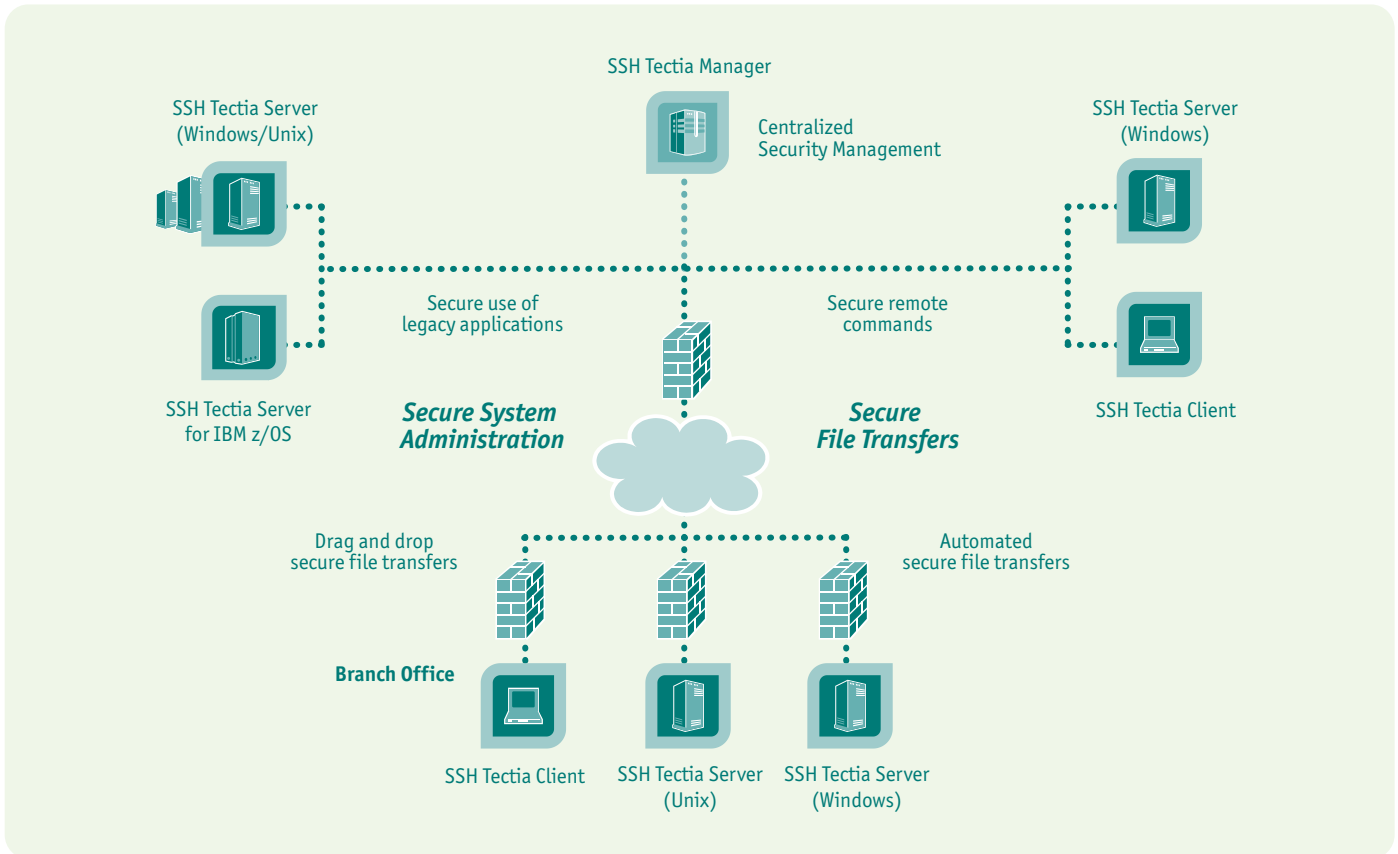




## SSH Tectia® Client and Server 6.0

End-to-End Communications Security for Enterprises,  
Government Agencies, and Financial Institutions



SSH Communications Security is a world-leading provider of enterprise security solutions and end-to-end communications security, and the original developer of the Secure Shell protocol. The SSH Tectia® Client and Server products offer strong, FIPS 140-2 certified encryption and flexible authentication to address the critical security requirements of large enterprises, government agencies, and financial institutions.

