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 sense of depth and protection. The entire logo is set against a circular background that appears to be a globe with a grid of latitude and longitude lines.

F-SECURE[®]

F-Secure SSH

for Windows

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 © 2003 F-Secure Corporation. All rights reserved.

#12000006-3E20

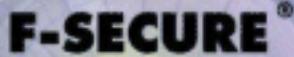
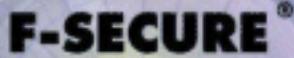
The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font. Below the text is a stylized shield or triangle shape composed of several overlapping, semi-transparent layers in shades of purple and blue, creating a sense of depth and security.

Table of Contents

1. Welcome!	1
1.1 Overview	1
1.2 The F-Secure SSH Product Family	1
F-Secure SSH Client	2
1.3 About the SSH Protocol	2
1.4 Public-Key Authentication	3
User Authentication	4
Cryptographic Methods	4
1.5 Keyboard-Interactive Authentication	5
1.6 Tunneling	6
Local Tunneling	6
Creating a Tunnel to a Third Host	8
Remote Tunneling	10
2. Installing F-Secure SSH 5.3 Client for Windows	11
2.1 Installation	11
3. Using F-Secure SSH Client	12
3.1 Creating Random Seed	12
Connecting to a Remote Host	13
Changing Hosts	14

Disconnecting	14
Cloning a connection	14
3.2 Profiles	15
Creating Profiles	15
Editing Profiles	15
Opening a Profile	15
Organizing Profiles	16
Importing Profiles	16
3.3 Working with the Terminal Window	17
Toolbar, Status Bar and Menus	17
Working with Text in the Terminal Window	22
3.4 Working with the File Transfer Window	25
Downloading Files	25
Uploading Files	26
Toolbar, Status Bar and Menus	26
3.5 Working with the Tunnel View Window	36
Main Window	36
Toolbar, Status Bar and Menus	38
3.6 Settings	43
Connection Properties	44
Cipher Properties	46
Authentication Properties	47
Firewall Properties	49
Keyboard Properties	50
Keyboard Mappings Properties	52
Tunneling Properties	53
Local Tunneling Properties	53
Remote Tunneling Properties	57
Profile-Specific File Transfer Properties	60

File Transfer Remote Favorites	61
Terminal Properties	62
Colors Properties	64
Font Properties	66
Printing Properties	67
File Transfer Properties	68
File Transfer Advanced Properties	70
File Transfer Local Favorites	72
File Transfer Mode Properties	73
Appearance Properties	74
Security Properties	76
Host Keys Properties	78
User Keys Properties	79
PKI Certificate Properties	83
PKI LDAP Server Properties	85
PKCS #11 Properties	85
PKCS #11 Configuration Properties	87
3.7 Using the Command Line Applications (ssh2, scp2, sftp2)	88
Using ssh2	88
Using scp2	92
Using sftp2	94
About F-Secure Corporation	98
The F-Secure Product Family	99

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font above a stylized shield emblem. The shield is composed of several overlapping geometric shapes in shades of purple and black, forming a triangular shape with a smaller inverted triangle inside.

1. Welcome!

1.1 Overview

F-Secure SSH Client for Windows provides users with secure login connections over untrusted networks. It acts as a replacement for the telnet protocol. Version 5.3 supports the ssh2 protocol for file transfer and both ssh1 and ssh2 protocols for terminal connections and port forwarding. It can automatically detect the protocol version available on the remote host. Because of this new functionality, F-Secure no longer supports the old F-Secure SSH 1 Client.

F-Secure SSH provides protection for a wide range of security areas. By encrypting interactive terminal, file transfer 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.

1.2 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.

About the SSH Protocol

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 fully 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.

Furthermore, F-Secure SSH Client enables users to securely transfer files between client and server. All types of files can be transferred, including configuration files, documents, and Web pages.

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.

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.

Public-Key Authentication

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 accept the key of an unknown host and store 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 refuse access to any hosts which sends an unknown key.

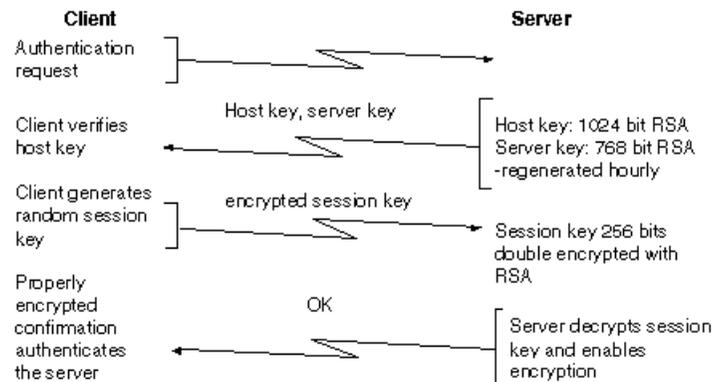


Figure 1: Host Authentication

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.

Public-Key Authentication

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

Keyboard-Interactive Authentication

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.

1.5 Keyboard-Interactive Authentication

Any currently supported authentication method that requires only the user's input, can be performed with keyboard-interactive. Currently, the following methods are supported:

- password
- securID
- PAM

New authentication methods that can be implemented with this method include, but are not limited to, the following:

- S/KEY (and other One-Time-Pads)
- hardware tokens printing a number or a string in response for a challenge sent by the server. (Like SecurID, but there are others like that.)
- legacy authentication methods.

If passing of some binary information is required (as in public-key authentication), keyboard-interactive cannot be used.

PAM has support for binary messages and client-side agents, and those cannot be supported with keyboard-interactive. However, currently there are no implementations that take advantage of the binary messages in PAM, and the specification may not be cast in stone yet.

1.6 Tunneling

When connecting to a remote server using telnet, your user name and password are sent over the Internet in plain text. Anyone can eavesdrop on your connection by using 'sniffer' software, which is freely available from the Internet. A sniffer can pick up your user name, password, and data while they are being transmitted over the Internet.

SSH can be used to effectively block any attempts to steal your password and valuable data. You can safely download your e-mail from your company's internal mail system from anywhere in the world. You can make secure telnet connections, and copy files across an untrusted network without any danger of revealing their contents to anyone. This can be achieved by using SSH tunneling, also known as port-forwarding.

Local Tunneling

A local tunnel is a secure, encrypted connection between the SSH client you are using and a remote SSHD server. Data is encrypted while it is traveling through this tunnel. However, data forwarded to a computer outside the tunnel will not be encrypted once it leaves the tunnel.

You set up your SSH client to listen to a specific port on your local host (the host you are making the connection from). When the client receives a request for data on that port, it transfers the request to a port on a remote host that you have specified.

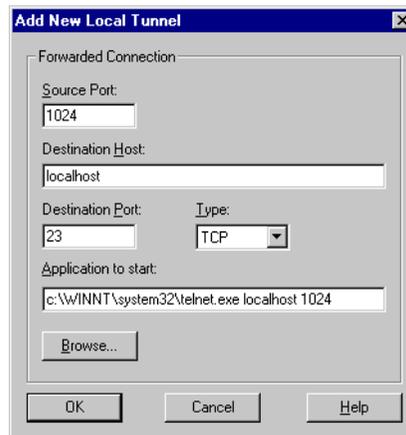
Suppose you want to create a local tunnel from one computer, called *my.computer.com*, to another computer, called *second.host.com*. To encrypt a telnet connection between these two computers, you would do the following:

1. Create an SSH connection from *my.computer.com* to *second.host.com*.
2. Tell the SSH client to listen to a specific port for TCP data requests on *my.computer.com*. The port should be greater than 1023, because many lower ports are used for other internet protocols.
3. Tell the SSH client to forward any requests received by *my.computer.com* at the specified port (port 1024, for example) to *second.host.com* at port 23 (the standard telnet port).
4. You can now connect to your own computer at port 1024, using telnet. You can define your own computer as '*127.0.0.1*' or '*localhost*'.

Tunneling

- As soon as you give the command `'telnet localhost 1024'`, the SSH client notices the request at port 1024, and immediately transfers the request through the encrypted tunnel to *second.host.com* at port 23. You are now connected to the telnet port of *second.host.com* through an SSH tunnel. You will be prompted for your user name and password just as if you were connecting directly to the telnetd server, except that all data transferred between your telnet client and the telnetd server is encrypted, making it unreadable by others.

In F-Secure SSH 5.3 for Windows, you create the tunnel in the *Local Tunneling* page of the *Properties* dialog box. The tunnel is opened as soon as you restart the SSH connection. The information needed to create the above tunnel is entered as follows:



You can start a telnet application by entering it into the *Application to Start* field, or you can run it from Windows.

The above procedure can be applied to tunneling many other kinds of data. If you create several tunnels for one connection, you just need to specify a source port that you have not yet used (>1023) and the destination port of the service you want to forward. Example commands:

- Use the following command to forward your e-mail from a pop3 server on *second.host.com*:
`ssh second.host.com -L 1110:localhost:110 (143 for imap)`

Tunneling

Then configure your e-mail client to read mail from *'localhost'*, port 1110.

- Use the following command to send e-mail through an smtp server on *second.host.com* using an e-mail editor from your own workstation:

```
ssh second.host.com -L 2525:localhost:25
```

Then configure your e-mail editor to send mail through *'localhost'* at port 2525.

- Use the following command to forward Web content from the http server on *second.host.com*:

```
ssh second.host.com -L 8080:localhost:80
```

You can then connect your Web browser to *'localhost:8080'* and receive the content.

Creating a Tunnel to a Third Host

Another way for using local tunnels is forwarding data through the SSH server to a third host. It is important to know that the data is no longer encrypted when it is transferred between the SSH server and the third host, only between your client and the server. However, when using this functionality to transfer data between your computer and a trusted intranet network, the server-to-third-host security is not an issue.

The main application for this is to enable people to access data, such as e-mail, Web content or news from an intranet server that does not allow direct connections to these servers. In many cases, your only way of accessing your company intranet from the internet is through a single SSH server. Once able to access that server, you can then continue from there to connect to the other servers running inside the intranet.

With SSH tunnels, you can create a connection directly to these servers otherwise inaccessible to you. This is done by specifying the destination host as something other than *'localhost'*.

Suppose you want to read your e-mail from a pop3 server in your company intranet, from home. You make an SSH connection to *my.company.com*, tell the SSH client to listen for data requests at some port in your home computer, for example 1110, and to forward any received data requests to the pop3 server at the pop3 port (110) of your company through the SSH server.

In UNIX, the SSH command is the following:

```
ssh my.company.com -L 1110:pop3.company.com:110
```

This command means, “Make an ssh connection to *my.company.com*, and create a local tunnel that listens to local port 1110 and forwards any TCP requests arriving at that port to the pop3 port (110) of *pop3.company.com*.”

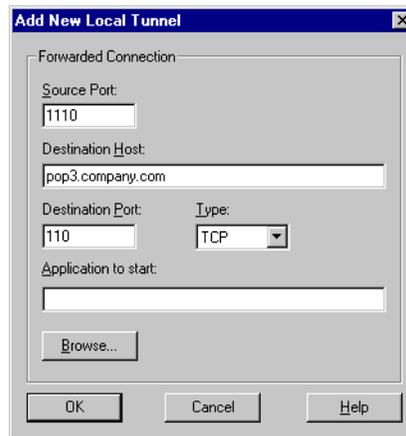
If you are using an imap mail server (port 143), the command is:

Tunneling

```
ssh my.company.com -L 1110:pop3.company.com:143
```

This done, you configure your e-mail client to search for e-mail at *'localhost'* at port *'1110'*. You will be asked for your username and password when the e-mail client first attempts to retrieve mail. You must give the ones for the e-mail server, not the ones for the SSH server.

In F-Secure SSH 5.3 for Windows, you create the tunnel in the *Local Tunneling* page of the *Properties* dialog box. The tunnel is opened as soon as you restart the SSH connection. The information needed to create the above tunnel is entered as follows:



This can all be applied to tunneling many other kinds of data. If you create several tunnels for one connection, you just need to specify a source port that you have not used yet (>1023 for UNIX non-root), the DNS name or IP address of the server and the destination port of the service you want to forward. Here are three example commands:

- To forward your telnet connection from a telnet server on *telnet.company.com* through the company's external SSH server:

```
ssh my.company.com -L 2323:telnet.company.com:23
```

Then connect to *'localhost'* at port 2323 with a telnet client.

- To send e-mail through an smtp server on *smtp.company.com* through the company's external SSH server, using an e-mail editor from your own workstation:

```
ssh my.company.com -L 2525:smtp.company.com:25
```

Tunneling

Then configure your e-mail editor to send mail through *'localhost'* at port 2525.

- To forward Web content from the http server on intraweb.company.com through the company's external SSH server:

```
ssh my.company.com -L 8080:intraweb.company.com:80
```

You can then connect your Web browser to *'localhost:8080'* to receive the content.

Remote Tunneling

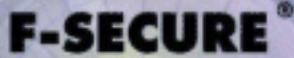
In remote tunneling, you do quite the opposite from local tunneling. You make an SSH connection to a server, then tell the SSH client to listen to data requests received by the host the SSH server is on, at the port you specify, and to transfer that data request to your computer, or a third host. Again, the data is not encrypted outside the tunnel, that is if you forward the data to a third host. Here are two example commands:

- To create an SSH tunnel to *my.company.com* and tell the SSH client to listen for data requests at port 2323 on that server, and forward all received data requests to port 23 of your workstation:

```
ssh my.company.com -R 2323:localhost:23
```

- To create an SSH tunnel to *my.company.com* and tell the SSH client to listen for data requests at port 2323 on that server, and forward all received data requests to port 23 of your *third.host.com*:

```
ssh my.company.com -R 2323:third.host.com:23
```

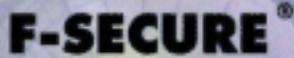
The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font. Below the text is a stylized shield or triangle shape composed of several overlapping, nested shapes in shades of purple and black.

2. Installing F-Secure SSH 5.3 Client for Windows

2.1 Installation

To install the F-Secure SSH Client, follow these steps:

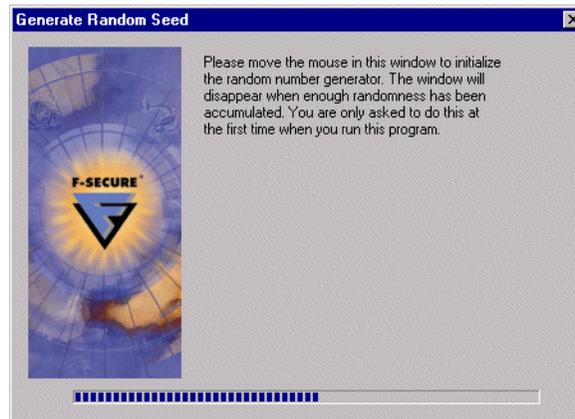
1. Run the F-Secure SSH Client setup program.
2. Enter the keycode you received with the software, when prompted.
3. When asked, provide the directory in which to install the program and the *Start* menu path in which to place the shortcuts.
4. Follow the installation wizard to the end.

The logo for F-Secure, featuring the text "F-SECURE" in a bold, black, sans-serif font above a stylized, black and white geometric shield-like symbol.

3. Using F-Secure SSH Client

3.1 Creating Random Seed

The first time you start the F-Secure SSH Client, a random seed generator will be launched. The random seed needs to be generated before any host or user keys can be generated. The random seed functions as the starting point for creating the keys. The random seed is also used to create randomness in all encryption processes and TCP packets.



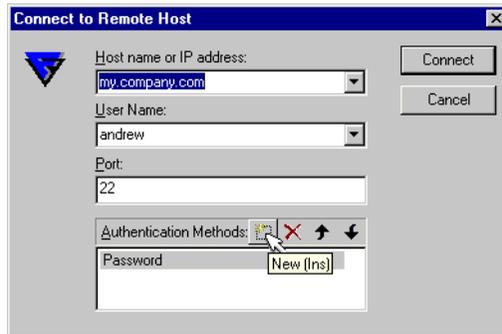
To create the random seed, move your mouse pointer in the window until the progress indicator reaches the end. When the random seed has been generated, F-Secure SSH Client will be launched.

Creating Random Seed

Connecting to a Remote Host

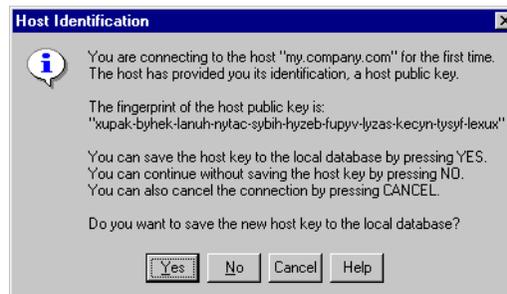
Start the F-Secure SSH Client from the Windows Start menu under *Programs > F-Secure SSH Client*. To connect to a remote computer, follow these steps:

When you start F-Secure SSH Client, the Connection dialog box should open automatically. If it does not, press **ENTER** or **SPACE**, or click the **Quick Connect** button in the *Profile Bar*. Type the name or IP address of the host you want to connect to, and your user name on the remote host. If you know that the SSH server uses a port other than the default 22, change the port number to that. Add an Authentication Method by clicking on the **New** button as shown in the picture below. You can add any of the three methods available, which are Password, Public Key and SecurID. You can change the order in which the different methods are tried by selecting a method with your mouse and moving it up or down on the list by clicking on the up and down arrows.



