

# e-Connectivity®—Integrated Design for Confidentiality and Security

Michael Torpey, e-Connectivity Program Manager, Ortho-Clinical Diagnostics

Ortho Clinical Diagnostics e-Connectivity® Interactive System Management feature provides real-time, secure two-way interactive connection between the VITROS® 5,1 FS Chemistry, VITROS® 5600 Integrated, VITROS® 3600 Immunodiagnostic, or VITROS® ECI/ECiQ Immunodiagnostic Systems, and Ortho Clinical Diagnostics Technical Support. The features provided by e-Connectivity® include:

- **Automatic Two-Way Data Exchange;** the ability to automatically send and receive data from Ortho Clinical Diagnostics Technical Support.
- **Real-Time Alerts;** VITROS® 5600 and 3600 Systems have the ability to automatically send data to Ortho Clinical Diagnostics Technical Support when specific events or statistical trends have been observed
- **Real-Time Alerts;** Remote Connectivity; connection of the VITROS® Systems to Ortho Clinical Diagnostics that enables Remote Diagnostics, including the ability for our Technical Support personnel to perform Remote Control operation, as well as monitor and review system configuration, data, and performance information.

These features provide for automatic transfer of data regarding multiple aspects of system performance to Ortho Clinical Diagnostics Technical Support for real-time analysis. Automatic download of system software updates can be performed. Also, Ortho Clinical Diagnostics Technical Support can be provided access to the VITROS® Systems to perform Remote Diagnostics, including Remote Control operation, so that technical challenges can be solved more efficiently.

e-Connectivity® provides comprehensive security and privacy through the application of the following features to help ensure patient and laboratory confidentiality:

- Only the operator can establish a connection for

Technical Support. Ortho Clinical Diagnostics cannot connect to the system.

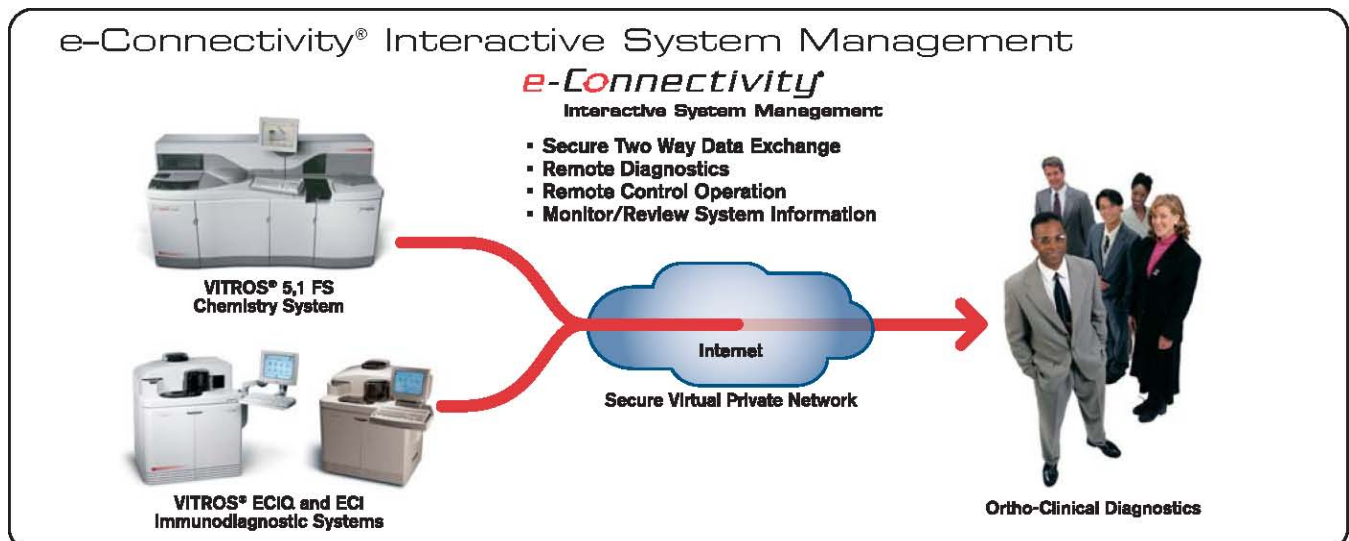
- The operator has full operational control when the system is connected to and accessed remotely by Ortho Clinical Diagnostics Technical Support.
- Ortho Clinical Diagnostics Technical Support cannot change results, information or data. The operator has full operational control for allowing access and retrieval of potential patient information used in Sample Programming and used in keyboard entries on system software screens
- Operators should configure the system so that patient information is excluded in data logger files retrieved during a data exchange
- e-Connectivity® makes use of web protocol communication technology; therefore, Ortho Clinical Diagnostics Technical Support does not have the ability to connect to any laboratory systems, computers, or networks.

## The primary features to help ensure security, privacy and confidentiality:

### Exclude Patient Information from Data Logger Files

Patient information potentially used in the Sample Programming Sample ID field can be encrypted before being entered into data logger files. Also, keyboard entries from system software screens that could include patient information such as demographics can be excluded from data logger files.

