OpenText™ Secure Shell

Encrypt and authenticate your remote connections to secure applications and data across open networks

Data security is an ongoing concern for organizations. Sensitive, proprietary information must be protected at all times—at rest and in motion. The challenge for organizations that provide access to applications and data on host systems is keeping the data secure while enabling access from remote computers and devices, whether in a local- or wide-area network.

PRODUCT SUMMARY

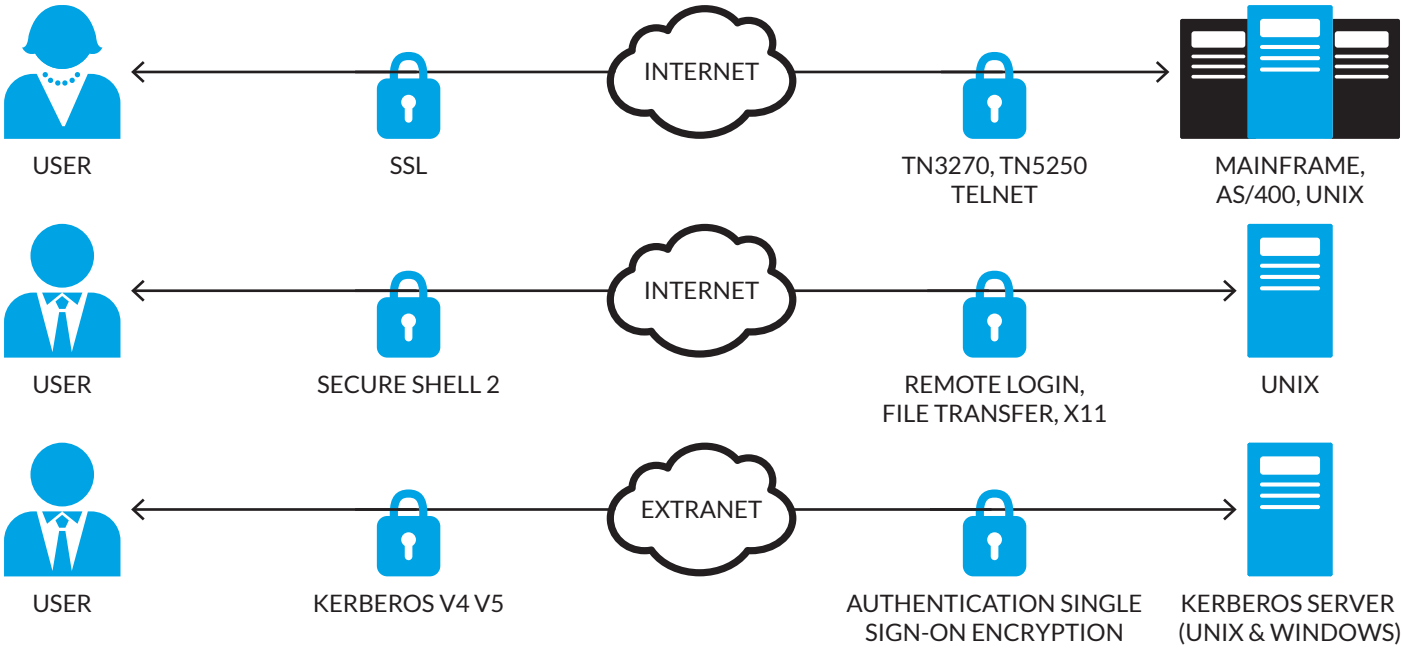
OpenText Secure Shell is an add-on product in the OpenText Connectivity suite that encrypts application traffic across networks. It helps organizations achieve security compliance by providing Secure Shell (SSH) capabilities. Moreover, seamless integration with other products in the Connectivity suite means zero disruption to the users who remotely access data and applications from web browsers and desktop computers.

OpenText Secure Shell is a comprehensive security solution that safeguards network traffic, including Internet communication, between host systems (mainframes, UNIX® servers and X Window System™ applications) and remote PCs and web browsers. When included with OpenText Exceed™ or OpenText HostExplorer™, it provides Secure Shell 2 (SSH-2), Secure Sockets Layer (SSL), LIPKEY, and Kerberos security mechanisms to ensure security for communication types such as X11, NFS, terminal emulation (Telnet), FTP and any TCP/IP protocol. OpenText Secure Shell encrypts data to meet the toughest standards and requirements such as FIPS 140-2.

