F-Secure SSH

for Windows

User’s Guide

 #12000006-3E20

Table of Contents

1. Welcome

1.1 About F-Secure SSH Client for Windows

F-Secure SSH Client closes the security holes in file transfer and remote login connections. With F-Secure SSH Client, you can safely connect and manage your Unix or Windows hosts while keeping all your passwords and transferred data secure from outsiders.

F-Secure SSH Client 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.

F-Secure SSH Client 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 Client 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.

F-Secure SSH Client contains components certified by National Institute of Standards and Technology (NIST).

1.2 Features

F-Secure SSH Client for Windows, as well as all other F-Secure SSH Client products, provides the following features and capabilities.

Secure Connections

F-Secure SSH Client provides users with secure login connections over untrusted networks. It 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.

Secure Authentication

F-Secure SSH Client guarantees authentication of both ends of the connection, and it guarantees the secrecy and integrity of transmitted data.

The SSH server can authenticate the user in a number of ways. If you want to use the password authentication method, the password is transmitted over the encrypted channel and cannot be seen by outsiders.

Secure File Transfers

F-Secure SSH Client provides a secure method for transferring files. When you transfer files using F-Secure SSH Client, you can be sure that no one is eavesdropping or altering the content. All types of files can be transferred, including configuration files, documents, and Web pages.

Secure Internet Tunneling

F-Secure SSH Client provides a secure transmission tunnel for data. For example, you can secure your e-mail connections or intranet and extranet browsing with tunneling. The tunneling is also known as port-forwarding.

Wide Range of Support

F-Secure SSH Client supports Public Key Infrastructure (PKI), smart cards and Advanced Encryption Standard (AES).

1.3 The F-Secure SSH Product Family

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

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

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

2. Installing F-Secure SSH Client

2.1 System Requirements

Operating System:	Windows 98/ME or NT 4/2000/XP/.net
Processor:	Pentium processor, 300MHz and up
Memory:	64 Mb
Disk space to install:	20 Mb

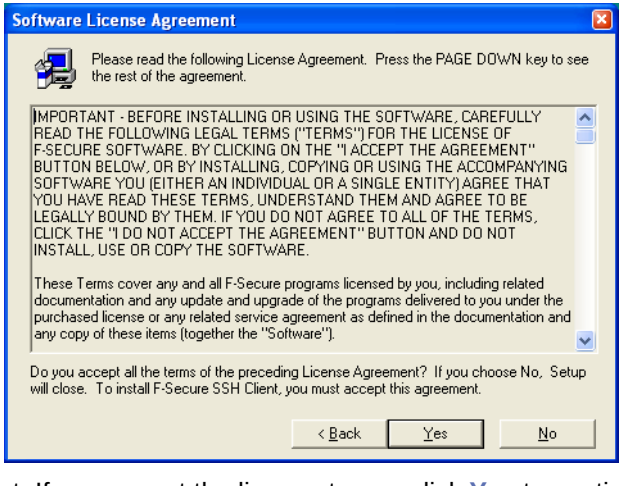
2.2 Installation

To install the F-Secure SSH Client, run the F-Secure SSH Client setup program.

Step 1

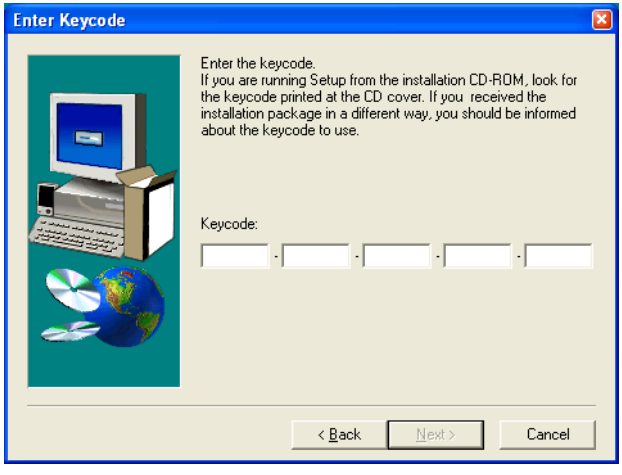
Read the welcome screen and click **Next** to continue.

Step 2



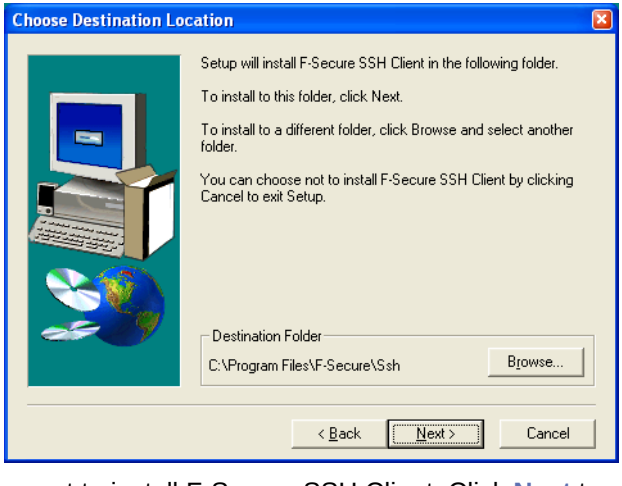
Read the license agreement. If you accept the license terms, click **Yes** to continue the installation.

Step 3



Enter the keycode provided to you. Click **Next** to continue.

Step 4

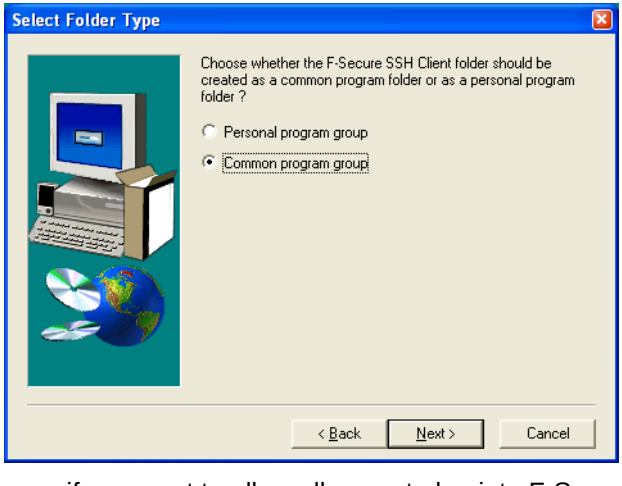


Select the folder where you want to install F-Secure SSH Client. Click **Next** to continue.

Step 5

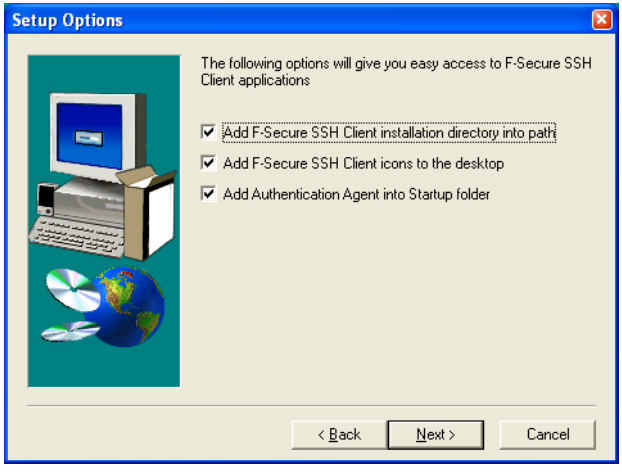
Select the folder in your Windows Start menu where you want to add F-Secure SSH Client icons. Click **Next** to continue.

Step 6



Select *Common program group* if you want to allow all users to log into F-Secure SSH Client or *Personal program group* if only the current user needs to log into F-Secure SSH Client. Click **Next** to continue.

Step 7



Select *Add F-Secure SSH Client installation directory into path* if you want to use command-line applications.

Select *Add F-Secure SSH Client icons to the desktop* to create shortcuts to the Windows desktop.

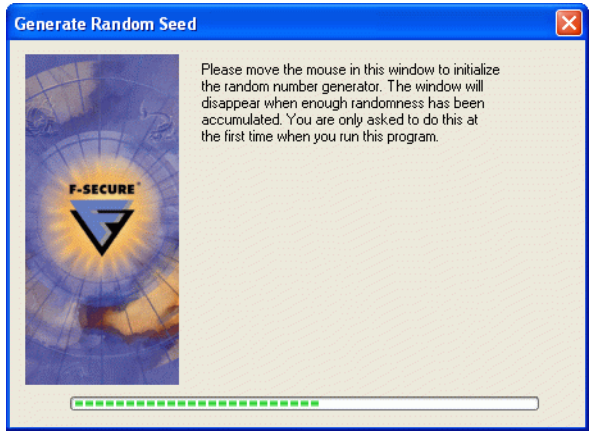
Select *Add Authentication Agent into Startup folder* to lauch F-Secure Authentication Agent automatically every time you start Windows.

Click **Next** to install F-Secure SSH Client.

2.3 Running F-Secure SSH Client for the First Time

Before you can use F-Secure SSH Client, you have to create a random seed. You need the random seed before you generate any host or user keys. The random seed functions as the starting point for creating keys. The random seed is also used to create randomness in all encryption processes and TCP packets.

Start F-Secure SSH Client to create a random seed.



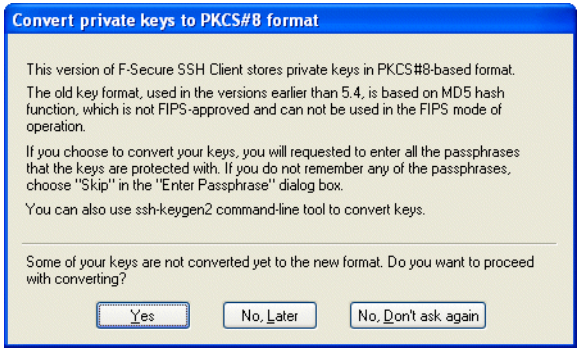
To create the random seed, move your mouse pointer in the window until the progress indicator reaches the end. When the random seed has been generated, F-Secure SSH Client starts.

2.4 Upgrading from Earlier Versions

To upgrade your F-Secure SSH Client, follow the installation instructions. For more information, see “*Installation*” on page 4.

Earlier versions of F-Secure SSH Client did not store private keys in FIPS-approved format. If you have private keys which have been created with an earlier version of F-Secure SSH Client and you want to use FIPS operation mode, you have to convert your keys into PKCS#8-based format.

When you start F-Secure SSH Client and you have keys which have not been converted yet, F-Secure SSH Client prompts you to convert them.



Click **Yes** to convert your keys to new format. You have to enter your passphrase for each key you convert.

Click **No, Later** to view the convert prompt again the next time you start F-Secure SSH Client. Click **No, Don’t Ask Again** to disable the automatic convert prompt.

3. Using F-Secure SSH Client

3.1 Overview

To start F-Secure SSH Client, open *F-Secure SSH Client* from the *Windows Start menu* > *Programs* > *F-Secure SSH Client*.

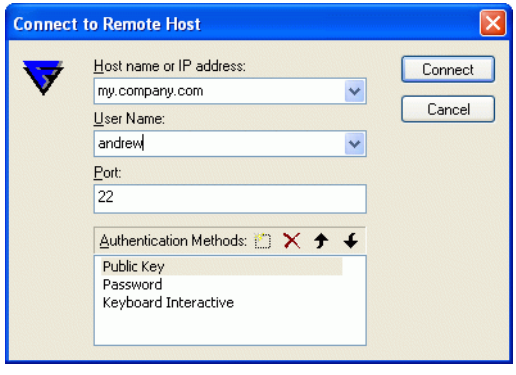
- You can use Quick Connect or create Profiles to connect to remote SSH servers. For information how to quickly connect to a remote SSH server, see “*Connecting to Remote Hosts*” on page 11. For more information about Profiles, see “*Using Profiles*” on page 14.
- For information on transferring files with F-Secure SSH Client, see “*Transferring Files*” on page 16.
- For information how to create and use SSH tunnels, see “*Tunneling*” on page 17.

3.2 Connecting to Remote Hosts

To connect to an SSH server, follow these steps:

1. By default, when you start F-Secure SSH Client the *Connection* dialog box opens automatically. You can open the *Connection* dialog by clicking **Quick Connect** in the *Profile Bar* or pressing ENTER or SPACE when you are not yet connected to any host and the terminal window is open.
2. Type the name or the IP address of the host you want to connect to, and your user name on the remote host. Change the port number if the remote SSH server uses a port other than the default 22.

3. Add an Authentication Method by clicking the New ( ) icon.

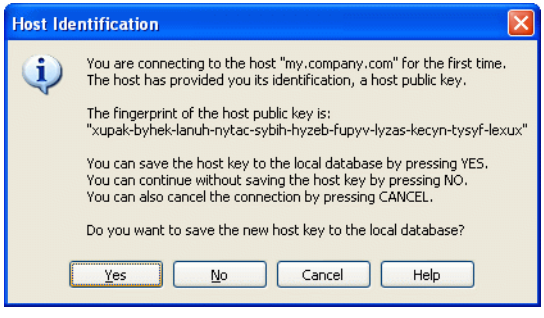


You can add any of available authentication methods: *Password*, *Public Key*, *SecurID*, *GSSAPI*, *PAM* and *keyboard-interactive*. For more information, see "*Authentication Methods*" on page 37.

You can change the order of methods by selecting a method with your mouse and moving it up or down on the list using the up and down arrows. If the first method on the list fails, F-Secure SSH Client tries to authenticate you with the following method.

4. Click **OK** when you have entered all the required information.

5. If this is the first time you connect to a particular host, the host provides you the public key as an identification.



   Click **Yes** to add the host key to the local host key database for future reference and to connect to the host. Click **No** to connect to the host without saving the the host key.

   Click **Cancel** to cancel the connection to the host. The host key is not saved to the database if you cancel the connection.

6. If the information you have provided is correct and the host you are connecting to supports SSH, you are now connected to the remote server.

Disconnecting from a Remote Host

To close the connection, do one of the following:

- If you have an active terminal session 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 the Disconnect ( ) icon in the toolbar.

You can change the host where you are connected without quitting F-Secure SSH Client. Disconnect from the host you are connected and connect to the other remote host as usual. For more information, see *“Connecting to Remote Hosts” on page 11.*

Cloning a Connection

If you want to create a new connection to the host that you are currently connected, you can clone the connection.

To clone the connection, choose *New Terminal* () or *New File Transfer* () from the *Window* menu or click their respective icons in the toolbar.

If the connection in your original window is open, the cloned windows are connected as well. All cloned windows (terminals and file transfer windows) use the same connection as the original window.

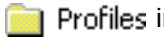
3.3 Using Profiles

Different 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 having to use the *Settings* view.

For more information how to open new connections from the *Settings* view, see "*Connection" on page 51.*

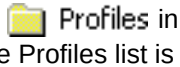
Creating a Profile

To create a Profile, follow these steps:

1. From the *File* menu, choose *Profiles* > *Add Profile*, or click  in the toolbar and select *Add Profile*.
2. Enter a name for the new Profile in the *Add Profile* dialog box.

You can create a new Profile from an open connection or from a previously saved Profile. For more information you can associate a connection with a Profile, see "*Connection*" on page 51.

Opening a Profile

To open a Profile, go to *File* > *Profiles* or click  in the toolbar and select the Profile you want to open. If you have not created any Profiles, the Profiles list is empty.

Editing Profiles

To edit a Profile, follow these steps:

1. Choose *Profiles* > *Edit Profile* from the *File* menu, or click Profiles in the toolbar and select *Edit Profile*.
2. Enter all the information you want to apply to the profile in the *Settings* panes. For more information, see "*Connection*" on page 51. Click **OK** when you are done.
3. Click the Save ( ) icon or select *Save* from the *File* menu to save the edited Profile.

Organizing Profiles

You can organize your Profiles into folders and subfolders from the *Edit Profiles* view.

- To create a new subfolder in the Profiles tree, right-click on a folder and select *New Folder*.
- To delete a folder, right-click on a folder and select *Delete*.
- To rename a Profile or a folder, right-click on it and select *Rename*.
- To move Profiles between folders, drag and drop a Profile into the destination folder, or use the copy and paste from the right-click menu.

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*, or click Profiles in the toolbar and select *Import Profile*.

