Open Text Secure Terminal™ 14
Easy and cost-effective solution for organizations to secure desktop assets and control costs

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.

Many organizations rely on UNIX systems to accomplish mission-critical operations. Traditionally, those UNIX systems have been accessed through insecure protocols, such as Telnet or FTP. Security conscious corporations have realized that although they could not rely on those protocols, they could not afford removing the UNIX systems.

Open Text Secure Terminal allows users to:

- Access mission-critical applications from their Microsoft® Windows® desktop or a browser through a secured terminal
- Transfer files securely from UNIX environments to their Windows desktop
Open Text Secure Terminal has been built to offer a large choice of security methods:

- **Secure Shell 2**—Open Text Secure Terminal supports state-of-the-art Secure Shell 2 protocol standards. Based on the work of the Secsh group, Open Text Secure Terminal implements the latest IETF RFC for Secure Shell2 authentication and encryption.

- **SSL**—Open Text Secure Terminal offers support for SSL v2/3 and TLS encryption and authentication.

- **Kerberos**—Open Text Secure Terminal supports Kerberos v4 and Kerberos v5 based on the work of the MIT.

Open Text Secure Terminal provides administrators with the latest technologies for securing their network communications. By getting the most from a wide range of encryption and authentication protocols, Open Text Secure Terminal ensures that mission-critical data are safely transmitted over the wires.

Migrating from a desktop-based product to a Web-based solution can be risky, especially when it affects functions such as access to legacy applications and mission-critical data. Open Text Secure Terminal can help achieve this transition with maximum security and efficiency. Whether in desktop-based or Web-based mode, Open Text Secure Terminal provides the same interface, the same features, the same power, and the same administrative options.

With its built-in Web capabilities, auto-upgrade features, Microsoft® System Management Server (SMS) integration and powerful administrative features, Open Text Secure Terminal introduces users to a new world of terminal emulation solutions. Thanks to its macro converter, terminal themes manager and advanced API support, Open Text Secure Terminal provides an easy migration path from existing terminal emulators.

Open Text Secure Terminal offers an easy way to protect corporate investments in legacy data while letting users benefit from the latest in desktop and Web-based technologies. It enables organizations to lower their total cost of ownership while deploying a state-of-the-art Web-based terminal emulator. Corporations are able to provide every user quick and convenient access to legacy information without having to undertake costly and painful installation on each desktop. Organizations that choose Open Text Secure Terminal save time and money by skipping the deployment process while increasing their productivity.

**New features**

- **Support Windows 7**—Guarantees excellent performance and best experience.

- **Native x64 support**—Native 64-bit support for Microsoft® Windows® x64 family and Windows 7.

- **Screen history**—Allows users to view and capture screen information while navigating.

- **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 terminal sessions to use a SOCKS server.

- **HTTP and SOCKS dynamic port forwarding**—Allows HTTP or SOCKS proxy enabled applications to use a Open Text Secure Terminal tunnel as a VPN to forward connections dynamically, to different hosts, from the tunnel endpoint.

- **Event-Monitoring server**—Monitors events generated by Open Text Connectivity Solutions applications, such as Open Text® HostExplorer®, Open Text Secure Terminal, Open Text® Exceed®. It logs client-specific actions and offers various administrative views to analyze that information.

- **Trace wizard**—This diagnostic tool allows customers to simplify the process of troubleshooting end-users issues and collecting trace information.

- **Feature access management**—This console allows administrators to disable various features of Open Text Secure Terminal and lockdown the user's terminal environment for security purposes.

- **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**—Open Text Secure Terminal 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.
## Key features

### Emulation features
- Emulation settings—VT 52 to VT 420, ANSI, SCO-ANSI, IBM® 3151, 42 character sets support, custom screen size, linemode support, TAPI
- Terminal customization—Keyboard mapper, color mapper, support for Unicode and variable width fonts, cursor customization, ability to map mouse actions, multiple terminal resizing option (font resize or terminal size re-negotiation)
- Application customization—Menu manager, configuration dialog manager, sound manager, custom right-click menu, toolbar manager
- Automation—Event manager, simple point-and-click graphical macro editor, advanced HostExplorer Basic™ macro editor, quick-keys, hotspots
- Printing—Multiple screen printing, print screen advanced options, host printing support, capture mode
- API—HLLAPI, EHLLAPI, WINHLLAPI, OHIO, OLE, COM
- Support for multiple code pages (Euro ready)
- Macro engine—Recording, editing, and playback—third-party macros conversion
- Support for HLLAPI, EHLLAPI, WINHLLAPI, OHIO, OLE, COM APIs
- File transfer client fully integrates with Windows Explorer

### Secure Shell 2
- Authentication method—Password, keyboard interactive, public/private key, Kerberos
- Support for SSH-Agent and passphrase caching
- Command line SCP utility with third-party compatibility mode
- Graphic monitoring of secure shell activity
- “Black box” secure shell tunnels with no user interface
- Key and certificate creation wizard
- Auto upload and multiple import/export format for public/private keys

### Other
- Native 64-bit support for Microsoft Windows x64 family and Windows 7
- Support for SSL v2/3 & TLS, LIPKEY, and Kerberos v4/5
- Integrated tools to manage public/private keys and X.509 certificates
- Support for SafeNet® USB token and SmartCard® authentication devices

## System requirements
- **Web-to-Host**—Server—any Web server on any operating system. Browser—Internet Explorer, Firefox®, Opera, and third-party java-enabled browser
- **Terminal services**—Windows Server 2008/2003 Terminal Services and Citrix® XenApp™ for Windows platforms
- **Minimum CPU requirements:** Pentium 4

---

`http://connectivity.opentext.com`

**Sales**
connsales@opentext.com
+ 1 905 762 6400 | 1 877 359 4866

**Support**
connsupport@opentext.com
+ 1 905 762 6400 | 1 800 486 0095

Visit online.opentext.com for more information about Open Text solutions. Open Text is a publicly traded company on both NASDAQ (OTEX) and the TSX (OTC). Copyright © 2009 by Open Text Corporation. Open Text and The Content Experts are trademarks or registered trademarks of Open Text Corporation. This list is not exhaustive. All other trademarks or registered trademarks are the property of their respective owners. All rights reserved. 09CONS0024EN