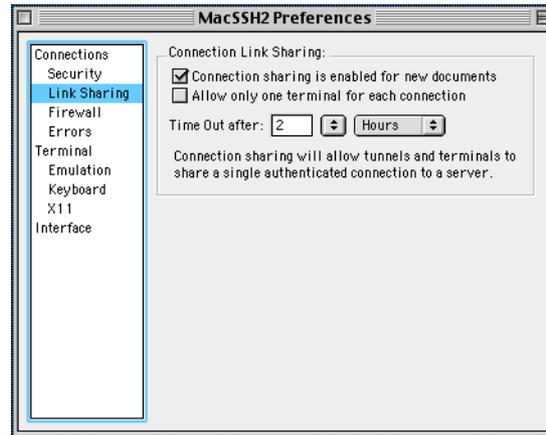
Security Preferences



Security Option	Description
Encryption Methods	Select your preferred encryption methods from the pop-up menus:
	Preferred — your first choice Alternative — your second choice Last Choice — used if your first two choices are not available
Message Authentication Code	Select your preferred methods for message authentication from the pop-up menus:
	Preferred — your first choice Alternative — your second choice Last Choice — used if your first two choices are not available
Enable Data Compression	When this box is checked, all data traveling through all your connections will be compressed to speed up the connection.

Security Option	Description
Enable keychain	When checked, you can use the keychain feature introduced in MacOS 9 to store your login passwords.

Link Sharing Preferences



Links Sharing Option	Description
Connection sharing is enabled for new documents	When checked, new terminals and tunnels are allowed to use an existing connection for transferring data, instead of making a new connection.
Allow only one terminal for each connection	When checked, only one terminal may use one connection, that is, each terminal will have its own connection. However, the number of tunnels for one connection is not limited.

Links Sharing Option	Description
Time Out after:	Sets the amount of time after which new connections cannot automatically share the existing connection, but will have to be authenticated again. It is especially useful to set the time to a few minutes if you keep a few tunnels open for a long time, and you want to make sure that other people accessing your computer will not be able to use the tunnels to open an authenticated connection to your UNIX account.

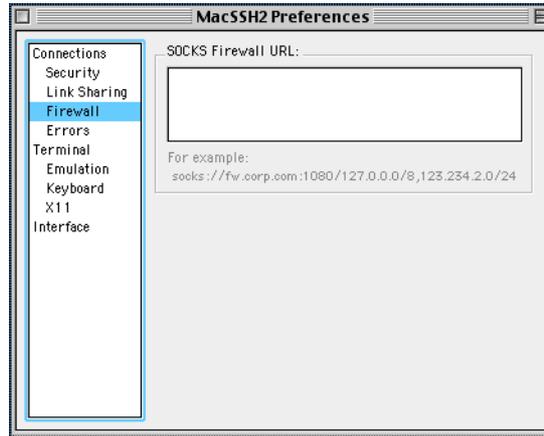
NOTE:

Due to protocol limitations, SSH1 connections are limited to one shell per connection.

Also, SSH1 tunnels require a shell connection, so a terminal has to be created and connected before or at the same time the tunnel connection is attempted. Use a group if necessary.

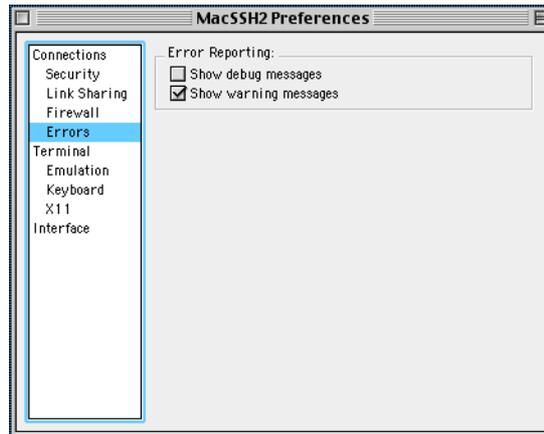
These limitations do not affect the SSH2 protocol. SSH2 is highly recommended for other reasons as well. Upgrade your server(s), if possible.