Comprehensive Security Across Networks

OpenText Secure Shell provides support for the following standards-based security protocols:

- **Secure Shell (SSH)**—a transport protocol that allows users to log on to other computers over a network, execute commands on remote machines, and securely move files from one machine to another. It provides powerful authentication and secure communications over insecure channels, and is intended as a replacement for rlogin, rsh, and rcp. By using OpenText Secure Shell, administrators can eliminate the possibility of unknown third parties eavesdropping and stealing sensitive information.
- **SSL/TLS**—a set of cryptographic libraries used by software applications to provide strong encryption and authentication for transmitting data over a network. SSL/TLS uses cipher suites that encrypt data in such a way that it becomes virtually impossible for any eavesdropper to decrypt the information. SSL/TLS also provides support for key exchange and X.509 certificates authentication.
- **Kerberos**—a network authentication protocol. It uses secret-key cryptography to provide strong authentication for client/server applications. Kerberos was created by Massachusetts Institute of Technology (MIT) as a solution to solve network security authentication problems and enable single sign-on.



OpenText Secure Shell encrypts traffic across networks using a variety of security mechanisms.

OpenText Connectivity Integrations

OpenText Secure Shell is fully and transparently integrated with other OpenText Connectivity products, such as:

- OpenText Exceed the leading X Window server for Windows® desktops
- OpenText NFS Client, the de facto NFS client for Windows PCs
- OpenText HostExplorer, the integrated traditional and web-to-host terminal emulation solution
- OpenText HostExplorer FTP, a Windows Explorer integrated FTP client

OpenText Secure Shell can also successfully provide Secure Shell and Kerberos services to third-party applications.

OpenText Connectivity Integrations

Certification

- Compatible with Windows 7 and 8
- FIPS 140-2 compliant
- *Citrix Ready*™

Supported Protocols

Secure Shell 2 (SSH-2)

- Secure terminal, SFTP, X11 forwarding, and generic port forwarding
- Authentication method: password, keyboard interactive, public/private key, Kerberos, X.509 certificates
- Support for SSH-Agent and passphrase caching
- Command-line SSH and SCP utility with third-party compatibility mode
- Graphic monitoring of Secure Shell activity
- Integrated SOCKS support with dynamic port forwarding
- Seamless integration with other OpenText Connectivity products
- "Black-Box" secure shell tunnels with no user interface
- Public/Private key and X.509 certificate creation wizard
- Auto-upload and multiple import/export format for public/private keys

SSL-LIPKEY

- Support for Low Infrastructure Public Key (LIPKEY)
- SSL v2/3 and TLS 1.2 encryption
- Support for X.509 certificate
- SafeNet® iKey™ 2000 USB-based authentication token support
- Support for smart card authentication

Kerberos

- Support for Kerberos v4 & v5 (authentication and encryption)
- Integration with Microsoft Windows Kerberos ticket cache
- Advanced ticket management function
- Simplified configuration file creation

	SSL-LIPKEY	KERBEROS	SECURE SHELL
GENERAL INFORMATION			
Primary Function	SSL v2/v3 & TLS client LIPKEY	Kerberos v4/v5 client	Secure Shell 2, SCP, SFTP
APPLICABLE TECHNOLOGY			
X11		✓	✓
FTP	✓	✓	✓
VT	✓	✓	✓
TN3270	✓	✓	✓
TN5250	✓	✓	✓
APPLICABLE PRODUCT			
Exceed PowerSuite™	✓	✓	✓
Exceed	✓	✓	✓
OpenText NFS Client	✓	✓	✓
HostExplorer	✓	✓	✓

http://connectivity.opentext.com

SALES • CONNSALES@OPENTEXT.COM • +1 905 762 6400 • 1 877 359 4866
SUPPORT • SUPPORT@OPENTEXT.COM • +1 519 888 9933 • 1 800 540 7292