

Welch Allyn Connex[®], VitalsLink by Cerner, and Connex CSK Network installation

Best practices overview



Advancing Frontline Care™

© 2015 Welch Allyn. All rights are reserved. To support the intended use of the product described in this publication, the purchaser of the product is permitted to copy this publication, for internal distribution only, from the media provided by Welch Allyn. No other use, reproduction, or distribution of this publication, or any part of it, is permitted without written permission from Welch Allyn.

Welch Allyn assumes no responsibility for any injury to anyone, or for any illegal or improper use of the product, that may result from failure to use this product in accordance with the instructions, cautions, warnings, or statement of intended use published in this manual.

For patent information, please visit www.welchallyn.com/patents.

For information about any Welch Allyn product, or to contact your nearest Welch Allyn representative, go to www.welchallyn.com/about/company/locations.htm.

Manual DIR 80018745 Ver C



Welch Allyn, Inc.
4341 State Street Road
Skaneateles Falls, NY 13153 USA



Welch Allyn Limited
Navan Business Park
Dublin Road, Navan
County Meath, Republic of Ireland

www.welchallyn.com

WelchAllyn®

Contents

1 - Introduction	1
About this document	1
Systems overview	1
2 - Best practices.	3
Required network settings and configurations	3
Recommended network settings and configurations	4
General network settings and configurations	5

1

Introduction

About this document

This document lists required, recommended, and basic settings and configurations for networks using Welch Allyn medical devices and systems. For vendor-specific required, recommended, and basic settings and configurations, go to the following web site: www.welchallyn.com/networkbestpractices.

Systems overview

Welch Allyn connected workstations, servers and patient monitors utilize standards based communications protocols including, but not limited to, 802.3 for wired Ethernet and 802.11a/b/g for wireless. This guide specifies the requirements and recommendations needed to successfully complete and maintain a Welch Allyn patient monitoring system in your wireless or wired network.

Implementation and maintenance of a stable and usable integrated network is the sole responsibility of the customer.

Although ultimately your responsibility, Welch Allyn recommends that you conduct a hazards analysis per IEC 80001 to determine if any issues exist that should be mitigated to ensure your patients safety.

2

Best practices

Required network settings and configurations

These configurations and settings are required to establish a durable connection between Welch Allyn devices and the wireless network. Failure to comply with these requirements will result in a failure to connect to the network, repeated disconnects or extended loss of telemetry data. Requirements in this section can be modified by requirements listed in the appropriate vendor-critical requirements documents.

Best practice	Affected types	Without best practice
<p>Authentication/encryption All versions:</p> <ul style="list-style-type: none"> • WEP 64 and 128 • WPA2 Personal <p>Radio software versions 3.00.01 and later also support:</p> <ul style="list-style-type: none"> • WPA2 Enterprise (EAP-TLS, EAP-TTLS, EAP-PEAP [MSCHAPv2]) <p>CSM radio also supports:</p> <ul style="list-style-type: none"> • WPA/WPA2 (TKIP), EAP-FFAST, PEAP-GTC (one-time passwords are not supported), PEAP-TLS <p>Note Welch Allyn CVSM radios use CCMP encryption. If TKIP is also enabled on the SSID, the 'CCMP and TKIP' security option must be selected on the device's configuration screen.</p>	Wireless	Other encryption methods not supported. No connectivity.
<p>Channel Switch Announcement (CSA) Disable</p>	Wireless	When CSA is enabled, data loss when changing channels may occur.
<p>DFS If DFS channels are used – a practice discouraged for patient monitors – the SSID must be broadcast when using CVSM radio SW V3.00.02 or earlier.</p>	Wireless	Welch Allyn devices will not initiate a connection on DFS channels unless the appropriate SSID is detected via WLAN Beacon.
<p>Interference Signal to Noise Ratio (SNR) ≥ 15dB</p>	Wireless	High noise level causes dropped packets.
<p>IP address assignment Must be performed through renewable DHCP lease (DHCP fixed to MAC is acceptable)</p>	Wireless and wired	The device cannot connect to the network without an IP address.
<p>Regulatory Domain Advertisement 802.11d announcement enabled</p>	Wireless	Failure to include a country code in 802.11 Beacon frames degrades connectivity and roaming performance.
<p>Signal strength Primary wireless signal: RSSI Value ≥ -65dBm (when 802.11a APs set to 25mW). A secondary wireless signal of -70dBm or better is highly recommended for redundancy. For proper Tx/Rx balance, RSSI readings must apply when APs at transmitting at 25mW or less.</p>	Wireless	The device radio transmits at 25mW power (nominal). AP signal strength and radio signal strength must be balanced. If not, dropped packets and loss of connectivity can result.
<p>Data rates Enable 802.11 a/g data rates of 6Mbps and higher. In areas where RSSI minimums (both primary and secondary) cannot be guaranteed, enabling all 802.11 data rates may be necessary to increase transmission range. The maximum data rate supported for CSM is 54Mbps for 802.11 a/g and 72Mbps for 802.11n.</p>	Wireless	Disabling low data rates can introduce coverage issues leading to increased disconnects and dropped data, particularly in areas with higher interference or congestion.

