ssh®
Securing the path to your information assets

Data Sheet

Tectia® SSH Client • Tectia® SSH Server

The Foundation of a Robust Secure Shell Infrastructure

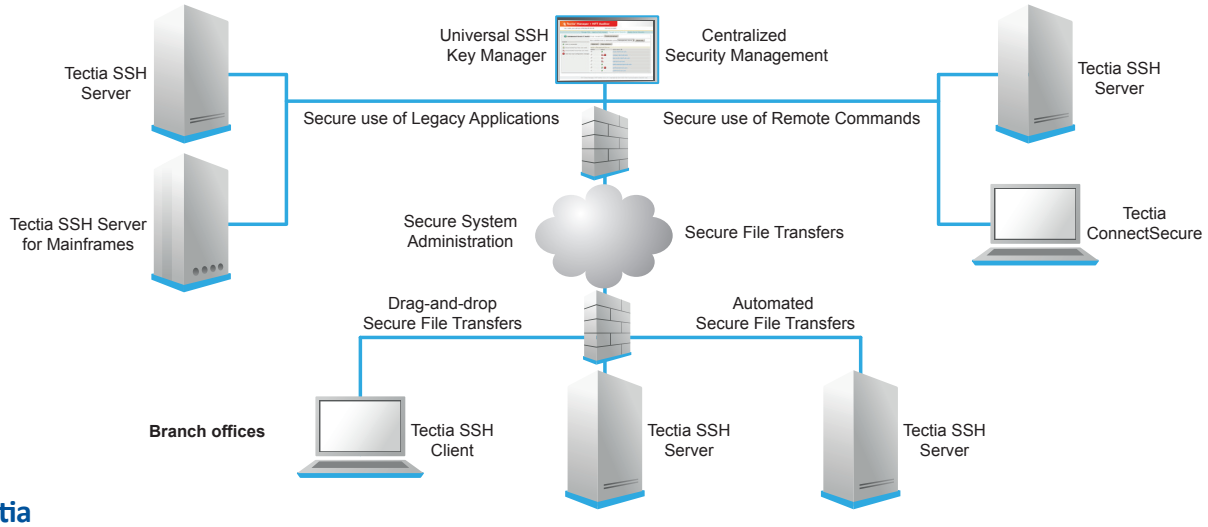
Enterprises and government organizations around the world use Tectia SSH Client and Server to secure their most critical IT processes including ad hoc and automated file transfers as well as remote systems administration. They chose Tectia for the features, reliability and manageability that are simply not available with open source solutions. They gain the assurance of deploying mature, commercial software backed by the support of the world's experts in Secure Shell technology. More than 3,000 customers across the globe, including 7 of the Fortune 10, trust SSH Communications Security to protect their information assets while ensuring mission critical business processes stay up and running.

Rapid, Transparent Deployment

Many enterprises require security for legacy applications that are business critical but difficult to change. Tectia SSH Client/Server adds a vital security layer to legacy applications without risky and costly changes to applications or procedures.

Reduce Risk, Gain Compliance

Threat of information loss is the most serious risk and compliance issue facing modern enterprises. Tectia SSH Client/Server enables enterprises to quickly address many of their most urgent and difficult to resolve information loss exposures.



Why Tectia

The Tectia Family of Secure Shell Client and Server products deliver value and cost savings not found in open source.

With Tectia You Get	Benefit
Compiled and tested packages for all key platforms including IBM Mainframes	Saves systems administrators tasks of tracking and obtaining updates from multiple sources. Reduces test time as well.
Available long term support versions	Stay with one version of Secure Shell across the enterprise even as OS versions change.
Consistent release cycle for all platforms	Less time spent tracking uncoordinated release cycles in different OS types.
Support for multiple authentication systems: X.509, SecurID, GSSAPI, CAC, etc.	Smooth integration with AAA infrastructure.
Mainframe support features	Easily convert legacy applications from FTP to SFTP.
GUI support for Windows. Drag and drop file transfers	Ease of use.
Connection profiles	Ease of use, saves time.
Interoperable, multiplatform	Tectia SSH Client and Server are fully interoperable with OpenSSH and standard SSHv2-compliant 3rd-party implementations. No issues creating secure connectivity with business partners or within mixed environments.
Automation	Secure application traffic without reprogramming.
Premium support – up to 24x7 available	Better business continuity. Open source has no committed support and some key features may in fact be written and supported by a single individual.

Features and Specifications

Secure File Transfer Features	• Strong encryption • SFTP and SCP command line tools • Multi-gigabit file size support • Compression
IBM z/OS support (for complete feature list see Tectia SSH Server for IBM z/OS data sheet)	• MVS and USS file system support • SFTP extensions for SITE commands • File type JES support • MVS dataset direct streaming • Automatic EBCDIC to ASCII conversion • Checkpoint/restart and file recovery
Application Connectivity	• Automatic application tunneling • Nested tunnel support • Automated connection set-up • Fully interoperable with OpenSSH • TCP/IP port forwarding • Multiplexing – multiple SSH sessions over a single TCP/IP connection • Transparent TCP tunneling* • Transparent FTP to SFTP Conversion*
Security	• IETF Compliant • Configurable rekeying policies • GSSAPI/Kerberos support • OpenSSH Keys support • 3rd party authentication support • FIPS certified cryptographic module
Supported Cryptographic Algorithms (partial list)	• DSA & RSA, ECDSA • AES • 3DES • HMAC (MD5, SHA-1,SHA-2) • Diffie-Hellman (SHA-1, SHA-2, Elliptic Curve)
PKI Support	• X.509v3 • X.509 v2 CRL fetching via HTTP. LDAP, offline • OSCP • PKCS #7, #12, #8, #11 • MSCAPI • Smartcard including CAC card support • Certificate support for User and Host Keys
Platform Support	• HP-UX (PA-RISC, IA-64) • IBM AIX (POWER) • Windows Vista, Server 2008, Windows 7, Windows 8, Windows 8.1, Windows 2012, 2012R2 • Red Hat (x86, x86-64) • Solaris (SPARC, X86-64) • SUSE (x86, x86-64) • IBM z/OS • SUSE for IBM System z • VMware ESX Server
Authentication Support	• Microsoft CA • Windows Domain • RSA SecurID • Microsoft IAS through RADIUS • FreeRADIUS • PAM • Kerberos • Inbuilt Password cache • Tectia MobileID

NOTE: Features marked with "*"are only available with Tectia ConnectSecure advanced SSH client. For details, see the Tectia ConnectSecure data sheet)