After giving the required information, click **OK**.

The first time you connect to a particular host, the following message will be displayed.



Creating Random Seed

If you click **Yes, the** host key will be added to the local host key database for future reference and you will be connected to the host. If you click **No**, the host key will not be saved, but you will still be connected to the host. Clicking **Cancel** will not save the host key, and will cancel the connection to the host.

You will now be connected to the remote server, as long as the information you have provided is correct and the host you are connecting to supports SSH.

Changing Hosts

If you want to change hosts without quitting the program, do the following:

1. Disconnect from the host you are connected to, either by choosing Disconnect from the File menu, clicking the Disconnect icon on the toolbar or by logging out of the server using the associated UNIX command (`exit`, `logout`, or `quit`).
2. Press `ENTER` or the `SPACE BAR` to open the Connection dialog box, or choose Connect from the File menu.
3. Type the name or IP address of the host you want to connect to, and enter your user name on the remote host. The authentication method should be set to Password, unless you have already created and transferred a public key to the host.
4. Click **OK**.

Disconnecting

To close the connection, do one of the following:

- If you have a terminal session active in the terminal window, enter the command to log out from the remote system. This command is commonly called `logout`, `exit`, or `quit`.
- Choose Disconnect from the File menu.
- Click on the Disconnect button in the toolbar.

Cloning a connection

You can clone a connection by either choosing *New Terminal* or *New File Transfer* from the *Window* menu, or by clicking their respective icons in the toolbar. If the connection in your original window is open, the clone windows will be connected as well. All cloned windows, both terminals and file transfer windows, use the connection made from the original window.

3.2 Profiles

Creating Profiles

Profiles allow you to save different configurations for your connections. In addition, they allow you to open multiple connections with different host names, user names and passwords without constantly having to return to the Settings dialog box. You can create a Profile from an existing open connection or from a previously saved Profile. For information on settings you can change in the Settings dialog box, see “Settings”.

To create a Profile, follow these steps:

1. From the *File* menu, choose *Profiles > Add Profile*. You can also click on the **Profiles** button in the toolbar and select *Add Profile* from the drop-down list that opens.
2. Give a name for the new profile in the *Add Profile* dialog box.

Editing Profiles

To edit a Profile, follow these steps:

1. From the *File* menu, choose *Profiles > Edit Profile*. You can also click on the **Profiles** button in the toolbar and select *Edit Profile* from the drop-down list that opens.
2. Go through the *Settings* panes and enter all the information you want to apply to the profile.
3. Click **OK** when you are done. Remember to save the Profile. You can save it by clicking on the **Save** button or selecting *Save* from the *File* menu.

Opening a Profile

To open a profile, go to *File > Profiles* or click the **Profiles** button on the toolbar and select the profile you want to open from the drop-down list that opens. If there are no profiles in the list, you need to create a profile.

You can also open a profile by right-clicking in the tree structure on the left pane of the *Edit Profile* dialog box and double-clicking on the Profile you want to open.

Profiles

Organizing Profiles

You can organize your Profiles into folders and subfolders from the *Edit Profiles* dialog box. To do that, follow these steps:

1. From the *File* menu, choose *Profiles > Edit Profile*. You can also click on the **Profiles** button in the toolbar and select *Edit Profile* from the drop-down list that opens.
2. You can create a new folder in the tree structure on the left pane of the dialog box. If you right-click on a folder and select *New Folder*, the folder will be created as a subfolder to that folder. If you right-click on the background and select *New Folder*, the folder will be created as a primary level folder.

Importing Profiles

You can import File Transfer Profiles from F-Secure SSH FTP versions 4.2 and later. You can also import Terminal profiles from the previous version of F-Secure SSH Client (4.2 and later). To do this, follow these steps:

- From the *File* menu, choose *Profiles > Import Profile*. You can also click on the **Profiles** button in the toolbar and select *Import Profile* from the drop-down list that opens.

For F-Secure SSH FTP Profiles:

- Select the Profile(s) you want to import from the list and click the **Import** button on the right side of the dialog box.

For F-Secure SSH Client Profiles:

- Click the **Import from F-Secure SSH Client** button. Browse for your saved *.ssh* files. Click **OK** to import the file(s).

3.3 Working with the Terminal Window

Toolbar, Status Bar and Menus

Toolbar

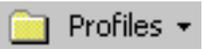
The toolbar in the F-Secure SSH Client is divided into eight sections.

Section	Description
	The first section contains just one button, the Save button. Clicking it will save any changes you may have done to the current settings to the current profile, including which windows are open. If you have not opened a profile, the settings are saved to the Default Profile.
	The second section contains two buttons. The Print button opens the <i>Print</i> dialog box. The Print Preview button shows you what the printout will look like. You can affect the formatting of the printout by adjusting the Printing Settings. For more information, see the section.
	The third section contains the Connect and Disconnect buttons. Only one of them is activate at a time; the other one is grayed. Clicking the Connect button opens a connection to the host specified in the currently active profile. If no host is specified in the settings, the <i>Quick Connection</i> dialog box will open.
	The next three buttons are Copy , Paste and Paste Selection . Copy and Paste are standard Windows clipboard tools. Paste Selection pastes the currently selected text at the prompt.
	The Find button can be used to search for text in the scrollback buffer.
	The next three buttons are New Terminal Window , New File Transfer Window and New Tunnel View Window . Respectively, they open a new Terminal, File Transfer or Tunnel View window. Their settings are based on the settings of the window you clicked them in. If you have an open connection when you click these buttons, they will be started with an open connection as well.

Working with the Terminal Window

Section	Description
	The Settings button opens the <i>Settings</i> dialog box where you can adjust all the settings for your current profile.
	The Online Help button opens the online help. The Help button lets you click on an item in the user interface and get more information on it.

Profiles Bar

Button	Description
	The Quick Connect button opens a new terminal window based on the default profile. Clicking on the Quick Connect button in an empty, unconnected terminal window opens the <i>Quick Connection</i> dialog box.
	The Profiles button opens a drop-down list that gives you access to adding, editing, importing and opening profiles.

Status Bar

At the bottom of your terminal window, the status bar displays information about the connection and current settings. To display the status bar, choose Status Bar from the View menu.



Connected to localhost - /C:/program files/f-sec | SSH2 - 3des-cbc - hmac-sha1 - zlib | 9 Items (4,9 KB) | 00:07:14

The status of your current connection is displayed on the left side of the status bar. It will display “Connected to...”, “Press Enter/Space to connect”, or “Connecting to...”.

The status bar also shows the ssh protocol being used, which cipher is being used, whether compression is enabled or not, the terminal window size (in characters), the cursor position (line and column) and the time elapsed since the connection was made.

Working with the Terminal Window

Menus

File menu option	Function
Save Layout	Saves both the current settings and the current window layout.
Save Settings	Saves all the current settings to the currently active profile.
Quick Connect	Opens the Quick Connection dialog box.
Profiles	Gives you access to adding, editing, importing and opening profiles.
Print...	Print the terminal output. You can print the buffer (up to 500 lines), the visible screen, or the selected text. You can direct the output to a file, and select the print quality and number of copies to print.
Print Setup...	Select the printer to use, paper size, paper source and orientation, and printer properties.
Print Preview	Displays what the printout will look like.
Page Setup	Opens the <i>Printing</i> pane of the <i>Settings</i> dialog box.
Log Session	Logs the session to a file.
Raw Log Session	Stores all data received by the terminal emulator, including escape sequences.
Connect	The Connect option will be active if there is no open connection. Choose Connect to open the connection dialog box for starting a connection using your current terminal settings.
Disconnect	The Disconnect option will be displayed if you have an open connection. Choose Disconnect to disconnect from the remote host.
Exit	Closes the terminal and exits F-Secure SSH 5.3 Client. Before exiting, you should disconnect from the server and close all programs that use tunnels created by SSH.

Working with the Terminal Window

Edit menu option	Function
Copy	Copy selected text to the clipboard.
Paste	Paste the text from the Windows clipboard to the terminal command line.
Paste Selection	Paste the selected text to the command line. This will leave the contents of the clipboard unchanged.
Select All	Select all text in the terminal window and scrollback buffer.
Select Screen	Select all the text visible in the terminal window.
Select None	Unselect any selections.
Find	Search for text in the scrollback buffer.
Settings	Edit the Settings for the active profile.

View menu option	Function
Toolbar	If selected, shows the toolbar below the menu bar.
Status Bar	If selected, shows the status bar at the bottom of the terminal window.
Profiles Bar	If selected, shows the Profiles bar below the toolbar.
Reset Toolbars	Resets the toolbars to their default positions.
Reset Terminal	Clears the visible terminal and the scrollback buffer.

Window menu option	Function
New Terminal	Opens a new terminal window using the settings from the current window's settings. If the current window is connected to a host, the new window will be connected, too, when it is opened.

Working with the Terminal Window

Window menu option	Function
New File Transfer	Opens a new file transfer window using the settings from the current window's settings. If the current window is connected to a host, the new window will also be connected, when it is opened.
New Tunnel View	Opens a new tunnel view window using the settings from the current window's settings. If the current window is connected to a host, the new window will also be connected, when it is opened.
New Terminal in Current Directory	Opens a new terminal window in the current directory.
New File Transfer in Current Directory	Opens a new terminal window in the current directory.
Close	Close the currently active terminal or file transfer window. This will not affect other clones of the connection. If you close the last window for a connection, the client disconnects from the server.
Close All Others	Close all windows for the current connection except the currently active window.

Working with the Terminal Window

Help menu option	Function
Contents	Start the Online Help that comes with the product.
F-Secure on the Web:	
Online Help	Open the Web Online Help HTML pages for F-Secure SSH Client 5.3.
Web Club	Connect to the F-Secure SSH Web Club through the Internet. An Internet connection must exist for this option to work.
Troubleshooting	Shows data the program has gathered during its operation. This data can be sent to F-Secure SSH support in case of problems with the software.
Debugging	Opens the Debugging dialog.
About	Displays version and copyright information.

Working with Text in the Terminal Window

Selecting All Lines in the Scrollback Buffer

To select all the text in the scrollback buffer, do one of the following:

- Drag the mouse across all of the lines.
- Go to the *Edit* menu and select *Select All*.
- Right-click, and click *Select All* on the shortcut menu.
- Click the mouse four times.

Selecting a Word on the Screen

To select a single word on the screen, do one of the following:

- Drag the mouse across the word.
- Double-click on the word.

Working with the Terminal Window

Selecting a Line of Text on the Screen

To select a line of text on the screen, do one of the following:

- Drag the mouse across the line of text.
- Triple-click on the line you want to select.

Finding Text in the Scrollback Buffer

To access the *Find* dialog box, do one of the following:

- Choose *Find* in the *Edit* menu.
- Right-click anywhere in the terminal and select *Find* in the menu that appears.

The *Find* dialog box is a standard Microsoft Windows Find box. You can enter the text you want to search for, and the direction of the search. Selecting the *Match whole word only* check box finds only whole words that match the search criteria.

Click  to view a menu with more search options.

Copying Text to the Clipboard

To copy text to the Clipboard, do one of the following:

- Select the text you want to copy.
- Choose *Copy* from the *Edit* menu. Or right-click and click *Copy* on the shortcut menu. Or press CTRL+INSERT.

After copying text to the clipboard, you can paste it into SSH or another Windows application.



You can also select to use X11 style selection from the Terminal pane of the Settings dialog box. X11 style selection means that any text that you select immediately replaces the contents of the clipboard.



You can right-click on the terminal window to open a shortcut menu that has most of the Edit commands.

Working with the Terminal Window

Pasting Text to the Command Line from the Clipboard

To paste text from the clipboard, do one of the following:

- Choose *Paste* from the *Edit* menu.
- Press SHIFT+INS.
- Right-click in the terminal window and click *Paste* on the shortcut menu.

Pasting the Selected Text Without Affecting the Clipboard

To directly paste text you have selected in the terminal window, do one of the following:

- Choose *Paste Selection* from the *Edit* menu.
- Right-click in the terminal window and click *Paste Selection* on the shortcut menu.
- If you have a three-button mouse, press the middle button.
- You can emulate a three-button mouse with a two-button mouse. Choose *Emulate 3-Button Mouse* from the *Appearance* page of the *Properties* dialog box. Select the text in the terminal window you want to paste, hold down the right mouse button, and click the left mouse button.

Clearing the Screen

To clear the screen while preserving the contents of the scrollback buffer, do one of the following:

- Choose *Clear Screen* from the *Edit* menu.
- Right-click the mouse and click *Clear Screen* on the shortcut menu.

Clearing the Scrollback Buffer

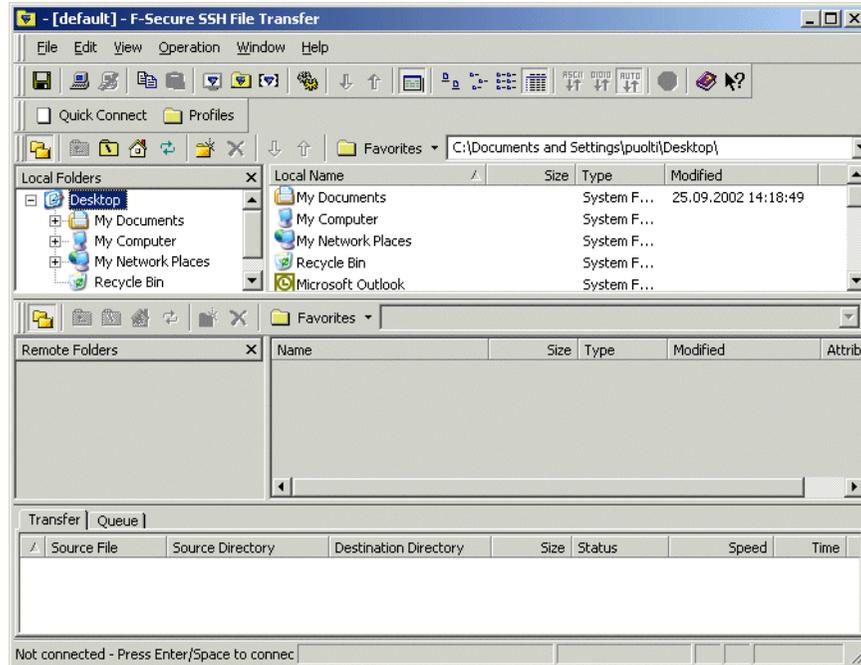
To clear the scrollback buffer while preserving the contents of the visible terminal, do one of the following:

- Choose *Clear Scrollback* from the *Edit* menu.
- Right-click the mouse and click *Clear Scrollback* on the shortcut menu.

Resetting the Terminal

To clear the contents of both the scrollback buffer and the visible terminal window, choose *Reset Terminal* from the *Edit* menu.

3.4 Working with the File Transfer Window



Downloading Files

To download files, first select them with your mouse. You can select multiple files by holding down the CTRL key while selecting. The files are downloaded to a directory on your computer that you select from the dialog box that opens. There are several ways to download the files:

- Right-click the mouse on one of the files selected for downloading and select Download from the menu that appears.
- Select *Download* from the *Operation* menu.
- Press Ctrl+D.
- Click and hold the left mouse button and drag the files to a folder on the local computer.

Working with the File Transfer Window

Uploading Files

To upload files, click the **Upload** button, press Ctrl+U or select Upload from the Operation menu. This opens a dialog box where you can select files to upload to the currently active directory on the remote host.

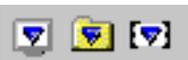
Select the files you wish to upload with your mouse. You can select multiple files by holding down the CTRL key while selecting. The files are uploaded to the currently active directory on the remote host.

You can also drag files from a Windows Explorer window to a folder on the remote host. You can start Windows Explorer either from the Window menu or by any of the standard Windows means.

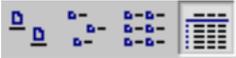
Toolbar, Status Bar and Menus

Toolbar

The toolbar in the F-Secure SSH File Transfer Client is divided into nine sections.

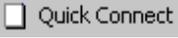
Section	Description
	The first section contains just one button, the Save button. Clicking it will save any changes you may have done to the current settings to the current profile, including which windows are open. If you have not opened a profile, the settings are saved to the Default Profile.
	The second section contains the Connect and Disconnect buttons. Only one of them is activate at a time; the other one is grayed. Clicking the Connect button opens a connection to the host specified in the currently active profile. If no host is specified in the settings, the <i>Quick Connection</i> dialog box will open.
	The next two buttons are Copy and Paste . They are the standard Windows clipboard tools. You can select any number of files and then copy them to the clipboard. Then, you go to the destination and paste them.
	The next three buttons are New Terminal Window , New File Transfer Window and New Tunnel View Window . Respectively, they open a new Terminal, File Transfer or Tunnel View Window. Their settings are based on the settings of the window you clicked them in. If you have an open connection when you click these buttons, they will be started with an open connection as well.

