Codonics® Virtua™ Firewall and Security

Release Notes

Overview

Codonics Virtua provides two user-configurable security features designed to reduce the threat from malicious software attacks by viruses, adware, worms and trojans. A software firewall restricts incoming access to specific network services. A method for external scanning of the Virtua hard drive by commercial anti-virus programs allows detection of files containing malicious software.

> IMPORTANT: Virtua security features should be part of an overall strategy for device security. Do not rely on these features as the only means for preventing malicious software attacks.

Firewall Configuration

Virtua utilizes the standard Windows XP Embedded firewall to block incoming connections to network services. The firewall operation is configured using parameters in the SmartDrive network profile:
\profiles\network\network.default.txt.
The following parameters control the operation of the firewall:

firewallEnabled
Settings: ***Boolean*** (true or false)
Default: **False**
Description:Enables the internal firewall when set to **true**. This limits incoming network connections according to the settings of the ***xxxFirewallPortOpen*** parameters.

httpFirewallPortOpen
Settings: ***Boolean*** (true or false)
Default: **True**
Description:**True** allows remote web browers to connect to Virtua and operate the device. **False** blocks remote web browser connections.

> **NOTE:** The web interface on the touch-screen display will always operate regardless of the **httpFirewallPortOpen** parameter.

smbFirewallPortOpen
Settings: ***Boolean*** (true or false)
Default: **True**
Description:**True** allows incoming SMB connections for remote mounting of mapped network drives. **False** blocks remote mounting of mapped network drives.

telnetFirewallPortOpen
Settings: ***Boolean*** (true or false)
Default: **False**
Description:**True** allows incoming telnet connections to Virtua for diagnostic purposes. **False** blocks incoming telnet connections.

Typical settings to enable the firewall would be:

network.default.txt
firewallEnabled = true
httpFirewallPortOpen = true
smbFirewallPortOpen = true
telnetFirewallPortOpen = false

Virus Scanning

Virtua can provide read-only access to internal hard drive partitions for scanning by commercial anti-virus programs. This is made available to IT departments as an alternative to loading anti-virus software on Virtua.

> IMPORTANT: Virtua is a medical device that contains software validated for proper operation only as configured from Codonics. Loading external software such as anti-virus programs can result in unsafe or ineffective operation. Codonics strongly advises against modification of the device or software in any way.

Access to the hard drive partitions is accomplished by remote mounting the partitions as network drives. The partitions and corresponding network names are:

Network Name	***Partition***
drive0	Program partition
drive1	First Data partition
drive2	Second Data partition (XR Only)

Access is read-only to prevent modification of the software.

If malicious software is detected, the remedy is to perform a full re-install of Virtua software from the Operating Software disc.

The mapped network drives are password protected to prevent unauthorized access to patient information. Please contact Codonics Technical Support department to obtain the username and password that allow access to the partitions.

NOTE: The current release of Virtua software uses a fixed username and password to mount the partitions. This will be configurable in future releases, but to protect the system from unauthorized access, the username and password are only distributed by Codonics Technical Support after verifying the recipient.

If the firewall is enabled, remote mounting of the partitions requires setting the parameter **smbFirewallPortOpen = TRUE**.

Virtua Security Design Features

Virtua software has security implemented at several levels. While this document focuses on the firewall and external virus scanning mechanisms, other precautions have been implemented:

- Windows XP Embedded configuration. The Windows XP Embedded operating system has many unnecessary components removed to limit software attacks.
- Autorun disabled. External software will not run when loaded in the CD/DVD drives or on the USB ports.
- Limited built-in applications. Virtua does not allow access to incoming email, outgoing web access or other applications not related to the function of the device. This greatly reduces the opportunity for malicious software to enter the system.
- No keyboard or mouse. Virtua does not include a keyboard or mouse. Users are limited to accessing Virtua using the web-based touch-screen interface or an external web-browser. Other applications cannot be loaded or accessed.

Technical Support

If problems occur during software installation, contact Codonics Technical Support between the hours of 8:30AM and 5:30PM EST (Weekends and U.S. holidays excluded).

Phone: 440-243-1198

Email: support@codonics.com

Website: www.codonics.com

Get it all with just one call
1-800-444-1198

CODONICS®
We bring the future into focus

17991 Englewood Drive
Middleburg Heights, OH 44130 USA
(440) 243-1198
(440) 243-1334 Fax
Email info@codonics.com
www.codonics.com

Codonics Limited KK
New Shibaura Bldg. F1
1-3-11, Shibaura
Minato-ku, Tokyo, 105-0023 JAPAN
Phone: 81-3-5730-2297
Fax: 81-3-5730-2295