

e-Connectivity[®] Technology for VITROS[®] Analyzers

Ortho Clinical Diagnostics e-Connectivity Technology Interactive System Management feature provides real-time, secure two-way interactive connection between the VITROS Family of Systems* and Ortho Care[™] Services.

Benefits of e-Connectivity Technology



Increased Uptime

Customers with connected analyzers save 1.5 calls/year leading to improved analyzer availability.



Faster Resolution

Ortho Care Representatives have information to resolve issues either by phone, or in advance of a service visit. Automatic scheduled transfer of system performance data is provided to the Ortho Care team for proactive analysis and resolution.



Inventory Management

Customers with e-Connectivity can enroll in Ortho PlusSM Inventory Management program (OPIM). The program allows customers to forecast and manage inventory automatically. OPIM is not available in all countries.



Time-Saving Updates

Receive the latest software version and assay information when released. A system notification is sent through the analyzer and is installed by the user when convenient.

Commitment to Cyber Security

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.



SECURE SSL/TLS

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) or Transport Layer Security (TLS) technology.

EXCLUDE PATIENT INFORMATION

Personally Identifiable Information (PII) is **not** collected in the accessible files. Additionally, the Sample ID assigned to the patient sample is encrypted by the software.

LIMITED ACCESS

To guarantee high security level and maintain patient data privacy and confidentiality, e-Connectivity limits access to specific hard drive directories. Only analyzer and assay performances data logger files can be collected.

*VITROS[®] 5,1 FS Chemistry, VITROS[®] 5600 Integrated, VITROS 4600[®] Chemistry, VITROS[®] 3600 Immunodiagnostic or VITROS[®] XT 7600



e-Connectivity Connection Model

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)** or **Transport Layer Security (TLS)** technology.

SSL/TLS technology is a combination of industry standard network tunneling, encryption, authentication, access control and auditing technologies/services used to securely transport data over the Internet. SSL creates a protected closed system connecting two networks. **All data exchanged is encrypted, secure and confidential using FIPS 140 compliant encryption to secure the data.**

e-Connectivity Technology was developed with security integrated into the design:

- Does not require an extra network device.
- No email server or internet browser available to the user.
- Fully integrated into your systems eliminating routine system operation.

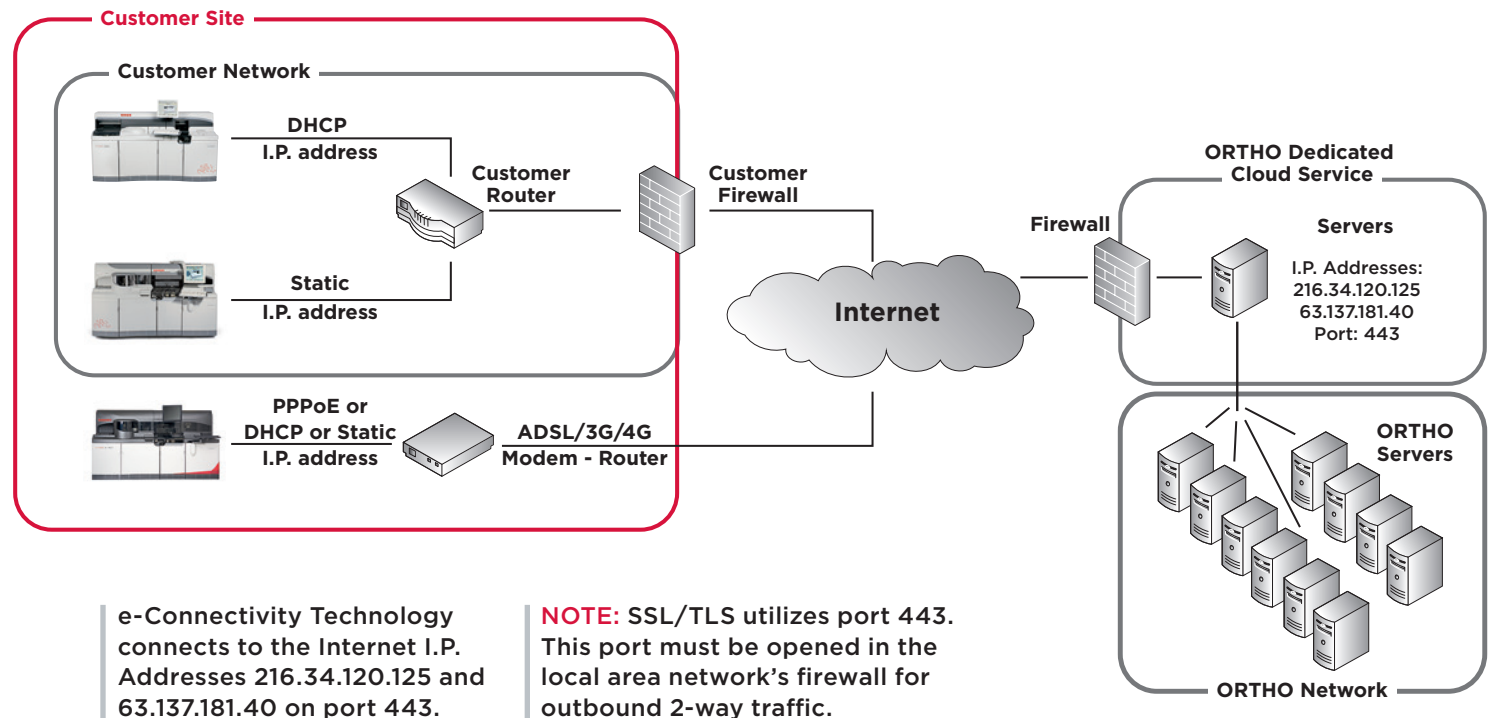
For specific use cases where internet access is required (ex. LIS communications, e-Connectivity), the VITROS systems provides a firewall that is configured to connect only to Ortho and only enables specific ports.