Working with the File Transfer Window

Section	Description
	<p>The Settings button opens the <i>Settings</i> dialog box where you can adjust all the settings for your current profile.</p>
	<p>The Download Dialog button opens the Download-Select Folder dialog that allows you to select a folder on the local computer and transfers the currently selected file into it.</p> <p>The Upload Dialog button opens the Upload - Select Files dialog that allows you to select a file and transfer it from the local computer into the remote host computer.</p>
	<p>Opens/closes the Transfer View window at the bottom of the page.</p>
	<p>The next four buttons are the standard Windows Explorer file display mode buttons. They are Large icons, Small icons, List, Details.</p>
	<p>The ASCII button sets file transfer to be in ASCII mode. The Binary button sets file transfer to be in binary mode. The Auto Select button sets all files to be transferred in binary mode, except files using a file extension specified on the ASCII Extensions list.</p>
	<p>The Cancel Transfer button stops the current transfer. It is only active when a transfer is in progress.</p>
	<p>The Online Help button opens the online help. The Help button lets you click on an item in the user interface and get more information on it.</p>

Working with the File Transfer Window

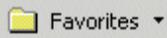
Profiles Bar

Button	Description
	The Quick Connect button opens a new terminal window based on the default profile. Clicking on the Quick Connect button in an empty, unconnected terminal window opens the <i>Quick Connection</i> dialog box.
	The Profiles button opens a drop-down list that gives you access to adding, editing, importing and opening profiles.

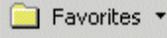
Local bar

Button	Description
	Pressing down the Show/Hide Local Folders button displays the a view of the subfolders of the local folder you currently have active.
	Next, there are three buttons for browsing the remote host file system. The first one, Go to parent folder , takes you to the parent directory of the directory you are currently in, provided you have the rights to access that directory. The second button, Go to root folder , takes you to the root directory of the file system, again provided you have the rights to access it. The third button, Go to user home directory , takes you to your assigned home directory on the system.
	Clicking the Refresh button refreshes the contents of the directory you are in.
	Clicking the New Folder button opens a new folder in the right-side local folder window and prompts you to name the new folder. Click the Delete button to delete the selected folder. A dialog is displayed that asks to confirm the deletion. (Click OK to delete the folder.)
	These two buttons are used for file access. the Download button initiates the download of the files you have selected on the remote host. If no files are selected, this button is grey. The Upload button opens a dialog box where you can select files to upload to the currently active directory on the remote host.

Working with the File Transfer Window

Button	Description
	Displays a menu of the folders you have selected to be your favorites.

Remote bar

Button	Description
	Pressing down the Show/Hide Remote Folders button displays the a view of the subfolders of the remote folder you currently have active.
	Next, there are three buttons for browsing the remote host file system. The first one, Go to parent folder , takes you to the parent directory of the directory you are currently in, provided you have the rights to access that directory. The second button, Go to root folder , takes you to the root directory of the file system, again provided you have the rights to access it. The third button, Go to user home directory , takes you to your assigned home directory on the system.
	Clicking the Refresh button refreshes the contents of the directory you are in.
	Clicking the New Folder button opens a new folder in the right-side remote folder window and prompts you to name the new folder. Click the Delete button to delete the selected folder. A dialog is displayed that asks to confirm the deletion. (Click OK to delete the folder.)
	Displays a menu of the folders you have selected to be your favorites.

Status Bar

At the bottom of your File Transfer window, the status bar displays information about the connection and current settings. To display the status bar, choose Status Bar from the View menu.

Connected to localhost - /C:/program files/f-sec | SSH2 - 3des-cbc - hmac-sha1 - zlib | 9 Items (4,9 KB) | 00:07:14

Working with the File Transfer Window

The status of your current connection is displayed on the left side of the status bar. It will display “Connected to...”, “Press Enter/Space to connect”, or “Connecting to...”.

The status bar also shows the currently active directory on the remote host, the ssh protocol being used, which cipher is being used, the number of items in the currently active folder or the number of selected items if you have selected something, and the time elapsed since the connection was made.

Working with the File Transfer Window

Menus

File menu option	Function
Save Layout	Saves both the current settings and the current window layout.
Save Settings	Saves all the current settings to the currently active profile.
Quick Connect	Opens the Quick Connection dialog box.
Profiles	Gives you access to adding, editing, importing and opening profiles.
Connect	The Connect option will be active if there is no open connection. Choose Connect to open the connection dialog box for starting a connection using your current terminal settings.
Disconnect	The Disconnect option will be displayed if you have an open connection. Choose Disconnect to disconnect from the remote host.
Exit	Closes the terminal and exits F-Secure SSH 5.3 Client. Before exiting, you should disconnect from the server and close all programs that use tunnels created by SSH.

Edit menu option	Function
Copy	Copy selected text to the clipboard.
Cut	Cut selected text to the clipboard.
Paste	Paste the text from the Windows clipboard to the terminal command line.
Select All	Select all text in the terminal window and scrollbar buffer.
Settings	Edit the Settings for the active profile.

Working with the File Transfer Window

View menu option	Function
Toolbar	If selected, shows the toolbar below the menu bar.
Status Bar	If selected, shows the status bar at the bottom of the terminal window.
Profiles Bar	If selected, shows the Profiles bar below the toolbar.
File Bar	If selected, shows the File bar below the Profiles bar.
Reset Toolbars	Resets the toolbars to their original positions
Local View	If selected, shows the Local View on the left side of the window. By default, Local View displays the contents of your local home directory - usually your Windows desktop.
Transfer View	If selected, shows the Transfer view at the bottom of the window.
Large Icons	Show the contents of the currently active folder as large icons.
Small Icons	Show the contents of the currently active folder as small icons.
List	Show the contents of the currently active folder as a list.
Details	Show the contents of the currently active folder as a list with details such as file size, modification time, attributes, etc.
Arrange Icons	Select whether to arrange the icons by name, type, size or date.
Show Root Folder	When selected, the directory tree starts from the root folder of the system. When unselected, the directory tree starts from your assigned home directory.
Show Hidden Files	When selected, you also see (and can select) hidden files. When not selected, you cannot see (or select) hidden files.
Refresh	Refresh the contents of the currently active directory.

Working with the File Transfer Window

Operation menu option	Function
View	View the currently selected file in read-only mode with the program associated with it. In the Settings, you can specify a program to use for viewing files that have no file associations.
Open	Open the currently selected file for editing with the program associated with it. You cannot open a file that does not have file associations.
Edit	Open a file for ASCII editing.
Upload	Opens a dialog box that asks you for files to download to the currently active folder on the remote host.
Download	Only available if you have selected a file or a folder on the remote host. Opens a dialog box that asks you where to download the file.
Upload Dialog	Opens the Upload-Select Files dialog that allows you to select a file and transfer it from the local computer into the remote host computer. The shortcut key for Upload Dialog is Ctrl+U.
Download Dialog	Open the Download-Select Folder dialog that allows you to select a folder on the local computer and transfer the currently selected file into it. The shortcut key for Download Dialog is Ctrl+D.
Cancel Transfer	To stop transferring the files, select the files that you do not want to be transferred, right-click the Transfer page and then select Cancel Transfer.
Up	Go to the parent folder of the currently active folder.
Root	Go to the root directory.
Home	Go to the home directory assigned to you on the remote host.
Go to Folder	Opens a dialog box that asks you for a folder to go to on the remote host.

Working with the File Transfer Window

Operation menu option	Function
New Folder	Creates a new folder in the currently active folder on the remote host. You need to give it a name.
Delete	Deletes the currently selected file(s) or folder(s).
Rename	Renames the currently selected file or folder.
Properties	View and change the permissions of the selected remote file(s). You can select multiple files and set their permissions at once. When setting multiple permissions at once, the permission check boxes have three functions: <ol style="list-style-type: none"> 1. Not selected. This removes the permission on all selected files. 2. Selected. This sets the permission on all selected files. 3. Grayed. This leaves the permission on each selected file as it was.
File Transfer Mode	Select your desired file transfer mode. <i>Auto Select</i> sets all files to be transferred in binary mode, except files using a file extension specified on the ASCII Extensions list.
Favorite Remote Folders	Add, delete or edit favorite remote folders.
Favorite Local Folders	Add, delete or edit favorite local folders.

Window menu option	Function
New Terminal	Opens a new terminal window using the settings from the current window's settings. If the current window is connected to a host, the new window will also be connected when it is opened.
New File Transfer	Opens a new file transfer window using the settings from the current window's settings. If the current window is connected to a host, the new window will also be connected when it is opened.

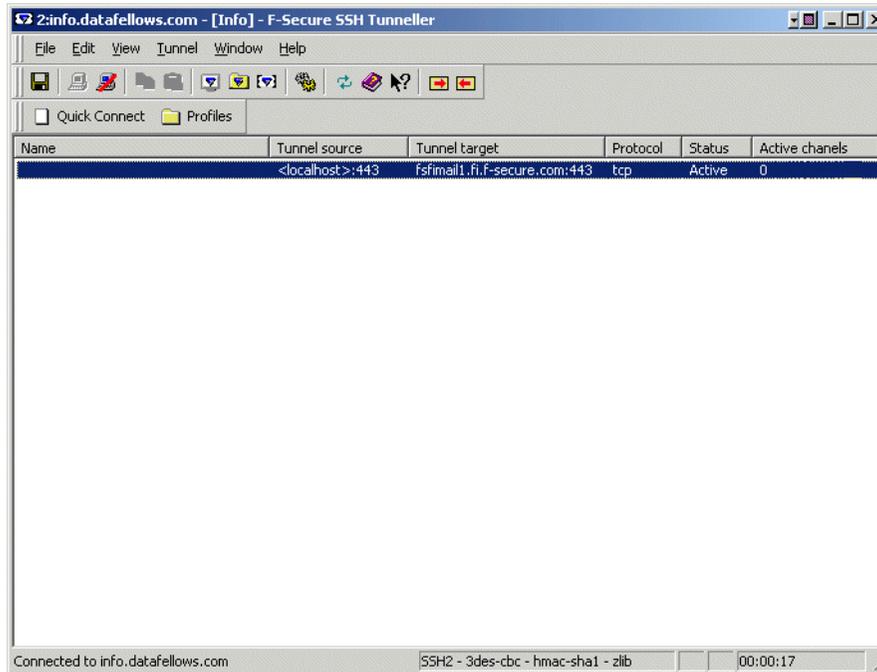
Working with the File Transfer Window

Window menu option	Function
New Tunnel View	Opens a new tunnel view window.
New Terminal in Current Directory	Opens a new terminal window in the current directory.
New File Transfer in Current Directory	Opens a new terminal window in the current directory.
New Explorer	Opens a new Windows Explorer window.
Close	Close the currently active terminal or file transfer window. This will not affect other clones of the connection. If you close the last window for a connection, the client disconnects from the server.
Close All Others	Close all windows for the current connection except the currently active window.

Help menu option	Function
Contents	Start the Online Help that comes with the product.
F-Secure on the Web:	
Online Help	Open the Web Online Help HTML pages for F-Secure SSH Client 5.3.
Web Club	Connect to the F-Secure SSH Web Club through the Internet. An Internet connection must exist for this option to work.
Troubleshooting	Shows data the program has gathered during its operation. This data can be sent to F-Secure SSH support in case of problems with the software.
Debugging	Opens the Debugging window.
About	Displays version and copyright information.

3.5 Working with the Tunnel View Window

Main Window



In the main Tunnel View Window, you see the status of the tunnels you have created. The first column shows the source of the tunnel as a valid address followed by the port number used at the source end of the tunnel. The second column shows the target of the tunnel in the same way, as a valid address followed by the port number the connection is forwarded to. The third column shows the protocol used in the tunnel, which can only be tcp or ftp. The fourth column shows the status of the tunnel. It can be either *Active*, *Not Ready*, *Not connected* or *Failed*.

An *Active* tunnel has been successfully created and connected and is available for the transfer of data through it. *Not connected* means that there is no connection to the host. *Not ready* means that the tunnel is being formed, but it is waiting for something, such as authentication. *Failed* means that an error of some kind has occurred. Usually it means that another tunnel is already using the same port at either end of the tunnel. Another possibility is that the user is not allowed to use the specified port for creating a tunnel. For

Working with the Tunnel View Window

example, in the UNIX environment usually only the root account has rights to create a tunnel to a port below 1024 on a UNIX machine.

The fifth column in the Tunnel View Window shows the number of transfers currently going through the tunnel.

Working with the Tunnel View Window

Toolbar, Status Bar and Menus

Toolbar

The toolbar in the F-Secure SSH File Transfer Client is divided into nine sections.

Section	Description
	The first section contains just one button, the Save button. Clicking it will save any changes you may have done to the current settings to the current profile, including which windows are open. If you have not opened a profile, the settings are saved to the Default Profile.
	The second section contains the Connect and Disconnect buttons. Only one of them is activate at a time; the other one is grayed. Clicking the Connect button opens a connection to the host specified in the currently active profile. If no host is specified in the settings, the <i>Quick Connection</i> dialog box will open.
	The next two buttons are Copy and Paste . They are the standard Windows clipboard tools. You can select any number of files and then copy them to the clipboard. Then, you go to the destination and paste them.
	The next three buttons are New Terminal Window , New File Transfer Window and New Tunnel View Window . Respectively, they open a new Terminal, File Transfer or Tunnel View window. Their settings are based on the settings of the window you clicked them in. If you have an open connection when you click these buttons, they will be started with an open connection as well.
	The Settings button opens the <i>Settings</i> dialog box where you can adjust all the settings for your current profile.
	Clicking the Refresh button refreshes the tunnel view window to show you the latest status of the tunnels you have created. The Online Help button opens the online help. The Help button lets you click on an item in the user interface and get more information on it.

Working with the Tunnel View Window

Section	Description
	The New Local Forwarding and New Remote Forwarding buttons can be used to open the dialog box for creating a new tunnel on the fly.

Profiles Bar

Button	Description
	The Quick Connect button opens a new terminal window based on the default profile. Clicking on the Quick Connect button in an empty, unconnected terminal window opens the <i>Quick Connection</i> dialog box.
	The Profiles button opens a drop-down list that gives you access to adding, editing, importing and opening profiles.

Status Bar

At the bottom of your Tunnel View window, the status bar displays information about the connection and current settings. To display the status bar, choose Status Bar from the View menu.



The status of your current connection is displayed on the left side of the status bar. It will display “Connected to...”, “Press Enter/Space to connect”, or “Connecting to...”.

The status bar also shows the ssh protocol, cipher, hmac and compression method being used.

Working with the Tunnel View Window

Menus

File menu option	Function
Save Layout	Saves both the current settings and the current window layout.
Save Settings	Saves all the current settings to the currently active profile.
Quick Connect	Opens the Quick Connection dialog box.
Profiles	Gives you access to adding, editing, importing and opening profiles.
Connect	The Connect option will be active if there is no open connection. Choose Connect to open the connection dialog box for starting a connection using your current terminal settings.
Disconnect	The Disconnect option will be displayed if you have an open connection. Choose Disconnect to disconnect from the remote host.
Exit	Closes the terminal and exits F-Secure SSH 5.3 Client. Before exiting, you should disconnect from the server and close all programs that use tunnels created by SSH.

Edit menu option	Function
Copy	Copy the selected text to the clipboard.
Paste	Paste the text from the Windows clipboard to the terminal command line.
Select All	Select all text in the terminal window and scrollbar buffer.
Settings	Edit the Settings for the active profile.

View menu option	Function
Toolbar	If selected, shows the toolbar below the menu bar.

Working with the Tunnel View Window

View menu option	Function
Status Bar	If selected, shows the status bar at the bottom of the terminal window.
Profiles Bar	If selected, shows the Profiles bar below the toolbar.
Reset Toolbars	Resets the toolbars to their original positions.
Refresh	Refreshes the contents of the currently active directory.

Tunnel menu option	Function
New Local Tunnel	Creates a new local tunnel on the fly.
New Remote Tunnel	Creates a new remote tunnel on the fly.

Window menu option	Function
New Terminal	Opens a new terminal window using the settings from the current window's settings. If the current window is connected to a host, the new window will be connected, too, when it is opened.
New File Transfer	Opens a new file transfer window using the settings from the current window's settings. If the current window is connected to a host, the new window will be connected, too, when it is opened.
New Tunnel View	Opens a new tunnel view window using the settings from the current window's settings. If the current window is connected to a host, the new window will be connected, too, when it is opened.
Close	Close the currently active terminal or file transfer window. This will not affect other clones of the connection. If you close the last window for a connection, the client disconnects from the server.
Close All Others	Close all windows for the current connection except the currently active window.

Working with the Tunnel View Window

Help menu option	Function
Contents	Start the Online Help that comes with the product.
F-Secure on the Web:	
Online Help	Open the Web Online Help HTML pages for F-Secure SSH Client 5.3.
Web Club	Connect to the F-Secure SSH Web Club through the Internet. An Internet connection must exist for this option to work.
Troubleshooting	Shows data the program has gathered during its operation. This data can be sent to F-Secure SSH support in case of problems with the software.
Debugging	Opens the Debugging window.
About	Displays version and copyright information.