Firewall Preferences



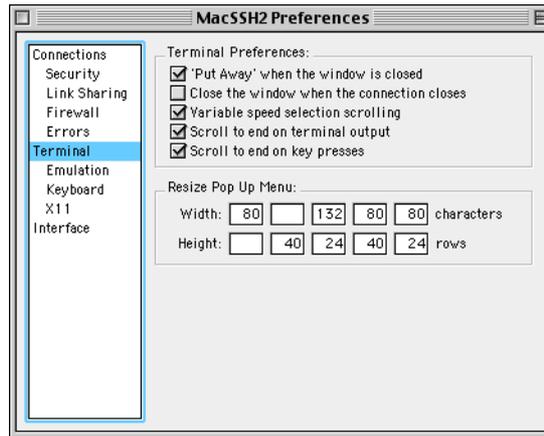
Firewall Option	Description
Socks Firewall URL:	If you are connecting from behind a SOCKS firewall, you can enter the URL and the port number of the firewall here.

Errors Preferences



Error Option	Description
Show debug messages	Check this box if you wish to receive debug messages. This is useful if you are encountering problems and want to identify their source. For example, debug gives you the SSH version on connect.
Show warning messages	Check this box if you wish to receive various warning messages. For example, the program will warn you when SSH1 is used.

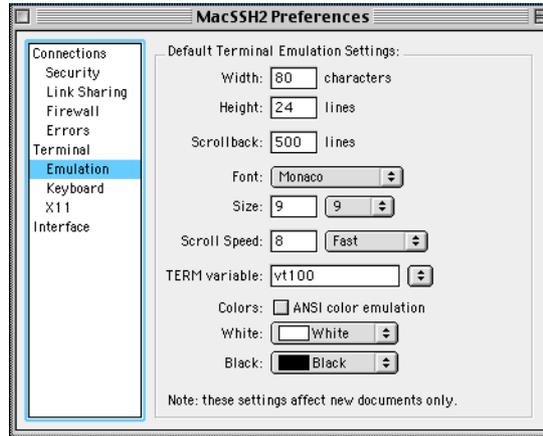
Terminal Preferences



Terminal Option	Description
'Put Away' when the window is closed	When a terminal window close box is clicked or the "close" command is used, the window can either be hidden from view or it can be put away. When this option is enabled, the window is destroyed. This option is on by default.

Terminal Option	Description
Close the window when the connection closes	When checked, windows are closed as you close the connections.
Variable speed selection scrolling	The speed with which the screen scrolls when you are selecting text with the mouse will depend on the distance of the mouse pointer from the terminal window. If this option is not selected, the screen will always scroll at the same speed.
Scroll to end on terminal output	If you have scrolled the terminal screen back and this box is checked, as soon as you get new output on the terminal window, the window is scrolled back to the end.
Scroll to end on key presses	If you have scrolled the terminal screen back and this box is checked, as soon as you press a key, the window is scrolled back to the end.
Terminal Resize Pop Up Menu	Define up to five different terminal size settings that can be directly changed from the pop-up menu in the status bar of the Connection Manager. If a box is left empty, the current terminal setting is used for it in the pop-up menu.

Emulation Preferences



Emulation Option	Description
Width:	Enter the default width of terminal windows in characters.
Height:	Enter the default height of terminal windows in lines.
Scrollback:	Enter the number of lines you want to keep in the scrollback buffer. If memory is low, F-Secure SSH Client may limit the number of scrollback lines to conserve memory.
Font:	Select the font you want to use in terminal windows from the pop-up menu.
Size:	Enter the size of the font, or select it from the pop-up menu.
Scroll Speed:	Enter the default scrolling speed of terminal windows, or select it from the pop-up menu. The speed is measured in lines per second.
TERM variable:	Select your preferred TERM environment variable to send to the host from the pop-up menu. This value changes only during each logon. If the value is changed while connected, the changes will take place the next time the connection is opened.

Emulation Option	Description
Colors:	Checking the box selects ANSI color emulation.

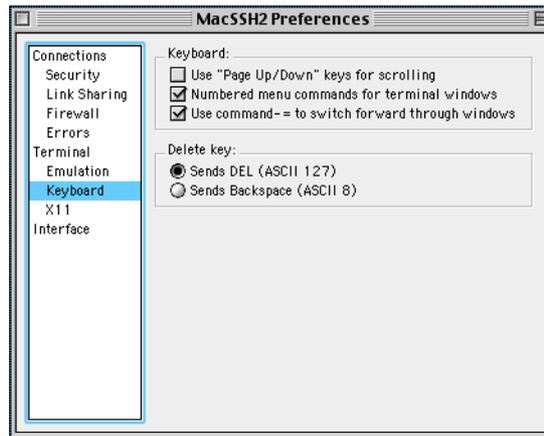
NOTE:

If you have a very large number of fonts, loading the font menu for the first time may take a while.

