Securing the path to your information assets

Data Sheet

# Tectia® SSH Server 6.4 for Linux on IBM System z

## Secure File Transfers and Data-In-Transit

Tectia Server for Linux on IBM System z provides the ultimate SSH data security solution with strong encryption and authentication for mainframe file transfers and data-in-transit.

### How to secure mainframe file transfers in complex environments?

Tectia Server for Linux on IBM System z offers a quick and easy method to replace interactive and unattended plaintext FTP connections with secure SFTP and SCP command-line tools. Confidentiality, data integrity and strong authentication are supported for both remote connections and data transfers.

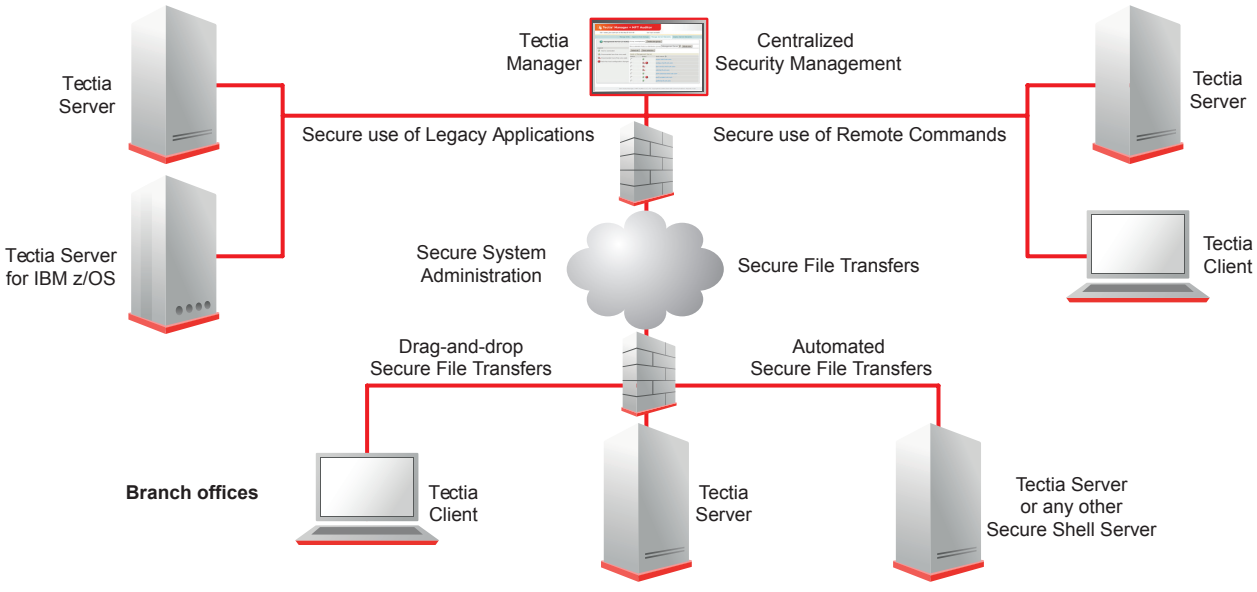
### "But our network is so complex..."

Tectia Server for Linux on IBM System z integrates easily into heterogeneous environments to secure mission critical data-in-transit and legacy applications. Tectia Server for Linux on IBM System z is designed to deliver end-to-end security to enterprise-class data centers running Linux on IBM mainframe systems by providing secure encrypted communication channels between IBM mainframe systems and other platforms. You can secure cross-platform connections and operations within distributed systems running Tectia for Windows, Unix and Linux, or other Secure Shell (including OpenSSH) implementations.

Tectia Server for Linux on IBM System z integrates with IBM's FIPS-certified cryptographic hardware facilities and hardware cryptographic acceleration. It also supports a wide variety of server and user authentication methods, such as public key and X.509 certificates for strong two-factor authentication.

### Gain compliance

Security compliance mandates such as PCI-DSS, SOX, HIPAA, FISMA and Basel II specify data confidentiality and authentication requirements. Tectia SSH client server solutions enable compliance without complex or burdensome modifications to infrastructure or applications.



## Features

### Secure File Transfer

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

With Tectia Server for IBM z/OS:

• Support for MVS and USS file systems
• SFTP Extensions for MVS dataset direct streaming
• SFTP Extensions for SITE command support
• Automatic EBCDIC-ASCII character conversion

### Ease of Use

• User-specific connection profiles for easy session setup
• Nested tunnels for end-to-end communications security in remote access

### User and Server Authentication

• User and server authentication with public keys
• User and server authentication with X.509 certificates
• User authentication with passwords
• 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

### Security

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

### Secure Application Connectivity

• Automatic tunneling
• FTP tunneling
• TCP tunneling (port forwarding)
• Secure forwarding of X11 sessions
• Support for connections to any standard Secure Shell server, including OpenSSH

## Specifications

### Supported Cryptographic Algorithms

Hardware Accelerated:

• AES (128 bit)
• 3DES (168 bit)
• SHA-1 and SHA-2 hash algorithm

Symmetric (Session Encryption) Algorithms:

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

Data Integrity Algorithms:

• HMAC MD5, HMAC SHA1, HMAC SHA224, HMAC SHA256, HMAC SHA384 and HMAC SHA512

Key Exchange Algorithms:

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

### Supported PKI Specifications

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

### Supported Third-Party Authentication Products

• Microsoft CA
• Windows domain authentication through GSSAPI
• Microsoft IAS through RADIUS
• FreeRADIUS

### Supported Server Platforms

• Red Hat Enterprise Linux 5.1, 6 (s390)
• SUSE Linux Enterprise Server 9 and 10 (s390)

Note: 31-bit glibc compatibility library is required on 64-bit operating systems