Settings

3.6 Settings

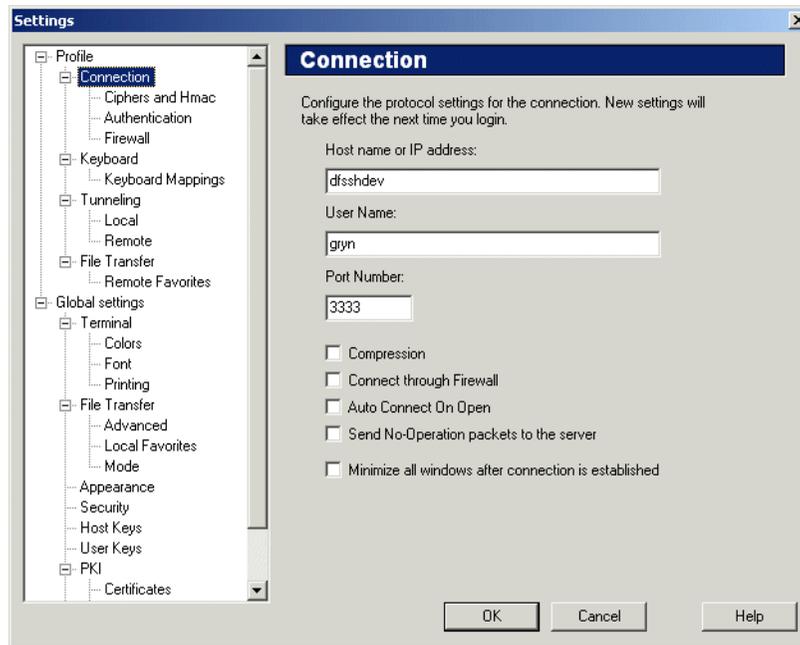
By selecting *Settings* from the *Edit* menu, or by clicking the *Settings* icon on the toolbar, you can modify the settings for the terminal display, connection information, the keyboard, secure TCP/IP connections, and other options.

Settings pane	Description
Connection	Specify information about the host, user, authentication type, firewall support, port, and ciphers used when connecting to a remote system.
Terminal	Choose the type of terminal you want to emulate, colors, fonts, keyboard and printing settings.
File Transfer	Configure the file transfer settings.
Tunneling	Specify the local and remote TCP/IP connections to be secured by forwarding them through the F-Secure SSH connection. Identify the names and connection parameters for the forwarded connections.
Appearance	Select what information is displayed in the terminal window.
Host Keys	View, import, export, and delete host keys.
User Keys	View, import, export, and delete your key pairs, upload them to a remote server, create new key pairs or change the passphrase of old ones.
Security	Remove logged data about your previous connections. Prevent unknown host keys from being accepted.

Settings

Connection Properties

Specifies options for the terminal connection and data transfer.



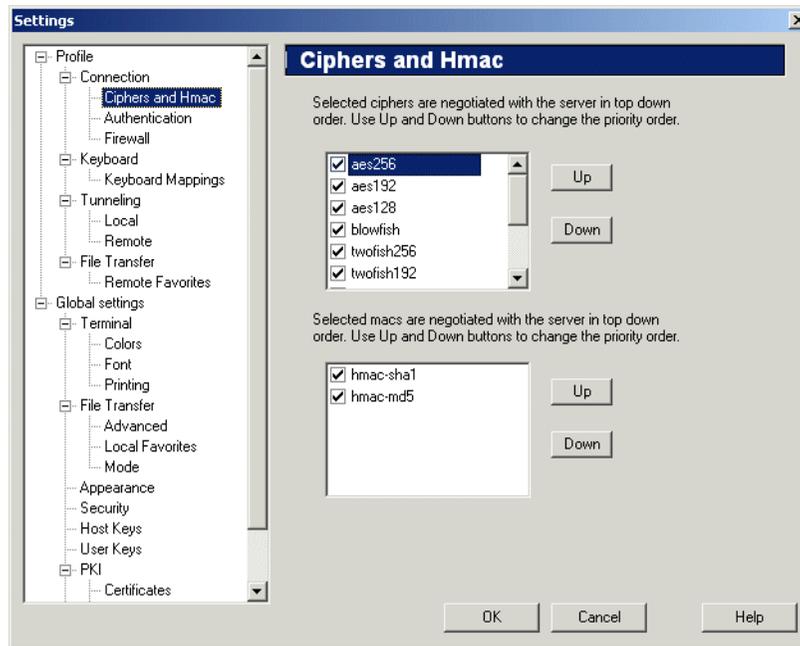
Connection option	Function
Host Name or IP address	Specifies the host name or the IP address of the remote machine to log in to.
User Name	Specifies the user name for logging in to the remote machine.
Port Number	The connection port number on the remote host. By default, the port number is 22.
Compression	When selected, all data is compressed, including data for forwarded X11 and TCP/IP connections. The compression algorithm is the same as used by the gzip program.

Settings

Connection option	Function
Connect through Firewall	Selecting this check box tells the client to connect through the firewall specified in the Firewall pane of the settings.
Auto-connect on open	Connects automatically to the host specified in a profile, when the profile is opened.
Send No-Operation Packets to the Server	Sends NOOP packets to the server at regular intervals to keep the connection alive even if there is no real traffic between the server and the client.
Minimize all windows after connection is established	Select to minimize all windows after you have established a connection.

Settings

Cipher Properties

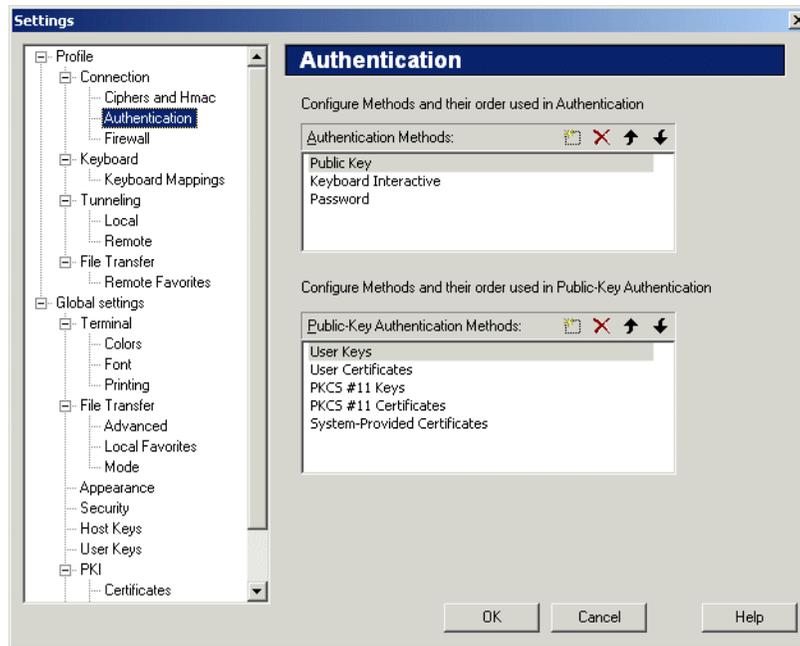


Allows you to select which ciphers to use for encrypting the session. You can move the ciphers you prefer to the top of the list. The ciphers are compared to the list of ciphers on the SSH server in the order you have listed them. The cipher that will be used is the first cipher on your list that matches a cipher available on the remote server.

From this pane, you can also select which MACs (message authentication code) to use. You can set the order of preference by moving the selected MAC up or down in the list using the **Up** and **Down** buttons.

Settings

Authentication Properties



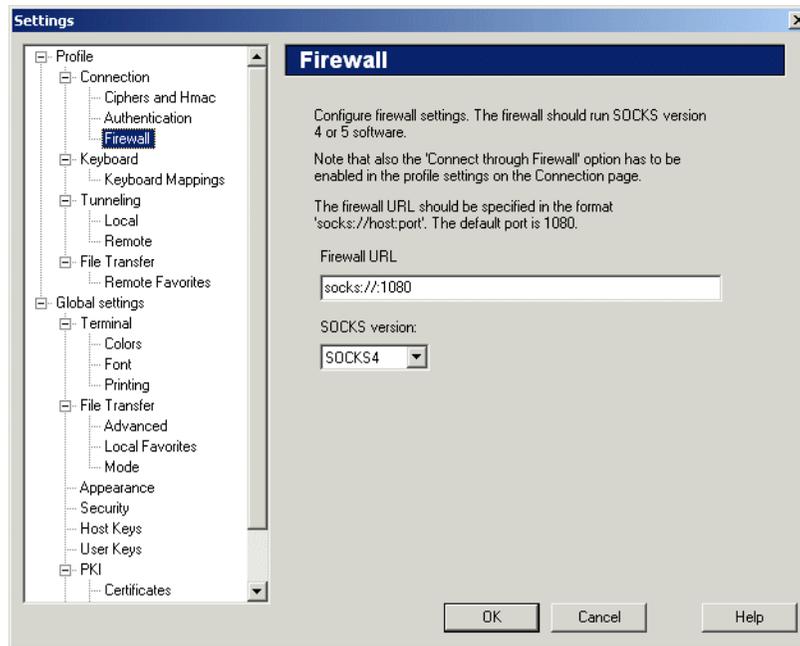
Authentication option	Function
Authentication Methods	You can specify 1-4 different authentication methods to try for a connection, and set their order of preference. Click New or press INS to add a new authentication method from a drop-down list to the available methods. Click Delete or press DEL to remove an authentication method from the list. You can select an authentication method and click on the arrows to move it up or down on the list. The preferred authentication method is the one on the top of the list.

Settings

Authentication option	Function
Public Key Authentication Methods	You can specify 1-5 different public key authentication methods to try for a connection, and set their order of preference. This list is only used if you have selected <i>Public Key</i> authentication as one of the authentication methods in the previous pane. Click New or press INS to add a new public key authentication method from a drop-down list to the available methods. Click Delete or press DEL to remove a public key authentication method from the list. You can select a public key authentication method and click on the arrows to move it up or down on the list. The preferred public key authentication method is the one on the top of the list.
Keyboard-Interactive Authentication Methods	Keyboard-Interactive is designed to allow the F-Secure SSH client to support several different types of authentication methods.

Settings

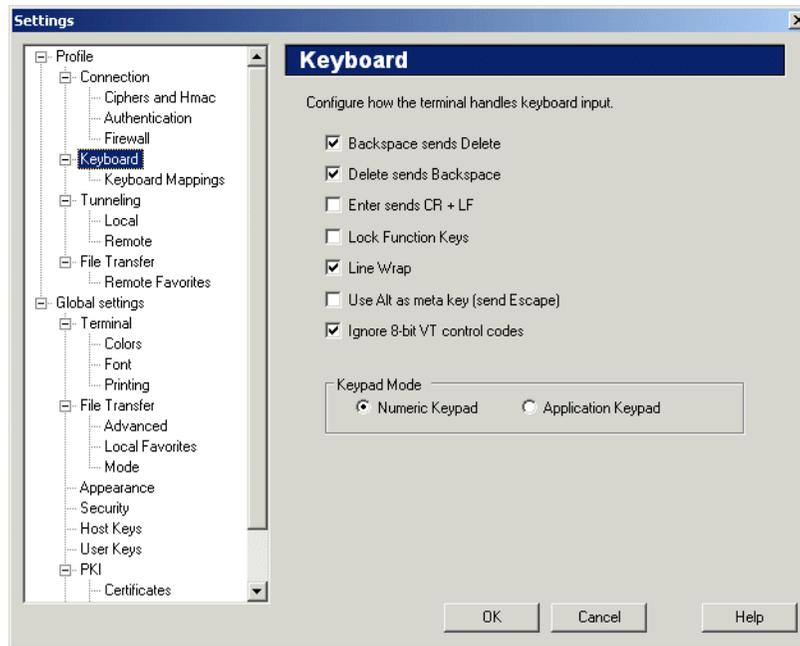
Firewall Properties



Firewall option	Function
Firewall Name	Enter the DNS or IP address of the firewall.
SOCKS version	Specifies the SOCKS version being used by the firewall.

Settings

Keyboard Properties



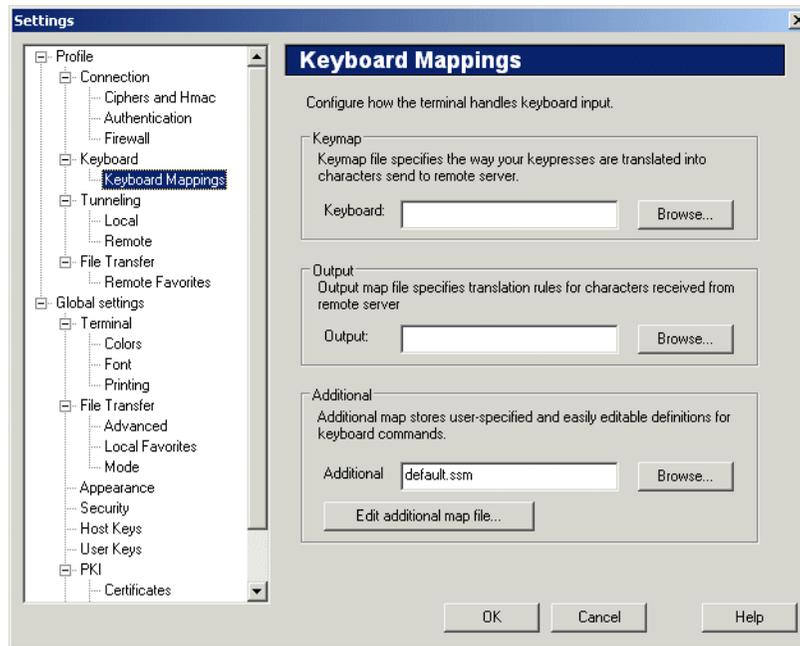
Settings

Specifies options used to translate key presses and received terminal data into characters displayed in the terminal window.

Keyboard Option	Function
Backspace Sends Delete	Causes the BACKSPACE key to send the DELETE key code.
Delete Sends Backspace	Causes the DELETE key to send the BACKSPACE key code.
Enter sends CR + LF	Enables or disables automatic insertion of line-feeds after a carriage return.
Lock Function Keys	Locks all VT100 function keys (F1 to F20) in order to prevent them from being programmed by VT100 escape codes.
Line Wrap	When selected, wraps lines that do not fit in the window. If line wrapping is not selected, the lines are simply cut at the right edge of the window.
Use Alt as meta key (Send escape)	When selected, pressing the ALT key sends the escape signal to the terminal.
Ignore 8-bit VT control codes	When selected, all 8-bit VT terminal control code sequences are ignored. Some applications require these control sequences. If you have selected this setting and encounter problems, unselect it. Note also that in order to enter the € (euro) symbol, you need to use 8-bit control codes in VT terminals, i.e. disable this setting.
Keypad Mode	You can select between the application numeric keypad mode and the VT100 numeric keypad Mode.

Settings

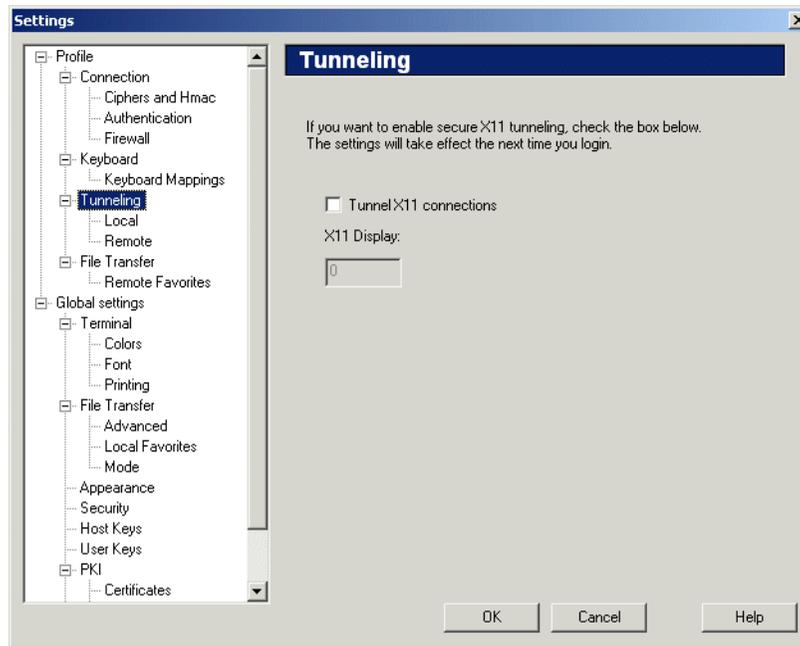
Keyboard Mappings Properties



Map Files Option	Description
Keyboard	Allows you to define your keyboard map file. To define a keymap file from a location other than the default location, click the Browse button.
Output	Allows you to define your keyboard map file for output. To define a keymap output file from a location other than the default location, click the Browse button.
Additional	Allows you to define additional keyboard shortcuts for many functions.
Edit additional map file...	Opens the keymap editor, which allows you to define additional key mappings, open saved key map files and create new key map files.

Settings

Tunneling Properties



Specifies options for the local and remote TCP/IP connections to be secured by F-Secure SSH.