TIP:

⌘↑ and ⌘↓ can be used to go through the items listed in the menus next to the text fields.

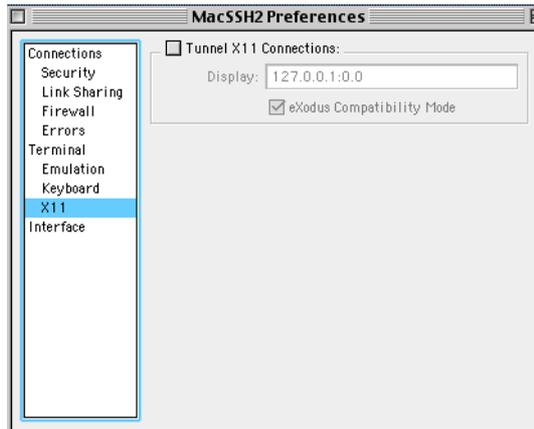
Keyboard Preferences



Keyboard Option	Description
Use "Page Up/Down" keys for scrolling	When checked, you can scroll the contents of the terminal window up and down with the PAGE UP/DOWN keys.

Keyboard Option	Description
Numbered menu commands for terminal windows	When checked, the terminal windows will be numbered on the list in the SSH menu. They can then be activated by pressing ⌘1, ⌘2, etc.
Use command+= to switch forward through windows	When checked, you can use the command+= key instead of command++ to scroll through all the F-Secure SSH windows you have open.
Delete key:	Select whether pressing the DEL key on the keyboard sends DEL or BACKSPACE to the terminal.

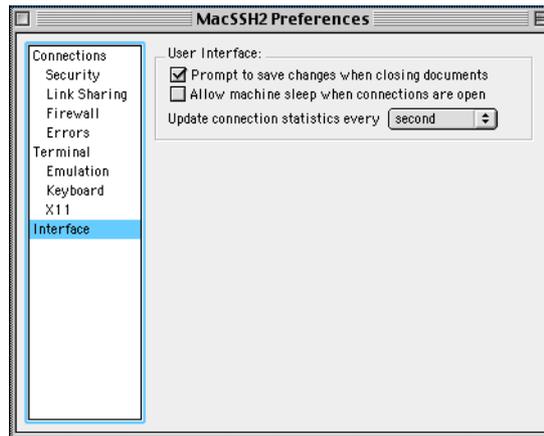
X11 Preferences



X11 Option	Description
Tunnel X11 Connections:	Select this check box if you want to enable X11 tunneling.

X11 Option	Description
Display:	Enter the display variable for your local X11 window server. SSH will replace this with a virtual display variable at the SSH server end. Most of the time you do not need to change this field.
eXodus Compatibility Mode	Select this check box if you are using eXodus for viewing the forwarded X11 content on your machine. Using this option will automatically replace <i>127.0.0.1</i> with your actual IP number.

Interface Preferences



Interface Option	Description
Prompt to save changes when closing documents	Select this check box if you want the client to ask you whether to save a document when you close one. This default affects new documents only.
Allow machine sleep when connections are open	This option is useful for laptop users running their laptops on batteries. If you select this check box, the laptop is allowed to go into sleep mode (and disconnect all connection) after a period of inactivity.

Interface Option	Description
Update Connection Statistics Every	Select from the pop-up menu how often the connection statistics will be updated in the Connection Manager.

2.12 Public-key authentication

F-Secure SSH Client for Macintosh creates a new random seed every time it is started. It then uses user actions to add true random elements to the pseudo random number generator. When generating new key pairs, a large amount of randomness is desirable. Therefore, you should use SSH for a while, or launch it and let it run in the background while you are working in some other program, before generating a new key pair. For normal tunneling or terminal use, a few seconds of activity will create sufficient randomness for secure connections.

To start using public-key authentication, you have to create a key-pair. Follow these steps:

Select Create Public Key Files from the File menu. The Public-key authentication Key Generator will open.

Enter a comment in the Comment field. This only identifies the key.

Select the Key Type (DSA or RSA) and the key length. The recommended key length is at least 1024 bits. Key lengths shorter than this are a security risk. Key lengths longer than 2048 bits do not provide a significant increase in security.