For F-Secure SSH FTP Profiles:

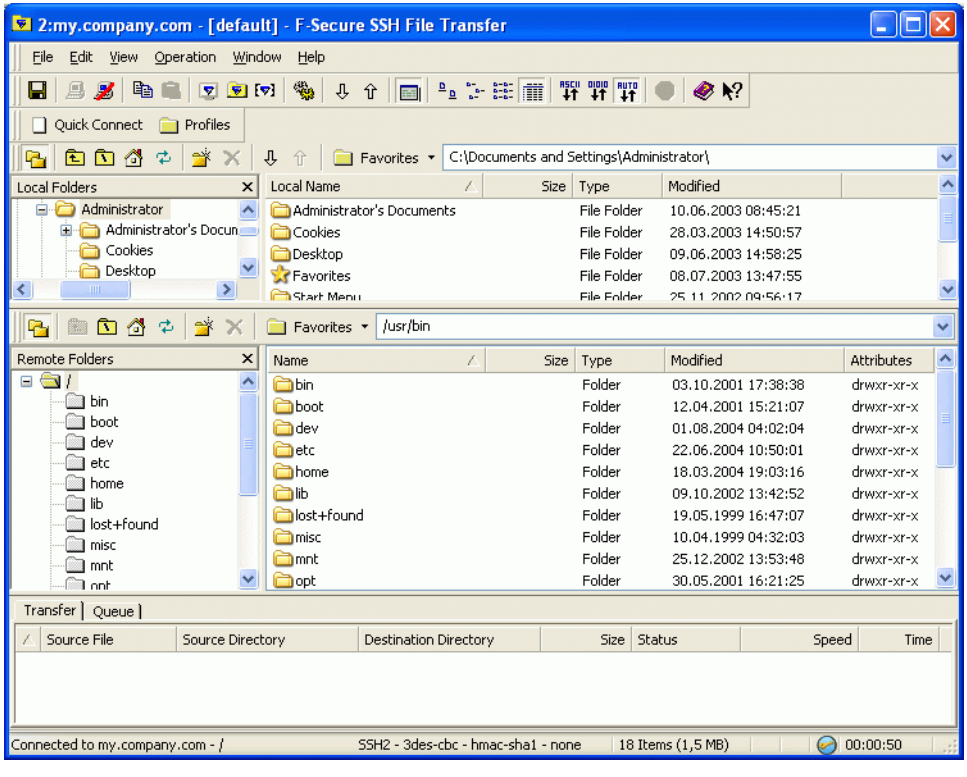
- Select the Profile(s) you want to import from the list and click **Import** on the right side of the dialog box.

For F-Secure SSH Client Profiles:

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

3.4 Transferring Files

To open the File Transfer window, start *F-Secure SSH File Transfer* from the *Windows Start menu* > *Programs* > *F-Secure SSH File Transfer*. If you have the F-Secure SSH Client open, you can choose *New File Transfer* ( ) from the *Window* menu or click the icon in the toolbar.



The File Transfer window shows local files folders and remote files and folders. You can browse both folder lists like you use Windows Explorer.

The Transfer View pane at the bottom of the File Transfer window displays the list of uploaded and downloaded files.

For icon and menu descriptions, see “*Menus and Toolbars*” on page 96.

Downloading Files

To download files, select the files you want to download and use one of the following methods:

- Drag and drop the files to a destination folder on the local computer.
- Right-click one of the selected files and select *Download*.
- Select *Download* from the *Operation* menu.
- Press CTRL+D.

Uploading Files

To upload files, select the files you want to upload and use one of the following methods:

- Drag and drop the files to a destination folder on the remote computer.
- Right-click one of the selected files and select *Upload*.
- Select *Upload* from the *Operation* menu.
- Press CTRL+U.

3.5 Tunneling

F-Secure SSH Client supports secure TCP/IP port-forwarding technology to connect arbitrary and otherwise insecure connections over a secure channel.

How Tunneling Works

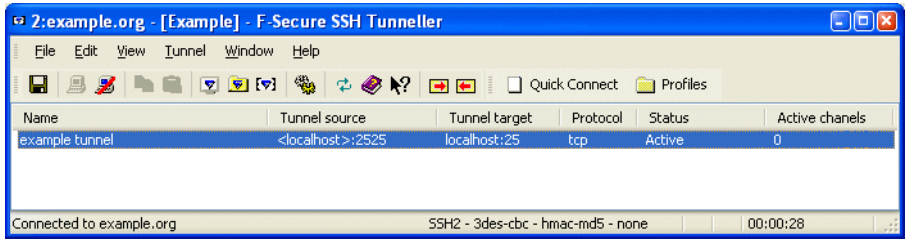
When you create a local tunnel, the following events take place:

1. F-Secure SSH Client creates a proxy server to the local computer for a source port of a TCP/IP service.
2. The proxy server waits for connections to the source port from any program.
3. When a program connects to the source port, F-Secure SSH Client forwards the request and the data over the secure channel to the remote host.
4. The SSH server on the remote host creates the final connection to the destination host and the destination port.

Most remote services that use TCP/IP can be secured, including client-server applications, database systems, and services such as http, telnet, pop, and smtp. F-Secure SSH Client also provides automatic forwarding for the X11 Windowing System commonly used on UNIX machines. For more information, see "*Tunneling*" on page 60.

Tunnel View Window

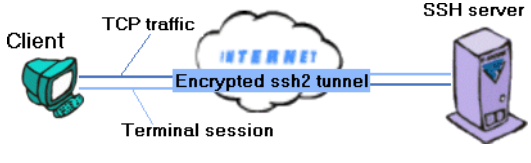
To open the Tunnel View window, start F-Secure SSH Client and choose *New Tunnel View* ([▽]) from the *Window* menu or click the icon in the toolbar.



In the Tunnel View window, you see the status of the tunnels you have created. The status can be either *Active*, *Not Ready*, *Not connected* or *Failed*.

- *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 not ready for use, for example it is waiting for an authentication.
- *Failed* means that an error has occurred. Another tunnel could be using the same port at either end of the tunnel already or you are not allowed to use the specified port for a tunnel. For 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.

Local Tunneling



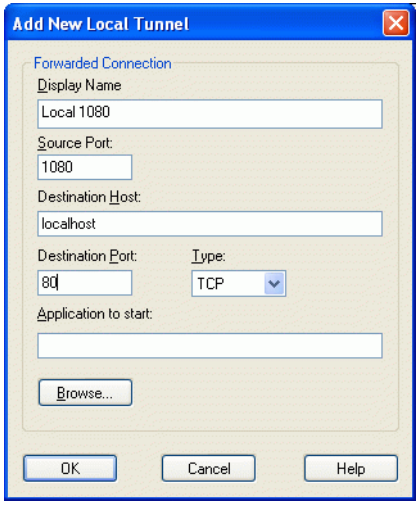
A local tunnel is a secure, encrypted connection between F-Secure SSH Client and the remote SSH server. All data that travels through the local tunnel is encrypted. However, note that any data that is forwarded to a computer outside the tunnel is not encrypted once it leaves the tunnel.

When you create a local tunnel, you set up F-Secure SSH Client to listen to a specific port on your local computer. When F-Secure SSH Client receives a data request on that port, it transfers the request to the specified port on a remote host.

Creating a Local Tunnel

Follow these instructions to create a local tunnel:

1. Open an SSH connection from your computer to an SSH server.
2. Open the Tunnel view and select *New Local Tunnel* from the *Tunnel* menu, or select *Settings* from the *Edit* menu and go to *Profile* > *Tunneling* > *Local* and click **Add**.



3. Enter a name for the tunnel in the *Display Name* field. Use a descriptive name that helps you to recognize the tunnel later.

4. Enter a source port that F-Secure SSH Client should listen for TCP data requests to the *Source Port* field. The source port is a port on which the computer you are making the connection from is listening for a connection.

   The source port number should be greater than 1023, as many lower ports are used for other internet protocols. However, F-Secure SSH Client does not restrict the use of these port numbers.

   If the protocol or the application that will use the tunnel has a fixed port number, the source port number should be the same, fixed port number.

   If you create several tunnels for one connection, you have to specify a source port that you have not yet used (>1023).

5. Enter the DNS name or the IP address as the *Destination Host* where the tunnel directs the connection from your own workstation.

   The destination host address is relative to the host you are connecting to, which means that a host such as *127.0.0.1* or *localhost* refers to the SSH server and not the computer from which you are initiating the tunnel. For more information about the destination host, see "*Creating a Tunnel to a Third Host*" on page 22.

6. Enter the port on the SSH server to which the connection is forwarded to the *Destination Port* field. The destination port should be the TCP/IP port where the application which uses the tunnel sends its data requests.

7. Select whether the tunnel is a TCP tunnel or an FTP tunnel.

8. If you want to start some application automatically when the tunnel is created, enter it into the *Application to start* field. Click **Browse** to browse for the application.

   If you do not want to start any application automatically, you can leave the *Application to start* field empty.

9. Click **OK**. The new local tunnel opens automatically.

10. When F-Secure SSH Client receives a request to the source port, it transfers the request through the encrypted tunnel to the SSH server at the destination port, and you are connected to the destination port through an SSH tunnel.

Examples

Reading E-mail from a POP3 Server

1. Create a local tunnel with the following values:

Source Port:	1110
Destination Host:	localhost
Destination Port:	110
Type:	TCP

2. Configure your e-mail client to read e-mail from *localhost* and port 1110.
3. Connect to the POP3 server with F-Secure SSH Client.

Sending E-mail through an SMTP Server

1. Create a local tunnel with the following values:

Source Port:	2525
Destination Host:	localhost
Destination Port:	25
Type:	TCP

2. Configure your e-mail client to send e-mail to *localhost* and port 2525.
3. Connect to the SMTP server with F-Secure SSH Client.

Receiving Web Content from a HTTP Server

1. Create a local tunnel with the following values:

Source Port:	8080
Destination Host:	localhost

Destination Port:	80
Type:	TCP

2. Connect to the HTTP server with F-Secure SSH Client.
3. Connect your web browser to '*localhost:8080*'.

Connecting to an FTP Server

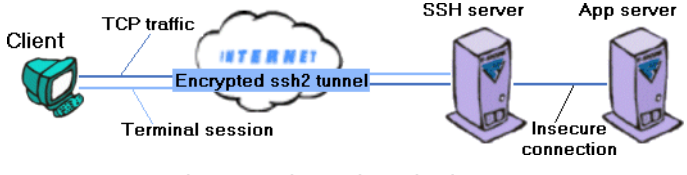
1. Create a local tunnel with the following values:

Source Port:	8021
Destination Host:	localhost
Destination Port:	21
Type:	FTP

2. Connect to the FTP server with F-Secure SSH Client.
3. Connect your FTP client to '*localhost*' at port 8021. You can use either active or passive FTP mode.

Creating a Tunnel to a Third Host

Another way of using local tunnels is to forward data through the SSH server to a third host. It is important to know that data is encrypted only when it travels between F-Secure SSH Client and the SSH server and it is no longer encrypted when it is tranferred between the SSH server and the third host. However, if you use this functionality to transfer data between your computer and a trusted intranet network, the server-to-third-host security is not an issue.

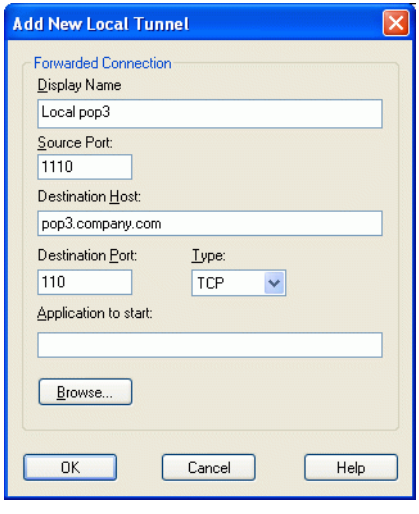


Usually, you can access your company intranet through a single SSH server. Once you access the server, you can connect to the other servers that run inside the intranet. In other words, you can create a tunnel to

a third host to access data, such as e-mail, Web content or news. This is done by specifying the destination host as something other than '*localhost*'.

For example, to read your e-mail from a pop3 server in your company intranet from home, follow these instructions:

1. Connect to *my.company.com* with F-Secure SSH Client.
2. Create a new tunnel where F-Secure SSH Client listens for data requests at port 1110 in your home computer and to forwards any received data requests to the pop3 server at the pop3 port (110) of your company through the SSH server.



   You can use either the DNS name or IP address of the server. If you create several tunnels for one connection, you need to specify a source port that you have not used yet and it should be greater than 1023.
3. Configure your e-mail client to search for e-mail at '*localhost*' at port '1110'.
4. When the e-mail client first attempts to retrieve mail you are asked to enter your username and password. Use the username and password for the e-mail server (do not use the SSH server authentication information).

Examples

Forwarding Telnet Connection from a Telnet Server

1. Connect to the SSH server.
2. Create a local tunnel with the following values:

Source Port:	2323
Destination Host:	telnet.company.com
Destination Port:	23
Type:	TCP

3. Connect to '*localhost*' at port 2323 with a telnet client.

Sending E-mail through an SMTP Server

1. Connect to the SSH server.
2. Create a local tunnel with the following values:

Source Port:	2525
Destination Host:	smtp.company.com
Destination Port:	25
Type:	TCP

3. Configure your e-mail editor to send mail through '*localhost*' at port 2525.

Forwarding Web Content from the HTTP Server

1. Connect to the SSH server.
2. Create a local tunnel with the following values:

Source Port:	8080

Destination Host:	intraweb.company.com
Destination Port:	80
Type:	TCP

3. Connect your Web browser to '*localhost*:8080' to receive the content.

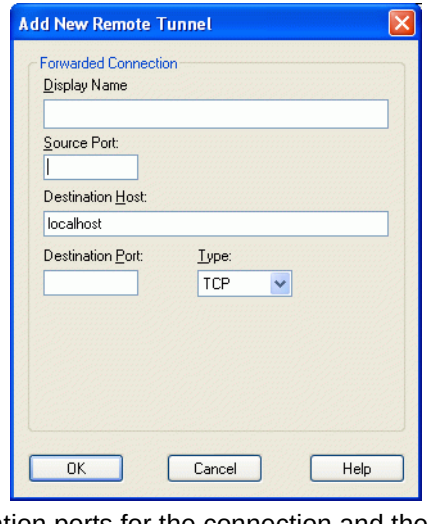
Remote Tunneling

In remote tunneling, you configure F-Secure SSH Client to listen to data requests that an SSH server receives at the specified port and then transfer those requests to your computer or through your computer to a third host. Note that the data is not encrypted outside the tunnel if you forward data to a third host.

Creating a Remote Tunnel

Follow these instructions to create a remote tunnel:

1. Open an SSH connection from your computer to an SSH server.
2. Open the Tunnel view and select *New Remote Tunnel* from the *Tunnel* menu, or select *Settings* from the *Edit* menu and go to *Profile* > *Tunneling* > *Remote* and click **Add**.



3. Specify the source and destination ports for the connection and the host to forward the connection to.

4. Enter a name for the tunnel in the *Display Name* field. Use a descriptive name that helps you to recognize the tunnel later.
5. Enter the port on the remote machine to which the client listens for connections to the *Source Port* field.
6. Enter the DNS name or the IP address of the host to which the connection is forwarded from the remote host when a connection to the specified port is requested as the *Destination Host*.

   The destination host address is relative to the host you are connecting from, which means that a host such as *127.0.0.1* or *localhost* to the computer from which you are making the SSH connection and not the remote computer to which you are connected.
7. Enter the port number on the destination host to which you want the connection to be forwarded to the *Destination Port* field.

Examples

Forwarding Telnet Connection to Local Computer

Create an SSH tunnel to *my.company.com* and configure F-Secure 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

1. Connect to the SSH server.
2. Create a remote tunnel with the following values:

Source Port:	2323
Destination Host:	localhost
Destination Port:	23
Type:	TCP

Forwarding Telnet Connection to a Third Host

Create an SSH tunnel to *my.company.com* and configure F-Secure SSH Client to listen for data requests at port 2323 on that server, and forward all received data requests to port 23 of *third.host.com*.

1. Connect to the SSH server.

2. Create a remote tunnel with the following values:

Source Port:	2323
Destination Host:	third.host.com
Destination Port:	23
Type:	TCP

3.6 Using Command Line Applications

F-Secure SSH Client includes multiple applications that can be used from the Windows command line:

- ssh2 – Log on to a remote machine and execute commands.
- scp2 – Copy files between hosts on a network.
- sftp2 – Start a secure file transfer session between two hosts.
- ssh-keygen2 – Create authentication keypairs.

Using ssh2

The ssh2 application starts secure terminal connections to remote hosts, executes commands on remote hosts and creates tunnels for the secure TCP packet and X11 connection transfers. The application can be used as a secure substitute for rlogin, rsh and telnet. It provides secure, encrypted communications between two hosts over an unsecure network.

The ssh2 application connects and logs in to the specified hostname. You must prove your identity to the remote host by using either the password or public-key authentication method.

Use the following format to start an ssh2 session from the 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, do not need to specify your user name. 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`.
- The ssh2 application uses settings from the following sources, in this order:
  - The configuration file, see "*Available Settings in ssh2_config* on page 113.
  - Command line options.

  The last obtained value is used.

Examples

```
ssh2 second.host.com
ssh2 user@third.host.com
ssh2 -l user third.host.com
```

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.
-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.
-W file	Reads password from a file.
-h	Displays brief help about command-line options.

Using scp2

The scp2 (Secure Copy) application is used to copy files over the network securely. It uses the SSH2 protocol and the same authentication for data transfer and it provides the same security as SSH2. Unlike rcp, scp2 asks for passwords or passphrases if they are needed for authentication.

When copying files, any filename may contain a host, user and port specification. You can copy files between two remote hosts.

