Welch Allyn Connex®
Network installation

Best practices overview

Radio software version 3.00.01 and later

Welch Allyn®

Advancing Frontline Care™

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 80018295 Ver B


Welch Allyn Protocol, Inc.
8500 SW Creekside Place
Beaverton, OR 97008-7101 USA

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

www.welchallyn.com

Welch Allyn®

Contents

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

It is up to you to conduct a hazards analysis per IEC 80001 to determine if any issues exist that should be mitigated to ensure patient safety.

Implementation of a stable and usable integrated network is the sole responsibility of the customer. This requirement is found in IEEE Standard 11073-00101, which states:

> Ultimately, the responsibility of ensuring that both medical devices and RF wireless technologies conform to specifications that satisfy necessary and sufficient QoS requirements (conformance) as well as interoperate in a satisfactory way on a shared network system(s) (interoperability) is the responsibility of the end user.

Although it is ultimately your responsibility, Welch Allyn endeavors to participate in your successes with these best practices.

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.

Critical for all Connex products

Best practice	Affected types	Without best practice
Authentication/encryption WEP 64 and 128, WPA2 Personal, WPA2 Enterprise (EAP-TLS, EAP-TTLS, EAP-PEAP [MSCHAPv2])	Wireless	Other encryption methods not supported. No connectivity.
Channel advertisement WLANs using DFS channels must broadcast their SSID	Wireless	The radio will not connect to DFS channels if the SSID is hidden.
Channel Switch Announcement (CSA) Disable	Wireless	When CSA is enabled, data loss when changing channels may occur.
DHCP leases Must be renewable	Wireless and wired	Connections are lost when the lease expires (forced reconnect).
Interference Signal to Noise Ratio (SNR) ≥15dB	Wireless	High noise level causes dropped packets.
IP address assignment Must be performed through DHCP (DHCP fixed to MAC is acceptable)	Wireless and wired	The device cannot connect to the network without an IP address.
Signal strength First wireless signal: RSSI Value ≥-65dBm for (802.11a APs set to 25mW)	Wireless	Dropped packets and loss of connectivity due to poor wireless coverage.
SSID name Maximum length of 16 characters	Wireless	The radio cannot be configured.

Critical for Connex CS and Connex RMS

Best practice	Affected types	Without best practice
Ports allowed • TCP: 281, 283 • UDP: 291, 7711-7719, 44435-44436 (only if Spot LXi is used with Connex)	Wired	Connections cannot be established.
Rendezvous Perform at least one of the following: • Allow UDP broadcasts on ports 7711-7719, or 44435-44436 (only if Spot LXi is used with Connex) • DNS name resolution for Connex servers using a locally configured name • Configure the device with a fixed IP address of the Connex server	Wired	Connections cannot be established from the Welch Allyn VLAN to the server.
SSID/Radio settings • a band Only	Wireless	Loss of connection and data, patient monitor will not connect.

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
Data Keep patient data and general IT data separated using a Stateful Firewall. Rules, policies, and roles should be separated from rules, policies, and rules used for other IT data.	Wireless and wired	IT changes to the firewall policies 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.
802.1X Authentication When using EAP (certificates) for authentication, enable OKC (opportunistic key caching) on the controller	Wireless	Increased chance of disconnect during roaming.
Priority Welch Allyn data should have priority over other data. Welch Allyn data is configured for 802.11e Access Category Voice.	Wireless and wired	Mixing of IT and patient data priority may result in lost data.
QoS Hardware Quality of Service (QoS) support should be configured to map 802.11e QoS bits to a hard-wired tag	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)	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 Welch Allyn patient monitoring are more likely. Patient data subject to issues on wired network such as broadcast storms. Shorter battery life for patient monitors.
Signal strength Second wireless signal: RSSI Value ≥-70dBm for (802.11a APs set to 25mW)	Wireless	Dropped packets and loss of connectivity due to poor wireless coverage.
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
Bandwidth[1] 7% Proportional Bandwidth allocation for APs and Welch Allyn virtual APs/Packet-Shaping	Wireless	Increased probability of dropped patient data packets on busy wireless networks.
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.
DFS DFS channels should not be used with life-critical medical devices	Wireless	Unexpected network outages.
DHCP Information • 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.
Power redundancy All network equipment used for patient monitoring should have a continuous power supply and emergency power	Wireless and wired	Data loss and downtime due to power outages.
SNMP read-only access Welch Allyn servers shall have SNMP read-only access to wireless controllers to log performance data and generate alerts	Wireless and wired	Limited ability to proactively respond to system issues. Debugging by Welch Allyn Remote Technical may not be possible. Extended troubleshooting times.
Spanning Tree Protocol (STP) STP should not run on the Welch Allyn segment of the network. Preferably, use resilient links.	Wireless and wired	Dropped connections.
SSID/Radio settings • 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.
VoIP traffic Limit VoIP traffic on 802.11a to no more than three open connections per AP	Wireless	Having more than three connections per AP has the potential to increase patient data loss.
Wired connection Interconnects between all switches and all WLAN controllers with gigabit Ethernet	Wired	With only 100Mbs connections dropped packets and data loss can occur.

1. The 7% bandwidth allocation will support up to 20 connected Welch Allyn patient monitors per AP. If no Welch Allyn patient monitors are associated with the AP the bandwidth is free to be used by other devices.