Welch Allyn
PartnerConnect ®

Welch Allyn PartnerConnect is an innovative feature of the Welch Allyn Partners in Care℠ Services program that enables remote diagnostics and management of devices and systems. Software installations, updates and upgrades can all be delivered and performed remotely. PartnerConnect also enables preemptive service capabilities on the Welch Allyn platform, allowing our Partners in Care Technical Support Center to remotely view your devices and system configurations via the Internet to provide:

- Device and system operational support
- Enhanced troubleshooting
- License delivery

- Software updates and enhanced options
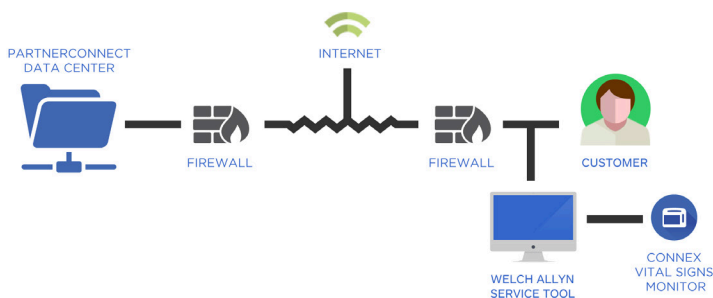- Installation assistance

Why Welch Allyn PartnerConnect?

PartnerConnect is designed to enable remote troubleshooting and diagnostics with minimal time and effort on your part. Automated device-related data transfers supply our service technicians with near real-time information, expediting problem resolution.

- Helps you schedule required maintenance to ensure device availability with maximum up-time
- Helps optimize device deployment to reduce total cost of ownership
- Lets you install firmware and software upgrades/updates at your convenience to minimize patient care disruption

- Enhances troubleshooting and installation assistance from our Technical Support Center and your IT/biomed department
- Enhances learning opportunities through troubleshooting and quick issue resolution via screen-sharing capability
- HIPAA compliant. **No patient identifiable data transferred.**

Device Data Flow

PARTNERCONNECT DATA CENTER

INTERNET

FIREWALL

FIREWALL

CUSTOMER

WELCH ALLYN SERVICE TOOL

CONNEX VITAL SIGNS MONITOR

Just like a browser accessing a website, PartnerConnect remote access software communicates with the PartnerConnect server using your existing network connection—with the Internet access and network security that's already in place, so there's no impact to your existing IT infrastructure.

Highly Secure

Welch Allyn recognizes that security is one of your primary concerns. Welch Allyn PartnerConnect utilizes your current network security model out into the cloud environment, ensuring that critical certification and compliance requirements are met. The system offers intentional granular attended, unattended or one-time control over user access, and can offer easy-to-use audit and tracking capabilities. It is important to note that the PartnerConnect Cloud solution is delivered via our ISO 27001 certified and SSAE 16/SOC 2 audited on-demand datacenters.

