



LOCKED DOWN. FREED UP.

SECURE THIN CLIENT™

Enabled for DoD x.509 CAC

Finally, a breakthrough that streamlines the process of enabling remote users to logon and authenticate to enterprise networks with an X.509 smartcard. All on a low-cost platform that eliminates the risks associated with connecting a personal home computer to the enterprise.

Blue Ridge/Secure Thin Client solution specifically enabled for DoD CAC can significantly reduce overall IT costs while improving security and end-user productivity. This integrated, pre-configured thin client platform reduces the impact of enterprise virus infections and shortens restore time after such an attack.

This innovative solution was specifically designed to enable remote users to logon and Authenticate to enterprise networks with an x.509 smartcard utilizing a low-cost platform, eliminating the risks associated with connecting personal home computer to the enterprise.

The secure thin client computer itself is a Wyse S90™ reduced footprint device that does not contain a hard drive. Instead, it uses flash memory to contain the operating system and the associated files. The Microsoft® Windows®XP embedded operating system makes this possible while including most of the functionality required by end-user applications. The hardware platform supports all of the usual peripheral attachments and the various ports can be disabled to prevent users from attaching unapproved devices.

Authentication to the enterprise is accomplished using ActivIdentity's ActivClient™ and Tumbleweed's Desktop Validator™. Together with the Blue Ridge Networks' FIPS 140-2 VPN client, the remote user can authenticate to an OCSP responder and logon to the Active Directory domain controller. This process provides for auditing and management of remote users through Active Directory.

One of the key features of the thin client platform is called the "write filter." Once activated, the write filter causes all files written by the operating system to be placed onto a RAM disk. No changes are made to the flash memory.

Features and Benefits:

- Ideal Solution for Teleworkers
- Highly Effective Anti-virus Protection
- HSPD-12 Two-Factor Authentication
- FIPS 140-2 Validated
- Integrated Active Directory Authentication
- Significantly Reduced Cost of Desktop Computing



The next time the device is booted, it has exactly the same file system image it did the first time it was booted — preventing alteration to the known and improved image. Most important, it prevents the introduction of viruses into the enterprise.

Tunnel Lock™

Tunnel Lock is a special driver that prevents the PC from communicating with any other systems except those at the Enterprise. The only communications allowed by the thin client computer are those to servers at the enterprise or to the Internet via the Enterprise firewall. This ensures that the PC is always under the control of the policy set by the IT organization.

A specially-designed VPN client integrates with the previously described features. It provides a highly secure connection to Enterprise servers using strong mutual authentication. It can only be activated when the authorized user inserts the x.509 PIV or CAC card into the card reader and authenticates to both OSCP and Active Directory.

The VPN tunnel to the enterprise can be configured to terminate under three conditions:

1. The user chooses to terminate the connection.
2. The user removes their PIV or CAC smartcard from the card reader.
3. The connection idle timeout period expires.

Whatever condition causes the tunnel to terminate, the user will be logged off the secure thin client immediately. This causes the RAM disk to be immediately purged from memory. Any downloaded files, web pages, cookies or viruses that may have been written to the C drive are gone.

In effect, the end of every connection to the Enterprise IT infrastructure resets the user's desktop computer to its original condition.

Recovering from enterprise-wide virus infections is difficult because end-user workstations are potentially being infected and re-infected in they're not under the direct control of the IT staff. Blue Ridge/Secure Thin Client reduces the impact of enterprise virus infections by eliminating the enduser PC as a storage place for viruses.

Specifications

Wyse S90 Thin Computer

Based on Windows XP Embedded operating system
 Integrated Microsoft RDP and Citrix ICA protocols
 512MB FLASH/256MB DDR RAM Standard

Processor

AMD Geode GX
 Display Support
 VESA monitor support with Data Display control
 16-bit/64K colors:
 up to 1280x1024@100Hz
 up to 1600x1200@90Hz
 24-bit/16.7M colors:
 up to 1280x1024@85Hz

Audio

Output: 1/8-inch mini, full 16-bit stereo
 48 KHz sample rate
 Input: 1/8-inch 8-bit mini microphone

Networking

10/100BaseT Fast Ethernet, twisted pair (RJ-45)

Input/Output/Peripheral Support

VGA-type Video output (db-15)
 Enhanced USB keyboard
 PS/2 mouse port and Windows keys
 PS/2 mouse included
 Local and/or network printers supported
 One serial port
 Four USB 2.0 ports (2 on front, 2 on back)

Firmware Features

Microsoft XPE Service Pack 1
 Microsoft Internet Explorer 6.0
 RDP 5
 ICA 7.0, Program Neighborhood

Management

Remote management, configuration, and upgrades through Wyse Rapport client management software

Physical Characteristics (H x W x D)

1.38 inches (34mm)
 6.94 inches (177mm)
 4.75 inches (121mm)
 6lbs (2.7kg)

Environmental

Temperature range
 Operating: 50° to 104°F (10° to 40° C)
 Storage: -40° to 149°F (-40° to 65° C)
 Fanless design
 Humidity
 20% to 80% noncondensing
 Operating altitude range
 0 to 10,000 feet (0 to 3,050 meters)

Power

Worldwide auto-sensing 100-240 VAC, 50/60Hz

Warranty

Three-year Limited Warranty

Regulatory compliance

German EKI-ITB 2000, ISO 9241-3/-8
 cULus 60950, TÜV-GS, EN 60950
 FCC Class B, CE, VCCI, C-Tick
 WEEE