Use the following format for copying files with scp2:

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

- All options start with “-“.
- The first filename is the source file and the second is the destination file. The source filename can include wildcards. When you copy multiple files using wildcards, you can only specify a path in the destination filename.
- The scp2 application does not create directories for you - the destination directory must exist before the file transfer.
- The host name needs to be specified 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 default ssh2 port.

Examples

To copy the file *program.exe* from your local hard drive to *second.host.com*, where your `user name` is *user*:

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

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

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

To copy files with a name containing any one character in the place of the question mark from the *program* directory under your home directory on *second.host.com* to the *C:\program* directory on your local hard drive:

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

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

Using sftp2

The sftp2 (Secure File Transfer) application is an ftp-like client that can be used in file transfer over the network. The sftp application uses SSH2 in data connections.

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

```
sftp2 [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 –b *filename* 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 *latest.zip* file and close the connection:
	`open andrews@my.company.com`
	`get latest.zip`
	`close`

-V	Show the version number of the software.

After initiating the sftp2 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. Directories are recursively copied with their contents. You can use the following switches with the get command: -p, --preserve-attributes - Try to retain file permissions and timestamps. -W,--whole-file - Do not make incremental checksums.

	-c,--checksum - Do an sha1 checksum to determine whether the file needs to be transferred if the source and destination files have the same size. By default, the checksum is done. You can toggle any switch with a "no" as an attribute. For example, “--checksum=no” turns off the sha1 checksum.
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.
lmkdir	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.
lrmdir 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. Directories are recursively copied with their contents. You can use the same options as with the get command.

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.

Using ssh-keygen2

The ssh-keygen2 application generates and manages authentication keys. You can use ssh2-keygen to create authentication keys when you want to use the public key authentication method.

Command Line Options

-b bits	Specifies the key length in bits, for example 1024.
-t dsa | rsa	Specifies the user key type, either DSA or RSA.
-c comment_string	Specifies the key's comment string.
-e file	Edits the specified key. You can change the passphrase or the comment of the key.
-p passphrase	Specifies the passphrase for the key.
-P	Specifies that the key will be saved with an empty passphrase.
-h or -?	Prints a short summary of ssh-keygen2 commands.
-q	Hides the progress indicator.
-1 file	Converts key from ssh1 format to ssh2 format.
-i file	Displays all information about a key.

-D file	Derives the public key from the private key file.
-B number	Specifies the number base for displaying key information. The default number base is 10.
-V	Displays the version information.
-r file	Stirs data from a file to the random pool.
-x file	Converts a private key from X.509 format to SSH2 format. The converted key is written to file_ssh2.
-k file	Converts a PKCS 12 file to an SSH2 format private key and certificate pair.
-7 file	Exports certificates from a PKCS 7 file.
-S file	Converts SecSH private key to F-Secure FSCLM format.
-H file	Converts F-Secure FSCLM private key to SecSH format.
-F file	Dump fingerprint of given publickey. The fingerprint is given in the Bubble Babble format, which makes the fingerprint look like a string of "real" words (making it easier to remember).

4. Authentication Methods

4.1 User Authentication Methods

The server can authenticate the user in a number of ways. F-Secure SSH Client supports the following authentication methods:

- Password authentication

  The traditional authentication method, where the password is transmitted over the encrypted channel and cannot be seen by outsiders.

  The server may require that you change your password after you log in.