On VITROS systems, the SSL/TLS tunnel is secured using a minimum 128-bit encryption. Encryption is accomplished by using a server side certificate from an authorized authority to encrypt the data exchanged.

SSL/TLS (version 1.0, 1.1, 1.2) with redacted ciphers per NIST/FIPS guidance

How to Connect Your Analyzer

e-Connectivity Technology requires a continuous broadband connection or direct connection to the customer LAN with access to the Ortho Clinical Diagnostics e-Connectivity server at a speed greater than or equal to 128 kbps.



e-Connectivity Technology connects to the Internet I.P. Addresses 216.34.120.125 and 63.137.181.40 on port 443.

NOTE: SSL/TLS utilizes port 443. This port must be opened in the local area network's firewall for outbound 2-way traffic.



Transmitted Data & Encryption

VITROS systems transmit files containing data associated with the results, condition codes, and other data that may be useful to troubleshoot the system along with verification information to ensure your system is operating within specification.

VITROS systems data logger files are automatically processed and managed with restricted access during their transfer to Ortho e-Connectivity servers. **Only designated Ortho employees with passwords have access to the e-Connectivity data.**

e-Connectivity delivers software safely and securely to the analyzers. All software downloaded is verified prior to notifying the operator that an upgrade is available. Software installation is always performed by system operator and cannot be done automatically.

Personally Identifiable Information (PII)

The e-Connectivity Technology limits the data exchange to specific hard drive directories only. These directories contain analyzer data logger files that do

not contain Personally Identifiable Information. By default, all sample IDs are encrypted (independently from the

SSL/TLS encryption) and can only be decrypted at the analyzer interface. Encryption is unique to each analyzer.

Network & Systems Security

The VITROS systems have built in firewall capabilities that are pre-configured to allow SSL/TLS secure access to Ortho Infrastructure only.

Other than the SSL/TLS, the devices are completely isolated from any other local or Internet network traffic. The devices may

also be configured by customers to support other connections via TCP/IP with ASTM/IP, HL7 when ports have been enabled.

Virus and Malware

The VITROS systems use an embedded real-time operating system in lieu of standard consumer desktop operating systems. There are currently no documented cases of a virus specifically designed for QNX. There are no existing virus or malware

scanners for the QNX Neutrino RTOS, and Ortho does not anticipate a need for these types of products on the VITROS systems. Ortho dedicated cloud service has an agreement with Ortho and provides

server patching, antivirus and security scan on the infrastructure. Ortho Dedicated Cloud service is an extension of Ortho Cybersecurity policy and plan.

Standard and References

The Ortho dedicated Cloud Service is certified ISO 27001.

In compliance with electronic record 21 CFR Part 11.

Ortho Clinical Diagnostics utilizes a partner, Parametric Technology Corporation (PTC), to host the cloud solution. PTC and Ortho Clinical Diagnostics have signed a confidentiality and non-disclosure (CNDA/NDA) agreements in place.

The e-Connectivity model is compliant with the General Data Protection Regulation (GDPR) in place in the European Union to provide common standards for the protection of data across the EU.

The e-Connectivity model is approved by the English National Health Service (NHS) network (N3), and the U.S. Department of Veteran Affairs.



Frequently Asked Questions

1

What's the charge for e-Connectivity?

▶ There is no charge for e-Connectivity.

2

How do I prepare my VITROS Systems for e-Connectivity?

▶ You will need to provide a broadband connection with access to the Internet at a speed greater than or equal to 128 kbps. The Internet connection can be DSL, cable or provided through a Local Area Network (LAN). Ortho provides the hardware and software necessary for e-Connectivity. See e-Connectivity Network Connection Specifications and Network Form for further information.

3

How is e-Connectivity installed?

▶ Your VITROS System requires a standard on-site service call for installation or configuration of the components necessary for e-Connectivity. It is often part of instrument installation. You will need to provide local network information so that the Ortho Service Representative can configure the e-Connected Systems. This information is collected on the e-Connectivity Network Connection Specifications and Network Form, which can be completed and returned to Ortho Care Technical Support.

