

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

Ortho Clinical Diagnostics e-Connectivity® Technology Interactive System Management feature provides real-time, secure two-way interactive connection between the VITROS® 5,1 FS Chemistry, VITROS® 5600 Integrated, VITROS 4600® Chemistry, VITROS® 3600 Immunodiagnostic, or VITROS® ECI/ECiQ Immunodiagnostic Systems, and Ortho Clinical Diagnostics Technical Support.



The features provided by e-Connectivity® Technology include:

Automatic Two-Way Data Exchange

The ability to automatically send and receive data from Ortho Technical Support.

Real-Time Alerts

VITROS® 5600, 4600 and 3600 Systems have the ability to automatically send data to Ortho Technical Support when specific events or statistical trends have been observed.

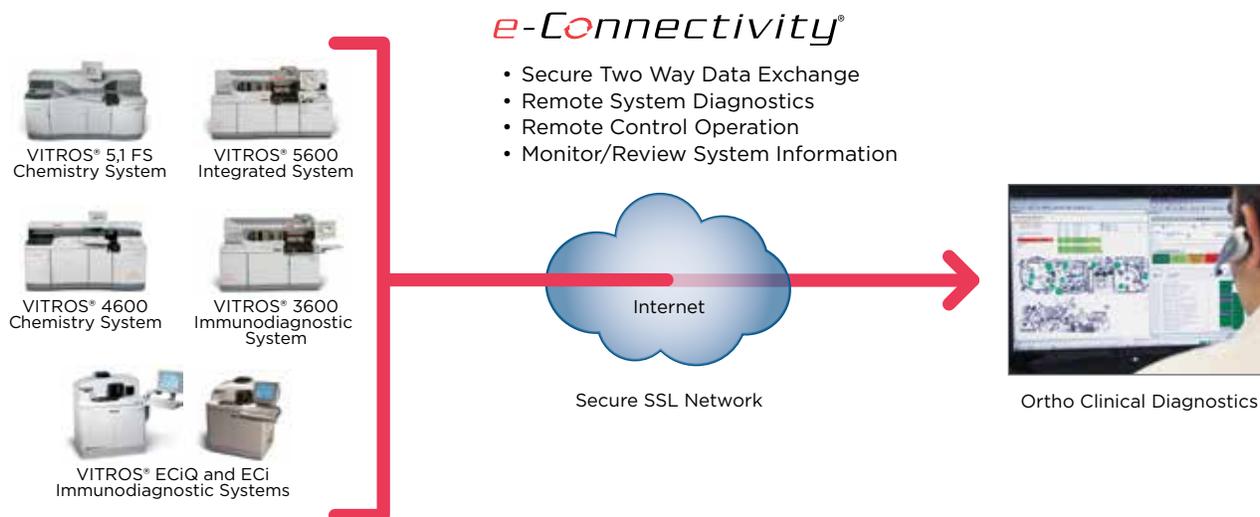
Real-Time Alerts

Remote Connectivity; connection of the VITROS® Systems to Ortho 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 Technical Support for real-time analysis. Automatic download of system software updates can be performed. Also, Ortho 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® Technology 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 cannot connect to the system.
- The operator has full operational control when the system is connected to and accessed remotely by Ortho Technical Support.
- Ortho 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 Technical Support does not have the ability to connect to any laboratory systems, computers, or networks.



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 personnel cannot access the encryption algorithm while interacting with the system, including when Ortho technical support personnel access the system for Remote Connectivity. In addition, the encryption algorithm does not change.

Ortho 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 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, 4600 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, 4600 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. 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.

Secure Socket Layer Network Technology

e-Connectivity® Technology establishes a secure connection between the VITROS® Systems and Ortho for transfer of data via the Internet using Secure Socket Layer (SSL) technology. A SSL is a combination of industry standard network tunneling, encryption, authentication, access control and auditing technologies/services used to securely transport data over the Internet. In essence a SSL creates a protected closed system connecting two networks. All data exchanged is encrypted, secure and confidential using Secure Socket Layer technology.

