ssh
Securing the path to your information assets

Data Sheet

Tectia® SSH Client/Server 6.4

The Gold-Standard in Data-in-Transit Security

Developed by the inventors of the SSH protocol, Tectia SSH Client and Tectia SSH Server are the core of our SSH Information Assurance Platform and are recognized as the gold-standard for data-in-transit security. More than 3,000 customers across the globe, including 7 of the Fortune 10, trust us to protect their information assets from cyber-criminals and insider threats while ensuring their mission critical business processes stay up and running. No matter the type or size of your organization, with SSH Communications Security you know you have an enterprise class, fully supported solution protecting your business information.

The Core of the SSH Information Assurance Platform:

Tectia SSH Client and Tectia SSH Server are not mere point solutions designed to get your information assets from point A to point B. Rather, our client and server form the core of our Information Assurance Platform - our fully interoperable, modular solution designed to help you save time & money, improve your security posture and meet or exceed compliance mandates.

A Rock Solid Security Platform Driven By Our Most Demanding Customers' Real World Use Cases:

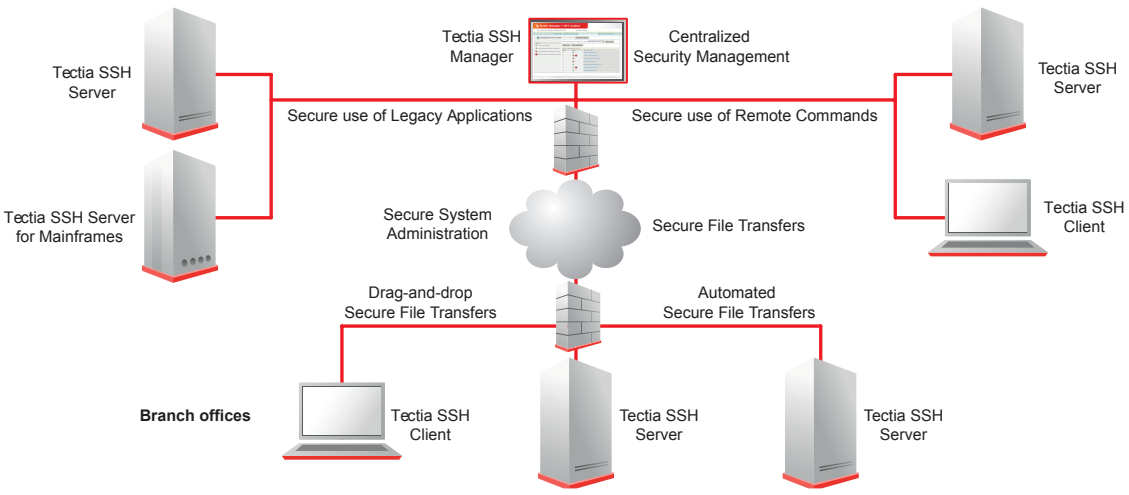
As the company that invented the SSH protocol, we understand how emerging threats and regulation mandates can create new risks, increase costs and result in compliance issues. That is why we work with our customers to learn about their vertically specific use cases and work hand-in-hand with some of the world's top security teams to develop solutions that solve real world problems.

Extend the Value of Your Implementation:

With Tectia SSH Client and Tectia SSH Server, not only will you benefit from a truly enterprise class secure file transfer solution, you will also have a rock solid, purpose-built platform designed to extend the value of your implementation far beyond what traditional open and commercial solutions can deliver.

The Enterprise Class SSH Platform

- **Fully Supported:** Unlike open source solutions, all of our products are fully backed by the world's most experienced technical support and R&D team.
- **Platform Based Approach:** Beyond a simple point solution, SSH delivers an integrated, modular platform that easily scales to meet your current and future security needs.
- **Heterogeneous Platform Support:** Tectia SSH Client and Tectia SSH Server supports Unix, Linux, and Windows to IBM z/OS and Linux on IBM System z, allowing you to utilize one solution across multiple platforms.



Features

Secure File Transfer

- Strong data encryption
- Strong file integrity checking
- Secure drag-and-drop file transfers with graphical user interface
- SFTP and SCP command-line tools for both interactive and unattended use
- Multi-gigabyte file-size support
- Anonymous secure file transfers with the SFTP protocol
- Data stream compression for low-speed connections

With Tectia SSH Server for IBM z/OS:

- Support for MVS and USS file systems
- SFTP Extensions for SITE commands
- MVS dataset direct streaming
- Automatic EBCDIC-ASCII character conversion
- Interfacing z/OS Job Entry Subsystem (JES)

Ease of Use

- Graphical user interfaces for end users and system administrators
- Users can create connection profiles for easy session setup
- Nested tunnels for end-to-end communications security in remote access
- Centralized, transparent Secure Shell management with Tectia Manager

Secure Application Connectivity

- Automatic tunneling of connections
- TCP/IP port forwarding
- Secure forwarding of X11 sessions
- Transparent TCP tunneling – no modifications required to the secured application *(1)*
- Easy configuration with comprehensive Filter Rules
- Automated connection setup – destination hostname captured from the data stream
- Configurable fallback to plaintext option *(1)*
- Support for connections to any standard Secure Shell server, including OpenSSH
- Support for IPv6

(1) Transparent TCP tunneling supported on Microsoft Windows XP, Vista and 7.

Security

- Multi-tier security architecture
- Compliance with the IETF Secure Shell standards
- Strong authentication of users and servers
- Strong encryption of data-in-transit
- Authentication agent functionality
- Configurable re-keying policies
- Multi-channel support – multiple secure sessions are multiplexed to a single TCP/IP connection

User and Server Authentication

- User authentication with passwords, public keys or two-factor user authentication with tokens or Tectia MobileID
- Public-key authentication for user and server
- Support for OpenSSH keys
- Keyboard-interactive interface for integration with third-party authentication methods
- Support for GSSAPI/Kerberos

Specifications

Supported Cryptographic Algorithms

Asymmetric (Public-Key) Algorithms:

- DSA and RSA

Symmetric (Session Encryption) Algorithms:

- AES (128 / 192 / 256 bit)
- 3DES (168 bit)

Data Integrity Algorithms:

- HMAC MD5, HMAC SHA-1, HMAC SHA224, HMAC SHA256, HMAC SHA384, HMAC SHA512

Key Exchange Algorithms:

- Diffie-Hellman (SHA-1 and SHA-2 methods)

Certifications

- FIPS 140-2 certified cryptographic module

Supported PKI

Specifications

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

Supported Platforms

- HP-UX 11iv1, 11iv2, 11iv3 (PA-RISC)
- HP-UX 11iv2, 11iv3 (IA-64)
- IBM AIX 5.3, 6.1, 7.1 (POWER)
- Microsoft Windows XP, Server 2003, Server 2003 R2, Vista (2), Server 2008, 7 (x86)
- Microsoft Windows Server 2003, Server 2003 R2, Vista *(2)*, Server 2008, Server 2008 R2, 7 (x64)
- Red Hat Enterprise Linux 4, 5, 6 (x86) & (x86-64)
- Oracle Solaris 9, 10, 11 (SPARC)
- Oracle Solaris 10, 11 (x86-64)
- SUSE Linux Enterprise Desktop 10, 11 (x86) & (x86-64)
- SUSE Linux Enterprise Server 9, 10, 11 (x86) & (x86-64)
- VMware ESX 3.5

(2) Windows Vista supported on Client and ConnectSecure.

Supported Third-Party Authentication Products

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

SSH Communications Security | sales@ssh.com | www.ssh.com