### SECURE FILE TRANSFERS

The SSH Tectia Client and Server products allow organizations to replace plaintext FTP connections with secure file transfers in cross-platform environments. On Windows, an intuitive graphical user interface enables drag-and-drop file transfers between Windows, Unix, Linux, and IBM mainframe systems. Unattended, automated file transfers between servers can be secured with the versatile command-line SFTP and SCP tools.

Additional enhanced file transfer features are available in SSH Tectia® ConnectSecure. Refer to the SSH Tectia ConnectSecure datasheet for further information.

### SECURE SYSTEM ADMINISTRATION

#### Replacement of Telnet, Rlogin, and FTP

The SSH Tectia Client and Server products, based on the award-winning SSH Secure Shell, are used by system administrators worldwide as a secure replacement for tools such as Telnet, FTP, and the Unix R-utilities.

### Secure Remote Commands

The SSH Tectia Client and Server products are also used in business-critical network environments for performing remote administrative tasks such as remote commands that require strong authentication and strong encryption before any operation is authorized on the remote servers.

### SECURE APPLICATION CONNECTIVITY

#### Secure RDP, VNC, TELNET, HTTP, IMAP, POP

To cost-effectively extend the useful lifetime of unsecured legacy applications and systems, SSH Tectia Client and Server provide enterprise IT and security departments with tools to strongly authenticate users and processes, and to transparently encrypt application data-in-transit without modifications to existing applications or infrastructure. These tools allow system administrators and users to securely use remote desktop software such as VNC and RDP, or business applications, such as e-mail and financial applications.

#### Automatic Secure Connection Setup

SSH Tectia Client can be used on Windows computers to transparently secure essential application connections with automatic secure connection setup. SSH Tectia Client can automatically open and secure the connection based on the information provided by the software that needs to be secured, thus eliminating the need to generate complicated configurations for connecting to a large amount of different servers.

## Features

### Security

- Multi-tier security architecture
- Configurable re-keying policies
- Authentication agent functionality
- Multiple channel support – multiple secure sessions are multiplexed to a single TCP/IP connection
- Compliance with the IETF Secure Shell (secsh) standards

### User and Server Authentication

- Password user authentication
- Public-key authentication (client and server)
- Two-factor user authentication based on smart cards and cryptographic tokens
- Keyboard-interactive interface for easy integration with third-party methods
- Support for GSSAPI/Kerberos
- Support for OpenSSH keys

### Ease of Use

- Windows graphical user interfaces for end users and system administrators
- User-specific connection profiles for easy session setup
- Nested tunnels for end-to-end communications security in remote access
- Centralized, transparent Secure Shell management with SSH Tectia Manager

### Secure File Transfer

- Secure drag-and-drop file transfers with Windows graphical user interface
- SFTP and SCP command-line tools for interactive and unattended use
- Multi-gigabyte file size support
- Strong data encryption
- Strong file integrity checking
- Anonymous secure file transfers with the SFTP protocol
- Data stream compression for low-speed connections
- SFTP Extensions for MVS dataset direct streaming <sup>(2)</sup>
- SFTP Extensions for SITE command support <sup>(2)</sup>
- Support for MVS and USS file systems <sup>(2)</sup>
- Automatic EBCDIC-ASCII Character Conversion <sup>(2)</sup>

### Secure Application Connectivity

- Automatic Tunneling
- TCP/IP port forwarding
- Secure forwarding of X11 sessions
- Transparent TCP Tunneling - no modifications required to the secured application <sup>(1)</sup>
- Easy configuration with comprehensive Filter Rules <sup>(1)</sup>
- Automated Connection Setup - destination hostname captured from the data stream <sup>(1)</sup>
- Configurable fallback to plaintext option <sup>(1)</sup>
- Support for connections to any Secure Shell server, including OpenSSH