Enter a Passphrase used to encrypt the private key. For good security, the passphrase should be at least 11 characters long and include both lowercase and uppercase letters, numbers, and special characters. If the private key is secured by other means, the passphrase does not have to be this long.

Select one of the following options in the Clipboard pop-up menu:

- 'Copy install script' copies a script to the Clipboard for transferring the public key to the server.
- 'Copy public key' copies only the contents of the public key to the Clipboard.
- 'Leave alone' will not copy anything to the Clipboard.

Click on the **Create New Key Pair** button.

**NOTE:**

SSH1 private keys can be opened and used, but they will be converted to the SSH2 format if they are saved.

Public keys are in the SSH2 format and cannot be used with SSH1 without conversion.

You will be prompted for the name of the private key file and the public key file, and the location for saving them. Do not give a file extension to the private key file. By default, the public key is named by adding the extension `.pub` to the private key file name.

Transferring the Public Key

There are two ways to transfer the public key to the server.

1. If you used the 'Copy install script' option when creating the key pair, you can connect to the server using password authentication. Then, immediately after connecting, you can paste the contents of the Clipboard to the terminal. After this you should be able to connect using public-key authentication.

WARNING:

The script disables any keys that you are already using on the server. The script creates backup files of the old `'authentication'` and `'identity.pub'` files. Old backup files will be overwritten if the script is used again, so use the script only if you do not want to use the old keys anymore. If you want to preserve old keys, use the following method.

2. If you used the 'Copy public key' option when creating the key pair, or if you want to transfer an existing key to the server, follow these steps:
3. Copy the contents of the public key to the Clipboard. You do not need to do this if you have just created a key-pair using the 'Copy public key' option.
4. Connect to the SSH2 server using password authentication.
5. If you do not have a directory `$HOME/.ssh2`, create it with the following command:

```
mkdir $HOME/.ssh2
```
6. Change to the `$HOME/.ssh2` directory:

```
cd $HOME/.ssh2
```
7. Open or create a file called *authorization* in your favorite UNIX text editor. Add the following line:

```
Key filename
```

where *filename* is any name you want to give to the public key on the server. It does not need to be the same as on your Macintosh. Save the *authorization* file and exit.
8. Create a new file for the public key and open it. Paste the public key from the Clipboard to the file, save the file and close it.
9. Change the permissions of the two files with the following commands:

```
chmod 600 $HOME/.ssh2/authorization
```

```
chmod 600 $HOME/.ssh2/filename
```

where *filename* is the name that you gave to the public key file on the server.

Disconnect from the server and connect again, now using public-key authentication to verify that the key has been installed correctly.

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font above a stylized, dark blue and black shield-like symbol. The shield has a white 'F' shape inside it. The logo is set against a circular background with a grid pattern, resembling a globe.

F-SECURE®

Technical Support

F-Secure Technical Support is available by e-mail or from our Web site. You can access our Web site from your Web browser.

Web Club

One of the most convenient ways to reach F-Secure for information and technical support is through the World Wide Web.

You can connect directly to our Web site at the following locations:

<http://www.f-secure.com/>

<http://www.europe.f-secure.com/>

The F-Secure Support Center can be found at:

<http://www.f-secure.com/support/>

Electronic Mail Support

If you have any questions about F-Secure that are not covered in the manual or on-line services at www.F-Secure.com, you can contact your local F-Secure distributor or F-Secure directly.

For basic technical assistance, please contact your F-Secure distributor. If there is no authorized F-Secure Business Partner in your country, you can request basic technical assistance from:

F-Secure-SSH-Support@F-Secure.com

Please include the following information along with your support request:

1. Name and version number of your F-Secure software program (including the build number).

2. Name and version number of your operating system (including the build number).
3. A detailed description of the problem, including any error messages displayed by the program, and any other details that might help us duplicate the problem.

When contacting F-Secure support by telephone, please do the following so that we may help you more effectively and save time:

- Be at your computer so you can follow instructions given by the support technician, or be prepared to write down instructions.
- Have your computer turned on and (if possible) in the state it was in when the problem occurred. Or you should be ready to replicate the problem on the computer with minimum effort.

After installing the F-Secure software, you may find a README file in the following location:

- F-Secure CD-ROM (“Documentation” folder).

The README file contains the latest information.

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font above a stylized, dark blue and black shield-like graphic. The shield has a white outline and a dark blue interior with a white 'F' shape. The logo is set against a circular background with a grid pattern.