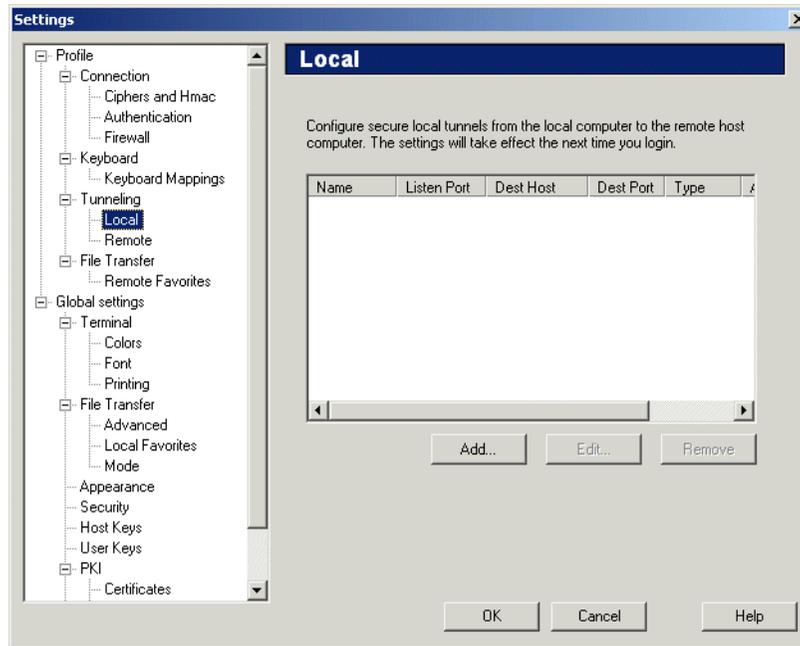
Tunneling Option	Function
Tunnel X11 connections	Enables X11 forwarding.
X11 display	Defines the X11 display number. For more information on this, consult your X11 server manual.

Local Tunneling Properties

Displays the local TCP/IP ports which have been forwarded. You can add, edit, and delete local tunnels from this tab. Tunnels can be added even while the connection is open. However, they are opened only

Settings

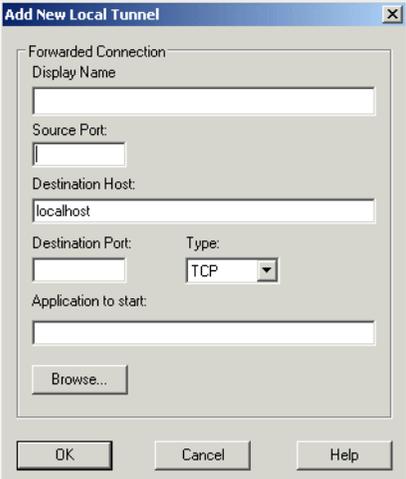
after you disconnect from the server and reconnect. But they cannot be edited or deleted while the connection is open.



Button	Function
Add	Define a new TCP/IP or FTP connection to be secured. Opens a dialog box for choosing the source port, destination host, port and protocol parameters. New tunnels will be opened as soon as you click OK .
Edit	Edit a previously defined tunnel. Opens a dialog box for choosing the source port, destination host, port and protocol parameters.
Remove	Delete the currently selected tunnel. This will only take effect after you click OK . To keep the tunnel, click Cancel .

Settings

Both **Add** and **Edit** open the following dialog box asking for information about the tunnel:



The dialog box is titled "Add New Local Tunnel" and contains the following fields and controls:

- Forwarded Connection** (grouped header)
- Display Name**: A text input field.
- Source Port**: A text input field.
- Destination Host**: A text input field containing "localhost".
- Destination Port**: A text input field.
- Type**: A dropdown menu with "TCP" selected.
- Application to start**: A text input field.
- Browse...**: A button located below the "Application to start" field.
- OK**, **Cancel**, and **Help**: Three buttons at the bottom of the dialog.

Settings

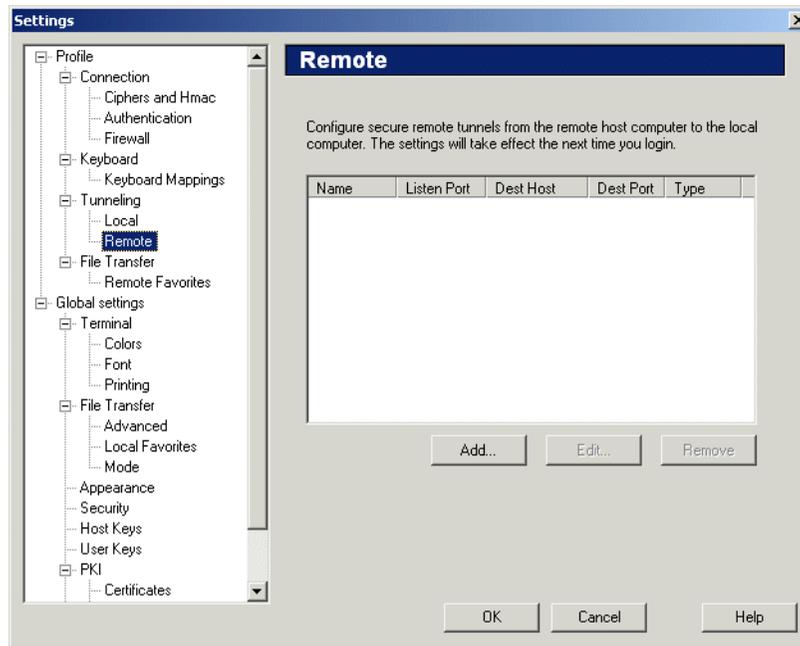
Tunnel Parameter	Description
Display Name	Enter a name for the tunnel.
Source Port	Enter the port on which your own workstation, i.e. the machine you are making the connection from, is listening for a connection.
Destination Host	Enter the DNS name or the IP address where the tunnel directs the connection from your own workstation. This address is relative to the host you are connecting to, which means that entering a host such as <i>127.0.0.1</i> or <i>localhost</i> refers to the machine to which the SSH connection is made and not the machine from which you are initiating the tunnel.
Destination Port	Enter the port on the remote machine to which the connection is forwarded.
Type	Select whether the tunnel is a TCP tunnel or an FTP tunnel. F-Secure SSH Client 5.3 supports both active and passive FTP forwarding.
Application to start	If you want a certain application to start every time you open a certain tunnel, enter the name of the application here. You can browse for the application by clicking Browse .



In F-Secure SSH version 5.1 and later, tunnels can be added on the fly. However, if you are editing or deleting tunnels, you need to restart your connection to the server for the changes to take effect.

Settings

Remote Tunneling Properties



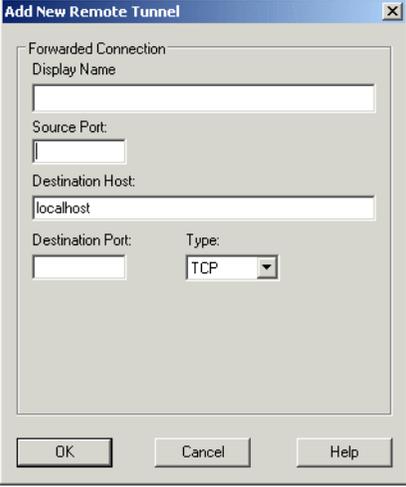
Remote Tunneling displays the remote TCP/IP ports that have been forwarded. You can add, edit, and delete remote tunnels from this tab.

Button	Function
Add	Define a new TCP/IP connection to be secured. Opens a dialog box for choosing the source port, destination host, and port parameters. New tunnels can be added even while connected.
Edit	Edit a previously defined tunnel. Opens a dialog box for choosing the source port, destination host, and port parameters.
Remove	Delete the currently selected tunnel. This will only take effect after you click OK . To keep the tunnel, click Cancel .

Settings

Click the **Add** or **Edit** button to display the *Add New Remote Tunnel* dialog box.

In this dialog box, you can specify the source and destination ports for the connection and the host to forward the connection to.



The image shows a dialog box titled "Add New Remote Tunnel" with a close button (X) in the top right corner. The dialog box contains the following fields and controls:

- Forwarded Connection** (Section Header)
- Display Name**: A text input field.
- Source Port**: A text input field.
- Destination Host**: A text input field containing the text "localhost".
- Destination Port**: A text input field.
- Type**: A dropdown menu currently set to "TCP".

At the bottom of the dialog box, there are three buttons: "OK", "Cancel", and "Help".

Settings

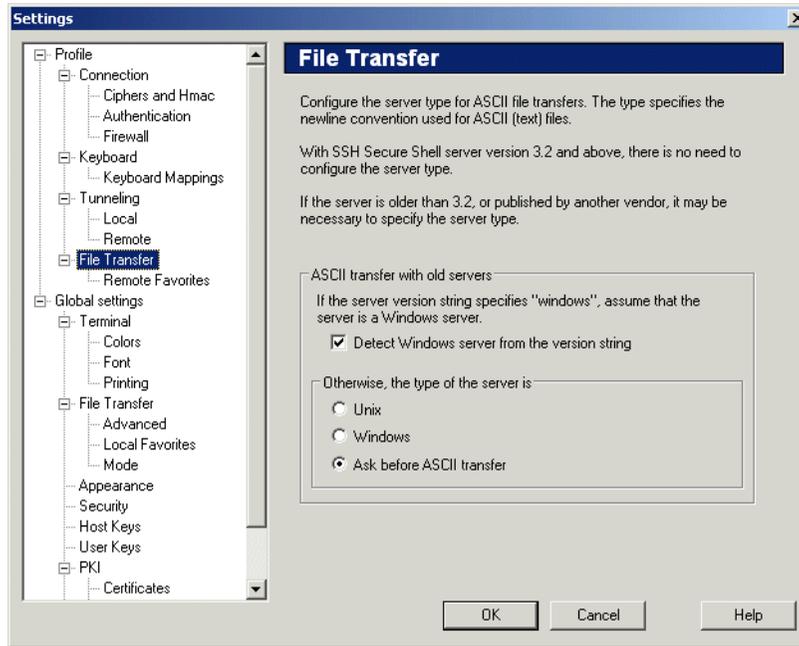
Tunnel Parameter	Description
Display Name	Enter a name for the tunnel.
Source Port	Enter the port on the remote machine to which the client listens for connections.
Destination Host	Enter the DNS name or IP address of the host to which the connection is forwarded from the remote host when a connection to the specified port is requested. This address is relative to the host you are connecting from, which means that entering a host such as <i>127.0.0.1</i> or <i>localhost</i> refers to the machine from which you are making the SSH connection and not the machine to which you are connecting.
Destination Port	Enter the port number on the destination host to which you want the connection to be forwarded.



In F-Secure SSH version 5.1 and later, tunnels can be added on the fly. However, if you are editing or deleting tunnels, you need to restart your connection to the server for the changes to take effect.

Settings

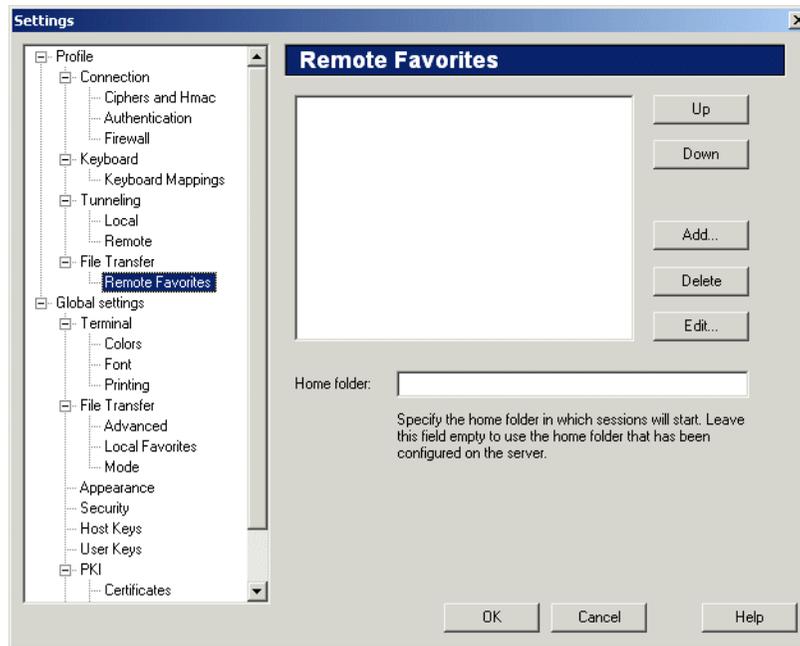
Profile-Specific File Transfer Properties



File Transfer Option	Description
Detect Windows server from the version string	Select this checkbox to automatically detect Windows servers and use the correct setting for them. For this feature to work correctly, the Windows server has to specify "windows" in its version string.
Unix	Select the Unix checkbox to use Unix-compatible line breaks.
Windows	Select the Windows checkbox to use Windows-compatible line breaks.
Ask before ASCII transfer	If you select this checkbox, the F-Secure SSH Client will ask you to specify the server type before each ASCII file transfer.

Settings

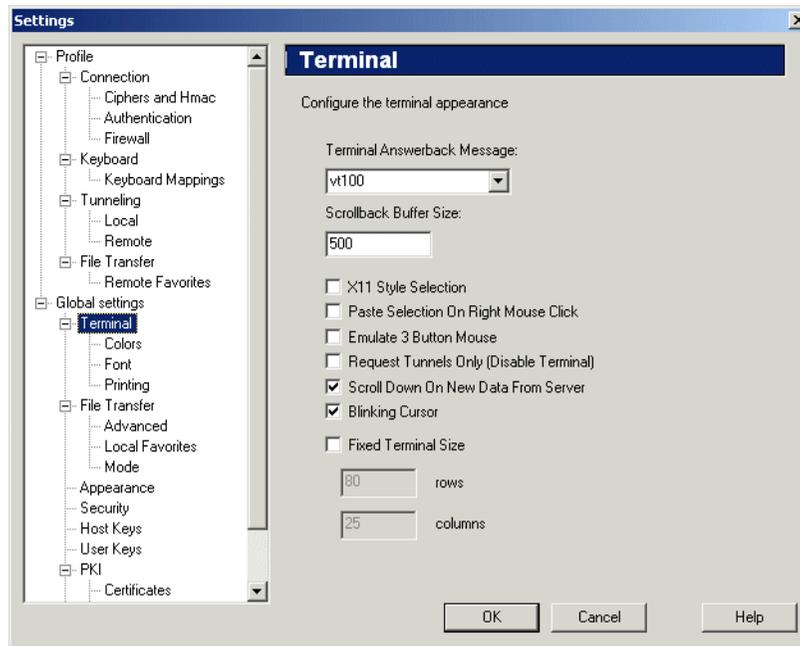
File Transfer Remote Favorites



Button	Function
Add	Click Add to add a commonly used directory to the list of favorite folders. Enter the name and path of the desired folder and click OK to effect changes.
Delete	Select a previously defined favorite from the list and click Delete to remove it. Click OK to effect changes.
Edit...	Select a previously defined favorite and click Edit to edit it's name or the path to the folder. Click OK to effect changes.
Home Folder	Specifies the folder in which the session starts. Leave the filed empty if you want to use the server-configured home folder.

Settings

Terminal Properties



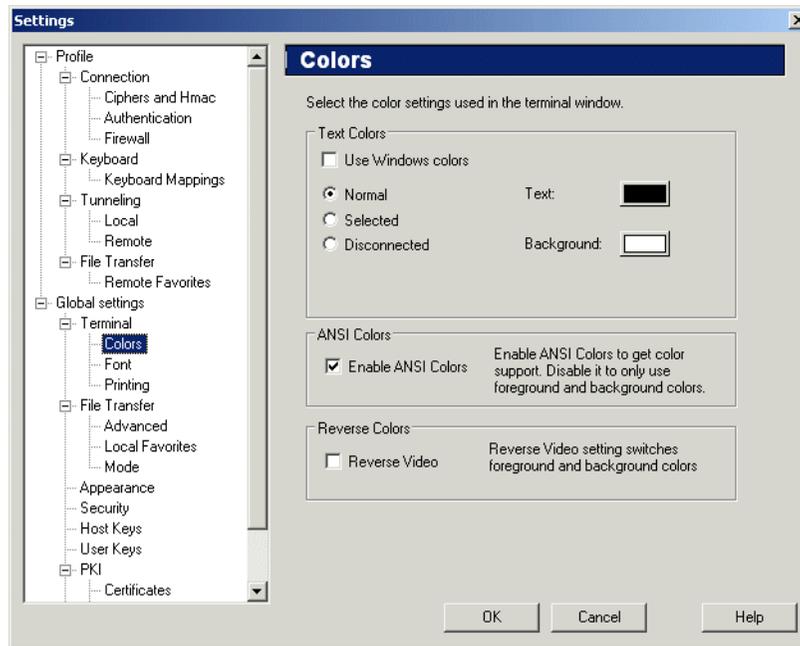
Terminal option	Function
Terminal answerback message	Enables you to choose the terminal you want to emulate. The available options are xterm, xterm-color, and vt100, 102, 220 and 320. You can select one from the list box. The vt100 emulation lets you use standard vt100 functions (such as remote printing) in an encrypted format.
Scrollback Buffer Size	You can set the terminal scrollback buffer size in lines by giving a value in the field. The valid range is between 1 and 30,000 lines.
X11 style selection	When selected, any text that you select in the terminal is copied to the clipboard automatically.

