

F-Secure® SSH

DISTRIBUTED BY WRQ

DATA SHEET

MAXIMIZING SECURITY FOR CRITICAL SERVERS, DATA TRANSFERS, AND CORPORATE APPLICATIONS

F-Secure® SSH is a cryptographic solution built to protect critical servers, data transfers, and corporate applications from Internet spies, hackers, and other known security threats. With F-Secure SSH, you can:

- Enable remote administration, even over the Internet, by encrypting passwords and setting up secure tunnels between critical servers and workstations.
- Transmit data without passwords and ensure that transfers are completed, even when connections have been interrupted.
- Access any TCP/IP-based application through a secure transmission tunnel.

You can use F-Secure SSH to access all major UNIX, Linux, and Windows servers from almost any client platform. And because F-Secure SSH supports a broad range of authentication mechanisms, you can easily choose the level of protection you need.

F-Secure SSH Technology

Network administrators are scrambling to close the security gaps left open by existing connectivity tools. Increasingly, they're replacing Telnet, FTP, and rlogin with a robust protocol suite called Secure Shell (SSH). SSH uses strong encryption and authentication methods to eliminate today's greatest security threats.

F-Secure SSH is based on the SSH protocol. It encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. F-Secure SSH has two components:

1 An SSH client on a Windows PC or UNIX workstation

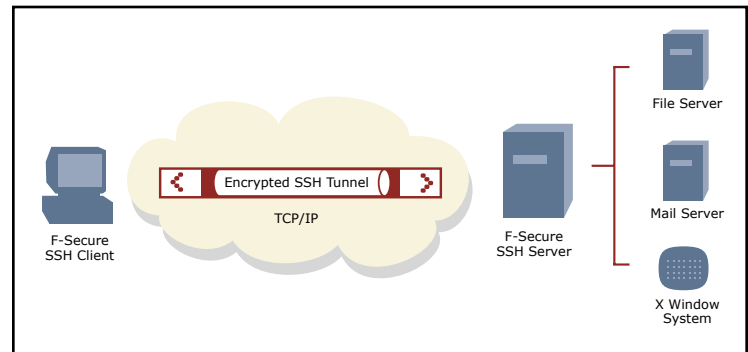
The F-Secure SSH client includes four integrated tools:

- F-Secure SSH Terminal, which secures remote logins over unknown or untrusted networks.
- F-Secure SSH File Transfer, which safely delivers confidential data to authorized users.
- F-Secure SSH Tunnel, which creates a secure transmission link for TCP-based applications.
- F-Secure Authentication Agent, which creates and stores private keys used in the SSH public key authentication method.

2 An SSH server on the system being accessed

The F-Secure SSH server authenticates and encrypts traffic at the server to:

- Safeguard terminal connections.
- Forward Internet protocols, including X11, POP3, SMTP, and HTTP.
- Protect file transfers.



Together, the F-Secure SSH client and server form a secure "tunnel" through which all communications travel.

Key Features

Broad platform support

The F-Secure SSH client and server run on all major UNIX, Linux, and Windows servers—the most common corporate platforms.

IETF standard for remote administration

Standardized by the Internet Engineering Task Force, the SSH protocol is used by millions of users and thousands of organizations around the world. If you're familiar with this popular protocol, you'll find it easy to use F-Secure SSH for remote host administration.

Secure file transfers

With F-Secure SSH, you can securely copy, move, remove, and edit remote files. These operations can even be automated, scripted, and unattended to save you time.

File transfers are quick, and you can be sure that no one is eavesdropping or altering content. When interrupted, transfers will resume where they left off.



Secure tunneling of TCP traffic

F-Secure SSH lets you forward any TCP/IP traffic through an SSH connection, including POP3, SMTP, and HTTP traffic. This means you can establish encrypted connections for remote users to essential corporate applications like e-mail—without worrying about privacy protection, integrity checking, authentication, or authorization.

Certified cryptographic libraries

F-Secure SSH was the first FIPS 140-2 level 2-certified SSH solution in the world. If you work in the U.S. government, FIPS certification is a must. If you are in financial services, health care, or any enterprise where data integrity and privacy are critical, the FIPS logo ensures that you have the highest-quality cryptographic solution.

Multiple encryption algorithms and message authentication codes

F-Secure SSH provides a full spectrum of ciphers (3DES, AES 128, AES 192, AES 256, Blowfish, CAST, and DES) and message authentication codes (HMAC-MD5 and HMAC-SHA1). The options you choose will depend on your required level of interoperability, performance, and security.

Support for diverse authentication technologies

F-Secure SSH works within your established authentication infrastructure, supporting a wide range of PKI-related technologies and smart cards.

Backed by an industry-leading support organization

F-Secure SSH is distributed exclusively by WRQ, a company that is consistently rated #1 in customer support. WRQ has more than 20 years of experience dealing with remote connections to host computers. When it comes to technical support, you can expect quick, expert responses to your questions and requests.

Support

SSH Protocol 2.0: IETF SecSh Internet draft

AES, 3DES, Blowfish, Twofish, CAST128, Arcfour, and DES encryption algorithms

MD5 and SHA-1 message integrity

DSS and RSA key authentication

Diffie-Hellman key exchange method

Windows domain authentication (GSSAPI and Microsoft Kerberos)

SecurID tokens

RADIUS protocol

X509.3 certificates, CMPv2 enrollment, PKCS#12 enrollment via web browser, and CRL checking from LDAP directories

Smart card interface: PKCS#11 and MSCAPI with Microsoft system certificates

Platforms

All major UNIX versions

Microsoft® Windows® 95

Microsoft Windows 98

Microsoft Windows Me

Microsoft Windows NT

Microsoft Windows 2000

Microsoft Windows XP

Microsoft Windows 2003

ABOUT WRQ

WRQ builds host-integration, terminal-emulation, and PC X-server software. We've been connecting legacy applications to emerging technologies since 1981. Our expertise helps companies get the most value from their hosts today as they advance their long-term IT strategy. Learn more about our Reflection® and Verastream® products at www.wrq.com.