A unique encryption algorithm is assigned to each VITROS® System. No two sample IDs will be encrypted the same way. Operators and Ortho Clinical Diagnostics personnel cannot access the encryption algorithm while interacting with the system, including when Ortho Clinical Diagnostics technical support personnel access the system for Remote Connectivity. In addition, the encryption algorithm does not change.



Ortho Clinical Diagnostics technical support personnel can analyze data without access to sample IDs. However, the System software provides the ability to encrypt and decrypt sample IDs when identification of encrypted sample IDs is necessary. Ortho Clinical Diagnostics technical support personnel cannot access the encryption/decryption feature remotely and must contact the operator to decrypt and identify a sample ID.

### **Access to Hospital or Lab networks, and Lab Information Systems**

The e-Connectivity® feature uses a TCP/IP network protocol, which is incompatible and unable to communicate with the RS-232 serial communication used by VITROS® 5,1 FS and ECi/ECiQ Systems for Laboratory Information Systems (LIS) connections. The systems do not contain any on-board capability to connect and allow communication between the two different communication protocols. Therefore, when an e-Connectivity® connection is established, access to hospital or laboratory networks, and a LIS is not possible.

In addition to the features of VITROS 5,1 FS System, VITROS® 5600 And 3600 Systems can now be configured to support LIS connections via TCP/IP with ASTM/IP and HL7. This is implemented by configuring the embedded hardware Firewall / IPsec router to allow port forwarding from the VITROS® 5600 or 3600 System to the IP address and Port of the hospital network as is configured by local IT. This port forwarding is only configured and active when ASTM/IP or HL7 has been enabled on the instrument. The security of e-Connectivity is not changed to implement this except for the specific port forwarding tunnel to the customers server.

### **Downloading Software Upgrades**

The operator has full operational control to configure the system for Automatic Two-Way Data Exchange, which includes downloading software, when a connection is established from a VITROS® System to Ortho Clinical Diagnostics. All software downloaded to a System is verified with a corresponding check sum file to confirm the software integrity prior to notifying the operator that a software upgrade is available.

Also, software can only be downloaded to the system and is not automatically installed. The system automatically prepares for installation of the downloaded software and only the operator installs the software, when ready.

### **Virtual Private Network Technology**

e-Connectivity® establishes a highly secure connection between VITROS® Systems and Ortho Clinical Diagnostics for transfer of data via the Internet using Virtual Private Network (VPN) technology. A VPN is a combination of industry standard network tunneling, encryption, authentication, access control and auditing technologies/services used to securely transport traffic over the Internet. In essence a VPN creates a protected closed system connecting two networks.

In addition to VPN technology protection, e-Connectivity® utilizes IPSEC 168 bit encryption to provide the maximum security available today. IPSEC provides additional network security services over and above the VPN to encrypt and verify data being exchanged. Encryption is the transformation of data to a form, which is impossible to read without the secret key. Unencrypted data is never sent when the system is connected. A unique encryption key is established with each e-Connectivity® session and dynamically changed throughout a data exchange. 168 bit encryption technology is not known to have been compromised and is considered the industry standard for encryption and for establishing secure network links.

All data exchanged is secure and confidential using the Virtual Private Network technology described above and no unencrypted data is ever sent.

### **Connection Authorization**

All VITROS® Systems with e-Connectivity® enabled must be authorized with Ortho Clinical Diagnostics Technical Support Centers prior to receiving permission to establish a connection to Ortho Clinical Diagnostics. The enabled systems must be registered with Ortho Clinical Diagnostics Technical Support before establishing a connection between the system and Ortho Clinical Diagnostics Technical Support and before Ortho Clinical Diagnostics Technical Support can access the system remotely.

### **Automatic Connection Timeout**

An automatic connection timeout feature is included with e-Connectivity®, which is operator configurable on VITROS® Systems. A default of 20 minutes is provided. This feature automatically monitors the time length of a connection and will automatically end the connection if activity is not detected based upon the configured timeout.

### **Unique IP Addresses**

To enable the e-Connectivity® feature, each VITROS® System is assigned a unique IP address. The IP addresses assigned to all systems are internal and non-routable Internet addresses that have no capability to be used externally. Also, a proxy server is used to conceal the actual network addresses utilized for e-Connectivity®.

### **Data Exchange Database**

When Ortho Clinical Diagnostics Technical Support receives data during an Automatic Two-Way Data Exchange, the data is stored in a read-only database accessible only by authorized Ortho Clinical Diagnostics technical support personnel. The database is located in an Ortho Clinical Diagnostics affiliate and utilizes anti-virus protection software.

### **Virus Protection**

e-Connectivity® uses a closed process that minimizes exposure to viruses. VITROS® Systems use the QNX operating system which has very few known occurrences of viruses. Anti-virus protection software is actively used at the Ortho Clinical Diagnostics Technical Support Centers, and on the servers and databases supporting e-Connectivity®.

## e-Connectivity® Confidentiality and Security Frequently Asked Questions

### Q. Where can more information be obtained regarding e-Connectivity®?

- A. More information is available at *e-connectivity.com*.

