Codonics® Virtua® Firewall and Security

Technical Brief

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 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: **False** enables ports managed by Virtua software. All other ports are blocked. **True** allows for control of the Virtua software managed ports using the settings of the ***xxxFirewallPortOpen*** parameters.

> **NOTE:** Beginning with Virtua software version 5.2.3, the Windows firewall is always enabled, which provides greater security over previous software versions.

dicomFirewallPortOpen

Settings: ***Boolean*** (true or false)
Default: **True**
Description:**True** allows incoming DICOM connections. **False** blocks incoming DICOM connections.

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.

httpServiceFirewallPortOpen

Settings: ***Boolean*** (true or false)
Default: **True**
Description:**True** allows remote web browser log file access. **False** blocks web browser log file access.

smbFileShareFirewallPortOpen

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.

vncFirewallPortOpen

Settings: ***Boolean*** (true or false)
Default: **True**
Description: **True** allows remote VNC viewer programs to connect to Virtua and operate the device. **False** blocks remote VNC connections.

enableSmb1Protocol

Settings: ***Boolean*** (true or false)
Default: **False**
Description: **False** blocks the older SMB1 protocol, but allows connections to newer SMB2 and SMB3 protocols. **True** allows SMB1 connections for rare cases where connection to an older Windows or Linux PC is required.

> **NOTE:** Telnet functionality is no longer available in Virtua 5.0.0 and later SW. Changing **telnetFirewallPortOpen** will have no effect.

Virus Scanning

Virtua can provide read-only access to internal hard drive Data partitions and read-write access to Configuration 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 (some XR only)
InternalMemDrive	Factory configuration partition
SmartDrive	User Configuration partition

Access to Data partitions is read-only to prevent modification of the software. Access to Configuration partitions is read-write to allow commercial anti-virus programs to clean these partitions before the user performs a re-install of Virtua 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 configuration. The Windows 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
800.444.1198

All registered and unregistered trademarks are the property of their respective owners. Specifications subject to change without notice.
Patents: www.codonics.com/ip/patents

Copyright © 2022 by Codonics, Inc. Printed in the U.S.A. Part No. 901-160-003.03.

CODONICS®
We bring the future into focus

17991 Englewood Drive
Middleburg Heights, OH
44130 USA
+1.440.243.1198
+1.440.243.1334 Fax
Email info@codonics.com
www.codonics.com

Codonics Trading Co, Ltd.
317 Xianxia Rd. Building B
Unit 1412
Changning Dist., Shanghai
P.R. China, 200051
86-21-62787701
86-21-62787719 Fax

Codonics Limited KK
Aquacity 9F
4-16-23, Shibaura
Minato-ku, Tokyo,
108-0023 JAPAN
Phone: 81-3-5730-2297
Fax: 81-3-5730-2295