

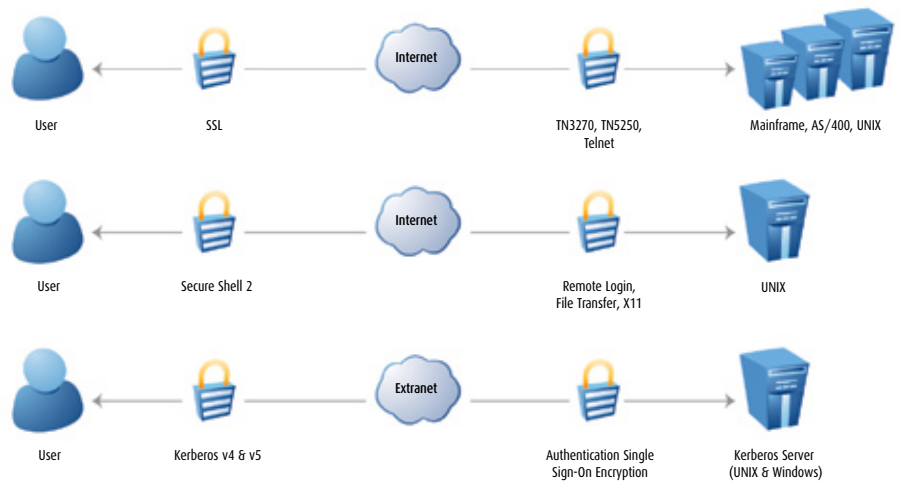


Connectivity Secure Shell™ 2007

Security concerns are receiving an unprecedented focus from IT organizations these days. While risks associated with security issues have been well understood, many companies are in dire need of a single integrated security solution for their Connectivity environment. By providing a robust and comprehensive security toolset, Connectivity Secure Shell™ 2007 allows organizations to meet their security goals while reducing their operating costs.

New Features

- > **SSH command line:** allows the user to run remote commands on the host, and to retrieve the output on the Windows® client machine. It supports a range of parameters including tunnel profiles.
- > **Microsoft® Windows Kerberos Authentication Support:** Connectivity Secure Shell™ now supports the Windows SSPI interface to acquire a security context which can be used to establish a Kerberos authentication in much the same manner as in an external Kerberos provider case (with MIT Kerberos or Connectivity Kerberos™ for instance).
- > **X509 Certificate Authentication**
- > **Integrated SOCKS Support:** SOCKS is a networking proxy protocol that enables hosts on one side of a SOCKS server to gain full access to hosts on the other side of the SOCKS server without requiring direct IP-reachability. This feature allows users to configure SSH sessions to use a SOCKS server.
- > **SOCKS Dynamic Port Forwarding:** allows a socksified application (one that supports using a socks proxy) to use a Connectivity Secure Shell tunnel as a VPN to forward connections dynamically, to different hosts, from the tunnel endpoint.
- > **Additional Browser Support:** Connectivity Secure Shell and other products that use the Hummingbird Deployment Wizard™ can now be deployed on Firefox®, Opera and 3rd party java-enabled browsers.
- > **Event Monitoring Server:** monitors events generated by Hummingbird Connectivity™ client applications (e.g. HostExplorer®, Connectivity Secure Shell™, Hummingbird FTP™, Exceed® etc.). It logs client-specific actions into an event database and offers various administrative views to analyze that information.



Key Benefits

The need for a safe and secure enterprise system is an important concern in today's business computing world. Security breaches can cause serious harm to a company that does not have the proper safeguards in place. Administrators are realizing that they cannot afford to take any chances with mission-critical enterprise information assets that affect the success of the organization.

Connectivity Secure Shell™ is a full-featured security suite that provides support for the following security standard-based protocols:

- > Secure Shell is 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 software, administrators can eliminate the act of eavesdropping on sensitive information such as user credentials.
- > SSL/TLS consist in a set of cryptographic libraries which can be 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 X509 certificates authentication.
- > Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos was created by MIT (Massachusetts Institute of Technology) as a solution to solve network security authentication problems.