  ```
  WARNING: Your password has expired.
  You must change your password now and login again!
  Changing password for <username>
  (current) UNIX password:
  Enter new UNIX password:
  Retype new UNIX password:
  passwd: password updated successfully
  ```

  Login with your new password after you have changed your password and the server closes the connection.

- Public Key authentication

  The possession of a particular DSA or RSA key serves as the authentication. The server has a list of accepted public keys.

  In SSH2, the DSA authentication is default. The RSA authentication is used in SSH1 and in some versions of SSH2. For more information, see “*Public Key Authentication*” on page 38.

- Keyboard-Interactive authentication

  A generic authentication method that can be used to implement different types of authentication

mechanisms. For example, currently the following keyboad-interactive authentication methods are supported by F-Secure SSH Servers:

- password
- securID
- PAM

New keyboad-interactive authentication methods that can be implemented include, for example, S/KEY and other One-Time-Pads, hardware tokens similar to SecurID, which print a number or a string in response for a challenge sent by the server, and legacy authentication methods. For more information, see “*Keyboard-Interactive Authentication*” on page 48.

The Keyboard-Interactive authentication method cannot be used if it requires passing some binary information, as in public-key authentication.

- PAM

  The Pluggable Authentication Module (PAM) is a new standard authentication framework. PAM can be used to integrate different authentication methods, thus unifying the authentication mechanisms. PAM can also integrate smart card authentication.

  PAM has support for binary messages and client-side agents that the Keyboard-Interactive authentication method does not support. However, currently there are no implementations that take advantage of the binary messages in PAM.

- SecurID

  The SecurID authentication requires a SecurID device, which generates numeric codes that are needed in the authentication.

- GSSAPI

  The Generic Security Services Application Programming Interface (GSSAPI) is a generic API for performing client-server authentication for users in the same domain. With GSSAPI support, F-Secure SSH Client can utilize NTLM and Kerberos authentication protocols. NTLM authentication is for NT domain users, and Kerberos for Windows 2000, XP and Windows 2003 domain users.

4.2 Public Key Authentication

You have to generate a new keypair and upload the public key to the SSH server to use the public key authentication method. For information how to generate a new public and private keypair, see “*Generating a New Keypair*” on page 40.

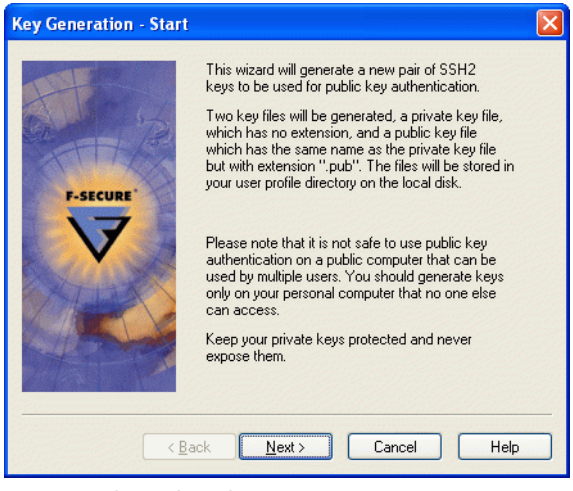
When you connect to the SSH server with public key authentication, you are asked to enter your passphrase associated with the private key. Enter your passphrase to connect to the remote host computer.

If you are not asked for the private key, make sure that you have uploaded your public key to the server. For more information, see “*Uploading the Public Key*” on page 43.

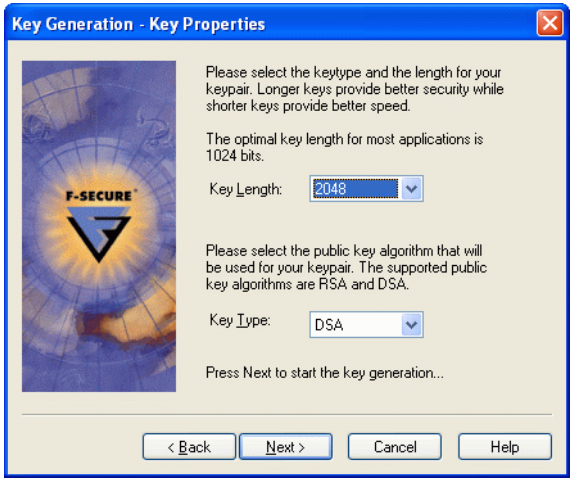
The SSH server may be configured to use some other authentication method with the public-key authentication for increased security. In this case, you have to authenticate yourself by the other authentication method before you can authenticate with the public-key authentication method.

Generating a New Keypair

1. Go to the *Settings* > *Global Settings* > *User Keys* view and click **Generate New Keypair** to start the key generation.

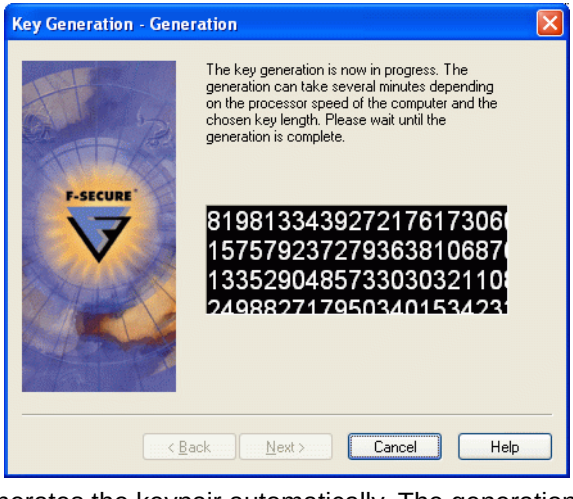


2. Click **Next** to start the key generation wizard.

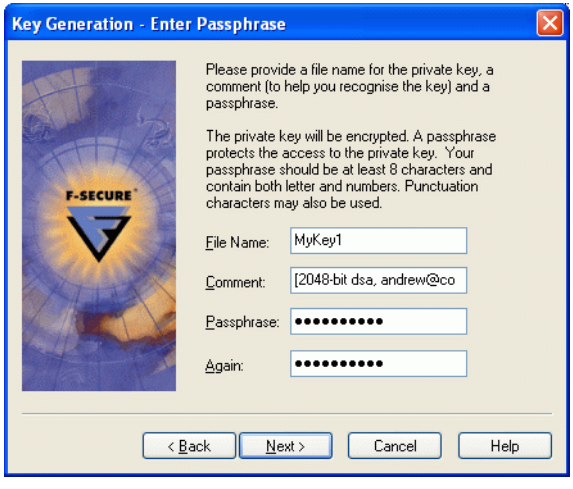


Item	Description
Key type	Select the public key algorithm to use. The available algorithms are DSA and RSA. In the SSH2 protocol, DSA is the default option. Use RSA if you want the key to be compatible with the SSH1 protocol. Note that in some versions of the SSH2-based software, RSA is not available. Select DSA to if you want to be sure that your key is compatible with all SSH2-based software..
Key length	Select the length of the key. Shorter keys are generated faster, but longer keys provide increased security.

3. Click **Next** to start the key generation.



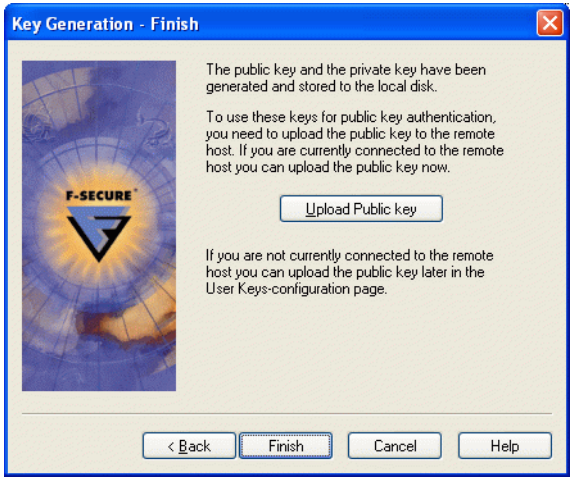
4. F-Secure SSH Client generates the keypair automatically. The generation can take several minutes, depending on the selected key size the speed of your computer. When the key generation is complete, you can click **Next** to continue.



Item	Description
File name	Enter the filename for the keypair.
Comment	Add a comment which helps you to recognize the key later.
Passphrase	Enter a good passphrase for the key. A good passphrase is at least 8 characters long and contains letters, numbers and non-alphabetic characters.
Again	Enter the passphrase again to make sure you entered it correctly.

Leaving the passphrase empty is a security risk.

5. Click **Next** to continue.



6. If you are connected to the remote host, you can upload the public key by clicking **Upload Public Key**. If you want to upload the public key later, click **Finish** to return to the Settings view.

Uploading the Public Key

You have to upload your public key to the remote host before you can use the public key authentication.

You can upload the public key to the SSH server automatically:

1. Connect to the remote host.
2. Click **Upload Public Key** in the *Settings* > *Global Settings* > *User Keys* view to upload the public key.

Follow these instructions to upload the public key manually:

1. Connect to the remote host and open the File Transfer window. For more information, see “*Transferring Files*” on page 16.
2. Make sure that you have *Show Hidden Files* selected in the View menu and go to .ssh2 directory in the remote host.
3. Your user keys are copied into the *UserKeys* directory under the installation directory. Browse to the UserKeys directory and select the public key file you want to copy to the remote host.

   The public key has the file extension .pub. Be careful you select the public key file and not the private key file that does not have a file extension.
4. Create a plain text file called *authorization*, for example with Windows Notepad.

   Type ‘`key [public key filename]`’ in the authorization file. For example, if the selected key is called *keyfile.pub*, enter the following text to the file:

   ```
   key keyfile.pub
   ```

   Save the authorization file and make sure that it does not have any filename extension (remove the default .txt extension).
5. Copy the selected public key and the authorization file to the .ssh2 directory in the remote host. For more information, see “*Uploading Files*” on page 17.

Public Key Infrastructure System

A Public Key Infrastructure (PKI) is a system that helps to establish secure communications by using digital certificates.

A PKI system includes end entities (communicating parties), trusted parties who sign and issue certificates (certification authorities) and parties who handle the identification of end entities (registration authorities).

A PKI uses asymmetric encryption to provide reliable authentication in an online environment. In asymmetric encryption, every entity has a public and private key pair. Private keys are secret and they used to sign and decrypt messages. Public keys can be published, for example, on a web server. Public keys are used to validate signatures and to encrypt messages.

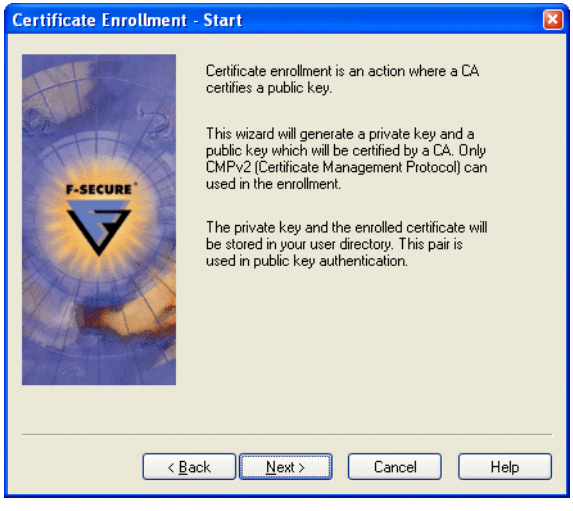
Before the public key can be used, it must be transferred securely to end entities to make sure it is genuine. Certificates can be used to distribute public keys. Certificates bind identity information about entities to their public keys. Certificates guarantee the indentity of the owner of the public key.

When the end entities are enrolled into the PKI and they have their certificates issued by the CA, their public keys are certified and they can communicate securely.

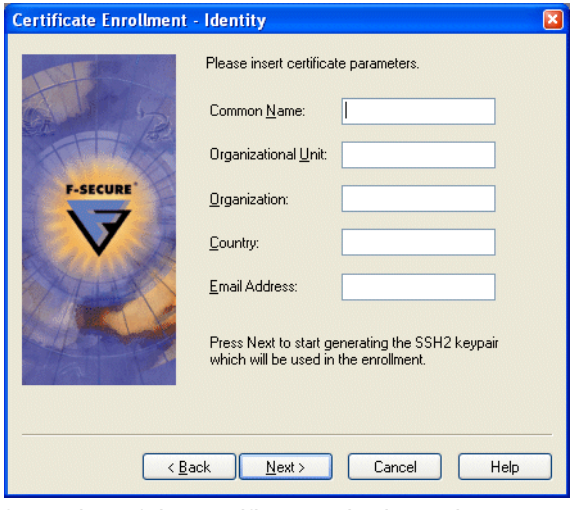
Certificate Enrollment Wizard

1. Go to the *Settings* > *Global Settings* > *PKI* > *Certificates* view and click **Enroll...** to start the certificate enrollment.

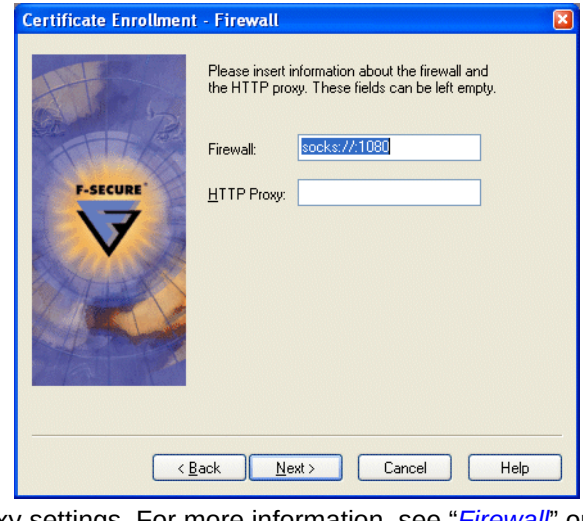
The certificate enrollment wizard can be used with CMPv2 compliant PKI solutions only.



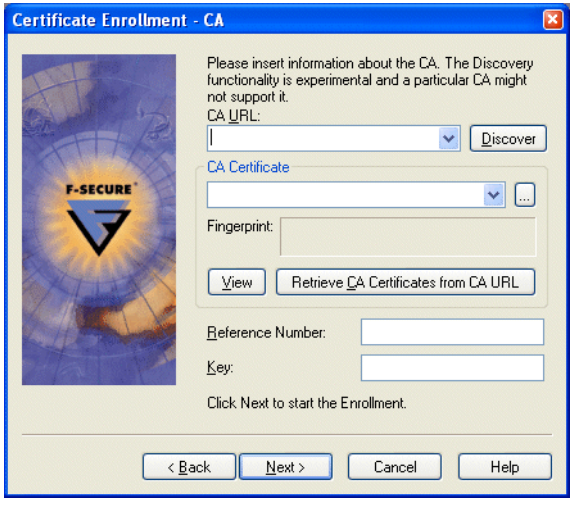
2. Click **Next** to continue.



3. Enter the identification information of the certificate to be issued.
4. Generate a new keypair. For more information, see "*Generating a New Keypair*" on page 40.



5. Specify firewall and proxy settings. For more information, see "*Firewall*" on page 56.



Item	Description
CA URL	Enter the certification authority server address. Click **Discover** to try to detect available certification authority services and CA certificates automatically.
CA Certificate	Select a CA certificate from the list, type in the filename of the certificate, or browse for the file by clicking **...**.
Fingerprint	Click **View** to display the contents of the current certificate. Click **Retrieve CA Certificates from CA URL** to retrieve CA certificates from the selected CA address.
Reference Number	Enter the reference number.
Key	Enter the key information.

6. Click **Next** to start the enrollment.
7. The enrollment may take some time. When the process is finished, click **Finish**.

4.3 Keyboard-Interactive Authentication

Any currently supported authentication method that requires only the user's input can be performed with the keyboard-interactive authentication. For example, currently the following keyboad-interactive authentication methods are supported by F-Secure SSH Servers:

- password
- SecurID
- PAM

PAM and SecurID are old style authentication methods and newer servers provide them as sub-methods of the keyboard interactive.

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.

5. Configuring F-Secure SSH Client

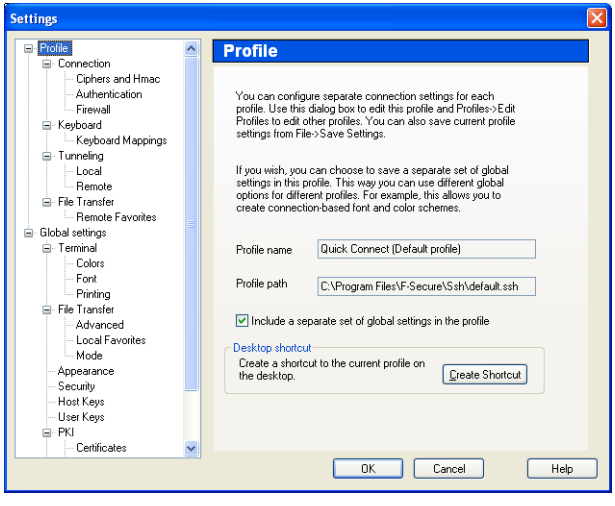
5.1 Overview

Select *Settings* from the *Edit* menu or click the *Settings* icon on the toolbar to modify the F-Secure SSH Client settings.

Use Profile Settings to configure separate settings for each profile. Use Global Settings to configure settings which affect all profiles. For more information about profiles, see “*Using Profiles*” on page 14.

5.2 Profile

In *Profile* settings pages, you can configure separate settings for each profile. When you open *Settings* view, you can edit the settings of the current profile. To edit other profiles, open *Profiles toolbar > Edit Profiles...*.

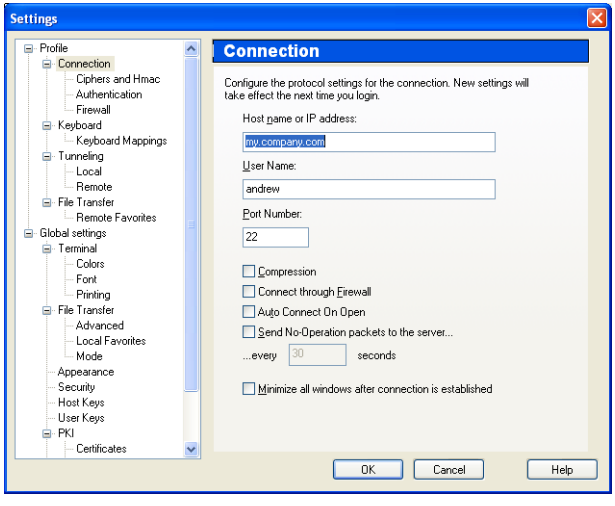


Profile name	Displays the name of the current profile.
Profile path	Displays the file name and path where the profile information is saved.
Include a separate set of global settings in the profile	Save a separate set of global settings with the current profile. Clear the check box to use the global settings.

Click **Create Shortcut** to create a a shortcut on the Windows desktop that opens the connection for the selected profile.

Connection

In the *Connection* page, you can configure the connection settings for each connection. New settings take effect the next time you login.



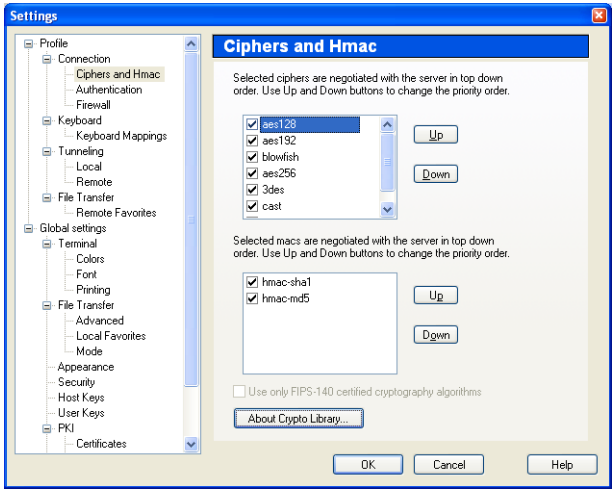
Host Name or IP address	Specify the host name or the IP address of the remote host.
User Name	Specify the user name you use when you log in to the remote host.
Port Number	Specify the port number on the remote host. The default port number is 22.
Compression	Compress all transferred data, including tunneled data.

Use compression if your connection speed is slow The compression efficiency depends on the transferred file types.

Connect through Firewall	Select the check box if you connect through a firewall. Specify the firewall in the *Firewall* settings. For more information, see “*Firewall*” on page 56.
Auto-connect on open	Connect to the host automatically when the profile is opened.
Send No-Operation Packets to the Server	Send no-operation (NOOP) packets to the server at specified intervals to keep the connection alive even if there is no traffic between the server and the client.
Minimize all windows after connection is established	Minimize all connection specific terminal, file transfer and tunnel windows after you have established the connection.

Ciphers and Hmac

In the *Ciphers and Hmac* page, you can select which cryptographic algorithms (cipher) and message authentication code (MACs) you want to use to encrypt data for the session.



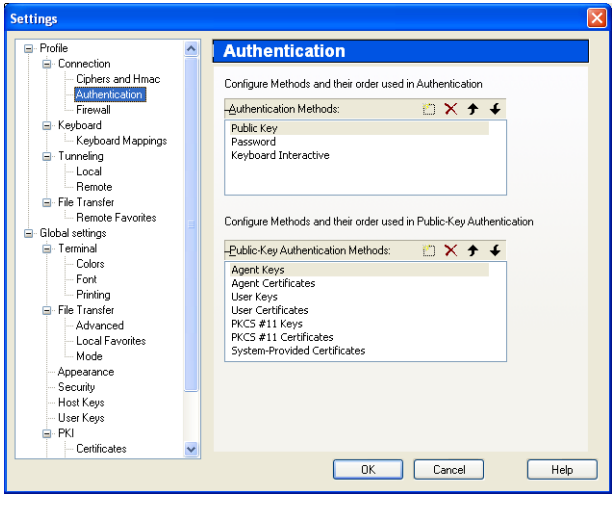
Ciphers	Select which ciphers you want to use. Clear the check box in front of the cipher to deactivate it. Ciphers are compared to the list of ciphers on the SSH server in the order you have listed them. The first cipher on the list that matches a cipher that is available on the remote server is used for the session. Use the **Up** and **Down** buttons to change the order of ciphers.
MACs	Select which MACs you want to use. Clear the check box in front of the MAC to deactivate it. Use the **Up** and **Down** buttons to change the order of preference.
Use only FIPS-140 certified cryptography algorithms	Select whether you want to use only Federal Information Processing Standard 140-2 certified cryptography algorithms. Note that if you want to use only FIPS-140 certified cryptography algorithms, you might be unable to connect to some servers.

You cannot change ciphers or library mode while you are connected to a remote host.

Click **About Crypto Library** to display information about the currently used cryptographic library mode.

Authentication

In the *Authentication* page, you can select how you authenticate yourself to the server. If you use the public key authentication method, you can configure its methods and the order in which they are used.



Authentication Methods	Select which authentication methods you want to use. For more information, see "*Authentication Methods*" on page 37. 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. Use the **Up** and **Down** buttons to change the order of preference.
Public Key Authentication Methods	Select which Public Key authentication methods you want to use, if you have selected *Public Key* authentication as one of the authentication methods in the *Authentication Methods* pane.

For more information about *User Keys* and *User Certificates*, see “*User Keys*” on page 83.

For more information about *PKCS#11 Keys*, *PKCS#11 Certificates* and *System-Provided Certificates*, see “*PKCS #11*” on page 87.

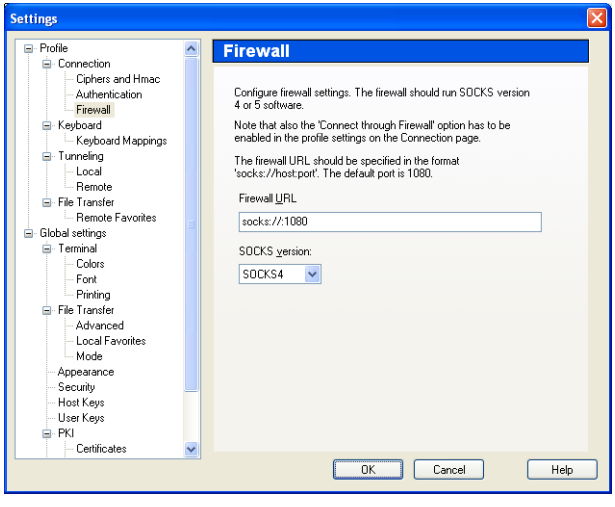
For more information about *Agent Keys* and *Agent Certificates*, see “*Agent Keys*” on page 89.

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.

Use the **Up** and **Down** buttons to change the order of preference.

Firewall

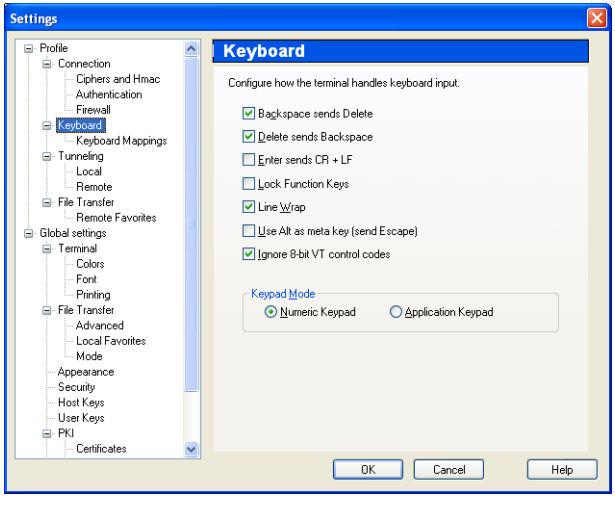
If you connect to the SSH server through a firewall, you need to configure the firewall settings in the *Firewall* page. Make sure that *Connect through Firewall* is selected in the Connection settings. For more information, see “*Connection*” on page 51.



Firewall URL	Enter the DNS or IP address of the firewall.
SOCKS version	Specify the SOCKS version that the firewall uses.

