Extreme Networks
Dräger Telemetry
SOLUTION GUIDE

Abstract: This document details the optimal configuration of the Extreme Wireless Controller for use with Dräger Patient Monitoring devices.

Published: June 2019
Introduction

Patient monitoring in the healthcare environment is one of the more challenging applications that reside on the network. In the past, telemetry providers installed their own infrastructure hardware to support this demanding, time sensitive, application.

However, the extra costs required for support and maintenance are pushing medical devices onto the corporate network in healthcare. Extreme Networks is committed to work with medical manufacturers to ensure that medical and network equipment is optimized for peak performance.

Dräger, founded in 1889, is an international leader in the fields of medical and safety technology. Extreme Networks together with Dräger have certified interoperability between the Extreme Wireless Controller and access points and Dräger’s Infinity OneNet patient monitoring solution.

Interoperability Summary

Interoperability began prior to Extreme Wireless Controller (EWC) software version 10.x. However, this document will only discuss version 10.01.x and above testing of software and access points.

Also included in this document is Extreme Networks next generation on premise Extreme Cloud Appliance controller which supports Extreme Networks 802.11ac wave 2 access points and the newest 802.11ax access points.

Certification tests included association, authentication, and roaming (where applicable) of the Dräger patient monitoring solution. The testcases were executed on the access points while running a loaded environment with 6 wireless Infinity Delta patient monitors, 12-16 Infinity M300 monitors, 2 IACS patient monitors and various other wired patient monitors as well as other competing traffic.
Test cases were performed in B@AP (bridged at ap) and B@EWC (bridged at controller) modes. Either configuration is acceptable depending on network configuration, but if doing B@EWC, please be cognizant of the traffic loads on the controller and monitor the link(s) for saturation.

Please contact your Draeger or Extreme Networks sales representative for specifics on ap models tests and any caveats to specific access point or software loads.

Dräger equipment was separated via vlans per the test specificaion executed at the Dräger faacility. The table below shows the information that will be relevant to the screen shots provided.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>SSID</th>
<th>Encryption</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>LWAPV4</td>
<td>Y</td>
<td>Infinity network devices w/ multicast (Delta and M540)</td>
</tr>
<tr>
<td>28</td>
<td>LWAPV2</td>
<td>Y</td>
<td>M300 (no multicast)</td>
</tr>
<tr>
<td>29</td>
<td>LWAPV3</td>
<td>N</td>
<td>Initial testing/competing traffic load</td>
</tr>
</tbody>
</table>

The following Extreme Networks versions of software/hardware have been tested.

<table>
<thead>
<tr>
<th>Extreme Wireless Controller</th>
<th>Access Points Tested</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>v10.01.01.x</td>
<td>3825, 3935</td>
<td></td>
</tr>
<tr>
<td>v10.21.06.x</td>
<td>3912</td>
<td></td>
</tr>
<tr>
<td>V10.41.06.x</td>
<td>3915</td>
<td>Covers 39xx family</td>
</tr>
<tr>
<td>V10.51.03.x</td>
<td>3935</td>
<td>Refresh on Extreme Cloud Appliance</td>
</tr>
<tr>
<td>XCA 4.56.02.0030</td>
<td>505/510</td>
<td>Extreme Cloud Appliance</td>
</tr>
</tbody>
</table>

Dräger equipment used:
- Infinity M300 : VF8.10
- Infinity Delta : VF9.1

**Overview**

The Dräger Infinity Delta bedside monitoring solution uses multicast packets for most of its communication. The bedside terminals both transmit and receive multicast traffic in addition to some TCP-based unicast traffic. In normal operation, the bedside terminal sends the multicast traffic to a central station for display and recording of data. However, the Infinity bedside monitors also allow a remote view. This allows one bedside monitor to display data from another bedside monitor simultaneously. This device is 802.11bg only.

The Dräger Infinity M300 device relies on unicast (i.e. TCP) communication to the central monitoring station. The M300 is a portable wireless-only device with a hardened case and rechargeable battery. Infinity M300 uses a standard wifi network supporting 802.11b/g/n (2.4Ghz) and 802.11a/n (5Ghz).
The Dräger M540 patient monitor, when not used with an M500 docking station, is wifi capable and supports 802.11bg only. The M540 is similar to the Delta monitor in that primary communication mechanism is via multicast with some TCP/unicast communications as well.

*Note:* Testing at the Dräger labs did not include the use of Extreme Control or Analytics. However, Extreme Analytics does include signatures for the Dräger Delta and M300 devices.

**Configuration**

This section provides the best practice recommendations for the Extreme Networks configuration with a Dräger deployment. It is important to note that this configuration has been testing the Dräger labs and certified. There maybe other factors that need to be considered in your deployment.

Multicast bridging and wireless Replication must be enabled in order to support the multicast requirements for many of the Dräger telemetry devices. These need to be enabled in order to support the remote view on the Delta monitors since these devices are both consumers and producers of multicast traffic.

In the WLAN settings, the WMM and U-APSD settings need to be enabled. There were issues found using the legacy powersave mode (ps-poll). If legacy powersave must be used then there will be an increased number of retransmissions and a noticeable difference in the duration the M300 device can be used on battery mode. Please use U-APSD powersave mode.

Finally, the radio settings for DTIM period should be set to 1 and a Beacon period set to 100 msec.

Instructions and screenshots are provided below for the Extreme Wireless Controller and Extreme Cloud Appliance.
Configure Topology for Multicast

Extreme Wireless Controller

Navigate to VNS -> Topologies

Select the Topology servicing the Dräger clients
Select the Multicast Filters tab
Extreme Cloud Appliance

Choose the network that needs to have the multicast enabled.
Edit the default VLAN information

Select the advanced button on the VLAN page

Add information for multicast bridging
Configure WLAN Services

Extreme Wireless Controller

Navigate to VNS -> WLAN Services
Select the WLAN Service for the Dräger clients
Select the QoS tab
Check the boxes to ENABLE WMM and U-APSD

Extreme Cloud Appliance

Go to Configure-> Networks
Click on the ADVANCED button toward the bottom of the page.

Enable the U-APSD (WMM-PS) flag and close
Save the configuration once back at the network page.
Configure AP Radio Settings

Extreme Wireless Controller

Navigate to AP tab -> APs
Select the ap(s) that service the Dräger clients (multiedit can be used
Select the Configure -> Radio 2 -> Advanced
Set the DTIM Period and Beacon Period to 100ms
This should be done for Radio2 (2.4Ghz) and Radio1 (5Ghz)
(Note: Screen shot taken when ap was no longer connected to the network. These fields would normally be populated for an active ap).
Extreme Cloud Appliance

Goto Configure->Sites
Select the appropriate SITE
Then, select DEVICE Groups

Edit the Profile

Then, select RADIOS, then ADVANCED
Set the DTIM value to 1