opentext™

Product overview

OpenText Secure Shell

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

- **Comprehensive security** across networks
- **Support** for Secure Shell (SSH)
- **Strong** SSL/TLS encryption
- **Powerful** Kerberos authentication support

Data security is an ongoing concern for organizations. Sensitive, proprietary information must always be protected—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.

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. Secure Shell encrypts data to meet the toughest standards and requirements, such as FIPS 140-2.

Secure Shell is an add-on product in the OpenText™ Connectivity suite, which 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.

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 Secure Shell, administrators can eliminate the possibility of unknown third parties eavesdropping and stealing sensitive information.

opentext™

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

- OpenText™ Exceed™, the leading X Window server for Microsoft® 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
- HostExplorer FTP, a Windows-integrated FTP client

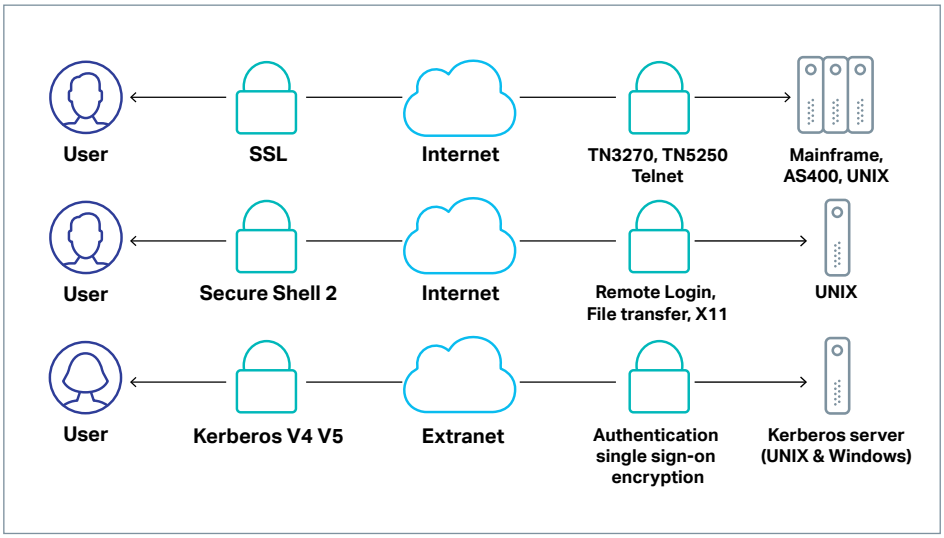
Secure Shell can also provide Secure Shell and Kerberos services to third-party applications.

OpenText Connectivity Integrations Certification

- Compatible with Windows 10, 8 and 7
- FIPS 140-2 compliant
- Citrix Ready® for XenApp® and XenDesktop® 7

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, which uses secret-key cryptography to provide strong authentication for client/server applications. The Massachusetts Institute of Technology (MIT) created Kerberos as a solution for network security authentication problems and to enable single sign-on.



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

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 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

opentext™

Learn more

Supported protocols cont.

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

	SSL-LIPKEY	Kerberos	Secure Shell
Primary function	SSL v2/v3 & TLS client LIPKEY	Kerberos v4/v5 client	Secure Shell 2, SCP, SFTP
X11		✓	✓
FTP	✓	✓	✓
VT	✓	✓	✓
TN3270	✓	✓	✓
TN5250	✓	✓	✓
Applicable product			
OpenText™ Exceed™ PowerSuite	✓	✓	✓
Exceed	✓	✓	✓
NFS Client	✓	✓	✓
HostExplorer	✓	✓	✓

opentext.com/contact Twitter | LinkedIn