Keyboard

In the *Keyboard* page, you can specify options used to translate key presses and received terminal data into characters displayed in the terminal window.

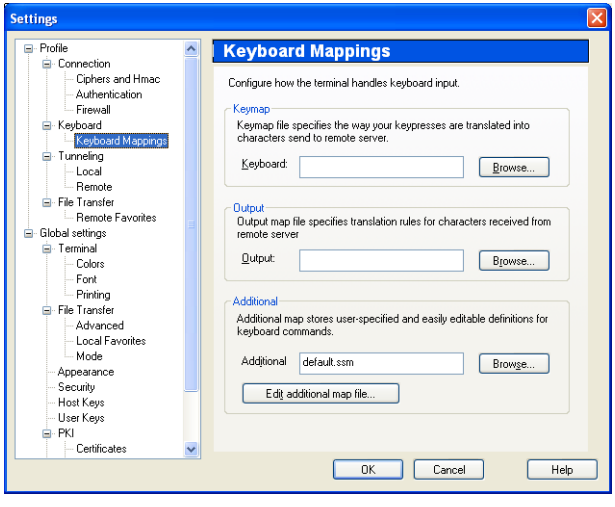


Backspace Sends Delete	Send the DELETE key code when you press the BACKSPACE key.
Delete Sends Backspace	Send the BACKSPACE key code when you press the DELETE key.
Enter sends CR + LF	Send a carriage return with a line feed character. If the check box is not selected, the ENTER key sends only the line feed character.
Lock Function Keys	Prevent all VT100 function keys (F1 to F20) from being programmed by VT100 escape codes.
Line Wrap	Wraps lines that do not fit in the window. If line wrapping is not selected, the lines are cut at the right edge of the window.

Use Alt as meta key (Send escape)	Send the escape signal to the terminal when you press the ALT key.
Ignore 8-bit VT control codes	Ignore all 8-bit VT terminal control code sequences. Note that some applications require these control sequences. In addition, you need to use 8-bit control codes in VT terminals to enter the € (euro) symbol. Clear the check box if you encounter any problems.
Keypad Mode	Select between the *Application Keypad* mode and the VT100 *Numeric Keypad* mode. Select *Numeric Keypad* to type numbers with the keypad and *Application Keypad* to use the keypad for the application control.

Keyboard Mappings

In the *Keyboard Mappings* page, you can configure how the terminal handles the keyboard input.



Keymap

Keyboard — Specify how your keypresses translate into characters in the remote server. Click **Browse** to browse for the keymap file.

Output

Output — Specify how the remote server characters display on the terminal window. Click **Browse** to browse for the keymap output file.

Additional

Additional — Specify keyboard shortcuts.

Click **Edit additional map file...** to open the keymap editor. The keymap editor allows you to define additional key mappings, open saved keymap files and create new key map files. For more information, see “*Keymap Editor*” on page 91.

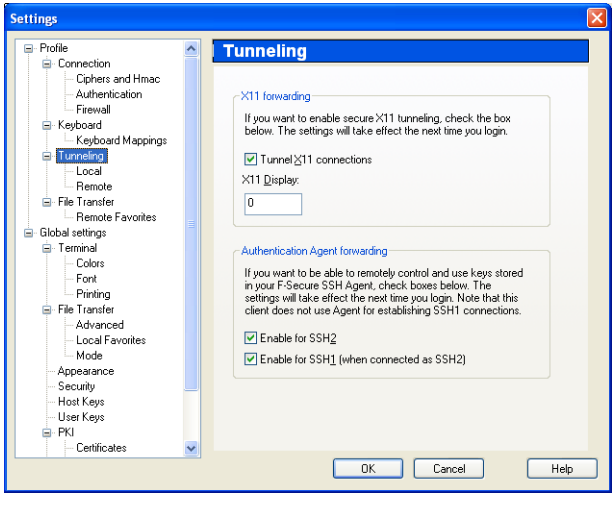
Tunneling

In *Tunneling* settings pages, you can configure local and remote TCP/IP connections to be secured by forwarding them through the SSH connection.

F-Secure SSH Client can tunnel X11 graphic connections from the remote host to an X-Windows server running on the local computer.

Note that you must have an X emulator running in the passive mode for X11 tunneling to work.

The tunneling settings take effect the next time you login.



X11 forwarding

Tunnel X11 connections	Enable the X11 forwarding.
X11 display	Define the X11 display number. For more information on this, consult your X11 server manual.

Authentication Agent forwarding

Enable for SSH2	Enable the remote control and use of keys stored in F-Secure SSH Authentication Agent.

Note that you cannot use F-Secure SSH Authentication Agent to establish SSH1 connections.

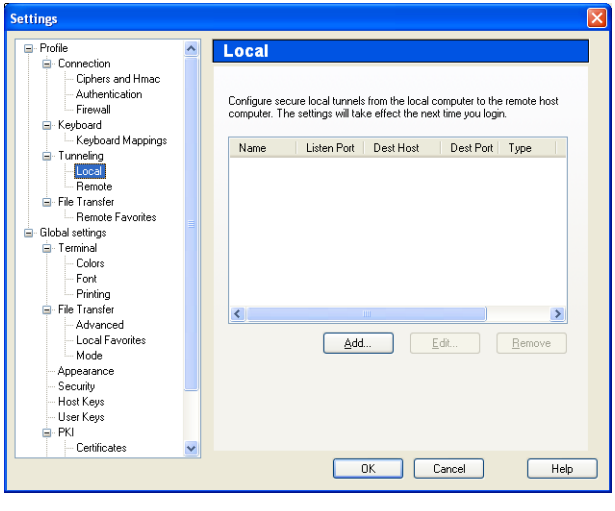
Enable for SSH1 (when connected as SSH2)

When you are connected to an Unix host with the SSH2 protocol, F-Secure SSH Authentication Agent can be used to connect to other Unix hosts using SSH1 or SSH2, and you can use `ssh-add1` as well as `ssh-add2`.

However, you have to use SSH2 protocol to connect from your Windows computer, the agent is not used or forwarded when you use SSH1 to create the initial connection.

Local Tunneling

In the *Local Tunneling* page, you can configure secure local tunnels from the local computer to the remote host. The page displays the local TCP/IP ports, which have been forwarded.



Name — Displays the name of the tunnel.

Listen Port — Displays the local port that the tunnel listens for TCP data requests.

Dest Host — Displays the destination host.

Dest Port	Displays the destination port where the connection is forwarded on the destination host.
Type	Displays the tunnel type, either TCP or FTP.
Application to start	Displays the name of the application that starts automatically when the tunnel is opened.

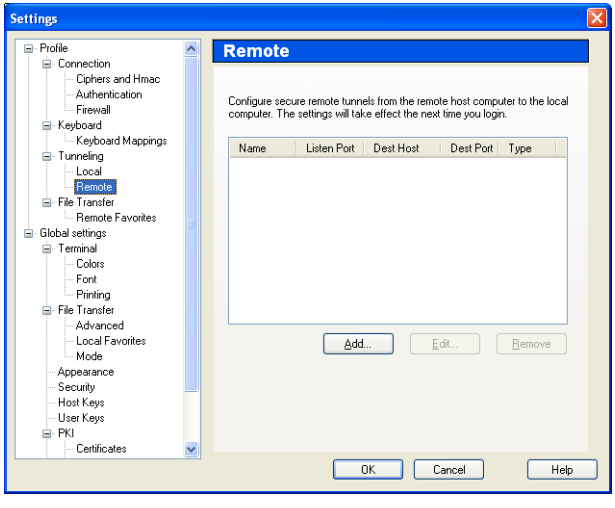
Click **Add** to define a new TCP/IP or FTP connection which you want to secure. Tunnels can be added even while the connection is open. For more information how to create a new local tunnel, see “*Local Tunneling*” on page 18.

Click **Edit** to edit a previously defined tunnel. You need to restart your connection to the remote host for the changes to take effect. For more information how to edit a local tunnel, see “*Local Tunneling*” on page 18.

Click **Remove** to delete the currently selected tunnel. You need to restart your connection to the remote host for the changes to take effect.

Remote Tunneling

In the *Remote Tunneling* page, you can configure secure remote tunnels. The page displays the remote TCP/IP ports, which have been forwarded.



Name	Displays the name of the tunnel.
Listen Port	Displays the remote port that the tunnel listens for TCP data requests on the remote host.
Dest Host	Displays the destination host where the connection is forwarded.
Dest Port	Displays the destination port where the connection is forwarded on the destination host.
Type	Displays the tunnel type, either TCP or FTP.

Click **Add** to define a new TCP/IP or FTP connection which you want to secure. Tunnels can be added even while the connection is open. For more information how to create a new local tunnel, see “*Remote Tunneling*” on page 25.

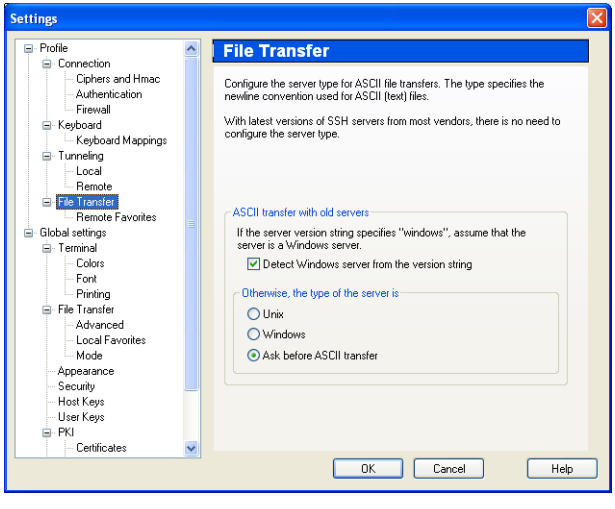
Click **Edit** to edit a previously defined tunnel. You need to restart your connection to the remote host for the changes to take effect. For more information how to edit a local tunnel, see “*Remote Tunneling*” on page 25.

Click **Remove** to delete the currently selected tunnel. You need to restart your connection to the remote host for the changes to take effect.

File Transfer

In the *File Transfer* page, you can configure the profile-specific file transfer settings. The profile-specific file transfer settings affect how ASCII (plain text) files are handled. For information about other file transfer settings, see “*File Transfer*” on page 73.

Some SSH servers give information to SSH clients about their new-line convention. If F-Secure SSH Client receives this information, plain text files are handled automatically and settings from this page are not used.



Detect Windows server from the version string	Detect Windows servers automatically and use the correct setting for them. If the SSH server has ”windows” in its version information string, F-Secure SSH Client detects it as a Windows server.
Otherwise, the type of the server is	Specify the server type if the automatic detection does not detect a Windows server or if the automatic detection is turned off.

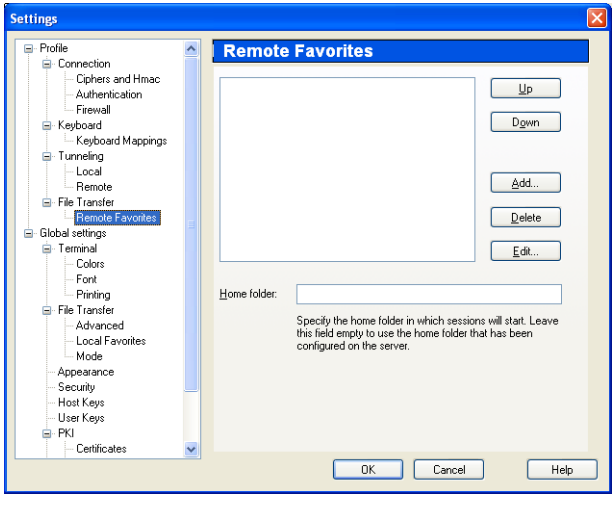
Select *Unix* to use Unix-compatible line breaks.

Select *Windows* to use Windows-compatible line breaks.

Select *Ask before ASCII transfer* to decide the server type before each ASCII file transfer.

Remote Favorites

In the *Remote Favorites* page, you can add commonly used remote directories to the list of favorite folders. Favorite folders appear in the favorite folder pull-down menu in the File Transfer window.



Remote Favorites

Click **Add** to add a new folder to the list of favorite remote folders. Enter a name and the path of the folder. The name specifies how the folder appears in the favorite folders list.

Click **Delete** to remove the selected folder from the list.

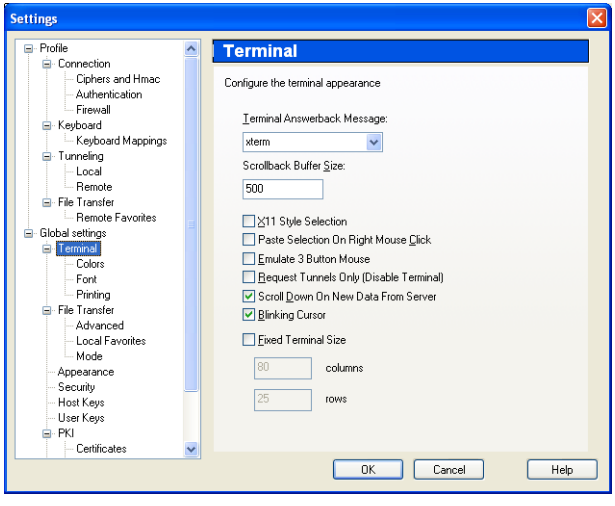
	Click **Edit** to to edit the name and the path of the selected folder in the list. Use **Up** and **Down** to change the order of favorites as they appear in the drop-down menu.
Home folder	Specify the folder where the session starts. Leave the field empty if you want to use the server-configured home folder.

5.3 Global Settings

The global settings affect all profiles, not just the currently open or selected profile.

Terminal

In *Terminal* settings pages, you can choose the type of terminal you want to emulate, colors, fonts, keyboard and printing settings.



Terminal answerback message	Choose the terminal you want to emulate. The available options are xterm, xterm-color, and vt100, 102, 220 and 320. The vt100 emulation lets you use standard vt100 functions (such as remote printing) in an encrypted format.
Scrollback Buffer Size	Set the terminal scrollback buffer size in lines. The scrollback buffer defines how many lines you can scroll back the terminal display to view previous terminal output. The valid range is between 1 and 30000 lines and the default value is 500 lines.

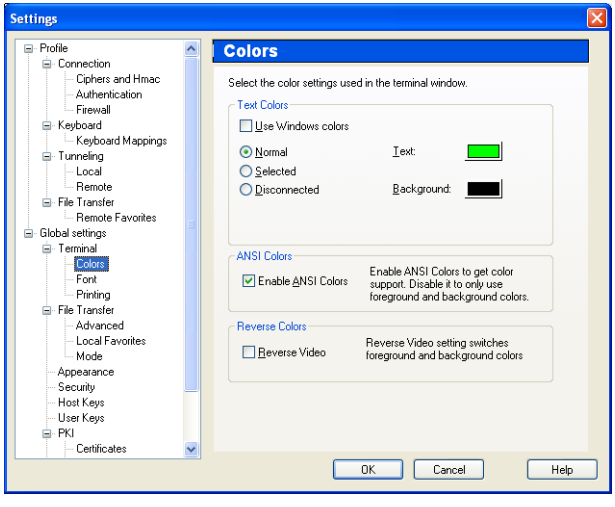
X11 style selection	Copy all selected text in the terminal to the clipboard automatically.
Paste selection on right mouse click	Paste the text in the clipboard by clicking the right mouse button.
Emulate 3 button mouse	Emulate a three-button mouse with a two-button mouse. Press and hold the right button and clicking the left button to emulate the third button.

The third button can be used to paste a selection in the terminal window.

Request Tunnels only (Disable Terminal)	Disable the terminal and use only tunneling.
Scroll down on new data from server	Scroll the terminal window down when the server sends new data to the terminal window while you are scrolling the scrollback buffer.
Blinking Cursor	Use a blinking cursor in the terminal window. Clear the check box to use a solid cursor.
Fixed terminal size	Use a fixed size terminal window which cannot be resized. Set the amount of *rows* and *columns* to set the size of the terminal window.

Colors

In the *Colors* page, you can select the colors used in the Terminal window.



Text Colors

Use Windows colors	Use your default Windows colors for the terminal. Clear the check box to choose colors for the background and text. *Normal* - Set colors you want to use in the normal terminal environment. *Selected* - Set colors for the selected text. *Disconnected* - Set colors which are displayed when the terminal window is open but the connection is disconnected.

ANSI Colors

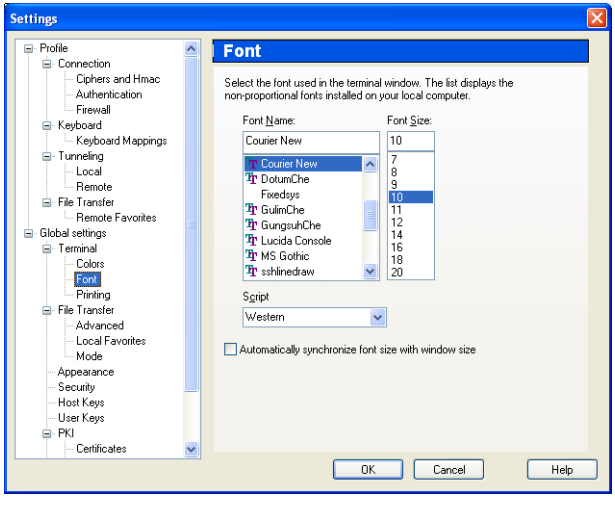
Enable ANSI Colors	Allow ANSI colors to be used in the terminal window.

Reverse Colors

Reverse Video	Reverse foreground and background colors to improve visibility.

Font

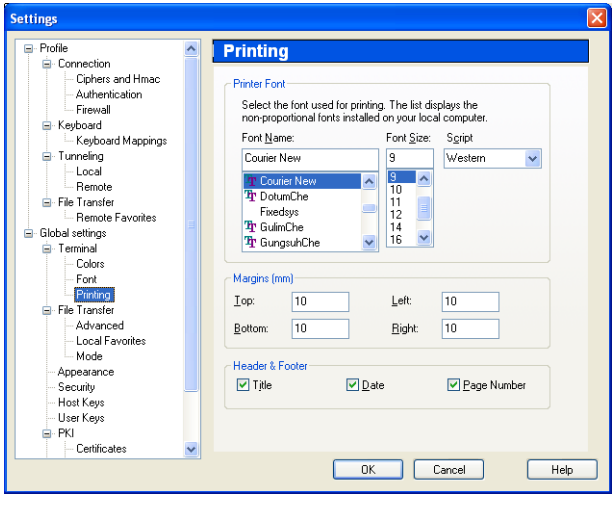
In the *Font* page, you can select the font used in the Terminal window.



Font Name	Specify the font you want to use. The list displays all currently available non-proportional fonts installed on your computer.
Font Size	Specify the font size.
Script	Select the character set you want to use.
Automatically synchronize font size with window size	Change the font size when you resize the terminal window.

Printing

In the *Printing* page, you can select the font and margins for printing.



Printer Font

Font Name	Specify the font to be used. The list displays all currently available fonts installed on your computer.
Font Size	Specify the font size.
Script	Select the character set you want to use.

Margins (mm)

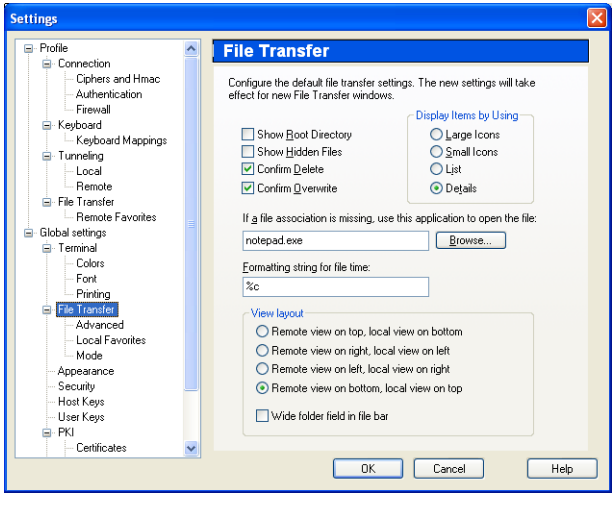
Top, Bottom, Left, Right	Set the top, bottom, left and right margin for printing. Units are millimeters from the edge of the paper.

Header & Footer

Title	Print the title of the terminal window in the header of each page of the printout.
Date	Print the current date in the header of each page of the printout.
Page Number	Print the page number in the footer of each page.

File Transfer

In the *File Transfer* settings pages, you can specify the settings for the File Transfer window.

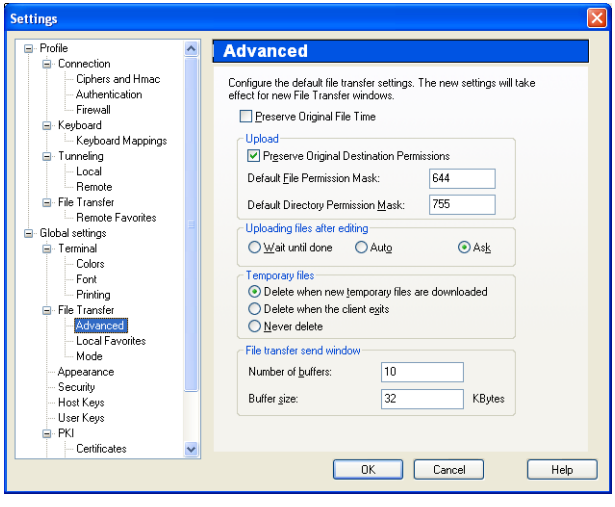


Show Root Directory	Show the root directory as the top directory in the directory tree. Otherwise, the home directory is shown as the top directory in the tree.
Show Hidden Files	Display hidden files.
Confirm Delete	Ask for the confirmation before deleting files.
Confirm Overwrite	Ask for the confirmation before overwriting files.

Display Items by Using	Display files and folders as *Large icons*, *Small icons*, *List* or *Details*.
If a file association is missing, use this application to open the file	Select an application which you want to use for viewing files that are not associated with any program. Click **Browse** to browse for the application.
Formatting string for the file time	Specify how the time and date stamps of the files are displayed in the File Transfer window. For information which combinations of variables you can use in the formatting string, see "*Time and Date Stamp Variables*" on page 110. By default, F-Secure SSH Client displays the date and time in the format that is defined in the Windows country settings (locale).
View layout	Select how the File Transfer window positions the local and remote view panes.
Wide folder field in the file bar	Hide Refresh (), New Folder () and Delete () icons from the file bar to display a wider folder field in the file bar. For more information, see "*File Bar*" on page 106.

Advanced

In the *Advanced* page, you can configure the file transfer settings.



Preserve Original File Time	Preserve the original file time stamp and do not change it to the current time when the file is transferred.

Upload

Preserve Original Destination Permissions	Do not change the file permissions when you upload the file. The transferred file has the same file permissions as the original file.
Default File Permission Mask	Specify the octal UNIX file permission mask which is used as the default value for uploaded files.
Default Directory Permission Mask	Specify the octal UNIX file permission mask which is used as the default value for uploaded directories. For more information about the octan UNIX file permission mask, see the documentation of the UNIX chmod command.

Uploading Files After Editing

Wait until done	Upload the remotely edited file back to the remote server as soon as you save changes and close the editor. The SFTP client cannot be used while you are editing the file and this setting is selected.
Auto	Upload the remotely edited file back to the remote server as soon as you save changes and close the editor. The SFTP client is fully operational while you are editing the file and this setting is selected.
Ask	Prompt before uploading the remotely edited file back to the remote server after you save changes and close the editor.

Temporary files

When you remotely view or edit a file, or drag-and-drop a remote file, it is downloaded and saved locally as a temporary file.

Delete when new temporary files are downloaded	Keep only the last remotely edited file in the local system. When you remotely edit a new file, it replaces and deletes the previously opened temporary file.
Delete when the client exits	Keep all remotely edited files in the local system. All temporary files are deleted when you close the client.
Never delete	Keep all remotely edited files in the local system and do not delete temporary files automatically.

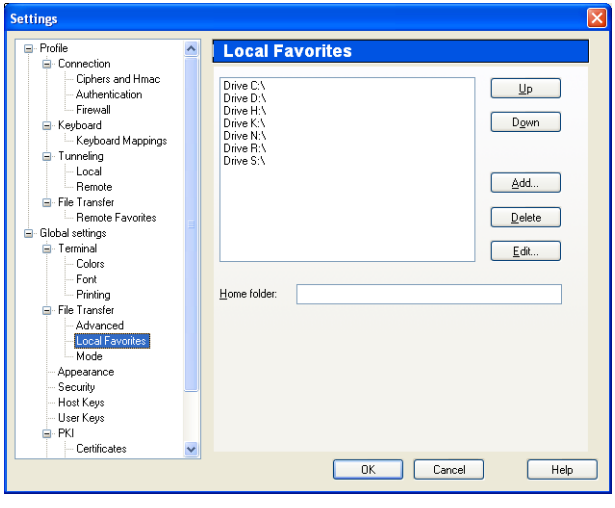
File transfer send window

Number of buffers	Specify the number of buffers used in file transfer. The default value is 10.
Buffer size	Specify the buffer size in kilobytes. The default value is 32 kilobytes.

You can change the number of buffers and the buffer size to optimize your SFTP file transfers. The optimal settings are different for different network connections.