4

Will e-Connectivity interfere with the performance of my VITROS Systems?

▶ No. e-Connectivity is fully integrated into your system so that routine system operation is maintained. For example, Automatic Two-Way Data Exchange, including software downloads, can occur without interruption to continuous system operation, including during sample and assay processing.

5

How will Ortho use the collected data?

▶ Our Ortho Care Technical Support centers and field engineers will analyze data for current and potential issues on individual systems, enabling service to be performed as quickly and conveniently as possible. In addition, aggregated data from multiple systems may point to needed software updates, as well as feature development needs for future systems.

VIRTUAL PRIVATE NETWORK (VPN)

6

Will I need a VPN on my hospital network (LAN)?

▶ No, you need to assign an IP address (Static or DHCP) and allow bidirectional traffic over port 443 through the site firewall. The assigned IP address will be configured by the Ortho Care installation team. The IP address and a working connection are needed at the time of installation.

7

Will I need to configure the instrument's connection?

▶ No. An Ortho Care Service Representative will configure the e-Connected Systems with local network information provided by you. However, a Key Operator password allows you to control and modify this configuration as well.

LOCAL AREA NETWORK CONNECTION CONFIGURATION

8

Will I need to configure my firewall(s)?

▶ **Possibly.** You will need to ensure that the e-Connected System on your network can communicate with Ortho (216.34.120.125 and 63.137.181.40) on TCP port 443 outbound 2-way traffic. This is the standard port used for SSL/TLS connections. If you have multiple firewalls, this configuration must be done for each firewall involved in the route. **It is extremely important that these ports are open for a timely and successful install of e-Connectivity and support to your System.**

9

Will I need to configure my router(s)?

▶ **Possibly.** If you have a router providing Network Address Translation (NAT), you will need to ensure that it supports NAT Traversal (NAT-T). NAT-T is used by the SSL/TLS protocol to allow for the traversal of encrypted packets across NAT-ed environments. If you have multiple routers, you must do this for each router involved in the route.

DSL/CABLE CONFIGURATION

10

How is DSL/Cable installed in my laboratory?

▶ You will need a local service provider (typically the telephone company or cable company) to install the DSL/Cable line into your laboratory. The provider should supply the equipment necessary to connect the Systems to the Internet. Please note that the equipment must support an Ethernet connection (i.e. not USB only).



Frequently Asked Questions

11

How do I ensure the DSL/Cable line is working?

▶ You should communicate with the service provider regarding how best to determine that the DSL/Cable line is functioning correctly. Several providers will perform all of the necessary work. Other providers will deliver the equipment and you will be required to make the connections and configure the equipment. If the service provider does the latter, then follow their instructions to install, configure and test it before Ortho connects the System.

12

How do you configure the connection if IT requires a login to the Internet Service Provider?

▶ The Ortho Care Service Engineer can enter the appropriate information into the e-Connected System. Some hardware (DSL and Cable modems) can support the configuration of this information. If this is the case, Ortho would prefer that the information is stored in the hardware supporting the connection.

OPERATING SYSTEM

13

What operating system is used on the VITROS Systems?

▶ The VITROS systems use QNX® RTOS as operating system. This is a real-time POSIX-compatible operating system designed for use in embedded devices. These systems do not contain any Microsoft® components. “QNX” and “Neutrino” are registered trademarks of QNX Software Systems, Ltd. “Microsoft” is a registered trademark of Microsoft Corporation.

CONFIDENTIALITY, SECURITY AND PRIVACY

14

How secure and private is e-Connectivity?

▶ Ortho Care Technical Support cannot change results, information or data. By default, all sample IDs are encrypted when they are copied in data logger files. If the Sample ID encryption is disabled, Ortho Clinical Diagnostics strongly recommends to not use Patient Information in the Sample ID field.

15

What data is transmitted through e-Connectivity?

▶ e-Connected systems transmit logged System information including results and Intellicheck® Technology verification data that can assist in ensuring your system is operating within specification. The system may also be capable of receiving software upgrades and assay information. All of this data is encrypted during transmission through the SSL connection.

16

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

▶ **Yes.** All VITROS systems include a firewall that blocks all incoming network traffic to prevent any unauthorized access. Only customer configured outbound traffic to Ortho e-Connectivity server and customer configured LIS servers is allowed.

17

Are my e-Connected Systems protected from viruses or other computers that may attempt to access the systems?

▶ e-Connectivity uses a secure connection mode. All assets at Ortho that could access this connection are maintained with the latest anti-virus and patches available per Ortho corporate standards and policies. The use of a firewall on the VITROS Systems prevents any unauthorized access to the system. It only allows communication from the VITROS System through the SSL/TLS connection to Ortho. The system is not exposed directly to the Internet and is protected by a firewall.