## Specifications

### Supported Cryptographic Algorithms

#### Asymmetric (Public-Key) Algorithms

- Diffie-Hellman, DSA, and RSA

#### Symmetric (Session Encryption) Algorithms

- AES (128 / 192 / 256 bit)
- 3DES (168 bit)
- Arcfour (128 bit)
- Blowfish (128 bit)
- SEED (128 bit)
- Twofish (128 / 192 / 256 bit)
- Cryptocore Rabbit Stream Cipher (128 bit)

#### Data Integrity Algorithms

- HMAC MD5 and HMAC SHA-1
- Cryptocore Badger MAC



### Supported PKI Specifications

- X.509 v3 certificate support
- X.509 v2 CRL fetching via HTTP, LDAP, offline
- OCSP
- PKIX CMPv2 support
- PKCS#7 and PKCS#12 import
- PKCS#8 and PKCS#11 key support
- MSCAPI support on Windows

### Supported Third-Party Authentication Products

- Entrust Authority™ Security Manager 7.1-7.2
- RSA Keon®
- Microsoft CA
- Windows domain authentication through GSSAPI
- RSA SecurID®
- SafeWord® through PAM
- Microsoft IAS through RADIUS
- FreeRADIUS
- Centrify Direct Control 3.0

### Supported Platforms <sup>(4)</sup>

- HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)
- HP-UX 11iv2, 11iv3 (IA64)
- IBM AIX 5.2, 5.3 (POWER)
- Microsoft Windows 2000, XP, Server 2003, Server 2003 x64, Vista <sup>(3)</sup>, Vista x64 <sup>(3)</sup> (x86)
- Red Hat Enterprise Linux 3, 4, 5, 5.1 (x86)
- Red Hat Enterprise Linux 3, 4, 5, 5.1 (x86-64)
- Sun Solaris 8, 9, 10 (SPARC)
- Sun Solaris 10 (x86-64)
- SUSE Linux Enterprise Desktop 10 (x86)
- SUSE Linux Enterprise Desktop 10 (x86-64)
- SUSE Linux Enterprise Server 9, 10 (x86)
- SUSE Linux Enterprise Server 9, 10 (x86-64)

<sup>(1)</sup> Transparent TCP Tunneling supported on Windows XP and 2000.

<sup>(2)</sup> Requires a separate SSH Tectia Server for IBM z/OS product.

<sup>(3)</sup> Supported on SSH Tectia Client only.

<sup>(4)</sup> The SSH Tectia products can run on any standard hardware capable of running the supported operating system versions.

#### FINLAND

Valimotie 17  
FI-00380 Helsinki  
Tel: +358 20 500 7000  
Fax: +358 20 500 7001  
sales.fi@ssh.com  
[www.ssh.com](http://www.ssh.com)

#### GERMANY

Lintorfer Str. 7  
De-40878 Ratingen  
Tel: +49 2102 30979 0  
Fax: +49 2102 30979 0  
sales.de@ssh.com  
[www.de.ssh.com](http://www.de.ssh.com)

#### USA

20 William Street G35  
Wellesley, MA 02481  
Tel: +1 781 247 2100  
Fax: +1 781 431 0864  
sales.americas@ssh.com  
[www.ssh.com](http://www.ssh.com)

#### JAPAN

sales.jp@ssh.com  
[www.ssh.com/jp/](http://www.ssh.com/jp/)

#### UNITED KINGDOM

SoanePoint, 6–8 Market Place  
Reading, Berkshire  
RG1 2EG  
Tel.: +44 (0) 1189 255 580  
Fax: +44 (0) 1189 255 586  
sales.uk@ssh.com  
[www.ssh.com](http://www.ssh.com)



© 2008 SSH Communications Security Corp. All rights reserved. ssh® and Tectia® are registered trademarks of SSH Communications Security Corp in the United States and in certain other jurisdictions. The SSH and Tectia logos are trademarks of SSH Communications Security Corp and may be registered in certain jurisdictions. RSA, RSA Secured, and SecurID are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. Entrust is a trademark of Entrust, Inc. in the United States and/or other countries. Entrust is a registered trademark of Entrust, Inc. in the United States and other countries. In Canada, Entrust is a registered trademark of Entrust Technologies Limited. All Entrust product and program names are trademarks of Entrust, Inc. All other names and marks are the property of their respective owners. FIPS 140-2 Validated™: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.