Local Favorites

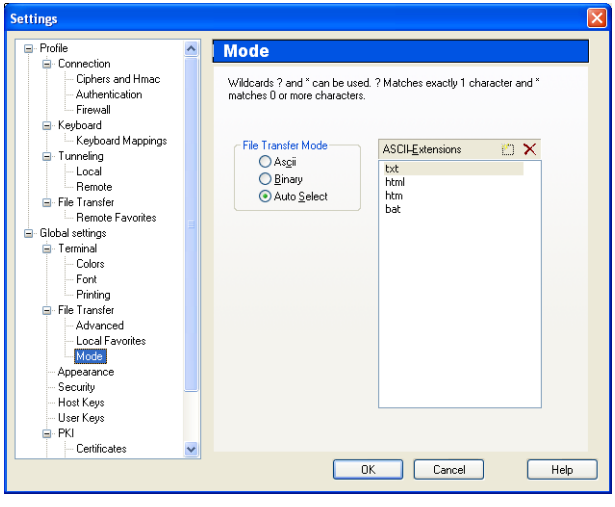
In the *Local Favorites* page, you can add commonly used local directories to the list of favorite folders. Favorite folders appear in the favorite folder pull-down menu in the File Transfer window.



Local Favorites	Click **Add** to add a new folder to the list of favorite local folders. Enter a name and the path of the folder. The name specifies how the folder appears in the favorite folders list. Click **Delete** to remove the selected folder from the list. Click **Edit** to to edit the name and the path of the selected folder in the list. Use **Up** and **Down** to change the order of favorites as they appear in the drop-down menu.
Home folder	Specify the folder that is initially displayed in the local view pane of the File Transfer window.

Mode

In the *Mode* page, you can specify the file transfer mode.

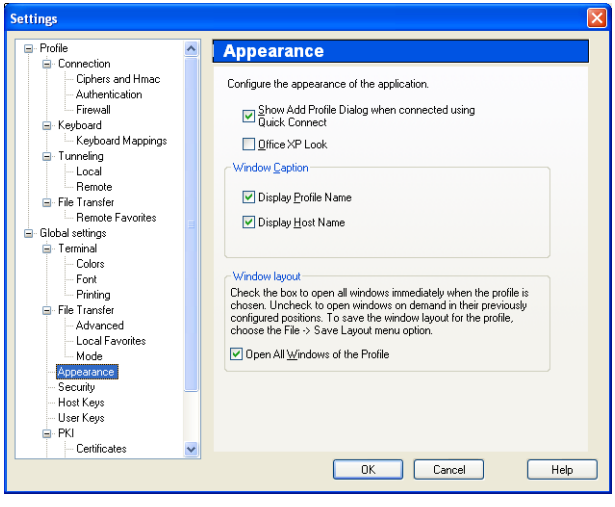


File Transfer Mode

ASCII	Set the file transfer mode to ASCII.
Binary	Set the file transfer mode to binary.
Auto Select	Set all files to be transferred in binary mode, except files which are specified in the ASCII Extensions list.
ASCII Extensions	List all the file extensions you wish to be transferred in ASCII mode. You can use wildcards * and ?.

Appearance

In the *Appearance* page, you can select what information is displayed in the Terminal window.



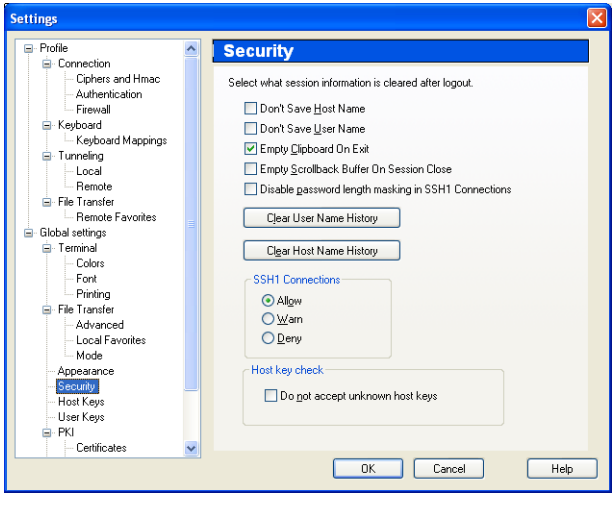
Show Add Profile Dialog when connected using Quick Connect	Display the *Add Profile* dialog when you connect to a new host using *Quick Connect*. You can quickly create a new profile for the new host and connection with the *Add Profile* dialog box.
Office XP Look	Match the visual style of F-Secure SSH Client to Microsoft Office XP.
Window Caption	
Display Profile Name	Display the name of the current profile in the title bar.
Display Host Name	Display the name of the connected host in the title bar.

Window Layout

Open All Windows of the Profile	Open all windows associated with the profile when you create the connection. You can create a connection with several windows open at the same time. For more information, see "*Using Profiles*" on page 14.

Security

In the *Security* page, you can remove your previous connection data and deny the use of unknown host keys.



Don't Save Host Name	Do not save the host names on the Quick Connect drop-down list for future sessions.
Don't Save User Name	Do not save the user names on the Quick Connect drop-down list 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 the remote server.
Disable password length masking in SSH1 connections	Do not use password length masking when logging in using the SSH1 protocol. By default, F-Secure SSH Client masks the password length in SSH1 connections by sending a random number of `ssh ignore` strings to the server before sending the password. Some operating systems cannot accept this. You should disable the password length masking if you experience problems with it.

Click **Clear User name history** to delete recent user name entries from the Logon Information dialog box.

Click **Clear Host name history** to delete recent host name entries from the Logon Information dialog box.

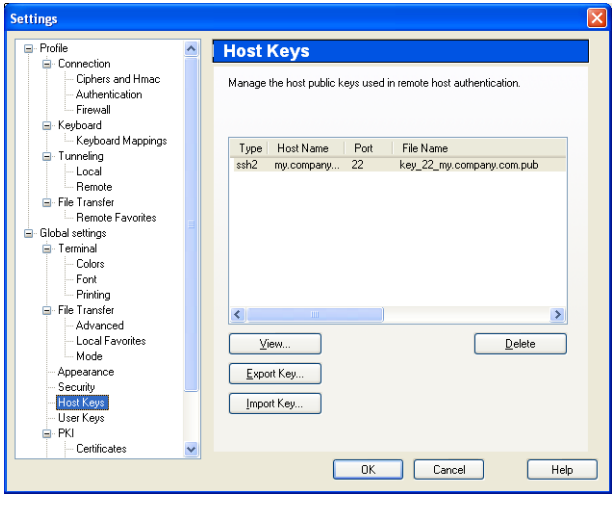
SSH1 Connections	Allow or deny SSH1 connections, or have F-Secure SSH Client issue a warning you when open an SSH1 connection.

If you are trying to connect to an incompatible SSH2 server and the connection fails, change the SSH1 Connections setting to Deny and try again. For more detailed information, see "Ssh1compatibility" on page 118.

Do not accept unknown host keys	Allow connections only to hosts whose host keys you have.

Host Keys

In the *Host Keys* page, you can view, import, export, and delete host keys. For more information, see "*Remote Host Authentication*" on page 93.



Type	Displays the host key type, either SSH1 or SSH2.
Host Name	Displays the host name of the host key.
Port	Displays the port that is associated with the host key.
File Name	Displays the file name of the host key file.

Click **View** to view the selected host key. You can copy the host key to the clipboard from the view window.

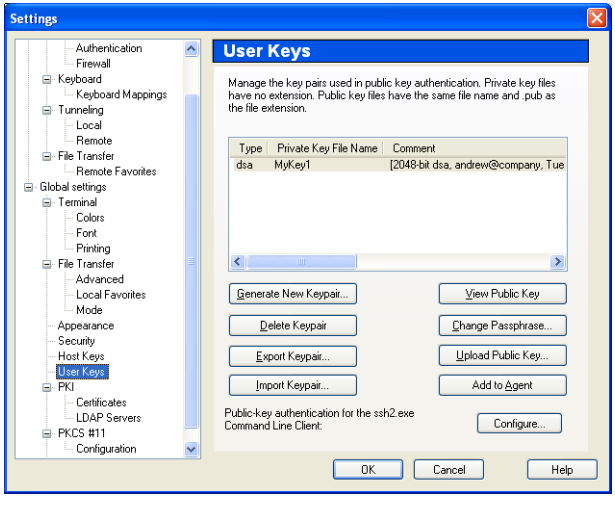
Click **Export Key** to export the selected key from F-Secure SSH Client to a host key file.

Click **Import Key** to import a public host key file to F-Secure SSH Client.

Click **Delete** to delete the selected host key from F-Secure SSH Client.

User Keys

In the User Keys page, you can 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.



Type	Displays the user key type, either DSA or RSA.
Private Key File Name	Displays the file name of the private keys.
Comment	Displays the comment you may have added to help you to recognize the key.

Click **Generate New Keypair** to generate a new public and private key. For more information, see “*Generating a New Keypair*” on page 40.

Click **Delete Keypair** to delete the selected user key pair.

Click **Export Keypair** to export the selected user key pair to files.

Click **Import Keypair** to import a keypair from a hard drive or a disk.

Click **View Public Key** to view the selected public key in a window.

Click **Change Passphrase** to change the passphrase for the highlighted key.

Click **Upload Public Key** to upload the public key to the remote host. For more information, see "*Generating a New Keypair*" on page 40.

Click **Add to Agent** to add the selected user key to F-Secure SSH Authentication Agent. For more information about F-Secure SSH Authentication Agent, consult the F-Secure SSH Authentication Agent User's Guide.

Click **Configure** to write a new identification file for the command line SSH2 client. The identification file lists all the keys that the command line client offers to the server during the public key authentication. You can edit the file manually afterwards. Note that creating a new identification file overwrites the existing file.

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.

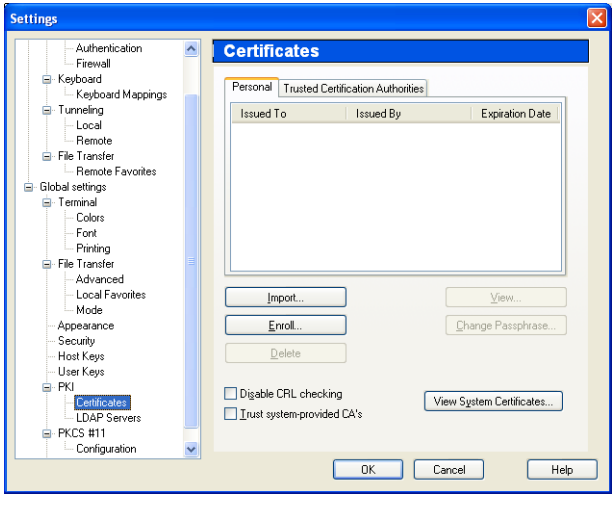
PKI

A Public Key Infrastructure (PKI) is a system that helps to establish secure communications by using digital certificates.

You have to generate the digital certificate with a Certification Authority (CA) software.

Certificates

In the Certificates page, you can import, expert and enroll personal and trusted CA certificates.



Issued To	Displays whom the certificate has been issued to.
Issued By	Displays who has issued the certificate.
Expiration Date	Displays the date when the certificate expires.

Click **Import** to import a certificate created with a Certificate Authority (CA) software. You can browse for the saved certificate file.

Click **Enroll** to 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. For more information, see "*Certificate Enrollment Wizard*" on page 45.

Click **Delete** to remove the selected certificate.

Click **View** to display the contents of the selected certificate.

Click **Change Passphrase** to 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.
Trust system-provided CA's	Trust Certification Authorities which are listed in the Windows certificate storage.

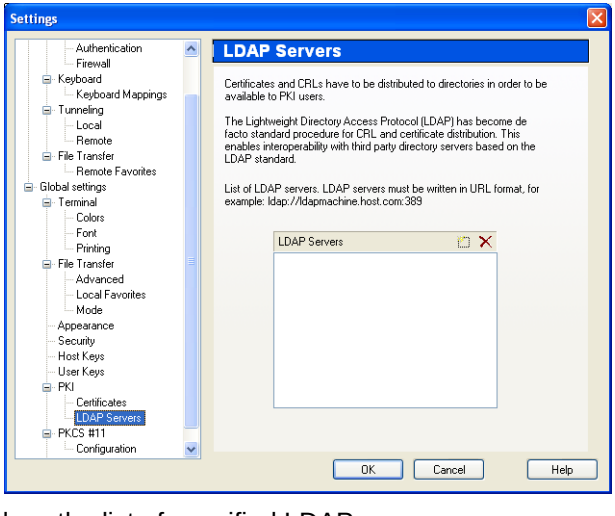
Click **View System Certificates** to open Windows certificate storage for viewing.

LDAP Servers

In *LDAP Servers* page, you can edit LDAP servers you use.

In order to use the PKI certificate, certificates and Certificate Revocation Lists (CRLs) have to be distributed to directories where other PKI users can retrieve them.

The Lightweight Directory Access Protocol (LDAP) is a standard protocol that can be used to distribute certificates and CRLs.



The *LDAP Servers* list displays the list of specified LDAP servers.

Click the New ( ) button to add a new LDAP server to the list. Enter the LDAP server in the URL format.

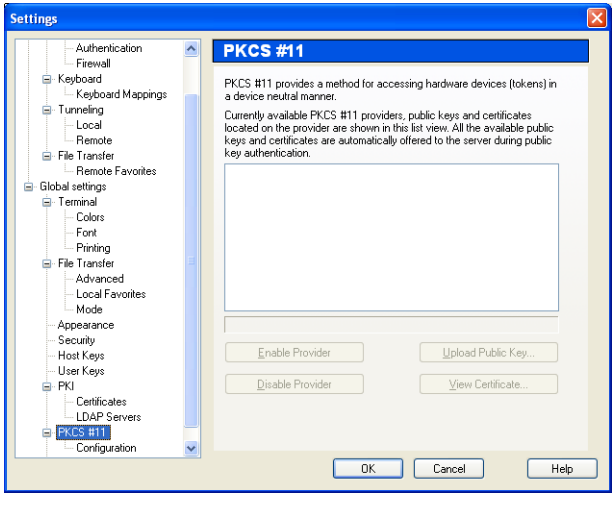
Click the Delete ( ) button to remove the selected LDAP server from the list.

PKCS #11

In the *PKCS #11* page, you can select which hardware devices you want to use during the authentication.

PKCS#11 is a standard that defines the interface between applications and devices that store encryption keys.

The PKCS #11 support provides a hardware device (token) access method. 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 PKCS #11 settings in F-Secure SSH Client.



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

Click **Enable Provider** to allow the use of the selected provider.

Click **Disable Provider** to deny the use of the selected provider.

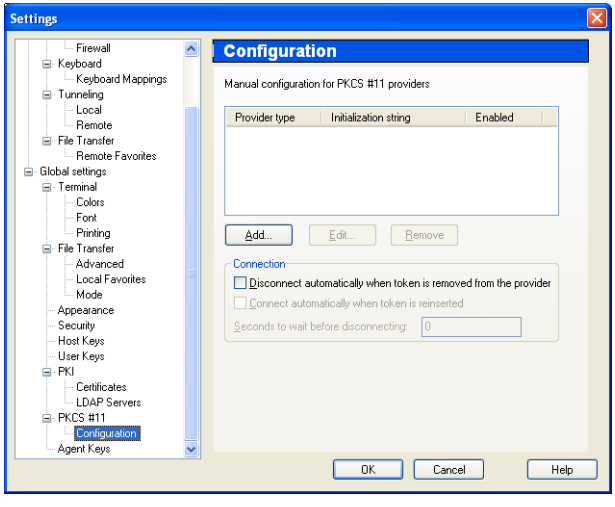
Click **Upload Public Key** to upload the public key from the token to the SSH server. You can then use the hardware token for your personal authentication. You have to be connected to the server to upload the public key.

Click **View Certificate** to display the contents of the selected certificate.

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

Configuration

In the *Configuration* page, you can configure PKCS #11 providers manually.



Provider type	Displays the type of the provider.
Initialization string	Displays the string of characters used for initialization.
Enabled	Displays whether the use of the provider is allowed or not. Click **Edit** to change the provider status.

Click **Add** to add a new PKCS #11 provider.

Click **Edit** to change the details of the PKCS #11 provider.

Click **Remove** to delete the PKCS #11 provider entry.

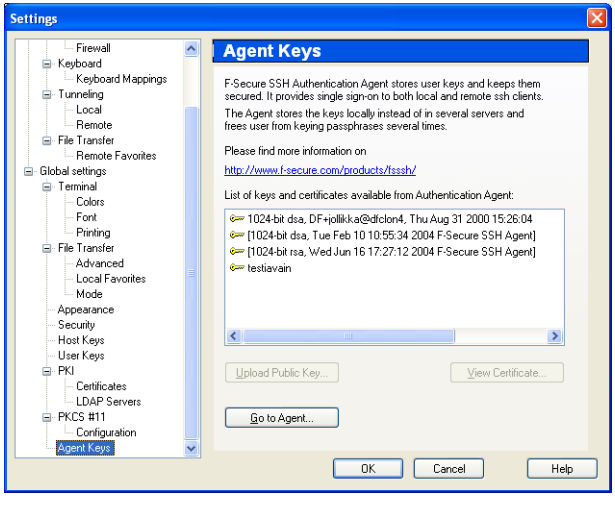
Disconnect automatically when token is removed from the provider	Keep the connection active only when the token is present.
Connect automatically when token is reinserted	Automatically establish the connection again when the token is reinserted.
Seconds to wait before disconnecting	Set the time after which the connection is disconnected when a token is removed.

Agent Keys

In the *Agent Keys* page, you can configure how F-Secure SSH Client operates with F-Secure SSH Authentication Agent.

F-Secure SSH Authentication Agent stores user keys and keeps them secured. It provides a single sign-on to both local and remote SSH clients.

F-Secure SSH Authentication Agent stores the keys locally instead of in several servers and frees the user from keying passphrases several times. For more information about F-Secure SSH Authentication Agent, consult the F-Secure SSH Authentication Agent User's Guide.



The Agent Keys list displays keys and certificates available from F-Secure SSH Authentication Agent.

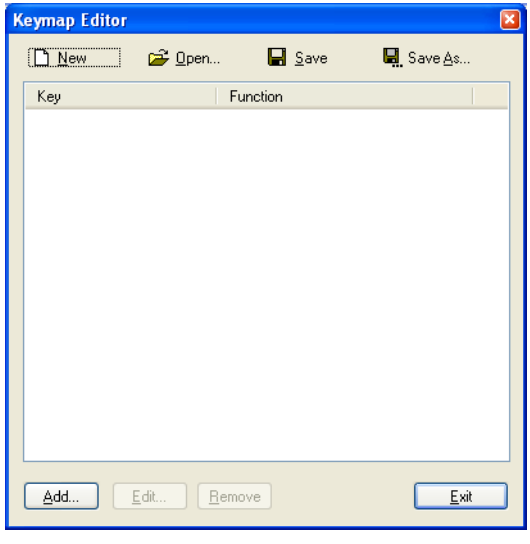
Click **Upload Public Key** to upload the public key to the remote host.

Click **Go to Agent** to open F-Secure SSH Authentication Agent user interface.

Click **View Certificate** to display information about the selected certificate.

5.4 Keymap Editor

The keymap editor allows you to define additional key mappings, open saved keymap files and create new key map files. To open the keymap editor, go to *Settings* > *Profile* > *Keyboard* > *Keyboard Mappings* and click **Edit additional map file...**.



Click **New** to start a new keymap file.

Click **Open** to open a keymap file.

Click **Save** to save the current keymap file. Click **Save As...** to save the current keymap file with a different name.

To add a new key to the keymap file, follow these instructions:

1. Click **Add...**.
2. Select a shortcut key you want to map. You can use key combinations by holding down SHIFT, CTRL and ALT keys.
3. Select the function you want the key to perform from the drop-down menu.
4. If the function requires arguments, select them in the *Agruments* field.

Click **Edit...** to edit selected key in the list.

Click **Remove** to remove the selected key from the list.

Click **Exit** to exit the keymap editor.

6. Cryptographic Methods

6.1 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.

6.2 Remote Host Authentication

The SSH protocol guarantees authentication on both the server side and the client side, and it guarantees the secrecy and integrity of transmitted data.

When you connect to an SSH server, the server sends its public host key and a public ‘server key’ that changes each hour. The host key is used to bind the connection to a specified SSH server. Recorded traffic cannot be decrypted even if the host key is compromised, as the server key is changed every hour.

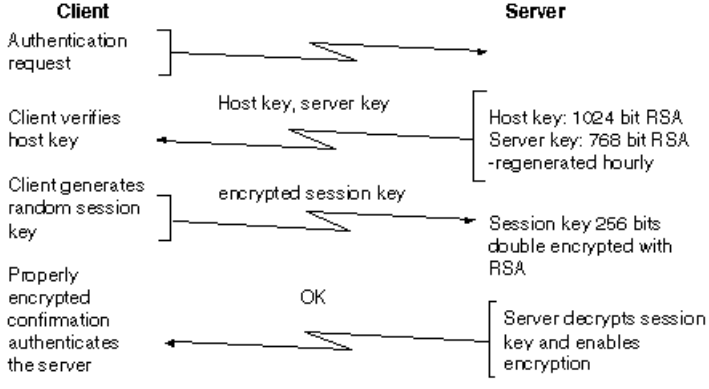


Figure 1: Host Authentication

1. During the authentication, F-Secure Anti-Virus compares the host key it receives from the server against its own database of known host keys.

   By default, F-Secure Anti-Virus accepts the key of the host where it connects and stores it in the database for future reference. However, F-Secure Anti-Virus can be configured to refuse connections to any hosts which send an unknown key.

2. The client generates a session key, a 256-bit random number, using a cryptographically strong random number generator. The client then encrypts the session key with an encryption algorithm that the server supports, using both the host key and the server key. The client then sends the encrypted session key to the server.

3. The server decrypts the session key that is receives from the client. Both the client and the server start using this session key, and the connection is encrypted.

4. The server sends an encrypted confirmation to the client. When the client receives the confirmation, it knows that the server has the proper private keys to decrypt the session key. The client has authenticated the server and transport-level encryption and integrity protection is in effect.

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.

6.3 Cryptographic Library

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

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

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

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

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

Appendix A. User Interface

A-1 Menus and Toolbars

Menus

File Menu

Item	Function
Save Layout	Save the current window layout.
Save Settings	Save current settings to the current profile, including which windows are open. If you do not have any profile open, the settings are saved to the Default Profile.
Quick Connect...	Open a connection to the host specified in the currently active profile, or the *Quick Connection* dialog box if the currently active profile does not have any specified host. For more information, see “*Connecting to Remote Hosts*” on page 11.
Profiles	Open a list of profiles where you can add, edit, import and open profiles. For more information, see “*Using Profiles*” on page 14.
Print…	Open the *Print* dialog box where you can print the terminal scrollback buffer. The *Print...* menu item is available in the Terminal window only.

Item	Function
Print Setup…	Open the *Print Setup* dialog box where you can select the printer you want to use, paper size, paper source and orientation, and printer properties. The *Print Setup...* menu item is available in the Terminal window only.
Print Preview...	Display what the printout looks like. You can change the formatting of the printout by adjusting the printing settings in the *Print* or *Print Setup* dialog boxes. The *Print Preview...* menu item is available in the Terminal window only.