Settings

Terminal option	Function
Paste selection on right mouse click	Enables fast copying of text on the terminal display. When you have this option selected, you can copy text simply by highlighting it and then paste it by clicking the right mouse button.
Emulate 3 button mouse	With a two-button mouse, you can emulate the third button by pressing and holding the right button and clicking the left button. The third button can be used to paste a selection in the terminal window (Paste Selection).
Request Tunnels only	Disables the terminal but allows all defined tunnels to be used.
Scroll down on new data from server	If unset, and you are scrolling up, do not scroll down if the server is sending data.
Blinking cursor	Makes the cursor blink in the terminal window.
Fixed terminal size	If active, resizing the window is disabled.

Settings

Colors Properties



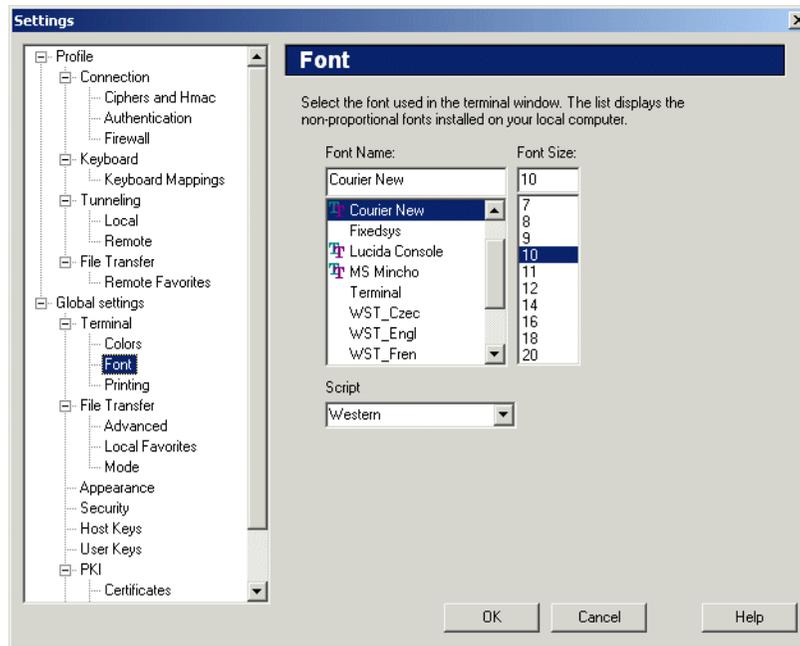
Color Options	Function
Use Windows colors	If selected, your default Windows colors will be used for the terminal connection. If not selected, you can choose colors for the background and text in four different situations:
	1. Normal — Colors displayed in the normal terminal environment.
	2. Selected — Colors for selected text.
	3. Disconnected — Colors displayed when you are disconnected but still have the terminal window open.
Text	Colors for text on the screen.

Settings

Color Options	Function
Background	Background colors.
Enable ANSI colors	Enables the use of ANSI colors in the terminal window.
Reverse Video	Reverses foreground and background colors. This is useful as background colors are normally restricted to a palette of 64 colors.

Settings

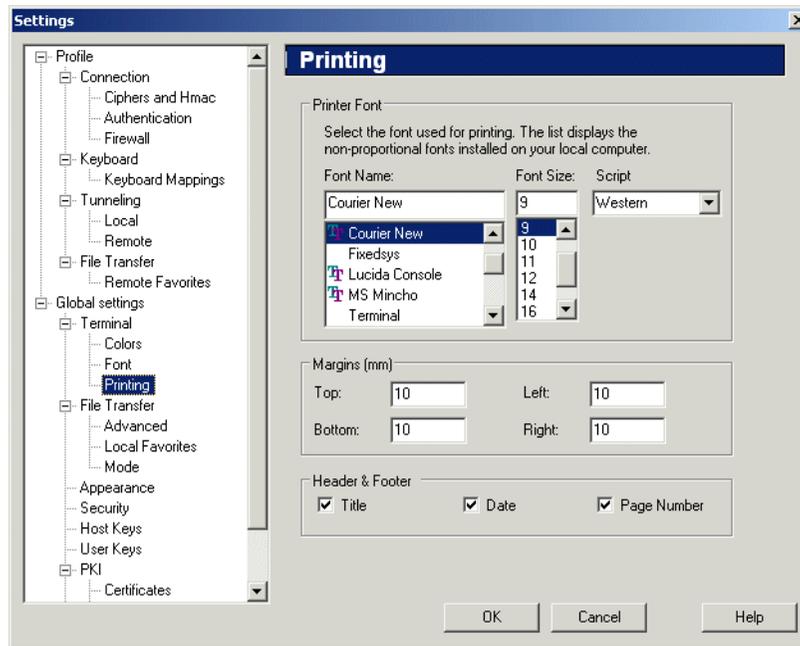
Font Properties



Font Options	Function
Name	Specifies the font to be used. The Fonts page lists currently available fonts for the terminal window.
Size	Specifies the font size.
Script	Select the character set to use from the drop-down list.

Settings

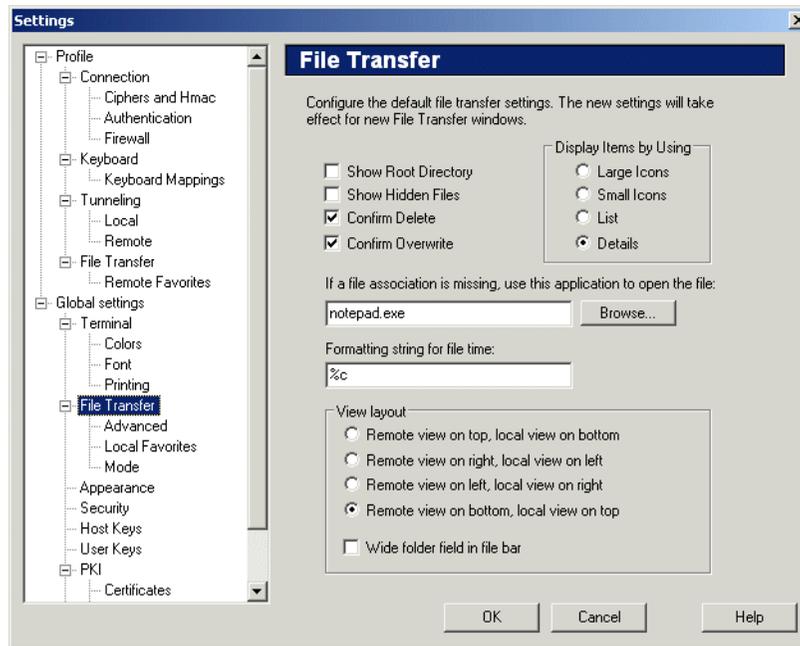
Printing Properties



Printing option	Description
Font Name	Select the font to use for printing the terminal scrollbar.
Font Size	Select the font size to use for printing.
Script	Select the character set to use from the drop-down list.
Margins	Set the margins for printing. The unit is millimeters from the edge of the paper.
Header & Footer	Select what extra data to print when printing the terminal output. <i>Title</i> prints the title of the terminal window in the header of each page of the printout. <i>Date</i> prints the current date in the header of each page of the printout. <i>Page Number</i> prints the page number in the footer of each page.

Settings

File Transfer Properties



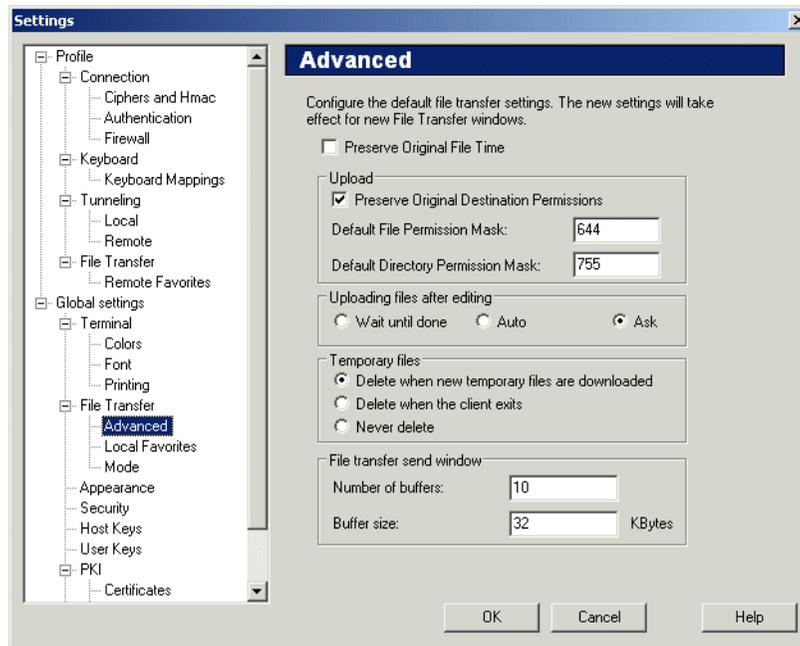
File Transfer option	Description
Show Root Directory	Show the root directory as the top directory in the directory tree. If this setting is not selected, the user's home directory is shown as the top directory in the tree.
Show Hidden Files	Display hidden files. If not selected, hidden files are not shown.
Confirm Delete	If selected, asks the user for confirmation before deleting files.
Confirm Overwrite	If selected, asks the user for confirmation before overwriting files.
Display Items by Using	You can select to display files in any of the standard ways that Windows Explorer™ shows files.

Settings

File Transfer option	Description
Missing association	Select an application to use for viewing files that are not associated with any program.
Formatting string for file time	Enter the formatting string used for giving the current file stamp to the program.
View layout	You can select how the File Transfer window positions the local and remote view panes.

Settings

File Transfer Advanced Properties



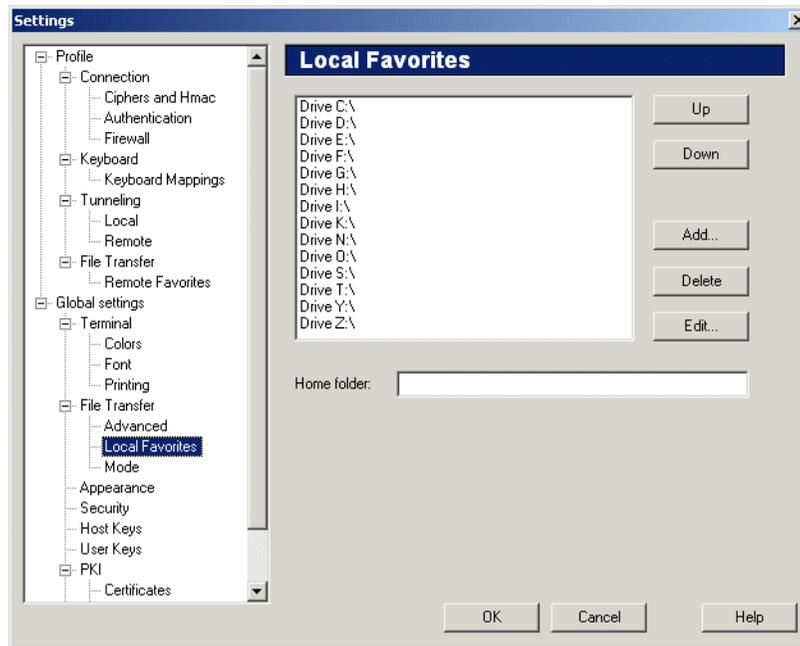
File Transfer option	Description
Preserve Original File Time	If selected, does not change the file time stamp to the current time when the file is transferred to the new host but keeps the old time stamp.
Preserve Original Destination Permissions	If selected, preserve the original file permissions located on the remote host computer. The transferred file uses the same file permissions as the original file.
Default File Permission Mask	The octal UNIX file permission mask (same as the UNIX chmod command) which is used as the default value for uploaded files.
Default Directory Permission Mask	The octal UNIX directory permission mask (same as the UNIX chmod command) which is used as the default value for uploaded directories.

Settings

File Transfer option	Description
Uploading Files After Editing	
Wait until done	When you edit a file remotely and this setting is selected, the file is uploaded back to the remote server as soon as you save your changes and close the editor. While you are editing the file, the SFTP client is on hold and cannot be used in any way.
Auto	When you edit a file remotely and this setting is selected, the file is uploaded back to the remote server as soon as you save your changes and close the editor. While you are editing the file, the SFTP client is still fully operational.
Ask	When you edit a file remotely and this setting is selected, you are prompted to upload the file back to the remote server as soon as you save your changes and close the editor
Temporary files	
Delete when new temporary files are downloaded	When you download a file for editing, it is saved locally as a temporary file. If this setting is selected, there is always only one temporary file saved locally, i.e. any file you download for editing replaces and thus deletes the previously opened temporary file.
Delete when the client exits	If this setting is selected, temporary files are saved locally and deleted when you close the client.
Never delete	If this setting is selected, temporary files are never deleted automatically from the local system.
File transfer send window	
Number of buffers	Enter the number of buffers used in file transfer. The default value is 10.
Buffer size	Enter the default buffer size (measured in kilobytes). The default value is 32 kilobytes.

Settings

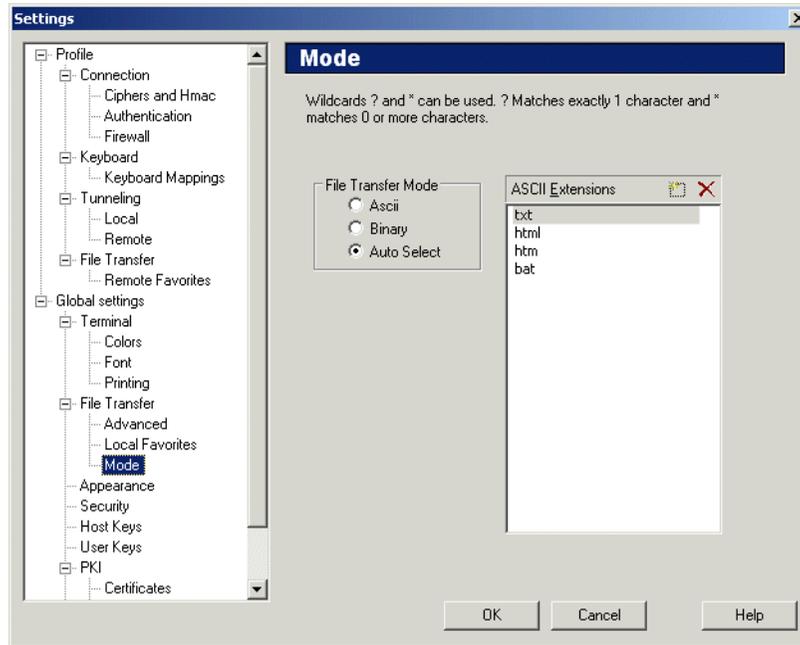
File Transfer Local Favorites



Button	Function
Add	Click Add to add a commonly used directory to the list of favorite folders. Enter the name and path of the desired folder and click OK to effect changes.
Delete	Select a previously defined favorite from the list and click Delete to remove it. Click OK to effect changes.
Edit...	Select a previously defined favorite and click Edit to edit it's name or the path to the folder. Click OK to effect changes.
Home folder	Enter the location of the home folder that is initially displayed in the local view pane of the File Transfer window.

Settings

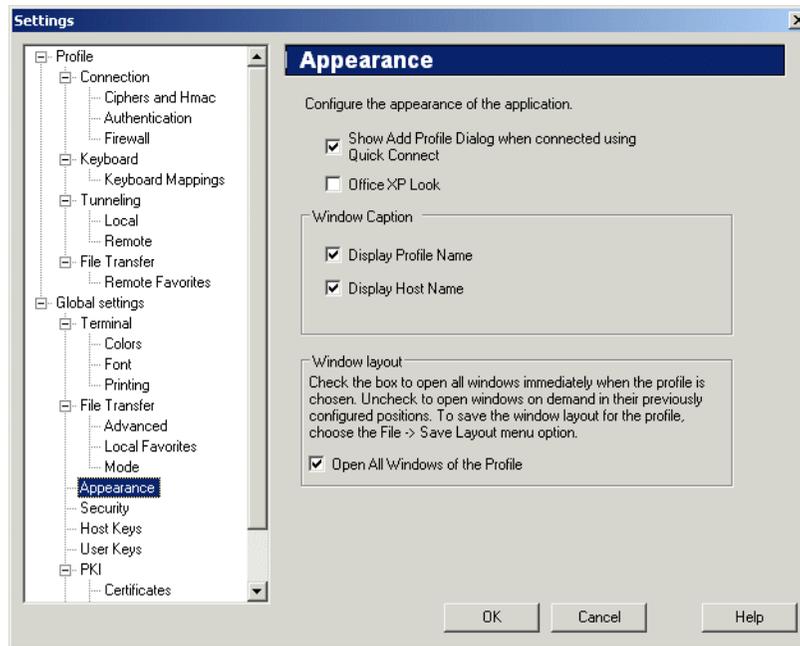
File Transfer Mode Properties



File Transfer Mode	Description
ASCII	By default, all files are transferred in ASCII mode.
Binary	By default, all files are transferred in binary mode.
Auto Select	By default, the files are transferred based on their extension. Specify file extensions to the ASCII Extensions list that should be transferred in ASCII mode. All other files are transferred in binary mode.
ASCII Extensions	List all the file extensions you wish to automatically be considered ASCII files and transferred in ASCII mode.