Best practice	Affected types	Without best practice
Ethernet connections to CVSM/CIWS/CSM must be configured to robustly support device with max data-rate of 100Mbps.	Wired	Mismatched configuration or autonegotiation failures may cause disconnects.
SSID name Maximum length of 32 characters ¹	Wireless	The radio cannot be configured.
Required ports open <ul style="list-style-type: none"> TCP: 281, 283 UDP for Spot LXi: 44435-44436 UDP for CVSM: 291, 7711-7719 	Wireless and wired	Connections cannot be established.
Rendezvous For Spot LXi: <ul style="list-style-type: none"> Allow UDP broadcasts (port forwarding) on ports 44435-44436. <p>For CVSM and CSM, perform at least one of the following:</p> <ul style="list-style-type: none"> Configure the device with a fixed IP address of the Connex server Configure the DNS server to resolve a locally defined DNS identity to up to three Connex server IP addresses. CVSM devices must be configured with DNS identity² Configure the DHCP server to support option 60 lookup of fixed Vendor Class Identifier "welchallyn-nrs." The corresponding option 43 value is an encapsulated list of up to three Connex Server IP addresses.³ Allow UDP broadcasts (port forwarding) on ports 7711-7719 (CVSM only) 	Wireless and wired	Connections cannot be established from the Welch Allyn VLAN to the server.
SSID/Radio settings <ul style="list-style-type: none"> a band (required for continuous monitoring, recommended for episodic data) b/g band (supported but not recommended for episodic data) a/b/g are acceptable for ConnexVM, Cerner and CSK CVSM/Spot LXi radios can be configured for one of the following two options: <ul style="list-style-type: none"> 802.11a 802.11/b/g CSM radio can be configured for one of the following four options. Band steering is supported for the first two options. <ul style="list-style-type: none"> 802.11a/b/g 802.11a/b/g/n (SISO) 802.11b/g 802.11b/g/n (SISO) 	Wireless	Loss of connection and data, patient monitor will not connect.

1. For CVSM software versions 1.7X and earlier and Spot LXi, there is a 16 character maximum.

2. Requires CVSM software version 2.00.05 and later.

3. Requires CVSM software version 2.10.00 and later with radio firmware versions 3.00.02 and later.

Recommended network settings and configurations

The best practices and configuration settings listed in the following table are recommended for best performance. Increased data packet loss or occasional disconnects are likely if these recommendations are not followed. Recommendations in this section can be modified by requirements listed in the appropriate vendor-critical requirements documents.

Best practice	Affected types	Without best practice
802.1X Authentication When using EAP (certificates) for authentication, enable OKC (opportunistic key caching) on the controller	Wireless	Increased chance of disconnect during roaming.
QoS Welch Allyn data should have priority over other data. Welch Allyn data is configured for 802.11e Access Category Voice. Hardware Quality of Service (QoS) support should be configured to map 802.11e QoS bits to a hard-wired tag	Wireless and wired	Increased probability of dropped patient data packets on busy wireless networks.
Roaming across subnets Keep the Welch Allyn wireless VLAN flat (no roaming across subnets or wireless controllers)	Wireless	Success for roaming across subnets depends on the hospital's Layer-3 network. Hospital is responsible for validation of proper roaming across subnets.
Rules/Firewall Use separate rules and roles for Welch Allyn patient data and other IT data. Rules and roles should be identified using Welch Allyn specific names.	Wireless	IT changes to the wireless controller that inadvertently affect patient monitoring are more likely. Patient data subject to issues on wired network such as broadcast storms. Shorter battery life for patient monitors.
Separate VLAN Keep Welch Allyn patient monitors on their own VLAN and SSID	Wireless and wired	IT changes to the wireless controller that inadvertently affect patient monitoring are more likely. Patient data subject to issues on wired network such as broadcast storms. Shorter battery life for patient monitors.
Wireless Multimedia (WMM) Enabled	Wireless	Monitors will disconnect during movement.