Page Setup...	Open the *Page Setup* dialog box where you can select the font you want to use for printing, page margins and header and footer information. For more information, see “*Printing*” on page 72. The *Page Setup...* menu item is available in the Terminal window only.
Log Session...	Store all information of the terminal window scrollback buffer to a file. The *Log Session...* menu item is available in the Terminal window only.
Raw Log Session...	Store all information of the terminal window scrollback buffer to a file, including escape sequences. The *Raw Log Session...* menu item is available in the Terminal window only.
Connect...	Open a connection to the host specified in the currently active profile, or the *Quick Connection* dialog box if the currently active profile does not have any specified host.
Disconnect	Disconnect the current connection.
Exit	Close the terminal and exits F-Secure SSH Client.

Edit Menu

Item	Function
Copy	Copy the current selection to the Windows clipboard.

Item	Function
Paste	Paste the Windows clipboard.
Paste Selection	Paste the currently selected text at the prompt. The *Paste Selection* menu item is available in the Terminal window only.
Select All	Select all text in the terminal window and the scrollback buffer, all files and folders in the current File Transfer window or all tunnels in the Tunnel View window.
Select Screen	Select all the visible text in the terminal window. The *Select Screen* menu item is available in the Terminal window only.
Select None	Clear all selections. The *Select None* menu item is available in the Terminal window only.
Find...	Open the *Find* dialog box where you can search for text in the scrollback buffer. The *Find...* menu item is available in the Terminal window only.
Settings...	Open the *Settings* dialog box where you can adjust all settings. For more information, see “*Configuring F-Secure SSH Client*” on page 49.

View Menu

Item	Function
Toolbar	Display or hide the toolbar. For more information, see “*Toolbar*” on page 103.
Status Bar	Display or hide the status bar.
Profiles Bar	Display or hide the profiles bar. For more information, see “*Profiles Bar*” on page 107.
File Bar	Display or hide the file bar. For more information, see “*File Bar*” on page 106. The *File Bar* menu item is available in the File Transfer window only.

Item	Function
Reset Toolbars	Reset all toolbars to their default positions.
Reset Terminal	Clear the visible terminal and the scrollback buffer. The *Reset Terminal* menu item is available in the Terminal window only.
Local View	Display or hide the Local View. The Local View displays the contents of the local computer. The *Local View* menu item is available in the File Transfer window only.
Transfer View	Display or hide the Transfer View pane at the bottom of the File Transfer window. The *Transfer View* menu item is available in the File Transfer window only.
Large Icons	Display directory contents as large icons. The *Large Icons* menu item is available in the File Transfer window only.
Small Icons	Display directory contents as small icons. The *Small Icons* menu item is available in the File Transfer window only.
List	Display directory contents as a list. The *Arrange Icons* menu item is available in the File Transfer window only.
Details	Display directory contents as a detailed list. The *Arrange Icons* menu item is available in the File Transfer window only.
Arrange Icons	Arrange icons by name, type, size or date. The *Arrange Icons* menu item is available in the File Transfer window only.
Show Root Folder	Display the directory tree with the root folder as the first folder of the tree. If the root folder is not shown, the directory tree starts from your home directory. The *Show Root Folder* menu item is available in the File Transfer window only.

Item	Function
Show Hidden Files	Display hidden files. The *Show Hidden Files* menu item is available in the File Transfer window only.
Refresh	Refresh the contents of the currently active directory. The *Refresh* menu item is available in the File Transfer window only.

Window Menu

Item	Function
New Terminal	Open a new Terminal window. If you have an open connection, the new window is started with an open connection as well.
New File Transfer	Open a new File Transfer window. If you have an open connection, the new window is started with an open connection as well.
New Tunnel View	Open a new Tunnel View window. If you have an open connection, the new window is started with an open connection as well.
New Terminal in Current Directory	Open a new Terminal window that starts in the same directory as the current Terminal or File Transfer window.
New File Transfer in Current DIrectory	Open a new File Transfer window that starts in the same directory as the current Terminal or File Transfer window.
New Explorer	Open a new Windows Explorer window. The *New Explorer* menu item is available in the File Transfer window only.
Close	Close the currently active window. If you close the last window for a connection, you are disconnected from the server.
Close All Others	Close all windows for the current connection except the currently active window.

Help Menu

Help menu option	Function
Contents	Open the online help.
F-Secure on the Web	Connect to the F-Secure web pages in the Internet.
Troubleshooting...	Show data the program has gathered during its operation. This data can be sent to F-Secure technical support in case of problems with the software.
Debugging...	Open the Debugging dialog where you can select to display debugging information in the Terminal window or select to log debugging data in a separate log file.
About	Display version and copyright information.

Operation Menu

The *Operation* menu is available in the File Transfer window only.

Item	Function
View	Display the currently selected file. You cannot edit the file you view. You can specify which program you want to use to view files in the settings. For more information, see “*File Transfer*” on page 65.
Open	Open the currently selected file for editing. You cannot open a file that does not have a software associated with it.
Edit	Open a file for text editing.
Upload	Upload selected files to the remote host.
Download	Download selected files from the remote host.
Upload Dialog...	Open a dialog where you can select the file that you want to upload to the remote computer.

Item	Function
Download Dialog...	Open a dialog where you can select the folder where you want to dowload the currently selected file.
Cancel Transfer	Cancel the transfer of the selected files in the Transfer View pane.
Up	Go to the parent directory of the directory you are currently in, if you have the access rights.
Root	Go to the root directory of the file system, if you have the access rights.
Home	Go to your assigned home directory on the system.
Go to Folder...	Open a dialog box where you can select the folder you want to go to on the remote host.
New Folder	Create a new folder.
Delete	Delete the selected file or folder.
Rename	Rename the currently selected file or folder.
Properties	Display and change the permissions of the selected remote file. You can select multiple files and set their permissions at once. Select the check box to set the permission on all selected files. Clear the check box to remove the permission on all selected files. Leave the check box gray to leave the permission as it was on each selected file.
File Transfer Mode	Set the file transfer mode. *Auto Select* sets all files to be transferred in binary mode, except files which are specified in the ASCII Extensions list in the settings.
Favorite Remote Folders	Edit the list of favorite remote folders.
Favorite Local Folders	Edit the list of favorite local folders.

Tunnel Menu

The *Tunnel* menu is available in the Tunnel View window only.

Tunnel menu option	Function
New Local Tunnel	Open the *New Local Forwarding* dialog box where you can create a new local tunnel.
New Remote Tunnel	Open the *New Remote Forwarding* dialog box where you can create a new remote tunnel.

Toolbars

Toolbar

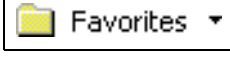
Icon	Function	Description
Common Icons		
	Save	Save current settings to the current profile, including which windows are open. If you do not have any profile open, the settings are saved to the Default Profile.
	Print	Open the *Print* dialog box where you can print the terminal scrollback buffer.
	Print Preview	Display what the printout looks like. You can change the formatting of the printout by adjusting the printing settings in the *Print* dialog box.
	Connect	Open a connection to the host specified in the currently active profile, or the *Quick Connection* dialog box if the currently active profile does not have any specified host.
	Disconnect	Disconnect the current connection.
	Copy	Copy the current selection to the Windows clipboard.

Icon	Function	Description
	Paste	Paste the Windows clipboard.
	Paste Selection	Paste the currently selected text at the prompt. The **Paste Selection** button is available in the Terminal window only.
	Find	Open the *Find* dialog box where you can search for text in the scrollback buffer. The **Find** button is available in the Terminal window only.
	New Terminal Window	Open a new Terminal window. If you have an open connection, the new window is started with an open connection as well.
	New File Transfer Window	Open a new File Transfer window. If you have an open connection, the new window is started with an open connection as well.
	New Tunnel View Window	Open a new Tunnel View window. If you have an open connection, the new window is started with an open connection as well.
	Settings	Open the *Settings* dialog box where you can adjust all settings.
	Online Help	Open the online help.
	Help	Change the cursor to the help cursor which lets you click on an item in the user interface to see the help topic associated with it.
File Transfer Icons		
	Download Dialog	Open a dialog where you can select the folder where you want to dowload the currently selected file.
	Upload Dialog	Open a dialog where you can select the file that you want to upload to the remote computer.
	Toggle Transfer View	Display or hide the Transfer View pane at the bottom of the File Transfer window.

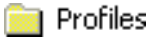
Icon	Function	Description
	Large Icons	Display directory contents as large icons.
	Small Icons	Display directory contents as small icons.
	List	Display directory contents as a list.
	Details	Display directory contents as a detailed list.
	Ascii	Set the file transfer mode to ASCII.
	Binary	Set the file transfer mode to binary.
	Auto Select	Set all files to be transferred in binary mode, except files which are specified in the ASCII Extensions list in the settings.
	Cancel Transfer	Stop the current transfer.
Tunnel View Icons		
	Refresh	Refresh the current view to show you the latest status of the tunnels you have created.
	New Local Forwarding	Open the *New Local Forwarding* dialog box where you can create a new local tunnel.
	New Remote Forwarding	Open the *New Remote Forwarding* dialog box where you can create a new remote tunnel.

File Bar

The File bar is available in the File Transfer window only.

Icon	Function	Description
	Show/Hide Folders	Display or hide the folder pane.
	Go To Parent Folder	Go to the parent directory of the directory you are currently in, if you have the access rights.
	Go To Root Folder	Go to the root directory of the file system, if you have the access rights.
	Go To Home Directory	Go to your assigned home directory on the system.
	Refresh	Refresh the current view to show the contents of the directory you are in.
	New Folder	Create a new folder.
	Delete	Delete the selected file or folder.
	Download	Download selected files from the remote host.
	Upload	Upload selected files to the remote host.
	Favorites	Display the list of favorite folders.

Profiles Bar

Icon	Description
	Open a connection to the host specified in the currently active profile, or the *Quick Connection* dialog box if the currently active profile does not have any specified host.
	Open a list of profiles where you can add, edit, import and open profiles.

A-2 Working with Text in the Terminal Window

Selecting Text

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.

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

To search for text in the scrollback buffer, access the *Find* dialog box:

- 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

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.

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 Text

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.

Appendix B. Time and Date Stamp Variables

B-1 Editing Time and Date Stamp

You can specify how the time and date stamps of the files are displayed in the File Transfer window by editing the date and time stamp formatting string.

By default, F-Secure SSH Client displays the date and time in the format that is defined in the Windows country settings (locale).

To edit the date and time stamp formatting string, open *Settings* > *Global Settings* > *File Transfer* and edit the *Formatting string for the file time* field.

B-2 List of Variables

To change the format of the time and date stamps, replace the default value with a string consisting of some of the following character combinations.

The default value is %c, which means that the date and time will be presented in the format defined in the Windows country settings (locale).

Variable	Description
%a	Abbreviated weekday name
%A	Full weekday name
%b	Abbreviated month name
%B	Full month name
%c	Date and time representation appropriate for locale
%d	Day of month as decimal number (01 - 31)
%H	Hour in 24-hour format (00 - 23)
%I	Hour in 12-hour format (01 - 12)
%j	Day of year as decimal number (001 - 366)
%m	Month as decimal number (01 - 12)
%M	Minute as decimal number (00 - 59)
%p	Current locale's A.M. / P.M. indicator for 12-hour clock
%S	Second as decimal number (00 - 59)
%U	Week of year as decimal number, with Sunday as first day of week (00 - 53)
%w	Weekday as decimal number (0 - 6; Sunday is 0)
%W	Week of year as decimal number, with Monday as first day of week (00 - 53)
%x	Date representation for current locale
%X	Time representation for current locale

Time and Date Stamp Variables

Variable	Description
%y	Year without century, as decimal number (00 - 99)
%Y	Year with century, as decimal number
%z, %Z	Time-zone name or abbreviation; no characters if time zone is unknown
%%	Percent sign

Appendix C. Available Settings in ssh2_config

The *ssh2_config* file is a configuration file for command-line utilities. It is located in the F-Secure SSH subfolder in your application data folder:

C:\Documents and settings\%user%\Application Data\F-Secure SSH\ssh2_config

or in Windows NT:

C:\WINNT\Profiles\%user%\Application Data\F-Secure SSH\ssh2_config

The ssh2_config configuration file is not created during the installation. You can create the file if you need to apply certain non-default settings every time you run a command-line tool.

When you edit the configuration file, use format "keyword arguments". You can enclose arguments in quotes, and use the standard C convention.

Empty lines and lines starting with '#' are ignored as comments.

You can configure these settings from the command line with the ‘-o’ option. For example:

```
ssh2 -o "AllowedAuthentications gssapi-with-mic" -o "macs hmac-sha1" user@host
```

The *ssh2_config* configuration file has the following settings:

AllowedAuthentications

Specifies the allowed authentications methods. You can specify multiple authentication methods and separate them with a comma (,). You can use the following methods with F-Secure SSH Client Windows version:

- password
- publickey
- keyboard-interactive
- gssapi-with-mic
- securid-1@ssh.com
- pam-1@ssh.com

The default argument is `publickey,keyboard-interactive,password`. Authentication methods are tried in the order they are listed. You should place the authentication method that requires the least amount of interaction first on the list, for example `gssapi-with-mic,publickey,password`, as gssapi does not require user input and publickey authentication can be automated with F-Secure SSH Authentication Agent.

AuthenticationSuccessMsg

Specifies whether to display "Authentication successful." after the authentication has completed successfully. This can be used to prevent malicious servers from inquiring additional password or passphrase information from the user. The argument must be `yes` or `no`. The default setting is `yes`.

BatchMode

Specifies whether to query for password or passphrase. If Batchmode is set to `yes`, the password query is disabled. This is useful in scripts and other batch jobs where there is no user to supply the password. If the `StrictHostKeyChecking` parameter is set to `ask`, F-Secure SSH Client answers `no` to all queries. The argument must be `yes` or `no`.

Ciphers

Specifies the ciphers to use for encrypting the session. Currently, `des`, `3des`, `blowfish`, `arcfour`, `aes128`, `aes192`, `aes256` and `cast` are supported. Multiple ciphers can be specified as a comma-separated list. Special values to this option are `any`, `anystd`, `anycipher`, `anystdcipher` and `none`.

`Anystd` allows only standard ciphers, including non-encrypting cipher mode `none` and `anycipher` excludes the `none` cipher mode but allows any other available ciphers. `Anystdcipher` includes only those ciphers mentioned in the IETF-SecSH-draft (excluding 'none').

ClearAllForwardings

Specifies whether to clear all remote and local forwarded ports defined so far. The argument must be `yes` or `no`. Note that scp always automatically clears all forwarded ports.

Compression

Specifies whether to use compression. The argument must be `yes` or `no`.

DefaultDomain

This specifies a default domain for your host. If a host name does not contain any dots ('.'), DefaultDomain is appended to host name for certificate validity checks.

DebugLogFile

All debugging strings are logged to this file.

DontReadStdin

Redirects input from /dev/null, in other words does not read stdin. The argument must be `yes` or `no`.

EscapeChar

Sets the escape character (default: ~). The escape character can also be set on the command line. The argument should be a single character, '^' followed by a letter, or `none` to disable the escape character entirely, which makes the connection transparent for binary data.

FipsMode

Switches the cryptographic library into FIPS mode, which restricts it to FIPS-approved cryptographic algorithms only. Sha1 MAC and des, 3des and aes ciphers are FIPS-approved.

ForcePTTYAllocation

Allocate a tty even if a command is given (i.e. ssh2 user@host command). The argument must be `yes` or `no`.

ForwardAgent

Specifies whether the connection to the authentication agent (if any) should be forwarded to the remote host. The argument must be `yes` or `no`.

ForwardX11

Specifies whether X11 connections are automatically redirected over the secure channel and DISPLAY set. The argument must be `yes` or `no`.

IdentityFile

Specifies the name of the your identification file.

KeepAlive

Specifies whether F-Secure SSH Client should send keepalive messages. If you send keepalive messages you can easily notice when the connection to the remote host is lost. However, sending keepalive messages means that the connection disconnects if the route is down temporarily.

The default argument is `yes`, and the client notices if the connection to the remote host is lost. This is important when using scripts. To disable keepalives, the value should be set to `no` in both the server and the client configuration files.

LocalForward

Specifies a TCP/IP port on the local machine that is forwarded over the secure channel to given host:port from the remote machine. The argument should be enclosed in double-quotes (""). The argument format is `port:remotehost:remoteport`.

MACS

Specifies the MAC (Message Authentication Code) algorithms to use for data integrity verification. Currently, supported MACs in F-Secure SSH Client are `hmac-sha1` and `hmac-md5`. Multiple MACs can be specified as a comma-separated list. Special values to this option are `any`, `anystd`, `anymac`, `anystdmac` and `none`.

`Anystd` allows only standard MACs, including `none` and `anymac` excludes `none` mode but allows any other available MACs. `Anystdmac` includes only those ciphers mentioned in the IETF-SecSH-draft (excluding 'none').

NoDelay

If `yes`, enable socket option TCP_NODELAY. The argument must be `yes` or `no`. The default argument is `no`.

NoOpTimeout

Specifies the interval between keepalive messages to server, in seconds.

NumberofPasswordPrompts

Specifies the number of password prompts before giving up. The argument must be an integer. Note that the server also limits the number of attempts, so setting this value larger than the server does not have any effect. Default value is three (3).

PasswordPrompt

Sets the password prompt that the user sees when connecting to a host. Variables '%U' and '%H' can be used to give the login name and the host.

Port

Specifies the port number to connect on the remote host. The default port number is 22.

QuietMode

Quiet mode. Causes all warnings and diagnostic messages to be suppressed. Only fatal errors are displayed. The argument must be `yes` or `no`.

RandomSeedFile

Specifies the name of your randomseed file.

RekeyIntervalSeconds

Specifies the number of seconds when the key exchange is done again. The default is 3600 seconds. A zero (0) value turns off rekey-requests. This does not prevent the server from requesting rekeys. Some servers may not have correct rekey-capabilities and your connection may be cut off if you connect to some server that is not sshd2.

RemoteForward

Specifies a TCP/IP port on the remote machine that is forwarded over the secure channel to given host:port from the local machine. The argument should be enclosed in double-quotes (""). The argument format is `port:remotehost:remoteport`.

SetRemoteEnv

Allows to set a specific environment variable for the application launched on a server, if server allows this. Format of the argument should be `variable=value`.

SocksServer

Overrides the value of SSH_SOCKS_SERVER. Otherwise, functions completely equivalently.

Ssh1compatibility

If this flag is set to `yes`, F-Secure SSH Client connects to SSH1 servers as well as SSH2 servers. The version string of the client is “SSH-1.99-3.2.3”. When the flag is `no`, F-Secure SSH Client does not connect to SSH1 servers and the version string is “SSH-2.00-3.2.3”

You can use this setting to connect to incompatible SSH2 servers which cannot process the SSH-1.99 version string. By default, the SSH1 compatibility mode is on.

StrictHostKeyChecking

If this flag is set to `yes`, F-Secure SSH Client does not add host keys automatically and refuses to connect to hosts whose host key has changed. This provides maximum protection and it forces you to manually add any new hosts. The argument must be `yes`, `no` or `ask`.

By default, this argument is `ask`, and new hosts will automatically be added to the known host files after you have confirmed that you really want to do that. If this argument is `no`, the new host is automatically added to known hosts. In either case, the host keys of known hosts are verified automatically. If the value is set to `ask`, you can change the key on the disk on the fly.

TryEmptyPassword

If this flag is set to `yes`, F-Secure SSH Client starts the password authentication by trying to enter an empty password. Note that this will count as a login attempt on most systems.

User

Specifies the username that should be used when logging in. This can be useful if you have a different user name in different hosts.

UserConfigDirectory

Specifies the path to the configuration directory where F-Secure SSH Client retrieves user keys, host keys, certificates and other configuration files. The default configuration directory is *F-Secure SSH* subfolder in your Windows application data directory. For example, *C:\Documents and Settings\username\Application Data\F-Secure SSH*

UseSocks5

If the argument is set to `yes`, uses the SOCKS 5 for SocksServer. If the argument is set to `no`, SOCKS 4 is used.

VerboseMode

Causes F-Secure SSH Client to print debugging messages about its progress. This is helpful when debugging connection, authentication, and configuration problems.

Appendix D. Error Codes

D-1 SCP Error Codes

Error code	Description
0	Operation was successful
1	General error in file copy
2	Destination is not directory, but it should be
3	Maximum symlink level exceeded
4	Connecting to host failed.
5	Connection broken
6	File does not exist
7	No permission to access file.
8	General error in sftp protocol
9	File transfer protocol mismatch
10	No file matches a given criteria
65	Host not allowed to connect

SCP Error Codes

Error code	Description
66	General error in ssh protocol
67	Key exchange failed
68	Reserved
69	MAC error
70	Compression error
71	Service not available
72	Protocol version not supported
73	Host key not verifiable
74	Connection failed
75	Disconnected by application
76	Too many connections
77	Authentication cancelled by user
78	No more authentication methods available
79	Invalid user name

D-2 SSH Error Codes

Error code	Description
0	Operation was successful
1	Generic error, usually because invalid command line options or malformed configuration
2	Connecion failed
65	Host not allowed to connect
66	General error in ssh protocol
67	Key exchange failed
68	Reserved
69	MAC error
70	Compression error
71	Service not available
72	Protocol version not supported
73	Host key not verifiable
74	Connection failed
75	Disconnected by application
76	Too many connections
77	Authentication cancelled by user
78	No more authentication methods available
79	Invalid user name

If the ssh2 command is successful, it returns the error code of the command. For example, if you run
`ssh2 user@examplehost net stop servicename`
the error code you receive from the ssh2 is the same error code that the `net stop` command returned to `examplehost`.

D-3 General Errors

Error code	Description
254	Failed to execute sub-process
255	ssh_fatal() called (internal error)

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.

About F-Secure Corporation

F-Secure Corporation is the leading provider of centrally managed security solutions for the mobile enterprise. The company's award-winning products include anti-virus, file encryption and network security solutions for all major platforms from desktops to servers and from laptops to handhelds. 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. Mobility challenges many of the fundamental assumptions upon which traditional IT systems have been based on. F-Secure supports businesses with a broad range of centrally managed and up to date security solutions to enable a truly mobile enterprise.

For the administrator, F-Secure enables a dispersed user base with policy-based management, automatic enforcement, instant alerts and reports. For the end-user, with F-Secure, security is invisible, automatic, reliable, always operating and up-to-date.

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 main office in San Jose, California, as well as offices in Germany, Sweden, Japan and the United Kingdom and regional offices in the USA. F-Secure is supported by a network of value added resellers and distributors in over 90 countries around the globe. Through licensing and distribution agreements the company's security applications are available for the products of the leading handheld equipment manufacturers, such as Nokia and Compaq.

F-Secure's customers 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 Cap Gemini, Barclays Bank, Tesco, Glanbia, Deutsche Telekom, Aachener-Munchener, J&W, Honda, Tokyo-Mitsubishi Bank, Partek, ICL Invia, Sonera, and Verizon.

F-Secure software products have received numerous international awards, prizes and citations. The company was named one of Europe's 50 Hottest Tech Firms in Time Magazine in its June 2000 edition and one of the Top 100 Technology companies in the world by Red Herring magazine in its September 1998 issue. F-Secure products have consistently won awards including the Editor's Choice by Tietokone (Finnish IT Magazine) in February 2002, the Pick of the 2001 from SC Magazine (West Coast Publishing) in 2001, Full Score of 100 % from AV-Test.org and PC Welt (IDG) in November 2001, Highest Detection and Disinfection Rates from CHIP Magazine (Vogel Burda Communications) in May 2000, and the Virus Bulletin 100% award in June 2002.

The F-Secure Product Family

F-Secure Anti-Virus F-Secure Anti-Virus automatically and transparently delivers the most powerful and up-to-date protection against various threats, such as computer viruses, worms and other malicious code, as well as hackers and intrusion attempts. F-Secure Anti-Virus protects your workstations, servers, firewalls, gateways, mobile devices, and e-mail/groupware servers and can be centrally managed from one single location.

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.