Settings

Appearance Properties



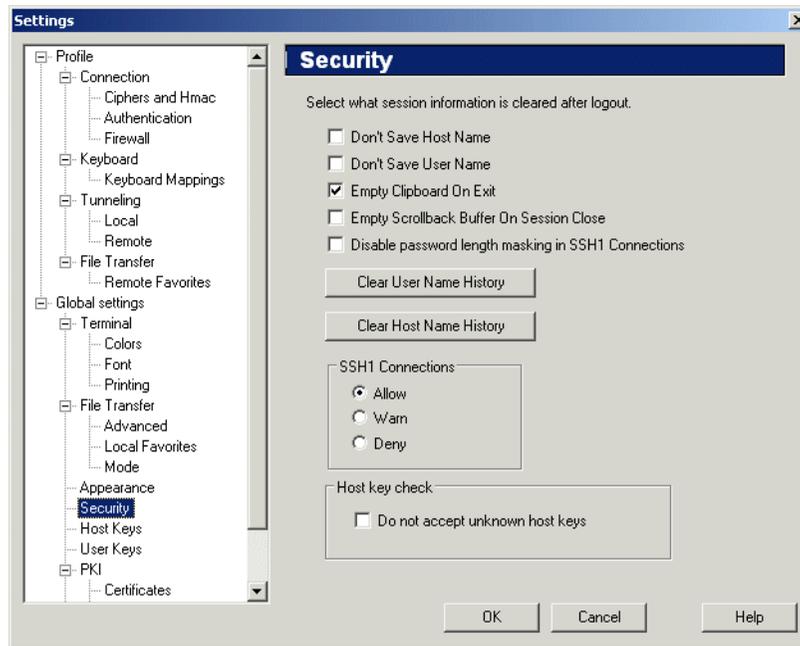
Appearance Options	Function
Show Add Profile Dialog when connected using Quick Connect	Briefly displays the Add Profile dialog when you connect to a new host using Quick Connect. You can easily add the new host to a new profile.
Office XP Look	Changes the appearance of the client to resemble Office XP applications.
Display Profile Name	When selected, the name of the current profile is shown in the title bar.
Display Host Name	When Selected, the name of the host to which you are connected is shown in the title bar.

Settings

Appearance Options	Function
Window Layout	If you have created a connection profile with several windows open at the same time and saved the layout, all of the windows associated with the profile are normally opened when you select the profile. With the Window Layout option you can override this behavior.

Settings

Security Properties



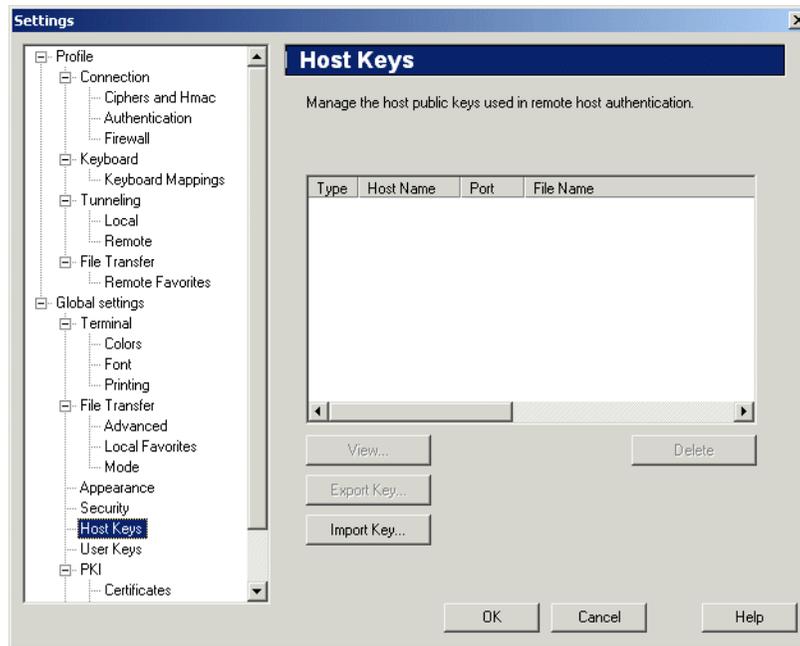
Option	Function
Don't Save Host Name	Do not save the host names on the drop-down list of the Quick Connect for future sessions.
Don't Save User Name	Do not save the user names on the drop-down list of the Quick Connect for future sessions.
Empty Clipboard On Exit	Remove all data from the clipboard when you exit from F-Secure SSH Client.
Empty Scrollback Buffer On Session Close	Remove all data from the scrollback buffer when you disconnect from a server.

Settings

Option	Function
Disable password length masking in SSH1 connections	By default, F-Secure SSH Client 5.3 for Windows masks the password length in SSH1 connections by sending a random number of SSH IGNORE strings to the server before the password. Some operating systems cannot accept this. If you experience problems with password length masking, disable it.
Clear User name history	Delete recent user name entries from the Logon Information dialog box.
Clear Host name history	Delete recent host name entries from the Logon Information dialog box.
SSH1 Connection	Select what to do when the client tries to connect to an SSH1 server. You can either Allow, Deny or Warn about SSH1 connections.
Do not accept unknown host keys	Allows connecting only to hosts whose host keys you have received.

Settings

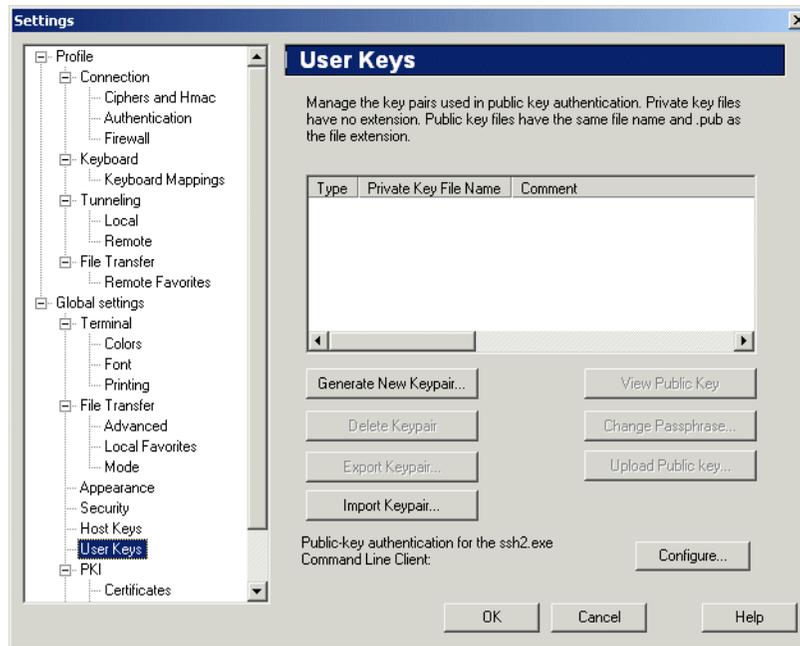
Host Keys Properties



Button	Function
View	View the selected host key. You can copy the host key to the clipboard from the view window.
Export Key	Export the selected key from the system registry to a host key file.
Import Key	Import a public host key file to the system registry.
Delete	Delete the selected host key from the system registry.

Settings

User Keys Properties



When you copy an RSA key to the clipboard, you will be prompted for the format of the key. If you want to use the key with an ssh2 server, select ssh2. If you want to use the key with an ssh1 server, select ssh1.

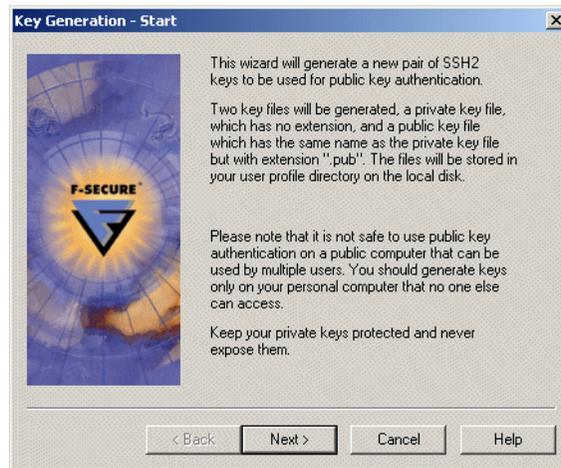
Button	Function
Generate New Keypair	Generate a new public and private key. See below this table.
Delete Keypair	Delete the selected user key pair from the system registry.
Export Keypair	Export the selected user key pair from the system registry to files.
Import Keypair	Import a keypair from a hard drive or diskette
View Public Key	View the selected public key in a window
Change Passphrase	Change the passphrase for the highlighted key.

Settings

Button	Function
Upload Public Key	Upload the public key to the remote host. See next page.

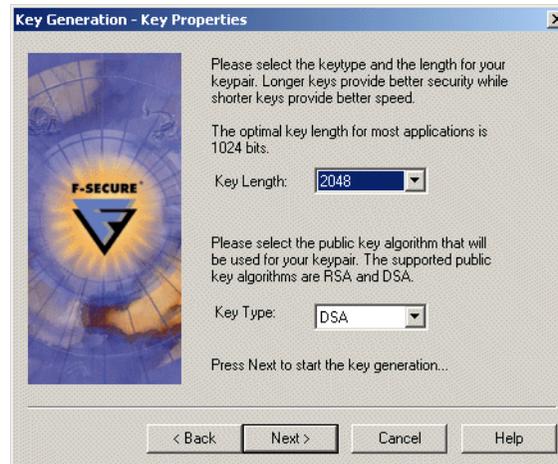
Generating a New Keypair

You can start the key generator from the User Keys pane of the Settings dialog box.

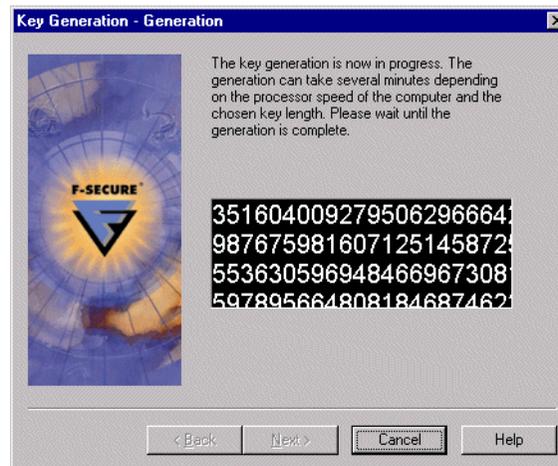


Settings

After the introduction screen, you need to select the key length and the public key algorithm to use. The available algorithms are RSA and DSA.



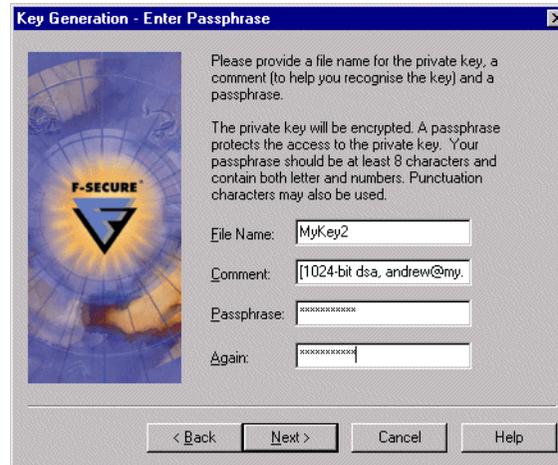
Click **Next** to start the key generation. During the generation, you will see a window with numbers rotating randomly. When the generation is complete, the numbers stop and you can click **Next**.



Next, enter a file name for the private key and a comment to help you recognize the key later. Enter a good passphrase for the key. A good passphrase is at least 8 characters long, and contain letters, numbers and non-alphabetic characters. Re-enter the passphrase to make sure you entered it correctly the first time.

Settings

The **Next** button will activate only when the two passphrases match. Leaving the passphrase empty is a security risk. If you do that, the program will warn you before letting you move on.



Key Generation - Enter Passphrase

Please provide a file name for the private key, a comment (to help you recognise the key) and a passphrase.

The private key will be encrypted. A passphrase protects the access to the private key. Your passphrase should be at least 8 characters and contain both letter and numbers. Punctuation characters may also be used.

File Name:

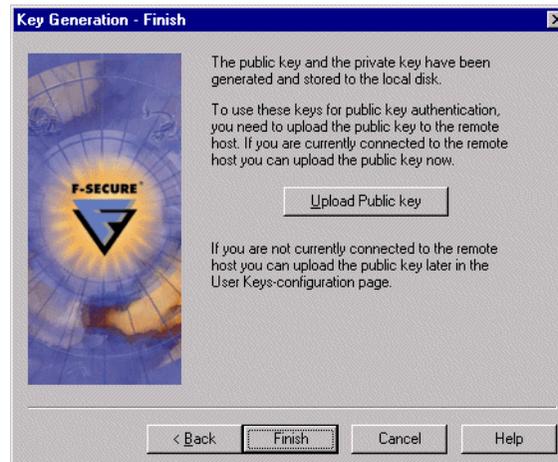
Comment:

Passphrase:

Again:

< Back Next > Cancel Help

Next, you can either click **Finish** to return to the User Keys pane of the settings, or you can upload the newly created public key to the remote host by clicking the **Upload Public Key** button. You need to be connected to the host already to be able to upload the key.



Key Generation - Finish

The public key and the private key have been generated and stored to the local disk.

To use these keys for public key authentication, you need to upload the public key to the remote host. If you are currently connected to the remote host you can upload the public key now.

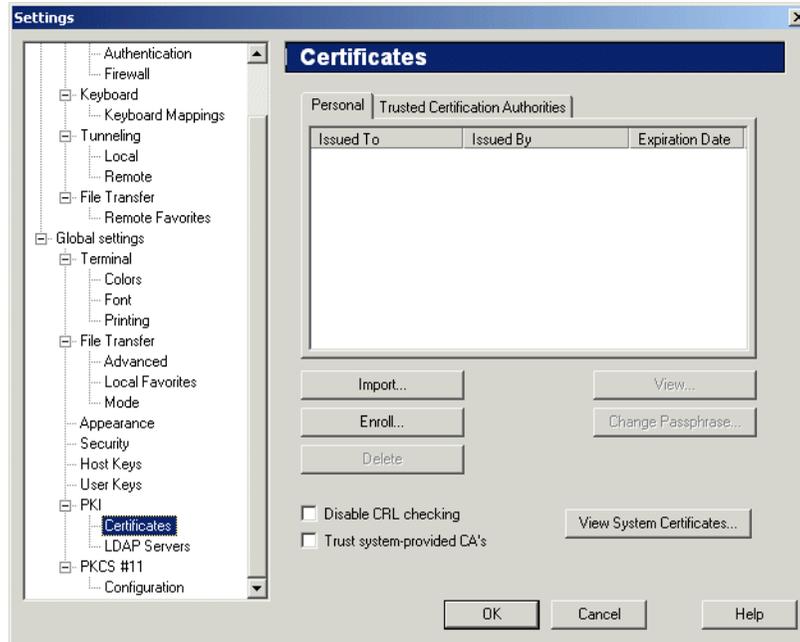
If you are not currently connected to the remote host you can upload the public key later in the User Keys-configuration page.

< Back Finish Cancel Help

Settings

PKI Certificate Properties

Public Key Infrastructure (PKI) is a system that uses digital certificates to increase the reliability of authentication. Before you can use the certificate authentication, certificates have to be created with a Certificate Authority (CA) software.



Button	Function
Import	Import a certificate created with Certificate Authority (CA) software. You can browse for the saved certificate file.
Enroll	Start the Certificate Enrollment wizard, which is used to request a Certificate Authority (CA) to issue a certificate. F-Secure SSH supports the CMP2 enrollment protocol.
Delete	Remove the selected certificate.