General network settings and configurations

The following best practices should be followed to maintain a robust system suited for medical patient monitoring.

Best practice	Affected types	Without best practice
VoIP traffic If the controller feature set allows, limit VoIP traffic on 802.11a to no more than three open connections per AP. Also, allocate a minimum of 7% AP bandwidth to Welch Allyn monitor traffic.	Wireless	Welch Allyn wireless traffic is tagged as VoIP QoS so it has priority in busy environments. For this to be effective, the amount of competing VoIP traffic must be constrained. Failure to allocate AP resources to Welch Allyn monitor traffic could increase patient data loss.
Controller redundancy Wireless controller hardware should include controller redundancy, either one to one or one to many (1:1 or N:1)	Wireless	Failure of a non-redundant controller would cause the entire system to fail.
Critical IT support The customer shall provide 24/7, mission-critical support for their network	Wireless and wired	Possible extended downtime if network support cannot be reached.
DHCP Information <ul style="list-style-type: none"> Primary DHCP Server = Primary server IP address Secondary DHCP Server = Secondary server IP address 	Wireless	Loss of connection and data.
Jitter Packet-to-Packet jitter shall be ≤ 400ms	Wireless and wired	Dropped packets, data loss and dropped connections.
Labeling Welch Allyn VLAN ports should be clearly marked on the physical switches	Wireless and wired	Harder to debug system issues. Mixing of IT and patient data could result in loss of data due to broadcast storms.
Network latency Round-trip peak network latency between a server and its patient monitor ≤800ms	Wireless and wired	Dropped packets and data loss.
Packet transport Packets should be passed through switches and routers in cut-through mode, or hardware based switching, not store-and-forward-only mode (applicable to older switches/hubs)	Wired	Dropped packets and data loss.

Best practice	Affected types	Without best practice
<p>Power redundancy All network equipment used for patient monitoring should have a continuous power supply and emergency power</p>	Wireless and wired	Data loss and downtime due to power outages.
<p>Wired connections Connections between switches, wireless controllers, servers and similar equipment should use gigabit Ethernet. In cases where connections to lower speed ports are unavoidable, do not rely on auto-negotiation. Explicitly configure speed and duplex settings to 100Mbps and Full Duplex.</p>	Wired	Unreliable network connection, and severely affected appliances connected through the interface. Lower speed connection interleaved between high speed connections could introduce bottleneck.
<p>Spanning Tree Protocol (STP) STP should be turned off for the Welch-Allyn specific wireless VLAN/SSID. Enable "port fast" for non-trunked wired interfaces connected to continuous monitors, wireless controllers, or Welch Allyn Servers.</p>	Wireless and wired	Dropped connections.
<p>SSID/Radio settings</p> <ul style="list-style-type: none"> • Radio Beacon Interval set to =100 msec • DTIM set to 10 • Enable short preamble • Disable channel 165 	Wireless	Loss of connection and data, patient monitor will not connect.
<p>WLAN Optimization</p> <ul style="list-style-type: none"> • Controller CPU utilization < 40% • Radio channel utilization < 40% • Number of SSIDs per AP ≤ 4 • Number of clients per AP ≤ 25 • Controller memory utilization ≤ 20Mb • Average RSSI of all clients ≤ -67 dBm • AP Received packet error rate ≤ 10% 	Wireless	When network performance is outside recommended parameters, there is the potential for loss or corruption of data.
<p>Separation Separation distance between wireless devices should be ≥ 2 meters</p>	Wireless	Possible data loss due to increased interference.