Outbound Information

PartnerConnect is noninvasive and never enters your network. The PartnerConnect Agent, installed locally, only sends device-relevant service data, *never patient identifiable data*, out of your network—so you'll never have to accept any outside connections for PartnerConnect to operate—and addresses are never revealed outside the network. PartnerConnect Agents are configured with FIPS mode enabled, which imposes the stricter security standards that are often required in government settings. The PartnerConnect Agent functionality along with our remote technical support sessions capabilities (described below) create a full service support offering.
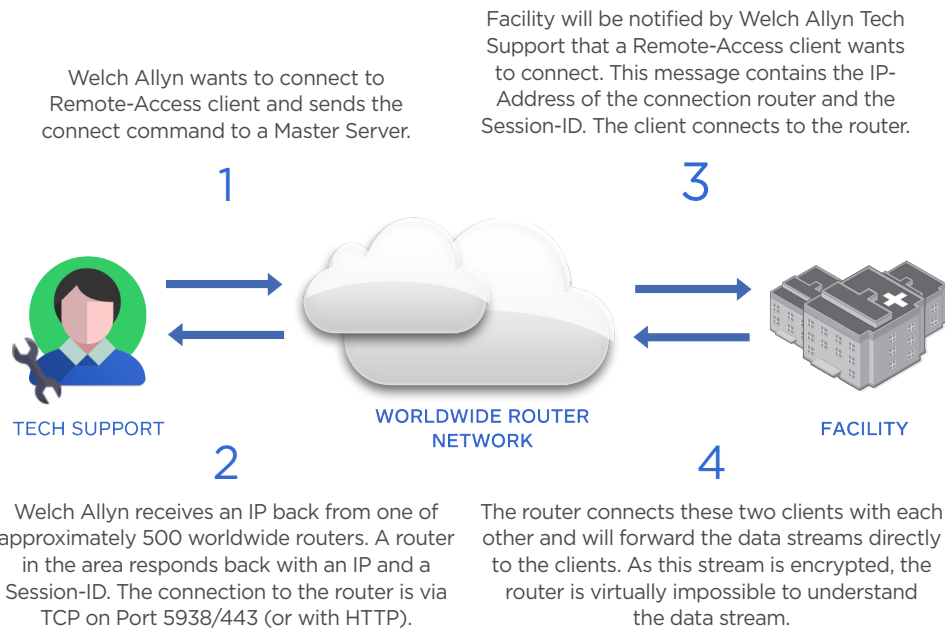
Encryption and Authentication

PartnerConnect works with a complete encryption based on RSA public/private key exchange and AES (128-Bit) session encoding. As the private key never leaves the client computer, it is ensured by this procedure that interconnected computers—including any routing servers—make it virtually impossible to decipher the data stream. Each PartnerConnect client has already implemented the public key of the master cluster and can thus encrypt messages for the master server and check the signature of the master, respectively. The PKI (Public Key Infrastructure) effectively prevents "Man-in-the-middle-attacks." In addition to the encryption, the password is never sent directly but only through a challenge-response procedure and is only saved on the local computer.

The connection IDs are automatically generated by the service itself based on hardware characteristics. The master servers check the validity of the ID before every connection so it is virtually impossible to generate and use fake IDs.

Delivery of Remote Technical Support

Included with PartnerConnect is our remote technical service capability. Welch Allyn service technicians have the ability to remotely access your systems to help perform upgrades, troubleshoot an issue or check performance. These connections allow real-time diagnostics of non-patient device data to help Welch Allyn technical support:

- Deliver the appropriate service level, while ensuring that all security measures are in place
- Access system event and error logs to define conditions
- Observe workflow to help isolate issues more quickly

Welch Allyn wants to connect to Remote-Access client and sends the connect command to a Master Server.

Facility will be notified by Welch Allyn Tech Support that a Remote-Access client wants to connect. This message contains the IP-Address of the connection router and the Session-ID. The client connects to the router.

1

3

TECH SUPPORT

WORLDWIDE ROUTER NETWORK

FACILITY

2

4

Welch Allyn receives an IP back from one of approximately 500 worldwide routers. A router in the area responds back with an IP and a Session-ID. The connection to the router is via TCP on Port 5938/443 (or with HTTP).

The router connects these two clients with each other and will forward the data streams directly to the clients. As this stream is encrypted, the router is virtually impossible to understand the data stream.

Creation of a Remote Support Session and Types of Connections

Remote connections may be configured to allow automatic approval, or only established upon your request and approval, and will always be limited locally at your site. Multiple remote connections can be opened to allow other Welch Allyn subject matter experts to connect instantly along with Welch Allyn technical support.

When creating a session, our remote service determines the optimal type of connection. After the handshake, a direct connection is typically established via either UDP or TCP (even behind standard gateways, NATs and firewalls).

