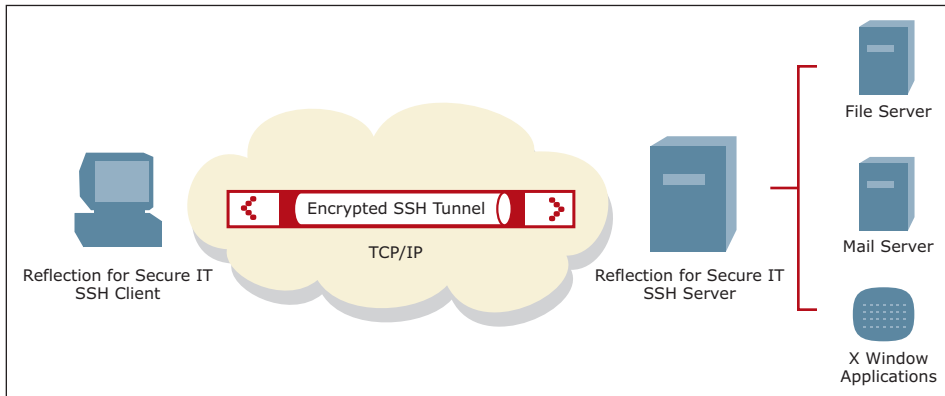


Reflection® for Secure IT Windows Server uses the SSH protocol to provide secure file transfer and remote administration services for Windows environments. It is part of the Reflection for Secure IT family of SSH clients and servers for Windows and UNIX—all designed to protect data in motion.



Together, the SSH client and server form a secure “tunnel” through which all communications travel.

Version 7.2 Highlights

- Microsoft Windows Server 2008 R2 (x86-64) support.
- Microsoft Cluster Service support.
- Use of mapped drives to access network directories during terminal sessions.
- Control over the number of connections allowed per user.
- Use of alternative credentials for accessing SFTP directories (for file transfers) and mapped drives (for terminal sessions).
- Customizable locations for server configuration files.
- Faster Active Directory domain authentication.

TECHNICAL SPECIFICATIONS

Secure Shell Access

- Secure remote terminal connections:
 - Configurable terminal provider (i.e., cmd.exe)
 - Configurable terminal default directory
 - NEW** - Use of mapped drives to access network directories during terminal sessions
- Secure remote command execution

Secure File Transfer

- SCP and SFTP protocol support
- SCP and SFTP special features:
 - Smart Copy (to eliminate redundant copying of identical source and target files)
 - File transfer resume after interrupted downloads
- SCP1 protocol support (for compatibility with OpenSSH clients)
- Virtual directory and chroot environment support

Access Control

- Assignable rights (allow or deny):
 - Terminal shell access
 - Exec requests
 - Local port forwarding
 - Remote port forwarding
 - SCP1 access

- SFTP/SCP2 access
- SFTP activities (Browse, Download, Upload, Delete, and Rename)
- Assignable to (subconfigurations):
 - Global
 - Groups
 - Users
 - Per client system (by IP address or domain name)

- Deny connections to users without Windows interactive access rights

- NEW** • Control over the number of connections allowed per user

- NEW** • Use of alternative credentials for accessing SFTP directories (for file transfers) and mapped drives (for terminal sessions)

Tunneling

- TCP port forwarding (local and remote)
- FTP protocol (active and passive mode)
- RDP protocol

Standards Support

- Compliance with IETF Secsh Internet drafts and RFCs 4250–4254, 4256, 4462, 4344, 4345, and 4716

Cryptographic Library Validation

- FIPS 140-2 Level 1 (Certificate #1027)

Algorithms

- Ciphers:
 - AES (128-, 192-, and 256-bit CTR)
 - AES (128-, 192-, and 256 bit-CBC)
 - 3DES (3 56-bit key EDE)
 - Blowfish (128-bit)
 - CAST (128-bit)
 - Arcfour (128- and 256-bit)
- MACs:
 - HMAC-MD5 (optional MD5 rejection available)
 - HMAC-MD5-96
 - HMAC-SHA1
 - HMAC-SHA1-96
 - HMAC-SHA256
 - HMAC-SHA512
 - RIPEMD160
- Key exchange:
 - Diffie-Hellman
 - GSS-API key exchange

Authentication

- Server authentication:
 - Public key (RSA and DSA)
 - PKI X.509 certificates
 - GSSAPI/Kerberos



TECHNICAL SPECIFICATIONS (continued)

- User authentication:
 - Password (local user and Windows domain user)
 - Public key:
 - RSA user keys
 - DSA user keys
 - OpenSSH public key interoperability
 - Keyboard interactive:
 - RSA SecurID
 - RADIUS
 - Keyboard-interactive password
 - PKI X.509 certificates
 - GSSAPI/Kerberos
 - Reflection PKI Services Manager:
 - Centralized configuration and management of PKI functions across multiple Reflection for Secure IT Windows servers, UNIX servers, and UNIX clients
 - Standalone service module supported on most platforms supported by Reflection for Secure IT Windows and UNIX servers
 - NEW - DoD PKI certified
 - FIPS 140-2 Level 1-validated for most supported platforms (Certificate #1048)
 - RFCs 2253, 2560, and 3280
 - X.509 certificates for server and client authentication (X.509 versions 1-3)
 - Version 2 X.509 CRL
 - OCSP revocation checks
 - NEW - HSPD-12 support
 - Support for LDAP and HTTP certificate and CRL repositories
 - Support for Microsoft Windows Certificate Store
 - Certificate extensions supported:
 - CDP
 - IDP
 - AIA
 - Policy constraints
 - Basic constraints
 - Name constraints
 - Extended key usage
 - Customizable configuration on per trust anchor basis
 - Fully customizable mapping of SSH user account names to certificates
 - NEW - SOCKS proxy support
 - NEW - PKI client command line utility for querying services availability and certificate validity
- Auditing**
- Configurable Windows Event Log level
 - Configurable Debug Log with local and UTC time stamps
- Notification of exceeded maximum password attempts
- Administrative Tools**
- NEW • Customizable locations for server configuration files
 - Section 508 support in the Reflection for Secure IT Windows Server configuration utility
- Operating Systems**
- NEW • Microsoft Windows Server 2008 R2 (x86-64)
 - Microsoft Windows Server 2008 (x86 and x86-64)
 - Microsoft Windows Server 2003 (x86 and x86-64)
 - NEW • Microsoft Cluster Service support
- System Requirements**
- Any system that meets the minimum requirements for the Microsoft Windows operating system
 - Disk space varies depending on the features installed
 - Network interface card

About Attachmate

Attachmate delivers advanced software for terminal emulation, legacy modernization, managed file transfer, and enterprise fraud management. With our technologies, more than 65,000 businesses worldwide are putting their IT assets to work in new and meaningful ways. www.attachmate.com



Corporate Headquarters
 1500 Dexter Avenue North
 Seattle, Washington 98109
 TEL 206 217 7500
 800 872 2829
 FAX 206 217 7515

EMEA Headquarters
 The Netherlands
 TEL +31 172 50 55 55
 FAX +31 172 50 55 51

Asia Pacific Headquarters
 Australia
 TEL +61 3 9825 2300
 FAX +61 3 9825 2399

Latin America Headquarters
 Mexico
 TEL +52 55 9178 4970
 FAX +52 55 5540 4886

WEB attachmate.com
 E-MAIL info@attachmate.com

For regional office information, visit www.attachmate.com.