Connection Authorization

All VITROS® Systems with e-Connectivity® enabled must be authorized with Ortho Technical Support Centers prior to receiving permission to establish a connection to Ortho. The enabled systems must be registered with Ortho Technical Support before establishing a connection between the system and Ortho Technical Support and before Ortho 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 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 technical support personnel. The database is located in an Ortho 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 Technical Support Centers, and on the servers and databases supporting e-Connectivity®.

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

A: More information is available at orthoclinicaldiagnostics.com

INSTALLATION AND CONFIGURATION

Q: What is required to enable my VITROS® Systems for e-Connectivity®?

A: A standard on-site service call will be required to install e-Connectivity®.

In addition, the lab network requirements are:

- Customer LAN
- 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 SSL traffic to the Internet Port 443 Note: SSL utilizes port 443 outbound and inbound. This port must be open in the local area network's firewall.
- Female RJ45 connector on the network port within 6 meters of the center of the 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 Technical Support

Q: Can another network device be used to connect the VITROS® Systems to Ortho?

A: No. e-Connectivity® Technology was developed with security integrated into the design. The VITROS® Systems provides a software firewall that is configured to connect only to OCD and enables specific ports for specific use cases (ie, LIS communications, remote review, and backups).

Q: Will e-Connectivity® interfere with the performance of my system?

A: No. e-Connectivity® Technology is fully integrated into your systems so that routine system operation is maintained.

Q: How will e-Connectivity® Technology be priced?

A: Currently there is no charge for e-Connectivity® Technology, and it is considered part of the product offering package with the purchase of an analyzer.

Q: How will Ortho use the collected data?

A: Our Technical Support Centers and Field Engineers will analyze it for existing or potential issues in individual systems, so service can be performed as quickly and conveniently as possible. In addition, analysis from anonymized analyzer performance data from multiple systems may point to needed software updates as well as feature development needs for future systems.

Q: Can I use a DSL/Cable internet connection?

A: Yes, with exception. The DSL/Cable line must support an Ethernet Connection. The OCD e-Connectivity® Technology solution currently does not support password input as required by some service providers.

SECURITY AND PRIVACY

Q: How secure and private is e-Connectivity® Technology?

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

Q: What data is transmitted through the SSL during a data exchange?

A: VITROS® Systems transmit files that contain data associated with the results, condition codes, and other data that may be useful to troubleshoot the system. The data also includes verification information that helps ensure your system is operating within specification. All of this data is encrypted during transmission through the SSL tunnel.

Q: Will Ortho be able to access any other computers on my Network?

A: No. The VITROS® Systems have built in firewall capabilities that are pre-configured to build a single SSL tunnel to an infrastructure located in Raritan NJ. Other than the tunnel, the devices are completely isolated from any other local or Internet network traffic. The devices also may support other connections via TCP/IP with ASTM/IP when ports have been enabled.

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

A: The SSL tunnel is secured using open SSL with a minimum 128 bit encryption. Encryption is accomplished by using a server side certificate from an authorized authority to encrypt the data exchanged.

Q: How often does the VITROS® Systems exchange data with the e-Connectivity® Technology infrastructure at Ortho?

A: Under normal conditions an upload of data will take place once daily at a configurable time. However, the user can initiate an additional data upload at any time, typically when contacting Ortho for support.

Q: How much data (size) is normally exchanged between the VITROS® Systems and the e-Connectivity® infrastructure at Ortho?

A: Under normal conditions the size of the daily upload will be ~25MB. S/W downloads may occur a few times per year and could be ~500MB.

Q: Do my LIS and e-Connectivity® talk through the same Ethernet connection?

A: LIS connection can be connected through the Ethernet port to share a link with e-Connectivity®, or may be routed through the Serial Port using a Serial to Ethernet adaptor. If routed through the Serial Port, the customer will need to provide two network ports

AGREEMENT METHOD

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

A: Yes. The systems contain a firewall. This solution prevents any unauthorized access to the System. It only allows communication from the system through the SSL tunnel to the Ortho e-Connectivity® Technology infrastructure. The system is not exposed directly to the Internet.