### Installation and Configuration

### Q. What are the network requirements for e-Connectivity®?

- A. The following are required for a network connection:
- Customer LAN, cable modem or DSL.
  - Continuous broadband connection or direct connection to the customer LAN with access to the Internet at a speed greater than or equal to 128 kbps.
  - Support the following local area network port speeds: Automatic, 100 and 10 Mbps with full-duplex, half-duplex and automatic detection of duplex.
  - Support IPsec pass through to the Internet I.P. Address of 148.177.0.108.

Note: IPsec utilizes port 500 outbound and inbound and port 4500 outbound and inbound. These ports must be open in the local area network's firewall and allow the specified protocol.

Note: IPSEC uses protocol 50 (ISAKMP). If the network utilizes Network Address Translation (NAT), NAT-Transversal (NAT-T) must be enabled. NAT-T operates on port 4500.

- Female RJ45 connector on the network port within 20 feet of the center of the VITROS® System.
- I.P. Address, Network Mask and Gateway I.P. Address either supplied automatically via DHCP (Dynamic Host Configuration Protocol) or statically assigned by the Information Technology (IT) department and provided to Ortho Clinical Diagnostics Technical Support.

### Q. Can another network router be used for a VPN tunnel to the Cisco router used by Ortho Clinical Diagnostics instead of the supplied Ortho Clinical Diagnostics VPN Device for a VITROS® System?

- A. No. e-Connectivity® was developed with security integrated into the design. The internal VPN device that connects the VITROS® System to the Internet via a VPN tunnel ensures the security of the data. The Data is encrypted before being transferred from the system, as Ortho Clinical Diagnostics is unable to monitor the remote network connections between the system and the Ortho Clinical Diagnostics VPN Routers at Ortho Clinical Diagnostics' networking affiliate. This design also provides the ability to treat the system as if it were not on your network.

### Security and Privacy

### Q. How secure and private is e-Connectivity®?

- A. e-Connectivity® was designed with a focus on security and is integrated into the design to help ensure confidentiality, security, and privacy. Ortho Clinical Diagnostics is committed to protecting patient privacy and data security in all customer interactions and recognizes the legal and ethical obligations of customers to protect patient privacy and data security.

### Q. What data is transmitted through the VPN during a data exchange?

- A. VITROS® Systems transmit data logger information that contains data associated with the encrypted sample IDs, as well as other data, including light units, slide/cuvette density, and voltages that are used to report results. The data also includes Intellicheck® Technology verification data that helps ensure your system is operating within specification. All of this data is encrypted during transmission through the VPN tunnel.

### Q. Will a VITROS® System be able to access any other computers on my Network?

- A. No. The VITROS® Systems have an internal VPN Device with built-in VPN/Firewall capabilities that are pre-configured to build a single VPN tunnel to a VPN router located in Raritan, NJ. Other than the tunnel, the VITROS® 5,1 FS and ECi/ECiQ Systems are completely isolated from any other local or Internet network traffic. VITROS® 5600 and 3600 Systems also support LIS connections via TCP/IP with ASTM/IP and HL7 when port forwarding has been enabled by local IT. Interfaces to Laboratory Information Systems (LIS) and printers are supported through the serial ports of the VITROS® Systems which do not support network traffic communications or transmissions.

For further information, refer to the information provided above, **“Access to Hospital or Laboratory networks, and Laboratory Information Systems”**.

For further information, refer to the information provided above, **“Virtual Private Network Technology”**

### Q. What type of encryption and authentication is provided for e-Connectivity®?

- A. The VPN tunnel is secured using IPSEC protocol 50 (Encapsulating Security Payload). Triple Data Encryption Standard (3DES), SHA authentication, and the Diffie-Hellman key agreement protocol are all utilized to ensure the data is secure. The Encapsulating Security Payload (ESP) protocol (protocol 50) is used to provide data confidentiality and authentication. Encryption is accomplished by using a symmetric key for both communicating parties (the VPN Device with the VITROS® Systems and Ortho Clinical Diagnostics computing affiliate's Cisco router) to encrypt and decrypt the data they exchange.

## e-Connectivity® — Integrated Design for Confidentiality and Security

The HMAC-SHA algorithms are used to provide authentication functionality. SHA uses a secret key and the variable-length input data to produce fixed-length output data known as a hash value.

The Diffie-Hellman key agreement protocol allows the two VPN endpoints to exchange a secret key over the Internet without any prior secrets. The Internet Engineering Task Force (IETF) formally defines the above standards on their website at [www.ietf.org](http://www.ietf.org):

- 3DES in Request for Comments (RFC) 1851, *The ESP Triple DES Transform*
- HMAC-SHA in RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*
- Diffie-Hellman in RFC 2631, *Diffie-Hellman Key*

**Q. Is a firewall in place to prevent unauthorized access to the VITROS® Systems?**

A. Yes. The Ortho Clinical Diagnostics VPN Router features an ICSA (International Computer Security Association) certified dynamic firewall. This device prevents any unauthorized access to the VITROS® Systems. It only allows communication from the systems through the VPN tunnel to the Ortho Clinical Diagnostics VPN router. The system is not exposed directly to the Internet.