The remote service will work if standard access to the Internet is possible. As an alternative to port 443 HTTPs, port 80 HTTPs is also available. In addition, it is also possible to open only port 5938 TCP on the outgoing side. Data traffic should then be able to pass through on this port without any problems. In some cases, port 17001 may be used for remote access to your systems, contingent upon the specific application being used for connections.
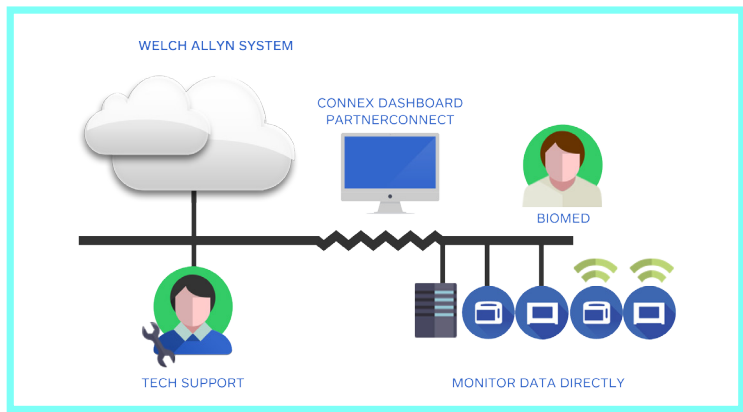
Application/Service	Port #	Protocol	Connection
PartnerConnect Agent	80/443	TCP(HTTPs)	External
TeamViewer® Remote Support Session	80/443 & 5938	TCP	External
Welch Allyn RSDS Gateway	3011 & 3030	TCP	Local
Axeda® Desktop Server	5920	TCP/UDP	Local
Axeda® Remote Desktop	443/17002, 80/17001	TCP	External
Welch Allyn Service Monitor	283	TCP	Local
Welch Allyn Service Tool	5094/5095	TCP	External

Welch Allyn Service Tool

System	Verify that the host computer meets the following hardware and software requirements: • Windows 7 or Windows XP with SP3 • Net Framework 3.5 (included with installation) • Processor: 400 MHz Pentium processor or equivalent (minimum); 1GHz Pentium processor or equivalent (recommended) • RAM: 1 GB (minimum); 2 GB (recommended) • Hard disk: Up to 10 GB of available space may be required • CD ROM drive • Display: 800 x 600, 256 colors (minimum); 1024 x 768 high color, 32-bit (recommended) • USB: 2.0
Networks	Internet connection required to download files. When you use the service tool to license or download firmware, network traffic travels over nonregistered ports. You must open these ports for TCP/IP and UDP traffic on your PC or network firewall: Ports Description • 5093, 5094 Welch Allyn licensing server • 5920 Welch Allyn PartnerConnect
Devices	Visit www.welchallyn.com for product service software compatibility information.

Connex® Dashboard/Service Monitor Technical Guidelines

Server/System	The Service Monitor Server relays technical and service messages and files to and from the medical device and the Connex Dashboard Server (PartnerConnect). We recommend a dedicated server for the Service Monitor to separate the clinical and service related data. The Service Monitor Server software is compatible with the following operating systems: • Microsoft Windows® 2008 R2 (64-bit) • Windows 7 (32-bit and 64-bit) • Windows 7 Embedded
	The following are our recommended minimum specifications for the Service Monitor Server (Virtual or Physical): • Dual-core 32-bit 2.0GHz • 4 GB memory • 40 GB of free disk space for software, log files and Interface transaction information2 • 100/1000 MB Ethernet Server specifications will need to be adjusted to the size of your facility and the number of connected devices.
Networks	Welch Allyn Service Software is a flexible solution that allows device service related messages and files to be transferred via a network that supports TCP/IP version 4. Internet access is required for the server hosting the Service Monitor.
Devices	Visit www.welchallyn.com for product service software compatibility information.

For more information please contact Welch Allyn Customer
Support at 1.800.535.6663 or visit www.welchallyn.com/service

WelchAllyn®
Advancing Frontline Care™