Settings

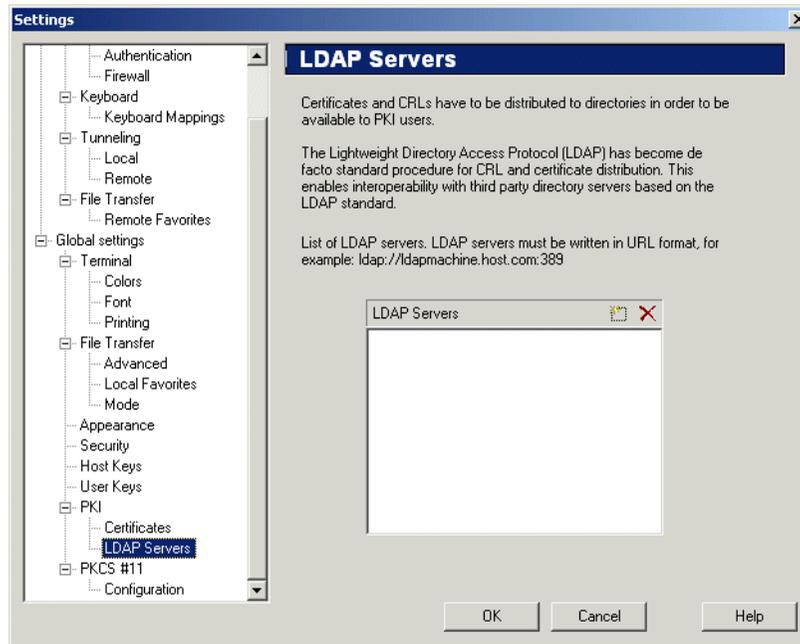
Button	Function
View	Display the contents of the selected certificate.
Change Passphrase	Change the passphrase associated with the selected certificate.
Disable CRL Checking	Prevent the use of the Certificate Revocation List (CRL). The CRL is used to check whether any of the used certificates have been revoked.
View System Certificates	Opens Windows certificate storage for viewing.

Settings

PKI LDAP Server Properties

Certificates and CRLs have to be distributed to directories so that PKI users can use them.

The Lightweight Directory Access Protocol (LDAP) has become de facto standard to distribute certificates and CRLs. Using the LDAP enables interoperability with third party directory servers, which are based on the LDAP standard.



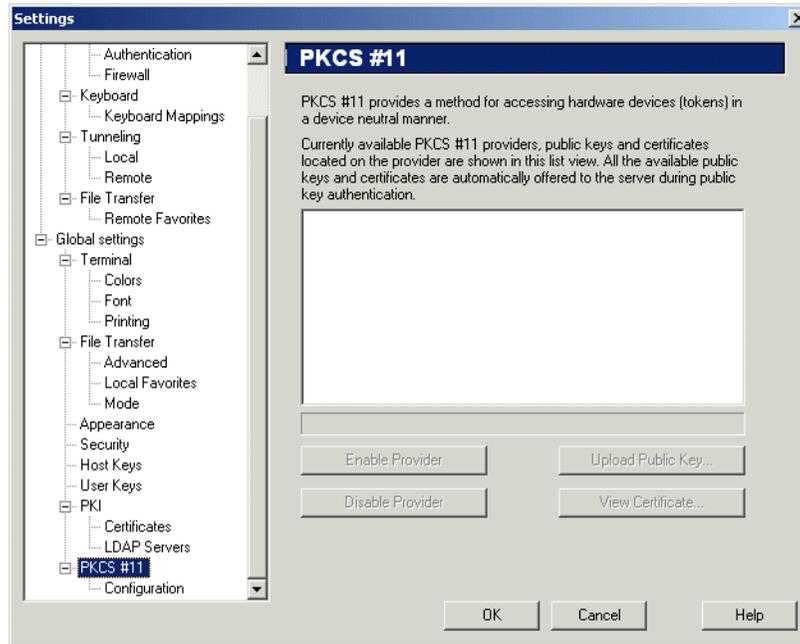
LDAP Servers list shows the list of used LDAP servers. Click the New button or press Ins to add a new LDAP server to the list. LDAP servers must be written in URL format. Click the **Delete** button or press DEL to remove the selected LDAP server from the list.

PKCS #11 Properties

PKCS #11 provides a hardware device (token) access method. PKCS #11 is a runtime interface to hardware tokens and software keys. You need a third party driver to be able to use a hardware token, such as a smart card or a USB token. Install the software included with the hardware token before you configure it in F-Secure SSH.

Settings

The PKCS #11 list shows the currently available providers, public keys and certificates located on the provider. All the available public keys and certificates are automatically used during the public key authentication.



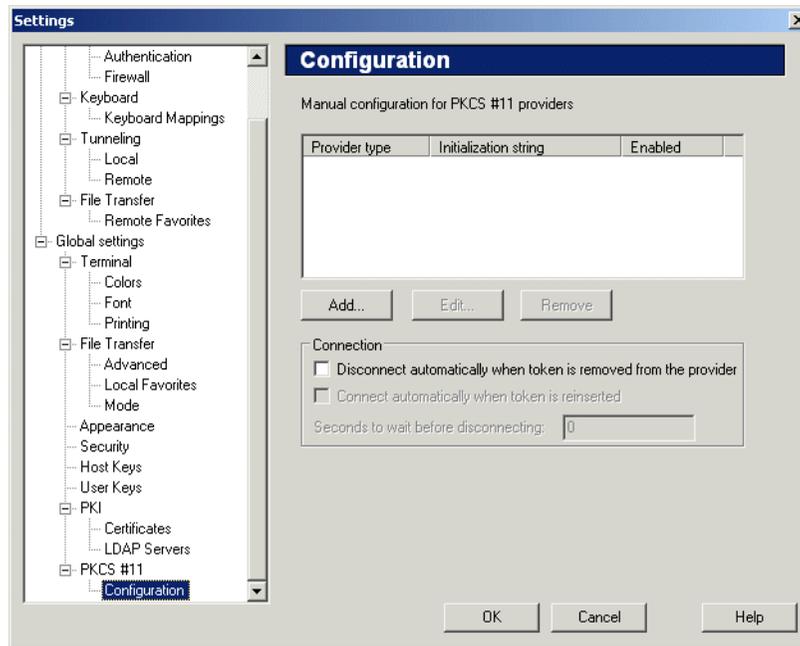
Button	Description
Enable Provider	Allow the use of the selected provider.
Disable Provider	Deny the use of the selected provider.
Upload Public Key	Upload the public key from the token to the server. You can then use the hardware token for your personal authentication. You have to be connected to a server to upload the public key.
View Certificate	Display the contents of the selected certificate.



The list does not update automatically. It is updated when you close and open the list again.

Settings

PKCS #11 Configuration Properties



Button	Description
Add	Add a new PKCS #11 provider.
Edit	Change the details of the PKCS #11 provider
Remove	Delete the PKCS #11 provider entry.

Check the *Disconnect automatically when token is removed from the provider* check box to keep the connection active only when the token is present. Set the time after which the connection is disconnected when a token is removed in *Seconds to wait before disconnecting* field. Check the *Connect automatically when token is reinserted* check box to automatically establish the connection again when the token is reinserted.

3.7 Using the Command Line Applications (ssh2, scp2, sftp2)

F-Secure SSH comes with three applications that can be used from the Windows command line:

- ssh2—An application for logging on to a remote machine and executing commands.
- scp2—An application for copying files between hosts on a network.
- sftp2—An application for starting a secure file transfer session between two hosts.

Using ssh2

ssh2 is used for starting a secure terminal connection to a remote host, executing commands on a remote host, and creating tunnels for the secure transfer of TCP packets and X11 connections. This utility can be used as a secure substitute for rlogin, rsh, and telnet. It provides secure, encrypted communications between two hosts over an unsecure network.

ssh2 connects and logs in to the specified hostname. A user must prove his identity to the remote machine by using one of the following authentication methods.

- password authentication
- public-key authentication

Use the following format for starting an ssh2 session from the UNIX command prompt:

```
ssh2 [options] host [command]
```

All options start with “-“.

If your user name on the remote host is the same as on the host you are connecting from, you only need to give ssh2 the host name. ssh2 logs you in with your default user name and just asks you for your password on the remote host.

Using the Command Line Applications (ssh2, scp2, sftp2)

Example:

```
my.company.com% ssh2 second.host.com
andrew's password:
Last login: Wed Jun 16 08:48:59 1999
second.host.com%

my.company.com% ssh joseph@third.host.com
Executing /usr/local/bin/ssh1 for ssh1 compatibility.
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Host 'third.host.com' added to the list of known hosts.
Creating random seed file ~/.ssh/random_seed. This may take a while.
joseph@third.host.com's password:
Last login: Wed Jun 16 10:22:07 1999 from my.company.com
Linux 2.0.35.
third.host.com:~$
```

If you have a different user name on the remote host, you need to include the user name in the command line when making a connection. You can either do this with the “-l” option or by using the format `username@remote.host`.

Example:

```
my.company.com% ssh -l joseph third.host.com
joseph's password:
Last login: Wed Jun 16 10:22:07 1999 from my.company.com
Linux 2.0.35.
third.host.com:~$
```

ssh2 obtains configuration data from the following sources, in this order:

1. System's global configuration file (typically `/etc/ssh2/ssh2_config`).
2. User's configuration file (`$HOME/.ssh2/ssh2_config`).
3. Command line options.

For each parameter, the last obtained value will be in effect.

Using the Command Line Applications (ssh2, scp2, sftp2)

Command Line Options

-l login_name	Specifies the user for login to the remote machine.
-n	Redirects input from /dev/null. (Do not read stdin.) This option can also be specified in the configuration file.
+x	Enables X11 connection forwarding. (Default)
-x	Disables X11 connection forwarding.
-F file	Specifies an alternative configuration file to use. Specified options are in addition to those read in the \$HOME/.ssh2/ssh2_config file.
-t	Allocates a tty, even if a command is given. This option can also be specified in the configuration file.
-v	Enables verbose mode. Verbose debugging messages are displayed. Same as '-d 2'. This option can also be specified in the configuration file.
-d debug_level	In this version, only debug level 2 can be defined. Displays verbose debugging messages.
-V	Displays version string.
-q	'Quiet' mode. No warning messages will be displayed. This option can also be specified in the configuration file.
-e char	Set escape character. Use 'none' to disable. This option can also be specified in the configuration file. (Default; ~)
-c cipher	Select encryption algorithm. Multiple -c options are allowed, and a single -c flag can have only one cipher. This option can also be specified in the configuration file.
-p port	Specifies the port to connect to on the remote host. This option can be specified in the configuration file.

Using the Command Line Applications (ssh2, scp2, sftp2)

- P Do not use privileged source port. Prevents the use of rhosts or rsarhosts authentications, but it can be used to bypass some firewalls that do not allow privileged source ports to pass. This option can also be specified in the configuration file. (Not yet implemented.)
- S Do not request a session channel. This can be used with port forwarding requests if a session channel (and tty) is not needed or provided by the server.
- L port:host:hostport Specifies that the given port on the local (client) host is to be forwarded to the given host and port on the remote side. This works by allocating a socket to listen to on the local side. Whenever a connection is made to this port, the connection is forwarded over the secure channel and a connection is made to host:hostport from the remote machine. Port-forwardings can also be specified in the configuration file. Only root can forward privileged ports.
- R port:host:hostport Specifies that the given port on the remote (server) host is to be forwarded to the given host and port on the local side. This works by allocating a socket to listen to on the remote side. Whenever a connection is made to this port, the connection is forwarded over the secure channel, and a connection is made to host:hostport from the local machine. Privileged ports can be forwarded only when logging in as root on the remote machine.
- +C Enables compression.
- C Disables compression. (Default)
- o 'option' Can be used to give options in the format used in the configuration files. This is useful for specifying options for which there is no separate command-line flag. The option has the same format as a line in the configuration file. Comment lines are not currently accepted by this option.
- h Displays brief help about command-line options.

Using the Command Line Applications (ssh2, scp2, sftp2)

Using scp2

scp2 (Secure Copy) is used to copy files over the network securely. It uses the ssh2 protocol for data transfer. It uses the same authentication and provides the same security as ssh2. Unlike rcp, scp2 will ask for passwords or passphrases if they are needed for authentication.

Any filename may contain a host, user, and port specification to indicate that the file is to be copied to or from that host. Copies between two remote hosts are permitted.

Use the following format for copying files with scp2:

```
scp2 [options] [[username@]host[#port]:]file [[username@]host[#port]:]file_or_dir
```

For example, to copy the file *program.exe* from your local hard drive to *second.host.com*, where your user name is andrews, you would enter:

```
scp2 program.exe andrews@second.host.com:program.exe
```

All options start with "-". The first filename is the source file and the second is the destination file. The source filename can include wildcards. For example:

```
scp2 prog* andrews@second.host.com:.
```

copies all files starting with "prog" from your currently selected local directory to your home directory on *second.host.com*.

```
scp2 program?.exe andrews@second.host.com:.\program
```

copies files whose name contains any one character in the exact place where the question mark is, such as *program1.exe* or *programa.exe*, to the *program* directory under your home directory on *second.host.com*.

When you are copying multiple files using wildcards, you can only specify a path in the destination filename. Scp2 does not create directories for you; if you define a directory as the destination, you need to have created it beforehand.

The host name needs to be given only if the host is a remote host. The user name is required only if it is different from the local user name. The port number is required only if it is not port 22, the standard ssh2 port.

Using the Command Line Applications (ssh2, scp2, sftp2)

Command Line Options

-D debug_level_spec	Prints extensive debug information to stderr. debug_level_spec is a number, from 0 to 99, where 99 specifies that all debug information should be displayed.
-d	With this option, scp2 will make sure that the destination file is a directory. If not, scp2 will exit with an error message.
-q	Quiet mode. Does not show the progress indicator while transferring files.
-Q	Does not show the progress indicator during file transfer.
-p	Tells scp2 to preserve file attributes and timestamps.
-u	Removes the source files after copying.
-r	Copies files and directories recursively when using wildcards.
-v	Makes scp2 verbose. Equal to the '-D2' option.
-V	Displays version information.
-c cipher	Selects the encryption algorithm that ssh2 will use. Multiple -c options are allowed, and a single -c flag can have only one cipher.
-C	Sets compression on. When not specifically defined, compression is turned off.
-P ssh2-port	Specifies the remote port to ssh2. Ports can also be defined individually for each file using the format hostname#port:filename.
-f firewall-name	If you are connecting through a firewall, you can use this parameter to specify the address of the firewall.
-F firewall-port	When connecting through a firewall, you can use this parameter to specify the port number the firewall uses.
-k directory	Stores host keys to and reads user keys from this directory instead of the default directory.

Using the Command Line Applications (ssh2, scp2, sftp2)

-V	Displays version information.
-h	Displays a brief help.

Using sftp2

sftp (Secure File Transfer) is an ftp-like client that can be used in file transfer over the network. sftp uses Ssh2 in data connections, so the file transport is secure.

Use the following format to start an sftp2 session from the UNIX command prompt:

```
sftp [options] [[user]host[#port]]
```

All options start with “-“

Command Line Options

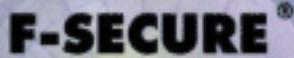
-d debug_level_spec	Debug mode. Makes sftp send verbose debug output to stderr. The debugging level is either a number (0 to 99), or a comma-separated list of assignments. "ModulePattern=debug_level".
-b filename	You can create a file that contains all the commands you want to perform in a session. Using the <code>-b filename</code> option you can then automate this list of commands. For example, by entering the following commands in the text file you can automatically open a connection, download the <i>latest.zip</i> file and close the connection: <pre>open <u>andrews@my.company.com</u> get latest.zip close</pre>
-V	Show the version number of the software.

After initiating the sftp session, you can execute the following commands:

cd	Changes the directory on the remote server.
close	Closes the connection, but does not quit sftp2.
get file1 [file2] [...]	Downloads the specified files to the currently active local directory.

Using the Command Line Applications (ssh2, scp2, sftp2)

help	By itself, 'help' prints the list of the available commands on the screen. 'help' followed by a command on the list gives a short description of the command.
lcd	Changes the local directory.
lls [local_dir] [local_file]	Lists the contents of the current local directory in short format.
mkdir	Create a directory in the local computer.
lpwd	Shows the current working directory on the local machine.
lrename filename newfilename	Renames a file in the local directory.
lrm [local_file]	Deletes the specified local file. This command does not accept wildcards.
lrmkdir dirname	Removes a local directory.
ls	Lists the contents of the current remote directory in short format.
mget	Identical to 'get'.
mkdir	Creates a new directory on the remote host.
mput	Identical to 'put'.
open <[user@]hostname[#port]>	Opens a connection to the specified host, using the specified user name and port number.
put file1 [file2] [...]	Uploads a local file to the remote host.
pwd	Shows the current working directory on the remote machine.
quit	Closes the connection and quits sftp2.
rename filename newfilename	Renames a file on the remote host.
rm remote_file	Removes a file from the remote host.
rmdir	Removes a directory from the remote host. This will only work on empty directories.

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 geometric shapes in shades of purple and black, creating a layered, triangular appearance.

Technical Support

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

Web Club

The F-Secure SSH Web Club provides assistance to F-Secure SSH users. To connect to the Web Club on our Web site, select *Web Club* from the *Help* menu.

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

<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 online services at <http://www.f-secure.com/>, you can contact your local F-Secure distributor or F-Secure Corporation directly.

For basic technical assistance, please contact your F-Secure distributor.

Electronic Mail Support

If there is no authorized F-Secure Business Partner in your country, you can request technical assistance from:

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

Please include the following information 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 which could 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 F-Secure folder in the Windows Start > Programs menu. The README file contains the latest information.



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.

If you want to give feedback about the document itself, send e-mail to documentation@f-secure.com.