F-SECURE®

About F-Secure Corporation

F-Secure is a leading strategic provider of powerful data security solutions. The Company's products help enterprises protect corporate information and conduct electronic commerce securely. Customers in nearly every industry – Government, Manufacturing, Retail, Telecommunications, Finance, Energy, Transportation, High Tech and more – rely on F-Secure products to make information secure, reliable and accessible. F-Secure supports businesses with a broad range of centrally managed and widely distributed best-of-breed data security applications built on a highly scalable management infrastructure.

Both internal corporate IT departments and external service providers use the F-Secure approach to effectively deliver Security as a Service™ to millions of users. With F-Secure, security is centrally managed, widely distributed, seamlessly integrated, totally automated and transparent to the user.

Founded in 1988, F-Secure has been listed on the Helsinki Stock Exchange since November 1999. The company is headquartered in Helsinki, Finland with North American headquarters in San Jose, California, as well as offices in Canada, Germany, Sweden, Japan and the United Kingdom as well as regional offices in the USA. F-Secure is supported by a network of VARs and Distributors in over 80 countries around the globe. Through strategic OEM agreements the company's security applications are integrated into the services and products of leading telecommunications equipment manufacturers, such as Cisco Systems, Ericsson, Nokia and Sonera.

F-Secure has tens of thousands of customers. These include many of the world's largest industrial corporations and best-known telecommunications companies; major international airlines; European governments, post offices and defense forces; and some of the world's largest banks. Well-known customers include NASA, the US Air Force, Yahoo, US Department of Defense Medical Branch, the US Naval Warfare Center, the San Diego Supercomputer Center, Lawrence-Livermore National Laboratory, IBM, Unisys, Siemens AG, EDS, Cisco, Nokia, Sonera, UUNet Technologies, Boeing, Bell Atlantic and MCI.

F-Secure software products have received numerous international awards, prizes and citations. The company was named one of the Top 100 Technology companies in the world by Red Herring magazine in its September 1998 issue. The Company was named one of the 25 Hottest Startups in the world 1998 and its products have consistently won awards including the West Coast Labs Anti-Virus Checkmark 1999, the Virus Bulletin 100% award 1999, the Editor's Choice from the German PC Professional magazine (member of Ziff-Davis group) 1999, Hot Product of the Year 1997 from Data Communications Magazine for F-Secure VPN; and the 1996 European Information Technology Prize.

The F-Secure Product Family

F-Secure Anti-Virus™ automatically and transparently delivers the most powerful and up-to-date protection against computer viruses and malicious code to your workstations, servers, firewalls, gateways, mobile devices, and e-mail/groupware servers under one common management framework.

F-Secure Distributed Firewall™ is a software-based personal firewall that protects the mobile workforce from one centrally managed location. It protects your computer while you connect to the corporate LAN in the office, work via the Internet while traveling on the road, or telecommute from home with your always-on, broadband connection.

F-Secure VPN+™ is a software-based virtual private network that provides end-to-end security by protecting every link in the corporate network including clients, servers, and gateways. It gives traveling employees secure access to corporate resources, IT staffs the ability to secure internal networks, and corporate partners secure access through an extranet.

F-Secure FileCrypto™ is the complete centrally managed solution for protecting files stored in desktops, laptops and wireless devices across the mobile enterprise. FileCrypto enables you to automatically, effortlessly, and transparently store local data securely and keep confidential files protected by offering transparent, on-the-fly encryption that is easy to manage and use.

F-Secure Policy Manager™ provides a flexible and scalable way to manage the security of multiple applications on multiple operating systems, from one central location. With a unique distributed architecture, the F-Secure Policy Manager keeps security software up-to-date, manages configurations, oversees enterprise compliance, and scales to handle large and mobile enterprises.

F-Secure SSH™ enables remote systems administrators to access corporate network resources securely by protecting the transmission of sensitive data. F-Secure SSH provides numerous features to make secure administration and remote access connections easy to use, in a user-friendly, terminal-based application running on a wide variety of platforms.

F-Secure Workstation Suite™ is a packaged solution integrating F-Secure Anti-Virus, FileCrypto, VPN+, and Distributed Firewall, providing all the essential functionality for desktop security. The suite includes F-Secure Policy Manager, which provides centralized management, empowering the corporate administrator to install, update, upgrade, and monitor the Workstation Suite from one location.