Connectivity Secure Shell allows organizations to secure their network by providing authentication and encryption capabilities to the following communication types:

- > X11
- > NFS
- > Any other type of TCP/IP protocol
- > Telnet
- > FTP

Connectivity Secure Shell is fully and transparently integrated with other Hummingbird Connectivity solutions such as:

- > Exceed®: the leading edge X-Window server for Windows desktops
- > NFS Maestro™: the de facto standard for NFS protocol on PCs
- > HostExplorer®: the integrated traditional and web-to-host terminal emulation solution
- > Hummingbird FTP™: the Windows Explorer integrated FTP client

Connectivity Secure Shell 2007 can also successfully provide Secure Shell and Kerberos services to 3rd party applications.

	Connectivity SSL-LIPKEY™	Connectivity Kerberos™	Connectivity Secure Shell™
General Information			
Primary Function	SSL v2/v3 & TLS client LIPKEY	Kerberos v4/v5 client	Secure Shell 2, SCP, SFTP, SSL v2/v3 & TLS, Kerberos v4/v5 client LIPKEY
No Charge	✓	✓	
Applicable Technology			
X11		✓	✓
FTP	✓	✓	✓
VT	✓	✓	✓
TN3270	✓	✓	✓
TN5250	✓	✓	✓
Applicable Product			
Exceed PowerSuite™	✓	✓	✓
Exceed®	✓	✓	✓
NFS Maestro Client™	✓	✓	✓
HostExplorer®	✓	✓	✓

Key Features

Supported Protocols

- > Secure Shell 2
- > SSL v2/3 & TLS
- > Kerberos v4 & v5
- > LIPKEY

Supported Software

- > Exceed PowerSuite 2007 & Exceed 2007
- > NFS Maestro Client™ 2007, NFS Maestro Solo™ 2007, NFS Maestro Server™ 2007, NFS Maestro Server™ 2007 Enterprise Edition, NFS Maestro Gateway™ 2007
- > HostExplorer® 2007
- > Other Hummingbird and 3rd party software (restrictions may apply)

Connectivity Secure Shell

- > Secure Terminal, SFTP, X11 forwarding and generic port forwarding
- > Authentication method: password, keyboard interactive, public/private key, Kerberos, X509 certificates
- > Support for SSH-Agent and Passphrase caching
- > Command line SSH and SCP utility with 3rd party compatibility mode
- > Graphic Monitoring of Secure Shell activity
- > Integrated SOCKS support with dynamic port forwarding
- > Seamless integration with other Hummingbird Connectivity™ software
- > “Black-box” secure shell tunnels with no user interface
- > Public/Private Key and X509 certificate creation wizard
- > Auto-upload and multiple import/export format for public/private keys

Connectivity SSL-LIPKEY

- > Support for Low Infrastructure Public Key (LIPKEY)
- > SSL/TLS encryption
- > Support for X509 certificate
- > SafeNet iKey™ 2000 USB-based authentication token support
- > Support for SmartCard® authentication

Connectivity Kerberos

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

System Requirements

- > **Operating Systems:** Windows 2000, Windows 2000 Professional, Windows 2000 Server, Windows XP, Windows XP Professional, Windows XP Professional X64 Edition, Windows Server™ 2003, Windows Server 2003, and Windows Server 2003 X64 Edition — Ready for Windows Vista
- > **Web-to-Host:** Server — any web server on any operating system and Browser — Internet Explorer, Firefox, Opera and 3rd party java-enabled browser
- > **Terminal Services:** Windows Server 2000/2003 Terminal Services and Citrix® Presentation Server™/Citrix Metaframe®

How Can Hummingbird Help You?

Corporate Headquarters: 1 Sparks Avenue, Toronto, Ontario M2H 2W1 Canada > Toll-Free Canada/USA: 1 877 FLY HUMM (359 4866) > Tel: +1 416 496 2200
> getinfo@hummingbird.com > <http://connectivity.hummingbird.com>

Copyright © 2006, Hummingbird Ltd. All rights reserved. Trademarks and logos are the intellectual property of Hummingbird Ltd. All other company and product names are trademarks of their respective owners.
DS-03-00-EN-101.07/06